ON THE HARDNESS OF COMPUTING ENDOMORPHISM RINGS OF SUPERSINGULAR ELLIPTIC CURVES

KIRSTEN EISENTRÄGER, SEAN HALLGREN, AND TRAVIS MORRISON

Abstract. Cryptosystems based on supersingular isogenies have been proposed recently for use in post-quantum cryptography. Three problems have emerged related to their hardness: computing an isogeny between two curves, computing the endomorphism ring of a curve, and computing a maximal order associated to it. While some of these problems are believed to be polynomial-time equivalent based on heuristics, their relationship is still unknown. We give the first reduction between these problems, with the aid of one more problem which we call Action-on-ℓ-Torsion. We show that computing ℓ-power isogenies reduces to computing maximal orders and Action-on-ℓ-Torsion.

We also define the notion of a compact representation of an endomorphism, and use this to show that endomorphism rings always have polynomial representation size. We then reduce the endomorphism ring problem to computing maximal orders and Action-on-ℓ-Torsion, thus laying the foundation for analysis of the hardness of endomorphism ring computation. This identifies these last two problems as one possible way to attack some systems, such as hash functions based on the ℓ-isogeny graph of supersingular elliptic curves. This gives the potential to use algebraic tools in quaternion algebras to solve the problems. We also discuss how these reductions apply to attacks on a hash function of Charles, Goren, and Lauter.

1. Introduction

Cryptosystems based on the hardness of computing isogenies between elliptic curves have received a lot of attention recently because of their potential to be resistant against quantum computers. The first systems proposed were based on ordinary elliptic curves. Stolbunov [Sto10] proposed a new Diffie-Hellman type system, with the goal of obtaining a quantum resistant cryptographic protocol. This system was based on the difficulty of computing isogenies between ordinary elliptic curves. The fastest classical algorithm for solving this problem is exponential, but recently Childs, Jao, and Soukharev [CJS14] showed that on a quantum computer, the private keys in this system can be recovered in sub-exponential time.

The focus has shifted to systems based on supersingular isogenies, and that will also be the focus of this paper. Cryptographic applications based on the hardness of computing isogenies between supersingular elliptic curves were first given in [CGL09] which constructed a hash function from the ℓ-isogeny graph of supersingular elliptic curves. In the construction

The first author was partially supported by National Science Foundation awards DMS-1056703 and CNS-1617802, and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0541. The second author was partially supported by National Science Foundation awards CNS-1617802 and CCF-1618287, and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0541. The third author was partially supported by National Science Foundation grants DMS-1056703 and CNS-1617802.

of their hash function, finding preimages is connected to finding certain ℓ-power isogenies (for ℓ a small prime) between supersingular elliptic curves.

Proposals for post-quantum key-exchange, signature and encryption schemes based on computing isogenies of supersingular elliptic curves were given by De Feo, Jao and Plût in [DFJP14], and for these systems there are currently no subexponential quantum attacks. Another signature scheme based on endomorphism ring computation is given in [GPS16, Section 4], where the secret key is a maximal order isomorphic to the endomorphism ring of a supersingular elliptic curve. While the original scheme in [DFJP14] had to reveal auxiliary points, this is not necessary in this scheme. There are some partial attacks on cryptosystems based on supersingular isogenies described in [GPST16, Ti17, Pet17].

In the supersingular case three problems have emerged as potential computational hardness assumptions related to the above systems. The first is computing isogenies between supersingular elliptic curves, the second one is computing the endomorphism ring of a supersingular elliptic curve, and the third is to compute a maximal order isomorphic to the endomorphism ring of a supersingular elliptic curve. In order to develop confidence that these new systems are secure against quantum computers, it is important to understand these problems, their relationships, and how they relate to the cryptosystems. The natural way to do this is to give polynomial-time reductions between the problems when possible, and there are heuristics for doing this [Koh96],[KLPT14]. However, one quickly runs into problems when attempting to find efficient reductions. For example, the main parameter for these problems is a large prime p, and it is not obvious that the endomorphism ring of an elliptic curve even has a basis with a representation size that is polynomial in $\log(p)$. The same problem exists for maximal orders.

Deuring's correspondence between maximal orders in a quaternion algebra and supersingular elliptic curves over $\mathbb{F}_{p^2}$ gives a problem which is categorically equivalent to the ℓ-PowerIsogeny problem, which is: given two maximal orders, compute an ideal which "links" them and has norm ℓ^e for some e. This problem is solved in [KLPT14] with an algorithm which the authors claim to run heuristically in polynomial time in $\log(p)$. They do not give a precise complexity analysis, but if one assumes that outputs of some quadratic forms are approximately uniformly randomly distributed and independent of the splitting behavior of the numbers represented, one can show that it is a polynomial time probabilistic algorithm. There is an analysis of a related algorithm in [GPS16], but only the powersmooth case is analyzed, while we need to use the original prime-power algorithm. We need to use the algorithm of [KLPT14] in our reductions, but not in our analysis of the representation size of any of the objects.

The problems of computing isogenies, endomorphism rings, and maximal orders have been studied and it is believed that they, or some subset of them, are equivalent. In fact, many authors do not distinguish between computing a basis of maps generating $\mathrm{End}(E)$ and identifying a maximal order isomorphic to it, a distinction made in this paper. To make progress we identify a fourth problem, which links the maximal order problem and a very restricted case of the endomorphism ring problem, called Action-on-ℓ-Torsion. This problem takes a basis of the maximal order and asks how the associated endomorphism ring acts on a constant number of curve points. In Section 4, we give an efficient reduction from computing ℓ-power isogenies to computing a maximal order and to the Action-on-ℓ-Torsion problem. In the reduction we need both problems because we need information from the algebraic side, about the maximal order, and also a small piece of information from the geometric

side, namely knowing how certain endomorphisms act on the ℓ-torsion. This shows that to construct ℓ-power isogenies, knowing the whole endomorphism ring is not necessary when the maximal order is known and one has information about how certain endomorphisms act on a few points. It was known before how to get a connecting ideal I between two supersingular elliptic curves E and E'. However, this is only the beginning step in our reduction, and the hard part is to obtain from the ideal I the desired isogeny as a composition of rational maps of degree ℓ in polynomial time. This was not done before.

In the reduction we find the quaternion analogue of a factorization of an isogeny of degree ℓ^k, prove it exists, and show that it can be computed in polynomial time. For a reduction between these problems to be meaningful, we must first prove that every isomorphism class of maximal orders contains one representative which has a representation that is of polynomial size, which we do in Section 3. In any case, our reductions identify the subroutine of computing the ℓ-power ideal as the last remaining piece to have a complete polynomial-time reduction.

We next address the endomorphism ring problem in Section 5. As mentioned, it is not obvious how to define the problem in a way so that reductions can be polynomial-time. We start by defining the notion of a compact representation of an endomorphism, which has as a requirement that it has size polynomial in $O(\log p)$. We prove that every endomorphism ring has a basis specified by compact representations. We then show that the endomorphism problem reduces to computing a maximal order and the Action-on-ℓ-Torsion problem.

The analysis we give of the representation size of the basic objects used, along with the reductions, provide a firm ground for someone from quantum computing to look for quantum algorithms. In particular, while our results will show that breaking the systems reduces to a potentially harder problem, the new problem will be on the algebraic side of quaternion algebras. Finally in Section 6, we relate these problems to attacking the hash function of [CGL09].

Related Work. Computing the endomorphism ring of a supersingular elliptic curve was first studied by Kohel [Koh96, Theorem 75], who gave an approach for finding four linearly independent endomorphisms, generating a finite-index subring of $\mathrm{End}(E)$. The algorithm was based on finding loops in the ℓ-isogeny graph of supersingular elliptic curves, and the running time of the probabilistic algorithm is $O(p^{1+\varepsilon})$. Another problem that has been considered is that of listing all isomorphism classes of supersingular elliptic curves together with a description of the maximal order in a quaternion algebra that is isomorphic to $\mathrm{End}(E)$. This was done in [Cer04] and improved in [CG14, Section 5.2]. However, this approach is necessarily exponential in $\log p$ because there are roughly $\lfloor p/12 \rfloor$ isomorphism classes of supersingular elliptic curves.

The problem of computing isogenies between supersingular elliptic curves has also been studied, both in the classical setting [DG16, Section 4] where the complexity of the algorithm is $\tilde{O}(p^{1/2})$, and in the quantum setting [BJS14], where the complexity is $\tilde{O}(p^{1/4})$.

Several papers observe that computing isogenies between given supersingular elliptic curves and computing endomorphism ring the endomorphism ring of a supersingular elliptic curve are deeply connected, as was first shown by Kohel. Statements appear in several papers that heuristically, these two problems should be equivalent [GPS16], [KLPT14, Section 5], but no concrete statements or proofs are given.

Algorithms for related problems appear in other work. In [GPS16] there is an algorithm for finding powersmooth degree isogenies. In [LP17], algorithms for related problems are given.

2. Background on Elliptic Curves

2.1. Isogenies, Endomorphism Rings, and Supersingular Elliptic Curves.

2.1.1. *Elliptic Curves and Isogenies.* By an elliptic curve E over a field k of characteristic $p > 3$ we mean a curve with equation $E : y^2 = x^3 + Ax + B$ for some $A, B \in k$. The points of E are the points (x, y) satisfying the curve equation, together with the point at infinity. These points form an abelian group. The j-invariant of an elliptic curve given as above is $j(E) = \frac{256 \cdot 27 \cdot A^3}{4A^3 + 27B^2}$. Two elliptic curves E, E' defined over a field k have the same j-invariant if and only if they are isomorphic over the algebraic closure of k.

Let E_1 and E_2 be elliptic curves defined over a field k of positive characteristic p. An *isogeny* $\varphi : E_1 \to E_2$ defined over k is a non-constant rational map defined over k which is also a group homomorphism from $E_1(k)$ to $E_2(k)$ [Sil09, III.4]. The degree of an isogeny is its degree as a rational map. When the degree d of the isogeny φ is coprime to p, then φ is separable and the kernel of φ is a subgroup of the points on E_1 of size d. Every isogeny of degree n greater than one can be factored into a composition of isogenies of prime degrees such that the product of the degrees equals n. If $\psi : E_1 \to E_2$ is an isogeny of degree d, the *dual isogeny* of ψ is the unique isogeny $\widehat{\psi} : E_2 \to E_1$ satisfying $\psi\widehat{\psi} = [d]$, where $[d] : E_1 \to E_1$ is the multiplication-by-d map.

We can describe an isogeny via its kernel. Given an elliptic curve E and a finite subgroup H of E, there is, up to isomorphism a unique isogeny $\varphi : E \to E'$ having kernel H (see [Sil09, III.4.12]). Hence we can describe an isogeny of E to some other elliptic curve by giving its kernel. We can compute equations for the isogeny from its kernel by using Vélu's formula [Vél71].

2.1.2. *Endomorphisms and Supersingular versus Ordinary Curves.* An isogeny of an elliptic curve E to itself is called an endomorphism of E. If E is defined over some finite field $\mathbb{F}_q$, then an endomorphism of E will be defined over a finite extension of $\mathbb{F}_q$. The set of endomorphisms of E defined over $\overline{\mathbb{F}_q}$ together with the zero map form a ring under the operations addition and composition. It is called the endomorphism ring of E, and is denoted by $\mathrm{End}(E)$. When E is defined over a finite field, then $\mathrm{End}(E)$ is isomorphic either to an order in a quadratic imaginary field or to an order in a quaternion algebra. In the first case we call E an *ordinary elliptic curve*. An elliptic curve whose endomorphism is isomorphic to an order in a quaternion algebra is called a *supersingular elliptic curve*. Every supersingular elliptic curve over a field of characteristic p has a model that is defined over $\mathbb{F}_{p^2}$ because the j-invariant of such a curve is in $\mathbb{F}_{p^2}$.

2.1.3. *ℓ-power Isogenies between Supersingular Elliptic Curves.* Let E, E' be two supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. It is a fact that for each prime $\ell \neq p$, E and E' are connected by a chain of isogenies of degree ℓ [Mes86]. By [Koh96, Theorem79], E and E' can be connected by m isogenies of degree ℓ, where $m = O(\log p)$. So any two supersingular elliptic curves can be connected by an isogeny of degree ℓ^m with $m = O(\log p)$. If ℓ is a fixed prime $< \log p$, then any ℓ-isogeny in the chain above can either be specified by rational maps or by giving the kernel of the isogeny, and both of these representations will have polynomial

size. By Vélu's formula, and since $\ell < \log p$, there is an efficient way to go back and forth between these two representations.

2.2. Quaternion Algebras, $B_{p,\infty}$ and the Deuring Correspondence.

2.2.1. *Quaternion Algebras.* For $a, b \in \mathbb{Q}^\times$, let $H(a,b)$ denote the quaternion algebra over $\mathbb{Q}$ with basis $1, i, j, ij$ such that $i^2 = a$, $j^2 = b$ and $ij = -ji$. That is,

$$H(a,b) = \mathbb{Q} + \mathbb{Q}\,i + \mathbb{Q}\,j + \mathbb{Q}\,ij.$$

It is a fact that any quaternion algebra over $\mathbb{Q}$ can be written in this form. Now let $B_{p,\infty}$ be the unique quaternion algebra over $\mathbb{Q}$ that is ramified exactly at p and ∞. Then $B_{p,\infty}$ is a definite quaternion algebra, so $B_{p,\infty} = H(a,b)$ for some $a, b \in \mathbb{Q}^\times$, and one can show a and b can be chosen to be negative integers. For example, when $p \equiv 3 \pmod 4$, then $B_{p,\infty} = H(-p,-1)$.

There is a *canonical involution* on $B_{p,\infty}$ which sends an element $\alpha = a_1 + a_2 i + a_3 j + a_4 ij$ to $\overline{\alpha} := a_1 - a_2 i - a_3 j - a_4 ij$. Define the *reduced trace* of an element α as above to be

$$\mathrm{Trd}(\alpha) = \alpha + \overline{\alpha} = 2a_1,$$

and the *reduced norm* to be

$$\mathrm{Nrd}(\alpha) = \alpha\overline{\alpha} = a_1^2 - aa_2^2 - ba_3^2 + aba_4^2.$$

We say that Λ is a *lattice* in $B_{p,\infty}$ if $\Lambda = \mathbb{Z}x_1 + \cdots + \mathbb{Z}x_4$ and the elements $x_1, \ldots, x_4$ are a vector space basis for $B_{p,\infty}$.

If $I \subseteq B_{p,\infty}$ is a lattice, the reduced norm of I, $\mathrm{Nrd}(I)$, is the positive generator of the fractional $\mathbb{Z}$-ideal generated by $\{\mathrm{Nrd}(\alpha) : \alpha \in I\}$. The quaternion algebra $B_{p,\infty}$ is an inner product space with respect to the bilinear form

$$\langle x, y \rangle = \frac{\mathrm{Nrd}(x+y) - \mathrm{Nrd}(x) - \mathrm{Nrd}(y)}{2}.$$

The basis $\{1, i, j, ij\}$ is an orthogonal basis with respect to this inner product.

2.2.2. *Orders in $B_{p,\infty}$ and Representation of Elements in $B_{p,\infty}$.* A subset $I \subseteq B_{p,\infty}$ is a *lattice* if I is finitely generated as a $\mathbb{Z}$-module and $I \otimes \mathbb{Q} \simeq B_{p,\infty}$. An *order* $\mathcal{O}$ of $B_{p,\infty}$ is a subring of $B_{p,\infty}$ which is also a lattice, and if $\mathcal{O}$ is not properly contained in any other order, we call it a *maximal order*. Define

$$\mathcal{O}_R(I) := \{x \in B_{p,\infty} : Ix \subseteq I\}$$

to be the *right order of the lattice* I, and we similarly define its left order $\mathcal{O}_L(I)$. If $\mathcal{O}$ is a maximal order in $B_{p,\infty}$ and $I \subseteq \mathcal{O}$ is a left ideal of $\mathcal{O}$, then $\mathcal{O}_R(I)$ is also a maximal order. Given any two maximal orders $\mathcal{O}, \mathcal{O}'$, there is a lattice $I \subseteq B_{p,\infty}$ such that $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I) = \mathcal{O}'$; we say that I connects $\mathcal{O}$ and $\mathcal{O}'$.

An element $\beta \in B_{p,\infty}$ is represented as a coefficient vector (a_1, a_2, a_3, a_4) in $\mathbb{Q}^4$ such that $\beta = a_1 + a_2 i + a_3 j + a_4 ij$ in terms of the basis $\{1, i, j, ij\}$ for $B_{p,\infty}$. This will be used for specifying basis elements of maximal orders $\mathcal{O}$ and elements of left ideals I of $\mathcal{O}$.

2.2.3. *The Deuring Correspondence and Describing Isogenies via Kernel Ideals.* For a detailed overview of the information in this section, see Chapter 42 in [Voi]. Let E be a supersingular elliptic curve defined over $\mathbb{F}_{p^2}$. In [Deu41] Deuring proved that the endomorphism ring of E is isomorphic to a maximal order in $B_{p,\infty}$. Under this isomorphism, degrees and traces of endomorphisms correspond to norms and traces of quaternions.

Fix E, a supersingular elliptic curve over $\mathbb{F}_{p^2}$. We can associate to each pair (E', ϕ) with ϕ an isogeny $E \to E'$ of degree n a left $\mathrm{End}(E)$-ideal $I = \mathrm{Hom}(E', E)\phi$ of norm n, and it was shown in [Koh96, Section 5.3] that every left $\mathrm{End}(E)$-ideal arises in this way. We now describe how to construct an isogeny from a left $\mathrm{End}(E)$-ideal.

Let I be a nonzero integral left ideal of $\mathrm{End}(E)$. Define $E[I]$ to be the scheme-theoretic intersection

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

Thus to each left ideal I of $\mathrm{End}(E)$ there is an associated isogeny $\phi_I : E \to E/E[I]$. If $\mathrm{Nrd}(I)$ is coprime to p, then

$$E[I] = \{P \in E(\overline{\mathbb{F}}_{p^2}) : \alpha(P) = 0 \quad \forall \alpha \in I\}.$$

3. Efficient Computations with Maximal Orders and Their Ideals

The main problem we consider in this paper is computing a maximal order associated with an elliptic curve E. In the following sections will show that computing isogenies and computing endomorphisms reduces to computing maximal orders, together with a problem about ℓ-torsion action. In this section we define the maximal order problem and show that maximal orders have polynomial-representation size, so that the reductions are meaningful. We will also show that the representation size of ideals inside these orders is related to their norms. Maximal orders are inside the algebra $B_{p,\infty}$, so we start with that.

Let p be a prime. In Proposition 5.1 of [Piz80] it is shown that $B_{p,\infty} = H(-1,-1)$ if $p = 2$, $B_{p,\infty} = H(-1,-p)$ if $p \equiv 3 \pmod 4$, $B_{p,\infty} = H(-2,-p)$ if $p \equiv 5 \pmod 8$, and $B_{p,\infty} = H(-q,-p)$ if $p \equiv 1 \pmod 8$, where $q \equiv 3 \pmod 4$ and p is not a square modulo q. In the last case, assuming GRH, such a prime q exists where $q = O(\log(p)^2)$; see [Ank52].

So given p, we choose a and b as above (depending on the congruence class of p) such that $B_{p,\infty} = H(a,b)$. We obtain a basis $1, i, j, ij$ for $B_{p,\infty}$ such that $i^2 = a$ and $j^2 = b$. We refer to this as the *standard basis* of $B_{p,\infty}$. As stated in Section 2.2.2, we represent elements of $B_{p,\infty}$ as their coefficient vectors in $\mathbb{Q}^4$ with respect to the standard basis.

Problem 1 (MaxOrder)**.** *Given p, the standard basis for $B_{p,\infty}$, and a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, output vectors β_1, β_2, β_3, $\beta_4 \in B_{p,\infty}$ that form a $\mathbb{Z}$-basis of a maximal order $\mathcal{O}$ in $B_{p,\infty}$ such that $\mathrm{End}(E) \cong \mathcal{O}$. In addition, the output basis is required to have representation size polynomial in $\log p$.*

To reduce problems to this problem in polynomial time, one requirement is that every maximal order has a basis with representation size that is polynomial in $\log(p)$. Since a prime p is given, and E is given as $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{p^2}$, the input size for this problem is $O(\log p)$.

To show that every maximal order has a polynomial representation size, we first show this is true for a special maximal order $\mathcal{O}_0$ and then express all other classes of maximal orders as right orders $\mathcal{O}_R(I)$ for I a left ideal class of $\mathcal{O}_0$. Since every left ideal class of $\mathcal{O}_0$ contains

an ideal whose reduced norm is $O(p^2)$, it will follow that in each conjugacy class of maximal orders, there is one with polynomial representation size.

Lemma 3.1. *Given a prime p and the standard basis for $B_{p,\infty}$ there is a maximal order $\mathcal{O}_0 \subseteq B_{p,\infty}$ containing the order generated by $\langle 1, i, j, ij\rangle$. The maximal order $\mathcal{O}_0$ has a basis of size polynomial in* $\log(p)$.

Proof. Proposition 5.2 of [Piz80] gives a basis $\{b_1, b_2, b_3, b_4\}$ for a maximal order $\mathcal{O}_0$ inside $B_{p,\infty}$ that contains the order $\langle 1, i, j, ij\rangle$. Specifically, it is shown that the coefficients of each b_k in terms of the standard basis are bounded as follows. When $p = 2$ or $p \equiv 3 \pmod 4$ or $5 \pmod 8$, the numerators are at most 2 and the denominators are either 2 or 4. If $p \equiv 1 \pmod 8$, then the numerators and denominators are at most q. □

For the remainder of this section, fix such an order $\mathcal{O}_0$ together with the small basis $\{b_1, \ldots, b_4\}$ as in Lemma 3.1. We will now show that ideals of $\mathcal{O}_0$ of norm N have representations of size polynomial in $\log(N)$ in terms of the basis $\{b_1, \ldots, b_4\}$.

Lemma 3.2. *Let I be a left ideal of $\mathcal{O}_0$. Then there is a $\mathbb{Z}$-basis $\langle \alpha_1, \ldots, \alpha_4\rangle$ of I, consisting of elements $\alpha_i \in \mathcal{O}_0$, such that the coefficients of the α_i expressed, in terms of the basis $\{b_1, b_2, b_3, b_4\}$ of $\mathcal{O}_0$, are bounded by* $\mathrm{Nrd}(I)^2$.

Proof. Let $\{\gamma_1, \ldots, \gamma_4\}$ be a $\mathbb{Z}$-basis of I and write γ_i as $\gamma_i = \sum_j a_{ij} b_j$. Let $A = (a_{ij})$ be the matrix whose rows are the coefficients of γ_i. Let $H = UA$ where H is the (row-)Hermite normal form of A and $U \in \mathrm{SL}_4(\mathbb{Z})$. Then the rows of H also generate I as a $\mathbb{Z}$-basis, H is upper triangular, $0 < h_{ii}$, and $h_{ij} < h_{jj}$ for $i < j$. We have $\mathrm{Nrd}(I)^2 = \det(A) = \prod h_{ii}$ and hence all $h_{ij} < \mathrm{Nrd}(I)^2$. This gives us the desired basis $\alpha_1, \ldots, \alpha_4$. □

We will now prove that every conjugacy class of maximal orders has a representative whose basis has representation size $O(\log(p))$ when written in terms of the standard basis $1, i, j, ij$ for $B_{p,\infty}$.

For this, we will show that the reduced norm Nrd is the Euclidean norm on $B_{p,\infty} = H(-q, -p)$ considered as a lattice in $\mathbb{R}^4$. (Here $q = 1, 2$ or a prime $\equiv 3 \pmod 4$ that is not a square modulo p, depending on the congruence class of p.) We can view orders $\mathcal{O}$ in $B_{p,\infty}$ as lattices in $\mathbb{R}^4$, and we will relate the covolume of a lattice to its discriminant. This is similar to the number field case. Together with Minkowski's Theorem, this will give us the desired result.

Note that $B_{p,\infty} \otimes \mathbb{R}$ is isomorphic to $\mathbb{H}$, the Hamiltonians. Let $1, i', j', i'j'$ be the basis of $\mathbb{H}$ with $i'^2 = j'^2 = -1$. Let

$$f : B_{p,\infty} \otimes \mathbb{R} \xrightarrow{\sim} \mathbb{H},$$

and let the isomorphism be given by $i \mapsto \sqrt{q}i'$, $j \mapsto \sqrt{p}j'$. Then the norm on $\mathbb{H}$, which is the (square of) the standard Euclidean norm on $\mathbb{R}^4$, is just the reduced norm on the image of $B_{p,\infty}$ in $\mathbb{H}$ under the isomorphism f. Let $\Lambda \subseteq \mathbb{R}^n$ be a lattice. Define its *covolume*, denoted $\mathrm{Covol}(\Lambda)$, to be $\sqrt{\det(L^T L)}$ for any matrix L consisting of a basis for Λ. If $\mathcal{O} \subseteq B_{p,\infty}$ is a lattice, define its covolume to be $\mathrm{Covol}(f(\mathcal{O}))$.

If a lattice $\mathcal{O} \subseteq B_{p,\infty}$ has generators $\beta_1, \ldots, \beta_4$, its *discriminant*, denoted $\mathrm{Disc}(\mathcal{O})$, is $\det((\mathrm{Trd}(\beta_i \overline{\beta_j})))$. If a lattice $\mathcal{O}$ is a maximal order in $B_{p,\infty}$, then $\mathrm{Disc}(\mathcal{O}) = p^2$.

Proposition 3.3. *Let $\mathcal{O}$ be a lattice in $B_{p,\infty}$. Then* $\mathrm{Covol}(\mathcal{O})^2 = \frac{1}{16}\mathrm{Disc}(\mathcal{O})$.

Proof. First, we claim that if $x, y \in B_{p,\infty}$, then $f(x) \cdot f(y) = \frac{1}{2}\operatorname{Trd}(x\overline{y})$. Here $\cdot$ means the dot product in $\mathbb{R}^4$. Indeed, writing $x = x_0 + x_1 i + x_2 j + x_3 ij$, $y = y_0 + y_1 i + y_2 j + y_3 ij$, we have

$$\begin{aligned} f(x) \cdot f(y) =& (x_0 + x_1\sqrt{q}i' + x_2\sqrt{p}j' + x_3\sqrt{qp}i'j') \cdot \\ & (y_0 + y_1\sqrt{q}i' + y_2\sqrt{p}j' + y_3\sqrt{qp}i'j') \\ =& x_0y_0 + qx_1y_1 + px_2y_2 + qpx_3y_3 \\ =& \frac{1}{2}\operatorname{Trd}(x\overline{y}) \end{aligned}$$

From this, the result follows: let $\beta_1, \ldots, \beta_4$ be a basis of $\mathcal{O}$, let M be the matrix with ith column $f(\beta_i)$. Then

$$\begin{aligned} \operatorname{Covol}(\mathcal{O}) &:= \det(M^T M)^{1/2} \\ &= \det((f(\beta_i) \cdot f(\beta_j))_{i,j})^{1/2} \\ &= \det(\frac{1}{2}(\operatorname{Trd}(\beta_i\overline{\beta_j})))^{1/2} \\ &= \frac{1}{4}\det(\operatorname{Trd}(\beta_i\overline{\beta_j}))^{1/2} \\ &= \frac{1}{4}\operatorname{Disc}(\mathcal{O})^{1/2}. \end{aligned}$$

□

We need the notion of a Minkowski-reduced basis of a lattice. A basis $\{v_1, \ldots, v_n\}$ of a lattice $\Lambda \subseteq \mathbb{R}^n$ is *Minkowski-reduced* if for $1 \leq k \leq n$,

$$||v_k||_2 \leq \sum_{i=1}^{n} x_i ||v_i||_2,$$

whenever $x_1, \ldots, x_n$ are coprime integers. Here $||\cdot||_2$ denotes the Euclidean norm. Given a lattice Λ in $\mathbb{R}^n$, define the *ith successive minimum of* Λ, $\lambda_i(\Lambda)$, to be the smallest nonnegative, real number r such that there are i linearly independent lattice vectors of Λ contained in the closed ball of radius r centered at the origin. So $\lambda_1(\Lambda)$ is the length of a shortest nonzero vector of Λ. For $n \leq 4$, there is a basis $v_1, \ldots, v_n$ of Λ such that $||v_i||_2 = \lambda_i(\Lambda)$; see [NS09]. Such a basis is Minkowski-reduced. When we refer to a Minkowski-reduced basis, we will always assume we choose such a basis.

Theorem 3.4 (Minkowski's second theorem)**.** *Let V denote the volume of the n-dimensional unit ball of $\mathbb{R}^n$. Then*

$$\frac{2^n}{n!}\frac{\operatorname{Covol}(\Lambda)}{V} \leq \prod_{i=1}^{n} \lambda_i(\Lambda) \leq \frac{2^n}{V}\operatorname{Covol}(\Lambda).$$

Corollary 3.5. *Let p be a prime, and let $\mathcal{O}_0$ be the maximal order of $B_{p,\infty}$ as above. Let $I \subseteq \mathcal{O}_0$ be a left-ideal and let $\mathcal{O} := \mathcal{O}_R(I)$. Let $\alpha_1, \ldots, \alpha_4$ be a basis of $\mathcal{O}$ such that $||\alpha_i||_2 = \lambda_i(\mathcal{O})$ for $i = 1, \ldots, 4$. Then*

$$\prod_{i=1}^{4} \operatorname{Nrd}(\alpha_i) \leq \operatorname{Disc}(\mathcal{O}) = p^2.$$

Proof. We use Minkowski's second theorem applied to $\mathcal{O}$, and the fact that by Proposition 3.3, $\mathrm{Covol}(\mathcal{O})^2 = \mathrm{Disc}(\mathcal{O})/16$. These two facts, together with $\mathrm{Nrd}(\alpha) = ||f(\alpha)||_2^2$ give us that

$$\prod \mathrm{Nrd}(\alpha_i) = \prod \lambda_i(\mathcal{O})^2 \leq \frac{16}{\pi^4/4} \mathrm{Disc}(\mathcal{O}) \leq p^2.$$

□

Now we prove the main theorem on representation sizes of maximal orders:

Theorem 3.6. *Every conjugacy class of maximal orders in $B_{p,\infty}$ has a $\mathbb{Z}$-basis $x_1, \ldots, x_4$ with $\mathrm{Nrd}(x_i) \in O(p^2)$. If we express x_r (for $1 \leq r \leq 4$) as a coefficient vector in terms of $1, i, j, ij$, then the rational numbers appearing have numerators and denominators whose representation size are polynomial in $\log(p)$.*

Proof. The map $[I] \to [\mathcal{O}_R(I)]$ is a surjection from left-ideal classes of $\mathcal{O}_0$ to isomorphism classes of maximal orders of $B_{p,\infty}$; see [Gro87], page 116. Every left ideal class of $\mathcal{O}_0$ contains an ideal I with $\mathrm{Nrd}(I) \in O(p^2)$; see [Vig80, Proposition 17.5.6]. Set $\mathcal{O} = \mathcal{O}_R(I)$ and let $\langle 1, x_2, x_3, x_4 \rangle$ be a Minkowski-reduced $\mathbb{Z}$-basis of $\mathcal{O}$. By Corollary 3.5, $\mathrm{Nrd}(x_i) \leq p^2$, since each x_i is integral. Since $\mathcal{O} = \mathcal{O}_R(I)$, it follows that $x_i \,\mathrm{Nrd}(I) \in I$. This implies that if we express x_i as a $\mathbb{Q}$-linear combination of the elements $1, i, j, ij$, then the denominators of the coefficients are divisors of $\mathrm{Nrd}(I) \cdot 4q$ where $q = \mathrm{Nrd}(j)$. The numerator of each coefficient is then bounded by $8pq \,\mathrm{Nrd}(I)$: indeed, if a/b is a coefficient of x_r, $(1 \leq r \leq 4)$, then $(a/b)^2 \leq \mathrm{Nrd}(x_r) \leq p^2$. Then

$$|a| \leq pb \leq 4pq \,\mathrm{Nrd}(I).$$

□

4. ℓ-PowerIsogeny Reduces to MaxOrder and Action-on-ℓ-Torsion

In this section we show that computing an ℓ-isogeny between two supersingular elliptic curves reduces to computing maximal orders of elliptic curves and solving the Action-on-ℓ-Torsion Problem.

Problem 2 (Action-on-ℓ-Torsion)**.** *Given p, a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, and four elements $\{\beta_1, \beta_2, \beta_3, \beta_4\}$ in a maximal order $\mathcal{O}$ of $B_{p,\infty}$ such that there exists an isomorphism $\iota : \mathrm{End}(E) \to \mathcal{O}$, output eight pairs of points on E, (P_1, Q_{1r}), (P_2, Q_{2r}) $(r = 1, \ldots, 4)$ such that P_1, P_2 form a basis for the ℓ-torsion $E[\ell]$ of E, and such that $Q_{1r} = \iota^{-1}(\beta_r)(P_1)$ and $Q_{2r} = \iota^{-1}(\beta_r)(P_2)$ for $r = 1, \ldots, 4$.*

The curve E is given as $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{p^2}$. In our applications, the β_i will be a Minkowski-reduced basis of a maximal order, so their representation size is bounded by a polynomial in $\log p$ by the result in the previous section. Also, ℓ will be chosen to be $O(\log p)$, and therefore the representation sizes of the input and output of the elements for Problem 2 are polynomial in $\log p$.

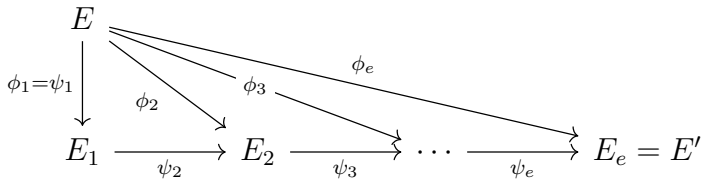
Problem 3 (ℓ-PowerIsogeny)**.** *Given a prime p, along with two supersingular elliptic curves E and E' over $\mathbb{F}_{p^2}$, output an isogeny from E to E' represented as a chain of k many isogenies whose degrees are ℓ.*

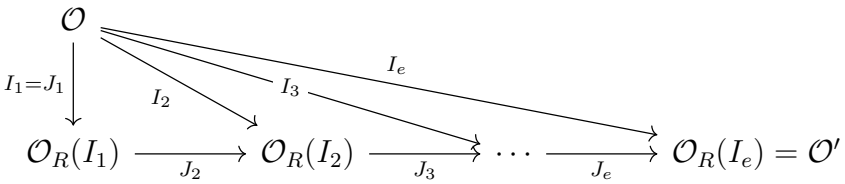
Since E is given as $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{F}_{p^2}$, the input size for this problem is $O(\log p)$. By Section 2.1.3, the representation size of the output is also polynomial in $\log p$, if $\ell \in O(\log p)$ and the isogenies are represented by rational maps.

4.1. **Outline of Reduction.** Given two supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$, and oracles for the problems Action-on-ℓ-Torsion and MaxOrder, we will construct an ℓ-power isogeny $E \to E'$ by constructing a chain of ℓ-isogenies through intermediate curves. First, the oracle will give us two maximal orders $\mathcal{O}, \mathcal{O}' \subseteq B_{p,\infty}$ with $\mathcal{O} \simeq \mathrm{End}(E)$ and $\mathcal{O}' \simeq \mathrm{End}(E')$. We then compute what is called a connecting ideal, meaning a left ideal of $\mathcal{O}$, whose left order is $\mathcal{O}$ and right order is $\mathcal{O}'$. Next we use the main algorithm of [KLPT14] to compute an equivalent ideal I whose norm is ℓ^e for some $e = O(\log(p))$. The isogeny $\phi_I : E \to E'$ corresponding to I has degree ℓ^e, so the representation size of the isogeny is exponential. To remedy this we will, given I, compute a chain of ℓ-isogenies $\psi_1, \ldots, \psi_e$ such that $\phi_I = \psi_e \circ \cdots \circ \psi_1$. Since $\psi_1, \ldots, \psi_e$ have degree ℓ, they are of polynomial representation size as rational maps. To obtain the ψ_i we will first show that there is a factorization of the ideal I. The proper notion here is that of a *filtration* of ideals, namely a sequence

$$I = I_e \subseteq I_{e-1} \subseteq \cdots \subseteq I_1 \subseteq I_0 = \mathcal{O}$$

such that the isogeny corresponding to I_k is a map ϕ_k from E to some intermediate curve E_k. The factorization of ϕ_I gives us a path starting at E and ending at E' of length e in the graph of isogenies of degree ℓ, and the filtration of I leads to a corresponding "path" between maximal orders in $B_{p,\infty}$. The maximal orders that appear in this path are $\mathcal{O}_R(I_k)$ and the ideal connecting $\mathcal{O}_R(I_k)$ to $\mathcal{O}_R(I_{k+1})$ is $J_k := I_{k-1}^{-1} I_k$. These paths are given in the following diagrams:





For each k, the isogeny $\phi_k : E_0 \to E_k$ has degree ℓ^k, and so corresponds to a left $\mathcal{O}$-ideal I_k of norm ℓ^k. We will show that $I_k = I + \mathcal{O}\ell^k$ is the desired ideal. As k grows, these ideals will have norms which are too big to find the corresponding isogenies, so we will compute the maps $\psi_k : E_{k-1} \to E_k$ which correspond to left ideals J_k of $\mathcal{O}_R(I_{k-1})$ of norm ℓ. Suppose we have computed ψ_k, the curve E_k, and J_{k+1} as above. We can use the oracle for MaxOrder to identify generators of J_{k+1} with endomorphisms of E_k. On the other hand, J_{k+1} corresponds to the isogeny ψ_{k+1}, whose kernel we compute using the information from the oracle Action-on-ℓ-Torsion. Using Vélu's formula, we can compute ψ_{k+1} from its kernel. This procedure iteratively computes the desired maps $\psi_1, \psi_2, \ldots, \psi_e$.

4.2. **Reduction from ℓ-PowerIsogeny to MaxOrder and Action-on-ℓ-Torsion.** In this section, we give the reduction from ℓ-Power Isogeny to the problems MaxOrder and Action-on-ℓ-Torsion.

Algorithm 4.1. *Reduction from ℓ-PowerIsogeny to MaxOrder and Action-on-ℓ-Torsion*
Input: E, E' supersingular elliptic curves over $\mathbb{F}_{p^2}$, a prime $\ell \neq p$.
Output: a chain of ℓ-isogenies connecting E and E'.

1. *Compute a basis $\langle 1, i, j, ij\rangle$ for $B_{p,\infty}$.*
2. *Call oracle MaxOrder on $p, \langle 1, i, j, ij\rangle, E$, resulting in $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ where $\mathrm{End}(E) \simeq \mathcal{O} := \langle \alpha_1, \alpha_2, \alpha_3, \alpha_4\rangle \subseteq B_{p,\infty}$.*
3. *Call oracle MaxOrder on $p, \langle 1, i, j, ij\rangle, E'$, resulting in $\alpha'_1, \alpha'_2, \alpha'_3, \alpha'_4$ where $\mathrm{End}(E') \simeq \mathcal{O}' := \langle \alpha'_1, \alpha'_2, \alpha'_3, \alpha'_4\rangle \subseteq B_{p,\infty}$.*
4. *Compute connecting ideal: use $\alpha_1, \ldots, \alpha_4$ and $\alpha'_1, \ldots, \alpha'_4$ to compute a left ideal I of $\mathcal{O}$ such that $\mathcal{O}_R(I) = \mathcal{O}'$ and $\mathrm{Nrd}(I) = \ell^e$ with $e = O(\log(p))$. Adjust I so that $I \not\subseteq \ell^k \cdot \mathcal{O}$ for any positive integer k.*
5. *For $0 \leq k \leq e$:*
   (a) *Compute $I_k := I + \mathcal{O}\ell^k$. This is a left ideal of $\mathcal{O}$ of norm ℓ^k. Also compute its right order $\mathcal{O}_R(I_k)$.*
   (b) *Compute a $\mathbb{Z}$-basis γ_1, γ_2, γ_3, γ_4 for the ideal $J_{k+1} := I_k^{-1} I_{k+1}$ of $\mathcal{O}_R(I_k)$.*
6. *Set $E_0 := E$.*
7. *For $0 \leq k \leq e-1$:*
   (a) *Compute a basis $\{P_1, P_2\}$ for $E_k[\ell]$.*
   (b) *Call oracle MaxOrder with $p, \langle 1, i, j, ij\rangle, E_k$, resulting in β_1, β_2, β_3, β_4 that generate $\mathcal{O}_k \subseteq B_{p,\infty}$.*
   (c) *Call oracle Action-on-ℓ-Torsion with parameters $p, P_1, P_2, \langle 1, i, j, ij\rangle, E_k, \beta_1$, β_2, β_3, β_4 resulting in $Q_{st} = \iota_k^{-1}(\beta_s)(P_t)$ for $s = 1, \ldots, 4$, $t = 1, 2$.*
   Here, $\iota_k : \mathrm{End}(E_k) \to \langle \beta_1, \ldots, \beta_4\rangle$ is an isomorphism.
   (d) *Compute $v \in B_{p,\infty}$ such that $v\mathcal{O}_R(I_k)v^{-1} = \mathcal{O}_k$.*
   (e) *Compute c_{rs} such that $v\gamma_r v^{-1} = \sum_s c_{rs}\beta_s$.*
   (f) *Find $x, y \in \mathbb{Z}/\ell\mathbb{Z}$, not both 0, such that $\sum_s c_{rs}(xQ_{s1} + yQ_{s2}) = 0$ for $r = 1, \ldots, 4$.*
   (g) *Compute ψ_{k+1} and its image E_{k+1} with kernel $\langle xP_1 + yP_2\rangle = E_k[\iota_k^{-1}(J_{k+1})]$ using Vélu's formula*
8. *Return $\psi_1, \psi_2, \ldots, \psi_e$.*

Theorem 4.2. *ℓ-PowerIsogeny efficiently reduces to MaxOrder and Action-on-ℓ-Torsion. In particular, given a prime p, a prime $\ell \neq p$, and supersingular elliptic curves E, E' over $\mathbb{F}_{p^2}$, Algorithm 4.1 returns isogenies $\psi_1, \ldots, \psi_e$ of degree ℓ whose composition is an isogeny $\psi := \psi_e \circ \cdots \circ \psi_1$ of degree ℓ^e from E to E'. Assuming ℓ is of size $O(\log(p))$, Algorithm 4.1 runs in time polynomial in $\log(p)$ and makes $O(\log(p))$ queries of MaxOrder and Action-on-ℓ-Torsion.*

Proof. By Theorem 3.6, the oracle returns a basis for $\mathcal{O}$ and for $\mathcal{O}'$ of polynomial size. To do Step 4, we first compute an arbitrary connecting ideal for $\mathcal{O}$ and $\mathcal{O}'$ in polynomial time using Algorithm 3.5 of [KV10]. An equivalent connecting ideal of norm ℓ^e, where $e = O(\log(p))$, can be computed in polynomial time as claimed in [KLPT14].

Define $E_k := E/E[I_k]$ (here by $E[I_k]$ we mean $E[\iota^{-1}(I_k)]$, where $\iota : \mathrm{End}(E) \to \mathcal{O}$ is an isomorphism). We need to show that I_k has norm ℓ^k and that the left $\mathcal{O}_R(I_k)$-ideal J_{k+1} corresponds to the isogeny $\psi_{k+1} : E_k \to E_{k+1}$ in the factorization $\phi_k = \psi_k \circ \phi_{k-1}$; this is

proved in Theorem 4.9. Right orders and products of ideals can be computed efficiently with linear algebra over $\mathbb{Z}$, hence Step 4 is efficient; see [Rón92], Theorem 3.2 for the statement on right orders. Inverses can be computed from the formula $I^{-1} = \frac{1}{\mathrm{Nrd}(I)}\overline{I}$. We make e calls to the oracle for generators of $\mathrm{End}(E_k)$ and their action on ℓ-torsion. If $\mathcal{O} \simeq \mathcal{O}_k$, we can compute v such that $v\mathcal{O}_k v^{-1} = \mathcal{O}$ in polynomial time by Lemma 2.5, Corollary 3.6, and Proposition 6.9 of [KV10]. By Theorem 4.9, the isogeny corresponding to I factors as the product of the isogenies corresponding to J_k, $k = 1, \ldots, e$, all of which have degree ℓ. Now compute the kernel of ψ_k using J_k and the action of $\mathrm{End}(E_{k-1})$ on the ℓ-torsion of E_{k-1}; see Proposition 4.10. Since ℓ is $O(\log(p))$, rational maps for ψ_k from its kernel can be efficiently computed. □

4.3. **Filtrations of Left-Ideals and Corresponding Isogeny Paths.** Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve and let I be a left ideal of $\mathrm{End}(E)$ of norm ℓ^e such that $I \not\subseteq \mathrm{End}(E) \cdot \ell^m$ for any positive integer m. In this section, we prove that for $k = 0, \ldots, e$, $I_k = I + \mathrm{End}(E) \cdot \ell^k$ is an ideal of norm ℓ^k and that

$$I = I_e \subseteq I_{e-1} \subseteq \cdots \subseteq I_1 \subseteq I_0 = \mathrm{End}(E).$$

Let ϕ_k be the isogeny corresponding to I_k. We want to show that $\phi_k : E \to E_k := E/E[I_k]$ is an isogeny of degree ℓ^k.

We first establish when an ideal corresponds to an isogeny with cyclic kernel.

Proposition 4.3. *Suppose $I \subseteq \mathrm{End}(E)$ is a left ideal with $\mathrm{Nrd}(I)$ coprime to p. Then I is not contained in $\mathrm{End}(E) \cdot m$ for any $m \in \mathbb{N}$ if and only if $E[I]$ is cyclic.*

Proof. Suppose that $I \subseteq \mathrm{End}(E) \cdot m$. Then $E[I] \supset E[\mathrm{End}(E) \cdot m] = E[m]$ and thus $m | \deg(\phi_I)$. Since p does not divide $\deg(\phi_I)$, it also does not divide m, so $E[m] \neq 0$ and has rank two as a $\mathbb{Z}/m\mathbb{Z}$-module. Hence $E[I]$ is not cyclic. For the other direction, suppose that $E[I]$ is not cyclic. Then, by the structure theorem of abelian groups,

$$E[I] \simeq \bigoplus_{i=1}^{j} \mathbb{Z}/k_i\mathbb{Z}$$

and we can choose the k_i uniquely such that $k_i | k_{i+1}$. Since $E[I]$ is not cyclic, $j \neq 1$ and hence $E[I]$ has two elements of order k_1 which are linearly independent. Thus $E[k_1] \subseteq E[I]$ and hence $I \supset \mathrm{End}(E) \cdot k_1$. □

Proposition 4.4. *Suppose $I \subseteq \mathrm{End}(E)$ and $N := \mathrm{Nrd}(I)$ is coprime to p. Also suppose $M | N$, and that I is not contained in $\mathrm{End}(E) \cdot m$ for any $m \in \mathbb{N}$. Then $I + \mathrm{End}(E) \cdot M$ has norm M.*

Proof. We claim that

$$E[I + M\mathcal{O}] = E[I] \cap E[M].$$

Indeed, for an arbitrary left ideal J of $\mathrm{End}(E)$ with $\mathrm{Nrd}(J)$ coprime to p, $E[J]$ is the intersection of the kernels of a generating set of J, and for two left $\mathrm{End}(E)$-ideals J, J', $J + J'$ is generated by $J \cup J'$. Since $E[I]$ is cyclic by Proposition 4.3, there is some $Q \in E[N]$ so that $E[I] = \langle Q \rangle$. Then $E[I] \cap E[M] = \langle [N/M]Q \rangle$, a group of order M as desired. □

4.4. **Matching up a Filtration of an Ideal with a Factorization of an Isogeny.** In this section, we show that the definition of J_k in Algorithm 4.1 gives us the ideal which corresponds to the isogeny $E_{k-1} \to E_k$ of degree ℓ. To do this, it suffices to understand the horizontal isogeny and corresponding ideal in the following diagram:

$$\begin{array}{ccc} E & & \\ {\scriptstyle I_{k-1}}\downarrow & \searrow^{I_k} & \\ E_{k-1} := E/E[I_{k-1}] & \xrightarrow[J_k]{} & E_k := E/E[I_k] \end{array}$$

We will describe the relationship between the horizontal isogeny and its kernel ideal for two arbitrary left ideals I, I' of $\mathrm{End}(E)$ satisfying $I' \subseteq I$, so in the above picture, we replace I_{k-1} with I and I_k with I'. The goal is to find, given $I' \subseteq I$, the horizontal isogeny $E_I \to E_{I'}$ by first computing its corresponding ideal $\tilde{J}$ in the following diagram:

$$\begin{array}{ccc} E & & \\ {\scriptstyle I}\downarrow & \searrow^{I'} & \\ E_I := E/E[I] & \xrightarrow[\tilde{J}]{} & E_{I'} := E/E[I'] \end{array}$$

Let $\phi_I : E \to E_I := E/E[I]$ and $\phi_{I'} : E \to E_{I'} := E/E[I']$ be the corresponding isogenies; then $E[I] \subseteq E[I']$ and hence $\phi_{I'}$ factors as $\phi_{I'} = \psi\phi_I$ for some isogeny $\psi : E_I \to E_{I'}$. We wish to view the kernel of ψ as $E_I[\tilde{J}]$ for some left ideal $\tilde{J}$ of $\mathrm{End}(E_I)$. We make this idea precise in the following proposition.

Proposition 4.5. *Let $I' \subseteq I$ be two left $\mathrm{End}(E)$-ideals whose norms are coprime to p. Then there exists a separable isogeny $\psi : E_I \to E_{I'}$ such that $\phi_I = \psi \circ \phi_{I'}$, and a left ideal $\tilde{J}$ of $\mathrm{End}(E_I)$ with $E_I[\tilde{J}] = \ker(\psi)$ such that $J = \iota(\tilde{J}) = I^{-1}I'$, where $\iota : \mathrm{End}(E_I) \to \mathrm{End}(E) \otimes \mathbb{Q}$ is the map in Lemma 4.7 below.*

To prove this, we need the following three lemmas:

Lemma 4.6. *For a left ideal I of $\mathrm{End}(E)$, the map*

$$\begin{aligned} \phi_I^* : \mathrm{Hom}(E_I, E) &\to I \\ \psi &\mapsto \psi\phi_I \end{aligned}$$

is an isomorphism of left $\mathrm{End}(E)$-modules.

Proof. This is Lemma 42.2.6 of [Voi]. It also follows from Proposition 48 of [Koh96]. □

Lemma 4.7. *Set $B = \mathrm{End}(E) \otimes \mathbb{Q}$. The map*

$$\begin{aligned} \iota : \mathrm{End}(E_I) &\to B \\ \beta &\mapsto \frac{1}{\deg(\phi_I)} \widehat{\phi_I} \beta \phi_I \end{aligned}$$

is injective, and its image is $\mathcal{O}_R(I)$.

Proof. This is Lemma 42.2.8 of [Voi] or Proposition 3.9 of [Wat69]. □

Lemma 4.8. *We have a bijection*

$$g : \mathrm{Hom}(E_{I'}, E_I) \to I^{-1}I'$$
$$\psi \mapsto \frac{1}{\deg(\phi_I)}\widehat{\phi_I}\psi\phi_{I'}.$$

Proof. This is Lemma 42.2.19 of [Voi]. □

Now we can prove the proposition.

Proof of Proposition 4.5. We have that $I^{-1} = \frac{1}{\mathrm{Nrd}(I)}\overline{I}$. Consider an element $x \in I^{-1}I'$ of the form

$$x = \frac{1}{\deg(\phi_I)}\widehat{\alpha'}\beta',$$

where $\alpha' \in I$, $\beta' \in I'$. Then by Lemma 4.6, there exists $\alpha \in \mathrm{Hom}(E_I, E)$ and $\beta \in \mathrm{Hom}(E_{I'}, E)$ with

$$\alpha' = \alpha\phi_I, \beta' = \beta\phi_{I'}.$$

Thus

$$x = \frac{1}{\deg(\phi_I)}\widehat{\phi_I}\widehat{\alpha}\beta\phi_{I'} = g(\widehat{\alpha}\beta),$$

where $g : \mathrm{Hom}(E_{I'}, E_I) \to I^{-1}I'$ is the map in Lemma 4.8. Since $E[I] \subseteq E[I']$, and $\phi_I, \phi_{I'}$ are separable, by Corollary III.4.11 of [Sil09] there exists a unique separable isogeny $\psi : E_I \to E_{I'}$ such that $\phi_{I'} = \psi \circ \phi_I$. Then define

$$\tilde{J} := \{\alpha \in \mathrm{End}(E_1) : \alpha(P) = 0 \quad \forall P \in \ker(\psi)\}.$$

Now map $g^{-1}(x) = \widehat{\alpha}\beta \in \mathrm{Hom}(E_{I'}, E_I)$ to an element of $\tilde{J}$ using ψ^*: $\widehat{\alpha}\beta\psi = \psi^*(\widehat{\alpha}\beta) \in \tilde{J}$. Finally, compute

$$\begin{aligned} x &= \frac{1}{\deg(\phi_I)}\widehat{\phi_I}\widehat{\alpha}\beta\phi_{I'} \\ &= \frac{1}{\deg(\phi_I)}\widehat{\phi_I}\widehat{\alpha}\beta\psi\phi_I \\ &= \iota(\widehat{\alpha}\beta\psi) \\ &= \iota(\psi^*(\widehat{\alpha}\beta)) \\ &= (\iota \circ \psi^* \circ g^{-1})(x). \end{aligned}$$

In other words, we have

$$g = \iota \circ \psi^*.$$

From this, we conclude that the left ideal of $\mathcal{O}_R(I_1)$ corresponding to $\tilde{J}$ indeed is $I^{-1}I'$. □

Combining the above results, we have our main theorem on matching up filtrations of ideals with factorizations of isogenies:

Theorem 4.9. *Suppose that $I \subseteq \mathrm{End}(E)$ satisfies $\mathrm{Nrd}(I) = \ell^e$ where $\ell \neq p$ is a prime and $I \not\subset \mathrm{End}(E) \cdot \ell^k$ for any $k \in \mathbb{N}$. Then there exists a filtration*

$$I = I_e \subsetneq I_{e-1} \subsetneq \ldots \subsetneq I_1 \subsetneq I_0 = \mathrm{End}(E)$$

and a chain of isogenies

$$E = E_0 \xrightarrow{\psi_1} E_1 \xrightarrow{\psi_2} \cdots \xrightarrow{\psi_{e-2}} E_{e-1} \xrightarrow{\psi_e} E_e = E'$$

such that if we set $\phi_k : E \to E/E[I_k]$*, then* $\phi_{k+1} = \psi_k\phi_k$*. Moreover, for* $k = 0, \ldots, e-1$*, the map* $\psi_{k+1} : E_k \to E_{k+1}$ *has degree* ℓ*, and its kernel ideal in* $\mathrm{End}(E_k)$ *is isomorphic to* $I_k^{-1}I_{k+1} \subseteq \mathcal{O}_R(I_k)$ *under the map*

$$\begin{aligned} \iota_k : \mathrm{End}(E_k) &\to \mathcal{O}_R(I_k) \\ \rho &\mapsto \frac{1}{\deg(\phi_k)}\hat{\phi}_k\rho\phi. \end{aligned}$$

Proof. For $k = 0, 1, \ldots, e$, define $I_k := I + \mathrm{End}(E) \cdot \ell^k$. By Proposition 4.4, $\mathrm{Nrd}(I_k) = \ell^k$. Let $\phi_I : E \to E_e := E/E[I_e] = E/E[I]$ be the isogeny corresponding to $I = I_e$. Set $\mathcal{O}_k := \mathcal{O}_R(I_k) \subseteq \mathrm{End}(E) \otimes \mathbb{Q}$, and $J_k := I_{k-1}^{-1}I_k$. Then $\mathrm{Nrd}(J_k) = \ell$. Let $E_k := E/E[I_k]$. From the ideals J_k, we have isogenies $\psi_k : E_{k-1} \to E_k$ such that

$$\phi = \psi_e \circ \cdots \circ \psi_1$$

by Proposition 4.5 applied inductively to the ideals $I_{k+1} \subsetneq I_k$. □

4.5. **Going From an Ideal of Norm ℓ to a Corresponding Subgroup of Order ℓ.** At the beginning of Step 7 of the algorithm, we have an isogeny $E_{k-1} \to E_k$ represented by a left $\mathcal{O}_R(I_{k-1})$-ideal J_k. We wish to specify the subgroup of E_{k-1} which is the kernel of this isogeny. If $\widetilde{J_k} \subseteq \mathrm{End}(E_{k-1})$ is the ideal isomorphic to J_k, recall from Section 2.2.3 that

$$E_{k-1}[\widetilde{J_k}] = \bigcap_{\gamma \in \tilde{J}_k} \ker(\gamma_k),$$

and it suffices to compute $\ker(\gamma_1) \cap \cdots \cap \ker(\gamma_4)$, where $\gamma_1, \ldots, \gamma_4$ are a $\mathbb{Z}$-basis of $\widetilde{J_k}$. Once we have $E_{k-1}[\widetilde{J_k}]$, we can use Vélu's formula to compute ψ_k.

Step 7 in our algorithm computes $E_{k-1}[\tilde{J}_k]$ and is similar to Algorithm 2 in [GPS16]. In our version, we are working with ideals in consecutive endomorphism rings, rather than in the endomorphism ring of the starting curve, and we give proofs of correctness along with analysis of input size of left ideals of a maximal order.

Proposition 4.10. *Let* E *be a supersingular elliptic curve over* $\mathbb{F}_{p^2}$*, and assume* $\iota : \mathrm{End}(E) \to \mathcal{O} \subseteq B_{p,\infty}$ *is an isomorphism, where* $\mathcal{O}$ *has a basis of size polynomial in* $\log p$*. Let* $I \subseteq \mathcal{O}$ *be an ideal of norm* ℓ^e *for a prime* $\ell \neq p$ *with* $\ell = O(\log(p))$*. For* $k = 1, \ldots, e$*, define* $I_k := I + \mathcal{O} \cdot \ell^k$ *and* $J_k = I_{k-1}^{-1}I_k \subseteq \mathcal{O}_R(I_{k-1})$ *and* $E_k := E/E[\iota^{-1}(I_k)]$ *as in Theorem 4.9. Then if we are given* $\iota_{k-1}(\mathrm{End}(E_{k-1}))$ *in* $B_{p,\infty}$ *where* $\iota_{k-1} : \mathrm{End}(E_{k-1}) \otimes \mathbb{Q} \to B_{p,\infty}$ *is an isomorphism of quaternion algebras, along with the action of* $\mathrm{End}(E_{k-1})$ *on* $E_{k-1}[\ell]$*, we can compute the kernel of the isogeny corresponding to* $\iota_{k-1}^{-1}(J_k)$ *in time polynomial in* $\log p$*.*

Proof. We wish to determine $E_{k-1}[\iota_{k-1}^{-1}(J_k)]$ so that we can compute the corresponding isogeny $\psi_k : E_{k-1} \to E_k$. If J_k has a $\mathbb{Z}$-basis $\gamma_1, \ldots, \gamma_4 \in \mathcal{O}_R(I_{k-1})$, we need to understand how the γ_i act as endomorphisms of E_{k-1}. Suppose we are given the action of generators $\phi_1, \ldots, \phi_4$ of $\mathrm{End}(E_{k-1})$ on $E_{k-1}[\ell]$ and the image of an embedding $\iota_{k-1} : \mathrm{End}(E_{k-1}) \to B_{p,\infty}$. Set $\mathcal{O}_{k-1} := \iota_{k-1}(\mathrm{End}(E_{k-1}))$; then we can compute $v \in B_{p,\infty}^\times$ such that $\mathcal{O}_{k-1} = v\mathcal{O}_R(I_{k-1})v^{-1}$ in polynomial time by [KV10]. By expressing $v\gamma_i v^{-1}$ in terms of $\iota_{k-1}(\phi_j)$, say

$$v\gamma_r v^{-1} = \sum_s c_{rs}\iota_{k-1}(\phi_s),$$

we discern the kernel of the isogeny corresponding to of J_k as follows. We require a nonzero point $P \in E_{k-1}[\ell]$ such that for all $r = 1, \ldots, 4$,

$$\sum_s c_{rs}\phi_s(P) = 0.$$

Because we assume that we are given $\phi_s(P)$ for $s = 1, \ldots, 4$ and $P \in E_{k-1}[\ell]$, we can find such a P by just calculating the sum for all $r = 1, \ldots, 4$ and $P \neq 0 \in E_{k-1}[\ell]$. □

5. The EndomorphismRing Problem

In this section we study the computational hardness of computing endomorphism rings of supersingular elliptic curves. Kohel began the study of this problem in [Koh96], but our focus will be on polynomial-time reductions between problems connected to endomorphism rings. The inputs are p and the curve, and so the running time must be polynomial in $\log p$. This brings up two important questions: 1) does the endomorphism ring of an elliptic curve have a polynomial representation size? And 2) If it does, can the endomorphisms be evaluated in polynomial time? Answering these two questions is very important in order to have a meaningful definition of the endomorphism ring problem. In this section, we lay the framework for reductions involving endomorphism rings. To have any meaningful efficient reduction, or to analyze how hard it is to compute the endomorphism ring, we need to know what the representation size of an endomorphism ring is. In particular, we need to discuss what we mean by *computing the endomorphism ring*.

We will define a compact representation of endomorphisms which has polynomial size, and show that the endomorphism ring of any supersingular elliptic curve has a basis of such representations. This answers question 1. We also show that these representations can be evaluated efficiently at arbitrary points, answering question 2. We then define the problem EndomorphismRing in terms of this new definition, and show that it efficiently reduces to MaximalOrder and Action-on-ℓ-Torsion for $\ell = 2, 3$. We also identify another problem that it reduces to, which is related to computing isogenies.

5.1. **Representation Size of Endomorphism Rings.** There are two typical ways to represent the endomorphism ring of E. The first is to give rational functions $F_1(x, y), \ldots, F_4(x, y)$ and $G_1(x, y), \ldots, G_4(x, y)$ such that $\phi_i : (x, y) \mapsto (F_i(x, y), G_i(x, y))$ $(i = 1, \ldots, 4)$ are endomorphisms of E that form a basis for $\mathrm{End}(E)$. The second is to give the kernel of the maps ϕ_i, which in general is not good enough for computations. However, it is not known if a basis for $\mathrm{End}(E)$ exists in either representation that is of polynomial size. For example, the basis may contain an endomorphism of exponential degree, where exponentially many coefficients would be needed to describe it in general. For the case of using the kernel, the generators may lie in a finite field of exponential degree over the base field, and there will be exponentially many points in the kernel.

5.2. **Compact Representations of Endomorphisms.** We will now show that the endomorphism ring $\mathrm{End}(E)$ of any supersingular elliptic curve $E/\mathbb{F}_{p^2}$ has compact representations if $p \equiv 3 \pmod 4$. The proof will require a special curve E_0 for which a basis of the endomorphism ring is known; such a curve exists if $p \not\equiv 1 \pmod{12}$.

For simplicity, we will focus on the case where $p \equiv 3 \pmod 4$ is a prime and let $E_0 : y^2 = x^3 + x$. Let $\pi : E_0 \to E_0$ denote the Frobenius map, and let $\phi : E_0 \to E_0$ be the map $(x, y) \mapsto (-x, \sqrt{-1}y)$. The maps $1 + \phi\pi$ and $\phi + \pi$ both have kernels containing $E[2]$, so

they factor through the map $[2] : E_0 \to E_0$. Let $(1 + \phi\pi)/2$ and $(\phi + \pi)/2$ represent the maps in these factorizations. It can be shown that $1, \phi, (1 + \phi\pi)/2, (\phi + \pi)/2$ form a basis for $\mathrm{End}(E_0)$, see [GPS16]. As rational maps, the size of this basis may not be polynomial in $\log p$, but the description as rational linear combinations of $1, \phi, \pi, \phi\pi$ uniquely identifies them, and so it is enough that ϕ and π have polynomial size. This representation allows for efficient evaluation at points P of E_0 by writing $P = [2]Q$ and then evaluating linear combinations of $1, \phi, \pi, \phi\pi$ at Q. Define $[\beta_1, \beta_2, \beta_3, \beta_4] := [1, \phi, (1 + \phi\pi)/2, (\phi + \pi)/2]$. We will use $\beta_1, \beta_2, \beta_3, \beta_4$ in our definition of compact representatives of endomorphisms for all other supersingular elliptic curves $E/\mathbb{F}_{p^2}$.

Definition 5.1 (Compact representation of an endomorphism)**.** *Let $p \equiv 3 \pmod 4$ be a prime, let $E_0 : y^2 = x^3 + x$, and $\beta_1, \ldots, \beta_4 := 1, \phi, (1+\phi\pi)/2, (\phi+\pi)/2$ be the endomorphisms of E_0 as above. Let $E/\mathbb{F}_{p^2}$ be another supersingular elliptic curve, and let $\rho \in \mathrm{End}(E)$. Define a* compact representation *of ρ to be a list*

$$[d, [c_1, \ldots, c_4], [\phi_1, \ldots, \phi_m], [\widehat{\phi_1}, \ldots, \widehat{\phi_m}]],$$

where $c_1, \ldots, c_4, d \in \mathbb{Z}$, ϕ_i are isogenies on a path from E_0 to E, and the total size of the list

$$\log(|d|) + \log(|c_1|) + \cdots + \log(|c_4|) + \sum_{i=1}^{m} \log(\deg(\phi_m))$$

is at most polynomial in $\log(p)$, and

$$\rho = \frac{1}{d}\left(\phi_m \circ \cdots \circ \phi_1 \circ \left(\sum_{i=1}^{4} c_i\beta_i\right) \circ \widehat{\phi_1} \circ \cdots \circ \widehat{\phi_m}\right).$$

Theorem 5.2. *Let $p \equiv 3 \pmod 4$ and let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve. Then there exist two lists of four compact representatives of endomorphisms of E, such that each list represents a $\mathbb{Z}$-basis of $\mathrm{End}(E)$.*

Moreover, assume $\rho \in \mathrm{End}(E)$ is a linear combination of the endomorphisms corresponding to one such basis, and assume that its coefficient vector in terms of this basis is of size polynomial in $\log(p)$. Using the two lists, we can evaluate ρ at arbitrary points of E in time polynomial in $\log(p)$ and the size of the point P.

Proof. Let $\mathcal{O}_0$ be the maximal order in $B_{p,\infty}$ with basis

$$b_1, \ldots, b_4 := 1, i, (1 + ij)/2, (i + j)/2.$$

Then $\mathcal{O}_0 \cong \mathrm{End}(E_0)$ and $b_1, \ldots, b_4$ correspond to $\beta_1, \ldots, \beta_4$ under an isomorphism. There exist chains of isogenies $\phi_1, \ldots, \phi_m$ and $\psi_1, \ldots, \psi_n$ between E_0 and E with $\deg(\phi_k) = 2$ and $\deg(\psi_k) = 3$, and with $m, n = O(\log(p))$. Set $\phi = \phi_m \circ \cdots \circ \phi_1$ and $\psi = \psi_n \circ \cdots \circ \psi_1$. Let $I \subseteq \mathcal{O}_0$ and $J \subseteq \mathcal{O}_0$ be the left $\mathcal{O}_0$-ideals corresponding to ϕ and ψ respectively.

There exist rational numbers c^I_{rs} whose denominators are divisors of $2\,\mathrm{Nrd}(I)$ and rational numbers c^J_{rs} whose denominators are divisors of $2\,\mathrm{Nrd}(J)$ such that

$$\gamma^I_r := \sum_s c^I_{rs} b_s, 1 \le r \le 4$$

is a a Minkowski-reduced basis of $\mathcal{O}_R(I)$, and

$$\gamma^J_r := \sum_s c^J_{rs} b_s, 1 \le r \le 4$$

is a Minkowski-reduced basis of $\mathcal{O}_R(J)$. This follows from Theorem 3.6 and its proof. We can also efficiently find $v \in B_{p,\infty}$ such that $v\mathcal{O}_R(I)v^{-1} = \mathcal{O}_R(J)$ [KV10].

Then $\rho_r^J := \frac{1}{2^m}\phi\gamma_r^I\widehat{\phi}$ and $\rho_r^I := \frac{1}{3^n}\psi\gamma_r^J\widehat{\psi}$ $(r = 1, \ldots, 4)$ each form a basis for $\mathrm{End}(E)$. Then our compact representations are, for $r = 1, \ldots, 4$,

$$[\mathrm{Nrd}(I), c_{r1}^I, \ldots, c_{r4}^I, [\phi_1, \ldots, \phi_m,], [\widehat{\phi_1}, \ldots, \widehat{\phi_m}]],$$
$$[\mathrm{Nrd}(J), c_{r1}^J, \ldots, c_{r4}^J, [\psi_1, \ldots, \psi_n], [\widehat{\psi_1}, \ldots, \widehat{\psi_n}]].$$

Observe that we can efficiently evaluate ρ_r^J at any point P of E whose order is coprime to 2. This is because $[2^m]\rho_r^I$ can be evaluated at P as it is a composition of the $\widehat{\phi_k}$, an integer linear combination of the β_k and then ϕ_k, all of which we can efficiently evaluate in terms of the size of P. Set $Q = [2^m]\rho_r^I(P)$. Let N be the inverse of 2^m modulo the order of P. Then $[N]Q = \rho_r^I(P)$.

If we want to evaluate ρ_r^I at a point P with $P \in E[2^f]$, we will instead express $v\rho_r^I v^{-1}$ as an integral linear combination of $\rho_1^J, \ldots \rho_4^J$. We can evaluate each $\rho_1^J, \ldots, \rho_4^J$ at any point of order coprime to 3 by the same argument.

Thus we can evaluate at arbitrary points P: if P has order $2^f M$ with $(2, M) = 1$, then we can write P as a sum of a point P_2 of order 2^f and P_M of order M. We can then evaluate at P by evaluating it at each summand with the two above strategies. □

Computing compact representations of endomorphisms which can be evaluated at points of E and which generate $\mathrm{End}(E)$ is a natural interpretation of the problem of computing endomorphism rings, so we formally state it here before relating it to other isogeny problems.

Problem 4 (EndomorphismRing)**.** *Given a prime p and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, find a list of total length bounded by $O(\log(p))$ of compact representations of endomorphisms of E such that using this list, we can evaluate the corresponding endomorphisms at points of E, and such that the corresponding endomorphisms generate* $\mathrm{End}(E)$ *as a $\mathbb{Z}$-module.*

In the next section, we will discuss two reductions from EndomorphismRing.

5.3. **EndomorphismRing Reduces to MaxOrder and Action-on-2-Torsion and Action-on-3-Torsion.** In Algorithm 4.1, we used embeddings of endomorphism rings in $B_{p,\infty}$, together with their action on ℓ-torsion, to construct an ℓ-isogeny.

Theorem 5.3. *If $p \equiv 3 \pmod 4$, EndomorphismRing reduces to MaxOrder and Action-on-ℓ-Torsion for $\ell = 2$ and 3.*

Proof. Let E be a supersingular elliptic curve. Let E_0 be the curve $y^2 = x^3 + x$ and let $\mathcal{O}_0$ be the order isomorphic to $\mathrm{End}(E_0)$. By Theorem 5.2, the necessary data to give compact representations of generators of $\mathrm{End}(E)$ is a 2-power and 3-power isogeny from E_0 to E, and a basis for the right orders of the ideals which correspond to these isogenies in $B_{p,\infty}$. In the proof of Theorem 4.2, note that all of this data is constructed using the oracles for MaxOrder, and Problems Action-on-2-Torsion and Action-on-3-Torsion. □

5.4. **EndomorphismRing Reduces to an Isogeny Problem.** We can also reduce the problem EndomorphismRing to a variant of the ℓ-Isogeny Problem, where we require the ℓ-power isogeny to be represented both by a chain of ℓ-isogenies and by a left ideal in a maximal order.

Problem 5 (FindKernelIdeal)**.** *Given a prime p and a sequence of supersingular elliptic curves $E_0, \dots, E_{m-1}$ and ℓ-isogenies $\phi_k : E_{k-1} \to E_k$, $k = 1, \dots, m$, with $m = O(\log(p))$, along with a maximal order $\mathcal{O}_0 \subseteq B_{p,\infty}$ isomorphic to* $\mathrm{End}(E_0)$*, compute the ideal I of $\mathcal{O}_0 \subseteq B_{p,\infty}$ corresponding to $\phi_m \circ \cdots \circ \phi_1 : E_0 \to E_m$.*

Theorem 5.4. *EndomorphismRing reduces to ℓ-PowerIsogeny and FindKernelIdeal.*

Proof. Let E be a supersingular elliptic curve. Assume we are given $\phi_1, \dots, \phi_m$ and $\psi_1, \dots, \psi_n$ whose compositions are 2^m- and 3^n-isogenies $E_0 \to E$ and m, n are $O(\log(p))$. Also assume we are given ideals A and B of $\mathcal{O}_0$ such that A is the kernel ideal of $\phi := \phi_m \circ \cdots \phi_1 : E_0 \to E$ and B is the kernel ideal of $\psi := \psi_m \circ \cdots \circ \psi_1$. Then we can compute $\mathbb{Z}$-bases of $\mathcal{O}_R(A)$ and $\mathcal{O}_R(B)$. The sequences $\{\phi_r\}$ and $\{\psi_s\}$ for $r = 1, \dots, m$ and $s = 1, \dots, n$, along with $\mathbb{Z}$-bases of $\mathcal{O}_R(A)$ and $\mathcal{O}_R(B)$, gives us the compact representations of generators of $\mathrm{End}(E)$ constructed in the proof of Theorem 5.2. □

6. Applications to the CGL Hash Function

For the hash function in [CGL09] constructed from Pizer's Ramanujan graphs, there is a hash function associated to each supersingular elliptic curve $\tilde{E}$ (specified, up to isomorphism, by its j-invariant). Fix such a hash function corresponding to $\tilde{E}$. The input to the hash function is a binary number of k digits, and from this one computes a sequence of k 2-isogenies, starting at $\tilde{E}$, whose composition maps to some other supersingular curve E'. The j-invariant of E' is the output of the hash function.

Under this construction, preimage resistance of this function corresponds exactly to the problem of finding a 2-power isogeny between $\tilde{E}$ and E' of a specified degree. So given our reduction in Section 4 we have the following theorem.

Theorem 6.1. *Finding preimages (of unspecified length) for the hash function constructed in* [CGL09] *reduces to Problem MaxOrder and Problem Action-on-2-Torsion.*

The problem of finding collisions also reduces to these two problems and we have the following theorem.

Theorem 6.2. *Finding collisions (of unspecified length) for the hash function constructed in* [CGL09] *reduces to Problem MaxOrder and Problem Action-on-2-Torsion.*

Proof. Finding a collision just amounts to finding two different 2-power isogenies between $\tilde{E}$ and E'. This can be done as follows. First, use Algorithm 4.1 to find one 2-power isogeny between $\tilde{E}$ and E', given as a list of isogenies of degree 2. Look at the first 2-isogeny starting at $\tilde{E}$. For the second part, choose a different 2-isogeny from $\tilde{E}$ to another curve E_1 in the first step, and then use Algorithm 4.1 to find a 2-power isogeny from E_1 to E'. Concatenating the two-isogeny from $\tilde{E}$ to E_1 with the 2-power isogeny from E_1 to E' gives a second different 2-power isogeny from $\tilde{E}$ to E'. □

Remark 6.3. *This produces a collision for the hash, but not of a specified degree.*

Acknowledgments

We thank John Voight for many helpful discussions regarding orders in quaternion algebras and their connection with supersingular elliptic curves.

References

[Ank52] N. C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[BJS14] Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *Progress in cryptology—INDOCRYPT 2014*, volume 8885 of *Lecture Notes in Comput. Sci.*, pages 428–442. Springer, Cham, 2014.

[Cer04] J. M. Cerviño. Supersingular elliptic curves and maximal quaternionic orders. In *Mathematisches Institut, Georg-August-Universität Göttingen: Seminars Summer Term 2004*, pages 53–60. Universitätsdrucke Göttingen, Göttingen, 2004.

[CG14] Ilya Chevyrev and Steven D. Galbraith. Constructing supersingular elliptic curves with a given endomorphism ring. *LMS J. Comput. Math.*, 17(suppl. A):71–91, 2014.

[CGL09] Denis X. Charles, Eyal Z. Goren, and Kristin Lauter. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009.

[CJS14] Andrew Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Univ. Hamburg*, 14(1):197–272, 1941.

[DFJP14] Luca De Feo, David Jao, and Jérôme Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *J. Math. Cryptol.*, 8(3):209–247, 2014.

[DG16] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Des. Codes Cryptogr.*, 78(2):425–440, 2016.

[GPS16] Steven D. Galbraith, Christophe Petit, and Javier Silva. Signature schemes based on supersingular isogeny problems. Cryptology ePrint Archive, Report 2016/1154, 2016. `http://eprint.iacr.org/2016/1154`.

[GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yan Bo Ti. On the security of supersingular isogeny cryptosystems. In *Advances in cryptology—ASIACRYPT 2016. Part I*, volume 10031 of *Lecture Notes in Comput. Sci.*, pages 63–91. Springer, Berlin, 2016.

[Gro87] Benedict H. Gross. Heights and the special values of L-series. In *Number theory (Montreal, Que., 1985)*, volume 7 of *CMS Conf. Proc.*, pages 115–187. Amer. Math. Soc., Providence, RI, 1987.

[KLPT14] David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion l-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17:418–432, 2014.

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

[KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010.

[LP17] Kristin Lauter and Christophe Petit. Hard and easy problems for supersingular isogeny graphs. Preprint, 2017.

[Mes86] J.-F. Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242. Nagoya Univ., Nagoya, 1986.

[NS09] Phong Q. Nguyen and Damien Stehlé. Low-dimensional lattice basis reduction revisited. *ACM Trans. Algorithms*, 5(4):Art. 46, 48, 2009.

[Pet17] Christophe Petit. Faster algorithms for isogeny problems using torsion point images. Preprint, 2017.

[Piz80] Arnold Pizer. An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra*, 64(2):340–390, 1980.

[Rón92] Lajos Rónyai. Algorithmic properties of maximal orders in simple algebras over $\mathbf{Q}$. *Comput. Complexity*, 2(3):225–243, 1992.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer, New York, 2009.

[Sto10] 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.

[Ti17] Yan Bo Ti. Fault attack on supersingular isogeny cryptosystems. In *Post-quantum cryptography*, volume 10346 of *Lecture Notes in Comput. Sci.*, pages 107–122. Springer, Cham, 2017.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[Vig80] Marie-France Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[Voi] John Voight. *Quaternion Algebras*. Version v0.9.7, September 3, 2017.

[Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. (4)*, 2:521–560, 1969.

Department of Mathematics, The Pennsylvania State University, University, Park, PA 16802, USA

E-mail address: eisentra@math.psu.edu

URL: http://www.personal.psu.edu/kxe8/

Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA 16802, USA

E-mail address: hallgren@cse.psu.edu

Department of Mathematics, The Pennsylvania State University, University, Park, PA 16802, USA

E-mail address: txm950@psu.edu

URL: http://www.personal.psu.edu/txm950/