Deuring for the People:

Supersingular Elliptic Curves with Prescribed Endomorphism Ring in General Characteristic

Jonathan K. Eriksen, Lorenz Panny, Jana Sotáková, Mattia Veroni

Academia Sinica, Taipei, Taiwan

Eindhoven, 13 July 2023

What?

Deering correspondence:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

What?

Deuring correspondence:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

What?

Deuring correspondence:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

This talk: **How?**

What?

Deuring correspondence:

Almost exact equivalence between the worlds of maximal orders in certain quaternion algebras and of supersingular elliptic curves.

The correspondence is polynomial-time in the $\Longrightarrow$ direction.

This talk: **How?**

(The $\Longleftarrow$ direction is exponential-time as far as we know.)

$\longrightarrow$ See for instance Annamaria Iezzi's talk in MS28 on Tuesday.

PSA

PSA

[ˈdɔʏ̯ʁɪŋ]

Why?

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

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

Why?

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

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.

Why?

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

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.
- **SQIsign** builds on the $\Longrightarrow$ direction constructively.

Why?

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

(Wesolowski '21: "Orientations and the supersingular endomorphism ring problem").

- $\approx$All isogeny assumptions reduce to the $\Longleftarrow$ direction.
- **SQIsign** builds on the $\Longrightarrow$ direction constructively.
- Essential tool for both constructions and attacks.

History lesson

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

History lesson

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

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 $Q_{\infty,p}$.

History lesson

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

  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 lesson

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

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

History lesson

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

  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 $Q_{\infty,p}$.

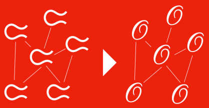
- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014)) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.
- **2017**: They publish it.

History lesson

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

  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 $Q_{\infty,p}$.

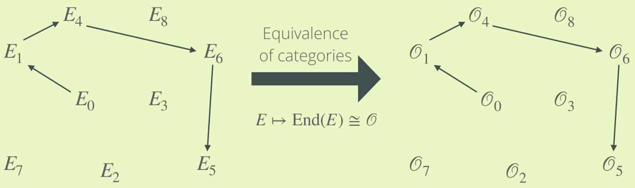
- **2004**: Cerviño gives a (necessarily exponential-time) algorithm to compute all pairs $(E, \mathcal{O})$ for a given p.
- **2013**: Chevyrev–Galbraith give an exponential-time algorithm to compute $\mathcal{O} \mapsto E$.
- **201_**: Petit–Lauter (using Kohel–Lauter–Petit–Tignol (2014)) find a heuristically polynomial-time algorithm for $\mathcal{O} \mapsto E$.
- **2017**: They publish it.
- **2021**: Wesolowski assumes GRH and gives a provably polynomial-time variant.



The Deuring Correspondence

Deuring correspondence

world of supersingular curves / **world of maximal orders**



curve-order dictionary

supersingular curves	**quaternion orders**
curve E (up to Galois conjugacy)	maximal order $\mathcal{O}$ (up to isomorphism)
isogeny $\varphi : E_1 \to E_2$	integral ideal I_φ that is left $\mathcal{O}_1$-ideal and right $\mathcal{O}_2$-ideal
endomorphism $\psi : E \to E$	principal ideal $(\beta) \subset \mathcal{O}$
and this continues for the *degree*, the *dual*, *equivalence*, *composition*...	and this continues for the *norm*, the *dual*, *equivalence*, *multiplication*...

Curve world

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

Curve world

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

Curve world

- Universe: Characteristic p. Assume $p \geq 5$.
- 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 $\mathbb{Q}^4$.
- Quaternion lattices are represented by **a** $\mathbb{Z}$-basis.

Computationally, ...

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

General theme: Things are easy in quaternion land.

From curves to quaternions

$$E \mapsto \mathrm{End}(E)$$

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

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

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

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

In decreasing order of obviousness, one can show that

$$\omega^3 = [1],\ \omega\pi + \pi\omega = -\pi,\ \text{and}\ \pi^2 = [-p].$$

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

$$E \mapsto \mathrm{End}(E)$$

From curves to quaternions

$$E \mapsto \mathrm{End}(E)$$

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

From curves to quaternions

$$E \mapsto \mathrm{End}(E)$$

- 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
    $$\mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}, \; (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is polynomial-time.

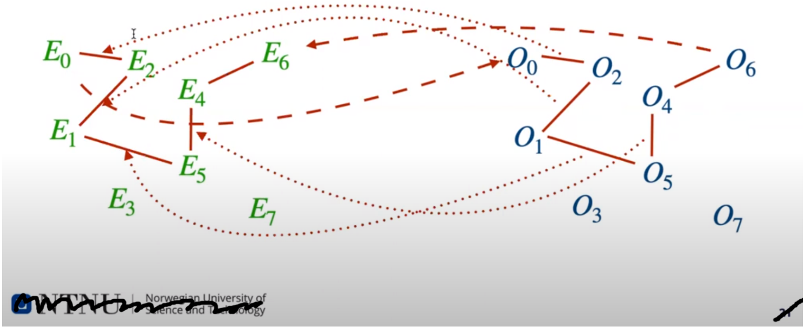
From curves to quaternions

$$E \mapsto \mathrm{End}(E)$$

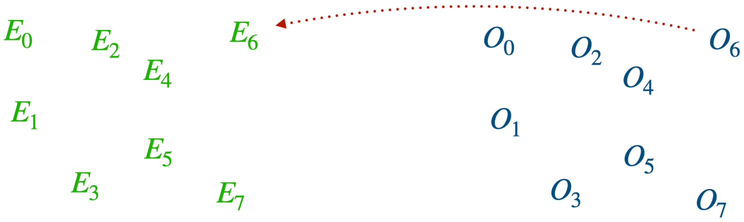
- Subtlety: Identifying explicit endomorphisms with abstract elements of $B_{p,\infty}$ is generally not totally trivial.
  - Distinction between *MaxOrder* and *EndRing* problems.
  - Gram–Schmidt-type procedure using the trace pairing
    $$\mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}, \ (\alpha, \beta) \mapsto \widehat{\alpha}\beta + \alpha\widehat{\beta}.$$
    This is polynomial-time.
  - Multiple q define the *same* $B_{p,\infty}$.
    Need to convert from $\mathbf{i}^2 = -q$ basis to $\mathbf{i}'^2 = -q'$ basis.

From quaternions to curves

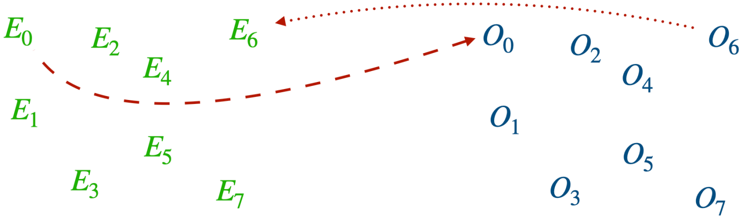
From quaternions to curves



From quaternions to curves

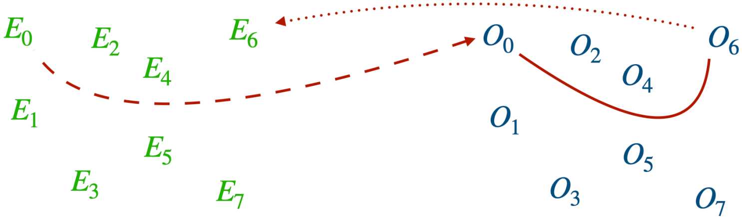


From quaternions to curves



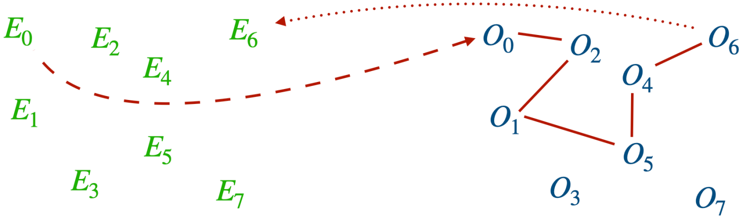
- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.

From quaternions to curves



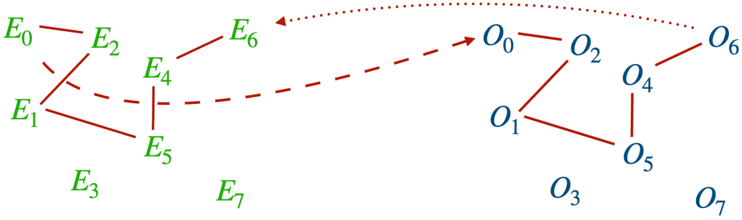
- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal.
  Solve the "isogeny problem" in quaternion land.

From quaternions to curves



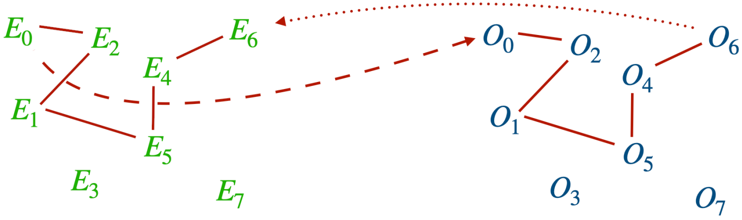
- Step 0: Base curve.
  Any curve over $\mathbb{F}_p$ with a known small-degree endomorphism.
- Step 1: Connecting ideal + KLPT🪄.
  Solve the "isogeny problem" in quaternion land.

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 $H_I = \bigcap_{\omega \in I} \ker \omega$.

Step 2: Ideal-to-isogeny

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

Algorithms:

- Write $I = (N, \alpha)$ 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 $H_I = \bigcap_{\omega \in I} \ker \omega$.

Algorithms:

- Write $I = (N, \alpha)$ 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 $H_I = \bigcap_{\omega \in I} \ker \omega$.

Algorithms:

- Write $I = (N, \alpha)$ 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 $\ker(\alpha|_{E[N]}) = \overline{\alpha}(E[N])$. No logarithms!

Step 2: Ideal-to-isogeny

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

Algorithms:

- Write $I = (N, \alpha)$ 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 $\ker(\alpha|_{E[N]}) = \overline{\alpha}(E[N])$. No logarithms!

Crucial observation: Complexity depends on factorization of N.

Step 2: Ideal-to-isogeny

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

<u>Algorithms:</u>

- Write $I = (N, \alpha)$ 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 $\ker(\alpha|_{E[N]}) = \overline{\alpha}(E[N])$. No logarithms!

Crucial observation: Complexity depends on factorization of N.
$\frown$ No choice in N: It's the norm of I.

Step 1: Convenient connecting ideals

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

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

Step 1: Convenient connecting ideals

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

1. Compute $\mathcal{O}\mathcal{O}' = \mathrm{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.

Step 1: Convenient connecting ideals

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

1. Compute $\mathcal{O}\mathcal{O}' = \mathrm{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.

KLPT

...finds an equivalent ideal of controlled norm.

Step 1: Convenient connecting ideals

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

1. Compute $\mathcal{O}\mathcal{O}' = \mathrm{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.

KLPT🪄

...finds an equivalent ideal of controlled norm.

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

Step 1: Convenient connecting ideals

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

1. Compute $\mathcal{O}\mathcal{O}' = \mathrm{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.

KLPT🪄

...finds an equivalent ideal of controlled norm.

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

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

1. Compute $\mathcal{O}\mathcal{O}' = \text{span}_{\mathbb{Z}}(\{\alpha\beta : \alpha \in \mathcal{O}, \beta \in \mathcal{O}'\}) \subseteq B_{p,\infty}$.
2. That's all, but typically the norm of $\mathcal{O}\mathcal{O}'$ is horrible.

KLPT

...finds an equivalent ideal of controlled norm.

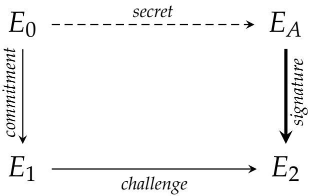
Typical cases: Norm $\ell^\bullet$, powersmooth norm $\ell_1^{e_1} \cdots \ell_r^{e_r}$.

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

Fact: Equivalent ideals $\rightsquigarrow$ isomorphic codomains.

SQIsign

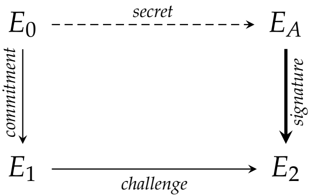
...is a signature scheme based on the Deuring correspondence.



⟶ See Antonin Leroux's talk in MS118 on Friday, or `https://sqisign.org`!

SQIsign

...is a signature scheme based on the Deuring correspondence.



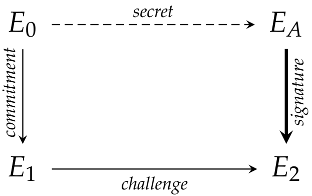
⟶ See Antonin Leroux's talk in MS118 on Friday, or https://sqisign.org!

!! SQIsign relies on very special choices of p.

⟶ See Michael Meyer's talk in MS105 on Friday.

SQIsign

...is a signature scheme based on the Deuring correspondence.



$\longrightarrow$ See Antonin Leroux's talk in MS118 on Friday, or `https://sqisign.org`!

!! SQIsign relies on very special choices of p.

$\longrightarrow$ See Michael Meyer's talk in MS105 on Friday.

- Cryptographic reductions and general computer algebra want it to be fast for arbitrary fields. $\rightsquigarrow$ Our work!

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

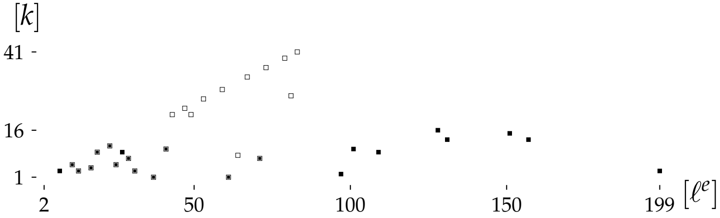
- Norm is big $\rightsquigarrow$ We have to work in field extensions.

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

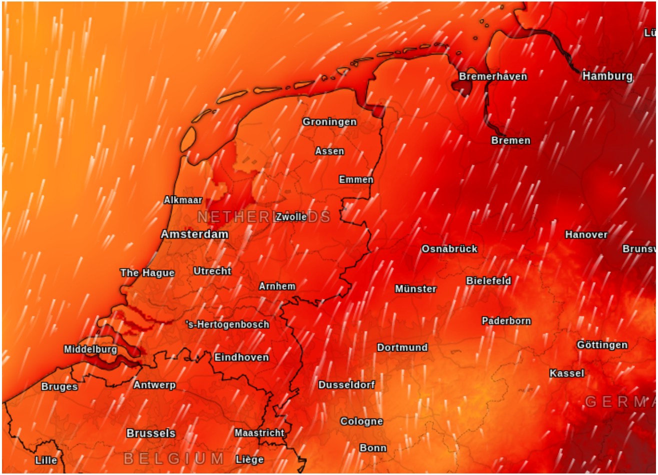
$\rightsquigarrow$ Tradeoff: *number* of operations $\longleftrightarrow$ *cost* of arithmetic.

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

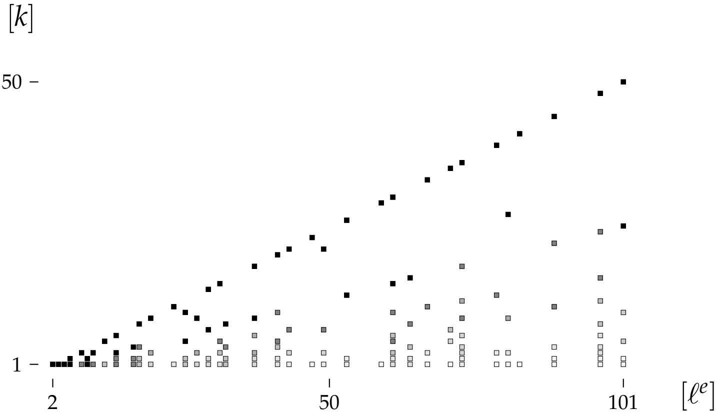


Heatmap



Bremerhaven
Hamburg
Groningen
Assen
Bremen
Emmen
Alkmaar
NETHERLANDS
Zwolle
Amsterdam
Hanover
Osnabrück
The Hague
Utrecht
Arnhem
Münster
Bielefeld
's-Hertogenbosch
Paderborn
Middelburg
Dortmund
Göttingen
Eindhoven
Bruges
Antwerp
Dusseldorf
Kassel
Cologne
Brussels
Maastricht
Bonn
Lille
BELGIUM
Liège

Heatmap



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

Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by smaller minimal polynomials of isogenies.

  They are irreducible divisors of the kernel polynomial.

Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by 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

- We can replace (big) kernel polynomials by 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. ⇝ 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 $g_{\text{ker}} \leftarrow \gcd(g_2, f)$ 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.

Cool trick #2: Isogenies from minimal polynomials

- We can replace (big) kernel polynomials by 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 $g_{\mathrm{ker}} \leftarrow \gcd(g_2, f)$ and $f_1 \leftarrow f/g_{\mathrm{ker}}$.
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 together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- 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 together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- 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 $\vartheta : E \to E$ with the isomorphism $\tau : (x, y) \mapsto (-qx, \sqrt{-q}^3 y)$ makes it normalized.

Step 0 (cool trick #3): Base curves

- Step 0 is to construct a supersingular elliptic curve together with a small-degree endomorphism.
  Often easy to explicitly write down; tricky in general.

- 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, such a maximal order is almost unique.

Cool open-source code

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

Cool open-source code

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

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

Cool open-source code

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

```
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])
```

Cool open-source code

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

```
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)
```

Cool open-source code

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

```
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)
```

Cool open-source code

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

```
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)