Challenges in generating random supersingular elliptic curves over finite fields of large characteristic

ANNAMARIA IEZZI
Université Grenoble Alpes

René25
Tahiti - August 18, 2025

Today's problem

Given a large prime p, compute an explicit equation, or equivalently a j-invariant, for a supersingular elliptic curve over $\overline{\mathbb{F}_p}$ without revealing its endomorphism ring.

Today's problem

Given a large prime p, compute an explicit equation, or equivalently a j-invariant, for a supersingular elliptic curve over $\overline{\mathbb{F}_p}$ without revealing its endomorphism ring.

This problem makes sense since computing the endomorphism ring of a supersingular elliptic curve over a finite field is a hard problem.

The inspiration for this talk comes from:

J. Booher, R. Bowden, J. Doliskani, T. B. Fouotsa, S. D. Galbraith, S. Kunzweiler, S.-P. Merz, C. Petit, B. Smith, K. E. Stange, Y. B. Ti, C. Vincent, J. F. Voloch, C. Weitkämper, and L. Zobernig.
Failing to hash into supersingular isogeny graphs.
https://eprint.iacr.org/2022/518.pdf, **(2022)**.
The Computer Journal, Volume 67, Issue 8, August 2024, Pages 2702–271

M. Mula, N. Murru, and F. Pintore.
On Random Sampling of Supersingular Elliptic Curves.
https://eprint.iacr.org/2022/528, **(2022)**.
Ann. Mat. Pura Appl. (4) 204, No. 3, 1293-1335 (2025).

Endomorphisms of elliptic curves

- An endomorphism of an elliptic curve E defined over a field K is an isogeny $\alpha : E \to E$ or the zero morphism.

Endomorphisms of elliptic curves

- An endomorphism of an elliptic curve E defined over a field K is an isogeny $\alpha : E \to E$ or the zero morphism.
- We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

Endomorphisms of elliptic curves

- An endomorphism of an elliptic curve E defined over a field K is an isogeny $\alpha : E \to E$ or the zero morphism.

- We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

  We can define two operations on $\mathrm{End}(E)$. Let $\alpha, \beta \in \mathrm{End}(E)$:

$$\alpha + \beta : \begin{array}{rcl} E & \to & E \\ P & \mapsto & \alpha(P) + \beta(P) \end{array} \qquad \alpha \circ \beta : \begin{array}{rcl} E & \to & E \\ P & \mapsto & \alpha(\beta(P)) \end{array}$$

  $(\mathrm{End}(E), +, \circ)$ is a ring, called the (geometric) endomorphism ring.

Endomorphisms of elliptic curves

- An endomorphism of an elliptic curve E defined over a field K is an isogeny $\alpha : E \to E$ or the zero morphism.

- We denote $\mathrm{End}(E) := \{\text{endomorphisms of } E \text{ over } \overline{K}\}$.

  We can define two operations on $\mathrm{End}(E)$. Let $\alpha, \beta \in \mathrm{End}(E)$:

$$\alpha + \beta : \begin{array}{rcl} E & \to & E \\ P & \mapsto & \alpha(P) + \beta(P) \end{array} \qquad \alpha \circ \beta : \begin{array}{rcl} E & \to & E \\ P & \mapsto & \alpha(\beta(P)) \end{array}$$

  $(\mathrm{End}(E), +, \circ)$ is a ring, called the (geometric) endomorphism ring.

- We denote $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$. the endomorphism algebra of E.

Trivial endomorphisms

For every $n \in \mathbb{Z}$, the multiplication-by-n map

$$\begin{array}{rrcl} [n]: & E & \to & E \\ & P & \mapsto & nP = \underbrace{P + \cdots + P}_{n \text{ times}} \end{array}$$

is an endomorphism. We call it a **trivial** or **scalar endomorphism.**

Trivial endomorphisms

For every $n \in \mathbb{Z}$, the multiplication-by-n map

$$\begin{array}{rccc} [n]: & E & \rightarrow & E \\ & P & \mapsto & nP = \underbrace{P + \cdots + P}_{n \text{ times}} \end{array}$$

is an endomorphism. We call it a **trivial** or **scalar endomorphism.**

Therefore there is an embedding:

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E) \\ n & \mapsto & [n]. \end{array}$$

Trivial endomorphisms

For every $n \in \mathbb{Z}$, the multiplication-by-n map

$$\begin{array}{rccc} [n]: & E & \to & E \\ & P & \mapsto & nP = \underbrace{P + \cdots + P}_{n \text{ times}} \end{array}$$

is an endomorphism. We call it a **trivial** or **scalar endomorphism.**

Therefore there is an embedding:

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathrm{End}(E) \\ n & \mapsto & [n]. \end{array}$$

and $\mathrm{End}(E)$ has also the structure of a free $\mathbb{Z}$-module.

The Frobenius endomorphism

When $K = \mathbb{F}_q$ is a finite field, then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \rightarrow & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

The Frobenius endomorphism

When $K = \mathbb{F}_q$ is a finite field, then we always have the Frobenius endomorphism defined as

$$\begin{array}{rccc} \pi_E : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

The Frobenius endomorphism

When $K = \mathbb{F}_q$ is a finite field, then we always have the Frobenius endomorphism defined as

$$\begin{array}{cccc} \pi_E : & E & \to & E \\ & (x, y) & \mapsto & (x^q, y^q). \end{array}$$

So

$$\mathbb{Z} \subseteq \mathbb{Z}[\pi_E] \subseteq \mathrm{End}(E).$$

Attention: in some cases $\pi_E \in \mathbb{Z}$ and $\mathbb{Z}[\pi_E] = \mathbb{Z}$.

Over finite fields

When K is a finite field, End(E) is always lager than $\mathbb{Z}$.

Over finite fields

When K is a finite field, $\mathrm{End}(E)$ is always lager than $\mathbb{Z}$.

- If E is **ordinary** then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and $\mathrm{End}(E)$ is isomorphic to an order inside L.

Over finite fields

When K is a finite field, $\text{End}(E)$ is always lager than $\mathbb{Z}$.

- If E is **ordinary** then $\text{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and $\text{End}(E)$ is isomorphic to an order inside L.
- If E is **supersingular** then $\text{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and

  $$\text{End}(E) \simeq \mathcal{O},$$

  where $\mathcal{O}$ is a maximal order inside $B_{p,\infty}$.

Over finite fields

When K is a finite field, $\mathrm{End}(E)$ is always lager than $\mathbb{Z}$.

- If E is **ordinary** then $\mathrm{End}^0(E)$ is isomorphic to the imaginary quadratic field $L = \mathbb{Q}(\pi_E)$ and $\mathrm{End}(E)$ is isomorphic to an order inside L.

- If E is **supersingular** then $\mathrm{End}^0(E) \simeq B_{p,\infty}$ (the quaternion algebra ramified exactly at p and ∞) and

$$\mathrm{End}(E) \simeq \mathcal{O},$$

where $\mathcal{O}$ is a maximal order inside $B_{p,\infty}$. In particular

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma,$$

where $\alpha, \beta, \gamma \in \mathrm{End}(E)$ are nontrivial endomorphisms.

Motivation: isogeny-based cryptography

Motivation: isogeny-based cryptography

- A new kind of elliptic curve cryptography.

Motivation: isogeny-based cryptography

- A new kind of elliptic curve cryptography.
- Introduced in 1997 by Couveignes, gained interest in the math-crypto community starting in the 2010s.

Motivation: isogeny-based cryptography

- A new kind of elliptic curve cryptography.
- Introduced in 1997 by Couveignes, gained interest in the math-crypto community starting in the 2010s.
- Based on the *isogeny problem* (between supersingular elliptic curves), which is conjectured to be hard even for quantum computers, making it a candidate for post-quantum cryptography.

Motivation: isogeny-based cryptography

- A new kind of elliptic curve cryptography.
- Introduced in 1997 by Couveignes, gained interest in the math-crypto community starting in the 2010s.
- Based on the *isogeny problem* (between supersingular elliptic curves), which is conjectured to be hard even for quantum computers, making it a candidate for post-quantum cryptography.
- Two proposals to the NIST Post-Quantum Cryptography standardization process:
  - **SIDH/SIKE** (2017): key exchange protocol, broken in 2022.
  - **SQI-Sign** (2023): signature scheme, now in round 2.

Equivalent supersingular computational problems

ISOGENY

Isogeny problem

Given two isogenous elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, find an isogeny $\varphi : E_1 \to E_2$.

Equivalent supersingular computational problems

ISOGENY

Isogeny problem
Given two isogenous elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, find an isogeny $\varphi : E_1 \to E_2$.

ENDRING

Supersingular endomorphism ring problem
Given a supersingular elliptic curve defined over over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

Equivalent supersingular computational problems

ISOGENY

Isogeny problem
Given two isogenous elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, find an isogeny $\varphi : E_1 \to E_2$.

ENDRING

Supersingular endomorphism ring problem
Given a supersingular elliptic curve defined over over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

ONEEND

One Endomorphism problem
Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

Equivalent supersingular computational problems

ISOGENY

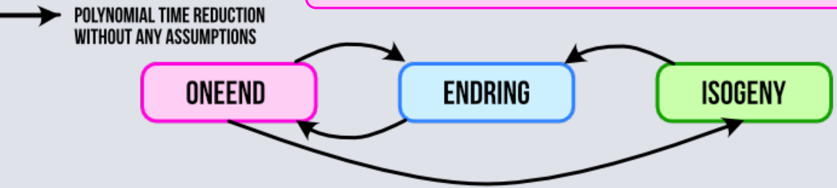
Isogeny problem
Given two isogenous elliptic curves E_1 and E_2 defined over $\mathbb{F}_{p^2}$, find an isogeny $\varphi : E_1 \to E_2$.

ENDRING

Supersingular endomorphism ring problem
Given a supersingular elliptic curve defined over over $\mathbb{F}_{p^2}$, compute its endomorphism ring.

ONEEND

One Endomorphism problem
Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.



2018 - K. Eisenträger, S. Hallgren, K. Lauter, T. Morrison, and C. Petit
Supersingular isogeny graphs and endomorphism rings: Reductions and solutions.

Advances in Cryptology – EUROCRYPT 2018.

2020 - K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, and J. Park.
Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs.
Proceedings of the Fourteenth Algorithmic Number Theory Symposium.

2022 - B. Wesolowski
The supersingular isogeny path and endomorphism ring problems are equivalent.
2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)

2024 - A. Page and B. Wesolowski
The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent.
Advances in Cryptology – EUROCRYPT 2024

2025 - A. H. Le Merdy and B. Wesolowski
The supersingular endomorphism ring problem given one endomorphism.
Preprint

2025 - A. H. Le Merdy and B. Wesolowski
Unconditional foundations for supersingular isogeny-based cryptography.
Preprint

ONEEND

One Endomorphism problem

Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, compute $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:**

$$\left\{ \begin{array}{c} \overline{\mathbb{F}}_p\text{-isomorphism classes of supersingular elliptic curves} \\ \text{defined over } \overline{\mathbb{F}}_p \end{array} \right\}$$

$$\updownarrow$$

$$\{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}$$

- **Edges:** isogenies of degree ℓ (up to a certain equivalence).

Supersingular ℓ-isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$.

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:**

$$\left\{ \begin{array}{c} \overline{\mathbb{F}}_p\text{-isomorphism classes of supersingular elliptic curves} \\ \text{defined over } \overline{\mathbb{F}}_p \end{array} \right\}$$

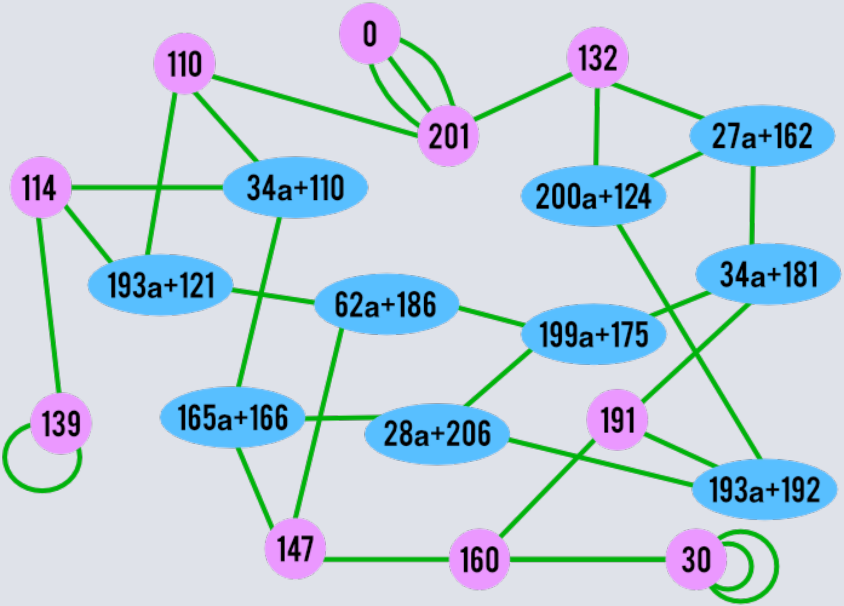
$$\updownarrow$$

$$\{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}$$

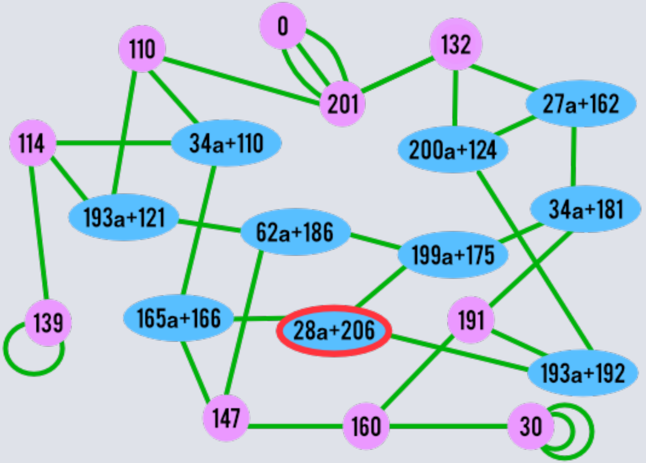
- **Edges:** isogenies of degree ℓ (up to a certain equivalence).

$$\text{Number of vertices} \sim \frac{p}{12}.$$

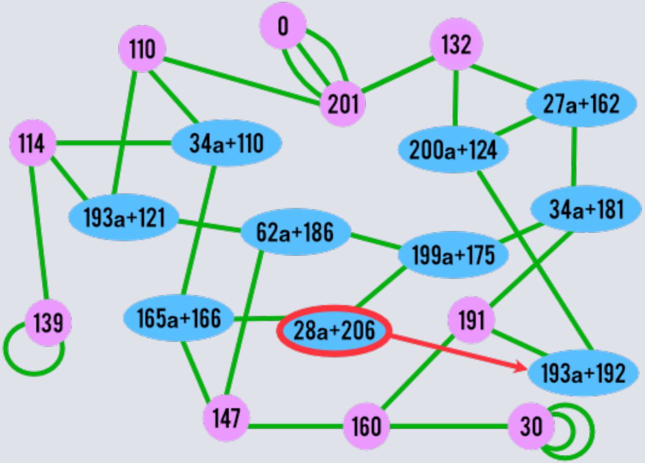
A toy example: $\mathcal{G}_2(\overline{\mathbb{F}}_{227})$



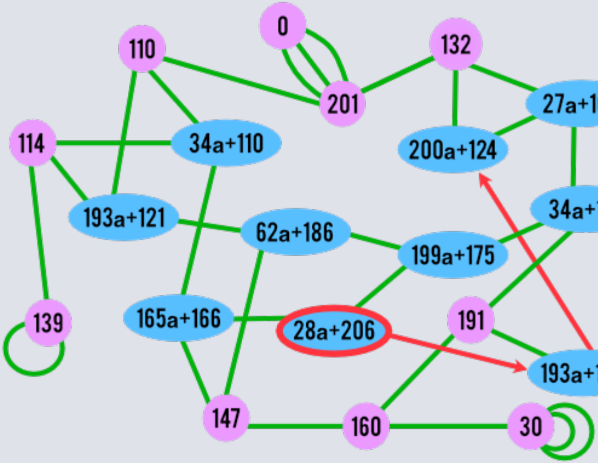
A nontrivial endomorphism in the graph



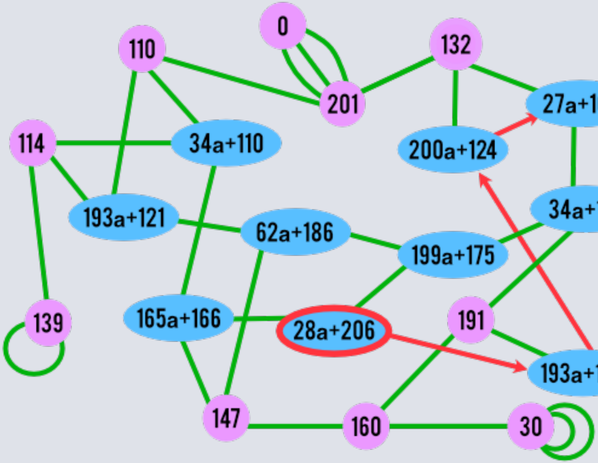
A nontrivial endomorphism in the graph



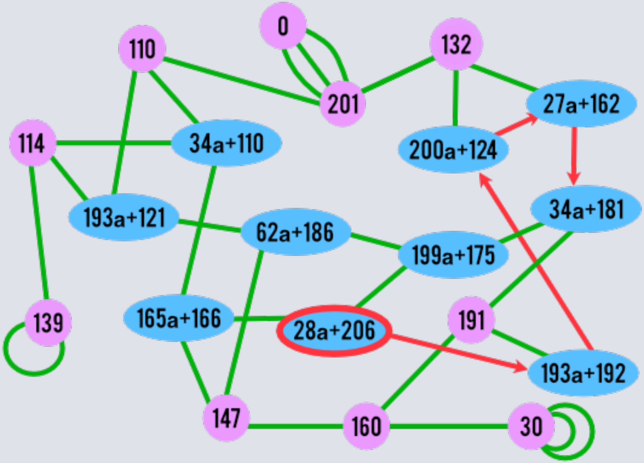
A nontrivial endomorphism in the graph



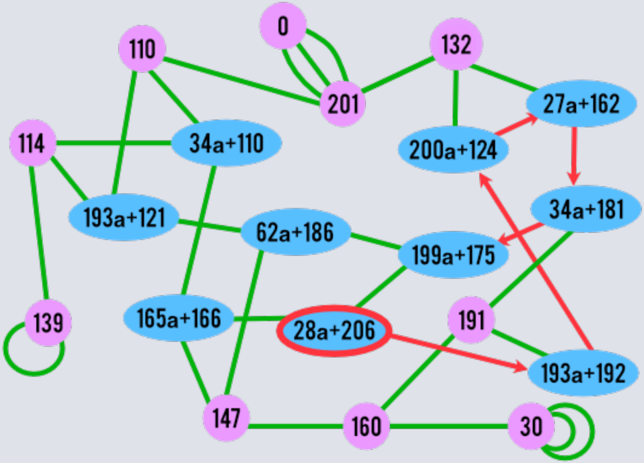
A nontrivial endomorphism in the graph



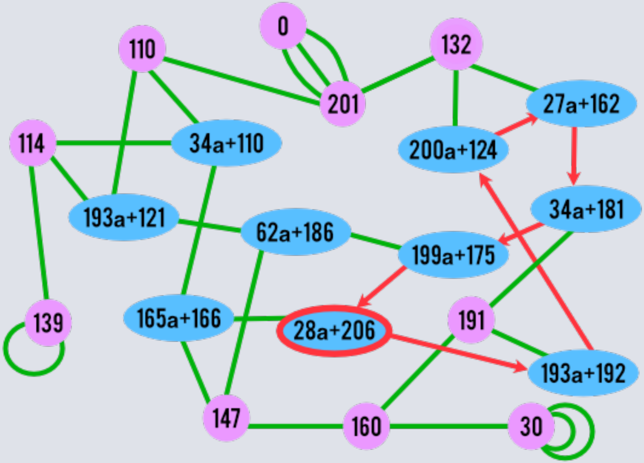
A nontrivial endomorphism in the graph



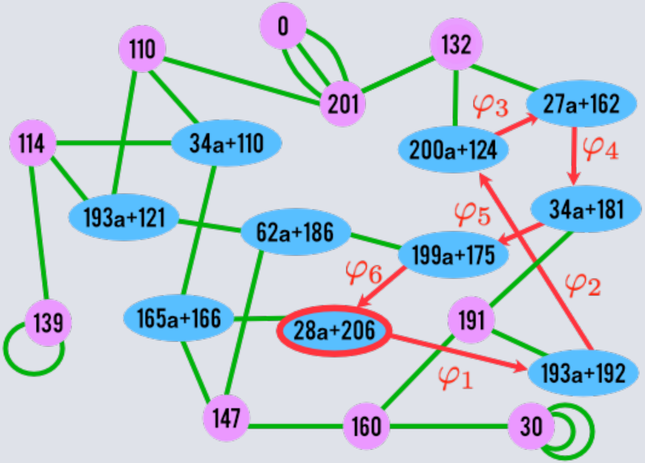
A nontrivial endomorphism in the graph



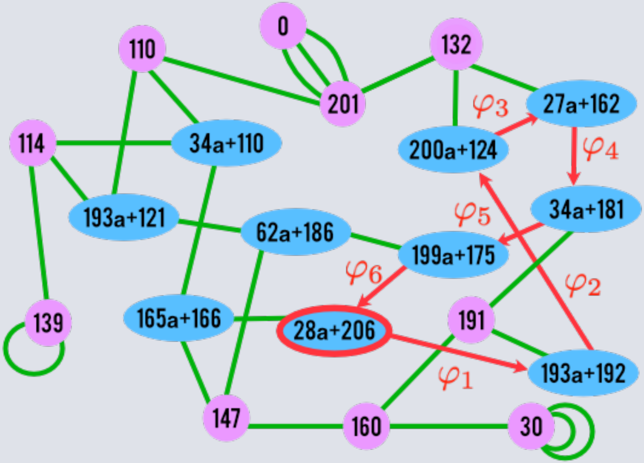
A nontrivial endomorphism in the graph



A nontrivial endomorphism in the graph



A nontrivial endomorphism in the graph



$$\varphi_6 \circ \varphi_5 \circ \cdots \circ \varphi_1 \in \mathrm{End}(E_{28a+206}).$$

Algorithms for computing nontrivial enndomorphisms

D. Kohel
Endomorphism rings of elliptic curves over finite fields.
PhD thesis, University of California, Berkeley, (1996).

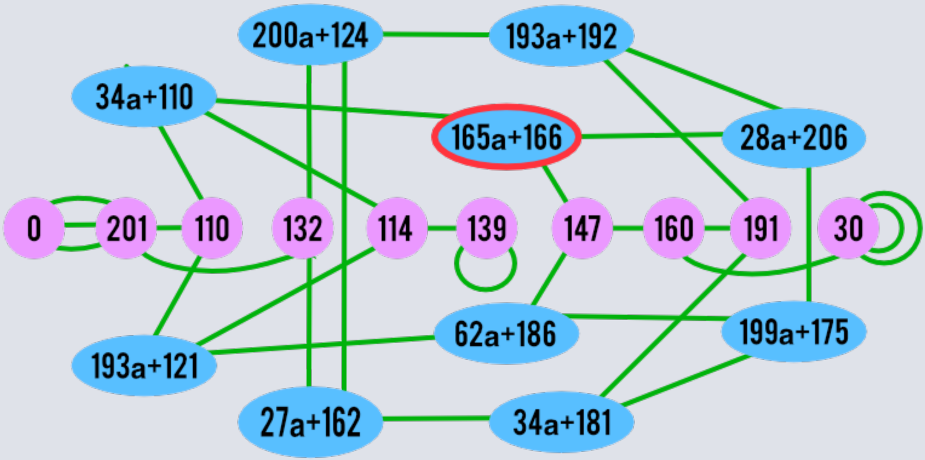
C. Delfs, and S.D. Galbraith
Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$.
Des. Codes Cryptography 78, No. 2, 425-440 (2016).

K. Eisenträger, S. Hallgren, C. Leonardi, T. Morrison, and J. Park.
Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs.
Proceedings of the Fourteenth Algorithmic Number Theory Symposium, pages 215–232, (2020).

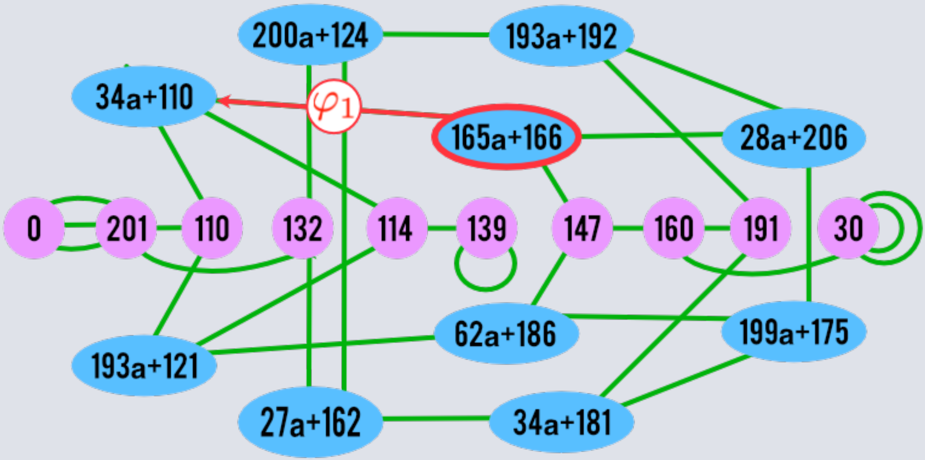
A. Page and B. Wesolowski
The Supersingular Endomorphism Ring and One Endomorphism Problems are Equivalent
Advances in Cryptology – EUROCRYPT 2024

J. Fuselier, A. I., M. Kozek, T. Morrison, and C. Namoijam
Computing supersingular endomorphism rings using inseparable endomorphisms.
Journal of Algebra, Volume 668, pp 145–189, (2025)

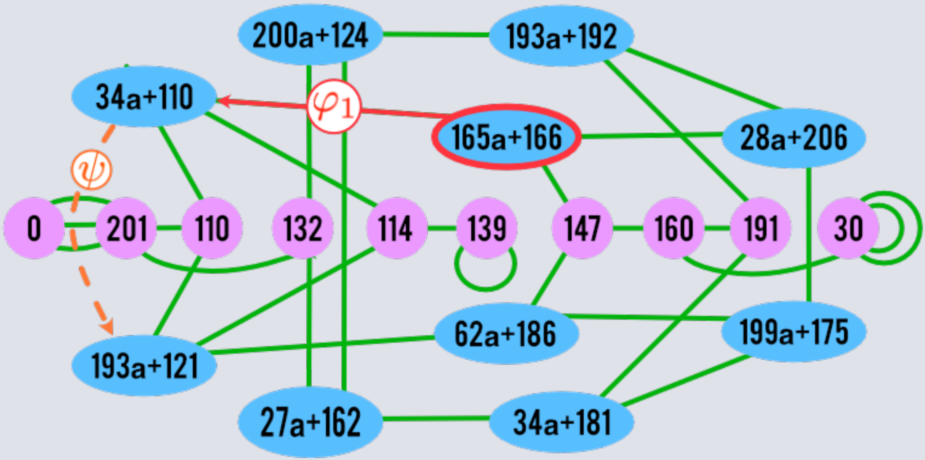
Our idea (Fuselier, I., Kozek, Morrison, Namoijam)



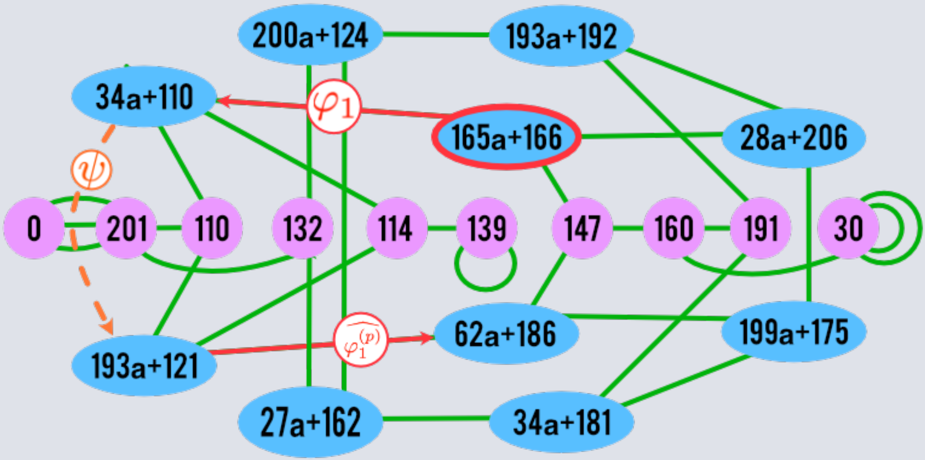
Our idea (Fuselier, I., Kozek, Morrison, Namoijam)



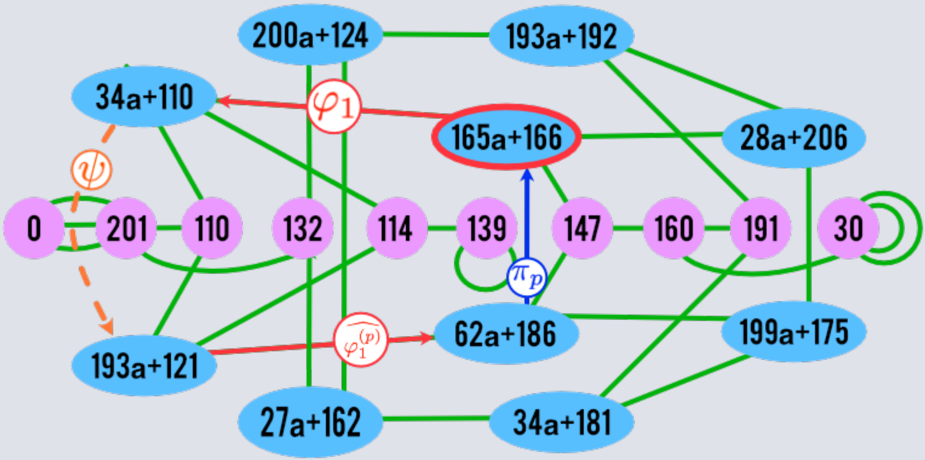
Our idea (Fuselier, I., Kozek, Morrison, Namoijam)



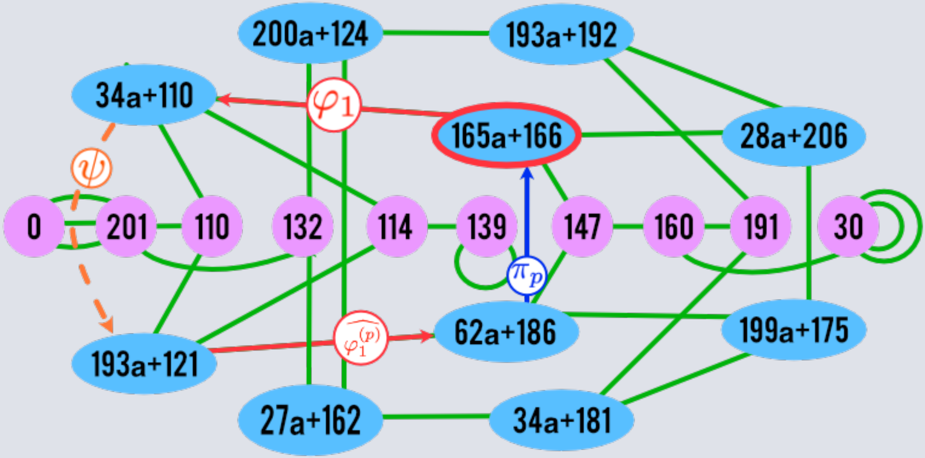
Our idea (Fuselier, I., Kozek, Morrison, Namoijam)



Our idea (Fuselier, I., Kozek, Morrison, Namoijam)

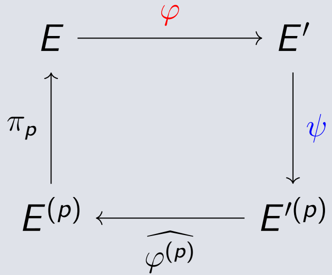


Our idea (Fuselier, I., Kozek, Morrison, Namoijam)



We call $\pi_p \circ \widehat{\varphi_1^{(p)}} \circ \psi \circ \varphi_1$ an *inseparable reflection*.

Inseparable reflections



- $\varphi\colon E \to E'$ is a cyclic isogeny of degree ℓ^t,
- $\psi\colon E' \to E'^{(p)}$ is an isogeny of degree d,

where ℓ is prime, and d is square-free and coprime with ℓ.

$$\alpha := \pi_p \circ \widehat{\varphi^{(p)}} \circ \psi \circ \varphi$$

is an **inseparable reflection** of degree $dp\ell^{2t}$.

Our algorithm: performance analysis

1. **Time Complexity** for computing one endomorphism:

   $$\tilde{O}(\sqrt{p}), \text{ under GRH}$$

2. **Storage requirement** for computing one endomorphism:

   $$O((\log(p))^2)$$

Our algorithm: performance analysis

1. **Time Complexity** for computing one endomorphism:

$$\tilde{O}(\sqrt{p}), \text{ under GRH}$$

2. **Storage requirement** for computing one endomorphism:

$$O((\log(p))^2)$$

3. **Towards the full endomorphism ring**: If α and β are two endormorphisms computed in this way (in two different ℓ-isogeny graphs), then:

   - α and β do not commute.
   - $\Lambda := \mathbb{Z} + \alpha\mathbb{Z} + \beta\mathbb{Z} + \alpha\beta\mathbb{Z}$ is Bass.

Back to today's problem

Given a large prime p, compute an explicit equation, or equivalently a j-invariant, for a supersingular elliptic curve over $\overline{\mathbb{F}_p}$ without revealing its endomorphism ring.

Back to today's problem

Given a large prime p, compute an explicit equation, or equivalently a j-invariant, for a supersingular elliptic curve over $\overline{\mathbb{F}_p}$ without revealing its endomorphism ring.

Such a curve is called in the literature a hard curve.

In isogeny-based cryptography...

Knowing the endomorphism ring of the starting curve (public parameter):

In isogeny-based cryptography...

Knowing the endomorphism ring of the starting curve (public parameter):

- Sometimes it is **required for protocol construction** (this is the case of SQISign).

In isogeny-based cryptography...

Knowing the endomorphism ring of the starting curve (public parameter):

- Sometimes it is **required for protocol construction** (this is the case of SQISign).
- It may **lead to insecurity** (e.g., the CGL hash function is not collision resistant when starting from a curve with a known endomorphism ring).

In isogeny-based cryptography...

Knowing the endomorphism ring of the starting curve (public parameter):

- Sometimes it is **required for protocol construction** (this is the case of SQISign).
- It may **lead to insecurity** (e.g., the CGL hash function is not collision resistant when starting from a curve with a known endomorphism ring).

In any case knowing both the endomorphism rings of two supersingular elliptic curves E_1 and E_2 allows one to compute an isogeny $\varphi : E_1 \to E_2$ in polynomial time.

We'll present some ideas from:

- **J. Booher, R. Bowden, J. Doliskani, T. B. Fouotsa, S. D. Galbraith, S. Kunzweiler, S.-P. Merz, C. Petit, B. Smith, K. E. Stange, Y. B. Ti, C. Vincent, J. F. Voloch, C. Weitkämper, and L. Zobernig.**
  Failing to hash into supersingular isogeny graphs.
  https://eprint.iacr.org/2022/518.pdf, **(2022)**.
  The Computer Journal, Volume 67, Issue 8, August 2024, Pages 2702–271

- **M. Mula, N. Murru, and F. Pintore.**
  On Random Sampling of Supersingular Elliptic Curves.
  https://eprint.iacr.org/2022/528, **(2022)**.
  Ann. Mat. Pura Appl. (4) 204, No. 3, 1293-1335 (2025).

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

(3) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

(3) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;

(4) $\sharp E(\mathbb{F}_q) \equiv 1 \pmod p$ (equivalently $\mathrm{tr}(\pi_E) \equiv 0 \pmod p$);

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

(3) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;

(4) $\sharp E(\mathbb{F}_q) \equiv 1 \pmod{p}$ (equivalently $\mathrm{tr}(\pi_E) \equiv 0 \pmod{p}$);

(5) $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$:

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

(3) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;

(4) $\sharp E(\mathbb{F}_q) \equiv 1 \pmod{p}$ (equivalently $\mathrm{tr}(\pi_E) \equiv 0 \pmod{p}$);

(5) $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$:

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma, \quad \alpha, \beta, \gamma \in \mathrm{End}(E).$$

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

(3) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;

(4) $\sharp E(\mathbb{F}_q) \equiv 1 \pmod{p}$ (equivalently $\mathrm{tr}(\pi_E) \equiv 0 \pmod{p}$);

(5) $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$:

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma, \quad \alpha, \beta, \gamma \in \mathrm{End}(E).$$

(6) The Hasse invariant of E is 0.

Is $j_0 \in \mathbb{F}_{p^2}$ a supersingular j-invariant?

Is $j_0 \in \mathbb{F}_{p^2}$ a supersingular j-invariant?

To determine whether a given j-invariant corresponds to a supersingular elliptic curve:

- Use **René's algorithm** to compute the trace of Frobenius of the corresponding elliptic curve.
- The curve is supersingular if the trace t satisfies $t \equiv 0 \pmod{p}$.

Is $j_0 \in \mathbb{F}_{p^2}$ a supersingular j-invariant?

To determine whether a given j-invariant corresponds to a supersingular elliptic curve:

- Use **René's algorithm** to compute the trace of Frobenius of the corresponding elliptic curve.
- The curve is supersingular if the trace t satisfies $t \equiv 0 \pmod{p}$.
- **Time complexity:** $O(\log^5 p)$.

Exhaustive search

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\mathrm{Prob}(j \in \mathbb{F}_{p^2}$ is supersingular$)$

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\text{Prob}(j \in \mathbb{F}_{p^2} \text{ is supersingular}) \approx \frac{1}{12p}$.

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\mathrm{Prob}(j \in \mathbb{F}_{p^2} \text{ is supersingular}) \approx \frac{1}{12p}$.

$\mathrm{Prob}(j \in \mathbb{F}_p \text{ is supersingular})$

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\mathrm{Prob}(j \in \mathbb{F}_{p^2} \text{ is supersingular}) \approx \frac{1}{12p}$.

$\mathrm{Prob}(j \in \mathbb{F}_p \text{ is supersingular}) = \frac{\tilde{O}(\sqrt{p})}{p}$

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\mathrm{Prob}(j \in \mathbb{F}_{p^2} \text{ is supersingular}) \approx \frac{1}{12p}$.

$\mathrm{Prob}(j \in \mathbb{F}_{p} \text{ is supersingular}) = \frac{\tilde{O}(\sqrt{p})}{p} \approx \frac{1}{\sqrt{p}}$.

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\text{Prob}(j \in \mathbb{F}_{p^2} \text{ is supersingular}) \approx \frac{1}{12p}$.

$\text{Prob}(j \in \mathbb{F}_p \text{ is supersingular}) = \frac{\tilde{O}(\sqrt{p})}{p} \approx \frac{1}{\sqrt{p}}$.

Supersingular *j*-invariants are rare!

Exhaustive search

$$S_p = \{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}.$$

$$\sharp S_p = \left\lfloor \frac{p-1}{12} \right\rfloor + \begin{cases} 0 & : p \equiv 1 \pmod{12} \\ 1 & : p \equiv 5, 7 \pmod{12} \\ 2 & : p \equiv 11 \pmod{12} \end{cases}$$

$\text{Prob}(j \in \mathbb{F}_{p^2} \text{ is supersingular}) \approx \frac{1}{12p}$.

$\text{Prob}(j \in \mathbb{F}_p \text{ is supersingular}) = \frac{\tilde{O}(\sqrt{p})}{p} \approx \frac{1}{\sqrt{p}}$.

Supersingular j-invariants are rare!

For p of cryptographic size, exhaustive search for supersingular j-invariants is computationally infeasible in both $\mathbb{F}_{p^2}$ and $\mathbb{F}_p$.

The cSRS problem

Given a prime p, generate uniformly random supersingular curves E over $\mathbb{F}_{p^2}$ (or equivalently superingular j-invariants in $\mathbb{F}_{p^2}$) without revealing anything about the endomorphism ring.

Crypto **S**upersingular **R**andom **S**ampling problem **(cSRS)**

A simpler problem

Given a prime p, generate uniformly random supersingular curves E over $\mathbb{F}_{p^2}$ (or equivalently superingular j-invariants in $\mathbb{F}_{p^2}$) ~~without revealing anything about the endomorphism ring.~~

~~Crypto~~ **S**upersingular **R**andom **S**ampling problem

(~~c~~SRS)

Deuring's theorem (part 1)

Theorem. Let p be a prime number, $p \geq 5$.

Let E be an elliptic curve over a number field K, with $\mathrm{End}(E)$ isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field L. Let $\mathfrak{p}$ be a prime ideal of K above p, and suppose that E has a good reduction modulo $\mathfrak{p}$, denoted by $\tilde{E}$.

Deuring's theorem (part 1)

Theorem. Let p be a prime number, $p \geq 5$.

Let E be an elliptic curve over a number field K, with $\mathrm{End}(E)$ isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field L. Let $\mathfrak{p}$ be a prime ideal of K above p, and suppose that E has a good reduction modulo $\mathfrak{p}$, denoted by $\tilde{E}$.

Then $\tilde{E}$ is supersingular if and only if there is only one prime ideal of L above p (i.e., p does not split over L).

Deuring's theorem (part 1)

Theorem. Let p be a prime number, $p \geq 5$.

Let E be an elliptic curve over a number field K, with $\mathrm{End}(E)$ isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field L. Let $\mathfrak{p}$ be a prime ideal of K above p, and suppose that E has a good reduction modulo $\mathfrak{p}$, denoted by $\tilde{E}$.

Then $\tilde{E}$ is supersingular if and only if there is only one prime ideal of L above p (i.e., p does not split over L).

Rermark: p does not split over L of discriminant D if and only if $\left(\frac{D}{p}\right) \neq 1$.

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

1: Set $q \leftarrow 3$

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

1: Set $q \leftarrow 3$
2: **while** $\left(\frac{-q}{p}\right) = 1$ **do**
3: Assign q to the next prime equivalent to $3 \pmod 4$
4: **end while**

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

1: Set $q \leftarrow 3$
2: **while** $\left(\frac{-q}{p}\right) = 1$ **do**
3: Assign q to the next prime equivalent to $3 \pmod 4$
4: **end while**
5: Compute the Hilbert class polynomial $H_{\mathcal{O}}$ relative to the quadratic order $\mathcal{O}$ of discriminant $-q$

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

1: Set $q \leftarrow 3$
2: **while** $\left(\frac{-q}{p}\right) = 1$ **do**
3: Assign q to the next prime equivalent to $3 \pmod 4$
4: **end while**
5: Compute the Hilbert class polynomial $H_{\mathcal{O}}$ relative to the quadratic order $\mathcal{O}$ of discriminant $-q$
6: Find a root $\alpha \in \mathbb{F}_p$ of $H_{\mathcal{O}}$ modulo p

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

Set $q \leftarrow 3$
while $\left(\frac{-q}{p}\right) = 1$ **do**
    Assign q to the next prime equivalent to $3 \pmod 4$
end while
Compute the Hilbert class polynomial $H_{\mathcal{O}}$ relative to the quadratic order $\mathcal{O}$ of discriminant $-q$
Find a root $\alpha \in \mathbb{F}_p$ of $H_{\mathcal{O}}$ modulo p
Set $j \leftarrow \alpha$

Bröker's algorithm

Input: A prime $p \geq 5$.
Output: A supersingular j-invariant $j \in \mathbb{F}_p$.

```
Set q ← 3
while (−q/p) = 1 do
    Assign q to the next prime equivalent to 3 (mod 4)
end while
Compute the Hilbert class polynomial H_O relative to the
quadratic order O of discriminant −q
Find a root α ∈ F_p of H_O modulo p
Set j ← α
```

Complexity: $\tilde{O}((\log p)^3)$

Remarks

(1) **Broker's algorithm does not sample uniformly random supersingular elliptic curves**.

Remarks

(1) **Broker's algorithm does not sample uniformly random supersingular elliptic curves**.

For any p, the output belongs to a pre-determined subset of all possible supersingular j-invariants over $\mathbb{F}_{p^2}$, i.e. the roots of $H_{\mathcal{O}}$ in $\mathbb{F}_p$, which are $\tilde{O}(\sqrt{q})$.

Remarks

(1) **Broker's algorithm does not sample uniformly random supersingular elliptic curves**.

For any p, the output belongs to a pre-determined subset of all possible supersingular j-invariants over $\mathbb{F}_{p^2}$, i.e. the roots of $H_{\mathcal{O}}$ in $\mathbb{F}_p$, which are $\tilde{O}(\sqrt{q})$.

$$\Downarrow$$

Random walks in the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$ starting from an output of Broker's algorithm.

Deuring's theorem (part 2)

Theorem. Let $\mathcal{E}$ be an elliptic curve over $\overline{\mathbb{F}_p}$ and let $\alpha_0 \in \mathrm{End(E)} \setminus \mathbb{Z}$.

Then there exists an elliptic curve E defined over a number field K, an endomorphism α of E and a good reduction $\tilde{E}$ of E at a prime $\mathfrak{p}$ of K above p, such that $\mathcal{E}$ is isomorphic to $\tilde{E}$ and α_0 corresponds to $\tilde{\alpha}$ (the reduction of α at $\mathfrak{p}$) under the isomorphism

$$\eta : \tilde{E} \to \mathcal{E}, \qquad \eta \circ \tilde{\alpha} \circ \eta^{-1} = \alpha_0.$$

Remarks

(2) **If E is an output of Bröker's algorithm, then $\mathrm{End}(E)$ can be computed efficiently.**

Remarks

(2) **If E is an output of Bröker's algorithm, then** $\mathrm{End}(E)$ **can be computed efficiently.**

- A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$.
- In particular $\mathrm{End}(E)$ contains a non-trivial endomorphism of small degree, so the endomorphism ring can be heuristically computed in polynomial time (Love–Boneh 2020).

Remarks

(2) **If E is an output of Bröker's algorithm, then** $\mathrm{End}(E)$ **can be computed efficiently.**

- A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$.
- In particular $\mathrm{End}(E)$ contains a non-trivial endomorphism of small degree, so the endomorphism ring can be heuristically computed in polynomial time (Love–Boneh 2020).

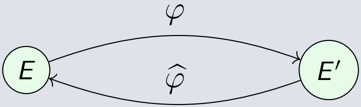
(3) Walks in the isogeny graph translate the information about the endomorphism ring from a curve to another:

Remarks

(2) **If E is an output of Bröker's algorithm, then** $\mathrm{End}(E)$ **can be computed efficiently.**

- A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$.
- In particular $\mathrm{End}(E)$ contains a non-trivial endomorphism of small degree, so the endomorphism ring can be heuristically computed in polynomial time (Love–Boneh 2020).

(3) Walks in the isogeny graph translate the information about the endomorphism ring from a curve to another:



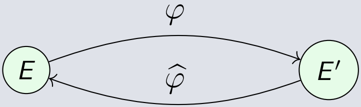
$$\alpha \in \mathrm{End}(E) \dashrightarrow \frac{1}{\deg \varphi}(\varphi \circ \alpha \circ \widehat{\varphi}) \in \mathrm{End}(E')$$

Remarks

(2) **If E is an output of Bröker's algorithm, then** $\mathrm{End}(E)$ **can be computed efficiently.**

- A copy of $\mathcal{O}$ is embedded in $\mathrm{End}(E)$.
- In particular $\mathrm{End}(E)$ contains a non-trivial endomorphism of small degree, so the endomorphism ring can be heuristically computed in polynomial time (Love–Boneh 2020).

(3) Walks in the isogeny graph translate the information about the endomorphism ring from a curve to another:



$$\alpha \in \mathrm{End}(E) \dashrightarrow \frac{1}{\deg \varphi}(\varphi \circ \alpha \circ \widehat{\varphi}) \in \mathrm{End}(E')$$

So, the combination of Broker's algorithm and random walks solves the SRS, but not the cSRS problem.

Equivalent definitions for supersingular elliptic curves over finite fields

Theorem. Let $q = p^n$, where p is a prime number, and let E be an elliptic curve over $\mathbb{F}_q$. Then the following are equivalent:

(1) E is a supersingular elliptic curve;

(2) $E[p^r] = \{O_E\}$, for one (all) $r \geq 1$;

(3) The map $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$;

(4) $\sharp E(\mathbb{F}_q) \equiv 1 \pmod{p}$;

(5) $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$:

$$\mathrm{End}(E) = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\beta + \mathbb{Z}\gamma, \quad \alpha, \beta, \gamma \in \mathrm{End}(E).$$

(6) The Hasse invariant of E is 0.

Hasse invariant

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if the Hasse invariant of E is 0.

Hasse invariant

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if the Hasse invariant of E is 0.

Let $p > 2$ be a prime number, the *Hasse polynomial* or *supersingular polynomial* is

$$H_p(t) = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 t^j$$

Hasse invariant

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if the Hasse invariant of E is 0.

Let $p > 2$ be a prime number, the *Hasse polynomial* or *supersingular polynomial* is

$$H_p(t) = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 t^j$$

Proposition. Let E_λ denote the elliptic curve

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \qquad \text{(Legendre form)}$$

then E_λ is supersingular if and only if $\lambda \in \mathbb{F}_{p^2}$ is a root of $H_p(t)$.

Hasse invariant

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if the Hasse invariant of E is 0.

Let $p > 2$ be a prime number, the *Hasse polynomial* or *supersingular polynomial* is

$$H_p(t) = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 t^j$$

Proposition. Let E_λ denote the elliptic curve

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \qquad \text{(Legendre form)}$$

then E_λ is supersingular if and only if $\lambda \in \mathbb{F}_{p^2}$ is a root of $H_p(t)$.

How to find a root of $H_p(t)$ efficiently?

Larger endomorphism ring

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Larger endomorphism ring

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Idea. Find roots of the polynomial

$$f_{n,m,p}(x) := \gcd(\Phi_n(x, x^p), \Phi_m(x, x^p)).$$

Larger endomorphism ring

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Idea. Find roots of the polynomial

$$f_{n,m,p}(x) := \gcd(\Phi_n(x, x^p), \Phi_m(x, x^p)).$$

This method produces curves known to have endomorphisms of degree nm, np and mp,

Larger endomorphism ring

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if $\text{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Idea. Find roots of the polynomial

$$f_{n,m,p}(x) := \gcd(\Phi_n(x, x^p), \Phi_m(x, x^p)).$$

This method produces curves known to have endomorphisms of degree nm, np and mp, and since we wish to avoid endomorphisms of small degree we should take at least one of n and m to be exponentially large.

Larger endomorphism ring

An elliptic curve E over $\mathbb{F}_q$ is supersingular if and only if $\mathrm{End}(E)$ is an order in a quaternion algebra over $\mathbb{Q}$.

Idea. Find roots of the polynomial

$$f_{n,m,p}(x) := \gcd(\Phi_n(x, x^p), \Phi_m(x, x^p)).$$

This method produces curves known to have endomorphisms of degree nm, np and mp, and since we wish to avoid endomorphisms of small degree we should take at least one of n and m to be exponentially large.

How to find roots in $\mathbb{F}_{p^2}$ of the polynomial $f_{n,m,p}(x)$ efficiently?

Reverse René's algorithm

For $p > 3$, an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if $\sharp E(\mathbb{F}_p) = p + 1$.

Reverse René's algorithm

For $p > 3$, an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if $\sharp E(\mathbb{F}_p) = p + 1$.

Idea. Given $p > 3$, construct E over $\mathbb{F}_p$ such that $\sharp E(\mathbb{F}_p) = p + 1$.

Reverse René's algorithm

For $p > 3$, an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if $\sharp E(\mathbb{F}_p) = p + 1$.

Idea. Given $p > 3$, construct E over $\mathbb{F}_p$ such that $\sharp E(\mathbb{F}_p) = p + 1$.

$$p = \prod_{i=1}^{r} \ell_i - 1, \text{ where } \ell_i \text{ are small distinct odd primes.}$$

Reverse René's algorithm

For $p > 3$, an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if $\sharp E(\mathbb{F}_p) = p + 1$.

Idea. Given $p > 3$, construct E over $\mathbb{F}_p$ such that $\sharp E(\mathbb{F}_p) = p + 1$.

$$p = \prod_{i=1}^{r} \ell_i - 1, \text{ where } \ell_i \text{ are small distinct odd primes.}$$

Then $\sharp E(\mathbb{F}_{p^2}) = \prod_{i=1}^{r} \ell_i^2$, so the ℓ_i-torsion is $\mathbb{F}_{p^2}$-rational, $\forall\, \ell_i$.

Reverse René's algorithm

For $p > 3$, an elliptic curve E over $\mathbb{F}_p$ is supersingular if and only if $\sharp E(\mathbb{F}_p) = p + 1$.

Idea. Given $p > 3$, construct E over $\mathbb{F}_p$ such that $\sharp E(\mathbb{F}_p) = p + 1$.

$$p = \prod_{i=1}^{r} \ell_i - 1, \text{ where } \ell_i \text{ are small distinct odd primes.}$$

Then $\sharp E(\mathbb{F}_{p^2}) = \prod_{i=1}^{r} \ell_i^2$, so the ℓ_i-torsion is $\mathbb{F}_{p^2}$-rational, $\forall\, \ell_i$.

$$\Downarrow$$

Compute solutions of the system in the variables x_{ℓ_i} and a:

$$\begin{cases} \psi_{\ell_i}(x_{\ell_i}, a) = 0, & \forall i = 1, \dots, r \\ x_{\ell_i}^{p^2} - x_{\ell_i} = 0, & \forall i = 1, \dots, r \end{cases}$$

where $\psi_{\ell_i}(x_i, a)$ is the division polynomial of order ℓ_i of the curve parameterized by a.

Another approach based on then umber of rational points?

An elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular if and only if $\sharp E(\mathbb{F}_{p^2}) \equiv 1 \pmod{p}$.

Another approach based on then umber of rational points?

An elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular if and only if $\sharp E(\mathbb{F}_{p^2}) \equiv 1 \pmod{p}$.

Remark: $\mathbb{F}_{p^2}$-maximal curves of genus 1 are supersingular elliptic curve defined over $\mathbb{F}_{p^2}$

Another approach based on then umber of rational points?

An elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular if and only if $\sharp E(\mathbb{F}_{p^2}) \equiv 1 \pmod{p}$.

Remark: $\mathbb{F}_{p^2}$-maximal curves of genus 1 are supersingular elliptic curve defined over $\mathbb{F}_{p^2}$

$$\sharp E(\mathbb{F}_{p^2}) = p^2 + 1 + 2p$$

Another approach based on then umber of rational points?

An elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular if and only if $\sharp E(\mathbb{F}_{p^2}) \equiv 1 \pmod{p}$.

Remark: $\mathbb{F}_{p^2}$-maximal curves of genus 1 are supersingular elliptic curve defined over $\mathbb{F}_{p^2}$

$$\sharp E(\mathbb{F}_{p^2}) = p^2 + 1 + 2p$$

$$\Downarrow$$

$$t = -2p \equiv 0 \pmod{p}$$

Another approach based on then umber of rational points?

An elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular if and only if $\sharp E(\mathbb{F}_{p^2}) \equiv 1 \pmod{p}$.

Remark: $\mathbb{F}_{p^2}$-maximal curves of genus 1 are supersingular elliptic curve defined over $\mathbb{F}_{p^2}$

$$\sharp E(\mathbb{F}_{p^2}) = p^2 + 1 + 2p$$

$$\Downarrow$$

$$t = -2p \equiv 0 \pmod{p}$$

$$\Downarrow$$

E is supersingular.

Another approach based on then umber of rational points?

An elliptic curve E over $\mathbb{F}_{p^2}$ is supersingular if and only if $\sharp E(\mathbb{F}_{p^2}) \equiv 1 \pmod{p}$.

Remark: $\mathbb{F}_{p^2}$-maximal curves of genus 1 are supersingular elliptic curve defined over $\mathbb{F}_{p^2}$

$$\sharp E(\mathbb{F}_{p^2}) = p^2 + 1 + 2p$$

$$\Downarrow$$

$$t = -2p \equiv 0 \pmod{p}$$

$$\Downarrow$$

E is supersingular.

Can techniques for constructing maximal curves be adapted or extended to produce $\mathbb{F}_{p^2}$-maximal curve of genus 1, for a large prime p?


Māuruuru roa