# Computational aspects of class group actions and applications to post-quantum cryptography

Houben, M.R.

# Chapter 5

# Weak instances of class group action based cryptography via self-pairings

This chapter consists of a paper written together with Wouter Castryck, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. It has been published as

Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. Weak instances of class group action based cryptography via self-pairings. In *Advances in Cryptology – CRYPTO 2023*, pages 762–792, Lecture Notes in Computer Science, vol 14083. Springer, Cham. `https://doi.org/10.1007/978-3-031-38548-3_25`.

All authors of this paper contributed equally to the work.

Compared to the published version we added Section 5.8, which appears as Appendix A in the eprint version [5]. We also fixed some typos. The numbering (of e.g. theorems and definitions) in the published version is different.

**Acknowledgements**

We owe thanks to Luca De Feo, Damien Robert, Katherine Stange and the anonymous reviewers for various helpful comments, discussions and suggestions. We thank Abel Laval for pointing out a typo in Equation (5.7).

## Abstract

In this paper we study non-trivial self-pairings with cyclic domains that are compatible with isogenies between elliptic curves oriented by an imaginary quadratic order $\mathcal{O}$. We prove that the order $m$ of such a self-pairing necessarily satisfies $m \mid \Delta_{\mathcal{O}}$ (and even $2m \mid \Delta_{\mathcal{O}}$ if $4 \mid \Delta_{\mathcal{O}}$ and $4m \mid \Delta_{\mathcal{O}}$ if $8 \mid \Delta_{\mathcal{O}}$) and is not a multiple of the field characteristic. Conversely, for each $m$ satisfying these necessary conditions, we construct a family of non-trivial cyclic self-pairings of order $m$ that are compatible with oriented isogenies, based on generalized Weil and Tate pairings.

As an application, we identify weak instances of class group actions on elliptic curves assuming the degree of the secret isogeny is known. More in detail, we show that if $m^2 \mid \Delta_{\mathcal{O}}$ for some prime power $m$ then given two primitively $\mathcal{O}$-oriented elliptic curves $(E, \iota)$ and $(E', \iota') = [\mathfrak{a}](E, \iota)$ connected by an unknown invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$, we can recover $\mathfrak{a}$ essentially at the cost of a discrete logarithm computation in a group of order $m^2$, assuming the norm of $\mathfrak{a}$ is given and is smaller than $m^2$. We give concrete instances, involving ordinary elliptic curves over finite fields, where this turns into a polynomial time attack.

Finally, we show that these self-pairings simplify known results on the decisional Diffie–Hellman problem for class group actions on oriented elliptic curves.

## 5.1 Introduction

Isogeny based cryptography using class group actions was originally proposed in the works of Couveignes [13] and Rostovtsev–Stolbunov [32] (CRS), and both use ordinary elliptic curves. In particular, let $\mathcal{O}$ be an order in an imaginary quadratic number field $K$, then there is a natural action of the ideal-class group $\mathrm{Cl}(\mathcal{O})$ on the set of ordinary elliptic curves (up to isomorphism) over a finite field $\mathbf{F}_q$ whose endomorphism ring is isomorphic to $\mathcal{O}$. Since it is difficult to construct ordinary elliptic curves with many small rational subgroups and large enough $\mathrm{Cl}(\mathcal{O})$, computing the class group action in CRS is rather slow. CSIDH [7, 3] significantly improved the efficiency of the CRS approach by considering the set of supersingular elliptic curves over a large prime field $\mathbf{F}_p$ and restricting to the $\mathbf{F}_p$-rational endomorphisms. These form a subring of the full endomorphism ring which again is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic number field. Since $\#E(\mathbf{F}_p) = p + 1$ for such supersingular elliptic curves, it now becomes trivial to force the existence of small rational subgroups by choosing $p$ such that $p + 1$ has small prime factors. The OSIDH protocol by Colò and Kohel [12] (and more rigorously by Onuki [27]) extended this even further by using oriented elliptic curves: here one considers elliptic curves together with an $\mathcal{O}$-orientation, which is simply an injective ring homomorphism $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$. OSIDH provides a convenient unifying framework for CRS and CSIDH, but also contains many new families of potential cryptographic interest. While the original Colò–Kohel proposal does not seem viable [15], a more recent proposal [16] looks promising.

A different approach to isogeny based cryptography is taken by SIDH [21], which relies on random walks in the isogeny graph of supersingular elliptic curves over $\mathbf{F}_{p^2}$. To make the protocol work however, it needs to reveal the action of the secret isogeny $\phi : E \to E'$ on a basis of $E[m]$, where $m$ typically is a power of 2 or 3. This extra information was recently exploited in a series of papers [30, 4, 23] resulting in a polynomial time attack on SIDH. This attack not only showed that SIDH is totally insecure, but also added a very powerful technique to the isogeny toolbox: it is possible to recover a secret isogeny $\phi : E \to E'$ between two elliptic curves $E$ and $E'$, all defined over a finite field $\mathbf{F}_q$, in polynomial time if the following information is available:

- the action of $\phi$ on a basis of $E[m]$ is given where $m$ is sufficiently smooth,
- the degree $d = \deg(\phi)$ is known and coprime with $m$,
- $m^2 > d$.

The origins of this paper trace back to the simple question: to what extent can the above technique be applied to the class group action setting and are there weak instances where this results in a polynomial time attack? To illustrate which problems need to be solved, we will focus on the CSIDH setting (the more general oriented case is deferred to later sections). In particular, assume $E$ and $E'$ are two supersingular elliptic curves over $\mathbf{F}_p$ connected by a secret isogeny $\phi : E \to E' := [\mathfrak{a}]E$ with $\ker(\phi) = E[\mathfrak{a}]$ and $\mathfrak{a} \subseteq \mathcal{O}$ an invertible ideal. To be able to apply the above technique to recover $\phi$, we need to know the degree of $\phi$ and its action on a basis of $E[m]$ for some smooth $m$.

Whether the degree of $\phi$ is known depends on how the class group action is implemented, e.g. in side-channel protected implementations, the degree is sometimes fixed and thus known. For example, this may be the case for the "dummy-free" constant-time variant of CSIDH that was proposed in [9]. In CSIDH variants that employ dummy computations to achieve constant-time, fault attacks that skip isogeny computations could allow an attacker to determine whether an isogeny was a dummy computation or not, and thus deduce information about the private key. In the dummy-free approach the parity of each secret exponent $e_i$ in CSIDH is fixed and sampled from an interval $[-e, e]$. For $e = 1$, which was suggested both in [9] and in [10], the degree of any secret isogeny is thus fixed to a publicly known value, i.e. the product of all the split primes used in the CSIDH group action. In the remainder of the paper, we will assume the degree of $\phi$ is known. Note that by construction, the degree is automatically smooth, so this does not impose a further restriction.

Determining the action of the secret isogeny $\phi$ on a basis of $E[m]$ for a chosen $m$ is a somewhat more challenging task, since we only have $E$, $E'$ and the degree of $\phi$ at our disposal. To make partial progress, note that we can choose $m = \ell^r$ for some small odd prime $\ell$ not dividing $d = \deg(\phi)$ that splits in $\mathbf{Q}(\sqrt{-p})$. Then $E[m]$ is spanned by two eigenspaces $\langle P\rangle, \langle Q\rangle$ of the Frobenius endomorphism $\pi_p$ corresponding to two different eigenvalues. Since $\phi$ commutes with $\pi_p$, $E'[m]$ will also be spanned by two eigenspaces $\langle P'\rangle, \langle Q'\rangle$ of $\pi_p$ on $E'$ corresponding to these same eigenvalues, so we already have that $\langle P'\rangle = \langle \phi(P)\rangle$ and $\langle Q'\rangle = \langle \phi(Q)\rangle$. In particular, there exist units $\lambda, \mu \in \mathbf{Z}/m\mathbf{Z}$ such that $P' = \lambda\phi(P)$ and $Q' = \mu\phi(Q)$. Using the independence of the points $P$ and $Q$ (resp. $P'$ and $Q'$) and compatibility of the classical Weil pairing $e_m$ with isogenies, we obtain

$$e_m(P', Q') = e_m(\lambda\phi(P), \mu\phi(Q)) = e_m(P, Q)^{\lambda\mu d}\,.$$

By computing a discrete logarithm (note that $\ell$ is assumed small, so computing the discrete logarithm is easy), we can therefore eliminate one variable, say $\mu$, since $d$ is assumed known, so we are left with determining $\lambda$. It is tempting to use the same trick again by pairing $P'$ with itself, which would lead to

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

Unfortunately, the classical Weil pairing $e_m$ results in a trivial self-pairing, i.e. we always have $e_m(P, P) = 1$. What we thus require is a non-trivial self-pairing $f_m$ compatible with isogenies, which implies $f_m(\phi(P)) = f_m(P)^d$, and thus $f_m(P') = f_m(P)^{\lambda^2 d}$, with both sides of order $m$ say. We thus recover $\lambda$ up to sign and as such we can recover $\pm\phi$. The existence of non-trivial self-pairings therefore is crucial to the success of the attack.

## Contributions

- We give a self-contained overview of generalized Weil [20] and Tate [2] pairings, filling some gaps in the existing literature and relating both pairings by extending a result in [20]. Although these generalized pairings are more powerful than the classical Weil and Tate pairings, they do not seem to be well known in the

cryptographic community.

- We formally define a cyclic self-pairing of order $m$ on an elliptic curve $E$ to be a homogeneous degree-2 function $f_m : C \to \mu_m$ with cyclic domain $C \subseteq E$ such that $\mathrm{im}(f_m)$ spans $\mu_m$. We derive necessary conditions for the existence of non-trivial cyclic self-pairings of order $m$ on $\mathcal{O}$-oriented elliptic curves that are compatible with oriented isogenies. In particular, we show that $m$ cannot be a multiple of the field characteristic and that $m \mid \Delta_\mathcal{O}$, with $\Delta_\mathcal{O}$ the discriminant of $\mathcal{O}$ (and even $2m \mid \Delta_\mathcal{O}$ if $4 \mid \Delta_\mathcal{O}$ and $4m \mid \Delta_\mathcal{O}$ if $8 \mid \Delta_\mathcal{O}$). Note that our results only apply to self-pairings compatible with isogenies, which is required to make the above attack work. This is in stark contrast to considering an individual elliptic curve, where non-trivial cyclic self-pairings of order $m$ always exist (as soon as $m$ is not a multiple of the field characteristic), e.g. by choosing any cyclic order-$m$ subgroup $C = \langle P \rangle$ and simply defining $f_m(\lambda P) = \zeta_m^{\lambda^2}$ with $\zeta_m$ some fixed primitive $m$-th root of unity.

- For $m$ satisfying these necessary conditions we construct cyclic self-pairings of order $m$ compatible with oriented isogenies, based on generalized Weil and Tate pairings.

- Using these non-trivial cyclic self-pairings, we are the first to identify weak instances of class group action based cryptography. In the best case, we obtain a polynomial time attack on the vectorization problem when $\deg(\phi)$ is known and powersmooth, $\ell^{2r} \mid q - 1$, $E(\mathbf{F}_q)[\ell^\infty]$ is cyclic of order at least $\ell^{2r}$, and $\ell^{2r} > \deg(\phi)$. This for instance would be the case if one would use a setup like SiGamal [26], but using the group action underlying CRS instead of CSIDH. Note however that our attack does not apply to SiGamal itself for two major reasons: here $\Delta_\mathcal{O} = -4p$ and the degree of the secret isogeny is not known.

- We present a more elegant version of existing results [8, 6] on the decisional Diffie–Hellman problem for class group actions. In particular, in Remark 5.5.3 we give a conceptual explanation for a phenomenon observed in [8, App. A]. This also illustrates why the general framework of oriented elliptic curves can be useful even if one is only interested in elliptic curves over $\mathbf{F}_q$ equipped with the natural Frobenius orientation.

## 5.2 Background

Throughout this paper, $k$ denotes a perfect field (e.g., a finite field $\mathbf{F}_q$) with algebraic closure $\overline{k}$, and $K$ is an imaginary quadratic number field with maximal order $\mathcal{O}_K$.

### 5.2.1 Oriented elliptic curves

Our main references are Colò–Kohel [12] and Onuki [27], although we present matters in somewhat greater generality (in the sense that we also cover non-supersingular

elliptic curves). A $K$-*orientation* on an elliptic curve $E/k$ is an injective ring homomorphism

$$\iota : K \hookrightarrow \mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q},$$

where $\mathrm{End}(E)$ denotes the full ring of endomorphisms of $E$ (i.e., defined over $\overline{k}$). The couple $(E, \iota)$ is called a $K$-*oriented elliptic curve*.

**Example 5.2.1** The standard example to keep in mind is that of an elliptic curve $E$ over a finite field $\mathbf{F}_q$ for which the $q$-th power Frobenius endomorphism $\pi_q$ is not a scalar multiplication (that is, we exclude supersingular elliptic curves $E/\mathbf{F}_{p^{2r}}$ on which Frobenius acts as $[\pm p^r]$). In that case we have an orientation

$$\iota : \mathbf{Q}(\sigma) \hookrightarrow \mathrm{End}^0(E) : \sigma \mapsto \pi_q, \qquad \sigma = \frac{t_E + \sqrt{t_E^2 - 4q}}{2} \tag{5.1}$$

with $t_E$ the trace of Frobenius of $E$ over $\mathbf{F}_q$. We call this the *Frobenius orientation*. If (and only if) $E$ is ordinary then $\iota$ is an isomorphism. If $E$ is supersingular then the image of $\iota$ is the subalgebra $\mathrm{End}_q^0(E) = \mathrm{End}_q(E) \otimes_{\mathbf{Z}} \mathbf{Q}$, with $\mathrm{End}_q(E)$ the ring of $\mathbf{F}_q$-rational endomorphisms of $E$. By abuse of notation, we will occasionally just identify $\sigma$ with $\pi_q$ and refer to $\iota$ as a $\mathbf{Q}(\pi_q)$-orientation. ☆

**Example 5.2.2** More generally, every endomorphism $\alpha \in \mathrm{End}(E) \setminus \mathbf{Z}$ naturally gives rise to an orientation. Indeed, such an endomorphism necessarily satisfies $\alpha^2 - t\alpha + n = 0$ where the trace $t = \mathrm{Tr}(\alpha)$ and the norm $n = N(\alpha)$ (which we recall is equal to the degree of $\alpha$) satisfy $t^2 - 4n < 0$. Fixing

$$\sigma = \frac{t + \sqrt{t^2 - 4n}}{2} \in \mathbf{C}$$

we obtain an orientation $\iota : \mathbf{Q}(\sigma) \hookrightarrow \mathrm{End}^0(E)$, which is unique if we impose that $\iota(\sigma) = \alpha$. Every orientation arises in this way. ☆

For an order $\mathcal{O} \subseteq K$, we say that a $K$-orientation $\iota : K \hookrightarrow \mathrm{End}^0(E)$ is an $\mathcal{O}$-*orientation* if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. If moreover $\iota(\mathcal{O}') \not\subseteq \mathrm{End}(E)$ for every strict superorder $\mathcal{O}' \supsetneq \mathcal{O}$ in $K$, then we say that it concerns a *primitive* $\mathcal{O}$-orientation. Note that any $K$-orientation $\iota$ is a primitive $\mathcal{O}$-orientation for a unique order $\mathcal{O} \subseteq K$, namely for the order $\iota^{-1}(\mathrm{End}(E))$. We call this order the *primitive order* for the $K$-orientation. Let us also introduce the following weaker notion:

**Definition 5.2.3** An $\mathcal{O}$-orientation on an elliptic curve $E/k$ is said to be *locally primitive* at a positive integer $m$ if the index of $\mathcal{O}$ inside the primitive order is coprime to $m$. △

The following is a convenient sufficient condition for local primitivity:

**Lemma 5.2.4** *Let $E/k$ be an elliptic curve, let $\sigma \in \mathrm{End}(E)$ and let $m$ be a positive*

*integer such that*

*(i)* $\mathrm{char}(k) \nmid m$,

*(ii)* $E[\ell, \sigma] \cong \mathbf{Z}/\ell\mathbf{Z}$ *for every prime divisor* $\ell \mid m$.

*Then the natural* $\mathbf{Z}[\sigma]$*-orientation on* $E$ *is locally primitive at* $m$*. As a partial converse, we have that this orientation is not locally primitive at* $m$ *as soon as* $E[\ell, \sigma] \cong \mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}$ *for some prime divisor* $\ell \mid m$.

*Proof.* If the orientation is not locally primitive at $m$, then we must have $(\sigma - a)/\ell \in \mathrm{End}(E)$ for a prime divisor $\ell \mid m$ and some $a \in \mathbf{Z}$. Thus $\sigma$ would act as multiplication-by-$a$ on $E[\ell]$. By assumption (ii) we necessarily have $a = 0$, but then $E[\ell, \sigma] = E[\ell] \cong \mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}$ in view of assumption (i): a contradiction. Conversely, if $E[\ell, \sigma] \cong \mathbf{Z}/\ell\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}$ then by [36, Cor. III.4.11] we know that there exists an $\alpha \in \mathrm{End}(E)$ such that $\alpha \circ [\ell] = \sigma$, so the primitive order must contain $\sigma/\ell$, hence the $\mathbf{Z}[\sigma]$-orientation is not locally primitive at $m$. □

**Example 5.2.5** The Frobenius orientation on an elliptic curve $E$ over a finite field $\mathbf{F}_q$ is also a $\mathbf{Z}[\pi_q]$-orientation. If $E(\mathbf{F}_q)[\ell] \cong \mathbf{Z}/\ell\mathbf{Z}$ for some prime number $\ell \nmid q$, then by Lemma 5.2.4 applied to $\sigma = \pi_q - 1$ this orientation is locally primitive at $\ell$. If $E[\ell] \subseteq E(\mathbf{F}_q)$ then it is not. ☆

If $\phi : E \to E'$ is an isogeny and if $\iota$ is a $K$-orientation on $E$, then we can define an induced $K$-orientation $\phi_*(\iota)$ on $E'$ by letting

$$\phi_*(\iota)(\alpha) = \frac{1}{\deg(\phi)} \phi \circ \iota(\alpha) \circ \hat{\phi}, \quad \forall \alpha \in K,$$

where $\hat{\phi}$ denotes the dual isogeny of $\phi$. Given two $K$-oriented elliptic curves $(E, \iota)$ and $(E', \iota')$, we say that an isogeny $\phi : E \to E'$ is $K$*-oriented* if $\iota' = \phi_*(\iota)$; in this case, we write $\phi : (E, \iota) \to (E', \iota')$. The dual of a $K$-oriented isogeny is automatically $K$-oriented as well. Two $K$-oriented elliptic curves $(E, \iota)$ and $(E', \iota')$ are called *isomorphic* if there exists an isomorphism $\phi : E \to E'$ such that $\phi_*(\iota) = \iota'$.

**Example 5.2.6** Let $E, E'$ be elliptic curves over $\mathbf{F}_q$ with the same trace of Frobenius, so that they can both be viewed as $K$-oriented elliptic curves with $K = \mathbf{Q}(\sigma)$ as in (5.1). Then an isogeny $\phi : E \to E'$ is $K$-oriented if and only if it is $\mathbf{F}_q$-rational. ☆

### 5.2.2 Class group actions

The set

$$\mathcal{Ell}_{\overline{k}}^{\mathrm{all}}(\mathcal{O}) = \{\, (E, \iota) \mid E \text{ ell. curve over } \overline{k}, \iota \text{ primitive } \mathcal{O}\text{-orientation on } E \,\}/\cong$$

of primitively $\mathcal{O}$-oriented elliptic curves over $\overline{k}$ up to isomorphism comes equipped with an action by the ideal class group of $\mathcal{O}$, which we denote by $\mathrm{Cl}(\mathcal{O})$. For elliptic

curves over $\mathbf{C}$ with complex multiplication, this is a classical result. The case where $k$ is a finite field and the orientation is by Frobenius is treated in [35, 38]. This group action, which we describe below in more detail, is free, but in general not transitive, see e.g. [35, Thm. 4.5] and [27, Prop. 3.3] for some subtleties. To avoid issues arising from the non-transitivity, we define

$$\mathcal{E}\ell\ell_{\overline{k}}(\mathcal{O}) \subseteq \mathcal{E}\ell\ell_{\overline{k}}^{\mathrm{all}}(\mathcal{O})$$

to be an arbitrary but fixed orbit (in practice, where we want to study a secret relation between two primitively $\mathcal{O}$-oriented elliptic curves, it will concern the orbit containing these two curves.)

The action is defined as follows. Let $(E, \iota)$ be a primitively $\mathcal{O}$-oriented elliptic curve and let $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$ be an ideal class, represented by an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm coprime to $\max\{1, \mathrm{char}(k)\}$; every ideal class admits such a representative by [14, Cor. 7.17]. One defines the $\mathfrak{a}$-torsion subgroup as

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

which turns out to be finite (of order $N(\mathfrak{a}) = \#(\mathcal{O}/\mathfrak{a})$, to be more precise). Thus there exists an elliptic curve $E'$ and a separable isogeny $\phi_{\mathfrak{a}} : E \to E'$ with $\ker(\phi_{\mathfrak{a}}) = E[\mathfrak{a}]$, which is unique up to post-composition with an isomorphism. The isomorphism class of $(E', \phi_{\mathfrak{a}*}(\iota))$ is independent of the choice of the representing ideal $\mathfrak{a}$. One then lets $[\mathfrak{a}](E, \iota)$ be this isomorphism class, and this turns out to define a free group action.

### 5.2.3 Horizontal, ascending and descending isogenies

Let $\ell \neq \mathrm{char}(k)$ be a prime number and consider an $\ell$-isogeny $\phi : (E_1, \iota_1) \to (E_2, \iota_2)$ of $K$-oriented elliptic curves. Let $\mathcal{O}_1 \subseteq K$ be the primitive order of $\iota_1$ and let $\mathcal{O}_2 \subseteq K$ be the primitive order of $\iota_2$. Then one of the following is true:

- $\mathcal{O}_1 \subseteq \mathcal{O}_2$ and $[\mathcal{O}_2 : \mathcal{O}_1] = \ell$, in which case $\phi$ is called *ascending*,
- $\mathcal{O}_1 = \mathcal{O}_2$, in which case $\phi$ is called *horizontal*,
- $\mathcal{O}_2 \subseteq \mathcal{O}_1$ and $[\mathcal{O}_1 : \mathcal{O}_2] = \ell$, in which case $\phi$ is called *descending*.

It is clear that the dual of an ascending isogeny is descending and vice versa. All horizontal isogenies are of the form $\phi_{\mathfrak{a}}$ for some invertible ideal $\mathfrak{a} \subseteq \mathcal{O}_1 = \mathcal{O}_2$ of norm $\ell$, with dual $\phi_{\overline{\mathfrak{a}}}$. Ascending isogenies are of the form $\phi_{\mathfrak{a}}$ for some *non*-invertible ideal $\mathfrak{a} \subseteq \mathcal{O}_1$ of norm $\ell$, while descending isogenies are not of the form $\phi_{\mathfrak{a}}$ at all.

## 5.3 Generalized Weil and Tate pairings

We review some properties of the generalized Weil and Tate pairings on elliptic curves, with a focus on how the latter can be defined in terms of the former. The main sources of inspiration for this section were papers by Bruin [2] and Garefalakis [20], although

now we should highlight the work by Robert [31, §4], which appeared near the submission time of the current article and takes this discussion to a deeper level. Nevertheless, while the following statements may be well-known to some experts, we did not succeed in pinpointing exact references for all of them, so we take the opportunity to fill some apparent gaps in the existing literature.

### 5.3.1 Weil pairing

Following [20] and [36, Ex. III.3.15], to any elliptic curve isogeny $\psi : E \to E'$ over a perfect field $k$ such that $\mathrm{char}(k) \nmid \deg(\psi)$ one can associate the *$\psi$-Weil pairing*

$$e_\psi : \ker(\psi) \times \ker(\hat{\psi}) \to \overline{k}^* : (P, Q) \mapsto \frac{g \circ \tau_P}{g},$$

where $\hat{\psi} : E' \to E$ denotes the dual of $\psi$. Here, $g \in k(E)$ is any function with divisor $\psi^*(Q) - \psi^*(0_{E'})$ and $\tau_P$ denotes the translation-by-$P$ map. It can be argued that $(g \circ \tau_P)/g$ is indeed constant. The $\psi$-Weil pairing takes values in $\mu_m$, with $m$ any positive integer such that $\ker(\psi) \subseteq E[m]$. When applied to the multiplication-by-$m$ map on an elliptic curve $E$ one recovers the classical $m$-Weil pairing, as it is defined in [36, §III.8].

**Lemma 5.3.1** *The $\psi$-Weil pairing is bilinear, non-degenerate,* $\mathrm{Gal}(\overline{k}, k)$*-invariant and further satisfies:*

1. Skew-symmetry: *for any isogeny $\psi : E \to E'$ we have*

$$e_\psi(P, Q) = e_{\hat{\psi}}(Q, P)^{-1} \qquad \text{for all } P \in \ker(\psi),\ Q \in \ker(\hat{\psi}),$$

2. Compatibility Weil-I: *for any chain of isogenies $E \xrightarrow{\phi} E' \xrightarrow{\psi} E''$ we have*

   (a) $e_{\psi\circ\phi}(P, Q) = e_\psi(\phi(P), Q) \qquad \text{for all } P \in \ker(\psi \circ \phi),\ Q \in \ker(\hat{\psi}),$

   (b) $e_{\psi\circ\phi}(P, Q) = e_\phi(P, \hat{\psi}(Q)) \qquad \text{for all } P \in \ker(\phi),\ Q \in \ker(\hat{\phi} \circ \hat{\psi}),$

3. Compatibility Weil-II: *for any positive integer $m$ and any isogeny $\phi : E \to E'$ we have*

$$e_m(\phi(P), Q) = e_m(P, \hat{\phi}(Q)) \qquad \text{for all } P \in E[m],\ Q \in E'[m].$$

*Proof.* We refer to [20, §2] and [36, Ex. III.3.15(c)] for bilinearity, non-degeneracy, Galois invariance and Compatibility Weil-I(a). Compatibility Weil-II is just a restatement of [36, III.Prop. 8.2]. Skew-symmetry is well-known in case $\psi = m$. The general case can be found in [31, §4.1], although this can also been seen as a consequence of the case $\psi = m$. Indeed, write $m = \deg(\psi)$ and pick any point $R \in E'$ such that $\hat{\psi}(R) = P$ and likewise pick any point $S \in E$ such that $\psi(S) = Q$. Observe that $R, S$

are $m$-torsion points. Then one checks that

$$e_\psi(P,Q) = e_\psi(\hat{\psi}(R),\psi(S)) = e_m(R,\psi(S)) = e_m(\psi(S),R)^{-1} = \\ e_m(S,\hat{\psi}(R))^{-1} = e_{\hat{\psi}}(\psi(S),\hat{\psi}(R))^{-1} = e_{\hat{\psi}}(Q,P)^{-1}$$

as wanted. Here the first and last equality use Compatibility Weil-I(a), the third equality uses skew-symmetry for the classical $m$-Weil pairing, and the fourth equality uses Compatibility Weil-II. Compatibility Weil-I(b) is an immediate consequence of Compatibility Weil-I(a) and skew-symmetry. □

For $\psi = m$ there is an equivalent definition of the Weil pairing which is more amenable to computation via Miller's algorithm [24].

**Lemma 5.3.2** *Let $P, Q \in E[m]$. Choose divisors*

$$D_P \sim (P) - (0_E) \qquad \text{and} \qquad D_Q \sim (Q) - (0_E)$$

*whose supports are disjoint from $\{(Q),(0_E)\}$ and $\{(P),(0_E)\}$, respectively. Let $f_{m,P}, f_{m,Q} \in k(E)$ be such that*

$$\mathrm{div}(f_{m,P}) = m(P) - m(0_E), \qquad \mathrm{div}(f_{m,Q}) = m(Q) - m(0_E).$$

*Then $e_m(P,Q) = (-1)^m f_{m,P}(D_Q)/f_{m,Q}(D_P)$.*

*Proof.* See e.g. [25]. □

There is no known analogue of this result for the more general $\psi$-Weil pairing; see [28, §3.6] for a discussion. Note that it is possible to relax the assumption on the supports of $D_P, D_Q$ by working with normalized functions, along the lines of [25, Def. 4].

### 5.3.2 Tate pairing

The literature describes a number of related pairings on elliptic curves that are all being referred to as the Tate pairing. We focus on the case $k = \mathbf{F}_q$. Following Bruin [2], to any $\mathbf{F}_q$-rational isogeny $\psi : E \to E'$ such that $\ker(\psi) \subseteq E[m] \subseteq E[q-1]$ we associate the $\psi$-Tate pairing

$$T_\psi : (\ker(\hat{\psi}))(\mathbf{F}_q) \times \frac{E'(\mathbf{F}_q)}{\psi(E(\mathbf{F}_q))} \to \mu_m \subseteq \mathbf{F}_q^*$$

defined by $T_\psi(P,Q) = e_{\hat{\psi}}(P, \pi_q(R) - R)$, where $R$ is arbitrary such that $\psi(R) = Q$. This is sometimes called the *reduced* Tate pairing in order to distinguish it from the Frey–Rück Tate pairing (see below); this terminology is particularly common in case $\psi = m$.

*Remark* 5.3.3 Bruin instead writes $e_\psi(\pi_q(R)-R,P)$, so in view of the skew-symmetry we appear to have inverted the pairing value; however, this inversion compensates for the fact that Bruin follows a different convention for the Weil pairing [2, §4]. In particular, our two definitions of the $\psi$-Tate pairing match. $\Diamond$

**Lemma 5.3.4** *The $\psi$-Tate pairing is bilinear, non-degenerate, $\mathrm{Gal}(\overline{\mathbf{F}}_q,\mathbf{F}_q)$-invariant and moreover satisfies:*

1. Compatibility Tate-I: *for any chain of $\mathbf{F}_q$-rational isogenies $E \xrightarrow{\phi} E' \xrightarrow{\psi} E''$ we have*

$$T_{\psi\circ\phi}(P,Q) = T_\psi(P,Q) \qquad \text{for all } P \in (\ker(\hat{\psi}))(\mathbf{F}_q)\ ,\ Q \in E''(\mathbf{F}_q),$$

2. Compatibility Tate-II: *for any positive integer $m$ and any $\mathbf{F}_q$-rational isogeny $\phi : E \to E'$ we have*

$$T_m(\phi(P),Q) = T_m(P,\hat{\phi}(Q)) \qquad \text{for all } P \in E[m](\mathbf{F}_q),\ Q \in E'(\mathbf{F}_q).$$

*Proof.* For compatibility Tate-I we note that

$$T_{\psi\circ\phi}(P,Q) = e_{\hat{\phi}\circ\hat{\psi}}(P,\pi_q(R)-R) = e_{\hat{\psi}}(P,\pi_q(\phi(R))-\phi(R))$$

for any $R$ such that $\psi(\phi(R)) = Q$; here we used Compatibility Weil-I(b) and the fact that $\phi$ is defined over $\mathbf{F}_q$. But this is indeed equal to $T_\psi(P,Q)$, because $\psi(\phi(R)) = Q$. Compatibility Tate-II is an immediate consequence of Compatibility Weil-II. $\square$

Notice that applying Compatibility Tate-I to $E' \xrightarrow{\phi} E \xrightarrow{\psi} E'$, where $\phi$ is such that $[m] = \psi\circ\phi$ (e.g., $\phi = \hat{\psi}$ in case $\psi$ is cyclic of degree $m$), shows that

$$T_\psi(P,Q) = T_m(P,Q) \qquad \text{for all } P \in (\ker(\hat{\psi}))(\mathbf{F}_q)\ ,\ Q \in E'(\mathbf{F}_q)$$

from which one sees that the $\psi$-Tate pairing is just a restriction of the $m$-Tate pairing. This is in stark contrast with the $\psi$-Weil pairing, whose relation to the $m$-Weil pairing is much more convoluted.

The following is an alternative interpretation of the $\psi$-Tate pairing in terms of the Weil pairing. This generalizes Garefalakis' main observation [20, §5].

**Proposition 5.3.5** *Consider an $\mathbf{F}_q$-rational isogeny $\psi : E \to E'$ between elliptic curves over $\mathbf{F}_q$ and assume that*

$$\ker(\psi) \subseteq E[q-1].$$

*Then we obtain a well-defined pairing*

$$\frac{E'(\mathbf{F}_q)}{\psi(E(\mathbf{F}_q))} \times (\ker(\hat{\psi}))(\mathbf{F}_q) \to \mathbf{F}_q^*$$

*from the* $(\pi_q - 1)$*-Weil pairing*

$$e_{\pi_q - 1} : E'(\mathbf{F}_q) \times \ker(\hat{\pi}_q - 1) \to \mathbf{F}_q^*$$

*on* $E'$*, by restricting the domain of the second argument to* $\ker(\hat{\pi}_q - 1) \cap \ker(\hat{\psi})$*. Moreover,*

$$T_\psi(P, Q) = e_{\pi_q - 1}(Q, P)^{-1}$$

*for all* $P \in (\ker(\hat{\psi}))(\mathbf{F}_q)$ *and* $Q \in E'(\mathbf{F}_q)$*.*

*Proof.* We first show that

$$\ker(\hat{\pi}_q - 1) \cap \ker(\hat{\psi}) = \ker(\pi_q - 1) \cap \ker(\hat{\psi}) = (\ker(\hat{\psi}))(\mathbf{F}_q).$$

Indeed, we have $\ker(\hat{\psi}) \subseteq E'[q-1]$ and $\#\ker(\pi_q - 1) = \#\ker(\hat{\pi}_q - 1) = q - t + 1$, with $t$ the trace of Frobenius. From this it follows that

$$\ker(\pi_q - 1) \cap \ker(\hat{\psi}),\ \ker(\hat{\pi}_q - 1) \cap \ker(\hat{\psi}) \ \subseteq\ E'[t-2].$$

Using that $(\hat{\pi}_q - 1) + (\pi_q - 1) = t - 2$, the desired equality follows.

Next, we observe that any point $Q \in (\ker(\hat{\psi}))(\mathbf{F}_q)$ pairs trivially with $\psi(P)$ for any $P \in E(\mathbf{F}_q)$:

$$e_{\pi_q - 1}(\psi(P), Q) = e_{(\pi_q - 1) \circ \psi}(P, Q) = e_{\psi \circ (\pi_q - 1)}(P, Q) = e_{\pi_q - 1}(P, \hat{\psi}(Q)) = 1,$$

where the first three equalities use Compatibility Weil-I(a), the rationality of $\psi$, and Compatibility Weil-I(b), respectively. So we indeed end up with a pairing whose domain coincides with that of $T_\psi$, up to reordering the factors.

Finally, to see that both pairings are each other's inverses, take $P \in (\ker(\hat{\psi}))(\mathbf{F}_q)$ and $Q \in E'(\mathbf{F}_q)$. From Compatibility Tate-I we know that

$$T_\psi(P, Q) = T_{\psi \circ (\pi_q - 1)}(P, Q) = e_{(\hat{\pi}_q - 1) \circ \hat{\psi}}(P, (\pi_q - 1)(R)) = e_{\hat{\psi} \circ (\hat{\pi}_q - 1)}(P, (\pi_q - 1)(R))$$

with $R$ such that $\psi \circ (\pi_q - 1)R = Q$. Compatibility Weil-I(b) allows us to rewrite this as

$$e_{\hat{\pi}_q - 1}(P, \psi((\pi_q - 1)(R))) = e_{\hat{\pi}_q - 1}(P, Q)$$

which indeed equals $e_{\pi_q - 1}(Q, P)^{-1}$ by skew-symmetry. □

We will extend this observation to a wider class of pairings in Section 5.5.

Following [18] and [31, §4.4–4.5] one can also consider the *Frey–Rück* $\psi$-Tate pairing

$$t_\psi : (\ker(\hat{\psi}))(\mathbf{F}_q) \times \frac{E'(\mathbf{F}_q)}{\psi(E(\mathbf{F}_q))} \to \frac{\mathbf{F}_q^*}{(\mathbf{F}_q^*)^m} : (P, Q) \mapsto f_{m,P}(D_Q)$$

with $f_{m,P}$ and $D_Q$ as in Lemma 5.3.2.[1] It allows for an efficient evaluation through

[1] It may seem suspicious, at first sight, that $f_{m,P}(D_Q)$ does not depend on $\psi$. However, here too,

Miller's algorithm. The Frey-Rück $\psi$-Tate pairing relates to the reduced $\psi$-Tate pairing $T_m$ via the rule

$$T_\psi(P,Q) = t_\psi(P,Q)^{(q-1)/m}, \tag{5.2}$$

see [2, §4] and [31, Rmk. 4.14], which is the reason for calling the former reduced. In particular, also $T_\psi$ can be evaluated efficiently.

*Remark* 5.3.6 It may be tempting to rephrase Lemma 5.3.2 as

$$e_m(P,Q) = t_m(P,Q)/t_m(Q,P),$$

however one should be careful with this: other representatives of $t_m(P,Q)$ and $t_m(Q,P)$ may fail to quotient to $e_m(P,Q)$. See [19, §IX.6] for a discussion. ♢

## 5.4 Self-pairings

In this section we analyze self-pairings, which we formally define as follows:

**Definition 5.4.1** A *self-pairing* on a finite subgroup $G$ of an elliptic curve $E/k$ is a homogeneous function

$$f : G \to \overline{k}^*$$

of degree 2. In other words, for all $P \in G$ and $\lambda \in \mathbf{Z}$ it holds that $f(\lambda P) = f(P)^{\lambda^2}$. △

As the terminology suggests, our primary examples come from the application of a bilinear pairing to a point and itself. More generally, it is natural to consider

$$f : G \to \overline{k}^* : P \mapsto e(\tau_1(P), \tau_2(P)) \tag{5.3}$$

for endomorphisms $\tau_1, \tau_2 \in \mathrm{End}(E)$ (possibly scalar multiplications), with $e$ a bilinear pairing on a group that contains $\tau_1(G) \times \tau_2(G)$.

**Example 5.4.2** Let $m \geq 2$ be an integer. The skew-symmetry of the classical Weil pairing implies that $e_m(P,P) = 1$ for any $P \in E[m]$. More generally, the $m$-Weil pairing becomes trivial whenever it is evaluated at two points belonging to the same cyclic subgroup $\langle P \rangle \subseteq E[m]$:

$$e_m(\tau_1 P, \tau_2 P) = e_m(P,P)^{\tau_1 \tau_2} = 1 \qquad \text{for any } \tau_1, \tau_2 \in \mathbf{Z}.$$

In particular, if one wants to build non-trivial self-pairings from the classical Weil pairing, then this requires the use of at least one non-scalar $\tau_i$. ☆

**Example 5.4.3** The following example is inspired by [19, p. 193]. Consider the elliptic curve $E : y^2 = x^3 + 1$ over a finite field $\mathbf{F}_q$ with $q \equiv 1 \bmod 3$. It comes equipped with

the Frey–Rück $\psi$-Tate pairing is just a restriction of the Frey–Rück $m$-Tate pairing.

the $\mathbf{F}_q$-rational automorphism $\tau : (x, y) \mapsto (\omega x, y)$, with $\omega$ a primitive $3^{\text{rd}}$ root of unity. Let $\ell \mid \#E(\mathbf{F}_q)$ be a prime satisfying $\ell \equiv 2 \bmod 3$. Then the self-pairing

$$E[\ell] \to \mathbf{F}_q^* : P \mapsto e_\ell(P, \tau(P))$$

takes non-trivial values for any $P \neq 0_E$. Indeed, every non-zero $P \in E[\ell]$ is mapped to an independent point because there are no non-trivial eigenvectors for the action of $\tau$ on $E[\ell]$: its characteristic polynomial $x^2 + x + 1$ is irreducible mod $\ell$. Since $\tau$ is defined over $\mathbf{F}_q$, this reasoning also proves that $E[\ell] \subseteq E(\mathbf{F}_q)$. ☆

**Example 5.4.4** As a more interesting example, consider an ordinary elliptic curve $E/\mathbf{F}_q$ with endomorphism ring $\mathbf{Z}[\pi_q]$, and assume $m \mid q - 1$. The natural reduction map $E(\mathbf{F}_q) \to E(\mathbf{F}_q)/m(E(\mathbf{F}_q))$ allows us to view the reduced $m$-Tate pairing as a bilinear map

$$T_m : E(\mathbf{F}_q)[m] \times E(\mathbf{F}_q) \to \mu_m. \tag{5.4}$$

By doing so, we may give up on the right non-degeneracy, but the pairing is still left non-degenerate, that is, for any non-trivial point $P \in E(\mathbf{F}_q)[m]$ there exists a point $Q \in E(\mathbf{F}_q)$ such that $T_m(P, Q) \neq 1$. Since $\mathrm{End}(E) = \mathbf{Z}[\pi_q]$, the group $E(\mathbf{F}_q)$ is cyclic (see [22, Thm. 1] or apply Lemma 5.2.4 to $\sigma = \pi_q - 1$). Thus, in this case, we have an induced self-pairing

$$E(\mathbf{F}_q) \to \mu_m : P \mapsto T_m(\tau P, P), \tag{5.5}$$

where $\tau$ denotes scalar multiplication by the index $[E(\mathbf{F}_q) : E(\mathbf{F}_q)[m]]$. This self-pairing is non-trivial as soon as $E(\mathbf{F}_q)[m]$ is non-trivial. Note that we can restrict the domain $E(\mathbf{F}_q)$ to its $m$-primary part $E(\mathbf{F}_q)[m^\infty]$ without affecting this property. ☆

*Remark* 5.4.5 By the definition of $T_m$, the image of (5.5) can be rewritten as

$$e_m\left(\tau P, \frac{\pi_q - 1}{m}(P)\right)$$

which seems to be an instance of (5.3) with $e$ the $m$-Weil pairing. However, note that $(\pi_q - 1)/m$ is *not* an endomorphism of $E$. On the other hand, it *does* descend (or rather ascend) to an endomorphism when considered on $E/\langle P \rangle$ and this is enough for the pairing to be defined unambiguously. Recall from Proposition 5.3.5 that (5.5) can also be rewritten as $e_{\pi_q - 1}(P, \tau P)^{-1}$. ◊

Our definition of a self-pairing a priori allows for maps that do *not* come from a bilinear pairing. This is indeed possible and, interestingly, a small example has appeared in the literature. Let $E$ be an elliptic curve over a finite field $\mathbf{F}_q$ with $q \equiv 1 \bmod 4$ and $\#E(\mathbf{F}_q) \equiv 2 \bmod 4$. Then the "semi-reduced Tate pairing"

$$E(\mathbf{F}_q)[2] \to \mu_4 : P \mapsto f_{2,P}(D_R)^{\frac{q^2-1}{4}}, \qquad 2R = P \tag{5.6}$$

from [8, Rmk. 11] maps $0_E$ to 1 and it sends the point of order 2 to a primitive 4-th

root of unity. Such an increase of order is impossible for self-pairings coming from a bilinear pairing along the recipe (5.3). Yet it is easy to check that this does concern a self-pairing.

This is essentially the oddest thing that can happen:

**Lemma 5.4.6** *Self-pairings map points of order $n$ to $\gcd(n,2)n$-th roots of unity.*

*Proof.* Let $f : G \to \overline{k}^*$ be a self-pairing on an elliptic curve $E$. Let $P \in G$ have order $n$. Then from

$$f(P)^{n^2} = f(nP) = f(0_E) = f(0 \cdot 0_E) = f(0_E)^{0^2} = 1$$

and

$$f(P)^{n^2+2n} = \frac{f(P)^{(n+1)^2}}{f(P)} = \frac{f((n+1)P)}{f(P)} = 1$$

it follows that the order of $f(P)$ divides $\gcd(n^2, n^2+2n) = \gcd(n,2)n$. □

Let us now bring isogenies into the picture. Indeed, as discussed in the introduction, self-pairings are only interesting if they are non-trivial and enjoy compatibility with a natural class of isogenies, in the following sense:

**Definition 5.4.7** Consider two elliptic curves $E, E'$ over $k$ equipped with respective self-pairings $f : G \to \overline{k}^*$, $f' : G' \to \overline{k}^*$ for finite subgroups $G \subseteq E$, $G' \subseteq E'$. Let $\phi : E \to E'$ be an isogeny. We say that $f$ and $f'$ are *compatible* with $\phi$ if

$$\phi(G) \subseteq G', \qquad f'(\phi(P)) = f(P)^{\deg(\phi)}$$

for all $P \in G$. △

The most powerful case is where the domains $G = \langle P \rangle$, $G' = \langle P' \rangle$ are cyclic: then we know that $\phi(P) = \lambda P'$ for some $\lambda \in \mathbf{Z}$ and we can conclude

$$f'(P')^{\lambda^2} = f(P)^{\deg(\phi)}, \tag{5.7}$$

leaking information about $\lambda$ if $\deg(\phi)$ is known and vice versa. We will sometimes refer to self-pairings with cyclic domains as *cyclic self-pairings*. In the non-cyclic case, extracting such information becomes more intricate, although in certain cases it may still be possible; see Remark 5.6.8. We note that the self-pairing from Example 5.4.4 is cyclic, and it follows from Compatibility Tate-II that it is compatible with horizontal $\mathbf{F}_q$-rational isogenies; more specifically (and more generally), if $m \mid q-1$ and $E$, $E'$ are elliptic curves over $\mathbf{F}_q$ such that the $m$-primary parts of $E(\mathbf{F}_q)$, $E'(\mathbf{F}_q)$ are cyclic, then the self-pairings

$$E(\mathbf{F}_q)[m^\infty] \to \mu_m : P \mapsto T_m(\tau P, P), \qquad E'(\mathbf{F}_q)[m^\infty] \to \mu_m : P \mapsto T_m(\tau P, P),$$

with $\tau = [E(\mathbf{F}_q) : E(\mathbf{F}_q)[m]] = [E'(\mathbf{F}_q) : E'(\mathbf{F}_q)[m]]$, are compatible with any $\mathbf{F}_q$-

rational isogeny $\phi : E \to E'$.

The focus of the current paper lies, more generally, on non-trivial cyclic self-pairings on $\mathcal{O}$-oriented elliptic curves, for some arbitrary (but fixed) imaginary quadratic order $\mathcal{O}$. If we merely impose compatibility with endomorphisms coming from $\mathcal{O}$, then this already imposes severe restrictions:

**Proposition 5.4.8** *Let $\mathcal{O}$ be an imaginary quadratic order with discriminant $\Delta_\mathcal{O}$ and let $(E, \iota)$ be an $\mathcal{O}$-oriented elliptic curve over $k$. Assume that there exists a self-pairing*

$$f : C \to \overline{k}^*$$

*on some finite cyclic subgroup $C \subseteq E$ which is compatible with endomorphisms in $\iota(\mathcal{O})$. In other words, for every $\sigma \in \mathcal{O}$ and every $P \in C$ we have*

$$\iota(\sigma)(P) \in C, \qquad f(\iota(\sigma)(P)) = f(P)^{N(\sigma)}.$$

*Write $m = \#\langle f(C)\rangle$. Then*

*(i)* $\mathrm{char}(k) \nmid m$,

*(ii)* $m \mid \Delta_\mathcal{O}$,

*(iii) with $r$ the 2-valuation of $\Delta_\mathcal{O}$, we have:*

- *if $r = 2$ then $m \mid \Delta_\mathcal{O}/2$,*
- *if $r \geq 3$ then $m \mid \Delta_\mathcal{O}/4$.*

*Remark* 5.4.9 Note that the image of a self-pairing is not necessarily a group, which is why we write $\langle f(C)\rangle$ rather than $f(C)$. ◊

*Proof.* Statement *(i)* follows immediately from the fact that $\overline{k}^*$ contains no elements of order $\mathrm{char}(k)$.

As for *(ii)* and *(iii)*, let $P$ be a generator of $C$. Then $f(P)$ has order $m$. For any $\sigma \in \mathcal{O}$ we have that $\iota(\sigma)(P) = \lambda_\sigma P$ for some $\lambda_\sigma \in \mathbf{Z}$, and via

$$f(P)^{N(\sigma)} = f(\iota(\sigma)(P)) = f(\lambda_\sigma P) = f(P)^{\lambda_\sigma^2}$$

we see that $N(\sigma) \equiv \lambda_\sigma^2 \bmod m$. Writing $s$ for the 2-valuation of $m$, we make a case distinction:

- If $s \leq 1$ then from Lemma 5.4.6 we see that some multiple $R$ of $P$ must have order $m$. Let $\sigma$ be such that $\mathcal{O} = \mathbf{Z}[\sigma]$. From

  $$(\sigma - \hat{\sigma})^2 R = (\sigma^2 + \hat{\sigma}^2 - 2N(\sigma))R = (\lambda_\sigma^2 + \lambda_{\hat{\sigma}}^2 - 2N(\sigma))R = (2N(\sigma) - 2N(\sigma))R = 0$$

  it follows that $m \mid \Delta_\mathcal{O}$ as wanted.

- If $s \geq 2$ then Lemma 5.4.6 only shows the existence of a point $R \in C$ of order $m/2$ and we obtain the weaker conclusion $m \mid 2\Delta_{\mathcal{O}}$. But at least this implies that $\Delta_{\mathcal{O}}$ is even, so we must have $r \geq 2$. Write $\Delta_{\mathcal{O}} = -2^r n$ and consider elements in $\mathcal{O}$ of the form
$$\sigma = \frac{\sqrt{\Delta_{\mathcal{O}}}}{2} + 2^t a \qquad a, t \in \mathbf{Z}_{\geq 0},$$
so that $N(\sigma) = 2^{r-2}n + 2^{2t}a^2$ has to be a square modulo $2^s$ for every choice of $a, t$. We distinguish further:
  - If $r$ is odd, then also $r-2$ is odd and taking $a = 0$ immediately shows that $s \leq r-2$, as wanted.
  - If $r$ is even, then taking $t = (r-2)/2$ yields that $n + a^2$ must be a square modulo $2^{s-r+2}$ for all $a$. If $s \geq r$ then this gives a contradiction both in case $n \equiv 1 \bmod 4$ (take $a = 1$) and in case $n \equiv 3 \bmod 4$ (take $a = 0$). So $s \leq r-1$.

  It remains to show that if $r \geq 4$ is even then in fact $s \leq r-2$. But if $s = r-1$ then taking $t = (r-4)/2$ yields that $4n + a^2$ must be a square modulo 8 for all $a$, which gives a contradiction (take $a = 0$).

□

We will refer to the quantity $m = \#\langle f(C)\rangle$ as the *order* of the self-pairing $f$. In the next section, we will show, by explicit construction, that the necessary conditions from Proposition 5.4.8 are in fact *sufficient* for the existence of a family of cyclic self-pairings
$$f_{(E,\iota)} : C_{(E,\iota)} \to \overline{k}^*, \qquad (E, \iota) \in \mathcal{E}\ell\ell_{\overline{k}}(\mathcal{O}),$$
all satisfying $\#\langle \mathrm{im}(f_{(E,\iota)})\rangle = m$ and compatible with horizontal isogenies (the family will also cover many non-primitively $\mathcal{O}$-oriented elliptic curves and non-horizontal isogenies; more on that in Section 5.5).

*Remark* 5.4.10 One may want to relax the assumptions from Proposition 5.4.8 and impose compatibility with endomorphisms whose norm is coprime to $m$ only. This is good enough for the applications we have in mind, and the semi-reduced Tate pairing from (5.6) shows that this is a strict relaxation. Indeed, we know from [8, Thm. 10] that it is compatible with $\mathbf{F}_q$-rational isogenies of odd degree, but there exist $\mathbf{F}_q$-rational endomorphisms of even degree for which compatibility fails: denoting the pairing by $f$, we see from
$$f(P) = \zeta_4 \qquad \text{and} \qquad f((\pi_q - 1)P) = f(0_E) = 1$$
that it cannot be compatible with the endomorphism $\pi_q - 1$, since $N(\pi_q - 1) = \#E(\mathbf{F}_q) \equiv 2 \bmod 4$. This concerns a self-pairing of order 4 on a $\mathbf{Z}[\pi_q]$-oriented elliptic curve, so it would not be allowed for by Proposition 5.4.8 because $\Delta_{\mathbf{Z}[\pi_q]} \equiv 4 \bmod 8$. In Appendix 5.8 we will prove a relaxed version of Proposition 5.4.8, and we will also show (in a non-effective fashion) that the above example is part of a larger class of

self-pairings of 2-power order that are compatible with $K$-oriented isogenies of odd degree only. $\Diamond$

## 5.5 Constructing non-trivial self-pairings

Let $\mathcal{O}$ be an order in an imaginary quadratic number field $K$ and let $m \mid \Delta_{\mathcal{O}}$ be a divisor satisfying the necessary conditions from Proposition 5.4.8:

- $\mathrm{char}(k) \nmid m$,
- if $4 \mid \Delta_{\mathcal{O}}$ then $m \mid \Delta_{\mathcal{O}}/2$,
- if $8 \mid \Delta_{\mathcal{O}}$ then $m \mid \Delta_{\mathcal{O}}/4$.

We will construct a family of cyclic self-pairings of order $m$, one for each $(E, \iota) \in \mathcal{Ell}_{\overline{k}}(\mathcal{O})$, which is compatible with all horizontal isogenies. More generally, the construction will apply to all $\mathcal{O}$-oriented elliptic curves $(E, \iota)$ for which the orientation is locally primitive at $m$, in the sense of Definition 5.2.3. Compatibility will hold for any $K$-oriented isogeny between two such curves. Our construction is based on a natural generalization of the $\psi$-Tate pairing to $\mathcal{O}$-oriented elliptic curves, which we discuss first. We will actually only rely on the cases where $\psi$ is a scalar multiplication, but the discussion is fully general for the sake of analogy with the $\psi$-Tate pairing.

### 5.5.1 A generalization of the $\psi$-Tate pairing

Let $m \geq 2$ be any integer that is invertible in $k$. Consider two $\mathcal{O}$-oriented elliptic curves $(E, \iota)$, $(E', \iota')$ and let $\psi : E \to E'$ be a $K$-oriented isogeny between them. Assume that $\ker(\psi) \subseteq E[m]$ and let $\sigma \in \mathcal{O}$ be such that

$$\mathrm{Tr}(\sigma) \equiv 0 \bmod \gcd(m, N(\sigma)). \tag{5.8}$$

We define

$$T_{\psi}^{\sigma} : (\ker(\hat{\psi}))[\sigma] \times \frac{E'[\sigma]}{\psi(E[\sigma])} \to \mu_m \subseteq \overline{k}^* : (P, Q) \mapsto e_{\hat{\psi}}(P, \sigma(R))$$

where $R \in E$ is such that $\psi(R) = Q$ and we abusingly write $\sigma$ instead of $\iota(\sigma), \iota'(\sigma)$. This is well-defined: indeed,

- we have $(\psi \circ \sigma)(R) = (\sigma \circ \psi)(R) = \sigma(Q) = 0_{E'}$, so $\sigma(R) \in \ker(\psi)$,
- making another choice for $R$ amounts to replacing $R \leftarrow R + T$ for some $T \in \ker(\psi)$, and

  $$e_{\hat{\psi}}(P, \sigma T) = e_{\hat{\sigma} \circ \hat{\psi}}(P, T) = e_{\hat{\psi} \circ \hat{\sigma}}(P, T) = e_{\hat{\psi}}(\hat{\sigma}(P), T) = e_{\hat{\psi}}((\mathrm{Tr}(\sigma) - \sigma)(P), T) = 1$$

where the first and third equalities use Compatibility Weil-I and the last equality follows from

$$P \in \ker(\hat{\psi}) \cap \ker(\sigma) \subseteq E'[m] \cap E'[N(\sigma)] = E'[\gcd(m, N(\sigma))].$$

The reader should notice the analogy with the definition of the $\psi$-Tate pairing from Section 5.3. Indeed, applying the above to elliptic curves over $\mathbf{F}_q$ equipped with the natural Frobenius orientation and to $\sigma = \pi_q - 1$, we exactly recover the $\psi$-Tate pairing; the assumption $m \mid q-1$ that was made there indeed implies (5.8), i.e. $\mathrm{Tr}(\pi_q - 1) \equiv 0 \bmod \gcd(m, N(\pi_q - 1))$.

The pairing $T_\psi^\sigma$ is bilinear and non-degenerate. Possibly the easiest way to verify this is by noting that the statement and proof of Proposition 5.3.5 carry over: we have

$$T_\psi^\sigma(P, Q) = e_\sigma(Q, P)^{-1}$$

for all $P \in (\ker(\hat{\psi}))[\sigma]$ and $Q \in E'[\sigma]$, so these properties follow from those of the generalized Weil pairing. Our pairing also satisfies the direct analogues of Compatibilities Tate-I and Tate-II:

1. for any chain of $K$-oriented isogenies $E \xrightarrow{\phi} E' \xrightarrow{\psi} E''$ between $\mathcal{O}$-oriented elliptic curves we have

$$T_{\psi\circ\phi}^\sigma(P, Q) = T_\psi^\sigma(P, Q) \qquad \text{for all } P \in (\ker(\hat{\psi}))[\sigma],\ Q \in E''[\sigma],$$

2. for any positive integer $m$ and any $K$-oriented isogeny $\phi : E \to E'$ between $\mathcal{O}$-oriented elliptic curves we have

$$T_m^\sigma(\phi(P), Q) = T_m^\sigma(P, \hat{\phi}(Q)) \qquad \text{for all } P \in E[m, \sigma],\ Q \in E'[\sigma].$$

Again the proofs are copies of the corresponding properties of the $\psi$-Tate pairing.

### 5.5.2 Self-pairings from divisors of the discriminant

Now consider $m \in \mathbf{Z}_{\geq 2}$ such that $m \mid \Delta_\mathcal{O}$, unless $m$ is even in which case we make the stronger assumptions that $2m \mid \Delta_\mathcal{O}$ in case $4 \mid \Delta_\mathcal{O}$, and $4m \mid \Delta_\mathcal{O}$ in case $8 \mid \Delta_\mathcal{O}$. Furthermore assume that $\mathrm{char}(k) \nmid m$. Pick any generator $\sigma \in \mathcal{O}$ such that

$$m \mid \mathrm{Tr}(\sigma), \tag{5.9}$$

except in the special case where $v_2(m) = 1$, in which case we want

$$2m \mid \mathrm{Tr}(\sigma) \text{ if } 8 \mid \Delta_\mathcal{O}, \qquad m \mid \mathrm{Tr}(\sigma) \text{ but } 2m \nmid \mathrm{Tr}(\sigma) \text{ if } 8 \nmid \Delta_\mathcal{O}. \tag{5.10}$$

Such a generator always exists. Indeed, if $m$ is odd then we can choose whatever generator $\sigma \in \mathcal{O}$ and replace it by $\sigma - (\mathrm{Tr}(\sigma))/2 \bmod m$ if needed. If $m$ is even and $8 \mid \Delta_\mathcal{O}$ then we can just take $\sigma = \sqrt{\Delta_\mathcal{O}}/2$, whose trace is exactly zero. If $m$ is even and $8 \nmid \Delta_\mathcal{O}$ then we can take $\sigma = \sqrt{\Delta_\mathcal{O}}/2 + m/2$, with trace $m$.

Conditions (5.9–5.10) trivially imply (5.8), so from the foregoing it follows that to any elliptic curve $E$ equipped with an $\mathcal{O}$-orientation we can associate the non-degenerate bilinear pairing

$$T_m^\sigma : E[m,\sigma] \times \frac{E[\sigma]}{m(E[\sigma])} \to \mu_m \subseteq \overline{k}^*,$$

and we know that this family of pairings is compatible with $K$-oriented isogenies. As with the standard reduced Tate pairing in Example 5.4.4, we can also view $T_m^\sigma$ as a left non-degenerate bilinear pairing $E[m,\sigma] \times E[m^\infty,\sigma] \to \mu_m$.

Now assume that the orientation is locally primitive at $m$. Then the group $E[m^\infty,\sigma]$ is cyclic: if it were not cyclic, we would have $E[m'] \subseteq E[m^\infty,\sigma]$ for some positive divisor $m' \mid m$, but this would mean that $\sigma/m' \in \mathrm{End}(E)$, contradicting that $\sigma$ is a generator of $\mathcal{O}$ and the orientation is locally primitive. Next, note that our assumptions (5.9–5.10) together with

$$\Delta_\mathcal{O} = (\mathrm{Tr}(\sigma))^2 - 4N(\sigma)$$

imply that $m \mid N(\sigma)$. Along with the fact that $E[m^\infty,\sigma]$ is cyclic, this in turn yields that $E[m,\sigma]$ is cyclic of order $m$. By the left non-degeneracy, we see that $T_m^\sigma$ is surjective onto $\mu_m$ and that, again as in Example 5.4.4, it can be converted into a self-pairing

$$f_{(E,\iota)} : E[m^\infty,\sigma] \to \mu_m : P \mapsto T_m^\sigma(\tau P, P)$$

still satisfying $\#\langle \mathrm{im}(f_{(E,\iota)})\rangle = m$; here $\tau$ is the index of $E[m,\sigma]$ in $E[m^\infty,\sigma]$. This proves the claims made at the beginning of this section.

### 5.5.3 Computing the self-pairings

For the practical applications we have in mind, our base field $k$ will be a finite field $\mathbf{F}_q$, and then a compelling question is: what is the complexity of evaluating the self-pairings constructed above? Concretely, for an $\mathcal{O}$-oriented elliptic curve $(E,\iota)$ such that both $E$ and $\iota(\mathcal{O})$ are defined over $\mathbf{F}_q$, and a divisor $m \mid \Delta_\mathcal{O}$ at which the orientation is locally primitive, how efficiently can we find an appropriate $\sigma \in \mathcal{O}$ and compute

$$T_m^\sigma(\tau P, P) = e_\sigma(P, \tau P)^{-1}$$

with $P$ a generator of $E[m^\infty,\sigma]$ and $\tau$ the index of $E[m,\sigma]$ inside $E[m^\infty,\sigma]$? Here, by "appropriate" we mean that $\sigma$ should satisfy conditions (5.9–5.10), but it is not necessary that $\sigma$ is a generator of $\mathcal{O}$, as long as the orientation by $\mathbf{Z}[\sigma]$ remains locally primitive at $m$.

**Example 5.5.1** The situation is particularly nice for the Frobenius orientation in case $m \mid q-1$ and $m \mid \#E(\mathbf{F}_q)$. From the identities $\mathrm{Tr}(\pi_q - 1) = (q-1) - \#E(\mathbf{F}_q)$, $N(\pi_q - 1) = \#E(\mathbf{F}_q)$ and $\Delta_\mathcal{O} = \mathrm{Tr}(\pi_q-1)^2 - 4N(\pi_q-1)$ it is easy to check that $m$ satisfies our necessary conditions for the existence of an order-$m$ self-pairing. Morover,

they show that $\sigma = \pi_q - 1$ meets conditions (5.9–5.10). If the orientation by $\mathbf{Z}[\pi_q]$ is locally primitive at $m$ then the resulting order-$m$ self-pairing

$$E(\mathbf{F}_q)[m^\infty] \to \mathbf{F}_q^* : P \mapsto T_m^{\pi_q - 1}(\tau P, P) = T_m(\tau P, P), \qquad \tau = \frac{\#E(\mathbf{F}_q)[m^\infty]}{m}$$

becomes an instance of the reduced $m$-Tate pairing, so it can be computed via the Frey–Rück Tate pairing $t_m$ as in (5.2). The latter can be evaluated efficiently using Miller's algorithm, in time $O(\log^2 m \log^{1+\varepsilon} q)$ using fast multiplication. ☆

**Example 5.5.2** An interesting case is where $\sigma = \varsigma/b$ for some integer $b \geq 2$, where $\varsigma$ is some easier endomorphism. Then it suffices to compute $T_m^\varsigma(\tau P, Q)$ for any $Q \in E$ such that $bQ = P$. Indeed:

$$T_m^\varsigma(\tau P, Q) = e_m(\tau P, \varsigma(R)) = e_m(\tau P, \frac{\varsigma}{b}(bR)) = T_m^\sigma(\tau P, P),$$

with $R$ such that $mR = Q$, so that $m(bR) = P$. E.g., if $\varsigma = \pi_q - 1$, then this again allows us to resort to the Frey–Rück Tate pairing. ☆

*Remark* 5.5.3 In the previous example the group $E[m^\infty, \varsigma]$, unlike $E[m^\infty, \sigma]$, may not be cyclic. This sheds a new and more conceptual light on the "not walking to the floor" appendix to [8]. There $m$ was taken to be a prime divisor of $q - 1$; for the sake of exposition, let us ignore the technical (and less interesting) case $m = 2$ in what follows. It was assumed that $E$ is an ordinary elliptic curve over $\mathbf{F}_q$ not located on the crater of its $m$-isogeny volcano, and that

$$E[m^\infty, \pi_q - 1] = E(\mathbf{F}_q)[m^\infty] \cong \frac{\mathbf{Z}}{m^r\mathbf{Z}} \times \frac{\mathbf{Z}}{m^s\mathbf{Z}}$$

for some $r > s + 1$. For us, the weaker assumptions $r > s$ and $m \mid \Delta_{\mathrm{End}(E)}$ will do. One then simply notes that $\sigma := (\pi_q - 1)/m^s \in \mathrm{End}(E)$ and that, when viewing $E$ as a $\mathbf{Z}[\sigma]$-oriented elliptic curve, the orientation becomes locally primitive at $m$. By the assumption on $\Delta_{\mathrm{End}(E)}$ we still have

$$m \mid \Delta_{\mathbf{Z}[\sigma]} \qquad \text{and consequently} \qquad \mathrm{Tr}(\sigma) \equiv 0 \bmod m,$$

where the last congruence uses $\Delta_{\mathbf{Z}[\sigma]} = \mathrm{Tr}(\sigma)^2 - 4N(\sigma) = \mathrm{Tr}(\sigma)^2 - 4 \cdot \#E(\mathbf{F}_q)/m^{2s}$. Thus we have a self-pairing

$$E[m^\infty, (\pi_q - 1)/m^s] \to \mu_m : P \mapsto T_m^{(\pi_q - 1)/m^s}(m^{r-s-1}P, P)$$

of order $m$, with cyclic domain $E[m^\infty, (\pi_q - 1)/m^s] \cong \mathbf{Z}/m^{r-s}\mathbf{Z}$. When computing this self-pairing via the standard $m$-Tate pairing as in Example 5.5.2, using $\varsigma = \pi_q - 1$ and $b = m^s$, we recover the pairing discussed in [8, App. A]. ◊

Unfortunately, for general $\sigma$ we do not know of an analogue of the Frey–Rück Tate

pairing, nor of an analogue of Lemma 5.3.2 for the generalized Weil pairing. The best methods we can currently think of work by embedding the pairing into a standard Weil pairing, that is, with respect to scalar multiplication. In this way Miller's algorithm becomes available. The embedding is natural via the definition:

$$T_m^\sigma(\tau P, P) = e_m(\tau P, \sigma(R))$$

with $R \in E$ such that $mR = P$. Alternatively, using compatibility Weil-I one can rewrite

$$e_\sigma(P, \tau P)^{-1} = e_{N(\sigma)}(P, \tau R)^{-1}$$

with $R \in E$ a preimage of $P$ under $\sigma$. Since $m$ is typically a lot smaller than $N(\sigma)$, and since evaluating $\sigma$ seems easier than computing a preimage, the first method appears to be preferable in practice.

The complexity then depends heavily on the field of definition of the points in $E[m^\infty, \sigma]$. In the worst case, one may need to unveil the full $N(\sigma)$-torsion to see these points, requiring to switch to $\mathbf{F}_{q^a}$ with $a$ the order of $\pi_q$ acting on $E[N(\sigma)]$, which is $O(N(\sigma)^2)$. We must also divide $P$ by $m$ to get $R$, for which we may need to extend further to

$$\mathbb{F}_{q^{aa'}} \quad \text{with } a' = O(m^2).$$

Running Miller's algorithm for the $m$-Weil pairing over $\mathbf{F}_{q^{aa'}}$ could then cost an atrocious

$$O(\Delta_{\mathcal{O}}^{2+\varepsilon} m^{2+\varepsilon} \log^{1+\varepsilon} q),$$

where we have approximated $N(\sigma) \approx \Delta_{\mathcal{O}}$.

However, this is the absolute worst case: one typically expects $E[m^\infty, \sigma] \subseteq E[m^t]$ for some very small constant $t$, most likely $t = 1$, and then the estimate becomes

$$O(m^{2t+2+\varepsilon} \log^{1+\varepsilon} q).$$

E.g., in Proposition 5.6.5 this will be applied to moduli $m$ of sub-exponential size, leading to a sub-exponential workload. We note that the above estimates ignore the cost of determining $\iota(\sigma)$ and evaluating it on $R$. This heavily depends on how the orientation is given in practice, which is a separate discussion for which we refer to [39].

## 5.6 Applications

In this section, we present two applications of the non-trivial self-pairings from Section 5.5. In Section 5.6.1, we show how knowledge of the degree of a secret isogeny together with a non-trivial self-pairing on a large enough subgroup allows us to efficiently attack certain instances of class group action based cryptography. In Section 5.6.2, we use the generalized view of self-pairings to conceptualize previous results on the decisional Diffie–Hellman problem for class group actions [8, 6].

### 5.6.1 Easy instances of class group action inversion

Using the tools developed in the previous sections, we describe a special family of class group actions on oriented elliptic curves for which the vectorization problem is easy, i.e., the class group action can be efficiently inverted. More precisely, we give a high-level recipe for recovering a secret horizontal isogeny $\phi$ between two primitively $\mathcal{O}$-oriented elliptic curves $(E, \iota)$, $(E', \iota')$ whenever $d = \deg(\phi)$ is known and smaller than $m^2$, where $m$ is a prime power satisfying

$$m^2 \mid \Delta_{\mathcal{O}} \text{ if } m \text{ is odd}, \qquad 4m^2 \mid \Delta_{\mathcal{O}} \text{ if } m \text{ is even}.$$

It is also assumed that $\gcd(m, \mathrm{char}(k), d) = 1$. While it has been previously pointed out that factors dividing the discriminant can cause a decrease of security, see e.g. [3, Rmk. 2] or [8, §5.1], it was unknown that in special cases they allow for a full break of the vectorization problem.

**Attack strategy.**

Let $\sigma \in \mathcal{O}$ be such that $\mathrm{Tr}(\sigma) \equiv 0 \bmod m^2$ and the orientation by $\mathbf{Z}[\sigma]$ is locally primitive at $m$. As discussed in Section 5.5.2 such a $\sigma$ exists and is easy to find; we can even choose $\sigma$ to be a generator of $\mathcal{O}$, but in certain cases one may want to take a non-generator for reasons of efficiency.[2]

Recall, again from Section 5.5.2, that the groups $E[m^\infty, \sigma]$ and $E'[m^\infty, \sigma]$ are cyclic and we obtain self-pairings

$$f : E[m^\infty, \sigma] \to \mu_{m^2} \qquad \text{and} \qquad f' : E'[m^\infty, \sigma] \to \mu_{m^2}$$

of order $m^2$ by mapping $P \mapsto T^{\sigma}_{m^2}(\tau P, P)$, where

$$\tau = [E[m^\infty, \sigma] : E[m^2, \sigma]] = [E'[m^\infty, \sigma] : E'[m^2, \sigma]].$$

Now, pick respective generators $P$, $P'$ of $E[m^\infty, \sigma]$, $E'[m^\infty, \sigma]$. Because $\phi$ is $K$-oriented and its degree is coprime to $m$, we know that $P' = \mu\phi(P)$ for some unit $\mu \in \mathbf{Z}/m^2\mathbf{Z}$. The compatibility of $f$ and $f'$ with $K$-oriented isogenies then implies

$$f'(P') = f(P)^{d\mu^2}.$$

Knowing $d$, we can determine $\mu^2 \bmod m^2$ using a discrete logarithm computation in $\mu_{m^2}$, which leaves at most four options for $\mu \bmod m^2$: two options if $m$ is odd and four options if $m$ is a power of 2. Given a correct guess for $\mu \bmod m^2$, we obtain knowledge of pair of points

$$Q = \mu\tau P \qquad \text{and} \qquad Q' = \tau P'$$

of order $m^2$ that are connected via $\phi$.

[2] For instance, to allow for $\sigma$ of the form $(\pi_q - 1)/b$ as in Example 5.5.2.

*Remark* 5.6.1 Guessing $-\mu$ is in fact equally fine, because it is of course good enough to recover $-\phi = [-1] \circ \phi$. Therefore, only in the case where $m$ is a power of 2 there is an actual need for guessing between $\pm\mu$ and $\pm(1 + m^2/2)\mu$, where we have to repeat the procedure below in case of a wrong guess. ◊

Using a reduction by De Feo et al.,[3] the problem of recovering $\phi$ given its images on the cyclic subgroup $\langle Q \rangle$ of order $m^2$ can be reduced to the problem of recovering a related degree-$d$ isogeny $\phi_0 : E_0 \to E_0'$ given its images on $E_0[m]$. The idea is to compute the isogenies $\psi : E \to E_0$, $\psi' : E' \to E_0'$ with kernels generated by $mQ$ and $m\phi(Q)$, respectively, and complete the diagram:

$$\begin{array}{ccc} E_0 & \xrightarrow{\phi_0} & E_0' \\ {\scriptstyle\psi}\uparrow & & \uparrow{\scriptstyle\psi'} \\ E & \xrightarrow{\phi} & E' \end{array}$$

The points $Q_0 := \psi(Q)$ and $Q_0' := \psi'(Q') = \psi'(\phi(Q))$ are of order $m$ and we have $\phi_0(Q_0) = Q_0'$. Further, by picking any generator $R_0$ of $\ker(\hat{\psi})$ we obtain a basis $\{Q_0, R_0\}$ of $E_0[m]$. If we choose a generator $R_0'$ of $\ker(\hat{\psi}')$ then it is easy to argue that $R_0' = \lambda\phi_0(R_0)$ for some $\lambda \in \mathbf{Z}$ that is coprime to $m$. The exact value of $\lambda \bmod m$ can be recovered via a discrete logarithm computation by comparing

$$e_m(Q_0', R_0') = e_m(\phi_0(Q_0), \lambda\phi_0(R_0)) = e_m(Q_0, R_0)^{\lambda d} \quad \text{with} \quad e_m(Q_0, R_0),$$

hence we can assume that $\lambda = 1$. Thus, we are given the images of $\phi_0$ on a basis of $E_0[m]$. Since $m^2 > d$, we can use Robert's method from [30, §2], together with the refinement discussed in [30, §6.4], to evaluate $\phi_0$ on arbitrary inputs. In particular, we can evaluate $\phi_0$ on a basis of $E_0[d]$ in order to determine the kernel of $\phi_0$ explicitly; this kernel can then be pushed through $\hat{\psi}$ to obtain the kernel of $\phi$.

*Remark* 5.6.2 In our main use cases, namely attacking special instances of CRS, rather than evaluating $\phi_0$ on a basis of $E_0[d]$ (which may be defined over a huge field extension only) we want to proceed as follows. For simplicity, let us focus on the dummy-free set-up with $e = 1$ (see Section 5.1). Then we have $d = \ell_1\ell_2\cdots\ell_r$ for distinct small primes $\ell_i$ that split in $\mathcal{O}$. In this context, recovering $\phi$ amounts to finding for each $i = 1, 2, \ldots, r$ the prime ideal $\mathfrak{l}_i$ above $\ell_i$ (one out of two options) for which $E[\mathfrak{l}_i]$ is annihilated by $\phi$. Then $\phi$ is the isogeny corresponding to the invertible ideal $\mathfrak{l}_1\mathfrak{l}_2\cdots\mathfrak{l}_r \subseteq \mathcal{O}$. Since $\gcd(m, d) = 1$ this can be tested directly on $E_0$ by evaluating $\phi_0$ in a generator of $\psi(E[\mathfrak{l}_i])$. ◊

[3] The reduction was presented at the KU Leuven isogeny days in 2022 and an article about this is in preparation [17].

**Weak instances over $\mathbf{F}_q$.**

Whether or not the above strategy turns into an efficient algorithm depends amongst others on the field arithmetic involved, the cost of evaluating $\iota(\sigma)$, $\iota'(\sigma)$, and the cost of computing discrete logarithms in $\mu_{m^2}$. The following proposition gives instances where it indeed leads to a polynomial-time attack:

**Proposition 5.6.3** *Let $E$, $E'$ be elliptic curves defined over a finite field $\mathbf{F}_q$, equipped with their Frobenius orientations and connected by an unknown horizontal isogeny $\phi$ of known degree $d$, assumed $B$-powersmooth and coprime to $q$. Let $\mathcal{O} \subseteq \mathbf{Q}(\pi_q)$ be their joint primitive order. Assume that there exists a prime power $m = \ell^r$ satisfying $\ell \leq B$, $\ell \nmid qd$, $\ell^{2r} > d$, and*

$$\ell^{2r} \mid \Delta_{\mathcal{O}} \text{ if } \ell \text{ is odd}, \qquad \ell^{2r+2} \mid \Delta_{\mathcal{O}} \text{ if } \ell = 2.$$

*Further, assume that there exists a positive integer $b$ coprime to $q$ such that $\sigma = (\pi_q - 1)/b \in \mathcal{O}$, $\mathrm{Tr}(\sigma) \equiv 0 \bmod \ell^{2r}$ and $\ell \nmid [\mathcal{O} : \mathbf{Z}[\sigma]]$. Then the invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ for which $\phi = \phi_{\mathfrak{a}}$ can be computed in time* $\mathrm{poly}(\log q, B)$.

*Proof.* First note that

$$d = O(m^2) = O(|\Delta_{\mathcal{O}}|) \quad \text{and} \quad |\Delta_{\mathcal{O}}| = (4q - \mathrm{Tr}(\pi_q)^2)/[\mathcal{O} : \mathbf{Z}[\pi_q]]^2 = O(q)$$

so any subroutine which runs in time $\mathrm{poly}(d, m)$ also runs in time $\mathrm{poly}(q)$. The orientation by $\mathbf{Z}[\sigma]$ being locally primitive at $\ell$, we know that

$$E(\mathbf{F}_q) \cong E'(\mathbf{F}_q) \cong \frac{\mathbf{Z}}{bb'\mathbf{Z}} \times \frac{\mathbf{Z}}{bb'c\mathbf{Z}}$$

for positive integers $b', c$, where $\ell \nmid b'$, that can be determined in time $\mathrm{poly}(\log q)$ using a point-counting algorithm [34]. Define $\kappa = \gcd(\ell^\infty, c)$, where we note that our assumptions imply that $\ell^{2r} \mid \kappa$: indeed recall from Section 5.5.2 that $E[\ell^{2r}, \sigma] \subseteq E[\sigma] \cong \mathbf{Z}/b'\mathbf{Z} \times \mathbf{Z}/b'c\mathbf{Z}$ has order $\ell^{2r}$. A generator $P \in E[\ell^\infty, \sigma]$ is found by repeatedly sampling $X \leftarrow E(\mathbf{F}_q)$ until $P = \frac{bb'c}{\kappa} X$ has order $\kappa$. Following Example 5.5.2, the self-pairing

$$f(P) = T^{\sigma}_{\ell^{2r}}(\tau P, P) = T^{\frac{\pi_q - 1}{b}}_{\ell^{2r}}(\tau P, P) = T_{\ell^{2r}}(\tau P, \frac{b'c}{\kappa} X), \qquad \tau = \frac{\kappa}{\ell^{2r}}$$

can then be computed in time $\mathrm{poly}(\log q)$ via the Frey–Rück Tate pairing. Likewise, we can efficiently evaluate $f'$ at a generator $P' \in E'[\ell^\infty, \sigma]$, necessarily satisfying $P' = \mu\phi(P)$ for some $\mu$. As outlined above, via a discrete logarithm computation in $\mu_{\ell^{2r}}$, which can be done in time $\mathrm{poly}(\log q, B)$, we obtain $\mu^2 \bmod \ell^{2r}$. Assuming a correct guess for $\mu$, from this we obtain our order-$\ell^{2r}$ points $Q$, $Q' = \phi(Q)$ and we are all set for the torsion-point attack. Note that the points $Q, Q'$ are defined over $\mathbf{F}_q$, hence so are the curves $E_0$, $E_0'$ and evaluating $\phi_0$ at a point in $E_0(\mathbf{F}_{q^a})$ only involves arithmetic over $\mathbf{F}_{q^a}$. We then proceed as outlined in Remark 5.6.2, with the difference

that $d$ need not be square-free: we only require it to be powersmooth. This means that for each prime power $\ell_i^{e_i}$ dividing $d$, we have to test up to $2^{e_i} - 1 = O(B)$ ideals of norm $\ell_i^{e_i}$ for annihilation by $\phi_0$. All arithmetic can be done in an extension of degree $a = \text{poly}(B)$, from which the proposition follows. □

**Example 5.6.4** An example application of Proposition 5.6.3 is where $\ell^{2r} \mid q - 1$ for a small prime $\ell$ and $r \geq 1$ and $E(\mathbf{F}_q)[\ell^\infty]$ is cyclic of order at least $\ell^{2r}$. Then $m := \ell^r$ and $\sigma := \pi_q - 1$ meet the above requirements. Indeed:

- the orientation by $\mathbf{Z}[\pi_q - 1]$ is locally primitive at $\ell$ by Lemma 5.2.4,
- $\text{Tr}(\pi_q - 1) = q - 1 - \#E(\mathbf{F}_q) \equiv 0 \bmod \ell^{2r}$,
- $\Delta_{\mathbf{Z}[\pi_q - 1]} = \text{Tr}(\pi_q - 1)^2 - 4\#E(\mathbf{F}_q)$ is divisible by $\ell^{2r}$, and by $\ell^{2r+2}$ if $\ell = 2$.

Here is a baby example with $\ell = 2$. Let $E$ be the ordinary elliptic curve defined by

$$y^2 = x^3 + 106960359001385152381x + 100704579394236675333$$

over $\mathbf{F}_p$ with $p := 2^{30} \cdot 167133741769 + 1$. So here we take $\sigma := \pi_p - 1$ and $m := 2^{15}$. One checks that $E[\sigma] = E(\mathbf{F}_p)$ is a cyclic group of order

$$2^{30} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31,$$

in particular its subgroup $E(\mathbf{F}_p)[2^\infty]$ is cyclic of order $2^{30}$ as wanted. In this case it is easy to check that the $\mathbf{Z}[\sigma]$-orientation is primitive overall, i.e., not just locally at 2. This is a minimal example for a curve one would construct for a SiGamal-type encryption scheme [26] using the group action underlying CRS instead of the CSIDH group action; see below. By Proposition 5.6.3, one can recover horizontal isogenies of known powersmooth degree $d < 2^{30}$. We implemented the attack in the Magma computer algebra system [1],[4] only skipping the final step, i.e. computing the actual evaluation algorithm as described in [30]. ☆

**A generalization.**

The above recipe can be generalized to the case where multiple squared prime powers $m_1^2, \ldots, m_r^2$ divide $\Delta_\mathcal{O}$ and the degree $d$ of our secret isogeny $\phi$ is known and smaller than $m_1^2 \cdots m_r^2$. This time we use a cyclic self-pairing of order $m_1^2 \cdots m_r^2$ to recover $\mu^2 \bmod m_1^2 \cdots m_r^2$, with $\mu$ as before. Thus, we have $2^r$ or $2^{r+1}$ options for $\mu$ depending on whether one of the $m_i$ is even (or in fact $2^{r-1}$ or $2^r$ options in case we do not care about a global sign). The rest of the recipe follows mutatis mutandis.

**Proposition 5.6.5** (informal) *Let $E, E'$ be elliptic curves defined over a finite field $\mathbf{F}_q$, equipped with their Frobenius orientations and connected by an unknown horizontal isogeny $\phi$ of known degree $d$, assumed $B$-powersmooth and coprime to $q$. Let $\mathcal{O} \subseteq$*

[4] See `https://github.com/KULeuven-COSIC/Weak-Class-Group-Actions` for the code.

$\mathbf{Q}(\pi_q)$ *be their joint primitive order. Assume that there exist* $r \approx \sqrt{\log q}$ *prime powers* $m_1, \dots, m_r \in L_q(1/2)$ *coprime to* $qd$ *such that* $m_1^2 \cdots m_r^2 > d$ *and*

$$m_1^2 \cdots m_r^2 \mid \Delta_{\mathcal{O}} \qquad \text{and} \qquad 4m_1^2 \cdots m_r^2 \mid \Delta_{\mathcal{O}} \text{ if some } m_i \text{ is even.}$$

*Then it is expected that the invertible ideal* $\mathfrak{a} \subseteq \mathcal{O}$ *for which* $\phi = \phi_{\mathfrak{a}}$ *can be computed in time* $\mathrm{poly}(B) \cdot L_q(1/2)$.

*Proof sketch.* Let $\sigma \in \mathcal{O}$ be such that $\mathrm{Tr}(\sigma) \equiv 0 \bmod m_1^2 \cdots m_r^2$ and the orientation by $\mathbf{Z}[\sigma]$ is locally primitive at $m_1 \cdots m_r$. If it so happens that $\sigma = (\pi_q - 1)/b$ for some $b$ coprime to $q$ then we can just mimic the previous proof: the main difference is that, this time, there are about $2^r \approx 2^{\sqrt{\log q}} = L_q(1/2)$ possible guesses for the secret scalar $\mu$, from which the stated runtime follows.

In general however, it may not be possible to pick $\sigma$ of the said form, and then the domains $E[(m_1 \cdots m_r)^\infty, \sigma]$ and $E'[(m_1 \cdots m_r)^\infty, \sigma]$ of our self-pairings may be defined over a field extension of degree $L_q(1)$ only, in which case there is no hope for a sub-exponential runtime. For this reason, the attack should be broken up in pieces. Writing $m_1^{t_1} \cdots m_r^{t_r}$ for the order of $E[(m_1 \cdots m_r)^\infty, \sigma] \cong E'[(m_1 \cdots m_r)^\infty, \sigma]$, as discussed in Section 5.5.3 we heuristically expect that $t_i = O(1)$ for all $i = 1, \dots, r$. If this is indeed the case, then for each $i$ we can find generators $P_i \in E[m_i^\infty, \sigma]$, $P_i' \in E'[m_i^\infty, \sigma]$ over an extension of degree $L_q(1/2)$. The cyclic self-pairings

$$T^\sigma_{m_i^2}(\tau P, P) \quad \text{and} \quad T^\sigma_{m_i^2}(\tau P', P'), \qquad \tau = m_i^{t_i - 2}$$

can thus be computed in time $L_q(1/2)$ and this also accounts for the subsequent discrete logarithm computation. Assuming a correct guess for the scalar $\mu_i$ such that $P_i' = \mu_i \phi(P_i)$, we obtain a pair of order-$m_i^2$ points $Q_i$, $Q_i' = \phi(Q_i)$. Note that, while these points are defined over an extension of degree $L_q(1/2)$, the groups they generate are $\mathbf{F}_q$-rational because our orientation is by Frobenius. In particular, the isogenies $\psi_1$, $\psi_1'$ and codomains $E_{0,1}$, $E_{0,1}'$ corresponding to $Q_1, Q_1'$ are defined over $\mathbf{F}_q$. The idea is now to push the points $Q_2, Q_2'$ through $\psi_1, \psi_1'$ and repeat the argument, leading to a diagram

$$\begin{array}{ccc} E_{0,r} & \xrightarrow{\phi_0} & E'_{0,r} \\ {\scriptstyle\psi_r}\uparrow & & \uparrow{\scriptstyle\psi'_r} \\ \vdots & & \vdots \\ {\scriptstyle\psi_1}\uparrow & & \uparrow{\scriptstyle\psi'_1} \\ E & \xrightarrow{\phi} & E' \end{array}$$

The map $\phi_0$ on top comes equipped with its images on a basis of $E_{0,r}[m_i]$ for each $i = 1, \dots, r$. For the evaluation of $\phi_0$ on arbitrary inputs, we can then proceed as in [29, Prop. 2.9] and conclude as before. □

### Unaffected schemes.

From the above propositions it follows that a CRS-instantiation using curves whose discriminants are divisible by (large) powers of smallish primes may be vulnerable to a sub-exponential attack. In particular, from a security point of view, walking down the volcano to instantiate CRS is worse than CRS close to the crater. Each descending step on the $\ell$-volcano adds a factor $\ell^2$ to our discriminant and thus we can recover isogenies of degree $\ell^2$ times larger than a level above, using the attack outlined in this section. We examine how some proposed constructions avoid this problem already.

Schemes that use the maximal order as their orientation are not vulnerable to our attack. We need that a prime power, not a prime, divides the discriminant, because the De Feo et al. reduction works only for points of square order. The maximal order has a discriminant that is square-free, at worst after dividing by 4, so the above does not apply. The CSIDH variant CSURF is an example of a scheme that uses the maximal order [3], where the discriminant is not merely square-free but even prime. Similarly, in the original CSIDH proposal the discriminant is four times a large prime and thus there is no factor of the discriminant large enough to enable our attack.

Schemes that are close to the crater are also secure. For instance, the SCALLOP scheme [16] uses curves one level underneath the crater in the $f$-volcano, where $f$ is a large prime. Thus the discriminant is of the form $f^2 \cdot d$, where $d$ is square-free away from 4. Theoretically, we can still use a point of order $f^2$ to recover an isogeny of degree at most $f^2$. However, to actually see the $f$-torsion we would need to pass to an extension of degree $O(f)$, which is infeasible for large enough $f$.

Another scheme worth mentioning is the higher-degree supersingular group actions [11]. Here the order used is $\mathbf{Z}[\sqrt{-dp}]$ for some square-free $d$, which has discriminant $-dp$ or $-4dp$. Even if $d$ was a square, $d$ is chosen small relative to $p$, and as such applying the attack above to these orientations, we could recover an isogeny of degree $2d$ at best.

### Pairing-based attack strategy on SiGamal.

We end by commenting on a strategy, proposed to us by Luca De Feo and involving self-pairings, to break the IND-CPA security of the SiGamal public-key encryption scheme [26]. In SiGamal, the hardness of the IND-CPA game – i.e., given the encryption of one out of two known plaintexts, guessing which one has been encrypted – relies [26, Thm. 8] on an *ad hoc* assumption called the *P-CSSDDH assumption.*

More precisely, let $p$ be a prime of the form $2^r\ell_1 \cdots \ell_n - 1$, where $r \geq 2$ and $\ell_1, \ldots, \ell_n$ are distinct odd primes. Moreover, let $E_0$ be the supersingular elliptic curve over $\mathbf{F}_p$ of equation $y^2 = x^3 + x$, $P_0$ a random generator of $E_0(\mathbf{F}_p)[2^r]$ and $\mathfrak{a}, \mathfrak{b}$ random elements of odd norm in $\mathrm{Cl}(\mathbf{Z}[\pi_p])$. Then the P-CSSDDH assumption is as follows: given the curves $E_0, [\mathfrak{a}]E_0, [\mathfrak{b}]E_0, [\mathfrak{ab}]E_0$ and the points $P_0, P_1 = \phi_{\mathfrak{a}}(P_0)$ and $P_2 = \phi_{\mathfrak{b}}(P_0)$, no efficient algorithm can distinguish $P_3 = \phi_{\mathfrak{ab}}(P_0)$ from a uniformly random $2^r$-torsion point $P_3' \in [\mathfrak{a}][\mathfrak{b}]E_0(\mathbb{F}_p)$. Schematically:

$$\begin{array}{ccc} (E_0, P_0) & \xrightarrow{\quad\mathfrak{a}\quad} & ([\mathfrak{a}]E_0, P_1 = \phi_{\mathfrak{a}}(P_0)) \\ \Big\downarrow{\scriptstyle \mathfrak{b}} & & \Big\downarrow{\scriptstyle \mathfrak{b}} \\ ([\mathfrak{b}]E_0, P_2 = \phi_{\mathfrak{b}}(P_0)) & \xrightarrow[\quad\mathfrak{a}\quad]{} & ([\mathfrak{a}\mathfrak{b}]E_0, P_3 = \phi_{\mathfrak{a}\mathfrak{b}}(P_0), P_3') \end{array}$$

If there existed (efficiently computable) non-trivial self-pairings $f_i$ on the subgroups $\langle P_i \rangle$, say of order $2^s$, compatible with $\mathbf{F}_p$-rational isogenies of odd degree, then

$$\begin{aligned} f_1(P_1) &= f_1(\phi_{\mathfrak{a}}(P_0)) = f_0(P_0)^{N(\mathfrak{a})} \\ f_2(P_2) &= f_2(\phi_{\mathfrak{b}}(P_0)) = f_0(P_0)^{N(\mathfrak{b})} \\ f_3(P_3) &= f_3(\phi_{\mathfrak{a}\mathfrak{b}}(P_0)) = f_0(P_0)^{N(\mathfrak{a})N(\mathfrak{b})}. \end{aligned}$$

Thus, the P-CSSDDH challenge could then be reduced to a decisional Diffie–Hellman problem on $\mu_{2^s}$. However, the existence of such self-pairings $f_i$ is ruled out by Propositions 5.4.8 and 5.8.1. Since $\Delta_{\mathcal{O}} = -4p$ and $p \equiv 3 \bmod 4$ by construction, we are condemned to $s = 2$. This is of no use since $\mathfrak{a}$ and $\mathfrak{b}$ are assumed to have odd norm.

### 5.6.2 Decisional Diffie–Hellman revisited

Genus theory [14, Ch. I§3B] attaches to every imaginary quadratic order $\mathcal{O}$ a list of *assigned characters*, which form a set of generators for the group of quadratic characters $\chi : \mathrm{Cl}(\mathcal{O}) \to \{\pm 1\}$. In detail: if

$$\Delta_{\mathcal{O}} = -2^r m_1^{r_1} m_2^{r_2} \cdots m_n^{r_n}$$

denotes the factorization of $\Delta_{\mathcal{O}}$ into prime powers, then the assigned characters include

$$\chi_{m_i} : [\mathfrak{a}] \mapsto \left(\frac{N(\mathfrak{a})}{m_i}\right), \qquad i = 1, \ldots, n, \tag{5.11}$$

and this list is extended with a subset of

$$\delta : [\mathfrak{a}] \mapsto \left(\frac{-1}{N(\mathfrak{a})}\right), \qquad \epsilon : [\mathfrak{a}] \mapsto \left(\frac{2}{N(\mathfrak{a})}\right), \qquad \delta\epsilon : [\mathfrak{a}] \mapsto \left(\frac{-2}{N(\mathfrak{a})}\right).$$

Concretely, the character $\delta$ is included if $r = 2$ and $-\Delta_{\mathcal{O}}/4 \equiv 1 \bmod 4$, or if $r \geq 4$. The character $\epsilon$ is included if $r = 3$ and $-\Delta_{\mathcal{O}}/8 \equiv 3 \bmod 4$, or if $r \geq 5$. The character $\delta\epsilon$ is included if $r = 3$ and $-\Delta_{\mathcal{O}}/8 \equiv 1 \bmod 4$, or if $r \geq 5$. In all this, $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre/Jacobi symbol and it is assumed that $[\mathfrak{a}]$ is represented by an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm coprime with $\Delta_{\mathcal{O}}$.

In the context of breaking the decisional Diffie–Hellman problem for ideal class group actions, it was observed in [8, 6] that, given two primitively $\mathcal{O}$-oriented elliptic

curves

$$(E,\iota),\ (E',\iota') = [\mathfrak{a}](E,\iota)\ \in \mathcal{E}\ell\ell_{\overline{k}}(\mathcal{O})$$

that are connected by an unknown ideal class $[\mathfrak{a}]$, it is possible to compute $\chi([\mathfrak{a}])$ for any assigned character $\chi$, purely from the knowledge of $(E,\iota)$, $(E',\iota')$, and at the cost of essentially one discrete logarithm computation (e.g., in the group $\mu_m$ in case $\chi = \chi_m$ for an odd prime divisor $m \mid \Delta_{\mathcal{O}}$).

Even though we have not much to add over [8, 6] in terms of efficiency or generality, in this section we want to make the nearly obvious remark that cyclic self-pairings are excellently suited for accomplishing this task. Indeed, if $m$ is an odd prime divisor of $\Delta_{\mathcal{O}}$, then we can consider the cyclic self-pairings

$$f : C \to \mu_m \subseteq \overline{k}^*, \qquad f' : C' \to \mu_m \subseteq \overline{k}^*$$

of order $m$ from Section 5.5. Taking any generators $P \in C$, $P' \in C'$, we know that $P' = \lambda\phi_{\mathfrak{a}}(P)$ for some $\lambda \in \mathbf{Z}$ that is invertible mod $m$ and then

$$f'(P') = f(P)^{\lambda^2 N(\mathfrak{a})} \qquad \text{so that} \qquad \chi_m([\mathfrak{a}]) = \left(\frac{\log_{f(P)} f'(P')}{m}\right).$$

None of the methods from [8, 6] are literal applications of this simple strategy. Indeed, in the case of [8], which focuses on ordinary elliptic curves over finite fields, the self-pairing step is preceded by a walk to the floor of the $m$-isogeny volcano truncated at $\mathbf{Z}[\pi_q]$, in order to ensure cyclic rational $m^\infty$-torsion, at which point the usual reduced $m$-Tate pairing can be used. The method from [6] applies to arbitrary orientations and avoids such walks, but it does not use cyclic self-pairings; rather, it uses self-pairings with non-cyclic domains and, as a result, the argumentation becomes more intricate; see Remark 5.6.8 for a discussion. So we hope to have convinced the reader that, at least conceptually, this new method is simpler. It is also helpful in understanding and generalizing the "not walking to the floor" phenomenon from [8, App. A], as was already discussed in Remark 5.5.3.

*Remark* 5.6.6 If $r \geq 4$ then we can use the cyclic self-pairings of order $2^{r-2}$ from Section 5.5 for determining $N(\mathfrak{a}) \bmod 2^{r-2}$, and this is enough for evaluating $\delta, \epsilon, \delta\epsilon$ in case they exist. The situation is more subtle if

- $r = 2$ and $-\Delta_{\mathcal{O}}/4 \equiv 1 \bmod 4$ (to evaluate $\delta$),
- $r = 3$ (to evaluate one of $\epsilon$, $\delta\epsilon$).

Both cases can be handled by descending to elliptic curves that are primitively $(\mathbf{Z} + 2\mathcal{O})$-oriented, similar to the approach from [8, §3.1]. In the former case this may not be needed: according to Proposition 5.8.1, there may exist cyclic self-pairings that allow us to compute $N(\mathfrak{a}) \bmod 4$ directly. Indeed, for $k = \mathbf{F}_p$ and $\mathcal{O} = \mathbf{Z}[\sqrt{-p}]$ this is handled by the semi-reduced Tate pairing from [8, Rmk. 11], which was studied precisely for this purpose. But for arbitrary orientations we are currently missing such a pairing. $\Diamond$

*Remark* 5.6.7 If $m = \mathrm{char}(k)$ then our order-$m$ cyclic self-pairing is not available. However, in view of the character relation [8, Eq. (1)] it is always possible to discard one assigned character, so this concern is usually void.[5] This is in complete analogy with [8, 6]. ◊

*Remark* 5.6.8 In [6] an alternative attack to the DDH problem for oriented curves, that applies to arbitrary orientations, is described, using the Weil pairing rather than the Tate pairing. Here, the situation is slightly more intricate, in the sense that the domain of the self-pairing is no longer cyclic. More specifically, the self-pairing associated to [6, Thm. 1] may be constructed as follows. Let $\mathcal{O}$ be an imaginary quadratic order, let $E$ be an $\mathcal{O}$-oriented elliptic curve, and suppose that $m \mid \Delta_{\mathcal{O}}$ for some odd prime number $m$. Then we can write $\mathcal{O} = \mathbb{Z}[\sigma]$, for some $\sigma$ of norm coprime to $m$ [6, Lem. 1]. We define $f : E[m] \to \mu_m,\ f(P) := e_m(P, \sigma(P))$. One easily checks that this is indeed a non-trivial self-pairing compatible with horizontal isogenies. Interestingly, the proof of [6, Thm. 1] shows that $f$ can still be employed to recover the norm of a connecting ideal up to squares modulo $m$. A similar phenomenon occurs in [6, Prop. 1 & 2], where the associated self-pairings are maps $E[2] \to \mu_4$ and $E[4] \to \mu_8$ respectively. ◊

## 5.7 Conclusions and open problems

In this paper we have derived necessary and sufficient conditions for non-trivial cyclic self-pairings that are compatible with oriented isogenies, to exist. We have given examples of such pairings based on the generalized Weil and Tate pairings.

As an application, we have identified weak instances of class group actions assuming the degree of the secret isogeny is known and sufficiently small; some of these instances succumb to a polynomial time attack. We note that these cases are rare, but exist nonetheless; this situation is somewhat reminiscent of anomalous curves for which the ECDLP can be solved in polynomial time [33, 37]. These instances can be easily identified in that they require (large) square factors of $\Delta_{\mathcal{O}}$. This also shows that protocols that operate on or close to the crater are immune to this attack. To err on the side of caution it is probably best to limit oneself to (nearly) prime $\Delta_{\mathcal{O}}$.

The following problems remain open:

- In our attack we require square factors $m^2$ of $\Delta_{\mathcal{O}}$ to be able to derive the action of the secret isogeny on the full $E[m]$, which is required as input to the algorithm from [30]. However, it is well known that a degree $d$ isogeny is uniquely determined if it is specified on more than $4d$ points, so knowing the image of a single point of order $m > 4d$ should suffice. The problem remains to find a method akin to [30] that can handle such one-dimensional input.

- Is it possible to exploit partial information, e.g. how valuable is it to know the action of a secret isogeny on a single point of order $m < 4d$?

[5] If $\mathrm{char}(k) = 2$ then it seems like we may be missing more than one assigned character, but see [6, Footnote 1] for why this is not the case.

- At the moment we have only used the generalized Weil and Tate pairings for endomorphisms, whereas the definition also allows for more general isogenies $\psi$. Can this somehow be exploited in a more powerful attack?

- Our definition of a self-pairing on cyclic groups of even order allows for instances not derived from a bilinear pairing, e.g. the semi-reduced Tate pairing given in [8, Rmk. 11]. Proposition 5.8.1 below shows that such self-pairings indeed exist more generally, but unfortunately the proof does not give a method to efficiently compute them. Regardless of computational considerations, it would be interesting to find a more direct mathematical construction of these self-pairings and thereby genuinely complete the classification from Sections 5.4 and 5.5.

- Are there efficient Miller-type algorithms for computing the generalized Weil and Tate pairings? If not, do they exist for a larger class of endomorphisms than just $\sigma = \pi_q - 1$? At least, can these pairings be computed without needlessly extending the base field?

## 5.8 Relaxing the compatibility assumption

**Proposition 5.8.1** *We inherit the notation/assumptions from Proposition 5.4.8, but now we only require that our cyclic self-pairing*

$$f : C \to \overline{k}^*$$

*of order $m$ is compatible with endomorphisms $\iota(\sigma)$ for which $\gcd(N(\sigma), m) = 1$. Then $\mathrm{char}(k) \nmid m$, and writing $\Delta_{\mathcal{O}} = -2^r n$ with $n$ odd, we have:*

*(a) if $r = 0$ and $n \equiv 3 \bmod 8$ then $m \mid \Delta_{\mathcal{O}}$,*

*(b) if $r = 0$ and $n \equiv 7 \bmod 8$ then $m \mid 2\Delta_{\mathcal{O}}$,*

*(c) if $r = 2$ and $n \equiv 1 \bmod 4$ then $m \mid \Delta_{\mathcal{O}}$,*

*(d) if $r = 2$ and $n \equiv 3 \bmod 4$ then $m \mid \Delta_{\mathcal{O}}/2$,*

*(e) if $r = 3, 4$ then $m \mid \Delta_{\mathcal{O}}/4$,*

*(f) if $r \geq 5$ then $m \mid \Delta_{\mathcal{O}}/2$.*

*Conversely, if $m$ satisfies these necessary conditions, then we can equip every $\mathcal{O}$-oriented elliptic curve $(E, \iota)$ over $k$ for which the orientation is locally primitive at $m$ with a cyclic self-pairing*

$$f_{(E,\iota)} : C_{(E,\iota)} \to \overline{k}^*$$

*of order $m$, such that these self-pairings are compatible with all $K$-oriented isogenies of degree coprime with $m$ (as usual, $K$ denotes the imaginary quadratic number field containing $\mathcal{O}$).*

*Proof.* Write $m = 2^s m'$ with $m'$ odd. Note that the statement $\mathrm{char}(k) \nmid m$ is again immediate.

In order to prove the other divisibility conditions, it is easy to see that one can always find a generator $\sigma \in \mathcal{O}$ of norm coprime with $m'$, and by mimicking the proof of Proposition 5.4.8 (see the part "If $s \leq 1$ then ...") we find that $m' \mid \Delta_{\mathcal{O}}$. Since the self-pairing

$$C \to \overline{k}^* : P \mapsto f(P)^{m'} \tag{5.12}$$

has order $2^s$, the remaining divisibility conditions just follow from the case $m = 2^s$ which is discussed below. This ignores a subtlety, namely that (5.12) may be incompatible with endomorphisms $\sigma$ for which $\gcd(N(\sigma), 2^s m') \neq 1$, rather than just $\gcd(N(\sigma), 2^s) \neq 1$. However, it is easy to check that the proof below does not suffer from this.

As for the converse statement, the cyclic self-pairings

$$f_{(E,\iota),m'} : C_{(E,\iota),m'} \to \overline{k}^*$$

of order $m'$ that were constructed in Section 5.5 are compatible with $K$-oriented isogenies of *any* degree. So, here too, if we manage to find cyclic self-pairings

$$f_{(E,\iota),2^s} : C_{(E,\iota),2^s} \to \overline{k}^*$$

of order $2^s$ that are compatible with $K$-oriented isogenies of odd degree, then

$$C_{(E,\iota),2^s} \times C_{(E,\iota),m'} \to \overline{k}^* : P \mapsto f_{(E,\iota),2^s}(P) f_{(E,\iota),m'}(P)$$

is a family of cyclic self-pairings of the desired kind (we can assume that $C_{(E,\iota),2^s}$ is 2-primary, so that the domain is indeed cyclic).

Therefore, from now on we concentrate on the case $m = 2^s$, i.e., $m' = 1$. We proceed by the case distinction from the proposition statement:

(a) If $s \geq 1$ then by Lemma 5.4.6 we know that $C[2] \cong \mathbf{Z}/2\mathbf{Z}$. The generator $\sigma = (1+\sqrt{\Delta_{\mathcal{O}}})/2$ satisfies $\mathrm{Tr}(\sigma) \equiv N(\sigma) \equiv 1 \bmod 2$, so when acting on $E[2]$ it has characteristic polynomial $x^2 + x + 1$, which is irreducible. But by compatibility with $\sigma$ we know that $C[2]$ is an eigenspace: a contradiction.

(b) If $s \geq 2$ then as in the proof of Proposition 5.4.8 we find that $n = N(\sqrt{\Delta_{\mathcal{O}}})$ must be a square modulo 4: a contradiction. If $s = 1$ then we can construct the desired family of self-pairings as follows. Let $C_{(E,\iota)}$ be the subgroup of $E[2]$ that is fixed by $\sigma = (1 + \sqrt{\Delta_{\mathcal{O}}})/2$. This is a cyclic group of order 2 because the characteristic polynomial is $x^2 + x$ in this case. We then simply define

$$f_{(E,\iota)} : C_{(E,\iota)} \to \{\pm 1\} : P \mapsto -1, 0_E \mapsto 1$$

It is trivial that this family is compatible with $K$-oriented isogenies of odd degree (but note, as a sanity check for Proposition 5.4.8, that it is not compatible with the even-degree endomorphism $\sigma$).

We now discuss the cases $r \geq 2$. Note that the existence part is completely covered by Section 5.5, so it suffices to prove the necessary conditions, except in cases (c) and (f). We will use the notation

$$\sigma_a := a + \sqrt{\Delta_{\mathcal{O}}}/2$$

for any $a \in \mathbf{Z}$. This is an element of $\mathcal{O}$ with norm $a^2 + 2^{r-2}n$.

(c) If $s \geq 3$ then we arrive at a contradiction because $\{n, n+4\} = \{N(\sigma_0), N(\sigma_2)\}$ must both be squares modulo 8.

For existence when $s = 2$, fix an $\mathcal{O}$-oriented elliptic curve $(E, \iota)$ and consider the non-zero point $P \in E[2]$ annihilated by $\sigma_1$. This point exists because the characteristic polynomial of $\sigma_1$ mod 2 is $x^2$, and it is unique because otherwise $E[2] \subseteq \ker(\sigma_1)$ would imply that 4 divides $1 + n$, a contradiction. Consider the self-pairing

$$f_{(E,\iota)} \colon C_{(E,\iota)} \to \mu_4 \colon P \mapsto \zeta_4, 0_E \mapsto 1$$

where $C_{(E,\iota)} = \langle P \rangle$ and $\zeta_4$ is some fixed primitive 4-th root of unity. This is indeed a self-pairing of order 4: we have

$$f_{(E,\iota)}(\lambda P) = f_{(E,\iota)}(P)^{\lambda^2}$$

for any $\lambda \in \mathbf{Z}$ because odd squares are congruent to 1 modulo 4. It is easy to see that $f_{(E,\iota)}$ is compatible with oriented endomorphisms of odd degree. Indeed, every such endomorphism $\sigma$ can be written as $a + b\sigma_0$ for some integers $a$ and $b$, where exactly one among $a$ and $b$ is even since $N(\sigma) = a^2 + b^2 n$ is odd. Thus

$$f_{(E,\iota)}(\sigma(P)) = f_{(E,\iota)}((a+b)P) = f_{(E,\iota)}(P)^{a^2+b^2+2ab} = f_{(E,\iota)}(P)^{N(\sigma)}.$$

To turn this into a family of self-pairings compatible with odd-degree $K$-oriented isogenies, with every $\mathcal{O}$-oriented elliptic curve $(E', \iota')$ that is connected to $(E, \iota)$ via a $K$-oriented isogeny of degree 1 mod 4, we associate a self-pairing as above. If $(E', \iota')$ is connected via a $K$-oriented isogeny of degree 3 mod 4, then we do the same, except we map $P$ to $-\zeta_4$ instead of $\zeta_4$. This is unambiguous because if $(E', \iota')$ was connected to $(E, \iota)$ via $K$-oriented isogenies of degrees 1 and 3 mod 4, then $(E, \iota)$ would have an oriented endomorphism of degree 3 mod 4: a contradiction since we have shown above that all oriented endomorphisms have norm of the form $a^2 + b^2 n$. By construction, this family of self-pairings is then indeed compatible with $K$-oriented isogenies of odd degree.[6]

Finally, if $s = 1$, then we can just resort to our family of self-pairings from Section 5.5.

(d) If $s \geq 2$ then we find that $n = N(\sigma_0)$ must be a square modulo 4: a contradiction.

[6]The construction may not reach every $\mathcal{O}$-oriented elliptic curve $(E', \iota')$, because there may not exist an oriented isogeny to $(E, \iota)$, e.g. in view of [27, Prop. 3.3], but we can simply repeat the procedure inside every connected component.

(e) If $r = 3$ and $s \geq 2$ then $1 + 2n = N(\sigma_1)$ is a square mod 4, while if $r = 4$ and $s \geq 3$ then $1 + 4n = N(\sigma_1)$ is a square mod 8: contradictions.

(f) Assume $s \geq r$. By Lemma 5.4.6 we know that $C[2^{s-1}] \cong \mathbf{Z}/2^{s-1}\mathbf{Z}$. Since $f$ is compatible with $\sigma_a$ for every odd integer $a$, each of these endomorphisms acts on $C$ by scalar multiplication. But then the same must be true for $\sigma_0$: let $\lambda \in \mathbf{Z}$ be a corresponding scalar. Since $\mathrm{Tr}(\sigma_0) = 0$ the eigenvalues of $\sigma_0$ acting on $E[2^{s-1}]$ are then given by $\pm\lambda$ and therefore

$$-\lambda^2 \equiv N(\sigma_0) = 2^{r-2}n \bmod 2^{s-1}. \tag{5.13}$$

On the other hand, the compatibility implies that $N(\sigma_a) \equiv (\lambda + a)^2 \bmod 2^s$ for all odd integers $a$. Along with the above congruence this yields $a^2 - \lambda^2 \equiv (\lambda+a)^2 \bmod 2^{s-1}$. Plugging in $a = \pm 1$ we find that $(\lambda+1)^2 \equiv (\lambda-1)^2 \bmod 2^{s-1}$, so that $\lambda \equiv 0 \bmod 2^{s-3}$. This means that the left-hand side of (5.13) vanishes mod $2^{s-1}$, leaving us with $2^{r-2}n \equiv 0 \bmod 2^{s-1}$: a contradiction.

For existence when $s < r$, it suffices to assume that $s = r - 1$. Fix an $\mathcal{O}$-oriented elliptic curve $(E, \iota)$ such that the orientation is locally primitive at 2. Note that $2^{r-2} \mid N(\sigma_{2^{r-3}})$, so from Lemma 5.2.4 we see that $E[2^{r-2}, \sigma_{2^{r-3}}]$ is cyclic of order $2^{r-2}$. Fix a generator $P$ and define the self-pairing

$$f_{(E,\iota)} : C_{(E,\iota)} \to \mu_{2^{r-1}} : \lambda P \mapsto \zeta_{2^{r-1}}^{\lambda^2},$$

where $\zeta_{2^{r-1}}$ is some generator of $\mu_{2^{r-1}}$. As in (c), this is a well-defined self-pairing of order $2^{r-1}$. Indeed, for any $\lambda$ and $t$ we have

$$f_{(E,\iota)}((\lambda + 2^{r-2}t)P) = f_{(E,\iota)}(P)^{\lambda^2 + 2^{r-1}t\lambda + 2^{2(r-2)}t^2} = f_{(E,\iota)}(\lambda P).$$

To see compatibility with odd-degree endomorphisms, similar to in (c), we remark that every oriented endomorphism $\sigma$ can be written as $a + b\sigma_0$ for some integers $a$ and $b$. In particular, $N(\sigma) = a^2 + 2^{r-2}b^2$, which is odd if and only if $a$ is. Then

$$f_{(E,\iota)}(\sigma(P)) = f_{(E,\iota)}((a - 2^{r-3}b)P) = f_{(E,\iota)}(P)^{a^2 + 2^{r-2}ab} = f_{(E,\iota)}(P)^{N(\sigma)},$$

where the last equality follows from the fact that $ab \equiv b^2 \bmod 2$ because $a$ is odd, hence $2^{r-2}ab \equiv 2^{r-2}b^2 \bmod 2^{r-1}$. To turn this into a family of self-pairings compatible with odd-degree $K$-oriented isogenies, we proceed as in (c): if $(E', \iota')$ is a primitively $\mathcal{O}$-oriented elliptic curve (locally at 2) connected to $(E, \iota)$ via a $K$-oriented isogeny $\phi : E \to E'$ of odd degree, then we equip $(E', \iota')$ with the above self-pairing, except that we use

$$\zeta_{2^{r-1}}^{\deg(\phi)} \quad \text{instead of} \quad \zeta_{2^{r-1}}$$

as our primitive $2^{r-1}$-th root of unity, and we choose the specific generator

$P' = \phi(P)$ of $E'[2^{r-2}, \sigma_{2^{r-3}}]$.[7] To see that this self-pairing is independent of the choice of $\phi$, let

$$\phi_1, \phi_2 \colon E \to E'$$

be two $K$-oriented isogenies of odd degree, and write $P'_i$ for $\phi_i(P)$. Then $P'_1 = \lambda P'_2$ for some odd $\lambda$, and we need to check that $\deg(\phi_1) \equiv \lambda^2 \deg(\phi_2) \bmod 2^{r-1}$. Notice that $\hat{\phi}_2 \circ \phi_1$ is an oriented endomorphism of $E$ sending $P$ to $\lambda \deg(\phi_2) P$. By compatibility of $f_{(E,\iota)}$ with oriented endomorphisms of odd degree we have $(\lambda \deg(\phi_2))^2 \equiv \deg(\phi_1) \deg(\phi_2) \bmod 2^{r-1}$. The thesis immediately follows from the fact that $\deg(\phi_2)$ is a unit modulo $2^{r-1}$.

□

*Remark* 5.8.2 The above proof naturally raises the question whether the self-pairings in the boundary cases

- $s = r = 2$, $n \equiv 1 \bmod 4$,
- $s = r - 1 \geq 4$,

whose existence was shown in a non-effective way, admit a more direct description. Such a description would be needed for these self-pairings to be of any practical use. In the former case, we know that the answer is yes for the Frobenius orientation, thanks to the semi-reduced Tate pairing from (5.6); see also Remark 5.4.10. Unfortunately, this construction is of Frey–Rück type, i.e., involving Miller functions, and we do not know if/how it generalizes to arbitary orientations. ◊

[7] Here again, as in Footnote 6, the construction may not reach every instance of $(E', \iota')$, but we can repeat the procedure in every connected component.

## 5.9 Bibliography

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Peter Bruin. The Tate pairing for Abelian varieties over finite fields. *J. Théor. Nr. Bordx.*, 23:323–328, 2011.

[3] Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *PQCrypto 2020*, volume 12100 of *Lecture Notes in Computer Science*, pages 111–129. Springer, 2020.

[4] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 423–447. Springer, 2023.

[5] Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. Weak instances of class group action based cryptography via self-pairings. Full version on ePrint Archive available at `https://eprint.iacr.org/2023/549`, 2023.

[6] Wouter Castryck, Marc Houben, Frederik Vercauteren, and Benjamin Wesolowski. On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves. *Res. Number Theory*, 8(4):Paper No. 99, 18, 2022.

[7] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Asiacrypt 2018 Pt. 3*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[8] Wouter Castryck, Jana Sotáková, and Frederik Vercauteren. Breaking the decisional Diffie-Hellman problem for class group actions using genus theory. In *Crypto 2020 Pt. 2*, volume 12171 of *Lecture Notes in Computer Science*, pages 92–120. Springer, 2020.

[9] Daniel Cervantes-Vázquez, Mathilde Chenu, Jesús-Javier Chi-Dominguez, Luca De Feo, Francisco Rodriguez-Henriquez, and Benjamin Smith. Stronger and faster side-channel protections for CSIDH. In *Latincrypt 2019*, volume 11774 of *Lecture Notes in Computer Science*, pages 173–193. Springer, 2019.

[10] Jorge Chávez-Saab, Jesús-Javier Chi-Dominguez, Samuel Jaques, and Francisco Rodriguez-Henriquez. The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. *Journal of Cryptographic Engineering*, 12(3):349–368, 2022.

[11] Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 1(2):85–101, 2021.

[12] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptolology*, 14(1):414–437, 2020.

[13] Jean-Marc Couveignes. Hard homogeneous spaces, 2006. Unpublished article, available at `https://eprint.iacr.org/2006/291`.

[14] David A. Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication.* Pure and Applied Mathematics. Wiley, second edition, 2013.

[15] Pierrick Dartois and Luca De Feo. On the security of OSIDH. In *PKC 2022 Pt. 1*, volume 13177 of *Lecture Notes in Computer Science*, pages 52–81. Springer, 2022.

[16] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: scaling the CSI-FiSh. In *PKC 2023 Pt. 1*, volume 13940 of *Lecture Notes in Computer Science*, pages 345–375, 2023.

[17] Luca De Feo et al. Modular isogeny problems. Private communication.

[18] Gerhard Frey and Hans-Georg Rück. A remark concerning $m$-divisibility and the discrete logarithm in the divisor class group of curves. *Mathematics of Computation*, 62(206):865–874, 1994.

[19] Steven Galbraith. Pairings. In Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors, *Advances in Elliptic Curve Cryptography*, volume 317 of *LMS Lecture Note Series*, chapter 9, pages 183–213. Cambridge University Press, 2005.

[20] Theodoulos Garefalakis. The generalized Weil pairing and the discrete logarithm problem on elliptic curves. In *Latin 2002: Theoretical Informatics*, volume 2286 of *Lecture Notes in Computer Science*, pages 118–130. Springer, 2002.

[21] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[22] Hendrik W. Lenstra. Complex multiplication structure of elliptic curves. *J. Number Theory*, 56:227–241, 1996.

[23] Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 448–471. Springer, 2023.

[24] Victor S. Miller. Short programs for functions on curves, 1986. Unpublished note, available at `https://crypto.stanford.edu/miller/miller.pdf`.

[25] Victor S. Miller. The Weil pairing, and its efficient calculation. *Journal of Cryptology*, 17(4):235–261, 2004.

[26] Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. SiGamal: a supersingular isogeny-based PKE and its application to a PRF. In *Asiacrypt 2020 Pt. 2*, volume 12492 of *Lecture Notes in Computer Science*, pages 551–580. Springer, 2020.

[27] Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields Appl.*, 69:Paper No. 101777, 18, 2021.

[28] Damien Robert. Efficient algorithms for abelian varieties and their moduli spaces, 2021. Habilitation à Diriger des Recherches.

[29] Damien Robert. Some applications of higher dimensional isogenies to elliptic curves (overview of results), 2022. Preprint available at `https://eprint.iacr.org/2022/1704`.

[30] Damien Robert. Breaking SIDH in polynomial time. In *Eurocrypt 2023 Pt. 5*, volume 14008 of *Lecture Notes in Computer Science*, pages 472–503. Springer, 2023.

[31] Damien Robert. The geometric interpretation of the Tate pairing and its applications, 2023. Preprint available at `https://eprint.iacr.org/2023/177`.

[32] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies, 2006. Unpublished article, available at `https://eprint.iacr.org/2006/145`.

[33] Takakazu Satoh and Kiyomichi Araki. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. *Commentarii Mathematici Universitatis Sancti Pauli*, 47:81–92, 1998.

[34] René Schoof. Elliptic curves over finite fields and the computation of square roots mod $p$. *Mathematics of Computation*, 44(170):483—494, 1985.

[35] René Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46(2):183–211, 1987.

[36] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009.

[37] Nigel P. Smart. The discrete logarithm problem on elliptic curves of trace one. *Journal of Cryptology*, 12:193–196, 1999.

[38] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.

[39] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *IEEE FOCS 2021*, pages 1100–1111, 2022.