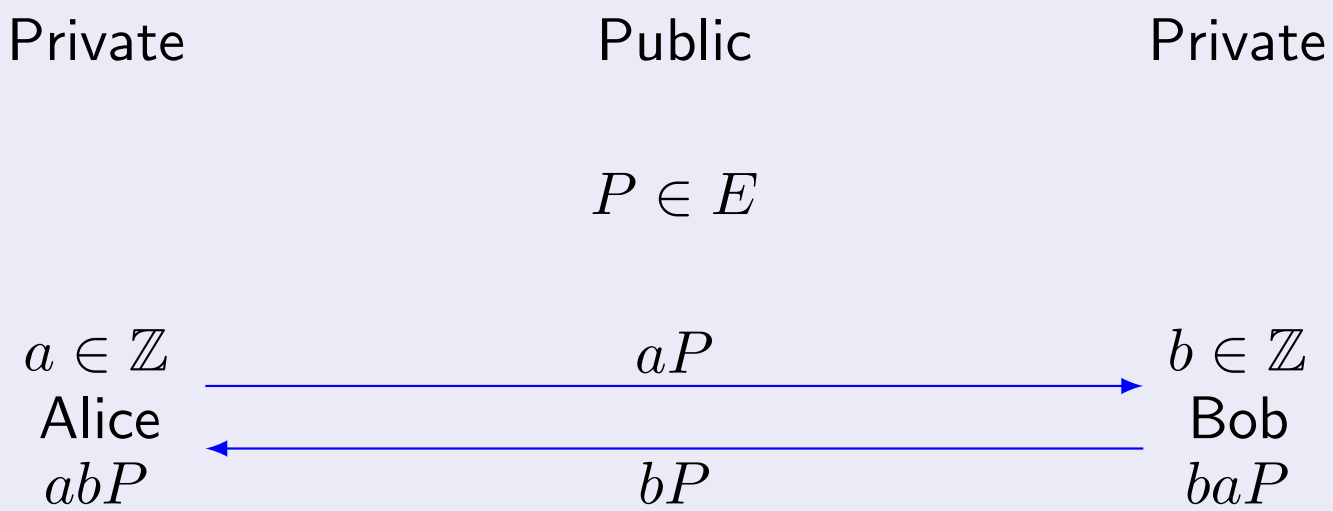
Algorithms for post-quantum commutative group actions

Marc Houben

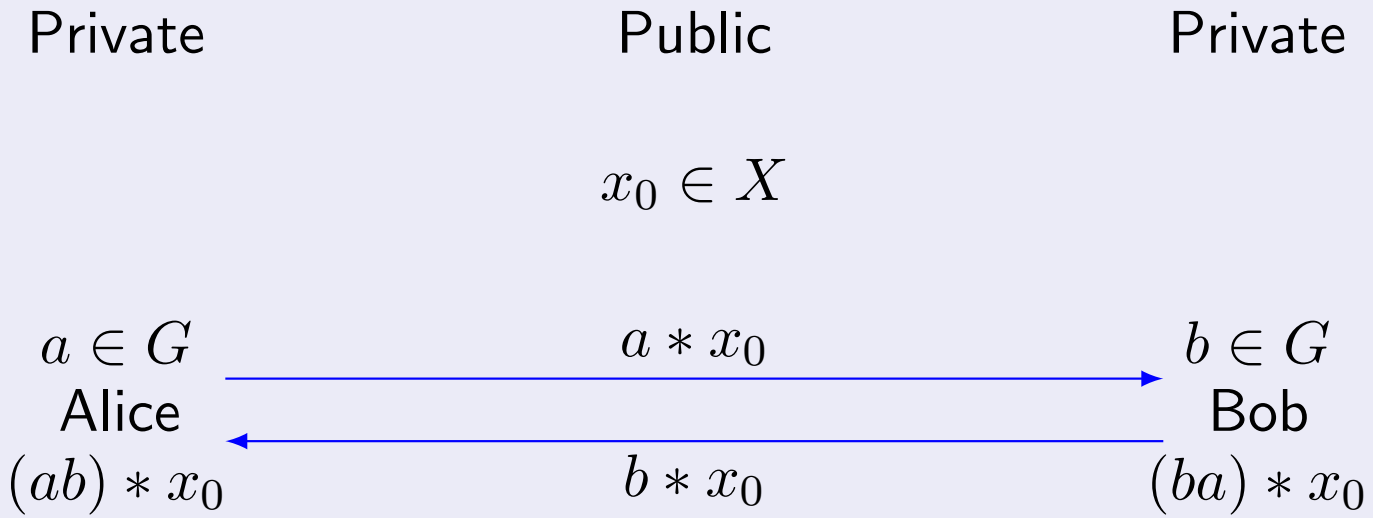
Inria Bordeaux

27 March 2026

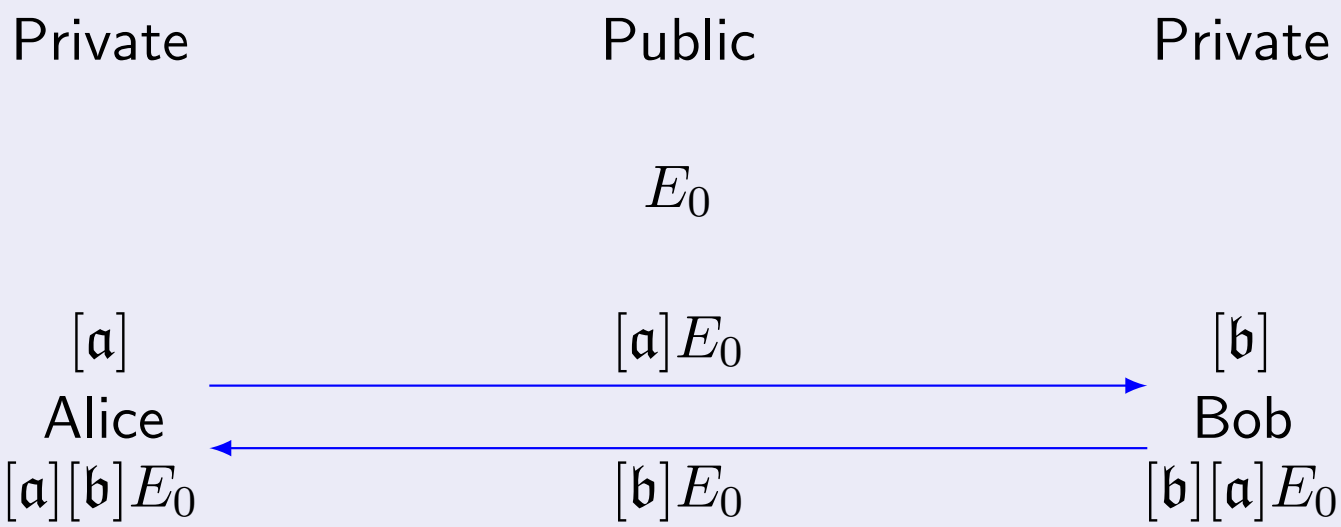
Elliptic Curve Diffie–Hellman (ECDH)



Key exchange from a group action $G \to \mathrm{Sym}(X)$



Class group action on elliptic curves



Commutative group actions in cryptography

- Closest analogue to classical Diffie–Hellman (NIKE).
- Convenient building block for advanced protocols, such as: threshold schemes, public key encryption, (advanced) signatures, oblivious transfer, ID protocols, (verifiable) pseudorandom functions, zero-knowledge proofs, quantum money, password authenticated key exchange, updatable encryption.
- Subject to subexponential quantum attacks (Kuperberg's algorithm).

Outline

- Class group actions, how do they work?
- Existing algorithms for CSIDH
- A deterministic algorithm
- Mitigating subexponential attacks

Complex Multiplication

Elliptic curves over $\mathbb{C}$

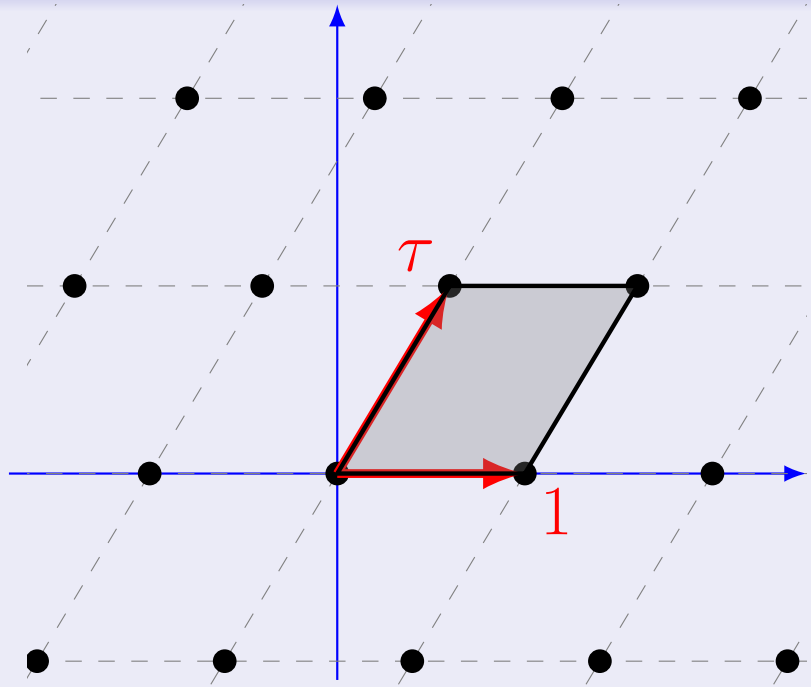
$$\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{\alpha \in \mathbb{C} \mid \alpha\Lambda_1 \subseteq \Lambda_2\}$$

Typically, $\mathrm{End}(\Lambda) = \mathrm{End}(\mathbb{Z}[\tau]) = \mathbb{Z}$.

If $a\tau^2 + b\tau + c = 0$ for coprime $a, b, c \in \mathbb{Z}$:

$$\mathrm{End}(\Lambda) \cong \mathbb{Z}[a\tau] = \mathcal{O} \subseteq K = \mathbb{Q}(\tau).$$

We say Λ has *complex multiplication*.



Elliptic curves over $\mathbb{F}_q$

Always have CM; most of the time the Frobenius endomorphism $\pi : (x, y) \mapsto (x^q, y^q)$ is imaginary quadratic.

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.

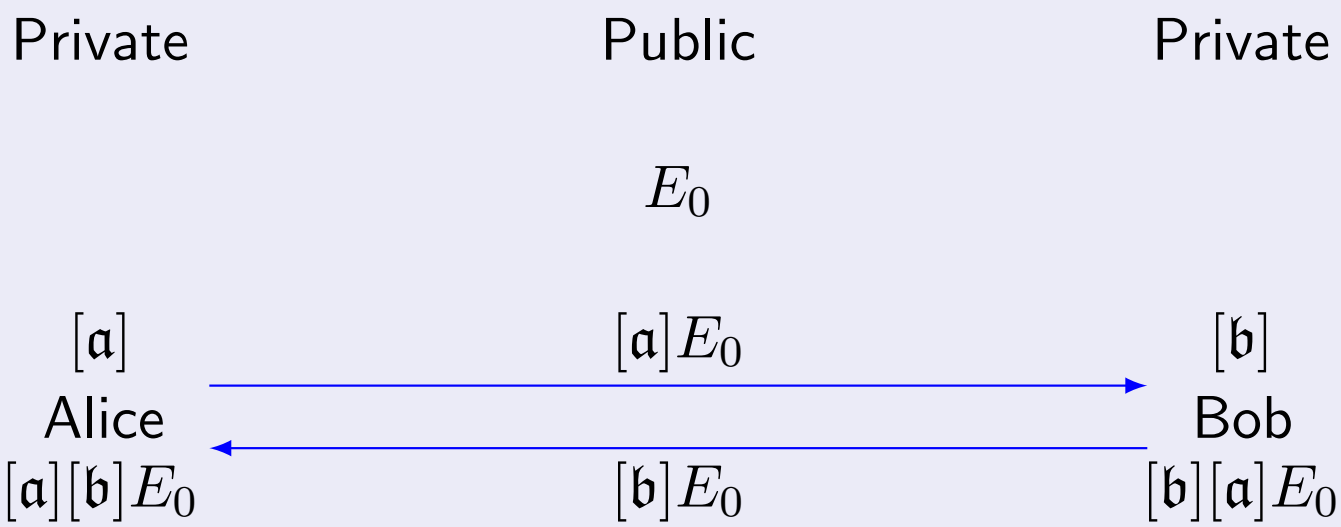
$$\ker \varphi_\mathfrak{a} = E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \iota(\alpha).$$

Theorem

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

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

Class group action on elliptic curves

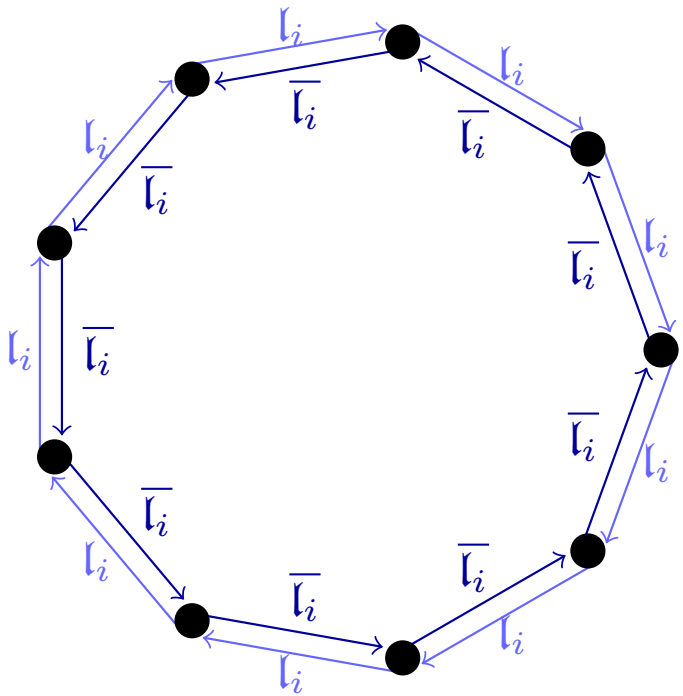


Let $E/\mathbb{F}_p$ be an elliptic curve, $\mathcal{O} = \mathbb{Z}[\pi] \hookrightarrow \mathrm{End}(E)$.

Suppose $\#E(\mathbb{F}_p) = p + 1 = 4 \cdot \prod_{i=1}^{n} \ell_i$.

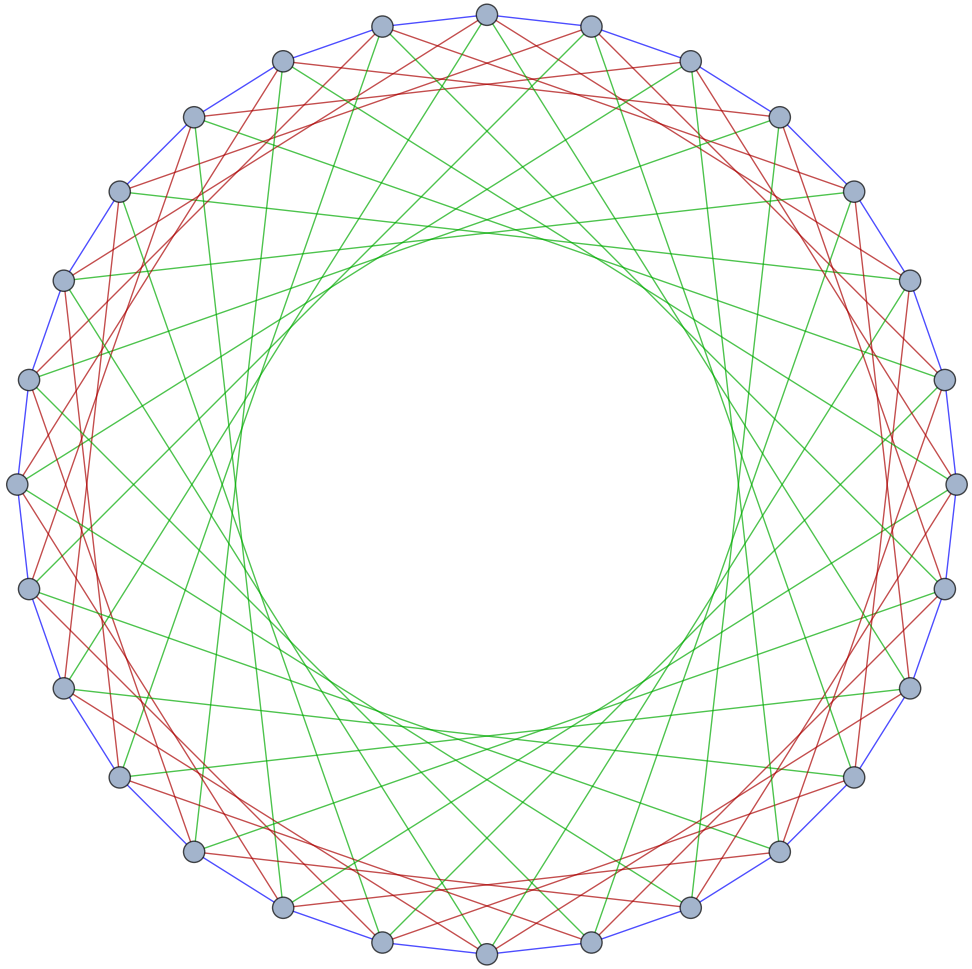
Then, as $\mathcal{O}$-ideals,

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



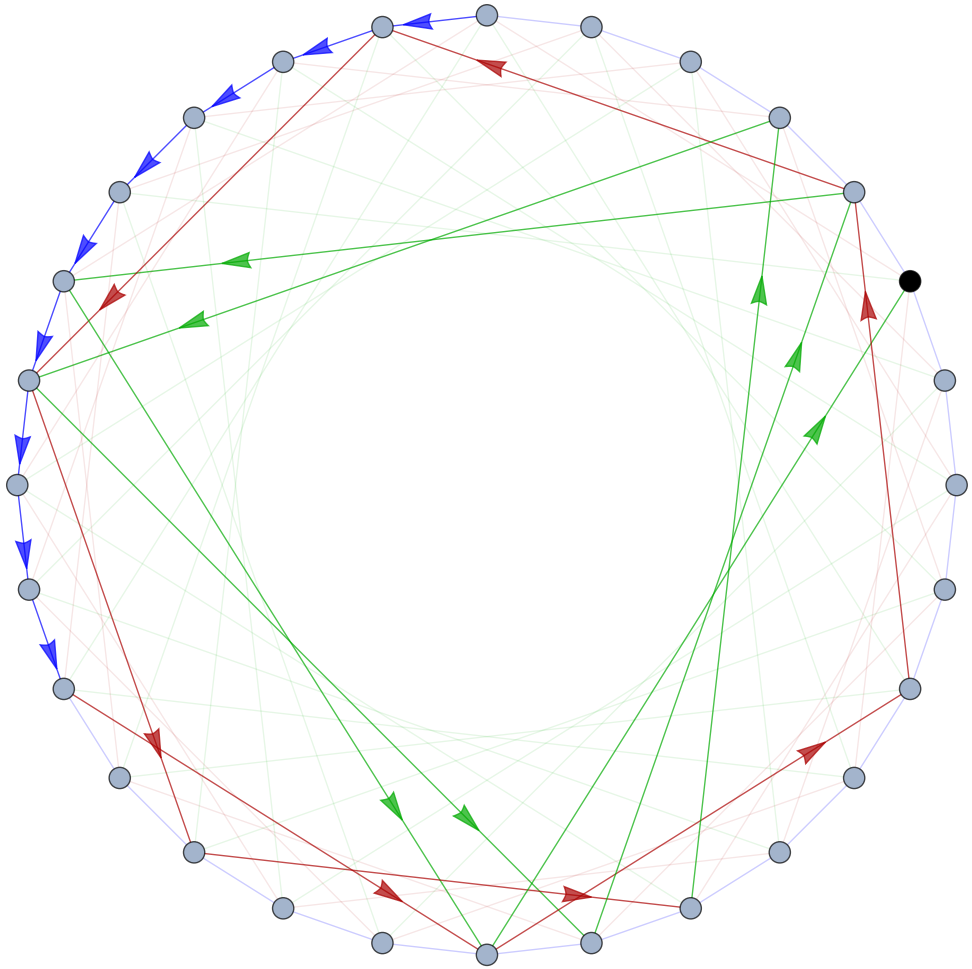
(Connected component of) a supersingular ℓ_i-isogeny graph over $\mathbb{F}_p$.

CSIDH



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

CSIDH



CSIDH-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 $\prod_i [\mathfrak{l}_i]^{a_i} E_B = \prod_i [\mathfrak{l}_i]^{a_i + b_i} E_0$.

(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

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

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

Algorithm

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

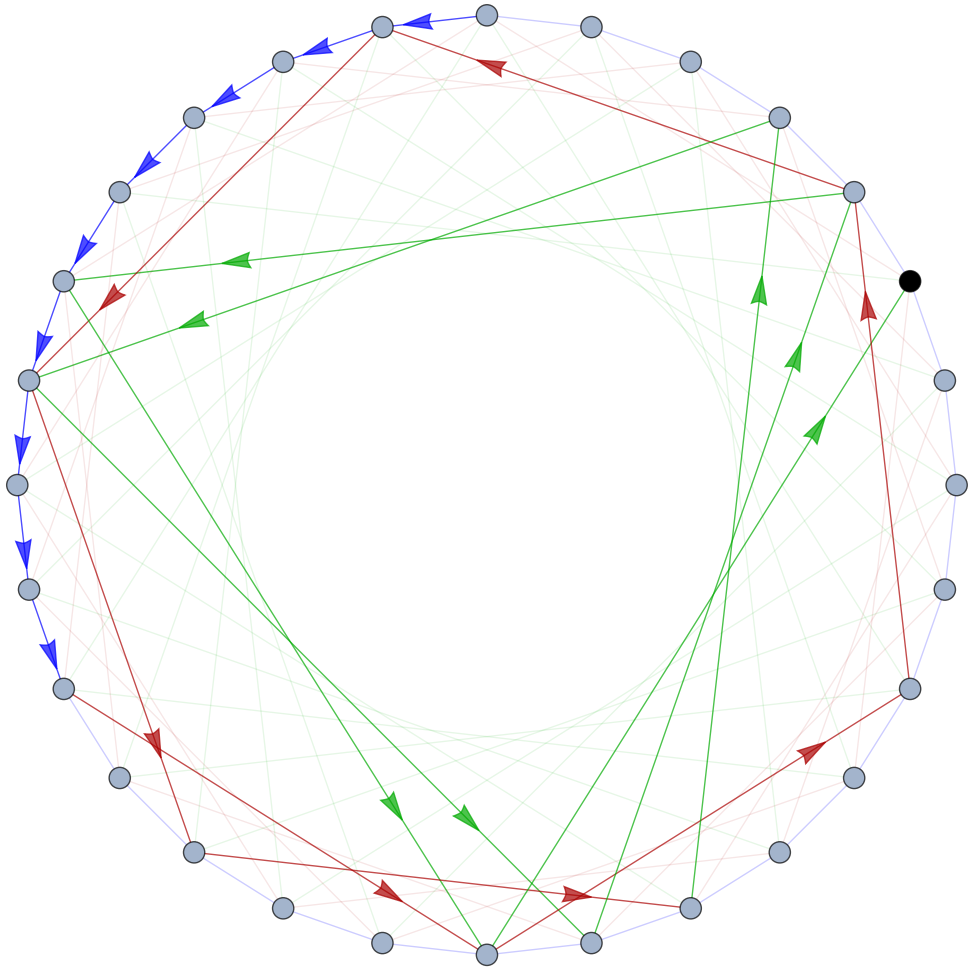
(ii) Compute $P = [\#E(\mathbb{F}_p)/\ell_i]R$.

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

(i) Inefficient. :(

(ii) Not constant time. :((

CSIDH



Method 1: dummy operations

Approach 1

For each ℓ_i, compute m_i isogenies of degree ℓ_i as

$$|s_i| = \underbrace{1 + \ldots + 1}_{s_i} + \underbrace{1 + \ldots + 1}_{m_i - s_i}.$$

Approach 2

For each ℓ_i, assert $m_i - s_i$ is even. Compute m_i isogenies of degree ℓ_i as

$$|s_i| = \underbrace{1 + \ldots + 1}_{s_i} + \underbrace{(1-1) + \ldots + (1-1)}_{m_i - s_i}.$$

Method 2: restrictive key space

Precompute points $P \in E_0[\pi - 1]$ and $Q \in E_0[\pi + 1]$ of order $\prod_{i=1}^{n} \ell_i$.

Approach

Assert that $s_i \in \{-1, 1\}$, i.e. compute exactly *one* ℓ_i-isogeny for every i.

Advantages

(i) No wasteful computations.

(ii) No random point sampling (?).

Disadvantages

(i) Small key space.

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

A brief history of constant time

(i) (2018) Meyer, M., Reith, S.: A faster way to the CSIDH.

(ii) (2019) Bernstein, D.J., Lange, T., Martindale, C., Panny, L.: Quantum circuits for the CSIDH: Optimizing quantum evaluation of isogenies.

(iii) (2019) Meyer, M., Campos, F., Reith, S.: On lions and elligators: An efficient constant-time implementation of CSIDH.

(iv) (2019) Jalali, A., Azarderakhsh, R., Kermani, M.M., Jao, D.: Towards optimized and constant-time CSIDH on embedded devices.

(v) (2019) Onuki, H., Aikawa, Y., Yamazaki, T., Takagi, T.: A faster constant-time algorithm of CSIDH keeping two points.

(vi) (2019) Cervantes-Vázquez, D., Chenu, M., Chi-Domínguez, J.J., De Feo, L., Rodríguez-Henríquez, F., Smith, B.: Stronger and faster side-channel protections for CSIDH.

(vii) (2020) Hutchinson, A., LeGrow, J.T., Koziel, B., Azarderakhsh, R.: Further optimizations of CSIDH: A systematic approach to efficient strategies, permutations, and bound vectors.

(viii) (2020) Moriya, T., Onuki, H., Takagi, T.: How to construct CSIDH on Edwards curves.

(ix) (2020) Chi-Domínguez, J.J., Rodríguez-Henríquez, F.: Optimal strategies for CSIDH.

(x) (2021) Banegas, G., Bernstein, D.J., Campos, F., Chou, T., Lange, T., Meyer, M., Smith, B., Sotáková, J.: CTIDH: faster constant-time CSIDH.

(xi) (2022) 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.

(xii) (2022) Chi-Domínguez, J.J., Reijnders, K.: Fully projective radical isogenies in constant-time.

(xiii) (2024) 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.

(xiv) (2025) Campos, F., Hellenbrand, A., Meyer, M., Reijnders, K.: dCTIDH: Fast & Deterministic CTIDH.

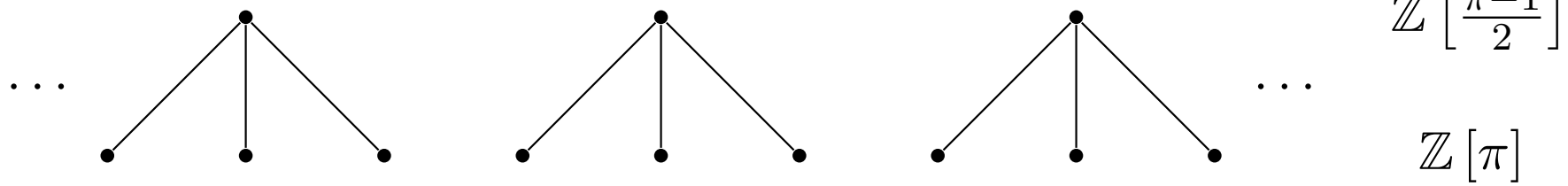
(xv) (2026) This talk.

green: dummy-based approach. blue: (also) studies restrictive key space approach. red: neither.

The 2-isogeny graph

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

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

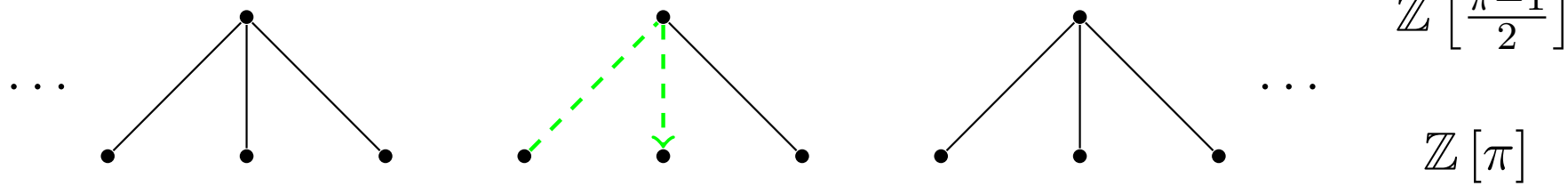


The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 3 \pmod 8$.

The 2-isogeny graph

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

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

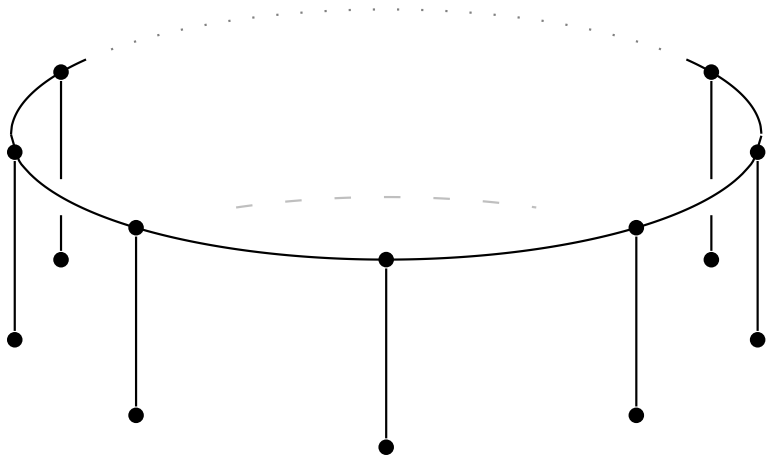


The supersingular $\mathbb{F}_p$-rational 2-isogeny graph if $p \equiv 3 \pmod 8$.

Moving to the surface

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

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



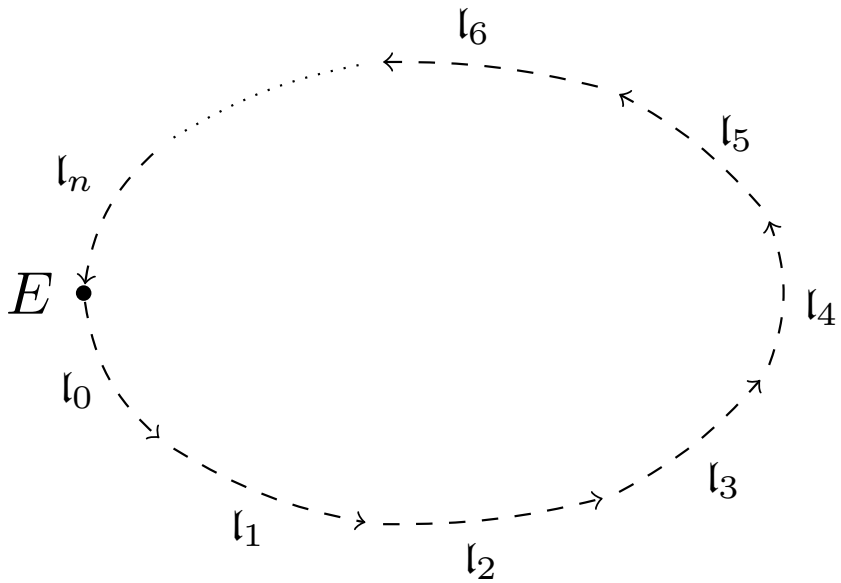
$\mathbb{Z}\left[\frac{\pi-1}{2}\right]$

$\mathbb{Z}[\pi]$

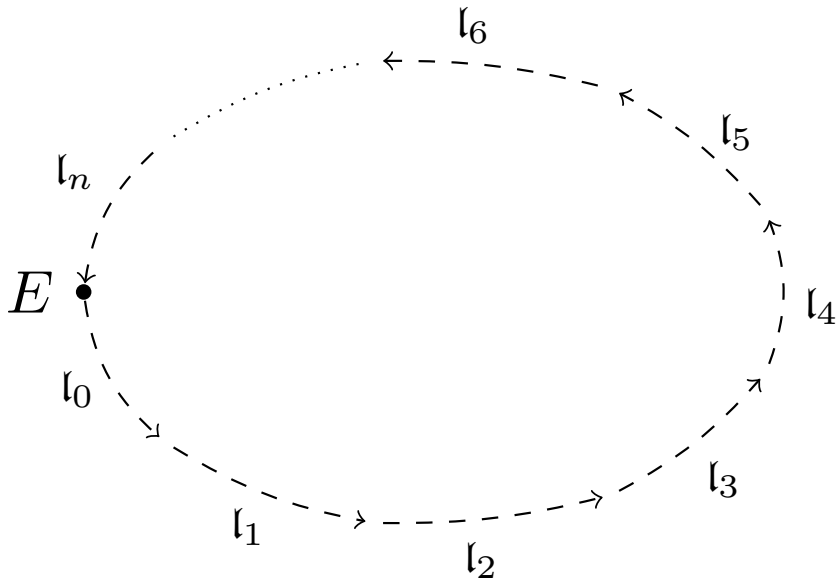
The supersingular $\mathbb{F}_p$-rational 2-isogeny graph (components) if $p \equiv 7 \pmod 8$.

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 $(1, \ldots, 1)$.

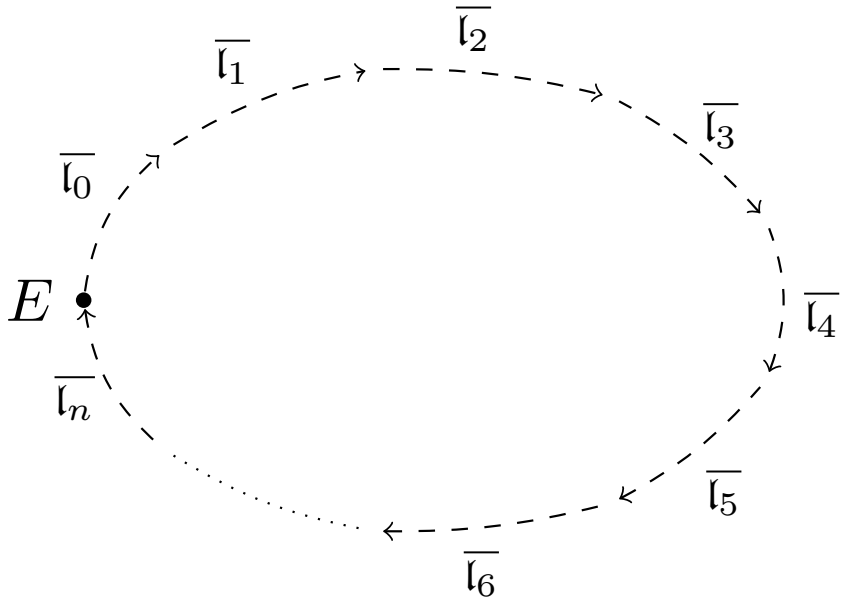


Acting by the ideal class $(1, \ldots, 1)$.

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

Similarly

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

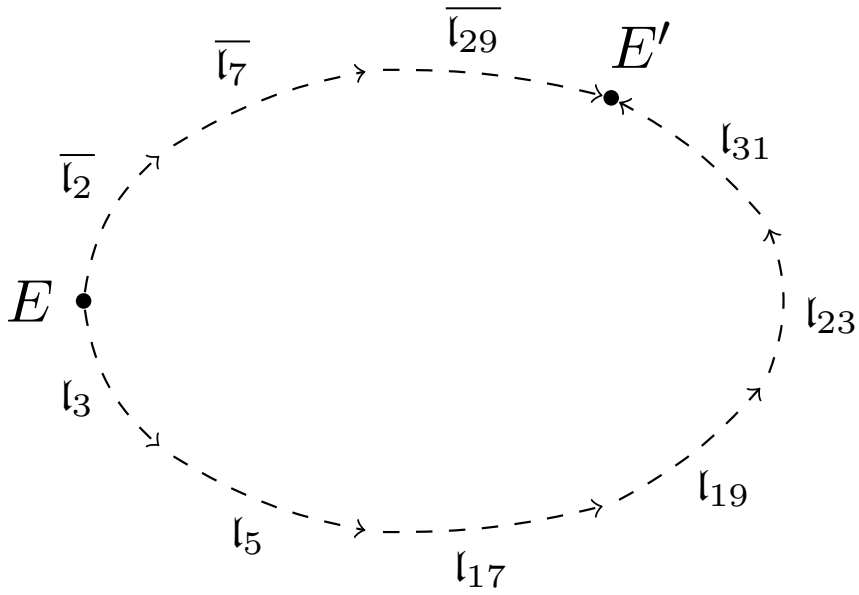


Acting by the ideal class $(-1, \ldots, -1)$.

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

Similarly

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

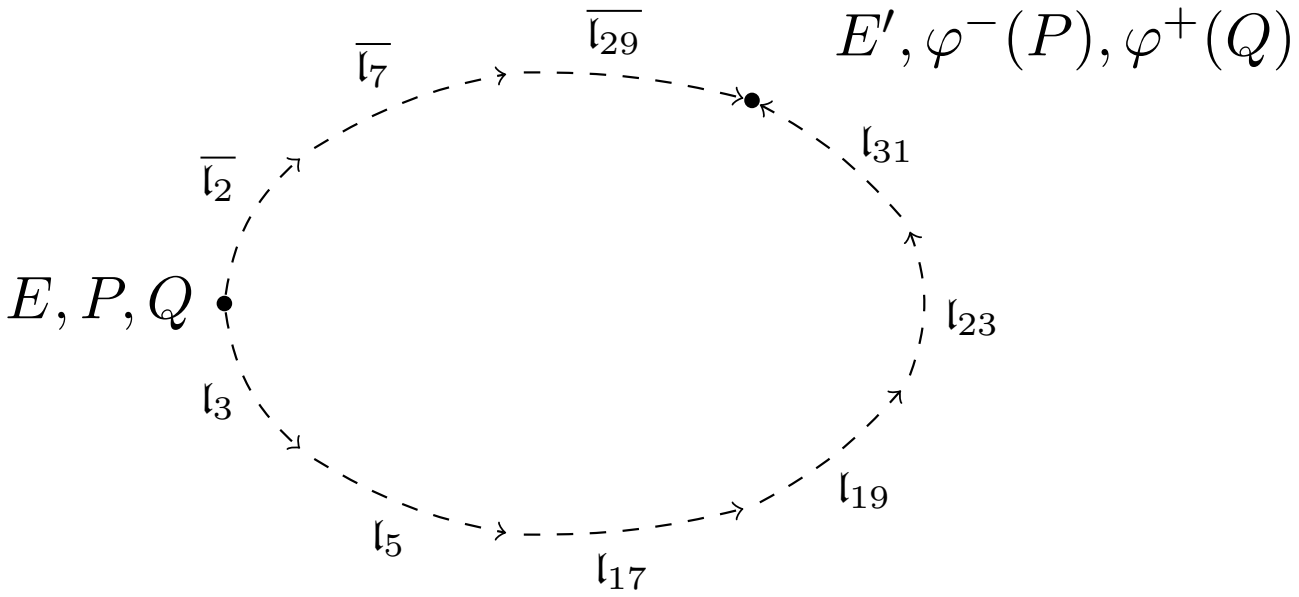


Acting by the ideal class $(0,1,1,0,1,1,1,0,1) \equiv (-1,0,0,-1,0,0,0,-1,0)$.

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

and

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



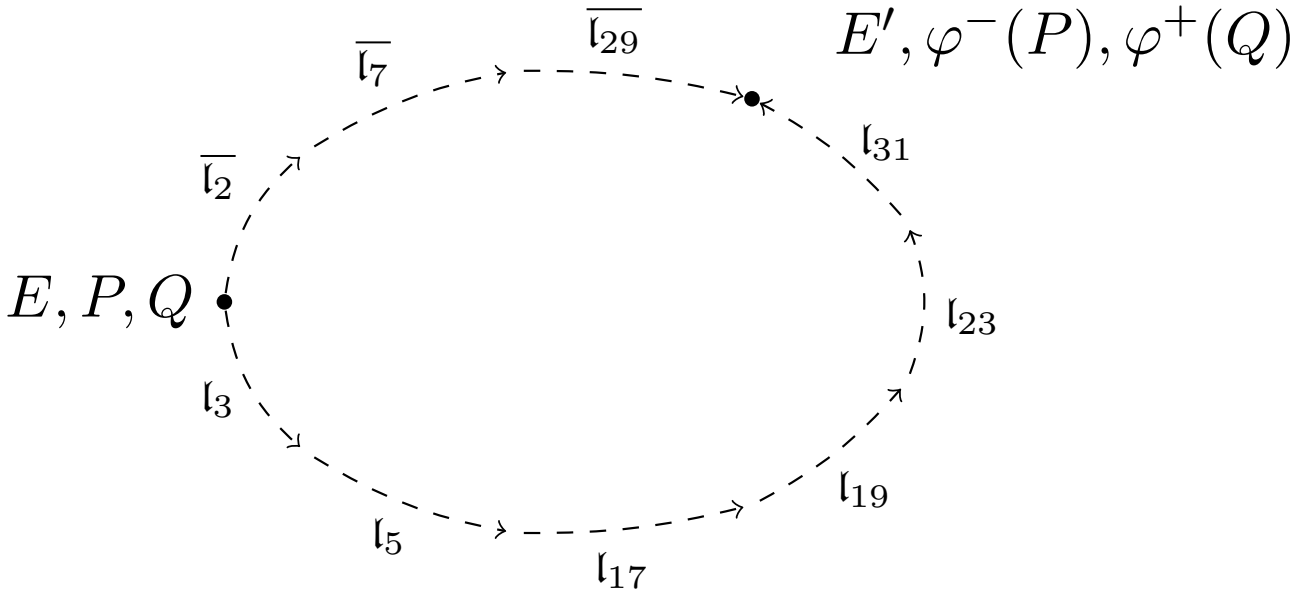
Observation (since $\langle P \rangle \cap \langle Q \rangle = \{0\}$)

$\varphi^-(P)$ 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 CSIDH

$R_0 \leftarrow (E, P, Q), R_1 \leftarrow (E, Q, P)$;
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.
  $\mathsf{cswap}(R_0, R_1, \neg\mathsf{sk}[i])$;
end for;
$R_0[1] \leftarrow R_1[2]$;
return R_0;

Quantum attacks

Commutative group actions are susceptible to Kuperberg's algorithm.

- Subexponential in the bitsize of $\#\operatorname{Cl}(\mathcal{O}) \approx 0.46|\operatorname{Disc}(\mathcal{O})|^{1/2}$.
- In case of CSIDH, we have $|\operatorname{Disc}(\mathcal{O})| = 4p$.

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)

Recent estimates[1] of CSIDH's p for various NIST levels.

[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).

General orientations

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

$$(\sigma) = \prod (\ell_i, \sigma)^{e_i} = \prod \mathfrak{l}_i^{e_i}, \quad \text{and} \quad E[\sigma] \cap E[\hat{\sigma}] = \{0\}.$$

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

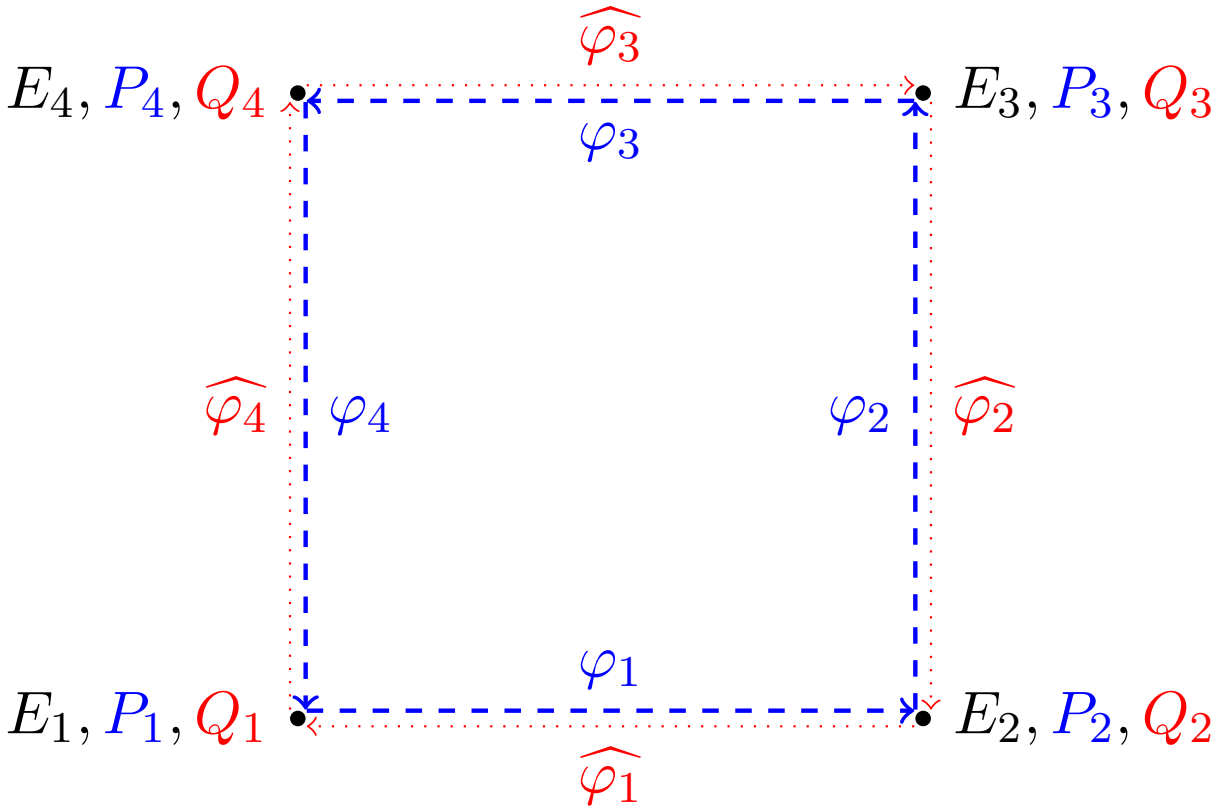
$$|\operatorname{Disc}(\mathcal{O})| = 4N(\sigma) - \operatorname{tr}(\sigma)^2 \leq 4N(\sigma) \lesssim 4qN(\sigma) \lesssim q.$$

CSIDH

Already has $|\operatorname{Disc}(\mathcal{O})| = 4p$.

Isogeny polygons

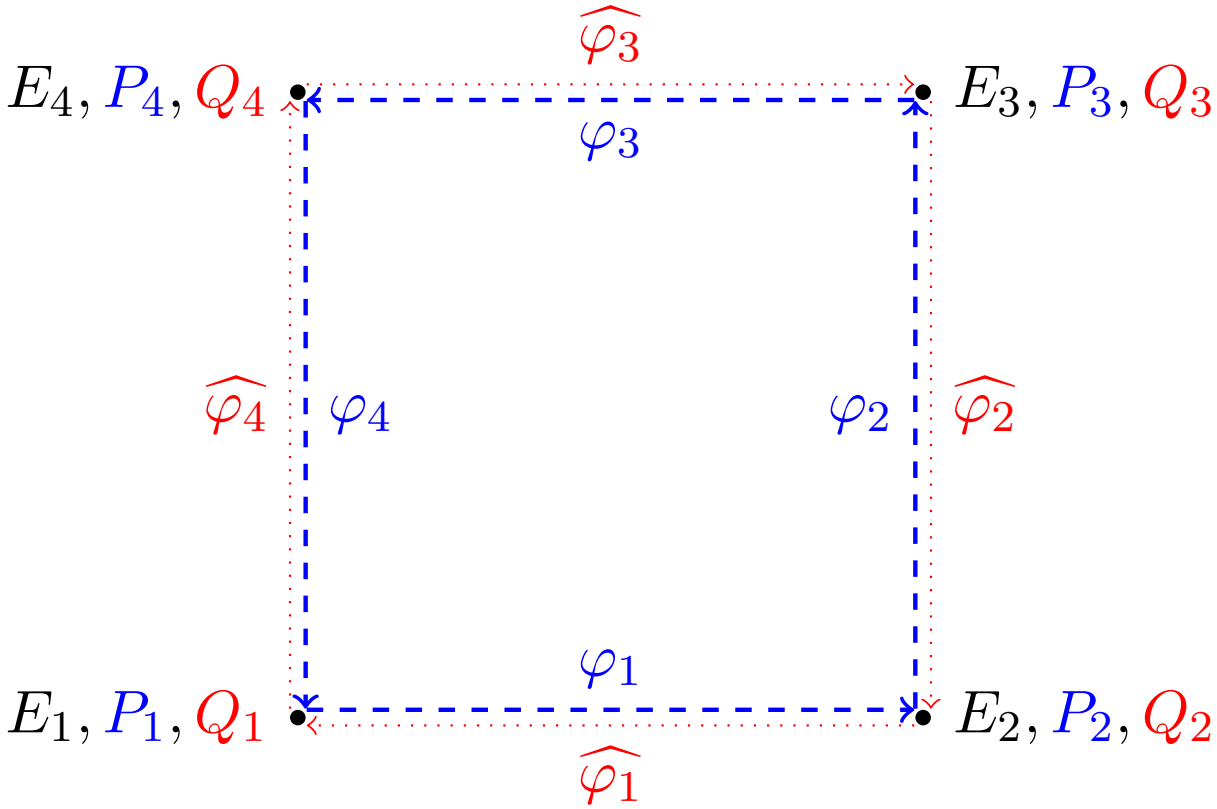
$$p+1 = 4 \cdot \prod \ell_i, \qquad (\sigma) = \prod (\ell_i, \sigma)^4 = \prod \mathfrak{l}_i^4.$$



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

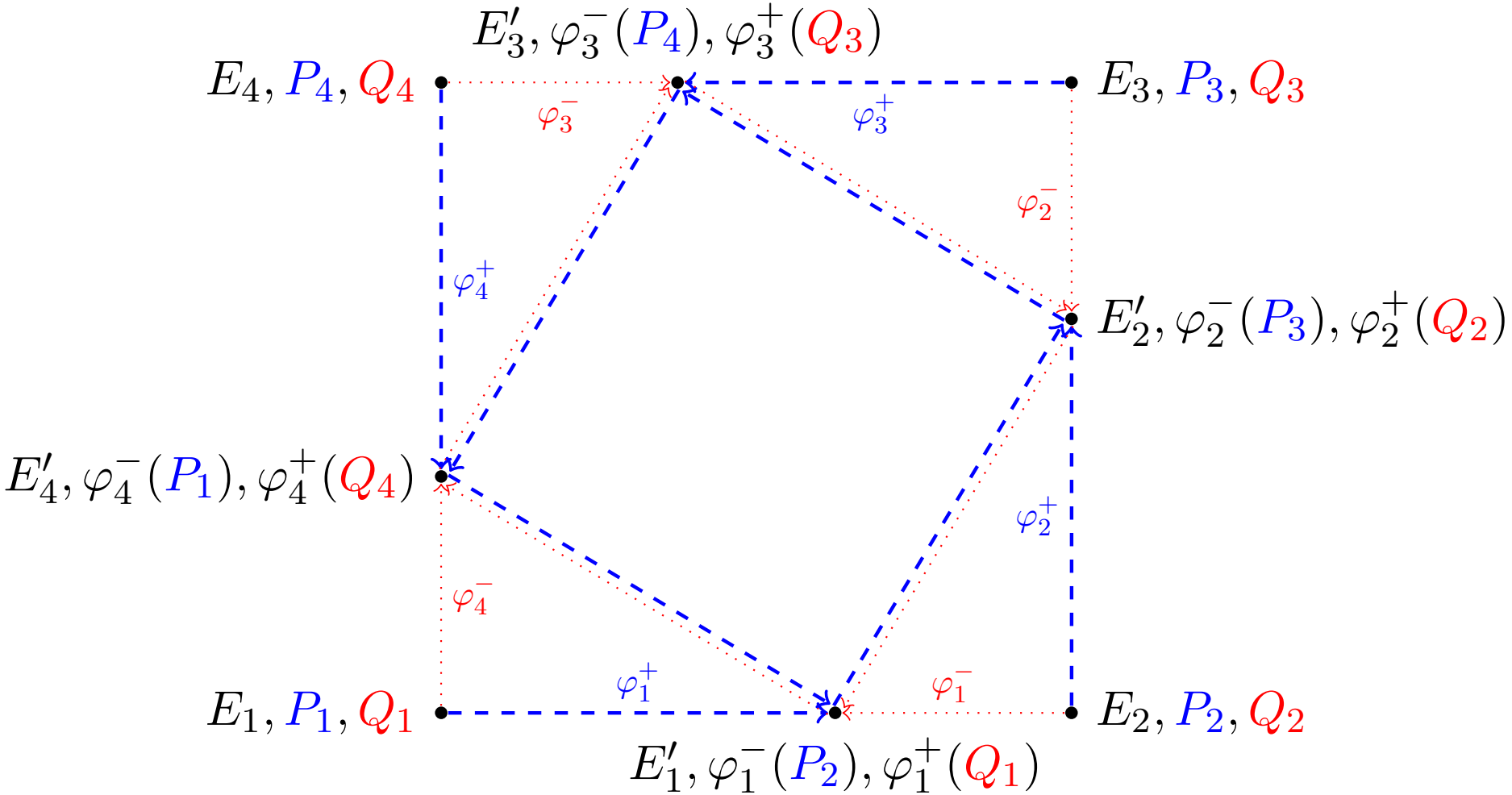
Isogeny polygons

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



$$\ker \varphi_1 = \langle P_1 \rangle \leftrightarrow \prod \mathfrak{l}_i = (1, \ldots, 1), \qquad \ker \widehat{\varphi_1} = \langle Q_2 \rangle \leftrightarrow (-1, \ldots, -1).$$

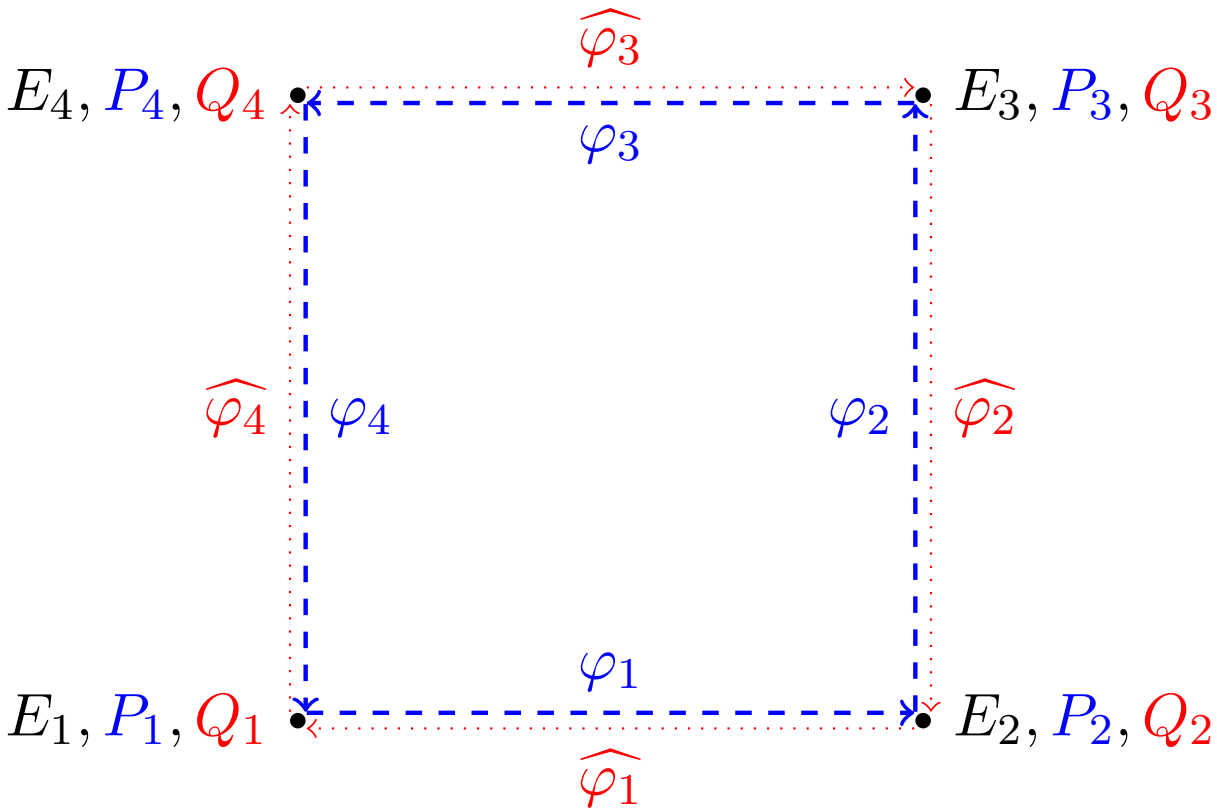
Acting by a binary ideal class



Example

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

Public key compression



Compressed orientation data

$(E_1, \iota) \leftrightarrow (E_1, \langle P_1 \rangle, \ldots, \langle P_r \rangle)$.

$\implies$ public keys of size $\approx 2\log_2(p) + \log_2(\mathrm{Disc}(\mathcal{O}))$.

Covering the full supersingular isogeny graph

Theorem (Elkies, Ono, Yang (2005))

Let p be a prime number, and denote by D a fundamental discriminant that does not split modulo p. For every $t \in \mathbb{Z}_{>0}$ there exists an integer $N_p(t)$ such that if $|D| > N_p(t)$, then every supersingular elliptic curve over $\mathbb{F}_{p^2}$ is $\mathcal{O}$-orientable in at least t non-isomorphic ways.

Experimentally

It looks like supersingular j-invariants are roughly uniformly represented as soon as $|\mathrm{Disc}(\mathcal{O})| > p^2$.

Parameter estimates

Parameter	Attack	Quantum	NIST level 1 bitsize
$\lvert \operatorname{Disc} \mathcal{O} \rvert$	Kuperberg	Yes	2048 (aggressive) 4096 (conservative)
p	BJS	Yes	230 (aggressive) 256 (conservative)
$\#\mathcal{K}$	vOW MITM	No	221 (aggressive) 256 (conservative)

Numbers

Let $q = p^2$, where

$$p = 2^{12} \cdot 3^6 \cdot 5^4 \cdot \underbrace{(7 \cdot 11 \cdot \ldots \cdot 281)}_{57 \text{ consecutive primes}} - 1 \approx 2^{409.2}.$$

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

$$N(\sigma) = \prod_i \ell_i^{5e_i}, \qquad \operatorname{tr}(\sigma) = 1800301,$$

such that

$$|\operatorname{Disc}(\sigma)| = 4N(\sigma) - \operatorname{tr}(\sigma) \approx 2^{2048} \text{ is prime.}$$

The twist trick

If $E/\mathbb{F}_p$ (e.g. $y^2 = x^3 + x$), and $q = p^2$, then

$$E(\mathbb{F}_q) = E[p+1] \qquad \text{and} \qquad E(\mathbb{F}_{q^2}) = E[(p+1)(p-1)].$$

Moreover, if $P \in E[p-1]$, then $x(P) \in \mathbb{F}_q$.

Using Kummer arithmetic...

points of order dividing $p-1$ are equally efficient.

More numbers

Let $p \approx 2^{255.45}$ such that

$$\begin{aligned} p+1 &= 2^5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \\ &\quad \cdot 103 \cdot 107 \cdot 131 \cdot 137 \cdot 149 \cdot 173 \cdot 199 \cdot 211 \cdot 277 \cdot 307 \\ &\quad \cdot 5370594787 \cdot 1039866451667097907655 9; \\ p-1 &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \cdot 89 \cdot 97 \\ &\quad \cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \\ &\quad \cdot 167 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 223 \cdot 233 \cdot 269 \\ &\quad \cdot 167936514812729522270554 81. \end{aligned}$$

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

$$N(\sigma) = \prod_i \ell_i^{13e_i}, \qquad \mathrm{tr}(\sigma) = 29171033,$$

such that

$$|\operatorname{Disc}(\sigma)| \approx 2^{4105} \text{ is prime.}$$

More numbers

Let $p \approx 2^{255.45}$ such that

$$\begin{aligned} p+1 &= 2^5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \\ &\quad \cdot 103 \cdot 107 \cdot 131 \cdot 137 \cdot 149 \cdot 173 \cdot 199 \cdot 211 \cdot 277 \cdot 307 \\ &\quad \cdot 5370594787 \cdot 1039866451667097907655 9; \\ p-1 &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \cdot 89 \cdot 97 \\ &\quad \cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \\ &\quad \cdot 167 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 223 \cdot 233 \cdot 269 \\ &\quad \cdot 167936514812729522270554 81. \end{aligned}$$

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

$$N(\sigma) = \prod_i \ell_i^{13e_i}, \qquad \mathrm{tr}(\sigma) = 29171033,$$

$\implies$ class group action $7\times$ faster than dCSIDH-4096 (excluding random point sampling), unoptimized in SageMath.

Open problem

Is there an efficient algorithm to validate public keys?

Equivalently...

can we efficiently *verify* the value of $\mathrm{tr}(\sigma)$ (given an efficient representation of σ)?

Summary

(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 (parallelizable) 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!

ia.cr/2025/847 *Deterministic algorithms for class group actions.*
ia.cr/2025/1098 *Isogeny-based key exchange from orientations of large discriminant.*

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 $E' := \left[\prod_i \mathfrak{l}_i^{s_i}\right] * E$, 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.
      $(E^+, P^+, Q') \leftarrow \textsc{EvalEllIsogeny}(E^+, K, P^+, Q')$; ▷ "Isogeny"
      $P^- \leftarrow [\ell_i]P^-$; ▷ "Multiply"
    else ▷ Same as above, but with the roles of E^+ and E^- swapped.
      $m \leftarrow m/\ell_i$; $K \leftarrow [m]P^-$;
      $(E^-, P^-, P') \leftarrow \textsc{EvalEllIsogeny}(E^-, K, P^-, P')$;
      $P^+ \leftarrow [\ell_i]P^+$;
    end if
  end for
end for
assert $E^+ = E^-$;
return (E^+, P', Q');