A Montgomery ladder for isogenies

Marc Houben

Inria Bordeaux

SQIparty

30 April 2025

CSIDH

Private	Public	Private
	E_0	
Alice		Bob

CSIDH

Private	Public	Private
	E_0	
$[\mathfrak{a}]$		$[\mathfrak{b}]$
Alice		Bob

CSIDH

Private	Public	Private
	E_0	
$[\mathfrak{a}]$		$[\mathfrak{b}]$
Alice	$\xrightarrow{[\mathfrak{a}]E_0}$	Bob
	$\xleftarrow[{[\mathfrak{b}]E_0}]{}$	

CSIDH

Private	Public	Private
	E_0	
$[\mathfrak{a}]$	$[\mathfrak{a}]E_0$	$[\mathfrak{b}]$
Alice	$\longrightarrow$ $\longleftarrow$	Bob
$[\mathfrak{a}][\mathfrak{b}]E_0$	$[\mathfrak{b}]E_0$	$[\mathfrak{b}][\mathfrak{a}]E_0$

Orientations

Orientations

Definition

Let $\mathcal{O} = \mathbb{Z}[\sigma]$ be an imaginary quadratic order. An $\mathcal{O}$-*orientation* is an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$.

Orientations

Definition

Let $\mathcal{O} = \mathbb{Z}[\sigma]$ be an imaginary quadratic order. An *$\mathcal{O}$-orientation* is an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$.

Example

In CSIDH, we have $E/\mathbb{F}_p$ and $\mathcal{O} = \mathbb{Z}[\pi]$, where $\pi = \mathrm{Frob}_p$.

Orientations

Definition

Let $\mathcal{O} = \mathbb{Z}[\sigma]$ be an imaginary quadratic order. An *$\mathcal{O}$-orientation* is an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$.

Example

In CSIDH, we have $E/\mathbb{F}_p$ and $\mathcal{O} = \mathbb{Z}[\pi]$, where $\pi = \mathrm{Frob}_p$.

Ideals $\mathfrak{a} \subseteq \mathcal{O}$ give rise to isogenies $\varphi_{\mathfrak{a}} : E \to \mathfrak{a} \cdot E$ of degree $N(\mathfrak{a})$,

Orientations

Definition

Let $\mathcal{O} = \mathbb{Z}[\sigma]$ be an imaginary quadratic order. An *$\mathcal{O}$-orientation* is an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$.

Example

In CSIDH, we have $E/\mathbb{F}_p$ and $\mathcal{O} = \mathbb{Z}[\pi]$, where $\pi = \mathrm{Frob}_p$.

Ideals $\mathfrak{a} \subseteq \mathcal{O}$ give rise to isogenies $\varphi_{\mathfrak{a}} : E \to \mathfrak{a} \cdot E$ of degree $N(\mathfrak{a})$, s.t.

$$\ker \varphi_{\mathfrak{a}} = E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \iota(\alpha).$$

Orientations

Definition

Let $\mathcal{O} = \mathbb{Z}[\sigma]$ be an imaginary quadratic order. An *$\mathcal{O}$-orientation* is an embedding $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$.

Example

In CSIDH, we have $E/\mathbb{F}_p$ and $\mathcal{O} = \mathbb{Z}[\pi]$, where $\pi = \mathrm{Frob}_p$.

Ideals $\mathfrak{a} \subseteq \mathcal{O}$ give rise to isogenies $\varphi_{\mathfrak{a}} : E \to \mathfrak{a} \cdot E$ of degree $N(\mathfrak{a})$, s.t.

$$\ker \varphi_{\mathfrak{a}} = E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \iota(\alpha).$$

Theorem

If the $\mathcal{O}$-orientation is primitive, this gives a free action

$$\mathrm{Cl}(\mathcal{O}) \circlearrowright \{(E, \iota)\}/\cong .$$

CSIDH

Private	Public	Private
	E_0	
$[\mathfrak{a}]$	$[\mathfrak{a}]E_0$ $\longrightarrow$	$[\mathfrak{b}]$
Alice		Bob
$[\mathfrak{a}][\mathfrak{b}]E_0$	$\longleftarrow$ $[\mathfrak{b}]E_0$	$[\mathfrak{b}][\mathfrak{a}]E_0$

Key exchange from a class group action

Private	Public	Private
	E_0	
$[\mathfrak{a}]$	$[\mathfrak{a}]E_0$	$[\mathfrak{b}]$
Alice	$\xrightarrow{\hspace{3em}}$ $\xleftarrow{\hspace{3em}}$	Bob
$[\mathfrak{a}][\mathfrak{b}]E_0$	$[\mathfrak{b}]E_0$	$[\mathfrak{b}][\mathfrak{a}]E_0$

Key exchange from a class group action

Private	Public	Private
	E_0	
$[\mathfrak{a}]$	$\xrightarrow{[\mathfrak{a}]E_0}$	$[\mathfrak{b}]$
Alice		Bob
$[\mathfrak{a}][\mathfrak{b}]E_0$	$\xleftarrow[{[\mathfrak{b}]E_0}]{}$	$[\mathfrak{b}][\mathfrak{a}]E_0$

(i) CRS

(ii) OSIDH

(iii) SCALLOP & friends

Let $E/\mathbb{F}_p$ be an elliptic curve, $\mathcal{O} = \mathbb{Z}[\pi] \hookrightarrow \mathrm{End}(E)$.

Let $E/\mathbb{F}_p$ be an elliptic curve, $\mathcal{O} = \mathbb{Z}[\pi] \hookrightarrow \mathrm{End}(E)$.

Suppose E is supersingular (i.e. $\overline{\pi} = -\pi$) and $p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

Let $E/\mathbb{F}_p$ be an elliptic curve, $\mathcal{O} = \mathbb{Z}[\pi] \hookrightarrow \mathrm{End}(E)$.

Suppose E is supersingular (i.e. $\overline{\pi} = -\pi$) and $p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

As $\mathcal{O}$-ideals

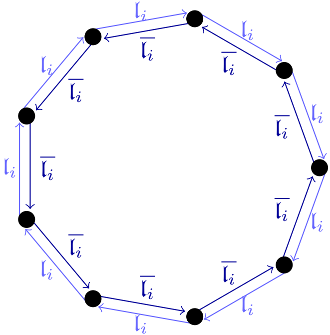
$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i \overline{\mathfrak{l}_i}.$$

Let $E/\mathbb{F}_p$ be an elliptic curve, $\mathcal{O} = \mathbb{Z}[\pi] \hookrightarrow \mathrm{End}(E)$.

Suppose E is supersingular (i.e. $\overline{\pi} = -\pi$) and $p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

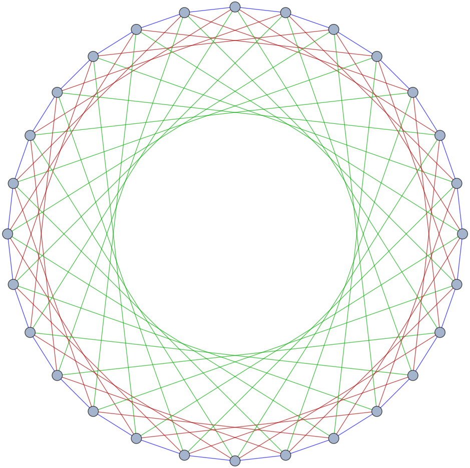
As $\mathcal{O}$-ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i \overline{\mathfrak{l}_i}.$$



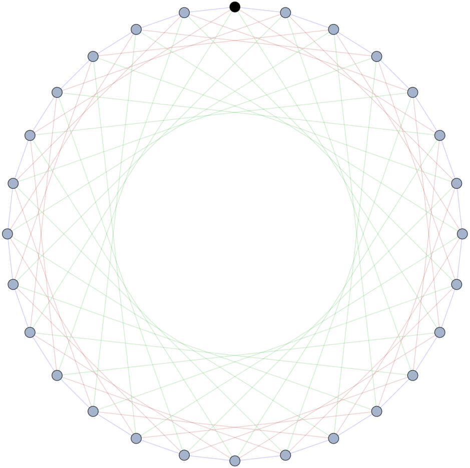
(Connected component of) the supersingular ℓ-isogeny graph over $\mathbb{F}_p$.

CSIDH

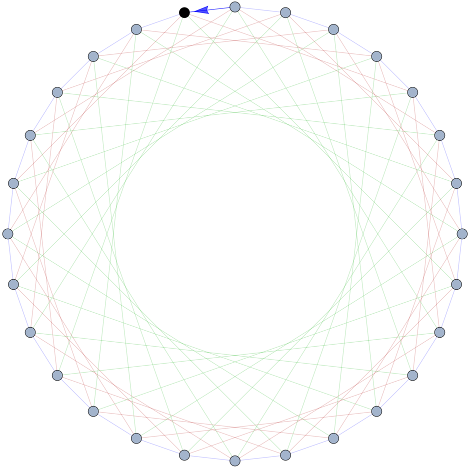


(Connected component of) a union of supersingular 3-, 5-, and 7-isogeny graphs over $\mathbb{F}_p$.

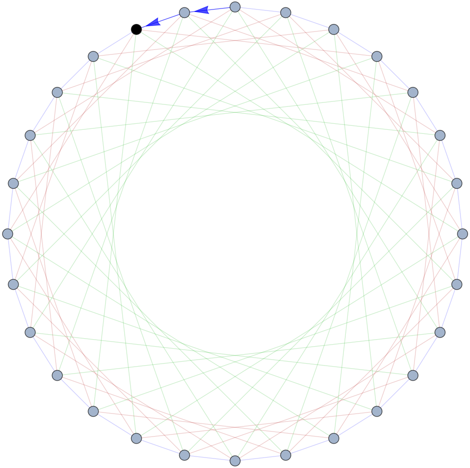
CSIDH



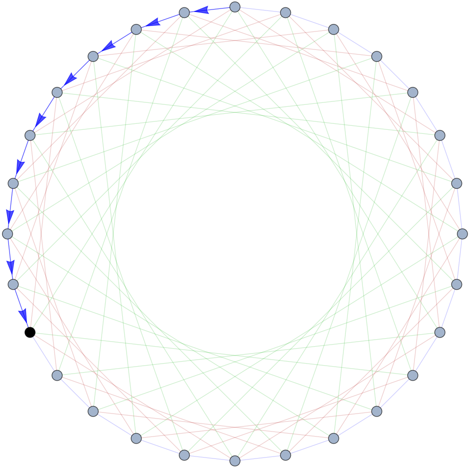
CSIDH



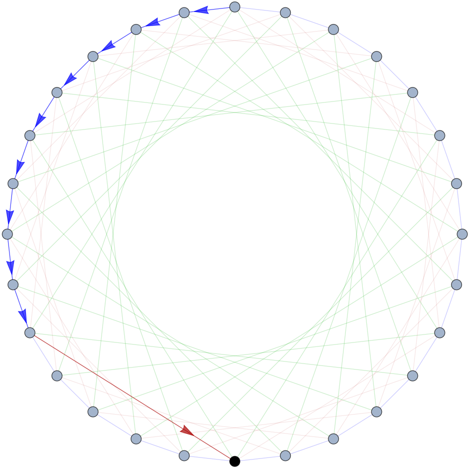
CSIDH



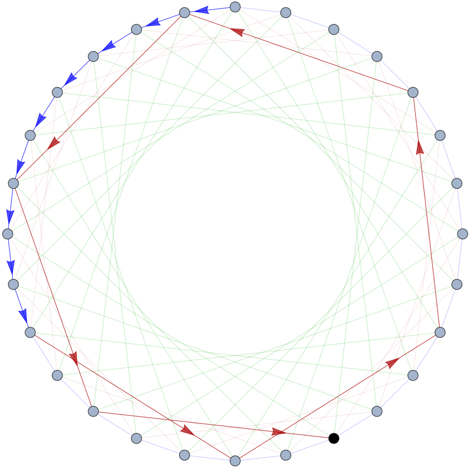
CSIDH



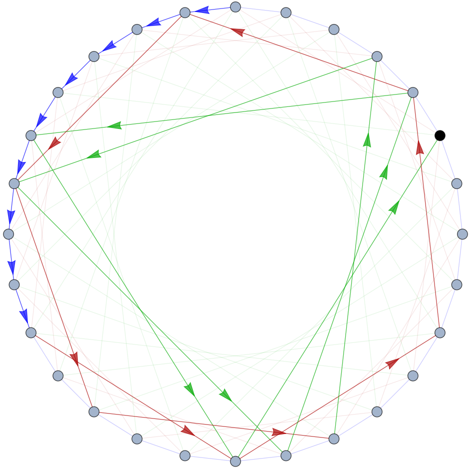
CSIDH



CSIDH



CSIDH



CSIDH-512

$$p = 4 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 373)}_{73 \text{ consecutive primes}} \cdot 587 - 1 \approx 2^{511}.$$

CSIDH-512

$$p = 4 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 373)}_{73 \text{ consecutive primes}} \cdot 587 - 1 \approx 2^{511}.$$

(i) $\mathsf{sk_A} = (a_1, \ldots, a_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_A} = E_A = \prod_i [\mathfrak{l}_i]^{a_i} E_0$.

CSIDH-512

$$p = 4 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 373)}_{\text{73 consecutive primes}} \cdot 587 - 1 \approx 2^{511}.$$

(i) $\mathsf{sk_A} = (a_1, \ldots, a_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_A} = E_A = \prod_i [\mathfrak{l}_i]^{a_i} E_0$.

(ii) $\mathsf{sk_B} = (b_1, \cdots, b_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_B} = E_B = \prod_i [\mathfrak{l}_i]^{b_i} E_0$.

CSIDH-512

$$p = 4 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 373)}_{73 \text{ consecutive primes}} \cdot 587 - 1 \approx 2^{511}.$$

(i) $\mathsf{sk_A} = (a_1, \ldots, a_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_A} = E_A = \prod_i [\mathfrak{l}_i]^{a_i} E_0$.

(ii) $\mathsf{sk_B} = (b_1, \cdots, b_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_B} = E_B = \prod_i [\mathfrak{l}_i]^{b_i} E_0$.

(iii) Alice computes $\prod_i [\mathfrak{l}_i]^{a_i} E_B = \prod_i [\mathfrak{l}_i]^{a_i + b_i} E_0$.

CSIDH-512

$$p = 4 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 373)}_{\text{73 consecutive primes}} \cdot 587 - 1 \approx 2^{511}.$$

(i) $\mathsf{sk_A} = (a_1, \ldots, a_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_A} = E_A = \prod_i [\mathfrak{l}_i]^{a_i} E_0$.

(ii) $\mathsf{sk_B} = (b_1, \cdots, b_{74}) \in \{-5, \ldots, 5\}^{74}$; $\mathsf{pk_B} = E_B = \prod_i [\mathfrak{l}_i]^{b_i} E_0$.

(iii) Alice computes $\prod_i [\mathfrak{l}_i]^{a_i} E_B = \prod_i [\mathfrak{l}_i]^{a_i + b_i} E_0$.

(iv) Bob computes $\prod_i [\mathfrak{l}_i]^{b_i} E_A = \prod_i [\mathfrak{l}_i]^{a_i + b_i} E_0$.

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Algorithm (OG CSIDH)

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.

(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i \overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.
(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.
(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

(i) Non-deterministic. :(

Computing the ℓ_i-isogenies

As $\mathcal{O} = \mathbb{Z}[\pi]$ -ideals

$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i\overline{\mathfrak{l}_i}.$$

$$E[\mathfrak{l}_i] = E[\ell_i, \pi - 1] = E(\mathbb{F}_p)[\ell_i]$$

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.
(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.
(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

(i) Non-deterministic. :(
(ii) Variable time. :((

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.

(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.

(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

Observation

Can compute action of $(a_1, \ldots, a_n) \in \{0, 1\}^n$ from one point $P \in E(\mathbb{F}_p) = E[\pi - 1]$ of order $\prod_{i=1}^{n} \ell_i$.

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.

(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

Observation

Can compute action of $(a_1, \ldots, a_n) \in \{0,1\}^n$ from one point $P \in E(\mathbb{F}_p) = E[\pi - 1]$ of order $\prod_{i=1}^n \ell_i$.

Partial fix

Add $P_0 \in E_0[\pi - 1], Q_0 \in E_0[\pi + 1]$ to public parameters.

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.
(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.
(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

Observation

Can compute action of $(a_1, \ldots, a_n) \in \{0,1\}^n$ from one point $P \in E(\mathbb{F}_p) = E[\pi - 1]$ of order $\prod_{i=1}^n \ell_i$.

Partial fix

Add $P_0 \in E_0[\pi - 1], Q_0 \in E_0[\pi + 1]$ to public parameters.

(i) Restrictive key space.

Algorithm (OG CSIDH)

(i) Sample a random point $R \in E(\mathbb{F}_p)$.

(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]Q$.

(iii) If P has order ℓ_i, compute $\varphi : E \to E/\langle P \rangle \cong [\mathfrak{l}_i]E$.

Observation

Can compute action of $(a_1, \ldots, a_n) \in \{0,1\}^n$ from one point $P \in E(\mathbb{F}_p) = E[\pi - 1]$ of order $\prod_{i=1}^n \ell_i$.

Partial fix

Add $P_0 \in E_0[\pi - 1], Q_0 \in E_0[\pi + 1]$ to public parameters.

(i) Restrictive key space.

(ii) Still need to sample points on E_A and E_B.

Volcanoes

Volcanoes

We have $N(\pi - 1) = p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

Volcanoes

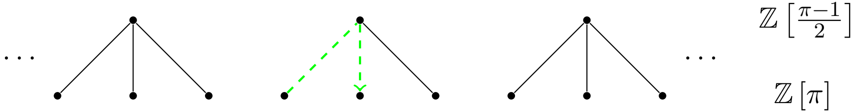
We have $N(\pi - 1) = p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

$$(\pi - 1) = (4, \pi - 1) \cdot \prod_{i=1}^{n} (\ell_i, \pi - 1).$$

Volcanoes

We have $N(\pi - 1) = p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

$$(\pi - 1) = (4, \pi - 1) \cdot \prod_{i=1}^{n} (\ell_i, \pi - 1).$$



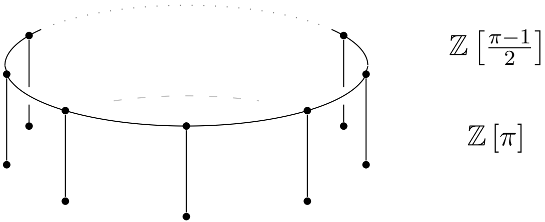
The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 3 \pmod 8$.

Moving to the surface

Assume $p = 8 \cdot \prod_{i=1}^{n} \ell_i - 1$.

Moving to the surface

Assume $p = 8 \cdot \prod_{i=1}^{n} \ell_i - 1$.

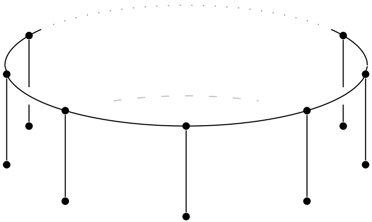


The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 7 \pmod 8$.

Moving to the surface

Assume $p = 8 \cdot \prod_{i=1}^{n} \ell_i - 1$.

$$\left(\frac{\pi - 1}{2}\right) = \left(2, \frac{\pi - 1}{2}\right) \cdot \prod_{i=1}^{n} \left(\ell_i, \frac{\pi - 1}{2}\right)$$



$\mathbb{Z}\left[\frac{\pi-1}{2}\right]$

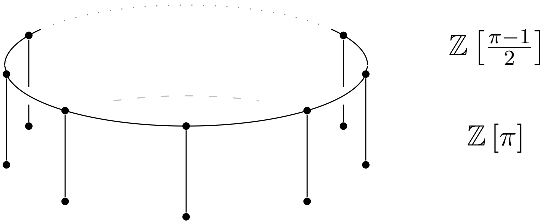
$\mathbb{Z}[\pi]$

The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 7 \pmod 8$.

Moving to the surface

Assume $p = 8 \cdot \prod_{i=1}^{n} \ell_i - 1$.

$$\left(\frac{\pi - 1}{2}\right) = \left(2, \frac{\pi - 1}{2}\right) \cdot \prod_{i=1}^{n} \left(\ell_i, \frac{\pi - 1}{2}\right) = \prod_{i=0}^{n} \left(\ell_i, \frac{\pi - 1}{2}\right)$$

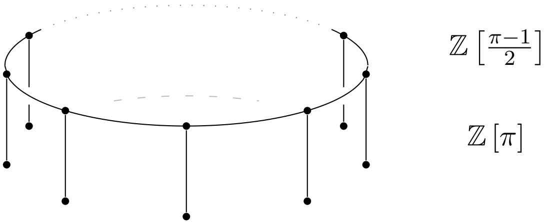


The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 7 \pmod 8$.

Moving to the surface

Assume $p = 8 \cdot \prod_{i=1}^{n} \ell_i - 1$.

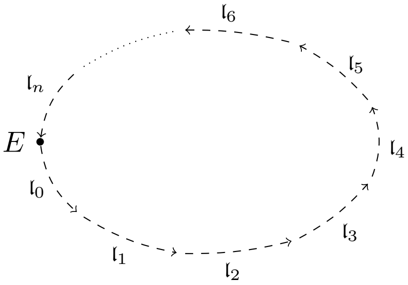
$$\left(\frac{\pi - 1}{2}\right) = \left(2, \frac{\pi - 1}{2}\right) \cdot \prod_{i=1}^{n} \left(\ell_i, \frac{\pi - 1}{2}\right) = \prod_{i=0}^{n} \left(\ell_i, \frac{\pi - 1}{2}\right) = \prod_{i=0}^{n} \mathfrak{l}_i.$$



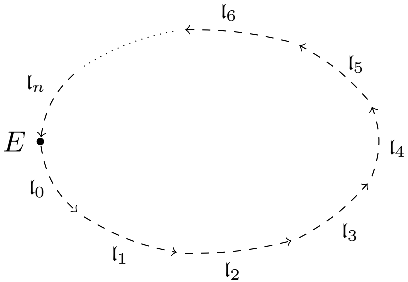
The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 7 \pmod 8$.

Acting by the trivial ideal class

$$\left(\frac{\pi - 1}{2}\right) = \prod_{i=0}^{n} \mathfrak{l}_i.$$

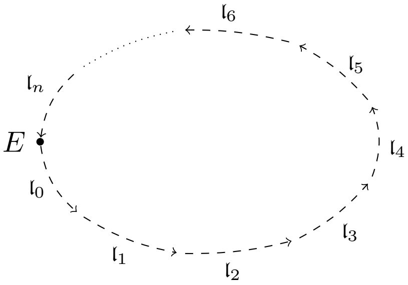


The action by the ideal class $(1, \ldots, 1)$.



Acting by the ideal class $(1, \ldots, 1)$.

$$\varphi^+ : E \to E/\langle P \rangle \cong E, \quad \text{where} \quad E\left[\frac{\pi - 1}{2}\right] = \langle P \rangle.$$

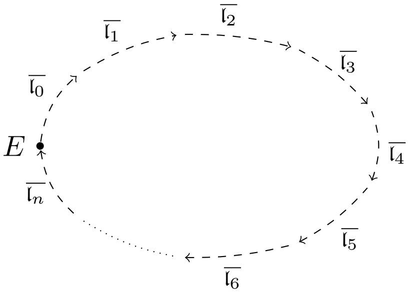


Acting by the ideal class $(1, \ldots, 1)$.

$$\varphi^+ : E \to E/\langle P \rangle \cong E, \quad \text{where} \quad E\left[\frac{\pi - 1}{2}\right] = \langle P \rangle.$$

Similarly

$$\varphi^- : E \to E/\langle Q \rangle \cong E, \quad \text{where} \quad E\left[\frac{\pi + 1}{2}\right] = \langle Q \rangle.$$

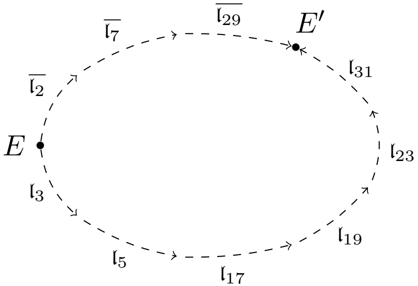


Acting by the ideal class $(1, \ldots, 1)$.

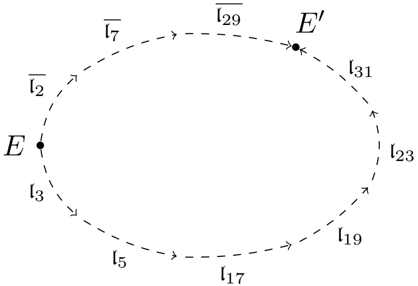
$$\varphi^+ : E \to E/\langle P \rangle \cong E, \quad \text{where} \quad E\left[\frac{\pi - 1}{2}\right] = \langle P \rangle.$$

Similarly

$$\varphi^- : E \to E/\langle Q \rangle \cong E, \quad \text{where} \quad E\left[\frac{\pi + 1}{2}\right] = \langle Q \rangle.$$

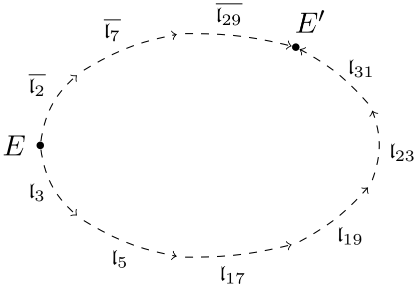


Acting by the ideal class $(0, 1, 1, 0, 1, 1, 1, 0, 1) \equiv (-1, 0, 0, -1, 0, 0, 0, -1, 0)$.



Acting by the ideal class $(0, 1, 1, 0, 1, 1, 1, 0, 1) \equiv (-1, 0, 0, -1, 0, 0, 0, -1, 0)$.

$$\varphi^+ : E \to E/\langle [2 \cdot 7 \cdot 29]P \rangle \cong E', \quad \text{where} \quad E\left[\frac{\pi - 1}{2}\right] = \langle P \rangle,$$

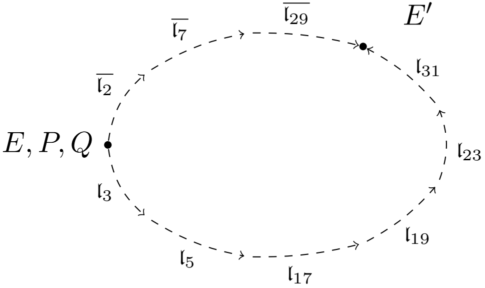


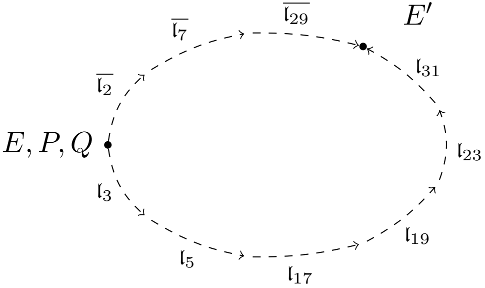
Acting by the ideal class $(0,1,1,0,1,1,1,0,1) \equiv (-1,0,0,-1,0,0,0,-1,0)$.

$$\varphi^+ : E \to E/\langle [2\cdot 7\cdot 29]P\rangle \cong E', \quad \text{where} \quad E\left[\frac{\pi-1}{2}\right] = \langle P\rangle,$$

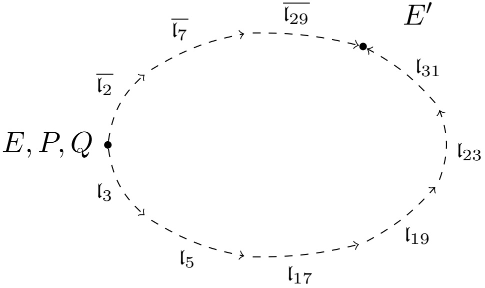
and

$$\varphi^- : E \to E/\langle [3\cdot 5\cdot 17\cdot 19\cdot 23\cdot 31]Q\rangle \cong E', \quad \text{where} \quad E\left[\frac{\pi+1}{2}\right] = \langle Q\rangle.$$


$\overline{\mathfrak{l}_{29}}$
E'
$\overline{\mathfrak{l}_7}$
$\mathfrak{l}_{31}$
$\overline{\mathfrak{l}_2}$
E, P, Q
$\mathfrak{l}_{23}$
$\mathfrak{l}_3$
$\mathfrak{l}_{19}$
$\mathfrak{l}_5$
$\mathfrak{l}_{17}$

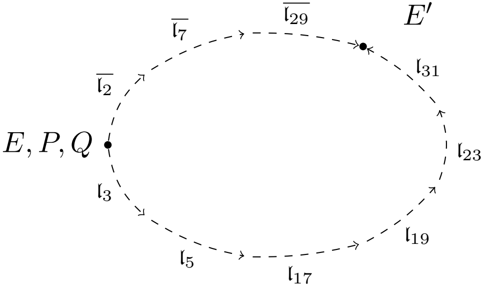

E, P, Q
E'
$\overline{\mathfrak{l}_2}$
$\overline{\mathfrak{l}_7}$
$\overline{\mathfrak{l}_{29}}$
$\mathfrak{l}_{31}$
$\mathfrak{l}_{23}$
$\mathfrak{l}_{19}$
$\mathfrak{l}_{17}$
$\mathfrak{l}_5$
$\mathfrak{l}_3$

Magic™



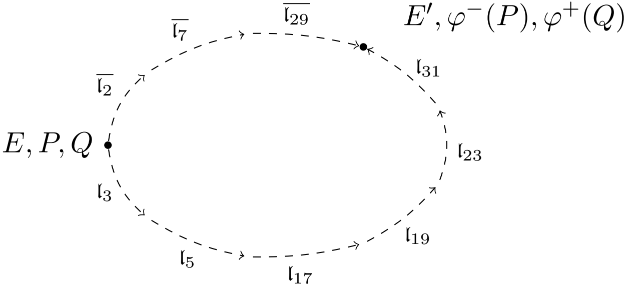
Magic™

$\varphi^-(P)$ generates $E'\left[\frac{\pi-1}{2}\right]$, and $\varphi^+(Q)$ generates $E'\left[\frac{\pi+1}{2}\right]$.



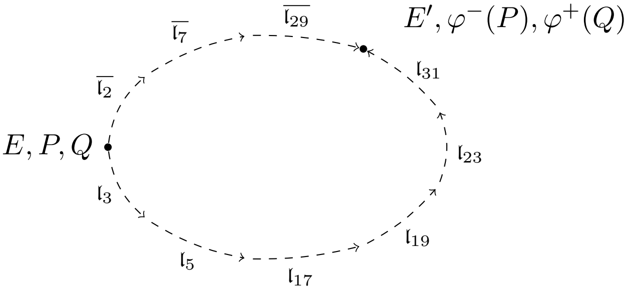
Magic™ (since $\langle P \rangle \cap \langle Q \rangle = \{0\}$)

$\varphi^-(P)$ generates $E'\left[\frac{\pi-1}{2}\right]$, and $\varphi^+(Q)$ generates $E'\left[\frac{\pi+1}{2}\right]$.



Magic™ (since $\langle P \rangle \cap \langle Q \rangle = \{0\}$)

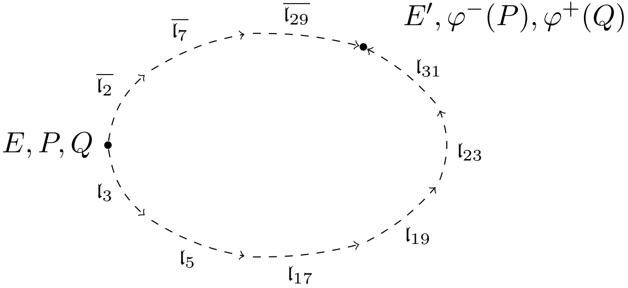
$\varphi^-(P)$ generates $E'\left[\frac{\pi-1}{2}\right]$, and $\varphi^+(Q)$ generates $E'\left[\frac{\pi+1}{2}\right]$.



Magic™ (since $\langle P \rangle \cap \langle Q \rangle = \{0\}$)

$\varphi^-(P)$ generates $E'\left[\frac{\pi-1}{2}\right]$, and $\varphi^+(Q)$ generates $E'\left[\frac{\pi+1}{2}\right]$.

$\Longrightarrow$ iterate to apply the action by any ideal class $(a_1, \ldots, a_n) \in \mathbb{Z}^n$.



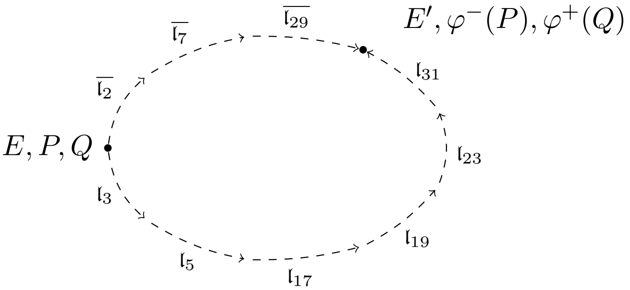
Magic™ (since $\langle P \rangle \cap \langle Q \rangle = \{0\}$)

$\varphi^-(P)$ generates $E'\left[\frac{\pi-1}{2}\right]$, and $\varphi^+(Q)$ generates $E'\left[\frac{\pi+1}{2}\right]$.

$\implies$ iterate to apply the action by any ideal class $(a_1, \ldots, a_n) \in \mathbb{Z}^n$.

Cost

One ℓ_i-isogeny for every i (i.e. one evaluation of $\frac{\pi-1}{2}$).



"Montgomery ladder" for binary ideal classes

$R_0 \leftarrow (E, P, Q), R_1 \leftarrow (E, Q, P)$;
for $i = 0 \ldots n$ **do**
  $\mathsf{cswap}(R_0, R_1, \neg\mathsf{sk}[i])$;
  $R_0 \leftarrow \mathsf{Isogeny}(R_0, \ell_i)$; ▷ Compute ℓ_i-isogeny from $R_0[1]$; push $R_0[1], R_0[2]$.
  $R_1 \leftarrow \mathsf{Multiply}(R_1, \ell_i)$; ▷ Multiply $R_1[1]$ by ℓ_i.
end for;
$R_0[1] \leftarrow R_1[2]$;
return R_0;

In CSURF,

$$\left(\frac{\pi-1}{2}\right)=\prod\left(\ell_i,\frac{\pi-1}{2}\right)=\prod\mathfrak{l}_i.$$

In CSURF,

$$\left(\frac{\pi - 1}{2}\right) = \prod \left(\ell_i, \frac{\pi - 1}{2}\right) = \prod \mathfrak{l}_i.$$

In general: $\mathcal{O} = \mathbb{Z}[\sigma]$

If $N(\sigma) = \prod \ell_i^{e_i}$,

In CSURF,

$$\left(\frac{\pi-1}{2}\right) = \prod \left(\ell_i, \frac{\pi-1}{2}\right) = \prod \mathfrak{l}_i.$$

In general: $\mathcal{O} = \mathbb{Z}[\sigma]$

If $N(\sigma) = \prod \ell_i^{e_i}$, then (assume $\gcd(N(\sigma), \mathrm{Disc}(\mathcal{O})) = 1$)

$$(\sigma) = \prod (\ell_i, \sigma)^{e_i} = \prod \mathfrak{l}_i^{e_i}.$$

In CSURF,

$$\left(\frac{\pi-1}{2}\right)=\prod\left(\ell_i,\frac{\pi-1}{2}\right)=\prod\mathfrak{l}_i.$$

In general: $\mathcal{O}=\mathbb{Z}[\sigma]$

If $N(\sigma)=\prod\ell_i^{e_i}$, then (assume $\gcd(N(\sigma),\mathrm{Disc}(\mathcal{O}))=1$)

$$(\sigma)=\prod(\ell_i,\sigma)^{e_i}=\prod\mathfrak{l}_i^{e_i}.$$

$\implies$ effective class group action over $\mathbb{F}_q$ if $E[\sigma]\subseteq E(\mathbb{F}_q)$.

In CSURF,

$$\left(\frac{\pi - 1}{2}\right) = \prod \left(\ell_i, \frac{\pi - 1}{2}\right) = \prod \mathfrak{l}_i.$$

In general: $\mathcal{O} = \mathbb{Z}[\sigma]$

If $N(\sigma) = \prod \ell_i^{e_i}$, then (assume $\gcd(N(\sigma), \mathrm{Disc}(\mathcal{O})) = 1$)

$$(\sigma) = \prod (\ell_i, \sigma)^{e_i} = \prod \mathfrak{l}_i^{e_i}.$$

$\implies$ effective class group action over $\mathbb{F}_q$ if $E[\sigma] \subseteq E(\mathbb{F}_q)$.

$$4N(\sigma) \lesssim 4q.$$

In CSURF,

$$\left(\frac{\pi-1}{2}\right) = \prod \left(\ell_i, \frac{\pi-1}{2}\right) = \prod \mathfrak{l}_i.$$

In general: $\mathcal{O} = \mathbb{Z}[\sigma]$

If $N(\sigma) = \prod \ell_i^{e_i}$, then (assume $\gcd(N(\sigma), \mathrm{Disc}(\mathcal{O})) = 1$)

$$(\sigma) = \prod (\ell_i, \sigma)^{e_i} = \prod \mathfrak{l}_i^{e_i}.$$

$\implies$ effective class group action over $\mathbb{F}_q$ if $E[\sigma] \subseteq E(\mathbb{F}_q)$.

$$|\,\mathrm{Disc}(\mathcal{O})| = 4N(\sigma) - \mathrm{tr}(\sigma)^2 \leq 4N(\sigma) \lesssim 4q.$$

In CSURF,

$$\left(\frac{\pi-1}{2}\right) = \prod \left(\ell_i, \frac{\pi-1}{2}\right) = \prod \mathfrak{l}_i.$$

In general: $\mathcal{O} = \mathbb{Z}[\sigma]$

If $N(\sigma) = \prod \ell_i^{e_i}$, then (assume $\gcd(N(\sigma), \mathrm{Disc}(\mathcal{O})) = 1$)

$$(\sigma) = \prod (\ell_i, \sigma)^{e_i} = \prod \mathfrak{l}_i^{e_i}.$$

$\implies$ effective class group action over $\mathbb{F}_q$ if $E[\sigma] \subseteq E(\mathbb{F}_q)$.

$$|\mathrm{Disc}(\mathcal{O})| = 4N(\sigma) - \mathrm{tr}(\sigma)^2 \leq 4N(\sigma) \lesssim 4q.$$

Quantum security

Depends on $\#\mathrm{Cl}(\mathcal{O}) \approx 0.46 |\mathrm{Disc}(\mathcal{O})|^{1/2}$.

CSIDH parameter estimates

Recent estimates of p for various NIST levels[1], based on SQALE[2].

Prime bits	f	n	Excluded	Included	Key Space	NIST level
p2048	2^{64}	226	$\{1361\}$	–	2^{221}	1 (aggressive)
p4096	2^{1728}	262	$\{347\}$	$\{1699\}$	2^{256}	1 (conservative)
p5120	2^{2944}	244	$\{227\}$	$\{1601\}$	2^{234}	2 (aggressive)
p6144	2^{3776}	262	$\{283\}$	$\{1693, 1697, 1741\}$	2^{256}	2 (conservative)
p8192	2^{4992}	338	$\{401\}$	$\{2287, 2377\}$	2^{332}	3 (aggressive)
p9216	2^{5440}	389	$\{179\}$	$\{2689, 2719\}$	2^{384}	3 (conservative)

[1] Campos, F., Chávez-Saab, J., Chi-Domínguez, J.J., Meyer, M., Reijnders, K., Rodríguez-Henríquez, F., Schwabe, P., Wiggers, T.: Optimizations and practicality of high-security CSIDH. CiC (2024).

[2] Chávez-Saab, J., Chi-Domínguez, J.J., Jaques, S., Rodríguez-Henríquez, F.: The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. Journal of Cryptographic Engineering (2022).

Larger orientations

$$p + 1 = 4\prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$

Larger orientations

$$p+1 = 4\prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$

$$\begin{tikzcd}
\bullet \arrow[d, dashed, "\varphi_4"'] & \bullet \arrow[l, dashed, "\varphi_3"'] \\
E_1 \arrow[r, dashed, "\varphi_1"'] & \bullet \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

Larger orientations

$$p + 1 = 4 \prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$

$$\begin{tikzcd}
\bullet \arrow[d, dashed, "\varphi_4"'] & \bullet \arrow[l, dashed, "\varphi_3"'] \\
E_1 \arrow[r, dashed, "\varphi_1"'] & \bullet \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

$\ker \varphi_1 = E_1 \left[\prod \mathfrak{l}_i\right] \subseteq \mathbb{F}_{p^2}.$

Larger orientations

$$p + 1 = 4 \prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$

$$\begin{tikzcd}
\bullet \arrow[d, dashed, "\varphi_4"'] & \bullet \arrow[l, dashed, "\varphi_3"'] \\
E_1, P_1 \arrow[r, dashed, "\varphi_1"'] & \bullet \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

$$\ker \varphi_1 = \langle P_1 \rangle \leftrightarrow \prod \mathfrak{l}_i = (1, \ldots, 1),$$

Larger orientations

$$p + 1 = 4 \prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$

$$\begin{tikzcd}
\bullet \arrow[d, dashed, "\varphi_4"'] & \bullet \arrow[l, dashed, "\varphi_3"'] \\
E_1, P_1, Q_1 \arrow[r, dashed, "\varphi_1"'] & \bullet \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

$$\ker \varphi_1 = \langle P_1 \rangle \leftrightarrow \prod \mathfrak{l}_i = (1, \ldots, 1), \qquad \ker \widehat{\varphi_4} = \langle Q_1 \rangle \leftrightarrow (-1, \ldots, -1).$$

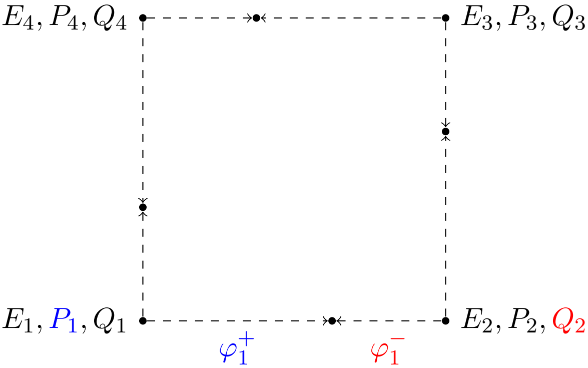
Larger orientations

$$p+1 = 4\prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$

$$\begin{tikzcd}
E_4, P_4, Q_4 \arrow[d, dashed, "\varphi_4"'] & E_3, P_3, Q_3 \arrow[l, dashed, "\varphi_3"'] \\
E_1, P_1, Q_1 \arrow[r, dashed, "\varphi_1"'] & E_2, P_2, Q_2 \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

$$\ker \varphi_1 = \langle P_1 \rangle \leftrightarrow \prod \mathfrak{l}_i = (1, \dots, 1), \qquad \ker \widehat{\varphi_4} = \langle Q_1 \rangle \leftrightarrow (-1, \dots, -1).$$

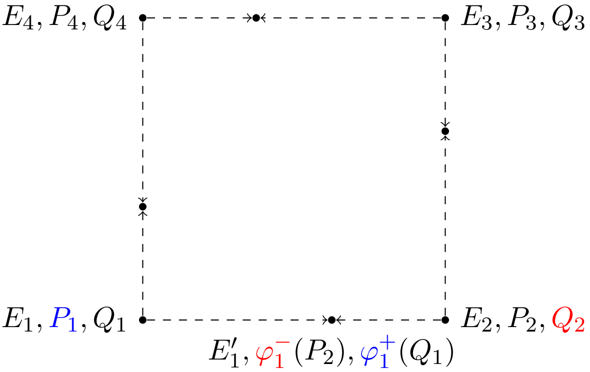
Acting by a binary ideal class



Example

$$\varphi_1^+ \leftrightarrow (1, 0, 1, 1, 0, \ldots), \qquad \varphi_1^- \leftrightarrow (0, -1, 0, 0, -1, \ldots).$$

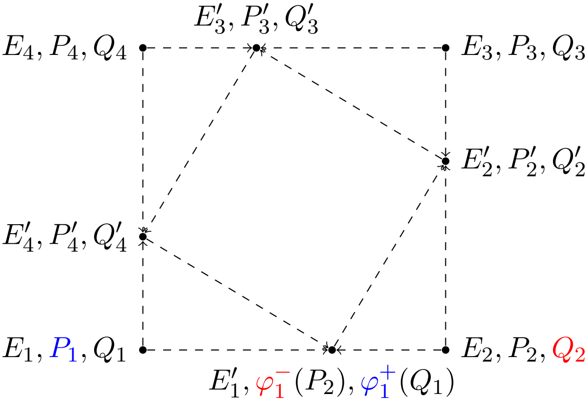
Acting by a binary ideal class



Example

$$\varphi_1^+ \leftrightarrow (1, 0, 1, 1, 0, \ldots), \qquad \varphi_1^- \leftrightarrow (0, -1, 0, 0, -1, \ldots).$$

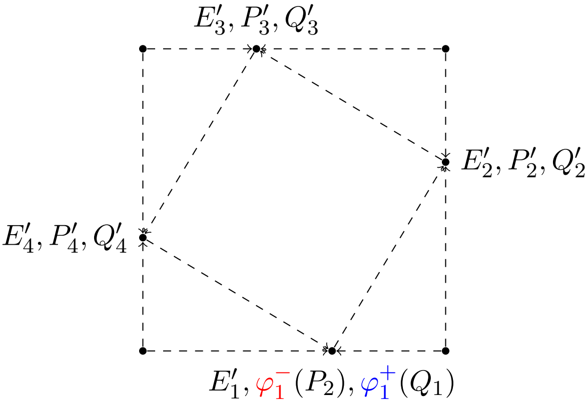
Acting by a binary ideal class



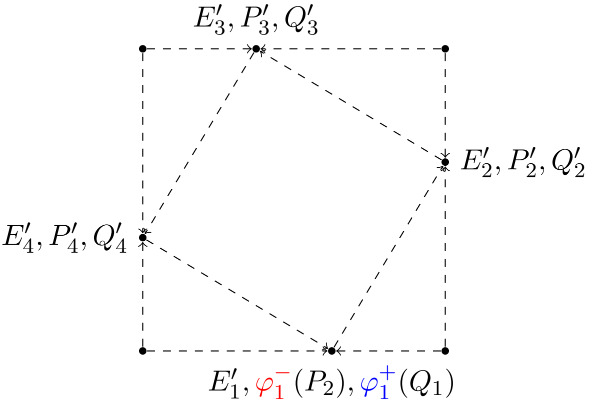
Example

$$\varphi_1^+ \leftrightarrow (1, 0, 1, 1, 0, \ldots), \qquad \varphi_1^- \leftrightarrow (0, -1, 0, 0, -1, \ldots).$$

Acting by a binary ideal class



Acting by a binary ideal class



Cost

Four ℓ_i-isogenies for every i, i.e. one evaluation of $\sigma = \prod \mathfrak{l}_i^4$.

Numbers

Let

$$p = 4 \cdot 3 \cdot 7 \cdot 13 \cdot 23 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 293)}_{61 \text{ consecutive primes}} - 1 \cong 2^{413}.$$

Numbers

Let

$$p = 4 \cdot 3 \cdot 7 \cdot 13 \cdot 23 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 293)}_{61 \text{ consecutive primes}} -1 \cong 2^{413}.$$

Then $E : y^2 = x^3 + x$ can be oriented by $\mathcal{O} = \mathbb{Z}[\sigma]$, where

$$N(\sigma) = \prod_i \ell_i^{5e_i}, \qquad \mathrm{tr}(\sigma) = 1130299,$$

such that

$$\mathrm{Disc}(\sigma) \cong 2^{2058} \text{ is prime.}$$

More numbers

Let

$$p = 4 \cdot 3 \cdot 5 \cdot 11 \cdot 13 \cdot 17 \cdot \underbrace{(3 \cdot 5 \cdot \ldots \cdot 337)}_{67 \text{ consecutive primes}} - 1 \cong 2^{457}.$$

Then $E : y^2 = x^3 + x$ can be oriented by $\mathcal{O} = \mathbb{Z}[\sigma]$, where

$$N(\sigma) = \prod_i \ell_i^{9e_i}, \qquad \operatorname{tr}(\sigma) = 3672029,$$

such that

$$\operatorname{Disc}(\sigma) \cong 2^{4100} \text{ is prime.}$$

High-level overview

High-level overview

(i) Evaluating a class group action is equivalent to factoring an endomorphism representing the orientation (and computing at least one of the factors).

High-level overview

(i) Evaluating a class group action is equivalent to factoring an endomorphism representing the orientation (and computing at least one of the factors).

(ii) This can be done in constant time at the cost of one evaluation of the endomorphism (i.e. by evaluating all of the factors).

High-level overview

(i) Evaluating a class group action is equivalent to factoring an endomorphism representing the orientation (and computing at least one of the factors).

(ii) This can be done in constant time at the cost of one evaluation of the endomorphism (i.e. by evaluating all of the factors).

(iii) We can increase $\log(|\operatorname{Disc}(\mathcal{O})|)$ by a factor r for a cost factor r.

High-level overview

(i) Evaluating a class group action is equivalent to factoring an endomorphism representing the orientation (and computing at least one of the factors).

(ii) This can be done in constant time at the cost of one evaluation of the endomorphism (i.e. by evaluating all of the factors).

(iii) We can increase $\log(|\operatorname{Disc}(\mathcal{O})|)$ by a factor r for a cost factor r.

(iv) In particular, there exist families of class group action-based NIKEs more efficient than CSIDH (at a given NIST security level).

Thank you!

Algorithm 1 Evaluating a class group action using two kernel points

Input: An elliptic curve E/k, generators $P \in E[\sigma], Q \in E[\hat{\sigma}]$, a vector of integers $(s_1, \ldots, s_n) \in [0, e_i]^n$.

Output: The curve $E' := [\prod_i \mathfrak{l}_i^{s_i}] * E$, generators $P' \in E'[\sigma], Q' \in E'[\hat{\sigma}]$.

$(E^+, P^+, Q') \leftarrow (E, P, Q)$; ▷ $P^+ \in E^+[\sigma]$ and $Q' \in E^+[\hat{\sigma}]$.
$(E^-, P^-, P') \leftarrow (E, Q, P)$; ▷ $P^- \in E^-[\hat{\sigma}]$ and $P' \in E^-[\sigma]$.
$m \leftarrow \prod_i \ell_i^{e_i}$;
for $i = 1, \ldots, n$ **do**
  for $j = 1, \ldots, e_i$ **do**
    if $j \leq s_i$ **then**
      $m \leftarrow m/\ell_i$; $K \leftarrow [m]P^+$; ▷ K has order ℓ_i.
      $(E^+, P^+, Q') \leftarrow$ EvalEllIsogeny(E^+, K, P^+, Q'); ▷ "Isogeny"
      $P^- \leftarrow [\ell_i]P^-$; ▷ "Multiply"
    else ▷ Same as above, but with the roles of E^+ and E^- swapped.
      $m \leftarrow m/\ell_i$; $K \leftarrow [m]P^-$;
      $(E^-, P^-, P') \leftarrow$ EvalEllIsogeny(E^-, K, P^-, P');
      $P^+ \leftarrow [\ell_i]P^+$;
    end if
  end for
end for
assert $E^+ = E^-$;
return (E^+, P', Q');