Hard problems in isogeny-based crypto

Monika Trimoska

Discrete Algebra and Geometry Seminar

Eindhoven, November 5, 2026

TU/e

Elliptic curves



What is an elliptic curve?

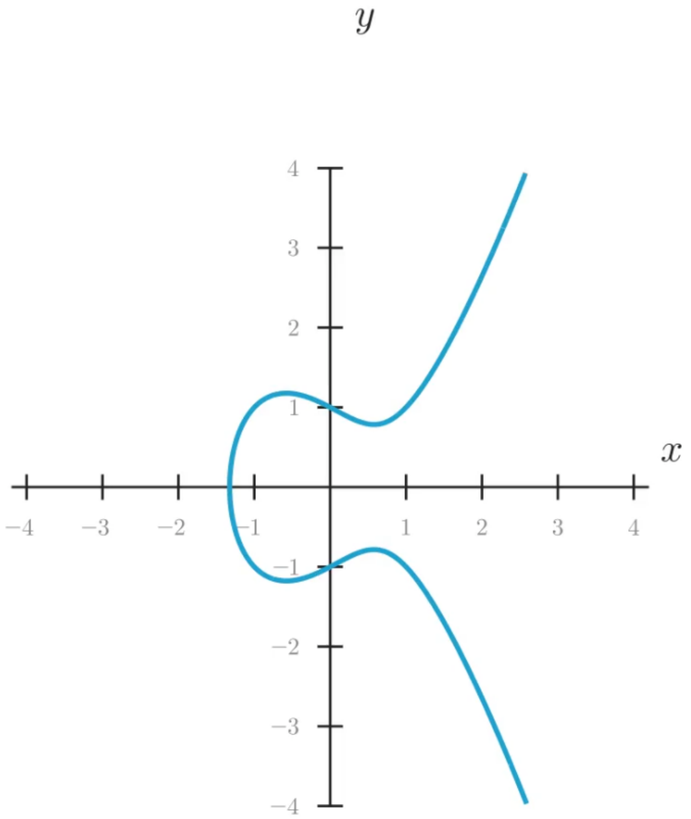
An elliptic curve is an algebraic curve that admits an affine equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

(general form of a Weierstrass curve)

with $a_i \in k$, where k is the field where the point is defined.

Example. $y^2 = x^3 - x + 1$



→ A point on E means that the point (x, y) satisfies the curve equation.

Elliptic curves over $\mathbb{F}_q$

In cryptography, we use elliptic curves over finite fields $\mathbb{F}_q$, $q = p^k$ (but we draw the figures over $\mathbb{R}$ because it's nicer).

→ We denote by $E(k)$ the set of k-rational points on E.

↳ defined over k

Hasse bound

$$\#E(\mathbb{F}_q) \in [q + 1 - 2\sqrt{(q)}, q + 1 + 2\sqrt{(q)}]$$

Elliptic curves in cryptography

- Short Weierstrass form

$$y^2 = x^3 + c_4 x + c_6$$

- The set of points on E with the addition law form a group.

- The group law is constructed geometrically.

Elliptic curves in cryptography

- Short Weierstrass form

$$y^2 = x^3 + c_4 x + c_6$$

- The set of points on E with the addition law form a group.

- The group law is constructed geometrically.

The ECDLP problem

Input: Two points $P, Q \in E(\mathbb{F}_q)$ with $Q \in \langle P \rangle$.
Question: Find an integer x such that $xP = Q$.

Elliptic curves in cryptography

A curve is

- non-singular (or smooth) if it does not have a singular point.

Jacobi criterion: a point on E is singular if (x, y) also satisfies the two partial derivatives $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

Elliptic curves in cryptography

A curve is

- non-singular (or smooth) if it does not have a singular point.

  Jacobi criterion: a point on E is singular if (x, y) also satisfies the two partial derivatives $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

- supersingular (also non-singular) if and only if $\#E(\mathbb{F}_p) = p + 1$ (for $p > 3$).

  equivalently: iff $E[p] = \{\infty\}$

  $E[n] = \{P \in E(\overline{\mathbb{F}_p}) \mid nP = \infty\}$ (the n-torsion group)

Elliptic curves in cryptography

A curve is

- non-singular (or smooth) if it does not have a singular point.

  Jacobi criterion: a point on E is singular if (x, y) also satisfies the two partial derivatives $2y + a_1x + a_3 = 0$ and $a_1y = 3x^2 + 2a_2x + a_4$.

- supersingular (also non-singular) if and only if $\#E(\mathbb{F}_p) = p + 1$ (for $p > 3$).

  equivalently: iff $E[p] = \{\infty\}$

  $E[n] = \{P \in E(\overline{\mathbb{F}_p}) \mid nP = \infty\}$ (the n-torsion group)

Supersingular curves and cyclic groups

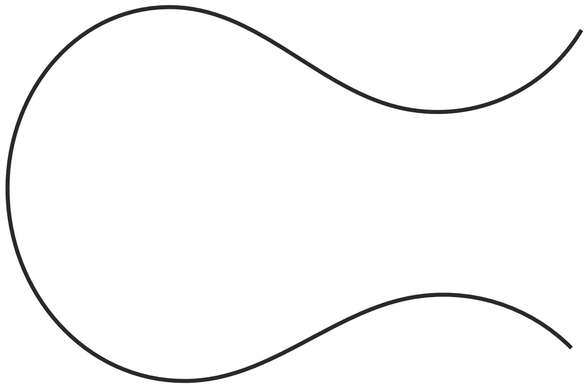
- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

Isogenies



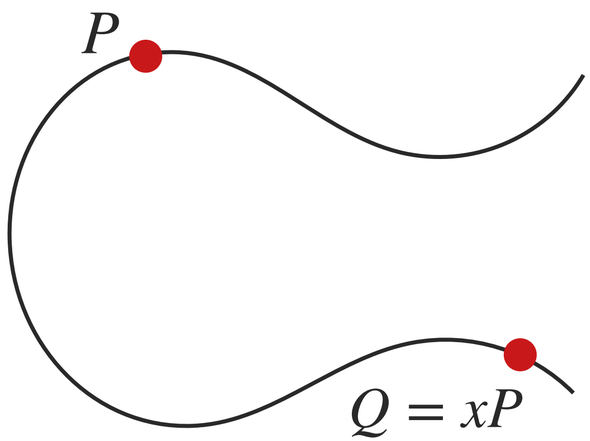
A familiar isogeny

The multiplication-by-d map



A familiar isogeny

The multiplication-by-d map

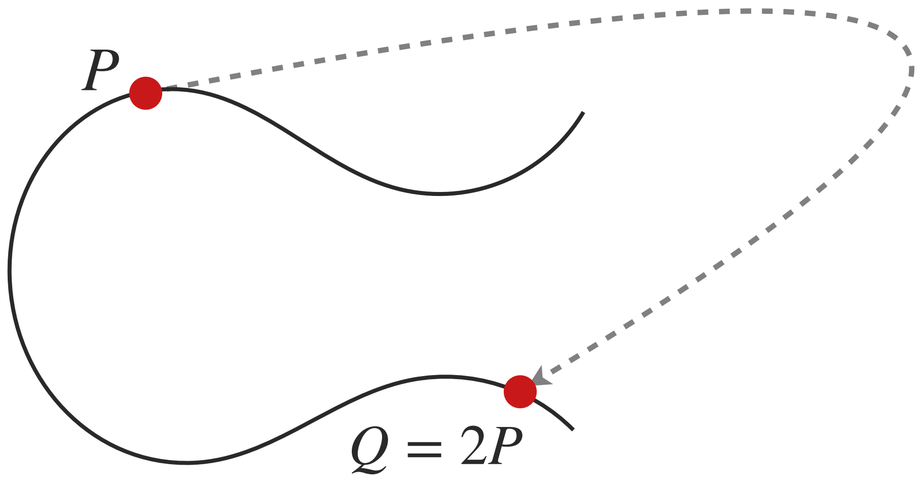


A familiar isogeny

The multiplication-by-d map

$$(x, y) \mapsto (\lambda^2 - 2x, \lambda x + y),$$

$$\lambda = \frac{3x^2 + a}{2y}$$



Isomorphisms

An isomorphism is a map between elliptic curves that is defined everywhere,
i.e., that is given by polynomials in x and y.

Isomorphisms

An isomorphism is a map between elliptic curves that is defined everywhere,
i.e., that is given by polynomials in x and y.

it is a degree-1 isogeny (will make sense on the next slide)
(can be viewed as a change of coordinates)

Isomorphisms

An isomorphism is a map between elliptic curves that is defined everywhere, i.e., that is given by polynomials in x and y.

it is a degree-1 isogeny (will make sense on the next slide)
(can be viewed as a change of coordinates)

j-invariant

- An invariant under isomorphisms.
- For a curve in short Weierstrass form $y^2 = x^3 + c_4 x + c_6$, we have

$$j = 1728 \cdot 4c_4^3/(4c_4^3 + 27c_6^2)$$

Isogenies

An isogeny φ of elliptic curves is a non-zero map $E \to E'$ that is

- given by rational functions
- that is a group homomorphism

Isogenies

An isogeny φ of elliptic curves is a non-zero map $E \to E'$ that is

- given by rational functions
- that is a group homomorphism

$\frac{f(x,y)}{g(x,y)}$, where f, g are polynomials

Isogenies

An isogeny φ of elliptic curves is a non-zero map $E \to E'$ that is

- given by rational functions
- that is a group homomorphism

$$\varphi(P + Q) = \varphi(P) + \varphi(Q)$$

$$\frac{f(x, y)}{g(x, y)}, \text{ where } f, g \text{ are polynomials}$$

Isogenies

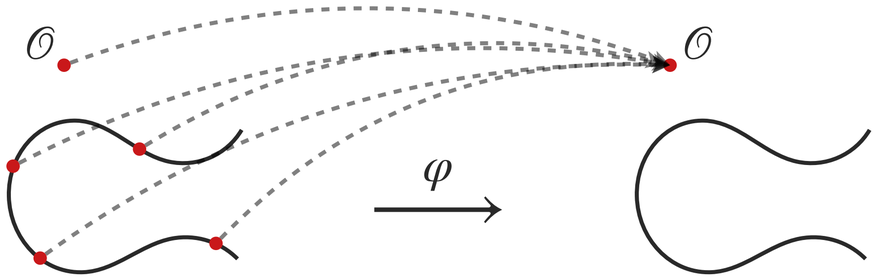
An isogeny φ of elliptic curves is a non-zero map $E \to E'$ that is

- given by rational functions
- that is a group homomorphism

$\varphi(P+Q) = \varphi(P) + \varphi(Q)$

$\frac{f(x,y)}{g(x,y)}$, where f, g are polynomials

→ An isogeny is uniquely defined by its kernel: $\{P \in E \,|\, \varphi(P) = \mathcal{O}_{E'}\}$.



Isogenies

An isogeny φ of elliptic curves is a non-zero map $E \to E'$ that is

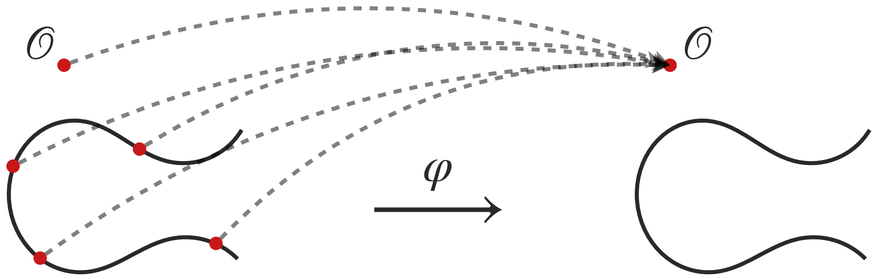
- given by rational functions
- that is a group homomorphism

$\varphi(P+Q) = \varphi(P) + \varphi(Q)$

$\frac{f(x,y)}{g(x,y)}$, where f, g are polynomials

→ An isogeny is uniquely defined by its kernel: $\{P \in E \,|\, \varphi(P) = \mathcal{O}_{E'}\}$.

→ The degree of a (separable) isogeny is the size of its kernel.



Isogenies

Example.

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \to \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2,9), (2, -9), \mathcal{O}\}$.

Isogenies

Example.

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \to \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2,9), (2,-9), \mathcal{O}\}$.

Isogenies

Example.

$$(x, y) \mapsto \left(\frac{x^3 - 4x^2 + 30x - 12}{(x-2)^2}, \frac{x^3 - 6x^2 - 14x + 35}{(x-2)^3} \cdot y\right)$$

defines a degree-3 isogeny of the elliptic curves

$$\{y^2 = x^3 + x\} \to \{y^2 = x^3 - 3x + 3\}$$

over $\mathbb{F}_{71}$. Its kernel is $\{(2,9), (2,-9), \mathcal{O}\}$.

ℓ-isogeny:

- $x \to \frac{f(x)}{g(x)}$, with $\deg(f) = \ell, \deg(g) = \ell - 1$
- $y \to \ldots$

Isogenies

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.
- Its kernel is $E[d] \cong \mathbb{Z}/d \times \mathbb{Z}/d$.

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

Compute an ℓ-isogeny

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

Obtain a kernel of an ℓ-isogeny

↳ Compute an ℓ-isogeny

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

Obtain a subgroup of order ℓ

↳ Obtain a kernel of an ℓ-isogeny

↳ Compute an ℓ-isogeny

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

Take the cyclic group generated by P

↳ Obtain a subgroup of order ℓ

↳ Obtain a kernel of an ℓ-isogeny

↳ Compute an ℓ-isogeny

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

Find a point P on E of order ℓ

↳ Take the cyclic group generated by P

↳ Obtain a subgroup of order ℓ

↳ Obtain a kernel of an ℓ-isogeny

↳ Compute an ℓ-isogeny

Computing isogenies

*We consider only supersingular curves from now on.

→ **Goal**: Compute an ℓ-isogeny from E.

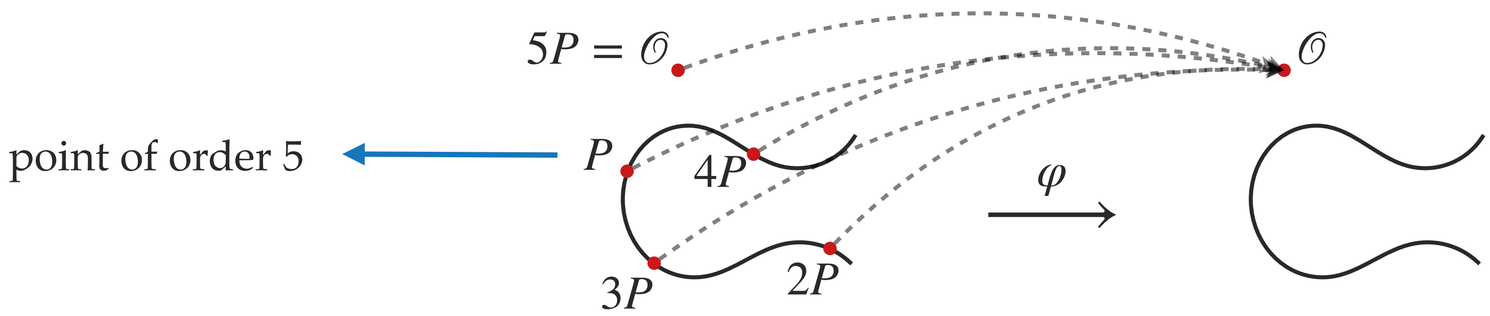
Find a point P on E of order ℓ

↳ Take the cyclic group generated by P

↳ Obtain a subgroup of order ℓ

↳ Obtain a kernel of an ℓ-isogeny

↳ Compute an ℓ-isogeny



Vélu's formulas

- For any finite subgroup G of E, there exists a unique (up to isomorphism) separable isogeny $\varphi_G : E \to E'$ with kernel G.

Vélu's formulas

→ For any finite subgroup G of E, there exists a unique (up to isomorphism) separable isogeny $\varphi_G : E \to E'$ with kernel G.

Vélu '71

- Formulas for computing E' and evaluating φ_G at a point.
- Complexity: $\Theta(\#G)$ → only suitable for small degrees.

Vélu's formulas

→ For any finite subgroup G of E, there exists a unique (up to isomorphism) separable isogeny $\varphi_G : E \to E'$ with kernel G.

Vélu '71

- Formulas for computing E' and evaluating φ_G at a point.
- Complexity: $\Theta(\#G)$ → only suitable for small degrees.

Let P have prime order ℓ on E_A.
For $1 \leq i < \ell$ let x_i be the x-coordinate of iP.
Let

$$\tau = \prod_{i=1}^{\ell-1} x_i, \quad \sigma = \sum_{i=1}^{\ell-1} \left(x_i - \frac{1}{x_i} \right), \quad f(x) = x \prod_{i=1}^{\ell-1} \frac{x x_i - 1}{x - x_i}.$$

Then the ℓ-isogeny with kernel $\langle P \rangle$ is given by

$$\varphi_\ell : E_A \to E_B, (x, y) \mapsto (f(x), c_0 y f'(x))$$

where $B = \tau(A - 3\sigma)$, and $c_0^2 = \tau$.

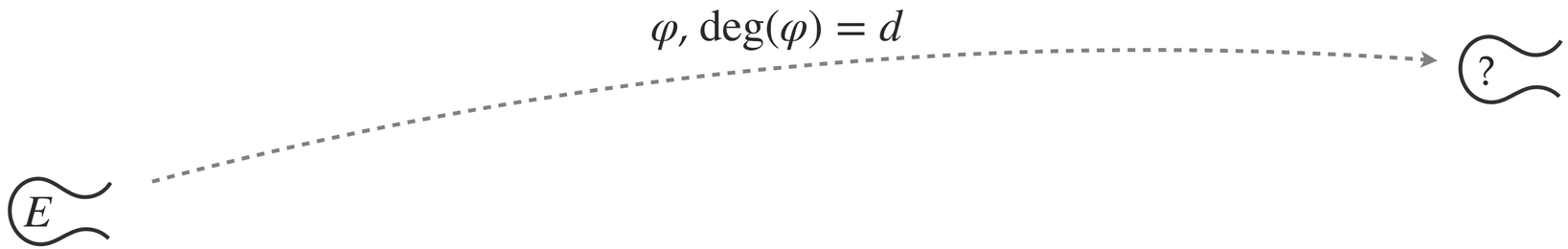
©Lange

Composing isogenies

→ **Goal**: Compute a d-isogeny from E.

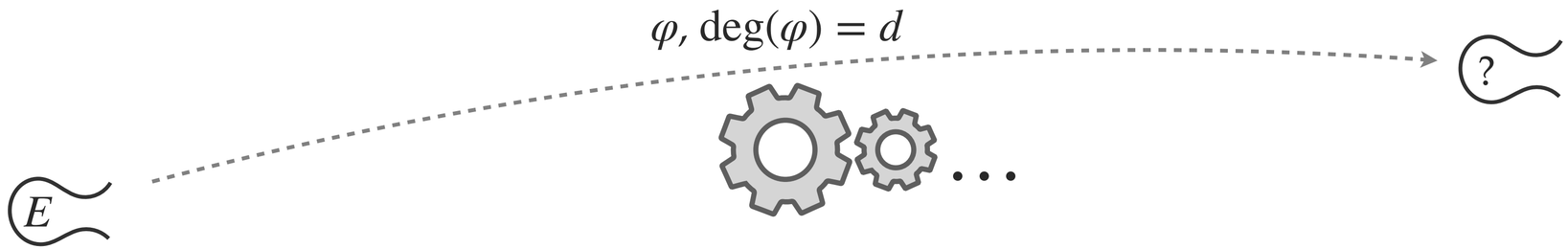
Composing isogenies

Goal: Compute a d-isogeny from E.



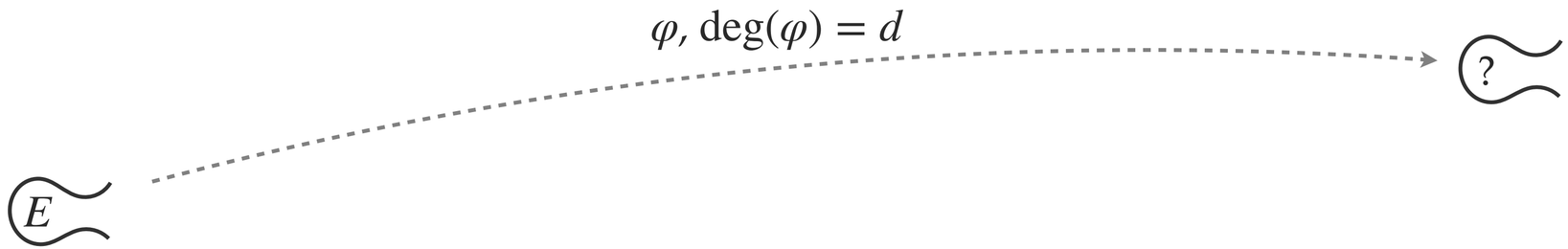
Composing isogenies

Goal: Compute a d-isogeny from E.



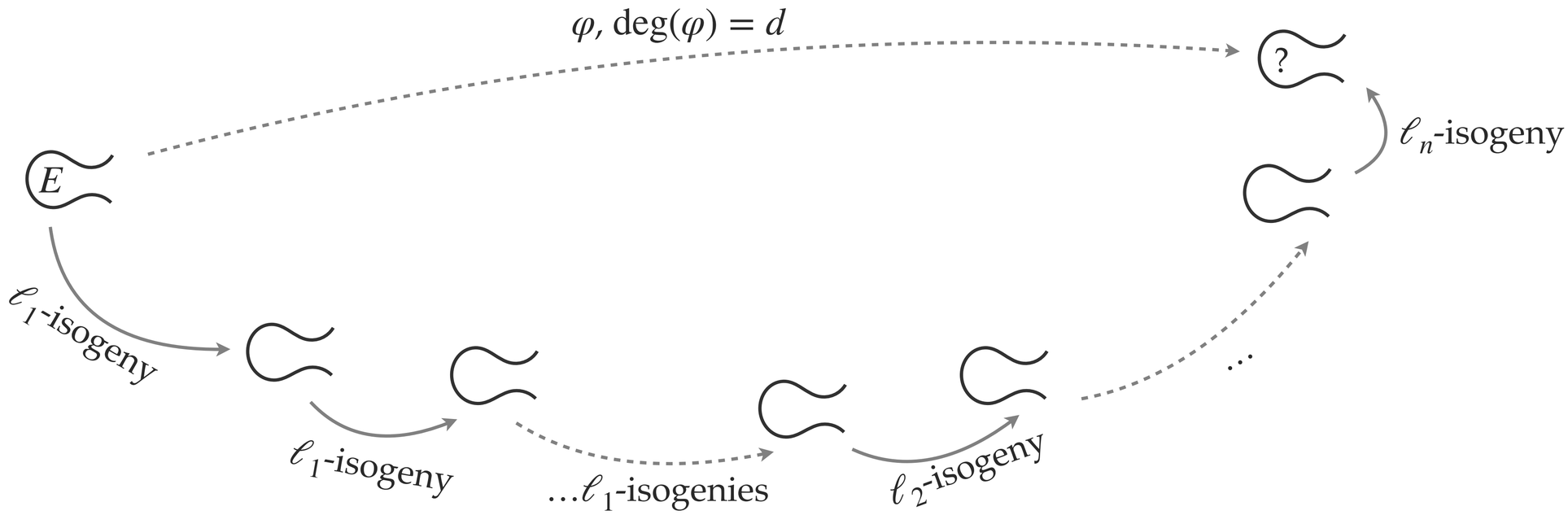
Composing isogenies

Goal: Compute a d-isogeny from E, with d a smooth integer ($d = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdots \ell_n^{e_n}$).



Composing isogenies

Goal: Compute a d-isogeny from E, with d a smooth integer ($d = \ell_1^{e_1} \cdot \ell_2^{e_2} \cdots \ell_n^{e_n}$).



Isogeny graphs

Supersingular curves and cyclic groups (recall)

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

Let ℓ be a prime factor of $p+1$.

There are exactly $(\ell+1)$ $\mathbb{F}_{p^2}$-rational ℓ-isogenies from each E.

There is exactly one $\mathbb{F}_p$-rational ℓ-isogeny from each E.

Isogeny graphs

- Vertices are (isomorphism classes) of supersingular elliptic curves.
- Edges are prime-degree isogenies between them.

Hard problem alert 

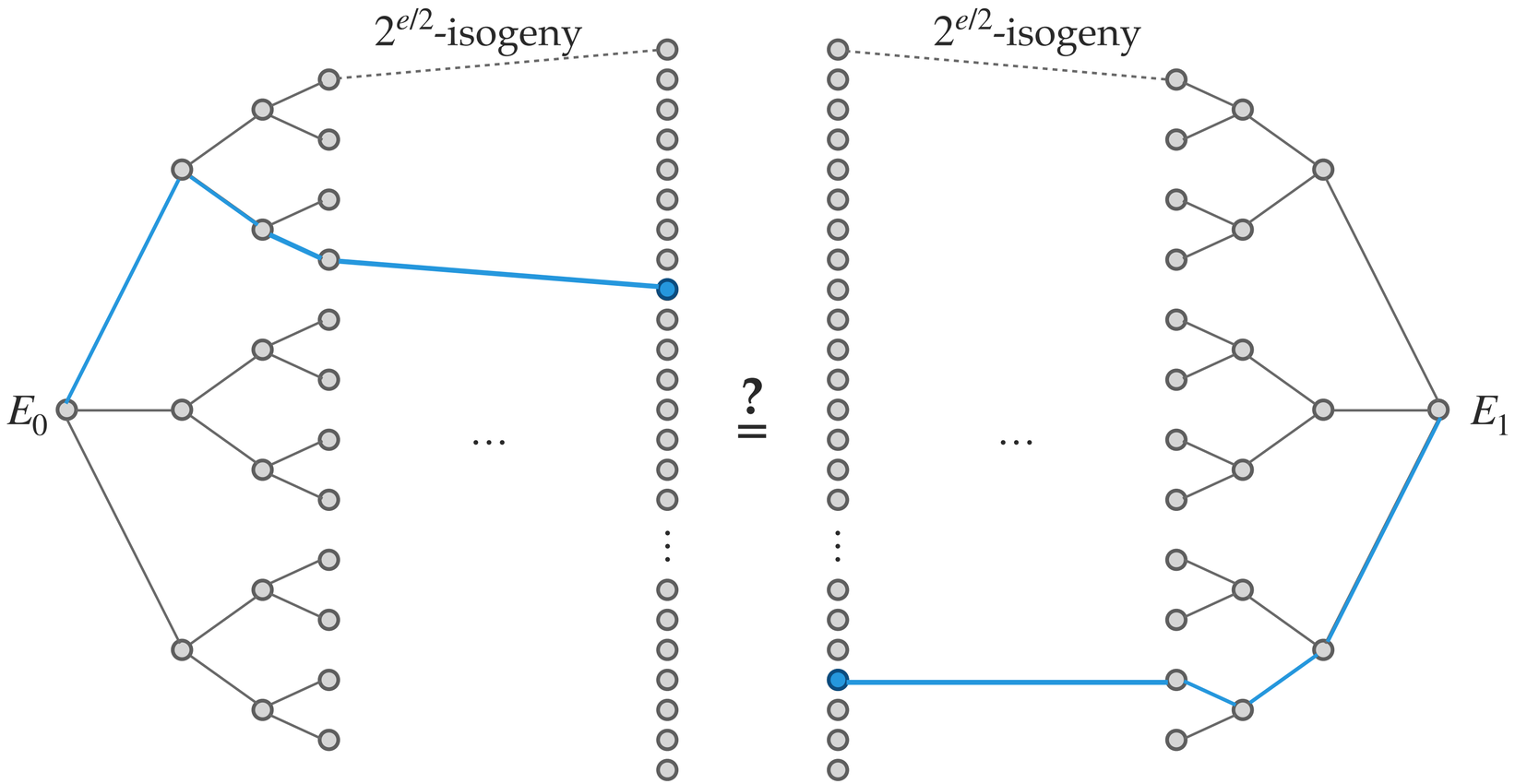
The supersingular isogeny problem

Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.

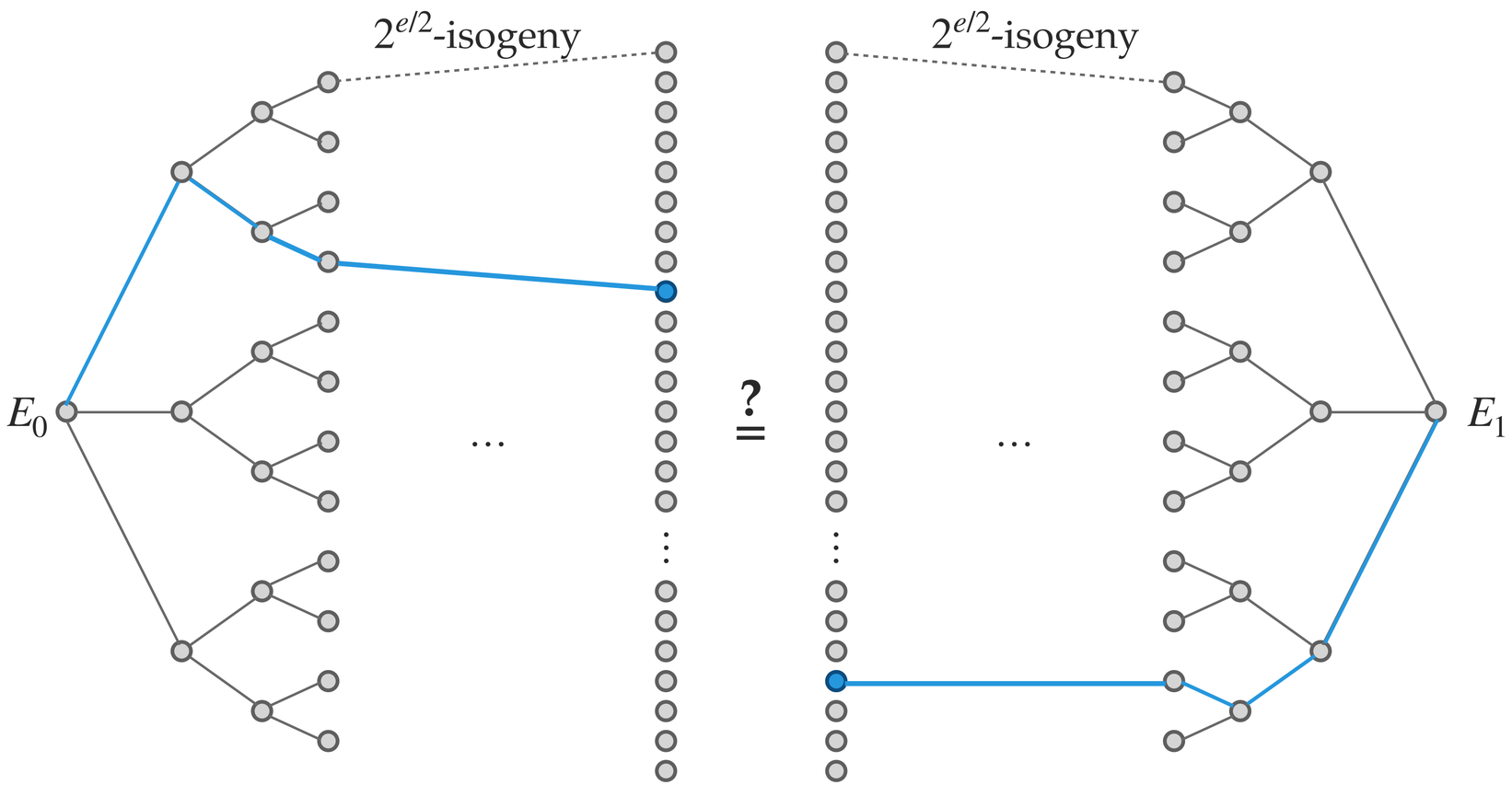
Meet-in-the-middle

Goal: Find a 2^e-isogeny from E_0 to E_1.



Meet-in-the-middle

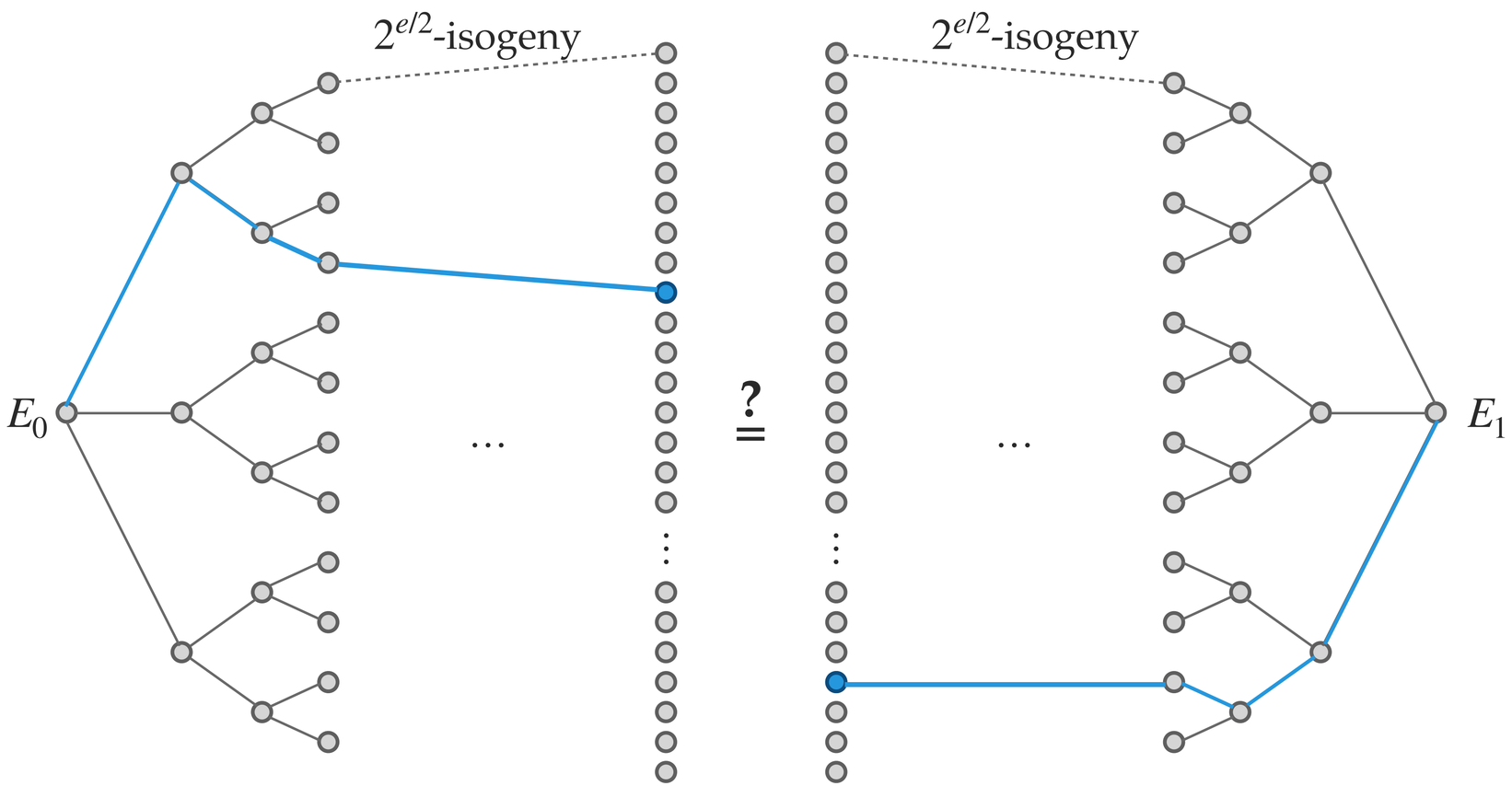
Goal: Find a 2^e-isogeny from E_0 to E_1.



Compute and store all curves on the left.

Meet-in-the-middle

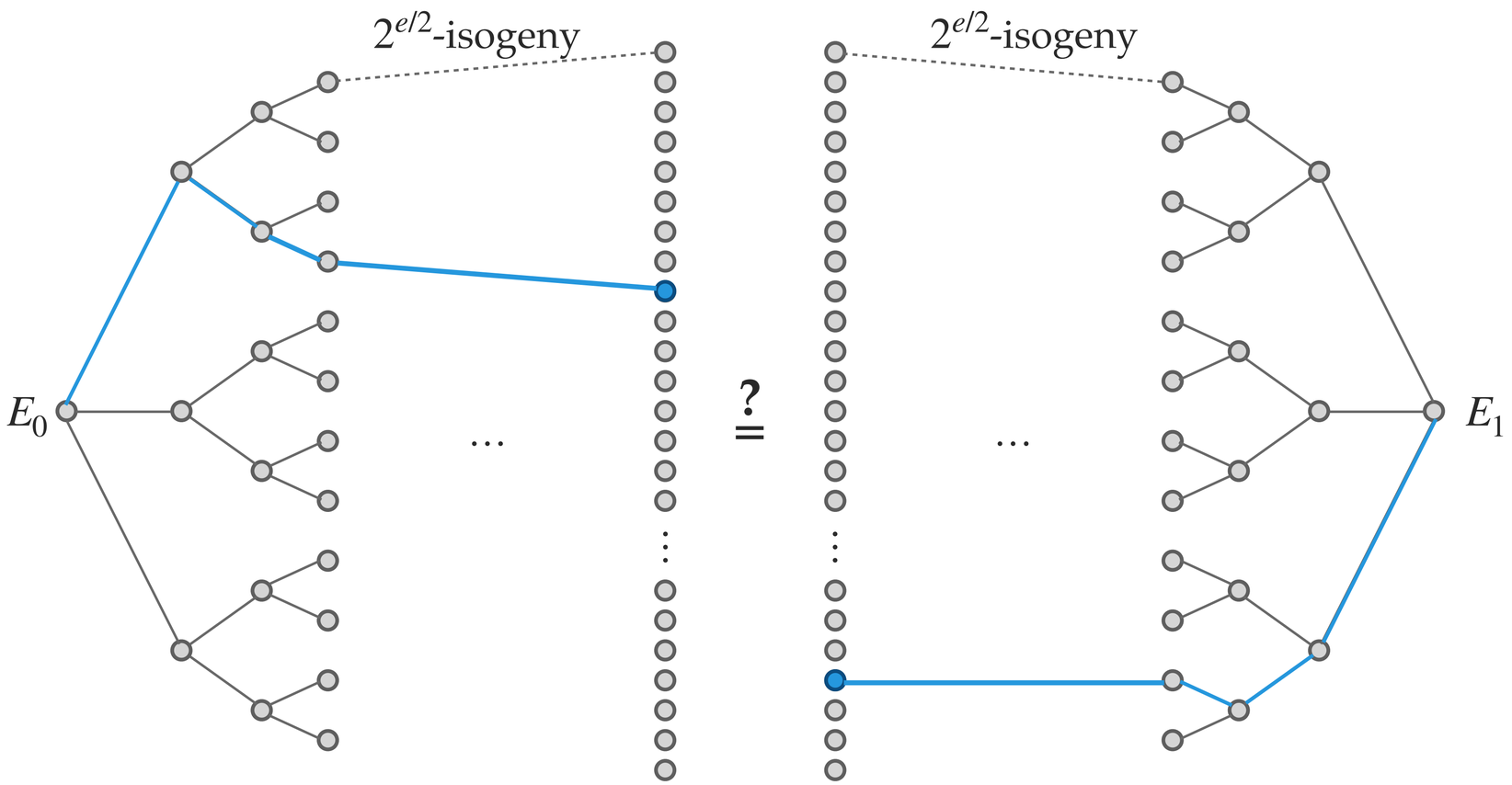
Goal: Find a 2^e-isogeny from E_0 to E_1.



- Compute and store all curves on the left.
- Compute a curve on the right and check for a collision until we find one.

Meet-in-the-middle

Goal: Find a 2^e-isogeny from E_0 to E_1.



- Compute and store all curves on the left.
- Compute a curve on the right and check for a collision until we find one.

$\mathcal{O}(2^{e/2})$

in both time and memory.

*Trade-offs are possible.

$\sqrt{\quad}$ algorithms for the isogeny problem

- The Meet-in-the-middle algorithm
- The van Oorschot and Wiener algorithm
- The Delfs-Galbraith algorithm

The Deuring correspondence



Endomorphism rings

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.

Endomorphism rings

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.

  → It is an endomorphism.

Endomorphism rings

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.
  - It is an endomorphism.
- Its kernel is $E[d] \cong \mathbb{Z}/d \times \mathbb{Z}/d$.

Endomorphism rings

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.
- Its kernel is $E[d] \cong \mathbb{Z}/d \times \mathbb{Z}/d$.

It is an endomorphism.

End(E)

- An endomorphism is an isogeny from a curve E to itself.

Endomorphism rings

Dual isogeny

- For isogeny $\varphi : E \to E'$ there exists a unique dual isogeny $\hat{\varphi} : E' \to E$.
- The composition $\hat{\varphi} \circ \varphi$ is the multiplication-by-d map on E and $\varphi \circ \hat{\varphi}$ the multiplication-by-d map on E', where $d = \deg(\varphi) = \deg(\hat{\varphi})$.

The multiplication-by-d map

- The multiplication-by-d map $[d] : E \to E$ is a degree-d^2 isogeny from E to E.
- Its kernel is $E[d] \cong \mathbb{Z}/d \times \mathbb{Z}/d$.

It is an endomorphism.

$\mathrm{End}(E)$

- An endomorphism is an isogeny from a curve E to itself.
- The set of endomorphisms forms a ring $\mathrm{End}(E)$ under $+$ and $\circ$.

Hard problem alert 

The EndRing problem

Input: A supersingular curve E.

Question: Find a basis of $\mathrm{End}(E)$.

Hard problems and reductions

The supersingular isogeny problem

Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.

The EndRing problem

Input: A supersingular curve E.

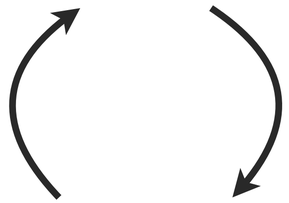
Question: Find a basis of $\mathrm{End}(E)$.

Hard problems and reductions

The supersingular isogeny problem

Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.



The EndRing problem

Input: A supersingular curve E.

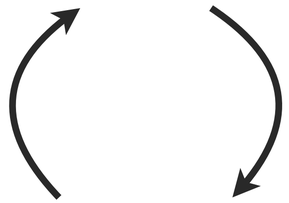
Question: Find a basis of $\mathrm{End}(E)$.

Hard problems and reductions

The supersingular isogeny problem

Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

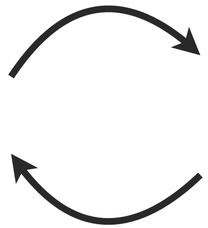
Question: Find an isogeny $\varphi : E \to E'$.



The EndRing problem

Input: A supersingular curve E.

Question: Find a basis of $\mathrm{End}(E)$.



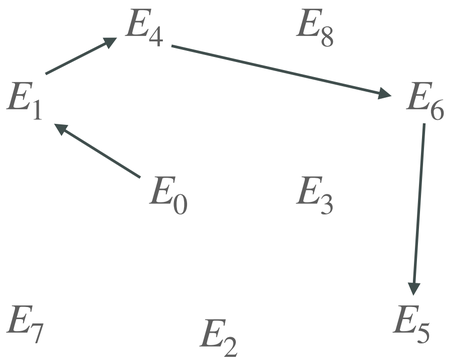
The OneEnd problem

Input: A supersingular curve E.

Question: Find one endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbb{Z}$.

The Deuring correspondence: a summary

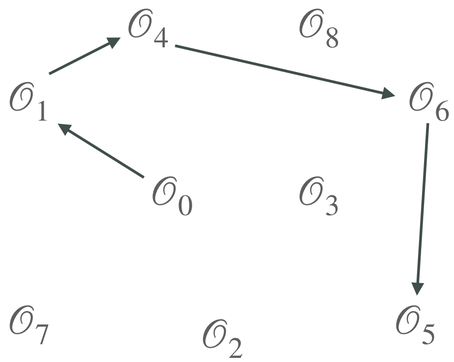
world of supersingular curves



Equivalence
of categories

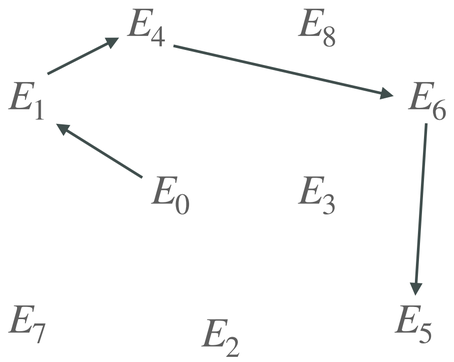
$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

world of maximal orders



The Deuring correspondence: a summary

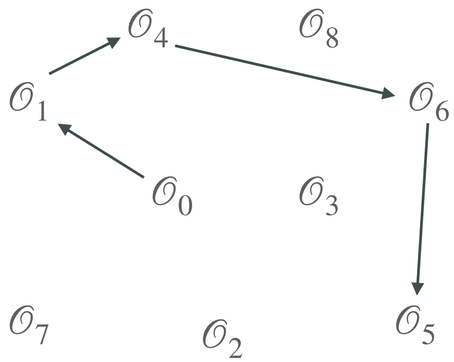
world of supersingular curves



Equivalence of categories

$E \mapsto \mathrm{End}(E) \cong \mathcal{O}$

world of maximal orders



Supersingular j-invariant of elliptic curve over $\mathbb{F}_{p^2}$ $j(E)$ (up to Galois conjugacy)	Maximal Order in $\mathcal{B}_{p,\infty}$ $\mathcal{O} \cong \mathrm{End}(E)$ (up to isomorphism)
(E_1, φ) with $\varphi : E \to E_1$	I_φ integral left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal
$\theta \in \mathrm{End}(E_0)$	Principal ideal $\mathcal{O}\theta$
$\deg(\varphi)$	$\mathrm{norm}(I_\varphi)$
$\hat{\varphi}$	$\overline{I_\varphi}$
$\varphi : E \to E_1, \psi : E \to E_1$	Equivalent ideals $I_\varphi \sim I_\psi$

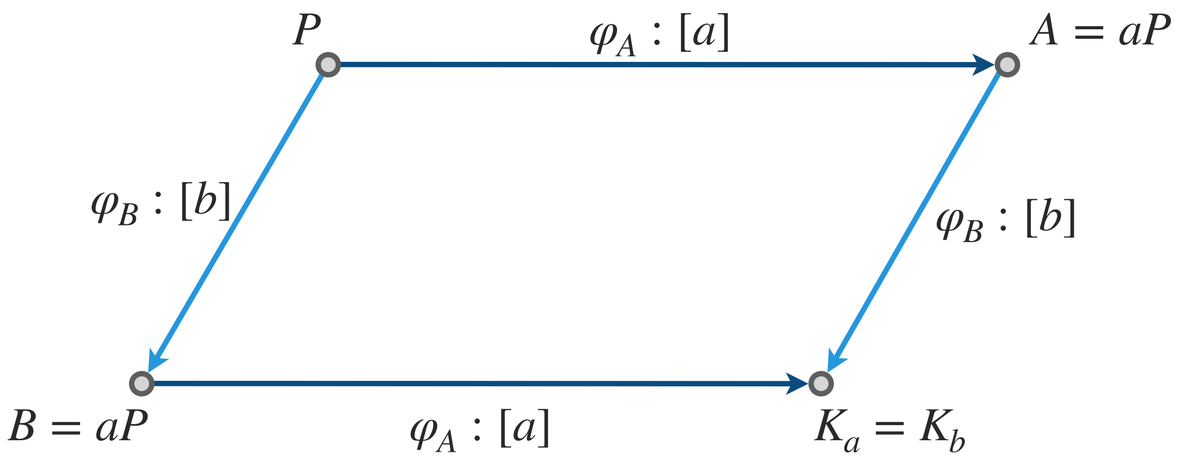
Cryptographic design



DH key exchange on graphs

Imagine *the dlog graph*

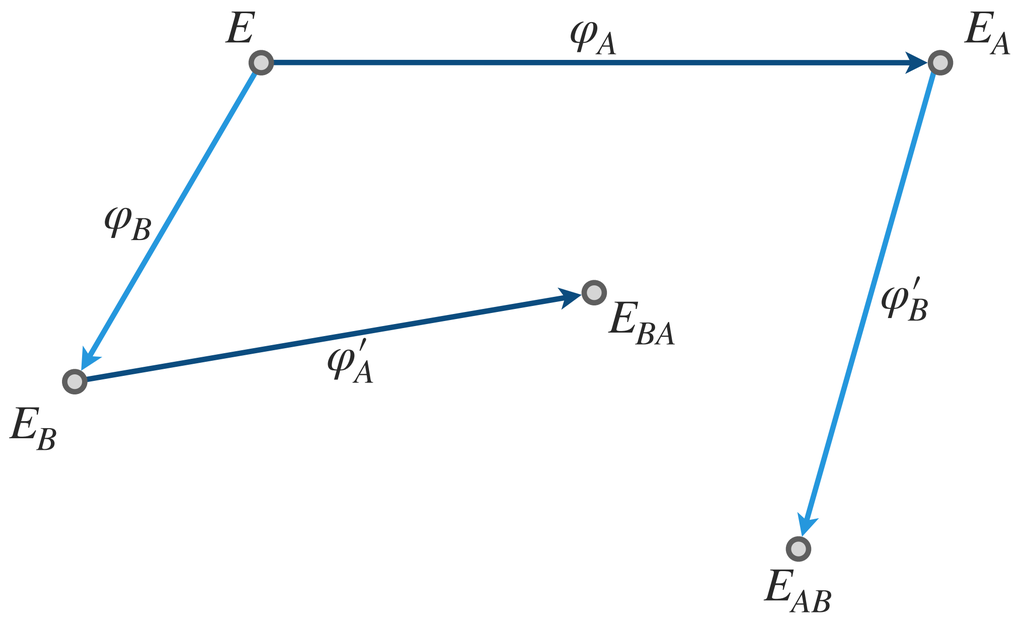
- Vertices are points on E.
- Edges are multiplication-by-i maps.



DH key exchange on isogeny graphs?

Isogeny graphs

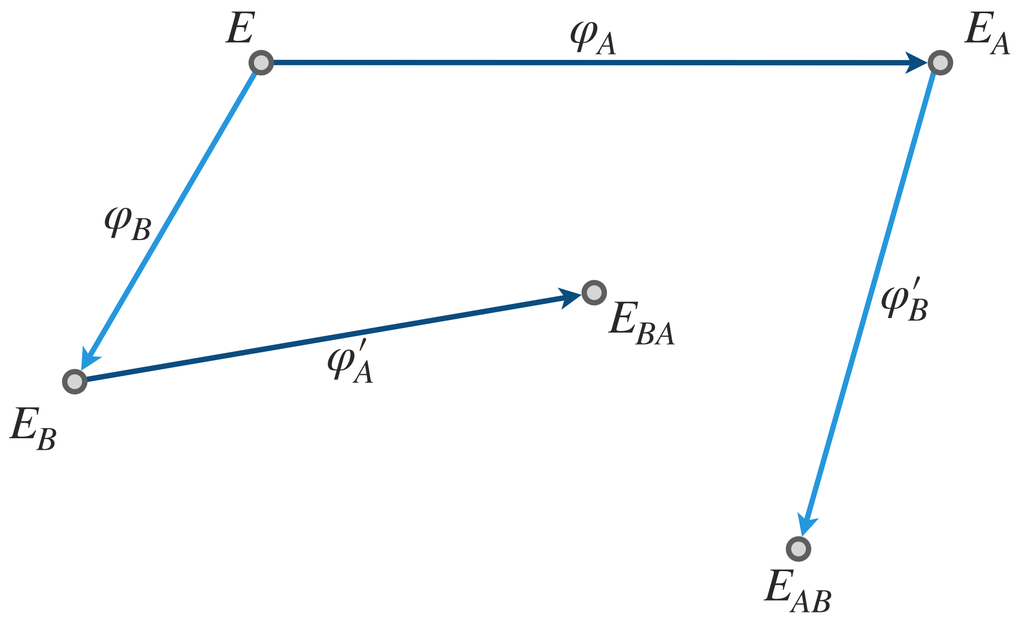
- Vertices are isomorphism classes of supersingular elliptic curves.
- Edges are prime-degree isogenies between them.



DH key exchange on isogeny graphs?

Isogeny graphs

- Vertices are isomorphism classes of supersingular elliptic curves.
- Edges are prime-degree isogenies between them.

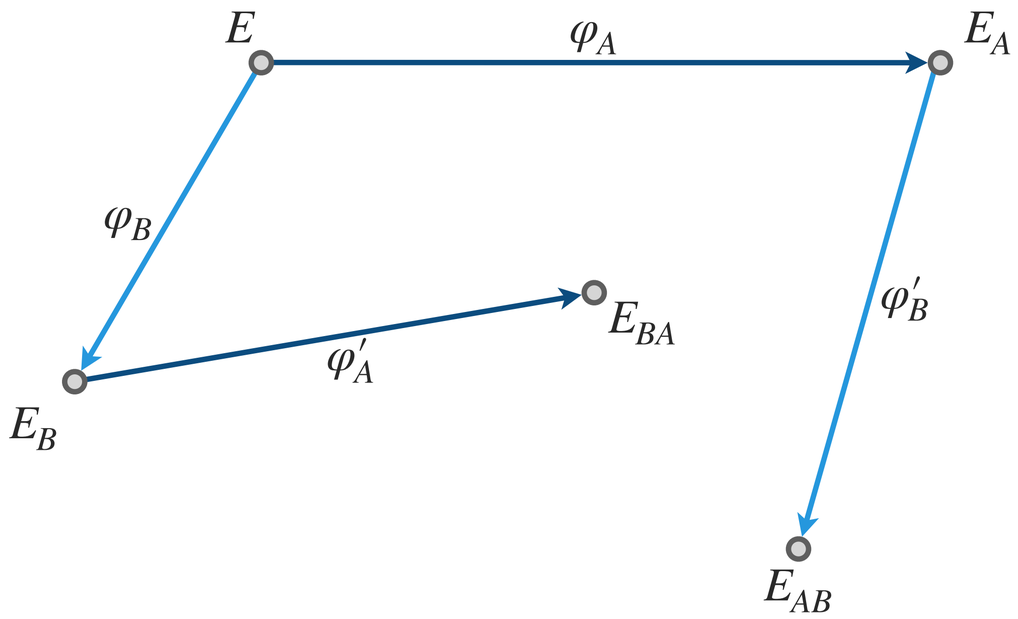


→ Walking on the isogeny graph is not commutative (a priori).

DH key exchange on isogeny graphs?

Isogeny graphs

- Vertices are isomorphism classes of supersingular elliptic curves.
- Edges are prime-degree isogenies between them.



→ Walking on the isogeny graph is not commutative (a priori).

↳ Alice & Bob do not end up on the same vertex (isomorphism class).

Commutative group action

Fundamental theorem of cyclic groups *additive notation.

Every subgroup of a cyclic group $G = \langle P \rangle$ is cyclic.
Moreover, if $\#G = N$, then the order of any subgroup of G is a divisor of N, and,
for each positive divisor k of N, the group G has exactly one subgroup of order k: namely, $\langle [N/k]P \rangle$.

Commutative group action

Fundamental theorem of cyclic groups *additive notation.

Every subgroup of a cyclic group $G = \langle P \rangle$ is cyclic.
Moreover, if $\#G = N$, then the order of any subgroup of G is a divisor of N, and,
for each positive divisor k of N, the group G has exactly one subgroup of order k: namely, $\langle [N/k]P \rangle$.

Supersingular curves and cyclic groups (recall)

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

Commutative group action

Fundamental theorem of cyclic groups *additive notation.

Every subgroup of a cyclic group $G = \langle P \rangle$ is cyclic.
Moreover, if $\#G = N$, then the order of any subgroup of G is a divisor of N, and,
for each positive divisor k of N, the group G has exactly one subgroup of order k: namely, $\langle [N/k]P \rangle$.

Let $p = 4 \cdot \ell_1 \cdots \ell_n - 1$.

Supersingular curves and cyclic groups (recall)

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

Commutative group action

Fundamental theorem of cyclic groups *additive notation.

Every subgroup of a cyclic group $G = \langle P \rangle$ is cyclic.
Moreover, if $\#G = N$, then the order of any subgroup of G is a divisor of N, and,
for each positive divisor k of N, the group G has exactly one subgroup of order k: namely, $\langle [N/k]P \rangle$.

Let $p = 4 \cdot \ell_1 \cdots \ell_n - 1$.

Supersingular curves and cyclic groups (recall)

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

There is exactly one $\mathbb{F}_p$-rational ℓ-isogeny from each E.

Commutative group action

Fundamental theorem of cyclic groups *additive notation.

Every subgroup of a cyclic group $G = \langle P \rangle$ is cyclic.
Moreover, if $\#G = N$, then the order of any subgroup of G is a divisor of N, and,
for each positive divisor k of N, the group G has exactly one subgroup of order k: namely, $\langle [N/k]P \rangle$.

Let $p = 4 \cdot \ell_1 \cdots \ell_n - 1$.

Supersingular curves and cyclic groups (recall)

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

There is exactly one $\mathbb{F}_p$-rational ℓ-isogeny from each E.

There are exactly $(\ell + 1)$ $\mathbb{F}_{p^2}$-rational ℓ-isogenies from each E.

Commutative group action

Fundamental theorem of cyclic groups *additive notation.

Every subgroup of a cyclic group $G = \langle P \rangle$ is cyclic.
Moreover, if $\#G = N$, then the order of any subgroup of G is a divisor of N, and,
for each positive divisor k of N, the group G has exactly one subgroup of order k: namely, $\langle [N/k]P \rangle$.

Let $p = 4 \cdot \ell_1 \cdots \ell_n - 1$.

Supersingular curves and cyclic groups (recall)

- $E(\mathbb{F}_p) \cong \mathbb{Z}/(p+1)$
- $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}/(p+1) \times \mathbb{Z}/(p+1)$

There is exactly one $\mathbb{F}_p$-rational ℓ-isogeny from each E.

There are exactly $(\ell + 1)$ $\mathbb{F}_{p^2}$-rational ℓ-isogenies from each E.

Taking the $E(\mathbb{F}_p)$ isogeny graph will give us a commutative group action.

The algebraic view

on why we have commutativity

→ $\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ is a subring of dimension 2 (a quadratic subring).

The algebraic view

on why we have commutativity

- $\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ is a subring of dimension 2 (a quadratic subring).
- Working in the $E(\mathbb{F}_p)$ isogeny graph corresponds to taking $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$, an order in an imaginary quadratic field.

The algebraic view

on why we have commutativity

- $\mathcal{O} = \mathbb{Z}[\alpha] \subset \mathrm{End}(E)$, for $\alpha \in \mathrm{End}(E) \backslash \mathbb{Z}$ is a subring of dimension 2 (a quadratic subring).
- Working in the $E(\mathbb{F}_p)$ isogeny graph corresponds to taking $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$, an order in an imaginary quadratic field.

Action of the class group

The ideal class group of $\mathcal{O}$
(It is a finite abelian group)

Set of $\mathcal{O}$-oriented
elliptic curves

$$\star : \mathrm{Cl}(\mathcal{O}) \times \mathrm{Ell}_{\mathcal{O}}(p) \to \mathrm{Ell}_{\mathcal{O}}(p)$$

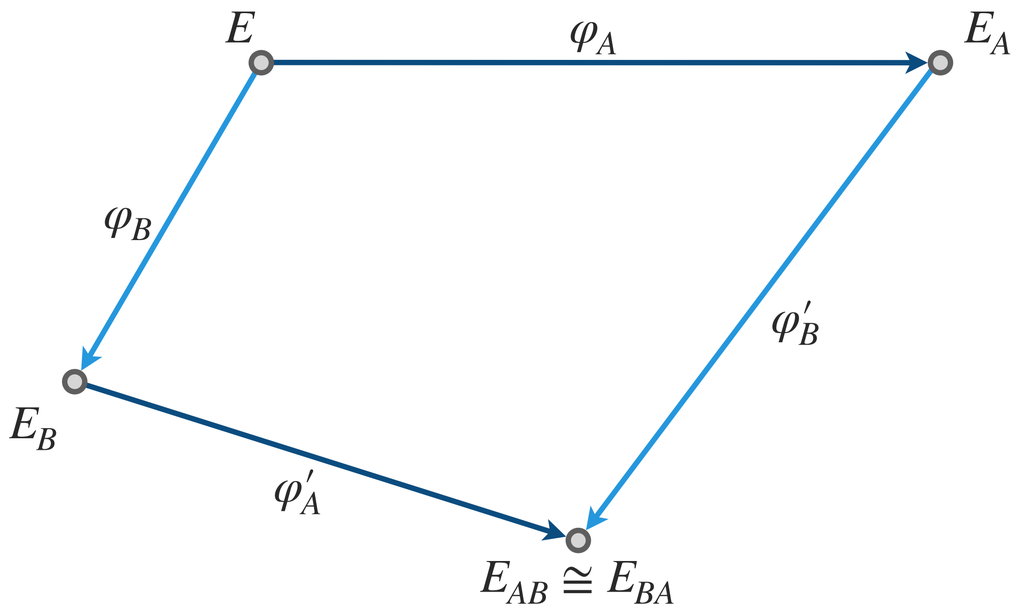
$$(\mathfrak{a}, E) \mapsto \mathfrak{a} \star E$$

- $\mathfrak{b} \star (\mathfrak{a} \star E) = (\mathfrak{b}\mathfrak{a}) \star E$
- $e \star E = E$

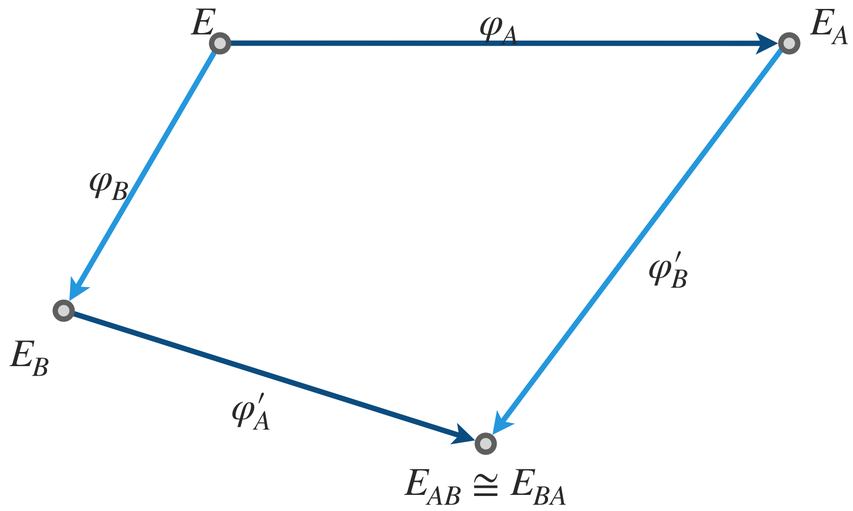
DH key exchange on isogeny graphs

Isogeny graphs $E(\mathbb{F}_p)$ with $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ a prime.

- Vertices are $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves.
- Edges are prime-degree isogenies between them.



CSIDH



- Choose small primes $\ell_1, \ldots, \ell_n$, making sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime → we can compute ℓ_i-steps in the positive or in the negative direction, for all ℓ_i.

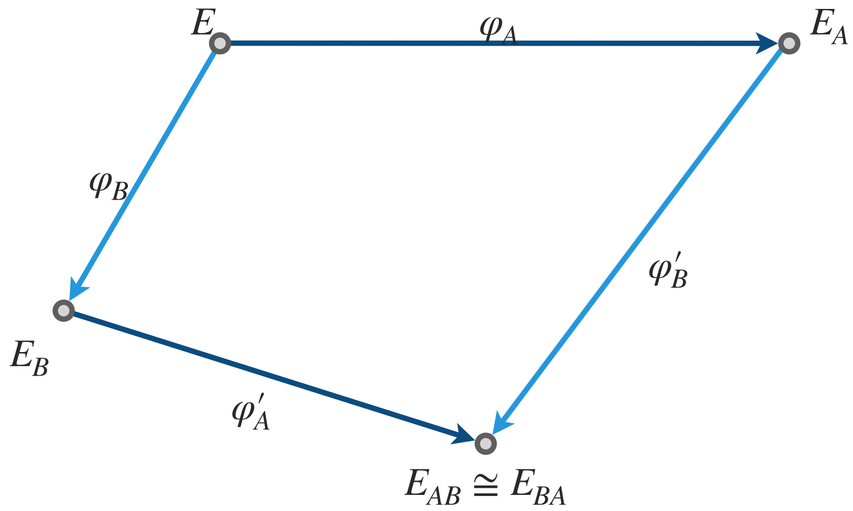
  Example. CSIDH-512: $p = 4 \cdot \prod \ell_i - 1$, for $\ell_i \in \{3,5,\ldots,377,587\}$ (the first 73 primes and 587).

- Vertices are supersingular curves $y^2 = x^3 + Ax^2 + x$ with $A \in \mathbb{F}_p$.

- Alice's (Bob's) path is an isogeny of degree $\prod \ell_i^{e_i}$.

  Example. CSIDH-512: Exponents are $-5 \leq e_i \leq 5$, for all $1 \leq i \leq 74$.

CSIDH



- Choose small primes $\ell_1, \ldots, \ell_n$, making sure $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ is prime → we can compute ℓ_i-steps in the positive or in the negative direction, for all ℓ_i.

  Example. CSIDH-512: $p = 4 \cdot \prod \ell_i - 1$, for $\ell_i \in \{3,5,\ldots,377,587\}$ (the first 73 primes and 587).

- Vertices are supersingular curves $y^2 = x^3 + Ax^2 + x$ with $A \in \mathbb{F}_p$.

- Alice's (Bob's) path is an isogeny of degree $\prod \ell_i^{e_i}$.

  Example. CSIDH-512: Exponents are $-5 \leq e_i \leq 5$, for all $1 \leq i \leq 74$.

↳ Generalizations exist, for other orientations than the Frobenius.

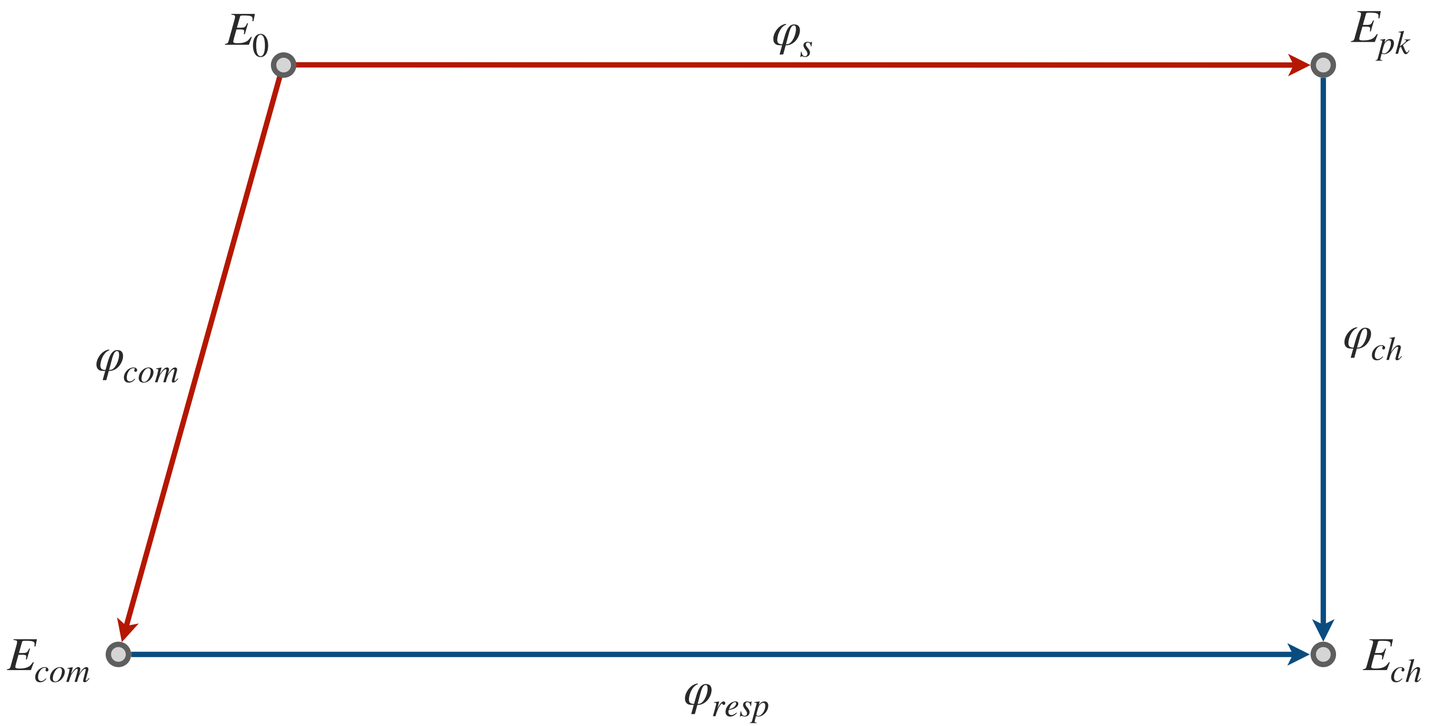
Hard problem alert 

The Vectorisation problem

Input: An imaginary quadratic order $\mathcal{O}$ with $d = |\mathrm{disc}(\mathcal{O})|$ and two $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω').

Question: Find an ideal $\mathfrak{a}$ such that $\mathfrak{a} \star (E, \omega) = (E', \omega')$.

SQIsign



isogeny is secret

isogeny is public

com : commitment

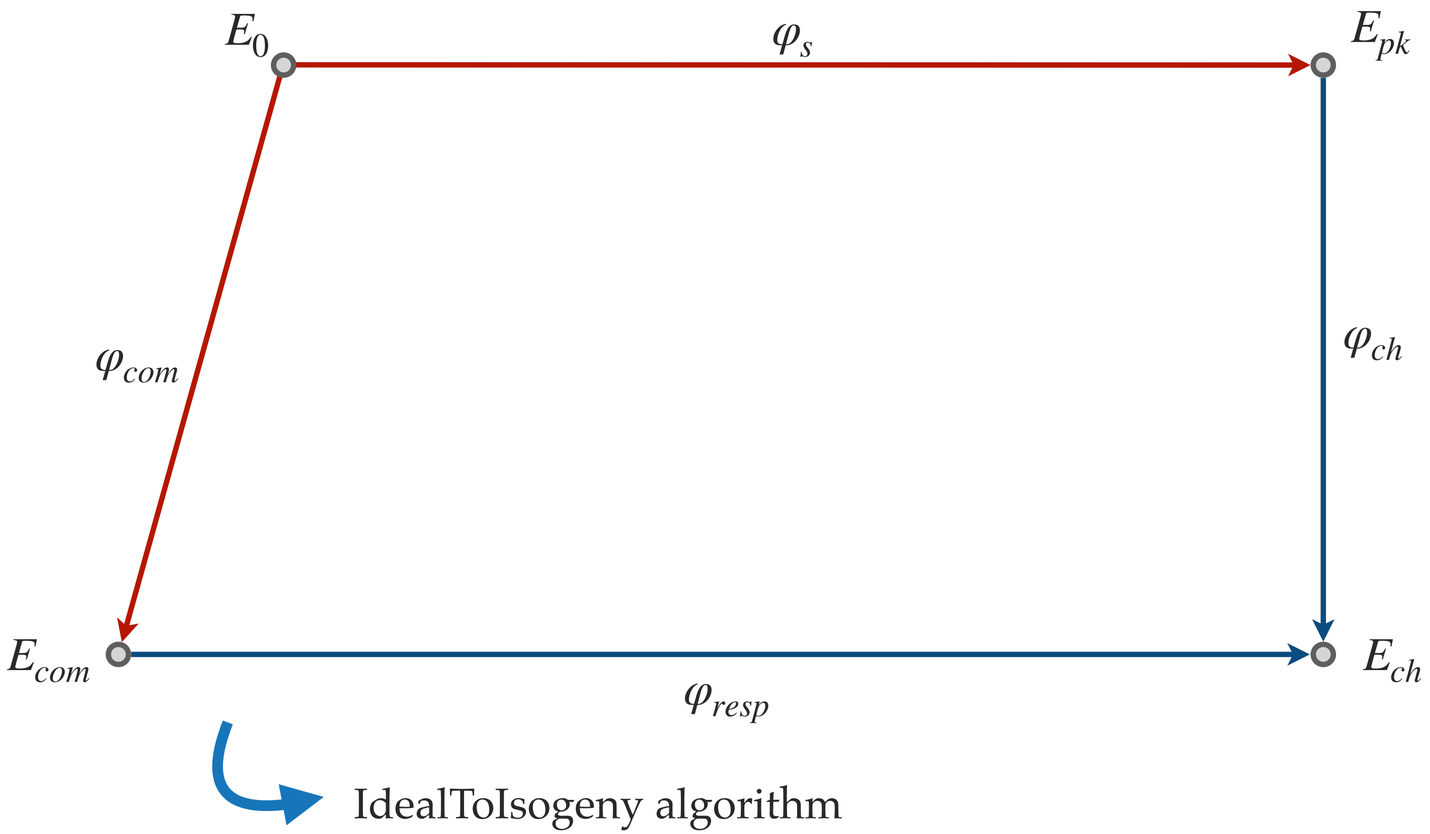
ch : challenge

resp : response

pk : public key

E_0 : denotes the special curve $x^2 = x^3 + x$
with *j*-invariant 1728 of which we know the EndRing.

SQIsign



isogeny is secret

isogeny is public

com : commitment

ch : challenge

resp : response

pk : public key

E_0 : denotes the special curve $x^2 = x^3 + x$
with *j*-invariant 1728 of which we know the EndRing.

Hard problem alert 

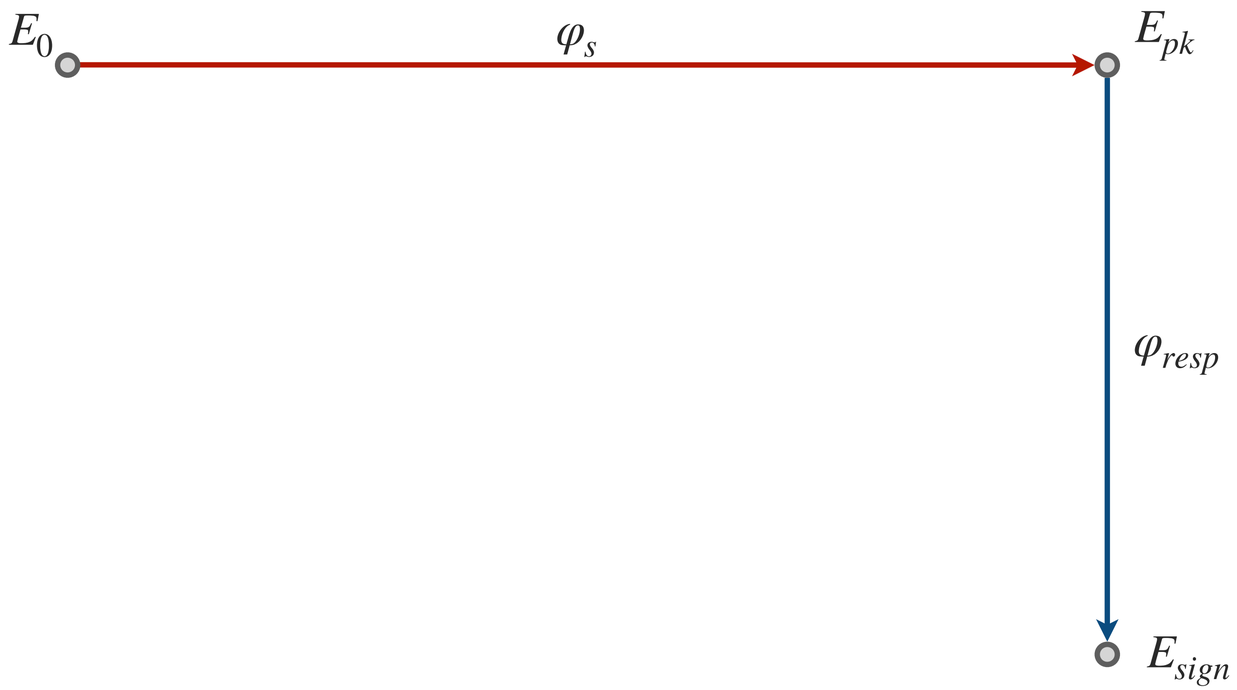
Large-degree isogeny problem

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$ and a positive integer n.

Question: Generate an isogeny $\varphi : E \to E'$ of degree n where E' is some other curve.

 Hard when n is not smooth.

PRISM



isogeny is secret

isogeny is public

pk : public key

ch : challenge

$resp$: response

n : the degree of φ_{resp}

E_0 : denotes the special curve $x^2 = x^3 + x$ with j-invariant 1728 of which we know the EndRing.

Hard problem alert 

Hashing into supersingular curves problem

Input: A prime p and a binary string m.

Question: Give an algorithm $\mathscr{A}$ that uses the input to generate a supersingular curve E defined over $\mathbb{F}_{p^2}$ such that there is no probabilistic polynomial-time algorithm which given the input computes $\mathrm{End}(E)$.

To sum up

To sum up

Because we don't know how to do

The Vectorisation problem

Input: An imaginary quadratic order $\mathcal{O}$ with $d = |\mathrm{disc}(\mathcal{O})|$ and two $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω').

Question: Find ar

Large-degree isogeny problem

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$ and a positive integer n.

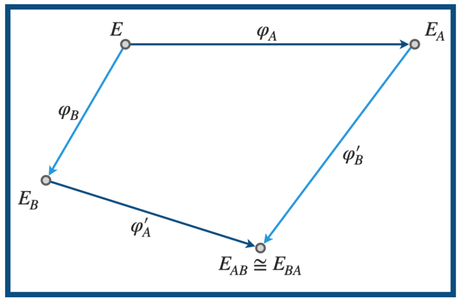
Question: Generate an isogeny $\varphi : E \to E'$ of degree n where E' is some other curve.

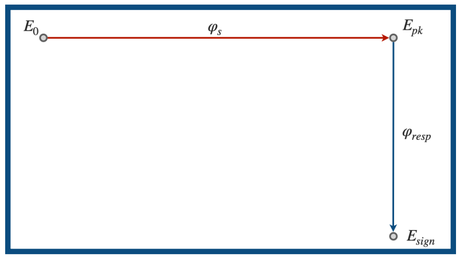
The supersingular isogeny problem

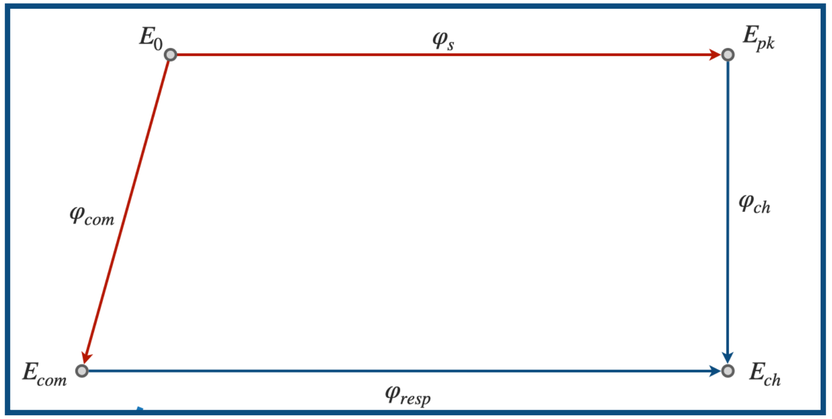
Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.

we are able to do







To sum up

Because we don't know how to do

The Vectorisation problem

Input: An imaginary quadratic order $\mathcal{O}$ with $d = |\mathrm{disc}(\mathcal{O})|$ and two $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω').

Question: Find ar

Large-degree isogeny problem

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$ and a positive integer n.

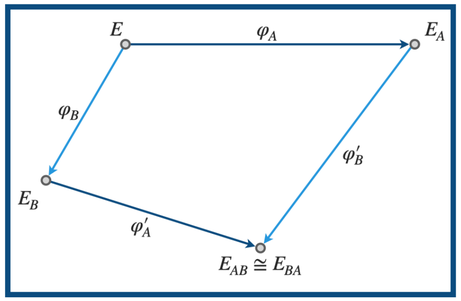
Question: Generate an isogeny $\varphi : E \to E'$ of degree n where E' is some other curve.

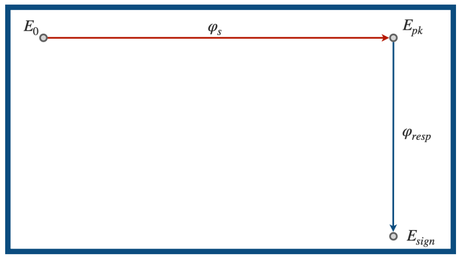
The supersingular isogeny problem

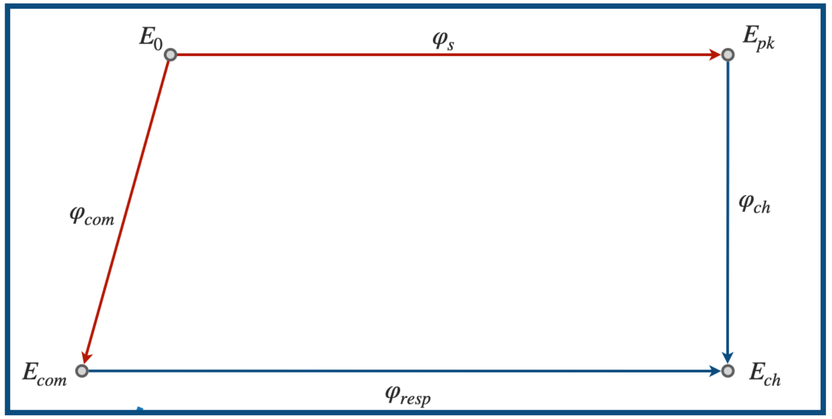
Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.

we are able to do







You can help us:

- Make sure we don't know how to do

To sum up

Because we don't know how to do

The Vectorisation problem

Input: An imaginary quadratic order $\mathcal{O}$ with $d = |\mathrm{disc}(\mathcal{O})|$ and two $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω').

Question: Find ar

Large-degree isogeny problem

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$ and a positive integer n.

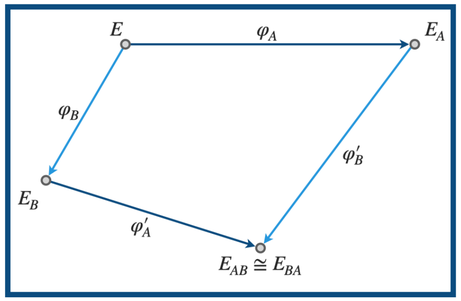
Question: Generate an isogeny $\varphi : E \to E'$ of degree n where E' is some other curve.

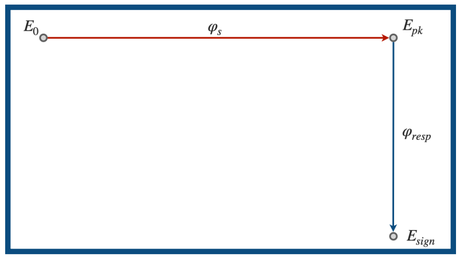
The supersingular isogeny problem

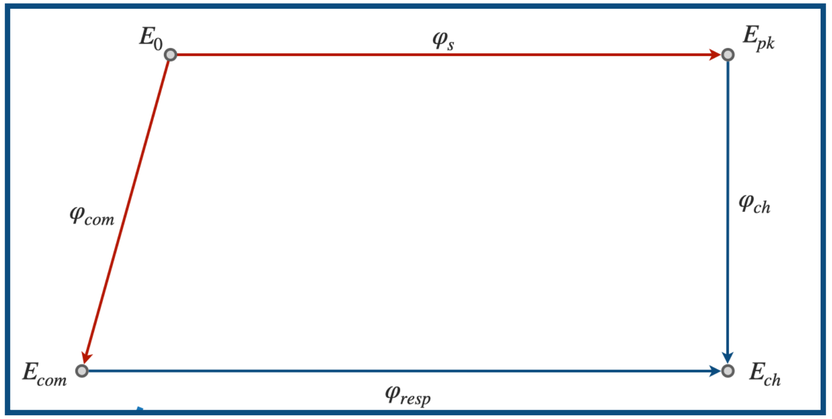
Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.

we are able to do







You can help us:

- Make sure we don't know how to do
- Make some poly-time subroutines more efficient and some representations more compact (design side).

To sum up

Because we don't know how to do

The Vectorisation problem

Input: An imaginary quadratic order $\mathcal{O}$ with $d = |\mathrm{disc}(\mathcal{O})|$ and two $\mathcal{O}$-oriented elliptic curves (E, ω) and (E', ω').

Question: Find ar

Large-degree isogeny problem

Input: A supersingular curve E defined over $\mathbb{F}_{p^2}$ and a positive integer n.

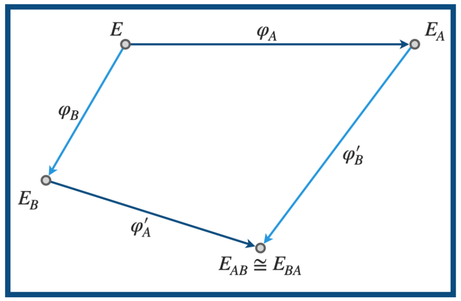
Question: Generate an isogeny $\varphi : E \to E'$ of degree n where E' is some other curve.

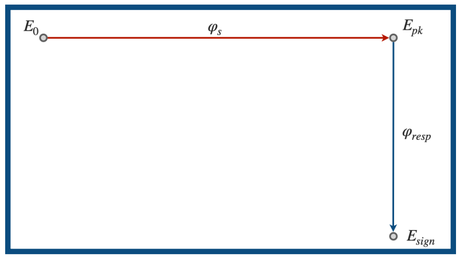
The supersingular isogeny problem

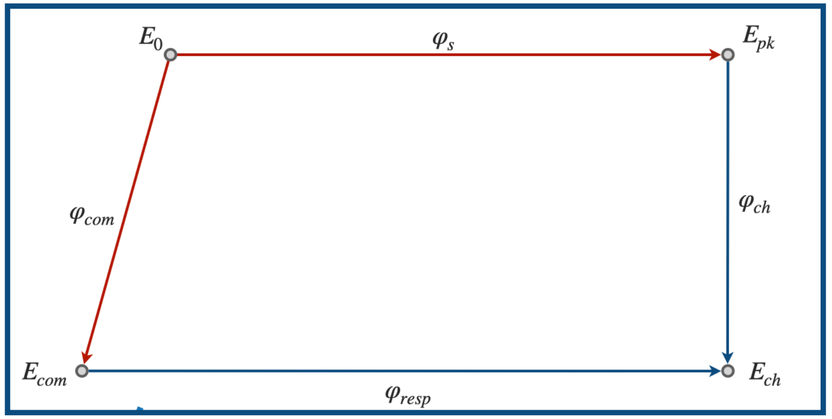
Input: Two supersingular curves E and E' defined over $\mathbb{F}_{p^2}$.

Question: Find an isogeny $\varphi : E \to E'$.

we are able to do







You can help us:

- Make sure we don't know how to do
- Make some poly-time subroutines more efficient and some representations more compact (design side).

Both can be done by exploring the underlying algebraic structure.