Courbes elliptiques — 4TMA902U

Responsables : G. Castagnos, D. Robert

Barreto-Naehrig curves and BLS signature

Barreto and Naehrig have proposed in 2005 a family of elliptic curves of equation $y^2 = x^3 + b$ over $\mathbf{F}_p$ with $p = 36u^4 + 36u^3 + 24u^2 + 6u + 1$. For some choices of u and b, these curves are such that $\ell = Card(\mathrm{E})$ is a prime number equal to $36u^4 + 36u^3 + 18u^2 + 6u + 1$.

In the following, we consider the elliptic curve BN254 which corresponds to the choice of $u = -(2^{62} + 2^{55} + 1)$ and $b = 2$. We denote E this curve.

1 Verify with Sage that this choice of u gives a prime p and a curve of prime order ℓ. What is the value of k, the embedding degree ? Can we use this curve for cryptographic applications ?

2 Find two points P and T that generate the ℓ−torsion, with $\mathrm{P} \in \mathrm{E}(\mathbf{F}_p)$ and $\mathrm{T} \in \mathrm{E}(\mathbf{F}_{p^k})$.

3 Write a function that computes the trace of a point of the curve $\mathrm{E}(\mathbf{F}_{p^k})$. Find a point Q of ℓ−torsion of trace O_E.

4 Let $\mathrm{G}_1 = \langle \mathrm{P} \rangle$, $\mathrm{G}_2 = \langle \mathrm{Q} \rangle$ and G_T the subgroup of ℓ−th roots of unity of $\mathbf{F}_{p^k}$. The reduced Tate pairing defines a type 3 pairing $\mathrm{G}_1 \times \mathrm{G}_2 \to \mathrm{G}_\mathrm{T}$. Verify its properties on examples.

5 With the hash function h that we have used for ECDSA, we want to define and hash function H with values in G_1. For that, we set $i = 0$ and compute $x \| a = h(m \| i)$ with $x \in \mathbf{F}_p$ and $a \in \{0, 1\}$. If $x^3 + b$ is a square in $(\mathbf{F}_p)^\times$ we denote y_0 and y_1 its square roots with $0 < y_0 < y_1 < p$. We set $\mathrm{H}(m) = (x, y_a)$. If $x^3 + b$ is not a square, set $i \to i + 1$.

6 The signature scheme BLS (Boneh, Lynn, Shacham, 2001) with a type 3 pairing is as follows : The secrete key is a random integer $x < \ell$. The public key is the point $\mathrm{U} = x\mathrm{Q} \in \mathrm{G}_2$. To sign m, we compute $\sigma = x\mathrm{H}(m) \in \mathrm{G}_1$. What problem an adversary must solve in order to forge a signature of m without knowing x ? Find the corresponding verification algorithm and implement this signature scheme.