Orientations and the supersingular endomorphism ring problem

Benjamin Wesolowski

Univ. Bordeaux, CNRS, Bordeaux INP, IMB, UMR 5251, F-33400, Talence, France
INRIA, IMB, UMR 5251, F-33400, Talence, France

Abstract. We study two important families of problems in isogeny-based cryptography and how they relate to each other: computing the endomorphism ring of supersingular elliptic curves, and inverting the action of class groups on oriented supersingular curves. We prove that these two families of problems are closely related through polynomial-time reductions, assuming the generalised Riemann hypothesis.
We identify two classes of essentially equivalent problems. The first class corresponds to the problem of computing the endomorphism ring of *oriented curves*. The security of a large family of cryptosystems (such as CSIDH) reduces to (and sometimes from) this class, for which there are heuristic quantum algorithms running in subexponential time. The second class corresponds to computing the endomorphism ring of *orientable curves*. The security of essentially all isogeny-based cryptosystems reduces to (and sometimes from) this second class, for which the best known algorithms are still exponential.
Some of our reductions not only generalise, but also strengthen previously known results. For instance, it was known that in the particular case of curves defined over $\mathbf{F}_p$, the security of CSIDH reduces to the endomorphism ring problem in subexponential time. Our reductions imply that the security of CSIDH is actually equivalent to the endomorphism ring problem, under polynomial time reductions (circumventing arguments that proved such reductions unlikely).

1 Introduction

We study two families of computational problems at the heart of isogeny-based cryptography, and how they relate to each other: computing the endomorphism ring of supersingular elliptic curves, and inverting the action of class groups on oriented supersingular curves. On one hand, the problem of computing endomorphism rings is of foundational importance to the field: its presumed hardness is necessary [GPST16,CPV20,FKM21] (and sometimes sufficient [CLG09,GPS20]) for the security of essentially all isogeny-based cryptosystems. On the other hand, the action of *ideal class groups* on sets of elliptic curves induces presumably hard inversion problems. This action, and the presumed hardness of its inversion, is the fertile ground upon which many cryptosystems have been built — from the early work of Couveignes [Cou06], to CSIDH [CLM+18] and its many variants [CD20,BKV19,CS21]. Thanks to the notion of *orientation* introduced by

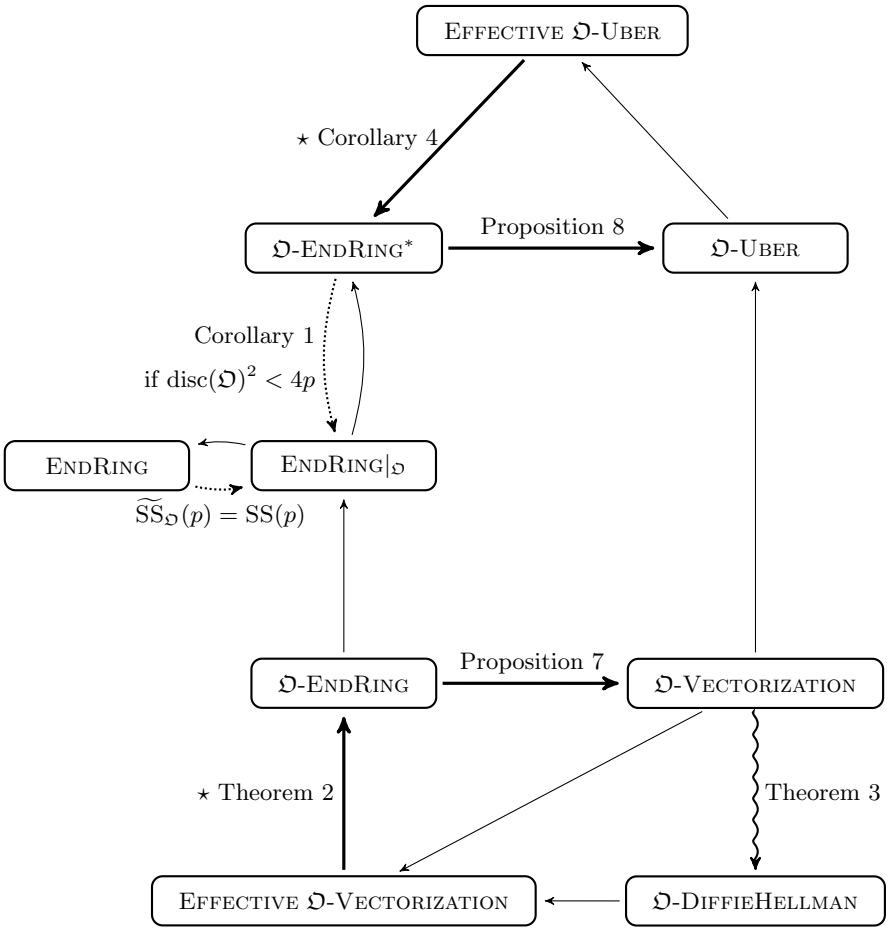

Fig. 1. Arrows represent probabilistic polynomial time reductions in $\log p$ and $\log(\mathrm{disc}(\mathfrak{O}))$, and for those marked by a star $\star$, in $\#(\mathrm{Cl}(\mathfrak{O})[2])$, the size of the 2-torsion of the class group. Arrows with no reference (thin or dotted) are trivial reductions. Thick arrows assume that the factorisation of $\mathrm{disc}(\mathfrak{O})$ is known. Dotted arrows assume the stated condition. The "snake" arrow is a quantum reduction. $\mathrm{SS}(p)$ is the set of all supersingular elliptic curves over $\mathbf{F}_{p^2}$ (up to isomorphism), and $\widetilde{\mathrm{SS}}_{\mathfrak{O}}(p)$ is the subset of $\mathfrak{O}$-orientable curves. Non-trivial reductions assume the generalised Riemann hypothesis.

Colò and Kohel [CK20], it has recently become clear that such actions play a ubiquitous role, even in cryptosystems where they were not expected, such as SIDH [JD11] and its variants (see [DDF+21]).

1.1 Oriented endomorphism ring problems

Isogenies are strongly structured morphisms between elliptic curves, and endomorphisms of an elliptic curve E are isogenies from E to itself. They form a ring, written $\mathrm{End}(E)$. Given a supersingular elliptic curve E over $\overline{\mathbf{F}}_p$, the endomorphism ring problem EndRing consists in computing a basis of $\mathrm{End}(E)$. This EndRing problem was proved in [Wes22] (and heuristically since [EHL+18]) to be equivalent to the problem of finding isogenies between supersingular elliptic curves, assuming the generalised Riemann hypothesis. Let $\mathfrak{O}$ be an order in a quadratic number field K. An orientation is an embedding

$$\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$$

which cannot be extended to a superorder of $\mathfrak{O}$. We call (E, ι) an $\mathfrak{O}$-oriented elliptic curve, and E is $\mathfrak{O}$-orientable. We introduce three *oriented* variants of the endomorphism ring problem, in increasing order of hardness (precise definitions are provided in Section 4):

- $\mathfrak{O}$-EndRing: given an $\mathfrak{O}$-oriented elliptic curve (E, ι), compute a basis of $\mathrm{End}(E)$. It is presumably easier than EndRing since ι provides additional information.
- EndRing$|_{\mathfrak{O}}$: given an $\mathfrak{O}$-orientable elliptic curve E, compute a basis of $\mathrm{End}(E)$. It is simply the restriction of EndRing to $\mathfrak{O}$-orientable inputs.
- $\mathfrak{O}$-EndRing*: given an $\mathfrak{O}$-orientable E, compute a basis of $\mathrm{End}(E)$ together with an $\mathfrak{O}$-orientation expressed in this basis.

1.2 Class group action problems

A key feature of $\mathfrak{O}$-orientations is that they induce a group action. Given an $\mathfrak{O}$-oriented (E, ι), and an invertible $\mathfrak{O}$-ideal $\mathfrak{a}$, one can construct another $\mathfrak{O}$-oriented elliptic curve $\mathfrak{a} \star (E, \iota) = (E^{\mathfrak{a}}, \iota^{\mathfrak{a}})$, and an isogeny $\varphi_{\mathfrak{a}} : E \to E^{\mathfrak{a}}$ connecting them. This construction induces a free action of the ideal class group $\mathrm{Cl}(\mathfrak{O})$ on $\mathfrak{O}$-oriented curves up to isomorphism. We define four variants of the problem of inverting this group action (precise definitions are provided in Section 3):

- $\mathfrak{O}$-Vectorization: given two $\mathfrak{O}$-oriented elliptic curves (E, ι) and (E', ι'), find an ideal $\mathfrak{a}$ such that E' is isomorphic to $E^{\mathfrak{a}}$. The *effective* variant asks for the isomorphism to preserve the orientation, and also requires a way to evaluate the action of $\mathfrak{a}$ on any other $\mathfrak{O}$-oriented curve. The *vectorization* terminology comes from Couveignes' work [Cou06]. The security of many cryptosystems reduces to this problem, such as CSIDH [CLM+18], CSI-FiSh [BKV19], CSURF [CD20], or generalisations to other orientations [CS21].
- $\mathfrak{O}$-Uber: given an $\mathfrak{O}$-oriented elliptic curve (E, ι) and an $\mathfrak{O}$-orientable E', find an ideal $\mathfrak{a}$ such that E' is isomorphic to $E^{\mathfrak{a}}$. The *effective* variant also requires a way to evaluate the action of $\mathfrak{a}$ on any other $\mathfrak{O}$-oriented curve. This *Uber* terminology was introduced in [DDF+21], where it was shown that the security of many cryptosystems reduces to this problem, including SIDH [JD11], OSIDH [CK20] and Séta [DDF+21].

1.3 Contribution

The main contribution of this article is the various reductions summarised in Figure 1, under the generalised Riemann hypothesis. Some of these reductions generalise and strengthen previously known results:

- The article [CPV20] was the first to investigate the relation between EndRing and the vectorisation problem, in the particular case of curves defined over $\mathbf{F}_p$ (i.e., $\sqrt{-p} \in \mathfrak{O}$). They prove that knowledge of the endomorphism ring of a CSIDH public key allows one to recover the ideal class of the secret key. This surprising result, however, only implies a subexponential reduction from breaking CSIDH to computing endomorphism rings, because it is not easy to find a *good* ideal class representative of the key. In essence, they prove a reduction from the vectorisation problem, but not from its effective variant. They argue that this effectiveness seems hard to reach, because if an efficient reduction could find good class representatives, then there would be an efficient algorithm to compute discrete logarithms in class groups of large discriminant. We circumvent this issue, proving in Section 6 that the effective vectorisation problem (hence breaking CSIDH) does reduce to the endomorphism ring problem in polynomial time. Our reductions not only apply to CSIDH or close variants restricted to $\mathbf{F}_p$, but to arbitrary orientations, including generalisations such as [CS21]. To reach this level of generality, we introduce the notion of $\mathfrak{O}$-twists and prove that they enjoy similar properties to quadratic twists, and can be used to extend some of the techniques introduced in [CPV20].
- Considering vectorisation as a group-action analog of the discrete logarithm problem, there is a corresponding Diffie–Hellman analog, $\mathfrak{O}$-DiffieHellman (sometimes called *parallelisation*). Properly instantiated, it corresponds to the problem of recovering the shared secret in CSIDH. In [GPSV21], it was proved that if the action of $\mathrm{Cl}(\mathfrak{O})$ is efficiently computable, then the (non-effective) $\mathfrak{O}$-Vectorization problem reduces to $\mathfrak{O}$-DiffieHellman in quantum polynomial time. This result hit a similar wall as [CPV20]: the action is only efficiently computable for hard-to-find good ideal class representatives. Here again, our reductions bypass this obstacle, proving in Section 7 that $\mathfrak{O}$-DiffieHellman is actually equivalent to $\mathfrak{O}$-Vectorization (and to its effective variant, and to $\mathfrak{O}$-EndRing) under quantum polynomial time reductions.

Finally, we focus in Section 8 on the case where $\mathfrak{O}$ is a non-maximal order, proving reductions from our problems of interest to their *a priori* easier counterpart for superorders (with smaller discriminants and class groups).

1.4 Notation

We denote by $\mathbf{Z}$ and $\mathbf{Q}$ the ring of integers and the field of rational numbers. For any prime power q, we denote by $\mathbf{F}_q$ the finite field with q elements, and $\overline{\mathbf{F}}_q$ its algebraic closure. We write $f = O(g)$ for the classic big O notation, which is

equivalent to $g = \Omega(f)$. The size of a set S is denoted by $\#S$. Let a and b be two integers. We write $a \mid b$ if a divides b, and $a \mid\mid b$ if $a \mid b$ and $\gcd(a, b/a) = 1$. All statements containing the mention (GRH) assume the generalised Riemann hypothesis.

2 Preliminaries

In this section, we recall relevant notions related to quaternion algebras, supersingular elliptic curves, their endomorphism rings, and orientations.

2.1 Quaternion algebras

To any prime number p, one can associate a quaternion algebra $B_{p,\infty}$ defined as

$$B_{p,\infty} = \mathbf{Q} + \mathbf{Q}\, i + \mathbf{Q}\, j + \mathbf{Q}\, ij,$$

with the multiplication rules $i^2 = -q$, $j^2 = -p$ and $ji = -ij$, where q is a positive integer that depends on p. More precisely, the latter is given by

$$q = \begin{cases} 1 & \text{if } p \equiv 3 \bmod 4, \\ 2 & \text{if } p \equiv 5 \bmod 8, \\ q_p & \text{if } p \equiv 1 \bmod 8, \end{cases}$$

where q_p is the smallest prime such that $q_p \equiv 3 \bmod 4$ and $\left(\frac{p}{q_p}\right) = -1$ (see [Piz80]). Assuming GRH, it follows from [LO77] that $q_p = O((\log p)^2)$, which can thus be computed in polynomial time in $\log p$. For the general theory of quaternion algebras, we refer the reader to [Vig06] or [Voi21].

Conjugation, trace and norm. Let $\alpha = x_1 + x_2 i + x_3 j + x_4 ij$ be a generic element in $B_{p,\infty}$. The algebra $B_{p,\infty}$ has a canonical involution $\alpha \mapsto \overline{\alpha} = x_1 - x_2 i - x_3 j - x_4 ij$. It induces the *reduced trace* and the *reduced norm*

$$\mathrm{Trd}(\alpha) = \alpha + \overline{\alpha} = 2x_1, \quad \mathrm{Nrd}(\alpha) = \alpha\overline{\alpha} = x_1^2 + qx_2^2 + p(x_3^2 + qx_4^2).$$

The latter is a positive definite quadratic map, which makes $B_{p,\infty}$ a quadratic space, and endows its finitely generated $\mathbf{Z}$-submodules with a lattice structure.

Maximal orders. An *order* in $B_{p,\infty}$ is a full-rank lattice that is also a subring. It is *maximal* if it is not contained in any other order.

For any lattice $\Lambda \subset B_{p,\infty}$, the *left order* and the *right order of* Λ are

$$\mathcal{O}_L(\Lambda) = \{\alpha \in B_{p,\infty} \mid \alpha\Lambda \subseteq \Lambda\}, \quad \text{and } \mathcal{O}_R(\Lambda) = \{\alpha \in B_{p,\infty} \mid \Lambda\alpha \subseteq \Lambda\}.$$

If $\mathcal{O}$ is a maximal order, and I is a left ideal in $\mathcal{O}$, then $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I)$ is another maximal order. Given two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$, their *connecting ideal* is the ideal

$$I(\mathcal{O}_1, \mathcal{O}_2) = \{\alpha \in B_{p,\infty} \mid \alpha\mathcal{O}_2\overline{\alpha} \subseteq [\mathcal{O}_2 : \mathcal{O}_1 \cap \mathcal{O}_2]\mathcal{O}_1\},$$

which satisfies $\mathcal{O}_L(I(\mathcal{O}_1, \mathcal{O}_2)) = \mathcal{O}_1$ and $\mathcal{O}_R(I(\mathcal{O}_1, \mathcal{O}_2)) = \mathcal{O}_2$. Let $\mathcal{O}$ be a maximal order. Two left $\mathcal{O}$-ideals I and J are *equivalent* if there exists $\alpha \in B_{p,\infty}$ such that $I = \alpha J$. If I and J are equivalent, then $\mathcal{O}_R(I) \cong \mathcal{O}_R(J)$.

2.2 Elliptic curves

Recall that an elliptic curve is an abelian variety of dimension 1, isogenies are non-trivial morphisms between them, and endomorphisms are isogenies from a curve to itself. For a detailed reference on elliptic curves, we refer the reader to [Sil86].

Isogenies and endomorphisms. The set of all isogenies from E to E' (over the algebraic closure of the field of definition), together with the trivial map of kernel E, is written $\mathrm{Hom}(E, E')$. It forms a $\mathbf{Z}$-module for point-wise addition $+$. The *endomorphism ring* $\mathrm{End}(E)$ of an elliptic curve E is the $\mathbf{Z}$-module $\mathrm{Hom}(E, E)$ together with the composition of maps $\circ$. We have an embedding $\mathbf{Z} \hookrightarrow \mathrm{End}(E) : m \mapsto [m]$, where $[m]$ is the multiplication-by-m map. The *degree* $\deg(\varphi)$ of an isogeny $\varphi : E \mapsto E'$ is the smallest positive element in $\mathbf{Z} \cap (\mathrm{Hom}(E', E) \circ \varphi)$. There is a unique isogeny $\hat{\varphi}$ such that $\hat{\varphi} \circ \varphi = [\deg(\varphi)]$, called the *dual* of φ. The degree is an integral quadratic map; it thereby endows the $\mathbf{Z}$-module $\mathrm{Hom}(E, E')$ with the structure of a lattice, with associated bilinear form

$$\langle \varphi, \psi \rangle = \frac{1}{2}\left(\hat{\varphi} \circ \psi + \hat{\psi} \circ \varphi\right).$$

If $\alpha \in \mathrm{End}(E)$, we write $E[\alpha] = \ker(\alpha)$. We also write $E[m] = \ker([m])$ for $m \in \mathbf{Z}$, and $E[S] = \cap_{\alpha \in S} E[\alpha]$ for $S \subseteq \mathrm{End}(E)$.

Efficient representation of isogenies. There are many ways to computationally represent isogenies. Rather that imposing a particular encoding, let us specify the required properties. As in [Wes22], we say that an isogeny $\varphi : E \to E'$ is given in an *efficient representation* if there is an algorithm to evaluate $\varphi(P)$ for any $P \in E(\mathbf{F}_{p^k})$ in time polynomial in the length of the representation of φ and in $k \log(p)$. We also assume that an efficient representation of φ has length $\Omega(\log(\deg(\varphi)))$. With these properties, the quadratic structure of $\mathrm{Hom}(E, E')$ is computationally available, thanks to the following lemma.

Lemma 1. *Given $\varphi, \psi \in \mathrm{Hom}(E, E')$ in efficient representation, one can compute $\langle \varphi, \psi \rangle$ in time polynomial in the length of the representation of φ and ψ, and in $\log p$.*

Proof. This is a straightforward generalisation of [EHL+18, Lemma 4]. □

Supersingular curves. Fix a prime number p. If E is an elliptic curve defined over $\overline{\mathbf{F}}_p$, it is supersingular if and only if its endomorphism ring $\mathrm{End}(E)$ is isomorphic to a maximal order in the quaternion algebra $B_{p,\infty}$ (hence $B_{p,\infty} \cong \mathrm{End}(E) \otimes \mathbf{Q}$). Up to $\overline{\mathbf{F}}_p$-isomorphism, all supersingular elliptic curves over $\overline{\mathbf{F}}_p$ are defined over $\mathbf{F}_{p^2}$, and there are $\lfloor p/12 \rfloor + \varepsilon$ of them, with $\varepsilon \in \{0, 1, 2\}$.

2.3 Orientations

Let K be a quadratic number field, with ring of integers $\mathfrak{O}_K$, and let $\mathfrak{O}$ be an arbitrary order in K.

Definition 1 (Orientation). *A* K-orientation *on an elliptic curve E is an embedding $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbf{Q}$. It is an* $\mathfrak{O}$-orientation *if $\iota(\mathfrak{O}) = \iota(K) \cap \mathrm{End}(E)$. Such a pair (E, ι) is called an* $\mathfrak{O}$-orientated *elliptic curve, and we say that E is* $\mathfrak{O}$-orientable*.*

Note that $\mathfrak{O}$-orientions as defined above correspond to the *primitive* $\mathfrak{O}$-orientions of [CK20]. If (E, ι) is an $\mathfrak{O}$-orientated elliptic curve, we will often consider ι as an embedding of $\mathfrak{O}$ into $\mathrm{End}(E)$ (which naturally extends to an embedding of K into $\mathrm{End}(E) \otimes \mathbf{Q}$). This relates to the notion of primitive embedding.

Definition 2. *Given two lattices Λ_1 and Λ_2, an embedding $\jmath : \Lambda_1 \hookrightarrow \Lambda_2$ is* primitive *if the group $\Lambda_2/\jmath(\Lambda_1)$ is torsion-free.*

Then, one can equivalently define the notion of $\mathfrak{O}$-orientation as a primitive embedding $\iota : \mathfrak{O} \hookrightarrow \mathrm{End}(E)$.

Given a K-orientated elliptic curve (E, ι), any isogeny $\varphi : E \to E'$ induces a K-orientation $\varphi_*(\iota)$ on E' defined as

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

Definition 3 (Oriented isogeny). *Given two K-oriented elliptic curves (E, ι) and (E', ι'), an isogeny $\varphi : (E, \iota) \to (E', \iota')$ is* K-oriented *if $\iota' = \varphi_*(\iota)$. If $\deg(\varphi)$ is prime, ι is an $\mathfrak{O}$-orientation and ι' an $\mathfrak{O}'$-orientation, then the isogeny is* horizontal *when $\mathfrak{O} = \mathfrak{O}'$,* ascending *when $\mathfrak{O} \subsetneq \mathfrak{O}'$, and* descending *when $\mathfrak{O} \supsetneq \mathfrak{O}'$. We say that an isogeny of composite degree is horizontal, ascending or descending if it factors as prime degree isogenies all of that type.*

We write $\mathrm{SS}_{\mathfrak{O}}(p)$ the set of $\mathfrak{O}$-oriented supersingular elliptic curves over $\overline{\mathbf{F}}_p$ up to K-oriented isomorphism.

Proposition 1 ([Onu21, Proposition 3.2]). *The set $\mathrm{SS}_{\mathfrak{O}}(p)$ is not empty if and only if p does not split in K and does not divide the conductor of $\mathfrak{O}$.*

Throughout, we suppose that p does not split in K and does not divide the conductor of $\mathfrak{O}$.

Encoding orientations. Computationally, an orientation is encoded by a generator ω of $\mathfrak{O}$ together with an efficient representation of the endomorphism $\iota(\omega)$.

3 Class groups acting on sets of elliptic curves

Fix an oriented curve $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$. An $\mathfrak{O}$-ideal $\mathfrak{a}$ induces a subgroup $E[\mathfrak{a}] = \cap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha))$, and an isogeny $\varphi_{\mathfrak{a}} : E \to E^{\mathfrak{a}}$ called the $\mathfrak{a}$-multiplication. The target $E^{\mathfrak{a}}$ is the $\mathfrak{a}$-transform of (E, ι). This construction induces an action of $\mathfrak{O}$-ideals on the set $\mathrm{SS}_{\mathfrak{O}}(p)$, defined by

$$\mathfrak{a} \star (E, \iota) = (E^{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota)),$$

which factors through $\mathrm{Cl}(\mathfrak{O})$. This action, well understood for ordinary elliptic curves with complex multiplication, was first studied in the context of oriented supersingular curves in [CK20] and [Onu21].

Theorem 1 ([Onu21]). *The action*

$$\mathrm{Cl}(\mathfrak{O}) \times \mathrm{SS}_{\mathfrak{O}}(p) \longrightarrow \mathrm{SS}_{\mathfrak{O}}(p) : (\mathfrak{a}, (E, \iota)) \longmapsto \mathfrak{a} \star (E, \iota)$$

is free and has at most two orbits. For any orbit A, and any $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, either $(E, \iota) \in A$, or both $(E, \bar{\iota})$ and $(E^{(p)}, \iota^{(p)})$ are in A.

Proof. This theorem combines [Onu21, Proposition 3.3] and [Onu21, Theorem 3.4]. The statement about $(E, \bar{\iota})$ is from the proof of [Onu21, Proposition 3.3]. □

Computing the action. The image $\mathfrak{a} \star (E, \iota)$ can be computed in time polynomial in the length of the encoding of (E, ι), in $\log(N(\mathfrak{a}))$ and in the largest prime-power factor of $N(\mathfrak{a})$. This is done by evaluating the action of $\iota(\mathfrak{a})$ on $E[N(\mathfrak{a})]$ to deduce $E[\mathfrak{a}]$, as in [CK20]. Evaluating the induced orientation $(\varphi_{\mathfrak{a}})_*(\iota)$ requires a division by $\deg(\varphi)$, which can be done in time polynomial in B if $N(\mathfrak{a})$ is B-powersmooth (meaning that all its prime-power factors are smaller than B). Yet, it should be noted that the efficiency of this representation degrades after applying the action of several such ideals, say n, because their product may only be B^n-powersmooth. This will not be an issue when only a constant number of actions are applied in this way (as in our forthcoming reductions), or when the endomorphism ring of the curves are known (in which case an efficient representation of the orientation can be recomputed, that does not depend on the ideal).

3.1 Computational problems

We now define two problems that translate whether or not the action is *one-way*.

Problem 1 ($\mathfrak{O}$-Vectorization*).* Given $(E, \iota), (E', \iota') \in \mathrm{SS}_{\mathfrak{O}}(p)$, find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $E' \cong E^{\mathfrak{a}}$.

Per Theorem 1, a solution $\mathfrak{a}$ of $\mathfrak{O}$-VECTORIZATION always exists since the isomorphism $E' \cong E^{\mathfrak{a}}$ does not care about the orientation. The *vectorization* terminology comes from Couveignes' work [Cou06], even though proper use of this terminology should require $(E', \iota') \cong \mathfrak{a} \star (E, \iota)$. We will see that this modification makes little difference, as $\mathfrak{O}$-VECTORIZATION will turn out to be equivalent to the following stronger problem.

*Problem 2 (*EFFECTIVE $\mathfrak{O}$-VECTORIZATION*).* Given three $\mathfrak{O}$-oriented supersingular curves $(E, \iota), (E', \iota'), (F, \jmath) \in \mathrm{SS}_{\mathfrak{O}}(p)$, find an $\mathfrak{O}$-ideal $\mathfrak{a}$ (or decide that it does not exist) such that $(E', \iota') \cong \mathfrak{a} \star (E, \iota)$, and an efficient representation of $\varphi_{\mathfrak{a}} : (F, \jmath) \to \mathfrak{a} \star (F, \jmath)$.

Now, a solution to EFFECTIVE $\mathfrak{O}$-VECTORIZATION does not necessarily exist, since (E, ι) and (E', ι') could be in the two distincts orbits described in Theorem 1. At first glance, the EFFECTIVE $\mathfrak{O}$-VECTORIZATION problem seems harder than $\mathfrak{O}$-VECTORIZATION for two reasons. First, an arbitrary ideal $\mathfrak{a}$ is unlikely to induce an efficient representation of $\varphi_{\mathfrak{a}}$. This has already proved to be a serious obstacle in the litterature [CPV20,GPSV21], where given an ideal class, heavy work goes into finding a *good* representative by a *smoothing* step which we do not know how to solve in polynomial time. Second, an isomorphism $E' \cong E^{\mathfrak{a}}$ does not imply that $(E', \iota') \cong \mathfrak{a} \star (E, \iota)$, and the information lost may be substantial as $h(\mathfrak{O})$ can be arbitrarily large while there are only approximately $p/12$ supersingular curves up to isomorphism. Despite these obstacles, we will show that these two problems are equivalent, by showing they are both equivalent to an oriented version of the endomorphism ring problem.

These two vectorisation problems are closely related to the following analog of the Diffie-Hellman problem.

Problem 3 ($\mathfrak{O}$-DIFFIEHELLMAN*).* Given an oriented curve $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, and its images $\mathfrak{a} \star (E, \iota)$ and $\mathfrak{b} \star (E, \iota)$ for the action of two unknown ideals $\mathfrak{a}$ and $\mathfrak{b}$, compute $\mathfrak{ab} \star (E, \iota)$.

In Couveignes' terminology, this is the *parallelisation* problem. It is clear that both problems $\mathfrak{O}$-VECTORIZATION and $\mathfrak{O}$-DIFFIEHELLMAN reduce to the EFFECTIVE $\mathfrak{O}$-VECTORIZATION problem, and the converse reductions are the object of Sections 5, 6 and 7.

Now, one may consider the same problems when no orientation ι' for E' is provided. This modification seems to make the problems much harder, and this presumed hardness (for large $\mathrm{disc}(\mathfrak{O})$) has been introduced in [DDF+21] as the *Uber isogeny assumption*.

Problem 4 ($\mathfrak{O}$-UBER*).* Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an $\mathfrak{O}$-orientable elliptic curve E', find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $E' \cong E^{\mathfrak{a}}$.

The original Uber isogeny assumption from [DDF+21] also asks for an effective way to apply the action of $\mathfrak{a}$, as in the following effective variant.

*Problem 5 (*Effective $\mathfrak{O}$-Uber*).* Given two $\mathfrak{O}$-oriented curves $(E, \iota), (F, \jmath) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an $\mathfrak{O}$-orientable curve E', find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $E' \cong E^{\mathfrak{a}}$, and an efficient representation of $\varphi_{\mathfrak{a}} : (F, \jmath) \to \mathfrak{a} \star (F, \jmath)$.

The main interest for these *Uber* problems is that the security of most isogeny based cryptosystems reduce to them [DDF+21, Section 5], even systems such as SIDH [JD11] for which no class group action is immediately visible.

3.2 Some known or simple algorithms

Let us briefly present algorithms to solve some of the problems introduced above.

Proposition 2. *The* Effective $\mathfrak{O}$-Uber *problem can heuristically be solved in expected time* $(\log p)^{O(1)} \operatorname{disc}(\mathfrak{O})$.

Proof. This is the running time of an exhaustive search restricted to powersmooth ideals, as discussed in [DDF+21, Section 5.3]. □

Proposition 3. *The* Effective $\mathfrak{O}$-Vectorization *problem can heuristically be solved in expected time* $(\log p)^{O(1)} \operatorname{disc}(\mathfrak{O})^{1/2}$.

Proof. This is the running time of the meet-in-the-middle approach, as described for instance in [DG16,CLM+18], but using only powersmooth walks. □

In the following, we use the classic notation

$$L_x(\alpha) = \exp\left(O\left((\log x)^{\alpha}(\log\log x)^{1-\alpha}\right)\right)$$

for subexponential complexities.

Proposition 4. *The* Effective $\mathfrak{O}$-Vectorization *problem can heuristically be solved in quantum subexponential time* $(\log p)^{O(1)} L_{\operatorname{disc}(\mathfrak{O})}(1/2)$.

Proof. The $\mathfrak{O}$-Vectorization problem reduces to the hidden shift problem with respect to the functions $f, f' : \mathrm{Cl}(\mathfrak{O}) \to \mathbf{F}_{p^2}$ defined by $f([\mathfrak{a}]) = j(\mathfrak{a} \star (E, \iota))$ and $f'([\mathfrak{a}]) = j(\mathfrak{a} \star (E', \iota'))$. It only remains to prove that the action can be evaluated in quantum subexponential time, then apply Kuperberg's algorithm [Kup05]. It is tempting to simply adapt the method of [CJS14], but they find smooth class representatives, when we need powersmooth class representatives. We take a cruder, simpler, but heuristic route. One can randomize the class representative of $[\mathfrak{a}]$, until it has a powersmooth norm. The number of $L_x(1/2)$-powersmooth numbers at most x is $L_x(1/2)$ (see [CN00, Section 3.1]), so under the heuristic assumption that norms of random class representatives behave like random integers of the same size, we may find an $L_d(1/2)$-powersmooth representative in time $L_d(1/2)$, with $d = \operatorname{disc}(\mathfrak{O})$. Its action can then be evaluated in time $L_d(1/2)$. □

4 Oriented versions of the endomorphism ring problem

4.1 The endomorphism ring problem

To define the endomorphism ring problem in its strongest form, we introduce the notion of ε-basis, thereby unifying the two variants EndRing and MaxOrder proved to be equivalent under the generalised Riemann hypothesis in [Wes22] (and heuristically since [EHL+18]).

Definition 4 (ε-basis). *Let $\varepsilon : B_{p,\infty} \to \mathrm{End}(E) \otimes \mathbf{Q}$ be an isomorphism. Given a lattice $L \subseteq B_{p,\infty}$, an ε-basis of L is a pair (α, θ) where $(\alpha_i)_{i=1}^{\mathrm{rank}(L)}$ is a basis of L and $\theta_i = \varepsilon(\alpha_i)$. Abusing language, we also call (α, θ) an ε-basis of the image lattice $\varepsilon(L)$.*

Remark 1. We will often talk about an ε-basis without specifying a priori an isomorphism ε. The ε is then implicit, and when L has full rank, it is uniquely determined by the ε-basis.

Encoding. Computationally, we suppose that elements in $B_{p,\infty}$ are encoded as vectors of rational numbers with respect to the basis $(1, i, j, ij)$. We assume that elements $\eta \otimes n^{-1}$ of $\mathrm{End}(E) \otimes \mathbf{Q}$ are encoded as pairs (η, n) where n is an integer and η is an endomorphism in efficient representation.

The endomorphism ring problem can be defined as either finding a basis of a maximal order $\mathcal{O}$ of $B_{p,\infty}$ isomorphic to $\mathrm{End}(E)$, or finding four endomorphisms that generate $\mathrm{End}(E)$. It was proved in [Wes22] that a basis of either $\mathcal{O}$ or $\mathrm{End}(E)$ can be transformed into an ε-basis of $\mathrm{End}(E)$, assuming GRH. We therefore define the endomorphism ring problem as follows.

*Problem 6 (*EndRing*).* Given a supersingular elliptic curve E over $\mathbf{F}_{p^2}$, find an ε-basis of $\mathrm{End}(E)$.

Proposition 5. *The* EndRing *problem can heuristically be solved in expected time $(\log p)^{O(1)} p^{1/2}$.*

Proof. This is the running time of the best known algorithms for EndRing, for instance [DG16] and [EHL+20]. □

4.2 Oriented variants of the endomorphism ring problem

The EndRing problem can naturally be restricted to $\mathfrak{O}$-orientable curves, resulting in the following problem.

*Problem 7 (*EndRing$|_{\mathfrak{O}}$*).* Given an $\mathfrak{O}$-orientable E, find an ε-basis of $\mathrm{End}(E)$.

Now, if an orientation is provided, we obtain the following variant.

*Problem 8 ($\mathfrak{O}$-*EndRing*).* Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, find an ε-basis of $\mathrm{End}(E)$.

One could require solutions to $\mathfrak{O}$-EndRing to be in some way compatible with the orientation. It is unnecessary: as formalised in the following lemma, it is actually easy to express a given orientation in terms of a given ε-basis.

Lemma 2. *Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an ε-basis of $\mathrm{End}(E)$, one can find an embedding $\jmath : \mathfrak{O} \hookrightarrow B_{p,\infty}$ such that $\varepsilon \circ \jmath = \iota$ in time polynomial in the length of the input.*

Proof. We can compute scalar products between endomorphisms with Lemma 1, so we can express the ι-basis in terms of the ε-basis. □

Finally, we consider the seemingly harder problem of computing the endomorphism ring *and* an orientation.

Problem 9 ($\mathfrak{O}$-EndRing*). Given a supersingular $\mathfrak{O}$-orientable curve E, find an ε-basis of $\mathrm{End}(E)$ and an embedding $\jmath : \mathfrak{O} \hookrightarrow B_{p,\infty}$ such that $\varepsilon \circ \jmath$ is an $\mathfrak{O}$-orientation.

Clearly, $\mathfrak{O}$-EndRing reduced to EndRing$|_{\mathfrak{O}}$, which reduces to $\mathfrak{O}$-EndRing*.

4.3 Computing an orientation from the endomorphism ring

While EndRing$|_{\mathfrak{O}}$ reduces to $\mathfrak{O}$-EndRing*, the converse boils down to the following question.

Question 1. Given an $\mathfrak{O}$-orientable curve E and an ε-basis of its endomorphism ring, can one compute an $\mathfrak{O}$-orientation of E in probabilistic polynomial time in $\log(p)$ and $\log(\mathrm{disc}(\mathfrak{O}))$?

We only provide a positive answer to this question when the discriminant of the order $\mathfrak{O}$ is small enough, in Proposition 6. The general case may be more difficult.

Proposition 6. *Given an $\mathfrak{O}$-orientable curve E and an ε-basis of its endomorphism ring, if $|\mathrm{disc}(\mathfrak{O})| < 2p^{1/2} - 1$, then one can compute an $\mathfrak{O}$-orientation of E in probabilistic polynomial time in $\log(p)$.*

Proof. Let ι be an $\mathfrak{O}$-orientation of E. Let $d = \mathrm{disc}(\mathfrak{O})$. Let ω be a reduced generator of $\mathfrak{O}$ (of trace either 0 or 1). Then, we have $\mathrm{Nrd}(\omega) \leq (d+1)/4$. For any $\beta \in \mathrm{End}(E)$, we have $|\mathrm{disc}(\mathbf{Z}[\beta])| = 4\,\mathrm{Nrd}(\beta) - \mathrm{Trd}(\beta)^2 \leq 4\,\mathrm{Nrd}(\beta)$. Also, for any $\beta \in \mathrm{End}(E) \setminus \iota(\mathfrak{O})$, it follows from [Kan89, Theorem 2'] that $\mathrm{disc}(\mathfrak{O})\,\mathrm{disc}(\mathbf{Z}[\beta]) \geq 4p$, hence

$$\mathrm{Nrd}(\beta) \geq \frac{p}{d} > \frac{d+1}{4} \geq \mathrm{Nrd}(\omega).$$

This proves that the shortest vector in $\mathrm{End}(E) \setminus \mathbf{Z}$ is a generator of $\iota(\mathfrak{O})$, which can be recovered in polynomial time. Expressing this generator as a linear combination of the ε-basis of $\mathrm{End}(E)$ provides an efficient representation of the orientation ι. □

Proposition 6 has the following immediate consequence.

Corollary 1. *If $|\mathrm{disc}(\mathfrak{O})| < 2p^{1/2} - 1$, then $\mathfrak{O}$-EndRing* and EndRing$|_{\mathfrak{O}}$ are equivalent.*

5 Endomorphism rings from orientations

In this section, we prove reductions from the family of endomorphism ring problems to the family of vectorisation problems. A key ingredient is the constructive Deuring correspondence in the 'order-to-curve' direction, Lemma 3, a result first heuristically proved in [EHL+18, Proposition 13]. Observing that it is easy to produce orders with a primitive embedding of $\mathfrak{O}$, we deduce in Lemma 4 that we can construct $\mathfrak{O}$-oriented elliptic curves of known endomorphism ring, to be used as starting points for vectorisation problems.

Lemma 3 (GRH). *There is an algorithm that given a maximal order $\mathcal{O} \subset B_{p,\infty}$, returns an elliptic curve E such that $\mathrm{End}(E) \cong \mathcal{O}$ together with an ε-basis of $\mathrm{End}(E)$, and runs in time polynomial in $\log(p)$ and the size of the basis of $\mathcal{O}$.*

Proof. From [EHL+18, Proposition 13] (but using [Wes22] instead of [KLPT14] to get rid of the heuristic assumptions), we get an elliptic curve E such that $\mathrm{End}(E) \cong \mathcal{O}$. From [Wes22, Algorithm 6], we deduce an ε-basis of $\mathrm{End}(E)$. □

Definition 5. *Let $\mathcal{O}$ be a maximal order in an algebra $B \cong B_{p,\infty}$, and $\jmath : \mathfrak{O} \hookrightarrow \mathcal{O}$ a primitive embedding. Let I be a left $\mathcal{O}$-ideal of prime norm ℓ, and let $\mathfrak{O}' = \mathcal{O}_R(I) \cap (\jmath(\mathfrak{O}) \otimes \mathbf{Q})$. The ideal I is* $\jmath$-descending *if $\mathfrak{O}' \subsetneq \jmath(\mathfrak{O})$,* $\jmath$-horizontal *if $\mathfrak{O}' = \jmath(\mathfrak{O})$, and* $\jmath$-ascending *if $\mathfrak{O}' \supsetneq \jmath(\mathfrak{O})$.*

Remark 2. It easily follows that an $\mathcal{O}$-oriented isogeny $\varphi : (E, \iota) \to (E, \iota')$ of prime degree is descending (respectively horizontal or ascending) if and only if the kernel ideal $I_\varphi = \{\alpha \in \mathrm{End}(E) | \ker \varphi \subseteq \ker \alpha\}$ is ι-descending (respectively ι-horizontal or ι-ascending). In particular, given $\mathcal{O}$ and $\jmath$, almost all ideals of norm ℓ are $\jmath$-descending, with at most two exceptions. Therefore, a $\jmath$-descending ideal can be found in time polynomial in $\log(\ell)$ by listing three ideals of norm ℓ, and testing them using [Rón92, Theorem 3.2].

Lemma 4 (GRH). *Given $\mathfrak{O}$ and the factorisation of its discriminant, one can find some $\mathfrak{O}$-oriented curve $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ together with an ε-basis of $\mathrm{End}(E)$ in probabilistic polynomial time in $\log(p)$ and $\log(\mathrm{disc}(\mathfrak{O}))$.*

Remark 3. There is a heuristic algorithm [LB20, Algorithm 1] that solves this task in the case where $\mathfrak{O}$ is maximal. Our approach in the proof below is different, assumes only GRH, and avoids potentially hard factorisations.

Proof. We start by computing some arbitrary maximal order $\mathcal{O}_0$ in $B_{p,\infty}$ (for instance, a special order as in [KLPT14, Section 2.3]). Let K be the quadratic field containing $\mathfrak{O}$, with ring of integers $\mathfrak{O}_K$. Let ω_K be a reduced generator of $\mathfrak{O}_K$, with minimal polynomial $x^2 - tx + n$. To find a quaternion $\omega \in B_{p,\infty}$ with the same minimal polynomial, solve

$$(t/2)^2 + qb^2 + p(c^2 + qd^2) = n$$

for $b, c, d \in \mathbf{Q}$ with [Sim06] (using the factorisation of $\mathrm{disc}(\mathfrak{O})$), and let $\omega = t/2 + bi + cj + dij$. Let a be the smallest integer such that $a\omega \in \mathcal{O}_0$. Let $I = \mathcal{O}_0\omega a + \mathcal{O}_0 a$.

We have $I\omega \subseteq I$, so $\omega \in \mathcal{O}_R(I)$, and $\mathcal{O}_R(I)$ can be computed with [Rón92, Theorem 3.2]. The corresponding embedding $\jmath : \mathfrak{O}_K \hookrightarrow \mathcal{O}_R(I) : \omega_K \mapsto \omega$ is primitive since $\mathfrak{O}_K$ is maximal, and it remains to descend to $\mathfrak{O}$. Let c be the conductor of $\mathfrak{O}$. For any prime power $\ell^k \mid\mid c$,

- let $\tilde{J}_\ell$ be any $\jmath$-descending $\mathcal{O}_R(I)$-ideal of norm ℓ (see Remark 2), and
- let $J_\ell \subseteq \tilde{J}_\ell$ an ideal of norm ℓ^k such that $J_\ell \not\subseteq \ell\mathcal{O}_R(I)$.

Each J_ℓ is the kernel ideal of a cyclic isogeny of norm ℓ^k whose first step (hence all steps, because of the volcano structure) is descending. Then, $J = \cap_\ell J_\ell$ is the kernel ideal of a descending isogeny of degree c, hence $\mathfrak{O} \hookrightarrow \mathcal{O}_R(J) : c\omega_K \mapsto c\omega$ is a primitive embedding. So we define $\mathcal{O} = \mathcal{O}_R(J)$. Applying Lemma 3, we can construct E with an ε-basis of $\mathrm{End}(E) \cong \mathcal{O}$. The orientation ι is provided by the induced efficient representation of the endomorphism $\iota(c\omega_K) = \varepsilon(c\omega)$. □

Proposition 7 (GRH). *Given the factorisation of* $\mathrm{disc}(\mathfrak{O})$*, the* $\mathfrak{O}$-EndRing *problem reduces to* $\mathfrak{O}$-Vectorization *in probabilistic polynomial time in* $\log(p)$ *and* $\log(\mathrm{disc}(\mathfrak{O}))$.

Proof. Suppose we are given an instance $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ of $\mathfrak{O}$-EndRing. Find $(E', \iota') \in \mathrm{SS}_{\mathfrak{O}}(p)$ together with an ε-basis of $\mathcal{O}' \cong \mathrm{End}(E')$ using Lemma 4. Solving $\mathfrak{O}$-Vectorization, find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $(E', \iota') = \mathfrak{a}\star(E, \iota)$. Then $I = \mathcal{O}' \cdot \iota'(\mathfrak{a})$, the kernel ideal of $\varphi_{\mathfrak{a}}$, is a connecting ideal between $\mathcal{O}' \cong \mathrm{End}(E')$ and $\mathcal{O}_R(I) \cong \mathrm{End}(E)$. The right-order $\mathcal{O}_R(I)$ can be computed with [Rón92, Theorem 3.2], thereby solving $\mathfrak{O}$-EndRing for (E, ι). □

Proposition 8 (GRH). *Given the factorisation of* $\mathrm{disc}(\mathfrak{O})$*,* $\mathfrak{O}$-EndRing* *reduces to* $\mathfrak{O}$-Uber *in probabilistic polynomial time in* $\log(p)$ *and* $\log(\mathrm{disc}(\mathfrak{O}))$.

Proof. We proceed as in Proposition 7, except that no $\mathfrak{O}$-orientation of E is provided, which still allows us to apply $\mathfrak{O}$-Uber instead of $\mathfrak{O}$-Vectorization. □

6 Reducing vectorisation to endomorphism ring

It is shown in [CPV20] that in the particular case of curves defined over $\mathbf{F}_p$, and $\sqrt{-p} \in \mathfrak{O}$, solving the endomorphism ring problem allows one to solve the $\mathfrak{O}$-Vectorization problem. They note however that in general, the resulting ideal does not necessarily have a smooth norm, so it is hard to compute its action. They conclude that this approach necessitates an expensive smoothing step, hence only provides a sub-exponential reduction of the security of CSIDH to the endomorphism ring problem. A priori, their methods seem very specific to the CSIDH setting, exploiting the action of Frobenius and quadratic twists. Introducing an appropriate generalisation of twisting, we prove in this section that $\mathfrak{O}$-Vectorization reduces to $\mathfrak{O}$-EndRing in all generality. Pushing the results farther, we circumvent the smoothness obstruction by proving polynomial time reductions between these problems and Effective $\mathfrak{O}$-Vectorization,

observing that the action of non-smooth ideals can be efficiently evaluated on elliptic curves of known endomorphism ring. The idea that endomorphisms allow one to evaluate non-smooth isogenies had been observed in [FKM21], and the following proposition extends it to the action of ideals on oriented curves.

Proposition 9 (GRH). *Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, an ε-basis of $\mathrm{End}(E)$, and an $\mathfrak{O}$-ideal $\mathfrak{a}$, one can compute $\mathfrak{a} \star (E, \iota)$ and an efficient representation of $\varphi_{\mathfrak{a}}$ in probabilistic polynomial time in $\log p$, $\log(\mathrm{disc}(\mathfrak{O}))$, $\log(N(\mathfrak{a}))$ and the length of the ε-basis of $\mathrm{End}(E)$.*

Proof. We are given an isomorphism $\varepsilon : \mathcal{O} \to \mathrm{End}(E)$. Let $\jmath : \mathfrak{O} \to \mathcal{O}$ such that $\varepsilon \circ \jmath = \iota$ (see Lemma 2). Let $I = \mathcal{O}\jmath(\mathfrak{a})$, and use [Wes22, Theorem 6.4] to find $\alpha \in I$ such that $J = I\overline{\alpha}/N(\mathfrak{a})$ has powersmooth norm. Then, J is the kernel ideal of an efficiently computable isogeny φ_J (for instance by adapting [GPS20, Lemma 5] to the provided ε-basis instead of the special $\mathcal{O}_0$; alternatively, one can observe that the special $\mathcal{O}_0$ case is sufficient because J is constructed to "pass" through $\mathcal{O}_0$ anyway). We have $\varphi_{\mathfrak{a}} = \varphi_J \circ \varepsilon(\alpha)/[\mathrm{Nrd}(J)]$, so $E^{\mathfrak{a}} = \varphi_J(E)$. It only remains to compute the $\mathfrak{O}$-orientation on $E^{\mathfrak{a}}$, i.e., an efficient representation of $((\varphi_{\mathfrak{a}})_*(\iota))(\omega)$ for some generator ω of $\mathfrak{O}$. We have

$$((\varphi_{\mathfrak{a}})_*(\iota))(\omega) = (\varphi_{\mathfrak{a}} \circ \iota(\omega) \circ \hat{\varphi}_{\mathfrak{a}})/N(\mathfrak{a}) = (\varphi_J \circ \varepsilon(\alpha\jmath(\omega)\overline{\alpha}) \circ \hat{\varphi}_J)/\mathrm{Nrd}(J).$$

One can compute the quaternion $\alpha\jmath(\omega)\overline{\alpha}$, and deduce an efficient representation of the numerator $\gamma = \varphi_J \circ \varepsilon(\alpha\jmath(\omega)\overline{\alpha}) \circ \hat{\varphi}_J$ thanks to the ε-basis. One can evaluate $((\varphi_{\mathfrak{a}})_*(\iota))(\omega)$ at any point P by first finding a point P' such that $\mathrm{Nrd}(J)P' = P$ (in polynomial time because $\mathrm{Nrd}(J)$ is powersmooth), then returning $\gamma(P')$. Therefore we have an efficient representation of the orientation $(\varphi_{\mathfrak{a}})_*(\iota)$. □

6.1 $\mathfrak{O}$-twists, a generalisation of quadratic twists

We now introduce the notion of $\mathfrak{O}$-twists, that enjoys properties similar to quadratic twists.

Definition 6 ($\mathfrak{O}$-twist). *We define the $\mathfrak{O}$-twisting involution as the map $\tau : \mathrm{SS}_{\mathfrak{O}}(p) \to \mathrm{SS}_{\mathfrak{O}}(p)$ defined as $\tau(E, \iota) = (E, \bar{\iota})$, where $\bar{\iota}(\alpha) = \iota(\overline{\alpha})$. The oriented curve $\tau(E, \iota)$ is the $\mathfrak{O}$-twist of (E, ι).*

Lemma 5. *We have $\tau(\mathfrak{a} \star (E, \iota)) = \overline{\mathfrak{a}} \star \tau(E, \iota)$.*

Proof. It follows from the fact that $\cap_{\alpha \in \overline{\mathfrak{a}}} \ker(\iota(\alpha)) = \cap_{\alpha \in \mathfrak{a}} \ker(\bar{\iota}(\alpha))$. □

Recall that sets of isogenies $\mathrm{Hom}(E, E')$ (and in particular $\mathrm{End}(E)$) are lattices. They have a quadratic structure, hence an associated notion of orthogonality. Given $S \subseteq \mathrm{Hom}(E, E')$, we write $S^{\perp} \subseteq \mathrm{Hom}(E, E')$ the set of isogenies orthogonal to all elements of S.

The following lemma can be seen as an analog of [CPV20, Lemma 11].

Lemma 6. *Let $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$. For any non-zero $\theta \in \mathrm{End}(E)$, we have $\theta \in \iota(\mathfrak{O})^{\perp}$ if and only if $\theta_*(\iota) = \bar{\iota}$.*

Proof. First suppose $\theta \in \iota(\mathfrak{O})^\perp$. Since $1 \in \mathfrak{O}$, we have $\theta \in 1^\perp$, i.e., $\theta = -\hat{\theta}$. Then, for any $\alpha \in \mathfrak{O}$, we have $0 = \theta \circ \bar{\iota}(\alpha) + \iota(\alpha) \circ \hat{\theta} = \theta \circ \bar{\iota}(\alpha) - \iota(\alpha) \circ \theta$. We get

$$\theta_*(\iota)(\alpha) = (\theta \circ \iota(\alpha) \circ \hat{\theta}) \otimes \frac{1}{\deg(\theta)} = (\bar{\iota}(\alpha) \circ \theta \circ \hat{\theta}) \otimes \frac{1}{\deg(\theta)} = \bar{\iota}(\alpha),$$

which proves the first implication. For the converse, suppose that $\theta_*(\iota) = \bar{\iota}$. Then, $\theta \circ \iota(\alpha) = \iota(\overline{\alpha}) \circ \theta$ for any $\alpha \in \mathfrak{O}$. Let $\omega \in \mathfrak{O}$ be a non-zero element of trace 0, so $\overline{\omega} = -\omega$. Write $\theta = x + \theta_0$ where $x \in \mathbf{Q}$ and $\hat{\theta}_0 = -\theta_0$. Then,

$$[x] \circ \iota(\omega) + \theta_0 \circ \iota(\omega) = \theta \circ \iota(\omega) = \iota(\overline{\omega}) \circ \theta = -\iota(\omega) \circ \theta = -\iota(\omega) \circ [x] - \iota(\omega) \circ \theta_0,$$

hence $[2x] \circ \iota(\omega) = \mathrm{Trd}(\hat{\theta}_0 \circ \iota(\omega)) \in \mathbf{Q}$, which implies $x = 0$ because $\iota(\omega) \notin \mathbf{Q}$. This proves $\theta = \theta_0$, which is orthogonal to 1. The above also implies that $\theta \circ \iota(\omega) = -\iota(\omega) \circ \theta$, which means that θ is orthogonal to ω, so $\theta \in \iota(\mathfrak{O})^\perp$. □

An issue with $\mathfrak{O}$-twisting is that it might not preserve $\mathrm{Cl}(\mathfrak{O})$-orbits. We introduce the following involution to resolve this.

Definition 7. *We define the involution $\tau_p : \mathrm{SS}_{\mathfrak{O}}(p) \to \mathrm{SS}_{\mathfrak{O}}(p)$ as $\tau_p(E, \iota) = (E, \bar{\iota})^{(p)}$, with $(E, \bar{\iota})^{(p)} = (E^{(p)}, (\phi_p)_*(\bar{\iota}))$ where $\phi_p : E \to E^{(p)}$ is the Frobenius isogeny.*

Proposition 10. *There exists an ideal $\mathfrak{a}$ such that $\tau_p(E, \iota) = \mathfrak{a} \star (E, \iota)$.*

Proof. The only troublesome case is if $\mathrm{SS}_{\mathfrak{O}}(p)$ partitions into two $\mathrm{Cl}(\mathfrak{O})$-orbits A and B. In that case, both τ and the Frobenius involution interchange A and B (Theorem 1). It follows that τ_p stabilizes A and B. □

It still enjoys some of the useful properties of $\mathfrak{O}$-twisting.

Lemma 7. *We have $\tau_p(\mathfrak{a} \star (E, \iota)) = \overline{\mathfrak{a}} \star \tau_p(E, \iota)$.*

Proof. It follows from Lemma 5 and the fact that $\mathfrak{a} \star (E, \iota)^{(p)} = (\mathfrak{a} \star (E, \iota))^{(p)}$. □

Corollary 2. *An isogeny $\varphi : (E, \iota) \to \tau_p(E, \iota)$ is K-oriented if and only if $\varphi \in (\phi_p \circ \iota(\mathfrak{O}))^\perp$, where $\phi_p : E \to E^{(p)}$ is the Frobenius isogeny.*

Proof. By the definition of τ_p, the isogeny φ is K-oriented if and only if $\varphi_*(\iota) = (\phi_p)_*(\bar{\iota})$. The latter is equivalent to $(\hat{\phi}_p)_*(\varphi_*(\iota)) = (\hat{\phi}_p)_*((\phi_p)_*(\bar{\iota}))$. Since

$$(\hat{\phi}_p)_*(\varphi_*(\iota)) = (\hat{\phi}_p \circ \varphi)_*(\iota), \text{ and } (\hat{\phi}_p)_*((\phi_p)_*(\bar{\iota})) = [p]_*(\bar{\iota}) = \bar{\iota},$$

we deduce that $(\hat{\phi}_p \circ \varphi)_*(\iota) = \bar{\iota}$. From Lemma 6, this is equivalent to $\hat{\phi}_p \circ \varphi \in \iota(\mathfrak{O})^\perp$, i.e., $\varphi \in \phi_p \circ (\iota(\mathfrak{O}))^\perp = (\phi_p \circ \iota(\mathfrak{O}))^\perp$. □

Corollary 3. *The integral lattice $(\phi_p \circ \iota(\mathfrak{O}))^\perp \subset \mathrm{Hom}(E, E^{(p)})$ is primitive (i.e., the greatest common divisor of the integers represented by the associated integral quadratic form is 1).*

Proof. There exist two coprime ideals $\mathfrak{a}$ and $\mathfrak{b}$ such that $\tau_p(E, \iota) = \mathfrak{a} \star (E, \iota) = \mathfrak{b} \star (E, \iota)$. We deduce from Corollary 2 that there are two lattice vectors $\varphi_{\mathfrak{a}}, \varphi_{\mathfrak{b}} \in (\phi_p \circ \iota(\mathfrak{O}))^\perp \subset \mathrm{Hom}(E, E^{(p)})$ of coprime norm. □

6.2 Vectorisation problems from endomorphism rings

We now prove that vectorisation problems reduce to endomorphism ring problems, with a strategy similar to that of [CPV20].

Lemma 8. *Let $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, a non-zero $\mathfrak{O}$-ideal $\mathfrak{a}$, and a left $\mathrm{End}(E)$-ideal I such that $E[\mathfrak{a}] = E[I]$. Then, $I \cap \iota(\mathfrak{O}) = \iota(\mathfrak{p}^k\mathfrak{a})$ for some $k \in \mathbf{Z}$, where $\mathfrak{p}$ is the prime ideal above p.*

Proof. This lemma is a generalisation of [CPV20, Lemma 14], from which we adapt the proof. Write $I = I_p \cap J$ and $\mathfrak{a} = \mathfrak{p}^i\mathfrak{b}$ where $\mathrm{Nrd}(I_p)$ is a power of p and $N(\mathfrak{b})$ and $\mathrm{Nrd}(J)$ are not divisible by p. We have $E[\mathfrak{b}] = E[J]$. Then, since all ideals coprime to p are kernel ideals, we have

$$\mathfrak{b} = \{\alpha \in \mathfrak{O} \mid E[\mathfrak{b}] \subseteq \ker(\iota(\alpha))\}, \text{ and}$$
$$J = \{\theta \in \mathrm{End}(E) \mid E[J] \subseteq \ker(\theta)\}.$$

Since $E[\mathfrak{b}] = E[J]$, we deduce that

$$J \cap \iota(\mathfrak{O}) = \{\theta \in \iota(\mathfrak{O}) \mid E[\mathfrak{b}] \subseteq \ker(\theta)\} = \iota(\mathfrak{b}).$$

There exists j such that $I_p \cap \iota(\mathfrak{O}) = \iota(\mathfrak{p}^j)$, hence $I \cap \iota(\mathfrak{O}) = \iota(\mathfrak{p}^{j-i}\mathfrak{a})$, proving the lemma. □

Lemma 9. *A separable K-oriented isogeny of prime degree is horizontal if and only if it is of the form $\psi \circ \varphi_{\mathfrak{a}}$ where ψ is a K-isomorphism and $\mathfrak{a}$ is invertible.*

Proof. Let $\varphi : (E, \iota) \to (E', \iota')$ be a separable K-oriented isogeny of prime degree ℓ. It can be written as $\varphi = \psi \circ \varphi_0$ where $\varphi_0 : E \to E/\ker(\varphi)$ is the canonical projection. Suppose it is horizontal. Then, its kernel is of the form $E[\mathfrak{a}]$ with $N(\mathfrak{a}) = \ell$, so $\varphi_0 = \varphi_{\mathfrak{a}}$. We have

$$\psi_*((\varphi_{\mathfrak{a}})_*(\iota)) = (\psi\varphi_{\mathfrak{a}})_*(\iota) = \varphi_*(\iota) = \iota',$$

so $\psi : \mathfrak{a} \star (E, \iota) \to (E', \iota')$ is a K-isomorphism. The converse is clear. □

Proposition 11 (GRH). *Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an ε-basis of $\mathrm{End}(E)$, one can find $\mathfrak{a}$ such that $\tau_p(E, \iota) = \mathfrak{a} \star (E, \iota)$ in probabilistic polynomial time in $\log(p)$ and $\log(\mathrm{disc}(\mathfrak{O}))$.*

Proof. From Corollary 3, the lattice $\Lambda = (\phi_p \circ \iota(\mathfrak{O}))^{\perp} \cap \mathrm{Hom}(E, E^{(p)})$ is primitive, so one can find $\varphi \in \Lambda$ of prime degree coprime to p and to the conductor of $\mathfrak{O}$ (for instance with the algorithm [Wes22, Proposition 3.6], which ensures that $\deg(\varphi)$ is a large enough prime, assuming GRH). The algorithm returns

$$\mathfrak{a} = \iota^{-1}((\mathrm{Hom}(E^{(p)}, E) \circ \varphi) \cap \iota(\mathfrak{O})).$$

It remains to show that this output is correct. From Corollary 2, we have that $\varphi : (E, \iota) \to \tau_p(E, \iota)$ is an $\mathfrak{O}$-isogeny, and it is horizontal. Applying Lemma 9, the isogeny φ is induced by an $\mathfrak{O}$-ideal $\mathfrak{b}$. We have $E[\mathfrak{b}] = \ker(\varphi) = E[(\mathrm{Hom}(E^{(p)}, E) \circ \varphi]$, so from Lemma 8, we have $\iota(\mathfrak{a}) = \iota(\mathfrak{b})$ (with no inseparable factor since the norm on both sides is coprime to p). Therefore $\mathfrak{a} = \mathfrak{b}$, hence $\tau_p(E, \iota) = \mathfrak{b} \star (E, \iota) = \mathfrak{a} \star (E, \iota)$. □

Lemma 10. *Suppose* $\tau_p(E_1, \iota_1) = \mathfrak{a} \star (E_1, \iota_1)$ *and* $\tau_p(E_2, \iota_2) = \mathfrak{b} \star (E_2, \iota_2)$*. Any ideal* $\mathfrak{c}$ *such that* $\mathfrak{c} \star (E_1, \iota_1) = (E_2, \iota_2)$ *satisfies* $\mathfrak{c}^2 \sim \mathfrak{a}\overline{\mathfrak{b}}$*.*

Proof. We have the chain of equalities

$$\begin{aligned}\overline{\mathfrak{b}}\mathfrak{a} \star (E_1, \iota_1) &= \overline{\mathfrak{b}} \star \tau_p(E_1, \iota_1) = \overline{\mathfrak{b}} \star \tau_p(\overline{\mathfrak{c}} \star (E_2, \iota_2)) \\ &= \mathfrak{c}\overline{\mathfrak{b}} \star \tau_p(E_2, \iota_2) = \mathfrak{c} \star (E_2, \iota_2) \\ &= \mathfrak{c}^2 \star (E_1, \iota_1),\end{aligned}$$

and we conclude from the fact that the action of the class group is free. □

Theorem 2 (GRH, Effective $\mathfrak{O}$-Vectorization **reduces to** $\mathfrak{O}$-EndRing**).** *Given* $\mathfrak{O}$ *and the factorisation of its discriminant, three* $\mathfrak{O}$*-oriented elliptic curves* $(E, \iota), (E', \iota'), (F, \jmath) \in \mathrm{SS}_{\mathfrak{O}}(p)$*, together with* ε*-bases of* $\mathrm{End}(E)$*,* $\mathrm{End}(E')$ *and* $\mathrm{End}(F)$*, one can compute (or assert that it does not exist) an* $\mathfrak{O}$*-ideal* $\mathfrak{c}$ *such that* $(E', \iota') = \mathfrak{c} \star (E, \iota)$ *and an efficient representation of* $\varphi_{\mathfrak{c}} : (F, \jmath) \to \mathfrak{c} \star (F, \jmath)$ *in probabilistic polynomial time in* $\log(p)$*,* $\log(\mathrm{disc}(\mathfrak{O}))$ *and* $\#(\mathrm{Cl}(\mathfrak{O})[2])$*.*

Proof. Suppose we are given $(E_1, \iota_1), (E_2, \iota_2) \in \mathrm{SS}_{\mathfrak{O}}(p)$, together with $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$. We can compute $\mathfrak{a}$ and $\mathfrak{b}$ such that $\tau_p(E_1, \iota_1) = \mathfrak{a} \star (E_1, \iota_1)$ and $\tau_p(E_2, \iota_2) = \mathfrak{b} \star (E_2, \iota_2)$ with Proposition 11. From Lemma 10, the ideal class of $\mathfrak{c}$ is one of the $\#(\mathrm{Cl}(\mathfrak{O})[2])$ square roots of $[\mathfrak{a}\overline{\mathfrak{b}}]$. They can be enumerated following [BS96, Section 6], and each of them can efficiently be checked for correctness with Propositon 9. Once the ideal $\mathfrak{c}$ has been found, compute an efficient representation of $\varphi_{\mathfrak{c}} : (F, \jmath) \to \mathfrak{c} \star (F, \jmath)$ with Propositon 9. □

Corollary 4 (GRH). *Given the factorisation of* $\mathrm{disc}(\mathfrak{O})$*,* Effective $\mathfrak{O}$-Uber *reduces to* $\mathfrak{O}$-EndRing* *in probabilistic polynomial time in* $\log(p)$*,* $\log(\mathrm{disc}(\mathfrak{O}))$ *and* $\#(\mathrm{Cl}(\mathfrak{O})[2])$*.*

Proof. Suppose we are given $(E, \iota), (F, \jmath) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an $\mathfrak{O}$-oriented elliptic curve E'. Solving $\mathfrak{O}$-EndRing*, one can find ε-bases of $\mathrm{End}(E)$, $\mathrm{End}(F)$ and $\mathrm{End}(E')$, and an $\mathfrak{O}$-orientation ι' of E'. The result follows from Theorem 2. □

7 The oriented Diffie-Hellman problem

In this section, we study the relation of $\mathfrak{O}$-DiffieHellman with other $\mathfrak{O}$-oriented problems, proving that it is essentially quantum-equivalent to the problem $\mathfrak{O}$-EndRing. First, we have the following simple reduction from the problem $\mathfrak{O}$-DiffieHellman to Effective $\mathfrak{O}$-Vectorization.

Proposition 12. $\mathfrak{O}$-DiffieHellman *reduces to* Effective $\mathfrak{O}$-Vectorization *in probabilistic polynomial time in* $\log(p)$*.*

Proof. Suppose we are given an oriented curve $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, and its images $\mathfrak{a} \star (E, \iota)$ and $\mathfrak{b} \star (E, \iota)$. Solving Effective $\mathfrak{O}$-Vectorization, one can recover the class of $\mathfrak{a}$, and apply its action on $\mathfrak{b} \star (E, \iota)$, thereby obtaining $(\mathfrak{a}\mathfrak{b}) \star (E, \iota)$. □

Now, it remains to prove that the Effective $\mathfrak{O}$-Vectorization problem reduces to $\mathfrak{O}$-DiffieHellman. In [GPSV21], it was proved that if the action of $\mathrm{Cl}(\mathfrak{O})$ is efficiently computable, then (non-effective) $\mathfrak{O}$-Vectorization reduces to $\mathfrak{O}$-DiffieHellman in quantum polynomial time. Unfortunately, the action of $\mathrm{Cl}(\mathfrak{O})$ is not efficiently computable in general, since only the action of *smooth* class representatives can be computed efficiently. Therefore the reduction does not run in polynomial time, and it does not apply to the effective variant of $\mathfrak{O}$-Vectorization. We resolve both limitations. First, we prove that the $\mathfrak{O}$-Vectorization problem does reduce to $\mathfrak{O}$-DiffieHellman in quantum polynomial time because an oracle for $\mathfrak{O}$-DiffieHellman provides an efficient way to evaluate the group action (by a trick similar to what is done in [GPSV21, Lemma 1]). Second, Proposition 7 and Theorem 2 immediately enhance the reduction from $\mathfrak{O}$-Vectorization to a reduction from Effective $\mathfrak{O}$-Vectorization.

Theorem 3 (GRH). $\mathfrak{O}$-Vectorization *reduces to* $\mathfrak{O}$-DiffieHellman *in quantum polynomial time in* $\log p$ *and* $\log(\mathrm{disc}(\mathfrak{O}))$.

Proof. This is essentially an application of a generalisation of Shor's algorithm for the discrete logarithm problem [Sho97], with the observation that an oracle for $\mathfrak{O}$-DiffieHellman makes the implicit group structure of a $\mathrm{Cl}(\mathfrak{O})$-orbit efficiently computable. More precisely, let $(E,\iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, and $(E',\iota') = \mathfrak{a} \star (E,\iota)$ be an instance of $\mathfrak{O}$-Vectorization. From [Bac90], assuming GRH, there is a bound B polynomial in $\log(\mathrm{disc}(\mathfrak{O}))$ such that $\mathfrak{B} = \{\mathfrak{p} \mid N(\mathfrak{p}) < B \text{ is prime}\}$ is a generating set of the group $\mathrm{Cl}(\mathfrak{O})$. Let

$$f : \mathbf{Z}^{\mathfrak{B}} \times \mathbf{Z} \times \mathrm{SS}_{\mathfrak{O}}(p) \longrightarrow \mathrm{SS}_{\mathfrak{O}}(p) : ((e_{\mathfrak{p}})_{\mathfrak{p}}, k, (F,\iota_F)) \longmapsto \left(\mathfrak{a}^k \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}} \right) \star (F,\iota_F).$$

From [Kit95], if one can evaluate f in quantum polynomial time, then one can solve the corresponding Abelian Stabilizer Problem and recover $(e_{\mathfrak{p}})_{\mathfrak{p}}$ such that $\mathfrak{a} \sim \prod_{\mathfrak{p}} \mathfrak{p}^{e_{\mathfrak{p}}}$ (thereby solving the $\mathfrak{O}$-Vectorization instance). It remains to prove that f can indeed be computed in polynomial time. This is only feasible thanks to the $\mathfrak{O}$-DiffieHellman oracle $\mathscr{O}$, which makes the implicit group multiplication $\odot$ on the orbit $\mathrm{Cl}(\mathfrak{O}) \star (E,\iota)$ efficiently computable, as

$$(\mathfrak{b} \star (E,\iota)) \odot (\mathfrak{c} \star (E,\iota)) = (\mathfrak{b}\mathfrak{c}) \star (E,\iota) = \mathscr{O}((E,\iota), \mathfrak{b} \star (E,\iota), \mathfrak{c} \star (E,\iota)).$$

Therefore, given any $k \geq 0$ and $\mathfrak{b} \star (E,\iota)$, one can compute $\mathfrak{b}^k \star (E,\iota) = (\mathfrak{b} \star (E,\iota))^{\odot k}$ by square-and-multiply. Then, for any $(e_{\mathfrak{p}})_{\mathfrak{p}} \in \mathbf{Z}^{\mathfrak{B}}_{\geq 0}$ and $k \geq 0$, one can efficiently compute

$$f((e_{\mathfrak{p}})_{\mathfrak{p}}, k, (F,\iota_F)) = \left(\bigodot_{\mathfrak{p}} (\mathfrak{p} \star (E,\iota))^{\odot e_{\mathfrak{p}}} \right) \odot (E',\iota')^{\odot k} \odot (F,\iota_F),$$

given the oriented curves $\mathfrak{p} \star (E,\iota)$. Since each $\mathfrak{p}$ has small norm, these $\mathfrak{p} \star (E,\iota)$ can be computed in polynomial time. To deal with negative exponents, we note

that the class number $h(\mathfrak{O})$ is computable in quantum polynomial time [BS16], so all exponents can be reduced modulo $h(\mathfrak{O})$. □

Corollary 5 (GRH). *The problem* CSIDH-DiffieHellman *of recovering CSIDH shared secrets reduces to the problem* $\text{EndRing}_{\mathbf{F}_p}$ *of computing the full endomorphism ring of supersingular elliptic curves defined over* $\mathbf{F}_p$*, under a probabilistic polynomial time reduction in* $\log p$*. Conversely,* $\text{EndRing}_{\mathbf{F}_p}$ *reduces to* CSIDH-DiffieHellman *in quantum polynomial time in* $\log p$*.*

Proof. The problem CSIDH-DiffieHellman is equal to $\mathfrak{O}$-DiffieHellman for some order $\mathfrak{O}$ containing $\sqrt{-p}$. There are at most two possibilities for $\mathfrak{O}$: either $\mathbf{Z}[\sqrt{-p}]$ or $\mathbf{Z}[(1+\sqrt{-p})/2]$. The latter is only possible when $p \equiv 3 \mod 4$. They differ by an index 2, and correspond to CSIDH on the *floor* or on the *surface* — see CSURF [CD20].

In either case, for such an order $\mathfrak{O}$, we now prove that $\text{EndRing}_{\mathfrak{O}}$ reduces to $\text{EndRing}_{\mathbf{F}_p}$. Let E be an $\text{EndRing}_{\mathfrak{O}}$-instance. Since E is $\mathfrak{O}$-orientable, there exists $\alpha \in \text{End}(E)$ of degree p. Since E is supersingular, α is purely inseparable, so it factors as $\alpha = \beta \circ \phi_p^E$ where $\phi_p^E : E \to E^{(p)}$ is the Frobenius and $\beta : E^{(p)} \to E$ is an isomorphism. This proves that $E \cong E^{(p)}$, hence $j(E) \in \mathbf{F}_p$ and one can compute an isomorphism $\gamma : E \to E'$ to a curve E' defined over $\mathbf{F}_p$. Therefore, the $\text{EndRing}_{\mathfrak{O}}$-instance E reduces to the $\text{EndRing}_{\mathbf{F}_p}$-instance E'.

Finally, we prove that $\text{EndRing}_{\mathbf{F}_p}$ reduces to $\mathfrak{O}$-EndRing. If E is defined over $\mathbf{F}_p$, then either $\iota : \sqrt{-p} \to \phi_p^E$ is an $\mathfrak{O}$-orientation on E, or there exists an isogeny $\varphi : E \to E'$ of degree 2 such that $\varphi_*(\iota)$ is an $\mathfrak{O}$-orientation on E' (see [DG16, Theorem 2.7]). So $\text{EndRing}_{\mathbf{F}_p}$ for E reduces to $\mathfrak{O}$-EndRing either for E or for one of its three 2-neighbours.

These new reductions at hand, the corollary follows from the other reductions summarised in Figure 1, given that the factorisation of $\text{disc}(\mathfrak{O})$ is either $-p$ or $-4p$, and from genus theory, $\#(\text{Cl}(\mathfrak{O})[2]) \leq 2$. □

8 The case of non-maximal orders

The OSIDH cryptosystem [CK20] exploits elliptic curves oriented by an order of the form $\mathbf{Z}+\ell^e\mathfrak{O}$, where ℓ is a small prime, and $\mathfrak{O}$ has small discriminant. It is observed however that with such parameters, the $(\mathbf{Z}+\ell^e\mathfrak{O})$-Vectorization problem is not hard, hence it would be unsafe for the protocol to provide full efficient encodings of $(\mathbf{Z}+\ell^e\mathfrak{O})$-orientations. In this section, we generalise this fact and study its consequences for relevant variants of the endomorphism ring problem.

Lemma 11. *Let c be a positive integer. Given $(E, \iota) \in \text{SS}_{\mathbf{Z}+c\mathfrak{O}}(p)$ in efficient representation, one can compute the kernel of an isogeny $\varphi : E \to E'$ of degree c such that $\varphi_*(\iota)$ is an $\mathfrak{O}$-orientation of E' in time polynomial in $\log p$, the largest prime factor of c, and, for each $\ell^e \mid\mid c$, the degree of the extension of $\mathbf{F}_p$ over which $E[\ell^e]$ is defined.*

Proof. Let $\varphi : (E, \iota) \to (E', \iota')$ be the unique ascending K-isogeny of degree c, where $\iota' = \varphi_*(\iota)$ is an $\mathfrak{O}$-orientation. We are given a generator ω of $\mathbf{Z}+c\mathfrak{O}$ and an efficient representation of $\iota(\omega)$. The generator is of the form $\omega = a + c\omega_0$ where ω_0 is a generator of $\mathfrak{O}$ and without loss of generality, $a = 0$. We have

$$\iota(\omega) = (\hat{\varphi}_*(\iota'))(\omega) = \frac{\hat{\varphi} \circ \iota'(\omega) \circ \varphi}{c} = \hat{\varphi} \circ \iota'(\omega_0) \circ \varphi.$$

It implies $\ker(\varphi) \subseteq \ker(\iota(\omega))$. Now $\ker(\iota(\omega))$ is cyclic (otherwise ι would not be a primitive embedding), so $\ker(\varphi) = \ker(\iota(\omega)) \cap E[c] = \cap_{\ell^e || c}(\ker(\iota(\omega)) \cap E[\ell^e])$ can be recovered in time polynomial in the largest prime factor of c, and, for each $\ell^e \,||\, c$, in the degree of the extension of $\mathbf{F}_p$ over which $E[\ell^e]$ is defined. □

In particular, if c is smooth and $E[c]$ is defined over a small extension of $\mathbf{F}_p$, given $(E, \iota) \in \mathrm{SS}_{\mathbf{Z}+c\mathfrak{O}}(p)$, it is easy to find the unique isogeny ascending to an $\mathfrak{O}$-orientable curve. This is the crux of so-called *torsion point attacks* on SIDH-like cryptosystems [Pet17,KMP+21], which can be reinterpreted as an attempt to recover a $(\mathbf{Z}+c\mathfrak{O})$-orientation from some information on the action of isogenies on torsion points, and some carefully chosen $\mathfrak{O}$.

Lemma 12 (GRH). *Given the kernel of an isogeny $\varphi : E \to E'$, and an ε-basis of E, one can compute an ε-basis of E' in time polynomial in the length of the input and the largest prime factor of* $\deg(\varphi)$.

Proof. This statement seems folklore; we give a proof for completeness. Let us describe a simple (and certainly not optimal) algorithm. We may assume that $\ker(\varphi)$ is cyclic. Choose any prime $\ell \mid \deg(\varphi)$, and let $\varphi_1 : E \to E_1 = E/(\ker(\varphi) \cap E[\ell])$. One can compute the left $\mathrm{End}(E)$-ideals I_1 of norm ℓ corresponding to φ_1 (for instance with an exhaustive search among the $\ell + 1$ possibilities, checking each guess by evaluating a basis on the kernel of φ_1). Now, $\mathcal{O}_R(I_1) \cong \mathrm{End}(E_1)$, and one can find an ε-basis of $\mathrm{End}(E_1)$ (for instance with [Wes22, Algorithm 6]). The isogeny φ factors as $\varphi' \circ \varphi_1$ with $\deg(\varphi') = \deg(\varphi)/\ell$, and one can iterate the procedure. □

Theorem 4 (GRH). $(\mathbf{Z}+c\mathfrak{O})$-EndRing *reduces to* $\mathfrak{O}$-EndRing* *in time polynomial in* $\log p$*, the largest prime factor of c, and, for each $\ell^e \,||\, c$, the degree of the extension of $\mathbf{F}_p$ over which $E[\ell^e]$ is defined.*

Proof. Let $(E, \iota) \in \mathrm{SS}_{\mathbf{Z}+c\mathfrak{O}}(p)$ be an instance of $(\mathbf{Z}+c\mathfrak{O})$-EndRing. From Lemma 11, we can compute (within the claimed running time) an isogeny $\varphi : E \to E'$ where E' is $\mathfrak{O}$-orientable. One can solve $\mathfrak{O}$-EndRing* for E' to find an ε-basis of $\mathrm{End}(E')$. Now, Lemma 12 allows us to find an ε-basis of $\mathrm{End}(E)$ thanks to the ε-basis of $\mathrm{End}(E')$ and the kernel of $\hat{\varphi}$. □

Lemma 13. $\mathfrak{O}$-EndRing* *can heuristically be solved in expected time polynomial in* $\log p$ *and* $\mathrm{disc}(\mathfrak{O})$.

Proof. By Proposition 8, one can reduce $\mathfrak{O}$-EndRing* to $\mathfrak{O}$-Uber in time polynomial in $\log p$ and $\log(\mathrm{disc}(\mathfrak{O}))$. Then, one can solve $\mathfrak{O}$-Uber with Proposition 2, under the same heuristics. □

Corollary 6. $(\mathbf{Z}+c\mathfrak{O})$-EndRing *can heuristically be solved in time polynomial in* $\log p$, $\mathrm{disc}(\mathfrak{O})$, *the largest prime factor of* c, *and, for each* $\ell^e \mid\mid c$, *the degree of the extension of* $\mathbf{F}_p$ *over which* $E[\ell^e]$ *is defined.*

Proof. It immediately follows from Theorem 4 and Lemma 13. □

This corollary implies that if $\mathfrak{O}$ has small discriminant and c is powersmooth, then knowledge of a $(\mathbf{Z}+c\mathfrak{O})$-orientation leaks the whole endomorphism ring.

Theorem 5 (GRH). *Suppose* c *is* $(\log p)^{O(1)}$*-powersmooth. Then, the problem* $(\mathbf{Z}+c\mathfrak{O})$-EndRing *reduces to* $\mathfrak{O}$-EndRing *in time polynomial in* $\log p$.

Proof. We proceed as in the proof of Theorem 4, but reducing to $\mathfrak{O}$-EndRing using the $\mathfrak{O}$-orientation $\varphi_*(\iota)$ on E'. The efficient representation of ι implies that one can efficiently evaluate $\hat{\varphi} \circ \iota(\alpha) \circ \varphi$, and the powersmoothness of c allows one to divide by c, so we have an efficient representation of $\varphi_*(\iota)$ to be used by the $\mathfrak{O}$-EndRing solver. □

9 Acknowledgements

This work was supported by the Agence Nationale de la Recherche under grants ANR MELODIA (ANR-20-CE40-0013) and ANR CIAO (ANR-19-CE48-0008).

References

Bac90. Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990.

BKV19. Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. CSI-FiSh: Efficient isogeny based signatures through class group computations. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security*, volume 11921 of *Lecture Notes in Computer Science*, pages 227–247. Springer, 2019.

BS96. Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2-class groups. *Journal de théorie des nombres de Bordeaux*, 8(2):283–313, 1996.

BS16. J.-F. Biasse and F. Song. Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields. In Robert Krauthgamer, editor, *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms – SODA 2016*, pages 893–902. SIAM, 2016.

CD20. Wouter Castryck and Thomas Decru. CSIDH on the surface. In *PQCrypto 2020 - International Conference on Post-Quantum Cryptography*, volume 12100, pages 111–129. Springer, 2020.

CJS14. Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.

CK20. Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *Journal of Mathematical Cryptology*, 14(1):414–437, 2020.

CLG09. Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *Journal of Cryptology*, 22(1):93–113, Jan 2009.

CLM+18. Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

CN00. Jean-Sébastien Coron and David Naccache. Security analysis of the Gennaro-Halevi-Rabin signature scheme. In Bart Preneel, editor, *Advances in Cryptology - EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 91–101. Springer, 2000.

Cou06. Jean Marc Couveignes. Hard homogeneous spaces. IACR Cryptology ePrint Archive, Report 2006/291, 2006. `https://eprint.iacr.org/2006/291`.

CPV20. Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, volume 12106 of *Lecture Notes in Computer Science*, pages 523–548. Springer, 2020.

CS21. Mathilde Chenu and Benjamin Smith. Higher-degree supersingular group actions. In *MathCrypt 2021 - Mathematical Cryptology*, 2021.

DDF+21. Luca De Feo, Cyprien Delpech de Saint Guilhem, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Christophe Petit, Javier Silva, and Benjamin Wesolowski. Séta: Supersingular encryption from torsion attacks. To appear in Advances in Cryptology - ASIACRYPT 2021, 2021.

DG16. Christina Delfs and Steven D Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016.

EHL+18. Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology – EUROCRYPT 2018*, pages 329–368, Cham, 2018. Springer International Publishing.

EHL+20. Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Open Book Series*, 4(1):215–232, 2020.

FKM21. Tako Boris Fouotsa, Péter Kutas, and Simon-Philipp Merz. On the isogeny problem with torsion point information. IACR Cryptology ePrint Archive, Report 2021/153, 2021. `https://eprint.iacr.org/2021/153`.

GPS20. Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *Journal of Cryptology*, 33(1):130–175, 2020.

GPST16. Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In Jung Hee Cheon

and Tsuyoshi Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security*, volume 10031 of *Lecture Notes in Computer Science*, pages 63–91, 2016.

GPSV21. Steven Galbraith, Lorenz Panny, Benjamin Smith, and Frederik Vercauteren. Quantum equivalence of the DLP and CDHP for group actions. *Mathematical Cryptology*, 1(1):40–44, 2021.

JD11. David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In Bo-Yin Yang, editor, *International Workshop on Post-Quantum Cryptography – PQCrypto 2011*, pages 19–34, 2011.

Kan89. Masanobu Kaneko. Supersingular j-invariants as singular moduli mod p. *Osaka Journal of Mathematics*, 26(4):849–855, 1989.

Kit95. A Yu Kitaev. Quantum measurements and the abelian stabilizer problem. *arXiv preprint quant-ph/9511026*, 1995.

KLPT14. David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.

KMP+21. Péter Kutas, Chloe Martindale, Lorenz Panny, Christophe Petit, and Katherine E. Stange. Weak instances of SIDH variants under improved torsion-point attacks. In *to appear in Advances in Cryptology - CRYPTO 2021*, Lecture Notes in Computer Science, 2021.

Kup05. Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

LB20. Jonathan Love and Dan Boneh. Supersingular curves with small noninteger endomorphisms. *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Open Book Series*, 4(1):7–22, 2020.

LO77. J.C. Lagarias and A.M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 409–464. Academic Press, London, 1977.

Onu21. Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields and Their Applications*, 69:101777, 2021.

Pet17. Christophe Petit. Faster algorithms for isogeny problems using torsion point images. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017*, volume 10625 of *Lecture Notes in Computer Science*, pages 330–353. Springer, 2017.

Piz80. Arnold Pizer. An algorithm for computing modular forms on $\gamma_0(n)$. *Journal of algebra*, 64(2):340–390, 1980.

Rón92. Lajos Rónyai. Algorithmic properties of maximal orders in simple algebras over $\mathbf{Q}$. *Computational Complexity*, 2(3):225–243, 1992.

Sho97. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

Sil86. Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Gradute Texts in Mathematics*. Springer-Verlag, 1986.

Sim06. Denis Simon. Quadratic equations in dimensions 4, 5 and more. Preprint, 2006. See [Wat13] for a published review.

Vig06. M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800. Springer, 2006.

Voi21. John Voight. *Quaternion Algebras*. Springer International Publishing, 2021. Graduate Texts in Mathematics, No. 288.

Wat13. Mark Watkins. Some comments about indefinite LLL. *Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms*, 587(233):32, 2013.

Wes22. Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *FOCS 2021-62nd Annual IEEE Symposium on Foundations of Computer Science*, 2022.