On Algebraic Embedding for Unstructured Lattices

Madalina Bolboceanu[1], Zvika Brakerski[2], and Devika Sharma[2]

[1] Bitdefender, Romania
[2] Weizmann Institute of Science, Israel*

Abstract. Lattice-based cryptography, the study of cryptographic primitives whose security is based on the hardness of so-called lattice problems, has taken center stage in cryptographic research in recent years. It potentially offers favorable security features, even against quantum algorithms. One of the main obstacles for wide adoption of this type of cryptography is its unsatisfactory efficiency. To address this point, efficient lattice-based cryptography usually relies on the intractability of problems on lattices with additional algebraic structure (such as so-called ideal-lattices or module-lattices). It is an important open question to evaluate the hardness of such lattice problems, and their relation to the hardness of problems on unstructured lattices.

It is a known fact that an unstructured lattice, which is simply an additive discrete group in Euclidean space, can be cast as an ideal-lattice in some *order* of a number field (and thus, in a rather trivial sense, that ideals in orders are as general as unstructured lattices). However, it is not known whether this connection can be used to imply useful hardness results for structured lattices, or alternatively new algorithmic techniques for unstructured lattices.

In this work we establish a gradient of hardness for the Order-LWE problem (a generalization of the well known Ring-LWE problem), as it varies over orders in a number field. Furthermore, we show that, in every number field, there are certain orders such that the corresponding Order-LWE problem is at least as hard as the (unstructured) LWE problem. So in general one should not hope to solve (any) Order-LWE more efficiently than LWE. However, we show that this connection holds in orders that are very "skewed" and hence, perhaps, irrelevant for improving efficiency in cryptographic applications. We further improve the hardness result for Order-LWE, to include *all* ideal lattices, closing a gap left in prior work. This establishes a direct connection between problems on unstructured lattices and the structured problem of Order-LWE.

Keywords: LWE, Order-LWE, Lattice Problems, Number fields.

* Supported by the Israel Science Foundation (Grant No. 3426/21), and by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482).

1 Introduction

The Learning with Errors (LWE) problem, as defined by Regev [Reg05], is a convenient way to construct numerous cryptographic primitives such that their security is based on the hardness of solving worst-case lattice problems on integer lattices.[3] See [Pei16] for an exposition. However, there is a drawback in basing cryptographic primitives on LWE in practice. It induces relatively high computational complexity and large instance size, at least quadratically in security parameter; an LWE-based encryption scheme, for instance, has long keys and ciphertexts, along with high encryption complexity.

It was known since the introduction of the NTRU cryptosystems [HPS98] and more rigorously by the results in [LM06, PR06] that the efficiency of the lattice-based cryptosystems could be significantly improved by instead using lattices stemming from algebraic number theory. Popularly known as *ideal lattices*, these are additive discrete groups residing in number fields that, owing to the works of Minkowski, can be viewed as lattices in the Euclidean space as well[4]. This (Minkowski) embedding of the number field into the Euclidean space preserves the algebraic structure. Inspired by this view, in [SSTX09], and then in [LPR10, LPR13], the authors defined the first known algebraic number theoretic analogs of LWE: Polynomial-LWE (PLWE) and Ring-LWE (RLWE), respectively. Roughly, they replaced the abelian group $\mathbb{Z}_q^n$ appearing in LWE by abelian groups that have an additional ring structure. For PLWE, it is the ring of polynomials $\mathbb{Z}[x]/(f(x))$, and for RLWE, it is the ring of integers $\mathcal{O}_K$ in a number field K. We will explain the properties of these algebraic objects below when needed. Similar to Regev's original result, the authors showed that each of these problems, PLWE and RLWE, is as hard as solving worst-case lattice problems on (a certain subset[5] of) their respective *ideal* lattices. Moreover, the PLWE and RLWE problems collapse in a single one, in the case of a power-of-two cyclotomic field.

Naturally, fixing a field K, not all lattices can be expressed as ideals of the ring $\mathcal{O}_K$ considered in the RLWE problem defined over K. Therefore, (such) ideal lattices constitute a subset of the class of all lattices. Furthermore, the algebraic structure on these lattices makes ideal-lattice problems potentially easier to solve than their counterparts on general lattices. Indeed, recently it has been shown that on some parameter regimes, state of the art quantum algorithms for ideal lattices asymptotically significantly outperform the best known (classical or quantum) algorithms for general lattices [CGS, CDPR16, CDW17, DPW19, PHS19, BRL20, BLNRL22]. A more recent work, [PXWC21], proves that there

[3] We prefer to keep the discussion at a high level at this point and not specify the exact lattice problem. In this context, relevant problems include Discrete Gaussian Sampling (DGS), Shortest Independent Vectors Problem (SIVP) and Bounded Distance Decoding (BDD). See the preliminary section for definitions.

[4] See Section 2.3 for details.

[5] This subset is the set of invertible ideals of the polynomial ring considered in PLWE. However, this subset forms the full set of ideals for the ring considered in the RLWE problem.

are prime ideals (lattices) in the power-of-two cyclotomic fields that admit efficient classical SVP algorithms and it is further generalized by [BGP22].

On the other hand, it is known that unstructured integer lattices can be endowed with an algebraic structure by embedding them into a (fixed) number field K. See Section 1.1. Under this embedding, the image of an integer lattice is an ideal of a subring (order[6]) in K. But there is no efficient way, known to us, to decide if the set of all integer lattices maps to the subset of ideals captured by the existing hardness results of RLWE (and its variant Order-LWE, described below). Therefore, in spite of making unstructured integer lattices into ideal lattices in this way, one may still not be able to compare the hardness of lattice problems on the two sets. We provide a way out of this problem, in this work, by extending the hardness results to include *all* ideals in K, not just a proper subset.

Since the introduction of Ring-LWE, various algebraically structured variants of the LWE problem have been defined, each with their own worst-case to average-case reduction: Module-LWE [LS12], Middle-Product LWE [RSSS17], and Order-LWE [BBPS19]. The Order-LWE problem, which will be of interest in this work, is a generalization of the Ring-LWE problem, and is obtained by replacing the ring of integers in Ring-LWE by one of its full-rank subrings, i.e. an order.[7] Improving and extending the results from [RSW18], the authors in [PP19] proved that all the above mentioned variants are at least as hard as Ring-LWE (with some order-dependent penalty in the parameters). On the other hand, by merely forgetting the ring (or module) structure on these structured LWE problems, one obtains (multiple) LWE samples, thereby proving that all the algebraically structured LWE problems are not harder than the (unstructured) LWE.

In this paper, we prove that every number field has certain orders such that their corresponding Order-LWE problem is equivalent to the unstructured LWE problem. Therefore, in a sense, Order-LWE can be viewed as a generalization of Regev's LWE. The result emphasizes how devious certain algebraic structures can be, and that it would be naïve to assume that algebraic versions of unstructured problems are necessarily simpler. We describe our work in more detail now.

1.1 This Work: General Lattices as Ideals

To compare lattice problems on (unstructured) integer lattices with the algebraic LWE problems, one may make a lattice into an ideal lattice as follows. Given a number field K over $\mathbb{Q}$ of degree n, the elements in K can be considered as formal polynomials of degree at most $(n-1)$ with rational coefficients. This induces a correspondence between (rational) n-dimensional vectors and field elements

[6] See the preliminary section for a definition.

[7] The current authors, in their previous work [BBPS19], provided a detailed background and motivation for the Order-LWE problem, and invite the reader to refer to it, if needed.

known as the *coefficient embedding* (from the field K into $\mathbb{Q}^n \subseteq \mathbb{R}^n$). Once a number field K is chosen and fixed, this correspondence allows to present any (rational) lattice as an additive *subgroup* of K, but not necessarily as an ideal in the aforementioned ring-of-integers. However, it is known that any such (discrete) subgroup $\mathcal{L}$ that corresponds to a full-rank lattice L in $\mathbb{Q}^n$ constitutes an ideal in some *full-rank subring* of the ring of integers (See Section 2.3). Such subrings are known as orders, and the maximal order in which the group $\mathcal{L}$ is an ideal is called its ring of multipliers[8], denoted as $\mathcal{O}_{\mathcal{L}}$.

Previously, [BBPS19] showed that solving the Order-LWE problem is at least as hard as solving lattice problems on ideals of that order. We could therefore hope that the above embedding would imply that for any lattice (respectively distribution over lattices) there exists an order (respectively distribution over orders) for which solving Order-LWE is at least as hard as solving short vector problems on this lattice (or distribution). Alas, [BBPS19] only relates the hardness of Order-LWE with the hardness of a subset of ideal lattices in the order, namely the set of *invertible* ideals. We recall that an ideal in the ring is invertible if it has an inverse which is also a (possibly fractional) ideal in the ring. While all ideals of the ring of integers are invertible, this is not necessarily the case for ideals of orders. Although a naive sounding restriction, it left the infinite set of non-invertible ideals uncaptured by an important average-case problem. In particular, the lattice $\mathcal{L}$ is not necessarily invertible in its ring of multipliers and we are unaware of an efficient way of deciding that. Therefore, prior to this work, the above derivation could not be made.

In Section 3, we improve the existing hardness result for Order-LWE to show that this problem is at least as hard as solving lattice problems on all ideal lattices of the order, under a regularity condition on the Order-LWE modulus. The approximation factor obtained is identical to the one in [BBPS19]. The novelty of this improvement is our generalization of the so-called Cancellation Lemma that is at the heart of ideal lattice hardness results such as [LPR10, PRSD17, BBPS19].[9] We believe that this extended lemma is of interest beyond the LWE setup. Inspired by the techniques used in the proof of the generalized Cancellation Lemma, we also show an equivalence between two variants of Order-LWE that were defined in [BBPS19] (a *primal* and *dual* variant).

Lastly, in Section 3, we extend the Ring-LWE hardness result. The strengthened result now includes solving lattice problems (DGS) for lattices that are not necessarily ideals in the ring of integers, but rather ideals in orders whose index is coprime with the Ring-LWE modulus. This comes at a cost on the approximation factor (for DGS) if the lattice is not an $\mathcal{O}_K$-ideal, which is directly related

[8] Some works, for e.g. [PP19], also call such ring as *coefficient ring*.

[9] The Cancellation Lemma provides a way to map a lattice point into its coefficient vector with respect to a basis of another, fixed and perhaps denser, lattice. The coefficient vector will constitute the LWE secret s. In order to preserve the algebraic structure, this needs to be done via multiplication by a field element. Prior results used the invertibility of the ideal to show that this is possible. See more details in Section 1.2.

to the conductor of the ring of multipliers of the lattice.[10] This result generalizes the Order-LWE to Ring-LWE reduction proved in [BBPS19]. See Section 3 for full statements and proofs.

In Section 4, we show that every number field has chain(s) of orders beginning from $\mathcal{O}_K$ such that their corresponding Order-LWE problems become (not necessarily strictly) harder. We prove that this gradient of hardness terminates at special 'skewed' orders. That is, we show that Order-LWE corresponding to these orders is equivalent to the unstructured LWE problem. More precisely, we show that for "reasonable" Gaussian noise, from say D_α, the noise in the (skewed) Order-LWE sample drowns the last $n-1$ coordinates of the Order-LWE instance. Thus only one coefficient survives, which is distributed like a (standard) LWE sample with a related noise parameter. We call such orders α-drowning and describe a recipe to construct them.

The α-drowning property makes the algebraic structure of the order unuseful for building efficient cryptographic schemes based on the hardness of the corresponding Order-LWE problem. However, in our opinion, since the Order-LWE problem covers the whole spectrum of the LWE problem, structured and unstructured, it is a useful problem to consider. Indeed, the chain of reductions described in Section 4, that starts with the Ring-LWE problem, and ends in the LWE problem disguised as an Order-LWE avatar, proposes several intermediate orders such that their corresponding Order-LWE problems are potentially harder than the Ring-LWE problem. This interpolation of Order-LWE between structured and unstructured problems, reminiscent of Module-LWE, sheds light on the interplay of the algebraic structure and the hardness of the LWE problem. It may perhaps in the future help yield an order that may be hard enough and algebraic enough for constructing a secure and yet efficient cryptographic scheme.

1.2 Technical Overview

In this section, we provide a somewhat more technical outline of our results in Sections 3, 4. To keep this overview simple, we present all the algebraic results for the case of a power-of-two cyclotomic field, i.e., $K = \mathbb{Q}[x]/(x^n+1)$, where n is a power of two. We will specify when the result holds in more generality, and invite the enthusiastic reader to seek details in the relevant section.

We begin with a brief description of the LWE problem: a secret vector $\vec{s}$ is sampled from $\mathbb{Z}_q^n$, for a modulus q, and an adversary gets access to an oracle that outputs pairs of the form $(\vec{a}, b = \frac{1}{q}\langle \vec{a}, \vec{s} \rangle + e \mod \mathbb{Z})$, for a uniform $\vec{a} \in \mathbb{Z}_q^n$ and a small 'noise' $e \in \mathbb{R}/\mathbb{Z}$, that typically follows a Gaussian distribution. The goal of the adversary is to distinguish this oracle from the one that outputs $(\vec{a}, b)$, with b uniform over $\mathbb{R}/\mathbb{Z}$. The Ring-LWE setup is described in a more algebraic environment, where the sample spaces are algebraic objects isomorphic to $\mathbb{Z}_q^n$.

[10] The conductor of an order is the maximal ideal which is shared between the order and the ring of integers. Properties of the conductor are often used to relate the order and the ring of integers.

It is well-known that the *ring of integers* of K is the ring of integer polynomials $\mathcal{O}_K := \mathbb{Z}[x]/(x^n+1)$.[11] Observe that $\mathcal{O}_K$ is a $\mathbb{Z}$-module of rank n, much like an integer lattice. Further, one can also define the dual $\mathcal{O}_K^\vee$ of $\mathcal{O}_K$, exactly like the dual of a lattice.[12] There is a canonical way of embedding the field K into $\mathbb{R}^n$ (more accurately, a copy of $\mathbb{R}^n$ that lies inside $\mathbb{C}^n$), with the so-called Minkowski embedding of K. (See Section 2.3.) The $\mathbb{R}$-vector space generated by the image of K is denoted by $K_\mathbb{R}$. Under this embedding one can view ideals in K as lattices in $K_\mathbb{R}$. For a modulus q, the Ring-LWE problem is defined as follows: for a secret polynomial $s \in \frac{\mathcal{O}_K^\vee}{q\mathcal{O}_K^\vee}$, the adversary gets access to an oracle that outputs pairs of the form

$$(a, \frac{1}{q} \cdot a \cdot s + e) \in \frac{\mathcal{O}_K}{q\mathcal{O}_K} \times \frac{K_\mathbb{R}}{\mathcal{O}_K^\vee},$$

where a is drawn uniformly over $\frac{\mathcal{O}_K}{q\mathcal{O}_K}$, and e is drawn from a small Gaussian over $K_\mathbb{R}$. Intuitively, in this case, e can be thought of as a polynomial with very small coefficients. The goal of the adversary here is to distinguish between the output of this oracle and the output of an oracle that gives uniform pairs over the same domain.

The (*primal* variant of the) Order-LWE problem is a genuine generalization of the Ring-LWE problem. For, once $\mathcal{O}_K$ is replaced by an *order* $\mathcal{O}$, a full rank subring of $\mathcal{O}_K$, the problem is defined exactly as above and denoted as $\mathcal{O}$-LWE. Some simple examples of orders to keep in mind could be the ring $\mathcal{O}_K$ itself, or $\mathbb{Z} + d\mathcal{O}_K$, for any integer d, or the ring of integer polynomials modulo f, i.e., $\mathbb{Z}[x]/(f)$, if the field in discussion is defined as $K = \mathbb{Q}[x]/(f)$. Moreover, in this problem the integer modulus q can be replaced by an $\mathcal{O}$ ideal modulus $\mathcal{Q}$, but for the sake of simplicity, we will present here our results with an integer modulus. A *dual* variant of this problem is defined by swapping the domains of the secret s and of the a.[13]

Extended hardness result of Order-LWE (Section 3). The authors in [BBPS19] defined the Order-LWE problem and showed that it is at least as hard as solving lattice problems on the 'invertible' ideal (lattices) of the order. When specialized to the order $\mathcal{O}_K$, this is the hardness result as proved in [LPR10, PRSD17], where there is no mention of invertibility of the ideal lattices considered, since all $\mathcal{O}_K$-ideals are invertible. This distinction only arises when working with ideals of a proper order $\mathcal{O}$ ($\neq \mathcal{O}_K$).[14]As the proof of the Order-LWE hardness result given in [BBPS19] followed the exact same blueprint

[11] See [Was83, Thm 2.6] for a proof.

[12] Formally this is done by replacing the Euclidean inner product by its number-theoretic analog, the bilinear Trace map $Tr : K \times K \to \mathbb{Q}$. The trace coincides with the Hermitian inner product on the Minkowski space $K_\mathbb{R}$, as $\langle \sigma(x), \overline{\sigma(y)} \rangle := Tr(xy)$, where $\sigma(x)$, $\sigma(y)$ are the images of x, y in $K_\mathbb{R}$, respectively, via the Minkowski embedding σ and $\overline{\sigma(y)}$ is the complex conjugate of $\sigma(y)$.

[13] This *primal-dual* terminology, from [BBPS19], differs from the one of [RSW18, PP19], as there, only the domain of s differs: in the primal variant, it is $\mathcal{O}_K/q\mathcal{O}_K$, whereas in the dual variant, it is $\mathcal{O}_K^\vee/q\mathcal{O}_K^\vee$.

[14] There exist ideals in orders that are not invertible. See [Conb, Example 3.5].

described for the hardness of Ring-LWE [PRSD17], it needed, using additionally discrete Gaussian samples (DGS) over an $\mathcal{O}$-ideal $\mathcal{I}$, to convert Bounded Distance Decoding (BDD) samples on its dual to LWE samples. This conversion required compatible isomorphisms, namely $\mathcal{I}/q\mathcal{I} \simeq \mathcal{O}/q\mathcal{O}$, respectively its dual counterpart, that send the discrete Gaussian sample to the first coordinate of an $\mathcal{O}$-LWE sample, respectively the BDD secret to the $\mathcal{O}$-LWE secret (See Section 2.5 for more details on the blueprint of the Order-LWE hardness proof.). Prior to this work, these maps were constructed using the so-called Cancellation Lemma, which necessarily required the $\mathcal{O}$-ideal involved in DGS to be invertible. That was the only reason the $\mathcal{O}$-LWE hardness result needed to be restricted to this sub-class of invertible $\mathcal{O}$-ideals. In this work, we show that the conclusion of the Cancellation Lemma holds even if the ideal is not invertible, as long as a regularity condition is satisfied (i.e., the LWE modulus q is coprime to the index $[\mathcal{O}_K : \mathcal{O}]$[15]). To prove this lemma, we use a generalization of ideal factorization, known as Jordan-Hölder filtration. To the best of our knowledge, the Jordan-Hölder filtration has not been used in this context prior to this work. Using this filtration, we observe that $\mathcal{I}$, a non-invertible $\mathcal{O}$-ideal, can be viewed as a sublattice of an invertible $\mathcal{O}$-ideal $\mathfrak{p}$. Therefore, we can apply the (usual) Cancellation Lemma to $\mathfrak{p}$ and map the elements of $\mathcal{I}$ to the elements of $\mathfrak{p}$ using the inclusion relation. The latter (inclusion) relation is of course not an isomorphism of $\mathcal{O}$-modules, a condition that is necessary to maintain the algebraic structure. However, in the context of Order-LWE reduction, what we need is an $\mathcal{O}$-isomorphism between the modulo q versions of these ideals (where q is the LWE modulus). Indeed, we show that under the aforementioned regularity condition, the inclusion relation between the ideals implies an $\mathcal{O}$-isomorphism modulo q.[16] This suffices to allow the proof to go through.

Additionally, under the coprimality condition, $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$,[17] we show that the dual and the primal $\mathcal{O}$-LWE problems from [BBPS19] are equivalent, thereby further strengthening the hardness result for the dual Order-LWE problem, as well. Previously, [BBPS19] showed the equivalence between these problems, but requiring a more involved condition on the order in use and not on the LWE modulus.

In the same section, we also extend the Ring-LWE hardness result. We described the details of the strengthened results previously. See the introduction above.

[15] This holds more generally, for arbitrary ideal moduli $\mathcal{Q}$ coprime with $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$, but for the simplicity of exposition, we treat the LWE modulus as integer.

[16] A concurrent work, namely an updated version of [PP19], showed that Cancellation Lemma also holds for non-invertible ideals, but requires instead *invertibility modulo an ideal* $\mathcal{Q}$. In our case, the ideal modulus $\mathcal{Q}$ is coprime with $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$, therefore, in particular, coprime with the conductor as well. This implies, by their remark, that all fractional ideals are invertible modulo $\mathcal{Q}$. Therefore, [PP19, Lem. 2.14] provides an isomorphism $\mathcal{O}/\mathcal{Q}\mathcal{O} \simeq \mathcal{I}/\mathcal{Q}\mathcal{I}$, for all fractional ideals $\mathcal{I}$ and thus, an alternative proof to ours.

[17] This holds more generally, for arbitrary ideal moduli coprime with the conductor of the order.

Equivalence of Order-LWE and (unstructured) LWE (Section 4). Let K be the power-of-two cyclotomic and let p be a prime such that $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n$, where $\mathfrak{p}_i$'s are prime ideals in $\mathcal{O}_K$. Then, the following chain of orders exists

$$\mathcal{O}_K \supseteq \mathbb{Z} + \mathfrak{p}_1 \supseteq \mathbb{Z} + \mathfrak{p}_1\mathfrak{p}_2 \supseteq \ldots \supseteq \mathbb{Z} + \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_{n-1} \supseteq \mathbb{Z} + p\mathcal{O}_K.$$

As proven in [PP19, Thm. 4.7], for orders $\mathcal{O}' \subseteq \mathcal{O}$, there is an error preserving reduction from $\mathcal{O}$-LWE to $\mathcal{O}'$-LWE, as long as the modulus q is coprime to $[\mathcal{O} : \mathcal{O}']$. Therefore we can derive the following chain of error preserving reductions, as long as $(p, q) = 1$,

$$\mathcal{O}_K\text{-LWE} \to (\mathbb{Z}+\mathfrak{p}_1)\text{-LWE} \to \ldots \to (\mathbb{Z}+\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_{n-1})\text{-LWE} \to (\mathbb{Z}+p\mathcal{O}_K)\text{-LWE}.$$

Observe that the $\mathbb{Z}$-basis of the order $\mathbb{Z}+p\mathcal{O}_K$ is given by the set $\{1, p\zeta, \ldots, p\zeta^{n-1}\}$, as $\mathcal{O}_K = \mathbb{Z}[\zeta]$, for a primitive root of unity ζ. For a large p, one of these basis elements is much shorter than the rest. It is in this sense that we call this order 'skewed'. We show that this skewed order is α-drowning. That is, for $p \geq \frac{1}{\alpha}$, the error sampled from a spherical Gaussian distribution D_α over $K_\mathbb{R}$ drowns the last $n-1$ coordinates of $K_\mathbb{R}/\mathcal{O}^\vee$ and it is only the coefficient corresponding to the basis element 1 that survives in this Order-LWE sample and looks like the second coordinate of an LWE sample. This implies that the Order-LWE problem corresponding to $\mathbb{Z} + p\mathcal{O}_K$ is equivalent to the unstructured LWE problem. To get an intuitive idea of the proof that $\mathbb{Z} + p\mathcal{O}_K$ is α-drowning, observe that the set $(\mathbb{Z} + p\mathcal{O}_K)^\vee$, in this special case, looks like [18]

$$(\mathbb{Z} + p\zeta\mathbb{Z} + \ldots + p\zeta^{n-1}\mathbb{Z})^\vee = \frac{1}{n}\mathbb{Z} + \frac{1}{pn}\zeta\mathbb{Z} + \ldots + \frac{1}{pn}\zeta^{n-1}\mathbb{Z}.$$

Consider a noise term e drawn from a spherical (in $K_\mathbb{R}$) Gaussian D_α.[19] Its coefficients in this basis are Gaussian with a diagonal covariance matrix whose diagonal entries are $(\alpha^2 n, \alpha^2 p^2 n, \ldots, \alpha^2 p^2 n)$. In the specified choice of parameters, $\alpha p\sqrt{n}$ is greater than the smoothing parameter of $\mathbb{Z}$, thereby proving that the last $n-1$ coefficients of e are indistinguishable from uniform elements in $\mathbb{R}/\mathbb{Z}$. Whereas the first coefficient looks like a part of a LWE-sample with error from $D_{\alpha\sqrt{n}}$. In Section 4, we describe α-drowning orders in any number field K and show that Order-LWE corresponding to them is equivalent to LWE. The proof, in this general case, requires a more involved analysis since the covariance matrix of the Gaussian over the basis of the order is not in general diagonal which makes it much more difficult to analyze.

Related work A concurrent work, [JL22], showed a variant of Cancellation Lemma, by presenting the isomorphisms $\mathcal{I}/q\mathcal{I} \simeq \mathcal{O}/q\mathcal{O}$, for all ideals $\mathcal{I}$ of the order $\mathcal{O}$ and for an integer modulus q satisfying $(q, [\mathcal{O}_K : \mathcal{O}]) = 1$. The map is described as multiplication by some special element t, obtained by a randomized

[18] See [Conc, Thm 3.7] for a proof.

[19] The Order-LWE problem is often considered with noise sampled from an elliptical Gaussian, or even a family of elliptical Gaussians, but we can simply consider the largest spherical Gaussian that is contained in that distribution.

algorithm and is classically efficient, without knowing the factorization of q. Using the [PRSD17] framework as we do, they develop the hardness result of decision Order-LWE for all ideals $\mathcal{I}$ in the given order, under the coprimality condition. We present the hardness result using any $\mathcal{O}$ ideal modulus $\mathcal{Q}$, as long as it is coprime with $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$, although the maps we describe for its proof are quantum efficient with the knowledge of factorization of the modulus.

2 Preliminaries

We describe the well-known results and some standard notations. Given a distribution D, when writing $x \leftarrow D$, we mean an element x sampled from this distribution. Given a set X, we denote by $U(X)$, the uniform distribution over this set. For a vector $\mathbf{x} \in \mathbb{C}^n$, we let $\|\mathbf{x}\|$ be its Euclidean norm, defined as $\|\mathbf{x}\| = (\sum_i |x_i|^2)^{1/2}$ and its infinity norm, defined as $\|\mathbf{x}\|_\infty = \max_i |x_i|$.

2.1 The Space H

To be able to speak about the geometric properties of a number field K of degree $n = s_1 + 2s_2$, (defined below), we embed it into the following space,

$$H = \{\mathbf{x} \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} | x_{s_1+s_2+j} = \overline{x_{s_1+j}}, \text{ for any } 1 \leq j \leq s_2\} \subseteq \mathbb{C}^n.$$

H is an n-dimensional vector space over $\mathbb{R}$, equipped with the inner product induced on $\mathbb{C}^n$, and hence isomorphic to (a copy of) $\mathbb{R}^n$. This is the space $K_\mathbb{R}$, up to an isomorphism, mentioned in the introduction.

2.2 Lattices

Given a finite dimensional vector space V over $\mathbb{R}$ (e.g. $\mathbb{R}^n$ or $H \subseteq \mathbb{C}^n$) a $\mathbb{Z}$-lattice $\mathcal{L}$ is an (discrete) additive group generated by a set (basis) $B = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_k\} \subseteq V$ of elements that are linearly independent over $\mathbb{R}$. In other words,

$$\mathcal{L} := \{\sum_{i=1}^{k} a_i \mathbf{v}_i : a_i \in \mathbb{Z}, \mathbf{v}_i \in B\}.$$

The integer k is called the rank of the lattice $\mathcal{L}$ and when $k = \dim_\mathbb{R} V$, the lattice $\mathcal{L}$ is said to be of full rank. Under the inner product on V (e.g. the Euclidean product for $\mathbb{R}^n$ or the Hermitian product for H), the dual lattice $\mathcal{L}^*$, is of the same rank as $\mathcal{L}$, and is defined as

$$\mathcal{L}^* := \{\mathbf{v} \in V : \langle \mathbf{v}, \mathbf{x} \rangle \in \mathbb{Z} \ \ \forall \mathbf{x} \in \mathcal{L}\}.$$

Let $B(0, r)$ denote the closed Euclidean ball of radius r around 0. The successive minimum of the lattice $\mathcal{L}$ is defined, for $1 \leq i \leq n$, as

$$\lambda_i(\mathcal{L}) := \inf\{r > 0 : \text{rank}_\mathbb{Z}(\text{span}_\mathbb{Z}(\mathcal{L} \cap B(0, r))) \geq i\}.$$

Lemma 2.1 ([Ban93]). $1 \leq \lambda_1(\mathcal{L}) \cdot \lambda_n(\mathcal{L}^*) \leq n$.

Gaussians and Smoothing Parameter Let V be a real inner product space of dimension n with an orthonormal basis $(\mathbf{v}_i)_{1\leq i\leq n}$. We identify an element $x \in V$ in a unique way with a vector $\mathbf{x} \in \mathbb{R}^n$, of its coordinates with respect to this basis. Recall that a symmetric matrix $\Sigma \in M_n(\mathbb{R})$ is said to be *positive (semi)definite* if $\mathbf{x}^T\Sigma\mathbf{x} > 0$ (or $\mathbf{x}^T\Sigma\mathbf{x} \geq 0$, resp.), for any non-zero $\mathbf{x} \in \mathbb{R}^n$. This property puts a partial order on the set of symmetric matrices: $\Sigma_1 \geq \Sigma_2$ if $\mathbf{x}^T(\Sigma_1 - \Sigma_2)\mathbf{x} \geq 0$, for any nonzero $\mathbf{x} \in \mathbb{R}^n$.

Definition 2.2. *For a positive definite matrix $\Sigma \in M_n(\mathbb{R})$ and a mean vector $\boldsymbol{c} \in \mathbb{R}^n$, define the Gaussian function $\rho_{\boldsymbol{c},\sqrt{\Sigma}} : V \to (0,1]$ as $\rho_{\boldsymbol{c},\sqrt{\Sigma}}(x) = e^{-\pi(\boldsymbol{x}-\boldsymbol{c})^T\Sigma^{-1}(\boldsymbol{x}-\boldsymbol{c})}$. We denote by $D_{\boldsymbol{c},\sqrt{\Sigma}}$, the normalized continuous Gaussian distribution over V corresponding to $\rho_{\boldsymbol{c},\sqrt{\Sigma}}$.*

When $\mathbf{c}$ is the zero vector, it is dropped from the subscript. When $\Sigma = \mathrm{diag}(r_i^2)$, for some $\mathbf{r} = (r_1, \ldots, r_n) \in \mathbb{R}^n$, the distribution is called an elliptical Gaussian and is denoted as $\rho_{\mathbf{r}}$ and $D_{\mathbf{r}}$. If all r_i's equal r, it is called a spherical Gaussians and is written as ρ_r and D_r. We will frequently use the fact that if x follows a Gaussian distribution of covariance matrix Σ, i.e., $x \leftarrow D_{\sqrt{\Sigma}}$, then $Tx \leftarrow D_{\sqrt{T\Sigma T^*}}$, where T is a linear transformation on V, and T^* is the conjugate-transpose operator. When working with elliptical Gaussians over H, we restrict our parameters to belong to the set $G = \{\mathbf{r} \in (\mathbb{R}^+)^n |\ \mathbf{r}_{s_1+s_2+j} = \mathbf{r}_{s_1+j},\ 1 \leq j \leq s_2\}$. We say for $\mathbf{r}_1$ and $\mathbf{r}_2$ in G that $\mathbf{r}_1 \geq \mathbf{r}_2$ if $\mathbf{r}_{1i} \geq \mathbf{r}_{2i}$, for all $1 \leq i \leq n$, and by $\mathbf{r} \geq r$ we mean that $\mathbf{r}_i \geq r$, for all $1 \leq i \leq n$.

Given a lattice $\mathcal{L}$ in V and a real positive definite matrix Σ, we define the discrete Gaussian distribution $D_{\mathcal{L},\sqrt{\Sigma}}$ on $\mathcal{L}$ as $D_{\mathcal{L},\sqrt{\Sigma}}(x) := \frac{\rho_{\sqrt{\Sigma}}(x)}{\rho_{\sqrt{\Sigma}}(\mathcal{L})}$, for any $x \in \mathcal{L}$.

Definition 2.3 (Smoothing Condition [Pei10, Def 2.2, 2.3]). *For a lattice $\mathcal{L}$ in V of rank n and a parameter $\varepsilon > 0$, we define the smoothing parameter of $\mathcal{L}$, $\eta_\varepsilon(\mathcal{L})$, as the smallest $r > 0$ such that $\rho_{1/r}(\mathcal{L}^* \setminus \{0\}) \leq \varepsilon$. For a positive definite matrix Σ, we say that $\sqrt{\Sigma} \geq \eta_\varepsilon(\mathcal{L})$ if $\rho_{\sqrt{\Sigma^{-1}}}(\mathcal{L}^* \setminus \{0\}) \leq \varepsilon$.*

We drop ε from the subscript of $\eta_\varepsilon(\mathcal{L})$ when it is an unspecified negligible function in n.

Lattice problems Let $\mathcal{L}$ be a full-rank lattice in a n dimensional real space V. We state the following standard lattice problems:

Definition 2.4 (Shortest Independent Vector Problem). *For an approximation factor $\gamma = \gamma(n) \geq 1$ and a family of rank-n lattices $\mathfrak{L}$, the $\mathfrak{L}$-$\mathtt{SIVP}_\gamma$ problem is: given a lattice $\mathcal{L} \in \mathfrak{L}$, output n linearly independent lattice vectors of norm at most $\gamma \cdot \lambda_n(\mathcal{L})$.*

Definition 2.5 (Discrete Gaussian Sampling). *For a family of rank-n lattices, $\mathfrak{L}$, and a function $\gamma : \mathfrak{L} \to G = \{\boldsymbol{r} \in (\mathbb{R}^+)^n |\ \boldsymbol{r}_{s_1+s_2+j} = \boldsymbol{r}_{s_1+j},\ 1 \leq j \leq s_2\}$, where $n = s_1 + 2s_2$, the $\mathfrak{L}$-$\mathtt{DGS}_\gamma$ problem is: given a lattice $\mathcal{L} \in \mathfrak{L}$ and $\boldsymbol{r} \geq \gamma(\mathcal{L})$, output a sample $x \in \mathcal{L}$ which follows a distribution statistically indistinguishable from $D_{\mathcal{L},\boldsymbol{r}}$.*

Definition 2.6 (Bounded Distance Decoding). *For a family of rank-n lattices $\mathfrak{L}$ and a function $\delta : \mathfrak{L} \to \mathbb{R}^+$, the $\mathfrak{L}$-$\mathtt{BDD}_\delta$ problem is: given a lattice $\mathcal{L} \in \mathfrak{L}$, a distance bound $d \leq \delta(\mathcal{L})$ and a coset $e + \mathcal{L}$, where $\|e\| \leq d$, find e.*

Definition 2.7 (Gaussian Decoding Problem [PRSD17]). *For a rank-n lattice $\mathcal{L} \subset H$ and a Gaussian parameter $g > 0$, the $\mathcal{L}$-$\mathtt{GDP}_\gamma$ problem is: given as input a coset $e + \mathcal{L}$, where $\boldsymbol{e} \in H$ is drawn from D_g, output $\boldsymbol{e}$.*

We recall here the reduction from SIVP to DGS from [Reg09].

Lemma 2.8 ([Reg09, Lem 3.17]). *For $\varepsilon = \varepsilon(n) \leq \frac{1}{10}$ and $\gamma \geq \sqrt{2}\eta_\varepsilon(\mathcal{L})$, there is a reduction from $\mathcal{L} - \mathtt{SIVP}_{2\sqrt{n}/\lambda_n(\mathcal{L})\cdot\gamma}$ to $\mathcal{L} - \mathtt{DGS}_\gamma$.*

2.3 Lattices in number fields: Orders and Ideals

A *number field* $K := \mathbb{Q}(\theta)$ of degree n is a $\mathbb{Q}$-vector space obtained by attaching a root θ of a monic, irreducible polynomial $f(x)$ of degree n. It is well-known that each such K has exactly n field embeddings $\sigma_i : K \to \mathbb{C}$, that map θ to each complex root of the minimal polynomial f. Embeddings whose image lie in $\mathbb{R}$ are called *real embeddings*, otherwise they are called *complex embeddings*. It is via these (s_1 real and $2s_2$ complex) embeddings that K is embedded into the space H, defined in Section 2.1. This is known as the Minkowski embedding, $\sigma : K \hookrightarrow H$. The $\mathbb{R}$-vector space generated by $\sigma(K)$ in H is called the Minkowski space $K_\mathbb{R}$. Given a geometric norm $\|\cdot\|$ on H, such as the Euclidean or infinity norm, we can define a norm on field elements by identifying them with their Minkowski embeddings, i.e. $\|x\| = \|\sigma(x)\|$, for any $x \in K$. By a lattice in K, we mean the image in $K_\mathbb{R}$, of a finitely generated $\mathbb{Z}$-module in K. The most extensively studied lattice in K is its ring of integers

$$\mathcal{O}_K := \{\beta \in K : \exists \ \text{(monic)}\ g(x) \in \mathbb{Z}[x] \text{ such that } g(\beta) = 0\}.$$

This ring is a full-rank lattice in K, i.e., $rank_\mathbb{Z}\ \mathcal{O}_K = n$. If $\mathcal{O}_K$ happens to coincide with $\mathbb{Z}[\theta]$, we say K is monogenic. A subring $\mathcal{O}$ of $\mathcal{O}_K$ satisfying $rank_\mathbb{Z}\ \mathcal{O} = n$ is said to be an *Order*. In other words, an order $\mathcal{O}$ equals $\mathbb{Z}g_1 \oplus \ldots \oplus \mathbb{Z}g_n$, for some basis $\{g_1, g_2, \ldots, g_n\} \subseteq \mathcal{O}$ of $K/\mathbb{Q}$. The set of all orders is a partial ordered set with respect to set containment and has $\mathcal{O}_K$ as the unique maximal element. We provide the proof of the next result in A.3.

Lemma 2.9. *Let $\mathcal{O}$ be an order in K. Then, $\mathcal{O}$ has a $\mathbb{Z}$-basis containing* 1.

An (integral) *ideal* $\mathcal{I}$ in $\mathcal{O}$ is an additive subgroup that is closed under scalar multiplication by $\mathcal{O}$, i.e. $x \cdot a \in \mathcal{I}$ for every $x \in \mathcal{O}$ and $a \in \mathcal{I}$. Every ideal is a $\mathbb{Z}$-module of rank n. Further, ideals in K can be thought of as integers in $\mathbb{Z}$, since they can be added, multiplied and (sometimes) divided. We invite the reader to refer to A.4 for a full exposition on ideals in K. A *fractional ideal* $\mathcal{I} \subset K$ of $\mathcal{O}$ is an ideal such that $d\mathcal{I} \subset \mathcal{O}$ for some $d \in \mathcal{O}$. A fractional ideal $\mathcal{I}$ is *invertible* if there exists a fractional ideal $\mathcal{J}$ such that $\mathcal{I} \cdot \mathcal{J} = \mathcal{O}$. If there exists such a $\mathcal{J}$, then it is unique and equal to $(\mathcal{O} : \mathcal{I}) = \{x \in K |\ x\mathcal{I} \subseteq \mathcal{O}\}$, and is denoted by

$\mathcal{I}^{-1}$. In general, an ideal in an order may not be invertible. See [Conb, Example 3.5]. However, in the special case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order, *every* fractional ideal is invertible. Integral ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{O}$ are *coprime*, if $\mathcal{I} + \mathcal{J} = \mathcal{O}$ and therefore we also have, $\mathcal{I}\mathcal{J} = \mathcal{I} \cap \mathcal{J}$ and $(\mathcal{I} \cap \mathcal{J})\mathcal{L} = \mathcal{I}\mathcal{L} \cap \mathcal{J}\mathcal{L}$, for any ideal $\mathcal{L}$. For the sake of this work, we assume that orders and ideals in K are described in terms of their $\mathbb{Z}$-bases.

The following lemma, known as the Cancellation Lemma, plays a crucial role in the hardness result for algebraic LWE's. Note that it uses the invertibility of the ideal $\mathcal{I}$.

Lemma 2.10 ([BBPS19, Thm 2.35]). *Let $\mathcal{I}$ and $\mathcal{J}$ be integral ideals of an order $\mathcal{O}$ and $\mathcal{M}$ a fractional ideal. Assume that $\mathcal{I}$ is an invertible ideal. Then, given the associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of $\mathcal{J}$, and an element $t \in \mathcal{I} \setminus \bigcup_{i=1}^{r} \mathcal{I}\mathfrak{p}_i$, the multiplication by t map θ_t, $\theta_t(x) = t \cdot x$, induces the following isomorphism of $\mathcal{O}$-modules*

$$\frac{\mathcal{M}}{\mathcal{J}\mathcal{M}} \xrightarrow{\sim} \frac{\mathcal{I}\mathcal{M}}{\mathcal{I}\mathcal{J}\mathcal{M}}.$$

This map can be efficiently inverted using $\mathcal{I}$, $\mathcal{J}$, $\mathcal{M}$ and t can be found using $\mathcal{I}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$.

Remark 2.11. The above result is proved in [BBPS19, Thm. 2.35] under a condition weaker than demanding that $\mathcal{I}$ be an invertible $\mathcal{O}$-ideal. The proof only requires the tuple $(t, \mathcal{I}, \mathcal{J}, \mathcal{M})$ to satisfy $t\mathcal{M} + \mathcal{I}\mathcal{J}\mathcal{M} = \mathcal{I}\mathcal{M}$.

In the improved hardness result in Section 3.1, we will deal with the scenario of non-invertible ideals. To circumvent this issue in some cases, we use the following result, which shows that under a coprimality condition, the inclusion induces an isomorphism. For general cases, where the coprimality condition does not hold, we give another recipe. See Section 3.1 for details.

Lemma 2.12 ([PP19, Lem. 2.15]). *Let $\mathcal{L}' \subseteq \mathcal{L}$ be two lattices in an order $\mathcal{O}$ in a number field K and $\mathcal{Q}$ an $\mathcal{O}$ ideal modulus such that it is coprime with $(\mathcal{L}' : \mathcal{L}) = \{x \in K : x\mathcal{L} \subseteq \mathcal{L}'\}$. Then the natural inclusion $\mathcal{L}' \subseteq \mathcal{L}$ induces the bijections*

$$f : \frac{\mathcal{L}'}{\mathcal{Q}\mathcal{L}'} \xhookrightarrow{\sim} \frac{\mathcal{L}}{\mathcal{Q}\mathcal{L}} \quad f(x) = x + \mathcal{Q}\mathcal{L}, \quad f^\vee : \frac{\mathcal{L}^\vee}{\mathcal{Q}\mathcal{L}^\vee} \xhookrightarrow{\sim} \frac{\mathcal{L}'^\vee}{\mathcal{Q}\mathcal{L}'^\vee} \quad f^\vee(x) = x + \mathcal{Q}\mathcal{L}'^\vee.$$

Moreover, this map is efficiently computable and invertible given a basis of $\mathcal{L}'$ relative to a basis of $\mathcal{L}$.

Notice that the result above holds also for ideal moduli being coprime with the (principal $\mathcal{O}$ ideal generated by the) index $[\mathcal{L} : \mathcal{L}']$, since this condition implies the coprimality with the set $(\mathcal{L}' : \mathcal{L})$, as $[\mathcal{L} : \mathcal{L}']\mathcal{O} \subseteq (\mathcal{L}' : \mathcal{L})$. We denote by $\xhookrightarrow{\sim}$ the isomorphism induced by the inclusion considered.

Duality For an element $a \in K$, the trace $Tr(a)$ is the sum $\sum_{i=1}^{n} \sigma_i(a)$, of images of a under all the embeddings of K. In other words, it is the sum of all coordinates of $\sigma(a)$.

Definition 2.13. *The dual of the lattice $\mathcal{L}$ is defined as*

$$\mathcal{L}^\vee = \{x \in K |\ Tr(x \cdot \mathcal{L}) \subseteq \mathbb{Z}\}.$$

The space $H \subseteq \mathbb{C}^n$ inherits the usual Hermitian inner product from $\mathbb{C}^n$. Therefore, for x, $y \in K$, the trace $Tr(xy) = \sum_{i=1}^{n} \sigma_i(xy) = \sum_{i=1}^{n} \sigma_i(x)\sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle$. This implies that $\sigma(\mathcal{L}^\vee) = \overline{\sigma(\mathcal{L})^*}$.

Embedding lattices into number fields We describe the (inverse of the) well-known coefficient embedding. Let $\vec{\theta} = (1, \theta, \theta^2, \ldots, \theta^{n-1})$. Let

$$L = \mathbb{Z}\vec{a}_1 + \mathbb{Z}\vec{a}_2 + \cdots + \mathbb{Z}\vec{a}_n \subseteq \mathbb{Z}^n,$$

be an integer lattice generated by n linearly independent elements $\vec{a}_1, \ldots, \vec{a}_n \in \mathbb{Z}^n$, with $\vec{a}_i = (a_{1i}, a_{2i}, \ldots a_{ni})^t$. In Section 3, we will deal with a special class of integer lattices, known as *p-ary integer lattices*, i.e., integer lattices L that satisfy $p\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$. Embed $\vec{a}_i$ in K as $a_i = \langle \vec{a}_i, \vec{\theta} \rangle = a_{1i} + a_{2i}\theta + \ldots + a_{ni}\theta^{n-1}$. It follows from the definition of the Trace function on K that a_i's are $\mathbb{Z}$-linearly independent and hence form an n-dimensional lattice in K. Denote by

$$\mathcal{L} = \mathbb{Z}a_1 + \mathbb{Z}a_2 + \cdots \mathbb{Z}a_n \subseteq \mathbb{Z}[\theta],$$

the embedding of L in K via this coefficient embedding. Define the Minkowski embedding; $\sigma : K \longrightarrow \mathbb{C}^n$ as $\sigma(a) = (\sigma_1(a), \sigma_2(a) \ldots \sigma_n(a))$, where σ_i's are the field embeddings defined earlier. Let $V_f = (\sigma_i(\theta^{j-1}))_{1 \le i,j \le n}$ denote the Vandermonde matrix corresponding to f. Then, the coefficient and the Minkowski embedding are related as follows: for any $a \in K$, the image $\sigma(a) = V_f \cdot \mathrm{coef}(a)$, where $\mathrm{coef}(a) \in \mathbb{Q}^n$ is made of the coefficients of a with respect to the power basis $\vec{\theta}$. In other words, the image of $\mathcal{L}$, under the Minkowski map, equals the image of L, under the $\mathbb{C}$-linear transformation defined by V_f: $\sigma(\mathcal{L}) = V_f \cdot L$. We would like to clarify that we consider $\sigma(\mathcal{L})$ as a lattice in $K_{\mathbb{R}}$ and hence a lattice in $\mathbb{R}^n$.

Let $s_n(V_f) \le \ldots \le s_1(V_f)$ be the singular values of V_f. Recall that the spectral norm of V_f is given by the maximum singular value, $s_1(V_f)$, whereas the spectral norm of V_f^{-1} is given by the inverse of the smallest singular value, $s_n(V_f)$. The following result describes how the embedding distorts the Euclidean norm and volume. A proof is included in A.5.

Lemma 2.14. *Let $\mathcal{L}$ be the image of L in K, under the coefficient embedding, with respect to $\vec{\theta}$. Then,*

(i) $s_n(V_f) \cdot \lambda_1(L) \le \lambda_1(\mathcal{L}) \le s_1(V_f) \cdot \lambda_1(L)$.
(ii) $\mathcal{L}$-DGS$_\alpha$ *is equivalent to* L-DGS$_{\alpha \cdot \sqrt{(V_f^* V_f)^{-1}}}$.

The Ring of Multipliers For any lattice $\mathcal{L}$ in a number field K, we define a *multiplier* of $\mathcal{L}$ as an element $x \in K$ such that $x\mathcal{L} \subseteq \mathcal{L}$. It turns out that the set of these multipliers has a ring structure, and moreover, forms an order in the field K. For more details, see [Neu99, Chapter 1, Sect.12].

Definition 2.15. *For a lattice $\mathcal{L} \subset K$, we define its ring of multipliers as*

$$\mathcal{O}_{\mathcal{L}} = \{x \in K |\ x\mathcal{L} \subseteq \mathcal{L}\}.$$

Both $\mathcal{L}$ and $\mathcal{L}^\vee$ are ideals of $\mathcal{O}_{\mathcal{L}}$. In fact, $\mathcal{O}_{\mathcal{L}}$ is the largest such order. In particular, if the lattice $\mathcal{L}$ is an order itself, then it is its own ring of multipliers. An interesting and important characterisation of $\mathcal{O}_{\mathcal{L}}$ is that $\mathcal{O}_{\mathcal{L}}^\vee = \mathcal{L}\mathcal{L}^\vee$. (See [Conb, Rem 4.2].) The following result describes an order that is contained in $\mathcal{O}_{\mathcal{L}}$. See A.6 for a proof.

Lemma 2.16. *Let $\mathcal{O}$ be an order in K and let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Then, the set $\mathbb{Z} + \mathcal{I}$, contained in $\mathcal{O}$, is an order in K. Further, given an additive subgroup $\mathcal{L} \subseteq \mathcal{O}$, it is an ideal of the order $\mathbb{Z} + m\mathcal{O}$, where m is the exponent of the (additive) quotient group $\mathcal{O}/\mathcal{L}$.*

Remark 2.17. When L is a p-ary integer lattice, i.e., $p\mathbb{Z}^n \subseteq L \subseteq \mathbb{Z}^n$, the embedded lattice $\mathcal{L} \subseteq K$ satisfies $p\mathcal{O}_K \subseteq \mathcal{L} \subseteq \mathcal{O}_K$. It is straightforward to check that $\mathcal{L}$ is closed under scalar multiplication by elements of $\mathbb{Z} + p\mathcal{O}_K$, which is an order, by Lemma 2.16.

The Conductor Ideal The non-maximality of an order $\mathcal{O}$ is reflected in a special ideal of $\mathcal{O}$ called the conductor ideal. We describe how this ideal is also closely related to the invertibility and unique factorization of $\mathcal{O}$-ideals.

Definition 2.18. *The* conductor *of an order $\mathcal{O}$ is defined to be the ideal*

$$\mathcal{C}_{\mathcal{O}} = (\mathcal{O} : \mathcal{O}_K) := \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}.$$

It is the maximal $\mathcal{O}_K$-ideal contained in $\mathcal{O}$.

There is a distinction between $\mathcal{O}$-ideals, based on invertibility. This distinction did not exist when dealing with $\mathcal{O}_K$-ideals, since all $\mathcal{O}_K$-ideals are invertible. But the picture is not all that bad.

Theorem 2.19. *[Conb, Th. 3.8, Cor. 3.11] The nonzero $\mathcal{O}$-ideals coprime to $\mathcal{C}_{\mathcal{O}}$ are invertible and also have unique factorization into prime ideals over $\mathcal{O}$. Further, they are in a multiplicative bijection with the set of nonzero $\mathcal{O}_K$-ideals coprime to $\mathcal{C}_{\mathcal{O}}$, via the maps $\mathcal{I} \mapsto \mathcal{I}\mathcal{O}_K$ and $\mathcal{J} \mapsto \mathcal{J} \cap \mathcal{O}$.*

Jordan-Hölder filtrations Jordan-Hölder filtrations may be considered as the analog of unique decomposition into prime ideals for $\mathcal{O}$-ideals, when $\mathcal{O}$ is a non-maximal order. Let $m = [\mathcal{O}_K : \mathcal{O}]$ be the index of $\mathcal{O}$ in $\mathcal{O}_K$. As $m\mathcal{O}_K$ is an $\mathcal{O}_K$-ideal contained in $\mathcal{O}$, we have $\mathcal{C}_{\mathcal{O}} | m\mathcal{O}_K$. Recall that, given two $\mathcal{O}$-ideals $\mathcal{I}$,

$\mathcal{J}$, we say that $\mathcal{I}$ divides $\mathcal{J}$, i.e. $\mathcal{I}|\mathcal{J}$, if there exists an $\mathcal{O}$-ideal $\mathcal{L}$ such that $\mathcal{J} = \mathcal{I}\mathcal{L}$. Define, for an ideal $\mathcal{I}$ of a ring R, $Spec_R(\mathcal{I})$ to be the set of prime ideals in R that contain $\mathcal{I}$. This set coincides with the set of associated primes of $\mathcal{I}$, defined in A.4.

Theorem 2.20 ([Cond, Thm 8.9]). *Let $\mathcal{O}$ be an order. Then for any integral ideal $\mathcal{I}$ there is a descending chain of ideals*

$$\mathcal{O} = \mathcal{I}_0 \supset \mathcal{I}_1 \supset \ldots \supset \mathcal{I}_l = \mathcal{I}, \tag{2.3.1}$$

where each quotient $\mathcal{I}_i/\mathcal{I}_{i+1}$ is a simple $\mathcal{O}$-module, i.e. for any $0 \leq i \leq l-1$, $\mathcal{I}_i/\mathcal{I}_{i+1} \sim \mathcal{O}/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$ of $\mathcal{O}$. These primes are the primes of $\mathcal{O}$ that contain $\mathcal{I}$ and their number is independent on the choice of the series. Furthermore, $[\mathcal{O} : \mathcal{I}] = \prod_{i=0}^{l-1} [\mathcal{O} : \mathfrak{p}_i]$.

Definition 2.21. *A finite chain for an $\mathcal{O}$-ideal $\mathcal{I}$ as in Theorem 2.20 is called a Jordan-Hölder filtration of $\mathcal{I}$.*

Lemma 2.22. *Let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Then, there exists an invertible ideal $\mathfrak{q}$ such that $\mathcal{I} \subseteq \mathfrak{q} \subseteq \mathcal{O}$ and $Spec_{\mathbb{Z}}([\mathfrak{q} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$, where $[\mathfrak{q} : \mathcal{I}]$ denotes the index of $\mathcal{I}$ in $\mathfrak{q}$. Further, given $\mathbb{Z}$ bases for $\mathcal{I}$, $\mathcal{O}$, $\mathcal{O}_K$, a $\mathbb{Z}$-basis for such a $\mathfrak{q}$ can be computed quantumly efficient.*

See A.8 for a detailed proof.

2.4 The LWE problem

Let n and q be positive integers.

Definition 2.23 (LWE distribution). *For $\vec{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ and an error distribution ψ over $\mathbb{R}/\mathbb{Z}$, define a sample of the distribution $A_{\vec{s},\psi}$ by generating $\vec{a} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$, $e \leftarrow \psi$ and outputting the pair $(\vec{a}, \frac{1}{q} \cdot \langle \vec{a}, \vec{s} \rangle + e \mod \mathbb{Z})$.*

Definition 2.24 (LWE, Average-Case Decision problem). *Let $q = q(n)$ be an integer and Υ a family of error distributions over $\mathbb{R}/\mathbb{Z}$. The average case decision LWE problem, denoted as $\mathrm{LWE}_{n,q,\psi}$ requires to distinguish independent samples from the distribution $A_{\vec{s},\psi}$, where $\vec{s} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$ and $\psi \leftarrow \Upsilon$, and the same number of samples from the uniform distribution over $(\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{R}/\mathbb{Z}$.*

Definition 2.25 (LWE, Average-Case Search problem). *Let $q = q(n)$ be an integer and Υ a family of error distributions over $\mathbb{R}/\mathbb{Z}$. The search LWE problem, denoted as search $\mathrm{LWE}_{q,\varphi}$, requires, given samples from the distribution $A_{\vec{s},\varphi}$, where $\vec{s} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$ and $\varphi \leftarrow \Upsilon$, find $\vec{s}$.*

2.5 The Order LWE problem

There is a line of work in studying algebraic versions of LWE: Ring-LWE [LPR10], Polynomial-LWE [SSTX09], Order-LWE [BBPS19] and $\mathcal{L}$-LWE [PP19]. In this paper we will focus on Order-LWE. To set it up, let K be a number field, $\mathcal{O}$ an order in it, $\mathcal{Q}$ an integral ideal of $\mathcal{O}$ and $u \in (\mathcal{O} : \mathcal{Q}) := \{x \in K |\ x\mathcal{Q} \subseteq \mathcal{O}\}$. For fractional $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$, we denote by $\mathcal{I}_{\mathcal{J}} := \mathcal{I}/\mathcal{J}\mathcal{I}$. We let $\mathbb{T}_{\mathcal{O}^\vee} := K_{\mathbb{R}}/\mathcal{O}^\vee$. The Order-LWE distribution and problem are stated as follows:

Definition 2.26 ($\mathcal{O}$-LWE distribution). *For $s \in \mathcal{O}_{\mathcal{Q}}^\vee$ and an error distribution ψ over $\mathbb{T}_{\mathcal{O}^\vee}$, define a sample of the distribution $\mathcal{O}_{s,\psi,u}$ over $\mathcal{O}_{\mathcal{Q}} \times \mathbb{T}_{\mathcal{O}^\vee}$ by generating $a \leftarrow U(\mathcal{O}_{\mathcal{Q}})$, $e \leftarrow \psi$ and outputting the pair $(a, b = u \cdot a \cdot s + e \bmod \mathcal{O}^\vee)$.*

Definition 2.27 ($\mathcal{O}$-LWE, Average-Case Decision problem). *Let Υ a family of error distributions over $K_{\mathbb{R}}$. The average case decision $\mathcal{O}$-LWE problem, denoted as $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon}$, requires to distinguish independent samples from the distribution $\mathcal{O}_{s,\psi,u}$, where $s \leftarrow U(\mathcal{O}_{\mathcal{Q}}^\vee)$ and $\psi \leftarrow \Upsilon$ and the same number of samples from the uniform distribution over $\mathcal{O}_{\mathcal{Q}} \times \mathbb{T}_{\mathcal{O}^\vee}$.*

Definition 2.28 ($\mathcal{O}$-LWE, Average-Case Search problem). *Let Υ a family of error distributions over $K_{\mathbb{R}}$. The average case search $\mathcal{O}$-LWE problem, denoted as search $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon}$, requires, given independently many samples from the distribution $\mathcal{O}_{s,\psi,u}$, where $s \leftarrow U(\mathcal{O}_{\mathcal{Q}}^\vee)$ and $\psi \leftarrow \Upsilon$, find s.*

In Section 3 we will also deal with the *dual* variant of the $\mathcal{O}$-LWE problem, denoted as the $\mathcal{O}^\vee$-LWE problem, and defined in [BBPS19, Def 3.3]. The only difference lies in swapping the domains of the secret s, $\mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$, and of the a, $\mathcal{O}/\mathcal{Q}\mathcal{O}$, in the definitions above. [20]

We mention that when $\mathcal{O} = \mathcal{O}_K$, $\mathcal{Q} = q\mathcal{O}_K$ and $u = 1/q$, the Order-LWE problem becomes the Ring-LWE problem. We describe the proof of the hardness result for the decision $\mathcal{O}$-LWE problem defined in Definition 2.27. The hardness results of Ring-LWE ([PRSD17]) and Order-LWE ([BBPS19]) involve the following family of error distributions. We denote by s_1 the number of real embeddings and by $2s_2$ the number of complex embeddings of the field. Recall the definition of the set G from Section 2.2.

Definition 2.29 ([BBPS19, Def 3.6]). *Fix an arbitrary $f(n) = \omega(\sqrt{\log n})$. For a positive real α and $u \in K$, a distribution sampled from $\Upsilon_{u,\alpha}$ is an elliptical Gaussian $D_{\mathbf{r}}$, where $\mathbf{r} \in G$ has the entries sampled as follows: for each $1 \leq i \leq s_1$, sample $x_i \leftarrow D_1$ and set $r_i^2 = \alpha^2(x_i^2 + (f(n) \cdot |\sigma_i(u)| / \|u\|_\infty)^2)/2$. For each $s_1 + 1 \leq i \leq s_1 + s_2$, sample $x_i, y_i \leftarrow D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + (f(n) \cdot |\sigma_i(u)| / \|u\|_\infty)^2)/2$. When $u \in K$ is such that $|\sigma_i(u)| = \|u\|_\infty$, for all i, we denote the distribution as Υ_α.*

The proof of the hardness results for algebraic LWE (Ring-LWE [LPR10, PRSD17], Polynomial-LWE [SSTX09], Module-LWE [LS12], Order-LWE [BBPS19])

[20] We stress on the fact that we use the terminology from [BBPS19], which differs from the *primal-dual* terminology from [RSW18, PP19].

follow the same blueprint. For a detailed proof, we refer the reader to [BBPS19]. Briefly, it iterates the following quantum step: given discrete Gaussian samples and an oracle for algebraic LWE, the quantum algorithm outputs narrower discrete Gaussian samples. To do this, it first transforms an $\mathcal{O}$-LWE oracle, using polynomially many discrete Gaussian samples, into a BDD solver, and then uses the BDD solver to output discrete Gaussian samples of narrower parameter. A sufficient condition required to make BDD-samples on a dual lattice $\mathcal{L}^\vee$, along with discrete Gaussian samples over $\mathcal{L}$, into $\mathcal{O}$-LWE samples is that there must exist ($\mathcal{O}$-module) isomorphisms $f : \mathcal{L}/\mathcal{QL} \xrightarrow{\sim} \mathcal{O}/\mathcal{QO}$, and $g : \mathcal{O}^\vee/\mathcal{QO}^\vee \xrightarrow{\sim} \mathcal{L}^\vee/\mathcal{QL}^\vee$, that satisfy the compatibility condition $u \cdot z \cdot x = u \cdot f(z) \cdot g^{-1}(x) \bmod \mathcal{O}^\vee$, for all $z \in \mathcal{L}/\mathcal{QL}$, $x \in \mathcal{L}^\vee/\mathcal{QL}^\vee$ with $u \in (\mathcal{O} : \mathcal{Q})$. For efficiency reasons, we require the isomorphisms f and g to be both efficiently computable and invertible. The compatibility condition yields well-defined LWE samples. Formally,

Theorem 2.30. *Let K be an arbitrary number field of degree n and let $\mathcal{O} \subset K$ an order. Let $\mathcal{Q}$ be an integral $\mathcal{O}$-ideal, $u \in (\mathcal{O} : \mathcal{Q})$ and let $\alpha \in (0, 1)$ be such that $\alpha/\|u\|_\infty \geq 2 \cdot \omega(1)$. Let $\mathcal{S}$ be a subset of $\mathcal{O}$-ideal lattices such that, for any $\mathcal{L} \in \mathcal{S}$, there exist ($\mathcal{O}$-module) isomorphisms $f : \mathcal{L}/\mathcal{QL} \xrightarrow{\sim} \mathcal{O}/\mathcal{QO}$ and $g : \mathcal{O}^\vee/\mathcal{QO}^\vee \xrightarrow{\sim} \mathcal{L}^\vee/\mathcal{QL}^\vee$, both efficiently computable and invertible, such that $u \cdot z \cdot x = u \cdot f(z) \cdot g^{-1}(x)$ mod $\mathcal{O}^\vee$ for any $x \in \mathcal{L}^\vee/\mathcal{QL}^\vee$ and $z \in \mathcal{L}/\mathcal{QL}$. Then, there is a polynomial-time quantum reduction from $\mathcal{S}$-DGS$_\gamma$ to $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon_{u,\alpha}}$, where*

$$\gamma = max\left\{\eta(\mathcal{QL}) \cdot \sqrt{2}\|u\|_\infty/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}.$$

Proof. (Overview) We first prove that the compatibility condition yields well-defined Order-LWE samples. Recall that the isomorphism f maps the discrete Gaussian sample z to the a part of the LWE sample, whereas the isomorphism g^{-1} maps the BDD-secret x to the LWE secret s. Then the compatibility condition yields $u \cdot z \cdot x = u \cdot a \cdot s \bmod \mathcal{O}^\vee$. Under well chosen parameters, as in Lemma [BBPS19, Lem 3.16], the discrete Gaussian distribution over $\mathcal{L}$ mod $\mathcal{QL}$ is almost the uniform distribution over $\mathcal{L}/\mathcal{QL}$ (see Lemma A.2) and since f is an isomorphism, a is almost uniform over $\mathcal{O}/\mathcal{QO}$. Let $y = x + e$ be the BDD coset and e', an additional error term. Then the LWE samples are defined as,

$$\begin{aligned}(a, b) &= (f(z), u \cdot z \cdot y + e' \mod \mathcal{O}^\vee)\\ &= (f(z), u \cdot z \cdot x + \tilde{e} \mod \mathcal{O}^\vee)\\ &= (f(z), u \cdot a \cdot s + \tilde{e} \mod \mathcal{O}^\vee).\end{aligned}$$

For a detailed analysis of the error term, we refer the reader to the proof of [BBPS19, Lem 2.36]. This shows that the compatibility condition implies the well-defined LWE samples and hence the algorithm in Lemma [BBPS19, Lem 3.16].

As described earlier, the hardness proof relies on applying Lemma [BBPS19, Lem 3.15] iteratively for transforming discrete Gaussian samples into discrete

Gaussian samples of a narrower parameter. This iterative step uses Lemma [BBPS19, Lem 3.16] and Lemma [PRSD17, Lem 6.7]. As a starting point for the iteration, samples from a discrete Gaussian distribution of a large enough parameter are efficiently generated using [Reg05, Lem 3.2]. □

Hardness results for Ring-LWE [LPR10] [PRSD17], Polynomial-LWE [SSTX09] and Order-LWE [BBPS19] use invertibility of the ideal lattices considered, to derive the compatible maps f and g.

Remark 2.31. Although Theorem 2.30 presents the hardness result for Order-LWE, a similar proof also derives the hardness result for the dual setting of Order-LWE, as defined in [BBPS19, Def 3.3], where $a \in \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$ and $s \in \mathcal{O}/\mathcal{Q}\mathcal{O}$. The only difference consists in switching the maps f and g in the BDD-to-$\mathcal{O}^\vee$-LWE reduction.

Gaussian distributions over $K_\mathbb{R}$ and $K_\mathbb{R}/\mathcal{O}^\vee$ The proofs of the following results follow from basic properties of the Gaussian vector distributions. See Section A.9. For an order $\mathcal{O} \subseteq K$ with a $\mathbb{Z}$-basis $\{p_i\}_{1\le i\le n}$, let $P_\mathcal{O} = (Tr(p_i \cdot \overline{p_j}))_{1\le i,j\le n}$.

Lemma 2.32 ([PP19, Sect 5.3.]). *Let e be drawn according to a Gaussian distribution D_α over $K_\mathbb{R}$. Then the coefficients of e with respect to a $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ satisfy a Gaussian distribution over $\mathbb{R}^n$ of covariance matrix $\alpha^2 \cdot P_\mathcal{O}$. In particular, $e \mod \mathcal{O}^\vee$ follows a Gaussian distribution over $\mathbb{R}^n$ mod $\mathbb{Z}^n$ of the same covariance matrix.*

3 New Hardness Results for $\mathcal{O}$-LWE

In this section, we extend and enhance the hardness results for decision Order-LWE from [BBPS19] as follows:

- We prove extended versions of worst-case hardness results for both decision primal and dual variants of Order-LWE that follow for all $\mathcal{O}$-ideals, with same approximation factors as in the previous hardness statements for Order-LWE and Ring-LWE.
- We extend the worst-case hardness result for decision Ring-LWE that follows not only for $\mathcal{O}_K$-ideals, but also for $\mathcal{O}$-ideals, for any order $\mathcal{O}$ of index coprime to the Ring-LWE ideal modulus $\mathcal{Q}$. However, it incurs a penalty in the approximation factor, which depends on the conductor of the order. This result is complementary to [BBPS19, Thm 3.8 & Cor. 5.2].

We mention that these reductions are non-uniform, as short ring elements and $\mathbb{Z}$-bases of orders and ideals involved are given as advice.

3.1 Worst-Case Hardness for All $\mathcal{O}$-ideals

We begin this section with a non-maximal order $\mathcal{O}$ in the number field K. Let $m = [\mathcal{O}_K : \mathcal{O}]$ be the index of $\mathcal{O}$ in $\mathcal{O}_K$ and $\mathcal{C}_\mathcal{O}$ its conductor. Recall that for an ideal $\mathcal{I}$ of a ring R, $Spec_R(\mathcal{I})$ is the set of all prime ideals in R that contain $\mathcal{I}$. We denote by $\mathrm{Id}(\mathcal{O})$ the set of all fractional $\mathcal{O}$-ideals and further remark that $\mathrm{Id}(\mathcal{O}_K) \subsetneq \mathrm{Id}(\mathcal{O})$. For an ideal modulus $\mathcal{Q}$ coprime with the principal $\mathcal{O}$ ideal generated by the index $[\mathcal{O}_K : \mathcal{O}]$ and $u \in (\mathcal{O} : \mathcal{Q}) = \{x \in K | x\mathcal{Q} \subseteq \mathcal{O}\}$, we denote the primal Order-LWE problem as $\mathcal{O}$-LWE$_{(\mathcal{Q},u)}$ and the dual Order-LWE problem ([BBPS19, Def 3.3]) as $\mathcal{O}^\vee$-LWE$_{(\mathcal{Q},u)}$. Our improved hardness results for these decision problems are as follows.

Theorem 3.1. *Let K be an arbitrary number field of degree n. Choose an ideal modulus $\mathcal{Q}$, coprime to $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$ and $u \in (\mathcal{O} : \mathcal{Q})$. Let $\alpha \in (0, 1)$ such that $\alpha/\|u\|_\infty \geq 2 \cdot \omega(1)$. Then there are polynomial time quantum reductions*

$$Id(\mathcal{O})\text{-}\mathtt{DGS}_\gamma \longrightarrow \mathcal{O}\text{-LWE}_{(\mathcal{Q},u),\Upsilon_{u,\alpha}} \tag{3.1.1}$$

$$Id(\mathcal{O})\text{-}\mathtt{DGS}_\gamma \longrightarrow \mathcal{O}^\vee\text{-LWE}_{(\mathcal{Q},u),\Upsilon_{u,\alpha}} \tag{3.1.2}$$

where $\gamma = max\left\{\eta(\mathcal{Q}\mathcal{L}) \cdot \sqrt{2}\|u\|_\infty/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}$.

As mentioned in the introduction, the hardness result for Order-LWE, as proved in [BBPS19], showed that $\mathcal{O}$-LWE is at least as hard as lattice problems on lattices that are *invertible* $\mathcal{O}$-ideals. The theorem above extends the result to include non-invertible $\mathcal{O}$-ideals as well, thereby closing the gap. We, however, restrict to the ideal modulus being coprime to $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$, which also implies being coprime with the conductor ideal $\mathcal{C}_\mathcal{O} = (\mathcal{O} : \mathcal{O}_K)$, as $[\mathcal{O}_K : \mathcal{O}]\mathcal{O} \subseteq \mathcal{C}_\mathcal{O}$. In the case of $\mathcal{Q} = q\mathcal{O}$ and $u = 1/q$, for some integer q, we can choose q as being coprime with the index $[\mathcal{O}_K : \mathcal{O}]$. No such assumption was made on the modulus in [BBPS19, Thm 3.8].

Note that both the hardness results compare the LWE problems with lattice problems on the same set of number field lattices, the $\mathcal{O}$-ideals. This is because the $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE problems are equivalent as long as the ideal modulus $\mathcal{Q}$ is coprime to $\mathcal{C}_\mathcal{O}$. This equivalence was also studied in [BBPS19, Rem. 3.5], but under a stronger assumption of $\mathcal{O}^\vee$ being an invertible $\mathcal{O}$-ideal. Moreover, this equivalence is also a consequence of [PP19, Cor.4.3], under the assumption of $\mathcal{O}$ and $\mathcal{O}^\vee$ being both *invertible modulo* $\mathcal{Q}$ ([PP19, Def 2.10]), a condition already implied by our choice of $\mathcal{Q}$.

Proposition 3.2. *Let K be an arbitrary number field of degree n and $\mathcal{O}$ be an order. Choose an $\mathcal{O}$ ideal modulus $\mathcal{Q}$, coprime to $\mathcal{C}_\mathcal{O}$, $u \in (\mathcal{O} : \mathcal{Q})$, and Υ a distribution over a family of error distributions over $K_\mathbb{R}$. Then, given bases for $\mathcal{O}$ and $\mathcal{O}_K$, the (search or decision) $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon}$ and the (search or decision) $\mathcal{O}^\vee$-LWE$_{(\mathcal{Q},u),\Upsilon}$ problems are equivalent by an efficient reduction, given bases of $\mathcal{O}$, $\mathcal{O}_K$, $\mathcal{O}_K^\vee$, $\mathcal{O}^\vee$, $\mathcal{Q}$ and prime ideals containing $\mathcal{Q}$.*

Proof. Define a map $f : \frac{\mathcal{O}}{\mathcal{Q}\mathcal{O}} \longrightarrow \frac{\mathcal{O}^\vee}{\mathcal{Q}\mathcal{O}^\vee}$ as a composition of the following three isomorphisms

$$\begin{array}{ccccc} \dfrac{\mathcal{O}}{\mathcal{Q}\mathcal{O}} & \xhookrightarrow{\sim} & \dfrac{\mathcal{O}_K}{\mathcal{Q}\mathcal{O}_K} & \xrightarrow{\sim} & \dfrac{\mathcal{O}_K^\vee}{\mathcal{Q}\mathcal{O}_K^\vee} & \xhookrightarrow{\sim} & \dfrac{\mathcal{O}^\vee}{\mathcal{Q}\mathcal{O}^\vee} \\ a & \to & a + \mathcal{Q}\mathcal{O}_K & \to & ta + \mathcal{Q}\mathcal{O}_K^\vee & \to & ta + \mathcal{Q}\mathcal{O}^\vee := f(a) \end{array}$$

The first and the last isomorphisms follow from Lemma 2.12, under the coprimality condition on $\mathcal{Q}$. The middle map is an application of the Cancellation Lemma 2.10 and we let $t \in \mathcal{O}_K^\vee$ be the element, multiplication by which, yields the isomorphism. The multiplier can be efficiently computed as in previous works [RSW18, Thm 3.1], [BBPS19, Prop 4.7], [PP19, Lem 2.13].[21] Then, for $a \in \mathcal{O}/\mathcal{Q}\mathcal{O}$ and $s \in \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$, the cosets $u \cdot a \cdot s + \mathcal{O}^\vee$ and $u \cdot f(a) \cdot f^{-1}(s) + \mathcal{O}^\vee$ are equal. To see this, let $s' = f^{-1}(s) \in \mathcal{O}/\mathcal{Q}\mathcal{O}$. Notice that, as f is isomorphism, then $f(a)$ and $f^{-1}(s')$ are uniform over their corresponding sets, as a and s are. Then,

$$\begin{aligned} u \cdot a \cdot s + \mathcal{O}^\vee &= u \cdot a \cdot f(s') + \mathcal{O}^\vee \\ &= u \cdot a \cdot (ts' + \mathcal{Q}\mathcal{O}^\vee) + \mathcal{O}^\vee \\ &= u \cdot ta \cdot s' + \mathcal{O}^\vee && \text{as } u \cdot a \cdot \mathcal{Q}\mathcal{O}^\vee \subseteq \mathcal{O}^\vee \\ &= u \cdot (ta + \mathcal{Q}\mathcal{O}^\vee) \cdot s' + \mathcal{O}^\vee && \text{as } u \cdot s' \cdot \mathcal{Q}\mathcal{O}^\vee \subseteq \mathcal{O}^\vee \\ &= f(a) \cdot f^{-1}(s) + \mathcal{O}^\vee \end{aligned}$$

Therefore, the $\mathcal{O}$-LWE samples $(a, b := u \cdot a \cdot s + e \mod \mathcal{O}^\vee)$, where $e \leftarrow \varphi$ for some $\varphi \leftarrow \Upsilon$, can be transformed to $\mathcal{O}^\vee$-LWE samples by considering $(f(a), b := u \cdot f(a) \cdot f^{-1}(s) + e \mod \mathcal{O}^\vee)$, where $f(a) \in \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$ and $f^{-1}(s) \in \mathcal{O}/\mathcal{Q}\mathcal{O}$. Conversely, the $\mathcal{O}^\vee$-LWE samples $(a', b' := u \cdot a' \cdot s' + e' \mod \mathcal{O}^\vee)$, where $e' \leftarrow \varphi$ for some $\varphi \leftarrow \Upsilon$, can be made into $\mathcal{O}$-LWE samples by taking $(f^{-1}(a'), b := u \cdot f^{-1}(a') \cdot f(s') + e' \mod \mathcal{O}^\vee)$, where $f^{-1}(a') \in \mathcal{O}/\mathcal{Q}\mathcal{O}$ and $f(s') \in \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$. It is easy to check that the transformation above sending (a, b) to $(f(a), b)$ maps uniform samples over $\mathcal{O}/\mathcal{Q}\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee$ to uniform samples over $\mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee \times K_\mathbb{R}/\mathcal{O}^\vee$. □

Taking the particular case of Theorem 3.1 for $\mathcal{Q} = q\mathcal{O}$ and $u = 1/q$, coupled with the reduction from SIVP to DGS (see Lemma 2.8) yields the following generalization of [LPR10, Thm 3.6], [PRSD17, Corollary 6.3]. See Section B.1.

Corollary 3.3. *Let K be an arbitrary number field of degree n. Let $\alpha \in (0, 1)$ satisfy $\alpha \cdot q \geq 2\omega(1)$ and q be an integer coprime to $[\mathcal{O}_K : \mathcal{O}]$. Then there is a polynomial time quantum reduction from*

$$Id(\mathcal{O})\text{-}\mathtt{SIVP}_{\gamma'} \longrightarrow \mathcal{O}\text{-LWE}_{(q\mathcal{O}, 1/q), \Upsilon_\alpha},$$

where $\gamma' = \omega(\frac{1}{\alpha})$.

In order to prove Theorem 3.1, we need the following lemma.

[21] The size of the multiplier is not relevant here.

Lemma 3.4. *Let $\mathcal{Q}$ be an ideal modulus coprime to $m\mathcal{O}$, for $m := [\mathcal{O}_K : \mathcal{O}]$ and $u \in (\mathcal{O} : \mathcal{Q})$. Let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Then, there exist (quantumly) efficiently computable and invertible $\mathcal{O}$-module isomorphisms,*

$$f : \frac{\mathcal{I}}{\mathcal{Q}\mathcal{I}} \xrightarrow{\sim} \frac{\mathcal{O}}{\mathcal{Q}\mathcal{O}} \quad \text{and} \quad g : \frac{\mathcal{O}^\vee}{\mathcal{Q}\mathcal{O}^\vee} \xrightarrow{\sim} \frac{\mathcal{I}^\vee}{\mathcal{Q}\mathcal{I}^\vee},$$

given bases of $\mathcal{I}$, $\mathcal{I}^\vee$,$\mathcal{O}$, $\mathcal{O}^\vee$, $\mathcal{Q}$ and prime ideals containing $\mathcal{Q}$. Further, if $a \in \mathcal{O}/\mathcal{Q}\mathcal{O}$ is the image of $z \in \mathcal{I}/\mathcal{Q}\mathcal{I}$ and $s \in \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$ is the pre-image of $x \in \mathcal{I}^\vee/\mathcal{Q}\mathcal{I}^\vee$, then $u \cdot z \cdot x = u \cdot a \cdot s \mod \mathcal{O}^\vee$.

Proof. Let $\mathfrak{p}$ be the invertible ideal that contains $\mathcal{I}$ as described in Lemma 2.22. Moreover, a basis of this ideal can be found quantumly efficient, thanks to the same lemma. Then, the modulus $\mathcal{Q}$ is coprime with $[\mathfrak{p} : \mathcal{I}]\mathcal{O}$, as $Spec_{\mathbb{Z}}([\mathfrak{p} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$. Indeed, assume by contrary that $\mathcal{Q}$ is not coprime to the index $[\mathfrak{p} : \mathcal{I}]$. Then there exists a maximal ideal $\mathfrak{m}$ for which $\mathcal{Q} + [\mathfrak{p} : \mathcal{I}]\mathcal{O} \subseteq \mathfrak{m}$. In particular, this says $\mathcal{Q} \subseteq \mathfrak{m}$ and $[\mathfrak{p} : \mathcal{I}]\mathcal{O} \subseteq \mathfrak{m}$. Denote by $[\mathfrak{p} : \mathcal{I}] = p_1^{n_1} \cdot \ldots \cdot p_k^{n_k}$, for some prime integers p_i of positive integer exponents n_i. Then since $\prod_i (p_i\mathcal{O})^{n_i} = [\mathfrak{p} : \mathcal{I}]\mathcal{O} \subseteq \mathfrak{m}$ and $\mathfrak{m}$ is in particular a prime ideal, we also have $p_i\mathcal{O} \subseteq \mathfrak{m}$, for some $i \in \{1, \ldots, k\}$. Moreover, as $Spec_{\mathbb{Z}}([\mathfrak{p} : \mathcal{I}]) = \{p_1, \ldots, p_k\} \subseteq Spec_{\mathbb{Z}}(m)$, we get that $m\mathcal{O} \subseteq p_i\mathcal{O} \subseteq \mathfrak{m}$. Together with $\mathcal{Q} \subseteq \mathfrak{m}$, we reach a contradiction with our choice of $\mathcal{Q}$.

As $\mathcal{Q}$ is indeed coprime with $[\mathfrak{p} : \mathcal{I}]\mathcal{O}$, it becomes also coprime with $(\mathcal{I} : \mathfrak{p})$, as needed in Lemma 2.12, since $[\mathfrak{p} : \mathcal{I}]\mathcal{O} \subseteq (\mathcal{I} : \mathfrak{p})$. By Lemma 2.12, this yields the following (classically) efficiently computable and invertible isomorphisms induced by inclusion,

$$\begin{aligned} f_1 : \frac{\mathcal{I}}{\mathcal{Q}\mathcal{I}} &\xrightarrow{\sim} \frac{\mathfrak{p}}{\mathcal{Q}\mathfrak{p}} \quad \text{and} \quad & g_1 : \frac{\mathfrak{p}^\vee}{\mathcal{Q}\mathfrak{p}^\vee} &\xrightarrow{\sim} \frac{\mathcal{I}^\vee}{\mathcal{Q}\mathcal{I}^\vee} \\ z &\mapsto f_1(z) = \tilde{z} & \tilde{x} &\mapsto g_1(\tilde{x}) = x \\ z + \mathcal{Q}\mathfrak{p} &= \tilde{z} + \mathcal{Q}\mathfrak{p} & \tilde{x} + \mathcal{Q}\mathcal{I}^\vee &= x + \mathcal{Q}\mathcal{I}^\vee \end{aligned}$$

Invertibility of $\mathfrak{p}$ and the Cancellation Lemma (Lemma 2.10) yield a $t \in \mathfrak{p}$ such that multiplication by t^{-1} induces the following efficiently computable and invertible isomorphisms:

$$\begin{aligned} f_2 : \frac{\mathfrak{p}}{\mathcal{Q}\mathfrak{p}} &\xrightarrow{\sim} \frac{\mathcal{O}}{\mathcal{Q}\mathcal{O}} \quad \text{and} \quad & g_2 : \frac{\mathcal{O}^\vee}{\mathcal{Q}\mathcal{O}^\vee} &\xrightarrow{\sim} \frac{\mathfrak{p}^\vee}{\mathcal{Q}\mathfrak{p}^\vee} \\ \tilde{z} &\mapsto f_2(\tilde{z}) = t^{-1}\tilde{z} := a & s &\mapsto g_2(s) = t^{-1}s := \tilde{x} \\ t^{-1}\tilde{z} + \mathcal{Q}\mathcal{O} &= a + \mathcal{Q}\mathcal{O} & t^{-1}s + \mathcal{Q}\mathfrak{p}^\vee &= \tilde{x} + \mathcal{Q}\mathfrak{p}^\vee \end{aligned}$$

The above map uses the fact that $\mathfrak{p}^\vee = \mathfrak{p}^{-1}\mathcal{O}^\vee$. See Proposition A.7($iv$). The multiplier can be efficiently computed as in previous works [RSW18, Thm 3.1], [BBPS19, Prop 4.7], [PP19, Lem 2.13].[22] Define $f = f_2 \circ f_1 : \mathcal{I}/\mathcal{Q}\mathcal{I} \to \mathcal{O}/\mathcal{Q}\mathcal{O}$ and $g = g_1 \circ g_2 : \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee \to \mathcal{I}^\vee/\mathcal{Q}\mathcal{I}^\vee$. Since all the maps involved are efficiently computable $\mathcal{O}$-module isomorphisms, so are f and g.

[22] The size of the multiplier is not relevant here.

Finally, we prove that f and g are compatible, i.e., for all $z \in \mathcal{I}/\mathcal{Q}\mathcal{I}$ and $x \in \mathcal{I}^\vee/\mathcal{Q}\mathcal{I}^\vee$, $u \cdot z \cdot x = u \cdot a \cdot s \mod \mathcal{O}^\vee$, whenever $f(z) = a$ and $g(s) = x$. Consider the coset,

$$\begin{aligned} u \cdot z \cdot x + \mathcal{O}^\vee &= u \cdot z \cdot (x + \mathcal{Q}\mathcal{I}^\vee) + \mathcal{O}^\vee \quad \text{as } u \cdot z \cdot \mathcal{Q}\mathcal{I}^\vee \subset u\mathcal{Q}\mathcal{I}\mathcal{I}^\vee \subseteq \mathcal{O}^\vee \\ &= u \cdot z \cdot (\tilde{x} + \mathcal{Q}\mathcal{I}^\vee) + \mathcal{O}^\vee \\ &= u \cdot z \cdot \tilde{x} + \mathcal{O}^\vee \\ &= u \cdot (z + \mathcal{Q}\mathfrak{p}) \cdot \tilde{x} + \mathcal{O}^\vee \quad \text{as } u \cdot \mathcal{Q}\mathfrak{p} \cdot \tilde{x} \subset u \cdot \mathcal{Q}\mathfrak{p}\mathfrak{p}^\vee \subseteq \mathcal{O}^\vee \\ &= u \cdot (\tilde{z} + \mathcal{Q}\mathfrak{p}) \cdot \tilde{x} + \mathcal{O}^\vee \\ &= u \cdot \tilde{z} \cdot \tilde{x} + \mathcal{O}^\vee. \end{aligned}$$

Therefore, $u \cdot z \cdot x = u \cdot \tilde{z} \cdot \tilde{x} \mod \mathcal{O}^\vee$. According to the notations, $a = f_2(\tilde{z})$ and $s = g_2^{-1}(\tilde{x})$. Using the definitions of f_2 and g_2,

$$\begin{aligned} u \cdot \tilde{z} \cdot \tilde{x} + \mathcal{O}^\vee &= u \cdot t^{-1}(\tilde{z} + \mathcal{Q}\mathfrak{p}) \cdot t(\tilde{x} + \mathcal{Q}\mathfrak{p}^\vee) + \mathcal{O}^\vee \\ &= u \cdot (a + \mathcal{Q}\mathcal{O}) \cdot (s + \mathcal{Q}\mathcal{O}^\vee) + \mathcal{O}^\vee \\ &= u \cdot a \cdot s + \mathcal{O}^\vee, \end{aligned}$$

therefore $u \cdot a \cdot s = u \cdot \tilde{z} \cdot \tilde{x} \mod \mathcal{O}^\vee$. This concludes the proof. □

Notice that the maps from Lemma 3.4 are constructed as quantumly efficient, because of the quantum construction of the basis of the intermediary ideal $\mathfrak{p}$ from Lemma 2.22.[23]

Proof (of Theorem 3.1). We use Theorem 2.30 to prove the hardness results. We show that in this case the set $\mathcal{S}$, as described in Theorem 2.30, equals the set of all $\mathcal{O}$-ideals for both $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE. The novelty of this generalization is in the fact that we convert BDD samples on non-invertible $\mathcal{O}$-ideals into LWE samples. Previously, as in the proof of [BBPS19, Theorem 3.7 & 3.8], this step used the Cancellation Lemma (Lemma 2.10) which unavoidably required the ideal for the BDD problem (or the dual ideal, which ever is relevant), to be invertible. We overcome this by using the improved cancellation Lemma 3.4. Let $\mathcal{I}$ be a non-invertible $\mathcal{O}$-ideal. Recall that without loss of generality, we may assume that $\mathcal{I} \subset \mathcal{O}$. Then, for all ideal moduli $\mathcal{Q}$ coprime to $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$, we obtain isomorphisms $f : \mathcal{I}/\mathcal{Q}\mathcal{I} \xrightarrow{\sim} \mathcal{O}/\mathcal{Q}\mathcal{O}$ and $g : \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee \xrightarrow{\sim} \mathcal{I}^\vee/\mathcal{Q}\mathcal{I}^\vee$. Further, Lemma 3.4 shows that these maps are compatible with respect to the condition mentioned in Theorem 2.30.

Now, let $\mathcal{I}$ be an integral $\mathcal{O}$-ideal. Given a BDD sample $y = x + e$ on $\mathcal{I}^\vee$ and a discrete Gaussian sample z from $\mathcal{I}$, we define $(a, b) \in \mathcal{O}/\mathcal{Q}\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee$ as $a = f(z)$ and $b = u \cdot z \cdot y + e' \mod \mathcal{O}^\vee$, for a small error e'. The compatibility of the maps f and g implies that the tuple (a, b) is a well-defined $\mathcal{O}$-LWE sample, i.e. $b = u \cdot f(z) \cdot g^{-1}(x) + \tilde{e} \mod \mathcal{O}^\vee$, for an error $\tilde{e}$ depending on e and e'. Eq. (3.1.2) then follows from the equivalence of $\mathcal{O}$-LWE and $\mathcal{O}^\vee$-LWE, Proposition 3.2. □

[23] This is improved in a concurrent work, [JL22, Lem.5.7], which presents in their *Ideal Clearing Lemma* a classical efficient algorithm to construct the same isomorphisms, for an ideal modulus $\mathcal{Q}$ generated by an integer q coprime to the index of the order.

3.2 Ring-LWE Hardness for Some Non $\mathcal{O}_K$-ideal Lattices

The authors in [LPR10, PRSD17] showed that solving Ring-LWE is at least as hard as solving short vector problems on the set of all ideals of the ring of integers $\mathcal{O}_K$. We extend this result to include lattice problems on lattices that are not necessarily ideals of $\mathcal{O}_K$. Although, in our reduction, we extend the set of lattices to a strict superset of $\mathcal{O}_K$-ideal lattices, a lattice $\mathcal{L}$ that is not an $\mathcal{O}_K$-ideal incurs a cost of an $\mathcal{O}_{\mathcal{L}}$-dependent factor in the approximation factor γ. We prove our generalized hardness result for Ring-LWE, often denoted as $\mathcal{O}_K$-LWE, by giving a polynomial time reduction from $\mathcal{O}$-LWE to $\mathcal{O}_K$-LWE and pre-composing it with our hardness result, Theorem 3.1, for $\mathcal{O}$-LWE. In our $\mathcal{O}$-LWE to $\mathcal{O}_K$-LWE reduction, the error parameter gets inflated by the conductor $\mathcal{C}_{\mathcal{O}}$ of $\mathcal{O}$ in $\mathcal{O}_K$.

Fix an order $\mathcal{O}$. Let $\mathcal{Q}$ be an $\mathcal{O}$ ideal modulus coprime to the conductor $\mathcal{C}_{\mathcal{O}} = (\mathcal{O} : \mathcal{O}_K)$, and therefore by Theorem 2.19 admits a unique factorization into a product of prime ideals over $\mathcal{O}$. Let $Spec_{\mathcal{O}}(\mathcal{Q}) := \{\mathfrak{q}_1, \ldots, \mathfrak{q}_r\}$. Let $u \in (\mathcal{O} : \mathcal{Q})$. Notice that by definition, it also belongs to $(\mathcal{O}_K : \mathcal{Q}\mathcal{O}_K)$.

Proposition 3.5. *Let K be a number field and $\mathcal{O} \subset \mathcal{O}_K$, an order. Let $\mathcal{Q}$ be an ideal modulus coprime with $\mathcal{C}_{\mathcal{O}}$, $u \in (\mathcal{O} : \mathcal{Q})$. Let Υ be a distribution over a family of error distributions over $K_{\mathbb{R}}/\mathcal{Q}\mathcal{O}^\vee$, and let $t \in \mathcal{C}_{\mathcal{O}} \setminus \bigcup_i \mathfrak{q}_i\mathcal{C}_{\mathcal{O}}$. Then there is a polynomial time reduction from (search or decision) $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon}$ to (search or decision) $\mathcal{O}_K$-LWE$_{(\mathcal{Q}\mathcal{O}_K,u),t\cdot\Upsilon}$, given the bases of $\mathcal{O}$, $\mathcal{O}_K$, $\mathcal{C}_{\mathcal{O}}$, $\mathcal{Q}$ and the primes $\mathfrak{q}_i$.*

Notice that the reduction increases the noise by a factor of t. We remark that the error parameter of the $\mathcal{O}_K$-LWE problem in Theorem 3.6 would be the least when t is the shortest lattice vector in $\mathcal{C}_{\mathcal{O}} \setminus \bigcup_i \mathfrak{q}_i\mathcal{C}_{\mathcal{O}}$. The existence of such a short multiplier can be proven either by using the combinatorial argument from [BBPS19, Lem 2.36] or by sampling according to a Gaussian distribution over the conductor ideal with a wide parameter, as in [RSW18, Thm 3.1], [BBPS19, Prop 4.7].[24] We would like to clarify that the statements in these previous works require that the ideal we sample t from be invertible. Their proofs, however, hold true for the conductor ideal. See Section B.3 for a discussion on the size of this multiplier.

Proof (of Prop. 3.5). Define the following maps,

$$f : \frac{\mathcal{O}}{\mathcal{Q}\mathcal{O}} \to \frac{\mathcal{O}_K}{\mathcal{Q}\mathcal{O}_K}, \qquad f^\vee : \frac{\mathcal{O}^\vee}{\mathcal{Q}\mathcal{O}^\vee} \xrightarrow{\cdot t} \frac{\mathcal{O}_K^\vee}{\mathcal{Q}\mathcal{O}_K^\vee}.$$

The first map f is induced by the inclusion $\mathcal{O} \subset \mathcal{O}_K$ and is an isomorphism under the assumption that $\mathcal{Q}$ is coprime to the conductor (Lemma 2.12). The second

[24] We would also like to point out that [PP19, Le. 2.13] shows another efficient way of constructing a multiplier t, via the Chinese Remainder Theorem application, but this does not give any control on its size. Same discussion holds also for [JL22, Lem.4.1], as the multiplier is constructed via a randomized algorithm that considers a linear combination of basis elements of the involved order.

map $f^\vee$ is induced by multiplication by t. It is an isomorphism for $\mathcal{I} = \mathcal{C}_\mathcal{O}$, $\mathcal{J} = \mathcal{Q}$ and $\mathcal{M} = \mathcal{O}^\vee$ as $t\mathcal{M} + \mathcal{I}\mathcal{J}\mathcal{M} = \mathcal{I}\mathcal{M}$. See Remark 2.11 and [BBPS19, Rem 2.33]. Both maps can be efficiently computed. We further extend the second map to $K_\mathbb{R}$, $\overline{f^\vee} : K_\mathbb{R}/\mathcal{O}^\vee \longrightarrow K_\mathbb{R}/\mathcal{O}_K^\vee$ as $\overline{f^\vee}(u \cdot x) = u \cdot t \cdot x$, for any $x \in K_\mathbb{R}/\mathcal{Q}\mathcal{O}^\vee$. With these maps, define the following transformation

$$\begin{aligned} \frac{\mathcal{O}}{\mathcal{Q}\mathcal{O}} \times \frac{K_\mathbb{R}}{\mathcal{O}^\vee} &\longrightarrow \frac{\mathcal{O}_K}{\mathcal{Q}\mathcal{O}_K} \times \frac{K_\mathbb{R}}{\mathcal{O}_K^\vee} \\ (a, b) &\mapsto (a' = f(a),\ b' = \overline{f^\vee}(b) := t \cdot b \mod \mathcal{O}_K^\vee). \end{aligned}$$

Since the maps, f and $\overline{f^\vee}$ are isomorphisms, this transformation maps uniform samples to uniform samples. Further, if $b = u \cdot a \cdot s + e \mod \mathcal{O}^\vee$ is sampled from the $\mathcal{O}$-LWE distribution $\mathcal{O}_{(\mathcal{Q},u),s,\varphi}$, where s is uniform in $\mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$ and $e \leftarrow \varphi$, for $\varphi \leftarrow \Upsilon$, then,

$$\begin{aligned} b' &= u \cdot f^\vee(a \cdot s) + \overline{f^\vee}(e) \mod \mathcal{O}_K^\vee \\ &= u \cdot a \cdot f^\vee(s) + \overline{f^\vee}(e) \mod \mathcal{O}_K^\vee \\ &= u \cdot f(a) \cdot f^\vee(s) + \overline{f^\vee}(e) \mod \mathcal{O}_K^\vee. \end{aligned}$$

The second equality follows from the fact that $f^\vee$ is an $\mathcal{O}$-module homomorphism. The third equality follows from the fact that these cosets are equal: $u \cdot a \cdot f^\vee(s) + \mathcal{O}_K^\vee = u \cdot (a + \mathcal{Q}\mathcal{O}_K) \cdot f^\vee(s) + \mathcal{O}_K^\vee = u \cdot f(a) \cdot f^\vee(s) + \mathcal{O}_K^\vee$. Finally, as $e \leftarrow \varphi$, its image $\overline{f^\vee}(e) \leftarrow t \cdot \varphi$. Moreover, the secret s, as is uniform over $\mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$, is mapped to $f^\vee(s)$, which is also uniform over $\mathcal{O}_K^\vee/\mathcal{Q}\mathcal{O}_K^\vee$, as $f^\vee$ is an isomorphism. This yields an efficient transformation from $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\Upsilon}$ to $\mathcal{O}_K$-LWE$_{(\mathcal{Q}\mathcal{O}_K,u),t\cdot\Upsilon}$. □

Pre-composing this reduction (Proposition 3.5) by the decision $\mathcal{O}$-LWE hardness result, Theorem 3.1 yields the following improved hardness result for decision $\mathcal{O}_K$-LWE.

Theorem 3.6. *Let K be a number field of degree n and $\mathcal{O} \subset \mathcal{O}_K$, an order. Let $\mathcal{Q}$ be an ideal modulus coprime to $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$ and $u \in (\mathcal{O} : \mathcal{Q})$. Let $Id(\mathcal{O})$ denote the set of $\mathcal{O}$-ideals. Choose $t \in \mathcal{C}_\mathcal{O} \setminus \bigcup_i \mathfrak{q}_i\mathcal{C}_\mathcal{O}$ and choose $\alpha \in (0, 1)$ such that $\alpha/\|u\|_\infty \geq 2\omega(1)$. Then there is a polynomial time quantum reduction from*

$$Id(\mathcal{O})\text{-}\mathtt{DGS}_\gamma \longrightarrow \mathcal{O}_K\text{-LWE}_{(\mathcal{Q}\mathcal{O}_K,u),t\cdot\Upsilon_{u,\alpha}},$$

where

$$\gamma = max\left\{\eta(\mathcal{Q}\mathcal{L}) \cdot \sqrt{2} \cdot \|u\|_\infty/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}.$$

Comparison with previous work. We note that [BBPS19, Thm 3.8, Cor 5.2] also showed a connection between Order-LWE and Ring-LWE. While the error and the approximation factors obtained from the two reductions are comparable, the results are complementary in terms of other parameters. Further, the prior requires a set of field elements that generate $\mathcal{O}^\vee$ over $\mathcal{O}_K^\vee$ to map between the

order and the ring of integers, which is similar to the role of our t. Our result poses a significant improvement in the size of the set of lattices and the set of relevant moduli, since it considers solving lattice problems on the set of all $\mathcal{O}$-ideals, whereas the prior result considers solving lattice problems on the set of $\mathcal{O}$-ideals whose duals are invertible. Our theorem also expands the choice of the moduli for the Ring-LWE problem: the previous result only holds under the assumption that the modulus q be a factor of $[\mathcal{O}_K : \mathcal{O}]$, reducing the choice for q to a finite set, whereas, Theorem 3.6 assumes that the ideal modulus $\mathcal{Q}$ (and in particular, the principal ideal $q\mathcal{O}$) is coprime to $[\mathcal{O}_K : \mathcal{O}]\mathcal{O}$, tapping an infinite set of choices and also complementing the previous result by bridging the gap.

Solving DGS on p-ary lattices. We view Theorem 3.6 in a different light. We first consider its particular case $\mathcal{Q} = q\mathcal{O}$ and $u = 1/q$, for q an integer coprime with the index $[\mathcal{O}_K : \mathcal{O}]$. Instead of solving DGS on $\mathcal{O}$-ideals, where $\mathcal{O}$ varies over the set of orders of indices coprime to a fixed modulus q, we use the $\mathcal{O}_K$-LWE oracle to solve DGS on the set of (embeddings of) all p-ary lattices. Recall that, when K is a monogenic field, the embedding $\mathcal{L}$ of an integer p-ary lattice satisfies $p\mathcal{O}_K \subseteq \mathcal{L} \subseteq \mathcal{O}_K$. This makes $\mathcal{L}$ an ideal of the order $\mathbb{Z} + p\mathcal{O}_K$. See Remark 2.17. However, this order may be strictly contained in the ring of multipliers $\mathcal{O}_\mathcal{L}$ of $\mathcal{L}$. The reduction described below, would, in turn solve DGS on integer p-ary lattices up to an approximation factor related to the field (of embedding) K. See Lemma 2.14. Owing to the results of [Ajt96, Reg05], it is sufficient to solve lattice problems on p-ary lattices, as solving lattice problems on p-ary lattices is at least as hard as solving lattice problems on general integer lattices.

Before going into the next result, we would like to remark that given a $\mathbb{Z}$-basis of an input lattice $\mathcal{L}$, we can derive a basis for its dual, and hence a set of generators for $\mathcal{O}_\mathcal{L}^\vee = \mathcal{L}\mathcal{L}^\vee$ (See [Conb, Rem 4.2]). Thanks to Hermite Normal Form, we therefore get a basis for $\mathcal{O}_\mathcal{L}^\vee$, and further for $\mathcal{O}_\mathcal{L}$. Moreover, as $\mathcal{C}_{\mathcal{O}_\mathcal{L}}^\vee = \mathcal{O}_K\mathcal{O}_\mathcal{L}^\vee$ ([BBPS19, Lem. 2.32]), we can get a basis for $\mathcal{C}_{\mathcal{O}_\mathcal{L}}^\vee$ and then for $\mathcal{C}_{\mathcal{O}_\mathcal{L}}$. Knowing these bases help us derive the efficient maps involved in Theorem 3.6.

Corollary 3.7. *Let K be a monogenic number field. Let $\mathcal{L} \subset K$ be a lattice such that $p\mathcal{O}_K \subseteq \mathcal{L}$, for a fixed prime p, along with its basis. Let an integer q, coprime to p, and an $\alpha \in (0, 1)$ such that $\alpha q/\|t\|_\infty \geq 2\omega(1)$. Given the primes $\mathfrak{q}_i$ containing $q\mathcal{O}_\mathcal{L}$ and $t \in \mathcal{C}_{\mathcal{O}_\mathcal{L}} \setminus \bigcup_i \mathfrak{q}_i\mathcal{C}_{\mathcal{O}_\mathcal{L}}$, there is a polynomial time quantum reduction*

$$\mathcal{L}\text{-DGS}_{\widetilde{\gamma}} \longrightarrow \mathcal{O}_K\text{-LWE}_{(q\mathcal{O}_K, 1/q), \Upsilon_\alpha}, \text{ where } \widetilde{\gamma} = max\left\{\eta(\mathcal{L}) \cdot \sqrt{2} \cdot \|t\|_\infty/\alpha \cdot \omega(1), \frac{\sqrt{2n}}{\lambda_1(\mathcal{L}^\vee)}\right\}.$$

See B.2 for a detailed proof. Observe that for the embedding $\mathcal{L}$ of an integer p-ary lattice, the approximation factor γ obtained above only makes sense as long as $\|t\|_\infty < p$. This may be achievable if $\mathcal{C}_{\mathcal{O}_\mathcal{L}}$ is a proper factor of $p\mathcal{O}_K$. We also provide in Section B.3 examples of lattices $\mathcal{L}$ and multipliers t whose infinity norm are less than p. However, the DGS problem on $\mathcal{L}$ can also be solved using either an $\mathcal{O}_\mathcal{L}$-LWE oracle or a $(\mathbb{Z} + p\mathcal{O}_K)$-LWE oracle. The approximation factor from both of these reductions is equal to γ, as in the hardness result,

Theorem 3.1, which is an improvement by $\|t\|_\infty$ from the approximation factor in the Corollary 3.7.

4 Gradients of hardness between Ring-LWE and LWE

In this section, we describe chains of Order-LWE problems that begin with the well-known Ring-LWE problem (often denoted as $\mathcal{O}_K$-LWE) and increase in hardness until they reach an Order-LWE problem that is equivalent to the unstructured LWE problem. The descending chain of orders (with respect to inclusion) creates a gradient of increasing hardness from Ring-LWE to LWE. Its relevance is two-fold; it describes a collection of orders in K such that their corresponding (Order-)LWE problems lie between Ring-LWE and LWE, the former being the most efficient and the latter, hardest and least efficient. Secondly, it instantiates the LWE problem in an algebraic avatar, as an Order-LWE problem. All the results in this section hold for both search and decision versions of the Order-LWE and LWE problems. Note that the equivalence between the LWE problem and the Order-LWE problem, Theorem 4.4, is non-uniform, since it uses as advice a special $\mathbb{Z}$-basis for the order in consideration.

To ease notation, we denote by $\mathcal{O}$-LWE$_{q,\psi}$, the Order-LWE problem for the order $\mathcal{O}$, with modulus ideal $q\mathcal{O}$, the element $u = 1/q$ and an error distribution ψ over $K_\mathbb{R}$. The following result is a building block in creating the chains. It gives an error preserving reduction between the Order-LWE problems, as long as the index of the two orders is coprime to the LWE modulus.

Theorem 4.1 ([PP19, Theorem 4.7]). *Given $\mathcal{O} \subseteq \mathcal{O}'$, an $\mathcal{O}$ ideal modulus $\mathcal{Q}$ such that it is coprime with $(\mathcal{O} : \mathcal{O}') = \{x \in K \; x\mathcal{O}' \subseteq \mathcal{O}\}$ and $u \in (\mathcal{O} : \mathcal{Q})$, there is an efficient, deterministic and error preserving reduction from (search or decision) $\mathcal{O}'$-LWE$_{(\mathcal{Q}\mathcal{O}',u),\psi}$ to (search or decision) $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\psi}$. In particular, if $\mathcal{O}'$ is the maximal order, $\mathcal{O}_K$, then we have an efficient, deterministic and error preserving reduction from $\mathcal{O}_K$-LWE$_{(\mathcal{Q}\mathcal{O}_K,u),\psi}$ to $\mathcal{O}$-LWE$_{(\mathcal{Q},u),\psi}$. Moreover, if $\mathcal{Q} = q\mathcal{O}$ and $u = 1/q$, for an integer q coprime with $[\mathcal{O}_K : \mathcal{O}]$, we have an efficient, deterministic and error preserving reduction from $\mathcal{O}_K$-LWE$_{q,\psi}$ to $\mathcal{O}$-LWE$_{q,\psi}$.*

Notice that it suffices for the ideal $\mathcal{Q}$ to be coprime with $[\mathcal{O}' : \mathcal{O}]\mathcal{O}$ in order for Theorem 4.1 to hold, as again $(\mathcal{O} : \mathcal{O}') \subseteq [\mathcal{O}' : \mathcal{O}]\mathcal{O}$. With repetitive application of Theorem 4.1, we get a chain of algebraic LWEs as follows. Let $\mathcal{L} \subset \mathcal{O}_K$ be a lattice in K. Then, $\mathcal{L}$ is an ideal of the order $\mathbb{Z} + m\mathcal{O}_K$, where m is the exponent of the quotient group $\mathcal{O}_K/\mathcal{L}$. See Lemma 2.16. The order $\mathbb{Z} + m\mathcal{O}_K$ may be strictly contained in the ring of multipliers, $\mathcal{O}_\mathcal{L}$. Hence, the inclusion, $\mathbb{Z} + m\mathcal{O}_K \subseteq \mathcal{O}_\mathcal{L} \subseteq \mathcal{O}_K$, by Theorem 4.1, implies the error preserving reduction

$$\mathcal{O}_K\text{-LWE}_{(\mathcal{Q}\mathcal{O}_K,u),\psi} \longrightarrow \mathcal{O}_\mathcal{L}\text{-LWE}_{(\mathcal{Q}\mathcal{O}_\mathcal{L},u),\psi} \longrightarrow (\mathbb{Z} + m\mathcal{O}_K)\text{-LWE}_{(\mathcal{Q},u),\psi},$$

as long as the $\mathbb{Z} + m\mathcal{O}_K$ ideal modulus $\mathcal{Q}$ is coprime to $m\mathcal{O}$. Coprimality of $\mathcal{Q}$ with $m\mathcal{O}$ is sufficient as both the indices, $[\mathcal{O}_\mathcal{L} : (\mathbb{Z}+m\mathcal{O}_K)]$ and $[\mathcal{O}_K : \mathcal{O}_\mathcal{L}]$ divide $[\mathcal{O}_K : m\mathcal{O}_K] = m^n$, owing to the fact that $m\mathcal{O}_K \subset \mathbb{Z} + m\mathcal{O}_K$ and therefore,

$\mathrm{Spec}([\mathcal{O}_\mathcal{L} : (\mathbb{Z} + m\mathcal{O}_K)]\mathcal{O}) \subseteq \mathrm{Spec}(m\mathcal{O})$ and $\mathrm{Spec}([\mathcal{O}_K : \mathcal{O}_\mathcal{L}]\mathcal{O}_\mathcal{L}) \subseteq \mathrm{Spec}(m\mathcal{O}_\mathcal{L})$. This chain of LWE problems, increasing in hardness, may be longer depending on the factorization of $m\mathcal{O}_K$ as an $\mathcal{O}_K$-ideal, as we describe in Theorem 4.2.

Let $Spec_{\mathcal{O}_K}(m\mathcal{O}_K) = \{\mathfrak{m}_1, \mathfrak{m}_2, \ldots, \mathfrak{m}_r\}$. Define $\mathcal{O}_i := \mathbb{Z} + \mathfrak{m}_1 \cdot \ldots \cdot \mathfrak{m}_i$. Then, by Lemma 2.16, each $\mathcal{O}_i$ is an order in K. Further, $\mathcal{O}_i \subset \mathcal{O}_j$, for $i \geq j$, and $\mathbb{Z} + m\mathcal{O}_K \subset \mathcal{O}_i$, for all i. By the same argument, for any lattice, $\mathcal{J} \subseteq \mathcal{O}_K$, the order $\mathbb{Z} + m\mathcal{J} \subseteq \mathbb{Z} + m\mathcal{O}_K$. This yields the following chain of orders: $\mathcal{O}_K \supseteq \mathcal{O}_1 \supseteq \cdots \supseteq \mathcal{O}_r \supseteq \mathbb{Z} + m\mathcal{O}_K \supseteq \mathbb{Z} + m\mathcal{J}$.

Theorem 4.2. *Let m be an integer and $\mathcal{J}$ be a lattice in $\mathcal{O}_K$. Let $\mathcal{Q}$ be an ideal modulus in $\mathbb{Z} + m\mathcal{J}$ such that it is coprime with $m(\mathbb{Z} + m\mathcal{J})$ and $[\mathcal{O}_K : \mathcal{J}](\mathbb{Z} + m\mathcal{J})$. Let $u \in (\mathbb{Z} + m\mathcal{J} : \mathcal{Q})$. Then, we have the following efficient, deterministic and error preserving reductions for the (search or decision) problems*

$$\mathcal{O}_K\text{-LWE}_{(\mathcal{Q}\mathcal{O}_K,u),\psi} \to \cdots \to \mathcal{O}_r\text{-LWE}_{(\mathcal{Q}\mathcal{O}_r,u),\psi} \to$$

$$(\mathbb{Z} + m\mathcal{O}_K)\text{-LWE}_{(\mathcal{Q}(\mathbb{Z}+m\mathcal{O}_K),u),\psi} \to (\mathbb{Z} + m\mathcal{J})\text{-LWE}_{(\mathcal{Q},u),\psi}.$$

In particular, for $\mathcal{Q} = q(\mathbb{Z} + m\mathcal{J})$ and $u = 1/q$, where q is a positive integer coprime with m and $[\mathcal{O}_K : \mathcal{J}]$, we have the following efficient, deterministic and error preserving reductions for the (search or decision) problems

$$\mathcal{O}_K\text{-LWE}_{q,\psi} \to \cdots \to \mathcal{O}_r\text{-LWE}_{q,\psi} \to (\mathbb{Z}+m\mathcal{O}_K)\text{-LWE}_{q,\psi} \to (\mathbb{Z}+m\mathcal{J})\text{-LWE}_{q,\psi}.$$

See C.1 for a detailed proof.

From now on, we focus on the Order-LWE problem with ideal modulus $\mathcal{Q}$ generated by a positive integer q and $u = 1/q$.

We now describe (non-maximal) orders such that the corresponding Order-LWE problems, with error sampled from a spherical Gaussian, become equivalent to the unstructured LWE problem. Suppose $\mathcal{O} \subseteq K$ be such an order. In unison with Theorem 4.2, this result yields various chains of algebraic LWEs in the field K that begin with Ring-LWE and terminate at LWE.

The $\mathbb{Z}$-bases of these special orders satisfy a particular property that we describe now. Some notation: let $\mathcal{O}$ be an order of K and a $\mathbb{Z}$-basis of it of the form $\vec{p} = \{p_0 = 1, p_1, \ldots, p_{n-1}\}$. See Lemma 2.9 for the existence of $\vec{p}$. Denote by $\vec{p}^\vee = \{p_i^\vee\}_{i=0}^{n-1}$, the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ that satisfies $Tr(p_i p_j^\vee) = \delta_{ij}$, where $Tr = Tr_{K_\mathbb{R}/\mathbb{R}}$.

Definition 4.3. *Let K be a number field of degree n and $e \in K_\mathbb{R}$ be sampled from the distribution D_α over $K_\mathbb{R}$, for some $\alpha > 0$. We say that an order $\mathcal{O}$ in K is α-**drowning** if for a $\mathbb{Z}$-basis $\vec{p}$ of $\mathcal{O}$, as described above, such that the coefficients $(e_0, e_1, \ldots, e_{n-1})$ of e with respect to the $\mathbb{Z}$-basis $\vec{p}^\vee$ of $\mathcal{O}^\vee$ satisfy the following: the marginal distribution of $e_0 \mod \mathbb{Z}$ is*

$$e_0 \mod \mathbb{Z} \leftarrow D_{\alpha\sqrt{n}} \mod \mathbb{Z},$$

and, for any $x_0 \in \mathbb{R}$, the conditional distribution,

$$(e_1, e_2, \ldots, e_{n-1}) \,|e_0 = x_0 \mod \mathbb{Z}^{n-1} \approx_{s.i} U((\mathbb{R}/\mathbb{Z})^{n-1}),$$

where $\approx_{s.i}$ means that the two distributions have statistical distance negligible in n.

Theorem 4.4. *Let K be a number field of degree n and let $\mathcal{O}$ be an α-drowning order, for $\alpha \cdot q \geq 2 \cdot \omega(1)$ and $\mathbb{Z}$ bases of $\mathcal{O}$ and $\mathcal{O}^\vee$, $\vec{p}$ and $\vec{p^\vee}$, as above. Then, the (search or decision) $\mathcal{O}$-LWE$_{q,D_\alpha}$ problem is equivalent to the (search or decision LWE$_{n,q,D_{\alpha\cdot\sqrt{n}}}$ problem.*

Proof. We first give a reduction from LWE to $\mathcal{O}$-LWE. This is the non-trivial part of the proof. As is standard, for this reduction, we define a transformation that sends uniform samples over $(\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{R}/\mathbb{Z}$ to uniform samples over $\mathcal{O}/q\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee$ and LWE samples to $\mathcal{O}$-LWE samples.

Let $Tr = Tr_{K_\mathbb{R}/\mathbb{R}}$ denote the trace map. For $i \in [n-1]$, sample uniform elements in $\mathbb{R}/\mathbb{Z}$; $u_i \leftarrow U(\mathbb{R}/\mathbb{Z})$. We define the transformation as follows: given a pair $(\vec{a}, b_0) \in (\mathbb{Z}/q\mathbb{Z})^n \times \mathbb{R}/\mathbb{Z}$, output

$$(a := a_1 p_0 + \ldots + a_n p_{n-1}, \;\; b := b_0 \; p_0^\vee + u_1 \; p_1^\vee + \ldots + u_{n-1} \; p_{n-1}^\vee) \in \mathcal{O}/q\mathcal{O} \times K_\mathbb{R}/\mathcal{O}^\vee.$$

It is straightforward to see that this transformation is well-defined and maps uniform samples from the domain to uniform samples in the range. We claim that if $b_0 = \frac{1}{q} \cdot \langle \vec{a}, \vec{s} \rangle + e$, with a secret $\vec{s} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$ and an error $e \leftarrow D_{\alpha\sqrt{n}}$, then $b \in K_\mathbb{R}/\mathcal{O}^\vee$, as defined above, is statistically indistinguishable from $b' := \frac{1}{q} \cdot a \cdot s + e' \in K_\mathbb{R}/\mathcal{O}^\vee$, where $s := \langle \vec{s}, \vec{p^\vee} \rangle = s_1 p_0^\vee + \ldots + s_n p_{n-1}^\vee \in \mathcal{O}^\vee/q\mathcal{O}^\vee$ and $e' \leftarrow D_\alpha$ over $K_\mathbb{R}$. In fact, we show that the coefficients of b are statistically indistinguishable from the coefficients of b' in the basis $\{p_i^\vee\}_i$ of $\mathcal{O}^\vee$. Notice that (a, b') is an $\mathcal{O}$-LWE$_{q,D_\alpha}$ sample with the uniformly sampled secret s, since $\vec{s} \leftarrow U((\mathbb{Z}/q\mathbb{Z})^n)$.

The linearity of the Trace map along with the equality, $Tr(p_i p_j^\vee) = \delta_{ij}$, implies that $a \cdot s = \sum_{i=0}^{n-1} Tr(a \cdot s \cdot p_i) \; p_i^\vee$, and $Tr(a \cdot s) = \sum_{i=1}^{n} a_i s_i = \langle \vec{a}, \vec{s} \rangle$. Therefore,

$$b = \frac{1}{q} \cdot \langle \vec{a}, \vec{s} \rangle \; p_0^\vee + e \; p_0^\vee + \sum_{i=1}^{n-1} u_i p_i^\vee = \left(\frac{1}{q} \cdot Tr(a \cdot s) + e \right) \cdot \; p_0^\vee + \sum_{i=1}^{n-1} u_i p_i^\vee \mod \widetilde{\mathcal{O}}^\vee,$$

whereas

$$b' = \left(\frac{1}{q} \cdot Tr(a \cdot s) + e'_0 \right) \cdot \; p_0^\vee + \sum_{i=1}^{n-1} \left(\frac{1}{q} \cdot Tr(a \cdot s \cdot p_i) + e'_i \right) \cdot p_i^\vee \mod \mathcal{O}^\vee.$$

Here, $e' = \sum_{i=0}^{n-1} e'_i \; p_i^\vee$ is the representation of the error (from the $\mathcal{O}$-LWE sample) in the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$. Since $\mathcal{O}$ is α-drowning, the marginal distribution of $e_0 \mod \mathbb{Z}$ is $D_{\alpha\sqrt{n}} \mod \mathbb{Z}$, whereas the conditional distribution of $(e'_1, \ldots, e'_{n-1}) | e'_0$ equals $x_0 \mod \mathbb{Z}^{n-1}$ is statistically indistinguishable from $U((\mathbb{R}/\mathbb{Z})^{n-1})$, for any $x_0 \in \mathbb{R}$. This shows that $(e'_0, e'_1, \ldots, e'_{n-1}) \mod \mathbb{Z}^n$ is statistically indistinguishable from $(e, u_1, \ldots, u_{n-1}) \mod \mathbb{Z}^n \leftarrow (D_{\alpha\sqrt{n}} \mod \mathbb{Z}) \times U((\mathbb{R}/\mathbb{Z})^{n-1})$. Therefore, the coefficients of b and of b' with respect to the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$ are statistically indistinguishable, as desired.

The converse, from $\mathcal{O}$-LWE to LWE, is a special case of [PP19, Thm 6.1]. □

Examples of α-drowning orders. We describe two orders and prove in Proposition 4.5 below that they are α-drowning, for an $\alpha > 0$ satisfying $\alpha \cdot q > 2 \cdot \omega(1)$ and well chosen positive integer m.

(*i*) For a number field K, let $\{1, \theta_1, \ldots, \theta_{n-1}\}$ be a fixed $\mathbb{Z}$-basis for $\mathcal{O}_K$. See Lemma 2.9 for its existence. For a $d \times d$ matrix M, let $e_d(M)$ denote the smallest eigenvalue of M. Let $\tau := e_{n-1}(T)$, where $T = (Tr(\theta_i\overline{\theta_j}) - \frac{1}{n} \cdot Tr(\theta_i)Tr(\theta_j))_{1 \le i,j \le n-1}$. Choose $r \in \mathbb{N}$ such that $\tau \cdot m^{2r-2} \ge n$. Let $\widetilde{\mathcal{O}} := \mathbb{Z} + m^r\mathcal{O}_K$. Then, a $\mathbb{Z}$-basis for $\widetilde{\mathcal{O}}$ is $\vec{p} := (p_i)_{i=0}^{n-1} = \{1, m^r\theta_1, \ldots, m^r\theta_{n-1}\}$. Let $\vec{p}^{\vee} = (p_0^{\vee}, p_1^{\vee}, \ldots, p_{n-1}^{\vee})$ be the (dual) $\mathbb{Z}$-basis for $\widetilde{\mathcal{O}}^{\vee}$. Then, for $\alpha > 0$ satisfying $\alpha \cdot q \ge 2\omega(1)$, the order $\widetilde{\mathcal{O}}$ **is α-drowning**. When $\mathcal{O}_K$ has an orthogonal $\mathbb{Z}$-basis containing 1, then the matrix T is a diagonal matrix with $\tau = e_{n-1}(T) \ge \sqrt{n}$. Therefore, the condition $\tau \cdot m^{2r-2} \ge n$ is achieved with $r = 1$. See Remark A.6.

(*ii*) In fields that are closed under complex conjugation, i.e. $\overline{K} \subseteq K$, one may be able to choose a smaller order $\widetilde{\mathcal{O}}'$ **that is α-drowning**. Note that all Galois fields and totally real number fields are closed under complex conjugation. As $\overline{K} \subseteq K$, we get that $Tr_{K/\mathbb{Q}}(x\overline{y}) \in \mathbb{Q}$, for $x, y \in K$. Therefore, by repeated application of [Cona, Lem. 4.6], $K = \mathbb{Q}\cdot 1 \oplus \mathbb{Q}\cdot\theta_1' \oplus \ldots \oplus \mathbb{Q}\cdot\theta_{n-1}'$, decomposes orthogonally into $\mathbb{Q}$ vector subspaces, for $\theta_i' \in K$. Consider the $\mathbb{Z}$-module generated by this orthogonal basis and call it $\mathcal{J}$. It is a full-rank lattice and hence an ideal in its ring of multipliers. We multiply by the integer scalar m to make sure that $\mathcal{J}$ is an integral ideal. Then, by Lemma 2.16, the set $\widetilde{\mathcal{O}}' := \mathbb{Z} + m\mathcal{J}$ is an order, generated by $\vec{p'} = (p_i')_{i=0}^{n-1} := \{1, m\theta_1', \ldots, m\theta_{n-1}'\}$ over $\mathbb{Z}$. Let $\vec{p}^{'\vee} = \{p_i^{'\vee}\}_{i=0}^{n-1}$ be the corresponding $\mathbb{Z}$-basis for $\widetilde{\mathcal{O}}^{'\vee}$.

Recall that, when $e \leftarrow D_\alpha$ over $K_\mathbb{R}$, the coefficients $(e_0, e_1, \ldots e_{n-1})$ of e, with respect to the $\mathbb{Z}$-basis of the dual of the order in consideration, call it $\mathcal{O}$, follow the Gaussian distribution of covariance matrix $\alpha^2 \cdot P_{\mathcal{O}}$. (See Lemma 2.32.) To prove that this order is α-drowning, we show that the $n-1 \times n-1$ covariance matrix of the conditional distribution of the coefficients $(e_1, \ldots e_{n-1})$ satisfies that the smallest singular value of its square root exceeds the smoothing parameter of $\mathbb{Z}^{n-1}$. This implies that given any value for e_0, the tuple $(e_1, \ldots e_{n-1}) \mod \mathbb{Z}^{n-1}$ is indistinguishable from a uniform element in $(\mathbb{R}/\mathbb{Z})^{n-1}$, by Lemma A.2. We also show that $e_0 \mod \mathbb{Z} \leftarrow D_{\alpha\sqrt{n}}$.

Proposition 4.5. *Let K be a number field of degree n and m be an integer greater than q. Then, for $\alpha > 0$ satisfying $\alpha \cdot q > 2 \cdot \omega(1)$,*

(i) $\widetilde{\mathcal{O}}$ is an α-drowning order;
(ii) when $\overline{K} \subseteq K$, the order $\widetilde{\mathcal{O}}'$ is α-drowning.

Proof. For both the cases, let $X_a := e_0$ and $X_b := (e_1, e_2, \ldots, e_{n-1})$. The covariance matrix for the appropriate order $\mathcal{O} = \widetilde{\mathcal{O}}$ or $\widetilde{\mathcal{O}}'$ can be expressed as,

$$\alpha^2 P_{\mathcal{O}} = \alpha^2 \left(Tr(p_i\overline{p_j})\right)_{ij} = \alpha^2 \begin{pmatrix} \Sigma_{aa} & \Sigma_{ab} \\ \Sigma_{ba} & \Sigma_{bb} \end{pmatrix},$$

where $\Sigma_{aa} \in M_{1\times 1}(\mathbb{R})$, $\Sigma_{bb} \in M_{n-1\times n-1}(\mathbb{R})$, and the matrices $\Sigma_{ab} = \Sigma_{ba}^t \in M_{1\times n-1}(\mathbb{R})$. The marginal distribution of X_a is a Gaussian distribution over $\mathbb{R}$ of covariance matrix $\alpha^2 \cdot \Sigma_{aa} = \alpha^2 \cdot Tr(p_0\overline{p_0}) = \alpha^2 \cdot n$. The conditional distribution of $X_b|X_a = x_0$ is a Gaussian distribution over $\mathbb{R}^{n-1}$ of mean $x_0\alpha^2\Sigma_{ba}(\alpha^2\Sigma_{aa})^{-1} = \frac{x_0}{n} \cdot \Sigma_{ba}$ and of covariance matrix $\alpha^2\left(\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}\right)$.

Proof of (i) When $\mathcal{O} = \widetilde{\mathcal{O}}$, the covariance matrix $\alpha^2\left(\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}\right) = \alpha^2 \cdot m^{2r} \cdot T$, where T was defined above. As r was chosen such that $\tau \cdot m^{2r-2} \geq n$, for $\tau = e_{n-1}(T)$, the smallest singular value, $s_{n-1}(\sqrt{T})$, of $\sqrt{T}$ equals $\sqrt{\tau}$, and

$$\alpha \cdot m^r \cdot s_{n-1}(\sqrt{T}) \geq \alpha \cdot m^r \cdot \sqrt{\tau} \geq \alpha \cdot m \cdot \sqrt{n} \geq \omega(1) \cdot \sqrt{n} > \eta(\mathbb{Z}^{n-1}).$$

The last inequality follows from the fact that $\eta(\mathbb{Z}^{n-1}) < \sqrt{n}$, for $\varepsilon = (e^{\pi n}/(2n-2)-1)^{-1}$. See Lemma A.3. Thus, since $\alpha^2 \cdot m^{2r} \cdot T \geq \alpha^2 \cdot m^{2r} \cdot s_{n-1}(\sqrt{T})^2$, by Lemma A.2, the distribution of $X_b|X_a = x_0 \bmod \mathbb{Z}^{n-1}$ is ε-close to the uniform distribution $U((\mathbb{R}/\mathbb{Z})^{n-1})$. Recall that, given symmetric matrices A, B, the standard notation $A \geq B$ means that $A - B$ is a positive semi-definite matrix. This proves the result.

Proof of (ii) When $\mathcal{O} = \widetilde{\mathcal{O}}'$, the $\mathbb{Z}$-basis $\vec{p'}$ is orthogonal. Therefore, the covariance matrix

$$\alpha^2\left(\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}\right) = \alpha^2 \cdot diag(m^2\|\theta_1'\|^2, \ldots, m^2\|\theta_{n-1}'\|^2).$$

Now, for $1 \leq i \leq n-1$, each e_i is an independent variable drawn from $D_{\sqrt{\alpha_i}}$, with $\alpha_i = \alpha^2 \cdot m^2\|\theta_i'\|^2$. As $\theta_i' \in \mathcal{O}_K$, $\|\theta_i'\| \geq \sqrt{n}$. (by Remark A.6.) Hence,

$$e_i \mod \mathbb{Z} \leftarrow D_{\sqrt{\alpha_i}} \mod \mathbb{Z} \quad \text{for } \sqrt{\alpha_i} \geq \alpha \cdot m \cdot \sqrt{n}.$$

Under the assumption on α and the fact that $m \geq q$, for $i > 0$, the parameter $\sqrt{\alpha_i} > \eta(\mathbb{Z})$. The last inequality follows from the fact that $\eta(\mathbb{Z}) < \sqrt{n}$, for $\varepsilon = (e^{\pi n}/2-1)^{-1}$. See Lemma A.3. Finally, by Lemma A.2, the distribution $D_{\sqrt{\alpha_i}} \bmod \mathbb{Z}$, for $i > 0$, is statistically ε-close to the uniform distribution $U(\mathbb{R}/\mathbb{Z})$. This proves the result. □

Remark 4.6. The parameters $m \geq q$ in Theorem 4.4 cannot satisfy $m \gg q$, as the Order-LWE problem would become trivially impossible to solve. This is because when $m \gg q$, the error parameter $\alpha > \frac{2\omega(1)}{q} \gg \frac{1}{m}$ is greater than the smoothing parameter of $(\mathbb{Z} + m\mathcal{O}_K)^\vee$, thereby making the second coordinate from the $(\mathbb{Z} + m\mathcal{O}_K)$-LWE problem, $b \in K_\mathbb{R}/(\mathbb{Z} + m\mathcal{O}_K)^\vee$, indistinguishable from uniform.

The α-drowning orders from Proposition 4.5 are particularly easy to describe in the case of the power-of-two cyclotomic extensions. See C.2 for a proof.

Corollary 4.7. *Let $K = \mathbb{Q}(\zeta_{2n})$ be a power of two cyclotomic extension. Let m and q be distinct integers, with $m \geq q$. Let $\alpha \in (0,1)$ be such that $\alpha \cdot q \geq 2 \cdot \omega(1)$. Then, for $\widetilde{\mathcal{O}} := \mathbb{Z} + m\mathcal{O}_K$, the problems $\widetilde{\mathcal{O}}$-$\mathrm{LWE}_{q,D_\alpha}$ and $\mathrm{LWE}_{n,q,D_{\alpha\cdot\sqrt{n}}}$ are equivalent.*

Acknowledgements. We thank the anonymous referees for their useful comments and suggestions.

Bibliography

[Ajt96] M. Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of STOC*, pages 99–108. ACM, 1996.

[Ban93] W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993.

[BBPS19] M. Bolboceanu, Z. Brakerski, R. Perlman, and D. Sharma. Order-lwe and the hardness of ring-lwe with entropic secrets. In *Proceedings of ASIACRYPT*, pages 91–120, 2019.

[BGP22] K. Boudgoust, E. Gachon, and A. Pellet-Mary. Some easy instances of ideal-svp and implications on the partial vandermonde knapsack problem. In *Proceedings of Crypto*, pages 480–509, 2022.

[Bla20] I Blanco-Chacón. On the rlwe/plwe equivalence for cyclotomic number fields. applicable algebra in engineering, communication and computing. pages 1–19, 2020.

[BLNRL22] O. Bernard, A. Lesavourey, T-H Nguyen, and A. Roux-Langlois. Log-s-unit lattices using explicit stickelberger generators to solve approx ideal-svp. In *Proceedings of Asiacrypt*, pages 677–708, 2022.

[BRL20] O. Bernard and A. Roux-Langlois. Twisted-phs: Using the product formula to solve approx-svp in ideal lattices. In *Proceedings of Asiacrypt*, page 349–380, 2020.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *Proceedings of EUROCRYPT*, pages 559–585, 2016.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. Short stickelberger class relations and application to ideal-svp. In *Proceedings of EUROCRYPT*, pages 324–348, 2017.

[CGS] P. Campbell, M. Groves, and D. Sheperd. Soliloquy: A cautionary tale. ETSI 2nd quantum-safe crypto workshop, 2014 https://docbox.etsi.org/workshop/2014/201410_CRYPTO/S07_Systems_and_Attacks/S07_Groves_Annex.pdf.

[Chu] T. Church. Math 210a: Modern algebra. Expository papers/Lecture notes. Available at: http://math.stanford.edu/~church/teaching/210A-F17/math210A-F17-hw3-sols.pdf.

[Cona] K. Conrad. Bilinear forms. https://kconrad.math.uconn.edu/blurbs/linmultialg/bilinearform.pdf.

[Conb] K. Conrad. The conductor ideal. https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf.

[Conc] K. Conrad. The different ideal. https://kconrad.math.uconn.edu/blurbs/gradnumthy/different.pdf.

[Cond] K. Conrad. Ideal factorization. https://kconrad.math.uconn.edu/blurbs/gradnumthy/idealfactor.pdf.

[DF91] D. S. Dummit and R. M. Foote. *Abstract Algebra*. Prentice Hall, 1991.

[DPW19] L. Ducas, M. Plançon, and B. Wesolowski. On the shortness of vectors to be found by the ideal-svp quantum algorithm. In *Proceedings of CRYPTO*, pages 322–351, 2019.

[HPS98] J. Hoffstein, J. Pipher, and J. H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS*, pages 267–288, 1998.

[JL22] C.S Jutla and C. Lin. Enhancing ring-lwe hardness using dedekind index theorem. 2022. https://eprint.iacr.org/2022/1631.

[LM06] V. Lyubashevsky and D. Micciancio. Generalized compact knapsacks are collision resistant. In *Proceedings of ICALP*, pages 144–155, 2006.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In *Proceedings of EUROCRYPT*, pages 1–23, 2010.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-lwe cryptography. In *Proceedings of EUROCRYPT*, pages 35–54, 2013.

[LS12] A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *IACR Cryptol. ePrint Arch.*, 2012:90, 2012.

[MR07] D. Micciancio and O. Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.

[Neu99] J. Neukirch. *Algebraic Number Theory*. 1999.

[Pei10] C. Peikert. An efficient and parallel gaussian sampler for lattices. In *Annual Cryptology Conference*, pages 80–97. Springer, 2010.

[Pei16] C. Peikert. A decade of lattice cryptography. *Found. Trends Theor. Comput. Sci.*, 10(4):283–424, 2016.

[PHS19] A. Pellet-Mary, G. Hanrot, and D. Stehlé. Approx-svp in ideal lattices with pre-processing. In *Proceedings of EUROCRYPT*, pages 685–716, 2019.

[PP19] C. Peikert and Z. Pepin. Algebraically structured lwe, revisited. In *Proceedings of TCC*, pages 1–23, 2019.

[PR06] C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In *Proceedings of TCC*, pages 145–166, 2006.

[PRSD17] C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. *IACR Cryptology ePrint Archive*, 2017:258, 2017.

[PXWC21] Y. Pan, J. Xu, N. Wadleigh, and Q. Cheng. On the ideal shortest vector problem over random rational primes. In *Proceedings of EUROCRYPT*, pages 559–583, 2021.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *STOC*, pages 84–93, 2005. Full version in [Reg09].

[Reg09] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.

[RSSS17] M. Rosca, A. Sakzad, D. Stehlé, and R. Steinfeld. Middle-product learning with errors. In *Proceedings of CRYPTO*, pages 283–297, 2017.

[RSW18] M. Rosca, D. Stehlé, and A. Wallet. On the ring-lwe and polynomial-lwe problems. In *Proceedings of EUROCRYPT*, pages 146–173, 2018.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *Proceedings of ASIACRYPT*, pages 617–635, 2009.

[Ste08] P. Stevenhagen. *The arithmetic of number rings*. 2008.

[Was83] L. C. Washington. *Introduction to Cyclotomic Fields*. 1983.

[Was04] L. Wasserman. *All of Statistics: A Concise Course in Statistical Inference*. Springer Texts in Statistics. Springer, 2004.

Appendix

A Additional definitions

A.1 More about space H

As a real vector space, it has a special orthonormal basis $(\mathbf{h}_i)_{1\leq i\leq n}$ given by the columns of the following matrix:

$$B = \begin{pmatrix} \mathrm{Id}_{s_1\times s_1} & 0 & 0 \\ 0 & \frac{1}{\sqrt{2}}\mathrm{Id}_{s_2\times s_2} & \frac{i}{\sqrt{2}}\mathrm{Id}_{s_2\times s_2} \\ 0 & \frac{1}{\sqrt{2}}\mathrm{Id}_{s_2\times s_2} & \frac{-i}{\sqrt{2}}\mathrm{Id}_{s_2\times s_2} \end{pmatrix}$$

A.2 Properties of Gaussian and smoothing parameters

Proposition A.1. *[Was04, Thm 2.44] Let X be a Gaussian vector over $\mathbb{R}^n$ of covariance matrix Σ. Suppose X splits as $X = (X_a, X_b)$ and its covariance matrix is written accordingly as:*

$$\Sigma = \begin{pmatrix} \Sigma_{aa} & \Sigma_{ab} \\ \Sigma_{ba} & \Sigma_{bb} \end{pmatrix}.$$

Then,
i) the marginal distribution of X_a is a Gaussian distribution of covariance matrix Σ_{aa}, and
ii) the conditional distribution of X_b, given the value for X_a as x_a, is a Gaussian distribution of covariance matrix $\Sigma_{bb} - \Sigma_{ba}\Sigma_{aa}^{-1}\Sigma_{ab}$ and mean $\Sigma_{ba}\Sigma_{aa}^{-1}x_a$.

Lemma A.2. *[MR07, Lem.4.1] If $\mathcal{L}$ is a full-rank lattice in $\mathbb{R}^n$, $\varepsilon \in (0,1)$ and $\sqrt{\Sigma} \geq \eta_\varepsilon(\mathcal{L})$, then the statistical distance between $D_{\sqrt{\Sigma}}$ mod $\mathcal{L}$ and the uniform distribution over $\mathbb{R}^n/\mathcal{L}$ is at most $\varepsilon/2$.*

Lemma A.3. *Let $\mathcal{L}$ be a full-rank lattice in V. Then the following hold:*

(i) [MR07, Lem 3.2, 3.3] $\eta_\varepsilon(\mathcal{L}) \leq \frac{\sqrt{n}}{\lambda_1(\mathcal{L}^*)}$, for $\varepsilon = 2^{-\Omega(n)}$. Moreover, for any positive $\varepsilon > 0$, $\eta_\varepsilon(\mathcal{L}) \leq \sqrt{\frac{ln(2n(1+1/\varepsilon))}{\pi}} \cdot \lambda_n(\mathcal{L})$.

(ii) [Reg09, Claim 2.13] $\eta_\varepsilon(\mathcal{L}) \geq \sqrt{\frac{ln(1/\varepsilon)}{\pi}} \cdot \frac{1}{\lambda_1(\mathcal{L}^*)}$, for any $\varepsilon \in (0,1)$.

From Lemma A.3 (i), (ii), we deduce that for $\varepsilon = e^{-n}$, $\eta_\varepsilon(\mathcal{L}) = \frac{\theta(\sqrt{n})}{\lambda_1(\mathcal{L}^*)}$.

A.3 Proof of Lemma 2.9

Proof. Let the notation $A \xrightarrow{\phi} B \xrightarrow{\psi} C$ mean that $\phi(A) \subseteq \ker(\psi) := \{b \in B : \psi(b) = 0\}$, for A, B, C as $\mathbb{Z}$ modules. Then, the following is a short exact sequence of $\mathbb{Z}$-modules, where the second map is inclusion and the third map is the projection.

$$0 \to \mathbb{Z} \to \mathcal{O} \to \mathcal{O}/\mathbb{Z} \to 0$$

To prove the claim, it suffices to show that $\mathcal{O}/\mathbb{Z}$ is a torsion free $\mathbb{Z}$-module, and hence a free $\mathbb{Z}$-module, [DF91, Chapter 12.1, Thm 5], as that would imply that the above sequence splits, i.e., $\mathcal{O} = \mathbb{Z} \oplus \mathcal{O}/\mathbb{Z}$. See [Chu, Lem. 2]. Then, a $\mathbb{Z}$-basis for $\mathcal{O}$ is the union of a $\mathbb{Z}$-basis for $\mathcal{O}/\mathbb{Z}$ and 1, a $\mathbb{Z}$-basis for $\mathbb{Z}$.

Finally, in order to see that $\mathcal{O}/\mathbb{Z}$ is torsion free, assume, to the contrary, that there is a non-zero $x \in \mathcal{O}/\mathbb{Z}$, such that $mx = 0 \mod \mathbb{Z}$. Then $x \in \frac{1}{m}\mathbb{Z} \cap \mathcal{O} \subseteq \mathbb{Q} \cap \mathcal{O}_K = \mathbb{Z}$, by definition of the ring of integers $\mathcal{O}_K$. □

A.4 Supplementary algebraic number theory preliminaries

The *sum* of two ideals $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}$ is defined by $\mathcal{I} + \mathcal{J} := \{x + y \mid x \in \mathcal{I}, y \in \mathcal{J}\}$, and their *product* is defined by $\mathcal{I} \cdot \mathcal{J} := \{\sum x_i y_i \mid x_i \in \mathcal{I}, y_i \in \mathcal{J}\}$. Their *intersection* is simply their set theoretic intersection, and their *quotient* is defined by $(\mathcal{I} : \mathcal{J}) := \{x \in K \mid x\mathcal{J} \subseteq \mathcal{I}\}$. All of the former sets are ideals in $\mathcal{O}$.

An integral ideal $\mathfrak{p} \subset \mathcal{O}$ is *prime* if for every pair of elements $x, y \in \mathcal{O}$, whenever $xy \in \mathfrak{p}$, then either $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$. Every integral ideal $\mathcal{I}$ of $\mathcal{O}$ contains a product of prime ideals $\mathcal{I} \supseteq \prod \mathfrak{p}_i$. For an integral ideal $\mathcal{I} \subseteq \mathcal{O}$, the set of *associated primes* of $\mathcal{I}$ is the set of all prime ideals of $\mathcal{O}$ that contain $\mathcal{I}$. We state the well-known Chinese Remainder Theorem.

Theorem A.4 (Chinese Remainder Theorem). *Let $\mathcal{I}$ be a fractional ideal over an order $\mathcal{O}$ and $\mathcal{J}_1, \mathcal{J}_2, \ldots, \mathcal{J}_l$ pairwise coprime $\mathcal{O}$-ideals. Then the canonical map of $\mathcal{O}$-modules*

$$\mathcal{I}/\prod_i \mathcal{I}\mathcal{J}_i \to \bigoplus_i \mathcal{I}/\mathcal{I}\mathcal{J}_i$$

is an isomorphism.

The *norm* of an ideal $\mathcal{I} \subset \mathcal{O}$ is its index as a subgroup of $\mathcal{O}$, i.e. $N(\mathcal{I}) := [\mathcal{O} : \mathcal{I}] = |\mathcal{O}/\mathcal{I}|$. For the special case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order, the norm is a multiplicative function, i.e. $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I}) \cdot N(\mathcal{J})$ for any integral $\mathcal{I}, \mathcal{J}$. A *fractional ideal* $\mathcal{I} \subset K$ of $\mathcal{O}$ is a set such that $d\mathcal{I} \subset \mathcal{O}$ for some $d \in \mathcal{O}$. We define its norm to be $N(\mathcal{I}) := N(d\mathcal{I})/|N(d)|$. Note that for any fractional ideals $\mathcal{I}, \mathcal{J}$, their sum, product, quotient and intersection are again fractional ideals.

The next lemma shows a bound on the (Euclidean) norm on short vectors in lattices in a number field K.

Lemma A.5 ([BBPS19, Lem 2.21]). *Let K be a number field of degree n and $\mathcal{I}$ an ideal over an order $\mathcal{O}$. Then*

$$\sqrt{n} \cdot N(\mathcal{I})^{1/n} \leq \lambda_1(\mathcal{I}).$$

Remark A.6. Since every order $\mathcal{O}$ contains 1, it follows that $\lambda_1(\mathcal{O}) \leq \sqrt{n}$. On the other hand, the first part in the inequality of Lemma A.5 tells that $\lambda_1(\mathcal{O}) \geq \sqrt{n}$, since $N(\mathcal{O}) = 1$. This proves that $\lambda_1(\mathcal{O})$ is exactly $\sqrt{n}$.

Duality Given a basis $(b_i)_{1 \leq i \leq n}$ of $\mathcal{L}$, a basis $(b_i^\vee)_{1 \leq i \leq n}$ of $\mathcal{L}^\vee$ can be found by considering $Tr(b_i \cdot b_j^\vee) = \delta_{ij}$, for any $1 \leq i, j \leq n$. When $\mathcal{L}$ is a fractional ideal over an order $\mathcal{O}$, it follows that $\mathcal{L}^\vee$ is also a fractional ideal over $\mathcal{O}$. We recall briefly some properties of duality:

Proposition A.7 ([Conc, Section 3], [Conb, Section 4]). *For any two lattices $\mathcal{I}$ and $\mathcal{J}$ in a number field K:*
i) $(\mathcal{I}^\vee)^\vee = \mathcal{I}$.
ii) if $\mathcal{I} \subset \mathcal{J}$, then $\mathcal{J}^\vee \subset \mathcal{I}^\vee$.
iii) if $\mathcal{I}$ is an $\mathcal{O}$ ideal, then $\mathcal{I} \cdot \mathcal{I}^\vee = \{x \in K | x\mathcal{I} \subseteq \mathcal{I}\}^\vee \subseteq \mathcal{O}^\vee$. $\mathcal{I} \cdot \mathcal{I}^\vee = \mathcal{O}^\vee$ if $\mathcal{O} = \mathcal{O}_\mathcal{I}$. If $\mathcal{O} = \mathcal{O}_K$, equality holds for any $\mathcal{I}$.
iv) if $\mathcal{I}, \mathcal{J}$ are ideals over $\mathcal{O}$ and $\mathcal{I}$ is invertible, then $(\mathcal{I}\mathcal{J})^\vee = \mathcal{I}^{-1}\mathcal{J}^\vee$.

A.5 Proof of Lemma 2.14

Recall that coef is the coefficient embedding and σ is the canonical embedding and they are related by the Vandermonde matrix V_f, as $V_f \cdot \text{coef}(a) = \sigma(a)$, for any $a \in K$. For more details on these two embeddings and the distortion between them, one can check [RSW18, Sec.4.2] and [Bla20, Sec.2.2.3]. For proving Lemma 2.14, we need to see how the canonical embedding distorts the Euclidean norm:

Lemma A.8. *Let $\mathcal{L}$ be the image of L in K, under the coefficient embedding, with respect to $\vec{\theta}$. Then, for any $a \in K$,*

$$s_n(V_f) \cdot \|coef(a)\| \leq \|\sigma(a)\| \leq s_1(V_f) \cdot \|coef(a)\|.$$

Proof. The proof follows easily from the definition of the singular values. Since $\sigma(a) = V_f \cdot \text{coef}(a)$, the norm

$$\|a\| := \|\sigma(a)\| = \|V_f \cdot \text{coef}(a)\| \leq \|V_f\| \cdot \|\text{coef}(a)\| = s_1(V_f) \cdot \|\text{coef}(a)\|.$$

The converse follows similarly, using $\mathrm{coef}(a) = V_f^{-1} \cdot \sigma(a)$ and $\|V_f^{-1}\| = 1/s_n(V_f)$.

The following result follows easily from properties of Gaussian distributions. We state it for the sake of completeness.

Lemma A.9. *Let $K = \mathbb{Q}(\theta)$ be a number field of degree n. If $e = e_0 + e_1\theta + \ldots + e_{n-1}\theta^{n-1}$ drawn from D_α over $K_\mathbb{R}$ then $(e_0, e_1, \ldots, e_{n-1})$ satisfies the distribution $D_{\alpha\sqrt{(Vf^* Vf)^{-1}}}$ over $\mathbb{R}^n$, where V_f is the Vandermonde matrix corresponding to the roots of θ. In the special case, when K is the power-of-two cyclotomic extension, the error distribution simplifies to $D_{\alpha\sqrt{(Vf^* Vf)^{-1}}} = D_{\alpha/\sqrt{n}}$.*

Proof of Lemma 2.14 *i*) By definition of the coefficient embedding, $x \in \mathcal{L}$ if and only if $\vec{x} := \mathrm{coef}(x) \in L$. If $\|x\| = \lambda_1(\mathcal{L})$, then by Lemma A.8,

$$\lambda_1(L) \leq \|\vec{x}\| \leq \|x\|/s_n(V_f) = \lambda_1(\mathcal{L})/s_n(V_f).$$

Conversely, let $\vec{y} \in L$ and let $y \in \mathcal{L}$ be such that $\vec{y} = \mathrm{coef}(y)$. If $\|\vec{y}\| = \lambda_1(L)$, then

$$\lambda_1(\mathcal{L}) \leq \|y\| \leq s_1(V_f) \cdot \|\vec{y}\| = s_1(V_f) \cdot \lambda_1(L).$$

ii) Let $x = x_0 + x_1\theta + \ldots + x_{n-1}\theta^{n-1}$ be sampled from the Gaussian distribution D_α over $K_\mathbb{R}$. Then, by Lemma A.9, the coefficients, $\vec{x} := (x_0, x_1, \ldots, x_{n-1}) \leftarrow D_{\alpha\cdot\sqrt{(V_f^* V_f)^{-1}}}$ over $\mathbb{R}^n$. The definition of the coefficient and the Minkowski embedding implies that $D_\alpha(x) = D_\alpha(V_f \cdot \vec{x}) = D_{\alpha\sqrt{(V_f^* V_f)^{-1}}}(\vec{x})$, for all $x \in \mathcal{L}$. It further implies that $\sum_{x\in\mathcal{L}} \rho_\alpha(x) = \sum_{\vec{x}\in L} \rho_{\alpha\sqrt{(V_f^* V_f)^{-1}}}(\vec{x})$. Therefore, the two discrete Gaussians coincide:

$$D_{\mathcal{L},\alpha} \equiv D_{L,\alpha\sqrt{(V_f^* V_f)^{-1}}}.$$

This observation lies at the heart of the equivalence stated in the proposition. The reduction from $\mathcal{L}$-$\mathtt{DGS}_\alpha$ to L-$\mathtt{DGS}_{\alpha\cdot\sqrt{V_f^{-1}(V_f^{-1})^*}}$ is described by an algorithm that takes as input a lattice $\mathcal{L} \subset K$ and outputs discrete Gaussian samples over $\mathcal{L}$, by using a $\mathtt{DGS}$ sampler for the lattice $L = V_f^{-1} \cdot \sigma(\mathcal{L})$ in $\mathbb{Z}^n$, as follows. Let $\vec{x} \leftarrow D_{L,\alpha\sqrt{(V_f^* V_f)^{-1}}}$, then $x := \langle \vec{x}, \vec{\theta} \rangle \in \mathcal{L}$ follows the distribution $D_{\mathcal{L},\alpha}$. The converse reduction is realized by a similar argument. □

A.6 Proof of Lemma 2.16

Proof. Since $\mathcal{I}$ is an ideal and hence, in particular, an additive group of rank n, the set $\mathbb{Z} + \mathcal{I}$ is an additive group of rank n. It is also clear that it is a subgroup of $\mathcal{O}$ and contains 1. To see that it is a ring, let $z_1 + i_1$ and $z_2 + i_2$ be two elements in $\mathbb{Z} + \mathcal{I}$. Then,

$$(z_1 + i_1)(z_2 + i_2) = z_1 z_2 + [i_1(z_2 + i_2) + z_1 i_2] \in \mathbb{Z} + \mathcal{I},$$

as $\mathcal{I}$ is closed under scalar multiplication by elements $(z_2 + i_2)$, $z_1 \in \mathcal{O}$.

Since $m\mathcal{O}$ is an ideal of $\mathcal{O}$, it follows by what we just proved that $\mathbb{Z} + m\mathcal{O}$ is an order. Recall that the exponent e of a group G is the smallest positive integer such that $e \cdot g = 0$, for all $g \in G$. In particular, this shows that since m is the exponent of the (additive) group $\mathcal{O}/\mathcal{L}$, $m\mathcal{O} \subseteq \mathcal{L}$. To prove that $\mathcal{L}$ is an ideal of $\mathbb{Z} + m\mathcal{O}$, we show that $\mathcal{L}$ is closed under scalar multiplication by elements in $\mathbb{Z} + m\mathcal{O}$, or equivalently, by elements in $m\mathcal{O}$. Using the fact that $m\mathcal{O} \subseteq \mathcal{L}$ and that $\mathcal{L} \subseteq \mathcal{O}$, we get that $m\mathcal{O} \cdot \mathcal{L} \subseteq m\mathcal{O} \cdot \mathcal{O} \subseteq m\mathcal{O} \subseteq \mathcal{L}$. □

A.7 Localization facts

We only describe the results used in the next section. To understand the concept of localization more thoroughly, we refer the reader to [Neu99, Ch. 1].

Definition A.10. *Let $\mathfrak{p}$ be a prime ideal of an order $\mathcal{O}$. Localization of $\mathcal{O}$ at $\mathfrak{p}$ is defined as the following set*

$$\mathcal{O}_{\mathfrak{p}} = \left\{ \frac{r}{s} |\ r \in \mathcal{O},\ s \notin \mathfrak{p} \right\}.$$

It is straightforward to check that $\mathcal{O}_{\mathfrak{p}}$ is a ring. Further, it has a unique maximal ideal, namely $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$, and therefore is a *local* ring. The complement of the unique maximal ideal is the group of units, $\mathcal{O}_{\mathfrak{p}}^* := \left\{ \frac{r}{s} |\ r, s \notin \mathfrak{p} \right\}$. The ideals of $\mathcal{O}_{\mathfrak{p}}$ are the sets $\mathcal{I}\mathcal{O}_{\mathfrak{p}} = \left\{ \frac{r}{s} |\ r \in \mathcal{I},\ s \notin \mathfrak{p} \right\}$, for any ideal $\mathcal{I}$ of $\mathcal{O}$. Notice that for ideals $\mathcal{I}$ such that $\mathcal{I} \nsubseteq \mathfrak{p}$, we have $1 \in \mathcal{I}_{\mathfrak{p}}$, hence $\mathcal{I}\mathcal{O}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}$. Localization also behaves nicely when performing ideal operations. In particular, for any fractional $\mathcal{O}$-ideals $\mathcal{I}$ and $\mathcal{J}$ and a prime $\mathcal{O}$-ideal $\mathfrak{p}$, $(\mathcal{I}\mathcal{J})_{\mathfrak{p}} = \mathcal{I}_{\mathfrak{p}}\mathcal{J}_{\mathfrak{p}}$ and $(\mathcal{I}/\mathcal{J})_{\mathfrak{p}} \simeq \mathcal{I}_{\mathfrak{p}}/\mathcal{J}_{\mathfrak{p}}$. Moreover, we can extend $\mathcal{O}$-module maps $f : \mathcal{I} \to \mathcal{J}$ to maps $f_{\mathfrak{p}} : \mathcal{I}_{\mathfrak{p}} \to \mathcal{J}_{\mathfrak{p}}$ as $f_{\mathfrak{p}}(r/s) := f(r)/s$.

We recall that if $\mathfrak{p}$ is an invertible prime ideal, then $\mathcal{O}_{\mathfrak{p}}$ is a Discrete Valuation Ring, and hence a Unique Factorization Domain, i.e. any proper ideal of it can be written as a unique product of prime ideals. ([Ste08, Prop 5.4], [DF91, Chapter 8.3,Thm 12])

A.8 Proof of Lemma 2.22

Lemma A.11 (Restatement of [Cond, Theorem 8.6]). *Let m be the index $[\mathcal{O}_K : \mathcal{O}]$ of an order $\mathcal{O}$. Let $\mathfrak{q}$ be a prime ideal in $\mathcal{O}$ that does not lie in $Spec_{\mathcal{O}}(m\mathcal{O})$. Then, $\mathfrak{q}$ is invertible.*

Proof. As $\mathfrak{q} \not\supseteq m\mathcal{O}$, the two ideals are co-maximal, i.e. $\mathfrak{q} + m\mathcal{O} = \mathcal{O}$. Let $\pi + mb = 1$, for some $\pi \in \mathfrak{q}$ and $b \in \mathcal{O}$.

Consider the ideal $\tilde{\mathfrak{q}} := \{y \in K : y\mathfrak{q} \subset \mathcal{O}\}$. By [Cond, Thm 3.2, Section 8], $\mathcal{O} \subsetneq \tilde{\mathfrak{q}}$. Choose $x \in \tilde{\mathfrak{q}} \setminus \mathcal{O}$. Then, $\mathfrak{q} \subseteq \mathfrak{q} + x\mathfrak{q} \subseteq \mathcal{O}$. As $\mathfrak{q}$ is a maximal ideal, we have the following two cases.

Case 1: $\mathfrak{q} + x\mathfrak{q} = \mathcal{O}$. Then, $\mathfrak{q}(\mathcal{O} + x\mathcal{O}) = \mathcal{O}$ and $\mathfrak{q}$ is invertible.

Case 2: $\mathfrak{q} + x\mathfrak{q} = \mathfrak{q}$. This implies that $x\mathfrak{q} \subset \mathfrak{q}$. Since $\mathfrak{q}$ is a finitely generated $\mathbb{Z}$-lattice, we get that $x \in \mathcal{O}_K$. Then,

$$x = x \cdot 1 = x \cdot (\pi + mb) \in x\mathfrak{q} + m\mathcal{O}_K \subset \mathfrak{q} + \mathcal{O} = \mathcal{O}$$

This contradicts the fact that $x \notin \mathcal{O}$. □

Remark A.12. Observe that if $\mathfrak{q}$ is a non-invertible prime, then by Lemma A.11, $\mathfrak{q} \supseteq m\mathcal{O}$, and the index $[\mathcal{O} : \mathfrak{q}] \mid [\mathcal{O} : m\mathcal{O}] = m^n$. Therefore, $Spec_{\mathbb{Z}}([\mathcal{O} : \mathfrak{q}]) \subseteq Spec_{\mathbb{Z}}(m)$.

Lemma 2.22 makes use of localization facts from A.7 and Jordan–Hölder filtrations for $\mathcal{O}$-ideals.

Proof of Lemma 2.22 Without loss of generality, we assume that $\mathcal{I}$ is a non-invertible $\mathcal{O}$-ideal and $Spec_{\mathbb{Z}}([\mathcal{O} : \mathcal{I}]) \nsubseteq Spec_{\mathbb{Z}}(m)$. For if $([\mathcal{O} : \mathcal{I}], m) = 1$, then $\mathcal{I}$ is an invertible $\mathcal{O}$-ideal. Further, if $Spec_{\mathbb{Z}}([\mathcal{O} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$, we may choose $\mathfrak{q} = \mathcal{O}$. By [Cond, Thm 8.9], every integral $\mathcal{O}$-ideal $\mathcal{I}$ has a Jordan-Hölder filteration, i.e, there exist $\mathcal{O}$-ideals $\mathcal{I}_0, \mathcal{I}_1, \ldots, \mathcal{I}_l$ such that

$$\mathcal{O} = \mathcal{I}_0 \supset \mathcal{I}_1 \supset \mathcal{I}_2 \cdots \supset \mathcal{I}_l = \mathcal{I}$$

where each quotient $\mathcal{I}_i/\mathcal{I}_{i+1}$ is a simple $\mathcal{O}$-module and hence isomorphic to $\mathcal{O}/\mathfrak{p}_i$, for some prime ideal $\mathfrak{p}_i$ of $\mathcal{O}$. We call such $\mathfrak{p}_i$ a Jordan–Hölder factor of $\mathcal{I}$. Further $[\mathcal{O} : \mathcal{I}] = \prod_{i=0}^{l-1} [\mathcal{O} : \mathfrak{p}_i]$.

Let $\mathfrak{p}$ be an invertible ideal that appears as a Jordan-Hölder factor of $\mathcal{I}$, with multiplicity $m_{\mathfrak{p}}$. We claim that $\mathcal{I} \subset \mathfrak{p}^{m_{\mathfrak{p}}}$.

Consider the localization of $\mathcal{O}$ at $\mathfrak{p}$, $\mathcal{O}_{\mathfrak{p}}$, and the following chain:

$$\mathcal{O}_{\mathfrak{p}} = \mathcal{I}_0\mathcal{O}_{\mathfrak{p}} \supset \mathcal{I}_1\mathcal{O}_{\mathfrak{p}} \supset \mathcal{I}_2\mathcal{O}_{\mathfrak{p}} \cdots \supset \mathcal{I}_l\mathcal{O}_{\mathfrak{p}} = \mathcal{I}\mathcal{O}_{\mathfrak{p}} \qquad (*)$$

If $\mathcal{I}_i/\mathcal{I}_{i+1} \simeq \mathcal{O}/\mathfrak{q}$, for $\mathfrak{q} \neq \mathfrak{p}$, then $\mathcal{I}_i\mathcal{O}_{\mathfrak{p}} = \mathcal{I}_{i+1}\mathcal{O}_{\mathfrak{p}}$. This is true, as

$$\begin{aligned} \mathcal{I}_i/\mathcal{I}_{i+1} \simeq \mathcal{O}/\mathfrak{q} &\implies \mathcal{I}_i \supseteq \mathcal{I}_{i+1} \supseteq \mathfrak{q}\mathcal{I}_i \\ &\implies \mathcal{I}_i\mathcal{O}_{\mathfrak{p}} \supseteq \mathcal{I}_{i+1}\mathcal{O}_{\mathfrak{p}} \supseteq \mathfrak{q}\mathcal{O}_{\mathfrak{p}}\mathcal{I}_i\mathcal{O}_{\mathfrak{p}} = \mathcal{I}_i\mathcal{O}_{\mathfrak{p}}, \end{aligned}$$

where the last equality follows from the fact that $\mathfrak{q} \neq \mathfrak{p}$. If $\mathcal{I}_i/\mathcal{I}_{i+1} \simeq \mathcal{O}/\mathfrak{p}$, then $\mathcal{I}_i\mathcal{O}_{\mathfrak{p}}/\mathcal{I}_{i+1}\mathcal{O}_{\mathfrak{p}} \simeq \mathcal{O}_{\mathfrak{p}}/\mathfrak{p}\mathcal{O}_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$, as localization behaves nicely with respect to isomorphisms. (Section A.7) Therefore, the series $(*)$ is the Jordan-Hölder filteration of $\mathcal{I}\mathcal{O}_{\mathfrak{p}}$ as an $\mathcal{O}_{\mathfrak{p}}$-ideal. Recall that $\mathfrak{p}$ is invertible and therefore, the local ring $\mathcal{O}_{\mathfrak{p}}$ is a Discrete Valuation Ring (DVR) ([Ste08, Prop 5.4]), and hence a Unique Factorization Domain (UFD). ([DF91, Chapter 8, Thm 12]). By uniqueness of the Jordan-Hölder filteration, we get that $\mathcal{I}\mathcal{O}_{\mathfrak{p}} = (\mathfrak{p}\mathcal{O}_{\mathfrak{p}})^{m_{\mathfrak{p}}}$. This shows that $\mathcal{I} \subset \mathcal{I}\mathcal{O}_{\mathfrak{p}} \cap \mathcal{O} = (\mathfrak{p}\mathcal{O}_{\mathfrak{p}})^{m_{\mathfrak{p}}} \cap \mathcal{O} = \mathfrak{p}^{m_{\mathfrak{p}}}$. Let $\mathfrak{p}_i$ (resp, $\mathfrak{p}'_j$) the invertible (resp, non-invertible) ideals that appear as Jordan-Hölder factors of $\mathcal{I}$, with multiplicity m_i (resp, m'_j). We claim that $\mathcal{I} \subseteq \mathfrak{q} := \prod_i \mathfrak{p}_i^{m_i}$.

Recall that, for each invertible factor $\mathfrak{p}_i$, the ideal $\mathcal{I} \subset \mathfrak{p}_i^{m_i}$. As the factors $\mathfrak{p}_i^{m_i}$'s are pairwise prime, we get

$$\mathcal{I} = \mathcal{I}(\mathfrak{p}_1^{m_1} + \mathfrak{p}_2^{m_2}) \subseteq \mathfrak{p}_1^{m_1}\mathfrak{p}_2^{m_2}$$

Continuing similarly, we get that $\mathcal{I} \subseteq \mathfrak{q}$.

Finally, for the index discussion, observe that

$$\begin{aligned}
[\mathfrak{q} : \mathcal{I}] &= \frac{[\mathcal{O} : \mathcal{I}]}{[\mathcal{O} : \mathfrak{q}]} \\
&= \frac{\prod_i [\mathcal{O} : \mathfrak{p}_i]^{m_i} \times \prod_j [\mathcal{O} : \mathfrak{p}'_j]^{m'_j}}{\prod_i [\mathcal{O} : \mathfrak{p}_i^{m_i}]} \\
&= \prod_j [\mathcal{O} : \mathfrak{p}'_j]^{m'_j}
\end{aligned}$$

Since $\mathfrak{q} := \prod_i \mathfrak{p}_i^{m_i}$, it follows from the Chinese remainder theorem (Theorem A.4) that $[\mathcal{O} : \mathfrak{q}] = \prod_i [\mathcal{O} : \mathfrak{p}_i^{m_i}]$. Moreover, since each $\mathfrak{p}_i$ is invertible, the quotients $\mathfrak{p}_i^n/\mathfrak{p}_i^{n+1}$ and $\mathcal{O}/\mathfrak{p}_i$ are isomorphic (Lemma 2.10) and hence $[\mathcal{O} : \mathfrak{p}_i^{m_i}] = [\mathcal{O} : \mathfrak{p}_i] \cdot [\mathfrak{p}_i : \mathfrak{p}_i^2] \cdot \ldots \cdot [\mathfrak{p}_i^{m_i - 1} : \mathfrak{p}_i^{m_i}] = [\mathcal{O} : \mathfrak{p}_i]^{m_i}$. Moreover, the non-invertible Jordan-Hölder factors contain $m\mathcal{O}$, by Lemma A.11. By Remark A.12, $Spec_{\mathbb{Z}}([\mathfrak{q} : \mathcal{I}]) \subseteq Spec_{\mathbb{Z}}(m)$.

In order to find a $\mathbb{Z}$-basis for $\mathfrak{q}$, inflate the $\mathcal{O}$-ideal $\mathcal{I}$ to the $\mathcal{O}_K$-ideal $\mathcal{I}\mathcal{O}_K$ and factorize $\mathcal{I}\mathcal{O}_K$ into prime ideals in $\mathcal{O}_K$. Since $\mathcal{C}_{\mathcal{O}}^{\vee} = \mathcal{O}_K\mathcal{O}^{\vee}$, as in [BBPS19, Lem 2.32], we can get a $\mathbb{Z}$ basis for $\mathcal{C}_{\mathcal{O}}$, as Hermite Normal Form yields a $\mathbb{Z}$ basis out of the set of generators of $\mathcal{O}_K\mathcal{O}^{\vee}$. Therefore, we can find the primes of $\mathcal{I}\mathcal{O}_K$, coprime to $\mathcal{C}_{\mathcal{O}}$. Let $\mathcal{Q}$ denote the product of primes in this decomposition, coprime to $\mathcal{C}_{\mathcal{O}}$. Then, by Theorem 2.19 and [Conb, Thm 6.1], $\mathfrak{q} = \mathcal{Q} \cap \mathcal{O}$ and the $\mathbb{Z}$-basis for $\mathfrak{q}$ is efficiently obtained from the $\mathbb{Z}$-bases of $\mathcal{Q}$ and $\mathcal{O}$. □

A.9 Gaussian distributions over $K_{\mathbb{R}}$ and $K_{\mathbb{R}}/\mathcal{O}^{\vee}$

Let $Tr = Tr_{K_{\mathbb{R}}/\mathbb{R}}$ and by $\overline{x}$ the complex conjugation of an element $x \in K_{\mathbb{R}}$. For an order $\mathcal{O} \subseteq K$, let $P_{\mathcal{O}} = (Tr(p_i \cdot \overline{p_j}))_{1 \le i,j, \le n}$, such that $\{p_i\}_{1 \le i \le n}$ is the $\mathbb{Z}$-basis of $\mathcal{O}$. Fix an orthonormal $\mathbb{R}$ basis of $K_{\mathbb{R}}$, $\vec{b} = (b_i)_{1 \le i \le n}$, i.e. $Tr(b_i \cdot \overline{b}_j) = \delta_{ij}$. Notice that for $x \in K_{\mathbb{R}}$, $x = \sum_{i=1}^{n} Tr(x \cdot \overline{b_i}) b_i = \sum_{i=1}^{n} Tr(x \cdot b_i)\overline{b_i}$. Consider the matrix $P_{\mathcal{O},\vec{b}} = (Tr(b_i \cdot p_j))_{1 \le i,j \le n}$. Observe that $P_{\mathcal{O},\vec{b}}^t \cdot P_{\mathcal{O},\vec{b}} = P_{\mathcal{O}}$, since

$$(P_{\mathcal{O}})_{ij} = Tr(p_i \cdot \overline{\sum_{k=1}^{n} Tr(p_j \cdot b_k)\overline{b_k}}) = \sum_{k=1}^{n} Tr(p_i \cdot b_k) \cdot Tr(b_k \cdot p_j) = (P_{\mathcal{O},\vec{b}})_i^t \cdot (P_{\mathcal{O},\vec{b}})_j,$$

meaning the ith row of $P^t_{\mathcal{O},\vec{b}}$ multiplied by the j-th column of $P_{\mathcal{O},\vec{b}}$. We used in the above equation the fact that Tr takes real values and it is $\mathbb{R}$ linear.

Proof of Lemma 2.32 First, notice that the coefficients of the error with respect to the $\mathbb{Z}$-basis of $\mathcal{O}^\vee$, $p^\vee$, can be seen from the following vector $Tr(e\cdot\vec{p}) = (Tr(e\cdot p_i))_{1\le i\le n}$. Indeed, let us write e in terms of the $\mathbb{Z}$-basis elements of $\mathcal{O}^\vee$ as $e = e_1p_1^\vee + \ldots + e_np_n^\vee$. By using the linearity of the trace over $\mathbb{R}$, we get that $Tr(e\cdot p_i) = \sum_{j=1}^{n} e_i Tr(p_j^\vee \cdot p_i) = e_i$.

Recall from Section 2.2 that given an orthonormal $\mathbb{R}$ basis $\vec{b} = (b_i)_{1\le i\le n}$ of $K_\mathbb{R}$, sampling e according to the Gaussian distribution D_α over $K_\mathbb{R}$ means sampling a vector of coefficients, $\overline{e}$, with respect to this $\vec{b}$ according to the same distribution over $\mathbb{R}^n$. So $e = \vec{b}^t\cdot\overline{e}$, where $\overline{e}$ follows the distribution D_α. Therefore, by using again the linearity of the trace over $\mathbb{R}$, we get the following:

$$Tr(\vec{p}\cdot e) = Tr(\vec{p}\cdot\vec{b}^t\cdot\overline{e}) = Tr(\vec{p}\cdot\vec{b}^t)\cdot\overline{e} = P^t_{\mathcal{O},\vec{b}}\cdot\overline{e}.$$

Since $\overline{e}$ satisfies the Gaussian distribution of covariance matrix $\alpha^2\cdot Id_{n\times n}$, it implies that $Tr(\vec{p}\cdot e)$ follows the Gaussian distribution of covariance matrix $\alpha^2\cdot P^t_{\mathcal{O},b}\cdot P_{\mathcal{O},b} = \alpha^2\cdot P_\mathcal{O}$. This completes the proof. □

B Deferred Proofs from Section 3

B.1 Proof of Corollary 3.3

Proof. An $\mathcal{O}$-LWE oracle with the error parameter $\alpha < \sqrt{\frac{\log n}{n}}$, solves DGS on an $\mathcal{O}$-ideal $\mathcal{L}$ up to an approximation factor $\gamma = \eta(\mathcal{L})\cdot\sqrt{2}/\alpha\cdot\omega(1)$. See [BBPS19, Remark 3.10] for details. Then, for $\varepsilon = e^{-n}$, Lemma A.3 ii) & 2.1 imply that,

$$\gamma = \eta(\mathcal{L})\cdot\frac{\sqrt{2}}{\alpha}\cdot\omega(1) \ge \frac{\sqrt{n}}{\lambda_1(\mathcal{L}^\vee)}\cdot\frac{\sqrt{2}}{\alpha}\cdot\omega(1) \ge \frac{\lambda_n(\mathcal{L})}{\sqrt{n}}\cdot\frac{\sqrt{2}}{\alpha}\cdot\omega(1)$$

Finally, Lemma 2.8 yields that this $\mathcal{O}$-LWE oracle solves SIVP on $\mathcal{L}$ up to an approximation factor of $\gamma' = \frac{\gamma\cdot\sqrt{n}}{\lambda_n(\mathcal{L})} = \omega(\frac{1}{\alpha})$. □

B.2 Proof of Corollary 3.7

Proof. The result follows from Theorem 3.6 with the order $\mathcal{O} = \mathcal{O}_\mathcal{L}$, $\mathcal{Q} = q\mathcal{O}$ and $u = 1/q$, as the index $[\mathcal{O}_K : \mathcal{O}_\mathcal{L}] \mid [\mathcal{O}_K : p\mathcal{O}_K]$ and therefore is a power of p, coprime to q. By properties of Gaussian distribution and Definition 2.29 of Υ_α, adding a compensatory Gaussian error leads to derive the reduction from $\mathcal{O}_K$-LWE$_{(q\mathcal{O}_K,1/q),t\cdot\Upsilon_{\alpha'}}$ to $\mathcal{O}_K$-LWE$_{(q\mathcal{O}_K,1/q),\Upsilon_\alpha}$ where $\alpha' = \alpha/\|t\|_\infty$, which helps complete the proof. □

B.3 On the size of the multiplier t

Let $\mathcal{O}$ be an order of conductor $\mathcal{C}_\mathcal{O}$ in the number field K of degree n and q be an integer. Take the associated primes of $q\mathcal{O}$, denoted as $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$. Recall that if q is coprime to the conductor, these primes come from the unique factorization of $q\mathcal{O}$. The proofs of the previous results, [BBPS19, Le. 2.36], [RSW18, Thm 3.1] and [BBPS19, Prop. 4.7], when applied to the conductor ideal, yield the existence of a short element $t \in \mathcal{C}_\mathcal{O} \setminus \bigcup_i \mathcal{C}_\mathcal{O}\mathfrak{q}_i$. Here, we analyze the size of t we gain, using these approaches.

As a corollary of [BBPS19, Le. 2.36], we obtain the following bound on the size of t.

Corollary B.1. *There exists an element $t \in \mathcal{C}_\mathcal{O} \setminus \bigcup_i \mathcal{C}_\mathcal{O}\mathfrak{q}_i$ such that*

$$\|t\| \leq O(n \cdot \sqrt{n \log n} \cdot \Delta_\mathcal{O}^{1/n} \cdot N(\mathcal{C}_\mathcal{O})^{1/n}).$$

As a corollary of [RSW18, Thm 3.1] and [BBPS19, Prop. 4.7], we obtain another bound on the size of t.

Corollary B.2. *Assuming q is coprime to the conductor, there exists an element $t \in \mathcal{C}_\mathcal{O} \setminus \bigcup_i \mathcal{C}_\mathcal{O}\mathfrak{q}_i$, whose norm is bounded with high probability as*

$$\|t\| \leq \sqrt{n} \cdot \sqrt{q} \cdot q^{2\delta} \cdot \Delta_\mathcal{O}^{1/n} \cdot N(\mathcal{C}_\mathcal{O})^{1/n},$$

where $\delta \in \left[\frac{4n + \log \Delta_\mathcal{O}}{n \log q}, 1\right]$.

We mention that the coprimality of q is an essential assumption in sampling t as in [RSW18, Thm 3.1], [BBPS19, Prop. 4.7] and hence, in deriving the second bound, whereas [BBPS19, Le. 2.36] uses no such assumption. Both results present bounds with common factors, namely $\sqrt{n}$, $\Delta_\mathcal{O}^{1/n}$ and $N(\mathcal{C}_\mathcal{O})^{1/n}$. Therefore, analyzing these bounds reduces to comparing $C \cdot n \cdot \sqrt{\log n}$ and $\sqrt{q} \cdot q^{2\delta}$, where C is the hidden constant involved in the first bound. For $q = \text{poly}(n)$, the first bound gets, asymptotically, better than the second one.

Examples for Corollary 3.7:

1) Let p be an integer and K a cyclotomic field of degree n, along with its ring of integers, $\mathcal{O}_K$. Take a lattice $\mathcal{L}$ as a proper divisor of $p\mathcal{O}_K$, so in particular it is an embedding of an integer p-ary lattice. Therefore $\mathcal{L}$ is in particular an ideal of $\mathcal{O}_K$, and moreover, its ring of multipliers $\mathcal{O}_\mathcal{L}$ and its conductor $\mathcal{C}_{\mathcal{O}_\mathcal{L}}$ are both equal to $\mathcal{O}_K$. By [Was83, Prop 2.7], $\Delta_K = n^n$. Therefore, by Corollary B.1, we get

$$\|t\|_\infty \leq \|t\| \leq O(n^2 \cdot \sqrt{n \log n}),$$

and by Corollary B.2

$$\|t\|_\infty \leq \|t\| \leq \sqrt{n} \cdot \sqrt{q} \cdot q^{2\delta} \cdot n \leq \sqrt{n} \cdot \sqrt{q^5} \cdot n.$$

If $p = \text{poly}(n)$, which typically is for p-ary lattices of rank n, and a convenient choice of q, we can get small multipliers of infinity norm less than p.

2) Let K be the number field $\mathbb{Q}[X]/(x^3 - m^2)$, for some integer m, and R be its polynomial ring, $\mathbb{Z}[x]/(x^3 - m^2)$. Let p be an integer and let $\mathcal{L}$ be a proper divisor of pR. In particular, the lattice $\mathcal{L}$ can be seen as an embedding of an integer p-ary lattice. Then $\mathcal{L}$ is an ideal of R, and hence its ring of multipliers $\mathcal{O}_\mathcal{L}$ contains R. Moreover, the conductor of $\mathcal{O}_\mathcal{L}$ contains the conductor of R, so the upper bounds derived by Corollaries B.1 and B.2, for $\mathcal{O} = \mathcal{O}_\mathcal{L}$, can be further bounded, from above with similar bounds obtained for $\mathcal{O} = R$. The discriminant of R, is $3^3 \cdot m^4$ ([Ste08, Example 7.9]), and the norm of conductor of R is m^2 ([RSW18, Lem D.1]). Therefore Corollary B.1 yields

$$\|t\|_\infty \leq \|t\| < O(n \cdot \sqrt{n \log n} \cdot (3^3 \cdot m^6)^{1/n}),$$

and Corollary B.2

$$\|t\|_\infty \leq \|t\| \leq \sqrt{n} \cdot \sqrt{q} \cdot q^{2\delta} \cdot (3^3 \cdot m^6)^{1/n} \leq \sqrt{n} \cdot \sqrt{q^5} \cdot (3^3 \cdot m^6)^{1/n}.$$

This computation can be generalized to the family of polynomials $x^n - m^2$, for suitably chosen n and m. As in previous example, for convenient choices of p and q, there can be found multipliers t of infinity norm less than p.

C Deferred Proofs from Section 4

C.1 Proof of Theorem 4.2

Proof. Each reduction follows from Theorem 4.1 under the observation that the indices $[\mathcal{O}_K : \mathcal{O}_i] \mid [\mathcal{O}_K : m\mathcal{O}_K] = m^n$, and $[\mathbb{Z} + m\mathcal{O}_K : \mathbb{Z} + m\mathcal{J}]$ is a factor of $m \cdot [\mathcal{O}_K : \mathcal{J}]$, as it is equal to

$$\left| \frac{(\mathbb{Z} + m\mathcal{O}_K)/m\mathcal{J}}{(\mathbb{Z} + m\mathcal{J})/m\mathcal{J}} \right| = \frac{|(\mathbb{Z} + m\mathcal{O}_K)/m\mathcal{O}_K| \cdot |m\mathcal{O}_K/m\mathcal{J}|}{|(\mathbb{Z} + m\mathcal{J})/m\mathcal{J}|} = \frac{|\mathbb{Z}/m\mathbb{Z}| \cdot |\mathcal{O}_K/\mathcal{J}|}{|\mathbb{Z}/\ (\mathbb{Z} \cap m\mathcal{J})|}.$$

Therefore, $\text{Spec}([\mathbb{Z}+m\mathcal{O}_K : \mathbb{Z}+m\mathcal{J}](\mathbb{Z}+m\mathcal{J})) \subseteq \text{Spec}(m \cdot [\mathcal{O}_K : \mathcal{J}](\mathbb{Z}+m\mathcal{J}))$, $\text{Spec}([\mathcal{O}_K : \mathcal{O}_1]\mathcal{O}_1) \subseteq \text{Spec}(m\mathcal{O}_1)$, and $\text{Spec}([\mathcal{O}_i : \mathcal{O}_{i+1}]\mathcal{O}_{i+1}) \subseteq \text{Spec}(m\mathcal{O}_{i+1})$, which shows that $[\mathbb{Z}+m\mathcal{O}_K : \mathbb{Z}+m\mathcal{J}](\mathbb{Z}+m\mathcal{J})$ and $\mathcal{Q}$ are coprime, $[\mathcal{O}_K : \mathcal{O}_1]\mathcal{O}_1$ and $\mathcal{Q}\mathcal{O}_1$ are coprime, and $[\mathcal{O}_i : \mathcal{O}_{i+1}]\mathcal{O}_{i+1}$ and $\mathcal{Q}\mathcal{O}_{i+1}$ are coprime. □

C.2 Proof of Corollary 4.7

Proof. Let $\{\theta_i\}_{i=0}^{n-1} = \{1, \zeta_{2n}, \ldots, \zeta_{2n}^{n-1}\}$ be a power basis of $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Note that this is an orthogonal $\mathbb{Z}$-basis with respect to the Trace map, i.e., $Tr(\theta_i\overline{\theta_j}) = 0$, when $i \neq j$, and $Tr(\theta_i\overline{\theta_i}) = n$. Therefore, the matrix $T = (Tr(\theta_i\overline{\theta_j}) - \frac{1}{n} \cdot Tr(\theta_i)Tr(\theta_j))_{1 \leq i,j \leq n-1}$ is the diagonal matrix $n \cdot Id_{n-1 \times n-1}$, and the smallest eigenvalue value $\tau := e_{n-1}(T)$ equals n. This implies that we may choose $r = 1$, for then $\tau \cdot m^{2r-2} \geq n$. Then, by either of the proofs of (i) or (ii) in Proposition 4.5, we have $\widetilde{\mathcal{O}}$ is α-drowning. The conclusion follows by applying Theorem 4.4. □