On the Isogeny Problem with Torsion Point Information

Boris Fouotsa Tako[1], Péter Kutas[2], Simon-Philipp Merz[3]

[1] Università Degli Studi Roma Tre, Italy
[2] University of Birmingham, UK
[3] Royal Holloway, University of London, UK

Abstract. It is well known 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 et al. 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 that secret isogenies in SIDH are short, and thus it does not extend to other SIDH-type schemes where 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. Lifting the solution of this linear system yields the secret isogeny. As a consequence, we show that the choice of the prime p in B-SIDH is tight.

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 [14, 27]. 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 [23].

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 mention this area for cryptographic use in 1997 [6], and the area gained traction in the following decade with new developments such as collision-resistant hashing [3] and key exchange [26, 29] based on isogeny problems. After Jao and De Feo introduced supersingular isogeny Diffie-Hellman (SIDH) [16], a

predecessor of the isogeny-based submission to NIST's standardisation procedure SIKE [15], the area has enjoyed increasing popularity.

The central problem in isogeny-based cryptography is to find an isogeny $\varphi : E_1 \to E_2$, i.e. a morphism both in the sense of algebraic geometry and group theory, between two given supersingular elliptic curves defined over a finite field $\mathbb{F}_q$. The problem of computing an arbitrary isogeny between two supersingular elliptic curves and the problem of computing the endomorphism rings $\mathrm{End}(E_1)$ and $\mathrm{End}(E_2)$ are broadly equivalent [10, 19]. Yet, in the ordinary case it is usually much easier to determine $\mathrm{End}(E_i)$ of an arbitrary E_i than computing an isogeny between two arbitrary curves [19].

There are infinitely many isogenies $E_1 \to E_2$, but attacking isogeny-based primitives such as SIDH requires 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 [13] it is shown how to recover secret isogenies in the case of SIDH, exploiting the observation that secret isogenies in SIDH are of particularly small degree. In the case where the isogeny one wishes to recover is not of particularly small degree, as is the case in B-SIDH [5], SÉTA [8] or an instantiation of SIDH with secret isogenies of larger degree, this observation no longer holds and the algorithm due to Galbraith et al. no longer applies.

Our contributions. We provide a heuristic polynomial-time algorithm which recovers an isogeny between two supersingular elliptic curves of a specific degree, given their endomorphism rings and some 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, the algorithm solves the following problem, whenever $N_1 < dN_2/16$.

Task 1.1. *Let N_1, N_2 be two 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 $End(E_1)$, $End(E_2)$, $\varphi(P_B)$, and $\varphi(Q_B)$, find an isogeny $\varphi' : E_1 \to E_2$ of degree N_1 such that $\varphi_{|E_1[N_2]} = \varphi'_{|E_1[N_2]}$.*

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 and a basis of M can be computed using the KLPT algorithm [18]. 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 every i and we know $\phi(P_B)$ and $\phi(Q_B)$. Since $\phi = x_1\psi_1 + x_2\psi_2 + x_3\psi_3 + x_4\psi_4$ 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. If we choose ψ_i in a suitable fashion we can compute a unique solution for x_i modulo N_2. 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 unique solution for $x_i \in \mathbb{Z}$.

The contribution of this paper can be seen as an extension of the reduction in [18] which allows to compute isogenies of any (not necessarily small) degree, whenever the endomorphism rings are known and certain torsion point information is provided. Together with known results on the computation of

endomorphism rings, this work implies that one cannot lower the prime p in B-SIDH significantly while maintaining the same security level. However, current parameter sets are not threatened.

Outline. In Section 2, we recall some necessary mathematical background, details of the SIDH key exchange as well as some related work. In Section 3, we give an algorithm to evaluate non-smooth 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. Moreover, we discuss the impact of this work on isogeny-based cryptography before concluding the paper in Section 4.

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 [28] and De Feo [7], respectively. Furthermore, we briefly recall some consequences of the KLPT algorithm [18] and the LLL lattice reduction [20]. Moreover, we sketch a related algorithm due to Galbraith et al. [13] which computes an isogeny of specific degree between two supersingular elliptic curves with known endomorphism ring, if this degree 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 unique separable isogeny whose kernel is G. We denote the corresponding curve 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 [31].

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*. 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 (in which case 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 if and only if they share the same j-invariant.

Example 2.1. The supersingular elliptic curve $E_0 : y^2 = x^3 + x$ has j-invariant 1728 and it is well-known that $\mathrm{End}(E_0)$ is the $\mathbb{Z}$-module generated by $1, \iota, \frac{1+j}{2}$ and $\frac{\iota+\iota j}{2}$, where ι denotes E_0's non-trivial automorphism, $(x, y) \mapsto (-x, iy)$, and j 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 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 $2 \log p$. The presumed hardness of path-finding in this graph is the hardness assumption underlying isogeny-based cryptography.

2.2 SIDH and B-SIDH

We give a brief description of SIDH [16] and B-SIDH [5] 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. 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 curve $E_0/\langle G_A, G_B\rangle$. 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 maximize the efficiency of the scheme. However, choosing a prime of the form $N_1N_2f - 1$ implies that the curves E_0 and E_A are much closer than the diameter of the supersingular isogeny graph, i.e. E_0 and E_A are connected by a path that is shorter than one would expect for two 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 [5]. 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 $p + 1$ and $p - 1$) 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).
- Isogenies are apriori defined over $\mathbb{F}_{p^4}$ as opposed to $\mathbb{F}_{p^2}$.

Though in this version the curves E and E_A are no longer closer than expected in the isogeny graph, 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 enables us to compute the isogenies using only operations over $\mathbb{F}_{p^2}$. For more details we refer to [5].

2.3 KLPT and lattice reduction

In this subsection we recall some facts about the Kohel-Lauter-Petit-Tignol (KLPT) algorithm [18] and the Lenstra-Lenstra-Lovász (LLL) lattice reduction [20].

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 [18, Lemma 8], we have the following result.

Lemma 2.2. *Let $\mathcal{O}_1$ and $\mathcal{O}_2$ be maximal orders in $B_{p,\infty}$. Then the Eichler-order $\mathcal{O}_1 \cap \mathcal{O}_2$ 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 2.2 shows that one can compute a connecting ideal between two maximal orders efficiently. However, this ideal will not have smooth norm in general. In [18], 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 isogenies from E_1 to E_2 are left $\mathcal{O}_1$- and right $\mathcal{O}_2$-modules. In particular, they form a $\mathbb{Z}$-lattice of rank 4 [32, 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 2.3. *[32, 42.2.7] Let $Hom(E_2, E_1)$ 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 ϕ_I denote the corresponding isogeny. Then the map $\phi_I^* : Hom(E_1, E_2) \to I$, $\psi \mapsto \psi \circ \phi_I$ is an isomorphism of left $\mathcal{O}_1$-modules.*

Since the KLPT-algorithm computes a connecting ideal between two maximal orders, the lemma 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. We will show later in Algorithm 1 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 [20]. 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 2.4. *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 will use later 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 [20, Equation (1.6)] and [17, p.546].

Lemma 2.5. *Let L be a full 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*

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

2.4 GPST

In [13, §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). In this section, we summarize their results. Moreover, 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 respecitvely. Since E_1 and E_2 are supersingular curves, their endomorphism rings are maximal orders in the rational quaternion algebra $B_{p,\infty}$. By [18, Lemma 8], 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. Yet, 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.

The secret isogenies in SIDH are of degree approximately $\sqrt{p}$, but for a pair of random supersingular elliptic curves over $\mathbb{F}_{p^2}$ it is unlikely to be connected by an isogeny of degree significantly smaller than $\sqrt{p}$. In [13] the authors leverage this observation to recover the sought isogeny.

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 [18, 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 [13] 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. Not using secret isogenies of unexpectedly short degree as is the case in B-SIDH, SÉTA or if SIDH is instantiated with secret isogenies of larger degree, renders the GPST approach infeasible.

3 Computing isogenies using torsion information

In this section we describe an algorithm for evaluating 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 the certain torsion images are known. Finally, we discuss the relevance of the latter algorithm to isogeny-based cryptography.

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.*

We extend an algorithm due to Petit and Lauter [25, Algorithm 3] which evaluates endomorphisms to an algorithm that evaluates isogenies of non-smooth degree between curves with known endomorphism rings. Let $(E_1, \mathcal{O}_1)$ be a given supersingular curve and its endomorphism ring, and let $w \in \mathcal{O}_1$. In order to evaluate $\phi_{w\mathcal{O}_1}$ 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). Let $\{w_1, w_2, w_3, w_4\}$ be a basis of $\mathcal{O}_1$ and let $\{\phi_1, \phi_2, \phi_3, \phi_4\}$ be the corresponding basis of $\mathcal{O}_0$. The idea of [25, Algorithm 3] is to use the KLPT algorithm to compute a powersmooth isogeny $\varphi : E_1 \to E_0$ of degree N and exploit the fact that $N\mathcal{O}_1 \subset \mathcal{O}_0$ to have $Nw \in \mathcal{O}_0$. More concretely, if $w = \frac{a_1w_1+a_2w_2+a_3w_3+a_4w_4}{N}$, then $\phi_{w\mathcal{O}_1} = \varphi^{-1} \circ \frac{a_1\phi_1+a_2\phi_2+a_3\phi_3+a_4\phi_4}{N} \circ \varphi$, where $\varphi^{-1} := \frac{1}{\deg \varphi}\widehat{\varphi}$ can be evaluated efficiently.

Now, 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, $IJ = w\mathcal{O}_1$ for some $w \in \mathcal{O}_1$ corresponds to an endomorphism $w \in \mathcal{O}_1$ of E_1. Using [25, Algorithm 3], we evaluate $Q = \phi_{w\mathcal{O}_1}(P)$, and compute $\phi_I(P) = \phi_J^{-1}(Q)$. We summarize 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 KLPT algorithm;

2 Compute an $\mathcal{O}_1$-left and $\mathcal{O}_0$-right ideal K of powersmooth norm N using KLPT algorithm;

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 [25, Alg. 3];

5 **return** $\phi_J^{-1}(Q)$

Lemma 3.2. *Algorithm 1 runs heuristically in polynomial time.*

Proof. Since the endomorphism rings of the curves E_0, E_1 and E_2 are known, the calls of the KLPT algorithm in Step 1 and Step 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 [24]. 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. The isogenies ϕ_1, ϕ_2, ϕ_3 and ϕ_4 can be efficiently evaluated by hypothesis. The ideals K and J have smooth norm, hence the isogenies ϕ_K, ϕ_K^{-1} and ϕ_J^{-1} can also be evaluated efficiently. It follows that Step 5 and Step 6 run also in polynomial time. □

3.2 Main algorithm

Next we generalise Algorithm 2 of [13]. There, an isogeny ϕ between two curves E_1 and E_2 with known endomorphism rings $\mathcal{O}_1$ and $\mathcal{O}_2$ is computed, given that the degree of the isogeny ϕ is minimal (ϕ is the isogeny between E and E' of smallest degree). The algorithm in [13] applies to the SIDH setting where the degree of the secret isogenies are minimal with non negligible probability or at least particularly short. Meanwhile, the torsion point information $\phi(P)$, $\phi(Q)$ available in SIDH-like schemes is not used. We exploit this torsion point information to compute isogenies of larger degrees as well.

Instead of solving for a minimal norm element of the connecting ideal $I(\mathcal{O}_1, \mathcal{O}_2)$ as in [13], we determine an LLL-reduced basis $\{\psi_1, \psi_2, \psi_3, \psi_4\}$ of I. The isogenies ψ_i, $i = 1, \ldots, 4$, can be evaluated at P and Q using Algorithm 1. Write $\phi = x_1\psi_1 + x_2\psi_2 + x_3\psi_3 + x_4\psi_4$ in this basis, then $\sum_{i=1}^{4} x_i\psi_i(P) = \phi(P)$ and $\sum_{i=1}^{4} x_i\psi_i(Q) = \phi(Q)$. We solve the corresponding linear system to recover x_1, x_2, x_3 and x_4. If such a solution does not exist, we restart with another LLL-reduced basis. This process is summarised in Algorithm 2.

Algorithm 2: 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 $E_1[N_2]$.

Output: ϕ.

1 Using KLPT, compute a basis of an $\mathcal{O}_1$-left and $\mathcal{O}_2$-right ideal I ;
2 Compute an LLL-reduced basis $\psi_1, \psi_2, \psi_3, \psi_4$ of I;
3 Compute $\psi_i(P), \psi_i(Q)$ using Algorithm 1 ;
4 Solve the system of linear equations modulo N_2 corresponding to $\sum_{i=1}^{4} x_i\psi_i(P) = \phi(P)$, $\sum_{i=1}^{4} x_i\psi_i(Q) = \phi(Q)$;
5 **if** system has no unique solution **then**
6 Go to Step 2 and choose a different reduced basis;
7 **else**
8 Lift unique solution x_1, x_2, x_3, x_4 modulo N_2 to integers;
9 Compute isogeny from the relation $\phi = \sum_{i=1}^{4} x_i\psi_i$;
10 **return** ϕ

Lemma 3.3. *Let d be the lowest degree of all isogenies between E_1 and E_2. A solution $x_1, \ldots, x_4$ to the system of linear equations modulo N_2 in Step 4 of Algorithm 2 can be lifted uniquely to the integers, if $\frac{N_1}{N_2} < \frac{d}{16}$.*

Proof. A solution $x_1, \ldots, x_4$ satisfies $\phi = \sum_{i=1}^{4} x_i\psi_i$, where ψ_i is an LLL-reduced basis. By Lemma 2.5, we have $|x_i| \leq \frac{8\deg(\phi)}{\deg(\psi_i)}$ (for this choose $\delta = 0.75$ and $n = 4$). If $|x_i| < \frac{N_2}{2}$, then a solution modulo N_2 can clearly be lifted uniquely to the interval $[-\frac{N_2}{2}, \frac{N_2}{2}]$. Thus, it is sufficient to show that $|x_i| < \frac{N_2}{2}$. Since the degree of every isogeny connecting E_1 and E_2 is at least d, one has $|x_i| \leq \frac{8\deg(\phi)}{\deg(\psi_i)} \leq \frac{8N_1}{d}$. Finally, $\frac{8N_1}{d} < \frac{N_2}{2}$ follows by the condition on the size of N_1 and N_2. □

Finally, we prove that Algorithm 2 succeeds heuristically in polynomial time.

Theorem 3.4. *Let d be the lowest degree of all isogenies between E_1 and E_2. Algorithm 2 solves Problem 1.1 heuristically in polynomial time, if $\frac{N_1}{N_2} < \frac{d}{16}$.*

Proof. Correctness of the algorithm follows from Lemma 3.3 and the preceding discussion. We are left to show the polynomial running time. Step 1 uses the KLPT algorithm [18], which runs in heuristic polynomial time. Step 2 is the LLL lattice reduction algorithm which also runs in polynomial time and Step 3 runs in polynomial time by Lemma 3.2. Whenever the solution of the system of Step 4 is unique, it can be computed in polynomial time by treating it as a system of linear diophantine equations and applying [11]. .

What is left to show is that one does not have to jump from Step 4 back to Step 2 too often. The system of Step 4 has a unique solution if and only if the determinant is coprime to N_2. Heuristically, the probability of this is approximately $\frac{\phi(N_2)}{N_2}$, where ϕ is Euler's totient function. It is easy to see that this quantity is the largest for N_2 being a product of the first k primes p_i. In that case $\phi(N_2)/N_2 = \prod_{i=1}^{k}(1 - 1/p_i)$, which can be bounded below using the inequality between harmonic and geometric means.

$$\left(\frac{k}{k + \sum_{i=1}^{k} 1/(p_i - 1)}\right)^k < \prod_{i=1}^{k}(1 - 1/p_i)$$

By Mertens' theorem [22], we can approximate $\sum_{i=1}^{k} \frac{1}{p_i}$ by $\log\log k$.

Since $(1 - x/n)^n$ is roughly e^{-x}, we can approximate the lower bound by $(1/\log k)^{\frac{k+\log\log k}{k}} > \frac{1}{(\log k)^2}$. Thus, the expected number of iterations of Step 3 through 5 is polynomial in $\log k$. □

Remark 3.5. As shown in Lemma 3.3, Algorithm 2 requires an amount of torsion point information that depends on the shortest isogeny between E_1 and E_2. As discussed in [13], the shortest isogeny between two supersingular elliptic curves chosen uniformly at random is heuristically $O(\sqrt{p})$. In particular, Algorithm 2 requires only $\frac{N_1}{N_2} < \sqrt{p}/16$ in this case. Finally, if more torsion point information is given than required by the algorithm, one can use a smaller part of it to make Algorithm 2 more efficient. Note that the system of linear equations will then be more likely to have a unique solution (e.g., in B-SIDH one could omit all small prime factors of $p^2 - 1$).

3.3 Relevance to isogeny-based cryptography

We use this subsection to summarize how Algorithm 2 impacts different isogeny-based constructions.

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 an 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 [19] and was later improved by Delfs-Galbraith [9] to a running time of $\tilde{O}(p^{1/2})$. The most recent algorithm is due to Eisenträger et al. [10] which 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 $\tilde{O}(p^{1/4})$.

The isogeny-based community has for long considered the meet in the middle attack (MiTM) [12] 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 [4] considered the van Oorschot-Wiener (vOW) parallel collision finding algorithm [30] 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 this attack, suggests that one can reduce the size of parameters that where previously fixed considering the generic MiTM attack. For an SIDH-like scheme in which the secret isogenies have degree roughly N, the scheme is secured against the MiTM attack if $2^{2\lambda} < N$, where λ is the desired security level. When considering the vOW attack, N may be considerably smaller compared to $2^{2\lambda}$. See for instance a recent proposal for the reduction of parameters in SIKE by Longa et al. [21]. However, one also needs to take the attack into account where one computes the endomorphism ring of curves and then uses Algorithm 2 to attack the secret isogeny. 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 $2^{2\lambda} < p$.

For the current parameters of SIDH and SÉTA, the prime p is an order of magnitude larger than $2^{2\lambda}$. Therefore, these schemes are not impacted by the results of this paper. For B-SIDH, the proposed prime p is roughly $2^{2\lambda}$. Provided the new analysis of the vOW collision search attack in [21], 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 as p would be smaller than $2^{2\lambda}$. Hence, the current B-SIDH parameters are tight.

4 Conclusion

We showed how to compute an isogeny of a specific degree between two supersingular elliptic curves, given their endomorphism rings and certain torsion point information of the isogeny. This can be seen as an extension of an algorithm due to Galbraith et al. [13] which did not use torsion point information but required the isogeny to be of small degree.

As a consequence, this paper allows us to estimate the security of schemes like B-SIDH, SÉTA and SIDH instantiated with larger degree isogenies when considering an attack that computes endomorphism rings. We stress that this work does not allow to break any of the recommended parameter sets. However,

our work shows that the prime chosen in B-SIDH cannot be lowered for the given security levels.

Acknowledgements. We would like to thank Craig Costello for his useful comments on a previous draft. Péter Kutas and Simon-Philipp Merz were supported by EPSRC grants EP/S01361X/1 and EP/P009301/1 respectively.

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

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

[5] 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.

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

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

[8] 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.

[9] 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.

[10] 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.

[11] Michael A Frumkin. Polynomial time algorithms in the theory of linear diophantine equations. In *International Conference on Fundamentals of Computation Theory*, pages 386–392. Springer, 1977.

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

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] Hendrik W. Lenstra Jr. Integer programming with a fixed number of variables. *Math. Oper. Res.*, 8(4):538–548, 1983.

[18] 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.

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

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

[21] 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`.

[22] Franz Mertens. Ein beitrag zur analytischen zahlentheorie. *Journal für die reine und angewandte Mathematik*, 1874(78):46–62, 1874.

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

[24] 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.

[25] 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`.

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

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

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

[29] 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.

[30] Paul C Van Oorschot and Michael J Wiener. Parallel collision search with cryptanalytic applications. *Journal of cryptology*, 12(1):1–28, 1999.
[31] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris, Séries A*, 273:305–347, 1971.
[32] John Voight. Quaternion algebras. *preprint*, 13:23–24, 2018.