Cryptography I, homework sheet 10

Due: 05 December 2013, 10:45

Please submit your homework electronically; the TAs do not want to receive homework on paper. Please bundle your scans into one pdf file. 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 `crypto13@tue.nl`.
In general, you may use computer algebra systems such as mathematica and sage; please submit your code as part of your homework if you end up using a system. Accepted systems/languages: Sage, mathematica, matlab, Pari-GP, Java.

Before the exam please train yourself in doing moduluar arithmetic. Better calculators are programmabge and is useful for you to teach it to do arithmetic modulo numbers; also XGCD is a useful program to implement. Do this before the exam. Of course you can also print and bring huge multiplication tables and hope that I use those numbers. My exercises will not assume that you have polynomial arithmetic.

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 $(X_1 : Y_1 : Z_1)$.

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

Take a look at `http://hyperelliptic.org/tanja/vortraege/20110307.pdf` to learn how to use the fast negation on elliptic curves to speed up Pollard's rho method. The first few slides should look very familiar to you. The only difference is that the rho method is written additively instead of multiplicatively.