Efficient post-quantum commutative group actions from orientations of large discriminant

Marc Houben

Inria Bordeaux

10 December 2025

Elliptic Curve Diffie–Hellman (ECDH)

Private	Public	Private
	$P \in E$	
$a \in \mathbb{Z}$	aP →	$b \in \mathbb{Z}$
Alice		Bob
abP	← bP	baP

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

Private	Public	Private
	$x_0 \in X$	
$a \in G$	$a * x_0$	$b \in G$
Alice	$\longrightarrow$ / $\longleftarrow$	Bob
$(ab) * x_0$	$b * x_0$	$(ba) * x_0$

Class group action on elliptic curves

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

Commutative group actions in cryptography

Commutative group actions in cryptography

- Closest analogue to classical Diffie–Hellman (NIKE).

Commutative group actions in cryptography

- Closest analogue to classical Diffie–Hellman (NIKE).
- Convenient building block for advanced protocols

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.

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).

In this work

- Class group actions, how do they work?
- A new representation for orientations
- Mitigating subexponential attacks

Isogenies

- Isogenies are maps $E_1 \to E_2$.

Isogenies

- Isogenies are maps $E_1 \to E_2$.
- Endomorphisms are isogenies $E \to E$.

Isogenies

- Isogenies are maps $E_1 \to E_2$.
- Endomorphisms are isogenies $E \to E$.
- The set of endomorphisms forms a ring $\mathrm{End}(E)$.

Isogenies

- Isogenies are maps $E_1 \to E_2$.
- Endomorphisms are isogenies $E \to E$.
- The set of endomorphisms forms a ring $\mathrm{End}(E)$.
- Every $\sigma \in \mathrm{End}(E)$ is either an integer or

$$\sigma^2 - t\sigma + d = 0,$$

where $\mathrm{Disc}(\sigma) = t^2 - 4d < 0$.

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 $\pi = \mathrm{Frob}_p$.

Definition

If $\varphi : E \to E/K$ and $\iota(\sigma)(K) \subseteq K$, then φ *is $\mathcal{O}$-oriented*.

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 $\pi = \mathrm{Frob}_p$.

Definition

If $\varphi : E \to E/K$ and $\iota(\sigma)(K) \subseteq K$, then φ *is $\mathcal{O}$-oriented*.

Ideals $\mathfrak{a} \subseteq \mathcal{O}$ give oriented 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 $\pi = \mathrm{Frob}_p$.

Definition

If $\varphi : E \to E/K$ and $\iota(\sigma)(K) \subseteq K$, then φ *is $\mathcal{O}$-oriented*.

Ideals $\mathfrak{a} \subseteq \mathcal{O}$ give oriented 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 oriented 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

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

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

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

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

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

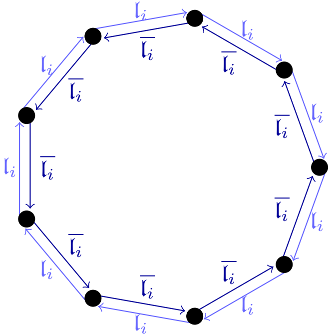
$$(\ell_i) = (\ell_i, \pi - 1)(\ell_i, \pi + 1) = \mathfrak{l}_i \overline{\mathfrak{l}_i}.$$

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

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

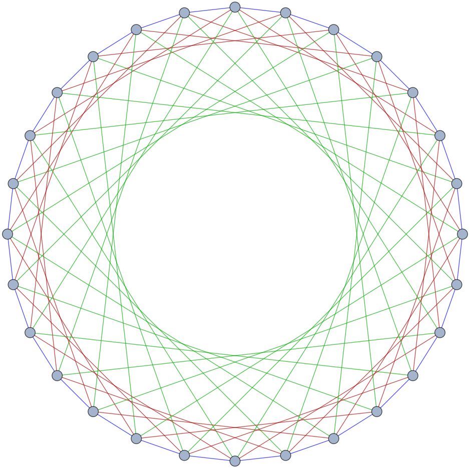
Then, as $\mathcal{O}$-ideals,

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



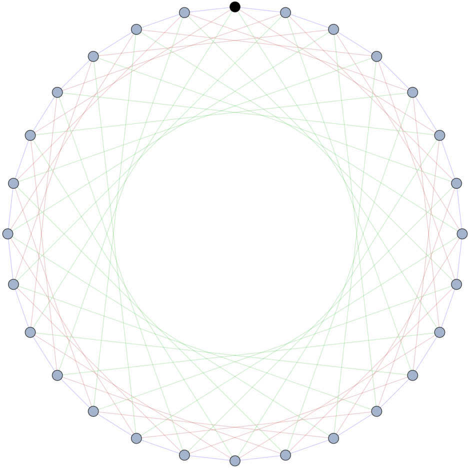
(Connected component of) a supersingular ℓ_i-isogeny graph over $\mathbb{F}_p$.

CSIDH

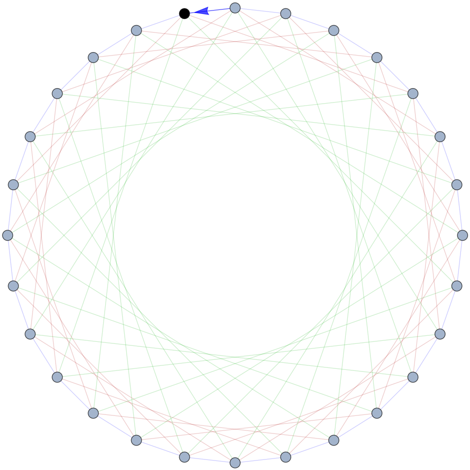


(Connected component of) a union of supersingular 3-, 5-, and 7-isogeny graphs over $\mathbb{F}_p$.

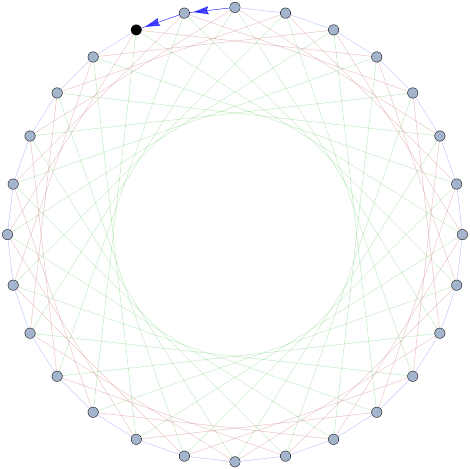
CSIDH



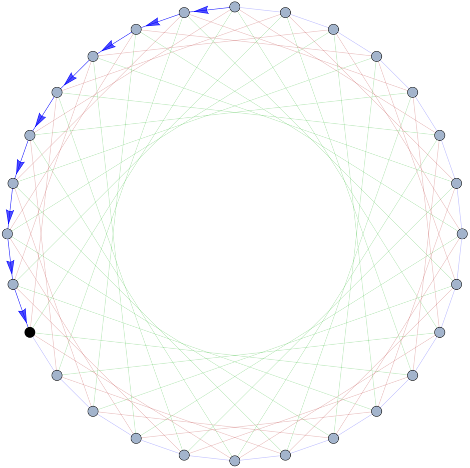
CSIDH



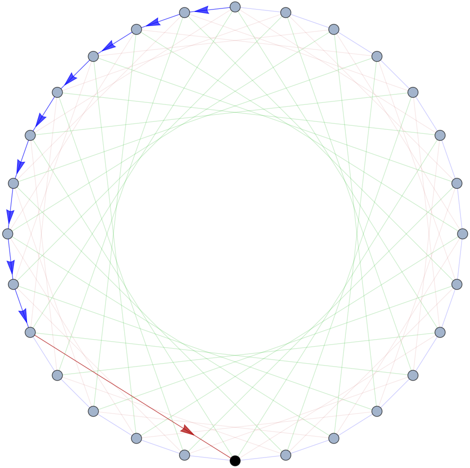
CSIDH



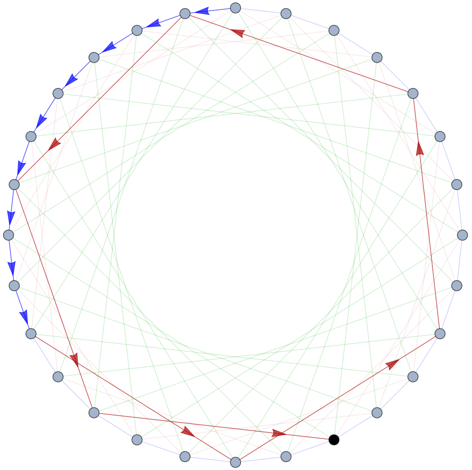
CSIDH



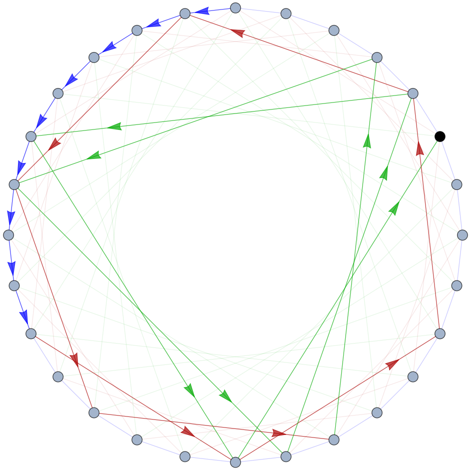
CSIDH



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

Quantum attacks

Commutative group actions are susceptible to Kuperberg's algorithm.

Quantum attacks

Commutative group actions are susceptible to Kuperberg's algorithm.

- Subexponential in the bitsize of $\#\operatorname{Cl}(\mathcal{O}) \approx 0.46|\operatorname{Disc}(\mathcal{O})|^{1/2}$.

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

Quantum attacks

Commutative group actions are susceptible to Kuperberg's algorithm.

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

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

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.

General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

$$\sigma(K) \subseteq K$$

General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

$$\sigma(K) \subseteq K \implies \sigma(R) = \lambda R$$

General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

$$\sigma(K) \subseteq K \implies \sigma(R) = \lambda R \implies R \in \ker(\sigma - \lambda).$$

General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

$$\sigma(K) \subseteq K \implies \sigma(R) = \lambda R \implies R \in \ker(\sigma - \lambda).$$

- Replacing σ by $\sigma - \lambda$, we may assume $K \subseteq E[\sigma]$

General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

$$\sigma(K) \subseteq K \implies \sigma(R) = \lambda R \implies R \in \ker(\sigma - \lambda).$$

- Replacing σ by $\sigma - \lambda$, we may assume $K \subseteq E[\sigma]$
  $\implies$ we have that φ is a *factor* of σ.

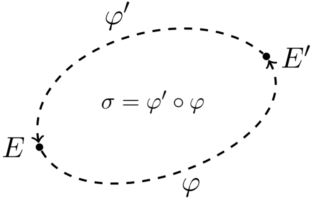
General orientations

- Let $\mathbb{Z}[\sigma] \hookrightarrow \mathrm{End}(E)$ be an orientation.
- Let $\varphi : E \to E' = E/K$ be an oriented isogeny, where $K = \langle R \rangle$.

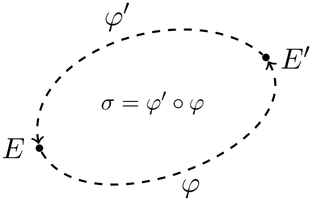
$$\sigma(K) \subseteq K \implies \sigma(R) = \lambda R \implies R \in \ker(\sigma - \lambda).$$

- Replacing σ by $\sigma - \lambda$, we may assume $K \subseteq E[\sigma]$

  $\implies$ we have that φ is a *factor* of σ.

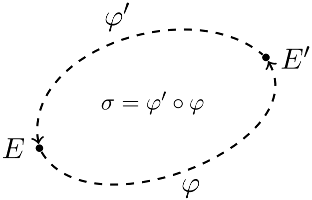


Evaluating a class group action $\equiv$ factoring an endomorphism.



Evaluating a class group action $\equiv$ factoring an endomorphism.

σ has many factors $\iff$ $N(\sigma)$ has many factors.



Evaluating a class group action $\equiv$ factoring an endomorphism.

σ has many factors $\iff$ $N(\sigma)$ has many factors.

In CSIDH

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

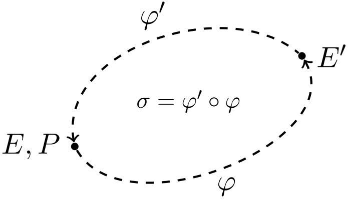
Representing the orientation

Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.

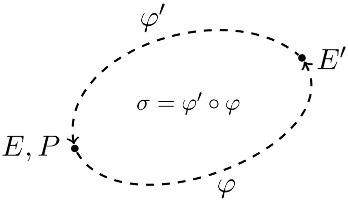
Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.



Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.

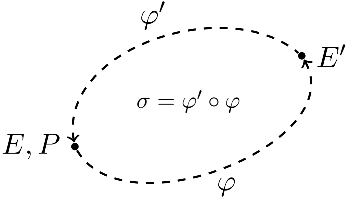


Problems

- What is $P' \in E'[\sigma]$?

Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.

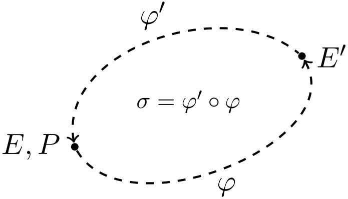


Problems

- What is $P' \in E'[\sigma]$?
- If $P \in E(\mathbb{F}_q)$ then

Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.

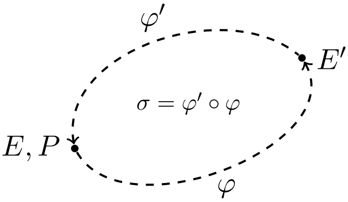


Problems

- What is $P' \in E'[\sigma]$?
- If $P \in E(\mathbb{F}_q)$ then $N(\sigma) \lesssim q$.

Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.

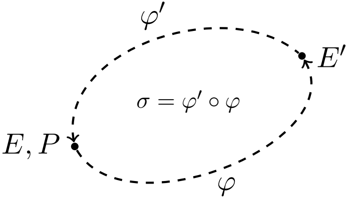


Problems

- What is $P' \in E'[\sigma]$?
- If $P \in E(\mathbb{F}_q)$ then $4N(\sigma) \lesssim 4q$.

Representing the orientation

Give $P \in E(\mathbb{F}_q)$ (of smooth order) such that $E[\sigma] = \langle P \rangle$.



Problems

- What is $P' \in E'[\sigma]$?
- If $P \in E(\mathbb{F}_q)$ then $|\operatorname{Disc}(\mathcal{O})| = 4N(\sigma) - \operatorname{tr}(\sigma)^2 \leq 4N(\sigma) \lesssim 4q$.

CSIDH

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

A new orientation representation

$$p + 1 = 4 \cdot \prod \ell_i, \qquad N(\sigma) = \prod \ell_i^4 = M^4$$

A new orientation representation

$$p + 1 = 4 \cdot \prod \ell_i, \qquad N(\sigma) = \prod \ell_i^4 = M^4$$

$$\begin{tikzcd}
E_4 \arrow[d, dashed, "\varphi_4"] & E_3 \arrow[l, dashed, "\varphi_3"'] \\
E_1 \arrow[r, dashed, "\varphi_1"] & E_2 \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

Splitting σ into four isogenies of degree $\deg \varphi_j = M$.

A new orientation representation

$$p + 1 = 4 \cdot \prod \ell_i, \qquad N(\sigma) = \prod \ell_i^4 = M^4$$

$$\begin{tikzcd}
E_4 \arrow[d, dashed, "\varphi_4"] & E_3 \arrow[l, dashed, "\varphi_3"] \\
E_1 \arrow[r, dashed, "\varphi_1"] & E_2 \arrow[u, dashed, "\varphi_2"']
\end{tikzcd}$$

$\ker \varphi_j \subseteq E[M] \subseteq E_j(\mathbb{F}_{p^2})$.

A new orientation representation

$$p + 1 = 4 \cdot \prod \ell_i, \qquad N(\sigma) = \prod \ell_i^4 = M^4$$

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

$$\ker \varphi_j = \langle P_j \rangle \leftrightarrow (1, \ldots, 1),$$

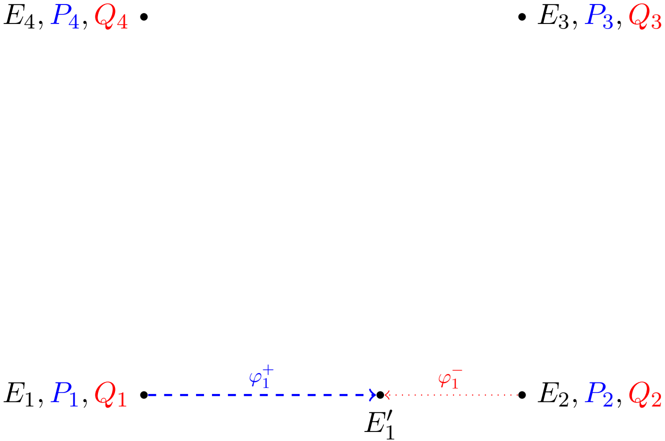
A new orientation representation

$$p + 1 = 4 \cdot \prod \ell_i, \qquad N(\sigma) = \prod \ell_i^4 = M^4$$

$$\begin{tikzcd}
E_4, P_4, Q_4 \arrow[rr, shift left, dotted, "\widehat{\varphi_3}"] \arrow[dd, shift left, dashed, "\varphi_4"] && E_3, P_3, Q_3 \arrow[ll, shift left, dashed, "\varphi_3"] \arrow[dd, shift left, dotted, "\widehat{\varphi_2}"] \\
\\
E_1, P_1, Q_1 \arrow[rr, shift left, dashed, "\varphi_1"] \arrow[uu, shift left, dotted, "\widehat{\varphi_4}"] && E_2, P_2, Q_2 \arrow[uu, shift left, dashed, "\varphi_2"] \arrow[ll, shift left, dotted, "\widehat{\varphi_1}"]
\end{tikzcd}$$

$$\ker \varphi_j = \langle P_j \rangle \leftrightarrow (1, \ldots, 1), \qquad \ker \widehat{\varphi_j} = \langle Q_{j+1} \rangle \leftrightarrow (-1, \ldots, -1).$$

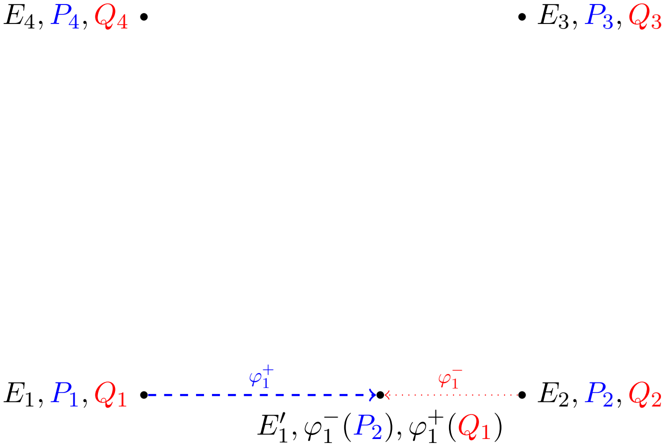
Acting by a non-trivial ideal class



Example

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

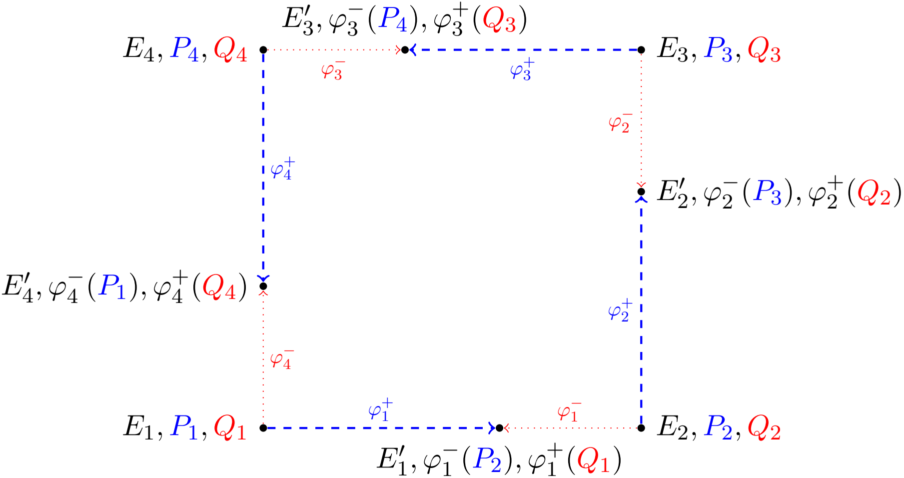
Acting by a non-trivial ideal class



Example

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

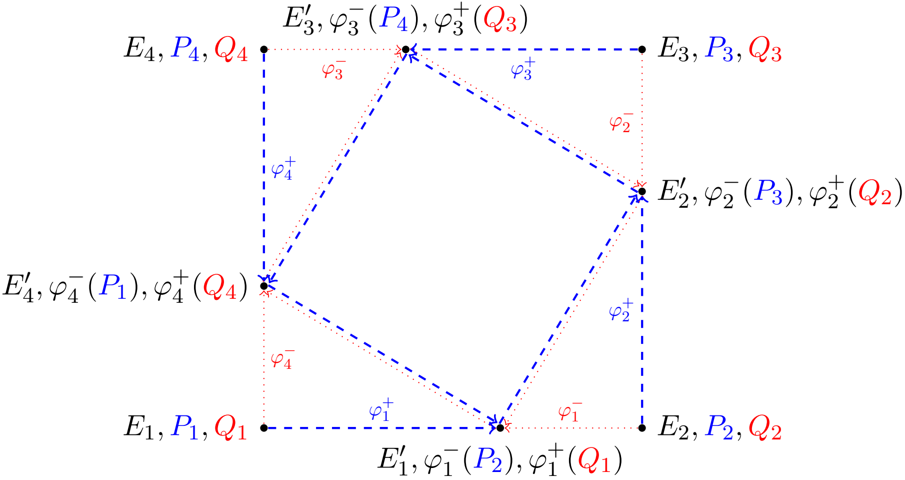
Acting by a non-trivial ideal class



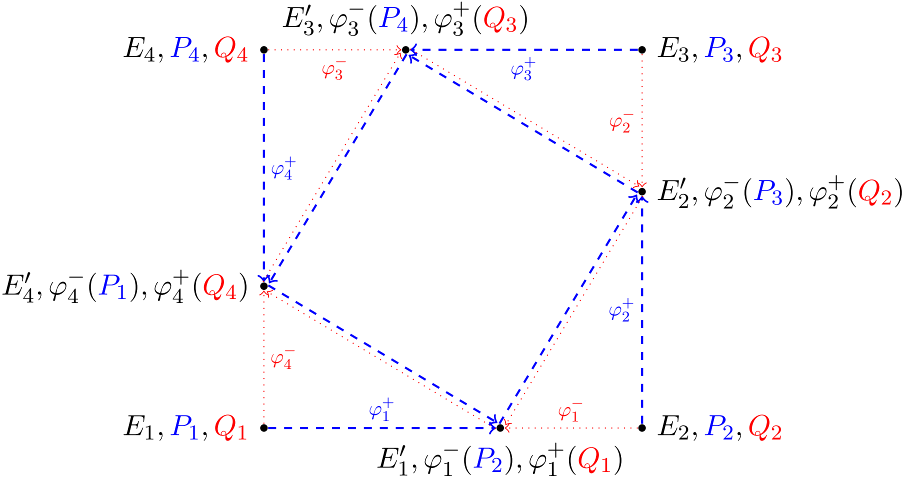
Example

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

Acting by a non-trivial ideal class



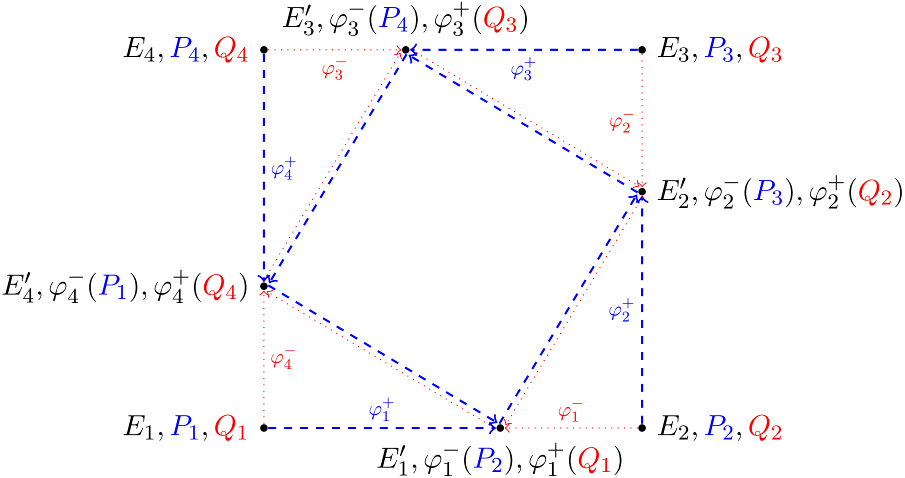
Acting by a non-trivial ideal class



Result

Orientation data on E'_1.

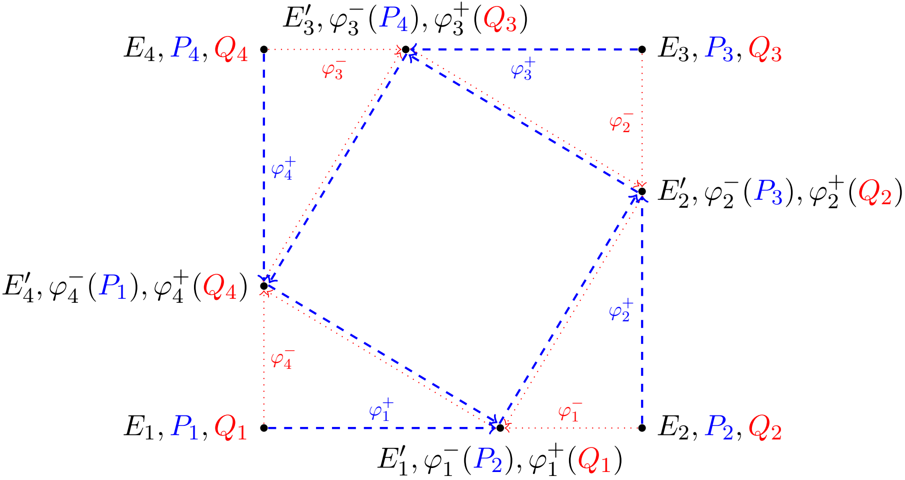
Acting by a non-trivial ideal class



Result

Orientation data on E_1'. Iterate to act by any exponent vector $\in \mathbb{Z}^n$.

Acting by a non-trivial ideal class

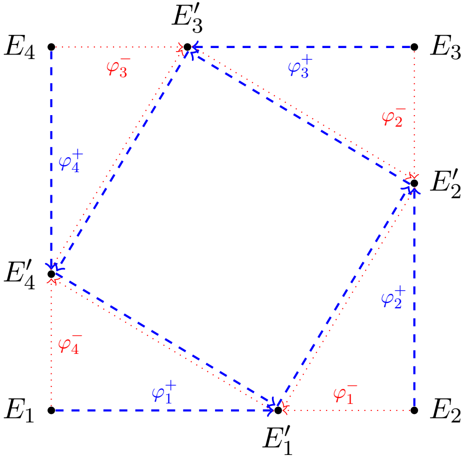


Cost of one iteration

Four ℓ_i-isogenies for every i, i.e. one evaluation of σ.

Properties of the algorithm

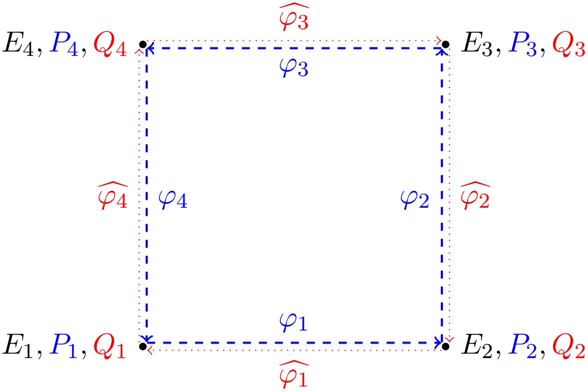
- Constant time
- Deterministic
- Dummy free
- Branchless
- Perfectly parallelizable



Public key compression

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

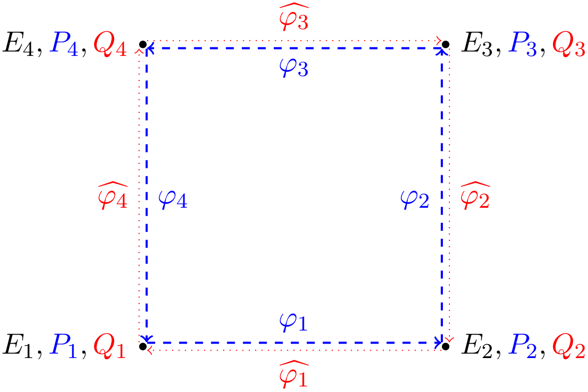
Public key compression



Compressed orientation data

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

Public key compression



Compressed orientation data

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

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

Numbers

Let $q = p^2$, where

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

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

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

More numbers

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

More numbers

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

$$
\begin{aligned}
p+1 &= 2^5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \\
&\cdot 103 \cdot 107 \cdot 131 \cdot 137 \cdot 149 \cdot 173 \cdot 199 \cdot 211 \cdot 277 \cdot 307 \\
&\cdot 5370594787 \cdot 103986645166709790765559; \\
p-1 &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \cdot 89 \cdot 97 \\
&\cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \\
&\cdot 167 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 223 \cdot 233 \cdot 269 \\
&\cdot 167936514812729522270554\,81.
\end{aligned}
$$

More numbers

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

$$
\begin{aligned}
p+1 &= 2^5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \\
&\cdot 103 \cdot 107 \cdot 131 \cdot 137 \cdot 149 \cdot 173 \cdot 199 \cdot 211 \cdot 277 \cdot 307 \\
&\cdot 5370594787 \cdot 1039866451667097907 6559; \\
p-1 &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \cdot 89 \cdot 97 \\
&\cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \\
&\cdot 167 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 223 \cdot 233 \cdot 269 \\
&\cdot 16793651481272952227055481.
\end{aligned}
$$

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

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

More numbers

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

$$\begin{aligned} p+1 &= 2^5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \\ &\quad \cdot 103 \cdot 107 \cdot 131 \cdot 137 \cdot 149 \cdot 173 \cdot 199 \cdot 211 \cdot 277 \cdot 307 \\ &\quad \cdot 5370594787 \cdot 1039866451667097907655 9; \\ p-1 &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \cdot 89 \cdot 97 \\ &\quad \cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \\ &\quad \cdot 167 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 223 \cdot 233 \cdot 269 \\ &\quad \cdot 16793651481272952227055481. \end{aligned}$$

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

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

More numbers

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

$$\begin{aligned} p+1 &= 2^5 \cdot 7^2 \cdot 11 \cdot 23 \cdot 29 \cdot 37 \cdot 41 \cdot 43 \cdot 53 \cdot 61 \cdot 67 \cdot 73 \cdot 79 \cdot 83 \\ &\quad \cdot 103 \cdot 107 \cdot 131 \cdot 137 \cdot 149 \cdot 173 \cdot 199 \cdot 211 \cdot 277 \cdot 307 \\ &\quad \cdot 5370594787 \cdot 1039866451667097907655 9; \\ p-1 &= 2 \cdot 3^2 \cdot 5 \cdot 13 \cdot 17 \cdot 19 \cdot 31 \cdot 47 \cdot 59 \cdot 71 \cdot 89 \cdot 97 \\ &\quad \cdot 101 \cdot 109 \cdot 113 \cdot 127 \cdot 139 \cdot 151 \cdot 157 \cdot 163 \\ &\quad \cdot 167 \cdot 179 \cdot 181 \cdot 191 \cdot 193 \cdot 223 \cdot 233 \cdot 269 \\ &\quad \cdot 16793651481272952227055481. \end{aligned}$$

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

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

$\Longrightarrow$ 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?

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

Summary

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

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).

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.

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 actions more efficient than CSIDH.

Thank you!

https://ia.cr/2025/1098