# Orient Express: Using Frobenius to Express Oriented Isogenies

Wouter Castryck[1], Riccardo Invernizzi[1], Gioella Lorenzon[1], Jonas Meers[2], Frederik Vercauteren[1]

[1] COSIC, KU Leuven, Belgium
[2] CASA, Ruhr-Universität Bochum, Germany

**Abstract.** In this paper we study supersingular elliptic curves primitively oriented by an imaginary quadratic order, where the orientation is given by an endomorphism that factors through the Frobenius isogeny. In this way, we partly recycle one of the main features of CSIDH, namely the fact that the Frobenius orientation can be represented for free. This leads to the most efficient family of ideal-class group actions in a range where the discriminant is significantly larger than the field characteristic $p$. Moreover, if we orient with a non-maximal order $\mathcal{O} \subset \mathbb{Q}(\sqrt{-p})$ and we assume that it is feasible to compute the ideal-class group of the maximal order, then also the ideal-class group of $\mathcal{O}$ is known and we recover the central feature of SCALLOP-like constructions.
We propose two variants of our scheme. In the first one, the orientation is by a suborder of the form $\mathbb{Z}[f\sqrt{-p}]$ for some $f$ coprime to $p$, so this is similar to SCALLOP. In the second one, inspired by the work of Chenu and Smith, the orientation is by an order of the form $\mathbb{Z}[\sqrt{-dp}]$ where $d$ is square-free and not a multiple of $p$. We give practical ways of generating parameters, together with a proof-of-concept SageMath implementation of both variants, which shows the effectiveness of our construction.

**Keywords:** Isogeny-based cryptography, class group action, Frobenius endomorphism.

## 1 Introduction

In recent years, there has been a surging interest in the cryptographic use of finite abelian group actions. This concept extends exponentiation in finite cyclic groups, while maintaining the flexibility needed for generalizing several discrete logarithm-based cryptographic constructions, with the Diffie–Hellman key exchange protocol as the main example. The primary motivation for this generalization is that there exist group actions which, unlike exponentiation, are believed to be hard to invert by quantum adversaries.

Unfortunately, we know of one family of post-quantum finite abelian group actions only: ideal-class groups of imaginary quadratic orders acting on sets of elliptic curves over finite fields via isogenies,[1] a construction originating from the

[1] The cryptographic use of ideal-class group actions on abelian varieties of higher dimension has seen preliminary exploration only [34].

theory of complex multiplication. Their cryptographic potential was first recognized by Couveignes [15] and, independently, by Rostovtsev and Stolbunov [33]. While the original proposal was to work with ordinary elliptic curves, the research focus has shifted entirely to supersingular elliptic curves. This is mainly for reasons of efficiency, but there is also greater flexibility: through the theory of orientations [14,28], supersingular elliptic curves admit actions by ideal-class groups of (infinitely) many different imaginary quadratic orders.

The most practical instantiation is CSIDH [10], coming from the so-called Frobenius orientation. Here one acts with the ideal-class group of a quadratic order containing $\mathbb{Z}[\sqrt{-p}]$ on the set of supersingular elliptic curves $E/\mathbb{F}_p$ up to $\mathbb{F}_p$-isomorphism, where $p$ denotes a large prime number; the required order of magnitude to achieve security is debated (see Section 6 for a discussion). Under this orientation the ring element $\sqrt{-p}$ corresponds to the $p$-th power Frobenius endomorphism $\pi_p : E \to E : (x, y) \mapsto (x^p, y^p)$. There are three main reasons why the (supersingular) Frobenius orientation stands out in terms of efficiency:

1. all curves and isogenies that one encounters during the group action evaluation are defined over $\mathbb{F}_p$;
2. it is easy to choose parameters such that there exist many prescribed ideals that are very easy to act with (e.g., having a small norm and ideal kernels consisting of $\mathbb{F}_p$-rational points),
3. representing the orientation comes at no cost, i.e., when given an elliptic curve $E/\mathbb{F}_p$, it is immediate how to evaluate the endomorphism $\pi_p$ corresponding to $\sqrt{-p}$ on it.

Reason 2 distinguishes the supersingular case from the ordinary case and was the main selling point of CSIDH. The focus of this article is on reason 3: this is a very powerful feature which was not recognized until other orientations started entering the picture, where the lack of this property is often an important bottleneck.

For the sake of flexibility in current and future applications of cryptographic group actions, it is desirable to cultivate a pool of practical orientations that is as diverse as possible. Indeed, there are good reasons for studying orientations by imaginary quadratic orders $\mathcal{O} \not\supseteq \mathbb{Z}[\sqrt{-p}]$. For example, certain applications like CSI-FiSh [6] require knowledge of the order (or even the structure) of the ideal-class group $\mathrm{cl}(\mathcal{O})$. In general, this is very hard to compute: our fastest known (classical) methods run in sub-exponential time [21]. Here, the leading family of proposals is SCALLOP [19,12,2], where $\mathcal{O}$ is chosen to be an order with large conductor in an imaginary quadratic field having a small(ish) class number. However, unlike the Frobenius case, representing such orientations is non-trivial. This situation was greatly improved through the use of higher-dimensional isogeny representations [12], but the cost remains really substantial.

### Orientations factoring through Frobenius

Inspired by the "higher-degree" supersingular group actions introduced by Chenu and Smith [13], in this paper we study orientations by orders $\mathcal{O}$ containing

$\mathbb{Z}[\sqrt{-dp}]$ with $p \nmid d$. On an $\mathcal{O}$-oriented supersingular elliptic curve $E/\mathbb{F}_{p^2}$, the endomorphism corresponding to $\sqrt{-dp}$ necessarily factors through the Frobenius isogeny:

$$E \xrightarrow{\tau} E^{(p)} \xrightarrow{\pi_p} E, \qquad \deg(\tau) = d.$$

Our motivation for studying this kind of orientations is easy to state: in order to represent the endomorphism $\pi_p \circ \tau$, it suffices to represent the isogeny $\tau$ since the Frobenius part comes for free. As such, we recover a part of the selling point highlighted in feature 3. The isogeny $\tau$ can then be represented in terms of interpolation data, i.e., by the images of a basis of $E[N]$ for some smooth integer $N \approx \sqrt{d}$ (which in practice is of the form $2^a$). Without the Frobenius boost, this lower bound would grow to $\sqrt{dp}$, negatively affecting

- the speed: longer higher-dimensional isogeny chains would need to be computed;
- the design flexibility: the $N$-torsion is expected to be defined over $\mathbb{F}_{p^2}$, putting severe constraints on $p$.

A nice by-product of orientations factoring through Frobenius is that the ideal class group actions are transitive, since by construction $p$ ramifies in $\mathcal{O}$. Recall from [28] that, in the inert case, the class group action has two orbits.

**Comparison with other frameworks**

The smaller bound on $N$ allows to work in a regime where the discriminant $|\Delta_{\mathcal{O}}|$ of the orienting order $\mathcal{O}$ is significantly larger than $p$. As far as we are aware, the only other practical instantiations of an orientation breaking through the $p$-barrier are

- the first version of SCALLOP, but our construction is simpler and orders of magnitude faster,
- a very recent and as-of-yet unpublished construction due to Houben, presented at SQIparty 2025 [22], also based on factoring endomorphisms into isogenies, but his construction does not account for factorizations through Frobenius, and thus does not benefit from the associated performance gains (that said, the construction is compatible with Frobenius factors, and when these are incorporated, the framework described below essentially becomes a special case of Houben's approach).

We believe that the large-discriminant range deserves further study, because for a given class group size (i.e., a given security level) it allows to work over smaller finite fields. In turn, this may lead to increased efficiency, or to greater flexibility in applications where the field size is constrained. Moreover, as soon as $|\Delta_{\mathcal{O}}| \approx p^2$, it seems reasonable to expect that, when forgetting about the orientation, the class group action samples close-to-uniformly from the entire set of supersingular elliptic curves over $\mathbb{F}_{p^2}$, which may be seen as a security feature (although this requires further study and justification).

When compared to CSIDH, orientations factoring through Frobenius do not offer any efficiency gains (yet?), but the following asymptotic trade-off is a glimmer on the horizon. Let us say that we are targeting a class group size having $2\mu$ bits, then we want $\log_2 d + \log_2 p \approx \mu$. If (as usual) one works with curve models satisfying

$$E(\mathbb{F}_{p^2}) \cong \frac{\mathbb{Z}}{(p+1)\mathbb{Z}} \times \frac{\mathbb{Z}}{(p+1)\mathbb{Z}}$$

and $\mathbb{F}_{p^2}$-rational interpolation data, then we must have $N \mid p+1$. If we allow $N$ to take up almost all of $p+1$, then this means that we can let $d$ grow up to about $p^2$, meaning that $\log_2 p \approx \frac{1}{3}\mu$. In other words, the bit size of our base field $\mathbb{F}_{p^2}$ is about $2\log_2 p \approx \frac{2}{3}\mu$, whereas in CSIDH the bit size of the base field $\mathbb{F}_p$ is invariably $\log_2 p \approx \mu$.

*Remark 1.* As mentioned, unfortunately, the cheaper field arithmetic does not result in an overall speed-up because it is negatively compensated by a larger number of field operations (mainly due to the computation of two-dimensional isogeny chains). Moreover, we stress that this is an aymptotic trade-off, which kicks in beyond the concrete class group sizes that are currently being proposed. The reason is that $p+1$ must leave room for a constant number of small prime divisors, needed for an efficient evaluation of the class group action.

When compared to the second-generation versions of SCALLOP [12,2], orientations factoring through Frobenius are quite a bit more efficient, thanks to the shorter isogeny chains and the smaller base field. Moreover, by letting $d = f^2$ be a square, we orient by a non-maximal order of $\mathbb{Q}(\sqrt{-p})$ and, if the class group structure of the maximal order is known, then also the class group structure of this suborder is known. Thus, in ranges where computing the class group of the maximal order of $\mathbb{Q}(\sqrt{-p})$ is feasible, we recover the main selling point of SCALLOP. Unfortunately, because of the constraint $N \mid p+1$, we cannot merely recycle the record class group computation from [6], but at least it shows that $\log_2 p \approx 512$ is well within reach. As explained above, this allows to take $d = f^2$ up to bit size 1024, apart from the space allocated for the small primes needed for evaluating the class group action. So this roughly covers the concrete parameter sizes that were proposed in [2]. Asymptotically, this selling point evaporates because computing the class group of the maximal order of $\mathbb{Q}(\sqrt{-p})$ becomes too costly. This being said, in most applications where $\mathrm{cl}(O)$ must be known, one also wants to work with genuinely effective group actions (EGAs, see Section 2.1), which neither the SCALLOP family nor our orientations can offer: indeed, with the current methods, acting with arbitrary class group elements comes at the cost of approximate closest-vector-problem computations in lattices of growing dimension [30].

This brings us to our final comparison: we work in the restricted effective group action (REGA) model. Using an exponential-time precomputation (i.e., lattice reduction), this can be turned into an EGA, but at any rate this is a point where it cannot compete with the Clapoti-family of proposals [29,31], which recently culminated in the efficient EGA framework PEGASIS [17]. But these constructions strongly rely on $|\Delta_{\mathcal{O}}| \lessapprox p$.

## 2 Background

### 2.1 Group-Action Based Cryptography

We recall the definition of a (restricted) effective group action from [1].

**Definition 1 (Abelian Group Action).** *Let $(\mathcal{G}, \cdot)$ be an abelian group with identity $1 \in \mathcal{G}$ and $\mathcal{X}$ a set. A map $\star : \mathcal{G} \times \mathcal{X} \to \mathcal{X}$ is called a* group action *if it satisfies the following properties:*

- *Identity: $1 \star x = x$ for all $x \in \mathcal{X}$.*
- *Compatibility: $(g \cdot h) \star x = g \star (h \star x)$ for all $g, h \in \mathcal{G}$ and $x \in \mathcal{X}$.*

**Definition 2 (Effective Group Action (EGA)).** *An abelian group action $(\mathcal{G}, \mathcal{X}, \star)$ is called* effective *if the following properties are satisfied:*

- *$\mathcal{G}$ is finite and there exists efficient (PPT) algorithms for membership testing, equality testing, (random) sampling, group operation and inversion.*
- *$\mathcal{X}$ is finite and there exist efficient algorithms for membership testing and for computing a unique representation.*
- *There exists a distinguished element $\widetilde{x} \in \mathcal{X}$ with known representation.*
- *There exists an efficient algorithm to evaluate the group action, i.e. to compute $g \star x$ given $g$ and $x$.*

In practice, the requirements of an effective group action are too strong. In particular, most isogeny-based instantiations of group actions lack the property of efficiently evaluating the group action for every $g \in \mathcal{G}$. Notable exceptions are Clapoti [29], its successor KLaPoTi [31] and PEGASIS [17]. All other (isogeny-based) group actions only satisfy the following weaker notion where the group action can only be efficiently evaluated for a generating set of small cardinality.

**Definition 3 (Restricted Effective Group Action (REGA)).** *Let $(\mathcal{G}, \mathcal{X}, \star)$ be an abelian group action and let $\mathbf{g} = \{g_1, \ldots, g_n\}$ be a generating set for $\mathcal{G}$. The action is said to be* $\mathbf{g}$-restricted *effective if the following properties are satisfied:*

- *$\mathcal{G}$ is finite and $n = \text{poly}\log|\mathcal{G}|$.*
- *$\mathcal{X}$ is finite and there exist efficient algorithms for membership testing and for computing a unique representation.*
- *There exists a distinguished element $\widetilde{x} \in \mathcal{X}$ with known representation.*
- *There exists an efficient algorithm to evaluate the group action $g_i \star x$ and $g_i^{-1} \star x$ for $i \in [n]$ and all $x \in \mathcal{X}$.*

We remark, however, that a REGA can often be turned into an EGA through some expensive precomputations. For more details, we refer to [19,12].

### 2.2 Oriented Elliptic Curves and their Class Group Actions

Up to our knowledge, all current candidate post-quantum abelian group actions involve isogenies between elliptic curves. This comes from the theory of complex multiplication. We give a quick theoretical overview; the statements below can be found in [14,28,35,36]. Let $K$ be an imaginary quadratic number field and let $E$ be an elliptic curve over an algebraically closed field $k$ of characteristic $p \geq 0$. A $K$-orientation on $E$ is an embedding

$$\iota : K \hookrightarrow \mathrm{End}^0(E)$$

of $K$ into the endomorphism algebra of $E$ (such an embedding may not exist). The couple $(E, \iota)$ is called a $K$-oriented elliptic curve. For an order $\mathcal{O} \subseteq K$, we say that $\iota$ is a primitive $\mathcal{O}$-orientation if $\mathcal{O} = \iota^{-1}\,\mathrm{End}(E)$.

If $\varphi : E \to E'$ is an isogeny, then there is a corresponding push-forward $K$-orientation on $E'$ given by

$$\iota' : K \hookrightarrow \mathrm{End}^0(E') : u \mapsto \frac{\varphi\iota(u)\hat{\varphi}}{\deg \varphi},$$

and we say that $\varphi : (E, \iota) \to (E', \iota')$ is an isogeny of $K$-oriented elliptic curves. If $\deg \varphi = 1$ then this is called an isomorphism, and we write $(E, \iota) \cong (E', \iota')$. If both $\iota$ and $\iota'$ are primitive $\mathcal{O}$-orientations then the isogeny $\varphi$ is called horizontal.

For any imaginary quadratic order $\mathcal{O}$, its ideal-class group $\mathrm{cl}(\mathcal{O})$ acts freely on

$$\mathcal{Ell}_k(\mathcal{O}) = \{\, \text{elliptic curves } E/k \text{ along with a primitive } O\text{-orientation } \iota \,\} \,/\, \cong \quad (1)$$

via horizontal isogenies, as soon as this set is non-empty. More concretely, for any ideal class $[\mathfrak{a}] \in \mathrm{cl}(\mathcal{O})$, represented by an invertible ideal $\mathfrak{a}$ whose norm is not divisible by $p$ (which can be assumed w.l.o.g.), and every $(E, \iota) \in \mathcal{Ell}_k(\mathcal{O})$, one defines $[\mathfrak{a}](E, \iota)$ as the codomain of the separable isogeny

$$\varphi_{\mathfrak{a}} : E \to E/E[\mathfrak{a}], \qquad E[\mathfrak{a}] = \bigcap_{u \in \mathfrak{a}} \ker \iota(u),$$

equipped with its induced $K$-orientation; it can be argued that such isogenies are indeed horizontal, and all separable horizontal isogenies arise in this way.

If $p = 0$ then this group action is sometimes called the complex multiplication torsor. Here, all curves in $\mathcal{Ell}_k(\mathcal{O})$ can be defined over a fixed number field (namely, the ring class field $L \supseteq K$ of $\mathcal{O}$), and the action is transitive. If $p > 0$ then there are four cases:

*(i)* If $p$ splits in $\mathcal{O}$ then all curves in $\mathcal{Ell}_k(\mathcal{O})$ are ordinary and defined over a fixed finite field $\mathbb{F}_q$, and again the action is transitive.

*(ii)* If $p$ ramifies in $\mathcal{O}$ but does not divide $[\mathcal{O}_K : \mathcal{O}]$ then all curves in $\mathcal{Ell}_k(\mathcal{O})$ are supersingular and can therefore be defined over $\mathbb{F}_{p^2}$; here too, the action is transitive.

*(iii)* If $p$ divides $[\mathcal{O}_K : \mathcal{O}]$ then $\mathcal{Ell}_k(\mathcal{O})$ is empty.

*(iv)* If $p$ is inert in $\mathcal{O}$ then all curves in $\mathcal{Ell}_k(\mathcal{O})$ are supersingular and thus definable over $\mathbb{F}_{p^2}$, but in this case there are two orbits. The Frobenius map $(E, \iota) \to (E^{(p)}, \iota^{(p)})$ jumps back and forth between these two orbits.

*Remark 2.* In the above statements, whenever we claim that all curves in $\mathcal{Ell}_k(\mathcal{O})$ can be defined over a fixed non-algebraically closed field (the ring class field $L$, or a finite field $\mathbb{F}_q$), then this also applies to their endomorphism rings, in particular to all endomorphisms in $\iota(\mathcal{O})$. However, we emphasize that in (1), the isomorphism $\cong$ remains to be interpreted over the algebraic closure.

### 2.3 Higher-Dimensional Isogeny Representations

Kani's Lemma [24] gives a tool for computing isogenies of dimension one using isogenies of dimension two. It was at the heart of the recent SIDH attacks [8,26,32], but it quickly turned into a powerful building block for isogeny-based protocols.

**Theorem 1 (Kani).** *Let $d_1, d_2$ and $N$ be pairwise coprime integers such that $N = d_1 + d_2$, and let $E_1$, $E_2$, $F_1$, and $F_2$ be elliptic curves connected by the following diagram of isogenies:*

$$\begin{array}{ccc} E_1 & \xrightarrow{\varphi_1} & F_1 \\ \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \varphi_2} \\ F_2 & \xrightarrow{\psi_1} & E_2 \end{array}$$

*such that* $\deg(\varphi_1) = \deg(\psi_1) = d_1$, $\deg(\varphi_2) = \deg(\psi_2) = d_2$ *and* $\varphi_2 \circ \varphi_1 = \psi_1 \circ \psi_2$. *Then the map*

$$\Phi = \begin{pmatrix} \varphi_1 & \hat{\varphi}_2 \\ -\psi_2 & \hat{\psi}_1 \end{pmatrix} : E_1 \times E_2 \to F_1 \times F_2$$

*is an $(N, N)$-isogeny of (principally polarized) abelian varieties with kernel*

$$\ker(\Phi) = \{(\hat{\varphi}_1(P), \varphi_2(P)) \mid P \in F_1[N]\}.$$

Assuming that $N$ is powersmooth, the isogeny $\Phi$ can be efficiently evaluated at any point on $E_1 \times E_2$. In practice, if $N = 2^a$ for some $a \geq 1$ (which will always be the case for us) one can use algorithms given in [18].

Kani's Lemma is mostly used in isogeny-based cryptography to represent isogenies of a given degree, leading to the following definition.

**Definition 4 (`2dim`-Representation).** *A* `2dim`-representation *for an isogeny $\varphi = \varphi_2 \circ \varphi_1$ of degree $d = d_1 \cdot d_2$ and with domain $E$ is a tuple*

$$(E, a, u, v, P, Q, \varphi(P), \varphi(Q))$$

*where $u, v \in \mathbb{N}$ under the condition that $ud_1 + vd_2 = 2^a$ and $(P, Q)$ a basis of $E[2^a]$.*

Definition 4 leverages the following result, which appeared in different shapes in the literature and that we report for convenience.

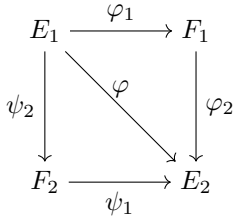
**Proposition 1.** *Let* $(E_1, a, u, v, P, Q, \varphi(P), \varphi(Q))$ *be a* `2dim`*-representation for an isogeny* $\varphi = \varphi_2 \circ \varphi_1 : E_1 \to E_2$*, where* $\varphi_1 : E_1 \to F_1$ *has degree* $d_1$*,* $\varphi_2 : F_1 \to E_2$ *has degree* $d_2$*, and*

$$ud_1 + vd_2 = 2^a \tag{2}$$

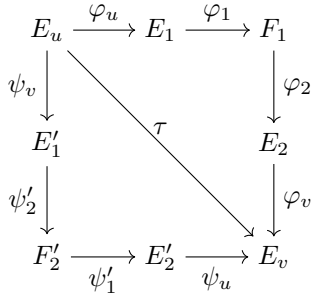
*where degree-*$u$ *isogenies from* $E_1$ *and degree-*$v$ *isogenies from* $E_2$ *are efficiently computable. Assume moreover* $d_1, d_2, u$ *and* $v$ *odd. Then we can efficiently evaluate:*

1. $\varphi_1$ *on any point on* $E_1$ *with order coprime with* $u$*;*
2. $\hat{\varphi}_2$ *on any point on* $E_2$ *with order coprime with* $v$*;*
3. $\varphi$ *on any point on* $E_1$*, with order coprime with* $uv$*.*

*Proof.* Equation (2) implies $\gcd(ud_1, vd_2) = 1$ and in particular $\gcd(d_1, d_2) = 1$. We have the following commuting square:




where $\psi_1$ is the pushforward of $\varphi_1$ and $\psi_2$ is the pullback of $\varphi_2$. In particular, $\deg(\varphi_1) = \deg(\psi_1) = d_1$ and $\deg(\varphi_2) = \deg(\psi_2) = d_2$. With the assumption that we can compute $u$-isogenies and $v$-isogenies from $E_1$ and $E_2$ respectively, and thanks to Equation (2), we can apply Theorem 1 to a new diagram, of the following form:




where $\varphi_u$ and $\varphi_v$ are any degree $u$ and $v$ isogenies, and $\tau = \varphi_v \circ \varphi_2 \circ \varphi_1 \circ \varphi_u = \varphi_v \circ \varphi \circ \varphi_u$. The map $\psi_u \circ \psi_1'$ is the pushforward of $\varphi_1 \circ \varphi_u$ and $\psi_2' \circ \psi_v$ is the pullback of $\varphi_v \circ \varphi_2$. Then, the map

$$\Phi = \begin{pmatrix} \varphi_1 \circ \varphi_u & \hat{\varphi}_2 \circ \hat{\varphi}_v \\ -\psi_2' \circ \psi_v & \hat{\psi}_1' \circ \hat{\psi}_u \end{pmatrix} : E_u \times E_v \to F_1 \times F_2$$

is a $(2^a, 2^a)$-isogeny with kernel

$$\ker(\Phi) = \{(\hat{\varphi_u} \circ \hat{\varphi_1}(P), \varphi_v \circ \varphi_2(P)) \mid P \in F_1[2^a]\} = \{([ud_1]P, \tau(P)) \mid P \in E_u[2^a]\}.$$

Thus, from the torsion point information and the knowledge of $\varphi_u$ and $\varphi_v$ we can compute $\ker(\Phi)$ and consequently evaluate $\Phi$. Now for given points $R \in E_u$ and $S \in E_v$, we have that

$$\Phi(R, 0) = (\varphi_1 \circ \varphi_u(R), -\psi_2' \circ \psi_v(R)), \quad \Phi(0, S) = (\hat{\varphi}_2 \circ \hat{\varphi}_v(S), \hat{\psi}_1' \circ \hat{\psi}_u(S)).$$

From the first components of these points, and with the knowledge of $\varphi_u$ and $\varphi_v$, we can recover $\varphi_1$ and $\hat{\varphi}_2$ on any point of order coprime with $u$ and $v$ respectively. This proves (1) and (2).
Now let $l$ be a prime and $R \in E_u[l]$. Let us assume that $l$ is coprime with $vd_2$ (otherwise it will be coprime with $ud_1$). Let $\langle P, Q \rangle = E_v[l]$. We can compute

$$\begin{aligned}\Phi(R, 0) &= (\varphi_1 \circ \varphi_u(R), -\psi_2' \circ \psi_v(R)),\\ \Phi(0, P) &= (\hat{\varphi}_2 \circ \hat{\varphi}_v(P), \hat{\psi}_1' \circ \hat{\psi}_u(P)),\\ \Phi(0, Q) &= (\hat{\varphi}_2 \circ \hat{\varphi}_v(Q), \hat{\psi}_1' \circ \hat{\psi}_u(Q)).\end{aligned}$$

Since $P$ and $Q$ form a basis of $E_v[l]$, and $\gcd(l, vd_2) = 1$, $P_1 = \hat{\varphi}_2 \circ \hat{\varphi}_v(P)$ and $Q_1 = \hat{\varphi}_2 \circ \hat{\varphi}_v(Q)$ form a basis of $F_1[l]$. We can then write $\varphi_1 \circ \varphi_u(R) = [x]P_1 + [y]Q_1$ and consequently

$$\tau(R) = \varphi_v \circ \varphi_2 \circ \varphi_1 \circ \varphi_u(R) = [xvd_2]P + [yvd_2]Q.$$

With the knowledge of $\varphi_u$ and $\varphi_v$, and consequently of their duals, we can recover the evaluation of $\varphi$ on points of order coprime with $uv$ from the evaluation of $\tau = \varphi_v \circ \varphi \circ \varphi_u$, which proves (3). □

This technique was first introduced in QFESTA [27], where the degree of $\varphi$ was restricted to the shape $q(2^a - q)$ (i.e. $u = v = 1$). Notably, together with the `RepresentInteger` algorithm of [20], this method allows us to find an endomorphism of degree $q(2^a - q)$ and hence find and evaluate isogenies of given (not necessarily smooth) degree $q$ from a curve with $j = 1728$. Building on this result, other works generalized it to the current form, most notably [29,4]. We refer to these papers for a more detailed exposition.

To efficiently compute degree $u$ (and $v$) isogenies from a given curve $E$, we generally have three options:

- if $u$ is smooth, a degree-$u$ isogeny can be computed from any curve;
- if $u$ is not smooth, we can compute a $u$-isogeny from $E$ with the technique from [27] mentioned above, assuming some additional information on $E$ (generally, the knowledge of the endomorphism ring is enough);
- if $u$ is non smooth and $\mathrm{End}(E)$ is unknown, there is no known way of efficiently computing a $u$-isogeny from $E$. A workaround consists in computing a $(u, u)$-isogeny in dimension 2, and moving the entire construction from Proposition 1 to dimension 4. This technique is explained in [17], and, while concretely feasible, it is significantly slower than the first two.

## 3 Orientations Factoring Through Frobenius

In this paper, we study case *(ii)* from the classification in Section 2.2. That is, we study primitively $\mathcal{O}$-oriented supersingular elliptic curves $E/\mathbb{F}_{p^2}$ in the case where $p$ ramifies in $\mathcal{O}$ but does not divide the conductor $[\mathcal{O}_K : \mathcal{O}]$. Necessarily $\mathcal{O}$ contains an element of the form

$$\sigma = \sqrt{-dp}$$

for some positive integer $d$ coprime with $p$. We take $\sigma$ such that $d$ is as small as possible, for reasons of efficiency (see below).

*Remark 3.* It may not be possible to pick $\sigma$ such that it concerns a generator of $\mathcal{O}$. Nevertheless a primitive orientation $\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E)$ is completely determined by $\iota(\sigma)$. To simplify notation, we will just assume that $\mathcal{O} = \mathbb{Z}[\sqrt{-dp}]$, since this has no effect on any of our conclusions. Only if we would want to act with ideals of norm 2, as in CSURF [7], then it would be important to be more careful. But in our case the 2-torsion is used for representing the orientation.

Since $[p]$ is purely inseparable, there must exist a degree-$d$ isogeny

$$\tau : E \xrightarrow{\tau} E^{(p)}$$

such that $\iota(\sigma) = \pi_p \circ \tau$, where $\pi_p : E \to E^{(p)}$ denotes the $p$-th power Frobenius isogeny. Clearly, in order to represent $\iota(\sigma)$, it suffices to represent the isogeny $\tau$, i.e. the degree-$p$ part of $\iota(\sigma)$ comes for free: this is the central observation on which this entire paper builds. E.g., using higher-dimensional isogeny representations, it suffices to specify how $\tau$ acts on a basis of $E[N]$ with $N > 2\sqrt{d}$. Clearly, this becomes more efficient for smaller values of $d$, which is why we take $d$ as small as possible for a given instance of $\mathcal{O}$.

Of course, the case $d = 1$ just corresponds to CSIDH [10], where we can always take $\tau = \mathrm{Id}$ and the orientation representation becomes totally implicit. (But one can also take $\tau = -\mathrm{Id}$ which leads to the twisted version of CSIDH.) Higher values of $d$ were studied by Chenu and Smith in [13], where they mainly focused on the cases $d = 2, 3$, but such small factors do not provide any additional security (in view of genus theory attacks, see Section 6.4); in contrast, the cases studied in this paper will correspond to large values of $d$ without small prime factors. From [13, Lemma 1] we recycle the following useful fact:

**Lemma 1.** $\hat{\tau} = \tau^{(p)}$.

*Proof.* We calculate

$$\tau^{(p)}\tau = \frac{-1}{p}\tau^{(p)}\pi^2\tau = \frac{-1}{p}\pi\tau\pi\tau = \frac{-1}{p}(\pi\tau)^2 = \frac{dp}{p} = d$$

and conclude by composing on the right with $\frac{1}{d}\hat{\tau}$. □

### 3.1 Representing the Orientation

To instantiate the framework described above, we will need an efficient way to encode and evaluate the isogeny $\tau$, which will be of large non-smooth degree. The only currently known method to do so is to embed them into 2-dimensional isogenies as described in Section 2.3. This will naturally put a constraint on the degrees we will choose for our orientation. In particular, we need to be able to solve Equation (2) where $d_1$ and $d_2$ are related to the norms of generators of the orders determining our orientations. In Section 4 and Section 5 we will discuss in more detail how this is done in practice.

### 3.2 Evaluating the Action

Given an efficient way of evaluating $\tau$ (and consequently $\sigma$), we can proceed to evaluate the group action. This is completely analogous to [12, Algorithm 3].

We start from an ideal $\mathfrak{a} = (m, \sigma - \lambda)$ of $O$ of odd norm $m$, coprime to $pd$, and an oriented curve $(E, \sigma)$. The first step is to compute the kernel $E[\mathfrak{a}]$ of $\mathfrak{a}$ on $E$. Let $X, Y$ be points of $E$ such that $\langle X, Y\rangle = E[m]$, $\sigma(X) = \lambda(X)$ and $\sigma(Y) = \mu(Y)$, where $(m) = \mathfrak{a}\overline{\mathfrak{a}} = (m, \sigma - \lambda)(m, \sigma - \mu)$. Notice that such $X, Y$ must exist since $(m)$ splits by construction. Any multiple of $X$ will generate $E[\mathfrak{a}]$. If we sample a random point $P \in E[m]$, we will have $P = aX + bY$ for some (unknown) $a, b$ and hence

$$\sigma(P) - \mu P = a(\sigma(X) - \mu X) + b(\sigma(Y) - \mu Y) = a(\lambda - \mu)X.$$

Thus, if $a \neq 0$, $\sigma(P) - \mu(P)$ generates the kernel of $\mathfrak{a}$. If $a = 0$ (which will happen with probability $1/m$), then $\sigma(P) - \mu(P) = 0$ and we will try again with another point $P'$. In particular, by choosing $P'$ to be independent from $P$, we can ensure $\sigma(P') - \mu P' = a'(\lambda - \mu)X$ with $a' \neq 0$.

*Remark 4.* This first step can be done on multiple ideals at the same time. Given ideals $\mathfrak{a}_i = (m_i, \sigma - \lambda_i)$ (with $m_i$ pairwise coprime), we sample a point $P \in E[\prod m_i]$ and define $\lambda$ to be the integer such that $\lambda \equiv \lambda_i \bmod m_i$ via the Chinese Reminder Theorem. We can then compute $R = \sigma(P) - \lambda P$ with a single evaluation of $\sigma$ (and in particular of $\tau$). By iterating the argument above, $(\prod_{j \neq i} m_j)R \in E[m_i]$, if non-zero, generates $\mathfrak{a}_i$.

Once a point $P$ generating the kernel $E[\mathfrak{a}]$ is found, the corresponding isogeny $\varphi_{\mathfrak{a}} : E \to E' \cong E/\langle P\rangle$ can be computed using Velu's formulae. Finally, we need to recover the orientation $\sigma' = \pi' \circ \tau'$ on $E'$. The involved isogenies respect the following diagram:

$$\begin{array}{ccccc} E & \xrightarrow{\tau} & E^{(p)} & \xrightarrow{\pi} & E \\ \downarrow{\scriptstyle \varphi_{\mathfrak{a}}} & & \downarrow{\scriptstyle \varphi_{\mathfrak{a}}^{(p)}} & & \downarrow{\scriptstyle \varphi_{\mathfrak{a}}} \\ E' & \xrightarrow{\tau'} & E'^{(p)} & \xrightarrow{\pi'} & E' \end{array}$$

and we have interpolation data of the form $(P, \tau(P))$ for $P \in E[2^a]$. Then, interpolation data for $\tau'$ is given by $(\varphi_{\mathfrak{a}}(P), -\frac{1}{p}\pi' \circ \varphi_{\mathfrak{a}} \circ \sigma(P))$.

*Remark 5.* At this step it is important not to publish $(\varphi_{\mathfrak{a}}(P), \varphi_{\mathfrak{a}}(Q))$ directly, where $(P, Q)$ is a basis of $E[2^a]$, as the secret isogeny $\varphi_{\mathfrak{a}}$ can otherwise be recovered by an attacker. However, a random scaling of the basis is enough to hide $\varphi_{\mathfrak{a}}$. In particular, picking a random basis on $E'$ and publishing its images under $\tau'$ does not leak any additional information.

### 3.3 Easily Acting Ideal Classes

As a byproduct of our construction, we obtain ideals that are very easy to act with, namely ideals of the form $I_l = (l, \sqrt{-dp})$ with $l|d$. Notice that in general $l$ will be a big prime, so acting with this ideal via a kernel computation is very expensive. First of all, we observe that such an ideal is 2-torsion (and typically has exact order 2) in the class group of $\mathbb{Z}[\sqrt{-dp}]$, since $I_l^2 = (l)$. To interpret the action of such an ideal, let us restrict to the case $d = l_1 l_2$ with $l_1, l_2$ distinct primes and $l_1 + l_2 = 2^a$. This will exactly match the setting of Section 5, but the argument can be adapted to work in general. When evaluating $\tau$ using the machinery from Section 2.3, we end up with the following diagram:

$$\begin{array}{ccc} E & \xrightarrow{\varphi_1} & F_1 \\ \downarrow{\scriptstyle \psi_2} & & \downarrow{\scriptstyle \varphi_2} \\ F_2 & \xrightarrow{\psi_1} & E^{(p)} \end{array}$$

where $\deg(\varphi_i) = \deg(\psi_i) = l_i$. Here we have $\tau = \varphi_2 \circ \varphi_1$. But recall from Lemma 1 that $\hat{\tau} = \tau^{(p)}$, so $\tau = \hat{\tau}^{(p)} = \hat{\varphi}_1^{(p)} \circ \hat{\varphi}_2^{(p)}$ is a factorization of $\tau$ into an $\ell_2$-isogeny followed by an $\ell_1$-isogeny: therefore, this is precisely the other side of the diagram, i.e., we can rewrite

$$\begin{array}{ccc} E & \xrightarrow{\varphi_1} & F_1 \\ \downarrow{\scriptstyle \hat{\varphi}_2^{(p)}} & & \downarrow{\scriptstyle \varphi_2} \\ F_1^{(p)} & \xrightarrow{\hat{\varphi}_1^{(p)}} & E^{(p)} \end{array}$$

Our goal is now to show that $I_1 = (l_1, \sqrt{-dp})$ corresponds to $\varphi_1$. This follows from the fact that $I_\tau = (d, \sqrt{-dp}) \subset I_1$, and so $\ker(I_1) \subset \ker(\tau)$ and $I_1$ has norm $l_1$. This shows that if we act with $I_1$ on $E$ we land on $F_1$. Moreover, the new orientation is given by

$$\sigma' = \frac{1}{l_1}\varphi_1 \sigma \hat{\varphi}_1 = \frac{1}{l_1}\varphi_1 \pi \varphi_2 \varphi_1 \hat{\varphi}_1 = \pi \varphi_1^{(p)} \varphi_2.$$

We proved that acting with $I_1$ effectively corresponds to flipping the diagram. In the same way, acting with $I_2$ correspond to flipping in the other direction

(we land on $F_1^{(p)}$), and acting with $I_p = (p, \sqrt{-dp})$ mirrors it (landing on $E^{(p)}$). Since to evaluate the action we have to construct all sides of the diagram anyway, we obtain three ideals whose action can be computed almost for free. However, all these ideals have order 2 in the class group (their squares are principal). So each $I_l$ provides only one bit of extra key space each. Moreover, their product is always trivial: we can see it directly in this case (e.g. acting with $I_1$ and then $I_2$ is the same as acting with $I_p$), but this is true more generally if we consider all the factors of $dp$. In conclusion: if there are $n$ different factors of $d$ whose corresponding isogeny appears in the evaluation of $\tau$, we have $n$ extra ideals of order 2 that we can evaluate efficiently, and consequently $n-1$ extra bits of key space. An alternative use of these bonus ideal classes lies in countering genus-theory attacks on the Decisional Diffie–Hellman problem (DDH), as illustrated in Section 6.4.

### 3.4 Split Primes and Exponents

In this work we focus on the key exchange setting, i.e. two parties (Alice and Bob) acting with small-norm ideals from a starting curve $E_0$. For an instantiation of our protocol we need to provide a list of small-norm ideals that we can easily act with. Typically, these will be of the form $\mathfrak{m}_i = (m_i, \sigma - \lambda)$ where $m_i$ is a small odd prime. A secret key then consists of a list of random exponents, one for each $\mathfrak{m}_i$, ranging in an interval $[-B, B]$ for some bound $B$. If we denote by $R$ the number of small-norm ideals, $B$ and $R$ will be crucial in determining the (classical) security of our key exchange protocol, as the size of the key space is $(2B+1)^R$. However, they will have no impact on the size of the class group, and hence on our quantum security, as argued in [11]. To prevent meet-in-the-middle attacks and guarantee 128 bits of security, we need $(2B+1)^R \approx 2^{256}$. On the other hand, we want to keep $B$ as small as possible, since it will determine the average number of times each party will need to compute an action. For a fixed $B$, we also choose $R$ to be as small as possible, while providing enough security, as it poses less constraints on parameter generation. The values for $B$ and $R$ reported in Table 1 are taken from [11, Tbl. 3] (we are in the OAYT setting).

**Table 1.** Exponent choices for 128 bits of security taken from [11, Tbl. 3]. $R$ is the number of acting ideals of small norm, with exponents in the interval $[-B, B]$.

| $B$ | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| $R$ | 139 | 95 | 79 | 70 | 64 |

*Remark 6.* As described here, our construction is a Restricted Effective Group Action (REGA). As it is the case for many similar constructions, it can be turned into an Effective Group Action (EGA) through some expensive precomputations, as mentioned in Section 2. We remark that such a choice will not alter our overall construction, but only eventually affect parameter choices.

## 4 The Square Case

In this section we consider orientations by $\sigma = \sqrt{-dp}$ with $d = f^2$, hence $\mathcal{O} = \mathbb{Z}[f\sqrt{-p}]$, where we recall the convention made in Remark 3. To facilitate parameter generation, we take $f = f_0 f_1$ the product of two large primes. This setting resembles SCALLOP-HD [12], where $\mathcal{O} = \mathbb{Z}[f\sqrt{-k}]$ for some small $k \in \mathbb{N}$. However, differently from SCALLOP-HD, we consider $p \gg k$, thus achieving much larger class groups while minimizing the size of the available 2-torsion required to represent the orientation. Indeed, the size of the class group of $\mathcal{O}$ in this setting is $h(\mathcal{O}) \approx \sqrt{dp} = f\sqrt{p}$. However, $d = f^2$ will have to satisfy some constraints. Let $\sigma = \tau \circ \pi_p = \sqrt{-dp} = f\sqrt{-p}$, where $\deg(\tau) = d = f^2$. To instantiate a class group action-based key exchange protocol as described in Section 3, we need to:

- represent $\tau$ with 2-dimensional isogenies;
- find ideals that are split in $\mathbb{Z}[f\sqrt{-p}]$ and easy to evaluate.

The first requirement imposes that the $2^a$-torsion points are defined over the base field, with $2^a > \sqrt{d} = f$. This forces $2^a \mid p + 1$. The second requirement, namely finding split ideals which are easy to evaluate, can be fulfilled by using the same strategy as in CSIDH. Imposing $m_i \mid p+1$ for a number of small primes $m_i$ ensures that the $m_i$-torsion points are defined over the base field and that they split in $\mathbb{Z}[f\sqrt{-p}]$, as we will detail in the next section.

### 4.1 Parameter Generation

**Choosing the Conductor.** As in the case of all SCALLOP variants, we require that $f_0, f_1$ are large primes to ensure the security of the protocol. For efficiency reasons, we additionally require that the isogeny $\tau$ of degree $f^2$ can be represented via a higher dimensional isogeny, as described in Section 2.3. Hence, we introduce two positive coprime integers $u, v \in \mathbb{N}$ and we require that Equation 2 is satisfied, namely, for fixed $u, v$ we define the binary quadratic form $Q_{u,v}(x, y) = ux^2 + vy^2$ and look for integer solutions to the equation $Q_{u,v}(x, y) = 2^a$. We can iterate over all combinations of $u, v$ for a fixed $a$, determined by the desired size of the class group, yielding candidates $x = f_0$, $y = f_1$ for the factors of the conductor $f$.

Lastly we choose $u$, $v$ small since we need to compute isogenies of degree $u$ and $v$ when evaluating $\tau$. This is not a strict requirement, as we will explain in Section 4.3.

**Choosing the Characteristic $p$.** In order to represent the orientation via a $(2^a, 2^a)$-isogeny, we need $2^a$-torsion points to be defined over the base-field, hence we require $2^a \mid p+1$, with $2^a > f$. Note that this last condition is already ensured for any $a$ such that $uf_0^2 + vf_1^2 = 2^a$. Additionally, the representation requires auxiliary isogenies, hence rational $u$, $v$-torsion points. Finally, for the computation of the class group action we need rational $m_i$-torsion points, hence

$m_i \mid p+1$, for small odd primes $m_i$ that split in $\mathbb{Z}[f\sqrt{-p}]$. Then, we take $p = 2^a c \prod m_i - 1$, where $uv \mid \prod m_i$ and where $c$ is a cofactor that ensures $p$ is prime; this way, all primes $m_i$ split in $\mathbb{Z}[f\sqrt{-p}]$. Indeed, $-p \equiv 1 \bmod m_i$ and thus the order discriminant $\Delta = -4f^2p$ is always a square modulo $m_i$.

### 4.2 Computing a Starting Curve and Finding the Orientation

To compute an $\mathcal{O}$-oriented starting curve $(E, \iota_E)$, we need to compute a descending $f$-isogeny starting from an elliptic curve that is oriented by $\mathbb{Z}[\sqrt{-p}]$, that is, a curve defined over $\mathbb{F}_p$.

To this end, we make use of the QFESTA technique [27] already mentioned in Section 2.3. In particular, we pick the elliptic curve $E_{1728} : y^2 = x^3 + x$, defined over $\mathbb{F}_p$ and use the `RepresentInteger` algorithm to compute a degree-$f$ isogeny $\varphi_f$ from $E_{1728}$. The algorithm yields a solution as long as $f(2^a - f) > p$. Depending on the choice of parameters, this condition might not hold, e.g. this is the case for the first parameter sets in Table 2. To circumvent this issue, we can make use of a variant introduced in [5], where `RepresentInteger` is used to find an endomorphism of degree $f(2^a - f)t$ for some smooth cofactor $t \mid p+1$, allowing to compute an isogeny of degree $tf$; since we can always compute smooth-degree isogenies from $E_{1728}$, the degree-$t$ part can then be removed. For more details on this strategy, we refer to [5].

The obtained $f$-isogeny $\varphi_f : E_{1728} \to E$ will be descending with overwhelming probability. Indeed, if $f_0, f_1$ are both inert in $\mathbb{Z}[\sqrt{-p}]$ we are guaranteed that any $f$-isogeny is descending and hence $E$ is oriented by the order $\mathbb{Z}[f\sqrt{-p}]$. On the other hand, even if $\left(\frac{-p}{f_i}\right) = 1$ for either factor $f_i \mid f$, there are exactly 2 horizontal and $f_i - 1$ descending isogenies. Since $f_0, f_1$ are large primes, a random $f$-isogeny is descending with overwhelming probability.

Once we have computed $\varphi_f$, we can take $\tau$ to be the composition of its dual $\widehat{\varphi_f}$ with the Frobenius conjugate $\varphi_f^{(p)}$. To this end, we only need to evaluate $\varphi_f$ and $\varphi_f^{(p)}$ on a basis $(P_0, Q_0)$ of $E_{1728}[2^a]$, followed by a base change to a canonical basis of $E[2^a]$; these steps are summarized in Algorithm 1. Note that the algorithm is correct because $\pi_p \circ \varphi_f \circ \pi_p \circ \widehat{\varphi_f} = [p] \circ \varphi_f^{(p)} \circ \widehat{\varphi_f}$ and $p \equiv -1 \bmod 2^a$.

The algorithm provides a `2dim`-representation of $\tau$, which is based on Proposition 1 and relies on auxiliary $u$ and $v$-isogenies, as illustrated in Fig. 1. Indeed, note that $\tau = \varphi_f^{(p)} \circ \widehat{\varphi_f}$ has degree $f^2 = f_0^2 f_1^2$, hence can be seen as a composition of an $f_0^2$-isogeny and an $f_1^2$-isogeny, whose degrees are chosen to satisfy Equation (2).

### 4.3 Parameter Choices

For a targeted order discriminant bit size, which we denote by $S$, we need to find

- a prime $p = 2^a c \prod m_i - 1$;

**Algorithm 1:** GenStartCurve

**Input:** A prime $p = 2^a c \prod \ell_i - 1$ and a conductor $f$
**Output:** A `2dim`-representation for an $\mathcal{O}$-oriented curve $(E, \iota_E)$, where $\mathcal{O} = \mathbb{Z}[f\sqrt{-p}]$

Let $E_{1728}/\mathbb{F}_{p^2}$ be the curve with $j = 1728$
Compute random isogeny $\varphi_f : E_{1728} \to E$ of degree $f$ via [27, Algorithm 2]
Choose deterministic bases $(R_0, S_0)$ of $E_{1728}[2^a]$ and $(R, S)$ of $E[2^a]$
Compute a matrix $\mathbf{A} \in \mathrm{GL}(2, 2^a)$ such that $(R_0, S_0) = \mathbf{A}(\pi_p(\widehat{\varphi}_f(R)), \pi_p(\widehat{\varphi}_f(S)))^\top$
$(R', S') \leftarrow -\mathbf{A}(\pi_p(\varphi_f(R_0)), \pi_p(\varphi_f(S_0)))^\top \in E^{(p)}[2^a]$
**return** $(E, R', S')$

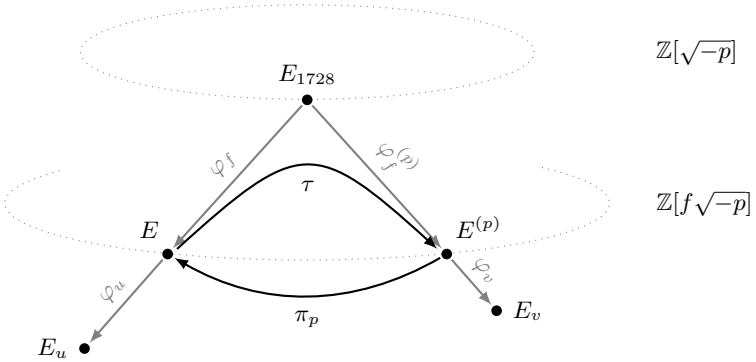



**Fig. 1.** An isogeny volcano with auxiliary isogenies $\varphi_u, \varphi_v$ for the `2dim`-representation of $\tau$.

– two primes $f_0$, $f_1$, such that $uf_0^2 + vf_1^2 = 2^a$ for some positive integers $u$, $v$ that are odd and coprime.

The number of primes $m_i$, is determined by the classical security of our protocol and by efficiency considerations, i.e. it depends on the number of times we will have to evaluate the action, as discussed in Section 3.4. Note that we must take into account that small prime divisors of $u$, $v$ are not usable for the class group action, as the corresponding torsion points will be needed to produce the auxiliary isogenies for the representation of $\tau$. Therefore, we will have $p = 2^a cM - 1$ with $M$ being the product of the first $R + n$ odd primes, where $n$ is the number of prime divisors of $uv$ among the first $R$ odd primes.

In order to find parameters for a class group discriminant $\Delta$ of expected bit size $S$, which mainly determines the class group size $h(\mathcal{O}) \approx \sqrt{|\Delta|} = 2f\sqrt{p}$ according to our previous discussions, we first estimate a range of corresponding values of $a$. Recall that $f \approx 2^a$ hence in general, for a given $S$ and $M$ we have $a \approx (S - \log_2 M)/3$. Note that, since $f_0$ and $f_1$ will have roughly the same bit size, we ensure $\log_2(f) > 2^{128}$ to avoid attacks via evaluation of prime-degree $f_i$-isogenies, as we will discuss in Section 6.3. Then, for a chosen value of $a$, iterating

on pairs $u$, $v$ we look for integer prime solutions $f_0$, $f_1$ to $Q_{u,v}(x, y) = 2^a$, of appropriate size. The values of $u$, $v$ are picked so that they are coprime and have few and small prime divisors. It is not a strict requirement that $u$, $v$ are of this form, as we could compute auxiliary isogenies from the starting curve and its Frobenius conjugate as push-forwards of $u$ and $v$-isogenies from $E_0$; then, during the action computation it suffices to compute their push-forwards through the isogeny we are acting with and its Frobenius conjugate.

In Table 2 we report on parameter sets that allow us to choose $B = 5$ and $B = 2$. For each set, $M$ is the product of all primes from 3 to the last prime reported in the table. We then set $p = 2^a cM + 1$. We set $d = f^2$, with $f = f_0 f_1$ where $f_0$ and $f_1$ are prime integer solutions to $2^a = uf_0^2 + vf_1^2$, not dividing $M$. The values of $c$, chosen to be coprime to $u$, $v$, are reported in the table, together with the size of $p$ and of the discriminant of the class group (note the class group size is half of the discriminant size).

**Table 2.** Parameter sets for the case $d = f^2$ with $f = f_0^2 f_1^2$, where $f_0, f_1$ are solutions to $uf_0^2 + vf_1^2 = 2^a$. The prime field characteristic is $p = 2^a cM - 1$, where $M$ is the product of distinct primes $m_i$ such that $m_1 = 3 \leq m_i \leq m_L$. Parameter $B$ is chosen to allow for 128 bit classical security.

| Discriminant size (bits) | $p$ size (bits) | $a$ | $m_L$ | $B$ | $c$ | $u$, $v$ |
|---|---|---|---|---|---|---|
| 1438 | 780 | 333 | 331 | 5 | 59 | 5, 3 |
| 4242 | 1897 | 1184 | 521 | 2 | 5 | 173, 83 |

## 5 The Square-Free Case

Let $d$ square-free, and $\mathcal{O} = \mathbb{Z}[\sqrt{-dp}]$. This setting was firstly studied in [13] for small $d$. The size of the class group of $\mathcal{O}$ in this setting is $h(\mathcal{O}) \approx \sqrt{dp}$. This means that by allowing $d$ to grow we can act with a larger class group for the same field size $p$. However, $d$ cannot grow indefinitely. Let $\sigma = \tau \circ \pi_p = \sqrt{-dp}$, where $\deg(\tau) = d$. To instantiate a CSIDH-like protocol in this setting we want to be able to

- represent $\tau$ with 2-dimensional isogenies;
- find ideals that are split for $\sigma$ and easy to evaluate.

The first requirements imposes the same conditions as in the previous case, which are described in Section 4: to represent $\tau$ we need access to the $2^a$ torsion, with $2^a > \sqrt{d}$, forcing $2^a \mid p + 1$ and giving us a lower bound on the size of $p$. The best result we can obtain with this approach is hence $d \approx p^2$, for a class group of size $\sqrt{dp} \approx \sqrt{p^3}$ over a field of size $p^2$.

However, we still have to take care of the second requirement, namely find split ideals which are easy to evaluate. The most natural way is again to adapt

the CSIDH approach to our setting: by imposing $m_i \mid p+1$ for enough small primes $m_i$ we gain access to the rational $m_i$ torsion. We still have to make sure that the ideal $(m_i)$ is split in $\mathcal{O}$ for all such $m_i$, but that can be achieved by a careful choice of $d$. On the other hand, this method imposes further constraints on $p$, forcing it to be bigger that the optimal size $\sqrt{d}$. Since the number of small ideals that we can evaluate is only relevant to the classical security of our scheme, and not the quantum one [11, Sec. 4], this effect is mitigated for higher quantum security levels. However, for small parameters this will become a significant limiting factor.

### 5.1 Finding the Orientation

A concrete way to instantiate the above setting is the following. Let us start by taking $E_0$ as the curve $y^2 = x^3 + 1$ in characteristic $p \equiv 2 \bmod 3$. Given a primitive 3rd root of unity $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$, the map $(x, y) \mapsto (\omega x, y)$ is an endomorphism on $E_0$, that we denote (with a slight abuse of notation) $\omega$ as well; in other terms, $\mathbb{Z}[\omega]$ naturally embeds into $\mathrm{End}(E_0)$. By [16, Prop. 4.7], a prime $l \neq 3$ appears as a norm of an element in $\mathbb{Z}[\omega]$ if and only if $l \equiv 1 \bmod 3$. As a consequence, for every prime $l \equiv 1 \bmod 3$ we can find an endomorphism on $E_0$ of norm $l$. We cannot choose $d$ to be prime, since we need to write it as $u(2^t - u)$ to embed $\tau$ into a 2-dimensional isogeny. The next natural choice is to look for $d = l_1 l_2$, with $l_1 \equiv l_2 \equiv 1 \bmod 3$. Let us fix $a$ even. Then $l_1 = 2^a - 3x$ and $l_2 = 2^a + 3x$ are both 1 mod 3, for any value of $x$. We can hence set $d = l_1 l_2 = l_1(2^{a+1} - l_1)$. Since in principle we have no restriction on $x$, we can try multiple values until both $l_1$ and $l_2$ are primes. We can then find elements $\alpha_1, \alpha_2 \in \mathbb{Z}[\omega]$ of norm $l_1, l_2$ respectively and define $\tau = \alpha_1 \alpha_2$.

There is still an aspect that we need to assess, namely how to access enough small ideals to act with. As already observed, by enforcing $m_i \mid p+1$ we can access the rational $m_i$ torsion for small primes. This also implies $-p \equiv 1 \bmod m_i$ is a square. To make sure that the ideal $(m_i)$ is split, we then need $\left(\frac{d}{m_i}\right) = 1$. If we impose $m_i \mid x$, we get $d = l_1 l_2 \equiv 2^{2a} \bmod m_i$, and so $d$ is a square modulo all the $m_i$ as required.

### 5.2 Parameter Generation

With the notation of the previous section, let us define $M = \prod_{i=1}^{R} m_i$. For a given $S$, denoting the bit size of the discriminant, we need to find

- a prime $p = 2^{a+1} c M - 1$;
- two primes $l_1 = 2^a - 3x$ and $l_2 = 2^a + 3x$, such that $\left(\frac{d}{m_i}\right) = 1$ for all $m_i$.

The value of $R$, and consequently of $M$, is determined by the classical security of our protocol and by efficiency considerations (the number of times we will have to evaluate the action), as discussed in Section 3.4. Asymptotically, the value of $M$ is just a constant, and should not impact the method outlined in Section 5.1.

However, if the security parameter $S$ is not big enough compared to $M$, we may run into trouble. In general, for a given $S$ and $M$ we would like to compute $a$ as $\lceil (S - \log_2 M)/3 \rceil$, then set $p = 2^{a+1}cM - 1$ (for a small cofactor $c$) and $d \approx 2^{2a}$ as outlined above. If we set $l_i = 2^a \pm x$ where $M \mid x$ this method will fail as soon as $\log_2 M > a$, or $S < 4 \log_2 M$, strongly limiting our parameter choices. Notice that for fixed $M$ and $a$ we have roughly $2^a/M$ choices for $l_1$ and $l_2$; since the probability of a number $l$ being prime is $1/\log l$, assuming independence between $l_1$ and $l_2$ the probability that they are both prime is roughly $1/a^2$, meaning that we need $2^a/M > a^2$ to find a valid pair (this estimate is extremely conservative; see Remark 7). If this is not true, we can relax the condition $M \mid x$ and replace it with $M' \mid x$, where $M' = \prod_{i=1}^{R'} m_i$ with $R' = R - k$. In this way, the condition $\left(\frac{d}{m_i}\right) = 1$ is automatically satisfied only by the $m_i$ for $i < R'$; this means that the number of attempts to find a valid pair $l_1, l_2$ grows by a factor $2^k$. On the other hand, the number of possibilities grows by a factor $\prod_{i=R'}^{R} m_i$, i.e. the product of the last $k$ primes. This product is certainly bigger than $2^k$, and generally by some margin. For instance, the last prime if we pick $B = 1$ in Table 1 is 809, which is 10 bits. This greatly improves our chance of finding valid parameters. While the choice of $k$ is limited by our computational capabilities, this is a one time computation.

We show the effectiveness of our method by computing a parameter set for a discriminant size of 1500 bits where $B = 5$ and so $M$ is 424 bits, way above the limit $S/4$. To investigate the scalability of our protocol we also provide a parameter with $S = 4000$, but there $B = 2$ and so we get $a > \log_2 M$. These parameters are reported in Table 3. The prime is $p = 2^{a+1}cM - 1$, and $d = l_1 l_2$ where $l_i = 2^a \pm xM'$, with $M'$ defined as above.

**Table 3.** Parameter sets for the case $d = l_1 l_2$ square-free, where $l_i = 2^a \pm xM'$ and $M'$ is the product of primes $m_i$ such that $3 \leq m_i \leq m_{L-k}$. The prime field characteristic is $p = 2^{a+1}cM - 1$, where $M$ is the product of distinct primes $m_i$ such that $m_1 = 3 \leq m_i \leq m_L$. Parameter $B$ is chosen to allow for 128 bit classical security.

| Discriminant size (bits) | $p$ size (bits) | $a$ | $m_L$ | $B$ | $c$ | $x$ | $k$ |
|---|---|---|---|---|---|---|---|
| 1506 | 786 | 360 | 313 | 5 | 2 | 2308855 | 11 |
| 4006 | 1802 | 1102 | 503 | 2 | 51 | 8075 | 0 |

*Remark 7.* The probability (loosely speaking) that a random number $n$ is prime is asymptotic to $1/\log n$. Hence, the probability that two random numbers $n_1, n_2 \approx n$ are prime at the same time is $1/(\log n)^2$. However, we are working with numbers of the form $2^a \pm xM$, with $M$ a product of many small primes. This already ensures that $l_1$ and $l_2$ are not divisible by all the $m_i$, greatly boosting their probability of being prime. Moreover, they are coprime with each other, making the probability slightly higher. Determining the number of representations of a number as a sum of two primes is a famous open problem in mathematics, known

as the *extended Goldbach's conjecture*; a more detailed treatment of the matter is outside the scope of this work. However, form this preliminary discussion we can already conclude that the estimate $1/a^2$ provided above is conservative.

### 5.3 Protocol Setup

Unlike in the square case, we can setup our protocol already on $E_0 : y^2 = x^3 + 1$, the curve of $j$-invariant 0. We can then efficiently evaluate $\tau = \alpha_1\alpha_2$ (where $\alpha_1$ and $\alpha_2$ are the endomorphisms of norm $l_1$ and $l_2$ described above) as an endomorphism. Notice that $\tau$ could also be represented by a 2-dimensional isogeny, namely

$$\Phi : E_0 \times E_0 \to E_0 \times E_0 = \begin{pmatrix} \alpha_1 & \hat{\alpha_2} \\ -\alpha_2 & \hat{\alpha_1} \end{pmatrix},$$

as detailed in Section 3.1. This representation is used to evaluate the orientation away from $E_0$. For this reason, the first step of the action from $E_0$ (namely, the first step of the public key generation) will be much faster than the subsequent ones.

Moreover, we observe the following interesting fact. Recall that, by construction, $\alpha_1, \alpha_2 \in \mathbb{Z}[\omega]$.

**Proposition 2.** *Let*

$$\Phi : E_0 \times E_0 \to E_0 \times E_0 = \begin{pmatrix} \alpha_1 & \hat{\alpha_2} \\ -\alpha_2 & \hat{\alpha_1} \end{pmatrix}$$

*be a $(2^n, 2^n)$-isogeny, with $\alpha_1, \alpha_2 \in \mathbb{Z}[\omega]$. Then we can write $\Phi$ as a composition of $n$ $(2,2)$ isogenies $\Psi_i : E_0 \times E_0 \to E_0 \times E_0$, $i = 1, \ldots, n$, of the form*

$$\Psi_i = \begin{pmatrix} \gamma & 1 \\ -1 & \hat{\gamma} \end{pmatrix}$$

*with $\gamma \in \mathbb{Z}[\omega]^\times$.*

*Proof.* We proceed by induction. The first step is to prove that if $\Phi$ is a $(2,2)$-endomorphism of $E_0 \times E_0$, it can always be expressed in the form above, up to post-composition with an isomorphism, or in other words up to multiplication on the left with an invertible matrix. Since $n(\alpha_1)+n(\alpha_2) = 2$, and $\mathbb{Z}[\omega]$ does not contain elements of norm 2 ([16, Prop. 4.7]), we must have $n(\alpha_1) = n(\alpha_2) = 1$. In particular $\alpha_1$, $\alpha_2$ are isomorphisms, and their inverses coincide with the dual. Then,

$$\begin{pmatrix} \alpha_2 & 0 \\ 0 & \hat{\alpha_2} \end{pmatrix} \begin{pmatrix} \alpha_1 & \hat{\alpha_2} \\ -\alpha_2 & \hat{\alpha_1} \end{pmatrix} = \begin{pmatrix} \alpha_2\alpha_1 & 1 \\ -1 & \hat{\alpha_1}\hat{\alpha_2} \end{pmatrix}$$

and the matrix on the right corresponds to $\Psi_1$ with $\gamma = \alpha_2\alpha_1$.

For the induction step, given the matrix $\Phi$ with $n(\alpha_1)+n(\alpha_2) = 2^n$, we want to write it as

$$\begin{pmatrix} \alpha_1 & \hat{\alpha_2} \\ -\alpha_2 & \hat{\alpha_1} \end{pmatrix} = \begin{pmatrix} \beta_1 & \hat{\beta_2} \\ -\beta_2 & \hat{\beta_1} \end{pmatrix} \begin{pmatrix} \gamma & 1 \\ -1 & \hat{\gamma} \end{pmatrix}$$

with the additional condition $n(\beta_1)+n(\beta_2) = 2^{n-1}$ and $n(\gamma) = 1$. By expanding the product, we obtain two equations

$$\begin{cases} \alpha_1 = \beta_1\gamma - \hat{\beta}_2 \\ \alpha_2 = \beta_2\gamma + \hat{\beta}_1 \end{cases}$$

that we can rearrange into

$$\begin{cases} \alpha_1 - \gamma\hat{\alpha_2} = -2\hat{\beta}_2 \\ \alpha_1 + \gamma\hat{\alpha_2} = 2\beta_1\gamma. \end{cases}$$

We are left with proving that there exists $\gamma \in \mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$ such that $\alpha_1 + \gamma\hat{\alpha_2} \equiv 0 \bmod 2$ for any given $\alpha_1, \alpha_2$ such that $n(\alpha_1) + n(\alpha_2) = 2^n$. Let us assume this is not true. We can then write down $\alpha_1, \alpha_2 \in \mathbb{Z}[\omega]$, and compute $\alpha_1 + \gamma\hat{\alpha_2} \bmod 2$ for each $\gamma \in \mathbb{Z}[\omega]$. We get a set of 4 binary equations (three choices for $\gamma$ plus the norm condition) which have to hold at the same time. Direct calculation shows that this is not possible. From the above system,

$$n(\beta_1) + n(\beta_2) = \frac{1}{4}(n(\alpha_1 - \gamma\alpha_2) + n(\alpha_1 + \gamma\alpha_2)) = \frac{1}{4}(2n(\alpha_1) + 2n(\alpha_2))$$

from which we conclude that $n(\beta_1) + n(\beta_2) = 2^{n-1}$.

As a consequence, our starting orientation $\Phi$ on $E_0 \times E_0$ can be written as a composition of $(2,2)$-endomorphisms. This ceases to be true as we move away from $E_0$, since we do no longer see all elements of $\mathbb{Z}[\omega]^\times$ as endomorphisms.

## 6 Security

As for the hardness of the vectorization problem, i.e., the problem of retrieving the secret ideal class $[\mathfrak{a}]$ connecting two public oriented elliptic curves $(E, \iota)$ and $(E', \iota') = [\mathfrak{a}](E, \iota)$, we largely fall back on the discussion from [11], which is restricted to Frobenius orientations aka CSIDH, but the analysis carries over to all orientations as long as one works in the REGA framework. In a nutshell, to achieve classical 128-bit security, the size of the key space should be in the order of 256 bits due to meet-in-the-middle attacks. It is believed that this is also suffices against a quantum adversary; Grover-type speed-ups over the standard meet-in-the-middle algorithm have been proposed in the past but are now considered unrealistic [23,11]. However, a much bigger quantum threat is Kuperberg's algorithm (and its descendants) for hidden-shift finding, which runs in time $L_{|\Delta|}(1/2)$. For this reason the discriminant $\Delta$ should be large (in absolute value). How large exactly is a topic of debate. Two of the main fuzzy factors are the cost of an oracle query and the cost of using quantum random access classical memory (QRACM). For NIST level 1, the authors of [11] propose a discriminant of 4096 bits, which is why these orders of magnitude were included in Table 2 and Table 3, along with the more aggressive choice $|\Delta| \approx 1596$.

Let us now discuss some (non-)threats that are specific to our proposal.

### 6.1 Known Endomorphisms

A priori, a security concern could be that the orientation gives away *two* endomorphisms of $E$ in interpolation form, thereby potentially revealing a full-rank subring of $\mathrm{End}(E)$: indeed, an eavesdropper has access to

$$\tau^{(p)} \circ \tau \qquad \text{and} \qquad \pi \circ \tau.$$

However, this was resolved in Lemma 1: the first map is just the multiplication-by-$d$ map. Thus, we only leak an embedding of $\mathcal{O}$, and this is the same as for all known class group actions.

### 6.2 Acting on Conjugate Pairs

Recall from Section 3.3 that the ideal class $[(p, \sqrt{-dp})]$ acts by Frobenius conjugation. Therefore, the action of $\mathrm{cl}(\mathbb{Z}[\sqrt{-dp}])$ on our set of oriented elliptic curves $E \xrightarrow{\tau} E^{(p)}$ induces a well-defined action of

$$\frac{\mathrm{cl}(\mathbb{Z}[\sqrt{-dp}]}{\langle[(p, \sqrt{-dp})]\rangle} \quad \text{on the set of conjugate pairs} \quad E \xrightarrow{\tau} E^{(p)}, E^{(p)} \xrightarrow{\tau^{(p)}} E.$$

Of course, this is just a special case of a general statement: for every subgroup $H \subset \mathrm{cl}(\mathcal{O})$, the quotient group $\mathrm{cl}(\mathcal{O})/H$ acts on the set of orbits under $H$. However, despite the size of $\mathrm{cl}(\mathcal{O})/H$ being smaller, in general this does not lead to a simpler vectorization problem: it is very hard to represent the orbits in a way that allows for the desired quantum state collapses in Kuperberg's algorithm. However, in the case of conjugate pairs this is much more natural, so it could allow for a faster run of Kuperberg's algorithm. But this just reduces the size of $\mathrm{cl}(\mathcal{O})$ with 1 bit, so the effect is minimal.

### 6.3 Walking Up the Volcano

In the setting of Section 4, namely when the orientation comes from $\mathbb{Z}[f\sqrt{-p}]$, a potential attack consists in walking up the isogeny volcano to solve the vectorization problem in a larger suborder of $\mathbb{Z}[\sqrt{-p}]$ (with smaller class group) instead. In our case $f = f_0 f_1$, so the cost of walking up is lower bounded by the cost of computing any $f_0$ (or $f_1$) isogeny from a random curve. Computing isogenies of large prime degree is considered cryptographically hard, with the best known classical algorithms running in $\widetilde{O}(d^2)$ where $d$ is the degree [3, Section 4.4]. Moreover, no quantum speed-up on such algorithms is currently known. To protect against such an attack it is thus sufficient to ensure $f_0, f_1 \approx 2^{64}$, which is way below the sizes we need for quantum security.

### 6.4 Genus Theory Attacks

Another potential attack consists in breaking the Decisional Diffie-Hellman (DDH) assumption using genus theory. Let $\mathcal{O}$ be the order giving the orientation, and

$\Delta = -2^a m_1^{e_1} \cdots m_r^{e_r}$ its discriminant, factored into powers of distinct primes. For any odd prime factor $m_i$ we have an assigned character

$$\chi_{m_i} : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\} : [I] \mapsto \left(\frac{N(I)}{m_i}\right)$$

where $[I]$ is assumed to be represented by an ideal of norm coprime with $m_i$. If $\Delta = -4n$ is even and $n \not\equiv 3 \bmod 4$ then this list is extended with one or two additional characters. Moreover, there is a unique non-trivial relation among the characters [9, Eq. (3)]. The authors of [9] give a way to evaluate such an assigned character on an ideal class $[I]$ given access only to $(E, \iota)$ and $[I](E, \iota)$. The cost of this evaluation is exponential in the size of $m_i$, meaning that we can only evaluate characters for small prime factors of the discriminant (and also the additional characters in case they occur). Being able to evaluate a non-trivial character effectively breaks the DDH assumption in our setting.

The discriminant of $\mathbb{Z}[\sqrt{-dp}]$ is $-4dp$. Since both $d$ and $p$ do not have small prime factors, the only characters that we have to avoid are the additional ones. In the concrete set-up from Section 4, $p \equiv 3 \bmod 4$ and $d = f^2 \equiv 1 \bmod 4$, so $dp \equiv 3 \bmod 4$ and there are no additional characters. In the set-up from Section 5, $p \equiv 3 \bmod 4$, and $l_1 \equiv -l_2 \bmod 4$ implying $d \equiv 3 \bmod 4$. As a consequence, $dp \equiv 1 \bmod 4$ and in this case there is a unique additional character

$$\delta : \mathrm{cl}(\mathcal{O}) \to \{\pm 1\} : [I] \mapsto (-1)^{(N(I)-1)/2}$$

(where now $[I]$ is assumed represented by an ideal of odd norm) which is non-trivial and whose action is easy to evaluate [9, Prop. 1]. Thus in this case the DDH assumption does not apply. One way out is to act with keys sampled from the subgroup $\ker \delta \subset \mathrm{cl}(O)$. This is easy to control: when acting with a key $(e_1, \ldots, e_R)$ representing an ideal class $[\mathfrak{m}_1]^{e_1} \cdots [\mathfrak{m}_R]^{e_R}$, one should verify that

$$e_1 \frac{m_1 - 1}{2} + \ldots + e_R \frac{m_R - 1}{2} \equiv 0 \bmod 2 \tag{3}$$

and try another key if this is violated. Unless $m_i \equiv 1 \bmod 4$ for all $i$ (in which case we are automatically sampling from $\ker \delta$), this reduces the size of the key space by about 1 bit. An alternative option is to also act with $[(p, \sqrt{-dp})]$, which just amounts to flipping as was explained in Section 3.3, whenever (3) is violated. This ideal class indeed has $\delta$-value equal to $-1$ because $p \equiv 3 \bmod 4$, so it multiplies any other ideal class with $\delta$-value $-1$ into $\ker \delta$.

### 6.5 Validating the Starting Curve

In this section we briefly discuss how to validate a starting curve, namely to verify that it was honestly generated. In our setting, the starting curve is a curve together with an orientation, and it is honestly generated if the orientation is by $\mathbb{Z}[\sqrt{-dp}]$ and primitive. Indeed, if the orientation was not primitive, the parties engaging in the protocol would act by ideals of a generally bigger order than

$\mathbb{Z}[\sqrt{-dp}]$, hence by elements of a smaller ideal class group. The class number of a suborder $O' \subset O$ of index $f$ is indeed roughly $f$ times bigger than the class number of $O$, as proven in [16, Theorem 7.24] and [25, Theorem 5.4].

We note that in the case where $\mathbb{Z}[\sqrt{-dp}]$ is a maximal order, namely when $d$ is square-free and $-dp \not\equiv 1 \bmod 4$, the starting curve must be honestly generated as long as the orientation generates an order of the correct discriminant, which can be checked via pairings. This is always the case in the setting of Section 5, where we have $p \equiv 3 \bmod 4$ and $l_1 \equiv -l_2 \bmod 4$, implying $d = l_1 l_2 \equiv 3 \bmod 4$ and hence $-dp \equiv 3 \bmod 4$.

We mention that, even if $\mathbb{Z}[\sqrt{-dp}]$ with $d$ square-free was not maximal, it would be a suborder of conductor 2 in the maximal order $\mathbb{Z}[\frac{1+\sqrt{-dp}}{2}]$; in this case, either 2 is inert, hence the class number of the suborder is the same as that of the maximal order, or 2 is split, hence the class number of the suborder is three times the size of that of the maximal order. Thus, a non-primitive orientation in this setting would either provide no advantage to an attacker, or reduce the security of only roughly 1 bit.

We are then going to discuss the setting of Section 4, where $\mathbb{Z}[\sqrt{-dp}]$ with $d = f^2$ has a non-trivial conductor $f = f_0 f_1$, and $f_0$ and $f_1$ are distinct primes. We recall that $f$-isogenies from a curve that is primitively oriented by $\mathbb{Z}[f\sqrt{-p}]$ are descending with overwhelming probability, as explained in Section 4.2. In particular, a starting curve that is computed via Algorithm 1 will always be honestly generated with overwhelming probability.

In order to validate the starting curve, one should first check that the given orientation $\sigma$ generates an order with the correct discriminant via pairings, then verify that the orientation is primitive by checking that $\sigma$ does not factor through multiplication by $f_0$ or $f_1$. For this second step, one can consider the given `2dim`-representation of $\tau$ and the corresponding isogeny diagram illustrated in Section 2.3, where $\tau$ is viewed as composition of $f_0^2$ and $f_1^2$-isogenies. According to Proposition 1, the codomain curve of the isogeny of degree $f_0^2$ can be computed; if it is equal to the domain then $\tau$, hence $\sigma$, has to factor through multiplication by $f_0$; similarly, if the codomain of the isogeny of degree $f_1^2$ equals its domain, then the orientation factors through multiplication by $f_1$.

We remark that the above considerations apply in the same way to public-key validation, which would be required to protect against active attacks on encryption schemes based on our construction in a static setting.

## 7 Implementation

We provide a proof-of-concept sage implementation of our protocol, to show feasibility and allow for a first comparison with other existing schemes. We stress that many known optimizations are still possible, especially in the setting of key exchange discussed in the paper.

### 7.1 Timings for the Case $d = f^2$

We report timings of an action computation from a starting curve in Table 4 for parameter sets from Table 2.

**Table 4.** Timings for the case $d = f^2$. Average timing for an action computation.

| Discriminant size | Avg. action | $B$ |
|---|---|---|
| 1438 | 100.50s | 5 |
| 4242 | 547.78s | 2 |

### 7.2 Timings for the Case $d$ Square-Free

As already discussed, in the maximal order case the first step of the action computed from $E_0$ is much faster than the other ones, since on $E_0$ evaluating the orientation does not require 2-dimensional isogenies. We report timings in Table 5, highlighting this difference. We compare timings for the first step of the action when starting from $E_0$ and from a random curve $E$; we then report timings for the remaining $B-1$ steps, which are all done from a random curve, separately. Notice that in general the last $B-1$ steps will be each on average faster than the first step from a random curve, since the exponents are progressively smaller.

A key generation will consist in a step from $E_0$ together with the remaining $B-1$ steps, while the key exchange will include a step from a given $E$ and the remaining $B-1$ steps. Notice that in the latter case the first step can sometimes be precomputed and included in the public key, as discussed in Section 7.3.

**Table 5.** Timings for the case $d$ square-free. Average timing of the first step of an action computation from $E_0$, average timing of the first step of an action computation from a random curve $E$ and average timing of the last $B-1$ steps of an action computation.

| Discriminant size | Avg. first step from $E_0$ | Avg. first step from $E$ | Avg. $B-1$ last steps | $B$ |
|---|---|---|---|---|
| 1506 | 3.77s | 9.17s | 26.82s | 5 |
| 4006 | 25.18s | 93.24s | 74.57s | 2 |

### 7.3 Sizes

A public key consists in two pair of points, $(P_1, Q_1) \in E$ and $(P_2, Q_2) = (\tau(P_1), \tau(Q_1)) \in E^{(p)}$. Recall that we are working over the prime field $\mathbb{F}_{p^2}$, where $p$ is of the form $p = 2^a cM - 1$. In general, we can always assume $(P_1, Q_1)$

to be a deterministic basis of $E$, and to be working with Montgomery curves. To send this information there are two main strategies:

- sending the points $(P_2, Q_2)$ directly; this allows us to recover the Montgomery coefficient of $E$, and compute $P_1, Q_1$ from there. We can stretch this a bit more, and send $P_2$ and only the $x$-coordinate of $Q_2$, together with a bit denoting the sign of its $y$ coordinate. Moreover, in this case the points $(P_i, Q_i)$ do not need to be a basis of the respective $2^a$-torsion, but can instead be points of $p+1$-torsion at no additional cost. This allows Alice to precompute one step of the action of Bob, and publish that in the public data. The size in this case is $6p$;
- sending the Montgomery coefficient of $E$ together with 4 coefficients in $\mathbb{Z}_{2^a}$, representing the coordinates of $P_2$ and $Q_2$ in terms of a deterministic basis of $E^{(p)}$. If we are mainly concerned about sizes, we can send only 3 such coefficients and recover the fourth one using pairings. The size in this case is $2p + 3a$.

## References

1. Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part II*, volume 12492 of *LNCS*, pages 411–439. Springer, Cham, December 2020.
2. Bill Allombert, Jean-François Biasse, Jonathan Komada Eriksen, Péter Kutas, Chris Leonardi, Aurel Page, Renate Scheidler, and Márton Tot Bagi. Faster SCALLOP from non-prime conductor suborders in medium sized quadratic fields. In *Public-Key Cryptography – PKC 2025*, volume 15676 of *Lecture Notes in Computer Science*, pages 333–363, 2025.
3. Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. PRISM: Simple and compact identification and signatures from large prime degree isogenies. In *Public-Key Cryptography – PKC 2025*, volume 15676 of *Lecture Notes in Computer Science*, pages 300–332, 2025.
4. Andrea Basso, Pierrick Dartois, Luca De Feo, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-West - the fast, the small, and the safer. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 339–370. Springer, Singapore, December 2024.
5. Andrea Basso and Luciano Maino. POKÉ: A compact and efficient PKE from higher-dimensional isogenies. In *Advances in Cryptology – Eurocrypt 2025 Part II*, volume 15602 of *Lecture Notes in Computer Science*, pages 94–123. Springer, 2025.
6. Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In *Proceedings of Asiacrypt 2019 Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247, 2019.
7. Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 111–129. Springer, Cham, 2020.

8. Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 423–447. Springer, Cham, April 2023.
9. Wouter Castryck, Marc Houben, Frederik Vercauteren, and Benjamin Wesolowski. On the decisional Diffie-Hellman problem for class group actions on oriented elliptic curves. *Research in Number Theory*, 4(8):article 99, 2022. Proceedings of ANTS-XV.
10. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *ASIACRYPT 2018, Part III*, volume 11274 of *LNCS*, pages 395–427. Springer, Cham, December 2018.
11. Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. The SQALE of CSIDH: sublinear Vélu quantum-resistant isogeny action with low exponents. *Journal of Cryptographic Engineering*, 12(3):349–368, 2022.
12. Mingjie Chen, Antonin Leroux, and Lorenz Panny. SCALLOP-HD: Group action from 2-dimensional isogenies. In Qiang Tang and Vanessa Teague, editors, *PKC 2024, Part II*, volume 14603 of *LNCS*, pages 190–216. Springer, Cham, April 2024.
13. Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. *Mathematical Cryptology*, 1:85–101, 2021.
14. Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. Cryptology ePrint Archive, Report 2020/985, 2020.
15. Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Paper 2006/291, 2006.
16. David A. Cox. *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*. Pure and Applied Mathematics: A Wiley Series of Texts, Monographs and Tracts. Wiley, 2013.
17. Pierrick Dartois, Jonathan Komada Eriksen, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, and Benjamin Wesolowski. PEGASIS: Practical effective class group action using 4-dimensional isogenies. In *Advances in Cryptology – Crypto 2025*, Lecture Notes in Computer Science, 2025. To appear.
18. Pierrick Dartois, Luciano Maino, Giacomo Pope, and Damien Robert. An algorithmic approach to (2, 2)-isogenies in the theta model and applications to isogeny-based cryptography. In Kai-Min Chung and Yu Sasaki, editors, *ASIACRYPT 2024, Part III*, volume 15486 of *LNCS*, pages 304–338. Springer, Singapore, December 2024.
19. Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: Scaling the CSI-FiSh. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023, Part I*, volume 13940 of *LNCS*, pages 345–375. Springer, Cham, May 2023.
20. Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *ASIACRYPT 2020, Part I*, volume 12491 of *LNCS*, pages 64–93. Springer, Cham, December 2020.
21. James L. Hafner and Kevin S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American Mathematical Society*, 2(4):837–850, 1989.

22. Marc Houben. A Montgomery ladder for isogenies. Talk given at SQIparty 2025, University of Lleida, Catalonia, Spain, April 28–30, 2025. Slides available at `http://www.cig.udl.cat/sitemedia/files/SQIparty2025/Wed_02_Houben.pdf`, 2025.
23. Samuel Jaques and André Schrottenloher. Low-gate quantum golden collision finding. In *Selected Areas in Cryptography*, volume 12804 of *Lecture Notes in Computer Science*. Springer, 2020.
24. Ernst Kani. The number of curves of genus two with elliptic differentials. 1997.
25. Gene S. Kopp and Jeffrey C. Lagarias. Class field theory for orders of number fields, 2022.
26. Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on SIDH. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 448–471. Springer, Cham, April 2023.
27. Kohei Nakagawa and Hiroshi Onuki. QFESTA: Efficient algorithms and parameters for FESTA using quaternion algebras. In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part V*, volume 14924 of *LNCS*, pages 75–106. Springer, Cham, August 2024.
28. Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields and Their Applications*, 69, 2021. Article No. 101777.
29. Aurel Page and Damien Robert. Introducing clapoti(s): Evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, Report 2023/1766, 2023.
30. Lorenz Panny. CSI-FiSh really isn't polynomial-time. Blah post available at `https://yx7.cc/blah/2023-04-14.html`, 2023.
31. Lorenz Panny, Christophe Petit, and Miha Stopar. KLaPoTi: An asymptotically efficient isogeny group action from 2-dimensional isogenies. Cryptology ePrint Archive, Report 2024/1844, 2024.
32. Damien Robert. Breaking SIDH in polynomial time. In Carmit Hazay and Martijn Stam, editors, *EUROCRYPT 2023, Part V*, volume 14008 of *LNCS*, pages 472–503. Springer, Cham, April 2023.
33. Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145, 2006.
34. Sogo Pierre Sanon. *Endomorphism rings of ordinary abelian varieties*. PhD thesis, TU Kaiserslautern, 2022.
35. René Schoof. Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory, Series A*, 46(2):183–211, 1987.
36. William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969.