Women in Mathematics
Advanced Course : Review Session 2

Let B be a quaternion algebra and E an supersingular elliptic curve whose endomorphism ring is an order $\mathcal{O} \subset B$. We recall that the security of isogeny-based cryptosystems relies on the hardness of several problems.

Problem 1. *Given an elliptic curve E, compute the endomorphism ring* $\mathrm{End}(E)$.

Problem 2. *Given two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, find an efficiently computable isogeny $\phi : E \to E'$.*

The goal of this review session is to prove a reduction from **Problem 2** to **Problem 1**.
Let I be a left $\mathcal{O}$-ideal. We define

$$E[I] = \{P \in E(\bar{\mathbb{F}_p}) | \alpha(P) = 0, \text{ for all } \alpha \in I\}.$$

We define $\phi_I : E \to E_I$ the isogeny with kernel $E[I]$.

Exercice 1.

1. The pullback map

$$\begin{array}{rcl} \phi_I^* : Hom(E_I, E) & \to & I \\ \psi & \to & \psi\phi_I \end{array}$$

   is an isomorphism of $\mathbb{Z}$-modules.
2. Let $\mathcal{O}' = \mathrm{End}(E_I)$. Show that I is a right $\mathcal{O}'$-ideal.
   Hint : Use the embedding

$$\begin{array}{rcl} \iota : \mathrm{End}(E_I) & \to & B \simeq \mathrm{End}(E) \otimes \mathbb{Q} \\ \iota(\beta) & = & \frac{1}{\deg \phi_I}(\hat{\phi_I}\beta\phi_I). \end{array}$$

Exercice 2. Show that :

1. Given an isogeny $\phi : E \to E'$ between two supersingular elliptic curves, there exists a left $\mathcal{O}$-ideal I and an isomorphism $\rho : E_I \to E'$ such that $\phi = \rho\phi_I$.
2. For every maximal order $\mathcal{O}' \subset B$ there exists E' such that $\mathcal{O}' \simeq \mathrm{End}(E')$.

Exercice 3. Let E and E' be two supersingular elliptic curves and assume that there is an efficient algorithm for computing $\mathrm{End}(E)$ and $\mathrm{End}(E')$. Prove that there is an algorithm which computes a path in the ℓ-isogeny graph between E and E'. For this, we will assume known the following result :

Theorem. [Kohel-Lauter-Petit-Tignol] Given two orders $\mathcal{O}$ and $\mathcal{O}'$ in a quaternion algebra B, there is an probabilistic polynomial time algorithm for computing an ideal I of reduced norm ℓ^k connecting $\mathcal{O}$ and $\mathcal{O}'$ (We say that an ideal I connects $\mathcal{O}$ and $\mathcal{O}'$ if I is a left $\mathcal{O}$-ideal and a right $\mathcal{O}'$-ideal.