On the Hardness of the Computational Ring-LWR Problem and its Applications

Long Chen[1,2], Zhenfeng Zhang[1,3(✉)], and Zhenfei Zhang[4]

[1] TCA Laboratory, State Key Laboratory of Computer Science, Institute of Software, Chinese Academy of Sciences, China
{chenlong,zfzhang}@tca.iscas.ac.cn
[2] New Jersey Institute of Technology, USA
[3] University of Chinese Academy of Sciences, China
[4] OnBoard Security Inc., Wilmington, USA
zzhang@onboardsecurity.com

Abstract. In this paper, we propose a new assumption, the *Computational Learning With Rounding over rings*, which is inspired by the computational Diffie-Hellman problem. Assuming the hardness of R-LWE, we prove this problem is hard when the secret is small, uniform and invertible. From a theoretical point of view, we give examples of a key exchange scheme and a public key encryption scheme, and prove the worst-case hardness for both schemes with the help of a random oracle. Our result improves both speed, as a result of not requiring Gaussian secret or noise, and size, as a result of rounding. In practice, our result suggests that decisional R-LWR based schemes, such as Saber, Round2 and Lizard, which are among the most efficient solutions to the NIST post-quantum cryptography competition, stem from a provable secure design. There are no hardness results on the decisional R-LWR with polynomial modulus prior to this work, to the best of our knowledge.

1 Introduction

Organizations and research groups are looking for candidate algorithms to replace RSA and ECC based schemes [48, 49] due to the threat of quantum computers [58]. Among all candidates, lattice based solutions seem to offer the most promising solutions. One of the fundamental features enabled by the Learning With Errors (LWE) [57, 39] / the Small Integer Solution (SIS) [1, 45] family of problems, is that the *average-case* security of the cryptosystem stems from the *worst-case* hardness of well studied lattice problems [2, 45, 57, 51, 39, 16, 55].

The celebrated work of worst-case/average-case reductions was firstly presented in [57, 51] for LWE and in [39] for R-LWE. In both cases, the errors follow a rounded Gaussian distribution. Albeit great improvements in a sequence of work [35, 52, 29, 28, 30, 56, 13, 3, 47], Gaussian sampling is still the most intricate part to implementing (R-)LWE based schemes.

An average-case/worse-case reduction without Gaussian sampling is a long standing problem. It has been studied by a series of works from different angles

[43, 26, 44, 9, 12]. Generally, there are two ways to solve this problem. One may either reduce LWE to LWE with uniform/binary errors [43, 26, 44, 9], or reduce LWE to the Learning With Rounding (LWR) problem [10, 5, 12, 4]. Here the (R-)LWR problem, introduced in [10], is a variant of (R-)LWE where random errors are replaced by a deterministic rounding function. Interestingly, there exists a reduction from LWE with uniform errors to LWR [12] that indicates a connection between the aforementioned two solutions.

In addition to avoiding Gaussian sampling, it is also common to resort to a ring setting [39, 41, 55]. However, the above methods are no longer applicable, since the reductions from generic LWE to "binary LWE" in [43, 26, 44, 9] all rely on a search-to-decision reduction from [43]. How to carry over this reduction to the ring setting is still an open problem. Moreover, there is no reduction from R-LWE to the decisional version of R-LWR when the modulus is polynomial, to our best knowledge.[5]

Another obstacle of deploying (R-)LWE based cryptosystems is that the sizes of public keys and the ciphertexts are significantly larger than those of RSA and ECC [13]. One direction to lower the size of public keys/ciphertexts, is to choose a smaller modulus q. However, a smaller q leads to a higher (and sometime non-negligible) decryption error rate. In some cases, this may result in an invalidation of a security proof. For example, in [3], the failure probability is around 2^{-61} for a security level of 128. The security proof in [14, 3, 13] only provides an indistinguishability between a session key derived by Bob and a uniformly random string. Now that Alice and Bob may derive different session keys with a non-negligible probability, it is also essential to prove the the pseudorandomness of Alice's key. This is not captured by the existing proofs. In addition, many schemes rely on the the Fujisaki-Okamoto transformation [33] to achieve CCA-2 security. This also requires a negligible failure probability [36]. In history we have seen non-negligible failure lead to attacks, such as [37].

A trivial solution to decryption errors is to perform key validation. This, however, needs additional round trips for the protocol. An alternative solution is to further tuning the parameters. For example, to use a narrower secret/error. However, the worst-case hardness theorems for R-LWE [39, 55] require the widths of the error distributions to exceed certain $\Omega(\sqrt{n})$ bounds, where n is the degree of the secret polynomial. On the other hand, if the errors are smaller than $\sqrt{n}$, LWE can be solved in polynomial time using the Arora-Ge's algorithm [7] with $m = O(n^2)$ samples. There is a natural extension of this attack to R-LWE by viewing each R-LWE instance as n LWE samples. In general, as pointed out in [54], error distributions that are too far from the provably hard ones shall not be used, to avoid weak instances of the R-LWE problem [31, 32, 17, 18] .

Due to its great simplicity and efficiency, R-LWR based constructions, namely, Saber [24], Round2 [8], Lizard [21], Round5 [11] and OKCN[38], are among the most promising candidates to the NIST post-quantum cryptography

[5] [10] proved hardness of decisional Ring-LWR for super-polynomial q is as secure as decisional Ring-LWE for super-polynomial q. However, the hardness of decisional Ring-LWE for super-polynomial q is not well understood yet.

competition [48]. See [42] for a comparison of performance versus security among all lattice based candidates. Specifically, SABER [24] provides a decisional module-LWR based KEM, to which R-LWR can be viewed as a special case. The KEM and PKE algorithms in ROUND2 [8] may be based on *either* decisional LWR or decisional R-LWR, while the algorithms in the ring version of LIZARD [21] is based on *both* of decisional R-LWE and decisional R-LWR. Thus, the hardness of R-LWR is a long await result in the community, to show that those three schemes indeed stem from a provable secure design.

1.1 Our Contributions

In the literature, there exists a reduction from search R-LWE to search R-LWR [12], using the tool of Rényi Divergence (RD). However, it is hard to instantiate a scheme directly from this result since cryptosystems are usually based on decisional problems. On the other hand, it seems very difficult to provide a reduction from decisional R-LWE to decisional R-LWR when the modulus is polynomial, due to the limitation of RD in dealing with decisional problems [9].

To bridge this gap, we propose a new assumption, the Computational Learning With Rounding over rings (R-CLWR) in this paper, in analogy to the Computational Diffie-Hellman (CDH) assumption. Next, we provide a reduction from decisional R-LWE to R-CLWR when the secret of the R-LWE instances is uniform from the set of all invertible elements whose coefficients lie in a small interval $[-\beta, \beta]^n$ for some integer $\beta < q$. Combining the existing average-case/worst-case reduction for R-LWE [39, 55], we prove that the R-CLWR problem is hard, assuming the hardness of some worst-case lattice problems.

Applications. We give two applications of R-CLWR, a public key encryption (PKE) scheme in §5 and a Diffie-Hellman type key exchange scheme in §6. *Asymptotically speaking*, our scheme improves a classical R-LWE based solutions in two ways:

1. we allow for smaller size of public keys/ciphertexts as a result of rounding;
2. we remove the cumbersome Gaussian samplings.

We remark that it is hard to find overlaps between the concrete world and the asymptotic world. In *practice*, most of the NIST submissions and other schemes [14, 3, 13] only consider the best known cryptanalytic attacks [20, 42] and ignore the average-case/worst-case proof. For the same reason, none of the Ring-LWE/LWR based NIST candidates sample errors from rounded Gaussian. Our result is asymptotic. Thus, we do not provide a direct comparison between our scheme and the NIST submissions in this paper. Instead, we give asymptotic parameters for both R-LWE scheme and our R-CLWR based scheme for a fair comparison. In addition, we also assume that the decryption failure probability needs to be exponentially small within this asymptotic world.

	R-LWE	R-CLWR
Samples - KeyGen	2	1
Samples - Encrypt	3	1
Sampler	Gaussian	Uniform & Invertible
Modulus	$\Omega(n^{5.5}\log^{0.5} n)$	$\Omega(n^{3.75}\log^{0.25} n)$

- A R-LWE based scheme needs to proceed two Gaussian samplings during key generation and three Gaussian samplings during encryption. The modulus of the public key and the ciphertext is $q = \Omega(n^{5.5}\log^{0.5} n)$.
- A R-CLWR based scheme needs to proceed one sampling during the key generation and one sampling during the encryption. The sampling procedure is to simply draw an element from a small interval and output when it is invertible, The modulus of the public key and the ciphertext is $p = \Omega(n^{3.75}\log^{0.25} n)$.

To show the power of our result, we give security proofs for a variant of Saber and Round2, as well as Lizard, based on the R-CLWR assumption. Nonetheless, since the worst-case connection does not imply definite security for any concrete choice of parameters, our proofs will be based on asymptotic simplifications of their original algorithms.

Technique Overview. The notion of R-CLWR is inspired by the following observation. Decisional Diffie-Hellman (DDH) based schemes, such as ElGamal [34], are provable secure under the CDH assumption and the random oracle model (ROM). There, instead of distinguishing the ciphertexts of different plaintexts, the adversary needs to find a pre-image of the hash function using the public key and ciphertexts. Therefore, with the help of ROM, one converts the underlying decisional problem into a computational problem. At a high level, we apply same methodology to lattice based cryptography and reduce the security of the cryptosystem (a decisional problem) to a computational problem. In doing so, we are able to utilize the tool of RD. A similar idea is also used in the secure analysis of Newhope [3].

To present the R-CLWR problem, first, let us present a set of *interactive experiments* between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$. There exist a source $\mathcal{S}$ where the $\mathcal{C}$ gets all its input from. For simplicity, assuming all sources $\mathcal{S}$ can be partitioned in two parts: a variable part *var* that is different for distinct sources, and a constant part *con* that remains the same for all sources. We view the challenger as a function that takes inputs $X \leftarrow var$ and $aux \leftarrow con$, and outputs two quantities, Input and Target (from $\mathcal{A}$'s point of view).

Next, we are ready to describe a computational assumption based on the above experiments. Suppose there are two experiments, namely, Exp_1 and Exp_2. In Exp_1, X_1 contains a set of R-LWR samples that are sampled from var_1. In Exp_2, X_2 contains a set of uniform samples from var_2. Assuming all the rest variables in those experiments remain identical (i.e., $\mathcal{A}$ and $\mathcal{C}$), if the success probability in Exp_2 is negligible for any adversary, then, that in Exp_1 will also be negligible. Intuitively, this definition captures that, assuming all rest variables

remain the same, $\mathcal{A}$ cannot learn more information from R-LWR samples than from uniform samples.

In what it follows, we provide definitions for the R-CLWR assumption (Def. 7) and the R-CRLWE assumption (Def. 8), along with the following reductions:

$$\text{R-LWE (decisional)} \Longrightarrow \text{R-CRLWE} \Longrightarrow \text{R-CLWR}.$$

As stated earlier, the first "$\Longrightarrow$" allows us to convert a decisional problem into a computational problem, so that RD becomes applicable to the second "$\Longrightarrow$". Then, the key becomes to show that RD between an R-LWR sample $(a, \lfloor as \rfloor_p)$ and a *rounded* R-LWE sample $(a, \lfloor as + e \rfloor_p)$ is small. A natural way to obtain this result is to extend the estimation of [12] to meet the requirement of the average-case/worst-case reduction for R-LWE [39, 55]. We highlight the challenge for this task at a high level. For R-LWE, [12] requires the error distribution to be bounded, the coefficients to be independent, and the secret to be invertible over the ring. By contrast, in the first "$\Longrightarrow$" the worst case hardness results [39, 55] require the error to follow rounded Gaussian over the H space (see §2) where the secret is not necessarily invertible unless the ring R_q is also a finite field. This rules out common rings such as $x^n + 1$ with n a power of 2. We solve this issue with rejection sampling arguments. We will provide more details in §4.

It is also worth pointing out that conversions between R-LWE instances and R-LWR instances are not straightforward. For simplicity, let $(a, as+e) \in R_q^2$ be an R-LWE instance, and $(a', \lfloor a's' \rfloor_p) \in R_q \times R_p$ be an R-LWR instance. Notice that a and $as+e$ are both in R_q, while $\lfloor a's' \rfloor_p$ is in R_p. In a security proof, we need to replace $as + e$ with a random element u, and pass u to the next R-LWE instance as a public input. In comparison, for R-LWR, $\lfloor as \rfloor_p$ is in R_p instead of R_q; and it will not be a valid public input to the next R-LWR instance, unless we change the modulus for the hardness assumption from q to p. This is indeed an issue for Round2 [8], whose proof only works when q dividable by p. We solve this problem by introducing a new probabilistic function $\text{Inv}(\cdot)$ in this paper that "lifts" an R_p element back to R_q. Particularly, we have $\lfloor \text{Inv}(\lfloor a \rfloor_p) \rfloor_p = \lfloor a \rfloor_p$ and $\text{Inv}(\lfloor a \rfloor_p)$ is uniform in R_q when a is uniform in R_q. Note that q is not required to be dividable by p. This allows for NTT friendly prime q-s for efficient implementations. We will provide details in §5.

2 Preliminaries

For a set S and a probability distribution χ over S, denote by $x \leftarrow_\$ \chi$ sampling $x \in S$ according to χ. When χ is a uniform distribution over S, denote by $x \leftarrow_\$ \mathcal{U}(S)$ to sample x uniformly at random from S. For simplicity, we sometimes write it as $x \leftarrow_\$ S$. Additionally, we use $\mathcal{U}(\lfloor \mathbb{Z}_q \rfloor_p)$ to denote the distribution of $\lfloor x \rfloor_p$ where $x \leftarrow_\$ \mathcal{U}(\mathbb{Z}_q)$.

2.1 The Rounding Function

For any integer modulus $q \geq 2$, $\mathbb{Z}_q$ denotes the quotient ring of integers modulo q. We define a (floor) rounding function $\lfloor \cdot \rfloor_p : \mathbb{Z}_q \to \mathbb{Z}_p$ as $\lfloor x \rfloor_p = \lfloor (p/q) \cdot \bar{x} \rfloor \bmod p$,

where $q \geq p \geq 2$ will be apparent from the context, $\bar{x}$ is an integer congruent to $x \bmod q$. We extend $\lfloor \cdot \rceil_p$ componentwise to vectors and matrices over $\mathbb{Z}_q$, and coefficient-wise (with respect to the "power basis") to the quotient ring R_q. Note that in [10, 12, 4], LWR is defined with the function $\lfloor \cdot \rceil_p$, while it can be extended directly to $\lfloor \cdot \rfloor_p$ with a similar definition while preserving the proof. We opt to use $\lfloor \cdot \rfloor_p$ for the following reason: in the implementation when q and p are both powers of some common base b (e.g., 2), $\lfloor \cdot \rfloor_p$ is equivalent to dropping the least-significant digit(s) in base b. Moreover, $\lfloor x \rfloor_p$ is uniformly random in $\mathbb{Z}_p$ if x is uniformly random in $\mathbb{Z}_q$ when p divides q.

2.2 Rényi divergence.

In [9], Bai et al. show that Rényi divergence (RD) is a powerful tool to improve or generalize security reductions in lattice-based cryptography. The formal definition is shown below.

Definition 1 (Rényi divergence). *Let $\mathcal{P}$, $\mathcal{Q}$ be two distributions s.t. $Supp(\mathcal{P}) \subseteq Supp(\mathcal{Q})$. For $a \in (1, +\infty)$, the Rényi divergence of order a is defined by*

$$\mathsf{RD}_a(\mathcal{P} \| \mathcal{Q}) = \left(\sum_{x \in Supp(\mathcal{P})} \left(\mathcal{P}(x)^a / \mathcal{Q}(x)^{a-1} \right) \right)^{\frac{1}{a-1}}.$$

Specifically, the Rényi divergence of order $+\infty$ is given by

$$\mathsf{RD}_\infty(\mathcal{P} \| \mathcal{Q}) = \max_{x \in Supp(\mathcal{P})} \left(\mathcal{P}(x) / \mathcal{Q}(x) \right).$$

The Rényi divergence has following useful properties.

Lemma 1 ([9]). *For two distributions $\mathcal{P}$, $\mathcal{Q}$ and two families of distributions $(\mathcal{P}_i)_i$, $(\mathcal{Q}_i)_i$, the Rényi divergence verifies the following properties:*

- ***Data processing inequality.*** *For any function f, $RD_a(\mathcal{P}_f \| \mathcal{Q}_f) \leq RD_a(\mathcal{P} \| \mathcal{Q})$.*
- ***Multiplicativity.*** *$RD_a(\prod_i \mathcal{P}_i \| \prod_i \mathcal{Q}_i) = \prod_i RD_a(\mathcal{P}_i \| \mathcal{Q}_i)$.*
- ***Probability preservation.*** *For any event $E \subseteq Supp(\mathcal{Q})$ and $a \in (1, +\infty)$,*

$$\mathcal{Q}(E) \geq \mathcal{P}(E)^{a/(a-1)} / RD_a(\mathcal{P} \| \mathcal{Q}),$$

$$\mathcal{Q}(E) \geq \mathcal{P}(E) / RD_\infty(\mathcal{P} \| \mathcal{Q}).$$

2.3 Lattice and Algebra

Now we are ready to present a few well-known results related to lattice based cryptography. For more details, see [39, 54, 46, 40, 55].

Lattice. A (full-rank) lattice is a set of the form $L = \sum_{i \leq n} \mathbb{Z}\mathbf{b}_i$, where $\mathbf{b}_i$'s are linearly independent vectors in $\mathbb{R}^n$. The integer n is called the *lattice dimension*, and the $\mathbf{b}_i$'s are called a *basis* of L. The *first minimum* $\lambda_1(L)$ (resp. $\lambda_1^\infty(L)$) is the Euclidean (resp. infinity) norm of any shortest non-zero vector of L. If $\mathfrak{B} = (\mathbf{b}_i)_i$ is a basis matrix of L, the fundamental parallelepiped of $\mathfrak{B}$ is the set $P(\mathfrak{B}) = \left\{\sum_{i \leq n} c_i \mathbf{b}_i : c_i \in [0,1)\right\}$. The volume $|\det(\mathfrak{B})|$ of $P(\mathfrak{B})$ is an invariant of the lattice L, denoted by $\det(L)$. Minkowski's theorem states that $\lambda_1(L) \leq \sqrt{n}(\det L)^{1/n}$. The k-th successive minima $\lambda_k(L)$ for any $k \leq n$ is defined as the smallest r such that L contains at least k linearly independent non-zero vectors of norm $\leq r$. The dual lattice of L is defined as $L^* = \{\mathbf{c} \in \mathbb{R}^n : \forall i, \langle \mathbf{c}, \mathbf{b}_i \rangle \in \mathbb{Z}\}$.

***H* Space.** We follow the framework of [39] by working over the H *Space* to deal with ideal lattices. Recall that $H \subseteq \mathbb{R}^{s_1} \times \mathbb{C}^{s_2}$ is defined as

$$H := (x_1, \ldots, x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+s_2+j} = \overline{x_{s_1+j}},\ \forall j \in 1, \ldots, s_2$$

for some nonnegative integers s_1, s_2 with $n = s_1 + 2s_2$. As shown in [39], H is isomorphic to $\mathbb{R}^n$.

Let $f(x) \in \mathbb{Q}[x]$ be a (monic) polynomial of degree n that is irreducible over $\mathbb{R}$, and ζ be a root of $f(x)$ such that $f(\zeta) = 0$. A *number field* is then a field extension $K = \mathbb{Q}(\zeta)$ obtained by adjoining an element ζ to the rationals. There exists an isomorphism between $K \cong \mathbb{Q}[X]/(f(X))$, given by $\zeta \mapsto X$. Hence, elements in K can be represented with polynomials, using *the power basis* $\{1, \zeta, \ldots, \zeta^{n-1}\}$.

The Ring of Integers of a cyclotomic number field, denoted by R, is the set of all algebraic integers in the number field K. Hence, $R \subset K$ forms a ring under the same operations in K. In addition $\mathbb{Z}[\zeta] \cong \mathbb{Z}[X]/f(X)$ under the above isomorphism. In other words, the power basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$ for R has a $\mathbb{Z}$-basis. Looking ahead, we will use $R_q = R/qR$ to denote the localisation of R, for some modulus q. When dealing with R_q, we assume that the coefficients are in $[-q/2, q/2)$ (except for R_2 where the coefficients are in $\{0, 1\}$).

Canonical embedding. For a given f, there are n none-necessarily distinct roots or power basis. This allows us to define n embeddings $\sigma_i : K \to \mathbb{C}$ by sending ζ to one of the roots of f. The *canonical embedding* $\sigma : K \to \mathbb{C}^n$ is the concatenation of all the embeddings for n, i.e. $\sigma(a) = (\sigma_i(a))_{i \in n}, a \in K$. Let $\mathbf{R}$ be an $n \times n$ Vandermonde matrix

$$\mathbf{R} = \begin{pmatrix} 1, \sigma_1(\zeta), \ldots, \sigma_1^{n-1}(\zeta) \\ \vdots \qquad\qquad \vdots \\ 1, \sigma_n(\zeta), \ldots, \sigma_n^{n-1}(\zeta) \end{pmatrix}.$$

Then $\sigma(a) = \mathbf{Ra}$, where $\mathbf{a}$ is the vector of the coefficients of the polynomial a.

The *trace* and *norm* are the sum and product, respectively, of the canonical embeddings: $Tr(x) = \sum_{i \in [n]} \sigma_i(x)$ and $\mathcal{N}(x) = \prod_{i \in [n]} \sigma_i(x)$. The norm of an ideal I is its index as an additive subgroup of R, i.e., $\mathcal{N}(I) = |R/I|$.

In addition, with a proper indexation, the image H of σ is the $\mathbb{Q}$ vector space generated by the columns of $\sqrt{2} \cdot \mathbf{T}$ where:

$$\mathbf{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathbf{I}_{\phi(m)/2} & i\mathbf{I}_{\phi(m)/2} \\ \mathbf{I}_{\phi(m)/2} & -i\mathbf{I}_{\phi(m)/2} \end{pmatrix}$$

with $i = \sqrt{-1}$ and $\mathbf{I}$ is the identity matrix. In other words, for any element $x \in \mathbb{Q}(\zeta)$, there exists a vector $\mathbf{v} \in \mathbb{Q}^n$ such that $\sigma(x) = \mathbf{R}\mathbf{x} = \sqrt{2}\mathbf{T}\mathbf{v}$, and vice versa. For the rest of the paper, we will refer to the column vectors of $\mathbf{T}$ as *the canonical basis* for the embedding space H.

Defining

$$\mathbf{B} := 1/\sqrt{2} \cdot \mathbf{T}^{-1}\mathbf{R} \tag{1}$$

the transformation matrix from the canonical basis to the power basis, then, for any $a \in \mathbb{Q}(\zeta)$, there exists a corresponding vector $\mathbf{v} = \mathbf{B}\mathbf{a}$ where $\mathbf{a}$ is the vector form of a. It is straightforward to see that $\mathbf{B}$ is invertible since both $\mathbf{R}$ and $\mathbf{T}$ are nonsingular. Hence we also have $\mathbf{v} = \mathbf{B}^{-1}\mathbf{x}$. This allows us to bound the norm of $\mathbf{v}$ in functions of $\mathbf{x}$. According to the results in the functional analysis[6], there are positive constants c_1 and c_2 such that

$$c_1\|\mathbf{x}\| \leq \|\mathbf{B}^{-1}\mathbf{x}\| \leq c_2\|\mathbf{x}\| \tag{2}$$

for any $\mathbf{x}$. The absolute values of c_1 and c_2 depends solely on $\mathbf{B}$ which is only determined by the ring R, and $c_1^n \leq \det(\mathbf{B}^{-1}) \leq c_2^n$.

For cyclotomic rings $\mathbb{Z}[x]/(x^n + 1)$ where n is a power of 2, we have $c_1 = c_2$ since $\mathbf{B}$ is an orthogonal matrix [27]. Estimating the asymptotic bounds for other rings is still an open problem, although it was shown in [23], that even if c_1 and c_2 were not bounded by some constant, they seems to grow very slowly in n. Hence in this paper, we assume that

$$c_2 \leq (1 + 1/n)^{\tau_1} c_1 \tag{3}$$

for some constant τ_1, c_1 and c_2.

The Ideal Lattice. We follow [39] by viewing an ideal I in R as a lattices with a $\mathbb{Z}$-basis $U = \{u_1, ..., u_n\}$, under the canonical embedding σ. Correspondingly, denote the volume $vol(I) := vol(\sigma(I))$ of an ideal, the minimum distance $\lambda_1(I) := \lambda_1(\sigma(I))$, etc.

The (absolute) discriminant $\Delta_K = vol(R)^2$ of a number field K is the squared volume of its ring of integers $R = O_K$, viewed as a lattice; equivalently,

$$\Delta_K = |\det(Tr(u_i \cdot u_j))| = |\det(\mathbf{U}^* \cdot \mathbf{U})|$$

[6] The following statement can be found in most functional analysis textbooks. Here we refer to [50] Corollary 2.3.1.: Let X, Y be two Banach space, if $T : X \to Y$ is a one-to-one onto bounded linear operator, there are two positive numbers $a, b > 0$, such that $a\|x\| \leq \|Tx\| \leq b\|x\|, \quad \forall x \in X$.

where $\mathbf{U} = \sigma(U)$ for an arbitrary $\mathbb{Z}$ -basis $U = (u_1, \ldots, u_n)$ of R . A useful dimension-normalized quantity is the *root discriminant* $\delta_K := \sqrt{\Delta_K}^{1/n} = vol(R)^{1/n}$ (sometimes also denoted δ_R). It is a measurement of the "sparsity" of the algebraic integers in K. It follows directly from the definition that $vol(I) = \mathcal{N}(I) \cdot \sqrt{\Delta_K}$ for any fractional ideal I in K. The following standard fact is an immediate consequence of Minkowski's first theorem (for the upper bound) and the arithmetic mean-geometric mean inequality (for the lower bound).

Lemma 2 ([54]). *For any fractional ideal I in a number field K of degree n,*

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

Dual lattice. For any lattice L in K (i.e., for the $\mathbb{Z}$-span of any $\mathbb{Q}$-basis of K), its dual is defined as $L^\vee = \{x \in K : Tr(xL) \in \mathbb{Z}\}$. Recall that the ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta] := \mathbb{Z}[X]/(f)$. Let $I^\vee \subset K$ be the dual fractional ideal of I. Under the canonical embedding, $I^\vee$ embeds as the complex conjugate of the (usual defined) dual lattice of I, i.e., $\sigma(I^\vee) = \overline{\sigma(I)^*}$. Specifically, the dual (or co-different ideal) of $\mathbb{Z}[\zeta]$, denoted by $\mathbb{Z}[\zeta]^\vee$, is the fractional ideal $\frac{1}{f'(\zeta)}\mathbb{Z}[\zeta]$, where f' is the derivative of f [22]. That is, given a vector $\mathbf{a}$ corresponding to $a \in R^\vee$, we can injectively map a to $b = f'(\zeta)a \in R$ though a linear transformation $\mathbf{Da} = \mathbf{b}$. Similar to matrix $\mathbf{B}$, here, the matrix $\mathbf{D}$ is determined by the ring R, and there exist constants c_3 and c_4 such that

$$c_3\|\mathbf{x}\| \leq \|\mathbf{D}^{-1}\mathbf{x}\| \leq c_4\|\mathbf{x}\| \tag{4}$$

for any $\mathbf{x}$. Again, it is an open problem to give asymptotical bounds for c_3 and c_4, except for the case of cyclotomic ring $\mathbb{Z}[x]/(x^n + 1)$ with n is a power of 2, where $c_3 = c_4 = 1/n$. Therefore, for the rest of rings, we assume that

$$c_4 \leq (1 + 1/n)^{\tau_2}\, c_3 \tag{5}$$

for some constant τ_2, c_3 and c_4.

For a function $\mathcal{F}$ that maps lattices to non-negative reals, the *bounded distance decoding problem* (BDD) over H is defined as given a lattice $L \subset H$, a distance bound $d \leq \mathcal{F}(L)$, and a coset $\mathbf{e} + L$ where $\|\mathbf{e}\| \leq d$, find $\mathbf{e}$.

2.4 Gaussian Distribution

For $\alpha > 0$, the *continuous* Gaussian distribution D_α^H of parameter (or width) α over H is defined to by a probability density function $f(\mathbf{x}) = \frac{1}{\alpha^n}\rho_\alpha(\mathbf{x}) = \frac{1}{\alpha^n}\exp\left(-\pi\frac{\langle \mathbf{x},\mathbf{x}\rangle}{\alpha^2}\right)$. This naturally induce a distribution over the field tensor product $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$ with respect to the canonical basis. When converting to the power basis, the random vector $\mathbf{y} = \mathbf{Bx}$ follows a probability density function $f'(\mathbf{y}) = \frac{1}{\alpha^n\sqrt{\mathbf{\Sigma}}}\exp\left(-\pi\frac{\mathbf{y}^T\mathbf{\Sigma}^{-1}\mathbf{y}}{\alpha^2}\right)$, where $\mathbf{\Sigma} = \mathbf{BB}^T$ for $\mathbf{B}$ defined in (1). The *rounded Gaussian*, denoted by $\bar{D}_\alpha^H$, is the distribution $\lfloor x \rceil \bmod q \in R_q$ where $x \leftarrow D_\alpha^H$ and the rounding is performed over the power basis.

Next we recall an important definition, the *smoothing parameter* [46], and its various related lattice quantities.

Definition 2. *For a lattice L and positive real $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(L)$ is defined to be the smallest r such that $\rho_{1/r}(L^*/\{0\}) \leq \varepsilon$.*

Lemma 3 ([46]). *For any n-dimensional lattice L, we have $\eta_{2^{-2n}}(L) \leq \sqrt{n}/\lambda_1(L^*)$, and $\eta_\varepsilon(L) \leq \sqrt{\ln(n/\varepsilon)}\lambda_n(L)$ for all $0 < \varepsilon < 1$.*

Lemma 4 ([46]). *For any lattice L, $\varepsilon > 0$, $r \geq \eta_\varepsilon(L)$, and $\mathbf{c} \in H$, the statistical distance between $(D_r + \mathbf{c}) \bmod L$ and uniform distribution modulo L is at most ε.*

The next lemma describes the tail cutting property of a Gaussian distribution.

Lemma 5 (Tail Cutting). *A one-dimensional Gaussian D_α over $\mathbb{R}$ satisfies the tail bound $\Pr_{x \leftarrow D_\alpha}[|x| \geq B] \leq 2\exp(-\pi(B/\alpha)^2)$ for any $B \geq 0$. Particularly, if $B > \sqrt{n}\alpha$ for some integer n, $\Pr_{x \leftarrow D_\alpha}[|x| \geq B]$ is exponentially small in n.*

2.5 The learning with errors problem over the ring

The first hardness result for decisional R-LWE problem is for cyclotomic fields [39, 40], assuming that the BDD problem is hard. In [55], the result is extended to any ring, with the help of a *discrete Gaussian sampling* problem.

Let K be some number field of dimension n. Let $R = \mathcal{O}_K$ be its ring of integers which embeds as a lattice. $R^\vee \subset K$ is the dual fractional ideal of R. For simplicity and convenience for our applications, we present the problem in its discretized, "normal" form [6], where the secret are drawn from the same distribution with the error. See [40, 41, 54] for more general forms.

Definition 3 (R-LWE Distribution). *For an $s \in R_q^\vee$ and a distribution χ over the field tensor product $K_\mathbb{R} = K \otimes_\mathbb{Q} \mathbb{R}$, a sample from the R-LWE distribution $\mathcal{O}_{s,\chi}$ over $R_q \times K_\mathbb{R}/qR^\vee$ is generated by choosing $a \leftarrow R_q$ uniformly at random, choosing $e \leftarrow \chi$, and outputting $(a, b = a \cdot s + e)$.*

Definition 4 (R-LWE Average-Case Decisional Problem). *The decision version of the R-LWE problem, denoted by R-DLWE$_{q,\chi',\chi}$, is to distinguish with non-negligible advantage between independent samples from $\mathcal{O}_{s,\chi}$ for some s chosen from χ', and the same number of uniformly random and independent samples from $R_q \times K_\mathbb{R}/qR^\vee$.*

The claim that R-DLWE$_{q,\chi',\chi}$ is hard for any probabilistic polynomial time distinguisher $\mathcal{A}$ is equivalent to the following statement: Let $\Pr(\mathcal{A}^{\mathcal{O}_{\chi,s}} = 1) = p_0(s)$ and $\Pr(\mathcal{A}^{\mathcal{U}(R_q \times R_q)} = 1) = p_1$. Denote by S_ε the set where for any elements $s \in S$, $|p_0(s) - p_1| > \varepsilon$ except for some negligible ε. Then there is a negligible δ such that $\Pr(s \in S | s \leftarrow \chi') < \delta$.

Theorem 1 ([40, 41]). *Let K be the m-th cyclotomic number field with dimension $n = \psi(m)$ and $R = \mathcal{O}_K$ be its ring of integers. Let $\xi = \xi(n) > 0$, and let $q = q(n) \geq 2$, $q = 1 \bmod m$ be a poly(n)-bounded prime such that $\xi q \geq \omega(\sqrt{\log n})$. Then there is a polynomial-time quantum reduction from $\tilde{O}(\sqrt{n}/\xi)$-approximate SIVP (or SVP) on ideal lattices in K to the problem of solving R-DLWE$_{q,D_\alpha}$, given $l - 1$ samples, where $\alpha = q\xi \cdot (nl/log(nl))^{1/4}$.*

The theorem above captures reductions from ideal lattice GapSVP (GapSIVP) to R-LWE. To guarantee an average-case/worst-case reduction as in [40], the error distribution χ needs to be a continuous Gaussian distribution D_α^H over H. In practice, it is more convenient to work with a discretized "non-dual" form of R-LWE [27], where the secret and the error are both in R_q instead of $R_q^\vee$. Accordingly, samples will be of the form $(a_i, b_i = s \cdot a_i + e_i \bmod qR) \in R_q \times R_q$. To achieve so, we multiply the error distribution by $t = f'(\zeta)$, then discretize it by rounding each coefficient in the power basis to the nearest integer. Consequently, the error distribution becomes $\overline{t \cdot D_\alpha^H}$ over R. In the paper we adapt the "normal" form R-LWE [6], i.e., the secret is also drawn from the distribution $\overline{t \cdot D_\alpha^H}$.

3 Warm Up

Our computational assumption is defined by the success probability among multiple experiments, where each experiment is a sequence of interactions between a challenger $\mathcal{C}$ and an adversary $\mathcal{A}$ as defined in Def. 5. In addition, we use a third party, the Source, denoted by $\mathcal{S}$, who is responsible for generating the samples for $\mathcal{C}$, as illustrated in Figure 1.

Definition 5 (Exp$(\mathcal{C}, \mathcal{A})$). *The experiment is defined as a sequence of interactions as follows:*

1. *$\mathcal{S}$ samples from var and con to obtain a sample (X, aux), and sends it to $\mathcal{C}$;*
2. *$\mathcal{C}$ computes* (Input, Target) $\leftarrow \mathcal{C}(X, aux)$*, and sends* Input *to the $\mathcal{A}$;*
3. *$\mathcal{A}$ replies with a guess* Output.

The adversary wins the experiment if Target = Output.

We claim that the success probability of $\mathcal{A}$ will depend on three factors: a), the distribution of the source *var*; b) the distribution of the Target; and c) the connection between Input and Target, i.e., the combination of $\mathcal{C}$ and $\mathcal{A}$. Our goal is to ensure that, for variance Exp$_i$, the success probability of $\mathcal{A}_i$ will only depend on the distribution of the source $\mathcal{S}_i$. To achieve so, we use a same challenger $\mathcal{C}$ and adversary $\mathcal{A}$ pair throughout the experiments.

As a result, those experiments will reveal the impact of different $\mathcal{S}$-s on $\mathcal{A}$'s success probability. If $\mathcal{A}$ successfully guesses an Output for an X_i, we can deduce that $\mathcal{C}$ leaks enough information about $\mathcal{S}$ for the adversary to compute Target. Thus, for two sources $\mathcal{S}_1$ and $\mathcal{S}_2$, our definition captures that, no matter what information is leaked through $\mathcal{C}$, if an adversary cannot compute Target from X_1

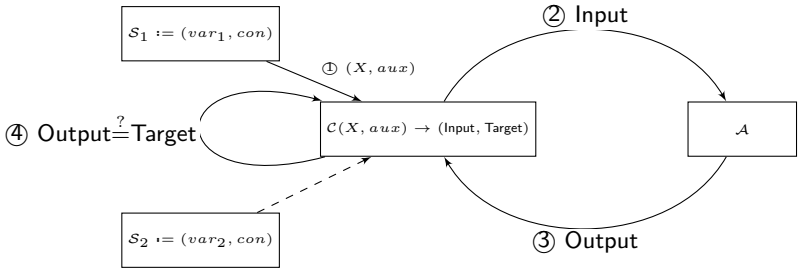

Fig. 1. Data flow for our experiments

for source $\mathcal{S}_1$, then it cannot compute Target from X_2 for source $\mathcal{S}_2$. That is, the adversary cannot learn more information from $\mathcal{S}_1$ than from $\mathcal{S}_2$ for a fixed $\mathcal{C}$.

Then, for any PPT challenger $\mathcal{C}$, if the success probability of any adversary $\mathcal{A}$ in Exp_1 of Table 1 is negligible, so does $\mathcal{A}$ in Exp_2.

$\mathsf{Exp}_1(\mathcal{C}, \mathcal{A})$	$\mathsf{Exp}_2(\mathcal{C}, \mathcal{A})$
$X_1 \leftarrow var_1$	$X_2 \leftarrow var_2$
$aux \leftarrow con$	$aux \leftarrow con$
$\mathsf{Input}_1, \mathsf{Target}_1 \leftarrow \mathcal{C}(X_1, aux)$	$\mathsf{Input}_2, \mathsf{Target}_2 \leftarrow \mathcal{C}(X_2, aux)$
$\mathsf{Output}_1 \leftarrow \mathcal{A}(\mathsf{Input}_1)$	$\mathsf{Output}_2 \leftarrow \mathcal{A}(\mathsf{Input}_2)$
Success if $\mathsf{Output}_1 = \mathsf{Target}_1$	Success if $\mathsf{Output}_2 = \mathsf{Target}_2$

Table 1. Exp_1 v.s. Exp_2

To show that the above model is useful in a security proof, let us present a proof of an (informal) Diffie-Hellman version of the assumption within the above model. Looking ahead, we will use a similar approach to proof R-CLWR.

Definition 6 (The Diffie-Hellman analogue to our assumption). *Let $\mathbb{G}$ be a group. Let $\mathcal{Z}_s$ be the distribution of $(a, b) = (g, g^s)$ where $g \leftarrow_\$ \mathbb{G}$ is a randomly chosen group element and s is an randomly chosen and fixed index. Accordingly, let $\mathcal{U}$ be the distribution of $(a, b) = (g, u)$ where $g, u \leftarrow_\$ \mathbb{G}$. Let var_1 denote the distribution $\mathcal{Z}_s^l$ and var_2 denote the distribution $\mathcal{U}^l$. Let con be an arbitrary distribution over $\{0,1\}^*$ which is independent of var_1 and var_2. For a fixed PPT challenger $\mathcal{C}$, $\mathring{P}_{\mathcal{C}}(\mathcal{A})$ is the probability for a PPT adversary $\mathcal{A}$ to win the $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A})$ with $\mathcal{S}_1$ in Table 1, while $\mathring{Q}_{\mathcal{C}}(\mathcal{A})$ is that for $\mathcal{A}$ to the $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A})$ with $\mathcal{S}_2$. Then, if $\mathring{Q}_{\mathcal{C}}$ is negligible for any PPT adversary $\mathcal{A}$, so is $\mathring{P}_{\mathcal{C}}$.*

We claim that this assumption implies the CDH assumption. Recall that CDH says that given g^x and g^y for a randomly chosen element g, no PPT adversary is able to compute g^{xy}. Slightly different with the traditional CDH assumption, here we require g is randomly chosen from a cyclic group instead of a fixed element. So $g, g^x, g^y g^{xy}$ all can be as distributions. We sketch a reduction through the following games.

Game 1. The Input for $\mathcal{A}$ is (g^x, g^y), and the Target is g^{xy}.
Game 2. The Input for $\mathcal{A}$ is (u, g^y) for some random u, and the Target is u^y.
Game 3. The Input for $\mathcal{A}$ is (u, v) for some random u and v, and the Target is w for some random w.

Observe that, in Game 3, u, v and w are independent, therefore the success probability of the adversary will be $1/|\mathbb{G}|$, which is negligible.

In the rest of the reduction, we will firstly proof the success probability of the adversary in Game 2 is also negligible. To meet the notation, we set var_1 to be the distribution of $((a_1, b_1), (a_2, b_2))$ for $(a_1, b_1) = (g, g^y)$ and $(a_2, b_2) = (u, u^y)$, and var_2 to be that for $(a_1, b_1) = (g, v)$ and $(a_2, b_2) = (u, w)$. Set con to be dummy. $\mathcal{C}$ is then defined as given $X = ((a_1, b_1), (a_2, b_2))$, compute $\mathsf{Input} = (a_2, b_1)$ and $\mathsf{Target} = b_2$. As per Def. 6, if the success probability of Exp_2 in Table 2 is negligible, so is that of Exp_1. Therefore, the success probability of the adversary in Game 2 is negligible.

	$\mathsf{Exp}_1(\mathcal{C}, \mathcal{A})$	$\mathsf{Exp}_2(\mathcal{C}, \mathcal{A})$
	$((g, g^y), (u, u^y)) \leftarrow var_1$	$((g, v), (u, w)) \leftarrow var_2$
Source	$\perp \leftarrow con$	$\perp \leftarrow con$
	$X_1 \leftarrow ((g, g^y), (u, u^y)), \perp)$	$X_2 \leftarrow (((g, v), (u, w)), \perp)$
Challenger	$\mathsf{Input}_1 \leftarrow (u, g^y)$	$\mathsf{Input}_2 \leftarrow (u, v)$
	$\mathsf{Target}_1 \leftarrow u^y$	$\mathsf{Target}_2 \leftarrow w$
Attacker	$\mathsf{Output}_1 \leftarrow \mathcal{A}((u, g^y))$	$\mathsf{Output}_2 \leftarrow \mathcal{A}(u, v)$
	Success if $\mathsf{Output}_1 = u^y$	Success if $\mathsf{Output}_2 = w$

Table 2. Reduction between Game 2 and 3

Then we will proof the success probability of the adversary in Game 1 is also negligible. Let con be the distribution of choosing an arbitrary index y; var_1 be the distribution of (a_1, b_1) for $(a_1, b_1) = (g, g^x)$; and var_2 be that for $(a_1, b_1) = (g, v)$. Accordingly, $\mathcal{C}$ is defined as given $X = ((a_1, b_1), y)$ and computes $\mathsf{Input} = (b_1, a_1^y)$ and $\mathsf{Target} = b_1^y$. As per Def. 6, if the success probability of Exp_2 in Table 3 is negligible, so is that of Exp_1. Therefore, the success probability of the adversary in Game 1 is negligible.

	$\mathsf{Exp}_1(\mathcal{C}, \mathcal{A})$	$\mathsf{Exp}_2(\mathcal{C}, \mathcal{A})$
	$(g, g^x) \leftarrow var_1$	$(g, u) \leftarrow var_2$
Source	$y \leftarrow con$	$y \leftarrow con$
	$X_1 \leftarrow ((g, g^x), y)$	$X_2 \leftarrow ((g, u), y)$
Challenger	$\mathsf{Input}_1 \leftarrow (g^x, g^y)$	$\mathsf{Input}_2 \leftarrow (u, g^y)$
	$\mathsf{Target}_1 \leftarrow g^{xy}$	$\mathsf{Target}_2 \leftarrow u^y$
Attacker	$\mathsf{Output}_1 \leftarrow \mathcal{A}(g^x, g^y)$	$\mathsf{Output}_2 \leftarrow \mathcal{A}(u, g^y)$
	Success if $\mathsf{Output}_1 = g^{xy}$	Success if $\mathsf{Output}_2 = u^y$

Table 3. Reduction between Game 1 and 2

In the next section, we will give more details on how to instantiate the framework as per Def. 6 where the underlying discrete log problem is replaced by a lattice problem.

4 The Computational Ring-LWR Assumption

For simplicity, we make use of the following additional notations. We refer to a uniformly distribution over $[-\beta, \beta]$ as U_β. Accordingly, denote by U_β^n the distribution over R_q where each coefficient is no greater than β. For a distribution χ over K, we say $\bar{\chi}$ is the discretization distribution over R, which is obtained by rounding each coefficient in the power basis to the nearest integer. For a distribution χ' over R, denote by $(\chi')^\times$ the distribution of the output of the following process: sample an element $a \leftarrow \chi'$, output a if a is invertible; repeat until an output is obtained.

Now we are ready to give a formal definition of the R-CLWR assumption. This definition, as hinted in previous section, allows us to prove that an adversary cannot learn more information from R-CLWR sample inputs than from uniform inputs. Our definition follows the framework of the Table 1. The only variation here is on the definitions of var_1 and var_2.

Definition 7 (Computational Ring-LWR Assumption). *Let q, p and l be positive integers. Fix an s that is chosen from a distribution χ over R. Denote by $\mathcal{X}_s$ the distribution of $(a, \lfloor as \rfloor_p)$ where $a \leftarrow_\$ R_q$; and denote by $\mathcal{U}$ the distribution of $(a, \lfloor b \rfloor_p)$ where $a, b \leftarrow_\$ R_q$. Let $\mathcal{S}_i = (var_i, con)$, where var_1 denotes the distribution $\mathcal{X}_s^l$; var_2 denote the distribution $\mathcal{U}^l$; and con is an arbitrary distribution over $\{0,1\}^*$ which is independent from var_1 and var_2. For a fixed PPT challenger $\mathcal{C}$, let $P_{\mathcal{C},\mathcal{A}}(\chi)$ be the probability for a PPT adversary $\mathcal{A}$ to win $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A})$ with $\mathcal{S}_1$, while $Q_{\mathcal{C},\mathcal{A}}$ be that for $\mathcal{A}$ to win $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A})$ with $\mathcal{S}_2$.*

The computational ring-LWR assumption with regard to a secret distribution χ, denoted by R-$\mathsf{CLWR}_{p,q,l,\chi}$, or R-$\mathsf{CLWR}_\chi$ for short, is that for any challenger $\mathcal{C}$, if $Q_{\mathcal{C},\mathcal{A}}$ is negligible for any PPT adversary $\mathcal{A}$, so is $P_{\mathcal{C},\mathcal{A}}$.

Correspondingly, we also define the *computational rounded learning with errors over the ring* (R-CRLWE) assumption. Notice its difference from a computational LWE over the ring assumption, which, by the analogy to R-CLWR, replaces R-LWR samples $(\lfloor as \rfloor_p)$ with R-LWE samples $(as + e)$. By contrast, in R-CRLWE, one replaces R-LWR samples with *rounded* R-LWE samples $(\lfloor as + e \rfloor_p)$.

Definition 8 (Computational Ring-RLWE Assumption). *Let q, p, l, s, χ and $\mathcal{U}$ be the same as Def. 7. Denote by $\mathcal{Y}_{s,\chi'}$ the distribution of $(a, \lfloor as + e \rfloor_p)$ where $a \leftarrow_\$ R_q$ and $e \leftarrow \chi'$ over R. Let $\mathcal{S}_i = (var_i, con)$, where var_1 denotes the distribution $\mathcal{Y}_{s,\chi'}^l$; var_2 denotes the distribution $\mathcal{U}^l$; con denotes an arbitrary distribution over $\{0,1\}^*$ which is independent of S_1 and S_2. For a fixed PPT challenger $\mathcal{C}$, let $P'_{\mathcal{C},\mathcal{A}}(\chi, \chi')$ be the probability for a PPT adversary $\mathcal{A}$ to $\mathsf{Exp}_1(\mathcal{C}, \mathcal{A})$ with $\mathcal{S}_1$, while $Q_{\mathcal{C},\mathcal{A}}$ to be that for $\mathcal{A}$ to win $\mathsf{Exp}_2(\mathcal{C}, \mathcal{A})$ with $\mathcal{S}_2$.*

The computational ring-RLWE assumption with a secret distribution χ and an error distribution χ', denoted by R-$\mathsf{CRLWE}_{p,q,l,\chi,\chi'}$ or R-$\mathsf{CRLWE}_{\chi,\chi'}$ for short,

is that for any challenger $\mathcal{C}$, if $Q_{\mathcal{C},\mathcal{A}}$ is negligible for any PPT adversary $\mathcal{A}$, so is $P'_{\mathcal{C},\mathcal{A}}(\chi,\chi')$.

This definition suggests that the adversary cannot learn more information from R-CRLWE inputs than from uniform inputs. Next, we show that the R-CLWR assumption holds for uniform secrets, assuming the hardness of the decisional R-LWE assumption. Formally, we will have the following theorem.

Theorem 2 (Main Theorem). *Following the notions in Def. 7 and Def. 8. For any ring R satisfying (3) and (5), the largest degree of the irreducible factors modulo integer q of the polynomial f is less than k_q. If l is a constant, $\alpha \geq c_2c_4\sqrt{n\ln(2n)}q^{k_q/n}\cdot\delta_K$, $\beta = \Omega(nl\alpha)$ and $q/p = \Omega(nl\alpha/c_2c_4)$, there is a reduction from the decisional ring-LWE assumption $R\text{-}\mathsf{LWE}_{q,\overline{t\cdot D_\alpha^H},\overline{t\cdot D_\alpha^H}}$ to the computational ring-LWR assumption $R\text{-}\mathsf{CLWR}_{p,q,l,(U_\beta^n)^\times}$.*

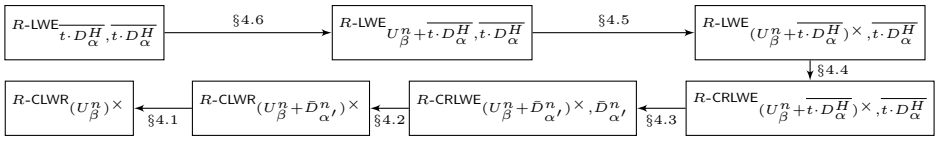

Fig. 2. Reduction flow from R-LWE to R-CLWR

Combing with the worst-case/average-case reduction in Theorem 1, the hardness of our R-CLWR problem will be based on the worse-case hardness of lattice problems. It is worth pointing out that, the majority of practical cryptosystems uses a cyclotomic ring $R = \mathbb{Z}[x]/(x^n+1)$ where n is a power of 2. For this ring, we have the following result.

Corollary 1. *Following the same notations. For $R = \mathbb{Z}[x]/(x^n+1)$ where n is a power of 2, if l is a constant, $\alpha \geq 2\sqrt{n\ln(2n)}\cdot q^{2/n}$, $\beta = \Omega(nl\alpha)$ and $q/p = \Omega(n^2l\alpha)$, there is a reduction from the decisional ring-LWE assumption $R\text{-}\mathsf{LWE}_{q,\overline{t\cdot D_\alpha^H},\overline{t\cdot D_\alpha^H}}$ to the computational ring-LWR assumption $R\text{-}\mathsf{CLWR}_{p,q,l,(U_\beta^n)^\times}$.*

4.1 From $R\text{-}\mathsf{CLWR}_{(U_\beta^n+\bar{D}_{\alpha'}^n)^\times}$ to $R\text{-}\mathsf{CLWR}_{(U_\beta^n)^\times}$

We begin with proving the following lemma which shows the RD between the two distributions on $\mathbb{Z}$, namely U_β and $U_\beta + \bar{D}_\alpha$, is bounded by $1+1/n$.

Lemma 6. *Following the same notion. In addition, let U_β be a uniform distribution from $[-\beta,\beta]$ over $\mathbb{Z}$ where $\beta > \alpha$. Let the distribution $\psi = \bar{D}_\alpha + U_\beta$. Then $\mathsf{RD}_2(U_\beta \parallel \psi) \leq 1+\frac{\alpha}{c\beta}$ where $c = \frac{(1-\exp(-\pi))^2}{2} \approx 0.4577$. Specifically, when $\beta > n\alpha/c$, $\mathsf{RD}_2(U_\beta \parallel \psi) < 1+1/n$.*

Proof. Please see the full version [19].

With Lemma 6, we are ready to proof the first reduction.

Lemma 7. *Following the same notation, if $\beta = \Omega(nl\alpha)$, $P_{\mathcal{C},\mathcal{A}}(U_\beta^n) \leq 2P_{\mathcal{C}}(U_\beta^n + \bar{D}_\alpha^n)$. Hence there is a reduction from R-$\mathsf{CLWR}_{(U_\beta^n+\bar{D}_{\alpha'}^n)^\times}$ to R-$\mathsf{CLWR}_{(U_\beta^n)^\times}$.*

Proof. Note that $P_{\mathcal{C},\mathcal{A}}((U_\beta^n)^\times) \leq P_{\mathcal{C},\mathcal{A}}((U_\beta^n+\bar{D}_\alpha^n)^\times)\cdot \mathsf{RD}_2\left(U_\beta \| U_\beta + \bar{D}_\alpha\right)^{nl}$. Lemma 6 says $\mathsf{RD}_2\left(U_\beta \| U_\beta + \bar{D}_\alpha\right)^{nl} \leq 2$ when $\beta = \Omega(nl\alpha)$. On the other hand, assuming the hardness of R-$\mathsf{CLWR}_{(U_\beta^n+\bar{D}_\alpha^n)^\times}$, we have that for any challenger $\mathcal{C}$, $P_{\mathcal{C},\mathcal{A}}((U_\beta^n + \bar{D}_\alpha^n)^\times)$ is negligible when $Q_{\mathcal{C},\mathcal{A}}$ is negligible. By the above result, $P_{\mathcal{C},\mathcal{A}}((U_\beta^n)^\times)$ is also negligible. So the assumption R-$\mathsf{CLWR}_{(U_\beta^n)^\times}$ holds. □

4.2 From R-$\mathsf{CRLWE}_{(U_\beta^n+\bar{D}_{\alpha'}^n)^\times,\bar{D}_{\alpha'}^n}$ to R-$\mathsf{CLWR}_{(U_\beta^n+\bar{D}_{\alpha'}^n)^\times}$

The following lemma is adapted from [12] with a slight modification on the noise distribution. We provide a proof for completeness.

Lemma 8 ([12]). *Assume $B < q/2p$. For every unit $s \in R_q$ and noise distribution χ that is balanced over R_q and each coefficient is bounded by B with probability larger than δ, we have $\mathsf{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s) \leq (1 + 2pB/q)^n/\delta^n$ where $\mathcal{X}_s$ is the random variable $(a, \lfloor a \cdot s \rfloor_p)$ and $\mathcal{Y}_s$ is the random variable $(a, \lfloor a \cdot s + e \rfloor_p)$ with $a \leftarrow R_q$ and $e \leftarrow \chi$.*

Proof. By the definition,

$$\begin{aligned} RD_2(X_s \| Y_s) &= E_{a \leftarrow R_q} \frac{Pr(X_s = (a, \lfloor a \cdot s \rfloor_p))}{Pr(Y_s = (a, \lfloor a \cdot s + e \rfloor_p))} \\ &= E_{a \leftarrow R_q} \frac{1}{\Pr_{e \leftarrow \chi}\left(\lfloor a \cdot s + e \rfloor_p = \lfloor a \cdot s \rfloor_p\right)}. \end{aligned}$$

We define the set $border_{p,q}(B) = \left\{x \in \mathbb{Z}_q : \left|x - \frac{q}{p}\lfloor x \rfloor_p\right| < B\right\}$. For a ring element $a \in R_q$, we use a_i to denote the ith coefficient in the power basis. For fixed s and for any $t \in [n]$, we define the set

$$BAD_{s,t} = \{a \in R_q : |\{i \in [n], (a \cdot s)_i \in border_{p,q}(B)\}| = t\}.$$

These are candidate a-s for which $a \cdot s$ has exactly t coefficients which are dangerously close to the rounding boundary. Fix an arbitrary t and $a \in BAD_{s,t}$. For any $i \in [n]$ such that $(a \cdot s)_i \notin border_{p,q}(B)$, $\Pr_{e_i}[\lfloor (as)_i + e_i \rfloor_p = \lfloor (as)_i \rfloor_p] \geq \delta$. For any $i \in [n]$ such that $(a \cdot s)_i \in border_{p,q}(B)$, we still have $\lfloor (a \cdot s)_i + e_i \rfloor_p = \lfloor (a \cdot s)_i \rfloor_p$ as long as $e_i \in [-B, \ldots, 0]$. By the assumption on the noise distribution, we have $\Pr_{e_i}[\lfloor (a \cdot s)_i + e_i \rfloor_p = \lfloor (a \cdot s)_i \rfloor_p] \geq 1/2$. Because e is independent over all coefficients and a has exactly t coefficients in $border_{p,q}(B)$, $\Pr_{e \leftarrow \chi}\left(\lfloor a \cdot s + e \rfloor_p = \lfloor a \cdot s \rfloor_p\right) \geq \frac{1}{2^t}\delta^{n-t} \geq \frac{1}{2^t}\delta^n$.

Since s is a unit in R_q, $a \cdot s$ will be uniform over R_q and

$$\Pr\left[a \in BAD_{s,t}\right] \leq \binom{n}{t}\left(1 - \frac{|border_{p,q}(B)|}{q}\right)^{n-t}\left(\frac{|border_{p,q}(B)|}{q}\right)^t.$$

Conditioning on the event $a \in BAD_{s,t}$, we conclude

$$\mathsf{RD}_2(X_s \| Y_s) \leq \delta^{-n} \sum_{t=0}^{n} 2^t \cdot \Pr[a \in BAD_{s,t}] = \delta^{-n} \left(1 + \frac{|border_{p,q}(B)|}{q}\right)^n.$$

□

Lemma 9. *Adopt the same notions and symbols in Def. 7 and Def. 8. If* $p > \frac{q\sqrt{\pi}}{2nl\alpha\sqrt{\ln(2nl)}}$, *we have* $P_{\mathcal{C},\mathcal{A}}(U_\beta^n + \bar{D}_\alpha^n)^\times \leq e^2 P'_{\mathcal{C},\mathcal{A}}(U_\beta^n + \bar{D}_\alpha^n)^\times$. *Hence there is a reduction from* R-$\mathsf{CRLWE}_{(U_\beta^n + \bar{D}_{\alpha'}^n)^\times, \bar{D}_{\alpha'}^n}$ *to* R-$\mathsf{CLWR}_{(U_\beta^n + \bar{D}_{\alpha'}^n)^\times}$.

Proof. We have $P_{\mathcal{C},\mathcal{A}}(U_\beta^n + \bar{D}_\alpha^n) \leq P'_{\mathcal{C},\mathcal{A}}(U_\beta^n + \bar{D}_\alpha^n) \cdot RD_2(\mathcal{X}_s \| \mathcal{Y}_s)^l$. Note that a one-dimensional Gaussian D_α over $\mathbb{R}$ satisfies the tail bound $\Pr_{x \leftarrow D_\alpha}[|x| \geq B] \leq 2\exp(-\pi(B/\alpha)^2)$ for any $B \geq 0$. We set $B = \sqrt{\frac{\ln(2nl)}{\pi}}\alpha$, so $2\exp(-\pi(B/\alpha)^2) \leq 1/nl$ and $\delta \geq 1 - \frac{1}{nl}$. Also we set $p > q/2nlB$, then we have

$$\mathsf{RD}_2(\mathcal{X}_s \| \mathcal{Y}_s)^l \leq (1 + 2pB/q)^{nl}/\delta^{nl} \leq \frac{(1 + 1/nl)^{nl}}{(1 - 1/nl)^{nl}} \leq e^2 \tag{6}$$

Assuming R-$\mathsf{CRLWE}_{(U_\beta^n + \bar{D}_{\alpha'}^n)^\times, \bar{D}_{\alpha'}^n}$ assumption holds, then for any $\mathcal{C}$ and $\mathcal{A}$, $P'_{\mathcal{C},\mathcal{A}}\left((U_\beta^n + \bar{D}_{\alpha'}^n)^\times, \bar{D}_{\alpha'}^n\right)$ is negligible so long as $Q_{\mathcal{C},\mathcal{A}}$ is negligible. By the result of (6), $P_{\mathcal{C},\mathcal{A}}(U_\beta^n + \bar{D}_{\alpha'}^n)^\times$ is also negligible. This proves the R-$\mathsf{CLWR}_{(U_\beta^n + \bar{D}_{\alpha'}^n)^\times}$ assumption. □

4.3 From R-$\mathsf{CRLWE}_{\left(U_\beta^n + \overline{t \cdot D_\alpha^H}\right)^\times, \overline{t \cdot D_\alpha^H}}$ to R-$\mathsf{CRLWE}_{\left(U_\beta^n + \bar{D}_{\alpha'}^n\right)^\times, \bar{D}_{\alpha'}^n}$

Lemma 10. *Following the same notations. Additionally, let* $\overline{t \cdot D_\alpha^H}$ *be the discretization of* $t \cdot D_\alpha^H$, *where* D_α^H *is the continuous Gaussian with width* α *over the* H *space.* $\bar{D}_{\alpha'}^n$ *is the discretization of the continuous Gaussian with width* α *according to the power basis.* $\mathcal{Y}'_{\overline{t \cdot D_\alpha^H}, \overline{t \cdot D_\alpha^H}}$ *is the random variable* $(a, \lfloor a \cdot s + e \rfloor_p)$ *with* $a \leftarrow_\$ R_q$ *and* $s, e \leftarrow \overline{t \cdot D_\alpha^H}$, *and* $\mathcal{Y}'_{\bar{D}_{\alpha'}^n, \bar{D}_{\alpha'}^n}$ *is the random variable* $(a, \lfloor a \cdot s + e \rfloor_p)$ *with* $a \leftarrow_\$ R_q$ *and* $s, e \leftarrow \bar{D}_{\alpha'}^n$. *For any ring* R *satisfying (3) and (5), when* $\alpha/c_1c_3 \leq \alpha' \leq \left(1 + \frac{1}{n}\right)^{\tau_1 + \tau_2} \alpha/c_2c_4$, *we have* $\mathsf{RD}_\infty\left(\mathcal{Y}'_{\overline{t \cdot D_\alpha^H}, \overline{t \cdot D_\alpha^H}} \| \mathcal{Y}'_{\bar{D}_{\alpha'}^n, \bar{D}_{\alpha'}^n}\right) \leq e^{\tau_1 + \tau_2}$.

Proof. According to the data processing inequality of Rényi divergence, it is sufficient to show $\mathsf{RD}_\infty\left(D_\alpha^n \| t \cdot D_\alpha^H\right) \leq e^{\tau_1 + \tau_2}$. So we need to prove for all $\mathbf{x} \in \mathbb{R}^n$, $\rho(\mathbf{x})/\rho'(\mathbf{x}) \leq e^{\tau_1 + \tau_2}$. Recall that $t \cdot D_\alpha^H$ has the probability density function over the power basis $\rho(\mathbf{x}) = (\alpha^n \det(\mathbf{D}) \det(\mathbf{B}))^{-1} \exp\left(-\pi \mathbf{x}^T \left(\mathbf{D}^{-1}\right)^T \mathbf{\Sigma}^{-1} \mathbf{D}^{-1} \mathbf{x}/\alpha^2\right)$, and D_α^n has the probability density function over the power basis $\rho'(\mathbf{x}) = \alpha'^{-n} \exp\left(-\pi \mathbf{x}^T \mathbf{x}/\alpha'^2\right)$. Hence,

$$\frac{\rho(\mathbf{x})}{\rho'(\mathbf{x})} = \frac{\alpha'^n}{\alpha^n \det(\mathbf{D}) \det(\mathbf{B})} \exp\left(\pi \left(\frac{\mathbf{x}^T \mathbf{x}}{\alpha'^2} - \frac{\mathbf{x}^T \left(\mathbf{D}^{-1}\right)^T \mathbf{\Sigma}^{-1} \mathbf{D}^{-1} \mathbf{x}}{\alpha^2}\right)\right).$$

According to (2) and (4), $\mathbf{\Sigma} = \mathbf{B}^T\mathbf{B}$, $\|\mathbf{D}^{-1}\mathbf{x}\| \geq c_1\|\mathbf{x}\|$ for any $\mathbf{x} \in \mathbb{R}^n$ and $\|\mathbf{B}^{-1}\mathbf{y}\| \geq c_3\|\mathbf{y}\|$ for any $\mathbf{y} \in \mathbb{R}^n$. If $\alpha' \geq \alpha/c_1c_3$, we have $\frac{\mathbf{x}^T(\mathbf{D}^{-1})^T\mathbf{\Sigma}^{-1}\mathbf{D}^{-1}\mathbf{x}}{\alpha^2} \geq \frac{c_1^2c_3^2\mathbf{x}^T\mathbf{x}}{\alpha^2} \geq \frac{\mathbf{x}^T\mathbf{x}}{\alpha'^2}$. Therefore,

$$\frac{\rho(\mathbf{x})}{\rho'(\mathbf{x})} \leq \frac{\alpha'^n}{\alpha^n \det(\mathbf{D})\det(\mathbf{B})} \leq e^{\tau_1+\tau_2}$$

when $\alpha' \leq \left(1+\frac{1}{n}\right)^{\tau_1+\tau_2}\alpha c_2c_4 \leq \left(1+\frac{1}{n}\right)^{\tau_1+\tau_2}\alpha|\det(\mathbf{D})|^{1/n}|\det(\mathbf{B})|^{1/n}$. According to (3) and (5), we have $c_2 \leq \left(1+\frac{1}{n}\right)^{\tau_1}c_1$ and $c_3 \leq \left(1+\frac{1}{n}\right)^{\tau_2}c_4$. Therefore there must exist at least an α' that satisfies $\alpha/c_1c_3 \leq \alpha' \leq \left(1+\frac{1}{n}\right)^{\tau_1+\tau_2}\alpha/c_2c_4$. □

Lemma 11. *Adopt the same notions and symbols as above. For any ring R satisfying (3) and (5), when $\alpha/c_1c_3 \leq \alpha' \leq (1+1/n)^{\tau_1+\tau_2}\alpha/c_2c_4$, we have $P'_{\mathcal{C},\mathcal{A}}\left(\left(U_\beta^n + \overline{t\cdot D_\alpha^H}\right)^\times, \overline{t\cdot D_\alpha^H}\right) \leq e^{l(\tau_1+\tau_2)}P'_{\mathcal{C},\mathcal{A}}\left(\left(U_\beta^n + \bar{D}_\alpha^n\right)^\times, \bar{D}_\alpha^n\right)$. Hence there is a reduction from R-CRLWE$_{\left(U_\beta^n+\overline{t\cdot D_\alpha^H}\right)^\times, \overline{t\cdot D_\alpha^H}}$ to R-CRLWE$_{\left(U_\beta^n+\bar{D}_{\alpha'}^n\right)^\times, \bar{D}_{\alpha'}^n}$.*

4.4 From R-LWE$_{(U_\beta^n+\overline{t\cdot D_\alpha^H})^\times, \overline{t\cdot D_\alpha^H}}$ to R-CRLWE$_{(U_\beta^n+\overline{t\cdot D_\alpha^H})^\times, \overline{t\cdot D_\alpha^H}}$

Lemma 12. *Adopt the same notions and symbols in Def. 7 and Def. 8. Assume the advantage of any probabilistic polynomial time algorithm to solve the decisional* R-LWE *problem R-LWE$_{(U_\beta^n+\overline{t\cdot D_\alpha^H})^\times, \overline{t\cdot D_\alpha^H}}$ is less than ε, then we have $\left|P'_{\mathcal{C},\mathcal{A}}\left(\left(U_\beta^n + \overline{t\cdot D_\alpha^H}\right)^\times, \overline{t\cdot D_\alpha^H}\right) - Q_{\mathcal{C},\mathcal{A}}\right| < \varepsilon$ for any PPT adversary $\mathcal{A}$.*

Proof. We construct an adversary $\mathcal{B}$ who breaks the decisional R-LWE problem as follows. At the high level, $\mathcal{B}$ will play the role as the challenger $\mathcal{C}$ in the experiment. Given samples $(x_1, y_1), \ldots, (x_l, y_l)$, the algorithm $\mathcal{B}$ sets $a_i = x_i$ and $b_i = \lfloor y_i \rfloor_p$ for $i \leqslant l$, and $X = (a_1, b_1), \ldots, (a_l, b_l)$. Since $\mathcal{B}$ can obtain all the view of any challenger $\mathcal{C}$, $\mathcal{B}$ can simulate all the behaviors of $\mathcal{C}$ and compute the corresponding Input and Target. $\mathcal{B}$ also check whether the Output of $\mathcal{A}$ equals the Target. If the check is passed, $\mathcal{B}$ outputs 1; otherwise it outputs 0.

When $(x_1, y_1), \ldots, (x_l, y_l)$ are R-LWE samples,

$$\Pr(\mathcal{B}((x_1, y_1), \ldots, (x_l, y_l)) = 1) = P'_{\mathcal{C},\mathcal{A}}\left(\left(U_\beta^n + \overline{t\cdot D_\alpha^H}\right)^\times, \overline{t\cdot D_\alpha^H}\right);$$

by contrast, when $(x_1, y_1), \ldots, (x_l, y_l)$ are uniform samples,

$$\Pr(\mathcal{B}((x_1, y_1), \ldots, (x_l, y_l)) = 1) = Q_{\mathcal{C},\mathcal{A}}$$

for adversary $\mathcal{A}$. Thus, assuming the hardness of decisional ring-LWE, we have $\left|P'_{\mathcal{C},\mathcal{A}}\left(\left(U_\beta^n + \overline{t\cdot D_\alpha^H}\right)^\times, \overline{t\cdot D_\alpha^H}\right) - Q_{\mathcal{C},\mathcal{A}}\right| < \varepsilon$ for negligible ε.

□

4.5 From R-$\mathsf{LWE}_{U_\beta^n+\overline{t\cdot D_\alpha^H},\overline{t\cdot D_\alpha^H}}$ to R-$\mathsf{LWE}_{(U_\beta^n+\overline{t\cdot D_\alpha^H})^\times,\overline{t\cdot D_\alpha^H}}$

Lemma 13. *Let $D_{\hat{\alpha}}^n$ be a continuous Gaussian with width $\hat{\alpha}$ and D_α^H be a continuous Gaussian over H with width α. Let $t = f'(\zeta)$. If the assumption (3) and (5) holds, when $\frac{\alpha}{(1+1/n)^{\tau_1+\tau_2}c_1c_3} \le \hat{\alpha} \le \frac{\alpha}{c_2c_4}$, we have $RD_\infty(D_{\hat{\alpha}}^n | t\cdot D_\alpha^H) \le e^{\tau_1+\tau_2}$.*

The proof is similar to Lemma 10. We omit the details and recommend readers to refer the full version [19].

Lemma 14. *Let $D_{\hat{\alpha}}^n$ be a continuous Gaussian distribution over $K_\mathbb{R}$ where $K \cong \mathbb{Q}[X]/(f(X))$. The largest degree of the irreducible factors modulo integer q of the polynomial f is less than k_q. Let $\hat{\alpha} \ge \sqrt{n\ln(n/\varepsilon)}q^{k_q/n}\cdot\delta_K$ and β is any positive integer. If $a \leftarrow U_\beta^n + \overline{D_{\hat{\alpha}}^n}$, the probability of that a is invertible is larger than $1 - q^{-k_q} - \varepsilon$.*

Proof. Our goal is to bound the probability that a is in $\mathcal{I} := \langle q, \phi\rangle$ by $q^{-n/k_q}+\varepsilon$, for any $k \le k_q$, when $a \leftarrow U_\beta^n + \overline{D_{\hat{\alpha}}^n}$. Specifically, denote $a := a_1 + a_2$ where $a_1 \leftarrow U_\beta^n$ and $a_2 \leftarrow \overline{D_{\hat{\alpha}}^n}$. We have $\mathcal{N}(\mathcal{I}) \ge q^{k_q}$. By Minkowski's theorem, this implies $\lambda_1(\mathcal{I}) \le \sqrt{n}q^{k_q/n}$. Since $\mathcal{I}$ is an ideal of R, we have $\lambda_n(\mathcal{I}) = \lambda_1(\mathcal{I})$. Then, in Lemma 2, we have $\lambda_n(\mathcal{I}) \le \sqrt{n}q^{k_q/n}\cdot\delta_K$, and in Lemma 3, we have $\eta_\varepsilon(\mathcal{I}) \le \sqrt{\ln(n/\varepsilon)}\lambda_n(\mathcal{I}) \le \sqrt{n\ln(n/\varepsilon)}q^{k_q/n}\cdot\delta_K$. In addition, Lemma 4 shows that the statistical distance between $b \bmod \mathcal{I}$ and a uniform distribution modulo $\mathcal{I}$ is less than ε for $b \leftarrow D_{\hat{\alpha}}^n$. Since $a_1 = \lfloor b \rceil \in R$ and $\mathcal{I} \subseteq R$, a_1 will be uniform in $R \bmod \mathcal{I}$ with a statistical distance ε. This implies that $a = a_1 + a_2$ is uniform in $R \bmod \mathcal{I}$ with statistical distance ε. So we have $a = 0 \bmod \mathcal{I}$ with probability less than $q^{-k_q} + \varepsilon$. When we set $\varepsilon = 1/2$, we get the desired result. □

Lemma 15. *Following the above notations. For any ring R satisfying (3) and (5), when $\alpha \ge c_2c_4\sqrt{n\ln(2n)}q^{2/n}\cdot\delta_K$, there is a reduction from R-$\mathsf{LWE}_{U_\beta^n+\overline{t\cdot D_\alpha^H},\overline{t\cdot D_\alpha^H}}$ to R-$\mathsf{LWE}_{(U_\beta^n+\overline{t\cdot D_\alpha^H})^\times,\overline{t\cdot D_\alpha^H}}$.*

Proof. Let $\Pr(\mathcal{A}^{\mathcal{O}_{\chi,s}} = 1) = p_0(s)$, $\Pr(\mathcal{A}^{\mathcal{U}(R_q\times R_q)} = 1) = p_1$ and the set S_ε denote the all s that $|p_0(s) - p_1| > \varepsilon$ for any non-negligible ε, then we have

$$
\begin{aligned}
&\Pr\left(s \in S_\varepsilon | s \leftarrow U_\beta^n + \overline{t\cdot D_\alpha^H}\right)\\
=&\Pr\left(s \in S_\varepsilon | s \leftarrow \left(U_\beta^n + \overline{t\cdot D_\alpha^H}\right)^\times\right)\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{t\cdot D_\alpha^H}\right)\\
+&\Pr\left(s \in S_\varepsilon | s \leftarrow U_\beta^n + \bar{D}_\alpha^H \text{and output when } s \text{ not invertible}\right)\\
&\Pr\left(s \text{ is not invertible} | s \leftarrow U_\beta^n + \bar{D}_\alpha^H\right)\\
\ge&\Pr\left(s \in S_\varepsilon | s \leftarrow \left(U_\beta^n + \overline{t\cdot D_\alpha^H}\right)^\times\right)\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{t\cdot D_\alpha^H}\right).
\end{aligned}
$$

Next, Lemma 13 says for $\frac{\alpha}{(1+1/n)^{\tau_1+\tau_2}c_1c_3} \leq \hat{\alpha} \leq \frac{\alpha}{c_2c_4}$,

$$\begin{aligned}\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{t \cdot D_\alpha^H}\right) &\geq \frac{\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{D_{\hat{\alpha}}^n}\right)}{RD_\infty(D_{\hat{\alpha}}^n \parallel t \cdot D_\alpha^H)} \\ &\geq \frac{\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{D_{\hat{\alpha}}^n}\right)}{\exp(\tau_1+\tau_2)}\end{aligned}$$

In addition, in Lemma 14 we have proved $\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{D_{\hat{\alpha}}^n}\right)$ is non-negligible for $\hat{\alpha} \geq \sqrt{n\ln(n/\varepsilon)}q^{k_q/n} \cdot \delta_K$. So $\Pr\left(s \in R_q^\times | s \leftarrow U_\beta^n + \overline{t \cdot D_\alpha^H}\right)$ is also non-negligible. This implies $\Pr\left(s \in S | s \leftarrow U_\beta^n + \overline{t \cdot D_\alpha^H}\right)$ is non-negligible as long as $\Pr\left(s \in S | s \leftarrow \left(U_\beta^n + \overline{t \cdot D_\alpha^H}\right)^\times\right)$ is also non-negligible, i.e. an adversary can solve $R\text{-}\mathsf{LWE}_{U_\beta^n + \overline{t \cdot D_\alpha^H}, \overline{t \cdot D_\alpha^H}}$ so long as it can solve $R\text{-}\mathsf{LWE}_{\left(U_\beta^n + \overline{t \cdot D_\alpha^H}\right)^\times, \overline{t \cdot D_\alpha^H}}$. □

4.6 From $R\text{-}\mathsf{LWE}_{\overline{t \cdot D_\alpha^H}, \overline{t \cdot D_\alpha^H}}$ to $R\text{-}\mathsf{LWE}_{U_\beta^n + \overline{t \cdot D_\alpha^H}, \overline{t \cdot D_\alpha^H}}$

Lemma 16. *Let $\psi = \overline{t \cdot D_\alpha^H} + U_\beta^n$ be a distribution. If there is a PPT algorithm $\mathcal{A}'$ that distinguishes $\mathcal{O}_{s,\chi}$ from $\mathcal{U}$ within m queries for $s \leftarrow \psi$, then there is a PPT algorithm $\mathcal{A}$ which distinguishes $\mathcal{O}_{s,\chi}$ from $\mathcal{U}$ within m queries for $s \leftarrow \overline{t \cdot D_\alpha^H}$.*

Proof. Given m elements $(a_i, b_i) \in R_q \times R_q$, drawn from either $\left(\mathcal{O}_{s,\bar{D}_\alpha}\right)^m$ for $s \leftarrow \overline{t \cdot D_\alpha^H}$, or $(\mathcal{U}(R_q \times R_q))^m$, the reduction algorithm chooses $s' \leftarrow U_\beta^n$ and outputs m elements $(a_i, b_i + a_i s') \in R_q \times R_q$. Obviously, when (a_i, b_i) are drawn from $\mathcal{O}_{s,\bar{D}_\alpha}$, $(a_i, b_i + a_i s')$ are drawn from $\mathcal{O}_{s+s',\bar{D}_\alpha}$ and the distribution of $s + s'$ will be $\psi = \overline{t \cdot D_\alpha^H} + U_\beta^n$. When (a_i, b_i) are all drawn from $\mathcal{U}(R_q \times R_q)$, $(a_i, b_i + a_i s')$ are also drawn from $\mathcal{U}(R_q \times R_q)$. □

5 Application I: A Public Key Encryption

In this section, we will provide an IND-CPA secure PKE scheme based on the R-CLWR assumption. Our scheme improves R-LWE based schemes in both time and space efficiency. At a high level, our scheme uses the standard KEM-DEM approach, where the KEM, similar to that of [53], stems from an IND-CPA secure scheme.

5.1 Reconciliation Mechanism.

Reconciliation was firstly proposed by [25], and has a few variants, for example, [53, 3]. In this paper, for the ease of presentation, we will follow the work of [53].

Let us define the reconciliation rounding function as $[\cdot]_{2,q} : x \to \left\lfloor \frac{2}{q} \cdot x \right\rceil \bmod 2$, and the reconciliation cross-rounding function as $\langle \cdot \rangle_{2,q} : x \to \left\lfloor \frac{4}{q} \cdot x \right\rceil \bmod 2$. Then the algorithm $\textsc{Rec}$ will be defined as follows. On input $y \in \mathbb{Z}_q$ and $z \in \{0,1\}$, $\textsc{Rec}(y,z)$ outputs $[x]_{2,q}$, where x is the closest element to y such that $\langle x \rangle_{2,q} = z$. First, when q is even, we have following results.

Lemma 17. *If $x \in \mathbb{Z}_q$ is uniformly random, $[x]_{2,q}$ is uniformly random given $\langle x \rangle_{2,q}$.*

Lemma 18. *If $|x-y| < q/8$, then we have $\textsc{Rec}(y, \langle x \rangle_{2,q}) = [x]_{2,q}$.*

On the other hand, when the modulus q is odd, we make use of a randomized doubling function: let $\textsc{Dbl} : \mathbb{Z}_q \to \mathbb{Z}_{2q}, x \mapsto \textsc{Dbl}(x) = 2x - e$, where e is sampled from $\{-1, 0, 1\}$ with probabilities $p_{-1} = p_1 = 1/4$ and $p_0 = 1/2$. We have two similar lemmas.

Lemma 19. *For odd q, if $x \in \mathbb{Z}_q$ is uniformly random and $\bar{x} \leftarrow_{\$} \textsc{Dbl}(x)$, then $[\bar{x}]_{2,2q}$ is uniformly random given $\langle \bar{x} \rangle_{2,2q}$.*

Lemma 20. *For odd q , let $|x-y| < q/8$ for $x, y \in \mathbb{Z}_q$. Let $\bar{x} = \textsc{Dbl}(x)$. Then $\textsc{Rec}\left(y, \langle \bar{x} \rangle_{2,2q}\right) = [\bar{x}]_{2,2q}$.*

Moreover, the above reconciliation mechanism can be extended coefficient-wise to R_q with respect to the power basis.

5.2 PKE Schemes

Before describing our R-CLWR based PKE, let us recall a variant of the R-LWE based scheme in [53]. This scheme slightly differentiate from [53] in that the element a in a public key is derived from a PRNG which can be modeled as a random oracle. This modification is adopted by many (R-)LWE based schemes such as [3, 13, 15]. For simplicity, we choose the ring $R = \mathbb{Z}[x]/(x^n + 1)$ where n is a power of 2. Here q is odd, since Theorem 1 requires a prime q.

Ring-LWE Based PKE. Let $\mathcal{H} : \{0,1\}^n \to \{0,1\}^k$ be a hash function for integer k. $\mathcal{G} : \{0,1\}^{k'} \to R_q$ be a pusedorandom generator. The R-LWE based scheme consists of the following three algorithms.

- $\mathsf{RLWE.KeyGen}(1^\lambda)$: Given the security parameter λ, choose $seed \leftarrow \{0,1\}^{k'}$, $a = \mathcal{G}(seed) \in R_q$ and $s, e_1 \leftarrow \overline{t \cdot D_\alpha^H}$. Output $(seed, b = sa + e_1) \in \{0,1\}^{k'} \times R_q$ as the public key and s as the secret key.
- $\mathsf{RLWE.Encryption}(pk = (seed, b), m \in \{0,1\}^k)$: Given the message m, choose $r, e_2, e_3 \leftarrow \overline{t \cdot D_\alpha^H}$. Compute $\hat{v} = br + e_2$ and $v = \langle \textsc{Dbl}(\hat{v}) \rangle_{2,2q}$. Also compute $a = \mathcal{G}(seed)$, $u = ra + e_3$ and $w = \mathcal{H}\left([\textsc{Dbl}(\hat{v})]_{2,2q}\right) \oplus m$. The ciphertext is $ct = (u, v, w) \in R_q \times \{0,1\}^n \times \{0,1\}^k$.
- $\mathsf{RLWE.Decryption}(ct = (u, v, w), sk = s)$: Compute $v' = su$ and output $m' = w \oplus \mathcal{H}(\textsc{Rec}(v', v))$.

Correctness. In fact, $\hat{v} = br + e_2 = (as + e_1)r + e_2 = asr + (e_1 r + e_2)$ and $v' = su = (ar + e_3)s = asr + se_3$. Suppose each coefficient of e_1, e_2, e_3, r, s is bounded by B with overwhelming probability, we have $|e_2 r + e_1| \leq nB^2 + B$ and $|se_3| \leq nB^2$. To ensure correctness, we need to make sure $|\hat{v} - v'| < q/8$, hence we require

$$2nB^2 + B < q/8. \tag{7}$$

Ring-CLWR Based PKE. Next, we describe the R-CLWR version of the above scheme. Firstly, as mentioned in the §1.1, we make use of a probabilistic function $\text{INV}(\cdot) : \mathbb{Z}_p \to \mathbb{Z}_q$ that takes $x \in \mathbb{Z}_p$ as input and uniform randomly chooses an element from the set $\{u \in \mathbb{Z}_q | \lfloor u \rfloor_p = x\}$ as the output. Apparently, we have $\lfloor \text{INV}(\lfloor x \rfloor_p) \rfloor_p = \lfloor x \rfloor_p$ and $\text{INV}(\lfloor x \rfloor_p)$ is uniform in $\mathbb{Z}_q$ when x is uniform in $\mathbb{Z}_q$. We extend $\text{INV}(\cdot)$ coefficient-wisely to R_q with respect to the power basis. Also note that both $\text{INV}(\cdot)$ and its extension to R_q are polynomial time algorithms. so long as p, q and n are of polynomial size.

- $\mathsf{RCLWR.KeyGen}(1^\lambda)$: Given the security parameter λ, choose a $seed \leftarrow \{0,1\}^{k'}$ and $a = \mathcal{G}(seed) \in R_q$. Then, sample s from $(U_\beta^n)^\times$ by repeating $s \leftarrow U_\beta^n$ until s is invertible. Output $(seed, b = \lfloor sa \rfloor_p)$ as the public key and s as the secret key.
- $\mathsf{RCLWR.Encryption}(pk = (seed, b), m \in \{0,1\}^k)$: Given a message m, sample r from $(U_\beta^n)^\times$ by repeating $r \leftarrow U_\beta^n$ until r is invertible. Compute $\bar{v} = \lfloor \text{INV}(b) r \rfloor_p$, $\hat{v} = \text{INV}(\bar{v})$ and $v = \langle \text{DBL}(\hat{v}) \rangle_{2,2q}$. Also compute $a = \mathcal{G}(seed)$, $u = \lfloor ra \rfloor_p$ and $w = \mathcal{H}([\text{DBL}(\hat{v})]_{2,2q}) \oplus m$. The ciphertext is $ct = (u, v, w) \in R_p \times \{0,1\}^n \times \{0,1\}^k$.
- $\mathsf{RCLWR.Decryption}(ct = (u, v, w), sk = s)$: Compute $v' = s\text{INV}(u)$ and output $m' = w \oplus \mathcal{H}(\text{REC}(v', v))$.

Correctness. To show the correctness of the scheme, we need to make sure $|\hat{v} - v'| < q/4$. Specifically, we have

$$\hat{v} = \text{INV}(\bar{v}) = \text{INV}(b) r + e_1 = (as + e_2) r + e_1 = asr + (e_2 r + e_1)$$

and

$$v' = s\text{INV}(u) = (ar + e_3)s = asr + se_3.$$

When the secret is drawn from a uniform distribution U_β^n, we have $|e_1| \leq q/p$, $|e_2| \leq q/p$ $|e_3| \leq q/p$, $|r| \leq \beta$, $|s| \leq \beta$. We have $|e_2 r + e_1| \leq n\beta q/p + q/p$ and $|se_3| \leq n\beta q/p$, hence we require

$$2n\beta q/p + q/p < q/8. \tag{8}$$

5.3 Security Proof

In this subsection, we prove the IND-CPA security of the above PKEbased on R-CLWR assumption as per Def. 7.

First, we will reduce the IND-CPA security to searching the pre-image of a hash function $\mathcal{H}$ through the following Game.

1. The challenger $\mathcal{C}$ gives the adversary $\mathcal{A}$ the public key pk.
2. $\mathcal{A}$ chooses two messages m_0 and m_1 and gives them to the challenger.
3. $\mathcal{C}$ chooses a random bit b and gives $\mathcal{A}$ a ciphertext ct_b that encrypts m_b.
4. The adversary $\mathcal{A}$ outputs a bit b' as a guess of b.

Since $\mathcal{H}$ is modeled as a random oracle, the adversary $\mathcal{A}$ will successfully guess the bit b with probability $1/2$, unless he has previously queried the value $[\textsc{Dbl}(\hat{v})]_{2,2q}$ corresponding to the challenge ciphertext to the random oracle. Therefore, we can construct an adversary $\mathcal{A}'$ from $\mathcal{A}$, which, upon inputting the public key pk and $(u, v) \in R_p \times \{0,1\}^n$, outputs the value $[\textsc{Dbl}(\hat{v})]_{2,2q}$. In a bit more details, when $\mathcal{A}'$ receives pk and $(u, v) \in R_p \times \{0,1\}^n$, it returns pk to $\mathcal{A}$. When $\mathcal{A}$ generates the message pair (m_0, m_1), $\mathcal{A}'$ chooses $r \leftarrow \{0,1\}^n$, $b \leftarrow \{0,1\}$ and sends $\mathcal{A}$ the ciphertexts $(u, v, m_b \oplus r)$. In the meantime, $\mathcal{A}'$ answers the $\mathcal{H}$ queries of $\mathcal{A}$ by keeping a random oracle table. Since we have assumed that $\mathcal{A}$ successfully guesses the bit b with a non-negligible advantage, the value of $[\textsc{Dbl}(\hat{v})]_{2,2q}$ must be queried by $\mathcal{A}$ with a non-negligible probability. Consequently, $\mathcal{A}'$ can successfully output the value $[\textsc{Dbl}(\hat{v})]_{2,2q}$ with a non-negligible probability.

Next, we will show that the success probability of $\mathcal{A}'$ is negligible under the R-CLWRassumption. Specifically, we can construct following games.

Game 1. Choose $a \leftarrow R_q$ and $s, r \leftarrow (U_\beta^n)^\times$. $b = \lfloor sa \rfloor_p$, $\bar{v} = \lfloor \textsc{Inv}(b) r \rfloor_p$, $\hat{v} = \textsc{Inv}(\bar{v})$, $v = \langle \textsc{Dbl}(\hat{v}) \rangle_{2,2q}$ and $u = \lfloor ra \rfloor_p$. $\mathcal{A}'$ is given (u, v) and its target is to compute $[\textsc{Dbl}(\hat{v})]_{2,2q}$.

Game 2. Choose $a \leftarrow R_q$ and $s, r \leftarrow (U_\beta^n)^\times$. $b \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$, $\bar{v} = \lfloor \textsc{Inv}(b) r \rfloor_p$, $\hat{v} = \textsc{Inv}(\bar{v})$, $v = \langle \textsc{Dbl}(\hat{v}) \rangle_{2,2q}$ and $u = \lfloor ra \rfloor_p$. $\mathcal{A}'$ is given (u, v) and its target is to compute $[\textsc{Dbl}(\hat{v})]_{2,2q}$.

Game 3. Choose $a \leftarrow R_q$ and $s, r \leftarrow (U_\beta^n)^\times$. $c \leftarrow R_q$, $\bar{v} = \lfloor cr \rfloor_p$, $\hat{v} = \textsc{Inv}(\bar{v})$, $v = \langle \textsc{Dbl}(\hat{v}) \rangle_{2,2q}$ and $u = \lfloor ra \rfloor_p$. $\mathcal{A}'$ is given (u, v) and its target is to compute $[\textsc{Dbl}(\hat{v})]_{2,2q}$.

Game 4. Choose $a \leftarrow R_q$ and $s, r \leftarrow (U_\beta^n)^\times$. $c \leftarrow R_q$, $\bar{v} \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$, $\hat{v} = \textsc{Inv}(\bar{v})$, $v = \langle \textsc{Dbl}(\hat{v}) \rangle_{2,2q}$ and $u \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$. $\mathcal{A}'$ is given (u, v) and its target is to compute $[\textsc{Dbl}(\hat{v})]_{2,2q}$.

Firstly, we define var_1,var_2, con and $\mathcal{C}$ as follows. We set con as the distribution of choosing r from $(U_\beta^n)^\times$. Let var_1 be the distribution of (a, b) where $b = \lfloor sa \rfloor_p$ and var_2 be the distribution of (a, b) where $b \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$. The challenger $\mathcal{C}$ computes $\mathsf{Input} = (\lfloor ra \rfloor_p, \langle \textsc{Dbl}(\textsc{Inv}(\lfloor \textsc{Inv}(b) r \rfloor_p)) \rangle_{2,2q}) = (u, v)$ and $\mathsf{Target} = [\textsc{Dbl}(\textsc{Inv}(\lfloor \textsc{Inv}(b) r \rfloor_p))]_{2,2q}$. According to the R-CLWR assumption, if the success probability for any $\mathcal{A}$ is negligible when $b \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$, that is also negligible when (a, b) is an R-LWR instance. Therefore, the success probability of Game 1 is negligible if that of Game 2 is negligible.

Secondly, the success probability of Game 2 and that of Game 3 are same, since $\textsc{Inv}(b)$ is uniform in R_q for $b \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$, and the views and the goals of the adversary in both games remain the same.

Thirdly, we define var_1, var_2, con and $\mathcal{C}$ as follows. We set con to be dummy. Let var_1 be the distribution of $((c, \bar{v}), (a, u))$ where $\bar{v} = \lfloor cr \rfloor_p$ and $u = \lfloor ra \rfloor_p$, while S_2 to be the distribution of $((c, \bar{v}), (a, u))$ where $\bar{v}, u \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$. The

challenger $\mathcal{C}$ computes the $\mathsf{Input} = (u, \langle \textsc{Dbl}(\textsc{Inv}(\bar{v}))\rangle_{2,2q}) = (u, v)$ and $\mathsf{Target} = [\textsc{Dbl}(\textsc{Inv}(\bar{v}))]_{2,2q}$.

According to the R-CLWR assumption, if the success probability for any $\mathcal{A}$ is negligible when $\bar{v}, u \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$, then that is also negligible when $((c, \bar{v}), (a, u))$ is an R-LWR instance. Therefore, the success probability of Game 3 is negligible if that of Game 4 is negligible.

Finally, u and $\bar{v}$ are independent in Game 4. Since $\bar{v} \leftarrow \mathcal{U}(\lfloor R_q \rfloor_p)$, $\textsc{Inv}(\bar{v})$ is uniform in R_q. According to Lemma 19, $[\textsc{Dbl}(\textsc{Inv}(\bar{v}))]_{2,2q}$ is uniformly random given $\langle \textsc{Dbl}(\textsc{Inv}(\bar{v}))\rangle_{2,2q}$, so the success probability of Game 4 is negligible.

Combining all above analyses, we conclude that the success probability of $\mathcal{A}'$ in Game 1 is negligible under the R-CLWR assumption. In other words, the R-CLWR based PKE scheme is IND-CPA secure.

5.4 Parameters and Comparisons

Time Complexity. As discussed in the introduction, the sampling subroutine is usually the most intricate part during the implementations. In an R-LWE based scheme, one needs to produce two samplings during the key generation and three samplings during the encryption. In comparison, in an R-CLWR based scheme, one only needs to proceed a single sampling for each key generation and encryption. Moreover, an R-LWE based scheme needs to sample from rounded Gaussian, while we can simply sample uniformly from a small interval and reject when it is non-invertible for an R-CLWR based scheme.

In terms of efficiency, we believe that our sampling subroutine will be much more efficient for the following reasons. First, it allows us to save a huge amount of entropy in practice. Secondly, and more importantly, a single sampling routing becomes more efficient in our case as we only require uniform sampling.

Nonetheless one may be concerned that the overall improvement may not be as much due to the required rejection sampling. Here, we give two arguments. Firstly, the total number of samples required to generate a valid one will be small according to Hoeffding's inequality. This is shown in Lemma 21. In the meantime, the invertibitiy check for a ring element can be carried out efficiently through the extended GCD algorithm.

Lemma 21. *Let D^n_α be a continuous Gaussian distribution over $K_\mathbb{R}$ where $K \cong \mathbb{Q}[X]/(f(X))$. The largest degree of the irreducible factors modulo integer q of the polynomial f is less than k_q. Let $\hat{\alpha} \geq \sqrt{n \ln(n/\varepsilon)} q^{k_q/n} \cdot \delta_K$ and $\beta > 3n\hat{\alpha}$. If $b \leftarrow U^n_\beta$, the probability of that b is invertible is larger than $1 - 2q^{-k_q} - 2\varepsilon$.*

Proof. According to Lemma 14, when $a \leftarrow U^n_\beta + \overline{D^n_{\hat{\alpha}}}$, the probability of that a is non-invertible is smaller than $q^{-k_q} + \varepsilon$. According to Lemma 6, $\mathsf{RD}_2(U^n_\beta \parallel U^n_\beta + \overline{D^n_{\hat{\alpha}}}) = \mathsf{RD}_2(U_\beta \parallel U_\beta + \overline{D_{\hat{\alpha}}})^n \leq 2$. So

$$\Pr(b \text{ is non-inv}) \leq \Pr(a \text{ is non-inv}) \cdot \mathsf{RD}_2\left(U^n_\beta \parallel U^n_\beta + \overline{D^n_{\hat{\alpha}}}\right) \leq 2q^{-k_q} + 2\varepsilon. \quad \square$$

Space Complexity. Next, we will choose the parameters for these two schemes to deliver a fair comparison. As motivated in the introduction, we aim to keep decryption failure probability less than $O(1/e^n)$.

For the R-LWE based scheme, as per average-case/worst-case reduction in Theorem 3, $\alpha = \Omega(n^{1/4}\log^{1/4} n)$. Since $R = \mathbb{Z}[x]/(x^n+1)$, we have $c_1 = c_2 = 1/\sqrt{n}$, $c_3 = c_4 = 1/n$. Since $t = n \cdot \zeta^{n-1}$, each coefficient of the error from $\overline{t \cdot D_\alpha^H}$ is one-dimensional rounded Gaussian with width $\alpha' = n^{1.5}\alpha$, which is smaller than $B = \Omega(n^{0.5}\alpha') = \Omega(n^{0.5}\alpha/c_2c_4) = \Omega(n^{2.25}\log^{1/4} n)$ with probability $1 - O(e^{-n})$. To make sure that (7) holds with probability $1 - O(e^{-n})$, we must choose $q = \Omega(n^{5.5}\log^{0.5} n)$. If we set $q = n^{5.5}\log^{0.5} n$, the public key has size of $k' + n\log(q) = k' + 2.75 \cdot n\log n$ and the ciphertext has size of $k + n + n\log(q) = k + n + 2.75 \cdot n\log n$.

For the R-CLWR based scheme with uniform secret, according to the reductions, $\beta = \Omega(n\alpha') = \Omega(n^{2.75}\log^{1/4} n)$ and $q/p = \Omega(n^{2.75}\log^{0.75} n)$. To make sure that (8) holds with overwhelming probability, we can choose $q = n^{6.5}\log n$ and $p = n^{3.75}\log^{1/4} n$. That results in the public key of size $k' + n\log(p) = k' + 0.9375 \cdot n\log n$ and the ciphertext of size $k + n + n\log(p) = k + n + 0.9375 \cdot n\log n$.

6 Application II: Diffie-Hellman type Key Exchange

For completeness, we also describe a key exchange protocol based on R-CLWR with binary secret. The protocol is described in Table 4. Alice and Bob previously share the public ring element $a \in R_q$. For every new exchange instance, Alice and Bob generate their secret ring elements s, s' respectively, which are uniformly over $(U_\beta^n)^\times$. κ and κ' are the session key which are finally acquired by Alice and Bob respectively.

Alice		**Bob**
$s \leftarrow_\$ (U_\beta^n)^\times$		
$b = \lfloor as \rceil_p \in R_p$		
	$\xrightarrow{b}$	
		$s' \leftarrow_\$ (U_\beta^n)^\times$
		$w' = \lfloor \textsc{Inv}(b)s' \rangle \rfloor_p$
		$b' = \lfloor as' \rfloor_p \in R_p^k$
		$c = \langle \textsc{Dbl}(\textsc{Inv}(w')) \rangle_{2,q}$
		$km' = [\textsc{Dbl}(\textsc{Inv}(w'))]_{2,2q}$
		$\kappa' = \mathcal{H}(km')$
	$\xleftarrow{b',c}$	
$d = \left\lceil \frac{q}{p} b' \right\rfloor s$		
$km = \textsc{Rec}\,(\textsc{Dbl}(d), c)$		
$\kappa = \mathcal{H}(km)$		

Table 4. A key exchange protocol based on R-CLWR.

The security proof is similar to the PKEscheme in Section 5, since the pusedo-randomness of κ' can be reduced from the computational problem that $\mathcal{A}'$ inputs (b, b', c) and outputs km'. So the proof is similar to the PKE scheme.

7 Application III: New proofs for variant schemes

In this section, we will prove the IND-CPA security of a variant of SABER and ROUND2, under the R-CLWR assumption, for proper parameters and distributions. Below we give an asymptotic simplification of their algorithms. There are two differences between the scheme to be presented and SABER/ROUND2. First, our scheme does not encrypt the message m directly, instead, we encrypt a bit string g and mask m by a one-time pad. Second, during the encryption, we lifted b to R_q before multiplying it by r and rounding. These two modifications make the scheme suitable for our computational assumption.

Theorem 3. *The simplified Round2 and Saber scheme is IND-CPA secure under the R-CLWR assumption R-CLWR$_{p,q,1,\chi}$ and R-CLWR$_{p,q,2,\chi'}$ under the random oracle model.*

The proof is similar to subsection 5.3, and please refer to the full version [19].

Similarly, we can prove the IND-CPA security of the PKE scheme of the ring version of Lizard under R-LWE and R-CLWR, for proper parameters and distributions. We also need an asymptotic simplification of the algorithm that is similar to the scheme in previous subsection.

Theorem 4. *The simplified Lizard scheme is IND-CPA secure under the ring-CLWR assumption R-LWE$_{q,\chi}$ and R-CLWR$_{p,q,2,\chi'}$ in the random oracle model.*

The proof can be found in the full version [19].

8 Conclusion

The learning with rounding over the ring problem is the most practical variants within the (R-)LWX family of problems. However, it is yet still unclear on how to build a proof for polynomial modulus and uniform secret. In this paper, we take an alternative approach by proposing the computational learning with rounding problem over the ring and show that variance practical schemes, including those that are among most practical solutions in NIST PQC competitions, can be derived from this provable secure framework.

Acknowledge

The authors would like to thank Jiang Zhang, Jeffrey Hoffstein and Yunlei Zhao for thoughtful discussions. Also we would like to thank the anonymous reviewers for their valuable comments. This work is supported by the National Key Research and Development Program of China (No. 2017YFB0802000), the National Natural Science Foundation of China (No. U1536205).

References

1. Miklós Ajtai. Generating hard instances of lattice problems (extended abstract). In *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 99–108, 1996.
2. Miklós Ajtai and Cynthia Dwork. A public-key cryptosystem with worst-case/average-case equivalence. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing, El Paso, Texas, USA, May 4-6, 1997*, pages 284–293, 1997.
3. Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange - A new hope. In *25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.*, pages 327–343, 2016.
4. Jacob Alperin-Sheriff and Daniel Apon. Dimension-preserving reductions from LWE to LWR. *IACR Cryptology ePrint Archive*, 2016:589, 2016.
5. Joël Alwen, Stephan Krenn, Krzysztof Pietrzak, and Daniel Wichs. Learning with rounding, revisited - new reduction, properties and applications. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, pages 57–74, 2013.
6. Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Advances in Cryptology - CRYPTO 2009, 29th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2009. Proceedings*, pages 595–618, 2009.
7. Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. *Automata, languages and programming*, pages 403–415, 2011.
8. Hayo Baan, Sauvik Bhattacharya, Oscar Garcia-Morchon, Ronald Rietman, Ludo Tolhuizen, Jose-Luis Torre-Arce, and Zhenfei Zhang. Round2: Kem and pke based on glwr. Cryptology ePrint Archive, Report 2017/1183, 2017. `https://eprint.iacr.org/2017/1183`.
9. Shi Bai, Adeline Langlois, Tancrède Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: Using the rényi divergence rather than the statistical distance. In Tetsu Iwata and Jung Hee Cheon, editors, *Advances in Cryptology - ASIACRYPT 2015 - 21st International Conference on the Theory and Application of Cryptology and Information Security, Auckland, New Zealand, November 29 - December 3, 2015, Proceedings, Part I*, volume 9452 of *Lecture Notes in Computer Science*, pages 3–24. Springer, 2015.
10. Abhishek Banerjee, Chris Peikert, and Alon Rosen. Pseudorandom functions and lattices. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 719–737. Springer, 2012.
11. Sauvik Bhattacharya, Oscar Garcia-Morchon, Thijs Laarhoven, Ronald Rietman, Markku-Juhani O Saarinen, Ludo Tolhuizen, and Zhenfei Zhang. Round5: Compact and fast post-quantum public-key encryption. *Submitted for publication, August*, 2018.
12. Andrej Bogdanov, Siyao Guo, Daniel Masny, Silas Richelson, and Alon Rosen. On the hardness of learning with rounding over small modulus. In *Theory of Cryptography - 13th International Conference, TCC 2016-A, Tel Aviv, Israel, January 10-13, 2016, Proceedings, Part I*, pages 209–224, 2016.
13. Joppe W. Bos, Craig Costello, Leo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring!

practical, quantum-secure key exchange from LWE. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1006–1018, 2016.
14. Joppe W. Bos, Craig Costello, Michael Naehrig, and Douglas Stebila. Post-quantum key exchange for the TLS protocol from the ring learning with errors problem. In *2015 IEEE Symposium on Security and Privacy, SP 2015, San Jose, CA, USA, May 17-21, 2015*, pages 553–570, 2015.
15. Joppe W. Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, and Damien Stehlé. CRYSTALS - kyber: a cca-secure module-lattice-based KEM. *IACR Cryptology ePrint Archive*, 2017:634, 2017.
16. Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013*, pages 575–584, 2013.
17. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Attacks on search RLWE. *IACR Cryptology ePrint Archive*, 2015:971, 2015.
18. Hao Chen, Kristin E. Lauter, and Katherine E. Stange. Vulnerable galois RLWE families and improved attacks. *IACR Cryptology ePrint Archive*, 2016:193, 2016.
19. Long Chen, Zhenfeng Zhang, and Zhenfei Zhang. On the hardness of the computational ring-lwr problem and its applications. Cryptology ePrint Archive, Report 2018/536, 2018. `https://eprint.iacr.org/2018/536`.
20. Yuanmi Chen and Phong Q. Nguyen. BKZ 2.0: Better lattice security estimates. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.
21. Jung Hee Cheon, Duhyeong Kim, Joohee Lee, and Yong Soo Song. Lizard: Cut off the tail! // practical post-quantum public-key encryption from LWE and LWR. *IACR Cryptology ePrint Archive*, 2016:1126, 2016.
22. Kieth Conrad. The different ideal. *Expository papers/Lecture notes. Available at: http://www. math. uconn. edu/ kconrad/blurbs/gradnumthy/different. pdf*, 2009.
23. Ivan Damgård, Valerio Pastro, Nigel Smart, and Sarah Zakarias. Multiparty computation from somewhat homomorphic encryption. In *Advances in Cryptology–CRYPTO 2012*, pages 643–662. Springer, 2012.
24. Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik Vercauteren. Saber: Module-lwr based key exchange, cpa-secure encryption and cca-secure KEM. In *Progress in Cryptology - AFRICACRYPT 2018 - 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings*, pages 282–305, 2018.
25. Jintai Ding. A simple provably secure key exchange scheme based on the learning with errors problem. *IACR Cryptology ePrint Archive*, 2012:688, 2012.
26. Nico Döttling and Jörn Müller-Quade. Lossy codes and a new variant of the learning-with-errors problem. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 18–34, 2013.
27. Léo Ducas and Alain Durmus. Ring-lwe in polynomial rings. In *Public Key Cryptography - PKC 2012 - 15th International Conference on Practice and Theory in Public Key Cryptography, Darmstadt, Germany, May 21-23, 2012. Proceedings*, pages 34–51, 2012.

28. Leo Ducas, Alain Durmus, Tancrede Lepoint, and Vadim Lyubashevsky. *Lattice Signatures and Bimodal Gaussians*. Springer Berlin Heidelberg, 2013.
29. Leo Ducas and Phong Q. Nguyen. Faster gaussian lattice sampling using lazy floating-point arithmetic. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 415–432, 2012.
30. Nagarjun C. Dwarakanath and Steven D. Galbraith. Sampling from discrete gaussians for lattice-based cryptography on a constrained device. *Appl. Algebra Eng. Commun. Comput.*, 25(3):159–180, 2014.
31. Kirsten Eisenträger, Sean Hallgren, and Kristin Lauter. Weak instances of plwe. In *International Workshop on Selected Areas in Cryptography*, pages 183–194. Springer, 2014.
32. Yara Elias, Kristin E Lauter, Ekin Ozman, and Katherine E Stange. Provably weak instances of ring-lwe. In *Annual Cryptology Conference*, pages 63–92. Springer, 2015.
33. Eiichiro Fujisaki and Tatsuaki Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, pages 537–554, 1999.
34. Taher El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pages 10–18, 1984.
35. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206. ACM, 2008.
36. Dennis Hofheinz, Kathrin Hövelmanns, and Eike Kiltz. A modular analysis of the fujisaki-okamoto transformation. In *Theory of Cryptography - 15th International Conference, TCC 2017, Baltimore, MD, USA, November 12-15, 2017, Proceedings, Part I*, pages 341–371, 2017.
37. Nick Howgrave-Graham, Phong Q. Nguyen, David Pointcheval, John Proos, Joseph H. Silverman, Ari Singer, and William Whyte. The impact of decryption failures on the security of NTRU encryption. In *Advances in Cryptology - CRYPTO 2003, 23rd Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 2003, Proceedings*, pages 226–246, 2003.
38. Zhengzhong Jin and Yunlei Zhao. Optimal key consensus in presence of noise. *arXiv preprint arXiv:1611.06150*, 2016.
39. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 - June 3, 2010. Proceedings*, pages 1–23, 2010.
40. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. *Journal of the ACM (JACM)*, 60(6):43, 2013.
41. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In *Advances in Cryptology–EUROCRYPT 2013*, pages 35–54. Springer, 2013.
42. Amit Deo Alex Davidson Rachel Player Eamonn Postlethwaite Fernando Virdia Thomas Wunderer Martin R. Albrecht, Benjamin R. Curtis. Estimate all the LWE, NTRU schemes! `https://estimate-all-the-lwe-ntru-schemes.github.io/docs/`. Accessed May 4, 2018.
43. Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In *Advances in Cryptology -*

CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings, pages 465–484, 2011.
44. Daniele Micciancio and Chris Peikert. Hardness of sis and lwe with small parameters. In *Advances in Cryptology–CRYPTO 2013*, pages 21–39. Springer, 2013.
45. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 372–381, 2004.
46. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM Journal on Computing*, 37(1):267–302, 2007.
47. Daniele Micciancio and Michael Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. *IACR Cryptology ePrint Archive*, 2017:259, 2017.
48. NIST. Post-Quantum Cryptography - Round 1 Submissions. `https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Round-1-Submissions`.
49. NSA. Information Assurance. `https://www.nsa.gov/what-we-do/information-assurance/`.
50. Liu Peide. *Functional Analysis Foundation*. Wuhan University Press, 2001.
51. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342. ACM, 2009.
52. Chris Peikert. An efficient and parallel gaussian sampler for lattices. In *Advances in Cryptology - CRYPTO 2010, 30th Annual Cryptology Conference, Santa Barbara, CA, USA, August 15-19, 2010. Proceedings*, pages 80–97, 2010.
53. Chris Peikert. Lattice cryptography for the internet. In *Post-Quantum Cryptography - 6th International Workshop, PQCrypto 2014, Waterloo, ON, Canada, October 1-3, 2014. Proceedings*, pages 197–219, 2014.
54. Chris Peikert. How (not) to instantiate ring-lwe. In *International Conference on Security and Cryptography for Networks*, pages 411–430. Springer, 2016.
55. Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz. Pseudorandomness of ring-lwe for any ring and modulus. In *Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017*, pages 461–473, 2017.
56. Thomas Pöppelmann, Léo Ducas, and Tim Güneysu. Enhanced lattice-based signatures on reconfigurable hardware. In *CHES*, pages 353–370, 2014.
57. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005*, pages 84–93, 2005.
58. Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *Siam Review*, 41(2):1484–1509, 1996.