Master CSI, AGTN/ALGANT 2018-2019

Courbes elliptiques — 4TMA902U

Responsables : G. Castagnos, D. Robert

Supersingular curves and pairings

Let p be a prime number with $p > 3$ and $p \equiv 2 \pmod 3$. We denote by E the elliptic curve of equation $y^2 = x^3 + 1$ over $\mathbf{F}_p$.

1 Choose a prime number p and define this curve with Sage. Compute its number of points with Sage.

2 Show that $x \mapsto x^3 + 1$ is a permutation of $\mathbf{F}_p$, and that $E(\mathbf{F}_p)$ has $p + 1$ points.

3 Show that there exists $\zeta \neq 1 \in \mathbf{F}_{p^2}$ such that ζ is a solution of $x^3 - 1 = 0$. We denote by ϕ the map that sends a point $Q = (x, y)$ of $E(\mathbf{F}_p)$ to $\phi(Q) = (\zeta x, y)$ and sends O_E to itself. Prove that $\phi(Q) \in E(\mathbf{F}_{p^2})$. We assume that ϕ is a morphism for the group law of the points of the curve.

In the following, we denote $\ell > 3$ a prime factor of $p + 1$ and $G = \langle P \rangle$ with P a point of $E(\mathbf{F}_p)$ of order ℓ.

4 Implement a function that takes an integer λ as input, and that outputs (with the previous notations) ℓ of λ bits, p, P and ζ.

5 Write a function computing ϕ.

6 Show that the embedding degree of ℓ in $\mathbf{F}_p$ is 2. Show that P and $\phi(P)$ generate the ℓ−torsion of the curve E. Verify it on a small example.

7 Let $e_{w,\ell}$ the Weil pairing. We define the modified Weil pairing , $\hat{e}_{w,\ell} : G \times G \to \mu_\ell \subset (\mathbf{F}_{p^2})^\times$ by

$$\hat{e}_{w,\ell}(P, Q) = e_{w,\ell}(P, \phi(Q)).$$

Show that $\hat{e}_{w,\ell}$ is bilinear and non degenerate.

8 Write a function that computes this pairing. Verify its properties on a small example.

9 Use this pairing to reduce a discrete logarithm computation from $E(\mathbf{F}_p)$ to $\mathbf{F}_{p^2}$.

10 Use this pairing to do a tripartite key exchange.