To the **End** and back

Lorenz Panny

Technische Universität München

Mathematics for post-quantum cryptanalysis

Budapest, 8 August 2024

What?

The Deuring correspondence:

Almost exact equivalence between two (*a priori*) very different worlds:

What?

The Deuring correspondence:

Almost exact equivalence between two (*a priori*) very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.

What?

The Deuring correspondence:

Almost exact equivalence between two *a priori* very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

What?

The Deuring correspondence:

Almost exact equivalence between two (*a priori*) very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

What?

The Deuring correspondence:

Almost exact equivalence between two *(a priori)* very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

The correspondence is through the endomorphism ring.

What?

The Deuring correspondence:

Almost exact equivalence between two (*a priori*) very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

The correspondence is through the endomorphism ring.

:-) The "$\Leftarrow$" direction is easy, the "$\Rightarrow$" direction seems hard!

What?

The Deuring correspondence:

Almost exact equivalence between two (*a priori*) very different worlds:

- Supersingular elliptic curves defined over $\mathbb{F}_{p^2}$.
- Quaternions: Maximal orders in a certain algebra $B_{p,\infty}$.

Isogenies become connecting ideals in quaternion land.

The correspondence is through the endomorphism ring.

☺ The "$\Leftarrow$" direction is easy, the "$\Rightarrow$" direction seems hard!

$\rightsquigarrow$ *Cryptography!*

Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.

Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.
- **SQIsign** builds on the "$\Leftarrow$" direction constructively.

Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.
- **SQIsign** builds on the "$\Leftarrow$" direction constructively.
- Essential tool for both constructions and attacks.

Why?

We now know that **the Deuring correspondence lies at the heart of contemporary isogeny-based cryptography.**

- $\approx$All isogeny security reduces to the "$\Rightarrow$" direction.
- **SQIsign** builds on the "$\Leftarrow$" direction constructively.
- Essential tool for both constructions and attacks.

Constructively, *partially* known endomorphism rings are useful.
$\rightsquigarrow$ **Oriented curves** and **the isogeny class-group action**. 🏝️

Curve world

- Universe: Characteristic p. Assume $p \geq 5$ throughout.
- Supersingular elliptic curves: $E[p] = \{\infty\}$.

Curve world

- Universe: Characteristic p. Assume $p \geq 5$ throughout.
- Supersingular elliptic curves: $E[p] = \{\infty\}$.
- Isogenies, endomorphisms, and so on and so forth.

Curve world

- Universe: Characteristic p. Assume $p \geq 5$ throughout.
- Supersingular elliptic curves: $E[p] = \{\infty\}$.
- Isogenies, endomorphisms, and so on and so forth.
- Famous examples:
  - $p \equiv 3 \pmod 4$ and $E\colon y^2 = x^3 + x$ with j-invariant 1728.
  - $p \equiv 2 \pmod 3$ and $E\colon y^2 = x^3 + 1$ with j-invariant 0.

Computationally...

- We work with curves defined over $\mathbb{F}_{p^2}$ such that $\pi = [-p]$.
  (This choice is natural: It includes the base-changes of curves defined over $\mathbb{F}_p$.)

Computationally...

- We work with curves defined over $\mathbb{F}_{p^2}$ such that $\pi = [-p]$.
  (This choice is natural: It includes the base-changes of curves defined over $\mathbb{F}_p$.)
- The group structure is known over all extensions:
  $E(\mathbb{F}_{p^{2k}}) \cong \mathbb{Z}/n \times \mathbb{Z}/n$ where $n = p^k - (-1)^k$.

Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.

Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ is a 4-dimensional $\mathbb{Q}$-vector space.
  Write $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$.

Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ is a 4-dimensional $\mathbb{Q}$-vector space.
  Write $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$.
- Multiplication defined by relations $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$, $\mathbf{ji} = -\mathbf{ij}$.
  Here q is a positive integer satisfying some conditions with respect to p.
  ⚠ All valid q define isomorphic algebras $B_{p,\infty}$.

Quaternion universe

- Everything lives in a particular quaternion algebra $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ is a 4-dimensional $\mathbb{Q}$-vector space.
  Write $B_{p,\infty} = \mathbb{Q} \oplus \mathbb{Q}\mathbf{i} \oplus \mathbb{Q}\mathbf{j} \oplus \mathbb{Q}\mathbf{ij}$.
- Multiplication defined by relations $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$, $\mathbf{ji} = -\mathbf{ij}$.
  Here q is a positive integer satisfying some conditions with respect to p.
  ⚠ All valid q define isomorphic algebras $B_{p,\infty}$.
- The algebra $B_{p,\infty}$ has a conjugation $\overline{}$ which negates $\mathbf{i}, \mathbf{j}, \mathbf{ij}$.
  The norm and trace of an element α are $\alpha\overline{\alpha} \in \mathbb{Z}_{\geq 0}$ and $\alpha + \overline{\alpha} \in \mathbb{Z}$.

Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.

Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.

Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.
- An order is a fractional ideal which is a subring of $B_{p,\infty}$.
  A maximal order is one that is not contained in any strictly larger order.

Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.
- An order is a fractional ideal which is a subring of $B_{p,\infty}$.
  A maximal order is one that is not contained in any strictly larger order.
- A fractional ideal I is a left $\mathcal{O}$-ideal if $\mathcal{O}I \subseteq I$. (Similarly on the right.)

Quaternion world

- Maximal orders in the quaternion algebra $B_{p,\infty}$.
- Left- and right-ideals, principal ideals, and so on.

Definitions:

- A (fractional) ideal is a rank-4 lattice contained in $B_{p,\infty}$.
- An order is a fractional ideal which is a subring of $B_{p,\infty}$.
  A maximal order is one that is not contained in any strictly larger order.
- A fractional ideal I is a left $\mathcal{O}$-ideal if $\mathcal{O}I \subseteq I$. (Similarly on the right.)
  We say I connects $\mathcal{O}$ and $\mathcal{O}'$ if $\mathcal{O}I \subseteq I$ and $I\mathcal{O}' \subseteq I$.

Computationally, ...

- We typically work with one fixed choice of q for each p.

Computationally, ...

- We typically work with one fixed choice of q for each p.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.

Computationally, ...

- We typically work with one fixed choice of q for each p.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.
- All the basic algorithms are essentially linear algebra.

Computationally, ...

- We typically work with one fixed choice of q for each p.
- Quaternions are represented as vectors in $\mathbb{Q}^4$.
- All the basic algorithms are essentially linear algebra.

General theme: Things are easy in quaternion land.

From curves to quaternions

$$E \mapsto \mathcal{O}$$

(The presumably hard direction.)

Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\iota^2 = [-1]$, $\pi\iota = -\iota\pi$, and $\pi^2 = [-p]$.

Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\iota^2 = [-1]$, $\pi\iota = -\iota\pi$, and $\pi^2 = [-p]$.

Hence, in the quaternion algebra where $\mathbf{i}^2 = -1$ and $\mathbf{j}^2 = -p$, the pair (ι, π) corresponds to $(\mathbf{i}, \mathbf{j})$.

Example #1

Assume $p \equiv 3 \pmod 4$.

Then $E\colon y^2 = x^3 + x$ is supersingular, and it has endomorphisms

$$\begin{aligned} \iota\colon\ (x,y) &\longmapsto (-x, \sqrt{-1}\cdot y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\iota^2 = [-1]$, $\pi\iota = -\iota\pi$, and $\pi^2 = [-p]$.

Hence, in the quaternion algebra where $\mathbf{i}^2 = -1$ and $\mathbf{j}^2 = -p$, the pair (ι, π) corresponds to $(\mathbf{i}, \mathbf{j})$.

In fact, the image in $B_{p,\infty}$ of a $\mathbb{Z}$-basis of $\mathrm{End}(E)$ is given by

$$\{1, \quad \mathbf{i}, \quad (\mathbf{i}+\mathbf{j})/2, \quad (1+\mathbf{ij})/2\}\,.$$

Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega\colon\ (x,y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega\colon\ (x,y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi\colon\ (x,y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\omega^3 = [1]$, $\omega\pi + \pi\omega = -\pi$, and $\pi^2 = [-p]$.

Example #2

Assume $p \equiv 2 \pmod{3}$.

Then $E \colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\omega \colon \ (x, y) \longmapsto (\zeta_3 \cdot x, y)\,,$$
$$\pi \colon \ (x, y) \longmapsto (x^p, y^p)\,.$$

In decreasing order of obviousness, one can show that
$$\omega^3 = [1],\ \omega\pi + \pi\omega = -\pi, \text{ and } \pi^2 = [-p].$$

Hence, in the quaternion algebra where $\mathbf{i}^2 = -3$ and $\mathbf{j}^2 = -p$, the pair $(2\omega + 1, \pi)$ corresponds to $(\mathbf{i}, \mathbf{j})$.

Example #2

Assume $p \equiv 2 \pmod 3$.

Then $E\colon y^2 = x^3 + 1$ is supersingular, and it has endomorphisms

$$\begin{aligned} \omega\colon \ (x, y) &\longmapsto (\zeta_3 \cdot x, y)\,, \\ \pi\colon \ (x, y) &\longmapsto (x^p, y^p)\,. \end{aligned}$$

In decreasing order of obviousness, one can show that
$\omega^3 = [1]$, $\omega\pi + \pi\omega = -\pi$, and $\pi^2 = [-p]$.

Hence, in the quaternion algebra where $\mathbf{i}^2 = -3$ and $\mathbf{j}^2 = -p$, the pair $(2\omega + 1, \pi)$ corresponds to $(\mathbf{i}, \mathbf{j})$.

In fact, the image in $B_{p,\infty}$ of a $\mathbb{Z}$-basis of $\mathrm{End}(E)$ is given by

$$\{1, \quad (1 + \mathbf{i})/2, \quad (\mathbf{j} + \mathbf{ij})/2, \quad (\mathbf{i} + \mathbf{ij})/3\}\,.$$

From curves to quaternions

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

From curves to quaternions

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

Equivalently (Wesolowski 2021, assuming GRH):

The isogeny problem.
Given two supersingular elliptic curves,
find any isogeny between them.

From curves to quaternions

The supersingular endomorphism-ring problem.
Given a supersingular elliptic curve,
find its endomorphism ring.

Equivalently (Wesolowski 2021, assuming GRH):

The isogeny problem.
Given two supersingular elliptic curves,
find any isogeny between them.

As far as we know, these are *hard* problems (even quantumly).

Endomorphism rings via cycle finding

Recall: Cycles in isogeny graphs are endomorphisms.

Endomorphism rings via cycle finding

Recall: Cycles in isogeny graphs are endomorphisms.

- Heuristically, "a few" "random-ish" endomorphisms probably form a generating set for $\mathrm{End}(E)$.

Endomorphism rings via cycle finding

Recall: Cycles in isogeny graphs are endomorphisms.

- Heuristically, "a few" "random-ish" endomorphisms probably form a generating set for $\mathrm{End}(E)$.
- To find cycles, use generic graph algorithms.
  Meet-in-the-middle: Build breadth-first tree, wait for a collision.

Endomorphism rings via cycle finding

Recall: Cycles in isogeny graphs are endomorphisms.

- Heuristically, "a few" "random-ish" endomorphisms probably form a generating set for $\mathrm{End}(E)$.
- To find cycles, use generic graph algorithms.
  Meet-in-the-middle: Build breadth-first tree, wait for a collision.

!! Time $\widetilde{O}(\sqrt{p})$, but requires the same amount of memory!

Endomorphism rings via cycle finding

Recall: Cycles in isogeny graphs are endomorphisms.

- Heuristically, "a few" "random-ish" endomorphisms probably form a generating set for $\mathrm{End}(E)$.
- To find cycles, use generic graph algorithms.
  Meet-in-the-middle: Build breadth-first tree, wait for a collision.

!! Time $\widetilde{O}(\sqrt{p})$, but requires the same amount of memory!

!! Parallel collision finding (vOW) yields a time-memory tradeoff.

Endomorphism rings via cycle finding

Recall: Cycles in isogeny graphs are endomorphisms.

- Heuristically, “a few” “random-ish” endomorphisms probably form a generating set for $\mathrm{End}(E)$.
- To find cycles, use generic graph algorithms.
  Meet-in-the-middle: Build breadth-first tree, wait for a collision.

!! Time $\widetilde{O}(\sqrt{p})$, but requires the same amount of memory!

!! Parallel collision finding (vOW) yields a time-memory tradeoff.

$\rightsquigarrow$ **Approach #1**: Find “enough” isogeny cycles.

(Then find relations between them and construct an embedding into $B_{p,\infty}$.)

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\langle\cdot,\cdot\rangle\colon \operatorname{End}(E)\times\operatorname{End}(E)\to\mathbb{Z},\ (\alpha,\beta)\mapsto\widehat{\alpha}\beta+\alpha\widehat{\beta}.$$
    This is (heuristically) polynomial-time.

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\langle \cdot, \cdot \rangle \colon \operatorname{End}(E) \times \operatorname{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is (heuristically) polynomial-time.

Main steps:

Find $\mathbb{Q}$-linear combinations of the input endomorphisms of the form...

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing

    $$\langle \cdot, \cdot \rangle\colon \operatorname{End}(E) \times \operatorname{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$

    This is (heuristically) polynomial-time.

Main steps:

Find $\mathbb{Q}$-linear combinations of the input endomorphisms of the form...

1. $(1, \alpha, \beta, \gamma)$, all orthogonal *[standard Gram–Schmidt]*;

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\langle\cdot,\cdot\rangle\colon\ \mathrm{End}(E)\times\mathrm{End}(E)\to\mathbb{Z},\ (\alpha,\beta)\mapsto\widehat{\alpha}\beta+\alpha\widehat{\beta}.$$
    This is (heuristically) polynomial-time.

Main steps:

Find $\mathbb{Q}$-linear combinations of the input endomorphisms of the form...

1. $(1,\alpha,\beta,\gamma)$, all orthogonal *[standard Gram–Schmidt]*;
2. $(1,\iota,\beta',\gamma')$ such that additionally $\iota^2=-q$ *[a ternary quadratic form]*;

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\langle \cdot, \cdot \rangle \colon \mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is (heuristically) polynomial-time.

Main steps:

Find $\mathbb{Q}$-linear combinations of the input endomorphisms of the form...

1. $(1, \alpha, \beta, \gamma)$, all orthogonal *[standard Gram–Schmidt]*;
2. $(1, \iota, \beta', \gamma')$ such that additionally $\iota^2 = -q$ *[a ternary quadratic form]*;
3. $(1, \iota, \pi, \gamma'')$ such that additionally $\pi^2 = -p$ *[a binary quadratic form]*;

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\langle \cdot, \cdot \rangle \colon \operatorname{End}(E) \times \operatorname{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is (heuristically) polynomial-time.

Main steps:
Find $\mathbb{Q}$-linear combinations of the input endomorphisms of the form...

1. $(1, \alpha, \beta, \gamma)$, all orthogonal *[standard Gram–Schmidt]*;
2. $(1, \iota, \beta', \gamma')$ such that additionally $\iota^2 = -q$ *[a ternary quadratic form]*;
3. $(1, \iota, \pi, \gamma'')$ such that additionally $\pi^2 = -p$ *[a binary quadratic form]*;
4. $(1, \iota, \pi, \iota\pi)$ *[simple rescaling]*.

From concrete to abstract endomorphisms

- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\langle \cdot, \cdot \rangle \colon \operatorname{End}(E) \times \operatorname{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is (heuristically) polynomial-time.

Main steps:

Find $\mathbb{Q}$-linear combinations of the input endomorphisms of the form...

1. $(1, \alpha, \beta, \gamma)$, all orthogonal *[standard Gram–Schmidt]*;
2. $(1, \iota, \beta', \gamma')$ such that additionally $\iota^2 = -q$ *[a ternary quadratic form]*;
3. $(1, \iota, \pi, \gamma'')$ such that additionally $\pi^2 = -p$ *[a binary quadratic form]*;
4. $(1, \iota, \pi, \iota\pi)$ *[simple rescaling]*.

This defines an isometry $\operatorname{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \xrightarrow{\sim} B_{p,\infty}$ w.r.t. $\langle \cdot, \cdot \rangle$.

Endomorphism rings via isogeny finding

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \operatorname{End}(E) &\hookrightarrow \overbrace{\operatorname{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}}^{=:B_{p,\infty}}\,; \\ \alpha &\mapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

Endomorphism rings via isogeny finding

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \mathrm{End}(E) &\hookrightarrow \overbrace{\mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}}^{=: B_{p,\infty}}\,; \\ \alpha &\mapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

Under this embedding, $\mathrm{End}(E) = \mathcal{O}_R(I) = \{\alpha \in B_{p,\infty} : I\alpha \subseteq I\}$, where $I := \mathrm{Hom}(E, E_0)\varphi$ is the ideal of E_0 associated to φ.

Endomorphism rings via isogeny finding

From any isogeny $\varphi\colon E_0 \to E$, we obtain (abstractly) an embedding of the endomorphism ring

$$\begin{aligned} \operatorname{End}(E) &\hookrightarrow \overbrace{\operatorname{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}}^{=:B_{p,\infty}}\,; \\ \alpha &\mapsto \widehat{\varphi}\alpha\varphi/\deg(\varphi)\,. \end{aligned}$$

Under this embedding, $\operatorname{End}(E) = \mathcal{O}_R(I) = \{\alpha \in B_{p,\infty} : I\alpha \subseteq I\}$, where $I := \operatorname{Hom}(E, E_0)\varphi$ is the ideal of E_0 associated to φ.

$\rightsquigarrow$ **Approach #2**: Choose "special" E_0, find an isogeny $E_0 \to E$.
(Then recover the associated ideal and the codomain endomorphism ring.)

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

1. Find any isogeny $\varphi_0 \colon E_0 \to E_0'$ where $E_0'/\mathbb{F}_p$.
2. Find any isogeny $\varphi_1 \colon E_1 \to E_1'$ where $E_1'/\mathbb{F}_p$.

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

1. Find any isogeny $\varphi_0 \colon E_0 \to E_0'$ where $E_0'/\mathbb{F}_p$.
2. Find any isogeny $\varphi_1 \colon E_1 \to E_1'$ where $E_1'/\mathbb{F}_p$.
3. Find any isogeny $\psi \colon E_0' \to E_1'$ defined over $\mathbb{F}_p$.

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

1. Find any isogeny $\varphi_0\colon E_0 \to E_0'$ where $E_0'/\mathbb{F}_p$.
2. Find any isogeny $\varphi_1\colon E_1 \to E_1'$ where $E_1'/\mathbb{F}_p$.
3. Find any isogeny $\psi\colon E_0' \to E_1'$ defined over $\mathbb{F}_p$.
4. Return $\widehat{\varphi}_1 \circ \psi \circ \varphi_0$.

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

1. Find any isogeny $\varphi_0\colon E_0 \to E_0'$ where $E_0'/\mathbb{F}_p$.
2. Find any isogeny $\varphi_1\colon E_1 \to E_1'$ where $E_1'/\mathbb{F}_p$.
3. Find any isogeny $\psi\colon E_0' \to E_1'$ defined over $\mathbb{F}_p$.
4. Return $\widehat{\varphi}_1 \circ \psi \circ \varphi_0$.

All three steps can be done in time $\widetilde{O}(\sqrt{p})$...

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

1. Find any isogeny $\varphi_0 \colon E_0 \to E_0'$ where $E_0'/\mathbb{F}_p$.
2. Find any isogeny $\varphi_1 \colon E_1 \to E_1'$ where $E_1'/\mathbb{F}_p$.
3. Find any isogeny $\psi \colon E_0' \to E_1'$ defined over $\mathbb{F}_p$.
4. Return $\widehat{\varphi}_1 \circ \psi \circ \varphi_0$.

All three steps can be done in time $\widetilde{O}(\sqrt{p})$...

- ...in a trivially parallelizable manner;

The Delfs–Galbraith algorithm

...is probably(?) the best known algorithm for solving the supersingular isogeny problem:

Given $E_0, E_1/\mathbb{F}_{p^2}$ supersingular, find an isogeny $E_0 \to E_1$.

1. Find any isogeny $\varphi_0 \colon E_0 \to E_0'$ where $E_0'/\mathbb{F}_p$.
2. Find any isogeny $\varphi_1 \colon E_1 \to E_1'$ where $E_1'/\mathbb{F}_p$.
3. Find any isogeny $\psi \colon E_0' \to E_1'$ defined over $\mathbb{F}_p$.
4. Return $\widehat{\varphi}_1 \circ \psi \circ \varphi_0$.

All three steps can be done in time $\widetilde{O}(\sqrt{p})$...

- ...in a trivially parallelizable manner;
- ...with negligible memory requirements.

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi \alpha_0 \widehat{\varphi} / \deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi \alpha_0 \widehat{\varphi} / \deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Evaluation at some point $P \in E$:

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi\alpha_0\widehat{\varphi}/\deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Evaluation at some point $P \in E$:

- Compute any $Q \in E$ such that $[\deg(\varphi)]Q = P$.

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi\alpha_0\widehat{\varphi}/\deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Evaluation at some point $P \in E$:

- Compute any $Q \in E$ such that $[\deg(\varphi)]Q = P$.
- Return $\varphi(\alpha_0(\widehat{\varphi}(Q)))$.

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi\alpha_0\widehat{\varphi}/\deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Evaluation at some point $P \in E$:

- Compute any $Q \in E$ such that $[\deg(\varphi)]Q = P$.
- Return $\varphi(\alpha_0(\widehat{\varphi}(Q)))$.

!! In general Q lies in a huge field extension.

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi\alpha_0\widehat{\varphi}/\deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Evaluation at some point $P \in E$:

- Compute any $Q \in E$ such that $[\deg(\varphi)]Q = P$.
- Return $\varphi(\alpha_0(\widehat{\varphi}(Q)))$.

!! In general Q lies in a huge field extension.

- Theoretical polynomial-time solution: Compute an 8-dimensional isogeny which embeds $\varphi\alpha_0\widehat{\varphi}/\deg(\varphi)$...

Dividing endomorphisms

!! The representation of $\alpha \in \mathrm{End}(E)$ we obtain is fractional:

$$\alpha = \varphi\alpha_0\widehat{\varphi}/\deg(\varphi)\,,$$

where $\alpha_0 \in \mathrm{End}(E_0)$.

Evaluation at some point $P \in E$:

- Compute any $Q \in E$ such that $[\deg(\varphi)]Q = P$.
- Return $\varphi(\alpha_0(\widehat{\varphi}(Q)))$.

!! In general Q lies in a huge field extension.

- Theoretical polynomial-time solution: Compute an 8-dimensional isogeny which embeds $\varphi\alpha_0\widehat{\varphi}/\deg(\varphi)$...

$\Longrightarrow$ This is a (practically) very inconvenient representation.

From curves to quaternions

Plenty of algorithms to compute $E \mapsto \mathrm{End}(E)$ in time $\widetilde{O}(\sqrt{p})$.

It is not immediately obvious which one works best in practice.

From quaternions to curves

$$\mathcal{O} \mapsto E$$

(The "easy" direction.)

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$.
  Let $\mathcal{O}_0 := \mathrm{End}(E_0)$.

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$.
  Let $\mathcal{O}_0 := \mathrm{End}(E_0)$.

Theorem. The (contravariant) functor

$$E \longmapsto \mathrm{Hom}(E, E_0)$$

defines an equivalence of categories between

- supersingular elliptic curves with isogenies; and
- invertible left $\mathcal{O}_0$-modules
  with nonzero left $\mathcal{O}_0$-module homomorphisms.

The main theorem

- Fix a supersingular elliptic curve $E_0/\mathbb{F}_{p^2}$.
  Let $\mathcal{O}_0 := \mathrm{End}(E_0)$.

Theorem. The (contravariant) functor

$$E \longmapsto \mathrm{Hom}(E, E_0)$$

defines an equivalence of categories between

- supersingular elliptic curves with isogenies; and
- invertible left $\mathcal{O}_0$-modules
  with nonzero left $\mathcal{O}_0$-module homomorphisms.

Corollary (Deuring). Isomorphism classes of supersingular elliptic curves are in bijection with the (left) class set $\mathrm{Cls}_L(\mathcal{O}_0)$.

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$.

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$.

- Given $\psi\colon E_0 \to E$, the associated $\mathcal{O}_0$-ideal is $\mathrm{Hom}(E, E_0)\psi$.

Ideals & isogenies

One particular consequence of this equivalence is that

isogenies from E_0 correspond to left ideals of $\mathcal{O}_0$.

- Given $\psi \colon E_0 \to E$, the associated $\mathcal{O}_0$-ideal is $\mathrm{Hom}(E, E_0)\psi$.

<u>Important consequence:</u> The isogeny $\varphi_I \colon E_0 \to E$ defined by a left $\mathcal{O}_0$-ideal I has kernel $\bigcap_{\alpha \in I} \ker \alpha \le E_0$.

History and algorithms

- **1941**: Deuring proves the correspondence.

Wenn aber **R** eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

History and algorithms

- **1941**: Deuring proves the correspondence.

> Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.

History and algorithms

- **1941**: Deuring proves the correspondence.

  Wenn aber R eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.

History and algorithms

- **1941**: Deuring proves the correspondence.

  Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014)) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.

History and algorithms

- **1941**: Deuring proves the correspondence.

> Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014) 🪄) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.
- **2021**: Wesolowski assumes GRH and gives a provably polynomial-time variant.

History and algorithms

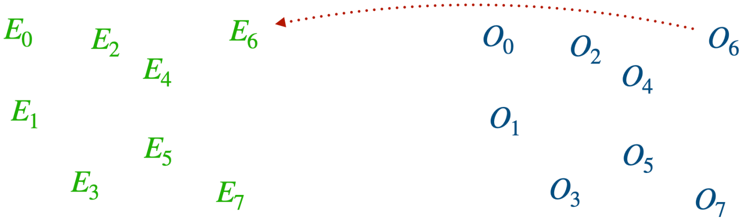
- **1941**: Deuring proves the correspondence.

> Wenn aber $\mathfrak{R}$ eine vorgegebene Maximalordnung in $Q_{\infty,p}$ ist, in der der Primteiler von p Hauptideal ist, so gibt es genau eine Invariante j, zu der dieser Multiplikatorenring gehört, sie ist absolut rational. Ist der Primteiler von p kein Hauptideal, so gibt es zwei konjugierte Invarianten vom Absolutgrad 2 zu diesem Multiplikatorenring. Die Anzahl der j, zu denen eine Maximalordnung von $Q_{\infty,p}$ als Multiplikatorenring gehört, ist gleich der Klassenzahl von $Q_{\infty,p}$.

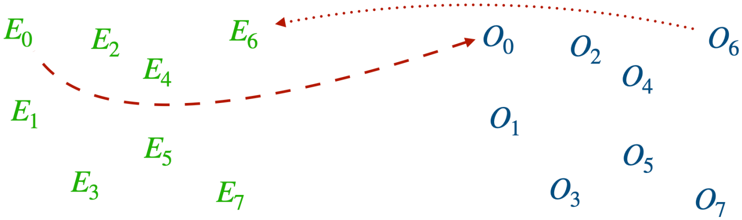
- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014) 🪄) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.
- **2021**: Wesolowski assumes GRH and gives a provably polynomial-time variant.
- **2023**: Eriksen–Panny–Sotáková–Veroni develop practical optimizations and publish a fully general implementation.

From quaternions to curves

From quaternions to curves

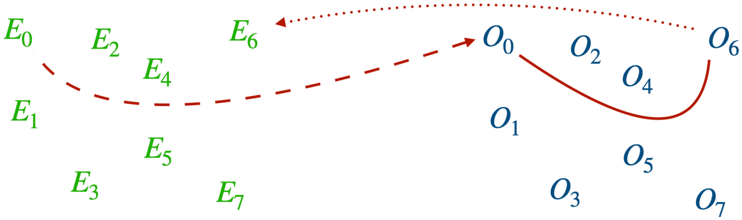


From quaternions to curves



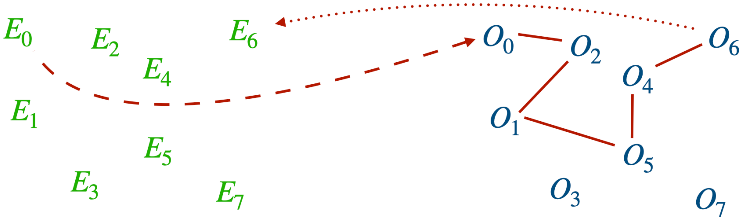
- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.

From quaternions to curves



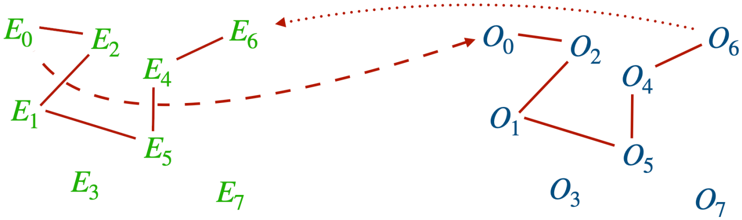
- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal.
  Solve the "isogeny problem" in quaternion land.

From quaternions to curves



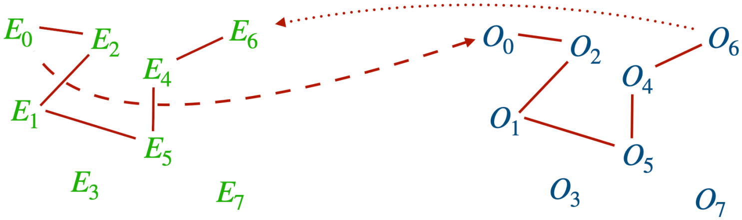
- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT🪄.
  Solve the "isogeny problem" in quaternion land.

From quaternions to curves



- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT.
  Solve the "isogeny problem" in quaternion land.
- Step 2: Ideal-to-isogeny.
  Map the solution "down" to curve land.

From quaternions to curves



- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT🪄.
  Solve the "isogeny problem" in quaternion land.
- Step 2: Ideal-to-isogeny.
  Map the solution "down" to curve land.

I will talk about these *in reverse order*.

Step 2: Ideal-to-isogeny

The isogeny φ_I defined by an ideal I has kernel $H_I = \bigcap_{\alpha \in I} \ker \alpha$.

Step 2: Ideal-to-isogeny

The isogeny φ_I defined by an ideal I has kernel $H_I = \bigcap_{\alpha \in I} \ker \alpha$.

Algorithms:

- Write $I = \mathcal{O}_0(N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.

Step 2: Ideal-to-isogeny

The isogeny φ_I defined by an ideal I has kernel $H_I = \bigcap_{\alpha \in I} \ker \alpha$.

Algorithms:

- Write $I = \mathcal{O}_0(N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, ..., H'_r \rangle$.

Step 2: Ideal-to-isogeny

The isogeny φ_I defined by an ideal I has kernel $H_I = \bigcap_{\alpha \in I} \ker \alpha$.

Algorithms:

- Write $I = \mathcal{O}_0(N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, \ldots, H'_r \rangle$.
- If φ_I is cyclic, we have $\ker(\alpha|_{E[N]}) = \widehat{\alpha}(E[N])$. No logarithms!

Step 2: Ideal-to-isogeny

The isogeny φ_I defined by an ideal I has kernel $H_I = \bigcap_{\alpha \in I} \ker \alpha$.

Algorithms:

- Write $I = \mathcal{O}_0(N, \alpha)$ with $N \in \mathbb{Z}_{>0}$. Then $H_I = \ker(\alpha|_{E[N]})$.
- Better: Factor $N = \ell_1^{e_1} \cdots \ell_r^{e_r}$, let $H'_k = \ker(\alpha|_{E[\ell_k^{e_k}]})$.
  Then $H_I = \langle H'_1, ..., H'_r \rangle$.
- If φ_I is cyclic, we have $\ker(\alpha|_{E[N]}) = \widehat{\alpha}(E[N])$. No logarithms!

Crucial observation: Complexity depends on factorization of N.

Step $0.\overline{9}$: Connecting ideals

Finding **a** connecting $(\mathcal{O}, \mathcal{O}')$-ideal is straightforward:

1. Compute $\mathcal{O}\mathcal{O}' = \text{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.

Step $0.\overline{9}$: Connecting ideals

Finding **a** connecting $(\mathcal{O}, \mathcal{O}')$-ideal is straightforward:

1. Compute $\mathcal{O}\mathcal{O}' = \operatorname{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.
   (Also, it's integral only in trivial cases $\rightsquigarrow$ scale by denominator in $\mathbb{Z}$.)

Step 1: Convenient connecting ideals

KLPT🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Step 1: Convenient connecting ideals

KLPT

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^{\bullet}$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

Step 1: Convenient connecting ideals

KLPT🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Step 1: Convenient connecting ideals

KLPT🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

Step 1: Convenient connecting ideals

<u>**KLPT**</u>🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^{\bullet}$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

<u>Fact:</u> Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* φ_J will be different from φ_I.

Step 1: Convenient connecting ideals

KLPT🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* φ_J will be different from φ_I.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J \varphi_I$ is an endomorphism.

Step 1: Convenient connecting ideals

KLPT🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1}\cdots\ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* φ_J will be different from φ_I.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J\varphi_I$ is an endomorphism.
  - As a quaternion, it is simply given by γ! (Proof: $I\gamma^{-1}\bar{J}\gamma$)

    $\rightsquigarrow$ We can evaluate ω without computing φ_I first.

Step 1: Convenient connecting ideals

KLPT

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1}\cdots\ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* φ_J will be different from φ_I.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J\varphi_I$ is an endomorphism.
  - As a quaternion, it is simply given by γ! (Proof: $I\gamma^{-1}\bar{J}\gamma$)
    $\rightsquigarrow$ We can evaluate ω without computing φ_I first.
  - Hence, for T coprime to N', with $S := N'^{-1} \bmod T$,

$$\varphi_I|_{E[T]} = S\varphi_J\omega|_{E[T]}\,.$$

Step 1: Convenient connecting ideals

KLPT🪄

...finds an equivalent ideal $J = I\overline{\gamma}/N$ of controlled norm N'.

Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

The determining factor of success is the size of the norm. Estimate $\approx p^3$.

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic *codomains*.

- The resulting *isogeny* φ_J will be different from φ_I.
- We can "fix" the evaluation a posteriori:
  - The composition $\omega := \widehat{\varphi}_J \varphi_I$ is an endomorphism.
  - As a quaternion, it is simply given by γ! (Proof: $I\gamma^{-1}\bar{J}\gamma$)

    $\rightsquigarrow$ We can evaluate ω without computing φ_I first.
  - Hence, for T coprime to N', with $S := N'^{-1} \bmod T$,

$$\varphi_I|_{E[T]} = S\varphi_J\omega|_{E[T]} .$$

$\rightsquigarrow$ Do it twice with coprime degrees to evaluate on any point.

Cool trick #1: Convenient torsion is convenient

- Norm is big $\rightsquigarrow$ we have to work in field extensions.

Cool trick #1: Convenient torsion is convenient

- Norm is big $\rightsquigarrow$ we have to work in field extensions.

!! Lots of choice for prime powers ℓ^e.
Trick: Look for $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ with k small.

Cool trick #1: Convenient torsion is convenient

- Norm is big $\rightsquigarrow$ we have to work in field extensions.

!! Lots of choice for prime powers ℓ^e.
Trick: Look for $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ with k small.

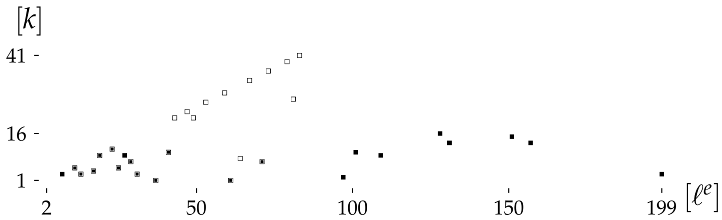
$\rightsquigarrow$ Tradeoff: *number* of operations $\longleftrightarrow$ *cost* of arithmetic.

Cool trick #1: Convenient torsion is convenient

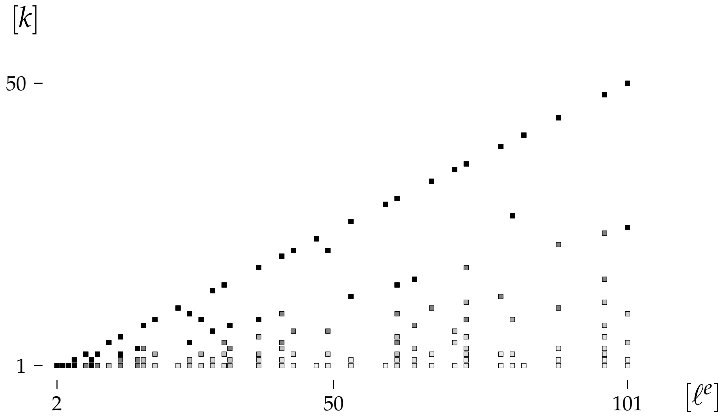
- Norm is big $\rightsquigarrow$ we have to work in field extensions.

!! Lots of choice for prime powers ℓ^e.
Trick: Look for $E[\ell^e] \subseteq E(\mathbb{F}_{p^{2k}})$ with k small.

$\rightsquigarrow$ <u>Tradeoff:</u> *number* of operations $\longleftrightarrow$ *cost* of arithmetic.



Heatmap



Average extension k required to access ℓ^e-torsion.

Cool trick #2: Isogenies from minimal polynomials

Another algorithmic trick for kernel *points* lying in extensions:

Cool trick #2: Isogenies from minimal polynomials

Another algorithmic trick for kernel *points* lying in extensions:

- Replace (big) kernel polynomials by possibly much smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.

Cool trick #2: Isogenies from minimal polynomials

Another algorithmic trick for kernel *points* lying in extensions:

- Replace (big) kernel polynomials by possibly much smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.
- Shoup's algorithm gives a fast method to push minimal polynomials through isogenies. $\rightsquigarrow$ Evaluating isogeny chains.

Cool trick #2: Isogenies from minimal polynomials

Another algorithmic trick for kernel *points* lying in extensions:

- Replace (big) kernel polynomials by possibly much smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.

- Shoup's algorithm gives a fast method to push minimal polynomials through isogenies. $\rightsquigarrow$ Evaluating isogeny chains.

Algorithm 5: `PushSubgroup`(E, f, φ)

Input: Elliptic curve $E/\mathbb{F}_q$, minimal polynomial $f \in \mathbb{F}_q[X]$ of a subgroup $G \leq E$, isogeny $\varphi\colon E \to E'$ defined over $\mathbb{F}_q$.

Output: Minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of the subgroup $\varphi(G) \leq E'$.

Write the x-coordinate map of φ as a fraction g_1/g_2 of polynomials $g_1, g_2 \in \mathbb{F}_q[X]$.
Let $g_{\ker} \leftarrow \gcd(g_2, f)$ and $f_1 \leftarrow f/g_{\ker}$.
Compute $g_1 \cdot g_2^{-1} \bmod f_1 \in \mathbb{F}_q[X]$ and reinterpret it as a quotient-ring element $\alpha \in \mathbb{F}_q[X]/f_1$.
Find the minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of α over $\mathbb{F}_q$ using Shoup's algorithm.
Return f^φ.

Cool trick #2: Isogenies from minimal polynomials

Another algorithmic trick for kernel *points* lying in extensions:

- Replace (big) kernel polynomials by possibly much smaller minimal polynomials of isogenies.
  They are irreducible divisors of the kernel polynomial.
- Shoup's algorithm gives a fast method to push minimal polynomials through isogenies. $\rightsquigarrow$ Evaluating isogeny chains.

Algorithm 5: $\texttt{PushSubgroup}(E, f, \varphi)$

Input: Elliptic curve $E/\mathbb{F}_q$, minimal polynomial $f \in \mathbb{F}_q[X]$ of a subgroup $G \leq E$, isogeny $\varphi\colon E \to E'$ defined over $\mathbb{F}_q$.

Output: Minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of the subgroup $\varphi(G) \leq E'$.

Write the x-coordinate map of φ as a fraction g_1/g_2 of polynomials $g_1, g_2 \in \mathbb{F}_q[X]$.
Let $g_{\text{ker}} \leftarrow \gcd(g_2, f)$ and $f_1 \leftarrow f/g_{\text{ker}}$.
Compute $g_1 \cdot g_2^{-1} \bmod f_1 \in \mathbb{F}_q[X]$ and reinterpret it as a quotient-ring element $\alpha \in \mathbb{F}_q[X]/f_1$.
Find the minimal polynomial $f^\varphi \in \mathbb{F}_q[X]$ of α over $\mathbb{F}_q$ using Shoup's algorithm.
Return f^φ.

Complexity: $O(k^2) + \widetilde{O}(n)$. Naïvely $O(nk(\log k)^{O(1)})$.

Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve E_0 together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general $\left(p \equiv 1 \pmod{12}\right)$.

Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve E_0 together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general $\big(p \equiv 1 \pmod{12}\big)$.

- Ingredient #1: Bröker's algorithm.
  Find q such that $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$ defines $B_{p,\infty}$, find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial H_{-q}, construct a curve with this j-invariant.

Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve E_0 together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general $\big(p \equiv 1 \pmod{12}\big)$.

- Ingredient #1: Bröker's algorithm.
  Find q such that $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$ defines $B_{p,\infty}$, find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial H_{-q}, construct a curve with this j-invariant.

- Ingredient #2: The Bostan-Morain-Salvy-Schost algorithm.
  Algorithm to compute a *normalized* degree-q isogeny in time $\widetilde{O}(q)$.
  Composing the desired endomorphism $\vartheta\colon E \to E$ with the isomorphism $\tau\colon (x,y) \mapsto (-qx, \sqrt{-q}^3 y)$ makes it normalized.

Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve E_0 together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general $\big(p \equiv 1 \pmod{12}\big)$.

- Ingredient #1: Bröker's algorithm.
  Find q such that $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$ defines $B_{p,\infty}$, find a root $j \in \mathbb{F}_p$ of the Hilbert class polynomial H_{-q}, construct a curve with this j-invariant.

- Ingredient #2: The Bostan-Morain-Salvy-Schost algorithm.
  Algorithm to compute a *normalized* degree-q isogeny in time $\widetilde{O}(q)$.
  Composing the desired endomorphism $\vartheta\colon E \to E$ with the isomorphism $\tau\colon (x, y) \mapsto (-qx, \sqrt{-q}^3 y)$ makes it normalized.

- Ingredient #3: Ibukiyama's theorem.
  Explicit basis for a maximal order of $B_{p,\infty}$ with an endomorphism $\sqrt{-q}$.
  In fact, there are only very few maximal orders containing $\sqrt{-q}$.

Open-source code

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

(Eriksen, Panny, Sotáková, Veroni; 2023)

Open-source code

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

(Eriksen, Panny, Sotáková, Veroni; 2023)

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
```

Open-source code

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

(Eriksen, Panny, Sotáková, Veroni; 2023)

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
```

Open-source code

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

(Eriksen, Panny, Sotáková, Veroni; 2023)

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
sage: E0, iota, O0 = starting_curve(F2)
```

Open-source code

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

(Eriksen, Panny, Sotáková, Veroni; 2023)

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
sage: E0, iota, O0 = starting_curve(F2)
sage: I = random_ideal(O0)
sage: I
Fractional ideal (-2227737332 - 2733458099/2*i - 36405/2*j
    + 7076*k, -1722016565/2 + 1401001825/2*i + 551/2*j
    + 16579/2*k, -2147483647 - 9708*j + 12777*k, -2147483647
    - 2147483647*i - 22485*j + 3069*k)
```

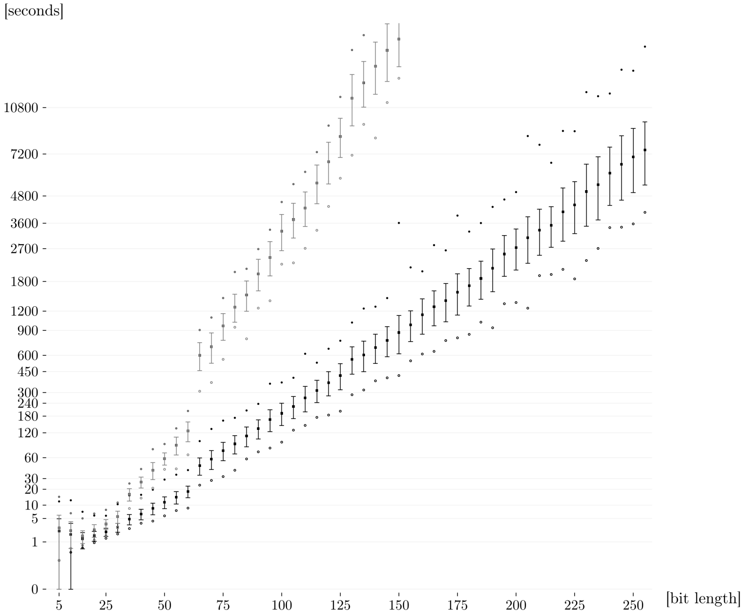
Open-source code

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

(Eriksen, Panny, Sotáková, Veroni; 2023)

```
sage: from deuring.broker import starting_curve
sage: from deuring.randomideal import random_ideal
sage: from deuring.correspondence import constructive_deuring
sage: F2.<i> = GF((2^31-1, 2), modulus=[1,0,1])
sage: E0, iota, O0 = starting_curve(F2)
sage: I = random_ideal(O0)
sage: I
Fractional ideal (-2227737332 - 2733458099/2*i - 36405/2*j
    + 7076*k, -1722016565/2 + 1401001825/2*i + 551/2*j
    + 16579/2*k, -2147483647 - 9708*j + 12777*k, -2147483647
    - 2147483647*i - 22485*j + 3069*k)
sage: E1, phi, _ = constructive_deuring(I, E0, iota)
sage: phi
Composite morphism of degree 14763897348161206530374369280
                = 2^29*3^3*5*7^2*11*13*17*31*41*43^2*61*79*151:
  From: Elliptic Curve defined by y^2 = x^3 + x over
            Finite Field in i of size 2147483647^2
  To:   Elliptic Curve defined by y^2 = x^3 + (1474953432*i
                +1816867654)*x + (581679615*i+260136654)
            over Finite Field in i of size 2147483647^2
```

Timings (SageMath, single core)



Timings (SageMath, single core)

We've been informed of one run for a ≈ 500-bit characteristic that took only about 7 hours.

$\rightsquigarrow$ Definitely practical for parameter setup, cryptanalysis, etc.!

Questions?

(Also feel free to email me: `lorenz@yx7.cc`)