IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 10, Issue 6 Ver. V (Nov - Dec. 2014), PP 21-29
www.iosrjournals.org

Encryption on Elliptic Curves over Z_{pq} with Arithmetic on $E(Z_{pq})$ via $E(Z_p)$ and $E(Z_q)$.

P. Anuradha Kameswari, L. Praveen Kumar
Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India.

Abstract : *In the study of Diophantine equations elliptic curves play a vital role due to its application in proof of famous Fermat's Las t Theorem (FLT) and were further developed with its applications in factoring and primality. In this paper we define elliptic curve E(K) over the field K and describe the arithmetic on elliptic curve and give the group law with respect to the characteristic of K.. Due to its group structure and its analogue nature to multiplicative group of a finite field , elliptic curves find their way in enormous applications in cryptography. In this paper we also describe the group law for elliptic curve over a finite ring and propose a public key encryption with elliptic curve over the ring Z_{pq} for p, q are primes.*

Keywords: *Elliptic Curve, Cryptosystem.*

I. Introduction

A rational point is a point (x,y) in a plane with both co-ordinates rational and a line is a rational line if its coefficients are rational. A conic is rational if its equation given as $ax^2+bxy+cy^2+dx+cy+f=0$ with a,b,c,d,e,f are all rational numbers. It is noted that with existence of one rational point there is a method of evaluating all the rational points on the conic by establishing a one to one correspondence with rational points on a line. In the study of rational points on the rational cubics it is noted if the cubic is singular the the method of finding the rational points is based on that of conics. In the extensive research for rational points on rational cubics C, where the cubic is non singular we have the rational points by Mordell's Theorem (1921). It is proved that C has rational points then all rational points form a group that is finitely generated. He proved this by using certain group laws. The cubic of the form $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ is called **Weierstrass generalized** equation and also is named as elliptic curve. These curves arise in the study of arc lengths of ellipses given in terms of elliptic functions.

In the study of rational points on cubic curves it is preferred to study the projective curve version. Any rational solution (x,y) of f(x,y)=0 gives rise to an integral solution (X,Y,Z) of the corresponding homogenous polynomial F(X,Y,Z)=0 and any integer solution (X,Y,Z) with $Z\neq0$ gives a rational solution (X/Z,Y/Z) of f(x,y)=0; and many different integer solutions may lead to same rational solution namely (X,Y,Z) and (tX,tY,tZ) lead to same rational solution (X/Z,Y/Z) and the solutions with $Z=0,X\neq0Y\neq0$ F(X,Y,Z)=0 are said to correspond to solutions " at infinity" and as this gives a clear picture of all solutions of f(x,y)=0 it is preferred to study the projective curve version.

Let *K* be a field then the projective space P_k^2 is the set of all equivalence classes [(X,Y,Z)] for $X,Y,Z\in K$ such that X,YorZ$\neq$0 with the relation (X,Y,Z)(X',Y',Z') iff (X',Y',Z')=(λX,λY,λZ) given as for $\lambda\in$K each equivalence class $[(X,Y,Z)]\in P_k^2$ is called a point and for all $Z\neq0$ the point [(X,Y,Z)] = [X,Y,1] called finite points and the points [X,Y,0] are called points at infinity. Then for any set of zeros of f(x,y) a projective version is obtained by considering the homogeneous polynomial F(X,Y,Z) of degree n with $Z^nf(X/Z,Y/Z)$ = F(X,Y,Z); The set $\{[X,Y,Z]\in P_k^2;\ F(X,Y,Z)=0\}$ = [X,Y,1] $\cup$ [X,Y,0] is the projective version of the zeros of f(x,y). For the Weierstrass equation $Y^2 = X^3+AX+B$ the projective version is the $\{[X,Y,1];\ X,Y\in K,\ Y^2Z = X^3+AXZ^2+BZ^3\} \cup \{[X,Y,0];\ Y^2Z=X^3+AXZ^2+BZ^3\}$ $F(X,Y,0) = 0\Rightarrow X^3 = 0\Rightarrow X=0$. The point at infinity of the Weierstrass equation are given as [(0,Y,0)] = [(0,1,0)] denoting this as ∞ we have the set of all zeros of Weierstrass equation is given as $\{(X,Y)\in K\times K;\ Y^2 = X^3+AX+B\} \cup \{\infty\}$. This set of zeros of the Weierstrass equation on a Field *K* is called the Elliptic curve over the Field *K* is denoted as *E(K).* i.e., *E(K)* = $\{(X,Y)\in K\times K;\ Y^2=X^3+AX+B\} \cup \{\infty\}$

II. Elliptic Curve *E(K)*

The generalized Weierstrass equation for an elliptic curve E is

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6.$$

The discriminant of the curve is defined as

$$\Delta=-b_2^2b_8-8b_4^3-27b_6^2+9b_2b_4b_6, \text{where} \quad b_2=a_1^2+4a_2, b_4=a_1a_3+2a_4, b_6=a_3^2+4a_6,$$

$$b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2,$$

$$c_4=b_2^2-24b_4, c_6=-b_2^3+36b_2b_4-216b_6.$$

The generalized Weierstrass equation for any field K with respect to characteristic of K≠2 can be expressed as $Y^2=X^3+a_2'X^2+a_4'X+a_6'$ with $Y=y+\frac{a_1x}{2}+\frac{a_3}{2}$ and some constants a_2', a_4', a_6'. If the characteristic K≠3 then it can be expressed as $Y^2=X^3+AX+B$ with $X=x+\frac{a_2'}{3}$. This equation is called the Weierstrass equation. Therefore for any field K with characteristic ≠2, 3 the elliptic curve E over K is denoted by *E(K)* and is given as

$$E(K)=\{(x,y)\in K\times K; y^2=x^3+Ax+B\}\cup\{\infty\},$$

where ∞ is the point at infinity and $A,B\in K \text{ such that } 4A^3+27B^2\neq 0$.

Adding points on *E(K)* over a field K of characteristic ≠ 2,3 :

Let $P_1=(x_1,y_1), P_2=(x_2,y_2)$ be two points on elliptic curve E given by the equation $y^2=x^3+Ax+B$. Draw the line L through P_1 and P_2. Then L intersects E in a third point P'_3. Reflect P'_3 across the x-axis to obtain P_3. Now define $P_1+P_2=P_3$.

A Formula to compute P_1+P_2 in terms of the coordinates of P_1 and P_2:

First assume that $P_1\neq P_2$ and that neither point is ∞. Draw the line L through P_1 and P_2. Its slope is

$$m=\frac{y_2-y_1}{x_2-x_1}.$$

Suppose that $x_1\neq x_2$. The equation of L is

$$y=m(x-x_1)+y_1.$$

To find the intersection with E, substitute y to get

$$(m(x-x_1)+y_1)^2=x^3+Ax+B.$$

This can be rearranged to the form

$$x^3-m^2x^2+(-2m^2x_1-2my_1+A)x-m^2x_1^2-y_1^2-2mx_1y_1+B=0.$$

We know that sum of the roots of the cubic equation is the coefficient of $-x^2$. In our case, the two roots of the above cubic equation are x_1 and x_2, we recover the third as $x_3=m^2-(x_1+x_2)$ and $y=m(x_3-x_1)+y_1$.

Now, reflect across the x-axis to obtain the point $P_3=(x_3,y_3)=(x_3,-y)$:

$$x_3=m^2-x_1-x_2,$$

$$y_3=m(x_1-x_3)-y_1.$$

In the case that $x_1=x_2$ but $y_1\neq y_2$, the line through P_1 and P_2 is a vertical line, which therefore intersects E in ∞. Reflecting ∞ across the x-axis yields the same point ∞. Therefore, in this case $P_1+P_2=\infty$.

Doubling of a point:
Now consider the case when $P_1=P_2=(x_1,y_1)$. When the two points coincide, the line through them is a tangent line. Then take the line L to be the tangent line at the point P_1. Implicit differentiation allows us to find the slope m of L:

$$2y\frac{dy}{dx}=3x^2+A, \text{som}=\frac{dy}{dx}=\frac{3x_1^2+A}{2y_1}.$$

If $y_1=0$ then the line is vertical and then $P_1+P_2=\infty$.
Therefore, assume that $y_1\neq 0$. The equation of L is $y=m(x-x_1)+y_1$.
We obtain the cubic equation

$$x^3-m^2x^2+(-2m^2x_1-2my_1+A)x-m^2x_1^2-y_1^2-2mx_1y_1+B=0.$$

This time, we know only one root, namely x_1, but it is a double root since L is a tangent to E at P_1. Therefore, Proceeding as before, we obtain

$$x_3=m^2-2x_1,$$
$$y_3=m(x_1-x_3)-y_1.$$

The addition defined is summarized as group law in the following.
Group Law:

Let E be an elliptic curve defined by $y^2=x^3+Ax+B$ over the field K with characteristic not equal to 2 and 3. Let $P_1=(x_1,y_1)$ and $P_2=(x_2,y_2)$ be two points on E with $P_1,P_2\neq\infty$. Define $P_1+P_2=P_3=(x_3,y_3)$ accordingly as:

1. If $P_1\neq P_2$ with $x_1\neq x_2$, then $x_3=m^2-x_1-x_2$,

$$y_3=m(x_1-x_3)-y_1. \text{ where } m=\frac{y_2-y_1}{x_2-x_1}.$$

If $P_1\neq P_2$ with $x_1=x_2$ but $y_1\neq y_2$ then $P_1+P_2=\infty$.

2. If $P_1=P_2$ and $y_1\neq 0$, then $x_3=m^2-2x_1$, $y_3=m(x_1-x_3)-y_1$, where $m=\frac{3x_1^2+A}{2y_1}$.

If $y_1=0$, then $P_1+P_2=\infty$.

3. We define $P+\infty=P$ for all points P on E. i.e. ∞ is the identity on E.

Example:
Consider the elliptic curve *E* over real numbers and also take the points $P_1=(x_1; y_1)=(2; 9)$ and $P_2=(x2; y2)=(3; 10)$ on it. The line passing through the points P_1 and P_2 is $y=x+7$, where m=1 and k=7.
The third point P_3 on L and *E* is evaluated as follows:

$$x_3=m^2-x_1-x_2=-4,$$
$$y=mx_3+k=3.$$

Then we have $P_1+P_2=(x_3,y_3)=(x_3,-y)=(-4,-3)$.

In computing $2P_1$, we first calculate slope m, $m=\frac{f'(x_1)}{2y_1}=\frac{f'(2)}{18}=\frac{2}{3}$.

Then substituting this value of m in the formula for x_3 and y_3, we have

$$x_3=m^2-2x_1=\frac{-32}{9},$$
$$y_3=m(x_1-x_3)-y_1=\frac{-143}{27}$$
$$2P_1=(x_3,y_3)=\left(\frac{-32}{9},\frac{-143}{27}\right).$$

Adding points on *E(K)* over a field K of characteristic 3 :

If K is a field of characteristic 3, then an elliptic curve over K is the set of points satisfying the equation

$$y^2=x^3+Ax^2+Bx+C,$$

together with a point at infinity ∞.

Let $P_1=(x_1,y_1),P_2=(x_2,y_2)$ be two points on elliptic curve E given by the equation $y^2=x^3+Ax^2+Bx+C$. Draw the line L through P_1 and P_2. Then L intersects E in a third point P'_3. Reflect P'_3 across the x-axis to obtain P_3. Now define $P_1+P_2=P_3$.

A Formula to compute P_1+P_2 in terms of the coordinates of P_1 and P_2:

First assume that $P_1\neq P_2$ and that neither point is ∞. Draw the line L through P_1 and P_2. Its slope is

$$m=\frac{y_2-y_1}{x_2-x_1}.$$

Suppose that $x_1\neq x_2$. Then equation of L is then

$$y=m(x-x_1)+y_1.$$

To find the intersection with E, substitute y to get

$$(m(x-x_1)+y_1)^2=x^3+Ax^2+Bx+C.$$

This can be rearranged to the form

$$x^3+(-m^2+A)x^2+(-2m^2x_1-2my_1+B)x-m^2x_1^2-y_1^2-2mx_1y_1+C=0.$$

We know that sum of the roots of the cubic equation is the coefficient of $-x^2$. In our case, the two roots of the above cubic equation are x_1 and x_2, then we can recover the third as $x_3=(m^2-A)-(x_1+x_2)$ and $y=m(x-x_1)+y_1$. Now, reflect across the x-axis to obtain the point $P_3=(x_3,y_3)$:

$$x_3=m^2-A-x_1-x_2,$$
$$y_3=m(x_1-x_3)-y_1.$$

In the case that $x_1=x_2$ but $y_1\neq y_2$, the line through P_1 and P_2 is a vertical line, which therefore intersects E in ∞. Reflecting ∞ across the x-axis yields the same point ∞. Therefore, in this case $P_1+P_2=\infty$.

Doubling of a point:

Now consider the case when $P_1=P_2=(x_1,y_1)$. When the two points coincide, the line through them is a tangent line. Then take the line L to be the tangent line at the point P_1. Implicit differentiation allows us to find the slope m of L:

$$2y\frac{dy}{dx}=3x^2+2Ax+B, \quad \text{so } m=\frac{dy}{dx}=\frac{3x_1^2+2Ax+B}{2y_1}.$$

If $y_1=0$ then the line is vertical and then $P_1+P_2=\infty$.

Therefore, assume that $y_1\neq 0$. The equation of L is $y=m(x-x_1)+y_1$.

We obtain the cubic equation

$$x^3+(-m^2+A)x^2+(-2m^2x_1-2my_1+B)x-m^2x_1^2-y_1^2-2mx_1y_1+C=0.$$

This time, we know only one root, namely x_1, but it is a double root since L is a tangent to E at P_1. Therefore, proceeding as before, we obtain

$$x_3=m^2-A-2x_1,$$
$$y_3=m(x_1-x_3)-y_1.$$

Adding points on *E(K)* over a field K of characteristic 2 :

For any P∈E(K), define P+∞=P and if Q is the negation of a point P i.e. P+Q=∞, note the x−coordinates in P,Q are equal and the line through P,Q is a vertical line, which intersects E in the point at infinity. We have $Q=(x,y_1)$ and $y^2+(a_1x+a_3)y-(x^3+a_2x^2+a_4x+a_6)=0$ is a quadratic equation in y with roots y, y_1 and the sum of the roots (y,y_1) of a monic quadratic polynomial equals the negative of the coefficient of the linear term, we have $y+y_1=-(a_1x+a_3)$ then $y_1=-a_1x-a_3-y$.

Therefore F is the negation of a point P.

When K is a field of characteristic 2, the elliptic curve over K is the set of points satisfying either $y^2+xy=x^3+a_2x^2+a_6$ or $y^2+a_3y=x^3+a_4x+a_6$ together with a point at infinity.

Adding the points P_1 and P_2:

To add two points P_1 and P_2, draw the line L through P_1 and P_2. It will intersect E in a third point $P_3'=(x,y)$ and compute $P_3=-P_3'=(x,-a_1x-a_3-y)$ then $P_1+P_2=P_3$.

Doubling of a point:

The formula for doubling a point $P=(x_0,y_0)$ in characteristic 2 :

(I) the equation $y^2+xy=x^3+a_2x^2+a_6$ can be expressed as $y^2+xy+x^3+a_2x^2+a_6=0$ and implicit differentiation yields $xy'+(y+x^2)=0$, therefore the slope of the line L through $P=(x_0,y_0)$ is $m=\frac{y_0+x_0^2}{x_0}$ and the line is $y=m(x-x_0)+y_0=mx+b$ for some b. If (x_1,y_1) is the intersection of L and E, we have

$$(mx+b)^2+x(mx+b)+x^3+a_2x^2+a_6=x^3+(m^2+m+a_2)x^2+(1+2m)bx+b^2+a_6=0$$

and as the sum of the roots $x_0+x_0+x_1=m^2+m+a_2$,

$$x_1=m^2+m+a_2=\frac{y_0^2+x_0^4+x_0y_0+x_0^3+a_2x_0^2}{x_0^2}=\frac{x_0^4+a_6}{x_0^2}$$

$$y_1=m(x_1-x_0)+y_0$$

The required point $2P=(x_2,y_2)=-(x_1,y_1)=\left(\frac{x_0^4+a_6}{x_0^2},\ x_1+y_1\right)$.

(II) Next the equation $y^2+a_3y=x^3+a_4x+a_6$ can be rewrite as $y^2+a_3y+x^3+a_4x+a_6=0$. and implicit differentiation yields $a_3y'+(a_4+x^2)=0$, therefore the slope of the line L through $P=(x_0,y_0)$ is $m=\frac{a_4+x_0^2}{a_3}$ and the line is $y=m(x-x_0)+y_0=mx+b$ for some b if (x_1,y_1) is the intersection of L and E,

we have , $(mx+b)^2+a_3(mx+b)+x^3+a_4x+a_6=x^3+m^2x^2+(a_4+2mb+a_3m)x+b^2a_3b+a_6=0$.

and as sum of the roots $x_0+x_0+x_1=m^2$, $x_1=m^2=\frac{x_0^4+a_4^2}{a_3^2}$,

$$y_1=m(x_1-x_0)+y_0.$$

The required point $2P=(x_2,y_2)=-(x_1,y_1)=\left(\frac{x_0^4+a_4^2}{a_3^2},a_3+y_1\right)$.

III. Elliptic curves over Rings

A finite collection $(a_i)_{i\in I}$ of elements of a ring **R** is said to be primitive if it generates **R** as an **R**- ideal i.e., there exists $b_i \in R$; for all $i\in I$ such that $\sum_{i\in I} b_i a_i = 1$. observe that for **R**=Z and Z_n primitive means the $\gcd(a_1,a_2,\ldots)=1$ and $\gcd(n, a_1, a_2,\ldots) = 1$ respectively. To define elliptic curve ***E*** on **R** in normal form and addition law for ***E***. We consider **R** to be a ring satisfying the following

(i) $b\in \mathbf{R}^*$

(ii) For all positive integers n,m and every n×m matrix (a_{ij}) over **R** such that $\{a_{11},a_{12},\ldots,a_{nn}\}$ is positive and all the 2×2 determinants vanish i.e., $\begin{vmatrix} a_{ij} & a_{il} \\ a_{kj} & a_{kl} \end{vmatrix} = 0$ for all $1\le i<k\le n, 1\le j<l\le m$, there exists an **R**- linear combination of rows of (a_{ij}) that is primitive as element in $\mathbf{R}^m$.

Now let the group $G=\mathbf{R}^*$ act on $\mathbf{R}^3$ by the action given as for any $u\in G,(x,y,z)\in \mathbf{R}^*, u*(x,y,z)=(ux,uy,uz)$ and for any $P = (x; y; z) \in \mathbf{R}^3$ denote the orbit G_P as (x:y:z), then the set

$$P^2(R) = \text{Set of orbits GP of G under} \mathbf{R}^3$$
$$=\{(x:y:z);(x,y,z)\in \mathbf{R}^3\}$$

is called the projective plane over **R**. Now we define the elliptic curve **E** over **R** by a homogeneous equation $\boldsymbol{E(R)}=y^2z=x^3+axz^2+bz^3$ with a, b $\in$**R** such that $4a^3+27b^2\in \mathbf{R}^*$ and the points on **E**(R) as $\boldsymbol{E(R)}=\{(x:y:z)\in P^2(\boldsymbol{R}); y^2z=x^3+axz^2+bz\}$. Note that as the condition (ii) is asserted in [8] by a method with an efficient algorithm when **R** is a finite ring, we define the group law in E(**R**) for **R** finite. To add two points $P_1=(x_1:y_1:z_1)$ and $P_2=(x_2:y_2:z_2)$ on $E(\boldsymbol{R})$, consider the polynomial expansions $(q_1:r_1:s_1),(q_2:r_2:s_2)$ in x_1,y_1,z_1,x_2,y_2,z_2,a which can be obtained by repeating the arguments as for the group laws of elliptic curves over fields using the two options for the slope m of the line through P_1 and P_2 for $P_1\neq -P_2$ given as

$$m=\frac{y_1-y_2}{x_1-x_2} \text{ or } m=\frac{x_1^2+x_1x_2+x_2^2+a}{y_1+y_2}$$

and for the points $P_1=\infty=P_2$ i.e., (q_3,r_3,s_3) in the neighborhood (0,0) we obtain a formula that is meaningful as given in [8]. Using the nine polynomial expressions $q_i r_i s_i, i=1,2,3$ we consider the matrix $A=\begin{pmatrix} q_1r_1s_1 \\ q_2r_2s_2 \\ q_3r_3s_3 \end{pmatrix}$ now note this a primitive matrix. For if A generates an ideal $I\neq R$ then we have $I\subseteq M$, M maximal ideal and for P_1,P_2, one of the three formulas is meaningful for P_1+P_2 but for P_1m, P_2m none of the formulas are meaningful for P_1+P_2m in the field R/M.

Further note all the 2×2 determinants of the matrix are zero of the three formulas is meaningful for any P_1,P_2. Hence the hypotheses (ii) is satisfied for the matrix A therefore there exists an R-linear combination of rows $(q_0,r_0,s_0)\in R^3$ that is primitive. Now we define the sum of P_1 and P_2 on E(**R**) as P_1+P_2, where $P_1+P_2=(q_0:r_0:s_0)$. There group laws allow us to work with elliptic curves over rings, the following corollary simplifies the working with elliptic curve over the ring $\boldsymbol{R}=E(Z_n)$.

Corollary:

Let n_1 and n_2 be odd integers with $\gcd(n_1,n_2)=1$. Let E be an elliptic curve defined over $Z_{n_1n_2}$. Then there is a group isomorphism such that, $E(Z_{n_1n_2})\simeq E(Z_{n_1})\oplus E(Z_{n_2})$.[14]

In the next section we construct a cryptosystem exploiting this isomorphism in particular for $R=Z_{pq}$, where p,q are primes. The evaluation of all points on $E(Z_{pq})$ depends on points of $E(Z_p)$ and $E(Z_q)$ which are obtained using the less complicated group laws on elliptic curves over the fields.

IV. Cryptosystem based on arithmetic of Elliptic curve

Let E be an elliptic curve over the finite field F_q and let P and Q be points in $E(F_q)$. The problem of finding an integer n such that Q = nP is called Elliptic Curve Discrete Logarithm Problem (ECDLP). In this section we describe a cryptosystem using ECDLP which is based on arithmetic of elliptic curves over a ring $R=Z_{pq}$ for p, q distinct primes via the arithmetic on $E(Z_p)$ and $E(Z_q)$.

In the following cryptosystem Sender and Receiver generate a common key basing on discrete log of elliptic curves modulo n and then start the communication.

Generating the common key:

- Sender chooses random primes p,q and selects an elliptic curve, $E=E(Z_{pq})=X^3+AX+B$ modulo pq and a point $T=(T_p,T_q)$ on E where $T_p \in E(Z_p)$, $T_q \in E(Z_q)$, also chooses an integer r then makes (E,T,rT) public.
- Receiver chooses an integer s and makes (E,T,sT) public then Sender and Receiver agree upon rsT as secret key.

Encryption:

Sender represents the message, M fixes a random points $G_q \in E(Z_q)$, $G_p \in E(Z_p)$ and encrypts M as $C=M+r(G^q-sT)$, $D=M+r(G^p-sT)$ where $M=(M_p,M_q)$, $M_p \in E(Z_p)$, $M_q \in E(Z_q)$ and $G^q=(\infty,G_q)$, $G^p=(G_p,\infty)$

Then

$$\begin{aligned} C &= M+r(G^q-sT) \\ &= (M_p,M_q)+r((\infty,G_q)-s(T_p,T_q)) \\ &= (M_p-rsT_p,\ M_q+rG_q-rsT_q) \\ &= (C_p,C_q) \end{aligned}$$

$$\begin{aligned} D &= M+r(G^p-sT) \\ &= (M_p,M_q)+r((G_p,\infty)-s(T_p,T_q)) \\ &= (M_p+rG_p-rsT_p,\ M_q-rsT_q) \\ &= (D_p,D_q) \end{aligned}$$

then C,D are made public.

Decryption:

Receiver decrypts the message M by computing C+rsT, D+rsT as

$$\begin{aligned} C+rsT &= (C_p,C_q)+(rsT_p,rsT_q) \\ &= (C_p+rsT_p,\ C_q+rsT_q) \\ &= (M_p,M_q+rG_q) \end{aligned}$$

$$\begin{aligned} D+rsT &= (D_p,D_q)+(rsT_p,rsT_q) \\ &= (D_p+rsT_p,\ D_q+rsT_q) \\ &= (M_p+rG_p,M_q) \end{aligned}$$

Here C+rsT modulo p = M_p, D+rsT modulo q = M_q and retrieve the message $M \in E(Z_{pq})$ by using Chinese Reminder Theorem.

Example: Let p=13, q=11 and Suppose Sender and Receiver agree upon an elliptic curve $E:Y^2=X^3+X+1$ over $Z_{pq}=Z_{143}$

To count the Points on $E(Z_{143})$ we make a list of the possible values of X, then of the square roots Y of X^3+X+1 modulo 13 and modulo 11. The following tables represent the points on $E(Z_{13})$, $E(Z_{11})$ respectively.

X	X^3+X+1	Y	Points
0	1	1,12	(0,1),(0,12)
1	3	4,9	(1,4),(1,9)
2	11	-	-
3	5	-	-
4	4	2,11	(4,2),(4,11)
5	1	1,12	(5,1),(5,12)
6	2	-	-
7	0	0	(7,0)
8	1	1,12	(8,1),(8,12)
9	11	-	-
10	10	6,7	(10,6),(10,7)
11	4	2,11	(11,2),(11,11)
12	12	5,8	(12,5),(12,8)

The points on $E(Z_{13})$ are {(0,1),(0,12),(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),(12,5),(12,8),∞} and $\#E(Z_{13})=18$

X	X^3+X+1	Y	Points
0	1	1,10	(0,1)(0,10)
1	3	5,6	(1,5),(1,6)
2	11	0	(2,0)
3	9	3,8	(3,3),(3,8)
4	3	5,6	(4,5),(4,6)
5	10	-	-
6	3	5,6	(6,5),(6,6)
7	10	-	-
8	4	2,9	(8,2),(8,9)
9	2	-	-
10	10	-	-

The points on $E(Z_{11})$ are {(0,1),(0,10),(1,5),(1,6),(2,0),(3,3),(3,8),(4,5),(4,6),(6,5),(6,6),(8,2),(8,9),∞} and $\#E(Z_{11})=14$.

Generating the common key:

• Sender chooses random primes say 13, 11 and selects an elliptic curve, $E = E(Z_{143}) = X^3 + X + 1$ and a point $T = (T_{13}, T_{11}) = ((4, 2), (1, 6))$ on E where $(4, 2) \in E(Z_{13})$, $(1, 6) \in E(Z_{11})$, also chooses an integer $r = 4$ then makes $(E, T, rT) = (E(Z_{143}), ((4, 2), (1, 6)), 4((4, 2), (1, 6)))$ public.

• Receiver chooses an integer $s = 11$, $(E, T, sT) = (E(Z_{143}), ((4, 2), (1, 6)), 11((4, 2), (1, 6)))$ makes public. Then Sender and Receiver agree upon $rsT = 44((4, 2), (1, 6))$ as secret key.

Encryption:
Sender represents the message as a point $M = (114, 137) \in E(Z_{143})$, fixes random points such as, $G_{11} = (3, 8) \in E(Z_{11})$, $G_{13} = (1, 4) \in E(Z_{13})$ and encrypts M as $C= M + r(G_{11} - sT)$, $D = M + r(G_{13} - sT)$ where $M =((10, 7), (4, 5)), (10, 7) \in E(Z_{13})$; $(4, 5) \in E(Z_{11})$ and take $G_{11} = (\infty, G_{11})$, $G_{13} = (G_{13}, \infty)$ note that $G_{11}, G_{13} \in E(Z_{143})$ and we have,

$$
\begin{aligned}
C &= M + r(G_{11} - sT) \\
&= ((10; 7), (4; 5)) + 4((\infty, (3, 8)) - 11((4, 2), (1, 6))) \\
&= ((10, 7) - 44(4, 2), (4, 5) + 4(3, 8) - 44(1, 6)) \\
&= ((10, 7) + (11, 11), (4, 5) + (0, 10) + (6, 5)) \\
&= ((8, 1) + (4, 6)) \\
&= (C_{13}, C_{11})
\end{aligned}
$$

$$
\begin{aligned}
D &= M + r(G_{13} - sT) \\
&= ((10, 7), (4, 5)) + 4(((1, 4), \infty) - 11((4, 2), (1, 6))) \\
&= ((10, 7) + 4(1, 4) - 44(4, 2), (4, 5) - 44(1, 6)) \\
&= ((10, 7) + (4, 2), (4, 5) + (6, 5)) \\
&= ((8, 12), (1, 6)) \\
&= (D_{13}, D_{11})
\end{aligned}
$$

then C, D are made public.

Decryption:
Receiver decrypts the message M by computing C+rsT, D+rsT as

C+rsT = ((8,1),(4,6))+(44(4,2),44(1,6))
= ((8,1)+44(4,2), (4,6)+44(1,6))
= ((8,1)+(11,2), (4,6)+(6,6))
= ((10,7), (1,5))

D+rsT = ((8,12),(1,6))+(44(4,2),44(1,6))
= ((8,12)+44(4,2), (1,6)+44(1,6))
= ((8,12)+(11,2), (1,6)+(6,6))
= ((8,1), (4,5))

Here C+rsT modulo 13 = M_{13}=(10,7) and D+rsT modulo 11 = M_{11}=(4,5) .
By using Chinese Remainder Theorem, solving the following congruences :

$x \equiv 10 \mod 13$
$x \equiv 4 \mod 11$
and

$y \equiv 7 \mod 13$
$y \equiv 5 \mod 11$

The receiver retrieves the message M = $(x, y) = (114,137) \in E(Z_{143})$

V. Conclusion

In the construction of Elgamal public key encryption with Elliptic curves E over a finite field F_q a message $M \in E(F_q)$ is encrypted as C = M+kB with B = sP for (P, sP) the public key of the receiver and (P, kP) the public key of the sender. The receiver decrypt M as (C−s(kP)) = M + ksP – skP = M. In this context the receiver has to use different random secret key k each time a message M is sent to receiver as in the case when M is sales announcement that is public a day later the Eavesdropper deduces new message M ' as M' = M−C−C' ; where as in the Elgamal like cryptosystem developed in this paper with elliptic curve over Z_n for $n = pq$, same public (P, kP) key be used by the sender for all the further communications also. This construction exploits the isomorphism $E(Z_{pq}) = E(Z_p) \oplus E(Z_q)$ and enables us age of this Elgamal like cryptosystem for a wider usage. The security is same as Elgamal to the discretelog problem for the group $E(F_q)$.

References

[1]. R. Balasubramanian "Elliptic Curves and Cryptography" proceedings of the advanced instructional workshop on Algebraic number theory, HBA (2003)325-345
[2]. I.F.Blake, G. Seroussi and N. P. Smart "Elliptic Curves in Cryptography", volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge, 2000.
[3]. J. Buchmann"Introduction to cryptography" , Springer-Verlag 2001
[4]. Jeffery Hoftstein, Jill Pipher, Joseph H. Silverman, " An Introduction to Mathematical Cryptography", Springer
[5]. D. Husemoller. Elliptic Curves, 2nd edition, volume 111 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2004. With appendices by O. Forster, R. Lawrence, and S. Theisen.
[6]. Neal Koblitz " Algebraic Aspects of Cryptography", volume 3 of Algorithms and Computation in Mathematics. Springer-Verlag, Berlin, 1998.
[7]. Neal Koblitz "A course in number theory and cryptography ISBN 3-578071-8,SPIN 10893308 "
[8]. H.W. Lenstra, JR. Elliptic Curves and Number-Theoretic Algorithms . Proceedings of the International Congress of Mathematicians, Berkeley, California, USA, 1986
[9]. J. H. Silverman. The Arithmetic of Elliptic Curves, volume 106 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.
[10]. J. H. Silerman. Advanced Topics in the Arithmatic of Elliptic Curves, Volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.
[11]. J. H. Silverman. Elliptic curves and cryptography. In Public-Key Cryptography, volume 62 of Proc. Sympos. Appl. Math., pages 91- 112. Amer. Math. Soc., Providence, RI, 2005.
[12]. J. H. Silverman and J. Tate. Rational Points on Elliptic Curves. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992
[13]. R.Thangadurai "Classical Cryptosystems " proceedings of the advanced instructional workshop on Algebraic number theory,HBA (2003)287-301
[14]. Lawrence C. Washington "Elliptic Curves Number Theory and Cryptography" 2nd edition, CRC press
[15]. Lawrence C. Washington, Wade Trappe "Introduction to Cryptography with Coding Theory" 2nd edition, Pearson.