Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Thursday, 14.09.2006

Index-calculus-HEC exercises

[ICH1] Given an elliptic curve $E/\mathbb{F}_q : y^2 = x^3 + ax + b$, we could try a substitution $\tilde{x} = x^d$ to embed E into a hyperelliptic curve C and then solve the discrete logarithm problem in the group $\mathrm{Pic}^0_C(\mathbb{F}_q)$ using index calculus. Why doesn't that give a faster attack for the ECDLP?
Hint: What genus would you need for C?

[ICH2] Assuming the number of prime divisors of degree d is $\sim \frac{1}{d}q^d$, explain why we use all prime divisors of degree $\leq B$ (smoothness bound) even though removing those of degree $\leq B/2$ would reduce the size of the factor base, and therefore of the cost to solve the linear algebra problem.

[ICH3] Find all prime divisors of degree ≤ 3 of

$$y^2 + y = x^{19} + x^{17} + x + 1$$

defined over $\mathbb{F}_2$.

CM2 exercises

[CM21] Use the Tonelli-Shanks Algorithm to compute the square root of 17 modulo $p = 101$.

[CM22] Use Cornacchia's algorithm to compute integers $x, y \in \mathbb{Z}$ that satisfy $x^2 + 7y^2 = 4 \cdot 23$.

[CM23] Let $E_a : Y^2 = X^3 + aX - a$ be an elliptic curve defined over $\mathbb{F}_p$ and define $P = (1, 1) \in E_a(\mathbb{F}_p)$. Suppose that we both have $(p + 1 - t)P = 0$ and $(p + 1 + t)P = 0$. Show that the order of P is bounded by $4\sqrt{p}$.

Fast-HEC exercises

[FHEC1] Let $C : y^2 + h(x)y = f(x)$ be a genus 2 curve over $\mathbb{F}_{2^n}$. Give a relation between the degree of h and the 2-torsion group.

[FHEC2] Let $I_1 = \langle u_1(x), y - v_1(x)\rangle, I_2 = \langle u_2(x), y - v_2(x)\rangle$ be ideals in $\mathbb{F}_q[x, y]/(y^2 + h(x)y - f(x))$. Compute the product and show how to represent it with two generators.

[FHEC3] Use Cantor's algorithm to derive the explicit formulae for elliptic curves.

Parings-I exercises

[PI1] Let $G_1 = \langle P \rangle$ be a group of prime order ℓ and let there exist two more groups G_1' and G of the same group order so that there exists a pairing

$$e : G_1 \times G_1' \to G.$$

Show how to use the pairing to transfer the DLP in G_1 to the DLP in G_1'.

[PI2] Show that the Tate-Lichtenbaum pairing is bilinear in the second argument. You may use that the pairing is well defined.

[PI3] In **PC2** we saw that for $p \equiv 2 \bmod 3$ the curve $E_b/\mathbb{F}_p : y^2 = x^3 + b$ has $|E_b(\mathbb{F}_p)| = p + 1$. Compute the embedding degree for this curve and show how it can be used in ID-based cryptography, i.e. show how one can map arbitrary ID strings to points on $E_b(\mathbb{F}_p)$. Note that that is enough since there is a *distortion map* $\varphi : E_b(\mathbb{F}_p) \to E_b(\mathbb{F}_{p^2})$ defined by $\varphi(x, y) \mapsto (x, \xi_3 y)$ mapping to $E_b(\mathbb{F}_{p^2}) \setminus E_b(\mathbb{F}_p) \cup \{P_\infty\}$.