POINT ADDITION ON ELLIPTIC CURVES

DR.S.VASUNDHARA

Abstract: Number theory is a classical discipline in mathematics and has been studied already in ancienttimes. It is the study of relations among the integers. Cryptography is the art of secretlytransmitting information and is as such as old as people trying to hide their secrets. In this paper we discussed the point addition on Elliptic curves over real numbers and finite fields .

Key words: Number theory, Cryptography, Elliptic curves,

Introduction: The use of elliptic curves in cryptography was first proposed by Neil Koblitz and Victor Miller in 1985. Koblitz and Miller did not invent a new cryptographic algorithm but they implemented certain existing algorithms using elliptic curve arithmetic. Since its founding elliptic curve cryptography has been studied a lot in the academic world. The use of elliptic curves in cryptography is very inviting because shorter key lengths can be used than in the case of conventional cryptography e.g. RSA.

As points on an elliptic curve over $GF(2^n)$form a finite group of order $n = E(GF(2^n))$, with the point addition as a group operation. Multiplication over an elliptic curve is defined as in Section it is performed by sequentially adding a point to itself. Multiplication is the basic operation of any elliptic curve cryptosystem and many efficient algorithms to compute it have been developed. All elliptic curve cryptography (ECC) algorithms rely on the fact that calculating the point multiplication *kP*, where *k* is an integer and *P* is a point on an elliptic curve, is relatively easy and fast, but it is a very hard task to calculate *k*, if *P* and *kP* are given. The problem that must be solved, to calculate *k*, is called elliptic curve discrete logarithm problem and it requires an exponential time to solve.

Elliptic curve cryptography has better security with a shorter key length than any other published public-key cryptography method. Elliptic curve cryptosystem with a 173-bit key is considered as secure as RSA using a 1024-bit key and ECC with a 313-bit key is considered as secure as 4096-bit RSA . Elliptic curve cryptography is thus a very attractive alternative, especially in communication systems with limited bandwidth.

Elliptic curves have been studied by mathematicians for more than a century. An extremely rich theory has been developed around them, and in turn they have been the basis of numerous new developments in mathematics. As far as cryptography is concerned, elliptic curves have

been used for factoring and primality proving. The idea of using elliptic curves for public-key cryptosystems is due to Victor Miller [Miller85] and Neal Koblitz [Koblitz87] in the mid-eighties. As with all cryptosystems, and especially with public-key cryptosystems, it takes years of public evaluation before a reasonable level of confidence in a new system is established. The elliptic curve public-key cryptosystems (ECPKCs) seem to have reached that level now. In the last couple of years, the first commercial applications have appeared(email security, web security, smart cards, etc.). Before we look at how the ECPKC s work, we will give a short introduction to elliptic curves

Mathematical of Elliptic Curve Cryptography: Definition of elliptic curves: Elliptic curves are not ellipses. They are called this because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, an elliptic curve is the set of solutions of an equation of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5$ .....(1)

Where the coefficients ai are elements of some field (R, Z or Zp) which satisfy some Simple conditions in order to avoid singularities. Such an equation is said to be Cubic, or of degree 3, because the highest exponent it contains is 3. The Eq.1 is Called Weierstrass*equation*. Also included in the definition of any elliptic curve is a single element denoted O and called *point of infinity* or the *zero point*

An elliptic curve over real numbers may be defined as the set of points (x, y) which satisfy an elliptic curve equation of the form:

$y^2 = x^3 + ax + b$, where x, y, a and b are real numbers.

Each choice of the numbers a and b yields a different elliptic curve. For example, a =1 and b =1 gives the elliptic curve with equation $y^2 = x^3 +x +1$; the graph of this curve is shown below:

If $x^3 + ax + b$ contains no repeated factors, or equivalently if $4a^3 + 27b^2$ is not 0, then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group. An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity.

Figure:1

Elliptic Curve (y2 = x3+x +1)

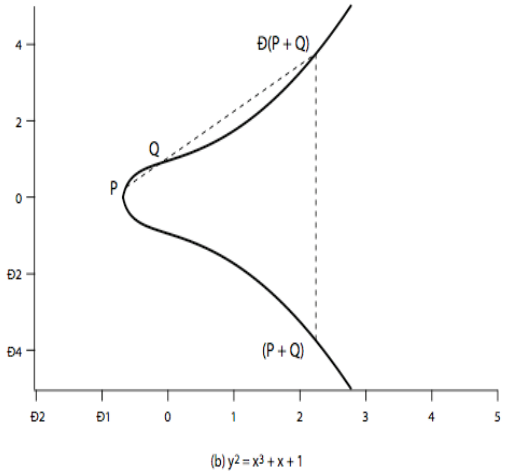

Figure 1.1

2 Point addition: **Elliptic Curve Addition**: A Geometric Approach:

P + Q = R is the additive property defined geometrically.

Elliptic curve groups are additive groups; that is, their basic function is addition. The addition of two points in an elliptic curve is defined geometrically The negative of a point P = (X_1,Y_1) is its reflection in the x-axis: the point -P is $(X_1,-Y_1)$. Notice that for each point P on an elliptic curve, the point -P is also on the curve.

Adding distinct points P and Q :The resulted point of adding two different points on the elliptic curve is computed as shown below in figure 2

When P = (X_1,Y_1) and Q = (X_2,Y_2) are not negative of each other,(X_1,Y_1)+ (X_2,Y_2)= (X_3,Y_3); where $X_1 \neq X_2$ P + Q = R where $\lambda = (Y_2 - Y_1) / (X_2 - X_1)$

$X_3 = \lambda^2 - X_1 - X_2$ and

$Y_3 = -Y_1 + \lambda (X_1 - X_3)$

Note that λ is the slope of the line through P and Q.

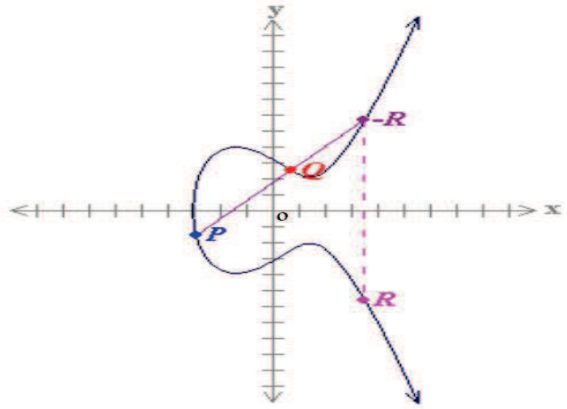

Figure 2.1

Point Addition: Suppose that P and Q are two distinct points on an elliptic curve, and the P is not -Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is P + Q = R..

Shows how a point can be doubled graphically on the elliptic curve. Suppose we want to double a point P on the elliptic curve. A tangent line to the curve and passing by P is taken to double the point. The line must cross the curve through another point; the point is noted as -R. Then we reflect the point –R in the x-axis to the point R where R=2P.

The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point; thus the Elliptic curves over real numbers: $y^2=x^3+ax+b$ with a=9,b=-2

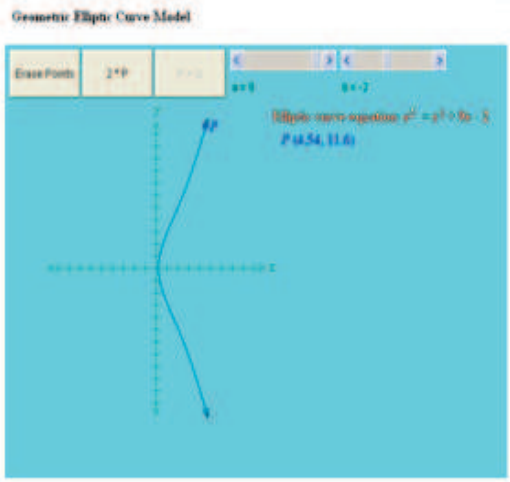

Figure 2.4

y2=x3+ax+b with a=10,b=-10

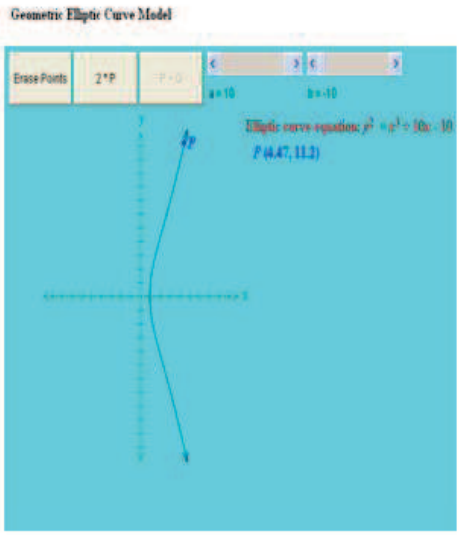

Figure 2.5

Arithmetic in Elliptic Curve Group over F_p Point addition: Note that these rules are exactly the same as those for elliptic curve groups over real numbers with the exception that computations are performed modulo p.

There are several major differences between elliptic curve groups over F_p and over real numbers. Elliptic curve groups over F_p have a finite number of points, which is a desirable property for cryptographic purposes. Since these curves consist of a few discrete points, it is not clear how to "connect the dots" to make their graph look like a curve. It is not clear how geometric relationships can be applied. As a result, the geometry used in elliptic curve groups over real numbers cannot be used for elliptic curve groups over F_p. However, the algebraic rules for the arithmetic can be adapted for elliptic curves over F_p. Unlike elliptic curves over real numbers, computations over the field of F_p involve no round off error - an essential property required for a cryptosystem

The rules for addition over Ep(a,b): Correspond to the algebraic technique described for elliptic curve defined over real numbers. For all points $P,Q \in E_p(a,b)$;

1.P+O=P.

2.If $P=(x_p,y_p)$, then $P+(x_p,-y_p)=O$. The point $(x_p,-yp)$ is the negative of P, denoted as –P. For example , in $E_{23}(1,1)$, for P=(13,7), we have –P=(13,-7).But -7 mod 23=16.Therefore –P=(13,16), which is also in $E_{23}(1,1)$

3.if $P=(x_P,y_P)$ and $Q=(x_Q,y_Q o$ with $P \neq -Q$, then $R=P+Q=(x_R,y_R)$ is determined by the following rules:

$X_R=(\lambda^2-x_P-x_Q) \bmod p$, $Y_R=(\lambda(x_P-x_R)-y_P) \bmod p$

Where

$\lambda=(\frac{y_Q-y_P}{x_Q-x_P}) \bmod p$ if $P \neq Q$

$(\frac{3x_P{}^2+a}{2y_P}) \bmod p$ if P=Q

Multiplication is defined as repeated addition; for example, 4P=P+P+P+P.

For example let P=(3,10) and Q=(9,7) in $E_{23}(1,1)$.Then

$\lambda=(\frac{7-10}{9-3}) \bmod 23=(\frac{-3}{6}) \bmod 23=(\frac{-1}{2}) \bmod 23=11$

xR=(112-3-9) mod 23=109 mod 23=17

y_R=(11(3-17)-10) mod 23=-164 mod 23=20

so P+Q=(17,20).To find 2P

$\lambda\frac{=(3(32)+1}{2x10}) \bmod 23=(\frac{5}{20}) \bmod 23=(\frac{1}{4}) \bmod 23=6$

$y^2=x^3+ax+b$ with finite field over mod 23.

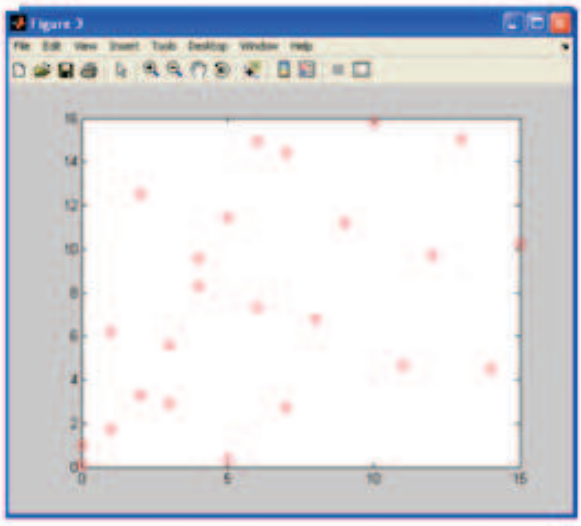

Figure 3.1

References:

1. Certicom, "standards for Efficient Cryptography,SEC 1:Elliptic curve
2. Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSPCBK, Version 2.1.USA: SANS Press, 2003.
3. J.Edge,an introduction to elliptic curve ,cryptography, ttp://Iwn.net/Articles/174127/.2006.
4. N.Koblitz,A course in Number theory and cryptography,2nd ed.,brookes/Cole,1997.
5. J.H.Silverman,The Arithmetic of Elliptic curves, Springer –Verlag,1986

Dr.S.Vasundhara, Asst professor of Mathematics
Gnits. Hyderabad.