The Supersingular Isogeny Path and Endomorphism Ring Problems: Unconditional Reductions

MAHER MAMAH

Department of Mathematics, The Pennsylvania State University, Univeristy Park, USA

Abstract. In this paper we study several computational problems related to current post-quantum cryptosystems based on isogenies between supersingular elliptic curves. In particular we prove that the supersingular isogeny path and endomorphism ring problems are unconditionally equivalent under polynomial time reductions. We show that access to a factoring oracle is sufficient to solve the Quaternion path problem of KLPT and prove that these problems are equivalent, where previous results either assumed heuristics or the generalised Riemann Hypothesis (GRH). Consequently, given Shor's quantum algorithm for factorisation, our results yield unconditional quantum reductions between the isogeny path and EndRing problem. Recently these reductions have become foundational for the security of isogeny-based cryptography.

1. Introduction

Isogeny-based cryptography has gained increasing attention in recent years due to its potential resistance to quantum computers. While polynomial-time quantum algorithms are known to compromise widely used public key cryptosystems like RSA and Elliptic Curve Cryptography (ECC), the best-known classical and quantum algorithms for breaking certain isogeny-based schemes still require exponential time. The security of several isogeny-based encryption schemes primarily hinges on a presumed hard problem: finding an isogeny between two arbitrary supersingular elliptic curves known as *the supersingular isogeny path problem.*

As the range of primitives that can be derived from isogenies continues to grow, new problems are emerging. One such important problem is what we call the *Endomorphism ring problem*, denoted EndRing, which asks to compute the ring of endomorphisms of a supersingular elliptic curve E. This problem has been studied since the time of Kohel [Koh96] and has recently gaind considerable attention. The security of several cryptosystems relies on the hardness of the first problem like [GPS16], [CPV20]. Others, like the Charles-Goren-Lauter [CGL09] hash function depends on the difficulty of computing endomorphism rings of elliptic curves.

In 2014, Kohel, Lauter, Petit and Tignol [KLPT14] introduced an algorithm that solves an analogue of the supersingular isogeny path problem in a quaternion algebra; however, the algorithm relies on several heuristics. Later Eisentraeger et al. [EHL$^+$18] used KLPT's heuristic algorithm to prove the equivalence of the isogeny path and endomorphism ring problems under polynomial time reductions. More recently in 2021, B. Wesolowski was able to rigorously prove that the two problem are indeed equivalent assuming the generalised Riemann hypothesis.

Upon analysing the approach followed in [KLPT14] and [Wes21] to address the quaternion path problem, one notable challenge (among others) appears to be integer factorization. Since the best classical algorithm for integer factorization is sub-exponential, in this paper, we use a factorisation

oracle alongside techniques in [EHL+18] and [Wes21] to construct unconditional rigorous algorithms which reduce the first problem to the second and vise versa. This theoretical result marks an important step towards a rigorous analysis of these computational problems, as the literature until now relies heavily on heuristics. As we develop our tools in this paper, we will see how we obtain results which were assumed to be beyond reach of analytic number theory techniques.

1.1. **Isoegny-Based Cryptography.** In order to understand foundational problems of current isoegny-based cryptosystems it is important to understand the supersingular setting. For any primes p and ℓ, there is an associated supersingular ℓ-isogeny graph. This graph is regular, with degree $\ell+1$, and contains approximately $p/12$ vertices. Each vertex corresponds to a supersingular elliptic curve, and the edges represent ℓ-isogenies between these curves. A key property of these graphs is that they are Ramanujan graphs, meaning they are optimal expanders. As a result, random walks on the graph quickly converge to the uniform distribution. Starting from an elliptic curve E, one can compute a sequence of random ℓ-isogenies until reaching a uniformly distributed endpoint E'. Given only E and E', it is believed to be computationally hard to reconstruct a path between them. This problem is the aforementioned *supersingular isogeny path* which was first incarnated in the Charles Goren Lauter hash function [CGL09]; precisely we have the following fundamental problem.

Problem 1.1 (ℓ-IsogenyPath) Given a prime p and two supersingular elliptic curves E_0 and E over $\mathbb{F}_p^2$ find a path in the ℓ-isogeny graph.

A few years after Charles, Goren and Lauter designed their hash function, Jao and De Feo proposed a variant of the Diffie-Hellman protocol based on supersingular isogeny problems, which is now known as the supersingular isogeny key exchange protocol SIDH [JDF11]. Looking at the problem from a different prespective it is been proven in [GPS16] that an efficient algorithm to solve the closely related *endomorphism ring problem* allows one to break SIDH. Recently [CD22], [MM22] and [Rob22] were able to break SIDH by utilizing torsion points information which turned to be sufficient to to find an isogeny between two supersingular elliptic curves.
Another encryption scheme which seems of great interest is CSIDH introduced by [CLM+18]. The scheme relies on the commutative action of the ideal class group and orientations of elliptic curves and it was proven to reduce to the *endomorphism ring problem* according to [CPV20]. A closely related scheme was introduced in section 4 of [GPS17] where the secret key is a maximal order isomorphic to the endomorphism ring of a supersingular elliptic curve. This leads us to study the following two problems.

Problem 1.2 (EndRing) Given a prime p and a supersingular elliptic curves E over $\mathbb{F}_{p^2}$, output four endomorphisms of E in efficient representation that generate the endomorphism ring of E.

By an efficient representation for endomorphisms α, we mean that there is an algorithm to evaluate $\alpha(P)$ for any $P \in E(\mathbb{F}_{p^k})$ in time polynomial in the length of the representation of α and in $k\log(p)$. We also assume that an efficient representation of α has length $\Omega(\log(\deg(\alpha)))$. The next problem is the quaternionic version that asks for an abstract description of $\mathrm{End}(E)$.

Problem 1.3 (MaxOrder) Given a prime p and a supersingular elliptic curve E, find four quaternions in $B_{p,\infty}$ that generate a maximal order $\mathcal{O} \subset B_{p,\infty}$ such that $\mathcal{O} \cong \mathrm{End}(E)$.

These two problem were first studied from a theoretical point of view which stemmed out as problems in arithmetic geometry. Although the problems appear similar, it was not immediately clear how to demonstrate their equivalence until the methods presented in [EHL+18] were developed. To address these issues alongside the ℓ-IsogenyPath problem, it is essential to study another equally important problem known as QuaternionPath. This problem, which was first studied by [KLPT14], serves as the primary tool for deriving our reductions and represents the quaternionic counterpart

of the isogeny path problem. We'll also specialise to a perhaps more effective version called the B-PSQuaternionPath.

Problem 1.4 (QuaternionPath) Given two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in $B_{p,\infty}$ and a set $\mathcal{N}$ of positive integers, find a left $\mathcal{O}_1$-ideal I such that $\mathrm{Nrd}(I) \in \mathcal{N}$ and $\mathcal{O}_R(I) \cong \mathcal{O}_2$ (definitions provided in Section 2.2). If $\mathcal{N}$ is the set of powers of a prime ℓ, we call the corresponding problem QuaternionPath . If $\mathcal{N}$ is the set of B-powersmooth integers for some $B > 0$, we call the corresponding problem B-PSQuaternionPath.

1.2. **Contributions** In this paper, we prove that the three problems ℓ-IsogenyPath, EndRing and MaxOrder are unconditionally equivalent under polynomial time reductions given access to a factoring oracle $\mathscr{O}$. This presents a great enhancement over previous heuritic and conditional results upon GRH like [EHL$^+$18] and [Wes21]. We develop rigorous technqiues and algorithms inspired by previous works, mainly [EHL$^+$18] and [Wes21], to solve norm form equation in a quaternion algebra and some analytic methods of prime sampling by a quaternary quadratic form. This will allow us to solve the QuaternionPath problem and more importantly its variant B-PSQuaternionPath. The algorithms present rigorous and powerful cryptanalytic tools for modern isogeny-based cryptography.

The key to establishing the equivalence of the three problems is the development of an efficient algorithm that can solve both the QuaternionPath problem and its powersmooth vairniant. The design and analysis of this new algorithm are covered across multiple sections of this article.

- In section 3 we study the problem of sampling primes represented by quaternary quadratic forms. We combine algorithmic techniques in euclidean lattices and results on the least locally represented integer by a quaternary quadratic form which is not representable. We employ our algorithm in the quaternionic scenraio to prove that given an ideal in maximal order we can find a equivalent ideal of prime norm. This serves as preconditioning step and has a heuristic analogue in [KLPT14].

- In section 4, we study the number of ways of representing an integer n by a quaternary quadratic form. The proof resorts to analytic number theory and our result, theorem 4.2, is the key ingredient to construct our main algorithm to solve certain diophantine equations in the following section.

- In section 5, we utilize the factoring oracle $\mathscr{O}$ and the previous result in section 4 to design an algorithm which finds integral solutions (s, t, x, y) to equations of the form

  $$af(s,t) + f^{\gamma}(x,y) = n$$

  where n and b are positive integers, f is positive definite, integral, binary quadratic form, and γ is a 2×2 integral matrix.

- In section 6, we glue everything together and solve the QuaternionPath problem in Theorem 6.1. Accordingly, the ℓ-power case is an immediate corollary and we specialize to the powersmooth case.

It is important to note that in our paper, as in [Wes21], we focus on provability rather than computability and efficiency. Even though our algorithms run in polynomial time, some constants are certainly not tight and bounds in terms of our parameter p maybe bigger than [KLPT14], yet overall the results present certain enhancements to [Wes21]. Hence, from a viewpoint of efficiency we recommend to follow [KLPT14]'s heuristic algorithm, and refer to our algorithm in special cases where

KLPT fails.

With this new algorithm in hand, we prove various reductions between ℓ-IsogenyPath, EndRing and MaxOrder. The reductions will be similar, in a sense, to other algorithms in the literature particularly [EHL$^+$18].

- We start, in section 7, by proving that ℓ-IsogenyPath and MaxOrder are equivalent. We accomplish that by replacing the heuristic algorithm of [KLPT14] in the previous methods by our unconditional algorithm.
- Eventually, we prove the equivalence of EndRing and MaxOrder in section8. The reduction is exactly as in [EHL$^+$18], but with our rigorous algorithm and the factoring oracle $\mathscr{O}$ replacing the heuristics assumed there.

It is worthy to note all our reductions preserve the property of having a polynomially bounded output size, which is a requirement in [EHL$^+$18].

1.3. **Factoring oracle.** In this paper, we assume access to a factoring oracle, denoted by $\mathscr{O}$, for factoring exponentially large numbers, particularly in Section 5 and onwards. The problem of factorization appears to be inevitable when addressing the QuaternionPath problem, and subsequently, the equivalence between EndRing, MaxOrder and the ℓ-IsogenyPath problem. The difficulty arises from the use of *Cornacchia's algorithm*, which solves Diophantine equations of the form $x^2 + dy^2 = m$. This algorithm is central to our approach and runs efficiently, provided we have the factorization of m. It is important to note, however, that Sections 3 and 4 do not rely on the oracle $\mathscr{O}$ in any way. This contrasts with [Wes21], where both sections heavily depend on the generalized Riemann hypothesis, as do the subsequent sections. It is also worth emphasizing that our assumption of having a factoring oracle is reasonable, especially given our focus on designing quantum-resistant cryptosystems. In this context, Shor's quantum algorithm for factorization naturally plays the role of our oracle. Consequently, our results yield unconditional quantum polynomial reductions between each of EndRing, MaxOrder and the ℓ-IsogenyPath problem.

2. Preliminaries

2.1 **Background on Elliptic curves.** We refer the reader to [Sil86] for a detailed discussion on this topic. An elliptic curve E over a field K of characteristic $p > 3$ is defined by the equation $y^2 = x^3 + Ax + B$ for $A, B \in K^\times$ with $4A^3 + 27B^2 \neq 0$. The K-rational points of E which are $(x, y) \in K^2$ satisfying the equation with an additional neutral element called the point at infinity ∞ form an abelian group.
An isogeny $\varphi : E_1 \to E_2$ defined over K is a non-constant map which is also a group homomorphism that takes ∞_1 to ∞_2. The degree of an isogeny is the degree of φ as a rational map. Every isogeny of degree $n > 1$ can be factored into a composition of isogenies of prime degrees such that the product of the degrees equals n. If $deg(\varphi) = d$ then there exist a unique isogeny called the dual isogeny denoted $\hat{\varphi} : E_2 \to E_1$ such that $\varphi\hat{\varphi} = [d]$ where $[d] : E_2 \to E_1$ is the multiplication-by-d map. An isomorphism is an isogeny $\iota : E_1 \to E_2$ of degree 1. We say that E_1 and E_2 are isomorphic over k (an extension of K) if there is an isomorphism between them that is defined over k. The j invariant of E as defined by the above equation is $j(E) = \frac{265 \cdot 27 \cdot A^3}{4A^3 + 27B^2}$. An isogeny with a degree that is coprime to p is uniquely determined by its kernel. Given the kernel, the isogeny can be computed in polynomial time with respect to the degree of the isogeny and $\log(p)$ using Vélu's formula [Vel71].

Endomorphism ring and Supersingular versus Ordinary curves An isogeny from E into

itself is called an endomorphism of E. If E is defined over $\mathbb{F}_q$ then an endomorphism of E will be defined over a finite extension of $\mathbb{F}_q$. The set of endomorphisms of E with the zero map form a ring under pointwise addition and composition which is called the endomorphism ring of E and denoted by $\mathrm{End}(E)$. If $\mathrm{End}(E)$ is isomorphic to an order in a imaginary quadratic field then the curve is said to be *ordinary*. Otherwise if $\mathrm{End}(E)$ is isomorphic to a maximal order in a Quaternion algebra in $B_{p,\infty}$ (defined in section 2.2) then E is said to be *supersingular*. Every supersingular elliptic curve over a field of characteristic p has an isomorphic curve that is defined over $\mathbb{F}_{p^2}$ because the j-invariant of such a curve is in $\mathbb{F}_{p^2}$.
Up to k-isomorphism, all supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$, with approximatley $\lfloor \frac{p}{12} \rfloor$ such curves. Let l be a prime different from p. The supersingular l-isogeny graph (for p) consists of vertices corresponding to these supersingular elliptic curves (up to isomorphism), with an edge connecting E_1 to E_2 for each l-isogeny from E_1 to E_2. This graph is regular with degree $l+1$ since each curve E possesses $l+1$ subgroups H of order l, each generating an isogeny with kernel H. The l-isogeny graph is Ramanujan, meaning that random walks on this graph converge rapidly to the uniform distribution, and any two curves in the graph are linked by an isogeny of degree l^m with $m = O(\log p)$.

2.2 Quaternion Algebras and the Deuring Correspondence

For a detailed account on the arithmetic of quaternion algebras we refer the reader to [Voi21]. For $a, b \in \mathbb{Q}^\times$, let $B(a,b)$ denote the quaternion algebra over $\mathbb{Q}$, with basis $1, i, j, ij$, i.e.

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

such that $i^2 = a$, $j^2 = b$ and $ij = -ji$. The quaternion algebra B has a *canonical involution* that sends $\alpha = x_1 + x_2 i + x_3 j + x_4 ij$ to $\bar{\alpha} = x_1 - x_2 i - x_3 j - x_4 ij$, and we define both the reduced trace and norm of an element α in B by

$$\mathrm{Trd}(\alpha) = \alpha + \bar{\alpha} = 2x_1, \qquad \mathrm{Nrd}(\alpha) = \alpha\bar{\alpha} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2.$$

We say Λ is a lattice in B if $\Lambda = \mathbb{Z}x_1 + \mathbb{Z}x_2 + \mathbb{Z}x_3 + \mathbb{Z}x_4$ where the x_i's form a basis for the vector space B over $\mathbb{Q}$.
If $I \subset B$ is a lattice, then the reduced norm of I, $\mathrm{Nrd}(I) = \gcd(\mathrm{Nrd}(\alpha) | \alpha \in \Lambda)$. We associate to Λ the normalised quadratic map

$$q_\Lambda : \Lambda \to \mathbb{Z}, \qquad \alpha \mapsto \tfrac{\mathrm{Nrd}(\alpha)}{\mathrm{Nrd}(\Lambda)}$$

and notice that $\frac{\mathrm{Nrd}(\alpha)}{\mathrm{Nrd}(\Lambda)} \in \mathbb{Z}$ as $\mathrm{Nrd}(\Lambda) | \mathrm{Nrd}(\alpha)$. The quaternion algebra B is an inner product space with respect to the bilinear form

$$\langle x, y \rangle = \frac{1}{2}(\mathrm{Nrd}(x+y) - \mathrm{Nrd}(x) - \mathrm{Nrd}(y)),$$

and the basis $\{1, i, j, ij\}$ is an orthogonal basis with respect to this inner product.
An order $\mathcal{O}$ in B is a full rank lattice that is also a subring. It is maximal if it is not contained in any other order. For an lattice Λ we define the *left order* and *right order* of Λ to be

$$\mathcal{O}_L(\Lambda) = \{\alpha \in B |\ \alpha\Lambda \subseteq \Lambda\}, \quad \mathcal{O}_R(\Lambda) = \{\alpha \in B |\ \Lambda\alpha \subseteq \Lambda\}\}.$$

If $\mathcal{O}$ is a maximal order and I is a left $\mathcal{O}$-ideal, then $\mathcal{O}_R(I)$ is also a maximal order. Given two maximal order $\mathcal{O}$ and $\mathcal{O}'$, then there exist a lattice I, called a connecting ideal, such that $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I) = \mathcal{O}'$.

Let $\mathcal{O}$ be a maximal order. We say $\mathcal{O}$-ideals I and J are equivalent if there exists an $\alpha \in B^\times$ such that $I = \alpha J$. The set of classes of this equivalenece relation is called the *left*-ideal class set of $\mathcal{O}$ and is denoted by $\mathrm{Cls}(\mathcal{O})$.
For a maximal order $\mathcal{O}$ in $B_{p,\infty}$, the discriminant is $\mathrm{disc}(\mathcal{O}) = p^2$. Moreover, for any left $\mathcal{O}$-ideal I, we have $\#(\mathcal{O}/I) = \mathrm{Nrd}(I)^2$, and the associted normalized quadratic map q_I has determinant p^2.
Let p be a prime and $B_{p,\infty}$ be the unique quaternion algebra ramified exactly at at p and ∞. The following lemma from [EHL$^+$18] gives the structure of $B_{p,\infty}$.

Lemma 2.1 ([EHL$^+$18], proposition 1)**.** *Let $p > 2$, then $B_{p,\infty} = \left(\frac{-q,-p}{\mathbb{Q}}\right)$ where*

$$q = \begin{cases} 1 & \text{if } p \equiv 3 \mod 4 \\ 2 & \text{if } p \equiv 5 \mod 8 \\ q_p & \text{if } p \equiv 1 \mod 8 \end{cases}$$

where q_p is the smallest prime such that $q_p \equiv 3 \mod 4$ and $\left(\frac{p}{q_p}\right) = -1$. Assuming GRH, we have that $q_p = O(\log^2 p)$ and hence can be computed in polynomial time in $\log p$.

Proof. This exactly proposition 1 from [EHL$^+$18] where the conditional result is treated there and the unconditional part comes from [Piz80]. □

Remark 1. Notice that this is the only case were the generalised Riemann hypothesis is assumed which is not directly related to the problems at hand, but rather to the very structure of the quaternion algebra we're working in. The problem of the least quadratic non-residue has been studied extensively in the past century especially by Erdős and Linnik. It's worthy to note that GRH presents an efficiently computable result and unconditional results hold yet they are a bit far from practical. For instance the following lemma due to Linnik [Lin41] tells us that not a lot of primes p have an exceptionally large least quadratic non-residue q_p.

Theorem 2.2 (Linnik)**.** *Let $\epsilon > 0$, then there exists a constant C_ϵ such that for all N there are at most C_ϵ primes $p \leq N$ with $q_p > N^\epsilon$.*

In the remainder of this article, the algebra $B_{p,\infty}$ will consistently be linked to the pair $(-q, -p)$ as defined in Lemma 2.1, along with the corresponding basis $(1, i, j, ij)$. For each p, we identify a maximal order $\mathcal{O}_0$ in $B_{p,\infty}$, along with a relevant suborder $R + Rj$, as described in the following lemma. This order $\mathcal{O}_0$ will be referred to as the special maximal order of $B_{p,\infty}$.

Lemma 2.3. *For any $p > 2$, the quaternion algebra $B_{p,\infty}$ contains the maximal order*

$$\mathcal{O}_0 = \begin{cases} \langle 1, i, \frac{i+ij}{2}, \frac{1+j}{2} \rangle & \text{if } p \equiv 3 \mod 4 \\ \langle 1, i, \frac{2-i+ij}{4}, \frac{-1+i+j}{2} \rangle & \text{if } p \equiv 5 \mod 8 \\ \langle \frac{1+i}{2}, \frac{j+ij}{2}, \frac{i+cij}{q}, ij \rangle & \text{if } p \equiv 1 \mod 8 \end{cases}$$

where in the last case c is a constant such that $q | c^2 p + 1$. Assuming the Generalized Riemann Hypothesis (GRH), the maximal order O_0 contains the suborder $R + Rj$ with an index of $O((\log p)^2)$, where R is the ring of integers of $\mathbb{Q}(i)$. If ω is a reduced generator of R, then the reduced norm

$$Nrd(s + t\omega + xj + y\omega j) = f(s, t) + pf(x, y),$$

where f is a principal, primitive, positive definite, integral binary quadratic form with discriminant $disc(\mathbb{Q}(i)) = O((\log p)^2)$.

Proof. This is a combination of *lemma 1* in [KLPT14] and *proposition 1* from [EHL+18]. □

The next lemma states that the integers represented by the normalised quadratic map q_I correspond to norms of ideals in the same equivalence class as I.

Lemma 2.4 ([KLPT14], Lemma 5)**.** *Let I be a left $\mathcal{O}$-ideal and $\alpha \in I$. Then $I\bar{\alpha}/Nrd(I)$ is an equivalent left $\mathcal{O}$-ideal of norm $q_I(\alpha)$.*

The Deuring correspondence. For a detailed account on the Deuring correspondence we refer the reader to chapter 42 of [Voi21]. The Deuring correspondence associates each maximal order in $B_{p,\infty}$ with a supersingular elliptic curve E, where the maximal order is isomorphic to $\mathrm{End}(E)$, more precisely it is a bijection between the sets

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{maximal orders in } B_{p,\infty} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{supersingular elliptic curves} \end{array} \right\} / \mathrm{Gal}(\mathbb{F}_p^2/\mathbb{F}_p).$$

Given the Deuring correspondence and our special maximal order from lemma 2.3, it is natural to ask if we can efficiently compute the corresponding supersingular elliptic curve. The following lemma deals with this problem.

Lemma 2.5 ([EHL+18], Proposition 3)**.** *Let $\mathcal{O}_0$ be as defined in Lemma 2.3. There exists an algorithm that, for any prime $p > 2$, computes an elliptic curve E_0 over $\mathbb{F}_p$ and an element $\iota \in End(E_0)$ such that the mapping*

$$\mathcal{O}_0 \to End(E_0) : 1, i, j, ij \mapsto [1], \iota, \pi, \iota\pi$$

is an isomorphism. This algorithm runs in time polynomial in $\log p$ (we assume GRH if $p \equiv 1 \mod 8$).

The Deuring correspondence is more than a mere bijection; it also preserves morphisms between the two categories. For any isogeny $\varphi : E_1 \to E_2$, we define $I_\varphi = \mathrm{Hom}(E_2, E_1)\varphi$, where $\mathrm{Hom}(E_2, E_1)$ denotes the set of isogenies from E_2 to E_1. The object I_φ is a left $\mathrm{End}(E_1)$-ideal, which implies that $\mathcal{O}_L(I_\varphi) \cong \mathrm{End}(E_1)$. Moreover, $\mathcal{O}_R(I_\varphi) \cong \mathrm{End}(E_2)$. In this sense, I_φ serves to connect $\mathrm{End}(E_1)$ with $\mathrm{End}(E_2)$, just as φ connects E_1 to E_2. This construction maintains the 'quadratic structure' in that $\mathrm{Nrd}(I_\varphi) = \deg(\varphi)$.

Conversely, if I is a left $\mathrm{End}(E_1)$-ideal, we can define an isogeny φ_I as the unique isogeny with kernel $\bigcap_{\alpha \in I} \ker(\alpha)$. These two constructions are mutual inverses, meaning that for any I and φ, we have $I_{\varphi_I} = I$ and $\varphi_{I_\varphi} = \varphi$. The transition from I to φ_I can be computed efficiently, provided that I is an ideal in the special order $\mathcal{O}_0$ from Lemma 2.3, and that $\mathrm{Nrd}(I)$ is powersmooth (its prime-power factors are polynomially bounded). This is stated in the following lemma. The case $p \equiv 3 \mod 4$ is discussed in [GPS20], but as noted in [EHL+18], the result easily extends to arbitrary p.

Lemma 2.6 ([GPS20], Lemma 5)**.** *Let $\mathcal{O}_0$ be as defined in Lemma 2.3 and E_0 as specified in Lemma 2.5. There is an algorithm that, given a left $\mathcal{O}_0$-ideal I with norm $N = \prod \ell_i^{e_i}$, produces the corresponding isogeny $\varphi_I : E_0 \to E_1$. The complexity of this algorithm is polynomial in $\log p$ and $\max_i(\ell_i^{e_i})$ (we assume GRH if $p \equiv 1 \mod 8$).*

Lemma 2.6 tells us that transition from an ideal into an isogeny can be computed efficiently in $\log p$ and $\max_i(l_i^{e_i})$. The next lemma shows us that going the other way, i.e. computing the ideal from an isogeny, can also be done efficiently.

Lemma 2.7 ([Wes21]. Lemma 7.1)**.** *Let $\mathcal{O}_0$ and E_0 be as in Lemmata 2.3 and 2.5. There exists an algorithm which, given an isogeny $\varphi : E_0 \to E$ of degree $\prod_i \ell_i^{e_i}$, returns the corresponding left $\mathcal{O}_0$-ideal I_φ. The complexity of this algorithm is polynomial in $\log p$ and $\max_i(l_i^{e_i})$ (we assume GRH if $p \equiv 1 \mod 8$).*

2.3 Brandt Graph and Supersingular ℓ-isogeny graph.

Definition 2.8 (Brandt Graph)**.** *Let p be a prime number, and $\mathcal{O}$ a maximal order in $B_{p,\infty}$. Let I, J be two left $\mathcal{O}$-ideals. We say J is an ℓ-neighbor of I if $J \subseteq I$ and $Nrd(J) = \ell \cdot Nrd(I)$. The ℓ-Brandt graph is the graph with vertices $Cls(\mathcal{O})$ and an edge from $[I_i]$ to $[J]$ for each ℓ-neighbor $J \subseteq I_i$, where $(I_i)_{i=1}^{\#\mathrm{Cls}(\mathcal{O})}$ is a list of ideal class representatives.*

Through the Deuring correspondence, the ℓ-Brandt graph is isomorphic to the ℓ-isogeny graph (up to the action of $\mathrm{Gal}(F_{p^2}/F_p)$). Starting with a random walk, at each step, the current vertex represents an elliptic curve E, and one randomly selects one of the $\ell + 1$ outgoing isogenies to determine the next vertex. Alternatively, given a left O-ideal I, one can randomly choose one of the $\ell + 1$ left submodules $M \subset I/\ell I$, with the next vertex being $M + \ell I$. The next theorem will be beneficial when we design our algorithms, it states that random walks between ideal classes also converge rapidly to a uniform distribution. which is a consequence of the fact that ℓ-Brandt graph (and ℓ-isogeny graph) has the Ramanujan property.

Theorem 2.9 ([Wes21]. Theorem 6.2)**.** *Let p be a prime number, and $\mathcal{O}$ a maximal order in $B_{p,\infty}$. Let N_p be the size of the ideal class set of $\mathcal{O}$. Let I be the ideal obtained from a random walk of norm $n = \prod_i \ell_i^{e_i}$. Then, for any ideal class C, we have*

$$\left|\Pr[I \in C] - \frac{1}{N_p}\right| \leq \prod_i \left(\frac{2\sqrt{\ell_i}}{\ell_i + 1}\right)^{e_i}.$$

2.4 Binary and Quaternary Quadratic Forms.

Most of our techniques and results which will be needed in the upcoming sections rely heavily on the theory of Quadratic forms, primarly binary and quaternary ones. We refer the reader to [Coh13] for some theoretical and computational aspects. A quadratic form $Q(x)$ in r variables is a polynomial whose terms all have degree 2. Its defined as $Q(x) = x^t A x$ where $A = (a_{ij})$ is a symmetric $r \times r$ matrix called the Gram matrix. A quadratic form is integral if $Q(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}^r$, equivalently if all diagonal entries are integral and non-diagonal entries belong to $\frac{1}{2}\mathbb{Z}$. We let $length(Q)$ be the binary length of its coefficients. We also say Q represents an integer n if $Q(x) = n$ for some $x \in \mathbb{Z}^r$. A quadratic form Q is called positive-definite if $Q(x) \geq 0\ \forall x \in \mathbb{R}^r$ with equality if and only if $x = 0$; it is primitive if all its coefficients are coprime. The level N of a quadratic form $Q = x^t A x$ is defined to be the least $N \in \mathbb{Z}$ such that $NA^{-1} \in M_{r\times r}(\mathbb{Z})$. A quadratic form is binary if $r = 2$ and quaternary if $r = 4$ and its discriminant is related to the determinant of the Gram matrix by

$$\mathrm{disc}(Q) = \begin{cases} (-1)^{r/2} \det(2G) & \text{if } r \text{ is even} \\ \frac{1}{2}(-1)^{\frac{r+1}{2}} \det(2G) & \text{if } r \text{ is odd.} \end{cases}$$

We define the bilinear form associated to Q as

$$\langle x, y\rangle_Q = \frac{1}{2}(Q(x + y) - Q(x) - Q(y)).$$

A lattice L associated to Q is a free $\mathbb{Z}$-module of finite rank together with a positive definite quadratic form Q on $L \otimes R$. In particular if $(b_i)_i$ is a $\mathbb{Z}$-basis for L and $x = \sum_{1 \leq i \leq n} x_i b_i \in L$ with $x_i \in \mathbb{Z}$, then the definition of a quadratic form implies that

$$Q(x) = \sum_{1 \leq i,j \leq n} q_{i,j} x_i x_j \text{ with } q_{i,j} = \langle b_i, b_j \rangle_Q.$$

Conversely, any positive definite quadratic form induces a lattice structure on $\mathbb{Z}^r$, via the canonical basis, and the discriminant of the lattice is the discriminant of the quadratic form associated to it via any of its basis. If $\gamma \in M_{r \times r}(\mathbb{Z})$ we denote by Q^γ the quadratic form $Q(\gamma x)$. The volume of Q is defined to be $\text{Vol}(Q) = |\det(G)|^{1/2}$ and the covering radius $\mu(Q)$ is the smallest μ such that for all $y \in \mathbb{R}^r$ we have $\min_{x \in \mathbb{Z}^r} Q(x - y) < \mu^2$. From a lattice point of view the covering radius is the distance between any vector $x \in \mathbb{R}^r$ and the closest lattice point to x. We will need the following handy lemma to bound the covering radius.

Lemma 2.10 ([Wes21], Lemma2.3)**.** *If Q is integral then $\mu(Q) \leq \frac{1}{2} r^{1/2} \gamma_r^{r/2} \text{Vol}(Q)$ where γ_r is Hermite's constant.*

3. Quadratic forms and prime sampling

In this section we study the following problem: given an ideal I, find another ideal J equivalent to I whose norm is a prime. Using lemma 2.4, this is equivalent to finding primes represented by the Quaternary quadratic form q_I as defined in section 2.2.

3.1 **Sampling primes** Let Q be a primitive, integral, positive definite quaternary quadratic form. In this section we discuss the problem of sampling vectors from $\{x \in \mathbb{Z}^4 \mid Q(x) \leq \rho\}$ such that $Q(x)$ is a prime. To do that we need some lemmas.

Definition: *The i^{th} successive minimum λ_i of a quadratic form Q of dimension n is defined as the smallest value $r > 0$ such that there exist i linearly independent lattice vectors $v_1, v_2, ...v_i$ with $Q(v_j) \leq \lambda_i$ for all $j = 1, 2, ...i$.*

Now we develop an algorithm which samples integral vectors within a 4-ellipsoid. For practical reasons we will specialize our generalisation of Lemma 3.3 from [Wes21] using a particular bound so that our ellipsoid contains enough lattice points.

Lemma 3.1. *Let Q be a primitive, postive definite, integral Quaternary quadratic form, and let $\rho \geq 4\mu^2(Q) > 0$ where $\mu(Q)$ is the covering radius of Q. There is an algorithm that samples uniformly random elements from*

$$\{x \in \mathbb{Z}^4 \mid Q(x) \leq \rho\}$$

in polynomial time in $\log(\rho)$ and in length(f).

Proof. The approach is analogous to the one in [Wes21] we'll just use the restriction on ρ and the result will follow for four variables.
Let $B_Q(r) = \{v \in \mathbb{R}^4 | Q(v) \leq r^2\}$ be the ellipsoid around the origin define by the quadratic form. Let $r = p^{1/2}$, our goal is to sample vectors from $B_Q(r) \cap \mathbb{Z}^4$. We first compute a Minkowski-reduced basis (b_1, b_2, b_3, b_4) of Q with $Q(b_1) \leq Q(b_2) \leq Q(b_3) \leq Q(b_4)$. Now we know that $Q(b_4) \leq \lambda_4 \leq 2\mu \leq r$ where λ_4 is the 4^{th} *successive minimum* (in fact $Q(b_4) = \lambda_4$), i.e we have enough lattice points within the ellipsoid. Let $V = \{v \in \mathbb{R}^4 | Q(v) = min_{\lambda \in \mathbb{Z}^4} f(v + \lambda)\}$ be the Voronoi cell aorund the origin, i.e all points in V are closer to the origin than any other lattice point. For any $v \in \mathbb{R}^4$, we

define the closest lattice vector $\lambda(v) \in \mathbb{Z}^4$ to satisfy $v \in V + \lambda(v)$. Computing the closest lattice vector (CLV) is often expensive as it's complexity is exponential in the dimesnion but since we're working in dimension 4, we can compute the CLV efficiently and its unique for almost all v. We sample according to algorithm 1.

To show there is a good probability that $\lambda(v)$ will land in $B_Q(r)$, we use the fact that $r - \mu > 0$,

Algorithm 1 QuadSampling(Q, ρ)

Input: Positive definite quaternary quadratic form Q and a bound $\rho \geq 4\mu^2(Q)$
Output: uniform $x \in \mathbb{Z}^4$ such that $Q(x) \leq \rho$

while $\lambda \notin B_Q(r)$ **do**
    Sample a uniform $v \in B_Q(r + \mu)$;
    Solve the closest vector problem $\lambda(v)$;
end while
return $\lambda(v)$.

this implies

$$\Pr[\lambda(v) \in B_Q(r)] \geq \Pr[v \in B_Q(r - \mu)] = \frac{\mathrm{Vol}(B_Q(r - \mu))}{\mathrm{Vol}(B_Q(r + \mu))} = \frac{(r - \mu)^4}{(r + \mu)^4} \geq \frac{(1 - 2^{-1})^4}{(1 + 2^{-1})^4} \geq 0.012,$$

i.e. the process succeeds after a constant number of trials. Finally, our output vector is uniform where the result follows analogously as in [Wes21]. □

The approach taken in [Wes21] to sample vectors $v \in \mathbb{Z}^4$ such that $Q(v)$ is a prime is by transforming our quaternary quadratic form into a binary form f of discriminant D and use the well-known result on primes by Lagarias and Odlyzko [LO77] (assuming GRH) which states that

$$\pi_f(\rho) = \frac{\delta\rho}{h(D)\log\rho} + O(\rho^{1/2}\log(|D|\rho)),$$

where $\pi_f(\rho) = \#\{v \in \mathbb{Z}^2 | f(v) \leq \rho \text{ is a prime}\}$, $h(D)$ is the class number and δ is either 1 or 1/2. In order to be able to sample vectors which represent primes without relying on GRH we will need to take a completely different route and look into the theory of quaternary quadratic forms.
It is a well known result [Tar29] that every sufficiently large integer n that is locally represented by a quateranry quadratic form Q is represented by Q. Hence our approach will be the following: We will prove that a quaternary quadratic form $Q(x) = x^t Ax$ of determinant q^2, for some prime q, represents every integer n coprime to q greater than some bound B_q. We then apply the prime number theorem as primes will be dense in our set of representable integers with $n > B_q$. To achieve that we will need the following lemmas.

Lemma 3.2. *Let $Q = x^T Ax$ be a primitive, integral positive-definite quateranry quadratic form, and $\det(A) = q^2$ for some prime q. Then the level of Q is q, and Q locally represents all positive integers.*

Proof. First, we prove that the level of Q is q using a classification of Shimura's (see [Shi6], Section 6.3). Let $\mathfrak{S}_n$ denote the set of matrices $T \in \mathrm{GL}_n(\mathbb{Q})$ that are symmetric, have integer diagonal entries, and whose off-diagonal entries are either integral or half-integral. Shimura calls an element of T *reduced* if whenever P is an invertible matrix with integer entries and $P^{-1}T(P^{-1})^T \in \mathfrak{S}_n$, then $\det(P) = \pm 1$. We first claim that the matrix A in the statement of the lemma above is reduced.

If it were not reduced, then there would be a matrix P with $|\det(P)| > 1$ so that $P^{-1}(A)(P^{-1})^T \in \mathfrak{S}_n$. The determinant of this matrix must be d for some integer d, but also, it equals $\det(P^{-1})^2 \cdot q^2$. It follows that $\det(P) = q$. However, this would imply that $P^{-1}A(P^{-1})^T$ is the Gram matrix for a positive-definite Quaternary form with determinant 1. Shimura says at the beginning of [Shi6] that it is classically known that a positive-definite form with determinant 1 must have the number of variables $\equiv 0 \pmod 8$. (For a proof of this, see Corollary 2 on page 53 of [Ser73] or Theorem 6.4 of [Shi6].) Since $4 \not\equiv 0 \pmod 8$, this is a contradiction and so the matrix A must be reduced.

In Theorem 6.4 of [Shi6], a classification is given of reduced forms that depends on four parameters: σ (the signature of Q), δ (either 1 or the discriminant of the ring of integers of a quadratic field), e_0 and e_1. The integer e_0 must divide δ, e_1 must be prime to δ, and we must have that the determinant is $|\delta|e_1^2$ and the level of the form is $|\delta|e_1$. We must have $\delta = 1$ and $e_1^2 = q^2$. Therefore, the level of the form is $|\delta|e_1 = 1 \cdot q = q$.

Now we turn to showing that Q locally represents every positive integer. Criteria to establish this are well-known and quite old in the quadratic forms literature. Assume first that $q > 2$.

Lemma 1 of Gordan Pall's paper [Pall46] is sufficient for our purposes. It shows that the form Q stated above represents every element of $\mathbb{Z}_r$ for any odd prime $r \neq q$. Moreover, since the level of the form is q, its Jordan decomposition has the form $\langle \alpha_1, \alpha_2, q\alpha_3, q\alpha_4 \rangle$ where $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Z}_q^\times$. The lemma of [Pall46] now implies that Q represents every element of $\mathbb{Z}_q$. For $r = 2$, calculations in the proof of Proposition 15 of [Rouse14] show that since the determinant of Q is $\equiv 1 \pmod 8$, Q is equivalent over $\mathbb{Z}_2$ to $xy + zw$, which represents every element of $\mathbb{Z}_2$.

For $q = 2$, there is a unique Quaternary form of determinant q^2, namely $Q(x, y, z, w) = x^2 + y^2 + z^2 + w^2 + xw + yw + zw$. Lemma 1 from Pall46's paper easily implies that Q represents every element of $\mathbb{Z}_r$ for $r > 2$, and it is simple to check that Q represents the integers $\{1, 3, 5, 7, 2, 6, 10, 14\}$. It follows that Q represents the 8 squareclass in $\mathbb{Z}_2$ and so Q locally represents all positive integers. □

Lemma 3.3. *Let $Q = x^T Ax$ be a primitive, integral positive-definite quaternary quadratic form, and $\det(A) = q^2$ for some prime q. Then for every $\epsilon > 0$, Q represents all integers $n \gg_\epsilon q^{4+\epsilon}$ with $(n, q) = 1$.*

Proof. Theorem 1 of [Rouse18] shows that Q represents all integers n coprime to q, provided that n is locally represented by Q and $n \gg_\epsilon \max\{N(Q)^{3/2+\epsilon}D(Q)^{5/4+\epsilon}, N(Q)^{2+\epsilon}D(Q)^{1+\epsilon}\}$, where $N(Q)$ and $D(Q)$ are the level and discriminant of Q respectively. The result then follows from our previous lemma. □

The next proposition allows us to sample vectors $x \in \mathbb{Z}^4$ such that $Q(x)$ is a prime.

Proposition 3.4. *Let $Q = x^T Ax$ be a primitive, integral positive-definite Quaternary quadratic form, and $\det(A) = q^2$ for some prime q. There is an algorithm that finds an integral vector $x \in \mathbb{Z}^4$ such that $Q(x)$ is a prime number at most $O_\delta(q^{4+\delta})$ for a suitable δ, and runs in expected polynomail time in length(f) and log(q).*

Proof. From Lemma 3.1, one can sample a uniformly random integral vector x such that $Q(x) \leq \rho$ and $\rho \geq 4\mu^2(Q)$. Using the bound $\mu(Q) \leq \frac{1}{2}r^{1/2}\gamma_r^{r/2}\mathrm{Vol}(f)$ from lemma 2.10 we obtain that $\mu(Q) \ll \mathrm{Vol}(f) = q$. Additionally we know from the previous lemma 3.3, that Q represents all integers greater than $q^{4+\epsilon}$ coprime to q. Hence if we let $\rho = q^{4+\delta}$ where δ is to be adjusted, then

the probability of choosing an integer $Q(x) = n \ll q^{4+\epsilon}$ for any $0 < \epsilon < \delta \leq \frac{1}{2}$ is very low provided that q is large enough and δ is suitably chosen. Hence our chosen integer $Q(x) = n$ will be larger than $q^{4+\epsilon}$ with a good probability, and the result follows from the prime number theorem. □

3.2 **Computing equivalent ideals of prime norm** Consider a maximal order $\mathcal{O}$ in $B_{p,\infty}$ and a left $\mathcal{O}$-*ideal* I. We can compute another equivalent ideal J with a prime norm using proposition 3.4.

Algorithm 2 EquivalentPrimeIdeal$_\delta(I)$

Input: A left ideal I in a maximal order $\mathcal{O}$.
Output: An ideal J of prime norm, and an element $\alpha \in I$ such that $J = I\bar{\alpha}/\mathrm{Nrd}(I)$.
1: Find an element $\alpha \in I$ such that $q_I(\alpha)$ is a prime; {Proposition 3.4}.
2: **return** $J = I\bar{\alpha}/\mathrm{Nrd}(I)$, and α.

Theorem 3.5. *For a suitable $0 < \delta \leq 1/2$, Algorithm 2 is correct and runs in expected polynomial time in $\log(Nrd(I))$ and $\log p$,and the output J has reduced norm $Nrd(J) = O_\delta(p^{4+\delta})$.*

Proof. It follows straightforwardly from Proposition 3.4, where $Q = q_I$ is a primitive integral positive definite Quaternary quadratic form of determinant p^2. □

Remark 2. In [KLPT14] the heuristic algorithm is expected to return an equivalent ideal of norm $\mathrm{Nrd}(J) = O(p^{1/2})$ most of the times, and $\mathrm{Nrd}(J) = O(p)$ in the worst case. In [Wes21] the output ideal J is expected to have $\mathrm{Nrd}(J) = O_\epsilon(p^{2+\epsilon})$ assuming the generalized Riemann hypothesis. Even though our result is certainly not as tight as the previous ones, nevertheless the size of the norm will be good enough for our applications. We conclude this section with a proposition that modifies the last algorithm to output an ideal with certain properties.

Proposition 3.6. *Given a left ideal I, a bound $\rho > p^{4+\epsilon}$ for $\epsilon > 0$, and a prime $l \neq p$, there is an algorithm which returns an ideal J equivalent to I such that $\mathrm{Nrd}(J)$ is a prime between ρ and $\rho^{1+\theta}$ for a suitable $\theta > 0$, and l is a non-quadratic residue modulo $\mathrm{Nrd}(J)$. The algorithm runs in polynomial time in $\log(\mathrm{Nrd}(I)), \log(p)$ and l.*

Proof. The proof of this proposition is given in ([Wes21], Proposition 3.8), and ours follows analogously. The condition on θ is to ensure that the probability of choosing an integer less than ρ is small, provided that ρ is large enough. □

4. Number of representations of an integer by a quadratic form

In this section we study the number of representations of an integer by a quadratic form. We let Q be a primitive, integral, positive definite quaternary quadratic form and we denote by $r_Q(n) = \#\{x \in \mathbb{Z}^4 | Q(x) = n\}$. The bounds in this section, particularly corollary 4.4, will be critical for designing our main algorithm in the next section. The next proposition from ([Iwa12], Theorem 20.9) gives an asymptotic for $r_Q(n)$, and though the result is more general, we'll state it for 4 variables for our purposes.

Theorem 4.1. *Let $Q(x)$ be an integral positive definite quadratic form of 4 variables. Then for any $n > 0$, the number of integral solutions $x = (x_1, x_2, x_3, x_4)$ to $Q(x) = n$ satisfies*

$$r(n, Q) = \frac{(2\pi)^2 n}{|det(A)|^{1/2}} \mathcal{S}(n, Q) + O_{\epsilon,Q}(n^{\frac{3}{4}+\epsilon}), \tag{1}$$

where $\mathcal{S}(n,Q)$ is the so-called Singular series defined as

$$\mathcal{S}(n,Q)=\sum_{c=1}^{\infty}c^{-4}g_c(n,Q)$$

with

$$g_c(n,Q)=\sum\nolimits^{*}_{d\ (mod\ c)}\ \sum\nolimits_{h\ (mod\ c)}exp\left(\frac{2\pi id}{c}(Q(h)-n)\right),$$

A is the Gram matrix of Q and $\epsilon>0$, with the implied constants depending on ϵ and the quadratic form Q.

Note that ϵ with it's implied constants cause no harm as we can control the value of ϵ and accordingly we can fix it, but to eliminate the dependence of the implied constants on the quadratic form, we will modify the proof of Theorem 4.1 in [Iwa12].

Theorem 4.2. *Let $Q(x)$ be an integral positive definite quadratic form of 4 variables. Then for any $n>0$, the number of integral solutions $x=(x_1,x_2,x_3,x_4)$ to $Q(x)=n$ satisfies*

$$r(n,Q)=\frac{(2\pi)^2n}{|det(A)|^{1/2}}\mathcal{S}(n,Q)+O_\epsilon(N^2n^{\frac{3}{4}+\epsilon}),\tag{2}$$

where A is the Gram matrix of Q, and N is the level of Q, $\mathcal{S}(n,Q)$ and $g_c(n,Q)$ are as defined in Theorem 4.1.

Proof. Following Iwaniec's proof of the lemma, one notices that the only occurrence of the implied constants depending on the Quadratic form Q is coming from ([Iwa12][Lemma 20.1) which states that

$$G_m\left(\frac{d}{c}\right)=\sum_{h\ (mod\ c)}exp\left(\frac{2\pi id}{c}(Q(h)+h^tm)\right)\ll_Q c^{\frac{r}{2}}.$$

Working out the details, we obtain

$$\begin{aligned}\left|G_m\left(\frac{d}{c}\right)\right|^2&=\sum\nolimits^{*}_{x,y\ (mod\ c)}exp\left(\frac{2\pi id}{c}(Q((x)-Q(y)+(x-y)^tm)\right)\\&=\sum\nolimits^{*}_{y,z\ (mod\ c)}exp\left(\frac{2\pi id}{c}(y^tAz-Q(z)+z^tm)\right)\\&\le c^r\cdot|\{z(mod\ c)\mid Az\equiv 0\ (mod\ c)\}|\\&\le c^r\cdot|\{z(mod\ c)\mid NA^{-1}Az\equiv 0\ (mod\ c)\}|\\&=c^r\cdot|\{z(mod\ c)\mid Nz\equiv 0\ (mod\ c)\}|\\&=c^r\cdot gcd(N,c)^r\\&\le c^rN^r\end{aligned}$$

taking square roots both sides, we get the desired result. Now substituting in (20.112) in the proof of [Iwa12], we get the statement of the theorem. □

Now in order for the main term to dominate the error term, we need to make sure $\mathcal{S}(n,Q)>0$.

Lemma 4.3. *Given an integral positive definite Quaternary quadratic form $Q(x) = x^T Ax$, if*

$$Q(x) \equiv n \ (mod\ 2^7|det(A)|^3) \tag{3}$$

is solvable, then there exist an absolute constant $\kappa > 0$

$$\mathcal{S}(n, Q) \geq \frac{\kappa}{\log\log(n)}. \tag{4}$$

Proof. Denote by $\chi(q) = \left(\frac{|det(A)|}{q}\right)$ the legendre symbol. Using [Dub14] we can determine in polynomial time if 3 is solvable or not. If solvable, then from ([Iwa04],11.76) we have

$$\mathcal{S}(n, Q) \asymp \prod_{p|n} \left(1 + \frac{\chi(p)}{p}\right),$$

i.e there exist a constant c_1 such that

$$\mathcal{S}(n, Q) \geq c_1 \prod_{p|n} \left(1 + \frac{\chi(p)}{p}\right) \geq c_1 \prod_{p|n} \left(1 - \frac{1}{p}\right) = c_1 \frac{\varphi(n)}{n} \geq \frac{\kappa}{\text{loglog}(n)}.$$

where we have used the fact that $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \geq \frac{c_2 n}{\log\log(n)}$ and this concludes the proof of the lemma. □

For our applications, we'll need the following immediate corollary.

Corollary 4.4. *For every $\epsilon > 0$ and $n \gg_\epsilon N^{8+\epsilon}|det(A)|^{2+\epsilon}$*

$$r(n, Q) \gg_\epsilon \frac{1}{|det(A)|^{1/2}} \frac{n}{\log\log n}, \tag{5}$$

provided that the congruence in 3 is solvable.

5. Solving diophantine equations

In this section we gather and employ our previous results to solve Diophantine equations of the form

$$af(s, t) + bf(x, y) = n \tag{6}$$

where f is some binary quadratic form, and $a, b, n \in \mathbb{Z}$. In fact we'll be proving the following slightly more general theorem.

Theorem 5.1. *For every $\epsilon > 0$ there exists $C_\epsilon > 0$ and an algorithm $\mathcal{A}$ such that the following holds. Let b, and n be positive integers, and f a reduced, primitive, principal, positive definite, integral binary quadratic form whose discriminant $disc(f)$ is fundamental. Let $\gamma \in M_{2\times 2}(\mathbb{Z})$ of rank 2 and content 1, and let $a > 0$ which divides $det(\gamma)$. Suppose $det(\gamma)$, $disc(f)$ and b are pairwise coprime and $gcd(det(\gamma)b, n) = gcd(a, 2) = 1$. Then $\mathcal{A}(f, \gamma, b, n)$ returns an integral solution (s, t, x, y) of the equation*

$$af(s, t) + bf^\gamma(x, y) = n \tag{7}$$

provided that $n \geq C_\epsilon(N^{8+\epsilon}|det(A)|^{2+\epsilon})$ *where* A *is the gram matrix of*

$$Q(s,t,x,y) = af(s,t) + bf^\gamma(x,y)$$

viewed as a Quaternary quadratic form, N *is the level of* Q*, and* $Q(s,t,x,y) \equiv n$ *is solvable modulo* $2^7 det^3(A))$*. Assuming access to a factoring oracle* $\mathscr{O}$*, the algorithm runs in expected polynomial time in disc(f), length(*γ*),* $2^{\omega(a)}$*,* $\log(n)$*, and the output is random with min-entropy* $\Omega(\log(n))$*.*

In [Wes21] Wesolowski uses genus theory of quadratic forms and prime ideals in a quadratic extension to solve a similar diophantine equation where $a = \det(\gamma)^2$. The reason behind his approach is because he looks for primes ℓ represented by f and at the same time satisfy the generalised Hardy-Littlwood problem $al + bf(x,y) = n$. We know that Cornacchia's algorithm allows us to solve the diophantine equation

$$f(s,t) = m$$

in polynomial time in $\log(m)$ and $disc(f)$ provided that we know the factorisation of m. As primality test can be done efficiently, he requires m to be a prime. Using our factoring oracle $\mathscr{O}$, we need not take that route which allows us to solve the problem by appealing to the theory of Quateranry quadratic forms without relying on GRH.
In order to prove the main theorem 5.1 we first need a proposition.

Proposition 5.2. ([Wes21], Proposition 5.2)**.** *Let* g *be a primitive, positive definite, integral, binary quadratic form. Let* a*,* b*,* n *be positive integers, and suppose that* a *divides disc(g) and* $gcd(a, 2bn) = 1$*. Let* X *be the set of integral solutions* (z,x,y) *of the equation*

$$az + bg(x,y) = n, \tag{8}$$

with $z > 0$*. If there exists a solution modulo* a*, then* X *is the disjoint union of* $2^{\omega(a)}$ *sets* X_i *with*

$$\#X_i = \frac{\pi n}{ba\ Vol(g)} + O\left(\left(\frac{n}{b}\right)^{1/2} + aVol(g)\right), \tag{9}$$

and knowing the factorisation of a *allows one to sample uniformly from any* X_i *in polynomial time.*

Proof. This is exactly *Proposition* 5.2 from [Wes21]. □

Proof of Theorem 5.1. The proof is almost complete, we just need to combine our results from previous sections. Note that Proposition 5.2 allows us to sample a uniform integral solution (z,x,y) to 8 in polynomial time up to a very small error $O(n^{-1/2})$. Everytime we sample a solution (z,x,y) of 8 from X with $g = f^\gamma$ we factorise z using our oracle $\mathscr{O}$, Cornacchia's algorithm should then be able to efficiently solve $f(s,t) = z$ or return that no solution exists. In the latter case we sample another solution. We would be done then if a large number of these solutions satisfy $z = f(x,y)$. In order to ensure this condition, notice that if we let $Q(s,t,x,y) = af(s,t) + bf^\gamma(x,y)$ then $r(n,Q)$ is the number of solution (z,x,y) to 8 with $z = f(s,t)$. Using Corollary 4.4, we obtain

$$r(n,Q) \gg \frac{1}{det^{1/2}(A)} \frac{n}{\log\log(n)}$$

given $n \geq C_\epsilon(N^{8+\epsilon}|det(A)|^{2+\epsilon})$ and $Q(s,t,x,y) \equiv n$ is solvable modulo $2^7 det^3(A))$.
Since $det(A) = a^2b^2 disc^2(f)\ det(\gamma)$ and

$$\#X \ll \frac{2^{\omega(a)} n}{ba\ disc^{1/2}(f)\ |det(\gamma)|^{1/2}},$$

we obtain

$$\frac{r(n,Q)}{\#X} \gg \frac{1}{2^{\omega(a)} disc^{1/2}(f)} \frac{1}{\text{loglog}(n)}. \tag{10}$$

Therefore, we expect to sample and factorise z $O(2^{\omega(a)} disc^{1/2}(f)\text{loglog}(n))$ times until we find a solution (s,t,x,y) for 7. Since sampled solutions in X behave almost uniformly we expect the *min-entropy* $H_{min}(X) = -\log(P_{max}) = \Omega(\log n)$; this concludes the proof. □

Remark 3. Note that even though $2^{\omega(a)}$ might be sub-exponential in $\log b$, in our application $\omega(a)$ will be a constant (in fact $\omega(a) \leq 1$).

5.2. **Finding elements in a special maxinmal order** The following immediate corollary allows us to sample elements from the special maximal order O_0 in $B_{p,\infty}$ as defined in the lemma 2.3.

Corollary 5.3. *There exists an algorithm $\mathcal{A}$ such that the following holds. For any integer n and prime p with $(n,p) = 1$ and $n \gg_\epsilon p^{12+\epsilon}$ for every $\epsilon > 0$, $\mathcal{A}$ finds an element $\alpha \in \mathcal{O}_0$ with $\text{Nrd}(\alpha) = n$. Using our oracle $\mathscr{O}$, the algorithm runs in expected polynomial time in terms of $\log(p)$, $\log(n)$.*

Proof. From lemma 2.3 we know that elements $\alpha = s + t\omega + xj + y\omega j \in R + Rj \subset \mathcal{O}_0$ satisfy

$$\text{Nrd}(\alpha) = f(x,y) + pf(s,t),$$

where $disc(f) = O(\log^2(p))$ in the worst case (here its the only time we assume GRH). We note that in order to apply Theorem 5.1 we need $f(x,y) + pf(s,t) \equiv n \ mod \ 2^7 det^3(A)$ to be solvable. The equivalence is immediate modulo any prime q, we then apply Hensel's Lemma (Multivariable version) to lift the solution to a suitable prime power and then use the Chinese remainder theorem to obtain a solution module $2^7 det^3(A)$. The condition on ϵ comes from the fact that we need $n > C_\epsilon N^{8+\epsilon} det^{2+\epsilon}(A)$ where $N = p \cdot disc(f)$ is the level of our quadratic form $f(x,y) + pf(s,t)$, i.e. $n \gg_\epsilon p^{12+\epsilon} \log(p)^{36+\epsilon}$, assuming p is large enough. □

6. Solving the quaternion path problem

For the remaining sections we consider our special maximal order $\mathcal{O}_0$ from lemma 2.3 in the quaternion algebra $B_{p,\infty}$. The main idea of this section is to solve the QuaternionPath problem. Since there exist efficient algorithms to compute connecting ideals between maximal orders, see for instance [KV10], our problem is reduced to the following: given a maximal order $\mathcal{O}$ in $B_{p,\infty}$, a left $\mathcal{O}$-ideal I, and an integer N, find an equivalent ideal J of $\text{Nrd}(J) = N$. In [[KLPT14], section 4.6], its been argued that the general case reduces to the special maximal order $\mathcal{O}_0$ and hence we focus on this one.

6.2. **Solving the quaternion path problem.**

Theorem 6.1. *For every $\epsilon > 0$ there exists a constant C_ϵ such that for integers $n_1, n_2 \geq C_\epsilon p^{345+\epsilon}$ with $n_2 l^e \not\equiv 2, 4 \pmod 8$ for $e \in \{0,1\}$, and a prime ℓ, Algorithm 3 is correct and runs in expected polynomial time in $\log p$, $\log n_i$, $\log \text{Nrd}(I)$, assuming access to a factoring oracle $\mathscr{O}$.*

Proof. Most of the steps have been explained thoroughly in [Wes21] like 3, 6 and 8, where the proof follows analogously. The constraints on n_1 and n_2 are coming from Theorem 5.1, where the level of our Gram matrix is $N^2 p^2 disc(f)$ and $det(A) = N^5 p^2 disc^2(f)$.

Step 5. The approach is exactly as in [Wes21], where our γ also has large entropy from 5.1. We just use our unconditional result, namely corollary 5.3 which requires $N \geq C_\epsilon p^{12+\epsilon}$

Step.9 From 5.1, we require $N^2 f(s,t) + p f^\Gamma(x,y) = n_2 l^e$ to be solvable modulo $2^7 det^3(A)$ where A is the Gram matrix of $N^2 f(s,t) + p f^\Gamma(x,y)$. Using Hensel's lemma and the Chinese Remiander Theorem, its sufficient to prove the equation is solvable modulo N, p, and $disc(f)$.
Since ℓ is a quadratic non residue modulo N, we choose the parity of the exponent e depending on whether $p f^\Gamma(x,y)$ is a quadratic residue or not.
Reducing the equation modulo p and using the fact that N is invertible mod p, gives $f(s,t) \equiv N^{-2} n_2 l^e$, where $f(s,t) = s^2 + qt^2$ with $q = 1, 2$ or q_p depending whether $p \equiv 3 \mod 4$, $p \equiv 5 \mod 8$, or $p \equiv 1 \mod 8$ according to lemma 2.1. Using the fact that in $\mathbb{Z}/p\mathbb{Z}$ every element is a sum of two squares, and a sum of a quadratic residue and non residue we obtain a solution *modulo p*.
To ensure there's a solution in $\mathbb{Z}/disc(f)\mathbb{Z}$ we take it into cases and follow Wesolowski's proof. Assume $p \equiv 1 \mod 8$. From lemma 2.1, we know that the discriminant $\text{disc}(f)$ is a negative odd prime. According to Theorem 3.15 from [Cox11], there is only one type of quadratic form with this discriminant, which means f can represent every quadratic residue in $\mathbb{Z}/\text{disc}(f)\mathbb{Z}$. Since N and $\text{disc}(f)$ are relatively prime, the form f^Γ also represents all quadratic residues in $\mathbb{Z}/\text{disc}(f)\mathbb{Z}$. By Lemma 2.2, p isn't a quadratic residue. In $\mathbb{Z}/\text{disc}(f)\mathbb{Z}$, any element can be written as the sum of a quadratic residue and a quadratic non-residue, so $n_2 l^e$ can be represented this way as well. Similarly, if $\text{disc}(f) = 4$, there is a solution when $n_2 l^e \not\equiv 2 \mod 4$, and if $\text{disc}(f) = 8$, there is a solution when $n_2 l^e \not\equiv 4 \mod 8$; this finishes the proof. □

Algorithm 3 QuaternionPath$_\epsilon(I, n_1, n_2, l)$

Input: A left ideal I in a special maximal order $\mathcal{O}_0$, positve integers n_1, n_2 and a prime ℓ.
Output: An equivalent ideal J of norm $n_1 n_2$ or $n_1 n_2 l$.

Define R, ω, and f as in lemma 2.3;
while β has not been found **do**
  Random walk in the Brandt graph to obtain $I' \subset I$ of norm n_1; {Theorem 2.9}
  Find an element $\rho \in I'$ such that $I'' = I'\rho/\text{Nrd}(I)$ equivalent to I' of prime norm $N \in [C_\epsilon p^{12+\epsilon}, C_\epsilon p^{12.5+\epsilon}]$ and ℓ is a quadratic non residue modulo N; {Proposition 3.6, *with* $\theta = \frac{1}{2}$}.
  Find an element $\gamma \in \mathcal{O}_0$ such that $\text{Nrd}(\gamma) = N$; {Corollary 5.3}
  Find an element $\beta \in R$ such that $I'' = \mathcal{O}_0 N + \mathcal{O}_0 \beta j$ if it exists;
end while
Find a matrix $\Gamma \in M_{2\times 2}(\mathbb{Z})$ such that $\mathbb{Z}\beta + RN = \{x + y\omega \mid (x,y) \in \mid \Gamma\mathbb{Z}^2\}$;
Find an integral solution (s,t,x,y) of $N^2 f(s,t) + p f^\Gamma(x,y) = n_2 l^e$ for $e \in \{0,1\}$; {Theorem 5.1}
Set $(x', y') = \Gamma(x,y)$, and $\alpha = (s + t\omega)N + (x' + y'\omega)j$;
Set $\delta = \rho\gamma\alpha/N \in I' \subset I$;
return $J = I\bar{\delta}/\text{Nrd}(I)$

Remark 5. In [[Wes21], theorem 6.3] the analogous result requires $\log(n_i) > (\log p)^c$, for some integer $c > 0$ (in fact one can show that $c \geq 2$). Hence theorem 6.1 provides a significat enhancement over the previous results. Additionally for the purposes of analysis and applications, for instance as in [GPS20], the output ideal is assumed to satisfy $\log(\text{Nrd}(J)) = O(\log p)$.

Theorem 6.1 immediately specializes to the prime power norm case, where one can choose n_1 and n_2 to be large enough powers of ℓ, where ℓ is a prime. However for most applications we require our ideal to be B-powersmooth for some bound $B > 0$. This becomes useful when computing isogenies of large degrees by decomposing them into isogenies whose degrees are powersmooth. For that purpose, we prove the following important corollary to solve the B-PSQuaternionPath problem

which enhances the bound B from [Wes21], essentially replacing $(\log p)^c$ for large c by a more refined bound of order $\log p$.

Theorem 6.2. *For every $\epsilon > 0$ there exists a constant $C_\epsilon > 0$ and an algorithm $\mathcal{A}$ which on input a left $\mathcal{O}_0$-ideal I, returns an equivalent ideal J whose norm is $(C_\epsilon \log p)$-powersmooth. Given $\mathscr{O}$, the algorithm runs in expected polynomial time in $\log p$ and $\log \mathrm{Nrd}(I)$.*

Proof. As stated in [Wes21], its enough to find two powersmooth integers n_1 and n_2 to apply Theorem 6.1. Let C_ϵ be a constant to be adjusted, and let

$$n_1 = n_2 = \prod_{\substack{l \text{ prime} \\ \log p < l < C_\epsilon \log p}} l$$

Using Theorem 6.9 from [Dus10] which states that

$$\frac{x}{\ln x}\left(1 + \frac{1}{\ln x}\right) \leq \pi(x) \leq \frac{x}{\ln x}\left(1 + \frac{1.2762}{\ln x}\right) \quad \forall x > 599, \tag{11}$$

we obtain that

$$\log(n_i) = \sum_l \log(l) \geq (\log\log p)\log p\left(\frac{C_\epsilon}{\log(C_\epsilon \log p)} - \frac{1}{\log\log p}\right) \geq (C_\epsilon/2 - 1)\log p,$$

by adjusting C_ϵ so that $C_\epsilon/2 - 1 > 345 + c_\epsilon$ ensures that $n_i > c_\epsilon p^{345+\epsilon}$ where c_ϵ is the constant from theorem 6.1; this finishes the proof. (notice we secretly assume $\log p > 599$ to apply 11) □

We finish this section with an algorithm which on input a left $\mathcal{O}_0$-ideal of prime power norm, outputs the corresponding isogeny φ_I.

Algorithm 4 Ideal to prime power isogeny

Input: A left $\mathcal{O}_0$-ideal of norm l^e with ℓ prime, $l \neq p$ and $l \nmid I$.
Output The corresponding isogeny φ_I of degree l^e.

1: Find the constant C_ϵ from Theorem 6.2;
2: **for** $i = 1, 2, ...e$ **do**
3: Set $I_i = I + \mathcal{O}_0 l^i$;
4: Find J_i equivalent to I_i of $(C_\epsilon \log p)$-powersmooth norm; {Theorem 6.2}
5: Translate J_i into an isogeny ψ_i; {Lemma 2.6}
6: Set E_i to be the target curve of ψ_i;
7: Compute the *ℓ-isogeny* φ_i from E_{i-1} to E_i using Velu's formulae; [Vel71]
8: **end for**
9: **return** $\varphi_e \circ \cdots \varphi_1$.

Lemma 6.3. *Algorithm 4 is correct an runs in expected polynomial time in $\log p$, ℓ and e, (if $p \equiv 1 \mod 8$ we assume GRH).*

Proof. This version appeared in ([Wes21]-Algorithm 4), using Theorem 6.2 instead makes the result unconditional. □

7. Equivalence Of MaxOrder And IsogenyPath

7.1. **Reducing IsogenyPath to MaxOrder.** We now show the first direction in our reduction, namely if we have two supersingular elliptic curves E_1 and E_2 with $End(E_1) \cong \mathcal{O}_1$ and $End(E_2) \cong \mathcal{O}_2$ then we can find an isogeny path from E_1 to E_2 in the ℓ-isogeny graph.

Algorithm 5 Reducing ℓ-IsogenyPath to MaxOrder.

Input: Two supersingular elliptic curves E_1, E_2 over $\mathbb{F}_{p^2}$. We assume we have access to an algorithm $\mathcal{A}_{MaxOrder}$ which solves the MaxOrder problem and outputs $\mathcal{O}_1 \cong End(E_1)$, $\mathcal{O}_2 \cong End(E_2)$ in $B_{p,\infty}$.
Output An ℓ-isogeny $\varphi : E_1 \to E_2$.

Find $\mathcal{O}_1$ and $\mathcal{O}_2$ in $B_{p,\infty}$ using $\mathcal{A}_{\text{MaxOrder}}$;
Find C_ϵ from Theorem 6.2 for $\epsilon > 0$;
Set $e = \lceil \frac{C_\epsilon \log p}{\log \ell} \rceil$;
Find the special order and curve $(\mathcal{O}_0, E_0)$ from lemmas 2.3 and 2.5;
for $i = 1, 2$ **do**
    Compute ideal $I_i = I(\mathcal{O}_0, \mathcal{O}_i)$ connecting $\mathcal{O}_0$ to $\mathcal{O}_i$; { [KV10]}
    Compute J_i equivalent to I_i using QuaternionPath$_\epsilon(I_i, \ell^e, \ell^e, \ell)$; {Algorithm 3}
    Translate J_i into the corresponding isogeny φ_i; {Algorithm 4}
end for
return $\varphi = \varphi_2 \circ \hat{\varphi}_1$.

Theorem 7.1. *Given $\mathscr{O}$, algorithm 5 is correct and runs in expected polynomial time in* $\log p$, ℓ *and the length of outputs $\mathcal{O}_1$, $\mathcal{O}_2$ of $\mathcal{A}_{MaxOrder}$ (if $p \equiv 1 \mod 8$ we assume GRH).*

Proof. The idea is to make use of our special maximal order $\mathcal{O}_0$, by connecting it to each of $\mathcal{O}_1$ and $\mathcal{O}_2$ and then use the QuaternionPath algorithm. This reduction is similar to Algorithm 7 in [EHL+18]. However instead of reducing to EndRing as in [EHL+18] we reduce to MaxOrder, and we use our unconditional result instead of [KLPT14]. □

7.2. **Reducing MaxOrder to IsogenyPath.** In the reverse direction, given a supersingular elliptic curve E, we prove that an isoegny from E_0 (with known endomorphism ring) to E allows one to retrieve the endomorphism ring of E.

Theorem 7.2. *Given $\mathscr{O}$, algorithm 6 is correct and runs in expected polynomial time in* $\log p$, *and output size of the $\mathcal{A}_{l\text{-IsogenyPath}}$, in addition to the complexity time to perform $\mathcal{A}_{\ell\text{-IsogenyPath}}$.*

Proof. A version of this algorithm has first appeared in [[DMPS19]-6.2], and then [Wes21]. Writing $\varphi_i : E_{i-1} \to E_i$ with $E_e = E$, we see that each step of the loop J_i is equivalent to the ideal induced by the isogeny $\varphi_i \circ \cdots \circ \varphi_0$. Since the running time of the algorithm in 2.7 is polynomial in $\max(l_i^{e_i})$, i.e. polynomial in p, we resort to Theorem 6.2 instead of 6.1 in constructing our equivalent ideal J_i, and this proves the correctness of the algorithm. The running time follows from our previous results in each step of our algorithm. In particular, if we're given two arbitrary supersingular elliptic curves E_1 and E_2, then one can recover both maximal orders $\mathcal{O}_1 \cong End(E_1)$ and $\mathcal{O}_2 \cong End(E_2)$. This can be done by constructing an ℓ-isogeny path from our special curve E_0 to E_1 and E_2, and applying Algorithm 5. □

Algorithm 6 Reducing MaxOrder to ℓ-IsogenyPath

Input: A supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$. We assume there is an algorithm $\mathcal{A}_{\ell\text{-IsogenyPath}}$ which solves the ℓ-IsogenyPath problem.
Output: A basis for $O \cong End(E)$ in $B_{p,\infty}$.

Compute $(\mathcal{O}_0, E_0)$ the special maximal order and curve using lemma 2.5;
Compute C_ϵ from Theorem 6.2 for $\epsilon > 0$;
Find an isogeny $\varphi = \varphi_e \circ \cdots \circ \varphi_1 : E_0 \to E$ with $\deg(\varphi_i) = \ell$ using $\mathcal{A}_{l\text{-IsogenyPath}}(E_0, E)$
Set $\psi_0 = id_{E_0}$
for $i = 1, 2, \ldots, e$ **do**
    Compute the ideal I_i corresponding to $\varphi_i \circ \psi_i$; {Lemma 2.7}
    Compute J_i of $(C_\epsilon \log p)$-powersmooth norm in the same class as I_i; {Theorem 6.2}
    Translate J_i into it's corresponing isogeny ψ_i; {Lemma 2.6}
end for
Compute $O_R(J_e)$; [[Ron92], Theorem 3.2]
Set $\mathcal{O} = O_R(J_e)$
return a basis for $\mathcal{O}$.

8. Equivalence Of MaxOrder And Endomorphism Ring

In this section we prove that the Maximal Order and Endomorphism ring problems are equivalent. We start by proving the easier direction.

8.1. **Reducing EndRing to MaxOrder.** Given a supersingular elliptic curve E, if we have an algorithm which solves MaxOrder, we show to recover the endomorphism ring of E.

Theorem 8.1. *Given $\mathcal{O}$, algorithm 7 is correct and runs in expected polynomial time in* $\log p$ *and the length of output of* $\mathcal{A}_{\text{MaxOrder}}$.

Proof. This version of the algorithm appeared in [[EHL$^+$18]-Algorithm 4], we just use our unconditional result instead of [KLPT14]. The endomorphisms' representation is certainly not the most natural, yet we can still evaluate points P on our elliptic curve E in polynomial time. □

Algorithm 7 Reducing EndRing to MaxOrder

Input: A supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, with $p \neq \ell$. We suppose we have an algorithm $\mathcal{A}_{\text{MaxOrder}}$ which solves the MaxOrder problem.
Output: Four endomorphisms of E that generate $End(E)$.

Use Algorithm $\mathcal{A}_{\text{MaxOrder}}$ to obtain a maximal order $\mathcal{O} \cong End(E)$.
Compute C_ϵ from Theorem 6.2 for $\epsilon > 0$;
Compute $(\mathcal{O}_0, End(E_0))$ the special maximal order using lemma 2.5;
Find an ideal I connecting $\mathcal{O}_0$ and $\mathcal{O}$; [KV10]
Compute an ideal J of $(C_\epsilon \log p)$-powersmooth norm N in the same class as I; {Theorem 6.2}
Translate J into its corresponding isogeny φ; {Lemma 2.6}
Set $1, \phi_2, \phi_3, \phi_4$ to be the generators of $End(E_0)$;
Set $(1, \omega_2, \omega_3, \omega_4)$ and $(1, \alpha_2, \alpha_3, \alpha_4)$ to be the generators of $\mathcal{O}$ and $\mathcal{O}_0$ respectively.
Find integers $(c_{ij})_{i,j=1}^4$ such that $\text{Nrd}(J)\omega_i = \sum_{j=1}^4 c_{ij}\alpha_j$
return $(N, \varphi, (c_{ij})_{i,j=1}^4)$ representing the endomorphisms $\frac{1}{N}\sum_{j=1}^4 c_{ij}\varphi\phi_j\hat{\varphi}$.

8.2. **Reducing MaxOrder to EndRing:** This is last direction in our reductions, namely that MaxOrder reduces to EndRing. The approach in [EHL+18] succeeds under heuristic assumptions that some numbers appearing in the algorithm behave like random numbers and hence are easy to factor. The approach followed in [Wes21] was to force such numbers to be primes, to avoid factorisation, and make use of a sampling algorithm (essentially 3.4 with GRH) along with an explicit parameterisation of solutions of quadratic forms. Since we assume we can factor integers with our oracle $\mathscr{O}$, we will follow [EHL+18], and for the sake of specialization to Shor's quantum algorithm which runs in $O(\log^3(p))$ we will show that such integers are at most $p^{O(1)}$ rather than doubly exponential in p.

Algorithm 8 Reducing MaxOrder to EndRing

Input: A supersingular elliptic curve E over $\mathbb{F}_{p^2}$. We assume there is an algorithm $\mathcal{A}_{\text{EndRing}}$ which solves the EndRing problem.

Output: A maximal order $\mathcal{O} \subset B_{p,\infty}$ such that $\mathcal{O} \cong End(E)$.

1: Use $\mathcal{A}_{\text{EndRing}}$ to output four endomorphism $1, \alpha_2, \alpha_3, \alpha_4$ generating $End(E)$;
2: Compute the Gram matrix G_0 of the sequence $(1, \alpha_2, \alpha_3, \alpha_4)$
3: Find a rational invertible linear transformation mapping $(1, \alpha_2, \alpha_3, \alpha_4)$ to some $(1, \beta_2, \beta_3, \beta_2\beta_3)$ where $1, \beta_2, \beta_3, \beta_2\beta_3$ are orthogonal basis for $B_{p,\infty}$ over $\mathbb{Q}$;
4: Factorise the numerator and denomenantor of $\text{Nrd}(\beta_2)$ and $\text{Nrd}(\beta_3)$ using $\mathscr{O}$;
5: Compute $a, b, c \in \mathbb{Q}$ such $\text{Nrd}(\iota) = q$, where $\iota = a\beta_2 + b\beta_3 + c\beta_2\beta_3$; [Sim05]
6: Find a rational invertible linear transformation mapping $(1, \beta_2, \beta_3, \beta_2\beta_3)$ to $(1, \iota, \delta, \iota\delta)$ for some $\delta \in B_{p,\infty}$, with $(1, \iota, \delta, \iota\delta)$ orthogonal basis for $B_{p,\infty}$ over $\mathbb{Q}$;
7: Factorise the numerator and denominator of $\text{Nrd}(\delta)$ using $\mathscr{O}$;
8: Compute $a, b \in \mathbb{Q}$ such that $\text{Nrd}(\delta)(a^2 + qb^2) = p$ using Cornacchia's algorithm; [Cor08]
9: Find a a rational invertible linear transformation sending $(1, \iota, \delta, \iota\delta)$ to $(1, \iota, \lambda, \iota\lambda)$;
10: Invert and compose all linear transformation to write $(1, \alpha_2, \alpha_3, \alpha_4)$ in terms of $(1, \iota, \lambda, \iota\lambda)$;
11: Compute a basis for $\mathcal{O}$ in $B_{p,\infty}$;
12: **return** the basis of $\mathcal{O}$.

Theorem 8.2. *Given $\mathscr{O}$, algorithm 8 is correct and runs in expected polynomial time in* $\log p$ *and the length of output of $\mathcal{A}_{\text{EndRing}}$.*

Proof. This is exactly Algorithm 6 from [EHL+18], the only subtlety is in steps 4, 5.

Step 4. In order to be able to factorise the numerator and denominator of $\text{Nrd}(\beta_2)$ and $\text{Nrd}(\beta_3)$ we need to show that they're at most $p^{O(1)}$ in order for Shor's algorithm to run in polynomial time. Using the fact that the height of a matrix $||G|| \leq \det(G)$ (the largest entry of the matrix in absolute value) and that the Gram matrix $G_0 = (v_1, v_2, v_3, v_4) = (a_{ij})_{i,j}$ has determinant $\det(G_0) = \det(End(E)) = p^2$, we obtain $|a_{i,j}| \leq p^2$.
Since the matrix $G = (q_1, q_2, q_3, q_4)$ corresponding to $(1, \beta_2, \beta_3, \beta_2\beta_3)$ is obtained by applying Gram-Schmidt orthogonalization process to G_0, we conclude that the Numerator and denominator of each entry of G is at most $p^{O(1)}$, and so is the numerator and denominator of $\text{Nrd}(\beta_2)$, $\text{Nrd}(\beta_3)$ and $\text{Nrd}(\delta)$ in step 7.

Step 5. This step can be solved using an algorithm of [[Sim05]- section 8] where instead of finding $a, b, c \in \mathbb{Q}$, we find an integral solution $(a', b', c', d') \in \mathbb{Z}^4$ satisfying

$$\text{Nrd}(\beta_2)a'^2 + \text{Nrd}(\beta_3)b'^2 + \text{Nrd}(\beta_2)\text{Nrd}(\beta_3)c'^2 = qd'^2.$$

The algorithm runs in polynomial time provided that the factorisation of the numerator and denominator of $\mathrm{Nrd}(\beta_i)$ are given. This finishes the proof. □

9. Acknowledgements

The author expresses his sincere gratefulness to Dr. Kirsten Eisentraeger for her assistance and guidance on this paper. The author would also like to thank Dr. Robert Vaughan and Jerermy Rouse for their feedback on several aspects of this paper related to analytic number theoretic results.

References

[CD22] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH (preliminary version). Cryptology ePrint Archive, (2022).

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

[CLM+18] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: an effi- cient post-quantum commutative group action. In Thomas Peyrin and Steven D. Galbraith, editors, Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, volume 11274 of Lecture Notes in Computer Science, pages 395–427. Springer, (2018).

[Cox11] David A Cox. Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication, volume 34. John Wiley & Sons, 2011.

[CPV20] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. In Anne Canteaut and Yuval Ishai, editors, Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, volume 12106 of Lecture Notes in Computer Science, pages 523–548. Springer, 2020.

[Coh13] Henri Cohen. A course in computational algebraic number theory, volume 138. Springer Science & Business Media, (2013).

[Cor08] Cornacchia, G.: Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} c_h x^{(}n - h)y^h$. Giornale di Matematiche di Battaglini. 46: 33–90 (1908).

[DMPS19] Luca De Feo, Simon Masson, Christophe Petit, and Antonio Sanso. Verifiable delay functions from supersingular isogenies and pairings. In Steven D. Galbraith and Shiho Moriai, editors, Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, volume 11921 of Lecture Notes in Computer Science, pages 248–277. Springer, (2019).

[Dub14] C. Dubey and T. Holenstein, "Sampling a Uniform Solution of a Quadratic Equation Modulo a Prime Power," in *Leibniz International Proceedings in Informatics* (2014).

[Dus10] Dusart, Pierre. "Estimates of Some Functions Over Primes without R.H." arXiv: Number Theory (2010): n. pag.

[EHL+18] Eisenträger, Kirsten, Sean Hallgren, Kristin E. Lauter, Travis Morrison and Christophe Petit. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions." International Conference on the Theory and Application of Cryptographic Techniques (2018).

[GPS16] Galbraith, S.D., Petit, C., Shani, B., Ti, Y.B.: On the security of super- singular isogeny cryptosystems. In: Cheon, J.H., Takagi, T. (eds.) ASI- ACRYPT 2016, Part I. LNCS, vol. 10031, pp. 63–91. Springer, Heidelberg (2016).

[GPS17] Galbraith, S.D., Petit, C., Silva, J.: Identification protocols and signature schemes based on supersingular isogeny problems. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10624, pp. 3–33. Springer, Cham (2017)

[GPS20] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. Journal of Cryptology, 33(1):130–175, 2020.

[Iwa04] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Colloquium Publications, vol. 53, Providence, RI: American Mathematical Society, (2004).

[Iwa12] H. Iwaniec, *Topics in Classical Automorphic Forms* Providence, RI: American Mathematical Society, (2012).

[JDF11] Jao, D., De Feo, L.: Towards quantum-resistant cryptosystems from super- singular elliptic curve isogenies. In: Yang, B.-Y. (ed.) PQCrypto 2011. LNCS, vol. 7071, pp. 19–34. Springer, Heidelberg (2011).

[KLPT14] Kohel, David R., Kristin E. Lauter, Christophe Petit and Jean-Pierre Tignol. “On the quaternion -isogeny path problem.” LMS J. Comput. Math. 17 (2014): 418-432.

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

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

[Lin41] Linnik, U.V.: The large sieve. C. R. (Doklady) Acad. Sci. URSS (N.S.) 30, 292–294 (1941).

[LO77] J.C. Lagarias and A.M. Odlyzko. Effective versions of the Chebotarev density theorem. In Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pages 409–464. Academic Press, London, (1977).

[MM22] Luciano Maino and Chloe Martindale. An attack on SIDH with arbitrary starting curve. Cryptology ePrint Archive, 2022.

[Pall46] Gordon Pall. The completion of a problem of Kloosterman. Amer. J. Math., 68:47–58, (1946).

[Piz80] Arnold Pizer. An algorithm for computing modular forms on 0(n). Journal of algebra, 64(2):340–390, (1980).

[Rob22] Damien Robert. Breaking SIDH in polynomial time. Cryptology ePrint Archive, (2022).

[Ron92] Rónyai, L. Algorithmic properties of maximal orders in simple algebras over Q. Computational Complexity 2, 225–243 (1992

[Rouse14] Jeremy Rouse. Quadratic forms representing all odd positive integers. Amer. J. Math., 136(6):1693–1745, (2014)

[Rouse18] Rouse, Jeremy A. Integers represented by positive-definite quadratic forms and Petersson inner products. Acta Arithmetica (2018)

[Ser73] J.-P. Serre. A course in arithmetic, volume No. 7 of Graduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg, (1973). Translated from the French.

[Sil86] Joseph H. Silverman. The Arithmetic of Elliptic Curves, volume 106 of Gradute Texts in Mathematics. Springer-Verlag, (1986).

[Sim05] Simon, D.: Quadratic equations in dimensions 4, 5 and more. Preprint (2005).

[Shi6] Goro Shimura. Classification, construction, and similitudes of quadratic forms. Amer. J. Math., 128(6):1521–1552, (2006).

[Tar29] W. Tartakowsky, Die Gesamtheit der Zahlen, die durch eine positive quadratische Form $f(x_1, ..., , x_s)$ darstellbar sind, Izv. Akad. Nauk. SSSR 7 (1929), 111–122, 165–195.

[Vel71] J. V elu. Isog enies entre courbes elliptiques. Comptes rendus de l'Acad emie des Sciences, S eries A-B, 273:A238–A241, (1971).

[Voi21] John Voight. Quaternion Algebras. Springer International Publishing. Graduate Texts in Mathematics, No. 288, (2021)

[Wes21] B. Wesolowski, "The supersingular isogeny path and endomorphism ring problems are equivalent," 2021 IEEE 62nd Annual Symposium on Foundations of Computer Science (FOCS), Denver, CO, USA, (2022), pp. 1100-1111.