Further Connections Between Isogenies of Supersingular Curves and Bruhat-Tits Trees

Steven Galbraith[1], Valerie Gilchrist[2], Shai Levin[1], and Ari Markowitz[1]

[1]University of Auckland, New Zealand
[2]Université Libre de Bruxelles, Belgium

November 2024

Abstract

We further explore the explicit connections between supersingular curve isogenies and Bruhat-Tits trees. By identifying a supersingular elliptic curve E over $\mathbb{F}_p$ as the root of the tree, and a basis for the Tate module $T_\ell(E)$; our main result is that given a vertex M of the Bruhat-Tits tree one can write down a generator of the ideal $I \subseteq \mathrm{End}(E)$ directly, using simple linear algebra, that defines an isogeny corresponding to the path in the Bruhat-Tits tree from the root to the vertex M. In contrast to previous methods to go from a vertex in the Bruhat-Tits tree to an ideal, once a basis for the Tate module is set up and an explicit map $\Phi : \mathrm{End}(E)\otimes_{\mathbb{Z}_\ell} \to M_2(\mathbb{Z}_\ell)$ is constructed, our method does not require any computations involving elliptic curves, isogenies, or discrete logs. This idea leads to simplifications and potential speedups to algorithms for converting between isogenies and ideals.

1 Introduction

The *supersingular ℓ-isogeny graph*; whose vertices are $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves over $\mathbb{F}_{p^2}$, and whose edges are ℓ-isogenies, is a well studied graph with various applications to cryptography, such as [4, 5, 7, 12–14].

A separable isogeny is determined up to isomorphism by its kernel, so an ℓ-isogeny $\phi : E \to E'$ is defined by a cyclic subgroup $\ker(\phi) \subset E(\overline{\mathbb{F}}_p)$ of order

*Authors listed in alphabetical order: see `https://www.ams.org/profession/leaders/CultureStatement04.pdf`. Galbraith and Levin are supported by funding from the Ministry for Business, Innovation and Employment, New Zealand. Gilchrist is supported by a FRIA grant by the National Fund for Scientific Research (F.N.R.S.) of Belgium. Markowitz is supported by the University of Auckland Doctoral Scholarship.

Date of this document: 2024-12-05.

ℓ. The Deuring Correspondence associates to an isogeny $\phi : E \to E'$ of supersingular curves an ideal I in $\mathcal{O} \cong \mathrm{End}(E)$ such that the left order of I is $\mathcal{O}$ and the right order is $\mathcal{O}' \cong \mathrm{End}(E')$. The norm of the ideal I is equal to the degree of the isogeny. It is known that an isogeny of degree ℓ^k having cyclic kernel can be represented in any of the following ways:

1. A non-backtracking walk of length k in the supersingular ℓ-isogeny graph from E to E'.
2. A cyclic subgroup of $E[\ell^k]$.
3. A maximal order $\mathcal{O}'$ in the quaternion algebra such that $[\mathcal{O} : \mathcal{O} \cap \mathcal{O}'] = \ell^k$. (See Exercise 9 of Section 23 of [21].)
4. A left $\mathcal{O}$-ideal I of norm ℓ^k.

It is well known [2, 18] that the *ℓ-adic Bruhat-Tits tree*; an infinite, rooted $(\ell+1)$-regular tree, is a covering graph of the ℓ-isogeny graph. The vertices (and edges) of such a tree may be represented with equivalence classes of matrices in $M_2(\mathbb{Q}_\ell)$, with representatives

$$\begin{pmatrix} \ell^r & 0 \\ m & \ell^s \end{pmatrix}$$

(for integers $r, s \geq 0$, $0 \leq m < \ell^s$ and $\gcd(m, \ell) = 1$), corresponding to a vertex of distance $r + s$ from the root. Whilst performing computations, such as path-finding, between vertices in the matrix description is straightforward, curiously, this is not the case in the isogeny graph. In particular, a fundamental assumption in isogeny-based cryptography is that it is computationally infeasible to find paths between arbitrary vertices for a graph of sufficient size. This problem is also equivalent to computing an effective basis of a supersingular elliptic curve's endomorphism ring, which is isomorphic to a quaternionic maximal order [22].

These reasons motivate the investigation of the explicit connections between the Bruhat-Tits tree and the supersingular ℓ-isogeny graph, for example see Amorós, Iezzi, Lauter, Martindale, and Sotáková [2]. In this work, the authors describe how to explicitly translate between non-backtracking isogenies, vertices of the Bruhat-Tits tree, and maximal orders of $B_{p,\infty}$ corresponding to endomorphism rings of supersingular elliptic curves over characteristic p. In particular, fix a curve E, and a representation for its endomorphism ring $\mathrm{End}(E) \cong \mathcal{O} \subseteq B_{p,\infty}$ as the root of the tree (which corresponds to the matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$). A representation of $B_\ell = B_{p,\infty} \otimes \mathbb{Q}_\ell$ as $M_2(\mathbb{Q}_\ell)$ is shown in [2] such that there exists a bijection between vertices in the Bruhat-Tits tree and maximal orders in B_ℓ. Recent developments have further shown this correspondence may be leveraged for applications to constructing digital signature schemes [17], and more efficient computation of endomorphism rings [9].

Our Contributions In [2] it is shown how to associate to a vertex in the Bruhat-Tits tree any of the first 3 items listed above for representing an ℓ^k-isogeny. The main contribution of this paper is to show how to include the

4th item in this picture. More precisely, we extend the work of [2] to explicitly translate between paths in the tree and ideals, fully realising the Deuring Correspondence in the Bruhat-Tits tree setting.

In particular, while [2] gives a description for translating between (1)-(3) and endomorphism rings of the image curve of the isogeny paths, we construct an efficient map which allows translating between vertices of the Bruhat-Tits tree and corresponding *kernel ideals*. This also allows a new way to go from cyclic kernels of isogenies directly to kernel ideals.

We express our main result in the following theorem.

Theorem 1 (Informal)**.** *Fix distinct primes p, ℓ and a supersingular elliptic curve E such that* $\mathrm{End}(E) \cong \mathcal{O} \subseteq B_{p,\infty}$*. Let $\theta_1, \theta_2, \theta_3, \theta_4$ be a $\mathbb{Z}$-module basis for $\mathcal{O}$. Identify the root of the ℓ-adic Bruhat-Tits tree with E. Then there exist explicitly computable matrices $M_1, \ldots, M_4$ such that, for any vertex M in the Bruhat-Tits tree of distance k from the root, any solution to the linear equations $M \equiv \sum_i \alpha_i M_i \mod \ell^{k+1}$ gives an endomorphism $\alpha = \sum_i \alpha_i \theta_i \in \mathcal{O}$ for which $I = (\alpha, \ell^k)$ is the ideal corresponding to the isogeny whose kernel is described by M via an explicitly computable basis of the Tate-module.*

Our tool may prove useful for cryptographic applications, where modern cryptographic protocols, such as [1, 3, 7, 16], make frequent use of translating between kernel-representation, as scalar multiples of a basis of $E[\ell^k]$, and ideal-representation for isogenies.

In addition we give a new method to efficiently compute the end-point elliptic curve corresponding to a long walk in the Bruhat-Tits tree (see Section 4.1) and give new translation maps between ideals and isogenies (see Sections 4.2 and 4.3).

2 Background

$\mathbb{Q}_\ell$ denotes the set of ℓ-adic rational numbers, $\mathbb{Z}_\ell$ denotes the set of ℓ-adic integers, and $v_\ell(x)$ is the ℓ-adic valuation of an ℓ-adic rational number. We write $B_{p,\infty}$ for the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞. If $\mathcal{O}$ is an order and $\alpha, \beta \in \mathcal{O}$ then we write (α, β) or $\mathcal{O}(\alpha, \beta)$ for the left-$\mathcal{O}$-ideal generated by α and β. If $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ then $\mathrm{adj}\, M = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.

2.1 Isogenies and elliptic curves

We give a brief overview of some of the relevant concepts related to isogenies and elliptic curves. For a more thorough exploration of isogenies and elliptic curves the reader can refer to the textbook from Silverman [20], and for an in-depth treatment of the isogeny graph as it relates to isogeny-based cryptography see the lecture notes from De Feo [11]. We focus entirely on the supersingular case in this paper.

Isogenies are non-constant maps between elliptic curves. It is conjectured that given two elliptic curves, finding an isogeny mapping from one to the other

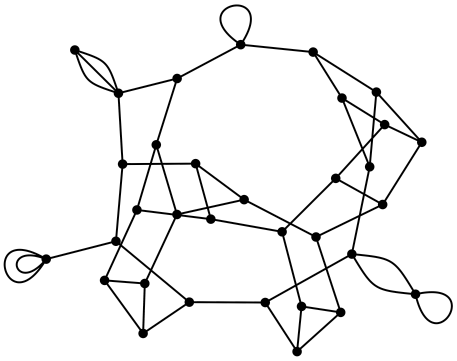

Figure 1: The supersingular 2-isogeny graph over $\mathbb{F}_{383^2}$.

is a (quantumly) hard problem. One way to think about these maps is via the *ℓ-isogeny graph*.

Definition 1. *Fix two primes $\ell < p$, $\ell \neq p$. The* supersingular ℓ-isogeny graph *is a graph whose vertex set is $\overline{\mathbb{F}}_p$-isomorphism classes of supersingular elliptic curves. The edge set is such that two vertices are connected if and only if there exists an ℓ-isogeny between the two isomorphism classes.*

In this setting, finding an isogeny of degree ℓ^k between two curves is equivalent to finding a path in the graph. Note that cycles in this graph are equivalent to *endomorphisms*, that is, isogenies whose domain and codomain are the same curve. The supersingular ℓ-isogeny graph is connected and $(\ell + 1)$-regular.

The *Deuring Correspondence* gives a direct correspondence between the world of isogenies, and that of ideals in a quaternion algebra. We present the basic ideas but for a more thorough introduction to the Deuring Correspondence see the textbook from Voight [21] or the doctoral thesis of Leroux [15].

Consider a supersingular elliptic curve, E over $\overline{\mathbb{F}}_p$. Then the endomorphism ring of E is isomorphic to a maximal order in the quaternion algebra, $B_{p,\infty}$, which is defined over $\mathbb{Q}$ and ramified at p and ∞. Thus, every other prime $\ell \neq p$ will be split in $B_{p,\infty}$, meaning $B_\ell := B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is isomorphic to $M_2(\mathbb{Q}_\ell)$.

Maximal orders $\mathcal{O}$ are 4-dimensional $\mathbb{Z}$-modules and we will often represent them by writing down a basis $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ as a $\mathbb{Z}$-module. We sometimes denote this by $\langle \theta_1, \theta_2, \theta_3, \theta_4 \rangle_{\mathbb{Z}}$.

Isogenies between elliptic curves correspond to ideals in $\mathrm{End}(E)$. Consider two (supersingular) elliptic curves, E, E', whose endomorphism rings are isomorphic to the maximal orders $\mathcal{O}, \mathcal{O}'$ respectively. Then an isogeny, $\varphi : E \to E'$ corresponds to an ideal $I_\varphi \subset \mathcal{O}$ whose left order is $\mathcal{O}$ and whose right order is $\mathcal{O}'$. The degree of the isogeny is the norm of the ideal, which is the square-root of the index $[\mathcal{O} : I_\varphi] = [\mathcal{O}' : I_\varphi]$ (see Voight [21, Proposition 16.4.2]). This notion is made explicit in the following definition.

Definition 2. *Let E be an elliptic curve such that* $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$. *Then for $\alpha \in \mathcal{O}$ where $v_\ell(\mathrm{N}(\alpha)) = k$, we define the isogeny $\phi_\alpha : E \to E'$ of degree ℓ^k by the kernel* $\ker \phi_\alpha = \{P \in E[\ell^k] \mid \alpha(P) = 0\}$. *For a given isogeny $\phi : E \to E'$, we may also refer to its kernel ideal, $I_\phi = \{\alpha \in \mathcal{O} \mid \alpha(\ker \phi) = 0\}$.*

Note that α is an endomorphism of degree $\ell^k d$ for some d co-prime to ℓ, and $\phi_\alpha : E \to E'$ is the ℓ-power part of α. So there is also an isogeny of degree d from E' back to E. We will not need any of this below, but mention it in case the reader is confused by the relationship between $\alpha : E \to E$ and $\phi_\alpha : E \to E'$.

Our results are ℓ-adic in nature so we need some definitions.

Consider the group of ℓ^n-torsion points, $E[\ell^n]$. Since $\ell \neq p$ we have $E[\ell^n] \cong \mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. The Tate module is defined to be

$$T_\ell(E) = \lim_{\leftarrow} E[\ell^n],$$

where the connecting maps are given by the multiplication by ℓ map, $[\ell]$. Note that $T_\ell(E) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ so that $T_\ell(E)$ admits a basis. This basis consists of pairs $(P_n, Q_n)_{n=1}^\infty$ where (P_n, Q_n) is a basis of $E[\ell^n]$, and $\ell P_{n+1} = P_n, \ell Q_{n+1} = Q_n$. It is immediate that $\mathrm{End}(T_\ell(E)) = M_2(\mathbb{Z}_\ell)$.

A Theorem of Tate (see [2, Section 4.2.1]) is that $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathrm{End}(T_\ell(E))$. If $\mathcal{O} = \mathrm{End}(E)$ then we will write $\mathcal{O}_\ell$ for $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$.

Lemma 1. *Let $\mathcal{O}$ be a maximal order of the quaternion algebra $B_{p,\infty}$ and I be a left or right ideal of $\mathcal{O}$. Then I is locally principal. That is, $I_\ell := I \otimes \mathbb{Z}_\ell$ is principal for all primes $\ell \neq p$, and is generated by any element $\alpha \in I$ of minimal valuation.*

Proof. Since either $\mathcal{O} = O_L(I)$ or $\mathcal{O} = O_R(I)$, by [21, Prop. 16.6.16], we have that I is invertible. Then by [21, Thm. 16.1.3] I_ℓ is principal. Following the approach in [21, 16.6.9], we see that any element of minimum valuation generates I_ℓ. □

Lemma 2. *Let $\mathcal{O}$ be a maximal order of $B_{p,\infty}$ and I be a left ideal of $\mathcal{O}$ of norm $\mathrm{N}(I) = \ell^k$. Let $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ and $I_\ell = I \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Let $\alpha \in I_\ell$ be such that $I_\ell = (\alpha)$. Let $\alpha^* \in \mathcal{O}$ be such that $\alpha^* \equiv \alpha \mod \ell^{k+1}$. Then $I = (\alpha^*, \ell^k)$.*

Proof. By Lemma 1, I_ℓ is locally principal and has a generator α such that $v_\ell(\mathrm{N}(\alpha)) = k$.

Let $\mathcal{O} = \langle \theta_1, \theta_2, \theta_3, \theta_4 \rangle_{\mathbb{Z}}$, then

$$\alpha = a_1\theta_1 + a_2\theta_2 + a_3\theta_3 + a_4\theta_4$$

for $a_1, a_2, a_3, a_4 \in \mathbb{Z}_\ell$. Now,

$$\alpha^* = a_1^*\theta_1 + a_2^*\theta_2 + a_3^*\theta_3 + a_4^*\theta_4$$

where $a_i^* = a_i \mod \ell^{k+1}$. Since $a_i^* \in \mathbb{Z}$, we have that $\alpha^* \in \mathcal{O}$, and since

$$\mathrm{N}(\alpha^*) = \mathrm{N}(\alpha) + n\ell^{k+1}$$

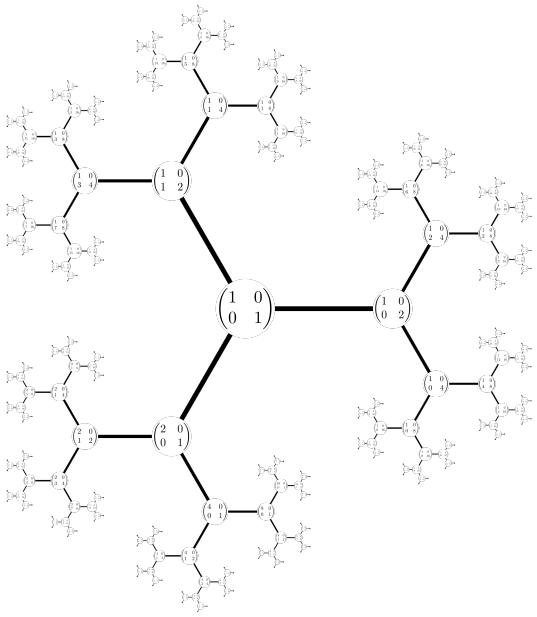

Figure 2: The 2-adic Bruhat-Tits Tree

for some $n \in \mathbb{Z}_\ell$, we have that $v_\ell(\mathrm{N}(\alpha^*)) = v_\ell(\mathrm{N}(\alpha)) = k$.

Since $\ell^k \in I$ it follows that $\alpha^* \in I_\ell \cap \mathcal{O} = I$. Hence $(\alpha^*, \ell^k) \subseteq I$.

Finally, we will show $I = (\alpha^*, \ell^k)$ by showing that $(\alpha^*, \ell^k) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = I_\ell$. This is immediate, since $\alpha^* \in I_\ell$ is an element of minimal valuation, so by Lemma 1, α^* is also a generator of $I \otimes \mathbb{Z}_\ell$. □

2.2 The Bruhat-Tits tree and the isogeny graph

The Bruhat-Tits tree is an infinite tree with vertex set $PGL_2(\mathbb{Q}_\ell)/PGL_2(\mathbb{Z}_\ell)$. Vertices also correspond to lattices. We describe how to work with the matrix representation, and then later show the connections with elliptic curves and maximal orders in the quaternion algebra $M_2(\mathbb{Q}_\ell)$. For a more thorough treatment of these topics, see [2, 9, 21].

Given matrices in $M_2(\mathbb{Q}_\ell)$, we define an equivalence relation that identifies the vertices of the Bruhat-Tits tree.

Definition 3. *Let $M, M' \in M_2(\mathbb{Q}_\ell)$. We say that M and M' are* equivalent *if there exists some $U \in GL_2(\mathbb{Z}_\ell)$ and non-zero $\lambda \in \mathbb{Q}_\ell$ such that $M = \lambda M' U$. In this case, we say $M \sim M'$. We denote an equivalence class using some representative, M, as $[M]$. We say that a representative is in* standard form *if*

$$M = \begin{bmatrix} \ell^r & 0 \\ m & \ell^s \end{bmatrix} \quad \textit{for some } m, r, s \in \mathbb{Z}_{\geq 0},\ 0 \leq m < \ell^s$$

such that $\min_{i,j} v_\ell(M_{i,j}) = 0$.

The standard form is an ℓ-adic analogue of the *Hermite normal form* for integer matrices [6, §2.4].

Lemma 3. *Every invertible matrix in $M_2(\mathbb{Q}_\ell)$ is equivalent to a unique matrix in standard form.*

Proof. We prove existence. Let $M \in \mathrm{GL}_2(\mathbb{Q}_\ell) \subset M_2(\mathbb{Q}_\ell)$. We apply a series of column operations to put M in the desired form. First, swap the columns if necessary to ensure that $v_\ell(M_{1,2}) \geq v_\ell(M_{1,1})$. Next, add a multiple of the first column to the second so that $M_{1,2} = 0$. Since the matrix has rank 2, we know $M_{2,2} \neq 0$. Multiplying the columns by units ensures that $M_{1,1}$ and $M_{2,2}$ are powers of ℓ. We then add a $\mathbb{Z}_\ell$-multiple of the second column to the first so that $0 \leq M_{2,1} < \ell^s$, where $s = v_\ell(M_{2,2})$. Finally, we multiply M by ℓ^{-a} where $a = \min_{i,j} v_\ell(M_{i,j})$, putting M into the desired form.

To prove uniqueness, suppose

$$M = \begin{bmatrix} \ell^r & 0 \\ m & \ell^s \end{bmatrix}, \quad M' = \begin{bmatrix} \ell^{r'} & 0 \\ m' & \ell^{s'} \end{bmatrix}$$

are equivalent matrices in standard form. Write $M = \lambda M' U$ for some $\lambda \in \mathbb{Q}_\ell$ and $U \in \mathrm{GL}_2(\mathbb{Z}_\ell)$. Note that $M' = \lambda^{-1} M U^{-1}$. It follows that $v_\ell(\lambda) = 0$, since otherwise the minimum valuation of the entries of either M or M' is nonzero. To ensure $M'_{1,1}$ is a power of ℓ, it must be that $\lambda = 1$. Observe that

$$U = M'^{-1} M = \begin{bmatrix} \ell^{r-r'} & 0 \\ \ell^{-s'}(m - m'\ell^{r-r'}) & \ell^{s-s'} \end{bmatrix}.$$

Since $U \in \mathrm{GL}_2(\mathbb{Z})$, it follows that $s = s'$ and $r = r'$. Hence $v_\ell(m - m') \geq s$, so $m = m'$. □

2.3 A correspondence between $B_{p,\infty} \otimes \mathbb{Q}_\ell$ and $M_2(\mathbb{Q}_\ell)$

Let $B_{p,\infty}$ be the quaternion algebra ramified at p and ∞. For example, when $p \equiv 3 \pmod 4$ we have that $B_{p,\infty}$ is generated by $\{1, i, j, k\}$, where $i^2 = -1, j^2 = -p$, and $k = ij = -ji$. Generators for $B_{p,\infty}$ in other cases are given in [2].

Define $B_\ell := B_{p,\infty} \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Since $B_{p,\infty}$ is ramified at only p and ∞, it will be split at every prime $\ell \neq p$. By definition this means that $B_\ell \cong M_2(\mathbb{Q}_\ell)$. When $p \equiv 3 \mod 4$ and $\ell > 2$ we explicitly define the bijection $\Phi_0 : B_\ell \to M_2(\mathbb{Q}_\ell)$ such that

$$1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, i \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, j \mapsto \begin{bmatrix} \sqrt{-p} & 0 \\ 0 & -\sqrt{-p} \end{bmatrix}, k \mapsto \begin{bmatrix} 0 & -\sqrt{-p} \\ -\sqrt{-p} & 0 \end{bmatrix}.$$

Here $\sqrt{-p}$ denotes an ℓ-adic number such that $x^2 = -p$. This map also respects quaternionic conjugation, since $\Phi_0(\bar{\alpha}) = \mathrm{adj}(\Phi_0(\alpha))$, where $\mathrm{adj}\, M$ is the adjugate of M (swapping the diagonal elements and negating the off-diagonals).

The trace and norm of an element $\alpha \in B_\ell$ are equal to the matrix trace and determinant (respectively) of $\Phi_0(\alpha)$ in $M_2(\mathbb{Q}_\ell)$.

3 Main results

3.1 Constructing the Localized Matrix Representation of Endomorphism Rings

Let E be a supersingular elliptic curve, $\mathcal{O} = \mathrm{End}(E) \subset B_{p,\infty}$, and $\mathcal{O}_\ell = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. By [21, Lemma 23.2.3], if $\Phi : B_{p,\infty} \otimes \mathbb{Q}_\ell \to M_2(\mathbb{Q}_\ell)$ is an isomorphism, then $\Phi(\mathcal{O}_\ell)$ is conjugate to $M_2(\mathbb{Z}_\ell)$ by an element of $\mathrm{GL}_2(\mathbb{Q}_\ell)$. For the purposes of this paper, we wish construct a representation $\Phi\colon B_\ell \to M_2(\mathbb{Q}_\ell)$ directly, such that $\Phi(\mathcal{O}_\ell) = M_2(\mathbb{Z}_\ell)$.

Lemma 4. *Let E be a supersingular elliptic curve and $\mathcal{O} = \mathrm{End}(E)$. Let $\{\theta_1, \theta_2, \theta_3, \theta_4\}$ be a $\mathbb{Z}$-module basis for $\mathcal{O}$. Fix a basis $\{R, S\}$ for the Tate module $T_\ell(E)$. For each $1 \le i \le 4$ let $a_i, b_i, c_i, d_i \in \mathbb{Z}_\ell$ be such that*

$$\theta_i(R) = a_i R + b_i S, \qquad \theta_i(S) = c_i R + d_i S.$$

Then $M_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ lies in $M_2(\mathbb{Z}_\ell)$. Consider the map

$$\Phi : \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to M_2(\mathbb{Z}_\ell)$$

defined by $\Phi(\theta_i) = M_i = \left(\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right)$ and extended by $\mathbb{Z}_\ell$-linearity. Then Φ is injective, surjective, is a ring anti-isomorphism (i.e., $\Phi(\alpha \circ \beta) = \Phi(\beta)\Phi(\alpha)$), and $\Phi(\bar{\alpha}) = \mathrm{adj}\,\Phi(\alpha)$.

Note that $\Phi(1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Proof. It is immediate from the construction that, for any $u, v \in \mathbb{Z}_\ell$, $\theta_i(uR + vS) = xR + yS$ if and only if $(x, y) = (u, v)M_i$. Hence, for any $\alpha \in \mathrm{End}(E)$ we have

$$\alpha(uR + vS) = xR + yS \qquad \text{where} \qquad (x, y) = (u, v)\Phi(\alpha). \tag{1}$$

From this it follows that

$$\Phi(\alpha \circ \beta) = \Phi(\beta)\Phi(\alpha)$$

for all $\alpha, \beta \in \mathcal{O}_\ell$.

The map Φ is injective, since if $\alpha \neq 0$ and $\Phi(\alpha) = 0$ then $\alpha(R) = \alpha(S) = 0$ and α corresponds to an isogeny of finite non-zero degree but infinite kernel.

Surjectivity follows since $\mathcal{O}_\ell$ is a maximal order, and so is $M_2(\mathbb{Z}_\ell)$. So $\Phi(\mathcal{O}_\ell)$ cannot be a sub-order of $M_2(\mathbb{Z}_\ell)$.

Finally, since $\Phi(\bar{\alpha}\alpha) = \Phi([\deg(\alpha)])$ is $\deg(\alpha)$ times an identity matrix, it follows that $\Phi(\bar{\alpha}) = \mathrm{adj}\,\Phi(\alpha)$. □

Remark 1. From the point of view of practical computations a statement like $\theta_i(R) = a_i R + b_i S$ should be interpreted as a statement about points of order ℓ^k for every k. For each k, there are compatible points R_k, S_k of order ℓ^k and integers $a_{i,k}, b_{i,k}$ such that $\theta_i(R_k) = a_{i,k} R_k + b_{i,k} S_k$ etc.

Remark 2. The representation maps described in Lemma 4 satisfy the formula

$$\Phi(\alpha \circ \beta) = \Phi(\beta)\Phi(\alpha),$$

and thus are *anti-isomorphisms*. This is a side-effect of acting on the right on row vectors, instead of acting on the left on column vectors. We choose this particular notation for matrix vertices of the Bruhat-Tits tree in order to be consistent with the prior notation of [2]. If it causes the reader distress then they may apply transposes to get a homomorphism.

The next Lemma is an immediate consequence of equation (1) in the above proof.

Lemma 5. *Let E be a supersingular elliptic curve such that* $\mathrm{End}(E) = \mathcal{O} \subset B_{p,\infty}$*, and let $\Phi : \mathcal{O} \otimes \mathbb{Z}_\ell \to M_2(\mathbb{Z}_\ell)$ be the anti-isomorphism described in Lemma 4. Then there exists a bijection $\eta : T_\ell(E) \to \mathbb{Z}_\ell^2$, such that for all $\alpha \in \mathcal{O}_\ell$, and $T \in T_\ell(E)$:*

$$\eta(\alpha(T)) = \eta(T) \cdot \Phi(\alpha). \tag{2}$$

This map also respects the reduction map from $T_\ell(E)$ to $E[\ell^k]$ (i.e., it also holds for $T \in E[\ell^k]$).

Proof. Let R, S be a basis for $T_\ell(E)$. As explained above, such a choice of basis defines a map $\Phi : \mathcal{O} \otimes \mathbb{Z}_\ell \to M_2(\mathbb{Z}_\ell)$.

Define $\eta(R) = (1, 0)$ and $\eta(S) = (0, 1)$. Then, as explained, for any $u, v \in \mathbb{Z}_\ell$ then $\theta_i(uR + vS) = xR + yS$ if and only if $(x, y) = (u, v)M_i$. By $\mathbb{Z}_\ell$-linearity since any $\alpha \in \mathcal{O}_\ell$ is a $\mathbb{Z}_\ell$-linear combination of the θ_i, we have that Equation (2) holds. □

3.2 Equivalence of isogenies from matrices and quaternions

Given a curve E, it's endomorphism right $\mathcal{O}$ and the representation Φ into $M_2(\mathbb{Z}_\ell)$, we now explain how to translate between different representations of vertices of the Bruhat-Tits tree: matrices, endomorphisms generating principal ideals, and their corresponding isogenies.

Fix a root vertex of the tree E such that $\mathrm{End}(E) = \mathcal{O} = \langle \theta_1, \theta_2, \theta_3, \theta_4 \rangle_\mathbb{Z}$. Let I_1 be a left-$\mathcal{O}$-ideal of norm ℓ^k for some integer k, such that I_1 does not contain (ℓ). Such an ideal corresponds to an ℓ^k-isogeny with cyclic kernel, and therefore to a vertex in the Bruhats-Tits tree that is at distance k from the root vertex, E. Then, by Lemma 1, $I_1 \otimes \mathbb{Z}_\ell \subset \mathcal{O} \otimes \mathbb{Z}_\ell$ is a principal ideal.

We now state our main result, which is that our representation Φ allows us to efficiently translate between ideals and kernels via vertices of the Bruhat-Tits tree.

Theorem 2. *Let E be a supersingular elliptic curve such that* $\mathrm{End}(E) = \mathcal{O} = \langle \theta_1, \theta_2, \theta_3, \theta_4 \rangle_\mathbb{Z}$ *for $\theta_i \in B_{p,\infty}$, and let $\Phi : \mathcal{O} \otimes \mathbb{Z}_\ell \to M_2(\mathbb{Z}_\ell)$, and $\eta : T_\ell(E) \to$*

$\mathbb{Z}_\ell^2$ *be isomorphisms*[1] *such that Equation* (2) *holds. Then there exists a basis* $P, Q \in T_\ell(E)$ *such that every standard form matrix,*

$$M = \begin{bmatrix} \ell^r & 0 \\ m & \ell^s \end{bmatrix} \quad m, r, s \in \mathbb{Z}_{\geq 0},\ k = r + s$$

corresponds to a locally principal ideal generated by $\alpha = \Phi^{-1}(M) \mod \ell^{k+1}$*, which is the kernel ideal of an isogeny* $\phi_\alpha : E \to E'$ *given by the kernel:*

$$\ker \phi_\alpha = \langle \ell^r P_k + mQ_k, \ell^s Q_k \rangle,$$

where P_k *and* Q_k *are the projections of* P *and* Q *to* $E[\ell^k]$*.*

Proof. Let $\alpha = \Phi^{-1}(M) \mod \ell^{k+1}$. We note that:

$$\ker \phi_\alpha = \ker \alpha \cap E[\ell^k] = \bar{\alpha}(E[\ell^k])$$

Hence, $\bar{\alpha}(R_k) \in \ker \phi_\alpha$ for all $R_k \in E[\ell^k]$. Since the matrix M has determinant ℓ^k, we have that $v_\ell(\alpha) = k$ and by Lemma 1 α generates the kernel ideal corresponding to the isogeny ϕ_α.

By Lemma 5, we know that the map $\eta : T_\ell(E) \to \mathbb{Z}_\ell^2$ explains the action of $\Phi(\alpha)$ on $T_\ell(E)$. Hence,

$$\bar{\alpha}(R_k) = \eta^{-1}(\eta(R_k) \cdot \operatorname{adj} M)$$

for all $R_k \in E[\ell^k]$, where

$$\operatorname{adj} M = \begin{pmatrix} \ell^s & 0 \\ -m & \ell^r \end{pmatrix}.$$

Let $P = \eta^{-1}(0, -1)$ and $Q = \eta^{-1}(1, 0)$. THen

$$\bar{\alpha}(P) = \eta^{-1}(\eta(P) \operatorname{adj} M) = \eta^{-1}((0, -1) \operatorname{adj} M) = \eta^{-1}(m, -\ell^r) = \ell^r P + mQ$$

and

$$\bar{\alpha}(Q) = \eta^{-1}((1, 0) \operatorname{adj} M) = \ell^s Q.$$

Hence, $\ker(\phi_\alpha) = \bar{\alpha}(E[\ell^k]) = \langle \bar{\alpha}(P), \bar{\alpha}(Q) \rangle = \langle \ell^r P + mQ, \ell^s Q \rangle$. □

Remark 3. Note that in our applications we will always have $r = 0$ or $s = 0$, and when $r = 0$ then $m = 0$. Hence the group $\langle \ell^r P + mQ, \ell^s Q \rangle$ can always we written as

$$\langle \ell^r P + (m + \ell^s) Q \rangle.$$

We use this formulation in our algorithms.

Our representation map Φ allows us to go directly between $\mathbb{Z}_\ell$-modules: $\mathcal{O}_\ell$ and $M_2(\mathbb{Z}_\ell)$. However, when $p = 3 \mod 4$ and $\mathcal{O} = \langle \theta_1, \theta_2, \theta_3, \theta_4 \rangle_\mathbb{Z}$ where $v_\ell(\theta_i) \geq 0$ for all θ_i's, then simply choosing $\Phi = \Phi_0$ is sufficient, where Φ_0 is the isomorphism of quaternion algebras from Section 2.3. We show a special case for this in the example below.

[1] More precisely, Φ is an anti-isomorphism. See Remark 2.

Example 1. Let $p = 3 \mod 4$ and $\ell \geq 3$. Let $i^2 = -1$, $j^2 = -p$ in the quaternion algebra $B_{p,\infty}$. Consider E_0 such that $\mathrm{End}(E_0) = \mathcal{O}_0 = \langle 1, i, \frac{i+j}{2}, \frac{1+ij}{2} \rangle$. We choose the representation Φ_0 from Section 2.3, which maps $\mathcal{O}_0$ to $M_2(\mathbb{Z}_\ell)$ when $\ell \neq 2$.

We show how to compute this representation using the method of Lemma 4.

Let $R \in T_\ell(E)$ be such that $\langle R \rangle \cap E[\ell]$ is non-trivial. Further let R be an eigenvector of j with eigenvalue $\lambda = \sqrt{-p}$. Let $S = i(R)$. Note that

$$j(S) = j(i(R)) = -i(j(R)) = -i(\lambda R) = -\lambda i(R) = -\lambda S,$$

hence S is an eigenvector of j with eigenvalue $-\lambda$. It also follows that $\{R, S\}$ is a basis for $T_\ell(E)$.

Following the method in Lemma 4 we have $\Phi(j) = \left(\begin{smallmatrix} \lambda & 0 \\ 0 & -\lambda \end{smallmatrix}\right)$, $\Phi(i) = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. One sees these are the same matrices as written down in Section 2.3, so $\Phi = \Phi_0$.

Defining M as

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \alpha_1 \Phi(\theta_1) + \alpha_2 \Phi(\theta_2) + \alpha_3 \Phi(\theta_3) + \alpha_4 \Phi(\theta_4) \tag{3}$$

where $a, b, c, d \in \mathbb{Z}_\ell$. We will show that $\Phi^{-1}(M) \in \mathcal{O}_\ell$, and hence confirm that Φ is surjective.

We see that

$$\begin{aligned} a &= \alpha_1 + \frac{\alpha_3}{2}\sqrt{-p} + \frac{\alpha_4}{2}, & b &= \alpha_2 + \frac{\alpha_3}{2} - \frac{\alpha_4}{2}\sqrt{-p}, \\ c &= -\alpha_2 - \frac{\alpha_3}{2} - \frac{\alpha_4}{2}\sqrt{-p}, & d &= \alpha_1 - \frac{\alpha_3}{2}\sqrt{-p} + \frac{\alpha_4}{2}. \end{aligned}$$

Solving this system of equations, we obtain

$$\begin{aligned} \alpha_1 &= \frac{(a+d)\sqrt{-p} + b + c}{2\sqrt{-p}}, & \alpha_2 &= \frac{(b-c)\sqrt{-p} - a + d}{2\sqrt{-p}}, \\ \alpha_3 &= \frac{a-d}{\sqrt{-p}}, & \alpha_4 &= \frac{-b-c}{\sqrt{-p}}. \end{aligned}$$

Hence, the α_i's will all be in $\mathbb{Z}_\ell$ when $\ell \neq 2$ (and Φ is clearly surjective). Next, since $i, j \in \mathcal{O}$ we may define the map $\eta : T_\ell(E) \to \mathbb{Z}_\ell^2$ in a more convenient way.

Let $v = (1, 0)$ be an eigenvector of $\Phi(j)$ with eigenvalue λ, and let $w = v\Phi(i) = (0, 1)$. By the same reasoning as above, w is an eigenvector of $\Phi(j)$ with eigenvalue $-\lambda$. Let $\eta \colon T_l(E) \to \mathbb{Z}_l^2$ be the linear isomorphism such that $\eta(R) = v$ and $\eta(S) = w$. Now, by construction, Equation (2) holds for R, S and $\alpha \in \{1, i, j, ij\}$. Hence, by $\mathbb{Z}_\ell$-linearity (and since $\ell \neq 2$), the equation holds for all $T_\ell(E)$ and $\mathcal{O}$. Now setting $P = \eta^{-1}(0, -1) = -S, Q = \eta^{-1}(1, 0) = R$ we may now apply the machinery of Theorem 2 for our needs.

Let $P = \eta^{-1}(0, -1) = -S$ and $Q = \eta^{-1}(1, 0) = R$. Given a matrix $M = \left(\begin{smallmatrix} 1 & 0 \\ m & \ell^k \end{smallmatrix}\right)$ corresponding to an endomorphism α we have

$$\alpha(P + [m]Q) = \alpha([m]R - S)$$

which corresponds to

$$(m, -1) \left(\begin{smallmatrix} 1 & 0 \\ m & \ell^k \end{smallmatrix} \right) = (0, 0).$$

This confirms that $P + [m]Q$ is the kernel of the isogeny ϕ_α corresponding to the given vertex in the Bruhat-Tits tree.

Example 2. As in the previous example, let $p = 3 \mod 4$ and $\mathrm{End}(E_0) = \mathcal{O}_0 = \langle 1, i, \frac{i+j}{2}, \frac{1+ij}{2} \rangle$; but this time, let $\ell = 2$. Now Φ_0 does not send $\mathcal{O} \otimes \mathbb{Z}_2$ to $M_2(\mathbb{Z}_2)$. Hence, we must construct Φ as in Lemma 4. For this, we choose a concrete example. Recall that

$$E_0 : y^2 = x^3 + x,$$

we choose the Mersenne prime $p = 2^{31} - 1$, working over $\mathbb{F}_{p^2} \cong \mathbb{F}_p[i]$ (where $i^2 = -1$) and projecting $T_2(E)$ onto $E[2^{30}]$. We chose an arbitrary basis

$$R_{30} = (1837916331 \cdot i + 985307470, 1546747127 \cdot i + 1565582437),$$

$$S_{30} = (1319845929 \cdot i + 78610875, 1085330991 \cdot i + 1076131300)$$

such that $\langle R_{30}, S_{30} \rangle = E[2^{30}]$. Now, by computing the actions of the generators of $\mathcal{O}$ on this basis, and solving the two-dimensional discrete logarithm, we obtain that Φ modulo 2^{31} is the linearisation of the map which sends:

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad i \mapsto \begin{pmatrix} 978557856 & 48674073 \\ 703423703 & 95183968 \end{pmatrix}$$

$$\frac{i+j}{2} \mapsto \begin{pmatrix} 364000032 & 305689881 \\ 1011325952 & 709741792 \end{pmatrix} \quad \frac{1+ij}{2} \mapsto \begin{pmatrix} 201420800 & 402803584 \\ 317984800 & 872321025 \end{pmatrix}$$

Next, as a sanity check of Theorem 2, we compute $a, b, c, d \in \mathbb{Z}/2^{31}\mathbb{Z}$ such that:

$$\begin{pmatrix} 2^r & 0 \\ m & 2^s \end{pmatrix} = a\Phi(1) + b\Phi(i) + c\Phi\left(\frac{i+j}{2}\right) + d\Phi\left(\frac{1+ij}{2}\right) \mod 2^{30}.$$

Which corresponds to an endomorphism:

$$\alpha = a + bi + c\left(\frac{i+j}{2}\right) + d\left(\frac{1+ij}{2}\right) \in \mathcal{O}.$$

Let $P_{30} = -S_{30}, Q_{30} = R_{30}$ as in Theorem 2. We now consider an arbitrary matrix M, such as $r = 0, s = 30, m = 3$. By simple linear algebra we obtain the coefficients:

$$(a, b, c, d) = (737652097, 866413973, 363817451, 672179455).$$

The kernel of the isogeny $\phi_\alpha : E \to E'$ is generated by

$$K = P_{30} + 3Q_{30} = (879099442 \cdot i + 324669990, 1472827626 \cdot i + 1784986333).$$

Lastly, $v_\ell(\mathrm{N}(\alpha)) = 30$ and it can be verified that $\alpha(K) = (0 : 1 : 0)$, and hence α is a generator for $I_{\phi_\alpha} \otimes \mathbb{Z}_\ell$.

Implementation As in Example 2, we ran sagemath experiments for computing Φ (working in projections onto $\mathbb{Z}/2^{k+1}\mathbb{Z}$) using code adapted from the QFESTA implementation[2]. The experiments executed successfully for a range of cryptographically sized primes, taking around 1 second for $\log p \approx 256$. In order to avoid working over an extension of $\mathbb{F}_{p^2}$, given that $p = 2^a f - 1$, we work over the 2^k torsion for $k < a$ since it is not true in general that for $\mathbb{F}_{p^2}$-rational $P \in E[2^a]$, there exists a $\mathbb{F}_{p^2}$-rational Q such that $2Q = P$, and solving for such a Q is necessary in the evaluation of the fractional generators of $\mathcal{O}$.

4 Applications to Isogeny and Ideal Translations

Our main contribution in this paper is to explain how to directly pass between vertices in the Bruhat-Tits tree (represented by matrices in standard form) and $\mathcal{O}$-ideals, where $\mathcal{O}$ is the endomorphism ring of a supersingular elliptic curve E identified with the root of the tree. In this section we show how this connection allows to simplify some algorithms for passing between ideals and isogenies.

Our first novel application (Section 4.1) is primarily a theoretical one. Let E be a supersingular elliptic curve identified with the root $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in the ℓ-adic Bruhat-Tits tree. Given a vertex in the tree at distance k from the root, a natural computational task is to compute the image of the corresponding ℓ^k-isogeny from E in the isogeny graph. Such a task would be required, for example, in the implementation of the signature scheme outlined in [17, p. 35]. Currently the most efficient way to determine the j-invariant of the image curve is by Leroux [15, Algorithm 23]. It requires $poly(k)$ operations. The algorithm breaks up the isogeny into $O(k/f)$ distinct ℓ^f-isogenies, and computed each step by determining some information about the next curve in the path (e.g., its endomorphism ring and the connecting ideal). This involves evaluating endomorphisms on points of order ℓ^f.

Our method, in some cases at least, allows to directly go from the matrix corresponding to the vertex to the ideal $I \subseteq \mathcal{O}$. One can then smooth the ideal using KLPT and then compute the image of the isogeny efficiently in a manner that is independent of k. Of course, the complexity must still grow linearly with k, since the input size is $O(k)$ bits and the norm of the ideal I is ℓ^k.

Our second contribution in this section is to discuss how the matrix representation techniques from Section 3.1 can be used in translation algorithms between isogenies and quaternionic ideals. The IsogenyToIdeal and IdealToIsogeny subroutines in SQIsign [7] tackle exactly this problem. Most notably, our versions of these algorithms (see Section 4.2 and Section 4.3) differ from the prior versions in that they avoid the explicit evaluation of endomorphisms on points once the basis for the Tate module is set up.

[2] Available at `https://github.com/hiroshi-onuki/QFESTA-SageMath`

4.1 Computing elliptic curves corresponding to vertices in Bruhat-Tits tree

Using the explicit correspondence between vertices in the Bruhat-Tits tree and quaternion ideals defined in Section 3.1 we show how to take (long) walks in the isogeny graph.

Fix a supersingular starting curve E_0 with endomorphism ring $\mathcal{O}_0$, that is sufficiently nice (for example, has basis containing i, j with $i^2 = -1$ and $j^2 = -p$). There exists an eigenbasis (R, S) for the Tate module $T_l(E_0)$ with respect to the choice of generators for $\mathcal{O}_0$. This is defined implicitly but is not efficiently computable since points of order ℓ^k may be defined over large field extensions.

Consider the vertex in the Bruhat-Tits tree

$$v = \begin{bmatrix} 1 & 0 \\ m & \ell^k \end{bmatrix},$$

where k is arbitrarily large. Since $0 \leq m < \ell^k$ the input size is $O(k)$ bits for fixed ℓ. This vertex corresponds to a path in the isogeny graph starting at E_0 and ending at another supersingular elliptic curve E_1.

One way to compute the j-invariant of E_1 is to compute a basis (P, Q) for the Tate module and to compute the point $T = P + mQ$, and use it to compute $E_1 = E_0/\langle T \rangle$. From here the j-invariant can be computed. This approach is infeasible in general since the computations are likely to be over a large field extension in order for T to be defined. Other methods are described in the literature such as in the thesis of Leroux [15, Algorithm 23], where, given an ideal I of norm ℓ^k, the algorithm returns the corresponding isogeny in time polynomial in $O(k)$ (when all other parameters are fixed). Notably, this algorithm requires knowledge of an ideal and isogeny mapping the left order of I back to a special endomorphism ring $\mathcal{O}_0$. With this extra information, and after breaking up the ideal I into a filtration of ideals of the form $I = I_v \subset \cdots \subset I_0$, where I_0 is exactly the left order of I, the algorithm progressively applies KLPT [14] to these smaller ideals and converts them to isogenies with the IdealToIsogeny algorithm. This is necessary so that the kernels of the smaller ideals are defined over a small enough field extension.

We now sketch our new approach to this problem, making use of Theorem 2 and the results from Section 3.2. Given the vertex M in the Bruhat-Tits tree, we use linear algebra modulo ℓ^{k+1} to write down $\alpha = a + bi + cj + dij \in \mathcal{O}$. Here $a, b, c, d \in \mathbb{Z}_{\ell^{k+1}}$ so the representation has size $O(k)$ bits and requires $O(k^2)$ bit operations to compute using naive arithmetic (asymptotically one could use quasi-linear arithmetic to compute α in $\tilde{O}(k)$ operations). From here, we can compute a $\mathbb{Z}$-basis for the ideal $I = (\alpha, \ell^k)$ by taking powers of α. Note that all integers are modulo ℓ^{k+1} so the size of integer coefficients does not blow up. One then performs lattice basis reduction on this ideal in time $O(k^2)$ (or quasi-linear using fast arithmetic) since the lattice dimension is 4.

At this stage we have a basis for the ideal I and can apply the method of [14, Section 3.1] (generating a random small element of the ideal) to obtain

Algorithm 1: NewIsogenyToIdeal

Input : E, $\mathcal{O} = \mathrm{End}(E)$, ℓ, k, $T \in E[\ell^k]$
Output: kernel ideal I_ϕ where $\phi : E \to E/\langle R \rangle$

1 Compute basis R, S of $E[\ell^k]$ and corresponding map $\Phi : \mathcal{O} \otimes_{\mathbb{Z}} (\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \to M_2(\mathbb{Z}/\ell^{k+1}\mathbb{Z})$, as in Section 3.2.
2 Compute P, Q as in Theorem 2.
3 Compute discrete log to get a, b such that $T = [a]P + [b]Q$
4 Compute associated vertex M in Bruhat-Tits tree in standard form
5 Compute $\alpha = \Phi^{-1}(M)$, set $\alpha^\star = \alpha \mod \ell^{k+1}$.
6 **return** $(\alpha^\star, \ell^k)$

an equivalent ideal I' of prime norm bounded as $O(p)$. The operations are all $O(k^2)$ or quasi-linear bit operations and the output is now independent of k.

Once the ideal I' is computed, we apply KLPT to convert I' to an ideal of smooth norm. This makes it possible to then evaluate the end point of the corresponding isogeny. The isogeny computations have complexity independent of the original value k, and so can be considered as $O(1)$. So we have very efficiently computable maps from v to an ideal, and hence from a Bruhat-Tits tree vertex to an elliptic curve.

The key point about our approach is that we never need to write down points of order ℓ or a power of ℓ, nor compute the map Φ.

Furthermore, this also gives an efficient method for computing a maximal order isomorphic to $\mathcal{O}_1$, the order corresponding to the vertex v in the tree.

4.2 A new IsogenyToIdeal algorithm

The IsogenyToIdeal problem is to go from a cyclic ℓ^k-isogeny (e.g., a point of order ℓ^k in E) to an ideal in $\mathcal{O} = \mathrm{End}(E)$ such that I is the ideal of the isogeny. It is known that the ideal will always be of the form (α, ℓ^k) and have $\mathrm{N}(I) = \ell^k$.

The main idea is to use the map $\Phi : \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \to M_2(\mathbb{Z}_\ell)$ restricted to the ℓ^{k+1} part. If $M \in M_2(\mathbb{Z})$ is a matrix in standard form representing the ℓ^k-isogeny, then the ideal is generated by any $\alpha \in \mathcal{O}$ such that $\Phi(\alpha) \equiv M \pmod{\ell^{k+1}\mathcal{O}}$. Due to Lemma 5, computing such an α is just linear algebra modulo ℓ^{k+1}: we compute 4 integers a, b, c, d such that $M \equiv a\Phi(\theta_1) + b\Phi(\theta_2) + c\Phi(\theta_3) + d\Phi(\theta_4) \pmod{\ell^{k+1}}$, and then $\alpha = a\theta_1 + b\theta_2 + c\theta_3 + d\theta_4$. It follows that the norm of α is congruent modulo ℓ^{k+1} to the determinant of M, which is ℓ^k. Hence, given a curve E and effective knowledge of its endomorphism ring $\mathcal{O}$, we are able to efficiently translate kernels of cyclic ℓ^k isogenies in $E[\ell^k]$ to generators for their kernel ideals in $\mathcal{O}$. We outline this approach in Algorithm 1. Note that, since we are assuming the input isogenies are cyclic, we represent the isogenies by a point $T \in E[\ell^k]$ which generates their kernel.

Algorithm 2: KernelToIdeal (Leroux' thesis)

Input : A point P of order D in $E[D]$
Output: The ideal $I(P)$

1 Compute $\iota : \mathrm{End}(E) \hookrightarrow B_{p,\infty}$ and set $\mathcal{O} = \iota(\mathrm{End}(E))$
2 Compute basis $\theta_1, \theta_2, \theta_3, \theta_4$ of $\mathrm{End}(E)$ such that the norm of each θ_i is coprime to D
3 Find i, j such that $\theta_i(P), \theta_j(P)$ is a basis of $E[D]$
4 Take $k \neq i, j$ and compute a, b such that $\theta_k(P) = a\theta_i(P) + b\theta_j(P)$
5 Compute $\alpha = \iota(\theta_k - a\theta_i - b\theta_j)$
6 **return** (α, D)

Complexity. For comparison we use the KernelToIdeal algorithm from Leroux' thesis [15, Algorithm 20], which is in turn based on an algorithm from Galbraith, Petit, and Silva (GPS) [13]. The algorithm is given in Algorithm 2. Leroux proves this algorithm has complexity $O(\sqrt{D})$, where D is the degree of the isogeny. The bottleneck here is the discrete logarithm computation. When D is power-smooth then one uses Pohlig-Hellman to compute the discrete logs efficiently. Hence, it requires the input isogeny to have smooth degree to be practical.

Our approach, Algorithm 1, also requires a discrete logarithm computation on elliptic curve points, which will be the bottleneck of the algorithm. In the case $D = \ell^k$ both methods require k iterations of solving a two-dimensional discrete logarithm problem in $E[\ell]$. When considering concrete costs, however, Algorithm 1 avoids the evaluations of endomorphisms that are necessary in Algorithm 2. Instead, the non-dominating costs are only linear algebra.

4.3 A new IdealToIsogeny algorithm

Suppose, given a curve of endomorphism ring $\mathcal{O}$ and a left $\mathcal{O}$-ideal $I = \mathcal{O}(\alpha, \ell^k)$, that we would like to determine the ℓ^k-isogeny whose kernel ideal corresponds to I via the Deuring correspondence. This is possible using the techniques from Section 3.1, and in particular, Theorem 2.

We begin by fixing our torsion basis, which in nice cases is defined in terms of the eigenvalues of Frobenius. These eigenvalues can be computed using the characteristic polynomial of Frobenius. From here we require the unique linear combination of the torsion basis that will provide us with our kernel generator. To obtain this information we use α to identify its node in the Bruhat-Tits tree, and compute its Tate module labeling. The algorithm is outlined in Algorithm 3.

Complexity. Again we turn to Leroux's thesis [15, Algorithm 19] as a baseline for comparison. We recall the algorithm in Algorithm 4. Leroux proves that this algorithm has complexity $O(\sqrt{D})$, where D is the norm of the input ideal.

Algorithm 3: NewIdealToIsogeny

Input : E, $\mathcal{O} = \mathrm{End}(E)$, $\alpha \in \mathcal{O}$ such that (α, ℓ^k) is an ideal in $\mathcal{O}$ of norm ℓ^k and cyclic kernel
Output: kernel representation of isogeny corresponding to ideal under Deuring correspondence

1 Compute basis R, S for $E[\ell^k]$ and corresponding map $\Phi : \mathcal{O} \otimes_{\mathbb{Z}} (\mathbb{Z}/\ell^{k+1}\mathbb{Z}) \to M_2(\mathbb{Z}/\ell^{k+1}\mathbb{Z})$ and mapping η as in Section 3.1.
2 Compute the matrix $M := \Phi(\alpha)$.
3 Reduce M to standard form $\left(\begin{smallmatrix} \ell^r & 0 \\ m & \ell^s \end{smallmatrix}\right)$.
4 Compute $P = \eta^{-1}(0, -1), Q = \eta^{-1}(1, 0)$.
5 Compute $R = [\ell^r]P + [m + \ell^s]Q$.
6 **return** R

Algorithm 4: IdealToKernel (Leroux' thesis)

Input : A curve E_1, a cyclic ideal $I \subset B_{p,\infty}$
Output: A generator P_I of $E_1[I]$

1 Compute $D = \mathrm{N}(I)$ and $\mathcal{O}_1 = \mathcal{O}_L(I)$.
2 Compute a generator $\alpha \in I$ such that $I = \mathcal{O}_1\langle \alpha, D \rangle$.
3 Compute a basis P, Q of $E_1[D]$.
4 Compute $R = \alpha(P), S = \alpha(Q)$.
5 **if** *The order of* $R < D$ **then**
6 Swap P with Q and R with S
7 Compute $a = \mathsf{DLP}_D(R, S)$.
8 **return** $[a]P - Q$

In Algorithm 3 the bottle neck is Step 1, where we must compute the ℓ^k-torsion basis. This can be done (as a precomputation) by randomly sampling points from the curve, and multiplying them by a scalar (cofactor). Though we also require the two points to be linearly independent, this is still done easily in practice with only a few tries necessary. We assume for now that the torsion basis exists over a small extension field of the base field, thus the complexity of both this step and Algorithm 3 is $O(\log(p))$.

Powersmooth norms. Suppose we are given a left $\mathcal{O}_0$ and right $\mathcal{O}_1$ ideal, $I = (N, \alpha)$, where the prime factorisation of $\mathrm{N}(I) = N = \ell_1^{k_1} \dots \ell_n^{k_n}$. Then we may relate this to an isogeny $\phi_I : E_0 \to E_1$ via the Deuring Correspondence in the usual way, where $\mathrm{End}(E_i) \cong \mathcal{O}_i$ for $i = 1, 2$. So far we have been representing the kernel subgroup using one single generator, but we can also choose to represent it by a list of generators, one for each $\ker \phi_I \cap E[\ell_i^{k_i}]$. By CRT,

this list can be used to generate the entire kernel subgroup. This representation of an isogeny was called the *multigenerator representation* in the recent survey from Robert [19]. To compute the multigenerator representation of ϕ_I using Algorithm 3, we can input the ideal $(\ell_i^{k_i}, \alpha)$ (instead of the original ideal (N, α)) for each i. This gives us our desired list of generators.

Note that while Algorithms 1 and 3 work for any prime power of the form ℓ^k, in practice the speed of Algorithm 3 does not scale well for large ℓ^k. This is because we must compute ℓ^k-torsion bases, which for large k are likely to exist only over a very large field extension of $\mathbb{F}_{p^2}$. Hence, as with most previous works, we only recommend to use Algorithms 1 and 3 in the power-smooth case.

Remark 4. In Deuring for the People [10], Komada Eriksen, Panny, Sotáková, and Veroni give algorithms for the translations between ideals and isogenies, but focus on generalizing the context. In their IdealToIsogeny algorithm they deviate from previous state-of-the-art in that they avoid all of the point divisions by computing a torsion group that is slightly larger than necessary. Like Algorithm 3, their algorithm also has $O(\log(p))$ complexity and similarly avoids using any discrete logarithms. We expect that any difference in performance would come from the fact that the arithmetic in the non-dominating subroutines in Algorithm 3 is mainly linear algebra, avoiding endomorphism evaluation and thereby simplifying the overall algorithm.

5 Conclusion

Previous work [2] explored the connection between the Bruhat-Tits tree, the ℓ-isogeny graph, and the world of quaternion algebras. In this work we explain how to fit ideals into this picture, and in Section 3 show that one can compute the ideal corresponding to an isogeny using simple linear algebra. Then in Section 4 we showed how this mapping can be used to translate between a given ideal and isogeny, a computation that has been the bottleneck of algorithms in the NIST candidate signature scheme, SQIsign [7].

It remains unclear exactly how our algorithms would impact the efficiency of SQIsign, and tackling this question is outside of the scope of our work. In particular, due to the quick evolution of the scheme and now the several variants, changing the IdealToIsogeny algorithm in the overall signature is a highly non-trivial task, with many trade-offs to consider. Some other works that use IdealToIsogeny include the signature scheme GPS [13], the cryptanalytic work on CGL in [8], and the recent timed commitment scheme [1]. We leave the exploration of how Algorithms 1 and 3 impact the efficiency of these schemes as future work.

References

[1] Knud Ahrens. SIGNITC: Supersingular isogeny graph non-interactive timed commitments. Cryptology ePrint Archive, Paper 2024/1225, 2024.

[2] Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, and Jana Sotáková. *Explicit Connections Between Supersingular Isogeny Graphs and Bruhat–Tits Trees*, pages 39–73. Springer International Publishing, Women in Numbers Europe III: Research Directions in Number Theory, 2021.

[3] Andrea Basso, Luca De Feo, Pierrick Dartois, Antonin Leroux, Luciano Maino, Giacomo Pope, Damien Robert, and Benjamin Wesolowski. SQIsign2D-west: The fast, the small, and the safer. Cryptology ePrint Archive, Paper 2024/760, 2024.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an efficient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, *ASIACRYPT 2018*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

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

[6] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[7] Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. SQISign: compact post-quantum signatures from quaternions and isogenies. *ASIACRYPT 2020*, 2020.

[8] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: Reductions and solutions. In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018*, volume 10822 of *Lecture Notes in Computer Science*, pages 329–368. Springer, 2018.

[9] Kirsten Eisenträger and Gabrielle Scullard. Connecting Kani's lemma and path-finding in the Bruhat-Tits tree to compute supersingular endomorphism rings. *CoRR*, abs/2402.05059, 2024.

[10] Jonathan Komada Eriksen, Lorenz Panny, Jana Sotáková, and Mattia Veroni. Deuring for the people: Supersingular elliptic curves with prescribed endomorphism ring in general characteristic. LuCaNT, 2023.

[11] Luca De Feo. Isogeny graphs in cryptography, July 2019.

[12] Luca De Feo, Tako Boris Fouotsa, Péter Kutas, Antonin Leroux, Simon-Philipp Merz, Lorenz Panny, and Benjamin Wesolowski. SCALLOP: scaling the csi-fish. In Alexandra Boldyreva and Vladimir Kolesnikov, editors, *PKC 2023*, volume 13940 of *Lecture Notes in Computer Science*, pages 345–375. Springer, 2023.

[13] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *J. Cryptol.*, 33(1):130–175, 2020.

[14] 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.

[15] Antonin Leroux. *Quaternion algebras and isogeny-based cryptography*. PhD thesis, École Polytechnique, 2022.

[16] Antonin Leroux. Verifiable random function from the deuring correspondence and higher dimensional isogenies. Cryptology ePrint Archive, Paper 2023/1251, 2023.

[17] Chloe Martindale. A new post-quantum digital signature scheme, 2023. presentation at SIAM-AG 2023, TU Eindhoven, slides available at `https://www.martindale.info/talks/SIAM.pdf`.

[18] Piermarco Milione. *Shimura curves and their p-adic uniformizations*. PhD thesis, Universitat de Barcelona, 2015.

[19] Damien Robert. On the efficient representation of isogenies (a survey). Number-Theoretic Methods in Cryptology, 2024.

[20] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate texts in mathematics*. Springer, 1986.

[21] John Voight. *Quaternion algebras*. Number 288 in Graduate texts in mathematics. Springer.

[22] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 1100–1111, 2022.