$\boxed{3}$

Cryptography I
Homework sheet 10

Erwin van Duijnhoven 0719562

Rick Staals 0716184

December 4, 2013

Question 1

State projective doubling formulas for Edwards curves taking $3M + 4S$, i.e. give the result and suitable sub-expressions to compute $(X_3 : Y_3 : Z_3)$ given $(X_1 : Y_1 : Z_1)$.

0/5

Solution:

Doubling means that we have to compute $2(x, y)$ for x and y on the Edwards curve.

$$2(x,y) = \left(\frac{2xy}{x^2+y^2}, \frac{y^2-x^2}{2-x^2-y^2}\right)$$

For this we use the representation $(X_1 : Y_1 : Z_1)$ where $x = \frac{X_1}{Z_1}$ and $y = \frac{Y_1}{Z_1}$

$$\begin{aligned}
\tilde{A} &= \frac{X_1^2}{Z_1^2} \\
\tilde{B} &= \frac{Y_1^2}{Z_1^2} \\
\tilde{C} &= \frac{2X_1Y_1}{Z^2} \\
\tilde{D} &= \tilde{A} + \tilde{B} \\
2 - \tilde{D} &= \frac{2Z_1^2 - X_1^2 - Y_1^2}{Z_1^2}
\end{aligned}$$

$$\begin{aligned}
A &= X_1^2 \\
B &= Y_1^2 \\
E &= Z_1^2 \\
C &= 2Y_1 \cdot X_1 \\
X_3 &= C \cdot (2E - A - B) \\
Y_3 &= (B - A) \cdot (A + B) \\
Z_3 &= \cancel{2(A+B) - (A+B)^2} \\
&\quad (A+B)(2E - A - B)
\end{aligned}$$

You did not use E

write $2X_1Y_1 = (X_1+Y_1)^2 - A - B$ to replace a multiplication by a square

Show that $\left(\frac{X_3}{Z_3}, \frac{Y_3}{Z_3}\right) = 2 \cdot \left(\frac{X_1}{Z_1}, \frac{Y_1}{Z_1}\right)$

Which uses 3 multiplications and 4 squarings.

Question 2

Compute the twisted Edwards curve corresponding to the Montgomery curve $v^2 = u^3 + 486662u^2 + u$ over $\mathbb{F}_{2^{20}-3}$.

3/5

The point $P = (2, 117777)$ is on the Montgomery curve. Compute the point corresponding to $2P$ on the twisted Edwards curves by

(a) computing $2P$ on the Montgomery curve and mapping the results to the twisted Edwards cure and

(b) computing the point P' corresponding to p on the Edwards curve and then computing $2P'$ on the twisted Edwards curve.

The results from these two ways of computing should be equal. Check that they are on the twisted Edwards curve.

Solution:

We calculate everything modulo $2^{20} - 3 = 1048573$.

First we want to compute the corresponding Edwards curve. We know that

$$486662 = 2\left(\frac{a+d}{a-d}\right)$$

$$1 = \frac{4}{a-d}$$

so

$$a = 486664$$

$$d = 486660$$

That's quick! How did you determine a and d?

so the corresponding twisted Edwards curve is

$$486664x^2 + y^2 = 1 + 486660x^2y^2$$

(a) Because we are doubling P we use

$$\lambda = \frac{3x_P^2 + 2 \cdot 486662 \cdot x_P + 1}{2y_P}$$

$$x_{2P} = B\lambda^2 - A - x_P - x_P$$

$$y_{2P} = \lambda(x_P - x_{2P}) - y_P$$

Therefore, $\lambda = 23125$, $x_{2P} = 555302$ and $y_{2P} = 443254$.

Now map this to the twisted Edwards curve

(b) First we calculate P':

$$P' = \left(\frac{u}{v}, \frac{u-1}{u+1}\right) = \left(\frac{2}{117777}, \frac{1}{3}\right) = (2 \cdot 325682, 699049) = (651364, 699049)$$

Because we are doubling P', we use the doubling calculation on the Edwards curve.

$$(x_{2P'}, y_{2P'}) = \left(\frac{2 \cdot 651364 \cdot 699049}{486664 \cdot 651364^2 + 699049^2}, \frac{699049^2 - 486664 \cdot 651364^2}{2 - 486664 \cdot 651364^2 - 699049^2}\right)$$

$$= \left(\frac{783767}{205448}, \frac{610109}{843127}\right) = (883728, 62341)$$

$$\left(P = \left(\frac{1 + y_{2P'}}{1 - y_{2P'}}, \frac{1 + y_{2P'}}{(1 - y_{2P'})x_{2P'}}\right) = \left(\frac{62342}{986232}, \frac{62342}{421900}\right) = (555302, 443254) \right)$$

Both methods give the same result but via the Montgomery curve the calculations were a lot quicker.

Check and show that (883728, 62341) indeed lies on the twisted Edwards curve