



The Supersingular ℓ -Isogeny Path and Endomorphism Ring Problems: Tighter Unconditional Reductions

Maher Mamah  

University of Waterloo, Department of Combinatorics and Optimization, Waterloo, Canada

Abstract. We prove that the supersingular ℓ -isogeny path problem and the endomorphism ring problem are equivalent via polynomial time reductions given access to a factoring oracle. While prior work related the endomorphism Ring problem to the general Isogeny Path problem, the ℓ -isogeny path case remained out of reach unconditionally. We show that a factoring oracle suffices to solve the Quaternion Path Problem of KLPT, removing the heuristic and GRH-based assumptions of previous works. Combined with Shor’s factoring algorithm, this yields unconditional quantum polynomial time equivalences between ℓ -ISOGENY PATH and ENDOMORPHISM RING. Our result strengthens a previous work of Wesolowski’s reduction by trading the generalized Riemann Hypothesis for a factoring oracle and achieving polynomial-time equivalences with significantly lower polynomial degree, whereas the original reduction incurs a polynomial overhead of impractically high degree.

Keywords: isogeny-based cryptography · isogeny path problem · endomorphism ring problem · reductions

1 Introduction

Isogeny-based cryptography has attracted significant attention for its potential quantum resistance. While RSA and classical elliptic-curve cryptography admit polynomial-time quantum attacks, the best known attacks on many isogeny-based schemes remain exponential. Their security often relies on the presumed hardness of the *supersingular isogeny path problem*: given two supersingular elliptic curves, find an isogeny between them.

A closely related problem is the *endomorphism ring problem* (ENDRING), which asks to compute the endomorphism ring of a supersingular elliptic curve. Studied since Kohel [Koh96], it underlies several cryptosystems, including [GPST16, CPV20, CLG09, DFKL⁺20, BBC⁺25].

Kohel, Lauter, Petit, and Tignol [KLPT14] introduced a heuristic algorithm for the quaternionic analogue of isogeny path, the *quaternion path problem*. Using this, Eisenträger et al. [EHL⁺18] proved a heuristic polynomial-time equivalence between isogeny path and ENDRING; Wesolowski [Wes22] later proved the equivalence unconditionally under GRH.

A closer look at [KLPT14, Wes22] shows that integer factorization is a fundamental bottleneck in the quaternion path problem. We show that this difficulty is intrinsic and requires new techniques. Our methods are inspired by [Wes22] but differ in several key respects. In particular, whereas previous approaches rely on variants of the Generalized

The author acknowledge support of the NSERC Alliance Consortia Quantum Grant “Accelerating the transition to quantum-resistant cryptography” (ALLRP 578463–2022), and the NSERC Discovery Grant program, held by Dr. David Jao and Douglas Stebila

E-mail: mmamah@uwaterloo.ca (Maher Mamah)



Riemann Hypothesis and incur large polynomial overheads, we show that working in the quantum setting allows one not only to remove the dependence on GRH but also to obtain conceptually simpler and substantially tighter results. We note that in the case where the underlying prime field $p \equiv 1 \pmod{8}$ GRH needs to be assumed to obtain an efficient representation of the underlying quaternion algebra, otherwise it's unnecessary in our core reduction; see [Remark 1](#) for more discussion on this.

Isogeny-based problems. Fix primes p and ℓ (typically $\ell = 2$ or 3). Supersingular elliptic curves over $\mathbb{F}_{p^2}$ form the vertices of the supersingular ℓ -isogeny graph, with edges given by ℓ -isogenies. This graph is $(\ell + 1)$ -regular, has about $p/12$ vertices, and is Ramanujan, hence rapidly mixing. Many cryptographic constructions rely on the presumed hardness of navigating this graph. This motivates the following problem.

Problem 1 (ℓ -ISOGENYPATH). Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, find an isogeny $\varphi : E \rightarrow E'$ of degree ℓ^e for some $e \geq 0$.

This may be viewed as finding a path between E and E' in the ℓ -isogeny graph. Several cryptographic schemes (e.g. [\[CLG09, GPS20\]](#)) rely on the hardness of this problem. A relaxed variant removes the restriction on the degree.

Problem 2 (ISOGENYPATH). Given supersingular elliptic curves $E, E'/\mathbb{F}_{p^2}$, find an efficiently computable isogeny $\varphi : E \rightarrow E'$.

While Problem 2 is formally weaker, it is not a priori clear whether it is easier. Understanding the relationship between these problems leads naturally to endomorphism computations.

Indeed, endomorphism rings of supersingular elliptic curves over $\mathbb{F}_{p^2}$ are isomorphic to maximal orders in the quaternion algebra $B_{p,\infty}$. This motivates the following problems.

Problem 3 (ENDRING). Given a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, compute a generating set for $\text{End}(E)$ in efficient representation.

Problem 4 (MAXORDER). Given p and $E/\mathbb{F}_{p^2}$ supersingular, compute a maximal order $\mathcal{O} \subset B_{p,\infty}$ such that $\mathcal{O} \simeq \text{End}(E)$.

It was shown in [\[PW24\]](#) that ISOGENYPATH and ENDRING are unconditionally equivalent under polynomial-time reductions. However, these reductions are not tight classically (see [\[ABDF⁺25, Section 6\]](#)). In a recent work [\[LMW25\]](#), Le Merdy and Wesolowski proved unconditional reductions between Problems 2, 3, and 4. The ℓ -ISOGENYPATH problem, however, remained open unconditionally and plays a vital role in protocols like SQIsign [\[AAA⁺25\]](#).

These problems are most naturally studied in the quaternionic setting, where isogenies correspond to ideals between maximal orders, leading to the following problem.

Problem 5 (QUATERNIONPATH). Given maximal orders $\mathcal{O}_1, \mathcal{O}_2 \subset B_{p,\infty}$ and a set $\mathcal{N} \subset \mathbb{Z}_{>0}$, find a left $\mathcal{O}_1$ -ideal I with $\text{Nrd}(I) \in \mathcal{N}$ and right order $\mathcal{O}_R(I) \simeq \mathcal{O}_2$. If $\mathcal{N} = \{\ell^e : e \in \mathbb{N}\}$, we write ℓ -QUATERNIONPATH.

When $\mathcal{N}$ consists of B -power smooth integers, we call the problem B -PSQUATERNIONPATH.

Contributions & Organization of the paper. Section 2 reviews background material on elliptic curves, the supersingular setting, and quadratic forms. Section 2 develops the analytic tools required for representing integers and primes by quaternary quadratic forms and plays a foundational role in the remainder of the paper.

In Section 3, we present algorithms for sampling vectors $\mathbf{v} \in \mathbb{Z}^4$ such that a special quaternary quadratic form $Q(\mathbf{v})$ is prime, equivalently sampling ideals of prime norm within a fixed ideal class of a maximal order. Section 4 introduces the main algorithm for solving norm form equations of the type

$$af(s, t) + bg(x, y) = n,$$

where f and g are definite quadratic forms.

Section 5 contains the principal result of the paper, giving an algorithmic solution to the QUATERNIONPATH problem and its variant B -PSQUATERNIONPATH. Finally, we establish the equivalence between ℓ -ISOGENYPATH and MAXORDER in Section 6, between ENDRING and MAXORDER in Section 7, and between ISOGENYPATH and ℓ -ISOGENYPATH in Section 7.

In a nutshell, establishing the equivalence of the aforementioned problems reduces to solving the QUATERNIONPATH problem. This is accomplished in Theorem 7, which constitutes the main technical contribution and accounts for the largest part of the work.

More specifically, the approach requires first sampling quaternionic ideals of prime norm within a prescribed ideal class, and then solving the above Diophantine equation, together with some linear algebra computations. Addressing both the prime-norm ideal sampling and the solution of these equations relies on obtaining sufficiently tight analytic estimates, which form the focus of section 2.

A Note on previous reductions. From a theoretical and practical standpoint, existing reductions exhibit significant limitations. As previously mentioned, the conditional reductions of [Wes22] as stated and proved, while polynomial-time in theory, are far from tight. More precisely, given an algorithm that solves the ENDRING problem in time $T(n)$, where n denotes the input size, the corresponding reduction in [Wes22] yields an algorithm for ℓ -ISOGENYPATH running in time $T(n) + q(n)$, where $q(n)$ is a polynomial overhead with $\deg(q) > 12320$. Consequently, despite being polynomial-time asymptotically, such reductions incur an overhead that renders them impractical for cryptographic parameter sizes. In other words, we have no guarantee that ENDRING and ℓ -ISOGENYPATH problem are equivalently hard except when p is astronomically large. We refer the interested reader to Remark 5 for more details regarding the claimed degree overhead and Remark 3 on our reduction's complexity.

Factoring oracle. We assume access to a factoring oracle $\mathcal{O}$ for factoring large integers, which is required from Section 4 onward. Factoring appears unavoidable in our treatment of QUATERNIONPATH: previous approaches use Cornacchia's algorithm to solve equations such as $x^2 + dy^2 = m$, which requires the factorization of m and becomes inefficient when m is highly composite. In our setting, such highly composite inputs may arise. We use the algorithm of [Mam25], which solves $f(s, t) = m$ for definite binary quadratic forms f and remains efficient when $\text{disc}(f) = \text{polylog}(m)$, as is the case here. In the post-quantum setting, Shor's algorithm plays naturally the required factoring oracle.

1.1 Background on Elliptic curves.

We refer the reader to [Sil86] for background. An elliptic curve E over a field K of characteristic $p > 3$ is defined by

$$y^2 = x^3 + Ax + B,$$

with $A, B \in K$ and $4A^3 + 27B^2 \neq 0$. Its K -rational points consist of the solutions in K^2 together with the point at infinity ∞ .

An isogeny $\varphi : E_1 \rightarrow E_2$ over K is a non-constant rational group homomorphism sending ∞_1 to ∞_2 . Its degree is its degree as a rational map, and any isogeny of degree $n > 1$ factors into prime-degree isogenies. If $\deg(\varphi) = d$, then there is a unique dual isogeny $\hat{\varphi} : E_2 \rightarrow E_1$ such that $\hat{\varphi} \circ \varphi = [d]$. Isomorphisms are precisely the degree-1 isogenies. The j -invariant of E is

$$j(E) = \frac{256 \cdot 27 A^3}{4A^3 + 27B^2}.$$

If $\deg(\varphi)$ is coprime to p , then φ is uniquely determined by its kernel and can be computed efficiently via Velu's formulas [Vél71].

Endomorphism rings and supersingular curves. An endomorphism is an isogeny $E \rightarrow E$, and these form a ring $\text{End}(E)$ along with the zero map. If $\text{End}(E)$ is an order in an imaginary quadratic field, then E is *ordinary*; if it is a maximal order in the quaternion algebra $B_{p,\infty}$, then E is *supersingular*. Every supersingular elliptic curve in characteristic p is isomorphic to one over $\mathbb{F}_{p^2}$, and up to isomorphism there are about $\lfloor p/12 \rfloor$ such curves.

For a prime $\ell \neq p$, the supersingular ℓ -isogeny graph has supersingular curves as vertices and ℓ -isogenies as edges. It is $(\ell + 1)$ -regular and Ramanujan; in particular, random walks mix rapidly and any two vertices are connected by an isogeny of degree ℓ^m with $m = O(\log p)$; see [Koh96].

1.2 Quaternion Algebras and the Deuring Correspondence

For background on quaternion algebras, see [Voi21]. For $a, b \in \mathbb{Q}^\times$, let $B(a, b) = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$ be the quaternion algebra over $\mathbb{Q}$ defined by $i^2 = a$, $j^2 = b$, and $ij = -ji$. It has canonical involution $x_1 + x_2i + x_3j + x_4ij = x_1 - x_2i - x_3j - x_4ij$, reduced trace $\text{Trd}(\alpha) = \alpha + \bar{\alpha} = 2x_1$, and reduced norm $\text{Nrd}(\alpha) = \alpha\bar{\alpha} = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2$.

A lattice $\Lambda \subset B$ is a full-rank $\mathbb{Z}$ -module. Its reduced norm is $\text{Nrd}(\Lambda) = \gcd(\text{Nrd}(\alpha) : \alpha \in \Lambda)$, and the associated normalized quadratic form is

$$q_\Lambda(\alpha) = \text{Nrd}(\alpha) / \text{Nrd}(\Lambda) \in \mathbb{Z}.$$

The reduced norm also defines the bilinear form $\langle x, y \rangle = \frac{1}{2}(\text{Nrd}(x + y) - \text{Nrd}(x) - \text{Nrd}(y))$, with respect to which $\{1, i, j, ij\}$ is an orthogonal basis.

An order $\mathcal{O} \subset B$ is a full-rank lattice that is also a subring; it is maximal if it is not properly contained in another order. For a lattice Λ , define its left and right orders by

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

If $\mathcal{O}$ is maximal and I is a left $\mathcal{O}$ -ideal, then $\mathcal{O}_R(I)$ is also maximal. Conversely, given maximal orders $\mathcal{O}, \mathcal{O}'$, there exists a connecting lattice I such that $\mathcal{O}_L(I) = \mathcal{O}$ and $\mathcal{O}_R(I) = \mathcal{O}'$. Two left $\mathcal{O}$ -ideals I, J are equivalent if $I = \alpha J$ for some $\alpha \in B^\times$; the set of equivalence classes is denoted $\text{Cls}(\mathcal{O})$.

Now let $B_{p,\infty}$ be the quaternion algebra ramified exactly at p and ∞ . For a maximal order $\mathcal{O} \subset B_{p,\infty}$, one has $\text{disc}(\mathcal{O}) = p^2$. Moreover, for any left $\mathcal{O}$ -ideal I , we have $\#(\mathcal{O}/I) = \text{Nrd}(I)^2$, and the normalized quadratic form q_I has determinant p^2 .

The following description of $B_{p,\infty}$ is due to [EHL⁺18].

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

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

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

Remark 1. This is the only point where GRH is used: not for the core problems themselves, but only to obtain an efficient description of the ambient quaternion algebra. Unconditionally, the least quadratic non-residue may be larger, although exceptionally large values are rare by the following Theorem of Linnik [Lin41].

Theorem 1 (Linnik). *For every $\varepsilon > 0$, there exists a constant C_ε such that, for all N , at most C_ε primes $p \leq N$ satisfy $q_p > N^\varepsilon$.*

In the remainder of this paper, we assume that such a q_p has been found and that $B_{p,\infty}$ is represented by the pair $(-q, -p)$ with basis $(1, i, j, ij)$. We will note in our reductions when GRH needs be assumed for $p \equiv 1 \pmod{8}$. We next recall a special maximal order, introduced in [KLPT14], that will play a central role in our applications.

Lemma 2 (Proposition 1 [EHL⁺18]). *For any $p > 2$, the algebra $B_{p,\infty}$ contains the maximal order*

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

where in the last case c satisfies $q \mid c^2p + 1$. Assuming GRH, $\mathcal{O}_0$ contains the suborder $R + Rj$ with index $O((\log p)^2)$, where R is the ring of integers of $\mathbb{Q}(i)$. If ω is a reduced generator of R , then

$$\text{Nrd}(s + tw + xj + y\omega j) = f(s, t) + p f(x, y),$$

where f is a principal, primitive, positive-definite integral binary quadratic form of discriminant $\text{disc}(\mathbb{Q}(i))$.

This norm form will be a key tool in our applications, allowing us to construct elements of prescribed norm in the order.

1.3 Deuring Correspondence.

For background, see [Voi21, Chapter 42]. Deuring's correspondence identifies endomorphism rings of supersingular elliptic curves over $\mathbb{F}_{p^2}$ with maximal orders in $B_{p,\infty}$, up to conjugation, preserving reduced norms and traces.

More precisely, an isogeny $\varphi : E \rightarrow E'$ of degree n determines a left $\text{End}(E)$ -ideal

$$I_\varphi = \text{Hom}(E', E)\varphi$$

of norm n , and Waterhouse showed that every nonzero left ideal arises this way [Wat69, Theorem 3.5]. Conversely, for a nonzero integral left ideal $I \subset \text{End}(E)$, define

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

Then I determines an isogeny $\varphi_I : E \rightarrow E/E[I]$, with $I_{\varphi_I} = I$ and $\varphi_{I_\varphi} = \varphi$. If $\text{Nrd}(I)$ is coprime to p , this isogeny is separable and

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

The ideal–isogeny translations are efficient in $\log p$ and in the largest prime-power factor of the norm or degree; hence powersmooth isogenies are central in isogeny-based cryptography. See [GPS20, Lemma 5] and [Wes22, Lemma 7.1].

Remark. Although ideals of arbitrary norm can be translated to isogenies in rigorous polynomial time via higher-dimensional isogenies [PR23], it is unclear how to use only point-evaluation access in our setting. We therefore restrict to the powersmooth translations of [GPS20].

2 Representation of integers by Quadratic forms

In this section, we study representations of integers by quadratic forms. We consider the number of triples satisfying $az + bg(x, y) = n$, with $z = f(s, t)$ for some $s, t \in \mathbb{Z}$ and f and g are definite binary quadratic forms. We also need estimates for the number of vectors $v \in \mathbb{Z}^4$ such that a quaternary form (a quadratic form with 4 variables) $Q(v)$ is prime. Readers interested mainly in the applications may skip the proofs and focus on the stated bounds. In particular, Theorem 4 and Proposition 4 are the main inputs for the algorithm in Section 4. As our work builds on the framework of Wesolowski [Wes22], we follow the notation and terminology from Section 2.1 therein.

2.1. Number of representations of an integer by a quadratic form. Let Q be a primitive (with coprime coefficients), integral, positive-definite quaternary quadratic form, and set

$$r_Q(n) = \#\{x \in \mathbb{Z}^4 : Q(x) = n\}.$$

We begin with [IK04, Theorem 20.9], which gives an asymptotic formula for $r_Q(n)$. We state only the four-variable case needed here.

Theorem 2. *Let $Q(x)$ be an integral positive definite quadratic form of 4 variables. Then for any integer $n > 0$, the number of integral solutions $x = (x_1, x_2, x_3, x_4)$ to $Q(x) = n$ satisfies*

$$r_Q(n) = \frac{(2\pi)^2 n}{|\det(A)|^{1/2}} \mathfrak{S}(n, Q) + O_{\varepsilon, Q}(n^{\frac{3}{4} + \varepsilon}), \quad (1)$$

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

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

with

$$g_c(n, Q) = \sum_{d \pmod{c}}^* \sum_{h \pmod{c}} \exp\left(\frac{2\pi i d}{c} (Q(h) - n)\right),$$

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

Note that ε with its implied constants cause no harm, but to eliminate the dependence of the implied constants on the quadratic form, we will modify the proof of Theorem 20.9 in [IK04]. The next Theorem extracts the dependency of the implied constants on Q , explicitly. We recall that the level of a quadratic form Q is the smallest positive integer N such that NG^{-1} has integral entries, where G denotes the Gram matrix of Q .

Theorem 3. *Let $Q(x)$ be an integral positive definite quadratic form of 4 variables. Then for any integer $n > 0$, the number of integral solutions $x = (x_1, x_2, x_3, x_4)$ to $Q(x) = n$ satisfies*

$$r_Q(n) = \frac{(2\pi)^2 n}{|\det(A)|^{1/2}} \mathfrak{S}(n, Q) + O_{\varepsilon}(N^2 n^{\frac{3}{4} + \varepsilon}), \quad (2)$$

where A is the Gram matrix of Q , and N is the level of Q , $\mathfrak{S}(n, Q)$ and $g_c(n, Q)$ are as defined in Theorem 2.

Proof. Following the proof of Theorem 20.9 of [IK04], one notices that the only occurrence of the implied constants depending on the Quadratic form Q is coming from [IK04, Lemma 20.1]) which states that

$$G_m \left(\frac{d}{c} \right) = \sum_{h \pmod{c}} \exp\left(\frac{2\pi i d}{c} (Q(h) + h^t m)\right) \ll_Q c^{\frac{r}{2}},$$

where in our case here we set $r = 2$. Working out the details, we obtain

$$\begin{aligned}
\left| G_m \left(\frac{d}{c} \right) \right|^2 &= \sum_{x,y \pmod{c}}^* \exp \left(\frac{2\pi i d}{c} (Q(x) - Q(y) + (x-y)^t m) \right) \\
&= \sum_{y,z \pmod{c}}^* \exp \left(\frac{2\pi i d}{c} (y^t A z - Q(z) + z^t m) \right) \\
&\leq c^r \cdot |\{z \pmod{c} \mid A z \equiv 0 \pmod{c}\}| \\
&\leq c^r \cdot |\{z \pmod{c} \mid N A^{-1} A z \equiv 0 \pmod{c}\}| \\
&= c^r \cdot |\{z \pmod{c} \mid N z \equiv 0 \pmod{c}\}| \\
&= c^r \cdot \gcd(N, c)^r \\
&\leq c^r N^r
\end{aligned}$$

taking square roots of both sides, we get the desired result. Now substituting in (20.112) in the proof of [IK04], we get the statement of the theorem. $\square$

Now in order for the estimate to make sense, we need to ensure $\mathfrak{S}(n, Q) > 0$.

Lemma 3. *Given an integral positive definite quaternary quadratic form $Q(x) = x^T A x$, if*

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

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

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

Proof. Denote by $\chi(q) = \left(\frac{|\det(A)|}{q} \right)$ the legendre symbol. If (3) is solvable, then from ([Iwa97], 11.76) we have

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

i.e there exists an absolute constant c_1 such that

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

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

Remark. In the case that (3) is solvable, ([Iwa97], 11.76) states that $\mathfrak{S}(n)$ actually ranges between $(\log \log 3n)^{-1}$ and $\log \log 3n$.

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

Corollary 1. *For every $\varepsilon > 0$ and $n \gg_\varepsilon N^{8+\varepsilon} |\det(A)|^{2+\varepsilon}$, where N is the level of the form $Q = x^t A x$,*

$$r_Q(n) \gg_\varepsilon \frac{1}{|\det(A)|^{1/2}} \frac{n}{\log \log n}, \quad (5)$$

provided that the congruence in (3) is solvable.

Remark. We note that since $A^{-1} = \text{adj}(A) / \det A$ with $\text{adj}(A) \in M_n(\mathbb{Z})$ we have $N \leq \det A$.

2.2. Number of triplet solutions to $az + bg(x, y) = n$. We study solutions to $az + bg(x, y) = n$ where z is represented by a primitive positive definite binary quadratic

form f . Let f, g be primitive positive definite integral binary quadratic forms with discriminants Δ_f and $\Delta_g = f_0^2 D$, and let $a, b, n > 0$ satisfy $(a, 2nb) = (b, 2n) = 1$ and $a \mid \Delta_g$. We seek a lower bound for

$$S(n) = \{(x, y, z) \in \mathbb{Z}^3 : az + bg(x, y) = n, z = f(s, t) \text{ for some } (s, t) \in \mathbb{Z}^2\}.$$

Without the representability condition on z , the classical lattice-point estimate gives

$$\#\{(z, x, y) \in \mathbb{Z}^3 : az + bg(x, y) = n, z > 0\} \sim \frac{\pi n}{ab |\text{disc}(g)|^{1/2}}.$$

Writing $r_f(k) = \#\{(s, t) \in \mathbb{Z}^2 : f(s, t) = k\}$, and similarly $r_g(k)$, we use the standard bound

$$r_f(k), r_g(k) \ll \tau(k) \ll \exp\left(\frac{C \log k}{\log \log k}\right).$$

If $Q(s, t, x, y) = af(s, t) + bg(x, y)$ has no local obstruction, so $\mathfrak{S}(n) > 0$, then

$$r_Q(n) = \sum_{az+bm=n} r_f(z) r_g(m).$$

Thus the trivial bound above and Corollary 1 imply

$$\#S(n) \gg_\varepsilon \frac{n \exp(-C \log n / \log \log n)}{|\det Q|^{1/2}}$$

for $n \gg_\varepsilon N^{8+\varepsilon} |\det Q|^{2+\varepsilon}$. For our applications we need a logarithmic saving; this follows from the sparsity of integers k for which $r_f(k)$ is large. The main result of this subsection is the following theorem, where $\omega(k)$ denotes the number of distinct prime divisors of k .

Theorem 4. *Let f and g be primitive, integral, positive definite, reduced binary quadratic forms with $\Delta_f \leq -3$ fundamental, and let a, b, n be positive integers such that $(a, 2nb) = (b, 2n) = 1$ and $\omega(a) = 0$ or 1. Assume the congruence (3) is solvable such that $\mathfrak{S}(n) > 0$, and $n \gg_\varepsilon a^{30+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$ for any $\varepsilon > 0$. Then,*

$$\#S(n) \gg_\varepsilon \left(\frac{C_{f,g,a}^{-1/\alpha}}{ab |\Delta_f|^{1+1/\alpha} |\Delta_g|} \right) n (\log n)^{-\gamma},$$

where $\gamma \approx 7.532..$, $\alpha = 1/\ln 2$, and

$$C_{f,g,a} = 4^{\omega(\Delta_g)} \log^2(a \Delta_g).$$

The proof of this theorem is conceptually straightforward. However, it requires an upper bound for the quantity

$$\sum_{\substack{z \leq X \\ z \equiv k \pmod{m}}} r_g^2(z), \quad (k, m) = 1,$$

for which we record the required estimate in the following proposition. By standard heuristics in analytic number theory, the quantity above is expected to be $\ll \frac{X \log X}{a |\Delta_g|}$. Since the proof relies on Heath-Brown's δ -method and is largely independent of the main cryptographic narrative, interested readers can find the proof in the full eprint version [Mam24]. The argument is a refinement of [Lin17], making the implicit constants explicit.

Proposition 1. *Assuming the hypothesis of Theorem 4, then for $X \gg_\varepsilon a^{30+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$ we have*

$$\sum_{\substack{z \leq X \\ z \equiv k \pmod{a}}} r_g^2(n) \ll \frac{4^{\omega(\Delta_g)} \log^2(a \Delta_g)}{a |\Delta_g|} X \log X,$$

The following lemma is the key ingredient in the proof of the main theorem.

Lemma 4. *Let $T > 1$ and $\alpha > 0$. Then*

$$\sum_{\substack{az+bm=n \\ r_f(z)>T}} r_f(z)r_g(m) \ll_{\alpha,\varepsilon} T^{-\alpha/2} \frac{n}{ab} \left(\frac{4^{\omega(\Delta_g)} \log^2(a\Delta_g)}{|\Delta_g|} \right)^{1/2} (\log n)^{2^{1+\alpha}},$$

for $n \gg_{\varepsilon} a^{30+\varepsilon} b |\Delta_g|^{51/4+\varepsilon}$.

Proof. By Rankin's trick and Cauchy-Schwarz we have

$$\begin{aligned} \sum_{\substack{z \leq n/a \\ z \equiv na^{-1} \pmod{b} \\ r_f(z) > T}} r_f(z)r_g\left(\frac{n-az}{b}\right) &\leq \left(\sum_{\substack{z \leq n/a \\ z \equiv na^{-1} \pmod{b} \\ r_f(z) > T}} r_f(z)^2 \right)^{1/2} \left(\sum_{\substack{z \leq n/a \\ z \equiv na^{-1} \pmod{b}}} r_g((n-az)/b)^2 \right)^{1/2} \\ &\leq T^{-\alpha/2} \left(\sum_{\substack{k \leq n/a \\ k \equiv na^{-1} \pmod{b}}} r_f(k)^{2+\alpha} \right)^{1/2} \left(\sum_{\substack{m \leq n/b \\ m \equiv nb^{-1} \pmod{a}}} r_g(m)^2 \right)^{1/2}. \quad (\star) \end{aligned}$$

Using the inequality $r_f(n) \ll \tau(n)$ and proposition 1, we have

$$(\star) \ll T^{-\alpha/2} \left(\sum_{\substack{k \leq n/a \\ k \equiv na^{-1} \pmod{b}}} \tau(k)^{2+\alpha} \right)^{1/2} \left(\frac{4^{\omega(\Delta_g)} \log^2(a\Delta_g)}{ab|\Delta_g|} n(\log n) \right)^{1/2},$$

which, by standard analytic estimates is

$$\ll T^{-\alpha/2} \frac{n}{ab} \left(\frac{4^{\omega(\Delta_g)} \log^2(a\Delta_g)}{|\Delta_g|} \right)^{1/2} (\log n)^{2^{1+\alpha}},$$

as desired. □

Proof of Theorem 4. Notice that we have a natural surjection from the set

$$R_Q(n) = \{(s, t, x, y) \in \mathbb{Z}^4 \mid Q(s, t, x, y) = af(s, t) + bg(x, y) = n\}$$

to

$$S(n) = \{(z, x, y) \in \mathbb{Z}^3 \mid az + bg(x, y) = n, z = f(s, t)\}$$

sending $(s, t, x, y) \mapsto (f(s, t), x, y)$, accordingly

$$\begin{aligned} r_Q(n) &= \sum_{\substack{(z,x,y) \in S(n) \\ r_f(z) \leq T}} r_f(z) + \sum_{\substack{(z,x,y) \in S(n) \\ r_f(z) > T}} r_f(z) \\ &\ll_{\varepsilon,\alpha} T \# S(n) + T^{-\alpha/2} \frac{n}{ab} \left(\frac{4^{\omega(\Delta_g)} \log^2(a\Delta_g)}{|\Delta_g|} \right)^{1/2} (\log n)^{2^{1+\alpha}} \end{aligned}$$

for $n \gg_{\varepsilon} a^{30+\varepsilon} b |\Delta_g|^{51/4+\varepsilon}$. Choosing

$$T = a^{-1/\alpha} |\Delta_f|^{1/\alpha} \left(4^{\omega(\Delta_g)} \log^2(a\Delta_g) \right)^{1/\alpha} (\log n)^{(2^{2+\alpha})/\alpha}.$$

and using corollary 1 with

$$n \gg_{\varepsilon} N^{8+\varepsilon} |\det(A)|^{2+\varepsilon} \gg a^{20+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{10+\varepsilon},$$

we obtain

$$\#S(n) \gg_{\varepsilon, \alpha} T^{-1} \frac{n}{ab(\Delta_f \Delta_g)^{1/2}} \gg_{\varepsilon, \alpha} \left(\frac{C_{f,g,a}^{-1/\alpha}}{ab |\Delta_f|^{1+1/\alpha} |\Delta_g|} \right) n (\log n)^{-(2^{2+\alpha})/\alpha}$$

for $n \gg_{\varepsilon} a^{30+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$ and any fixed $\alpha > 0$ with $C_{f,g,\alpha} = 4^{\omega(\Delta_g)} \log^2(a \Delta_g)$. The choice $\alpha = 1/\ln 2$ is to minimize the power saving logarithm, which justifies $\gamma \approx 7.532$.

2.3 Number of representations of primes by quaternary form. Given a primitive positive definite integral quaternary quadratic form Q of $\det Q = q^2$ where q is prime, in this subsection we seek estimates for the number of representations of primes by this form between two given close bounds. Namely, for x, y with $y < x$, we're interested in obtaining lower bounds for

$$\sum_{\substack{y \leq p \leq x \\ p \text{ prime}}} r_Q(p). \quad (6)$$

The main idea is to utilize corollary 1 since Q is quaternary definite, as we have estimates in this case for $r_Q(n)$ when $n \gg_{\varepsilon} N^{8+\varepsilon} |\det(A)|^{2+\varepsilon}$. However for the estimate to make sense, we need to show that the singular series doesn't vanish, i.e that the congruence in 3 is solvable. It suffices, by the Chinese remainder theorem, to ensure solvability mod p^k for $k \in \mathbb{Z}^+$ for primes $p \nmid 2 \det(A)$. In fact, we shall prove a stronger result, but first we introduce the following definition.

Definition 1. A quadratic form is said to *locally represent an integer n at p* , if $Q(v) \equiv n \pmod{p^k}$ is solvable for all $k > 0$.

Since the following result is standard in quaternion algebras and not central to our applications, we defer the proof to the supplementary material.

Lemma 5. Let $Q = x^T A x$ be a primitive, integral positive-definite quaternary 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.

Now that $\mathfrak{S}(n) > 0$ with respect to the form Q , we turn to the problem of finding lower bounds to (6).

Proposition 2. Let $Q = x^t A x$ be a primitive, positive definite, integral quaternary quadratic form with determinant $\det A = q^2$ for some prime q . Suppose that x and y are sufficiently large, satisfying $x \gg y \gg_{\varepsilon} q^{12+\varepsilon}$ for arbitrary $\varepsilon > 0$. Then, the sum of representation counts over prime numbers in the interval $[y, x]$ satisfies the lower bound

$$P_Q(x, y) := \sum_{\substack{y \leq p \leq x \\ p \text{ prime}}} r_Q(p) \gg_{\varepsilon} \frac{x^2}{q \log x \log \log x}.$$

Proof. The fact that the congruence (3) is solvable by lemma 5 and $y \gg_{\varepsilon} p^{12+\varepsilon}$ corollary 1 implies

$$P_Q(x, y) := \sum_{\substack{y \leq p \leq x \\ p \text{ prime}}} r_Q(p) \gg_{\varepsilon} \sum_{\substack{y \leq p \leq x \\ p \text{ prime}}} \frac{p}{q \log \log p} \gg_{\varepsilon} \frac{1}{q \log \log x} \sum_{\substack{y \leq p \leq x \\ p \text{ prime}}} p.$$

A standard application of Euler's summation and bounds for $\pi(x)$ from [Dus10] gives

$$\sum_{\substack{y \leq p \leq x \\ p \text{ prime}}} p = \int_y^x u \, d\pi(u) = x\pi(x) - y\pi(y) - \int_y^x \pi(u) du \gg \frac{x^2}{\log x};$$

the result follows. $\square$

3 Prime Norms and quadratic Forms 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. Alternatively, this is equivalent to finding vectors $v \in \mathbb{Z}^4$ such that the corresponding quaternary form $q_I(v)$ is prime.

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 $v_1, v_2, \dots, v_i$ with $Q(v_j) \leq \lambda_i$ for all $j = 1, 2, \dots, i$.

Now we develop an algorithm which samples integral vectors within a 4-ellipsoid. For practical reasons, we will specialize our generalization of Lemma 3.3 from [Wes22] using a particular bound so that our ellipsoid contains enough lattice points.

Lemma 6. Let Q be a primitive, positive 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 the length of Q .

Proof. Our approach is analogous to the one presented in [Wes22]. By utilizing the restriction on ρ , the result will naturally follow for the four-variable case.

Let $B_Q(r) = \{v \in \mathbb{R}^4 \mid Q(v) \leq r^2\}$ be the ellipsoid around the origin defined by the quadratic form. Let $r = \rho^{1/2}$, 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 4th successive minimum (in fact $Q(b_4) = \lambda_4$), i.e we have enough lattice points within the ellipsoid. Let $V = \{v \in \mathbb{R}^4 \mid Q(v) = \min_{\lambda \in \mathbb{Z}^4} Q(v + \lambda)\}$ be the Voronoi cell around 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 dimension 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 $r - \mu > 0$, this implies

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

i.e. the process succeeds after a constant number of trials. Finally, our output vector is uniform where the result follows analogously as in [Wes22]. $\square$

Algorithm 1 QUADSAMPLING(Q, ρ)

```

1: Input: Positive definite quaternary quadratic form  $Q$  and a bound  $\rho \geq 4\mu^2(Q)$ 
2: Output: uniform  $x \in \mathbb{Z}^4$  such that  $Q(x) \leq \rho$ 
3: while  $\lambda \notin B_Q(\rho)$  do
4:   Sample a uniform  $v \in B_Q(\rho + \mu)$ ;
5:   Solve the closest vector problem  $\lambda(v)$ ;
6: end while
   return  $\lambda(v)$ .

```

The approach taken in [Wes22] 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 using the well-known result on primes and the effective Chebotarev density's theorem 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 $\pi_f(\rho) = \#\{v \in \mathbb{Z}^2 \mid f(v) \leq \rho \text{ is a prime}\}$, $h(D)$ 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 take a different route through the theory of quaternary forms and use proposition 2.

Proposition 3. *Let $Q = x^T A x$ be a primitive, integral positive-definite quaternary quadratic form, and $\det(A) = q^2$ for some prime q sufficiently large. There is an algorithm that finds an integral vector $x \in \mathbb{Z}^4$ such that $Q(x)$ is a prime number at most $O_\delta(q^{12+\delta})$ for a fixed $\delta \in (0, 1/2)$ and runs in expected polynomial time in $\log q$.*

Proof. From Lemma 6, one can sample a uniformly random integral vector x such that $Q(x) \leq \rho$, where $4\mu^2(Q) \leq \rho$ and $\mu(Q) \ll \text{Vol}(Q) = q$. Let $\varepsilon > 0$ be given small enough, and suppose that $\rho \gg_\delta q^{12+\delta}$, where $0 < \varepsilon < \delta \leq 1/2$ is a constant to be adjusted.

A result of Landau [Lan15] gives,

$$\#\{v \in \mathbb{Z}^4 \mid Q(v) \leq r\} = \frac{(2\pi)^2}{|\det Q|^{1/2} \Gamma(3)} r^2 + O(r^{6/5+\varepsilon}).$$

Applying Lemma 6, the probability that a sampled vector $v \in \mathbb{Z}^4$ satisfies $Q(v) \ll_\varepsilon q^{12+\varepsilon}$ is very small, provided that δ is suitably chosen (q is sufficiently large). More precisely,

$$\Pr[Q(x) \ll_\varepsilon q^{12+\varepsilon}] = \frac{\#\{v \in \mathbb{Z}^4 \mid Q(v) \leq q^{12+\varepsilon}\}}{\#\{v \in \mathbb{Z}^4 \mid Q(v) \leq \rho\}} \ll \frac{q^{23+\varepsilon}}{\rho^2} \ll \frac{1}{q^{2\delta-\varepsilon}}.$$

Since the sampled vectors will, with overwhelming probability, satisfy

$$q^{12+\varepsilon} \ll_\varepsilon Q(v) \ll_\delta q^{12+\delta},$$

using Proposition 2, we obtain

$$\Pr[Q(v) \text{ is prime}] \gg_\delta \frac{1}{\log q \log \log q}.$$

This completes the proof. □

3.2 Sampling Equivalent ideals of prime norm We now return to the problem of sampling a left $\mathcal{O}$ -ideal J in the same class of a given left ideal I .

Algorithm 2 EQUIVALENTPRIMEIDEAL $_{\delta}(I)$

- 1: **Input:** A left ideal I in a maximal order $\mathcal{O}$.
 - 2: **Output:** An ideal J of prime norm, and an element $\alpha \in I$ such that $J = I\bar{\alpha}/\text{Nrd}(I)$.
 - 3: Find an element $\alpha \in I$ such that $q_I(\alpha)$ is a prime; {Proposition 3}.
 - 4: **return** $J = I\bar{\alpha}/\text{Nrd}(I)$, and α .
-

Theorem 5. For a fixed $\delta \in (0, 1/2)$, Algorithm 2 is correct and runs in expected polynomial time in $\log p$, and the output J has reduced norm $\text{Nrd}(J) = O_{\delta}(p^{12+\delta})$.

Proof. It follows straightforwardly from Proposition 3, where $Q = q_I$ is a primitive integral positive definite quaternary quadratic form of determinant p^2 . $\square$

Remark . In [KLPT14] the heuristic algorithm is expected to return an equivalent ideal of norm $\text{Nrd}(J) = O(p^{1/2})$ most of the time, and $\text{Nrd}(J) = O(p)$ in the worst case. In [Wes22] the output ideal J is expected to have $\text{Nrd}(J) = O_{\varepsilon}(p^{2+\varepsilon})$ assuming the generalized Riemann hypothesis. Even though our result is certainly not as tight as the previous ones, nevertheless the size of the norm is still polynomial in the input size and will be sufficient for our purposes. We conclude this section with a proposition that modifies the last algorithm to output an ideal with certain properties.

Proposition 4. Given a left ideal I , a bound $\rho \asymp_{\delta} p^{12+\delta}$ for $\delta > 0$, and a prime $l \neq p$, there is an algorithm which returns an ideal J equivalent to I such that $\text{Nrd}(J)$ is a prime between ρ and $\rho^{1+\theta}$ for any $0 < \theta \leq 1/2$, and l is a non-quadratic residue modulo $\text{Nrd}(J)$. The algorithm runs in expected polynomial time in $\log p$.

Proof. The proof of this proposition follows from Theorem 5 together with [Wes22, Proposition 3.8], and proceeds along analogous lines. The condition on θ ensures that the norm of the sampled ideal J is sufficiently large. Finally, the number of primes $z = \text{Nrd}(J)$ in an interval $[X, Y]$ for which l is a quadratic residue modulo z is approximately $\frac{1}{2}(\pi(Y) - \pi(X))$, since such primes occur with density $1/2$ by the Chebotarev Density Theorem. Consequently, this restriction increases the running time by at most a factor of 2. $\square$

4 Solving Diophantine Equations

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

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

where f and g are positive definite binary quadratic forms, and $a, b, n \in \mathbb{Z}$. In our applications Δ_f is polynomial in the input size, nevertheless for the sake of completeness we state our next theorem in full generality.

Theorem 6. For every $\varepsilon > 0$, there exist a constant $c_{\varepsilon} > 0$ and an algorithm $\mathcal{A}$ such that the following holds. Let f and g be reduced, primitive, positive definite, integral binary quadratic forms where $\text{disc}(f) = \Delta_f$ is fundamental. Let a, b, n be positive integers satisfying $(a, 2bn) = (b, 2n) = 1$ and assume a divides Δ_g with $a = 1$ or a prime power. Then $\mathcal{A}(f, g, b, n)$ returns an integral solution (s, t, x, y) to the equation

$$Q(s, t, x, y) = af(s, t) + bg(x, y) = n \tag{8}$$

provided that $n \gg_{\varepsilon} a^{30+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$ and $Q(s, t, x, y) \equiv n$ is solvable modulo $2^7 \det^3(Q)$. Assuming access to a factoring oracle $\mathcal{O}$, the algorithm runs in expected polynomial time in Δ_f , $2^{\omega(\Delta_g)}$, $\log(ab)$, and $\log(n)$, where $\omega(\cdot)$ denotes the number of distinct prime factors. The output is random with min-entropy $\Omega(\log n)$.

In [Wes22], Wesolowski employs genus theory of quadratic forms and prime ideals in a quadratic extension to solve a more specific Diophantine equation, where $a = \det(\gamma)^2$ and $g = f^\gamma = f(\gamma(\cdot))$. His approach is motivated by the need to find primes ℓ represented by f that also satisfy the generalized Hardy-Littlewood equation

$$a\ell + bf(x, y) = n.$$

It is well known that Cornacchia's algorithm finds a solution to the Diophantine equation $f(s, t) = z$ in polynomial time in $\log z$ and $\log \Delta_f$, provided that the factorization of z is known and m doesn't have too many prime factors. Since primality testing can be performed efficiently, Wesolowski requires z to be prime.

A mere access to a factoring oracle is not sufficient to solve $f(s, t) = z$ especially when z is highly composite. However, some recently developed algorithms in [Mam25] find solutions to $f(s, t) = z$ where there is a tradeoff between the size of Δ_f and $2^{\omega(z)}$. Precisely put, if Δ_f is small, i.e. polynomial in $\log n$, then algorithm 1 of [Mam25], which is a classical subset-sum algorithm, finds a solution efficiently.

By leveraging our factoring oracle $\mathcal{O}$ and the fact that $\Delta_f = \text{polylog}(n)$, we circumvent these obstacles, allowing us to solve the problem using the theory of quaternary quadratic forms without relying on the Generalized Riemann Hypothesis (GRH).

Proof of theorem 6. Most of our work has been done in section 2, we just have to gather our tools. Assume we have access to a factoring oracle $\mathcal{O}$, $n \gg_\varepsilon a^{30+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$, and $Q(s, t, x, y) \equiv n \pmod{2^7 \det^3 Q}$ is solvable. Using ([Wes22], proposition 5.2) we can sample almost uniform (up to small error $O(n^{-1/2})$) integral solutions (z, x, y) to $az + bg(x, y) = n$ with $z > 0$ in polynomial time, and the sample space X has cardinality

$$\#X = \frac{2^{\omega(a)} \pi n}{ab \text{Vol}(g)} + O\left(2^{\omega(a)} \left(\frac{n}{b}\right)^{1/2} + a2^{\omega(a)} \text{Vol}(g)\right) \ll \frac{2^{\omega(a)} \pi n}{ab \text{Vol}(g)}. \quad (9)$$

Each time we sample a solution (z, x, y) we factor z using $\mathcal{O}$; we use [Mam25, algorithm 1] to efficiently find a solution or decide that $z = f(s, t)$ is not solvable. In the latter case, we sample another triplet solution. We would be done if we can show that a large proportion of the sampled solutions (z, x, y) satisfy $z = f(s, t)$. Thanks to Theorem 4, we have

$$\#\{(z, x, y) \in \mathbb{Z}^3 \mid az + bg(x, y) = n, z = f(s, t)\} \gg_\varepsilon \left(\frac{C_{f,g,a}^{-1/\alpha}}{ab |\Delta_f|^{1+1/\alpha} |\Delta_g|} \right) n (\log n)^{-\gamma},$$

and $C_{f,g,a} = 4^{\omega(\Delta_g)} \log^2(a\Delta_g)$. Combining this with (9), we obtain

$$\Pr[(z, x, y) \in X, z = f(s, t)] \geq c_\varepsilon \frac{C_{f,g,a}^{-1}}{2^{\omega(a)} |\Delta_f|^{1+1/\alpha} \log^\gamma n},$$

for a constant c_ε . Hence, we expect the sampling process to succeed after

$$O\left(2^{\omega(a)} C_{f,g,a} |\Delta_f|^{1.7} (\log n)^{7.54}\right)$$

many trials. 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. $\square$

Remark. The algorithm's total running time is polynomial provided that $\omega(m) \ll \log \log n$ where $m = \Delta_f, \Delta_g$, i.e. those integers should not be highly composite. This is satisfied readily in the next corollary.

5.2. Finding elements in a special maximal order The following immediate corollary allows us to sample elements from the special maximal order $\mathcal{O}_0$ in $B_{p,\infty}$ as defined in the lemma 2.

Corollary 2. *There exists an algorithm $\mathcal{A}$ such that the following holds. For any integer n and prime p with $(n, p) = 1$ and $n \gg_{\varepsilon} p^{20+\varepsilon}$ for every $\varepsilon > 0$, $\mathcal{A}$ finds an element $\alpha \in \mathcal{O}_0$ with $\text{Nrd}(\alpha) = n$. Using the oracle $\mathcal{O}$, the algorithm runs in expected polynomial time in terms of $\log(p)$ and $\log(n)$.*

Proof. From lemma 2 we know that elements $\alpha = s + tw + xj + y\omega j \in R + Rj \subset \mathcal{O}_0$ satisfy

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

where $\text{disc}(f) = O(\log^2 p)$ (we assume the least quadratic non-residue has been found and has size polynomial in $\log p$). Notice that $\omega(\Delta_f) = 1$ for all cases in 1, hence the algorithm is efficient. However, in order to apply Theorem 6 we need $f(x, y) + pf(s, t) \equiv n \pmod{2^7 \det^3(A)}$ to be solvable. It is enough to show the solvability modulo 2^3 , p and $\text{disc}(f)$, then use Hensel's lemma and Chinese remainder theorem, which are both straightforward but require some computations in the case mod 2^3 . The condition on ε comes from the fact that we need $n \gg_{\varepsilon} a^{30+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$. $\square$

5 Solving the QUATERNIONPATH Problem

For the remaining sections we consider our special maximal order $\mathcal{O}_0$ from lemma 2 in the quaternion algebra $B_{p,\infty}$. The main result here is Theorem 7 that solves the QUATERNIONPATH. 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], it's been argued that the general case reduces to the special maximal order $\mathcal{O}_0$ and hence we focus on this one. We note that for $p \equiv 1 \pmod{8}$ we assume GRH to obtain an efficient representation of the Quaternion algebra $B_{p,\infty} = (-q, -p | \mathbb{Q})$ with $q = O(\log^2 p)$.

6.2. Solving the quaternion path problem.

Theorem 7. *For every $\varepsilon > 0$ there exists a constant c_{ε} such that for integers $n_1, n_2 \geq c_{\varepsilon} p^{1089+\varepsilon}$ and a prime ℓ with $n_2 \ell^e \not\equiv 2, 4 \pmod{8}$ for $e \in \{0, 1\}$, Algorithm 3 is correct and runs in expected polynomial time in ℓ , $\log p$, $\log n_i$, and $\log \text{Nrd}(I)$, assuming access to a factoring oracle $\mathcal{O}$. If $p \equiv 1 \pmod{8}$ we assume the generalized Riemann hypothesis.*

Proof. The algorithm has the same approach as in ([Wes22], Theorem 6.3), we will just comment on the steps where our variants are implemented.

Step 3. The Brandt graph is the quaternionic analogue of the isogeny graph. Fixing a maximal order $\mathcal{O}_0$, its vertices are the left ideal classes $[I]$ of $\mathcal{O}_0$ -ideals, equivalently the maximal orders $\mathcal{O}_R(I)$ arising as their right orders. For $\log n_1 \geq \log(c_{\varepsilon} p^{1089+\varepsilon})$, the output ideal will lie in any class with probability between $1/2N_p$ and $3/2N_p$, i.e. its almost uniform (In fact, from lemma 1 of [GPS20], $\log n_1 \geq (1 + \varepsilon) \log p$ suffices).

Step 4, 5 To utilize proposition 4, the norm of the desired ideal should be at least $\rho = c_{\varepsilon} p^{12+\varepsilon}$, but to have a concrete bounds on $\text{Nrd}(I')$ we take $\theta = 1/2$. Given $N \geq c_{\varepsilon} p^{12+\varepsilon}$, we can sample an equivalent ideal with the required properties using corollary 4.

Step 6 As dealt with in ([KLPT14], section 4.3), this step can be solved using linear algebra over $\mathbb{Z}/N\mathbb{Z}$. Additionally, it's been proven by [Wes22], that the randomization of the ideal in step 3 and the large entropy of γ in step 5, ensure that this step succeeds since I''/NO_0 and $O_0\gamma/NO_0$ are expected to differ from the, at most, two fixed points under the action of $(R/NR)^{\times}$.

Steps 8,9 Given β , we find the matrix $\Gamma \in M_{2 \times 2}(\mathbb{Z})$ with $\det \Gamma = N$ which can be done by computing square roots modulo N , as outlined in ([KLPT14], section 4.4). Theorem 6 works efficiently in Step 9 since $n \gg_\varepsilon p^{1089+\varepsilon} \gg_\varepsilon a^{30+\varepsilon} b^{20+\varepsilon} |\Delta_f|^{10+\varepsilon} |\Delta_g|^{51/4+\varepsilon}$ and $\omega(\Delta_f), \omega(\Delta_g) \ll 1$.

What remains is to show that

$$N^2 f(s, t) + p f^\Gamma(x, y) = n_2 \ell^e$$

is solvable modulo $2^7 \det(A)^3$, where A is the Gram matrix of the quaternary form $N^2 f(s, t) + p f^\Gamma(x, y)$. Since Q is quaternary, it suffices to prove solvability modulo 2^3 , N , p , and Δ_f , and then combine the resulting congruences using Hensel's lemma and the Chinese remainder theorem.

For the modulus 2^3 , this can be verified by a direct (albeit tedious) computation, using that f is a principal form; the problem reduces to representing 3 and 5 modulo 8. Finally, since ℓ is a quadratic nonresidue modulo N , we choose the parity of the exponent e according to whether $p f^\Gamma(x, y)$ is a quadratic residue modulo N .

Reducing the equation modulo p and using the fact that N is invertible mod p , gives $f(s, t) \equiv N^{-2} n_2 \ell^e$, where $f(s, t)$ is a principal form of $\Delta_f = -4, -8$, or $-q_p$ depending whether $p \equiv 3 \pmod{4}$, $p \equiv 5 \pmod{8}$, or $p \equiv 1 \pmod{8}$ according to lemma 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 .

The existence of a solution modulo Δ_f has been established in detail in the analogous result of [Wes22], and we therefore do not repeat the argument here. $\square$

Remark 2. We note that even though the resulting ideal has norm $N \approx p^{1089+\varepsilon}$, its bit-size is roughly $1089 \log p$, making it significantly smaller than the size required in the analogous result of [Wes22], where $N \gg p^{\log^c(p)}$.

Remark 3. The dominant cost of Algorithm 2 is solving the norm-form equation in Step 9. By the proof of Theorem 6, this is roughly $O(F \cdot 2^{\omega(a)} C_{f,g,a} |\Delta_f|^{1.7} (\log n)^{7.54})$, where F is the cost of factoring and $\Delta_f = O(\log^2 p)$ in the worst case. Using Shor's algorithm, $F = O(\log^3 p)$, our algorithm is projected to have quantum complexity $O(\log^{15.24}(p))$, compared to the implicit $O((\log p)^c)$ in [Wes22].

On the polynomial overhead in Wesolowski's reduction. Since this material is necessarily notation-heavy and involves chasing constants through multiple intermediate results, we separate it from the main narrative: readers only interested in the high-level statement may skip the bookkeeping entirely, while readers wishing to verify the claimed overhead can check this remark. Throughout this discussion we assume familiarity with the setup and notation of [Wes22]. The purpose of this remark is purely quantitative: we explain why the polylogarithmic exponent appearing in the running time of Wesolowski's reduction [Wes22] is forced to be very large.

More precisely, the exponent c in the $\Omega(\log^c p)$ running time in [Wes22, Theorem 6.3] ultimately depends on the small exponent implicit in the analytic input used in the reduction. Concretely, Theorem 5.1 of [Wes22] (which is invoked via Theorem 6.3 to solve QUATERNIONPATH) inherits its exponent from the distribution results in Corollary 4.2 / Theorem 4.3 of [Wes22]. These in turn rely on [ABL21, Theorem 2.1] (with minor modifications in [Wes22]).

Let $\delta' > 0$ be the constant coming from Theorem 2.1 of [ABL21] upon assuming GRH and suppose we wish to work uniformly in the range

$$c, d \leq x^{\delta'},$$

with a power-saving error of size $\ll x^{1-\delta'}$. In the proof of [ABL21, Thm. 2.1] an auxiliary parameter R is introduced and the main quantity is decomposed as $S_1 + S_2$. The tail term

Algorithm 3 QUATERNIONPATH $_{\varepsilon}(I, n_1, n_2, \ell)$

-
- 1: **Input:** A left ideal I in a special maximal order $\mathcal{O}_0$, positive integers n_1, n_2 and a prime ℓ .
 - 2: **Output:** An equivalent ideal J of norm $n_1 n_2$ or $n_1 n_2 \ell$.
 - 3: Define R, ω , and f as in lemma 2;
 - 4: **while** β has not been found **do**
 - 5: Random walk in the Brandt graph to obtain $I' \subset I$ of norm n_1 ; {[GPS20], Lemma 1 }
 - 6: Find an element $\rho \in I'$ such that $I'' = I'\rho/\text{Nrd}(I)$ equivalent to I' of prime norm $N \in$
 - 7: $[c_{\varepsilon} p^{12+\varepsilon}, c_{\varepsilon} p^{12.5+\varepsilon}]$ and ℓ is a quadratic non residue modulo N ; {Proposition 4, with $\theta = \frac{1}{2}$ }.
 - 8: Find an element $\gamma \in \mathcal{O}_0$ such that $\text{Nrd}(\gamma) = N$; {Corollary 2}
 - 9: Find an element $\beta \in R$ such that $I'' = \mathcal{O}_0 N + \mathcal{O}_0 \beta j$ if it exists;
 - 10: **end while**
 - 11: Find a matrix $\Gamma \in M_{2 \times 2}(\mathbb{Z})$ such that $\mathbb{Z}\beta + RN = \{x + y\omega \mid (x, y) \in \Gamma\mathbb{Z}^2\}$;
 - 12: Find an integral solution (s, t, x, y) of $N^2 f(s, t) + pf^{\Gamma}(x, y) = n_2 \ell^e$ for $e \in \{0, 1\}$; {Theorem 6}
 - 13: Set $(x', y') = \Gamma(x, y)$, and $\alpha = (s + t\omega)N + (x' + y'\omega)j$;
 - 14: Set $\delta = \rho\gamma\alpha/N \in I' \subset I$;
 - 15: **return** $J = I\bar{\delta}/\text{Nrd}(I)$
-

satisfies [ABL21, (4.2)]

$$S_2 \ll c x (\log x)^{O(1)} R^{-1/11}.$$

Writing $R = x^{\delta}$ and using $c \leq x^{\delta'}$ gives

$$S_2 \ll x^{1+\delta'-\delta/11+o(1)}.$$

Hence $S_2 \ll x^{1-\delta'}$ is ensured as soon as $\delta \geq 22\delta'$; in particular we may choose $R := x^{22\delta'}$.

In addition, the proof explicitly reduces the problem to proving the key estimate in the enlarged modulus range

$$Q \leq x^{1/2+4\delta} \quad ([\text{ABL21, p. 17}]).$$

At this point a dispersion-type input is invoked (their citation of [BF186, Lemma 2]), which is available for Q up to the classical level $Q \leq x^{4/7-\varepsilon}$. Equating $x^{1/2+4\delta} \leq x^{4/7-\varepsilon}$ shows that it suffices to require

$$4\delta < \frac{1}{14}, \quad \text{hence we may take any fixed } \delta < \frac{1}{56}.$$

Combining this with the constraint $\delta \geq 22\delta'$ coming from S_2 , we obtain the explicit admissible choice

$$\delta' < \frac{1}{56 \cdot 22} = \frac{1}{1232}.$$

Therefore, under GRH one may take the exponent in the range $c, d \leq x^{\delta'}$ (and the corresponding power saving $\ll x^{1-\delta'}$) to be any fixed constant $\delta' < 1/1232$.

Finally, in the proof of [Wes22, Theorem 4.1], Wesolowski invokes [ABL21, Theorem 2.1] and subsequently reduces the resulting exponent further (by additional factors of 5 and 2; see [Wes22, p. 12]). With our explicit choice this yields

$$\delta' < \frac{1}{12320}.$$

Recalling that the exponent c discussed above (in Wesolowski's framework) is at least the reciprocal of this parameter, we obtain

$$c > \frac{1}{\delta'} > 12320,$$

which explains the claimed degree-12320 polynomial overhead.

We stress that this lower bound is very conservative. In practice, the exponent δ' implicit in [ABL21, Theorem 2.1] is expected to be significantly smaller, which further increase the resulting degree c . $\square$

The following corollaries give solutions to the two important variants of the QUATERNIONPATH problems, namely ℓ -QUATERNIONPATH and B -PSQUATERNIONPATH.

Corollary 3. *For every $\varepsilon > 0$ there exists a constant $C_\varepsilon > 0$ and algorithms $\mathcal{A}$ and $\mathcal{B}$ which on input a maximal order $\mathcal{O} \subset B_{p,\infty}$ and left $\mathcal{O}$ -ideal I , $\mathcal{A}$ returns an equivalent ideal J whose norm is a prime power ℓ^e or and $\mathcal{B}$ returns an equivalent $(C_\varepsilon \log p)$ -powersmooth ideal. Given a factoring oracle $\mathcal{O}$, the algorithm runs in expected polynomial time in $\log p$ and $\log \text{Nrd}(I)$ (with GRH if $p \equiv 1 \pmod{8}$)*

Proof. Notice first that the maximal order is not necessarily the special extremal order in Lemma 1, but as stated at the beginning of the section, Theorem 9 of [KLPT14] generalizes the special case $\mathcal{O}_0$ to arbitrary maximal orders in $B_{p,\infty}$. For the ℓ -QUATERNIONPATH, we can take n_1, n_2 large enough powers of ℓ and apply algorithm 3 to obtain $\mathcal{A}$.

For BS-QUATERNIONPATH, as outlined in [Wes22], it's enough to find two powersmooth integers n_1 and n_2 to apply Theorem 7. Let C_ε be a constant to be adjusted, and let

$$n_1 = n_2 = \prod_{\substack{\ell \text{ prime} \\ \log p < \ell < C_\varepsilon \log p}} \ell$$

Using Theorem 6.9 from [Dus10], which states that

$$\pi(x) \geq \frac{x}{\ln x} \left(1 + \frac{1}{\ln x}\right) \quad \forall x > 599, \quad (10)$$

we obtain that

$$\log(n_i) = \sum_{\substack{\ell \text{ prime} \\ \log p < \ell < C_\varepsilon \log p}} \log(\ell) \geq (\log \log p) \log p \left(\frac{C_\varepsilon}{\log(C_\varepsilon \log p)} - \frac{1}{\log \log p} \right) \geq (C_\varepsilon/2 - 1) \log p,$$

by adjusting C_ε so that $C_\varepsilon/2 - 1 > \max(599, 1089 + \log c_\varepsilon)$ ensures that $n_i > c_\varepsilon p^{350+\varepsilon}$ where c_ε is the constant from Theorem 7; this finishes the proof. $\square$

We finish with the ideal-to-isogeny conversion needed below.

Lemma 7. *Given a left $\mathcal{O}_0$ -ideal I of norm ℓ^e , with $\ell \neq p$, the corresponding degree- ℓ^e isogeny φ_I can be computed unconditionally in expected polynomial time in $\log p$, ℓ , and e , assuming a factoring oracle $\mathcal{O}$ (with GRH if $p \equiv 1 \pmod{8}$).*

Proof. Let C_ε be as in Corollary 3. For $i = 1, \dots, e$, set

$$I_i = I + \mathcal{O}_0 \ell^i.$$

Replace I_i by an equivalent ideal J_i of $(C_\varepsilon \log p)$ -powersmooth norm using Corollary 3, translate J_i into an isogeny ψ_i using [GPS20, Lemma 5], and let E_i be its codomain. The

successive curves E_{i-1} and E_i are connected by an ℓ -isogeny φ_i , computable by Vélú's formulae [Vél71]. Therefore

$$\varphi_I = \varphi_e \circ \cdots \circ \varphi_1.$$

Correctness follows from the ideal–isogeny correspondence. This is [Wes22, Algorithm 4], with Corollary 3 replacing the heuristic step, giving the claimed expected polynomial runtime. $\square$

6 Equivalence of MaxOrder and ℓ -IsogenyPath

In a recent paper by Le Merdy and Wesolowski [LMW25], they demonstrate the unconditional equivalence of ISOGENYPATH, MAXORDER, and ENDRING without explicitly relying on the ℓ -ISOGENYPATH. It is immediate that ℓ -ISOGENYPATH implies ISOGENYPATH, which, according to their paper, further implies MAXORDER. However, the reverse direction leading to ℓ -ISOGENYPATH remains conditional on the Generalized Riemann Hypothesis (GRH). We now begin by proving this equivalence.

7.1. Reducing ℓ -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 $\text{End}(E_1) \cong \mathcal{O}_1$ and $\text{End}(E_2) \cong \mathcal{O}_2$ then we can find an isogeny path from E_1 to E_2 in the ℓ -isogeny graph.

Theorem 8. *Let $\ell \neq p$ be a prime. Given a factoring oracle $\mathcal{O}$ and oracle access to an algorithm $\mathcal{A}_{\text{MaxOrder}}$ solving the MAXORDER problem, one can solve the ℓ -ISOGENYPATH problem in expected polynomial time in $\log p$, ℓ , and the output size of $\mathcal{A}_{\text{MaxOrder}}$ (with GRH if $p \equiv 1 \pmod{8}$).*

Proof. Given $E_1, E_2/\mathbb{F}_{p^2}$, use $\mathcal{A}_{\text{MaxOrder}}$ to compute $\mathcal{O}_i \cong \text{End}(E_i) \subset B_{p,\infty}$ for $i = 1, 2$. Let $(\mathcal{O}_0, E_0)$ be the special order and curve from Lemma 2 and [EHL⁺18, Proposition 3]. For C_ε as in Corollary 3, set

$$e = \left\lceil \frac{1089 \log p + \log C_\varepsilon}{\log \ell} \right\rceil.$$

For each $i = 1, 2$, compute a connecting ideal $I_i = I(\mathcal{O}_0, \mathcal{O}_i)$ using [KV10], apply $\text{QUATERNIONPATH}_\varepsilon(I_i, \ell^e, \ell^e, \ell)$ to obtain an equivalent ideal J_i of ℓ -power norm, and translate J_i via lemma 7 into an isogeny $\varphi_i : E_0 \rightarrow E_i$. Then

$$\varphi = \varphi_2 \circ \widehat{\varphi}_1 : E_1 \rightarrow E_2$$

is an ℓ -power degree isogeny, hence an ℓ -isogeny path. Correctness and the claimed running time follow from the invoked subroutines and Corollary 3. $\square$

7.2. Reducing MAXORDER to ISOGENYPATH. These reductions seem to be folklore, however for the sake of completeness, we will give the full algorithm. Given a supersingular elliptic curve E , we prove that an isogeny from E_0 (with known endomorphism ring) to E allows one to retrieve the endomorphism ring of E .

Theorem 9. *Given a factoring oracle $\mathcal{O}$ and oracle access to $\mathcal{A}_{\ell\text{-IsogenyPath}}$, the MAXORDER problem over $\mathbb{F}_{p^2}$ can be solved in expected polynomial time in $\log p$, the output size of $\mathcal{A}_{\ell\text{-IsogenyPath}}$ (with GRH if $p \equiv 1 \pmod{8}$).*

Proof. Given $E/\mathbb{F}_{p^2}$, compute the special pair $(\mathcal{O}_0, E_0)$ from Lemma 2 and [EHL⁺18, Proposition 3]. Use $\mathcal{A}_{\ell\text{-IsogenyPath}}(E_0, E)$ to obtain

$$\varphi = \varphi_e \circ \cdots \circ \varphi_1 : E_0 \rightarrow E, \quad \deg(\varphi_i) = \ell.$$

Set $\psi_0 = \text{id}_{E_0}$. For $i = 1, \dots, e$, compute the ideal I_i corresponding to $\varphi_i \circ \psi_{i-1}$ using [GPS20, Lemma 5]; replace it, via Corollary 3, by an equivalent ideal J_i of $(C_\varepsilon \log p)$ -powersmooth norm; and translate J_i back to an isogeny ψ_i as in [Wes22, Lemma 7.1]. Inductively, J_i represents the ideal induced by $\varphi_i \circ \dots \circ \varphi_1$.

Thus J_e corresponds to an isogeny from E_0 to E , so

$$\mathcal{O} := \mathcal{O}_R(J_e) \cong \text{End}(E).$$

A basis for $\mathcal{O}$ is computed using [Rón92, Theorem 3.2]. Correctness follows from the ideal–isogeny correspondence, and the running time follows from the cited subroutines and the assumed cost of $\mathcal{A}_{\ell\text{-IsogenyPath}}$. $\square$

7 Equivalence of MaxOrder and EndRing

Here we prove that MAXORDER and ENDRING are polynomial-time equivalent.

Reducing EndRing to MaxOrder

Theorem 10. *Given a factoring oracle $\mathcal{O}$ and oracle access to $\mathcal{A}_{\text{MaxOrder}}$, ENDRING over $\mathbb{F}_{p^2}$ can be solved in expected polynomial time in $\log p$ and the output size of $\mathcal{A}_{\text{MaxOrder}}$ (with GRH if $p \equiv 1 \pmod{8}$).*

Proof. Given $E/\mathbb{F}_{p^2}$, compute $\mathcal{O} \cong \text{End}(E)$ using $\mathcal{A}_{\text{MaxOrder}}$. Let $(\mathcal{O}_0, E_0)$ be the special pair from Lemma 2 and [EHL⁺18]. Compute a connecting ideal $I : \mathcal{O}_0 \rightarrow \mathcal{O}$ using [KV10], replace it by an equivalent ideal J of $(C_\varepsilon \log p)$ -powersmooth norm N via Corollary 3, and translate J into an isogeny $\varphi : E_0 \rightarrow E$. If $N\omega_i = \sum_j c_{ij}\alpha_j$ in bases of $\mathcal{O}$ and $\mathcal{O}_0$, then

$$\frac{1}{N} \sum_j c_{ij} \varphi \phi_j \hat{\varphi}$$

generate $\text{End}(E)$. Correctness follows from the ideal–isogeny correspondence, and the running time from the cited subroutines. $\square$

Reducing MaxOrder to EndRing

We follow the approach outlined in [EHL⁺18] with some modifications to drop the factoring oracle.

Theorem 11. *Given an oracle access to $\mathcal{A}_{\text{EndRing}}$, MAXORDER over $\mathbb{F}_{p^2}$ can be solved in expected polynomial time in $\log p$ and the output size of $\mathcal{A}_{\text{EndRing}}$.*

Proof. Given $E/\mathbb{F}_{p^2}$, use $\mathcal{A}_{\text{EndRing}}$ to compute generators $1, \alpha_2, \alpha_3, \alpha_4$ of $\text{End}(E)$. By [EHL⁺18, Lemmas 4 and 5], one can compute in polynomial time a rational invertible map ι sending these generators to an orthogonal basis $1, \gamma, \beta, \gamma\beta$ of $\text{End}(E) \otimes \mathbb{Q}$. Since E is supersingular, $\text{End}(E) \otimes \mathbb{Q}$ is the quaternion algebra ramified exactly at p and ∞ ; in particular $\gamma^2, \beta^2 < 0$, and $\text{End}(E) \otimes \mathbb{Q}$ is explicitly identified, via ε , with $(\gamma^2, \beta^2 \mid \mathbb{Q})$. Using [EHL⁺18, Lemmas 4 and 5] again, together with the known ramification places, we compute in polynomial time an explicit isomorphism $j : (\gamma^2, \beta^2 \mid \mathbb{Q}) \rightarrow B_{p,\infty}$, without an need for a factoring oracle. Therefore $(j \circ \varepsilon \circ \iota)(\text{End}(E))$ is a maximal order in $B_{p,\infty}$, giving the desired solution to MAXORDER. $\square$

We prove that ISOGENYPATH and ℓ -ISOGENYPATH are polynomial-time equivalent. Clearly, one direction is immediate.

Theorem 12. *Given a factoring oracle $\mathcal{O}$ and oracle access to $\mathcal{A}_{\text{ISOGENYPATH}}$, the ℓ -ISOGENYPATH problem can be solved in polynomial time (with GRH if $p \equiv 1 \pmod{8}$).*

Proof. By Theorem 8, ℓ -ISOGENYPATH reduces to MAXORDER; by Theorem 11, MAXORDER reduces to ENDRING; and by [PW24], ENDRING reduces unconditionally in polynomial time to ISOGENYPATH. Therefore an ISOGENYPATH oracle, together with $\mathcal{O}$, solves ℓ -ISOGENYPATH in polynomial time. $\square$

References

- [AAA⁺25] Marius A. Aardal, Gora Adj, Diego F. Aranha, Andrea Basso, Isaac Andrés Canales Martínez, Jorge Chávez-Saab, Maria Corte-Real Santos, Pierrick Dartois, Luca De Feo, Max Duparc, Jonathan Komada Eriksen, Tako Boris Fouotsa, Décio Luiz Gazzoni Filho, Basil Hess, David Kohel, Antonin Leroux, Patrick Longa, Luciano Maino, Michael Meyer, Kohei Nakagawa, Hiroshi Onuki, Lorenz Panny, Sikhar Patranabis, Christophe Petit, Giacomo Pope, Krijn Reijnders, Damien Robert, Francisco Rodríguez-Henríquez, Sina Schaeffler, and Benjamin Wesolowski. SQuSign. Technical report, National Institute of Standards and Technology, 2025. URL: <https://sqisign.org>.
- [ABDF⁺25] M. A. Aardal, A. Basso, L. De Feo, S. Patranabis, and B. Wesolowski. A complete security proof of sqisign. In *Advances in Cryptology – CRYPTO 2025*, volume 16005 of *Lecture Notes in Computer Science*, pages 190–222. Springer, 2025. doi:10.1007/978-3-032-01887-8_7.
- [ABL21] Edgar Assing, Valentin Blomer, and Junxian Li. Uniform Titchmarsh divisor problems. *Advances in Mathematics*, 393, 2021. doi:10.1016/j.aim.2021.108076.
- [BBC⁺25] Andrea Basso, Giacomo Borin, Wouter Castryck, Maria Corte-Real Santos, Riccardo Invernizzi, Antonin Leroux, Luciano Maino, Frederik Vercauteren, and Benjamin Wesolowski. PRISM: Simple and compact identification and signatures from large prime degree isogenies. In Tibor Jager and Jiaxin Pan, editors, *Public-Key Cryptography – PKC 2025*, volume 15676 of *Lecture Notes in Computer Science*, pages 300–332, Cham, 2025. Springer. doi:10.1007/978-3-031-91826-1_10.
- [BFI86] E. Bombieri, J. B. Friedlander, and H. Iwaniec. Primes in arithmetic progressions to large moduli. *Acta Mathematica*, 156:203–251, 1986. doi:10.1007/BF02399204.
- [CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009. doi:10.1007/s00145-007-9002-x.
- [CPV20] Wouter Castryck, Lorenz Panny, and Frederik Vercauteren. Rational isogenies from irrational endomorphisms. In *Advances in Cryptology – EUROCRYPT 2020*, volume 12106 of *LNCS*, pages 523–548. Springer, 2020. doi:10.1007/978-3-030-45724-2_18.
- [DFKL⁺20] Luca De Feo, David Kohel, Pierre Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign: Compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology – EUROCRYPT 2020*, volume 12106 of *Lecture Notes in Computer Science*, pages 523–548. Springer, 2020. doi:10.1007/978-3-030-64837-4_3.

- [Dus10] Pierre Dusart. Estimates of some functions over primes without r.h., 2010. Preprint.
- [EHL⁺18] Kirsten Eisenträger, Sean Hallgren, Kristin E. Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *EUROCRYPT 2018*, 2018. doi:[10.1007/978-3-319-78372-7_11](https://doi.org/10.1007/978-3-319-78372-7_11).
- [GPS20] Steven D. Galbraith, Christophe Petit, and Javier Silva. Identification protocols and signature schemes based on supersingular isogeny problems. *J. Cryptology*, 33(1):130–175, 2020. doi:[10.1007/s00145-019-09316-0](https://doi.org/10.1007/s00145-019-09316-0).
- [GPST16] Steven D. Galbraith, Christophe Petit, Barak Shani, and Yuval Ti. On the security of supersingular isogeny cryptosystems. In *ASIACRYPT 2016*, volume 10031 of *LNCS*, pages 63–91. Springer, 2016. doi:[10.1007/978-3-662-53887-6_3](https://doi.org/10.1007/978-3-662-53887-6_3).
- [IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic Number Theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004. doi:[10.1090/coll/053](https://doi.org/10.1090/coll/053).
- [Iwa97] Henryk Iwaniec. *Topics in Classical Automorphic Forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997. doi:[10.1090/gsm/017](https://doi.org/10.1090/gsm/017).
- [KLPT14] David Kohel, Kristin E. Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS J. Comput. Math.*, 17:418–432, 2014. doi:[10.1112/S1461157014000379](https://doi.org/10.1112/S1461157014000379).
- [Koh96] David Kohel. *Endomorphism rings of elliptic curves over finite fields*. PhD thesis, University of California, Berkeley, 1996.
- [KV10] Markus Kirschmer and John Voight. Algorithmic enumeration of ideal classes for quaternion orders. *SIAM J. Comput.*, 39(5):1714–1747, 2010. doi:[10.1137/080734467](https://doi.org/10.1137/080734467).
- [Lan15] Edmund Landau. Zur analytischen zahlentheorie der definiten quadratischen formen. *Berliner Sitzungsberichte*, 31:458–476, 1915.
- [Lin41] U. V. Linnik. The large sieve. *Dokl. Akad. Nauk SSSR*, 30:292–294, 1941.
- [Lin17] S. Lindqvist. Weak approximation results for quadratic forms in four variables, 2017. Preprint, arXiv:2405.05592.
- [LMW25] Arthur Herlédan Le Merdy and Benjamin Wesolowski. Unconditional foundations for supersingular isogeny-based cryptography. In *Theory of Cryptography (TCC 2025), Proceedings, Part III*, volume 16270 of *Lecture Notes in Computer Science*, pages 266–297. Springer, 2025. doi:[10.1007/978-3-032-12296-4_9](https://doi.org/10.1007/978-3-032-12296-4_9).
- [LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the chebotarev density theorem. In *Algebraic Number Fields*, pages 409–464. Academic Press, 1977.
- [Mam24] Maher Mamah. The supersingular ℓ -isogeny path and endomorphism ring problems: Tighter unconditional reductions. Cryptology ePrint Archive, Paper 2024/1569, 2024. URL: <https://eprint.iacr.org/2024/1569>.

- [Mam25] Maher Mamah. Enhanced algorithms for the representation of integers by binary quadratic forms: reduction to subset sum. arXiv, 2025.
- [PR23] Aurel Page and Damien Robert. Introducing clapoti(s): evaluating the isogeny class group action in polynomial time. Cryptology ePrint Archive, 2023.
- [PW24] Aurel Page and Benjamin Wesolowski. The supersingular endomorphism ring and one endomorphism problems are equivalent. In *EUROCRYPT 2024*. Springer, 2024. doi:[10.1007/978-3-031-58751-1_14](https://doi.org/10.1007/978-3-031-58751-1_14).
- [Rón92] Lajos Rónyai. Algorithmic properties of maximal orders in simple algebras over $\mathbb{Q}$. *Computational Complexity*, 2(3):225–243, 1992. URL: <https://doi.org/10.1007/BF01272075>.
- [Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986. doi:[10.1007/978-1-4757-1920-8](https://doi.org/10.1007/978-1-4757-1920-8).
- [Vél71] J. Vélú. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris*, 273:238–241, 1971.
- [Voi21] John Voight. *Quaternion Algebras*, volume 288 of *Graduate Texts in Mathematics*. Springer, 2021. doi:[10.1007/978-3-030-56694-4](https://doi.org/10.1007/978-3-030-56694-4).
- [Wat69] William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure*, 2:521–560, 1969.
- [Wes22] Benjamin Wesolowski. The supersingular isogeny path and endomorphism ring problems are equivalent. In *FOCS 2022*, pages 1100–1111. IEEE, 2022. doi:[10.1109/FOCS52979.2021.00109](https://doi.org/10.1109/FOCS52979.2021.00109).