On the Hardness of Ring/Module/Polynomial LWR Problems

Yang Wang[1,2]✉[0000−0001−9274−8195], Yanmin Zhao[3]✉, and Mingqiang Wang[1,2]✉

[1] School of Mathematics, Shandong University, Jinan, Shandong, 250100, P.R. China
[2] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, Shandong, 250100, P.R. China
[3] Department of Computer Science, The University of Hong Kong, P.R. China
wyang1114@sdu.edu.cn
wangmingqiang@sdu.edu.cn
ymzhao@cs.hku.hk

Abstract. The Learning with Rounding (LWR) problem is an important variant of the Learning with Errors (LWE) problem. Recently, Liu *et al.* proposed a comprehensive study of LWR problems defined over algebraic number fields in CRYPTO 2020. However, their search-to-decision reductions of LWR problems depend heavily on the existence of the so-called *Normal Integral Basis* (NIB). Meanwhile, the aesthetic deficiency is a lack of discussions of choices of secret s, and one may could not show the *worst-case* hardness of decision LWR problems *strictly* even for fields with NIB. In this paper, we give a more refined analysis of reductions between different LWR problems. Our contributions are summarized as follows: (1) We give a search-to-decision reduction of ring/module LWR problems defined over *any* number field $K = \mathbb{Q}[x]/(\Phi(x))$ which is *Galois* over $\mathbb{Q}$ with suitable parameters, *regardless of the existence of NIB*. (2) To the best of our knowledge, we give the first reduction from search ring/module LWE problems to corresponding search/decision LWR problems. Hence, combining known hardness results of LWE problems, we could reduce *worst-case* ideal/module lattices problems to search/decsion LWR problems *strictly*. (3) For the first time, we show the *worst-case* hardness of search/decision polynomial LWR problems defined over polynomial rings $\mathbb{Z}_q[x]/(\Phi(x))$ with *comparable small parameters*, which could be regarded as a theoretical support for some ring/module LWR based crypto-systems, e.g. the NIST Round 3 candidate - Saber. As a finish, we also give some hardness results of middle product polynomial LWR problems.

Keywords: Lattice-based Cryptography · Ring/Module LWR Problems · Polynomial LWR Problems · Hardness Reduction

1 Introduction

Cryptographic primitives based on hard lattice problems play a key role in the area of post-quantum cryptographic researches, due to their abilities of

resisting attacks by quantum computers [28] and their versatility. Till now, we could design almost all crypto-primitives based on hard lattices problems [22], and some of them are very closed to practical applications [10, 15, 16]. In the final round competitions (Round 3) of post-quantum cryptography standardization called by NIST, 7 out of 15 candidates are lattice-based.

The Learning with Rounding problem was first proposed by Banerjee *et al.* in [8], and was used as a building block in constructing efficient, low-depth pseudo-random functions. Later, there have been a number of further applications [4, 5, 7, 15, 17]. LWR could be regarded as a "deterministic" LWE without sampling error e, thereby enjoying the advantage that, e is usually sampled from some discrete Gaussians, and such sampling procedure is in general costly, difficult to implement and vulnerable to side-channel attacks. In [8], Banerjee *et al.* showed a reduction from LWE to LWR (including its ring variant) with arbitrarily many samples. However, this reduction requires the modulus q to be at least super-polynomial. Alwen *et al.* [4] reduced the modulus q to polynomial sizes by imposing some certain number theoretical restrictions on it. Later, Bogdanov *et al.* removed the number theoretical restrictions on modulus q, and provide new search-to-decision reduction of LWR problems over Euclidean lattices by using Rényi divergence and the tool called learning heavy Fourier coefficients in [9]. Alperin-Sheriff *et al.* [3] further improved the parameter sets for reductions from LWE to LWR. In particular, their reduction is dimension-preserving with a polynomial-sized modulus.

The above hardness results of LWR problems with polynomial bounded parameters are all limited in Euclidean lattices. While practical lattice-based crypto-systems are usually designed over ring/module LWR problems [5, 15]. To overcome the lack of provably hardness for decisional ring/nodule LWR problems, computational learning with rounding over rings assumption are proposed [6, 12]. However, the relations between computational LWR problems and decisional Ring/Module LWR problems remain unclear, and it seems that decisional LWR problems are much more powerful in many applications.

In CRYPTO 2020, Liu *et al.* [19] conducted a comprehensive study on establishing hardness reductions for Ring/Module LWR problems. Their results confirmed that similar algebraic framework as LWE proposed in [23] also fits to LWR problems. They also give the first search-to-decision reduction of Ring/Module LWR problems by using a similar route as Ring/Module LWE problems [18, 20]. Ring/module LWR problems with leaky secrets are also considered. Both negative results of ring LWR and positive results of module LWR are given. However, their search-to-decision reductions of Ring/Module LWR problems rely heavily on the existence of normal integral basis of number field K. Also, their reduction only works for some special set of secret s, which is only a negligible part of $\mathcal{O}_k^\vee/q\mathcal{O}_K^\vee$ [4]. As a result, we could not deduce a *strictly* worst-case to average-case reductions from worst-case ideal/module lattice problems to decisional LWR problems by simply combining reductions form search LWE problems to search LWR problems and reductions from search LWR problems to decisional LWR

[4] Here, $\mathcal{O}_K^\vee$ is the dual of the ring of integers R of a number field K.

problems. Finally, whether similar reductions and hardness results can be extended to polynomial LWR problems is still open. Since it is more natural and convenient to use polynomial rings in applications, we believe that it's meaningful and instructive to investigate hardness reductions of polynomial LWR problems, as well.

1.1 Our Contributions

In this paper, we make a detailed analysis of reductions between Ring/Module LWR problems and Polynomial LWR problems.

We give a search-to-decision reduction of Ring/Moulde LWR problems over any number filed $K = \mathbb{Q}[x]/(\Phi(x))$ which is Galois over $\mathbb{Q}$, regardless of the existence of NIB. More precisely, we also use rounding functions with respect to some basis B to define LWR problems, but our reductions do not depend on the basis we use. So, under some necessary conditions, our results show that if search ring/module LWR problems are one-way with respected to some basis B, then decision ring/module LWR problems are pseudo-random with respected to the same basis.

We then give an efficient attack for search ring/module LWR problems with secrets in some special sets (which cover the cases proposed in [19]). By combining this attack, reductions from search ring/module LWE problems to search ring/module LWR problems with secrets in $(R_q^\vee)^\times$ [5], a proper intermediate problem which we called extended search ring/modul LWR problems, and our search-to-decision reduction of Ring/Moulde LWR problems, we propose reductions from search ring/module LWE problems, hence worst-case ideal/module lattices problems, to decision ring/module LWR problems with secrets in $(R_q^\vee)^\times$.

For the first time we prove the hardness of search/decision polynomial LWR problems defined over any polynomial ring $\mathbb{Z}[x]/(\Phi(x))$, as long as the corresponding filed $K = \mathbb{Q}[x]/(\Phi(x))$ is Galois over $\mathbb{Q}$. For suitable modulus q, we first give an isomorphism $\mathbb{Z}_q[x]/(\Phi(x)) \cong R_q^\vee$, then show the equivalences between search/decision polynomial LWR problems and corresponding LWR problems (with respect to some $\mathbb{Z}_q$ basis). These, combining our reductions from search ring/module LWE problems to search ring/module LWR problems, give connections between search ring/module LWE problems and search/decision polynomial LWR problems with comparable small parameters. For example, if $K = \mathbb{Q}(\zeta_l)$ is power-of-2 cyclotomic field and the number of samples $L = \tilde{O}(1)$, we could get a reduction from worst-case $\mathrm{SIVP}_{\tilde{O}(n^{\frac{9}{4}})}$ to search polynomial LWR problems with modulus $q \approx \tilde{O}(n^2)$. We also give some results (maybe not very satisfactory) about hardness of decision middle-product polynomial LWR problems.

[5] Here, $R = \mathcal{O}_K$ is the ring of integers of K, $R^\vee$ is the dual fractional ideal of R, $R_q^\vee = R^\vee/qR^\vee$, and $(R_q^\vee)^\times$ denotes the subset of $R_q^\vee$ consisting of R-invertible elements via the R-module isomorphism $R_q \cong R_q^\vee$.

1.2 Technique Overviews

For simplicity, we set $K = \mathbb{Q}[x]/(\Phi(x)) = \mathbb{Q}(\zeta)$ to be a Galois extension over $\mathbb{Q}$ with dimension n, $R = \mathcal{O}_K$ and take ring LWR problems as examples. Assume B is a set of basis, we also define the rounding function $\lfloor \rceil_{B,q,p}$ for some modulus $q = p \cdot Q$ [6] with respect to $B = (b_1, \cdots, b_n)$: $\lfloor a \rceil_{B,q,p} = \sum_{i=1}^{n} \lfloor a_i \rceil_{q,p} \cdot b_i$, where $a = \sum_{i=1}^{n} a_i \cdot b_i$ and $\lfloor x \rceil_{q,p} = \lfloor \frac{p}{q} \cdot x \rceil$. Assume further p, Q are different primes and $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_{\mathfrak{g}}$ with $\mathfrak{g} = \Omega(n)$. An instance of ring LWR problems with respect to basis B is of the form $(a, b = \lfloor a \cdot s \rceil_{B,q,p})$ for some fixed secret s. Recall that, the search-to-decision reduction road-map of [19] is as following:

$$\text{S-LWR} \mapsto \ \mathfrak{p}_i\text{-S-LWR} \mapsto \ \text{W-D-LWR}^i \mapsto \ \text{D-LWR},$$

which is also used in [18, 20] for proving the pseudo-randomness of ring/module LWE problems. For some $s \in R_q^\vee$, the $\mathfrak{p}_i$-S-LWR problem is to find $s \bmod \mathfrak{p}_i^\vee$, and the W-D-LWR^i problem is to distinguish $(a, \lfloor a \cdot s \rceil_{B,q,p} + h_{i-1})$ and $(a, \lfloor a \cdot s \rceil_{B,q,p} + h_i)$, where h_i is sampled uniformly at random modulo $\mathfrak{p}_j$ for $j \in \{1, \cdots, i-1\}$ and is 0 modulo $\mathfrak{p}_j$ for $j \in \{i, \cdots, \mathfrak{g}\}$. The main thoughts can be summarized as follows. Since $K/\mathbb{Q}$ is Galois, actions of element σ_i in the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ are transitive on the set $\{\mathfrak{p}_1, \cdots, \mathfrak{p}_{\mathfrak{g}}\}$. To solve $\mathfrak{p}_j$-S-LWR problem, one could transfer instance (a, b) to $(\sigma_{j,i}(a), \sigma_{j,i}(b))$, and use the $\mathfrak{p}_i$-S-LWR oracle to find solution $\sigma_{j,i}(s) \bmod \mathfrak{p}_i R^\vee$, then $\sigma_{i,j}(\sigma_{j,i}(s))$ is the required solution. Here, $\sigma_{j,i}(\mathfrak{p}_j) = \mathfrak{p}_i$. Via the Chinese Remainder Theorem (CRT), one could recover $s \bmod pR^\vee$. The reason why we need NIB is that we have

$$\sigma_i(\lfloor a \cdot s \rceil)_{B,q,p} = \lfloor \sigma_i(a) \cdot \sigma_i(s) \rceil_{\sigma_i(B),q,p} \tag{1}$$

for any $\sigma_i \in \mathrm{Gal(K/\mathbb{Q})}$. Since we only assume the oracle has ability to find s with respect to B, we must require $\sigma_i(B) = B$. Meanwhile, we could only recover $b \bmod pR^\vee$ by using the above method. For modulus $p|q$, there are $(\frac{q}{p})^n$ many possible elements in $R_q^\vee$ correspond to the same $s \bmod pR^\vee$. So the authors of [19] choose to restrict $s \in R_p^\vee$.

For simplicity, we assume all the problems, except D-LWR, are worst-case in the sense that $\mathfrak{O}$ should solve corresponding problem with probability ≈ 1. Reductions from $\mathfrak{p}_i$-S-LWR to W-D-LWR^i could be done via transferring (a, b) to $(a + \frac{q}{p}y, b + h + x \cdot y)$ with suitable h, y by trying all the possible $x \in R^\vee/\mathfrak{p}_i R^\vee$ if we require p to split "well" in the sense that $N(\mathfrak{p}_i) \leq \mathrm{Poly}(n)$. Reductions from W-D-LWR^i to D-LWR can be divided into two parts: a reduction from W-D-LWR^i to worst-case D-LWR through a standard hybrid discussion, and a reduction from worst-case D-LWR to D-LWR by using the secret re-randomizing technique and a similar analysis proposed in [25]. The secret re-randomizing technique needs to require s to be invertible, so authors of [19] choose to restrict the secret s in the set $R_p^\vee \cap (R_q^\vee)^\times$.

Choices of Secret Sets: Elements of $R_p^\vee$ are different form those of $R_q^\vee$ (since they are different cosets in mathematics). The published version of [19] does

[6] Condition $p|q$ seems to be a common requirement [4, 6, 9, 12, 19].

not specify the formal definition of the set $R_p^\vee \cap (R_q^\vee)^\times$, while the full version seems to be unavailable now. We note that assume $q = Q \cdot p$ with $\gcd(p, Q) = 1$, which is also the parameter set used in [19], we have $R_q^\vee \cong R_Q^\vee \times R_p^\vee$ by CRT. If we identity elements of $R_p^\vee$ via this isomorphism, then $R_p^\vee \cap (R_q^\vee)^\times$ is an empty set, since any invertible element a of $R_q^\vee$ must satisfy $a \neq 0 \bmod QR^\vee$ and $a \neq 0 \bmod pR^\vee$. We choose to constrain s in the set

$$(R_q^\vee \cap R_p^\vee)^\times := \{x \in R_q^\vee : x = 0 \bmod Q \cdot R^\vee, x \neq 0 \bmod \mathfrak{p}_i \cdot R^\vee \text{ for all } i \in [\mathfrak{g}]\}$$

remove the need of NIB in the search-to-decision reduction of LWR problems first. Then, we discuss how to give similar reduction with secret set $(R_q^\vee)^\times$.

Removing dependence of NIB: Both sets $(R_q^\vee \cap R_p^\vee)^\times$ and $(R_q^\vee)^\times$ is σ_i-invariant for all $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$. To get rid of the dependence of NIB, a *vital observation* is that solving (both search and decisional, worst-case and average-case) LWR problems with respect to basis B is equivalent to solving LWR problems with respect to *any* basis B' in the set $\mathcal{S}_B := \{\sigma_i(B) : \sigma_i \in \mathrm{Gal}(K/\mathbb{Q})\}$. This follows easily from equation (1) and the fact σ_i do not change the distribution of s, when s obeys to the uniform distribution over $(R_q^\vee \cap R_p^\vee)^\times$. Therefore, we could use the following reduction road-map:

$$\text{S-LWR} \;\mapsto\; \mathfrak{p}_i\text{-S-LWR}_{\mathcal{S}_B} \mapsto\; \text{W-D-LWR}^i_{\mathcal{S}_B} \mapsto\; \text{D-LWR}.$$

Here, symbol $\mathcal{S}_B$ represents that we require the oracle $\mathfrak{O}$ to solve corresponding problems with respect to any basis in $\mathcal{S}_B$. Then, S-LWR could be reduced to $\mathfrak{p}_i$-S-LWR$_{\mathcal{S}_B}$ for *arbitrary* basis B, as we have "enhance" the ability of corresponding oracles.

Notice that remaining reductions are basis-preserving. The above *vital observation* is used in the reduction form W-D-LWR$^i_{\mathcal{S}_B}$ to worst-case D-LWR, since the "enhanced" ability is just the original ability of the worst-case D-LWR solver $\mathfrak{O}$. In fact, we do not add any additional requirements on corresponding $\mathfrak{O}$.

Attacks on LWR problems with secrets in $(R_q^\vee \cap R_p^\vee)^\times$: A natural question is that if we could reduce search LWE problems to search LWR problems with these special secrets by using a R*é*nyi divergence argument as before? Though one may deduce the hardness results of search LWE problems with secrets in $(R_q^\vee \cap R_p^\vee)^\times$ via a similar discussion as in [20], the resulted parameters are too large and we can't reduce search LWE problems to search LWR problems with these special secrets. In fact, though the number of secret in $(R_q^\vee \cap R_p^\vee)^\times$ is exponential, LWR problems with these parameter settings are easy to solve.

Assume $r_1, r_2 \in \mathbb{Z}_q$ are the "CRT basis" of the isomorphism $\mathbb{Z}_q \cong \mathbb{Z}_Q \times \mathbb{Z}_p$, i.e. $a = r_1 \cdot a_1 + r_2 \cdot a_2$ for $a \in \mathbb{Z}_q, a_1 \in \mathbb{Z}_Q$ and $a_2 \in \mathbb{Z}_p$. Since $\mathbb{Z} \subseteq R \subseteq R^\vee$, we could represent $a \in R_q$ and $s \in R_q^\vee$ via r_1 and r_2 as following: $a = r_1 \cdot a_1 + r_2 \cdot a_2$ and $s = r_1 \cdot s_1 + r_2 \cdot s_2$ for $a \in R_q, s \in R_q^\vee$ and $a_1 \in R_Q, a_2 \in R_p, s_1 \in R_Q^\vee, s_2 \in R_p^\vee$. Then, elements in $(R_q^\vee \cap R_p^\vee)^\times$ correspond to the cases $s_1 = 0$ and $s_2 \in (R_p^\vee)^\times$. For any $a = r_1 \cdot a_1 + r_2 \cdot a_2$ and $s = r_2 \cdot s_2$ and any basis B, we have $b = \lfloor a \cdot s \rceil_{B,q,p} = Q_p^{-1} \cdot a_2 \cdot s_2$ (see Lemma 7), where Q_p^{-1} is the integer such

that $r_2 = Q \cdot Q_p^{-1} \bmod q$. Since $a_2 \in R_p^\times$ with high probability, we could solve $s_2 \in R_p^\vee$ and recover $s = r_2 \cdot s_2 \bmod qR^\vee$ easily.

This simple attack also means that for $q = p \cdot Q$ with $\gcd(p, Q) = 1$, when given samples of the form $(a, \lfloor a \cdot s \rceil_{B,q,p})$, the secret $s := r_1 \cdot s_1 + r_2 \cdot s_2 \in R_q^\vee$ should at least be chosen from some subset of $R_q^\vee$ with the s_1-component having enough entropy. Otherwise, the corresponding search LWR problems are easy.

Worst-Case Hardness of LWR Problems: To show the worst-case hardness of decision LWR problems, we choose secret set to be $R_q^\vee$. If so, how to recover the whole s, not just $s \bmod pR^\vee$ is the biggest obstacle. To overcome this, we define the extended search LWR problem (denoted by Ext-S-LWR), whose instance is of the form $(a_1, a_2, \lfloor a_1 \cdot s \rceil_{B,q,Q}, \lfloor a_2 \cdot s \rceil_{B,q,p})$, as an intermediate problem. Next, we define the weak search LWR problems, denoted by Weak-S-LWR, in which we only require to recover $s \bmod pR^\vee$ when given $(a, \lfloor a \cdot s \rceil_{B,q,p})$. Then, if one could solve Weak-S-LWR problem, we could use the recovered $s_2 := s \bmod pR^\vee$, partial information $(a_1, \lfloor a_1 \cdot s \rceil_{B,q,Q})$ and similar algorithm as the above attack to recover full $s \bmod qR^\vee$ and solve Ext-S-LWR problem.

The reason we choose to define Ext-S-LWR problem as $(a_1, a_2, \lfloor a_1 \cdot s \rceil_{B,q,Q}, \lfloor a_2 \cdot s \rceil_{B,q,p})$, not the seemed more natural form $(a, \lfloor a \cdot s \rceil_{B,q,Q}, \lfloor a \cdot s \rceil_{B,q,p})$, is that we could easily bound the Rényi distance between two LWE samples $(a_1, a_2, a_1 \cdot s + e_1, a_2 \cdot s + e_2)$ and one Ext-S-LWR sample $(a_1, a_2, \lfloor a_1 \cdot s \rceil_{B,q,Q}, \lfloor a_2 \cdot s \rceil_{B,q,p})$ due to the somewhat independent of $a_1 \cdot s$ and $a_2 \cdot s$. Hardness of Ext-S-LWR could be guaranteed by search LWE problem, and our search-to-decision reductions could be modified to this situation. These gives a reduction from search LWE problem to decision LWR problem.

Connecting Polynomial LWR and Ring LWR: Similar to LWE problems [27], we could also define polynomial/primal/dula LWR problems wit secrets in $\mathbb{Z}_q[x]/(\Phi(x)), R_q, R_q^\vee$. To relate these LWR problems, a *crucial observation* is that the rounding function we use also transfers basis of $R_q^\vee$ to basis $R_p^\vee$ (from $B \bmod qR^\vee$ to $B \bmod pR^\vee$) implicitly. We could regard it as a $\mathbb{Z}$-module homomorphism. Meanwhile, the above search-to-decision reduction also works for any $\mathbb{Z}_q$-basis B of $R_q^\vee$, since by CRT, $B \bmod pR^\vee$ is a $\mathbb{Z}_p$-basis of $R_p^\vee$.

To connect Polynomial LWR problem and Ring LWR problem, our techniques are as follows:

(1) The isomorphism $\varphi_{R,R^\vee} : R_q \cong R_q^\vee$ and its inverse (which is denoted by $\varphi_{R^\vee,R}$) are also $\mathbb{Z}$-module isomorphisms, since $\mathbb{Z} \subseteq R$. Then, the primal LWR problem with respect to some $\mathbb{Z}_q$-basis B is equivalent to the (dual) LWR problem with respect to $\mathbb{Z}_q$ basis $\varphi_{R,R^\vee}(B)$. That is to say, there is a correspondence between primal LWR problem and LWR problems via $\mathbb{Z}_q$ basis.

(2) For prime modulus p such that $p \nmid \Delta_k$ and $p \nmid |R/\mathbb{Z}[\zeta]|$, we have a ring isomorphism $\varphi_{p,R} : \mathbb{Z}_p[x]/(\Phi(x)) \cong R_p$ via the sequence of isomorphism $\mathbb{Z}_p[x]/(\Phi(x)) \cong \mathbb{Z}_p[x]/(\Phi_1(x)) \times \cdots \times \mathbb{Z}_p[x]/(\Phi_{\mathfrak{g}}(x)) \cong \mathbb{Z}[x]/(p, \Phi_1(x)) \times \cdots \times \mathbb{Z}[x]/(p, \Phi_{\mathfrak{g}}(x)) \cong R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_{\mathfrak{g}} \cong R_p$, where $\Phi(x) = \Phi_1(x) \cdots \Phi_{\mathfrak{g}}(x) \bmod p$. Then, if $q = Q \cdot p$ with p, Q different primes such that $\gcd(q, \Delta_k) = 1$ and $\gcd(q, |R/\mathbb{Z}[\zeta]|) = 1$, R_q admits a $\mathbb{Z}_q$ power basis, namely $\bar{\zeta} := \varphi_{q,R}(x \bmod \Phi(x) \cdot \mathbb{Z}_q[x])$. Meanwhile, the ring isomorphism $\varphi_{q,R}$ is also a $\mathbb{Z}$-module, since each component appeared in

the sequence of isomorphism is a $\mathbb{Z}$-module. Then, we could show that Polynomial LWR problem is equivalent to primal LWR problem with respect to basis $B := \{1, \bar{\zeta}, \cdots, \bar{\zeta}^{n-1}\}$ (hence is equivalent to LWR problem with respect to basis $B' = \varphi_{R,R^\vee}(B)$).

Combining our reductions from S-LWE problem to D-LWR problem with respect to $\mathbb{Z}_q$ basis $B' = \varphi_{R,R^\vee}(B)$, we could show the hardness of polynomial LWR problems. For cyclotomic field $K = \mathbb{Q}(\zeta_l) = \mathbb{Q}[x]/(\Phi_l(x))$ with $\zeta_l = e^{2\pi \boldsymbol{i} \cdot \frac{1}{l}}$, one could get reduction from S-LWE problems to polynomial LWR problems directly without using facts showed in **(2)**. However, parameters depend on the $\mathbb{Z}_q$ basis we use. A good choice for cyclotomic fields is the decoding basis of $R^\vee$ and the powerful basis of R [21]. Only for l to be a prime-power, the usual power basis B of R equals to its powerful basis, and the decoding basis does not equal to $\varphi_{R,R^\vee}(B)$. So, to save loss of parameters, we first show a compact reduction from S-LWE problem to primal-S-LWE problem for cyclotomic field. Then, we could apply our discussions to primal variant S-LWE/Ext-S-LWR/Weak-S-LWR problems, and get a tight hardness result of polynomial LWR problem defined over polynomial ring $\mathbb{Z}_q[x]/(\Phi_l(x))$ with l a prime-power.

1.3 Organizations

We will introduce some useful definitions and results in Section 2. Search-to-decision reductions of Ring/Module LWR problems are put in Section 3. We will discuss the worst-case hardness of (extended) Ring/Module LWR problems in Section 4. Hardness of polynomial LWR problems, as well as some results about middle-product polynomial LWR problems, is discussed in Section 5

2 Preliminaries

Throughout this paper, symbol $[n]$ represents the set $\{1, \cdots, n\}$ for any positive integer n. When we write $X \hookleftarrow \xi$, we mean the random variable X obeys to the distribution ξ. For a finite set S, we will use $|S|$ to denote its cardinality and $U(S)$ to denote the uniform distribution over S. For two positive integers $p \leq q$, we define $\lfloor \cdot \rceil_{q,p} : \mathbb{Z}_q \mapsto \mathbb{Z}_p$ by $\lfloor x \rceil_{q,p} = \lfloor \frac{p}{q} \cdot x \rceil$. We will use column vectors by default, unless specified. For a matrix $M \in \mathbb{R}^{n \times n}$, we use $\mathfrak{s}_1(M) \geq \cdots \geq \mathfrak{s}_n(M)$ to represent its singular values.

2.1 Number Fields and Lattices

We consider number field $K = \mathbb{Q}(\zeta) \cong \mathbb{Q}[x]/(\Phi(x))$, which is Galois over $\mathbb{Q}$. Here, $\Phi(x) \in \mathbb{Q}[x]$ is the "defining polynomial" of K, it is also the minimum polynomial of ζ. Assume $[K : \mathbb{Q}] = n := \mathfrak{r}_1 + 2\mathfrak{r}_2$ for some positive integers $\mathfrak{r}_1, \mathfrak{r}_2$ (for Galois extensions, either $\mathfrak{r}_1$ or $\mathfrak{r}_2$ is zero), there are n embeddings $\{\sigma_i\}$'s, which are also $\mathbb{Q}$-isomorphism of K, from K to $\mathbb{C}$. We set $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i : i = 1, \cdots, n\}$ and use the canonical embedding σ on K, who maps $x \in K$ to $(\sigma_1(x), \cdots, \sigma_n(x)) \in H$, where $H = \{(x_1, \cdots, x_n) \in \mathbb{R}^{\mathfrak{r}_1} \times \mathbb{C}^{2\mathfrak{r}_2} : \ x_{n+1-i} =$

$\overline{x_{\mathfrak{r}_1+i}},\ \forall i \in [\mathfrak{r}_2]\}$. The space H is isomorphic to $\mathbb{R}^n$ as an $\mathbb{R}$ vector space [20, 30]. As usual, we set $R := \mathcal{O}$ to be the ring of integers of K. The discriminant of K is defined as $\Delta_K = \det((\sigma_i(\alpha_j))_{1\le i,j\le n})^2$, where $\{\alpha_i\}$'s is any basis of R. A lattice is defined as a discrete additive subgroup of H. The dual lattice of $\Lambda \subseteq H$ is defined as $\Lambda^\vee = \{\boldsymbol{y} \in H :\ \forall\ \boldsymbol{x} \in \Lambda,\ < \boldsymbol{x}, \overline{\boldsymbol{y}} >= \sum_{i=1}^n x_i \cdot y_i \in \mathbb{Z}\}$. An integral ideal $I \subseteq R$ is a usual ideal defined in the ring R, and a fractional ideal $J \subseteq K$ is a set such that $dJ \subseteq R$ is an integral ideal for some $d \in R$. It is well known that both I and J admit $\mathbb{Z}$-basis and we can require $d \in \mathbb{Z}$. So, for any (fractional) ideal I, $\sigma(I)$ is a lattice of H. The dual of I is defined as $I^\vee = \{a \in K :\ \mathrm{Tr}(a \cdot I) \subseteq \mathbb{Z}\}$, where $\mathrm{Tr}(a) = \sum_{i=1}^n \sigma_i(a)$ and $\mathrm{N}(a) = \prod_{i=1}^n \sigma_i(a)$ for $a \in K$. The norm of an integral ideal I is defined as $N(I) = |R/I|$.

For any rational prime q, we have prime ideal decomposition $qR = \mathfrak{q}_1^{\mathfrak{e}} \cdots \mathfrak{q}_{\mathfrak{g}}^{\mathfrak{e}}$ with positive integers $\mathfrak{e} \cdot \mathfrak{f} \cdot \mathfrak{g} = n$. Here, $N(\mathfrak{q}_i) = q^{\mathfrak{f}}$ for $i \in [n]$. For our discussions, we say a prime q is split-well, if $\gcd(q, \Delta_K) = 1$ (i.e. $\mathfrak{e} = 1$, prime q is non-ramified) and $\mathrm{N}(\mathfrak{q}) = q^{\mathfrak{f}} \le \mathrm{poly}(n)$. For any modulus q, there is an efficiently computable R module isomorphism $\varphi_{R,R^\vee} : R_q \cong R_q^\vee$ [20, Lemma 2.15]. We define $R_q^\times$ to be the set consisting of invertible elements (under multiplication) of R_q. Though $R_q^\vee$ is not a ring, we could define the set $(R_q^\vee)^\times$ as $\{s \in R_q^\vee :\ \exists\ a \in R_q,\ \text{s.t. } a \cdot s = 1 \bmod qR^\vee\}$. Then, we have $\varphi_{R,R^\vee}(R_q^\times) = (R_q^\vee)^\times$.

For any $s > 0$, $\boldsymbol{c} \in H$, which is taken to be $s = 1$ or $\boldsymbol{c} = 0$ when omitted, define the (spherical) Gaussian function $\rho_{s,\boldsymbol{c}} : H \to (0, 1]$ as $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) = e^{-\pi \frac{||\boldsymbol{x}-\boldsymbol{c}||^2}{s^2}}$. By normalizing this function, we obtain the continuous Gaussian probability distribution $D_{s,\boldsymbol{c}}$ of parameter s, whose density function is given by $s^{-n} \cdot \rho_{s,\boldsymbol{c}}(\boldsymbol{x})$.

2.2 Definition of LWR/LWE Problems

Let's recall the definition of the (dual) Ring/Module LWR problems [19].

Definition 1. *Let $K = \mathbb{Q}(\zeta)$ be a number field with $[K : \mathbb{Q}] = n$, $R = \mathcal{O}_K$, $q \ge p \ge 2$ be two integers, $M = R^d$ with d a positive integer, $B = (b_1, \cdots, b_n)$ be some basis of $R^\vee$ and χ be some distribution over $R_q^\vee$.*

- *The rounding function $\lfloor \cdot \rceil_{B,q,p} : R_q^\vee \mapsto R_p^\vee$ with respect to basis B is defined as $\lfloor a \rceil_{B,q,p} = \sum_{i=1}^n \lfloor a_i \rceil_{q,p} \cdot b_i \in R_p^\vee$ for $a = \sum_{i=1}^n a_i \cdot b_i \in R_q^\vee$.*
- *For $\boldsymbol{s} := (s_1, \cdots, s_d)^T \in (R_q^\vee)^d$, we define the* LWR *distribution with respect to basis B as $A_{q,p,\boldsymbol{s}}^M(B)$ obtained by sampling $\boldsymbol{a} := (a_1, \cdots, a_d)^T \hookleftarrow U(R_q^d)$ and returning the pair $(\boldsymbol{a}, b = \lfloor \sum_{i=1}^d a_i \cdot s_i \bmod qR^\vee \rceil_{B,q,p}) \in R_q^d \times R_p^\vee$.*
- *The search LWR problem with respect to basis B, denoted by $\text{S-LWR}_{B,q,p,\chi}^M$, consists in finding $\boldsymbol{s}$ with a polynomial number of samples sampled from $A_{q,p,\boldsymbol{s}}^M(B)$ for some arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi^d) \subseteq (R_q^\vee)^d$.*
- *The decision LWR problem with respect to basis B, denoted by $\text{D-LWR}_{B,q,p,\chi}^M$, consists in distinguishing a polynomial number of samples, which are sampled either from $A_{q,p,\boldsymbol{s}}^M(B)$ or from $U(R_q^d \times R_p^\vee)$, with non-negligible probability for $\boldsymbol{s} = (s_1, \cdots, s_d)^T \hookleftarrow \chi^d$.*

We remark that for some special modulus p and q (e.g. $p|Q$), it is possible to change B to some $\mathbb{Z}_q$ basis of $R_q^\vee$ in Definition 1. For $d = 1$, we get the Ring-LWR problems. While $d \geq 2$ corresponds to Module-LWR problems. The definition of search variant LWR problems is worst-case in the sense that we require $\boldsymbol{s}$ to be arbitrary in some set, and usually require to solve corresponding problems with probability ≈ 1. While, the decision variants could be regarded as average-case, since we just require $\boldsymbol{s}$ to obey some distributions (usually, $\boldsymbol{s} \hookleftarrow U((R_q^\vee)^d)$, i.e. $\chi = U(R_q^\vee)$) and require to solve corresponding problems with non-negligible probability. Definitions of LWR problems are first formalized in [19], and are closely related to the basis we used.

We will also use the primal LWR problems, which could be regarded as the counterpart of primal LWE problems [27]. The difference between primal LWR problems and (dual) LWR problems is that secrets are chosen from R_q^d and calculations are performed modulo qR (or pR). Correspondingly, we will use symbols Primal-$A^M_{q,p,\boldsymbol{s}}(B)$, Primal-S-LWR$^M_{B,q,p,\chi}$ and Primal-D-LWR$^M_{B,q,p,\chi}$ to denote primal LWR distributions and primal search/decision LWR problems. The definition of LWE (dual) problems is given as follows.

Definition 2. *Let $K = \mathbb{Q}(\zeta)$ be a number field with $[K : \mathbb{Q}] = n$, $R = \mathcal{O}_K$, $M = R^d$ with d a positive integer, $q \geq 2$ and ψ be some distribution over H.*

- *For $\boldsymbol{s} \in (R_q^\vee)^d$, we define the* LWE *distribution $A^M_{q,\boldsymbol{s},\psi}$ as the distribution over $R_q^d \times \mathbb{T}_{R^\vee}$ obtained by sampling $\boldsymbol{a} := (a_1, \cdots, a_d)^T \hookleftarrow U(R_q^d)$, $e \hookleftarrow \psi$ and returning the pair $(\boldsymbol{a}, b = \sum_{i=1}^d a_i \cdot s_i + e \bmod qR^\vee)$.*
- *The search LWE problem, denoted by* S-LWE$^M_{q,\Psi}$*, consists in finding $\boldsymbol{s}$ with a polynomial number of samples sampled from $A^M_{q,\boldsymbol{s},\psi}$ for some arbitrary $\boldsymbol{s} \in (R_q^\vee)^d$.*

Similarly, the primal LWE problems are defined as $\boldsymbol{s} \in R_q^d$, and calculations are carried out modqR. As a finish of this subsection, we give the definition of polynomial LWR problems.

Definition 3. *Let $K = \mathbb{Q}(\zeta) = \mathbb{Q}[x]/(\Phi(x))$ be a number field with $[K : \mathbb{Q}] = n$, $q \geq p \geq 2$ be two integers, d is a positive integer, and χ be some distribution over $\mathcal{R} := \mathbb{Z}_q[x]/(\Phi(x))$. Set $B = \{1, x, \cdots, x^{n-1}\}$.*

- *For $\boldsymbol{s} \in \mathcal{R}^d$, we define the polynomial LWR distribution (with respect to basis B) as* Poly-$A^d_{q,p,\boldsymbol{s}}(B)$ *obtained by sampling $\boldsymbol{a} \hookleftarrow U(R^d)$ and returning the pair $(\boldsymbol{a}, b = \lfloor \sum_{i=1}^d a_i \cdot s_i \bmod q\mathcal{R} \rceil_{B,q,p}) \in \mathcal{R}^d \times \mathbb{Z}_p[x]/(\Phi(x))$.*
- *The polynomial search LWR problem, denoted by* Poly-S-LWR$^d_{q,p,\chi}$*, consists in finding $\boldsymbol{s}$ with a polynomial number of samples sampled from* Poly-$A^d_{q,p,\boldsymbol{s}}(B)$ *for some arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi^d) \subseteq \mathcal{R}^d$.*
- *The polynomial decision LWR problem, denoted by* Poly-D-LWR$^d_{q,p,\chi}$*, consists in distinguishing a polynomial number of samples, which are sampled either from* Poly-$A^d_{q,p,\boldsymbol{s}}(B)$ *or from $U(\mathcal{R}^d \times \mathbb{Z}_p[x]/(\Phi(x)))$, with non-negligible probability for $\boldsymbol{s} \hookleftarrow \chi^d$.*

3 One-wayness versus Pseudo-randomness of LWR Problems over Galois Extensions

As a warm up, we shall discuss the search-to-decision reductions of LWR problems defined in *any* number field K that is Galois over $\mathbb{Q}$ with secrets s belongs to some special sets in this section.

Throughout this section, we use the following setting of parameters, unless otherwise specified. We let $K = \mathbb{Q}[x]/(\Phi(x)) = \mathbb{Q}(\zeta)$ be a number field which is Galois over $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$ and Galois group $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \cdots, \sigma_n\}$, $R = \mathcal{O}_K$, and $M = R^d$ with d a positive integer. We also set modulus $q = Q \cdot p$ for simplicity, where $\gcd(Q, p) = 1$, p is a split-well prime with prime ideal decomposition $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_{\mathfrak{g}}$ and $\gcd(p, \Delta_k) = 1$.

Our reduction works under *any* $\mathbb{Z}_q$-basis of $R_q^\vee$, not necessarily the $\mathbb{Z}$-basis of $R^\vee$. Assume that $(b_1, \cdots, b_n) =: B = B \bmod qR^\vee$ is any $\mathbb{Z}_q$-basis of $R_q^\vee$, we define the set $\mathcal{S}_B$ as $\{\sigma_i(B) : \sigma_i \in \mathrm{Gal}(K/\mathbb{Q})\}$. Since $p|q$ and $\gcd(Q, p) = 1$, we have $qR^\vee \subseteq pR^\vee \subseteq R^\vee$, and $R^\vee/qR^\vee \cong R^\vee/QR^\vee \times R^\vee/pR^\vee$. Therefore, the coset $B \bmod pR^\vee$ is also a $\mathbb{Z}_p$-basis of $R_p^\vee$ [7]. Let χ_0 be the uniform distribution over $(R_q^\vee \cap R_p^\vee)^\times$. Here, the set $(R_q^\vee \cap R_p^\vee)^\times$ is defined as $\{x \in R_q^\vee : x = 0 \bmod Q \cdot R^\vee, x \neq 0 \bmod \mathfrak{p}_i \cdot R^\vee \text{ for all } i \in [\mathfrak{g}]\}$. Notice that, the distribution χ_0 of $\boldsymbol{s}$ is σ_i-invariant (i.e. $\sigma_i(\chi_0) = \chi_0$) for any $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$, since $\sigma_i(\mathfrak{p}_j) = \mathfrak{p}_j$ for all $i \in [n]$ and $j \in [\mathfrak{g}]$.

Our reduction route is similar as those used in [18–20], which is stated as follows:

$$\text{S-LWR}^M_{B,q,p,\chi_0} \mapsto \mathfrak{p}_i\text{-S-LWR}^M_{\mathcal{S}_B,q,p,\chi_0} \mapsto \text{W-D-LWR}^{M,i}_{\mathcal{S}_B,q,p,\chi_0} \mapsto \text{D-LWR}^M_{B,q,p,U((R_q^\vee \cap R_p^\vee)^\times)}.$$

Before starting reductions, let's first give some supporting lemmas. Notice that in the following lemma, we have already used the fact that changing of modulus also changes the basis we use (i.e. from $\mathbb{Z}_q$ basis to $\mathbb{Z}_p$ basis).

Lemma 1. *For any $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ with $i \in [n]$, any $\boldsymbol{a} \in R_q^d$ and $\boldsymbol{s} \in (R_q^\vee)^d$, we have*

$$\sigma_i(\lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{B,q,p}) = \lfloor \sigma_i(\boldsymbol{a})^T \cdot \sigma_i(\boldsymbol{s}) \rceil_{\sigma_i(B),q,p}.$$

Proof. Fix an arbitrary $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$, and set $\tau = \sigma_i$ for convenience. For any $\boldsymbol{a} = (a_1, \cdots, a_d)^T \in R_q^d$ and $\boldsymbol{s} = (s_1, \cdots, s_d)^T \in (R_q^\vee)^d$, we denote $\lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{B,q,p}$ by b. Setting $b' = \sum_{i=1}^d a_i \cdot s_i = \sum_{i=1}^n x_i \cdot b_i$ with $x_i \in \mathbb{Z}_q$, we have $b = \sum_{i=1}^n \lfloor x_i \rceil_{q,p} \cdot b_i$ and $\tau(b) = \sum_{i=1}^n \lfloor x_i \rceil_{q,p} \cdot \tau(b_i)$, since $\lfloor x_i \rceil_{q,p} \in \mathbb{Z}_p$ and $\tau(pR^\vee) = pR^\vee$. On the other hand, $\tau(\sum_{i=1}^d a_i \cdot s_i) = \tau(b') = \sum_{i=1}^n x_i \cdot \tau(b_i)$ since $x_i \in \mathbb{Z}_q$ and $\tau(qR^\vee) = qR^\vee$. So, we have $\lfloor \tau(\sum_{i=1}^d a_i \cdot s_i) \rceil_{\tau(B),q,p} = \sum_{i=1}^n \lfloor x_i \rceil_{q,p} \cdot \tau(b_i)$, and the result of this lemma is concluded.

Our reduction uses the following simple but crucial obversion, that solving LWR problems with respect to $\mathbb{Z}_q$-basis B is equivalent to solving LWR problems with respect to $\mathbb{Z}_q$-basis $\sigma_i(B)$ for all $i \in [n]$.

[7] In the followings, we will omit the symbol mod $pR^\vee$ if no ambiguity will be caused.

Lemma 2. *For any $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$ with $i \in [n]$, S/D-LWR$^M_{B,q,p,\chi_0}$ is equivalent to S/D-LWR$^M_{\sigma_i(B),q,p,\chi_0}$. I.e., for any $B \in \mathcal{S}_B$, the corresponding S/D-LWR$^M_{B,q,p,\chi_0}$ problem is equivalent to each other.*

Proof. We also fix an arbitrary $\sigma_i \in \mathrm{Gal}(K/\mathbb{Q})$, and set $\tau = \sigma_i$ for convenience. We take D-LWR problem as an example, since proofs are similar.

Assume that an oracle $\mathfrak{O}$ could solve D-LWR$^M_{B,q,p,\chi_0}$ with probability δ when given L samples, we shall show that we could use $\mathfrak{O}$ to solve D-LWR$^M_{\tau(B),q,p,\chi_0}$ with the same probability when given the same number of samples. When given L samples $\{(\boldsymbol{a}_k, b_k\}_{k=1}^L$ sampled from either $A^M_{q,p,\boldsymbol{s}}(\tau(B))$ with $\boldsymbol{s} \hookleftarrow \chi_0^d$ or $U(R_q^d \times R_p^\vee)$, we transfer $\{(\tau^{-1}(\boldsymbol{a}_k), \tau^{-1}(b_k))\}_{k=1}^L$ to $\mathfrak{O}$ and accept the decision returned by $\mathfrak{O}$. When $\{(\boldsymbol{a}_k, b_k\}_{k=1}^L$ are sampled from $U(R_q^d \times R_p^\vee)$, then it is easy to verify that $\{(\tau^{-1}(\boldsymbol{a}_k), \tau^{-1}(b_k))\}_{k=1}^L$ are aslo distributed uniformly over $R_q^d \times R_p^\vee$. While, if $\{(\boldsymbol{a}_k, b_k)\}_{k=1}^L$ are sampled from $A^M_{q,p,\boldsymbol{s}}(\tau(B))$ for some $\boldsymbol{s} \hookleftarrow \chi_0^d$, we could easily deduce that $\tau^{-1}(b_k) = \lfloor \tau^{-1}(\boldsymbol{a}_k)^T \cdot \tau^{-1}(\boldsymbol{s}) \rceil_{B,q,p}$ with $\tau^{-1}(\boldsymbol{a}_k) \hookleftarrow U(R_q^d)$ and $\tau^{-1}(\boldsymbol{s}) \hookleftarrow \chi_0^d$ by Lemma 1, since $\tau^{-1}(\sum_{i=1}^d a_{k,i} \cdot s_i) = \sum_{i=1}^d \tau^{-1}(a_{k,i}) \cdot \tau^{-1}(s_i)$. We could expect $\mathfrak{O}$ to solve corresponding problems with probability δ, as desired.

Reduction from D-LWR$^M_{\tau(B),q,p,\chi_0}$ to D-LWR$^M_{B,q,p,\chi_0}$ is similar, so we omit it.

Now, let's discuss the search to decision reductions of Ring/Module LWR problems. As we have already explained, this reduction is divided into three steps.

Reductions from S-LWR$^M_{B,q,p,\chi_0}$ to $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$

Let's first give the formal definition of $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ problem.

Definition 4. *The $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ problem is: given a polynomial number of samples from $A^M_{q,p,\boldsymbol{s}}(B)$ for some arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi_0^d)$ and $B \in \mathcal{S}_B$, find $\boldsymbol{s} \bmod \mathfrak{p}_i R^\vee := (s_1 \bmod \mathfrak{p}_i R^\vee, \cdots, s_d \bmod \mathfrak{p}_i R^\vee)$.*

Notice that these problems are all worst-case. Reductions from S-LWR$^M_{B,q,p,\chi_0}$ to $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ for any $i \in [\mathfrak{g}]$ could be deduced by the following two lemmas.

Lemma 3. *$\mathfrak{p}_1$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ problem is equivalent to $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ problem for any $i \in [\mathfrak{g}]$.*

Proof. We only need to show that if there is an oracle $\mathfrak{O}$ which could solve $\mathfrak{p}_1$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ problem with L samples, we can use it to solve $\mathfrak{p}_2$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ problem. Other reductions are all similar.

For any fixed basis $B \in \mathcal{S}_B$, when given L samples $\{(\boldsymbol{a}_k, b_k)\}_{k=1}^L$ sampled from $A^M_{q,p,\boldsymbol{s}}(B)$ for some arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi_0^d)$, we need to recover $\boldsymbol{s} \bmod \mathfrak{p}_2 R^\vee$. Since $K/\mathbb{Q}$ is Galois, there exists at least one $\sigma_j \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma_j(\mathfrak{p}_2) = \mathfrak{p}_1$. We then give $\{\sigma_j(\boldsymbol{a}_k), \sigma_j(b_k)\}_{k=1}^L$ (under the representations with respect to basis $\sigma_j(B)$) to $\mathfrak{O}$ and could expect to get some $\boldsymbol{s}'$. Lemma 1 shows that

$\sigma_j(b_k) = \sigma_j(\lfloor \boldsymbol{a}_k^T \cdot \boldsymbol{s} \rceil_{B,q,p}) = \lfloor \sigma_j(\boldsymbol{a}_k)^T \cdot \sigma_j(\boldsymbol{s}) \rceil_{\sigma_j(B),q,p}$. Since χ_0 is σ_j-invariant, $\{\sigma_j(\boldsymbol{a}_k), \sigma_j(b_k)\}_{k=1}^L$ are distributed identically to $A^M_{q,p,\sigma_j(\boldsymbol{s})}(\sigma_j(B))$. Therefore, oracle $\mathfrak{O}$ will return $\boldsymbol{s}' = \sigma_j(\boldsymbol{s}) \bmod \mathfrak{p}_1 R^\vee$ by assumption. Since $\sigma_j^{-1}(\mathfrak{p}_1 R^\vee) = \mathfrak{p}_2 R^\vee$, we can deduce that $\sigma_j^{-1}(\boldsymbol{s}') = \boldsymbol{s} \bmod \mathfrak{p}_2 R^\vee$ is the desired solution.

Lemma 4. *There is an efficient* PPT *reduction from* S-LWR$^M_{B,q,p,\chi_0}$ *to* $\mathfrak{p}_1$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$.

Proof. First notice that by our definition of χ_0, recovering $\boldsymbol{s} \bmod qR^\vee$ is equivalent to recovering $\boldsymbol{s} \bmod pR^\vee$. Our goal is to find $\boldsymbol{s} \bmod \mathfrak{p}_k R^\vee$ for every $k \in [\mathfrak{g}]$. Then, we could recover $\boldsymbol{s} \bmod pR^\vee$ efficiently via the Chinese Remainder Theorem $R_p^\vee \cong R^\vee/\mathfrak{p}_1 R^\vee \times \cdots \times R^\vee/\mathfrak{p}_\mathfrak{g} R^\vee$. Assume $\mathfrak{p}_1$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ oracle $\mathfrak{O}$ requires L samples to output $\boldsymbol{s} \bmod \mathfrak{p}_1 R^\vee$. Since there exist $\{\sigma_i\}$'s such that $\sigma_i(\mathfrak{p}_i) = \mathfrak{p}_1$, we make L queries to $A^M_{q,p,\boldsymbol{s}}(B)$, get $\{(\boldsymbol{a}_k, b_k)\}_{k=1}^L$, and send each L samples $\{\sigma_i(\boldsymbol{a_k}), \sigma_i(b_k)\}_{k=1}^L$ to $\mathfrak{O}$. Analysis similar to Lemma 3 shows that we could get $\boldsymbol{s} \bmod \mathfrak{p}_i R^\vee$ for all $i \in [\mathfrak{g}]$, and the Chinese Remainder Theorem ensures we could recover $\boldsymbol{s} \bmod pR^\vee$ successfully.

Reductions from $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ to W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$

The formal definition of W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ problem is as following.

Definition 5. *Let* $i \in [\mathfrak{g}]$,

- *For some* $\boldsymbol{s} \in \mathrm{Supp}(\chi_0^d)$, *the distribution* $A^{M,i}_{q,p,\boldsymbol{s}}(B)$ *over* $R_q^d \times R_p^\vee$ *is defined as: sample* $(\boldsymbol{a}, b) \hookleftarrow A^M_{q,p,\boldsymbol{s}}(B)$ *and output* $(\boldsymbol{a}, b + h)$, *where* $h \in R_p^\vee$ *is uniformly at random over* mod $\mathfrak{p}_j R^\vee$ *for all* $j \le i$, *and* 0 *over* mod $\mathfrak{p}_j R^\vee$ *for other* $j > i$.
- *The* W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ *problem is: given a polynomial number of samples from* $A^{M,j}_{q,p,\boldsymbol{s}}(B)$ *for some arbitrary* $\boldsymbol{s} \in \mathrm{Supp}(\chi_0)$, $B \in \mathcal{S}_B$ *and* $j \in \{i-1, i\}$, *determine* j.

The proof of the following lemma uses a similar route as [18, 20], and the ring-variant has been proved to be effective in [19]. We put its detailed proof in Appendix A for completeness, since our reductions contain the reductions of module cases and the full version of [19] seems to be unavailable now.

Lemma 5. *For any* $i \in [\mathfrak{g}]$, *there is an efficient* PPT *reduction from* $\mathfrak{p}_i$-S-LWR$^M_{\mathcal{S}_B,q,p,\chi_0}$ *problem to* W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ *problem.*

Reductions from W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ to D-LWR$^M_{B,q,p,\chi_0}$

Slightly different from the route used in [19], we choose to divide reduction from W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ to D-LWR$^M_{B,q,p,\chi_0}$ into two parts: one is a reduction from W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ to *worst-case* D-LWR$^M_{B,q,p,\chi_0}$ (where one needs to solve decision LWR problems for some arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi_0^d)$ with probability $\approx$

1) by noticing $A^{M,0}_{q,p,B} = A^{M}_{q,p,B}$ and $A^{M,\mathfrak{g}}_{q,p,B} = U(R^{\vee}_{p})$, and using a standard hybrid argument. The other is a reduction from worst-case D-LWR$^{M}_{B,q,p,\chi_0}$ to D-LWR$^{M}_{B,q,p,\chi_0}$ by using the technique of secret re-randomization. Since these techniques have been used in many lattice-based reductions [18, 20, 25], we just give the following lemma and put its proof in Appendix A.

Lemma 6. *There is an efficient* PPT *reduction from* W-D-LWR$^{M,i}_{\mathcal{S}_B,q,p,\chi_0}$ *problem for some* $i \in [\mathfrak{g}]$ *to* D-LWR$^{M}_{B,q,p,\chi_0}$ *problem.*

The number of samples used in reductions of Lemma 6 depends on the advantage of solving D-LWR$^{M}_{B,q,p,\chi_0}$ problem. For more details, one could refer to Appendix A. Combing Lemmas 4, 5 and 6, we could deduce the following Theorem.

Theorem 1. *Assume that* $K = \mathbb{Q}(\zeta)$ *is an algebraic number field which is Galois over* $\mathbb{Q}$, $R = \mathcal{O}_K$, $M = R^d$ *with* d *a positive integer,* p *is a split-well prime, modulus* $q = Q \cdot p$ *satisfies that* $\gcd(Q, p) = 1$ *and* $\gcd(p, \Delta_K) = 1$, B *is any* $\mathbb{Z}_q$*-basis of* $R^{\vee}_{q}$. *Let* $\chi_0 = U((R^{\vee}_{q} \cap R^{\vee}_{p})^{\times})$, *there is an efficient* PPT *reduction from* S-LWR$^{M}_{B,q,p,\chi_0}$ *problem to* D-LWR$^{M}_{B,q,p,\chi_0}$ *problem.*

That is to say, if search LWR problem is one-way with respect to some *arbitrary* basis of $R^{\vee}$ (or $\mathbb{Z}_q$-basis of $R^{\vee}_{q}$), then the corresponding decision LWR problem is pseudo-random. However, we could not deduce a reduction from worst-case ideal/module lattices problems to decision LWR problem by combining Theorem 4.11 of [19] and Theorem 1, since $\frac{|\mathrm{Supp}(\chi_0^d)|}{|(R^{\vee}_{q})^d|} = \mathrm{negl}(n)$. How to show the worst-case hardness of decision ring/module LWR problems will be discussed in Section 4.

4 On the Worst-Case Hardness of Ring/Module LWR Problems

In Section 3, we constrain the secret set to be $(R^{\vee}_{q} \cap R^{\vee}_{p})^{\times}$, which is a negligible part of $R^{\vee}_{q}$. So, we could not using known methods (e.g. methods used in [9, 19]) to show the worst-case hardness of LWR problems with these special secrets. In fact, we shall show that there is a PPT algorithm to solve Ring/Module-LWR problems with secrets constrained in $(R^{\vee}_{q} \cap R^{\vee}_{p})^{\times}$ in this section. Then, combing this PPT algorithm and reductions showed in Section 3, we'll show the worst-case hardness of Ring-LWR problems with secrets in $(R^{\vee}_{q})^{\times}$. In this section, we use symbols as defined in Section 3, unless otherwise specified.

4.1 Attacks on LWR with Special Secrets

In this subsection, we will give a simple attack to the search variant of LWR problems with secrets chosen in $(R^{\vee}_{q} \cap R^{\vee}_{p})^{\times}$ (and similar sets), though there are still exponential many secrets. The intuition is quiet simple. Using CRT, we

could represent the b-component of a LWR sample to a linear form of (part of) $\boldsymbol{a}$ and $\boldsymbol{s}$ for suitable parameters, if the secrets $\boldsymbol{s}$ are too special.

Let's recall some facts about CRT first. For $q = Q \cdot p$ with $\gcd(p, Q) = 1$, we could calculate the ring isomorphism $\mathbb{Z}_q \cong \mathbb{Z}_Q \times \mathbb{Z}_p$ easily. In fact, these exists some $x, y \in \mathbb{Z}$ such that $px+Qy = 1$. We define $p_Q^{-1} = x \bmod Q$, $Q_p^{-1} = y \bmod p$, and set $r_1 = p \cdot p_Q^{-1} \bmod q$, $r_2 = Q \cdot Q_p^{-1} \bmod q$. Then, the isomorphism of $\mathbb{Z}_q \cong \mathbb{Z}_Q \times \mathbb{Z}_p$ is defined as $s = r_1 \cdot s_1 + r_2 \cdot s_2$ with $s \in \mathbb{Z}_q$, $s_1 \in \mathbb{Z}_Q$ and $s_2 \in \mathbb{Z}_p$. Since $\mathbb{Z} \subseteq R \subseteq R^\vee$, r_1 and r_2 (which will also be fixed throughout this paper unless specified) could also be regarded as a CRT "basis" of the ring/module isomorphism $R_q \cong R_Q \times R_p$ and $R_q^\vee \cong R_Q^\vee \times R_p^\vee$.

Lemma 7. *For any distribution ϕ over $(R_q^\vee \cap R_p^\vee)^\times$, there is a PPT algorithm for solving* S-LWR$^M_{B,q,p,\phi}$ *with a polynomial number samples, where $B = \{b_1, \cdots, b_n\}$ is any $\mathbb{Z}_q$-basis of $R_q^\vee$.*

Proof. For any $s = (s_1, \cdots, s_d)^T \hookleftarrow \phi^d$, we represent $s_j = r_2 \cdot s_{j,2}$ for some $s_{j,2} \in (R_p^\vee)^\times$ and $j \in [d]$. Assume $\boldsymbol{a} = (a_1, \cdots, a_d)^T$ with $a_j = r_1 \cdot a_{j,1} + r_2 \cdot a_{j,2} \in R_q$, we get $\boldsymbol{a}^T \cdot \boldsymbol{s} = r_2 \cdot \sum_{j=1}^n a_{j,2} \cdot s_{j,2} \bmod qR^\vee$, since $r_2^2 = r_2 \bmod q$ and $r_1 \cdot r_2 = 0 \bmod q$.

Assume further that $\sum_{j=1}^d a_{j,2} \cdot s_{j,2} = \sum_{i=1}^n x_i \cdot b_i \bmod qR^\vee$, we have

$$\begin{aligned}
\lfloor a \cdot s \rceil_{B,q,p} &= \lfloor r_2 \cdot \sum_{j=1}^{d} a_{j,2} \cdot s_{j,2} \rceil_{B,q,p} = \lfloor r_2 \cdot \sum_{i=1}^{n} x_i \cdot b_i \bmod qR^\vee \rceil_{B,q,p} \\
&= \sum_{i=1}^{n} \lfloor \frac{1}{Q} \cdot r_2 \cdot x_i \rceil_{q,p} \cdot b_i \bmod pR^\vee \\
&= Q_p^{-1} \cdot \sum_{i=1}^{n} x_i \cdot b_i \bmod pR^\vee = Q_p^{-1} \cdot \sum_{j=1}^{d} a_{j,2} \cdot s_{j,2} \bmod pR^\vee.
\end{aligned}$$

Since $a_{j,2} \hookleftarrow U(R_p)$ for $j \in [d]$, with a polynomial number of samples, we could find d samples $\{(\boldsymbol{a}_k = (a_{k,1}, \cdots, a_{k,d})^T, b_k)\}_{k=1}^d$ such that the $d \times d$ matrix A consisted of $a_{k,j,2}$ for $k, j \in [d]$ is invertible in $R_p^{d \times d}$ with probability ≈ 1 (e.g. using Lemma 9 of [29]). Namely, in this case, we have $(b_1, \cdots, b_d)^T = Q_p^{-1} \cdot A \cdot (s_{1,2}, \cdots, s_{d,2})^T \bmod pR^\vee$.

Hence, if we could get such samples, we have that $Q_p \cdot A^{-1} \cdot (b_1, \cdots, b_d)^T \bmod pR^\vee$ is the desired solution.

Remark 1. We choose $(R_q^\vee \cap R_p^\vee)^\times$ to be the secret set just for simplicity. It is easy to check that for any secret set of the form

$$S_{\boldsymbol{s}} := \{\boldsymbol{s} = (s_1, \cdots, s_d) \in (R_q^\vee)^d : |s_j \bmod QR^\vee| \leq \mathrm{poly}(n) \text{ for } j \in [d]\},$$

attack proposed in Lemma 7 also works for $d = O(1)$. Since in this case, we can check all the possible values of $\{s_{j,1}\}_{j=1}^d$'s to eliminate the bias appeared in the b-components. For more details, one can also refer to the proof of Lemma 8. Via the above attack, we could also deduce that the search variant LWR problems used in [19] is *not hard*.

4.2 Reducing Worst-Case Lattice Problems to LWR Problems

To show the worst-case hardness of S-LWR problems, Rényi divergence is a powerful tool [6, 9, 12, 19]. Usually, the requirement is that the proportion of secrets should be a non-negligible part of $R_q^\vee$. For our purpose, we need to introduce an intermediate problem which we call the extended LWR problems. We set the distribution $\chi_1 = U((R_q^\vee)^\times)$, where $(R_q^\vee)^\times := \{s = r_1 \cdot s_1 + r_2 \cdot s_2 \bmod qR^\vee$, s.t. $s_1 \in (R_Q^\vee)^\times$ and $s_2 \in (R_p^\vee)^\times\}$. Given any $\mathbb{Z}_q$ basis B of $R_q^\vee$, the (worst-case) extended search Ring/Module LWR problems with parameters q, Q, p is denoted by Ext-S-LWR$^M_{B,q,Q,p,\chi'}$, whose instances are of the form $(\boldsymbol{a}_1, \boldsymbol{a}_2, \lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q}, \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p}) \in R_q^d \times R_q^d \times R_Q^\vee \times R_p^\vee$ for some fixed $\boldsymbol{s} \in \mathrm{Supp}(\chi_1^d)$ and $\boldsymbol{a}_1, \boldsymbol{a}_2 \hookleftarrow U(R_q^d)$.

Comparing with methods used in [19], we utilize a different approach to prove the worst-case hardness of Ext-S-LWR problem. For a fixed basis B of $R^\vee$, we will first add some additional errors sampled from some appropriate Gaussian distribution to the b-components of LWE samples to amend the distribution of coefficients of errors with respect to basis B to a sphere Gaussian distribution. Then, we could use similar method as [6, 9, 12] to estimate corresponding Rényi divergences, and give a reduction from search LWE problems to Ext-S-LWR problems. We present the following theorem, whose proof is put in Appendix B. Notice that the field K used in Theorem 2 need not to be Galois over $\mathbb{Q}$.

Theorem 2. *Let B be any basis of $R^\vee$, and α, σ be two posotive reals such that $\sigma > \alpha \cdot \mathfrak{s}_1(B^{-1})$. There is a* PPT *reduction from* S-LWE$^M_{q,D_\alpha}$ *to* Ext-S-LWR$^M_{B,q,p,\chi_1}$ *for modulus $q \geq \max\{Q, p\} \cdot \frac{\sigma}{\sqrt{\pi}} \cdot \ln n \cdot n \cdot L$. Here, L is the half of the number of samples used, and such that $L \leq n^{\ln n - 1}$.*

Remark 2. It seems to be natural to define the Ext-S-LWR problem with instances of the form $(\boldsymbol{a}, \lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{B,q,Q}, \lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{B,q,p})$. However, for modulus $q = Q \cdot p$ with $\gcd(p, Q) = 1$, there exists elements $\{x\}$'s of $\mathbb{Z}_q$ such that $\Pr_e[(\lfloor x + e \rceil_{q,Q}, \lfloor x + e \rceil_{q,p}) \neq (\lfloor x \rceil_{q,Q}, \lfloor x \rceil_{q,p})] = 1$. Therefore, the corresponding Rényi distance is unbounded. The main reason is that coefficients for rounding operation $q \mapsto p$ and $q \mapsto Q$ are correlated in this case. For our choices, it is easy to show that the coefficients of $\boldsymbol{a}_1^T \cdot \boldsymbol{s}$ and $\boldsymbol{a}_2^T \cdot \boldsymbol{s}$ are independent from each other, and are distributed uniform over $\mathbb{Z}_q$. So, we could analyze the two rounding operations separately.

For cyclotomic field $K = \mathbb{Q}(\zeta_l)$ with $\zeta_l = e^{2\pi \boldsymbol{i} \cdot \frac{1}{l}}$, there is a basis, namely the decoding basis, of $R^\vee$ with $\mathfrak{s}_1(B^{-1}) = \sqrt{l} = \tilde{O}(n)$ [21]. Hence, in this case, if we use decoding basis, $q \geq \max\{p, Q\} \cdot \frac{\alpha \cdot L}{\sqrt{\pi}} \cdot \tilde{O}(n^2)$ is sufficient. There are quantum reductions from worst-case basic ideal lattice problems (e.g. SIVP$_\gamma$) over K to search Ring/Module LWE problems [18, 20]. However, for S-LWE problems, the error distributions are worst-case in the sense that one need to solve corresponding S-LWE problems with error distributions coming from a set of distributions (e.g. $\Psi_{\leq\alpha}$ [18, 20]). It is possible to amend the error distributions to some spherical Gaussians [1, 20, 24] via a Rényi divergence arguments. Hence,

for cyclotomic fields, if we set $d = \tilde{O}(1)$ and $L = \tilde{O}(1)$, we could also get a reduction from worst-case SIVP_γ problem with $\gamma = \tilde{O}(\frac{\sqrt{n}}{\alpha'})$ to Ext-S-LWR$^M_{B,q,p,\chi_1}$ problem with $q = \tilde{O}(n^{\frac{9}{2}} \cdot (\alpha')^2)$.

Next, we present a reduction from Ext-S-LWR problem to a weak version of Ring/Module LWR problem, denoted by Weak-S-LWR. Its instances are of the form $(\boldsymbol{a}, \lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{B,q,p}) \in R_q \times R_p^\vee$ for some fixed $\boldsymbol{s} \in \mathrm{Supp}((\chi_1)^d)$ and $\boldsymbol{a} \hookleftarrow U(R_q^d)$, but we only ask an adversary to recover $s_{i,2} := s_i \bmod pR^\vee$ for $s_i \in \boldsymbol{s}$. Notice that the reduction from Weak-S-LWR problem to S-LWR problem is trivial.

Lemma 8. *There is a* PPT *reduction from* Ext-S-LWR$^M_{B,q,Q,p,\chi_1}$ *to* Weak-S-LWR$^M_{B,q,p,\chi_1}$ *for any* $\mathbb{Z}_q$*-basis* $B = \{b_1, \cdots, b_n\}$ *of* $R_q^\vee$.

Proof. For some fixed $\boldsymbol{a}_1 = (a_{1,1}, \cdots, a_{1,d})^T, \boldsymbol{a}_2 = (a_{2,1}, \cdots, a_{2,d})^T \in R_q^d$ and $\boldsymbol{s} = (s_1, \cdots, s_d)^T \in (R_q^\vee)^d$, we assume that $s_i = r_1 \cdot s_{i,1} + r_2 \cdot s_{i,2} \bmod qR^\vee$ and $a_{k,i} = r_1 \cdot a_{k,i,1} + r_2 \cdot a_{k,i,2} \bmod qR$ for $k \in \{1,2\}$ and $i \in [d]$. Then, we have

$$\begin{aligned}\boldsymbol{a}_k^T \cdot \boldsymbol{s} \bmod qR^\vee &= r_1 \cdot \sum_{j=1}^{d} a_{k,j,1} \cdot s_{j,1} + r_2 \cdot \sum_{j=1}^{d} a_{k,j,2} \cdot s_{j,2} \bmod qR^\vee \\ &=: r_1 \cdot \sum_{i=1}^{n} x_{k,1,i} \cdot b_i + r_2 \cdot \sum_{i=1}^{n} x_{k,2,i} \cdot b_i \bmod qR^\vee.\end{aligned}$$

Through a similar calculation as Lemma 7, we have

$$\lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q} = p_Q^{-1} \cdot \sum_{j=1}^{d} a_{1,j,1} \cdot s_{j,1} + \sum_{i=1}^{n} \lfloor \frac{Q \cdot Q_p^{-1}}{p} \cdot x_{1,2,i} \rceil \cdot b_i \bmod QR^\vee$$

and

$$\lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p} = Q_p^{-1} \cdot \sum_{j=1}^{d} a_{2,j,2} \cdot s_{j,2} + \sum_{i=1}^{n} \lfloor \frac{p \cdot p_Q^{-1}}{Q} \cdot x_{2,1,i} \rceil \cdot b_i \bmod pR^\vee.$$

Recall that $Q \cdot Q_p^{-1} = 1 \bmod p$, we could recover $\{s_{j,1}\}$'s $\subseteq R_Q^\vee$ as in Lemma 7 from $\lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q}$ if we know $\{s_{j,2}\}$'s $\subseteq R_p^\vee$. Since in this case, the term $\sum_{i=1}^{n} \lfloor \frac{Q \cdot Q_p^{-1}}{p} \cdot x_{1,2,i} \rceil \cdot b_i \bmod QR^\vee$ is efficiently computable via $s_{j,2}, a_{2,j,2}$ and r_2 with $j \in [d]$.

Therefore, when given L Ext-S-LWR$^M_{B,q,p,\chi_1}$ samples $\{\boldsymbol{a}_{i,1}, \boldsymbol{a}_{i,2}, b_{i,1}, b_{i,2}\}_{i=1}^L$, we just transfer $\{\boldsymbol{a}_{i,2}, b_{i,2}\}_{i=1}^L$ to Weak-S-LWR$^M_{B,q,p,\chi_1}$ oracle $\mathcal{O}$ and could expect to get $s_{j,2} = s_j \bmod pR^\vee$ for $s_j \in \boldsymbol{s}$. Then, we could recover $\boldsymbol{s} \in R_q^\vee$ via the about observation and CRT effectively.

It is easy to verify that reductions proposed in Section 3 also work for Weak-S-LWR problems with secrets in $\mathrm{Supp}(\chi_1) = (R_q^\vee)^\times$. The only things [8] one

[8] In the reduction from $\mathfrak{p}_i$-Weak-S-LWR$^M_{S(B),q,p,\chi_1}$ to W-D-LWR$^{M,i}_{S(B),q,p,\chi_1}$, we may need to change the $\boldsymbol{a}'$-component to $\boldsymbol{a} + \frac{q}{p} \cdot r_2 \cdot (y, 0, \cdots, 0)^T$, compared with $\boldsymbol{a} + \frac{q}{p} \cdot (y, 0, \cdots, 0)^T$ in the proof of Lemma 5.

need to do is to modify definitions of corresponding intermediate problems to Weak-S-LWR cases. The reduction road-map is S-LWE$\mapsto$Ext-S-LWR$\mapsto$Weak-S-LWR$\mapsto$ $\mathfrak{p}_i$-Weak-S-LWR$\mapsto$W-D-LWR^i $\mapsto$D-LWR.

Overall, we could deduce the following theorem.

Theorem 3. *Assume K is a number field which is Galois over $\mathbb{Q}$ with $[K : \mathbb{Q}] = n$, $R = \mathcal{O}_K$, $R^\vee$ is the dual ideal of R, B is a set of basis of $R^\vee$, modulus $q = Q \cdot p$ such that p is a spilt-well prime and $\gcd(Q, p) = 1$, d is an integer and $M = R^d$. Let α, σ be two posotive reals such that $\sigma > \alpha \cdot \mathfrak{s}_1(B^{-1})$, and $\chi_1 = U((R_q^\vee)^\times)$. There is a* PPT *reduction from* S-LWE$^M_{q,D_\alpha}$ *to* D-LWR$^M_{B,q,p,\chi_1}$ *for modulus $q \geq \max\{Q, p\} \cdot \frac{\sigma}{\sqrt{\pi}} \cdot \ln n \cdot n \cdot L$. Here, L is the half of the number of samples used, and such that* $\mathrm{poly}(n) \leq L \leq n^{\ln n - 1}$.

5 On the Hardness of Polynomial LWR Problems

We shall discuss the one-wayness and pseudo-randomness of polynomial LWR problems, and show the worst-case hardness of Poly-S/D-LWR problems over any number field K which is Galois over $\mathbb{Q}$ in this section. Some results about middle-product polynomial LWR problems are also given.

5.1 Polynomial LWR Problems over General Galois Extension

Notice that for general Galois extension $K = \mathbb{Q}[x]/(\Phi(x)) = \mathbb{Q}(\zeta)$, its ring of integers R may not be isomorphic to $\mathbb{Z}[x]/(\Phi(x)) \cong \mathbb{Z}[\zeta]$. Usually, $\mathbb{Z}[\zeta]$ is just an order [9], not an ideal, of K. Our main ingredient is a ring ($\mathbb{Z}$ module) isomorphism between the polynomial ring $\mathcal{R}_q$ and R_q for suitable modulus q. Recall that we have the following prime ideal decomposition [14]. For any fixed prime p such that $p \nmid |R/\mathbb{Z}[\zeta]|$ and $p \nmid \Delta_K$, we assume $\Phi(x) = \Phi_1(x) \cdots \Phi_{\mathfrak{g}}(x) \bmod p$ with $\deg(\Phi_i(x)) = \mathfrak{f}$ for $i \in [\mathfrak{g}]$. Here, $\Phi_i(x)$ is irreducible polynomial in $\mathbb{Z}_p[x]$ and $\Phi_i(x) \neq \Phi_j(x)$ for any $i \neq j \in [\mathfrak{g}]$. Then, the prime ideal decomposition of p is $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_{\mathfrak{g}}$ with $\mathfrak{p}_i = (p, \Phi_i(\zeta)) \cdot R$, and the norm of $\mathfrak{p}_i$ is $\mathrm{N}(\mathfrak{p}_i) = p^{\mathfrak{f}}$ for $i = 1, \cdots, \mathfrak{g}$. In particular, we have $\mathfrak{g} \cdot \mathfrak{f} = n$.

Next, let's show that there exists some power-basis of R_q for suitable square-free modulus q, even if R may have no power-basis.

Lemma 9. *Let p be a prime such that $p \nmid \Delta_K$ and $p \nmid |R/\mathbb{Z}[\zeta]|$. Assume $\Phi(x) = \Phi_1(x) \cdots \Phi_{\mathfrak{g}}(x) \bmod p$ with $\deg(\Phi_i(x)) = \mathfrak{f}$ for $i \in [\mathfrak{g}]$, here $\Phi_i(x)$ is irreducible polynomial in $\mathbb{Z}_p[x]$ and $\Phi_i(x) \neq \Phi_j(x)$ for any $i \neq j \in [\mathfrak{g}]$. Then, we have the following ring ($\mathbb{Z}$-module) isomorphisms:*

$$\begin{aligned} R_p = R/pR &\cong R/\mathfrak{p}_1 \times \cdots \times R/\mathfrak{p}_{\mathfrak{g}} \\ &\cong \mathbb{Z}[x]/(p, \Phi_1(x)) \times \cdots \times \mathbb{Z}[x]/(p, \Phi_{\mathfrak{g}}(x)) \\ &\cong \mathbb{Z}_p[x]/(\Phi_1(x)) \times \cdots \times \mathbb{Z}_p[x]/(\Phi_{\mathfrak{g}}(x)) \\ &\cong \mathbb{Z}_p[x]/(\Phi(x)). \end{aligned}$$

[9] An order of K is a subring with unity, whose $\mathbb{Q}$ span is K.

Proof. Note that we have $pR = \mathfrak{p}_1 \cdots \mathfrak{p}_{\mathfrak{g}}$ with $\mathfrak{p}_i = (p, \Phi_i(\zeta))R \subsetneqq R$ and $\mathrm{N}(\mathfrak{p}_i) = p^{\mathfrak{f}}$ for $i = 1, \cdots, \mathfrak{g}$. The first and last isomorphisms come form CRT. Since p is a prime, $\mathbb{Z}_p[x]$ is a principal ideal domain. So, $F_i := \mathbb{Z}_p[x]/(\Phi_i(x))$ is a finite field. The natural map $\psi_1 : \mathbb{Z}[x] \mapsto \mathbb{Z}_p[x]/(\Phi_i(x))$ is a surjection with kernel $\mathrm{Ker}(\psi_1) = (p, \Phi_i(x))$. So, the third isomorphism is concluded. We can also deduce that $(p, \Phi_i(x))$ with $i \in [\mathfrak{g}]$ is a maximal ideal of $\mathbb{Z}[x]$.

Now we consider the map $\psi_2 : \mathbb{Z}[x] \mapsto R/\mathfrak{p}_i$, defined by $\psi_2(f(x)) = f(\zeta) + \mathfrak{p}_i$. It's easy to check ψ_2 is a ring homomorphism. Since we choose $p \nmid |R/\mathbb{Z}[\zeta]|$, and $|R/(Z[\zeta] + pR)|$ is a factor of $\gcd(|R/\mathbb{Z}[\zeta]|, |R/pR|) = 1$, we get $|R/(Z[\zeta] + pR)| = 1$, which is equivalent to $\mathbb{Z}[\zeta] + pR = R$. Note that $pR \subseteq \mathfrak{p}_i$, we have $\mathbb{Z}[\zeta] + \mathfrak{p}_i = R$, which implies that ψ_2 is surjective. Using the fact that ideal $(p, \Phi_i(x))$ is maximal, $\psi_2((p, \Phi_i(x))) \subseteq (p, \Phi_i(\zeta))$ and $\mathfrak{p}_i = (p, \Phi_i(\zeta)) \subsetneqq R$, we have $\mathrm{Ker}(\psi_2) = (p, \Phi_i(x))$, since the kernel of ψ_2 is an ideal of $\mathbb{Z}[x]$. So, $R/\mathfrak{p}_i \cong \mathbb{Z}[x]/(p, \Phi_i(x))$.

Via the proof of Lemma 9, we get that $(1, \zeta \bmod pR, \cdots, (\zeta \bmod pR)^{n-1} = \zeta^{n-1} \bmod pR)$ is a $\mathbb{Z}_p$ power basis of R_p for suitable prime p. Assume $q = Q \cdot p$ with Q, p two different primes such that $\gcd(q, \Delta_K) = 1$ and $\gcd(q, |R/\mathbb{Z}[\zeta]|) = 1$. We have two ring isomorphisms $R_p \cong \mathbb{Z}_p[x]/(\Phi(x))$ and $R_Q \cong \mathbb{Z}_Q[x]/(\Phi(x))$ by Lemma 9. Meanwhile, we also have $\mathbb{Z}_q[x]/(\Phi(x)) \cong \mathbb{Z}_Q[x]/(\Phi(x)) \times \mathbb{Z}_p[x]/(\Phi(x))$ (by the First Isomorphism Theorem of rings) and $R_q \cong R_Q \times R_p$ by the CRT. Therefore, we could deduce a ring isomorphism $\varphi_{q,R} : \mathbb{Z}_q[x]/(\Phi(x)) \cong R_q$ for this special kind of modulus q. In particular, R_q admits a $\mathbb{Z}_q$ power basis consisting of powers of $\varphi_{q,R}(x \bmod \Phi(x) \cdot \mathbb{Z}_q[x]) = \zeta \bmod qR$.

Recall that for any modulus q, there exists an R-module isomorphism $\varphi_{R,R^\vee} : R_q \cong R_q^\vee$ (e.g. applying Lemma 2.15 of [20]). We denote its inverse by $\varphi_{R^\vee,R}$. More precisely, assume the prime ideal decomposition of qR is known, we could compute an element $t \in (R^\vee)^{-1}$ such that $t \cdot R^\vee + qR = R$ efficiently by [20, Lemma 2.14]. Meanwhile, we could also compute an element $c \in t \cdot R^\vee$ such that $c = 1 \bmod qR$ by [20, Lemma 2.13]. The map $\varphi_{R^\vee,R} : R_q^\vee \mapsto R_q$ is defined as $\varphi_{R^\vee,R}(u \bmod qR^\vee) = t \cdot u \bmod qR$ for $u \in R_q^\vee$. On the other hand, for any $a \in R$, $\frac{c}{t} \cdot a \in R^\vee$ is the element corresponding to a such that $t \cdot \frac{c \cdot a}{t} \bmod qR = a \bmod qR$, so the map $\varphi_{R,R^\vee} : R_q \mapsto R_q^\vee$ is defined as $\varphi_{R,R^\vee}(a \bmod qR) = \frac{c}{t} \cdot a \bmod qR^\vee = \frac{a}{t} \bmod qR^\vee$ for $a \in R_q$. In the followings, we will reuse the symbols $\varphi_{R,R^\vee}$ and $\varphi_{R^\vee,R}$ for different modulus q if no ambiguity is caused.

For any $\mathbb{Z}_q$-basis $\bar{B}$ of $R_q^\vee$, $\varphi_{R^\vee,R}(\bar{B})$ is a set of $\mathbb{Z}_q$-basis of R_q. If we set $\chi_2 = U(R_q^\times)$, then we have $\chi_2 = \varphi_{R^\vee,R}(\chi_1)$. We can deduce the following lemma.

Lemma 10. *The* Primal-(S)D-$\mathrm{LWR}^M_{\varphi_{R^\vee,R}(\bar{B}),q,p,\chi_2}$ *problem is equivalent to the* (S)D-$\mathrm{LWR}^M_{\bar{B},q,p,\chi_1}$ *problem.*

Proof. Denote $\varphi_{R^\vee,R}$ by φ for simplicity. Notice that φ is a R-module isomorphism and $\mathbb{Z} \subseteq R$, this lemma follows by checking the equation $\varphi(\lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{\bar{B},q,p}) = \lfloor \varphi(\boldsymbol{a}^T \cdot \boldsymbol{s}) \rceil_{\varphi(\bar{B}),q,p} = \lfloor \boldsymbol{a} \cdot \varphi(\boldsymbol{s}) \rceil_{\varphi(\bar{B}),q,p}$ via a similar process as in the proof of Lemma 1, here $\boldsymbol{a} \hookleftarrow U(R_q^d)$ and $\boldsymbol{s} \in (R_q^\vee)^d$.

Remark 3. We note that reductions of the lattice LWR problems in [19] (as well as the LWE case [23]) does not contain the direction of reductions from LWR problems to primal LWR problems.

Let's set $\bar{\zeta} = \zeta \bmod qR$, and $\bar{B}_1 = \{1, \bar{\zeta}, \cdots, \bar{\zeta}^{n-1}\}$. Then, we have $\bar{B}_1$ is a $\mathbb{Z}_q$-basis of R_q, and $\bar{B}_2 := \varphi_{R,R^\vee}(\bar{B}_1)$ is a $\mathbb{Z}_q$-basis of $R_q^\vee$. Let $\xi = \frac{c}{t} \cdot \zeta$ and set $B_2 := (1, \xi, \cdots, \xi^{n-1})$, then we also have $B_2 \bmod qR^\vee = \bar{B}_2$. Set χ_3 be the uniform distribution over the set $\varphi_{q,R}^{-1}(R_q^\times) = \mathcal{R}_q^\times$. Similar as proof of Lemma 10, we could get the following lemma.

Lemma 11. *The* Poly-(S)D-LWR$^d_{q,p,\chi_3}$ *problem is equivalent to the* Primal-(S)D-LWR$^M_{\bar{B}_1,q,p,\chi_2}$ *problem.*

Combining Lemmas 10 and 11, we get:

$$\text{Poly-(S)D-LWR}^d_{q,p,\chi_3} \Leftrightarrow \text{Primal-(S)D-LWR}^M_{\bar{B}_1,q,p,\chi_2} \Leftrightarrow \text{(S)D-LWR}^M_{\bar{B}_2,q,p,\chi_1}.$$

To show the hardness of Poly-S/D-LWR problems, we use reductions proposed in Section 4. However, B_2 is usually not a set of basis of $R^\vee$ for general Galois extension K. Assume B is an arbitrary basis of $R^\vee$, then we have $B_2 = B \cdot T$ with some $T \in \mathbb{Z}^{n\times n}$. Meanwhile, $T \bmod q$ is invertible in $\mathbb{Z}_q^{n\times n}$, since both $\bar{B} := B \bmod qR^\vee$ and $\bar{B}_2$ are $\mathbb{Z}_q$ bases of $R_q^\vee$. Combining results showed in Section 4, we could deduce the following theorem via reductions

$$\begin{aligned}&\text{S-LWE Problems} \Rightarrow \text{Ext-S-LWR Problems}\\ \Rightarrow &\begin{cases}\text{Weak-S-LWR Problems} \Rightarrow \text{S-LWR Problems} \Leftrightarrow \text{Poly-S-LWR Problems.}\\ \text{Weak-S-LWR Problems} \Rightarrow \text{D-LWR Problems} \Leftrightarrow \text{Poly-D-LWR Problems.}\end{cases}\end{aligned}$$

Theorem 4. *Assume $K = \mathbb{Q}(\zeta)$ is a number field with $[K : \mathbb{Q}] = n$, which is Galois over $\mathbb{Q}$, $R = \mathcal{O}_K$, $R^\vee$ is the dual ideal of R, modulus $q = Q \cdot p$ with p and Q different primes such that $\gcd(q, \Delta_K) = 1$ and $\gcd(q, |R/\mathbb{Z}[\zeta]|) = 1$, d is an integer and $M = R^d$. Let $B_2 := (1, \xi, \cdots, \xi^{n-1})$ with ξ defined as above Lemma 11, and α, σ be reals such that $\sigma > \alpha \cdot \mathfrak{s}_1(B_2^{-1})$. If* S-LWE$^M_{q,D_\alpha}$ *is one-way and modulus $q \geq \max\{Q, p\} \cdot \frac{\sigma}{\sqrt{\pi}} \cdot \ln n \cdot n \cdot L$, then* Poly-S-LWR$^d_{q,p,\chi_3}$ *is one-way, and* Poly-D-LWR$^d_{q,p,\chi_3}$ *is pseudo-random. Here, L is the half of the number of samples used, and such that* $\text{Poly}(n) \leq L \leq n^{\ln n - 1}$.

5.2 Polynomial LWR Problems over Cyclotomic Rings

Recall that the parameter q in Theorem 2 depends on the basis of $R^\vee$. However, even for the l-th cyclotomic fields $K = \mathbb{Q}(\zeta_l)$ with $\zeta_l = e^{\frac{2\pi i}{l}}$, the decoding basis of $R^\vee$ does not equal to the basis B_2 defined above Lemma 11. Moreover, for non-prime-power cyclotomic fields, the powerful basis of R does not equal to the power basis (i.e. B_1 defined above Lemma 11) of R. To show the hardness of Poly-S/D-LWR problems with tighter parameters, we use reductions:

$$\begin{aligned}&\text{S-LWE Problems} \Rightarrow \text{Primal-S-LWR Problems} \Rightarrow \text{Primal-Ext-S-LWR Problems}\\ \Rightarrow &\begin{cases}\text{Primal-Weak-S-LWR Problems} \Rightarrow \text{Primal-S-LWR Problems} \Leftrightarrow \text{Poly-S-LWR Problems.}\\ \text{Primal-Weak-S-LWR Problems} \Rightarrow \text{Primal-D-LWR Problems} \Leftrightarrow \text{Poly-D-LWR Problems.}\end{cases}\end{aligned}$$

Lemma 12. *For the l-th cyclotomic fields $K = \mathbb{Q}(\zeta_l)$, there is a* PPT *reduction from* S-LWE$^M_{q,D_\alpha}$ *to* Primal-S-LWE$^M_{q,D_{\alpha\cdot\hat{l}}}$. *Here, $\hat{l} = \frac{l}{2}$ when l is even, and $\hat{l} = l$ when l is odd.*

Proof. By [27, Theorem 2.13], for any $\boldsymbol{s} \in (R^\vee_q)^d$ and $t \in (R^\vee)^{-1}$ such that $tR^\vee + qR = R$, the map $(\boldsymbol{a}, b) \mapsto (\boldsymbol{a}, t \cdot b)$ transforms $A^M_{q,\boldsymbol{s},D_\alpha}$ to Primal-$A^M_{q,t\cdot\boldsymbol{s},D_{\boldsymbol{r}}}$ with $\boldsymbol{r} = (|\sigma_1(t)| \cdot \alpha, \cdots, |\sigma_n(t)| \cdot \alpha)$, and $U(R^d_q \times H/qR^\vee)$ to $U(R^d_q \times H/qR)$. Let $g = \prod_{p|l}(1-\zeta_p)$, then we have $g \in R$, $R^\vee = \frac{g}{\hat{l}} \cdot R$ and $gR + qR = R$ for any prime q such that $(q, l) = 1$ [21, Lemmas 2.16 and 2.18]. Hence, $(R^\vee)^{-1} = \frac{\hat{l}}{g} \cdot R$. By taking $t = \hat{l}$, we get a transformation from $A^M_{1,\boldsymbol{s},D_\alpha}$ to Primal-$A^M_{q,\hat{l}\cdot\boldsymbol{s},D_{\alpha\cdot\hat{l}}}$, and from $U(R^d_q \times H/qR^\vee)$ to $U(R^d_q \times H/qR)$. We get the result as desired.

Reduction from Primal-S-LWR Problems to Primal-Ext-S-LWR Problems is similar to Theorem 2. Combining Lemmas 11 and 12, and the fact that when l is a prime-power, the power basis B of R has singular values $\mathfrak{s}_1(B) = \sqrt{\hat{l}}$ and $\mathfrak{s}_n(B) = \sqrt{\frac{l}{\mathrm{rad}(l)}}$. Here, $\mathrm{rad}(l) = \prod_{p|l} p$. Notice that we don't need to use Lemma 9, so requirements on q can be relaxed. We could deduce the following theorem.

Theorem 5. *Assume cyclotomic field $K = \mathbb{Q}(\zeta_l) = \mathbb{Q}[x]/(\Phi_l(x))$ with l a prime-power, $n = \varphi(l)$, $R = \mathcal{O}_K$, $M = R^d$ with some positive integer d. Let modulus $q = Q \cdot p$ with p a spilt-well prime,* $\gcd(p, Q) = 1$ *and $q \nmid \Delta_K$. If* S-LWR$^M_{q,D_\alpha}$ *is hard and $q \geq \max\{p, Q\} \cdot \frac{\sigma \cdot L \cdot n \cdot \ln n}{\sqrt{\pi}}$ with $\sigma > \alpha \cdot \hat{l} \cdot \sqrt{\frac{l}{\mathrm{rad}(l)}}$, then both* Poly-S-LWR$^d_{q,p,\chi_3}$ *and* $^d_{q,p,\chi_3}$ *are hard. Here, $\chi_3 = U((\mathbb{Z}_q[x]/(\Phi_l(x)))^\times)$, and L is the half of the number of samples used, and such that* $\mathrm{Poly}(n) \leq L \leq n^{\ln n - 1}$.

For the case $l = 2^k$, if we set $d = \tilde{O}(1)$, $p \approx Q$ and $\sigma = \tilde{O}(\alpha \cdot n^{\frac{3}{2}})$, then $q = \tilde{O}(\alpha^2 \cdot n^5 \cdot L^2)$ is sufficient. For Poly-S-LWR problem, if we assume $L = \tilde{O}(1)$, then for $q = \tilde{O}(\alpha^2 \cdot n^5)$, a reduction from S-LWE$^M_{q,D_\alpha}$ to Poly-S-LWR$^d_{q,p,\chi_3}$ is obtained. Since for $\alpha = \tilde{O}(\alpha' \cdot n^{\frac{1}{4}})$, there is a quantum reduction from worst-case ideal/module SIVP$_{\tilde{O}(\frac{\sqrt{n}}{\alpha'})}$ to S-LWE$^M_{q,D_\alpha}$ [1, 18, 20, 24], as long as $\alpha' \cdot q \geq \tilde{O}(1)$. We could set $q = \tilde{O}(n^2)$ and $\alpha' = \tilde{O}(n^{-\frac{7}{4}})$, then a reduction from worst-case ideal/module SIVP$_{\tilde{O}(n^{\frac{9}{4}})}$ to Poly-S-LWR$^d_{q,p,\chi_3}$ (as well as the worst-case Poly-D-LWR) problem is obtained. For Poly-D-LWR$^d_{q,p,\chi_3}$ problem, parameters (mainly the poly(n)) still depend on the advantage of adversary.

5.3 Middle Product Polynomial LWR Problems

In this subsection, we set $f(x) = x^m + 1$ for some positive integer m [10]. For any $a = \sum_{i=0}^{m-1} a_i \cdot x^i \in \mathbb{Z}_q[x]/(f(x))$, define two vectors $\overrightarrow{a} := (a_0, \cdots, a_{m-1})^T$ and $\overleftarrow{a} := (a_{m-1}, \cdots, a_0)^T$. We adopt similar notations as those proposed in [26].

[10] In fact, $f(x) = x^m + c$ for any $c \in \mathbb{Z}$ is sufficient. Such $f(x)$ has advantages that some rounding operations are preserved.

Symbol $\mathbb{Z}_q^{<n}[x]$ is used to denote the set of polynomials in $\mathbb{Z}_q[x]$ of degree $< n$. For any integer $d > 0$ and $a \in \mathbb{Z}_q[x]$, we let $\mathrm{Rot}_f^d(a)$ denote the matrix in $\mathbb{Z}_q^{d\times m}$ whose i-th row is given by the coefficients of the polynomial $a \cdot x^{i-1} \bmod f$ for $i \in [d]$. We also use $\mathrm{Rot}_f(a)$ instead of $\mathrm{Rot}_f^m(a)$. We define $\mathbf{M}_f \in \mathbb{Z}_q^{m\times m}$ such that for any $1 \le i, j \le m$, the coefficient $(\mathbf{M}_f)_{i,j}$ is the constant coefficient of $x^{i+j-2} \bmod f$. Notice that in our setting, we have $\mathbf{M}_f = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & -1 & \cdots & 0 & 0 \end{pmatrix}$.

For any integers $d, k > 0$ and $a \in \mathbb{Z}_q^{<n}[x]$, we set $\mathrm{Toep}^{d,k}(a)$ to be the matrix in $\mathbb{Z}_q^{d\times(k+d-1)}$, whose i-th row is given by the coefficients of $a \cdot x^{i-1}$ for $i \in [d]$. For integers d_a, d_b, d, k such that $d_a + d_b - 1 = d + 2k$, the middle product $\odot_d : \mathbb{Z}_q^{<d_a}[x] \times \mathbb{Z}_q^{<d_b}[x] \mapsto \mathbb{Z}_q^{<d}[x]$ is defined as $a \odot_d b := \lfloor \frac{a\cdot b \bmod x^{k+d}}{x^k} \rfloor$, here terms with x^i for $i < 0$ are rounded off. For $a \in \mathbb{Z}_q^{<n+d-1}[x]$ with coefficients $(a_1, \cdots, a_{n+d-2})^T$, the Hankel matrix of a is defined as $\mathrm{Hank}(a) = \begin{pmatrix} a_0 & a_1 & \cdots & a_{d-1} & \cdots & a_{n-1} \\ a_1 & a_2 & \cdots & a_d & \cdots & a_n \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{d-1} & a_d & \cdots & a_{2d-2} & \cdots & a_{n+d-2} \end{pmatrix} \in \mathbb{Z}_q^{d\times n}$. For integers $n, d > 0$, we define the set $(\mathbb{Z}_q^{<n+d-1}[x])^\times$ consisting of polynomials of $\mathbb{Z}_q^{<n+d-1}[x]$ with Hankel matrix of full rank d.

We will need the following lemma [6, 26].

Lemma 13. *We have the following facts.*

1. *For any $a \in \mathbb{Z}_q^{<m}[x]$ and integer $0 < d < m$, we have $\mathrm{Rot}_f^d(a)\cdot(1, 0, \cdots, 0)^T = \mathbf{M}_f^d \cdot \overrightarrow{a}$.*
2. *For any integers $d, k > 0$ and any $a \in \mathbb{Z}_q^{<k}[x]$, we have $\mathrm{Rot}_f^d(a) = \mathrm{Toep}^{d,k}(a)\cdot \mathrm{Rot}_f^{k+d-1}(1)$.*
3. *For any integers $d, k > 0$, let $r \in \mathbb{Z}_q^{<k+1}[x]$, $a \in \mathbb{Z}_q^{<d+k}[x]$ and $b = r \odot_d a$. Then we have $\overrightarrow{b} = \mathrm{Toep}^{d,k+1}(r) \cdot \overleftarrow{a}$.*

The middle-product LWR problem is defined as follows.

Definition 6. *Let $n, d, p, q > 0$ be integers,*

- *For $s \in \mathbb{Z}_q^{<n+d-1}[x]$, we define the middle-product LWR distribution, denoted by $\text{MP-A}_{s,n,d,q,p}$, over $\mathbb{Z}_q^{<n}[x] \times \mathbb{Z}_p^{<d}[x]$ as the one obtained by sampling $a \hookleftarrow U(\mathbb{Z}_q^{<n}[x])$ and returning $(a, b = \lfloor a \odot_d s \rceil_{q,p})$.*
- *The (average-case) middle-product search LWR problem, denoted by $\text{MP-S-LWR}_{n,d,q,p}$, consists in recovering $s \in \mathbb{Z}_q^{<n+d-1}[x]$ with non-negligible probability for $s \hookleftarrow U((\mathbb{Z}_q^{<n+d-1}[x])^\times)$, when given a polynomial number samples from $\text{MP-A}_{s,n,d,q,p}$.*
- *The (average-case) middle-product decision LWR problem, denoted by $\text{MP-D-LWR}_{n,d,q,p}$, consists in distinguishing between a polynomial number of samples from $\text{MP-A}_{s,n,d,q,p}$ and the same number of samples from $U(\mathbb{Z}_q^{<n}[x] \times \mathbb{Z}_p^{<d}[x])$, with non-negligible probability over the choice $s \hookleftarrow U((\mathbb{Z}_q^{<n+d-1}[x])^\times)$.*

As usual, the worst-case middle-product search/decision LWR problem, denoted by W-MP-S/D-LWR, could be defined by asking an adversary to recover s (or distinguishing corresponding distributions) with probability ≈ 1 for some arbitrary $s \in (\mathbb{Z}_q^{<n+d-1}[x])^\times$. Here, we choice to constrain $s \in (\mathbb{Z}_q^{<n+d-1}[x])^\times$ in order to connecting MP-S/D-LWR problem to worst-case ideal lattice problems, due to the following observation.

Lemma 14. *Let d, n be positive integers. For any $s \in (\mathbb{Z}_q[x]/(f(x)))^\times$, set $s' \in \mathbb{Z}_q^{<n+d-1}[x]$ with $\overleftarrow{s'} = \mathrm{Rot}_f^{n+d-1}(1) \cdot \mathrm{Rot}_f(s) \cdot (1, 0, \cdots, 0)^T$. Then, we have that the rank of $\mathrm{Hank}(s')$ is d, i.e. $s' \in (\mathbb{Z}_q^{<n+d-1}[x])^\times$.*

Proof. First notice that, by our choice of $f(x)$, $s \in (\mathbb{Z}_q[x]/(f(x)))^\times$ if and only if $\mathrm{Rot}_f(s)$ is invertible in $\mathbb{Z}_q^{m \times m}$, since multiplication induced by s in the ring $\mathbb{Z}_q[x]/(f(x))$ corresponds to matrix $\mathrm{Rot}_f^T(s)$. A direct calculation shows that

$$\overleftarrow{s'} = (s_0, -s_{m-1}, \cdots, -s_1, -s_0, s_{m-1}, \cdots)^T \in \mathbb{Z}_q^{n+d-1}.$$

Therefore, if we define $s'' \in \mathbb{Z}_q^{<n+d-1}[x]$ such that $\overrightarrow{s''} = \overleftarrow{s'}$, then we get

$$\mathrm{Hank}(s'') = \begin{pmatrix} s_0 & -s_{m-1} & -s_{m-2} & \cdots & -s_1 & \cdots \\ -s_{m-1} & -s_{m-2} & -s_{m-3} & \cdots & -s_0 & \cdots \\ -s_{m-2} & -s_{m-3} & -s_{m-4} & \cdots & s_{m-1} & \cdots \\ \vdots & \vdots & \vdots & & \vdots & \\ -s_{m-d+1} & -s_{m-d} & -s_{m-d-1} & \cdots & s_{m-d+2} & \cdots \end{pmatrix}_{d \times n}.$$

So, the first m columns of $\mathrm{Hank}(s'')$ is the matrix which is consisted of the first column of $\mathrm{Rot}_f(s)$ and the last $d-1$ columns of $\mathrm{Rot}_f(s)$ up to a fact -1. Hence, the rank of $\mathrm{Hank}(s'')$ is d, and so is the rank of $\mathrm{Hank}(s')$.

Now, we could deduce the following reduction.

Theorem 6. *For integers $d \le m \le n$ and modulus $p|q$, there is a* PPT *reduction from search/decision polynomial LWR problems defined over $\mathbb{Z}_q[x]/(f(x)) \times \mathbb{Z}_p[x]/(f(x))$ to* W-MP-S/D-LWR$_{n,d,q,p}$.

Proof. Given an instance $(a, b) \in \mathbb{Z}_q[x]/(f(x)) \times \mathbb{Z}_p[x]/(f(x))$ with $b = \lfloor a \cdot s \rceil_{q,p}$ for some $s \in \mathbb{Z}_q[x]/(f(x))$, we set $a' = a + f \cdot r \in \mathbb{Z}_q^{<n}[x]$ with $r \hookleftarrow U(\mathbb{Z}_q^{<(n-m)}[x])$, and analyze the term $\mathbf{M}_f^d \cdot \overrightarrow{b}$. We have

$$\begin{aligned}
&\mathbf{M}_f^d \cdot \overrightarrow{b} \\
&= \mathrm{Rot}_f^d(\lfloor a \cdot s \rceil_{q,p}) \cdot (1, 0, \cdots, 0)^T && \text{(By Lemma 13)} \\
&= \lfloor \mathrm{Rot}_f^d(a \cdot s) \cdot (1, 0, \cdots, 0)^T \rceil_{q,p} && (f \text{ is rounding-preserved}) \\
&= \lfloor \mathrm{Rot}_f^d(a) \cdot \mathrm{Rot}_f(s) \cdot (1, 0, \cdots, 0)^T \rceil_{q,p} && \text{(By definition)} \\
&= \lfloor \mathrm{Rot}_f^d(a') \cdot \mathrm{Rot}_f(s) \cdot (1, 0, \cdots, 0)^T \rceil_{q,p} && (a = a' \bmod f) \\
&= \lfloor \mathrm{Toep}^{d,n}(a') \cdot \mathrm{Rot}_f^{n+d-1}(1) \cdot \mathrm{Rot}_f(s) \cdot (1, 0, \cdots, 0)^T \rceil_{q,p}. && \text{(By Lemma 13)}
\end{aligned}$$

Therefore, we get $\mathbf{M}_f^d \cdot \overrightarrow{b} = \lfloor a' \odot_d s' \rceil_{q,p}$, where $s' \in \mathbb{Z}_q^{<n+d-1}[x]$ and $\overleftarrow{s'} = \mathrm{Rot}_f^{n+d-1}(1) \cdot \mathrm{Rot}_f(s) \cdot (1, 0, \cdots, 0)^T$ by Lemma 13.

For search variant problems, we need to note that the first row of matrix $\mathrm{Rot}_f^{n+d-1}(1) \cdot \mathrm{Rot}_f(s)$ is a re-order of coefficients of s. So, if one could recover $\overleftarrow{s'}$, he could also recover s easily. For decision variant problems, we only need to notice that $\mathbf{M}_f^d \cdot \overrightarrow{b} \hookleftarrow U(\mathbb{Z}_p^{<d}[x])$ if $b \hookleftarrow U(\mathbb{Z}_p[x]/(f(x)))$, due to the special form of $\mathbf{M}_f$.

Results showed in Theorem 6 are not satisfactory. Since we do't know how to show the average-case hardness of MP-D-LWR problems. The main obstacle is that the secret re-randomizing technique could not be used here. For search variant problems, it's possible to reduce MP-LWE problems to MP-LWR problems via the Rényi divergence. While for MP-D-LWR problems, no known results have been showed.

In fact, if we define $\mathcal{S}_f = \{s' \in \mathbb{Z}_q^{<n+d-1}[x] : \exists\ s \in \mathbb{Z}_q[x]/(f(x)),\ \text{s.t. } \overleftarrow{s'} = \mathrm{Rot}_f^{n+d-1}(1) \cdot \mathrm{Rot}_f(s) \cdot (1, 0, \cdots, 0)^T\}$, which is a subset of $(\mathbb{Z}_q^{<n+d-1}[x])^\times$ by Lemma 14, Theorem 6 also gives a reduction from average-case Poly-D-LWR problems defined over $\mathbb{Z}_q[x]/(f(x))$ with secrets $s \hookleftarrow U((\mathbb{Z}_q[x]/(f(x)))^\times)$ to average-case MP-D-LWR problems with secrets $s \hookleftarrow U(\mathcal{S}_f)$. Thus, Combining our results in Subsection 5.2, for secrets $s \hookleftarrow U(\mathcal{S}_f)$ and m a power-of-2 integer, the hardness of corresponding MP-LWR problems could be guaranteed by worst-case ideal lattice problems defined over corresponding number field.

This is also not satisfactory, since it violate the original intention for designing middle-product LWE/LWR problems. It classifies the secrets of MP-LWR problems in set $(\mathbb{Z}_q^{<n+d-1}[x])^\times$. Different category seems to have different security level. However, for search variant problems, there seems to be no such divergence (via MP-S-LWE $\mapsto$ MP-S-LWR approach). We just proposed our partial results about MP-D-LWR problems here. Whether we could show the average-case hardness of MP-D-LWR problems with secrets over $(\mathbb{Z}_q^{<n+d-1}[x])^\times$ or $\mathbb{Z}_q^{<n+d-1}[x]$ needs further discussions.

Acknowledgement: The authors are supported by the National Key Research and Development Program of China (Grant No. 2018YFA0704702), and the National Natural Science Foundation of China (Grant No. 61832012).

A Missing proofs of Section 3

Proof of Lemma 5: In order to find $\boldsymbol{s} \bmod \mathfrak{p}_i R^\vee = (s_1 \bmod \mathfrak{p}_i R^\vee, \cdots, s_d \bmod \mathfrak{p}_i R^\vee)$, we try to find each of the d coordinates of $\boldsymbol{s}$ by using the $\text{W-D-LWR}_{\mathcal{S}_B,q,p,\chi}^{M,i}$ oracle $\mathfrak{O}$. Since prime p is well-split, we have $|N(\mathfrak{p}_i)| \leq \mathrm{poly}(n)$ and there are only $\mathrm{poly}(n)$ many candidates of $s_j \bmod \mathfrak{p}_i R^\vee$. Therefore, it is possible to try them all in order to find the correct one.

Fix an arbitrary $B \in \mathcal{S}_B$, to find $s_1 \bmod \mathfrak{p}_i R^\vee$, we first sample y uniformly at random $\bmod\ \mathfrak{p}_i R^\vee$, and set $y = 0 \bmod \mathfrak{p}_j R^\vee$ for all $j \neq i$. Then, we sample h

uniformly at random over mod $\mathfrak{p}_j R^\vee$ for all $j \le i-1$, and set $h = 0 \bmod \mathfrak{p}_j R^\vee$ for other $j \ge i$. Let $x \bmod \mathfrak{p}_i R^\vee \in R^\vee/\mathfrak{p}_i R^\vee$ be the guess of $s_1 \bmod \mathfrak{p}_i R^\vee$, we transfer $(\boldsymbol{a}', b') := (\boldsymbol{a} + \frac{q}{p} \cdot (y, 0, \cdots, 0)^T, b + h + x \cdot y)$ to the oracle $\mathfrak{O}$ and output the corresponding $x \bmod \mathfrak{p}_i R^\vee$ if $\mathfrak{O}$ returns $i-1$. Note that $p|q$, we have $b' = b + h + x \cdot y = \lfloor \sum_{i=1}^d a_i \cdot s_i \rceil_{B,q,p} + h + x \cdot y = \lfloor (\boldsymbol{a}')^T \cdot \boldsymbol{s} \rceil_{B,q,p} + h + y \cdot (x - s_1) \bmod pR^\vee$. If $x = s_1 \bmod \mathfrak{p}_i R^\vee$, then by our choice of y and CRT, we get that $(\boldsymbol{a}', b')$ is distributed identically to $A^{M,i-1}_{q,p,\boldsymbol{s}}(B)$; while if $x \neq s_1 \bmod \mathfrak{p}_i R^\vee$, we have $y \cdot (x - s_1) \hookleftarrow U(R^\vee/\mathfrak{p}_i R^\vee)$ since $R^\vee/\mathfrak{p}_i R^\vee$ is a finite field, and $(\boldsymbol{a}', b')$ is distributed identically to $A^{M,i}_{q,p,\boldsymbol{s}}(B)$. Hence, by attempting at most $\mathrm{poly}(n)$ guesses, we could recover $s_1 \bmod \mathfrak{p}_i R^\vee$ with the help of $\mathfrak{O}$.

Repeating the above process d times enable us to recover $s_j \bmod \mathfrak{p}_i R^\vee$ for all $j \in [d]$.

Before proving Lemma 6, we give the formal definition of *worst-case* decision LWR problems.

Definition 7. *Let $K, R, R^\vee, B, q, p, \chi$ be the same as defined in Section 3, the worst-case decision LWR problems, denoted by* $\text{W-D-LWR}^M_{B,q,p,\chi}$ *is: distinguish a polynomially many samples which are sampled from either $A^M_{q,p,\boldsymbol{s}}(B)$ or $U(R_q^d \times R_p^\vee)$ with probability ≈ 1 for some arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi^d)$.*

Proof of Lemma 6: First, we could deduce that for any basis $B \in \mathcal{S}_B$, the $\text{W-D-LWR}^M_{B,q,p,\chi}$ problem is equivalent to each other via a similar calculation as Lemma 2. Fix an arbitrary $B \in \mathcal{S}_B$ and an arbitrary $\boldsymbol{s} \in \mathrm{Supp}(\chi^d)$, assume there exists an oracle $\mathfrak{O}$ which could solve $\text{W-D-LWR}^M_{B,q,p,\chi}$ with advantage $\delta \approx 1$. If we define a sequence of distributions $\mathrm{Dist}_i := A^{M,i}_{q,p,\boldsymbol{s}}(B)$ for $i \in \{0, 1, \cdots, \mathfrak{g}\}$, then $\delta = |\Pr[\mathfrak{O}(A^{M,0}_{q,p,\boldsymbol{s}}(B)) = 1] - \Pr[\mathfrak{O}(A^{M,\mathfrak{g}}_{q,p,\boldsymbol{s}}(B)) = 1]|$ and we have

$$\begin{aligned}\delta &\le \sum_{i=1}^{\mathfrak{g}} |\Pr[\mathfrak{O}(A^{M,i-1}_{q,p,\boldsymbol{s}}(B)) = 1] - \Pr[\mathfrak{O}(A^{M,i}_{q,p,\boldsymbol{s}}(B)) = 1]| \\ &= \sum_{i=1}^{\mathfrak{g}} \delta_i \le \mathfrak{g} \cdot \delta_{\max},\end{aligned}$$

where $\delta_i := |\Pr[\mathfrak{O}(A^{M,i-1}_{q,p,\boldsymbol{s}}(B)) = 1] - \Pr[\mathfrak{O}(A^{M,i}_{q,p,\boldsymbol{s}}(B)) = 1]|$ is the advantage of an adversary $\mathfrak{O}$ to solve $\text{W-D-LWR}^{M,i}_{\mathcal{S}_B,q,p,\chi}$ problem, and $\delta_{\max} = \max_{i \in [\mathfrak{g}]} \delta_i$. Therefore, if oracle $\mathfrak{O}$ could solve $\text{W-D-LWR}^M_{B,q,p,\chi}$ problem, it could also solve $\text{W-D-LWR}^{M,i^*}_{\mathcal{S}_B,q,p,\chi}$ problem for at least one $i^* \in [\mathfrak{g}]$ with probability $\gtrsim \frac{1}{\mathfrak{g}}$. Repeating $\mathfrak{g}$ times could ensure that $\mathfrak{O}$ could be used to solve $\text{W-D-LWR}^{M,i^*}_{\mathcal{S}_B,q,p,\chi}$ with probability ≈ 1.

Note that for any $s \in (R_q^\vee \cap R_p^\vee)^\times$, $s \cdot r \hookleftarrow U((R_q^\vee \cap R_p^\vee)^\times)$ if $r \hookleftarrow U(R_q^\times)$. For a given $(\boldsymbol{a}, b) \in R_q^d \times R_p^\vee$, we consider the map $f_{\boldsymbol{r}} : R_q^d \times R_p^\vee \mapsto R_q^d \times R_p^\vee$ defined by $f_{\boldsymbol{r}}((\boldsymbol{a}, b)) := (\boldsymbol{a}', b)$ for $\boldsymbol{r} = (r_1, \cdots, r_d)^T \in (R_q^\times)^d$, where $\boldsymbol{a}' = (a_1 \cdot r_1, \cdots, a_d \cdot r_d)^T$. If $(\boldsymbol{a}, b)$ comes from uniform distribution, so are $(\boldsymbol{a}', b)$.

While if $(\boldsymbol{a}, b)$ is sampled from $A^M_{q,p,\boldsymbol{s}}(B)$ for some arbitrary $\boldsymbol{s} \in (R_q^\vee \cap R_p^\vee)^\times$, we have $b = \lfloor (\boldsymbol{a}')^T \cdot \boldsymbol{s}' \rceil_{B,q,p}$, where $\boldsymbol{s}' = (s_1 \cdot r_1^{-1}, \cdots, s_d \cdot r_d^{-1})^T \hookleftarrow U(((R_q^\vee \cap R_p^\vee)^\times)^d)$.

Now assume there exists an oracle $\mathfrak{O}'$ which could solve D-LWR$^M_{B,q,p,\chi}$ with non-negligible probability $\delta' \geq \frac{1}{n^{c_1+c_2}}$. Here, we assume for n^{-c_1} of all possible $\boldsymbol{s}$, the acceptance probability of $\mathfrak{O}'$ on inputs from $A^M_{q,p,\boldsymbol{s}}(B)$ and on inputs from U differ by at least n^{-c_2}. Let $\mathcal{D}$ denote the output distribution of D-LWR$^M_{B,q,p,\chi}$ problem. Repeat the following n^{c_1+1} times: choose a vector $\boldsymbol{r} \hookleftarrow U((R_q^\times)^d)$, then estimate the acceptance probability of $\mathfrak{O}'$ on U and $f_{\boldsymbol{r}}(\mathcal{D})$ by calling $\mathfrak{O}'$ $32 \cdot n^{2c_2+1}$ times on each of the input distributions. If the two estimates differ by more than $\frac{n^{-c_2}}{2}$, then we stop and decide to accept. Otherwise we continue. If the procedure ends without accepting, we reject. The correctness could be obtained via a standard analysis as in [25].

(**The detailed analyses are proposed as follows.**) We assume $\Pr[\mathfrak{O}'(U) = 1] = p_U$ and $\Pr[\mathfrak{O}'(A^M_{q,p,\boldsymbol{s}}(B)) = 1] = p_{A,\boldsymbol{s}}$, then for n^{-c_1} of all possible $\boldsymbol{s}$, we have $|p_U - p_{A,\boldsymbol{s}}| \geq n^{-c_2}$. The distribution of the outputs of $\mathfrak{O}'$ could be regarded as a binomial distribution. We try to estimate the value of p_U (and $p_f := \Pr[\mathfrak{O}'(f_{\boldsymbol{r}}(\mathcal{D})) = 1]$) by repeating enough measurements. Namely, we count the number of acceptances outputted by $\mathfrak{O}'$ on input U (denoted by N_U) and $f_{\boldsymbol{r}}(\mathcal{D})$ (denoted by N_f). We also compute $\hat{p}_U = \frac{N_U}{N}$ and $\hat{p}_f = \frac{N_f}{N}$ with $N = 32 \cdot n^{2c_2+1}$. By Hoeffding's bound, we get

$$\Pr[|\hat{p}_U - p_U| \geq t] \leq 2e^{-2N \cdot t^2}$$

and

$$\Pr[|\hat{p}_f - p_f| \geq t] \leq 2e^{-2N \cdot t^2}.$$

If we take $t = \frac{1}{8} \cdot n^{-c_2}$, we have $\Pr[|\hat{p}_U - p_U| \geq \frac{1}{8} \cdot n^{-c_2}] \leq 2e^{-n}$. Therefore, if $\mathcal{D} = U$, we have $|\hat{p}_U - \hat{p}_f| \leq |\hat{p}_U - p_U| + |p_U - \hat{p}_f| < \frac{1}{4} \cdot n^{-c_2} < \frac{1}{2} \cdot n^{-c_2}$ with probability $(1 - 2e^{-n})^2 > 1 - 4e^{-n}$. While if $\mathcal{D} = A^M_{q,p,\boldsymbol{s}'}(B)$ and $\boldsymbol{s}'$ falls in the n^{-c_1} parts of all possible $\boldsymbol{s}$, we have

$$|\hat{p}_U - \hat{p}_f| = |\hat{p}_U - p_U + p_U - p_{A,\boldsymbol{s}'} + p_{A,\boldsymbol{s}'} - \hat{p}_f| \geq \frac{1}{2} \cdot n^{-c_2}$$

with probability $\geq 1 - 4e^{-n}$. Since $\{\boldsymbol{s}'\}$'s are distributed independently at random, the probability that there exists at least one time such that the corresponding $\boldsymbol{s}'$ falls in the n^{-c_1} parts of all possible $\boldsymbol{s}$ is $1 - (1 - n^{-c_1})^{n^{c_1+1}} \geq 1 - e^{-n}$. Hence, with probability $\geq 1 - 5e^{-n}$, correctness holds.

B Worst-Case Hardness of Extended LWR Problems

There are quantum reductions from worst-case basic ideal lattice problems (e.g. SIVP$_\gamma$) over K to search Ring/Module LWE problems [18, 20]. However, for S-LWE problems, the error distributions are worst-case in the sense that one need to solve corresponding S-LWE problems with error distributions coming from a set of distributions (e.g. $\Psi_{\leq\alpha}$ [18, 20]). It is possible to amend the error

distributions to some spherical Gaussians [1, 20, 24] via a Rényi divergence arguments. Parameters of the resulted error distributions depend on the number of samples used. So, we choose to use a single error distribution (and will use $\psi = D_\alpha$ for some $\alpha > 0$) to discuee S-LWE problems for convenience. Note that, we usually have $\alpha \leq \sqrt{\frac{\log n}{n}}$ in applications. Meanwhile, if we constrain secrets to the set $(R_q^\vee)^\times$, the hardness of the corresponding problem does not decrease. We'll still use $\text{S-LWE}_{q,\psi}^M$ to denote corresponding problems.

Assume B is an arbitrary basis of $R^\vee$. For any $\boldsymbol{e} \hookleftarrow D_\alpha$, assume $\boldsymbol{e} = B \cdot \boldsymbol{e}'$ [11] with coefficient vertor $\boldsymbol{e}' \in \mathbb{R}^n$. We want to modify the distribution of $\boldsymbol{e}'$ to some sphere Gaussian distribution. To do so, we choose $\boldsymbol{e}'' \hookleftarrow D_{\sqrt{\Sigma}}$ with $\Sigma = \sigma^2 \cdot I - \alpha^2 \cdot B^{-1} \cdot B^{-T}$ and $\sigma > \alpha \cdot \mathfrak{s}_1(B^{-1})$ first. Then, add $B \cdot \boldsymbol{e}''$ to the b-component of LWE samples. The coefficients of the revised error $\boldsymbol{e} + B \cdot \boldsymbol{e}''$ is $B^{-1} \cdot \boldsymbol{e} + \boldsymbol{e}''$, which is distributed as D_σ by [11, Proposition 3.2].

Given two distributions X and Y, we define $\text{RD}_2(X||Y) = E_{a \hookleftarrow X}[\frac{\Pr[X=a]}{\Pr[Y=a]}]$.

We need the following standard fact, which is slightly better than the results showed in [2], about the Gaussian distribution.

Lemma 15. *For any $C > 0$ and 1-dimensional Gaussian distribution D_s, we have*

$$\Pr_{x \hookleftarrow D_s}[|x| \geq C \cdot s] \leq e^{-\pi \cdot C^2}.$$

Proof. We will use the following tail bound, which comes from [13] to prove this lemma:

$$\frac{1}{\sqrt{2\pi}} \cdot \int_z^{+\infty} e^{-\frac{x^2}{2}} \mathrm{d}x \leq \frac{1}{2} \cdot e^{-\frac{z^2}{2}}.$$

We have

$$\begin{aligned} \Pr_{x \hookleftarrow D_s}[|x| \geq C \cdot s] &= 2 \int_{C \cdot s}^{+\infty} \frac{1}{s} \cdot e^{-\pi \cdot \frac{x^2}{s^2}} \mathrm{d}x \\ &= \frac{2}{\sqrt{2\pi}} \int_{C \cdot \sqrt{2\pi}}^{+\infty} e^{-\frac{y^2}{2}} \mathrm{d}y \\ &\leq e^{-\pi \cdot C^2}, \end{aligned}$$

as desired.

Now, we could show the worst-case hardness of extended LWR problems.

Lemma 16. *Let B be an arbitrary basis of $R^\vee$, there is a* PPT *reduction from* $\text{S-LWE}_{q,D_\alpha}^M$ *to* $\text{Ext-S-LWR}_{B,q,p,\chi'}^M$ *for modulus $q = Q \cdot p$ with $\gcd(p, Q) = 1$ and $q \geq \max\{p, Q\} \cdot \frac{\sigma}{\sqrt{\pi}} \cdot \ln n \cdot n \cdot L$, where $\sigma > \alpha \cdot \mathfrak{s}_1(B^{-1})$, and L is (half of) the number of samples used, and such that $L \leq n^{\ln n - 1}$.*

[11] Notice that, we use B to simplify formulation. Here, it should be $\varphi(B)$

Proof. When given two LWE sample $(\boldsymbol{a}_1, b_1 = \boldsymbol{a}_1^T \cdot \boldsymbol{s} + e_1)$ and $(\boldsymbol{a}_2, b_2 = \boldsymbol{a}_2^T \cdot \boldsymbol{s} + e_2)$ with $e_1, e_2 \hookleftarrow D_\alpha$, we sample $e_1', e_2' \hookleftarrow D_{\sqrt{\Sigma}}$, where $\Sigma = \sigma^2 \cdot I - \alpha^2 \cdot B^{-1} \cdot B^{-T}$ with $\sigma > \alpha \cdot \mathfrak{s}_1(B^{-1})$. Let $\mathcal{X}_{\boldsymbol{s}}$ denote the distribution of $(\boldsymbol{a}_1, \boldsymbol{a}_2, \lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q}, \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p})$, and $\mathcal{Y}_{\boldsymbol{s}}$ denote the distribution of $(\boldsymbol{a}_1, \boldsymbol{a}_2, \lfloor b_1 + e_1' \rceil_{B,q,Q}, \lfloor b_2 + e_2' \rceil_{B,q,p})$. Next, we want to bound

$$\begin{aligned}
&\mathrm{RD}_2(\mathcal{X}_{\boldsymbol{s}} || \mathcal{Y}_{\boldsymbol{s}}) \\
&= E_{\boldsymbol{a}_1, \boldsymbol{a}_2 \hookleftarrow U(R_q^d)}[\frac{\Pr[\mathcal{X}_{\boldsymbol{s}} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q}, \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p})]}{\Pr[\mathcal{Y}_{\boldsymbol{s}} = (\boldsymbol{a}_1, \boldsymbol{a}_2, \lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} + e_1'' \rceil_{B,q,Q}, \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} + e_2'' \rceil_{B,q,p})]}] \\
&= E_{\boldsymbol{a}_1, \boldsymbol{a}_2 \hookleftarrow U(R_q^d)}[\frac{1}{\mathrm{pro}}],
\end{aligned}$$

where $e_i'' = e_i + e_i'$, and $\mathrm{pro} = \Pr_{e_i, e_i'}[(\lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} + e_1 + e_1' \rceil_{B,q,Q}, \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} + e_2 + e_2' \rceil_{B,q,p}) = (\lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q}, \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p})]$ for $i = 1, 2$. Notice that $\boldsymbol{a}_1$ is independent from $\boldsymbol{a}_2$, the coefficients of $\boldsymbol{a}_1^T \cdot \boldsymbol{s}$ and $\boldsymbol{a}_2^T \cdot \boldsymbol{s}$ are all independent from each other, and are distributed uniformly over $\mathbb{Z}_q$ since we have constrained $\boldsymbol{s}_i \in (R_q^\vee)^\times$ for $i \in [2]$. Hence, we get

$$\begin{aligned}
\mathrm{pro} = \Pr_{e_1, e_1'}[\lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} + e_1 + e_1' \rceil_{B,q,Q} = \lfloor \boldsymbol{a}_1^T \cdot \boldsymbol{s} \rceil_{B,q,Q}] \\
\cdot \Pr_{e_2, e_2'}[\lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} + e_2 + e_2' \rceil_{B,q,p} = \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p}].
\end{aligned}$$

Assume without loss of generality that $Q < p$. The coefficients of error $e_2 + e_2'$ with respect to basis B obeys to the distribution D_σ. By using Lemma 15 with $C = \frac{\ln n}{\sqrt{\pi}}$, the absolute value of each coefficient of $e + e'$ is bounded by $N := \frac{\sigma}{\sqrt{\pi}} \cdot \ln n$ with probability $\delta = 1 - n^{-\ln n}$. Now, we could analyze the rounding operation by coefficient. Define the bounder elements in $\mathbb{Z}_q$ with respect to N and modulus p, q by

$$\mathrm{Bor}_{q,p}(N) := \{x \in \mathbb{Z}_q : \lfloor x + N \rceil_{q,p} \neq \lfloor x \rceil_{q,p}\},$$

then it yields $|\mathrm{Bor}_{q,p}(N)| \leq N \cdot p$, since by our choice of parameters, we have $Q > N$. For $0 \leq t \leq n$, let's also define

$$\mathrm{Bad}_{\boldsymbol{s},t} := \{\boldsymbol{a} \in R_q^d : |\{i \in [n] : (\boldsymbol{a}^T \cdot \boldsymbol{s})_i \in \mathrm{Bor}_{q,p}(N)\}| = t\}.$$

Now, for any fixed t and $\boldsymbol{a} \in \mathrm{Bad}_{\boldsymbol{s},t}$, if $(\boldsymbol{a}^T \cdot \boldsymbol{s})_i \notin \mathrm{Bor}_{q,p}(N)$ for $i \in [n]$, we have $\Pr_{e_2, e_2'}[\lfloor (\boldsymbol{a}^T \cdot \boldsymbol{s} + e_2 + e_2')_i \rceil_{q,p} = \lfloor (\boldsymbol{a}^T \cdot \boldsymbol{s})_i \rceil_{q,p}] \geq \delta$. While, if $(\boldsymbol{a}^T \cdot \boldsymbol{s})_i \in \mathrm{Bor}_{q,p}(N)$, we have $\Pr_{e_2, e_2'}[\lfloor (\boldsymbol{a}^T \cdot \boldsymbol{s} + e_2 + e_2')_i \rceil_{q,p} = \lfloor (\boldsymbol{a}^T \cdot \boldsymbol{s})_i \rceil_{q,p}] \geq \frac{1}{2}$, since the distribution of one-dimension Gaussian distribution D_σ is balanced [12]. In this case, we get $\Pr_{e_2, e_2'}[\lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} + e_2 + e_2' \rceil_{B,q,p} = \lfloor \boldsymbol{a}^T \cdot \boldsymbol{s} \rceil_{B,q,p}] \geq \frac{\delta^{n-t}}{2^t} \geq \frac{\delta^n}{2^t}$. Note that,

$$\Pr[\boldsymbol{a} \in \mathrm{Bad}_{\boldsymbol{s},t}] \leq \binom{n}{t} \cdot (1 - \frac{|\mathrm{Bor}_{q,p}(N)|}{q})^{n-t} \cdot (\frac{|\mathrm{Bor}_{q,p}(N)|}{q})^t,$$

[12] I.e. $\Pr_{x \hookleftarrow D_\sigma}[x \geq 0] = \Pr_{x \hookleftarrow D_\sigma}[x \leq 0] \geq \frac{1}{2}$.

we have

$$
\begin{aligned}
&E_{\boldsymbol{a}_2 \hookleftarrow U(R_q^d)}[\frac{1}{\Pr_{e_2,e_2'}[\lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} + e_2 + e_2' \rceil_{B,q,p} = \lfloor \boldsymbol{a}_2^T \cdot \boldsymbol{s} \rceil_{B,q,p}]}] \\
&\leq \sum_{t=0}^{n} \sum_{\boldsymbol{a} \in \mathrm{Bad}_{\boldsymbol{s},t}} \delta^{-n} \cdot 2^t \\
&= \delta^{-n} \cdot \sum_{t=0}^{n} \binom{n}{t} \cdot (1 - \frac{|\mathrm{Bor}_{q,p}(N)|}{q})^{n-t} \cdot (2 \cdot \frac{|\mathrm{Bor}_{q,p}(N)|}{q})^t \\
&= \delta^{-n} \cdot (1 + \frac{|\mathrm{Bor}_{q,p}(N)|}{q})^n \leq \delta^{-n} \cdot (1 + \frac{pN}{q})^n.
\end{aligned}
$$

Therefore, we could deduce that

$$
\mathrm{RD}_2(\mathcal{X}_{\boldsymbol{s}} || \mathcal{Y}_{\boldsymbol{s}})^L \leq \frac{(1 + \frac{pN}{q})^{2nL}}{\delta^{2nL}} \leq (\frac{1 + (nL)^{-1}}{1 - (nL)^{-1}})^{2nL} \leq e^4,
$$

where we have use the fact that $\delta = 1 - n^{-\ln n} \geq 1 - \frac{1}{nL}$ for $L \leq n^{\ln n - 1}$. By the property of Rényi divergence, we get the desire results.

References

1. Albrecht, M.R., Deo, A.: Large modulus ring-lwe ≥ module-lwe. Cryptology ePrint Archive, Report 2017/612 (2017), https://eprint.iacr.org/2017/612
2. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. Journal of Mathematical Cryptology **9**(3), 169 – 203 (2015)
3. Alperin-Sheriff, J., Apon, D.: Dimension-preserving reductions from lwe to lwr. Cryptology ePrint Archive, Report 2016/589 (2016)
4. Alwen, J., Krenn, S., Pietrzak, K., Wichs, D.: Learning with rounding, revisited. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013. pp. 57–74. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
5. Baan, H., Bhattacharya, S., Fluhrer, S., Garcia-Morchon, O., Laarhoven, T., Rietman, R., Saarinen, M.J.O., Tolhuizen, L., Zhang, Z.: Round5: Compact and fast post-quantum public-key encryption. In: Ding, J., Steinwandt, R. (eds.) Post-Quantum Cryptography. pp. 83–102. Springer International Publishing, Cham (2019)
6. Bai, S., Boudgoust, K., Das, D., Roux-Langlois, A., Wen, W., Zhang, Z.: Middle-product learning with rounding problem and its applications. In: Galbraith, S.D., Moriai, S. (eds.) Advances in Cryptology – ASIACRYPT 2019. pp. 55–81. Springer International Publishing, Cham (2019)
7. Banerjee, A., Peikert, C.: New and improved key-homomorphic pseudorandom functions. In: Garay, J.A., Gennaro, R. (eds.) Advances in Cryptology – CRYPTO 2014. pp. 353–370. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
8. Banerjee, A., Peikert, C., Rosen, A.: Pseudorandom functions and lattices. In: Pointcheval, D., Johansson, T. (eds.) Advances in Cryptology – EUROCRYPT 2012. pp. 719–737. Springer Berlin Heidelberg, Berlin, Heidelberg (2012)

9. Bogdanov, A., Guo, S., Masny, D., Richelson, S., Rosen, A.: On the hardness of learning with rounding over small modulus. In: Kushilevitz, E., Malkin, T. (eds.) Theory of Cryptography. pp. 209–224. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
10. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehle, D.: Crystals - kyber: A cca-secure module-lattice-based kem. In: 2018 IEEE European Symposium on Security and Privacy (EuroS P). pp. 353–367 (April 2018)
11. Brakerski, Z., Döttling, N.: Hardness of lwe on general entropic distributions. In: Canteaut, A., Ishai, Y. (eds.) Advances in Cryptology – EUROCRYPT 2020. pp. 551–575. Springer International Publishing, Cham (2020)
12. Chen, L., Zhang, Z., Zhang, Z.: On the hardness of the computational ring-lwr problem and its applications. In: Peyrin, T., Galbraith, S. (eds.) Advances in Cryptology – ASIACRYPT 2018. pp. 435–464. Springer International Publishing, Cham (2018)
13. CHIANI, M.: New exponential bounds and approximations for the computation of error probability in fading channels. IEEE Trans. Wired. Commun. **2**(4), 840–845 (2003)
14. Cohen, H.: A Course in Computational Algebraic Number Theory. 0072-5285, Springer, Berlin, Heidelberg (1993)
15. D'Anvers, J.P., Karmakar, A., Sinha Roy, S., Vercauteren, F.: Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure kem. In: Joux, A., Nitaj, A., Rachidi, T. (eds.) Progress in Cryptology – AFRICACRYPT 2018. pp. 282–305. Springer International Publishing, Cham (2018)
16. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: Crystals-dilithium: A lattice-based digital signature scheme. IACR Transactions on Cryptographic Hardware and Embedded Systems pp. 238–268 (01 2018)
17. Lai, Q., Liu, F.H., Wang, Z.: Almost tight security in lattices with polynomial moduli – prf, ibe, all-but-many ltf, and more. In: Kiayias, A., Kohlweiss, M., Wallden, P., Zikas, V. (eds.) Public-Key Cryptography – PKC 2020. pp. 652–681. Springer International Publishing, Cham (2020)
18. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography **75**(3), 565–599 (Jun 2015)
19. Liu, F.H., Wang, Z.: Rounding in the rings. In: Micciancio, D., Ristenpart, T. (eds.) Advances in Cryptology – CRYPTO 2020. pp. 296–326. Springer International Publishing, Cham (2020)
20. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010. pp. 1–23. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
21. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-lwe cryptography. In: Johansson, T., Nguyen, P.Q. (eds.) Advances in Cryptology – EUROCRYPT 2013. pp. 35–54. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
22. Peikert, C.: A decade of lattice cryptography. Found. Trends Theor. Comput. Sci. **10**(4), 283–424 (Mar 2016)
23. Peikert, C., Pepin, Z.: Algebraically structured lwe, revisited. In: Hofheinz, D., Rosen, A. (eds.) Theory of Cryptography. pp. 1–23. Springer International Publishing, Cham (2019)
24. Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-lwe for any ring and modulus. In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing. pp. 461–473. STOC 2017, ACM, New York, NY, USA (2017)

25. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 34:1–34:40 (Sep 2009)
26. Roşca, M., Sakzad, A., Stehlé, D., Steinfeld, R.: Middle-product learning with errors. In: Katz, J., Shacham, H. (eds.) Advances in Cryptology – CRYPTO 2017. pp. 283–297. Springer International Publishing, Cham (2017)
27. Rosca, M., Stehlé, D., Wallet, A.: On the ring-lwe and polynomial-lwe problems. In: Nielsen, J.B., Rijmen, V. (eds.) Advances in Cryptology – EUROCRYPT 2018. pp. 146–173. Springer International Publishing, Cham (2018)
28. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of the 35th Annual Symposium on Foundations of Computer Science. pp. 124–134. IEEE Computer Society, USA (1994)
29. Wang, Y., Wang, M.: Module-lwe versus ring-lwe, revisited. Cryptology ePrint Archive, Report 2019/930 (2019), https://eprint.iacr.org/2019/930
30. Wang, Y., Wang, M.: Provably secure ntruencrypt over any cyclotomic field. In: Cid, C., Jacobson Jr., M.J. (eds.) Selected Areas in Cryptography – SAC 2018. pp. 391–417. Springer International Publishing, Cham (2019)