NTNU | Norwegian University of Science and Technology

DEURING FOR THE PEOPLE

Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic

Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, Mattia Veroni

March 1, 2023

Contents

Introduction

The Deuring Correspondence

General Strategy for Computing

Details, Details, Details

Setting the Stage 1/3

- The *Deuring Correspondence* gives a bridge between two settings.
  - The geometric world of supersingular elliptic curves.
  - The arithmetic world of quaternion algebras.
- In the geometric world, problems we care about are *hard*.
- In the arithmetic world, problems we care about are *easy*.
- Translating between these settings happens via the endomorphism ring.

Setting the Stage 2/3

- Going from a supersingular elliptic curves to a maximal order is hopefully hard
  - Given E, computing $\mathrm{End}(E)$.
- Going the other way is easy™.
  - Given $\mathrm{End}(E)$, computing E.
  - Fast for specifically chosen primes p (SQISign).
  - Harder for general p (still known to be polytime in general)
- This work: Reasonably efficient for general p too, and we provide an easy-to-use SageMath code!

Setting the Stage 3/3

- Why is this a natural problem to study?
  - The strategy we outline requires working with $E[T]$, where $T > p^3$, and where T is smooth.
  - Using techniques from SQISign, this can be reduced to $T > p^{5/4+\epsilon}$.
  - Having $E[T] \subseteq E(\mathbb{F}_{p^2})$ not feasible in general, how detrimental is this to performance?
- Why is this a useful problem to study?
  - Having an algorithm that works for general characteristic is nice for playing around with.
  - Protocol usage down the line (e.g. as precomputation)?
  - Tighter security reductions.
- Key point:
  - Can “always” choose $T > p^3$ reasonably smooth, such that $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ for k reasonably small for all $\ell^e \mid T$ (even though $E[T]$ might only live in a huge extension field).

Supersingular curves

Let E be an elliptic curve.

- The *endomorphism ring* End(E) is the *ring* of all isogenies from E to itself (+ zero map).
  - Addition is pointwise, and multiplication is composition.
- E is *supersingular* if it satisfies:
  - End(E) is isomorphic to a maximal order in a quaternion algebra.
  - $\#E(\mathbb{F}_{p^k}) \equiv 1 \pmod p$. Important, because we know the order of $E(\mathbb{F}_{p^k})$.

Let E be supersingular.

- E is isomorphic to a curve defined over $\mathbb{F}_{p^2}$.
- $\phi : E \to E'$ can always be defined over $\mathbb{F}_{p^2}$, potentially by composing with some isomorphisms.

Quaternion Algebras

- A quaternion algebra B over $\mathbb{Q}$ has elements which look like

$$\alpha = x + y\mathbf{i} + z\mathbf{j} + w\mathbf{k}, \qquad x, y, z, w \in \mathbb{Q}$$

  and where multiplication is defined by $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$ and $\mathbf{i}^2 = -q, \mathbf{j}^2 = -p$.
- Values q and p determine *ramified places*. Throughout this presentation, we'll be looking at quaternion algebras $B_{p,\infty}$, i.e. ramified at p and ∞.
- We define the *norm* as

$$\mathrm{nrd}(\alpha) = \alpha\bar{\alpha}$$

  where $\bar{\alpha} = x - y\mathbf{i} - z\mathbf{j} - w\mathbf{k}$.

Quaternion Lattices

- Given any $\mathbb{Q}$-basis $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ of B, a $\mathbb{Z}$-lattice is

$$I = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} + \alpha_3\mathbb{Z} + \alpha_4\mathbb{Z}$$

- We extend the norm to lattices by $\mathrm{nrd}(I) = gcd(\{\mathrm{nrd}(\alpha) \mid \alpha \in I\})$.
- An *order* is a lattice $\mathcal{O} \subseteq B$, which is also a subring (i.e. $1 \in \mathcal{O}$, and closed under multiplication).
  - An order is *maximal* if it is not strictly contained in any other orders.
- Given a lattice I, we define its left order as

$$\mathcal{O}_L(I) = \{\alpha \in B \mid \alpha I \subseteq I\}$$

- A left $\mathcal{O}$-ideal I satisfies $\mathcal{O} \subseteq \mathcal{O}_L(I)$, and $\mathcal{O} = \mathcal{O}_L(I)$ if $\mathcal{O}$ is maximal.
  - $\mathcal{O}_R(I) \neq \mathcal{O}$ in general, but $\mathcal{O}_R(I)$ is still an order.

Quaternion Lattices - Example

The lattice

$$I \;=\; \mathbb{Z}\,79 \,\oplus\, \mathbb{Z}\,\frac{79+79\mathbf{i}}{2} \,\oplus\, \mathbb{Z}\,(37+3\mathbf{i}+\mathbf{j}) \,\oplus\, \mathbb{Z}\,\frac{791+453\mathbf{i}+7\mathbf{j}+\mathbf{k}}{14}$$

has $\mathrm{nrd}(I) = 79$. Further, its left and right orders are

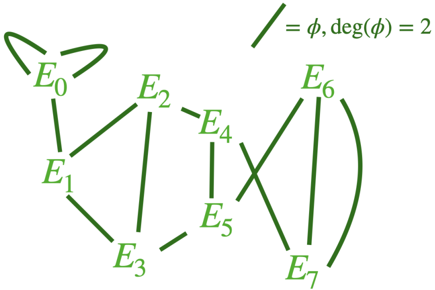
$$\mathcal{O}_L(I) = \mathbb{Z} \oplus \mathbb{Z}\,\frac{1+\mathbf{i}}{2} \oplus \mathbb{Z}\,\frac{\mathbf{j}+\mathbf{k}}{2} \oplus \mathbb{Z}\,\frac{2\mathbf{i}-\mathbf{k}}{7},$$

and

$$\mathcal{O}_R(I) = \mathbb{Z} \oplus \mathbb{Z}\,\frac{1+79\mathbf{i}}{2} \oplus \mathbb{Z}\,(3\mathbf{i}+\mathbf{j}) \oplus \mathbb{Z}\,\frac{553+35467\mathbf{i}+987\mathbf{j}+\mathbf{k}}{1106}.$$

In a sense, I *connects* these two orders.

Supersingular curve graph



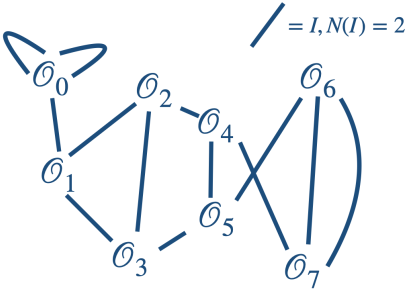
Fix some prime p, and another prime ℓ.

- *Vertices*: Isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$
- *Edges*: Isogenies of degree ℓ (up to post-isomorphism).

Quaternion order graph

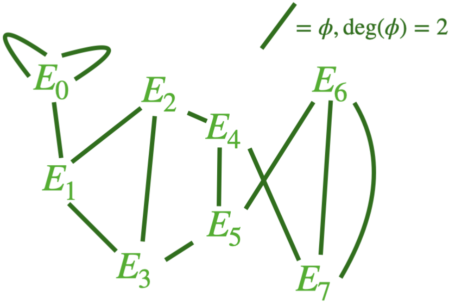
Fix some prime p, and another prime ℓ.

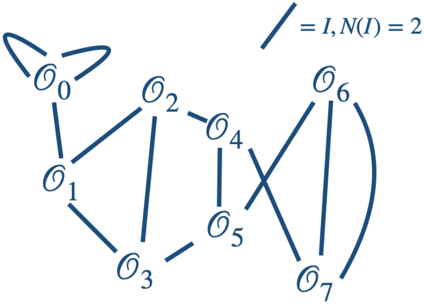
- *Vertices*: Isomorphism classes of (oriented) maximal orders $\mathcal{O}_i \in B_{p,\infty}$
- *Edges*[1]: Ideals of norm ℓ, with endpoints being its $\mathcal{O}_L(I)$ and $\mathcal{O}_R(I)$.



[1] This is a bit handwavy; these ideals are identified up to *something*.

Deuring Correspondence





Introduction

The Deuring Correspondence

General Strategy for Computing

Details, Details, Details

We focus on the following problem

Problem:
Given a maximal order $\mathcal{O} \in B_{p,\infty}$, compute a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \cong \mathcal{O}$.

Solving this:

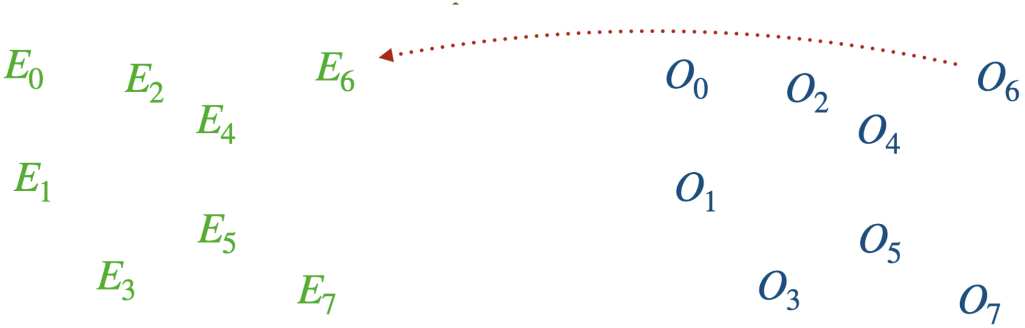
Step 0: Fix a base curve $E_0/\mathbb{F}_p$, with *effective* endomorphism ring $\mathcal{O}_0$.

Step 1: Find an ideal I with $\mathcal{O}_L(I) = \mathcal{O}_0, \mathcal{O}_R(I) = \mathcal{O}$ of *suitable norm*.

Step 2: Compute the isogeny $\phi_I : E_0 \to E$ corresponding to the ideal I.

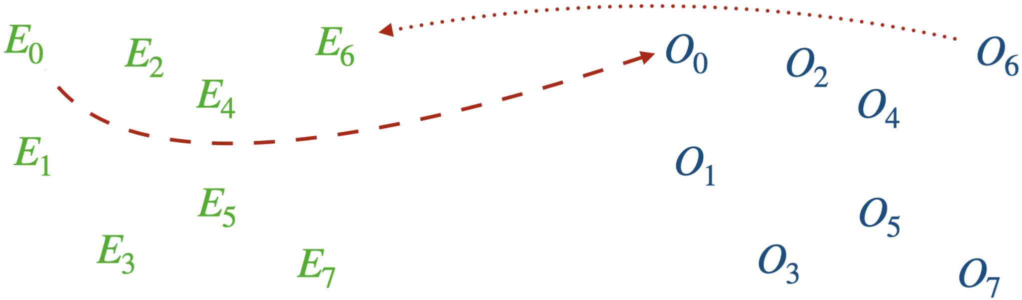
Problem

Given a maximal order $\mathcal{O} \in B_{p,\infty}$, compute a supersingular elliptic curve $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \cong \mathcal{O}$.



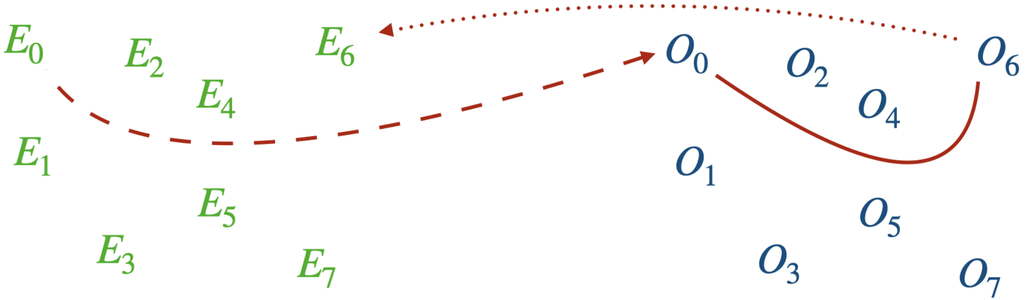
Step 0

Fix a base curve $E_0/\mathbb{F}_p$, with *effective* endomorphism ring $\mathcal{O}_0$.



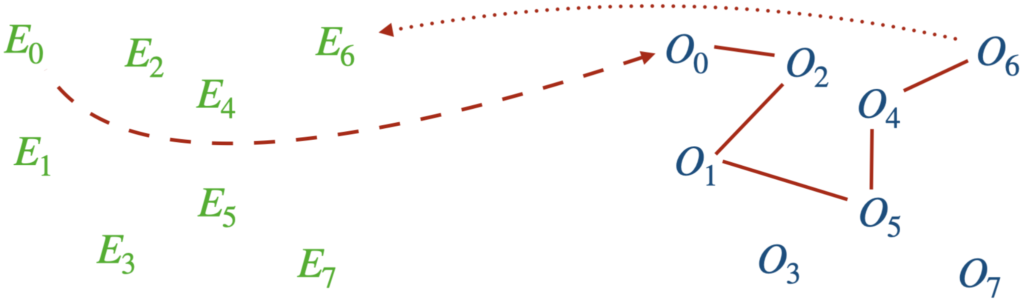
Step 1.1

Find an ideal J with $\mathcal{O}_L(J) = \mathcal{O}_0, \mathcal{O}_R(J) = \mathcal{O}$.



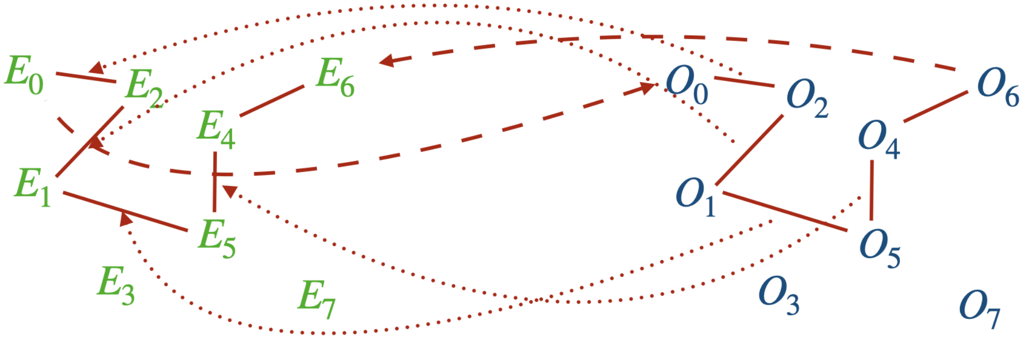
Step 1.2

Find an ideal $I \sim J$ of *suitable norm*.



Step 2

Compute the isogeny $\phi_I : E_0 \to E$ corresponding to the ideal I.



Effective endomorphism ring

- Knowing that $\mathrm{End}(E) \simeq \mathcal{O}$ might be insufficient for many tasks.
- Given an $\alpha \in \mathcal{O}$ (a quaternion), we want to be able to evaluate $\alpha(P)$ for points $P \in E$ (computing an endomorphism).
  - *Effective endomorphism ring* is when we can do the latter.
- Example: $p \equiv 2 \pmod 3$, then $E_0 : y^2 = x^3 + 1$ has effective endomorphism ring

$$\mathbb{Z} \oplus \mathbb{Z}\frac{1+\mathbf{i}}{2} \oplus \mathbb{Z}\frac{\mathbf{j}+\mathbf{k}}{2} \oplus \mathbb{Z}\frac{\mathbf{i}+\mathbf{k}}{3}$$

where the endomorphism $\mathbf{j}$ is Frobenius and $\omega = \frac{\mathbf{i}-1}{2}$ is given by

$$\omega(x, y) = (\zeta_3 \cdot x, y), \qquad \zeta_3^3 = 1, \zeta_3 \neq 1$$

Solving step 0

- If $p \not\equiv 1 \pmod{12}$, there are always “standard” choices.
- If $p \equiv 1 \pmod{12}$, use Bröker’s algorithm to generate a supersingular curve over $\mathbb{F}_p$.
  - Corresponding maximal order is known.
  - Endomorphism corresponding to $\mathbf{j}$ is Frobenius.
  - Must recover endomorphism corresponding to $\mathbf{i}$.

Step 2 - Ideal to Isogeny

Recall: Step 1 will find an ideal I with $\mathcal{O}_L(I) = \mathcal{O}_0, O_R(I) = \mathcal{O}$.

- Use the *kernel of the ideal I*, defined as

$$E[I] = \{P \in E \mid \alpha(P) = 0, \forall \alpha \in I\}$$

- The isogeny corresponding to I is

$$\phi_I : E \to E/E[I]$$

- "Find $E[I]$ by evaluating I on the $\mathrm{nrd}(I)$-torsion on E"

Step 2 - In practice

- Set $T = \mathrm{nrd}(I)$. Can write I as $\mathcal{O}_0(T, \alpha)$, for any $\alpha \in I, \gcd(T^2, \mathrm{nrd}(\alpha)) = T$. So
$$E[I] = E[T] \cap \ker \alpha = \bar{\alpha}(E[T])$$
- Explicitly: Let $\langle P, Q \rangle = E[T]$. Then ϕ_I has kernel $\langle \bar{\alpha}(P), \bar{\alpha}(Q) \rangle$.
- Cost: P, Q might only be defined over huge extension fields.
  - Work with prime powers separately. Okay, since isogenies between supersingular curves can always be made $\mathbb{F}_{p^2}$-rational.
  - We give a cool algorithm for computing $\mathbb{F}_{p^2}$-rational isogenies from irrational points.
- Cost: Going from $E[I]$ to ϕ_I depends on the smoothness of $T = \mathrm{nrd}(I)$.
- Hence we would love to control $\mathrm{nrd}(I)$. This is where KLPT comes in!

Step 1 - KLPT

KLPT allows us to "control the norm of $\mathcal{O}_0$-ideals".

Input: A maximal order $\mathcal{O}_0$ of a special form, a left ideal I, integer $T > p^3$.

Output: A left $\mathcal{O}_0$-ideal $J \sim I$ with $\mathrm{nrd}(J) \mid T$.

KLPT assumes that $\mathcal{O}_0$ is of a special form, namely so that

$$R + \mathbf{j}R \subseteq \mathcal{O}_0$$

for an imaginary quadratic order R of small discriminant.

Step 1 - What norm to target?

Generic: Pick the smallest B such that a $T = \prod \ell_i^{e_i} < p^3$, with $\ell_i^{e_i} < B$ exists.

- Call this strategy *naïve powersmooth*.

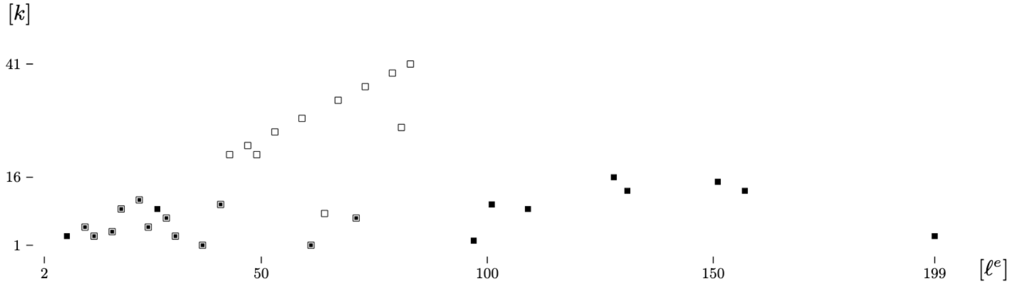
There is no reason to fix such a choice. Instead, look at the factorization of $p^k \pm 1$ to pick favorable torsion. Specifically, for each prime power $\ell^e \mid T$:

- Cost: $E[\ell^e]$ might only be defined over huge extension fields.
  - ℓ^e should divide $p^k \pm 1$ for small k.
- Cost: Going from $E[I]$ to ϕ_I depends on the smoothness of $T = \mathrm{nrd}(I)$.
  - ℓ should be small.

We implement greedy algorithm to select T to minimize the total cost w.r.t a *cost model* based on these factors above.

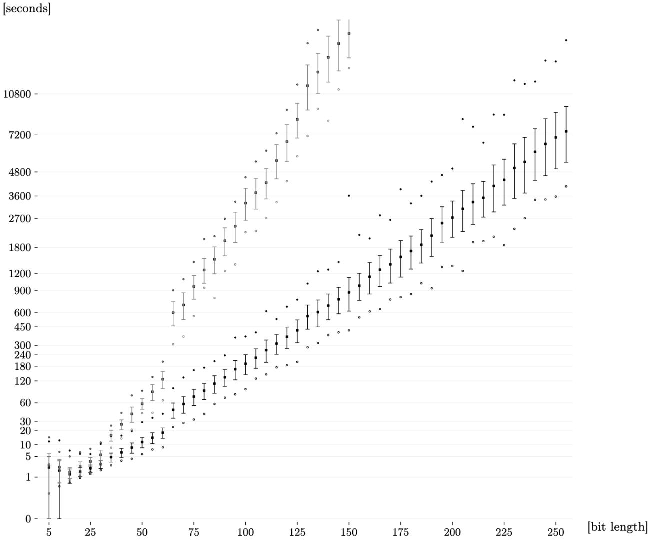
A Thousand Words

□: Naïve powersmooth
■: Our optimisation



Timings

- Gray: Naïve powersmooth
- Black: Our optimisation



Summary

Goal: Given a maximal order $\mathcal{O} \in B_{p,\infty}$, compute $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \cong \mathcal{O}$.

Step 0: Fix a base curve $E_0/\mathbb{F}_p$, with *effective* endomorphism ring $\mathcal{O}_0$.

- Bröker + Finding the effective isomorphism.

Step 1: Find an ideal I with $\mathcal{O}_L(I) = \mathcal{O}_0, \mathcal{O}_R(I) = \mathcal{O}$ of *suitable norm*.

- Target norm chosen carefully to optimise Step 2.
- KLPT

Step 2: Compute the isogeny $\phi_I : E_0 \to E$ corresponding to the ideal I.

- Finding kernel of the ideal is easy, as long as its defined over a reasonable extension field.
- Work with prime powers separately, means we can stay over smaller extension fields.
- Find the corresponding $\mathbb{F}_{p^2}$-rational isogeny.

Summary

- We have implemented this algorithm in SageMath.
  - Try our code! `https://github.com/friends-of-quaternions/deuring`
- Reasonably efficient, for primes up to 256 bit.
- This + SageMath implementation of SQISign with accompanying blog post (Coming soon™) by Maria Corte-Real Santos and Giacomo Pope (++), hopefully will make SQISign-stuff more accessible for SageMath fans!

Thank you for your attention

NTNU | Norwegian University of Science and Technology