Extending class group action attacks via sesquilinear pairings

Joseph Macula[1[0000−1111−2222−3333]] and Katherine E. Stange[1[0000−0003−2294−0397]]

University of Colorado Boulder, USA
Joseph.Macula@colorado.edu,kstange@math.colorado.edu

Abstract. We introduce a new tool for the study of isogeny-based cryptography, namely pairings which are sesquilinear (conjugate linear) with respect to the $\mathcal{O}$-module structure of an elliptic curve with CM by an imaginary quadratic order $\mathcal{O}$. We use these pairings to study the security of problems based on the class group action on collections of oriented ordinary or supersingular elliptic curves. This extends work of [4] and [13].

Keywords: Isogeny-based cryptography · Pairings · Elliptic Curves.

1 Introduction

The use of isogeny graphs in cryptography dates to [8,10,24]. The latter proposals were for public-key cryptography based on an ordinary isogeny graph. In particular, the class group $\mathrm{Cl}(\mathcal{O})$ of an order $\mathcal{O}$ in an imaginary quadratic field K acts on the set of ordinary elliptic curves over $\overline{\mathbb{F}}_p$ with CM by $\mathcal{O}$. For efficiency, CSIDH was proposed [6], making use of supersingular curves with an action by the class group of the Frobenius field. More recently, this was generalized to OSDIH [9], making use of other imaginary quadratic fields in the endomorphism algebra. This paper concerns *oriented* elliptic curves, which refers to attaching the data of an embedding of a particular imaginary quadratic order $\mathcal{O}$ into the endomorphism ring. All these public-key proposals are examples of class group actions on oriented curves.

The security of these schemes relies on variants of the Diffie-Hellman problem for the class group action. The security of these problems has drawn a great deal of interest, and not all instances of the problem have so far proven to be secure. If the class group is even, the decisional Diffie-Hellman problem is broken by the use of genus theory [7,5]. These papers make use of the Weil and Tate pairings to compute certain associated characters. More recently, [4] makes use of generalizations of Weil and Tate pairings to break certain instances of the class group action problem (i.e., determining which class group element takes one given oriented curve to another) when the discriminant has a large smooth square factor and the degree is known. Pairings have also appeared in the study of oriented elliptic curves in [17], to navigate the isogeny graph.

The attacks in [4] use pairings to reduce a hidden isogeny problem with known degree for the class group action to the SIDH problem recently broken using higher dimensional abelian varieties [2,20,23]. In short, if the degree of a secret isogeny $\phi : E \to E'$ is known, and it is known that $\phi P \in \mathbb{Z}P'$ for $P \in E$ and $P' \in E'$, then we can make use of a relationship of the form

$$\langle P, P\rangle^{\deg \phi} = \langle \phi P, \phi P\rangle = \langle kP', kP'\rangle = \langle P', P'\rangle^{k^2}$$

by solving a discrete logarithm to obtain the relationship $k^2 \equiv \deg \phi \pmod{m}$, and thereby solve for k. With this, we (essentially) obtain the image ϕP of P, which is the type of information provided in the SIDH problem. The classical SIDH problem (for which we now have efficient methods) requires the image of two basis points, and this provides only one. To close the gap, [4] uses results of [13] which reduce SIDH_1, in which only one torsion point is provided, to classical SIDH, provided the order of the point is square. More recent work presented but not yet available [3] uses pairings to generalize the SIDH attacks so that torsion images of any sufficiently large subgroup suffice.

These attacks require that the degree of the secret isogeny is known, which is the case in some implementations; see [4] for some details. Furthermore, in [13, Lemma 14], the authors give a heuristic reduction from the group action problem to the same problem with known degree. **In this paper we will assume throughout that the degree of the secret isogeny is known.**

In this paper we introduce a new tool for understanding these results and pushing such attacks further. In [26], certain new generalized pairings $\widehat{W}$ and $\widehat{T}$ (generalizing the usual Weil and Tate pairings) are defined, which are $\mathcal{O}$-sesquilinear, meaning that

$$\langle \alpha x, \beta y\rangle = \langle x, y\rangle^{\overline{\alpha}\beta}$$

for $\alpha, \beta \in \mathcal{O}$. In particular, they take values in an $\mathcal{O}$-module formed by extending scalars from the usual domain $\mathbb{F}_q^*$.

In particular, we can now assume only that $\phi P \in \mathcal{O}P'$ and obtain a relationship

$$\langle P, P\rangle^{\deg \phi} = \langle \phi P, \phi P\rangle = \langle \lambda P', \lambda P'\rangle = \langle P', P'\rangle^{N(\lambda)},$$

where $\lambda \in \mathcal{O}$. The new pairings are amenable to a Miller-type effective algorithm for their computation, and carry all the useful properties of the Weil and Tate pairings, especially compatibility with $\mathcal{O}$-oriented isogenies.

The paper [4] provides a taxonomy of known generalized pairings, but all of these are only $\mathbb{Z}$-bilinear with image in $\mathbb{F}_q^*$.

One important difference of these sesquilinear pairings from the generalized pairings previously considered is their non-degeneracy. In [4], there is a classification theorem for *cyclic self-pairings*, namely homogeneous degree-2 functions $f_m : C \to \mu_m$ where C is a cyclic subgroup of $E[m]$ whose image under f_m spans μ_m. As shown in [4], these can often be formed from generalizations of the classical reduced m-Tate pairing; for a simple such construction, see [4, Example 4.4]. In particular, such functions are helpful when they are compatible with oriented isogenies ϕ, meaning $f_m \circ \phi = f_m^{\deg \phi}$. They essentially show that compatible cyclic self-pairings can only be non-trivial for m dividing the discriminant $\Delta_{\mathcal{O}}$ of

$\mathcal{O}$. This limits the applicability of their attacks on the class group action to situations where the discriminant has a good factorization. We demonstrate that by extending to $\mathcal{O}$-sesquilinear pairings, whose domain is not $\mathbb{Z}$-cyclic but instead $\mathcal{O}$-cyclic, we obtain many more non-trivial self-pairings to work with.

The use of these new $\mathcal{O}$-sesquilinear pairings offers several clarifying conceptual advantages, and partially answers several of the open problems posed in [4]. However, they are not a magic bullet: we show (Theorem 7) that the computation of these pairings is essentially equivalent to the computation of the $\mathcal{O}$-orientation, provided discrete logarithms are efficient in μ_m (for example, if m is smooth).

Conceptual contributions.

1. We introduce the new $\mathcal{O}$-sesquilinear pairings $\widehat{W}$ and $\widehat{T}$ in the cryptographic context.
2. We show that these pairings give rise to many non-degenerate $\mathcal{O}$-cyclic self-pairings, without a requirement that m divide the discriminant (Theorem 6).
3. We characterize elliptic curves for which $E[m]$ is a cyclic $\mathcal{O}$-module (Theorem 3): $E[m]$ is $\mathcal{O}$-cyclic if and only if the $\mathcal{O}$-orientation is m-primitive.
4. We show an equivalence between computation of an $\mathcal{O}$-orientation and the computation of $\mathcal{O}$-sesquilinear pairings for m smooth (Theorem 7).
5. Corollary 1 and Theorem 9 (described in more detail below) provide evidence for a trade-off between the amount of known level structure of a secret isogeny $\phi : E \to E'$ of degree d and how much of the endomorphism rings of E and E' we need to represent to find ϕ. As shown in [27], the fixed-degree isogeny problem with full level structure is equivalent to finding a representation of the full endomorphism ring of E and E', while [2,20,23] show that the fixed-degree isogeny problem with minimal level structure requires no knowledge of even a partial representation of the endomorphism rings of E and E'. As described in *Cryptographic contributions* items 2 and 3 below, knowledge of an intermediate level structure can be combined with a representation of only "half" of the endomorphism rings of E and E', to provide attacks on hidden isogenies of known degree. See also the work in [13], which explores varying amounts of level structure.

Cryptographic contributions.

1. We extend the applicability of the (sometimes polynomial) attacks from [4] on the class group action problem (Section 8). These attacks run for smooth m dividing the discriminant. We recover these attacks using the new pairings in a slightly different way, with the advantage that our pairing computations do not require going to a large field extension. This partially addresses one of the open questions of [4, Section 7]. Example 3 gives an explicit situation in which the reach of attacks is extended.
2. We demonstrate a pairing-based reduction from SIDH_1 to SIDH in the oriented situation for $E[m]$, where m is smooth and coprime to the discriminant

(Theorem 9), resulting in an attack when $m^2 > \deg \phi$. This partially addresses the first and second open problems in [4, Section 7]. Existing attacks on SIDH_1 (which apply without orientation information) require $m > \deg \phi$.
3. We reduce the hard problem underlying FESTA [1] to finding an orientation of the secret isogeny $\phi : E \to E'$ (i.e. an orientation of both curves and the isogeny between them) (Corollary 1). This follows from an attack on the Diagonal SIDH Problem (Theorem 10).
4. We show how these pairings, using orientation information, easily reveal *partial* information on the image of a torsion point P of order m for m smooth (Theorem 8). This results in an algorithm to break CSIDH or other class-group-based schemes in square root of exponential time by running the SIDH attack on $\sqrt{m}$ candidate m-torsion points as images under ϕ (Remark 4).
5. Our results should be considered a cautionary tale for the design of decisional problems based on torsion point images, such as in [21], since the possible images of torsion points is restricted. We discuss this in Remark 5.
6. In the supersingular case, we demonstrate a method of finding the secret isogeny in the presence of two independent known orientations (which amounts to an explicit subring of the endomorphism ring of rank 4), provided the secret isogeny is oriented for both orientations. This is not a surprise, as this problem could be solved by the KLPT algorithm if the endomorphisms are obtained by walking the graph (see [12], and also [18,27]), but it provides a new method via a simple reduction to the SIDH problem. (Section 9.)

2 Background

2.1 Notations.

We study elliptic curves, typically denoted E, E' etc., defined over finite fields, denoted by $\mathbb{F}$ in general. Denote an algebraic closure of $\mathbb{F}$ by $\bar{\mathbb{F}}$. The identity on E is denoted $\mathcal{O}_E$, and $\mathrm{End}(E)$ is the endomorphism ring over $\overline{\mathbb{F}}$. We study imaginary quadratic fields, denoted K in general, and orders in such fields, denoted by $\mathcal{O}$, $\mathcal{O}'$ etc. Greek letters typically denote elements of the orders. When considering the action of an element $\alpha \in \mathcal{O}$ on a point P, we write $[\alpha]P$. The Greek letter ϕ always refers to an isogeny. For ease of notation, we write ϕP instead of $\phi(P)$. Throughout the paper, we write μ_m for the copy of μ_m in a finite field.

2.2 Orientations.

We study $\mathcal{O}$-*oriented* elliptic curves over finite fields, which are curves together with the information of an embedding $\iota : \mathcal{O} \to \mathrm{End}(E)$. This extends to an embedding of the same name, $\iota : K \to \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}(E)$, and the $\mathcal{O}$-orientation is called *primitive* if $\iota(K) \cap \mathrm{End}(E) = \mathcal{O}$. If the index $[\iota(K) \cap \mathrm{End}(E) : \iota(\mathcal{O})]$ is coprime to n, we say the orientation is n-*primitive*. Given an $\mathcal{O}$-orientation, there is a unique $\mathcal{O}' \supseteq \mathcal{O}$ for which ι becomes a $\mathcal{O}'$-primitive orientation, namely

$\mathcal{O}' = \iota(K) \cap \mathrm{End}(E)$. Given an elliptic curve E with an $\mathcal{O}$-orientation, we define the *relative conductor* of $\mathcal{O}$ to be the index $[\mathcal{O}' : \mathcal{O}]$, for which the orientation is $\mathcal{O}'$-primitive.

If $\phi : E \to E'$ is an isogeny between two $\mathcal{O}$-oriented elliptic curves (E, ι) and (E', ι') is such that $\phi \circ \iota(\alpha) = \iota'(\alpha) \circ \phi$ for all $\alpha \in \mathcal{O}$, then we say that ϕ is an oriented isogeny. Throughout the paper, we will generally fix a single $\mathcal{O}$-orientation for any curve, so we will often drop the ι, writing simply $[\alpha]$ for $\iota(\alpha)$, writing $\mathcal{O} \subseteq \mathrm{End}(E)$, and characterizing oriented isogenies as those for which $\phi \circ [\alpha] = [\alpha] \circ \phi$. This saves on notation.

2.3 Computational assumptions

With regards to computations, we use the word *efficient* to mean polynomial time in the size of the input. Throughout the paper, when we assume that if we are given an $\mathcal{O}$-oriented elliptic curve, we mean that we are given an explicit orientation, and that, in particular that, given an element $\alpha \in \mathcal{O}$, we can compute its action $[\alpha]$ on a point P on E efficiently.

We assume throughout that the degree of the hidden isogeny is known.

We assume that m is smooth, meaning that its factors are polynomial in size, so that discrete logarithms in μ_m or $E[m]$ are computable in polynomial time. In particular, we can write any element of $E[m]$ in terms of a given basis.

2.4 The Tate-Lichtenbaum Frey-Rück Pairing.

We review the definition and basic properties of the Tate-Lichtenbaum pairing.

Definition 1. *Let $m > 1$ be an integer. Let E be an elliptic curve defined over a field $\mathbb{F}$ (assumed finite in this paper). Suppose that $P \in E(\mathbb{F})[m]$. Choose divisors D_P and D_Q of disjoint support such that $D_P \sim (P) - (\mathcal{O})$ and $D_Q \sim (Q) - (\mathcal{O})$. Then $mD_P \sim 0$, hence there is a function f_P such that $\mathrm{div}(f_P) = mD_P$. The Tate-Lichtenbaum pairing*

$$t_m : E(\mathbb{F})[m] \times E(\mathbb{F})/mE(\mathbb{F}) \to \mathbb{F}^*/(\mathbb{F}^*)^m$$

is defined by

$$t_m(P, Q) = f_P(D_Q).$$

The standard properties of the Tate pairing are as follows. Proofs can be found in many places, for example [22] and [4, Sec 3.2].

Proposition 1. *Definition 1 is well-defined, and has the following properties:*

1. *Bilinearity: for $P, P' \in E(\mathbb{F})[m]$ and $Q, Q' \in E(\mathbb{F})$*

$$\begin{aligned} t_m(P + P', Q) =& t_m(P, Q) t_m(P', Q), \\ t_m(P, Q + Q') =& t_m(P, Q) t_m(P, Q'). \end{aligned}$$

2. *Non-degeneracy: Let $\mathbb{F}$ be a finite field containing the m-th roots of unity μ_m. For nonzero $P \in E(\mathbb{F})[m]$, there exists $Q \in E(\mathbb{F})$ such that*

$$t_m(P, Q) \neq 1.$$

Furthermore, for $Q \in E(\mathbb{F}) \backslash mE(\mathbb{F})$, there exists a $P \in E(\mathbb{F})[m]$ such that

$$t_m(P, Q) \neq 1.$$

In particular, for P of order m, there exists Q such that $t_m(P, Q)$ has order m, and similarly for the other entry.

3. *Compatibility: For a point $P \in E(\mathbb{F})[m]$, an isogeny $\phi : E \to E'$, and a point $Q \in E'(\mathbb{F})$,*

$$t_m(\widehat{\phi} P, Q) = t_m(P, \phi Q).$$

3 Structure of $E[\alpha]$

Suppose E has an $\mathcal{O}$-orientation. Let $\alpha \in \mathcal{O}$. We wish to know when $E[\alpha]$ is cyclic as an $\mathcal{O}$-module. The following two theorems of Lenstra are relevant.

Theorem 1 ([19, Proposition 2.1]). *Let E be an elliptic curve over an algebraically closed field k, and $\mathcal{O}$ a subring of $\mathrm{End}_k(E)$ such that as $\mathbb{Z}$-modules, $\mathcal{O}$ is free of rank 2 and $\mathrm{End}_k(E)/\mathcal{O}$ is torsion-free. Then for every separable element $\alpha \in \mathcal{O}$, $E[\alpha] \cong \mathcal{O}/\alpha\mathcal{O}$ as $\mathcal{O}$-modules.*

When α is inseparable, Lenstra has a similar result. With $\mathcal{O}$ as above, char $k = p > 0$, and $K = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q}$, he observes that there is a p-adic valuation ν on K with $\nu(\alpha) = \log(\deg_i \alpha)/\log p$ for $\alpha \in \mathcal{O}$. Following his notation, we define $V = \{x \in K : \nu(x) \geq 0\}$.

Theorem 2 ([19, Proposition 2.4]). *Let the notation and hypotheses be as above. Then for every non-zero element $\alpha \in \mathcal{O}$ there is an isomorphism of $\mathcal{O}$-modules $E[\alpha] \oplus (V/\alpha V) \cong \mathcal{O}/\alpha\mathcal{O}$.*

Theorem 3. *Let E be an elliptic curve over $\mathbb{F}$, K an imaginary quadratic field, and $\mathcal{O}$ an order in K such that E has an $\mathcal{O}$-orientation, which is primitive when extended to $\mathcal{O}'$. Let $f = [\mathcal{O}' : \mathcal{O}]$ be the relative conductor of $\mathcal{O}$. For $\alpha \in \mathcal{O}$ with $N(\alpha)$ coprime to f (i.e., such that the $\mathcal{O}$-orientation is $N(\alpha)$-primitive), then $E[\alpha]$ is cyclic as an $\mathcal{O}$-module. Specifically:*

1. *If α is separable, then $E[\alpha] \cong \mathcal{O}/\alpha\mathcal{O}$.*
2. *If α is inseparable, then $E[\alpha]$ is isomorphic to a proper cyclic $\mathcal{O}$-submodule of $\mathcal{O}/\alpha\mathcal{O}$.*

As a partial converse, as soon as α factors through multiplication by n for some $n > 1$ that divides f, $E[\alpha]$ is not cyclic as an $\mathcal{O}$-module. In particular, if $\alpha = m \in \mathbb{Z}$, then $E[m]$ is a cyclic $\mathcal{O}$-module if and only if m and f are coprime.

Proof. Suppose first that α is separable. Let ι be an $\mathcal{O}$-orientation for E and $\mathcal{O}'$ be the order of K for which ι is a primitive orientation. Then as an abelian group the quotient $\mathrm{End}(E)/\mathcal{O}'$ is torsion-free and Theorem 1 tells us that $E[\alpha] \cong \mathcal{O}'/\alpha\mathcal{O}'$ as $\mathcal{O}'$-modules. We have $N(\alpha) = N(\alpha\mathcal{O}') = |\mathcal{O}'/\alpha\mathcal{O}'|$, so since $N(\alpha)$ is coprime to f, it follows from [11, Proposition 7.18, 7.20] that the natural injection $\mathcal{O}/\alpha\mathcal{O} \to \mathcal{O}'/\alpha\mathcal{O}'$ is an isomorphism of $\mathcal{O}$-modules.

Suppose then that α is inseparable. Let $\mathcal{O}'$ be as above. From Theorem 2 we have $E[\alpha] \oplus V/\alpha V \cong \mathcal{O}'/\alpha\mathcal{O}'$, so $E[\alpha]$ is isomorphic as an $\mathcal{O}'$-module to $(\mathcal{O}'/\alpha\mathcal{O}')/(V/\alpha V)$ and hence is a cyclic $\mathcal{O}'$-module. Since $\mathcal{O}'/\alpha\mathcal{O}' \cong \mathcal{O}/\alpha\mathcal{O}$ as $\mathcal{O}$-modules, again by our assumption that $N(\alpha)$ is coprime to f, it follows that $E[\alpha]$ is cyclic as an $\mathcal{O}$-module.

Finally, suppose α factors through $[n]$ for some $n > 1$ with $n \mid f$. Then as a $\mathbb{Z}$-module, $E[\alpha] \cong \mathbb{Z}/b\mathbb{Z} \times \mathbb{Z}/c\mathbb{Z}$ with $n \mid b \mid c$. Let $\{P, Q\}$ be a generating set for $E[\alpha]$ with $\mathrm{ord}(P) = b, \mathrm{ord}(Q) = c$ and let $\mathcal{O}' = \mathbb{Z}[\sigma]$ for some σ. Then $\mathcal{O} = \mathbb{Z}[f\sigma]$. Since any element of $\mathcal{O}$ is a $\mathbb{Z}$-linear combination of $[1]$ and $[f\sigma]$, whether or not $E[\alpha]$ is cyclic as an $\mathcal{O}'$-module is determined by the action of $f\sigma$. We have $[f\sigma]Q = [n\sigma]Q'$, where $Q' = [f/n]Q$.

If $[\sigma]Q' = [s]P + [t]Q$, then $[f\sigma]Q = [ns]P + [nt]Q$, and we cannot obtain P from the action of any $\mathbb{Z}$-linear combination of $[1]$ and $[f\sigma]$ on Q. Thus, Q cannot be a generator for $E[\alpha]$ as an $\mathcal{O}$-module. Since Q was an arbitrary order c point, and since no point of order strictly less than c can generate $E[\alpha]$ as an $\mathcal{O}$-module (endomorphisms send points of E of order m to points of E of order dividing m), $E[\alpha]$ cannot be a cyclic $\mathcal{O}$-module.

Example 1. Consider the ordinary curve $y^2 = x^3 + 30x + 2$ over $\mathbb{F}_{101}$. Denoting the Frobenius endomorphism by π, $\mathbb{Z}[\pi]$ has conductor 2 in the maximal order and $[\mathbb{Z}[\pi] : \mathbb{Z}[\pi^2]] = 18$. Thus, Theorem 3 implies $E[3]$ is not cyclic as a $\mathbb{Z}[\pi^2]$-module. Indeed, making a base change to $\mathbb{F}_{101^2}$, the 3-torsion of E is rational. On the other hand, $E[3]$ is cyclic as a $\mathbb{Z}[\pi]$-module. With $\mathbb{F}_{101^2} = \mathbb{F}_{101}(a)$ and $x^2 - 4x + 2$ the minimal polynomial of a, we have $P = (41a + 16, 39a + 19) \in E[3]$ and $\pi(P) = (60a + 79, 62a + 74) \notin \langle P \rangle$, hence $\mathbb{Z}[\pi]P = E[3]$.

4 Sesquilinear pairings

We follow [26] in this section. Suppose $\mathcal{O} = \mathbb{Z}[\tau]$ is an imaginary quadratic order. Let E have CM by $\mathcal{O}$. Let $\rho : \mathcal{O} \to \mathrm{GL}_2(\mathbb{Z})$ be the left-regular representation of $\mathcal{O}$ acting on the basis 1 and τ. Then we endow the Cartesian square $(\mathbb{F}^*)^{\times 2}$ with an $\mathcal{O}$-module action via

$$(x, y)^\alpha = \rho(\alpha) \cdot (x, y) = (x^a y^b, x^c y^d), \quad \text{where} \quad \rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

In the case of an $\mathcal{O}$-module, by *order* of an element we mean the $\mathbb{Z}$-order; we can also discuss the annihilator as an $\mathcal{O}$-module, which may be distinct from this.

For each $\alpha \in \mathcal{O}$, we define a bilinear pairing

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

as follows. Write

$$\rho(\alpha) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad \rho(\overline{\alpha}) = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Observe that this corresponds to the ring facts

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

We take $P \in E[\overline{\alpha}]$, Define $f_P = (f_{P,1}, f_{P,2})$, where

$$\begin{aligned} \operatorname{div}(f_{P,1}) &= a([-\tau]P) + b(P) - (a+b)(\mathcal{O}), \\ \operatorname{div}(f_{P,2}) &= c([-\tau]P) + d(P) - (c+d)(\mathcal{O}). \end{aligned}$$

Choose an auxiliary point R and define

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

Then, choosing R so that the necessary supports are disjoint (i.e. the support of $\operatorname{div}(f_{P,i})$ and $D_{Q,j}$ are disjoint for each pair i, j), the pairing is defined as

$$\widehat{T}_\alpha^\tau(P,Q) := (f_{P,1}(D_{Q,1}), f_{P,2}(D_{Q,1}))\,(f_{P,1}(D_{Q,2}), f_{P,2}(D_{Q,2}))^{\overline{\tau}}$$

which can also be expressed as

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

Remark 1. In [26], it is shown how it is possible to think of these definitions as divisors in $\mathcal{O} \otimes_{\mathbb{Z}} \operatorname{Pic}^0(E)$:

$$D_Q = D_{Q,1} + \tau \cdot D_{Q,2}, \quad D_P = ([-\tau]P) - (\mathcal{O}) + \tau \cdot ((P) - (\mathcal{O})),$$

and analogously define f_P satisfying $\operatorname{div}(f_P) = \alpha \cdot D_P$, so that the definition above has the form $f_P(D_Q)$ as for the classical Tate pairing. For simplicity here, we stick to the direct definition above. In that same paper, analogous constructions are also given for quaternion orders and Weil-like pairings.

Theorem 4 ([26, Theorems 5.4, 5.5, 5.6]). *The pairing above is well-defined and satisfies*

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

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

2. *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 $Q \in E(\mathbb{F})$,*

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

3. *Coherence: Suppose $P \in E[\overline{\alpha\beta}](\mathbb{F})$, and $Q \in E(\mathbb{F})/[\alpha\beta]E(\mathbb{F})$. Then*

$$\widehat{T}^{\tau}_{\alpha\beta}(P,Q) \bmod ((\mathbb{F}^*)^{\times 2})^{\beta} = \widehat{T}^{\tau}_{\beta}([\overline{\alpha}]P, Q \bmod [\beta]E).$$

Suppose $P \in E[\overline{\alpha}](\mathbb{F})$, and $Q \in E(\mathbb{F})/[\alpha\beta]E(\mathbb{F})$. Then

$$\widehat{T}^{\tau}_{\alpha\beta}(P,Q) \bmod ((\mathbb{F}^*)^{\times 2})^{\alpha} = \widehat{T}^{\tau}_{\alpha}(P, [\beta]Q \bmod [\alpha]E).$$

4. *Non-degeneracy: Let $\mathbb{F}$ be a finite field, and let E be an elliptic curve defined over $\mathbb{F}$. Let $\alpha \in \mathcal{O}$ be coprime to 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*

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

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.
5. *Let t_n be the n-Tate-Lichtenbaum pairing as described in Section 2. Then*

$$\widehat{T}^{\tau}_{n}(P,Q) = \left(t_n(P,Q)^{2N(\tau)} t_n([-\tau]P,Q)^{Tr(\tau)},\ t_n([\tau-\overline{\tau}]P,Q)\right).$$

6. *Provided both of the following quantities are defined,*

$$\widehat{T}^{\tau}_{N(\alpha)}(P,Q) = \widehat{T}^{\tau}_{\alpha}(P,Q)^{\overline{\alpha}} \pmod{((\mathbb{F}^*)^{\times r})^{\alpha}}$$

Theorem 5. *The pairing $\widehat{T}^{\tau}_{\alpha}(P,Q)$ is efficiently computable. That is, it takes polynomially many operations in the field of definition of P and Q.*

Proof. This follows from the definition given above, which is amenable to a Miller-style pairing algorithm; details are in [26, Algorithm 5.7].

To use the pairings $\widehat{T}^{\tau}_{\alpha}$, the most expedient computation method is the formulas given in Theorem 4 items (5) and (6). In particular, in our applications of $\widehat{T}^{\tau}_{\alpha}$ to form a discrete logarithm problem, in most use cases it suffices to compute $\widehat{T}^{\tau}_{\alpha}(P,Q)^{\overline{\alpha}}$ instead. But if one wishes, one can compute $\overline{\alpha}^{-1} \pmod{\alpha}$ (provided α and $\overline{\alpha}$ are coprime), and use

$$\widehat{T}^{\tau}_{\alpha}(P,Q) = \widehat{T}^{\tau}_{N(\alpha)}(P,Q)^{\overline{\alpha}^{-1}} \pmod{((\mathbb{F}^*)^{\times 2})^{\alpha}}.$$

This may not apply when α divides the discriminant.

Definition 2. *Also for cryptographic applications, it is convenient to apply a final exponentiation to obtain a* reduced pairing*, as is common with the classical Tate pairing. This will move the pairing into the roots of unity:*

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

Lemma 1. *Consider the image $N(\mathcal{O})$ of $\mathcal{O}$ under the norm map. Then $N(\mathcal{O})$ modulo m is a subset of $\{x^2 : x \in \mathbb{Z}/m\mathbb{Z}\}$ only if m and $\Delta_{\mathcal{O}}$ share a non-trivial factor.*

Proof. We may assume, by Sunzi's Theorem (Chinese Remainder Theorem), that m is a prime power p^k. If p is split, the statement follows from the fact that the norm map from $\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}$ to $\mathbb{Q}_p$ is surjective. If p is inert, the norm map from $\mathbb{Q}_p \otimes_{\mathbb{Z}} \mathcal{O}$ to $\mathbb{Q}_p$ is not surjective, but is surjective on the residue field, so $N(\mathcal{O})$ modulo p^k does include non-squares.

Theorem 6. *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 $s \mid m' \mid s^2$. In particular, if $\mathcal{O}P = E[m]$, then the self-pairing has order m; and if $\mathcal{O}P = \mathbb{Z}P$, then the self-pairing is trivial.*

Proof. Let $m' \mid m$ be the order of $\widehat{T}_m^\tau(P,P)$. Suppose s is the maximal divisor of m so that $E[s] \subseteq \mathcal{O}P$. Then, in particular, $[s\tau]P \in \mathbb{Z}P$. Thus $\mathcal{O}[s]P = \mathbb{Z}[s]P$. We will show that $m' \mid s^2$ and $s \mid m'$.

Let $\lambda \in \mathcal{O}$. Then $[\lambda s]P = [ks]P$ for some $k = k(\lambda) \in \mathbb{Z}$, and then

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

Ranging over all $\lambda \in \mathcal{O}$, we conclude that $N(\lambda)$ are squares modulo $m'' = m'/\gcd(m', s^2)$, the multiplicative order of $\widehat{T}_m^\tau([s]P,[s]P)$, contradicting that m is coprime to the discriminant unless $m'' = 1$ by Lemma 1. Therefore $m' \mid s^2$.

On the other hand, by Theorem 4 item (4), there exists some Q so that $\widehat{T}_m^\tau(P,Q)$ has order m. Let $t = m/s$. Then there is a basis for $E[m]$ of the form P, P' where $[t]P' = [\lambda]P$ for some $\lambda \in \mathcal{O}$. Writing $Q = [a]P + [b]P'$,

$$\widehat{T}_m^\tau(P,Q)^t = \widehat{T}_m^\tau(P,[t]([a]P + [b]P')) = \widehat{T}_m^\tau(P,[ta + b\lambda]P) = \widehat{T}_m^\tau(P,P)^{ta+b\lambda}.$$

This has order s on the left. Therefore $\widehat{T}_m^\tau(P,P)$ must have order a multiple of s. Hence $s \mid m'$.

Remark 2. In [4], the authors study cyclic self-pairings on oriented elliptic curves, namely homogeneous functions $f : \langle P \rangle \to \overline{\mathbb{F}}^*$ of degree 2 which are compatible with endomorphisms from the orientation, in the sense that $\langle P \rangle$ is stabilized by such endomorphisms and $f(\phi P) = f(P)^{\deg \phi}$ for such endomorphisms. They show that non-trivial such pairings can only exist for P of order m dividing $\Delta_{\mathcal{O}}$. The reason our pairings are not ruled out by this result is that our pairings need not be defined on a cyclic subgroup stabilized by the orientation. In fact, their result can be recovered from Theorem 6, which implies that the pairings $\widehat{T}_\alpha^\tau$ are trivial on cyclic subgroups stabilized by $\mathcal{O}$.

Theorem 7. *Let E be an elliptic curve defined over a finite field $\mathbb{F}$, and let $m \in \mathbb{Z}$. Let a basis for $E[m]$ be given. Suppose arithmetic in $\mathbb{F}$, discrete logarithms* *in $\mathbb{F}^*$ modulo m, and group law computations on $E[m]$ can all be accomplished in polynomial time. Suppose E is known to be oriented by $\mathcal{O} = \mathbb{Z}[\tau]$ (but the orientation ι is not given), and suppose m is coprime to the discriminant $\Delta_{\mathcal{O}}$. Then the computation of arbitrary pairings $\widehat{T}_m^\tau(P,Q)$ on $E[m]$ is equivalent in polynomial time to the computation of the action of $[\tau]$ on $E[m]$.*

Proof. Note that since τ is known abstractly, computation of $[\tau]$ allows for computation of $[\overline{\tau}] = [Tr(\tau)] - [\tau]$.

If $[\tau]$ is computable, then by Theorem 4 (5) one can compute $\widehat{T}_m^\tau(P,Q)$ by computing 3 multiplications by $[\tau]$ or $[\overline{\tau}]$, one addition, and 3 classical Tate pairings.

Conversely, suppose one can compute $\widehat{T}_m^\tau(P,Q)$ for any $P,Q \in E[m]$. We will show how to compute the action of $[\tau]$ on $E[m]$. The pairing is non-degenerate as a consequence of the given hypotheses. Choose $P \in E[m]$ uniformly randomly as a linear combination of the given basis. Compute $\widehat{T}_m^\tau(P,P)$. If it is not of order m, choose another P.

For now, we assume that $\mathcal{O}P = E[m]$. Choose $Q \in E[m]$ so that P,Q form a basis for $E[m]$. Then $Q = [\lambda]P$ for some $\lambda \notin \mathbb{Z}$; then

$$\widehat{T}_m^\tau(P,Q) = \widehat{T}_m^\tau(P,P)^\lambda.$$

Since $\widehat{T}_m^\tau(P,P)$ is of order m by Theorem 6, we can compute λ modulo m by two pairing computations and a discrete logarithm in $(\mathbb{F}^*)^{\times 2}/((\mathbb{F}^*)^{\times 2})^m \cong \mu_m$.

By construction, we can write $\tau = a + b\lambda$ modulo m, so we can compute $[\tau]P = [a]P + [b]Q$.

To compute $[\tau]R$ for arbitrary R, we first determine $\mu \in \mathcal{O}$ modulo m such that $R = [\mu]P$ (we may use the same discrete log method as above), and then we have $[\tau]R = [\mu][\tau]P$.

If $\mathcal{O}P \neq E[m]$, then the algorithm is not guaranteed to be correct. Therefore, we run the algorithm several times using different random P of order m. More than half of the $P \in E[m]$ of order m should generate $E[m]$ as an $\mathcal{O}$-module, since $E[m] \cong \mathcal{O}/m\mathcal{O}$ by Theorem 3, and $\mathcal{O}$ can fix at most two order m subgroups. Any such P has self-pairing of order m (by non-degeneracy), so repeating sufficiently often and taking the majority rule answer, this will succeed with overwhelming probability in polynomial time.

Remark 3. Given any basis for $E[m]$, the pairing $\widehat{T}_m^\tau$ allows us to compute the 'eigenspaces', i.e. a basis P,Q such that $[\tau]P \in \langle P\rangle$ and $[\tau]Q \in \langle Q\rangle$. That is, knowing the pairing values on the original basis, we can solve for points with trivial self-pairing.

Example 2. Consider the elliptic curve $y^2 = x^3 + x$ over $\mathbb{F}_p$, $p = 541$. A basis for $E[5]$ is $P = (109, 208)$, $Q = (53, 195)$. If we compute the self-pairings $\widehat{T}_5^{[i]}([a]P + [b]Q, [a]P + [b]Q)$, for $a, b = 0, \ldots, 4$, we obtain the following: the left matrix shows the real parts and the right matrix the imaginary parts, taken log base a generator of $\mathbb{F}_p$, namely, 48. So, for example, the second entry on the fourth row indicates that $\widehat{T}_5^{[i]}([4]P+[2]Q,[4]P+[2]Q)=(g^3,g^4)$.

$$\begin{pmatrix} 0&4&1&1&4\\ 0&2&2&0&1\\ 0&0&3&4&3\\ 0&3&4&3&0\\ 0&1&0&2&2 \end{pmatrix}, \quad \begin{pmatrix} 0&2&3&3&2\\ 0&1&1&0&3\\ 0&0&4&2&4\\ 0&4&2&4&0\\ 0&3&0&1&1 \end{pmatrix}.$$

From this we observe that $\widehat{T}_5^{[i]}(P,P)=\widehat{T}_5^{[i]}([2]P+Q,[2]P+Q)=1$. This is as dictated by Theorem 6, because $[i]P=[3]P$ and $[i]([2]P+Q)=[2]([2]P+Q)$.

5 Recovering partial torsion image information

Our first observation is that when $E[m]$ is a cyclic $\mathcal{O}$-module, the pairings recover *partial* information about the action of a hidden oriented isogeny ϕ on $E[m]$.

Theorem 8. *Let E and E' be $\mathcal{O}$-oriented supersingular curves over $\overline{\mathbb{F}}_p$ upon which we can efficiently compute the action of a generator τ for $\mathcal{O}$. Assume that the discrete logarithm in μ_m and group operations on $E[m]$ are efficient. Assume also that $E[m]$ is a cyclic $\mathcal{O}$-module, and that the hidden oriented isogeny $\phi : E \to E'$ has known degree coprime to m. Suppose we are given P and P' such that $\mathcal{O}P=E[m]$ and $\mathcal{O}P'=E'[m]$. Then we can efficiently recover $N(\lambda)$ modulo m for $\lambda\in\mathcal{O}$ such that $\phi P=[\lambda]P'$.*

Proof. We have

$$\widehat{T}_m^{\tau}(P,P)^{\deg\phi}=\widehat{T}_m^{\tau}(\phi P,\phi P)=\widehat{T}_m^{\tau}(\lambda P',\lambda P')=\widehat{T}_m^{\tau}(P',P')^{N(\lambda)}.$$

Note that by Theorem 6, $\widehat{T}_m^{\tau}(P,P)$ has order m. Since m is smooth, using the reduced pairing, we can solve a discrete log problem in μ_m to obtain $N(\lambda)$ modulo m.

Remark 4. This result would provide a square-root improvement on an exhaustive search over image points of P. More precisely, one could attack the class group action problem by trying all possible image points ϕP for P, infer $\phi[\tau]P=[\tau]\phi P$, and therefore use the image of the m-torsion as input to the SIDH attacks, checking for success at each attempt. This is similar to [14, Section 4.1], for example. Here, the knowledge of $N(\lambda)$ restricts ϕP to only $O(m)$ possible images, not m^2. This may provide another $O(\sqrt{p})$ runtime classical attack on CSIDH, for example. Attacks with this runtime already exist using random walks [15,16]. To run such an exhaustive search SIDH attack, we need the degree of ϕ to be known and $m^2>\deg\phi$, m to be coprime to $\deg\phi$, and m to be smooth. Since we have great freedom in choosing m, we can expect to choose an m around $\sqrt{\deg\phi}$. Then we have to try approximately m different images $\lambda P'$ of P which give $N(\lambda)$ as computed, running the SIDH attack on each. This attack applies very generally in the setup of the theorem above, whereas the attacks of [16] require a variety of hypotheses.

Remark 5. This and other similar results in this paper and in [13] are a caution against decision Diffie-Hellman problems in which one must decide if a given point is the image point of a specified torsion point under a hidden isogeny. A result like the previous one reduces the possibilities for the torsion image (without pinning it down entirely). For an example, the IND-CPA hardness of SiGamal [21] depends upon such a problem, called the P-CSSDDH assumption. This is discussed in [4, Section 6.1], where the authors lament the triviality of the available self-pairings. There are non-trivial pairings of the type $\widehat{T}$ and $\widehat{W}$ which would apply to the SiGamal situation, but only if we had access to a different orientation on the curves and isogeny. The Frobenius orientation used in the P-CSSDDH assumption results in a trivial pairing once again, because the torsion is contained in the base field.

Remark 6. There is a sense in which we cannot hope to obtain more information than $N(\lambda)$ modulo m using these methods. If we post-compose our isogeny with an endomorphism from $\mathcal{O}$ of norm 1 modulo m, then we do not change the degree modulo m, but we do change λ, replacing it with another λ' having the same norm modulo m. To detect the difference, we must feed in more information than just the degree modulo m. In fact, it is possible to recover the same result by a different method. Take a basis for E and E' and change basis so that the Weil pairing takes a canonical diagonal form. Then the set of possible endomorphisms in $\mathcal{O}$ that preserve this diagonal form turns out to be the same 'degree of freedom' of λ observed above. The pairings from [4] can be seen as getting around this by assuming $\lambda \in \mathbb{Z}$, in which case $N(\lambda)$ pins down λ more effectively.

Remark 7. In principle, the result above doesn't require using $\widehat{T}$; it could be phrased in terms of one of the coordinates in Theorem 4 (5). This wouldn't violate the classification of cyclic self-pairings in [4] because the domain is not $\mathbb{Z}$-cyclic.

6 Reduction from SIDH$_1$ to SIDH

In [13], the authors consider a variety of variants on the SIDH problem which can be parameterized by the information available about the action of ϕ on the m-torsion (*level structure* information). In particular, they define the following problem.

Problem 1 (SIDH$_1$). Fix $d, m \in \mathbb{Z}$. Let E, E' be elliptic curves defined over $\mathbb{F}_q$, where m is coprime to q. Let $P \in E[m]$ have order m. Suppose there exists an isogeny $\phi : E \to E'$ of known degree d and ϕP is given. Find ϕ.

This can be compared to the classical SIDH problem, in which we are given full torsion image information.

Problem 2 (SIDH). Fix $d, m \in \mathbb{Z}$. Let E, E' be elliptic curves defined over $\mathbb{F}_q$, where m is coprime to q. Let P, Q form a basis for $E[m]$. Suppose there exists an isogeny $\phi : E \to E'$ of known degree d and ϕP and ϕQ are given. Find ϕ.

In either case we refer to m as the *level* of the SIDH or SIDH_1 problem. The authors of [13] show that if m has a large smooth square factor, then SIDH_1 of level m (a single torsion point image of order m) reduces to SIDH of level $O(\sqrt{m})$ (two torsion point images of order $O(\sqrt{m})$). More recently, a manuscript in preparation (presented at Caipi Symposium 2024 [3]) generalizes the SIDH attacks of [2,20,23], directly attacking SIDH_1 without the requirement that m have a large square factor. Both approaches require that $m > \deg \phi$.

Here we show that, *if we have an oriented isogeny*, knowing a single image of order m is enough to reduce to SIDH of level m (on the same curve), assuming only that m is smooth, with no assumption on m being square, and no loss in level. Thus using the SIDH attacks requires only $m^2 > \deg \phi$.

Theorem 9. *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 is smooth and 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 coprime to m. Then the problem $SIDH_1$ of level m to find ϕ 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 ϕ.*

Proof. We are given ϕR for some point $R \in E[m]$ of order m. We wish to recover a second torsion point image, resulting in an SIDH problem. First, by Sunzi's Theorem, we can reduce the problem to prime powers $m = p^k$. By assumption, p is not ramified. Hence we may assume p is a split or inert.

Case that p is inert. We know $\mathcal{O}R$ is an $\mathcal{O}$-submodule of $E[m] \cong \mathcal{O}/m\mathcal{O}$. If p is inert, it must be isomorphic to $\mathcal{O}/p^s\mathcal{O}$. However, $\mathcal{O}/p^s\mathcal{O}$ doesn't have elements of additive order p^k unless $s = k$. Thus $\mathcal{O}R = E[m]$. Given any other point Q, we may compute η such that $Q = [\eta]R$ (using basis R and $[\tau]R$). Then $\phi Q = \phi[\eta]R = [\eta]\phi R$.

Case that p is split. Write $m = p^k = \mathfrak{b}\overline{\mathfrak{b}}$, where $N(\mathfrak{b}) = m$. Then we have, without loss of generality, S, T a basis for $E[m]$ so that $\mathfrak{b}T = \{\mathcal{O}\}$, and $\overline{\mathfrak{b}}S = \{\mathcal{O}\}$. Similarly, let S' and T' be a basis for $E[m]$ so that $\mathfrak{b}T' = \{\mathcal{O}\}$ and $\overline{\mathfrak{b}}S' = \{\mathcal{O}\}$. To find such a basis, one could use Remark 3 or more standard methods.

Now the mapping ϕ, as a matrix from basis S, T to basis S', T', is diagonal, with some integers k_1 and k_2 on the diagonal. By writing R and ϕR in the relevant bases, namely $R = [a]S + [b]T$, $\phi R = [c]S' + [d]T'$, we learn that $ak_1 \equiv c, bk_2 \equiv d \pmod{m}$. We also know that $\deg \phi \equiv k_1 k_2 \pmod{m}$. Without loss of generality, at least one of a or b is coprime to m, so we know at least one of k_1 or k_2, and the degree equation then gives us the other.

7 Diagonal SIDH

The following problem arises in [13, Lemma 6 and Section 5.6].

Problem 3 (Diagonal SIDH). Fix $d, m \in \mathbb{Z}$. Let E, E' be elliptic curves defined over $\mathbb{F}_q$, where m is coprime to q. Let $P, Q \in E[m]$ form a basis. Suppose there exists an isogeny $\phi : E \to E'$ of known degree d. Suppose that generators P' of $\langle \phi P \rangle$ and Q' of $\langle \phi Q \rangle$ are known.

Interestingly, when the curves are oriented, the Diagonal SIDH problem is amenable to a pairing-based attack, at least for certain conditions on $E[m]$.

Theorem 10. *Suppose E and E' are $\mathcal{O}$-oriented (and one can compute the action of the endomorphisms efficiently, as usual). Let m 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 $\mathcal{O}Q = E[m]$.*

Proof. Let the Diagonal SIDH problem be given in terms of basis P, Q for $E[m]$ and generators P' and Q' for $\langle \phi P \rangle$ and $\langle \phi Q \rangle$ respectively. Assume without loss of generality that $\mathcal{O}P = E[m]$. Then by Theorem 8, we can efficiently recover $N(\lambda)$ such that $\phi P = \lambda P'$. However, the Diagonal SIDH setup guarantees that $\lambda \in \mathbb{Z}$, hence we have recovered λ^2 modulo m. By assumption, this gives only polynomially many possible values for λ, each of which can be tested by running the SIDH attacks, until one recovers ϕ.

An instance of the Diagonal SIDH problem is the problem underlying the FESTA cryptosystem [1, Problem 7]. In this case m is chosen to be a power of 2, so the attack above would apply if FESTA were instantiated in a situation where the isogeny was oriented (for known orientations). Assuming an $\mathcal{O}$-orientation, the condition $\mathcal{O}P = E[m]$ or $\mathcal{O}Q = E[m]$ is reasonably likely to occur by chance if not explicitly avoided.

Corollary 1. *The hard problem underlying FESTA reduces to finding explicit $\mathcal{O}$-orientations of the curves E and E' and the isogeny ϕ between them.*

Remark 8. In [13, Section 5.6], it is shown how to reformulate the problem of finding an isogeny of fixed degree d between oriented curves (the class group action problem) as a Diagonal SIDH problem, where m is a product of primes split in $\mathcal{O}$. The method of reduction, in brief, uses the eigenspaces associated to a split prime in the orientation, which must map to each other. However, the conditions under which Theorem 10 applies – that m have few square roots, and P or Q be generators of $E[m]$ as an $\mathcal{O}$-module – both fail in the Diagonal SIDH problems that result from the reduction of [13]. This means we cannot chain these attacks together to attack class group action problems!

8 When N divides the discriminant

Suppose $N \mid \Delta_{\mathcal{O}}$, where $N = N(\tau)$ for $\tau \in \mathcal{O}$. In this case the pairing $\widehat{T}_N^\tau$ becomes trivial. However, a modification is more interesting. Let $n \in \mathbb{Z}$, and define

$$T'_n(P, Q) = (t_n([\tau]P, Q), t_n(P, Q)) \in ((\mathbb{F}^*)/(\mathbb{F}^*)^n))^{\times 2}.$$

This modification does not preserve all of the properties of Theorem 4 but importantly, it inherits compatibility from t_n, so that for $\phi : E \to E'$ compatible with $\mathcal{O}$, we have

$$T'_n(\phi Q, \phi Q) = T'_n(Q, Q)^{\deg \phi}.$$

In [4], the authors use generalized pairings to determine the image of a single torsion point in $E[N]$, and then reduce to SIDH with $E[\sqrt{N}]$ when N is a smooth square. In fact, recent further development of the SIDH attacks (in preparation [3]) generalize to image information on subgroups of a large enough size, not just full torsion subgroups, which effectively removes the restriction that N be square.

Inspired by this result, we develop a similar reduction using the pairing above. The main advantage of our situation over that in [4] is the computation of the pairing, which requires only operations in the field of definition of $E[N]$. Because the pairings used in [4] may require a move to the field of definition of $E[N^2]$, our pairings result in a speedup in cases where that field of definition is large.

Lemma 2. *Let E have an orientation by $\mathcal{O} = \mathbb{Z}[\tau]$, and let $P \in E[m]$ be such that $\langle [\tau]P \rangle \cap \langle P \rangle = \{0\}$. Let t be the minimal positive integer such that $[t]E[m] \subseteq \mathcal{O}P$. Let f be the relative conductor of $\mathcal{O}$, so that $\tau = f\tau'$ for another endomorphism τ'. Let $g = \gcd(m, f)$ and let $n = \gcd(N(\tau'), m)$. Then, $g \le t \le gn$.*

Proof. As a direct consequence of the hypotheses, $[\tau]P = [f][\tau']P \in E[m/g]$. On the other hand, $[\tau]P$ has order at least m/gn. Therefore $[\tau]P$ has order s satisfying $m/gn \le s \le m/g$. By assumption, $\langle [\tau]P \rangle \cap \langle P \rangle = \{0\}$. Therefore, s is the maximal integer dividing m such that $E[s] \subseteq \mathcal{O}P$. But $E[s] = [m/s]E[m]$.

Proposition 2. *Let E be an elliptic curve oriented by $\mathcal{O} = \mathbb{Z}[\tau]$. Let $\mathbb{F}$ be a finite field containing the m-th roots of unity. Suppose $E[m] = E[m](\mathbb{F})$ is a cyclic $\mathcal{O}$-module. Let $P \in E[m]$. Then the multiplicative order $T'_m(P, P)$ is m/t where t is the minimal positive integer such that $[t]E[m] \subseteq \mathcal{O}P$.*

Proof. The classical Tate-Lichtenbaum pairing

$$t_m : E[m](\mathbb{F}) \times E(\mathbb{F})/[m]E(\mathbb{F}) \to \mathbb{F}^*/(\mathbb{F}^*)^m$$

is non-degenerate and, for P of order m, there exists a Q so $t_m(P, Q)$ has order m (Proposition 1). Let t be the minimal positive integer for which $[t]E[m] \subseteq \mathcal{O}P$. Then $[t]Q = [a + \tau b]P$ for some a, b having $\gcd(a, b, m) = 1$.

$$\begin{aligned} T'_m(P, Q)^t &= T'_m(P, [a + \tau b]P) \\ &= T'_m(P, P)^a T'_m(P, [\tau]P)^b \\ &= (t_m([\tau]P, P)^a t_n(P, P)^{N(\tau)b}, t_m(P, P)^a t_m([\tau]P, P)^b). \end{aligned}$$

The left side has order m/t. Thus the right side has order m/t; applying a linear transformation, $T'_m(P, P)$ must have order m/t.

In the following, we assume $E[m]$ is a cyclic $\mathcal{O}$-module. By Theorem 3, it suffices that the $\mathcal{O}$-orientation be m-primitive.

Theorem 11. *Let E and E' be $\mathcal{O}$-oriented elliptic curves. Suppose there exists an oriented $\phi : E \to E'$ of known degree d. Let m be smooth, coprime to d, and chosen so that there are only polynomially many square roots of 1 modulo m. Suppose there exists $\tau \in \mathcal{O}$ with norm $N(\tau) \equiv \Delta_{\mathcal{O}} \equiv 0 \pmod{m}$. Suppose that $E[m]$ is a cyclic $\mathcal{O}$-module. Suppose $P \in E[m]$ such that $\mathcal{O}P = E[m]$. Then a subset $S \subset E[m]$ of polynomial size containing $\phi(P)$ can be computed in polynomially many operations in the field of definition of $E[m]$.*

Proof. As explained in [4, Section 5.2], we can find $\tau \in \mathcal{O}$ such that $N(\tau) \equiv Tr(\tau) \equiv 0 \pmod{m}$. Hence the minimal polynomial of τ is x^2 modulo m, and τ^2 acts as 0 on $\mathcal{O}/m\mathcal{O}$. Choose a point $P \in E[m]$ such that $\mathcal{O}P = E[m]$. Choose a point $P' \in E'[m]$ such that $\mathcal{O}P' = E'[m]$. Then $T'_m(P, P)$ and $T'_m(P', P')$ have order m by Proposition 2. Then

$$T'_m(P, P)^{\deg\phi} = T'_m(\phi P, \phi P) = T'_m(\lambda P', \lambda P') = T'_m(P', P')^{N(\lambda)}.$$

Using a discrete logarithm, we can compute $N(\lambda) \pmod{m}$. Write $\lambda = a + b\tau$. Then $N(\lambda) \equiv a^2 \pmod{m}$. Since the factorization of m is known, by assumption, we have an efficiently computable set of polynomial size of possible values of a. Compute $[a][\tau]P'$. For the correct a, this is the image of $[\tau]P$ under ϕ, since

$$\phi[\tau]P = \lambda[\tau]P' = [a][\tau]P'.$$

Trying all possible values of a, we obtain the set $\{[a][\tau]P' : a^2 \equiv N(\lambda) \pmod{m}\}$ required by the statement.

The results of [4,13] can now be applied if m is a smooth square, d is powersmooth and $m > d$, to reduce to a solvable instance of SIDH. Alternatively, loosening the restriction that m is a square will be possible with the new generalizations of SIDH mentioned above [3].

Example 3. The following example is based on an example communicated to the authors by Wouter Castryck. Let $E : y^2 = x^3 + x$. Let p be a prime of the form $4 \cdot 3^r - 1$ with $r > 0$. This curve is supersingular with $j = 1728$ and endomorphisms $[i] : (x, y) \mapsto (-x, iy)$ and $\pi_p : (x, y) \mapsto (x^p, y^p)$. Let

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

Then $\tau^2 = -\frac{p+1}{4} = -3^r$, so $N(\tau) = 3^r$. Since $\pi_p^2 = [-p]$, $E(\mathbb{F}_{p^2}) \cong (\mathbb{Z}/(p+1)\mathbb{Z})^2 \cong (\mathbb{Z}/4 \cdot 3^r\mathbb{Z})^2$ [25, Ex. 5.16.d]. Therefore $E[3^r] \subseteq E(\mathbb{F}_{p^2})$.

We can choose $m = 3^r$, which is a square when r is even. Let Q be an $\mathcal{O}$-generator of $E[3^r]$. Then by Proposition 2, $T'_m(Q, Q)$ has order 3^r, and the polynomially many operations to run the attack of Theorem 11 take place in $\mathbb{F}_{p^2}$. The SIDH portion of the attack requires that $d < m = 3^r$.

By contrast, using the methods of [4, Section 6.1], one would need a generalized pairing value of T_m^τ for which only methods of computation taking place in the field of definition of $E[3^{2r}]$ are known.

9 Supersingular class group action in the presence of another orientation

Theorem 12. *Let E and E' be elliptic curves for both of which we know orientations by two orders $\mathcal{O}$ and $\mathcal{O}'$ which generate a rank 4 sub-order of the endomorphism ring. Let $\phi : E \to E'$ be an isogeny of known degree d. Let m be smooth, coprime to the discriminants of $\mathcal{O}$ and $\mathcal{O}'$, and suppose 1 has only polynomially many square roots modulo m. Suppose ϕ respects both the $\mathcal{O}$ and $\mathcal{O}'$ orientations. Let $P \in E[m]$. Then a subset of $E'[m]$ of polynomial size containing ϕP can be computed in polynomially many operations in the field of definition of $E[m]$.*

Proof. By assumption, m is coprime to the discriminants. Thus we can choose $P \in E[m]$ so that $\mathcal{O}P = E[m]$. Similarly, let $P' \in E'[m]$ be chosen so that $\mathcal{O}P' = E'[m]$. Suppose $\phi P = [\lambda]P'$ for some $\lambda \in \mathcal{O}$. As in Theorem 9, we can compute $N(\lambda)$ modulo m.

Let $\sigma \in \mathcal{O}'$ be chosen to have norm coprime to m and be of the form $\sigma = a\sigma_1 + b\sigma_2$ with a and b coprime to m, where $\sigma_1 \in \mathcal{O}$ and σ_2 is perpendicular to $\mathcal{O}$ in the geometry afforded by the norm map on the quaternion algebra, so that $\sigma_2\lambda = \overline{\lambda}\sigma_2$. Write λ^σ for an element which participates in the equivalence $\lambda^\sigma\sigma \equiv \sigma\lambda \pmod{m}$. This can be computed by taking $\lambda^\sigma = \sigma\lambda\overline{\sigma}N$ where N is an integer equivalent to $N(\sigma)^{-1} \pmod{m}$. Then $\overline{\lambda^\sigma} \equiv a\overline{\lambda} + b\lambda \pmod{m}$. Then

$$\begin{aligned}
\widehat{T}_m^\tau([\sigma]P, P)^{\deg\phi} &= \widehat{T}_m^\tau(\phi[\sigma]P, \phi P) \\
&= \widehat{T}_m^\tau([\sigma]\phi P, \phi P) \\
&= \widehat{T}_m^\tau(\sigma[\lambda]P', [\lambda]P') \\
&= \widehat{T}_m^\tau([\lambda^\sigma][\sigma]P', [\lambda]P') \\
&= \widehat{T}_m^\tau([\sigma]P', P')^{\overline{\lambda^\sigma}\lambda}.
\end{aligned}$$

Since the norm of σ is coprime to m, $\widehat{T}_m^\tau([\sigma]P, P)$ has the same order as $\widehat{T}_m^\tau(P, P)$, which is m by Theorem 6. Thus, we can compute $\overline{\lambda^\sigma}\lambda$ modulo m by performing a discrete logarithm in μ_m.

Using knowledge of $\overline{\lambda^\sigma}\lambda \equiv aN(\lambda) + b\lambda^2$ and $N(\lambda)$, both modulo m, and recalling b is coprime to m, we obtain λ^2 modulo m.

Using $N(\lambda)$ and λ^2, we can solve for polynomially many possibilities for λ modulo m. Then we have obtained ϕP. From this we can compute any other ϕR by solving for $R = [\mu]P$ and observing that $\phi R = \phi[\mu]P = [\mu]\phi P$.

Acknowledgments.

The authors are grateful to Damien Robert and Wouter Castryck for helpful discussions. Both authors are supported by NSF CAREER CNS-1652238 and NSF DMS-2401580 (PI K. E. Stange).

Disclosure of Interests.

The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Basso, A., Maino, L., Pope, G.: FESTA: fast encryption from supersingular torsion attacks. In: Advances in cryptology—ASIACRYPT 2023. Part VII, Lecture Notes in Comput. Sci., vol. 14444, pp. 98–126. Springer, Singapore ([2023] ©2023). https://doi.org/10.1007/978-981-99-8739-9_4, https://doi-org.colorado.idm.oclc.org/10.1007/978-981-99-8739-9_4
2. Castryck, W., Decru, T.: An efficient key recovery attack on SIDH. In: Advances in cryptology—EUROCRYPT 2023. Part V, Lecture Notes in Comput. Sci., vol. 14008, pp. 423–447. Springer, Cham ([2023] ©2023). https://doi.org/10.1007/978-3-031-30589-4_15, https://doi-org.colorado.idm.oclc.org/10.1007/978-3-031-30589-4_15
3. Castryck, W., Decru, T., Maino, L., Martindale, C., Panny, L., Pope, G., Robert, D., Wesolowski, B.: Isogeny interpolation (2024), manuscript in preparation, presented at Caipi Symposium, Rennes, April 30, 2024, https://caipi_symposium.pages.math.cnrs.fr/page-web/editions/avr24.html
4. Castryck, W., Houben, M., Merz, S.P., Mula, M., Buuren, S.v., Vercauteren, F.: Weak instances of class group action based cryptography via self-pairings. In: Handschuh, H., Lysyanskaya, A. (eds.) Advances in Cryptology – CRYPTO 2023. pp. 762–792. Springer Nature Switzerland, Cham (2023)
5. Castryck, W., Houben, M., Vercauteren, F., Wesolowski, B.: On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves. Res. Number Theory **8**(4), Paper No. 99, 18 (2022). https://doi.org/10.1007/s40993-022-00399-6, https://doi-org.colorado.idm.oclc.org/10.1007/s40993-022-00399-6
6. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Advances in cryptology—ASIACRYPT 2018. Part III, Lecture Notes in Comput. Sci., vol. 11274, pp. 395–427. Springer, Cham (2018). https://doi.org/10.1007/978-3-030-03332-3_15, https://doi-org.colorado.idm.oclc.org/10.1007/978-3-030-03332-3_15
7. Castryck, W., Sotáková, J., Vercauteren, F.: Breaking the decisional Diffie-Hellman problem for class group actions using genus theory: extended version. J. Cryptology **35**(4), Paper No. 24, 30 (2022). https://doi.org/10.1007/s00145-022-09435-1, https://doi-org.colorado.idm.oclc.org/10.1007/s00145-022-09435-1
8. Charles, D.X., Lauter, K.E., Goren, E.Z.: Cryptographic hash functions from expander graphs. J. Cryptology **22**(1), 93–113 (2009). https://doi.org/10.1007/s00145-007-9002-x, https://doi-org.colorado.idm.oclc.org/10.1007/s00145-007-9002-x
9. Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. J. Math. Cryptol. **14**(1), 414–437 (2020). https://doi.org/10.1515/jmc-2019-0034, https://doi-org.colorado.idm.oclc.org/10.1515/jmc-2019-0034
10. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291 (2006), https://eprint.iacr.org/2006/291, https://eprint.iacr.org/2006/291

11. Cox, D.A.: Primes of the Form x^2+ny^2: Fermat, Class Field Theory, and Complex Multiplication. Third Edition with Solutions. AMS Chelsea Publishing (2022)
12. Eisenträger, K., Hallgren, S., Leonardi, C., Morrison, T., Park, J.: Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. In: ANTS XIV—Proceedings of the Fourteenth Algorithmic Number Theory Symposium. Open Book Ser., vol. 4, pp. 215–232. Math. Sci. Publ., Berkeley, CA (2020). https://doi.org/10.2140/obs.2020.4.215, https://doi-org.colorado.idm.oclc.org/10.2140/obs.2020.4.215
13. De Feo, L., Fouotsa, T.B., Panny, L.: Isogeny problems with level structure. Springer-Verlag (2024)
14. Fouotsa, T.B., Moriya, T., Petit, C.: M-SIDH and MD-SIDH: countering SIDH attacks by masking information. In: Advances in cryptology—EUROCRYPT 2023. Part V, Lecture Notes in Comput. Sci., vol. 14008, pp. 282–309. Springer, Cham ([2023] ©2023). https://doi.org/10.1007/978-3-031-30589-4_10, https://doi-org.colorado.idm.oclc.org/10.1007/978-3-031-30589-4_10
15. Galbraith, S.D.: Constructing isogenies between elliptic curves over finite fields. LMS J. Comput. Math. **2**, 118–138 (1999). https://doi.org/10.1112/S1461157000000097, https://doi-org.colorado.idm.oclc.org/10.1112/S1461157000000097
16. Galbraith, S.D., Hess, F., Smart, N.P.: Extending the GHS Weil descent attack. In: Advances in cryptology—EUROCRYPT 2002 (Amsterdam), Lecture Notes in Comput. Sci., vol. 2332, pp. 29–44. Springer, Berlin (2002). https://doi.org/10.1007/3-540-46035-7_3, https://doi-org.colorado.idm.oclc.org/10.1007/3-540-46035-7_3
17. Ionica, S., Joux, A.: Pairing the volcano. Math. Comp. **82**(281), 581–603 (2013). https://doi.org/10.1090/S0025-5718-2012-02622-6, https://doi-org.colorado.idm.oclc.org/10.1090/S0025-5718-2012-02622-6
18. Kohel, D., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion ℓ-isogeny path problem. LMS J.Comput. Math. (2014)
19. Lenstra, Jr., H.W.: Complex multiplication structure of elliptic curves. J. Number Theory **56**(2), 227–241 (1996). https://doi.org/10.1006/jnth.1996.0015, https://doi-org.colorado.idm.oclc.org/10.1006/jnth.1996.0015
20. Maino, L., Martindale, C., Panny, L., Pope, G., Wesolowski, B.: A direct key recovery attack on SIDH. In: Advances in cryptology—EUROCRYPT 2023. Part V, Lecture Notes in Comput. Sci., vol. 14008, pp. 448–471. Springer, Cham ([2023] ©2023). https://doi.org/10.1007/978-3-031-30589-4_16, https://doi-org.colorado.idm.oclc.org/10.1007/978-3-031-30589-4_16
21. Moriya, T., Onuki, H., Takagi, T.: SiGamal: a supersingular isogeny-based PKE and its application to a PRF. In: Advances in cryptology—ASIACRYPT 2020. Part II, Lecture Notes in Comput. Sci., vol. 12492, pp. 551–580. Springer, Cham ([2020] ©2020). https://doi.org/10.1007/978-3-030-64834-3_19, https://doi-org.colorado.idm.oclc.org/10.1007/978-3-030-64834-3_19
22. Robert, D.: The geometric interpretation of the Tate pairing and its applications. Cryptology ePrint Archive, Paper 2023/177 (2023), https://eprint.iacr.org/2023/177, https://eprint.iacr.org/2023/177
23. Robert, D.: Breaking SIDH in polynomial time. In: Advances in cryptology—EUROCRYPT 2023. Part V, Lecture Notes in Comput. Sci., vol. 14008, pp. 472–503. Springer, Cham ([2023] ©2023). https://doi.org/10.1007/978-3-031-30589-4_17, https://doi-org.colorado.idm.oclc.org/10.1007/978-3-031-30589-4_17

24. Rostovtsev, A., Stolbunov, A.: Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Paper 2006/145 (2006), https://eprint.iacr.org/2006/145, https://eprint.iacr.org/2006/145
25. Silverman, J.H.: The Arithmetic of Elliptic Curves, Second Edition. Springer (2009)
26. Stange, K.E.: Sesquilinear pairings on elliptic curves (2024), https://arxiv.org/abs/2405.14167
27. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. In: 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science—FOCS 2021, pp. 1100–1111. IEEE Computer Soc., Los Alamitos, CA ([2022] ©2022). https://doi.org/10.1109/FOCS52979.2021.00109, https://doi-org.ezproxy.lib.ucalgary.ca/10.1109/FOCS52979.2021.00109