SCALLOP-HD: group action from 2-dimensional isogenies

Mingjie Chen[1] and Antonin Leroux[2,3]

[1] University of Birmingham, UK
m.chen.1@bham.ac.uk
[2] DGA-MI, Bruz, France
antonin.leroux@polytechnique.org
[3] IRMAR, UMR 6625, Université de Rennes, France

Abstract. We present SCALLOP-HD, a novel group action that builds upon the recent SCALLOP group action introduced by De Feo, Fouotsa, Kutas, Leroux, Merz, Panny and Wesolowski in 2023. While our group action uses the same action of the class group $\mathrm{Cl}(\mathfrak{O})$ on $\mathfrak{O}$-oriented curves where $\mathfrak{O} = \mathbb{Z}[f\sqrt{-1}]$ for a large prime f as SCALLOP, we introduce a different orientation representation: The new representation embeds an endomorphism generating $\mathfrak{O}$ in a 2^e-isogeny between abelian varieties of dimension 2 with Kani's Lemma, and this representation comes with a simple algorithm to compute the class group action. Our new approach considerably simplifies the SCALLOP framework, potentially surpassing it in efficiency — a claim to be confirmed by implementation results. Additionally, our approach streamlines parameter selection. The new representation allows us to select efficiently a class group $\mathrm{Cl}(\mathfrak{O})$ of smooth order, enabling polynomial-time generation of the lattice of relation, hence enhancing scalability in contrast to SCALLOP.

To instantiate our SCALLOP-HD group action, we introduce a new technique to apply Kani's Lemma in dimension 2 with an isogeny diamond obtained from commuting endomorphisms. This method allows one to represent arbitrary endomorphisms with isogenies in dimension 2, and may be of independent interest.

1 Introduction

The group action framework is a powerful abstract tool to build cryptographic protocols such as non-interactive key exchange [CLM+18], signatures [BKV19], threshold schemes [CS20,DFM20], ring signatures [BKP20], group signatures [BDK+23], partial-blind signatures [KLLQ23], updatable encryption [LR22], and, among other things, various applications as discussed in [ADFMP20].

Isogenies provide the only known way to instantiate this framework in a manner resistant to quantum computers. There are two achievable flavours of group action: the "restricted" group action (REGA) such as the one introduced for the CSIDH key exchange in [CLM+18], and the "full" variant (EGA) introduced for the CSI-FiSh signature scheme in [BKV19]. While the restricted

variant is already interesting, the full variant is required by the more elaborate constructions.

Unfortunately, isogeny-based group action suffer from various problems. First, the underlying hard problem can be solved in subexponential time by a quantum computer [BLMP19,BS20,Pei20] which renders their security hard to estimate and reduces their efficiency. Second, current methods for instantiating the full variant require subexponential precomputation as demonstrated in [BKV19,DFFK+23] and reaffirmed in a recent blog post by Panny[4]. This makes it computationally infeasible to obtain the full variant that meets the quantum security requirements from NIST.

The second obstacle is what motivated the introduction of the recent SCAL-LOP scheme in [DFFK+23] where the precomputation (while still subexponential) is much more practical than in the setting of CSI-FiSh [BKV19]. The authors of SCALLOP demonstrated the interest of their constructions by scaling the parameters to sizes known to be computationally unreachable in the setting of CSI-FiSh. However, the efficiency of SCALLOP is much worse than CSIDH, and the amount of precomputation required to reach the higher levels of security (equivalent to the CSIDH-8192 variant of [CSCDJRH22] for instance) promises to be quite extensive.

The improvements in scalability achieved by SCALLOP, when compared to CSI-FiSh, arise from using a distinct group and set in the group action. However, in order to define their group action, the set elements are no longer just j-invariants of supersingular elliptic curves, but curves together with extra data called "orientation". The necessity of carrying the orientation and computing the group action on the orientation is what renders the efficiency of SCALLOP bad in comparison to CSI-FiSh.

Recently, the field of isogeny-based cryptography has seen a major breakthrough with the successful cryptanalysis of the SIDH key exchange scheme by [CD23,MMP+23,Rob23]. This result was obtained by embedding isogenies between elliptic curves (isogenies of dimension 1) inside isogenies of higher dimension (2, 4 and 8) using Kani's Lemma [Kan97]. Since then, these novel ideas have been used several times to build some post-quantum protocols such as encryption [BMP23], signature [DLRW23], or VRF [Ler23]. In short, our new construction SCALLOP-HD uses these ideas to represent orientations more efficiently and this leads to various improvements over SCALLOP that we list in the next section.

1.1 Contribution.

In this work, we revisit the SCALLOP group action with the high dimensional isogenies at the heart of the attacks against SIDH. We show that these new techniques, and in particular, the idea of Robert [Rob22] that an arbitrary degree isogeny can be efficiently represented using high dimension isogenies allows us to simplify the framework of SCALLOP. Concretely, the improvements of

---

[4] https://yx7.cc/blah/2023-04-14.html

SCALLOP-HD compared to the original SCALLOP can be summarized as follows:

1. A new orientation representation that uses the embedding techniques based of higher dimensional isogenies.
2. A simplified algorithm to compute the group action using Kani's Lemma in dimension 2 that we expect will improve the efficiency.
3. The improvement from a subexponential to a polynomial complexity of the computation of the class group's lattice of relation: the bottleneck in the precomputation required by SCALLOP. This leaves only the complexity required for performing lattice reduction algorithms on the lattice of relation the non-polynomial time part in precomputation of the SCALLOP-HD group action.

In doing so, we introduce a novel way of applying Kani's Lemma in dimension 2 by building isogeny diamonds from two endomorphisms lying in the same quadratic order. This can be used to represent orientations and endomorphisms in dimension 2. We believe this new technique is interesting in its own right, and it was recently used in [Ler23] to provide a new algorithm to perform the Deuring correspondence using isogenies in dimension 2. We also briefly discuss another example where this new technique can be used in a recent endomorphism division algorithm in Remark 15.

Organization of the paper. The rest of this paper is organized as follows. In Section 2, we introduce necessary mathematical background. Then, Section 3 explains how to construct group action from isogenies and outlines the progress towards obtaining a scalable EGA. In Section 4, we present the new orientation representation alongside the resulting group action formula. Section 5 introduces the SCALLOP-HD group action. Section 6 discusses some remarks on the security of SCALLOP-HD. We conclude in Section 7 by summarizing the paper and discussing future work.

2   Preliminaries

2.1   Quaternion algebras, supersingular elliptic curves, isogenies and the Deuring correspondence

Quaternion algebras Let p be a prime and let $\mathcal{B}_{p,\infty}$ denote the unique (up to isomorphism) quaternion algebra ramified precisely at p and ∞. We fix a $\mathbb{Q}$-basis $\langle 1, \mathbf{i}, \mathbf{j}, \mathbf{k} \rangle$ of $\mathcal{B}_{p,\infty}$ that satisfies $\mathbf{i}^2 = -q$, $\mathbf{j}^2 = -p$ and $\mathbf{k} = \mathbf{ij} = -\mathbf{ji}$ for some integer q. A *fractional ideal* I in $B_{p,\infty}$ is a $\mathbb{Z}$-lattice of rank 4. We denote by $n(I)$ the *norm* of I as the largest rational number such that $n(\alpha) \in n(I)\mathbb{Z}$ for any $\alpha \in I$. An order $\mathcal{O}$ is a subring of $B_{p,\infty}$ that is also a fractional ideal. An order is called *maximal* when it is not contained in any other larger order. A fractional ideal is *integral* if it is contained in its *left order* $\mathcal{O}_L(I) = \{\alpha \in \mathcal{B}_{p,\infty} \mid \alpha I \subset I\}$, or equivalently in its *right order* $\mathcal{O}_R(I) = \{\alpha \in \mathcal{B}_{p,\infty} \mid I\alpha \subset I\}$.

Supersingular elliptic curves and isogenies Let E, E_1, E_2 be elliptic curves defined over a finite field of characteristic p. An isogeny from E_1 to E_2 is a nonconstant rational map that is simultaneously a group homomorphism. An isogeny from a curve E to itself is an *endomorphism*. The set $\mathrm{End}(E)$ of all endomorphisms of E forms a ring under addition and composition. $\mathrm{End}(E)$ is either an order in an imaginary quadratic field and E is called *ordinary*, or a maximal order in $\mathcal{B}_{p,\infty}$, in which case E is called *supersingular*.

The Deuring correspondence Fix a supersingular elliptic curve E_0, and an order $\mathcal{O}_0 \simeq \mathrm{End}(E_0)$. The curve/order correspondence allows one to associate to each outgoing isogeny $\varphi : E_0 \to E_1$ an integral left $\mathcal{O}_0$-ideal, and every such ideal arises in this way (see [Koh96] for instance). Through this correspondence, the ring $\mathrm{End}(E_1)$ is isomorphic to the right order of this ideal. This isogeny/ideal correspondence is defined in [Wat69], and in the separable case, it is explicitly given as follows.

Definition 1. *Given I an integral left $\mathcal{O}_0$-ideal coprime to p, we define the I-torsion $E_0[I] = \{P \in E_0(\overline{\mathbb{F}}_{p^2}) : \alpha(P) = 0 \text{ for all } \alpha \in I\}$. To I, we associate the separable isogeny φ_I of kernel $E_0[I]$. Conversely given a separable isogeny φ, the corresponding ideal is defined as $I_\varphi = \{\alpha \in \mathcal{O}_0 : \alpha(P) = 0 \text{ for all } P \in \ker(\varphi)\}$.*

We summarize properties of the Deuring correspondence in Table 1, borrowed from [DFKL+20].

Supersingular j-invariants over $\mathbb{F}_{p^2}$	Maximal orders in $\mathcal{B}_{p,\infty}$
$j(E)$ (up to Galois conjugacy)	$\mathcal{O} \cong \mathrm{End}(E)$ (up to isomorphism)
(E_1, φ) with $\varphi : E \to E_1$	I_φ integral left $\mathcal{O}$-ideal and right $\mathcal{O}_1$-ideal
$\theta \in \mathrm{End}(E_0)$	Principal ideal $\mathcal{O}\theta$
$\deg(\varphi)$	$n(I_\varphi)$

Table 1. The Deuring correspondence, a summary [DFKL+20].

2.2 Quadratic orders and orientations on supersingular elliptic curves

Let d be a positive square-free integer and $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with discriminant D_K. Let $\mathfrak{O} \subseteq K$ be an order with discriminant $D_{\mathfrak{O}}$. Explicitly, $\mathfrak{O} = \mathbb{Z}[\frac{D_{\mathfrak{O}} + \sqrt{D_{\mathfrak{O}}}}{2}]$. Any element $\alpha \in \mathfrak{O}$ can be written as $x + y\frac{D_{\mathfrak{O}} + \sqrt{D_{\mathfrak{O}}}}{2}$ with $x, y \in \mathbb{Z}$, and $\{1, \alpha\}$ is a $\mathbb{Z}$-basis of $\mathfrak{O}$ if and only if $y = 1$. One can compute the norm of α and thus derive the norm form $f_{\mathfrak{O}}$ of $\mathfrak{O}$:

$$f_{\mathfrak{O}}(x,y) = x^2 + D_{\mathfrak{O}}xy + y^2 \frac{D_{\mathfrak{O}}(D_{\mathfrak{O}} - 1)}{4}.$$

For any order $\mathfrak{O}$, the class group $\mathrm{Cl}(\mathfrak{O})$ consists of the invertible fractional ideals of $\mathfrak{O}$ up to principal factors and is of order $D_{\mathfrak{O}}^{o(1)}$. When $\mathfrak{O} = \mathfrak{O}_K$ is the maximal order, computing $\mathrm{Cl}(\mathfrak{O}_K)$ takes time $L_{D_K}(1/2)$ classically [HM89] and polynomial time quantumly [BS16]. When $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_K$ where f is a prime and $\mathrm{Cl}(\mathfrak{O}_K) = \{1\}$, there is a simple characterization of $\mathrm{Cl}(\mathfrak{O})$ as discussed in [FFK$^+$23, Appx. A]. Specifically, $\mathrm{Cl}(\mathfrak{O})$ satisfies the following short exact sequence

$$1 \to \mathfrak{O}_K^* / \mathfrak{O}^* \to (\mathfrak{O}_K/(f))^* / (\mathfrak{O}/(f))^* \to \mathrm{Cl}(\mathfrak{O}) \to 1,$$

and they showed that

$$(\mathfrak{O}_K/(f))^* / (\mathfrak{O}/(f))^* \cong \begin{cases} \mathbb{F}_f^* & \text{if } f \text{ splits in } K, \\ \mathbb{F}_{f^2}^* / \mathbb{F}_f^* & \text{if } f \text{ is inert in } K. \end{cases}$$

In particular, this suggests that $\mathrm{Cl}(\mathfrak{O})$ is always cyclic as it is isomorphic to a quotient of a cyclic group, and $\mathrm{Cl}(\mathfrak{O})$ is easy to compute in these cases. Furthermore, this implies that $\#\mathrm{Cl}(\mathfrak{O}) = \left(f - \left(\frac{-1}{f} \right) \right) \frac{1}{|\mathfrak{O}_K^*|/2}$.

Quadratic orders and their class groups are playing an increasingly important role in isogeny-based cryptography, in particular since Colò and Kohel introduced orientations on supersingular elliptic curves in [CK20]. In what follows, we recall the basic definitions and important properties regarding orientations.

Definition 2. *Let E be a supersingular elliptic curve over $\mathbb{F}_{p^2}$, K be an imaginary quadratic field and $\mathfrak{O} \subseteq K$ be a suborder. Then a K-orientation on E is a ring homomorphism $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$. This K-orientation induces an $\mathfrak{O}$-orientation on E if $\iota(\mathfrak{O}) = \mathrm{End}(E) \cap \iota(K)$. In this case, the pair (E, ι) is called a $\mathfrak{O}$-oriented curve and E is a $\mathfrak{O}$-orientable curve.*

Note that here we use $\mathfrak{O}$-orientation to indicate the *primitive* $\mathfrak{O}$-orientation from [CK20].

Let E' be another supersingular curve and $\varphi : E \to E'$ be an isogeny. Let ι be a K-orientation on E, then there is an induced K-orientation $\iota' = \varphi_*(\iota)$ on E' defined to be $\varphi_*(\iota)(\omega) := \frac{1}{\deg(\varphi)} \varphi \circ \iota(\omega) \circ \widehat{\varphi} \in \mathrm{End}(E') \otimes \mathbb{Q}$. An isogeny of K-oriented elliptic curves $\varphi : (E, \iota) \to (E', \iota')$ is an isogeny $\varphi : E \to E'$ such that $\iota' = \varphi_*(\iota)$; we call this a K-oriented isogeny. A K-oriented isogeny is a *K-isomorphism* if it is an isomorphism of the underlying curves.

For a fixed imaginary quadratic order $\mathfrak{O} \subseteq K$, we consider the collection of all $\mathfrak{O}$-oriented curves and define the following set:

$$\mathcal{S}_{\mathfrak{O}}(p) = \{ (E, \iota) \mid (E, \iota) \text{ is an } \mathfrak{O}\text{-oriented curve} \} / \sim,$$

where two oriented curves are equivalent if they are K-isomorphic.

Here we recall the following conditions for the set $\mathcal{S}_{\mathfrak{O}}(p)$ to be non-empty.

Proposition 3 ([Onu21, Proposition 3.2]). *The set $\mathcal{S}_{\mathfrak{O}}(p)$ is not empty if and only if p does not split in K and does not divide the conductor of $\mathfrak{O}$.*

When $\mathcal{S}_{\mathfrak{O}}(p)$ is non-empty, the set of invertible $\mathfrak{O}$-ideals acts on it. Specifically, let $\mathfrak{a}$ be an such an ideal and $(E, \iota_E) \in \mathcal{S}_{\mathfrak{O}}(p)$, then

$$\mathfrak{a} \star (E, \iota_E) := (E_{\mathfrak{a}}, \iota_{E_{\mathfrak{a}}}),$$

where $E_{\mathfrak{a}}$ is the codomain of the isogeny $\phi_{\mathfrak{a}}$ whose kernel is $E[\mathfrak{a}] := \cap_{a \in \mathfrak{a}} \ker \iota_E(a)$ and $\iota_{E_{\mathfrak{a}}}$ is the induced orientation on $E_{\mathfrak{a}}$ by $\phi_{\mathfrak{a}}$. Principal $\mathfrak{O}$-ideals act trivially on (E, ι_E), therefore this action induces an action of $\mathrm{Cl}(\mathfrak{O})$ on $\mathcal{S}_{\mathfrak{O}}(p)$. It was shown in [Onu21] that this is action is free and it has one or two orbits.

2.3   New isogeny representation in higher dimensions

An isogeny representation is a way to *effectively* represent the isogeny so that there is an *efficient* algorithm for evaluating the isogeny on given points. Common representations include rational maps, isogeny chains, and kernel representation. However, these methods are no longer compact or efficient when the degree d of the isogeny is a large prime and the kernel points are defined over a large degree extension field of $\mathbb{F}_p$.

The Deuring correspondence allows us to efficiently represent such isogenies with their corresponding ideals in maximal quaternion orders, this is call the *ideal representation*. This, however, reveals the endomorphism rings for both the domain and codomain curve. To remedy the situation, Leroux in [Ler22a] introduced another representation called the *suborder representation* which is not strictly an isogeny representation but satisfies a weaker definition as introduced in [CII+23] and requires to reveal the endomorphism ring of the domain curve.

Finally, Robert [Rob22] suggested to use the techniques used in SIDH attacks [CD23,MMP+23,Rob23] to obtain a new isogeny representation, by embedding the desired isogeny between supersingular elliptic curves into an isogeny between abelian varieties of higher dimension. While not named as such in Robert's paper, we refer to it as *high dimension representation* in our paper. This new representation doesn't reveal the endomorphism rings and is much more efficient than suborder representation. It consists only of evaluation of the isogeny to be represented on points of smooth order, and in the right setting it can be pretty easy to compute. While used destructively at first, it has been recently used constructively for building various protocols [DLRW23,Ler23,BMP23,DMS23]. For a detailed account of of the "old" isogeny representations, like the kernel or ideal representation, see [Ler22b]. In what follows, we explain in more details the idea of *high dimension representation* in dimension 2. The main result behind this representation is Kani's Lemma [Kan97] that we present below as Lemma 4.

Lemma 4 (Kani). *Let us consider a commutative diagram of isogenies between principally polarized abelian varieties of dimension g*

$$
\begin{array}{ccc}
A' & \xrightarrow{\varphi'} & B' \\
\psi \uparrow & & \uparrow \psi' \\
A & \xrightarrow{\varphi} & B
\end{array}
$$

where φ and φ' are a-isogenies and ψ and ψ' are b-isogenies for integers a, b. The isogeny $F : A \times B' \longrightarrow B \times A'$ given in matrix notation by

$$F := \begin{pmatrix} \varphi & \widetilde{\psi'} \\ -\psi & \widetilde{\varphi'} \end{pmatrix}$$

is a d-isogeny between abelian varieties of dimension $2g$ with $d = a + b$, for the product polarisations.

If $\ker \widetilde{\varphi} \cap \ker \psi' = \{0\}$, the kernel of F is

$$\ker(F) = \{(\widetilde{\varphi}(x), \psi'(x)) \mid x \in B[d]\}.$$

Similarly, if $\ker \varphi \cap \ker \psi = \{0\}$, then

$$\ker(\widetilde{F}) = \{(\varphi(x), \psi(x)) \mid x \in A[d]\}.$$

The commutative diagram in Lemma 11 is often called as an isogeny diamond. Following the notations introduced in [Ler23], we call a *2*dim-representation of an isogeny $\varphi : A \to B$ between two elliptic curves A, B any data from which the isogeny F obtained by applying Lemma 4 with $g = 1$ can be computed efficiently. The idea is that φ can be recovered from F by pre-composition with any embedding $A \to A \times B'$ that acts as the identity on A, and post-composition with the canonical projection $B \times A' \to B$.

To represent the orientation of our SCALLOP-HD group action in Section 4.1, we will use the *2*dim-representation of an endomorphism with a commutative diagram obtained from two commuting endomorphisms. There, we will also provide in Lemma 11 a formula for $\ker F$ when the intersection of $\ker \varphi$ and $\ker \psi$ is a cyclic group of order 2.

Remark 5. One could also embed the isogeny φ in isogenies between abelian varieties in dimension 4 or 8, as discussed for the SQISignHD protocol in [DLRW23]. The higher the dimension, the easier it is to generate the isogeny diamond, however, the complexity of computing isogenies between abelian varieties scales exponentially with the dimension. This is why it is generally better to use the smallest possible dimension. In SQISignHD, it is argued that dimension 2 isogenies do not provide a clear advantage over the original SQISign scheme [DFKL+20] due to the complexity to set-up the isogeny diamond, which is the main reason why SQISignHD works with dimension 4 and dimension 8. In our case, thanks to the idea of using isogeny diamond built from commuting endomorphisms, we will be able to work dimension 2 to achieve better efficiency.

3   Group action in isogeny-based cryptography

Informally, a group action is a map of the form $\star : G \times X \to X$, where G is a group and X is a set, such that for any $g_1, g_2 \in G$ and any $x \in X$, we have

$$g_1 \star (g_2 \star x) = (g_1 g_2) \star X.$$

We revisit here the concepts of effective group action (EGA) and restricted effective group action (REGA) from [ADFMP20], which capture the essence of two types of group actions used in isogeny-based cryptography. To clarify the distinction between the two and align with subsequent discussions, we exclude details concerning the set X — specifically, membership testing, unique representation, and the existence of the origin in X.

Definition 6. *(EGA) A group action $(G, X, \star)$ is effective if the following properties are satisfied:*

1. *The group G is finite and there exist efficient (PPT) algorithms for:*
   (a) *Membership testing, i.e., to decide if a given bit string represents a valid group element in G.*
   (b) *Equality testing, i.e., to decide if two bit strings represent the same group element in G.*
   (c) *Sampling, i.e., to sample an element g from a distribution $\mathcal{D}_G$ on G.*
   (d) *Operation, i.e., to compute gh for any $g, h \in G$.*
   (e) *Inversion, i.e., to compute g^{-1} for any $g \in G$.*
2. *There exists an efficient algorithm that given (some bit-string representation of) any $g \in G$ and any $x \in X$, outputs $g \star x$.*

Definition 7. *(REGA) Let $(G, X, \star)$ be a group action and let $\mathbf{g} = \{g_1, \ldots, g_n\}$ be a (not necessarily minimal) generating set for G. The action is said to be $\mathbf{g}$-restricted effective if the following properties are satisfied:*

1. *G is finite and $n = \mathsf{poly}(\log |G|)$.*
2. *There exists an efficient algorithm that given any $i \in [n]$ and any bit string representation of $x \in X$, outputs $g_i \star x$ and $g_i^{-1} \star x$.*

Existing instantiation of this definition from isogenies are all based on the ideal class group action. Specifically, it's the action of $\mathrm{Cl}(\mathfrak{O})$ on $\mathcal{S}_{\mathfrak{O}}(p)$ for some imaginary quadratic $\mathfrak{O}$ as defined in Section 2.2. This action can be made a REGA immediately by choosing a generating set $\mathbf{g} = \{\mathfrak{l}_1, \ldots, \mathfrak{l}_n\}$, where each $\mathfrak{l}_i$ is a prime ideal of small norm. To further convert this action into an EGA, challenges arise in sampling elements from a distribution $\mathcal{D}_G$ on G, and computing the action $g \star x$ for $g \in G$ sampled from $\mathcal{D}_G$ and $x \in X$. In this paper, we restrict our interest to the uniform distribution $\mathcal{U}_G$.

In [BKV19], Beullens, Kleinjung, and Vercauteren laid out a general strategy to turn the class group action from a REGA to an EGA as follows:

1. **Offline phase:**
   1.1 *Class group computation* - Compute a generator $\mathfrak{g}$ of the class group $\mathrm{Cl}(\mathfrak{O})$, which is possible because generically $\mathrm{Cl}(\mathfrak{O})$ is cyclic.

1.2 *Construct the lattice of relations* $\mathcal{L}$ - This lattice is generated by the column vectors of the following matrix

$$
\begin{pmatrix}
1 & 0 & 0 & \dots & 0 & 0 \\
0 & 1 & 0 & \dots & 0 & 0 \\
0 & 0 & 1 & \dots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \dots & 1 & 0 \\
r_1 & r_2 & r_3 & \dots & r_n & \#\mathrm{Cl}(\mathfrak{O})
\end{pmatrix},
$$

where $r_i's$ are integers such that $[\mathfrak{l}_i] = [\mathfrak{g}^{r_i}]$.

1.3 *Lattice reduction* - Compute a reduced basis of $\mathcal{L}$ suitable for solving approximate-CVP.

2. **Online phase:**

2.1 *Solve approximate-CVP* - Given $\mathfrak{g}^e \in \mathrm{Cl}(\mathfrak{O})$, solve approximate-CVP to find a decomposition $\mathfrak{g}^e = \prod_{i=1}^{i=n} \mathfrak{l}_i^{e_i}$ with small exponents.

2.2 *Group action evaluation* - Compute the action $(\prod_{i=1}^{i=n} \mathfrak{l}_i^{e_i}) \star (E, \iota_E)$ for $(E, \iota_E) \in \mathcal{S}_{\mathfrak{O}}(p)$.

This strategy allowed Beullens, Kleinjung and Vercautern to extend the REGA behind the CSIDH key exchange [CLM+18] to an EGA, leading to the construction of the signature scheme CSI-FiSh. They worked with the imaginary quadratic order $\mathbb{Z}[\sqrt{-p}]$ which has a discriminant of 154 digits. The primary challenge for them was computing the class group $\mathrm{Cl}(\mathbb{Z}[\sqrt{-p}])$, and the remaining steps were efficient, essentially due to the fact that they could use a relatively small n and consequently, a lattice with rather small dimension. However, their method can't be scaled for bigger prime p due to the infeasibility of the class group computations.

To address this, SCALLOP[DFFK+23] proposed the use of a distinct class of quadratic orders of the form $\mathfrak{O} = \mathbb{Z}[f\sqrt{-d}]$, where f is a large prime and d is a small positive integer. While this sidesteps the class group computation challenges as discussed in Section 2.2 and enhances scalability, it introduces representation complexities for the set elements — oriented curves (E, ι_E). In order to achieve an efficient representation, an generator of $\mathfrak{O}$ of smooth norm should be found, constraining the choice of f and yielding a class group with a non-smooth size. Consequently, the second step of precomputation — computing the lattice of relation — remains subexponential in time due to the need to solve discrete logarithms in groups with subexponential order sizes. Moreover, SCALLOP demands more computations to perform the group action, rendering it much slower than CSI-FiSh.

The security of CSIDH, CSI-FiSh and SCALLOP relies on the hardness of the vectorization problem. Abstractly, for a transitive group action, this problem is defined as follows.

Problem 8. (Vectorization) Given $x, y \in X$, find $g \in G$ such that $y = g \star x$.

According to [Wes22, Proposition 3], the fastest known generic classically method to solve the vectorization problem associated to the group action has complexity $l^O(1)|D_{\mathfrak{O}}|^{1/4}$ where l denotes the length of the input. In the setting of SCALLOP, this is $\log(p + |D_{\mathfrak{O}}|)^{O(1)} \min(p^{1/2}, f^{1/2})$ [DFFK$^+$23, Section 4].

The main quantum approach to solve the vectorization problem is given by Kuperberg's abelian hidden-shift algorithm [Kup05] and descendants, where the hidden "shift" corresponds to the secret group element g given x and $y = g \star x$. Despite known to take sub-exponential time, determining the precise quantum cost for concrete group actions is hard. Since 2020, a series of papers [BLMP19,BS20,Pei20,CSCDJRH22] studied the quantum security of CSIDH, leading to the conclusion that CSIDH-512 and CSIDH-1024 could not achieve NIST security level 1. Instead, [BS20] recommended that the CSIDH prime p should be upgraded to at least 2260 or 5280 bits, according to what they named as *aggressive* and *conservative* modes, respectively. [CSCDJRH22] recommended to use a CSIDH prime of 4096 bits for the level 1 security and 6144 bits for level 2. These analyses, together with the desire of obtaining EGAs from isogeny, have spurred the urgency to scale. Since the ideas of the quantum algorithms essentially work for all CRS style group action, we will also model the security of SCALLOP using the analyses for CSIDH. Specifically, this means we match the size of the field characteristic p and the class group size $\#\mathrm{Cl}(\mathfrak{O})$ with that of CSIDH to estimate the quantum security level of SCALLOP. In this line of research, CSI-FiSh was only able to scale to achieve the security level of CSIDH-512, and SCALLOP managed to scale to achieve the security level of CSIDH-1024.

4   *2*dim-representation of orientations and endomorphisms

In this section, we introduce a new representation called *2*dim-representation of orientations and endomorphisms. Since representing an endomorphism θ amounts to representing any $\theta + n \in \mathbb{Z}[\theta]$, representing orientations and endomorphisms are essentially the same thing in different languages. Therefore, even though the results in this section are mostly stated with respect to orientations, they apply to endomorphisms as well.

In Section 4.1, we introduce the definition of our *2*dim-representation for orientations and discuss how to recover the orientation from the *2*dim-representation, then in Section 4.2, we show that any orientation (endomorphism) admits a *2*dim-representation that can be computed in polynomial time. Finally, in Section 4.3, we conclude with a formula that computes the $\mathrm{Cl}(\mathfrak{O})$-action on the set $\mathcal{S}_{\mathfrak{O}}(p)$ with set elements given by *2*dim-representations.

While our *2*dim-representation is introduced to represent orientations appearing in SCALLOP-HD, this technique can be applied in other algorithms in isogeny as well.

4.1 *2*dim-representation

Let (E, ι_E) be an $\mathfrak{O}$-oriented supersingular elliptic curve. Motivated by the idea of *2*dim representation of isogenies, we introduce the following definition.

Definition 9. *Let $\mathfrak{O}$ be an imaginary quadratic order with discriminant $D_{\mathfrak{O}}$ and odd conductor f. Given an $\mathfrak{O}$-oriented supersingular elliptic curve (E, ι_E), take any $\omega \in \mathfrak{O}$ such that $\mathfrak{O} = \mathbb{Z}[\omega]$ and define $\omega_E := \iota_E(\omega)$. Let $\beta \in \mathfrak{O}$ such that $n(\omega) + n(\beta) = 2^e$ for some $e \in \mathbb{N}$ and $2 \nmid \beta$. Let P, Q be a basis of $E[2^e]$. Then the tuple $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$ is called a 2dim-representation of (E, ι_E).*

Given a *2*dim-representation $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$ of (E, ι_E), let $\beta_E := \iota_E(\beta)$, we immediately have the following isogeny diamond.

$$\begin{array}{ccc} E & \xrightarrow{\hat{\omega}_E} & E \\ \beta_E \uparrow & & \beta_E \uparrow \\ E & \xrightarrow{\hat{\omega}_E} & E. \end{array}$$

From here, we can define an isogeny $F_E : E^2 \to E^2$ by the matrix

$$F_E := \begin{pmatrix} \hat{\omega}_E & \hat{\beta}_E \\ -\beta_E & \omega_E \end{pmatrix}.$$

And as discussed in Section 2.3, if $\ker \omega_E \cap \ker \beta_E = \{0\}$, then

$$\ker F_E = \{(\omega_E(R), \beta_E(R)) \mid R \in E[2^e]\}.$$

Since β is a translated scalar multiplication of ω_E, knowing the evaluation of ω_E on $E[2^e]$ suffices to compute $\ker F_E$.

At first glance, it may seem like we are missing conditions such as those on the norms of ω, β in Definition 9 in order to use the formula above. As it turns out, we can't guarantee having solutions such that $\ker \omega_E \cap \ker \beta_E = \{0\}$ all the time. We introduce the following lemmata to deal with our specific cases.

Lemma 10. *Let $(E, \iota_E), \mathfrak{O}, \omega, \beta$ be as in Definition 9, then one of the followings hold:*

I. $\ker \omega_E \cap \ker \beta_E = \{0\}$ *or* $\ker \hat{\omega}_E \cap \ker \beta_E = \{0\}$.
II. $\ker \omega_E \cap \ker \hat{\omega}_E \cap \ker \beta_E \cap \ker \hat{\beta}_E = \langle P \rangle$ *for some nontrivial 2-torsion element P.*

Proof. We first start with the observation that $\gcd(n(\omega), n(\beta))$ is a 2-power since they sum to 2^e. Therefore, to analyze the kernel intersections above, it suffices to study the action of the endomorphisms $\omega_E, \hat{\omega}_E, \beta_E, \hat{\beta}_E$ on 2-torsions. Let us now consider the ideal $\mathfrak{O}\langle \omega, 2 \rangle$. Since ω satisfies that $\mathfrak{O} = \mathbb{Z}[\omega]$, norm $n(\mathfrak{O}\langle \omega, 2 \rangle)$ of ideal $\mathfrak{O}\langle \omega, 2 \rangle$ is either 1 or 2. Similarly, since $2 \nmid \beta$ by assumption, $n(\mathfrak{O}\langle \beta, 2 \rangle)$ is either 1 or 2.

– If $n(\mathfrak{O}\langle\omega,2\rangle) = 1$ then we have $\ker\omega_E \cap E[2] = \{0\}$ and we are in case I.
– If $n(\mathfrak{O}\langle\omega,2\rangle) = 2$, then $\ker\omega_E \cap E[2] = \{P\}$ for some $P \neq 0 \in E[2]$. In this case, $n(\mathfrak{O}\langle\hat{\omega},2\rangle) = 2$ as well.
  – If $2 \nmid \mathrm{tr}(\omega)$, which is equivalent to say $D_\mathfrak{O} \neq 0 \bmod 4$, then $\ker\hat{\omega} = \langle S\rangle$ for some $S \in E[2]$ and $S \neq 0, R$. It's clear that we are in case I now.
  – If $2 \mid \mathrm{tr}(\omega)$, which is equivalent to say $D_\mathfrak{O} \equiv 0 \bmod 4$, then $\ker\hat{\omega} = \ker\omega = \langle P\rangle$.
  –– If $\mathfrak{O}\langle\omega,2\rangle \neq \mathfrak{O}\langle\beta,2\rangle$, then we are in case I.
  –– If $\mathfrak{O}\langle\omega,2\rangle = \mathfrak{O}\langle\beta,2\rangle$, then we are in case II.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ □

Following the proof of Lemma 10, one can see that for $(E,\iota_E),\mathfrak{O},\omega,\beta$ as in Definition 9, case II happens if and only if $n(\mathfrak{O}\langle\omega,2\rangle) = 2, D_\mathfrak{O} \equiv 0 \bmod 4$ and $\mathfrak{O}\langle\omega,2\rangle = \mathfrak{O}\langle\beta,2\rangle$.

Lemma 11. *Let $F_E : E^2 \to E^2$, be a 2^e isogeny defined as above. Let us assume that $\ker\beta_E \cap \ker\omega_E \cap \ker\hat{\omega}_E \cap \ker\hat{\beta}_E = \{0,P\}$ for a point $P \in E[2]$, then*

$$\ker F_E = \{(\omega_E(R),\beta_E(R)), R \in E[2^e]\} + \{(0,0),(0,P)\}. \qquad (1)$$

Proof. Consider the map that sends $R \in E[2^e]$ to $(\omega_E(R),\beta_E(R))$, it has kernel $\langle P\rangle$ and therefore the set $S := \{(\omega_E(R),\beta_E(R)), R \in E[2^e]\}$ has size 2^{2e-1}. Similarly, with $S_P = S + (0,P)$, we see that $\#S_P = 2^{2e-1}$. Moreover, $S \cap S_P = \emptyset$, because if $\omega_E(R_1) = \omega_E(R_2)$, and $\beta_E(R_1) = P + \beta_E(R_2)$, we must have $R_1 - R_2 \in \ker\omega_E \cap E[2^e]$ which implies that $R_1 - R_2 \in \{0,P\}$. In that case we have also $\beta_E(R_1) = \beta_E(R_2)$ and so we cannot have $\beta_E(R_1) = P + \beta_E(R_2)$. In conclusion we have proven that $\#(S + S_P) = 2^{2e}$. To conclude the proof, it suffices to show that $(0,P) \in \ker F_E$, which can be easily verified since $P \in \ker\beta_E \cap \ker\omega_E \cap \ker\hat{\omega}_E \cap \ker\hat{\beta}_E$. $\qquad\qquad$ □

4.2   Computing a 2dim-representation

Proposition 12. *Let $\mathfrak{O}$ be an imaginary quadratic order of odd conductor, then any $(E,\iota_E) \in \mathcal{S}_\mathfrak{O}(p)$ admits a 2dim-representation as in Definition 9.*

Proof. To prove this result, it suffices we can always find $e \in \mathbb{N}, \omega, \beta \in \mathfrak{O}$ such that

$$\mathfrak{O} = \mathbb{Z}[\omega],\ 2 \nmid \beta,\ n(\omega) + n(\beta) = 2^e.$$

Using the explicit representation of $\mathfrak{O}$ given in Section 2.2, $\omega = x + \frac{D_\mathfrak{O}+\sqrt{D_\mathfrak{O}}}{2}$ and $\beta = y + z\frac{D_\mathfrak{O}+\sqrt{D_\mathfrak{O}}}{2}$ for some integers x,y,z. Therefore, the last condition above translates to finding an integer solution of the following equation:

$$x^2 + D_\mathfrak{O}x + \frac{D_\mathfrak{O}(D_\mathfrak{O}-1)}{4} + y^2 + D_\mathfrak{O}yz + \frac{D_\mathfrak{O}(D_\mathfrak{O}-1)}{4}z^2 = 2^e. \qquad (2)$$

Rewriting Eq. (2) and multiply both sides by 4 gives rise to the following:

$$(2x + D_{\mathfrak{O}})^2 + (2y + D_{\mathfrak{O}}z)^2 = 2^{e+2} + D_{\mathfrak{O}}(z^2 + 1). \tag{3}$$

This equation can be solved efficiently by taking a random z and trying to express $2^{e+2} + D_{\mathfrak{O}}(1 + z^2)$ as a sum of two-squares with Cornacchia's algorithm. When e is large enough, we will be able to try enough z that one will give a solution. However, solving the equation is not enough as we need to satisfy the additional constraint that $2 \nmid \beta$, which is equivalent to requiring that y, z are not both even.

For that, we are going to distinguish several cases depending on the value of $D_{\mathfrak{O}} \mod 16$. Since $\mathfrak{O}$ is an order of odd prime conductor, there are only three possibilities: either $\mathfrak{O}$ is equal to 1 mod 4 or it is equal to -4 or 8 modulo 16. We will see that we can find a suitable solution for all those three cases.

– If $D_{\mathfrak{O}} \equiv 1 \mod 4$, we choose z to be odd integers, then $2^{e+2} + D_{\mathfrak{O}}(z^2 + 1) \equiv 2 \mod 4$. When this can be written as a sum of two squares, we must have $2x + D_{\mathfrak{O}}$ and $2y + D_{\mathfrak{O}}z$ both are odd integers, then it's clear that we can solve x, y from $2x + D_{\mathfrak{O}}$ and $2y + D_{\mathfrak{O}}z$. In this case, we have a solution x, y, z where z is odd.
– If $D_{\mathfrak{O}} \equiv 0 \mod 4$ Since $D_{\mathfrak{O}}$ is always 0 mod 4, we can rewrite Eq. (3) as

$$(x + D_{\mathfrak{O}}/2)^2 + (y + zD_{\mathfrak{O}}/2)^2 = 2^e + (D_{\mathfrak{O}}/4)(z^2 + 1). \tag{4}$$

– If $D_{\mathfrak{O}} \equiv -4 \mod 16$, we choose z to be odd integers, then $2^e + (D_{\mathfrak{O}}/4)(z^2 + 1) \equiv 2 \mod 4$. When this can be written as sum of two squares, it leads to a solution x, y, z with z odd.
– If $D_{\mathfrak{O}} \equiv 8 \mod 16$, we choose z to be even integers, then $2^e + (D_{\mathfrak{O}}/4)(z^2 + 1) \equiv 2 \mod 4$. When this can be written as sum of two squares, $x + D_{\mathfrak{O}}/2$ and $y + zD_{\mathfrak{O}}/2$ are both odd, and therefore y will be odd. This means that we will have a solution x, y, z with y odd.

We now detail the resolution of Eq. (3) with the OrientDiamondDim2 algorithm. The name suggests this algorithm is for building an isogeny diamond for a 2dim-representation of an orientation. Proposition 14 shows that such a diamond can be constructed in polynomial time. We also consider a constant C that is an implicit parameter of OrientDiamondDim2.

The complexity statement on Algorithm 1 only holds assuming some plausible heuristic regarding the distribution of number of the form $2^e + D(1 + z^2)$ that we state below as Heuristic 13.

Heuristic 13. *Let $e, D_{\mathfrak{O}}$ be as in Algorithm 1.*

– *If $D_{\mathfrak{O}} = 1 \mod 4$, and z are sampled as random odd integers then the integers $2^{e+2} + D_{\mathfrak{O}}(1 + z^2)$ behave like random odd integers of the same size that are congruent to 2 modulo 4.*
– *If $D_{\mathfrak{O}} = -4 \mod 16$, and z are sampled as random odd integers then the integers $2^e + (D_{\mathfrak{O}}/4)(z^2 + 1)$ behave like random integers of the same size that are congruent to 2 mod 4.*

Algorithm 1 OrientDiamondDim2($D_\mathfrak{O}$)

Input: An imaginary quadratic order $\mathfrak{O}$ with discriminant $D_\mathfrak{O}$.
Output: $\omega, \beta \in \mathfrak{O}$ such that $\mathfrak{O} = \mathbb{Z}[\omega]$, $n(\omega) + n(\beta)$ is a 2-power and $2 \nmid \beta$.
1: Let e be the smallest integer such that $2^{e+2} > C(\log |D_\mathfrak{O}|)|D_\mathfrak{O}|$.
2: Set $x := 0$, $y := 0$.
3: **if** $D_\mathfrak{O} = 1 \mod 4$ **then**
4:     **for** $z \in 2 \times [1, \lfloor \sqrt{\frac{2^{e+1}}{|D_\mathfrak{O}|}} - 1 \rfloor] - 1$ **do**
5:         $M := 2^{e+2} + D_\mathfrak{O}(z^2 + 1)$.
6:         **if** $M = 2M'$ where M' is a prime such that $M' \equiv 1 \bmod 4$ **then**
7:             Use Cornacchia's algorithm to find X, Y such that $X^2 + Y^2 = M$.
8:             Set $x = (X - D_\mathfrak{O})/2$ and $y = (Y - zD_\mathfrak{O})/2$.
9:             **break**
10:        **end if**
11:    **end for**
12: **else if** $D_\mathfrak{O} = -4 \mod 16$ **then**
13:    **for** $z \in 2 \times [1, \lfloor \sqrt{\frac{2^{e+1}}{|D_\mathfrak{O}|}} - 1 \rfloor] - 1$ **do**
14:        $M := 2^e + (D_\mathfrak{O}/4)(z^2 + 1)$.
15:        **if** $M = 2M'$ where M' is a prime such that $M' \equiv 1 \bmod 4$ **then**
16:            Use Cornacchia's algorithm to find X, Y such that $X^2 + Y^2 = M$.
17:            Set $x = X - D_\mathfrak{O}/2$ and $y = Y - zD_\mathfrak{O}/2$.
18:            **break**
19:        **end if**
20:    **end for**
21: **else if** $D_\mathfrak{O} = 8 \mod 16$ **then**
22:    **for** $z \in 2 \times [1, \lfloor \sqrt{\frac{2^{e+2}}{|D_\mathfrak{O}|}} - 1 \rfloor]$ **do**
23:        $M := 2^e + (D_\mathfrak{O}/4)(z^2 + 1)$.
24:        **if** $M = 2M'$ where M' is a prime such that $M' \equiv 1 \bmod 4$ **then**
25:            Use Cornacchia's algorithm to find X, Y such that $X^2 + Y^2 = M$.
26:            Set $x = X - D_\mathfrak{O}/2$ and $y = Y - zD_\mathfrak{O}/2$.
27:            **break**
28:        **end if**
29:    **end for**
30: **end if**
31: **if** $x = 0$ and $y = 0$ **then**
32:    **Return** $\perp$.
33: **end if**
34: $\omega := x + \frac{D_\mathfrak{O} + \sqrt{D_\mathfrak{O}}}{2}$, $\beta := y + z\frac{D_\mathfrak{O} + \sqrt{D_\mathfrak{O}}}{2}$.
35: **return** ω, β.

    – If $D_{\mathfrak{O}} = 8 \mod 16$, *and z are sampled as random even integers then the integers $2^e + (D_{\mathfrak{O}}/4)(z^2 + 1)$ behave like random integers of the same size that are congruent to* $2 \mod 4$.

Proposition 14. *Assuming Heuristic 13,* OrientDiamondDim2 *is correct, runs in $O\left(\mathsf{poly}\left(C\log(|D_{\mathfrak{O}}|)\right)\right)$, and there exists a constant C' such that the computation has succeeded with probability at least:* $1 - (1 - C'/\log(|D_{\mathfrak{O}}|))^{\sqrt{C\log(D_{\mathfrak{O}})}}$.

Proof. The correctness of Algorithm 1 follows from the observation that the outputs ω, β will always satisfy that $\mathfrak{O} = \mathbb{Z}[\omega]$, $2 \nmid \beta$ and $n(\omega) + n(\beta) = 2^e$. In particular, the condition that $2 \nmid \beta$ is taken care of in all three cases by ensuring that y, z are not both even. The complexity follows from the fact that we perform $O(\sqrt{C\log(|D_{\mathfrak{O}})|}$ iteration of the loop and that the operations required inside each iteration are logarithmic in $|D_{\mathfrak{O}}|$. The integers M have size $C(\log|D_{\mathfrak{O}}|)|D_{\mathfrak{O}}|$ and we assume that they behave like random integers under Heuristic 13, therefore there is a constant C' such that $M/2$ is prime with probability higher than $C'/(\log|D_{\mathfrak{O}}|)$. The bound on the success probability follows directly from there. □

Remark 15. We choose to work with isogenies in dimension 2 of degree $n = 2^e$ for efficiency of computing such isogenies in practice, and we later choose p such that 2^e-torsion is defined over $\mathbb{F}_{p^2}$ in the set up of SCALLOP-HD. However, in other use cases of our *2*dim-representation technique for representing orientations and endomorphisms, it might be interesting to have n to be a powersmooth integer. We believe the results above generalize easily to the powersmooth situation. Therefore, our *2*dim-representation can be applied to [MW23, Algorithm 1] to replace the isogeny computations in dimension 8 with computations in dimension 2, improving its efficiency.

4.3   Class group action evaluation

Let $[\mathfrak{a}] \in \mathrm{Cl}(\mathfrak{O})$ where $\mathfrak{a}$ is an integral $\mathfrak{O}$-ideal such that $\gcd(n(\mathfrak{a}), 2) = 1$. We now explain how to calculate the group action introduced in Section 2.2 in the context of the *2*dim-representation.

    Let $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$ be a *2*dim-representation of (E, ι_E), to calculate a *2*dim-representation for $(E_{\mathfrak{a}}, \iota_{E_{\mathfrak{a}}})$, we can keep the same ω and β. Since $\gcd(n(\mathfrak{a}), 2) = 1$, $\{\phi_{\mathfrak{a}}(P), \phi_{\mathfrak{a}}(Q)\}$ form a basis of $E_{\mathfrak{a}}[2^e]$. By definition,

$$\iota_{E_{\mathfrak{a}}}(\phi_{\mathfrak{a}}(P, Q)) = \frac{1}{n(\mathfrak{a})}\phi_{\mathfrak{a}} \circ \omega_E \circ \hat{\phi}_{\mathfrak{a}}(\phi_{\mathfrak{a}}(P, Q)) = \phi_{\mathfrak{a}}(\omega_E(P, Q)).$$

    Let $\{R, S\}$ be a basis for $E_{\mathfrak{a}}[2^e]$, such as the one computed by a deterministic algorithm that computes a basis. Given $P, Q, \omega_E(P), \omega_E(Q) \in E[2^e]$, to compute $\iota_{E_{\mathfrak{a}}}(\omega)(R)$ and $\iota_{E_{\mathfrak{a}}}(\omega)(S)$, we first write R, S as linear combinations of $\phi_{\mathfrak{a}}(P)$ and $\phi_{\mathfrak{a}}(Q)$, then compute $\iota_{E_{\mathfrak{a}}}(\omega)(R)$ and $\iota_{E_{\mathfrak{a}}}(\omega)(S)$ from $\iota_{E_{\mathfrak{a}}}(\phi_{\mathfrak{a}}(P)) = \phi_{\mathfrak{a}}(\omega(P))$ and $\iota_{E_{\mathfrak{a}}}(\phi_{\mathfrak{a}}(Q)) = \phi_{\mathfrak{a}}(\omega(Q))$.

5   SCALLOP-HD group action

In this section, we introduce SCALLOP-HD, an effective group action (EGA). SCALLOP-HD builds on SCALLOP by using choosing the same group action, i.e., $\mathrm{Cl}(\mathfrak{O})$ acts on $\mathcal{S}_{\mathfrak{O}}(p)$ for $\mathfrak{O} = \mathbb{Z}[f\sqrt{-d}]$. However, SCALLOP-HD deviates from SCALLOP by representing the set elements different. Precisely, SCALLOP-HD uses the 2dim-representation for $(E, \iota_E) \in \mathcal{S}_{\mathfrak{O}}(p)$. It turns out that this choice significantly simplifies the group action computation, and removes some of the constraints on parameter choices, which essentially is due to the fact that we no longer need to find a generator of $\mathfrak{O}$ of smooth norm, removing the trade-off between the smoothness of the generator norm and the group size $\#\mathrm{Cl}(\mathfrak{O})$. As has been mentioned before, SCALLOP-HD has better scalability and has the potential of being more efficient.

5.1   Outline of SCALLOP-HD

It's clear from Section 3 that to introduce an EGA using the class group action, one needs to

1. specify the group and the set,
2. convert the action into a REGA by choosing the set $\mathbf{g}$ as in Definition 7,
3. and derive an EGA following the strategy outlined in Section 3.

To define the group action, we start with choosing the field characteristic p and the quadratic order $\mathfrak{O}$, they determine the group $\mathrm{Cl}(\mathfrak{O})$ and the set $\mathcal{S}_{\mathfrak{O}}(p)$. When making these choices, there are two aspects one needs to take into consideration – first, from a security point of view, the vectorization problem of the action should be hard; second, from an efficiency point of view, p should be of a particular form so that the torsion points involved in subsequent calculations are defined over $\mathbb{F}_{p^2}$, and additionally $\mathfrak{O}$ should be an order for which $\#\mathrm{Cl}(\mathfrak{O})$ is as smooth as possible for an efficient generation of the lattice of relation $\mathcal{L}$ (Section 3). In SCALLOP-HD, each element (E, ι_E) will be given using the 2dim-representation, and we also specify the relevant parameters ω, β as a part of the group action definition. We discuss the details in Section 5.2.

To perform the group action, it's essential to possess an element from the set $\mathcal{S}_{\mathfrak{O}}(p)$. Acquiring this element, given our choice of of $\mathfrak{O}$, isn't straightforward. We introduce the SetUpCurveHD algorithm in Section 5.3 specifically for this purpose.

Once the group action is set up, we proceed in the conventional manner to convert it into a REGA. Let $\{\ell_1, \ldots, \ell_n\}$ be the first n odd primes that split in $\mathfrak{O}$ for $n = O(\log f)$, then we choose the set $\mathbf{g}$ to consist of the ideals $\{\mathfrak{l}_1, \ldots, \mathfrak{l}_k\}$ with $\mathfrak{l}_i$ being one of the prime ideal above ℓ_i. To further convert the REGA to an EGA, the offline phase is discussed in Section 5.4 and the online phase is discussed in Section 5.5.

5.2   Set up the group action

In this section, we explicit various choice of parameters for setting up the group action.

Choice of the quadratic order. Let $\mathfrak{O}_0$ be an imaginary quadratic order of class number equal to 1, as in SCALLOP, we choose $\mathfrak{O}$ to be of the form $\mathbb{Z} + f\mathfrak{O}_0$ for a large prime f. The size of f will be determined by the target security level. For the efficient precomputation of the lattice of relations (elaborated further in Section 5.4), we want to ensure that $\#\mathrm{Cl}(\mathfrak{O}) = \left(f - \left(\frac{-1}{f}\right)\right)\frac{1}{|\mathfrak{O}_0^*|/2}$ is as smooth as possible.

To find a good f, we generate powersmooth integers s that have the same size as f and are divisible by 4. This is achieved by multiplying together powers of random integers below a specified smoothness bound, and then multiplying the outcome by 4. Following this, one checks whether $s+1$ or $s-1$ is prime. If either is, it becomes the value of f. Since prime numbers are ample, this step runs in polynomial time with a polynomial size smoothness bound.

Choosing the field characteristic p. To ensure that the set $\mathcal{S}_{\mathfrak{O}}(p)$ is non-empty, we need to choose p that does not split in $\mathfrak{O}$ and does not divide the conductor f according to Proposition 3. Moreover, the form of p is determined by the torsion subgroups needed. To efficiently represent the orientation, we require that 2^e-torsion is defined over $\mathbb{F}_{p^2}$. For efficient computation of the group action, we also require to have the $\prod_{1 \leq i \leq n} \ell_i$-torsion defined over $\mathbb{F}_{p^2}$. These conditions on torsion points amounts to selecting a prime of the form:

$$p = c2^e \prod_{i=1}^{n} \ell_i \pm 1,$$

where c is a small cofactor.

Representing the orientation. Recall that a *2*dim-representation of an orientation is given by the tuple $(E, \omega, \beta, P, Q, \omega_E(P), \omega_E(Q))$. Once we have fixed $\mathfrak{O}$ from the previous discussion, we can determine the integer e and $\omega, \beta \in \mathfrak{O}$ for instance using the OrientDiamondDim2 algorithm.

In SCALLOP-HD group action, ω, β will be part of public parameters, therefore, they can be omitted from the orientation representation. Furthermore, we can use a deterministic algorithm that computes a basis of $E[2^e]$ for any curve E, this way we omit P, Q from the representation to make it even compacter. That being said, in the actual application of SCALLOP-HD group action, the orientation representation will be of the form $(E, \omega_E(P), \omega_E(Q))$.

5.3   Set up a starting curve

The computation of one $\mathfrak{O}$-oriented curve is necessary to set-up the scheme. This starting curve can be used to generate every other oriented curve by applying the

group action. Concretely, computing one 2dim-representation for a $\mathfrak{O}$-oriented curve means the following: compute any f-isogeny starting from an $\mathfrak{O}_0$-oriented curve E_0 and evaluate it on a basis of $E_0[2^e]$.

For this, we propose to revisit SetUpCurve [DFFK⁺23, Algorithm 1] as our setting remains very similar to SCALLOP. Since the conductor f is a big prime, we cannot hope to compute any isogeny of degree f directly. The trick behind SetUpCurve is to use an endomorphism of norm fS where S is a smooth integer and to express the f isogeny as the composition of this endomorphism and an isogeny of degree S. Such endomorphisms can be found with the FullRepresent-Integer [DFLLW23, Algorithm 1] as soon as $fS \approx p$. Since our ultimate goal is to evaluate the orientation on the 2^e torsion, the best option would be to take S coprime to 2, and with our choice of prime characteristic, we would have $S = \prod_i \ell_i$. Unfortunately, since $2^e \approx f^2$, we have $f \prod_i \ell_i \approx p/f$. This means that we must include other factors in S to reach the desired size. The only remaining available torsion is the power of 2. Since $2^{e/2} \approx f$, we should have $f2^{e/2} \prod_i \ell_i \approx p$. This means that we will be able to find endomorphisms of norm $\ell_1^h f 2^{e/2} \prod_{i>1} \ell_i$ for some small exponent h. In that case, we can circumvent the fact that S is not coprime to 2 by using a trick presented in [DLRW23, section 5.4] to cut the computation of the 2-dimensional isogeny in two, which allows us to divide by two the torsion requirement. For the group action computation, we prefer to use the full 2^e-torsion because the computation is more direct, but for the set-up of the scheme it is not a problem to sacrifice a bit of efficiency. The idea we just outlined gives the algorithm SetUpCurveHD that we describe below.

We start with an element $(E_0, \iota_0) \in \mathcal{S}_{\mathfrak{O}_0}(p)$. For simplicity of the discussion, we take $p = 3 \mod 4$, $\mathfrak{O}_0 = \mathbb{Z}[\mathbf{i}]$ and E_0 the curve of equation $y^2 = x^3 + x$. Let $\mathcal{O}_0$ be a maximal quaternion order such that $\mathrm{End}(E_0) \cong \mathcal{O}_0$, and we can fix an explicit isomorphism $\rho_0 : \mathcal{O}_0 \hookrightarrow \mathrm{End}(E_0)$ such that $\rho_0(\mathbf{i})$ is given by the automorphism $\iota(x,y) \to (-x, \sqrt{-1}y)$. Then the orientation ι_0 is derived from the inclusion $\mathfrak{O}_0 \subseteq \mathcal{O}_0$ and the isomorphism ρ_0.

Proposition 16. SetUpCurveHD *is correct and terminates in* $O(c\mathsf{poly}(\log(p)))$.

Proof. To prove correctness, we need to verify that the output $(E, (R, S))$ is a correct 2dim-representation of an element in $\mathcal{S}_{\mathfrak{O}}(p)$. Let us assume that the verification made in the loop passed. We will start by proving correctness under that assumption, then we will justify why the verification always passes.

When the verification passes, it means that there exists $\omega_E \in \mathrm{End}(E)$ of same norm and trace as ω. Thus, $\mathbb{Z}[\omega_E] \cong \mathbb{Z}[\omega] = \mathfrak{O}$, and sending ω to ω_E defines a $\mathfrak{O}$-orientation ι_E on E (we explain later in the proof why this is an optimal embedding of $\mathfrak{O}$ into $\mathrm{End}(E)$). Moreover, $R, S = \omega_E(P, Q)$ for a deterministic basis $\{P, Q\}$ of $E[2^e]$. Therefore, $(E, (R, S)) = (E, \omega_E(P, Q))$ is a valid 2dim-representation of $(E, \iota_E) \in \mathcal{S}_{\mathfrak{O}}(p)$.

Now, let us justify that there always is an i that passes the verification. The element $\gamma \in \mathcal{O}_0$ provides us with a principal ideal $\mathcal{O}_0\gamma$, whose corresponding isogeny $\rho_0(\varphi_\gamma)$ is an endomorphism of E_0. Moreover, we have that (up to composing with some isomorphisms if necessary) $\varphi_\gamma = \psi' \circ \varphi \circ \varphi_f$ where $\varphi_f : E_0 \to E$

Algorithm 2 SetUpCurveHD(p, f)

Input: p, f, e, ω, β as defined in Section 5.2 and $\mathfrak{O}_0, (E_0, \iota_0)$ as defined above.

Output: A 2dim-representation for $(E, \iota_E) \in \mathcal{S}_{\mathfrak{O}}(p)$ where $\mathfrak{O} = \mathbb{Z} + f\mathfrak{O}_0$.

1: Set h such that $\ell_1^h > p/(f2^{e/2} \prod_{i>1} \ell_i)$ and compute $\gamma \in \mathcal{O}_0$ of norm $f2^{e/2}\ell_1^h \prod_{i>1} \ell_i$ with FullRepresentInteger. Repeat that, until $\mathcal{O}_0\langle\gamma, f\rangle$ do not commute with $\mathbf{i}$.

2: Compute the isogeny $\psi : E_0 \to E'$ of degree $2^{e/2} \prod_i \ell_i$ corresponding to the ideal $\mathcal{O}_0\langle\overline{\gamma}, 2^{e/2} \prod_i \ell_i\rangle$.

3: Compute P_0, Q_0 a basis of $E_0[2^e]$ and compute $R_0, S_0 = \iota(P_0, Q_0)$.

4: Compute the points $P_0, Q_0, R_0, S_0 = \rho_0(\gamma)(P_0, Q_0, R_0, S_0)$.

5: Make the list $(\varphi_i : E' \to E_i)_{1 \le i \le m}$ of all isogenies of degree ℓ_1^{h-1} from E'.

6: **for** $i \in [1, m]$: **do**

7:    Compute $P_i, Q_i, R_i, S_i = ([(\ell_1^h \prod_{i>1} \ell_i)^{-1} \mod 2^{e/2}])\varphi_i \circ \psi(P_0, Q_0, R_0, S_0)$.

8:    Compute $R_i, S_i = [f](R_i, S_i)$.

9:    Try to use P_i, Q_i, R_i, S_i to build two isogenies $F_1 : E_i^2 \to C$ and $\hat{F}_2 : E_i^2 \to C$.

10:    If it works, check that $F = F_2 \circ F_1$ is a dimension 2 representation for endomorphisms $\omega_{E_i}, \beta_{E_i}$.

11:    If yes, verify that $\mathrm{tr}(\omega_{E_i}), n(\omega_{E_i})$ is the same as $\mathrm{tr}(\omega), n(\omega)$. If yes, break from the loop.

12: **end for**

13: Set $E = E_i$, and compute a deterministic basis P, Q of $E[2^e]$.

14: Use F to compute $R, S = \omega_E(P, Q)$.

15: **return** $(E, (R, S))$.

---

has degree f, $\varphi : E \to E'$ has degree ℓ_1^{h-1} and $\psi' : E' \to E_0$ has degree $2^{e/2} \prod_i \ell_i$. By [DFFK+23, Proposition 16], E is an $\mathfrak{O}$-orientable curve unless φ_f corresponds to one of the $1 + \left(\frac{d_0}{f}\right)$ horizontal f-isogenies of domain E_0. Let us assume for now that it is not. The endomorphism $\omega_E = \iota_E(\omega)$ is equal to $[x] + \varphi_f \circ \rho_0(\mathbf{i}) \circ \hat{\varphi}_f$. By design, the ideal $\langle\overline{\gamma}, 2^{e/2} \prod_i \ell_i\rangle$ corresponds to the isogeny $\hat{\psi}'$. Thus, we have that the isogeny ψ computed in Step 2, is the isogeny $\hat{\psi}'$. Then, if we take the index i_0 such that $\varphi_{i_0} = \hat{\varphi}$, we get that E_{i_0} is the curve E that we are looking for. Then, it can be verified that P_{i_0}, Q_{i_0} is equal to $[2^{e/2}]\varphi_f(P_0, Q_0)$, so it is a basis of $E_{i_0}[2^{e/2}]$. It can also be verified that the equality $R_{i_0}, S_{i_0} = \varphi_f \circ \rho_0(\mathbf{i}) \circ \hat{\varphi}_f(P_{i_0}, Q_{i_0})$. From there, the image points $\omega_E(P_{i_0}, Q_{i_0})$ and $\beta_E(P_{i_0}, Q_{i_0})$ can be recovered, and this is enough to build the two isogenies $\hat{F}_2$ and F_1 as described in [DLRW23, Section 5.4]. Then, F is the correct endomorphism on E^2 constructed from isogeny diamond formed by ω_E and β_E, and so the check for norm and trace equality will pass.

To finish the proof of correctness, we simply need to prove that the case where φ_f might be one of the bad isogenies cannot happen. In that case, we have that φ_f is one of the horizontal isogenies and since $\mathfrak{O}_0$ has class number one, this means that φ_f commutes with $\rho_0(\mathbf{i})$ which is equivalent to the fact that ideal corresponding to φ_f commutes with $\mathbf{i}$. Since this ideal is exactly equal to $\mathcal{O}_0\langle\gamma, f\rangle$, this situation is prevented from happening.

Regarding complexity, we have $\ell_1^{h-1} < p/(f 2^{e/2} \prod_i \ell_i)$ and since we have $f = O(2^{e/2})$, the loop is repeated at most $O(c)$ times. The computations over the quaternions are in $O(\mathsf{poly}(\log(p)))$. Then, since we have the explicit isomorphism ρ_0, we can compute ψ and evaluate $\rho_0(\gamma)$ over the 2^e-torsion in $O(\mathsf{poly}(\log(p)))$ (remember that the 2^e-torsion is defined over $\mathbb{F}_{p^2}$ and $2^e < p$). Then, the computation of each φ_i is in $O(\mathsf{poly}(\log(p)))$ and computing s_i and checking the trace has $O(\mathsf{poly}(\log(p)))$ complexity with the CheckTrace algorithm introduced in [Ler22a]. Computing the norm can be done very similarly with the same complexity. This proves the result.   □

5.4 Offline phase

The remaining operations required to be done in the precomputation are exactly the same as in SCALLOP. First, we need to generate the relation lattice associated to the ideal basis $(\mathfrak{l}_i)_{1 \leq i \leq n}$. Second, we need to find a reduced basis of this lattice. These operations can be done exactly as explained in [DFFK+23]. The lattice of relations is generated by solving some discrete logarithms in the class group. Then, the reduced basis is found using standard lattice reduction techniques.

The only real difference between SCALLOP and our new construction is the complexity of those operations. In particular, with our choice of quadratic order, the generation of the lattice of relations takes polynomial time. Indeed, the choice of f ensures that the class group has order $\left(f - \left(\frac{-1}{f} \right) \right) \frac{1}{|\mathcal{O}_0^*|/2}$ with a polynomial smoothness bound. This means that the Pohlig-Hellman method succeeds in solving discrete logarithm in polynomial time and so the full lattice of relations can be generated in polynomial time (whereas it has sub-exponential complexity in general). Unfortunately, the complexity of the basis reductions remains subexponential, which means that the overall complexity of the precomputation is still subexponential. However, as explained in [DFFK+23], the dimension of the relation lattice is quite small in practice and so a nearly-optimal basis can be found efficiently.

5.5 Online phase

We now describe precisely an algorithm GroupAction to perform the group action for SCALLOP-HD given an ideal $\mathfrak{a} = \prod_{1 \leq i \leq n} \mathfrak{l}_i^{e_i}$ where $\mathfrak{l}_i$ is an ideal of norm ℓ_i. In GroupAction below, we restrict to the case $\mathfrak{a} = \prod_i \mathfrak{l}_i$ to simplify the exposition as the generic algorithm simply consists in several executions of the sub-algorithm for $\prod_i \mathfrak{l}_i$.

Proposition 17. *Algorithm 3* GroupAction *is correct and runs in*

$$\tilde{O} \left(\mathsf{poly} \left(\log(p) \log(f) n \right) \sqrt{\max_{1 \leq i \leq n} \ell_i} \right).$$

Algorithm 3 GroupAction$((E, \iota_E), \mathfrak{a})$

Input: p, f, e, ω, β as defined in Section 5.2, 2dim-representation $(E, \omega_E(P), \omega_E(Q))$ of (E, ι_E), and an ideal $\mathfrak{a} = \prod_{1 \le i \le n} \mathfrak{l}_i$, where each $\mathfrak{l}_i$ is an ideal of prime norm ℓ_i
Output: 2dim-representation of $\mathfrak{a} \star (E, \iota_E) = (E_\mathfrak{a}, \iota_{E_\mathfrak{a}})$
1: Compute a deterministic basis P, Q of $E[2^e]$.
2: Set x_β, y_β the values in $\mathbb{Z}$ such that $\beta = x_\beta + y_\beta \omega$.
3: **if** $n(\mathfrak{O}\langle \omega, 2 \rangle) = 2, D_\mathfrak{D} \equiv 0 \bmod 4$ and $\mathfrak{O}\langle \omega, 2 \rangle = \mathfrak{O}\langle \beta, 2 \rangle$ **then**
4:    Compute P_0 the generator of $\ker \omega_E \cap E[2]$.
5:    Compute $F : E^2 \to E^2$ the 2^e-isogeny of kernel $\langle (\omega_E(P), [x_\beta]P + [y_\beta]\omega_E(P)), (\omega_E(Q), [x_\beta]Q + [y_\beta]\omega_E(Q)) \rangle + \{(0,0), (0, P_0)\}$.
6:    Compute the value λ_i such that $\mathfrak{l}_i = \mathfrak{O}\langle \omega - \lambda_i, \ell_i \rangle$.
7: **else if** $n(\mathfrak{O}\langle \omega, 2 \rangle) = 1$ or $\mathfrak{O}\langle \omega, 2 \rangle = \mathfrak{O}\langle \beta, 2 \rangle$ **then**
8:    Compute $F : E^2 \to E^2$ the 2^e-isogeny of kernel generated by $(\omega_E(P), [x_\beta]P + [y_\beta]\omega_E(P)), (\omega_E(Q), [x_\beta]Q + [y_\beta]\omega_E(Q))$.
9:    Compute the value λ_i such that $\mathfrak{l}_i = \mathfrak{O}\langle \omega - \lambda_i, \ell_i \rangle$.
10: **else**
11:    Compute $F : E^2 \to E^2$ the 2^e-isogeny of kernel generated by $(P - \omega_E(P), [x_\beta]P + [y_\beta]\omega_E(P)), (Q - \omega_E(Q), [x_\beta]Q + [y_\beta]\omega_E(Q))$.
12:    Compute the value λ_i such that $\mathfrak{l}_i = \mathfrak{O}\langle \hat{\omega} - \lambda_i, \ell_i \rangle$.
13: **end if**
14: **for** $i \in [1, \ldots, n]$ **do**
15:    Let P_i, Q_i be a basis of ℓ_i in $E[\ell_i]$.
16:    Compute $(\star, U_i) = F(0_E, P_i)$ and $(\star, V_i) = F(0_E, Q_i)$.
17:    Set R_i as one point of order ℓ_i among $\{[2\mathrm{tr}(\omega) - \lambda_i]P_i - U_i, [2\mathrm{tr}(\omega) - \lambda_i]Q_i - V_i\}$.
18: **end for**
19: Compute $\varphi_\mathfrak{a} : E \to E_\mathfrak{a}$, the isogeny of kernel $G_\mathfrak{a} = \bigcap_{1 \le i \le n} \langle R_i \rangle$.
20: Compute a deterministic basis R, S of $E_\mathfrak{a}[2^e]$.
21: Compute $\iota_{E_\mathfrak{a}}(\omega)(R)$ and $\iota_{E_\mathfrak{a}}(\omega)(S)$ using $\varphi_\mathfrak{a}(\omega_E(P))$ and $\varphi_\mathfrak{a}(\omega_E(Q))$.
22: **return** $E_\mathfrak{a}, \iota_{E_\mathfrak{a}}(\omega)(R), \iota_{E_\mathfrak{a}}(\omega)(S)$.

Proof. Let us start by proving correctness. We discuss the details for the first two "if" cases, and for the last "if" case, we simply replace ω by $\hat{\omega}$ in the following discussion. Since $\omega, \beta \in \mathfrak{O}$ we have that the endomorphisms $\omega_E, \iota_E(\beta)$ commutes and since we have $2^e = n(\omega) + n(\beta)$, by Lemma 11, the 2^e-isogeny $F_E : E^2 \to E^2$ is correctly computed from its kernel. Then, we have that $F(0, R) = (\star, \omega_E(R))$ for any point R. Thus, we do have $U_i = \omega_E(P_i), V_i = \omega_E(Q_i)$ for each $1 \le i \le n$. The kernel of $\omega_E - \lambda_i$ is equal to $(\hat{\omega}_E - \lambda_i)(E[\ell_i])$ and since $\hat{\omega}_E = [2\mathrm{tr}(\omega)] - \omega_E$, the point R_i computed is a generator of $\ker(\omega_E - \lambda_i) = \ker \varphi_{\mathfrak{l}_i} = \ker \varphi_{\mathfrak{a}} \cap E[\ell_i]$. Thus, the computation of $\varphi_{\mathfrak{a}}$ is correct, and the computation of the $2\mathsf{dim}$-representation of $\mathfrak{a} \star (E, \iota_E)$ is correct by the formulas given in Section 4.3. The last step is merely changing the evaluation to the deterministic basis using linear algebra.

For the complexity, the 2^e-isogeny F_E can be computed evaluated in $O\left(\mathsf{poly}\left(\log(p)e\right)\right) = O\left(\mathsf{poly}\left(\log(p)\log(f)\right)\right)$. Then, since the points of $E[\ell_i]$ are defined over $\mathbb{F}_{p^2}$, the cost to compute the bases P_i, Q_i and to compute U_i, V_i through evaluation of F is $O\left(\mathsf{poly}\left(\log(p)\log(f)n\right)\right)$.

Finally, using the Velusqrt formulas introduced in [BDFLS20], it is possible to compute the isogeny $\varphi_{\mathfrak{a}}$ of norm $\prod_{1 \le i \le n} \ell_i$ in $\tilde{O}\left(\mathsf{poly}\left(\log(p)n\right)\sqrt{\max_{1 \le i \le n} \ell_i}\right)$. This proves the result. $\square$

6   Some remarks on security

The security of SCALLOP-HD is identical to that of SCALLOP because the group action has the same exact structure. In this section, we take the opportunity to discuss the impact of recent developments from the papers [CII+23,CV23] on the security of SCALLOP and SCALLOP-HD.

In [DFFK+23], one proposed method to attack SCALLOP is to compute the ideal corresponding to the isogeny φ_f of degree f connecting the $\mathfrak{O}_0$-oriented curve E_0 with the $\mathfrak{O}$-oriented curve E. In [CII+23], a polynomial-time quantum algorithm is introduced to perform that computation when there is an efficient way to evaluate this f-isogeny on points of powersmooth order. Since the endomorphism ω_E can be written as $d + \varphi_f \circ \omega_0 \circ \hat{\varphi}_f$ for some integer d and $\omega_0 \in \mathrm{End}(E_0)$, the security of SCALLOP then reduces to the following question:

Can we use the effective orientation ω_E revealed in SCALLOP(-HD) to evaluate φ_f?

As far as we know, the answer to this question is no (at least not in polynomial time). In fact, the problem of evaluating the descending isogeny φ_f was already discussed in [DFFK+23, Section 7] even though the algorithm from [CII+23] didn't exist at the time. The discussion presented in [DFFK+23, Section 7] is still relevant and justifies why evaluating φ_f from ω_E appears hard. One possible way to reduce the search space introduced in [DFFK+23, Section 7] would be to use non-trivial self-pairings (i.e. pairing such that $e(P, P)$ is not 1). However, there are no known self-pairings in the context of SCALLOP(-HD) and some negative results regarding the existence of these objects were even recently shown in [CHM+23].

Recently, [CV23] introduced a generalization of the "lollipop method" to recover an isogeny from a partial torsion information. More concretely, it targets the following setting. Let $\varphi : E_0 \to E$ be an isogeny of degree f and P, Q be a basis of $E_0[N]$ for some big enough integer N. The goal is to recover φ from the knowledge of T, S where T, S is a basis of $E[N]$ equal to $X \cdot \varphi(P, Q)$ for some secret matrix X contained in some subset of $GL_2(\mathbb{Z}/N\mathbb{Z})$. Typically, [CV23] targets the case where X is diagonal, but they introduce a generic framework that can handle a broader variety of families of Xs. The fact that X is unknown is the main obstacle to apply the usual isogeny recovery attacks or the attack from [CII$^+$23]. The paper [CV23] shows how to overcome this obstacle when the parameters d, N, p allow the existence (and efficient computation) of an endomorphism $\rho \in \mathrm{End}(E_0)$ satisfying various constraints.

Below, we try to apply this attack to recover the isogeny φ_f using the knowledge of the orientation. In particular, we will have a look at the case where X is diagonal. Indeed, when taking N as a product of split primes in $\mathfrak{O}_0$, P, Q to be two generators of the eigenspaces of ω_0 in $E_0[N]$ and T, S generators of the eigenspaces of $\omega_E \in E[N]$, we are exactly in the desired setting where the unknown matrix is diagonal (since eigenspaces of ω_0 are mapped to eigenspaces of ω_E by φ_f).

When N is powersmooth, the points P, Q, T, S can be computed in polynomial time by evaluating ω_0 and ω_E, and solving some discrete logarithms. The method introduced in [CD23] works by computing a non-trivial endomorphism $\rho = \kappa \circ \sigma$ such that $[\varphi_f]_*\sigma$ can be computed efficiently, the matrix of the action of ρ in the basis P, Q commutes with the matrix X and $\deg \kappa \leq N^2/f^2$. When those conditions are satisfied, it can be shown that the image of the isogeny $\psi = [\sigma]_*\varphi_f \circ \kappa \circ \hat{\varphi}_f$ on T, S can be computed exactly, allowing for its efficient computation with higher dimensional isogenies. In a number of cases, this is enough to recover φ_f directly, but not always. In the setting of SCALLOP-HD, this is not necessarily new information if the endomorphism $\hat{\psi} \circ [\varphi_f]_*\sigma$ belongs to $\iota_E(\mathfrak{O})$. On the other hand, when it does not, then we obtain a full quaternion suborder of $\mathrm{End}(E)$ in that matter, and that might be enough to evaluate φ_f with an adaptation of [Ler22a, Algorithm 5] and then, we can apply the attack from [CII$^+$23].

Thus, the question becomes: can we find such an endomorphism ρ satisfying all the previous constraints? While we do not know how to prove formally that the answer is always no, we provide examples where we can prove that finding a suitable ρ is impossible.

As far as we know, there are essentially three types of isogenies σ for which we have an efficient way to compute the push-forward $[\varphi_f]_*\sigma$:

1. The identity.
2. The Frobenius.
3. Horizontal isogenies (used in the group action).

Let us consider the case where σ is the identity. We want to find $\rho \in \mathrm{End}(E_0)$ that acts as a diagonal matrix on the subgroups generated by P and Q. As we

explained before, we have an attack if we can find $\rho \notin \mathbb{Z}[\omega_0]$ (otherwise we don't learn anything new).

Let $\mathcal{O}_0$ be a quaternion maximal order isomorphic to $\mathrm{End}(E_0)$ and I, J, the two left $\mathcal{O}_0$-ideals of norm N corresponding to the subgroups generated by P and Q under the Deuring correspondence. Then, ρ will act as a diagonal matrix on the two subgroups if and only if it is contained inside the quaternion order $\mathcal{O} = (\mathbb{Z} + I) \cap (\mathbb{Z} + J)$ which is an Eichler order of level N^2. This is a lattice of volume equal to Cp^2N^4 for some small constant C. And this means the four successive minimas $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ satisfy

$$p^2 N^4 \leq \lambda_1 \lambda_2 \lambda_3 \lambda_4 \leq 16 C p^2 N^4 \tag{5}$$

However, since $\mathbb{Z}[\omega_0]$ is contained inside $\mathcal{O}$ by design, and $\mathfrak{O}_0$ is a quadratic order of very small discriminant, we know that the two first successive minimas are 1 and $n(\omega_0)$ (assuming that ω_0 is the element of smallest norm in $\mathbb{Z}[\omega_0] \smallsetminus \mathbb{Z}$, which we can do without any loss of generality). Moreover, since $\omega_0 \in \mathcal{O}$, we can always multiply any element by ω_0, this means that we must have $\lambda_4 \leq n(\omega_0)\lambda_3$, and so we can deduce that $\lambda_3 \geq pN^2$. This means that the smallest element ρ we can expect to find in $\mathcal{O} \smallsetminus \mathbb{Z}[i]$ has norm greater than pN^2. But, to make the attack work, we need that $N^2 > f^2 \deg \rho$. These two conditions are clearly not compatible, and this means that there is no hope to find a suitable ρ to make the attack work in this setting.

Let us now consider the case where σ is the Frobenius isogeny. When $\mathcal{O}_0$ contains j (which we can assume since the class number of $\mathfrak{O}_0$ is 1 and it has been shown in [CPV20] that the only $\mathfrak{O}_0$-oriented is $\mathbb{F}_p$-rational when p is big enough), finding ρ when σ is the Frobenius implies that ρ is contained inside $\mathcal{O} \cap \mathcal{O}_0 j$. It can be verified that the successive minimum of this lattice are small linear combinations of $p, p\omega_0, Nj, N\omega_0 j$ and thus the solutions outside of $\mathbb{Z}[i]$ have norm bigger than N^2. Thus, it is once again not possible to find ρ with $N^2 > f^2 \deg \rho$. A similar reasoning can be applied to prove that a suitable endomorphism ρ cannot be found when σ is an $\mathfrak{O}_0$-horizontal isogeny.

Thus, we have proven that the lollipop method cannot be applied to the setting of SCALLOP-HD when considering the torsion information revealed by the orientation on the points whose order is a product of split primes.

The same reasoning cannot be applied if we consider inert primes. Indeed, in that case, the matrix will probably not be diagonal. However, this also means that we don't really know what kind of matrix is required for the endomorphism ρ. Thus, it seems hard to use the lollipop method in that case.

7   Conclusion and future work

SCALLOP-HD represents the progression of a series of efforts to enhance the scalability of EGAs based on isogenies. Beginning with CSI-FiSh, which established the foundational strategy and gave a notable example, there was a significant challenge in computing larger class groups. SCALLOP then built upon the work of CSI-FiSh by overcoming this limitation, but needed subexponential time

for generating the lattice of relation. SCALLOP-HD takes this advancement a step further, making precomputation polynomial time except for the lattice reduction algorithms. While these algorithms are theoretically subexponential in complexity, the dimensions are in fact manageable in practice.

SCALLOP-HD is heavily based on the SCALLOP group action [DFFK+23]. The main difference stems from the way the orientation is computed. In SCALLOP, an effective orientation is obtained from an endomorphism of smooth degree, whereas in SCALLOP-HD, an effective orientation is obtained from a 2dim-representation of an arbitrary degree endomorphism. The relaxation of the constraint on the degree of the endomorphism is the main advantage of SCALLOP-HD as it improves scalability and simplifies the group action computation at the cost of requiring the computation of a 2^e-isogeny between abelian variety of dimension 2.

The 2dim-representation technique we developed in order to represent set elements in SCALLOP-HD is interesting in its own right. It has already seen applications in [Ler23] and Remark 15, bringing down the dimension needed to compute the isogenies between abelian varieties from 4 or 8 to 2.

The main remaining problem is to make an efficient implementation of SCALLOP-HD. This is a non-trivial task due to the need of isogeny computation in higher dimension. Several algorithms and implementations already exists [CDS20,Kun22], [MMP+23,BMP23,DLRW23,CDPMR23], but there are some on-going efforts to improve significantly the efficiency of these computations, and we intend to provide a full implementation of SCALLOP-HD once the state of the art on this topic is somewhat stable. In the end, we believe that the efficiency of SCALLOP-HD's group action computation could outperform SCALLOP's due to its simplicity.

References

ADFMP20.   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.

BDFLS20.   Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. *Open Book Series*, 4(1):39–55, 2020.

BDK+23.   Ward Beullens, Samuel Dobson, Shuichi Katsumata, Yi-Fu Lai, and Federico Pintore. Group signatures and more from isogenies and lattices: generic, simple, and efficient. *Designs, Codes and Cryptography*, pages 1–60, 2023.

BKP20.   Ward Beullens, Shuichi Katsumata, and Federico Pintore. Calamari and falafl: logarithmic (linkable) ring signatures from isogenies and lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 464–492. Springer, 2020.

BKV19.   Ward Beullens, Thorsten Kleinjung, and Frederik Vercauteren. Csi-fish: efficient isogeny based signatures through class group computations. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 227–247. Springer, 2019.

BLMP19.   Daniel J Bernstein, Tanja Lange, Chloe Martindale, and Lorenz Panny. Quantum circuits for the csidh: optimizing quantum evaluation of isogenies. In *Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19–23, 2019, Proceedings, Part II 38*, pages 409–441. Springer, 2019.

BMP23.   Andrea Basso, Luciano Maino, and Giacomo Pope. Festa: Fast encryption from supersingular torsion attacks. *Cryptology ePrint Archive*, 2023.

BS16.   Jean-François Biasse and Fang Song. *Efficient quantum algorithms for computing class groups and solving the principal ideal problem in arbitrary degree number fields*, pages 893–902. 2016.

BS20.   Xavier Bonnetain and André Schrottenloher. Quantum security analysis of csidh. In *Advances in Cryptology–EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10–14, 2020, Proceedings, Part II 30*, pages 493–522. Springer, 2020.

CD23.   Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 423–447. Springer, 2023.

CDPMR23.   Jesús-Javier Chi-Domínguez, Amalia Pizarro-Madariaga, and Edgardo Riquelme. Computing quotient groups of smooth order with applications to isogenies over higher-dimensional abelian varieties. *Cryptology ePrint Archive*, 2023.

CDS20.   Wouter Castryck, Thomas Decru, and Benjamin Smith. Hash functions from superspecial genus-2 curves using richelot isogenies. *Journal of Mathematical Cryptology*, 14(1):268–292, 2020.

CHM+23.   Wouter Castryck, Marc Houben, Simon-Philipp Merz, Marzio Mula, Sam van Buuren, and Frederik Vercauteren. Weak instances of class group action based cryptography via self-pairings. In *Annual International Cryptology Conference*, pages 762–792. Springer, 2023.

CII+23.   Mingjie Chen, Muhammad Imran, Gábor Ivanyos, Péter Kutas, Antonin Leroux, and Christophe Petit. Hidden stabilizers, the isogeny to endomorphism ring problem and the cryptanalysis of psidh. Cryptology ePrint Archive, Paper 2023/779, 2023. https://eprint.iacr.org/2023/779.

CK20.   Leonardo Colò and David Kohel. Orienting supersingular isogeny graphs. *J. Math. Cryptol.*, 14(1):414–437, 2020.

CLM+18.   Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In *Advances in Cryptology - ASIACRYPT 2018*, pages 395–427, 2018.

CPV20.   Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 523–548. Springer, 2020.

CS20.   Daniele Cozzo and Nigel P Smart. Sashimi: cutting up csi-fish secret keys to produce an actively secure distributed signing protocol. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings 11*, pages 169–186. Springer, 2020.

CSCDJRH22.   Jorge Chávez-Saab, Jesús-Javier Chi-Domínguez, Samuel Jaques, and Francisco Rodríguez-Henríquez. The sqale of csidh: sublinear vélu quantum-resistant isogeny action with low exponents. *Journal of Cryptographic Engineering*, 12(3):349–368, 2022.

CV23.   Wouter Castryck and Frederik Vercauteren. A polynomial time attack on instances of m-sidh and festa. *ASIACRYPT*, 2023.

DFFK+23.   Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. Scallop: scaling the csi-fish. *PKC*, 2023.

DFKL+20.   Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign: Compact post-quantum signatures from quaternions and isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 64–93, Cham, 2020. Springer International Publishing.

DFLLW23.   Luca De Feo, Antonin Leroux, Patrick Longa, and Benjamin Wesolowski. New algorithms for the deuring correspondence: towards practical and secure sqisign signatures. In *Advances in Cryptology– EUROCRYPT 2023: 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part V*, pages 659–690. Springer, 2023.

DFM20.   Luca De Feo and Michael Meyer. Threshold schemes from isogeny assumptions. In *Public-Key Cryptography–PKC 2020: 23rd IACR International Conference on Practice and Theory of Public-Key Cryptography, Edinburgh, UK, May 4–7, 2020, Proceedings, Part II 23*, pages 187–212. Springer, 2020.

DLRW23.   Pierrick Dartois, Antonin Leroux, Damien Robert, and Benjamin Wesolowski. Sqisignhd: New dimensions in cryptography. *Cryptology ePrint Archive*, 2023.

DMS23.   Thomas Decru, Luciano Maino, and Antonio Sanso. Towards a quantum-resistant weak verifiable delay function. *Cryptology ePrint Archive*, 2023.

FFK+23.   Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. Scallop: scaling the csi-fish. Cryptology ePrint Archive, Paper 2023/058, 2023. https://eprint.iacr.org/archive/2023/058/20230303:083840.

HM89.   James Lee Hafner and Kevin S. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American Mathematical Society*, 2:837–850, 1989.

Kan97.   Ernst Kani. The number of curves of genus two with elliptic differentials. *Journal für die reine und angewandte Mathematik (Crelles Journal)*, 1997:122 – 93, 1997.

KLLQ23.   Shuichi Katsumata, Yi-Fu Lai, Jason T LeGrow, and Ling Qin. Csi-otter: Isogeny-based (partially) blind signatures from the class group action with a twist. In *Annual International Cryptology Conference*, pages 729–761. Springer, 2023.

Koh96.   David Russell Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.

Kun22.   Sabrina Kunzweiler. Efficient computation of $(2^{\hat{}}\,n, 2^{\hat{}}\,n)$-isogenies. *Cryptology ePrint Archive*, 2022.

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

Ler22a.   Antonin Leroux. A new isogeny representation and applications to cryptography. In *Advances in Cryptology–ASIACRYPT 2022: 28th International Conference on the Theory and Application of Cryptology and Information Security, Taipei, Taiwan, December 5–9, 2022, Proceedings, Part II*, pages 3–35. Springer, 2022.

Ler22b.   Antonin Leroux. *Quaternion Algebra and isogeny-based cryptography.* PhD thesis, Ecole doctorale de l'Institut Polytechnique de Paris, 2022.

Ler23.   Antonin Leroux. Verifiable random function from the deuring correspondence and higher dimensional isogenies. *Cryptology ePrint Archive*, 2023.

LR22.   Antonin Leroux and Maxime Roméas. Updatable encryption from group actions. *Cryptology ePrint Archive*, 2022.

MMP$^+$23. Luciano Maino, Chloe Martindale, Lorenz Panny, Giacomo Pope, and Benjamin Wesolowski. A direct key recovery attack on sidh. In *EUROCRYPT*, 2023.

MW23.   Arthur Herlédan Le Merdy and Benjamin Wesolowski. The supersingular endomorphism ring problem given one endomorphism. Cryptology ePrint Archive, Paper 2023/1448, 2023. https://eprint.iacr.org/2023/1448.

Onu21.   Hiroshi Onuki. On oriented supersingular elliptic curves. *Finite Fields App.*, 69, 2021.

Pei20.   Chris Peikert. He gives c-sieves on the csidh. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 463–492. Springer, 2020.

Rob22.   Damien Robert. Evaluating isogenies in polylogarithmic time. *Cryptology ePrint Archive*, 2022.

Rob23.   Damien Robert. Breaking sidh in polynomial time. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 472–503. Springer, 2023.

Wat69.   William C Waterhouse. Abelian varieties over finite fields. In *Annales scientifiques de l'École normale supérieure*, volume 2, pages 521–560, 1969.

Wes22.   Benjamin Wesolowski. Orientations and the supersingular endomorphism ring problem. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *Lecture Notes in Computer Science*, pages 345–371. Springer, 2022.