Computing Quaternion Embeddings and Endomorphism rings of Supersingular Oriented Elliptic curves

MAHER MAMAH

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

Abstract. In this paper, we investigate several computational problems motivated by post-quantum cryptosystems based on isogenies and ideal class group actions on oriented elliptic curves. Our main technical contribution is an efficient algorithm for embedding the ring of integers of an imaginary quadratic field K into some maximal order of the quaternion algebra $B_{p,\infty}$ ramified at a prime p and infinity. Assuming the Generalized Riemann Hypothesis (GRH), our algorithm runs in probabilistic polynomial time, improving upon previous results that relied on heuristics or required the factorization of $\mathrm{disc}(K)$. Notably, this algorithm may be of independent interest.
Our approach enhances the work of Love and Boneh [LB20] on computing isogenies between M-small elliptic curves by eliminating heuristics and improving computational efficiency. Furthermore, given a quadratic order $\mathfrak{O}$ in K, we show that our algorithm reduces the computational *endomorphism ring problem* of $\mathfrak{O}$-oriented elliptic curves to the *Vectorization* problem in probabilistic polynomial time, assuming the conductor of $\mathfrak{O}$ can be efficiently factorized. Previously, the best known result required the full factorization of $\mathrm{disc}(\mathfrak{O})$, which may be exponentially large.
Additionally, when the conductor of $\mathfrak{O}$ can be efficiently factorized, we establish a polynomial-time equivalence between the *Quaternion Order Embedding Problem*, which asks to embed a quadratic order $\mathfrak{O}$ into a maximal order in $B_{p,\infty}$, and computing *horizontal isogenies* between $\mathfrak{O}$-oriented elliptic curves. Leveraging this reduction, we propose a rigorous algorithm, under GRH, that solves the *quaternion order embedding problem* in time $\tilde{O}(|\mathrm{disc}(\mathfrak{O})|^{1/2})$, improving upon previous methods that required higher asymptotic time and relied on several heuristics.

1. Introduction

Isogeny-based cryptography has attracted significant attention in recent years due to its strong potential for resistance against quantum computers. While polynomial-time quantum algorithms can break widely used public-key cryptosystems such as RSA and Elliptic Curve Cryptography (ECC), the most advanced classical and quantum algorithms for certain isogeny-based schemes still require exponential time to break.
In this paper, we study two types of computational problems that play a crucial role in many current isogeny-based cryptographic protocols: inverting the ideal class group action on supersingular elliptic curves, known as the VECTORIZATION problem, and computing the endomorphism ring of such curves. The former problem lies at the core of several protocols such as CSIDH [CLM+18] and OSIDH [CK20], as well as many variants ([CS21], [BKV19]). The hardness assumption of the latter problem is critically important for the security of numerous protocols and cryptosystems, including [CLG09] and [GPS20].
The first instance of these group action protocols was introduced in [CLM+18] with CSIDH (pronounced "seaside"), where the ideal class group of the ring $\mathbb{Z}[\sqrt{-p}]$ acts on the set of supersingular $\mathbb{F}_p$-elliptic curves. The problem reduces to computing an ideal class $[\mathfrak{a}]$ such that $E' = [\mathfrak{a}] \cdot E$, where E and E' are supersingular elliptic curves defined over $\mathbb{F}_p$ (see section 3).
In 2020, Colo and Kohel [CK20] introduced the notion of *orientation*, which refers to an embedding of a quadratic imaginary order into the endomorphism ring of an elliptic curve, with such a curve being termed *oriented*. This concept of *orientation* established a more rigorous foundation for the problem of inverting the action of the ideal class group and generalized CSIDH to work with various orders, not limited to $\mathbb{Z}[\sqrt{-p}]$, as in OSIDH.

On the other hand, the *Endomorphism Ring Problem* (ENDRING) asks to compute a basis for the endomorphism ring of a supersingular elliptic curve E over $\mathbb{F}_{p^2}$. It has been rigorously shown

in [Wes21], under the Generalized Riemann Hypothesis (GRH), that ENDRING is equivalent to computing isogenies between supersingular elliptic curves.
Alternatively, given an orientation on an elliptic curve by an imaginary quadratic order $\mathfrak{O}$, i.e., $\mathfrak{O} \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$, this orientation provides knowledge of a non-scalar endomorphism. Consequently, one may ask about the relationship between the $\mathfrak{O}$-VECTORIZATION problem and the modified variant of the Endomorphism Ring Problem, denoted by $\mathfrak{O}$-ENDRING when an orientation is provided. Wesolowski [Wes22] demonstrated that these two problems are equivalent under polynomial-time reductions, provided the factorization of $\mathrm{disc}(\mathfrak{O})$ is known. More recently, Eriksen and Leroux [EL24] improved upon the latter result in one direction, namely showing that $\mathfrak{O}$-VECTORIZATION reduces to $\mathfrak{O}$-ENDRING without requiring the factorization of $\mathrm{disc}(\mathfrak{O})$. However, no known improvement has been made in the reverse direction.

A seemingly unrelated problem which has recently gained considerable attention in the context of orientations, known as *the Quaternion Order Embedding problem*, asks to find an embedding of an imaginary quadratic order $\mathfrak{O} \hookrightarrow \mathcal{O}$ where $\mathcal{O}$ is a given maximal order in $B_{p,\infty}$. This problem, initially studied by [ACD+23] and later on by [EL24], proved helpful in computing isogenies of fixed degree between supersingular elliptic curves, a task of utmost importance in isogeny-based cryptography. It is worthy to note that the best known algorithm to solve this problems runs heuristically in $O(|\mathrm{disc}(\mathfrak{O})|^{\frac{3}{4}}/p)$, which is exponential for $|\mathrm{disc}(\mathfrak{O})| \gg p^{4/3}$.

Contributions. In this paper, we improve upon the other direction of reducing the $\mathfrak{O}$-ENDRING to the $\mathfrak{O}$-VECTORIZATION problem. We demonstrate that the full factorization of $\mathrm{disc}(\mathfrak{O})$ is unnecessary; instead, it is sufficient to factorize the conductor of $\mathfrak{O}$. Further improvements on this result would require solving an instance of a descending isogeny problem (definitions provided later), which remains beyond current capabilities. Our main technical contribution lies in addressing the problem of embedding the ring of integers $\mathfrak{O}_K$ of an imaginary quadratic field K into $B_{p,\infty}$, the quaternion algebra ramified at p and ∞. This problem reduces to solving the norm form equation of $B_{p,\infty}$ over $\mathbb{Q}$. We adapt techniques similar to those in [Sim05] and [Cast11] and demonstrate how the special properties of the norm form of $B_{p,\infty}$ can be exploited to achieve this. Accordingly, we provide a probabilistic polynomial-time algorithm solving this task under the assumption of the Generalized Riemann Hypothesis (GRH), where previously known algorithms ([Wes22], [LB20]) either required the factorization of $\mathrm{disc}(\mathfrak{O}_K)$ as input or relied on heuristics. The largest portion of the work will be devoted to developing the necessary tools for devising the algorithm, which will span several sections.

- In Sections 2, 3, and 4, we provide the necessary background material on oriented elliptic curves, including precise definitions and the latest advancements in the field.
- In Section 5, we cover the necessary background on the theory of quadratic forms and fundamental theorems such as the Hasse-Minkowski theorem, and the Smith Normal form.
- In Section 6, we develop a pre-conditioning algorithm that minimizes the determinant of our norm form to a square-free value. This step is crucial for our main algorithm, enabling us to eliminate the factorization assumption on $\mathrm{disc}(\mathfrak{O}_K)$ by leveraging specific properties of the norm form equation and its Smith normal form.
- In Section 7, we provide analytic estimates, using Chebotarev's density theorem, for primes represented by quaternary quadratic forms satisfying certain residuosity conditions. The proof resorts to analytic number theory, and the results, namely theorems 7.7 and 7.8, unlock the analysis of algorithm 2.
- In Section 8, we present the complete algorithm to solve the norm form equation of $B_{p,\infty}$ over $\mathbb{Q}$. Consequently, we describe the algorithm that embeds the ring of integers of an imaginary quadratic field into $B_{p,\infty}$.
- In Section 9, we show how we use our result from section 8 to reduce $\mathfrak{O}$-ENDRING to $\mathfrak{O}$-VECTORIZATION in polynomial time, assuming the factorization of the conductor of $\mathfrak{O}$ is provided. The approach will be essentially similar to [Wes22].

- Finally in section 10, we gather previous tools and demonstrate that the *Quaternion Order Embedding Problem* is equivalent to computing *horizontal isogenies* in polynomial time, given the factorization of the conductor of $\mathfrak{O}$. Additionally, we also give a rigorous algorithm, under GRH, that solves the quaternion order embedding problem in time $\tilde{O}(|\mathrm{disc}(\mathfrak{O})|^{1/2})$, enhancing the results of [EL24].

Remark. All statements containing the mention (GRH) assume the Generalized Riemann Hypothesis.

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 $\mathbb{F}_{p^2}$.

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

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

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 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*

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

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 $\log p$.

2.3. **Orientations and Optimal Embeddings.**

Let K be an imaginary quadratic field, with ring of integers $\mathfrak{O}_K$, and an arbitrary order $\mathfrak{O}$.

Definition 2.2. *A K-orientation on an elliptic curve is an embedding $\iota : K \hookrightarrow \mathrm{End}(E) \otimes \mathbb{Q}$. It is an $\mathfrak{O}$-orientation if $\iota(\mathfrak{O}) = \iota(K) \cap \mathrm{End}(E)$. Such an orientation is said to be a primitive orientation, and we call (E, ι) and E' $\mathfrak{O}$-oriented and $\mathfrak{O}$-orientable elliptic curves respectively.*

For simplicity in this paper, we will use the term orientation, even though we really mean a primitive orientation. The next definition gives an analogue of the previous one in the language of maximal orders in a quaternion algebra.

Definition 2.3. *Given a maximal order $\mathcal{O} \subset B$ where B is a quaternion algebra, and an embedding $\iota : K \hookrightarrow B$, we define an $\mathfrak{O}$-oriented order to be the pair $(\mathcal{O}, \iota)$ whenever $\iota(\mathfrak{O}) \subseteq \mathcal{O}$. Further, $(\mathcal{O}, \iota)$ is said to be a primitively $\mathfrak{O}$-oriented order if $\iota(\mathfrak{O}) = \iota(K) \cap \mathcal{O}$ and ι is called an optimal embedding. Moreover, if $\mathcal{O}$ admits an $\mathfrak{O}$-orientation/embedding, we say $\mathcal{O}$ is $\mathfrak{O}$-orientable.*

Remark. In a sense, $\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$ is an optimal embedding if $\mathfrak{O}$ can't be enlarged to a superorder $\mathfrak{O}' \supsetneq \mathfrak{O}$ such that $\iota(\mathfrak{O}') \subseteq \mathcal{O}$.
We now state the Quaternion order embedding problem which has been firstly studied in [ACD$^+$23] and further in [EL24].

Problem 1 **($\mathfrak{O}$-EMBEDDING)** Given an $\mathfrak{O}$-orientable maximal order $\mathcal{O} \subseteq B_{p,\infty}$, find an optimal embedding $\iota : \mathfrak{O} \hookrightarrow \mathcal{O}$.

We'll study this problem further in section 9 and prove some useful reductions.

Now given an oriented elliptic curve (E, ι), any isogeny $\varphi : E \to E'$ induces a K-orientation $\varphi_*(\iota)$ on E' defined as

$$\varphi_*(\iota)(\alpha) = \frac{1}{\deg\varphi} \otimes (\varphi \circ \iota(\alpha) \circ \hat{\varphi}).$$

The twist of (E, ι) is defined to be $(E, \bar{\iota})$ where $\bar{\iota}(\alpha) = \iota(\bar{\alpha})$, and the Frobenius $(E^{(p)}, \iota^{(p)}) = (E, (\phi_p)_*(\iota))$ where $\phi_p : E \to E^{(p)}$ is the Frobenius isogeny.

Definition 2.4 (**Oriented isogeny**). *Given two K-oriented elliptic curves (E, ι) and (E', ι'), an isogeny $\varphi : (E, \iota) \to (E', \iota')$ is K-oriented if $\varphi_*(\iota) = \iota'$. If $\deg(\phi)$ is prime, ι is a $\mathfrak{O}$-orientation, and ι' is a $\mathfrak{O}'$-orientation, then the isogeny is:*

- ***horizontal**, if $\mathfrak{O} = \mathfrak{O}'$,*
- ***ascending**, if $\mathfrak{O} \subset \mathfrak{O}'$,*
- ***descending**, if $\mathfrak{O} \supset \mathfrak{O}'$.*

We say that an isogeny of composite degree is horizontal, ascending, or descending if it factors into prime degree isogenies, all of the same type.

Remark. If $\varphi_*(\iota)$ is an optimal embedding of $\mathfrak{O}$ into $\mathrm{End}(E')$, i.e $\varphi_*(\iota)(K) \cap \mathrm{End}(E') = \varphi_*(\iota)(\mathfrak{O})$ then φ is horizontal. Otherwise $\varphi_*(\iota)$ is optimal for some another order in K.

We write $\mathrm{SS}_{\mathfrak{O}}(p)$ to denote the set of $\mathfrak{O}$-oriented supersingular elliptic curves over $\mathbb{F}_p$ up to K-oriented isomorphism. We write $(E, \iota) \cong (E', \iota')$ if there exists a K-oriented isomorphism between them. The next proposition gives the condition for $\mathrm{SS}_{\mathfrak{O}}(p)$ to be non-empty.

Proposition 2.5 (**[Onu21], Proposition 3.2**). *The set $\mathrm{SS}_{\mathfrak{O}}(p)$ is non-empty if and only if p doesn't split in K and p doesn't divide the conductor of $\mathfrak{O}$.*

Remark. Notice that equivalently, a quadratic order can be embedded in $B_{p,\infty}$ if and only if p does not split in K and does not divide the conductor of $\mathfrak{O}$. Hence, we assume in the rest of the paper that p satisfies these properties.

Volcanoes. Here, we briefly discuss the structure of the oriented ℓ-isogeny graph of supersingular elliptic curves. Let $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, let $\ell \neq p$ be a prime, and let Δ be the discriminant of $\mathfrak{O}$. Let $\left(\frac{\Delta}{\ell}\right)$ be the Legendre symbol. From ([Onu21], proposition 4.1), the K-oriented isogenies of degree ℓ from (E, ι) are distributed as follows:

- There are $\ell - \left(\frac{\Delta}{\ell}\right)$ descending isogenies,
- If $\mathfrak{O}$ is maximal at ℓ, there are $\frac{\Delta}{\ell} + 1$ horizontal, and no ascending isogeny,
- If $\mathfrak{O}$ is non-maximal at ℓ, there is no horizontal, and one ascending isogeny.

3. Class group action on the set of Elliptic curves.

Fix an oriented curve $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$. An $\mathfrak{O}$-ideal $\mathfrak{a}$ induces a subgroup

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker(\iota(\alpha)),$$

and an isogeny $\varphi : E \to E'$ of degree $N(\mathfrak{a})$, where E' is the codomain of the isogeny associated with (E, ι) under the action of $\mathfrak{a}$ and we call it the $\mathfrak{a}$-transform of (E, ι). This construction induces an action of $\mathfrak{O}$-ideals on the set $\mathrm{SS}_{\mathfrak{O}}(p)$, defined by

$$\mathfrak{a} \star (E, \iota) = (E^{\mathfrak{a}}, (\varphi_{\mathfrak{a}})_*(\iota)).$$

Theorem 3.1 (**[Wes22], Theorem 1**). *The action*

$$\mathrm{Cl}(\mathfrak{O}) \times SS_{\mathfrak{O}}(p) \to SS_{\mathfrak{O}}(p) : ([\mathfrak{a}], (E, \iota)) \mapsto \mathfrak{a} \star (E, \iota)$$

is free and has at most two orbits. For any orbit A, and any $(E, \iota) \in SS_{\mathfrak{O}}(p)$, either $(E, \iota) \in A$, or both $(E, \bar{\iota})$ and $(E^{(p)}, \iota^{(p)})$ are in A.

Now that we have given the necessary background on orientations and class group action on oriented elliptic curves, we proceed by posing some computational problems which will be our primary interest in this paper.

Problem 2 **($\mathfrak{O}$-VECTORIZATION).** Given (E, ι), $(E', \iota') \in \mathrm{SS}_{\mathfrak{O}}(p)$, find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $E' \cong E^{\mathfrak{a}}$.

The importance of this $\mathfrak{O}$-VECTORIZATION problem is that many the security of many protocols like CSIDH and OSIDH and CSI-FiSH relies on the hardness assumption for this problem. If we require that no orientation be given on E', we obtain a seemingly much harder problem known as the $\mathfrak{O}$-UBER problem which has been introduced in [DDF+21].

Problem 3 **($\mathfrak{O}$-UBER).** Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an $\mathfrak{O}$-orientable elliptic curve E', find an $\mathfrak{O}$-ideal $\mathfrak{a}$ such that $E' \cong E^{\mathfrak{a}}$.

The significance of the $\mathfrak{O}$-UBER problem is that much of current isogeny-based cryptosystems seem to depend on its computational hardness like SIDH, SIKE, CSIDH and some other variants. For more details on this, we refer the reader to ([DDF+21], section 5).
Its been noted in [Wes22] that the $\mathfrak{O}$-VECTORIZATION and $\mathfrak{O}$-UBER problems can be heuristically solved in expected time $l^{O(1)}|\mathrm{disc}(\mathfrak{O})|^{1/4}$ and $l^{O(1)}|\mathrm{disc}(\mathfrak{O})|^{1/2}$ respectively, where l is the length of the input. Those results present the best know algorithm to tackle these problems which either rely on exhaustive search or the meet-in-the-middle approach.

4. The Oriented Endomorphism ring problem

The endomorphism ring problem denoted ENDRING, in its most generic form, asks to compute the endomorphism ring of a given supersingular elliptic curve E over $\mathbb{F}_{p^2}$. The best known algorithms run classically in $\tilde{O}(p^{1/2})$ [PW24] and quantumly in $\tilde{O}(p^{1/4})$ due to [CJS14]. To avoid the need to keep going back and forth between the endomorphism algebra $\mathrm{End}(E) \otimes \mathbb{Q}$ and $B_{p,\infty}$, we utilize the concept of ε-basis which was introduced in [Wes22].

Definition 4.1. *Let $\varepsilon : B_{p,\infty} \to \mathrm{End}(E) \otimes \mathbb{Q}$ be an isomorphism. Given a lattice $L \subseteq B_{p,\infty}$, an ε-basis of L is a pair (α, θ), where $(\alpha_i)_{i=1}^{\mathrm{rank}(L)}$ is a basis of L and $\theta_i = \varepsilon(\alpha_i)$. Abusing language, we also call (α, θ) an ε-basis of the image lattice $\varepsilon(L)$.*

Remark. We will often talk about an ε-basis without specifying a priori an isomorphism ε. The ε is then implicit, and when L has full rank, it is uniquely determined by the ε-basis.

The main concept behind the ε-basis of an endomorphism ring is its connection to the equivalence of two key problems. It was shown in [Wes21] that MAXORDER and ENDRING are equivalent under the assumption of the Generalized Riemann Hypothesis (GRH). Therefore, given a basis for one problem, it is possible to compute a basis for the other in polynomial time. It is then possible to define the endomorphism ring problem as follows:

Problem 4 **(ENDRING).** Given a supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, find an ε-basis of $\mathrm{End}(E)$.

When we additionally provide partial information and restrict to $\mathfrak{O}$-oriented curves we obtain the next variant of ENDRING.

Problem 5 **($\mathfrak{O}$-ENDRING).** Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, find an ε-basis for $\mathrm{End}(E)$.

This seemingly makes the problem easier, as an orientation provides us with the knowledge of a non-scalar endomorphism. Moreover, we don't require the solutions to $\mathfrak{O}$-ENDRING to be

compatible with the orientation, as it is easy to express the orientation in terms of a given ε-basis, thanks to the next lemma.

Lemma 4.2 ([Wes22], Lemma 2)**.** *Given $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ and an ε-basis of $\mathrm{End}(E)$, one can find an embedding $\jmath : \mathfrak{O} \hookrightarrow B_{p,\infty}$ such that $\varepsilon \circ \jmath = \iota$, in time polynomial in the length of the input.*

A seemingly much harder problem is the following, which asks to compute an orientation and the endomorphism ring.

Problem 6 **($\mathfrak{O}$-ENDRING*)**. Given a supersingular $\mathfrak{O}$-orientable curve E, find an ε-basis of $\mathrm{End}(E)$ and an embedding $\jmath : \mathfrak{O} \hookrightarrow B_{p,\infty}$ such that $\varepsilon \circ \jmath$ is an $\mathfrak{O}$-orientation.

Its been shown in [Wes22] that $\mathfrak{O}$-ENDRING and $\mathfrak{O}$-ENDRING* resepctively reduce to $\mathfrak{O}$-VECTORIZATION and $\mathfrak{O}$-UBER, assuming we're given the factorization of $\mathrm{disc}(\mathfrak{O})$. We will show how we can enhance this result in section 8.
We now introduce a new computational problem which asks to find a horizontal isogeny between two elliptic curves.

Problem 7 **($\mathscr{H}$-ISOGENY)** Given $\mathfrak{O}$-oriented and $\mathfrak{O}$-orientable elliptic curves (E, ι) and E', along with ε-basis of their endomorphism rings, find a horizontal isogeny $\varphi : E \to E'$.

In section 9, we will show that $\mathfrak{O}$-EMBEDDING and $\mathscr{H}$-ISOGEY are equivalent under polynomial time reductions assuming GRH and a factorization of the conductor of $\mathfrak{O}$ is provided. We hope that this will further open new ways to solving the $\mathfrak{O}$-EMBEDDING problem, as the best known algorithm runs heuristically in exponential time in $\log|\mathrm{disc}(\mathfrak{O})|$ for large $|\mathrm{disc}(\mathfrak{O})|$.

5. Quadratic forms and their invariants

In this section we give the necessary background needed for our work with Quadratic forms over $\mathbb{Q}$. The main reference will be [Ser73] and [Cas78]. A quadratic form $Q(x)$ in n variables over $\mathbb{Q}$ is a polynomial whose terms all have degree 2 with coefficients in $\mathbb{Q}$. Its defined as $Q(x) = x^t A x$ where $A = (a_{ij})$ is a symmetric $r \times r$ matrix called the Gram matrix. For convenience, we will occasionally refer to Q interchangeably as the quadratic form and its associated Gram matrix. We will aslo occasionally write $\mathrm{diag}[a_1, \cdots .a_n]$ to denote a diagonal form. A quadratic form is integral if $Q(x) \in \mathbb{Z}$ for $x \in \mathbb{Z}^n$, equivalently if all diagonal entries are integral and non-diagonal entries belong to $\frac{1}{2}\mathbb{Z}$. A quadratic form Q is primitive if all its coefficients are coprime. A vector $x \in \mathbb{Q}^n$ is isotropic if $Q(x) = 0$. We associate to a quadratic form the symmetric bilinear form

$$\langle x, y\rangle = \frac{1}{2}\left(Q(x+y) - Q(x) - Q(y)\right),$$

and one has $Q(x) = \langle x, x\rangle$. This establishes a bijective correspondence between *quadratic forms* and *symmetric bilinear forms*. Given the bilinear form, one can recover the Gram matrix by computing $g_{i,j} = \langle e_i, e_j\rangle$ where $(e_i)_{i=1}^n$ is the canonical basis. A *quadratic space* V over $\mathbb{Q}$ is a vector space of finite dimension together with a quadratic map $q : V \to \mathbb{Q}$ such that for any (hence all) basis $(b_i)_{i=1}^n$ of V, we have that $q\left(\sum_{i=1}^n x_i b_i\right)$ is a quadratic form in x_i.

Remark 1. If we change the basis (e_i) by means of an invertible matrix X, the matrix A' of Q with respect to the new basis is $X^t A X$, where X^t denotes the transpose of X, and we say Q' associated to A' is equivalent to Q over $\mathbb{Q}$. In particular,

$$\det(A') = \det(A) \cdot \det(X)^2,$$

which shows that $\det(A)$ is determined up to multiplication by an element of $\mathbb{Q}^{*2}$; it is called the *discriminant* of Q and denoted by $\mathrm{disc}(Q)$.

Definition 5.1. *Let $n > 0$, we denote by $Sym(n, \mathbb{Z})$ the set of square $n \times n$, symmetric matrices with non-zero determinant with integer coefficients.*

Definition 5.2. *A basis $(e_1, \dots, e_n)$ of a quadratic module (V, Q) is called orthogonal if it is composed of elements that are pairwise orthogonal with resepct to the quadratic form Q.*

This is equivalent to saying that the matrix of Q with respect to this basis is diagonal:

$$\begin{bmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{bmatrix}$$

If $x = \sum x_i e_i$, we then have:

$$Q(x) = a_1 x_1^2 + \cdots + a_n x_n^2$$

Theorem 5.3. *Every quadratic module (V, Q) has an orthogonal basis.*

Proof. The proof of this theorem is given in ([Ser73], p: 30) □

Definition 5.4. *If Q is real, non-degenerate, it can be written in a basis where its matrix is diagonal, and let s denote the number of positive coefficients, and r the number of negative coefficients; the signature of Q is the pair (r, s).*

Proposition 5.5. *The signature of a quadratic form does not depend on the basis in which it is written.*

Proof. The proof of this result is detailed in ([Ser73], p.64) □

Definition 5.6. *If s or r is zero, Q is said to be definite (positive if $s = 0$, negative if $r = 0$). Otherwise, it is said to be indefinite.*

Remark. It is worthy to note that most of our work will be dedicated to indefinite forms.

Let Q be a quadatic form with $Q \sim a_1 x_1^2 + \cdots a_n x_n^2$ (i.e with respect to an orthogonal basis), and let Δ denote the class of $\det Q$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ where $\mathbb{Q}_p$ is the field of p-adic numbers, we have:

$$\Delta = a_1 \cdots a_n \quad \text{in } \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}.$$

In the following, we will often denote the same element of $\mathbb{Q}_p^*$ and its class modulo $\mathbb{Q}_p^{*2}$ with the same notation.

We now recall the definition of the Hilbert symbol.

Definition 5.7. *Let K be a field, and let $a, b \in K^*$. We define:*

$$(a, b) = \begin{cases} 1 & \text{if the equation } x^2 - az^2 - by^2 = 0 \text{ has a nontrivial solution in } K, \\ -1 & \text{otherwise.} \end{cases}$$

The number (a, b) is called the *Hilbert symbol* of a and b relative to K.

Remark: When the field considered is a p-adic field, we will denote this symbol by $(a, b)_p$. If the field is $\mathbb{R}$, it is denoted by $(a, b)_\infty$.

Proposition 5.8. *Let $a, b \in K^*$. Then:*

- *If $K = \mathbb{R}$, we have:*

$$(a, b)_\infty = \begin{cases} 1 & \text{if } a > 0 \text{ or } b > 0, \\ -1 & \text{otherwise.} \end{cases}$$

- *If $K = \mathbb{Q}_p$, write $a = p^\alpha u$ and $b = p^\beta v$ where $u,\ v\ \in \mathbb{Z}_p^*$, then we have:*
  - *If $p \neq 2$:*

$$(a, b)_p = (-1)^{\alpha\beta(\frac{p-1}{2})} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha,$$

– *If $p = 2$:*

$$(a, b)_2 = (-1)^{(\frac{u-1}{2})(\frac{v-1}{2})} \left(\frac{u}{2}\right)^{\beta} \left(\frac{v}{2}\right)^{\alpha},$$

where $\left(\frac{\cdot}{p}\right)$ represents the Legendre symbol modulo p.

Proof. The proof of this proposition is available in ([Ser73], p.23). □

Definition 5.9. *We define the Hasse-Witt invariant of Q to be*

$$\epsilon_p(Q) = \prod_{i<j} (a_i, a_j)_p \in \{-1, 1\}$$

Theorem 5.10. *The number $\epsilon_p(Q)$ does not depend on the basis $(e_i)_{i=1}^n$.*

Proof. More details can be found in ([Ser73], page: 35) □

Remark. From this we have that $\Delta = a_1 \cdots a_n \in Q_p/Q_p^{*2}$ and $\epsilon_p(Q)$ are invriants of the equivalence class of Q.
The next theorem will be important for our applications; it gives sufficients and necessay conditions for a quadratic form to be isotropic (equivalently represents 0) over $\mathbb{Q}_p$.

Theorem 5.11. *For Q to represent 0 over $\mathbb{Q}_p$, it is necessary and sufficient that the following conditions are satisfied:*
If $n = 2$, then $\Delta = -1$ in $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. If $n = 3$, then $(-1, -\Delta)_p = \epsilon_p$. If $n = 4$, then $\Delta \neq 1$, and if $\Delta = 1$, we have $\epsilon_p = (-1, -1)_p$. Finally, if $n \geq 5$, the condition is automatically satisfied.

Proof. See Theorem 6 of ([Ser73], page: 36) □

We now state the theorem of Hasse-Minkowski for quadratic forms to represent 0 over $\mathbb{Q}$,

Theorem 5.12. *(Hasse-Minkowski) For a non-degenerate quadratic form Q to represent 0 over $\mathbb{Q}$, it is necessary and sufficient that f represents 0 over $\mathbb{Q}_p$ for every prime p and over $\mathbb{R}$.*

Proof. See ([Cas78], page: 75). □

For application purposes we will need the stronger version of Hasse-Minkowski's theorem for indefinite ternary quadratic forms which possibly excludes one prime.

Theorem 5.13. *Let Q be a non-degenerate ternary form over $\mathbb{Q}$. Suppose that Q is isotropic over $\mathbb{Q}_p$ for all p (including $p = \infty$) with one possible exception p_0 (which may be either ∞ or a finite prime). Then f is isotropic over $\mathbb{Q}$.*

Proof. See ([Cas78], page:82) for more details. This theorem is based essentially on Hilbert's reciprocity law. □

It turns out that in principle we don't have to check completions at each prime, but rather only primes $p|2 \det Q$. The next theorem is a classical result, and a simple proof of that can be found in ([Cast11], proposition 2.2.3).

Theorem 5.14. *Let Q be a quadratic form of dimension $n \geq 3$ over $\mathbb{Z}$. For Q to represent 0 over $\mathbb{Q}$, it is necessary and sufficient that Q represents 0 over $\mathbb{Q}_p$ for every prime p dividing $2 \det Q$ and over $\mathbb{R}$.*

6. Minimization of norm form in a quaternion algebra

In this section we look at the first pre-conditioning step to ensure the existence of a rational solution to the norm form equation arising in the quaternion algebra $B_{p,\infty}$. In order to embed the ring of integers $\mathfrak{O}_K = \mathbb{Z}[\alpha]$ of the imaginary quadratic field K, we'd need to find an element $\beta \in B_{p,\infty}$ with $t = \mathrm{tr}(\beta) = \mathrm{tr}(\alpha)$ and $\mathrm{N}(\beta) = \mathrm{N}(\alpha) = n$, i.e solve the norm form equation

$$(t/2)^2 + qx_1^2 + px_2^2 + pqx_3^2 = n$$

with $x_1, x_2, x_3 \in \mathbb{Q}$. Alternatively we'd like to solve $qx_1^2 + px_2^2 + pqx_3^2 - dx_4^2 = 0$ for some constant d. According to heuristics we can avoid factorizing the determinant of a quadratic form $Q(x)$ if the determinant is square-free, which is of course not the case in our extended norm form equation

$$Q(x_1, x_2, x_3, x_4) = qx_1^2 + px_2^2 + pqx_3^2 - dx_4^2. \tag{1}$$

For simplicity we will assume that d is square-free, and we'll show that this doesn't really cause any trouble but will simplify our work and speed up computations. We will also assume that p, q and d are coprime, otherwise we can divide by the common factor, for which the procedure will be even simpler. We now recall the definition of Smith normal form which will be an essential tool in our preconditioning step.

Definition 6.1 (Smith Normal Form)**.** *Let $A \in \mathcal{M}_n(\mathbb{Z})$ be a matrix with nonzero determinant. Then there exist a unique matrix D, called the Smith Normal Form (SNF) of A, and two matrices $U, V \in GL_n(\mathbb{Z})$ such that:*

$$D = UAV,$$

where:

$$D = \begin{bmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_n \end{bmatrix},$$

and for $1 \leq i \leq n$, $d_i \in \mathbb{Z}, d_i > 0$, with the divisibility condition:

$$d_n \mid d_{n-1} \mid \cdots \mid d_2 \mid d_1,$$

where d_i are called the invariant factors of A.

We will denote the invariant factors we're working with by d_i, for the rest of the paper, when there is no possible confusion.

Definition 6.2. *We denote by $Sym^*(n, \mathbb{Z})$ the set of square and symmetric $n \times n$ integral matrices such that $d_2 = 1$, where d_2 is the second invariant factor coming from SNF.*

We now give the outline of our procedure to find rational solution to (1) without factoring the determinant, which is essentially inspired by [Cast11].

Outline of Algorithm Given the quadratic form $Q(x)$ from (1), which we will sometimes refer to as Q_4, our goal is to find a rational solution to $Q(x) = 0$ without factorizing $\det Q$. To achieve this, we're going to complete the matrix Q into a 5-dimensional quadratic form Q_5 whose determinant will be a prime ℓ. We will call this the completion step. We can then use [Sim05] to obtain an isotropic vector for Q_5, which will allow us to obtain an isotropic vector for Q by looking at the intersection of suitable hyperbolic spaces and hence a solution for (1). The main idea is that the algorithm of [Sim05] is very efficient provided we have the factorization of the determinant which is trivial in the case of a prime ℓ. The resulting matrix will be completed such that

$$Q_5 = \left[\begin{array}{c:c} Q_4 & X \\ \hdashline X^t & z \end{array}\right], \tag{2}$$

where $X \in \mathbb{Z}^4$ and $z \in \mathbb{Z}$, will be chosen such that $\det Q_5 = \ell$ is a prime. The following lemma will be useful to express the determinant of the completed matrix.

Lemma 6.3. *Let Q_n be in $Sym(n, \mathbb{Z})$. For a completed matrix, similar to (2), we have:*

$$\det Q_{n+1} = z \det Q_n - X^t \operatorname{Co}(Q_n) X, \tag{2}$$

where $\operatorname{Co}(Q_n)$ is the cofactor matrix of Q_n satisfying $Co(Q_n) = det(Q_n) \cdot Q_n^{-1}$.

Proof. The proof is a straightforward computation. For more details see ([Cast11], 3.1.3). □

To see the values taken by $\det Q_5$, we will need the following theorem.

Theorem 6.4. *Let Q_4 be in $Sym(n, \mathbb{Z})$, then for all $X \in \mathbb{Z}^4$ and all $z \in \mathbb{Z}$ we have $d_2(Q) | \det Q_5$ where Q_5 is the completed matrix from 2 and $d_2(Q)$ is the second invariant factor of SNF.*

Proof. Using the Smith Normal Form, $D = UQV$, where: D is diagonal with elementary divisors $d_1, \ldots, d_5$, $U, V \in GL_n(\mathbb{Z})$, with $\det U, \det V = \pm 1$.

The cofactor matrix of Q is:

$$\operatorname{Co}(Q) = \operatorname{Co}(V^{-1}) \operatorname{Co}(D) \operatorname{Co}(U^{-1}) = \det U \det V (V^t \operatorname{Co}(D) U^t) = \pm (U \operatorname{Co}(D) V)^t.$$

Since D is diagonal, $\operatorname{Co}(D)$ is also diagonal, and all its entries are divisible by $d_2(Q)$. Thus:

$$X^t \operatorname{Co}(Q) X = \pm X^t (U \operatorname{Co}(D) V)^t X \equiv 0 \pmod{d_2(Q)}.$$

Combining this congruence with the formula of the previous lemma proves the result. □

Remark. The above lemma shows that if $d_2(Q) \neq 1$, then we will not be able complete Q_4 into a matrix Q_5 of a prime determinant. Hence we will have to do some minimizations on Q_4 until we have $d_2(Q) = 1$.

Lemma 6.5. *If we apply a change of basis using the matrix V from the SNF of Q, i.e. $Q' = V^t Q V$, where $d_i(Q) \neq 1$ and $d_{i+1}(Q) = 1$, then the first i rows and columns of the matrix will be divisible by $d_i(Q)$.*

Proof. This has been stated in [Castel12] and proven in more details in ([Cast11], lemma 2.2.3). □

To minimize Q, we firstly examine the Smith normal form of $Q(x_1, x_2, x_3, x_4) = qx_1^2 + px_2^2 + pqx_3^2 - dx_4^2$ and accordingly give the minimization algorithm.

Lemma 6.6. *For the quadratic form $Q(x)$ given by (1) the smith normal form of the matrix of Q is given by*

$$D = UQV = \begin{bmatrix} pqd & 0 & 0 & 0 \\ 0 & pq & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Proof. This is a straightforward computation using the algorithm for Smith normal form. □

Theorem 6.7 (Minimization)**.** *On input the matrix Q of the quadratic form given by (1), algorithm 1 outputs two integral 4×4 matrices Q_f and G, with Q_f $\mathbb{Q}$-equivalent to Q, such that*

$$(pq) \cdot Q_f = G^t Q G,$$

$$det Q_f = \frac{1}{(pq)^2} \det Q = d,$$

and runs in polynomial time in $\log(pqd)$.

Algorithm 1 MINIMIZATION(Q)

Input: Diagonal indefinite form $Q_4 = \text{diag}[q, p, pq, -d]$ such that $d_2(Q) \neq 1$ and $d_3(Q) = 1$.
Output: $Q_f \in Sym^*(4, \mathbb{Z})$ equivalent to Q, and change of basis matrix G such that $(pq) \cdot Q_f = G^t Q G$.

1: Compute the SNF of Q and the unimodular matrices U and V; [Cost89]
2: Set $G = V$ and $Q = G^t Q G$;
3: Set Q_2 the left bottom 2×2 submatrix;
4: Apply a modified version of Gram-Shmidt orthogonalization process to Q_2 and $m = pq$
5: If the Gram-Schmidt process returns a vector S, store it and go to step 10. If it returns p or q, go back to step 4 and apply Gram-Shmidt to Q_2 with $m = p$ or $m = q$.
6: Denote by D_2 the returned matrix and G_2 the corresponding change of basis matrix;
7: Let $d = gcd(D_2(1,1), m)$, if $d > 1$ go back to step 5 with $m = d$;
8: Solve $D_2(1,1)x_0^2 + D_2(2,2)y_0^2 \equiv 0 \mod m$;
9: Set $S = (x_0, y_0)$ to be the solution from step 8
10: Compute H; a 2×2 matrix whose first column is equal to S using Hermite Normal form algorithm.
11: Set $G_2 = G_2 \cdot H$;
12: Set G_3 to be the 4×4 diagonal matrix whose first 2×2 submatrix is the identity and the 2×2 bottom right matrix equal to G_2
13: Set $G_4 = \text{diag}[1, 1, 1, m]$ and $G_5 = G_3 \cdot G_4$;
14: Set $G = G \cdot G_5$ and $Q' = (1/m)G^t Q G$;
15: If $m \neq pq$, go to step 1 replacing Q by Q'
16: Apply the LLL algorithm to reduce Q', and denote by Q_f the returned form and by G' the corresponding change of basis; [DSim05]
17: Set $G = G \cdot G'$
18: **return** Q_f and G.

Proof. Steps 1,2 We compute the SNF of Q and then apply a change of basis using V to get $Q^{(1)} = V^t Q V$ where the first 2 rows and columns are divisible by $d_2(Q) = pq$.

Steps 3,4 We denote by Q_2 the restriction of $Q^{(1)}$ to the space spanned by the last 2 column vectors which corresponds to the left bottom 2×2 submatrix. We'd like to have $Q_2(1,1) \equiv 0 \mod m$ where $m = pq$. This will allow us to multiply the last columnn and row by m and then divide the entire matrix by m which will eliminate the square part of the determinant.

Step 5. We apply the Gram-Shmidt orthogonalization process $\mod m$. If we find an non-invertible element $\mod m$ then we obtained a divisor p or q of m, for which we repeat the process replacing m by that divisor. During the process, if we find a vector whose norm is 0 modulo m, we just have to skip this step since this vector is exactly what we need.

Steps 7, 8. When the process ends it gives us a change of basis matrix G_2, which is upper triangular with entries between 0 and $m-1$ and 1's on the diagonal, such that D_2 has the form

$$D_2 = G_2^t Q_2 G_2 = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mod m.$$

We are then interested in solving the equation $ax^2 + by^2 \equiv 0 \mod m$. If the coefficient a is not invertible modulo m we have found a factor of m, so we can continue the process with both factors, obtain the solution for each of them and combine them using the Chinese remainder theorem and Hensel's lemma if needed, so we assume a is invertibe modulo m. In general, for composite m, solving the above congruence is equivalent to finding quadratic residues, which turns to be equivalent to factoring m. However, since we know $m|pq$ where p and q are known primes, we can efficiently solve the equation and use the Chinese remainder theorem, if necessary, to obtain a solution mod

pq. We thus obtain a solution $S = (x_0, y_0)$ to the above equation.

Step 10. We complete the single vector family $\{S\}$ to a unimodular matrix H using Hermite Normal form algorithm, and we extend the matrix H to a matrix G_3 of dimension 4 by taking the identity matrix Id_2 and replacing the 2×2 lower-right block by $G_2 \cdot H$. We now apply G_3 to $Q^{(1)}$ and obtain $Q^{(2)}$, which has the form

$$G_3^t Q^{(1)} G_3 = Q^{(2)} = \begin{bmatrix} mM_{2,2}^{(1)} & mM_{2,2}^{(2)} \\ \\ mM_{2,2}^{(3)} & \begin{matrix} m* & * \\ * & * \end{matrix} \end{bmatrix}$$

where the $*$ are integers and $M_{2,2}^{(i)}$ represents a 2 by 2 matrix.

Steps 13,14. Once Q is in the above form it is sufficient to multiply on the right and left by

$$G_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & m \end{bmatrix},$$

for which it multiplies the last row and column by m, and the entire matrix will be divisible by m. We finally divide the matrix by m. We have thus multiplied the determinant of Q by m^2 and divided it by m^4, so that $\det Q' = \frac{1}{m^2} det(Q)$.

Step 15. If $m \neq pq$ then the corresponding matrix Q' has a determinant $(pq/m)^2 d$, for which we repeat the process replacing Q by Q'. The algorithm succeeds again since the the first upper two entries of the SNF are $(pq/m)d$ and pq/m respectively from which we can again solve the equation in step 8.

Step 16. This step includes a reduction step using an LLL algorithm for indefinite quadratic forms given in [DSim05]. This reduction is done to have concrete bounds for the size of the coefficients at the end of the algorithm.

The running time of the algorithm is clearly polynomial in the input, as most of the steps are simple linear algebra operations. □

Remark. The notion of equivalence between quadratic forms used here simply means that both corresponding quadratic equations have the same solutions up to a change of basis. Notice that a solution $X^t Q_f X = 0$ implies that $(GX)^t Q (GX) = 0$ for which we can deduce a solution to Q using G and vice versa. Hence its more convenient to work with the minimized form which has a square-free determinant d.

7. Completing the quadratic form

In this section we study the completion step of extending our quaternary form into a 5-dimensional form with prime determinant. We will also give the heuristic assumption to ensure some conditions on local solvability which will be essential to construct our global solution over $\mathbb{Q}$. We now explain how to choose the integer z in the completion step and how to control the signature of our completed quadratic form.

7.1. Constructing a new quadratic form

Lemma 7.1. *Let $Q_4 \in Sym^*(4,\mathbb{Z})$ be an indefinite quadratic form with signature (r,s) and determinant Δ. Let X be an 4-dimensional column vector with integer entries, and let $\bar{\beta}$ be a coset representative of the residue class of $X^t\mathrm{Co}(Q)X \mod \Delta$. Define*

$$z := \frac{X^t\mathrm{Co}(Q_4)X - \bar{\beta}}{\Delta_4} \quad \textit{and} \quad Q_5 = \begin{bmatrix} Q_4 & X \\ X^t & z \end{bmatrix}.$$

The signature of Q_5 is determined by the signs of $\bar{\beta}$ and $\det Q_4$ as follows:

$$sign(Q_5) = \begin{cases} (r, s+1), & \text{if } \bar{\beta}\det Q_4 > 0, \\ (r+1, s), & \text{if } \bar{\beta}\det Q_4 < 0. \end{cases}$$

Furthermore, we have $\bar{\beta} = -\det Q_5$.

Proof. The transition from Q_4 to Q_5 involves augmenting the matrix with an additional row and column. By restricting Q_5 to the subspace generated by the first four basis vectors, we retrieve the original form Q_4. Consequently, the process of completing Q_4 with an extra row and column preserves its signature within its initial subspace. As a result, the signature of Q_5 can be determined from the signature of Q_4 by analyzing the signs of Δ_4 and Δ_5. If the signature of Q_4 is (r,s), the signature of Q_5 can be determined using the sign of Δ_5, since $\mathrm{sgn}(\Delta_4) = (-1)^s$. Specifically:

- If $\Delta_4 > 0$, then $s \equiv 0 \mod 2$. Choosing $\bar{\beta} > 0$, we obtain $\Delta_5 < 0$. Thus, the determinant changes sign, and the signature of Q_5 is $(r, s+1)$.
- If $\Delta_4 < 0$ and we choose $\bar{\beta} < 0$, then $\Delta_5 > 0$, and the signature of Q_5 will be $(r, s+1)$.
- If $\Delta_4 > 0$, choosing $\bar{\beta} < 0$, we obtain $\Delta_5 > 0$. Hence, the signature of Q_5 is $(r+1, s)$.
- If $\Delta_4 < 0$, then $s \equiv 1 \mod 2$. Therefore, if we choose $\bar{\beta} > 0$, we have $\Delta_5 < 0$, and the signature of Q_5 will be $(r+1, s)$.

□

The next theorem will be pivotal in our analysis of the completion step which establishes congruence conditions modulo the determinant of an n-dimensional quadratic form.

Theorem 7.2. *Let $Q_n \in Sym^*(n,\mathbb{Z})$ with determinant Δ_n, then there exist an integer δ coprime to Δ_n, and $\alpha \in \mathbb{Z}$ such that for all $X \in \mathbb{Z}^n$*

$$X^t\mathrm{Co}(Q_n)X \equiv \delta\alpha^2 \mod \Delta_n$$

Moreover, α can be given by the first coordinate of $Y = V^tX$, where V is given by the Smith normal form of Q_n.

Proof. Since $Q_n \in Sym^*(n,\mathbb{Z})$, the the SNF of Q_n yield two unimodular matrices U and V such that, with lemma 6.5, we have

$$UQ_nV = D = \begin{bmatrix} |\Delta_n| & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix}, \quad \textit{and} \quad V^tQ_nV = \left[\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q_{n-1} & \\ 0 & & & \end{array}\right] \mod \Delta_n.$$

We have

$$\mathrm{Co}(V^tQ_nV) = \left[\begin{array}{c|ccc} \Delta_{n-1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{array}\right] \mod \Delta_n \tag{3}$$

where Δ_{n-1} is the determinant of Q_{n-1}. We now show that Δ_{n-1} is coprime to Δ_n.
Firstly, V being unimodular implies that $\det(V^tQ_nV) = 1$, and lemma 6.5 implies that the first row and column of V^tQ_nV are divisible by Δ_n. Expanding the cofactor matrix according to the first column we obtain $\Delta_n = \lambda_{1,1}\Delta_n \cdot \Delta_{n-1} + \sum_{i=2}^{n} \lambda_{i,1}\Delta_n \det(Q_{i,1})$ where $Q_{i,1}$ denotes the matrix extracted from Q_n for which that i^{th} row and first column have been removed and $\lambda_{i,1}$ denotes the coefficient of the i^{th} row in the first column. Now note that the coefficients of the first row of each $Q_{i,1}$ is divisible by Δ_n and so is $\det(Q_{i,1})$. Hence dividing the equation by Δ_n we obtain

$$1 = \lambda_{1,1}\Delta_{n-1} + \Delta_n \sum_{i=2}^{n} \mu_{i,1} \quad \text{for } \mu_{i,1} \in \mathbb{Z},$$

and this proves that $(\Delta_n, \Delta_{n-1}) = 1$. Next we have

$$\mathrm{Co}(V^tQ_nV) = \Delta_n(V^tQ_nV)^{-1} = (V^{-1})\Delta_n Q_n^{-1}(V^t)^{-1} = (V^{-1})\mathrm{Co}(Q_n)(V^t)^{-1}. \tag{4}$$

Let $X = (V^t)^{-1}Y$ for $Y \in \mathbb{Z}^n$, using 3 and 4, we obtain

$$X^t\mathrm{Co}(Q_n)X = Y^t\mathrm{Co}(V^tQ_nV)Y \equiv \Delta_{n-1}y_1^2 \pmod{\Delta_n},$$

proving the claim. □

7.2. **Prime estimates for the determinant of the completed form.**

We now provide an estimate for the number of primes taken by the determinant of our new form. For completeness, we present the full proof, following a similar approach to that in [Cast11]. The theorem is based on an effective version of the Chebotarev density's theorem, under GRH, due to Lagarias and Odlyzko [LO77]. The reader only interested in computational applications can safely read theorems 7.7 and 7.8 before skipping to the next section.
To prove the theorem, we first derive an upper bound for the discriminant of a multi-quadratic extension.

Let $p_1, \ldots, p_t$ be odd prime numbers. We define

$$p_i^* = \begin{cases} p_i & \text{if } p_i \equiv 1 \pmod 4, \\ -p_i & \text{if } p_i \equiv 3 \pmod 4, \end{cases} \tag{5}$$

such that $p_i^* \equiv +1 \pmod 4$ for all i, and

$$L = \mathbb{Q}(\sqrt{p_1^*}, \cdots, \sqrt{p_t^*}). \tag{6}$$

Proposition 7.3. *Let $p_1, \ldots, p_t$ be positive prime numbers. Denote by L the number field $\mathbb{Q}(\sqrt{p_1^*}, \cdots, \sqrt{p_t^*})$ as defined above, and let d_L be its discriminant. Then,*

$$|d_L| \leq \left(\prod_{i=1}^{t} p_i\right)^{2^{t-1}}.$$

Proof. The proof is merely computational, with a detailed version found in ([Cast11, Theorem 4.1.1]). □

We now recall the setting needed for Chebotarev density's theorem. Let K be a number field over $\mathbb{Q}$, and L be a normal extension of K with Galois group $G = \mathrm{Gal}(L/K)$. Let d_L denote the discriminant of L and n_L be the degree of the extension $[L : \mathbb{Q}]$. If $\mathfrak{l}$ is an unramified prime ideal of K in L, we denote by the Artin symbol $\left[\frac{L/K}{\mathfrak{l}}\right]$ the conjugacy class of the Frobenius automorphisms of L corresponding to prime ideals $\ell|\mathfrak{l}$ in L. For each conjugacy class C of G we define

$$\pi_C(x, L/K) = \#\left\{\mathfrak{l} \in K, \text{unramified in } L : \left[\frac{L/K}{\mathfrak{l}}\right] = C, N_{L/K}(\mathfrak{l}) \leq x\right\}.$$

Assuming GRH for the Dedekind Zeta function, we have the following effective version of the Chebotarev density's theorem due to Lagarias and Odlyzko [LO77].

Theorem 7.4 (**GRH**). *There exists an absolute effective constant c_1 such that, under GRH and $x > 2$, we have*

$$\left|\pi_C(x, L/K) - \frac{|C|}{|G|}\mathrm{Li}(x)\right| \leq c_1 \left(\frac{|C|}{|G|}x^{1/2}\log(|d_L|x^{n_L}) + \log(d_L)\right),$$

where $\mathrm{Li}(x) = \displaystyle\int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$.

At this stage, we require the following lemma to prove our main theorem.

Lemma 7.5. *Let $n = \prod_i^t p_i$ be a square free odd integer such that $p_i^* = \pm p_i \equiv 1 \pmod 4$ are defined as in 5 then for a prime ℓ and δ coprime to n,*

$$\ell \equiv \delta\alpha^2 \pmod n \iff \left(\frac{\delta}{p_i}\right) = \left(\frac{p_i^*}{\ell}\right). \tag{7}$$

Proof. Starting with $\ell \equiv \delta\alpha^2 \pmod n$, this is equivalent to saying

$$\ell \equiv \delta\alpha^2 \mod p_i \quad \forall i.$$

Since δ is invertible modulo n, this is equivalent to saying $\left(\frac{\ell\delta^{-1}}{p_i}\right) = +1$ obtaining

$$\left(\frac{\ell}{p_i^*}\right) = \left(\frac{\delta}{p_i}\right).$$

By our construction of $p_i^* \equiv 1 \mod 4$ and quadratic reciprocity, the result follows. □

We now give the main theorem on prime estimates taken by the determinant of the completed form.

Theorem 7.6 (**GRH**). *Let n be a square-free, odd integer. Denote by $\pi_\delta(x, n)$ the number of prime numbers $\ell \nmid n$ less than x for which there exists an integer α such that $\ell \equiv \delta\alpha^2 \pmod n$. Assuming GRH, we have*

$$\left|\pi_\delta(x, n) - \frac{1}{2^{\omega(n)}}\mathrm{Li}(x)\right| \leq c_1 \left(\frac{1}{2}x^{1/2}\log(nx) + 2^{\omega(n)-1}\log(n)\right),$$

where c_1 is given by theorem 7.4 and $\omega(n)$ denotes the number of distinct prime factors of n.

Proof. Let $n = \prod_{i=1}^t p_i$ and L be the number field given by:

$$L = \mathbb{Q}(\sqrt{p_1^*}, .., \sqrt{p_t^*}).$$

as in 6, and denote by d_L the discriminant of this field.
Let ℓ be a prime ideal of K, and in our case, we take $K = \mathbb{Q}$. For an unramified prime ℓ, this is equivalent to ℓ is different from the primes p_i for all i. Since L is a multi-quadratic extension, we observe that

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \prod_{i=1}^t \mathrm{Gal}(\mathbb{Q}(\sqrt{p_i^*})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^t.$$

This means there is a correspondence between the map that associates ℓ to the Frobenius element Frob_ℓ relative to $\mathrm{Gal}(L/\mathbb{Q})$ and the one that associates ℓ to the t-tuple of Frobenius elements restricted to the fields $\mathbb{Q}(\sqrt{p_i^*})$. In this case, these restrictions are precisely the maps associating ℓ to

the Artin symbol $\left(\frac{p_i^*}{\ell}\right)$ according to the value of p_i^*. The Artin symbol of Theorem 7.4 corresponds to the t-tuple of Jacobi symbols ([Jan73], page. 90).

We now apply Theorem 7.4 to our case by rewriting the conditions as:

$$\begin{aligned}\pi_C(x, L/\mathbb{Q}) &= \left\{ \ell \leq x : \ 1 \leq i \leq t, \ \left(\frac{p_i^*}{\ell}\right) = \left(\frac{\delta}{p_i}\right) \right\}. \\ &= \left\{ \ell \leq x : \ell \nmid n, \ \exists \alpha, \ \ell \equiv \delta\alpha^2 \pmod{n} \right\} \\ &= \pi_\delta(x, n),\end{aligned}$$

where the conjugacy class C in theorem 7.4 is taken to be $C(\ell) = \left(\left(\frac{\delta}{p_1}\right), \ldots, \left(\frac{\delta}{p_t}\right)\right)$which corresponds precisely to a specific choice of t-tuple of Jacobi symbols. Since L is Galois of degree $2^{\omega(n)}$, we have

$$\left| \pi_\delta(x, n) - \frac{1}{2^{\omega(n)}} \mathrm{Li}(x) \right| \leq c_1 \left(\frac{1}{2^{\omega(n)}} x^{1/2} \log(|d_L| x^{2^{\omega(n)}}) + 2^{\omega(n)-1} \log(n) \right).$$

Combining the latter inequality with proposition 7.3 yields the result. □

It turns out that, for application purposes, we need the primes satisfying the congruence condition to have n as a quadratic residue, i.e. $\left(\frac{n}{\ell}\right) = 1$. Accordingly the next theorem modifies the last result to suit this condition.

Theorem 7.7 (GRH). *Let n be a square-free, odd integer. Denote by $\pi_\delta(n)$ the number of prime numbers $\ell \nmid n$ less than n for which there exists an integer α such that $\ell \equiv \delta\alpha^2 \pmod{n}$ and $\left(\frac{n}{\ell}\right) = 1$. Assuming GRH,*

$$\begin{cases} \pi_\delta(n) = \frac{1}{2^{\omega(n)}} \mathrm{Li}(n) + O(n^{1/2} \log(n)) & \text{if } \ n \equiv 1 \pmod 4 \\ \pi_\delta(n) = \frac{1}{2^{\omega(n)+1}} \mathrm{Li}(n) + O(n^{1/2} \log(n)) & \text{if } \ n \equiv 3 \pmod 4 \end{cases}$$

if δ is a quadratic residue modulo n, and

$$\begin{cases} \pi_\delta(n) = \left(\frac{1}{2} - \frac{1}{2^{\omega(n)}}\right) \mathrm{Li}(n) + O(n^{1/2} \log(n)) & \text{if } \ n \equiv 1 \pmod 4 \\ \pi_\delta(n) = \left(\frac{1}{2} - \frac{1}{2^{\omega(n)+1}}\right) \mathrm{Li}(n) + O(n^{1/2} \log(n)) & \text{if } \ n \equiv 3 \pmod 4 \end{cases}$$

if δ is a quadratic non-residue mod n, where the implied constants are efficiently computable.

Proof. We will modify the proof of theorem 7.6 to account for the condition $\left(\frac{n}{\ell}\right) = 1$. Assume first that δ is a quadratic residue modulo n, which implies that ℓ is a quadratic residue as well. Using the reciprocity law of Jacobi symbol, and the fact that n is odd, we obtain $\left(\frac{n}{\ell}\right) = (-1)^{\frac{n-1}{2}\frac{\ell-1}{2}}$, for which the Legendre condition is automatic if $n \equiv 1 \mod 4$ and we obtain the desired result in that case from theorem 7.6. If $n \equiv 3 \mod 4$, then $\left(\frac{n}{\ell}\right) = \left(\frac{-1}{\ell}\right)$. In this case, we apply theorem 7.4 to the field $L = \mathbb{Q}(\sqrt{p_1^*}, .., \sqrt{p_t^*}, \sqrt{-1})$ with $x = n$ where $n = \prod p_i$ and p_i^* are as in 5; we thus obtain

$$\pi_\delta(n) = \frac{1}{2^{\omega(n)+1}} \mathrm{Li}(n) + O(n^{1/2} \log(n)),$$

where $[K : \mathbb{Q}] = \frac{1}{2^{\omega(n)+1}}$ and $\omega(n) \leq \sqrt{n}$.
If δ is a quadratic non-residue, the result follows immediately by looking at all primes ℓ satisfying $\left(\frac{n}{\ell}\right) = 1$ for which there are $\frac{1}{2}\mathrm{Li}(n) + O(n^{1/2} \log(n))$ of them, and excluding the primes in previous cases. □

Next, we consider the case where n is even.

Theorem 7.8 (GRH). *Let $n = 2p_1 \cdots p_t$ be a square-free integer. Denote by $\pi_\delta(n)$ the number of prime numbers $\ell \nmid n$ less than n for which there exists an integer α such that $\ell \equiv \delta\alpha^2 \pmod{n}$ and $\left(\frac{n}{\ell}\right) = 1$. Then*

$$\pi_\delta(n) = \frac{1}{2^{\omega(n)}} \mathrm{Li}(n) + O(n^{1/2} \log n)$$

if δ is a quadratic residue, and

$$\pi_\delta(n) = \left(\frac{1}{2} - \frac{1}{2^{\omega(n)}}\right) \mathrm{Li}(n) + O(n^{1/2} \log n)$$

if δ is a quadratic non-residue mod n, where the implied constants are efficiently computable.

Proof. Let $F = \mathbb{Q}(\sqrt{p_1^*}, \cdots, \sqrt{p_t^*})$ be as before, and define $L = F(\sqrt{n})$. Assuming δ is a quadratic residue mod n, notice that the conditions on ℓ, namely $\ell \equiv \delta\alpha^2 \pmod{n}$ and $\left(\frac{n}{\ell}\right) = 1$, are equivalent to the splitting of ℓ in L. Since $n \in F \iff n \equiv 1 \pmod 4$ this implies that $[L : \mathbb{Q}] = \frac{1}{2^{t+1}} = \frac{1}{2^{\omega(n)}}$. Hence, applying theorem 7.4 to L, by looking for primes splitting in L, yields the desired result. The case of δ being a quadratic non-residue is completely analogous to the previous theorem. □

The following lemma will be useful as it will allow us to control some conditions on local solvability to ensure a global solution for Q_4; it expresses the Hasse-Witt invariant of Q_5 as a Legendre symbol in terms of $\det Q_5$ and $\det Q_4$. This will be helpful in our applications as computing Legendre symbols is easier than computing the Hasse-Witt invariant of a quadratic form.

Proposition 7.9. *Let Q_4 be the quadratic form as defined in (1), and Q_5 be the completed form as in (2). Assume that the completed form Q_5 has an odd prime determinant ℓ. Then the Hasse-Witt invariant of Q_5 at ℓ satisfies*

$$\epsilon_\ell(Q_5) = \left(\frac{\det Q_4}{\ell}\right)$$

where $\left(\frac{\cdot}{\ell}\right)$ denotes the Legendre symbol modulo ℓ.

Proof. Let $X \in \mathbb{Z}^4$ be uniformly chosen, and let z be given as in Lemma 7.1 such that the completed form has a prime determinant ℓ. Let $u \in \mathbb{Z}^4$ and $v \in \mathbb{Z}$. We wish to put $Q_5(u, v)$ in a special orthogonal sum form, which will allow us to compute the Hasse-Witt invariant easily. To achieve this, note that

$$Q_5(u, v) = u^{\mathrm{T}} Q_4 u + 2v(X^t u) + zv^2,$$

and Q_4^{-1} exists since $\det Q_4^{-1} \neq 0$. Setting the change of variables $u' = u - vQ_4^{-1}X$ yields:

$$\begin{aligned} Q_5(u', v) &= \left(u - vQ_4^{-1}X\right)^t Q_4 \left(u - vQ_4^{-1}X\right) + 2vX^t \left(u - vQ_4^{-1}X\right) + zv^2 \\ &= u^t Q_4 u - 2vu^t X + v^2 X^t Q_4^{-1} X + 2vX^t u - 2v^2 X^t Q_4^{-1} X + zv^2 \\ &= u^t Q_4 u + \left(z - X^t Q_4^{-1} X\right) v^2 \\ &= Q_4(u) + Sv^2, \end{aligned}$$

where $S = z - X^t Q_4^{-1} X = \frac{\det(Q_4) z - X^t \operatorname{Co}(Q_4) X}{\det Q_4} = -\ell(\det Q_4)^{-1}$, using Lemma 7.1. Once Q_5 is the orthogonal sum of Q_4 and $[S]$, lemma 2.3 of ([Cas78],p: 58) yields

$$\epsilon_\ell(Q_5) = \epsilon_\ell(Q_4) \cdot \epsilon_\ell([S]) \cdot (\det Q_4, S)_\ell,$$

where $(\cdot, \cdot)_\ell$ denotes the Hilbert symbol. We immediately have $\epsilon_\ell([S]) = 1$, as it is an empty product, and the consideration of the coefficients of Q_4 and $\gcd(\det Q_4, \ell) = 1$ along with Proposition 5.8 implies that $\epsilon_\ell(Q_4) = 1$. Accordingly, $\epsilon_\ell(Q_5) = (\det Q_4, -\ell(\det Q_4)^{-1})_\ell$. Since $(a, bc)_\ell = (a, b)_\ell (a, c)_\ell$ and $\ell \nmid \det Q_4$, the result follows from proposition 5.8. □

We now present the completion algorithm. To ensure a global solution for the quadratic form Q_4 in (1), it is necessary for the signature (r, s) of Q_5 to satisfy $r, s \geq 2$ and for the Hasse-Witt invariant to satisfy $\epsilon_\ell(Q_5) = 1$.

Algorithm 2 COMPLETION(Q)

Input: An indefinite, non-degenerate quaternary form Q of square-free determinant.
Output: An indefinite, non-degenerate 5-dimensional quadratic form Q_5 of odd prime determinant ℓ with signature (r, s) where $r, s \geq 2$, and $\epsilon_\ell(Q_5) = 1$.

1: Compute the signature of Q.
2: **while** ℓ is not prime **or** $\left(\frac{\det Q}{\ell}\right) \neq 1$ **do**
3: Sample a random integral vector $X = (x_i)_{i=1}^4$ where $x_i \in [0, |\det Q|^4]$.
4: Compute $L = X^t \mathrm{Co}(Q) X$, setting $\ell \equiv L \pmod{\det Q}$ with $0 < \ell < \det Q$.
5: **if** $r = 1$ and $\det Q > 0$ **then**
6: Set $\ell = \ell - \det Q$.
7: **end if**
8: **if** $s = 1$ **then**
9: Set $\ell = \ell - \det Q$.
10: **end if**
11: **end while**
12: Set $z = \dfrac{L - \ell}{\det Q}$.
13: **return** $\begin{bmatrix} Q & X \\ X^t & z \end{bmatrix}$.

Theorem 7.10 (GRH). *Given an indefinite non-degenrate quaternary quadratic form Q of square-free determinant, algorithm 2 completes Q into an indefinite 5-dimensional quadratic form of odd prime determinant ℓ with signature (r, s) where $r, s \geq 2$ and Hasse-Witt invariant $\epsilon_\ell(Q_5) = 1$. Moreover, the algorithm runs in probabilistic polynomial time in* $\log(\det Q)$.

Proof. Starting with Theorem 7.2, for every $X \in \mathbb{Z}^4$ we have

$$X^t \mathrm{Co}(Q) X \equiv \delta \alpha^2 \pmod{\det Q},$$

for some α and δ coprime to $\det Q$. Hence, sampling a uniform integral vector X is equivalent to sampling a uniform $\ell \in (0, \det Q)$ such that $\ell \equiv \delta\alpha^2 \pmod{\det Q}$, since $\alpha = V^t X$, where V is one of the unimodular matrices arising from the Smith Normal Form (SNF) of Q.
For convenience, we set $n = \det Q$. From Theorems 7.7 and 7.8, as well as Proposition 7.9, the number of primes ℓ less than n that satisfy $\ell \equiv \delta\alpha^2 \pmod{n}$ for some α and $\epsilon_\ell(Q_5) = \left(\frac{n}{\ell}\right) = 1$ is

$$\pi_\delta(n) \geq \frac{1}{2^{\omega(n)+1}} \mathrm{Li}(n) - 2C_1 \sqrt{n} \log n,$$

for an effective constant c_1. For sufficiently large n, the main term dominates, and we obtain

$$\pi_\delta(n) \geq \frac{C}{2^{\omega(n)+1}} \frac{n}{\log n}$$

for some absolute constant C, using the fact that $\mathrm{Li}(n) \sim \frac{n}{\log n}$. Notice that ℓ is uniformly sampled from the set of quadratic residues (QR) or quadratic non-residues (QRN), depending on whether δ is a quadratic residue or a quadratic non-residue, respectively.

Using the fact that $|\mathrm{QR}| = \frac{\phi(n)}{2^{\omega(n)}}$ and the bounds $\varphi(n) \leq n$ and $\varphi(n) \geq \frac{cn}{\log\log n}$ for an absolute constant c, the probability that ℓ is a prime, in both cases (QR) and (QNR), is

$$\Pr[\ell \text{ is a prime}] \geq \frac{C}{\log n},$$

for an absolute computable constant C. This proves that ℓ is expected to be a prime satisfying the aforementioned conditions after $O(\log \det Q)$ trials. The fact that $r, s \geq 2$ in the signature of Q_5 follows from steps 5 and 8 and Lemma 7.1. □

Remark. As stated in a remark in [Ser81], it is possible to take $c_1 = 2$ in theorem 7.6. In practice, computations show that $\pi_\delta(n) > 0$ for $n \geq 3 \times 10^{12}$. Since we're reducing everything mod $\det(Q)$, the bounds in step 3 don't make much of a difference.

8. Solving the norm form equation

In this section, we give the algorithms for finding an isotropic vector to 1 and and the quaternion embedding problem. The trick is to extend the dimension of our form and then look at the intersection of suitable hyperbolic planes which is similar to the approach of [Castel12]. Since we're looking for a rational solution and the norm form is homogeneous, it suffices to solve

$$Q(x_1, x_2, x_3, x_4) = qx_1^2 + px_2^2 + pqx_3^2 - dx_4^2 = 0$$

over $\mathbb{Z}$ and then divide by x_4^2, where d is a square-free integer. Put precisely, we prove the following theorem.

Theorem 8.1 (GRH). *Given indefinite quaternary quadratic form $Q(x_1, x_2, x_3, x_4) = qx_1^2 + px_2^2 + pqx_3^2 - dx_4^2$ where p, q are primes, d is square-free, and p, q, d are coprime, algorithm 3 finds an isotropic vector $x \in \mathbb{Z}^4$ such that $Q(x) = 0$ and runs in probabilistic polynomial time in $\log p$, $\log q$ and $\log d$.*

Algorithm 3 SolveNormForm(Q)

Input: Indefinite quaternary form $Q = \text{diag}[q, p, pq, -d]$, where p and q are primes and d is square-free.

Output: A vector $x \in \mathbb{Z}^4$ such that $Q(x) = 0$.

1: Minimize Q to obtain a reduced form Q_f using Algorithm 1.
2: Complete Q_f to a 5-dimensional form Q_5 with a prime determinant using Algorithm 2.
3: Solve $X^t Q_5 X = 0$ using [Sim05].
4: Decompose $Q_5 = H \oplus Q_3$, where H is a hyperbolic plane and Q_3 is a ternary form.
5: Solve $X^t Q_3 X = 0$ using [Sim05].
6: Decompose $Q_3 = H' \oplus Q_1$, where H' is a hyperbolic plane and Q_1 is a unary form.
7: Deduce a solution x to the original form Q.
8: **return** x.

Proof. Step 1. In this step we apply algorithm 1 and obtain a reduced matrix $Q^{(2)} \in Sym^*(4, \mathbb{Z})$ and a unimodular matrix G_2 such that $pq \cdot Q^{(2)} = G_2^t Q G_2$.

Step 2. Since $\det Q^{(2)} = d$, which is square-free, we can use algorithm 2 to complete $Q^{(2)}$ to a 5-dimensional form Q_5 of prime determinant ℓ with $\epsilon_\ell(Q^{(2)}) = 1$ and signature $(r, s) \geq (2, 2)$ whose restriction to the subspace generated by the first 4 vectors of the basis is equal to $Q^{(2)}$.

Step 3. Since Q_5 is indefinite, it is isotropic by Theorem 5.11. Furthermore, as $\det(Q_5) = \ell$ is a prime, we apply Simon's algorithm [Sim05], which runs efficiently, to obtain an integral vector v such that $v^t Q_5 v = 0$. Without loss of generality, we assume that v is primitive.

Step 4. In this step, we outline the process of finding a hyperbolic plane containing v; the existence of such a plane is given by ([Ser73], p: 30, Proposition 3). First, complete v into a unimodular matrix G_3 having v as its first column (this can be done by using the Hermite normal form algorithm of a primitive vector). We then have $Q_5^{(1)} = G_3^t Q_5 G_3$ where the upper left-entry is zero. Let $w = [Q_5^{(1)}(1,2), Q_5^{(1)}(1,3), Q_5^{(1)}(1,4), Q_5^{(1)}(1,5)]$, and use HNF algorithm to find G_4 such that $w \cdot G_4 = (a, 0, 0, 0)$ where a is the gcd of the entries of w. Since a divides the first row and column

of $Q_5^{(1)}$ we have $a^2 | \det Q_5$ and since $\det Q_5 = \ell$ is a prime, we have $a = 1$. Setting $G_5 = \begin{bmatrix} 1 & 0 \\ 0 & G_4 \end{bmatrix}$, we obtain

$$Q_5^{(2)} = G_5^t Q_5^{(1)} G_5 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ 0 & b_3 & * & * & * & * \\ 0 & b_4 & * & * & * & * \\ 0 & b_5 & * & * & * & * \\ 0 & b_6 & * & * & * & * \end{bmatrix}.$$

Now let

$$G_6 = \begin{bmatrix} 1 & \lceil -\frac{b_2}{2} \rceil & -b_3 & -b_4 & -b_5 & -b_6 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

we then have

$$Q_5^{(3)} = G_6^t Q_5^{(2)} G_6 = \left[\begin{array}{cc:ccc} 0 & 1 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 \\ \hdashline 0 & 0 & & & \\ 0 & 0 & & Q_3 & \\ 0 & 0 & & & \end{array}\right], \tag{8}$$

where $Q_3 \in Sym(3, \mathbb{Z})$, α is either 0 or 1 and $\det Q_3 = -\det Q_5 = -\ell$. Once we have this form, its clear that $Q_5^{(3)} = H \perp Q_3$ where $\perp$ denotes the orthogonal sum.

Step 5. Since $Q_5^{(3)} = H \perp Q_3$, where H is a hyperbolic plane, the signature of Q_3 is $(r-1, s-1)$. The fact that $r, s \geq 2$ implies that Q_3 has both negative and positive eigenvalues, which further implies that Q_3 is isotropic over $\mathbb{R}$.

To ensure a global solution for Q_3, we must verify the existence of a solution at each completion $\mathbb{Q}_r$ for prime r. Using Theorems 5.13 and 5.14, it suffices to prove solvability over $\mathbb{Q}_\ell$. From ([Cas78], p. 58), the decomposition $Q_5^{(3)} = H \perp Q_3$ and the equivalence of Q_5 and $Q_5^{(3)}$ imply that

$$\epsilon_\ell(Q_5) = \epsilon_\ell(Q_5^{(3)}) = \epsilon_\ell(Q_3)(-1, -\ell)_\ell.$$

Since $\epsilon_\ell(Q_5) = 1$ by construction, and the fact that $(-1, -1)_\ell = 1$ for $\ell \neq 2$, Theorem 5.11 implies Q_3 is isotropic over $\mathbb{Q}_\ell$, and hence a global solution exists. We apply Simon's algorithm once again with $\det(Q_3) = -\ell$, the algorithm efficiently computes a primitive solution w satisfying $w^t Q_3 w = 0$.

Step 6. This step is exactly the same as step 4 applied to the form Q_3. Denote by B the change of basis matrix, which puts Q_3 in the form of 8. Set

$$G_7 = \left[\begin{array}{cc:ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & & & \\ 0 & 0 & & B & \\ 0 & 0 & & & \end{array}\right]$$

and $G_8 = G_3 G_5 G_6 G_7$. We thus obtain

$$G_8^t Q_5 G_8 = \left[\begin{array}{cc:cc:c} 0 & 1 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & \beta & 0 \\ \hdashline 0 & 0 & 0 & 0 & Q_1 \end{array}\right],$$

with $\alpha, \beta = 0$ or 1.

Step 7. Once we have the above form, note that the first and third column vectors of G_8 are solutions to the equation $X^t Q_5 X = 0$. Moreover, they are orthogonal with respect to Q_5. Consequently, every linear combination of these vectors is a solution as well.

We consider a combination where the last coefficient is zero and denote this vector by z, writing $z = \begin{bmatrix} u \\ 0 \end{bmatrix}$, where $u \in \mathbb{Z}^4$. Since Q_5 is the completion of $Q^{(2)}$, u is a non-trivial solution to the equation $X^t Q^{(2)} X = 0$. Therefore, $x = G_2 \cdot u$ is an isotropic vector for Q. This completes the proof. □

We now give the main theorem of embedding an imaginary quadratic field into $B_{p,\infty}$.

Theorem 8.2 (**GRH**). *Given an imaginary quadratic field K and a prime p that does not split in K, there exists an algorithm that finds an embedding $\iota : K \hookrightarrow B_{p,\infty}$ in probabilistic polynomial time in terms of $\log p$ and $\log |\mathrm{disc}(K)|$. Moreover, denoting by $\mathfrak{O}_K$ the ring of integers of K, the algorithm finds a maximal order $\mathcal{O} \subset B_{p,\infty}$ such that $\iota : \mathfrak{O}_K \hookrightarrow \mathcal{O}$ is an optimal embedding.*

Proof. Let ω be a Minkowski reduced generator (of trace 0 or 1) of the ring of integers $\mathcal{O}_K$ with minimal polynomial $x^2 - tx + n$ where t and n are the trace and norm of ω respectively. Finding an element $\alpha \in B_{p,\infty}$ with trace t and norm n is sufficient to deduce an embedding $K \hookrightarrow B_{p,\infty}$, which amounts to solving

$$(t/2)^2 + qx_1^2 + px_2^2 + pqx_3^2 = n, \tag{9}$$

for $x_1, x_2, x_3 \in \mathbb{Q}$. To do that, we'll restrict to zero-trace elements, and see that $2\alpha - t$ is a zero-trace quaternion with a square-free norm $d = |4n - t^2| = |\mathrm{disc}(K)|$. Once found we can translate back and find α; thus we're interested in solving the following equation over $\mathbb{Q}$

$$qx_1^2 + px_2^2 + pqx_3^2 - dx_4^2 = 0.$$

Once we have this form, we use algorithm 3 to find an isotropic vector $x \in \mathbb{Z}^4$, and by homogeneity of the equation we obtain a solution for 9.
To find the maximal order $\mathcal{O}$, we start by computing a special maximal order $\mathcal{O}_0$ (such as the special extremal order in [KLPT14], section 2.3). Let m be the smallest integer such that $m\alpha \in \mathcal{O}_0$, and define $I = \mathcal{O}_0 m\alpha + \mathcal{O}_0 m$. Notice that $I\alpha \subseteq I$, hence $\alpha \in \mathcal{O}_R(I) = \mathcal{O}$ which can be computed efficiently ([Ron92], Theorem 3.2). Since $\mathfrak{O}_K$ is maximal $\iota : \mathfrak{O}_K \hookrightarrow \mathcal{O}$ is an optimal embedding. Moreover, the running time is clearly ploynomial in $\log p$ and $\log d$ as it follows from the previous algorithms. □

Remark. Notice that even though $\mathrm{disc}(K)$ might be square-free up to multiplication by 4, this can be easily handled by looking for an element of norm $\mathrm{disc}(K)/4$ and then multiply by 2 due to the homogeneity of the norm form.

Remark. Theorem 8.2 improves upon the result ([LB20], Lemma 7.2) by removing the heuristic assumptions. Regarding computations, our algorithm appears to have lower time complexity compared to theirs.

9. Reducing $\mathfrak{O}$-EndRing to $\mathfrak{O}$-Vectorization

In this section we show that $\mathfrak{O}$-ENDRING reduces to the $\mathfrak{O}$-VECTORIZATION problem in probabilistic polynomial time, assuming the conductor of $\mathfrak{O}$ can be efficiently factorized. This improves upon the result of [Wes22] which required the full factorization of $\mathrm{disc}(\mathfrak{O})$. The main technical lemma is to produce some $\mathfrak{O}$-oriented elliptic curve that will be our starting point for the $\mathfrak{O}$-VECTORIZATION problem. We now define the quaternionic counterparts of horizontal, ascending, and descending isogenies. From now on, we will fix a quadratic field K containing our order $\mathfrak{O}$.

Definition 9.1. *Let $\mathcal{O}$ be a maximal order in an algebra $B \cong B_{p,\infty}$, and $\jmath : \mathfrak{O} \hookrightarrow \mathcal{O}$ a optimal embedding. Let I be a left $\mathcal{O}$-ideal of prime norm ℓ, and let $\mathfrak{O}' = \mathcal{O}_R(I) \cap (\jmath(\mathfrak{O}) \otimes \mathbb{Q})$. The ideal I is* $\jmath$-descending *if $\mathfrak{O}' \subsetneq \jmath(\mathfrak{O})$,* $\jmath$-horizontal *if $\mathfrak{O}' = \jmath(\mathfrak{O})$, and* $\jmath$-ascending *if $\mathfrak{O}' \supsetneq \jmath(\mathfrak{O})$.*

Remark. Its been shown in ([Wes22], Remark 5.) that its possible to find a $\mathfrak{O}$-descending left $\mathcal{O}$-ideal in polynomial time, which is due to the volcano structure of ℓ-oriented isogeny graph.

Lemma 9.2 (GRH). *Given the factorization of the conductor of $\mathfrak{O}$, one can efficiently find an $\mathfrak{O}$-oriented elliptic curve $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$, along with an ε-basis of $\mathrm{End}(E)$, in probabilistic polynomial time with respect to $\log(p)$ and $\log(|\mathrm{disc}(\mathcal{O})|)$.*

Proof. We first find an optimal embedding $\jmath : \mathfrak{O}_K \hookrightarrow \mathcal{O}'$ for some maximal order $\mathcal{O}' \subset B_{p,\infty}$ using Theorem 8.2 which we can do in polynomial time in $\log|\mathrm{disc}(K)|$. Following the approach of ([Wes22], Lemma 4), we let f be the conductor of $\mathfrak{O}$. For any prime power $\ell^k | f$ (with $(\ell, f/\ell^k) = 1$), let $\mathfrak{J}_\ell$ be a descending $\mathcal{O}'$-ideal of norm ℓ (can be done in polynomial time using our remark above), and $J_\ell \subseteq \mathfrak{J}_\ell$ be an ideal of norm ℓ^k such that $J_\ell \not\subseteq \ell\mathcal{O}'$. Notice that the isogeny induced by the each kernel ideal J_ℓ is cyclic since $J_\ell \not\subseteq \ell\mathcal{O}'$ (and the fact $E[I] \subseteq E[J]$ if and only if $J \subseteq I$). Additionally each φ_{J_ℓ} is a descending isogeny due to the volcano structure and the fact that the first step corresponding to $\mathfrak{J}_\ell$ is descending. Hence $J = \cap_{\ell | f} J_\ell$ is the kernel ideal of a descending isogeny of degree f and

$$\begin{aligned} \iota : \mathfrak{O} &\hookrightarrow \mathcal{O}_R(J) \\ f\omega_K &\mapsto c\omega \end{aligned}$$

is an optimal embedding. Defining $\mathcal{O} = \mathcal{O}_R(J)$, we can construct an elliptic curve E with with an ε-basis for $\mathrm{End}(E) \cong \mathcal{O}$ using lemma 3 of [Wes22]. The orientation ι is provided by the induced efficient representation of the endomorphism $\iota(c\omega_K) = \varepsilon(c\omega)$. □

Theorem 9.3 (GRH). *Given the factorization of the conductor of $\mathfrak{O}$, the* $\mathfrak{O}$-ENDRING *problem reduces to* $\mathfrak{O}$-VECTORIZATION *in probabilistic polynomial time in $\log p$ and the length of the instance.*

Proof. We follow a similar approach to that of [Wes21]. Let $(E, \iota) \in \mathrm{SS}_{\mathfrak{O}}(p)$ be an instance of $\mathfrak{O}$-ENDRING. Find an $\mathfrak{O}$-oriented elliptic curve $(E', \iota') \in \mathrm{SS}_{\mathfrak{O}}(p)$ along with an ε-basis of its endomorphism ring $\mathcal{O}' \cong \mathrm{End}(E')$ using lemma 9.2. Given an oracle that solves the $\mathfrak{O}$-VECTORIZATION we obtain an ideal $\mathfrak{a}$ such that $E = E'^{\mathfrak{a}}$. Accordingly, the kernel ideal $I = \mathcal{O}'\iota'(\mathfrak{a})$ of $\varphi_{\mathfrak{a}}$ is an $(\mathcal{O}', \mathcal{O})$-connecting ideal and $\mathcal{O}_R(I) \cong \mathcal{O}$ which can be computed efficiently using ([Ron92], Theorem 3.2). □

Theorem 9.4 (GRH). *Given the factorization of the conductor of $\mathfrak{O}$, $\mathfrak{O}$-EndRing* reduces to* $\mathfrak{O}$-UBER *in probabilistic polynomial time in $\log p$ and the length of the instance.*

Proof. The approach is exactly like our previous theorem and we can still solve the $\mathfrak{O}$-UBER instead of $\mathfrak{O}$-VECTORIZATION, without an orientation given, and find an ε-basis of $\mathrm{End}(E)$. Obtaining an ideal $\mathfrak{a}$, we can always choose our class representative to have norm coprime to the conductor of $\mathfrak{O}$ such that $\varphi_{\mathfrak{a}}$ is horizontal ([Onu21],proposition 3.5) which induces a primitive orientation on E, thereby solving $\mathfrak{O}$-ENDRING*. □

10. Equivalence of $\mathscr{H}$-Isogeny AND $\mathfrak{O}$-Embedding

In this section, we show the equivalence between the $\mathscr{H}$-ISOGENY and $\mathfrak{O}$-EMBEDDING problems, under GRH and the assumption that the conductor of $\mathfrak{O}$ can be efficiently factorized. Recently, Eriksen and Leroux showed how $\mathfrak{O}$-EMBEDDING can be utilized to compute isogenies of fixed degree between supersingular elliptic curves, which is a problem of utmost importance in isogeny-based cryptography. The current best algorithm that solves $\mathfrak{O}$-EMBEDDING, proposed by [EL24], has an exponential complexity of $O(|\mathrm{disc}(\mathfrak{O})|^{3/4}/p)$ and relies on several heuristic assumptions. We enhance this result by proposing a rigorous algorithm under GRH which runs in $\tilde{O}(|\mathrm{disc}(\mathfrak{O})|^{1/2})$.

6.1. **Reducing $\mathscr{H}$-ISOGENY to $\mathfrak{O}$-EMBEDDING.** In [EL24], the authors show that the $\mathfrak{O}$-VECTORIZATION problem reduces to $\mathfrak{O}$-ENDRING in polynomial time; we now show how to utilize that to solve the problem at hand.

Theorem 10.1. *Given an oracle that solves* $\mathfrak{O}$-EMBEDDING*, there exists an algorithm that solves* $\mathscr{H}$-ISOGENY *in probabilistic polynomial time in* $\log p$, $\log|\mathrm{disc}(\mathfrak{O})|$ *and the length of the instance of* $\mathfrak{O}$-EMBEDDING*.*

Proof. Given $\mathfrak{O}$-oriented and $\mathfrak{O}$-orientable elliptic curves (E,ι) and E' respectively with ε-basis of their endomorphism rings, we can find an orientation ι' on E' using an oracle for $\mathfrak{O}$-EMBEDDING (by composing ε with the quaternion embedding). Once found, we can solve the $\mathfrak{O}$-VECTORIZATION using ([EL24], Algorithm 4) obtaining an $\mathfrak{O}$-ideal $\mathfrak{a}$ such $E' \cong E^{\mathfrak{a}}$. For a class representative $\mathfrak{a}$ of norm prime to the conductor of $\mathfrak{O}$, $\varphi_{\mathfrak{a}} : E \to E'$ is a horizontal isogeny ([Onu21], proposition 3.5). □

6.2 **Reducing $\mathfrak{O}$-EMBEDDING to $\mathscr{H}$-ISOGENY.** We now show the reduction in the other direction, where we assume GRH and that the factorization of the conductor of $\mathfrak{O}$ is given.

Theorem 10.2 (**GRH**). *Given the factorization of the conductor of* $\mathfrak{O}$ *and an oracle that solves* $\mathscr{H}$-ISOGENY*, there exists an algorithm that solves* $\mathfrak{O}$-EMBEDDING *in probabilistic polynomial time in* $\log p$, $\log|\mathrm{disc}(\mathfrak{O})|$ *and the length of the instance of* $\mathscr{H}$-ISOGENY*.*

Proof. Let $\mathcal{O} \subset B_{p,\infty}$ be an $\mathfrak{O}$-orientable maximal order. Let E be an elliptic curve with an ε-basis of its endomorphism ring such that $\mathrm{End}(E) \cong \mathcal{O}$ ([Wes22], Lemma 3). We can then sample an $\mathfrak{O}$-oriented elliptic curve $(E',\iota') \in \mathrm{SS}_{\mathfrak{O}}(p)$ with an ε'-basis of its endomorphism ring $\mathrm{End}(E') \cong \mathcal{O}'$ using lemma 9.2. Solving $\mathscr{H}$-ISOGENY(E',E) we obtain a horizontal isogeny $\varphi : E' \to E$ with a ι'-horizontal kernel ideal I. Thus ι' is an optimal embedding for $\mathcal{O}_R(I)$ which can be computed efficiently using ([Ron92], Theorem 3.2) and $\mathcal{O}_R(I) = \alpha\mathcal{O}\alpha^{-1}$ for some $\alpha \in B_{p,\infty}^{\times}$ which can be computed efficiently in our case (see remark 6.10 of [KV10]). Hence, $\iota = \alpha^{-1}\iota'\alpha$ is an optimal embedding $\mathfrak{O} \hookrightarrow \mathcal{O}$. □

Remark. Alternatively one can compute $\varphi_*(\iota')$ which is a primitive orientation on E, and $\iota = \varepsilon \circ \varphi_*(\iota')$ is an optimal embedding.

We now give a rigorous algorithm, under GRH, to solve $\mathfrak{O}$-EMBEDDING.

Theorem 10.3 (**GRH**). *Given an order* $\mathfrak{O}$ *of an imaginary quadratic field* K *and an* $\mathfrak{O}$*-orientable maximal order* $\mathcal{O} \subset B_{p,\infty}$*, there exist an algorithm which solves* $\mathfrak{O}$-EMBEDDING$(\mathcal{O})$ *in probabilistic time* $\tilde{O}(|\mathrm{disc}(\mathfrak{O})|^{1/2})$.

Proof. We start by factoring the conductor f of $\mathfrak{O}$, which can be done in subexponential time in $\log f$ and hence in $\log|\mathrm{disc}(\mathfrak{O})|$. Given the factorization of f, we compute an $\mathfrak{O}$-oriented maximal order $(\mathcal{O}',\iota)$ in $B_{p,\infty}$ in polynomial time in $\log|\mathrm{disc}(\mathfrak{O})|$ using lemma 9.2. We can additionally compute an $\mathfrak{O}$-orientable elliptic curve E and $\mathfrak{O}$-oriented curve $(E',\jmath)$ with an ε, ε'-basis such that $\mathrm{End}(E) \cong \mathcal{O}$ and $\mathrm{End}(E') \cong \mathcal{O}'$ with $\jmath = \varepsilon' \circ \iota$ using lemma 3 of [Wes22].
Now let $(\ell_i)_i$ be a set of small primes splitting in K with $\mathfrak{l}_i$ prime ideals lying above ℓ_i. We can apply an exhaustive search to find a combination $\mathfrak{a} = \prod \mathfrak{l}_i^{e_i}$ such that $\mathfrak{a} \cdot E' \cong E$, which we can expect to find in time $O(\#\mathrm{SS}_{\mathfrak{O}}(p))$. Using proposition 2.1 of [DDF+21] we have that $\#\mathrm{SS}_{\mathfrak{O}}(p)$ is bounded above by $O(h(\mathfrak{O})) = O(|\mathrm{disc}(\mathfrak{O})|^{1/2}\log|\mathrm{disc}(\mathfrak{O})|)$. It remains to show that computing the action $\mathfrak{a} \cdot E'$ can be done in polynomial time. Given the orientation $\jmath : \mathfrak{O} \hookrightarrow \mathrm{End}(E')$ and the ε-basis of $\mathrm{End}(E)$, we can compute both the action and the target curve of $\mathfrak{a} \cdot E'$ in rigorous polynomial time, as established in [Wes22], Proposition 9. Consequently, we can verify whether $E'^{\mathfrak{a}} \cong E$ in polynomial time with respect to $\log p$, $\log|\mathrm{disc}(\mathfrak{O})|$, $\log N(\mathfrak{a})$, and the length of the ε-basis.
Once we determine the right ideal $\mathfrak{a}$, we can find an equivalent ideal with norm coprime to the conductor f, ensuring that $\varphi_{\mathfrak{a}} : E' \to E$ is a horizontal isogeny. Consequently, this provides a solution to the $\mathfrak{O}$-EMBEDDING$(\mathcal{O})$ via Theorem 10.2.

□

11. Future Work

One important ingredient used in our reductions is lemma 9.2 which samples an $\mathfrak{O}$-oriented elliptic curve together with an ε-basis of its endomorphism ring. The problem of factoring the conductor c of $\mathfrak{O}$ in our lemma, boils down to computing a descending isogeny of degree c. In particular, given an $\mathfrak{O}_K$-oriented elliptic curve (E, ι), where $\mathfrak{O}_K$ is the ring of integer of K, along with an ε-basis of its endomorphism ring, is it possible to efficiently compute an isogeny $\varphi : E \to E'$ where φ is descending of degree c and E' is some $(\mathbb{Z} + c\mathfrak{O}_K)$-oriented elliptic curve?
A solution to such a problem would then drop the factorization assumption on the conductor of $\mathfrak{O}$, and establish the equivalence between $\mathfrak{O}$-ENDRING and the $\mathfrak{O}$-VECTORIZATION problem along with the equivalence between $\mathscr{H}$-ISOGENY and $\mathfrak{O}$-EMBEDDING.

References

[ACD+23] Arpin, S., Clements, J., Dartois, P., Eriksen, J. K., Kutas, P., and Wesolowski, B. "Finding Orientations of Supersingular Elliptic Curves and Quaternion Orders." *arXiv preprint*, arXiv:2308.11539 (2023).

[BKV19] Beullens, Ward, Kleinjung, Thorsten, and Vercauteren, Frederik. *CSI-FiSh: Efficient Isogeny Based Signatures through Class Group Computations.* In Steven D. Galbraith and Shiho Moriai (Eds.), *Advances in Cryptology - ASIACRYPT 2019: 25th International Conference on the Theory and Application of Cryptology and Information Security*, Vol. 11921 of *Lecture Notes in Computer Science*, 227–247. Springer, 2019.

[Cast11] Castel, Pierre. *Un Algorithme de Résolution des Équations Quadratiques en Dimension 5 Sans Factorisation.* Ph.D. thesis, Laboratoire de Mathématiques Nicolas Oresme, 2011.

[Castel12] Castel, Pierre. "Solving Quadratic Equations in Dimension 5 or More Without Factoring." In *Tenth Algorithmic Number Theory Symposium*, 2013.

[Cas78] Cassels, J. W. S. *Rational Quadratic Forms.* 1978.

[CJS14] Childs, Andrew, Jao, David, and Soukharev, Vladimir. "Constructing Elliptic Curve Isogenies in Quantum Subexponential Time." *Journal of Mathematical Cryptology*, 8(1): 1–29, 2014.

[CK20] Colò, Leonardo, and Kohel, David. "Orienting Supersingular Isogeny Graphs." *Journal of Mathematical Cryptology*, 14(1): 414–437, 2020.

[CLG09] Charles, Denis X., Lauter, Kristin E., and Goren, Eyal Z. "Cryptographic Hash Functions from Expander Graphs." *Journal of Cryptology*, 22(1): 93–113, January 2009.

[CLM+18] Castryck, Wouter, Lange, Tanja, Martindale, Chloe, Panny, Lorenz, and Renes, Joost. *CSIDH: An Efficient Post-Quantum Commutative Group Action.* In Thomas Peyrin and Steven D. Galbraith (Eds.), *Advances in Cryptology - ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security*, Vol. 11274 of *Lecture Notes in Computer Science*, 395–427. Springer, 2018.

[Cost89] Iliopoulos, Costas S. "Worst-Case Complexity Bounds on Algorithms for Computing the Canonical Structure of Finite Abelian Groups and the Hermite and Smith Normal Forms of an Integer Matrix." *SIAM Journal of Computing*, 18(4): 658–669, 1989.

[CS21] Chenu, Mathilde, and Smith, Benjamin. "Higher-Degree Supersingular Group Actions." In *MathCrypt 2021 - Mathematical Cryptology*, 2021.

[DDF+21] De Feo, Luca, Delpech de Saint Guilhem, Cyprien, Fouotsa, Tako Boris, Kutas, Péter, Leroux, Antonin, Petit, Christophe, Silva, Javier, and Wesolowski, Benjamin. "Séta: Supersingular Encryption from Torsion Attacks." *ASIACRYPT*, 2021.

[EHL+18] Eisenträger, Kirsten, Hallgren, Sean, Lauter, Kristin, Morrison, Travis, and Petit, Christophe. "Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions." In Jesper Buus Nielsen and Vincent Rijmen (Eds.), *Advances in Cryptology – EUROCRYPT 2018*, 329–368. Springer International Publishing, 2018.

[EL24] Eriksen, Jonathan Komada, and Leroux, Antonin. "Computing Orientations from the Endomorphism Ring of Supersingular Curves and Applications." *Preprint.*

[GPS20] Galbraith, Steven D., Petit, Christophe, and Silva, Javier. "Identification Protocols and Signature Schemes Based on Supersingular Isogeny Problems." *Journal of Cryptology*, 33(1): 130–175, 2020.

[PW24] Page, Aurel, and Wesolowski, Benjamin. "The Supersingular Endomorphism Ring and One Endomorphism Problems Are Equivalent." *IACR Cryptology ePrint Archive*, 2023:1399, 2023.

[Jan73] Janusz, Gerald J. *Algebraic Number Fields.* Vol. 55 of *Pure and Applied Mathematics.* Academic Press, 1973.

[KLPT14] Kohel, David, Lauter, Kristin, Petit, Christophe, and Tignol, Jean-Pierre. "On the Quaternion l-Isogeny Path Problem." *LMS Journal of Computation and Mathematics*, 17(A): 418–432, 2014.

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

[LB20] Love, Jonathan, and Boneh, Dan. "Supersingular Curves with Small Noninteger Endomorphisms." *ANTS XIV: Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, *Open Book Series*, 4(1): 7–22, 2020.

[Onu21] Onuki, Hiroshi. "On Oriented Supersingular Elliptic Curves." *Finite Fields and Their Applications*, 69: 101777, 2021.

[Ron92] Rónyai, Lajos. "Algorithmic Properties of Maximal Orders in Simple Algebras over $\mathbb{Q}$." *Computational Complexity*, 2(3): 225–243, 1992.

[Sil86] Silverman, Joseph H. *The Arithmetic of Elliptic Curves.* Vol. 106 of *Graduate Texts in Mathematics.* Springer-Verlag, 1986.

[Sim05] Simon, Denis. "Quadratic Equations in Dimensions 4, 5, and More." *Preprint*, 2006. (See Watkins [2013] for a published review.)

[Ser81] Serre, Jean-Pierre. "Quelques Applications du Théorème de Densité de Chebotarev." *Publications Mathématiques de l'IHES*, 54: 123–201, 1981.

[Ser73] Serre, Jean-Pierre. *A Course in Arithmetic.* Vol. 7 of *Graduate Texts in Mathematics.* Springer-Verlag, 1973.

[DSim05] Simon, Denis. "Solving Quadratic Equations Using Reduced Unimodular Quadratic Forms." *Mathematics of Computation*, 74: 1531–1543, 2005.

[LO77] Lagarias, J. C., and Odlyzko, A. M. "Effective Versions of the Chebotarev Density Theorem." In *Algebraic Number Fields: L-Functions and Galois Properties* (Proc. Sympos., Univ. Durham, Durham, 1975), 409–464. Academic Press, 1977.

[Vel71] Vélu, J. "Isogénies entre Courbes Elliptiques." *Comptes Rendus de l'Académie des Sciences, Séries A-B*, 273: A238–A241, 1971.

[Voi21] Voight, John. *Quaternion Algebras.* Vol. 288 of *Graduate Texts in Mathematics.* Springer International Publishing, 2021.

[Wat13] Watkins, Mark. "Some Comments About Indefinite LLL." *Diophantine Methods, Lattices, and Arithmetic Theory of Quadratic Forms*, 587(233): 32, 2013.

[Wes21] Wesolowski, Benjamin. "The Supersingular Isogeny Path and Endomorphism Ring Problems Are Equivalent." In *FOCS 2021-62nd Annual IEEE Symposium on Foundations of Computer Science*, 2022.

[Wes22] Wesolowski, Benjamin. "Orientations and the Supersingular Endomorphism Ring Problem." *IACR Cryptology ePrint Archive*, 2021:1583, 2021.