LECTURE 2: Reductions between hard problems in isogeny-based cryptography

PROBLEM 1 (ℓ-Isogeny Path): Given primes $p \neq \ell$ and E_1, E_2 sup. sing. ell curves over $\mathbb{F}_{p^2}$, find a path from E_1 to E_2 in $G(p, \ell)$.

DEFNS: R = domain with field of fractions F
B = fin dim'l F-algebra

- $M \subseteq B$ is an R-lattice if M is fin. gen. as an R-module and $MF = B$.
- An R-order $\mathcal{O} \subseteq B$ is an R-lattice that is also a subring of B.
- An order $\mathcal{O} \subseteq B$ is maximal if it is not properly contained in another order.
- char $F \neq 2$ An F-algebra B is a quaternion algeba if there is an F-basis $1, i, j, ij$ for B s.t. $i^2 = a$, $j^2 = b$, $ji = -ij$ for some $a, b \in F^\times$.

Such a B

<u>ramifies</u> at a prime q (resp ∞) if $B \otimes \mathbb{Q}_q$ (resp. $B \otimes \mathbb{R}$) is a division algebra.

Otherwise, B is <u>split</u> at q (resp ∞)

In this case $B \otimes \mathbb{Q}_q \simeq M_2(\mathbb{Q}_q)$ (resp. $B \otimes \mathbb{R} \simeq M_2(\mathbb{R})$).

E supersing. ell curve in char p.

$\mathrm{End}(E)$ is a maximal order in $B_{p,\infty}$; $B_{p,\infty}$ = unique quat. alg. over $\mathbb{Q}$ ramified exactly at p and ∞.

<u>Deuring</u> <u>correspondence</u>:

$$\{\text{maximal orders in } B_{p,\infty}\}/\sim \;\longleftrightarrow\; \{j \in \mathbb{F}_{p^2} : j = j(E) \text{ for supersingular } E\}/\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$$

PROBLEM 2 (EndRing)
Given sup. sing. $E/\mathbb{F}_{p^2}$, find four endomorph. of E, given in an eff. repres., that generate $\mathrm{End}(E)$.

PROBLEM 3 (MAX ORDER) Given E as before, find an order in $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$.

PROBLEM 4 (ISOGENY) Given E_1, E_2 sup. sing over $\mathbb{F}_{p^2}$, find an isogeny from E_1 to E_2.

REDUCTIONS BETWEEN PROBLEMS

$$\begin{tikzcd} \text{MAX ORDER} \arrow[d, shift left] \\ \text{ENDRING} \arrow[u, shift left] \arrow[d, shift left] \\ \text{ISOGENY} \arrow[u, shift left] \arrow[r] & \ell\text{-ISOGENY PATH} \end{tikzcd}$$

We'll give a reduction from MAX ORDER to ℓ-ISOGENY PATH

Assume: we have an oracle for ℓ-ISOGENY PATH.

MAX ORDER $\longrightarrow$ ℓ-ISOGENY PATH

Input: supersing. $E/\mathbb{F}_{p^2}$
Output: $\mathcal{O} \cong \mathrm{End}(E)$, given access to ℓ-ISOGENY PATH oracle

starting point: generate second curve $\tilde{E}$, $\tilde{\mathcal{O}} \cong \mathrm{End}(\tilde{E})$ which is known.

Idea for reduction:
Given E, generate $\tilde{E}$, $\tilde{\mathcal{O}}$ and run oracle for ℓ-ISOGENY PATH on input $(\tilde{E}, E)$. Will get an eff. repres. of an ℓ-power isogeny

from $\tilde{E}$ to E, say given as $\varphi : \tilde{E} \xrightarrow{\varphi_1} E_1 \xrightarrow{\varphi_2} \cdots \to E_e = E$

$$\varphi = \varphi_e \circ \cdots \circ \varphi_1 \quad \deg \varphi_i = \ell$$

Right and left orders, kernel ideals

Let $I \subseteq B_{p,\infty}$ be a $\mathbb{Z}$-lattice

right order of $I =$

$$\mathcal{O}_R(I) := \{x \in B_{p,\infty} : Ix \subseteq I\}$$

Similarly, define $\mathcal{O}_L(I)$.

When I is a left ideal in a maximal order $\mathcal{O}$ in $B_{p,\infty}$, then

$\mathcal{O}_R(I)$ is a maximal order $\mathcal{O}'$,

and $\mathcal{O}_L(I) = \mathcal{O}$.

We say that I connects $\mathcal{O}$ and $\mathcal{O}'$.

Translating isogenies into ideals and ideals into isogenies.

Given an isogeny $\varphi : E \to E'$ of degree n, can define a left $\mathrm{End}(E)$-ideal $I_\varphi := \mathrm{Hom}(E', E)\cdot\varphi$

Then $\mathcal{O}_L(I_\varphi) \cong \mathrm{End}(E)$ and $\mathcal{O}_R(I_\varphi) \cong \mathrm{End}(E')$.

So I_φ connects E and E'.

Conversely, given left ideal I of $\mathrm{End}(E)$, there is a subscheme $E[I]$ of E and an isogeny

$$\varphi_I : E \longrightarrow E/E[I]$$

If $\mathrm{Nrd}(I)$ is coprime to p, then

$$E[I] = \{P \in E(\overline{\mathbb{F}}_{p^2}) : \alpha(P) = 0 \ \forall \alpha \in I\}$$

The two constructions are mutal inverses.

I_φ is the <u>kernel ideal</u> of φ.

<u>Naive approach</u> for the reduction

MAX ORDER $\longrightarrow$ ℓ-ISOGENY PATH

given $E/\mathbb{F}_{p^2}$, construct $\widehat{E}$ and $\widetilde{\mathcal{O}}$.

- call oracle for ℓ-ISOGENY PATH on $(\widehat{E}, E)$ to get

  $\varphi = \varphi_e \circ \cdots \circ \varphi_1 : \widehat{E} \to E$ φ_i has deg ℓ

- $\boxed{\text{Compute the kernel ideal } I_\varphi \text{ for } \varphi.}$

- Compute $\mathcal{O}_R(I_\varphi)$ to obtain a max. order $\mathcal{O} \simeq \mathrm{END}(E)$.

computing kernel ideal is poly in $\max(\ell_i^{e_i})$ where $\mathrm{Norm}(I_\varphi) = \prod \ell_i^{e_i}$