# Rounding in the Rings

Feng-Hao Liu[1] and Zhedong Wang[2]

[1] Florida Atlantic University, FL, USA. fenghao.liu@fau.edu.
[2] Florida Atlantic University, FL, USA. wangz@fau.edu. (Corresponding Author)

**Abstract.** In this work, we conduct a comprehensive study on establishing hardness reductions for (Module) Learning with Rounding over rings (RLWR). Towards this, we present an algebraic framework of LWR, inspired by a recent work of Peikert and Pepin (TCC '19). Then we show a search-to-decision reduction for Ring-LWR, generalizing a result in the plain LWR setting by Bogdanov et al. (TCC '15). Finally, we show a reduction from Ring-LWE to Module Ring-LWR (even for leaky secrets), generalizing the plain LWE to LWR reduction by Alwen et al. (Crypto '13). One of our central techniques is a new ring leftover hash lemma, which might be of independent interests.

## 1 Introduction

Lattice-based cryptography has attracted significant attention due to its nice mathematical structure and versatility – first it is one of very few promising candidates against quantum algorithms [42], and moreover, it serves as a solid foundation on which a wide range of (advanced) crypto systems can be based, e.g., [36]. Particularly, many lattice-based crypto systems are directly based on the *learning with error* (LWE) problem [40], which enjoys search-to-decision reductions [29,30,33,40] and as well worst-case hardness from some lattice problems, under quantum or classical reductions [10, 33, 40]. With these results, we are more confident in the hardness of LWE, both the decision and search forms, and thus the derived LWE-based crypto systems.

However, the "plain" LWE-based solutions are usually considered impractical due to the large keys/parameters and the requirement of performing rather complicated Gaussian samplings (albeit significant improvements in recent years [23–25,30,31,34]). To tackle these two technical challenges, researchers have proposed other efficient variants of LWE:

- LWE over rings (Ring-LWE). This problem [26] is a compact variant of the plain LWE specialized in some ring in a number field. This Ring-LWE based schemes have significantly smaller keys, and computation of ring multiplications can be further accelerated by Fast Fourier Transform [27]. These advantages make Ring-LWE one of the most competitive candidates for developing practical post-quantum crypto schemes.
- Learning with rounding (LWR). This problem [6] is a de-randomized variant of the plain LWE, where random errors are replaced by the deterministic

rounding. Many crypto systems can be naturally derived from LWR, such as pseudorandom functions [6], lossy trapdoor functions, reusable extractors, and deterministic encryption [3]. As these systems do not require Gaussian samplings, they are in general much easier to implement and more efficient.

A natural combination of these two is *learning with rounding over rings* (Ring-LWR), which in fact has been proposed in the original LWR work [6] as a more efficient version of the plain LWR. Moreover, several submissions to the NIST's post-quantum competition have built their schemes with competitive efficiency from Ring-LWR (or a more general Module Ring-LWR), such as [7,18] (round 2 submissions). Thus, Ring-LWR is also a promising direction towards developing practical post-quantum solutions.

Even though Ring-LWR provides substantial efficiency gains, our understanding about its hardness is rather limited, compared with what we have developed in the Ring-LWE [26,38] and plain LWR [3,5,6,8] settings. To fully enjoy the efficiency brought from the ring structure, it is necessary to determine whether the additional structure would weaken the underlying hard problem. Toward this goal, this work focuses on the following endeavor:

**Main Task:** Determine the hardness of Ring-LWR.

While Ring-LWE/LWR and plain LWE/LWR share many nice mathematical features, establishing hardness results in the ring settings is however tricky. As there are several ad-hoc instantiations of Ring-LWE that can be broken by relatively simple attacks [11–13,20,21], the selection of parameters can be much subtler than in the plain LWE/LWR setting. To handle this, the work [35] conducted a comprehensive research about the existing attacks and hardness results, and then pointed out that several instantiations of Ring-LWE that have security reductions (e.g., from some worst-case ideal lattice problems [26,38]) avoid all the known attacks. Thus, establishing meaningful security reductions would not only guarantee theoretic hardness but also provide important guidance of how to avoid vulnerabilities, which is significant in practical applications. Motivated by this, we then focus on how to build meaningful reductions for Ring-LWR.

**Challenges for Ring-LWR.** We know a simple reduction from (Ring)-LWE to (Ring)-LWR if the ratio of the moduli $q/p$ is super-polynomial [6]. This parameter setting however, requires larger dimension $n$ for the security need of the underlying (Ring)-LWE [1] (and its derived schemes). To achieve better efficiency, the community then turned to determine the hardness of LWR for polynomial moduli, and in subsequent work [3,5,8] several significant reductions have been developed for plain LWR. Unfortunately, these results cannot be generalized to the ring setting for various technical reasons as we summarize below.

– The work [8] derived a search-to-decision reduction for LWR, meaning that LWR is pseudorandom as long as it is one-way. This reduction relies on the ability to predict a random linear function over the secret given the help of the distinguisher of LWR. This property however, does not hold in the ring

setting, as there are super-polynomially many possibilities of $r \cdot s$ for some random ring element $r$ (as a random function) and secret $s$. Even though there is a reduction of search Ring-LWE to search Ring-LWR via Rényi Distance (RD) [8], there is still a disconnection for proving pseudorandom of Ring-LWR from Ring-LWE, even for bounded samples.
- The work [3] takes another approach, proving that the plain LWR remains pseudorandom (for bounded samples), even if the secret comes from an imperfect source (yet with sufficient min entropy). Their result relies on the leftover hash lemma over $\mathbb{Z}_q$ (i.e., inner product in $\mathbb{Z}_q$ is a strong extractor), which does not generalize to the ring setting. This is a critical technical obstacle for porting the LWR results [3] to the ring setting. How to analyze the ring setting was explicitly left as an open interesting question [3].

To mitigate the gap between plain LWR and Ring-LWR, a recent work [14] introduced a new variant called Computational Ring-LWR, which captures security of the following concept – an adversary's winning probability remains similar in a computation game (of some search problem), no matter whether the challenge is generated by using Ring-LWR samples as randomness or truly random samples. The work [14] showed that security of Computational Ring-LWR can be based on Search Ring-LWE via an RD analysis, and can be used to analyze security of several NIST submissions.

This approach still leaves several fundamental questions. For example, whether Ring-LWR is pseudorandom under some more well-studied assumptions remains elusive. As a result, we do not know the core reason why the computational Ring-LWR is hard – maybe Ring-LWR is already pseudorandom, or maybe it is not pseudorandom yet just does not give significant help to solve other computational problems. Additionally, the computational nature of the problem is usually inconvenient to analyze indistinguishability-based security (e.g., security of an encryption scheme or a PRF), as we need to reduce indistinguishability from the search problem. Usually, this is not an easy task, and might require the help of random oracles as the examples in the work [14]. It remains unclear whether the computational Ring-LWR can be used *natively* to analyze indistinguishability-based security in the plain model.

### 1.1 Our Contributions

In this work, we conduct a systematic study on the (Module) Ring-LWR problem (and its generalizations), even in the presence of leakage (weak secret). The problem can be described in the following form: determine whether samples of $(\boldsymbol{a}, \lfloor \boldsymbol{a} \cdot \boldsymbol{s} \rceil)$ are pseudorandom, where $\lfloor \cdot \rceil$ is some rounding function from modulo $q$ to modulo $p$, and $\boldsymbol{a}, \boldsymbol{s}$ are vectors of size $k$ from some appropriate spaces (e.g., the ring of integers of some number field). For an appropriate ring and $k = 1$, the problem is specialized to Ring-LWR, and for general $k > 1$, Module Ring-LWR. Below we describe our contributions.

**Contribution 1.** As a warm up, we show that the algebraic LWE framework of Peikert and Pepin [37] is portable to the setting of LWR while preserving many important reduction results. Below we elaborate.

Following the notion of Module $\mathcal{L}$-LWE, we define Module $\mathcal{L}$-LWR for a certain number field lattice $\mathcal{L}$ – in this case, we have $\boldsymbol{s} \in (\mathcal{L}_q^\vee)^k$ and $\boldsymbol{a} \in (\mathcal{O}_q^\mathcal{L})^k$ where $\mathcal{L}^\vee$ denotes the dual of $\mathcal{L}$, $\mathcal{O}^\mathcal{L}$ denotes the coefficient ring, and $q$ is some modulus. By using this notion, we are able to express Ring-, Module-, Order-, and Poly-LWR in a natural way, similar to the Module $\mathcal{L}$-LWE framework [37]. (We refer the readers to the work [37] for more discussions for why we use the dual lattice space $\mathcal{L}^\vee$.) Next, we prove the following two $\mathcal{L}$-LWR reductions similar to those for $\mathcal{L}$-LWE [37]:

- a reduction from Module $\mathcal{L}$-LWR to Module $\mathcal{L}'$-LWR for $\mathcal{L}' \subseteq \mathcal{L}$, assuming the modulus $q$ is co-prime with the index $|\mathcal{L}/\mathcal{L}'|$, and
- a reduction from $\mathcal{O}$-LWR to Middle-product-LWR for an order $\mathcal{O}$ with a (tweaked) power basis.

As the ring of integers $\mathcal{O}_K$ is the maximal Order in a number field $K$, via these reductions the hardness of (Module) Ring-LWR would imply that of (Module) $\mathcal{O}'$-LWR for any other Order $\mathcal{O}'$ as well as that of the Middle-Product-LWR [4]. Thus, our main focus would be the hardness of (Module) Ring-LWR, as it would imply hardness of many other variants.

**An important add-on.** In addition to the above generalization to $\mathcal{L}$-LWR from the work [37], we add an *important* specification to the procedure of rounding a ring element – we must specify a basis $\mathbf{B} = \{b_i\}_{i\in[n]}$ to which the ring element is rounded with respect. More specifically, we define rounding a ring element $\alpha$ with respect to $\mathbf{B}$ as the following steps:

1. Interpret $\alpha = \sum_{i\in[n]} a_i b_i$ for $a_i \in \mathbb{Z}_q$.
2. Output $\lfloor \alpha \rceil = \sum_{i\in[n]} \lfloor a_i \rceil b_i$.

As the selection of basis can affect our reduction results, either in parameter quality or even feasibility, this specification is critical. While all known prior work [2, 6, 8] (to our knowledge) used the coefficient embedding (the power basis), our hardness results would suggest to work with alternative bases for certain parameters as required by the reductions.

Below we do two important case studies: (1) Ring-LWR without leakage, and (2) (Module) Ring-LWR with leakage. These results will provide as hardness foundations for further algebraic structured LWR via the reduction above, such as Order-, Poly-, Middle-Product-, and many other possible variants of LWR.

**Contribution 2.** We identify a sufficient condition and prove a search-to-decision reduction for Ring-LWR. Thus under this condition, Ring-LWR is pseudorandom as long as it is one-way, generalizing a plain LWR result of [8].

Particularly, let $R = \mathcal{O}_K$ be the ring of integers over some Galois extension $K$, and $p$ be a polynomial-sized modulus such that $p|q$ and $\langle p \rangle$ completely splits[3] over $\mathcal{O}_K$, i.e., $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$ for $n$ being the dimension of $K/\mathbb{Q}$, and $\mathbf{B}$ be a *normal integral basis* of $K$. Then there exists a search-to-decision reduction

[3] Actually the result is more general, as the reduction only requires that $\langle p \rangle$ splits into a product of *small* ideals.

for Ring-LWR when rounding is with respect to the basis $\mathbf{B}$. Furthermore, the quality/parameters of the reduction depend on a certain "norm" of $\mathbf{B}$, which is the shorter the better.

We next derive a search Ring-LWE to search Ring-LWR reduction via an RD analysis[4], yet this only holds for a bounded number of samples. Our search-to-decision Ring-LWR however, is not sample preserving, as the number of samples depends on the advantage of the decision Ring-LWR distinguisher. Thus, combining the two reductions can only derive a search Ring-LWE to $1/\lambda^c$-secure decision Ring-LWR, i.e., hardness of Ring-LWE can only guarantee weak pseudorandomness of Ring-LWR. Nevertheless, we can apply the hardness amplification technique of [43] to achieve $\mathsf{negl}(\lambda)$-security by a parallel repetition up to $\omega(1)$ times. This would give us a modular way to design fully secure schemes such as PRFs from Ring-LWR, based on the hardness of Ring-LWE.

On the other hand, by the Hilbert-Speiser and Kronecker-Weber theorems, normal integral bases only exist for certain cyclotomic fields (and their subfields), and moreover, a field $K$ might have multiple normal integral bases [22]. We can choose a good one using the idea of [27]. Moreover, by selecting appropriate rounding functions, the hardness result can be generalized to the case of cyclotomic fields of power of 2, which do not have normal integer bases. We discuss these in details in Section 4.3.

**Contribution 3.** Next we study whether Ring-LWR holds under leakage. Towards this goal, we show a negative result for Ring-LWR (i.e., $k = 1$). Next, we prove some positive results for Module Ring-LWR (for bounded samples) of larger dimensions $k$'s.

For Ring-LWR such that $\langle p \rangle$ completely splits, we do have a search-to-decision reduction, and a hardness guarantee from Ring-LWR (even just $1/\lambda^c$-security) as Contribution 2. However, if information of $\{s \mod \mathfrak{p}_i\}$'s for a constant fraction of the ideals is leaked, then one can apply a similar attack as [9] to break search LWR completely given only one sample, with a significant probability. Thus, only an entropy lower bound is not sufficient to derive hardness of Ring-LWR against general leakage of say $0.1 \cdot n \log q$ bits.

On the other hand for larger $k$'s, we show that Module Ring-LWR remains pseudorandom under leakage assuming (Module) Ring-LWE (in some cases, $k = 1$, namely Ring-LWE, is sufficient!). Towards this goal, we prove a general ring leftover hash lemma, showing that the inner product over ring elements is a strong extractor, as long as the source, when taken modulo over *any ideal factor* of $p\mathcal{O}_K$, has sufficient entropy. The leftover hash lemma holds regardless of how $p\mathcal{O}_K$ factors, as its factoring only affects the parameters but not feasibility. More interestingly, it also does not require $K$ to be Galois extension as required by

[4] A similar reduction appeared in the work [8], but their Ring-LWE* adds errors in the coefficient-embedding space. "The" Ring-LWE of [26] suggests to add errors in the canonical-embedding space. A direct application of the analysis [8] to "the" Ring-LWE setting would result in significantly worse parameters, e.g., [14] took this approach and can only analyze the case with a constant number of samples.

the search-to-decision reduction in Contribution 2. By using this new leftover hash lemma, we generalize the plain LWR result [3] to the Ring setting, showing Module Ring-LWR is pseudorandom, even for entropic secrets under certain appropriate conditions. Similar to the result of [3], our analysis requires the number of samples to be smaller to the modulus $q$, and thus the reduction holds for a fixed number of samples.

Our ring leftover hash lemma generalizes prior work [27–29], and might be of independent interests. We further elaborate on our improvements over prior results in the next section.

### 1.2 Technical Overview

We overview the most interesting techniques in Contributions 2 and 3.

**Search-to-decision Reduction for Ring-LWR.** We first give an overview of our first reduction when $\langle q \rangle$ completely splits. Our reduction follows the search-to-decision framework of Ring-LWE [26], but makes several important changes.

Let $K$ be a Galois extension over $\mathbb{Q}$ with dimension $n$, $\mathbf{B}$ be a normal integral basis of $K$, $p|q$ such that the rounding $\lfloor \cdot \rceil$ maps ring elements from modulo $q$ to modulo $p$, and $\langle p \rangle = \mathfrak{p}_1 \dots \mathfrak{p}_n$. Our reduction uses two intermediate problems: (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}$ and (W)-$D$-$\mathsf{RLWR}^i$, where the former is the problem of finding $s \mod \mathfrak{p}_i$ (for worst-case secret $s$), and the latter is to distinguish $(a, \lfloor a \cdot s \rceil + h_i)$ from $(a, \lfloor a \cdot s \rceil + h_{i+1})$ for $h_j$ being a distribution that is uniformly random over modulo $\mathfrak{p}_1 \dots \mathfrak{p}_j$ and 0 over modulo $\mathfrak{p}_{j+1} \dots \mathfrak{p}_n$, for the worst-case secret. Then, our reduction follows the path below:

$$\text{Search-}\mathsf{RLWR} \xrightarrow{(1)} \text{(W)-}\mathfrak{p}_i\text{-}\mathsf{RLWR} \xrightarrow{(2)} \text{(W)-D-}\mathsf{RLWR}^i \xrightarrow{(3)} \text{Decision-}\mathsf{RLWR}.$$

We first note that (3) follows from a simple hybrid argument and a worst-case to average-case re-randomization (as the work [8]); (2) can be derived by a similar technique use in the work [26]. Thus in this section, we just overview the most interesting part (1).

Essentially, we would like to show that suppose one can find $s \mod \mathfrak{p}_i$ for some ideal $\mathfrak{p}_i$, then he can find $s \mod \mathfrak{p}_j$ for all the other ideals, and thus by the Chinese Remainder Theorem, find $s \mod \langle p \rangle$. This idea can be achieved in the Ring-LWE case [26] by using the fact that automorphisms in Galois extensions permutes ideals, i.e., for every $i, j \in [n]$, there exists an automorphism $\sigma$ such that $\mathfrak{p}_i = \sigma(\mathfrak{p}_j)$. Fixed such $i, j$ and $\sigma$, the reduction works as follows: given a sample $(a, b = as + e)$, the reduction computes $a' = \sigma(a), b' = \sigma(b) = \sigma(a) \cdot \sigma(s) + \sigma(e)$, by the homomorphic property of the automorphism. The work [26] chooses $e$ in the canonical embedding space such that the distribution of $\sigma(e)$ remains the same for every automorphism. Therefore, the (W)-$\mathfrak{p}_i$-$\mathsf{RLWE}$ solver on input $(a', b')$ would return $s' = \sigma(s) \mod \mathfrak{p}_i$. Then by a simple calculation we have $\sigma^{-1}(s') = s \mod \mathfrak{p}_j$.

In the $\mathsf{RLWR}$ case, we have $(a, b = \lfloor as \rceil)$, and can still compute $(a' = \sigma(a), b' = \sigma(b))$. However, the required equation $\sigma(b) = \lfloor \sigma(s)\sigma(a) \rceil$ might not

hold as $\sigma$ and $\lfloor \cdot \rceil$ might not commute in general. Consequently, $(a', b')$ might not be a valid RLWR instance, which the underlying (W)-$\mathfrak{p}_i$-RLWR solver might fail to solve. Thus, the straight-forward analysis would break down.

To tackle this issue, we prove a key fact that as long as the rounding is with respect to a normal integral basis $\mathbf{B}$, then rounding and automorphisms commute. This suffices to bring the Ring-LWE result to the Ring-LWR. Below we describe our insights.

Recall that $\mathbf{B}$ is a normal integral basis if it is $\mathbb{Z}$-bases that can be represented as $\{b_i = \sigma_i(\gamma)\}_{i\in[n]}$ for some $\gamma \in \mathcal{O}_K$. Every element $x \in \mathcal{O}_K$ can be written as $\sum_{i\in[n]} x_i b_i$ for $x_i \in \mathbb{Z}$. If rounding is with respect to $\mathbf{B}$, we have:

$$\sigma(\lfloor x \rceil) = \sigma\Big(\sum_{i\in[n]} \lfloor x_i \rceil b_i\Big) = \sum_{i\in[n]} \lfloor x_i \rceil \sigma(b_i).$$

We next observe that $\sigma(\mathbf{B}) = \mathbf{B}$ (up to some re-ordering), as $\sigma$ just permutes the normal integral basis. Thus we can further re-write the above equation as:

$$\Big\lfloor \sum_{i\in[n]} x_i \sigma(b_i) \Big\rceil = \Big\lfloor \sigma\Big(\sum_{i\in[n]} x_i b_i\Big) \Big\rceil = \lfloor \sigma(x) \rceil.$$

This proves what we desired.

**Module Ring-LWR under Leakage.** Next we overview how to prove pseudorandom of Module Ring-LWR even for entropic secrets. Briefly speaking, the (Module, Ring)-LWR samples have the form $(\mathbf{A}, \lfloor \mathbf{A} \cdot \boldsymbol{s} \rceil_{q\to p})$ for matrix $\mathbf{A} \in R_q^{\ell\times k}$ and $\boldsymbol{s} \in R_q^k$. Here for simplicity of exposition, we use $R_q$ for both the secret and randomness spaces. More general results on $R_q^\vee$ can be obtained via isomorphisms, such as $R/qR \cong R^\vee/qR^\vee$.

To achieve this, we first take a look at a prior approach [3] who successfully achieved the task in the plain LWR setting. Their proof framework can be summarized as the following.

1. We first break $\mathbf{A} = (\mathbf{A}', \boldsymbol{a})$ where $\mathbf{A}'$ is the first $\ell - 1$ rows.
2. We switch $\mathbf{A}'$ into some lossy matrix $\tilde{\mathbf{A}}'$.
3. Then we show that the conditional entropy $H(\boldsymbol{s}|\tilde{\mathbf{A}}', \lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q\to p})$ is still high.
4. Thus, from a leftover hash lemma we have $(\tilde{\mathbf{A}}', \lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q\to p}), \boldsymbol{a}, \lfloor \boldsymbol{a} \cdot \boldsymbol{s} \rceil_{q\to p}) \approx (\tilde{\mathbf{A}}', \lfloor \tilde{\mathbf{A}}' \cdot \boldsymbol{s} \rceil_{q\to p}), \boldsymbol{a}, \lfloor u \rceil_{q\to p})$, as $\boldsymbol{a}$ acts as a fresh random seed.
5. We switch back $\tilde{\mathbf{A}}'$ to $\mathbf{A}'$.

We can prove that LWR (even for entropic secrets) is pseudorandom by repeatedly applying Steps 2 - 5 on all rows of $\mathbf{A}$ as [3].

Steps 1, 2, 3, 5 are portable to the ring setting, even though we need to take care of some mathematical subtleties in the ring. The major barrier in the ring setting comes from the lack of a ring leftover hash lemma, i.e., showing inner product of ring elements is a strong extractor, namely $(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s} \rangle) \approx (\boldsymbol{a}, u)$. For this task, we only know some partial results: the lemma holds (1) if each element

in $\boldsymbol{s}$ is uniform from a fixed domain [28]; (2) or if each element of $\boldsymbol{s}$ comes from the Gaussian distribution [27] or some specific noisy leaky Gaussian [17]. Under more general leakage functions, it was unclear how inner product over rings behaves. Therefore, it is not inferred from the prior results [17, 27, 28] whether (Module) Ring-LWR remains hard against more general leakage functions.

**A Ring Leftover Hash Lemma.** Next we describe our new ideas to tackle the challenge. We start with the approach of [29], which proved that the leftover hash lemma follows if one can bound the collision probability of $\mathcal{D} = (\boldsymbol{a}, \boldsymbol{s})$. Let $(\boldsymbol{a}, \boldsymbol{a}')$ and $(\boldsymbol{s}, \boldsymbol{s}')$ be two independent samples, and we are interested in the following quantity.

$$\begin{aligned}\mathsf{Col}(\mathcal{D}) &= \mathsf{Pr}[(\boldsymbol{a} = \boldsymbol{a}') \wedge (\boldsymbol{a} \cdot \boldsymbol{s} = \boldsymbol{a}' \cdot \boldsymbol{s}' \bmod qR)] \\ &= \mathsf{Pr}[\boldsymbol{a} = \boldsymbol{a}'] \cdot \mathsf{Pr}[\boldsymbol{a} \cdot \boldsymbol{s} - \boldsymbol{a}' \cdot \boldsymbol{s}' = 0 \bmod qR | \boldsymbol{a} = \boldsymbol{a}'] \\ &= \frac{1}{q^{n\ell}} \cdot \mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{s} - \boldsymbol{s}') = 0 \bmod qR].\end{aligned}$$

To further bound this quantity, in the integer case ($R = \mathbb{Z}$) the work [29] partitions the space using $\gcd(\boldsymbol{s} - \boldsymbol{s}') = d$ for every factor $d$ of $q$. For each factor $d$, the distribution $\boldsymbol{a} \cdot (\boldsymbol{s} - \boldsymbol{s}')$ would be uniformly random over $\mathbb{Z}_d/\mathbb{Z}_q$, allowing us to compute the exact probability of $\mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{s} - \boldsymbol{s}') = 0 \bmod qR | \gcd = d] = d/q$. Furthermore, $\mathsf{Pr}[\gcd(\boldsymbol{s} - \boldsymbol{s}') = d] \leq \mathsf{Pr}[\boldsymbol{s} = \boldsymbol{s}' \bmod d] = \mathsf{Col}(\boldsymbol{s} \bmod d)$. Thus, if the collision probability of $\boldsymbol{s} \bmod d$ is small for any factor of $q$, then we are able to bound the collision probability of $\mathsf{Col}(\mathcal{D})$, implying the desired leftover hash lemma.

In the ring setting however, a ring element might have multiple factorizations, so it is not clear how GCD of ring elements should be. As $R$ might not even be a GCD domain, a general proof cannot rely on this fact. To tackle this issue, we move to *ideal factorization* instead of ring element factorization. By a classic algebraic number theory result (thanks to Dedekind, Kummer, and others), each proper ideal of ring of integers (i.e., $R = \mathcal{O}_K$) factors into a product of prime ideals (or their power), and the factorization is unique up to permutation. Therefore, we can write $q\mathcal{O}_K = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2} \dots \mathfrak{q}_g^{e_g}$ without loss of generality. This result holds for a general number field $K$, not just Galois extensions.

Next we define a notion *maximal belonging* for a vector $\boldsymbol{x} \in R_q^k$, generalizing the spirit of GCD in the view of *ideals*. Let $\mathcal{I}$ be an ideal factor of $qR$, and we denote $\boldsymbol{x} \in_{\max} \mathcal{I}$ if (i) every element in the vector belongs to the ideal $\mathcal{I}$, and (ii) for every ideal $\mathcal{J}$ such that $\mathcal{I} | \mathcal{J}$, there exists one element of $\boldsymbol{x}$, say $x_j$ that $x_j \notin \mathcal{J}$. With this notion, we show that if $\boldsymbol{x} \in_{\max} \mathcal{I}$ for some factor $\mathcal{I}$ of $qR$, then the distribution of $\boldsymbol{a} \cdot \boldsymbol{x}$ is uniform over $\mathcal{I}$ for a uniformly random $\boldsymbol{a}$. This allows us to calculate $\mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{s} - \boldsymbol{s}') = 0 \bmod qR | (\boldsymbol{s} - \boldsymbol{s}') \in_{\max} \mathcal{I}] = N(\mathcal{I})/q^n$, and $\mathsf{Pr}[(\boldsymbol{s} - \boldsymbol{s}') \in_{\max} \mathcal{I}] \leq \mathsf{Pr}[\boldsymbol{s} = \boldsymbol{s}' \bmod \mathcal{I}] = \mathsf{Col}(\boldsymbol{s} \bmod \mathcal{I})$. From these facts, we are able to show, suppose the collision probability of $\boldsymbol{s} \bmod \mathcal{I}$ is small for any ideal factor $\mathcal{I}$ of $qR$, then the leftover hash lemma holds. This translates into an entropy requirement of $H(\boldsymbol{s} \bmod \mathcal{I})$ for every ideal factor $\mathcal{I}$.

We note that proving these results requires to tackle non-trivial mathematical arguments in the ring setting. Particularly, we use some important observations:

(1) $\mathcal{I}/\langle q\rangle \cong \mathfrak{q}^{x_1}/\mathfrak{q}^{e_1} \times \mathfrak{q}^{x_2}/\mathfrak{q}^{e_2} \times \cdots \times \mathfrak{q}^{x_g}/\mathfrak{q}^{e_g}$ for some $x_i \in [e_i]$ where $\mathcal{I}$ factors into $\prod_{i\in[g]} \mathfrak{q}_i^{x_i}$, and (2) each $\mathfrak{q}_i^{x_i}/\mathfrak{q}_i^{e_i} \cong \left(\mathfrak{q}_i^{x_i}/\langle q\rangle\right)/\left(\mathfrak{q}_i^{e_i}/\langle q\rangle\right)$ is further isomorphic to a principle ideal to some power quotient the principle ideal to another larger power. (1) is from the fact of unique ideal factorization and the Chinese Remainder Theorem; (2) is from a theorem of Dedekind that each $\mathfrak{q}_i$ is a prime ideal isomorphic to $\langle q, f_i(\alpha)\rangle$ for some monic irreducible polynomial $f_i$ in $\mathbb{Z}_q[x]$. We refer the details in Section 5.2.

**Parameters and Implications.** By using the leftover hash lemma, we are able to derive some interesting entropy requirements: the lemma holds if $H(\boldsymbol{s} \bmod \mathcal{I}) \geq n\log q + O(\log(1/\varepsilon)) + \delta$ (for every ideal factor $\mathcal{I}$). For a general field $K$, we would need $\delta = n\log q$, resulting a more strict requirement on entropy. For special cases such as (1) $K$ is a cyclotomic field, or (2) each prime ideal of $qR$ has large norm, we can derive a sharper parameter $\delta = O(\log q)$ or even $O(1)$. Intuitively, the leftover hash lemma anyway needs to extract a ring element (entropy $n\log q$), and thus the term $n\log q + O(\log(1/\varepsilon))$ is necessary similar to the regular leftover hash lemma in $\mathbb{Z}_q$. The extra term $\delta$ may depend on the structure of the ring and/or how $q\mathcal{O}_K$ factors.

The next natural question is, how small can $k$ (the dimension of the vector $\boldsymbol{a}$ and $\boldsymbol{s}$) be to reach the lemma's requirement for extraction? Clearly, $k = 1$ is not possible as a one dimension $\boldsymbol{s}$ cannot provide sufficient entropy. Suppose $q\mathcal{O}_K$ only has ideals with large norms, i.e., each $N(\mathfrak{q}_i)$ is large, say $q^{n/2}$, then a constant $\ell$ might suffice for $\boldsymbol{s}$ to reach the entropy requirement. On the other hand, if each $N(\mathfrak{q}_i)$ is small, say $q$, then each coordinate of $\boldsymbol{s}$ modulo $\mathfrak{q}_i$ can only provide $\log q$ bits of entropy. To reach the entropy bound, it would require at least $k = \Omega(n)$. Therefore, a completely-split $q\mathcal{O}_K$ would be less favorable for randomness extraction compared with a low-split $q\mathcal{O}_K$, e.g., $q\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$, where each $N(\mathfrak{q}_i) = q^{n/2}$. Our new leftover hash lemma would suggest to use an appropriate $q$ (such that $q\mathcal{O}_K$ factors in a nice way) in future Ring-LWE/R applications.

**Open Directions.** Our leftover hash lemma, together with [3], shows Module-Ring-LWR (for sufficiently large $k$) remains pseudorandom for bounded samples. An interesting open question is to determine whether Ring-LWR ($k = 1$) is hard if $s \bmod \mathcal{I}$ has sufficient entropy for every ideal factor $\mathcal{I}$. Proving or disproving this would require new ideas beyond the current techniques: we cannot use leftover hash lemma in the $k = 1$ case as argued above. On the other hand, the attack of [9] does not work either, as it requires to leak completely $s \bmod \mathcal{I}$ for some ideal factor $\mathcal{I}$. Another interesting question is to extend the result to the case of unbounded samples, which is a significant open question since [6].

## 2 Preliminaries

**Notations** Let $\lambda$ denote the security parameter. For an integer $n$, let $[n]$ denote the set $\{1, ..., n\}$. We use bold lowercase letters (e.g. $\boldsymbol{a}$) to denote vectors and bold capital letters (e.g. $\mathbf{A}$) to denote matrices. For a positive integer $q \geq 2$, let $\mathbb{Z}_q$ be the ring of integers modulo $q$. For a distribution on a set $X$, we

write $x \xleftarrow{\$} X$ to denote the operation of sampling a random $x$ according to $X$. For distributions $X, Y$, we let $\mathsf{SD}(X, Y)$ denote their statistical distance. We write $X \overset{s}{\approx} Y$ or $X \overset{c}{\approx} Y$ to denote statistical closeness or computational indistinguishability, respectively. We use $\mathsf{negl}(\lambda)$ to denote the set of all negligible functions $\mu(\lambda) = \lambda^{-\omega(1)}$.

### 2.1 Rounding Function in $\mathbb{Z}_q$

For any integer modulus $q \geq 2$, we use the '*rounding*' function defined in [6] – for $q \geq p \geq 2$, let $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$ be the function as $\lfloor x \rceil_p = \lfloor (p/q) \cdot \bar{x} \rceil_p \bmod p$, where $\bar{x} \in \mathbb{Z}$ is any integer congruent to $x \bmod q$.

### 2.2 The Space $H$

When working with number fields and algebraic number theory, it is convenient to work with a certain linear subspace $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ for some integers $s_1, s_2 > 0$ such that $s_1 + 2s_2 = n$, defined as

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

As described in the work [26], we can equip $H$ with norms, which would naturally define norms of elements in a number field or ideal lattice via an embedding that maps field elements into $H$. We will present more details next.

It is not hard to verify 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 $\{\boldsymbol{h}_i\}_{i \in [n]}$ defined as: for $j \in [n]$, let $\boldsymbol{e}_i \in \mathbb{C}^n$ be the vector with 1 in its $j$th coordinate, and 0 elsewhere; then for $j \in [s_1]$, we define $\boldsymbol{h}_j = \boldsymbol{e}_j \in \mathbb{C}^n$, and for $s_1 < j < s_1 + s_2$ we take $\boldsymbol{h}_j = \frac{1}{\sqrt{2}}(\boldsymbol{e}_j + \boldsymbol{e}_{j+s_2})$ and $\boldsymbol{h}_{j+s_2} = \frac{1}{\sqrt{-2}}(\boldsymbol{e}_j - \boldsymbol{e}_{j+s_2})$.

We can equip $H$ with the $\ell_2$ and $\ell_\infty$ norms induced on it from $\mathbb{C}^n$. Namely, for $\boldsymbol{x} \in H$ we have $\|\boldsymbol{x}\|_2 = \sum_i (|x_i|^2)^{1/2} = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ and $\|\boldsymbol{x}\|_\infty = \max_i |x_i|$. $\ell_p$ norms can be defined similarly.

### 2.3 Algebraic Number Theory Background

Algebraic number theory is the study of number fields. Below we present the requisite concepts and notations used in this work. More backgrounds and complete proofs can be found in any introductory book on the subject, e.g., [15, 44].

#### Number Fields and Their Geometry

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

A number field $K = \mathbb{Q}(\alpha)$ of degree $n$ has exactly $n$ field embeddings (injective homomorphisms) $\sigma_i : K \to \mathbb{C}$. Concretely, these embeddings map $\alpha$ to each of the complex roots of its minimal polynomial $f$. An embedding whose images lies in $\mathbb{R}$ is said to be *real*, or otherwise it is *complex*. Because roots of $f$ come in conjugate pairs, so do the complex embeddings. The number of real embeddings is denoted as $s_1$ and the number of pairs of complex embeddings is denoted as $s_2$, satisfying $n = s_1 + 2s_2$ with $\sigma_i$ for $1 < i < s_1$ being the real embeddings and $\sigma_{s_1+s_2+i} = \overline{\sigma_{s_1+i}}$ for $1 \leq i \leq s_2$ being the conjugate pairs of complex embeddings.

The *canonical embedding* $\sigma : K \leftarrow \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ is then defined as $\sigma(x) = (\sigma_1(x), \cdots \sigma_n(x))$. Note that $\sigma$ is a ring homomorphism from $K$ to $H$, where multiplication and addition in $H$ are both component-wise.

By identifying elements of $K$ and their canonical embeddings on $H$, we can define the norms on $K$. For any $x \in K$ and any $p \in [1, \infty]$, the $\ell_p$ norm of $x$ is simply $\|x\|_p = \|\sigma(x)\|_p$. Then we have that $\|xy\|_p \leq \|x\|_\infty \cdot \|y\|_p \leq \|x\|_p \cdot \|y\|_p$, for any $x, y \in K$ and $p \in [1, \infty]$.

The canonical embedding also allows us to view Gaussian distribution $D_{\boldsymbol{r}}$ over $H$, or their discrete analogues over a lattice $\mathcal{L} \subset H$, as distributions over $K$. Formally, the continuous distribution $D_{\boldsymbol{r}}$ is actually over the field tensor product $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$, which is isomorphic to $H$.

The *trace* $\mathrm{Tr} = \mathrm{Tr}_{K/\mathbb{Q}} : K \to \mathbb{Q}$ of an element $a \in K$ can be defined as the sum of the embeddings: $\mathrm{Tr}(a) = \sum_i \sigma_i(a)$. The *norm* $N = N_{K/\mathbb{Q}} : K \to \mathbb{Q}$ can be defined as the product of all the embeddings: $N(a) = \prod_i \sigma_i(a)$. Clearly, the trace is $\mathbb{Q}$-linear, and also notice that $\mathrm{Tr}(a \cdot b) = \sum_i \sigma_i(a)\sigma_i(b) = \langle \sigma(a), \overline{\sigma(b)} \rangle$, so $\mathrm{Tr}(a \cdot b)$ is a symmetric bilinear form akin to the inner product of the embeddings of $a$ and $b$. The norm $N$ is multiplicative.

**Ring of Integers and Ideals**

An *algebraic integer* is an algebraic number whose minimal polynomial over the rationals has integer coefficients. For a number field $K$, we denote its subset of algebraic integers by $\mathcal{O}_K$. This set forms a ring, called the *ring of integers* of the number field. The norm of any algebraic integer is in $\mathbb{Z}$.

An (*integer*) *ideal* $\mathcal{I} \subseteq \mathcal{O}_K$ is an additive subgroup that is closed under multiplication by $R$. Every ideal in $\mathcal{O}_K$ is the set of all $\mathbb{Z}$-linear combinations of some basis $\{b_1, \cdots, b_n\} \subset \mathcal{I}$. The *norm* of an ideal $\mathcal{I}$ is its index as a subgroup of $\mathcal{O}_K$, i.e., $N(\mathcal{I}) = |\mathcal{O}_K / \mathcal{I}|$. The sum of two ideals $\mathcal{I}, \mathcal{J}$ is the set of all $x + y$ for $x \in \mathcal{I}, y \in \mathcal{J}$, and the product ideal $\mathcal{I}\mathcal{J}$ is the set of all sums of terms $xy$. We also have that $N(\langle a \rangle) = |N(a)|$ for any $a \in \mathcal{O}_K$, and $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I}) \cdot N(\mathcal{J})$. The following lemma states the condition of an element not belonging to an ideal, we put the proof in full version of this paper.

**Lemma 2.1** *Let $a \in \mathcal{O}_K$ be an element, $\mathcal{I} \subset \mathcal{O}_K$ be an ideal. If $\|a\|_2 < \sqrt{n} \cdot N(\mathcal{I})^{\frac{1}{n}}$, then $a \notin \mathcal{I}$.*

An ideal $\mathfrak{p} \subsetneq \mathcal{O}_K$ is *prime* if $ab \in \mathfrak{p}$ for some $a, b \in \mathcal{O}_K$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (or both). In $\mathcal{O}_K$, an ideal $\mathfrak{p}$ is prime if and only if it is maximal, which implies

that the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field of order $N(\mathfrak{p})$. An ideal $\mathcal{I}$ is called to *divide* ideal $\mathcal{J}$, which is written as $\mathcal{I}|\mathcal{J}$, if there exists another ideal $\mathcal{H} \in \mathcal{O}_K$ such that $\mathcal{J} = \mathcal{H}\mathcal{I}$. Two ideal $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}_K$ are *coprime* if $\mathcal{I} + \mathcal{J} = \mathcal{O}_K$. The following lemma states the coprime condition of the power of primes, we put the proof in the full version of this paper.

**Lemma 2.2** *Let $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}_K$ be two ideals, and $\mathcal{I}$ is coprime to $\mathcal{J}$, then $\mathcal{I}^x$ is coprime to $\mathcal{J}^y$ for any integers $x, y \geq 1$.*

A *fraction ideal* $\mathcal{I} \subset K$ is a set such that $d\mathcal{I} \subseteq \mathcal{O}_K$ is an integral ideal for some $d \in \mathcal{O}_K$. Its norm is defined as $N(\mathcal{I}) = N(d\mathcal{I})/|N(d)|$. A fractional ideal $\mathcal{I}$ is *invertible* if there exists a fractional ideal $\mathcal{J}$ such that $\mathcal{I} \cdot \mathcal{J} = \mathcal{O}_K$, which is unique and denoted as $\mathcal{I}^{-1}$. The set of fractional ideals form a group under multiplication, and the norm is multiplicative homomorphism on this group.

An *order* $\mathcal{O}$ of $K$ is a subring with unity, i.e., $1 \in \mathcal{O}$ and $\mathcal{O}$ is closed under multiplication, and the $\mathbb{Q}$ span of $\mathcal{O}$ is equal to $K$. It's easy to see that $\mathcal{O}_K$ is an order, and it is the maximal order: every order $\mathcal{O} \subseteq \mathcal{O}_K$. For any order $\mathcal{O}$ of $K$, we have $\mathcal{O} \cdot \mathcal{O}^\vee = \mathcal{O}^\vee$ and $\mathrm{Tr}((\mathcal{O} \cdot \mathcal{O}^\vee) \cdot \mathcal{O}) = \mathrm{Tr}(\mathcal{O}^\vee \cdot \mathcal{O}) \subseteq \mathbb{Z}$.

### 2.4 Duality

For any lattice $\mathcal{L} \subseteq K$ (i.e., for the $\mathbb{Z}$-span of any $\mathbb{Q}$-basis of $K$), its *dual* is defined as $\mathcal{L}^\vee = \{x \in K : \mathrm{Tr}(x\mathcal{L}) \subseteq \mathbb{Z}\}$.

Then $\mathcal{L}^\vee$ embeds as the complex conjugate of the dual lattice,i.e., $\sigma(\mathcal{L}^\vee) = \overline{\sigma(\mathcal{L})}^*$ due to the fact that $\mathrm{Tr}(xy) = \sum_i \sigma_i(x)\sigma_i(y) = \langle \sigma(x), \overline{\sigma(y)} \rangle$. It is easy to check that $(\mathcal{L}^\vee)^\vee = \mathcal{L}$, and that if $\mathcal{L}$ is a fractional ideal, then $\mathcal{L}^\vee$ is one as well.

We point out that the ring of integers $R = \mathcal{O}_K$ is not self-dual, nor are an ideal and its inverse dual to each other. For any fractional ideal $\mathcal{I}$, its dual ideal is $\mathcal{I}^\vee = \mathcal{I}^{-1} \cdot R^\vee$. The factor $R^\vee$ is a fractional ideal whose inverse $(R^\vee)^{-1}$, called the *different ideal*, is integral and of norm $N((R^\vee)^{-1}) = \Delta_K$. The fractional ideal $R^\vee$ itself is often called the *codifferent*.

For any $\mathbb{Q}$-basis $\mathbf{B} = \{b_j\}$ of $K$, we denote its dual basis by $\mathbf{B}^\vee = \{b_j^\vee\}$, which is characterized by $\mathrm{Tr}(b_i \cdot b_j^\vee) = \delta_{ij}$, the Kronecker delta. It is immediate that $(B^\vee)^\vee = B$, and if $\mathbf{B}$ is a $\mathbb{Z}$-basis of some fractional ideal $\mathcal{I}$, then $\mathbf{B}^\vee$ is a $\mathbb{Z}$-basis of its dual ideal $\mathcal{I}^\vee$. If $a = \sum_j a_j \cdot b_j$ for $a_j \in \mathbb{R}$ is the unique presentation of $a \in K_\mathbb{R}$ in basis $\mathbf{B}$, then $a_j = \mathrm{Tr}(a \cdot b^\vee)$.

The following lemma generalized Lemma 4.4 of [28] determines the distribution of $\langle \boldsymbol{a}, \boldsymbol{s} \rangle$ for random $\boldsymbol{a} \in (R/\mathcal{I}R)^\ell$ and fixed $\boldsymbol{s} \in (R^\vee/\mathcal{I}R^\vee)^\ell$, we put the proof in full version of this paper.

**Lemma 2.3 ( [28])** *Let $R = \mathcal{O}_K$ be the ring of integers of a number field $K$, $\mathcal{I}$ be an ideal of $R$, and $\boldsymbol{s} = (s_1, \cdots, s_\ell) \in (R^\vee/\mathcal{I}R^\vee)^\ell$ be a vector of ring elements. If $\boldsymbol{a} = (a_1, \cdots, a_\ell) \in (R/\mathcal{I}R)^\ell$ are uniformly random, then $\sum_i a_i \cdot s_i \bmod \mathcal{I}R^\vee$ is uniformly random over the ideal $\langle s_1, \cdots, s_\ell \rangle / \mathcal{I}R^\vee$. In particular, $\mathsf{Pr}\left[\sum_i a_i \cdot s_i = 0 \bmod \mathcal{I}R^\vee\right] = 1/|\langle s_1, \cdots, s_\ell \rangle / \mathcal{I}R^\vee|$.*

### 2.5 Prime Splitting and Chinese Remainder Theorem

For an integer prime $p \in \mathbb{Z}$, the factorization of the principal ideal $\langle p \rangle \subset R = \mathcal{O}_K$ for a number field $K$ (where $K/\mathbb{Q}$ is a field extension with degree $n$) is as follows.

**Lemma 2.4 (Dedekind [16])** *Let $K = \mathbb{Q}(\alpha)$ be a number field for $\alpha \in \mathcal{O}_K$, and $F(x)$ be the minimal polynomial of $\alpha$ in $\mathbb{Z}[x]$. For any prime $p$, the ideal $p\mathcal{O}_K$ factors into prime ideals as $\langle p \rangle = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, where $N(\mathfrak{p}_i) = p^{f_i}$ for $f_i = [\mathcal{O}_K/\mathfrak{p}_i : \mathbb{Z}_p]$, and $n = \sum_{i=1}^{g} e_i f_i$.*

*Moreover if $p$ does not divide the index of $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$, then we have further structures as following. We can express $F(x) = f_1(x)^{e_1} \dots f_g(x)^{e_g} \mod p$, where each $f_i(x)$ is a monic irreducible polynomial in $\mathbb{Z}_p[x]$. There exists a bijection between $\mathfrak{p}_i$'s and $f_i(x)$'s such that $\mathfrak{p}_i = \langle p, f_i(\alpha) \rangle$, and $f_i = \deg f_i(x)$.*

For each $\mathfrak{p}_i$, we have $\mathfrak{p}_i | p\mathcal{O}_K$, which can be written as $\mathfrak{p}_i | \langle p \rangle$, and call $\mathfrak{p}_i$ a factor of $\langle p \rangle$. Next we recall the Chinese Remainder Theorem (CRT) for the fraction ideal over a number field $K$.

**Lemma 2.5 (Chinese Remainder Theorem [9])** *Let $\mathcal{I}$ be a fractional in over $K$, and let $\mathfrak{p}_i$ be pairwise coprime ideals in $R = \mathcal{O}_K$, then natural ring homomorphism is an isomorphism: $\mathcal{I}/\Big(\prod_i \mathfrak{p}_i\Big)\mathcal{I} \to \bigoplus_i (\mathcal{I}/\mathfrak{p}_i\mathcal{I})$.*

As a corollary of Chinese Remainder Theorem above, the following lemma states the equivalence of prime ideal factors of $qR$ and $qR^\vee$ under isomorphism.

**Lemma 2.6 (Lemma 2.35 of [9])** *Let $\mathcal{I}, \mathcal{J}$ be integral ideals in an order $\mathcal{O}$ and let $\mathcal{M}$ be a fractional $\mathcal{O}$-ideal. Assume that $\mathcal{I}$ is invertible. Given the associated primes of $\mathcal{J}, \mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_k$, and an element $t \in \mathcal{I} \setminus \bigcup_{j=1}^{k} \mathfrak{p}_j\mathcal{I}$ the map*

$$\begin{aligned} \theta_t : \mathcal{M}/\mathcal{J}\mathcal{M} &\to \mathcal{I}\mathcal{M}/\mathcal{I}\mathcal{J}\mathcal{M} \\ x &\mapsto t \cdot x \end{aligned}$$

*induces an isomorphism of $\mathcal{O}$-modules. Moreover, $\theta_t$ is efficiently inverted given $\mathcal{I}, \mathcal{J}, \mathcal{M}$ and $t$, and $t$ can be computed given $\mathcal{I}$ and $\mathfrak{p}_1, \cdots, \mathfrak{p}_k$.*

In particular, let $\mathcal{I} = (R^\vee)^{-1}, \mathcal{J} = qR, \mathcal{M} = R^\vee$, then $R/qR \cong R^\vee/qR^\vee$.

### 2.6 The Ring-LWE Problem

We now provide the formal definition of the ring-LWE problem and describe the hardness result shown in [26, 38].

**Definition 2.7 (Ring-LWE Distribution)** *For a secret $s \in R_q^\vee$ ($R = \mathcal{O}_K$) and a distribution $\phi$ over $K_\mathbb{R}$, a sample from the Ring-LWE distribution $A_{s,\phi}$ over $R_q \times (K_\mathbb{R}/qR^\vee)$ is generated by choosing $a \leftarrow R_q$ uniformly random, choosing $e \leftarrow \phi$, and outputting $(a, b = a \cdot s + e \mod qR^\vee)$.*

**Definition 2.8 (Ring-LWE, Average-case Decision Problem)** *The* average-case decision *version of the Ring-*LWE *problem, denoted* $R$-DLWE$_{\ell,q,\phi}$ *is to distinguish between* $\ell$ *independent samples from* $A_{s,\phi}$ *for a random choice of a secret* $s \leftarrow R_q^\vee$ *of degree* $n$*, and the same number of uniformly random and independent samples from* $R_q \times (K_\mathbb{R}/qR^\vee)$.

The subscript $\ell$ of the number of samples is usually omitted if there is no special explanation. The hardness of RLWE can be reduced from the hardness of hard problems over ideal lattices, ref. Full version of this paper.

## 3 Generalized Learning with Rounding

In this section, we present a new algebraic framework of LWR that generalizes previous RLWR notions [6, 8, 14], which mainly focused on primal ring elements and rounding over their polynomial coefficient representations. Essentially, we show that the unified framework of algebraic LWE in a recent work [37] can be portable to the LWR setting while maintaining important features. Under our algebraic LWR framework, we can naturally express several variants of Ring-, Order-, and Poly-LWR in a single problem parameterized by a number field lattice, and derive hardness results for these variants of LWRs and as well middle-product LWR based on RLWR.

Moreover, we can derive new and tighter hardness results for (Module) RLWR based on RLWE, even in the entropic secret cases. Thus, the hardness of RLWE would provide a foundation for RLWR and these algebraic variants via our new framework. In the rest of this section, we present the algebraic framework of LWR and relate the hardness of RLWR to the other variants of LWRs. Later in Sections 4 and 5, we present our new hardness results.

### 3.1 Rounding with Respect to Specific Basis

Recall that for a monogenic field $K$ (e.g., cyclotomic fields), an element $a \in R_q = (\mathcal{O}_K)_q$ can be treated as a polynomial of integer coefficients, as $(\mathcal{O}_K)_q = \mathbb{Z}_q[\alpha] \cong \mathbb{Z}_q[x]/f(x)$, where $f(x)$ is the minimal polynomial of $\alpha$. Let $a(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathbb{Z}_q[x]/f(x)$, and we can naturally define *rounding* $\lfloor \cdot \rceil_p$ of $a(x)$ as:

$$\lfloor a(x) \rceil_p =: \lfloor a_0 \rceil_p + \lfloor a_1 \rceil_p x + \cdots + \lfloor a_{n-1} \rceil_p x^{n-1}.$$

To our knowledge, all prior work [6, 8, 14] use this coefficient embedding in the primal $R_q$ when studying rounding in the ring. This choice however, is not optimal for ideal lattices. As "the" RLWE problem is defined in the dual form for several analytical advantages as argued in [26], i.e., the secret and the inner products are in the dual space $R_q^\vee = (\mathcal{O}_K)_q^\vee$, the natural analog RLWR of RLWE should be defined in the dual form. However, an element in the dual in general might not be able to described as an integral polynomial, and thus it is not clear how to define rounding in this case. One might consider to use the relation $R_q^\vee = t^{-1}R_q$ for some $t^{-1} \in R_q^\vee$ to move elements from the dual to the primal

(e.g., see [35, 41]). This approach goes back to the primal RLWR (RLWE) case, which would lose some analytical advantages, e.g., tightness of parameters in our reduction. We explain this further in Section 4. Thus, we would like to stick to the dual form of RLWR, similar to the RLWE setting [26].

To tackle the above issue, we observe that an element $a \in R^\vee$ (also $R_q^\vee$) can also be uniquely represented as integer linear combinations of a certain $\mathbb{Z}$-basis of $R^\vee$, say $\mathbf{B} = \{b_1, \cdots, b_n\}$, i.e., $a = x_1 b_1 + \cdots + x_n b_n$, where all $x_i \in \mathbb{Z}$. Under this basis, rounding an element can be easily defined. Since there are multiple possible bases, it is important to specify to which basis the rounding is with respect. Thus, below we explicitly define a rounding function that is also parameterized by a basis.

**Definition 3.1** *Let $K = \mathbb{Q}(\alpha)$ be a number field with degree $n$, and $\mathcal{I}$ be a fractional ideal over $K$ with a $\mathbb{Z}$-basis $\mathbf{B} = \{b_1, \cdots, b_n\}$. Then for any integers $q \geq p \geq 2$, we define the rounding function (with respect to basis $\mathbf{B}$) $\lfloor \cdot \rceil_{\mathbf{B},p} : \mathcal{I}_q \to \mathcal{I}_p$ as*

$$\lfloor a \rceil_{\mathbf{B},p} = \lfloor x_1 \rceil_p b_1 + \cdots + \lfloor x_n \rceil_p b_n \mod p\mathcal{I},$$

*where $\mathcal{I}_q$ (similarly $\mathcal{I}_p$) is the quotient groups $\mathcal{I}/q\mathcal{I}$, and $a = x_1 b_1 + \cdots + x_n b_n \in \mathcal{I}_q, x_1, \cdots, x_n \in \mathbb{Z}_q$. The rounding function for $\mathbb{Z}_q \to \mathbb{Z}_p$, i.e., $\lfloor \cdot \rceil_p$, is the same as we described in Section 2.1.*

Throughout this paper, when we define a rounding function of a ring elements, there must be a reference basis associated with it. In situations where the basis $\mathbf{B}$ is clear, we might omit it in the subscript for succinctness of notion.

### 3.2 $\mathcal{L}$-LWR and MP-LWR Problems

Following the framework of [37], we next present an algebraic form of LWR that captures Ring-, Order-, Poly-LWR. Similar to the work [37], we derive two hardness results: (1) we prove a reduction from $\mathcal{L}$-LWR to $\mathcal{L}'$-LWR for $\mathcal{L}' \subseteq \mathcal{L}$, and (2) we prove hardness of middle-product LWR (namely, MP-LWR) and a variant multivariate MP-LWR (denoted as MV-MP-LWR), based on the hardness of Order-LWR. Due to the limitation of space, the definitions and reductions of MP-LWR are in full version of this paper. As $\mathcal{O}_K$ is the maximal order, the hardness of Order-, MP-, and Poly-LWR can be based on the hardness of RLWR.

Next we define Coefficient Ring $\mathcal{O}^{\mathcal{L}}$ of a lattice $\mathcal{L}$ in a number field $K$, following the framework of [37]. Intuitively, we have the secret vector $s \in \mathcal{L}^\vee$, and the public random element $a \in \mathcal{O}^{\mathcal{L}}$. Then the product $s \cdot a$ will lie in the space $\mathcal{L}^\vee$, consistent with the prior RLWE structure.

#### Coefficient Ring

**Definition 3.2 (Coefficient Ring)** *For a lattice $\mathcal{L} \subseteq K$, we define the* coefficient ring *of it as $\mathcal{O}^{\mathcal{L}} := \{x \in K : x\mathcal{L} \subseteq \mathcal{L}\}$.*

Then, the following lemmas can be derived.

**Lemma 3.3 ( [37])** *$\mathcal{O}^{\mathcal{L}} = (\mathcal{L} \cdot \mathcal{L}^{\vee})^{\vee}$, $\mathcal{L}$ and $\mathcal{L}^{\vee}$ have the same coefficient ring $\mathcal{O}^{\mathcal{L}} = \mathcal{O}^{\mathcal{L}^{\vee}}$. Particularly, if $\mathcal{L}$ is an order $\mathcal{O}$ or it dual $\mathcal{O}^{\vee}$ of $K$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$.*

**Lemma 3.4 ( [37])** *The coefficient ring $\mathcal{O}^{\mathcal{L}}$ is an order of $K$, and $\mathcal{O}^{\mathcal{L}} \subseteq \mathcal{O}_K$.*

### $\mathcal{L}$-LWR Problem

With the definition above, we define a general algebraic LWR problem as follows.

**Definition 3.5 ($\mathcal{L}$-LWR distribution)** *Let $\mathcal{L}$ be a lattice in a number field $K$, $\mathcal{O}^{\mathcal{L}}$ be the coefficient ring of $\mathcal{L}$, $q \geq p \geq 2$, $k \geq 1$ be positive integers, and $\mathbf{B}$ be a basis of $\mathcal{L}^{\vee}$. For $\boldsymbol{s} \in (\mathcal{L}_q^{\vee})^k$, a sample from the $\mathcal{L}$-LWR distribution $L^k_{\boldsymbol{s},q,p}(\mathcal{L}, \mathbf{B})$ over $(\mathcal{O}_q^{\mathcal{L}})^k \times \mathcal{L}_p^{\vee}$ is generated by choosing $\boldsymbol{a} \leftarrow (\mathcal{O}_q^{\mathcal{L}})^k$ uniformly at random, outputting $(\boldsymbol{a}, b = \lfloor \langle \boldsymbol{a}, \boldsymbol{s} \rangle \rceil_{\mathbf{B},p})$.*

**Definition 3.6 ($\mathcal{L}$-LWR problem, decision)** *The decision problem $D$-$\mathcal{L}$-$\mathsf{LWR}^k_{\mathbf{B},q,p,\ell,\psi}$ is to distinguish between $\ell$ samples from $L^k_{\boldsymbol{s},q,p}(\mathcal{L}, \mathbf{B})$ where $\boldsymbol{s} \leftarrow \psi$, and $\ell$ samples from $U((\mathcal{O}_q^{\mathcal{L}})^k \times \mathcal{L}_p^{\vee})$.*

**Definition 3.7 ($\mathcal{L}$-LWR problem, search)** *The decision problem $S$-$\mathcal{L}$-$\mathsf{LWR}^k_{\mathbf{B},q,p,\ell,\psi}$ is given $\ell$ samples from $L^k_{\boldsymbol{s},q,p}(\mathcal{L}, \mathbf{B})$ for $\boldsymbol{s} \leftarrow \psi$, find $\boldsymbol{s}$.*

For simplicity of notation, we omit the subscript $\psi$ for the uniform distribution for the above two definitions. Below the computational problems are all *average-case*, where distinguishability/solvability is referred to the case when the secret $\boldsymbol{s}$ comes from some distribution. We also define their *worst-case* variants by adding (W), i.e., (W)-$S$-$\mathcal{L}$-LWR, where solvability means finding solutions for any $\boldsymbol{s}$ in the support of $\psi$, i.e., for any $\boldsymbol{s} \in \mathsf{Supp}(\psi)$.

The definitions above generalize the algebraic LWR variants defined over number fields or polynomial rings. Let $k = 1$. If $\mathcal{L}$ is an order $\mathcal{O}$ of $K$ or its dual $\mathcal{O}^{\vee}$, then $\mathcal{O}^{\mathcal{L}} = \mathcal{O}$. Therefore, by takeing $\mathcal{L} = O_K$, we obtain the original Ring-LWR problems defined in [6]. Alternatively, by taking $\mathcal{L} = \mathcal{O}^{\vee}$, we get the "primal" form of Order-LWR over $\mathcal{O}$, which is corresponding to the Poly-LWR problem if further taking $\mathcal{O} = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$. Furthermore, if we take $\mathcal{L} = \mathcal{O}$, a natural "dual" variant of Order-LWR is obtained, where $s \in \mathcal{O}^{\vee}/q\mathcal{O}^{\vee}$ and $\lfloor s \cdot a \rceil_p \in \mathcal{O}^{\vee}/p\mathcal{O}^{\vee}$. We also get other problems that are not covered by above ones if we take $\mathcal{L}$ to be neither an order nor its dual. For $k \geq 2$, this generalizes the Module RLWR to arbitrary lattices.

### 3.3 Reductions and Hardness Results

Below we present a $\mathcal{L}$-LWR to $\mathcal{L}'$-LWR reduction. Due to space limit, we present another reduction about MP-RLWR in full version of this paper.

**Reduction from $\mathcal{L}$-LWR to $\mathcal{L}'$-LWR**

For any lattices $\mathcal{L}' \subseteq \mathcal{L}$ in $K$, we define the *natural inclusion map* $h : \mathcal{L}'_q \to \mathcal{L}_q$ as the map that sends $x + q\mathcal{L}'$ to $x + q\mathcal{L}$ for any $x \in \mathcal{L}'$. Similarly, the *natural inclusion map* $g : \mathcal{O}_q^{\mathcal{L}'} \to \mathcal{O}_q^{\mathcal{L}}$ sends $x + q\mathcal{O}^{\mathcal{L}'}$ to $x + q\mathcal{O}^{\mathcal{L}}$. The following lemmas presents the conditions under which maps of this kind are bijections.

**Lemma 3.8 ( [37])** *Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in number field $K$ and $q$ be a positive integer. Then the natural inclusion map $h : \mathcal{L}'_q \to \mathcal{L}_q$ is a bijection if and only if $q$ is coprime with the index $|\mathcal{L}/\mathcal{L}'|$; in this case, $h$ is efficient computable and invertible given an arbitrary basis of $\mathcal{L}'$ relative to a basis of $\mathcal{L}$. The same conclusions holds for the natural inclusion map $\bar{h} : \mathcal{L}_q^\vee \to (\mathcal{L}'_q)^\vee$.*

**Lemma 3.9 ( [37])** *Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in number field $K$ and $q$ be a positive integer that is coprime with the index $|\mathcal{L}/\mathcal{L}'|$. If $\mathcal{O}^{\mathcal{L}'} \subseteq \mathcal{O}^{\mathcal{L}}$, then the natural inclusion map $g : \mathcal{O}_q^{\mathcal{L}'} \to \mathcal{O}_q^{\mathcal{L}}$ is a bijection.*

The following Theorem presents the reduction from $\mathcal{L}$-LWR to $\mathcal{L}'$-LWR, due to the limitation of space, we put the full proof of it in full version of this paper.

**Theorem 3.10** *Let $\mathcal{L}' \subseteq \mathcal{L}$ be lattices in a number field $K$ with degree $n$, $q \geq p \geq 2$, $k \geq 1$ be positive integers where $p|q$, and $\mathbf{B}$ be a basis of $\mathcal{L}^\vee$. If $\mathcal{O}^{\mathcal{L}'} \subseteq \mathcal{O}^{\mathcal{L}}$, and the natural inclusion maps $g : O_q^{\mathcal{L}'} \to \mathcal{O}_q^{\mathcal{L}}$ is an efficiently invertible bijection, then there is an efficient deterministic transformation which:*

- *maps distribution $U((\mathcal{O}_q^{\mathcal{L}})^k \times \mathcal{L}_p^\vee)$ to distribution $U((\mathcal{O}_q^{\mathcal{L}'})^k \times {\mathcal{L}'_p}^\vee)$*
- *maps distribution $L^k_{\boldsymbol{s},q,p}(\mathcal{L}, \mathbf{B})$ to distribution $L^k_{\boldsymbol{s}',q,p}(\mathcal{L}', \mathbf{B}')$, where $\boldsymbol{s}' = \boldsymbol{s} \mod q(\mathcal{L}')^\vee$, $\mathbf{B}' = \mathbf{B} \mod q(\mathcal{L}')^\vee$.*

**Corollary 3.11** *Adopt the notations from theorem 3.10, and assume that $|\mathcal{L}/\mathcal{L}'|$ is coprime with $q$, that $\mathcal{O}^{\mathcal{L}'} \subseteq \mathcal{O}^{\mathcal{L}}$, and that bases of $\mathcal{L}', \mathcal{O}^{\mathcal{L}'}$ relative to bases of $\mathcal{L}, \mathcal{O}^{\mathcal{L}'}$ (respectively) are known. Then there is an efficient deterministic reduction from $\mathcal{L}$-$\mathsf{LWR}^k_{\mathbf{B},q,p,\ell,U}$ to $\mathcal{L}'$-$\mathsf{LWR}^k_{\mathbf{B}',q,p,\ell,U'}$ for both the search and decision versions, where $U$ and $U'$ are the uniformly random distributions over $\mathcal{L}_q^\vee$ and $(\mathcal{L}'_q)^\vee$ respectively, $\mathbf{B}$ and $\mathbf{B}'$ are $\mathbb{Z}_q$-bases of $\mathcal{L}_q^\vee$ and $(\mathcal{L}'_q)^\vee$ respectively, and $\mathbf{B}' = \mathbf{B} \bmod q(\mathcal{L}')^\vee$.*

# 4 New Hardness Results of Ring-LWR

## 4.1 Search RLWR to decision RLWR

**Definition 4.1 (Normal Integral Basis)** *Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G$. We say that $K/\mathbb{Q}$ has a normal integral basis (NIB) if there exists an element $\alpha \in \mathcal{O}_K$ such that the Galois conjugates of $\alpha$ form an $\mathbb{Z}$-basis of $\mathcal{O}_K$.*

We denote $R_q^*$ (or $(R_q^\vee)^*$) as the set that consists of all invertible elements in $R_q$ (or $R_q^\vee$). Next, we present a hardness result of decision $\mathsf{RLWR}$ based on search $\mathsf{RLWR}$ under appropriate parameters.

**Theorem 4.2** *Let $\mathbf{B}$ be a normal integral basis of a Galois extension $K/\mathbb{Q}$ of degree $\varphi(m) = n$, $q \geq p \geq 2$ be integers where $p|q$, $p$ is a prime, and $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$ where $g = n/c$ for a constant $c \in \mathbb{Z}$. Then there exists an efficient reduction from $S$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell',\psi}$ to $D$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}$, where $\psi$ denotes the uniform distribution over $R_p^\vee \cap (R_q^\vee)^*$, $\psi'$ denotes the uniform distribution over $U\big((R_q^\vee)^*\big)$, $\ell' = gp^c\ell \cdot \mathsf{poly}(1/\varepsilon)$, and $\varepsilon$ is the advantage of $D$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}$ oracle.*

At a high level, the proof of Theorem 4.2 consists of three reductions following the approach of [26]. We summarize the reduction route as follows, and explain the parameters later:

$$S\text{-}\mathsf{RLWR}_{\mathbf{B},q,p,\ell',\psi} \xrightarrow{(1)} (\mathrm{W})\text{-}\mathfrak{p}_i\text{-}\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi} \xrightarrow{(2)} (\mathrm{W})\text{-}D\text{-}\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'} \xrightarrow{(3)} D\text{-}\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}.$$

We note that the above step (3) consists of two sub-steps: one is a reduction from (W)-$D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi}$ to average case $D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'}$, followed by another reduction from average case $D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi}$ to (average case) $D$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}$.

### $S$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell',\psi}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$

**Definition 4.3 ((W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$)** *The worst-case (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ problem is: given $\ell''$ samples from $L_{s,q,p}(R,\mathbf{B})$ for some arbitrary $s \in \mathsf{Supp}(\psi)$, find $s \bmod \mathfrak{p}_i R^\vee$.*

**Lemma 4.4 ($S$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell',\psi}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$)** *Let $\mathbf{B}$ be a normal integral basis as used in $\mathsf{RLWR}$. Then for every $i \in \{1,\cdots,g\}$, there exists a deterministic poly-time reduction from $S$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell',\psi}$ to (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$, where $\psi = R_p^\vee \cap (R_q^\vee)^*$, $\ell' = g\ell''$.*

*Proof.* To prove this theorem, we will work on an arbitrary $i \in \{1,\cdots,g\}$. The same argument can be extended to all the other $i$'s. Throughout the rest of the poof, we will view $i$ as an arbitrary fixed index.

We first observe a simple fact. For $k \in \{1,\cdots,g\}$, let $\sigma_k$ be an automorphism that maps $\mathfrak{p}_k$ to $\mathfrak{p}_i$. We know that all these automorphisms exist as $K$ is a Galois extension. Then the reduction proceeds as follow.

- For each $k \in \{1,\cdots,g\}$, the reduction runs through the following steps.
  - Make $\ell''$ queries to the oracle $L_{s,q,p}(R,\mathbf{B})$.
  - For each given sample $(a,b)$, transform it to $(\sigma_k(a),\sigma_k(b))$.
  - Send the $\ell''$ transformed samples to the $\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ oracle
  - Upon receiving the answer $x \in R^\vee/\mathfrak{p}_i R^\vee$, store $\sigma_k^{-1}(x) \in R^\vee/\mathfrak{p}_k R^\vee$.
- Next, the reduction combines all $\{\sigma_k^{-1}(x)\}_{k\in\{1,\cdots,g}$ by the Chinese Remainder Theorem. Then it outputs the combined value $s' \in R_p^\vee$.

We now show that for each $k \in [g]$, $\sigma_k^{-1}(x) = s \bmod \mathfrak{p}_k R^\vee$. To show this, we prove that the distribution of the transformed samples is correctly distributed as the $\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ oracle requires. Particularly, for each $(a,b) \leftarrow L_{s,q,p}(R,\mathbf{B})$, $\sigma_k(a)$ is uniformly random in $\sigma_k(R_q) = R_q$ as $\sigma_k$ is an automorphism. Next we would like to show that $\sigma_k(b) = \lfloor \sigma_k(a) \cdot \sigma_k(s) \rceil_{\mathbf{B},p}$. If this holds, then $(\sigma_k(a), \sigma_k(b))$ would be the correct distribution that the $\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ oracle expects, and then the oracle would return $x = \sigma_k(s) \bmod \mathfrak{p}_i R^\vee$ (with a non-negligible probability). Thus, we have $\sigma_k^{-1}(x) = s \bmod \mathfrak{p}_k R^\vee$. Now we focus on proving $\sigma_k(b) = \lfloor \sigma_k(a) \cdot \sigma_k(s) \rceil_{\mathbf{B},p}$.

We analyze the term $b = \lfloor a \cdot s \rceil_{\mathbf{B},p}$. Without loss of generality, we write $a \cdot s \bmod qR^\vee = \sum_{i=1}^n \alpha_i b_i$ under the $\mathbb{Z}_q$-basis $\mathbf{B} = \{b_1, \cdots, b_n\}$ for $\alpha_i \in \mathbb{Z}_q$, $i \in [n]$. When rounding with respect to this basis, we can write $b = \sum_{i=1}^n \lfloor \alpha_i \rceil_p b_i \in R_p^\vee$. By taking the automorphism $\sigma_k$, we have $\sigma_k(b) = \sigma_k\Big(\sum_{i=1}^n \lfloor \alpha_i \rceil_p b_i\Big) = \sum_{i=1}^n \lfloor \alpha_i \rceil_p \sigma_k(b_i)$. Next we observe that $\sigma_k(a \cdot s \bmod qR^\vee) = \sigma_k(a) \cdot \sigma_k(s) \bmod qR^\vee$, which is also equal to $\sigma_k\big(\sum_{i=1}^n \alpha_i b_i\big)$. Then we have $\lfloor \sigma_k(a) \cdot \sigma_k(s) \rceil_{\mathbf{B},p} = \lfloor \sigma_k\big(\sum_{i=1}^n \alpha_i b_i\big) \rceil_{\mathbf{B},p}$ $= \lfloor \sum_{i=1}^n \alpha_i \sigma_k(b_i) \rceil_{\mathbf{B},p}$.

As $\mathbf{B}$ is a normal integer basis, we know that $\sigma_k$ acts as a permutation over the basis, i.e., $\sigma_k(\mathbf{B})$ is equivalent to $\mathbf{B}$ up to a permutation. Thus,

$$\lfloor \sigma_k(a) \cdot \sigma_k(s) \rceil_{\mathbf{B},p} = \lfloor \sum_{i=1}^n \alpha_i \sigma_k(b_i) \rceil_{\mathbf{B},p} = \sum_{i=1}^n \lfloor \alpha_i \rceil_p \sigma_k(b_i) = \sigma_k(b).$$

Finally, by the Chinese Reminder Theorem, $s \bmod pR^\vee$ can be reconstructed from $\{s \bmod \mathfrak{p}_k R^\vee\}_{k=1}^g$. Since the secret distribution $\psi$ has support over $R_p^\vee \cap (R_q^\vee)^*$, we have $s = s \bmod pR^\vee$. This completes the proof. □

### (W)-$\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ to (W)-$D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi}$

**Definition 4.5 (Hybrid RLWR distribution)** *For $i \in \{1, \cdots, g\}$, $s \in R_p^\vee$, we define the distribution $L^i_{s,q,p}(R,\mathbf{B})$ over $R_q \times R_p^\vee$ as: sample $(a,b) \leftarrow L_{s,q,p}(R,\mathbf{B})$ and output $(a, b+h)$ where $h \in R_p^\vee$ is uniformly random over mod $\mathfrak{p}_i R^\vee$ for all $j \le i$, and 0 over mod all the other ideals, i.e., $\mathfrak{p}_j R^\vee$'s for $j > i$.*

We note that $L^0_{s,q,p}(R,\mathbf{B})$ is the same as $L_{s,q,p}(R,\mathbf{B})$, $L^g_{s,q,p}(R,\mathbf{B})$ is the uniformly random distribution over $R_q \times R_p^\vee$, and the other $L^i_{s,q,p}(R,\mathbf{B})$'s are intermediate hybrids, which will be used via a hybrid argument later.

**Definition 4.6 ((W)-$D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'}$)** *The worst-case $D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'}$ problem is defined as follows: given $\ell$ samples from $L^j_{s,q,p}(R,\mathbf{B})$ for arbitrary $s \in \mathsf{Supp}(\psi')$ and $j \in \{i-1, i\}$, determine $j$.*

**Lemma 4.7 ($\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ to (W)-$D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'}$)** *For any $i \in \{1, \cdots, g\}$, and ideal $\mathfrak{p}_i$ with $N(\mathfrak{p}_i) = p^{n/g} = p^c$ where $c \ge 1$ is a constant integer, there exists a probabilistic polynomial time reduction from $\mathfrak{p}_i$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell'',\psi}$ to (W)-$D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'}$ where $\psi = R_p^\vee \cap (R_q^\vee)^*$, $\psi' = (R_q^\vee)^*$, $\ell'' = p^c \ell \cdot \mathsf{poly}(1/\varepsilon)$, and $\varepsilon$ is the advantage of the (W)-$D$-$\mathsf{RLWR}^i_{\mathbf{B},q,p,\ell,\psi'}$ oracle.*

The proof of this lemma is similar to that of Lemma 5.9 in [26]. Due to the space limit, we put it in full version of this paper.

#### (W)-$D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$ to $D$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}$

**Definition 4.8 ($D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$)** *The average-case $D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$ problem is defined as follows: given $\ell$ samples from $L^{j}_{s,q,p}(R,\mathbf{B})$ for $s \leftarrow U(\psi')$ and $j \in \{i-1, i\}$, determine $j$.*

**Lemma 4.9 (Worst-case to average-case)** *For every $i \in \{1, \cdots, g\}$ and the uniform distribution $\psi'$ over $(R_q^\vee)^*$, there exists a randomized poly-time reduction from worst-case (W)-$D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$ to average-case $D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$.*

The lemma can be proved by the technique of re-randomization of the secret. Due to the space limit, we put the proof in full version of this paper.

**Lemma 4.10 ($D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$ to $D$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}$)** *For any oracle solving the $D$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi'}$ problem with advantage $\varepsilon$, there exists an $i \in \{1, \cdots, g\}$ and an efficient algorithm that solves $D$-$\mathsf{RLWR}^{i}_{\mathbf{B},q,p,\ell,\psi'}$ with advantage $\varepsilon/g$ using this oracle.*

The lemma can be proved by a simple hybrid argument. We put the proof in full version of this paper.

The proof of Theorem 4.2 follows from Lemmas 4.4, 4.7, 4.9, and 4.10.

### 4.2 Search RLWE to Search RLWR

Before presenting the main theorem, we describe some notations that will be used later. First, the ring LWE problem will take parameters to specify the modulus, and the distributions of secret and the error. We will use $\phi$ to denote the error distribution, $\psi$ to denote the secret distribution (same as $\mathsf{RLWR}$). Thus, $\mathsf{RLWE}_{q,\phi,\ell,\psi}$ means the ring LWE problem with modulus $q$, error distribution $\phi$, $\ell$ samples, and secret distribution $\psi$. Next, we use $U_\beta(\mathbf{B})$ to denote the distribution over $R_q^\vee$ that each coefficient with respect to the basis $\mathbf{B}$ over $R^\vee$ is sampled uniformly at random in the interval $[-\beta, \beta]$.

**Theorem 4.11 ($S$-$\mathsf{RLWE}_{q,\phi,\ell,\psi}$ to $S$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi}$)** *Let $\phi$ be a $B_e$-bounded distribution over the canonical imbedding space $H$, $\mathbf{B}$ be a basis of $R^\vee$ with dual basis $\mathbf{B}'$ such that $\|\sigma(b'_j)\|_2 \leq B_d$, and $q \geq 18pB_dB_e\ell n$. Then there exists a poly-time reduction from $S$-$\mathsf{RLWE}_{q,\phi,\ell,\psi}$ to $S$-$\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi}$, where $\psi = R_p^\vee \cap (R_q^\vee)^*$.*

Our reduction can be obtained by the following two steps:

$$S\text{-}\mathsf{RLWE}_{q,\phi,\ell,\psi} \xrightarrow{(1)} S\text{-}\mathsf{RLWE}_{q,\phi+U_\beta(\mathbf{B}),\ell,\psi} \xrightarrow{(2)} S\text{-}\mathsf{RLWR}_{\mathbf{B},q,p,\ell,\psi}.$$

The first reduction is straight-forward. The second reduction uses an RD analysis similar to the work [8]. We note that it is possible to use bound the Rènyi

Divergence of the instances from the first and the third problems. However, this will incur large parameter loss, e.g., the work [14] takes this approach, and they are only able to analyze a constant number of samples, i.e., $\ell = O(1)$.

Due to space limit, we put the proof in full version of this paper.

### 4.3 On Normal Integer Basis and Cyclotomic Fields of Power of 2

Our hardness results require a short normal integral basis by combining Theorem 4.2 and Theorem 4.11. As we discussed in the introduction, by Hilbert-Speiser and Kronecker-Weber theorems, normal integral bases exist for cyclotomic fields with prime-power-free periods and their subfields. It's not hard to determine such a basis in squared-free fields using the idea of [27]. We describe the selection of the bases in full version of this paper.

One very special type of cyclotomic fields is the case of power of 2. This field does not have normal integer basis, but our main Theorem 4.2 can be generalized to this setting *if* we select specify types of rounding function $\lfloor \cdot \rceil$. Note: for normal integer bases (NIB), Theorem 4.2 holds with respect to *any* rounding function. With a careful inspection, the most significant property we need for the theorem is that rounding commutes with automorphisms, which is true if $\mathbf{B}$ is an NIB. However, for cyclotomic fields of power of 2, we know that there is a case where $\sigma(x) = -x$, in which $\lfloor \sigma(x) \rceil$ might be different from $\sigma(\lfloor x \rceil)$ for a general rounding function $\lfloor \cdot \rceil$. Nevertheless, if we use specific rounding function that imposes this constraint, then Theorem 4.2 also holds. A particular example is to round coefficients in the following way: for $z \in \mathbb{R}$, define $\lfloor z \rceil = \mathsf{Sign}(z) \cdot \mathsf{round}(|z|)$ for any rounding function $\mathsf{round} : \mathbb{R}^+ \cup \{0\} \to \mathbb{Z}^+ \cup \{0\}$.

## 5 Module Ring-LWR under Leakage

In this section, we study whether (Module) Ring-LWR is hard in the presence of leakage. As discussed in the introduction, we first present a negative result for Ring-LWR, and thus simply an entropy lower bound is not sufficient to derive leakage resilience over Ring-LWR. Next we show general positive results for Module Ring-LWR, for sufficiently large dimensions. As a key technical building block, we prove a general ring leftover hash lemma.

### 5.1 A Negative Result for Ring-LWR under Leakage

First, we show that Ring-LWR might be completely insecure if the attacker obtains some leakage of the secret. The idea of our attack is similar to that of Ring-LWE by Bolboceanu et al. [9]. Below we present the details.

Let $\mathfrak{q} \supset qR$ be an integral ideal in $R$, we let $\bar{\mathfrak{q}} = q\mathfrak{q}^{-1}$ denote its complement with respect to $qR$. Then we have that $\bar{\mathfrak{q}}^\vee = (q\mathfrak{q}^{-1})^\vee = \frac{1}{q}(\mathfrak{q}^{-1})^\vee = \frac{1}{q}\mathfrak{q}R^\vee$ with respect to $R^\vee$. Before presenting the attack on Ring-LWR, we first recall the attack of Ring-LWE in [9].

**Lemma 5.1 ( [9])** *Let $K, R$ be a degree $n$ number field and its ring of integers, $\mathfrak{q} \supset qR$ be an integral $R$-ideal, and $\bar{\mathfrak{q}} = q\mathfrak{q}^{-1}$ be its complement. There exists a non-uniform algorithm such that for any secret distribution $\psi$, any error distribution $\phi$ satisfying that $\mathsf{Pr}_{e \leftarrow \phi}[\|e\|_2 < 1/(2\lambda_n(\bar{\mathfrak{q}}))]$ is non-negligible, the algorithm solves search $\mathsf{RLWE}_{q,\phi,1,\psi}$ with a non-negligible probability.*

Then the attack can be described by the the corollary below.

**Corollary 5.2 (Attack for RLWR with Entropic Secrets)** *Let $K, R$ be a degree $n$ cyclotomic field and its ring of integers, $\mathbf{B}$ be a basis of $R$ with $B_d$-bounded $\ell_\infty$ norm for all its elements, $q = pp'$ where $p$ is a prime such that $pR$ completely splits as prime ideals over $R$.*

*Then for every integer $\eta \in [n]$, letting $\epsilon = \eta/n$, if $p^\epsilon > 2n^{5/2}p'B_d$, there exists a distribution $\psi$ over $R_p^\vee$ with entropy $(1-\epsilon)n \log p$ such that $\mathsf{RLWR}_{\mathbf{B},q,p,1,\psi}$ can be solved with a non-negligible probability.*

*Proof.* Let $qR = pp'R = \prod_i^n \mathfrak{p}_i \cdot p'R$, where $pR = \prod_i^n \mathfrak{p}_i$. We define the distribution $\psi$ as follows: given a parameter $\eta \in [n]$, set ideal $\mathcal{I} = \prod_i^\eta \mathfrak{p}_i$. Then a sample from $\psi$ is generated by choosing $s \leftarrow \mathcal{I}R^\vee/pR^\vee$ uniformly random in this ideal.

For a given $L_{s,q,p}(R, \mathbf{B})$ sample $(a, b = \lfloor a \cdot s \rceil_{\mathbf{B},p}), s \leftarrow \psi$, $b$ can be written as $b = \frac{p}{q}a \cdot s + \delta$, where $\delta = \lfloor a \cdot s \rceil_{\mathbf{B},p} - \frac{p}{q}a \cdot s$ can be viewed as the deterministic noise induced by rounding. The coefficients of the noise with respect to $\mathbf{B}$ belong to $[-1, 1]$ (real numbers). First we set $b' = \frac{1}{p}b = \frac{1}{q}a \cdot s + \frac{1}{p}\delta$ (as an element in $K_\mathbb{R}$). By Lemma 5.1, we know that if $\|\frac{1}{p}\delta\|_2 < 1/(2\lambda_n(\bar{\mathfrak{q}}))$ with non-negligible probability, $s$ can be recovered by non-negligible probability.

It remains to bound the $\ell_2$ norm of $\frac{1}{p}\delta$. According the definition of $\delta$, the coefficients of $\frac{1}{p}\delta$ with respect to $\mathbf{B}$ belong to $[-\frac{1}{p}, \frac{1}{p}]$. Writing $\frac{1}{p}\delta = \langle \mathbf{B}, \boldsymbol{c} \rangle$, then by Cauchy-Schwarz inequality: $\|\frac{1}{p}\delta\|_2 \le \|\sum_{i=1}^n c_i\sigma(b_i)\|_2 \le \sum_{i=1}^n |c_i| \cdot \|\sigma(b_i)\|_2 \le \frac{1}{p}\sum_{i=1}^n \|\sigma(b_i)\|_2$. Furthermore $\|\sigma(b_i)\|_2 = (\sum_{i=1}^n |\sigma(b_i)|^2)^{1/2} \le \sqrt{n}B_d$. We can bound the $\ell_2$ norm of $\frac{1}{p}\delta$ by $\frac{1}{p}n^{3/2}B_d$.

On the other hand, by similar calculation as [9], we know that $\lambda_n(\bar{\mathfrak{q}}) \le \frac{nq}{p^{\eta/n}} = np'p^{1-\epsilon}$. By the parameters setting, we have that $\|\frac{1}{p}\delta\| < \frac{1}{2\lambda_n(\bar{\mathfrak{q}})}$, as desired. □

**Remark 5.3** *Corollary 5.2 can be easily generalized to the case where the secret is uniformly random over $R^\vee/pR^\vee$, yet the attacker learns the information of $s' = s \mod \mathcal{I}R^\vee$ for $\mathcal{I} = \prod_{i=1}^\eta \mathfrak{p}_i$. We can set $b' = \frac{1}{p}b - \frac{1}{q}as' = \frac{1}{q}a \cdot (s - s') + \frac{1}{p}\delta$. Then this reduces back to the entropic secret as $s - s' \in \mathcal{I}$. By applying Corollary 5.2, the attacker learns $s - s'$, and then he can recover $s$.*

### 5.2 Towards Leakage Resilience of Module Ring-LWR

Next, we proceed to prove that Module Ring-LWR is pseudorandom for entropic secrets (under some entropy requirements) for larger dimensions. To achieve this, we first prove a general leftover hash lemma in the ring setting as a new tool. By using the leftover hash lemma, we are able to generalize the plain LWR hardness

result of [3] to the ring setting. Depending on the splitting of $qR$, we are able to achieve different range of parameters. We present two important case studies: (1) $qR$ is low-splitting, i.e., it splits into fewer but larger ideals, and (2) general cases where $qR$ can be arbitrary. In the former case, we are able to achieve smaller parameters, as low-splitting is in favor of randomness extraction by the leftover hash lemma. We will elaborate further below.

**New Tool: A New Algebraic Leftover Hash Lemma**

**Definition 5.4 (Hash Family over (Algebraic) Lattice)** *Let $q, k \geq 2$ be integers, $\mathcal{L}$ be lattice over the number field $K$, and $\mathcal{O}^{\mathcal{L}}$, $\mathcal{L}^{\vee}$ be its coefficient ring and dual lattice, respectively. We define the following hash function family $\mathcal{H}(\mathcal{O}^{\mathcal{L}}, \mathcal{X}, q, k) = \{f_{\boldsymbol{a}} : (\mathcal{L}_q^{\vee})^k \to \mathcal{L}_q^{\vee}\}_{\boldsymbol{a} \in (\mathcal{O}_q^{\mathcal{L}})^k}$ as $f_{\boldsymbol{a}}(\boldsymbol{x}) = \sum_{i=1}^{k} x_i \cdot a_i \bmod q(\mathcal{L})^{\vee}$, for all $\boldsymbol{x} \in \mathcal{X} \subseteq (\mathcal{L}_q^{\vee})^k$, where $\sum_i x_i \cdot a_i$ is computed by using the field addition and multiplication over $K$.*

In this paper, we consider $\mathcal{L} = R = \mathcal{O}_K$ and $\mathcal{L} = \mathcal{O}$ for an arbitrary order of $K = \mathbb{Q}(\alpha)$ (or their dual $R^{\vee}$ and $\mathcal{O}^{\vee}$). We remark that for any $\mathcal{O} \subseteq \mathcal{O}_K$, there exists an isomorphism between $\mathcal{O}_q$ and $R_q$ as long as $|\mathcal{O}/R|$ is coprime with $q$ [37]. For brevity, we focus on the case of $\mathcal{L} = R = \mathcal{O}_K$, and analogous properties of $\mathcal{O}$ will follow by which of $\mathcal{O}_K$ according to the isomorphism.

Next we introduce the following variant of the Leftover Hash Lemma [19], generalized to the ring of integers of any arbitrary number field $K$ (not necessarily a Galois extension). Before presenting the description of the lemma, we first define the distribution as follows

$$\mathcal{D}(\mathcal{H}, R_q^{\vee}) = \{(f_{\boldsymbol{a}}, b) | f_{\boldsymbol{a}} \xleftarrow{\$} \mathcal{H}(R, \mathcal{X}, q, k), b = f_{\boldsymbol{a}}(\boldsymbol{x}) \text{ for } \boldsymbol{x} \leftarrow \mathcal{X}\}.$$

For simplicity, we will use $\boldsymbol{a}$ to stand for the description of $f_{\boldsymbol{a}}$ in the distribution $\mathcal{D}(\mathcal{H}, R_q^{\vee})$, and then $\mathcal{D}(\mathcal{H}, R_q^{\vee})$ can be simply denoted as $\mathcal{D}((R_q)^k, R_q^{\vee}) = \{(\boldsymbol{a}, b) | \boldsymbol{a} \xleftarrow{\$} (R_q)^k, b = f_{\boldsymbol{a}}(\boldsymbol{x}) \text{ for } \boldsymbol{x} \leftarrow \mathcal{X}\}$. Our goal is to prove that $\mathcal{D}(\mathcal{H}, R_q^{\vee})$ is statistically close to the uniform distribution if the input distribution $\mathcal{X}$ satisfies a certain entropy condition.

To achieve this, we need some preparation of the following definition: we say that vector $\boldsymbol{r} \in (R^{\vee})^k$ *maximal belongs* to a factor $\mathcal{I}$ of $qR$, abbreviated as $\boldsymbol{r} \in_{\max} \mathcal{I}R^{\vee}$ if the following conditions hold.

- For every coordinate $r_i$ of $\boldsymbol{r}$, we have $r_i \in \mathcal{I}R^{\vee}$.
- For any ideal $\mathcal{J} | qR$ such that $\mathcal{I} | \mathcal{J}$, there exists at least one coordinate $r_j$ such that $r_j \notin \mathcal{J}R^{\vee}$.

Now we present our main result as follows:

**Theorem 5.5 (Algebraic Leftover Hash Lemma)** *For any hash function family $\mathcal{H}(R, \mathcal{X}, q, k)$ over a number field $K = \mathbb{Q}(\alpha)$ with degree $n$ and $\gcd(q, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$, we have*

$$\Delta\big(\mathcal{D}(\mathcal{H}, R_q^{\vee}), U(\mathcal{H}, R_q^{\vee})\big) \leq \frac{1}{2} \sqrt{\sum_{\substack{\mathfrak{q} \neq \langle 1 \rangle \\ \mathfrak{q} | qR}} N(\mathfrak{q}) \mathsf{Col}(\mathcal{X}_{\mathfrak{q}})},$$

*where* $\mathcal{X}_{\mathfrak{q}} = \{\boldsymbol{x} \bmod \mathfrak{q}R^\vee | \boldsymbol{x} \leftarrow \mathcal{X}\}$, $\mathsf{Col}(\mathcal{X}_{\mathfrak{q}})$ *is the collision probability of* $\mathcal{X}_{\mathfrak{q}}$, *and* $\mathfrak{q}$ *ranges over all divisors* (except $\langle 1 \rangle$) *of the ideal* $\langle q \rangle = qR$.

*Proof.* As discussed above, we need to bound $\Delta\big(\mathcal{D}((R_q)^k, R_q^\vee), U((R_q)^k, R_q^\vee)\big)$. To do this, we first derive an upper bound on the statistical distance between $\mathcal{D}((R_q)^k, R_q^\vee)$ and $U((R_q)^k, R_q^\vee)$ (which are written as $\mathcal{D}$ and $U$ for simplicity) in terms of the collision probability $\mathsf{Col}(\mathcal{D})$.

$$\begin{aligned}
\Delta(\mathcal{D}, U) &= \frac{1}{2} \sum_{(\boldsymbol{a},b) \in U} \left| \mathsf{Pr}[(\boldsymbol{a}, b) \leftarrow \mathcal{D}] - \frac{1}{|U|} \right| \\
&\leq \frac{1}{2} \sqrt{|U|} \sqrt{\sum_{(\boldsymbol{a},b) \in U} \left( \mathsf{Pr}[(\boldsymbol{a}, b) \leftarrow \mathcal{D}] - \frac{1}{|U|} \right)^2} \\
&= \frac{1}{2} \sqrt{|U|} \sqrt{-\frac{1}{|U|} + \sum_{(\boldsymbol{a},b) \in U} \mathsf{Pr}[(\boldsymbol{a}, b) \leftarrow \mathcal{D}]^2} \\
&\leq \frac{1}{2} \sqrt{|U| \cdot \mathsf{Col}(\mathcal{D}) - 1}.
\end{aligned} \tag{1}$$

Next we bound $\mathsf{Col}(\mathcal{D})$ as follows, where all probabilities run through two independently copies of $\boldsymbol{a}, \boldsymbol{a}' \leftarrow (R_q)^k$ and $\boldsymbol{x}, \boldsymbol{y} \leftarrow \mathcal{X}$:

$$\begin{aligned}
\mathsf{Col}(\mathcal{D}) &= \mathsf{Pr}[(\boldsymbol{a} = \boldsymbol{a}') \wedge (\boldsymbol{a} \cdot \boldsymbol{x} = \boldsymbol{a}' \cdot \boldsymbol{y} \bmod qR^\vee)] \\
&= \mathsf{Pr}[\boldsymbol{a} = \boldsymbol{a}'] \cdot \mathsf{Pr}[\boldsymbol{a} \cdot \boldsymbol{x} - \boldsymbol{a}' \cdot \boldsymbol{y} = 0 \bmod qR^\vee | \boldsymbol{a} = \boldsymbol{a}'] \\
&= \frac{1}{q^{nk}} \cdot \mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{x} - \boldsymbol{y}) = 0 \bmod qR^\vee].
\end{aligned} \tag{2}$$

Now we further bound the probability $\mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{x} - \boldsymbol{y}) = 0 \bmod qR^\vee]$. To do this, we first let $q = p_1^{r_1} \cdots p_t^{r_t}$ be the prime (integer) factorization, and the consider the the (ideal) decomposition of $qR$. Since $\gcd(q, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$, we can apply Lemma 2.4 on each prime factor and obtain $p_i R = \prod_{j \in [g_i]} \mathfrak{p}_{i,j}^{e'_{i,j}}$ where $\mathfrak{p}_{i,j} = \langle p_i, f_{i,j}(\alpha) \rangle$ for some monic irreducible polynomial $f_{i,j}(x) \in \mathbb{Z}_{p_i}[x]$, for $i \in [t]$. Thus, $qR = p_1^{r_1} \cdots p_t^{r_t} R = \prod_{i,j} \mathfrak{p}_{i,j}^{e_{i,j}}$, where $e_{i,j} = e'_{i,j} r_i$ for every $i \in [t], j \in [g_i]$. We also have $qR^\vee = \prod_{i,j} \mathfrak{p}_{i,j}^{e_{i,j}} R^\vee$ by Lemma 2.6.

Then we observe a simple fact that any possible $\boldsymbol{x} - \boldsymbol{y}$ in the range must maximal belong to $\mathcal{J}R^\vee$ for only one ideal factor $J | qR$. We sketch a simple proof by contradiction. Assume there are $\mathcal{J}_1 \neq \mathcal{J}_2$ that a vector $\boldsymbol{x} \in_{\max} \mathcal{J}_1$ and $\boldsymbol{x} \in_{\max} \mathcal{J}_2$. Then it is not hard to see that $\boldsymbol{x}$ maximal belongs to their LCM, i.e., $\mathcal{J}_1 \cap \mathcal{J}_2$, a strictly smaller ideal. Then we know that $\mathcal{J}_1 | \mathcal{J}_1 \cap \mathcal{J}_2$, and every element of $\boldsymbol{x}$ belongs to $\mathcal{J}_1 \cap \mathcal{J}_2$, reaching a contradiction to $\boldsymbol{x} \in_{\max} \mathcal{J}_1$.

As $\{(\boldsymbol{x} - \boldsymbol{y}) \in_{\max} \mathcal{J}\}_{\mathcal{J} | qR^\vee}$ forms a partition (as argued above), we can use the total probability to re-write the following equation:

$$\begin{aligned}
&\mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{x} - \boldsymbol{y}) = 0 \bmod qR^\vee] \\
&= \sum_{\mathcal{J} | qR^\vee} \mathsf{Pr}[\boldsymbol{a} \cdot (\boldsymbol{x} - \boldsymbol{y}) = 0 \bmod qR^\vee | \boldsymbol{x} - \boldsymbol{y} \in_{\max} \mathcal{J}R^\vee] \cdot \mathsf{Pr}[\boldsymbol{x} - \boldsymbol{y} \in_{\max} \mathcal{J}R^\vee].
\end{aligned} \tag{3}$$

We know the probability $\mathsf{Pr}[\boldsymbol{x}-\boldsymbol{y} \in_{\max} \mathcal{J}R^\vee] \leq \mathsf{Pr}[\boldsymbol{x}-\boldsymbol{y}=0 \bmod \mathcal{J}R^\vee] = \mathsf{Col}(\mathcal{X}_\mathcal{J})$ for every $\mathcal{J}|qR$. Thus, it remains to compute

$$\mathsf{Pr}\left[\boldsymbol{a}\cdot(\boldsymbol{x}-\boldsymbol{y})=0 \bmod qR^\vee | \boldsymbol{x}-\boldsymbol{y} \in_{\max} \mathcal{J}R^\vee\right].$$

Without loss of generality, we let $\mathcal{J}=\prod_{i,j}\mathfrak{p}_{i,j}^{x_{i,j}}, 0\leq x_{i,j}\leq e_{i,j}$. By Chinese Reminder Theorem 2.5, we have $R^\vee/qR^\vee \cong \bigoplus_{i,j} R^\vee/\mathfrak{p}_{i,j}^{e_{i,j}}$. Thus, we can view a random ring element in $R^\vee/qR^\vee$ as independently random coordinates in $\{R^\vee/\mathfrak{p}_{i,j}^{e_{i,j}}\}_{i,j}$. Therefore, we write:

$$\begin{aligned}
&\mathsf{Pr}[\boldsymbol{a}\cdot(\boldsymbol{x}-\boldsymbol{y})=0 \bmod qR^\vee | \boldsymbol{x}-\boldsymbol{y} \in_{\max} \mathcal{J}R^\vee] \\
=&\prod_{i,j}\mathsf{Pr}[\boldsymbol{a}\cdot(\boldsymbol{x}-\boldsymbol{y})=0 \bmod \mathfrak{p}_{i,j}^{e_{i,j}}R^\vee | \boldsymbol{x}-\boldsymbol{y} \in_{\max} \mathcal{J}R^\vee] \\
=&\prod_{i,j}\mathsf{Pr}[\boldsymbol{a}_{i,j}\cdot(\boldsymbol{x}-\boldsymbol{y})_{i,j}=0 \bmod \mathfrak{p}_{i,j}^{e_{i,j}}R^\vee | \boldsymbol{x}-\boldsymbol{y} \in_{\max} \mathcal{J}R^\vee],
\end{aligned} \tag{4}$$

where $\boldsymbol{a}_{i,j}=\boldsymbol{a} \bmod \mathfrak{p}_{i,j}^{e_{i,j}}, (\boldsymbol{x}-\boldsymbol{y})_{i,j}=\boldsymbol{x}-\boldsymbol{y} \bmod \mathfrak{p}_{i,j}^{e_{i,j}}R^\vee$.

Next we will determine the ideal generated by the vector $(\boldsymbol{x}-\boldsymbol{y})_{i,j} = ((\boldsymbol{x}-\boldsymbol{y})_{i,j}[1],\cdots,(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k])$, so that we can apply Lemma 2.3 to bound the probability $\mathsf{Pr}[\boldsymbol{a}_i\cdot(\boldsymbol{x}-\boldsymbol{y})_i=0 \bmod \mathfrak{p}_{i,j}^{e_{i,j}}R^\vee | \boldsymbol{x}-\boldsymbol{y} \in_{\max} \mathcal{J}R^\vee]$ for each $i,j$.

**Claim 5.6** *The ideal generated by vector $(\boldsymbol{x}-\boldsymbol{y})_{i,j}$ is $\mathfrak{p}_{i,j}^{x_{i,j}}R^\vee$.*

*Proof.* Below we will use $r_p$ to denote a ring element $r$ modulo an integer $p$, i.e., $r_p = r \mod p$, for short.

By definition of $(\boldsymbol{x}-\boldsymbol{y}) \in_{\max} \mathcal{J}$, we know that for each $\eta\in[k]$, $(\boldsymbol{x}-\boldsymbol{y})_{i,j}[\eta] \in \mathfrak{p}_{i,j}^{x_{i,j}}R^\vee/\mathfrak{p}_{i,j}^{e_{i,j}}R^\vee$. Therefore, the ideal $\langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}\rangle$ generated by vector $(\boldsymbol{x}-\boldsymbol{y})_{i,j}$ satisfies $\langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}\rangle \subseteq \mathfrak{p}_{i,j}^{x_{i,j}}R^\vee$.

On the other hand, there exists $k'\in[k]$ such that $(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k'] \notin \mathfrak{p}_{i,j}^{x_{i,j}+1}R^\vee/\mathfrak{p}_{i,j}^{e_{i,j}}R^\vee$. It is clear that the principle ideal $\langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k']\rangle$ generated by $(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k']$ satisfies that $\langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k']\rangle \subseteq \langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}\rangle$. Thus in order to show $\langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}\rangle = \mathfrak{p}_{i,j}^{x_{i,j}}R^\vee$, it suffices to show $\mathfrak{p}_{i,j}^{x_{i,j}}R^\vee \subseteq \langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k']\rangle$.

According to Lemma 2.6 and the isomorphism theorem, we have

$$\mathfrak{p}_{i,j}^{x_{i,j}}R^\vee/\mathfrak{p}_{i,j}^{e_{i,j}}R^\vee \cong \mathfrak{p}_{i,j}^{x_{i,j}}R/\mathfrak{p}_{i,j}^{e_{i,j}}R \cong \left(\mathfrak{p}_{i,j}^{x_{i,j}}/\langle p_i\rangle\right)/\left(\mathfrak{p}_{i,j}^{e_{i,j}}/\langle p_i\rangle\right) = \left\langle f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\right\rangle/\left\langle f_{i,j}^{e_{i,j}}(\alpha)_{p_i}\right\rangle,$$

and as well

$$\mathfrak{p}_{i,j}^{x_{i,j}+1}R^\vee/\mathfrak{p}_{i,j}^{e_{i,j}}R^\vee \cong \mathfrak{p}_{i,j}^{x_{i,j}+1}R/\mathfrak{p}_{i,j}^{e_{i,j}}R \cong \left\langle f_{i,j}^{x_{i,j}+1}(\alpha)_{p_i}\right\rangle/\left\langle f_{i,j}^{e_{i,j}}(\alpha)_{p_i}\right\rangle.$$

Then we can see that, there exists an element $r\cdot f_{i,j}^{x_{i,j}}(\alpha)_{p_i} \in \left\langle f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\right\rangle/\left\langle f_{i,j}^{e_{i,j}}(\alpha)_{p_i}\right\rangle$ that is equivalent to $(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k']$ under the isomorphism, satisfying $r\in R, r\notin \left\langle f_{i,j}(\alpha)_{p_i}\right\rangle$. Therefore, $\mathfrak{p}_{i,j}^{x_{i,j}}R^\vee \subseteq \langle(\boldsymbol{x}-\boldsymbol{y})_{i,j}[k']\rangle$ is equivalent to $\left\langle f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\right\rangle \subseteq \left\langle r\cdot f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\right\rangle$, under the view of the isomorphism. It remains to show $\left\langle f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\right\rangle \subseteq \left\langle r\cdot f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\right\rangle$.

To see this, we denote $u = r \bmod f_{i,j}(\alpha)_{p_i} \in R_{p_i}/\langle f_{i,j}(\alpha)_{p_i}\rangle$. We notice that $R_{p_i}/\langle f_{i,j}(\alpha)_{p_i}\rangle \cong R/\mathfrak{p}_{i,j}$, which is a field as $\mathfrak{p}_{i,j}$ is a prime ideal according to

Lemma 2.4. Therefore, $u \neq 0$ is invertible over $R_{p_i}/\langle f_{i,j}(\alpha)_{p_i}\rangle$, and hence there is an element $v \in R_{p_i}/\langle f_{i,j}(\alpha)_{p_i}\rangle$ such that $vr = 1 \bmod f_{i,j}(\alpha)_{p_i}$. From this, there exist $vr \in \langle r\rangle, tf_{i,j}(\alpha)_{p_i} \in \langle f_{i,j}(\alpha)_{p_i}\rangle$ such that $vr + tf_{i,j}(\alpha)_{p_i} = 1$, so $\langle r\rangle$ is coprime to $\langle f_{i,j}(\alpha)_{p_i}\rangle$. Furthermore, according to Lemma 2.2, $\langle r\rangle$ is coprime to $\langle f_{i,j}^{e_{i,j}}(\alpha)_{p_i}\rangle$, and thus $r$ is invertible over $R_{p_i}/\langle f_{i,j}^{e_{i,j}}(\alpha)_{p_i}\rangle$. Therefore, any element $\mu \cdot f_{i,j}^{x_{i,j}}(\alpha)_{p_i} = \mu \cdot r^{-1} r \cdot f_{i,j}^{e_{i,j}}(\alpha)_{p_i} \in \langle f_{i,j}^{e_{i,j}}(\alpha)_{p_i}\rangle$ also belongs to $\langle r \cdot f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\rangle$. This reaches our desired conclusion that $\langle f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\rangle \subseteq \langle r \cdot f_{i,j}^{x_{i,j}}(\alpha)_{p_i}\rangle$. □

From Lemma 2.3 and Claim 5.6, we know that $\mathsf{Pr}[\boldsymbol{a}_i \cdot (\boldsymbol{x}-\boldsymbol{y})_i = 0 \bmod \mathfrak{p}_{i,j}^{e_{i,j}} R^\vee | \boldsymbol{x} - \boldsymbol{y} \in_{\max} \mathcal{J}R^\vee] = \frac{N(\mathfrak{p}_{i,j}^{x_{i,j}})}{N(\mathfrak{p}_{i,j}^{e_{i,j}})}$. Then we continue to compute equation (4):

$$\begin{aligned} &\prod_{i,j} \mathsf{Pr}[\boldsymbol{a}_i \cdot (\boldsymbol{x}-\boldsymbol{y})_i = 0 \bmod \mathfrak{p}_{i,j}^{e_{i,j}} | \boldsymbol{x} - \boldsymbol{y} \in_{\max} \mathcal{J}R^\vee] \\ =&\prod_{i,j} \frac{N(\mathfrak{p}_{i,j}^{x_{i,j}})}{N(\mathfrak{p}_{i,j}^{e_{i,j}})} = \prod_{i,j} \frac{N(\mathfrak{p}_{i,j})^{x_{i,j}}}{N(\mathfrak{p}_{i,j}^{e_{i,j}})} = \frac{N(\mathcal{J})}{\prod_i N(p_i)} = \frac{N(\mathcal{J})}{q^n}. \end{aligned} \tag{5}$$

Combine equations (1),(2),(3),and using the facts $N(R) = 1$, $\mathsf{Col}(\mathcal{X}_R) = 1$, yields the bound in the lemma. □

From our leftover hash lemma, we can derive the following corollaries for three important cases: (1) the general case, (2) $K$ is a cyclotomic field, and (3) $qR$ does not have a "small" ideal factor (in the norm). Due to the limitation of space, we defer the proof to full version of this paper.

**Corollary 5.7** *Let $k, e, q$ be integers, $\varepsilon \in (0,1)$, and $R = \mathcal{O}_K$ be the ring of integers of a number field $K = \mathbb{Q}(\alpha)$ with degree $n$, such that $\gcd(q, [\mathcal{O}_K : \mathbb{Z}[\alpha]) = 1$ and $e \geq 2\log\left(\frac{1}{\varepsilon}\right) + 2n\log q - 2$. Suppose $\boldsymbol{s}$ is chosen from some distribution $\mathcal{X}$ over $(R_q^\vee)^k$ such that $H_\infty(\boldsymbol{s} \bmod \mathfrak{q}) \geq e$ for any ideal $\mathfrak{q}|qR$, and $\boldsymbol{a} \xleftarrow{\$} (R_q)^k, u \xleftarrow{\$} R_q^\vee$ are uniformly random and independent of $\boldsymbol{s}$. Then we have that $\Delta\big[(\boldsymbol{a}, \langle \boldsymbol{a}, \boldsymbol{s}\rangle \bmod qR^\vee), (\boldsymbol{a}, u)\big] \leq \varepsilon$.*

**Corollary 5.8 (Cyclotomic Fields)** *Adopt the notations in Corollary 5.7. Let $K$ be a cyclotimic number field of degree $n$. The conclusion holds for $e \geq 2\log\left(\frac{1}{\varepsilon}\right) + (n+2)\log q - 2$.*

**Corollary 5.9 (Large Ideal Factors)** *Adopt the notations in Corollary 5.7. The conclusion holds if for any prime ideal factor $\mathfrak{p}_{i,j}$ of $qR$, we have $N(\mathfrak{p}_{i,j}) \geq n\log q + 1$, and $e \geq 2\log\left(\frac{1}{\varepsilon}\right) + n\log q$.*

### 5.3 Hardness of Module-RLWR

In this section, we present hardness results of Module Ring-LWR, by applying our new leftover hash lemma to the proof framework of [3]. We first present a definition of module-RLWR under weak secrets, a generalization of the plain weak LWR in the work [3].

**Definition 5.10 (Weak Module-RLWR)** *Let $n, p, q, \ell, k$ be positive integers, $R = \mathcal{O}_K$ be the ring of integers of a number field $K$ with degree $n$, $\mathbf{B}$ be a basis of $R^\vee$, and the decomposition of $qR$ be $\mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$ where each $\mathfrak{q}_i$ is a prime ideal over $R^\vee$. The (decision) $\mathsf{wRLWR}^k_{\mathbf{B},q,p,\ell,\gamma,e}$ assumption is defined as: let $(\boldsymbol{s}, \mathsf{aux})$ be a pair of correlated random variable where*

- *each coefficient $s_i[j]$ of each $s_i$ relative to $\mathbf{B}$ has range in $[-\gamma, \gamma]$ for $i \in [k], j \in [n]$;*
- *$H_\infty(\boldsymbol{s} \bmod \mathfrak{q}_j | \mathsf{aux}) \geq e$ for each prime ideal factor $\mathfrak{q}_j$ of $qR$.*

*The task is to distinguish the following two distributions:*

$$(\mathsf{aux}, \mathbf{A}, \lfloor \mathbf{A} \cdot \boldsymbol{s} \rceil_{\mathbf{B},p}) \text{ versus } (\mathsf{aux}, \mathbf{A}, \lfloor \boldsymbol{u} \rceil_{\mathbf{B},p}),$$

*where $\mathbf{A} \xleftarrow{\$} (R_q)^{\ell \times k}$, $\boldsymbol{u} \xleftarrow{\$} (R_q^\vee)^\ell$ are uniform and independent of $(\boldsymbol{s}, \mathsf{aux})$.*

Below we describe two interesting case studies: (1) when $qR$ is low-splitting, i.e., it factors into fewer but larger ideals (in norm), and (2) the general case. For the low-splitting case, we are able to achieve the following theorem.

**Theorem 5.11 (Hardness of Module-RLWR for Low-splitting Case)** *Let $\lambda, n, p, q, \ell, k, \gamma$ be positive integers, $R = \mathcal{O}_K$ be the ring of integers of a number field $K = \mathbb{Q}(\alpha)$ with degree $n$, $\mathbf{B}$ be a basis of $R^\vee$ with $B_{d_1}$ bounded $\ell_\infty$ norm for all entries, all entries of its dual basis $\mathbf{B}'$ be $B_{d_2}$-bounded in $\ell_\infty$ norm, $t \in (R^\vee)^{-1}$ such that $tR^\vee + qR = R$, $\phi$ be a $\beta$-bounded distribution over $K_\mathbb{R}$ for some real $\beta > 0$, such that $q \geq 2B_{d_1}B_{d_2}\beta\gamma k\ell p n^{\frac{5}{2}}$ and $\gcd(q, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$.*

*Assume that the decomposition of $qR$ can be expressed as $\prod_{i,j} \mathfrak{p}_{i,j}^{e_{i,j}}$, where each $\mathfrak{p}_{i,j}$ is a prime ideal over $R$, and $N(\mathfrak{p}_{i,j}) \geq 2^\lambda \geq n \log q + 1$. Then we have the following:*

- *(High entropy secret) There exists a poly-time reduction from $\mathsf{RLWE}_{q,t^{-1}\cdot\phi,\ell}$ to $\mathsf{wRLWR}^k_{\mathbf{B},q,p,\ell,\gamma,e}$, where $e \geq \big(2n + \lambda\big) \log q + 2\lambda$.*
- *(Uniform secret) There exists a poly-time reduction from $\mathsf{RLWE}_{q,t^{-1}\cdot\phi,\ell}$ to $\mathsf{RLWR}^k_{\mathbf{B},q,p,\ell}$, where $k \geq \frac{\log q}{\lambda \log(2\gamma)}\big((2n + \lambda) \log q + 2\lambda\big)$.*

The theorem can be proved by similar techniques as [3] together with Theorem 5.5. As the proof structure is similar to that in the prior work, for completeness we describe the proof in full version of this paper.

**Theorem 5.12 (Hardness of Module-RLWR for General Cases)** *Let $\lambda, n, p, q, \ell, f, k, \gamma$ be positive integers, $R = \mathcal{O}_K$ be the ring of integers of a field extension $K = \mathbb{Q}(\alpha)$ with degree $n$, $K'$ be a number field and $R'$ be the ring of integers of $K'$ that is a rank-$f$ free $R$-module with known basis, $\mathbf{B}$ be a basis of $R^\vee$ with $B_{d_1}$ bounded $\ell_\infty$ norm for all entries, and also all entries of its dual basis $\mathbf{B}'$ be with $B_{d_2}$-bounded $\ell_\infty$ norm, $t \in (R'^\vee)^{-1}$ such that $tR'^\vee + qR' = R'$, $\phi$ be a $\beta$-bounded distribution over $K_\mathbb{R}$ for some real $\beta > 0$, such that $q \geq 2B_{d_1}B_{d_2}\beta\gamma k\ell p n^{\frac{5}{2}}$ and $\gcd(q, [\mathcal{O}_K : \mathbb{Z}[\alpha]]) = 1$. Then we have the following:*

– *(High entropy secret) There exists a poly-time reduction from* $\mathsf{RLWE}_{q,t^{-1}\phi',\ell}$ *to* $\mathsf{wRLWR}^k_{\mathbf{B},q,p,\ell,\gamma,e}$*, where* $\phi'$ *is a distribution over* $K'_{\mathbb{R}}$ *such that* $\phi = \mathrm{Tr}_{K'_{\mathbb{R}}/K_{\mathbb{R}}}(\phi')$ *and* $e \geq \big((f+2)n+\lambda\big)\log q + 2\lambda - 2$.
– *(Uniform secret) There exists a poly-time reduction from* $\mathsf{RLWE}_{q,t^{-1}\phi',\ell}$ *to* $\mathsf{RLWR}^k_{\mathbf{B},q,p,\ell}$*, where* $\phi'$ *is as above and* $k \geq \frac{\log q}{\log(N(\mathfrak{q}_i)_{\min})\log(2\gamma)}\big(((f+2)n+\lambda)\log q + 2\lambda - 2\big)$.

The proof of this theorem is similar to that of Theorem 5.11, we detail it in full version of this paper.

For the case of cyclotomic fields, according to Corollary 5.8, we have the following tighter result.

**Corollary 5.13** *Adopt the notations of Theorem 5.12. Let* $K$ *be a cyclotomic field of degree* $n$*, then*

– *(High entropy secret) There exists a poly-time reduction from* $\mathsf{RLWE}_{q,t^{-1}\phi',\ell}$ *to* $\mathsf{wRLWR}^k_{\mathbf{B},q,p,\ell,\gamma,e}$*, where* $k \geq \big((f+1)n+\lambda+2\big)\log q + 2\lambda - 2$.
– *(Uniform secret) There exists a poly-time reduction from* $\mathsf{RLWE}_{q,t^{-1}\phi',\ell}$ *to* $\mathsf{RLWR}^k_{\mathbf{B},q,p,\ell}$*, where* $k \geq \frac{\log q}{\log(N(\mathfrak{q}_i)_{\min})\log(2\gamma)}\big(((f+1)n+\lambda+2)\log q + 2\lambda - 2\big)$.

**Acknowledgement.** The authors would like to thank Han Wang for insightful discussions and anonymous reviewers of Crypto 2020 for their comments. This work is supported by NSF Awards CNS-1657040 and CNS-1942400. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the sponsors.

## References

1. M. R. Albrecht, R. Player, and S. Scott. On the concrete hardness of learning with errors. *Journal of Mathematical Cryptology*, 9(3):169–203, 2015.
2. J. Alperin-Sheriff and D. Apon. Dimension-preserving reductions from lwe to lwr.
3. J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs. Learning with rounding, revisited - new reduction, properties and applications. In R. Canetti and J. A. Garay, editors, *CRYPTO 2013, Part I*, volume 8042 of *LNCS*, pages 57–74. Springer, Heidelberg, Aug. 2013.
4. S. Bai, K. Boudgoust, D. Das, A. Roux-Langlois, W. Wen, and Z. Zhang. Middle-product learning with rounding problem and its applications. In *ASIACRYPT 2019, Part I*, LNCS, pages 55–81. Springer, Heidelberg, Dec. 2019.
5. S. Bai, A. Langlois, T. Lepoint, D. Stehlé, and R. Steinfeld. Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance. In T. Iwata and J. H. Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 3–24. Springer, Heidelberg, Nov. / Dec. 2015.
6. A. Banerjee, C. Peikert, and A. Rosen. Pseudorandom functions and lattices. In Pointcheval and Johansson [39], pages 719–737.
7. S. Bhattacharya, O. Garcia-Morchon, T. Laarhoven, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, and Z. Zhang. Round5: Compact and fast post-quantum public-key encryption. *IACR Cryptology ePrint Archive*, 2018:725, 2018.

8. A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen. On the hardness of learning with rounding over small modulus. In E. Kushilevitz and T. Malkin, editors, *TCC 2016-A, Part I*, volume 9562 of *LNCS*, pages 209–224. Springer, Heidelberg, Jan. 2016.
9. M. Bolboceanu, Z. Brakerski, R. Perlman, and D. Sharma. Order-LWE and the hardness of ring-LWE with entropic secrets. In *ASIACRYPT 2019, Part II*, LNCS, pages 91–120. Springer, Heidelberg, Dec. 2019.
10. Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In D. Boneh, T. Roughgarden, and J. Feigenbaum, editors, *45th ACM STOC*, pages 575–584. ACM Press, June 2013.
11. W. Castryck, I. Iliashenko, and F. Vercauteren. Provably weak instances of ring-LWE revisited. In M. Fischlin and J.-S. Coron, editors, *EUROCRYPT 2016, Part I*, volume 9665 of *LNCS*, pages 147–167. Springer, Heidelberg, May 2016.
12. H. Chen, K. Lauter, and K. E. Stange. Attacks on search rlwe. 2015.
13. H. Chen, K. E. Lauter, and K. E. Stange. Vulnerable galois rlwe families and improved attacks. *IACR Cryptology ePrint Archive*, 2016:193, 2016.
14. L. Chen, Z. Zhang, and Z. Zhang. On the hardness of the computational ring-LWR problem and its applications. In *ASIACRYPT 2018, Part I*, LNCS, pages 435–464. Springer, Heidelberg, Dec. 2018.
15. K. Conrad. The different ideal. Expository papers. Available at: `https://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf`.
16. K. Conrad. Factoring ideals after dedekind. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf`.
17. D. Dachman-Soled, H. Gong, M. Kulkarni, and A. Shahverdi. Partial key exposure in ring-lwe-based cryptosystems: Attacks and resilience. *IACR Cryptology ePrint Archive*, 2018:1068, 2018.
18. J.-P. D'Anvers, A. Karmakar, S. Sinha Roy, and F. Vercauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem. In A. Joux, A. Nitaj, and T. Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2018*, pages 282–305, Cham, 2018. Springer International Publishing.
19. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM journal on computing*, 38(1):97–139, 2008.
20. K. Eisenträger, S. Hallgren, and K. Lauter. Weak instances of plwe. In *International Conference on Selected Areas in Cryptography*, pages 183–194. Springer, 2014.
21. Y. Elias, K. E. Lauter, E. Ozman, and K. E. Stange. Provably weak instances of ring-LWE. In R. Gennaro and M. J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 63–92. Springer, Heidelberg, Aug. 2015.
22. A. Fröhlich. A normal integral basis theorem. *Journal of Algebra*, 39(1):131–137, 1976.
23. N. Genise and D. Micciancio. Faster Gaussian sampling for trapdoor lattices with arbitrary modulus. In Nielsen and Rijmen [32], pages 174–203.
24. N. Genise, D. Micciancio, and Y. Polyakov. Building an efficient lattice gadget toolkit: Subgaussian sampling and more. In V. Rijmen and Y. Ishai, editors, *EUROCRYPT 2019, Part II*, LNCS, pages 655–684. Springer, Heidelberg, May 2019.
25. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.

26. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Heidelberg, May / June 2010.
27. V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-LWE cryptography. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 35–54. Springer, Heidelberg, May 2013.
28. D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *43rd FOCS*, pages 356–365. IEEE Computer Society Press, Nov. 2002.
29. D. Micciancio and P. Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In P. Rogaway, editor, *CRYPTO 2011*, volume 6841 of *LNCS*, pages 465–484. Springer, Heidelberg, Aug. 2011.
30. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, s-maller. In Pointcheval and Johansson [39], pages 700–718.
31. D. Micciancio and M. Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 455–485. Springer, Heidelberg, Aug. 2017.
32. J. B. Nielsen and V. Rijmen, editors. *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*. Springer, Heidelberg, Apr. / May 2018.
33. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In M. Mitzenmacher, editor, *41st ACM STOC*, pages 333–342. ACM Press, May / June 2009.
34. C. Peikert. An efficient and parallel Gaussian sampler for lattices. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 80–97. Springer, Heidelberg, Aug. 2010.
35. C. Peikert. How (not) to instantiate ring-lwe. In *International Conference on Security and Cryptography for Networks*, pages 411–430. Springer, 2016.
36. C. Peikert et al. A decade of lattice cryptography. *Foundations and Trends® in Theoretical Computer Science*, 10(4):283–424, 2016.
37. C. Peikert and Z. Pepin. Algebraically structured LWE, revisited. In *TCC 2019, Part I*, LNCS, pages 1–23. Springer, Heidelberg, Mar. 2019.
38. C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of ring-LWE for any ring and modulus. In H. Hatami, P. McKenzie, and V. King, editors, *49th ACM STOC*, pages 461–473. ACM Press, June 2017.
39. D. Pointcheval and T. Johansson, editors. *EUROCRYPT 2012*, volume 7237 of *LNCS*. Springer, Heidelberg, Apr. 2012.
40. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.
41. M. Rosca, D. Stehlé, and A. Wallet. On the ring-LWE and polynomial-LWE problems. In Nielsen and Rijmen [32], pages 146–173.
42. P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th FOCS*, pages 124–134. IEEE Computer Society Press, Nov. 1994.
43. S. Tessaro. Security amplification for the cascade of arbitrarily weak PRPs: Tight bounds via the interactive hardcore lemma. In Y. Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 37–54. Springer, Heidelberg, Mar. 2011.
44. W.Stein. *A brief introduction to classical and adelic algrbraic number theory*. 2004. `https://modular.math.washington.edu/papers/ant/`, last accessed 12 Otc 2009.