Comparison of Elliptic Curve and Edwards Curve

Shivapriya Hiremath, Stephanie Smith

June 14, 2013

1 INTRODUCTION

In this project we have implemented the Elliptic Curve and Edwards Curve in Java. We compared the execution times of Elliptic Curve and Edwards Curve in Affine Coordinate System, Projective Coordinate System and in Inverted Edwards Coordinate System for different sizes of the curve equations. We also implemented a Random Number Generator using Edwards curve, where in we randomly find a point on the curve or on a unit circle.

2 ELLIPTIC CURVE

An Elliptic Curve (EC) is a smooth, non singular, projective algebraic curve which can be defined by an equation of the form: $y^2 = x^3 + ax + b$ where a and b are real numbers.

Elliptic curve point multiplication is the operation of successively adding a point along an elliptic curve to itself repeatedly. It is used in elliptic curve cryptography (ECC) as a means of producing a trapdoor function. Given the above curve, we define point multiplication as the repeated addition of a point along that curve, denoted as $d[P] = P + P + P + ... + P$ for some scalar (integer) d and a point P = (x, y) that lies on the curve.

In this project, we implement the point multiplication using Binary Multiplication algorithm on various Standard Curves of different sizes, making use of Affine and Projective Coordinate System.

2.1 ELLIPTIC CURVE POINT MULTIPLICATION

In point multiplication a point P on the elliptic curve is multiplied with a scalar d using elliptic curve equation to obtain another point Q on the same elliptic curve i.e. $d[P] = Q$
Point multiplication is achieved by two basic Elliptic curve operations :

1. Point addition, adding two points P and Q to obtain another point R i.e., $R = P + Q$
2. Point doubling, adding a point P to itself to

obtain another point Q i.e., $Q = 2P$

2.2 Affine and Projective Point Notations

Points can be represented in various formats. In this assignment , the point is represented in the :
1.Affine Point Format $(X, Y) = (x, y)$
2.Projective Point Format (Jacobian) $(X, Y) = (x/z^2, y/z^3) = (x, y, z)$

2.3 Binary Method

The binary method is a simple method for point multiplication. The integer d is represented as
$d = d_{n-1}2^{n-1} + d_{n-2}2^{n-2} + ...+ d_1 + d_0$
Where $d_i \varepsilon\{0,1\}$, $n = 0, 1, 2... n-1$
That is $d = \Sigma\, d_j 2^j$, where $d_j \varepsilon$ {0, 1}

This method scans the bits of d either from left-to-right or right-to-left. The binary method for the computation of $d[P]$ on the canonical form of d where $d_i \varepsilon\{0, 1, -1\}$ can be defined for a point P and a scalar value of d as follows:

Algorithm:**Binary Method**
Input: Binary representation of d and point P
$d = (d_{n-1}...d_1 d_0)$, $d_i \varepsilon$ {0, 1, −1}
Output: $d[P]$
1. $Q = P$
2. **for** $i = n-2$ to 0 do
3.1 $Q = 2Q$ (Doubling)
3.2 **if** d_i =1 then
3.3 $Q = Q + P$ (Addition)
4. $i = i - 1$
5. **return** Q

This algorithm has been implemented for both affine point and the projective point notation.

2.4 Addition

Point addition is defined as taking two points along a curve E and computing where a line through them interesects the curve. We use the negative of the intersection point as the result of addition.
The operation is denoted by $P + Q = R$, or $(x_p, y_p) + (x_q, y_q) = (x_r, y_r)$.This can algebraically be calulated by:

$$\lambda = \frac{y_q - y_p}{x_q - x_p}$$

$$x_r = \lambda^2 - a - x_p - x_q$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Where a is the multiplication factor of x^2 in the elliptic field.

2.5 Doubling

Point doubling is similar to point addition, except we take the tangent of a isngle point and find the intersection with the tangent line.

$$\lambda = \frac{3x_p^2 + 2ax_p + b}{2y_p}$$

$$x_r = \lambda^2 - a - 2x_p$$

$$y_r = \lambda(x_p - x_r) - y_p$$

Note that only λ has changed with respect to the point addition problem.

3 Edwards Curve

Edwards proposed a new normal form for elliptic curves and gave an addition law that is remarkably symmetric in the x and y coordinates. The equation of an Edwards curve over a field K is given by :

$$x^2 + y^2 = 1 + dx^2y^2$$

for some scalar $d \in K$ $\{0,1\}$. Also the following form with parameters c and d is called an Edwards curve:

$$x^2 + y^2 = c^2(1 + dx^2y^2)$$

where $c, d \in K$ with $cd(1 - c^4d) \neq 0$.

4 Implementation

4.1 Addition Law

It is possible to add points on an elliptic curve, and obtain another point that belongs to the curve. When two points (x_1, y_1) and (x_2, y_2) on an Edwards curve are added, the result is another point which has coordinates:

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\right)$$

The neutral element of this addition is (0, 1). The inverse of any point (x_1, y_1) is $(-x_1, y_1)$. The point (0, -1) has order 2: this means that the sum of this point to itself gives the "zero element" that is the neutral element of the group law, i.e. 2(0, -1) = (0, 1).

If d is not a square in K, then there are no exceptional points: the denominators $1 + dx_1x_2y_1y_2$ and $1 - dx_1x_2y_1y_2$ are always nonzero. Therefore, the Edwards addition law is complete when d is not a square in K. This means that the formulas work for all pairs of input points on the edward curve with no exceptions for doubling, no exception for the neutral element, no exception for negatives, etc.[1] In other words, it is defined for all pairs of input points on the Edwards curve over K and the result gives the sum of the input points.

If d is a square in K, then the same operation can have exceptional points, i.e. there can be pairs (x_1, y_1) and (x_2, y_2) where $1 + dx_1x_2y_1y_2 = 0$ or $1 - dx_1x_2y_1y_2 = 0$.

One of the attractive feature of the Edwards Addition law is that it is strongly unified i.e. it can also be used to double a point, simplifying protection against side-channel attack. The addition formula above is faster than other unified formulas and has the strong property of completeness [1]

4.2 Example of addition law :

Let's consider the elliptic curve in the Edwards form with $d = 2$

$$x^2 + y^2 = 1 + 2x^2y^2$$

and the point $P_1 = (0, 1)$ on it. It is possible to prove that the sum of P_1 with the neutral element (0,1) gives again P_1. Indeed, using the formula given above, the coordinates of the point given by this sum are:

$$x_3 = \frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2} = 1$$

$$y_3 = \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2} = 0$$

Edwards curves have attracted great interest for several reasons. When curve parameters are chosen properly, the addition formulas use only $10M + 1S$. The formulas are strongly uniïňĄed, i.e., work without change for doublings; even better, they are complete, i.e., work without change for all inputs.

4.3 Inverted Edwards coordinates

The Edwards curve equation can be written using projective coordinates as:

$$(X^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$$

An inverted Edwards point $(X_1 : Y_1 : Z_1)$ corresponds to the affine point $(Z_1/X_1, Z_1/Y_1)$ on the Edwards curve.It is easy to convert from standard Edwards coordinates $(X_1 : Y_1 : Z_1)$ to inverted Edwards coordinates: simply compute $(Y_1Z_1 : X_1Z_1 : X_1Y_1)$ with three multiplications. The same computation also performs the opposite conversion from inverted Edwards coordinates to standard Edwards coordinates. The addition formulas for inverted Edwards coordinates use only $9M + 1S$. The formulas are not complete but still are strongly unified. Inserting Z_i/X_i for x_i and Z_i/Y_i for y_i in the Edwards addition law (assuming $X_iY_iZ_i \neq 0$) we obtain

$$\begin{aligned}&\left(\frac{Z_1}{X_1}, \frac{Z_1}{Y_1}\right) + \left(\frac{Z_2}{X_2}, \frac{Z_2}{Y_2}\right)\\ &= \left(\frac{(X_2Y_1 + X_1Y_2)Z_1Z_2}{X_1X_2Y_1Y_2 + dZ_1^2Z_2^2} mod p, \frac{(X_1X_2 - Y_1Y_2)Z_1Z_2}{X_1X_2Y_1Y_2 - dZ_1^2Z_2^2} mod p\right)\\ &= \left(\frac{Z_3}{X_3}, \frac{Z_3}{Y_3}\right)\end{aligned} \tag{4.1}$$

where

$$X_3 = (X_1X_2 - Y_1Y_2)(X_1X_2Y_1Y_2 + dZ_1^2Z_2^2)$$

$$Y_3 = (X_2Y_1 + X_1Y_2)(X_1X_2Y_1Y_2 - dZ_1^2Z_2^2)$$

$$Z_3 = (X_1X_2 - Y_1Y_2)(X_2Y_1 + X_1Y_2)Z_1Z_2$$

This shows the idea behind inverted Edwards coordinates, namely that in this representation only Z_3 needs to be multiplied with Z_1Z_2, which saves 1M in total.

5 Random Number Generator

A Random Number Generator can be implemented using the Edwards Curve.

5.1 RNG 1 : Edwards Curve onto unit circle

A point (x, y) on the Edwards curve Ed projects to the point (u, v) in the same quadrant on the unit circle as $(u, v) = (\alpha x, \alpha y)$, where

$$\alpha = \frac{1}{\sqrt{x_2 + y_2}}$$

5.2 RNG 2 : Unit circle onto Edwards Curve

A point (u, v) on the unit circle projects back to the point (x, y) in the same quadrant on the Edwards curve Ed as $(x, y) = (\beta u, \beta v)$, where,

$$\beta = \frac{\sqrt{2}}{\sqrt{1 + \sqrt{1 - 4du^2v^2}}}$$

5.3 RNG 3 : Edwards Curve onto Edwards Curve

A point (x_0, y_0) on the Edwards curve Ed_0 projects to the point (x_1, y_1) in the same quadrant on the Edwards curve Ed_1 as $(x_1, y_1) = (\gamma x_0, \gamma x_1)$, where

$$\gamma = \frac{\sqrt{2}}{\sqrt{x_0^2 + y_0^2 + \sqrt{(x_0^2 + y_0^2)^2 - 4d_1x_0^2y_0^2}}}$$

6 Results and Conclusion

From the figure 6.1 the resulting times are to be expected. Based on our results we find that elliptic affine takes the longest of all the three. Edwards affine improves on time because there is a smaller amount of additions. Elliptic Projective improves on time because there are no required divisions. Edwards Inverted is the fastest because there are

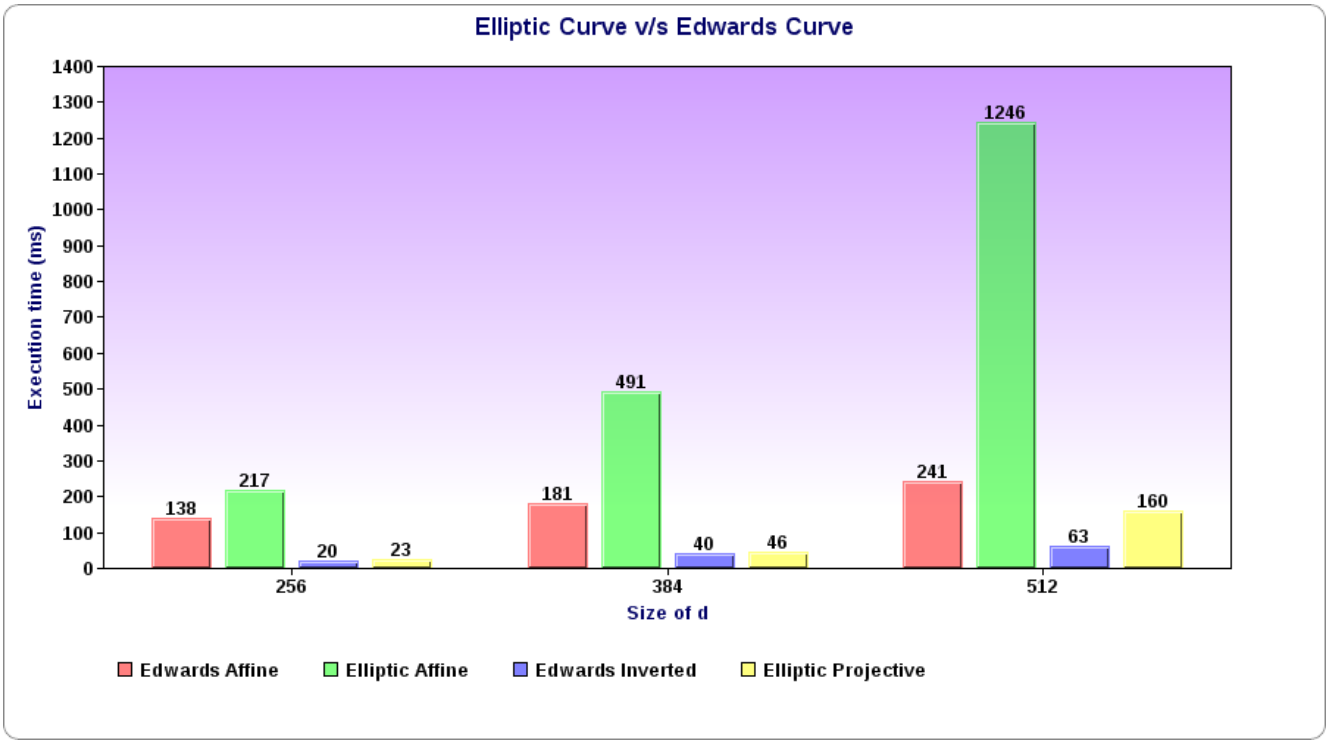

Figure 6.1: Comparison of Elliptical and Edwards Curve

no division and there is a smaller amount of multiplications.
We also ran times for random number generator and found that Unite cirle onto Edwards Curve takes the shortest amount of time, and Edwards Curve onto Edwards Curve take the longest amount of time.

7 REFERENCES

[1]Bernstein, Daniel J., and Tanja Lange. "Faster addition and doubling on elliptic curves." Advances in cryptology-ASIACRYPT 2007. Springer Berlin Heidelberg, 2007. 29-50.

[2]Edwards, Harold. "A normal form for elliptic curves." Bulletin of the American Mathematical Society 44.3 (2007): 393-422

[3]http://galg.acrypta.com/index.php

[4]http://cs.ucsb.edu/~koc/ac/docs/w03/ecc-protocols.pdf

[5]http://cs.ucsb.edu/~koc/ac/docs/w04/09-ecc.pdf

[6]http://cs.ucsb.edu/~koc/ac/docs/wpp/rng/rng.pdf