# On the Active Security of the PEARL-SCALLOP Group Action

Tako Boris Fouotsa[1], Marc Houben[2,3], Gioella Lorenzon[4], Ryan Rueger[5,6], and Parsa Tasbihgou[7]

research@borisfouotsa.com, marc.houben@math.u-bordeaux.fr, gioella.lorenzon@esat.kuleuven.be, ryan@rueg.re, parsa.tasbihgou@epfl.ch

[1] University of Manchester, M13 9PL, United Kingdom
[2] Inria Bordeaux, France
[3] Institut de Mathématiques de Bordeaux, France
[4] COSIC, KU Leuven, Belgium
[5] IBM Research Europe, Switzerland
[6] Technische Universität München, Germany
[7] Ecole Polytechnique Federal de Lausanne, Switzerland

**Abstract.** We present an active attack against the PEARL-SCALLOP group action. Modelling Alice as an oracle that outputs the action by a secret ideal class on suitably chosen oriented elliptic curves, we show how to recover the secret using a handful of oracle calls (four for the parameter set targeting a security level equivalent to CSIDH-1024), by reducing to the computation of moderately-sized group action discrete logarithms. The key ingredient to the attack is to employ curves with non-primitive orientations inherent to the PEARL-SCALLOP construction. We provide methods for public-key validation — that is, for deciding whether a given orientation is primitive — and discuss their practicality.

**Keywords:** Isogeny-based cryptography, class group actions, active attacks

## 1 Introduction

Class group actions on elliptic curves were introduced as a building block for post-quantum cryptography by Couveignes, Rostovtsev, and Stolbunov [35,90]. The resulting key exchange protocol, colloquially known as CRS, was the first cryptographic scheme to base its security on the hardness of finding isogenies between elliptic curves over finite fields, marking the origin of the field of isogeny-based cryptography. CSIDH [25] is an amendment to CRS that employs supersingular elliptic curves instead of ordinary ones, giving rise to the first practical variant of the protocol. Based on the more general theory of class group actions on oriented supersingular elliptic curves, several alternatives have since emerged,

Authors listed alphabetically ams.org/profession/leaders/CultureStatement04.pdf.

such as OSIDH [33] (no longer considered viable [39]), $(d, \epsilon)$-structures [31], the SCALLOP family [43,30,4], and large discriminant instantiations [24,62].

To this date, class group actions on elliptic curves are the only known approach instantiate *commutative* post-quantum group actions. Although commutativity of the action exposes a vulnerability to subexponential quantum attacks [66,67,87], it is also the most compelling attribute: commutative group actions give rise to the closest existing analogue of classical Diffie–Hellman (in fact, a natural generalization thereof) in a post-quantum scenario.[8] One of the major selling points is that this allows to instantiate a non-interactive key exchange (NIKE), for which few (post-quantum) alternatives are known [52,88]. Most notably, however, commutative group actions are especially powerful building block for constructing advanced cryptographic primitives. This includes blind signatures [63,59], threshold schemes [45,37,5], oblivious transfer [68], ID protocols [6], oblivious pseudorandom functions [15,60,46], verifiable random functions [73], zero-knowledge proofs [29], public key encryption [80], password authenticated key exchange [2], updatable encryption [75,72], and quantum money [78].

The precise features desired of the class group action depend on the targeted primitive. For instance, it is often desirable for the underlying class group to be known. Indeed, this is one approach for instantiating an *effective* group action, which is crucial for e.g. signature schemes [13,12,11] (although more recently, other methods for obtaining effective class group actions have been developed [84,85,41]). Moreover, some threshold schemes [45, Sec. 3] crucially rely on a known class group structure as a necessary ingredient for the protocol. The SCALLOP family [43,30,4], of which PEARL-SCALLOP [4] is the most efficient candidate, specifically targets parameter sets where the class group structure is efficiently computable.

To the best of our knowledge — apart from some particularly dubious parameter choices [53] — no attacks specific to the SCALLOP constructions have appeared in the literature. Cryptanalysis of class group actions is largely centered around CSIDH, and involves cost analysis of quantum attacks [10,16,86,28], side-channel analysis [20] — with a particular focus on constant time implementations [77,76,27,32,7,17,18,61], fault injections [19,69,71,8,70], and pairing-based attacks [26,23,22,53].

An avenue that remains largely unstudied in the general context of class group actions is that of *active attacks*, by which we mean an attacker model in which adversaries may deviate from an honest execution of the protocol in an attempt to extract secret information.[9] Such attacks — sometimes referred to as *adaptive* attacks — have been considered in isogeny-based cryptography mainly in the setting of SIDH-like protocols [57,47,48,9,65,51,50,56], although other isogeny-based schemes (not based on class group actions) have also been considered [79,95,81,74].

[8] Classical Diffie–Hellman can be viewed as relying on a commutative group action $(\mathbf{Z}/q\mathbf{Z})^\times \circlearrowright G$, where $G$ is a cyclic group of order $q$.

[9] We do not consider fault injections and side channel analysis as part of the attacker model.

**Our Contributions.**

- We present an active attack against instances of the isogeny class group action in which the conductor of the orientation is a product of medium-sized primes; this is precisely the setting of PEARL-SCALLOP.
  The efficacy of our attack crucially relies on access to a *static CDH oracle* (sometimes also called the *strong oracle* [57,65] in the context of active attacks). More concretely, we model Alice as an oracle that, on input of an oriented elliptic curve $(E, \iota)$, returns $(E', \iota') = [\mathfrak{a}] * (E, \iota)$, where $[\mathfrak{a}]$ is her secret ideal class.
  Contrary to other active attacks in the isogeny-based literature, this attack is *not* "adaptive"; indeed, all inputs to the oracle calls are precomputed, and in particular independent of the secret $[\mathfrak{a}]$. Moreover, the attack does not rely on side-channel information.
- We show that our attack significantly affects the security of PEARL-SCALLOP for all proposed parameter sets. For example, for the CSIDH-1024 equivalent, we can recover the secret using four oracle calls together with four group action inversions for groups of size $\sim 128$ bits.
- We describe public-key validation algorithms to mitigate the attack, and discuss their efficiency. We show that they significantly impact the practicality of PEARL-SCALLOP.

**Technical overview.** We now present the main idea of our attack. Let $\mathcal{O}_K$ be the maximal order of an imaginary quadratic number field $K$, and suppose that $\mathcal{O} \subseteq \mathcal{O}_K$ is a suborder of conductor $f_1 \cdots f_r$, where $f_1, \ldots, f_r$ are primes, each roughly of size $2^{128}$. This gives rise to a sequence of suborders $\mathcal{O}_K = \mathcal{O}^{(0)} \supsetneq \ldots \supsetneq \mathcal{O}^{(r)} = \mathcal{O}$, where, say, $\mathcal{O}^{(i)}$ has conductor $f_1 \cdots f_i$.

We think of curves primitively oriented by one of these orders as sitting inside of an isogeny volcano[10] [92], where the curves at the top are (primitively) oriented by $\mathcal{O}_K$ and the curves at the bottom are primitively oriented by $\mathcal{O}$. [11] Adjacent levels of the volcano are connected by oriented isogenies of large prime degree; the *ascending* isogeny from a curve oriented by $\mathcal{O}^{(i)}$ to one oriented by $\mathcal{O}^{(i-1)}$ is of degree $f_i$.

In (a simplified version of) PEARL-SCALLOP, one acts by the class group $\mathrm{Cl}(\mathcal{O})$ on curves that are primitively oriented by $\mathcal{O}$, *i.e.* curves at the bottom of the volcano.[12] For this to be a cryptographically useful group action, PEARL-SCALLOP sets parameters so that (a) the class group $\mathrm{Cl}(\mathcal{O})$ is sufficiently large, so solving vectorization (*i.e.* finding an ideal class connecting two given curves at the bottom of the volcano) is hard; and (b) computing ascending isogenies is infeasible, because their degree is a large prime.

[10] One difference with the usual isogeny volcano, whose edges correspond to $\ell$-isogenies for a fixed prime $\ell$, is that our descending/ascending isogenies have various different degrees.

[11] We recall that curves sitting "at level $i$" in the volcano, namely curves that are primitively oriented by $\mathcal{O}^{(i)}$, are also (non-primitively) oriented by $\mathcal{O}^{(i+1)}, \ldots, \mathcal{O}^{(r)}$.

[12] In reality, the conductor of $\mathcal{O}$ also has some small smooth divisor.

Now suppose that we are trying to recover a secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$, given access to an oracle that, on input of an $\mathcal{O}$-oriented elliptic curve $(E, \iota)$, returns $(E', \iota') = [\mathfrak{a}] * (E, \iota)$. The crucial subtlety to exploit here is that the $\mathcal{O}$-orientation is *not* assumed to be primitive. Indeed, as it will turn out, the group action underlying the PEARL-SCALLOP protocol is well defined on any $\mathcal{O}$-oriented curve. On input of a primitively $\mathcal{O}'$-oriented curve $(E, \iota)$, where $\mathcal{O}' \supseteq \mathcal{O}$, one naturally obtains $[\mathfrak{a}\mathcal{O}'] * (E, \iota)$, where $[\mathfrak{a}\mathcal{O}'] \in \mathrm{Cl}(\mathcal{O}')$. Now, by calling the oracle on curves that are higher up in the volcano — *i.e.* where the vectorization problem is easier — and subsequently finding a connecting ideal class, we obtain non-trivial information about the secret ideal class.

A more precise description of the attack is as follows. We first call the oracle on a curve $(E_0, \iota_0)$ that is at the top of the isogeny volcano: it will return $(E_0^{\mathfrak{a}}, \iota_0^{\mathfrak{a}}) = [\mathfrak{a}\mathcal{O}_K] * (E, \iota)$. Then, given that $\mathrm{Cl}(\mathcal{O}_K)$ is not too large (say of size $\sim 2^{128}$), we can compute an $\mathcal{O}_K$-ideal $\mathfrak{a}_0$ such that $[\mathfrak{a}_0\mathcal{O}_K] = [\mathfrak{a}\mathcal{O}_K]$ by solving the vectorization problem (*i.e.* finding a connecting ideal class) between $(E_0, \iota_0)$ and $(E_0^{\mathfrak{a}}, \iota_0^{\mathfrak{a}})$, using either a classical or a quantum algorithm.

Next, we call the oracle on a curve $(E_1, \iota_1)$ that is one level down in the volcano, *i.e.* primitively oriented by the order $\mathcal{O}^{(1)}$ of conductor $f_1$, obtaining $(E_1^{\mathfrak{a}}, \iota_1^{\mathfrak{a}}) = [\mathfrak{a}\mathcal{O}^{(1)}] * (E_1, \iota_1)$. Applying $[\mathfrak{a}_0 \cap \mathcal{O}^{(1)}]$ to $(E_1, \iota_1)$, we obtain a curve $(E_1', \iota_1')$. Crucially, since $[\mathfrak{a}_0\mathcal{O}_K] = [\mathfrak{a}\mathcal{O}_K]$, we now have that the ascending $f_1$-isogenies from $(E_1', \iota_1')$ and $(E_1^{\mathfrak{a}}, \iota_1^{\mathfrak{a}})$ map to a common curve at the top of the volcano. This implies that the connecting ideal class $[\mathfrak{c}_i]$ between the two curves lies in the kernel $\kappa_1$ of the projection $\mathrm{Cl}(\mathcal{O}^{(1)}) \to \mathrm{Cl}(\mathcal{O}_K)$, which is roughly of size $\#\kappa_1 \approx f_1$. Given that $f_1$ is not too large, we can again solve the vectorization problem, this time inside the group $\kappa_1$. From this, we can obtain an $\mathcal{O}^{(1)}$-ideal $\mathfrak{a}_1$ such that $[\mathfrak{a}_1\mathcal{O}^{(1)}] = [\mathfrak{a}\mathcal{O}^{(1)}]$. Continuing this process down the isogeny volcano, we eventually obtain an $\mathcal{O}^{(r)}$-ideal (*i.e.* an $\mathcal{O}$-ideal) $\mathfrak{a}_r$ such that $[\mathfrak{a}_r] = [\mathfrak{a}]$.

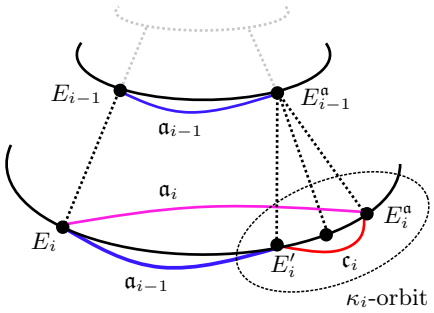


Fig. 1: A simplified sketch of the attack. We have omitted the orientations for visual clarity, and used representatives $\mathfrak{a}$ instead of classes $[\mathfrak{a}]$. We translate the information $\mathfrak{a}_{i-1}$ down one level by acting on $E_i$. Then we solve a vectorisation problem within the $\kappa_i$-orbit, to obtain the "correction" $\mathfrak{c}_\mathfrak{i}$ which delivers $\mathfrak{a}_i$. Note that we never evaluate the descending isogenies.

**Outline.** In Section 2, we compile preliminary results; in particular, we show that the PEARL-SCALLOP class group action is well defined in case of a non-primitively oriented curve, and that known algorithms already compute this action without modification. In Section 3, we describe our attack in the context of various active attacker models, and discuss the security implications. Finally, in Section 4, we describe methods to validate public keys and discuss their practicality.

**Acknowledgements.** We would like to thank the organisers of the Isogeny Club Brainstorm Days at Eurocrypt 2025, where this project was started. We also thank Jonathan Komada Eriksen and Lorenz Panny for useful discussions.

The second-listed author was supported by the France 2030 program, managed by the French National Research Agency under grant agreement No. ANR-22-PETQ-0008 PQ-TLS. The third-listed author was supported by the Fonds voor Wetenschappelijk Onderzoek (FWO) under grant number 1139225N; by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement ISOCRYPT – No. 101020788); by the Research Council KU Leuven grant C14/24/099; and by CyberSecurity Research Flanders with reference number VOEWICS02. The fourth-listed author was supported by SNSF Consolidator Grant CryptonIs 213766.

## 2 Preliminaries

### 2.1 The class group action on oriented elliptic curves

Throughout this subsection, all elliptic curves are assumed to be defined over a perfect field $k$ of characteristic $p > 0$. By $\mathrm{End}(E)$ we mean the endomorphism ring over $\overline{k}$ and by $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes \mathbf{Q}$ the (full) endomorphism algebra. Our main references are [93,83]. For cryptographic applications of the isogeny class group action, we refer to [3].

**Imaginary quadratic orders.** An imaginary quadratic order $\mathcal{O}$ is an order in an imaginary quadratic number field $K$. It can always be written as $\mathcal{O} = \mathbf{Z}[\sigma] = \{a + b\sigma \mid a, b \in \mathbf{Z}\}$ for some algebraic integer $\sigma \in K$. The *discriminant* $\mathrm{Disc}(\mathcal{O}) \in \mathbf{Z}_{<0}$ of $\mathcal{O}$ is the discriminant of $\sigma$; it defines $\mathcal{O}$ uniquely up to ring isomorphism. An imaginary *fundamental discriminant* $d$ is a negative integer that is either (i) squarefree and $d \equiv 1 \pmod 4$, or (ii) of the form $d = 4 \cdot d'$, where $d'$ is squarefree and $d' \equiv 2, 3 \pmod 4$. An imaginary quadratic order is maximal with respect to inclusion, *i.e.* equal to the ring of integers of its fraction field, if and only if its discriminant is fundamental. The *class group* $\mathrm{Cl}(\mathcal{O})$ of $\mathcal{O}$ is the group of invertible fractional $\mathcal{O}$-ideals modulo its subgroup of principal fractional $\mathcal{O}$-ideals.

**Inclusions of orders.** If $\mathcal{O}_1 \supseteq \mathcal{O}_2$, then $\mathrm{Disc}(\mathcal{O}_1) = f^2 \mathrm{Disc}(\mathcal{O}_2)$ for some integer $f \in \mathbf{Z}_{>0}$, called the *relative conductor* of $\mathcal{O}_2$ in $\mathcal{O}_1$. The ideal $f\mathcal{O}_1$ is the largest ideal (with respect to inclusion) of $\mathcal{O}_1$ that is contained in $\mathcal{O}_2$ [34, Thm. 1.3] and is called the *conductor ideal*. If $\mathcal{O}_1 = \mathbf{Z}[\sigma]$ then $\mathcal{O}_2 = \mathbf{Z}[f\sigma]$. If $\mathcal{O}_1 \supseteq \mathcal{O}_2 \supseteq \mathcal{O}_3$, then the relative conductor of $\mathcal{O}_3$ in $\mathcal{O}_1$ is the product of the relative conductors of $\mathcal{O}_2$ in $\mathcal{O}_1$ and of $\mathcal{O}_3$ in $\mathcal{O}_2$. There is an exact sequence relating the class groups of $\mathcal{O}_1 \supseteq \mathcal{O}_2$ [64, Theorem 5.4]:

$$1 \to \frac{\mathcal{O}_1^\times}{\mathcal{O}_2^\times} \to \frac{(\mathcal{O}_1/f\mathcal{O}_1)^\times}{(\mathcal{O}_2/f\mathcal{O}_1)^\times} \to \mathrm{Cl}(\mathcal{O}_2) \to \mathrm{Cl}(\mathcal{O}_1) \to 1. \tag{1}$$

**Orientations.** With $K$ still being an imaginary quadratic number field, we define a *$K$-orientation* on an elliptic curve $E$ to be (necessarily injective) ring homomorphism $\iota\colon K \to \mathrm{End}^0(E)$. If $\mathcal{O} \subseteq K$ is an imaginary quadratic order, then $\iota$ is called an *$\mathcal{O}$-orientation* if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. If an $\mathcal{O}$-orientation does not extend to a strictly larger imaginary quadratic order $\mathcal{O}' \subseteq K$, then it is called *primitive*.

**Definition 2.1.** *A $K$-orientation $\iota\colon K \to \mathrm{End}^0(E)$ is primitive for a unique order $\mathcal{O}^{\mathrm{pr}}(\iota) \subseteq K$, called the* primitive order (of $\iota$). *It is given by $\mathcal{O}^{\mathrm{pr}}(\iota) = \iota^{-1}(\mathrm{End}(E))$. The* absolute conductor of $\iota$, *denoted $f^{\mathrm{pr}}(\iota)$, is the conductor of $\mathcal{O}^{\mathrm{pr}}(\iota)$ in the ring of integers $\mathcal{O}_K$.*

If $(E, \iota)$ is a $K$-oriented elliptic curve and $\varphi\colon E \to E'$ is an isogeny, then the *induced* $K$-orientation $\varphi_*(\iota)$ on $E'$ is given by

$$\varphi_*(\iota)(\alpha) := \frac{1}{\deg \varphi} \varphi \circ \iota(\alpha) \circ \hat{\varphi}$$

for all $\alpha \in K$. Let $\mathfrak{O} := \mathcal{O}^{\mathrm{pr}}(\iota), \mathfrak{O}' := \mathcal{O}^{\mathrm{pr}}(\varphi_*(\iota))$ denote the primitive orders of $\iota$ and $\varphi_*(\iota)$ respectively. If $\deg \varphi = \ell$ is prime, then either

(i) $\mathfrak{O} = \mathfrak{O}'$ and we call $\varphi$ *horizontal*; or
(ii) $\mathfrak{O} \subsetneq \mathfrak{O}'$ and we call $\varphi$ *ascending*; or
(iii) $\mathfrak{O} \supsetneq \mathfrak{O}'$ and we call $\varphi$ *descending*.

In the last two cases, the relative conductor is $\ell$. We will use the same terminologies (horizontal, ascending, descending) for isogenies whose degree is not prime, if the primitive orders of the domain and codomain are comparable, in the sense that one is contained in the other.

**Class group actions.** Let $(E, \iota)$ be an $\mathcal{O}$-oriented elliptic curve, and denote by $\mathcal{O}^{\mathrm{pr}}$ the associated primitive order. Write $f_{\mathcal{O}^{\mathrm{pr}}/\mathcal{O}}$ for the relative conductor of $\mathcal{O}$ in $\mathcal{O}^{\mathrm{pr}}$. To an ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm coprime to $p, f_{\mathcal{O}^{\mathrm{pr}}/\mathcal{O}}$, we associate a separable isogeny $\varphi_{\mathfrak{a}}\colon E \to \mathfrak{a} * E$ of degree $N(\mathfrak{a})$ with kernel

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

The isogeny $\varphi_{\mathfrak{a}}$ is horizontal if and only if $\mathfrak{a}$ is invertible. In that case, the oriented curve $(\mathfrak{a} * E, (\varphi_{\mathfrak{a}})_*(\iota))$ depends — up to $K$-oriented isomorphism — only on the ideal class of $\mathfrak{a}$. This induces a well-defined group action

$$\mathrm{Cl}(\mathcal{O}) \circlearrowright \{(E, \iota) \mid E/\overline{k} \text{ an elliptic curve, } \iota \text{ an } \mathcal{O}\text{-orientation}\}/\cong . \tag{2}$$

If $f_{\mathcal{O}^{\mathrm{pr}}/\mathcal{O}} = 1$ (*i.e.* if the orientation is primitive) then this action is free, and the number of orbits is at most two [94, Thm. 1].

**Acting by exponent vectors.** Let $K$ be an imaginary quadratic number field and let $\ell_1, \ldots, \ell_n$ be a collection of (distinct) primes that split in $\mathcal{O}_K$. Suppose $\sigma$ generates $\mathcal{O}_K = \mathbf{Z}[\sigma]$. Since each prime $\ell_j$ split, the reduction modulo $\ell_j$ of the minimal polynomial of $\sigma$ has two distinct eigenvalues $\lambda_j, \mu_j \in \mathbf{Z}/\ell_j\mathbf{Z}$. This corresponds to a factorization of the principal ideal generated by $\ell_j$ into prime ideals of norm $\ell_j$, as

$$(\ell_j) = (\ell_j, \sigma - \lambda_j)(\ell_j, \sigma - \mu_j).$$

Let us choose, for each $1 \leq j \leq n$, one of the two eigenvalues. That is, we fix a choice of prime ideal $\mathfrak{l}_j \subseteq \mathcal{O}_K$ above $\ell_j$, say $\mathfrak{l}_j = (\ell_j, \sigma - \lambda_j)$. Then we obtain a well-defined group homomorphism

$$\varpi \colon \mathbf{Z}^n \to \mathrm{Cl}(\mathcal{O}_K),\ (s_1, \ldots, s_n) \mapsto [\mathfrak{l}_1]^{s_1} \cdots [\mathfrak{l}_n]^{s_n} .$$

In the context of class group actions, once a map $\varpi$ has been defined, elements $(s_1, \ldots, s_n) \in \mathbf{Z}^n$ are also referred to as *exponent vectors*. Our choice of $\mathfrak{l}_j$ essentially amounts to determining which ideal of norm $\ell_j$ is considered *positive* (*i.e.* corresponding to $s_j = 1$). Using $\varpi$, we can extend (2) to an action

$$\mathbf{Z}^n \circlearrowright \{(E, \iota) \mid E/\overline{k} \text{ an elliptic curve, } \iota \text{ an } \mathcal{O}_K\text{-orientation}\}/\cong .$$

Since the action (2) on primitively oriented elliptic curves is free, the stabilizer of every point is the kernel of $\varpi$. If $\mathcal{O} \subseteq \mathcal{O}_K$ is an order of absolute conductor coprime to $\ell_j$, then $\ell_j$ splits in $\mathcal{O}$, and $\mathfrak{l}_j \cap \mathcal{O}$ is an invertible $\mathcal{O}$-ideal of norm $\ell_j$. Choosing $\mathfrak{l}_j \cap \mathcal{O}$ as the "positive" ideal, we can further extend to a group action

$$\mathbf{Z}^n \circlearrowright \left\{ (E, \iota) \,\middle|\, E/\overline{k},\ \iota \text{ a } K\text{-orientation, } \gcd\left(\textstyle\prod_j \ell_j, f^{\mathrm{pr}}(\iota)\right) = 1 \right\} / \cong, \tag{3}$$

where, explicitly,

$$(s_1, \cdots, s_n) * (E, \iota) := \left( [\mathfrak{l}_1 \cap \mathcal{O}^{\mathrm{pr}}(\iota)]^{s_1} \ldots [\mathfrak{l}_n \cap \mathcal{O}^{\mathrm{pr}}(\iota)]^{s_n} \right) * (E, \iota).$$

Here, the stabilizer of $(E, \iota)$ is the kernel $\Lambda$ of the map $\varpi^{\mathrm{pr}} \colon \mathbf{Z}^n \to \mathrm{Cl}(\mathcal{O}^{\mathrm{pr}}(\iota))$. If $\varpi^{\mathrm{pr}}$ is surjective, then we have $\mathrm{Cl}(\mathcal{O}^{\mathrm{pr}}(\iota)) \cong \mathbf{Z}^n/\Lambda$, and we call $\Lambda$ the *relation lattice* of $\mathcal{O}^{\mathrm{pr}}(\iota)$.

**Compatibility of the action between levels.** Let $\mathcal{O}' \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ be orders of absolute conductor $f', f$ respectively. We recall that the $\mathcal{O}$-ideals prime to $f$ are in bijection with the $\mathcal{O}_K$-ideals prime to $f$ via the norm-preserving maps of extension $(I \mapsto I\mathcal{O}_K)$ and restriction $(J \mapsto J \cap \mathcal{O})$ [36, Prop. 7.20]; and because an ideal $I \subseteq \mathcal{O}$ is prime to an integer $m$ if and only if its norm $\mathrm{N}(I)$ is [36, Lem. 7.18][13], this bijection restricts to a bijection between $\mathcal{O}$-ideals prime to $f'$ and $\mathcal{O}_K$-ideals prime to $f'$. Together, we conclude that restriction and extension deliver a bijection between $\mathcal{O}$-ideals prime to $f'$ and $\mathcal{O}'$-ideals prime to $f'$.

Consider now a prime $\mathcal{O}_K$-ideal $\mathfrak{l} = (\ell, \sigma - \lambda)$ above $\ell$. Then

$$\mathfrak{l} \cap \mathcal{O} = \ell\mathcal{O} + f(\sigma - \lambda)\mathcal{O} = (\ell, f(\sigma - \lambda)),$$

and similarly for $\mathfrak{l} \cap \mathcal{O}'$.

**Lemma 2.2.** *If $f, f' \in \mathbf{Z}_{>0}$ are coprime to $\ell$, then $(\ell, f(\sigma - \lambda)) = (\ell, f'(\sigma - \lambda))$ as $\mathcal{O}$-ideals.*

*Proof.* This is exactly the statement that the extension of $\mathfrak{l} \cap \mathcal{O}'$ to $\mathcal{O}$ is $\mathfrak{l} \cap \mathcal{O}$, which follows from the fact that extension and restriction of ideals coprime to the conductor is bijective. □

**Corollary 2.3.** *Let $(E, \iota)$ be a $K$-oriented elliptic curve. Let $\mathbf{Z}[\sigma] = \mathcal{O}^{\mathrm{pr}}(\iota)$ and $f = f^{\mathrm{pr}}(\iota)$. Let $\omega \in K$ be any element such that $\iota(\omega) \in \mathrm{End}(E)$. Denote by $f'$ the relative conductor of $\mathbf{Z}[\omega]$ in $\mathbf{Z}[\sigma]$, and assume that $\gcd(\ell, f') = 1$ for a prime $\ell$. Write $\omega = c + f'\sigma$ for some $c \in \mathbf{Z}$. Then, if $\mathfrak{l} = (\ell, \sigma - \lambda)$ is a prime $\mathcal{O}_K$-ideal above $\ell$,*

$$E[(\ell, \omega - c - f'\lambda)] = E[\mathfrak{l} \cap \mathcal{O}^{\mathrm{pr}}(\iota)].$$

*Proof.* We have

$$E[(\ell, \omega - c - f'\lambda)] = E[(\ell, f'\sigma - f'\lambda)] = E[(\ell, f\sigma - f\lambda)] = E[\mathfrak{l} \cap \mathcal{O}^{\mathrm{pr}}(\iota)],$$

where the second equality follows from Lemma 2.2. □

This result is essentially [4, Prop. 3.1]; it implies that we can evaluate the group action (3) using the image under $\iota$ of *any* element $\omega \in \mathcal{O}^{\mathrm{pr}}(\iota)$ (not necessarily a generator for the primitive order), as long as the absolute conductor of $\mathbf{Z}[\omega]$ is coprime to all primes $\ell_1, \ldots, \ell_n$.

## 2.2 PEARL-SCALLOP

PEARL-SCALLOP is a group action based on oriented isogenies of supersingular elliptic curves, which was proposed in [4] as a variant of SCALLOP [43]. The orienting imaginary quadratic order is a suborder of a maximal order with a class number that is large but efficiently computable, and the conductor is taken to be a product of a few large primes, rather than a single large prime.

[13] Cox proves this for $m = f$, but the statement still holds for any integer $m$.

PEARL-SCALLOP features a representation of the orientation by an endomorphism whose degree is a power of 2. This avoids higher-dimensional isogeny representations, in contrast to SCALLOP-HD [30], and simplifies a constraint on the norm of the acting ideal. We give here a brief summary of PEARL-SCALLOP.

**The orientation.** Let $f, d \in \mathbf{Z}_{>0}$, $\mathcal{O} = \mathbf{Z}[f\sqrt{-d}]$ be an order inside the imaginary quadratic number field $K$, $\omega$ an element of smooth norm inside $\mathcal{O}$, and $g$ the relative conductor of $\mathbf{Z}[\omega]$ in $\mathbf{Z}[f\sqrt{-d}]$. Given a (maximal supersingular) $\mathcal{O}$-oriented elliptic curve $(E, \iota)$ along with an efficient representation of the endomorphism $\iota(\omega)$, one can efficiently compute the action of any prime-normed $\mathcal{O}$-ideal $I$ so long its norm is prime to $g$ and polynomially sized in the input. This is shown in [4, Prop. 3.1], and also follows from Corollary 2.3.

For completeness, we give a self-contained description here. If $\delta$ is a generator of $\mathbf{Z}[f\sqrt{-d}]$, then $g\delta$ is a generator of $\mathbf{Z}[\omega]$, hence $g\delta = c + \omega$ for some $c \in \mathbf{Z}$. Let $\mathfrak{l} = (\ell, a + \delta)$ be an ideal of $\mathbf{Z}[\delta]$ with prime norm $\ell$, coprime to $g$. Then $\mathfrak{l} = (\ell, g(a + \delta)) = (\ell, ga + c + \omega)$, and computing the isogeny corresponding to the action of $[\mathfrak{l}]$ amounts to computing the isogeny with kernel $E[\ell] \cap E[\iota(\omega) + [ga + c]] = (\widehat{\iota(\omega)} + [c + ga])(E[\ell])$. In other words, to compute the action of $\mathfrak{l}$ on $E$ one essentially needs to compute eigenvectors of $\widehat{\iota(\omega)}$ on $E[\ell]$.

The endomorphism $\iota(\omega)$ is represented by a pair cyclic isogenies $\varphi_P, \varphi_Q$ which compose to $\iota(\omega) = \widehat{\varphi_Q}\varphi_P$, and these isogenies are in turn represented by generators $P, Q$ of their kernels. From now on, we will drop the orientation $\iota$ in the notation, and write for example $\omega$ for $\iota(\omega)$.

In practice, $\deg(\omega) = 2^{2e} \mid (p+1)^2$ for some $e \in \mathbf{Z}_{>0}$, and $\{P, Q\}$ is a basis of $E[2^e]$. The prime $p$ is taken to be of the form $p = c2^e \prod_{i=1}^{n} \ell_i - 1$, where $\ell_1, \dots \ell_n$ are split odd primes not dividing the relative conductor $g$, and $c$ is a small cofactor such that $p$ satisfies $(\mathrm{Disc}(\mathcal{O}) \mid p) = -1$. This last condition ensures that the set of $\mathcal{O}$-oriented supersingular elliptic curves in characteristic $p$ is nonempty [83, Prop. 3.2]).

**Evaluating the action.** When evaluating the action of an ideal of $\mathcal{O}$, one first finds a smooth normed representative $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{l}_i^{e_i}$ of its class in $\mathrm{Cl}(\mathcal{O})$ using the pre-computed class group structure (see [4, Sec. 4] for more details); then one repeatedly applies Algorithm 1 ([4, Algorithm 2]) to ideals of the form $\prod_{i=1}^{n} \mathfrak{l}_i^{b_i}$ with $b_i \in \{0, 1\}$ until the action by $\mathfrak{a}$ has been computed. The evaluation procedure is standard, and has a standard optimization obtained by using a different point sampling method (see [4, Algorithm 3]), but the core idea remains the same.

**Generating a starting curve.** A starting elliptic curve, together with a representation of an $\mathcal{O}$-orientation, is computed in the following way. First, one considers a definite quaternion algebra $\mathcal{B}_{p,\infty}$, ramified at $p$ and infinity, and a special $p$-extremal maximal quaternion order $\mathcal{O}_0 \subseteq \mathcal{B}_{p,\infty}$ where the quaternion

**Algorithm 1** GroupAction$(\mathfrak{a}, E, P, Q)$

**Input:** A smooth $\mathcal{O}$-ideal $\mathfrak{a} = \prod_{i=1}^{N} \mathfrak{l}_i$, an $\mathcal{O}$-oriented elliptic curve $E$, points $P, Q \in E$ generating isogenies such that $\hat{\varphi}_Q \circ \varphi_P$ is an endomorphism corresponding to an element of $\mathcal{O}$ of norm $2^{2e}$.
**Output:** An $\mathcal{O}$-oriented curve $(E_\mathfrak{a}, P_\mathfrak{a}, Q_\mathfrak{a}) = \mathfrak{a} * (E, P, Q)$.

Let $B_1, B_2$ be a basis of $E[L]$ where $L = \prod_{i=1}^{N} \ell_i$.
Let $\hat{\omega} = \hat{\varphi}_P \circ \varphi_Q$.
Compute $B_1' = \hat{\omega}(B_1)$, $B_2' = \hat{\omega}(B_2)$.
**for** $i \in \{1, \dots n\}$ **do**
    Compute $K_i = [L/\ell_i]([\lambda_i]B_1 + B_1')$ where $\mathfrak{l}_i = (\ell_i, \lambda_i + \omega)$.
    **if** $K_i = 0_E$ **then**
        Compute $K_i = [L/\ell_i]([\lambda_i]B_2 + B_2')$.
    **end if**
**end for**
Compute $\varphi_\mathfrak{a} \colon E \to E_\mathfrak{a}$ from its kernel $K = \langle K_1, \dots K_n \rangle$.
**return** $(E_\mathfrak{a}, \varphi_\mathfrak{a}(P), \varphi_\mathfrak{a}(Q))$.

embedding problem is easily solvable. Then, one tries different smooth values $h$ until a (primitive) embedding of $\mathbf{Z} + h\mathcal{O}$ in $\mathcal{O}_0$ is found (this is done using the heuristic algorithm GenericOrderEmbeddingFactorisation, see [49, Algorithm 3]).

From a curve $E_0$ such that $\mathrm{End}(E_0) \cong \mathcal{O}_0$, it is then easy to compute an ascending $h$-isogeny to a curve $E$, which will be oriented by $\mathcal{O}$. Finally, one needs to find points $P, Q$ representing the smooth element $\omega \in \mathcal{O}$. This is done by factoring the ideal generated by $\omega$ in $\mathcal{O}_E \cong \mathrm{End}(E)$ as a product of smooth-norm ideals, pulling back these ideals through the ideal corresponding to the ascending $h$-isogeny, and eventually obtaining the corresponding kernel generators. This is a standard technique used also in SQIsign [44], from which PEARL-SCALLOP takes algorithms IdealToIsogeny and IdealToKernel. The procedure is summarised in [4, Algorithm 1], which we do not report here as it will not be needed for the rest of the paper.

**Parameters.** The two key properties of PEARL-SCALLOP are that its orientation is by an order $\mathcal{O} = \mathbf{Z}[d\sqrt{-d}]$ with $f$ a product of a few medium-sized primes, and that this orientation can be encoded by an element of smooth norm. These properties respectively make the class group computation feasible, whilst allowing for efficient evaluation.

To find such $f$ and $\omega$, the idea is to consider powers $m$ of a generic element $a + \sqrt{-d} \in \mathbf{Z}[\sqrt{-d}]$ satisfying the norm equation $a + d^2 = 2N^2$ with $N$ smooth, until the coefficient of $\sqrt{-d}$ in $(a + \sqrt{-d})^m$ is divided by a few large primes.

For parameters targeting a security level equivalent to CSIDH-1024, the authors set $N = 2^{129}$, and consider $(a + \sqrt{-d})^4$ so that the coefficient of $\sqrt{-d}$ equals $24a(a - N)(N + a)/3$. They pick $a$ and $d = 2N^2 - a^2$ so that $a$, $N - a$ and $(N + a)/3$ are 128-bit primes that split in $\mathbf{Q}(\sqrt{-d})$, in order to ensure easier discrete logarithms in the class group computation. Thanks to [4, Lemma 3.3],

the splitting condition is achieved when the above three factors are prime, and $a < N$ satisfies $a \equiv 19 \bmod 24$.

A similar approach is taken for parameters equivalent to CSIDH-$\{2048, 4096\}$, obtaining a conductor divided by seven primes of size 299 bits and 640 bits, respectively. Finally, the authors propose an intermediate set of parameters achieving a discriminant of $\mathbf{Q}(f\sqrt{-d})$ of size roughly 1500 bits. We refer to the original paper [4, Section 3] for more details.

### 2.3 Interpolating and Dividing Isogenies

In this subsection we briefly cover isogeny representations by embedding into higher dimensional isogenies and an algorithm to test whether a given isogeny factors through multiplication by an integer, with [89] as our main reference. This content will be relevant for Section 4, where we will discuss how to validate PEARL-SCALLOP public keys, in particular how to verify whether a given orientation is primitive.

**Embedding isogenies.** Robert's *embedding lemma* [89, Ex. 5.16] tells us that every $n$-isogeny $\varphi\colon (A, \lambda_A) \to (B, \lambda_B)$ between $g$-dimensional principally polarised Abelian varieties can be embedded into a $2ug$-dimensional $N$-isogeny

$$\Phi = (\alpha, (\widetilde{\varphi}\,\mathrm{id}_u); -(\varphi\,\mathrm{id}_u), \widetilde{\alpha}) : A^u \times B^u \to A^u \times B^u,$$

for any $N > n$, when $N - n$ is the sum of $u \in \{1, 2, 4\}$ integer squares. Here, $\widetilde{\varphi} = \lambda_A^{-1}\hat{\varphi}\lambda_B$ denotes the *polarised dual*[14] of $\varphi$; $(\varphi\,\mathrm{id}_u)\colon A^u \to B^u$ denotes the $u \times u$ matrix with $\varphi$ on the diagonal; and $\alpha$ is a $u \times u$ integer matrix which induces a polarised endomorphism on both $A^u, B^u$ and has determinant $N - n$ [89, Prop. 5.15][15]. Moreover, if $N$ is prime to $n$ and to the characteristic of the base field, we have

$$\ker(\Phi) = \{((N-n)P, (\mathrm{id}_u\,\varphi) \circ \alpha(P)) \mid P \in A^u[N]\}\,. \tag{4}$$

**Interpolating isogenies.** Given *interpolation data* $\{(P_i, \varphi(P_i), Q_i, \varphi(Q_i))\}_i$ of an $n$-isogeny $\varphi$ on a *CRT basis* $\{(P_i, Q_i)\}_i$[16] of $A[N]$ and a decomposition of $N - n$ as the sum of $u$ squares[17], one can one can write down the corresponding matrix $\alpha$ and generators of $\ker(\Phi)$ as described by (4).

With $\ker(\Phi)$ computed this way, one can evaluate $\Phi$ (and therefore $\varphi$) on points $R$ in $A \times B$ in time $\widetilde{O}(aed(m\ell)^g \log(q))$, where $\mathbb{F}_q$ is the field of definition of $A, B$; $N = \ell_1^{e_1} \cdots \ell_a^{e_a}$; $e = \max_i(e_i)$; $\ell = \max_i(\ell_i)$; $d$ is such that all $R + P_i, R + Q_i$ live in $A(\mathbb{F}_{q^d})$; and $m$ is the level of theta coordinates describing

[14] Robert calls this the *contragredient* in [89].

[15] For example, when $N - n = x^2 + y^2$, then $\alpha = (x, y; -y, x)$ is a polarisation-respecting endomorphism on $A^2, B^2$.

[16] *i.e.* $\{P_i, Q_i\}$ is a basis of $A[\ell_i^{e_i}]$ where $N = \ell_1^{e_1} \cdots \ell_a^{e_a}$ and $\ell_1, \ldots, \ell_a$ are coprime

[17] which requires factoring $N - n$ in general

$A, B$ [89, Lem. 5.7]. With the $N$-torsion *accessible*[18] this justifies calling such interpolation data an *HD-representation* of $\varphi$, because it gives rise to an efficient representation of $\varphi$.

We remark that it is possible to efficiently evaluate $\Phi$ (and therefore $\varphi$) if $\varphi$ is only known on $A[N_1] \cup A[N_2] \subseteq A[N]$ where $N = N_1N_2$ by *splitting the HD-representation* [89, Sec. B.2]. Informally, this is because it is possible to decompose $\Phi = \Phi_2\Phi_1$ into $N_i$-isogenies which satisfy $\ker(\Phi_1) \subseteq A[N_1]$ and $\ker(\widetilde{\Phi_2}) \subseteq B[N_2]$. We remark this does not require $N_1$ coprime to $N_2$ and is in particular true for $N_1 = N_2$.

More precisely, $\ker(\Phi_1) = \ker(\Phi) \cap (A^u \times B^u)[N_1]$ [42, Prop. 13], and so we have $\ker(\Phi_1) = \{((N-n)P, (\mathrm{id}_u\, \varphi) \circ \alpha(P)) \mid P \in (A^u \times B^u)[N_1]\}$.[19] Likewise for the polarised dual, $\ker(\widetilde{\Phi_2}) = \{((N-n)P, (\mathrm{id}_u\, \varphi) \circ \alpha(P)) \mid P \in (A^u \times B^u)[N_2]\}$, where the values $\widetilde{\varphi}(P)$ are recovered from knowing $\varphi(P)$ by computing discrete logarithms in $\mu_N$. Indeed, by properties of the Weil pairing, $e_{B,N}(\varphi(P), Q) = e_{A,N}(P, \widetilde{\varphi}(Q))$.

**Testing for division.** To test whether a given $n$-isogeny $\varphi$ factors through scalar multiplication by $m$, one can produce apparent interpolation data for $\psi = \varphi/m$ by computing $\{(P_i, \varphi(P_i)/m, Q_i, \varphi(Q_i)/m\}_i^j$ on some CRT bases of the $d_j$-torsion, with $N = d_1d_2 > n/m^2$ prime to $m$.

From this interpolation data, one obtains a maximally isotropic subgroup of $E_1^u \times E_2^u$ by selecting a powersmooth polarised degree $N$, finding a $u \times u$ matrix $\alpha$ which induces a polarised endomorphism on $E_1^u \times E_2^u$ with determinant $N - n/m^2$ and writing down the subgroup as in (4). This subgroup is the kernel of *some* $N$-isogeny $\Phi\colon E_1^u \times E_2^u \to A$ and because $N$ is powersmooth, it is possible to compute the codomain $A$ of $\Phi$ in polynomial time.

If $A \ncong E_1^u \times E_2^u$, then $\Phi$ does not encode one-dimensional isogenies, hence $\varphi$ certainly does not factor through multiplication by $m$; if $A \cong E_1^u \times E_2^u$, then $\Phi$ is a $u \times u$ matrix of $n_{ij}$-isogenies $\Phi_{ij}$ which needs further investigation. Using pairing computations on the images of $\Phi_{ij}$, the degree $n_{ij}$ of $\Phi_{ij}$ can be recovered, and the isogeny $\Phi_{i'j'}$ of degree $n_{i'j'} = n/m^2$ can be identified [89, Lem. 6.2]. Evaluating on a point $P$ of order $N \geq 4n/m^2 + 1$, and testing for equality $\varphi(P)/m = \Phi_{i'j'}(P)$, one can conclude whether $m$ divides $\varphi$ or not.

## 3 An Active attack

We now present a powerful active attack against the PEARL-SCALLOP group action, which uses a *static action-CDH* oracle to model the party being attacked. We also demonstrate two less effective attacks using the weaker *hashed static action-CDH* and *static action-DDH* oracles. Whilst the attacks do not impact the conjectured security of the currently proposed parameter sets, the corresponding oracles have much stronger cryptographic motivation (cf. Subsection 3.3), and so we discuss their use for completeness.

[18] *i.e.* is defined over an extension of degree polynomial in $\log(p)$ [89, Def. A.1]

[19] under the continued assumption that $N$ is prime to $n$.

### 3.1 Notation

Let $K$ be an imaginary quadratic number field and let $\mathcal{O}_K = \mathbf{Z}[\sigma]$ be its ring of integers. Let $f \in \mathbf{Z}_{>0}$ be a square-free integer and write $f = \prod_{i=1}^{r} f_i$ for its prime factorization. Denote by $\mathcal{O}$ the order of conductor $f$ in $\mathcal{O}_K$. For $0 \leq i \leq r$, we will also write $\mathcal{O}^{(i)}$ for the order of conductor $f_1 \cdots f_i$ in $\mathcal{O}_K$, so that $\mathcal{O}^{(0)} = \mathcal{O}_K$ and $\mathcal{O}^{(r)} = \mathcal{O}$. Let $n \in \mathbf{Z}_{>0}$ and let $\ell_1, \ldots, \ell_n$ denote prime numbers that split in $\mathcal{O}$ (in particular, they are all coprime to the conductor $f$). For every $\ell_j$, fix one of the two prime ideals $\mathfrak{l}_j \subseteq \mathcal{O}$ that lies above it, and write $\mathfrak{l}_j^{(i)} = \mathfrak{l}_j \mathcal{O}^{(i)}$ for its extension to $\mathcal{O}^{(i)}$. Define

$$\varpi^{(i)} \colon \mathbf{Z}^n \to \mathrm{Cl}(\mathcal{O}^{(i)}), \quad (s_1, \ldots, s_n) \mapsto \left[\mathfrak{l}_1^{(i)}\right]^{s_1} \cdots \left[\mathfrak{l}_n^{(i)}\right]^{s_n}.$$

Assume that every $\varpi^{(i)}$ is surjective. The $i$-th *relation lattice* $\Lambda^{(i)}$ is defined to be the kernel of $\varpi^{(i)}$. We also write $\Lambda^{(-1)} = \mathbf{Z}^n$. Note that the relationship between the orders and the relation lattices is strictly inclusion preserving, that is, $\mathcal{O}^{(i)} \subsetneq \mathcal{O}^{(j)}$ implies $\Lambda^{(i)} \subsetneq \Lambda^{(j)}$.

We say that an $\mathcal{O}$-oriented curve $(E, \iota)$ is *at level* $i$ if $\mathcal{O}^{\mathrm{pr}}(\iota) = \mathcal{O}^{(i)}$. In particular, if $(E, \iota)$ is at level $i$, then its stabilizer for the action in (3) is $\Lambda^{(i)}$. Moreover, we say that two curves $(E, \iota), (E', \iota')$ at level $i$ are *siblings* if they lie below the same curve on level $i-1$, *i.e.* there exists a vector $\mathbf{v_i}$ in $\Lambda^{(i-1)}$ such that $\mathbf{v_i} * (E, \iota) = (E', \iota')$.

### 3.2 The attacks

We describe our attacks using the language of exponent vectors. That is, we consider the class group action as given by (3). This agrees with the usual method for evaluating the group action in practice (cf. Algorithm 1). Assume that all lattices of relations $\Lambda^{(i)}$ have been computed. Moreover, assume that a precomputed list of $\mathcal{O}$-oriented curves $(E_0, \iota_0), \ldots, (E_r, \iota_r)$ with $(E_i, \iota_i)$ at level $i$ is known. Note that we do not assume knowledge of isogenies between different $(E_i, \iota_i)$ levels. Write $\kappa_i = \Lambda^{(i-1)}/\Lambda^{(i)}$ for the kernel of the surjective map $\mathrm{Cl}(\mathcal{O}^{(i)}) \to \mathrm{Cl}(\mathcal{O}^{(i-1)})$. Recall that $\#\kappa_0 = \#\,\mathrm{Cl}(\mathcal{O}^{(0)}) = h(D_K) \approx \sqrt{-D_K}$ [91] and $\#\kappa_i = f_i - (D_K \mid f_i) = f_i \pm 1$ [36, Th. 7.24], where $D_K = \mathrm{Disc}(\mathcal{O}_K)$.

Suppose now that Alice has secret key $\mathbf{a}$ in $\mathbf{Z}^n$. We describe three active attacks to recover $\mathbf{a}$ by modelling the interaction with Alice through one of the following three oracles. We discuss the cryptographic motivation of these oracles later.

(i) *Static action-CDH oracle* $\mathcal{A}^{\mathbf{a}}$. On input an $\mathcal{O}$-oriented curve $(E, \iota)$, the oracle returns $\mathbf{a} * (E, \iota)$.
(ii) *Hashed static action-CDH oracle* $\mathcal{A}^{\mathbf{a}}_{\mathsf{H}}$. On input an $\mathcal{O}$-oriented curve $(E, \iota)$, the oracle returns the hash $\mathsf{H}(\mathbf{a} * (E, \iota))$.
(iii) *Static action-DDH oracle* $\mathcal{A}^{\mathbf{a}}_{?}$. On input an $\mathcal{O}$-oriented curve $(E, \iota)$ and a bitstring $\mathsf{h}$, the oracle returns the bit $b = 1$ if $\mathsf{H}(\mathbf{a} * (E, \iota)) = \mathsf{h}$, else $b = 0$.

The corresponding attacks are as follows.

*Attack 3.1 (Using the static action-CDH oracle).* Query $\mathcal{A}^{\mathbf{a}}$ on the curves $(E_i, \iota_i)$ to obtain $(E_i^{\mathbf{a}}, \iota_i^{\mathbf{a}})$. Then inductively proceed as follows.

(i) *Base case.* Solve the vectorisation problem between $(E_0, \iota_0)$ and $(E_0^{\mathbf{a}}, \iota_0^{\mathbf{a}})$ to obtain $[\mathbf{c}_0]$ in $\mathbf{Z}^n/\Lambda^{(0)}$. Then $\mathbf{a}_0 := \mathbf{c_0}$ is equal to $\mathbf{a}$ modulo $\Lambda^{(0)}$.
(ii) *Inductive step.* Assume that $\mathbf{a}_{i-1} = \mathbf{a}$ modulo $\Lambda^{(i-1)}$ is known. Compute $(E_i', \iota_i') = \mathbf{a}_{i-1} * (E_i, \iota_i)$ using any polynomial-time algorithm for evaluating the class group action (e.g. using [84]). Solve the vectorisation problem between the sibling curves $(E_i', \iota_i')$ and $(E_i^{\mathbf{a}}, \iota_i^{\mathbf{a}})$ to obtain $[\mathbf{c}_i]$ in $\Lambda^{(i-1)}/\Lambda^{(i)}$. Then $\mathbf{a}_i := \mathbf{a}_{i-1} + \mathbf{c}_i$ is equal to $\mathbf{a}$ modulo $\Lambda^{(i)}$.

*Attack 3.2 (Using the hashed static action-CDH oracle).* Query $\mathcal{A}_{\mathsf{H}}^{\mathbf{a}}$ on the curves $(E_i, \iota_i)$ to obtain $\mathsf{h}_i = \mathsf{H}((E_i^{\mathbf{a}}, \iota_i^{\mathbf{a}}))$. Then inductively proceed as follows.

(i) *Base case.* Compute $\mathbf{a}_0$ such that $\mathsf{H}(\mathbf{a}_0 * (E_0, \iota_0)) = \mathsf{h}_0$ using brute force, by acting by (representatives of) elements in $\mathbf{Z}^n/\Lambda^{(0)}$. Note that we then obtain $\mathbf{a}_0 = \mathbf{a}$ modulo $\Lambda^{(0)}$.
(ii) *Inductive step.* Assume that $\mathbf{a}_{i-1} = \mathbf{a}$ modulo $\Lambda^{(i-1)}$ is known. Compute $(E_i', \iota_i') = \mathbf{a}_{i-1} * (E_i, \iota_i)$ using any polynomial-time algorithm for evaluating the class group action (e.g. using [84]). Compute $\mathbf{a}_i$ such that $\mathsf{H}(\mathbf{a}_i * (E_i, \iota_i)) = \mathsf{h}_i$ using brute force, by acting by (representatives of) elements in $\Lambda^{(i)}/\Lambda^{(i-1)}$. We obtain $\mathbf{a}_i = \mathbf{a}$ modulo $\Lambda^{(i)}$.

*Attack 3.3 (Using the static action-DDH oracle).* Query $\mathcal{A}_?^{\mathbf{a}}$ on the curves $(E_i, \iota_i)$, together with a guess $\mathsf{h}_{g,i} = \mathsf{H}(\mathbf{g}_i * (E_i, \iota_i))$ obtained from $\mathbf{g}_i$ in $\Lambda^{(i-1)}/\Lambda^{(i)}$ until $\mathsf{h}_{g,i} = \mathsf{h}_i = \mathsf{H}((E_i^{\mathbf{a}}, \iota_i^{\mathbf{a}}))$ is found. Then proceed with the hashed static action-CDH attack, Attack 3.2.

We remark that in each of the attacks, the queries to the $\mathcal{A}^{\mathbf{a}}, \mathcal{A}_{\mathsf{H}}^{\mathbf{a}}, \mathcal{A}_?^{\mathbf{a}}$ oracles are independent to the secret $\mathbf{a}$, making these attacks non-adaptive; in particular allowing for the expensive computation to be offline. This is a small detail of Attack 3.3: it really makes all (independent) $\mathcal{A}_?^{\mathbf{a}}$ queries first, before proceeding to the inductive loop; this does not affect the overall complexity and avoids a more analogous strategy to Attack 3.2, with guesses submitted to the oracle at every level, which would result in an adaptive attack.

We now proceed with a precise analysis of the attacks' complexities.

**Lemma 3.4.** *Attack 3.1 makes $r+1$ $\mathcal{A}^{\mathbf{a}}$-oracle queries and can be implemented classically using $\widetilde{O}(\max(\{f_i\}_i, |D_K|^{1/2})^{1/2})$ group action computations, and quantumly using $\exp(O(\log(\max(\{f_i\}_i, |D_K|^{1/2}))^{1/2}))$ group action computations. Note that group action* computations *(*i.e. *computing $\mathbf{s} * (E, \iota)$ for some known vector $\mathbf{s}$ in $\mathbf{Z}^n$) are done without querying the $\mathcal{A}^{\mathbf{a}}$ oracle.*

*Proof.* We immediately see that, crucially, the attack performs vectorisation successively at every level, not simultaneously; hence costs are added, not multiplied.

The initial vectorisation in the base case (at the *crater* of the isogeny volcano), occurs in the class group of $\mathcal{O}_K$ which is of size $\widetilde{O}(|D_K|^{1/2})$. The vectorisation problem at level $i$ between $(E'_i, \iota'_i)$ and $(E_i^{\mathbf{a}}, \iota_i^{\mathbf{a}})$ is within the same $\Lambda^{(i-1)}$-orbit precisely because $\mathbf{a}_i = \mathbf{a}$ modulo $\Lambda^{(i-1)}$. Each of these $\Lambda^{(i-1)}$-orbits is simply acted on by $\kappa_i = \Lambda^{(i-1)}/\Lambda^{(i)}$, where we recall that $\#\kappa_i = f_i \pm 1$.

Having identified the sizes of the groups in which vectorisation occurs, we obtain the stated complexities by employing meet-in-the-middle search [55] in the classical case and Kuperberg's linear hidden shift algorithm [66] in the quantum setting. □

**Lemma 3.5.** *Attack 3.2 makes $r+1$ $\mathcal{A}_{\mathsf{H}}^{\mathbf{a}}$-oracle queries; and can be implemented classically using $\widetilde{O}(\max(\{f_i\}_i, |D_K|^{1/2}))$ hashed group action computations, and quantumly using $\widetilde{O}(\max(\{f_i\}_i, |D_K|^{1/2})^{1/2})$ hashed group action computations. Note that hashed group action* computations *(*i.e. *computing $\mathsf{H}(\mathbf{s} * (E, \iota))$ for some known vector $\mathbf{s}$ in $\mathbf{Z}^n$) are done without using the $\mathcal{A}_{\mathsf{H}}^{\mathbf{a}}$ oracle.*

*Proof.* As in Attack 3.1, the vectorisation problems can be solved successively at every level. The main computational cost is brute-force pre-image search in the sets $\kappa_i = \Lambda^{(i-1)}/\Lambda^{(i)}$. Classically, this can be done using $\widetilde{O}(|D_K|^{1/2})$ hashed group action computations at the crater, and with $O(f_i)$ hashed group action computations at lower levels. Quantumly, we get a quadratic speedup using Grover's search algorithm [58] over the classical brute force search to obtain the stated complexity. □

**Lemma 3.6.** *Attack 3.3 can be implemented using $\widetilde{O}(\max(\{f_i\}, |D_K|^{1/2}))$ classical $\mathcal{A}_{?}^{\mathbf{a}}$-oracle queries and hashed group action computations; and quantumly implemented making $\widetilde{O}(\max(\{f_i\}_i, |D_K|^{1/2})^{1/2})$ $\mathcal{A}_{?}^{\mathbf{a}}$-oracle queries and hashed group action computations.* □

*Proof.* As in the previous two attacks, the vectorisation problems can be solved successively at every level. Classically, to obtain the correct guess $\mathbf{g}_i$, one must first compute $\widetilde{O}(|D_K|^{1/2})$ group actions and then submit these as queries to the $\mathcal{A}_{?}^{\mathbf{a}}$ oracle at the crater, and $O(f_i)$ queries at lower levels; quantumly we may use Grover search to reduce this to $\widetilde{O}(|D_K|^{1/4})$ action computations and queries at the crater, and to $O(f_i^{1/2})$ action computations and queries at levels below. □

**Implications for concrete PEARL-SCALLOP parameters.** Using the parameter sets targeting a security level equivalent to CSIDH-$\{1024, 2048, 4096\}$, we see that — classically — Attack 3.1 (which assumes access to the *static action-CDH oracle*) requires $\approx 2^{64}$, $2^{150}$, $2^{320}$ group action evaluations respectively. Since PEARL-SCALLOP targets 128 classical bits of security, this constitutes a significant classical security reduction for the CSIDH-1024 case.

The quantum security, however, is substantially affected for all parameter sets. Indeed, Kuperberg's algorithm [66] is a generic algorithm for solving discrete logarithms for commutative group actions, that is subexponential in the size of the group. Compared to $\mathrm{Cl}(\mathcal{O})$, which is of size $\approx 512, 1024, 2048$ bits for the

CSIDH-$\{1024, 2048, 4096\}$ parameter sets respectively, the relative vectorization groups $\kappa_i := \ker\left(\mathrm{Cl}(\mathcal{O}^{(i)}) \to \mathrm{Cl}(\mathcal{O}^{(i-1)})\right)$ are significantly smaller; of (maximal) size $128, 300$, and 640 bits respectively. Moreover, since $\Lambda^{(i)} \supseteq \Lambda^{(r)}$ for all $i$, the quantum cost of the group action evaluation oracle (cf. [10]) is at most as large as the one for $\mathrm{Cl}(\mathcal{O}) = \mathrm{Cl}(\mathcal{O}^{(r)})$-vectorization (on which the proposed quantum security is based).

The *hashed static action-CDH oracle* (Attack 3.2) and *static action-DDH oracle* (Attack 3.3) versions of the attack do not directly compromise the conjectured classical or quantum security. Indeed, we note that the quantum versions of the attacks likely do not outperform solving the full vectorization problem for $\mathrm{Cl}(\mathcal{O})$ using Kuperberg's algorithm.

### 3.3 Motivating the oracles

We discuss the motivation of all three oracles in descending strength.

**The static action-CDH oracle $\mathcal{A}^{\mathbf{a}}$.** First, we emphasize that the $\mathcal{A}^{\mathbf{a}}$ oracle truly gives rise to a *static* action-CDH oracle, and not a full action-CDH oracle. This is an important distinction, because action-CDH and action-DLOG are quantumly equivalent [54]. The cost for evaluating $(t\mathbf{a})*E$ is $t$ $\mathcal{A}^{\mathbf{a}}$ calls, whereas a full action-CDH oracle would only require $O(\log(t))$ calls, by double-and-adding. Efficient computation of $(t\mathbf{a}) * E$ is a crucial ingredient in the quantum action-CDH to action-DLOG reduction.

Still, the $\mathcal{A}^{\mathbf{a}}$ oracle is very powerful, because it fully impersonates Alice: any interaction in any cryptographic protocol that defines Alice through knowing $\mathbf{a}$ can be performed by the oracle $\mathcal{A}^{\mathbf{a}}$. However, it is still meaningful to speak of key recovery from such an oracle because versions of this oracle appear in some threshold settings.

For example, a naive implementation of the threshold ElGamal decryption scheme described in [45, Sec. 3.2] exposes the $\mathcal{A}^{\mathbf{a}}$ oracle. Indeed, during decapsulation, the first user will apply their secret to an adversarially chosen curve and relay the result to the next user in the threshold group. Since the parties are assumed to communicate publicly, this value can be extracted by the same adversary that submitted the curve. Even if the parties used secure channels for communication, the adversary could be part of the threshold group, which is a common threat model in the threshold setting.

**The hashed static action-CDH oracle $\mathcal{A}^{\mathbf{a}}_{\mathbf{H}}$.** This oracle is akin to obtaining the session key obtained through a key exchange, where the hash function is replaced with a key-derivation function.

The query complexity $r+1$ of our attack is dictated by the number $r$ of (large) prime divisors of the conductor $f$, *i.e.* logarithmic in $f$. Concretely though, to make the ascending isogenies computationally infeasible, the conductor is usually

particularly non-smooth, with only a handful of large factors *e.g.* 3 for PEARL-SCALLOP's CSIDH-1024 parameters set. As such, just 4 leaked session keys would give sufficient information to mount the offline attack.

**The static action-DDH oracle $\mathcal{A}^{\mathsf{a}}_{?}$.** This oracle is naturally instantiated in many internet communication protocols. An adversary may initiate communications with a server by submitting many non-primitively oriented curves, and if they can decrypt the responses, meaning they have correctly guessed the session keys, they can proceed with the inductive phase of the attack.

## 4 Validating primitive orientations

One method to thwart these active "class group downgrade" attacks is to *validate* the orientation of the curves before continuing with the protocol. In the language of cryptographic group actions [3], with $G$ acting on $X$, validation means that parties simply ensure that a proposed element $x$, *e.g.* given as a bitstring, actually encodes an element in the set $X$ before acting with their secrets $g$ in $G$. In the context of a NIKE, this is referred to as *public-key validation*, since parties act by their secrets on (potentially adversarially generated) *public keys*.

In the context of class group actions on oriented elliptic curves, a public key is often essentially a curve $E$ together with an orientation $\iota$. We note that every orientation $\iota\colon K \to \mathrm{End}^0(E)$ is uniquely defined by the image $\gamma = \iota(\omega)$ of a generator $\omega$ of $\mathcal{O}^{\mathrm{pr}}(\iota)$. Conversely, every non-scalar endomorphism $\gamma$ of $E$ defines a $\mathbf{Q}(\sqrt{\mathrm{disc}(\gamma)})$-orientation $\iota_\gamma$ characterised by $(\mathrm{tr}(\gamma) - \sqrt{\mathrm{disc}(\gamma)})/2 \mapsto \gamma$. In practice, orientations are usually explicitly encoded through an endomorphism. Indeed, the only family of isogeny class group computations that do *not* do this are the CSIDH/CSURF families [25,21], for there the orientation is implicitly given by the Frobenius endomorphism.

Hence, we assume that the orientation is given as an endomorphism $\omega$ on $E$. To verify that $(E, \iota_\omega)$ is in fact a primitive $\mathcal{O}$-orientation for the desired order $\mathcal{O}$, one must verify that $\mathbf{Z}[\omega]$ has the correct discriminant, which establishes that $\mathbf{Z}[\omega] \cong \mathcal{O}$, and that $\iota_\omega$ is a *primitive* $\mathbf{Z}[\omega]$-orientation. We treat these two challenges in the next two subsections.

### 4.1 Verifying the discriminant

The general setting of an oriented group action requires that the orientation $\omega$ is given by an *efficient representation* [89, Sec. 2.1]. In particular, this means that the degree of $\omega$ is (implicitly or explicitly) given.

Concretely, we recall that in PEARL-SCALLOP $\omega$ is represented as a pair of points $P, Q \in E$ of order $2^e$ which generate the kernels of isogenies $\varphi_P, \varphi_Q$, respectively, and satisfy $\widehat{\varphi_Q}\varphi_P = \omega$. The order $\mathcal{O}$ by which $E$ should be primitively oriented by has discriminant $f^2 D_K$, and the degree of $\omega$ should be $2^{2e}$, both values supplied in the public parameters of the scheme. To verify the degree of $\omega$, one checks that $P$ and $Q$ have order $2^e$ and that $\widehat{\varphi_Q}\varphi_P$ is a cyclic

endomorphism. Since $\widehat{\varphi_Q}\varphi_P$ has degree $2^{2e}$, its cyclicity could be checked by verifying that $\widehat{\varphi_Q}\varphi_P(E[2]) \neq \{0\}$. Nevertheless, we postpone the cyclicity check to the primitivity check, as the orientation being primitive implies that $\widehat{\varphi_Q}\varphi_P$ is cyclic.

Then, to verify the that discriminant satisfies $\mathrm{disc}(\omega) = \mathrm{tr}(\omega)^2 - 4\deg(\omega) = \mathrm{disc}(\mathcal{O})$, it remains to verify that the trace satisfies $\mathrm{tr}(\omega)^2 = \mathrm{disc}(\mathcal{O}) + 4\deg(\omega)$. Whilst one can *compute* the trace in polynomial time, with reasonable runtimes in practice [82], we must merely *verify* that the (square of the) trace of the given endomorphism matches what we expect. This distinction allows to avoid potentially expensive discrete logarithm computations.

In general, a natural way to check the trace is to evaluate $\omega$ and its dual $\hat{\omega}$ on one of the points of a basis $\{S_1, S_2\}$ of $E[N]$ for some integer $N$, compute the Weil pairing

$$e_N(S_1, (\omega + \hat{\omega})(S_2)) = e_N(S_1, S_2)^{\mathrm{tr}(\omega)}$$

and check whether it matches $e_N(S_1, S_2)^{\pm\sqrt{\mathrm{disc}(\mathcal{O})+4\deg(\omega)}}$ for the expected value of the discriminant $\mathrm{disc}(\mathcal{O})$.

This test only verifies the value of $\mathrm{tr}(\omega)$ modulo $N$, hence only becomes sufficient when $N \geq 2\sqrt{\deg(\omega)}$. Indeed, assuming $\omega$ is not (multiplication by) an integer, the order $\mathbf{Z}[\omega]$ it generates has negative discriminant $\mathrm{Disc}(\mathbf{Z}[\omega]) = \mathrm{tr}(\omega)^2 - 4\deg(\omega)$ and so $\mathrm{tr}(\omega)^2 < 4\deg(\omega)$. This is also the Hasse-Weil bound for an endomorphism $\omega$. Note that verifying the correct sign of $\mathrm{tr}(\omega)$ is not needed, since only the square is relevant for the discriminant. In fact, we can always assume that the parameters are chosen such that $\mathrm{tr}(\omega)$ is positive, as one can always replace $\omega$ by $-\omega$.

In the rest of this subsection, we improve on this idea to design a trace validation method to validate the trace $t$ of any supersingular endomorphism $\theta$ in $\mathrm{End}(E)$ of known degree $d$ satisfying $4\sqrt{d}+1 \leq p+1$, by evaluating exclusively $\hat{\omega}$. This is especially relevant for PEARL-SCALLOP, because we see that the group-action evaluation algorithm (Algorithm 1) already evaluates $\hat{\omega}$ on a large torsion basis. We note that an early rejection due to an incorrect orientation does not leak any secret information, because the values of $\hat{\omega}$ do not depend on secrets, even if they are re-used later in conjunction with the secret key to compute the action. Finally, we note that when validating the trace up to sign one can relax the requirement on $d$ to $2\sqrt{d} + 1 \leq p + 1$.

Recall that the field characteristic $p$ has the shape $p + 1 = c2^e \prod_{i=1}^{n} \ell_i$ where the ideals lying above the primes $\ell_i$ are used to evaluate the group action; and the concrete parameter choices enforce that $p \geq 2^{2e} = \deg(\omega)$.

**Lemma 4.1.** *Let $E$ be a supersingular curve and let $\theta \in \mathrm{End}(E)$ be an endomorphism of degree $d$ and of positive trace. Let $t$ be an integer such that $0 \leq t \leq 2\sqrt{d}$ and let $R$ be a point of order $N \geq 2\sqrt{d} + 1$. If $\theta^2(R) - [t]\theta(R) + [d]R = 0$, then $\mathrm{tr}(\theta) = t$.*

*Proof.* Let $u > 0$ be the trace of $\theta$. Then $\theta^2(R) - [u]\theta(R) + [d]R = 0$. Hence, we have that $\theta^2(R) - [u]\theta(R) + [d]R = \theta^2(R) - [t]\theta(R) + [d]R$, that is $[u]\theta(R) = [t]\theta(R)$, implying that $u \equiv t \mod N$. Since $0 \leq u, t \leq 2\sqrt{d} < N$, we conclude $u = t$. □

To verify the trace of a given $\omega$ using Lemma 4.1, we only need to check that the (purported) minimal polynomial of $\omega$ holds on a single point $R$ of order $N \geq 2\sqrt{\deg(\omega)} + 1 = 2^{e+1} + 1$.

We now describe how to check that $\hat{\omega}^2(R) - [t]\hat{\omega}(R) + [\deg(\omega)]R = 0$. Let $S_1$,$S_2$ be a basis of $E[N]$, let $S_1' = \hat{\omega}(S_1)$ and $S_2' = \hat{\omega}(S_2)$. Write $\hat{\omega}(R) = [x]S_1 + [y]S_2$, then

$$e_N(\hat{\omega}(R), S_2) = e_N(S_1, S_2)^x, \quad e_N(S_1, \hat{\omega}(R)) = e_N(S_1, S_2)^y, \text{ and}$$

$$\hat{\omega}^2(R) = \hat{\omega}([x]S_1 + [y]S_2) = [x]\hat{\omega}(S_1) + [y]\hat{\omega}(S_2) = [x]S_1' + [y]S_2'.$$

Hence, we obtain that $\hat{\omega}^2(R) - [t]\hat{\omega}(R) + [\deg(\omega)]R = 0$ if and only if $\hat{\omega}^2(R) = [t]\hat{\omega}(R) - [\deg(\omega)]R$, which holds if and only if $[t]\hat{\omega}(R) - [\deg(\omega)]R = [x]S_1' + [y]S_2'$. Setting $R_2 = [t]\hat{\omega}(R) - [\deg(\omega)]R$, the last equality holds if and only if

$$e_N(R_2, S_2') = e_N(S_1', S_2')^x = e_N(S_1, S_2)^{x\deg(\omega)} = e_N(\hat{\omega}(R), S_2)^{\deg(\omega)} \text{ and}$$

$$e_N(S_1', R_2) = e_N(S_1', S_2')^y = e_N(S_1, S_2)^{y\deg(\omega)} = e_N(S_1, \hat{\omega}(R))^{\deg(\omega)}.$$

Notice that if one chooses $R = S_1$, then $\hat{\omega}(R) = S_1'$ and

$$e_N(S_1', R_2) = e_N(S_1', [t]S_1' - [\deg(\omega)]S_1) = e_N(S_1, S_1')^{\deg(\omega)} = e_N(S_1, \hat{\omega}(R))^{\deg(\omega)},$$

meaning that the second check always passes. We are hence left with only one pairing equality to be tested.

To summarize, let $S_1, S_2$ be a basis of $E[N]$, let $S_1' = \hat{\omega}(S_1)$ and $S_2' = \hat{\omega}(S_2)$. The trace check is done by setting $R_2 = [t]\hat{\omega}(S_1) - [\deg(\omega)]S_1$, and checking whether the following equality holds

$$e_N(R_2, S_2') = e_N(S_1', S_2)^{\deg(\omega)}.$$

In the summary of our orientation validation (Section 4.3), we will be using a point $R = S_1$ of order a (small) multiple of $p + 1$.

### 4.2 Testing for primitivity

We now present two different algorithms to test for primitivity: the first method follows a more folklore approach to verify primitivity by computing a handful of group actions on carefully selected ideals; the second method applies more recently developed techniques, employing higher-dimensional isogenies to test the orienting endomorphism for divisibility by primes dividing the conductor.

The only requirement of the first method is that the class group structure is known, which is exactly the setting which all SCALLOP variants target. Conversely, the second method always runs in polynomial time for all isogeny class group actions, and when the discriminant of the orienting endomorphism is sufficiently small in comparison to the available 2-torsion, it can be concretely implemented with very performant algorithms.

On balance, the PEARL-SCALLOP parameters allow for concrete instantiations in which the second method likely outperforms the first.

**Using the group action** If a given $\mathcal{O}$-orientation $\iota$ on $E$ is non-primitive, so that $\mathcal{O}' = \mathcal{O}^{\mathrm{pr}}(\iota) \supsetneq \mathcal{O}$, then the action on $(E, \iota)$ by any ideal $\mathfrak{a} \subseteq \mathcal{O}$ such that $\mathfrak{a}\mathcal{O}'$ represents a trivial element in $\mathrm{Cl}(\mathcal{O}')$ is trivial, even if $\mathfrak{a}$ represents a non-trivial class in $\mathrm{Cl}(\mathcal{O})$. As a consequence, testing triviality of the action by such an ideal for every superorder $\mathcal{O}'$ of $\mathcal{O}$ allows one to test whether $(E, \iota)$ is primitive or not.

Moreover, if an $\mathcal{O}$-orientation cannot be extended to an intermediate order $\mathcal{O} \subsetneq \mathcal{O}'' \subseteq \mathcal{O}'$, then clearly it cannot be extended to $\mathcal{O}'$. Consequently, to verify whether $(E, \iota)$ is primitively oriented by $\mathcal{O}$, it suffices to perform this action-triviality test for all orders $\mathcal{O}''$ in which $\mathcal{O}$ has prime relative conductor. In other words, if $\mathcal{O}$ has conductor $f = \prod_{i=1}^{r} f_i$ in $\mathcal{O}_K$, then it suffices to test orders $\mathcal{O}_{f_i}$ with conductor $f/f_i$ on $\mathcal{O}_K$, for all $1 \leq i \leq r$.

To carry out this check, one is faced with the problem of finding non-principal ideals of $\mathcal{O}$ that become principal when lifted to $\mathcal{O}_{f_i}$, namely ideals whose class is in the kernel of the map $\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i})$ from (1). We sketch here how one can compute such ideals, provided that the structure of $\mathrm{Cl}(\mathcal{O})$ and $\mathrm{Cl}(\mathcal{O}_{f_i})$ is known.

*Remark 4.2.* The outlined strategy is reminiscent of [14, Sec. 3.2], in which the purported conductor of the endomorphism ring of an *ordinary* curve is verified. Our situation is different, because the parameters of our isogeny volcano allow us to compute the class group structure at every level $\mathcal{O}^{(i)}$, and so we do not need to FindRelations during certification.

In PEARL-SCALLOP, the group structure of $\mathrm{Cl}(\mathcal{O})$ is computed in the parameter generation phase, and public (see [4, Section 2.3] on how it is computed in practice). It is given as a set of $\mathcal{O}$-ideals $\{\mathfrak{l}_j\}_{1 \leq j \leq n}$ whose classes generate the whole class group, and a basis of the relation lattice $\Lambda_{\mathcal{O}}$ (equal to $\Lambda^{(r)}$ in the notation of Section 3.1). Similarly, one can compute $\mathrm{Cl}(\mathcal{O}_{f_i})$ by computing its relation lattice $\Lambda_{f_i}$. Then, since

$$\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i}) \cong \Lambda_{\mathcal{O}_{f_i}}/\Lambda_{\mathcal{O}},$$

we can sample vectors $(e_1, \dots e_n) \in \Lambda_{\mathcal{O}_{f_i}}$ that are not zero modulo $\Lambda_{\mathcal{O}}$, so that the product $\mathfrak{g} = \prod_{i=1}^{n} \mathfrak{l}_i^{e_i}$ is an element of $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i}))$.

Alternatively, another way to find ideals in $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i}))$ and express them in terms of a given set of generators of $\mathrm{Cl}(\mathcal{O})$ is described in [39, Section 3.3], in a context where $\mathcal{O}$ has absolute conductor which is a power of a small prime, and hence $\mathrm{Cl}(\mathcal{O})$ is cyclic or almost cyclic. Nevertheless, we can also use a similar approach for a conductor which is a product of distinct primes that split in $\mathcal{O}_K$, as is the case for PEARL-SCALLOP. Indeed, we can prove that $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i})) \cong \mathbf{F}_{f_i}^{\times}$ for any prime $f_i$ that splits in $\mathcal{O}_K$ (see Lemma 4.3 below), in particular it is a (cyclic) subgroup of order $f_i - 1$ in $\mathrm{Cl}(\mathcal{O})$. Assuming $\mathrm{Cl}(\mathcal{O})$ to be cyclic, or enforcing parameters to ensure this condition, to find an element in $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i}))$, it then suffices to find an element in $\mathrm{Cl}(\mathcal{O})$ whose order divides $f_i - 1$; namely, upon computing the orders of the classes corresponding to each $\mathfrak{l}_i$ in $\mathrm{Cl}(\mathcal{O})$ we can sample vectors $(e_1, \dots, e_n) \in \mathbf{Z}^n$ that

are non-zero modulo $\Lambda_{\mathcal{O}}$, until the class of the product $\mathfrak{g} = \prod_{i=1}^{n} \mathfrak{l}_i^{e_i}$ has order dividing $f_i - 1$ in $\mathrm{Cl}(\mathcal{O})$, yielding an element in $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i}))$. Note that we are only requiring knowledge of the relation lattice of $\mathcal{O}$, rather than that of each $\mathcal{O}_{f_i}$ as well. The property of $\ker(\mathrm{Cl}(\mathcal{O}) \to \mathrm{Cl}(\mathcal{O}_{f_i}))$ being cyclic can be leveraged when $G = \gcd_i(f_i - 1) \neq 1$, which is the case *e.g.* for the concrete parameter sets of the PEARL-SCALLOP implementation, as one could then look for an element $\mathfrak{g}$ in $\mathrm{Cl}(\mathcal{O})$ whose order divides $G$, and carry out a full non-triviality test by evaluating the action of one single ideal $\mathfrak{g}$.

**Lemma 4.3.** *Let $K$ be an imaginary quadratic field and let $\ell$ be a prime that splits in $K$. Let $\mathcal{O}_1 \supseteq \mathcal{O}_2$ be orders of $K$ such that $\mathcal{O}_2$ has relative conductor $\ell$ in $\mathcal{O}_1$. Assuming that $\mathcal{O}_1^\times = \{\pm 1\}$, then*

$$\ker(\mathrm{Cl}(\mathcal{O}_2) \to \mathrm{Cl}(\mathcal{O}_1)) \cong \mathbf{F}_\ell^\times.$$

Before proving the lemma, we remark that the requirement $\mathcal{O}_1^\times = \{\pm 1\}$ only excludes $\mathcal{O}_1$ being the maximal order of $K = \mathbf{Q}(\sqrt{-1})$ or of $K = \mathbf{Q}(\sqrt{-3})$.

*Proof.* If $\mathcal{O}_1^\times = \{\pm 1\}$ then $\mathcal{O}_2^\times = \{\pm 1\}$, and the exact sequence (1) becomes

$$1 \to \frac{(\mathcal{O}_1/\ell\mathcal{O}_1)^\times}{(\mathcal{O}_2/\ell\mathcal{O}_1)^\times} \to \mathrm{Cl}(\mathcal{O}_2) \to \mathrm{Cl}(\mathcal{O}_1) \to 1.$$

In particular, $\ker(\mathrm{Cl}(\mathcal{O}_2) \to \mathrm{Cl}(\mathcal{O}_1)) \cong \frac{(\mathcal{O}_1/\ell\mathcal{O}_1)^\times}{(\mathcal{O}_2/\ell\mathcal{O}_1)^\times}$. Assume without loss of generality that $K \cong \mathbf{Q}(X)/(X^2 + D)$ for some square-free integer $D$. Let $L$ be the absolute conductor of $\mathcal{O}_2$, then $\ell$ divides $L$ and $L/\ell$ is the absolute conductor of $\mathcal{O}_1$. Then,

$$\mathcal{O}_1/\ell\mathcal{O}_1 \cong \frac{\mathbf{Z}[X]/(X^2 + DL^2/\ell^2)}{\ell(\mathbf{Z}[X]/(X^2 + DL^2/\ell^2))} \cong \frac{\mathbf{F}_\ell[X]}{(X^2 + DL^2/\ell^2)}.$$

Since $\ell$ splits in $K$, it holds that $\left(\frac{-D}{\ell}\right) = 1$, hence

$$\frac{\mathbf{F}_\ell[X]}{(X^2 + DL^2/\ell^2)} \cong \mathbf{F}_\ell \times \mathbf{F}_\ell.$$

Since $\mathcal{O}_2/\ell\mathcal{O}_1$ is a subring of $\mathcal{O}_1/\ell\mathcal{O}_1$, and $[\mathcal{O}_1/\ell\mathcal{O}_1 : \mathcal{O}_2/\ell\mathcal{O}_1] = \ell$, it follows that $\mathcal{O}_2/\ell\mathcal{O}_1 \cong \mathbf{F}_\ell$, embedding diagonally into $\mathcal{O}_1/\ell\mathcal{O}_1 \cong \mathbf{F}_\ell \times \mathbf{F}_\ell$. Finally,

$$\frac{(\mathcal{O}_1/\ell\mathcal{O}_1)^\times}{(\mathcal{O}_2/\ell\mathcal{O}_1)^\times} \cong \frac{\mathbf{F}_\ell^\times \times \mathbf{F}_\ell^\times}{\mathbf{F}_\ell^\times} \cong \mathbf{F}_\ell^\times,$$

where the last isomorphism is given by $(x, y) \mapsto xy^{-1}$. □

Notice that computing the special test ideals $\mathfrak{g}$ is done once for each parameter set during the parameter generation stage and can be published as part of public parameters. As such, computing the test ideals themselves does not need

to be done during protocol execution; however, before computing any group action by a secret ideal, one must first compute the action of the test ideals on the given curve to validate its orientation. In PEARL-SCALLOP, this amounts to $r$ additional group action computations. Concretely, for the CSIDH-1024 parameters, $r = 3$, yielding a slowdown factor of 4.

We leave it as an open question to investigate whether it is possible to find particularly cheap test ideals to compute, *e.g.* whose exponent vectors have low $\ell_1$-norm.

**Using a division algorithm.** We now present another approach for validating whether a given orientation is primitive. In essence, we only need to check whether a well-chosen endomorphism coming from the orientation is cyclic.

**Lemma 4.4.** *Let $E$ be an elliptic curve and $\gamma$ an endomorphism of discriminant $\mathrm{Disc}(\gamma) = f^2 d_0$, where $d_0$ is a fundamental discriminant. Then $\iota_\gamma$ is a primitive $\mathbf{Z}[\gamma]$-orientation on $E$ if and only if $\gamma_0 = 2\gamma - \mathrm{tr}(\gamma) + \mathrm{Disc}(\gamma)/\rho$ is not divisible by $2\rho$ for any prime factor $\rho > 1$ of $f$. If $d_0 \equiv 0 \bmod 4$ or $f \equiv 0 \bmod 4$, then the last condition is equivalent to $\gamma_1 = 2\gamma - \mathrm{tr}(\gamma)$ not being divisible by $2\rho$ for any prime factor $\rho > 1$ of $f$.*

*Proof.* Viewing $\gamma$ as an algebraic integer, we see that $(2\gamma - \mathrm{tr}(\gamma) + \mathrm{Disc}(\gamma)/\rho)/(2\rho)$ generates the index-$\rho$ superorder of $\mathbf{Z}[\gamma]$ for any prime divisor $\rho$ of $f$. As such, if the endomorphism $2\gamma - \mathrm{tr}(\gamma) + \mathrm{Disc}(\gamma)/\rho$ factors through scalar multiplication by $2\rho$ for a divisor $\rho$ of $f$, the orientation $\iota_\gamma$ is not $\mathbf{Z}[\gamma]$-primitive.

If $d_0 \equiv 0 \bmod 4$ or $f \equiv 0 \bmod 4$ then $d_0' = (f^2/\rho^2)d_0 \equiv 0 \bmod 4$, and so $(\mathrm{Disc}(\gamma)/\rho)/(2\rho) = (f^2 d_0)/(2\rho^2) = d_0'/2$ is an integer, hence $(2\gamma - \mathrm{tr}(\gamma))/(2\rho)$ also generates the index-$\rho$ superorder of $\mathbf{Z}[\gamma]$. □

*Remark 4.5.* In all PEARL-SCALLOP sets of parameters, $d_0$ is odd, but $f$ turns out to be divided by 8 [4, Sections 3.2, 3.3].

The above lemma delivers us a primitivity testing algorithm. Indeed, the current instantiations of the isogeny class group action encode the orientations of curves $E$ by endomorphisms $\gamma$ in efficient isogeny representation with a discriminant $df^2$. Because it is given in efficient isogeny representation, the degree of $\gamma$ is known and its trace can be verified as a function of the degree and the supposed discriminant, as described in Section 4.1. Once the discriminant is known to be $\mathrm{tr}(\gamma)^2 - 4\deg(\gamma) = f^2 d$, it remains to verify whether $2\gamma - \mathrm{tr}(\gamma)$ is divisible by $2\rho$ for any prime divisor $\rho$ of $f$.

The general problem of testing whether an isogeny $\varphi\colon E_1 \to E_2$ is divisible by an integer can be solved in asymptotic polynomial time [89, Prop. 6.6]. However, we realize that the case of PEARL-SCALLOP is particularly tame, resulting in the computation of 4-dimensional 2-isogenies instead of 8-dimensional $N$-isogenies (which would be necessary in general). Indeed, computing 4-dimensional 2-isogenies can be done efficiently in practice [38,41].

We note that in the setting of PEARL-SCALLOP the conductor $f$ is the product of a few large primes, the fundamental discriminant $D_K$ is 1 modulo 4,

and the endomorphism $\omega_0 = 2\omega - \mathrm{tr}(\omega)$ has degree $4\deg(\omega) - \mathrm{tr}(\omega)^2 = -f^2 D_K$. Picking $N = 2^\bullet$, one sees that the quantity $N - \deg(\varphi) = 2^\bullet + f^2 D_K$ is 1 modulo 4, and so there is hope that concrete parameters can be chosen so that it is a sum of two squares. Robert's *embedding lemma* and the subsequent *division algorithm* (cf. Section 2.3) would then tell us that $\omega_0$ can be tested for division by computing 4-dimensional 2-isogenies.

By tweaking the parameter generation of PEARL-SCALLOP and rejecting early by using bounded trial divisions whilst testing whether $2^{e_i} + (f/f_i)^2 D_K$ is a sum of two squares, we found the following CSIDH-1024 parameters within $\approx 2^{25}$ re-randomisations, taking $\approx 6$ Core-GHz-Hours[20]. The parameters are defined through the seeds

$$a = 271392203191938564610043121904428032251, \quad N = 2^{129},$$

and derived from the expressions $d = 2N^2 - a^2$, $f_1 = a, f_2 = (a+N)/3, f_3 = N - a, f = f_1 f_2 f_3$, ensuring that the quantities $2^{e_i} + (f/f_i)^2 D_K$ are sums of two squares with $e_1 = 1039, e_2 = 1036, e_3 = 1037$. We recall that the $e_i$ determine the length of the 4-dimensional 2-isogeny chains, and so play a role in the cost of computing them.

The "unofficial" CSIDH-512 parameters provided with the PEARL-SCALLOP implementation on GitHub[21] have $f = f_1$ of 128 bits and $d = 1 \pmod 4$ of 256 bits. Their concrete choices lead to $2^{256} - d$ being a perfect square, in which case a 2-dimensional 2-isogeny chain suffices for validation. Such isogenies have been implemented in the context of SQISign [1] and take mere milliseconds for the NIST-V parameters (which also correspond to a field of characteristic $2^{500}$).

We note that for the CSIDH-$\{1024, 2048, 4096\}$ parameters, the large factors $m$ of $f$ are of size $\{128, 299, 640\}$ bits and so $\deg((2\omega - \mathrm{tr}(\omega))/m) = (4\deg(\omega) - \mathrm{tr}(\omega)^2)/m^2 = (f/m)^2 D_K \approx \{2^{768}, 2^{1450}, 2^{2816}\}$, but the available $2^\bullet$-torsion is $2^e \approx \{2^{512}, 2^{1024}, 2^{2048}\}$. This necessitates *splitting the HD-representation*; a technical endeavour, but with very little overhead, since the two isogeny chains one computes are half as long.

*Remark 4.6.* We remark that in the precise setting of PEARL-SCALLOP, $\omega$ generates an order of conductor $gf$, where $g$ is a small smooth number. To verify (non-)divisibility by these small factors, we evaluate on the respective torsion subgroups, instead of invoking the expensive higher-dimensional test.

**Performance comparison.** To give a rough estimate of the cost of the 4-dimensional isogenies in the second primitivity test for the CSIDH-1024 parameter set, we compare to the qt-PEGASIS implementation of [40, Tab. 1].

Their C implementation takes 146 milliseconds to compute one chain of 4-dimensional 2-isogenies of length roughly 1024 steps over a *prime* field $\mathbb{F}_p$ of

[20] Or, more precisely, about 40 seconds on a server with 255 cores and a clock speed of 2.2 GHz.

[21] https://github.com/biasse/SCALLOP-params

characteristic roughly $2^{1024}$. Since the isogenies of PEARL-SCALLOP are defined over $\mathbb{F}_{p^2}$, and the arithmetic in 4-dimensional isogeny computation is mostly addition and multiplication [38, Table 1], a rough figure of 0.5 ($\approx 3 \cdot 0.15$) seconds can be used to estimate the cost of the corresponding 4-dimensional 2-isogeny chain over $\mathbb{F}_{p^2}$. Repeating for all 3 factors of the conductor $f = f_1 f_2 f_3$, this gives a total overhead of around 1.5 seconds.

This very favourably compares to the PEARL-SCALLOP C++ implementation, which takes 58 seconds to evaluate one action at the CSIDH-1024 parameters, and would require an additional $r = 3$ group action computations.

*Remark 4.7.* We remind that PEARL-SCALLOP is exactly constructed to allow for computing the class group structure, something which appears to be out of reach for the parameters in qt-PEGASIS, which [40] implements. So even though [40] can be used to implement a much faster class group action, we note it has less features.

### 4.3 Summary of the key validation

We now summarize our key validation. Recall that the base prime is of the form $p = c2^e \prod_{i=1}^{n} \ell_i - 1$. Let $f = f_0 \cdot f_1 \cdots f_k$ be the conductor of $\mathcal{O}$, where $f_i$ for $1 \leq i \leq k$ are the large prime factors and $f_0$ the (very) small smooth factor of $f$. Let $q = q_1 \cdots q_r$ be the product of the prime factors of $f_0$. Let $(E, P, Q)$ be a PEARL-SCALLOP public key that we want to validate and act upon with an ideal $\mathfrak{a} = \prod_{i=1}^{N} \mathfrak{l}_i$ of norm $L = \prod_{i=1}^{N} \ell_i = N(\mathfrak{a})$.

For evaluating the group action, we need to compute $\hat{\omega}(E[L])$, while for the primitivity test with respect to the large prime factors $f_i$ for $1 \leq i \leq k$ of the conductor $f$, we need to evaluate $2\hat{\omega} - \mathrm{tr}(\hat{\omega})$ on $E[2^e]$ before running the divisibility test discussed in Section 2.3 and 4.2. When checking the primitivity of the orientation with respect to the small prime factors $q_i$ for $1 \leq i \leq r$ of $f_0$, one can directly evaluate $2\omega - \mathrm{tr}(w)$ on $E[q_i]$ and check that $(2\hat{\omega} - \mathrm{tr}(\hat{\omega}))(E[q_i]) \neq \{0\}$. We hence need the evaluation of $2\hat{\omega} - \mathrm{tr}(\hat{\omega})$ on $E[q2^e]$, which can be derived from that of $\hat{\omega}$ on $E[q2^e]$. To batch all these evaluations, we set $q = 2q_1 \cdots q_r$ and $M = (p+1)q'$ where $q' = q/\gcd(p+1, q)$ and evaluate $\hat{\omega}$ on $E[M]$. This evaluation allows to check whether $\hat{\omega}$ is an endomorphism on $E$ by rejecting if the image points do not lie on $E$. Moreover, it is used to check the trace as described in Section 4.1. One then retrieves the evaluation of $2\hat{\omega} - \mathrm{tr}(\hat{\omega})$ on $E[q_i]$ or $E[2q_i]$ if $q_i = 2$, and (relying on Lemma 4.4) uses it to check whether the orientation is primitive with respect to the small prime factors $q_i$ of $f_0$. One also retrieves the evaluation of $2\hat{\omega} - \mathrm{tr}(\hat{\omega})$ on $E[2^e]$, and uses it to check whether the orientation is primitive with respect to the large prime factors $f_i$ for $1 \leq i \leq k$ of $f$. If all the checks pass, one retrieves $\hat{\omega}(E[L])$ from $\hat{\omega}(E[M])$ and proceeds to the computation of the group action. The full process is summarized in Algorithm 2.

*Remark 4.8.* In Algorithm 2, steps 1-29 constitute the key validation, while steps 30-33 constitute the group action evaluation — these are the only steps where the secret key is used. Consequently, whether key validation succeeds or fails reveals no information about the secret key.

**Algorithm 2** GroupActionWithKeyValidation$(\mathfrak{a}, E, P, Q)$

**Input:** A smooth $\mathcal{O}$-ideal $\mathfrak{a} = \prod_{i=1}^{n} \mathfrak{l}_i$, an $\mathcal{O}$-oriented elliptic curve $E$, points $P, Q \in E$ generating isogenies such that $\hat{\varphi}_Q \circ \varphi_P$ is an endomorphism corresponding to an element of $\mathcal{O}$ of norm $2^{2e}$ and of trace $t$. The large prime factors $f_i$ $(1 \leq i \leq k)$ and the very small smooth factor $f_0$ of the conductor $f = f_0 \cdot f_1 \cdots f_k$ of $\mathcal{O}$. Let $q = 2q_1 \cdots q_r$ be the product of the prime factors of $f_0$.
**Output:** An $\mathcal{O}$-oriented curve $(E_\mathfrak{a}, P_\mathfrak{a}, Q_\mathfrak{a}) = \mathfrak{a} * (E, P, Q)$, or Invalid.

Let $q' = q/\gcd(p+1, q)$ and let $M = (p+1)q'$.
Let $S_1, S_2$ be a basis of $E[M]$.
Compute $\hat{\omega} = \hat{\varphi}_P \circ \varphi_Q$ together with $S_1' = \hat{\omega}(S_1)$, $S_2' = \hat{\omega}(S_2)$.
**if** $\hat{\omega}$ is not an endomorphism of $E$ **then**
    **return** Invalid. ▷ $\omega$ is not an endomorphism
**end if**
Let $R_2 = [t]S_1' - [\deg(\omega)]S_1$.
**if** $e_M(R_2, S_2') \neq e_M(S_1', S_2)^{\deg(\omega)}$ **then**
    **return** Invalid. ▷ Trace is incorrect
**end if**
Let $U_1 = [2]S_1' - [\mathrm{tr}(\omega)]S_1$, $U_2 = [2]S_2' - [\mathrm{tr}(\omega)]S_2$. ▷ Evaluating $2\hat{\omega} - \mathrm{tr}(\hat{\omega})$
Let $Q_1 = [M/q]U_1$, $Q_2 = [M/q]U_2$
**for** $i \in \{1, \ldots r\}$ **do**
    **if** $q_i = 2$ **then**
        **if** $[q/4]Q_1 = 0 = [q/4]Q_2$ **then**
            **return** Invalid. ▷ Non-primitive orientation WRT 2
        **end if**
    **else**
        **if** $[q/q_i]Q_1 = 0 = [q/q_i]Q_2$ **then**
            **return** Invalid. ▷ Non-primitive orientation WRT $q_i$
        **end if**
    **end if**
**end for**
Let $T_1 = [M/2^e]S_1$, $T_1' = [M/2^e]U_1$, $T_2 = [M/2^e]S_2$, $T_2' = [M/2^e]U_2$
**for** $i \in \{1, \ldots k\}$ **do**
    **if** $\{(T_j, [f_i^{-1}]T_j'), j \in \{1, 2\}\}$ represents an isogeny of degree $f^2 D_K / f_i^2$ **then**
        **return** Invalid. ▷ Non-primitive orientation WRT $f_i$
    **end if**
**end for** ▷ End of the key validation
Let $L = \prod_{i=1}^{N} \ell_i = N(\mathfrak{a})$.
Compute $B_1 = [M/L]S_1$, $B_2 = [M/L]S_2$, $B_1' = [M/L]S_1'$, $B_2' = [M/L]S_2'$.
Use $B_1$, $B_1'$, $B_2$ and $B_2'$ to compute $(E_\mathfrak{a}, \varphi_\mathfrak{a}(P), \varphi_\mathfrak{a}(Q)) = \mathfrak{a} * (E, P, Q)$. ▷ Alg.1.
**return** $(E_\mathfrak{a}, \varphi_\mathfrak{a}(P), \varphi_\mathfrak{a}(Q))$.

## References


1. Aardal, M.A., Adj, G., Aranha, D.F., Basso, A., Canales Martínez, I.A., Chávez-Saab, J., Santos, M.C., Dartois, P., De Feo, L., Duparc, M., Eriksen, J.K., Fouotsa, T.B., Filho, D.L.G., Hess, B., Kohel, D., Leroux, A., Longa, P., Maino, L., Meyer, M., Nakagawa, K., Onuki, H., Panny, L., Patranabis, S., Petit, C., Pope, G., Reijnders, K., Robert, D., Rodríguez Henríquez, F., Schaeffler, S., Wesolowski, B.: SQIsign. Tech. rep., National Institute of Standards and Technology (2024), available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-2-additional-signatures
2. Abdalla, M., Eisenhofer, T., Kiltz, E., Kunzweiler, S., Riepel, D.: Password-authenticated key exchange from group actions. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022, Part II. LNCS, vol. 13508, pp. 699–728. Springer, Cham (Aug 2022). https://doi.org/10.1007/978-3-031-15979-4_24
3. Alamati, N., De Feo, L., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 411–439. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_14
4. Allombert, B., Biasse, J.F., Eriksen, J.K., Kutas, P., Leonardi, C., Page, A., Scheidler, R., Bagi, M.T.: Faster SCALLOP from non-prime conductor suborders in medium sized quadratic fields. In: Jager, T., Pan, J. (eds.) PKC 2025, Part III. LNCS, vol. 15676, pp. 333–363. Springer, Cham (May 2025). https://doi.org/10.1007/978-3-031-91826-1_11
5. Atapoor, S., Baghery, K., Cozzo, D., Pedersen, R.: CSI-SharK: CSI-FiSh with sharing-friendly keys. In: Simpson, L., Baee, M.A.R. (eds.) ACISP 23. LNCS, vol. 13915, pp. 471–502. Springer, Cham (Jul 2023). https://doi.org/10.1007/978-3-031-35486-1_21
6. Baghery, K., Cozzo, D., Pedersen, R.: An isogeny-based id protocol using structured public keys. In: Paterson, M.B. (ed.) Cryptography and Coding. pp. 179–197. Springer International Publishing, Cham (2021)
7. Banegas, G., Bernstein, D.J., Campos, F., Chou, T., Lange, T., Meyer, M., Smith, B., Sotáková, J.: CTIDH: faster constant-time CSIDH. IACR TCHES **2021**(4), 351–387 (2021). https://doi.org/10.46586/tches.v2021.i4.351-387, https://tches.iacr.org/index.php/TCHES/article/view/9069
8. Banegas, G., Krämer, J., Lange, T., Meyer, M., Panny, L., Reijnders, K., Sotáková, J., Trimoska, M.: Disorientation faults in CSIDH. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 310–342. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_11
9. Basso, A., Kutas, P., Merz, S.P., Petit, C., Weitkämper, C.: On adaptive attacks against jao-urbanik's isogeny-based protocol. In: Nitaj, A., Youssef, A.M. (eds.) AFRICACRYPT 20. LNCS, vol. 12174, pp. 195–213. Springer, Cham (Jul 2020). https://doi.org/10.1007/978-3-030-51938-4_10
10. Bernstein, D.J., Lange, T., Martindale, C., Panny, L.: Quantum circuits for the CSIDH: Optimizing quantum evaluation of isogenies. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part II. LNCS, vol. 11477, pp. 409–441. Springer, Cham (May 2019). https://doi.org/10.1007/978-3-030-17656-3_15
11. Beullens, W., Dobson, S., Katsumata, S., Lai, Y.F., Pintore, F.: Group signatures and more from isogenies and lattices: Generic, simple, and efficient. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part II. LNCS, vol. 13276, pp. 95–126. Springer, Cham (May / Jun 2022). https://doi.org/10.1007/978-3-031-07085-3_4

12. Beullens, W., Katsumata, S., Pintore, F.: Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 464–492. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_16
13. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 227–247. Springer, Cham (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_9
14. Bisson, G., Sutherland, A.V.: Computing the endomorphism ring of an ordinary elliptic curve over a finite field. Cryptology ePrint Archive, Report 2009/100 (2009), https://eprint.iacr.org/2009/100
15. Boneh, D., Kogan, D., Woo, K.: Oblivious pseudorandom functions from isogenies. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 520–550. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_18
16. Bonnetain, X., Schrottenloher, A.: Quantum security analysis of CSIDH. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 493–522. Springer, Cham (May 2020). https://doi.org/10.1007/978-3-030-45724-2_17
17. Campos, F., Chávez-Saab, J., Chi-Domínguez, J.J., Meyer, M., Reijnders, K., Rodríguez-Henríquez, F., Schwabe, P., Wiggers, T.: Optimizations and practicality of high-security CSIDH. CiC **1**(1), 5 (2024). https://doi.org/10.62056/anjbksdja
18. Campos, F., Hellenbrand, A., Meyer, M., Reijnders, K.: dCTIDH: Fast & deterministic CTIDH. Cryptology ePrint Archive, Report 2025/107 (2025), https://eprint.iacr.org/2025/107
19. Campos, F., Kannwischer, M.J., Meyer, M., Onuki, H., Stöttinger, M.: Trouble at the CSIDH: Protecting CSIDH with dummy-operations against fault injection attacks. Cryptology ePrint Archive, Report 2020/1005 (2020), https://eprint.iacr.org/2020/1005
20. Campos, F., Meyer, M., Reijnders, K., Stöttinger, M.: Patient zero & patient six: Zero-value and correlation attacks on CSIDH and SIKE. In: Smith, B., Wu, H. (eds.) SAC 2022. LNCS, vol. 13742, pp. 234–262. Springer, Cham (Aug 2024). https://doi.org/10.1007/978-3-031-58411-4_11
21. Castryck, W., Decru, T.: CSIDH on the surface. In: Ding, J., Tillich, J.P. (eds.) Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020. pp. 111–129. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-44223-1_7
22. Castryck, W., Houben, M., Merz, S.P., Mula, M., van Buuren, S., Vercauteren, F.: Weak instances of class group action based cryptography via self-pairings. In: Handschuh, H., Lysyanskaya, A. (eds.) CRYPTO 2023, Part III. LNCS, vol. 14083, pp. 762–792. Springer, Cham (Aug 2023). https://doi.org/10.1007/978-3-031-38548-3_25
23. Castryck, W., Houben, M., Vercauteren, F., Wesolowski, B.: On the decisional Diffie–Hellman problem for class group actions on oriented elliptic curves. Research in Number Theory **8**(4), 99 (2022). https://doi.org/https://doi.org/10.1007/s40993-022-00399-6
24. Castryck, W., Invernizzi, R., Lorenzon, G., Meers, J., Vercauteren, F.: Orient express: Using frobenius to express oriented isogenies. Cryptology ePrint Archive, Paper 2025/1047 (2025), https://eprint.iacr.org/2025/1047

25. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Cham (Dec 2018). https://doi.org/10.1007/978-3-030-03332-3_15
26. Castryck, W., Sotáková, J., Vercauteren, F.: Breaking the decisional Diffie-Hellman problem for class group actions using genus theory: Extended version. Journal of Cryptology **35**(4), 24 (Oct 2022). https://doi.org/10.1007/s00145-022-09435-1
27. Cervantes-Vázquez, D., Chenu, M., Chi-Domínguez, J.J., De Feo, L., Rodríguez-Henríquez, F., Smith, B.: Stronger and faster side-channel protections for CSIDH. In: Schwabe, P., Thériault, N. (eds.) LATINCRYPT 2019. LNCS, vol. 11774, pp. 173–193. Springer, Cham (Oct 2019). https://doi.org/10.1007/978-3-030-30530-7_9
28. Chávez-Saab, J., Chi-Domínguez, J.J., Jaques, S., Rodríguez-Henríquez, F.: The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. Journal of Cryptographic Engineering **12**(3), 349–368 (Sep 2022). https://doi.org/10.1007/s13389-021-00271-w
29. Chen, M., Lai, Y.F., Laval, A., Marco, L., Petit, C.: Malleable commitments from group actions and zero-knowledge proofs for circuits based on isogenies. In: Chattopadhyay, A., Bhasin, S., Picek, S., Rebeiro, C. (eds.) INDOCRYPT 2023, Part I. LNCS, vol. 14459, pp. 221–243. Springer, Cham (Dec 2023). https://doi.org/10.1007/978-3-031-56232-7_11
30. Chen, M., Leroux, A., Panny, L.: SCALLOP-HD: Group action from 2-dimensional isogenies. In: Tang, Q., Teague, V. (eds.) PKC 2024, Part II. LNCS, vol. 14603, pp. 190–216. Springer, Cham (Apr 2024). https://doi.org/10.1007/978-3-031-57725-3_7
31. Chenu, M., Smith, B.: Higher-degree supersingular group actions. Cryptology ePrint Archive, Report 2021/955 (2021), https://eprint.iacr.org/2021/955
32. Chi-Domínguez, J.J., Reijnders, K.: Fully projective radical isogenies in constant-time. In: Galbraith, S.D. (ed.) CT-RSA 2022. LNCS, vol. 13161, pp. 73–95. Springer, Cham (Mar 2022). https://doi.org/10.1007/978-3-030-95312-6_4
33. Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. Journal of Mathematical Cryptology, vol. 14, pp. 414–437 (2020). https://doi.org/10.1515/jmc-2019-0034
34. Conrad, K.: The conductor ideal of an order, https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf
35. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291 (2006), https://eprint.iacr.org/2006/291
36. Cox, D.A.: Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, Pure and Applied Mathematics, vol. 116. Wiley, 2nd edn. (2013)
37. Cozzo, D., Smart, N.P.: Sashimi: Cutting up CSI-FiSh secret keys to produce an actively secure distributed signing protocol. In: Ding, J., Tillich, J.P. (eds.) Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020. pp. 169–186. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-44223-1_10
38. Dartois, P.: Fast computation of 2-isogenies in dimension 4 and cryptographic applications. Cryptology ePrint Archive, Report 2024/1180 (2024), https://eprint.iacr.org/2024/1180
39. Dartois, P., De Feo, L.: On the security of OSIDH. In: Hanaoka, G., Shikata, J., Watanabe, Y. (eds.) PKC 2022, Part I. LNCS, vol. 13177, pp. 52–81. Springer, Cham (Mar 2022). https://doi.org/10.1007/978-3-030-97121-2_3

40. Dartois, P., Duparc, M.: Chasing rabbits through hypercubes: better algorithms for higher dimensional 2-isogeny computations. Cryptology ePrint Archive, Paper 2026/114 (2026), https://eprint.iacr.org/2026/114
41. Dartois, P., Eriksen, J.K., Fouotsa, T.B., Merdy, A.H.L., Invernizzi, R., Robert, D., Rueger, R., Vercauteren, F., Wesolowski, B.: PEGASIS: Practical effective class group action using 4-dimensional isogenies. In: CRYPTO 2025, Part I. pp. 67–99. LNCS, Springer, Cham (Aug 2025). https://doi.org/10.1007/978-3-032-01855-7_3
42. Dartois, P., Leroux, A., Robert, D., Wesolowski, B.: SQISignHD: New dimensions in cryptography. Cryptology ePrint Archive, Report 2023/436 (2023), https://eprint.iacr.org/2023/436
43. De Feo, L., Fouotsa, T.B., Kutas, P., Leroux, A., Merz, S.P., Panny, L., Wesolowski, B.: SCALLOP: Scaling the CSI-FiSh. In: Boldyreva, A., Kolesnikov, V. (eds.) PKC 2023, Part I. LNCS, vol. 13940, pp. 345–375. Springer, Cham (May 2023). https://doi.org/10.1007/978-3-031-31368-4_13
44. De Feo, L., Leroux, A., Longa, P., Wesolowski, B.: New algorithms for the Deuring correspondence - towards practical and secure SQISign signatures. In: Hazay, C., Stam, M. (eds.) EUROCRYPT 2023, Part V. LNCS, vol. 14008, pp. 659–690. Springer, Cham (Apr 2023). https://doi.org/10.1007/978-3-031-30589-4_23
45. De Feo, L., Meyer, M.: Threshold schemes from isogeny assumptions. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 187–212. Springer, Cham (May 2020). https://doi.org/10.1007/978-3-030-45388-6_7
46. Delpech de Saint Guilhem, C., Pedersen, R.: New proof systems and an OPRF from CSIDH. In: Tang, Q., Teague, V. (eds.) PKC 2024, Part II. LNCS, vol. 14603, pp. 217–251. Springer, Cham (Apr 2024). https://doi.org/10.1007/978-3-031-57725-3_8
47. Dobson, S., Galbraith, S.D., LeGrow, J., Ti, Y.B., Zobernig, L.: An adaptive attack on 2-sidh. International Journal of Computer Mathematics: Computer Systems Theory **6**(4), 387–404 (2021). https://doi.org/10.1080/23799927.2021.2018115
48. Dobson, S., Li, T., Zobernig, L.: A note on a static SIDH protocol. Cryptology ePrint Archive, Report 2019/1244 (2019), https://eprint.iacr.org/2019/1244
49. Eriksen, J.K., Leroux, A.: Computing orientations from the endomorphism ring of supersingular curves and applications. CiC **1**(3), 5 (2024). https://doi.org/10.62056/ae0fhbmo
50. Fouotsa, T.B., Petit, C.: SHealS and HealS: Isogeny-based PKEs from a key validation method for SIDH. In: Tibouchi, M., Wang, H. (eds.) ASIACRYPT 2021, Part IV. LNCS, vol. 13093, pp. 279–307. Springer, Cham (Dec 2021). https://doi.org/10.1007/978-3-030-92068-5_10
51. Fouotsa, T.B., Petit, C.: A new adaptive attack on SIDH. In: Galbraith, S.D. (ed.) CT-RSA 2022. LNCS, vol. 13161, pp. 322–344. Springer, Cham (Mar 2022). https://doi.org/10.1007/978-3-030-95312-6_14
52. Gajland, P., de Kock, B., Quaresma, M., Malavolta, G., Schwabe, P.: SWOOSH: Efficient lattice-based non-interactive key exchange. In: Balzarotti, D., Xu, W. (eds.) USENIX Security 2024. USENIX Association (Aug 2024), https://www.usenix.org/conference/usenixsecurity24/presentation/gajland
53. Galbraith, S., Gilchrist, V., Robert, D.: Improved algorithms for ascending isogeny volcanoes, and applications. Cryptology ePrint Archive, Paper 2025/1243 (2025), https://eprint.iacr.org/2025/1243

54. Galbraith, S., Panny, L., Smith, B., Vercauteren, F.: Quantum equivalence of the DLP and CDHP for group actions. Cryptology ePrint Archive, Report 2018/1199 (2018), https://eprint.iacr.org/2018/1199
55. Galbraith, S.D., Hess, F., Smart, N.P.: Extending the GHS Weil descent attack. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 29–44. Springer, Berlin, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_3
56. Galbraith, S.D., Lai, Y.F.: Attack on SHealS and HealS: The second wave of GPST. In: Cheon, J.H., Johansson, T. (eds.) Post-Quantum Cryptography - 13th International Workshop, PQCrypto 2022. pp. 399–421. Springer, Cham (Sep 2022). https://doi.org/10.1007/978-3-031-17234-2_19
57. Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of supersingular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds.) ASIACRYPT 2016, Part I. LNCS, vol. 10031, pp. 63–91. Springer, Berlin, Heidelberg (Dec 2016). https://doi.org/10.1007/978-3-662-53887-6_3
58. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: 28th ACM STOC. pp. 212–219. ACM Press (May 1996). https://doi.org/10.1145/237814.237866
59. Hanzlik, L., Lai, Y.F., Mula, M., Paracucchi, E., Slamanig, D., Tang, G.: Tanuki: New frameworks for (concurrently secure) blind signatures from post-quantum groups actions. Cryptology ePrint Archive, Paper 2025/1100 (2025), https://eprint.iacr.org/2025/1100
60. Heimberger, L., Hennerbichler, T., Meisingseth, F., Ramacher, S., Rechberger, C.: OPRFs from isogenies: Designs and analysis. In: Zhou, J., Quek, T.Q.S., Gao, D., Cárdenas, A.A. (eds.) ASIACCS 24. ACM Press (Jul 2024). https://doi.org/10.1145/3634737.3645010
61. Houben, M.: Deterministic algorithms for class group actions. In: CRYPTO 2025, Part I. pp. 100–130. LNCS, Springer, Cham (Aug 2025). https://doi.org/10.1007/978-3-032-01855-7_4
62. Houben, M.: Efficient post-quantum commutative group actions from orientations of large discriminant. Cryptology ePrint Archive, Paper 2025/1098 (2025), https://eprint.iacr.org/2025/1098
63. Katsumata, S., Lai, Y.F., LeGrow, J.T., Qin, L.: CSI-Otter: Isogeny-based (partially) blind signatures from the class group action with a twist. In: Handschuh, H., Lysyanskaya, A. (eds.) CRYPTO 2023, Part III. LNCS, vol. 14083, pp. 729–761. Springer, Cham (Aug 2023). https://doi.org/10.1007/978-3-031-38548-3_24
64. Kopp, G.S., Lagarias, J.C.: Class field theory for orders of number fields (2022), https://arxiv.org/abs/2212.09177
65. Kunzweiler, S., Ti, Y.B., Weitkämper, C.: Secret keys in genus-2 SIDH. In: AlTawy, R., Hülsing, A. (eds.) SAC 2021. LNCS, vol. 13203, pp. 483–507. Springer, Cham (Sep / Oct 2022). https://doi.org/10.1007/978-3-030-99277-4_23
66. Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM Journal on Computing **35**(1), 170–188 (2005)
67. Kuperberg, G.: Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In: 8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013). Leibniz International Proceedings in Informatics (LIPIcs), vol. 22, pp. 20–34. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik (2013). https://doi.org/10.4230/LIPIcs.TQC.2013.20, http://drops.dagstuhl.de/opus/volltexte/2013/4321

68. Lai, Y.F., Galbraith, S.D., Delpech de Saint Guilhem, C.: Compact, efficient and UC-secure isogeny-based oblivious transfer. In: Canteaut, A., Standaert, F.X. (eds.) EUROCRYPT 2021, Part I. LNCS, vol. 12696, pp. 213–241. Springer, Cham (Oct 2021). https://doi.org/10.1007/978-3-030-77870-5_8
69. LeGrow, J., Hutchinson, A.: An analysis of fault attacks on CSIDH. Cryptology ePrint Archive, Report 2020/1006 (2020), https://eprint.iacr.org/2020/1006
70. LeGrow, J.T.: A faster method for fault attack resistance in static/ephemeral CSIDH. Journal of Cryptographic Engineering **13**(3), 283–294 (Sep 2023). https://doi.org/10.1007/s13389-023-00318-0
71. LeGrow, J.T., Hutchinson, A.: (Short paper) analysis of a strong fault attack on static/ephemeral CSIDH. In: Nakanishi, T., Nojima, R. (eds.) IWSEC 21. LNCS, vol. 12835, pp. 216–226. Springer, Cham (Sep 2021). https://doi.org/10.1007/978-3-030-85987-9_12
72. Leroux, A., Roméas, M.: Updatable encryption from group actions. In: Saarinen, M.J., Smith-Tone, D. (eds.) Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part II. pp. 20–53. Springer, Cham (Jun 2024). https://doi.org/10.1007/978-3-031-62746-0_2
73. Levin, S., Pedersen, R.: Faster proofs and VRFs from isogenies. Cryptology ePrint Archive, Report 2024/1626 (2024), https://eprint.iacr.org/2024/1626
74. Lim, D., Ti, Y.B.: Adaptive attack on static POKÉ keys. Cryptology ePrint Archive, Paper 2025/1541 (2025), https://eprint.iacr.org/2025/1541
75. Meers, J., Riepel, D.: CCA secure updatable encryption from non-mappable group actions. In: Saarinen, M.J., Smith-Tone, D. (eds.) Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I. pp. 137–169. Springer, Cham (Jun 2024). https://doi.org/10.1007/978-3-031-62743-9_5
76. Meyer, M., Campos, F., Reith, S.: On lions and elligators: An efficient constant-time implementation of CSIDH. In: Ding, J., Steinwandt, R. (eds.) Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019. pp. 307–325. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-25510-7_17
77. Meyer, M., Reith, S.: A faster way to the CSIDH. In: Chakraborty, D., Iwata, T. (eds.) INDOCRYPT 2018. LNCS, vol. 11356, pp. 137–152. Springer, Cham (Dec 2018). https://doi.org/10.1007/978-3-030-05378-9_8
78. Montgomery, H., Sharif, S.: Quantum money from class group actions on elliptic curves. In: Chung, K.M., Sasaki, Y. (eds.) ASIACRYPT 2024, Part IX. LNCS, vol. 15492, pp. 33–64. Springer, Singapore (Dec 2024). https://doi.org/10.1007/978-981-96-0947-5_2
79. Moriya, T., Onuki, H.: The wrong use of FESTA trapdoor functions leads to an adaptive attack. Cryptology ePrint Archive, Report 2023/1092 (2023), https://eprint.iacr.org/2023/1092
80. Moriya, T., Onuki, H., Takagi, T.: SiGamal: A supersingular isogeny-based PKE and its application to a PRF. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 551–580. Springer, Cham (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_19
81. Moriya, T., Onuki, H., Xu, M., Zhou, G.: Adaptive attacks against FESTA without input validation or constant-time implementation. In: Saarinen, M.J., Smith-Tone, D. (eds.) Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part II. pp. 3–19. Springer, Cham (Jun 2024). https://doi.org/10.1007/978-3-031-62746-0_1
82. Morrison, T., Panny, L., Sotáková, J., Wills, M.: The sea algorithm for endomorphisms of supersingular elliptic curves (2025), https://arxiv.org/abs/2501.16321

83. Onuki, H.: On oriented supersingular elliptic curves. Finite Fields and Their Applications (2021), https://doi.org/10.1016/j.ffa.2020.101777
84. Page, A., Robert, D.: Introducing clapoti(s): Evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, Report 2023/1766 (2023), https://eprint.iacr.org/2023/1766
85. Panny, L., Petit, C., Stopar, M.: KLaPoTi: An asymptotically efficient isogeny group action from 2-dimensional isogenies. Cryptology ePrint Archive, Report 2024/1844 (2024), https://eprint.iacr.org/2024/1844
86. Peikert, C.: He gives C-sieves on the CSIDH. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 463–492. Springer, Cham (May 2020). https://doi.org/10.1007/978-3-030-45724-2_16
87. Regev, O.: A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space (2004), https://arxiv.org/pdf/quant-ph/0406151
88. Robert, D.: The module action for isogeny based cryptography. Cryptology ePrint Archive, Report 2024/1556 (2024), https://eprint.iacr.org/2024/1556
89. Robert, D.: On the efficient representation of isogenies (a survey). Cryptology ePrint Archive, Report 2024/1071 (2024), https://eprint.iacr.org/2024/1071
90. Rostovtsev, A., Stolbunov, A.: Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145 (2006), https://eprint.iacr.org/2006/145
91. Siegel, C.: Über die classenzahl quadratischer zahlkörper. Acta Arithmetica **1**(1), 83–86 (1935), http://eudml.org/doc/205054
92. Sutherland, A.: Isogeny volcanoes. The Open Book Series **1**(1), 507–530 (Nov 2013). https://doi.org/10.2140/obs.2013.1.507
93. Sutherland, A.: Lecture notes for MIT course 18.783: Elliptic Curves (2023), https://math.mit.edu/classes/18.783/2023/LectureNotes17.pdf
94. Wesolowski, B.: Orientations and the supersingular endomorphism ring problem. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022, Part III. LNCS, vol. 13277, pp. 345–371. Springer, Cham (May / Jun 2022). https://doi.org/10.1007/978-3-031-07082-2_13
95. Zhou, G., Xu, M.: An efficient adaptive attack against FESTA. Cryptology ePrint Archive, Report 2024/345 (2024), https://eprint.iacr.org/2024/345