IBM Research Zurich
Université de Rennes 1

Master's thesis

On Oriented Supersingular Isogeny Diffie-Hellman

Pierrick Dartois

Under the supervision of Luca De Feo

Abstract

Shor discovered in 1995 [1] that quantum computers powerful enough could break all cryptographic primitives based on discrete logarithm and integer factorization such as the widespread RSA and commonly used elliptic curve cryptography. Ever since, efforts have been made to find quantum-safe cryptographic primitives. Since the foundational works of Couveignes in the end of the 1990's [2] and the discovery of Supersingular Isogeny Diffie-Hellman (SIDH) by De Feo, Jao and Plût in 2011 [3], isogeny-based cryptography has become a promising area of research in post-quantum cryptography. Oriented Supersingular Isogeny Diffie-Hellman (OSIDH) is a key exchange protocol due to Kohel and Colò [4], generalizing the ideas of Commutative Supersingular Isogeny Diffie-Hellman (CSIDH) due to Castryck et. al. (2018) [5], itself inspired from Couveignes' cryptosystem. The goal of this master's thesis is to study OSIDH. We conduct a cryptanalysis and propose an original attack running on a classical computer. We implement this attack in `SageMath` [6] with toy parameters. We come to the conclusion that OSIDH is not secure if its parameters are not chosen carefully. Unfortunately, a secure choice of parameters impedes new cryptographic constructions based on the OSIDH framework.

Contents

1 Mathematical framework of OSIDH **6**

1.1 Oriented supersingular elliptic curves . . . 6

1.2 Reduction and oriented supersingular elliptic curves . . . 8

1.2.1 Motivation . . . 8

1.2.2 Reduction of elliptic curves with complex multiplication by $\mathcal{O}$ . . . 8

1.3 The ideal class group action . . . 11

1.4 Oriented supersingular isogeny graphs . . . 15

1.4.1 Volcano structure of oriented supersingular isogeny graphs . . . 15

1.4.2 Graph refolding and the forgetful map . . . 18

1.5 Isogeny chains and ladders . . . 20

1.5.1 Definition . . . 20

1.5.2 A practical way to construct descending ℓ-ladders . . . 22

2 The OSIDH cryptosystem **25**

2.1 A first naive Diffie Hellman protocol . . . 25

2.2 The OSIDH protocol . . . 26

3 Cryptanalysis of OSIDH **30**

3.1 A first attack using quaternions . . . 30

3.1.1 Step 1: compute $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$ . . . 30

3.1.2 Step 2: find a connecting ideal between $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$ . . . 33

3.1.3 Step 3: find an equivalent ideal J to I that is generated by a prime ideal $\mathfrak{N}$ of $\mathcal{O}_n$ 34

3.1.4 Step 4: express $[\mathfrak{N}]$ as a product of the $[\mathfrak{q}_j]$ with small exponents . . . 35

3.2 A second attack using the class group action only . . . 37

3.2.1 Expressing $\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Cl}(\mathcal{O}_i))$ in terms of the $\mathfrak{q}_j$ . . . 38

3.2.2 Reducing the exponents of $\mathfrak{a}_i \cdot \mathfrak{b}$ . . . 38

3.2.3 Implementation . . . 39

3.3 Onuki's attack . . . 39

3.4 A variant of Onuki's attack based on lattice reduction . . . 43

3.4.1 Estimating the first minimum of L in infinity norm . . . 43

3.4.2 Countermeasures to our attack . . . 45

3.4.3 Implementation . . . 46

3.5 Kuperberg's attack . . . 47

A Mathematical prerequisites and complements **51**

A.1 $\mathfrak{p}$-adic integers . . . 51

A.2 Reduction of elliptic curves . . . 52

A.3 Some prerequisites on quaternions . . . 53

A.4 The Deuring correspondence . . . 54

A.5 Structure of the ideal class group $\mathrm{Cl}(\mathcal{O}_n)$ . . . 55
A.5.1 Determining the structure of $(\mathcal{O}_K/\mathfrak{l}^n)^\times$ . . . 57
A.5.2 Case $\ell \geq e+2$ . . . 61
A.5.3 Case $\ell < e+2$ . . . 62

B Algorithms **65**
B.1 Proper representation of an integer by a positive definite primitive quadratic form . . . 65
B.2 The KLPT algorithm . . . 65
B.3 Effective Deuring correspondence . . . 70
B.4 Discrete logarithm and basis computation in finite abelian groups . . . 72
B.4.1 Discrete logarithm in a basis . . . 72
B.4.2 Basis computation from a generating set . . . 76
B.4.3 Specialization to the case of the ideal class group $\mathrm{Cl}(\mathcal{O}_n)$ . . . 78
B.5 Lattice of relations of a finite abelian group . . . 79
B.6 Kuperberg's algorithm . . . 80
B.6.1 Hidden reflection problem in the cyclic case . . . 81
B.6.2 Principle of the sieve: producing new states . . . 84
B.6.3 Sieving procedure in the case $N = r^n$ . . . 85

C Constructing hash proof systems with the OSIDH framework **90**
C.1 Definition of a hash proof system . . . 90
C.2 Hash proof system form weak-pseudorandom restricted effective group actions . . . 91
C.3 An original hash proof system combining SIDH with OSIDH . . . 93
C.3.1 Settings and public data . . . 95
C.3.2 The Hash Proof System HashOSIDH . . . 96

Acknowledgements

I am particularly grateful to my supervisor Luca De Feo. Early on, had he not placed his trust in me and fought the bureaucratic obstacles, my internship with IBM would not have been possible. Thank you Luca for your patience, your kindness, your rigour and your pedagogical qualities all along this internship. Thank you as well for giving me the opportunity to discover the beautiful landscapes of Switzerland on the week-ends.

I also would like to thank the IBM cryptography team for their warm welcome. I think about Romain Gay, Jonathan Bootle, Julia Hesse, Bertram Poettering, Vadim Lyubashevsky and Michael Osborne in particular. Last but not least, I am also very grateful to my professor Elisa Lorenzo Garcia for her strong support.

Introduction

In the incoming years, quantum computers might threaten mainstream cryptographic primitives based on the hardness of factoring integers and the discrete logarithm problem, creating the need for quantum-resistant primitives. Lattice based schemes seem to be the most promising and prevail in the US National Institute of Standards and Technology (NIST) competition meant to standardize post-quantum protocols. Indeed, among the finalists in the third round, three key encryption mechanisms out of four and two digital signature schemes out of three are lattice based. Nonetheless, isogeny based cryptography is not to be overlooked. Indeed, there is an isogeny based third round alternate candidate in the NIST competition: Supersingular Isogeny Key Encapsulation (SIKE) [7], based on Supersingular Isogeny Diffie-Hellman (SIDH) protocol [3] of De Feo and Jao. Even though isogeny based protocols are relatively slow, they are compact compared to their lattice based and code based analogues. However, poor time performance of isogeny based protocol is not inevitable, since a fast (and compact) isogeny signature scheme (SQISign) [8] has been proposed recently by De Feo, Kohel, Leroux, Petit and Wesolowski. Another advantage of isogeny based cryptography is to maintain diversity among post-quantum cryptographic primitives, since there is no theoretical guarantee preventing the existence of efficient quantum algorithms to solve lattice problems.

The goal of this thesis is to study Oriented Supersingular Isogeny Diffie Hellman (OSIDH), a new isogeny based primitive due to Colò and Kohel [4]. OSIDH is a generalization of Commutative Supersingular Isogeny Diffie Hellman (CSIDH) [5] due to Castryck, Lange, Martindale, Panny and Renes based itself on the foundational isogeny based protocol of Couveignes [2], rediscovered by Rostovtsev and Stolbunov [9].

As the latter, OSIDH relies on a *cryptographic group action* (also called effective group action), as defined in [10]. Namely, it means that we have a group G acting faithfully and transitively on a set X with the following security property: if $x \in X$ and $g \in G$, it is computationally hard to recover g with the knowledge of $(x, g \cdot x)$ only[1]. In the case of CSIDH and OSIDH, the cryptographic group action is *restricted*, meaning that we can only compute the action of a set S of group elements and their inverse. However, this restriction is not an issue in general when S generates G. One can naturally define a Diffie-Hellman protocol in a cryptographic group action $(G, X, \cdot)$, provided that G is abelian. Indeed, if we fix a public element $x_0 \in X$, Alice and Bob will select random elements g and $h \in G$ respectively (or random products of elements of a generating set S and their inverse if the action is restricted). Alice will compute $g \cdot x_0$ and Bob $h \cdot x_0$. Alice will transmit $g \cdot x_0$ to Bob and Bob will transmit $h \cdot x_0$ to Alice. Then Alice will act on Bob's data with g and Bob will act on Alice's data h, so that they both recover the shared secret:

$$g \cdot (h \cdot x_0) = h \cdot (g \cdot x_0) = (gh) \cdot x_0.$$

The security of such a protocol relies on the hardness to recover g knowing $(x, g \cdot x)$.

In CSIDH, X is the set of supersingular elliptic curves defined over $\mathbb{F}_p$ for $p \equiv 3$ [8] and G is the ideal class group $\mathrm{Cl}(\mathcal{O})$ of the ring $\mathcal{O} := \mathbb{Z}[\sqrt{-p}]$ isomorphic to the ring of $\mathbb{F}_p$-rational endomorphisms for all

[1] Alternate (but similar) security assumptions can be made. For instance, there is a decisional security hypothesis: given a secret element $g \in G$, an attacker cannot distinguish tuples $(x_i, g \cdot x_i)$ with $x_i \in X$ sampled uniformly at random from tuples (x_i, y_i) with $y_i \in X$ sampled uniformly at random.

$E \in X$. The group action is given by $\mathfrak{a} \cdot E := E/E[\mathfrak{a}]$ for every $\mathcal{O}$-ideal $\mathfrak{a}$ and $E \in X$. S is a set of splitting prime ideals $\mathfrak{l}_1, \cdots, \mathfrak{l}_t$ respectively lying above primes $\ell_1, \cdots, \ell_t$ such that $|E(\mathbb{F}_p)| = p + 1 = 4\prod_{i=1}^{t} \ell_i$ for all $E \in X$, so that the action of $\mathfrak{l}_i$ and $\overline{\mathfrak{l}_i}$ on E are efficiently computable by Vélu's formulas [11] because the ℓ_i-torsion is $\mathbb{F}_p$-rational. See [5] for details.

In CSIDH, the elliptic curves E in X are all oriented by the quadratic order $\mathcal{O} = \mathbb{Z}[\sqrt{-p}] \simeq \mathrm{End}_{\mathbb{F}_p}(E)$, meaning that we have an embedding $\mathcal{O} \hookrightarrow \mathrm{End}(E)$, mapping $\sqrt{-p}$ to the Frobenius endomorphism. In OSIDH, we do not restrict to supersingular elliptic curves defined over $\mathbb{F}_p$ and consider different orientations than the ring of $\mathbb{F}_p$-rational endomorphisms but the idea is roughly the same. What really changes is that the orientation used $\mathcal{O}$ is no longer the maximal order of $K := \mathcal{O} \otimes \mathbb{Q} = \mathbb{Q}(\sqrt{-p})$, the field of discriminant $-4p$. In OSIDH, K has a very small discriminant $\ll p$ and $\mathcal{O}$ has a huge prime power conductor ℓ^n. As in CSIDH, we have a restricted class group action by splitting prime ideals of $\mathcal{O}$, $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$, but the effective computation of the action by these primes is significantly different and involves ℓ-isogeny chains of length n. However, unfortunately, the security of OSIDH is weaker than that of CSIDH.

Overview of the thesis

Chapter 1 develops the useful mathematical framework of OSIDH, following the presentation of Colò and Kohel [4] and its improvements by Onuki [12]. We introduce the notions of oriented supersingular elliptic curves and isogenies and properly define an ideal class group action based on this notion. Then, we study oriented ℓ-isogeny graphs and apply our results to the study of ℓ-isogeny chains used as an algorithmic foundation to compute the cryptographic group action.

Chapter 2 introduces the OSIDH protocol. First, we present a (broken) naive Diffie-Hellman key exchange. Then, we present the real OSIDH protocol as introduced by Colò and Kohel in [4, § 5.2], which is an "implicit" version of the first one.

Chapter 3 introduces different attacks of OSIDH. First, we present two attacks against the naive Diffie-Hellman protocol due to Colò and Kohel. Then, we present an attack due to Onuki [12, § 6.3] on the stronger version of the protocol. We present an improvement of this attack based on a lattice reduction and some countermeasures to this new attack. We provide an implementation of our attack available on Github [13] running with toy parameters. We also provide test results indicating that this attack could scale up to realistic parameters like those proposed in [4, p.434] with optimizations and additional computational resources, since the limiting factor is the runtime of the protocol itself. We conclude this chapter with Kuperberg's quantum attack [14].

In the course of my internship, I also attempted to construct a hash proof system, another primitive based on the cryptographic group action property of OSIDH. Unfortunately, our cryptanalysis of OSIDH makes this primitive insecure so our construction fails. However, this attempt is presented in Appendix C.

Chapter 1

Mathematical framework of OSIDH

This chapter presents the essential mathematics to fully understand oriented supersingular elliptic curves. This notion was first introduced by Colò and Kohel [4] but we follow the approach of Onuki [12] which is more precise. After introducing the notion of orientation, we study oriented supersingular elliptic curves obtained by reducing elliptic curves defined over number fields in order to properly define an ideal class group action on oriented supersingular elliptic curves. Then, we study oriented isogeny graphs to prepare the study of isogeny chains and ladders, which are the algorithmic foundations of OSIDH.

1.1 Oriented supersingular elliptic curves

Let E/k be an elliptic curve defined over a field k. We denote by $\mathrm{End}^0(E)$ the tensor product $\mathrm{End}(E)\otimes\mathbb{Q}$. Let K be a quadratic imaginary number field.

Definition 1.1. A *K-orientation* of E is an embedding $\iota : K \hookrightarrow \mathrm{End}^0(E)$. 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 $\iota(\mathcal{O}) = \mathrm{End}(E)\cap\iota(K)$.

This definition only makes sense when E is a supersingular elliptic curve, otherwise, we always have $\iota(K) = \mathrm{End}^0(E)$, so there is (up to complex conjugation), only one such orientation (see [15, Corollary III.9.4 and Theorem V.3.1]). Hence, in the following, we shall always work with supersingular elliptic curves defined over $k = \mathbb{F}_{p^2}$.

Lemma 1.2. *Let (E,ι) be a K-oriented elliptic curve. Then :*

(i) *For all $\alpha \in \iota^{-1}(\mathrm{End}(E))$, $\iota(\overline{\alpha}) = \widehat{\iota(\alpha)}$, $\mathrm{Tr}(\iota(\alpha)) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ and $\deg(\iota(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$.*

(ii) *$\iota^{-1}(\mathrm{End}(E))$ is an order of K. In particular, every K-oriented elliptic curve admits a primitive orientation by an order of K.*

Proof. **(i)** Let $\alpha \in \iota^{-1}(\mathrm{End}(E))$. If $\alpha \in \mathbb{Z}$ then $\overline{\alpha} = \alpha$ and $\iota(\alpha) = \widehat{\iota(\alpha)}$, so that $\iota(\overline{\alpha}) = \widehat{\iota(\alpha)}$,

$$\mathrm{Tr}(\iota(\alpha)) = \iota^{-1}(\iota(\alpha) + \widehat{\iota(\alpha)}) = 2\alpha = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \quad \text{and} \quad \deg(\iota(\alpha)) = \iota^{-1}(\iota(\alpha)\widehat{\iota(\alpha)}) = \alpha\overline{\alpha} = N_{K/\mathbb{Q}}(\alpha).$$

Otherwise, $[\mathbb{Q}(\alpha) : \mathbb{Z}] = 2$ so that $X^2 - \mathrm{Tr}(\iota(\alpha))X + \deg(\iota(\alpha))$ is the minimal polynomial of α (it annihilates $\iota(\alpha)$, thus it annihilates α) so we can identify the trace and the norm.

(ii) By (i), $\iota^{-1}(\mathrm{End}(E)) \subseteq \mathcal{O}_K$ because every $\alpha \in \iota^{-1}(\mathrm{End}(E))$ is annihilated by the polynomial $X^2 - \mathrm{Tr}(\iota(\alpha))X + \deg(\iota(\alpha)) \in \mathbb{Z}[X]$. Then either $\iota^{-1}(\mathrm{End}(E)) = \mathbb{Z}$ or $\iota^{-1}(\mathrm{End}(E))$ is an order of K. The first case is impossible, otherwise we would have an embedding $K \hookrightarrow \mathbb{Q}$ with $[K : \mathbb{Q}] = 2$. □

Definition 1.3. Let (E, ι) be a K-oriented elliptic curve and $\varphi : E \longrightarrow F$ an isogeny. Then, we define a K-orientation $\varphi_*(\iota)$ on F by:

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

Let (E, ι_E) and (F, ι_F) be two K-oriented elliptic curves. An isogeny $\varphi : E \longrightarrow F$ is *K-oriented* if $\varphi_*(\iota_E) = \iota_F$. We denote this by $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$.

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.

Lemma 1.4. *There exist non-negative coprime integers $m, m' \in \mathbb{N}^*$ such that $\mathbb{Z} + m\mathcal{O} = \mathbb{Z} + m'\mathcal{O}'$ and $mm' | \deg(\varphi)$.*

Proof. Let f and f' be respectively the conductors of $\mathcal{O}$ and $\mathcal{O}'$. Let $e := \gcd(f, f')$. Then $f := m'e$ and $f' := me$ with $m, m' \in \mathbb{N}^*$, coprime. Then :

$$\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K = \mathbb{Z} + em'\mathcal{O}_K \quad \text{and} \quad \mathcal{O}' = \mathbb{Z} + f'\mathcal{O}_K = \mathbb{Z} + em\mathcal{O}_K$$

and we trivially have $\mathbb{Z} + m\mathcal{O} = \mathbb{Z} + mm'e\mathcal{O}_K = \mathbb{Z} + m'\mathcal{O}'$.

Since φ is K-oriented, we have $\deg(\varphi)\iota_F = \varphi\iota_E\widehat{\varphi}$, so that $\deg(\varphi)\iota_F(\mathcal{O}) \subseteq \mathrm{End}(E) \cap \iota_F(K) = \iota_F(\mathcal{O}')$ and $\deg(\varphi)\mathcal{O} \subseteq \mathcal{O}'$. Multiplying the equation $\deg(\varphi)\iota_F = \varphi\iota_E\widehat{\varphi}$ by $\widehat{\varphi}$ on the left and φ on the right, we get that $\deg(\varphi)\iota_E = \widehat{\varphi}\iota_F\varphi$ and we conclude that $\deg(\varphi)\mathcal{O}' \subseteq \mathcal{O}$.

It follows that :

$$\mathbb{Z} + m\deg(\varphi)\mathcal{O}' \subseteq \mathbb{Z} + m\mathcal{O} = \mathbb{Z} + m'\mathcal{O}'.$$

Taking a generator ω of $\mathcal{O}$ ($\mathcal{O} = \mathbb{Z}[\omega]$), we get that $m\deg(\varphi)\omega = a + bm'\omega$ for certain integers $a, b \in \mathbb{Z}$. It follows that $a = 0$ and $m\deg(\varphi) = bm'$ so that $m' | \deg(\varphi)$ because m and m' are coprime. By symmetry, $m | \deg(\varphi)$, so $mm' | \deg(\varphi)$. □

Proposition 1.5. *We assume that $\ell := \deg(\varphi)$ is a prime number. Then one of the following statements holds:*

(i) *$\mathcal{O} = \mathcal{O}'$, in which case, we say that φ is* horizontal.

(ii) *$\mathcal{O} \supsetneq \mathcal{O}'$ and $[\mathcal{O} : \mathcal{O}'] = \ell$, in which case, we say that φ is* descending.

(iii) *$\mathcal{O} \subsetneq \mathcal{O}'$ and $[\mathcal{O}' : \mathcal{O}] = \ell$, in which case, we say that φ is* ascending.

Proof. It follows immediately by the previous lemma. We have $\mathbb{Z} + m\mathcal{O} = \mathbb{Z} + m'\mathcal{O}'$ with m and m' coprime non-negative integers and $mm' | \ell$. Then, either $m = m' = 1$, in which case $\mathcal{O} = \mathcal{O}'$ or $m = \ell$ and $m' = 1$ in which case $\mathcal{O} \supsetneq \mathcal{O}' = \mathbb{Z} + \ell\mathcal{O}$ and $[\mathcal{O} : \mathcal{O}'] = \ell$ or $m = 1$ and $m' = \ell$ in which case $\mathcal{O} = \mathbb{Z} + \ell\mathcal{O}' \subsetneq \mathcal{O}'$ and $[\mathcal{O}' : \mathcal{O}] = \ell$. □

This is a first result indicating that K-oriented supersingular elliptic curves are similar to ordinary elliptic curves. We shall see deeper similarities (and differences) when we study K-oriented isogeny-graphs and the ideal class group action.

Example 1.6. We introduce an example of horizontal K-isogeny that will be reused later. Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve, ϕ_p the p-th power Frobenius defined on E and $E^{(p)}$ its image. Suppose that E admits a primitive $\mathcal{O}$-orientation ι. We denote by $\iota^{(p)}$ the K-orientation of $E^{(p)}$ given by $\iota^{(p)} := (\phi_p)_*(\iota)$. Then $(E^{(p)}, \iota^{(p)})$ is a primitive $\mathcal{O}$-orientation. In other words, ϕ_p is horizontal.

Indeed, if $\alpha \in \mathcal{O}$, then there exists $\psi \in \mathrm{End}(E^{(p)})$ such that $\phi_p \circ \iota(\alpha) = \psi \circ \phi_p$. ψ is obtained by raising the coefficients of the rational fractions defining $\iota(\alpha)$ to the power p. It follows that:

$$\iota^{(p)}(\alpha) = \frac{1}{p}\phi_p\iota(\alpha)\widehat{\phi_p} = \frac{1}{p}\psi\phi_p\widehat{\phi_p} = \frac{1}{p}\psi \circ [p] = \psi,$$

so that $\iota^{(p)}(\alpha) \in \mathrm{End}(E^{(p)})$. It follows that $\mathcal{O} \subseteq \left(\iota^{(p)}\right)^{-1}\left(\mathrm{End}\left(E^{(p)}\right)\right)$. Since:

$$\iota(\alpha) = \frac{1}{p}\widehat{\phi_p}\iota^{(p)}(\alpha)\phi_p,$$

we obtain the converse inclusion by similar arguments. Whence ϕ_p is horizontal.

Definition 1.7. A K-oriented isogeny $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$ is an isomorphism if φ is an isomorphism $E \longrightarrow F$ and its inverse defines a K-oriented isogeny $(F, \iota_F) \longrightarrow (E, \iota_E)$.

1.2 Reduction and oriented supersingular elliptic curves

1.2.1 Motivation

Let $\mathrm{SS}(p)$ be the set of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$ up to isomorphism (*i.e.* the set of supersingular j-invariants). Let $\mathrm{SS}_{\mathcal{O}}(p)$ and $\mathrm{SS}^{pr}_{\mathcal{O}}(p)$ be respectively the sets $\mathcal{O}$-oriented supersingular elliptic curves (respectively primitive) up to K-oriented isomorphism. As in the ordinary case, we have a group action :

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

We shall prove later that this action is well-defined (see Theorem 1.18 in particular). Although, contrary to the ordinary case, this action is not faithfully transitive the following example outlines.

Example 1.8. Let E be the elliptic curve defined over $\mathbb{F}_p$ by the Weierstrass equation $y^2 = x^3 + x$ with $p \equiv 3\ [4]$ (so that E is supersingular). Let $a \in \mathbb{F}_{p^2}$ such that $a^2 = -1$ and the isomorphism:

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

Since $\phi^2 = [-1]$, we have two primitive $\mathbb{Z}[i]$-orientations:

$$\begin{array}{rcl} \iota : \mathbb{Q}(i) & \longrightarrow & \mathrm{End}^0(E) \\ i & \longmapsto & \phi \end{array} \quad \text{and} \quad \begin{array}{rcl} \iota' : \mathbb{Q}(i) & \longrightarrow & \mathrm{End}^0(E) \\ i & \longmapsto & -\phi \end{array}.$$

These orientations are not isomorphic. Indeed, otherwise we would have an automorphism $\varphi \in \mathrm{Aut}(E)$ such that $\varphi_*(\iota) = \iota'$. However:

$$\mathrm{Aut}(E) = \{[1], [-1], \phi, -\phi\}$$

and we trivially have $[\pm 1]_*(\iota) = \iota$ and:

$$\forall \alpha \in \mathbb{Q}(i), \quad \phi_*(\iota)(\alpha) = \phi\iota(\alpha)\widehat{\phi} = \phi\iota(\alpha)(-\phi) = -\iota(i)\iota(\alpha)\iota(i) = \iota(-i^2\alpha) = \iota(\alpha),$$

so that $[\phi]_*(\iota) = \iota$. By the same computations, $[-\phi]_*(\iota) = \iota$. Then $(E, \iota) \not\simeq (E, \iota')$ so there are at least two isomorphism classes of primitive $\mathbb{Z}[i]$-orientations.

However, 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 $\mathrm{SS}^{pr}_{\mathbb{Z}[i]}(p)$ cannot be transitive.

We shall prove, nonetheless, that this result holds when we restrict to the good reductions of elliptic curves with complex multiplication by $\mathcal{O}$ over the complex numbers.

1.2.2 Reduction of elliptic curves with complex multiplication by $\mathcal{O}$

This paragraph is a bit technical and uses the mathematical prerequisites of Appendix A.2 on the reduction of elliptic curves defined over a number field.

We fix L a number field containing K and an elliptic curve E/L such that $\mathrm{End}(E) \simeq \mathcal{O}$. This is always possible if we take for E the elliptic curve defined over the complex numbers associated to the

complex torus $\mathbb{C}/\mathcal{O}$. Since E has complex multiplication by $\mathcal{O}$, we know that $j(E)$ is integral over $\mathbb{Z}$ by [16, Theorem II.6.1] so E is defined over the number field L generated by K and $j(E)$. We fix a *normalized* ring isomorphism $[.]_E : \mathcal{O} \longrightarrow \mathrm{End}(E)$, meaning that $[\alpha]_E^* \omega = \alpha\omega$ for all $\alpha \in \mathcal{O}$, where ω is the invariant differential of E (see [16, Proposition II.1.1]).

Let p be a prime number (≥ 5) and $\mathfrak{p}$ be a place above p. We suppose that E has good reduction modulo $\mathfrak{p}$. Then, we can define a K-orientation $[.]_{\overline{E}} : K \longrightarrow \mathrm{End}^0(\overline{E})$ as follows:

$$\forall \alpha \in \mathcal{O}, \quad [\alpha]_{\overline{E}} := [\alpha]_E \mod \mathfrak{p}.$$

Lemma 1.9. *Let E and F be two elliptic curves defined over L with complex multiplication by $\mathcal{O}$ and good reduction modulo $\mathfrak{p}$. If E and F are isomorphic, then the orientations $(\overline{E}, [.]_{\overline{E}})$ and $(\overline{F}, [.]_{\overline{F}})$ are K-isomorphic.*

Proof. Let $\lambda : E \longrightarrow F$ be an isomorphism. Since $[.]_E$ and $[.]_F$ are normalized, we have $[\alpha]_F = \lambda \circ [\alpha]_E \circ \lambda^{-1}$ for all $\alpha \in \mathcal{O}$ by [16, Corollary II.1.1.1]). Reducing this equality modulo $\mathfrak{p}$, we get by functoriality of the reduction that $[.]_{\overline{F}} = \overline{\lambda}_*([.]_{\overline{E}})$ where $\overline{\lambda} : \overline{E} \longrightarrow \overline{F}$ is the reduction of λ modulo $\mathfrak{p}$. This completes the proof. □

To understand better the reduction, we need two classical results due to Deuring:

Theorem 1.10 (Deuring, 1941)**.** *Let L be a number field and E an elliptic curve over L such that $\mathrm{End}(E) \simeq \mathcal{O}$. Let $\mathfrak{p}$ be a place above p. Suppose that E has good reduction modulo $\mathfrak{p}$. Then $\overline{E}$ is supersingular if and only if p does not split in K.*

Moreover, if $c := p^r c_0$ is the conductor of $\mathcal{O}$, with $r, c_0 \in \mathbb{N}$ such that $p \not| c_0$, then we have:

$$[.]_{\overline{E}}^{-1}(\mathrm{End}(\overline{E})) = \mathbb{Z} + c_0 \mathcal{O}_K.$$

Proof. See [17, chapter 13, Theorem 12]. The result given here is slightly more general than the one proved in [17] because the computation of $[.]_{\overline{E}}^{-1}(\mathrm{End}(\overline{E}))$ is only done in the ordinary case. However, the same ideas stand (one just needs to work with $[K]_{\overline{E}}$ instead of $\mathrm{End}^0(\overline{E})$). □

Theorem 1.11 (Deuring lifting theorem, 1941)**.** *Let F be an elliptic curve defined over a finite field k of characteristic p and $\psi \in \mathrm{End}(F)$. Then there exists a number field L, a place $\mathfrak{p}$ of $\mathcal{O}_L$ lying above p, an elliptic curve E/L and an endomorphism $\varphi \in \mathrm{End}(E)$ such that the reduction of E modulo $\mathfrak{p}$ is isomorphic to F and φ modulo $\mathfrak{p}$ is ψ.*

Proof. See [17, chapter 13, Theorem 14]. □

Proposition 1.12. *$\mathrm{SS}_{\mathcal{O}}^{pr}(p)$ is not empty if and only if p does not split in K and does not divide the conductor of $\mathcal{O}$.*

Proof. $\Longleftarrow$ We suppose that p does not split in K and that p does not divide the conductor of $\mathcal{O}$. Let L be a number field containing K and an elliptic curve E/L such that $\mathrm{End}(E) \simeq \mathcal{O}$. Then $j(E)$ is an algebraic integer by [16, Theorem II.6.1] so E has potential good reduction by Proposition A.3. Replacing L by a finite field extension if necessary, we may then assume that E has good reduction modulo $\mathfrak{p}$. Since p does not split in K and does not divide the conductor of $\mathcal{O}$, we get that the reduction of E mod $\mathfrak{p}$, $\overline{E}$ is supersingular and that $[.]_{\overline{E}}^{-1}(\mathrm{End}(\overline{E})) = \mathcal{O}$, by the Theorem 1.10. It follows that $(\overline{E}, [.]_{\overline{E}}) \in \mathrm{SS}_{\mathcal{O}}^{pr}(p)$.

$\Longrightarrow$ Suppose that $\mathrm{SS}_{\mathcal{O}}^{pr}(p) \neq \emptyset$ and let $(F, \iota) \in \mathrm{SS}_{\mathcal{O}}^{pr}(p)$. Let $\alpha \in \mathcal{O}$ be a generator of $\mathcal{O}$: $\mathcal{O} = \mathbb{Z}[\alpha]$. Then by Theorem 1.11, there exist a number field L containing K (we may take an extension of L if necessary), a place $\mathfrak{p}$ of $\mathcal{O}_L$ lying above p, an elliptic curve E/L and an endomorphism $\varphi \in \mathrm{End}(E)$ such that E has good reduction modulo $\mathfrak{p}$, the reduction modulo $\mathfrak{p}$, denoted by $\overline{E}$ is isomorphic to F and $\varphi \mod \mathfrak{p} = \iota(\alpha)$. Since α generates $\mathcal{O}$, it is not an integer and neither is φ (because φ is a root of the minimal polynomial of α since the reduction mod $\mathfrak{p}$ is a ring homomorphism and ι is

injective), so we have $\mathrm{End}^0(E) = \mathbb{Q}(\varphi)$ and the reduction map $\mathrm{End}(E) \longrightarrow \mathrm{End}(F)$ has its image in $\mathbb{Q}(\varphi \bmod \mathfrak{p}) = \mathbb{Q}(\iota(\alpha)) = \iota(\mathbb{Q}(\alpha)) = \iota(K)$. Since (F, ι) is a primitive $\mathcal{O}$-orientation and the reduction map is injective, we have an injective ring homomorphism:

$$\mathrm{End}(E) \overset{\bmod \mathfrak{p}}{\longrightarrow} \mathrm{End}(F) \cap \iota(K) \overset{\iota^{-1}}{\longrightarrow} \mathcal{O}$$

and an injective ring homomorphism $\mathcal{O} \longrightarrow \mathrm{End}(E)$ mapping α to φ. Whence $\mathrm{End}(E) \simeq \mathcal{O}$ so by Theorem 1.10, p does not divide the conductor of $\mathcal{O}$. Moreover, p does not split in K because $F = \overline{E}$ is supersingular. □

In the following, we assume that p does not split in K and does not contain the conductor of $\mathcal{O}$, so that $\mathrm{SS}^{pr}_{\mathcal{O}}(p)$ is not empty. Let $\mathrm{Ell}(\mathcal{O})$ be the set of isomorphism classes of elliptic curves defined over $\mathbb{C}$ with complex multiplication by $\mathcal{O}$ (*i.e.* with endomorphism ring isomorphic to $\mathcal{O}$). As we saw, every class $[E] \in \mathrm{Ell}(\mathcal{O})$ admits a representative E defined over a number field L_E containing K and any place $\mathfrak{p}$ lying above p has potential good reduction modulo $\mathfrak{p}$, so there is a finite field extension L'/L_E and a place $\mathfrak{P}$ lying above $\mathfrak{p}$ such that E has good reduction modulo $\mathfrak{P}$. Let L'_E be the field generated by the union of these extensions when $\mathfrak{p}$ varies. It is still a number field because there are finitely many places in $\mathcal{O}_L$ lying above p ($\mathcal{O}_L$ is Dedekind). Moreover, $\mathrm{Ell}(\mathcal{O})$ is finite (by [16, Proposition II.2.1.(b)]). Then, the field L generated by all the fields L'_E is a number field (containing K) and every elliptic curve E with complex multiplication by $\mathcal{O}$ is defined over L (up to isomorphism) and has good reduction modulo any place $\mathfrak{p}$ of L lying above p. We shall fix L and $\mathfrak{p}$ in the following. Then, we have a map given by the reduction modulo $\mathfrak{p}$:

$$\begin{array}{rcl} \rho : \mathrm{Ell}(\mathcal{O}) & \longmapsto & \mathrm{SS}^{pr}_{\mathcal{O}}(p) \\ E & \longmapsto & (\overline{E}, [.]_{\overline{E}}) \end{array}.$$

This map is actually not surjective (that is why the action described in Example 1.8 fails to be transitive), however we have a comforting result.

Proposition 1.13. *For all $(F, \iota) \in \mathrm{SS}^{pr}_{\mathcal{O}}(p)$, we either have $(F, \iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$ or $(F^{(p)}, \iota^{(p)}) \in \rho(\mathrm{Ell}(\mathcal{O}))$.*

Proof. Let $(F, \iota) \in \mathrm{SS}^{pr}_{\mathcal{O}}(p)$. Then, as in the proof of the direct implication of Proposition 1.12, there exist a number field L' containing K, a place $\mathfrak{p}'$ of $\mathcal{O}_{L'}$ lying above p, an elliptic curve E/L' such that E has good reduction modulo $\mathfrak{p}'$, the reduction modulo $\mathfrak{p}'$, $\overline{E}$ is isomorphic to F and $\mathrm{End}(F) \simeq \mathcal{O}$. We also have obtained in the proof of Proposition 1.12, that $(\overline{E}, [.]_{\overline{E}})$ is a primitive $\mathcal{O}$-orientation satisfying $[K]_{\overline{E}} = \iota(K)$. Then the composition:

$$K \overset{[.]_{\overline{E}}}{\longrightarrow} [K]_{\overline{E}} = \iota(K) \overset{\iota^{-1}}{\longrightarrow} K$$

is a field automorphism so it is either the identity or the complex conjugation, so we either have $[\alpha]_{\overline{E}} = \iota(\alpha)$ or $[\alpha]_{\overline{E}} = \iota(\overline{\alpha})$ for all $\alpha \in K$. In the first case, $(\overline{E}, [.]_{\overline{E}})$ is K-isomorphic to (F, ι).

Now we assume that $[\alpha]_{\overline{E}} = \iota(\overline{\alpha})$ for all $\alpha \in K$. Replacing L' by the field extension generated by the conjugates of a generator of L' if necessary, we may assume that $L'/\mathbb{Q}$ is Galois. Let $G_{\mathfrak{p}'}$ be the decomposition group of $\mathfrak{p}'$:

$$G_{\mathfrak{p}'} := \{\sigma \in \mathrm{Gal}(L', \mathbb{Q}) \mid \sigma(\mathfrak{p}') = \mathfrak{p}'\}.$$

There exists $\sigma \in G_{\mathfrak{p}'}$ whose restriction to K is not trivial. Indeed, otherwise by [18, Corollary I.3], K would be contained in the subfield L'' fixed by $\mathfrak{p}'$, which is the maximal field subextension of L' in which p splits completely. But p does not split in K so there is only one prime ideal $\mathfrak{q}$ lying above p and all prime ideals of L'' lying above p would be lying above $\mathfrak{q}$ so there would be at most $[L'' : K] < [L'' : \mathbb{Q}]$ such prime ideals by [18, chapter I, Proposition 11] and p would not split completely in L''. Contradiction.

Then, we may take $\sigma \in G_{\mathfrak{p}'}$ such that $\sigma_{|K}$ is the complex conjugation. As in [16, § II.2], we define a

map:

$$\begin{array}{ccc} \mathrm{End}(E) & \longrightarrow & \mathrm{End}(E^\sigma) \\ \phi & \longmapsto & \phi^\sigma \end{array},$$

where E^σ is obtained from E by letting σ act on the coefficients of its Weierstrass equation and ϕ^σ is given by the action of σ on the coefficients of the rational fractions defining ϕ. We have by [16, Theorem II.2.2.(a)], $([\overline{\alpha}]_E)^\sigma = [\sigma(\overline{\alpha})]_{E^\sigma} = [\alpha]_{E^\sigma}$ for all $\alpha \in K$. Hence:

$$\forall \alpha \in K, \quad [\alpha]_{E^\sigma} \mod \mathfrak{p}' \equiv ([\overline{\alpha}]_E)^\sigma \mod \mathfrak{p}' \equiv ([\overline{\alpha}]_E \mod \mathfrak{p}')^{\overline{\sigma}} = ([\overline{\alpha}]_{\overline{E}})^{\overline{\sigma}} = (\iota(\alpha))^{\overline{\sigma}},$$

where $\overline{\sigma} \in \mathrm{Gal}(\mathcal{O}_{L'}/\mathfrak{p}', \mathbb{F}_p)$ is obtained by reduction of σ modulo $\mathfrak{p}'$. Furthermore, $\overline{E^\sigma} = F^{\overline{\sigma}}$. By the following lemma, we can assume that $\overline{\sigma}$ is either the identity or the p-th power Frobenius. It follows that $[.]_{\overline{E^\sigma}} = \iota$ or $\iota^{(p)}$ *i.e.* that the reduction $(\overline{E^\sigma}, [.]_{\overline{E^\sigma}})$ is either K-isomorphic to (F, ι) or $(F^{(p)}, \iota^{(p)})$.

Lemma 1.14. *Let H be the subgroup of $G_{\mathfrak{p}'}$ formed by elements fixing K. Then, the coset σH is formed of elements of $G_{\mathfrak{p}'}$ whose restriction on K is the complex conjugation. The reduction $\overline{\sigma}\overline{H}$ of σH mod $\mathfrak{p}'$ contains either the identity or the p-th power Frobenius.*

Proof. By [18, propostion I.14], the reduction map $G_{\mathfrak{p}'} \longrightarrow G := \mathrm{Gal}(\mathcal{O}_{L'}/\mathfrak{p}', \mathbb{F}_p)$ is a surjective group homorphism. Since $G_{\mathfrak{p}'} := H \sqcup \sigma H$, we also have $G = \overline{H} \cup \overline{\sigma}\overline{H}$. If $\overline{\sigma} \in \overline{H}$, then $G = \overline{H} = \overline{\sigma}\overline{H}$ and both the identity or the p-th power Frobenius are in $\overline{\sigma}\overline{H}$.

Let us assume that $\overline{\sigma} \notin \overline{H}$. Then $G = \overline{H} \sqcup \overline{\sigma}\overline{H}$ and $\overline{H}$ is a subgroup of index 2 in G. Since G is cyclic and generated by the p-th power Frobenius σ_p, $\overline{H}$ is generated by σ_p^2, so that:

$$\overline{H} = \{\sigma_p^k \mid k \text{ even}\} \quad \text{and} \quad \overline{\sigma}\overline{H} = \{\sigma_p^k \mid k \text{ odd}\}.$$

Then $\overline{\sigma}\overline{H}$ contains σ_p, which completes the proof of the lemma. □

In both cases ($[\alpha]_{\overline{E}} = \iota(\alpha)$ or $[\alpha]_{\overline{E}} = \iota(\overline{\alpha})$ for all $\alpha \in K$), we have obtained an elliptic curve E over L' with good reduction mod $\mathfrak{p}'$ such that $\mathrm{End}(E) \simeq \mathcal{O}$ and $(\overline{E}, [.]_{\overline{E}})$ is K-isomorphic to (F, ι) or $(F^{(p)}, \iota^{(p)})$.

If $L' \subseteq L$ and $\mathfrak{p}' \subseteq \mathfrak{p}$, the proof is complete. We now prove that we can reduce to this case. Let M be the field generated by L' and the K-conjugates of a generator of L. Then M/K is a Galois extension of L/K and L'/K. Let $\mathfrak{P}$ and $\mathfrak{P}'$ be prime ideals of $\mathcal{O}_M$ lying above $\mathfrak{p}$ and $\mathfrak{p}'$ respectively. Since p does not split in K, there is a unique prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ lying above p, so that $\mathfrak{p}, \mathfrak{p}', \mathfrak{P}$ and $\mathfrak{P}'$ lie above $\mathfrak{q}$. By transitivity of the Galois group action on prime ideals [18, Proposition I.11], there exists $\sigma \in \mathrm{Gal}(M, K)$ such that $\sigma(\mathfrak{P}') = \mathfrak{P}$. Then, by [16, Theorem II.2.2.(a)], we have $([\alpha]_E)^\sigma = [\sigma(\alpha)]_{E^\sigma} = [\alpha]_{E^\sigma}$. It follows that:

$$\forall \alpha \in K, \quad [\alpha]_{E^\sigma} \mod \mathfrak{P} \equiv ([\alpha]_E)^\sigma \mod \sigma(\mathfrak{P}') \equiv ([\alpha]_E \mod \mathfrak{P}')^{\overline{\sigma}} = ([\alpha]_{\overline{E}})^{\overline{\sigma}},$$

where $\overline{\sigma} : \mathcal{O}_M/\mathfrak{P}' \longrightarrow \mathcal{O}_M/\mathfrak{P}$ is the finite field isomorphism induced by σ. Since the fields are finite, this isomorphism could be seen as a finite field automorphism fixing $\mathcal{O}_K/\mathfrak{q}$, *i.e.* as a power of the Frobenius $p^{N(\mathfrak{q})}$-th power. Moreover, we have for all $\tau \in G_{\mathfrak{P}}$, $\tau\sigma(\mathfrak{P}') = \tau(\mathfrak{P}) = \mathfrak{P}$ and the reduction map $G_{\mathfrak{P}} \longrightarrow \mathrm{Gal}(\mathcal{O}_M/\mathfrak{P}, \mathcal{O}_K/\mathfrak{q})$ is surjective so we may assume that $\overline{\sigma}$ is the identity. Hence, we get that the reduction of $(E^\sigma, [.]_{E^\sigma})$ modulo $\mathfrak{P}$ is $(\overline{E}, [.]_{\overline{E}})$. Since $\mathrm{End}(E^\sigma) \simeq \mathrm{End}(E) \simeq \mathcal{O}$ by [16, Proposition II.2.1], we have $[E^\sigma] \in \mathrm{Ell}(\mathcal{O})$ so there exists an elliptic curve E' defined over L with good reduction modulo $\mathfrak{p}$ isomorphic to E^σ. As $\mathfrak{P}$ lies above $\mathfrak{p}$, this completes the proof. □

1.3 The ideal class group action

We shall now define a group action of $\mathrm{Cl}(\mathcal{O})$ on $\rho(\mathrm{Ell}(\mathcal{O}))$, as announced previously, and prove that it is faithful and transitive. Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}$. According to [19, Corollary 7.17], we can

assume that $N(\mathfrak{a})$ is prime to p without changing the class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O})$. We shall always work under this assumption in the following. We define the $\mathfrak{a}$-torison of E by:

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

$E[\mathfrak{a}]$ is finite, so [15, Proposition III.4.12] ensures that there exists an elliptic curve E' and a separable isogeny $\varphi : E \longrightarrow E'$ such that $\ker(\varphi) = E[\mathfrak{a}]$. (E', φ) is unique up to isomorphism. Indeed, if $\varphi' : E \longrightarrow E''$ has the kernel, then there exists an isomorphism $\lambda : E' \longrightarrow E''$ such that $\varphi' = \lambda \circ \varphi$. Then, we have $\varphi'_*(\iota) = \lambda_*(\varphi_*(\iota))$ and λ being an endomorphism, $(E', \varphi_*(\iota))$ is K-isomorphic to $(E'', \varphi'_*(\iota))$. Then, $(E', \varphi_*(\iota))$ is uniquely determined by $\mathfrak{a}$ up to K-isomorphism. In the following, for a given ideal $\mathfrak{a}$ of $\mathcal{O}$ we shall refer to E', φ and $(E', \varphi_*(\iota))$ as $E/E[\mathfrak{a}]$, $\varphi_\mathfrak{a}$ and $\mathfrak{a} \cdot (E, \iota)$ respectively.

Proposition 1.15. *Let (E, ι) be a primitively $\mathcal{O}$-oriented elliptic curve and $\mathfrak{a}$ an ideal of $\mathcal{O}$ of norm prime to p.*

(i) *Let $(E', \iota') := \mathfrak{a} \cdot (E, \iota)$, $\mathcal{O}' := \iota'^{-1}(\mathrm{End}(E'))$ and $\mathfrak{b}$ an ideal of $\mathcal{O}'$ of norm prime to p. We suppose that $\mathcal{O}' \subseteq \mathcal{O}$. Then $\ker(\varphi_\mathfrak{b} \circ \varphi_\mathfrak{a}) = E[\mathfrak{b}\mathfrak{a}]$.*

(ii) $\deg(\varphi_\mathfrak{a}) = N(\mathfrak{a})$.

(iii) *$\varphi_\mathfrak{a}$ is either horizontal or ascending ($\mathcal{O} \subseteq \mathcal{O}'$).*

(iv) *If $\mathfrak{a}$ is invertible, then $\varphi_\mathfrak{a}$ is horizontal. In addition, we have $\ker(\widehat{\varphi_\mathfrak{a}}) = E'[\overline{\mathfrak{a}}]$.*

Proof. **(i)** This is a difficult result, beyond the scope of this thesis, that becomes natural with the framework of abelian varieties. The classical reference for this fact is Waterhouse's thesis [20, Proposition 3.12] but the proof of Milne given in his lecture notes on complex multiplication [21, Proposition 7.28] may be easier to follow.

(ii) See [20, Theorem 3.15] or [21, Proposition 7.29].

(iii) We may assume that $E[\mathfrak{a}]$ is cyclic. Indeed, we suppose that this is not the case. The theorem of finite abelian group structure and the Chinese remainder theorem ensure that $E[\mathfrak{a}]$ is isomorphic to a product of its Sylow subgroups. Since $E[\mathfrak{a}]$ is not cyclic, it contains a non cyclic q-Sylow subgroup (otherwise, it would be cyclic by the Chinese remainder theorem). Hence, the q-torsion subgroup of $E[\mathfrak{a}]$ is of the form $(\mathbb{Z}/q\mathbb{Z})^b$ with $b \geq 2$, so that $E[q] \simeq (\mathbb{Z}/q\mathbb{Z})^2 \subseteq E[\mathfrak{a}] \subseteq \ker(\iota(\alpha))$ for all $\alpha \in \mathfrak{a}$. Since $E[q] \simeq (\mathbb{Z}/q\mathbb{Z})^2$ here, $[q] = \iota(q)$ is separable and for all $\alpha \in \mathfrak{a}$, we have a factorization $\iota(\alpha) = \lambda_\alpha \circ \iota(q)$ with $\lambda_\alpha = \iota(\alpha/q) \in \mathrm{End}(E)$ by [15, Corollary III.4.11]. Hence, $\mathfrak{a}$ is divisible by q, and furthermore, $E[q] \subseteq \ker(\varphi_\mathfrak{a})$ so $\varphi_\mathfrak{a}$ factors through $[q] = \iota(q)$ which is horizontal, so we may replace it by $\mathfrak{a}/q$. Applying this process iteratively makes $E[\mathfrak{a}]$ cyclic.

Let $n := \deg(\varphi_\mathfrak{a}) = N(\mathfrak{a})$. Then $E[\mathfrak{a}] \subseteq E[n]$. Since $\varphi_\mathfrak{a}$ is separable by construction, $|E[\mathfrak{a}]| = n$ so that $E[\mathfrak{a}] \simeq \mathbb{Z}/n\mathbb{Z}$ and p does not divide n so that $E[n] \simeq (\mathbb{Z}/n\mathbb{Z})^2$. Hence there exists a $\mathbb{Z}/n\mathbb{Z}$-basis (P, Q) of $E[n]$ such that P generates $E[\mathfrak{a}]$, according to the following lemma.

Lemma 1.16. *Let $(G, +)$ be an abelian group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ and $g \in G$ of order n. Then, there exists $h \in G$ such that (g, h) generate G.*

Proof. Let (g', h') be a $\mathbb{Z}/n\mathbb{Z}$-basis of G (it does exist because G is a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2). Then there exists $k, l \in \mathbb{N}$ such that $kg' + lh' = g$. Since g is of order n, $\gcd(n, k, l) = 1$ so there exists $u, v, w \in \mathbb{Z}$ such that $un + vk + wl = 1$. Let $h := -wg' + vh'$. We prove that (g, h) generates G *i.e.* that $(\lambda, \mu) \in (\mathbb{Z}/n\mathbb{Z})^2 \longmapsto \lambda g + \mu h \in G$ is surjective. By cardinality, it suffices to show that this group homomorphism is injective. Let $(\lambda, \mu) \in (\mathbb{Z}/n\mathbb{Z})^2$ such that $\lambda g + \mu h = 0$. Then $(\lambda k - w\mu)g' + (\lambda l + \mu w)h' = 0$ so that $\lambda k - w\mu \equiv 0\ [n]$ and $\lambda l + \mu w \equiv 0\ [n]$ because (g', h') be a $\mathbb{Z}/n\mathbb{Z}$-basis. Then $0 \equiv v(\lambda k - w\mu) + w(\lambda l + \mu w) \equiv \lambda\ [n]$ and $0 \equiv l(\lambda k - w\mu) - k(\lambda l + \mu w) \equiv \mu\ [n]$, which completes the proof. □

Let $P' \in E$ such that $P = nP'$ (it does exist because $[n]$ is surjective as any non-zero isogeny). Then, $[n] \circ \varphi_{\mathfrak{a}}(P') = \varphi_{\mathfrak{a}}([n]P') = \varphi_{\mathfrak{a}}(P) = O$ and $[n] \circ \varphi_{\mathfrak{a}}(Q) = \varphi_{\mathfrak{a}}([n]Q) = O$ so that $\varphi_{\mathfrak{a}}(P'), \varphi_{\mathfrak{a}}(Q) \in E'[n]$. Furthermore, by [15, Proposition III.8.2], we have:

$$e_n(\varphi_{\mathfrak{a}}(P'), \varphi_{\mathfrak{a}}(Q)) = e_n(\widehat{\varphi_{\mathfrak{a}}}\varphi_{\mathfrak{a}}(P'), Q) = e_n([n]P', Q) = e_n(P, Q).$$

Where e_n is the Weil pairing, as defined in [15, III.8]. So $(\varphi_{\mathfrak{a}}(P'), \varphi_{\mathfrak{a}}(Q))$ generates $E'[n]$ by the following lemma.

Lemma 1.17. *Let $(R, S) \in E[n]^2$. Then, (R, S) generates $E[n]$ if and only if $e_n(R, S)$ is a primitive n-th root of unity.*

Proof. $\implies$ Suppose that (R, S) generates $E[n]$. Let $d \in \mathbb{Z}$ such that $e_n(R, S)^d = 1$. Then for all $a, b \in \mathbb{Z}$, we have:

$$e_n([a]R + [b]S, [d]S) = e_n(R, S)^{ad} = 1,$$

so that $e_n(T, [d]S) = 1$ for all $T \in E[n]$. Since e_n is non-degenerate, $[d]S = O$ and $n|d$.

$\impliedby$ Suppose that $e_n(R, S)$ is a primitive n-th root of unity. Let $a, b \in \mathbb{Z}$ such that $[a]R + [b]S = O$. Then:

$$1 = e_n([a]R + [b]S, S) = e_n(R, S)^a \quad \text{and} \quad 1 = e_n(R, [a]R + [b]S) = e_n(R, S)^b,$$

so that $n|a$ and $n|b$. Hence (R, S) generates $E[n]$. □

We have for all $\alpha \in \mathfrak{a}$ and $\beta \in \mathcal{O}$:

$$\iota(\alpha) \circ \iota(\beta) \circ \widehat{\varphi_{\mathfrak{a}}} \circ \varphi_{\mathfrak{a}}(P') = \iota(\alpha\beta)([n]P') = \iota(\beta) \circ \iota(\alpha)(P) = O,$$

so that $\iota(\beta) \circ \widehat{\varphi_{\mathfrak{a}}} \circ \varphi_{\mathfrak{a}}(P') \in \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) = E[\mathfrak{a}]$ and we have for all $\beta \in \mathcal{O}$:

$$\varphi_{\mathfrak{a}} \circ \iota(\beta) \circ \widehat{\varphi_{\mathfrak{a}}} \circ \varphi_{\mathfrak{a}}(P') = O.$$

We also trivially have for all $\beta \in \mathcal{O}$:

$$\varphi_{\mathfrak{a}} \circ \iota(\beta) \circ \widehat{\varphi_{\mathfrak{a}}} \circ \varphi_{\mathfrak{a}}(Q) = \varphi_{\mathfrak{a}} \circ \iota(\beta)([n]Q) = \varphi_{\mathfrak{a}} \circ \iota(\beta)(O) = O.$$

Then $E'[n] \subseteq \ker(\varphi_{\mathfrak{a}} \circ \iota(\beta) \circ \widehat{\varphi_{\mathfrak{a}}})$ since $(\varphi_{\mathfrak{a}}(P'), \varphi_{\mathfrak{a}}(Q))$ generates $E'[n]$. By [15, Corollary III.4.11], it follows that n divides $\varphi_{\mathfrak{a}} \circ \iota(\beta) \circ \widehat{\varphi_{\mathfrak{a}}}$, so that $\iota'(\beta) = \varphi_{\mathfrak{a}*}(\iota)(\beta) \in \mathrm{End}(E')$ for all $\beta \in \mathcal{O}$. Hence $\mathcal{O} \subseteq \iota'^{-1}(\mathrm{End}(E')) = \mathcal{O}'$ and $\varphi_{\mathfrak{a}}$ is horizontal or ascending.

(iv) First, we prove that $\ker(\widehat{\varphi_{\mathfrak{a}}}) = E'[\overline{\mathfrak{a}}\mathcal{O}']$. Since $\mathfrak{a}$ is invertible [19, Lemma 7.14.(iii)] ensures that $\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O} = n\mathcal{O}$ *i.e.* that $\overline{\mathfrak{a}} = n\mathfrak{a}^{-1}$.

We keep the notations of (iii) and the point Q in particular. Since $Q \in E[n]$, we have $\varphi_{\mathfrak{a}}(Q) \in \ker(\widehat{\varphi_{\mathfrak{a}}})$. But $(\varphi_{\mathfrak{a}}(P'), \varphi_{\mathfrak{a}}(Q))$ generate $E[n]$ so $\varphi_{\mathfrak{a}}(Q)$ is of order $n = \deg(\widehat{\varphi_{\mathfrak{a}}})$ so $\varphi_{\mathfrak{a}}(Q)$ generates $\ker(\widehat{\varphi_{\mathfrak{a}}})$. For all $\alpha \in \mathfrak{a}$ and $\beta \in \mathfrak{a}^{-1}$, we have:

$$\iota(\alpha) \circ \iota(n\beta)(Q) = \iota(\alpha\beta)([n]Q) = O.$$

Hence $\iota(n\beta)(Q) \in \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)) = E[\mathfrak{a}]$ so that for all $\beta \in \mathfrak{a}^{-1}$:

$$O = \varphi_{\mathfrak{a}}(\iota(n\beta)(Q)) = \iota'(n\beta)\varphi_{\mathfrak{a}}(Q)$$

and $\varphi_{\mathfrak{a}}(Q) \in E'[n\mathfrak{a}^{-1}\mathcal{O}'] = E'[\overline{\mathfrak{a}}\mathcal{O}']$. It follows that $\ker(\widehat{\varphi_{\mathfrak{a}}}) \subseteq E'[\overline{\mathfrak{a}}\mathcal{O}']$.

Conversely, let $R \in E'[\overline{\mathfrak{a}}\mathcal{O}']$. Since $\varphi_{\mathfrak{a}}$ is not constant, it is surjective and there exists $S \in E$ such that $R = \varphi_{\mathfrak{a}}(S)$. For all $\beta \in \mathfrak{a}^{-1}$, we have:

$$\varphi_{\mathfrak{a}}(\iota(n\beta)(S)) = \iota'(n\beta)(\varphi_{\mathfrak{a}}(S)) = \iota'(n\beta)(R) = O,$$

so that $\iota(\alpha)\circ\iota(n\beta)(S) = O$ for all $\alpha \in \mathfrak{a}$. Since $\mathfrak{a}\mathfrak{a}^{-1} = \mathcal{O}$, there exists $\alpha_1, \cdots, \alpha_r \in \mathfrak{a}$ and $\beta_1, \cdots, \beta_r \in \mathfrak{a}^{-1}$ such that $\sum_{i=1}^{r} \alpha_i\beta_i = 1$ and we have:

$$[n]S = \iota\left(\sum_{i=1}^{r} \alpha_i n\beta_i\right)(S) = \sum_{i=1}^{r} \iota(\alpha_i)\iota(n\beta_i)(S) = O.$$

Hence $O = [n]S = \widehat{\varphi_{\mathfrak{a}}}(\varphi_{\mathfrak{a}}(S)) = \widehat{\varphi_{\mathfrak{a}}}(R)$ and $R \in \ker(\widehat{\varphi_{\mathfrak{a}}})$.

We conclude that $\ker(\widehat{\varphi_{\mathfrak{a}}}) = E'[\overline{\mathfrak{a}}\mathcal{O}']$, so that $\widehat{\varphi_{\mathfrak{a}}}$ is the isogeny $\varphi_{\overline{\mathfrak{a}}\mathcal{O}'}$ associated to the ideal $\overline{\mathfrak{a}}\mathcal{O}'$. Applying (iii) in the other direction, we get that $\mathcal{O}' \subseteq \mathcal{O}$ *i.e.* that $\varphi_{\mathfrak{a}}$ is horizontal. □

The previous proposition was our first step towards the proof of the desired theorem:

Theorem 1.18. $\mathrm{Cl}(\mathcal{O})$ *acts faithfully and transitively on* $\rho(\mathrm{Ell}(\mathcal{O}))$ *via:* $(\mathfrak{a}, (E,\iota)) \longmapsto \mathfrak{a}\cdot(E,\iota)$.

Proof. First of all, we prove that the map $(\mathfrak{a}, (E,\iota)) \longmapsto \mathfrak{a}\cdot(E,\iota)$ defines a group action of $\mathrm{Cl}(\mathcal{O})$ on $\rho(\mathrm{Ell}(\mathcal{O}))$.

Let $(F,\iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$ and let $E \in \mathrm{Ell}(\mathcal{O})$ such that $\rho(E) = (F,\iota)$ *i.e.* such that $(\overline{E}, [.]_{\overline{E}}) \simeq (F,\iota)$. Let $\mathfrak{a}$ be an invertible ideal of $\mathcal{O}$ of norm prime to p. It is a general fact that the kernel of the reduction modulo $\mathfrak{p}$ of an isogeny is the reduction modulo $\mathfrak{p}$ of its kernel. It follows that the reduction modulo $\mathfrak{p}$ of $E[\mathfrak{a}] := \bigcap_{\alpha\in\mathfrak{a}} \ker([\alpha]_E)$ is:

$$\overline{E[\mathfrak{a}]} = \bigcap_{\alpha\in\mathfrak{a}} \overline{\ker([\alpha]_E)} = \bigcap_{\alpha\in\mathfrak{a}} \ker(\overline{[\alpha]_E}) = \bigcap_{\alpha\in\mathfrak{a}} \ker([\alpha]_{\overline{E}}) = \overline{E}[\mathfrak{a}] = F[\mathfrak{a}].$$

By [15, Proposition III.4.12], there exists an isogeny $\phi : E \longrightarrow E'$ such that $\ker(\phi) = E[\mathfrak{a}]$. By the theory of complex multiplication over the complex numbers, we have $E' \in \mathrm{Ell}(\mathcal{O})$ (see [16, Proposition II.2.1.(a).(ii)] which is still valid for any order $\mathcal{O}$ and not only for $\mathcal{O}_K$). Then, we can assume that E' is defined over L and has good reduction modulo $\mathfrak{p}$. The reduction of ϕ modulo $\mathfrak{p}$, denoted by $\overline{\phi} : \overline{E} \longrightarrow \overline{E'}$, has kernel $\overline{E[\mathfrak{a}]} = F[\mathfrak{a}]$ so $\overline{E'}$ is isomorphic to $F/F[\mathfrak{a}]$ and $\overline{\phi} = \varphi_{\mathfrak{a}}$. Furthermore, we have for all $\alpha \in K$, $\phi[\alpha]_E = [\alpha]_{E'}\phi$ by [16, Corollary II.1.1.1]. The reduction modulo $\mathfrak{p}$ of this formula ensures that $\varphi_{\mathfrak{a}*}(\iota) = \overline{\phi}_*([.]_{\overline{E}}) = [.]_{\overline{E'}}$. Whence:

$$\mathfrak{a}\cdot(F,\iota) = (F/F[\mathfrak{a}], \varphi_{\mathfrak{a}*}(\iota)) = (\overline{E'}, [.]_{\overline{E'}}) = \rho(E').$$

We have proved that we have a well defined map $(\mathfrak{a}, (E,\iota)) \in \mathcal{I}_p(\mathcal{O}) \times \rho(\mathrm{Ell}(\mathcal{O})) \longmapsto \mathfrak{a}\cdot(E,\iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$, where $\mathcal{I}_p(\mathcal{O})$ is the set of invertible ideals of $\mathcal{O}$ of norm prime to p. Since any class of $\mathrm{Cl}(\mathcal{O})$ admits a representative in $\mathcal{I}_p(\mathcal{O})$, it remains to prove that principal ideals fix $\rho(\mathrm{Ell}(\mathcal{O}))$.

Let $\alpha \in \mathcal{O}$ and $(E,\iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$. Then $E[\alpha\mathcal{O}] = \ker(\iota(\alpha))$, so $E/E[\alpha\mathcal{O}] \simeq E$ because $\iota(\alpha) \in \mathrm{End}(E)$. Furthermore:

$$\forall\beta \in K, \quad \iota(\alpha)_*(\iota)(\beta) = \frac{1}{\deg(\iota(\alpha))}\iota(\alpha)\iota(\beta)\widehat{\iota(\alpha)} = \frac{1}{N_{K/\mathbb{Q}}(\alpha)}\iota(\alpha)\iota(\beta)\iota(\overline{\alpha}) = \frac{1}{N_{K/\mathbb{Q}}(\alpha)}\iota(\alpha\overline{\alpha}\beta) = \iota(\beta),$$

so that $\alpha\mathcal{O}\cdot(E,\iota) \simeq (E,\iota)$. Hence the map reduces to $\mathrm{Cl}(\mathcal{O})$.

Let $\mathfrak{a}, \mathfrak{b}$ be invertible ideals of $\mathcal{O}$ of norm prime to p and $(E,\iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$. Then we have $\ker(\varphi_{\mathfrak{b}}\circ\varphi_{\mathfrak{a}}) = E[\mathfrak{b}\mathfrak{a}]$ by point (i) of Proposition 1.15, so that $\varphi_{\mathfrak{b}}\circ\varphi_{\mathfrak{a}} = \varphi_{\mathfrak{b}\mathfrak{a}}$ and $\varphi_{\mathfrak{b}*}(\varphi_{\mathfrak{a}*}(\iota)) = (\varphi_{\mathfrak{b}}\circ\varphi_{\mathfrak{a}})_*(\iota)$. It follows that:

$$\mathfrak{b}\cdot(\mathfrak{a}\cdot(E,\iota)) = (\mathfrak{b}\mathfrak{a})\cdot(E,\iota).$$

Hence, $(\mathfrak{a}, (E,\iota)) \in \mathrm{Cl}(\mathcal{O}) \times \rho(\mathrm{Ell}(\mathcal{O})) \longmapsto \mathfrak{a}\cdot(E,\iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$ is a group action.

We now prove that it is faithful. Let $\mathfrak{a}$ be an invertible ideal of $\mathcal{O}$ of norm prime to p and $(E,\iota) \in \rho(\mathrm{Ell}(\mathcal{O}))$ such that $\mathfrak{a}\cdot(E,\iota) = (E,\iota)$. Then $\varphi_{\mathfrak{a}} \in \mathrm{End}(E)$ and $\varphi_{\mathfrak{a}*}(\iota) = \iota$. It follows that:

$$\forall\alpha \in K, \quad \varphi_{\mathfrak{a}}\circ\iota(\alpha) = \iota(\alpha)\circ\varphi_{\mathfrak{a}} \quad (\star).$$

We claim that $\varphi_{\mathfrak{a}} \in \iota(K) \cap \mathrm{End}(E) = \iota(\mathcal{O})$. Let us suppose the contrary by contradiction. Let K' be the field generated by $\iota(K)$ and $\varphi_{\mathfrak{a}}$. Then $K \subsetneq K'$ and $[K' : \mathbb{Q}] = [K' : K][K : \mathbb{Q}] \geq 4$ so $K' = \mathrm{End}^0(E)$ since $\mathrm{End}^0(E)$ has dimension at most 4 by [15, Corollary III.7.5]. Then, K' is a quaternion algebra by [15, Theorem V.3.1] so is non-commutative, contradicting $(\star)$. Hence, there exists $\alpha \in \mathcal{O}$ such that $\varphi_{\mathfrak{a}} = \iota(\alpha)$. It follows that $\ker(\iota(\alpha)) = E[\mathfrak{a}] = \bigcap_{\beta \in \mathfrak{a}} \ker(\iota(\beta))$ and consequently, that all $\iota(\beta)$ for $\beta \in \mathfrak{a}$ factor through $\iota(\alpha)$ *i.e.* that $\beta/\alpha \in \mathcal{O}$. Hence $\mathfrak{a} \subseteq \alpha\mathcal{O}$. Furthermore, point (ii) of Proposition 1.15 and [19, Lemma 7.14.(i)] ensure that:

$$N(\mathfrak{a}) = \deg(\varphi_{\mathfrak{a}}) = \deg(\iota(\alpha)) = N(\alpha) = N(\alpha\mathcal{O}),$$

so that $\mathfrak{a} = \alpha\mathcal{O}$, which achieves the proof of the faithfulness.

Finally, we obtain the transitiveness by a cardinality argument: by faithfulness, every orbit has cardinality $|\mathrm{Cl}(\mathcal{O})|$ but we know by [16, Proposition II.1.2.(b)] that $|\mathrm{Cl}(\mathcal{O})| = |\mathrm{Ell}(\mathcal{O})| \geq |\rho(\mathrm{Ell}(\mathcal{O}))|$. □

Remark 1.19. By the last cardinality argument, we also obtain that the reduction map ρ is injective.

1.4 Oriented supersingular isogeny graphs

1.4.1 Volcano structure of oriented supersingular isogeny graphs

We fix a quadratic imaginary number field K, and a prime number such that p does not split in K. We want to study isogeny graphs of K-oriented supersingular elliptic curves.

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 reduction maps $\rho_{\mathcal{O}} : \mathrm{Ell}(\mathcal{O}) \longrightarrow \mathrm{SS}^{pr}_{\mathcal{O}}(p)$ for all orders $\mathcal{O}$ of K with conductor prime to p that we defined in Paragraph 1.2.2.

Definition 1.20. We say that two K-oriented isogenies $\varphi : (E, \iota_E) \longrightarrow (F, \iota_F)$ and $\varphi : (E', \iota_{E'}) \longrightarrow (F', \iota_{F'})$ are *K-equivalent* if there exists two K-oriented isomorphisms $\lambda : (E, \iota_E) \xrightarrow{\sim} (E', \iota_{E'})$ and $\lambda' : (F, \iota_F) \xrightarrow{\sim} (F', \iota_{F'})$ such that $\varphi' = \lambda' \circ \varphi \circ \lambda^{-1}$.

Definition 1.21. 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.

Considering dual isogenies, we see that this graph is undirected. Note that two vertices of this graph may have the same j-invatiant but not the same K-orientation up to K-isomorphism, that is why they are distinct in $G_\ell(K, p)$ (see Figures 1.1 and 1.2). Hence, $G_\ell(K, p)$ is very different from the supersingular ℓ-isogeny graph over $\mathbb{F}_{p^2}$. In particular, unlike the latter whose cardinality is close to $p/12$ (by [15, Theorem V.4.1.(c)]), $G_\ell(K, p)$ is infinite (since K has infinitely many orders of conductor prime to p). However, we have the following result:

Proposition 1.22. *Let $G_\ell(K)$ be the graph whose vertices are elliptic curves with complex multiplication by an order of K with conductor prime to p, defined over $\mathbb{C}$ up to isomorphism and whose edges are ℓ-isogenies up to composition by isomorphisms. Then ρ induces a graph isomorphism between $G_\ell(K)$ and $G_\ell(K, p)$ and $G_\ell(K, p)$ is stable by ℓ-isogenies.*

Proof. By the definition of $G_\ell(K, p)$ and by the injectivity of ρ, we have a bijection between the set of vertices. Since the reduction map preserves the degree (along with the trace as a ring homomorphism), any ℓ-isogeny between two vertices of $G_\ell(K)$ reduces to an ℓ-isogeny between two vertices of $G_\ell(K, p)$.

Conversely, if (E,ι) is a vertex of $G_\ell(K,p)$ and if $\varphi:(E,\iota)\longrightarrow(E',\iota')$ is a K-oriented ℓ-isogeny, one can lift E, E' and φ by lifting the kernel as we did in the proof of Theorem 1.18. It follows that (E',ι') is in the image of ρ, so that $(E',\iota')\in G_\ell(K,p)$. This completes the proof. □

It follows from the previous result that every connected component of $G_\ell(K,p)$ is an isogeny volcano, as Kohel proved [22, Proposition 23]. We recall the result and its proof here.

Proposition 1.23. *Let $(E,\iota)\in G_\ell(K,p)$ be a supersingular primitively $\mathcal{O}$-oriented elliptic curve and $\Delta_K:=\mathrm{disc}(K)$. Then:*

(i) *If $\ell\nmid[\mathcal{O}_K:\mathcal{O}]$, there are $1+\left(\frac{\Delta_K}{\ell}\right)$ horizontal, $1/[\mathcal{O}^\times:(\mathbb{Z}+\ell\mathcal{O})^\times]\left(\ell-\left(\frac{\Delta_K}{\ell}\right)\right)$ descending and no ascending ℓ-isogenies with origin (E,ι) up to K-isomorphism.*

(ii) *If $\ell|[\mathcal{O}_K:\mathcal{O}]$, then there are no horizontal, ℓ descending and one ascending ℓ-isogenies up to K-isomorphism.*

Here, $\left(\frac{\cdot}{\ell}\right)$ denotes the Kronecker symbol, given for $\ell\neq 2$ by:

$$\forall a\in\mathbb{Z},\quad \left(\frac{a}{\ell}\right):=\begin{cases}0 & \text{if } a\equiv 0 \mod \ell\\ 1 & \text{if } a \mod \ell \text{ is a square in } \mathbb{F}_\ell^*\\ -1 & \text{otherwise}\end{cases}$$

and for $\ell=2$ by:

$$\forall a\in\mathbb{Z},\quad \left(\frac{a}{\ell}\right):=\begin{cases}0 & \text{if } a\equiv 0 \mod 2\\ 1 & \text{if } a\equiv\pm 1 \mod 8\\ -1 & \text{if } a\equiv\pm 3 \mod 8.\end{cases}$$

Proof. By Proposition 1.22, we can work over $\mathbb{C}$ to prove this classical result. The proof follows [23, Theorem 23.5], as it is more elementary than Kohel's proof.

First we notice that all ℓ-isogenies with given domain E are determined by their kernel (by [15, Corollary III.4.11]) which is a cyclic subgroup of order ℓ in $E[\ell]$. Considering the action of $(\mathbb{Z}/\ell\mathbb{Z})^*$ on the set of non-zero elements of $E[\ell]\simeq(\mathbb{Z}/\ell\mathbb{Z})^2$ by scalar multiplication, whose orbits are exactly the cyclic subgroups of order ℓ in $E[\ell]$ (deprived from the neutral element), we obtain that there are:

$$\frac{\ell^2-1}{\ell-1}=\ell+1$$

such subgroups. Hence, there are $\ell+1$ isogenies of degree ℓ up to isomorphic choices of the codomain.

We first assume that E is the complex torus $\mathbb{C}/\Lambda$ with Λ homothetic to $\mathcal{O}$. To simplify, we set $\Lambda:=\ell\mathcal{O}$. Let $\varphi:E\longrightarrow E'$ be an ℓ-isogeny. Let Λ' be the lattice associated to E'. Then, up to homotety we can assume that $\Lambda\subseteq\Lambda'$ and that φ is induced by this inclusion. Then, $\Lambda=\ell\mathcal{O}$ has index ℓ in Λ', so that $\ell\Lambda'\subseteq\Lambda=\ell\mathcal{O}$ *i.e.* $\Lambda'\subseteq\mathcal{O}$ and we have:

$$[\mathcal{O}:\Lambda']=\frac{[\mathcal{O}:\Lambda']}{[\Lambda':\Lambda]}=\frac{\ell^2}{\ell}=\ell.$$

Let $\tau\in\overline{\mathbb{Q}}$ be a generator of $\mathcal{O}$. Then $\mathcal{O}$ is the lattice $[1,\tau]$ and Λ' is one of the sublattices of index ℓ, $\Lambda_i:=[\ell,\tau+i]$ for $i\in[\![0\ ;\ \ell-1]\!]$ or $\Lambda_\ell:=[1,\ell\tau]$ according to the following lemma.

Lemma 1.24. *A sublattice of index ℓ of $[1,\tau]$ is of the form $[\ell,\tau+i]$ for $i\in[\![0\ ;\ \ell-1]\!]$ or $[1,\ell\tau]$.*

Proof. Let us write $L:=[1,\tau]$ and let $L'\subseteq L$ be a sublattice of index ℓ. Then L' has rank 2 and we have $L':=[a+b\tau,c+d\tau]$ with $a,b,c,d\in\mathbb{Z}$. Let $\delta:=\gcd(a,c)$ and $\delta':=\gcd(b,d)$. Since L' has index ℓ, we have $\ell,\ell\tau\in L'$, so $\delta|\ell$ and $\delta'|\ell$. However, both cannot equal ℓ, otherwise we would have $L'\subseteq\ell L$ and ℓL has index ℓ^2, so either δ or δ' equals 1.

Suppose $\delta' = \ell$. Then, $\delta = 1$ so there exists $u, v \in \mathbb{Z}$ such that $ua + vc = 1$, so that $1 + (ub + vd)\tau = u(a + b\tau) + v(c + d\tau) \in L'$ and $\ell | ub + vd$ so $1 \in L'$ because $\ell\tau \in L'$. Hence, $[1, \ell\tau] \subseteq L'$ and this inclusion is an equality because $[1, \ell\tau]$ has index ℓ in L.

Suppose $\delta' = 1$. Then, there exists $u, v \in \mathbb{Z}$ such that $ub + vd = 1$, and $(ua + vc) + \tau = u(a + b\tau) + v(c + d\tau) \in L'$. Adding or subtracting ℓ as many times as necessary, we obtain that $\tau + i \in L'$ with $i \in [\![0\ ;\ \ell - 1]\!]$, so $[\ell, \tau + i] \subseteq L'$ and this inclusion is an equality because $[\ell, \tau + i]$ has index ℓ in L. □

Let $\mathcal{O}' := \mathrm{End}(E)$. By the theory of complex multiplication, we have:

$$\mathcal{O}' = \{\alpha \in \mathbb{C} \mid \alpha\Lambda' \subseteq \Lambda'\}.$$

Hence $\mathcal{O}' = \mathcal{O}$ if and only if Λ' is a proper ideal of $\mathcal{O}$ of norm ℓ. If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, there are $1 + \left(\frac{\Delta_K}{\ell}\right)$ such ideals, corresponding to horizontal isogenies and otherwise there is no such ideal (hence no horizontal isogeny), by the following lemma.

Lemma 1.25. *If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, there are $1 + \left(\frac{\Delta_K}{\ell}\right)$ proper ideals of norm ℓ in $\mathcal{O}$. Otherwise, all ideals of norm ℓ are not proper.*

Proof. Let $\mathfrak{l}$ be an ideal of norm ℓ. Then $\mathfrak{l}$ is proper by, [19, Lemma 7.18.(ii)] if and only if $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$. Furthermore, $\mathfrak{l}\bar{\mathfrak{l}} = \ell\mathcal{O}$ by [19, Lemma 7.14.(iii)], so that $\ell \in \mathfrak{l}$ and $\mathfrak{l}\mathcal{O}_K\bar{\mathfrak{l}}\mathcal{O}_K = \ell\mathcal{O}_K$ and $N(\mathfrak{l}\mathcal{O}_K)N(\bar{\mathfrak{l}}\mathcal{O}_K) = N(\ell\mathcal{O}_K) = \ell^2$ by [19, Lemma 7.14.(ii)]. Hence $N(\mathfrak{l}\mathcal{O}_K) = \ell$ because the norm of an ideal is invariant under complex conjugation. Moreover, $\mathfrak{l}\mathcal{O}_K \cap \mathcal{O} \supseteq \mathfrak{l}$ and we have an equality because the injection $\mathcal{O}/\mathfrak{l}\mathcal{O}_K \cap \mathcal{O} \hookrightarrow \mathcal{O}_K/\mathfrak{l}\mathcal{O}_K$ ensures that $N(\mathfrak{l}\mathcal{O}_K \cap \mathcal{O})|N(\mathfrak{l}\mathcal{O}_K) = \ell$. Hence, the maps $\mathfrak{l} \longmapsto \mathfrak{l}\mathcal{O}_K$ and $\ell' \longmapsto \ell' \cap \mathcal{O}$ are reciprocal bijections between the sets of ideals of norm ℓ in $\mathcal{O}$ and $\mathcal{O}_K$.

Hence, we can assume that $\mathcal{O} = \mathcal{O}_K$. Let $\alpha \in \mathbb{C}$ such that $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and let $\Pi := X^2 - tX + n \in \mathbb{Z}[X]$ the minimal polynomial of α. Then, by [18, Proposition I.25] the ideals containing ℓ are of the form $\mathfrak{l}_Q := \ell\mathcal{O}_K + Q(\alpha)\mathcal{O}_K$ where $Q \in \mathbb{Z}[X]$ is such that the reduction of Q modulo ℓ is a factor of Π in $\mathbb{F}_\ell[X]$. $\mathfrak{l}_Q$ has norm ℓ if and only if Q is a factor of degree 1.

If $\ell \neq 2$, such a factor exists if and only if $\Delta_K = t^2 - 4n$ is a square in $\mathbb{F}_\ell$. Hence, there are no ideal of norm ℓ if $\left(\frac{\Delta_K}{\ell}\right) = -1$, one such ideal if $\left(\frac{\Delta_K}{\ell}\right) = 0$ *i.e.* $\Delta_K \equiv 0\ [\ell]$ and two such ideals if $\left(\frac{\Delta_K}{\ell}\right) = 1$.

Suppose now that $\ell = 2$. Then $\Delta_K \equiv 0, 1\ [4]$. If $\Delta_K \equiv 0\ [4]$, then t is even so $\Pi \equiv X^2\ [2]$ or $\Pi \equiv X^2 + 1 = (X + 1)^2\ [2]$ and Π has one factor of degree 1, so there is $1 = 1 + \left(\frac{\Delta_K}{2}\right)$ ideal of norm 2. If $\Delta_K \equiv 1\ [4]$, then t is odd so $t \equiv \pm 1\ [4]$ and $t^2 \equiv 1\ [8]$. Hence, $4n \equiv 1 - \Delta_K\ [8]$, so n is even when $\Delta_K \equiv 1\ [8]$ and $\Pi \equiv X^2 + X \equiv X(X + 1)\ [2]$ has two factors of degree 1, so there are $2 = 1 + \left(\frac{\Delta_K}{2}\right)$ ideal of norm 2. On the contrary, n is odd when $\Delta_K \equiv 5\ [8]$ and $\Pi \equiv X^2 + X + 1\ [2]$ has no factor of degree 1, so there is $0 = 1 + \left(\frac{\Delta_K}{2}\right)$ ideal of norm 2. □

If $\ell \nmid [\mathcal{O}_K : \mathcal{O}]$, then we cannot have $\mathcal{O} \subseteq \mathcal{O}'$ and $\ell | [\mathcal{O}' : \mathcal{O}]$ so there is no ascending isogeny by Proposition 1.5. Hence, we have $\ell - \left(\frac{\Delta_K}{\ell}\right)$ descending isogenies.

Now, we assume that $\ell | [\mathcal{O}_K : \mathcal{O}]$. Then, there exists an order $\mathcal{O}'' \subseteq \mathcal{O}_K$ containing $\mathcal{O}$ with index ℓ. Hence, we have $\mathcal{O}'' = \mathbb{Z}[\alpha]$ with $\ell\alpha = \tau$. Since α is an algebraic integer, we have $\alpha^2 - t\alpha + n = 0$, with $t := \mathrm{Tr}_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ and $n := N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$. Since φ cannot be horizontal the Proposition 1.5 ensures that $\varphi : E \longrightarrow E'$ is ascending if and only if $\mathcal{O}' = \mathcal{O}''$ and that otherwise, φ is descending and $\mathcal{O}' \subsetneq \mathcal{O} \subsetneq \mathcal{O}''$. We have $\alpha\ell = \tau \in \Lambda_0 = [\ell, \tau]$ and $\alpha\tau = \ell\alpha^2 = \ell(t\alpha - n) = t\tau - \ell n \in \Lambda_0$ so $\mathcal{O}''$ fixes Λ_0, so that $\mathcal{O}' \supset \mathcal{O}''$ so Λ_0 corresponds to an ascending isogeny. For all $i \in [\![1\ ;\ \ell - 1]\!]$, we have $\alpha(\tau + i) = \ell\alpha^2 + \alpha i = \ell(t\alpha - n) + \alpha i = t\tau - \ell n + \alpha i \notin \mathcal{O}$ because $\alpha i \notin \mathcal{O}$ and but $\Lambda_i = [\ell, \tau + i] \subseteq \mathcal{O}$ so Λ_i is not stable by multiplication by $\mathcal{O}''$. Eventually, $\alpha \notin \mathcal{O} \supseteq \Lambda_\ell = [1, \ell\tau]$ so Λ_ℓ is not stable by multiplication by $\mathcal{O}''$. Whence there are ℓ descending isogenies and only one ascending isogeny.

Now we treat the general case: Λ is no longer homothetic to $\mathcal{O}$ but we can reduce to this case. Since the action of $\mathrm{Cl}(\mathcal{O})$ on $\mathrm{Ell}(\mathcal{O})$ and maps $E = \mathbb{C}/\Lambda$ and an ideal $\mathfrak{a}$ of $\mathcal{O}$ to $\mathbb{C}/\mathfrak{a}^{-1}\Lambda$ and since $\mathbb{C}/\mathcal{O} \in \mathrm{Ell}(\mathcal{O})$, we can assume that Λ is an ideal $\mathfrak{a}$ of $\mathcal{O}$. Multiplying $\mathfrak{a}$ by a principal ideal does not change the isomorphism

class of E and, furthermore, every ideal class in $\mathrm{Cl}(\mathcal{O})$ contains infinitely many ideals of prime norm by [19, Theorems 7.7. (iii) and 9.12] so we may assume that $q := N(\mathfrak{a})$ is a prime number $\neq \ell$. We consider the isogeny $\varphi_{\mathfrak{a}} : E = \mathbb{C}/\mathfrak{a} \longrightarrow E_0 := \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{a} = \mathbb{C}/\mathcal{O}$ whose kernel is $E[\mathfrak{a}]$. We saw that $\mathfrak{b} \longmapsto \mathfrak{b}\mathcal{O}'$ and $\mathfrak{b} \longmapsto \mathfrak{b} \cap \mathcal{O}'$ are bijections between ideals of norm q of $\mathcal{O}$ and $\mathcal{O}'$, respectively when $\mathcal{O} \subseteq \mathcal{O}'$ and $\mathcal{O} \supseteq \mathcal{O}'$. Then, we can associate an ideal $\mathfrak{a}'$ of norm q in $\mathcal{O}'$ to $\mathfrak{a}$. Consider the isogeny $\varphi_{\mathfrak{a}'} : E' \longrightarrow E'_0$ such that $\ker(\varphi_{\mathfrak{a}'}) = E'[\mathfrak{a}']$. We claim that the isogeny $\varphi_0 : E_0 \longrightarrow E'_0$ such that $\ker(\varphi_0) = \varphi_{\mathfrak{a}}(\ker(\varphi_{\mathfrak{a}'} \circ \varphi))$ makes the diagram commute :

$$\begin{array}{ccc} E & \xrightarrow{\varphi_{\mathfrak{a}}} & E_0 \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \varphi_0} \\ E' & \xrightarrow{\varphi_{\mathfrak{a}'}} & E'_0 \end{array} .$$

By [15, Corollary III.4.11], it suffices to prove that $\ker(\varphi_{\mathfrak{a}'} \circ \varphi) = \ker(\varphi_0 \circ \varphi_{\mathfrak{a}})$. We clearly have $\ker(\varphi_{\mathfrak{a}'} \circ \varphi) \subseteq \ker(\varphi_0 \circ \varphi_{\mathfrak{a}})$ and we conclude because both $\varphi_{\mathfrak{a}'} \circ \varphi$ and $\varphi_0 \circ \varphi_{\mathfrak{a}}$ have degree ℓq. $\varphi_{\mathfrak{a}}$ and $\varphi_{\mathfrak{a}'}$ are horizontal so φ is ascending, horizontal or descending if and only if φ_0 is too. Since $E_0 \simeq \mathbb{C}/\mathcal{O}$, we conclude by the case we treated above.

To conclude, it remains to identify descending ℓ-isogenies with the same domains and codomains. This will explain the factor $[\mathcal{O}^\times : \mathcal{O}'^\times]$ in case (i) ($\ell \nmid [\mathcal{O}_K : \mathcal{O}]$).In case (ii) ($\ell | [\mathcal{O}_K : \mathcal{O}]$), this factor will not appear because we will have $\mathcal{O}^\times = \mathcal{O}'^\times = \{\pm 1\}$ since the only orders with non-trivial unit group are maximal in $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$ by [19, Exercise 5.9].

Let $\varphi, \psi : E \longrightarrow E'$ be two descending ℓ-isogenies. Then φ and ψ are represented by the complex multiplication by α and $\beta \in K$ respectively. By [15, exercise 6.10.(b)], the endomorphisms $\psi \circ \widehat{\varphi}$ and $\varphi \circ \widehat{\psi} \in \mathrm{End}(E')$ are represented by $\ell\beta\alpha^{-1}$ and $\ell\alpha\beta^{-1} \in \mathcal{O}' = [1, \ell\tau]$ respectively. Let us write $\ell\beta\alpha^{-1} = a + b\ell\tau$, $\ell\alpha\beta^{-1} = c + d\ell\tau$, with $a, b, c, d \in \mathbb{Z}$, $\tau^2 - t\tau + n = 0$, with $t := \mathrm{Tr}_{K/\mathbb{Q}}(\tau) \in \mathbb{Z}$ and $n := N_{K/\mathbb{Q}}(\tau) \in \mathbb{Z}$. Then, we have:

$$\ell^2 = \ell\beta\alpha^{-1}\ell\alpha\beta^{-1} = (a + b\ell\tau)(c + d\ell\tau) = ac + \ell(bc + ad)\tau + \ell^2 bd\tau^2 = ac + tbd\ell^2 + \ell(bc + ad - \ell nbd)\tau.$$

It follows that $\ell^2 | ac$. If $\ell \nmid c$, then $\ell^2 | a$ and $bc + ad - \ell nbd = 0$ so $\ell^2 | b$ so $\ell^2 | \ell\beta\alpha^{-1}$ *i.e.* $\psi \circ \widehat{\varphi}$ factors through $[\ell^2]$, which is impossible because $\deg(\psi \circ \widehat{\varphi}) = \ell^2$ and $\deg([\ell^2]) = \ell^4$. Hence $\ell | c$. For the same reason, $\ell | a$. Hence, $\beta\alpha^{-1} \in \mathcal{O}$ and $\alpha\beta^{-1} \in \mathcal{O}$ so that $\alpha\beta^{-1} \in \mathcal{O}^\times$. φ and ψ are already considered up to multiplication by an element of $\mathrm{Aut}(E')$. But $\mathrm{Aut}(E')$ corresponds to $\mathcal{O}'^\times$ by complex multiplication. Hence, there are $[\mathcal{O}^\times : \mathcal{O}'^\times]$ descending ℓ-isogenies $E \longrightarrow E'$. □

Remark 1.26. In the course of this proof, we obtained that every horizontal ℓ-isogeny comes from a proper prime ideal of norm ℓ.

1.4.2 Graph refolding and the forgetful map

Forgetting the K-orientation, one can always consider supersingular ℓ-isogeny graphs whose set of vertices is $\mathrm{SS}(p)$, the set of isogeny classes of supersingular elliptic curves. We have a natural map $\mathrm{Ell}(K) \longrightarrow \mathrm{SS}(p)$, called the *forgetful map*. This map cannot be injective since $\mathrm{Ell}(K)$ is infinite (because K has infinitely many orders of conductor prime to p) and $\mathrm{SS}(p)$ is finite of cardinality close to $\frac{p}{12}$ (by [15, Theorem V.4.1.(c)]). As a consequence, K-oriented supersingular isogeny graphs refold when we forget the orientation (see Figures 1.1 and 1.2).

However, the cryptographic constructions of OSIDH use j-invariants alone so the $\mathcal{O}$-orientations we consider on a given elliptic curves might be ambiguous. That is why we look for partial injectivity results of the forgetful map. Indeed, we can always restrict the set of vertices to the finite subset:

$$\mathrm{SS}_{\mathcal{O}}(p) \cap \mathrm{im}(\rho) = \bigcup_{\mathcal{O} \subseteq \mathcal{O}'} \rho(\mathrm{Ell}(\mathcal{O}'))$$

formed of (not necessarily primitively) $\mathcal{O}$-oriented supersingular elliptic curves obtained by the reduction map ρ.

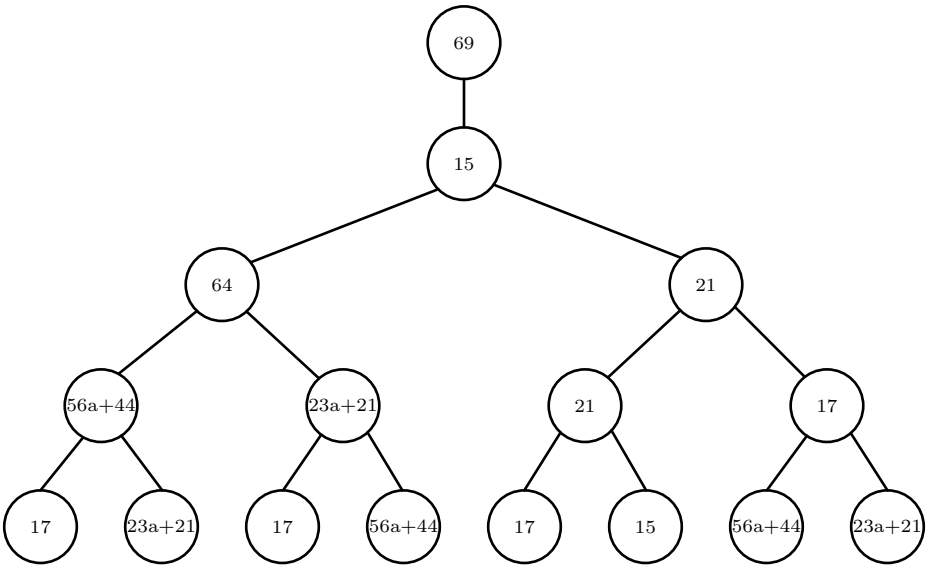

Figure 1.1: Representation of a connected component (with volcano structure) of $G_2(\mathbb{Q}(i), 79)$, the $\mathbb{Q}(i)$-oriented supersingular 2-isogeny graph over $\mathbb{F}_{79^2}$ up to depth 4. Here, a is the generator of $\mathbb{F}_{79^2}/\mathbb{F}_{79}$ and satisfies $a^2 - a + 3 = 0$.

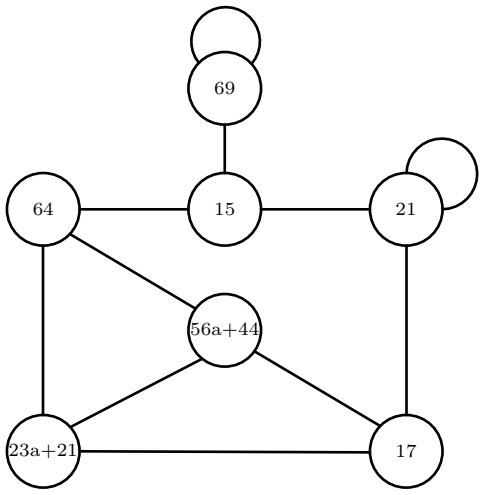

Figure 1.2: Supersingular 2-isogeny graph over $\mathbb{F}_{79^2}$.

Theorem 1.27. *Let $\Delta := \mathrm{disc}(\mathcal{O})$. If $|\Delta| < p$, then the map $\mathrm{SS}_{\mathcal{O}}(p) \cap \mathrm{im}(\rho) \longrightarrow \mathrm{SS}(p)$ is injective.*

Actually, this theorem is a direct consequence of the following proposition:

Proposition 1.28. *Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve admitting two distinct K-orientations $(E, \iota_1), (E, \iota_2) \in \mathrm{im}(\rho)$. Let $\mathcal{O}_1 := \iota_1^{-1}(\mathrm{End}(E))$ and $\mathcal{O}_2 := \iota_2^{-1}(\mathrm{End}(E))$ and $\Delta_i := \mathrm{disc}(\mathcal{O}_i)$ for all $i \in \{1, 2\}$. Then $\Delta_1 \Delta_2 \geq p^2$.*

Proof. This proof uses quaternion arithmetic (especially in case 2). We refer to [24] and Appendix A.3 for the prerequisites.

Case 1: Suppose that $\iota_1(\mathcal{O}_1) = \iota_2(\mathcal{O}_2)$. Then, $\iota_2^{-1} \circ \iota_1$ is a field automorphism of K inducing an isomorphism $\mathcal{O}_1 \xrightarrow{\sim} \mathcal{O}_2$. Hence $\mathcal{O}_1 = \mathcal{O}_2$ and we either have $\iota_2(\alpha) = \iota_1(\alpha)$ or $\iota_2(\alpha) = \iota_1(\overline{\alpha})$ for all $\alpha \in K$. Since ι_1 and ι_2 are distinct, the latter equation holds. Considering Galois action like in the proof of Proposition 1.13, we get that $(E, \iota_2) = (E^{(p)}, \iota_1^{(p)})$. In particular, $E = E^{(p)}$. Then, we have $(E, \iota_1), (E, \iota_1^{(p)}) \in \rho(\mathrm{Ell}(\mathcal{O}))$, where $\mathcal{O} := \mathcal{O}_1 = \mathcal{O}_2$. Since the action of $\mathrm{Cl}(\mathcal{O})$ on $\rho(\mathrm{Ell}(\mathcal{O}))$ is transitive by Theorem 1.18, there exists an invertible ideal $\mathfrak{a} \subseteq \mathcal{O}$ of norm prime to p such that $\mathfrak{a} \cdot (E, \iota_1) = (E, \iota_1^{(p)})$. Let $\varphi := \varphi_{\mathfrak{a}}$ and ϕ_p the p-th power Frobenius endomorphism. Then $\iota_2 = \phi_{p*}(\iota_1) = \varphi_*(\iota_1)$. It follows that:

$$\forall \alpha \in K, \quad \frac{1}{p}\phi_p \iota(\alpha) \widehat{\phi_p} = \frac{1}{d}\varphi \iota(\alpha) \widehat{\varphi},$$

with $d := \deg(\varphi)$. Multiplying by $\widehat{\varphi}$ on the left and by ϕ_p on the left, we get that $\widehat{\varphi} \circ \phi_p$ commutes with $\iota(K)$, so the exists $\alpha \in \mathcal{O}$ such that $\widehat{\varphi} \circ \phi_p = \iota(\alpha)$ (otherwise, $\iota(K)$ and $\widehat{\varphi} \circ \phi_p$ would generate the quaternion algebra $\mathrm{End}^0(E)$, which would be commutative). Hence, $N(\alpha) = \deg(\widehat{\varphi} \circ \phi_p) = dp$, so $p | N(\alpha) = \alpha\overline{\alpha}$. Hence, if p is inert, then $p\mathcal{O}$ is prime so $\alpha \in p\mathcal{O}$ or $\overline{\alpha} \in \mathcal{O}$. Either way $\alpha \in p\mathcal{O}$, so $p^2 | N(\alpha)$ and $p | d$. But $d = N(\mathfrak{a})$ by point (ii) of Proposition 1.15 and $N(\mathfrak{a})$ is prime to p. Contradiction. Since p does not split in K, p ramifies so we have $\left(\frac{\Delta_K}{p}\right) = 0$ *i.e.* $p | \Delta_K | \Delta$ by Lemma 1.25. Hence, $|\Delta| \geq p$, so $\Delta_1\Delta_2 = \Delta^2 \geq p^2$.

Case 2: Suppose that $\iota_1(\mathcal{O}_1) \neq \iota_2(\mathcal{O}_2)$. Then, $\iota_1(\mathcal{O}_1)$ and $\iota_2(\mathcal{O}_2)$ do not commute (the commutativity implies the equality, by arguments we already gave). Let α_i be the image by ι_i of a generator of $\mathcal{O}_i$ for all $i \in \{1, 2\}$. Then, the commutator $\beta := [\alpha_1, \alpha_2] = \alpha_1\alpha_2 - \alpha_2\alpha_1$ is not zero. By computation, we get the following expression for the reduced norm of β:

$$\mathrm{nrd}(\beta) = \frac{\Delta_1\Delta_2 - T^2}{4} \quad (\star),$$

with $T := 2\,\mathrm{Tr}(\alpha_1\alpha_2) - \mathrm{Tr}(\alpha_1)\,\mathrm{Tr}(\alpha_2)$. By [24, Theorem 42.1.19], $\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a quaternion algebra that ramifies at p and ∞ and $\mathrm{End}(E)$ is a maximal order in $\mathrm{End}^0(E)$. Since $\mathrm{End}^0(E)$ ramifies at p, $B_p := \mathrm{End}^0(E) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is the unique division quaternion algebra over $\mathbb{Q}_p$, so we have an embedding $\mathrm{End}^0(E) \hookrightarrow B_p$ mapping $\mathrm{End}(E)$ to the valuation ring O_p of B_p formed of elements with non-negative p-adic valuation. Furthermore, there is a unique maximal two sided ideal $P_p \subseteq O_p$ (see [24, Theorem 13.3.11]). P_p is formed of elements of positive p-adic valuation:

$$P_p = \{\alpha \in O_p \mid v_p(\mathrm{nrd}(\alpha)) > 0\} = \{\alpha \in O_p \mid \mathrm{nrd}(\alpha) \equiv 0\ [p]\}.$$

By [24, Theorem 13.3.11.(b)] again, the quotient O_p/P_p is the finite field $\mathbb{F}_{p^2}$ so it is commutative. It follows that $\beta = [\alpha_1, \alpha_2] \in P_p$, so that $\mathrm{nrd}(\beta) \equiv 0\ [p]$.

By $(\star)$, it follows that $\sqrt{\Delta_1\Delta_2} + |T| \equiv 0\ [2p]$ or $\sqrt{\Delta_1\Delta_2} - |T| \equiv 0\ [2p]$ ($\sqrt{\Delta_1\Delta_2} \in \mathbb{Z}$ since $\mathcal{O}_1, \mathcal{O}_2 \subseteq K$). Moreover, $\mathrm{End}^0(E)$ ramifies at ∞ so the norm is a positive definite function by [24, Exercise 2.4] and we have $N(\beta) > 0$ since $\beta \neq 0$. It follows that $\sqrt{\Delta_1\Delta_2} > |T|$, so that $2p \leq \sqrt{\Delta_1\Delta_2} + |T| \leq 2\sqrt{\Delta_1\Delta_2}$ *i.e.* $\Delta_1\Delta_2 \geq p^2$. □

1.5 Isogeny chains and ladders

1.5.1 Definition

We now introduce the basic algorithmic foundations of the OSIDH protocol.

Definition 1.29. An *ℓ-isogeny chain* of length n is a sequence of ℓ-isogenies:

$$E_0 \xrightarrow{\varphi_0} E_1 \xrightarrow{\varphi_1} \cdots \xrightarrow{\varphi_{n-2}} E_{n-1} \xrightarrow{\varphi_{n-1}} E_n\ .$$

We say that it is K-oriented if all elliptic curves E_i $(0 \leq i \leq n)$ and isogenies $\varphi_i : E_i \longrightarrow E_{i+1}$

$(0 \leq i \leq n-1)$ are *K-oriented*.

A K-oriented ℓ-isogeny chain $(\varphi_i : E_i \longrightarrow E_{i+1})_{0 \leq i \leq n-1}$ is *descending*, *horizontal* or *ascending* if all the φ_i are respectively descending, horizontal or ascending.

In the following, we shall only consider K-oriented isogeny chains, so we shall omit to mention that they are K-oriented.

Definition 1.30. An *ℓ-ladder* of length n and degree q is a commutative diagram of ℓ-isogeny chains $(\varphi_i : E_i \longrightarrow E_{i+1})_{0 \leq i \leq n-1}$ and $(\varphi'_i : F_i \longrightarrow F_{i+1})_{0 \leq i \leq n-1}$:

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\varphi_0} & E_1 & \xrightarrow{\varphi_1} & \cdots & \xrightarrow{\varphi_{n-2}} & E_{n-1} & \xrightarrow{\varphi_{n-1}} & E_n \\ \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & & & \downarrow{\scriptstyle \psi_{n-1}} & & \downarrow{\scriptstyle \psi_n} \\ F_0 & \xrightarrow{\varphi'_0} & F_1 & \xrightarrow{\varphi'_1} & \cdots & \xrightarrow{\varphi'_{n-2}} & F_{n-1} & \xrightarrow{\varphi'_{n-1}} & F_n \end{array}$$

such that $\psi_i : E_i \longrightarrow F_i$ is a q-isogeny for all $i \in [\![0 \ ; \ n]\!]$. Such an ℓ-ladder is often denoted by $\psi : (E_i, \varphi_i)_{0 \leq i \leq n-1} \longrightarrow (F_i, \varphi'_i)_{0 \leq i \leq n-1}$ and referred to as a q-isogeny between ℓ-isogeny chains.

An ℓ-ladder $\psi : (E_i, \varphi_i)_{0 \leq i \leq n-1} \longrightarrow (F_i, \varphi'_i)_{0 \leq i \leq n-1}$ is *descending*, *horizontal* or *ascending* if all the φ_i are respectively descending, horizontal or ascending. It is *level* if $\psi_0 : E_0 \longrightarrow F_0$ is horizontal.

Lemma 1.31. *Suppose ℓ and q are distinct prime numbers. Let $\psi : ((E_i, \iota_i), \varphi_i) \longrightarrow ((F_i, \iota'_i), \varphi'_i)$ be an ℓ-lader of length n between K-oriented ℓ-isogeny chains. Then ψ is level if and only if $\iota_i^{-1}(\mathrm{End}(E_i)) = {\iota'}_i^{-1}(\mathrm{End}(F_i))$ for all $i \in [\![0 \ ; \ n]\!]$. In particular, if ψ is level and descending, horizontal or ascending, then the ℓ-isogeny chain $(\varphi'_i : F_i \longrightarrow F_{i+1})_{0 \leq i \leq n-1}$ is respectively descending, horizontal or ascending.*

Proof. Suppose that ψ is level. Then we prove that $\mathcal{O}_i := \iota_i^{-1}(\mathrm{End}(E_i))$ equals $\mathcal{O}'_i := {\iota'}_i^{-1}(\mathrm{End}(F_i))$ by induction on $i \in [\![0 \ ; \ n]\!]$. Since ψ_0 is horizontal, the result follows immediately at $i = 0$.

Now, let $i \in [\![0 \ ; \ n-1]\!]$ and suppose that $\mathcal{O}_i = \mathcal{O}'_i$. Suppose that $\varphi_i : E_i \longrightarrow E_{i+1}$ is descending. Then $\mathcal{O}_{i+1} \subseteq \mathcal{O}_i$ and $[\mathcal{O}_i : \mathcal{O}_{i+1}] = \ell$ by Proposition 1.5, and $\varphi'_i : F_i \longrightarrow F_{i+1}$ must be descending too, otherwise, we would have $\mathcal{O}_{i+1} \subseteq \mathcal{O}_i = \mathcal{O}'_i \subseteq \mathcal{O}'_{i+1}$ and $\ell = [\mathcal{O}_i : \mathcal{O}_{i+1}] | [\mathcal{O}'_{i+1} : \mathcal{O}_{i+1}]$ so ψ_{i+1} is ascending and $[\mathcal{O}'_{i+1} : \mathcal{O}_{i+1}] = q$ by Proposition 1.5. Contradiction because $\ell \nmid q$. Hence φ'_i is descending and $\mathcal{O}_{i+1} = \mathcal{O}'_{i+1}$ since they have the same conductor. We treat the cases where φ_i is horizontal and ascending likewise. Whence the result, ψ beign trivially level when $\mathcal{O}_i = \mathcal{O}'_i$ for all $i \in [\![0 \ ; \ n]\!]$. □

We now introduce a way to obtain a level and descending ℓ-ladder. Let q and ℓ be distinct prime numbers distinct from p. Let $\mathcal{O}_0$ be an order of K whose conductor is prime to ℓ, p and q (for instance $\mathcal{O}_0 = \mathcal{O}_K$). Let $\mathcal{O}_i := \mathbb{Z} + \ell^i \mathcal{O}_0$ for all $i \in [\![0 \ ; \ n]\!]$.

Suppose that q splits in K. Let $\mathfrak{q}$ be a prime ideal of $\mathcal{O}_0$ lying above q. Then $\mathfrak{q}$ is proper and has norm q and so does $\mathfrak{q}^{(i)} := \mathfrak{q} \cap \mathcal{O}_i$ for all $i \in [\![0 \ ; \ n]\!]$ (as we proved in Lemma 1.25).

Let $(\varphi_i : (E_i, \iota_i) \longrightarrow (E_{i+1}, \iota_{i+1}))$ be a descending ℓ-isogeny chain of length n such that E_i is primitively $\mathcal{O}_i$-oriented for all $i \in [\![1 \ ; \ n]\!]$. For all $i \in [\![0 \ ; \ n]\!]$, let:

$$(F_i, \iota'_i) := \mathfrak{q}^{(i)} \cdot (E_i, \iota_i) = (E_i / E_i[\mathfrak{q}^{(i)}], \psi_{i*}(\iota_i)),$$

where $\psi_i := \varphi_{\mathfrak{q}^{(i)}}$. Then, there is an ℓ-isogeny chain $(\varphi'_i : F_i \longrightarrow F_{i+1})$ such that the following diagram commutes:

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\varphi_0} & E_1 & \xrightarrow{\varphi_1} & \cdots & \xrightarrow{\varphi_{n-2}} & E_{n-1} & \xrightarrow{\varphi_{n-1}} & E_n \\ \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & & & \downarrow{\scriptstyle \psi_{n-1}} & & \downarrow{\scriptstyle \psi_n} \\ F_0 & \xrightarrow{\varphi'_0} & F_1 & \xrightarrow{\varphi'_1} & \cdots & \xrightarrow{\varphi'_{n-2}} & F_{n-1} & \xrightarrow{\varphi'_{n-1}} & F_n \end{array}$$

i.e. forms a descending ℓ-ladder. The ℓ-isogeny chain $(\varphi'_i : F_i \longrightarrow F_{i+1})_{0 \leq i \leq n-1}$ at the bottom of the diagram will be denoted by $\mathfrak{q} \cdot ((E_i, \iota_i), \varphi_i)$ or simply $\mathfrak{q} \cdot (E_i, \varphi_i)$. The φ'_i are well-defined by [15, corollary III.4.11] according to the following lemma:

Lemma 1.32. $\ker(\psi_i) \subseteq \ker(\psi_{i+1} \circ \varphi_i)$ *for all* $i \in [\![0\ ;\ n-1]\!]$.

Proof. Let $i \in [\![0\ ;\ n-1]\!]$ and $P \in \ker(\psi_i) = E_i[\mathfrak{q}^{(i)}]$. Then, for all $\alpha \in \mathfrak{q}^{(i)}$, $\iota_i(\alpha)(P) = O$, so $\varphi_i \circ \iota_i(\alpha)(P) = O$. Since:

$$\iota_{i+1} = \varphi_{i*}(\iota_i) = \frac{1}{\ell}\varphi_i \iota_i \widehat{\varphi_i}$$

we get that $\varphi_i \circ \iota_i(\alpha) = \iota_{i+1}(\alpha) \circ \varphi_i$ for all $\alpha \in K$. Since $\mathfrak{q}^{(i+1)} \subseteq \mathfrak{q}^{(i)}$, it follows that $\iota_{i+1}(\alpha) \circ \varphi_i(P) = O$ for all $\alpha \in \mathfrak{q}^{(i+1)}$, so that $\varphi_i(P) \in E_{i+1}[\mathfrak{q}^{(i+1)}] = \ker(\psi_{i+1})$. This completes the proof. □

1.5.2 A practical way to construct descending ℓ-ladders

The last element of this chain $(F_n, \iota'_n) = \mathfrak{q}^{(n)} \cdot (E_n, \iota_n)$ is actually what we want to compute. We start the computation at level $i = 0$ and descend the ladder. If $\mathfrak{q} = \mathfrak{q}^{(0)}$ is principal, then ψ_0 is an endomorphism and the ℓ-ladder is level so the computation of (F_0, ι'_0) is trivial ($(F_0, \iota'_0) = (E_0, \iota_0)$). It is always the case when $\mathrm{Cl}(\mathcal{O}_0)$ is trivial i.e. when $\mathcal{O}_0 = \mathcal{O}_K$ and:

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

by [19, theorem 7.30.(i)]. We shall always assume $\mathrm{Cl}(\mathcal{O}_0) = \mathrm{Cl}(\mathcal{O}_K)$ is trivial in the following.

Now, we explain the descent. First, we assume that $|\mathrm{disc}(\mathcal{O}_n)| < p$, so that all K-oriented elliptic curves of the ladder can be represented as j-invariants by theorem **??** and we can use modular equations. Assume that the ladder is constructed up to level i.We want to compute $j(F_{i+1})$, the ℓ-isogeny such that the following diagram commutes:

$$\begin{array}{ccc} E_i & \xrightarrow{\varphi_i} & E_{i+1} \\ \downarrow{\scriptstyle \psi_i} & & \downarrow{\scriptstyle \psi_{i+1}} \\ F_i & \xrightarrow{\varphi'_i} & F_{i+1} \end{array}$$

where φ'_i is a ℓ-isogeny ψ_{i+1} is a q-isogeny.Then, $j(F_{i+1})$ is a solution of the modular equations:

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

However, *a priori* this equation can admit multiple solutions so we want to make sure that the solution is unique and corresponds to $(F_{i+1}, \iota'_{i+1}) = \mathfrak{q}^{(i+1)} \cdot (E_{i+1}, \iota_i)$. This will be the case under some assumptions.

Proposition 1.33. *Let* $\Delta_K := \mathrm{disc}(K)$. *We assume that:*

(i) $p > q\ell^{2n}|\Delta_K|$.

(ii) $(F_0, \iota'_0) = \mathfrak{q}^{(0)} \cdot (E_0, \iota_0)$ *and* $(F_1, \iota'_1) = \mathfrak{q}^{(1)} \cdot (E_1, \iota_1)$.

(iii) $(\mathfrak{q}^{(1)})^2$ *is not principal in* $\mathcal{O}_1$.

(iv) $j(F_i)$ *is a solution of:*

$$\gcd(\Phi_\ell(j(F_{i-1}), x), \Phi_q(j(E_i), x)) = 0 \quad (\star)_{i-1}$$

for all $i \in [\![1\ ;\ n]\!]$.

Then $(F_i, \iota'_i) = \mathfrak{q}^{(i)} \cdot (E_i, \iota_i)$ *for all* $i \in [\![0\ ;\ n]\!]$.

Proof. We prove by induction on $i \in [\![0\ ;\ n]\!]$ that $(F_i, \iota'_i) = \mathfrak{q}^{(i)} \cdot (E_i, \iota_i)$. We already know that the result holds for $i = 0$ and $i = 1$.

Let $i \in [\![1\ ;\ n-1]\!]$. Let us assume that $(F_i, \iota'_i) = \mathfrak{q}^{(i)} \cdot (E_i, \iota_i)$. Since $j(F_{i+1})$ is solution of $(\star)_i$, there exist an ℓ-isogeny $\varphi'_i : F_i \longrightarrow F_{i+1}$ and a q-isogeny $\psi_{i+1} : E_{i+1} \longrightarrow F_{i+1}$. Since $(F_i, \iota'_i) = \mathfrak{q}^{(i)} \cdot (E_i, \iota_i)$ and $\mathfrak{q}^{(i)}$ is invertible (its norm is q, which is prime to $[\mathcal{O}_K : \mathcal{O}_i] = \ell^i$), ψ_i is an horizontal isogeny by point

(iv) of Proposition 1.15. Hence, we have ${\iota'_i}^{-1}(\mathrm{End}(F_i)) = \mathcal{O}_i$ (with $\iota'_i = \psi_{i*}(\iota_i)$). Since φ'_i has degree ℓ, $\varphi'_{i*}(\iota'_i)^{-1}(\mathrm{End}(F_{i+1}))$ is a suborder of $\mathcal{O}_K$ of index ℓ^{i-1}, ℓ^i or ℓ^{i+1} by Proposition 1.5. Since ψ_{i+1} has degree q, $\psi_{i+1*}(\iota_{i+1})^{-1}(\mathrm{End}(F_{i+1}))$ is a suborder of $\mathcal{O}_K$ of index ℓ^{i+1} or $q\ell^{i+1}$. Hence, if $\varphi'_{i*}(\iota'_i)$ and $\psi_{i+1*}(\iota_{i+1})$ were distinct K-orientation, we would have $q^2\ell^{4i+4}\Delta_0^2 \geq p^2$ by Proposition 1.28,contradicting point (i). Whence, $\varphi'_{i*}(\iota'_i) = \psi_{i+1*}(\iota_{i+1})$ *i.e.* :

$$(\varphi'_i \circ \psi_i)_*(\iota_i) = (\psi_{i+1} \circ \varphi_i)_*(\iota_i).$$

Let $\phi := \varphi'_i \circ \psi_i$ and $\psi := \psi_{i+1} \circ \varphi_i$. Then, $\widehat{\psi} \circ \phi$ commutes with $\iota_i(K)$ (since ψ and ϕ have the same degree) and there exists $\alpha \in \mathcal{O}_i$ such that $\widehat{\psi} \circ \phi = \iota_i(\alpha)$.

We shall prove that $\alpha = q\ell$, so that $\varphi'_i \circ \psi_i = \psi_{i+1} \circ \varphi_i$, whence $\ker(\psi_{i+1}) = \varphi_i(\ker(\varphi'_i \circ \psi_i)) = E_{i+1}[\mathfrak{q}^{(i+1)}]$ and the proof will be complete.

Let $\iota'_{i+1} := \phi_*(\iota_i) = \psi_*(\iota_i)$. Since φ'_i has degree ℓ and ψ_{i+1} has degree $q \neq \ell$, the argument given in the proof of Lemma 1.31 ensures that ψ_{i+1} is horizontal, *i.e.* that ${\iota'_{i+1}}^{-1}(\mathrm{End}(F_{i+1})) = \mathcal{O}_{i+1}$. ψ_{i+1} being horizontal of degree q, Remark 1.26 ensures that ψ_{i+1} is given by an invertible ideal of norm q, that is to say $\mathfrak{q}^{(i)}$ or $\overline{\mathfrak{q}}^{(i)}$, so we either have $\ker(\psi_{i+1}) = E_{i+1}[\mathfrak{q}^{(i+1)}]$ or $\ker(\psi_{i+1}) = E_{i+1}[\overline{\mathfrak{q}}^{(i+1)}]$. We assume that the latter holds.

We have:

$$\iota'_{i+1}(\alpha) = \frac{1}{q\ell}\psi \circ \iota_i(\alpha) \circ \widehat{\psi} = \frac{1}{q\ell}\psi \circ \widehat{\psi} \circ \phi \circ \widehat{\psi} = \phi \circ \widehat{\psi} \in \mathrm{End}(F_{i+1}),$$

so that $\alpha \in \mathcal{O}_{i+1}$. Let $\tau \in K$ be a generator of $\mathcal{O}_i$. Then, $\ell\tau$ is a generator of $\mathcal{O}_{i+1}$ so there exist $a, b \in \mathbb{Z}$ such that $\alpha = a + b\ell\tau$, so that:

$$N(\alpha) = \alpha\overline{\alpha} = (a + b\ell\tau)(a + b\ell\overline{\tau}) = a^2 + ab\ell\,\mathrm{Tr}(\tau) + \ell^2 b^2 N(\tau).$$

Since $\ell^2 q^2 = \deg(\iota_i(\alpha)) = N(\alpha)$, it follows that $\ell | a$. Hence, $\alpha \in \ell\mathcal{O}_i$. Let $\beta := \frac{\alpha}{\ell} \in \mathcal{O}_i$. Then:

$$\widehat{\varphi_i} \circ \widehat{\psi_{i+1}} \circ \varphi'_i \circ \psi_i = [\ell] \circ \iota_i(\beta) \quad \text{so that} \quad [\ell q] \circ \varphi'_i \circ \psi_i = [\ell] \circ \psi_{i+1} \circ \varphi_i \circ \iota_i(\beta),$$

i.e.

$$[q] \circ \varphi'_i \circ \psi_i = \psi_{i+1} \circ \varphi_i \circ \iota_i(\beta) \quad (\star).$$

Let $P \in E_i[\mathfrak{q}^{(i)}] = \ker(\psi_i)$. Then $[q] \circ \varphi'_i \circ \psi_i(P) = O$, so that $\psi_{i+1} \circ \varphi_i \circ \iota_i(\beta)(P) = O$ *i.e.* $\varphi_i \circ \iota_i(\beta)(P) \in \ker(\psi_{i+1}) = E_{i+1}[\overline{\mathfrak{q}}^{(i+1)}]$. Hence, for all $\gamma \in \overline{\mathfrak{q}}^{(i+1)}$, we have:

$$O = \iota_{i+1}(\gamma) \circ \varphi_i \circ \iota_i(\beta)(P) = \varphi_i \circ \iota_i(\gamma\beta)(P),$$

so that $\iota_i(\gamma\beta)(P) \in \ker(\varphi_i)$. But for all $\gamma \in \mathfrak{q}^{(i+1)}$, we have $\iota_i(\gamma\beta)(P) = O$ because $P \in E_i[\mathfrak{q}^{(i)}]$. Since q splits in K,$\mathfrak{q}^{(i+1)}$ and $\overline{\mathfrak{q}}^{(i+1)}$ are distinct and we have $\mathfrak{q}^{(i+1)} + \overline{\mathfrak{q}}^{(i+1)} = \mathcal{O}_{i+1}$. It follows that $\iota_i(\beta)(P) \in \ker(\varphi_i)$. But $\ker(\varphi_i)$ is a cyclic group of order ℓ and the order of $\iota_i(\beta)(P) \in E_i[\mathfrak{q}^{(i)}]$, which is a cyclic group of order q. Hence, the order of $\iota_i(\beta)(P)$ divides $\gcd(\ell, q) = 1$ *i.e.* $\iota_i(\beta)(P) = O$. We just have proved that $\ker(\psi_i) = E_i[\mathfrak{q}^{(i)}] \subseteq \ker(\iota_i(\beta))$. Then, by [15, Corollary III.4.11], there exists an isogeny $\lambda : F_i \longrightarrow E_i$ such that:

$$\iota_i(\beta) = \lambda \circ \psi_i.$$

By $(\star)$, it follows that $[q] \circ \varphi'_i = \psi_{i+1} \circ \varphi_i \circ \lambda$.

Let $P \in F_i[\mathfrak{q}^{(i)}]$. Since $F_i[\mathfrak{q}^{(i)}] \subseteq F_i[q]$, we have $[q] \circ \varphi'_i(P) = \varphi'_i([q]P) = O$ so that $\psi_{i+1} \circ \varphi_i \circ \lambda(P) = O$ *i.e.* $\varphi_i \circ \lambda(P) \in \ker(\psi_{i+1}) = E_{i+1}[\overline{\mathfrak{q}}^{(i+1)}]$. Hence, for all $\gamma \in \overline{\mathfrak{q}}^{(i+1)}$, we have:

$$O = \iota_{i+1}(\gamma) \circ \varphi_i \circ \lambda(P) = \varphi_i \circ \iota_i(\gamma) \circ \lambda(P),$$

so that $\iota_i(\gamma) \circ \lambda(P) \in \ker(\varphi_i)$. But $\ker(\varphi_i)$ has order ℓ and $\iota_i(\gamma) \circ \lambda(P) \in E_i[q]$ so $\iota_i(\gamma) \circ \lambda(P) = O$. We

also have for all $\gamma \in \mathfrak{q}^{(i+1)}$:

$$\iota_i(\gamma) \circ \lambda(P) = \lambda \circ \iota_i'(\gamma)(P) = O,$$

since $\lambda_*(\iota_i') = (\lambda \circ \psi_i)_*(\iota_i) = (\iota_i(\beta))_*(\iota_i) = \iota_i$. Since $\mathfrak{q}^{(i+1)} + \overline{\mathfrak{q}}^{(i+1)} = \mathcal{O}_{i+1}$, it follows that $\lambda(P) = O$. Hence $F_i[\mathfrak{q}^{(i)}] \subseteq \ker(\lambda)$ and λ has degree q, so $F_i[\mathfrak{q}^{(i)}] = \ker(\lambda)$. Since E_i is the codomain of λ, we have $(E_i, \iota_i) = \mathfrak{q}^{(i)} \cdot (F_i, \iota_i') = (\mathfrak{q}^{(i)})^2 \cdot (E_i, \iota_i)$ and $(\mathfrak{q}^{(i)})^2$ is principal by faithfulness of the group action (Theorem 1.18). Hence, there exists $\gamma \in \mathcal{O}_i$ such that $(\mathfrak{q}^{(i)})^2 = \gamma\mathcal{O}_i$, so that $\gamma \in (\mathfrak{q}^{(i)})^2 \subseteq (\mathfrak{q}^{(1)})^2$ *i.e.* $\gamma\mathcal{O}_1 \subseteq (\mathfrak{q}^{(1)})^2$ but $N((\mathfrak{q}^{(1)})^2) = N((\mathfrak{q}^{(i)})^2) = N(\gamma)$ (by [19, Proposition 7.20.(i)]) so $\gamma\mathcal{O}_1 = (\mathfrak{q}^{(1)})^2$, which contradicts (iii). We conclude that $\ker(\psi_{i+1}) = E_{i+1}[\mathfrak{q}^{(i+1)}]$, so that $(F_{i+1}, \iota_{i+1}') = \mathfrak{q}^{(i+1)} \cdot (E_{i+1}, \iota_{i+1})$. This completes the proof. □

Under the assumptions of Proposition 1.33, $(\star)_i$ admits only one solution for all $i \geq 1$, and there is no ambiguity to determine $j(F_{i+1})$. Since $\mathrm{Cl}(\mathcal{O}_K)$ is trivial, we also know that $j(F_0) = j(E_0)$. However, the solution of (E_0) can be $j(F_1) = j(E_1/E_1[\mathfrak{q}^{(1)}])$ or $j(E_1/E_1[\overline{\mathfrak{q}}^{(1)}])$. Fortunately, $(\mathfrak{q}^{(1)})^2$ is not principal, so that $\mathfrak{q}^{(1)}$ and $\overline{\mathfrak{q}}^{(1)}$ have distinct images in $\mathrm{Cl}(\mathcal{O}_1)$ and $j(E_1/E_1[\mathfrak{q}^{(1)}]) \neq j(E_1/E_1[\overline{\mathfrak{q}}^{(1)}])$ by faithfulness of the ideal class group action and by Theorem 1.27. Hence, we need to compute both j-invariants. This can be made by computing $E_1[\mathfrak{q}^{(1)}]$ and $E_1[\overline{\mathfrak{q}}^{(1)}]$ and using Vélu's formulas [11].

Remark 1.34. The choice of direction $\mathfrak{q}$ and $\overline{\mathfrak{q}}$ at step $i = 1$ is not compulsory, and the non-principality of $(\mathfrak{q}^{(1)})^2$ in $\mathcal{O}_1$ can be a restrictive hypothesis in general, especially if we consider multiple prime ideals like in the real OSIDH cryptosystem. Actually, when $(\mathfrak{q}^{(i)})^2$ is principal in $\mathcal{O}_i$, $j(E_i/E_i[\mathfrak{q}^{(i)}]) = j(E_i/E_i[\overline{\mathfrak{q}^{(i)}}])$ and equation $(\star)_{i-1}$ admits only one solution, so there is no ambiguity till $(\mathfrak{q}^{(i)})^2$ is no longer principal in $\mathcal{O}_i$. Instead of determining the direction at rank 1, we may then determine the direction at rank i_0 such that $(\mathfrak{q}^{(i_0)})^2$ is not principal in $\mathcal{O}_{i_0}$.

Such an index i_0 always exists. Indeed, if $(\mathfrak{q}^{(i)})^2 = \alpha\mathcal{O}_i$ for a certain $\alpha \in \mathcal{O}_i$, then $N(\alpha) = q^2$ by [19, Lemma 7.14.(i)]. Let τ be a generator of $\mathcal{O}_K$, t its trace and d its norm. Then, $\mathcal{O}_i = \mathbb{Z} + \ell^i\tau\mathbb{Z}$ and $\alpha = a + b\ell^i\tau$ with $a, b \in \mathbb{Z}$, so that:

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

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

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

There is no integral root when this quantity is < 0, *i.e.* once $i \geq i_0 := \lfloor \log_\ell(2q/\sqrt{|\Delta_K|}) \rfloor + 1$. Hence, if $i \geq i_0$, we must have $b = 0$, so $a = q$ and $(\mathfrak{q}^{(i_0)})^2 = q\mathcal{O}_i$, so that $\mathfrak{q}^2 = q\mathcal{O}_K$ and q ramifies in K, which is impossible. It follows that $(\mathfrak{q}^{(i)})^2$ is not principal for $i \geq i_0$.

Chapter 2

The OSIDH cryptosystem

2.1 A first naive Diffie Hellman protocol

Let K be a quadratic imaginary number field such that $\mathcal{O}_K$ has a trivial ideal class group $\mathrm{Cl}(\mathcal{O}_K)$. In practice, $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. Let p be a prime that does not split in K. Let ℓ be a prime distinct from p, $n \in \mathbb{N}^*$ (the length of the descending ℓ-isogeny chains) and $\mathcal{O}_i := \mathbb{Z} + \ell^i \mathcal{O}_K$ for all $i \in [\![0\ ;\ n]\!]$.

Let $q_1, \cdots, q_t$ be distinct primes, distinct from ℓ and p that all split in K and let $\mathfrak{q}_j$ be a prime $\mathcal{O}_K$-ideals lying above q_j for all $j \in [\![1\ ;\ t]\!]$. When there is no ambiguity, we shall denote $\mathfrak{q}_j$ instead $\mathfrak{q}_j^{(n)} := \mathfrak{q}_j \cap \mathcal{O}_n$. We can assume that the ideal classes $[\mathfrak{q}_j]$ of the $\mathfrak{q}_j$ in $\mathrm{Cl}(\mathcal{O}_n)$ generate $\mathrm{Cl}(\mathcal{O}_n)$. The action of the $[\mathfrak{q}_j]$ and $[\mathfrak{q}_j]^{-1} = [\overline{\mathfrak{q}_j}]$ on $\rho(\mathrm{Ell}(\mathcal{O}_n))$ can be effectively computed by the method of Paragraph 1.5.2 provided that we represent every element $(E, \iota) \in \rho(\mathrm{Ell}(\mathcal{O}_n))$ as the last element of a descending ℓ-isogeny chain:

$$(E_0, \iota_0) \longrightarrow \cdots \longrightarrow (E_n, \iota_n) = (E, \iota).$$

Hence, the set $\mathrm{Cl}(\mathcal{O}_n)$ acts upon is not $\rho(\mathrm{Ell}(\mathcal{O}_n))$ per se, but the set of descending ℓ-isogeny chains of length n with origin in $\rho(\mathrm{Ell}(\mathcal{O}_K))$ (see Figure 2.1).

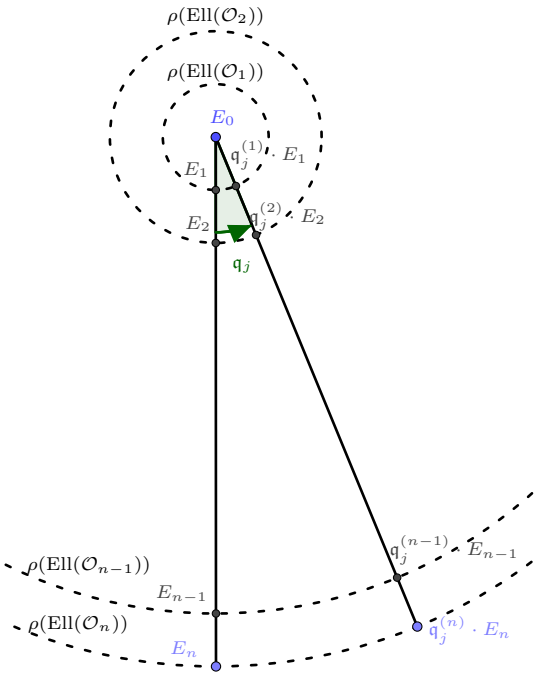

Figure 2.1: Action of the prime ideal $\mathfrak{q}_j$ on the descending ℓ-isogeny chain.

Alice and Bob separately choose secret exponents $e_1, \cdots, e_t$ and $f_1, \cdots, f_t$ 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 Paragraph 1.5.2.

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

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

The key exchange protocol is illustrated in Figure 2.2.

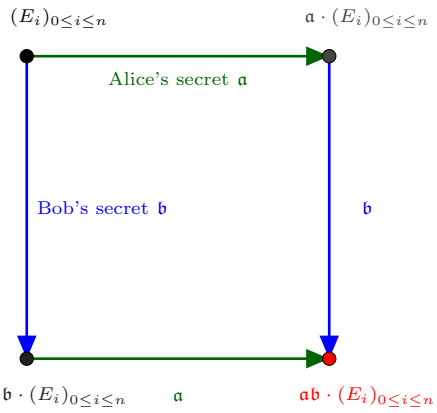

Figure 2.2: Naive Oriented Supersingular Isogeny Diffie-Hellman key exchange protocol. Public data in black, Alice's secret data in green, Bob's secret data in blue, shared secret in red.

Unfortunately, this protocol is insecure because the the attacker can recover the secret ideal class $[\mathfrak{a}]$ with the knowledge of the chains $(E_i, \iota_i)_{0 \leq i \leq n}$ and $\mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$. We present two attacks due to Colò and Kohel [4, § 5.1] in Sections 3.1 and 3.2. To secure OSIDH, the authors came up with a way to perform the key exchange that does not involve an explicit exchange of the chains.

2.2 The OSIDH protocol

OSIDH is basically the Diffie-Hellmann key exchange presented in the previous section. However, the parties do not exchange the chains $(E_{A,i}, \iota_{A,i})$ and $(E_{B,i}, \iota_{B,i})$ (which makes them vulnerable to an attack) while still giving enough data to recover $(E_{AB,i}, \iota_{AB,i})$.

Alice still computes $(E_{A,i}, \iota_{A,i}) := \mathfrak{a} \cdot (E_i, \iota_i)$ but only transmits the end of the chain $E_{A,n}$, which is the most interesting part (since $\mathrm{Cl}(\mathcal{O}_n)$ is the biggest class group). Bob wants to compute $E_{AB,n} = \mathfrak{b} \cap \mathcal{O}_n \cdot E_{A,n}$ but without any further information, he cannot do this computation. Indeed, he needs at least to know the $\mathcal{O}_n$-orientation of $E_{A,n}$ to determine the class group action (computing the kernels and using Vélu's formulas) and this information is contained in the whole isogeny chain $(E_{A,i}, \iota_{A,i})$ (since $\iota_{A,n}$ could be obtained with the knowledge $\iota_{A,0}$ and the ℓ-isogenies $E_{A,i} \longrightarrow E_{A,i+1}$ for all $i \in [\![0 \ ; \ n-1]\!]$). Otherwise, to compute $\mathfrak{q}_j \cdot E_{A,n} = E_{A,n}/E_{A,n}[\mathfrak{q}_j]$, Bob does not know how to chose between the $q_j + 1$ possible values of $E_{A,n}[\mathfrak{q}_j]$. Actually, the action of powers of $\mathfrak{q}_j$ and $\overline{\mathfrak{q}}_j$ on $E_{A,n}$ for all $j \in [\![1 \ ; \ t]\!]$ is enough to determine $E_{AB,n}$.

We recall that $\mathfrak{a}$ and $\mathfrak{b}$ can be written:

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

with small exponents $e_1, \cdots, e_t, f_1, \cdots, f_t \in [\![-r\ ;\ r]\!]$. Note that we allow negative exponents as we identify $\mathfrak{q}_j^{-k}$ with $\overline{\mathfrak{q}}_j^{k}$ for all $k \in \mathbb{N}^*$ and $j \in [\![1\ ;\ t]\!]$. In the OSIDH protocol, Alice computes for all $j \in [\![1\ ;\ t]\!]$ the chains $\mathfrak{q}_j^k \cdot (E_{A,i}, \iota_{A,i})$ and transmits to Bob the ending element $[\mathfrak{q}_j]^k \cdot E_{A,n}$ for all $k \in [\![-r\ ;\ r]\!]$, forming the q_j-isogeny chain:

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

This data is enough for Bob to compute $[\mathfrak{b}] \cdot E_{A,n}$. We explain how. Suppose that $f_1, f_2 \geq 0$. Bob knows the chain:

$$E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_1]^{f_1} \cdot E_{A,n}$$

and $[\mathfrak{q}_2] \cdot E_{A,n}$, which enables him to construct the ladder:

$$\begin{array}{ccccccc}
[\mathfrak{q}_2] \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1][\mathfrak{q}_2] \cdot E_{A,n} & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1]^{f_1-1}[\mathfrak{q}_2] \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2] \cdot E_{A,n} \\
{\scriptstyle q_2}\uparrow & & \uparrow & & \uparrow & & \uparrow \\
E_{A,n} & \xrightarrow{q_1} & [\mathfrak{q}_1] \cdot E_{A,n} & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1]^{f_1-1} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1]^{f_1} \cdot E_{A,n},
\end{array}$$

using q_1 and q_2-modular equations only as in Paragraph 1.5.2. This can be done without ambiguity (there is always a unique solution to the system of modular equations) by the same arguments we used in Proposition 1.33. Indeed, we know that the elliptic curve at the top left corner is $[\mathfrak{q}_2] \cdot E_{A,n}$, that $(\mathfrak{q}_2^{(n)})^2$ is not principal in $\mathcal{O}_n$ and that the map $\mathrm{SS}_{\mathcal{O}_n}(p) \cap \mathrm{im}(\rho) \longrightarrow \mathrm{SS}(p)$ is injective by Theorem 1.27. Going further, Bob obtains $[\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^2 \cdot E_{A,n}$ from $[\mathfrak{q}_2]^2 \cdot E_{A,n}$ and the chain:

$$[\mathfrak{q}_2] \cdot E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2] \cdot E_{A,n}$$

and repeats the process until reaching $[\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2} \cdot E_{A,n}$. The method consists in computing the following diagram, horizontal chain by horizontal chain, starting from the bottom:

$$\begin{array}{ccccccc}
[\mathfrak{q}_2]^{f_2} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1][\mathfrak{q}_2]^{f_2} \cdot E_{A,n} & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1]^{f_1-1}[\mathfrak{q}_2]^{f_2} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2} \cdot E_{A,n} \\
\uparrow & & \uparrow & & \uparrow & & \uparrow \\
[\mathfrak{q}_2]^{f_2-1} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1][\mathfrak{q}_2]^{f_2-1} \cdot E_{A,n} & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1]^{f_1-1}[\mathfrak{q}_2]^{f_2-1} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2-1} \cdot E_{A,n} \\
\vdots & & \vdots & \ddots & \vdots & & \vdots \\
[\mathfrak{q}_2] \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1][\mathfrak{q}_2] \cdot E_{A,n} & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1]^{f_1-1}[\mathfrak{q}_2] \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2] \cdot E_{A,n} \\
{\scriptstyle q_2}\uparrow & & \uparrow & & \uparrow & & \uparrow \\
E_{A,n} & \xrightarrow{q_1} & [\mathfrak{q}_1] \cdot E_{A,n} & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1]^{f_1-1} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_1]^{f_1} \cdot E_{A,n}.
\end{array}$$

For negative exponents, the method is the same but starts from $[\mathfrak{q}_1]^{-1} \cdot E_{A,n}$, $[\mathfrak{q}_1]^{-2} \cdot E_{A,n}$...

In order to compute $[\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2}[\mathfrak{q}_3]^{f_3} \cdot E_{A,n}$, Bob computes a diagram as above with the chains:

$$E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_1]^{f_1} \cdot E_{A,n}$$

$$\text{and} \quad [\mathfrak{q}_1]^{f_1} \cdot E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_1]^{f_1}[\mathfrak{q}_2]^{f_2} \cdot E_{A,n}$$

at the bottom (the latter following the first) and the chain:

$$E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_3]^{f_3} \cdot E_{A,n},$$

on the left side.

More generally, for $j \in [\![1\ ;\ t-1]\!]$, assuming Bob has already computed the chains:

$$E_{A,n} \longrightarrow [\mathfrak{q}_1] \cdot E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_1]^{f_1} \cdot E_{A,n},$$

$$\vdots$$

$$\prod_{k=1}^{j-1} [\mathfrak{q}_k]^{f_k} \cdot E_{A,n} \longrightarrow \left(\prod_{k=1}^{j-1} [\mathfrak{q}_k]^{f_k}\right) [\mathfrak{q}_j] \cdot E_{A,n} \longrightarrow \cdots \longrightarrow \prod_{k=1}^{j} [\mathfrak{q}_k]^{f_k} \cdot E_{A,n}.$$

Bob can compute the following diagram from bottom and left to top and right for all $k \in [\![1\ ;\ j]\!]$:

$$\begin{array}{ccccccc}
[\mathfrak{q}_{j+1}]^{f_{j+1}} \prod_{l=1}^{k-1} [\mathfrak{q}_l]^{f_l} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_{j+1}]^{f_{j+1}} \left(\prod_{l=1}^{k-1} [\mathfrak{q}_l]^{f_l}\right) [\mathfrak{q}_k] \cdot E_{A,n} & \longrightarrow & \cdots & \longrightarrow & [\mathfrak{q}_{j+1}]^{f_{j+1}} \prod_{l=1}^{k} [\mathfrak{q}_l]^{f_l} \cdot E_{A,n} \\
\uparrow & & \uparrow & & & & \uparrow \\
\vdots & & \vdots & & \ddots & & \vdots \\
\uparrow & & \uparrow & & & & \uparrow \\
[\mathfrak{q}_{j+1}] \prod_{l=1}^{k-1} [\mathfrak{q}_l]^{f_l} \cdot E_{A,n} & \longrightarrow & [\mathfrak{q}_{j+1}] \left(\prod_{l=1}^{k-1} [\mathfrak{q}_l]^{f_l}\right) [\mathfrak{q}_k] \cdot E_{A,n} & \longrightarrow & \cdots & \longrightarrow & [\mathfrak{q}_{j+1}] \prod_{l=1}^{k} [\mathfrak{q}_l]^{f_l} \cdot E_{A,n} \\
\uparrow{\scriptstyle q_{j+1}} & & \uparrow & & & & \uparrow \\
\prod_{l=1}^{k-1} [\mathfrak{q}_l]^{f_l} \cdot E_{A,n} & \xrightarrow{q_k} & \left(\prod_{l=1}^{k-1} [\mathfrak{q}_l]^{f_l}\right) [\mathfrak{q}_k] \cdot E_{A,n} & \longrightarrow & \cdots & \longrightarrow & \prod_{l=1}^{k} [\mathfrak{q}_l]^{f_l} \cdot E_{A,n},
\end{array}$$

starting from the chain:

$$E_{A,n} \longrightarrow \cdots \longrightarrow [\mathfrak{q}_{j+1}]^{f_{j+1}} \cdot E_{A,n}$$

on the left side for $k = 1$. The result for $k = j$ on the right side of the diagram is:

$$\prod_{k=1}^{j} [\mathfrak{q}_k]^{f_k} \cdot E_{A,n} \longrightarrow \left(\prod_{k=1}^{j} [\mathfrak{q}_k]^{f_k}\right) [\mathfrak{q}_{j+1}] \cdot E_{A,n} \longrightarrow \cdots \longrightarrow \prod_{k=1}^{j+1} [\mathfrak{q}_k]^{f_k} \cdot E_{A,n},$$

making it possible to repeat the procedure once again at rank $j+1$. For $j = t$, Bob finally obtains at the end of the chain:

$$\prod_{k=1}^{t} [\mathfrak{q}_k]^{f_k} \cdot E_{A,n} = [\mathfrak{b}] \cdot E_{A,n}.$$

In parallel, Alice performs the symmetric process with the data sent by Bob.

The real OSIDH protocol as introduced in [4, § 5.2] is presented in Figure 2.3.

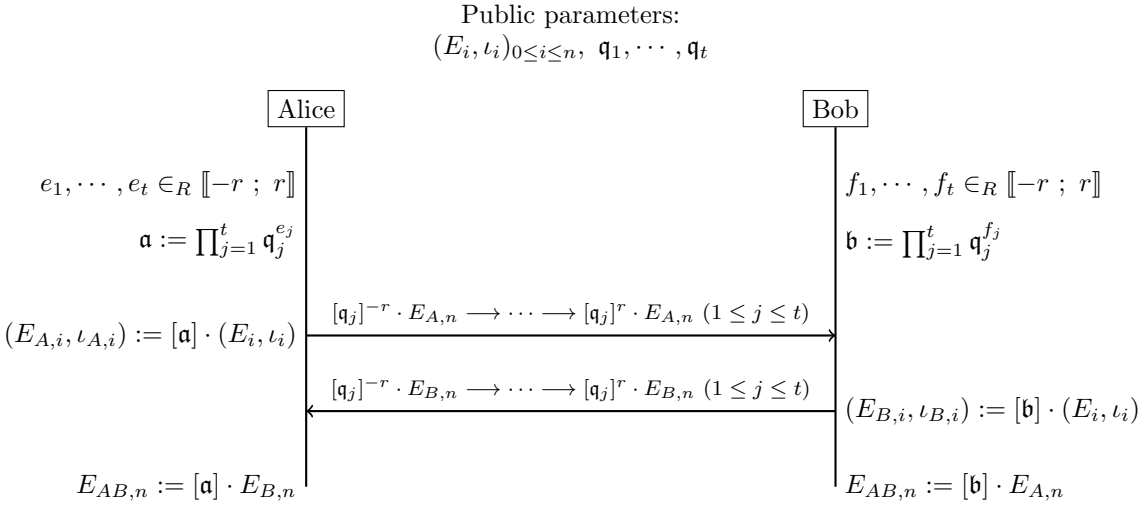

Figure 2.3: The OSIDH protocol as presented in [4, § 5.2].

Chapter 3

Cryptanalysis of OSIDH

This chapter studies different attacks against the OSIDH cryptosystem. In the first two sections, we present two attacks on the naive Diffie Hellman protocol of Paragraph 2.1, recovering the secret ideal classes when the chains are explicitely exchanged. These attacks are due to [4, § 5.1] but we provide more details. In particular, both attacks include a lattice reduction step that was not suggested in the original article and that we use in another attack.

The three next sections study attacks on the real OSIDH key exchange. Section 3.3 presents an attack due to Onuki [12, § 6.3] exploiting the fact that one can recover a descending ℓ-isogeny chain with the knowledge of a K-oriented endomorphism at each level. Section 3.4 presents an original attack based on this approach and coupled with a lattice reduction. Finally, Section 3.5 presents Kuperberg's quantum attack.

We also provide implementations of the attacks of Sections 3.5 and 3.4 in `SageMath` [6] for toy parameters. The source code can be found on Github [13].

3.1 A first attack using quaternions

This section makes an intensive use of quaternion arithmetic. We refer to Appendix A.3 and to the lecture notes of Voight [24] for results and vocabulary.

We recall here the problem we have to solve: given a chain $(E_i, \iota_i)_{0\leq i\leq n}$ and a chain $(F_i, \iota'_i)_{0\leq i\leq n} = \mathfrak{a}\cdot(E_i,\iota_i)_{0\leq i\leq n}$ with a secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$, we want to recover $[\mathfrak{a}]$, or more exactly, exponents $e_1, \cdots, e_t \in \mathbb{Z}$ (relatively small) such that $[\mathfrak{a}] = \prod_{j=1}^{t}[\mathfrak{q}_j]^{e_j}$, so that the action of $[\mathfrak{a}]$ on descending ℓ-isogeny chains of length n can be easily computed. The attack consists in the following steps:

1. Recover $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$ from the chains $(E_i, \iota_i)_{0\leq i\leq n}$ and $(F_i, \iota'_i)_{0\leq i\leq n}$.
2. Compute a connecting ideal I between $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$, defining an isogeny $E_n \longrightarrow F_n$ by the Deuring correspondence.
3. Find an equivalent ideal J to I that is generated by a prime ideal $\mathfrak{N}$ of $\mathcal{O}_n$ norm $N \neq \ell$.
4. Find an ideal $\mathfrak{a} \subseteq \mathcal{O}_n$ equivalent to $\mathfrak{N}$ and decompose its class $[\mathfrak{a}]$ in $\mathrm{Cl}(\mathcal{O}_n)$ as a product of powers of the prime ideal classes $[\mathfrak{q}_j]$.

3.1.1 Step 1: compute $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$

If $E/\mathbb{F}_{p^2}$ is a supersingular elliptic curve, we know that $\mathrm{End}(E)$ is a maximal order in the quaternion algebra $B_{p,\infty}$ ramifying at p and ∞ (by [24, Theorem 42.1.9]). We have an explicit description of $B_{p,\infty}$ as $B_{p,\infty} = H(a,b)$ $(a,b\in\mathbb{Q})$, with $H(a,b) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$ and:

$$i^2 = a, \quad j^2 = b, \quad k = ij, \quad ij = -ji.$$

This description follows from [25, Proposition 5.1]:

$$B_{p,\infty} = \begin{cases} H(-1,-1) & \text{if } p = 2 \\ H(-1,-p) & \text{if } p \equiv 3\ [4] \\ H(-2,-p) & \text{if } p \equiv 5\ [8] \\ H(-q,-p) & \text{if } p \equiv 1\ [8] \end{cases}$$

with $q \equiv 3\ [4]$ and $\left(\frac{q}{p}\right) = -1$. Using an isomorphism $\mathrm{End}^0(E) := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_{p,\infty}$, one can express a $\mathbb{Z}$-basis of $\mathrm{End}(E)$ in terms of i,j,k. However, given an endomorphism of E expressed in the $\mathbb{Z}$-basis of $\mathrm{End}(E)$ or equivalently, in terms of 1, i,j, k it is not trivial in general to know how to evaluate it on points of E, but this evaluation will be necessary to find the endomorphism rings of the elleptic curves in the chains $(E_i, \iota_i)_{0 \le i \le n}$ and $(F_i, \iota'_i)_{0 \le i \le n}$.

More precisely, following [26], we shall need to evaluate in polynomial time in $\log(p) = \Theta(n)$ any element of the $\mathbb{Z}$-basis of $\mathrm{End}(E)$ at points of E defined over a field extension of $\mathbb{F}_p$ of polynomial degree in $\log(p)$. If it is the case, any linear combination of elements of such a basis with coefficients in polynomial size in $\log(p)$ can be evaluated in polynomial time in $\log(p)$. Such a basis will be said *useful*. We may restrict the possibility to evaluate to points with **known order** prime to a certain integer $f \in \mathbb{Z}$, in which case the basis will be said *f-useful*. We also want this basis to be *concise*, that is to say storable in polynomial space in $\log(p)$, *e.g.* with an expression in terms of 1, i,j, k (via the isomorphism $\mathrm{End}^0(E) \simeq B_{p,\infty}$) of polynomial size in $\log(p)$.

In the following of this section, for symplicity, we shall mean polynomial in $\log(p)$ everytime we use the term polynomial.

Definition 3.1. The data given by an isomorphism $\Phi : B_{p,\infty} \xrightarrow{\sim} \mathrm{End}^0(E)$ together with a basis of $\mathrm{End}(E)$ that is (f-)useful and concise (relatively to Φ) is called an (f-)*compact representation* of $\mathrm{End}(E)$.

Generally, an order $\mathcal{R} \subseteq B_{p,\infty}$ or a lattice $I \subseteq B_{p,\infty}$ will be said *concise* when given with a concise $\mathbb{Z}$-basis.

Example 3.2. For $p \equiv 3\ [4]$, let E_0 be the elliptic curve defined by the Weierstrass equation $y^2 = x^3 + x$. Then $\mathrm{End}(E_0)$ admits a compact representation given by the isomorphism:

$$\Phi_0 : B_{p,\infty} = H(-1,-p) \longrightarrow \mathrm{End}^0(E_0)$$

mapping i to $\phi : (x,y) \longmapsto (-x, ay)$ (with $a^2 = -1$) and j to the Frobenius $\pi : (x,y) \longmapsto (x^p, y^p)$. The family $\left(1, \phi, \frac{\phi+\pi}{2}, \frac{1+\pi\phi}{2}\right)$ is a useful and concise basis of $\mathrm{End}(E_0)$.

In general, the first curve of the chain E_0 will be chosen to have a compact representation as in Example 3.2, in order to simplify the protocol execution. We shall prove that the knowledge of the chain $(E_i, \iota_i)_{0 \le i \le n}$ will help us construct a compact representation of $\mathrm{End}(E_i)$ for all $i \in [\![0\ ;\ n]\!]$, ensuring that we can deduce a basis of $\mathrm{End}(E_{i+1})$ from a basis of $\mathrm{End}(E_i)$ for all $i \in [\![0\ ;\ n-1]\!]$.

Lemma 3.3. *The map:*

$$\psi \in \mathrm{End}^0(E_i) \longmapsto \frac{1}{\ell}\varphi_i \psi \widehat{\varphi_i} \in \mathrm{End}^0(E_{i+1})$$

is an isomorphism of quaternion algebras inducing a ring isomorphism between quaternion orders:

$$\mathbb{Z} + \ell\,\mathrm{End}(E_i) \simeq \mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}.$$

As a consequence, $\mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}$ has index ℓ^3 in $\mathrm{End}(E_{i+1})$.

Proof. Everything is clear, except maybe the last assertion. Since, $\mathbb{Z} + \ell\,\mathrm{End}(E_i) \simeq \mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}$, we have:

$$\mathrm{disc}(\mathbb{Z} + \ell\,\mathrm{End}(E_i)) = \mathrm{disc}(\mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}),$$

by [24, Corollary 15.2.9]. By [24, Theorem 15.5.5], we also have:

$$\mathrm{disc}(\mathrm{End}(E_i)) = \mathrm{disc}(\mathrm{End}(E_{i+1})) = 16p^2,$$

since $\mathrm{End}(E_i)$ and $\mathrm{End}(E_{i+1})$ are maximal. Finally, by [24, Lemma 15.2.15], we have:

$$\mathrm{disc}(\mathrm{End}(E_i)) = [\mathrm{End}(E_i) : \mathbb{Z} + \ell\,\mathrm{End}(E_i)]^2\,\mathrm{disc}(\mathbb{Z} + \ell\,\mathrm{End}(E_i))$$

and:

$$\mathrm{disc}(\mathrm{End}(E_{i+1})) = [\mathrm{End}(E_{i+1}) : \mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}]^2\,\mathrm{disc}(\mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}),$$

so that:

$$[\mathrm{End}(E_{i+1}) : \mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}] = [\mathrm{End}(E_i) : \mathbb{Z} + \ell\,\mathrm{End}(E_i)] = \ell^3.$$

□

Proposition 3.4. *Assume that E_0 admits a compact representation. Then, E_i admits an ℓ-compact representation for all $i \in [\![0\ ;\ n]\!]$ and one can deduce $\mathrm{End}(E_{i+1})$ from $\mathrm{End}(E_i)$ in polynomial time (in $\log(p)$) for all $i \in [\![0\ ;\ n-1]\!]$. Hence, one can recover $\mathrm{End}(E_n)$ from $\mathrm{End}(E_0)$ in polynomial time (in $\log(p)$).*

Proof. Let $i \in [\![0\ ;\ n]\!]$ and let $\alpha_1, \cdots, \alpha_4$, $\beta_1^{(i)}, \cdots, \beta_4^{(i)}$ be respectively a concise and useful $\mathbb{Z}$-basis of $\mathrm{End}(E_0)$ and a $\mathbb{Z}$-basis of $\mathrm{End}(E_i)$. Without loss of generality, we can assume that $\alpha_1 = [1]_{E_0}$ and $\beta_1^{(i)} = [1]_{E_i}$. Let $\phi_i := \varphi_{i-1} \circ \cdots \circ \varphi_0$. Then, by Lemma 3.3, $\mathbb{Z} + \phi_i\,\mathrm{End}(E_0)\widehat{\phi_i}$ has index ℓ^{3i} in $\mathrm{End}(E_i)$ so that:

$$\beta_r^{(i)} = \frac{1}{\ell^{3i}} \sum_{s=1}^{4} c_{r,s} \circ \phi_i \circ \alpha_s \widehat{\phi_i},$$

with $c_{r,1}, \cdots, c_{r,4} \in \mathbb{Z}$ for all $r \in [\![1\ ;\ 4]\!]$. Assuming, the $c_{r,s}$ have polynomial size (in $\log(p)$), we get a compact representation of $\mathrm{End}(E_i)$. Indeed, $(\beta_1^{(i)}, \cdots, \beta_4^{(i)})$ is clearly concise so we only need to prove the ℓ-usefulness of this basis.

Let $P \in E(k)$ with $[k : \mathbb{F}_p]$ polynomial and order prime to ℓ. To evaluate $\beta_r^{(i)}(P)$, we first evaluate $[\ell^{3i}]\beta_r^{(i)}(P) = \sum_{s=1}^{4} c_{r,s} \circ \phi_i \circ \alpha_s \widehat{\phi_i}(P)$. First, since φ_j has degree ℓ for all $j \in [\![0\ ;\ i-1]\!]$, the φ_j and $\widehat{\varphi_j}$ can be evaluated with $O(\ell)$ operations over k (using Vélu's formulas [11] for instance), so it can be performed in polynomial time. Using efficient scalar multiplication techniques like double and add, sliding windows, w-NAF or Yao's method, the scalar multiplication by the $c_{r,s}$ can be performed in time $O(\log(|c_{r,s}|)$, which is polynomial. $(\alpha_1, \cdots, \alpha_4)$ being useful, $[\ell^{3i}]\beta_r^{(i)}(P)$ can be evaluated in polynomial time. Knowing the order m of P which is prime to ℓ, we find an inverse u of ℓ^{3i} modulo m in time $O(\min(\log(m), \log(\ell^{3i})))$ using extended euclidean algorithm. But $\log(m)$ is polynomial (in $\log(p)$) by Hasse-Weil's bound and $\log(\ell^{3i}) = O(\log(p))$ since $p > |\Delta_K|\ell^{2n}$ by Proposition 1.33, so we may find u in polynomial time and obtain $[u][\ell^{3i}]\beta_r^{(i)}(P) = \beta_r^{(i)}(P)$. Hence, the ℓ-usefulness follows.

The fact that $c_{r,s}$ can be chosen in polynomial size remains to be proved. It will follow naturally from the algorithm computing $\mathrm{End}(E_{i+1})$ from $\mathrm{End}(E_i)$. Let $\mathcal{R} := \mathrm{End}(E_{i+1})$ and $\mathcal{R}' := \mathbb{Z} + \varphi_i\,\mathrm{End}(E_i)\widehat{\varphi_i}$. Let $\gamma_r^{(i)} := \varphi_i \circ \beta_r^{(i)} \circ \widehat{\varphi_i}$ for all $r \in [\![1\ ;\ 4]\!]$. Then, $(\gamma_1^{(i)}, \cdots, \gamma_4^{(i)})$ is a $\mathbb{Z}$-basis of $\mathcal{R}'$ and $[\mathcal{R} : \mathcal{R}'] = \ell^3$ so if we fix a $\mathbb{Z}$-basis $(\beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)})$ of $\mathcal{R}$, there is a matrix $M \in M_4(\mathbb{Z})$ of determinant ℓ^3 such that:

$${}^t(\gamma_1^{(i)}, \cdots, \gamma_4^{(i)}) = M\,{}^t(\beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)})$$

Since $\gamma_1^{(i)} = 1$ (by assumption, $\beta_1^{(i)} = 1$) and we may assume without loss of generality, that $\beta_1^{(i+1)} = 1$, the first row of M is $\begin{pmatrix} 1 & 0 & 0 & 0 \end{pmatrix}$. Since $\mathcal{R}$ is determined by the basis $(\beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)})$ up to action by $GL_4(\mathbb{Z})$, we can multiply M on the right by any matrix of $GL_4(\mathbb{Z})$. Hence, we can reduce M to its

Hermite normal form (HNF), so that M is triangular inferior of the form:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \ell^{n_1} & m_{2,3} & m_{2,4} \\ 0 & 0 & \ell^{n_2} & m_{3,4} \\ 0 & 0 & 0 & \ell^{n_3} \end{pmatrix},$$

with $n_1, n_2, n_3 \in \mathbb{N}$ such that $n_1 + n_2 + n_3 = 3$ and $m_{r,s} \in [\![0\ ;\ \ell^{n_r} - 1]\!]$ for all $r \in \{2, 3\}$ and $s \geq r + 1$. Hence, there are at most:

$$\sum_{n_1+n_2+n_3=3} \ell^{2n_1+n_2} \leq \binom{5}{2}\ell^6 = 10\ell^6$$

possible values for M, hence for $\langle \beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)} \rangle = \mathcal{R}$. One can test each value by expressing $\beta_r^{(i+1)}\beta_s^{(i+1)}$ in the basis $(\beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)})$ for all $r, s \in [\![1\ ;\ 4]\!]$, in order to check if the coefficients are integers and test if $\mathrm{disc}(\mathcal{R}) = 16p^2$. If yes, $\mathcal{R}$ is a maximal order and one can test if $\mathcal{R} = \mathrm{End}(E_{i+1})$ in polynomial time by finding an elliptic curve $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \simeq \mathcal{R}$ using Algorithm 1, and checking if $j(E) = j(E_{i+1})$ or $j(E_{i+1})^p$, since E_{i+1} is characterized by its endomorphism ring up to Galois action of the Frobenius by [24, Lemma 42.4.1]. Note that this algorithm runs under the assumption that $(\beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)})$ is compact and ℓ-useful. Expressing M^{-1}, we see immediately that $(\beta_1^{(i+1)}, \cdots, \beta_4^{(i+1)})$ is compact and ℓ-useful if $(\beta_1^{(i)}, \cdots, \beta_4^{(i)})$ is, so we conclude by induction that it is the case if we initialize at $(\beta_1^{(0)}, \cdots, \beta_4^{(0)}) = (\alpha_1, \cdots, \alpha_4)$. Hence, we can compute $\mathrm{End}(E_{i+1})$ from $\mathrm{End}(E_i)$ in a bounded number of instances of a polynomial time algorithm. This completes the proof. □

Now we explain how to solve the following problem, which will help us to test the different possible values for E_{i+1}.

Problem 3.5. Given E_0 and $\mathcal{R}_0 \subseteq B_{p,\infty}$ an ℓ-compact representation of $\mathrm{End}(E_0)$ and a concise[1] maximal order $\mathcal{R}$, find $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \simeq \mathcal{R}$.

Actually, this problem can be solved in polynomial time using the following algorithm. This algorithm is based on the Deuring correspondence between integral left $\mathcal{R}_0$-ideals and isogenies with domain E_0 (see Appendix A.4), on an algorithm explicitly computing this correspondence (see Appendix B.3) and on a quaternion arithmetic algorithm due to Kohel, Lauter, Petit and Tignol [27] (see Appendix B.2).

Algorithm 1: Algorithm to solve Problem 3.5.

Data: E_0 an elliptic curve, $\mathcal{R}_0$, an ℓ-compact representation of $\mathrm{End}(E_0)$ and $\mathcal{R}$, a concise maximal order.

Result: $E/\mathbb{F}_{p^2}$ such that $\mathrm{End}(E) \simeq \mathcal{R}$.

1 Compute a connecting ideal I between $\mathcal{R}_0$ and $\mathcal{R}$ (take $I := \mathcal{R}_0\mathcal{R}$ and multiply it by an integer if necessary to ensure $I \subseteq \mathcal{R}$);

2 Find an equivalent ideal $J \sim I$ of powersmooth norm using KLPT (see Appendix B.2, Algorithm 3);

3 Compute the isogeny $\phi : E_0 \longrightarrow E$ of kernel $E_0[J]$ using effective Deuring correspondence (see Appendix B.3, Algorithm 4);

4 Return E;

3.1.2 Step 2: find a connecting ideal between $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$

Knowing ℓ-concise representations $\mathcal{R}$ and $\mathcal{R}'$ (as maximal order of $B_{p,\infty}$) of $\mathrm{End}(E_n)$ and $\mathrm{End}(F_n)$ respectively, we obtain an ℓ-concise representation of their product $I := \mathcal{R}\mathcal{R}'$ which is a connecting

[1] Given by a $\mathbb{Z}$-basis with coefficients in polynomial size (in $\log(p)$) in terms of $1, i, j, k$.

left-$\mathcal{R}$-ideal, meaning that:

$$O_L(I) := \{\alpha \in B_{p,\infty} \mid \alpha \cdot I \subseteq I\} = \mathcal{R} \quad \text{and} \quad O_R(I) = \{\alpha \in B_{p,\infty} \mid I \cdot \alpha \subseteq I\} = \mathcal{R}'.$$

To make I integral (*i.e.* such that $I \subseteq \mathcal{R}$) we may multiply this basis by an integer of size $O(\log(p))$, so that the basis remains ℓ-concise. We compute a $\mathbb{Z}$-basis of I in polynomial time in $\log(p)$ by computing the hermite normal form of the matrix of a generating set of I in a basis of $\mathcal{R}$.

3.1.3 Step 3: find an equivalent ideal J to I that is generated by a prime ideal $\mathfrak{N}$ of $\mathcal{O}_n$

This paragraph is a bit technical and makes intensive use of the quaternion arithmetic ideas of KLPT (see Appendix B.2). The reader could either skip it or read Appendix B.2 before.

As in step a of KLPT (Algorithm 3), we can find $\delta \in I$ of norm $N \operatorname{nrd}(I)$ with $N \neq p$ prime and $N = O(\sqrt{p}\log^2(p))$ (in general), in time $O(\log(p))$. By Lemma B.1, $J := I\overline{\delta}/\operatorname{nrd}(I) \sim I$ is integral and $\operatorname{nrd}(J) = N$.

We now prove that J is generated by a prime ideal of $\mathcal{O}_n$ lying above N. We may assume that $\mathcal{R} \simeq \operatorname{End}(E_n)$ is special with respect to $R = \mathcal{O}_n$, in the sense of the following definition:

Definition 3.6. We say that a maximal order $\mathcal{R} \subseteq B_{p,\infty}$ is *special* if $j \in \mathcal{R}$ (with $j^2 = -p$) and there exists a subring of rank 2, $R \subset \mathcal{R}$, such that $R^\perp \subseteq Rj$, where $R^\perp$ is the orthogonal of R for the scalar product given by:

$$(\alpha, \beta) \in B_{p,\infty}^2 \longmapsto (\alpha|\beta) := \operatorname{nrd}(\alpha + \beta) - \operatorname{nrd}(\alpha) - \operatorname{nrd}(\beta) = \operatorname{Tr}(\alpha\overline{\beta}).$$

Indeed, we usually take for E_0 the elliptic curve of equation $y^2 = x^3 + x$ with $p \equiv 3$ [4], $K = \mathbb{Q}(i)$ with $i^2 = -1$ and $\mathcal{O}_K = \mathbb{Z}[i] \subseteq \operatorname{End}(E_0) \simeq \langle 1, j, \frac{i+j}{2}, \frac{1+k}{2}\rangle$ (see Example B.3). Since $\mathcal{O}_K \subseteq (j\mathcal{O}_K)^\perp$, $\operatorname{End}(E_0)$ is special for $R = \mathcal{O}_K$. The inclusion $\mathbb{Z} + \ell^n \operatorname{End}(E_0) \hookrightarrow \operatorname{End}(E_n) \simeq \mathcal{R}$ ensures that $\mathcal{R}$ is special with $R = \mathbb{Z} + \ell^n\mathcal{O}_K = \mathcal{O}_n$.

Let $\mathcal{S}$ be the suborder $\mathcal{O}_n \oplus j\mathcal{O}_n$ in $\mathcal{R}$. Then, $J \cap \mathcal{S} = J \cap \mathcal{O}_n \oplus (J \cap j\mathcal{O}_n)$ is a left $\mathcal{S}$-ideal and we have a natural injective ring homomorphism $\mathcal{S}/J \cap \mathcal{S} \hookrightarrow \mathcal{R}/J$. It follows that $[\mathcal{S} : J \cap \mathcal{S}]|[\mathcal{R} : J] = N^2$. Besides, by orthogonality of $\mathcal{O}_n$ and $j\mathcal{O}_n$, we have a group homomorphism:

$$\mathcal{S}/J \cap \mathcal{S} \simeq \mathcal{O}_n/J \cap \mathcal{O}_n \times j\mathcal{O}_n/J \cap j\mathcal{O}_n,$$

so that $[\mathcal{S} : J \cap \mathcal{S}] = [\mathcal{O}_n : J \cap \mathcal{O}_n][j\mathcal{O}_n : J \cap j\mathcal{O}_n]$. We obviously have, $[\mathcal{O}_n : J \cap \mathcal{O}_n] > 1$, otherwise, $1 \in J$ so $J = \mathcal{R}$ and $\operatorname{nrd}(J) = 1 \neq N$, so $[\mathcal{O}_n : J \cap \mathcal{O}_n] = N$ or N^2. In the latter case, $[j\mathcal{O}_n : J \cap j\mathcal{O}_n] = 1$ so $j \in J$. But $\operatorname{nrd}(j) = p$ and $N \nmid p$. Contradiction. So $[\mathcal{O}_n : J \cap \mathcal{O}_n] = N$ and $J \cap \mathcal{O}_n$ is a prime ideal of norm N in $\mathcal{O}_n$.

Hence, according to the following lemma, we can find an element $\alpha \in J \cap \mathcal{O}_n$ such that $\gcd(\operatorname{nrd}(\alpha), N^2) = N$ in polynomial time in $\log(p)$. It follows that $J = \mathcal{R}N + \mathcal{R}\alpha = \mathcal{R} \cdot J \cap \mathcal{O}_n$ as in step b of KLPT.

Lemma 3.7. *Let $\mathfrak{N}$ be an ideal of $\mathcal{O}_n$ of prime norm N. Then, there exists $\alpha \in \mathfrak{N}$ such that $\gcd(N(\alpha), N^2) = N$ and $\mathfrak{N} = \langle N, \alpha\rangle$. One can find α in time $O(\log^4(N))$.*

Proof. Let $\theta \in K$ be a generator of $\mathcal{O}_K$, $t := \operatorname{Tr}(\theta)$ and $s := N(\theta)$. Since $\mathfrak{N}$ has norm N, N is not inert in K so there is a root $\lambda \in \mathbb{Z}$ of the reduction modulo N of the minimal polynomial of θ: $\Pi_\theta := X^2 - tX + s$ such that $\mathfrak{N} = \langle N, \ell^n(\theta - \lambda)\rangle$, so we may set $\alpha := \ell^n(\theta - \lambda)$. Then, we have:

$$N(\alpha) = \ell^{2n}(\lambda^2 - t\lambda + s) = \ell^{2n}\Pi_\theta(\lambda) \equiv 0\ [N].$$

Since $\ell \nmid N$, if $N(\alpha) \equiv 0\ [N^2]$, then $\Pi_\theta(\lambda) \equiv 0\ [N^2]$ and:

$$N(\alpha+N) = \ell^{2n}((\lambda+N)^2 - t(\lambda+N)+s) = \ell^{2n}(\Pi_\theta(\lambda) + N\Pi'_\theta(\lambda) + N^2) \equiv \ell^{2n} N\Pi'_\theta(\lambda)\ [N^2],$$

but $\Pi'_\theta(\lambda) \neq 0\ [N]$, since N does not divide Δ_K (recall that $N = \Omega(\sqrt{p})$ is big and that Δ_K is small). Hence, $\gcd(N(\alpha+N), N^2) = N$.

To find α, the dominant operation is finding the roots of Π_θ modulo N. This can be done with Tonelli-Shanks [28, Algorithm 1.5.1] algorithm, computing a square root of Δ_K modulo N, in time $O(\log^4(N))$. □

3.1.4 Step 4: express $[\mathfrak{N}]$ as a product of the $[\mathfrak{q}_j]$ with small exponents

In order to be able to compute the action of $[\mathfrak{N}]$ on descending ℓ-isogeny chains, we need to express this ideal class as a product of the $[\mathfrak{q}_j]$ in $\mathrm{Cl}(\mathcal{O}_n)$:

$$[\mathfrak{N}] = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e_j} \quad (\star),$$

with exponents $e_1, \cdots, e_t \in \mathbb{Z}$ as small as possible. Indeed, *a priori* these exponents have order of magnitude $|\mathrm{Cl}(\mathcal{O}_n)| \simeq \ell^n$, making the action impossible to compute as it would require to apply the ladder computation of Paragraph 1.5.2 exponentially many times. For that reason, after expressing $[\mathfrak{N}]$ as a product, a reduction of the exponents modulo the relations lattice of the $[\mathfrak{q}_j]$ needs to be performed.

Expressing $[\mathfrak{N}]$ as a product of the $[\mathfrak{q}_j]$

The idea here is to compute a basis of $\mathrm{Cl}(\mathcal{O}_n)$ in terms of the $[\mathfrak{q}_j]$, (in the sense of Definition B.7) and to compute the discrete logarithm of $[\mathfrak{N}]$ in this basis (in the sense of Definition B.8). Actually, by the following lemma, the group basis will consist in one or two elements.

Lemma 3.8. *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.5. □

Since $|\mathrm{Cl}(\mathcal{O}_n)|$ is smooth (with a factor ℓ^{n-1} and all other prime factors $\leq \ell+1$), we get that discrete logarithms can be computed in polynomial time in n by Pohlig-Hellman methods. As a consequence, one can compute a basis of $|\mathrm{Cl}(\mathcal{O}_n)|$ in terms of the $[\mathfrak{q}_j]$ in time $O(tn^2)$ (by Lemma B.17) and the discrete logarithm of $[\mathfrak{N}]$ in such a basis can be computed in time $O(n^2)$ using Algorithm 7. This way, we obtain an expression of $[\mathfrak{N}]$ as $(\star)$ with big exponents e_j.

Reducing the exponents modulo the relations lattice of the $[\mathfrak{q}_j]$

We want to make the vector $e := (e_1, \cdots, e_t)$ as short as possible, which can be done by computing the closest vector c to e in the lattice:

$$L := \left\{ (f_1, \cdots, f_t) \in \mathbb{Z}^t \,\middle|\, \prod_{j=1}^{t} [\mathfrak{q}_j]^{f_j} = [1] \right\}.$$

Knowing a basis of $\mathrm{Cl}(\mathcal{O}_n)$ and an algorithm to efficiently compute discrete logarithms, a $\mathbb{Z}$-basis of this lattice could be computed in polynomial time in t and n (actually, in time $O(t^3 + tn^2)$) using Algorithm 9.

An approximation of the closest vector c is sufficient, because the search for such a vector may be very costly. There is a tradeoff between the norm of the vector $e' := e - c$ and the the cost of this approximation. Computing the action of $[\mathfrak{N}] = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_j}$ has time complexity:

$$\Theta\left(n \sum_{j=1} P(q_j, n) |e'_j| \right),$$

where P is a polynomial. Since:

$$\|e'\|_2 \leq \sum_{j=1} P(q_j, n)|e'_j| \leq \|e'\|_2 \sqrt{\sum_{j=1}^{t} P(q_j, n)^2},$$

the time complexity of the action of $[\mathfrak{N}]$ is $\|e'\|_2$, up to a polynomial factor in n, t and the q_j. Hence, we can optimize e' in ℓ_2 norm. There is a trade-off between the tightness of our approximation to optimize the performance of the action of $[\mathfrak{N}]$ and the time complexity of finding a close vector.

Theorem 3.9. *[29, Theorem 3.3] Let $\Lambda \subseteq \mathbb{Z}^d$ be a lattice of rank d, $B := (b_1, \cdots, b_d)$, a basis of Λ, a target $x \in \mathbb{R}^d$ and $k \in \mathbb{N}^*$ such that $d > 2k$. Under some heuristic assumptions, there exists an algorithm finding $c \in \Lambda$ such that:*

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

where GH is the Gaussian heuristic function given by:

$$GH(k) := \frac{\Gamma\left(\frac{k}{2} + 1\right)^{\frac{1}{k}}}{\sqrt{\pi}}.$$

This algorithm runs in time:

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

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 algorithm for CVP (with preprocessing) is due to [30] and runs in time $T_{CVP}(k) = 2^{c_1 k + o(k)}$ with $c_1 \approx 0.264$. The best known algorithm for SVP is due to [31] and runs in time $T_{SVP}(k) = \left(\frac{3}{2}\right)^{k/2 + o(k)} = 2^{c_2 k + o(k)}$ with $c_2 \approx 0.292$.

Corollary 3.10. *Applying the algorithm of Theorem 3.9, one can recover an ideal $\mathfrak{a} \subseteq \mathcal{O}_n$ which is a product of the $\mathfrak{q}_j$ with small exponents such that $(F_i)_{0 \leq i \leq n} = \mathfrak{a} \cdot (E_i)_{0 \leq i \leq n}$ in time:*

$$2^{c_2 k + o(k)} P(k, n, t, \max_{1 \leq j \leq t} q_j),$$

where P is a polynomial and $k \in [\![1\ ;\ \lceil t/2 \rceil - 1]\!]$, a parameter to be chosen. For this value of k, one can compute the action of $[\mathfrak{a}]$ on any chain in time:

$$GH(k)^{\frac{t}{2k}} \ell^{\frac{n}{t}} Q(n, t, \max_{1 \leq j \leq t} q_j),$$

where Q is a polynomial.

Proof. The corollary is a restatement of what we have seen before. We simply apply the algorithm of Theorem 3.9 to $\Lambda = L$ and get the desired complexity, since $\mathrm{Covol}(L) = h(\mathcal{O}_n)$. Indeed, since the $[\mathfrak{q}_j]$ generate $\mathrm{Cl}(\mathcal{O}_n)$, we have an exact sequence:

$$\{0\} \longrightarrow L \hookrightarrow \mathbb{Z}^t \xrightarrow{\varphi} \mathrm{Cl}(\mathcal{O}_n) \longrightarrow \{0\},$$

where $L \hookrightarrow \mathbb{Z}^t$ is the natural inclusion and $\varphi : (e_1, \cdots, e_t) \in \mathbb{Z}^t \longmapsto \prod_{j=1}^t [\mathfrak{q}_j]^{e_j} \in \mathrm{Cl}(\mathcal{O}_n)$. It follows that:

$$\mathrm{Covol}(L) = |\mathbb{Z}^t / L| = h(\mathcal{O}_n).$$

□

This attack is still subexponential, but much more damaging to the cryptosystem. To ensure a security level of $\lambda = 128$ bits, we need $t \geq 16064$, which is utterly unrealistic.

For smaller and more realistic parameters, like those Colò and Kohel proposed in [4, Section 6] ($t = 74$ for $n = 256$, $\ell = 2$ and $r = 5$), the closest vector approximation can be computed with polynomial algorithms such as Babai's nearest plane algorithm [32] running in $O(t^6)$ because the outputted exponents will have reasonable size.

3.2 A second attack using the class group action only

We recall here the problem we have to solve: given a chain $(E_i, \iota_i)_{0 \leq i \leq n}$ and a chain $(F_i, \iota'_i)_{0 \leq i \leq n} = \mathfrak{a} \cdot (E_i, \iota_i)_{0 \leq i \leq n}$ with a secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$, we want to recover $[\mathfrak{a}]$. We have seen that this could be done by recovering the structure of the endomorphism rings $\mathrm{End}(E_i)$ and $\mathrm{End}(F_i)$. However, this might not be necessary and we present here a simpler approach to this problem.

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 $\mathcal{O}_i$, so that $\mathfrak{a}_i$ is determined up to multiplication 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, $[\mathfrak{a}_{i+1} \cap \mathcal{O}_i] = [\mathfrak{a} \cap \mathcal{O}_i] = [\mathfrak{a}_i \cap \mathcal{O}_i]$ 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 determine an ideal $\mathfrak{b} = \prod_{j=1}^t \mathfrak{q}_j^{d_j}$ such that $\mathfrak{b} \cap \mathcal{O}_i$ is principal and:

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

Then, we can set $\mathfrak{a}_{i+1} := \mathfrak{a}_i \cdot \mathfrak{b}$, so that $e_{i+1,j} := e_{i,j} + d_j$ for all $j \in [\![1\ ;\ t]\!]$. Actually, $\mathfrak{a}_{i+1} \cap \mathcal{O}_{i+1}$ is determined modulo a principal ideal of $\mathcal{O}_{i+1}$ and $\mathfrak{b} \cap \mathcal{O}_{i+1}$ as well. As a consequence, $[\mathfrak{b} \cap \mathcal{O}_{i+1}]$ 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 cardinality 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 $i = 0$, so we only have to test a limited number of values for $\mathfrak{b}$ until $(\star)$ is satisfied.

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

3.2.1 Expressing $\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Cl}(\mathcal{O}_i))$ in terms of the $\mathfrak{q}_j$

By Lemma 3.8, we know that $\mathrm{Cl}(\mathcal{O}_n)$ is either cyclic or of the form $\mathrm{Cl}(\mathcal{O}_n) \simeq (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/h_{n-1}\mathbb{Z})$ with $h_{n-1} := |\mathrm{Cl}(\mathcal{O}_{n-1})|$.

We describe how to proceed when $\mathrm{Cl}(\mathcal{O}_n)$ is cyclic. If we assume that the $\mathfrak{q}_j$ generate $\mathrm{Cl}(\mathcal{O}_n)$, we can compute an $\mathcal{O}_K$-ideal $\mathfrak{g}$ such that $[\mathfrak{g} \cap \mathcal{O}_n]$ generates $\mathrm{Cl}(\mathcal{O}_n)$, as one of the $\mathfrak{q}_j$ or a as product of some $\mathfrak{q}_j$. By the surjection $\mathrm{Cl}(\mathcal{O}_{i+1}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Cl}(\mathcal{O}_i)$, we get that $[\mathfrak{g} \cap \mathcal{O}_i]$ generates $\mathrm{Cl}(\mathcal{O}_i)$ for all $i \in [\![0\ ;\ n-1]\!]$ and that:

$$\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Cl}(\mathcal{O}_i)) = \langle [\mathfrak{g} \cap \mathcal{O}_{i+1}]^{h_i} \rangle,$$

with $h_i := |\,\mathrm{Cl}(\mathcal{O}_i)|$.

Now, we assume that $\mathrm{Cl}(\mathcal{O}_n) \simeq (\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/h_{n-1}\mathbb{Z})$. In that case, as previously, we obtain easily an ideal $\mathfrak{g}$ expressed as one of the $\mathfrak{q}_j$ or as a product of some $\mathfrak{q}_j$ such that $[\mathfrak{g} \cap \mathcal{O}_n]$ has order h_{n-1}. We also obtain that $[\mathfrak{g} \cap \mathcal{O}_i]$ has order h_{i-1} for all $i \in [\![2\ ;\ n]\!]$ (for instance by Lemma A.14.(iv)). As previously, it follows that:

$$\ker(\mathrm{Cl}(\mathcal{O}_{i+1}) \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Cl}(\mathcal{O}_i)) = \langle [\mathfrak{g} \cap \mathcal{O}_{i+1}]^{h_{i-1}} \rangle$$

for all $i \in [\![2\ ;\ n-1]\!]$. For $i = 0, 1$, the kernel can be very easily computed because the class groups are small.

Either way, we can easily express every ideal $\mathfrak{b}$ such that $\mathfrak{b} \cap \mathcal{O}_{i+1}$ lies in the above kernel in terms of the $\mathfrak{q}_j$.

3.2.2 Reducing the exponents of $\mathfrak{a}_i \cdot \mathfrak{b}$

Once $\mathfrak{b}$ is expressed in terms of the $\mathfrak{q}_j$, *i.e.* when the d_j are known, we still have to make sure that the exponents $e_{i+1,j} = e_{i,j} + d_j$ of $\mathfrak{a}_i \cdot \mathfrak{b}$ are small. Actually, $e_{i+1} := (e_{i+1,j})_{1 \leq j \leq t}$ is determined up to translation by an element of the lattice:

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

Hence, we can apply the method of Paragraph 3.1.4 to find $f \in L_{i+1}$ relatively close to e_{i+1} and compute the action of $[\mathfrak{b} \cdot \mathfrak{a}_i] = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_{i+1,j}}$ with $e'_{i+1} := e_{i+1} - f$.

Using Algorithm 9, one can find a basis of L_{i+1} in time $O(t^3 + t(i+1)^2)$. Using Babai's nearest plane algorithm [32], one can find $f \in L_{i+1}$ close to e_{i+1} in time $O(t^6)$. Then, we can compute the action of $[\mathfrak{b} \cdot \mathfrak{a}_i] = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_{i+1,j}}$ with $e'_{i+1} := e_{i+1} - f$.

Theorem 3.11. *One can recover the secret ideal class $\mathfrak{a}$ in time:*

$$O\left(n^3 t^2 + n^4 + t^6 + n\ell T_{CL}\right),$$

where T_{CL} is the time complexity of the computation of the class group action on a given elliptic curve by the method of Paragraph 1.5.2 when exponents are outputted by Babai's nearest plane algorithm and where the O constant depends only on ℓ.

3.2.3 Implementation

We implemented the attack described above with `SageMath` [6]. The source code can be found in [13], more specifically in the files `OSIDH_protocol.py` and `OSIDH_attack.py`.

We tested our implementation with toy parameters: $n = 28$, $t = 10$, $\ell = 2$, $r = 3$ (and $K = \mathbb{Q}(i)$). These parameters have been chosen so that $(2r+1)^t \simeq h(\mathcal{O}_n) \simeq \ell^n$ to ensure the key space:

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

covers the whole class group $\mathrm{Cl}(\mathcal{O}_n)$.

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 $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$, our attack found $[\mathfrak{a}]$ in 90 s.[2] The drawback of our performance is not the attack itself but rather the class group action on the chains. Indeed, computing with modular polynomials is very costly. For that reason, the protocol runs very slowly: with our parameters, the naive Diffie Hellman key exchange runs in 37 s and the strong version of OSIDH runs in 83 s, which is almost the running time of the attack.

Testing the attack with realistic parameters like those Colò and Kohel proposed ($t = 74$ for $n = 256$, $\ell = 2$ and $r = 5$) would require us to manage modular polynomials much more efficiently of to find an alternative method to compute the class group action.

3.3 Onuki's attack

As we saw in Paragraph 3.1, the knowledge of the chains $(E_i, \iota_i)_{0\leq i\leq n}$ and $(E_{A,i}, \iota_{A,i})_{0\leq i\leq n} = \mathfrak{a}\cdot(E_i, \iota_i)_{0\leq i\leq n}$, gives away enough information to recover the secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$. We present an attack due to Onuki [12, § 6.3] recovering the chain of ℓ-isogenies $(\varphi_i : E_i \longrightarrow E_{i+1})_{0\leq i\leq n-1}$ given E_0 and E_n together with the chains:

$$\mathfrak{q}_j^{-r}\cdot E_n \longrightarrow \cdots \longrightarrow E_n \longrightarrow \cdots \longrightarrow \mathfrak{q}_j^{r}\cdot E_n$$

for all $j \in [\![1\ ;\ n]\!]$. There is a variant of this attack based on the shortest vector problem (SVP) in a lattice of dimension t (see Paragraph 3.4).

Assume that the attacker knows an endomorphism $\iota_n(\beta)$ for a known value $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ that we write $\beta := a + b\ell^n\theta$, where θ is a generator of $\mathcal{O}_K$ and $a, b \in \mathbb{Z}$, with $b \wedge \ell = 1$. Since $\iota_n(a) = [a]$ is easy to compute, we can assume that $a = 0$ *i.e.* that $\beta = b\ell^n\theta$. We assume that $\iota_n(\beta)$ can be efficiently evaluated on ℓ-torsion points. Then the attacker can compute the subgroup $G := \ker(\iota_n(\beta)) \cap E_n[\ell]$ in polynomial time in $\log(p)$.

Lemma 3.12. $G = \ker(\widehat{\varphi}_{n-1})$.

Proof. We have:

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

and $b\ell^{n-1}\theta \in \mathcal{O}_{n-1}$, so that $\iota_{n-1}(b\ell^{n-1}\theta) \in \mathrm{End}(E_{n-1})$, and consequently, $\ker(\widehat{\varphi}_{n-1}) \subseteq \ker(\iota_n(\beta))$. Since $\deg(\varphi_{n-1}) = \ell$, we have also $\ker(\widehat{\varphi}_{n-1}) \subseteq E_n[\ell]$ 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 whole ℓ-torsion subgroup $E_n[\ell]$. If the latter holds, $\iota_n(\beta)$ factors through $[\ell]$ by [15, Corollary III.4.11] and $\beta/\ell = b\ell^{n-1}\theta \in \mathcal{O}_n$, so $\ell | b$. Contradiction. Hence, $G = \ker(\widehat{\varphi}_{n-1})$. □

[2] The running times provided here were extracted from a single test so they are subject to some statistical variation. However, all other tests performed were consistent with these results. Obviously, the reproducibility of these results depend on the machine used to run the tests. Here, we used a MacBook Pro Retina 2015 with a 2.5 GHz quad-core processor and 16 GB RAM.

Hence, we can compute $\widehat{\varphi}_{n-1}$ using Vélu's formulas in $O(\ell)$ operations over the field of definition of $E_n[\ell]$. With this information, we can recover φ_{n-1} easily, by evaluating $\widehat{\varphi}_{n-1}$ on $E_{n-1}[\ell]$, since $\ker(\varphi_{n-1}) = \widehat{\varphi}_{n-1}(E_{n-1}[\ell])$, and using Vélu's formulas again.

With the knowledge of $\widehat{\varphi}_{n-1} : E_n \longrightarrow E_{n-1}$, along with the horizontal chain:

$$[\mathfrak{q}_j]^{-r} \cdot E_n \longrightarrow \cdots \longrightarrow E_n \longrightarrow \cdots \longrightarrow [\mathfrak{q}_j]^{r} \cdot E_n$$

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

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

for all $j \in [\![1 \ ; \ t]\!]$, by the methods of Paragraph 1.5.2.

We conclude that the attacker can compute the chain of isogenies $(\varphi_i : E_i \longrightarrow E_{i+1})_{0 \leq i \leq n-1}$, if at each index $i \in [\![1 \ ; \ n]\!]$, if they have access to an oracle providing $\iota_i(\beta_i)$ for $\beta_i \in \mathcal{O}_i \setminus \mathcal{O}_{i+1}$, when E_i is given. Now, we present such an oracle (for E_n), due to Onuki. An alternate oracle relying on SVP will be presented in Paragraph 3.4.

First, we look for $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ such that $\beta\mathcal{O}_n = \mathfrak{a} \cdot \mathfrak{b}$, with a big factor $\mathfrak{a} := \prod_{j=1}^{t} \mathfrak{q}_j^{e_j}$ whose exponents $e_1, \cdots, e_t$ lye in $[\![-r \ ; \ r]\!]$ and $\mathfrak{b} \subseteq \mathcal{O}_n$, any ideal. In practice, we test different values of $\beta := a + b\theta$ 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 when $N(\beta)$ has a big enough divisor $Q := \prod_{j=1}^{t} q_j^{e_j}$ with $e_1, \cdots, e_t \in [\![-r \ ; \ r]\!]$, let's say $Q \geq x$, where the threshold x is to be chosen. Then, we compute the $\mathfrak{q}_j$-adic valuation of β for all $j \in [\![1 \ ; \ t]\!]$ (using [33, Algorithm 2.3.13] for instance) to express the ideal $\mathfrak{a}$.

With the knowledge of the chain:

$$[\mathfrak{q}_j]^{-r} \cdot E_n \longrightarrow \cdots \longrightarrow E_n \longrightarrow \cdots \longrightarrow [\mathfrak{q}_j]^{r} \cdot E_n$$

for all $j \in [\![1 \ ; \ r]\!]$, using the techniques of Paragraph 2.2, it is easy to compute the isogeny $\varphi_{\mathfrak{a}} : E_n \longrightarrow [\mathfrak{a}] \cdot E_n$ of kernel $E_n[\mathfrak{a}]$.

It remains to compute the isogeny $\varphi_{\mathfrak{b}} : [\mathfrak{a}] \cdot E_n \longrightarrow [\mathfrak{a} \cdot \mathfrak{b}] \cdot E_n = E_n$ of kernel $[\mathfrak{a}] \cdot E_n[\mathfrak{b}]$. We know that $\deg(\varphi_{\mathfrak{b}}) = N(\mathfrak{b}) = N(\beta)/N(\mathfrak{a})$, so we can compute $\deg(\varphi_{\mathfrak{b}})$ and factor it into primes:

$$\deg(\varphi_{\mathfrak{b}}) = \prod_{k=1}^{s} \ell_k^{f_k}$$

with $\ell_1, \cdots, \ell_s$ distinct prime numbers and $f_1, \cdots, f_s \in \mathbb{N}^*$ using general number field Seive in subexponential time:

$$\exp\left(O\left(\log(N(\mathfrak{b}))^{\frac{1}{3}} \log\log(N(\mathfrak{b}))^{\frac{2}{3}}\right)\right)$$

and use a meet-in-the-middle technique to recover $\varphi_{\mathfrak{b}}$ as follows. We divide our search in two approximately equal parts, by exhaustive search among isogenies $\phi_1 : [\mathfrak{a}] \cdot E_n \longrightarrow E$ of degree $\deg(\phi_1) = \prod_{k=1}^{s} \ell_k^{g_k}$ and and $\phi_2 : E_n \longrightarrow E'$ of degree $\deg(\phi_2) = \prod_{k=1}^{s} \ell_k^{h_k}$, where the exponents are chosen, so that $h_k + g_k = f_k$ for all $k \in [\![1 \ ; \ s]\!]$ and $\deg(\phi_1) \simeq \deg(\phi_2) \simeq \sqrt{\deg(\varphi_{\mathfrak{b}})}$. We stop our exhaustive search when we find a collision $E = E'$ and return $\varphi_{\mathfrak{b}} = \widehat{\phi}_2 \circ \phi_1$. ϕ_1 (respectively ϕ_2) is represented as chains of g_k (respectively g_k) ℓ_k-isogenies for $k \in [\![1 \ ; \ s]\!]$. Hence, there are $\prod_{k=1}^{s}(\ell_k + 1)^{g_k}$ (respectively $\prod_{k=1}^{s}(\ell_k + 1)^{h_k}$) possible isogenies (counting the number of possible kernels of each isogeny of the chain). Hence, the exhaustive search has complexity:

$$\Omega\left(\prod_{k=1}^{s}(\ell_k + 1)^{g_k} + \prod_{k=1}^{s}(\ell_k + 1)^{h_k}\right) = \Omega(\sqrt{\deg(\varphi_{\mathfrak{b}})}) = \Omega\left(\sqrt{\frac{N(\beta)}{\prod_{j=1}^{t} q_j^{e_j}}}\right).$$

Remark 3.13. Note that we have no theoretical guarantee that we actually find the isogeny $\varphi_{\mathfrak{b}}$:

$[\mathfrak{a}] \cdot E_n \longrightarrow E_n$ with this method. Make sure of it would require knowledge of the K-orientation of the domain or codomain, which are hidden.

Here, we estimate the time complexity of Onuki's attack in order to provide sharper security bounds. Indeed, Onuki's estimates were very pessimistic.

Lemma 3.14. *We make the heuristic assumption that $N(\beta)$ has the same arithmetic properties as a uniform variable in $[\![N_{min}\ ;\ N_{max}]\!]$ when $\beta := a + b\theta$ with (a, b) sampled uniformly in $[\![-m\ ;\ m]\!] \times [\![-m\ ;\ m]\!] \setminus \ell\mathbb{Z}$. Then, the average time complexity of Onuki's attack [12, § 6.3] is:*

$$C(x) \geq \frac{x}{2(r+1)^t} + \frac{\kappa N_{min}^{\frac{3}{2}}}{x^{\frac{3}{2}}(r+1)^t},$$

where $\kappa := \frac{1}{4\sqrt{q_1}}\left(1 - \frac{1}{q_1}\right)$ and x is the threshold for the value of the norm of the ideal $\mathfrak{a} = \prod_{j=1}^t \mathfrak{q}_j^{e_j}$ dividing β. The optimal value for the threshold is $x_m := (3\kappa)^{\frac{2}{5}} N_{min}^{\frac{3}{5}} (r+1)^{-\frac{2t}{5}}$ and the optimal average time complexity is:

$$C(x_m) = \Omega\left(\frac{N_{min}^{\frac{3}{5}}}{(r+1)^{\frac{2t}{5}}}\right).$$

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:

$$\begin{aligned} |S(x)| &\leq \sum_{\substack{(e_1,\cdots,e_t) \in [\![0\ ;\ r]\!]^t \\ x \leq \prod_{j=1}^t q_j^{e_j} \leq N_{max}}} \left(\left\lfloor \frac{N_{max}}{\prod_{j=1}^t q_j^{e_j}} \right\rfloor - \left\lceil \frac{N_{min}}{\prod_{j=1}^t q_j^{e_j}} \right\rceil \right) \\ &\leq \sum_{\substack{(e_1,\cdots,e_t) \in [\![0\ ;\ r]\!]^t \\ x \leq \prod_{j=1}^t q_j^{e_j} \leq N_{max}}} \left(\frac{N_{max} - N_{min}}{\prod_{j=1}^t q_j^{e_j}} + 1 \right) \\ &\leq \left(\frac{N_{max} - N_{min}}{x} + 1 \right) |\{(e_1, \cdots, e_t) \in [\![0\ ;\ r]\!]^t \mid x \leq \prod_{j=1}^t q_j^{e_j} \leq N_{max}\}| \\ &\leq \left(\frac{N_{max} - N_{min}}{x} + 1 \right) (r+1)^t \leq 2(N_{max} - N_{min}) \frac{(r+1)^t}{x} \quad (1) \end{aligned}$$

under the fairly reasonable assumption that $x \leq N_{max} - N_{min}$ (this is plausible since $x \leq N_{max}$ and

$N_{max} \simeq m^2 N_{min}$ with $m \gg 1$). It follows that the search for β costs:

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

The average cost of the meet-in-the-middle procedure to find the isogeny associated to $\mathfrak{b}$ is:

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

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

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

with:

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

We take $A := N_{max}/(q_1 x)$, 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:

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

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

$$|T(A)| \geq \left\lfloor \frac{N_{max}}{x} \right\rfloor - \left\lceil \frac{N_{max}}{q_1 x} \right\rceil \geq \frac{N_{max}}{x} - \frac{N_{max}}{q_1 x} - 1 \geq \frac{N_{max}}{2x}\left(1 - \frac{1}{q_1}\right),$$

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

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

But we know that $x \leq N_{max} - N_{min}$. It follows that:

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

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

$$C(x) \geq C_1(x) + C_2(x) \geq \frac{x}{2(r+1)^t} + \frac{\kappa N_{min}^{\frac{3}{2}}}{x^{\frac{3}{2}}(r+1)^t},$$

with $\kappa := \frac{1}{4\sqrt{q_1}}\left(1 - \frac{1}{q_1}\right)$. The optimal value for x is obtained by differenciating of the function defined over $\mathbb{R}_+^*$: $x \longmapsto \frac{x}{2(r+1)^t} + \frac{\kappa N_{min}^{\frac{3}{2}}}{x^{\frac{3}{2}}(r+1)^t}$. □

Since, we have $N_{min} = \Omega(\ell^{2n})$, to ensure a level of security of λ bits, one has to choose the parameters so that:

$$\frac{\ell^{\frac{6n}{5}}}{(r+1)^{\frac{2t}{5}}} \geq 2^{\lambda},$$

i.e. :

$$n \geq \frac{5\log(2)}{6\log(\ell)}\lambda + \frac{t}{3}\log(r+1).$$

Example 3.15. For $\lambda = 128$ bits, $\ell = 2$, $r = 3$ and $t = 100$ (parameters proposed by Onuki), we get

$n \geq 153$. This is much less than the first estimate of Onuki (see [12, § 6.3]) for the same parameters ($n = 1428$) and even less than Colò and Kohel's choice in [4, Section 6] ($n = 256$).

However, this attack can be dramatically improved if we replace the exhaustive search of endomorphisms by a reduction of the relations lattice. This will lead to a significant revision of the security parameters.

3.4 A variant of Onuki's attack based on lattice reduction

This is a variant of Onuki's attack : given E_0 and E_n and the horizontal chains:

$$\mathfrak{q}_j^{-r} \cdot E_n \longrightarrow \cdots \longrightarrow E_n \longrightarrow \cdots \longrightarrow \mathfrak{q}_j^{r} \cdot E_n \quad (j \in [\![1 \ ; \ t]\!]),$$

we recover the whole chain $(E_i, \iota_i)_{0 \leq i \leq n}$ with an oracle returning an endomorphism $\iota_i(\beta_i)$ with $\beta_i \in \mathcal{O}_i \setminus \mathcal{O}_{i+1}$ when given E_i for $i \in [\![1 \ ; \ n]\!]$. However, the oracle is different here. Instead of searching for $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ (for $i = n$) with smoothness conditions on its norm coupled with a meet-in-the-middle attack, we directly look for $\beta \in \mathcal{O}_n \setminus \mathcal{O}_{n+1}$ as a product of the $\mathfrak{q}_j$ with exponents in $[\![-2r \ ; \ 2r]\!]$ by solving the equation:

$$\prod_{j=1}^{t} [\mathfrak{q}_j]^{e_j} = [1]$$

in $\mathrm{Cl}(\mathcal{O}_n)$, with $e_1, \cdots, e_t \in [\![-2r \ ; \ 2r]\!]$ non-trivial. Then, we write $e_j := e'_j + e''_j$ with $e'_j, e''_j \in [\![-r \ ; \ r]\!]$ for all $j \in [\![1 \ ; \ t]\!]$ and compute the isogenies:

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

and finally compute $\iota_n(\beta) = \hat{\psi} \circ \varphi$ with with $\beta \mathcal{O}_K = \prod_{j=1}^{t} \mathfrak{q}_j^{e_j}$.

As we saw in Paragraph 3.1.4, we can find a basis of the lattice:

$$L := \left\{ (e_1, \cdots, e_t) \in \mathbb{Z}^t \,\middle|\, \prod_{j=1}^{t} [\mathfrak{q}_j]^{e_j} = [1] \right\}$$

in polynomial time in n and t. Our problem reduces to finding a short vector in L for the norm ℓ_∞, hoping that this vector has norm $\leq 2r$ to make sure that we can compute $\iota_n(\beta)$ by the method presented above. Hence, an estimation of the infinity norm of the shortest vector in L is necessary.

3.4.1 Estimating the first minimum of L in infinity norm

We want to estimate, at least statistically the first minimum of L for the norm ℓ_∞, depending on the parameters:

$$\lambda_1^{(\infty)}(L) := \min_{v \in L \setminus \{0\}} \|v\|_\infty.$$

We provide a first estimate here:

Lemma 3.16. *We have* $\lambda_1^{(\infty)}(L) \leq h(\mathcal{O}_n)^{\frac{1}{t}}$.

Proof. As in Corollary 3.10, we get that $\mathrm{Covol}(L) \leq h(\mathcal{O}_n)$.

The conclusion follows from the classical result $\lambda_1^{(\infty)}(L) \leq \mathrm{Covol}(L)^{\frac{1}{t}}$, which is a corollary of Minkowski's convex body Theorem [18, Theorem V.3]. We recall its proof here. We consider the ball for ℓ_∞ norm:

$$B_\infty(0, r) := \{v \in \mathbb{R}^t \mid \|v\|_\infty \leq r\},$$

where $r := \mathrm{Covol}(L)^{\frac{1}{t}}$, whose volume is $2^t \mathrm{Covol}(L)$ and which is centrally-symmetric. Then, by Minkowski's convex body theorem, we have a non-zero lattice point in $B_\infty(0,r)$, so that $\lambda_1^{(\infty)}(L) \leq r = \mathrm{Covol}(L)^{\frac{1}{t}}$. This completes the proof. □

Remark 3.17. Since $h(\mathcal{O}_n) = \frac{\ell^{n-1}}{[\mathcal{O}_K^\times : \mathcal{O}_n^\times]} \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right) \simeq \ell^n$ by [19, Theorem 7.24], we conclude that $\lambda_1^{(\infty)}(L) = O(\ell^{\frac{n}{t}})$. Hence, we have to make sure that $2r < \ell^{\frac{n}{t}}$ to have a chance that $2r < \lambda_1^{(\infty)}(L)$. Of course, n has to be sufficiently larger than t to make this inequality possible.

However, we do not know how thight the estimate $\lambda_1^{(\infty)}(L) \leq h(\mathcal{O}_n)^{\frac{1}{t}}$ is, and therefore if the choice of parameters $2r < O(\ell^{\frac{n}{t}})$ is sufficient. Assuming that the $[\mathfrak{q}_j]$ generate $\mathrm{Cl}(\mathcal{O}_n)$, we have $\mathrm{Covol}(L) = h(\mathcal{O}_n)^{\frac{1}{t}}$, and $\mathrm{Covol}(L)$ is close to this bound if the $[\mathfrak{q}_j]$ generate a big enough subgroup. Heuristically, it makes sense to assume that $\lambda_1^{(\infty)}(L)$ is relatively close to $\mathrm{Covol}(L)^{\frac{1}{t}}$ in general, namely that $\lambda_1^{(\infty)}(L) = \Theta(\mathrm{Covol}(L)^{\frac{1}{t}})$, as the following asymptotical result indicates.

Let $N, n \in \mathbb{N}^*$ and $\mathcal{I}_{N,n}$ be the set of full-rank sublattices of $\mathbb{Z}^n$ of covolume N.

Lemma 3.18. **(i)** *$\mathcal{I}_{N,n}$ is finite.*

(ii) *Let Λ be a random variable following the uniform distribution on $\mathcal{I}_{N,n}$. Then, for all $\varepsilon > 0$, there exists $n_0, N_0 \in \mathbb{N}^*$ such that for all $n \geq n_0$ and $N \geq N_0$:*

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

Proof. **(i)** Since a lattice of $\mathcal{I}_{N,n}$ is determined by an integral basis of determinant $\pm N$, up to multiplication on the right by a matrix of $SL_n(\mathbb{Z})$, we get that $\mathcal{I}_{N,n}$ is in bijection with the quotient of:

$$S_N := \{M \in M_n(\mathbb{Z}) \mid \det(M) = \pm N\}$$

by the group action of $SL_n(\mathbb{Z})$ by multiplication on the right. We prove that this quotient $S_N/SL_n(\mathbb{Z})$ is finite. Taking the column echelon reduced matrix, we get that modulo $SL_n(\mathbb{Z})$ every $M \in S_N$ is in the class of a HNF matrix:

$$\begin{pmatrix} d_1 & a_{1,2} & \cdots & a_{1,n} \\ 0 & d_2 & \cdots & a_{2,n} \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{pmatrix},$$

with $d_1, \cdots, d_n \in \mathbb{N}^*$ such that $\prod_{i=1}^n d_i = N$ and $a_{i,i+1}, \cdots, a_{i,n} \in [\![0\ ;\ d_i - 1]\!]$ for all $i \in [\![1\ ;\ n]\!]$. There are only finitely many such matrices. (i) follows.

(ii) This result has already been proved in [34, Theorem 11] for the norm ℓ_2. The reasoning would be exactly the same here. We only have to replace the function $h(n) = \frac{1}{\mathrm{Vol}(B_2(0,1))^{\frac{1}{n}}}$ by the constant $\frac{1}{\mathrm{Vol}(B_\infty(0,1))^{\frac{1}{n}}} = \frac{1}{2}$ in the inequality. □

Remark 3.19. As always,we assume that $\mathrm{Cl}(\mathcal{O}_n)$ is generated by the $[\mathfrak{q}_j]$. Assuming that L behaves like a random lattice with uniform distribution in $\mathcal{I}_{h(\mathcal{O}_n),t}$, we get that:

$$\lambda_1^{(\infty)}(L) \leq \left(1 + \frac{\log\log(t)}{t}\right)\frac{h(\mathcal{O}_n)^{\frac{1}{t}}}{2}.$$

To ensure that the key space covers $\mathrm{Cl}(\mathcal{O}_n)$, we require the surjectivity of the map:

$$f : (e_1, \cdots, e_t) \in [\![-r\ ;\ r]\!]^t \longmapsto \prod_{j=1}^t [\mathfrak{q}_j]^{e_j} \in \mathrm{Cl}(\mathcal{O}_n).$$

It follows that $h(\mathcal{O}_n) \leq (2r+1)^t$, so that:

$$2r \geq h(\mathcal{O}_n)^{\frac{1}{t}} - 1 > \left(1 + \frac{\log\log(t)}{t}\right) \frac{h(\mathcal{O}_n)^{\frac{1}{t}}}{2} \geq \lambda_1^{(\infty)}(L)$$

for $h(\mathcal{O}_n)$ big enough, so the SVP attack is possible.

Example 3.20. For instance, with the parameters of [4, p. 28]: $\ell = 2$, $r = 5$, $t = 74$ and $n = 256$, we get the upper bound for $\lambda_1^{(\infty)}(L)$ is:

$$\left(1 + \frac{\log\log(t)}{t}\right) \frac{\ell^{\frac{n}{t}}}{2} \approx 5.61,$$

so that $\lambda_1^{(\infty)}(L) \leq 5 < 2r = 10$ and the attack is indeed possible.

3.4.2 Countermeasures to our attack

There are two ways of countering our attack:

1. Increase t sufficiently to ensure that finding a short vector $e \in L$ such that $\|e\|_\infty \leq 2r$ is computationally very hard.
2. Make any SVP attack impossible by choosing our parameters so that $\lambda_1^{(\infty)}(L) > 2r$.

The safest way to find a vector $e \in L$ such that $\|e\|_\infty \leq 2r$ is the SVP algorithm in infinity norm due to [35], whose space and time complexities are $2^{0.62t+o(t)}$ and $2^{0.415t+o(t)}$ respectively. Hence, to ensure 128 bits of security, choosing $t \geq 207$ would be enough. However, in practice, algorithms with much less time complexity like BKZ [36] provide vectors far shorter than their theoretical bounds (see Paragraph 3.4.3). Considering the fact that SVP algorithms in infinity norm could always be improved, this makes the first method risky. Besides, relying on lattice based problem to ensure the security of OSIDH would damage its relevance as an isogeny based cryptosystem, since one of the main arguments in favor of isogeny based cryptography is diversity, meaning introducing primitives based on distinct computational problems and assumptions that of lattice based primitives prevailing in the NIST competition.

The second method is much safer but it has a strong drawback. As explained in Remark 3.19, if the key space covers $\mathrm{Cl}(\mathcal{O}_n)$, then OSIDH is vulnerable to our attack. Hence, we need to restrict the key space to ensure $\lambda_1^{(\infty)}(L) > 2r$. By making that choice, we dramatically reduce the relevance of OSIDH for other cryptographic constructions beyond Diffie-Hellman key exchange because we no longer have a restricted effective group action (see Appendix C).

Besides, our attack can still be performed when $\lambda_1^{(\infty)}(L) > 2r$. Indeed, let us assume that we found a short vector $e \in L$ with norm $\|e\|_\infty > 2r$. Then, we may write $e := e' + e'' + d$ with $e', e'', d \in \mathbb{Z}^t$ such that $\|e'\|_\infty = \|e''\|_\infty = r$ and d has infinity norm as small as possible. As previously, we can compute the isogenies:

$$\varphi : E_n \longrightarrow E' := \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_j} \cdot E_n \qquad \text{and} \qquad \psi : E_n \longrightarrow E'' := \prod_{j=1}^{t} [\mathfrak{q}_j]^{-e''_j} \cdot E_n = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e'_j + d_j} \cdot E_n.$$

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

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

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 a K-oriented endomorphism. However, likewise,we can estimate the complexity of this attack.

Proposition 3.21. *Under the heuristic assumption that L behaves like a random lattice among lattices of covolume $h(\mathcal{O}_n)$ and that the shortest vector of L 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 shortest 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 exhaustive search and its time complexity is (up to polynomial factors):

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

By assumption d' and d'' cut d in half and $e = e' + e'' + d$, so that:

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

and $\|d\|_\infty \geq \|e\|_\infty - 2r \geq \lambda_1^{(\infty)}(L) - 2r$. But by 3.18, we have:

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

The result follows. □

Example 3.22. For the parameters chosen by Colò and Kohel in [4, Section 6] ($\ell = 2$, $t = 74$, $r = 5$ and $K = \mathbb{Q}(i)$), the smallest value possible for q_1 (as a splitting prime $\neq \ell$) is $q_1 = 5$. To ensure a security level of $\lambda = 128$ bits, we need to take n such that:

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

It follows that $n \geq 575$. The value $n = 256$ was initially proposed, and the parameters were chosen so that the key space just covers $\mathrm{Cl}(\mathcal{O}_n)$. (with few or no redundancies). With $n \geq 575$, the key space is way smaller than $\mathrm{Cl}(\mathcal{O}_n)$.

3.4.3 Implementation

This attack was implemented in `SageMath` [6], partly with realistic parameters and completely (end-to-end) with toy parameters. The source code is available on Github [13], more specifically:

- in the files `Group_basis.py`, `Relations_lattice.py` and `Find_SVP.py` for the partial attack with realistic parameters;
- in the files `OSIDH_attack.py` and `OSIDH_attack_tests.py` for the end-to-end attack with toy parameters.

With the parameters of [4, p. 28]: $\ell = 2$, $r = 5$, $t = 74$ and $n = 256$ $K = \mathbb{Q}(i)$, and $q_1, \cdots, q_t$ the t smallest splitting primes in $\mathcal{O}_K$ the relation lattice L was computed in 2 h 31 using `SageMath` [6], including 1 h 28 for the group basis computation with Algorithm 8 and 1 h 03 for the relations lattice per se with 9. Have we known before performing the test that $\mathrm{Cl}(\mathcal{O}_n)$ was cyclic and generated by $[\mathfrak{q}_1]$,

the group basis computation could have been dramatically accelerated. The BKZ algorithm [36] was applied to L using the `fpylll` library [37] with a block size $k = 4$ to find a vector $e \in L$ of infinity norm $\|e\|_\infty = 9 < 2r$ in less that 0.5 s, proving that our lattice based attack could be very efficient in practice with large parameters.

With toy parameters ($n = 28$, $t = 10$,$\ell = 2$, $r = 3$ and $K = \mathbb{Q}(i)$), we performed an end-to-end attack on a protocol execution between two parties Alice and Bob. This attack included:

1. Our lattice based chain recovery of both Alice's and Bob's chains.
2. A recovery of Alice's ideal class using the implementation presented in Paragraph 3.2.3.
3. The shared secret chain computation by acting with Alice's ideal class on Bob's chain.

Step 1 ran in 288.6 s (144.3 s per chain), step 2 ran in 90 s and step 3 ran in 6.4 s for a total execution time of 385 s. In comparison, the protocol ran in 83.1 s.

As explained in Paragraph 3.2.3, the main limiting factor to test our attack with real parameters is the ideal class group action. Roughly speaking, our implementation of the protocol is "as slow as the attack".

3.5 Kuperberg's attack

OSIDH is broken whenever the attacker is able to recover the secret ideal class $[\mathfrak{a}] \in \mathrm{Cl}(\mathcal{O}_n)$, given the public chain $(E_i, \iota_i)_{0 \leq i \leq n}$ and the public data of Alice, namely the t horizontal chains:

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

for all $j \in [\![1 \ ; \ t]\!]$ (with $(E_{i,A}, \iota'_i)_{0 \leq i \leq n} := [\mathfrak{a}] \cdot (E_i, \iota_i)_{0 \leq i \leq n}$). We consider the functions:

$$f : [\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O}_n) \longmapsto [\mathfrak{c}] \cdot E_n \qquad \text{and} \qquad g : [\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O}_n) \longmapsto [\mathfrak{c}] \cdot E_{A,n}.$$

We know that f and g are injective and that $g([\mathfrak{c}]) = f([\mathfrak{a}][\mathfrak{c}])$ for all $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O}_n)$. Hence, our attack reduces to the Hidden Shift Problem.

Problem 3.23 (Hidden Shift Problem (HSP))**.** Given $f, g : G \longrightarrow S$ two injective functions such that there exists $s \in G$ such that $g(x) = f(sx)$ for all $x \in G$, the problem is to determine s.

Theorem 3.24 (Kuperberg)**.** *We keep the notations of Problem 3.23. Given an oracle computing f and g, there exists a quantum algorithm finding s with $2^{O(\sqrt{\log_2(|G|)})}$ qubits and quantum queries.*

Proof. See Appendix B.6. □

Remark 3.25. Actually, we know how to evaluate f and g on products of powers of the prime ideals $[\mathfrak{q}_j]$ but not on the whole group $\mathrm{Cl}(\mathcal{O}_n)$ a priori. This could be an obstacle to Kuberberg's algorithm because we need an oracle computing these functions for any group element. Assuming those ideal classes $[\mathfrak{q}_j]$ generate $\mathrm{Cl}(\mathcal{O}_n)$, these oracles can be computed provided that we can easily express any ideal class $[\mathfrak{c}] \in \mathrm{Cl}(\mathcal{O}_n)$ as a product of the $[\mathfrak{q}_j]$: $[\mathfrak{q}_j] = \prod_{j=1}^{t} [\mathfrak{q}_j]^{e_j}$, with small exponents e_j, and the additional restriction $e_j \in [\![-r \ ; \ r]\!]$ for all $j \in [\![1 \ ; \ t]\!]$ to compute g. This can be done relatively efficiently with a basis computation of $\mathrm{Cl}(\mathcal{O}_n)$, a discrete logarithm computation and Babai's algorithm with respect to the relations lattice, as explained earlier.

However, the condition $|e_j| \leq r$ might be an issue if the parameters are chosen so that $(2r+1)^t \ll |\mathrm{Cl}(\mathcal{O}_n)|$. Hence, we can avoid both our lattice based classical attack and Kuperberg's attack with this choice of parameters.

Bibliography

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

[2] Jean-Marc Couveignes. Hard homogeneous spaces. Cryptology ePrint Archive, Report 2006/291, 2006. `https://eprint.iacr.org/2006/291`.

[3] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies post-quantum cryptography. volume 2011, pages 19–34, 11 2011.

[4] Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. Cryptology ePrint Archive, Report 2020/985, 2020. `https://eprint.iacr.org/2020/985`.

[5] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. Cryptology ePrint Archive, Report 2018/383, 2018. `https://eprint.iacr.org/2018/383`.

[6] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*, 2021. `https://www.sagemath.org`.

[7] David Jao, Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev, David Urbanik, Geovandro Pereira, Koray Karabina, and Aaron Hutchinson. SIKE. Technical report, National Institute of Standards and Technology, 2020. available at `https://csrc.nist.gov/projects/post-quantum-cryptography/round-3-submissions`.

[8] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing.

[9] Alexander Rostovtsev and Anton Stolbunov. Public-Key Cryptosystem Based On Isogenies. Cryptology ePrint Archive, Report 2006/145, 2006. `https://eprint.iacr.org/2006/145`.

[10] Navid Alamati, Luca De Feo, Hart Montgomery, and Sikhar Patranabis. Cryptographic group actions and applications. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 411–439, Cham, 2020. Springer International Publishing.

[11] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-rendus de l'Académie des Sciences*, 273:238–241, july 1971. Available at `https://gallica.bnf.fr`.

[12] Hiroshi Onuki. On oriented supersingular elliptic curves, 2020. `https://arxiv.org/abs/2002.09894`.

[13] P. Dartois. Osidh. `https://github.com/Pierrick-Dartois/OSIDH`, 2021.

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

[15] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[16] J. H. Silverman. *Advanced Topics in The Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[17] Serge Lang. *Elliptic Functions*. Springer-Verlag, 1987.

[18] Serge Lang. *Algebraic Number Theory*. Springer-Verlag, 1994.

[19] David A. Cox. *Primes of the form $x^2 + ny^2$*. Wiley, 2013.

[20] William C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969. `http://eudml.org/doc/81852`.

[21] J. S. Milne. Complex multiplication, 2020. `https://www.jmilne.org/math/CourseNotes/cm.html`.

[22] David Kohel. Endomorphism rings of elliptic curves over finite fields, 1996. `http://iml.univ-mrs.fr/~kohel/pub/thesis.pdf`.

[23] A. Sutherland. Elliptic curves lecture notes, 2017. `https://dspace.mit.edu/bitstream/handle/1721.1/122962/18-783-spring-2017/contents/lecture-notes/index.htm`.

[24] J. Voight. Quaternion algebras. v.0.9.23, August 2020. `https://math.dartmouth.edu/~jvoight/quat.html`.

[25] A. Pizer. An algorithm for computing modular forms on $\gamma_0(n)$. *Journal of Algebra*, 64:340–340, 06 1980.

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

[27] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion ℓ-isogeny path problem, 2014.

[28] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, 1993.

[29] Thomas Espitau and Paul Kirchner. The nearest-colattice algorithm: Time-approximation tradeoff for approx-cvp. *Open Book Series*, 4:251–266, 12 2020.

[30] Léo Ducas, Thijs Laarhoven, and Wessel P.J. van Woerden. The randomized slicer for cvpp: sharper, faster, smaller, batchier. Cryptology ePrint Archive, Report 2020/120, 2020. `https://eprint.iacr.org/2020/120`.

[31] Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. pages 10–24, 01 2016.

[32] L. Babai. On lovász' lattice reduction and the nearest lattice point problem (shortened version). In *STACS*, 1985.

[33] H. Cohen. *Advanced Topics in Computational Algebraic Number Theory*. Springer-Verlag, 2000.

[34] Thomas Espitau Yoshinori Aono and Phong Q. Nguyen. Random lattices : theory and practice. `https://espitau.github.io/bin/random_lattice.pdf`.

[35] Divesh Aggarwal and Priyanka Mukhopadhyay. Improved algorithms for the shortest vector problem and the closest vector problem in the infinity norm, 2018.

[36] C. P. Schnorr. A hierarchy of polynomial time lattice basis reduction algorithms. *Theoretical Computer Science*, (53):201–224, 1987.

[37] The FPLLL development team. fpylll, a Python wraper for the fplll lattice reduction library, Version: 0.5.6. Available at `https://github.com/fplll/fpylll`, 2021.

[38] Gerald J. Janusz. *Algebraic Number Fields*. American Mathematical Society, Rhode Island, US, 1996.

[39] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer New York, New York, NY, 1982.

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

[41] L. E. Dickson. *Introduction to the theory of numbers*. The University of Chicago Press, 1951.

[42] B. Helfrich. Algorithms to construct minkowski reduced and hermite reduced lattice bases. *Theoretical Computer Science*, 41:125–139, 08 1985.

[43] B. L. Van der Waerden. Die reduktionstheorie der positiven quadratischen formen. *Acta Mathematica*, 96:265–309, 1956.

[44] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. Cryptology ePrint Archive, Report 2016/1154, 2016. `https://eprint.iacr.org/2016/1154`.

[45] Andrew V. Sutherland. Structure computation and discrete logarithms in finite abelian p-groups. *Mathematics of Computation*, 80(273):477–500, Apr 2010.

[46] Michael A. Nielsan and Isaac L. Chaung. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, UK, 10th anniversary edition edition, 2010.

[47] Dimitri Petritis. Quantum mechanics foundations and applications, January 2020. `https://perso.univ-rennes1.fr/dimitri.petritis/enseignement/mq/iq.pdf`.

[48] Ronald Cramer and Victor Shoup. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption. In Lars R. Knudsen, editor, *Advances in Cryptology — EUROCRYPT 2002*, pages 45–64, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg.

[49] Rosario Gennaro and Yehuda Lindell. A framework for password-based authenticated key exchange. In Eli Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, pages 524–543, Berlin, Heidelberg, 2003. Springer Berlin Heidelberg.

[50] Olivier Blazy, David Pointcheval, and Damien Vergnaud. Round-optimal privacy-preserving protocols with smooth projective hash functions. In Ronald Cramer, editor, *Theory of Cryptography*, pages 94–111, Berlin, Heidelberg, 2012. Springer Berlin Heidelberg.

[51] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. volume 37, pages 372– 381, 11 2004.

[52] Everett W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Mathematica*, 85(2):229–247, 1993.

Appendix A

Mathematical prerequisites and complements

A.1 $\mathfrak{p}$-adic integers

Let K be a number field and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ lying above a prime number p. We define the $\mathfrak{p}$-*adic valuation* on $\mathcal{O}_K$ as follows:

$$\forall x \in \mathcal{O}_K, \quad v_\mathfrak{p}(x) := \sup\{k \in \mathbb{N} \mid x \in \mathfrak{p}^k\} \in \mathbb{N} \cup \{+\infty\}.$$

This valuation can be easily extended to K by the formula $v_\mathfrak{p}(x/y) := v_\mathfrak{p}(x) - v_\mathfrak{p}(y)$ for all $x, y \in \mathcal{O}_K$ with $y \neq 0$. $v_\mathfrak{p}$ is indeed a valuation, meaning that for all $x, y \in K$:

(i) $v_\mathfrak{p}(x) = +\infty \iff x = 0$.

(ii) $v_\mathfrak{p}(xy) = v_\mathfrak{p}(x) + v_\mathfrak{p}(y)$.

(iii) $v_\mathfrak{p}(x + y) \geq \min(v_\mathfrak{p}(x), v_\mathfrak{p}(y))$.

This valuation extends the p-adic valuation on $\mathbb{Q}$ in the sense that $v_\mathfrak{p} = \frac{1}{e} v_p$ on $\mathbb{Q}$, where e is the ramification index of $\mathfrak{p}$ above p. Moreover, it can be proved that all elements of $\mathcal{O}_K$ have nonnegative $\mathfrak{p}$-adic valuations.

We can associate a norm to $v_\mathfrak{p}$ by setting $|x|_\mathfrak{p} := p^{-v_\mathfrak{p}(x)}$ for all $x \in K$. Unlike the complex module, this norm is non-archimedean (because of property (iii)). One can define the $\mathfrak{p}$-adic completion $K_\mathfrak{p}$ of K for this norm $|.|_\mathfrak{p}$, so that all Cauchy sequences converge. Formally, the completion is defined as the quotient of the ring of Cauchy sequences by the maximal ideal of sequences converging to zero. We can extend the valuation to $K_\mathfrak{p}$ by setting for all $x \in K_\mathfrak{p}$, $v_\mathfrak{p}(x) := \lim v_\mathfrak{p}(x_n)$, where $(x_n)_{n\in\mathbb{N}}$ is a Cauchy sequence representing x. It can be proved that $K_\mathfrak{p}$ is complete for the extended valuation (or equivalently, the extended norm) [38, Theorem II.2.1]. Of course, we also have an injection $K \hookrightarrow K_\mathfrak{p}$ and $K_\mathfrak{p}$ is unique for these properties.

Let:

$$\mathcal{O}_{K,\mathfrak{p}} := \{x \in K_\mathfrak{p} \mid v_\mathfrak{p}(x) \geq 0\}$$

be the ring of *integers* of $K_\mathfrak{p}$. It can be proved that $\mathcal{O}_{K,\mathfrak{p}}$ is integrally closed and has a unique maximal ideal:

$$\mathfrak{m}_\mathfrak{p} := \{x \in K_\mathfrak{p} \mid v_\mathfrak{p}(x) \geq 1\}.$$

This ideal is principal and a generator $\pi \in \mathfrak{m}_\mathfrak{p}$ is called a *uniformizer*. Hence $\mathcal{O}_{K,\mathfrak{p}}$ is a *discrete valuation ring*. Every element $x \in K_\mathfrak{p}$ can be uniquely written as $x = \pi^{v_\mathfrak{p}(x)} u$ with $u \in \mathcal{O}_{K,\mathfrak{p}}^\times$ (*i.e.* such that

$v_\mathfrak{p}(u) = 0$) and admits a unique series development:

$$x = \pi^{v_\mathfrak{p}(x)} \sum_{n=0}^{+\infty} a_n \pi^n,$$

where the a_n lye in a subset of $\mathcal{O}_K$ in bijection with $\mathcal{O}_K/\mathfrak{p}$ via the reduction modulo $\mathfrak{p}$ (see [38, Proposition II.2.8]). As a consequence, we obtain a natural ring isomorphism:

$$\mathcal{O}_{K,\mathfrak{p}}/\pi^n\mathcal{O}_{K,\mathfrak{p}} \xrightarrow{\sim} \mathcal{O}_K/\mathfrak{p}^n$$

for all $n \in \mathbb{N}^*$. In particular, the *residue field* $\mathcal{O}_{K,\mathfrak{p}}/\pi\mathcal{O}_{K,\mathfrak{p}}$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}$.

Theorem A.1 (Hensel's lemma)**.** *Let $F \in \mathcal{O}_{K,\mathfrak{p}}[X]$ and $\overline{F} \in \mathcal{O}_K/\mathfrak{p}[X]$ its reduction modulo $\mathfrak{m}_\mathfrak{p}$. Let $g, h \in \mathcal{O}_K/\mathfrak{p}[X]$ be two coprime polynomials such that $\overline{F} = g \cdot h$. Then, there exist $G, H \in \mathcal{O}_{K,\mathfrak{p}}[X]$ such that $F = G \cdot H$ and $G \equiv g \mod \mathfrak{m}_\mathfrak{p}$ and $G \equiv g \mod \mathfrak{m}_\mathfrak{p}$.*

Proof. See [38, Lemma II.3.5]. □

Corollary A.2. *Let $f \in \mathcal{O}_K/\mathfrak{p}[X]$ admitting a simple root $\alpha \in \mathcal{O}_K/\mathfrak{p}[X]$ and $F \in \mathcal{O}_{K,\mathfrak{p}}[X]$ such that $F \equiv f \mod \mathfrak{m}_\mathfrak{p}$. Then, there exists $\tilde{\alpha} \in \mathcal{O}_{K,\mathfrak{p}}$ such that $F(\tilde{\alpha}) = 0$ and $\tilde{\alpha} \equiv \alpha \mod \mathfrak{m}_\mathfrak{p}$.*

In particular, if f factors completely in $\mathcal{O}_K/\mathfrak{p}[X]$ with simple roots, then so does F in $\mathcal{O}_{K,\mathfrak{p}}[X]$ and the roots of F reduce to the roots of f modulo $\mathfrak{m}_\mathfrak{p}$.

A.2 Reduction of elliptic curves

Let R be a discrete valuation ring with unique prime ideal $\mathfrak{m}$, a uniformizer π and valuation v. Let L be its field of fractions and $k := R/\mathfrak{m}$ be the residue field and $p := \mathrm{char}(k)$. In practice, L will be a number field, R will be the localization of $\mathcal{O}_L$ at a place $\mathfrak{p}$ lying above p so that $\mathfrak{m} := \mathfrak{p}\mathcal{O}_{L,\mathfrak{p}}$ and π will be any element of $\mathfrak{m} \setminus \mathfrak{m}^2$. In this case, we shall talk by abuse, of reduction modulo $\mathfrak{p}$ instead of reduction modulo $\mathfrak{m}$.

Let E be an elliptic curve defined over L. We assume that $p \geq 5$ so that E admits a simplified Weierstrass equation $y^2 = x^3 + ax + b$ with $a, b \in L$. For all $u \in L^*$, we can substitute $x' := u^2x$ and $y' := u^3y$ so that are changed into: $a' := u^4a$ and $b' := u^6b$. With these substitutions, we can always assume that $a, b \in R$. We can even find a Weierstrass equation with $a, b \in R$ so that $v(\Delta(E))$ is minimal [15, Proposition VII.1.3.(a)].

Then we can reduce a minimal Weierstrass equation modulo $\mathfrak{m} = \pi R$ to obtain a curve $\overline{E}$ over k. If $\overline{E}$ is singular we say that E has *bad reduction* modulo $\mathfrak{m}$. Otherwise, $\overline{E}$ is an elliptic curve and we say that E has *good reduction* modulo $\mathfrak{m}$. It is clear that E has good reduction if and only if $v(\Delta(E)) = 0$ ($\Delta(E)$ being the minimal discriminant). If L is a number field, this case is not very frequent because $\mathcal{O}_L$ is a Dedekind domain so $\Delta(E)$ is the product of finitely many prime ideals so there are finitely many places with bad reduction.

However, we would like to avoid bad reduction in all cases. It would be possible if we had more freedom in the choice of u in the substitutions to get the minimal Weierstrass equation of E. This may be done if we take a finite field extension L'/L. In this case, we say that E has *potential good reduction.*

Proposition A.3. *E has potential good reduction if and only if $j(E) \in R$.*

Proof. See [15, Proposition VII.5.5]. □

One we have reduced an elliptic curve E to a nonsigular one $\overline{E}$ modulo $\mathfrak{m}$, we can reduce points working in projective coordinates and using scalars to make sure the coordinates are in integral (see [15, VII.2 and VII.3] for details). The point reduction is a group homomorphism $E(\overline{L}) \longrightarrow E(\overline{k})$. If n is prime to $p = \mathrm{char}(k)$, it induces an isomorphism $E[n] \longrightarrow \overline{E}[n]$.

We can also reduce morphisms but the mathematical foundations of this reduction is far beyond the scope of this report and uses Néron models (see [16, chapter IV] for a presentation of Néron models and the forum `stackexchange.com` for the definition of morphism reduction). However, the properties of the reduction of morphisms can be stated simply. Let E and F be ellpitic curve over L with good reduction modulo $\mathfrak{m}$. Then there is a group homomorphism :

$$\mathrm{Hom}(E,F) \longrightarrow \mathrm{Hom}(\overline{E},\overline{F}).$$

This map is in fact injective. But it is not always surjective : for instance, when $E = F$ are defined over a number field and $\overline{E} = \overline{F}$ is supersingular. See the results of Deuring ([17, chapter 13]) for more about this topic.

This definition is functorial, meaning that the reduction of the composite of two isogenies is the composite of the reductions of these isogenies.

A.3 Some prerequisites on quaternions

We give the results of this section without proof. The reader may refer to [24] for a complete presentation. A *quaternion algebra* over a field k is a 4-dimensional k-algebra B such that there exists $i, j \in B$ and $a, b \in k^*$ such that:

$$i^2 = a, \quad j^2 = b \quad \text{and} \quad ij = -ji$$

We denote $B = H_k(a,b)$ or simply $H(a,b)$.

If $B = H(a,b)$ is a quaternion algebra, then there is an involution called the *conjugation*, given by:

$$\forall \alpha := x + yi + zj + tij \in B, \quad \overline{\alpha} := x - (yi + zj + tij).$$

We define the *reduced norm* nrd and the *reduced trace* Tr as follows:

$$\forall \alpha \in B, \quad \mathrm{nrd}(\alpha) := \alpha\overline{\alpha} = \overline{\alpha}\alpha \quad \text{and} \quad \mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$$

Every element $\alpha \in B$ is annihilated by $X^2 - \mathrm{Tr}(\alpha)X + \mathrm{nrd}(\alpha)$, so its degree over k is ≤ 2.

If $\mathrm{char}(k) \neq 2$, then a quaternion algebra B defined over k is either a division algebra or a isomorphic to $M_2(k)$ [24, Theorem 5.4.4]. When $k = \mathbb{R}$ there is (up to isomorphism) only one quaternion division algebra which is the Hamilton quaternion algebra $\mathbb{H} := H_{\mathbb{R}}(-1,-1)$ [24, Corollary 3.5.8]. When $k = \mathbb{Q}_p$ is the p-adic field for a given prime number $p \neq 2$, the same result holds [24, Theorem 12.1.5].

Let B be a quaternion algebra defined over $\mathbb{Q}$. We say that B *ramifies* at a prime p if $B \otimes \mathbb{Q}_p$ is a division algebra and similarly, we say that B ramifies at ∞ if $B \otimes \mathbb{R} \simeq \mathbb{H}$. The latter happens if and only if $a < 0$ and $b < 0$. The set $\mathrm{Ram}(B)$ of places where B ramifies is finite and has even cardinality [24, Proposition 14.2.1] and for every set of places Σ of even cardinality (included in the union of prime numbers with $\{\infty\}$), there exists a quaternion algebra B over $\mathbb{Q}$ such that $\mathrm{Ram}(B) = \Sigma$ [24, Proposition 14.2.7]. Moreover, two quaternion algebra B and B' defined over $\mathbb{Q}$ are isomorphic if and only if $\mathrm{Ram}(B) = \mathrm{Ram}(B')$ [24, Proposition 14.3.1]. Hence, it makes sense to talk about "the" quaternion algebra $B_{p,\infty}$ ramifying at p and ∞ (useful in the context of elliptic curves arithmetic).

In the following, we only consider quaternion algebras defined over $\mathbb{Q}$. Let B be such an algebra. We say that $I \subseteq B$ is a *lattice* if it is a sub-$\mathbb{Z}$-module of B of rank 4. A lattice $\mathcal{R} \subset B$ is an *order* if it is also a subring of B (with unity: $1 \in \mathcal{R}$). If $I \subseteq B$ is a lattice, we define its *left-order* and its *right-order* by:

$$O_L(I) := \{\alpha \in B \mid \alpha \cdot I \subseteq I\} \quad \text{and} \quad O_R(I) := \{\alpha \in B \mid I \cdot \alpha \subseteq I\}$$

respectively. A *maximal order* is an order of B that is maximal for the inclusion. Unlike in number fields,

there is not a unique maximal order in a quaternion algebra. If $\mathcal{R} \subseteq B$ is an order, then $\mathcal{R}$ is integral over $\mathbb{Z}$, but not integrally closed in general (even if $\mathcal{R}$ is maximal).

Let $\mathcal{R}$ be an order of B. A (fractional) *left-ideal* I of $\mathcal{R}$ is a lattice $I \subseteq B$ such that $\alpha I \subseteq I$ for all $\alpha \in \mathcal{R}$. If $\mathcal{R}$ is maximal, we then have $\mathcal{R} = O_L(I)$. We define right-ideals similarly.

Let $I, J \subseteq B$ be two lattices. We say they are *left-equivalent* and denote $I \sim_L J$ or simply $I \sim J$ if there exists $\beta \in B$ such that $J = I\beta$. In that case, $O_L(I) = O_L(J)$.

We say that a lattice $I \subseteq B$ is *integral* if $I^2 \subseteq I$. This is actually equivalent to $I \subseteq O_R(I) \cap O_L(J)$ [24, Lemma 16.2.8].

Let $\mathcal{R}$ and $\mathcal{R}'$ be maximal orders of B. A *connecting ideal* between $\mathcal{R}$ and $\mathcal{R}'$ is a lattice I such that $O_L(I) = \mathcal{R}$ and $O_R(I) = \mathcal{R}'$. By [24, Lemma 17.4.7], $I := \mathcal{R} \cdot \mathcal{R}'$ is a connecting ideal between $\mathcal{R}$ and $\mathcal{R}'$.

If $I \subseteq B$ is a lattice and $(\alpha_1, \cdots, \alpha_4)$ is a $\mathbb{Z}$-basis of I, we define the *discriminant* of I by:

$$\mathrm{disc}(I) := \det\left(\mathrm{Tr}(\alpha_i \alpha_j)\right)_{1 \leq i,j \leq 4}.$$

It can be proved that such a quantity does not depend on the choice of a $\mathbb{Z}$-basis. If $I \subseteq J$ are two lattices, then we have $\mathrm{disc}(I) = [J : I]^2 \, \mathrm{disc}(J)^2$ [24, Lemma 15.2.15].

If $I \subseteq B$ is a lattice, we define the *reduced* norm of I by:

$$\mathrm{nrd}(I) := \gcd\{\mathrm{nrd}(\alpha) \mid \alpha \in I\}.$$

The reduced norm is multiplicative. Besides,if I is an right or left integral ideal of a maximal order $\mathcal{R}$, then we have $\mathrm{nrd}(I)^2 = [\mathcal{R} : I]^2$ [24, Theorem 16.1.3].

A.4 The Deuring correspondence

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve and $\mathcal{R} = \mathrm{End}(E)$. By [24, Theorem 42.1.9], $\mathcal{R}$ is a maximal order in the quaternion algebra $B_{p,\infty} \simeq \mathrm{End}^0(E)$ ramifying at p and ∞. Any left integral $\mathcal{R}$-ideal $I \subseteq \mathcal{R}$ of norm prime to p defines a separable isogeny $\phi_I : E \longrightarrow E_I$ whose kernel is:

$$E[I] = \bigcap_{\alpha \in I} \ker(\alpha).$$

This definition can be generalized to ideals I of norm divisible by p by factoring them as follows $I = P^r I'$ where P is the only two sided $\mathcal{R}$-ideal of norm p and I' is an integral left $\mathcal{R}$-ideal of norm prime to p. One pre-compose the isogeny associated to I' by the the r-th Frobenius map (see [24, 42.2.4]). The isogeny ϕ_I associated to I has degree $n(I)$, the reduced norm of I (by [24, Proposition 42.2.16.(a)]).

If I is an integral $\mathcal{R}$-ideal, then the left-order of I is:

$$O_L(I) := \{\alpha \in B_{p,\infty} \mid \alpha \cdot I \subseteq I\} = \mathcal{R}$$

and by [24, Lemma 42.2.9]:

$$O_R(I) := \{\alpha \in B_{p,\infty} \mid I \cdot \alpha \subseteq I\} \simeq \mathrm{End}(E_I).$$

If $I \sim J$, then $E_I \simeq E_J$ (by [24, Lemma 42.2.13]).

Conversely, one can associate an integral left $\mathcal{R}$-ideal to any finite subgroup $H \subseteq E(\overline{\mathbb{F}_p})$:

$$I(H) = \{\alpha \in \mathcal{R} \mid \forall P \in H, \quad \alpha(P) = 0\}$$

and in particular, one can define the *kernel ideal* of an isogeny $\phi : E \longrightarrow F$ as $I(\ker(\phi))$, which is

isomorphic to $\mathrm{Hom}(F,E)$ as a left $\mathcal{R}$-module via:

$$\psi \in \mathrm{Hom}(F,E) \longmapsto \psi \circ \phi \in I(\ker(\phi))$$

by [24, Lemma 42.2.7]. Unsurprisingly, we always have $I(E[I]) = I$ (by [24, Proposition 42.2.16.(b)]) and every isogeny $\phi : E \longrightarrow F$ is determined by its kernel ideal $I := I(\ker(\phi))$ as follows: there exists an isomorphism $\lambda : E_I \xrightarrow{\sim} F$ such that $\phi = \lambda \circ \phi_I$ (by [24, Corollary 42.2.21]).

If $\mathcal{R}'$ is a maximal order of $B_{p,\infty}$, then there exists a connecting integral ideal between $\mathcal{R}$ and $\mathcal{R}'$, that is to say a lattice $I \subseteq \mathcal{R} \cap \mathcal{R}'$ such that $O_L(I) = \mathcal{R}$ and $O_R(I) = \mathcal{R}'$. This ideal can easily be constructed by taking $I = \mathcal{R}\mathcal{R}'$ and multiplying it by a certain integer to eliminate cumbersome denominators (see [24, Lemma 17.4.7]). We then have $\mathrm{End}(E_I) \simeq \mathcal{R}'$, so we just proved that any maximal order is the endomorphism ring of a supersingular elliptic curve. For a given maximal order $\mathcal{R}$, there are only two elliptic curves at most with $\mathcal{R}$ as endomorphism ring up to isomorphism and one is the image of the other by the p-th power Frobenius (see [24, Lemma 42.4.1]).

A.5 Structure of the ideal class group $\mathrm{Cl}(\mathcal{O}_n)$

Let K be a quadratic imaginary field such that $h(\mathcal{O}_K) = 1$, ℓ a small prime, $n \in \mathbb{N}^*$ a big integer and $\mathcal{O}_n = \mathbb{Z} + \ell^n \mathcal{O}_K$ the order of conductor ℓ^n. In this paragraph, we determine the structure of $\mathrm{Cl}(\mathcal{O}_n)$ and show that this group is either cyclic or quasi-cyclic. Most results of this paragraph are due to [19, chapter 7] and [33, chapter 4].

Lemma A.4. *Let K be a quadratic imaginary field such that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial, $f \in \mathbb{N} \setminus \{0,1\}$ and $\mathcal{O} := \mathbb{Z} + f\mathcal{O}_K$ be the order of K of conductor f. Then, we have an exact sequence:*

$$\{1\} \longrightarrow \{\pm 1\} \xrightarrow{\phi_1} (\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times \xrightarrow{\phi_2} (\mathcal{O}_K/f\mathcal{O}_K)^\times \xrightarrow{\phi_3} \mathrm{Cl}(\mathcal{O}) \longrightarrow \{1\}.$$

Where the group homomorphisms are given by:

$$\phi_1 : x \in \{\pm 1\} \longmapsto (x,x) \in (\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times,$$

$$\phi_2 : (\overline{x},\omega) \in (\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times \longmapsto [x \cdot \omega] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times,$$

$$\textit{and} \quad \phi_3 : [\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times \longmapsto [\alpha\mathcal{O}_K \cap \mathcal{O}] \in \mathrm{Cl}(\mathcal{O}).$$

Proof. We have to prove that ϕ_1 is injective (which is trivial), $\ker(\phi_2) = \mathrm{im}(\phi_1)$, $\ker(\phi_3) = \mathrm{im}(\phi_2)$ and that ϕ_3 is surjective. The surjectivity of ϕ_3 comes from the fact that every ideal of $\mathcal{O}$ is given by the intersection of an ideal of $\mathcal{O}_K$ with $\mathcal{O}$ by [19, Proposition 7.20] and that every ideal of $\mathcal{O}_K$ is principal.

We trivially have $\ker(\phi_2) \supseteq \mathrm{im}(\phi_1)$. Conversely, let $(\overline{x},\omega) \in (\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times$ such that $x \cdot \omega \equiv 1 \mod f\mathcal{O}_K$ so there exists $a,b \in \mathbb{Z}$ such that:

$$x \cdot \omega = 1 + fa + fb\theta,$$

where θ is a generator of $\mathcal{O}_K$. If $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ then $\mathcal{O}_K^\times = \{\pm 1\}$ so $b = 0$ and $(\overline{x},\omega) \in \{\pm(1,1)\} = \mathrm{im}(\phi_1)$. If $K = \mathbb{Q}(i)$, we may take $\theta := i$ and we have $\mathcal{O}_K^\times = \{\pm 1, \pm i\}$. The case $\omega = \pm i$ is impossible, otherwise f would divide 1, so we must have $\omega = \pm 1$ and we conclude as previously. If $K = \mathbb{Q}(\sqrt{-3})$, then we may assume that $\theta := (-1 + i\sqrt{3})/2$ and we have $\mathcal{O}_K^\times = \{\pm 1, \pm\theta, \pm\theta^2\}$. As previously, the case $\omega = \pm\theta$ is impossible. If $\omega = \pm\theta^2 = \mp(\theta + 1)$, then we must have $fb = \mp x$ so $f|x$ and $\overline{x} = 0 \notin (\mathbb{Z}/f\mathbb{Z})^\times$. Hence, $\omega = \pm 1$ and we conclude as previously. Hence, $\ker(\phi_2) = \mathrm{im}(\phi_1)$.

Now, we prove that $\ker(\phi_3) \supseteq \mathrm{im}(\phi_2)$. Let $(\overline{x},\omega) \in (\mathbb{Z}/f\mathbb{Z})^\times \times \mathcal{O}_K^\times$. Then:

$$(x \cdot \omega\mathcal{O}_K) \cap \mathcal{O} = (x\mathcal{O}_K) \cap \mathcal{O} = x\mathcal{O},$$

since $x \in \mathcal{O}$, so $\phi_2(\overline{x}, \omega) \in \ker(\phi_3)$. Conversely, let $[\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$ such that $[\alpha\mathcal{O}_K \cap \mathcal{O}] = [1]$. Then, there exists $\beta \in \mathcal{O}$ such that $\alpha\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$. Hence:

$$\alpha\mathcal{O}_K = (\alpha\mathcal{O}_K \cap \mathcal{O}) \cdot \mathcal{O}_K = \beta\mathcal{O}_K,$$

so that $\alpha = \beta u$ and $\beta = \alpha v$ with $u, v \in \mathcal{O}_K$, so that $\beta = \beta uv$, $uv = 1$ and $u \in \mathcal{O}_K^\times$. Let us write $\beta := a + bf\theta$ with $a, b \in \mathbb{Z}$. Since $[\alpha] \in (\mathcal{O}_K/f\mathcal{O}_K)^\times$, there exists $\gamma \in \mathcal{O}_K$ such that $\alpha\gamma \equiv 1 \mod f\mathcal{O}_K$ and we get that $N(\alpha)N(\gamma) \equiv 1\ [f]$, so that f and $N(\alpha)$ are coprime. Since $N(\beta) = N(\alpha)$, it follows that a is prime to f.Hence $\overline{a} \in (\mathbb{Z}/f\mathbb{Z})^\times$ and:

$$[\alpha] = [au] = \phi_2(\overline{a}, u).$$

This completes the proof. □

By the exact sequence of the lemma, 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:

$$(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/(\mathbb{Z}/\ell^n\mathbb{Z})^\times \twoheadrightarrow \mathrm{Cl}(\mathcal{O}_n) \quad (\star\star).$$

Hence, we shall deduce the structure of $\mathrm{Cl}(\mathcal{O}_n)$ from the structure of $(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/(\mathbb{Z}/\ell^n\mathbb{Z})^\times$.

The structure of $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ is well known (it is either cyclic or quasi cyclic for $\ell = 2$). Now, we determine the structure of $(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times$. By the following lemma, this problem reduces to determining $(\mathcal{O}_K/\mathfrak{l}^n)^t imes$ where $\mathfrak{l}$ is a prime ideal of $\mathcal{O}_K$ lying above ℓ.

Lemma A.5. *Let K be a number field and $\mathfrak{a}, \mathfrak{b} \subseteq \mathcal{O}_K$ two coprime integral ideals ($\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$). Then, we have:*

$$(\mathcal{O}_K/\mathfrak{ab})^\times \simeq (\mathcal{O}_K/\mathfrak{a})^\times \times (\mathcal{O}_K/\mathfrak{b})^\times.$$

Proof. We construct a split exact sequence:

$$\{1\} \longrightarrow (\mathcal{O}_K/\mathfrak{a})^\times \xrightarrow{\phi} (\mathcal{O}_K/\mathfrak{ab})^\times \underset{\psi}{\overset{\sigma}{\leftrightarrows}} (\mathcal{O}_K/\mathfrak{b})^\times \longrightarrow \{1\}.$$

Let $a \in \mathfrak{a}$ and $b \in \mathfrak{b}$ such that $a + b = 1$. Then, we set, for all $x, y, z \in \mathcal{O}_K$:

$$\phi(\overline{x}) = \overline{bx + a}, \quad \psi(\overline{y}) = \overline{y} \quad \text{and} \quad \sigma(\overline{z}) = \overline{az + b},$$

where the overline denotes the residue class modulo $\mathfrak{a}, \mathfrak{b}$ or $\mathfrak{ab}$, depending on the context.

ψ is trivially a well-defined and surjective group homomorphism since $\mathfrak{ab} \subseteq \mathfrak{b}$.

Similarly, if $x, x' \in \mathcal{O}_K$ satisfy $x - x' \in \mathfrak{a}$ then $bx + a - (bx' + a) = b(x - x') \in \mathfrak{ab}$ so ϕ is well-defined as a map $\mathcal{O}_K/\mathfrak{a} \longrightarrow \mathcal{O}_K/\mathfrak{ab}$. Besides, if $xx' \equiv 1 \mod \mathfrak{a}$ then:

$$(bx + a)(bx' + a) = b^2xx' + ab(x + x') + a^2 \equiv a^2 + b^2 \mod \mathfrak{ab}.$$

But $a^2 = a(1 - b) \equiv a \mod \mathfrak{ab}$ and $b^2 = b(1 - a) \equiv b \mod \mathfrak{ab}$, so that:

$$(bx + a)(bx' + a) \equiv a + b \equiv 1 \mod \mathfrak{ab},$$

so ϕ maps invertibles to invertibles and is well defined. By the same arguments (exchanging the roles of $\mathfrak{a}$ and $\mathfrak{b}$), we get that σ is well defined.

If $x, x' \in \mathcal{O}_K$ are invertible modulo $\mathfrak{a}$, we also have:

$$\phi(\overline{x})\phi(\overline{x'}) = \overline{(bx+a)(bx'+a)} = \overline{b^2xx' + ab(x+x') + a^2} = \overline{b^2xx' + a^2} = \overline{bxx' + a} = \phi(\overline{xx'}),$$

since $a^2 \equiv a \mod \mathfrak{ab}$ and $b^2 \equiv b \mod \mathfrak{ab}$. Hence, ϕ is a group homomorphism and by symmetry, σ as well.

If $\phi(\overline{x}) = 1$, then $bx + a \equiv 1 \mod \mathfrak{ab}$ so $bx \equiv 1 \mod \mathfrak{a}$ so $x \equiv 1 \mod \mathfrak{a}$ *i.e.* $\overline{x} = \overline{1}$, since $b = 1 - a \equiv 1 \mod \mathfrak{a}$. Hence, ϕ is injective.

Finally, we have $\psi \circ \sigma = \mathrm{id}$, since $a \equiv 1 \mod \mathfrak{b}$ so we have indeed a split exact sequence. It follows that:

$$\Phi : (\overline{x}, \overline{y}) \in (\mathcal{O}_K/\mathfrak{a})^\times \times (\mathcal{O}_K/\mathfrak{b})^\times \longmapsto \phi(\overline{x})\sigma(\overline{y}) \in (\mathcal{O}_K/\mathfrak{ab})^\times$$

is a group isomorphism. □

A.5.1 Determining the structure of $(\mathcal{O}_K/\mathfrak{l}^n)^\times$

Proposition A.6. *Let f be the inertia index of $\mathfrak{l}$ and $q := \ell^f$. $G := (\mathcal{O}_K/\mathfrak{l}^n)^\times$,*

$$W := \{x \in G \mid x^{q-1} = 1\}$$

and $G_\mathfrak{l} := (1+\mathfrak{l})/(1+\mathfrak{l}^n)$ (seen as a subgroup of G). Then:

(i) *$W \simeq (\mathcal{O}_K/\mathfrak{l})^\times$, so W is cyclic of order $q-1$.*

(ii) *$G_\mathfrak{l}$ is a ℓ-group of order q^{n-1}.*

(iii) *$G \simeq W \times G_\mathfrak{l}$.*

Proof. **(i)** $\mathcal{O}_K/\mathfrak{l}$ is a finite field with q elements so the invertible elements form a cyclic group of order $q-1$ and all of them are roots of $X^{q-1} - 1$, so $X^{q-1} - 1$ is completely factored in $\mathcal{O}_K/\mathfrak{l}[X]$ with simple roots:

$$X^{q-1} - 1 \equiv \prod_{x \in (\mathcal{O}_K/\mathfrak{l})^\times} (X - x) \mod \mathfrak{l}.$$

By Hensel's lemma (see Corollary A.2), this factorization can be lifted in $\mathcal{O}_{K,\mathfrak{p}}[X]$. By reducing it modulo $\mathfrak{l}^n$, we obtain a factorization mod $\mathfrak{l}^n$:

$$X^{q-1} - 1 \equiv \prod_{y \in E} (X - y) \mod \mathfrak{l}^n.$$

Where $E \subseteq \mathcal{O}_K/\mathfrak{l}^n$ is set of $q-1$ elements reducing to $(\mathcal{O}_K/\mathfrak{l})^\times$ modulo $\mathfrak{l}$. Actually, $E \subseteq (\mathcal{O}_K/\mathfrak{l}^n)^\times$ because $x \in E$ implies that x is invertible with inverse x^{q-2} and we even have $E \subseteq W$. Let us consider the group homomorphism:

$$\varphi : x \in W \longmapsto (x \mod \mathfrak{l}) \in (\mathcal{O}_K/\mathfrak{l})^\times.$$

Since $\varphi(E) = W$, φ is surjective. Now, if $x \in W$, then:

$$0 = x^{q-1} - 1 \equiv \prod_{y \in E} (x - y) \mod \mathfrak{l}^n.$$

But x modulo $\mathfrak{l}$, is only congruent to one element of $(\mathcal{O}_K/\mathfrak{l})^\times$, so there exists $y \in E$ such that $x \equiv y \mod \mathfrak{l}$ and for all $y' \in E \setminus \{y\}$, $x \not\equiv y \mod \mathfrak{l}$. As a consequence, we must have $x = y$ so $y \in E$.As a consequence, φ is injective.

(ii) We have a bijection $G_\mathfrak{l} = (1+\mathfrak{l})/(1+\mathfrak{l}^n) \longmapsto \mathfrak{l}/\mathfrak{l}^n$ mapping $1+x$ to x. We also have a natural exact sequence:

$$\{1\} \longrightarrow \mathfrak{l}/\mathfrak{l}^n \longrightarrow \mathcal{O}_K/\mathfrak{l}^n \longrightarrow \mathcal{O}_K/\mathfrak{l} \longrightarrow \{1\},$$

so that:

$$N(\mathfrak{l}^n) = N(\mathfrak{l})|\mathfrak{l}/\mathfrak{l}^n| \quad i.e. \quad |\mathfrak{l}/\mathfrak{l}^n| = N(\ell)^{n-1} = \ell^{f(n-1)} = q^{n-1},$$

so that $G_\mathfrak{l}$ is indeed an ℓ-group of cardinality q^{n-1}.

(iii) Let us consider the group homomorphism:

$$\psi : (x,y) \in W \times G_\mathfrak{l} \longmapsto x \cdot y \in G.$$

Let $(x,y) \in W \times G_\mathfrak{l}$ such that $\psi(x,y) = xy = 1$. Since $y \equiv 1 \mod \mathfrak{l}$, we have $x \equiv 1 \mod \mathfrak{l}$, so that $x = 1$, by injectivity of the morphism φ of point (i), and $y = 1$. So ψ is injective.

If $z \in G$, then we consider a lift $x \in W$ of $z \mod \mathfrak{l}$ (by surjectivity of the map φ of point (i)) and we set $y := x^{-1}z$. Then, $y \equiv 1 \mod \mathfrak{l}$ so $y \in G_\mathfrak{l}$ and $\psi(x,y) = z$. Hence, ψ is an isomorphism.

□

It remains to determine the structure of $G_\mathfrak{l} := (1+\mathfrak{l})/(1+\mathfrak{l}^n)$. The main idea here is to prove that the multiplicative group $G_\mathfrak{l}$ is isomorphic to the additive group $\mathcal{O}_K/\mathfrak{l}^{n-1}$ under some conditions. Fortunately, the group structure of $\mathcal{O}_K/\mathfrak{l}^{n-1}$ will be easy to determine.

To linearise the multiplicative structure, we shall use the $\mathfrak{l}$-adic logarithm.

Definition A.7. Let $K_\mathfrak{l}$ be the $\mathfrak{l}$-adic completion of K. For all $x \in K_\mathfrak{l}$ such that $v_\mathfrak{l}(x) \geq 1$, we define the $\mathfrak{l}$-*adic logarithm* of $1+x$ by:

$$\log_\mathfrak{l}(1+x) := \sum_{i=1}^{+\infty} \frac{(-1)^{i-1}}{i} x^i.$$

Let e be the ramification index of $\mathfrak{l}$ above ℓ. Then, for all $x \in K_\mathfrak{l}$ such that $v_\mathfrak{l}(x) > e/(\ell-1)$, we define the $\mathfrak{l}$-*adic exponential* of x by:

$$\exp_\mathfrak{l}(x) := \sum_{i=0}^{+\infty} \frac{x^i}{i!}.$$

Proposition A.8. *Let $x, y \in K_\mathfrak{l}$ and e be the ramification index of $\mathfrak{l}$ above ℓ. Then:*

(i) $\log_\mathfrak{l}(1+x)$ *is well defined if* $v_\mathfrak{l}(x) \geq 1$ *and* $\exp_\mathfrak{l}(x)$ *is well defined if* $v_\mathfrak{l}(x) > e/(\ell-1)$.

(ii) *If* $v_\mathfrak{l}(x) \geq 1$ *and* $v_\mathfrak{l}(y) \geq 1$, *we have:*

$$\log_\mathfrak{l}((1+x)(1+y)) = \log_\mathfrak{l}(1+x) + \log_\mathfrak{l}(1+y).$$

If $v_\mathfrak{l}(x) > e/(\ell-1)$ *and* $v_\mathfrak{l}(y) > e/(\ell-1)$,*we have:*

$$\exp_\mathfrak{l}(x+y) = \exp_\mathfrak{l}(x)\exp_\mathfrak{l}(y).$$

(iii) *If* $v_\mathfrak{l}(x) > e/(\ell-1)$, *then* $v_\mathfrak{l}(\log_\mathfrak{l}(1+x)) = v_\mathfrak{l}(x)$ *and* $v_\mathfrak{l}(\exp_\mathfrak{l}(x)-1) = v_\mathfrak{l}(x)$.

(iv) *If* $v_\mathfrak{l}(x) > e/(\ell-1)$, *then we have:*

$$\exp_\mathfrak{l}(\log_\mathfrak{l}(1+x)) = 1+x \qquad \textit{and} \qquad \log_\mathfrak{l}(\exp_\mathfrak{l}(x)) = x.$$

Proof. **(i)** In the $\mathfrak{l}$-adic topology, a series converge if and only if its terms converge towards zero. If $v_\mathfrak{l}(x) \geq 1$, the we have for all $i \in \mathbb{N}^*$:

$$v_\mathfrak{l}\left(\frac{(-1)^{i-1}}{i}x^i\right) = iv_\mathfrak{l}(x) - v_\mathfrak{l}(i) = iv_\mathfrak{l}(x) - ev_\ell(i) \geq i - e\frac{\log(i)}{\log(\ell)}.$$

Hence, $v_{\mathfrak{l}}\left(\frac{(-1)^{i-1}}{i}x^i\right) \xrightarrow[i\to+\infty]{} +\infty$ and the series $\log_{\mathfrak{l}}(1+x)$ converge.

For all $i \in \mathbb{N}$, we have:

$$v_{\mathfrak{l}}\left(\frac{x^i}{i!}\right) = iv_{\mathfrak{l}}(x) - v_{\mathfrak{l}}(i!) = iv_{\mathfrak{l}}(x) - ev_\ell(i!),$$

with:

$$v_\ell(i!) = \sum_{k=1}^{+\infty}\left\lfloor\frac{i}{\ell^k}\right\rfloor = \sum_{k=1}^{\lfloor\log_\ell(i)\rfloor}\frac{i}{\ell^k} = \frac{i}{\ell}\frac{1-\frac{1}{\ell^{\lfloor\log_\ell(i)\rfloor}}}{1-\frac{1}{\ell}} = \frac{i-\frac{i}{\ell^{\lfloor\log_\ell(i)\rfloor}}}{\ell-1} \leq \frac{i-1}{\ell-1} < \frac{i}{\ell-1},$$

so that, if $v_{\mathfrak{l}}(x) > e/(\ell-1)$:

$$v_{\mathfrak{l}}\left(\frac{x^i}{i!}\right) = i\left(v_{\mathfrak{l}}(x) - \frac{ev_\ell(i!)}{i}\right) > i\left(v_\ell(x) - \frac{e}{\ell-1}\right) \geq i$$

and $v_{\mathfrak{l}}\left(\frac{x^i}{i!}\right) \xrightarrow[i\to+\infty]{} +\infty$. Hence, $\exp_\ell(x)$ converges.

(ii) The equalities hold in the ring of formal series (and can be proved over the complex numbers) so they hold as long as the series involved converge, which is true by (i) for the values of $v_{\mathfrak{l}}(x)$ and $v_{\mathfrak{l}}(x)$ that we assumed.

(iii) We assume that $v_{\mathfrak{l}}(x) > e/(\ell-1)$. To prove that $v_{\mathfrak{l}}(\log_{\mathfrak{l}}(1+x)) = v_{\mathfrak{l}}(x)$, it suffices to prove that $v_{\mathfrak{l}}(x^i/i) > v_{\mathfrak{l}}(x)$ for all $i \geq 2$. Let $i \geq 2$. Then:

$$v_{\mathfrak{l}}\left(\frac{x^i}{i}\right) - v_{\mathfrak{l}}(x) = (i-1)v_{\mathfrak{l}}(x) - ev_\ell(i) > e\left(\frac{i-1}{\ell-1} - v_\ell(i)\right) \geq e(v_\ell(i!) - v_\ell(i)) = ev_\ell((i-1)!) \geq 0,$$

since we have seen that $v_\ell(i!) \leq (i-1)/(\ell-1)$. Hence, $v_{\mathfrak{l}}(\log_{\mathfrak{l}}(1+x)) = v_{\mathfrak{l}}(x)$.

Now, if $i \geq 2$, we have:

$$v_{\mathfrak{l}}\left(\frac{x^i}{i!}\right) - v_{\mathfrak{l}}(x) = (i-1)v_{\mathfrak{l}}(x) - ev_\ell(i!) > (i-1)\frac{e}{\ell-1} - e\frac{i-1}{\ell-1} = 0.$$

So we conclude that $v_{\mathfrak{l}}(\exp_{\mathfrak{l}}(x)-1) = v_{\mathfrak{l}}(x)$, as previously.

(iv) (iii) ensures that the series involved in the equalities to be proved converge. Since those equalities hold in the ring of formal series, we conclude as in (ii). □

Corollary A.9. *Suppose that $\ell \geq e+2$. Then $\log_{\mathfrak{l}}$ and $\exp_{\mathfrak{l}}$ induce reciprocal group isomorphisms between $G_{\mathfrak{l}} = (1+\mathfrak{l})/(1+\mathfrak{l}^n)$ and $\mathfrak{l}/\mathfrak{l}^n$ (for $n \in \mathbb{N}^*$).*

Proof. Since $\ell \geq e+2$, we have $e/(\ell-1) < 1$ so $\exp_{\mathfrak{l}}$ is well defined on $\mathfrak{l}$ by Proposition A.6.(i). Point (iii) of this Proposition ensures that $G_{\mathfrak{l}}$ maps to $\mathfrak{l}/\mathfrak{l}^n$ via $\log_{\mathfrak{l}}$ and that $\mathfrak{l}/\mathfrak{l}^n$ maps to $G_{\mathfrak{l}}$ via $\exp_{\mathfrak{l}}$. By point (ii), those are group homomorphisms and by point (iv), those homomorphisms are reciprocal isomorphisms. □

Lemma A.10. *For $n \in \mathbb{N}^*$, we have an isomorphism of additive groups $\mathcal{O}_K/\mathfrak{l}^{n-1} \simeq \mathfrak{l}/\mathfrak{l}^n$.*

Proof. We have $\mathfrak{l}^2 \subsetneq \mathfrak{l}$ (otherwise, these ideals would have the same norm), so there exists $\alpha \in \mathfrak{l} \setminus \mathfrak{l}^2$. We consider the additive homomorphism $x \in \mathcal{O}_K \longmapsto \alpha x \in \mathfrak{l}$. Since this homomorphism maps $\mathfrak{l}^{n-1}$ to $\mathfrak{l}^n$, it induces a homomorphism $\phi : \mathcal{O}_K/\mathfrak{l}^{n-1} \longrightarrow \mathfrak{l}/\mathfrak{l}^n$. If $x \in \mathcal{O}_K$ satisfies $\alpha x \in \mathfrak{l}^n$, then:

$$v_{\mathfrak{l}}(x) = v_{\mathfrak{l}}(\alpha x) - v_{\mathfrak{l}}(\alpha) \geq n-1,$$

so that $x \in \mathfrak{l}^{n-1}$. Hence, ϕ is injective, and this is an isomorphism because:

$$|\mathfrak{l}/\mathfrak{l}^n| = \frac{N(\mathfrak{l})^n}{N(\mathfrak{l})} = N(\mathfrak{l})^{n-1} = |\mathcal{O}_K/\mathfrak{l}^{n-1}|,$$

since we have the exact sequence:

$$\{1\} \longrightarrow \mathfrak{l}/\mathfrak{l}^n \longrightarrow \mathcal{O}_K/\mathfrak{l}^n \longrightarrow \mathcal{O}_K/\mathfrak{l} \longrightarrow \{1\}.$$

□

Proposition A.11. *Let K be a number field and $\mathfrak{l}$, a prime ideal of $\mathcal{O}_K$ lying over a prime number ℓ. Let $k \in \mathbb{N}^*$, e and f respectively the ramification and inertia index of $\mathfrak{l}$ above ℓ, q and r be the quotient and remainder in the euclidean division of $k+e-1$ by e: $k+e-1 = eq+r$ ($r \in [\![0\ ;\ e-1]\!]$). Then, we have the following additive group isomorphism:*

$$(\mathcal{O}_K/\mathfrak{l}^k) \simeq (\mathbb{Z}/\ell^q\mathbb{Z})^{(r+1)f} \times (\mathbb{Z}/\ell^{q-1}\mathbb{Z})^{(e-r-1)f}.$$

Proof. We have $|\mathcal{O}_K/\mathfrak{l}^k| = N(\mathfrak{l}^k) = \ell^{kf}$ so $\mathcal{O}_K/\mathfrak{l}^k$ is a ℓ-group and the structure theorem of finite abelian group ensures that:

$$\mathcal{O}_K/\mathfrak{l}^k = \prod_{i\geq 1}(\mathbb{Z}/\ell^i\mathbb{Z})^{a_i},$$

where $(a_i)_{i\geq 1}$ is an almost zero sequence of integers such that:

$$\sum_{i=1}^{+\infty} i a_i = kf \quad (1).$$

We shall now obtain more relations as above to compute all the a_i. Let $j \in \mathbb{N}^*$. Then:

$$\ell^j(\mathcal{O}_K/\mathfrak{l}^k) = \prod_{i\geq j+1} (\mathbb{Z}/\ell^{i-j}\mathbb{Z})^{a_i},$$

so that:

$$\log_\ell(|\ell^j(\mathcal{O}_K/\mathfrak{l}^k)|) = \sum_{i=j+1}^{+\infty} (i-j)a_i \quad (2).$$

But $\ell^j(\mathcal{O}_K/\mathfrak{l}^k) = \mathfrak{b}/\mathfrak{l}^k$ with $\mathfrak{b} = \ell^j\mathcal{O}_K + \mathfrak{l}^k$. Since $\mathfrak{b}$ is an integral ideal of $\mathcal{O}_K$, which is Dedekind by [19, Corollary 5.6], $\mathfrak{b}$ can be written as a product of prime ideals:

$$\mathfrak{b} = \prod_{i=1}^{r} \mathfrak{l}_i^{e_i},$$

where $\mathfrak{l}_i$ are distinct primes and the e_i are positive integers. This decomposition is unique.Since $\mathfrak{l}^k \subseteq \mathfrak{b}$, we have $\mathfrak{l}^k \subseteq \mathfrak{l}_i$ for all $i \in [\![1\ ;\ r]\!]$, so $\mathfrak{l} \subseteq \mathfrak{l}_i$ since $\mathfrak{l}$ is prime, so $r = 1$ and $\mathfrak{l}_1 = \mathfrak{l}$ *i.e.* $\mathfrak{b}$ is a power of $\mathfrak{l}$ and:

$$v_\mathfrak{l}(\mathfrak{b}) = \min(v_\mathfrak{l}(p^j\mathcal{O}_K), v_\mathfrak{l}(\mathfrak{l}^k)) = \min(ej, k),$$

so that $\mathfrak{b} = \mathfrak{el}^{\min(ej,k)}$. Furthermore, since $\mathfrak{l}^k \subseteq \mathfrak{b}$, we have a natural exact sequence:

$$\{0\} \longrightarrow (\mathfrak{b}/\mathfrak{l}^k) \longrightarrow (\mathcal{O}_K/\mathfrak{l}^k) \longrightarrow (\mathcal{O}_K/\mathfrak{b}) \longrightarrow \{0\},$$

so that:

$$|\mathfrak{b}/\mathfrak{l}^k| = \frac{|\mathcal{O}_K/\mathfrak{l}^k|}{|\mathcal{O}_K/\mathfrak{b}|} = \frac{N(\mathfrak{l}^k)}{N(\mathfrak{b})} = \ell^{f(k-\min(ej,k))} = \ell^{f(k-\min(ej,k))} = \ell^{f\max(k-ej,0)}.$$

By (2), it follows that:

$$f\max(k-ej,0) = \sum_{i=j+1}^{+\infty} (i-j)a_i \quad (3).$$

It follows that $a_i = 0$ for all $i > \lceil k/e \rceil$. Let q and r be the quotient and remainder in the euclidean

division of $k+e-1$ by e: $k+e-1 = eq+r$ ($r \in [\![0\ ;\ e-1]\!]$). Then $q = k/e+(k+e-1)/e \in [k/e, k/e+1[$, so that $q = \lceil k/e \rceil$. By (3) applied at $j = q-1$, we get that:

$$a_q = f(k - e(q-1)) = f(r+1).$$

Applying (3) again at $j = q-2$, we get:

$$a_{q-1} = f(k-e(q-2)) - 2a_q = f(r+1+e) - 2f(r+1) = f(e-r-1).$$

Since:

$$qa_q + (q-1)a_{q-1} = qf(r+1) + (q-1)f(e-r-1) = qfe - f(e-r-1) = f(qe+r+1-e) = kf,$$

we have $a_i = 0$ for all $i \in [\![1\ ;\ q-2]\!]$ by (1). The result follows. □

Corollary A.12. *Let $n \geq 2$, e and f be respectively the ramification and inertia index of $\mathfrak{l}$ above ℓ and q and r the quotient and remainder in the euclidean division of $n+e-2$ by e: $n+e-2 = eq+r$ with $r \in [\![0\ ;\ e-1]\!]$. We assume that $\ell \geq e+2$. Then, we have:*

$$(\mathcal{O}_K/\mathfrak{l}^n)^\times \simeq (\mathbb{Z}/(\ell^f-1)\mathbb{Z}) \times (\mathbb{Z}/\ell^q\mathbb{Z})^{(r+1)f} \times (\mathbb{Z}/\ell^{q-1}\mathbb{Z})^{(e-r-1)f}.$$

Proof. This result follows directly from Proposition A.6, Lemma A.10 and Proposition A.11. □

A.5.2 Case $\ell \geq e+2$

Hence, we assume that $\ell \geq e+2$. Then, by the previous corollary, 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 [39, Theorem IV.2], $(\mathbb{Z}/\ell^n\mathbb{Z})^\times$ is cyclic, so that:

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

To compute the quotient, $(\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/(\mathbb{Z}/\ell^n\mathbb{Z})^\times$, we need the following result.

Lemma A.13. **(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, $|\phi_2(g_1, 1)|||g_1|$ ($|x|$ being the order of x) and by Lagrange's theorem $|\phi_2(g_1, 1)|||H_2|$ and $|g_1|||G_1|||H_1|$. 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 $(\mathbb{Z}/d\mathbb{Z})^2/\mathrm{im}(\varphi) \simeq \mathbb{Z}(-\overline{v}, \overline{u}) \simeq \mathbb{Z}/d\mathbb{Z}$.

(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 the previous lemma 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.

A.5.3 Case $\ell < e + 2$

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 A.14. **(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, $\alpha \in \mathcal{O}_K^\times \cdot \mathcal{O}_{i+1}$.*

(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 $d\ell$., *i.e.* $k\ell | d\ell$ so $k | d$. 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 previous 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. What happens is usually that either $\mathrm{Cl}(\mathcal{O}_2)$ and $\mathrm{Cl}(\mathcal{O}_3)$ are cyclic, in that 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` [40] and obtained the following results:

$\mathrm{disc}(K)$ \ 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	$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3 \cdot 2^{n-2}\mathbb{Z})$	

Finally, we have proved the following result:

Theorem A.15. *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).

Appendix B

Algorithms

B.1 Proper representation of an integer by a positive definite primitive quadratic form

We follow the approach of [41, § 46, pp. 73-75]. We want to solve $f(x, y) = u$ for $x, y \in \mathbb{Z}$ with $\gcd(x, y) = 1$, where $f := [a, b, c]$ is a positive definite primitive quadratic form of discriminant $d < 0$. The following algorithm determines if a solution exists and provides one.

Algorithm 2: Proper representation of an integer

Data: An integer $u \in \mathbb{N}$ and $[a, b, c]$, a positive definite primitive quadratic form of discriminant $d < 0$.

Result: A solution (x, y) of the equation $f(x, y) = u$ if there exists one, the boolean value False otherwise.

1 Find a solution $v \in [\![0\ ;\ 2u]\!]$ to $v^2 \equiv d\ [4u]$, *e.g.* using Tonelli-Shanks algorithm [28, Algorithm 1.5.1] when u is prime to find a square root mod u, and conclude by Chinese remainder theorem. If d is not a square mod $4u$, return False;
2 Compute $w \in \mathbb{Z}$ such that $v^2 - 4uw = d$;
3 Find the reduced form $[a', b', c']$ of $[a, b, c]$ and the associated unimodular transformation $x := a_1x' + b_1y'$, $y := c_1x + d_1y$ associated to it, using Gauss reduction algorithm described in [19, Theorem 2.8];
4 Find the reduced form $[u', v', w']$ of $[u, v, w]$ and the associated unimodular transformation $x := a_2x' + b_2y'$, $y := c_2x + d_2y$ associated to it;
5 **if** $[a', b', c'] = [u', v', w']$ **then**
6 | $x := a_2d_1 - b_2c_1$, $y := -a_2b_1 + b_2a_1$;
7 | Return (x, y);
8 **else**
9 | Return False;
10 **end**

It could be proved that this algorithm is correct and terminates in polynomial time in the size (number of bits) of u, a, b, c.

B.2 The KLPT algorithm

Let p be a prime number. In this section, we shall mean polynomial in $\log(p)$ every time we use the term polynomial.

We fix $\mathcal{R}$ a concise maximal order of $B_{p,\infty}$ and $I \subseteq \mathcal{R}$ an integral and concise left $\mathcal{R}$-ideal (as defined in Definition 3.1). The KLPT algorithm due to Kohel, Lauter, Petit and Tignol [27] finds an equivalent integral ideal $J \sim I$ of powersmooth norm in polynomial time (in $\log(p)$). The main idea of this algorithm lies in the following lemma:

Lemma B.1. *Let Then for all $\alpha \in I$, $J := I\frac{\overline{\alpha}}{\mathrm{nrd}(I)}$ is an integral left $\mathcal{R}$-ideal equivalent to I and* $\mathrm{nrd}(J) = \frac{\mathrm{nrd}(\alpha)}{\mathrm{nrd}(I)}$, nrd *being the reduced norm.*

Proof. We have $\alpha \in I$ so $\overline{\alpha} \in \overline{I}$ and $I\overline{\alpha} \subseteq I\overline{I}$. But $I\overline{I} = \mathrm{nrd}(I)\mathcal{R}$ (by [24, 16.6.14]), so that $J = I\frac{\overline{\alpha}}{\mathrm{nrd}(I)} \subseteq \mathcal{R}$ and J is integral.

Finally, by multiplicativity of the reduced norm [24, Lemma 16.3.7], we have:

$$\mathrm{nrd}(J) = \mathrm{nrd}(I)\,\mathrm{nrd}\left(\frac{\overline{\alpha}}{\mathrm{nrd}(I)}\right) = \mathrm{nrd}(I)\frac{\mathrm{nrd}(\alpha)}{\mathrm{nrd}(I)^2} = \frac{\mathrm{nrd}(\alpha)}{\mathrm{nrd}(I)}.$$

□

Hence, by the previous lemma, the goal of this algorithm is to find $\alpha \in I$ of norm $\mathrm{nrd}(I)S$ where S is a powersmooth integer. The different steps of the algorithm are presented below (see Algorithm 3). For this algorithm to work, $\mathcal{R}$ may not be any maximal order, but rather a *special* order defined as follows:

Definition B.2. We say that a maximal order $\mathcal{R} \subseteq B_{p,\infty}$ is *special* if $j \in \mathcal{R}$ (with $j^2 = -p$) and there exists a subring of rank 2, $R \subset \mathcal{R}$, such that $R^\perp \subseteq Rj$, where $R^\perp$ is the orthogonal of R for the scalar product given by:

$$(\alpha, \beta) \in B_{p,\infty}^2 \longmapsto (\alpha|\beta) := \mathrm{nrd}(\alpha + \beta) - \mathrm{nrd}(\alpha) - \mathrm{nrd}(\beta) = \mathrm{Tr}(\alpha\overline{\beta}).$$

Example B.3. Recall the setting of Example 3.2. When $p \equiv 3$ [4] and $E_0 : y^2 = x^3 + x$, and the endomorphism ring is isomorphic to $\mathcal{R}_0 := \langle 1, j, \frac{i+j}{2}, \frac{1+k}{2}\rangle$ and we may take $R := \mathbb{Z}[i] \subseteq \mathcal{R}_0$.

Remark B.4. In practice, it will be very useful to have $|\operatorname{disc}(R)|$ sufficiently small, *i.e.* polynomial (in $\log(p)$). For any p, we can always find an order $\mathcal{R}$ with $|\operatorname{disc}(R)| = O(\log(p)^2)$, and even $\operatorname{disc}(R) = -4$ (as in Example B.3) and $\operatorname{disc}(R) = -8$ when $p \not\equiv 1$ [8] (see [27, Section 2.3]). We shall always assume that $|\operatorname{disc}(R)| = O(\log(p)^2)$ in the following.

As previously announced, the following algorithm works under the hypothesis that $\mathcal{R}$ is special but it can be generalized by using a connecting ideal to a special order and two instances of this algorithm (see [27, Theorem 9]).

Algorithm 3: The KLPT algorithm

Data: A special order $\mathcal{R}$ and an integral left $\mathcal{R}$-ideal $I \subseteq \mathcal{R}$.

Result: An equivalent integral ideal $J \sim I$ of powersmooth norm.

1 **Step a:** Find $\delta \in I$ of norm $N\,\mathrm{nrd}(I)$ where N is a prime number $\neq p$ and compute $I' := I\overline{\delta}/\,\mathrm{nrd}(I)$;

2 **Step b:** Find $\alpha \in I'$ such that $I' = \mathcal{R}N + \mathcal{R}\alpha$;

3 **Step c:** Find $\beta_1 \in \mathcal{R}$ of norm NS_1, with S_1 powersmooth;

4 **Step d:** Find $\beta_2 \in jR$ such that $\alpha \equiv \beta_1\beta_2 \mod \mathcal{R}N$;

5 **Step e:** Find $\beta_2' \in \mathcal{R}$ with powersmooth norm S_2 and $\lambda \in (\mathbb{Z}/N\mathbb{Z})^*$ such that $\beta_2' \equiv \lambda\beta_2 \mod \mathcal{R}N$;

6 **Step f:** Set $\beta := \beta_1\beta_2'$ and return $J := I'\overline{\beta}/N$;

Step a

$\mathbb{H} := B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{R}^4$ is a normed vector space for the norm associated to the scalar product of Definition B.2, given by $\|\alpha\|^2 := 2\,\mathrm{nrd}(\alpha)$ for all $\alpha \in \mathbb{H}$. As a lattice, I admits a Minkowski reduced $\mathbb{Z}$-basis, defined as follows:

Definition B.5. Let $\Lambda \subseteq \mathbb{R}^d$ be a lattice. of rank r. A *Minkowski reduced basis* of Λ is a $\mathbb{Z}$-basis $(b_1, \cdots, b_r)$ of Λ such that for all $i \in [\![1\ ;\ r]\!]$, b_i is the shortest vector (for the euclidean norm) such that $(b_1, \cdots, b_i)$ can be completed into a $\mathbb{Z}$-basis of Λ.

[42] provides an algorithm finding a Minkowski reduced basis $(b_1, \cdots, b_r)$ of Λ given a basis $(e_1, \cdots, e_r)$ of Λ when $\Lambda \subseteq \mathbb{Z}^d$ (we can always reduce to this case by multiplying all vectors by the lcm of their denominators). If $B := \max_{1 \leq i \leq r} \|b_i\|$, then the algorithm performs in time $O\left(\left(\frac{5}{4}\right)^{4r^3} d \log(B)\right)$ and returns an output $(b_1, \cdots, b_r)$ with integer components of size $O(r^4(r\log(r) + \log(B)))$. In the case of I ($d = r = 4$), since it is given by a $\mathbb{Z}$-basis expressed in terms of $1, i, j, k$ with a basis of size polynomial, this algorithm will perform in polynomial time in $\log(p)$ and returns an output of polynomial size in $\log(p)$.

Now, given a Minkowski reduced basis $(\alpha_1, \cdots, \alpha_4)$ of I, we look for $\delta := \sum_{i=1}^4 a_i \alpha_i$ with integers $a_i \in [\![-m\ ;\ m]\!]$ for $m \in \mathbb{N}^*$ well chosen. Let $q_I := \operatorname{nrd}/\operatorname{nrd}(I)$. We argue that $q_I(\delta) = O(m^2\sqrt{p})$ heuristically, and $q_I(\alpha) = O(m^2p^2)$ in the worst case. Indeed, by [43, Teil I. § 7] the norms of the α_i are the successive minimas of the lattice:

$$\forall 1 \leq i \leq 4, \quad \|\alpha_i\| = \lambda_i(I) := \min\{\|v_i\| \mid v_1, \cdots, v_i \in I \textit{ linearly independent } \|v_1\| \leq \cdots \leq \|v_i\|\}.$$

By Minkowski's second theorem, it follows that:

$$\frac{2}{3}\frac{\operatorname{Covol}(I)}{\operatorname{Vol}(\mathbb{B}_4)} \leq \prod_{i=1}^4 \|\alpha_i\| \leq 16\frac{\operatorname{Covol}(I)}{\operatorname{Vol}(\mathbb{B}_4)},$$

where $\mathbb{B}_4$ is the unit ball, so that $\operatorname{Vol}(\mathbb{B}_4) = \frac{\pi^2}{2}$ and:

$$\operatorname{Covol}(I) = [\mathcal{O} : I]\sqrt{\operatorname{disc}(\mathcal{R})} = \operatorname{nrd}(I)^2 p,$$

so that:

$$\frac{p^2}{9\pi^4} \leq \prod_{i=1}^4 q_I(\alpha_i) \leq \frac{64p^2}{\pi^4}.$$

Hence comes the heuristics $q_I(\alpha_i) = O(\sqrt{p})$, which is experimentally verified in [27]. Hence the heuristics $q_I(\delta) = O(m^2 q_I(\alpha_4)) = O(m^2\sqrt{p})$ and the output ideal $I' := I\bar{\delta}/\operatorname{nrd}(I)$ has norm $N := q_I(\delta) = O(m^2\sqrt{p})$
.

We heuristically assume that the distribution of the random variable $q_I(\delta)$ given by sampling integers $a_1, \cdots, a_4 \in [\![-m\ ;\ m]\!]$ is statistically indistinguishable from the uniform distribution on the interval $[\![q_I(\alpha_1)\ ;\ m^2 q_I(\alpha_4)]\!]$, so for m large enough, *e.g.* $m = \lceil \log(p) \rceil$, this interval contains prime numbers. Due to the distribution of prime numbers in $\mathbb{Z}$, $q_I(\delta)$ reaches a prime number after $O(\log(m^2 q_I(\alpha_4))) = O(\log(p))$ operations.

Step b

Since $N = \operatorname{nrd}(I') = \gcd\{\operatorname{nrd}(\alpha) | \alpha \in I'\}$, there exists $\alpha \in I'$ such that $N^2 \nmid \operatorname{nrd}(\alpha)$. Finding such an $\alpha \in I'$ is sufficient. Indeed, in that case, $\alpha \notin \mathcal{R}N$ since $\operatorname{nrd}(\mathcal{R}N) = N^2$, so that $\mathcal{R}N \subsetneq \mathcal{R}N + \mathcal{R}\alpha \subseteq I'$. It follows that $[I' : \mathcal{R}N + \mathcal{R}\alpha] | [I' : \mathcal{R}N]$ and $[I' : \mathcal{R}N + \mathcal{R}\alpha] < [I' : \mathcal{R}N]$ but $[I' : \mathcal{R}N] = \operatorname{nrd}(\mathcal{R}N)^2/\operatorname{nrd}(I')^2 = N^2$ so $[I' : \mathcal{R}N + \mathcal{R}\alpha] \in \{1, N\}$. Since $[I' : \mathcal{R}N + \mathcal{R}\alpha]$ is a square, we must have $[I' : \mathcal{R}N + \mathcal{R}\alpha] = 1$ *i.e.* $I' = \mathcal{R}N + \mathcal{R}\alpha$.

Finding a suitable element α can be done in $O(1)$ sampling operations on a basis of I' with small coefficients (*e.g.* of size $O(\log(p))$). Indeed, by similar combinatoric arguments we gave above, we get that every $\alpha \in I'$ such that $N^2 | \operatorname{nrd}(\alpha)$ are in $\mathcal{R}N$, but $[I' : \mathcal{R}N] = N^2$ so the probability that $N^2 | \operatorname{nrd}(\alpha)$ is negligible.

Step c

We fix S_1 a powersmooth number (actually, other conditions could be required) and look for $\beta_1 \in \mathcal{R}$ of norm NS_1. We restrict to $\beta_1 \in R + jR$ to use the fact that $R^\perp = jR$. Indeed, writing $R = \mathbb{Z}[\omega]$ for a

given generator $\omega \in R$, and writing $\beta_1 = x_1 + \omega y_1 + j(x_2 + \omega y_2)$ with $x_1, y_1, x_2, y_2 \in \mathbb{Z}$, we get that:

$$\mathrm{nrd}(\beta_1) = f(x_1, y_1) + pf(x_2, y_2),$$

where f is the quadratic form $f(x, y) := x^2 - txy + s$ with $t := \mathrm{Tr}(\omega)$ and $s = \mathrm{nrd}(\omega)$, of discriminant $\Delta := t^2 - 4s = \mathrm{disc}(R)$. By choice of ω, we can always assume that $t = -1$ when $\Delta \equiv 1$ [4] and $t = 0$ when $\Delta \equiv 0$ [4], so that f is the principal form.

Let $M := NS_1$. Solving the equation $\mathrm{nrd}(\beta_1) = M$ will be done in two steps: first finding $x_2, y_2 \in \mathbb{Z}$ such that $f(x_1, y_1) = M - pf(x_2, y_2)$ has a solution, and second solve the equation in $x_1, y_1 \in \mathbb{Z}$. The first condition to find a solution is $pf(x_2, y_2) < M$. Let Φ be an increasing function such that $|\Delta| < \Phi(M) < \frac{M}{p}$. To make sure this condition holds, we take S_1 big enough $S_1 = \Omega(\sqrt{p})$, so that $M = \Omega(p)$, and $\Phi(x) = \log(x)^e$, where $e \in \mathbb{N}$ is such that $|\Delta| = o(\log(p)^e)$. We restrict the sampling of x_2, y_2 to the interval $\left[\!\left[-\lfloor\sqrt{\Phi(M)/|\Delta|}\rfloor + 1 \ ; \ \lfloor\sqrt{\Phi(M)/|\Delta|}\rfloor - 1\right]\!\right]$, so that:

$$f(x_2, y_2) = \left(x_2 - \frac{t}{2}y_2\right)^2 + \frac{|\Delta|}{4}y_2^2 < \Phi(M)\left(\frac{1}{|\Delta|}\left(1 - \frac{t}{2}\right)^2 + \frac{1}{4}\right) \leq \Phi(M),$$

since $t \in \{-1, 0\}$ and $|\Delta| \geq 3$, and finally $pf(x_2, y_2) < p\Phi(M) < M$.

To find a solution (x_1, y_1) to the equation :

$$f(x_1, y_1) = M - pf(x_2, y_2) \quad (\star)$$

(and check whether there exists one or not), we use an algorithm introduced in [41, § 46, pp. 73-75] based on Gauss reduction of integer quadratic forms (see Algorithm 2 in Appendix B.1), which is polynomial with the chosen input values. Let $u := M - pf(x_2, y_2)$. Then $(\star)$ admits a solution if and only if Δ is a square mod $4u$ and the form $g_u(x, y) := ux^2 + vxy + wy^2$ is equivalent to f (where $v \in [\![0 \ ; \ 2u]\!]$ is a square root of Δ mod $4u$ and $v^2 - 4uw = \Delta$). Since $\Delta \equiv 0, 1$ [4], the condition Δ is a square mod $4u$ is equivalent to Δ is a square mod u. In order to be able to find a square root v of Δ by Tonelli-Shanks algorithm [28, Algorithm 1.5.1], we require u to be prime. By Dirichlet's arithmetic progression theorem, the density of primes congruent to M mod p is $\frac{1}{p-1}$, which is very close to the density of integers congruent to M mod p (which is $\frac{1}{p}$). Hence, we can heuristically assume that the probability to find $u \in [M - p\Phi(M), M]$ prime is approximately $1/\log(M)$ when we sample x_2, y_2. Assuming the distribution of the class $[g_u]$ among the classes of forms of discriminant Δ is uniform when sampling x_2, y_2, we expect to find a solution after $h(\Delta)\log(M)$ tests, so in a polynomial time since Δ is polynomial and solving $(\star)$ can be done in polynomial time.

Step d

We look for $\beta_2 \in jR$ such that $\alpha \equiv \beta_1\beta_2 \mod \mathcal{R}N$, or equivalently, we look for an equivalence class $[\beta_2] \in jR/\mathcal{R}N$ such that $I'/\mathcal{R}N = (\mathcal{R}/\mathcal{R}N)[\beta_1][\beta_2]$. We have a group action of $(R/NR)^\times$ on the proper non-zero left-ideals of $\mathcal{R}/N\mathcal{R}$ by multiplication on the right. Hence, restricting our search to invertible elements, in order to find $[\beta_2] \in [j](R/NR)^\times$, $I'/N\mathcal{R}$ needs to be in the orbit of $(\mathcal{R}/N\mathcal{R})[\beta_1][j]$.

Lemma B.6. *(i)* $\mathcal{R}/N\mathcal{R} \simeq (R + jR)/N(R + jR) \simeq M_2(\mathbb{Z}/N\mathbb{Z})$.

(ii) The proper non-zero left-ideals of $M_2(\mathbb{Z}/N\mathbb{Z})$ *are all principal and generated by a matrix of the form:*

$$M_{a,b} := \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

with $(a, b) \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$.

Moreover, for $(a, b), (a', b') \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$, *the matrices* $M_{a,b}$ *and* $M_{a',b'}$ *generate the same ideal*

if and only if the equality of classes $(a:b) = (a':b')$ *holds in* $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ $(\exists \lambda \in (\mathbb{Z}/N\mathbb{Z})^*,\ (a,b) = \lambda \cdot (a',b'))$*. Hence, there are* $N+1$ *proper non-zero left-ideals in* $M_2(\mathbb{Z}/N\mathbb{Z})$*.*

(iii) There exists an orbit of at least $N-2$ *elements under the action of* $(R/NR)^\times$ *on proper left-ideals of* $\mathcal{R}/N\mathcal{R}$*.*

Proof. **(i)** We have $B_{p,\infty} \otimes \mathbb{Q}_N \simeq M_2(\mathbb{Q}_N)$ since N does not ramify in $B_{p,\infty}$. Hence, the inclusion $\mathcal{R} \subseteq B_{p,\infty}$ induces an injection $\mathcal{R} \hookrightarrow M_2(\mathbb{Z}_N)$. Taking the quotient modulo N, we get an injection $\mathcal{R}/N\mathcal{R} \hookrightarrow M_2(\mathbb{Z}/N\mathbb{Z})$. But $|\mathcal{R}/N\mathcal{R}| = N^4 = |M_2(\mathbb{Z}/N\mathbb{Z})|$ so $\mathcal{R}/N\mathcal{R} \simeq M_2(\mathbb{Z}/N\mathbb{Z})$.

A similar reasoning ensures that $(R+jR)/N(R+jR) \simeq M_2(\mathbb{Z}/N\mathbb{Z})$ as well.

(ii) Let I be a proper non-zero left-deal of $M_2(\mathbb{Z}/N\mathbb{Z})$. Then I contains a non-zero element M. M has rank 1, otherwise it would be invertible and we would have $I = M_2(\mathbb{Z}/N\mathbb{Z})$, contradicting the properness of I. Since I is a left-ideal, we can change M by left operations. Hence, swapping rows if necessary so that the first is non-zero and eliminating the second, we get M of the desired form $M = M_{a,b}$ for $(a,b) \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$.

If $M' \in I$ is another non-zero matrix of I, we get that $M' = PM_{a',b'}$ for $(a',b') \in (\mathbb{Z}/N\mathbb{Z})^2 \setminus \{0\}$ and $P \in GL_2(\mathbb{Z}/N\mathbb{Z})$. If (a',b') and (a,b) where linearly independent, swapping the rows $M_{a',b'} = P^{-1}M' \in I$ and adding $M_{a,b}$, we get that:

$$\begin{pmatrix} a & b \\ a' & b' \end{pmatrix} \in I \cap GL_2(\mathbb{Z}/N\mathbb{Z}),$$

contradicting the properness of I. Hence $M' = PM_{a',b'} = \lambda P M_{a,b}$ where $\lambda \in (\mathbb{Z}/N\mathbb{Z})^*$ is such that $(a',b') = \lambda \cdot (a,b)$, so I is principal and generated by $M_{a,b}$. We also have obtained that every matrix $M_{a',b'}$ generating I verifies $(a:b) = (a':b')$, completing the proof of point (ii).

(iii) N does not ramify in R since $N \nmid |\operatorname{disc}(R)|$. Indeed, $|\operatorname{disc}(R)|$ is polynomial while $N = \Omega(\sqrt{p})$, according to the heuristics of step c. Hence $(R/NR) \simeq \mathbb{F}_{N^2}$ if N is inert in R and $(R/NR) \simeq (\mathbb{Z}/N\mathbb{Z})^2$ if N splits in R. It follows that $|(R/NR)^\times| \geq (N-1)^2$, so that all elements of $(R/NR)^\times$ are not in $(\mathbb{Z}/N\mathbb{Z})^*$.

Let $[\mu] \in (R/NR)^\times \setminus (\mathbb{Z}/N\mathbb{Z})^*$. Using the isomorphism $\mathcal{R}/N\mathcal{R} \simeq M_2(\mathbb{Z}/N\mathbb{Z})$, we identify $[\mu]$ with a matrix:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}).$$

Let $[\lambda] \in \mathcal{R}/N\mathcal{R}$ corresponding to the matrix $M_{1,0}$. Then, $[\lambda]([\mu]+\nu)$ corresponds to $M_{a+\nu,b}$ for all $\nu \in \mathbb{Z}/N\mathbb{Z}$ but $[\mu]+\nu \in (R/NR)^\times$ if and only if $[\mu]+\nu$ is invertible *i.e.* ν is not a root of the characteristic polynomial of $[\mu]$. So ν can take at least $N-2$ values.Since $\nu \in \mathbb{Z}/N\mathbb{Z} \longmapsto (a+\nu : b) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ is injective, it follows that the orbit of $[\lambda]$ has at least $N-2$ elements. □

By Lemma B.6, $(\mathcal{R}/N\mathcal{R})[\beta_1][j]$ and $I'/N\mathcal{R}$ will be in the same orbit with probability $\geq \frac{N-2}{N+1}$, which is overwhelming so the equation $\alpha \equiv \beta_1\beta_2 \mod \mathcal{R}N$ will almost always admit a solution $\beta_2 \in jR$. If it is not the case, we can always repeat steps b and c. The equation can be solved in polynomial time in $\log(p)$, simply using linear algebra in a $\mathbb{Z}$-basis of $\mathcal{R}$.

Step e

We are looking for $\lambda \in [\![0\ ;\ N-1]\!]$ and $\gamma \in \mathcal{R}$ such that $\beta_2' := \lambda\beta_2 + N\gamma$ has powersmooth norm S_2. We restrict to $\gamma \in R+jR$. Let us write $\beta_2 := j(C+D\omega)$ and $\gamma := a+b\omega+j(c+d\omega)$ with $C,D,a,b,c,d \in \mathbb{Z}$. We want to solve the equation:

$$S_2 = \operatorname{nrd}(\beta_2') = N^2 f(a,b) + pf(\lambda C + Nc, \lambda D + Nd) \quad (\star),$$

where $\lambda, a, b, c, d \in \mathbb{Z}$ are unknown, where $f(x,y) := x^2 - txy + sy^2$ with $t := \operatorname{Tr}(\omega)$ and $s := \operatorname{nrd}(\omega)$.

First, we reduce this equation modulo N: $\lambda^2 pf(C,D) \equiv S_2\ [N]$. This equation has a solution if and only if $pf(C,D)S_2$ is a square modulo N, so we may chose S_2 to ensure it and find $\lambda \not\equiv 0\ [N]$ in time $O(\log^4(N)) = O(\log^4(p))$ by Tonelli-Shanks Algorithm [28, Algorithm 1.5.1].

Now reducing $(\star)$ mod N^2 and factoring by N, we get:

$$\lambda(2C - tD)c + \lambda(2sD - tC)d \equiv \frac{S_2 - \lambda^2 pf(C,D)}{N}\ [N] \quad (\star\star).$$

We have $\lambda \not\equiv 0\ [N]$, and $(2C - tD)(2sD - tC) \not\equiv 0\ [N]$ with overwhelming probability (and if it is the case, we can always repeat steps c and d until this condition is satisfied). As a consequence, the equation above has N solutions modulo N and we can determine all of them in time $O(\log^2(N)) = O(\log^2(p))$ using extended Euclid algorithm. We pick one of them at random satisfying:

$$|\lambda C + Nc| \leq N^2 \qquad \text{and} \qquad |\lambda D + Nd| \leq N^2,$$

so that:

$$f(\lambda C + Nc, \lambda D + Nd) \leq N^2 \left(\left(1 - \frac{t}{2}\right)^2 + \frac{|\Delta|}{4} \right) \leq N^2 \frac{9 + |\Delta|}{4} \leq |\Delta| N^2.$$

To make sure $S_2 - pf(\lambda C + Nc, \lambda D + Nd) > 0$, we may have chosen $S_2 > p|\Delta|N^2$ from the beginning. We repeat the sampling of c, d among the solutions of $(\star\star)$ until $(S_2 - pf(\lambda C + Nc, \lambda D + Nd))/N^2$ is a prime. Assuming the distribution of the random values we get is fairly uniform, we find a prime in approximately $\log(p|\Delta|N^2)$ sampling operations. We then solve:

$$f(a,b) := \frac{S_2 - pf(\lambda C + Nc, \lambda D + Nd)}{N^2},$$

using Algorithm 2. If this equation has no solution, we repeat the sampling again. On the hole, we need $h(\Delta)\log(p|\Delta|N^2) = \tilde{O}(\log(p))$ test to find a solution. Hence, step e is polynomial.

Step f

Let $\beta := \beta_1 \beta_2'$. Then, $\beta \equiv \lambda\beta_1\beta_2 \mod \mathcal{R}N \equiv \lambda\alpha \mod \mathcal{R}N$. Since $\mathcal{R}N \subseteq I'$, it follows that $\beta \in I'$. Hence $J := I'\overline{\beta}/N$ is an integral left-ideal of norm $\mathrm{nrd}(J) = \mathrm{nrd}(\beta)/N = S_1 S_2$ by Lemma B.1, which is powersmooth.

B.3 Effective Deuring correspondence

Given an elliptic curve E_0 of known endomorphism ring $\mathcal{R}_0$ admitting an ℓ-compact representation and a left ideal $I \subseteq \mathcal{R}_0$ of powersmooth norm prime to ℓ, we want to compute the isogeny $\phi_I : E_0 \longrightarrow E$ of kernel $E_0[I]$ defined by Deuring correspondence (see Appendix B.1). The algorithm we present here is due to [44]. The authors chose to present it in the case of Example B.3 ($p \equiv 3\ [4]$, $E_0 : y^2 = x^3 + x$ and $\mathcal{R}_0 = \left\langle 1, j, \frac{i+j}{2}, \frac{1+k}{2} \right\rangle$). Our presentation is simply a generalization.

We write $I := \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4 \rangle$ where the α_i are ℓ-useful and concise, *i.e.* written in an ℓ-useful and concise $\mathbb{Z}$-basis of $\mathcal{R}_0$ (as defined in Paragraph 3.1.1) with coefficients of polynomial size in $\log(p)$. In particular, the α_i can be evaluated in polynomial time in $\log(p)$ at any point of E_0 of order prime to ℓ defined over a field extension of $\mathbb{F}_p$ of polynomial degree in $\log(p)$.

Let us write $\mathrm{nrd}(I) := \prod_{i=1}^r \ell_i^{e_i}$, with $\ell_1, \cdots, \ell_r$ prime numbers $\neq \ell, p$ and $e_1, \cdots, e_r \in \mathbb{N}^*$. We assume that the $\ell_i^{e_i}$ are all bounded by an integer $B \in \mathbb{N}^*$. Since $|\ker(\phi_I)| = \deg(\phi_I) = \mathrm{nrd}(I)$ is exponentially large in $\log(p)$, one cannot describe ϕ_I via its kernel or formulas. The algorithm represents ϕ_I as a chain of isogenies $\phi_i : E_{i-1} \longrightarrow E_i$ for $i \in [\![1\ ;\ r]\!]$ such that $\deg(\phi_i) = \ell_i^{e_i}$ for all $i \in [\![1\ ;\ r]\!]$ and $E_r = E$.

Factoring I by integers if necessary, we may assume that $E[I]$ is cyclic. Then, for all $i \in [\![1\ ;\ r]\!]$, there exists $R_i \in E_0[\ell_i^{e_i}]$ of order $\ell_i^{e_i}$ such that $\alpha_k(R_i) = 0$ for all $k \in [\![1\ ;\ 4]\!]$. Then $\sum_{i=1}^r R_i$ is of E_0 order

$\prod_{i=1}^{r} \ell_i^{e_i} = \mathrm{nrd}(I)$ and in $E_0[I]$ so it generates $E_0[I]$. We may then define the ϕ_i as follows: $\phi_0 := [1]_{E_0}$ and for all $i \in [\![1\ ;\ r]\!]$, $\ker(\phi_i) = \langle \phi_{i-1} \circ \cdots \circ \phi_0(R_i) \rangle$. (using Vélu's formulas [11]). Indeed, by induction, for $i \in [\![1\ ;\ r]\!]$, $\phi_{i-1} \circ \cdots \circ \phi_1(R_i)$ has order $\ell_i^{e_i}$ since $\phi_{i-1} \circ \cdots \circ \phi_0$ has degree $\prod_{j=1}^{i-1} \ell_j^{e_j}$, which is prime to $\ell_i^{e_i}$ so ϕ_i has degree $\ell_i^{e_i}$. Moreover, $\ker(\phi_r \circ \cdots \circ \phi_0) \supseteq \langle \sum_{i=1}^{r} R_i \rangle$ and we have an equality by a degree argument so that $\phi_I = \phi_r \circ \cdots \circ \phi_0$.

Hence, the following algorithm:

Algorithm 4: Effective Deuring correspondence

Data: E_0 an elliptic curve, $\mathcal{R}_0$, an ℓ-compact representation of $\mathrm{End}(E_0)$ and $I \subseteq \mathcal{R}_0$ a left-ideal of powersmooth norm $\mathrm{nrd}(I) = \prod_{i=1}^{r} \ell_i^{e_i}$ prime to ℓ and p, with a concise $\mathbb{Z}$-basis $(\alpha_1, \cdots, \alpha_4)$.

Result: The isogeny associated to I: $\phi_I : E_0 \longrightarrow E$, expressed as a product $\phi_I = \phi_r \circ \cdots \circ \phi_1$, with $\deg(\phi_i) = \ell_i^{e_i}$ for all $i \in [\![1\ ;\ r]\!]$.

$\phi_0 := [1]_{E_0}$;
for $i = 1$ **to** r **do**
  Find (P_i, Q_i), a $\mathbb{Z}/\ell_i^{e_i}\mathbb{Z}$-basis of $E_0[\ell_i^{e_i}]$ using Algorithm 5;
  Find $a, b \in (\mathbb{Z}/\ell_i^{e_i}\mathbb{Z})$ such that $R_i := aP_i + bQ_i$ has order ℓ^i and $\alpha_k(R_i) = 0$ for $k \in [\![1\ ;\ 4]\!]$. This can be done by finding the discrete logarithm of $(\alpha_k(Q_i))_{1 \le k \le 4}$ in the group E_0^4 with basis $(\alpha_k(P_i))_{1 \le k \le 4}$ (in this case $b = 1$), and if it fails, finding the discrete logarithm of $(\alpha_k(P_i))_{1 \le k \le 4}$ with basis $(\alpha_k(Q_i))_{1 \le k \le 4}$ (in this case $a = 1$);
  Compute $S_i := \phi_{i-1} \circ \cdots \circ \phi_0(R_i)$;
  Compute the isogeny $\phi_i : E_{i-1} \longrightarrow E_i$ with kernel $\langle S_i \rangle$ by Vélu's formulas;
end
Return $\phi_1, \cdots, \phi_r$;

Algorithm 5: Computing the basis of a torsion subgroup

Data: $E_0/\mathbb{F}_{p^2}$ an elliptic curve and N a (relatively small) integer prime to p.

Result: A $\mathbb{Z}/N\mathbb{Z}$-basis (P, Q) of $E_0[N]$.

Find a root $x \in \overline{\mathbb{F}_p}$ of the N-th division polynomial $\Psi_N^2(X)$;
Find $y \in \overline{\mathbb{F}_p}$ such that $(x, y) \in E_0$ and set $P := (x, y)$;
Compute order(P);
while *order*$(P) \neq N$ **do**
  Find a **new** root $x \in \overline{\mathbb{F}_p}$ of $\Psi_N^2(X)$;
  Find $y \in \overline{\mathbb{F}_p}$ such that $(x, y) \in E_0$ and set $P := (x, y)$;
  Compute order(P);
end
Find a **new** root $x' \in \overline{\mathbb{F}_p}$ of $\Psi_N^2(X)$;
Find $y' \in \overline{\mathbb{F}_p}$ such that $(x', y') \in E_0$ and set $Q := (x', y')$;
Compute order$(e_N(P, Q))$;
while *order*$(e_N(P, Q)) \neq N$ **do**
  Find a **new** root $x' \in \overline{\mathbb{F}_p}$ of $\Psi_N^2(X)$;
  Find $y' \in \overline{\mathbb{F}_p}$ such that $(x', y') \in E_0$ and set $Q := (x', y')$;
  Compute order$(e_N(P, Q))$;
end
Return (P, Q);

B.4 Discrete logarithm and basis computation in finite abelian groups

In this section, we present some algorithms due to Sutherland [45] to compute discrete logarithms and basis of finite abelian groups, with the intent to apply them to $\mathrm{Cl}(\mathcal{O}_n)$.

The first three paragraphs are general and apply to any finite abelian group. However, the case of $\mathrm{Cl}(\mathcal{O}_n)$ is much simpler because this group is either cyclic of the product of $\mathbb{Z}/\ell\mathbb{Z}$ and a cyclic group.

B.4.1 Discrete logarithm in a basis

Throughout this paragraph, if G is a finite group and $g \in G$, we shall denote by $|g|$ the order of g. If $\mathcal{F} := (g_1, \cdots, g_r) \in G^r$ and $x \in \mathbb{Z}^r$, we shall denote:

$$\mathcal{F}^x := \prod_{i=1}^{r} g_i^{x_i}.$$

Definition B.7. Let G be a finite abelian group. We say that the family $\mathcal{F} := (g_1, \cdots, g_r) \in G^r$ is *free* if for all $x \in \mathbb{Z}^r$, $\prod_{i=1}^r g_i^{x_i} = 1$ if and only if $|g_i||x_i$ for all $i \in [\![1\ ;\ r]\!]$.

A *basis* of G is a free family $\mathcal{B} := (g_1, \cdots, g_r) \in G^r$ generating G. Equivalently, $\mathcal{B}$ is a basis of G if for every element $h \in G$ there exists a unique $x \in \prod_{i=1}^r [\![0\ ;\ |g_i| - 1]\!]$ such that $\mathcal{B}^x = h$.

A basis is *primitive* if it does not contain a trivial element: $g_i \neq 1$ for all $i \in [\![1\ ;\ r]\!]$.

Definition B.8. Let $h \in G$ and $\mathcal{B} := (g_1, \cdots, g_r) \in G^r$ be a basis of G. The *discrete logarithm of h in the basis $\mathcal{B}$*, denoted by $\mathrm{DL}_{\mathcal{B}}(h)$ is the unique tuple $x \in \prod_{i=1}^r [\![0\ ;\ |g_i| - 1]\!]$ (or equivalently, $x \in \prod_{i=1}^r \mathbb{Z}/|g_i|\mathbb{Z}$) such that $\mathcal{B}^x = h$.

Definition B.9. A finite abelian group G is *effective* if:

(i) Given $a, b \in G$, we can compute $a \cdot b \in G$.

(ii) Given $a \in G$, we can compute $a^{-1} \in G$.

(iii) Given $a, b \in G$, we can test whether $a = b$.

(iv) $|G|$ and its decomposition into primes are known.

In the following, we fix an effective finite abelian group G, a basis $\mathcal{B} := (g_1, \cdots, g_r)$ of G and $h \in G$. We present an algorithm to compute $DL_{\mathcal{B}}(h)$. Let $N := |G|$ and its decomposition into primes:

$$N = \prod_{i=1}^{s} p_i^{\alpha_i}.$$

For all $i \in [\![1\ ;\ s]\!]$, let $N_i := \frac{N}{p_i^{\alpha_i}}$ and:

$$G_i := \{g^{N_i} \mid g \in G\}.$$

Lemma B.10. **(i)** *We have two group isomorphisms:*

$$\begin{array}{rcl} \phi : G & \xrightarrow{\sim} & \prod_{i=1}^s G_i \\ g & \longmapsto & (g^{N_i})_{1 \leq i \leq s} \end{array} \quad \text{and} \quad \begin{array}{rcl} \psi : \prod_{i=1}^s G_i & \xrightarrow{\sim} & G \\ (g_i)_{1 \leq i \leq s} & \longmapsto & \prod_{i=1}^s g_i. \end{array}$$

It follows that G_i is the p_i-Sylow subgroup of G for all $i \in [\![1\ ;\ s]\!]$.

(ii) *For $e \in \mathbb{Z}$, let $G^e := \{g^e \mid g \in G\}$ and $\mathcal{B}^{(e)} := (g_1^e, \cdots, g_r^e)$. Then $\mathcal{B}^{(e)}$ is a basis of G^e. In particular, $\mathcal{B}_i := \mathcal{B}^{(N_i)} = (g_1^{N_i}, \cdots, g_r^{N_i})$ is a basis of G_i for all $i \in [\![1\ ;\ s]\!]$.*

(iii) *To compute $x := DL_{\mathcal{B}}(h)$, it suffices to compute $x_i := DL_{\mathcal{B}_i}(h^{N_i})$ for all $i \in [\![1\ ;\ s]\!]$. We then recover each component x_j of x ($j \in [\![1\ ;\ r]\!]$) by the Chinese remainder theorem:*

$$x_j \equiv x_{i,j}\ [p_i^{\alpha_i}].$$

Proof. **(i)** Let $g \in G$ such that $g^{N_i} = 1$ for all $i \in [\![1\ ;\ s]\!]$. Then $|g||N_i$ for all $i \in [\![1\ ;\ s]\!]$. But $\gcd(N_1, \cdots, N_s) = 1$, so that $|g| = 1$ and $g = 1$. Hence ϕ is injective, so $\prod_{i=1}^{s} |G_i| \geq |G|$.

If $(g_i)_{1\leq i\leq s} \in \prod_{i=1}^{s} G_i$ is such that $\prod_{i=1}^{s} g_i = 1$, then we get that $\prod_{j=1}^{s} g_j^{N_i} = g_i^{N_i} = 1$ for all $i \in [\![1\ ;\ s]\!]$, since $|g_j||p_j^{\alpha_j}$ for all $j \in [\![1\ ;\ s]\!]$. Hence $|g_i||N_i$ and $|g_i||p_i^{\alpha_i}$ so $g_i = 1$ because N_i and $p_i^{\alpha_i}$ are coprime. Hence ψ is injective. It follows that $\prod_{i=1}^{s} |G_i| = |G|$ so that ϕ and ψ are isomorphisms.

(ii) Trivially, $\mathcal{B}^{(e)}$ generates G^e and furthermore, if $x \in \mathbb{Z}^t$ is such that ${\mathcal{B}^{(e)}}^x = 1$ then $|g_j||ex_j$ for all $j \in [\![1\ ;\ r]\!]$, since $\mathcal{B}$ is a basis of G, so that $|g_j^e| = |g_j|/\gcd(e, |g_j|)|e/\gcd(e, |g_j|)x_j$. Since $|g_j|/\gcd(e, |g_j|)$ and $e/\gcd(e, |g_j|)$ are coprime, we get that $|g_j^e||x_j$, for all $j \in [\![1\ ;\ r]\!]$. Whence (ii).

(iii) For all $x \in \mathbb{Z}^r$, we have:

$$\mathcal{B}^x = h \Longleftrightarrow \phi(\mathcal{B}^x h^{-1}) = 1 \Longleftrightarrow \forall i \in [\![1\ ;\ s]\!]\,, \quad \mathcal{B}^{N_i x} = \mathcal{B}_i^x = h^{N_i}.$$

By unicity of the discrete logarithm, it follows that for all $i \in [\![1\ ;\ s]\!]$ and $j \in [\![1\ ;\ r]\!]$, we have $x_j \equiv x_{i,j}\ [p_i^{\alpha_i}]$, where $x_i := (x_{i,j})_{1\leq j\leq s} := DL_{\mathcal{B}_i}(h^{N_i})$. □

With the previous lemma, we reduce our computation to the computation of discrete logarithms in p-groups, so we can assume that G is a p-group. Let $e(G)$ be the exponent of G and $\sigma = \sigma(G) := \log_p(e(G))$. We show how to reduce our computation of discrete logarithms in G to the computation of σ discrete logarithms in a p-subgroup of exponent p. Indeed, if $x = (x_1, \cdots, x_r) := \mathrm{DL}_{\mathcal{B}}(h)$, we can write in basis p:

$$\forall i \in [\![1\ ;\ r]\!]\,, \quad x_i := \sum_{k=0}^{\sigma_i - 1} x_{i,\sigma_i-1-k} p^k = \sum_{k=0}^{\sigma_i-1} x_{i,k} p^{\sigma_i-1-k},$$

with $\sigma_i := \log_p(|g_i|) \leq \sigma$ and $x_{i,k} \in [\![0\ ;\ p-1]\!]$ for all $k \in [\![0\ ;\ \sigma_i - 1]\!]$. It follows that for all $l \in [\![0\ ;\ \sigma - 1]\!]$:

$$h^{p^l} = \mathcal{B}^{p^l x} = \prod_{i=1}^{r} g_i^{\sum_{k=0}^{\sigma_i-1} x_{i,\sigma_i-1-k} p^{k+l}} = \prod_{i=1}^{r} g_i^{\sum_{k=0}^{\sigma_i-1} x_{i,k} p^{\sigma_i-1-k+l}} = \prod_{i=1}^{r} g_i^{p^{\sigma_i-1} \sum_{k=0}^{\min(l,\sigma_i-1)} x_{i,k} p^{l-k}},$$

i.e.

$$\underbrace{h^{p^l} \prod_{\substack{1\leq i\leq r \\ l\leq \sigma_i-1}} g_i^{-p^l \sum_{k=0}^{l-1} x_{i,k} p^{\sigma_i-1-k}}}_{h_l} = \prod_{\substack{1\leq i\leq r \\ l\leq \sigma_i-1}} g_i^{p^{\sigma_i-1} x_{i,l}}.$$

Hence, assuming that the x_i are known for $l \geq \sigma_i$ and that the $x_{i,k}$ are known for $l \leq \sigma_i - 1$ and $k \in [\![0\ ;\ l-1]\!]$, we can compute the $x_{i,l}$ for $l \leq \sigma_i - 1$ as:

$$(x_{i,l})_{l\leq\sigma_i-1} := \mathrm{DL}_{\mathcal{C}_l}(h_l),$$

with:

$$\mathcal{C}_l := (g_i^{p^{\sigma_i-1}})_{l\leq\sigma_i-1}.$$

Hence, we reduced to the case where G is a p-group of exponent $e(G) = p$. This can be done in time $O((\sqrt{p}+1)^r)$, for instance with Baby-step, Giant-step algorithm.

Lemma B.11. *Algorithm 6 is correct. This algorithm performs at most:*

$$m^r + 2\left(\left\lfloor \frac{p}{m} \right\rfloor + 1\right)^r - 2r - 3$$

Algorithm 6: Multivariate Baby-step Giant-step in a p-group of exponent p

Data: G an effective abelian p-group of exponent p, a basis $\mathcal{B} := (g_1, \cdots, g_r)$ of G and $h \in G$.
Result: $\mathrm{DL}_{\mathcal{B}}(h)$.
1 Set $m \leftarrow \lceil \sqrt{p} \rceil$;
2 Compute $\prod_{i=1}^{r} g_i^{j_i}$ for all $(j_1, \cdots, j_r) \in [\![0\ ;\ m-1]\!]^r$ and store the result in a hash table;
3 Compute $h \prod_{i=1}^{r} g_i^{mk_i}$ for $(k_1, \cdots, k_r) \in [\![0\ ;\ \lfloor \frac{p}{m} \rfloor]\!]^r$ until we find a collision $h \prod_{i=1}^{r} g_i^{mk_i} = \prod_{i=1}^{r} g_i^{j_i}$ for $(j_1, \cdots, j_r) \in [\![0\ ;\ m-1]\!]^r$;
4 Return $(j_i - mk_i)_{1 \leq i \leq r}$ modulo p;

multiplications and $\left(\lfloor \frac{p}{m} \rfloor + 1\right)^r$ *lookups in a hash table. Hence, assuming the table lookups and group operations have constant cost, the algorithm performs in* $O((\sqrt{p}+1)^r)$.

Proof. To prove the corectness it suffices to prove that a collision is found on line 3, *i.e.* that the indices $j_i - mk_i$ cover $\mathbb{Z}/p\mathbb{Z}$. Since they cover the interval $[\![-m \lfloor \frac{p}{m} \rfloor\ ;\ m-1]\!]$ of cardinality:

$$m \left\lfloor \frac{p}{m} \right\rfloor + m \geq \left(\frac{p}{m} - 1\right) m + m = p,$$

they indeed cover $\mathbb{Z}/p\mathbb{Z}$ and the algorithm is correct.

On line 2, the algorithm computes:

$$S_r := \{ \prod_{i=1}^{r} g_i^{j_i} \mid (j_1, \cdots, j_r) \in [\![0\ ;\ m-1]\!] \}.$$

Let $\mu(S_r)$ the number of multiplications necessary to compute S_r. Knowing S_{r-1}, one can compute S_r by computing $1, g_r, g_r^2, \cdots, g_r^{m-1}$ ($m-2$ multiplications) and multiplying each element of $S_r \setminus \{1\}$ by these elements $((m-1)(|S_{r-1}|-1)$ multiplications). It follows that:

$$\mu(S_r) = (m-1)(|S_{r-1}|-1)+m-2+\mu(S_{r-1}) = (m-1)(m^{r-1}-1)+m-2+\mu(S_{r-1}) = (m-1)m^{r-1}-1+\mu(S_{r-1}).$$

Since $\mu(S_1) = m-2$, it follows that:

$$\mu(S_r) = \sum_{k=1}^{r-1} ((m-1)m^k - 1) + m - 2 = m(m^{r-1}-1) - (r-1) + m - 2 = m^r - r - 1.$$

Similarly, computing $\prod_{i=1}^{r} g_i^{mk_i}$ for all $(k_1, \cdots, k_r) \in [\![0\ ;\ \lfloor \frac{p}{m} \rfloor]\!]^r$ requires:

$$\left(\left\lfloor \frac{p}{m} \right\rfloor + 1\right)^r - r - 1$$

multiplications. Taking into account the multiplications by h, we get:

$$\left(\left\lfloor \frac{p}{m} \right\rfloor + 1\right)^r - r - 1 + \left(\left\lfloor \frac{p}{m} \right\rfloor + 1\right)^r - 1 = 2\left(\left\lfloor \frac{p}{m} \right\rfloor + 1\right)^r - r - 2$$

multiplications in line 3. We also have as many table lookups as elements computed in line 3, hence $\left(\lfloor \frac{p}{m} \rfloor + 1\right)^r$ table lookups. This completes the proof. □

Assuming again that G is general (not a p group), the following algorithm computes the discrete logarithm $\mathrm{DL}_{\mathcal{B}}(h)$ in G.

Proposition B.12. *Algorithm 7 is correct and computes* $DL_{\mathcal{B}}(h)$ *with:*

$$O\left(\sum_{i=1}^{s} \sigma_i((\sqrt{p_i}+1)^r + r\log(N)) + rs\log^2(N)\right)$$

Algorithm 7: Multivariate discrete logarithm in an effective finite abelian group

Data: G an effective abelian group, $N := |G|$ and its decomposition into primes $N := \prod_{i=1}^{s} p_i^{\alpha_i}$, a basis $\mathcal{B} := (g_1, \cdots, g_r)$ of G and $h \in G$.
Result: $\mathrm{DL}_{\mathcal{B}}(h)$.

1 **for** $i = 1$ **to** s **do**
2 $\quad N_i \leftarrow \frac{N}{p_i^{\alpha_i}}$;
3 $\quad \mathcal{B}_i = (b_1, \cdots, b_r) \leftarrow (g_1^{N_i}, \cdots, g_r^{N_i})$;
4 $\quad h_i \leftarrow h^{N_i}$;
5 $\quad$ **for** $j = 1$ **to** r **do**
6 $\quad\quad \sigma_{i,j} \leftarrow \log_{p_i} |g_j^{N_i}|$;
7 $\quad$ **end**
8 $\quad \sigma_i \leftarrow \max_{1 \le i \le r} \sigma_{i,j}$;
9 $\quad x_i \leftarrow (0)_{1 \le j \le r}$;
10 $\quad$ **for** $l = \sigma_i - 1$ **to** 0 **do**
11 $\quad\quad h_{i,l} \leftarrow h_i^{p^l} \prod^{r}_{\substack{1 \le j \le r \\ l \le \sigma_{i,j} - 1}} b_j^{-p_i^l x_{i,j}}$;
12 $\quad\quad \mathcal{C}_{i,l} \leftarrow (b_j^{p_i^{\sigma_i - 1}})_{\substack{1 \le j \le r \\ l \le \sigma_{i,j} - 1}}$;
13 $\quad\quad y \leftarrow DL_{\mathcal{C}_{i,l}}(h_{i,l})$ (using Algorithm 6);
14 $\quad\quad (x_{i,j})_{\substack{1 \le j \le r \\ l \le \sigma_{i,j} - 1}} \leftarrow (x_{i,j} + p_i^{\sigma_{i,j} - 1 - l} y_j)_{\substack{1 \le j \le r \\ l \le \sigma_{i,j} - 1}}$;
15 $\quad$ **end**
16 **end**
17 Compute $x \in \prod_{j=1}^{r} [\![0 \ ; \ |g_j| - 1]\!]$ such that $x_j \equiv x_{i,j} [p_i^{\alpha_i}]$ for all $i \in [\![1 \ ; \ s]\!]$ and $j \in [\![1 \ ; \ r]\!]$ using Chinese remainder theorem [28, Algorithm 1.3.12];
18 Return x;

elementary operations, where $N := |G| = \prod_{i=1}^{s} p_i^{\alpha_i}$ and σ_i is the logarithm in basis p_i of the exponent of the p_i-Sylow of G for all $i \in [\![1 \ ; \ s]\!]$.

Proof. The correctness follows directly from what we explained above.

For the complexity, we count the operations line by line. Line 2 is negligible, lines 3 and 4 require $r+1$ exponentiations by N_i, that can be performed with $\log(N_i)$ multiplications for all $i \in [\![1 \ ; \ s]\!]$. Hence, line 3 and 4 cost:

$$O\left((r+1)\sum_{i=1}^{s} \log(N_i)\right)$$

multiplications. Computing the exponents on line 6 requires at most $\sigma_i r$ exponentiations by p_i for all $i \in [\![1 \ ; \ s]\!]$, for a total cost of:

$$O\left(r\sum_{i=1}^{s} \sigma_i \log(p_i)\right)$$

multiplications. Line 11 requires at most r exponentiations of order of magnitude $p_i^{\sigma_i}$, r multiplications and an exponentiation by p_i^l for all $i \in [\![1 \ ; \ s]\!]$ and $l \in [\![0 \ ; \ \sigma_i - 1]\!]$, for a total cost of:

$$O\left(\sum_{i=1}^{s}\sum_{l=0}^{\sigma_i - 1} (r\sigma_i \log(p_i) + l\log(p_i) + r)\right) = O\left(rs\sum_{i=1}^{s} \sigma_i(1 + \sigma_i \log(p_i)) + \sum_{i=1}^{s} \frac{\sigma_i(\sigma_i - 1)}{2} \log(p_i)\right)$$

multiplications. The $\mathcal{C}_{i,l}$ on line 12 can be computed outside of the loop on l and inside the loop on i for a total cost of:

$$O\left(r\sum_{i=1}^{s} (\sigma_i - 1)\log(p_i)\right)$$

multiplications. Line 13 requires the computation of a discrete logarithm in p_i-group of exponent p_i, whose complexity is $O(\sqrt{p_i} + 1)^r)$ (by Lemma B.11) for all $i \in [\![1 \ ; \ s]\!]$ and $j \in [\![0 \ ; \ \sigma_i - 1]\!]$, for a total

cost of:

$$O\left(\sum_{i=1}^{s} \sigma_i(\sqrt{p_i}+1)^r\right)$$

elementary operations. Line 14 is negligible. Finally, line 17 requires the computation of r Chinese remainders with s variable integers of order of magnitude N, using Algorithm [28, Algorithm 1.3.12], hence applying rs times extended Euclid's algorithm for a total cost of $O(rs\log^2(N))$. Taking the dominant terms into account only, we get the announced time complexity. □

B.4.2 Basis computation from a generating set

Let us recall the notations of the previous paragraph: let G be an effective finite abelian group, $N := |G|$ and its decomposition into primes $N = \prod_{i=1}^{s} p_i^{\alpha_i}$. For all $i \in [\![1\ ;\ s]\!]$, let $N_i := \frac{N}{p_i^{\alpha_i}}$ and $G_i := \{g^{N_i} \mid g \in G\}$.

Lemma B.13. **(i)** *Let $S := \{s_1, \cdots, s_t\}$ be a generating set of G. Then, for all $i \in [\![1\ ;\ s]\!]$, $S^{(N_i)} := \{s_1^{N_i}, \cdots, s_t^{N_i}\}$ generates G_i.*

(ii) *Let $\mathcal{B}_i$ be a basis of G_i for all $i \in [\![1\ ;\ s]\!]$. Then, $\mathcal{B} := \bigvee_{i=1}^{r} \mathcal{B}_i$, the concatenation of the $\mathcal{B}_i$, is a basis of G.*

(iii) *If G is a p-group G, then all of its basis have the same cardinality, which is called the* rank *of G.*

Proof. **(i)** Trivial.

(ii) It follows directly from the fact that:

$$\begin{array}{rcl} \psi : \prod_{i=1}^{s} G_i & \xrightarrow{\sim} & G \\ (g_i)_{1\leq i\leq s} & \longmapsto & \prod_{i=1}^{s} g_i. \end{array}$$

is an isomorphism, as proved in point (i) of Lemma B.10.

(iii) Let $\mathcal{B} := \{g_1, \cdots, g_r\}$ be a primitive basis of G. Then, all the orders $|g_i|$ are non-trivial powers of p.Without loss of generality, we can reorder the g_i, so that $|g_1|| \cdots ||g_r|$ and we trivially have:

$$G \simeq \prod_{i=1}^{r} (\mathbb{Z}/|g_i|\mathbb{Z})$$

via the isomorphism $x \in \prod_{i=1}^{r}(\mathbb{Z}/|g_i|\mathbb{Z}) \longmapsto \mathcal{B}^x \in G$. Hence, $|g_1|, \cdots, |g_r|$ are the invariant factors of G so there are unique and in particular, their number is fixed and depends only on G. □

The previous lemma indicates that it suffices to find basis of the p_i-Sylow subgroups G_i of G to compute a basis of G. In the following, we assume that G is a p-group.

Definition B.14. Let $\mathcal{B} := (g_1, \cdots, g_r)$ be a free family of G and $h \in G$. We denote by $\mathrm{DL}^*_{\mathcal{B}}(h)$ the tuple $(x, e) \in \mathbb{Z}^u \times \mathbb{Z}$ such that $e \in \mathbb{N}$ is the smallest integer such that $h^{p^e} \in \langle \mathcal{B}^{(p^e)} \rangle = \langle g_1^{p^e}, \cdots, g_r^{p^e} \rangle$ and $x := \mathrm{DL}_{\mathcal{B}^{(p^e)}}(h^{p^e})$, so that $h^{p^e} = \mathcal{B}^{p^e x}$.

Lemma B.15. *Let $\mathcal{B} := (g_1, \cdots, g_r)$ be a free family of G, $n_i := \log_p(|g_i|)$ for all $i \in [\![1\ ;\ r]\!]$, $m_0 := \min_{1\leq i\leq r} n_i$, $m := \max_{1\leq i\leq r} n_i$, $(x, e) := \mathrm{DL}^*_{\mathcal{B}}(h)$ and $h' := h\mathcal{B}^{-x}$. Suppose that $|h| \leq p^m$. Then:*

(i) *$|h'| = p^e$.*

(ii) *If furthermore $|h'| \leq p^{m_0}$, then $\mathcal{B}' := \mathcal{B} \vee (h')$ is a free family.*

Proof. **(i)** By the definition of $\mathrm{DL}^*_{\mathcal{B}}(h)$, we have $h^{p^e} = \mathcal{B}^{p^e x}$, so that $h'^{p^e} = (h\mathcal{B}^{-x})^{p^e} = 1$. If $h'^{p^{e'}} = 1$ for $e' < e$, then we would have $h^{p^{e'}} = \mathcal{B}^{p^{e'} x}$ and e would not be minimal for this equality. Hence, $|h'| = p^e$.

(ii) We assume that $|h'| \leq p^{m_0}$ and that $\mathcal{B}' := \mathcal{B} \vee (h')$ is not free. Then, we have a non-trivial relation $h'^k = \mathcal{B}^y$ for $k \in \mathbb{Z} \setminus \{0\}$ and $y \in \mathbb{Z}^r \setminus \{0\}$. Let us write $k := k'p^f$ with $k \in \mathbb{Z} \setminus \{0\}$ and $f \in [\![0\ ;\ e-1]\!]$ such that $\gcd(k', p) = 1$. Let l be an inverse of k' modulo p^{e-f}. Then, we get $h'^{p^f} = \mathcal{B}^z$ with $z := ly$.

$p^f \nmid z$. Indeed, otherwise, set $v := x + z/p^f$. Then:

$$h^{p^f} = (h'\mathcal{B}^x)^{p^f} = \mathcal{B}^{z+p^f x} = \mathcal{B}^{p^f v},$$

but $f < e$, so it contradicts the minimality of e.Hence, $p^f \nmid z$.

We also have $m_0 \geq e > f$ since $|h'| \leq p^{m_0}$, so that:

$$1 = h'^{p^{m_0}} = \mathcal{B}^{p^{m_0-f}z}$$

and consequently, $p^{n_i} | p^{m_0-f} z_i$ so $p^{m_0} | p^{m_0-f} z_i$ and $p^f | z_i$ for all $i \in [\![1\ ;\ r]\!]$. Contradiction. Hence, $\mathcal{B}'$ is free. □

Our basis computation algorithm follows from the previous lemma. Assume that we already have constructed the free family $\mathcal{B} := (g_1, \cdots, g_r)$ and that we have a generating set $S := \{s_1, \cdots, s_t\}$ (that is not free in general) such that $\langle \mathcal{B} \cup S \rangle = G$. We assume that $|s_i| \leq p^{m_0}$ for all $i \in [\![1\ ;\ t]\!]$. Let $(x_i, e_i) := \mathrm{DL}^*_{\mathcal{B}}(s_i)$ for all $i \in [\![1\ ;\ t]\!]$. Then, $e_i \leq \log_p(|s_i|) \leq m_0$ and $s'_i := s_i \mathcal{B}^{-x_i}$ has order e_i for all $i \in [\![1\ ;\ t]\!]$. We select $i_0 \in [\![1\ ;\ t]\!]$ such that e_{i_0} is maximal, set $g_{r+1} := s'_{i_0}$, $\mathcal{B}' := \mathcal{B} \vee (g_{r+1})$ and $S' := \{s'_1, \cdots, s'_t\} \setminus \{s'_{i_0}\}$. Then, $\mathcal{B}'$ is still free by point (ii) of the lemma, we still have $\langle \mathcal{B}' \cup S' \rangle = G$ and $\log_p(|s'_i|) = e_i \leq \min(m_0, e_{i_0})$ so that our invariants from the beginning are still satisfied with $\mathcal{B}'$ and S'.

Applying these principles, we can compute a basis from a generating set using the following algorithm due to [45].

Algorithm 8: Basis computation in a p-group.

Data: G an effective abelian p-group, a generating set of G, $S := \{s_1, \cdots, s_t\}$.
Result: A primitive basis of G: $\mathcal{B} := (g_1, \cdots, g_r)$.

$\mathcal{B} \leftarrow \emptyset$;
$e_i \leftarrow \log_p(|s_i|)$ for all $i \in [\![1\ ;\ t]\!]$;
if $\forall i \in [\![1\ ;\ t]\!],\ e_i = 0$ **then**
  Return $\mathcal{B}$;
else
  $i_0 \leftarrow \mathrm{argmax}_{1 \leq i \leq t} e_i$;
  $\mathcal{B} \leftarrow \mathcal{B} \vee (s_{i_0})$;
  $S \leftarrow S \setminus \{s_{i_0}\}$ and $t \leftarrow |S|$;
end
while $t \neq 0$ *and* $\max_{1 \leq i \leq t} e_i > 0$ **do**
  for $i := 1$ **to** t, $e_i > 0$ **do**
    $(x_i, e_i) \leftarrow \mathrm{DL}^*_{\mathcal{B}}(s_i)$ (try to compute $\mathrm{DL}_{\mathcal{B}^{(p^e)}}(h^{p^e})$ for $e := 0$ to e_i using Algorithm 7 until the computation succeeds);
    $s_i \leftarrow s_i \mathcal{B}^{-x_i}$;
  end
  if $\forall i \in [\![1\ ;\ t]\!],\ e_i = 0$ **then**
    Return $\mathcal{B}$;
  else
    $i_0 \leftarrow \mathrm{argmax}_{1 \leq i \leq t} e_i$;
    $\mathcal{B} \leftarrow \mathcal{B} \vee (s_{i_0})$;
    $S \leftarrow S \setminus \{s_{i_0}\}$ and $t \leftarrow |S|$;
  end
end
Return $\mathcal{B}$;

Proposition B.16. *Algorithm 8 terminates and is correct. It performs:*

$$O(t^2(\sigma^2(\sqrt{p}+1)^r + \sigma r n^2 \log^2(p)))$$

elementary operations, where $t := |S|$, p^σ is the exponent of G, $|G| = p^n$ and r is the rank of G.

Proof. The algorithm terminates because the number of elements in S decreases at each iteration of the loop, unless all the e_i are zero in which case the termination is immediate. As explained above, the algorithm respects the following loop invariant: $\mathcal{B}$ is a free family, $\langle \mathcal{B} \cup S \rangle = G$ and the orders of the element of S are smaller than all the orders of elements of $\mathcal{B}$. When the algorithm terminates, S is either empty or equal to $\{1\}$, so $\mathcal{B}$ generates G and is a basis. Hence, the algorithm is correct.

Now, we compute the complexity. The order computation on line 2 requires at most $t\sigma$ exponentiations by p, each of them costing $O(\log(p))$ group multiplications, for a total cost of $O(t\sigma \log(p))$.Operations on lines 3 to 9 are negligible. The while loop is executed at most t times (t being the initial cardinality of $|S|$ here). At the j-th iterations of the while loop, we have $|S| \leq t - j$ so we execute lines 12 and 13 at most $t - j$ times. Everytime it is executed, line 12 requires at most σ computations of the discrete logarithm in a p-group with a basis of r elements so we have a complexity of:

$$O(\sigma^2((\sqrt{p}+1)^r + r\log(|G|)) + \sigma r \log^2(|G|)) = O(\sigma^2(\sqrt{p}+1)^r + \sigma r n^2 \log^2(p)),$$

using Algorithm 7. Everytime line 13 is executed, j exponentiations and j multiplications are performed, for a cost of $O(j(\sigma \log(p) + 1))$. Hence, the total cost of line 12 and 13 (counting the number of times they are executed) is:

$$\begin{aligned} &O\left((\sigma^2(\sqrt{p}+1)^r + \sigma r n^2 \log^2(p)) \sum_{j=1}^{t} (t-j) + (\sigma \log(p) + 1) \sum_{j=1}^{t} j\right) \\ &= O(t^2(\sigma^2(\sqrt{p}+1)^r + \sigma r n^2 \log^2(p))) \end{aligned}$$

The time complexity of the algorithm follows. □

B.4.3 Specialization to the case of the ideal class group $\mathrm{Cl}(\mathcal{O}_n)$

By Theorem A.15, $\mathrm{Cl}(\mathcal{O}_n)$ is either cyclic or of the form $(\mathbb{Z}/\ell\mathbb{Z}) \times (\mathbb{Z}/h_{n-1}\mathbb{Z})$ with $h_{n-1} := |\mathrm{Cl}(\mathcal{O}_{n-1})|$.

We want to find a basis of $\mathrm{Cl}(\mathcal{O}_n)$ given the generating set $S := \{[\mathfrak{q}_1], \cdots, [\mathfrak{q}_t]\}$. In that case, we do not need to use Sutherland's algorithm (Algorithm 8). First, we compute all the orders of the $[\mathfrak{q}_j]$. Then, we build $g_1 \in \mathrm{Cl}(\mathcal{O}_n)$ whose order is $|g_1| = \mathrm{lcm}_{1 \leq j \leq t} |[\mathfrak{q}_j]|$ (the exponent of $\mathrm{Cl}(\mathcal{O}_n)$). In general, one of the $[\mathfrak{q}_j]$ will convene. Otherwise, we may take the product of all the $[\mathfrak{q}_j]$.

If $\mathrm{Cl}(\mathcal{O}_n)$ is cyclic, then g_1 is a generator and we are done. Otherwise, $|g_1| = h_{n-1}$ and to find a basis of $\mathrm{Cl}(\mathcal{O}_n)$, it suffices to find $g_2 \notin \langle g_1 \rangle$ of order ℓ. We simply try to compute the discrete logarithm of $[\mathfrak{q}_j]$ with respect to g_1 with Algorithm 7 (for $r = 1$) and stops when it fails. If it fails for $j \in [\![1\ ;\ t]\!]$, we must have $[\mathfrak{q}_j]^\ell \in \langle g_1 \rangle$ so we find the discrete logarithm $k := DL_{g_1}([\mathfrak{q}_j]^\ell)$. Since $\mathrm{Cl}(\mathcal{O}_n)$ has exponent h_{n-1}, we must have $g_1^{kh_{n-1}/\ell} = [\mathfrak{q}_j]^{h_{n-1}} = [1]$, so that $h_{n-1} | kh_{n-1}/\ell$ *i.e.* $\ell | k$. Set $k' := k/\ell$ and $g_2 := [\mathfrak{q}_j] g_1^{-k'}$. Then g_2 is convenient.

Lemma B.17. *Assume that $h(\mathcal{O}_K) = 1$ and that ℓ is relatively small. Then, given a generating set of $\mathrm{Cl}(\mathcal{O}_n)$ with t elements, one can compute a basis in time $O(tn^2)$ in the worst case.*

Proof. To compute the orders of the $[\mathfrak{q}_j]$, one only has to compute their exponentiation by all the divisors of $h_n = |\mathrm{Cl}(\mathcal{O}_n)|$. Since $h_n = \frac{\ell^{n-1}}{[\mathcal{O}_K^\times : \mathcal{O}_1^\times]} \left(\ell - \left(\frac{\Delta_K}{\ell}\right)\right)$, there are $O(n)$ such divisors and each exponentiation takes $O(\log(h_n)) = O(n)$ operations. Hence, the total cost of this step is $O(tn^2)$.

Computing g_1 costs $O(t)$ operation in the worst case (multiplying all the $[\mathfrak{q}_j]$).

Computing a discrete logarithm by Algorithm 7 costs $O(n^2)$ and there are $t+1$ such discrete logarithms to compute in the worst case. The total complexity follows. □

B.5 Lattice of relations of a finite abelian group

Given a finite abelian group G and a generating set $S = \{s_1, \cdots, s_t\}$ of G, we want to compute a $\mathbb{Z}$-basis of the following lattice:

$$L = \left\{ (e_1, \cdots, e_t) \in \mathbb{Z}^t \;\middle|\; \prod_{j=1}^{t} s_j^{e_j} = 1 \right\}.$$

Using Algorithm 8, we can compute a basis $\mathcal{B} := (g_1, \cdots, g_r)$ of G and then use Algorithm 7 to compute the discrete logarithm $x_j := \mathrm{DL}_{\mathcal{B}}(s_j)$ for all $j \in [\![1 \ ; \ t]\!]$.

We then have for all $e \in \mathbb{Z}^t$:

$$\begin{aligned} e \in L &\iff \prod_{j=1}^{t} s_j^{e_j} = 1 \iff \mathcal{B}^{\sum_{j=1}^{t} e_j x_j} = 1 \iff \forall k \in [\![1 \ ; \ r]\!], \quad \sum_{j=1}^{t} e_j x_{j,k} \equiv 0 \ [|g_k|] \\ &\iff X_k \cdot e \equiv 0 \ [|g_k|] \end{aligned}$$

with $X_k := (x_{j,k})_{1 \leq j \leq t}$, seen as a line vector for all $k \in [\![1 \ ; \ r]\!]$ and e seen as a column vector.Hence:

$$L = \bigcap_{k=1}^{r} L_k,$$

with $L_k := \{e \in \mathbb{Z}^t \mid X_k \cdot e \equiv 0 \ [|g_k|]\}$ for all $k \in [\![1 \ ; \ r]\!]$. To compute L, it is useful to introduce dual lattices.

Definition B.18. Let $\Lambda \subset \mathbb{R}^d$ be a full-rank lattice. Then, the *dual lattice* of Λ, denoted by Λ^* is the lattice:

$$\Lambda^* := \{x \in \mathbb{R}^d \mid \forall y \in \Lambda, \quad \langle x, y \rangle \in \mathbb{Z}\},$$

where $\langle ., . \rangle$ is the usual scalar product.

Lemma B.19. *Let $\Lambda, \Lambda_1, \cdots, \Lambda_r \subset \mathbb{R}^d$ be full-rank lattices. Then:*

(i) *If B is a $\mathbb{Z}$-basis of Λ, then $(B^T)^{-1}$ is a $\mathbb{Z}$-basis of Λ^*.*

(ii) $\Lambda^{**} = \Lambda$.

(iii) *Suppose that $\bigcap_{k=1}^{r} \Lambda_k$ has full-rank. Then $\left(\bigcap_{k=1}^{r} \Lambda_k\right)^* = \sum_{k=1}^{r} \Lambda_k^*$.*

Proof. **(i)** Let us write $B = (b_1 | \cdots | b_d)$ and $(B^T)^{-1} = (b_1^* | \cdots | b_d^*)$ in columns. Then, for all $i, j \in [\![1 \ ; \ d]\!]$, we have:

$$\langle b_i^*, b_j \rangle = b_i^T \cdot b_j = (B^{-1} \cdot B)_{i,j} = \delta_{i,j} \in \mathbb{Z}.$$

It follows that Λ^* contains $(B^T)^{-1}$. Conversely, let $x \in \Lambda^*$. Since $(B^T)^{-1}$ is invertible, the b_i^* form a $\mathbb{R}$-basis of $\mathbb{R}^d$ so we can write $x = \sum_{i=1}^{d} x_i b_i^*$ with $x_1, \cdots, x_d \in \mathbb{R}$. Hence, for all $j \in [\![1 \ ; \ d]\!]$:

$$\langle x, b_j \rangle = \sum_{i=1}^{d} x_i \langle b_i^*, b_j \rangle = \sum_{i=1}^{d} x_i \delta_{i,j} = x_j \in \mathbb{Z},$$

so x is an integer linear combination of the b_i^* and $(B^T)^{-1}$ is indeed a basis of Λ^*.

(ii) It follows immediately from (i).

(iii) By (ii), it suffices to prove that $\bigcap_{k=1}^{r} \Lambda_k = (\sum_{k=1}^{r} \Lambda_k^*)^*$. Let $x \in \mathbb{R}^d$. Then, we have:

$$x \in \bigcap_{k=1}^{r} \Lambda_k \iff \forall k \in [\![1\ ;\ r]\!], \forall y \in \Lambda_k^*,\ \langle x, y\rangle \in \mathbb{Z} \iff \forall y \in \sum_{k=1}^{r} \Lambda_k^*,\ \langle x, y\rangle \in \mathbb{Z} \iff x \in \left(\sum_{k=1}^{r} \Lambda_k^*\right)^*.$$

The result follows. □

L has full rank since $G \simeq \mathbb{Z}^t/L$ is finite so we may apply point (iii) of the previous lemma to get:

$$L^* = \sum_{k=1}^{r} L_k^*.$$

Hence, it suffices to obtain generating families of the lattices L_k^* to obtain a generating family of L^*. We then compute the HNF of the matrix of this generating family to obtain a basis C of L^*. We the easily obtain a basis $B := (C^T)^{-1}$ of L.

Actually, the following lemma ensures that $L_k^* = |g_k|^{-1}(\mathbb{Z} \cdot X_k^T + |g_k|\mathbb{Z}^t)$, so we can apply this method to determine B.

Lemma B.20. *Let $v \in \mathbb{Z}^d$, $q \in \mathbb{N}^*$,*

$$\Lambda_q^{\perp}(v) = \{x \in \mathbb{Z}^d \mid \langle v, x\rangle \equiv 0\ [q]\} \quad \textit{and} \quad \Lambda_q(v) = \{y \in \mathbb{Z}^d \mid \exists \lambda \in \mathbb{Z}, \quad y \equiv \lambda \cdot v\ [q]\}.$$

Then $\Lambda_q^{\perp}(v)^* = q^{-1}\Lambda_q(v)$.

Proof. By Lemma B.19, points (i) and (ii), it suffices to prove that $\Lambda_q(v)^* = q\Lambda_q^{\perp}(v)$. Let $x \in \mathbb{Z}^d$.Then:

$$\begin{aligned} x \in \Lambda_q(v)^* &\iff x \in (\mathbb{Z} \cdot v + q\mathbb{Z}^d)^* \iff \langle v, x\rangle \in \mathbb{Z} \quad \text{and} \quad \forall y \in \mathbb{Z}^d, \quad \langle qy, x\rangle \in \mathbb{Z} \\ &\iff \exists x' \in \mathbb{Z}^d, \quad x = \frac{1}{q}x' \quad \text{and} \quad \langle v, x'\rangle \equiv 0\ [q] \iff x \in q^{-1}\Lambda_q^{\perp}(v) \end{aligned}$$

This completes the proof. □

Algorithm 9: Relation lattice basis computation.

Data: G an effective abelian group, a generating set of G, $S := \{s_1, \cdots, s_t\}$ and a basis of G, $\mathcal{B} = (g_1, \cdots, g_r)$ (computed with Algorithm 8 for instance).
Result: A basis of the relations lattice $L := \{(e_1, \cdots, e_t) \in \mathbb{Z}^t \mid \prod_{j=1}^{t} s_j^{e_j} = 1\}$.

$x_j := (x_{j,k})_{1 \le k \le r} \leftarrow \mathrm{DL}_{\mathcal{B}}(s_j)$ for $j \in [\![1\ ;\ t]\!]$;
$X_k \leftarrow (x_{j,k})_{1 \le j \le t}$ for all $k \in [\![1\ ;\ r]\!]$;
$m \leftarrow \mathrm{lcm}(|g_j|)_{1 \le j \le t}$;
$M \leftarrow \left(m/|g_1|X_1^T| \cdots |m/|g_r|X_r^T|mI_t\right) \in M_{t,t+r}(\mathbb{Z})$;
$M' \leftarrow HNF(M)$ using [28, Algorithm 2.4.4];
$C \leftarrow (M'_{i,j})_{\substack{1 \le i \le t \\ r+1 \le j \le r+t}}$;
$B \leftarrow m(C^T)^{-1}$;
Return B;

B.6 Kuperberg's algorithm

The presentation of this section follows Kuperberg's foundational article [14]. Let us consider a finite abelian group G with multiplicative law. We define the *dehedral group* associated to G as the semi-direct product:

$$D_G := G \rtimes_{\phi} (\mathbb{Z}/2\mathbb{Z}),$$

with $\phi : \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Aut}(G)$ given by $\phi(1)(g) := g^{-1}$ for all $g \in G$, so that D_G is the set $G \times (\mathbb{Z}/2\mathbb{Z})$ with inner product given by:

$$\forall g, g' \in G, \epsilon, \epsilon' \in (\mathbb{Z}/2\mathbb{Z}), \quad (g, \epsilon) \cdot (g', \epsilon') = (g\phi(\epsilon)(g'), \epsilon + \epsilon') = (gg'^{-\epsilon}, \epsilon + \epsilon').$$

When G is cyclic of order N, D_G is isomorphic to the *dihedral group of order N* denoted by D_N generated by a *reflection* y (of order 2) and a *rotation* x (of order N) related by $yxyx = 1$. Elements of $\langle x \rangle$ are called rotations and the others are called reflections. Similarly, when G is not cyclic, we can set $y := (1, 1)$ whose order is 2 and embed G in D_G, so that D_G is generated by y and G and for all $g \in G$, $ygyg = 1$. Elements of G are called are called rotations and the others are called reflections. y is called the *standard reflection* but actually, any other reflection y' satisfies $y'gy'g = 1$ for all $g \in G$ and $\langle y' \rangle \cdot G = D_G$.

Problem B.21 (Hidden Shift Problem)**.** Let G be a group. Given $f, g : G \longrightarrow S$ two injective functions such that there exists $s \in G$ such that $g(x) = f(sx)$ for all $x \in G$, the problem is to determine s.

Problem B.22 (Hidden Subgroup Problem)**.** Let G be a group. Given $f : G \longrightarrow S$ a function such that there exists an unknown subgroup $H \subseteq G$ satisfying:

$$\forall x, y \in G, \quad f(x) = f(y) \Longleftrightarrow y \in Hx,$$

hence, inducing an injective map $G/H \longrightarrow S$, the problem is to determine H.

Problem B.23 (Hidden Reflection Problem)**.** Hidden reflection problem is a particular case of the hidden subgroup problem when G is dihedral and H is generated by a reflection.

Lemma B.24. *The hidden subgroup problem in a finite abelian group G is equivalent to the hidden reflection problem in the dihedral group D_G.*

Proof. Let $f, g : G \longrightarrow S$ two injective functions such that there exists $s \in G$ such that $g(x) = f(sx)$ for all $x \in G$. Let $h : D_G \longrightarrow S$ defined as follows:

$$\forall x \in G, \quad h(x) := f(x) \quad \text{and} \quad h(yx) := g(x).$$

It follows that for all $u, v \in D_G$, $h(u) = h(v) \Longleftrightarrow v \in Hu$ with $H := \langle ys^{-1} \rangle$.

Conversely, let $h : D_G \longrightarrow S$ inducing an injective map $D_G/H \longrightarrow S$ where H is generated by a reflection $y' \in D_G$, that we may write $y' := ys^{-1}$ with $s \in G$. Then, let $f, g : G \longrightarrow S$ given by:

$$\forall x \in G, \quad f(x) := h(x) \quad \text{and} \quad g(x) := h(yx).$$

Then, f and g are injective and $g(x) = f(sx)$ for all $x \in G$. □

Hence, in the latter, we explain how to solve the hidden reflection problem.We start our explanation for G cyclic: $G \simeq \mathbb{Z}/N\mathbb{Z}$. We shall then explain how the general case reduces to this case.

B.6.1 Hidden reflection problem in the cyclic case

In the following, we fix $H := \langle yx^s \rangle$ with y the standard reflection, x a generator of the rotation subgroup and $s \in \mathbb{Z}/N\mathbb{Z}$, the *slope* of our hidden reflection. We also fix $f : D_N \longrightarrow S$, a function such that for all $u, v \in D_N$, $f(u) = f(v)$ if and only if $v \in Hu$. Our goal is to find s when f is given.

We explain how operations are performed on a quantum computer using the formalism of [46, chapter 8] and the lecture notes of Dimitri Petritis [47, chapters 2 and 3], modelling quantum states as density

operators and quantum operations as unitary operators or partial traces. We assume that $S := \{0,1\}^e$ is a set of bits.We associate to f a unitary operator U_f, defined on the Hilbert space $\mathbb{C}[D_N \times S]$ as:

$$\forall g \in D_N, s \in S, \quad U_f|g,s\rangle := |g, s \oplus f(g)\rangle,$$

where $\oplus$ is the bitwise addition (xor). Assuming there is a classical circuit to compute f, we can create a quantum circuit representing U_f. Hence, our classical oracle computing f translates into a quantum oracle computing U_f.

Let us denote for all finite sets $F \subseteq E$, $|F\rangle \in \mathbb{C}[E]$ the unitary vector:

$$|F\rangle := \frac{1}{\sqrt{|F|}} \sum_{f \in F} |f\rangle.$$

The first step of Kuperberg's algorithm is to prepare the system in the quantum pure state $\rho_0 := |\psi\rangle\langle\psi|$ where $|\psi\rangle := |D_N\rangle|0^e\rangle \in \mathbb{C}[D_N \times S]$. Then, we operate by U_f and discard the output register $\mathbb{C}[S]$. After this operation, the system is in the mixed state:

$$\rho_1 = \mathrm{Tr}_{\mathbb{C}[S]}(U_f \cdot \rho_0 \cdot U_f^\dagger),$$

defined on $\mathbb{C}[D_N]$.

The second step is to operate by quantum Fourier transform $\mathcal{F}_N$, defined on $\mathbb{C}[D_N]$ as follows:

$$\forall k \in [\![0\ ;\ N-1]\!], \epsilon \in \{0,1\}, \quad \mathcal{F}_N|y^\epsilon x^k\rangle := \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \omega_N^{jk} |y^\epsilon x^j\rangle,$$

with $\omega_N := e^{\frac{2i\pi}{N}}$, leaving system be in the state:

$$\rho_2 := \mathcal{F}_N \cdot \rho_1 \cdot \mathcal{F}_N^\dagger,$$

defined on $\mathbb{C}[D_N]$.

Since D_N is in bijection (as a set) to the Cartesian product of y with $\langle x\rangle$, we have $\mathbb{C}[D_N] \simeq \mathbb{C}[\mathbb{Z}/2\mathbb{Z}] \otimes \mathbb{C}[\mathbb{Z}/N\mathbb{Z}]$, and in this decomposition, every basis vector $|y^\epsilon x^k\rangle$ with $\epsilon \in \mathbb{Z}/2\mathbb{Z}$ and $k \in \mathbb{Z}/N\mathbb{Z}$ can be represented as $|\epsilon\rangle|k\rangle$. The third operation of Kuperberg's algorithm is to measure the last register $|k\rangle$ of the system ρ_2.

Lemma B.25. *We have:*

$$\rho_1 = \frac{1}{N} \sum_{g \in \langle x\rangle} |Hg\rangle\langle Hg|$$

$$\textit{and} \quad \rho_2 = \frac{1}{2N} \sum_{k=0}^{N-1} (|0k\rangle + \omega_N^{ks}|1k\rangle)(\langle 0k| + \omega_N^{-ks}\langle 1k|).$$

Hence, after the measurement step, the system is in the pure state:

$$|\psi_k\rangle := \frac{1}{\sqrt{2}}(|0\rangle + \omega_N^{ks}|1\rangle).$$

Proof. We have:

$$\begin{aligned}
\rho_1 &= \mathrm{Tr}_{\mathbb{C}[S]}(U_f \cdot \rho_0 \cdot U_f^\dagger) = \mathrm{Tr}_{\mathbb{C}[S]}(U_f |D_N 0^e\rangle\langle D_N 0^e| U_f^\dagger) \\
&= \mathrm{Tr}_{\mathbb{C}[S]}\left(\frac{1}{2N}\sum_{g,g'\in D_N} U_f|g,0^e\rangle\langle g',0^e|U_f^\dagger\right) = \frac{1}{2N}\,\mathrm{Tr}_{\mathbb{C}[S]}\left(\sum_{g,g'\in D_N}|g,f(g)\rangle\langle g',f(g')|\right) \\
&= \frac{1}{2N}\sum_{s\in S}\sum_{g,g'\in D_N}\langle s|f(g)\rangle\langle f(g')|s\rangle|g\rangle\langle g'| = \frac{1}{2N}\sum_{s\in f(D_N)}\sum_{\substack{g,g'\in D_N\\ f(g)=f(g')=s}}|g\rangle\langle g'| \\
&= \frac{1}{2N}\sum_{g\in\langle x\rangle}\sum_{h,h'\in H}|h\rangle\langle h'| = \frac{1}{N}\sum_{g\in\langle x\rangle}|Hg\rangle\langle Hg|
\end{aligned}$$

where we used the fact that every element of D_N can be uniquely written as the product of an element of H and an element of $\langle x\rangle$, so that $D_N/H \simeq \langle x\rangle$ and the fact that f induces a injective map $D_N/H \simeq \langle x\rangle \longrightarrow S$.

For all $k \in \mathbb{Z}/N\mathbb{Z}$, we have:

$$\mathcal{F}_N|Hx^k\rangle = \frac{1}{\sqrt{2}}\mathcal{F}_N(|x^k\rangle + |yx^{k+s}\rangle) = \frac{1}{\sqrt{2N}}\sum_{j=0}^{N-1}(\omega_N^{jk}|x^j\rangle + \omega_N^{j(k+s)}|yx^j\rangle),$$

so that:

$$\begin{aligned}
\mathcal{F}_N|Hx^k\rangle\langle Hx^k|\mathcal{F}_N^\dagger &= \frac{1}{2N}\sum_{j=0}^{N-1}(\omega_N^{jk}|x^j\rangle + \omega_N^{j(k+s)}|yx^j\rangle)\sum_{l=0}^{N-1}(\omega_N^{-lk}\langle x^l| + \omega_N^{-l(k+s)}\langle yx^l|) \\
&= \frac{1}{2N}\sum_{0\le j,l\le N-1}(\omega_N^{(j-l)k}|x^j\rangle\langle x^l| + \omega_N^{j(k+s)-lk}|yx^j\rangle\langle x^l| + \omega_N^{jk-l(k+s)}|x^j\rangle\langle yx^l| \\
&\quad + \omega_N^{(j-l)(k+s)}|yx^j\rangle\langle yx^l|)
\end{aligned}$$

and finally:

$$\begin{aligned}
\rho_2 &= \mathcal{F}_N\rho_1\mathcal{F}_N^\dagger = \frac{1}{N}\sum_{k=0}^{N-1}\mathcal{F}_N|Hx^k\rangle\langle Hx^k|\mathcal{F}_N^\dagger \\
&= \frac{1}{2N^2}\sum_{0\le j,l\le N-1}\left(\sum_{k=0}^{N-1}\omega_N^{(j-l)k}\right)\left(|x^j\rangle\langle x^l| + \omega_N^{js}|yx^j\rangle\langle x^l| + \omega_N^{-ls}|x^j\rangle\langle yx^l| + |yx^j\rangle\langle yx^l|\right) \\
&= \frac{1}{2N^2}\sum_{0\le j,l\le N-1}N\delta_{j,l}\left(|x^j\rangle\langle x^l| + \omega_N^{js}|yx^j\rangle\langle x^l| + \omega_N^{-ls}|x^j\rangle\langle yx^l| + |yx^j\rangle\langle yx^l|\right) \\
&= \frac{1}{2N}\sum_{k=0}^{n-1}\left(|x^k\rangle\langle x^k| + \omega_N^{ks}|yx^k\rangle\langle x^k| + \omega_N^{-ks}|x^j\rangle\langle yx^k| + |yx^k\rangle\langle yx^k|\right) \\
&= \frac{1}{2N}\sum_{k=0}^{n-1}(|x^k\rangle + \omega_N^{ks}|yx^k\rangle)(\langle x^k| + \omega_N^{-ks}\langle yx^k|) = \frac{1}{2N}\sum_{k=0}^{N-1}(|0k\rangle + \omega_N^{ks}|1k\rangle)(\langle 0k| + \omega_N^{-ks}\langle 1k|)
\end{aligned}$$

It is now clear that if we measure the last register $\mathbb{C}[\mathbb{Z}/N\mathbb{Z}]$ and find the value k, then the system is in the following state right after the measurement:

$$\frac{I\otimes|k\rangle\langle k|\cdot\rho_2\cdot I\otimes|k\rangle\langle k|}{\mathrm{Tr}(I\otimes|k\rangle\langle k|\cdot\rho_2\cdot I\otimes|k\rangle\langle k|)} = \frac{1}{2}(|0k\rangle + \omega_N^{ks}|1k\rangle)(|0k\rangle + \omega_N^{-ks}|1k\rangle),$$

which is a the pure state associated to:

$$|\psi_k\rangle := \frac{1}{\sqrt{2}}(|0\rangle + \omega_N^{ks}|1\rangle),$$

the last register $|k\rangle$ being omitted because it does not carry any information. □

We have just described a procedure to compute states $|\psi_k\rangle = \frac{1}{\sqrt{2}}(|0\rangle + \omega_N^{ks}|1\rangle)$ with uniformly random values of $k \in \mathbb{Z}/N\mathbb{Z}$ as follows:

Algorithm 10: Procedure to produce the states $|\psi_k\rangle$ with $k \in \mathbb{Z}/N\mathbb{Z}$ uniformly random.

Data: $f : D_N \longrightarrow S$ with a hidden reflection yx^s and a quantum oracle to compute U_f.
Result: A state $|\psi_k\rangle$ together with k, for $k \in \mathbb{Z}/N\mathbb{Z}$ uniformly random.
1 Prepare the system in the pure state $\rho_0 := |D_N\rangle|0^e\rangle\langle 0^e|\langle D_G|$ over the Hilbert space $\mathbb{C}[D_N \times S]$;
2 Let U_f act on ρ_0 and discard the output register to produce $\rho_1 := \mathrm{Tr}_{\mathbb{C}[S]}(U_f \cdot \rho_0 \cdot U_f^\dagger)$;
3 Apply the quantum Fourier transform to obtain $\rho_2 := \mathcal{F}_N \cdot \rho_1 \cdot \mathcal{F}_N^\dagger$;
4 Measure the register $\mathbb{C}[\mathbb{Z}/N\mathbb{Z}]$ of ρ_2 to obtain $k \in \mathbb{Z}/N\mathbb{Z}$ and $|\psi_k\rangle$;
5 Return k and $|\psi_k\rangle$;

With this procedure, we can produce as many states $|\psi_k\rangle$ as we want and then apply a sieving procedure to all those states in order to determine s. The sieving relies on the ability to produce a new state when two states are given.

B.6.2 Principle of the sieve: producing new states

Let $|\psi_k\rangle$ and $|\psi_l\rangle$ be two sampled states. We consider the joint state:

$$|\psi_k\psi_l\rangle = \frac{1}{2}\left(|00\rangle + \omega_N^{ks}|10\rangle + \omega_N^{ls}|01\rangle + \omega_N^{(k+l)s}|11\rangle\right)$$

and we let the C-NOT gate $C^\neg$ given by:

$$\forall a, b \in \{0,1\}, \quad C^\neg|a,b\rangle = |a, a+b \mod 2\rangle$$

operate on $|\psi_k\psi_l\rangle$. The system is now in the pure state:

$$C^\neg|\psi_k\psi_l\rangle = \frac{1}{2}\left(|00\rangle + \omega_N^{(k+l)s}|10\rangle + \omega_N^{ls}|01\rangle + \omega_N^{ks}|11\rangle\right).$$

Then, we measure the second bit. If we measure the value 0, then the state becomes:

$$\frac{1}{\sqrt{2}}\left(|0\rangle + \omega_N^{(k+l)s}|1\rangle\right) = |\psi_{k+l}\rangle$$

and if we measure the value 1, then the state becomes:

$$\frac{1}{\sqrt{2}}\left(\omega_N^{ls}|0\rangle + \omega_N^{ks}|1\rangle\right) = \omega_N^{ls}|\psi_{k-l}\rangle,$$

which can be assimilated to $|\psi_{k-l}\rangle$ because collinear unit states are equivalent. Hence, we either obtain $|\psi_{k+l}\rangle$ or $|\psi_{k-l}\rangle$ by the end of this procedure. By measurement, we also know if we obtained $k+l$ or $k-l$.

Algorithm 11: State creation.

Data: Two state $|\psi_k\rangle$ and $|\psi_l\rangle$.
Result: A state $|\psi_{k\pm l}\rangle$ together with the integer $k \pm l$, where the sign $\pm$ is an unbiased coin flip.
1 Let the C-NOT gate operate on $|\psi_k\psi_l\rangle$ to obtain $|\Psi\rangle := C^\neg|\psi_k\psi_l\rangle$;
2 Measure the second bit of Ψ;
3 If the result of the measure is $\epsilon \in \{0,1\}$, we obtain $|\psi_{k+(-1)^\epsilon l}\rangle$;
4 Output $|\psi_{k+(-1)^\epsilon l}\rangle$ and $k + (-1)^\epsilon l$;

B.6.3 Sieving procedure in the case $N = r^n$

In this paragraph, we describe how this sieving procedure works when N is a prime power $N := r^n$, with r relatively small. However, this could be generalized to any value of N (see [14, Algorithm 2] for details). Here, we shall not deal with the general case because it is not necessary for our application to $G = \mathrm{Cl}(\mathcal{O}_n)$ whose p-groups have small values of p.

Goal of the sieving: reduce the problem to $D_{N/r}$

If $s \equiv a\ [r]$ for $a \in [\![0\ ;\ r-1]\!]$ then our hidden reflection yx^s is in the subgroup $G_a := \langle yx^a, x^r\rangle$, which is isomorphic to $D_{N/r}$. Hence, we have reduced our problem to the hidden reflection in $D_{N/r}$, provided that we can find $s \mod r$.

To find $s \mod r$, we use states $|\psi_k\rangle$ with $k := br^{n-1}$ and $b \in [\![1\ ;\ r-1]\!]$. With sufficiently many copies of $|\psi_k\rangle$ (for the same k), we can recover $s \mod r$ by *state tomography*, as explained in [46, § 8.4.2, p.389]. We consider the Pauli matrices:

$$\sigma_0 := I_2, \quad \sigma_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{and} \quad \sigma_3 := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

The system $(\sigma_j/\sqrt{2})_{0\leq j\leq 3}$ is a basis for the Hilbert-Schmidt scalar product:

$$(A, B) \in M_2(\mathbb{C}) \longmapsto (A|B) := \mathrm{Tr}(A^\dagger \cdot B).$$

Hence, our state $\rho := |\psi_k\rangle\langle\psi_k|$ is fully determined by the equation:

$$\rho = \frac{1}{2}\sum_{j=0}^{3} \mathrm{Tr}(\sigma_j \cdot \rho)\sigma_j.$$

Actually, the trace $\mathrm{Tr}(\sigma_j \cdot \rho)$ is the expected value of the observable σ_j when the system is in state ρ so we may evaluate it by law of large numbers, provided that we have enough copies of ρ to test. By the central limit theorem, if we have m observations $z_1, \cdots, z_m$, the statistical $\frac{1}{m}\sum_{l=1}^{m} z_l$ should approximate $\mathrm{Tr}(\sigma_j \cdot \rho)$ with precision $1/\sqrt{m}$. Actually, we have

$$\mathrm{Tr}(\sigma_0 \cdot \rho) = \frac{1}{2}, \quad \mathrm{Tr}(\sigma_1 \cdot \rho) = \cos\left(\frac{2\pi bs}{r}\right), \quad \mathrm{Tr}(\sigma_2 \cdot \rho) = \sin\left(\frac{2\pi bs}{r}\right) \quad \text{and} \quad \mathrm{Tr}(\sigma_3 \cdot \rho) = 0,$$

so we only have to measure $\mathrm{Tr}(\sigma_1 \cdot \rho)$ and $\mathrm{Tr}(\sigma_2 \cdot \rho)$, to determine ρ.

The sieve

For all $k \in \mathbb{Z}/N\mathbb{Z}$ (seen as an integer in $[\![0\ ;\ N-1]\!]$), let $\alpha(k)$ be the number of trailing zeros in the decomposition of k in basis r. We describe a sieving procedure maximizing the value of α. We start with a list L_0 of sub-exponential size containing states $|\psi_k\rangle$ with $k \in \mathbb{Z}/N\mathbb{Z}$ uniformly random, provided by repeated quantum oracle queries following Algorithm 10.

Let $k := \lceil \log_2(r) \rceil$, $m := \lceil \sqrt{(n-1)/k} \rceil$ and $m' := \lceil (n-1)/m \rceil$. For $j \in [\![0\ ;\ m'-1]\!]$, we assume that we have a list L_j of states $|\psi_k\rangle$ with k having mj trailing zeros ($\alpha(k) \geq mj$). We construct a list L_{j+1} of states $|\psi_k\rangle$ such that $\alpha(k) \geq m(j+1)$ as follows: we divide L_j into pairs of states $|\psi_k\rangle$ and $|\psi_l\rangle$ such that k and l share m digits next to their trailing zeros (or $n-1-m(m'-1)$ digits if $j = m'-1$). Then, we apply Algorithm 11 to produce a state $|\psi_{k\pm l}\rangle$. If the result is $k-l$, we add the new state $|\psi_{k-l}\rangle$ to L_{j+1}. Otherwise, we do nothing.

Finally, the list $L_{m'}$ will contain *final states* $|\psi_k\rangle$ such that $r^{n-1}|k$. Provided that $L_{m'}$ contains sufficiently many of these states, we can find $s \mod r$ and reduce our problem to $D_{N/r}$. To sum up,

we obtain the following version of Kuperberg's algorithm in the case of a cyclic r-group. Note that this algorithm is recursive.

Algorithm 12: Kuperberg's algorithm in a cyclic r-group.

Data: $N := r^n$ with r prime, $f : D_N \longrightarrow S$ with a hidden reflection yx^s and a quantum oracle to compute U_f.

Result: $s \in \mathbb{Z}/N\mathbb{Z}$.

Use Algorithm 10 repeatedly to produce a list L_0 of states $|\psi_k\rangle$ with $k \in \mathbb{Z}/N\mathbb{Z}$ uniformly random;

$k \leftarrow \lceil \log_2(r) \rceil$, $m \leftarrow \lceil \sqrt{(n-1)/k} \rceil$, $m' \leftarrow \lceil (n-1)/m \rceil$;

for $j := 0$ **to** $m' - 1$ **do**

  Initiate L_{j+1} as the empty list;

  Divide L_j into a maximal list P_j of pairs $|\psi_k\rangle$ and $|\psi_l\rangle$ such that k and l share $\min(m, n-1-mj)$ r-digits next to their trailing zeros;

  For every pair $\{|\psi_k\rangle, |\psi_l\rangle\} \in P_j$, apply Algorithm 11 to create a new state $|\psi_{k\pm l}\rangle$ and add this state to L_{j+1} if $\pm = +$;

end

All sates of $L_{m'}$ are of the form $|\psi_{br^{n-1}}\rangle$ with $b \in [\![0\ ;\ r-1]\!]$. Extract all the copies of $|\psi_{br^{n-1}}\rangle$ with a fixed value $b \neq 0$ chosen to maximize the number of these copies. ;

Apply state tomography (see Paragraph B.6.3) to recover $a := s \mod r$ from the copies of $|\psi_{br^{n-1}}\rangle$;

Compute recursively the slope $s' \in \mathbb{Z}/r^{n-1}\mathbb{Z}$ for the hidden reflection problem induced by f in $G_a := \langle yx^a, x^r \rangle$;

Return $a + rs'$;

The number of states in L_0 to make sure that $L_{m'}$ contains enough copies of the same non trivial state to perform state tomography.

Lemma B.26. *Let $k := \lceil \log_2(r) \rceil$, $m := \lceil \sqrt{(n-1)/k} \rceil$ and $m' := \lceil (n-1)/m \rceil$. Suppose that $|L_0| \geq 4 \cdot 2^{km+2m'}$. Then, $|L_{m'}| \geq 2^{km}$ with overwhelming probability:*

$$\mathbb{P}\left(|L_{m'}| \geq 2^{km}\right) \geq \left(1 - e^{-2^{\frac{m'}{3}-1}}\right)^{m'}.$$

Before proving the lemma, we prove the following classical inequality due to Chernoff:

Lemma B.27. *Let $X_1, \cdots, X_M$ be M independent Bernoulli variables of parameter $\frac{1}{2}$ and $S_M := \sum_{i=1}^{M} X_i$. Then, for all $b \in]0, 1[$, we have:*

$$\mathbb{P}\left(S_M \leq \frac{N(1-b)}{2}\right) \leq \cosh(b)^N e^{-Nb^2} \leq e^{-\frac{Nb^2}{2}}.$$

Proof. We have by Markov's inequality:

$$\begin{aligned}
\mathbb{P}\left(S_M \leq \frac{N(1-b)}{2}\right) &= \mathbb{P}\left(M - S_M \geq \frac{N(1+b)}{2}\right) = \mathbb{P}\left(e^{2b(M-S_M)} \geq e^{Nb(1+b)}\right) \\
&\leq \mathbb{E}\left(e^{2b(M-S_M)}\right) e^{-Nb(1+b)} = \mathbb{E}\left(\prod_{i=1}^{M} e^{2b(1-X_i)}\right) e^{-Nb(1+b)} \\
&= \mathbb{E}(e^{2b(1-X_1)})^N e^{-Nb(1+b)} \quad \text{(the } X_i \text{ being i.i.d)} \\
&= \left(\frac{1+e^{2b}}{2}\right)^N e^{-Nb(1+b)} = \left(\frac{e^b + e^{-b}}{2}\right)^N e^{-Nb^2} = \cosh(b)^N e^{-Nb^2}
\end{aligned}$$

To conclude, it suffices to prove that $\cosh(b) \leq e^{\frac{b^2}{2}}$. Actually, this equality holds for all $b \geq 0$. Let:

$$g : t \in \mathbb{R}_+ \longmapsto \ln(2) + \frac{t^2}{2} - t - \ln\left(1 + e^{-2t}\right).$$

To prove the desired inequality,it is sufficient and necessary to prove that g is non-negative on $\mathbb{R}_+$. g is $\mathcal{C}^2$ and:

$$\forall t \in \mathbb{R}_+, \quad g'(t) = t - 1 + \frac{2}{e^{2t}+1} \quad \text{and} \quad g''(t) = 1 - \frac{4e^{2t}}{(1+e^{2t})^2} = 1 - \frac{1}{\cosh(t)^2}.$$

Since $\cosh \geq 1$ on $\mathbb{R}_+$, it follows that $g'' \geq 0$ on $\mathbb{R}_+$, so that $g'(t) \geq g'(0) = 0$ for all $t \in \mathbb{R}_+$, so g is increasing and $g(t) \geq g(0) = 0$ for all $t \in \mathbb{R}_+$. This completes the proof. □

Proof. (of Lemma B.26) We prove by induction that we have for all $j \in [\![0\ ;\ m']\!]$:

$$\mathbb{P}\left(|L_j| \geq C_j 2^{km+2(m'-j)}\right) \geq \left(1 - e^{-2^{\frac{m'}{3}-1}}\right)^j,$$

with $C_0 := 4$ and for all $j \in [\![0\ ;\ m'-1]\!]$, $C_{j+1} := C_j(1 - 2^{j-\frac{4m'}{3}})(1 - 2^{2(j-m')})$.

This is trivial for $j = 0$. Let $j \in [\![0\ ;\ m'-1]\!]$. We assume that the result holds at rank j. Let P_j be a maximal list of pairs of states $|\psi_k\rangle$ and $|\psi_l\rangle$ of L_j such that k and l share $\min(m, n-1-mj)$ digits (in basis r) next to their trailing zeros. Since at most r^m elements of L_j do not belong to one of these pairs and $r \leq 2^k$, we have:

$$|P_j| \geq \frac{|L_j| - r^m}{2} \geq \frac{|L_j| - 2^{km}}{2}.$$

Assuming that $|L_j| \geq C_j 2^{km+2(m'-j)}$ and that $C_j \geq 1$ (that we shall prove later), we get that:

$$|P_j| \geq \frac{C_j 2^{km+2(m'-j)} - 2^{km}}{2} = 2^{km+2(m'-j)-1}(C_j - 2^{2(j-m')}) \geq 2^{km+2(m'-j)-1} C_j (1 - 2^{2(j-m')}).$$

When executing Algorithm 11 for each pair $\{|\psi_k\rangle, |\psi_l\rangle\} \in P_j$, we have a probability of $\frac{1}{2}$ to obtain the state $|\psi_{k+l}\rangle$ that we can add to L_{j+1}. Hence, $|L_{j+1}|$ is the sum of $|P_j|$ independent Bernoulli variables so for $b \in]0,1[$ to be chosen, Chernoff's inequality ensures that:

$$\mathbb{P}\left(|L_{j+1}| \leq \frac{|P_j|(1-b)}{2}\right) \leq e^{-\frac{|P_j|b^2}{2}} \quad i.e. \quad \mathbb{P}\left(|L_{j+1}| \geq \frac{|P_j|(1-b)}{2}\right) \geq 1 - e^{-\frac{|P_j|b^2}{2}}.$$

We set $b := 2^{j-\frac{4m'}{3}}$. Then, conditionally to the event $|L_j| \geq C_j 2^{km+2(m'-j)}$, we get:

$$\frac{|P_j|(1-b)}{2} \geq 2^{km+2(m'-j-1)} C_j (1 - 2^{2(j-m')})(1 - 2^{j-\frac{4m'}{3}}) = 2^{km+2(m'-j-1)} C_{j+1}$$

and:

$$\frac{|P_j|b^2}{2} \geq 2^{km+2(m'-j)-1} C_j (1 - 2^{2(j-m')}) 2^{2j-\frac{8m'}{3}} \geq 2^{km+\frac{m'}{3}-2} \geq 2^{\frac{m'}{3}-1},$$

since $C_j \geq 1$ and $km \geq 1$. It follows that:

$$\mathbb{P}\left(|L_{j+1}| \geq 2^{km+2(m'-j-1)} C_{j+1} \middle| |L_j| \geq C_j 2^{km+2(m'-j)}\right) \geq 1 - e^{-2^{\frac{m'}{3}}}.$$

The result follows immediately at rank $j+1$.

It remains to prove that $C_j \geq 1$ for all $j \in [\![0\ ;\ m']\!]$. Since the C_j are decreasing, we just have to

prove that $C_{m'} \geq 1$. But we have:

$$\begin{aligned}
C_{m'} &= C_0 \prod_{j=0}^{m'-1} \left(1 - 2^{j-\frac{4m'}{3}}\right)\left(1 - 2^{2(j-m')}\right) = C_0 \prod_{j=1}^{m'} \left(1 - 2^{-j-\frac{m'}{3}}\right)\left(1 - 2^{-2j}\right) \\
&= C_0 \exp\left(\sum_{j=1}^{m'} \left(\ln\left(1 - 2^{-j-\frac{m'}{3}}\right) + \ln\left(1 - 2^{-2j}\right)\right)\right) \\
&\geq 4 \exp\left(-\sum_{j=1}^{m'} \left(2^{-j-\frac{m'}{3}} + 2^{-2j-\frac{4m'}{3}-1} + 2^{-2j} + 2^{-4j-1}\right)\right) \\
&\geq 4 \exp\left(-\frac{1}{2^{\frac{m'}{3}+1}\left(1-\frac{1}{2}\right)} - \frac{1}{2^{\frac{4m'}{3}+3}\left(1-\frac{1}{2^2}\right)} - \frac{1}{2^2\left(1-\frac{1}{2^2}\right)} - \frac{1}{2^4\left(1-\frac{1}{2^4}\right)}\right) \\
&= 4 \exp\left(-\frac{1}{2^{\frac{m'}{3}}} - \frac{1}{3 \cdot 2^{\frac{4m'}{3}+1}} - \frac{1}{3} - \frac{1}{15}\right) \geq 1
\end{aligned}$$

as soon as $m' \geq 1$, which is obviously the case. □

Theorem B.28. *In the cyclic case with $N = r^n$ for r relatively small, Kuperberg's algorithm (Algorithm 12) terminates and is correct with overwhelming probability, requires $2^{O(\sqrt{\log_2(N)})}$ queries to the oracle U_f, runs in time $2^{O(\sqrt{\log_2(N)})}$ and uses $2^{O(\sqrt{\log_2(N)})}$ qubits.*

Proof. The termination and correctness follows from the explanations and results given above (Lemma B.26 in particular).

We keep the notations of Algorithm 12. By Lemma B.26, the size of the list L_0 is $4 \cdot 2^{km+2m'}$, where $k := \lceil \log_2(r) \rceil$, $m := \lceil \sqrt{(n-1)/k} \rceil$ and $m' := \lceil (n-1)/m \rceil$, so that, when $n \to +\infty$ and r is constant, $m = \sqrt{n/k} + O(1)$ and $m' = \sqrt{kn} + O(1)$ and:

$$km + 2m' = 3\sqrt{kn} + O(1) = 3\sqrt{\log_2(r)\log_r(N)} + O(1) = 3\sqrt{\log_2(N)} + O(1).$$

As a consequence, $2^{3\sqrt{\log_2(N)}+O(1)}$ quantum queries are necessary on line 1 of 12. Taking into account the n recursive calls we get that the number of quantum queries is:

$$\sum_{k=0}^{n-1} 2^{3\sqrt{\log_2(N/r^k)}+O(1)} \leq n 2^{3\sqrt{\log_2(N)}+O(1)} = 2^{O(\sqrt{\log_2(N)})}.$$

The operations performed on the lists L_j for $j \in [\![0\ ;\ m'-1]\!]$ are linear in the size of these lists which is bounded by $|L_0|$. As a consequence, the for loop in Algorithm 12 has a time complexity $m' 2^{3\sqrt{\log_2(N)}+O(1)} = 2^{O(\sqrt{\log_2(N)})}$. Line 8 and 9 of the algorithm do not change the complexity. Taking into account the recursion, we get a time complexity of $n 2^{O(\sqrt{\log_2(N)})} = 2^{O(\sqrt{\log_2(N)})}$.

The space complexity in terms of qubits is bounded by $|L_0| = 2^{O(\sqrt{\log_2(N)})}$. □

Remark B.29. The complexities given here only hold only if r is small and $n \to +\infty$. If $n = 1$ and $N = r$ is prime, Algorithm 12 is exponential in $\log_2(N)$. Hopefully, Kuperberg's provided an algorithm working in this case.

General case (G not cyclic)

We briefly explain (without proof) how the cyclic case can be generalized to any finite abelian group G. By the structure theorem of finite abelian groups, there exists integers $N_1, \cdots, N_a \geq 2$ such that:

$$G \simeq \prod_{i=1}^{a} \mathbb{Z}/N_i\mathbb{Z}.$$

We can even assume that the N_i are prime powers by the Chinese remainder theorem. As in the cyclic case, every element $g \in D_G$ can be uniquely written as $g = y^\epsilon \prod_{i=1}^a x_i^{t_i}$, with $\epsilon \in \mathbb{Z}/2\mathbb{Z}$ and $t_i \in \mathbb{Z}/N_i\mathbb{Z}$ for all $i \in [\![1\ ;\ a]\!]$, y being the standard reflection and x_i being generator of the factor $\mathbb{Z}/N_i\mathbb{Z}$ for $i\,[\![1\ ;\ a]\!]$. The hidden reflection is then determined by an a-dimensional slope $s \in \prod_{i=1}^a \mathbb{Z}/N_i\mathbb{Z}$.

A slightly modified version of Algorithm 10 (with a multidimensional quantum Fourier transform), when given the pure state $|D_G\rangle|0^e\rangle$, outputs a state:

$$|\psi_k\rangle := |0\rangle + e^{\sum_{j=1}^a \frac{2ik_j s_j \pi}{N_j}}|1\rangle,$$

with a random uniform vector $k := (k_1, \cdots, k_a) \in \prod_{i=1}^a \mathbb{Z}/N_i\mathbb{Z}$. The idea is to perform $2^{O(\log_2(|G|))}$ such quantum queries to obtain a list of such states $|\psi_k\rangle$ and then apply a sieving procedure to produce $2^{O(\log_2(N_i))}$ states $|\psi_k\rangle$ with k almost zero except at index $i \in [\![1\ ;\ a]\!]$, and then apply a new sieving in the group $\langle y, x_i\rangle \simeq D_{N_i}$ to recover s_i. If N_i is a prime power, Algorithm 12 can be applied.

As previously, this sieving procedure to discard vector components except at index $i \in [\![1\ ;\ a]\!]$ uses a variant of Algorithm 11 to produce states $|\psi_{k\pm l}\rangle$ with pairs of states $|\psi_k\rangle$ and $|\psi_l\rangle$ and maximizes an objective function α_i defined over $\prod_{j=1}^a \mathbb{Z}/N_j\mathbb{Z}$. For $i = a$, this objective function was explicitely defined by Kuperberg [14, proof of Theorem 7.1]. For $k \in \prod_{j=1}^a \mathbb{Z}/N_j\mathbb{Z}$, let $b(k) := \min\{1 \leq j \leq a | k_j \neq 0\}$ and if $b(k) < a$, set:

$$\alpha(k) := \sum_{j=1}^{b(k)} \lceil 1 + \log_2(N_j + 1)\rceil - \lceil \log_2(k_{b(k)} + 1)\rceil$$

if $b(k) = a$, set:

$$\alpha(k) := \sum_{j=1}^{a} \lceil 1 + \log_2(N_j + 1)\rceil.$$

Theorem B.30. *Hidden reflection problem in D_G can be solved in time $2^{O(\log_2(|G|))}$ with $2^{O(\log_2(|G|))}$ quantum queries and $2^{O(\log_2(|G|))}$ qubits.*

Proof. See [14, Theorem 7.1]. □

Appendix C

Constructing hash proof systems with the OSIDH framework

This chapter was an attempt to construct new cryptographic primitives with the OSIDH framework beyond key exchange. Indeed, OSIDH runs very slowly compared other isogeny-based Diffie-Hellman protocols such as SIDH (and even CSIDH) which are themselves slow compared to lattice based and code based key exchanged submitted to the NIST. Hence, the potential interest of OSIDH motivating this master's thesis was to go beyond key exchange and to find new primitives based on its framework. Here, we present how to construct hash proof systems with OSIDH but these constructions are unfortunately insecure.

C.1 Definition of a hash proof system

This notion was first introduced by Cramer and Shoup in [48]. We use the notations and follow the presentation of [10].

Definition C.1. A *hash proof system* is a tuple $\Pi := (\Lambda, \pi, \text{ProjEval}, L, \Sigma, W, \mathcal{K}, \mathcal{P}, \Gamma)$, where, on the one hand $L, \Sigma, W, \mathcal{K}, \mathcal{P}$ and Γ are sets such that:

(i) There exist efficient algorithms to sample elements from Σ and $\mathcal{K}$ with uniform distribution.

(ii) $L \subset \Sigma$ and W is the space of witnesses to test membership in L.

(iii) The uniform distributions on L and Σ are computationally indistinguishable (*subset membership problem*).

On the other hand, the *hash function* Λ, the *projection* $\pi : \mathcal{K} \longrightarrow \mathcal{P}$ and the *projective evaluation* $\text{ProjEval} : \mathcal{P} \times L \longrightarrow \Gamma$ are efficiently computable functions such that, for any algorithm (possibly inefficient) $\omega : L \longrightarrow W$ associating a membership witness $w = \omega(\sigma) \in W$ to every element $\sigma \in L$, we have a commutative diagram:

$$\begin{array}{ccc} \mathcal{K} \times L & \xrightarrow{\Lambda} & \Gamma. \\ {\scriptstyle \pi \times \omega}\downarrow & \nearrow_{\text{ProjEval}} & \\ \mathcal{P} \times W & & \end{array}$$

We additionally require Π to be *universal*, meaning that knowing $(\pi(k), \sigma)$ for $(k, \sigma) \in \mathcal{K} \times \Sigma \setminus L$ provides no information on the value of $\Lambda(k, \sigma)$. Formally, for $\varepsilon > 0$, we say that Π is ε-universal if:

$$H_\infty(\Lambda(k, \sigma) | (\pi(k), \sigma)) \geq \log(\varepsilon^{-1}),$$

where $H_\infty(.|.)$ is the conditional min-entropy defined below.

Definition C.2. Let X and Y be discrete random variables taking values in $\mathcal{X}$ and $\mathcal{Y}$ respectively. Then, the conditional min-entropy of X, knowing Y is the quantity:

$$H_\infty(X|Y) = -\log \max_{(x,y)\in\mathcal{X}\times\mathcal{Y}} \mathbb{P}(X = x|Y = y).$$

Hash proof systems can be used to construct cryptographic protocols such as public key encryption secure against ciphertext attack (IND-CCA) [48], authenticated key-exchange [49] and other protocols satisfying privacy preservation hypothesis [50]. However, these constructions require hash proof systems with stronger security assumptions.

C.2 Hash proof system form weak-pseudorandom restricted effective group actions

Definition C.3. [10, Definition 2] An *effective group action* is a triplet $(G, X, \cdot)$ where G is a finite group, X a finite set $\cdot : G \times X \longrightarrow X$ a transitive and faithful group action, such that:

(i) There are efficient algorithms on G to test membership, equality, to sample elements (with uniform distribution), compute the product of two elements and the inverse of one element.

(ii) There is an efficient algorithm to test membership in X and every element of X admits a unique (bitstring) representation.

(iii) We know (the bitstring representation of) an element $x_0 \in X$ called the *origin*.

(iv) There exists an efficient algorithm computing $g \cdot x$ when $g \in G$ and $x \in X$ are given.

In the context of OSIDH, we don't know how to efficiently compute the action of the whole group but only on a subset. The definition can be adapted to this case:

Definition C.4. [10, Definition 6] A *restricted effective group action* is a triplet $(G, X, \cdot, g)$ where G is a finite group, X a finite set $\cdot : G \times X \longrightarrow X$ a transitive and faithful group action, and $\mathcal{G} := \{g_1, \cdots, g_t\}$ a generating set of G such that:

(i) t is polynomial in $\log(|G|)$.

(ii) There is an efficient algorithm to test membership in X and every element of X admits a unique (bitstring) representation.

(iii) We know (the bitstring representation of) an element $x_0 \in X$ called the *origin*.

(iv) There exist efficient algorithms computing $g_i \cdot x$ and $g_i^{-1} \cdot x$ when $i \in [\![1\ ;\ t]\!]$ and $x \in X$ are given.

Remark C.5. We assume that G is abelian. Knowing the generating set $\mathcal{G} = \{g_1, \cdots, g_t\}$ of G, we can represent elements $g \in G$ as tuples of $\mathbb{Z}^t$ via the map:

$$\phi : e := (e_1, \cdots, e_t) \in \mathbb{Z}^t \longmapsto g^e := \prod_{i=1}^{t} g_i^{e_i} \in G$$

and compute the action of g^e on X when $e \in \mathbb{Z}^t$ has components of polynomial size. We can even sample on G with distributions statistically close to the uniform by sampling $e \in \mathbb{Z}^t$ with Gaussian distribution with standard deviation sufficiently bigger than the smoothing parameter of the lattice $\ker(\phi) \subseteq \mathbb{Z}^t$ (see [51, Sections 3 and 4]).

Definition C.6. A group action $(G, X, \cdot)$ is said *weak-pseudorandom* if given a randomly chosen secret $g \in G$, one cannot distinguish between the distribution of $(x, g \cdot x)$ and (x, y), where x and y are chosen uniformly at random in X.

Let $(G, X, \cdot)$ be an abelian weak-pseudorandom (restricted) effective group action. We can construct a hash proof system with it as follows: we fix $x_0, x_1 \in X$ with $x_1 = s \cdot x_0$ with $s \in G$ secret. Let:

$$\Sigma := \{(g_0 \cdot x_0, g_1 \cdot x_1) \mid g_0, g_1 \in G\} \quad \text{and} \quad L := \{(g \cdot x_0, g \cdot x_1) \mid g \in G\},$$

$W := G$, $\mathcal{K} := G \times \{0,1\}$ and $\mathcal{P} = \Gamma := X$. We define the hash function $\Lambda : (G \times \{0,1\}) \times \Sigma \longrightarrow X$ as follows:

$$\forall (h,b) \in G \times \{0,1\}, (y_0, y_1) \in \Sigma, \quad \Lambda((h,b),(y_0,y_1)) := h \cdot y_b$$

and set:

$$\forall (h,b) \in G \times \{0,1\}, \quad \pi(h,b) := h \cdot x_b,$$

$$\forall (x,g) \in X \times G, \quad \text{ProjEval}(x,g) := g \cdot x$$

$$\text{and} \quad \forall g \in G, \quad \omega((g \cdot x_0, g \cdot x_1)) := g,$$

so that $\Lambda = \text{ProjEval} \circ (\pi \times \omega)$ on $\mathcal{K} \times L$.

Theorem C.7. *[10, Theorem 1] The system* $\Pi := (\Lambda, \pi, \text{ProjEval}, L, \Sigma, G, G \times \{0,1\}, X, X)$ *defined above is a* 2^{-1}*-universal hash proof system.*

Proof. Under the hypothesis we made, the non-trivial points to prove are subset membership problem and universality.

Since the group action of G on X is faithful, sampling an element $(y_0, y_1) \in L$ with uniform distribution is equivalent to sampling $g \in G$ with uniform distribution and returning $(g \cdot x_0, g \cdot x_1)$. Writing $y_0 := g \cdot x_0$, we get that $g \cdot x_1 = g \cdot s \cdot x_0 = s \cdot g \cdot x_0 = s \cdot y_0$ because G is abelian. Since y_0 is uniform, $(g \cdot x_0, g \cdot x_1) = (y_0, s \cdot y_0)$ is indistinguishable from (y_0, y_1) sampled with uniform distribution from X^2 by weak-pseudorandomness. But $X^2 = \Sigma$ by transitivity of the group action. Hence, the uniform distributions on L and Σ are undistinguishable.

Let $(h,b) \in G \times \{0,1\}$ be a key (secret and sampled with uniform distribution) and $(y_0, y_1) = (g_0 \cdot x_0, g_1 \cdot x_1) \in \Sigma \setminus L$ be sampled with uniform distribution. Let us assume that an attacker with unbounded capabilities knows (y_0, y_1) and $\pi(h,b) = h \cdot x_b$ and wants to recover $\Lambda((h,b),(y_0,y_1)) = h \cdot y_b$. Since $\pi(h,b) = h \cdot x_b = hs^{2b-1} \cdot x_{1-b}$, the knowledge of (y_0, y_1) and $\pi(h,b)$ enables the unbounded attacker to infer that $\Lambda((h,b),(y_0,y_1)) = h \cdot y_b = hg_b \cdot x_b$ or:

$$\Lambda((h,b),(y_0,y_1)) = hs^{2b-1} \cdot y_{1-b} = hs^{2b-1} g_{1-b} \cdot x_{1-b} = hs^{2b-1} g_{1-b} s^{1-2b} \cdot x_b = hg_{1-b} \cdot x_b \neq hg_b \cdot x_b.$$

Hence, the attacker has a probability $\frac{1}{2}$ to guess the right value. It follows that:

$$H_\infty(\Lambda((h,b),(y_0,y_1)) | (\pi(h,b),(y_0,y_1))) = -\log\left(\frac{1}{2}\right),$$

so that Π is 2^{-1}-universal. □

Using the OSIDH framework, we can take $G := \text{Cl}(\mathcal{O}_n)$ (or the subgroup generated by the ideals $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$) and $X := \rho(\text{Ell}(\mathcal{O}_n))$. To simplify the computation of the group action using the techniques of Paragraph 1.5.2, we could represent elements of X as descending ℓ-isogeny chains $(E_i)_{0 \leq i \leq n}$. However, in that case, weak-pseudorandomness would not hold because of the attacks of Sections 3.1 and 3.2. Indeed, let us fix two descending ℓ-isogeny chains $(E_{0,i})_{0 \leq i \leq n}$ and $(E_{1,i})_{0 \leq i \leq n} := \mathfrak{s} \cdot (E_{0,i})_{0 \leq i \leq n}$, where $\mathfrak{s}$ is a secret randomly chosen ideal of $\mathcal{O}_n$. Then, sampling $[\mathfrak{a}], [\mathfrak{b}] \in \text{Cl}(\mathcal{O}_n)$ uniformly (using Gaussian distributions as explained in Remark C.5 if necessary) we can distinguish the distribution of pairs $([\mathfrak{a}] \cdot (E_{0,i}), [\mathfrak{a}] \cdot (E_{1,i}))$ and $([\mathfrak{a}] \cdot (E_{0,i}), [\mathfrak{b}] \cdot (E_{1,i}))$ by recovering $[\mathfrak{a}]$ and $[\mathfrak{b}]$.

To correct this, we use the technique introduced in Paragraph 2.2. Instead of representing elements of

$\rho(\mathrm{Ell}(\mathcal{O}_n))$ by descending ℓ-isogeny chains $(E_i)_{0\leq i\leq n}$, we represent them as the list of horizontal chains:

$$E_{n,j}^{(-r)} := (\mathfrak{q}_j^{(n)})^{-r} \cdot E_n \longrightarrow \cdots \longrightarrow E_n \longrightarrow \cdots \longrightarrow E_{n,j}^{(r)} := (\mathfrak{q}_j^{(n)})^{r} \cdot E_n$$

for all $j \in [\![1\ ;\ t]\!]$. Unfortunately, the attack of Section 3.4 undermines weak-pseudorandomness in this case too, unless the parameters are chosen so that the key space:

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

represents a very small portion of $\mathrm{Cl}(\mathcal{O}_n)$. Unfortunately, in that case, the projective evaluation is no longer easily computable because we are restricted to group actions by elements of this tiny key space. Hence, such a construction fails with OSIDH.

In the following, we tried to bypass these difficulties by combining OSIDH with Supersingular Isogeny Diffie Hellman (SIDH) due to De Feo, Jao and Plût [3]. Unfortunately, this attempt fails too because of our cryptanalysis of OSIDH.

C.3 An original hash proof system combining SIDH with OSIDH

Attempts have been made to construct a hash proof system using SIDH only which has stronger security than OSIDH. If the subset membership problem is indeed stronger, these constructions fail to ensure universality, which is a direct consequence of the transitivity and faithfulness of the class group action in the OSIDH framework. For that reason, combining the strengths of both frameworks could be fruitful. The main idea of the hash proof system presented here is to make the projection π act horizontally by ideal class group action (OSIDH component) and make ProjEval act vertically as quotient by cyclic kernels (SIDH component).

Let K be a quadratic imaginary number field such that $\mathrm{Cl}(\mathcal{O}_K)$ is trivial. Let $r \neq \ell$ be a small prime inert in K (*i.e.* such that $\left(\frac{\Delta_K}{r}\right) = -1$). Let ℓ be a small prime and $\mathcal{O}_i := \mathbb{Z}+\ell^i\mathcal{O}_K$ and $\mathcal{O}_{i,j} := \mathbb{Z}+\ell^i r^j \mathcal{O}_K$ for all $i, j \in \mathbb{N}$. We chose p of the form $p := fr^e \pm 1$ with $e \in \mathbb{N}^*$ big enough (to ensure SIDH security) and f big enough to construct descending ℓ-ladders and r-ladders efficiently with the techniques of Paragraph 1.5.2. Actually:

$$p > \max_{1\leq j\leq t}(q_j)\ell^{2n}r^{2e}|\Delta_K| \qquad \text{(see Lemma C.10).}$$

We also assume that p does not split in K (see Proposition 1.12).

Lemma C.8. *Let $E/\mathbb{F}_{p^2}$ such that $|E(\mathbb{F}_{p^2})| = (fr^e)^2$. Then:*

(i) *$E(\mathbb{F}_{p^2}) = E[fr^e]$. In particular, $E[r^e] \subseteq E(\mathbb{F}_{p^2})$.*

(ii) *Assume that $E \in \rho(\mathrm{Ell}(\mathcal{O}_n))$ and let $P \in E[r^e]$ be of order r^e. Then $E/\langle P\rangle \in \rho(\mathrm{Ell}(\mathcal{O}_{n,e}))$ (we recall that $\mathcal{O}_{n,e} = \mathbb{Z} + r^e\mathcal{O}_n = \mathbb{Z} + \ell^n r^e \mathcal{O}_K$).*

Proof. **(i)** Since $|E(\mathbb{F}_{p^2})| = (fr^e)^2 = (p \mp 1)^2$, the trace of the p^2-th Frobenius π_2 is $\mp 2p$, so we have $\pi_2^2 \pm [2p]\pi_2 + [p^2] = 0$ *i.e.* $(\pi_2 \pm [p])^2 = 0$ *i.e.* $\pi = \mp[p]$.

Let $P \in E[fr^e]$. Then for all $Q \in E[fr^e]$, we have:

$$e_{fr^e}(\pi_2(P), Q) = e_{fr^e}(\mp[p]P, Q) = e_{fr^e}(P, Q)^{\mp p} = e_{fr^e}(P, Q)^{\mp fr^e+1} = e_{fr^e}(P, Q),$$

so that $e_{fr^e}(\pi_2(P) - P, Q) = 1$. It follows that $\pi_2(P) = P$ *i.e.* $P \in E(\mathbb{F}_{p^2})$. Hence $E[fr^e] \subseteq E(\mathbb{F}_{p^2})$ and we have an equality since both sets have cardinality $(fr^e)^2$.

(ii) Let $\phi : E \longrightarrow E/\langle P\rangle$ be the isogeny of kernel $\langle P\rangle$. Then, we have $\phi = \phi_e \circ \cdots \circ \phi_0$ where $\phi_0 = [1]_E$ and for all $i \in [\![1\ ;\ e]\!]$, $\phi_i : E_{i-1} \longrightarrow E_i$ ($E_0 := E$, $E_e := E/\langle P\rangle$) has kernel generated by $\phi_{i-1} \circ \cdots \circ \phi_0(r^{e-i}P)$. For all $i \in [\![1\ ;\ r]\!]$, ϕ_i has degree r, so it suffices to prove that ϕ_i is descending. Since r is inert in K, by Proposition 1.23.(i), ϕ_1 is descending. Let $i \in [\![2\ ;\ e]\!]$. Assume that $\phi_1, \cdots, \phi_{i-1}$ are descending. By Proposition 1.23.(ii), ϕ_i is either descending or ascending. If it was ascending, since there is only one ascending isogeny, from E_{i-1}, we would have $\phi_i = \widehat{\phi_{i-1}}$ so that ϕ factors through $[r]$ and $E[r] \subseteq \ker(\phi)$. But $\ker(\phi)$ is cyclic and $E[r]$ is not. Contradiction. Hence, ϕ_i is descending. This completes the proof. □

Let q be a prime $\neq r, \ell, p$ splitting in K and $\mathfrak{q}$ a prime ideal of $\mathcal{O}_K$ lying above q. Let $\mathfrak{q}^{(i,j)} := \mathfrak{q} \cap \mathcal{O}_{i,j}$ for all $i, j \in \mathbb{N}$. To lighten the notations, the exponent (i, j) will often be omitted. Let $E \in \rho(\mathrm{Ell}(\mathcal{O}_n))$, such that $|E(\mathbb{F}_{p^2})| = (fr^e)^2$ and let $P \in E[r^e]$ of order r^e. For our construction, we need to compute the action of $\mathfrak{q}^{(n,e)}$ on $E/\langle P\rangle$ (with its induced $\mathcal{O}_{n,e}$-orientation). This computation uses descending r-ladders and the ideas of Paragraph 1.5.2.

Lemma C.9. *There is a descending r-ladder of length n and degree q:*

$$\begin{array}{ccccccccccc}
E_0 & \xrightarrow{\phi_1} & E_1 & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{e-1}} & E_{e-1} & \xrightarrow{\phi_e} & E_e \\
\downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & & & \downarrow{\scriptstyle \psi_{e-1}} & & \downarrow{\scriptstyle \psi_e} \\
F_0 := \mathfrak{q}\cdot E_0 & \xrightarrow{\phi'_1} & F_1 := \mathfrak{q}\cdot E_1 & \xrightarrow{\phi'_2} & \cdots & \xrightarrow{\phi'_{e-1}} & F_{e-1} := \mathfrak{q}\cdot E_{e-1} & \xrightarrow{\phi'_e} & F_e := \mathfrak{q}\cdot E_e
\end{array}$$

such that:

(i) $E_0 = E$ *and* $E_e = E/\langle P\rangle$.

(ii) $\phi := \phi_e \circ \cdots \circ \phi_1$ *has kernel* $\langle P\rangle$.

(iii) $\ker(\psi_i) = E_i[\mathfrak{q}]$ *for all* $i \in [\![0\ ;\ e]\!]$.

(iv) $\phi' := \phi'_e \circ \cdots \circ \phi'_1$ *has kernel* $\langle \psi_0(P)\rangle$ *or equivalently,* $\mathfrak{q}\cdot(E/\langle P\rangle) = (\mathfrak{q}\cdot E)/\langle \psi_0(P)\rangle$.

Proof. As in the proof of Lemma C.8, point (ii), we define $\phi_0 = [1]_E$ and for all $i \in [\![1\ ;\ e]\!]$, $\phi_i : E_{i-1} \longrightarrow E_i$ as the r-isogeny of kernel generated by $Q_i := \phi_{i-1} \circ \cdots \circ \phi_0(r^{e-i}P)$, so that points (i) and (ii) are satisfied. For all $i \in [\![0\ ;\ e]\!]$, $\psi_i : E_i \longrightarrow \mathfrak{q}\cdot E_i$ is the isogeny associated to $\mathfrak{q}$ ($\ker(\psi_i) = E_i[\mathfrak{q}]$), so that point (iii) is satisfied.

To prove the existence of the r-ladder satisfying point (iv), we simply prove that for all $i \in [\![1\ ;\ e]\!]$, $\psi_i \circ \phi_i$ factors through ψ_{i-1} by an isogeny ϕ'_i of kernel $\langle \psi_{i-1}(Q_i)\rangle$. By [15, Corollary III.4.11], it suffices to prove that $\ker(\psi_{i-1}) \subseteq \ker(\psi_i \circ \phi_i)$. The equality $\ker(\phi'_i) = \langle \psi_{i-1}(Q_i)\rangle$ will then follow from $\psi_i \circ \phi_i = \phi'_i \circ \psi_{i-1}$.

Let ι_{i-1} be the primitive $\mathcal{O}_{n,i-1}$-orientation defined on E_{i-1}. Then, $\iota_i := \phi_{i*}(\iota_{i-1})$ is a primitive $\mathcal{O}_{n,i}$-orientation because ϕ_i is vertical, as we saw when we proved Lemma C.8, point (ii). Let $P \in \ker(\psi_{i-1}) = E_{i-1}[\mathfrak{q}^{(n,i-1)}]$. Then, we have $\iota_{i-1}(\alpha)(P) = 0$ for all $\alpha \in \mathfrak{q}^{(n,i-1)}$, so that:

$$\iota_i(\alpha)(\phi_i(P)) = \frac{1}{r}\phi_i\iota_{i-1}(\alpha)\widehat{\phi_i}\phi_i(P) = \frac{1}{r}\phi_i\iota_{i-1}(\alpha)[r](P) = \phi_i\iota_{i-1}(\alpha)(P) = 0$$

for all $\alpha \in \mathfrak{q}^{(n,i)} \subseteq \mathfrak{q}^{(n,i-1)}$. Hence $\phi_i(P) \in E_i[\mathfrak{q}^{(n,i)}]$ *i.e.* $\psi_i \circ \phi_i(P) = 0$. This completes the proof. □

We can construct the r-ladder of Lemma C.8 with the techniques of Paragraph 1.5.2. For all $i \in [\![1\ ;\ e]\!]$, $j(F_i)$ is solution of:

$$\begin{cases} \Phi_q(j(E_i), x) = 0 \\ \Phi_r(j(F_{i-1}), x) = 0 \end{cases} \iff \gcd(\Phi_q(j(E_i), x), \Phi_r(j(F_{i-1}), x)) = 0 \quad (\star)_i.$$

Lemma C.10. *Conversely, consider a descending r-ladder of length e and degree q:*

$$\begin{array}{ccccccccc} E_0 & \xrightarrow{\phi_1} & E_1 & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{e-1}} & E_{e-1} & \xrightarrow{\phi_e} & E_e \\ \downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & & & \downarrow{\scriptstyle \psi_{e-1}} & & \downarrow{\scriptstyle \psi_e} \\ F_0 & \xrightarrow{\phi'_1} & F_1 & \xrightarrow{\phi'_2} & \cdots & \xrightarrow{\phi'_{e-1}} & F_{e-1} & \xrightarrow{\phi'_e} & F_e \end{array}$$

and assume that:

(i) $E_0 = E$ *and* $\ker(\phi_i) = \langle \phi_{i-1} \circ \cdots \circ \phi_0(r^{e-i}P) \rangle$ *for all* $i \in [\![1 \ ; \ e]\!]$ *(with* $\phi_0 = [1]_{E_0}$*).*

(ii) $p > q\ell^{2n}r^{2e}|\Delta_K|$.

(iii) $F_0 = \mathfrak{q} \cdot E_0$

(iv) $j(F_i)$ *is solution of* $(\star)_i$ *for all* $i \in [\![1 \ ; \ e]\!]$.

(v) $\mathfrak{q}^2$ *is not principal in* $\mathcal{O}_n$.

Then $\ker(\psi_i) = E_i[\mathfrak{q}]$ *and* $F_i = \mathfrak{q} \cdot E_i$ *for all* $i \in [\![1 \ ; \ e]\!]$.

Proof. See Proposition 1.33. The same ideas apply. □

In the following, we shall work under the hypothesis of Lemma C.10.

C.3.1 Settings and public data

Supersingular elliptic curves E_0 and E_1

We fix $E_0 \in \rho(\mathrm{Ell}(\mathcal{O}_n))$ and $E_1 := [\mathfrak{s}] \cdot E_0$ for a secret ideal class $[\mathfrak{s}] \in \mathrm{Cl}(\mathcal{O}_n)$ such that $|E_0(\mathbb{F}_{p^2})| = |E_1(\mathbb{F}_{p^2})| = (fr^e)^2 = (p \mp 1)^2$ (to ensure that $E_b[r^e] \subseteq E_b(\mathbb{F}_{p^2})$ for $b \in \{0, 1\}$, by Lemma C.8.(i)). E_0 can be constructed as the ending curve of a descending ℓ-isogeny chain $(E_{0,i})_{0 \le i \le n}$ obtained by random descent of the ℓ-isogeny graph from a known curve $E_{0,0} \in \rho(\mathrm{Ell}(\mathcal{O}_K))$. Unfortunately, this process does not guarantee the cardinality of $E_0(\mathbb{F}_{p^2})$, which can be in a limited set of values $\{(p-1)^2, p^2 - p + 1, p^2 + 1, p^2 + p + 1, (p+1)^2\}$. Since $|E(\mathbb{F}_{p^2})|$ is roughly uniform when $E/\mathbb{F}_{p^2}$ is sampled uniformly among elliptic curves defined over $\mathbb{F}_{p^2}$ as [52, Theorem 1.1] seems to indicate, there is heuristically a probability of success close to $\frac{1}{5}$. By repeating the descent of the ℓ-isogeny graph we may then reach the desired cardinality. For, E_1 we take the ending curve of $(E_{1,i})_{0 \le i \le n} := \mathfrak{s} \cdot (E_{0,i})_{0 \le i \le n}$ where $\mathfrak{s}$ is uniformly sampled among the $\mathcal{O}_n$-ideals of norm prime to r and ℓ, until $|E_1(\mathbb{F}_{p^2})| = (fr^e)^2$.

Basis of the r^e torsion of E_0 and E_1

We fix (P_0, Q_0), a basis of $E_0[r^e]$. To do that, we execute a slightly modified version of Algorithm 5, using the fact that $E_0[r^e] \subseteq E_0(\mathbb{F}_{p^2})$. First, we sample $P \in E_0(\mathbb{F}_{p^2})$ with uniform distribution and compute fP. Then $fP \in E_0[r^e]$ since $E_0(\mathbb{F}_{p^2}) = E_0[fr^e]$ by Lemma C.8.(i) and fP has order r^e with probability $1 - \frac{1}{r}$ (it can be checked by multiplying fP by r successively). If it is the case, we set $P_0 := fP$. Otherwise, we repeat this step. Then, we sample $Q \in E_0(\mathbb{F}_{p^2})$ in a similar way and compute fQ, until $e_{r^e}(P_0, fQ)$ has order r^e and set $Q_0 := fQ$ when this condition is met.

Then, we know that every point $R \in E_0[r^e]$ of order r^e is of the form $R = \lambda P_0 + \mu Q_0$ with $\lambda, \mu \in \mathbb{Z}/r^e\mathbb{Z}$ such that λ or μ is invertible modulo r^e. If $R' := \lambda' P_0 + \mu' Q_0$ is another point of order r^e, then $\langle R \rangle = \langle R' \rangle$ if and only if there exists $\nu \in (\mathbb{Z}/r^e\mathbb{Z})^\times$ such that $R' = \nu R$ *i.e.* $\lambda' = \nu\lambda$ and $\mu' = \nu\mu$. Hence, the cyclic subgroups of order r^e of E_0 are in bijection with $\mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$ via the map:

$$(\lambda : \mu) \in \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z}) \longmapsto \langle \lambda P_0 + \mu Q_0 \rangle.$$

For all $\alpha := (\lambda : \mu) \in \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$, we shall denote by $\langle\alpha\rangle$ the image subgroup $\langle\lambda P_0 + \mu Q_0\rangle$. Given an ideal $\mathfrak{a} \subseteq \mathcal{O}_n$, of norm prime to r and ℓ, and $\varphi_\mathfrak{a} : E_0 \longrightarrow \mathfrak{a} \cdot E_0$, the isogeny of kernel $E_0[\mathfrak{a}]$, $B_\mathfrak{a} := (\varphi_\mathfrak{a}(P_0), \varphi_\mathfrak{a}(Q_0))$ is a basis of $\mathfrak{a} \cdot E_0[r^e]$, since:

$$e_{r^e}(B_\mathfrak{a}) = e_{r^e}(\varphi_\mathfrak{a}(P_0), \varphi_\mathfrak{a}(Q_0)) = e_{r^e}(P_0, Q_0)^{\deg(\varphi_\mathfrak{a})} = e_{r^e}(P_0, Q_0)^{N(\mathfrak{a})},$$

with $N(\mathfrak{a}) \wedge r = 1$, so that $e_{r^e}(B_\mathfrak{a})$ is still a primitive r^e-th root of unity. For all $\alpha := (\lambda : \mu) \in \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$, we shall also denote by $\langle\alpha\rangle_{B_\mathfrak{a}}$ or simply $\langle\alpha\rangle$ the subgroup of $\mathfrak{a} \cdot E_b$ generated by $\lambda\varphi_\mathfrak{a}(P_0) + \mu\varphi_\mathfrak{a}(Q_0)$. By Lemma C.9, we know that $\mathfrak{a} \cdot E_0/\langle\alpha\rangle = (\mathfrak{a} \cap \mathcal{O}_{n,e}) \cdot (E_0/\langle\alpha\rangle)$.

In particular, we can consider $E_1/\langle\alpha\rangle = \mathfrak{s} \cdot E_0/\langle\alpha\rangle = (\mathfrak{s} \cap \mathcal{O}_{n,e}) \cdot (E_0/\langle\alpha\rangle)$ and the basis $(P_1, Q_1) := (\varphi_\mathfrak{s}(P_0), \varphi_\mathfrak{s}(Q_0))$ of $E_1[r^e]$. We assume that this basis is public along with (P_0, Q_0).

Public chains to compute the action of $\mathrm{Cl}(\mathcal{O}_n)$ horizontally and the action of $\mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$ vertically on E_0 and E_1

To have a restricted effective group action, we assume that $\mathrm{Cl}(\mathcal{O}_{n,e})$ is generated by $\mathfrak{q}_1^{(n,e)}, \cdots, \mathfrak{q}_t^{(n,e)}$, where $\mathfrak{q}_1, \cdots, \mathfrak{q}_t$ are prime ideals of $\mathcal{O}_K$ lying above small splitting primes $q_1, \cdots, q_t$ distinct from r, ℓ, p. We even assume that every ideal of $\mathrm{Cl}(\mathcal{O}_{n,e})$ can be written as a product of these primes with exponents in $[\![-s\ ;\ s]\!]$, $s \in \mathbb{N}^*$ being relatively small (negative exponents meaning exponentiation of the conjugate ideal). Not that that this hypothesis is essential to make the projection easily computable but makes OSIDH insecure. This is the very reason why our hash proof system fails.

We assume that the chains $(E_{b,i})_{0 \leq i \leq n}$ associated to $E_b = E_{b,n}$ for $b \in \{0, 1\}$ remain secret but that the chains:

$$E_{b,j}^{(-s)} := (\mathfrak{q}_j^{(n)})^{-s} \cdot E_b \longrightarrow \cdots \longrightarrow E_b \longrightarrow \cdots \longrightarrow E_{b,j}^{(s)} := (\mathfrak{q}_j^{(n)})^{s} \cdot E_b$$

are public for all $j \in [\![1\ ;\ t]\!]$. Note that these chains can efficiently be computed with the techniques of Paragraph 1.5.2. For all $\mathcal{O}_n$-ideal $\mathfrak{a}$, we denote by $\varphi_{b,\mathfrak{a}} : E_b \longrightarrow \mathfrak{a} \cdot E_b$, the isogeny of kernel $E_b[\mathfrak{a}]$. We assume that the basis $(P_{b,j}^{(k)}, Q_{b,j}^{(k)}) := (\varphi_{b,\mathfrak{q}_j^k}(P_b), \varphi_{b,\mathfrak{q}_j^k}(Q_b))$ of $E_{b,j}^{(k)}[r^e]$ is known for all $k \in [\![-s\ ;\ s]\!]$ and $j \in [\![1\ ;\ t]\!]$. It can be computed by expressing every isogeny of the chain above by exhaustive search among the $q_j + 1$ possible q_j-isogenies to match the j-invariant of the codomain.

C.3.2 The Hash Proof System HashOSIDH

Now, we construct the following hash proof system, that we shall call HashOSIDH. Let:

$$\Sigma := \left\{ \left(((E_{0,j}^{(k)}/\langle\alpha\rangle)_{\substack{1 \leq j \leq t \\ -s \leq k \leq s}}, (E_{1,j}^{(k)}/\langle\beta\rangle)_{\substack{1 \leq j \leq t \\ -s \leq k \leq s}} \right) \mid \alpha, \beta \in \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z}) \right\}$$

and:

$$L := \left\{ \left(((E_{0,j}^{(k)}/\langle\alpha\rangle)_{\substack{1 \leq j \leq t \\ -s \leq k \leq s}}, (E_{1,j}^{(k)}/\langle\alpha\rangle)_{\substack{1 \leq j \leq t \\ -s \leq k \leq s}} \right) \mid \alpha \in \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z}) \right\}.$$

To lighten the notations, the elements of Σ will be denoted $(E_0/\langle\alpha\rangle, E_1/\langle\beta\rangle)$ (and similarly for the elements of L), omitting the chains which are implicitly known.

The definition of the projection space $\mathcal{P}$ is more subtle and will become natural later (see the definition of π and Lemma C.11). We consider the set $\mathcal{S}$ of tuples (E, ι, P, Q) where (E, ι) is a primitively $\mathcal{O}_n$-oriented elliptic curve whose K-equivalence class is in $\rho(\mathrm{Ell}(\mathcal{O}_n))$ and (P, Q) is a basis of $E[r^e]$. We consider the equivalence relation $\sim$ over $\mathcal{S}$ defined as follows: $(E, \iota, P, Q) \sim (E', \iota', P', Q')$ if and only if there exists an isomorphism $\lambda : E \xrightarrow{\sim} E'$ such that $\lambda_*(\iota) = \iota'$ and $x, y \in \mathcal{O}_{n,e}$ of norm prime to $pr\ell$ such that $\lambda \circ \iota(x)(P) = \iota'(y)(P')$ and $\lambda \circ \iota(x)(Q) = \iota'(y)(Q')$. We set $\mathcal{P} := \mathcal{S}/\sim$. The elements of $\mathcal{P}$ will be denoted by $[E, P, Q]$, omitting the $\mathcal{O}_n$-orientation, which is unique on E under hypothesis (ii) of Lemma C.10, by Theorem 1.27.

We also set $\mathcal{K} := \mathrm{Cl}(\mathcal{O}_{n,e}) \times \{0,1\}$, $W := \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$ and $\Gamma := \rho(\mathrm{Ell}(\mathcal{O}_{n,e}))$. We define the functions:

$$\begin{array}{rcl} \Lambda : \mathrm{Cl}(\mathcal{O}_{n,e}) \times \{0,1\} \times \Sigma & \longrightarrow & \rho(\mathrm{Ell}(\mathcal{O}_{n,e})) \\ ((\mathfrak{a}], b), (F_0, F_1)) & \longmapsto & [\mathfrak{a}] \cdot F_b \end{array}$$

$$\text{and} \quad \begin{array}{rcl} \pi : \mathrm{Cl}(\mathcal{O}_{n,e}) \times \{0,1\} & \longrightarrow & \mathcal{P} \\ ([\mathfrak{a}], b) & \longmapsto & [[\mathfrak{a}\mathcal{O}_n] \cdot E_b, \varphi_{b,\mathfrak{a}}(P_b), \varphi_{b,\mathfrak{a}}(Q_b)] \end{array},$$

where $\varphi_{b,\mathfrak{a}} : E_b \longrightarrow (\mathfrak{a}\mathcal{O}_n) \cdot E_b$ is the isogeny of kernel $E_b[\mathfrak{a}\mathcal{O}_n]$, for all ideal $\mathfrak{a} \subseteq \mathcal{O}_{n,e}$ of norm prime to r and ℓ and $b \in \{0,1\}$. Note that, by the definition of $\mathcal{P}$, π is well defined, meaning that the class $\pi([\mathfrak{a}], b)$ does not depend on the representative $\mathfrak{a}$ chosen in the class $[\mathfrak{a}]$. In practice, the computed value of $\pi([\mathfrak{a}], b)$ is the value of a representative. Finally, we define:

$$\begin{array}{rcl} \mathrm{ProjEval} : \mathcal{P} \times \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z}) & \longrightarrow & \rho(\mathrm{Ell}(\mathcal{O}_{n,e})) \\ ([E,P,Q], \alpha := (a:b)) & \longmapsto & E/\langle\alpha\rangle_{(P,Q)} := E/\langle aP + bQ\rangle \end{array}$$

and:

$$\begin{array}{rcl} \omega : L & \longrightarrow & \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z}) \\ (E_0/\langle\alpha\rangle, E_1/\langle\alpha\rangle) & \longmapsto & \alpha \end{array}.$$

The well definition of ProjEval is a consequence of the following lemma:

Lemma C.11. *Let $(E,P,Q), (E',P',Q') \in \mathcal{S}$ such that $(E,P,Q) \sim (E',P',Q')$ and $\alpha \in \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$. Then $E/\langle\alpha\rangle_{(P,Q)} \simeq E'/\langle\alpha\rangle_{(P',Q')}$.*

Proof. Since $(E,P,Q) \sim (E',P',Q')$, there exists an isomorphism $\lambda : E \xrightarrow{\sim} E'$ and $x, y \in \mathcal{O}_{n,e}$ of norm prime to $pr\ell$ such that $\lambda \circ \iota(x)(P) = \iota'(y)(P')$ and $\lambda \circ \iota(x)(Q) = \iota'(y)(Q')$, where ι and ι' are the primitive $\mathcal{O}_n$-orientations of E and E' respectively. We set $\alpha := (a:b)$. Then, we have:

$$\begin{aligned} E'/\langle\alpha\rangle_{(P,Q)} &\simeq [y\mathcal{O}_{n,e}] \cdot (E'/\langle\alpha\rangle_{(P',Q')}) \quad (\text{since } y \in \mathcal{O}_{n,e}) \\ &= [y\mathcal{O}_{n,e}] \cdot (E'/\langle aP' + bQ'\rangle) \simeq [y\mathcal{O}_n] \cdot E'/\langle\iota'(y)(aP' + bQ')\rangle \quad (\text{by Lemma C.9.(iv)}) \\ &= E'/\langle\iota'(y)(aP' + bQ')\rangle = E'/\langle\lambda(a\iota(x)(P) + b\iota(x)(Q))\rangle \\ &\simeq E/\langle\iota(x)(aP + bQ)\rangle \quad (\text{since } \lambda \text{ is an isomorphism}) \\ &= [x\mathcal{O}_n] \cdot E/\langle\iota(x)(aP + bQ)\rangle \simeq [x\mathcal{O}_{n,e}] \cdot (E/\langle aP + bQ\rangle) \quad (\text{by Lemma C.9.(iv)}) \\ &= E/\langle aP + bQ\rangle = E/\langle\alpha\rangle_{(P,Q)} \quad (\text{since } x \in \mathcal{O}_{n,e}) \end{aligned}$$

□

We now justify that $\Pi := (\Lambda, \pi, \mathrm{ProjEval}, L, \Sigma, W, \mathcal{K}, \mathcal{P}, \Gamma)$ is (almost but not completely) a hash proof system.

Lemma C.12. *The following diagram is commutative:*

$$\begin{array}{ccc} (\mathrm{Cl}(\mathcal{O}_{n,e}) \times \{0,1\}) \times L & \xrightarrow{\Lambda} & \rho(\mathrm{Ell}(\mathcal{O}_{n,e})). \\ {\scriptstyle \pi\times\omega}\downarrow & \nearrow_{\mathrm{ProjEval}} & \\ \mathcal{P} \times \mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z}) & & \end{array}$$

Proof. This is a direct consequence of Lemma C.9. □

Lemma C.13. *Λ, π and* ProjEval *are efficiently computable (*i.e. *computable in polynomial time in the parameters $n, e, \ell, r, q_1, \cdots, q_t, s$).*

Proof. ProjEval$((E,P,Q),\alpha)$ is efficiently computable by computing the chain of r-isogenies whose product is the isogoneny of kernel $\langle\alpha\rangle_{(P,Q)}$ for all $[E,P,Q]\in\mathcal{P}$ and $\alpha\in\mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$. This computation can be optimized with computation trees, as in [3, Section 4.2.2].

Let $b\in\{0,1\}$. The chain:

$$(E_{b,j}^{(-s)},P_{b,j}^{(-s)},Q_{b,j}^{(-s)})\longrightarrow\cdots\longrightarrow(E_b,P_b,Q_b)\longrightarrow\cdots\longrightarrow(E_{b,j}^{(-s)},P_{b,j}^{(s)},Q_{b,j}^{(s)})$$

is public for all $j\in[\![1\ ;\ t]\!]$. Hence, under the hypothesis of Lemma C.10, we can compute efficiently the chain:

$$E_{b,j}^{(-s)}/\langle\alpha\rangle:=(\mathfrak{q}_j^{(n)})^{-s}\cdot(E_b/\langle\alpha\rangle)\longrightarrow\cdots\longrightarrow E_b/\langle\alpha\rangle\longrightarrow\cdots\longrightarrow E_{b,j}^{(s)}/\langle\alpha\rangle:=(\mathfrak{q}_j^{(n)})^{s}\cdot(E_b/\langle\alpha\rangle)$$

for all $j\in[\![1\ ;\ t]\!]$ and $\alpha\in\mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$, by computing the chain of r-isogenies whose product is the isogoneny of kernel $\langle\alpha\rangle_{(P_b,Q_b)}$ and using the techniques of Paragraph 1.5.2 to construct ladders on the right and on the left of this chain, whose last elements correspond to the chain above. Hence, given $\mathfrak{a}\subseteq\mathcal{O}_{n,e}$ expressed as a product of the $\mathfrak{q}_j$: $\mathfrak{a}=\prod_{j=1}^t\mathfrak{q}_j^{e_j}$, with $e_1,\cdots,e_t\in[\![-s\ ;\ s]\!]$, and $\alpha_0,\alpha_1\in\mathbb{P}^1(\mathbb{Z}/r^e\mathbb{Z})$:

$$\Lambda(([\mathfrak{a}],b),(E_0/\langle\alpha_0\rangle,E_1/\langle\alpha_1\rangle))=[\mathfrak{a}]\cdot(E_b/\langle\alpha_b\rangle)$$

is efficiently computable with the method of Paragraph 2.2, using the chains computed above.

Knowing the chain:

$$E_{b,j}^{(-s)}\longrightarrow\cdots\longrightarrow E_b\longrightarrow\cdots\longrightarrow E_{b,j}^{(-s)}$$

is public for all $j\in[\![1\ ;\ t]\!]$, we can easily compute $[\mathfrak{a}\mathcal{O}_n]\cdot E_b$ using the methods of Paragraph 2.2. To compute $\pi([\mathfrak{a}],b)$, we still have to compute the image of the basis (P_b,Q_b) by $\varphi_{b,\mathfrak{a}}$, the isogeny associated to $\mathfrak{a}$. $\varphi_{b,\mathfrak{a}}$ is obtained by composition of e_j q_j-isogenies for $j\in[\![1\ ;\ t]\!]$. Each q_j-isogeny can be computed using Vélu's formulas by an exhaustive search among the q_j+1 possible isogenies in order to map the j-invariant of the domain to the j-invariant of the codomain. The complexity of this exhaustive search is $O(s(q_j+1))$ uses of Vélu's formulas for all $j\in[\![1\ ;\ t]\!]$, which is costly but still polynomial. □

Remark C.14. Note that in the course of the proof, we used the fact that every ideal class of $\mathrm{Cl}(\mathcal{O}_{n,e})$ can be expressed as a product of powers of the $\mathfrak{q}_j$ with exponents in $[\![-s\ ;\ s]\!]$. This will eventually break HashOSIDH.

Lemma C.15. *HashOSIDH is 2^{-1}-universal.*

Proof. Let $([\mathfrak{a}],b)\in\mathrm{Cl}(\mathcal{O}_{n,e})\times\{0,1\}$ be a key (secret and sampled with uniform distribution). Let $(F_0,F_1)=(E_0/\langle\alpha_0\rangle,E_1/\langle\alpha_1\rangle)\in\Sigma\setminus L$ be sampled with uniform distribution. Since $(F_0,F_1)\notin L$, we have $\alpha_0\neq\alpha_1$. Let us assume that an attacker with unbounded capabilities knows (F_0,F_1) and $\pi([\mathfrak{a}],b)=[[\mathfrak{a}\mathcal{O}_n]\cdot E_b,\varphi_{b,\mathfrak{a}}(P_b),\varphi_{b,\mathfrak{a}}(Q_b)]$ and wants to recover $\Lambda(([\mathfrak{a}],b),(F_0,F_1))=\mathfrak{a}\cdot F_b$.

We assume that $b=0$. Let $\mathfrak{b}:=\mathfrak{a}\cdot(\overline{\mathfrak{s}}\cap\mathcal{O}_{n,e})$. We prove that $\pi([\mathfrak{a}],0)=\pi([\mathfrak{b}],1)$. Let (E,ι,P,Q) and (E',ι',P',Q') be representatives of $\pi([\mathfrak{a}],0)$ and $\pi([\mathfrak{b}],1)$ respectively. It suffices to prove that $(E,\iota,P,Q)\sim(E',\iota',P',Q')$. We know that there exists two isomorphisms $\lambda:E\xrightarrow{\sim}[\mathfrak{a}\mathcal{O}_n]\cdot E_0$ and $\lambda':E'\xrightarrow{\sim}[\mathfrak{b}\mathcal{O}_n]\cdot E_1$ and $x,y,x',y'\in\mathcal{O}_{n,e}$ of norm prime to $pr\ell$ such that:

$$\begin{cases}\lambda\circ\iota(x)(P)=\iota_{0,\mathfrak{a}}(y)\circ\varphi_{0,\mathfrak{a}}(P_0)\\ \lambda\circ\iota(x)(Q)=\iota_{0,\mathfrak{a}}(y)\circ\varphi_{0,\mathfrak{a}}(Q_0)\end{cases}\quad\text{and}\quad\begin{cases}\lambda'\circ\iota'(x')(P')=\iota_{1,\mathfrak{b}}(y')\circ\varphi_{1,\mathfrak{b}}(P_1)\\ \lambda'\circ\iota'(x')(Q')=\iota_{1,\mathfrak{b}}(y')\circ\varphi_{1,\mathfrak{b}}(Q_1)\end{cases}\quad(\star),$$

where $\iota_{0,\mathfrak{a}}$ and $\iota_{1,\mathfrak{b}}$ are the $\mathcal{O}_n$-orientations of $[\mathfrak{a}\mathcal{O}_n]\cdot E_0$ and $[\mathfrak{b}\mathcal{O}_n]\cdot E_1$ respectively. Since $E_1=[\mathfrak{s}]\cdot E_0$, we have $E_0=[\overline{\mathfrak{s}}]\cdot E_1$, so that $[\mathfrak{a}\mathcal{O}_n]\cdot E_0=[\mathfrak{b}\mathcal{O}_n]\cdot E_1$ and $\varphi_{1,\mathfrak{b}}=\varphi_{0,\mathfrak{a}}\circ\varphi_{1,\overline{\mathfrak{s}}}$. Under hypothesis (ii) of Lemma C.10, we then have $\iota_{0,\mathfrak{a}}=\iota_{1,\mathfrak{b}}$ by Theorem 1.27. Furthermore, $P_1=\varphi_{0,\mathfrak{s}}(P_0)$, so that:

$$\varphi_{1,\mathfrak{b}}(P_1)=\varphi_{0,\mathfrak{a}}\circ\varphi_{1,\overline{\mathfrak{s}}}\circ\varphi_{0,\mathfrak{s}}(P_0)=N(\mathfrak{s})\varphi_{0,\mathfrak{a}}(P_0)$$

and by the same argument $\varphi_{1,\mathfrak{b}}(Q_1) = N(\mathfrak{s})\varphi_{0,\mathfrak{a}}(Q_0)$. Combining that with $(\star)$, we get:

$$\begin{cases} \lambda^{-1} \circ \lambda \circ \iota(x'y)(P') = \iota(N(\mathfrak{s})xy')(P) \\ \lambda^{-1} \circ \lambda \circ \iota(x'y)(Q') = \iota(N(\mathfrak{s})xy')(Q) \end{cases},$$

so that $(E', \iota', P', Q') \sim (E, \iota, P, Q)$.

By similar arguments, we get that $\pi([\mathfrak{a}], b) = \pi([\mathfrak{b}], 0)$, with $\mathfrak{b} := \mathfrak{a} \cdot (\overline{\mathfrak{s}} \cap \mathcal{O}_{n,e})$, when $b = 1$. Hence, the attacker can guess $([\mathfrak{a}], b)$ or $([\mathfrak{b}], 1-b)$.

With its unbounded capabilities, the attacker can also guess α_0 and α_1 from $(F_0, F_1) = (E_0/\langle\alpha_0\rangle, E_1/\langle\alpha_1\rangle)$. We also have:

$$\begin{aligned} \Lambda(([\mathfrak{a}], b), (F_0, F_1)) &= [\mathfrak{a}] \cdot F_b = [\mathfrak{a}\mathcal{O}_n] \cdot E_b/\langle\alpha_b\rangle = [\mathfrak{b}\mathcal{O}_n] \cdot E_{1-b}/\langle\alpha_b\rangle \\ &\neq [\mathfrak{b}\mathcal{O}_n] \cdot E_{1-b}/\langle\alpha_{1-b}\rangle = \Lambda(([\mathfrak{b}], 1-b), (F_0, F_1)) \end{aligned}$$

since $\alpha_b \neq \alpha_{1-b}$, the inequality is a consequence of Lemma C.16 below. Hence, the attacker finds the value of the hash function with 1 bit of indetermination, so that:

$$H_\infty(\Lambda(([\mathfrak{a}], b), (F_0, F_1))|(\pi([\mathfrak{a}], b), (F_0, F_1))) = -\log\left(\frac{1}{2}\right).$$

□

Lemma C.16. *Let $E \in \rho(\mathrm{Ell}(\mathcal{O}_n))$. Then, the map:*

$$\begin{array}{rcl} \{\textit{cyclic subbroups of order } r^e \textit{ in } E[r^e]\} & \longrightarrow & \rho(\mathrm{Ell}(\mathcal{O}_{n,e})) \\ H & \longmapsto & E/H \end{array}$$

is injective.

Remark C.17. Note that under hypothesis (ii) of Lemma C.10, we can omit the $\mathcal{O}_{n,e}$-orientation when considering elements of $\rho(\mathrm{Ell}(\mathcal{O}_{n,e}))$, and see these elements as elliptic curves up to isomorphism, or equivalently, as j-invariants. Hence, we even have an injective map when considering j-invariants.

Proof. Let H, H' be two cyclic subgroups of order r^e in E such that $E/H = E/H'$. Then, as in the proof of Lemma C.8.(ii), we have descending r-isogeny chains $(E_i)_{0\leq i\leq e}$ and $(E'_i)_{0\leq i\leq e}$ whose composition are the isogenies $E \longrightarrow E/H$ and $E \longrightarrow E/H'$ respectively. We assume that these chains are distinct. Then, there exists $i \in [\![1\ ;\ e]\!]$ such that $E_i = E'_i$ and $E_{i-1} \neq E'_{i-1}$. Hence, E_i has two r-ascending isogenies, which contradicts Proposition 1.23. Then, the two chains are the same and we have $H = H'$. □

Actually, HashOSIDH satisfies all the hypothesis but the subset membership problem.Indeed, given $(E_0/\langle\alpha\rangle, E_1/\langle\beta\rangle) \in \Sigma$, our attack presented in Section 3.4 enables to recover the chains of $E_0/\langle\alpha\rangle$ and $E_1/\langle\beta\rangle$ *i.e.* to recoverα and β. As a consequence, the subset membership problem becomes easy: one only has to check if $\alpha = \beta$. The choice of other parameters to block the attack would make the computation of the projection much more difficult.