Cryptography I, homework sheet 10
Due: 4 December 2014, 10:45

Team up in groups of two or three to hand in your homework. We do not have capacity to correct all homeworks individually. To submit your homework, email it to crypto14@tue.nl or place it on the lecturer’s table before the lecture. Do not email Tanja or put homework in mailboxes.

For this homework you may use a computer or calculator only for the arithmetic in $\mathbb{F}_{13}$.

1. Find all points $(x_1, y_1)$ on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Verify that $P = (6, 3)$ and $Q = (3, 7)$ are on the curve. Compute $R = 2P + Q$.

2. Let $(X_1 : Y_1 : Z_1)$ and $(X_2 : Y_2 : Z_2)$ be projective input points to the Edwards addition. Use the affine formulas $(x_3, y_3) = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1y_1x_2y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1y_1x_2y_2}\right)$ to determine $(X_3 : Y_3 : Z_3)$ with $x_3 = \frac{X_3}{Z_3}$ and $y_3 = \frac{Y_3}{Z_3}$. How many squarings and multiplications does the computation need? Note, you should try to find common subexpressions and compute them only once.