Order-LWE and the Hardness of Ring-LWE with Entropic Secrets

Zvika Brakerski Renen Perlman
Weizmann Institute of Science*

Abstract

The Ring Learning with Errors problem (RLWE) introduced by Lyubashevsky, Peikert and Regev (LPR, Eurocrypt 2010, Eurocrypt 2013) quickly became a central element in cryptographic literature and a foundation to numerous cryptosystems. RLWE is an average case problem whose hardness is provably related to the worst case hardness of ideal lattice problems. However, in many cases optimizations and other considerations necessitate generating RLWE instances from distributions for which the worst case reduction does not apply, thus leaving the resulting cryptosystem secure only by heuristic reasons.

The focus of this work is RLWE with non-uniform distribution on *secrets*. A legal RLWE secret is (roughly) a uniform element in the ring of integers of a number field, modulo an integer q. We consider two main classes of "illegal" distributions of secrets.

The first is sampling from a *subring* of the intended domain. We show that this translates to a generalized form of RLWE that we call Order-LWE, we provide worst case hardness results for this new problem, and map out regimes where it is secure and where it is insecure. Two interesting corollaries are a (generalization of) the known hardness of RLWE with secrets sampled from the ring of integers of a subfield, and a new hardness results for the Polynomial-LWE (PLWE) problem, with different parameters than previously known.

The second is sampling from a k-wise independent distribution over the CRT representation of the secret. We cannot show worst case hardness in this case, but instead present a single average case problem (specifically, bounded distance decoding on a fixed specific distribution over lattices) whose hardness implies the hardness of RLWE for all such distributions of secrets.

1 Introduction

The introduction of the learning with errors (LWE) problem by Regev [Reg05] provided a convenient way to construct cryptographic primitives whose security is based on the hardness of *lattice problems*. LWE was used to construct various cryptographic primitives, including cutting edge primitives such as fully homomorphic encryption (FHE) [BV11b], and ones that are not known under other assumptions, such as attribute based encryption (ABE) for general policies [GVW13, BGG+14]. Two of the most appealing properties of LWE are the existence of a reduction from *worst-case* lattice problems [Reg05, Pei09, BLP+13, PRSD17] (which is most relevant to this work), and its conjectured post-quantum security.

*Supported by the Israel Science Foundation (Grant No. 468/14), Binational Science Foundation (Grants No. 2016726, 2014276), and by the European Union Horizon 2020 Research and Innovation Program via ERC Project REACT (Grant 756482) and via Project PROMETHEUS (Grant 780701).

On the other hand, one of the shortcomings of LWE is its relatively high computational complexity and large instance size (as a function of the security parameter). This leads, for example, to LWE-based encryption having long keys and ciphertexts, and also high encryption complexity. It was known since the introduction of the NTRU cryptosystem [HPS98] (even before LWE was introduced) and more rigorously in [LM06, PR06] that these aspects can be greatly improved by relying on lattices that stem from algebraic number theory. Lyubashevsky, Peikert and Regev [LPR10, LPR13] defined an algebraic number theoretic analog of LWE, called Ring-LWE (RLWE), which similarly to Regev's original result, is shown to be as hard as solving worst-case *ideal lattice* problems.

Ring-LWE and extensions quickly became a useful resource for the construction of various cryptographic primitives [BF11, BV11a, BGV12, GHS12, DDLL13, AP13, HS14, BKLP15, ADPS16, BVWW16] (an extremely non-exhaustive list of examples). Using RLWE is appealing due to its improved efficiency and its promise of security based on the hardness of worst case (ideal) lattice problems. However, as it often happens in concrete instantiations, in many cases achieving the best possible efficiency requires setting the parameters in a regime where the worst-case hardness proof of [LPR10, LPR13] does not apply, and the only guarantee is the lack of known attacks. In other cases (e.g. [BVWW16]) the extreme parameter setting was required for functionality purposes. While a gap between the provable and concrete security properties of a cryptosystem is expected, one would like to at least make sure that changing the distribution did not make the problem qualitatively easy. That is, we would like to show that the problem remains at least asymptotically hard even with the new distribution.

In the case of LWE, it has been shown over the years that the problem is quite robust to changes in the prescribed LWE distribution. In particular, it was shown that even if the LWE secret (a vector that, very roughly, represents the coordinates of a hidden lattice point) is not sampled uniformly as prescribed, but rather is leaked on [AGV09, DGK+10] or is just chosen from a binary distribution of sufficient entropy [GKPV10, BLP+13], then similar hardness to the original problem is preserved (with the obvious loss coming from the secret having smaller entropy). It is also almost trivial to verify that if the LWE secret is chosen uniformly from a linear subspace of its prescribed space, then security degrades gracefully with the dimension of the space.[1]

Much less is known for RLWE since its algebraic structure (which is the very reason for the efficiency gain) prevents using techniques such as randomness extraction that are instrumental to the aforementioned LWE robustness results.

In this work, we investigate the behavior of the RLWE problem on imperfect distributions of secrets, proving security in some cases and showing insecurity in others. Specifically we present some robustness results that can be interpreted as partial analogs to those known for LWE. We hope that these results will lead to better guidelines on what RLWE secret distributions should be considered secure. We believe that the framework we establish may find other uses in the investigation of the properties of RLWE and its variants.

1.1 Our Results

In the LWE problem, a secret vector $\mathbf{s}$ is sampled from $\mathbb{Z}_q^n$ for some modulus q. The adversary gets oracle access to samples of the form $(\mathbf{a}_i, b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \pmod q)$ where the $\mathbf{a}_i \in \mathbb{Z}_q^n$ are

[1] We note that there has also been much work on modifying the *noise distribution* of LWE, e.g. [BPR12, MP13]. However the focus of this work is the distribution of secrets.

uniform and e_i are small integers (say sampled from a discrete Gaussian with parameter $\ll q$). The adversary's goal is to distinguish this oracle from one where b_i is random.

For RLWE, we consider an extremely simplified setting for the sake of this high level overview. Concretely, we consider the $2n$ cyclotomic number field for n a power of two: $K = \mathbb{Q}[x]/\langle x^n + 1\rangle$. In this setting, the ring of integers is $R = \mathbb{Z}[x]/\langle x^n + 1\rangle$, and the RLWE problem with modulus q can be simplified as follows. Sample a random secret $s \in R/qR$,[2] and provide the adversary with oracle access to samples of the form $(a_i, a_i s + e_i)$, where $a_i \in R/qR$ is uniform and e_i is sampled from some "small" noise distribution (for the purpose of this outline, a polynomial with integer coefficients much smaller than q, say sampled from a Gaussian). The arithmetics is over $R_q = R/qR$, and the goal is to distinguish the samples from uniform. We would like to consider the case where q may be reducible in R, so for simplicity we consider the setting where q is prime s.t. $q = 1 \pmod{2n}$. In this case q factors into n ideals in R. This allows to apply the Chinese Remainder Theorem and conclude that any element in R_q can be represented as a vector of n elements in $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, so that addition and multiplication in R_q are performed point-wise on these vectors. This is called the CRT representation of elements in R_q. Let us denote the CRT representation of an element c by $c[1], \ldots, c[n]$.

We investigate the properties of RLWE when s is sampled from special distributions rather than uniformly.

Sampling from an ideal. In LWE, it is almost immediate that if q is not prime, e.g. $q = p_1 p_2$, the secret vector $\mathbf{s}$ is a multiple of p_1, and the e_i magnitude is sufficiently smaller than p_1, then LWE becomes easy to solve. One can just taking the quotient of b_i divided by p_1 and rounded to the nearest integer, thus getting a noiseless set of equations modulo p_2. However, if the noise magnitude is sufficiently larger than p_1, then the instance is secure (one can think about dividing the entire instance by p_1).

We show that in the ring setting a similar phenomenon occurs even when q is prime. Specifically, the analog is that the ideal generated by q splits in R, and s is sampled from an ideal which is a factor of qR. Contrary to the LWE setting, it is not obvious that this distribution leads to an insecure instance, since we cannot just round to the nearest integer. Instead, we show that the factors of q, interpreted as lattices, have a good decoding basis, and then rely on this basis to recover e if it is small enough. We complement this result by showing that if the noise is sufficiently large then RLWE hardness holds. This requires to define a version of RLWE modulo an arbitrary ideal (instead of modulo qR). This is a simple special case of a more general problem that we call Order-LWE (which is outlined below). See Section 5 for more details.

Sampling from a subring. In LWE, if we sample $\mathbf{s}$ from a k-dimensional linear subspace of $\mathbb{Z}_q^n$, then the problem quite easily translates to an instance of LWE where the dimension n is replaced with k. In the ring setting there is much more structure that makes such transformations harder to define and analyze. Previous works [BGV12,GHPS13,AP13] considered the notion of *ring-switching* which implies the hardness of RLWE even when s is sampled from the ring of integers of a *sub-field* of the field K. However, such transformations do not apply when K has no subfields or when it has no subfields of dimension k.

[2] An informed reader may notice that in the actual RLWE definition s needs to be sampled from the dual of this ring, but in the cyclotomic setting this distinction makes little difference and our choice makes the presentation simpler. Another simplifying choice for the exposition is to consider discrete noise distributions.

We propose wider range of distributions, in particular ones where s is sampled from a subring of R_q which is isomorphic to $\mathbb{Z}_q^k$. We notice that since the entire RLWE instance is taken modulo q, then we should only consider q-periodic subrings, such subrings have full rank and therefore comply with the algebraic definition of *order*. In terms of CRT representation, such subrings correspond to an onto mapping $\alpha : [n] \to [k]$, and the sampling process is done by sampling k elements $r_1, \ldots, r_k$ from $\mathbb{Z}_q$ uniformly, and then setting $s[j] = r_{\alpha(j)}$. Note that this set indeed constitutes a subring.[3]

Using our Order-LWE formulation (see below), we can prove that when sampling s uniformly from such order, the resulting RLWE instance is at least as hard as worst case ideal lattice problems, for a restricted set of rank-k ideals that lie in a specific linear subspace of dimension k. More formally, these ideals are all submodules of some rank k module that is induced by the chosen distribution of secrets. See Section 6 for more details.

Formulating Order-LWE and proving worst-case hardness. The two results mentioned above are proven using a generalization of the RLWE problem that we call Order-LWE. We believe that this generalization is natural and quite useful (and our aforementioned applications are just an example), but perhaps equally importantly shows that the techniques developed in previous works [LPR10, LPR13, PRSD17] can be extended even beyond the current state of the art. Technically, Order-LWE is simply RLWE but with the ring of integers of the field replaced with an arbitrary *order* in the field, and the modulus q replaced with some ideal in that order. An order is a full rank subring of the field, and in particular of the ring of integers (which is the maximal order in a number field). An example of an order in the $2n$ cyclotomic number field was given above.

Our worst-case hardness result asserts that when solving Order-LWE with respect to some order $\mathcal{O}$ (with a properly defined Gaussian noise distribution), is at least as hard as solving worst-case lattice problems (specifically Discrete Gaussian Sampling, which in turn implies solutions to problems such as the Shortest Independent Vector Problem) on all ideal lattices induced by *invertible ideals* of the order $\mathcal{O}$. The meaning of this result is of course subject to interpretations since it is not impossible that the set of invertible ideals relative to certain orders only contains "easy" lattices, rendering the result meaningless. As a sanity check we note that instantiating our result with $\mathcal{O}$ being the ring of integers implies the same RLWE hardness proven in [LPR10, LPR13, PRSD17]. See Section 3 for more details.

A Corollary: New Hardness for Polynomial-LWE. We notice that Order-LWE gives insight on the hardness of other computational problems underlying cryptographic constructions. Specifically, the Polynomial-LWE problem (PLWE) [SSTX09, BV11a] provides perhaps the simplest interface for LWE over polynomial rings. In PLWE, s, a are simply random polynomials with integer coefficients modulo a polynomial f and modulo q, and the noise e is just a polynomial with small coefficients. Indeed, in many useful cases (as in our running example above) it is straightforward to relate PLWE and RLWE, however for general ambient polynomials f the connection is far from immediate. Recently Rosca, Stehlé and Wallet [RSW18] showed a reduction relating the hardness of PLWE in the general case to RLWE and thus to worst-case lattice problems. However, their reduction incurs a penalty in the resulting approximation ratio of the worst-case problem. This penalty is a function of f and might be unbounded for an arbitrary f. Indeed, [RSW18] show

[3] Let us point out again that most formally the secret is sampled from the dual of the order but we neglect this distinction for the sake of simplicity.

that in many useful cases this penalty is polynomially bounded, but the question for the general case remains.

We notice that since the ring of polynomials with integer coefficients in a number field is an order and therefore our results on Order-LWE immediately imply a worst-case hardness result for PLWE. Perhaps surprisingly, the worst-case hardness result we achieve is quite different from [RSW18]. First of all, we do not incur the aforementioned penalty. Secondly, the class of lattices for which we show worst-case hardness is different (and in fact disjoint) from the class of lattices from [RSW18]. This is since the hardness Order-LWE refers is with respect to lattices defined by invertible ideals in the order. Thus our result strengthens previous results on the hardness of PLWE, showing that solving PLWE will result in efficient algorithm for short vector problems in additional lattices than those already known, and without incurring a penalty in the approximation factor. See Section 4 for more details.

Sampling from a k-wise Independent distribution. We now consider a class of distributions that do not adhere to uniform sampling from an algebraic structure. Instead we consider the class of distributions with the following property. The marginal distribution over any subset of k CRT coordinates is jointly (statistically close to) uniform.

For such distributions we are unable to prove worst case hardness. However, RLWE with any k-wise distribution is at least as hard as the following average case problem, that we call decisional bounded distance decoding on a hidden lattice. In this problem, the adversary needs to distinguish between a random oracle on R_q and an oracle of the following form. Upon initialization of the oracle, a set $T \subseteq [n]$ of cardinality k is sampled. Then for every oracle call, sample an element v_i as follows: $v_i[j]$ is random if $j \in T$, and 0 otherwise, sample a small noise element e_i, and return $(v_i + e_i)$. This is similar to a bounded distance decoding (BDD) problem since the elements v_i are sampled from an ideal lattice.

This assumption is similar to one made in [HPS+14], however they only require $k = n/2$, whereas we attempt to take k to be very small, e.g. $k = n^{0.1}$. We note that the hardness of the problem relies crucially on the set T being chosen at random in the beginning of the experiment rather than using a fixed set T (in other words, we cannot allow preprocessing that depends on T). This is since computing a good basis to the ideal lattice defined by T makes the problem easy. It is also important to mention that T itself does not need to be known to the adversary, in this sense this problem also resembles the approximate GCD problem [DGHV10]. Lastly, we note that it is sufficient for our purposes to limit the adversary of the decisional hidden-lattice BDD to only make 2 oracle calls. Namely, the problem is to distinguish two samples $(v_1 + e_1, v_2 + e_2)$ from two uniform elements in R_q. Despite our efforts, we were unable to find additional corroboration to the hardness of this problem and we leave it as an interesting open problem to characterize its hardness.

While the class of k-wise independent distributions might seem a little weird, it captures the spirit of some of the heuristic entropic distributions that were considered for RLWE. For example, consider the representation of the secret s as a formal polynomial modulo q (recall that R_q is a ring of polynomials), if each coefficient of s is sampled from a Gaussian, so that the total distribution has sufficient entropy (slightly above the necessary $k \log q$), then this distribution will be k-wise independent. This shows that sampling secrets with very low norm does not violate security under our new assumption. While it was previously known that sampling the secret from the distribution of noise keeps security intact (also known as RLWE in Hermite Normal Form [ACPS09]), we are

not aware of a proof of security when going below the noise rate. This can be seen as a step in the direction of matching the robustness of LWE results [GKPV10, BLP+13], that shows that LWE remains hard even with high entropy binary secrets. We note that low norm secrets are of importance in the FHE literature (e.g. [BGV12, HS14, HS15]), where it is desirable to reduce the norm of the secret as much as possible. In fact, in the HElib implementation [HS14,HS15] the secret is chosen to be a random extremely sparse polynomial. Heuristically, we believe sparse polynomials should translate into k-wise independent distributions, however we currently do not have a proof for this speculation.

Another example of an interesting k-wise independent distribution is the "entropic RLWE" formulation that came up in the obfuscation literature [BVWW16]. That setting consists of a large number of public elements $s_1, \ldots, s_m$, sampled from the noise distribution (which is Gaussian in the polynomial coefficient representation and thus can be shown to be k-wise independent in the CRT representation). The secret is generated by sampling a binary vector $\vec{z} = (z_1, \ldots, z_m)$ and outputting $s = \prod s_i^{z_i}$. Using the leftover hash lemma, one can show that so long as $\vec{z}$ has entropy sufficiently larger than $k \log q$, the resulting distribution will be k-wise independent as well. It is worth noting that to achieve the strongest notion of security for their obfuscator, [BVWW16] use $\vec{z}$ with entropy $\ll \log q$ to which our technique does not directly apply.

We believe that tighter results should be achievable by replacing the statistical k-wise independence condition with a computational one. Namely that there is no efficient distinguisher that takes a subset of k CRT coordinates of its choice and distinguishes them from uniform. This avenue could allow to go below entropy $\log q$ and thus allow us to show security for even narrower secret distributions. See Section 7 for more details.

1.2 Overview of Techniques

We outline the high level technical ideas that underly our various results. Again we relate here to the simplified RLWE setting described above. For the specific details and more general result refer to the specific sections.

Sampling from an ideal. In this setting, we can start with a RLWE instance that is provably secure when s is sampled uniformly, and propose a family of distributions of secrets s which have very high entropy, but still make the problem easy to solve. Specifically, let $T \subseteq [n]$ and consider s sampled so that all coordinates $s[j]$ for $j \in T$ are uniform in $\mathbb{Z}_q$, and $s[j] = 0$ if $j \notin T$. This distribution has entropy $|T| \log q$. Now let us consider even a single RLWE sample $(a, as + e)$ w.r.t this secret distribution. Clearly the CRT coordinates of e that correspond to $[n] \setminus T$ can be completely recovered (since for $j \in [n] \setminus T$ it holds that $(as)[j] = 0$ and thus $(as + e)[j] = e[j]$), but that by itself is not sufficient. In fact, even though e can be represented as a polynomial with small coefficients, its CRT representation is not small, since the marginal distribution of each individual CRT coordinate is uniform. However, if e is small enough then even by entropy considerations it is impossible for too many of its CRT slots to be jointly uniform, so at least information theoretically one could hope that recovering sufficiently many CRT slots of e could allow to reconstruct e and thus recover s. We show that this is indeed the case. Specifically, we notice that our distribution of s actually samples from an ideal $\mathcal{I}$ of qR. This means that $as + e \pmod{\mathcal{I}} = (e \bmod \mathcal{I})$. We now resort to the representation of $\mathcal{I}$ as a lattice, and conclude that so long as we have a sufficiently good decoding basis for $\mathcal{I}$, we will be able to recover e from $(e \bmod \mathcal{I})$. Indeed, in this case the ideal $\mathcal{I}$ is a product of factors of q, which behave "nicely", and a good decoding basis indeed exists. Note

that this decoding basis may be computationally hard to find given T, so our attack requires to be provided with the decoding basis for $\mathcal{I}$ as advice (computed, e.g., via inefficient preprocessing). Indeed, as we explained above, our k-wise independent result relies on the assumed hardness of decoding from $\mathcal{I}$ induced by a random T, so preprocessing does not seem to help.

Intuitively, if e is sufficiently large to make $(e \bmod \mathcal{I})$ completely uniform, plus "a little bit" of additional entropy, then the uniform $(e \bmod \mathcal{I})$ should cover up for the CRT coordinates in s that are set to 0, and there may be sufficient leftover noise entropy to ensure RLWE hardness. We show that this intuition is indeed correct and so long as e is sampled from a wide enough Gaussian, it is possible to consider the quotient of the RLWE instance w.r.t $\mathcal{I}$, and get an instance of a problem similar to RLWE, except q is replaced with a different ideal (essentially, the ideal corresponding to the set of coordinates T). This is a simple special case of Order-LWE.

In fact, since $\mathcal{I}$ has a good decoding basis, we exhibit a threshold phenomenon where a slight decrease in the noise can make the problem from provably hard to provably easy. The threshold, as can be expected from entropy calculations, is approximately when the coefficients of e as a polynomial are roughly of size $q^{1-|T|/n}$. This means that even for high-entropy secret distributions, e.g. $|T| = 0.5n$, one needs noise coordinates of amplitude $\approx \sqrt{q}$ in order for the instance not to be broken.

Sampling from a subring. As explained above, we wish to establish the hardness of RLWE when the secret is sampled from a subring (actually, an order). To this end we formulate Order-LWE which is similar to RLWE but with the *ambient space* being an order. To bridge the gap between RLWE over R_q with secret coming from an order, and Order-LWE where the entire arithmetics is over an order and not over R_q, we employ techniques similar to the ring switching described in [GHPS13]. Specifically, given a RLWE solver with subring secret, we would like to create an Order-LWE solver. To do this, we take multiple Order-LWE samples $\{(a_i, b_i)\}$ and "piece them together" using a short linear combination $v_1, \ldots, v_d$ s.t. $\sum a_i v_i$ is uniformly distributed over the entire R_q. In the case of the power of two cyclotomic from our example, we can consider v_i which are powers of the formal variable x.[4] Multiplying by such v_i will permute the CRT coefficients, and summing together sufficiently many of these permutations will destroy the subring structure and allow us to recover an element from R_q.

The hardness of Order-LWE. To prove the hardness of Order-LWE, we extend the techniques of [LPR10, LPR13, PRSD17]. Essentially, their outline (which is itself an adaptation of [Reg05]) shows how to translate an instance of the bounded distance decoding problem over the dual of the ideal into a set of RLWE samples.[5] At a high level this is done by looking at the set of coefficients of the given point, respective to some basis of the lattice in question, and interpreting it as the secret. Then multiplying by a Gaussian from the dual will result in an LWE sample. In the algebraic setting, these operations needs to be represented as a multiplication by a single field element. Showing that there exists a scalar that maps a lattice point into an element in the ring of integers is an easier task than over orders, due to its being a unique factorization domain. A more delicate argument needs to be applied in the context of general orders, and we show that this

[4] Powers of x were also used for the subfield setting in [GHPS13].

[5] More accurately, we follow in the footsteps of [PRSD17] and directly prove the hardness of the decision version of the problem. This means that the problem being solved is not exactly bounded distance decoding, but rather a Gaussian variant.

indeed can be done.

A Corollary: New Hardness for Polynomial-LWE. The corollary follows almost immediately. PLWE is not exactly an Order-LWE problem since in Order-LWE the secret s is sampled from the dual of the order, however a transformation is known and is analyzed in [RSW18]. Given this transformation, we can just apply our worst-case Order-LWE hardness.

Sampling from a k-wise independent distribution. We start by noticing that it is sufficient to prove the result for an adversary that takes a single RLWE sample. This is done by using a rerandomization technique from [LPR13] and assuming the hardness of standard RLWE (which translates to worst case hardness in ideal lattices). This transformation unfortunately also requires "noise swallowing", a technique that uses the fact that adding a Gaussian with super-polynomial Gaussian parameter will mask any random variable with polynomial amplitude. Using this technique necessitates a super-polynomial modulus q and is therefore undesirable, but we were unable to remove it from our argument. In fact we will use swallowing again down the line.

Assume there is an adversary that can distinguish between a single RLWE sample $(a, b = as+e)$ and uniform. We start by replacing a with a decisional hidden-lattice BDD sample $(v_1 + e_1)$, where v_1 only has k nonzero CRT coordinates (randomly chosen) and e_1 is small. The decisional hidden-lattice BDD assumption asserts that this distribution will be indistinguishable from the original one. Namely, we now have $(v_1+e_1, b = (v_1+e_1)s+e)$. Opening the parenthesis, we have $b = v_1s+e_1s+e$. We again use noise swallowing to argue that b is statistically close to $b = v_1s + e$, i.e. we use e to swallow e_1s, which can be done so long as s is small enough and e is large enough. Now we observe that since v_1 is zero on all but k CRT coordinates, and s is close to uniform in any subset of k coordinates, it follows that v_1s is statistically close to a fresh v_2 that is sampled from the same distribution as v_1 (i.e. has the same set of nonzero coordinates, but the value in each coordinate is randomly chosen). We get $b = v_2 + e$. We can now apply decisional hidden-lattice BDD again to claim that $(a, b) = (v_1 + e_1, v_2 + e)$ is indistinguishable from uniform, which completes the proof.

1.3 Paper Organization

Section 2 contains preliminaries and definitions. The Order-LWE problem is formally defined in Section 3, where the worst case hardness reduction is provided as well. The new hardness result for PLWE appears in Section 4. We then present our results on sampling secrets from ideals in Section 5, on sampling secrets from subrings in Section 6 and finally on sampling secrets from k-wise independent distributions in Section 7.

2 Preliminaries

2.1 Lattices and Gaussians

2.1.1 The Space H

When working with number fields from a geometric perspective, we usually work with the following space $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ for some numbers $s_1 + 2s_2 = n$, defined as

$$H = \{(x_1, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \mid x_{s_1+s_2+j} = \overline{x_{s_1+j}}, \forall j \in [s_2]\} \ .$$

Note that H, equipped with the inner product induced by $\mathbb{C}^n$, is isomorphic to $\mathbb{R}^n$, as an inner product space. This can be seen via the orthonormal basis $\{\mathbf{h}_i\}_{i\in[n]}$, defined as follows: for $j \in [n]$, let $\mathbf{e}_j \in \mathbb{C}^n$ be the vector with 1 in its jth coordinate, and 0 elsewhere; then for $j \in [s_1]$, we take $\mathbf{h}_j = \mathbf{e}_j \in \mathbb{C}^n$, and for $s_1 < j \leq s_1 + s_2$ we take $\mathbf{h}_j = \frac{1}{\sqrt{2}}(\mathbf{e}_j + \mathbf{e}_{j+s_2})$ and $\mathbf{h}_{j+s_2} = \overline{\mathbf{h}_j}$.

We will also equip H with the ℓ_p norm induced on it from $\mathbb{C}^n$.

2.1.2 Lattices

We define a *lattice* as a discrete additive subgroup of H. Equivalently, a lattice is the $\mathbb{Z}$-span of some set of k linearly independent *basis* vectors $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_k\} \subseteq H$:

$$\mathcal{L} = \left\{ \sum z_i \mathbf{b}_i \mid z_i \in \mathbb{Z} \right\} .$$

We refer to k as the *rank* of the lattice, and to n as its *dimension*. If $k = n$, we say that the lattice is *full-rank*.

The *minimum distance* $\lambda_1(\mathcal{L})$ os a lattice $\mathcal{L}$ in a given norm $\|\cdot\|$ is the length a the shortest nonzero lattice vector. More generally, we define the *ith successive minimum* as

$$\lambda_i(\mathcal{L}) := \inf\{r > 0 \mid \dim(\mathrm{span}(\mathcal{L} \cap \overline{\mathbf{B}}(0, r))) \geq i\} ,$$

where $\overline{\mathbf{B}}(0, r)$ is the closed ball of radius r around 0.

The *dual lattice* of $\mathcal{L} \subset H$ is defined as $\mathcal{L}^* = \{\mathbf{x} \in H \mid \langle \mathcal{L}, \mathbf{x} \rangle \subseteq \mathbb{Z}\}$. Notice that $\mathcal{L}^*$ has the same rank as λ.

2.1.3 Gaussians

For $r > 0$, define the Gaussian function $\rho_r : H \to (0, 1]$ as $\rho_r(\mathbf{x}) := \exp(-\pi \|\mathbf{x}\|^2 / r^2)$. By normalizing this function, we obtain the *continuous Gaussian probability distribution* of width r, denoted by D_r, whose density is given by $r^{-n} \cdot \rho_r(\mathbf{x})$. We extend this to *elliptical* (non-spherical) Gaussian distributions in the basis $\{\mathbf{h}_i\}_{i\in[n]}$ as follows. Define $G = \{\mathbf{r} \in (\mathbb{R}^+)^n \mid r_{s_1+s_2+i} = r_{s_1+i}, \forall i \in [s_2]\}$; not this has symmetry mirroring that of H. For consistency with prior works, we sometimes use $r \in \mathbb{R}^+$ as shorthand for the all-rs vector $r\mathbf{1} \in G$. For $\mathbf{r} \in G$, a sample from $D_{\mathbf{r}}$ is given by $\sum x_i \mathbf{h}_i$, where each x_i is chosen independently from the (one-dimensional) Gaussian distribution D_{r_i} over $\mathbb{R}$. We equip partial ordering on G defined by $\mathbf{r}' \geq \mathbf{r}$ if $r'_i \geq r_i$ for all i.

Micciancio and Regev [MR07] introduced a lattice quantity called the *smoothing parameter*, and related to it various lattice quantities.

Definition 2.1 (Smoothing Condition)**.** *For a lattice $\mathcal{L} \subset H$, positive real $\varepsilon > 0$ and $\mathbf{r} \in G$, we write $\mathbf{r} \geq \eta_\varepsilon(\mathcal{L})$ if $\rho_{1/\mathbf{r}}(\mathcal{L}^* \backslash \{\mathbf{0}\}) \leq \varepsilon$, where $1/\mathbf{r} = (1/r_1, \ldots, 1/r_n)$.*

The following lemma justifies the name "smoothing parameter", and is an immediate generalization of [MR07, Lemma 4.1] to elliptical Gaussians.

Lemma 2.1. *For any lattice $\mathcal{L} \subset H$, positive real $\varepsilon > 0$, and $\mathbf{r} \geq \eta_\varepsilon(\mathcal{L})$, the statistical distance between $D_{\mathbf{r}} \mod \mathcal{L}$ and the uniform distribution over $H/\mathcal{L}$ is at most $\varepsilon/2$.*

Another application of the smoothing parameter is as follows.

Theorem 2.2 (Theorem 3.1 [Pei10]). *Let $\mathcal{L}_1, \mathcal{L}_2 \subset H$ be lattices, and let $\mathbf{r}_1, \mathbf{r}_2 \in G$. Define $\mathbf{r} = \mathbf{r}_1 + \mathbf{r}_2$, and $\mathbf{r}_3 \in G$ by $1/(\mathbf{r}_3)_i := 1/(\mathbf{r}_1)_i + 1/(\mathbf{r}_2)_i$. Assume that $\sqrt{\mathbf{r}_1} \geq \eta_\varepsilon(\mathcal{L}_1)$ and that $\sqrt{(\mathbf{r}_3)} \geq \eta_\varepsilon(\mathcal{L}_2)$ for some positive $\varepsilon \geq 1/2$, and let $\mathbf{c}_1, \mathbf{c}_2 \in H$ be arbitrary. Consider the following probabilistic experiment:*

$$\text{Choose } \mathbf{x}_2 \leftarrow D_{\mathcal{L}_2 + \mathbf{c}_2, \sqrt{\mathbf{r}_2}}, \text{ then choose } \mathbf{x}_1 \leftarrow \mathbf{x}_2 + D_{\mathcal{L}_1 + \mathbf{c}_1 - \mathbf{x}_2, \sqrt{\mathbf{r}_1}} \ .$$

Then the marginal distribution of $\mathbf{x}_1$ is within statistical distance of 8ε of $D_{\mathcal{L}_1 + \mathbf{c}_1, \sqrt{\mathbf{r}}}$.

The following is a standard fact from [Reg05, Claim 2.13].

Lemma 2.3. *For any lattice $\mathcal{L} \subset H$ and $\varepsilon \in (0,1)$, we have $\eta_\varepsilon(\mathcal{L}) \geq \sqrt{\log(1/\varepsilon)}/\lambda_1(\mathcal{L}^*)$.*

2.1.4 Computational Problems

In the following computation problems, a lattice $\mathcal{L}$ is represented by an arbitrary basis $\mathbf{B}$, and a lattice coset $\mathbf{e} + \mathcal{L}$ is represented by its distinguished representative $\overline{\mathbf{e}} = (\mathbf{e} + \mathcal{L}) \cap \mathcal{P}(\mathbf{B})$, where $\mathcal{P}(\mathbf{B}) := \mathbf{B} \cdot [-1/2, 1/2)^n$ is the fundamental parallelepiped of $\mathbf{B}$. We sometimes omit the family of lattices when it is the family of all latices in H.

Definition 2.2 (Gap Shortest Vector Problem). *For an approximation factor $\gamma = \gamma(n) \geq 1$ and a family of lattices $\mathfrak{L}$, the $\mathfrak{L}$-GapSVP_γ is: given a lattice $\mathcal{L} \in \mathfrak{L}$ and length $d > 0$, output YES if $\lambda_1(\mathcal{L}) \leq d$ and NO if $\lambda_1(\mathcal{L}) \geq \gamma d$.*

Definition 2.3 (Discrete Gaussian Sampling). *For a family of lattices $\mathfrak{L}$ and a function γ that maps lattices from $\mathfrak{L}$ to G, the $\mathfrak{L}$-DGS_γ is: given a lattice $\mathcal{L} \in \mathfrak{L}$ and a parameter $\mathbf{r} \geq \gamma(\mathcal{L})$, output an independent sample from a distribution that is within negligible statistical distance of $D_{\mathcal{L},\mathbf{r}}$.*

Definition 2.4 (Bounded Distance Decoding). *For a family of lattices $\mathfrak{L}$ and a function δ that maps lattices from $\mathfrak{L}$ to positive reals, the $\mathfrak{L}$-BDD_δ is: given a lattice $\mathcal{L} \in \mathfrak{L}$, a distance bound $d \leq \delta(\mathcal{L})$, and a coset $\mathbf{e} + \mathcal{L}$ where $\|\mathbf{e}\| \leq d$, output $\mathbf{e}$.*

Lemma 2.4 (Babai's round-off algorithm [Bab86]). *For every family of lattices $\mathfrak{L}$, then there is an efficient algorithm that solves $\mathfrak{L}$-BDD_δ, for $\delta(\mathcal{L}) = 1/2\lambda_n(\mathcal{L}^*)$.*

Definition 2.5 (Gaussian Decoding Problem [PRSD17]). *For a lattice $\mathcal{L} \subset H$ and a Gaussian parameter $g > 0$, the $\mathsf{GDP}_{\mathcal{L},g}$ is: given a coset $\mathbf{e} + \mathcal{L}$ where $\mathbf{e} \in H$ was drawn from D_g, find $\mathbf{e}$.*

2.2 Learning with Errors (LWE)

We recall the Learning With Errors (LWE) problem and its hardness. Let n, q be positive integers with $q \geq 2$, and $\alpha > 0$ a Gaussian parameter. We denote $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, and the torus by $\mathbb{T} = \mathbb{R}/\mathbb{Z}$.

Definition 2.6 (LWE Distribution). *For $\mathbf{s} \in \mathbb{Z}_q^n$, the* LWE *distribution $A_{\mathbf{s},\alpha}$ over $\mathbb{Z}_q^n \times \mathbb{T}$ is sampled by independently choosing uniformly random $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_q^n$ and an error term $e \leftarrow D_\alpha$, and outputting $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle / q + e \mod \mathbb{Z})$.*

Definition 2.7 (Decisional Average-Case LWE Problem). *For an integer $q = q(n) \geq 2$, a distribution φ over $\mathbb{Z}_q^n$, and a Gaussian parameter $\alpha = \alpha(n) \in (0,1)$. The* (average-case) decision version of the LWE problem, *denoted by* $\mathrm{LWE}_{n,q,\varphi,\alpha}$ *is to distinguish between the distribution $A_{s,\psi}$ and the uniform one over $\mathbb{Z}_q^n \times \mathbb{T}$, where $s \leftarrow \varphi$.*

When φ is the uniform distribution over $\mathbb{Z}_q^n$ we sometimes omit it from the subscript for consistency with prior works. From the same reason, we sometimes omit n from the subscript when it is clear from the context.

Theorem 2.5 (Theorem 3.1 [Reg05], Theorem 5.1 [PRSD17]). *Let $q = q(n) \geq 2$ be an integer and let $\alpha = \alpha(n) \in (0,1)$ be a Gaussian parameter such that $\alpha q \geq 2\sqrt{n}$. There is a polynomial-time quantum reduction from DGS_γ to $\mathrm{LWE}_{q,\alpha}$ where $\gamma := \sqrt{2n}\eta(\mathcal{L})/\alpha$.*

Though the theorem above gives evidence to the hardness of the LWE problem, it only considers the case where φ is the uniform distribution. This question was answered in [GKPV10, BLP+13] for distributions over $\{0,1\}^n$, showing a reduction based on the min-entropy of φ.

Theorem 2.6 (Theorem 4 [GKPV10]). *Let $q \geq 2$ be a prime integer and let $\alpha, \beta \in (0,1)$ be Gaussian parameters such that $\alpha/\beta = \mathrm{negl}(n)$. Let φ be a distribution over $\{0,1\}^n$ having min-entropy k. Then for $\ell = \frac{k-\omega(\log n)}{\log q}$ there is a (classical) probabilistic polynomial time reduction from $\mathrm{LWE}_{\ell,q,\alpha}$ to $\mathrm{LWE}_{n,q,\varphi,\beta}$.*

2.3 Algebraic Number Theory

In this subsection we review the necessary algebraic background, with emphasis on orders in number fields, and their differences from the ring of integers. For a broader background, that also emphases orders, we refer to [Ste08].

2.3.1 Number Fields, Orders and Ideals

A *number field* is a field extension $K = \mathbb{Q}(\zeta)$ obtained by adjoining an element ζ to the rationals $\mathbb{Q}$, where ζ satisfies the relation $f(\zeta) = 0$ for some irreducible polynomial $f(x) \in \mathbb{Q}[x]$, called *minimal polynomial* of ζ, which is monic without the loss of generality. The *degree* n of th number field is the degree of f.

Let K be some number field of degree n. An *order* $\mathcal{O} \subset K$ is a ring that is generated by n elements over $\mathbb{Z}$, i.e. $\mathcal{O} = \bigoplus_{i=1}^{n} \mathbb{Z} g_i$ for some $\{g_1, \ldots, g_n\} \subset \mathcal{O}$. It follows that the set of orders in K has a unique maximal element (under inclusion), which is called the *maximal-order*, and is denoted by $\mathcal{O}_K$. An element in a number field $x \in K$ is said to be *integral* if it is the root of some monic polynomial with (rational) integer coefficients. The set of all integral elements in K form a ring, called the *ring of integers* and it turns out to be $\mathcal{O}_K$.

Let $\mathcal{O}$ be some order in K. An ideal $\mathcal{I} \subseteq \mathcal{O}$ is an additive subgroup that is closed under multiplication by $\mathcal{O}$, i.e. $x \cdot a \in \mathcal{I}$ for every $x \in \mathcal{O}$ and $a \in \mathcal{I}$. Ideals in $\mathcal{O}_K$ are sometimes called *integral*. Every ideal in $\mathcal{O}$ could be generated by n elements over Z.

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 *quotient* is defined by $(\mathcal{I} : \mathcal{J}) := \{x \in K \mid x\mathcal{J} \subseteq \mathcal{I}\}$, and their *intersection* is simply their set theoretic intersection. Each of the former sets forms an ideal in $\mathcal{O}$.

An integral ideal $\mathfrak{p} \subset \mathcal{O}$ is *prime* if 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 $\mathcal{I} \supseteq \prod \mathfrak{p}_i$. Fractional ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{O}$ are *coprime*, if $\mathcal{I} + \mathcal{J} = \mathcal{O}$. For an integral ideal $\mathcal{I} \subseteq \mathcal{O}$, the set of *associated primes* of $\mathcal{I}$ is the set of all prime ideal of $\mathcal{O}$ that contains $\mathcal{J}$.

The *norm* of an ideal $\mathcal{I} \subset \mathcal{O}$ is its index as a subgroup of, i.e. $N(\mathcal{I}) := [\mathcal{O} : \mathcal{I}] = |\mathcal{O}/\mathcal{I}|$. We note that the norm of an ideal is consistent with the norm for field element, specifically $N(a\mathcal{O}) = |N(a)|$ for every $a \in \mathcal{O}$. 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 is again a fractional ideal.

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 $\mathcal{J}$, then it is unique and equal to $(\mathcal{O} : \mathcal{I})$, and is denoted by $\mathcal{I}^{-1}$. The set of invertible ideals of $\mathcal{O}$ forms a multiplicative group, with $\mathcal{O}$ being the unit element. It is denoted by $\mathfrak{I}(\mathcal{O})$. In the special case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order, *every* fractional ideal is invertible. Moreover, every fractional ideal $\mathcal{I}$ of $\mathcal{O}_K$ has *unique factorization* into prime ideals $\mathcal{I} = \prod \mathfrak{p}_i^{e_i}$ for some prime ideals $\mathfrak{p}_i$ and integers $e_i \in \mathbb{Z}$. However, this does not hold for non-maximal orders. There are fractional ideals which are *not invertible*, and there are invertible ideals that are *not a product of prime ideals*. In fact, every invertible ideal in $\mathcal{O}$ is not invertible in any other order $\mathcal{O}'$. We refer to [Con] for an introductory for invertible ideals in an order, and to [Ste08] for a more thorough background.

2.3.2 Embeddings and Geometry

A number field $K = \mathbb{Q}(\zeta)$ of degree n has exactly n ring embeddings (injective homomorphisms) $\sigma_i : K \to \mathbb{C}$. Concretely, these embeddings map ζ to each of the complex root of its minimal polynomial f. An embedding whose images lies in $\mathbb{R}$ (corresponding to a real root of f) is called a *real embedding*; otherwise it is called a *complex embedding*. Because complex roots of f come in conjugate pairs, so too do the complex embeddings. The number of real embeddings is denoted s_1 and the number of pairs of complex embeddings is denoted s_2, so we have $n = s_1 + 2s_2$. Be convention, we let $\{\sigma_j\}_{j \in [s_1]}$ be the real embeddings, and we order the complex embeddings so that $\sigma_{s_1+s_2+j} = \overline{\sigma_{s_1+j}}$ for $j \in [s_2]$. The *canonical embedding* $\sigma : K \to \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ is then defined as

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_n(x)) \ .$$

By identifying elements of K with their canonical embeddings on H, we can speak of the norms on K. For any $x \in K$ and any $p \in [1, \infty]$, the ℓ_p-norm of x is simply $\|x\|_p = \|\sigma(x)\|_p$.

Using the canonical embedding also allows us to think of the Gaussian distribution $D_{\mathbf{r}}$ over H, or its discrete analogue over lattice in H, as a distribution over K. Strictly speaking, the distribution $D_{\mathbf{r}}$ is not over K, but rather over the field tensor product $K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R}$, which is isomorphic to H.

2.3.3 Trace and Norm

The *trace* $Tr = Tr_{K/\mathbb{Q}} : K \to \mathbb{Q}$, and norm $N = N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ of an element $x \in K$ are the sum an product respectively of the embeddings:

$$Tr(x) := \sum_{i=1}^{n} \sigma_i(x) \qquad N(x) := \prod_{i=1}^{n} \sigma_i(x) \ .$$

Moreover, the (absolute) norm of an element coincides with the norm of the ideal generated by it, in any order $\mathcal{O}$. That is $|N(x)| = N(x\mathcal{O})$. Also, for all $x, y \in K$,

$$Tr(x \cdot y) = \sum_{i=1}^{n} \sigma_i(x) \cdot \sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle \ .$$

2.3.4 Ideal Lattices

Recall that a fractional ideal $\mathcal{I}$ of any order $\mathcal{O}$ has a $\mathbb{Z}$-basis $U = \{u_1, \ldots, u_n\}$. Therefore, under the canonical embedding σ, the ideal yields a full-rank *ideal lattice* $\sigma(\mathcal{I})$ having basis $\{\sigma(u_1), \ldots, \sigma(u_n)\} \subset H$. In particular, orders themselves are ideal lattices.

The (absolute) *discriminant* $\Delta(\mathcal{O})$ of an order $\mathcal{O}$ is defined to be the square of the fundamental volume of $\sigma(\mathcal{O})$. Equivalently $\Delta(\mathcal{O}) = |\det(Tr(b_i \cdot b_j))|$, where $b_1, \ldots, b_n$ is any basis of $\mathcal{O}$. Consequently, the fundamental volume of any ideal lattice $\mathcal{I}$ of $\mathcal{O}$ is $N(\mathcal{I})\sqrt{\Delta(\mathcal{O})}$. We denote by Δ_K the discriminant of K which is the discriminant of the ring of integers $\Delta(\mathcal{O}_K)$. Moreover, the discriminant of an order $\mathcal{O}$ is related to the discriminant of K by $\Delta(\mathcal{O}) = [\mathcal{O}_K : \mathcal{O}]^2 \Delta_K$.

The following classical lemma gives upper and lower bounds on the minimum distance of an ideal lattice.

Lemma 2.7. *Let K be some number field of degree n, let $\mathcal{O}$ be an order, and $\mathcal{I}$ a fractional ideal in it. Then, in any ℓ_p norm, for $p \in [1, \infty]$:*

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

As a corollary we get the following

Lemma 2.8. *Let K be some number field of degree n, let $\mathcal{O}$ be an order, and $\mathcal{I}$ a fractional ideal in it, then $\eta_\varepsilon(\mathcal{I}) \leq N(\mathcal{I})^{1/n} \cdot \delta_K$, where $\varepsilon = 2^{-n}$.*

All the computational problems defined for general lattices are immediately generalized to ideal lattices.

2.3.5 Duality

Let K be a number field, and $\mathcal{O} \subset K$ be some order. For any fractional ideal $\mathcal{I}$ of $\mathcal{O}$, it *dual* is defined as

$$\mathcal{I}^\vee = \{x \in K \mid Tr(x\mathcal{I}) \subset \mathbb{Z}\} \ .$$

It follows that $\mathcal{I}^\vee$ is a fractional ideal, and that $\sigma(\mathcal{I}^\vee) = \overline{\sigma(\mathcal{I})^*}$. The dual of the order itself $\mathcal{O}^\vee$ is called *co-different* ideal. For the special case where $\mathcal{O} = \mathcal{O}_K$ is the maximal order, we have that $N(\mathcal{O}_K^\vee) = {\Delta_K}^{-1}$.

We mention some useful properties regarding dual ideals.

Lemma 2.9 ([Con09, Section 3] [Con, Section 4])**.** *Let K be a number field and $\mathcal{O} \subset K$ an order. For any $\mathcal{I}, \mathcal{J}$ fractional ideals of $\mathcal{O}$ the following holds*

1. $(\mathcal{I}^\vee)^\vee = \mathcal{I}$.
2. $\mathcal{I} \subset \mathcal{J} \iff \mathcal{J}^\vee \subset \mathcal{I}^\vee$.

3. $(\mathcal{I}+\mathcal{J})^\vee = \mathcal{I}^\vee \cap \mathcal{J}^\vee$.

4. $(\mathcal{I}\cap\mathcal{J})^\vee = \mathcal{I}^\vee + \mathcal{J}^\vee$.

5. $\mathcal{I}\cdot\mathcal{I}^\vee = \mathcal{O}^\vee$.

6. *Further assuming that* $\mathcal{I}$ *is invertible,* $(\mathcal{I}\mathcal{J})^\vee = \mathcal{I}^{-1}\mathcal{J}^\vee$.

From the last item, the following is an immediate corollary:

Corollary 2.10. *Let* $\mathcal{I}$ *be a fractional ideal in* K*, and let* $0 \neq \alpha \in K$ *be a nonzero field element. Then*

$$(\alpha\mathcal{I})^\vee = \frac{1}{\alpha}\mathcal{I}^\vee \ .$$

We give a simple lemma relating the smoothing parameter of product of ideals.

Lemma 2.11. *Let* K *be some number field, and* $\mathcal{O}\subset K$ *an order. Let* $\mathcal{I},\mathcal{J}$ *be fractional ideals of* $\mathcal{O}$*, where* $\mathcal{I}$ *is invertible. Then, for every* $\varepsilon > 0$*,*

$$\eta_\varepsilon(\mathcal{I}\cdot\mathcal{J}) \leq \lambda_1^\infty(\mathcal{I})\cdot\eta_\varepsilon(\mathcal{J}) \ .$$

Proof. By the definition of the smoothing parameter, and Lemma 2.9,

$$\begin{aligned}\eta_\varepsilon(\mathcal{I}\cdot\mathcal{J}) &= \arg\min_{s>0}\left\{\rho_{1/s}\left((\mathcal{I}\cdot\mathcal{J})^\vee\backslash\{0\}\right)\leq\varepsilon\right\}\\ &= \arg\min_{s>0}\left\{\rho_{1/s}\left(\left(\mathcal{I}^{-1}\cdot\mathcal{J}^\vee\right)\backslash\{0\}\right)\leq\varepsilon\right\}\end{aligned}$$

Let $v\in\mathcal{I}$ be such that $\|v\| = \lambda_1^\infty(\mathcal{I})$. Since $vR\subseteq\mathcal{I}$, then $v^{-1}R\supseteq\mathcal{I}^{-1}$, and so $v^{-1}\mathcal{J}^\vee\supseteq\mathcal{I}^{-1}\cdot\mathcal{J}^\vee$. Hence, we get that,

$$\arg\min_{s>0}\left\{\rho_{1/s}\left(\left(\mathcal{I}^{-1}\cdot\mathcal{J}^\vee\right)\backslash\{0\}\right)\leq\varepsilon\right\} \leq \arg\min_{s>0}\left\{\rho_{1/s}\left(\left(v^{-1}\cdot\mathcal{J}^\vee\right)\backslash\{0\}\right)\leq\varepsilon\right\} \ .$$

For every $x\in\mathcal{J}^\vee$, we have that

$$\left\|v^{-1}x\right\| \geq \min_{i\in[n]}\left|\sigma_i(v^{-1})\right|\|x\| = \|x\| \,/\, \|v\|_\infty = \|x\| \,/\lambda_1^\infty(\mathcal{I}) \ .$$

Thus,

$$\arg\min_{s>0}\left\{\rho_{1/s}\left(\left(v^{-1}\cdot\mathcal{J}^\vee\right)\backslash\{0\}\right)\leq\varepsilon\right\} \leq \arg\min_{s>0}\left\{\rho_{\lambda_1^\infty(\mathcal{I})/s}\left(\mathcal{J}^\vee\backslash\{0\}\right)\leq\varepsilon\right\} \ ,$$

and the Lemma follows. □

2.3.6 Cancellation of Ideals

In what follows we describe a generalization of a Lemma 2.15 from [LPR10] which we state below. Generally speaking it allows us to cancel invertible factors in the quotient $\mathcal{I}\mathcal{L}/\mathcal{I}\mathcal{J}\mathcal{L}$ onto $\mathcal{L}/\mathcal{J}\mathcal{L}$ by multiplying by an appropriate "tweak" factor. Before doing so, we recall the Chinese Remainder Theorem. Throughout, we let K be a number field and let $\mathcal{O}\subset K$ be some order in it.

Theorem 2.12 (Chinese Remainder Theorem)**.** *Let* $\mathcal{I}$ *be a fractional ideal of* $\mathcal{O}$*, and let* $\mathfrak{p}_1,\ldots,\mathfrak{p}_n\subset\mathcal{O}$ *be* n *distinct prime ideals. Then the canonical* $\mathcal{O}$*-modules homomorphism* $\mathcal{I}/\left(\prod\mathfrak{p}_i\right)\mathcal{I}\to\bigoplus\mathcal{I}/\mathfrak{p}_i\mathcal{I}$ *is an isomorphism.*

The generalization of the lemma above for general orders is as follows.

Lemma 2.13. *Let $\mathcal{I}, \mathcal{J}$ be integral ideals in the order $\mathcal{O}$, where $\mathcal{I}$ is invertible, and let $\mathcal{L}$ be any fractional ideal in $\mathcal{O}$. Then, given the associated primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of $\mathcal{J}$, there exists an efficiently computable $t \in \mathcal{I}$ such that the mapping $\theta_t : \mathcal{L}/\mathcal{J}\mathcal{L} \to \mathcal{I}\mathcal{L}/\mathcal{I}\mathcal{J}\mathcal{L}$ given by $\theta_t(x) = t \cdot x$ is well-defined, and induces an isomorphism of $\mathcal{O}_K$-modules. Moreover, θ_t is efficiently computable given $\mathcal{I}, \mathcal{J}, \mathcal{L}$ and t. Finally, t could be replaced by any element from $\mathcal{I} \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i\mathcal{I}$.*

We first show that the mentioned difference $\mathcal{I} \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i\mathcal{I}$ is nonempty.

Proposition 2.14. *Let $\mathcal{I}$ be an invertible ideal, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be n distinct prime ideals. Then, the difference $\mathcal{I} \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i\mathcal{I}$ is nonempty. Moreover, an element in the difference can be found efficiently given $\mathcal{I}$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$.*

Proof. Since $\mathcal{I}$ is invertible, and $\mathfrak{p}_i \subsetneq \mathcal{O}$ then $\mathcal{I}/\mathfrak{p}_i\mathcal{I} \neq 0$, for each $i \in [n]$. In particular, there exists $\bar{t} \neq 0 \in \bigoplus \mathcal{I}/\mathfrak{p}_i\mathcal{I}$. By the Chinese Remainder Theorem (Theorem 2.12), there exists a corresponding $t \in \mathcal{I}$, such that $t \notin \mathfrak{p}_i\mathcal{I}$ for any $i \in [n]$. In particular, such t is efficiently computable. □

The rest of the proof uses the *local to global* principle, which, loosely speaking, shows that it is enough to prove the lemma for a class of "simpler" rings, which are called *local rings*. We give a short definition and a few facts about *localization* which we need for the proof.

Definition 2.8. *Let $\mathfrak{p} \subset \mathcal{O}$ be a prime ideal. The* localization of $\mathcal{O}$ at $\mathfrak{p}$*, denoted by $\mathcal{O}_\mathfrak{p}$, is the ring defined by*

$$\mathcal{O}_\mathfrak{p} := \{r/s \mid r \in \mathcal{O}, s \in \mathcal{O} \setminus \mathfrak{p}\} \subset K \ .$$

It is easy to verify that it indeed forms a ring.

It follows that the ideals of $\mathcal{O}_\mathfrak{p}$ are exactly

$$\mathcal{I}_\mathfrak{p} := \{i/s \mid r \in \mathcal{I}, s \in \mathcal{O} \setminus \mathfrak{p}\} \subseteq \mathcal{O}_\mathfrak{p} \ ,$$

for every ideal $\mathcal{I}$ of $\mathcal{O}$. As a result, for every ideals $\mathcal{I}, \mathfrak{p}$, where $\mathfrak{p}$ is prime, if $\mathfrak{p}$ is not an associated prime of $\mathcal{I}$ (i.e. $\mathcal{I} \not\subseteq \mathfrak{p}$), then $1 \in \mathcal{I}_\mathfrak{p}$, or equivalently $\mathcal{I}_\mathfrak{p} = \mathcal{O}_\mathfrak{p}$. Localization also respects various operation on ideal. In particular, for every fractional ideals $\mathcal{I}, \mathcal{J}$ of $\mathcal{O}$, and prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the following holds: $(\mathcal{I}\mathcal{J})_\mathfrak{p} = \mathcal{I}_\mathfrak{p}\mathcal{J}_\mathfrak{p}$, and $(\mathcal{I}/\mathcal{J})_\mathfrak{p} \simeq \mathcal{I}_\mathfrak{p}/\mathcal{J}_\mathfrak{p}$.

Given a mapping between two fractional ideals $f : \mathcal{I} \to \mathcal{J}$, we can extend it to a mapping $f_\mathfrak{p} : \mathcal{I}_\mathfrak{p} \to \mathcal{J}_\mathfrak{p}$ between the localizations of those ideals at a prime ideal $\mathfrak{p}$. This is done by defining

$$f_\mathfrak{p}(r/s) := f(r)/s \ .$$

We return to the proof. For the next step, we recall two key lemmas. The first, shows that being an isomorphism is a local property.

Proposition 2.15 ([Cla11, Proposition 7.14])**.** *For every $\mathcal{O}$-module homomorphism $f : \mathcal{I} \to \mathcal{J}$, f is an isomorphism if and only if for all prime ideals $\mathfrak{p}$ of $\mathcal{O}$, $f_\mathfrak{p} : \mathcal{I}_\mathfrak{p} \to \mathcal{J}_\mathfrak{p}$ is an isomorphism.*

The second, is a local characterization of invertible ideals.

Proposition 2.16 ([Ste08, Proposition 4.4])**.** *A fractional ideal $\mathcal{I}$ of $\mathcal{O}$ is invertible if and only if for all prime ideals $\mathfrak{p}$ of $\mathcal{O}$, $\mathcal{I}_\mathfrak{p}$ is a principal $\mathcal{O}_\mathfrak{p}$-ideal. In this case, every $t \in \mathcal{I} \setminus \mathfrak{p}\mathcal{I}$ is a generator.*

The proof now follows easily.

Lemma 2.13. Let $t \in \mathcal{I} \setminus \bigcup_{i=1}^{n} \mathfrak{p}_i\mathcal{I}$, which always exists by Proposition 2.14, and consider the $\mathcal{O}$-module homomorphism θ_t. By Proposition 2.15, it is sufficient to prove that $(\theta_t)_\mathfrak{q} : (\mathcal{L}/\mathcal{J}\mathcal{L})_\mathfrak{q} \to (\mathcal{I}\mathcal{L}/\mathcal{I}\mathcal{J}\mathcal{L})_\mathfrak{q}$ is an isomorphism for every prime ideal $\mathfrak{q}$ of $\mathcal{O}$.

Assume that $\mathfrak{q} \neq \mathfrak{p}_i$ for each i. Then $\mathcal{J}_\mathfrak{q} = \mathcal{O}_\mathfrak{q}$, and $(\mathcal{L}/\mathcal{J}\mathcal{L})_\mathfrak{q} = (\mathcal{I}\mathcal{L}/\mathcal{I}\mathcal{J}\mathcal{L})_\mathfrak{q} = 0$ so the claim holds trivially. Otherwise, since $\mathcal{I}$ is invertible, and since $t \notin \mathfrak{q}\mathcal{I}$, then by Proposition 2.16, $\mathcal{I}_\mathfrak{p} = \langle t \rangle$, and therefore $(\theta_t)_\mathfrak{q}$ is an isomorphism. □

2.3.7 Submodules of $R_q^\vee$

Let K be some number field and R it ring of integers. Let $\overline{\mathcal{M}^\vee} \subset R_q^\vee$ be some R-submodule. By the Correspondence Theorem, we get that $\overline{\mathcal{M}^\vee} = \mathcal{M}^\vee/qR^\vee$, for some R-submodule $qR^\vee \subset \mathcal{M}^\vee \subset R^\vee$. By Lemma 2.9 and Corollary 2.10, we can equivalently formulate this as $R \subset \mathcal{M} \subset 1/qR$, or $qR \subset q\mathcal{M} \subset R$. Since $q\mathcal{M}$ is an R-submodule of R, then it is an ideal $\mathcal{I}$. Moreover, we have the following:

$$\left|\overline{\mathcal{M}^\vee}\right| = \left|\mathcal{M}^\vee/qR^\vee\right| = \left|(\mathcal{M}^{-1}R^\vee)/(q\mathcal{M}\mathcal{M}^{-1}R^\vee)\right| = |R/\mathcal{I}| = N(\mathcal{I})$$

We deduce the following corollary:

Corollary 2.17. *Every R-submodule $\overline{\mathcal{M}^\vee}$ of $R_q^\vee$ is of the form $q\mathcal{I}^\vee/qR^\vee$ for some ideal $qR \subset \mathcal{I} \subset R$. Moreover, $\left|\overline{\mathcal{M}^\vee}\right| = N(\mathcal{I})$.*

2.4 The Ring-LWE Problem

Let K be number field having s_1 real embeddings, s_2 pairs of complex ones, and degree $n = s_1 + 2s_2$. We denote its ring of integers by $R = \mathcal{O}_K$, and the torus by $\mathbb{T} = K_\mathbb{R}/R^\vee$. Let $q \geq 2$ be a (rational) integer, and for any fractional ideal $\mathcal{I}$ of K, let $\mathcal{I}_q = \mathcal{I}/q\mathcal{I}$.

Definition 2.9 (Ring-LWE Distribution)**.** *For $s \in R_q^\vee$, referred to as "the secret", and an error distribution ψ over $K_\mathbb{R}$, a sample from the R-LWE* distribution *$A_{s,\psi}$ over $R_q \times \mathbb{T}$ is generated by sampling $a \xleftarrow{\$} R_q$, $e \leftarrow \psi$, and outputting $(a, b = a \cdot s/q + e \mod R^\vee)$.*

Definition 2.10 (Ring-LWE, Average-Case Decision Problem)**.** *Let φ be a distribution over $R_q^\vee$, and let Υ be a distribution over a family of error distributions, each over $K_\mathbb{R}$. The* average-case Ring-LWE decision problem*, denoted R-LWE$_{q,\varphi,\Upsilon}$, is to distinguish between independent samples from $A_{s,\psi}$ for a random choice of a "secret" $s \leftarrow \varphi$, and an error distribution $\psi \leftarrow \Upsilon$, and the same number of uniformly random and independent samples from $R_q \times \mathbb{T}$.*

We recall here the error distribution defined in [PRSD17].

Definition 2.11. *Fix an arbitrary $f(n) = \omega(\sqrt{\log n})$. For a real $\alpha > 0$, a distribution sampled from Υ_α is an elliptical Gaussian $D_\mathbf{r}$, where $\mathbf{r} \in G$ is sampled as follows: for each $1 \leq i \leq s_1$, sample $x_i \leftarrow D_1$ and set $r_i^2 = \alpha^2(x_i^2 + f^2(n))/2$. For each $s_1 + 1 \leq i \leq s_1 + s_2$, sample $x_i, y_i \leftarrow D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + f^2(n))/2$.*

Theorem 2.18 ([PRSD17, Theorem 6.2])**.** *Let K be an arbitrary field of degree n and $R = \mathcal{O}_K$ its ring of integers. Let $\alpha = \alpha(n) \in (0, 1)$, and let $q = q(n) \geq 2$ be a (rational) integer such that*

$\alpha q \geq 2\omega(1)$. *There is a polynomial-time quantum reduction from* $\mathfrak{I}(R)$*-DGS*$_\gamma$ *to* R-LWE$_{q\Upsilon_\alpha}$ *for any*

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

3 Order-LWE and Its Hardness

In this section we present a natural generalization of the Ring-LWE problem, which we call "Order-LWE". Then we state and prove a reduction from worst-case ideal-lattice problems to it.

3.1 The Order-LWE problem

In the Order-LWE problem, elements are sampled from an *order* in a number field, rather than the field's ring of integers (the ring of integers is the maximal order in the field). Our definition also considers different (ideal) moduli.

Let K be some number field, $\mathcal{O} \subset K$ an order, and let $\mathcal{Q}, \mathcal{I} \subset K$ be ideals of $\mathcal{O}$ with $u \in (\mathcal{I} : \mathcal{Q})$, where $\mathcal{Q}$ is integral. We denote the torus by $\mathbb{T} = K_\mathbb{R}/\mathcal{I}\mathcal{O}^\vee$. For ideals $\mathcal{J}, \mathcal{L}$ of $\mathcal{O}$, we denote $\mathcal{J}_\mathcal{L} = \mathcal{J}/\mathcal{J}\mathcal{L}$.

Definition 3.1 (Order-LWE Distribution)**.** *For* $s \in \mathcal{O}_\mathcal{Q}^\vee$ *and an error distribution* ψ *over* $K_\mathbb{R}$*, the* $\mathcal{O}$-LWE *distribution* $A_{s,\psi,u}$ *over* $\mathcal{O}_\mathcal{Q} \times \mathbb{T}$ *is sampled by independently choosing a uniformly random* $a \xleftarrow{\$} \mathcal{O}_\mathcal{Q}$ *and an error term* $e \leftarrow \psi$*, and outputting* $(a, b = u \cdot (a \cdot s) + e \mod \mathcal{I}\mathcal{O}^\vee)$*.*

Note that this is well-defined by our choice of u, since we have that

$$(\mathcal{I} : \mathcal{Q}) \cdot \mathcal{Q} \cdot \mathcal{O}^\vee \subseteq \mathcal{I}\mathcal{O}^\vee \ ,$$

$$(\mathcal{I} : \mathcal{Q}) \cdot \mathcal{O} \cdot (\mathcal{Q}\mathcal{O}^\vee) = (\mathcal{I} : \mathcal{Q}) \cdot \mathcal{Q} \cdot \mathcal{O}^\vee \subseteq \mathcal{I}\mathcal{O}^\vee \ .$$

Note that the Ring-LWE is a special case, where $\mathcal{O} = \mathcal{O}_K$ is the ring of integers, $\mathcal{Q} = q\mathcal{O}_K$ for some rational integer $q \in \mathbb{Z}$, $\mathcal{I} = \mathcal{O}_K$, and $u = 1/q$ (since $\mathcal{O}_K$ is a maximal order, then $(\mathcal{I} : \mathcal{Q}) = \mathcal{I}\mathcal{Q}^{-1}$, which is $1/qR$ for the Ring-LWE setting).

Definition 3.2 (Order-LWE, Average-Case Decision Problem)**.** *Let* φ *be a distribution over* $\mathcal{O}_\mathcal{Q}^\vee$*, and let* Υ *be a distribution over a family of error distributions, each over* $K_\mathbb{R}$*. The* average-case Order-LWE decision problem*, denoted* $\mathcal{O}$-LWE$_{(\mathcal{Q},\mathcal{I},u),\varphi,\Upsilon}$*, is to distinguish between independent samples from* $A_{s,\psi,u}$ *for a random choice of a "secret"* $s \leftarrow \varphi$*, and an error distribution* $\psi \leftarrow \Upsilon$*, and the same number of uniformly random and independent samples from* $\mathcal{O}_\mathcal{Q} \times \mathbb{T}$*.*

When φ is the uniform distribution, we sometimes omit it from the subscript. We also omit $\mathcal{I}$ when it is equal to $\mathcal{O}$. If in addition $\mathcal{Q} = n\mathcal{O}$ for some rational integer $n \in \mathbb{Z}$, we simply write n for the subscript, and implicitly assume that $u = 1/n$. Using those notations gives us consistency with the usual notation, i.e. $\mathcal{O}$-LWE$_{q,\Upsilon}$=R-LWE$_{q,\Upsilon}$.

3.2 Hardness of Order-LWE

We now state the hardness result of the Order-LWE problem, and compare it to the hardness of Ring-LWE (see Theorem 2.18).

First, we generalize the error distribution Υ_α from Definition 2.11 to be elliptical according to u.

Definition 3.3. *Fix an arbitrary $f(n) = \omega(\sqrt{\log n})$. For $\alpha > 0$ and $u \in K$, a distribution sampled from $\Upsilon_{u,\alpha}$ is an elliptical Gaussian $D_{\mathbf{r}}$, where $\mathbf{r} \in G$ is sampled as follows: for $i = 1, \ldots, s_1$, 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 $i = s_1 + 1, \ldots, s_1 + s_2$, sample $x_i, y_i \leftarrow D_{1/\sqrt{2}}$ and set $r_i^2 = r_{i+s_2}^2 = \alpha^2(x_i^2 + y_i^2 + (f(n) \cdot |\sigma_i(u)| / \|u\|_\infty)^2)/2$.*

Note that for any $u \in K$ satisfying $\sigma_1(u) = \ldots = \sigma_n(u)$ (and therefore rational), $\Upsilon_{u,\alpha}$ degenerates to Υ_α. Otherwise, $\Upsilon_{u,\alpha}$ is strictly narrower than Υ_α.

We now present the main theorem for the Order-LWE problem. Recall the definition of the group of invertible ideals of an order $\mathcal{O}$, denoted by $\mathfrak{I}(\mathcal{O})$, and the DGS_γ problem (Definition 2.3).

Theorem 3.1. *Let K be an arbitrary number field of degree n and $\mathcal{O} \subset K$ an order. Let $\mathcal{Q}, \mathcal{I} \subset K$ be ideals of $\mathcal{O}$ with $u \in (\mathcal{I} : \mathcal{Q})$, where $\mathcal{Q}$ is integral, and let $\alpha \in (0, 1)$ be such that $\alpha / \|u\|_\infty \geq 2 \cdot \omega(1)$. There is a polynomial-time quantum reduction from $\mathfrak{I}(\mathcal{O})$-$\mathsf{DGS}_\gamma$ to $\mathcal{O}$-$\mathrm{LWE}_{(\mathcal{Q},\mathcal{I},u),\Upsilon_{u,\alpha}}$, and*

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

One can verify that Theorem 2.18, follows from the above as a special case. More generally, consider the case where we choose $\mathcal{Q} = q\mathcal{O}$ for some rational integer $q \neq 0$, $\mathcal{I} = \mathcal{O}$, and $u = 1/q$. Then $\eta(\mathcal{Q}\mathcal{L})\,\|u\|_\infty = \eta(\mathcal{L})$, and the parameters γ from Theorem 2.18 and Theorem 3.1 are equal.

As another special-case, we consider the simple extension of R-LWE where q is replaced by some other ideal in $\mathcal{O}_K$. Formally, consider $\mathcal{I} = \mathcal{O} = \mathcal{O}_K$, and u to be the shortest vector, in ℓ_∞-norm, in $(\mathcal{O}_K : \mathcal{Q}) = \mathcal{Q}^{-1}$. Using Lemma 2.11 and Lemma 2.7, we get that the first term in γ is at-most $\delta_k^2 \cdot \eta(\mathcal{L}) \cdot \sqrt{2}/\alpha \cdot \omega(1)$. By Lemma 2.3, $\eta(\mathcal{L}) > \omega(\sqrt{\log n})/\lambda_1\left(\mathcal{L}^\vee\right)$, so γ is equal to the first term for $\alpha < \sqrt{\log n/n}$. In this case, our result gives γ that is larger by at most δ_k^2 than when using modulus $\mathcal{Q} = q\mathcal{O}$. Finally, recall that when $\mathcal{O} = \mathcal{O}_K$ is a maximal order, then any fractional ideal $\mathcal{L} \subset K$ is invertible, so $\mathfrak{I}(\mathcal{O}_K)$ is the set of all fractional ideals in $\mathcal{O}_K$.

We turn to a high level proof of Theorem 3.1, which follows the blueprint analogous proofs in the context of LWE [Reg05], and R-LWE [LPR10, PRSD17]. The proof follows from the following iterative step. Let $r > 0$ be some real, we let $W_r \subset G$ be some subset of polynomial size, where each coordinate is at least by r. For the exact definition we refer to [PRSD17].

Lemma 3.2. *There exists an efficient quantum algorithm that given an oracle that solves $\mathcal{O}$-$\mathrm{LWE}_{(\mathcal{Q},\mathcal{I},u),\Upsilon_{u,\alpha}}$ and the following input:*

- *ideals $\mathcal{Q}, \mathcal{I} \subset K$ of $\mathcal{O}$ with $u \in (\mathcal{I} : \mathcal{Q})$, where $\mathcal{Q}$ is integral and contains a product of known prime ideals,*
- *a number $\alpha \in (0, 1)$,*
- *a fractional ideal $\mathcal{L} \in \mathfrak{I}(\mathcal{O})$,*
- *a real $r \geq \sqrt{2} \cdot \eta(\mathcal{Q}\mathcal{L})$ such that $r' := r \cdot \|u\|_\infty / \alpha \cdot \omega(1) \geq \sqrt{2n}/\lambda_1\left(\mathcal{L}^\vee\right)$,*
- *polynomially many samples from the discrete Gaussian distribution $D_{\mathcal{L},\mathbf{r}}$ for each $\mathbf{r} \in W_r$,*
- *and a vector $\mathbf{r}' \in G$ where $\mathbf{r}' \geq r'$,*

it outputs an independent sample from $D_{\mathcal{L},\mathbf{r}'}$.

Using Lemma 3.2, Theorem 3.1 follows in the same way as in previous works. We sketch the outline here for the sake of completeness.

We begin with sampling from wide enough Gaussian for each $\mathbf{r} \in W_r$, where $r \geq 2^{2n}\lambda_n(\mathcal{L})$ is large enough so that sampling from $D_{\mathcal{L},\mathbf{r}}$ can be done efficiently (see [Reg05, Lemma 3.2]). Then, given those samples, we apply the iterative step from Lemma 3.2 to generate samples from $D_{\mathcal{L},\mathbf{r}'}$ for each $\mathbf{r}' \in W_{r'}$. We repeat this step until we get the desired Gaussian parameter $s \geq \gamma$. Note that γ from the statement of the theorem, corresponds to values of r, r' satisfying the conditions of Lemma 3.2.

The proof of Lemma 3.2 itself follows from a combination of the two following lemmas. The first is a classical reduction from GDP (see Definition 2.5) to $\mathcal{O}$-LWE, which uses Gaussian samples. This is a generalization of [PRSD17, Lemma 6.6].

Lemma 3.3. *There exists a probabilistic polynomial-time (classical) algorithm that given an oracle that solves $\mathcal{O}$-LWE$_{(\mathcal{Q},\mathcal{I},u),\Upsilon_{u,\alpha}}$, and the following input:*

- *ideals $\mathcal{Q},\mathcal{I} \subset K$ with $u \in (\mathcal{I} : \mathcal{Q})$, where $\mathcal{Q}$ is integral and contains a product of known prime ideals,*
- *a number $\alpha \in (0,1)$,*
- *an invertible fractional ideal $\mathcal{L} \in \mathfrak{I}(\mathcal{O})$,*
- *a real $r \geq \sqrt{2} \cdot \eta(\mathcal{Q}\mathcal{L})$,*
- *and polynomially many samples from the discrete Gaussian distribution $D_{\mathcal{L},\mathbf{r}}$ for each $\mathbf{r} \in W_r$,*

it solves $\mathsf{GDP}_{\mathcal{L}^\vee,g}$ for any $g = o(1) \cdot \alpha/(\sqrt{2}r \cdot \|u\|_\infty)$.

The second is a quantum algorithm that produces narrower Gaussian samples given a GDP oracle.

Lemma 3.4 ([PRSD17, Lemma 6.7])**.** *There is an efficient quantum algorithm that, given any n-dimensional lattice $\mathcal{L}$, a real $g < \lambda_1(\mathcal{L}^\vee)/(2\sqrt{2n})$, a vector $\mathbf{r} \geq 1$, and an oracle that solves $\mathsf{GDP}_{\mathcal{L}^\vee,g}$ (with all but negligible probability), outputs an independent sample from $D_{\mathcal{L},\mathbf{r}/(2g)}$.*

3.3 Proof of Lemma 3.3

The proof of the lemma is similar to the one of [PRSD17, Lemma 6.6], and is based on parts of it. We begin with a reduction that translates BDD instances into $\mathcal{O}$-LWE samples. The Lemma is an adaptation of [PRSD17, Lemma 6.8] (which in turn is an adaptation of [LPR10, Lemma 4.7]).

Lemma 3.5. *There is a probabilistic polynomial time algorithm that takes as input*

- *ideals $\mathcal{Q},\mathcal{I} \subset K$ with $u \in (\mathcal{I} : \mathcal{Q}\mathcal{O}^\vee)$, where $\mathcal{Q}$ is integral and contains a product of known prime ideals,*
- *an invertible fractional ideal $\mathcal{L} \in \mathfrak{I}(\mathcal{O})$,*
- *a coset $e + \mathcal{L}^\vee$ and a bound $d \geq \|e\|_\infty$,*
- *a real $r \geq \sqrt{2} \cdot \eta(\mathcal{Q}\mathcal{L})$,*

- *and polynomially many samples from the discrete Gaussian distribution $D_{\mathcal{L},\mathbf{r}}$ for some $\mathbf{r} \geq r$.*

It outputs samples that are statistically close to the Order-LWE distribution $A_{s,u,D_{\mathbf{r}'}}$, where the coordinates of $\mathbf{r}'$ are given by $(r'_i)^2 := (r_i \left|\sigma_i(e)\sigma_i(u)\right|)^2 + (rd \left\|u\right\|_\infty)^2$.

Proof. By a scaling argument, we can assume without the loss of generality that $\mathcal{L} \subseteq \mathcal{O}$ is an integral ideal. Denote $y = x + e$, where $x \in \mathcal{L}^\vee$, such that $y \mod \mathcal{L}^\vee = e + \mathcal{L}^\vee$ is the input coset.

On inputs as in the statement of the Lemma, the algorithm works as follows:

1. Compute an element $t \in \mathcal{L}$ as in Lemma 2.13 for the ideal $\mathcal{L}, \mathcal{Q}$. In particular, the mapping $\theta_t : x \mapsto t \cdot x$ induces isomorphisms $\theta_t : \mathcal{O}/\mathcal{Q} \xrightarrow{\sim} \mathcal{L}/\mathcal{Q}\mathcal{L}$, and $\theta_t : \mathcal{L}^\vee/\mathcal{Q}\mathcal{L}^\vee \xrightarrow{\sim} \mathcal{O}^\vee/\mathcal{Q}\mathcal{O}^\vee$.
2. Sample $z \leftarrow D_{\mathcal{L},\mathbf{r}}$ and $e' \leftarrow D_{rd\left\|u\right\|_\infty}$.
3. Output $a = {\theta_t}^{-1}(z \mod \mathcal{Q}\mathcal{L})$ and $b = u \cdot (zy) + e' \mod \mathcal{I}\mathcal{O}^\vee$.

Clearly the algorithm is efficient. Therefore we need to show that the output satisfies the statement of the Lemma.

Since $\mathbf{r} \geq \eta(\mathcal{Q}\mathcal{L})$, then the distribution $D_{\mathcal{L},\mathbf{r}} \mod \mathcal{Q}\mathcal{L}$ is statistically close to uniform over $\mathcal{L}_\mathcal{Q}$. Since $\theta_t : \mathcal{O}/\mathcal{Q} \xrightarrow{\sim} \mathcal{L}/\mathcal{Q}\mathcal{L}$ is an isomorphism, and in particular a bijection, then a is distributed uniformly close to uniform over $\mathcal{O}_\mathcal{Q}$.

We turn to analyze the marginal distribution of b conditioned on some value of a. We have that

$$b = u \cdot z \cdot y + e' = u \cdot z \cdot x + u \cdot z \cdot e + e' \mod \mathcal{I}\mathcal{O}^\vee \ .$$

Consider the first term $uzx \mod \mathcal{I}\mathcal{O}^\vee$. By the way we choose a, we have that

$$z = \theta_t(a) = t \cdot a \mod \mathcal{Q}\mathcal{L} \ .$$

Since $u \in (\mathcal{I} : \mathcal{Q})$, $x \in \mathcal{L}^\vee = \mathcal{L}^{-1}\mathcal{O}^\vee$, and $z \in \mathcal{L}$, then

$$u \cdot z \cdot x = u \cdot t \cdot a \cdot x \mod \mathcal{I}\mathcal{O}^\vee \ .$$

Similarly, we have that

$$t \cdot x = \theta_t(x) = s \mod \mathcal{Q}\mathcal{O}^\vee \ ,$$

so

$$u \cdot a \cdot t \cdot x = u \cdot (a \cdot s) \mod \mathcal{I}\mathcal{O}^\vee \ .$$

Finally, we analyze the error term $u \cdot z \cdot e + e'$. Conditioned on a, the distribution of z is $D_{\mathcal{Q}\mathcal{L}+c,\mathbf{r}}$ for $c = {\theta_t}^{-1}(a)$. Since $\mathbf{r} \geq \eta(\mathcal{Q}\mathcal{L})$, then by Lemma 2.2 the distribution of $u \cdot z \cdot e + e'$ is statistically close to an elliptical Gaussian distribution with parameter

$$(r'_i)^2 = (r_i \sigma_i(e)\sigma_i(u))^2 + (rd \left\|u\right\|_\infty)^2$$

□

Note that when y is sampled as in $\mathsf{GDP}_{\mathcal{L}^\vee,g}$ with $g := \alpha/(\sqrt{2} \cdot r \cdot \left\|u\right\|_\infty)$ and then apply the lemma with $d := g \cdot f(n)$, we get the error distribution as in definition 3.3.

The final part of the proof follows from the following lemma.

Lemma 3.6 ([PRSD17, Adaptation of Lemma 6.6])**.** *There exists a probabilistic polynomial-time algorithm that given an oracle and inputs as in Lemma 3.3, and additionally an oracle that transforms a $\mathsf{GDP}_{\mathcal{L}^\vee,g}$ into samples from $A_{s,u,D_{\mathbf{r}'}}$ for some $s \in R^\vee_\mathcal{Q}$, and $\mathbf{r}'$ satisfying $\mathbf{r}'_i = t_i \cdot |\sigma_i(e)|^2 + v$, where $g = o(1) \cdot \alpha/(\sqrt{2}r \cdot \left\|u\right\|_\infty)$, t_i depends on r_i and v is independent of i, it solves $\mathsf{GDP}_{\mathcal{L}^\vee,g}$.*

4 New Hardness for Polynomial-LWE

The *polynomial learning with errors* problem, or PLWE in short, introduced by Stehlé et al. [SSTX09][6] is closely related to both the Ring-LWE and Order-LWE problems. PLWE has an advantage of having very simple interface which is useful for manipulations and thus also for applications and implementations. In a recent work, Rosca, Stehlé and Wallet [RSW18] showed a reduction from worst-case ideal-lattice problems to PLWE. In this section, we show that the hardness of Order-LWE that we proved in Section 3, implies a different worst-case hardness result for PLWE, essentially by relating it to a different class of lattices than those considered in [RSW18] while avoiding a loss incurred in their reduction which in some number fields could be large or even unbounded. In what follows we start with an informal description of the PLWE problem, the [RSW18] result, our result and a comparison. This is a followed by a more detailed and formal treatment.

Consider a number field K defined by an irreducible polynomial f, so that $K = \mathbb{Q}(x)/f$. Recall that the Ring-LWE distribution is defined with respect to some "secret" element s from the dual of the ring of integers of K (denoted $\mathcal{O}_K^\vee$). The Order-LWE distribution is defined similarly, but with s coming from an arbitrary order in K. In the PLWE setting, s is an element of the ring $\mathcal{O} := \mathbb{Z}[x]/f$, i.e. a polynomial with integer coefficients in the number field. There are number fields for which $\mathcal{O}_K \neq \mathcal{O}$, however it is always true that $\mathcal{O}$ is an order of K. We highlight that in PLWE, unlike Ring-LWE and Order-LWE, s is an element of the order itself, and not its dual. In particular, PLWE can be seen as a dual version of Order-LWE.[7]

The aforementioned [RSW18] presented a reduction from Ring-LWE to PLWE, and as an immediate corollary (using the worst case hardness of RLWE) they show a reduction from worst-case ideal-lattice problems to PLWE. Their reduction depends on properties of the polynomial f and consists of two steps. First, going from Ring-LWE to a problem they call "dual-PLWE", but in our terminology is simply Order-LWE over the order $\mathcal{O} := \mathbb{Z}[x]/f$. The second is a reduction from that specific instance of Order-LWE with order $\mathcal{O}$ to PLWE.

Combing the second step of [RSW18] (going from Order-LWE to PLWE) with our Theorem 3.1, we get an alternative reduction from worst-case ideal-lattice problems to PLWE. Whereas in the worst-case reduction of [RSW18] the approximation factor increase by a factor that depends on f, and could be unbounded in general, our hardness result avoids this increment. To compare, while incurs a smaller loss in the approximation factor for the worst-case problem, it applies to a different class of lattices. The two classes of lattices are disjoint (see further explanation after the formal result statement), thus our result provides independent corroboration to the hardness of PLWE while relying on a different worst-case problem.

The formal definitions and hardness result follow, along with a more detailed and formal comparison of the results. We let K be a number field of degree n defined by a polynomial f. We denote $\mathcal{O} := \mathbb{Z}[x]/f$, and $R := \mathcal{O}_K$. The PLWE distribution and problem are defined as follows.

Definition 4.1 (PLWE Distribution and Problem [SSTX09])**.** *For a rational integer $q \geq 2$, a ring element $s \in \mathcal{O}_q$, and an error distribution φ over $K_\mathbb{R}/\mathcal{O}$, the* PLWE distribution *over $\mathcal{O}_q \times K_\mathbb{R}/\mathcal{O}$, denoted by $B_{s,\varphi}$, is sampled by independently choosing a uniformly random $a \xleftarrow{\$} \mathcal{O}_q$ and an error term $e \leftarrow \varphi$, and outputting $(a, b = (a \cdot s)/q + e \mod \mathcal{O})$.*

[6] As "ideal-LWE". The name PLWE was used in [BV11a].

[7] Another difference between Ring/Order-LWE and PLWE is that in the latter, the error distribution is specified using the so called *coefficients embedding*, and not the *canonical embedding*. This is immaterial for this section and we avoid this distinction for the sake of simplicity.

The PLWE decision problem*, denoted $PLWE_{q,\Upsilon}$, is to distinguish between independent samples from $B_{s,\psi}$ for a random choice of $s \leftarrow \mathcal{O}_q$, and an error distribution $\psi \leftarrow \Upsilon$, and the same number of uniformly random and independent samples from $\mathcal{O}_q \times K_{\mathbb{R}}/\mathcal{O}$.*

We now turn to present and compare the two worst-case to average-case reductions.

Theorem 4.1 (Adapted from Theorem 4.2 of [RSW18])**.** *Let $q \geq 2$ be some rational integer,*[8] *and let $\mathbf{r}$ be a Gaussian parameter. Then, there exists a probabilistic polynomial time reduction from R-$\mathrm{LWE}_{q,\mathbf{r}}$ to $\mathcal{O}$-$\mathrm{LWE}_{q,t^2\mathbf{r}}$, where t is some element in $R^\vee$ whose size is bounded as a function of f.*

The factor term t in the theorem depends on f and could be arbitrarily large, however [RSW18] show that there are families of f (in particular ones that frequently occur in cryptographic constructions) for which t is polynomially bounded.

Combined with Theorem 2.18 we get the following.

Corollary 4.2 (The [RSW18] Worst-Case Hardness for PLWE)**.** *With the same notations as above, let $\alpha \in (0,1)$ such that $\alpha \|t\|_\infty^2 q \geq 2\omega(1)$. There is a reduction from $\mathfrak{I}(R)$-DGS_γ to $\mathcal{O}$-$\mathrm{LWE}_{q,\Upsilon_\alpha}$ for any*

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

Using Order-LWE (Theorem 3.1) we get the following.

Corollary 4.3 (Worst-Case Hardness of PLWE from Order-LWE)**.** *Let $q \geq 2$ be some rational integer, and let $\alpha \in (0,1)$ be such that $\alpha q \geq 2\omega(1)$. Then there is a reduction from $\mathfrak{I}(\mathcal{O})$-$\mathsf{DGS}_\gamma$ to $\mathcal{O}$-$\mathrm{LWE}_{q,\Upsilon_\alpha}$ for any*

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

In Corollary 4.3 the parameter α can be smaller by a factor of $\|t\|_\infty^2$. As a result, one gets hardness based on the worst-case hardness with a smaller approximation factor γ. Another difference between the two results is that the ideal-lattices in Corollary 4.2 are the invertible ideals in $R = \mathcal{O}_K$. In comparison, the ideal lattices in Corollary 4.3 are the invertible ideals in $\mathcal{O} = \mathbb{Z}[x]/f$. Note that those families are disjoint, as any ideal can be invertible in at most a single order. Despite being disjoint, the two families can be related by an ideal of both $\mathcal{O}$ and $\mathcal{O}_K$ called the *conductor ideal*, see [Con] for reference.

5 Sampling RLWE Secrets From Ideals

This section focuses on sampling the secret distribution from a (fractional) ideal of the ring of integers. We show in Section 5.1 that even if the ideal from which the secret is sampled has high entropy, this is not necessarily sufficient to guarantee security. In fact, noise levels that are sufficient to guarantee security for uniform secrets fail for secrets from high entropy ideals. Then in Section 5.2, we show that increasing the noise level even slightly above the level that we prove insecure is sufficient to restore security.

Throughout this section, let K be some number field of degree n, $R = \mathcal{O}_K$ its ring of integers, Δ_K its (absolute) discriminant, and $\delta_k = \Delta_K^{1/n}$ its root discriminant.

[8] The integer q needs to satisfy some property which is satisfied by all but finitely many integers and is immaterial for our purposes.

5.1 Insecure Instantiations

We show that when the secret is sampled from an ideal, even with high min-entropy, RLWE can become insecure. To this end, we present a family of high min-entropy distributions Φ, such that the search version of R-LWE$_{q,\varphi,\Upsilon}$ is solvable in polynomial time, for every $\varphi \in \Phi$ and q, Υ for which the "standard" RLWE (from Theorem 2.18) is secure.

We first present a general theorem and then explain how it is instantiated in the interesting special case of cyclotomic fields.

Theorem 5.1. *Let $\mathcal{Q} \subseteq qR$ be some integral ideal. Then, there exists a non-uniform polynomial time algorithm that solves search-R-LWE$_{q,\varphi,\Upsilon}$ with non-negligible probability for any distribution φ over $q\mathcal{Q}^\vee/qR^\vee$ and any distribution Υ over a family of error distributions, each over $K_\mathbb{R}$ and is $(1/(2\lambda_n(\mathcal{Q})), \varepsilon)$-bounded, for some non-negligible $\varepsilon = \varepsilon(n)$. Moreover, the algorithm can recover s given a single sample from $A_{s,\psi}$.*

Proof. Let $\{v_1, \ldots, v_n\} \subset \mathcal{Q}$ be a set of short independent set of vectors in the lattice $\mathcal{Q}$. Namely, a linearly independent set (over $\mathbb{Z}$) such that $\|v_i\| \leq \lambda_n(\mathcal{Q})$ for every $1 \leq i \leq n$.

Consider a sample $b = as/q + e \mod R^\vee$. Since $s \in q\mathcal{Q}^\vee/qR^\vee$, and $a \in R/qR$, it follows that $as/q \in \mathcal{Q}^\vee/R^\vee$. Condition on the event that $\|e\| \leq 1/(2\lambda_n(\mathcal{Q}))$, which occurs with non-negligible probability. Viewing b as a $\mathsf{BDD}_{\mathcal{Q}^\vee, 1/(2\lambda_n(\mathcal{Q}))}$ instance, and since for every $i \in [n]$

$$\|e \cdot v_i\| \leq \|e\| \cdot \|v_i\| \leq 1/2 \ ,$$

we get, by Lemma 2.4, that Babai's round-off algorithm outputs as/q. With non-negligible probability, a is invertible, so we can recover s. □

Consider the case where K is a cyclotomic field. Hence, by Lemma 2.7, $\lambda_n(\mathcal{Q}) = \lambda_1(\mathcal{Q}) \geq \sqrt{n}N(\mathcal{Q})^{1/n}$. Therefore, for $\alpha \leq O(N(\mathcal{Q})^{-1/n})$, the distribution Υ_α matches the condition from Theorem 5.1 (every distribution in Υ_α is $(O(\alpha\sqrt{n}), \mathrm{negl}(n))$-bounded). Assuming that q is prime, and splits completely over R, which is a useful case for applications, it follows that $N(\mathcal{Q}) = q^k$, and therefore the uniform distribution over $q\mathcal{Q}^\vee/qR^\vee$ has entropy $k \log q$, by Corollary 2.17. In particular, the ranges for α from Theorem 2.18 and Theorem 5.1 intersect whenever $k \leq (1 - o(1)) \cdot n \log q$. We summarize in below.

Corollary 5.2. *Let K be a cyclotomic number field of degree n. For every $\varepsilon > 0$ there exists a family of distribution Φ, each over $R_q^\vee$ and with min-entropy $(1-\varepsilon)n \log q$, such that R-LWE$_{q,\varphi,\Upsilon_\alpha}$ is solvable in polynomial time for every $\varphi \in \Phi$, whereas R-LWE$_{q,\Upsilon_\alpha}$ has hardness as in Theorem 2.18, where $\alpha = \omega(1/q)$ and $q = n^{O(1/\varepsilon)}$.*

5.2 Secure Instantiations

We begin with some notations for this subsection. Let $q \geq 2$ be a rational integer, and let $\mathcal{Q} \supset qR$. Consider the integral ideal $\mathcal{P} := q\mathcal{Q}^{-1}$, and note that $\mathcal{Q}$ and $\mathcal{P}$ are coprime and satisfy $\mathcal{Q}\mathcal{P} = \mathcal{Q} \cap \mathcal{P} = qR$. Using the identities from Lemma 2.9, we get that $R^\vee = q\mathcal{Q}^\vee + q\mathcal{P}^\vee$ and that $qR^\vee = q\mathcal{Q}^\vee \cap q\mathcal{P}^\vee$, and therefore, by the Chinese Remainder Theorem, we get that $R_q^\vee \simeq R_{q\mathcal{Q}^\vee}^\vee \times R_{q\mathcal{P}^\vee}^\vee$, given by $x \mapsto (x \mod q\mathcal{Q}^\vee, x \mod q\mathcal{P}^\vee)$ (see Theorem 2.12). For compactness of notations, we denote $[x]_{q\mathcal{Q}^\vee} := x \mod q\mathcal{Q}^\vee$. Finally, we extend the operators $[\cdot]_{q\mathcal{Q}^\vee}, [\cdot]_{q\mathcal{P}^\vee}$ to distributions over $K_\mathbb{R}$ naturally.

Theorem 5.3. *Let $q, \mathcal{Q}, \mathcal{P}$ be as described above, and let $\alpha \in (0,1)$. There is a polynomial time reduction from R-LWE$_{(\mathcal{Q},u),\Upsilon_\alpha}$ to R-LWE$_{q,U(q\mathcal{Q}^\vee/qR^\vee),\Upsilon_\alpha}$, where $u \in \mathcal{Q}^{-1}$ is a vector of norm $\|u\|_\infty \leq O\left(\frac{n\delta_K}{N(\mathcal{Q})^{1/n}}\right)$.*

Denote the uniform distribution $U(q\mathcal{Q}^\vee/qR^\vee)$ by φ. Combined with Theorem 3.1, we get that for error parameter $\alpha \geq \omega(n\delta_K N(\mathcal{Q})^{-1/n})$, solving R-LWE$_{q,\varphi,\Upsilon_\alpha}$ is at least as hard as solving worst case ideal-lattice problems. On the other hand, in the special case where K is a cyclotomic number field, by Corollary 5.2, for error parameter $\alpha \leq O(N(\mathcal{Q})^{-1/n})$, R-LWE$_{q,\varphi,\Upsilon_\alpha}$ becomes solvable in polynomial time. We summarize in below.

Corollary 5.4. *Let K be a cyclotomic number field of degree n, $R = \mathcal{O}_K$ it ring of integers, let $k = k(n) \in [n]$ be an integer, and let $q = q(n) \geq 2$ be an integer prime that splits completely over R. Let $\mathcal{Q} \supset qR$ be an integral ideal with norm q^k, and let φ be the uniform distribution over $q\mathcal{Q}^\vee/qR^\vee$ (which has min-entropy $k \log q$). Then, there exists a threshold $T = q^{-k/n}$ such that for every $\alpha \leq O(T)$, R-LWE$_{q,\varphi,\Upsilon_\alpha}$ is solvable in polynomial time using a single sample. But, if $\alpha \geq \omega(n\delta_K T)$ then R-LWE$_{q,\varphi,\Upsilon_\alpha}$ is indistinguishable from uniform assuming the hardness of $\mathfrak{I}(R)$-DGS_γ where*

$$\gamma = \max\left\{n \cdot \delta_K^2 \cdot \eta(\mathcal{L}) \cdot \sqrt{2}/\alpha \cdot \omega(1), \sqrt{2n}/\lambda_1\left(\mathcal{L}^\vee\right)\right\} .$$

Theorem 5.3. The reduction is quite straightforward. Given samples $(a_i, b_i) \in R_\mathcal{Q} \times K_\mathbb{R}/R^\vee$, do the following for each one. Sample uniformly at random an element $a_i' \xleftarrow{\$} R_\mathcal{P}$, and compute the unique $\tilde{a_i} \in R_q$ such that $[\tilde{a_i}]_\mathcal{Q} = a_i$ and $[\tilde{a_i}]_\mathcal{P} = a_i'$. Then, output $(\tilde{a_i}, b_i)$.

First, note that if (a_i, b_i) are distributed uniformly, then so does $(\tilde{a_i}, b_i)$. Thus, it remains to prove that if (a_i, b_i) are sampled from $A_{s,\varphi,u}$ (a distribution over $R_\mathcal{Q} \times K_\mathbb{R}/R^\vee$), where $s \xleftarrow{\$} R_\mathcal{Q}^\vee$, and $\varphi \leftarrow \Upsilon_\alpha$, then the resulting distribution of $(\tilde{a_i}, b_i)$ is $A_{\tilde{s},\varphi}$ (a distribution over $R_q \times K_\mathbb{R}/R^\vee$) where $\tilde{s} \xleftarrow{\$} q\mathcal{Q}^\vee/qR^\vee$, and $\varphi \leftarrow \Upsilon_\alpha$.

We prove using a hybrid argument.

Hybrid $\mathcal{H}_0$. This hybrid's distribution is the distribution of the outputs of the reduction. That is, we first sample $s \xleftarrow{\$} R_\mathcal{Q}^\vee$ and $\varphi \leftarrow \Upsilon_\alpha$. Then, for each i, we sample $a_i \xleftarrow{\$} R_\mathcal{Q}$, $a_i' \xleftarrow{\$} R_\mathcal{P}$, and compute $\tilde{a_i}$ to be the unique element satisfying $[\tilde{a_i}]_\mathcal{Q} = a_i$ and $[\tilde{a_i}]_\mathcal{P} = a_i'$. Sample $e \leftarrow \varphi$, set $b_i = (a_i s)u + e \mod R^\vee$ and output $(\tilde{a_i}, b_i)$.

Hybrid $\mathcal{H}_1$. In this hybrid, instead of sampling s over $R_\mathcal{Q}^\vee$, we sample $\tilde{s} \xleftarrow{\$} q\mathcal{Q}^\vee/qR^\vee$. Moreover, we set $b_i = (a_i\tilde{s})/q + e \mod R^\vee$, where $e \leftarrow \varphi$. To show that those hybrids are equivalent, we use the following technical claim.

Claim 5.4.1. *Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ be the prime factors of $\mathcal{Q}$. Assuming that $u \in \mathcal{Q}^{-1} \setminus \bigcup_i \mathcal{Q}^{-1}\mathfrak{p}_i$, the following distributions are equivalent:*

1. *Sample $\tilde{s} \xleftarrow{\$} q\mathcal{Q}^\vee/qR^\vee$, and output $\tilde{s}/q \mod R^\vee$.*
2. *Sample $s \xleftarrow{\$} R^\vee/\mathcal{Q}R^\vee$, and output $u \cdot s \mod R^\vee$.*

Proof. Denote $t := q \cdot u \in \mathcal{P}$, and note that since $q\mathcal{Q}^{-1} = \mathcal{P}$, then $t \in \mathcal{P} \setminus \bigcup_i \mathcal{P}\mathfrak{p}_i$. Therefore, by Lemma 2.13, we have that the mapping $\theta_t : x \mapsto t \cdot x$ induces an isomorphism from $R^\vee/\mathcal{Q}R^\vee$ to $q\mathcal{Q}^\vee/qR^\vee$. For every $s \in R^\vee/\mathcal{Q}R^\vee$, letting $\tilde{s} = \theta_t(\tilde{s}) \in q\mathcal{Q}^\vee/qR^\vee$, we have that

$$\tilde{s}/q \mod R^\vee = (t \cdot s)/q \mod R^\vee = u \cdot s \mod R^\vee \ .$$

Since θ_t is a bijection, then both s and $\tilde{s}$ are distributed uniformly over their respective domain. ■

Assume for now that u satisfies the condition above. We get that $\mathcal{H}_0 \equiv \mathcal{H}_1$.

Hybrid $\mathcal{H}_2$. In this hybrid, instead of setting $b_i = (a_i\tilde{s})/q + e \mod R^\vee$, we set $b_i = (\tilde{a}_i\tilde{s})/q + e \mod R^\vee$. We claim that $\mathcal{H}_1 \equiv \mathcal{H}_2$. Indeed, fix the values of a_i, a'_i. By the Chinese Remainder Theorem, the value of $\tilde{a}_i\tilde{s}$ is determined by $[\tilde{a}_i\tilde{s}]_{q\mathcal{P}^\vee}$ and $[\tilde{a}_i\tilde{s}]_{q\mathcal{Q}^\vee}$. Since $\tilde{s} \in q\mathcal{Q}^\vee$, then $[\tilde{a}_i\tilde{s}]_{q\mathcal{Q}^\vee} = 0$. Moreover, by our choice of $\tilde{a}_i$, we get that $[\tilde{a}_i]_{q\mathcal{P}^\vee} = [\tilde{a}_i]_{\mathcal{Q}R^\vee} = a_i$ (since $q\mathcal{Q}^\vee = \mathcal{P}R^\vee$).

Note that the distribution from the last hybrid is exactly $A_{\tilde{s},\varphi}$. Thus, to conclude the proof, we have to show that there such u as required by the previous claim.

Lemma 5.5. *There exists $u \in \mathcal{Q}^{-1} \setminus \bigcup_i \mathcal{Q}^{-1}\mathfrak{p}_i$ of norm $\|u\|_\infty \leq O\left(\frac{n\delta_K}{N(\mathcal{Q})^{1/n}}\right)$.*

We prove using a counting argument. We show that the number of elements in $\mathcal{Q}^{-1}$ with bounded ℓ_∞-norm is larger than the total number of elements in the union $\bigcup_i \mathcal{Q}^{-1}\mathfrak{p}_i$. This gives an existential proof, which is sufficient for our use.

We denote by $\mathcal{C}_r$ the hypercube (of dimension n) with edge length r, i.e. $\mathcal{C}_r = \{(\pm r, \ldots, \pm r)\}$. Note that a point $x \in \mathcal{C}_r$ if and only if $\|x\|_\infty \leq r$. We turn to bound the number of lattice points with bounded ℓ_∞-norm, or equivalently the number of lattice points that intersect the hypercube.

Claim 5.5.1. *For every $r > 0$, and lattice $\mathcal{L}$, we have that*

$$\frac{(2(r - \sqrt{n}\lambda_n(\mathcal{L})))^n}{\det(\mathcal{L})} \leq \left|\mathcal{L} \bigcap \mathcal{C}_r\right| \leq \frac{(2(r + \sqrt{n}\lambda_n(\mathcal{L})))^n}{\det(\mathcal{L})} \ .$$

Proof. Let $\{v_1, \ldots, v_n\} \subset \mathcal{L}$ be a set of short independent set of vectors in the lattice $\mathcal{L}$. Namely, a linearly independent set (over $\mathbb{Z}$) such that $\|v_i\| \leq \lambda_n(\mathcal{L})$ for every $1 \leq i \leq n$. Let $\{\tilde{v}_1, \ldots, \tilde{v}_n\}$ be the Gram-Schmidt orthogonalization of this set, and recall that $\|\tilde{v}_i\| \leq \|v_i\| \leq \lambda_n(\mathcal{L})$. We denote the box defined by $\{\tilde{v}_1, \ldots, \tilde{v}_n\}$ by $\mathcal{B}_{\vec{v}}$. Note that its volume is $\det(\mathcal{L})$ and that it is contained in $\mathcal{C}_{\sqrt{n}\lambda_n(\mathcal{L})}$.

Starting from the upper bound, we take the box $\mathcal{B}_{\vec{v}}$ around each lattice point. We get that

$$\bigcup_{x \in \mathcal{L} \cap \mathcal{C}_r} x + \mathcal{B}_{\vec{v}} \subseteq \mathcal{C}_{r+\sqrt{n}\lambda_n(\mathcal{L})} \ .$$

Indeed, for every $x \in \mathcal{L} \cap \mathcal{C}_r$ and $y \in x + \mathcal{B}_{\vec{v}}$, we have that $\|y\|_\infty \leq \|x\|_\infty + \sqrt{n}\lambda_n(\mathcal{L}) \leq r + \sqrt{n}\lambda_n(\mathcal{L})$, therefore $y \in \mathcal{C}_{r+\sqrt{n}\lambda_n(\mathcal{L})}$. Hence,

$$\left|\mathcal{L} \bigcap \mathcal{C}_r\right| \cdot \det(\mathcal{L}) \leq 2(r + \sqrt{n}\lambda_n(\mathcal{L})))^n \ ,$$

and the upper bound follows.

For the lower bound, we use the same covering, and note that

$$\mathcal{C}_{r-\sqrt{n}\lambda_n(\mathcal{L})} \subseteq \bigcup_{x\in\mathcal{L}\cap\mathcal{C}_r} x+\mathcal{B}_{\vec{v}} \ .$$

Let $y \in \mathcal{C}_{r-\sqrt{n}\lambda_n(\mathcal{L})}$ and let $x \in \mathcal{L}$ be the lattice point such that $y \in x+\mathcal{B}_{\vec{v}}$. Since $\|x\|_\infty \leq \|y\|_\infty + \sqrt{n}\lambda_n(\mathcal{L}) \leq r$, then $x \in \mathcal{C}_r$. We get that

$$(2(r-\sqrt{n}\lambda_n(\mathcal{L})))^n \leq \left|\mathcal{L} \bigcap \mathcal{C}_r\right| \cdot \det(\mathcal{L}) \ ,$$

which concludes the proof. ■

We now use those bound to count the number of lattice points. Indeed, we get that,

$$\begin{aligned}\left|\mathcal{Q}^{-1} \bigcap \mathcal{C}_r\right| &\geq \frac{(2(r-\sqrt{n}\lambda_n(\mathcal{Q}^{-1})))^n}{\det(\mathcal{Q}^{-1})} \\ &\geq \frac{(2(r-n\delta_K N(\mathcal{Q}^{-1})^{1/n}))^n}{\det(\mathcal{Q}^{-1})} \ ,\end{aligned}$$

where the last inequality is by Lemma 2.7. On the other hand, we have

$$\begin{aligned}\left|\bigcup_{i=1}^k \mathcal{Q}^{-1}\mathfrak{p}_i \bigcap \mathcal{C}_r\right| &\leq \sum_{i=1}^k \left|\mathcal{Q}^{-1}\mathfrak{p}_i \bigcap \mathcal{C}_r\right| \\ &\leq \sum_{i=1}^k \frac{(2(r+\sqrt{n}\lambda_n(\mathcal{Q}^{-1}\mathfrak{p}_i)))^n}{\det(\mathcal{Q}^{-1}\mathfrak{p}_i)} \\ &= \sum_{i=1}^k \frac{(2(r+\sqrt{n}\lambda_n(\mathcal{Q}^{-1}\mathfrak{p}_i)))^n}{N(\mathfrak{p}_\mathfrak{i})\det(\mathcal{Q}^{-1})} \\ &\leq \sum_{i=1}^k \frac{(2(r+n\delta_K N(\mathfrak{p}_\mathfrak{i})^{1/n} N(\mathcal{Q}^{-1})^{1/n}))^n}{N(\mathfrak{p}_\mathfrak{i})\det(\mathcal{Q}^{-1})} \\ &\leq k \cdot \frac{(2(r/q^{1/n}+n\delta_K N(\mathcal{Q}^{-1})^{1/n}))^n}{\det(\mathcal{Q}^{-1})}\end{aligned}$$

where the first inequality is the union bound, and the last is since each $\mathfrak{p}_i$ has norm at least q.

Comparing the two inequalities with get that for $r \geq \frac{n\delta_K}{N(\mathcal{Q})^{1/n}} \cdot \frac{1+k^{1/n}}{1-2(k/q)^{1/n}} = \Omega\left(\frac{n\delta_K}{N(\mathcal{Q})^{1/n}}\right)$, there exists $u \in \left(\mathcal{Q}^{-1} \setminus \bigcup_i \mathcal{Q}^{-1}\mathfrak{p}_i\right) \bigcap \mathcal{C}_r$. □

6 Sampling Secrets from Orders

Let K be a number field of dimension n, and $R = \mathcal{O}_K$ its ring of integers. In this section we consider distributions over orders $\mathcal{O} \subseteq R$, such that $s \in \mathcal{O}/qR \simeq \mathbb{Z}_q^k$. Specifically we assume the following settings. Let $q \geq 2$ be a rational prime that splits completely over R[9]. Therefore, we

[9] A similar argument can be stated for the general case. However, this leads to a very cumbersome statement, which we prefer to avoid.

have the ring isomorphism $R_q \simeq \mathbb{Z}_q^n$. Now, assume that $\overline{S} \subseteq R_q$ is a subring isomorphic to $\mathbb{Z}_q^k$. Therefore $\overline{S} = \mathcal{O}/qR$ for some order $qR \subseteq \mathcal{O} \subseteq R$.

Note that R is also an $\mathcal{O}$-module. Therefore, it has a generating set $\vec{v} = \{v_1, \ldots, v_d\} \subset R$, such that the mapping $\vec{x} = (x_1, \ldots, x_d) \mapsto \langle \vec{x}, \vec{v} \rangle = \sum x_i v_i$ from $\mathcal{O}^d$ is onto R. Since $\mathcal{O} \supset \mathbb{Z}$ we can always take $\vec{v} \subset R$ that spans R over $\mathbb{Z}$. We extend $\langle \cdot, \vec{v} \rangle$, the inner-product by $\vec{v}$ to distributions over $K_{\mathbb{R}}$, by sampling d i.i.d. samples and outputting their inner-product with $\vec{v}$.

Theorem 6.1. *Let $\mathcal{O} \subset R$ be an order as discussed above, and $\vec{v} = \{v_1, \ldots, v_d\} \subset R$ elements that span R over $\mathcal{O}$. Let Υ be a family of error distributions each over $K_{\mathbb{R}}/R\mathcal{O}^\vee$. Then, there exists a polynomial time reduction from $\mathcal{O}$-$\mathrm{LWE}_{(qR,R,1/q),\Upsilon}$ to R-$\mathrm{LWE}_{q,U(\mathcal{O}^\vee/qR\mathcal{O}^\vee),\langle\Upsilon,\vec{v}\rangle}$.*

Consider the special case where K is a cyclotomic field of degree n. Therefore, the "powerful-basis" $\vec{p}$ (see [LPR13, Section 4]) spans R over any order $\mathcal{O}$. In particular, we have that $\langle \Upsilon_\alpha, \vec{p} \rangle$ is wider by a factor of $\widetilde{O}(\sqrt{n})$ (see [LPR13, Lemma 4.3]). We conclude below.

Corollary 6.2. *Let K be a cyclotomic field of dimension n, R its ring of integers and let $q \geq 2$ be a rational prime integer that splits over R. Let $\alpha \in (0,1)$ be such that $\alpha \cdot q \geq 2 \cdot \widetilde{\omega}(\sqrt{n})$, and let $k \in [n]$ then there exists a distribution φ over $R_q^\vee$ with min-entropy $k \log q$ such that there exists a polynomial time reduction from $\mathcal{O}$-$\mathrm{LWE}_{(qR,R,1/q),\Upsilon_{\alpha'}}$ to R-$\mathrm{LWE}_{q,\varphi,\Upsilon_\alpha}$, and $\alpha' = \widetilde{O}(\alpha/\sqrt{n})$.*

The proof of Theorem 6.1 follows from the following lemma, which is a generalization of [GHPS13, Lemma 3.1] for the Order-LWE problem, instead of the ringed variant.

Lemma 6.3. *Let $\mathcal{O}' \subseteq \mathcal{O} \subset K$ be orders, $\mathcal{Q}', \mathcal{I}'$ and $\mathcal{Q}, \mathcal{I}$ ideals in $\mathcal{O}'$ and $\mathcal{O}$ respectively, where $\mathcal{Q}'$ and $\mathcal{Q}$ are integral and $\mathcal{Q} = \mathcal{Q}'\mathcal{O}$, $\mathcal{I} = \mathcal{I}'\mathcal{O}$. Let $\{v_1, \ldots, v_d\} \in \mathcal{O}$ be elements that span $\mathcal{O}$ over $\mathcal{O}'$. Let φ be a distribution over $\mathcal{O}'_{\mathcal{Q}'}$, let Υ be a family of distributions, each over $K_{\mathbb{R}}/\mathcal{I}(\mathcal{O}')^\vee$, and let $u \in (\mathcal{I}' : \mathcal{Q}') \cap (\mathcal{I} : \mathcal{Q})$. Then there is a probabilistic polynomial time reduction from $\mathcal{O}'$-$\mathrm{LWE}_{(\mathcal{Q}',\mathcal{I}',u),\varphi,\Upsilon}$ to $\mathcal{O}$-$\mathrm{LWE}_{(\mathcal{Q},\mathcal{I},u),\varphi,\langle\Upsilon,\vec{v}\rangle}$.*

Proof. We describe an efficient transformation that takes d elements from $\mathcal{O}'_{\mathcal{Q}'} \times K_{\mathbb{R}}/\mathcal{I}'(\mathcal{O}')^\vee$ and outputs an element from $\mathcal{O}_{\mathcal{Q}} \times K_{\mathbb{R}}/\mathcal{I}\mathcal{O}^\vee$. Then, we show that this transformation maps uniform samples to uniform, and $A_{s,\psi,u}$ to $A_{s,\langle\psi,\vec{v}\rangle,u}$ for any $s \leftarrow \varphi$, and $\psi \leftarrow \Upsilon$.

Given d samples $(a'_1, b'_1), \ldots, (a'_d, b'_d)$, the transformation outputs $(a = \sum a'_i v_i, b = \sum b'_i v_i)$. Note that since $\{v_i\}$ spans $\mathcal{O}$ over $\mathcal{O}'$, then it also spans $K_{\mathbb{R}}$ over itself, and maps $\mathcal{J}'$ to $\mathcal{J}'\mathcal{O}$, for any fractional ideal $\mathcal{J}'$ of $\mathcal{O}'$. In particular, it is well-defined over the cosets that arise in those distributions. We conclude that it maps the uniform distributions over $\mathcal{O}'_{\mathcal{Q}'}$ and $\mathbb{T}_{\mathcal{I}'\mathcal{O}'^\vee}$ to the uniform distributions over $\mathcal{O}_{\mathcal{Q}}$ and $\mathbb{T}_{\mathcal{I}\mathcal{O}^\vee}$, respectively.

Now, assume that $(a'_1, b'_1), \ldots, (a'_d, b'_d)$ are sampled from $A_{s,\psi,u}$. As noted before, we get that a is distributed uniformly over $\mathcal{O}_{\mathcal{Q}}$. Turning to b, we have that

$$b = \sum b'_i v_i = \sum (u \cdot a'_i \cdot s + e'_i) v_i = u \cdot a \cdot s + e$$

where each $e'_i \leftarrow \psi$, and therefore e is distributed as in $\langle \psi, \vec{v} \rangle$, which concludes the proof. □

Important Special Cases. We now discuss a family of orders $\mathcal{O}$ that give rise to particularly interesting secret distributions, in particular our example generalizes the example of sampling the secrets from a subfield that was studied in previous works [GHPS13]. Denote $qR = \prod \mathfrak{p}_i$ the prime

factorization of q, then the isomorphism $R_q \simeq \mathbb{Z}_q^n$ is given by $x \mapsto (x \mod \mathfrak{p}_i)_{i\in[n]}$. Now, let $\Omega = (\Omega_1, \ldots, \Omega_k)$ be a partition of $[n]$ into k disjoint subsets. Define

$$\overline{S} := \{\mathbf{x} \in \mathbb{Z}_q^n \mid \mathbf{x}_j = \mathbf{x}_{j'}, \forall j, j' \in \Omega_i, \forall i \in [k]\} ,$$

and note that it forms a subring isomorphic to $\mathbb{Z}_q^k$. It turns out that if $K' \subset K$ is a subfield, then its ring of integers $R' = \mathcal{O}_{K'}$ has this property for some partition of $[n]$, so in this case $\mathcal{O} = R' + qR$. Let $\mathcal{L}'$ be a fractional ideal of R'. Since R' is the maximal order, then $\mathcal{L}'$ is invertible in K'. One can verify that $\mathcal{L} := \mathcal{L}'\mathcal{O} = \mathcal{L}' + q\mathcal{L}'R$ is an invertible fractional ideal of $\mathcal{O}$.

For a general partition Ω of $[n]$, we have that $\mathcal{O}/qR \simeq \mathbb{Z}_q^k$. It follows that $\mathcal{O}$ has index q^{n-k} in R, and therefore $\mathcal{O} = M + qR$, where M is some $\mathbb{Z}$-module of rank k. Using a similar analysis as above, one can relate ideals in $\mathcal{O}$ to ideals of rank k in M.

7 k-Wise Independent Secrets and Hidden Lattice BDD

In this section we propose a new decisional problem and prove the hardness of a class of secret distributions based on that assumption. More precisely, our proposed problem is a decisional variant of the BDD problem, but where the ideal is secretly chosen from a large family of ideals at random. This allows us to prove the hardness for distributions which their "marginal" over the same family of ideals is uniform. By a marginal of a distribution φ over an ideal $\mathcal{Q}$, we mean $\varphi \mod \mathcal{Q}$.

We begin with the exact formulation of the decisional BDD problem, and then state and prove hardness result for the Ring-LWE problem with entropic secrets.

7.1 Decisional Bounded Distance Decoding

We first define the hidden lattice BDD (HLBDD) distribution, and then the decisional problem associated with it.

Definition 7.1 (Hidden Lattice BDD Distribution)**.** *Let $\mathcal{L}$ be some lattice, and let $\mathfrak{L}$ be a finite family of lattices, where each $\mathcal{L}' \in \mathfrak{L}$ is a superset $\mathcal{L}' \supseteq \mathcal{L}$. Let $\mathbf{r} \in G$ be a Gaussian parameter. The* Hidden Lattice BDD Distribution *over $K_\mathbb{R}/\mathcal{L}$, denoted by $C_{\mathcal{L},\mathfrak{L},\mathbf{r}}$, is sampled by choosing uniformly at random a lattice $\mathcal{L}' \xleftarrow{\$} \mathfrak{L}$, an element $x \xleftarrow{\$} \mathcal{L}'/\mathcal{L}$, and an error term $e \leftarrow D_\mathbf{r}$ and outputting $y = x + e \mod \mathcal{L}$.*

The decisional HLBDD problem is defined as follows.

Definition 7.2 (HLBDD Problem)**.** *Let $\mathcal{L}, \mathfrak{L}, \mathbf{r}$ be as in Definition 7.1. The* HLBDD Problem*, denote by $\mathsf{HLBDD}_{\mathcal{L},\mathfrak{L},\mathbf{r}}$ is to distinguish between 2 samples from the distribution $C_{\mathcal{L},\mathfrak{L},\mathbf{r}}$, and the same number of samples from the uniform distribution over $K_\mathbb{R}/\mathcal{L}$.*

One could also consider a more general variant, where the distinguisher gets polynomially many samples, instead of just 2. However, the latter is sufficient for our applications.

Remark 7.1. *If we modify Definition 7.1 of the Hidden Lattice BDD Distribution, to include a basis for the chosen lattice, then it is sufficient to sample $e \leftarrow D_\mathbf{r}$ and output $e \mod \mathcal{L}$. Moreover, by a hybrid argument, one can show that in this variant, it is sufficient to distinguish only a single sample from uniform.*

7.2 k-wise Independent Distributions

In this section we assume that K is the power-of-two cyclotomic field of degree n, and denote its ring of integers by R. Therefore, $R^\vee$ is just a scale of R, so we can assume that the Ring-LWE distribution is over $R_q \times K_\mathbb{R}/R$, and has $s \in R_q$. We begin by defining a family of ideal for the HLBDD problem.

Definition 7.3. *Let $q \geq 2$ a rational integer prime that splits completely over R. Denote $qR = \prod_{i=1}^{n} \mathfrak{p}_i$, where each $\mathfrak{p}_i \subseteq R$ is a prime ideal. For $k \in [n]$ we define the following family ideals,*

$$\mathfrak{P}_k := \left\{ \prod_{i \in T} \mathfrak{p}_i \mid T \subseteq [n],\ \ |T| = k \right\} ,$$

i.e. the set of all ideals containing qR that split into k prime ideals.

Note that for any $k \in [n]$ the sets of lattices $\mathfrak{P}_k$ and $\mathfrak{P}_{n-k}$ are related by the mapping $\mathcal{Q} \mapsto \mathcal{Q}^{-1}qR$, which is a bijection in both directions. This can be seen since this mapping is equivalent to $\prod_{i \in T} \mathfrak{p}_i \mapsto \prod_{i \notin T} \mathfrak{p}_i$.

We now state the main theorem of the section. Recall the notation $[\cdot]_\mathcal{Q}$ from the beginning of Subsection 5.2.

Theorem 7.1. *Let $q \geq 2$ a rational integer prime that splits completely over R. Let $k \in [n]$, and let φ be a distribution over R_q that is B-bounded, and that for every $\mathcal{P} \in \mathfrak{P}_k$, the distribution $[\varphi]_\mathcal{P}$ is uniform. Let $\mathbf{r}, \mathbf{r}', \mathbf{t}$ be Gaussian parameters such that $B \cdot \mathbf{t}/q\mathbf{r} = \mathrm{negl}(n)$ and $(f \cdot (B\mathbf{r}')^2 + q\mathbf{t}^2)/\mathbf{r} = \mathrm{negl}(n)$, for some super polynomial $f = f(n) = n^{\omega(1)}$. Then, there exists a polynomial time reduction from $\mathsf{HLBDD}_{R,\mathfrak{P}_{n-k},\mathbf{r}'}$ to R-$\mathrm{LWE}_{q,\varphi,D_\mathbf{r}}$, assuming the hardness of R-$\mathrm{LWE}_{q,D_\mathbf{t}}$.*

First, we reduce from R-$\mathrm{LWE}_{q,\varphi,\Upsilon}$ to a variant of Ring-LWE problem, where the distinguisher gets only a single sample. This is done by noise swallowing and is sketched in [LPR13]

Lemma 7.2. *Let φ be a distribution over R_q that is B-bounded, and let $\mathbf{r}, \tilde{\mathbf{r}}, \mathbf{t} \in G$ be Gaussian parameters such that $B\mathbf{t}/\mathbf{r} = \mathrm{negl}(n)$ and $(\tilde{\mathbf{r}}^2 + q\mathbf{t}^2)/\mathbf{r} = \mathrm{negl}(n)$. Then, assuming the hardness of R-$\mathrm{LWE}_{q,D_\mathbf{t}}$, there is a reduction from R-$\mathrm{LWE}_{q,\varphi,D_{\tilde{\mathbf{r}}}}$ where the adversary gets only a single sample, to R-$\mathrm{LWE}_{q,\varphi,D_\mathbf{r}}$ with polynomially many samples.*

Proof. Given a single sample $(\tilde{a}, \tilde{b}) \in R_q \times K_\mathbb{R}/R$, we do the following for each requested sample. Sample an element $z \leftarrow D_{q\mathbf{t}}$, and errors $e' \leftarrow D_\mathbf{t}$ and $e'' \leftarrow D_\mathbf{r}$, and output

$$(a = \tilde{a}z + qe', b = \tilde{b}z + e'') .$$

If $(\tilde{a}, \tilde{b})$ is distributed uniformly, then so does (a, b). Now, assume that $(\tilde{a}, \tilde{b})$ is a single sample from the R-$\mathrm{LWE}_{q,\varphi,D_\mathbf{r}}$ distribution, so $\tilde{b} = \tilde{a}s/q + \tilde{e}$ for some $s \leftarrow \varphi$ and $\tilde{e} \leftarrow D_{\tilde{\mathbf{r}}}$. We get that

$$b - as/q = \tilde{b}z + e'' - \tilde{a}zs/q - e's = \tilde{a}zs/q + \tilde{e}z + e'' - \tilde{a}zs/q - e's =: e .$$

The hardness of R-$\mathrm{LWE}_{q,D_\mathbf{t}}$ implies the hardness of R-$\mathrm{LWE}_{q,D_{q\mathbf{t}},D_\mathbf{t}}$. Thus, we get that a is indistinguishable from uniform. So, (a, b) is distributed as a Ring-LWE sample where $s \leftarrow \varphi$, and it remains to analyze the distribution of e.

We get that the distribution of $z\tilde{e}$ is $D_{\sqrt{\tilde{\mathbf{r}}^2 + q\mathbf{t}^2}}$. By our choice of $\mathbf{r}, \mathbf{t}, \tilde{\mathbf{r}}$, we get, by noise swallowing that the distribution of $z\tilde{e} + e''$ is statistically close to the one of e''. Similarly, since

φ is B-bounded, then also the distribution of $e's + e''$ is statistically close to the one of e''. We conclude that e is distributed statistically close to $D_{\mathbf{r}}$, and therefore (a, b) is distributed as in the distribution of $R\text{-LWE}_{q,\varphi,D_{\mathbf{r}}}$. □

Next, we reduce from HLBDD to R-LWE with a single sample. The proof of Theorem 7.1 follows from the combination of Lemma 7.2 and Lemma 7.3 below.

Lemma 7.3. *Let φ be a distribution over R_q that is B-bounded, and that for every $\mathcal{P} \in \mathfrak{P}_k$, the distribution $[\varphi]_{\mathcal{P}}$ is uniform. Let $\tilde{\mathbf{r}}, \mathbf{r}' \in G$ be Gaussian parameters such that $B\mathbf{r}'/q\tilde{\mathbf{r}} = \mathrm{negl}(n)$. Then, there is a reduction from $\mathsf{HLBDD}_{q,\mathfrak{P}_{n-k},\mathbf{r}'}$ to $R\text{-LWE}_{q,\varphi,D_{\tilde{\mathbf{r}}}}$ with a single sample.*

Proof. We prove using a hybrid argument.

Hybrid $\mathcal{H}_0$. In this hybrid we simply consider the distribution $A_{s,D_{\tilde{\mathbf{r}}}}$, where $s \leftarrow \varphi$.

Hybrid $\mathcal{H}_1$. In this hybrid, instead of sampling $a \xleftarrow{\$} R_q$, we do the following.

1. Sample an ideal $\mathcal{Q} \xleftarrow{\$} \mathfrak{P}_{n-k}$.
2. Sample an element $x_1 \xleftarrow{\$} \mathcal{Q}/qR$ and an error term $e_1 \leftarrow D_{\mathbf{r}'}$.
3. Output $a := x_1 + e_1 \mod qR$.

We therefore have

$$(a = x_1 + e_1 \mod qR,\ b = (x_1 \cdot s)/q + (e_1 \cdot s)/q + e \mod R) .$$

Assuming the hardness of $\mathsf{HLBDD}_{q,\mathfrak{P}_{n-k},\mathbf{r}'}$, we get that $\mathcal{H}_0 \approx \mathcal{H}_1$.

Hybrid $\mathcal{H}_2$. In this hybrid we replace the term $(e_1 \cdot s)/q$ with $e_2/q + e$, where $e_2 \xleftarrow{\$} D_{\mathbf{r}'}$. That is,

$$(a = x_1 + e_1 \mod qR,\ b = (x_1 \cdot s)/q + e_2/q + e \mod R) .$$

Recall that φ is B-bounded, and that $B\mathbf{r}'/q\tilde{\mathbf{r}} = \mathrm{negl}(n)$. Therefore, by noise swallowing, we get that $(e_1 \cdot s)/q + e$ is distributed statistically close to the distribution of e, which in turn, by the same argument, is close to $e_2/q + e$. We conclude that the hybrids $\mathcal{H}_1$ and $\mathcal{H}_2$ are statistically close.

Hybrid $\mathcal{H}_3$. Consider the ideal $\mathcal{P} = \mathcal{Q}^{-1}qR$, and note that $\mathcal{P} + \mathcal{Q} = R$ and that $\mathcal{P} \cap \mathcal{Q} = \mathcal{P}\mathcal{Q} = qR$. Therefore, by the Chinese Remainder Theorem, we have that $R_q \simeq R_{\mathcal{Q}} \times R_{\mathcal{P}}$ (see Theorem 2.12). We examine the distribution of b from the previous hybrid in CRT coordinates

$$([x_1]_{\mathcal{P}} \cdot [s]_{\mathcal{P}}/q + [e_2]_{\mathcal{P}}/q + [e]_{1/q\mathcal{P}}, [e_2]_{\mathcal{Q}}/q + [e]_{1/q\mathcal{Q}}) ,$$

where $[x_1]_{\mathcal{Q}} = 0$ since $x_1 \in \mathcal{Q}/qR$. In this hybrid we replace $x_1 \cdot s$ by a uniformly random $x_2 \xleftarrow{\$} \mathcal{Q}/qR$. Since $[s]_{\mathcal{P}}$ and $[x_2]_{\mathcal{P}}$ are distributed uniformly, and $[x_2]_{\mathcal{Q}} = 0$, we get that the hybrids $\mathcal{H}_2$ and $\mathcal{H}_3$ are statistically close.

Hybrid $\mathcal{H}_4$. Note that the resulting distribution from the previous hybrid is

$$(a = x_1 + e_1 \mod qR,\ b = (x_2 + e_2)/q + e \mod R)\ ,$$

where $x_1, x_2 \xleftarrow{\$} \mathcal{Q}/qR$, $e_1, e_2 \leftarrow D'_{\mathbf{r}}$ and $e \leftarrow D_{\tilde{\mathbf{r}}}$. In this hybrid we sample a and b uniformly at random. Assuming the hardness of $\mathsf{HLBDD}_{q,\mathfrak{P}_{n-k},\mathbf{r}'}$, we can replace $x_1 + e_1 \mod qR$ and $(x_2 + e_2)/q$ with the uniform distribution, and thus $\mathcal{H}_3 \approx \mathcal{H}_4$.

Putting it all together, we get that $A_{s,D_{\tilde{\mathbf{r}}}} = \mathcal{H}_0 \approx \mathcal{H}_4 = U(R_q \times K_{\mathbb{R}}/R)$. □

References

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Shai Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 595–618. Springer, 2009.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In Thorsten Holz and Stefan Savage, editors, *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343. USENIX Association, 2016.

[AGV09] Adi Akavia, Shafi Goldwasser, and Vinod Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In *Proceedings of the 6th Theory of Cryptography Conference*, pages 474–495, 2009.

[AP13] Jacob Alperin-Sheriff and Chris Peikert. Practical bootstrapping in quasilinear time. In Canetti and Garay [CG13], pages 1–20.

[Bab86] László Babai. On lovászlattice reduction and the nearest lattice point problem. *Combinatorica*, 6(1):1–13, 1986.

[BF11] Dan Boneh and David Mandell Freeman. Homomorphic signatures for polynomial functions. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 149–168. Springer, 2011.

[BGG+14] Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy. Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pages 533–556, 2014.

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In Shafi Goldwasser, editor, *ITCS*, pages 309–325. ACM, 2012. Invited to ACM Transactions on Computation Theory.

[BKLP15] Fabrice Benhamouda, Stephan Krenn, Vadim Lyubashevsky, and Krzysztof Pietrzak. Efficient zero-knowledge proofs for commitments from learning with errors over rings. In Günther Pernul, Peter Y. A. Ryan, and Edgar R. Weippl, editors, *Computer Security - ESORICS 2015 - 20th European Symposium on Research in Computer Security, Vienna, Austria, September 21-25, 2015, Proceedings, Part I*, volume 9326 of *Lecture Notes in Computer Science*, pages 305–325. Springer, 2015.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In Boneh et al. [BRF13], pages 575–584.

[BPR12] Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Advances in Cryptology–EUROCRYPT 2012*, pages 719–737. Springer, 2012.

[BRF13] Dan Boneh, Tim Roughgarden, and Joan Feigenbaum, editors. *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*. ACM, 2013.

[BV11a] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In Phillip Rogaway, editor, *CRYPTO*, volume 6841 of *Lecture Notes in Computer Science*, pages 501–521. Springer, 2011.

[BV11b] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In Rafail Ostrovsky, editor, *FOCS*, pages 97–106. IEEE, 2011.

[BVWW16] Zvika Brakerski, Vinod Vaikuntanathan, Hoeteck Wee, and Daniel Wichs. Obfuscating conjunctions under entropic ring LWE. In Madhu Sudan, editor, *Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, Cambridge, MA, USA, January 14-16, 2016*, pages 147–156. ACM, 2016.

[CG13] Ran Canetti and Juan A. Garay, editors. *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*. Springer, 2013.

[Cla11] Pete L Clark. Commutative algebra. *Department of Mathematics Georgia University*, 2011.

[Con] Kieth Conrad. The conductor ideal. Expository papers/Lecture notes. Available at: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/conductor.pdf.

[Con09] Kieth Conrad. The different ideal. Expository papers/Lecture notes. Available at: http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf, 2009.

[DDLL13] Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky. Lattice signatures and bimodal gaussians. In Canetti and Garay [CG13], pages 40–56.

[DGHV10] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *EUROCRYPT*, pages 24–43, 2010.

[DGK+10] Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In Daniele Micciancio, editor, *TCC*, volume 5978 of *Lecture Notes in Computer Science*, pages 361–381. Springer, 2010.

[GHPS13] Craig Gentry, Shai Halevi, Chris Peikert, and Nigel P Smart. Field switching in bgv-style homomorphic encryption. *Journal of Computer Security*, 21(5):663–684, 2013.

[GHS12] Craig Gentry, Shai Halevi, and Nigel P. Smart. Homomorphic evaluation of the AES circuit. In Reihaneh Safavi-Naini and Ran Canetti, editors, *CRYPTO*, volume 7417 of *Lecture Notes in Computer Science*, pages 850–867. Springer, 2012.

[GKPV10] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In Andrew Chi-Chih Yao, editor, *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*, pages 230–240. Tsinghua University Press, 2010.

[GVW13] Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In Boneh et al. [BRF13], pages 545–554.

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS98*, pages 267–288, 1998.

[HPS+14] Jeff Hoffstein, Jill Pipher, John M Schanck, Joseph H Silverman, and William Whyte. Practical signatures from the partial fourier recovery problem. In *International Conference on Applied Cryptography and Network Security*, pages 476–493. Springer, 2014.

[HS14] Shai Halevi and Victor Shoup. Algorithms in helib. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 554–571. Springer, 2014.

[HS15] Shai Halevi and Victor Shoup. Bootstrapping for helib. In Elisabeth Oswald and Marc Fischlin, editors, *Advances in Cryptology - EUROCRYPT 2015 - 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Sofia, Bulgaria, April 26-30, 2015, Proceedings, Part I*, volume 9056 of *Lecture Notes in Computer Science*, pages 641–670. Springer, 2015.

[LM06] Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In Michele Bugliesi, Bart Preneel, Vladimiro Sassone, and Ingo Wegener, editors, *Automata, Languages and Programming, 33rd International Colloquium, ICALP 2006, Venice, Italy, July 10-14, 2006, Proceedings, Part II*, volume 4052 of *Lecture Notes in Computer Science*, pages 144–155. Springer, 2006.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In Henri Gilbert, editor, *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, volume 6110 of *Lecture Notes in Computer Science*, pages 1–23. Springer, 2010.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 35–54. Springer, 2013.

[MP13] Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In Canetti and Garay [CG13], pages 21–39.

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

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In *STOC*, pages 333–342, 2009.

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

[PR06] Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography, Third Theory of Cryptography Conference, TCC 2006, New York, NY, USA, March 4-7, 2006, Proceedings*, volume 3876 of *Lecture Notes in Computer Science*, pages 145–166. Springer, 2006.

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

[Reg05] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In Harold N. Gabow and Ronald Fagin, editors, *STOC*, pages 84–93. ACM, 2005. Full version in [Reg09].

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

[RSW18] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-lwe and polynomial-lwe problems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 146–173. Springer, 2018.

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 617–635. Springer, 2009.

[Ste08] Peter Stevenhagen. The arithmetic of number rings. *Algorithmic number theory: lattices, number fields, curves and cryptography*, 44:209–266, 2008.