# Extending class group action attacks via sesquilinear pairings

Joseph Macula
Joint work with Katherine Stange

# Overview

# The Vectorization Problem

- $E$ a supersingular elliptic curve over finite field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = p$, $K$ an imaginary quadratic field, $\mathcal{O}$ an order in $K$

# The Vectorization Problem

- $E$ a supersingular elliptic curve over finite field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = p$, $K$ an imaginary quadratic field, $\mathcal{O}$ an order in $K$
- A *$K$-orientation* of $E$ is an embedding

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$$

If $\iota(\mathcal{O}) \subset \mathrm{End}(E)$, $\iota$ is an *$\mathcal{O}$-orientation*
If $\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E)$, $\iota$ is a *primitive* $\mathcal{O}$-orientation

# The Vectorization Problem

- $E$ a supersingular elliptic curve over finite field $\mathbb{F}$, $\mathrm{char}(\mathbb{F}) = p$, $K$ an imaginary quadratic field, $\mathcal{O}$ an order in $K$
- A *$K$-orientation* of $E$ is an embedding

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \cong B_{p,\infty}$$

  If $\iota(\mathcal{O}) \subset \mathrm{End}(E)$, $\iota$ is an *$\mathcal{O}$-orientation*
  If $\iota(\mathcal{O}) = \iota(K) \cap \mathrm{End}(E)$, $\iota$ is a *primitive* $\mathcal{O}$-orientation
- We denote a supersingular curve $E$ with a $K$-orientation $\iota$ by $(E, \iota)$

# The Vectorization Problem

- $SS_{\mathcal{O}}^{pr} := \{(E, \iota) : \iota \text{ a primitive } \mathcal{O}\text{-orientation}\} / \sim$

# The Vectorization Problem

- $SS_{\mathcal{O}}^{pr} := \{(E,\iota) : \iota \text{ a primitive } \mathcal{O}\text{-orientation}\}/\sim$
- $(E,\iota) \sim (E',\iota')$ if there exists $\phi : E \to E'$ an isomorphism with $\phi \circ \iota = \iota' \circ \phi$

# The Vectorization Problem

- $SS_{\mathcal{O}}^{pr} := \{(E,\iota) : \iota$ a primitive $\mathcal{O}$-orientation$\}/\sim$
- $(E,\iota) \sim (E',\iota')$ if there exists $\phi : E \to E'$ an isomorphism with $\phi \circ \iota = \iota' \circ \phi$
- Given $(E,\iota) \in SS_{\mathcal{O}}^{pr}$,$[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$, define

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

Then there exists $K$-oriented isogeny $\varphi_{\mathfrak{a}}$ with kernel $E[\mathfrak{a}]$. This gives an action of $\mathrm{Cl}(\mathcal{O})$ on $SS_{\mathcal{O}}^{pr}$ by

$$[\mathfrak{a}] \cdot (E,\iota) = (E/E[\mathfrak{a}], \iota_{\mathfrak{a}}), \iota_{\mathfrak{a}} = \frac{1}{\deg \varphi_{\mathfrak{a}}} \varphi_{\mathfrak{a}} \circ \iota \circ \hat{\varphi}_{\mathfrak{a}}$$

# The Vectorization Problem

- The class group action is free. In general, it is not transitive, but at worst there are two orbits (Onuki, 2021; ACL+ 2024)

# The Vectorization Problem

- The class group action is free. In general, it is not transitive, but at worst there are two orbits (Onuki, 2021; ACL+ 2024)
- The vectorization problem:

$$\text{Given a fixed orbit } X \text{ in } SS_{\mathcal{O}}^{pr},\ (E, \iota), (E', \iota') \in X,$$

$$\text{find } [\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}) \text{ such that } [\mathfrak{a}] \cdot (E, \iota) = (E', \iota')$$

# The Vectorization Problem

- The class group action is free. In general, it is not transitive, but at worst there are two orbits (Onuki, 2021; ACL+ 2024)
- The vectorization problem:

$$\text{Given a fixed orbit } X \text{ in } SS_{\mathcal{O}}^{pr},\ (E,\iota),(E',\iota') \in X,$$

$$\text{find } [\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}) \text{ such that } [\mathfrak{a}] \cdot (E,\iota) = (E',\iota')$$

- Vectorization problems in the wild: e.g., the underlying hard problem in CSIDH

# Motivating Question

- SIDH no longer secure, as shown by Castryck and Decru (2023), Robert (2023), Maino and Martindale, and Maino-Martindale-Panny-Pope-Wesolowski (2023)

# Motivating Question

- SIDH no longer secure, as shown by Castryck and Decru (2023), Robert (2023), Maino and Martindale, and Maino-Martindale-Panny-Pope-Wesolowski (2023)
- The upshot: for a given secret isogeny $\phi : E \to E'$, once we know
  (i) the degree, $d$, of $\phi$
  (ii) action of $\phi$ on $E[m]$ for $m$ sufficiently smooth and $m^2 > 4d$,

  we know $\phi$

# Motivating Question

- SIDH no longer secure, as shown by Castryck and Decru (2023), Robert (2023), Maino and Martindale, and Maino-Martindale-Panny-Pope-Wesolowski (2023)
- The upshot: for a given secret isogeny $\phi : E \to E'$, once we know
  (i) the degree, $d$, of $\phi$
  (ii) action of $\phi$ on $E[m]$ for $m$ sufficiently smooth and $m^2 > 4d$,

  we know $\phi$
- Question (CHM+23): Can this attack be applied to instances of the vectorization problem?

# An Instructive Example (from CHM+ 23):

Assume: $E, E'$ defined over $\mathbb{F}_p$, both with primitive orientation by $\mathbb{Z}[\sqrt{-p}]$; $\phi : E \to E'$ a secret $\mathbb{F}_p$-rational isogeny with $\ker \phi = E[\mathfrak{a}]$; $\deg phi = d$ known; $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$. If we know $\phi$, we can efficiently recover $[\mathfrak{a}]$.

- With $m = \ell^r$, $(\ell, d) = 1$, $\ell$ a small prime splitting in $\mathbb{Q}(\sqrt{-p})$, there are bases $\{P, Q\}, \{P', Q'\}$ for $E[m], E'[m]$, respectively, and

$$P' = \lambda\phi(P), \quad Q' = \mu\phi(Q), \quad \lambda, \mu \in \mathbb{Z}/m\mathbb{Z}^*$$

# An Instructive Example (from CHM+ 23):

Assume: $E, E'$ defined over $\mathbb{F}_p$, both with primitive orientation by $\mathbb{Z}[\sqrt{-p}]$; $\phi : E \to E'$ a secret $\mathbb{F}_p$-rational isogeny with $\ker\phi = E[\mathfrak{a}]$; $\deg phi = d$ known; $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$. If we know $\phi$, we can efficiently recover $[\mathfrak{a}]$.

- With $m = \ell^r$, $(\ell, d) = 1$, $\ell$ a small prime splitting in $\mathbb{Q}(\sqrt{-p})$, there are bases $\{P, Q\}, \{P', Q'\}$ for $E[m], E'[m]$, respectively, and

$$P' = \lambda\phi(P), \quad Q' = \mu\phi(Q), \quad \lambda, \mu \in \mathbb{Z}/m\mathbb{Z}^*$$

- Properties of the $m$-Weil pairing $e_m(\cdot,\cdot)$ imply

$$e_m(P', P') = e_m(P, P)^{\lambda^2 d}$$

# An Instructive Example (from CHM+ 23):

Assume: $E, E'$ defined over $\mathbb{F}_p$, both with primitive orientation by $\mathbb{Z}[\sqrt{-p}]$; $\phi : E \to E'$ a secret $\mathbb{F}_p$-rational isogeny with $\ker \phi = E[\mathfrak{a}]$; $\deg phi = d$ known; $[\mathfrak{a}] \in \mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$. If we know $\phi$, we can efficiently recover $[\mathfrak{a}]$.

- With $m = \ell^r$, $(\ell, d) = 1$, $\ell$ a small prime splitting in $\mathbb{Q}(\sqrt{-p})$, there are bases $\{P, Q\}, \{P', Q'\}$ for $E[m], E'[m]$, respectively, and

$$P' = \lambda\phi(P), \quad Q' = \mu\phi(Q), \quad \lambda, \mu \in \mathbb{Z}/m\mathbb{Z}^*$$

- Properties of the $m$-Weil pairing $e_m(\cdot, \cdot)$ imply

$$e_m(P', P') = e_m(P, P)^{\lambda^2 d}$$

- Unfortunately, $e_m(P, P) = 1$

## Self-Pairings

- Search for pairings non-degenerate on a cyclic subgroup of $E$ compatible with oriented isogenies

# Self-Pairings

- Search for pairings non-degenerate on a cyclic subgroup of $E$ compatible with oriented isogenies
- CHM+ (2023) construct such pairings. This yields efficient attacks on the vectorization problem when
  (i) The degree of the secret isogeny is known
  (ii) The discriminant $\Delta_{\mathcal{O}}$ of the primitive order contains a large smooth square factor
  (iii) To perform the necessary computations, may need to significantly extend the base field

  (N.B. work in preparation by CDM+ appears to remove condition (ii))

# Sesquilinear Pairings

Can be defined purely formally, thus even for curves without CM ("Sesquilinear Pairings on Elliptic Curves", Stange, 2024)

## First steps

- Given an imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$, let $\rho$ be the left-regular representation of $\mathcal{O}$ acting on basis $\{1, \tau\}$:

$$\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \alpha = a + c\tau, \alpha\tau = b + d\tau$$

# Sesquilinear Pairings

Can be defined purely formally, thus even for curves without CM ("Sesquilinear Pairings on Elliptic Curves", Stange, 2024)

## First steps

- Given an imaginary quadratic order $\mathcal{O} = \mathbb{Z}[\tau]$, let $\rho$ be the left-regular representation of $\mathcal{O}$ acting on basis $\{1, \tau\}$:

$$\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \iff \alpha = a + c\tau, \alpha\tau = b + d\tau$$

- Define action of $\mathcal{O}$ on $(\mathbb{F}^*)^{\times 2}$ by $(x, y)^\alpha = (x^a y^b, x^c y^d)$

## Sesquilinear Pairings

Let $E/\mathbb{F}$ have CM by $\mathcal{O}$. Given $\alpha \in \mathcal{O}$, we construct a pairing

$$\widehat{T}_\alpha^\tau : E[\overline{\alpha}](\mathbb{F}) \times E(\mathbb{F})/[\alpha]E(\mathbb{F}) \to (\mathbb{F}^*)^{\times 2}/((\mathbb{F}^*)^{\times 2})^\alpha$$

as follows:

With $\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$,

$$\alpha = a + c\tau, \alpha\tau = b + d\tau, \overline{\alpha} = d - c\tau, \overline{\alpha}\tau = -b + a\tau$$

- Take $P \in E[\overline{\alpha}]$, define functions $f_{P,1}, f_{P,2}$ such that

$$\mathrm{div}(f_{P,1}) = a([-\tau]P) + b(P) - (a+b)(\infty)$$
$$\mathrm{div}(f_{P,2}) = c([-\tau]P) + d(P) - (c+d)(\infty)$$

# Sesquilinear Pairings

- Define for $Q \in E(\mathbb{F})$,

  $$D_{Q,1} = ([-\tau]Q + [-\tau]R) - ([-\tau]R), \quad D_{Q,2} = (Q + R) - (R).$$

  with $R$ chosen so that the supports of $\mathrm{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair $i$, $j$

# Sesquilinear Pairings

- Define for $Q \in E(\mathbb{F})$,

$$D_{Q,1} = ([-\tau]Q + [-\tau]R) - ([-\tau]R), \quad D_{Q,2} = (Q + R) - (R).$$

with $R$ chosen so that the supports of $\mathrm{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair $i$, $j$

- Then $\widehat{T}_\alpha^\tau(P, Q) =$

$$(f_{P,1}(D_{Q,1}), f_{P,2}(D_{Q,1}))\,\overline{(f_{P,1}(D_{Q,2}), f_{P,2}(D_{Q,2}))}^{\tau}$$

# Sesquilinear Pairings

- Define for $Q \in E(\mathbb{F})$,

  $$D_{Q,1} = ([-\tau]Q + [-\tau]R) - ([-\tau]R), \quad D_{Q,2} = (Q + R) - (R).$$

  with $R$ chosen so that the supports of $\mathrm{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair $i$, $j$
- Then $\widehat{T}_{\alpha}^{\tau}(P, Q) =$

  $$(f_{P,1}(D_{Q,1}), f_{P,2}(D_{Q,1}))\,\overline{(f_{P,1}(D_{Q,2}), f_{P,2}(D_{Q,2}))}^{\tau}$$
- Unwinding the definitions, this turns out to be a somewhat natural extension of the Tate pairing; $\widehat{T}_{\alpha}^{\tau}(P, Q) = f_P(D_Q)$ for $f_P = f_{P,1} f_{P,2}^{\tau}$, $D_Q = D_{Q,1} + \tau \cdot D_{Q,2}$ (see Stange, 2024)

# Sesquilinear Pairings

Theorem (Stange 2024):

The pairing above is well-defined and satisfies

- **Sesquilinearity:** For $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_{\alpha}^{\tau}([\gamma]P, [\delta]Q) = \widehat{T}_{\alpha}^{\tau}(P, Q)^{\overline{\gamma}\delta}.$$

# Sesquilinear Pairings

Theorem (Stange 2024):

The pairing above is well-defined and satisfies

- **Sesquilinearity:** For $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_\alpha^\tau([\gamma]P, [\delta]Q) = \widehat{T}_\alpha^\tau(P, Q)^{\overline{\gamma}\delta}.$$

- **Compatibility:** Let $\phi : E \to E'$ be an isogeny between curves with CM by $\mathcal{O}$ and satisfying $[\alpha] \circ \phi = \phi \circ [\alpha]$. Then for $P \in E[\overline{\alpha}](\mathbb{F})$ and $Q \in E(\mathbb{F})$,

$$\widehat{T}_\alpha^\tau(\phi P, \phi Q) = \widehat{T}_\alpha^\tau(P, Q)^{\deg \phi}.$$

## Sesquilinear Pairings

Theorem (continued):

- **Non-degeneracy:** Let $\alpha \in \mathcal{O}$ be coprime to $\mathrm{char}(\mathbb{F})$ and the discriminant of $\mathcal{O}$. Let $N = N(\alpha)$. Suppose $\mathbb{F}$ contains the $N$-th roots of unity. Suppose there exists $P \in E[N](\mathbb{F})$ such that $\mathcal{O}P = E[N] = E[N](\mathbb{F})$. Then

$$\widehat{T}_\alpha^\tau : E[\overline{\alpha}](\mathbb{F}) \times E(\mathbb{F})/[\alpha]E(\mathbb{F}) \to (\mathbb{F}^*)^{\times 2}/((\mathbb{F}^*)^{\times 2})^\alpha,$$

is non-degenerate. Furthermore, if $P$ has annihilator $\overline{\alpha}\mathcal{O}$, then $T_\alpha(P, \cdot)$ is surjective; and if $Q$ has annihilator $\alpha\mathcal{O}$, then $T_\alpha(\cdot, Q)$ is surjective.

# Sesquilinear Pairings

These pairings are efficiently computable via a Miller-style algorithm (Algorithm 5.7, Stange, 2024)

Similar to the Tate pairing, a final exponentiation gives values in the roots of unity:

$$(\overline{\mathbb{F}}^*)/(\overline{\mathbb{F}}^*)^\alpha \to \mu_{N(\alpha)}^{\times 2} \subseteq (\overline{\mathbb{F}}^*)^{\times 2}, \quad x \mapsto x^{(q-1)\alpha^{-1}}.$$

# Sesquilinear Pairings

**Key idea:**

Sesquilinear pairings respect $\mathcal{O}$-module structure, not merely $\mathbb{Z}$-module structure. This yields new instances of non-trivial self-pairings.

# Sesquilinear Pairings

Recall that in the statement of non-degeneracy of $\widehat{T}_\alpha^\tau$, one condition is that $E[N]$ is a cyclic $\mathcal{O}$-module, where $N = N(\alpha)$.

- The following is a straightforward extension of results of (Lenstra, 1996)

# Sesquilinear Pairings

Recall that in the statement of non-degeneracy of $\widehat{T}_\alpha^\tau$, one condition is that $E[N]$ is a cyclic $\mathcal{O}$-module, where $N = N(\alpha)$.

- The following is a straightforward extension of results of (Lenstra, 1996)
- Theorem (M., Stange): $E/\mathbb{F}$, $K$ imaginary quadratic, $\mathcal{O} \subset K$, $E$ $\mathcal{O}$-oriented, $f = [\mathcal{O}' : \mathcal{O}]$, $\mathcal{O}'$ primitive orientation. $E[m]$ cyclic $\mathcal{O}$-module iff $(m, f) = 1$.

# Sesquilinear Pairings

So, there many instances where $\widehat{T}_\alpha^\tau$ is non-degenerate. This in turn yields non-degenerate self-pairings.

## Theorem (M., Stange):

Let $E$ be an elliptic curve oriented by $\mathcal{O} = \mathbb{Z}[\tau]$. Let $m$ be coprime to the discriminant $\Delta_{\mathcal{O}}$. Let $\mathbb{F}$ be a finite field containing the $m$-th roots of unity. Suppose $E[m] = E[m](\mathbb{F})$. Let $P$ have order $m$. Let $s$ be the maximal divisor of $m$ such that $E[s] \subseteq \mathcal{O}P$. Then the multiplicative order $m'$ of $\widehat{T}_m^\tau(P, P)$ satisfies $s \mid m' \mid 2s^2$.

In particular, if $\mathcal{O}P = E[m]$, then $s = m$ and the self-pairing has order $m$. If $\mathcal{O}P = \mathbb{Z}P$, then $s = 1$, and in fact, in this case, the self-pairing is trivial.

# Sesquilinear Pairings

## Proof (Sketch):

Properties of the sesquilinear pairing and assumptions on $s$ imply

$$\widehat{T}_m^\tau([s]P,[s]P)^{k^2} = \widehat{T}_m^\tau([s]P,[s]P)^{N(\lambda)}$$

so $N(\lambda)$ a square modulo order of $\widehat{T}_m^\tau([s]P,[s]P)$ for all $\lambda \in \mathcal{O}$.
Coprimality of $m$ with $\Delta_{\mathcal{O}}$ then implies order at most $2s^2$.
Conversely, for $t = m/s$,

$$\widehat{T}_m^\tau(P,Q)^t = \widehat{T}_m^\tau(P,P)^{ta+b\lambda}$$

for an appropriate choice for $Q$. So order of the self-pairing is at least $s$.

# Sesquilinear Pairings

Even when $m \mid \Delta_{\mathcal{O}}$, the sesquilinear pairing remains non-degenerate provided $m$ is not a divisor of the relative conductor:

$$\widehat{T}_m^{\tau} = \left(f_{P,1}(D_{Q,1}), f_{P,2}(D_{Q,1})\right)\left(f_{P,1}(D_{Q,2}), f_{P,2}(D_{Q,2})\right)^{\overline{\tau}} =$$

$$\left(f_{P,1}(D_{Q,1})f_{P,1}(D_{Q,2})^{Tr(\tau)}f_{P,2}(D_{Q,2})^{N(\tau)}, f_{P,2}(D_{Q,1})f_{P,1}(D_{Q,2})^{-1}\right) =$$

$$\left(t_m(P,Q)^{2N(\tau)}t_m([-\tau]P,Q)^{Tr(\tau)},\ t_m([\tau-\overline{\tau}]P,Q)\right)$$

with $t_m(P,Q)$ the $m$-Tate-Lichtenbaum pairing. Choosing $\tau = f\sqrt{d_K}$, non-degeneracy follows from non-degeneracy of the $m$-Tate-Lichtenbaum pairing.

# Computational Assumptions

- Efficient = polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ ($q$ the cardinality of base field where $E[m]$ fully rational)

# Computational Assumptions

- Efficient = polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ ($q$ the cardinality of base field where $E[m]$ fully rational)
- Having an $\mathcal{O}$-oriented curve means having an explicit orientation; given $\alpha \in \mathcal{O}$, can compute its action $[\alpha]$ on a point $P$ on $E$ efficiently

# Computational Assumptions

- Efficient $=$ polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ ($q$ the cardinality of base field where $E[m]$ fully rational)
- Having an $\mathcal{O}$-oriented curve means having an explicit orientation; given $\alpha \in \mathcal{O}$, can compute its action $[\alpha]$ on a point $P$ on $E$ efficiently
- Degree $d$ of hidden isogeny $\phi$ is known

# Computational Assumptions

- Efficient = polynomial in size of input, i.e., polynomial in $\log m$ (the torsion) and $\log q$ ($q$ the cardinality of base field where $E[m]$ fully rational)
- Having an $\mathcal{O}$-oriented curve means having an explicit orientation; given $\alpha \in \mathcal{O}$, can compute its action $[\alpha]$ on a point $P$ on $E$ efficiently
- Degree $d$ of hidden isogeny $\phi$ is known
- $m$ is coprime to the characteristic $p$ of the given field $\mathbb{F}$, and $m$ is smooth, meaning that its factors are polynomial in size, so that discrete logarithms in $\mu_m$ or $E[m]$ are computable in polynomial time. In particular, we can efficiently write any element of $E[m]$ in terms of a given basis

# Extending Prior Attacks

A slight modification of the sesquilinear pairing:

$$T'_m(P, Q) = (t_m([\tau]P, Q), t_m(P, Q))$$

This pairing remains non-degenerate whenever $E[m]$ is a cyclic $\mathcal{O}$-module, bilinear, compatible with $\mathcal{O}$-oriented isogenies. It yields the following result

Theorem (M., Stange):

Suppose $\phi : E \to E'$ of degree $d$, $m \mid \Delta_{\mathcal{O}}$, coprime to $d$, and chosen so that there are only polynomially many square roots of 1 modulo $m$. Suppose $P \in E[m]$ and $P' \in E'[m]$ such that $\mathcal{O}P = E[m]$, $\mathcal{O}P' = E'[m]$. Then there exists an efficiently computable point $Q \in E[m]$ of order $m$ such that a subset $S \subset E'[m]$ of polynomial size containing $\phi(Q)$ can be computed in polynomially many operations in the field of definition of $E[m]$.

# Extending Prior Attacks

- With knowledge of $\phi(Q)$ for an order $m$ point $Q$, $\mathcal{O}$-module structure of $E[m]$ and $\phi$ an $\mathcal{O}$-oriented isogeny yield knowledge of $\phi$ on $E[m]$.

# Extending Prior Attacks

- With knowledge of $\phi(Q)$ for an order $m$ point $Q$, $\mathcal{O}$-module structure of $E[m]$ and $\phi$ an $\mathcal{O}$-oriented isogeny yield knowledge of $\phi$ on $E[m]$.
- If $m$ a smooth square with $m > 4d$, reduces to SIDH attack.

# Extending Prior Attacks

- With knowledge of $\phi(Q)$ for an order $m$ point $Q$, $\mathcal{O}$-module structure of $E[m]$ and $\phi$ an $\mathcal{O}$-oriented isogeny yield knowledge of $\phi$ on $E[m]$.
- If $m$ a smooth square with $m > 4d$, reduces to SIDH attack.
- Work in preparation (CDM+24) appears to remove restriction that $m$ be a square.

# Extending Prior Attacks

- With knowledge of $\phi(Q)$ for an order $m$ point $Q$, $\mathcal{O}$-module structure of $E[m]$ and $\phi$ an $\mathcal{O}$-oriented isogeny yield knowledge of $\phi$ on $E[m]$.
- If $m$ a smooth square with $m > 4d$, reduces to SIDH attack.
- Work in preparation (CDM+24) appears to remove restriction that $m$ be a square.
- By exploiting $\mathcal{O}$-module structure, computations take place over field of definition of $E[m]$ instead of $E[m^2]$. This yields polynomial-time attacks on additional instances of the vectorization problem.

# Extending Prior Attacks

Proof (Sketch, for *m* odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo $m$; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$

# Extending Prior Attacks

Proof (Sketch, for $m$ odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo $m$; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$
- $T'_m(P, P)^{\deg \phi} = T'_m(P', P')^{N(\lambda)}$

# Extending Prior Attacks

Proof (Sketch, for $m$ odd):

- $\exists \tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo $m$; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$
- $T'_m(P, P)^{\deg \phi} = T'_m(P', P')^{N(\lambda)}$
- $\lambda \equiv a + b\tau$ modulo $m$, $N(\lambda) \equiv a^2 \pmod{m'}$, so $\phi[\tau]P = [a]\tau P'$ for some $a$

# Extending Prior Attacks

Proof (Sketch, for $m$ odd):

- $\exists\tau \in \mathcal{O}$ s.t. $\mathbb{Z}[\tau] \equiv \mathcal{O}$ modulo $m$; $Tr(\tau) \equiv N(\tau) \equiv 0 \pmod{m}$
- $T_m'(P, P)^{\deg\phi} = T_m'(P', P')^{N(\lambda)}$
- $\lambda \equiv a + b\tau$ modulo $m$, $N(\lambda) \equiv a^2 \pmod{m'}$, so $\phi[\tau]P = [a]\tau P'$ for some $a$
- Our assumptions imply set of possible values of $a$ is efficiently computable and of polynomial size

# Extending Prior Attacks

Example (adapted from Castryck):

$E : y^2 = x^3 + x$, $p = 4 \cdot 3^r - 1$. Then $j(E) = 1728$ and $E$ is supersingular. With $\pi_p$ the Frobenius endomorphism, $[i] : (x, y) \mapsto (-x, iy)$,

$$\tau := \frac{i + \pi_p}{2} \in \mathrm{End}(E).$$

$N(\tau) = 3^r$ and $Tr(\tau) = 0$. Let $\mathcal{O} = \mathbb{Z}[\tau]$, having $N(\tau) \mid \Delta_{\mathcal{O}}$. Let $m = 3^r$. Then $m \mid \Delta_{\mathcal{O}}$. $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/4 \cdot 3^r\mathbb{Z})^2$, so $E[3^r] \subset E(\mathbb{F}_{p^2})$. Provided $m > 4d$, all pairings computations take place in $E(\mathbb{F}_{p^2})$.

# Extending Prior Attacks

- This is in contrast to methods of CHM+23, where a base change to field of definition of $E[3^{2r}]$ is required.

# Extending Prior Attacks

- This is in contrast to methods of CHM+23, where a base change to field of definition of $E[3^{2r}]$ is required.
- This degree grows exponentially with $r$ (recall that polynomial runtime means polynomial in $\log m$ and $\log q$, $q$ cardinality of the field of definition of $E[m]$).

# Modular Isogeny Problems

- Definition (FFP, 2024): Let $E$ be an elliptic curve over a finite field $\mathbb{F}$ of characteristic $p$ and $m$ be a positive integer coprime to $p$. Let $\Gamma$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. A $\Gamma$*-level structure of level $m$ on $E$* is a $\Gamma$-orbit of a basis of $E[m]$.

# Modular Isogeny Problems

- Definition (FFP, 2024): Let $E$ be an elliptic curve over a finite field $\mathbb{F}$ of characteristic $p$ and $m$ be a positive integer coprime to $p$. Let $\Gamma$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. A *$\Gamma$-level structure of level $m$ on $E$* is a $\Gamma$-orbit of a basis of $E[m]$.
- For elliptic curves $E, E'$ with $\Gamma$-level structures of level $m$, $\phi : E \to E'$ respects the level structure if $\phi$ maps the specified $\Gamma$-orbit for $E[m]$ to the specified $\Gamma$-orbit for $E'[m]$.

# Modular Isogeny Problems

- Definition (FFP, 2024): Let $E$ be an elliptic curve over a finite field $\mathbb{F}$ of characteristic $p$ and $m$ be a positive integer coprime to $p$. Let $\Gamma$ be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. A *$\Gamma$-level structure of level $m$ on $E$* is a $\Gamma$-orbit of a basis of $E[m]$.
- For elliptic curves $E, E'$ with $\Gamma$-level structures of level $m$, $\phi : E \to E'$ respects the level structure if $\phi$ maps the specified $\Gamma$-orbit for $E[m]$ to the specified $\Gamma$-orbit for $E'[m]$.
- Many proposed isogeny-based protocols are instances of a *modular isogeny problem*: given an isogeny $\phi : E \to E'$ that respects a known $\Gamma$-level structure of level $m$, determine $\phi$.

# Modular Isogeny Problems

Examples:

- SIDH: $\Gamma = \{1\}$, so image of $\phi$ on a basis $\{P, Q\}$ for $E[m]$ is known.

# Modular Isogeny Problems

## Examples:

- SIDH: $\Gamma = \{1\}$, so image of $\phi$ on a basis $\{P, Q\}$ for $E[m]$ is known.
- $\mathrm{SIDH}_1$:

$$\Gamma = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\},$$

so image of $\phi$ on single basis point $P$ is known

# Modular Isogeny Problems

## Examples:

- SIDH: $\Gamma = \{1\}$, so image of $\phi$ on a basis $\{P, Q\}$ for $E[m]$ is known.
- $\text{SIDH}_1$:

$$\Gamma = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \right\},$$

  so image of $\phi$ on single basis point $P$ is known
- Diagonal SIDH:

$$\Gamma = \left\{ \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \right\},$$

  so image of subgroups $\langle P \rangle, \langle Q \rangle$ are known, $\{P, Q\}$ a basis for $E[m]$

# Modular Isogeny Problems

- Work of De Feo, Fouotsa, and Panny (2024) categorizes many current isogeny-based protocols by their implicit level structure.

# Modular Isogeny Problems

- Work of De Feo, Fouotsa, and Panny (2024) categorizes many current isogeny-based protocols by their implicit level structure.
- The authors establish several reductions between various modular isogeny problems, including the following:

# Modular Isogeny Problems

- Work of De Feo, Fouotsa, and Panny (2024) categorizes many current isogeny-based protocols by their implicit level structure.
- The authors establish several reductions between various modular isogeny problems, including the following:
- Theorem (FFP, 2024): With the degree $d$ of $\phi : E \to E'$ known and $m \in \mathbb{Z}$ such that $m$ has a large smooth square factor, the modular isogeny problem $\mathrm{SIDH}_1$ of level $m$ reduces to the modular isogeny problem SIDH of level $O(\sqrt{m})$

# Modular Isogeny Problems

### Theorem (M., Stange):

Let $E$ and $E'$ be $\mathcal{O}$-oriented supersingular curves over $\overline{\mathbb{F}}_p$, upon which we can efficiently compute the action of endomorphisms from $\mathcal{O}$. Assume that $m$ coprime to the discriminant. Assume also that $E[m]$ is a cyclic $\mathcal{O}$-module, and that the hidden isogeny $\phi : E \to E'$ has known degree $d$ coprime to $m$ and is compatible with the $\mathcal{O}$-orientations. Then the problem $\mathrm{SIDH}_1$ of level $m$ to find $\phi$ reduces, in a polynomial number of operations in the field of definition of $E[m]$, to SIDH of level $m$ on the same curve $E$ and same $\phi$.

# Modular Isogeny Problems

Theorem (M., Stange):

Suppose $E$ and $E'$ are $\mathcal{O}$-oriented. Let $m > 4 \deg \phi$ be a smooth integer such that modulo $m$, 1 has polynomially many square roots. Then Diagonal SIDH with known degree for an oriented isogeny $\phi : E \to E'$ is solvable in polynomial time, provided $\mathcal{O}P = E[m]$ or $\mathcal{O}Q = E[m]$.

Thank you!