On the Isogeny Problem with Torsion Point Information

Tako Boris Fouotsa[1], Péter Kutas[2,3], Simon-Philipp Merz[4], Yan Bo Ti[5]

[1] LASEC-EPFL, Switzerland
[2] University of Birmingham, UK
[3] Eötvös Loránd University, Hungary
[4] Royal Holloway, University of London, UK
[5] DSO, Singapore

Abstract. It has recently been rigorously proven (and was previously known under certain heuristics) that the general supersingular isogeny problem reduces to the supersingular endomorphism ring computation problem. However, in order to attack SIDH-type schemes, one requires a particular isogeny which is usually not returned by the general reduction. At Asiacrypt 2016, Galbraith, Petit, Shani and Ti presented a polynomial-time reduction of the problem of finding the secret isogeny in SIDH to the problem of computing the endomorphism ring of a supersingular elliptic curve. Their method exploits the fact that secret isogenies in SIDH are of degree approximately $p^{1/2}$. The method does not extend to other SIDH-type schemes, where secret isogenies of larger degree are used and this condition is not fulfilled.
We present a more general reduction algorithm that generalises to all SIDH-type schemes. The main idea of our algorithm is to exploit available torsion point images together with the KLPT algorithm to obtain a linear system of equations over a certain residue class ring. We show that this system will have a unique solution that can be lifted to the integers if some mild conditions on the parameters are satisfied. This lift then yields the secret isogeny. One consequence of this work is that the choice of the prime p in B-SIDH is tight.
Finally, we show that our reduction still applies for SIDH variations deploying recently proposed countermeasures against a series of classical polynomial time attacks against SIDH.

Keywords: post-quantum · isogeny-based cryptography · supersingular isogenies · endomorphism rings · SIDH

1 Introduction

Practical large scale quantum computers pose a threat to most cryptosystems currently in use [16, 34]. Recent advances in quantum computing and the need for long-term security in cryptography has led to a surge of interest in developing quantum secure replacements for these classical cryptographic algorithms. Moreover, NIST has started a procedure to determine new cryptographic standards for a post-quantum era [28].

Most of the standardisation candidates are based on lattices, codes or multivariate polynomial systems over finite fields. A more recent but promising area of post-quantum research is isogeny-based cryptography.

Couveignes was the first one to propose isogenies for cryptographic use in 1997 [7], and the area gained traction in the following decade with new independent developments such as collision-resistant hashing [4] and key exchange [33, 36] based on isogeny problems. After Jao and De Feo introduced supersingular isogeny Diffie–Hellman (SIDH) [18], a predecessor of the isogeny-based submission to NIST's standardisation procedure SIKE [17], the area has enjoyed increasing popularity.

The central problem in most of isogeny-based cryptography is to find an isogeny $\varphi : E_1 \to E_2$, i.e. a morphism in the sense of both algebraic geometry and group theory, between two given supersingular elliptic curves defined over a finite field $\mathbb{F}_q$. For two supersingular elliptic curves E_1 and E_2, the problem of computing an arbitrary isogeny between them and the problem of computing their endomorphism rings $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$ was recently proven to be equivalent under the assumption that the generalised Riemann hypothesis (GRH) holds by Wesolowski [41]. Yet, in the case where E_1 and E_2 are ordinary curves, it is usually much easier to determine $\mathrm{End}(E_i)$ of an arbitrary E_i than computing an isogeny between two arbitrary curves [22].

There are infinitely many isogenies $E_1 \to E_2$, but attacking isogeny-based primitives such as SIDH requires the attacker to recover an isogeny $\varphi : E_1 \to E_2$ of a specific degree. Generic algorithms are unlikely to return an isogeny of the correct degree given the endomorphism rings. In Section 4 of [15], it is shown how to recover secret isogenies in the case of SIDH. The attack exploits the observation that secret isogenies in SIDH are of degree $p^{1/2}$, which is relatively small compared to the diameters of the graphs involved. In the case where the isogeny one wishes to recover is not of particularly small degree, as is the case for example in B-SIDH [6], SÉTA [9] or instantiations of SIDH with secret isogenies of larger degree, the observation no longer holds and the algorithm of [15] no longer applies.

A unique trait of SIDH is that it reveals auxiliary points, which are the images of certain torsion points under the secret isogeny. A recent series of papers [3, 26, 32] exploits the presence of these points to break SIDH and associated schemes that also reveal auxiliary points. Some countermeasures have been proposed to foil the attacks by blinding the degree and/or the auxiliary points [12, 27]. We will show that the reduction of this paper still applies in presence of said countermeasures.

Our contributions. Assuming the generalised Riemann hypothesis, this paper provides a polynomial-time (in $\log p$) algorithm that recovers an isogeny with prescribed N_2-torsion point images between two supersingular elliptic curves of a specific degree N_1, given their endomorphism rings and some N_2-torsion point images under the isogeny. More precisely, let d be the least degree of any isogeny between two isogenous supersingular elliptic curves E_1 and E_2. Then, our algorithm solves the following task, whenever $N_1 < dN_2/16$.

Task 1.1. *Let N_1, N_2 be coprime integers and let $\varphi : E_1 \to E_2$ be a secret isogeny of degree N_1 between two supersingular elliptic curves. Let P_B, Q_B be a basis of $E_1[N_2]$. Given* $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$, $\varphi(P_B)$, *and* $\varphi(Q_B)$, *find an isogeny $\varphi' : E_1 \to E_2$ of degree N_1 such that $\varphi_{|E_1[N_2]} = \varphi'_{|E_1[N_2]}$.*

Since SIDH-type schemes such as B-SIDH tend to use balanced parameters, where $N_1 \approx N_2$, the condition that $N_1 < dN_2/16$ is very mild.

The main idea behind the algorithm is the following. Isogenies from E_1 to E_2 form a $\mathbb{Z}$-module M of rank 4. A basis of M can be computed using an algorithm due to Kirschmer and Voight [20] (or the KLPT algorithm [21]). Then, one computes an LLL-reduced basis $\psi_1, \psi_2, \psi_3, \psi_4$ of M. We show how to evaluate $\psi_i(P_B)$, $\psi_i(Q_B)$ for $i = 1, \ldots, 4$ and we are given $\varphi(P_B)$ and $\varphi(Q_B)$.

Since $\varphi = x_1\psi_1 + x_2\psi_2 + x_3\psi_3 + x_4\psi_4$ for some $x_i \in \mathbb{Z}$, this yields 4 linear equations in 4 variables, x_1, x_2, x_3, x_4, modulo N_2 (torsion point images can be represented by a 2×2 matrix with entries from $\mathbb{Z}/N_2\mathbb{Z}$ and each entry corresponds to an equation). We will show that this system of equations has a unique solution for x_i modulo N_2 which we also compute. Since the ψ_i form an LLL-reduced basis, we can bound the absolute value of the coefficients x_i by $N_2/2$ for $N_1 < dN_2/16$. This leads to a solution for $x_i \in \mathbb{Z}$.

The contribution of this paper can be seen as an extension of previous reductions by Kohel, Lauter, Petit, and Tignol [21] and Wesolowski [41] which allow to compute an isogeny (of no specific degree) between two supersingular elliptic curves, whenever the endomorphism rings of the curves are known. Note that Kohel et al. provide a heuristic polynomial-time algorithm for this reduction, whereas Wesolowski shows that this reduction works in polynomial-time in general assuming only GRH.

Since publication of the conference version of this work at PKC 2022 [13], a series of papers by Castryck and Decru, Maino and Martindale, and Robert [3, 26, 32] broke SIDH and various derivatives such as B-SIDH or SÉTA efficiently by using the auxiliary points published in the protocols. Our paper also targets these points for an attack, and it would seem like our paper is superseded by the aforementioned papers. However, there are two reason why our results are still relevant. We discuss how our attack fits into this new landscape of isogeny-based cryptography.

Firstly, in many cases we need less torsion point information than the aforementioned attacks. Secondly, countermeasures have been proposed that can foil the attacks by blinding the degree and/or the auxiliary points [12, 27]. We show how to extend the reduction of this paper to instances deploying these countermeasures.

Together with known results on the computation of endomorphism rings, a consequence of this work is an answer to the open question how small the size of the prime p in B-SIDH can be chosen. (Note, that by using a starting curve of unknown endomorphism ring and masking the torsion-point images, B-SIDH is not yet broken by recent attacks.) More precisely, this work implies that one cannot lower the size of the prime p in B-SIDH significantly, while maintaining the claimed security level. Yet, current parameter sets are not threatened by our reduction because parameters were selected in a cautious way (i.e., were larger than necessary if one only accounted for existing attacks at the time).

Our algorithm has a similar classical runtime to a generic meet-in-the-middle algorithm but is essentially memory-free whereas meet-in-the-middle requires an exponential amount of memory. Furthermore, the quantum version of our attack has a much better runtime than previously known quantum attacks ($O(p^{1/4})$ [11] compared to $O(p^{1/2})$ [19]). In previous quantum attacks, the authors showed that Tani's claw finding algorithm has better quantum complexity, but suffers from issues arising in quantum storage. Hereby, the running time of our algorithms is dominated by the computation of endomorphism rings of supersingular elliptic curves.

Outline. In Section 2, we recall some necessary mathematical background, details of the SIDH key exchange as well as related work. In Section 3, we give algorithms to evaluate non-smooth degree isogenies and to compute an isogeny of a specific degree between two supersingular elliptic curves with known endomorphism ring, if certain torsion point information is available. In Section 4, we will address the implications of the attacks that used auxiliary points to break SIDH. We discuss the impact of our paper on isogeny-based cryptography in Section 5 before we conclude the paper in Section 6.

2 Preliminaries

In this section, we recall some relevant background on elliptic curves and isogeny-based cryptography. For further introductory reading, we refer to Silverman [35] and De Feo [8] respectively. Furthermore, we briefly recall some consequences of the KLPT algorithm [21] and the LLL lattice reduction [23]. Moreover, we sketch a related algorithm due to Galbraith et al. [15] which computes an isogeny of specific degree between two supersingular elliptic curves with known endomorphism ring, if the degree of the sought after isogeny is sufficiently small.

2.1 Elliptic curves and isogenies

Let E_1, E_2 be elliptic curves defined over a field K. An isogeny between E_1 and E_2 is a non-constant rational map which is also a group homomorphism (or equivalently, fixes the point at infinity). The *degree* of an isogeny is its degree as a finite map of curves, i.e. the degree of the extension of function fields. An isogeny is called *separable* if the corresponding field extension is separable. For a separable isogeny, the degree equals the size of its kernel. Furthermore, for every finite subgroup G of an elliptic curve E, there exists a separable isogeny whose kernel is G. Up to post-composition with an isomorphism, the isogeny is unique. We denote the codomain of this isogeny by E/G. Given a finite subgroup $G \subset E$ the corresponding isogeny from E to E/G can be computed using Vélu's formulae [39].

Let $\phi : E_1 \to E_2$ be an isogeny of degree d. Then there exists a unique isogeny $\hat{\phi}$ with the property that $\phi \circ \hat{\phi} = [d]$, where $[d]$ denotes the multiplication by d. This isogeny $\hat{\phi}$ is called the *dual* of ϕ and it is also of degree d. An isogeny from E to itself is called an *endomorphism*. Together with the zero map, endomorphisms of E form a ring under addition and composition denoted by $\mathrm{End}(E)$.

Let E be defined over a finite field of characteristic p. Then $\mathrm{End}(E)$ is either an order in an imaginary quadratic field and E is called *ordinary*, or a maximal order in the rational quaternion algebra $B_{p,\infty}$ ramified at p and at infinity in which case E is called *supersingular*. For the rest of the paper we will restrict ourselves to supersingular elliptic curves.

For an elliptic curve $E : y^2 = x^3 + Ax + B$, its j*-invariant* is given by $j(E) = 1728\frac{4A^3}{4A^3+27B^2}$ and two curves are isomorphic over $\overline{K}$ if and only if they share the same j-invariant.

Example 2.1. For the supersingular elliptic curve $E_0 : y^2 = x^3 + x$ the above formula yields the j-invariant $j(E_0) = 1728$. It is well-known that $\mathrm{End}(E_0)$ is the $\mathbb{Z}$-module generated by $1, \iota, \frac{1+\pi}{2}$ and $\frac{\iota+\iota\pi}{2}$, where ι denotes E_0's non-trivial automorphism, $(x, y) \mapsto (-x, iy)$, and π is the Frobenius endomorphism, $(x, y) \mapsto (x^p, y^p)$.

Let ℓ be a prime number and define the supersingular ℓ-isogeny *graph* as follows. The vertices of the graph are isomorphism classes of supersingular elliptic curves represented by their j-invariant and two vertices are connected by an edge if and only if they are ℓ-isogenous. The supersingular ℓ-isogeny graph is connected, $(\ell + 1)$-regular and a Ramanujan expander graph. The diameter of the graph is between $\log p$ and $2 \log p$ [31, Theorem 1]. The presumed hardness of path-finding in this graph is the hardness assumption underlying isogeny-based cryptography.

Remark 2.2. In the rest of this paper we will call an integer smooth if its smoothness bound is polynomial in $\log p$ for a fixed p.

2.2 SIDH and B-SIDH

We give a brief description of SIDH [18] and B-SIDH [6] key exchanges.

The public parameters of SIDH are two coprime smooth numbers N_1 and N_2, a prime p of the form $p = N_1N_2f - 1$, where f is a small cofactor, and a supersingular elliptic curve E_0 defined over $\mathbb{F}_{p^2}$ together with points P_A, Q_A, P_B, Q_B such that $E_0[N_1] = \langle P_A, Q_A\rangle$ and $E_0[N_2] = \langle P_B, Q_B\rangle$.

The protocol proceeds as follows:

1. Alice chooses a random cyclic subgroup of $E_0[N_1]$ as $G_A = \langle P_A + [x_A]Q_A\rangle$ and Bob chooses a random cyclic subgroup of $E_0[N_2]$ as $G_B = \langle P_B+[x_B]Q_B\rangle$.
2. Alice and Bob compute the isogeny $\phi_A : E_0 \to E_0/\langle G_A\rangle =: E_A$ and the isogeny $\phi_B : E_0 \to E_0/\langle G_B\rangle =: E_B$, respectively.

3. Alice sends the curve E_A and the two points $\phi_A(P_B), \phi_A(Q_B)$ to Bob. Mutatis mutandis, Bob sends $\big(E_B, \phi_B(P_A), \phi_B(Q_A)\big)$ to Alice.
4. Alice and Bob use the given torsion points to obtain the shared secret $j(E_0/\langle G_A, G_B\rangle)$. To do so, Alice computes $\phi_B(G_A) = \phi_B(P_A) + [x_A]\phi_B(Q_A)$ and uses the fact that $E_0/\langle G_A, G_B\rangle \cong E_B/\langle \phi_B(G_A)\rangle$. Bob proceeds analogously.

In practice N_1 and N_2 are chosen to be powers of 2 and 3, respectively, to maximise the efficiency of the scheme. However, choosing a prime of the form $N_1 N_2 f - 1$ with $N_1 \approx N_2$ implies that the curves E_A, E_B are much closer at E_0 relative to the diameter of the supersingular isogeny graph, i.e. the paths connecting E_0 with E_A and E_B are shorter than one would expect for randomly chosen isogenous curves.

In order to avoid walking only in a small subgraph and to reduce the size of the prime p, Costello introduced the variant B-SIDH [6]. The main differences between SIDH and B-SIDH are

– N_1 and N_2 are smooth coprime divisors of $p-1$ and $p+1$ (or vice versa) respectively. Hence, $p-1$ and $p+1$ both need to have large smooth factors as opposed to just one of them in SIDH.
– For the best parameter choice, we have $N_1 \approx N_2 \approx p$ as opposed to $N_1 \approx N_2 \approx \sqrt{p}$ in SIDH.
– Kernel generators are a priori $\mathbb{F}_{p^4}$-rational as opposed to $\mathbb{F}_{p^2}$-rational.

In B-SIDH the curves E_0 and E_A are no longer closer than expected in the isogeny graph, but parameter selection might be harder and it seems at first to come at the expense of working over larger field extensions. However, to every supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, there exists a quadratic twist (i.e., a curve defined over $\mathbb{F}_{p^2}$ which is isomorphic to E over $\mathbb{F}_{p^4}$ but not over $\mathbb{F}_{p^2}$). If E has $(p+1)^2$ rational points over $\mathbb{F}_{p^2}$, then its twist has $(p-1)^2$ rational points over $\mathbb{F}_{p^2}$. Thus, when computing an isogeny of degree N_1 dividing $p+1$ one can work with the curves having $p+1$ rational points, and before computing an isogeny of degree N_2 dividing $p-1$, one switches to twists that have $p-1$ rational points. Technically, the switch makes it possible to compute the isogenies using only operations over $\mathbb{F}_{p^2}$. For more details we refer to [6].

A recent series of attacks breaks SIDH and B-SIDH efficiently using the provided torsion point information [3, 32]. So far, the countermeasures proposed to hinder the attacks are to mask the degree of the secret isogeny [27] or to mask the torsion point information by revealing a scalar multiple of the torsion points instead [12]. In Section 4, we describe how our reduction of this paper still applies in presence of said countermeasures.

2.3 KLPT and LLL lattice reduction

In this subsection, we recall some facts about the Kohel–Lauter–Petit–Tignol (KLPT) algorithm [21] and the Lenstra–Lenstra–Lovász (LLL) lattice reduction [23].

Let $B_{p,\infty}$ be the quaternion algebra ramified at p and at infinity. Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be maximal orders in $B_{p,\infty}$. Then the quaternion isogeny problem asks for a left ideal I connecting $\mathcal{O}_1$ and $\mathcal{O}_2$, i.e., a left ideal I of $\mathcal{O}_1$ which is also a right ideal of $\mathcal{O}_2$. By [21, Lemma 8], we have the following result.

Lemma 2.3. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be maximal orders in $B_{p,\infty}$. Then the intersection $\mathcal{O}_1 \cap \mathcal{O}_2$ has the same index M in $\mathcal{O}_1$ and $\mathcal{O}_2$. Furthermore,*

$$I(\mathcal{O}_1, \mathcal{O}_2) = \{\alpha \in B_{p,\infty} \mid \alpha \mathcal{O}_2 \overline{\alpha} \subset M\mathcal{O}_1\}$$

is a left ideal of $\mathcal{O}_1$ and a right ideal of $\mathcal{O}_2$ of reduced norm M. $I(\mathcal{O}_1, \mathcal{O}_2)$ can be computed in polynomial time.

Lemma 2.3 shows that one can compute a connecting ideal between two maximal orders efficiently. However, this ideal will not have smooth norm in general. In [21], the main algorithm shows how to compute an equivalent left ideal of $\mathcal{O}_1$ of norm ℓ^k where ℓ is some small prime number.

Let E_1, E_2 be supersingular elliptic curves with endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. Then the set of isogenies from E_1 to E_2 is a left $\mathcal{O}_1$-module and a right $\mathcal{O}_2$-module. In particular, they form a $\mathbb{Z}$-lattice of rank 4 [40, Lemma 42.1.11]. The $\mathbb{Z}$-lattice is isomorphic to a connecting left ideal I as an $\mathcal{O}_1$-module by the following lemma.

Lemma 2.4. *[40, 42.2.8] Let $\mathrm{Hom}(E_2, E_1)$ denote the set of isogenies from E_2 to E_1 and let $\mathcal{O}_1$ and $\mathcal{O}_2$ denote the endomorphism rings of E_1 and E_2 respectively. Let I be a connecting ideal of $\mathcal{O}_1$ and $\mathcal{O}_2$ and let $\phi_I : E_2 \to E_1$ denote the corresponding isogeny. Then the map $\phi_I^* : \mathrm{Hom}(E_1, E_2) \to I$, $\psi \mapsto \psi \circ \phi_I$ is an isomorphism of left $\mathcal{O}_1$-modules.*

Since the KLPT algorithm computes a connecting ideal between two maximal orders, Lemma 2.4 implies that one can compute a $\mathbb{Z}$-basis of $\mathrm{Hom}(E_1, E_2)$. However, the degree of these isogenies might not be smooth and it is not obvious that one can evaluate them efficiently. In Algorithm 1, we will show that one can evaluate these isogenies on points efficiently using the KLPT algorithm.

Next, we recall some basic facts about lattice reduction, which aims to transform an arbitrary input basis into a basis of "higher quality". In the following, we are interested in bases that are close to orthogonal.

Let $B := (b_1, \ldots, b_n)$ be the basis of a lattice L, let π_i denote the projection onto $\mathrm{span}(b_1, \ldots, b_{i-1})$ for $i = \{1, \ldots, n\}$ and let $B^* := (b_1^*, \ldots, b_n^*)$ be the *Gram–Schmidt orthogonalization* of B, where $b_i^* = \pi_i(b_i)$. Intuitively speaking, a good basis is one in which the sequence of Gram–Schmidt norms $\|b_1^*\|, \|b_2^*\|, \ldots, \|b_n^*\|$ does not decay too fast.

The Lenstra–Lenstra–Lovász (LLL) reduction calculates a short and nearly orthogonal lattice basis for any lattice in polynomial time [23]. We recall a more precise statement in the following proposition using the Gram–Schmidt coefficients $\mu_{i,j} := \frac{\langle b_i, b_j^* \rangle}{\langle b_j^*, b_j^* \rangle}$.

Proposition 2.5. *The LLL lattice reduction with factors (η, δ), where $\delta \in (0.25, 1)$ and $\eta \in [0.5, \sqrt{\delta}]$, provides in polynomial time a basis $B = (b_1, \ldots, b_n)$ that is size-reduced with $\mu_{i,j} < \eta$ for all $j < i$ and has Gram–Schmidt orthogonalization satisfying the Lovász condition $\delta \|b_i^*\|^2 \leq \|\mu_{i+1,i} b_i + b_{i+1}^*\|^2$.*

The default parameters for LLL reduction in MAGMA, which we use in this paper, are $\delta = 0.75$ and $\eta = 0.501$. Since LLL-reduced bases are in some sense close to orthogonal, we can expect short vectors in the lattice to have rather small coefficients with respect to the basis. This is captured by the following lemma which is a consequence of [23, Equation (1.8)] and Cramer's rule.

Lemma 2.6. *Let L be a full rank lattice with LLL-reduced basis $b_1, \ldots, b_n$ with factors (η, δ) and let $v := \sum_{i=1}^{n} \gamma_i b_i \in L$. Then*

$$|\gamma_i| \leq \left(\frac{4}{(4\delta - 1)}\right)^{n(n-1)/4} \frac{|v|}{|b_i|}.$$

Proof. By [23, Equation (1.8)], an LLL-reduced basis $b_1, \ldots, b_n$ satisfies

$$\prod_{i=1}^{n} |b_i| \leq \left(\frac{4}{(4\delta - 1)}\right)^{n(n-1)/4} \det(L).$$

Therefore, using Cramer's rule we get

$$\begin{aligned} |\gamma_i| &= \frac{\det(b_1, \ldots, b_{i-1}, v, b_{i+1}, \ldots, b_n)}{\det(L)} \leq \frac{|b_1| \cdots |b_{i-1}| \cdot |v| \cdot |b_{i+1}| \cdots |b_n|}{\det(L)} \cdot \frac{|b_i|}{|b_i|} \\ &\leq \left(\frac{4}{(4\delta - 1)}\right)^{n(n-1)/4} \cdot \frac{|v| \cdot \det(L)}{|b_i| \cdot \det(L)} = \left(\frac{4}{(4\delta - 1)}\right)^{n(n-1)/4} \cdot \frac{|v|}{|b_i|}. \end{aligned}$$ □

2.4 GPST

In [15, §4], Galbraith, Petit, Shani and Ti describe how to compute the secret isogeny of an SIDH instance efficiently, if the endomorphism rings of both the domain and the codomain of the isogeny are known (or can be computed). We summarise their results and we recall why the algorithm does not work as such outside of an SIDH setting.

Let $\varphi : E_1 \to E_2$ be a ℓ^n-degree isogeny one wishes to recover, given the two endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ of E_1 and E_2 respectively. Since E_1 and E_2 are supersingular curves, their endomorphism rings are maximal orders in the rational quaternion algebra $B_{p,\infty}$. By Lemma 2.3, one can recover an ideal connecting $\mathcal{O}_1$ and $\mathcal{O}_2$. Such an ideal corresponds to one of infinitely many isogenies between E_1 and E_2. This isogeny is in general not of degree ℓ^n and, in particular, it is not the same as φ. Yet, to attack SIDH, the isogeny needs to be of the correct degree and should also have the correct action on the torsion points.

The secret isogenies in SIDH are of degree approximately $\sqrt{p}$. However, a pair of random supersingular elliptic curves over $\mathbb{F}_{p^2}$ is unlikely to be connected by an isogeny of degree significantly smaller than $\sqrt{p}$. In [15], the authors leverage this observation to recover the target isogeny given the endomorphism rings of E_1 and E_2 as follows.

Given a connecting ideal I for the endomorphism rings, the authors compute a Minkowski reduced basis which is used to recover an element $\alpha \in I$ of minimal norm. By [21, Lemma 5], the ideal $I' := I\overline{\alpha}/\operatorname{Norm}(I)$ is another ideal connecting $\mathcal{O}_1$ and $\mathcal{O}_2$ of minimal norm, $\operatorname{Norm}(\alpha)$. Then, one can compute the isogeny $E_1 \to E_2$ of degree $\operatorname{Norm}(\alpha)$ corresponding to this ideal using Vélu's formulae. If the shortest isogeny between E_1 and E_2 is indeed of degree ℓ^n, this algorithm allows to recover such an isogeny of correct degree from the endomorphisms. The experimental results in [15] suggest that, by trying relatively few small elements α in the previous algorithm, one recovers an isogeny that can be used to attack SIDH with overwhelming probability.

Clearly, the approach outlined above relies crucially on the fact that the degree of the isogeny one wants to recover is among the smallest possible degrees of isogenies connecting E_1 and E_2. In schemes that do not use secret isogenies of relatively small degree (e.g., B-SIDH [6] or SÉTA [9]), the GPST approach is infeasible.

3 Computing isogenies using torsion information

In this section, we describe an algorithm to evaluate non-smooth degree isogenies; and an algorithm to compute a secret isogeny $\phi : E_1 \to E_2$ of degree N_1 between supersingular elliptic curves, provided that certain N_2-torsion images and the endomorphism rings of E_1 and E_2 are known.

3.1 Evaluating non-smooth degree isogenies

In this subsection, we provide an algorithm for the following problem.

Task 3.1. *Let E_1 and E_2 be two curves with given endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ respectively. Let I be an $\mathcal{O}_1$-left and $\mathcal{O}_2$-right ideal of norm N_1 and let $P \in E_1$. Evaluate $\phi_I(P)$, where ϕ_I is the isogeny corresponding to the ideal I.*

Remark 3.2. The isogeny ϕ_I corresponding to the left ideal I is only unique up to post-composition with isomorphisms. Here E_2 is a prescribed curve so one has only potential issues with automorphisms of E_2. The number of automorphisms of E_2 can be bounded by a constant (in most cases it is actually 2), so one has some slight amibguity in the end result of Task 3.1 which will eventually result in a constant overhead every time this subroutine is called.

To solve this task, we extend an algorithm due to Petit and Lauter [30, Algorithm 3] which evaluates endomorphisms. Note that a solution to Task 3.1 evaluates isogenies of non-smooth degree between curves with known endomorphism rings.

Petit–Lauter Algorithm [30, Alg. 3]: Let $(E_1, \mathcal{O}_1)$ denote a supersingular curve and its endomorphism ring, and let $w \in \mathcal{O}_1$. In order to evaluate the endomorphism $\phi_{\mathcal{O}_1 w}$ on a point $P \in E_1$, the algorithm by Petit and Lauter uses a curve $(E_0, \mathcal{O}_0)$ whose endomorphisms can be efficiently evaluated, e.g. the curve with j-invariant 1728 (see Example 2.1). The algorithm proceeds as follows.

Let $\{w_1, w_2, w_3, w_4\}$ be a basis of $\mathcal{O}_0$ and let $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ be the corresponding basis of $\mathrm{End}(E_0)$. The core idea of the algorithm is to use the KLPT algorithm to compute a powersmooth isogeny $\varphi : E_1 \to E_0$ of degree N.

Then, we have $N\mathcal{O}_1 \subset \mathcal{O}_0$ and thus $Nw \in \mathcal{O}_0$. For $w = \frac{a_1w_1+a_2w_2+a_3w_3+a_4w_4}{N}$ this implies

$$\phi_{w\mathcal{O}_1} = \varphi^{-1} \circ \frac{a_1\phi_1 + a_2\phi_2 + a_3\phi_3 + a_4\phi_4}{N} \circ \varphi,$$

where $\varphi^{-1} := \frac{1}{\deg \varphi}\widehat{\varphi}$. Since all the isogenies on the right-hand side can be evaluated efficiently, this allows to evaluate $\phi_{w\mathcal{O}_1}$.

Solving Task 3.1: Let $(E_2, \mathcal{O}_2)$ be a supersingular elliptic curve with its endomorphism ring, let I be an $\mathcal{O}_1$-left and $\mathcal{O}_2$-right ideal of non-smooth norm and let $P \in E_1$. We would like to evaluate the isogeny ϕ_I corresponding to the ideal I at the point P.

Using the KLPT algorithm, we compute an $\mathcal{O}_1$-right and $\mathcal{O}_2$-left ideal J whose smooth norm is coprime to that of I. Then, the ideal IJ represents an endomorphism $w \in \mathcal{O}_1$ of E_1. The element $w \in O_1$ can be recovered by computing the shortest vector in IJ. We obtain $IJ = w\mathcal{O}_1$ for some $w \in \mathcal{O}_1$. Using [30, Algorithm 3], we evaluate $Q = \phi_{w\mathcal{O}_1}(P)$, and compute $\phi_I(P) = \phi_J^{-1}(Q)$. We summarise the steps in Algorithm 1.

Algorithm 1: Evaluating non-smooth degree isogenies

Input: Elliptic curves E_1, E_2 with endomorphism rings $\mathcal{O}_1, \mathcal{O}_2$ and an $\mathcal{O}_1$-left and $\mathcal{O}_2$-right ideal I together with a point $P \in E_1$, an elliptic curve E_0 such that its endomorphism ring $\mathcal{O}_0$ is generated by endomorphisms $\phi_1, \phi_2, \phi_3, \phi_4$ that can be evaluated efficiently.

Output: $\phi_I(P)$.

1 Compute an $\mathcal{O}_1$-right and $\mathcal{O}_2$-left ideal J whose smooth norm is coprime to that of I using Wesolowski's algorithm [41] (or KLPT);
2 Compute an $\mathcal{O}_1$-left and $\mathcal{O}_0$-right ideal K of powersmooth norm N using Wesolowski's algorithm (or KLPT);
3 Set $IJ = w\mathcal{O}_1$ for some $w \in \mathcal{O}_1$ and find integers a_1, a_2, a_3 and a_4 such that $Nw = a_1w_1 + a_2w_2 + a_3w_3 + a_4w_4$;
4 Evaluate $Q = \phi_{IJ}(P) = \frac{\phi_K^{-1}\circ(a_1\phi_1+a_2\phi_2+a_3\phi_3+a_4\phi_4)\circ\phi_K(P)}{N}$ using [30, Alg. 3];
5 **return** $\phi_J^{-1}(Q)$

Lemma 3.3. *Assuming GRH, Algorithm 1 runs in polynomial time.*

Proof. The endomorphism rings of the curves E_0, E_1 and E_2 are known. For this case, Wesolowski gave a polynomial-time algorithm to compute a connecting smooth ideal in polynomial time assuming only GRH [41]. Previously, a similar (faster) polynomial-time algorithm, KLPT [21], was already known for this task, but it relies on heuristics. Thus, Steps 1 and 2 run in polynomial time.

The ideal I ($\mathcal{O}_1$-left and $\mathcal{O}_2$-right) and J ($\mathcal{O}_1$-right and $\mathcal{O}_2$-left) have coprime norms, hence the two-sided $\mathcal{O}_1$ ideal IJ corresponds to a non trivial endomorphism $w \in \mathcal{O}_1$ of E_1 that can be recovered by computing a Minkowski reduced basis of IJ. For lattices up to dimension 4, a Minkowski reduced basis can be computed in polynomial time [29]. The integers a_1, a_2, a_3 and a_4 are obtained by rewriting the quaternion Nw as an element of $\mathcal{O}_0$. Therefore, Step 3 runs in polynomial time. By hypothesis, the isogenies ϕ_1, ϕ_2, ϕ_3 and ϕ_4 can be evaluated efficiently. The ideals K and J have smooth norm, hence the isogenies ϕ_K, ϕ_K^{-1} and ϕ_J^{-1} have smooth degree and can also be evaluated efficiently. It follows that Step 4 and Step 5 run in polynomial time as well. □

3.2 Main algorithm

Next, we generalise Algorithm 2 of [15]. In [15], an isogeny ϕ between two curves E_1 and E_2 with known endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ is computed, if its degree is minimal (i.e., ϕ is the isogeny of smallest degree connecting E_1 and E_2). The algorithm in [15] applies to the SIDH setting where the degree of the secret isogenies are minimal with non-negligible probability (or otherwise at least of particularly small degree). Meanwhile, the torsion point information available in SIDH-like schemes is not used at all.

We will show in this section how the torsion point information in SIDH-like schemes can be exploited together with the knowledge of endomorphism rings to compute secret isogenies of arbitrary (larger but fixed) degree.

The strategy is as follows. Let $\phi : E_1 \to E_2$ be a secret isogeny, let P, Q be a basis of $E_1[N_2]$ and let $\phi(P)$, $\phi(Q)$ be the torsion information provided in SIDH-like schemes. Let $I(\mathcal{O}_1, \mathcal{O}_2)$ be a connecting ideal between the maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$. Instead of solving for a minimal norm element of the ideal $I(\mathcal{O}_1, \mathcal{O}_2)$ as in [15], we compute an LLL-reduced basis $\{\psi_1, \psi_2, \psi_3, \psi_4\}$ of I.

Using Algorithm 1, the isogenies ψ_i, $i = 1, \ldots, 4$, can be evaluated at the points P and Q. Next, we want to write ϕ in terms of our LLL-reduced basis, i.e. we want to find $(x_1, \ldots, x_4) \in \mathbb{Z}^4$ such that

$$\phi = x_1\psi_1 + x_2\psi_2 + x_3\psi_3 + x_4\psi_4, \tag{1}$$

Clearly, recovering x_i allows to compute the secret isogeny ϕ. Note that Equation 1 implies in particular

$$\sum_{i=1}^{4} x_i\psi_i(P) = \phi(P) \qquad \text{and} \qquad \sum_{i=1}^{4} x_i\psi_i(Q) = \phi(Q). \tag{2}$$

To compute x_1, x_2, x_3 and x_4, we first prove that a solution to Equation 2 is unique modulo N_2. Then, we use simple linear algebra methods to recover it.

Finally, we will show that knowing the x_i modulo N_2 is enough to recover them exactly (as integers).

Lemma 3.4. *Let E_1, E_2 be supersingular elliptic curves over $\mathbb{F}_{p^2}$ and let P, Q be a basis of $E_1[N_2]$. Let $\psi_1, \psi_2, \psi_3, \psi_4$ be a $\mathbb{Z}$-basis of $\mathrm{Hom}(E_1, E_2)$. The system of linear equations modulo N_2 corresponding to*

$$\sum_{i=1}^{4} x_i \psi_i(P) = \phi(P) \text{ and } \sum_{i=1}^{4} x_i \psi_i(Q) = \phi(Q)$$

has a unique solution $(x_1, x_2, x_3, x_4) \in (\mathbb{Z}/N_2\mathbb{Z})^4$.

Proof. Let P', Q' be a basis of $E_2[N_2]$. Every isogeny ϕ in $\mathrm{Hom}(E_1, E_2)$ can be identified with a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}/N_2\mathbb{Z})$ by writing its images on $E_1[N_2]$ as follows

$$\phi(P) = [a]P' + [c]Q', \quad \phi(Q) = [b]P' + [d]Q'.$$

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a matrix in $M_2(\mathbb{Z}/N_2\mathbb{Z})$. First, we prove that for any matrix A, there exists an isogeny $\phi \in \mathrm{Hom}(E_1, E_2)$ such that representation of ϕ is A.

Let $\psi : E_1 \to E_2$ be an isogeny such that the degree of ψ is coprime to N_2. Note that such an isogeny exists as the ℓ-isogeny graph is connected for any prime ℓ. Let M be the matrix corresponding to ψ. Since the degree of ψ is coprime to N_2, it corresponds to an invertible matrix in $M_2(\mathbb{Z}/N_2\mathbb{Z})$.

It is known (see [40, Theorem 42.1.9.]) that $\mathrm{End}(E_1)/N_2\,\mathrm{End}(E_1)$ is isomorphic to $M_2(\mathbb{Z}/N_2\mathbb{Z})$ (the injection is clear, surjectivity is the key result). Note that the isomorphism depends on a choice of basis of $E_1[N_2]$. Consider the isomorphism corresponding to the basis P, Q. Then, there exists an endomorphism $\theta \in \mathrm{End}(E_1)$ whose matrix representation is AM^{-1}. This implies that the matrix representation of $\phi = \theta \circ \psi$ is $AM^{-1}M = A$, i.e. there exists an isogeny from E_0 to E_1 that is represented by the matrix A.

Clearly, $\sum_{i=1}^{4} x_i \psi_i$ and $\sum_{i=1}^{4} y_i \psi_i$ are represented by the same matrix if $x_i \equiv y_i \pmod{N_2}$ for $i = 1, \ldots, 4$. Thus, there are at most $N_2^4 = |(\mathbb{Z}/N_2\mathbb{Z})^4|$ different matrices that one can obtain.

Now, the lemma follows by a simple counting argument. Since every matrix in $M_2(\mathbb{Z}/N_2\mathbb{Z})$ is represented for an isogeny, every matrix must uniquely correspond to a sum of the form $\sum_{i=1}^{4} x_i \psi_i$ modulo N_2. Consequently, if a matrix has two different representations of the form $\sum_{i=1}^{4} x_i \psi_i$, then they are the same modulo N_2 which finishes the proof. □

Remark 3.5. Essentially the main result of the proof is that $\mathrm{Hom}(E_1, E_2)$ modulo N_2 is isomorphic to $M_2(\mathbb{Z}/N_2\mathbb{Z})$ as a $\mathbb{Z}/N_2\mathbb{Z}$-module [37]. Informally, the key idea is that $\mathrm{Hom}(E_1, E_2)$ is a left ideal in $\mathrm{End}(E_1)$, hence it will be a left ideal in $M_2(\mathbb{Z}/N_2\mathbb{Z})$ modulo N_2. Since isogenies between E_1 and E_2 of degree coprime to N_2 exist, this left ideal will contain invertible matrices, hence it must be the entire matrix ring.

Now we provide details on how to recover x_1, x_2, x_3, x_4. Given $\psi_i(P)$, $\psi_i(Q)$ for $i = 1, 2, 3, 4$ and $\phi(P)$, $\phi(Q)$, where $\{\psi_1, \psi_2, \psi_3, \psi_3\}$ is the LLL-reduced basis of $\mathrm{Hom}(E_1, E_2)$, we would like to compute $(x_1, \cdots, x_4) \in (\mathbb{Z}/N_2\mathbb{Z})^4$ such that

$$\sum_{i=1}^{4}[x_i]\psi_i(P) = \phi(P) \qquad \text{and} \qquad \sum_{i=1}^{4}[x_i]\psi_i(Q) = \phi(Q).$$

Note that N_2 is a smooth integer and that $\phi(P)$ and $\phi(Q)$ form a basis of $E_2[N_2]$ as $\deg(\phi)$ and N_2 are coprime. For $i = 1, 2, 3, 4$, we can compute the integers $a_i, b_i, c_i, d_i \in \mathbb{Z}/N_2\mathbb{Z}$ such that $\psi_i(P) = [a_i]\phi(P) + [b_i]\phi(Q)$ and $\psi_i(Q) = [c_i]\phi(P) + [d_i]\phi(Q)$ by using the Weil pairing and solving discrete logarithms in a group of smooth order. Now, the integers $(x_1, \cdots, x_4) \in (\mathbb{Z}/N_2\mathbb{Z})^4$ satisfy

$$\phi(P) = \left[\sum_{i=1}^{4} x_i a_i\right]\phi(P) + \left[\sum_{i=1}^{4} x_i b_i\right]\phi(Q)$$

and

$$\phi(Q) = \left[\sum_{i=1}^{4} x_i c_i\right]\phi(P) + \left[\sum_{i=1}^{4} x_i d_i\right]\phi(Q).$$

We obtain

$$\begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} \cdot \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}.$$

By Lemma 3.4, there exists a unique solution $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix}$ to the previous equation. Hence the matrix

$$M := \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{pmatrix}$$

is invertible and the solution is given by $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 1 \end{pmatrix} \cdot M^{-1}$. The latter operation corresponds to adding the first and the fourth row of M^{-1}. We summarise this process in Algorithm 2.

Lemma 3.6. *Algorithm 2 is correct and runs in polynomial time provided that N_2 is smooth.*

Proof. Follows from the previous discussion. □

Lemma 3.7 gives a condition under which the solution computed in Algorithm 2 gives a solution to Equation 1.

Algorithm 2: Computing the linear system

Input: $\psi_i(P)$ and $\psi_i(Q)$ for $i = 1, \ldots, 4$, where ψ_i are a $\mathbb{Z}$-basis of $\mathrm{Hom}(E_1, E_2)$; $\phi(P)$ and $\phi(Q)$ of smooth order N_2.
Output: x_1, x_2, x_3, x_4 such that $\sum_{i=1}^{4}[x_i]\psi_i(P) = \phi(P)$, and $\sum_{i=1}^{4}[x_i]\psi_i(Q) = \phi(Q)$.

for $i = 1, \cdots, 4$ **do**
  Compute $a_i, b_i, c_i, d_i \in \mathbb{Z}/N_2\mathbb{Z}$ such that $\psi_i(P) = [a_i]\phi(P) + [b_i]\phi(Q)$ and $\psi_i(Q) = [c_i]\phi(P) + [d_i]\phi(Q)$;
Set M to be the 4×4 matrix whose rows are $\begin{pmatrix} a_i & b_i & c_i & d_i \end{pmatrix}$ for $i = 1, 2, 3, 4$;
Compute the inverse matrix M^{-1} of M;
Set $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 \end{pmatrix}$ to be the sum of the first and the fourth rows of M^{-1};
return x_1, x_2, x_3, x_4 *such that* $|x_i| < N_2/2$.

Lemma 3.7. *Let* $d := \min\{\deg(\varphi) \,|\, \varphi : E_1 \to E_2$ *is isogeny*$\}$. *If* $\frac{N_1}{N_2} < \frac{d}{16}$, *then given the solution* $x_1, \ldots, x_4$ *to the system of linear equations modulo* N_2 *returned by Algorithm 2, where* $\sum_{i=1}^{4}[x_i]\psi_i(P) = \phi(P)$, $\sum_{i=1}^{4}[x_i]\psi_i(Q) = \phi(Q)$, *we have* $\phi = \sum_{i=1}^{4}[x_i]\psi_i$ *in* $\mathrm{Hom}(E_1, E_2)$.

Proof. By Lemma 2.6, setting $\delta = 0.75$ and $n = 4$, we have that $\phi = \sum_{i=1}^{4}[\gamma_i]\psi_i$ where $|\gamma_i| \leq \frac{8\deg(\phi)}{\deg(\psi_i)} \leq \frac{8N_1}{d}$. It follows that $|\gamma_i| \leq \frac{8N_1}{d} < \frac{N_2}{2}$ since $\frac{N_1}{N_2} < \frac{d}{16}$ by hypothesis.

The solution (x_1, x_2, x_3, x_4) returned by Algorithm 2 satisfies $|x_i| < \frac{N_2}{2}$ for $i = 1, 2, 3, 4$. Moreover, by Lemma 3.4, this solution is unique modulo N_2. Thus, $\phi = \sum_{i=1}^{4}[x_i]\psi_i$ in $\mathrm{Hom}(E_1, E_2)$. □

The entire process of computing isogenies of a specific but arbitrary degree between two supersingular curves with known endomorphism ring is summarised in Algorithm 3.

Algorithm 3: Computing isogeny with torsion point information

Input: Supersingular elliptic curves E_1, E_2 with known endomorphism rings $\mathcal{O}_1, \mathcal{O}_2$ which are connected by an isogeny ϕ of degree N_1 and $\phi(P), \phi(Q)$, where P, Q are a basis of $E_1[N_2]$, such that $\frac{N_1}{N_2} < \frac{d}{16}$.
Output: ϕ.

Compute a basis of an $\mathcal{O}_1$-left and $\mathcal{O}_2$-right ideal I;
Compute an LLL-reduced basis $\psi_1, \psi_2, \psi_3, \psi_4$ of I;
Compute $\psi_i(P), \psi_i(Q)$ using Algorithm 1;
Use Algorithm 2 to solve for $|x_i| < N_2/2$ such that $\sum_{i=1}^{4}[x_i]\psi_i(P) = \phi(P)$, $\sum_{i=1}^{4}[x_i]\psi_i(Q) = \phi(Q)$;
Compute isogeny from the relation $\phi = \sum_{i=1}^{4}[x_i]\psi_i$;
return ϕ

Finally, we prove that Algorithm 3 succeeds in polynomial time.

Theorem 3.8. *Let* $d := \min\{\deg(\phi) \mid \phi : E_1 \to E_2$ *is isogeny*$\}$*. Assuming GRH, Algorithm 3 solves Problem 1.1 in polynomial time, whenever* $\frac{N_1}{N_2} < \frac{d}{16}$*.*

Proof. Correctness of the algorithm follows from Lemma 3.7 and the preceding discussion. We are left to show the polynomial running time. Step 1 could use the KLPT algorithm [21] or in fact the algorithm due to Kirschmer–Voight [20], as the connecting ideal does not need to have a smooth norm. This runs in polynomial time (to avoid heuristics we can also use the algorithm from [41]). Step 2 is the LLL lattice reduction algorithm which also runs in polynomial time. Step 3 and Step 4 run in polynomial time by Lemma 3.3 and Lemma 3.6, respectively. □

Remark 3.9. We could also have required the condition $\frac{N_1}{N_2} \leq \frac{d}{16}$ and in that case we get the condition that $|x_i| \leq N_2/2$. However, when N_2 is even and x_i is congruent to $N_2/2$, then the lift to the above range is not unique (as $-N_2/2$ and $N_2/2$ represent the same residue class). This is not an issue for Algorithm 3 as one will have multiple candidates (16 of them in the worst case) for ψ that can be tested. By looking at the degrees, the correct one can be chosen efficiently. More generally, one could relax the statement of Theorem 3.8 further by allowing non-unique lifts and adding an additional step to check for the correctness of solutions at the end of Algorithm 3.

Remark 3.10. As was shown in Lemma 3.7, Algorithm 3 requires an amount of torsion point information that depends on the degree d of the shortest isogeny between the supersingular elliptic curves E_1 and E_2.

For many applications of cryptographic interest balanced parameters are used where $N_1 \approx N_2$. Taking $\frac{N_1}{N_2} \approx 1$, the procedure above works whenever the two curves are not connected by an isogeny of degree smaller than 16. This can be checked easily with an exhaustive search.

Remark 3.11. Algorithm 3 does not use the fact that N_1 is smooth. If one wants to retrieve the secret isogeny as a rational map (as a composition of small degree maps), then clearly the smoothness of N_1 is still required. However, if one only wants to evaluate the secret isogeny at any point coprime to its degree (e.g. as in pSIDH [24]), then this can be accomplished by Algorithm 3 even if N_1 is not smooth.

3.3 Example

We will illustrate the attack with an example.

Consider the prime $p = 83701957499$, where we have $p + 1 = 2^2 \cdot 3^{14} \cdot 5^4 \cdot 7$. Let B be the quaternion algebra ramified at p and ∞ and generated over the rationals by i, j, k where $i^2 = -p$, $j^2 = -1$, and $k = ij$. Fix the finite field $\mathbb{F}_{p^2}$ where $\alpha^2 = -1$ generates $\mathbb{F}_{p^2}$ over $\mathbb{F}_p$.

Consider the elliptic curve given by $E_0 : y^2 = x^3 + x$ which has j-invariant 1728. The endomorphism ring of E_0 is generated by:

$$1, j, \frac{j + k}{2}, \frac{1 + i}{2}.$$

We let the secret isogeny be a 3^{14}-isogeny $\theta : E_0 \to E$. We use θ to recover the endomorphism ring of E which is generated by

$$\frac{5159993 + i + 10319986j + 11800766447346k}{9565938}, \frac{2i + 6291065j + 7411685041437k}{9565938}, \frac{3j + 196249k}{2}, 1594323k.$$

Note that in the real attack, we have made the assumption that $\mathrm{End}(E)$ is known, so we have only used the secret to calculate a known quantity.

Now, using the knowledge of both endomorphism rings, we are able to compute a connecting ideal between them and also compute the reduced basis of the ideal to be

$$\frac{227049 + i + 154612j}{2}, \frac{154612 - 227049j + k}{2}, \frac{121127 - 9i + 4995744j + 14k}{2}, \frac{4995744 - 14i - 121127j - 9k}{2}.$$

We can interpret these as endomorphisms and map the generators of the $E_0[5^4]$ through them.

We take the points

$$\begin{aligned} P_5 &= (75854242840\alpha + 62002351922, 51107649030\alpha + 19190692821), \\ Q_5 &= (17857458337\alpha + 504604508, 77775481527\alpha + 25718537048) \end{aligned}$$

to be the generators of $E_0[5^4]$.

In particular, by naming the reduced basis elements as $\psi'_1, \psi'_2, \psi'_3, \psi'_4$ respectively, we have that

$$\begin{aligned} \psi'_1(P_5) &= (9049577476\alpha + 26838535531, 9532248787\alpha + 18861270144)\,, \\ \psi'_1(Q_5) &= (14085392798\alpha + 75272963133, 35152660085\alpha + 3705843319)\,, \\ \psi'_2(P_5) &= (54148936824\alpha + 29574813, 27904476482\alpha + 79581351851)\,, \\ \psi'_2(Q_5) &= (6218706354\alpha + 14437916419, 19897519544\alpha + 26853032937)\,, \\ \psi'_3(P_5) &= (27253519435\alpha + 63921648196, 55371710596\alpha + 3587102479)\,, \\ \psi'_3(Q_5) &= (6221393886\alpha + 23453138168, 81414672111\alpha + 63571818133)\,, \\ \psi'_4(P_5) &= (20904892135\alpha + 45099774747, 32347928248\alpha + 14718113311)\,, \\ \psi'_4(Q_5) &= (16837240041\alpha + 11444980635, 5815630261\alpha + 82050564219)\,. \end{aligned}$$

Furthermore, we have the images of P_5 and Q_5 through the secret isogeny θ as given as part of the problem. Note that these ψ_i are not the same as the ones defined in the previous section as they are endomorphisms of E_0. However, they are just the original ψ_i composed with the isogeny between E_1 and E_0 coming from KLPT. We will denote the actual isogenies corresponding to them by ψ_i. They can be evaluated at P_5 and Q_5 by applying the connecting isogeny to them and multiplying it with the inverse of its degree modulo 5^4. These are points in E, and in particular, they are in the subgroup $E[5^4]$. This allows us to express them in terms of $\theta(P_5)$ and $\theta(Q_5)$ which we are given.

This results in the following 4×4 matrix

$$\begin{pmatrix} 222 & 128 & 484 & 474 \\ 311 & 363 & 337 & 12 \\ 184 & 477 & 307 & 574 \\ 344 & 566 & 191 & 132 \end{pmatrix}$$

whose first row represents the four coefficients that expresses $\psi_1(P_5)$ as a linear combination of $\theta(P_5)$ and $\theta(Q_5)$, and $\psi_1(Q_5)$ as a linear combination of $\theta(P_5)$ and $\theta(Q_5)$. For example,

$$\psi_2(Q_5) = [337]\theta(P_5) + [12]\theta(Q_5).$$

Inverting this matrix and summing the first and fourth rows allow us to recover the coefficients x_i's providing the expression of the secret isogeny as a linear combination of ψ_1, ψ_2, ψ_3 and ψ_4. The result of the computation is that

$$\theta = [14]\psi_1 + [9]\psi_2 + \psi_4.$$

One can check that this is correct without actually computing the ψ_i by computing that the degree of this linear combination is indeed 3^{14} (as the action on the 5^4-torsion is already correct).

Remark 3.12. As one can see in this example, the secret isogeny is not the isogeny between E_0 and E of smallest degree, hence the algorithm from [15] would not have been sufficient for finding θ. However, the secret isogeny in this setting is still the smallest degree isogeny with the given action on the N_2-torsion.

4 Efficacy of countermeasures to recent SIDH attacks

Several papers emerged recently that broke SIDH and SIDH-based schemes such as B-SIDH in classical polynomial time [3, 26, 32]. In this section, we will address the relevance of the previous sections and justify why the reduction is still important.

Firstly, observe that our reduction works in a more general context. Namely, [3] and [26] require the torsion point information is at least as big as the degree of the secret isogeny, i.e. $N_1 \approx N_2$. Robert's attack [32] only requires $N_1^2 > N_2$. In the case of B-SIDH this essentially matches our result. However, for the general SSI-T problem this is sometimes weaker than what we have. Namely, when $N_1 \ll p$ then we need less torsion-point information. For an example consider the case where $N_1 \approx p^{2/3}$. This is a case not covered by [15] and the polynomial attack by Robert requires that $N_2 \approx p^{1/3}$ [32]. However, our reduction still works whenever $N_2 \approx p^{1/6}$, which follows from Theorem 3.8 and the fact that the shortest isogeny between two supersingular elliptic curve has degree approximately $\sqrt{p}$.

The second remark concerns countermeasures. Since the attacks were published, two countermeasures have been proposed. In [27], Moriya proposes to mask the degree of the secret isogeny. This prevents all previous attacks. Yet, our attack still works in this case as only an upper bound on the degree is needed as we never use N_1 explicitly. A sufficient upper bound ($\sqrt{p}$ in SIDH and p in B-SIDH) is automatically provided to the attacker.

Another countermeasure proposed by Fouotsa [12] proposes to only reveal a secret multiple of the torsion-point images (coprime to the order of the torsion points) as this information is sufficient to compute the shared secret. To avoid being able to compute the secret multiple using pairings one has to use a prime p such that $p+1$ is a product of many small distinct primes. Assume we are not given exact torsion point images $\varphi(P_B)$ and $\varphi(Q_B)$, but their multiples $[\lambda]\varphi(P_B)$ and $[\lambda]\varphi(Q_B)$ instead (where λ is a secret integer). Then Task 1.1 becomes the following.

Task 4.1. *Let N_1, N_2 be coprime integers and let $\varphi : E_1 \to E_2$ be a secret isogeny of degree N_1 between two supersingular elliptic curves. Let P_B, Q_B be a basis of $E_1[N_2]$. Given $\mathrm{End}(E_1)$, $\mathrm{End}(E_2)$, $[\lambda]\varphi(P_B)$, and $[\lambda]\varphi(Q_B)$ for an unknown $\lambda \in \mathbb{Z}$ coprime to N_2, find an isogeny $\varphi' : E_1 \to E_2$ of degree N_1 such that $\varphi_{|E_1[N_2]} = \varphi'_{|E_1[N_2]}$.*

For the rest of this section, we will describe how our reduction can be extended to solve this task.

Using Algorithm 2 for this task mutatis mutandis, the resulting system of equations will have 5 variables and 4 equations instead. By Lemma 3.4 this equation has rank 4. Hence, there will be one degree of freedom and every solution lies on a line in $(\mathbb{Z}/N_2\mathbb{Z})^5$. Thus, there are too many solutions to try all of them. However, for slightly weaker bounds, we can still make our reduction work.

Theorem 4.2. *Let $d := \min\{\deg(\phi) \mid \phi : E_1 \to E_2 \text{ is isogeny}\}$. We can solve Task 4.1 in heuristic polynomial time, whenever $\frac{N_1}{d} < \frac{{N_2}^{3/4}}{8}$.*

Proof. As in the proof of Lemma 3.4, denote by $\{\psi_1, \psi_2, \psi_3, \psi_3\}$ an LLL reduced basis for $\mathrm{Hom}(E_1, E_2)$. Recall the inequality $\phi = \sum_{i=1}^{4} \gamma_i \psi_i$ where $|\gamma_i| \leq \frac{8\deg(\phi)}{\deg(\psi_i)} \leq \frac{8N_1}{d}$. For $\frac{N_1}{d} < \frac{{N_2}^{3/4}}{8}$ this implies $|\gamma_i| < {N_2}^{3/4}$. Thus, one is looking for a very special solution to the above homogeneous linear system. More precisely, the first 4 variables have to be smaller than ${N_2}^{3/4}$ and the last variable is smaller than N_2 (i.e., no condition is imposed on the last variable). This is an SIS-like lattice problem where the lattice constitutes of the integer solutions to this system of equations. The only difference is that one is not looking for a short vector in the Euclidean distance but for a short vector in a slightly different metric. The volume of the defined rectangle is N_2^4, i.e. the size of the lattice determinant. Thus heuristically, we expect there to be a unique lattice vector in this rectangle. This vector can be found in two different ways: either using a weighted inner product which puts large weights on the first 4 variables and very little weight on the last variable or by orthogonal projection to the vector $(0, 0, 0, 0, N_2)$ and using general lattice reduction in the projected lattice. Being left with a CVP problem in dimension 5, the problem can be solved efficiently. □

5 Relevance to isogeny-based cryptography

We use this section to summarise how Algorithm 3 impacts different isogeny-based constructions. Here we consider versions of SIDH and B-SIDH with the suggested countermeasures [12, 27].

First, we recall the current state-of-the-art regarding endomorphism ring computations as it is clearly the most time consuming part when attacking an isogeny-based cryptosystem using the reduction given by this paper.

Given a supersingular elliptic curve E defined over a finite field of characteristic p, the problem is to find $\mathrm{End}(E)$. The first algorithm to solve this is described in Kohel's thesis [22] and was later improved by Delfs–Galbraith [10] to a running time of $\tilde{O}(p^{1/2})$. The most recent algorithm is due to Eisenträger, Hallgren, Leonardi, Morrison, and Park [11] and runs in time $O(\log(p)^2 p^{1/2})$. The best known quantum algorithm is due to Biasse, Jao and Sankar [2] and has a running time of $\tilde{O}(p^{1/4})$.

For a long time, the isogeny-based community considered the meet in the middle attack (MiTM) [14] as best attack when addressing the security level of isogeny-based schemes. Meanwhile, this MiTM attack requires exponential storage, hence may be unrealistic. Recently, [1] and [5] considered the van Oorschot–Wiener (vOW) parallel collision finding algorithm [38] for the isogeny computation problem. The vOW collision search allows for a space-time trade-off in the generic MiTM, leading to a larger time complexity when limited storage is used.

Estimating the security level of isogeny-based schemes using vOW, suggests that one can reduce the size of parameters that where previously fixed considering the generic MiTM attack with unrealistic memory requirements. For an SIDH-like scheme in which the secret isogenies have degree roughly N, the scheme is secured against the MiTM attack by choosing $2^{2\lambda} < N$, where λ is the desired security level. When considering the vOW attack, N may be considerably smaller compared to $2^{2\lambda}$.

However, the attack where the endomorphism ring of curves is computed and then Algorithm 3 of this work is used to attack the secret isogeny has to be taken into account. Given the classical and quantum complexity $O(\log(p)^2 p^{1/2})$ and $\tilde{O}(p^{1/4})$ respectively, this implies that the parameter p must also satisfy $2^{2\lambda} < p$.

Applying our attack to SIDH instances has similar complexity as the attack by Galbraith, Petit, Shani and Ti [15]. Thus, it does not affect parameter choices in SIDH, where isogenies are of small degrees and pathfinding algorithms are more efficient.

However, our algorithm has bigger impact when isogeny degrees are larger relative to the size of the underlying finite field $\mathbb{F}_p$ since its complexity depends on p and not on N_1.

For B-SIDH, the proposed prime p is roughly $2^{2\lambda}$. Provided the new analysis of the vOW collision search attack in [25], one may be tempted to propose smaller B-SIDH primes in order to improve on B-SIDH's efficiency. However, doing so would make the scheme vulnerable to attacks that compute endomorphism rings and use the results of this paper. This is because p would be smaller than $2^{2\lambda}$.

Hence, one consequence of this paper is that the current choice of the parameter p in B-SIDH is tight. Furthermore, one can also interpret this result differently. Namely, any SIDH-like construction has to use parameters at least as large as B-SIDH, otherwise they become vulnerable. In other words, proposing schemes with longer isogeny walks than in B-SIDH does not provide any security benefit. This is not unexpected, as walks in B-SIDH have lengths which are comparable to the diameter of the supersingular isogeny graph.

Another interpretation of our result is that when torsion point images are provided, then the problem of finding one isogeny between two supersingular elliptic curves becomes equivalent to finding an isogeny of a specific degree for a wide range of parameters.

6 Conclusion

In this paper, we showed how to compute an isogeny of a specific degree between two supersingular elliptic curves, given their endomorphism rings and the images of some torsion points under the isogeny. This can be seen as an extension of an algorithm due to Galbraith, Petit, Shani and Ti [15] which did not use torsion point information but required the isogeny to be of small degree.

As a consequence, this paper gives an improved upper bound on the security of schemes like B-SIDH, SÉTA and SIDH variants instantiated with larger degree isogenies, by means of attacks that compute endomorphism rings of supersingular elliptic curves. In particular, our work provides a significant speed-up to existing quantum attacks on B-SIDH and it shows that the prime chosen in B-SIDH cannot be lowered for the targeted security levels. In the meantime certain attacks [3, 26, 32] broke SIDH, B-SIDH and SÉTA using the provided torsion point information and the degree of the secret isogeny. However, we show that our reduction still applies in presence of countermeasures that are aimed at thwarting these efficient attacks.

Acknowledgements We would like to thank Craig Costello and Christophe Petit for useful comments on a previous draft. We thank Alice Pellet–Mary for helpful discussions on CVP instances. Moreover, we thank the reviewers at PKC 2022 whose feedback helped improve the presentation of the paper. Péter Kutas and Simon-Philipp Merz were supported by EPSRC grants EP/S01361X/1 and EP/P009301/1 respectively. Further, Péter Kutas was supported by the Ministry of Innovation and Technology and the National Research, Development and Innovation Office within the Quantum Information National Laboratory of Hungary. Péter Kutas was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and by the ÚNKP-22-5 New National Excellence Program.

Bibliography

[1] Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, A. Menezes, and F. Rodríguez-Henríquez. On the cost of computing isogenies between supersingular elliptic curves. In *IACR Cryptol. ePrint Arch.*, 2018.

[2] Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *International Conference on Cryptology in India*, pages 428–442. Springer, 2014.

[3] Wouter Castryck and Thomas Decru. An efficient key recovery attack on sidh (preliminary version). *Cryptology ePrint Archive*, 2022.

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

[5] C. Costello, P. Longa, M. Naehrig, J. Renes, and Fernando Virdia. Improved classical cryptanalysis of sike in practice. In *Public Key Cryptography*, 2020.

[6] Craig Costello. B-SIDH: supersingular isogeny diffie-hellman using twisted torsion. In *Advances in Cryptology - ASIACRYPT 2020, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II*, pages 440–463, 2020.

[7] Jean-Marc Couveignes. Hard homogeneous spaces. *Preprint at https://eprint. iacr. org/2006/291*, 1999.

[8] Luca De Feo. Mathematics of isogeny based cryptography. *arXiv preprint arXiv:1711.04062*, 2017.

[9] Cyprien Delpech de Saint Guilhem, Péter Kutas, Christophe Petit, and Javier Silva. SéTA: Supersingular encryption from torsion attacks. *IACR Cryptol. ePrint Arch.*, 2019:1291, 2019.

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

[11] Kirsten Eisentraeger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs. *arXiv preprint arXiv:2004.11495*, 2020.

[12] Tako Boris Fouotsa. Sidh with masked torsion point images. *Cryptology ePrint Archive*, 2022.

[13] Tako Boris Fouotsa, Péter Kutas, Simon-Philipp Merz, and Yan Bo Ti. On the isogeny problem with torsion point information. In *IACR International Conference on Public-Key Cryptography*, pages 142–161. Springer, 2022.

[14] S. Galbraith. Constructing isogenies between elliptic curves over finite fields. *Lms Journal of Computation and Mathematics*, 2:118–138, 1999.

[15] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in Cryptology - ASIACRYPT 2016*, pages 63–91, 2016.

[16] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219, 1996.

[17] 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, and David Urbanik. SIKE: Supersingular isogeny key encapsulation. `http://sike.org/`, 2017.

[18] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *International Workshop on Post-Quantum Cryptography*, pages 19–34. Springer, 2011.

[19] Samuel Jaques and John M Schanck. Quantum cryptanalysis in the ram model: Claw-finding attacks on sike. In *Annual International Cryptology Conference*, pages 32–61. Springer, 2019.

[20] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM Journal on Computing*, 39(5):1714–1747, 2010.

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

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

[23] Arjen K. Lenstra, Hendrik Willem Lenstra, and László Lovász. Factoring polynomials with rational coefficients. *Mathematische annalen*, 261:515–534, 1982.

[24] Antonin Leroux. A new isogeny representation and applications to cryptography. *Cryptology ePrint Archive*, 2021.

[25] Patrick Longa, Wen Wang, and Jakub Szefer. The cost to break sike: A comparative hardware-based analysis with aes and sha-3. Cryptology ePrint Archive, Report 2020/1457, 2020. `https://eprint.iacr.org/2020/1457`.

[26] Luciano Maino and Chloe Martindale. An attack on sidh with arbitrary starting curve. *Cryptology ePrint Archive*, 2022.

[27] Tomoki Moriya. Masked-degree sidh. *Cryptology ePrint Archive*, 2022.

[28] National Institute for Standards and Technology (NIST). Post-quantum crypto standardization (2016), `https://csrc.nist.gov/projects/post-quantum-cryptography`.

[29] Phong Q. Nguyen and Damien Stehle. Low-dimensional lattice basis reduction revisited. In Duncan A. Buell, editor, *ANTS 2004*, pages 338–357, United States, 2004. Springer, Springer Nature.

[30] Christophe Petit and Kristin Lauter. Hard and easy problems for supersingular isogeny graphs. Cryptology ePrint Archive, Report 2017/962, 2017. `https://eprint.iacr.org/2017/962`.

[31] Arnold K. Pizer. Ramanujan graphs and hecke operators. *Bulletin of the American Mathematical Society*, 23(1):127–137, 1990.

[32] Damien Robert. Breaking sidh in polynomial time. *Cryptology ePrint Archive*, 2022.

[33] Alexander Rostovtsev and Anton Stolbunov. Public-key cryptosystem based on isogenies. *IACR Cryptology ePrint Archive*, 2006:145, 2006.

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

[35] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer Science & Business Media, 2009.

[36] Anton Stolbunov. Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Adv. Math. Commun.*, 4(2):215–235, 2010.

[37] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[38] Paul C Van Oorschot and Michael J Wiener. Parallel collision search with cryptanalytic applications. *Journal of cryptology*, 12(1):1–28, 1999.

[39] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273:305–347, 1971.

[40] John Voight. Quaternion algebras. *preprint*, 13:23–24, 2018.

[41] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. Cryptology ePrint Archive, Report 2021/919, 2021. `https://ia.cr/2021/919`.