On the Security of OSIDH

Pierrick Dartois, Luca de Feo

On the security of OSIDH

Pierrick Dartois[1,2] and Luca De Feo[2][0000−0002−9321−0773]

[1] Corps des Mines, Paris, France
[2] IBM Research Europe, Zürich, Switzerland
pierrick.dartois@mines-paristech.fr, pkc22@defeo.lu

Abstract. The Oriented Supersingular Isogeny Diffie–Hellman is a post-quantum key exchange scheme recently introduced by Colò and Kohel. It is based on the group action of an ideal class group of a quadratic imaginary order on a subset of supersingular elliptic curves, and in this sense it can be viewed as a generalization of the popular isogeny based key exchange CSIDH. From an algorithmic standpoint, however, OSIDH is quite different from CSIDH. In a sense, OSIDH uses class groups which are more structured than in CSIDH, creating a potential weakness that was already recognized by Colò and Kohel. To circumvent the weakness, they proposed an ingenious way to realize a key exchange by exchanging partial information on how the class group acts in the neighborhood of the public curves, and conjectured that this additional information would not impact security.
In this work we revisit the security of OSIDH by presenting a new attack, building upon previous work of Onuki. Our attack has exponential complexity, but it practically breaks Colò and Kohel's parameters unlike Onuki's attack. We also discuss countermeasures to our attack, and analyze their impact on OSIDH, both from an efficiency and a functionality point of view.

Keywords: Post-quantum cryptography · Isogenies · Cryptographic group actions

1 Introduction

Cryptographic group actions have recently attracted much interest owing to their supposed quantum-resistance and to their versatility. Brassard and Yung [11] initiated the study of group actions in cryptography, but it was Couveignes [18] and Rostovtsev and Stolbunov [39] who independently exhibited the first post-quantum key exchange based on a group action. The invention of CSIDH[3] [13], the first efficient post-quantum group action, spurred a wave of interest on the topic. Among the many applications of CSIDH, we may cite the

[3] The "Commutative Supersingular Diffie–Hellman", pronounced *sea-side*.

signature scheme CSI-FiSh [7], threshold [21] and ring [6] signatures, oblivious transfer [22,33], oblivious PRFs [8] and hash proof systems [2]. As of today, all known post-quantum group actions are obtained from isogenies of elliptic curves, either ordinary or supersingular, and are all understood as instances of the celebrated theory of *complex multiplication*.

Drawing inspiration from CSIDH, Colò and Kohel recently proposed a generalization they called OSIDH, for "Oriented Supersingular Diffie–Hellman" [17]. Like CSIDH, OSIDH is based on the action of the class group of a quadratic imaginary order on a set of supersingular curves. But while CSIDH's group action is fully determined by the Frobenius endomorphism, OSIDH's action is determined by an arbitrary endomorphism which they call an *orientation*. Besides the added technicalities involved in working with orientations, to complete a key exchange in OSIDH Alice and Bob need to exchange significantly more information than in CSIDH. Colò and Kohel conjectured nevertheless that this additional information does not adversely affect the security of the cryptosystem.

In this work, we present a new classical attack that casts doubts on the viability of OSIDH. Albeit exponential in complexity, we give evidence that it breaks in practice the parameters that Colò and Kohel suggested would match the security of CSIDH-512.[4] The only exponential step in our attack is an SVP computation in a lattice that depends exclusively on the system parameters. The attack can be countered by increasing the dimension of the lattice and the other parameters accordingly, however we argue that this patch is of dubious interest for post-quantum cryptography: besides making OSIDH prohibitively expensive, it makes it at best as secure as lattice based schemes, without the efficiency, the versatility and the security reductions that go with them.

A more advanced countermeasure is to stretch parameters to a point where, according to standard heuristics, no short enough vectors exist in the lattice. This countermeasure is less costly, yet we argue that it does not completely rescue OSIDH. Indeed, our attack shows that OSIDH fails at satisfying the standard axioms of a cryptographic group action, and thus powerful schemes such as CSI-FiSh [7] cannot be securely built on it. This pretty much confines OSIDH to the role of a key exchange of mostly theoretical interest, for the time being.

On the positive side, we argue that, because OSIDH is not properly speaking a cryptographic group action, Kuperberg's quantum algorithm does not appear to apply to it. It is conceivable, then, that the best quantum algorithm against OSIDH would have exponential, rather than subexponential, complexity.

1.1 Overview

The theory of complex multiplication establishes a link between the abelian extensions of quadratic imaginary number fields and elliptic curves. If $\mathcal{O}$ is an order in a quadratic imaginary number field, an elliptic curve is said to have

[4] CSIDH-512 was originally claimed to match the NIST-1 security level. Recent works have questioned the quantum security of CSIDH [9,36], but to this day CSIDH-512's classical security claim still holds unchanged.

complex multiplication (CM) by $\mathcal{O}$ when its endomorphism ring is isomorphic to $\mathcal{O}$. For example, ordinary curves over finite fields always have CM by some quadratic order.

An isogeny $\varphi : E \to E'$ between two curves with CM by the same order $\mathcal{O}$ is called *horizontal* [30]. The same way it identifies elements of $\mathcal{O}$ to endomorphisms, CM identifies (invertible) ideals of $\mathcal{O}$ to isogenies. Invertible fractional ideals of $\mathcal{O}$ form an abelian group, and their identification with isogenies defines a group action on the set of elliptic curves with CM by $\mathcal{O}$ by

$$\mathfrak{a} \cdot E := E',$$

where $\varphi_{\mathfrak{a}} : E \to E'$ is the isogeny associated to $\mathfrak{a} \subset \mathcal{O}$. By this definition, principal ideals of $\mathcal{O}$ act trivially, and the fundamental theorem of CM states that the ideal class group $\mathrm{Cl}(\mathcal{O})$—the quotient of the invertible by the principle ideals—acts faithfully and transitively on the set of elliptic curves with CM by $\mathcal{O}$. See [19,41,47] for more details.

The correspondence with isogenies lets us evaluate the action of $\mathrm{Cl}(\mathcal{O})$ effectively. A prime q that splits in $\mathcal{O}$ factors as a product $(q) = \mathfrak{q}\bar{\mathfrak{q}}$ of prime ideals of norm q. These are the only two ideals of norm q in $\mathcal{O}$, and to each corresponds an isogeny of degree q. As long as we can compute the two horizontal isogenies of degree q starting from E, we can thus evaluate the action of $\mathfrak{q}$ and $\bar{\mathfrak{q}}$. Which isogeny corresponds to which ideal can be determined by looking at how the Frobenius endomorphism of E acts on the kernels of the isogenies.

This is the idea at the heart of Couveignes' [18] and Rostovtsev and Stolbunov's [39] key exchange schemes: On the one hand the group action can be evaluated efficiently; on the other hand it is assumed to be hard, given two curves E, E' with CM by $\mathcal{O}$, to find the element $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ such that $\mathfrak{a} \cdot E = E'$, or, equivalently, a horizontal isogeny $\varphi : E \to E'$.

However, computing isogenies has complexity polynomial in the degree, and thus only for a small fraction of all ideals we can efficiently evaluate the CM action. We can work around this limitation by fixing a list of ideals of small norm $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_t$, and representing elements of $\mathrm{Cl}(\mathcal{O})$ as linear combinations of these generators:

$$\mathfrak{a} = \prod_{i=1}^{t} \mathfrak{q}_i^{e_i}.$$

Provided enough generators, any element $\mathfrak{a}$ can be represented by an exponent vector $(e_1, \ldots, e_t)$ of small norm, and the CM action can thus be evaluated using only $\sum_{i=1}^{t} |e_i|$ efficient isogeny computations.

Although any element of $\mathrm{Cl}(\mathcal{O})$ may be represented in this factored form, it is not necessarily the case that such representation can be easily computed for any input.

In [2], this is called a Restricted Effective Group Action (REGA), as opposed to Effective Group Actions (EGA) where the action of any group element can be efficiently evaluated. It is believed that REGAs are less powerful than EGAs, as some protocols are only known for the latter [21], and many others are much less efficient when instantiated from the former [20,7,2,6].

Given a set of generators $\mathfrak{q}_1, \dots \mathfrak{q}_t$, it is natural to introduce the *relation lattice*

$$L = \left\{ (e_1, \dots, e_t) \;\middle|\; \prod_{j=1}^{t} [\mathfrak{q}_i]^{e_i} = [1] \text{ in } \mathrm{Cl}(\mathcal{O}) \right\}. \tag{1}$$

Then, by definition $\mathrm{Cl}(\mathcal{O}) \simeq \mathbb{Z}^t/L$, *i.e.* two exponent vectors represent the same element of $\mathrm{Cl}(\mathcal{O})$ if and only if they differ by an element of L. If L can be computed, then any exponent vector $\mathbf{e}$ can be transformed in an equivalent vector $\mathbf{e}' = \mathbf{e} - \mathbf{c}$ of small norm by finding a close vector $\mathbf{c} \in L$ to $\mathbf{e}$. This is the idea behind CSI-FiSh [7], and a general technique to transform any REGA into an EGA, assuming these computations can be done efficiently.

OSIDH. Supersingular curves have endomorphism rings isomorphic to maximal orders in a quaternion algebra, but these contain infinitely many quadratic imaginary orders, which make it possible to define a CM group action on subsets of supersingular curve. For example, when $p \equiv 3$ [8] and $p > 3$, the endomorphism ring of any supersingular curve defined over a prime field $\mathbb{F}_p$ contains a subring isomorphic to $\mathcal{O} := \mathbb{Z}[\sqrt{-p}]$. This is, in fact, the subring of $\mathbb{F}_p$-rational endomorphisms of the curve. CSIDH [13] uses precisely this case to define a supersingular analogue of Couveignes and Rostovtsev–Stolbunov. The identification of the Frobenius endomorphism with $\sqrt{-p}$ makes it possible to compute the CM action exactly like in the ordinary case; moreover, the shift to supersingular curves enables a range of optimizations that make CSIDH vastly more practical.

OSIDH seeks to replicate the ideas of CSIDH, but using a different quadratic order $\mathcal{O} \hookrightarrow \mathrm{End}(E)$. To do so, it needs to construct a quadratic order $\mathcal{O}$ with exponentially large class group, and compute a curve in the associated CM orbit. This is done by starting from a maximal quadratic order with small class group, *e.g.* $\mathbb{Z}[i]$, for which it is easy to find an associated supersingular curve E_0. Then, a chain $E_0 \to E_1 \to \cdots \to E_n$ of *descending* (*i.e.* not horizontal) isogenies of degree ℓ is taken, to which is associated a chain of increasingly small orders $\mathcal{O}_i := \mathbb{Z} + \ell^i\mathcal{O}$. Colò and Kohel call the inclusion $\mathcal{O}_i \hookrightarrow \mathrm{End}(E_i)$ an $\mathcal{O}_i$*-orientation* of E_i, and, since $\mathcal{O}_{i+1} \subset \mathcal{O}_i$, the whole chain $E_0 \to \cdots \to E_n$ is $\mathcal{O}_n$-oriented. At each descending step the size of the class group $\mathrm{Cl}(\mathcal{O}_i)$ is multiplied roughly by ℓ (see [19, Theorem 7.24]), and it is proved that $\mathrm{Cl}(\mathcal{O}_n)$ acts faithfully and transitively on the set of (primitively) $\mathcal{O}_n$-oriented curves (see Theorem 1).

The action of $\mathrm{Cl}(\mathcal{O}_n)$ on descending chains $E_0 \to \cdots \to E_n$ can be computed efficiently using the same techniques as above (with a set of generating prime ideals). However Colò and Kohel remark that the inverse problem, that of computing the element $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_n)$ mapping a chain to another, is not hard, unlike in CSIDH. Ideally, one would like to only publish the final element of the chain E_n, and act with $\mathrm{Cl}(\mathcal{O}_n)$ on it. However in doing so the information on the orientation is lost, and thus the action of $\mathrm{Cl}(\mathcal{O}_n)$ cannot be computed.

Colò and Kohel suggest, instead, to publish E_n along with the information on how a list of generators $\mathfrak{q}_1, \dots, \mathfrak{q}_t \in \mathrm{Cl}(\mathcal{O}_n)$ acts on E_n up to a bounded distance.

Namely, they publish E_n along with *horizontal chains* $\mathfrak{q}_i^e \cdot E_n$ for all $1 \leq i \leq t$ and $-r \leq e \leq r$ for some pre-determined bound r. From this information, the action of exponentially many elements of $\mathrm{Cl}(\mathcal{O}_n)$ on E_n can be evaluated efficiently. Remarkably, the analogous information in CSIDH is publicly available, so it may be believed that publishing $\mathfrak{q}_i^e \cdot E_n$ in OSIDH does not harm security.

Our contribution. We show that the additional information conveyed by the horizontal isogeny chains in OSIDH can be leveraged to recover the descending chain $E_0 \to \cdots \to E_n$, and thus the secret.

Our attack builds upon the work of Onuki [35], who showed that being able to evaluate a single endomorphism of $\mathcal{O}_n$ on points of E_n is enough to recover the descending chain. For this, it is necessary to express the endomorphism as a cycle $E_n \to \cdots \to E_n$ of small degree isogenies, equivalently as a product $\prod_i \mathfrak{q}_i^{e_i}$. To find such an isogeny cycle, Onuki resorts to an expensive meet-in-the-middle procedure, which seems difficult to put into practice.

We observe that finding a product $\prod_i \mathfrak{q}_i^{e_i}$ corresponding to a cycle amounts to finding a vector in the relation lattice L defined in Eq. (1). A basis for L can be computed from the description of $\mathcal{O}_n$, without involving any elliptic curve computations, and in polynomial time, thanks to the special structure of $\mathcal{O}_n$. To obtain an effectively computable isogeny cycle, the vector in L must be short, so that we can use the published horizontal chains. Such a short vector, if it exists, can be found by an SVP computation: this is the only step in our attack which has exponential complexity, namely in the number t of public generators. After the short vector is found, all subsequent steps in Onuki's attack take polynomial time.

In practice, following CSIDH, Colò and Kohel suggested $t = 74$ for an instantiation of OSIDH deemed to be as secure as CSIDH-512. This falls well short of the dimension needed to thwart SVP attacks, and indeed in our experiments we were able to construct the lattice and find a short vector in less than one hour on an ordinary laptop.

A simple countermeasure is to increase the number of primes t and $\# \mathrm{Cl}(\mathcal{O}_n)$ accordingly, until the relation lattice becomes large enough to stop SVP computations, however this appears to be extremely expensive. A cheaper countermeasure would be to keep t relatively small, but increase the size of $\mathrm{Cl}(\mathcal{O}_n)$ so that no short enough vectors are expected to exist in L. We argue that, no matter what solution is chosen, one desirable property of CM group actions is lost: CSI-FiSh was made possible by the computation of the relation lattice of CSIDH-512; furthermore, each CSI-FiSh signature solves a CVP problem in dimension $t = 74$. Neither of these is possible with OSIDH after we apply one of the patches above. It seems, indeed, that the security of OSIDH is fundamentally in conflict with the possibility of evaluating the CM group action for any possible input, and thus that it cannot be used as a foundation for protocols based on EGAs or even REGAs.

Plan. In the next section we present the mathematical foundations of OSIDH, then in Section 3 we present the protocol itself. In Section 4 we present our attack, and in Section 5 the countermeasures against it, and their consequences, both positive and negative, for OSIDH.

2 Oriented supersingular elliptic curves

We start by briefly recalling the mathematical framework of OSIDH, presented in detail by Colò–Kohel [17] and Onuki [35].

2.1 Oriented elliptic curves and isogenies

Let K be a quadratic imaginary field and E an elliptic curve defined over a finite field. A K-*orientation* of E is an embedding $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$. If $\mathcal{O}$ is an order of K, we say that (E, ι) is an $\mathcal{O}$-*orientation* if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. An $\mathcal{O}$-orientation is *primitive* if $\mathcal{O}$ is maximal for this inclusion, or in other words, if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$.

Example 1. The elliptic curve $E : y^2 = x^3 + x$ defined over $\mathbb{F}_p$ ($p \equiv 3$ [4]) has a $\mathbb{Q}(i)$-orientation, mapping $i = \sqrt{-1}$ to the endomorphism

$$\phi : (x, y) \in E \longmapsto (-x, ay) \in E,$$

with $a \in \mathbb{F}_{p^2}$ such that $a^2 = -1$. This is a primitive $\mathbb{Z}[i]$-orientation.

When E is ordinary, $\mathrm{End}(E) \otimes \mathbb{Q}$ is itself a quadratic imaginary field, hence, there is only one K-orientation (up to complex conjugation). The case of supersingular elliptic curves is more interesting: $\mathrm{End}(E) \otimes \mathbb{Q}$ is a quaternion algebra and we can embed infinitely many quadratic fields inside, so there are infinitely many orientations of E.

Let (E, ι_E) and (F, ι_F) be two K-oriented elliptic curves. An isogeny $\varphi : E \longrightarrow F$ is K-*oriented* if $\varphi_*(\iota_E) = \iota_F$, where $\varphi_*(\iota_E)$ is the K-orientation of F defined as follows:

$$\forall \alpha \in K, \quad \varphi_*(\iota)(\alpha) = \frac{1}{\deg(\varphi)} \varphi \iota(\alpha) \widehat{\varphi}.$$

A K-oriented isogeny $\lambda : (E, \iota_E) \longrightarrow (F, \iota_F)$ is a (K-oriented) *isomorphism* if it has an inverse isogeny $F \longrightarrow E$ that is also K-oriented $(F, \iota_F) \longrightarrow (E, \iota_E)$.

Let $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$ be a K-oriented isogeny, $\mathcal{O} := \iota_E^{-1}(\mathrm{End}(E))$ and $\mathcal{O}' := \iota_F^{-1}(\mathrm{End}(F))$, so that ι_E is a primitive $\mathcal{O}$-orientation and ι_F is a primitive $\mathcal{O}'$-orientation. We say that φ is *horizontal*, *ascending* or *descending*, respectively when $\mathcal{O} = \mathcal{O}'$, $\mathcal{O} \subsetneq \mathcal{O}'$ or $\mathcal{O} \supsetneq \mathcal{O}'$. There is no reason for this to be verified in general, except when φ has prime degree. In that case, the index relating $\mathcal{O}$ and $\mathcal{O}'$ also divides $\deg(\varphi)$ [30, Chapter 4, Proposition 21]. Finally, an isomorphism is always horizontal.

2.2 Class group action

Let K be a quadratic imaginary field and $\mathcal{O}$ be an order of K. Let p be a prime number. We consider the set $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ of isomorphism classes of primitively $\mathcal{O}$-oriented supersingular elliptic curves defined over $\overline{\mathbb{F}}_p$.

Proposition 1. *[35, Proposition 3.2] $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ is not empty if and only if p does not split in K and is prime to the conductor of $\mathcal{O}$.*

In the following, we shall assume that $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ is not empty. We define a group action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$. Let $\mathfrak{a} \subseteq \mathcal{O}$ be an ideal of norm prime to p and (E, ι) be a primitively $\mathcal{O}$-oriented supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. We define the $\mathfrak{a}$-*torsion subgroup* by

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

By [42, Proposition III.4.12], there exists a separable isogeny $\varphi_{\mathfrak{a}} : E \longrightarrow F$ of kernel $E[\mathfrak{a}]$. If $\mathfrak{a}$ is an invertible $\mathcal{O}$-ideal (*i.e.* one whose norm is prime to the conductor of $\mathcal{O}$), then $\varphi_{\mathfrak{a}}$ is a horizontal isogeny by [35, Proposition 3.5]. In that case, we write

$$\mathfrak{a} \cdot (E, \iota) := (F, (\varphi_{\mathfrak{a}})_*(\iota)).$$

A separable isogeny being determined by its kernel up to isomorphism [42, Proposition III.4.11], we easily get that the isomorphism class of $\mathfrak{a} \cdot (E, \iota)$ only depends on $\mathfrak{a}$ and the isomorphism class of (E, ι).

Furthermore, if $\mathfrak{b}$ is another invertible $\mathcal{O}$-ideal of norm prime to p and if $\varphi_{\mathfrak{b}} : F \longrightarrow G$ has kernel $F[\mathfrak{b}]$, then $\ker(\varphi_{\mathfrak{b}} \circ \varphi_{\mathfrak{a}}) = E[\mathfrak{a}\mathfrak{b}]$, by [47, Proposition 3.12] or [34, Proposition 7.28]. Hence, if we set

$$\mathfrak{a}^{-1} \cdot (E, \iota) := \overline{\mathfrak{a}} \cdot (E, \iota),$$

we define an action of the group of fractional $\mathcal{O}$-ideals prime to p on $\mathrm{SS}_{\mathcal{O}}^{pr}(p)$. Since the action of principal ideals is trivial, we get an action of the ideal class group

$$\mathrm{Cl}(\mathcal{O}) \times \mathrm{SS}_{\mathcal{O}}^{pr}(p) \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(p).$$

This action is faithful [35, Theorem 3.4], but not transitive.

Example 2. The orientation of Example 1 and its composition with the complex conjugation are two non-isomorphic $\mathbb{Z}[i]$-orientations. But the ideal class group $\mathrm{Cl}(\mathbb{Z}[i])$ is trivial, so the orbits contain only one element. Hence, the group action of $\mathrm{Cl}(\mathbb{Z}[i])$ on $\mathrm{SS}_{\mathbb{Z}[i]}^{pr}(p)$ cannot be transitive.

This example illustrates the general case (see [35, Proposition 3.3]): there are always two orbits related by complex conjugation (or equivalently by the action of the p-th Frobenius isogeny). In [35, § 3.2], Onuki constructs one of these orbits "canonically", as the image of $\mathrm{Ell}(\mathcal{O})$, the set of isomorphism classes of elliptic curves defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$ by a reduction modulo p map: $\rho_{\mathcal{O}} : \mathrm{Ell}(\mathcal{O}) \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ (that he defines properly). Onuki also proves that:

Theorem 1. *[35, Theorem 3.4] The group* $\mathrm{Cl}(\mathcal{O})$ *acts faithfully and transitively on* $\rho_{\mathcal{O}}(\mathrm{Ell}(\mathcal{O}))$.

Since $\mathrm{Cl}(\mathcal{O})$ also acts freely and transitively on $\mathrm{Ell}(\mathcal{O})$ (see [41, Proposition II.1.2]) it follows that $\rho_{\mathcal{O}}$ is injective. In the following we shall restrict our attention to the ideal class group action on the orbit $\rho_{\mathcal{O}}(\mathrm{Ell}(\mathcal{O}))$.

2.3 Oriented supersingular isogeny graphs

Let $\mathrm{Ell}(K)$ be the union of $\mathrm{Ell}(\mathcal{O})$ for every order $\mathcal{O}$ of K with conductor prime to p and $\mathrm{SS}_K(p)$ be the set of K-oriented supersingular elliptic curves up to K-oriented isomorphism. Then, we have an injective map

$$\rho : \mathrm{Ell}(K) \longrightarrow \mathrm{SS}_K(p)$$

naturally induced by the maps $\rho_{\mathcal{O}} : \mathrm{Ell}(\mathcal{O}) \longrightarrow \mathrm{SS}_{\mathcal{O}}^{pr}(p)$ for all orders $\mathcal{O}$ of K with conductor prime to p.

We say that two K-oriented isogenies are *K-equivalent* if they are equal up to multiplication on the right and on the left by K-oriented isomorphisms. Let $\ell \neq p$ be a prime number. The *K-oriented supersingular ℓ-isogeny graph* $G_\ell(K,p)$ is the graph whose set of vertices is $\rho(\mathrm{Ell}(K))$ and whose edges are K-oriented ℓ-isogenies up to K-equivalence.

By the injectivity of ρ, this graph is isomorphic to the ℓ-isogeny graph of elliptic curves over $\mathbb{C}$ with complex multiplication by an order of K. It follows that $G_\ell(K,p)$ is infinite (unlike the supersingular ℓ-isogeny graph over $\overline{\mathbb{F}}_p$) and that every ℓ-isogeny from a vertex of $G_\ell(K,p)$ has codomain in $G_\ell(K,p)$.

In addition, as Kohel proved [30, Chapter 4, Proposition 23], the connected components of $G_\ell(K,p)$ have a volcano structure (see Figure 1). From each vertex on the crater, there are $1+\left(\frac{\Delta_K}{\ell}\right)$ horizontal and $1/[\mathcal{O}^\times : (\mathbb{Z}+\ell\mathcal{O})^\times]\left(\ell-\left(\frac{\Delta_K}{\ell}\right)\right)$ descending ℓ-isogenies up to K-equivalence. From each vertex outside of the crater, there are ℓ descending and one ascending ℓ-isogeny up to K-equivalence.

Unlike the supersingular ℓ-isogeny graph, $G_\ell(K,p)$ is infinite because vertices carry additional information: the K-orientation. Hence, the graph $G_\ell(K,p)$ refolds when we forget orientations and consider j-invariants only (see Figure 1). Equivalently, the forgetful map $\rho(\mathrm{Ell}(K)) \longrightarrow \mathrm{SS}(p)$ is not injective ($\mathrm{SS}(p)$ being the set of supersingular elliptic curves over $\overline{\mathbb{F}}_p$, up to isomorphism). This is inconvenient because in OSIDH, K-oriented elliptic curves are represented by their j-invariants only in order to use modular polynomials. Luckily, we have:

Theorem 2. *[17, Proposition 13] When restricted to the union of* $\mathrm{Ell}(\mathcal{O})$ *with* $|\operatorname{disc}(\mathcal{O})| < p$, *the forgetful map becomes injective.*

2.4 Effective computation of the ideal class group action

Let ℓ be a small prime ($\neq p$). For all $i \in \mathbb{N}$, let $\mathcal{O}_i := \mathbb{Z} + \ell^i\mathcal{O}_K$. OSIDH is based on the ideal class group action of $\mathrm{Cl}(\mathcal{O}_n)$ on the canonical orbit $\rho(\mathrm{Ell}(\mathcal{O}_n))$ for $n \in \mathbb{N}$ big enough. By Theorem 1, this is a cryptographic group action.

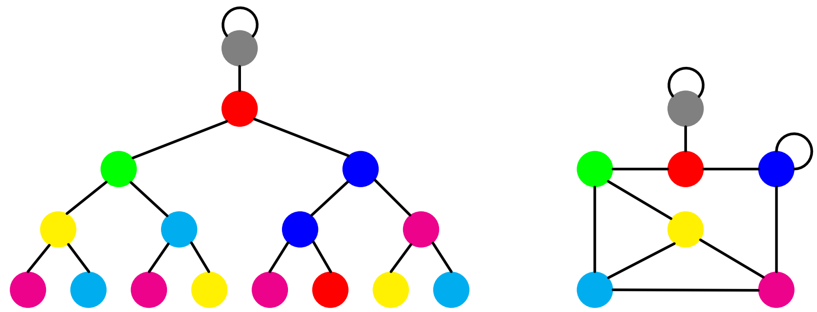

Fig. 1. On the left: Representation of a connected component (with volcano structure) of $G_2(\mathbb{Q}(i), 79)$, the $\mathbb{Q}(i)$-oriented supersingular 2-isogeny graph over $\mathbb{F}_{79^2}$ up to depth 4. **On the right :** Supersingular 2-isogeny graph over $\mathbb{F}_{79^2}$ (left graph refolded). **NB:** Elliptic curves with the same color have the same j-invariant.

Unfortunately, there is no known algorithm to compute the group action on $\rho(\mathrm{Ell}(\mathcal{O}_n))$ directly. Colò and Kohel's trick is to work in the K-oriented supersingular ℓ-isogeny graph. Instead of considering a vertex $(E_n, \iota_n) \in \rho(\mathrm{Ell}(\mathcal{O}_n))$ alone, we consider the *descending chain* of K-oriented ℓ-isogenies in the graph:

$$(E_0, \iota_0) \longrightarrow \cdots \longrightarrow (E_n, \iota_n),$$

with $(E_i, \iota_i) \in \rho(\mathrm{Ell}(\mathcal{O}_i))$ for all $i \in [\![1\ ;\ n]\!]$.

Let $\mathfrak{q} \subseteq \mathcal{O}_K$ be an ideal of norm prime to ℓ and p. Then, we have a commutative diagram of K-oriented isogenies:

$$\begin{array}{ccccccccc} (E_0, \iota_0) & \longrightarrow & (E_1, \iota_1) & \longrightarrow & \cdots & \longrightarrow & (E_{n-1}, \iota_{n-1}) & \longrightarrow & (E_n, \iota_n) \\ \downarrow & & \downarrow & & & & \downarrow & & \downarrow \\ (F_0, \iota'_0) & \longrightarrow & (F_1, \iota'_1) & \longrightarrow & \cdots & \longrightarrow & (F_{n-1}, \iota_{n-1}) & \longrightarrow & (F_n, \iota'_n), \end{array}$$

where $(F_i, \iota'_i) := (\mathfrak{q} \cap \mathcal{O}_i) \cdot (E_i, \iota_i)$, for all $i \in [\![0\ ;\ n]\!]$, the down arrows are the isogenies associated to the $\mathfrak{q} \cap \mathcal{O}_i$ and the arrows between the (F_i, ι'_i) are ℓ-isogenies. Such a diagram is called an *ℓ-ladder of degree* $q := N(\mathfrak{q})$ and the chain at the bottom $(F_i, \iota'_i)_{0 \le i \le n}$ is also denoted by $\mathfrak{q} \cdot (E_i, \iota_i)_{0 \le i \le n}$.

When the norm q is a small prime number, the descending ℓ-isogeny chain $(F_i, \iota'_i)_{0 \le i \le n}$ can be easily computed, assuming $(E_i, \iota_i)_{0 \le i \le n}$ is known. The ending element is the result of the group action by $\mathfrak{q} \cap \mathcal{O}_n$ we wanted to compute in the first place: $(F_n, \iota'_n) := (\mathfrak{q} \cap \mathcal{O}_n) \cdot (E_n, \iota_n)$. Assuming that $p > q\ell^{2n}|\operatorname{disc}(K)|$, we can perform this computation with j-invariants only and omit the orientations (this is a consequence of Theorem 2, see [35, Theorem 6.2]).

Assume that $j(F_i)$ is known. Then, $j(F_{i+1})$ is solution of the modular equations:

$$\begin{cases} \Phi_\ell(j(F_i), x) = 0 \\ \Phi_q(j(E_{i+1}), x) = 0 \end{cases} \iff \quad \gcd(\Phi_\ell(j(F_i), x), \Phi_q(j(E_{i+1}), x)) = 0. \qquad (\star_i)$$

For i big enough, Eq. ($\star_i$) admits only one solution [35, Theorem 6.2], so we can easily go down the chain of F_i.

To compute the first values of $j(F_i)$ we cannot use Eq. ($\star_i$) because there are multiple solutions (both $j(F_i) = j(\mathfrak{q} \cdot E_i)$ and $j(\overline{\mathfrak{q}} \cdot E_i)$ are solutions). Hence, we explicitly compute the torsion subgroups $E_i[\mathfrak{q} \cap \mathcal{O}_i]$ and use Vélu's formulas [46]. Colò and Kohel choose K so that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial ($K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ in practive), so that $j(F_0) = j(E_0)$ and we save the first computation.

With this algorithm, we can compute the ideal class group action, as visualized in Figure 2.

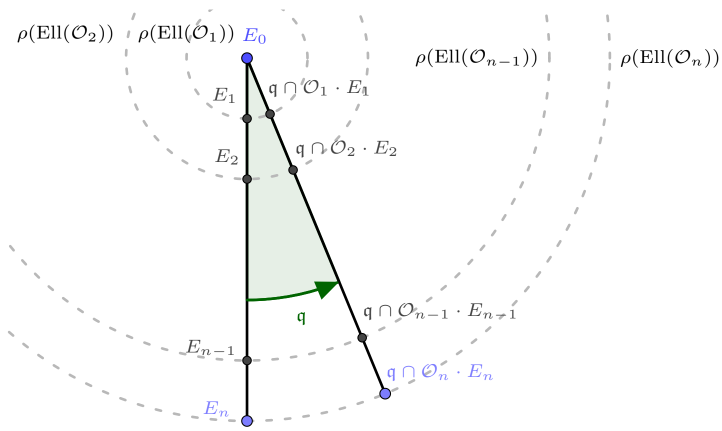

Fig. 2. Action of the prime ideal $\mathfrak{q}$ on the descending ℓ-isogeny chain.

3 Oriented Supersingular Isogeny Diffie–Hellman

The material of this section mostly replicates Colò and Kohel [17]. Nonetheless, in Section 3.3 we give a more detailed account of the attack on their straw man key exchange [17, § 5.1], and we improve it using lattice reduction.

3.1 The OSIDH setup

As explained in Section 2.4, we choose a quadratic imaginary number field K such that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial ($K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$), ℓ a small prime and p a large prime that does not split in K (cf. Proposition 1). Let $\mathcal{O}_i := \mathbb{Z} + \ell^i \mathcal{O}_K$ for all $i \in \mathbb{N}^*$ and $n \in \mathbb{N}^*$ large enough. OSIDH uses the group action of $\mathrm{Cl}(\mathcal{O}_n)$ on the orbit $\rho(\mathrm{Ell}(\mathcal{O}_n))$.

According to the terminology of [2], this is a restricted cryptographic group action (REGA), because we can use the algorithm of Section 2.4 with (prime) ideals of small norm only. Hence, we choose a set of generators: let $q_1, \ldots, q_t$ be small distinct primes, distinct from ℓ, and all splitting in K, and let $\mathfrak{q}_j$ be prime $\mathcal{O}_K$-ideals lying above q_j for all $j \in [\![1 \; ; \; t]\!]$. We assume that the $\mathfrak{q}_j \cap \mathcal{O}_n$ genrate $\mathrm{Cl}(\mathcal{O}_n)$.

3.2 A straw man key exchange scheme

With the setup of the previous section, let $(E_i, \iota_i)_{0 \leq i \leq n}$ be a public descending ℓ-isogeny chain (represented as a list of j-invariants) such that E_0 is primitively $\mathcal{O}_K$-oriented.

Alice and Bob separately choose secret exponents $e_1, \dots, e_t$ and $f_1, \dots, f_t$ lying in the integer range $[\![-r \; ; \; r]\!]$ (where r is a small positive integer) and respectively compute the action of

$$\mathfrak{a} := \prod_{j=1}^{t} \mathfrak{q}_j^{e_j} \qquad \text{and} \qquad \mathfrak{b} := \prod_{j=1}^{t} \mathfrak{q}_j^{f_j}$$

on $(E_i, \iota_i)_{0 \leq i \leq n}$ step by step, using the method of Section 2.4.

Then, Alice sends $\mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$ to Bob (as a list of j-invariants) and Bob sends $\mathfrak{b} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$ to Alice. In the end, Alice computes $\mathfrak{a} \cdot (\mathfrak{b} \cdot (E_i, \iota_i)_{0 \leq i \leq n})$ and Bob computes $\mathfrak{b} \cdot (\mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n})$, so that both parties share the chain

$$\mathfrak{a} \cdot (\mathfrak{b} \cdot (E_i, \iota_i)_{0 \leq i \leq n}) = \mathfrak{b} \cdot (\mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}) = \mathfrak{a}\mathfrak{b} \cdot (E_i, \iota_i)_{0 \leq i \leq n}.$$

We shall now see that this protocol is insecure: given knowledge of the chain $(E_i, \iota_i)_{0 \leq i \leq n}$ and of, say, $\mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$, an attacker can recover the secret ideal class $[\mathfrak{a}]$.

3.3 Inverting the class group action on descending chains

Given two chains $(E_i, \iota_i)_{0 \leq i \leq n}$ and $(F_i, \iota'_i)_{0 \leq i \leq n} := \mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$ with a secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$, we explain how to recover $[\mathfrak{a}]$. As Colò and Kohel indicate [17, § 5.1], there are two methods to do that. The first one exploits the chains to recover the full endomorphism rings $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$ [24,48], then computes a connecting ideal between those quaternion orders [31], and finally finds an equivalent ideal in $\mathcal{O}_n$. The second method, which we are now going to illustrate, only uses the ideal class group action.

For $i \in [\![0 \; ; \; n-1]\!]$, suppose that we know an ideal of $\mathfrak{a}_i = \prod_{j=1}^{t} \mathfrak{q}_j^{e_{i,j}}$ of $\mathcal{O}_K$, such that

$$\mathfrak{a}_i \cdot (E_k, \iota_k)_{0 \leq k \leq i} = (F_k, \iota'_k)_{0 \leq k \leq i}.$$

Then $[\mathfrak{a} \cap \mathcal{O}_i] = [\mathfrak{a}_i \cap \mathcal{O}_i]$ in $\mathrm{Cl}(\mathcal{O}_i)$ and $\mathfrak{a}_i \cap \mathcal{O}_i$ is determined up to multiplication by principal ideals of $\mathcal{O}_i$, *i.e.* by elements of $\mathcal{O}_i$. We look for an ideal $\mathfrak{a}_{i+1} = \prod_{j=1}^{t} \mathfrak{q}_j^{e_{i+1,j}}$ of $\mathcal{O}_K$ such that

$$\mathfrak{a}_{i+1} \cdot (E_k, \iota_k)_{0 \leq k \leq i+1} = (F_k, \iota'_k)_{0 \leq k \leq i+1}.$$

Then, $[\mathfrak{a}_{i+1} \cap \mathcal{O}_i] = [\mathfrak{a} \cap \mathcal{O}_i] = [\mathfrak{a}_i \cap \mathcal{O}_i]$ is in $\mathrm{Cl}(\mathcal{O}_i)$, *i.e.* $\mathfrak{a}_{i+1} \cap \mathcal{O}_i \equiv \mathfrak{a}_i \cap \mathcal{O}_i \mod P(\mathcal{O}_i)$. Hence, to determine $\mathfrak{a}_{i+1}$, one only has to find an ideal $\mathfrak{b}_i = \prod_{j=1}^{t} \mathfrak{q}_j^{d_j}$ such that $\mathfrak{b}_i \cap \mathcal{O}_i$ is principal and

$$[(\mathfrak{a}_i \cdot \mathfrak{b}_i) \cap \mathcal{O}_{i+1}] \cdot E_{i+1} = F_{i+1}. \qquad (\star)$$

Then, we can set $\mathfrak{a}_{i+1} := \mathfrak{a}_i \cdot \mathfrak{b}_i$, so that $e_{i+1,j} := e_{i,j} + d_j$ for all $j \in [\![1 \; ; \; t]\!]$. Both $\mathfrak{a}_{i+1} \cap \mathcal{O}_{i+1}$ and $\mathfrak{b}_i \cap \mathcal{O}_{i+1}$ are determined up to principal ideals of $\mathcal{O}_{i+1}$, thus $[\mathfrak{b}_i \cap \mathcal{O}_{i+1}]$ is in the kernel of the surjective group homomorphism

$$[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow [\mathfrak{c}\mathcal{O}_i] \in \mathrm{Cl}(\mathcal{O}_i),$$

whose order is ℓ for $i \geq 1$ and $\frac{1}{[\mathcal{O}_K^\times : \mathcal{O}_1^\times]} \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right)$ for $i = 0$ (by [19, Theorem 7.24]), so we only have to test a few values for $\mathfrak{b}_i$ until Eq. ($\star$) is satisfied.

However, we have to make sure that all the values of $\mathfrak{b}_i$ to be tested can be expressed in terms of the $\mathfrak{q}_j$, and that the exponents $e_{i+1,j}$ of $\mathfrak{a}_i \cdot \mathfrak{b}_i$ are short enough to make the computation of $[(\mathfrak{a}_i \cdot \mathfrak{b}_i) \cap \mathcal{O}_{i+1}] \cdot E_{i+1}$ practical.

Expressing $\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_i))$ in terms of the $\mathfrak{q}_j$. We need to investigate the structure of the ideal class groups, which turns out to be very simple.

Lemma 1. *One of the following results hold:*

(i) *For all $n \geq 1$, $\mathrm{Cl}(\mathcal{O}_n)$ is cyclic.*
(ii) *For all $n \geq 2$, $\mathrm{Cl}(\mathcal{O}_n) \simeq (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/h_{n-1}\mathbb{Z})$ with*

$$h_{n-1} := \# \mathrm{Cl}(\mathcal{O}_{n-1}) = \frac{\ell^{n-2}}{[\mathcal{O}_K^\times : \mathcal{O}_1^\times]} \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right),$$

where $\Delta_K := \mathrm{disc}(K)$.

The last case only happens when $\ell = 2$ or when $\ell \geq 3$ ramifies in K (this condition is necessary but not sufficient).

Proof. See appendix A.

The result above leads to a straightforward way to express $\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_i))$. The strategy is to first use Algorithm 1 to compute a basis of $\mathrm{Cl}(\mathcal{O}_n)$ *i.e.* a generator or a pair of generators without non trivial relations. Then to use Algorithm 2 to express the kernels for $i \in [\![0 \; ; \; n-1]\!]$. Both algorithms require discrete logarithm computations in the class group, however these only take polynomial time in n, since the order is smooth [38].

Algorithm 1: Computing a basis of $\mathrm{Cl}(\mathcal{O}_n)$.

Data: $\mathfrak{q}_1, \cdots, \mathfrak{q}_j$, n.
Result: A basis of $\mathrm{Cl}(\mathcal{O}_n)$.

Compute the order d_j of $[\mathfrak{q}_j] \in \mathrm{Cl}(\mathcal{O}_n)$ for all $j \in [\![1\ ;\ t]\!]$;
$m \leftarrow \mathrm{lcm}_{1 \leq j \leq t}\, d_j$;
Find a product of the $[\mathfrak{q}_j]$, $[\mathfrak{g}]$ of order m in $\mathrm{Cl}(\mathcal{O}_n)$;
if $m = \#\,\mathrm{Cl}(\mathcal{O}_n)$ **then**
  Return $\mathfrak{g}$;
else
  Find $[\mathfrak{q}_j] \notin \langle [\mathfrak{g}] \rangle$ (try to compute the discrete logarithm until it fails);
  Compute the discrete logarithm k of $[\mathfrak{q}_j]^\ell$ to base $[\mathfrak{g}]$; // $[\mathfrak{q}_j]^\ell \in \langle [\mathfrak{g}] \rangle$
  $k' \leftarrow k/\ell$; // $\ell \mid k$ since $[\mathfrak{q}_j]^\ell$'s order divides m/ℓ
  $[\mathfrak{h}] \leftarrow [\mathfrak{q}_j][\mathfrak{g}]^{-k'}$;
  Return $([\mathfrak{g}], [\mathfrak{h}])$;
end

Algorithm 2: Expressing $\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_i))$ in terms of the $\mathfrak{q}_j$.

Data: $\mathfrak{q}_1, \cdots, \mathfrak{q}_j$, a basis of $\mathrm{Cl}(\mathcal{O}_n)$, $i \in [\![0\ ;\ n-1]\!]$.
Result: A generator of $\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_i))$ in terms of the $\mathfrak{q}_j$.

if $\#\,\mathrm{Cl}(\mathcal{O}_n)$ *is cyclic* **then**
  $[\mathfrak{g}] \leftarrow$ entry generator of $\mathrm{Cl}(\mathcal{O}_n)$;
  $h_i \leftarrow \#\,\mathrm{Cl}(\mathcal{O}_i)$;
  Return $[\mathfrak{g} \cap \mathcal{O}_{i+1}]^{h_i}$;
else
  if $i \geq 3$ **then**
    $([\mathfrak{g}], [\mathfrak{h}]) \leftarrow$ entry basis of $\mathrm{Cl}(\mathcal{O}_n)$;
    $h_{i-1} \leftarrow \#\,\mathrm{Cl}(\mathcal{O}_i)/\ell$;
    Return $[\mathfrak{g} \cap \mathcal{O}_{i+1}]^{h_{i-1}}$;
  else
    Describe the kernel exhaustively;
  end
end

Reducing the exponents of $\mathfrak{a}_i \cdot \mathfrak{b}_i$. Once $\mathfrak{b}_i$ is expressed in terms of the $\mathfrak{q}_j$, *i.e.* when the exponents d_j are known, we still have to make sure that the exponents $e_{i+1,j} = e_{i,j} + d_j$ of $\mathfrak{a}_i \cdot \mathfrak{b}_i$ are small. We define the *relation lattice*

$$L_{i+1} := \left\{ (e_1, \ldots, e_t) \in \mathbb{Z}^t \,\middle|\, \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_{i+1}]^{e_j} = [1] \quad \text{in} \;\; \mathrm{Cl}(\mathcal{O}_{i+1}) \right\},$$

then two vectors $\mathbf{e}_{i+1} := (e_{i+1,j})_{1 \leq j \leq t}$ define the same element of $\mathrm{Cl}(\mathcal{O}_{i+1})$ if and only if they differ by an element of L_{i+1}. Thus we may compute L_{i+1} and then find an element $\mathbf{c} \in L_{i+1}$ close to $\mathbf{e}_{i+1}$, so to replace $\mathbf{e}_{i+1}$ by $\mathbf{e}'_{i+1} := \mathbf{e}_i - \mathbf{c}$.

We explain how to compute a basis of L_{i+1} when $\mathrm{Cl}(\mathcal{O}_{i+1})$ is cyclic. To do so, we start by computing a generator $[\mathfrak{g}]$ of $\mathrm{Cl}(\mathcal{O}_{i+1})$ using Algorithm 1. Then, we compute the discrete logarithms x_j of the $[\mathfrak{q}_j]$ to base $[\mathfrak{g}]$, which is easily done since $\mathrm{Cl}(\mathcal{O}_{i+1})$ has smooth order. Define the row vector $\mathbf{x} := (x_1, \ldots, x_t)$, and let $h_{i+1} = \#\,\mathrm{Cl}(\mathcal{O}_{i+1})$, then

$$L_{i+1} := \left\{ \mathbf{e} \in \mathbb{Z}^t \;\middle|\; \forall k \in [\![1\ ;\ r]\!], \quad \mathbf{x} \cdot \mathbf{e} \equiv 0\ [h_{i+1}] \right\},$$

where $\mathbf{x} \cdot \mathbf{e}$ denotes the dot product. The dual of this lattice is

$$L_{i+1}^* := \mathbb{Z}^t + \mathbb{Z}\frac{1}{h_{i+1}}\mathbf{x}^T,$$

so we easily find a basis C of L_{i+1}^* by computing the Hermite Normal Form of the matrix $(h_{i+1}I_t|\mathbf{x}^T)$, using [15, Algorithm 2.4.4]. Then, $B := (C^T)^{-1}$ is a basis of L_{i+1}.

When $\mathrm{Cl}(\mathcal{O}_{i+1})$ is not cyclic, we proceed similarly. We find a basis $([\mathfrak{g}], [\mathfrak{h}])$ using Algorithm 1, we compute the discrete logarithm (x_j, y_j) of the $[\mathfrak{q}_j]$ to this base, using Sutherland's Algorithm [43, Algorithm 2]. L_{i+1} is now defined by two equations $\mathbf{x} \cdot \mathbf{e} \equiv 0\ [h_i]$ and $\mathbf{y} \cdot \mathbf{e} \equiv 0\ [\ell]$, with $\mathbf{x} := (x_1, \ldots, x_t)$, $\mathbf{y} := (y_1, \ldots, y_t)$ and $h_i := \#\,\mathrm{Cl}(\mathcal{O}_i)$. The basis C of L_{i+1}^* is the Hermite Normal Form of the matrix $(h_i \ell I_t | \ell \mathbf{x}^T | h_i \mathbf{y}^T)$, and finally $B := (C^T)^{-1}$ is a basis of L_{i+1}.

All these operations are polynomial in $i \leq n$ and t. To find a vector $\mathbf{c} \in L_{i+1}$, close to $\mathbf{e}_{i+1}$ we can use Babai's nearest plane algorithm [3] running in time $O(t^6)$. Theoretically, the distance $\|\mathbf{c} - \mathbf{e}_{i+1}\|$ (in norm ℓ_2) will be exponential but in practice, for $t \sim 10^2$, this distance will be reasonably low, making this attack practical.

For bigger values of t, one has to find a balance between the time complexity of the CVP algorithm and the distance $\|\mathbf{c} - \mathbf{e}_{i+1}\|$, closely related to the time complexity of the operation $[\mathfrak{a}_i \cdot \mathfrak{b}] \cdot E_{i+1}$. This could be done with Espitau and Kirchner's algorithm [25], leading to a subexponential attack of time complexity $L_t[1/2, c] = \exp((c + o(1))\sqrt{t \log(t)})$, with $c \simeq 0.229$ (see Appendix B). To reach a security level of 128 bits would require to take $t \geq 3 \cdot 10^4$, which is unrealistic.

3.4 The OSIDH key exchange

To obtain a secure key exchange, one must avoid publishing the full chains $\mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$ and $\mathfrak{b} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$. Ideally, Alice and Bob would only exchange the final elements $E_{A,n} := [\mathfrak{a}] \cdot E_n$ and $E_{B,n} := [\mathfrak{b}] \cdot E_n$. However, this is not enough information for one party to evaluate the group action on the other party's public curve. Colò and Kohel proposed that the parties exchange the horizontal chains

$$[\mathfrak{q}_j]^{-r} \cdot E_{A,n} \to \cdots \to E_{A,n} \to \cdots \to [\mathfrak{q}_j]^r \cdot E_{A,n}$$

$$\text{and} \quad [\mathfrak{q}_j]^{-r} \cdot E_{B,n} \to \cdots \to E_{B,n} \to \cdots \to [\mathfrak{q}_j]^r \cdot E_{B,n}$$

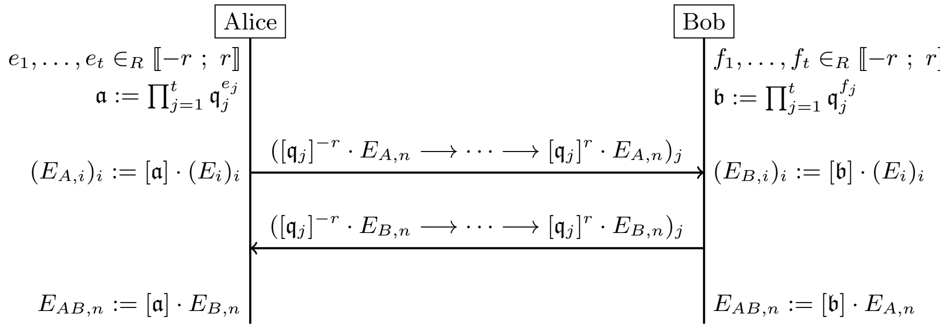

Fig. 3. The OSIDH protocol as presented in [17, § 5.2].

for all $j \in [\![1 \;;\; t]\!]$, instead. This is sufficient to compute $[\mathfrak{a}] \cdot E_{B,n}$ and $[\mathfrak{b}] \cdot E_{A,n}$, provided the exponents occurring in $\mathfrak{a}$ and $\mathfrak{b}$ are chosen in $[\![-r \;;\; r]\!]$. See [17, § 5.2] for details.

Colò and Kohel conjecture that this additional information cannot be leveraged to find the secrets, then, in [17, § 6], suggest a concrete set of parameters inspired by CSIDH-512. Concretely, they take $K = \mathbb{Q}(i)$, $\ell = 2$, and $n = 256$, to obtain a class group of size $\approx 2^{256}$, ensuring 2^{128} security against meet-in-the-middle attacks. Then, like in CSIDH, they set $r = 5$ and $t = 74$, so that $(2r+1)^t \approx 2^{256}$, which ensures that the secret key space covers nearly all of $\mathrm{Cl}(\mathcal{O}_n)$.

4 Our attack on OSIDH

As explained in Section 3.3, the knowledge of the descending ℓ-isogeny chains $(E_i, \iota_i)_{0 \le i \le n}$ and $(F_i, \iota'_i)_{0 \le i \le n} := [\mathfrak{a}] \cdot (E_i, \iota'_i)_{0 \le i \le n}$ is sufficient to recover the secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$. In this section, we prove that the knowledge of the $\mathfrak{q}_j$-action horizontal chains

$$[\mathfrak{q}_j]^{-r} \cdot F_n \to \cdots \to F_n \to \cdots \to [\mathfrak{q}_j]^{r} \cdot F_n$$

for all $j \in [\![1 \;;\; t]\!]$ may give away enough information to recover $(F_i, \iota'_i)_{0 \le i \le n}$, depending on the choice of parameters n, t and r.

4.1 Onuki's idea

In [35, § 6.3], Onuki claims that the knowledge of a K-oriented endomorphism $\iota'_n(\beta)$ with $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ is sufficient to recover the whole chain $(F_i, \iota'_i)_{0 \le i \le n}$.

We explain how such an endomorphism $\iota'_n(\beta)$ helps recover F_{n-1}, adapting the ideas of Petit's attack on SIDH [37] (in particular § 4.3). The same method can then be applied recursively to recover the whole chain. Let θ be a generator of $\mathcal{O}_K$. Then $\ell^n \theta$ generates $\mathcal{O}_n$ and we can write $\beta := a + b\ell^n\theta$ with $a, b \in \mathbb{Z}$ and $\ell \nmid b$ (since $\beta \notin \mathcal{O}_{n+1}$). Since $\iota'_n(a) = [a]$, we can infer $\iota'_n(b\ell^n\theta)$ from $\iota'_n(\beta)$.

Lemma 2. *We have* $\ker(\iota_n'(b\ell^n\theta))\cap F_n[\ell] = \ker(\widehat{\varphi}_{n-1})$, *where* $\varphi_{n-1} : F_{n-1} \longrightarrow F_n$ *is the last* K*-oriented isogeny of the chain* $(F_i, \iota_i')_{0\leq i\leq n}$.

Proof. Let $G := \ker(\iota_n'(b\ell^n\theta)) \cap F_n[\ell]$. We have

$$\iota_n'(b\ell^n\theta) = [\ell]\iota_n'(b\ell^{n-1}\theta) = \varphi_{n-1}\iota_{n-1}'(b\ell^{n-1}\theta)\widehat{\varphi}_{n-1}$$

and $b\ell^{n-1}\theta \in \mathcal{O}_{n-1}$, so that $\iota_{n-1}'(b\ell^{n-1}\theta) \in \mathrm{End}(F_{n-1})$, and consequently, $\ker(\widehat{\varphi}_{n-1}) \subseteq \ker(\iota_n'(b\ell^n\theta))$. Since $\deg(\varphi_{n-1}) = \ell$, we have also $\ker(\widehat{\varphi}_{n-1}) \subseteq F_n[\ell]$ so that $\ker(\widehat{\varphi}_{n-1}) \subseteq G$. So G is either cyclic of order ℓ and equal to $\ker(\widehat{\varphi}_{n-1})$ or of order ℓ^2 and equal to the entire ℓ-torsion subgroup $F_n[\ell]$. If the latter holds, $\iota_n'(b\ell^n\theta)$ factors through $[\ell]$ by [42, Corollary III.4.11] and $b\ell^{n-1}\theta \in \mathcal{O}_n$, so $\ell|b$. A contradiction. Hence, $G = \ker(\widehat{\varphi}_{n-1})$.

By the lemma, if we evaluate $\iota_n'(b\ell^n\theta)$ on $F_n[\ell]$, we can recover $\ker(\widehat{\varphi}_{n-1})$ and compute $\widehat{\varphi}_{n-1}$ with Vélu's formulas [46] to recover F_{n-1}. Using modular equations to push the chains using the algorithm of Section 2.4, we can also compute

$$[\mathfrak{q}_j]^{-r} \cdot F_{n-1} \to \cdots \to F_{n-1} \to \cdots \to [\mathfrak{q}_j]^r \cdot F_{n-1}$$

for all $j \in [\![1 ~;~ t]\!]$, with the knowledge of F_{n-1} and

$$[\mathfrak{q}_j]^{-r} \cdot F_n \to \cdots \to F_n \to \cdots \to [\mathfrak{q}_j]^r \cdot F_n.$$

Hence, we can apply our method recursively to recover the whole chain $(F_i)_{0\leq i\leq n}$.

Now, the problem is to find a K-oriented endomorphism $\iota_n'(\beta)$ with $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$. Onuki suggests to find β such that $\beta\mathcal{O}_n = I\cdot J$, where $I := \prod_{j=1}^t(\mathfrak{q}_j\cap\mathcal{O}_n)^{e_j}$ with $e_1, \cdots, e_t \in [\![-r ~;~ r]\!]$ and J is an $\mathcal{O}_n$-ideal of norm as small as possible. Then $\iota_n'(\beta)$ will be a composite of the isogenies $F_n \longrightarrow [I]\cdot F_n$ with kernel $F_n[I]$ and $[I]\cdot F_n \longrightarrow [IJ]\cdot F_n = F_n$, with kernel $[I]\cdot F_n[J]$. The first isogeny can be computed with the knowledge of the $\mathfrak{q}_j$-action chains

$$[\mathfrak{q}_j]^{-r} \cdot F_n \to \cdots \to F_n \to \cdots \to [\mathfrak{q}_j]^r \cdot F_n$$

for all $j \in [\![1 ~;~ t]\!]$ (applying the method of [17, § 5.2]). Onuki suggests a meet-in-the middle exhaustive search strategy to compute the second isogeny. However, there is no guarantee that we find a K-oriented isogeny with this method (which is essential for the attack to work). Besides, Onuki's attack is very costly. It not only requires the computation of the second isogeny (in $\Omega(\sqrt{N(J)})$ operations) but it also requires, before that, an exhaustive search for $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ with a big factor $I = \prod_{j=1}^t(\mathfrak{q}_j \cap \mathcal{O}_n)^{e_j}$ and a small factor J. The time complexity of such an attack is $\Omega(\ell^{2n/3}/(r+1)^{t/3})$ (see Appendix C). Hence, it would require more than 2^{100} operations with Colò and Kohel's parameters ($n = 256$, $t = 74$, $\ell = 2$ and $r = 5$). In [35, §6.3], Onuki underestimated the complexity as he neglected the exhaustive search for β, which led him to recommend $n \geq 10^3$.

In the following, we present another method based on a lattice reduction to find $\iota_n'(\beta)$ that breaks Colò and Kohel's parameters.

4.2 Finding endomorphisms via relations

Let us assume that

$$\beta\mathcal{O}_n = \prod_{j=1}^{t} (\mathfrak{q}_j \cap \mathcal{O}_n)^{e_j},$$

with $e_1, \ldots, e_t \in [\![-2r \ ; \ 2r]\!]$ and write $e_j := e'_j + e''_j$ with $e'_j, e''_j \in [\![-r \ ; \ r]\!]$ for all $j \in [\![1 \ ; \ t]\!]$. Then, with the knowledge of the $\mathfrak{q}_j$-action horizontal chains

$$[\mathfrak{q}_j]^{-r} \cdot F_n \to \cdots \to F_n \to \cdots \to [\mathfrak{q}_j]^{r} \cdot F_n$$

for all $j \in [\![1 \ ; \ t]\!]$, we can compute the isogenies

$$\varphi : F_n \longrightarrow \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_j} \cdot F_n \quad \text{and} \quad \psi : F_n \longrightarrow \prod_{j=1}^{t} [\mathfrak{q}_j]^{-e''_j} \cdot F_n = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_j} \cdot F_n,$$

and finally compute $\iota'_n(\beta) = \widehat{\psi} \circ \varphi$.

Hence, to find a suitable β and compute $\iota'_n(\beta)$, it suffices to find a non-zero vector of ∞-norm $\leq 2r$ in the relation lattice of the $\mathfrak{q}_j$ in $\mathcal{O}_n$

$$L_n := \left\{ (e_1, \ldots, e_t) \in \mathbb{Z}^t \,\middle|\, \prod_{j=1}^{t} [\mathfrak{q}_j \cap \mathcal{O}_n]^{e_j} = [1] \quad \text{in } \mathrm{Cl}(\mathcal{O}_n) \right\}.$$

As explained in Section 3.3, L_n can be computed in polynomial time in n and t. But can we find short enough vectors in L_n? Assuming that L_n behaves as a random lattice, the following results answer this question with an estimate of the first minimum for the ∞-norm $\lambda_1^{(\infty)}(L_n)$.

Lemma 3 (Aono, Espitau and Nguyen [49, Theorem 11]).

(i) *The set $\mathcal{I}_{N,d}$ for full-rank sublattices of $\mathbb{Z}^d$ with covolume N is finite.*
(ii) *Let Λ be a random variable following the uniform distribution on $\mathcal{I}_{N,d}$. Then, for all $\varepsilon > 0$, there exists $d_0, N_0 \in \mathbb{N}^*$ such that for all $d \geq d_0$ and $N \geq N_0$*

$$\mathbb{P}\left[\left| \lambda_1^{(\infty)}(\Lambda) - \frac{N^{\frac{1}{d}}}{2} \right| \leq \frac{\log\log(d)}{d} \frac{N^{\frac{1}{d}}}{2} \right] \geq 1 - \varepsilon.$$

Proof. **(i)** $\mathcal{I}_{N,d}$ is in bijection with the matrices of $M_d(\mathbb{Z})$ in Hermite Normal Form with discriminant $\pm N$. (i) follows.

(ii) This result has already been proved in [49, Theorem 11] for the norm ℓ_2. The reasoning would be exactly the same here. We only have to replace the Gaussian Heuristic function $h(d) = 1/\operatorname{Vol}(B_2(0,1))^{1/d}$ by the constant $1/\operatorname{Vol}(B_\infty(0,1))^{1/d} = 1/2$ in the inequality.

Lemma 4. $\operatorname{Covol}(L_n) = \#\operatorname{Cl}(\mathcal{O}_n)$.

Proof. We have an exact sequence

$$\{0\} \longrightarrow L_n \longrightarrow \mathbb{Z}^t \longrightarrow \mathrm{Cl}(\mathcal{O}_n) \longrightarrow \{0\},$$

where the first map is the natural inclusion $L_n \subseteq \mathbb{Z}^t$ and the second one is

$$(e_1, \ldots, e_t) \in \mathbb{Z}^t \longmapsto \prod_{j=1}^{t} [\mathfrak{q}_j]^{e_j} \in \mathrm{Cl}(\mathcal{O}_n).$$

It is surjective because the $[\mathfrak{q}_j]$ generate $\mathrm{Cl}(\mathcal{O}_n)$. As a consequence, $\mathrm{Cl}(\mathcal{O}_n) \simeq \mathbb{Z}^t/L_n$, so that $\mathrm{Covol}(L_n) = \#(\mathbb{Z}^t/L_n) = \#\,\mathrm{Cl}(\mathcal{O}_n)$.

Colò and Kohel recommend to define a secret key space

$$\left\{ \prod_{j=1}^{t} [\mathfrak{q}_j]^{e_j} \;\middle|\; (e_1, \ldots, e_t) \in [\![-r\ ;\ r]\!]^t \right\}$$

large enough to (heuristically) cover all of $\mathrm{Cl}(\mathcal{O}_n)$ without many redundancies to make it computationally hard to find short cycles in the key space that break OSIDH, as explained earlier. This leads to $\mathrm{Covol}(L_n) = \#\,\mathrm{Cl}(\mathcal{O}_n) \simeq (2r+1)^t$. Assuming that L_n behaves as a random lattice in $\mathcal{I}_{\#\,\mathrm{Cl}(\mathcal{O}_n),t}$, we have

$$\lambda_1^{(\infty)}(L_n) \leq \left(1 + \frac{\log\log(t)}{t}\right) \frac{(\#\,\mathrm{Cl}(\mathcal{O}_n))^{\frac{1}{t}}}{2} \simeq \left(1 + \frac{\log\log(t)}{t}\right)\left(r + \frac{1}{2}\right) \leq 2r$$

for t big enough. Hence, we expect L_n to contain short enough vectors, thus enabling our attack, at least in theory.

Complexity analysis. All operations in our attack are polynomial in n and t on a classical computer, except the search for a nontrivial vector $\mathbf{e} \in L_n \setminus \{0\}$ such that $\|\mathbf{e}\|_\infty \leq 2r$, which takes exponential time in t. The most direct way to find $\mathbf{e}$ is to solve the shortest vector problem (SVP) in ∞-norm, and the best known algorithm for this is due to Aggarwal and Mukhopadhyay [1], and runs in heuristic time $2^{0.62t+o(t)}$. We have no theoretical guarantee that shortest vectors in ℓ_2 norm are shortest vectors in ∞-norm but there is a margin between $\lambda_1^{(\infty)}(L_n)$ and $2r$, so SVP algorithms in ℓ_2 norm are relevant here. The best SVP algorithm in ℓ_2 norm is due to Becker, Ducas, Gama and Laarhoven [4] and runs in time $(3/2)^{t/2+o(t)} \simeq 2^{0.292t+o(t)}$.

Neglecting polynomial terms and factors, we may assume that our attack runs in $2^{0.292t+o(t)}$. Thus, to reach 128 bits of classical security, we would have at the very least to take $t \approx 400$. As for other parameters, the setup of OSIDH requires $n \simeq t\log(2r+1)/\log(\ell)$ (since $\ell^n \simeq \#\,\mathrm{Cl}(\mathcal{O}_n) \simeq (2r+1)^t$), however we are going to argue that this bound is not sufficient for security.

4.3 Extending the attack by exhaustive search

As we saw, our attack is possible only when $\lambda_1^{(\infty)}(L_n) \leq 2r$ and this inequality always holds when the key space covers $\mathrm{Cl}(\mathcal{O}_n)$. When the key space is significantly smaller than $\mathrm{Cl}(\mathcal{O}_n)$, *i.e.* when $\#\,\mathrm{Cl}(\mathcal{O}_n) \gg (2r+1)^t$, Lemma 3 ensures that $\lambda_1^{(\infty)}(L_n) \simeq (\#\,\mathrm{Cl}(\mathcal{O}_n))^{1/t}/2 > 2r$. Nevertheless, we can extend the attack to address this case.

Let us assume that we found a short vector $\mathbf{e} \in L_n$ with norm $\|\mathbf{e}\|_\infty > 2r$. Then, we may write $\mathbf{e} := \mathbf{e}' + \mathbf{e}'' + \mathbf{d}$ with $\mathbf{e}', \mathbf{e}'', \mathbf{d} \in \mathbb{Z}^t$ such that $\|\mathbf{e}'\|_\infty = \|\mathbf{e}''\|_\infty = r$ and $\mathbf{d}$ has ∞-norm as small as possible. As previously, we can compute the K-oriented isogenies

$$\varphi : F_n \longrightarrow F' := \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_j} \cdot F_n \quad \text{and} \quad \psi : F_n \longrightarrow F'' := \prod_{j=1}^{t} [\mathfrak{q}_j]^{-e''_j} \cdot F_n.$$

with kernel $F_n[\prod_{j=1}^t [\mathfrak{q}_j]^{e'_j}]$ and $F_n[\prod_{j=1}^t [\mathfrak{q}_j]^{-e''_j}]$ respectively. In order to compute the endomorphism of F_n associated to $\mathbf{e}$ (whose kernel is $F_n[\prod_{j=1}^t \mathfrak{q}_j^{e_j}]$), it remains to compute the isogeny $F' \longrightarrow F''$ associated to $\mathbf{d}$ (whose kernel is $F'[\prod_{j=1}^t \mathfrak{q}_j^{d_j}]$). Following Onuki's idea, we compute this isogeny by a meet-in-the-middle style search. Let us write $\mathbf{d} := \mathbf{d}' + \mathbf{d}''$ with $d'_j := \lfloor d_j/2 \rfloor$ and $d''_j := d_j - d'_j$ for all $j \in [\![1 \ ; \ t]\!]$. We compute K-oriented isogenies

$$\phi : F' \longrightarrow \prod_{j=1}^{t} [\mathfrak{q}_j]^{d'_j} \cdot F' \quad \text{and} \quad \phi' : F'' \longrightarrow \prod_{j=1}^{t} [\mathfrak{q}_j]^{-d''_j} \cdot F'' = \prod_{j=1}^{t} [\mathfrak{q}_j]^{d'_j} \cdot F'$$

of kernel $F'[\prod_{j=1}^t [\mathfrak{q}_j]^{d'_j}]$ and $F''[\prod_{j=1}^t [\mathfrak{q}_j]^{-d''_j}]$ respectively, by exhaustively testing all isogenies of degree $\prod_{j=1}^t q_j^{|d'_j|}$ and $\prod_{j=1}^t q_j^{|d''_j|}$ respectively, until the codomains of ϕ and ϕ' match. In that case, the desired endomorphism will be the composite $\widehat{\psi} \circ \widehat{\phi'} \circ \phi \circ \varphi$. Note that, as in Onuki's attack, we have no theoretical guarantee that such an isogeny will actually be K-oriented (which is necessary to perform the attack). However, assuming the attack succeeds, we can estimate its complexity.

Proposition 2. *Under the heuristic assumption that L_n behaves like a random lattice among lattices of covolume $\#\,\mathrm{Cl}(\mathcal{O}_n)$ and that the shortest vector of L_n can be found in negligible time, our attack performs in time*

$$\Omega\left((q_1+1)^{\frac{1}{4}\ell^{n/t}-r}\right),$$

where $q_1 := N(\mathfrak{q}_1)$ is assumed to be the smallest prime among the $q_j := N(\mathfrak{q}_j)$ for $j \in [\![1 \ ; \ t]\!]$.

Proof. The dominant step in our attack is clearly the meet-in-the-middle search, and its time complexity is (up to polynomial factors)

$$\Omega\left(\prod_{j=1}^{t}(q_j+1)^{|d'_j|} + \prod_{j=1}^{t}(q_j+1)^{|d''_j|}\right).$$

Indeed, we search among all composites of chains of q_j-isogenies of length $|d'_j|$ and $|d''_j|$ for $j \in [\![1\ ;\ t]\!]$. Besides, by [42, Corollary III.4.11], we know that the number of isogenies of prime degree q is $q+1$. The number of isogenies to test, and the time complexity of our exhaustive search follows. By assumption, $\mathbf{d}'$ and $\mathbf{d}''$ cut $\mathbf{d}$ in half and $\mathbf{e} = \mathbf{e}' + \mathbf{e}'' + \mathbf{d}$, so that

$$\|\mathbf{e}\|_\infty \leq \|\mathbf{e}'\|_\infty + \|\mathbf{e}''\|_\infty + \|\mathbf{d}\|_\infty = 2r + \|\mathbf{d}\|_\infty$$

and $\|\mathbf{d}\|_\infty \geq \|\mathbf{e}\|_\infty - 2r \geq \lambda_1^{(\infty)}(L) - 2r$. But by Lemma 3, we have

$$\lambda_1^{(\infty)}(L) \geq \left(1 - \frac{\log\log(t)}{t}\right) \frac{(\#\,\mathrm{Cl}(\mathcal{O}_n))^{\frac{1}{t}}}{2} \underset{t\to+\infty}{\sim} \frac{\ell^{\frac{n}{t}}}{2}.$$

The result follows.

In conclusion, to ensure an asymptotic security level of λ bits, we would need

$$(q_1+1)^{\frac{1}{4}\ell^{n/t}-r} \geq 2^\lambda \iff n \geq \frac{t}{\log(\ell)} \log\left(4r + \frac{4\lambda\log(2)}{\log(q_1+1)}\right).$$

Note that initially, Colò and Kohel proposed $n \simeq t\log(2r+1)/\log(\ell)$, so this bound is more restrictive.

4.4 Implementation of our attack

Tests on toy parameters. We implemented the OSIDH protocol and our attack in `Sagemath` [45] for toy parameters: $\ell = 2$, $r = 3$, $t = 10$, $n = 28$ and $K = \mathbb{Q}(i)$. The source code can be found on `Github`[5]. The attack is divided into three steps:

Step 1: Our lattice based chain recovery of both Alice's and Bob's chains.
Step 2: A recovery of Alice's ideal class using the algorithm presented in Section 3.2.
Step 3: The shared secret chain computation by acting with Alice's ideal class on Bob's chain.

Time performance results were obtained from a sample of 60 executions on a Mac Book Pro mid-2015 equipped with an Intel Core i7-4870HQ clocked at 2.5 GHz. They are presented in the following table:

	Protocol	Chain attack (half of step 1)	Step 2	Step 3	Complete attack
Average (in s)	84.83	135.44	98.19	6.97	376.05
Standard deviation (in s)	5.61	7.15	13.06	1.61	18.29
Margin of error (95 %) on the average (in s)	1.46	1.90	3.40	0.42	4.76

For the modular polynomials that were used in our implementation, we give credit to Sutherland's online database[6] computed with the algorithms of [12].

[5] See `https://github.com/Pierrick-Dartois/OSIDH`.
[6] See `https://math.mit.edu/~drew/ClassicalModPolys.html`.

Attacking real parameters. For 128 bits of classical security, Colò and Kohel suggest $\ell = 2$, $r = 5$, $t = 74$, $n = 256$ and $K = \mathbb{Q}(i)$. Our implementation of the full attack cannot handle such parameters, however our attempt at implementing the OSIDH protocol itself cannot handle them either. In fact, we are not aware of any implementation of OSIDH using the parameters originally suggested in [17, § 6].

Ironically, the practical bottleneck in the attack is not the exponential time lattice reduction step, but rather the class group action computation, which is essentially shared with OSIDH itself, and which runs in polynomial time (see Lemma 5). The culprit are the extremely large modular polynomials that the implementation needs to handle, requiring several GB of storage.

On the contrary, the lattice reduction step in the attack can easily handle the real parameters, and much more. Indeed, we were able to compute the relation lattice L_n for the originally proposed parameters in 64 minutes. Most of this time was spent computing the (polynomial time) discrete logarithms, while the lattice reduction step, performed via `fpylll`'s implementation of BKZ [44,40] with block size $k = 4$, found a vector $\mathbf{e} \in L_n$ of ∞-norm $\|\mathbf{e}\|_\infty = 9 < 2r$ in less than 0.5 s.

In conclusion, we believe that our lattice based attack could be very efficient in practice for the originally proposed parameters, as well as larger ones, provided one is able to efficiently implement OSIDH itself.

5 Countermeasures

Because our attack has exponential complexity, it is still possible to safely instantiate OSIDH by increasing parameters. We analyze here the available options.

5.1 Increase t, and everything else

The simplest countermeasure is to increase the number t of prime ideals $\mathfrak{q}_j$, which governs the dimension of the relation lattice, to the point where solving SVP becomes infeasible. As we saw in Section 4.2 if we use the Becker–Ducas–Gama–Laarhoven algorithm [4] to solve SVP in norm ℓ_2, we need at least $t \approx 400$ to achieve 128 bits of classical security. However, the size of $\mathrm{Cl}(\mathcal{O}_n)$, and thus the prime p, shall be increased accordingly to satisfy $\#\,\mathrm{Cl}(\mathcal{O}_n) \approx (2r+1)^t$. Otherwise, we could consider only the $t' < t$ first $\mathfrak{q}_j$ (where t' is such that $\#\,\mathrm{Cl}(\mathcal{O}_n) \approx (2r+1)^{t'}$) and still perform our attack with a smaller relation lattice of dimension t'. We may partly compensate this increase of t by decreasing r; we may in fact even restrict to just three values ($r = 1$) for the secret exponents, *e.g.* $e_j \in \{-1, 0, 1\}$. With $t \approx 400$, $\ell = 2$ and $r = 1$, this would lead to $n \approx 630$.

This increase is significant compared to $n = 256, t = 74$ as suggested by Colò and Kohel, or even $n = 1428, t = 100$ as suggested by Onuki [17, § 6.3], and we expect them to severely affect performance, as the following analysis indicates.

Lemma 5. *Let $(E_i)_{0\leq i\leq n}$ be a descending ℓ-isogeny chain such that E_0 is $\mathcal{O}_K$-oriented and $\mathfrak{a} := \prod_{j=1}^t \mathfrak{q}_j^{e_j}$ with $e_1, \dots, e_t$ sampled in $[\![-r \ ; \ r]\!]$. Then, the computation of $\mathfrak{a}\cdot(E_i)_{0\leq i\leq n}$ requires $O(nt^3\log^2(t)+n^2)$ operations over $\mathbb{F}_{p^2}$ on average, with the constant inside O depending on r and ℓ.*

Proof. See Appendix D.

A possibly even worse consequence of this countermeasure is that it tightly binds the security of OSIDH to a lattice assumption. Qualitatively, security would look much worse than that of any lattice based scheme, since it appears to be impossible to prove any kind of security reduction of OSIDH to a standard lattice problem. Quantitatively, it seems hard to justify the practical interest of such a slow scheme, when lattice based schemes are several orders of magnitude faster.

5.2 Increase $\#\,\mathrm{Cl}(\mathcal{O}_n)$, keep the same key space

Alternatively, we may ensure that $\#\,\mathrm{Cl}(\mathcal{O}_n)\simeq\ell^n$ is much larger than $(2r+1)^t$, so that the key space

$$\left\{\prod_{j=1}^t[\mathfrak{q}_j]^{e_j} \mid (e_1,\dots,e_t)\in[\![-r \ ; \ r]\!]^t\right\}$$

is far from covering all of $\mathrm{Cl}(\mathcal{O}_n)$, and thus $\lambda_1^{(\infty)}(L_n) > 2r$. The analysis in Section 4.3 suggests taking

$$n \geq \frac{t}{\log(\ell)}\log\left(4r+\frac{4\lambda\log(2)}{\log(q_1+1)}\right)$$

for a security level of λ bits.

We can adapt Colò and Kohel's choice of parameters ($K=\mathbb{Q}(i), \ell=2, r=5, t=74$) by taking $n=575$ instead of $n=256$ to attain $\lambda=128$ bits of security. The increase for n, and thus for p, is roughly comparable to the previous countermeasure; however, by keeping the same value for t, we do not need to introduce larger modular polynomials, and can thus hope for a significantly faster result.

Onuki's choice of parameters in [35, §6.3] ($n=1428$, $t=100$, $\ell=2$, $r=3$ and $K=\mathbb{Q}(i)$) also follows this countermeasure but such an increase in n is not necessary and results form a cost underestimation of his attack, as we explained in Section 4.1.

5.3 OSIDH and cryptographic group actions

Besides affecting efficiency, both countermeasures also have adverse effects on the possibility of using the OSIDH group action in contexts other than key exchange. Brassard and Yung [11], then Couveignes [18], then Alamati, De Feo, Montgomery and Patranabis [2] established the axiomatic foundations of cryptographic group actions. The latter call Effective Group Action (EGA) a group action $(G, X, \cdot)$ where, among other axioms, the value $g \cdot x$ can be efficiently computed for any $g \in G$ and any $x \in X$. They also observe that CSIDH does not naturally satisfy this axiom, and thus define a better abstraction named Restricted Effective Group Actions (REGA), where $g \cdot x$ can be efficiently evaluated for any x, but only for a few g taken from a fixed list.

OSIDH satisfies neither the axioms of EGAs, nor of REGAs. Indeed, the class group action of OSIDH can only be computed with the help of the horizontal chains, however these are "single use": after computing $G_n := \left(\prod_j \mathfrak{q}_j^{e_j}\right) \cdot F_n$ there is no way to compute the horizontal chains for G_n without knowing the secret descending chain $(F_i)_{0 \leq i \leq n}$, and thus of evaluating a new action on G_n. Colò and Kohel did not claim anything else than a key exchange, and for that the limitations of OSIDH are not an issue. However it is natural to ask whether the same primitives that are known from the CSIDH group action can be built from the OSIDH action. This is where the countermeasures to our attack become an obstacle.

An important step for CSIDH was the computation of the class group structure of CSIDH-512, paved the way for the CSI-FiSh signature scheme [7]. Thanks to this intensive computational effort, it became possible to compute a reduced basis for the relation lattice of CSIDH-512, which is used to evaluate the action of arbitrary exponent vectors, much in the same way as we did in Section 13, thus effectively making CSIDH-512 into an EGA. The class group structure of OSIDH is much easier to compute than in CSIDH, and thus one may have hoped that the analogue of CSI-FiSh would be easy to define. However it is clear that we cannot ask the OSIDH relation lattice to be, at the same time, easy and hard to reduce: easy for a CSI-FiSh style CVP computation, and hard to prevent our attack. Thus, it would seem that neither CSI-FiSh, nor any of the applications derived from it [21,6,2], can be replicated in the OSIDH context.

Remark 1. There seems to be a small positive upside, though, to OSIDH not being a cryptographic group action in the usual sense: the best generic attacks against (R)EGA, both classical and quantum, do not seem to apply to OSIDH!

Indeed, the best classical attack against (R)EGAs is a Pollard Rho-style random walk algorithm [26,27], which necessitates to compute long random walks by chaining many group actions. This is not possible for OSIDH, for which we argued the group action can only be evaluated a limited number of times. The next best algorithm would be a meet-in-the-middle search, which has the same time complexity, but worse space complexity.

Possibly more remarkably, the best quantum algorithm against (R)EGAs is Kuperberg's subexponential algorithm for the hidden shift problem [32]. This algorithm repeatedly calls a quantum oracle that evaluates the group action in superposition for all possible group elements. If we apply the countermeasure of Section 5.2, then the OSIDH group action can only be evaluated on a negligibly small subset of the whole class group. It has already been remarked that Kuperberg algorithm doesn't appear to work when the oracle is only used to evaluate the action for a small fraction of the group elements [14], and thus wouldn't apply to this variant of OSIDH. The next best quantum against OSIDH would be, again, a meet-in-the-middle strategy, possibly applying some Grover-style accelerations [29], which has exponential complexity, putting OSIDH in a much better place than CSIDH regarding quantum security.

6 Conclusion

We presented a new classical attack against OSIDH that practically breaks the parameters proposed for 128 bits security. The attack has exponential complexity, and can thus be countered by increasing parameters. However the increased parameters heavily impact the performance of a scheme which is already very slow, and they also severely limit the number of other cryptographic primitives one may hope to derive from the OSIDH group action.

It must be stressed that there is, as of today, no reduction of the security of OSIDH to a well studied isogeny problem, and thus the security of the countermeasures we propose remains somewhat dubious. More scrutiny of the security assumptions supporting OSIDH would be beneficial.

Interestingly, we remarked that one of the countermeasures we propose appears to defeat not only our attack, but also Kuperberg's quantum attack. It would be interesting to investigate the quantum security of OSIDH more in depth.

None of the countermeasures we propose is particularly efficient, and OSIDH itself is challenging to implement. A detailed study of performance optimizations applicable to OSIDH, and of potential efficiency-minded variants, would be very welcome.

References

1. Aggarwal, D., Mukhopadhyay, P.: Improved algorithms for the shortest vector problem and the closest vector problem in the infinity norm (2018)
2. Alamati, N., De Feo, L., Montgomery, H., Patranabis, S.: Cryptographic group actions and applications. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 411–439. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_14
3. Babai, L.: On Lovász' lattice reduction and the nearest lattice point problem (shortened version). In: STACS (1985)
4. Becker, A., Ducas, L., Gama, N., Laarhoven, T.: New directions in nearest neighbor searching with applications to lattice sieving. In: Krauthgamer, R. (ed.) 27th SODA. pp. 10–24. ACM-SIAM (Jan 2016). https://doi.org/10.1137/1.9781611974331.ch2
5. Berlekamp, E.R.: Factoring polynomials over large finite fields. Mathematics of Computation **24**(111), 713–735 (1970), http://www.jstor.org/stable/2004849
6. Beullens, W., Katsumata, S., Pintore, F.: Calamari and Falafl: Logarithmic (linkable) ring signatures from isogenies and lattices. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 464–492. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_16

7. Beullens, W., Kleinjung, T., Vercauteren, F.: CSI-FiSh: Efficient isogeny based signatures through class group computations. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019, Part I. LNCS, vol. 11921, pp. 227–247. Springer, Heidelberg (Dec 2019). https://doi.org/10.1007/978-3-030-34578-5_9
8. Boneh, D., Kogan, D., Woo, K.: Oblivious pseudorandom functions from isogenies. In: Moriai, S., Wang, H. (eds.) ASIACRYPT 2020, Part II. LNCS, vol. 12492, pp. 520–550. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-64834-3_18
9. Bonnetain, X., Schrottenloher, A.: Quantum security analysis of CSIDH. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 493–522. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45724-2_17
10. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput. **24**(3-4), 235–265 (1997). https://doi.org/10.1006/jsco.1996.0125, http://dx.doi.org/10.1006/jsco.1996.0125, computational algebra and number theory (London, 1993)
11. Brassard, G., Yung, M.: One-way group actions. In: Menezes, A.J., Vanstone, S.A. (eds.) CRYPTO'90. LNCS, vol. 537, pp. 94–107. Springer, Heidelberg (Aug 1991). https://doi.org/10.1007/3-540-38424-3_7
12. Brker, R., Lauter, K., Sutherland, A.V.: Modular polynomials via isogeny volcanoes. Mathematics of Computation **81**(278), 12011231 (Jul 2011). https://doi.org/10.1090/s0025-5718-2011-02508-1, http://dx.doi.org/10.1090/S0025-5718-2011-02508-1
13. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: An efficient post-quantum commutative group action. In: Peyrin, T., Galbraith, S. (eds.) ASIACRYPT 2018, Part III. LNCS, vol. 11274, pp. 395–427. Springer, Heidelberg (Dec 2018). https://doi.org/10.1007/978-3-030-03332-3_15
14. Chavez-Saab, J., Chi-Dominguez, J.J., Jaques, S., Rodriguez-Henriquez, F.: The SQALE of CSIDH: square-root Vélu quantum-resistant isogeny action with low exponents. Cryptology ePrint Archive, Report 2020/1520 (2020), https://eprint.iacr.org/2020/1520
15. Cohen, H.: A Course in Computational Algebraic Number Theory. Springer-Verlag (1993)
16. Cohen, H.: Advanced Topics in Computational Algebraic Number Theory. Springer-Verlag (2000)
17. Colò, L., Kohel, D.: Orienting supersingular isogeny graphs. Journal of Mathematical Cryptology **14**(1), 414–437 (2020). https://doi.org/10.1515/jmc-2019-0034
18. Couveignes, J.M.: Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291 (2006), https://eprint.iacr.org/2006/291
19. Cox, D.A.: Primes of the form $x^2 + ny^2$. Wiley (2013)
20. De Feo, L., Galbraith, S.D.: SeaSign: Compact isogeny signatures from class group actions. In: Ishai, Y., Rijmen, V. (eds.) EUROCRYPT 2019, Part III. LNCS, vol. 11478, pp. 759–789. Springer, Heidelberg (May 2019). https://doi.org/10.1007/978-3-030-17659-4_26
21. De Feo, L., Meyer, M.: Threshold schemes from isogeny assumptions. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 187–212. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45388-6_7
22. de Saint Guilhem, C., Orsini, E., Petit, C., Smart, N.P.: Semi-commutative masking: A framework for isogeny-based protocols, with an application to fully secure two-round isogeny-based OT. In: Krenn, S., Shulman, H., Vaudenay, S.

(eds.) CANS 20. LNCS, vol. 12579, pp. 235–258. Springer, Heidelberg (Dec 2020). https://doi.org/10.1007/978-3-030-65411-5_12

23. Ducas, L., Laarhoven, T., van Woerden, W.P.J.: The randomized slicer for CVPP: Sharper, faster, smaller, batchier. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) PKC 2020, Part II. LNCS, vol. 12111, pp. 3–36. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45388-6_1
24. Eisenträger, K., Hallgren, S., Lauter, K.E., Morrison, T., Petit, C.: Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In: Nielsen, J.B., Rijmen, V. (eds.) EUROCRYPT 2018, Part III. LNCS, vol. 10822, pp. 329–368. Springer, Heidelberg (Apr / May 2018). https://doi.org/10.1007/978-3-319-78372-7_11
25. Espitau, T., Kirchner, P.: The nearest-colattice algorithm: Time-approximation tradeoff for approx-CVP. Open Book Series **4**, 251–266 (12 2020). https://doi.org/10.2140/obs.2020.4.251
26. Galbraith, S.D., Hess, F., Smart, N.P.: Extending the GHS Weil descent attack. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 29–44. Springer, Heidelberg (Apr / May 2002). https://doi.org/10.1007/3-540-46035-7_3
27. Galbraith, S.D., Stolbunov, A.: Improved algorithm for the isogeny problem for ordinary elliptic curves. Applicable Algebra in Engineering, Communication and Computing **24**(2), 107–131 (Jun 2013). https://doi.org/10.1007/s00200-013-0185-0
28. Ireland, K., Rosen, M.: Springer New York, New York, NY (1982)
29. Jaques, S., Schrottenloher, A.: Low-gate quantum golden collision finding. Cryptology ePrint Archive, Report 2020/424 (2020), https://eprint.iacr.org/2020/424
30. Kohel, D.: Endomorphism rings of elliptic curves over finite fields (1996), http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf
31. Kohel, D.R., Lauter, K., Petit, C., Tignol, J.P.: On the quaternion-isogeny path problem. LMS Journal of Computation and Mathematics **17**(A), 418–432 (2014)
32. Kuperberg, G.: A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM Journal on Computing **35**(1), 170–188 (2005). https://doi.org/10.1137/S0097539703436345, https://doi.org/10.1137/S0097539703436345
33. Lai, Y.F., Galbraith, S.D., de Saint Guilhem, C.: Compact, efficient and UC-secure isogeny-based oblivious transfer. Cryptology ePrint Archive, Report 2020/1012 (2020), https://eprint.iacr.org/2020/1012
34. Milne, J.S.: Complex multiplication (2020), https://www.jmilne.org/math/CourseNotes/cm.html
35. Onuki, H.: On oriented supersingular elliptic curves (2020), https://arxiv.org/abs/2002.09894
36. Peikert, C.: He gives C-sieves on the CSIDH. In: Canteaut, A., Ishai, Y. (eds.) EUROCRYPT 2020, Part II. LNCS, vol. 12106, pp. 463–492. Springer, Heidelberg (May 2020). https://doi.org/10.1007/978-3-030-45724-2_16
37. Petit, C.: Faster algorithms for isogeny problems using torsion point images. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017, Part II. LNCS, vol. 10625, pp. 330–353. Springer, Heidelberg (Dec 2017). https://doi.org/10.1007/978-3-319-70697-9_12
38. Pohlig, S.E., Hellman, M.E.: An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Transactions on Information Theory **IT-24**(1), 106–110 (Jan 1978)

39. Rostovtsev, A., Stolbunov, A.: Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145 (2006), https://eprint.iacr.org/2006/145
40. Schnorr, C.P.: A hierarchy of polynomial time lattice basis reduction algorithms. Theoretical Computer Science (53), 201224 (1987). https://doi.org/10.1016/0304-3975(87)90064-8, https://doi.org/10.1016/0304-3975(87)90064-8
41. Silverman, J.H.: Advanced Topics in The Arithmetic of Elliptic Curves. Springer-Verlag (1994)
42. Silverman, J.H.: The Arithmetic of Elliptic Curves. Springer (2009)
43. Sutherland, A.V.: Structure computation and discrete logarithms in finite abelian p-groups. Mathematics of Computation **80**(273), 477500 (Apr 2010). https://doi.org/10.1090/s0025-5718-10-02356-2, http://dx.doi.org/10.1090/S0025-5718-10-02356-2
44. The FPLLL development team: fpylll, a Python wraper for the fplll lattice reduction library, Version: 0.5.6 (2021), https://github.com/fplll/fpylll, available at https://github.com/fplll/fpylll
45. The Sage Developers: SageMath, the Sage Mathematics Software System (Version 9.2) (2021), https://www.sagemath.org
46. Vélu, J.: Isogénies entre courbes elliptiques. Comptes-rendus de l'Académie des Sciences **273**, 238–241 (july 1971), available at https://gallica.bnf.fr
47. Waterhouse, W.C.: Abelian varieties over finite fields. Annales scientifiques de l'École Normale Supérieure **2**(4), 521–560 (1969), http://eudml.org/doc/81852
48. Wesolowski, B.: The supersingular isogeny path and endomorphism ring problems are equivalent. Cryptology ePrint Archive, Report 2021/919 (2021), https://ia.cr/2021/919
49. Yoshinori Aono, T.E., Nguyen, P.Q.: Random lattices : theory and practice, https://espitau.github.io/bin/random_lattice.pdf

A Proof of Lemma 1

Let K be a quadratic imaginary field such that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial. Let ℓ be a prime number, $n \in \mathbb{N}^*$ and $\mathcal{O}_n := \mathbb{Z} + \ell^n \mathcal{O}_K$ the order of K with conductor ℓ^n. We prove that $\mathrm{rk}(\mathrm{Cl}(\mathcal{O}_n)) \leq 2$.

First, recall that by [19, Exercise 7.30.(a)], we have an exact sequence

$$\{1\} \longrightarrow \{\pm 1\} \longrightarrow (\mathbb{Z}/\ell^n\mathbb{Z})^\times \times \mathcal{O}_K^\times \longrightarrow (\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times \longrightarrow \mathrm{Cl}(\mathcal{O}_n) \longrightarrow \{1\}, \quad (\star)$$

where the group homomorphisms are given by

$$x \in \{\pm 1\} \longmapsto (x, x) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \times \mathcal{O}_K^\times,$$

$$([x], \omega) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \times \mathcal{O}_K^\times \longmapsto [x \cdot \omega] \in (\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times$$

$$\text{and} \quad [\alpha] \in (\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times \longmapsto [\alpha\mathcal{O}_K \cap \mathcal{O}_n] \in \mathrm{Cl}(\mathcal{O}_n).$$

Actually, the surjectiveness of the last map follows from the principality of $\mathcal{O}_K$. By the exact sequence ($\star$), we have

$$\mathrm{Cl}(\mathcal{O}_n) \simeq (\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/((\mathbb{Z}/\ell^n\mathbb{Z})^\times \times \mathcal{O}_K^\times/\{\pm(1,1)\}).$$

Besides, we have an injective group homomorphism

$$x \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \longmapsto (x,1) \in (\mathbb{Z}/\ell^n\mathbb{Z})^\times \times \mathcal{O}_K^\times/\{\pm(1,1)\}$$

inducing a surjection

$$(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/(\mathbb{Z}/\ell^n\mathbb{Z})^\times \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Cl}(\mathcal{O}_n). \qquad (\star\star)$$

Hence, we study the structure of $(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/(\mathbb{Z}/\ell^n\mathbb{Z})^\times$.

Let e be the ramification index of ℓ in K.

Case 1: Suppose that $\ell \geq e+2$. Then, by [16, Lemma 4.2.1.(2)] and [16, Corollary 4.2.11], we have

$$(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times \simeq \begin{cases} (\mathbb{Z}/(\ell-1)\mathbb{Z})^2 \times (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 & \text{if } \ell \text{ splits in } K \\ (\mathbb{Z}/(\ell-1)\mathbb{Z}) \times (\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z}) & \text{if } \ell \text{ ramifies in } K \\ (\mathbb{Z}/(\ell^2-1)\mathbb{Z}) \times (\mathbb{Z}/\ell^{n-1}\mathbb{Z})^2 & \text{if } \ell \text{ is inert in } K \end{cases}$$

Since $\ell \geq e+2 \geq 3$, by [28, Theorem IV.2], $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ is cyclic, so that

$$(\mathbb{Z}/\ell^n\mathbb{Z})^\times \simeq \mathbb{Z}/\varphi(\ell^n)\mathbb{Z} = \mathbb{Z}/(\ell-1)\ell^{n-1}\mathbb{Z} \simeq (\mathbb{Z}/(\ell-1)\mathbb{Z}) \times (\mathbb{Z}/\ell^{n-1}\mathbb{Z}).$$

Lemma 6. **(i)** *Let $\Phi : G_1 \times G_2 \longmapsto H_1 \times H_2$ be an injective group homomorphism between finite groups. Suppose that $\#H_1$ and $\#H_2$ are coprime and that $\#G_i | \#H_i$ for $i \in \{1,2\}$. Then there exists injective group homomorphisms $\varphi_i : G_i \longrightarrow H_i$ for $i \in \{1,2\}$ such that*

$$\forall (g_1,g_2) \in G_1 \times G_2, \quad \Phi(g_1,g_2) = (\varphi_1(g_1), \varphi(g_2)).$$

(ii) *Let $d \in \mathbb{N}^*$ and $\varphi : \mathbb{Z}/d\mathbb{Z} \longmapsto (\mathbb{Z}/d\mathbb{Z})^2$ be an injective group homomorphism. Then*

$$(\mathbb{Z}/d\mathbb{Z})^2/\operatorname{im}(\varphi) \simeq \mathbb{Z}/d\mathbb{Z}.$$

(iii) *Let $\varphi : \mathbb{Z}/\ell^{n-1}\mathbb{Z} \longrightarrow (\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})$ be an injective group homomorphism, then*

$$(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \times (\mathbb{Z}/\ell^n\mathbb{Z})/\operatorname{im}(\varphi) \simeq \mathbb{Z}/\ell^n\mathbb{Z} \quad \text{or} \quad (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/\ell^{n-1}\mathbb{Z}).$$

Proof. **(i)** We may write $\Phi(g) := (\phi_1(g), \phi_2(g))$ for all $g \in G_1 \times G_2$, where $\phi_i : G_1 \times G_2 \longrightarrow H_i$ are group homomorphisms. Let $g_1 \in G_1$. Then, $|\phi_2(g_1,1)|$ divides $|g_1|$ ($|x|$ being the order of x) and by Lagrange's theorem $|\phi_2(g_1,1)|$ divides $\#H_2$ and $|g_1|$ divides $\#G_1$, so it divides $\#H_1$. Since $\#H_1$ and $\#H_2$ are coprime, we have $|\phi_2(g_1,1)| = 1$ so $\phi_2(g_1,1) = 1$. By similar arguments, $\phi_1(1,g_2) = 1$ for all $g_2 \in G_2$ and the result follows.

(ii) Let $\varphi(1) := (\overline{a}, \overline{b})$, with $a,b \in [\![0\ ;\ d-1]\!]$. Since φ is injective, $\varphi(1)$ has order d so a,b and d are coprime. As a consequence, there exists $u,v \in [\![0\ ;\ d-1]\!]$ such that $au + bv \equiv 1\ [d]$. As a consequence,

$$(\overline{x}, \overline{y}) \in (\mathbb{Z}/d\mathbb{Z})^2 \longmapsto (\overline{ax} - \overline{vy}, \overline{b}\overline{x} + \overline{uy}) \in (\mathbb{Z}/d\mathbb{Z})^2$$

is an automorphism of $\mathbb{Z}$-modules because its matrix in the canonical basis of $(\mathbb{Z}/d\mathbb{Z})^2$ has determinant $\overline{au+bv}=1$. It follows that

$$(\mathbb{Z}/d\mathbb{Z})^2 = \mathbb{Z}(\overline{a},\overline{b}) \oplus \mathbb{Z}(-\overline{v},\overline{u}) = \mathrm{im}(\varphi) \oplus \mathbb{Z}(-\overline{v},\overline{u}),$$

so that $(\mathbb{Z}/d\mathbb{Z})^2/\operatorname{im}(\varphi) \simeq \mathbb{Z}(-\overline{v},\overline{u}) \simeq \mathbb{Z}/d\mathbb{Z}$.

(iii) Let $a,b\in\mathbb{Z}$ such that $\varphi(1)=(\overline{a},\overline{b})$. Since φ is injective, $\varphi(1)$ has order ℓ^{n-1} so $\ell^{n-1}\overline{b}=0$ *i.e.* $\ell^n|\ell^{n-1}b$ *i.e.* $\ell|b$. So we may write $a:=\ell^e a'$ and $b:=\ell^f b'$ with a' and b' prime to ℓ, and $(e,f)\in\mathbb{N}\times\mathbb{N}^*$. It follows that

$$\ell^{n-1} = |\varphi(1)| = \mathrm{lcm}(|\overline{a}|,|\overline{b}|) = \mathrm{lcm}(\ell^{n-1-e},\ell^{n-f}) = \ell^{\max(n-1-e,n-f)},$$

so that $\max(n-1-e,n-f)=n-1$. If $e=0$, then $\overline{a}$ generates $\mathbb{Z}/\ell^{n-1}\mathbb{Z}$, so

$$(\mathbb{Z}/\ell^{n-1}\mathbb{Z})\times(\mathbb{Z}/\ell^n\mathbb{Z}) = \mathrm{im}(\varphi)\oplus\{0\}\times\mathbb{Z}/\ell^n\mathbb{Z},$$

and we immediately conclude that the quotient is isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z}$.

Else, we have $f=1$. To conclude, it suffices to prove that the quotient has exponent ℓ^{n-1}. Let $x,y\in\mathbb{Z}$. Then, $\ell^{n-1}(\overline{x},\overline{y})=(0,\overline{\ell^{n-1}y})=\varphi(\overline{\ell^{n-2}k})$ with $k\in\mathbb{Z}$ such that $kb'\equiv y\ [\ell]$ (such a k exists because b' and ℓ are coprime). Hence, the exponent of the quotient divides ℓ^{n-1}. Furthermore, if $\ell^{n-2}(\overline{1},0)=\varphi(\overline{k'})$ for some $k'\in\mathbb{Z}$ then $\ell^n|k'\ell b'$ so $\ell^{n-1}|k'$ since $\gcd(\ell,b')=1$. Hence, $\overline{k'}=0$ and $\ell^{n-2}(\overline{1},0)=0$. Contradiction. So $(\overline{1},0)$ has order ℓ^{n-1} in the quotient. This completes the proof.

Applying Lemma 6 and the fact that a quotient of cyclic groups is cyclic, we conclude that

$$(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/(\mathbb{Z}/\ell^n\mathbb{Z})^\times \simeq \begin{cases} (\mathbb{Z}/(\ell-1)\mathbb{Z})\times(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \text{ if } \ell \text{ splits} \\ \mathbb{Z}/\ell^n\mathbb{Z} \quad\text{or}\quad (\mathbb{Z}/\ell\mathbb{Z})\times(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \text{ if } \ell \text{ ramifies} \\ (\mathbb{Z}/(\ell+1)\mathbb{Z})\times(\mathbb{Z}/\ell^{n-1}\mathbb{Z}) \text{ if } \ell \text{ is inert.} \end{cases}$$

By the surjection ($\star\star$), we conclude that $\mathrm{Cl}(\mathcal{O}_n)$ is either cyclic or has rank 2 with a tiny cyclic factor of order ℓ, the last case happening only when ℓ ramifies in K.

Case 2: Now, we assume that $\ell < e+2$. Hence, $\ell=2$ or $\ell=3$ and ℓ ramifies in K. We shall conclude with the following lemma:

Lemma 7. (i) *Let $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal prime to ℓ that we may write $\mathfrak{a}=\alpha\mathcal{O}_K$ with $\alpha\in\mathcal{O}_K$ ($\mathrm{Cl}(\mathcal{O}_K)$ being trivial). Let $i\in\mathbb{N}^*$. Then $\mathfrak{a}\cap\mathcal{O}_i$ is principal if and only if $\alpha\in\mathcal{O}_K^\times\cdot\mathcal{O}_i$.*

(ii) *Let $i\in\mathbb{N}^*$ and $\alpha\in\mathcal{O}_i$. Then, $\alpha^\ell\in\mathcal{O}_{i+1}$. Assume furthermore that $i\geq 2$, $\ell\nmid N(\alpha)$ and $\alpha\in\mathcal{O}_i\setminus\mathcal{O}_{i+1}$. Then, $\alpha\in\mathcal{O}_{i+1}\setminus\mathcal{O}_{i+2}$.*

(iii) *Let $i\in\mathbb{N}^*$ and $\alpha\in\mathcal{O}_K^\times\cdot(\mathcal{O}_i\setminus\mathcal{O}_{i+1})$ such that $\ell\nmid N(\alpha)$. Then, $\alpha\notin\mathcal{O}_K^\times\cdot\mathcal{O}_{i+1}$.*

(iv) *Let $i_0\geq 2$ such that $\mathrm{Cl}(\mathcal{O}_{i_0})$ has exponent k and $\mathrm{Cl}(\mathcal{O}_{i_0+1})$ has exponent $k\ell$. Then, there exists an $\mathcal{O}_K$-ideal $\mathfrak{a}$ such that $\mathfrak{a}\cap\mathcal{O}_i$ has order $k\ell^{i-i_0}$ in $\mathrm{Cl}(\mathcal{O}_i)$ for all $i\geq i_0$ and $\mathrm{Cl}(\mathcal{O}_i)$ has exponent $k\ell^{i-i_0}$ for all $i\geq i_0$.*

Proof. **(i)** Assume that $\mathfrak{a} \cap \mathcal{O}_i$ is principal. Then, there exists $\beta \in \mathcal{O}_i$ such that $\mathfrak{a} \cap \mathcal{O}_i = \beta\mathcal{O}_i$. By [19, Proposition 7.20], it follows that $\alpha\mathcal{O}_K = \mathfrak{a} = (\mathfrak{a} \cap \mathcal{O}_i)\mathcal{O}_K = \beta\mathcal{O}_K$. Hence, $\alpha = \beta u$ and $\beta = \alpha v$ with $u, v \in \mathcal{O}_K$, so that $\beta = \beta uv$, $uv = 1$ and $u \in \mathcal{O}_K^\times$, so that $\alpha \in \mathcal{O}_K^\times \cdot \mathcal{O}_i$. The converse is trivial.

(ii) Let θ be a generator of $\mathcal{O}_K$. Let us write $\alpha = a + b\ell^i\theta$. Then

$$\alpha^\ell = a^\ell + \ell^{i+1}a^{\ell-1}b\theta + \sum_{k=2}^{\ell} \binom{\ell}{k} a^{\ell-k}\ell^{ik}b^k\theta^k \in \mathbb{Z} + \ell^{i+1}\mathcal{O}_K = \mathcal{O}_{i+1}.$$

Now, assume that $i \geq 2$, $\ell \nmid N(\alpha)$ and $\alpha \notin \mathcal{O}_{i+1}$. Since $\ell | \binom{\ell}{k}$ for all $k \in [\![1\ ;\ \ell-1]\!]$ and $i \geq 2$, we have

$$\sum_{k=2}^{\ell} \binom{\ell}{k} a^{\ell-k}\ell^{ik}b^k\theta^k \in \ell^{i+2}\mathcal{O}_K.$$

Hence, to conclude that $\alpha^\ell \notin \mathcal{O}_{i+2}$, it suffices to prove that $\ell \nmid a^{\ell-1}b$. But $\ell \nmid a$ since $\ell \nmid N(\alpha)$ and $\ell \nmid b$ since $\alpha \notin \mathcal{O}_{i+1}$. The result follows.

(iii) For $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, we have $\mathcal{O}_K^\times = \{\pm 1\}$ so the result trivially holds.

Assume that $K := \mathbb{Q}(\sqrt{-1})$. Let $\theta := \sqrt{-1}$. Then, $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $\mathcal{O}_K^\times = \{\pm 1, \pm\theta\}$. Let $\alpha \in \mathcal{O}_i$ that we may write $\alpha := a + b\ell^i\theta$ with $a, b \in \mathbb{Z}$. Then

$$\theta\alpha = -b\ell^i + a\theta.$$

Since $\ell \nmid N(\alpha)$, $\ell \nmid a$ so $\theta\alpha \notin \mathcal{O}_{i+1}$. The result follows in that case.

Assume that $K := \mathbb{Q}(\sqrt{-3})$. Let $\theta := (-1 + \sqrt{-3})/2$. Then, $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $\mathcal{O}_K^\times = \{\pm 1, \pm\theta, \pm\theta^2\}$. Let $\alpha \in \mathcal{O}_i \setminus \mathcal{O}_{i+1}$ that we may write $\alpha := a + b\ell^i\theta$ with $a, b \in \mathbb{Z}$. Then

$$\theta\alpha = a\theta + b\ell^i\theta^2 = a\theta - b\ell^i(\theta + 1) = -b\ell^i + (a - b\ell^i)\theta$$

$$\text{and} \quad \theta^2\alpha = -b\ell^i\theta + (a - b\ell^i)\theta^2 = a\theta - (a - b\ell^i)(\theta + 1) = b\ell^i - a + b\ell^i\theta.$$

Since $\ell \nmid N(\alpha)$, $\ell \nmid a$ so $\theta\alpha \notin \mathcal{O}_{i+1}$. Since $\alpha \notin \mathcal{O}_{i+1}$, $\ell \nmid b$ so that $\theta^2\alpha \notin \mathcal{O}_{i+1}$. The result follows.

(iv) Let $i \geq i_0$. Then, by [19, Proposition 7.20] every invertible ideal of $\mathcal{O}_i$ is of the form $\mathfrak{a} \cap \mathcal{O}_i$ for a certain $\mathcal{O}_K$-ideal $\mathfrak{a}$ prime to ℓ. Let us write $\mathfrak{a} := \alpha\mathcal{O}_K$ for $\alpha \in \mathcal{O}_K$. Then, $\mathfrak{a}^k \cap \mathcal{O}_{i_0}$ is principal (since $\mathrm{Cl}(\mathcal{O}_{i_0})$ has exponent k) so $\alpha^k \in \mathcal{O}_K^\times \cdot \mathcal{O}_{i_0}$ by (i) and by (ii), $\alpha^{k\ell^{i-i_0}} \in \mathcal{O}_K^\times \cdot \mathcal{O}_i$, so that $\mathfrak{a}^{k\ell^{i-i_0}} \cap \mathcal{O}_i$ is principal. Hence, the exponent of $\mathrm{Cl}(\mathcal{O}_i)$ divides $k\ell^{i-i_0}$.

Let $\mathfrak{a}$ be an $\mathcal{O}_K$-ideal prime to ℓ such that $\mathfrak{a} \cap \mathcal{O}_{i_0+1}$ has order $k\ell$ in $\mathrm{Cl}(\mathcal{O}_{i_0+1})$. Let us write $\mathfrak{a} := \alpha\mathcal{O}_K$ with $\alpha \in \mathcal{O}_K$. Let d be the order of $\mathfrak{a} \cap \mathcal{O}_{i_0}$ in $\mathrm{Cl}(\mathcal{O}_{i_0})$. Then, $\alpha^d \in \mathcal{O}_K^\times \cdot \mathcal{O}_{i_0}$ by (i), so that $\alpha^{d\ell} \in \mathcal{O}_K^\times \cdot \mathcal{O}_{i_0+1}$ by (ii), so that the order of $\mathfrak{a} \cap \mathcal{O}_{i_0+1}$ in $\mathrm{Cl}(\mathcal{O}_{i_0+1})$ divides $d\ell$, thus $k\ell | d\ell$, which implies $k | d$. But we also have $d | k$ because $\mathrm{Cl}(\mathcal{O}_{i_0})$ has exponent k, so $d = k$.

We have $\alpha^k \in \mathcal{O}_K^\times \cdot (\mathcal{O}_{i_0} \setminus \mathcal{O}_{i_0+1})$, otherwise, by (i), $\mathfrak{a} \cap \mathcal{O}_{i_0+1}$ would have order $\leq k$. By (ii), it follows that $\alpha^{k\ell^{i-i_0}} \in \mathcal{O}_K^\times \cdot (\mathcal{O}_i \setminus \mathcal{O}_{i+1})$ for all $i \geq i_0$.

Now, we prove by induction on $i \geq i_0$ that $\mathfrak{a} \cap \mathcal{O}_i$ has order $k\ell^{i-i_0}$. As we already saw, the result holds for $i \in \{i_0, i_0+1\}$. Let $i \geq i_0 + 1$. Assume that $\mathfrak{a} \cap \mathcal{O}_i$ has order $k\ell^{i-i_0}$. It follows that for all $d \in \mathbb{N}^*$, $\alpha^d \in \mathcal{O}_K^\times \cdot \mathcal{O}_i$ if and only if $k\ell^{i-i_0}|d$. As a consequence, $\alpha^{k\ell^{i+1-i_0}} \in \mathcal{O}_K^\times \cdot \mathcal{O}_{i+1}$ and if $d \in \mathbb{N}^*$ is such that $\alpha^d \in \mathcal{O}_K^\times \cdot \mathcal{O}_{i+1} \subseteq \mathcal{O}_K^\times \cdot \mathcal{O}_i$, then we must have $k\ell^{i-i_0}|d$ and $d|k\ell^{i+1-i_0}$ since the exponent of $\mathrm{Cl}(\mathcal{O}_{i+1})$ divides $k\ell^{i+1-i_0}$. But $\alpha^{k\ell^{i-i_0}} \notin \mathcal{O}_K \cdot \mathcal{O}_{i+1}$ since $\alpha^{k\ell^{i-i_0}} \notin \mathcal{O}_K \cdot (\mathcal{O}_i \setminus \mathcal{O}_{i+1})$ and by (iii). Hence, $\mathfrak{a} \cap \mathcal{O}_{i+1}$ has order $k\ell^{i+1-i_0}$. This completes the proof.

By point (iv) of the preceding lemma, we determine the structure of $\mathrm{Cl}(\mathcal{O}_n)$ by computing the exponent of $\mathrm{Cl}(\mathcal{O}_2)$ and $\mathrm{Cl}(\mathcal{O}_3)$. Since $\mathrm{Cl}(\mathcal{O}_K)$ is trivial, we have

$$\mathrm{disc}(K) \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\},$$

by [19, Theorem 7.30.(i)], so we have a limited number of computations to make. There are two cases: either both $\mathrm{Cl}(\mathcal{O}_2)$ and $\mathrm{Cl}(\mathcal{O}_3)$ are cyclic, in which case $\mathrm{Cl}(\mathcal{O}_n)$ is cyclic; or $\mathrm{Cl}(\mathcal{O}_{i_0}) \simeq (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/k\mathbb{Z})$ and $\mathrm{Cl}(\mathcal{O}_{i_0+1}) \simeq (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/k\ell\mathbb{Z})$ for certain integers $i_0 \geq 2$ and $k \geq 2$, in which case $\mathrm{Cl}(\mathcal{O}_n) \simeq (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/k\ell^{n-i_0}\mathbb{Z})$. We performed the computations with `Magma` [10] and obtained the following results:

disc(K) \ ℓ	2	3
-3	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$	$\mathbb{Z}/3^{n-1}\mathbb{Z}$
-4	$\mathbb{Z}/2^{n-1}\mathbb{Z}$	
-7	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2^{n-2}\mathbb{Z})$	
-8	$\mathbb{Z}/2^{n-1}\mathbb{Z}$	
-11	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3 \cdot 2^{n-2}\mathbb{Z})$	
-19	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3 \cdot 2^{n-2}\mathbb{Z})$	
-43	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3 \cdot 2^{n-2}\mathbb{Z})$	
-67	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3 \cdot 2^{n-2}\mathbb{Z})$	
-163	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3 \cdot 2^{n-2}\mathbb{Z})$	

B Time complexity of the chain attack of Section 3.3

We refer to Section 3.3 for the notations. As explained in Section 3.3, the dominant step in the attack is to find a close vector to $\mathbf{e}_{i+1}$ in L_{i+1} and compute the action of $[\mathfrak{a}_i \cdot \mathfrak{b}_i]$ on E_{i+1}. This operation has to be repeated at most $\simeq \ell$ times for all $i \in [\![0\ ;\ n-1]\!]$, so at most $n\ell$ times.

If we find $\mathbf{c} \in L_{i+1}$ close to $\mathbf{e}_{i+1}$ and set $\mathbf{e}'_{i+1} := \mathbf{e}_{i+1} - \mathbf{c}$, so that $[\mathfrak{a}_i \cdot \mathfrak{b}_i] = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_{i+1,j}}$ in $\mathrm{Cl}(\mathcal{O}_{i+1})$, then the time complexity of the operation $[\mathfrak{a}_i \cdot \mathfrak{b}_i] \cdot E_{i+1}$ is

$$\Theta\left((i+1)\sum_{j=1}^{t} P(q_j, n)|e'_{i+1,j}|\right),$$

where P is a polynomial. Hence, the complexity is $\Theta(\|\mathbf{e}'_{i+1}\|_1)$ up to a polynomial factor (in n, t and the q_j). Since $\|\mathbf{e}'_{i+1}\|_2 \leq \|\mathbf{e}'_{i+1}\|_1 \leq \sqrt{t}\|\mathbf{e}'_{i+1}\|_2$, the complexity becomes $\Theta(\|\mathbf{e}'_{i+1}\|_2)$ up to a polynomial factor.

Theorem 3. *[25, Theorem 3.3] Let $\Lambda \subseteq \mathbb{Z}^d$ be a lattice of rank d, $B := (\mathbf{b}_1, \ldots, \mathbf{b}_d)$, a basis of Λ, a target $\mathbf{x} \in \mathbb{R}^d$ and $k \in \mathbb{N}^*$ such that $d > 2k$. Under some heuristic assumptions, there exists an algorithm finding $\mathbf{c} \in \Lambda$ such that*

$$\|\mathbf{x} - \mathbf{c}\|_2 = \Theta\left(GH(k)^{\frac{d}{2k}} \operatorname{Covol}(\Lambda)^{\frac{1}{d}}\right),$$

where GH is the Gaussian heuristic function: $GH(k) := \Gamma(k/2+1)^{1/k}/\sqrt{\pi}$. This algorithm runs in time

$$(T_{CVP}(k) + T_{SVP}(k))P\left(k, d, \log\|\mathbf{x}\|_2, \log \max_{1\leq i\leq d} \|\mathbf{b}_i\|_2\right),$$

where $T_{CVP}(k)$ and $T_{SVP}(k)$ are the time complexities of oracles for CVP and SVP in dimension k for the norm ℓ_2 respectively and P is a polynomial.

The best known algorithms for CVP and SVP are due to [23] and [4] respectively. They run in time $T_{CVP}(k) = 2^{c_1 k + o(k)}$ and $T_{SVP}(k) = \left(\frac{3}{2}\right)^{k/2+o(k)} = 2^{c_2 k + o(k)}$ respectively, with $c_1 \approx 0.264$ and $c_2 \approx 0.292$. The time complexity of the attack follows

$$T := 2^{c_2 k + o(k)} + \frac{1}{\sqrt{\pi}^{\frac{1}{k}}} \Gamma\left(\frac{k}{2} + 1\right)^{\frac{t}{2k^2}} \ell^{\frac{n}{t}}$$

up to polynomial factors, where we used the fact that $\operatorname{Covol}(L_n) = \#\operatorname{Cl}(\mathcal{O}_n) \simeq \ell^n$ and neglected $T_{CVP}(k)$ compared to $T_{SVP}(k)$. Using the Stirling equivalent $\Gamma(k/2+1) \sim \sqrt{\pi k}(k/2e)^{k/2}$ as $k \to +\infty$ and setting $k := \lfloor \kappa\sqrt{t\log_2(t)} \rfloor$, with $\kappa := 1/\sqrt{8c_2}$ in order to optimize the complexity, we get

$$T = 2^{(\sqrt{c_2/8}+o(1))\sqrt{t\log_2(t)}} = \exp((c + o(1))\sqrt{t\log(t)}),$$

with $c := \sqrt{c_2/8\log(2)} \simeq 0.229$, assuming that ℓ and n are constant and $t \to +\infty$.

C Complexity analysis of Onuki's attack presented in Section 4.1

We use the notations of Section 4.1 explaining Onuki's attack which consists in computing a K-oriented endomorphism $\iota'_n(\beta) \in \operatorname{End}(F_n)$ for $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$. We look for β such that $\beta\mathcal{O}_n = I \cdot J$, with a big factor $I := \prod_{j=1}^t (\mathfrak{q}_j \cap \mathcal{O}_n)^{e_j}$, where $e_1, \cdots, e_t \in [\![-r\ ;\ r]\!]$, and a small factor J. Then $\iota'_n(\beta)$ will be computed as the composite of the isogeny associated to I and the isonegy associated to J. The first one is easy to compute with the knowledge of the action of powers of

$\mathfrak{q}_j$ on F_n. The second one can be computed by a meet-in-the-middle strategy in $\Omega(\sqrt{N(J)})$ operations (as explained in Section 4.3).

We proceed as follows to select a suitable β. Let θ be a generator of $\mathcal{O}_K$, so that $\ell^n\theta$ generates $\mathcal{O}_n$. We sample $\beta := a + b\ell^n\theta$ with a and b sampled uniformly at random in $[\![-m\ ;\ m]\!]$ and $[\![-m\ ;\ m]\!] \setminus \ell\mathbb{Z}$ respectively, for m big enough. We stop the sampling when $N(\beta)$ has a big enough divisor $Q := \prod_{j=1}^t q_j^{e'_j}$ with $e'_1, \cdots, e'_t \in [\![0\ ;\ r]\!]$, let's say $Q \geq x$, where the threshold x is to be chosen. We make the heuristic assumption that $N(\beta)$ has the same arithmetic properties as a uniform variable in $[\![N_{min}\ ;\ N_{max}]\!]$. Under this assumption, we have the following result:

Lemma 8. *The average time complexity of Onuki's attack [35, §6.3] is:*

$$C(x) \geq \frac{x}{(r+1)^t} + \frac{\kappa\sqrt{N_{max}}}{\sqrt{x}(r+1)^t},$$

where $\kappa := \frac{1}{2\sqrt{q_1}}\left(1 - \frac{1}{q_1}\right)$ *and* x *is the threshold for the value of the norm of the ideal* $J = \prod_{j=1}^t \mathfrak{q}_j^{e_j}$ *dividing* β*. The optimal value for the threshold is* $x_m := (\kappa/2)^{2/3} N_{max}^{1/2}(r+1)^{t/3}$ *and the optimal average time complexity is:*

$$C(x_m) = \Omega\left(\frac{\sqrt{N_{max}}}{(r+1)^{\frac{t}{3}}}\right) = \Omega\left(\frac{\ell^{\frac{2n}{3}}}{(r+1)^{\frac{t}{3}}}\right),$$

since $N_{max} \geq N_{min} \geq \ell^{2n}$*.*

Proof. Under the heuristic assumption we made, we can assume that $N := N(\beta)$ is a uniform random variable in the range $[\![N_{min}\ ;\ N_{max}]\!]$. We define the random variable:

$$Q := Q(N) = \prod_{j=1}^t q_j^{\min(r, v_{q_j}(N))}.$$

The cost of the exhaustive search for a suitable β is then:

$$C_1(x) = \frac{1}{\mathbb{P}(Q(N) \geq x)} = \frac{N_{max} - N_{min}}{\#S(x)},$$

with:

$$\begin{aligned} S(x) &:= \left\{ y \in [\![N_{min}\ ;\ N_{max}]\!] \;\middle|\; \prod_{j=1}^t q_j^{\min(r, v_{q_j}(y))} \geq x \right\} \\ &= \bigcup_{\substack{(e_1,\cdots,e_t) \in [\![0\ ;\ r]\!]^t \\ x \leq \prod_{j=1}^t q_j^{e_j} \leq N_{max}}} \left\{ k \prod_{j=1}^t q_j^{e_j} \;\middle|\; k \in \left[\!\!\left[\left\lceil \frac{N_{min}}{\prod_{j=1}^t q_j^{e_j}} \right\rceil\ ;\ \left\lfloor \frac{N_{max}}{\prod_{j=1}^t q_j^{e_j}} \right\rfloor \right]\!\!\right] \right\} \end{aligned}$$

so that:

$$\begin{aligned}
\#S(x) &\leq \sum_{\substack{(e_1,\cdots,e_t)\in[\![0\ ;\ r]\!]^t\\ x\leq\prod_{j=1}^t q_j^{e_j}\leq N_{max}}} \left(\left\lfloor\frac{N_{max}}{\prod_{j=1}^t q_j^{e_j}}\right\rfloor - \left\lceil\frac{N_{min}}{\prod_{j=1}^t q_j^{e_j}}\right\rceil\right)\\
&\leq \sum_{\substack{(e_1,\cdots,e_t)\in[\![0\ ;\ r]\!]^t\\ x\leq\prod_{j=1}^t q_j^{e_j}\leq N_{max}}} \frac{N_{max}-N_{min}}{\prod_{j=1}^t q_j^{e_j}}\\
&\leq \frac{N_{max}-N_{min}}{x}\#\left\{(e_1,\cdots,e_t)\in[\![0\ ;\ r]\!]^t \middle| x\leq\prod_{j=1}^t q_j^{e_j}\leq N_{max}\right\}\\
&\leq (N_{max}-N_{min})\frac{(r+1)^t}{x}. \qquad (1)
\end{aligned}$$

It follows that the search for β costs:

$$C_1(x) \geq \frac{x}{(r+1)^t}. \qquad (2)$$

The average cost of the meet-in-the-middle procedure to find the isogeny associated to J is:

$$C_2(x) \geq \mathbb{E}\left[\sqrt{\frac{N}{Q(N)}}\middle| Q(N)\geq x\right] \geq \sqrt{A}\mathbb{P}(N\geq AQ(N)|Q(N)\geq x),$$

where we used Markov's inequality with $A>0$ to be chosen. Hence:

$$C_2(x) \geq \sqrt{A}\frac{\mathbb{P}(\{N\geq AQ(N)\}\cap\{Q(N)\geq x\})}{\mathbb{P}(Q(N)\geq x)} = \frac{\sqrt{A}\#T(A)}{\#S(x)}, \qquad (3)$$

with:

$$\begin{aligned}
T(A) := \Bigg\{ k\prod_{j=1}^t q_j^{e_j} \Bigg|\ & N_{max}\geq\prod_{j=1}^t q_j^{e_j}\geq x\\
&\text{and}\quad k\in\left[\!\!\left[\max\left(\lceil A\rceil, \left\lceil\frac{N_{min}}{\prod_{j=1}^t q_j^{e_j}}\right\rceil\right)\ ;\ \left\lfloor\frac{N_{max}}{\prod_{j=1}^t q_j^{e_j}}\right\rfloor\right]\!\!\right]\Bigg\}.
\end{aligned}$$

We take $A := N_{max}/(q_1x)$, so that for all $e_1,\cdots,e_t\in[\![0\ ;\ r]\!]$ such that $N_{max}\geq\prod_{j=1}^t q_j^{e_j}\geq x$, we have:

$$\frac{N_{min}}{\prod_{j=1}^t q_j^{e_j}} \leq \frac{N_{min}}{x} < \frac{N_{max}}{q_1x} = A,$$

since $N_{max}/N_{min}\simeq m^2\gg q_1$. Without loss of generality, we can assume that x is a product of the q_j. Hence:

$$\#T(A) \geq \left\lfloor\frac{N_{max}}{x}\right\rfloor - A \geq \frac{N_{max}}{x} - \frac{N_{max}}{q_1x} - 1 = \frac{N_{max}}{2x}\left(1-\frac{1}{q_1}\right),$$

under the fair assumption that $x \leq N_{max}/2(1-1/q_1)$. This inequality combined with Eq. (1) and Eq. (3) leads to:

$$C_2(x) \geq \frac{(N_{max})^{\frac{3}{2}}(1-1/q_1)}{2\sqrt{q_1 x}(r+1)^t(N_{max}-N_{min})} \geq \frac{\sqrt{N_{max}}}{2\sqrt{q_1 x}(r+1)^t}\left(1-\frac{1}{q_1}\right). \quad (4)$$

Combining Eq. (2) and Eq. (4), we find that Onuki's attack has average complexity:

$$C(x) \geq C_1(x) + C_2(x) \geq \frac{x}{(r+1)^t} + \frac{\kappa\sqrt{N_{max}}}{\sqrt{x}(r+1)^t},$$

with $\kappa := \frac{1}{2\sqrt{q_1}}\left(1-\frac{1}{q_1}\right)$. The optimal value for x is obtained by differenciating of the function defined over $\mathbb{R}_+^*$:

$$x \longmapsto \frac{x}{(r+1)^t} + \frac{\kappa\sqrt{N_{max}}}{\sqrt{x}(r+1)^t}.$$

D Complexity analysis of the ideal class group action (Lemma 5)

Let $(E_i)_{0\leq i\leq n}$ be a descending ℓ-isogeny chain such that E_0 is $\mathcal{O}_K$-oriented and $\mathfrak{a} := \prod_{j=1}^t \mathfrak{q}_j^{e_j}$ with $e_1,\ldots,e_t$ sampled in $[\![-r\ ;\ r]\!]$. We evaluate the time complexity of the operation $\mathfrak{a}\cdot(E_i)_{0\leq i\leq n}$ (in terms of operations over $\mathbb{F}_{p^2}$).

First, we evaluate the complexity of the operation $\mathfrak{q}_j^{\pm 1}\cdot(E_i)_{0\leq i\leq n}$ for $j \in [\![1\ ;\ t]\!]$. Such an operation has to be repeated $r/2$ times and for all $j\in[\![1\ ;\ t]\!]$ on average for a generic ideal $\mathfrak{a}$.

Using the method of Sections 2.4 to compute $\mathfrak{q}_j^{\pm 1}\cdot(E_i)_{0\leq i\leq n}$, we need to solve n equations of the form $\gcd(\Phi_{q_j}(j_0,x),\Phi_\ell(j_1,x)) = 0$ with $j_0, j_1 \in \mathbb{F}_{p^2}$. For any prime m, the modular polynomial $\Phi_m(X,Y)$ has degree $m+1$ in X and Y, thus its evaluation in one variable requires $O((m+1)^2)$ operations over $\mathbb{F}_{p^2}$. Hence, the evaluation of $\Phi_{q_j}(j_0,x)$ and $\Phi_\ell(j_1,x)$ has complexity $O((q_j+1)^2)$ operations over $\mathbb{F}_{p^2}$, and computing the gcd of those polynomials has complexity $O((\ell+1)(q_j+1))$. Finally, finding the roots of the gcd (whose degree is $\leq \ell+1$) can be done with Berlekamp's algorithm [5] over $\mathbb{F}_{p^2}$ and requires $O(\log(p^2)) = O(n)$ operations over $\mathbb{F}_{p^2}$. Hence, solving these modular equations costs $O(n(q_j^2+n))$ operations over $\mathbb{F}_{p^2}$ (recall that we treat ℓ as a constant).

As breifly explained in the end of Section 2.4 and in detail in [17, §5, pp. 18-19], in order to remove any ambiguity in the roots of modular equations, we also have to compute explicitly $\mathfrak{q}_j\cdot E_{i_0}$ and $\mathfrak{q}_j^{-1}\cdot E_{i_0}$ where $i_0\in[\![0\ ;\ n]\!]$ is the first index such that $\mathfrak{q}_j^2\cap\mathcal{O}_{i_0}$ is not principal in $\mathcal{O}_{i_0}$. In order to do that, we compute $E_{i_0}[\mathfrak{q}_j]$ and $E_{i_0}[\overline{\mathfrak{q}_j}]$ and use Vélu's formulas [46]. The computation of these torsion subgroups cannot be done without knowing the K-orientation ι_{i_0} of E_{i_0}. Knowing the K-orientation ι_0 of E_0, we compute ι_{i_0} by computing each ℓ-isogeny of the chain

$$E_0 \xrightarrow{\varphi_0} E_1 \cdots E_{i_0-1} \xrightarrow{\varphi_{i_0-1}} E_{i_0},$$

when only j-invariants are known. Knowing E_i $(0 \leq i \leq i_0 - 1)$, the ℓ-isogeny $\varphi_i : E_i \longrightarrow E_{i+1}$ can be computed by exhaustively testing all ℓ-isogenies and applying Vélu's formulas everytime, until the j-invariant of the codomain matches $j(E_{i+1})$. As a consequence, computing ι_{i_0} costs $O(i_0(\ell+1)\ell)$ operations over $\mathbb{F}_{p^2}$. Once this is done, we write $\mathfrak{q}_j \cap \mathcal{O}_{i_0} := q_j\mathbb{Z} + \alpha\mathbb{Z}$ with $\alpha \in \mathcal{O}_{i_0}$ and evaluate $\iota_{i_0}(\alpha)$ and $\iota_{i_0}(\overline{\alpha})$ on $E_{i_0}[q_j]$ to compute $E_{i_0}[\mathfrak{q}_j]$ and $E_{i_0}[\overline{\mathfrak{q}_j}]$ and then apply Vélu's formulas. This step costs $O(q_j^2)$ operations over $\mathbb{F}_{p^2}$. It follows that the computation of $\mathfrak{q}_j \cdot E_{i_0}$ and $\mathfrak{q}_j^{-1} \cdot E_{i_0}$ costs $O(q_j^2 + i_0(\ell+1)\ell)$ operations over $\mathbb{F}_{p^2}$.

To complete our cost evaluation, we estimate i_0. Let $i \in [\![0\ ;\ n]\!]$, such that $(\mathfrak{q}_j)^2$ is principal in $\mathcal{O}_i$. Then $(\mathfrak{q}_j)^2 \cap \mathcal{O}_i = \alpha\mathcal{O}_i$ for a certain $\alpha \in \mathcal{O}_i$, then $N(\alpha) = q_j^2$ by [19, Lemma 7.14.(i)]. Let θ be a generator of $\mathcal{O}_K$, t its trace and d its norm. Then, $\mathcal{O}_i = \mathbb{Z} + \ell^i\theta\mathbb{Z}$ and $\alpha = a + b\ell^i\theta$ with $a, b \in \mathbb{Z}$, so that

$$q_j^2 = N(\alpha) = (a + b\ell^i\theta)(a + b\ell^i\overline{\theta}) = a^2 + ab\ell^i t + b^2\ell^{2i}d.$$

If $b \neq 0$, we get that a is a root of the polynomial $X^2 + b\ell^i tX + b^2\ell^{2i}d - q_j^2$ whose discriminant is

$$b^2\ell^{2i}(t^2 - 4d^2) + 4q_j^2 = b^2\ell^{2i}\Delta_K + 4q_j^2 \leq 4q_j^2 + \ell^{2i}\Delta_K.$$

There is no integral root when this quantity is < 0, *i.e.* once $i \geq i_1$ given by:

$$i_1 := \lfloor \log_\ell(2q_j/\sqrt{|\Delta_K|}) \rfloor + 1.$$

Hence, if $i \geq i_1$, we must have $b = 0$, so $a = q_j$ and $(\mathfrak{q}_j)^2 \cap \mathcal{O}_i = q_j\mathcal{O}_i$, so that $\mathfrak{q}_j^2 = q\mathcal{O}_K$ and q_j ramifies in K, which is impossible. It follows that $(\mathfrak{q}_j)^2$ is not principal for $i \geq i_1$ so $i_0 \leq i_1 = O(\log(q_j))$.

As a consequence, the total complexity of the operation $\mathfrak{q}_j^{\pm 1} \cdot (E_i)_{0 \leq i \leq n}$ is $O(nq_j^2 + n^2 + \ell^2 \log(q_j))$, so the total complexity of $\mathfrak{a} \cdot (E_i)_{0 \leq i \leq n}$ is

$$O\left(\frac{r}{2}\sum_{j=1}^{t}(nq_j^2 + n^2 + \ell^2\log(q_j))\right)$$

operations over $\mathbb{F}_{p^2}$.

Under the heuristic assumption that one prime out of two splits in K, we get that $q_j \sim 2j\log(j)$ as $j \to +\infty$. With the estimate $\sum_{j=1}^{t} j^2\log^2(j) \sim t^3\log^2(t)/3$ as $t \to +\infty$, obtained via the integral test for convergence we get that $O(nt^3\log^2(t) + n^2)$ operations over $\mathbb{F}_{p^2}$ are needed on average to compute $\mathfrak{a} \cdot (E_i)_{0 \leq i \leq n}$, ℓ and r being absorbed by the O constant.