# Deuring for the People: Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic

Jonathan Komada Eriksen [1] Lorenz Panny [2] Jana Sotáková [3] Mattia Veroni [1]

[1]Norwegian University of Science and Technology

[2]Academia Sinica, Taipei, Taiwan

[3]University of Amsterdam and QuSoft

July 13, 2023 LuCaNT

# Main actors

1. Prime $p$ large enough,
2. finite field $\mathbb{F}_{p^2}$ and extensions,
3. supersingular elliptic curves $E/\mathbb{F}_{p^2}$,

   Assume $\#E(\mathbb{F}_{p^2}) = (p+1)^2$,
   Frobenius over $\mathbb{F}_{p^2}$ acts as $[-p]$.
4. isogenies between elliptic curves:

   in our case: all defined over $\mathbb{F}_{p^2}$,
   given by: their kernels (for instance, given by generators), kernel polynomials*, rational maps, factored into a sequence of smaller-degree isogenies, ...
5. quaternion algebras

   $B_{p,\infty} = (-q, -p) = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}$
   with $ij = -ji = k$ and $j^2 = -p$ and $i^2 = -q$ for some $-q$ nonsquare mod $p$.

# Deuring correspondence

Let $B_{p,\infty}$ be a quaternion algebra ramified only at $p$ and $\infty$.

**Deuring correspondence**

The endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_{p^2}$ is isomorphic to a maximal order in $B_{p,\infty}$, and any maximal order in $B_{p,\infty}$ is isomorphic to an endomorphism ring of a supersingular elliptic curve over $\mathbb{F}_{p^2}$.

**Computing the endomorphism ring problem**

Starting from a curve $E$, give a maximal order $\mathcal{O}$ isomorphic to $\mathrm{End}(E)$.

**Constructive Deuring correspodence**

Given a maximal order $\mathcal{O}$ in $B_{p,\infty}$, find an elliptic curve $E$ with $\mathrm{End}(E) \cong \mathcal{O}$.

# Constructive Deuring correspodence

For $\mathcal{O} \subset B_{p,\infty}$, we want to find an elliptic curve $E$ with $\mathrm{End}(E) \cong \mathcal{O}$.

Fix a supersingular elliptic curve $E_0$ with $\mathrm{End}(E_0) = \mathcal{O}_0$.

**Another interpretation of the Deuring Correspondence**

Supersingular $j$-invariants in $\mathbb{F}_{p^2}$ are in a bijection with left-ideal classes in $\mathcal{O}_0$.

The ideal class of $[\mathcal{O}_0\mathcal{O}]$ corresponds to an elliptic curve $E$ with $\mathrm{End}(E) \cong \mathcal{O}$.

For any *integral* ideal $I \in [\mathcal{O}_0\mathcal{O}]$, construct isogeny of degree $\mathrm{norm}(I)$ with kernel

$$E_0[I] = \cap_{\alpha \in I} \ker(\alpha).$$

Then the codomain $E$ satisfies $\mathrm{End}(E) \cong \mathcal{O}$.

# Strategy

Want to compute an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}$.

**Strategy:**

1. Find some supersingular elliptic curve $E_0$ with effective endomorphism ring $\mathcal{O}_0$.
2. Compute an integral ideal $I$ in the class of $[\mathcal{O}_0\mathcal{O}]$, e.g. $N \cdot \mathcal{O}_0\mathcal{O}$ for some $N$.
3. Translate this ideal to an isogeny $E_0 \to E$.

**$p \equiv 3 \pmod 4$**

On the curve $E_0 : y^2 = x^3 + x$, Frobenius $\pi$ satisfies $\pi^2 = -p$. Also have an endomorphism $\iota$ with $\iota^2 = -1$.
Map $\pi \mapsto \mathbf{j}$ and $\iota \mapsto \mathbf{i}$. Then

$$\mathcal{O}_0 = \mathbb{Z} \oplus \mathbb{Z}\,\mathbf{i} \oplus \mathbb{Z}\,\frac{\mathbf{i}+\mathbf{j}}{2} \oplus \mathbb{Z}\,\frac{1+\mathbf{k}}{2}$$

# How to translate an ideal to an isogeny

Ideal $I \subset \mathcal{O}_0$ of norm $N$. Assume $I$ is cyclic: cannot factor out any integer.

1. find the kernel of the ideal: $E_0[I] = \cap_{\alpha \in I} \ker(\alpha) = \{P \in E_0 : \alpha(P) = 0 \text{ for all } \alpha \in I\}$.
   For any prime power $\ell^e \mid N$:
   - 1.1 find a basis $P, Q$ of the torsion $E[\ell^e] \subset E(\mathbb{F}_{p^k})$,
   - 1.2 determine the action of $I$ on $E[\ell^e]$,
   - 1.3 compute the kernel generator $G_\ell$.
   - 1.2 Avoid discrete logarithms:

     > Write $I = \alpha\mathcal{O} + N\mathcal{O}$.
     > Then the kernel point $G_\ell$ is $\overline{\alpha}(P)$ or $\overline{\alpha}(Q)$, whichever has full order.

   The kernel is then generated by all the $G_\ell$.
2. translate the kernel into isogenies: for every prime power $\ell^e \mid N$:
   - 2.1 compute an $\ell$-isogeny ($e$ times),
   - 2.2 each time, map all the kernel generators through the isogeny.

# Kohel-Lauter-Petit-Tignol algorithm

Maximal order $\mathcal{O}_0$ constructed as before. $I \subset \mathcal{O}_0$ ideal of norm $N$.

## Equivalent ideals

For any $\beta \in I$ of norm $NR$, the ideal

$$J = I \cdot \frac{\overline{\beta}}{N}$$

is an integral ideal in the same class and has norm $R$.

So to find an ideal of nicer norm, it is enough to find elements $\beta \in I$ of suitable norm.

## KLPT algorithm, simplified

If $R$ is smooth and $R > p^3$, you can find $\beta \in I$ of norm dividing $NR$ in polynomial time.

# How to choose R

Most often, the $\ell$ torsion is only defined over $\mathbb{F}_{p^{\ell-1}}$: extension of $\mathbb{F}_{p^2}$ of degree $\frac{\ell-1}{2}$.

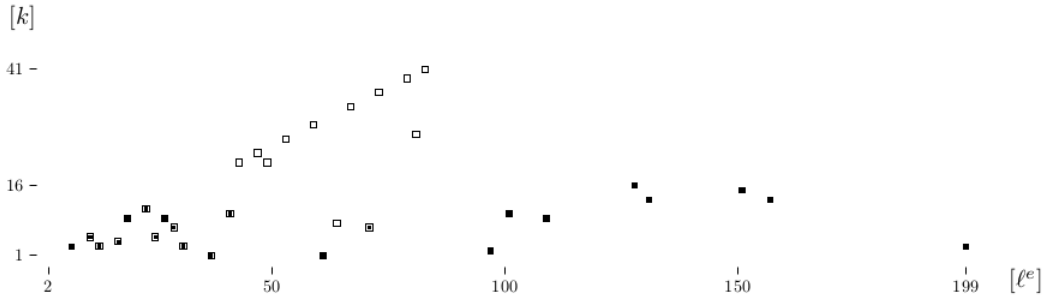
**Choice of $R$:**

Pick powers $\ell^e \mid R$ such that:

1. $\prod \ell^e > p^3$,
2. the torsion groups $E[\ell^e]$ are defined over small extensions of $\mathbb{F}_{p^2}$,
3. the $\ell$-isogenies do not get too expensive.

In practice, estimate/guess a cost model, and use a greedy algorithm to get a $R$ with smallest expected cost.

# Illustration for some $p$




**Black dots**

Small prime powers picked by our algorithm to optimize the extension degrees.

**White squares**

Primes picked by the naive power-smooth KLPT algorithm.

# Timings

x-axis: seconds
y-axis: bit-length

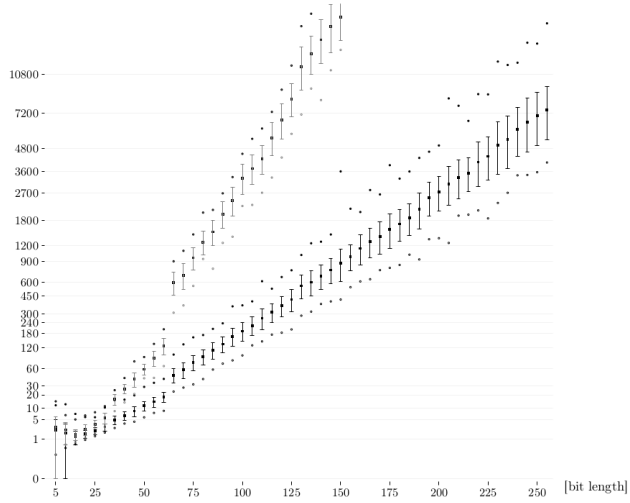
**Lower dots**

Our implementation, picking a good $R$, small extension degrees

**Upper dots**

Naive implementation, picking power smooth torsion groups, ignoring extension degrees.

100 bit primes: 2-3 minutes
256 bit primes: 2 hours



# Code!

## What can the code do for you?

1. Written in Sage (version $\geq 9.8$)
2. Handles all non-tiny primes!
   no congruence condition on $p$
3. Somewhat modular
   KLPT algorithm;
   constructing one supersingular curve
   with effective endomorphism ring

## What it can do but is not yet in repo

Handles maximal orders in **your** favorite quaternion algebra,
go between different representations of $B_{p,\infty}$

https://github.com/friends-of-quaternions/deuring

# Constructing one supersingular elliptic curve

For $p \equiv 3 \bmod 4$, we have $y^2 = x^3 + x$ with known *effective* endomorphism ring.

## Bröker method

For any prime $p \equiv 1 \bmod 4$, find a supersingular elliptic curve in $\mathbb{F}_{p^2}$ as:

- find the smallest prime $q$ that is a non-square mod $p$,
- find the unique root $j$ of $H_{-q}(X)$ in $\mathbb{F}_p$,
- construct elliptic curve $E_0$ with $j$-invariant $j$.

Certainly Frobenius $\pi$ satisfies $\pi^2 = -p$, and necessarily get $\vartheta^2 = -q$.

## Ibukiyama step

Identify $\vartheta \mapsto \mathbf{i}$ and $\pi \mapsto \mathbf{j}$. Then there are only two choices for endomorphism ring of $E_0$:

$$\mathcal{O}_0 \;=\; \mathbb{Z} \oplus \mathbb{Z}\frac{1+\mathbf{i}}{2} \oplus \mathbb{Z}\frac{\mathbf{j}+\mathbf{k}}{2} \oplus \mathbb{Z}\frac{c\mathbf{i} \pm \mathbf{k}}{q} \tag{1}$$

where $c$ is a fixed integer satisfying $c^2 \equiv -p \pmod{q}$.