Summer School on Elliptic and Hyperelliptic Curve Cryptography

Exercises for lectures on Thursday, 17.09.2008

Hyperelliptic curves

[HEC1] Let $C : y^2 = x^5 + 3x^3 + 1$ over $\mathbb{F}_7$.

a) Find 4 different points P_1, P_2, P_3, and P_4 on $C(\mathbb{F}_7)$.

b) Perform Cantors algorithm to add $D_1 = P_1+P_2-2P_\infty$ and $D_2 = P_3+P_4-2P_\infty$.

c) Extract the 1 or 2 new points of $D_1 + D_2$ and check if they lie on C and whether they are in $C(\mathbb{F}_7)$.

[HEC2] Let C be a genus-g hyperelliptic curve defined over a field K. In the lecture we defined $\mathrm{Pic}^0_C(\bar{K})$. In cryptography we consider finite fields $K = \mathbb{F}_q$ and restrict attention to the subgroup of $\mathbb{F}_q$-rational divisor classes, that are divisor classes which are left invariant under the q-power Frobenius map.

Let $\bar{D}$ be an $\mathbb{F}_q$-rational divisor class.

a) Find the field of definition of the polynomials in Mumford representation.

b) Each class can be represented as $\sum_{i=1}^{r} P_i - rP_\infty$ with affine points $P_i \in C(\bar{\mathbb{F}}_q)$ such that $P_i \neq -P_j$ for any $i \neq j$. Over which field are these points defined for a genus-2 curve? Where for a genus-3 curve? Where for a genus-g curve?

Pairings I

[P1] Let $E/\mathbb{F}_p$ be an elliptic curve, r a large prime dividing $\#E(\mathbb{F}_p) = p + 1 - t$. Show that k is the embedding degree of E with respect to r, if and only if $r \mid \Phi_k(t-1)$.

[P2] Show that for the Weil pairing $e(Q, P) = e(P, Q)^{-1}$.

[P3] a) Assume $k > 1$. Show that when computing the reduced Tate pairing we can multiply the functions in Miller's algorithm by any $a \in \mathbb{F}_{p^d}$ for $d \mid k$, $d \neq k$ without changing the pairing value.

b) Show that $t_r(P, P) = 1$ for $P \in E[r](\mathbb{F}_p)$ and $k > 1$.

[P4] Show that the final exponentiation is a group isomorphism $\mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r \to \mu_r$.

[P5] How can you construct a hash function $H : \{0,1\}^* \to E[r](\mathbb{F}_p)$ which can be used in the BLS signature scheme? Start from a given hash function $h : \{0,1\}^* \to \{0,1\}^l$ for some fixed bit-length l.

[P6] Describe tripartite key agreement 1) using an extension of the Diffie-Hellman protocol without pairings and 2) using an asymmetric pairing like the reduced Tate pairing on ordinary curves.