Hardness of Module-LWE and Ring-LWE on General Entropic Distributions

Hao Lin[1,2], Yang Wang,[1,2] Mingqiang Wang[1,2]

1. School of Mathematics and System Sciences, Shandong University, Jinan, Shandong 250100, PR China;
lhao17@mail.sdu.edu.cn, wyang1114@mail.sdu.edu.cn, wangmingqiang@sdu.edu.cn
2. China Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education.

Abstract. The hardness of Entropic LWE has been studied in a number of works. However, there is not work study the hardness of algebraically structured LWE with entropic secrets. In this work, we conduct a comprehensive study on establishing hardness reductions for *Entropic Module-LWE* and *Entropic Ring-LWE*. We show an entropy bound that guarantees the security of arbitrary *Entropic Module-LWE* and *Entropic Ring-LWE*, these are the first results on the hardness of algebraically structured LWE with entropic secrets. One of our central techniques is a new generalized leftover hash lemma over ring and a new decomposition theorem for continuous Gaussian distribution on $K_{\mathbb{R}}$, which might be of independent interests.

Keywords: Lattice-based cryptography, Module learning with errors, Ring learning with errors, Entropic Module-LWE, Entropic Ring-LWE.

1 Introduction

1.1 Background

The *learning with errors* (LWE) problem, introduced by Regev [Reg05], is used as a core computational problem in lattice-based cryptography. For a given dimension n, modulus q and error distribution χ, samples of the LWE distribution are constructed as $(\mathbf{a}, b = \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod 1)$, where $\mathbf{a}, \mathbf{s} \in \mathbb{Z}_q^n$ are chosen uniformly at random and e is drawn from the distribution χ. Distinguishing the LWE distribution from uniform is known as the decision LWE problem, whereas finding the secret $\mathbf{s}$ is known as the search LWE problem.

One primary attraction of LWE is that it can be supported by worst-case to average-case reductions from conjectured hard problems on general lattices [Reg05, LPR10, LS15, PRS17]. But while constructions based on LWE can have reasonably good asymptotic efficiency, they are often not as practically efficient as one might like, especially in terms of key and ciphertext sizes. To circumvent this inherent inefficiency, several works have introduced and studied a host of algebraically structured LWE variants.

Inspired by the early NTRU cryptosystem [HPS98] and Micciancio's initial worst-case to average-case reductions for "algebraically structured" lattices over polynomial rings [Mic02], Lyubashevsky et al. [LPR10] introduced *Ring-LWE* to improve the asymptotic and practical efficiency of LWE. Ring-LWE is parameterized by the ring of integers in a number field, and supported the hardness of Ring-LWE by a reduction from conjectured worst-case hard problems on lattices corresponding to ideals in the ring. Informally, for Ring-LWE we first choose a ring R, modulus q and error distribution χ over space $K_{\mathbb{R}}$. Then, to sample the Ring-LWE distribution, we sample $a \in R/qR$, $s \in R^\vee/qR^\vee$ uniformly and error e according to χ. Then we output $(a, b = \frac{1}{q}a \cdot s + e \bmod R^\vee)$ as the Ring-LWE sample, where $R^\vee$ denotes the dual of the ring R. Similar to the case of plain LWE, distinguishing the Ring-LWE distribution from uniform is known as the decision Ring-LWE problem, whereas finding the secret s is known as the search Ring-LWE problem.

Later, Brakerski et al. [BGV12,LS15] introduced *Module-LWE*, Module-LWE comes with hardness guarantees given by lattice problems based on module lattices. Since module lattices have more complicated algebraic structures than ideal lattices, Module-LWE might be able to offer a better level of security than Ring-LWE, while still offering performance advantages over LWE. Informally, for Module-LWE we first choose a ring R, dimension d, modulus q and error distribution χ over space $K_{\mathbb{R}}$. Then, to sample the Module-LWE distribution, we sample $\mathbf{a} \in (R/qR)^d$, $\mathbf{s} \in (R^\vee/qR^\vee)^d$ uniformly and error e according to χ. Then we output $(a, b = \frac{1}{q}\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod R^\vee)$ as the Moudle-LWE sample, where $R^\vee$ denotes the dual of the ring R. Similar to the case of Ring-LWE, distinguishing the Moudle-LWE distribution from uniform is known as the decision Module-LWE problem, whereas finding the secret $\mathbf{s}$ is known as the search module-LWE problem.

Goldwasser et al. [GKP+10] initiated a study on the hardness of LWE when $\mathbf{s}$ is not chosen uniformly at random. This study was motivated by the desire to achieve an *entropic* notion of security that will allow to guarantee that the problem remains hard even if some information about $\mathbf{s}$ is leaked. They show that if $\mathbf{s}$ is sampled from a binary distribution (i.e. supported over $\{0,1\}^n$), then LWE remains hard so long as $\mathbf{s}$ has sufficient entropy. Recently, Brakershi et al. [BD20] show that LWE is also hard so long as $\mathbf{s}$ has sufficient entropy.

Within the NIST standardization process, several candidates rely on the hardness of algebraically structured LWE, e.g., the key encapsulation mechanism Kyber [BDK+18] from the CRYSTALS suite. However, the question of hardness of algebraically structured LWE on imperfect secret distributions has not been studied. To fully enjoy the efficiency brought from the ring structure, it is necessary to determine whether the additional structure would weaken the underlying hard problem. Thus the hardness result for the entropic Moudle-LWE and entropic Ring-LWE is a natural question, and this work aims to conduct a systematic study on these problems.

1.2 Contributions and Technical Overview

Here we give an overview of our contributions. Our first main contribution is a reduction from primal Module LWE (primal Ring-LWE) to Entropic Module-LWE (Section 4). By this we can get the hardness of Entropic Module-LWE. To complete the reduction, we also bring in a new generalized leftover hash lemma over ring and a new decomposition theorem for continuous Gaussian distribution on $K_{\mathbb{R}}$, which might be of independent interest (Section 3). Our second main contribution is a reduction from Entropic Module-LWE to Entropic Ring-LWE (Section 5). By combining the result in Section 4, we can also get the hardness of Entropic Ring-LWE. To the best of our knowledge, these are the first results on the hardness of algebraically structured LWE with entropic secrets. Besides, in [BBP+19] Bolboceanu et al. think high entropy of secrets alone is insufficient to argue Entropic Ring-LWE security. But in this paper, we solve this problem, we prove that high entropy of secrets is enough for the hardness of Entropic Ring-LWE.

Hardness of Entropic Module-LWE. We first give an overview of how to prove the hardness of Entropic Module-LWE. At a high level, we prove the hardness of Entropic Module-LWE by following the structure of the hardness proof of Entropic LWE from Brakerski et al. [BD20]. Their proof framework can be summarized as the following.

- 1. First replace $\mathbf{A}$ by a lossy matrix $\mathbf{BC}+\mathbf{Z}$, and then replace $\mathbf{e}=\mathbf{Fe}_1+\mathbf{e}_2$;
- 2. Show that high noise lossiness $\tilde{H}_\infty(\mathbf{s} \mid \mathbf{s}+\mathbf{e})$ lead to hardness of Entropic LWE;
- 3. Show that high min-entropy $\tilde{H}(\mathbf{s})$ implies noise lossiness.

In the ring setting, by the hardness of primal Module-LWE we can also replace $\mathbf{A}$ by $\mathbf{BC}+\mathbf{Z}$. But since the error term is in $K_{\mathbb{R}}$ and the matrix multiplication in the ring is different from which in R^n, we need to create a new decomposition theorem for continuous Gaussian distribution on $K_{\mathbb{R}}$ first. We note that, if K is a number field which has exactly s_1 real embeddings and s_2 pairs complex embeddings, then when $\mathbf{F}$ is a fixed matrix in $R^{m\times d}$, $\mathbf{e}_1 \leftarrow (D_{r_1}(K_{\mathbb{R}}))^d$ and $\tilde{\mathbf{e}}=\mathbf{Fe}_1$, we have $\sigma_{H_i}(\tilde{\mathbf{e}})$ and $\sigma_{H_j}(\tilde{\mathbf{e}})$ are independent where $i\neq j$ and $|i-j|\neq s_2$. Thus, we can sample $\mathbf{e}_2$ in blocks and make the random variable $\mathbf{Fe}_1+\mathbf{e}_2$ is distribution according to $(D_r(K_{\mathbb{R}}))^m$. We refer the details in Section 3.2.

Besides, in step 2, when we prove the hardness of decision Entropic Module LWE, we need a generalized leftover hash lemma in the ring. We note that, when $K=\mathbb{Q}(\alpha)$ is a number field, where α is an algebraic integer, $f(x)$ is the minimum polynomial of α and $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, then we have R_q is a finite field. By this we can prove a new generalized leftover hash lemma over ring. We refer the details in Section 3.1.

The step 3 are portable to the ring setting, but we also need to take care of some mathematical subtleties in the ring. For the complete analysis and formal statement of the result, see Section 4.

Hardness of Entropic Ring-LWE. When work with Entropic Ring-LWE, we cannot get any leftover hash lemma in $k = 1$. Thus, the above method does not work. But we find that the reduction from Module LWE to Ring LWE [AD17] can be used to get the hardness of Entropic Ring-LWE. We note that if $\mathbf{G} = (1, q, \cdots, q^{d-1}) \in R^{1\times d}$, then the map $h_{\mathbf{G}} : (R_q^\vee)^d \mapsto R_{q^d}^\vee$ given by $h_{\mathbf{G}} = \mathbf{Gs}$ is a bijection. Therefore, if $\mathbf{s}$ is a random variable on $(R_q^\vee)^d$, then $\mathbf{h_G}(\mathbf{s})$ is a random variable on $R_{q^d}^\vee$ and $\tilde{H}_\infty(\mathbf{s}) = \tilde{H}_\infty(\mathbf{h_G}(\mathbf{s}))$. By this and the result from [AD17], we can prove the hardness of Entropic Ring-LWE. For decision Entropic Ring-LWE, we need to show a reduction from decision Entropic Module-LWE to decision Entropic Ring-LWE first, and this reduction can be derived by a similar technique used in the work [PRS17]. For the complete analysis and formal statement of the result, see Section 5.

1.3 Paper Organization

Section 2 contains preliminaries and definitions. In Section 3, we prove two probability lemmas over ring. The Entropic Module-LWE problem is formally defined in Section 4, where the hardness result is proved as well. Finally, we give the definition of Entropic Ring-LWE and prove the hardness result in Section 5.

2 Preliminaries

In this section we review some basic notions and mathematical notations used throughout the paper. We denote the security parameter by λ, and we say a function $f(\lambda)$ is negligible if $f(\lambda) \in \lambda^{-\omega(1)}$. For any positive integer n, we represent the set $\{1, \cdots, n\}$ by $[n]$.

We denote column vectors over $\mathbb{R}^n$ or $\mathbb{C}^n$ by bold lower case letters ($\mathbf{a}$, $\mathbf{b}$, etc.). Matrices over $\mathbb{R}^{m\times n}$ or $\mathbb{C}^{m\times n}$ are denoted by bold upper-case letters ($\mathbf{A}$, $\mathbf{B}$, etc.). For a vector $\mathbf{x}$ over $\mathbb{R}^n$ or $\mathbb{C}^n$, define the ℓ_2 norm as $\|\mathbf{x}\|_2 = (\sum_j |x_j|^2)^{1/2}$, define the ℓ_∞ norm as $\|\mathbf{x}\|_\infty = \max_j |x_j|$. We denote the identity matrix in n dimensions using $\mathbf{I}_n$. The transpose of a matrix or vector will be denoted by $(\cdot)^{\mathrm{T}}$, the conjugate transpose of a matrix or vector will be denoted by $(\cdot)^\dagger$ and the complex conjugate of $z \in \mathbb{C}$ will be written as $\bar{z}$.

An n-dimensional lattice is a discrete subgroup of $\mathbb{R}^n$. Any lattice Λ can be seen as the set of all integer linear combinations of a set of basis vectors $\{\mathbf{b}_1, \cdots, \mathbf{b}_j\}$. The lattices we will be considering will have full rank i.e. $j = n$. We use the matrix $\mathbf{B} = [\mathbf{b}_1, \cdots, \mathbf{b}_n]$ to denote a basis. $\widetilde{\mathbf{B}}$ is used to denote the Gram-Schmidt orthogonalization of columns in $\mathbf{B}$ (from left to right), $\|\mathbf{B}\|$ is the length of the longest vector in ℓ_2 norm of the columns of $\mathbf{B}$ and $\|\mathbf{B}\|_\infty$ is the length of the longest vector in ℓ_∞ norm of the columns of $\mathbf{B}$. The dual of a lattice Λ is defined as $\Lambda^* = \{\mathbf{x} \in \mathrm{span}(\Lambda) : \forall \mathbf{y} \in \Lambda, \langle \mathbf{x}, \mathbf{y}\rangle \in \mathbb{Z}\}$.

2.1 Algebraic Number Theory

Let K be some algebraic number field. The degree of K is equal to the dimension of K as a vector space over $\mathbb{Q}$. For any field element $\alpha \in K$, multiplication by α

is a $\mathbb{Q}$-linear transformation of K into itself, i.e.

$$m_\alpha : K \mapsto K \text{ given by } m_\alpha(x) = \alpha x.$$

The trace of α, denoted by $\mathrm{Tr}(\alpha)$, is defined as the trace of this linear transformation. An element $\alpha \in K$ is said to be integral if it is the root of a monic polynomial with integer coefficients. The set of all integral elements R forms the ring of integers of K. Let $R^\vee = \{x \in K \mid \mathrm{Tr}(xR) \subset \mathbb{Z}\}$ be the dual of R. R is a free $\mathbb{Z}$-module of rank n (the degree of K), i.e. it is the set of all $\mathbb{Z}$-linear combinations of some basis $B = \{b_1, \cdots, b_n\} \subset R$. Also let $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R}$ and define $\mathbb{T}_{R^\vee} := K_\mathbb{R}/R^\vee$.

An ideal $I \subset R$ is a nontrivial additive subgroup that is closed under multiplication by R. Two ideal $I, J \subset R$ are said to be coprime if $I + J = R$. A fractional ideal $I \subset K$ is a set such that $dI \subset R$ is an integral ideal for some $d \in R$. The product ideal IJ is the set of all finite sums of terms ab for $a \in I$, $b \in J$. Multiplication extends to fractional ideal in the obvious way, and the set of fractional ideals forms a group under multiplication; in particular, every fractional ideal I has a (multiplicative) inverse ideal, written I^{-1}.

The (absolute) discriminant Δ_K of a number field K is defined to be the square of the fundamental volume of $\sigma(R)$, the embedded ring of integers. Equivalently, $\Delta_K = |\det(\mathrm{Tr}(b_i \cdot b_j))|$ where $b_1 \cdots, b_n$ is any integral basis of R.

When working with number fields and ideal lattices, it is convenient to work with the space $\mathbb{H} \subset \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}$ for some number $s_1 + 2s_2 = n$, defined as

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

For $j \in [s_1]$, we set $\mathbf{h}_j = \mathbf{e}_j$, and for $j \in \{s_1 + 1, \cdots, s_1 + s_2\}$, we set $\mathbf{h}_j = \frac{\sqrt{2}}{2}(\mathbf{e}_j + \mathbf{e}_{j+s_2})$ and $\mathbf{h}_{j+s_2} = \frac{\sqrt{2}\boldsymbol{i}}{2}(\mathbf{e}_j - \mathbf{e}_{j+s_2})$, where $\mathbf{e}_j \in \mathbb{C}^n$ is the vector with 1 in its j-th coordinate and 0 elsewhere, $\boldsymbol{i}$ is the imaginary number such that $\boldsymbol{i}^2 = -1$. The set $\{\mathbf{h}_j\}_{j\in[n]}$ forms an orthonormal basis of $\mathbb{H}$ as a real vector space. Let $\mathbf{U}_H = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_n]^\dagger$, we can easily get a field isomorphic $\sigma_H : \mathbb{H} \mapsto \mathbb{R}^n$ where $\sigma_H(\mathbf{x}) = \mathbf{U}_H \cdot \mathbf{x}$. Thus $\mathbb{H} \cong \mathbb{R}^n$ as an inner product space. And we will also equip $\mathbb{H}$ with the ℓ_2 and ℓ_∞ norm induced on it from $\mathbb{C}^n$.

We will often use canonical embeddings to endow field elements with a geometry. A number field $K := \mathbb{Q}(\zeta)$ of degree n has exactly $n = s_1 + 2s_2$ field homomorphisms $\sigma_j : K \mapsto \mathbb{C}$ fixing each element of $\mathbb{Q}$. Let $\sigma_1, \cdots, \sigma_{s_1}$ be the real embeddings and $\sigma_{s_1+1}, \cdots, \sigma_n$ be complex. The complex embeddings come in conjugate pairs, so we have $\sigma_j = \overline{\sigma_{j+s_2}}$ for $j = s_1 + 1, \cdots, s_1 + s_2$ if we use an appropriate ordering of the embeddings. The canonical embedding is defined as $\sigma_C : K \to \mathbb{H}$ where

$$\sigma_C(x) := (\sigma_1(x), \cdots, \sigma_n(x))^\mathrm{T}.$$

We can also represent $\sigma_C(x)$ via the real vector $\sigma_H(x) \in \mathbb{R}^n$ through the change described above. So for any $x \in K$, $\sigma_H(x) = \mathbf{U}_H \cdot \sigma_C(x)$.

For the ring of integer R of the field K, we define the canonical embedding of the module R^d into the space $\mathbb{H}^d$ in the obvious way, i.e. by embedding each

component of R^d into $\mathbb{H}$ separately. It is well known that the dimension of ring of integers R as a $\mathbb{Z}$-module is equal to the degree of K over $\mathbb{Q}$, that means the lattice $\sigma_H(R)$ is of full rank. We often refer to the ring of integer R as a lattice. Whenever we do this, we are really referring to the lattice $\sigma_H(R)$.

2.2 Probability

The uniform probability distribution over some finite set $\mathcal{M}$ will be denoted by $U(\mathcal{M})$. If s is sampled from a distribution $\mathcal{D}$, we write $s \leftarrow \mathcal{D}$. Also, let $\mathbf{s} = (s_1, \cdots, s_m)^{\mathrm{T}} \leftarrow \mathcal{D}^d$ denote the act of sampling each component s_i according to $\mathcal{D}$ independently. We also write $\mathrm{Supp}(\mathcal{D})$ to mean the support of the distribution $\mathcal{D}$. For a continuous random variable X, denote the probability density function of X by $P_X(\cdot)$ and denote the probability density of X conditioned on an event E by $P_{X|E}(\cdot)$.

The statistical distance is a widely used measure of distribution closeness.

Definition 1 (Statistical distance). *Let X and Y be two discrete probability distributions on a discrete domain $\mathcal{E}$. Their statistical distance is defined as*

$$\Delta(X;Y) = \frac{1}{2}\sum_{x\in\mathcal{E}} |\Pr(X=x) - \Pr(Y=x)|.$$

Likewise, if X and Y are two continuous random variables defined on a measurable set $\mathcal{E}$. Their statistical distance is defined as

$$\Delta(X;Y) = \frac{1}{2}\int_{x\in\mathcal{E}} |P_X(x) - P_Y(x)|dx.$$

The following is the definition of min-entropy and conditional min-entropy.

Definition 2 (Min-entropy). *Given a discrete random variable X over $\mathcal{X}$, the min-entropy of X, denoted by*

$$\widetilde{H}_\infty(X) = -\log(\max_{x\in\mathcal{X}} \Pr[X=x]).$$

Definition 3 (Conditional min-entropy). *Let X be a discrete random variable over $\mathcal{X}$, Z be a random variable over $\mathcal{Z}$, define the conditional min-entropy of X given Z, denoted by*

$$\widetilde{H}_\infty(X \mid Z) = -\log(E_z[\max_{x\in\mathcal{X}} \Pr[X=x \mid Z=z]]).$$

We now state some fundamental properties of the conditional min-entropy.

Lemma 1 (Lemma 2.2 in [DOR+08]). *Let X, Y, Z be random variables, and Y has at most 2^λ possible values, then*

$$\widetilde{H}_\infty(X \mid (Y,Z)) \geq \widetilde{H}_\infty(X \mid Z) - \lambda.$$

Lemma 2 (Adapted from Lemma 5.1 in [BD20]). *Let R be the ring of integers of a field K with degree n, $R^\vee$ be the dual of R. Let q, d be positive integers. Let $\mathbf{s}$ be a random variable over $(R_q^\vee)^d$ with min-entropy $\widetilde{H}_\infty(\mathbf{s})$, χ be a random variable over $(K_\mathbb{R})^d$ and $\mathbf{e} \leftarrow \chi$. Set $\mathbf{y} = \frac{\mathbf{s}}{q} + \mathbf{e} \bmod R^\vee$ be the random variable over $(\mathbb{T}_{R^\vee})^d$. Then it holds that*

$$\widetilde{H}_\infty(\mathbf{s} \mid \mathbf{y}) \geq \widetilde{H}_\infty(\mathbf{s}) - \log[\int_{(\mathbb{T}_{R^\vee})^d} \max_{\mathbf{s}^*} p_{\mathbf{e}}(\mathbf{y} - \frac{\mathbf{s}^*}{q} + (R^\vee)^d) d\mathbf{y}].$$

2.3 Gaussian Measures

Definition 4 (Continuous Gaussian distribution). *The Gaussian function of parameter r and center c is defined as*

$$\rho_{r,c}(x) = \exp(-\pi(x-c)^2/r^2),$$

and the Gaussian distribution $D_{r,c}$ is the probability distribution whose probability density function is given by $\frac{1}{r}\rho_{r,c}$.

A matrix $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ is called positive definite, if it holds for every $\mathbf{x} \in \mathbb{R}^n \backslash \{\mathbf{0}\}$ that $\mathbf{x}^{\mathrm{T}}\mathbf{\Sigma}\mathbf{x} > 0$. For every positive definite matrix $\mathbf{\Sigma}$ there exists a unique positive definite matrix $\sqrt{\mathbf{\Sigma}}$ such that $(\sqrt{\mathbf{\Sigma}})^2 = \mathbf{\Sigma}$.

Definition 5 (Multivariate Gaussian distribution). *Let $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ be a positive definite matrix. The multivariate Gaussian function with covariance matrix $\mathbf{\Sigma}$ centred on $\mathbf{c} \in \mathbb{R}^n$ is defined as*

$$\rho_{\sqrt{\mathbf{\Sigma}},\mathbf{c}}(\mathbf{x}) = \exp(-\pi(\mathbf{x}-\mathbf{c})^{\mathrm{T}}\mathbf{\Sigma}^{-1}(\mathbf{x}-\mathbf{c})),$$

and the corresponding multivariate Gaussian distribution denoted $D_{\sqrt{\mathbf{\Sigma}},\mathbf{c}}$ is defined by the density function $\frac{1}{\sqrt{\det(\mathbf{\Sigma})}}\rho_{\sqrt{\mathbf{\Sigma}},\mathbf{c}}$.

Notice that the matrix $\mathbf{\Sigma}$ differs from the standard covariance matrix by a factor of 2π. However, for convenience, we refer to $\mathbf{\Sigma}$ as the covariance matrix throughout. Note that if the centre $\mathbf{c}$ is omitted, it should be assumed that $\mathbf{c} = \mathbf{0}$. If the covariance matrix is diagonal, we describe it using the vector of its diagonal entries. For example, suppose that $\mathbf{\Sigma}_{ij} = (r_i)^2\delta_{ij}$ and let $\mathbf{r} = (r_1, \cdots, r_n)^{\mathrm{T}}$. Then we would write $D_{\mathbf{r}}$ to denote the centred Gaussian distribution $D_{\mathbf{\Sigma}}$. Furthermore, if $r_1 = \cdots = r_n = r$, we would write D_r to denote this centred Gaussian distribution.

Using the identification of $\mathbb{H}$ as $\mathbb{R}^n$, we can extend the definition of multivariate Gaussian distribution on $\mathbb{R}^n$ to $\mathbb{H}$ as follows. Let $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ be a positive definite matrix, a sample from $D_{\mathbf{\Sigma}}$ on $\mathbb{H}$ is given by $\sum_{i\in[n]} x_i\mathbf{h}_i$, where $\mathbf{x} = (x_1, \cdots, x_n)^{\mathrm{T}} \leftarrow D_{\mathbf{\Sigma}}$ over $\mathbb{R}^n$.

We also have discrete Gaussian distributions i.e. normalised distributions defined over some discrete set (typically lattices or lattice cosets). The notation for a discrete Gaussian distribution over some n-dimensional lattice Λ and coset

vector $\mathbf{u} \in \mathbb{R}^n$ with parameter r is $D_{\Lambda+\mathbf{u},r}$. This distribution has probability mass function $\frac{\rho_r(\mathbf{y})}{\rho_r(\Lambda+\mathbf{u})}$, where $\rho_r(\Lambda+\mathbf{u}) = \sum_{\mathbf{x}\in\Lambda+\mathbf{u}} \rho_r(\mathbf{x})$. For the ring of integers R of a number field K and any $x \in K$, we define $D_{R+x,r}$ to be the discrete Gaussian over the coset $R + x$ of the lattice R, i.e. over the lattice coset $\sigma_H(R) + \sigma_H(x)$ of the lattice $\sigma_H(R)$.

Next we recall the definition and some lemmas of the smoothing parameter of a lattice that we will make use of.

Definition 6 (Smoothing parameter). *For a lattice Λ and any $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is defined as the smallest $s > 0$ s.t. $\rho_{1/s}(\Lambda^* \setminus \{0\}) \leq \epsilon$.*

Lemma 3 (Lemma 3.1 in [GPV08]). *For any $\epsilon > 0$ and n-dimensional lattice Λ with basis $\mathbf{B}$,*

$$\eta_\epsilon(\Lambda) \leq ||\widetilde{\mathbf{B}}||\sqrt{\log(2n(1+1/\epsilon))/\pi}.$$

Lemma 4 (Lemma 2.9 in [MR07]). *For any lattice Λ, positive real $s > 0$ and vector $\mathbf{c}$, $\rho_{s,\mathbf{c}}(\Lambda) \leq \rho_s(\Lambda)$.*

2.4 Ring-LWE and Module-LWE

Let K be a number field of degree n, R be the ring of integers of K, and $R^\vee$ be the dual of R. Also let $K_\mathbb{R} := K \otimes_\mathbb{Q} \mathbb{R}$ and define $\mathbb{T}_{R^\vee} := K_\mathbb{R}/R^\vee$. Note that the distribution over $K_\mathbb{R}$ are sampled by choosing an element of the space $\mathbb{H}$ according to the distribution and then mapping back to $K_\mathbb{R}$ via the isomorphism $\mathbb{H} \cong K_\mathbb{R}$. For example, sampling a distribution D over $K_\mathbb{R}$ is done by sampling D over $\mathbb{H} \cong \mathbb{R}^n$ and then mapping back to $K_\mathbb{R}$. Let $R_q = R/(qR)$ and $R_q^\vee = R^\vee/(qR^\vee)$ for some modulus $q \in \mathbb{Z}$, and let χ be a family of distributions over $K_\mathbb{R}$.

The ring variant of LWE was introduced by Lyubashevshy et al. in [LPR10]. The search problem $\mathrm{RLWE}(K, q, m, \chi)$ is given $(\mathbf{a}, \frac{1}{q}(\mathbf{a}\cdot s) + \mathbf{e} \bmod R^\vee)$, to find $s \in R_q^\vee$, where $\mathbf{a} \leftarrow U((R_q)^m)$, $s \leftarrow U(R_q^\vee)$ and $\mathbf{e} \leftarrow \chi^m$. The decisional version problem $\mathrm{DRLWE}(K, q, m, \chi)$ asks to distinguish between the distributions $(\mathbf{a}, \frac{1}{q}(\mathbf{a}\cdot s) + \mathbf{e} \bmod R^\vee)$ and $(\mathbf{a}, \mathbf{u})$, where $\mathbf{a}$, s and $\mathbf{e}$ are as in the search version and $\mathbf{u} \leftarrow U((\mathbb{T}_{R^\vee})^m)$.

The module variant of LWE was first introduced by Brakerski et al. [BGV12], and thoroughly studied by Langlois and Stehlé [LS15]. The search problem $\mathrm{MLWE}(K, d, q, m, \chi)$ is to find $\mathbf{s} \in (R_q^\vee)^d$ given $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$, where $\mathbf{A} \leftarrow U((R_q)^{m\times d})$, $\mathbf{s} \leftarrow U((R_q^\vee)^d)$ and $\mathbf{e} \leftarrow \chi^m$. The decisional version problem $\mathrm{DMLWE}(K, d, q, m, \chi)$ asks to distinguish between the distributions $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$ and $(\mathbf{A}, \mathbf{u})$, where $\mathbf{A}$, $\mathbf{s}$ and $\mathbf{u}$ are as in the search version and $\mathbf{u} \leftarrow U((\mathbb{T}_{R^\vee})^m)$.

As pointed out by Lyubashevsky et al. [LPR13], sometimes it can be more convenient to work with a discrete variant, where χ is a discrete error distribution over $R^\vee$. Langlois et al. [LS15] showed that $\mathrm{DMLWE}(K, d, q, m, D_{R^\vee,\sqrt{2}q\alpha})$ is at least as hard as $\mathrm{DMLWE}(K, d, q, m, D_\alpha)$ using discretization technique. Here the

DMLWE$(K, d, q, m, D_{R^\vee, \sqrt{2}q\alpha})$ problem asks to distinguish between the distributions $(\mathbf{A}, \mathbf{A}\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$ and $(\mathbf{A}, \mathbf{u})$, where $\mathbf{A} \leftarrow U((R_q)^{m\times d})$, $\mathbf{s} \leftarrow U((R_q^\vee)^d)$, $\mathbf{e} \leftarrow (D_{R^\vee, \sqrt{2}q\alpha})^m$ and $\mathbf{u} \leftarrow U((R_q^\vee)^m)$. By the same way, we can also get that DRLWE$(K, q, m, D_{R^\vee, \sqrt{2}q\alpha})$ is at least as hard as DRLWE(K, q, m, D_α).

Furthermore, Rosca et al. also considered primal-RLWE in [RSW18]. The primal-DRLWE$(K, q, m, D_{R,\alpha})$ problem asks to distinguish between the distributions $(\mathbf{a}, \mathbf{a}\cdot s + \mathbf{e} \bmod qR)$ and $(\mathbf{a}, \mathbf{u})$, where $\mathbf{a} \leftarrow U((R_q)^{m\times 1})$, $s \leftarrow U(R_q)$, $\mathbf{e} \leftarrow (D_{R,\alpha})^m$ and $\mathbf{u} \leftarrow U((R_q)^m)$. In [RSW18] Rosca et al. showed a reduction from RLWE to primal-RLWE with a limited error growth. Later, in [WW18] Wang et al. showed that when the field K is a cyclotomic field, the growth in the error term does not exceed $O(n \log\log n)$. Likewise, we can also consider primal-MLWE. The primal-DMLWE$(K, d, q, m, D_{R,\alpha})$ problem asks to distinguish between the distributions $(\mathbf{A}, \mathbf{A}\cdot\mathbf{s} + \mathbf{e} \bmod qR)$ and $(\mathbf{A}, \mathbf{u})$, where $\mathbf{A} \leftarrow U((R_q)^{m\times d})$, $\mathbf{s} \leftarrow U((R_q)^d)$, $\mathbf{e} \leftarrow (D_{R,\alpha})^m$ and $\mathbf{u} \leftarrow U((R_q)^m)$. By the same way, we can also get the reduction from MLWE to primal-MLWE.

We also consider the hardness of solving primal-DRLWE and primal-DMLWE for any $m = \text{poly}(n \log q)$, which are denoted by prime-DRLWE$(K, q, D_{R,\alpha})$ and prime-DMLWE$(K, d, q, D_{R,\alpha})$ separately. The matrix version of prime-DRLWE asks to distinguish between the distribution $(\mathbf{a}, \mathbf{a}\cdot\mathbf{s} + \mathbf{E} \bmod qR)$ and $(\mathbf{a}, \mathbf{U})$, where $\mathbf{a} \leftarrow U((R_q)^{m\times 1})$, $\mathbf{s} \leftarrow U((R_q)^{1\times d})$, $\mathbf{E} \leftarrow (D_{R,\alpha})^{m\times d}$ and $\mathbf{U} \leftarrow U(R_q)^{m\times d})$. The hardness of the matrix version for any $d = \text{poly}(n)$ can be established from prime-DRLWE$(K, q, m, D_{R,\alpha})$ via a routine hybrid argument. Likewise, the matrix version of prime-DMLWE asks to distinguish between the distribution $(\mathbf{A}, \mathbf{A}\cdot\mathbf{S}+\mathbf{E} \bmod qR)$ from $(\mathbf{A}, \mathbf{U})$, where $\mathbf{A} \leftarrow U((R_q)^{m\times k})$, $\mathbf{S} \leftarrow U((R_q)^{k\times d})$, $\mathbf{E} \leftarrow (D_{R,\alpha})^{m\times d}$ and $\mathbf{U} \leftarrow U((R_q)^{m\times d})$. The hardness of matrix version for any $d = \text{poly}(n)$ can also be established from DMLWE$(K, k, q, m, D_{R,\alpha})$ via a routine hybrid argument. For technical reasons, we use primal-DMLWE form in the proof in Section 4.

3 Probability Lemmas

In this section we give two results in probability theoretic. First, in Section 3.1 we give a generalized leftover hash lemma over $R_q^\vee$. Then, in Section 3.2 we give a decomposition theorem for Continuous Gaussian on $K_\mathbb{R}$.

3.1 Leftover Hash Lemma

Here we show a generalized leftover hash lemma over $R_q^\vee$. We are interested in the case of $K = \mathbb{Q}(\alpha)$ being the number field, where α is an algebraic integer, $f(x)$ is the minimum polynomial of α over $\mathbb{Q}$ and $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$.[1] In this case, we will prove that, $\mathbf{Cs}$ is statistically close to uniform distribution, as long as $\mathbf{s}$ has high min-entropy, where $\mathbf{C} \leftarrow U(R_q^{k\times d})$ and $\mathbf{s}$ is a

[1] Notice that if α is an algebraic integer, then we have $f(x) \in \mathbb{Z}[x]$. This proof can be found in [AW04].

random variable over $(R_q^\vee)^d$. We will first prove in this case R_q is a field, then show generalized leftover hash lemma over R_q. And finally, we get our generalized leftover hash lemma over $R_q^\vee$.

Now let us recall definition of universal hash function and some lemmas.

Definition 7 (Universal Hash Function Family). *A set $\mathcal{H}$ of functions $\mathcal{D} \mapsto \mathcal{R}$ is a universal hash function family, if for every distinct $x_1, x_2 \in \mathcal{D}$, the hash function family $\mathcal{H}$ satisfies the following constraint:*

$$\Pr[h(x_1) = h(x_2) : h \leftarrow \mathcal{H}] = \frac{1}{|\mathcal{R}|}.$$

Lemma 5 (Adapted from Lemma 2.4 in [DOR+08]). *Assume a set $\mathcal{H}$ of function $\mathcal{D} \mapsto \mathcal{R}$ is a universal hash function family. Then for any random variables X over $\mathcal{D}$ and Y, it holds that*

$$\Delta((h, h(X), Y); (h, u, Y)) \leq \frac{1}{2}\sqrt{|\mathcal{R}| \cdot 2^{-\widetilde{H}_\infty(X|Y)}},$$

where $h \leftarrow \mathcal{H}$, $u \leftarrow U(\mathcal{R})$.

Lemma 6 (Adapted from Lemma 2.14 in [LPR10]). *Let K be a number field of degree n, R be the ring of integers of K. Let I and J be ideals in R. Then there exists $t \in I$ such that the ideal $t \cdot I^{-1} \subset R$ is coprime to J. And let $\mathcal{M}$ be any fractional ideal in K. Then the function $\theta_t : K \mapsto K$ defined as $\theta_t(x) = t \cdot x$ induces an isomorphism from $\mathcal{M}/J\mathcal{M}$ to $I\mathcal{M}/IJ\mathcal{M}$.*

Lemma 7. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K. If $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, where q is a prime, then we have R_q is a finite field.*

Proof. Since $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, $\mathbb{Z}_q[x]/(f(x))$ is a finite field. It is easy to see that $\mathbb{Z}_q[x]/(f(x)) \cong \mathbb{Z}[x]/(q, f(x))$, hence $(q, f(x))$ is a maximal ideal of $\mathbb{Z}[x]$. Thus we only need to show that $R/qR \cong \mathbb{Z}[x]/(q, f(x))$. Let us consider the ring homomorphism $\Phi : \mathbb{Z}[x] \mapsto R/qR$, defined by

$$g(x) \mapsto g(\alpha) \bmod qR.$$

Clearly, $g(\alpha) \bmod qR \in R_q$, and $\ker(\Phi)$ contains ideal $(q, f(x))$. Since $\ker(\Phi)$ is also an ideal of $\mathbb{Z}[x]$, we have $\ker(\Phi) = (q, f(x))$. And by isomorphism theorem for rings we have $\mathbb{Z}[x]/(q, f(x)) \cong \mathrm{Im}(\Phi) \subset R/qR$. Since $|\mathbb{Z}_q[x]/(f(x))| = q^n$ and $|R/qR| = q^n$, we have $|\mathrm{Im}(\Phi)| = |\mathbb{Z}[x]/(q, f(x))| = |R/qR|$. Thus, we have $\mathrm{Im}(\Phi) = R/qR$. Consequently, we can get $R/qR \cong \mathbb{Z}[x]/(q, f(x))$. □

Remark 1. The requirement that α is an algebraic integer is trivial. Since for any algebraic number field K, we can find an algebraic integer θ such that $K = \mathbb{Q}(\theta)$. This proof can also be found in [AW04]. Besides, the requirement in Lemma 7 is also a necessary condition for R_q to be a field. The proof is similar, we also consider ring homomorphism $\Phi : \mathbb{Z}[x] \mapsto R/qR$, and then use isomorphism theorem.

We now prove the following variant of the leftover hash lemma over R_q.

Theorem 1. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K. Let q be a prime such that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, d, k be positive integers with $d > k$. Let $\mathbf{s}$ be a random variable defined on $(R_q)^d$ and let $\mathbf{C} \leftarrow U((R_q)^{k\times d})$ be chosen uniformly random. Furthermore let Y be a random variable possibly correlated with $\mathbf{s}$. Then it holds that*

$$\Delta((\mathbf{C}, \mathbf{Cs}, Y); (\mathbf{C}, \mathbf{u}, Y)) \leq \frac{1}{2}\sqrt{q^{nk} \cdot 2^{-\widetilde{H}_\infty(\mathbf{s}|Y)}},$$

where $\mathbf{u} \leftarrow U(R_q)^k$.

Proof. Let $\{h_{\mathbf{C}} : (R_q)^d \mapsto (R_q)^k\}$ be a family of hash functions given by $h_{\mathbf{C}}(\mathbf{s}) = \mathbf{Cs}$. In order to show that the statistical distance between $(\mathbf{C}, \mathbf{Cs}, Y)$ and $(\mathbf{C}, \mathbf{u}, Y)$, we only need to show $\{h_{\mathbf{C}}\}$ is a universal hash function family, and then apply Lemma 5.

Since $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, by Lemma 7, we have R_q is a field. Thus, for every distinct $\mathbf{s}^1, \mathbf{s}^2 \in (R_q)^d$, without loss of generality, we assume their first components are not equal, i.e. $s_1^1 \neq s_1^2$. In this case, we have $s_1^1 - s_1^2$ is an invertible element. Therefore, we have that $\mathbf{Cs}^1 = \mathbf{Cs}^2$ holds if and only if $\mathbf{C}$ satisfies that $c_{i1} = (s_1^1 - s_1^2)^{-1} \cdot [\sum_{j=2}^{d}(s_j^1 - s_j^2)c_{ij}]$. Therefore, we can easily get that

$$\Pr[\mathbf{Cs}^1 = \mathbf{Cs}^2 : \mathbf{C} \leftarrow U((R_q)^{k\times d})] = \frac{1}{q^{nk}} = \frac{1}{|(R_q)^k|}.$$

Consequently, we have $\{h_{\mathbf{C}}\}$ is a universal hash function family, and according to Lemma 5, we have

$$\Delta((\mathbf{C}, \mathbf{Cs}, Y); (\mathbf{C}, \mathbf{u}, Y)) \leq \frac{1}{2}\sqrt{q^{nk} \cdot 2^{-\widetilde{H}_\infty(\mathbf{s}|Y)}}.$$

□

Remark 2. It seems necessary that we restrict f to be an irreducible element in $\mathbb{Z}_q[x]$, and in this case R_q is a field. If R_q is not a field, since we do not have any requirements for the distribution of $\mathbf{s}$, we can consider an extreme case, $\mathbf{s}$ is an uniform distribution on an ideal I of R_q. In this case $\mathbf{Cs}$ will be some distribution on I^k, and the statistical distance will not be negligible.

We now prove our generalized leftover hash lemma over $R_q^\vee$ as follows.

Theorem 2. *Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K, $R^\vee$ be the dual of R. Let q be a prime such that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, d, k be positive integers with $d > k$. Let $\mathbf{s}$ be a random variable defined on $(R_q^\vee)^d$ and let $\mathbf{C} \leftarrow U((R_q)^{k\times d})$ be chosen uniformly*

random. Furthermore let Y be a random variable possibly correlated with $\mathbf{s}$. Then it holds that

$$\Delta((\mathbf{C}, \mathbf{Cs}, Y); (\mathbf{C}, \mathbf{u}, Y)) \leq \frac{1}{2}\sqrt{q^{nk} \cdot 2^{-\widetilde{H}_\infty(\mathbf{s}|Y)}},$$

where $\mathbf{u} \leftarrow U(R_q^\vee)^k$.

Proof. Let $I = (R^\vee)^{-1}$ and $J = qR$ be ideals in R, then by Lemma 6, there exists $t \in (R^\vee)^{-1}$ such that $tR^\vee$ is coprime to qR. Let $\mathcal{M} = R^\vee$ be a fractional ideal, then by Lemma 6, multiplication by t induces a R-module isomorphism from $R_q^\vee$ to R_q.

Likewise, let $\{\tilde{h}_{\mathbf{C}} : (R_q^\vee)^d \mapsto (R_q^\vee)^k\}$ be a family of hash functions given by $\tilde{h}_{\mathbf{C}}(\mathbf{s}) = \mathbf{Cs}$. For every distinct $\mathbf{s}^1, \mathbf{s}^2 \in (R_q^\vee)^d$, we have that $\mathbf{Cs}^1 = \mathbf{Cs}^2$ holds if and only if $\mathbf{C}t\mathbf{s}^1 = \mathbf{C}t\mathbf{s}^2$, where $t\mathbf{s}^1, t\mathbf{s}^2 \in (R_q)^d$. Therefore, by the proof in Theorem 1, we have $\{\tilde{h}_{\mathbf{C}}\}$ is also a universal hash function family. And by Lemma 5, the statement follows. □

3.2 Gaussian Decomposition

In this section, we show a new decomposition theorem for continuous Gaussian distribution on $K_{\mathbb{R}}$. We show that there exists an efficient sampling algorithm $D(\mathbf{F}, r, r_1)$, such that the random variable $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$ is distribution according to $(D_r(K_{\mathbb{R}}))^m$, where $\mathbf{e}_1 \leftarrow (D_{r_1}(K_{\mathbb{R}}))^d$, $\mathbf{e}_2 \leftarrow D(\mathbf{F}, r, r_1)$ and $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$. We first recall the definitions and lemmas of matrix norm and subgaussian distributions. Then, we prove an upper bound of spectral norm of a discrete Gaussian matrix. And finally, we prove our generalized decomposition theorem for continuous Gaussian distribution.

Definition 8. *For a matrix $\mathbf{X}$ over $\mathbb{R}^{m\times n}$, the largest singular value of matrix is defined by*

$$s_1(\mathbf{X}) = \sup_{\mathbf{u}\neq 0} \frac{\|\mathbf{Xu}\|_2}{\|\mathbf{u}\|_2}.$$

Subgaussian distributions are those on $\mathbb{R}$ which have tail dominated by Gaussians [Ver10]. An equivalent formulation is through the moment-generating function of the distribution, and this definition is commonly used throughout lattice-based cryptography [MP12].

Definition 9. *A real random variable X is subgaussian with parameter $s \geq 0$ if for all $t \in \mathbb{R}$,*

$$E(e^{2\pi tX}) \leq e^{\pi s^2 t^2}.$$

More generally, we say that a random vector $\mathbf{x}$ is subgaussian with parameter $s \geq 0$ if for all unit vectors $\mathbf{u} \in \mathbb{R}$, the random variable $\langle \mathbf{x}, \mathbf{u}\rangle$ is subgaussian with parameter s.

The subgaussian distribution admits the following properties.

Lemma 8 (Theorem 4.4.5 in [Ver18]). *Let $\mathbf{X} \in \mathbb{R}^{m\times d}$ be a random matrix with entries drawn independently from a subgaussian distribution with parameter $s \leq 0$. Then, there exists some universal constant $C \geq 0$ such that for any $t \geq 0$, with probability at least $1 - 2e^{-t^2}$ we have*

$$s_1(\mathbf{X}) \leq C \cdot s \cdot (\sqrt{m} + \sqrt{d} + t).$$

Lemma 9 (Adapted Lemma 2.8 in [MP12]). *Let $\Lambda \subset \mathbb{R}^{\mathrm{n}}$ be a lattice, then for any $s > 0$, $D_{\Lambda,s}$ is subgaussian with parameter s.*

Assume a number field K of degree n with ring of integers R has exactly s_1 real embeddings and s_2 pairs complex embeddings. Then for any matrix $\mathbf{F} = (f_{ij}) \in R^{m\times d}$, for any $j \in [s_1]$, we set[2]

$$\mathbf{F}^j = \begin{pmatrix} \sigma_j(f_{11}) & \cdots & \sigma_j(f_{1d}) \\ \vdots & & \vdots \\ \sigma_j(f_{m1}) & \cdots & \sigma_j(f_{md}) \end{pmatrix},$$

and for $j \in \{s_1 + 1, \cdots, s_1 + s_2\}$, we set

$$\mathbf{F}^j = \begin{pmatrix} \sqrt{2}\mathrm{Re}(\sigma_j(f_{11})) & \cdots & \sqrt{2}\mathrm{Re}(\sigma_j(f_{1d})) \\ \vdots & & \vdots \\ \sqrt{2}\mathrm{Re}(\sigma_j(f_{m1})) & \cdots & \sqrt{2}\mathrm{Re}(\sigma_j(f_{md})) \end{pmatrix},$$

$$\mathbf{F}^{j+s_2} = \begin{pmatrix} \sqrt{2}\mathrm{Im}(\sigma_j(f_{11})) & \cdots & \sqrt{2}\mathrm{Im}(\sigma_j(f_{1d})) \\ \vdots & & \vdots \\ \sqrt{2}\mathrm{Im}(\sigma_j(f_{m1})) & \cdots & \sqrt{2}\mathrm{Im}(\sigma_j(f_{md})) \end{pmatrix}.$$

We will be interested in $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, and we will give an upper bound of spectral norm of $\mathbf{F}^j$ in the following.

Lemma 10. *Let K be a number field of degree n which has exactly s_1 real embeddings and s_2 pairs complex embeddings. Let R be the ring of integers of K. Let $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, assume for convenience that $m \geq d$. Then with all but 2^{-m} probability it holds that $s_1(\mathbf{F}^j) \leq C \cdot \gamma \cdot \sqrt{m}$ for all $j \in [n]$, where C is a global constant.*

Proof. In order to show $s_1(\mathbf{F}^j) \leq C \cdot \gamma \cdot \sqrt{m}$, we only need to show that $\mathbf{F}^j$ is a random matrix with entries drawn independently from a subgaussian distribution, and then apply Lemma 8.

We first recall that $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$ means that samples each component f_{kl} according to $D_{R,\gamma}$ independently, and $f_{kl} \leftarrow D_{R,\gamma}$ means that $\sigma_H(f_{kl}) \leftarrow D_{\sigma_H(R),\gamma}$,

[2] Here d could be 1, and in this case $\mathbf{F}$ would be a vector.

where

$$\sigma_H(f_{kl}) = \begin{pmatrix} \sigma_1(f_{kl}) \\ \vdots \\ \sigma_{s_1}(f_{kl}) \\ \sqrt{2}\mathrm{Re}(\sigma_{s_1+1}(f_{kl})) \\ \vdots \\ \sqrt{2}\mathrm{Re}(\sigma_{s_1+s_2}(f_{kl})) \\ \sqrt{2}\mathrm{Im}(\sigma_{s_1+1}(f_{kl})) \\ \vdots \\ \sqrt{2}\mathrm{Im}(\sigma_{s_1+s_2}(f_{kl})) \end{pmatrix}.$$

Clearly, we have that for any $j \in [n]$, the entries of $\mathbf{F}^j$ are sampled from the same distribution independently.

Since $\sigma_H(R)$ is a lattice in $\mathbb{R}^n$, then by Lemma 9, $\sigma_H(f_{kl})$ is subgaussian with parameter γ. So by definition, we have $\langle \sigma_H(f_{kl}), \mathbf{e}_j \rangle$ is also subgaussian with parameter γ.

Thus for any $j \in [n]$, we have $\mathbf{F}^j$ is a random matrix with entries drawn independently from a subgaussian distribution with parameter γ. Therefore, by Lemma 8 and set $t = \sqrt{m}$, we have $s_1(\mathbf{F}^j) \leq 3C\gamma \cdot \sqrt{m}$ with probability at least $1 - 2e^{-m}$. Finally, we take a union bound over all j. This give us

$$\Pr[\exists j \in [n] : s_1(\mathbf{F}^j) \geq 3C\gamma \cdot \sqrt{m})] \leq n \cdot 2e^{-m} \leq 2^{-m}.$$

Set $C = 3C$ and the proof is established. □

We now show and prove a generalized decomposition theorem for continuous Gaussian distribution over $K_{\mathbb{R}}$. To avoid confusion, in the following proof, we use $D_r(K_{\mathbb{R}})$ to denote the Gaussian distribution over $K_{\mathbb{R}}$, and for $j \in \{s_1 + 1, \cdots, s_1 + s_2\}$, we set

$$\widetilde{\mathbf{F}}^j = \frac{\sqrt{2}}{2} \begin{pmatrix} \mathbf{F}^j & -\mathbf{F}^{j+s_2} \\ \mathbf{F}^{j+s_2} & \mathbf{F}^j \end{pmatrix}.$$

Theorem 3. *Let K be a number field of degree n which has exactly s_1 real embeddings and s_2 pairs complex embeddings. Let R be the ring of integers of K. Let $\mathbf{F} \in R^{m \times d}$ be a matrix with $s_1(\mathbf{F}^j) \leq \eta$ for any $j \in [n]$. Let $r, r_1 > 0$ be positive real numbers where $r > \sqrt{2}\eta \cdot r_1$. Let $\mathbf{e}_1 \leftarrow (D_{r_1}(K_{\mathbb{R}}))^d$ and $\mathbf{e}_2$ be the random variable in $(K_{\mathbb{R}})^m$ obtained in the following way: for $j \in [s_1]$, set $\mathbf{e}_2^j \leftarrow D_{\sqrt{\mathbf{\Sigma}_j}}$ where $\mathbf{\Sigma}_j = r^2\mathbf{I}_m - r_1^2\mathbf{F}^j(\mathbf{F}^j)^{\mathrm{T}}$; for $j \in \{s_1 + 1, s_1 + s_2\}$, set $((\mathbf{e}_2^j)^{\mathrm{T}}, (\mathbf{e}_2^{j+s_2})^{\mathrm{T}})^{\mathrm{T}} \leftarrow D_{\sqrt{\mathbf{\Sigma}_j}}$ where $\mathbf{\Sigma}_j = r^2\mathbf{I}_{2m} - r_1^2\widetilde{\mathbf{F}}^j(\widetilde{\mathbf{F}}^j)^{\mathrm{T}}$. Then the random variable $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$ is distribution according to $(D_r(K_{\mathbb{R}}))^m$.*

Proof. We first prove that $\mathbf{\Sigma}_j$ is positive definite for any $j \in [s_1 + s_2]$. For any $j \in [s_1]$ and any $\mathbf{x} \in \mathbb{R}^m/\{0\}$, we have

$$\mathbf{x}^{\mathrm{T}}\mathbf{\Sigma}_j\mathbf{x} \geq r^2\|\mathbf{x}\|_2^2 - r_1^2 \cdot s_1(\mathbf{F}^j)^2\|\mathbf{x}\|_2^2 \geq (r^2 - r_1^2\eta^2) \cdot \|\mathbf{x}\|_2^2 > 0,$$

as $r \geq \sqrt{2}\eta \cdot r_1$ and $s_1(\mathbf{F}^j) = s_1((\mathbf{F}^j)^{\mathrm{T}})$.

For any $j \in \{s_1+1, \cdots, s_1+s_2\}$ and any $\mathbf{x} = (\mathbf{y}^{\mathrm{T}}, \mathbf{z}^{\mathrm{T}})^{\mathrm{T}} \in \mathbb{R}^{2m}/\{0\}$, we have

$$\begin{aligned}\|(\widetilde{\mathbf{F}}^j)^{\mathrm{T}}\mathbf{x}\|_2^2 &= \frac{1}{2}[\|(\mathbf{F}^j)^{\mathrm{T}}\mathbf{y} + (\mathbf{F}^{j+s_2})^{\mathrm{T}}\mathbf{z}\|_2^2 + \|(\mathbf{F}^j)^{\mathrm{T}}\mathbf{z} - (\mathbf{F}^{j+s_2})^{\mathrm{T}}\mathbf{y}\|_2^2] \\ &\leq \frac{1}{2}[(\|(\mathbf{F}^j)^{\mathrm{T}}\mathbf{y}\|_2 + \|(\mathbf{F}^{j+s_2})^{\mathrm{T}}\mathbf{z}\|_2)^2 + (\|(\mathbf{F}^j)^{\mathrm{T}}\mathbf{z}\|_2 + \|(\mathbf{F}^{j+s_2})^{\mathrm{T}}\mathbf{y}\|_2)^2] \\ &\leq \eta^2(\|\mathbf{y}\|_2 + \|\mathbf{z}\|_2)^2 \leq 2\eta^2(\|\mathbf{y}\|_2^2 + \|\mathbf{z}\|_2^2) = 2\eta^2\|\mathbf{x}\|_2^2.\end{aligned}$$

So for any $j \in \{s_1+1, \cdots, s_1+s_2\}$ and any $\mathbf{x} = (\mathbf{y}^{\mathrm{T}}, \mathbf{z}^{\mathrm{T}})^{\mathrm{T}} \in \mathbb{R}^{2m}/\{0\}$, we also have

$$\mathbf{x}^{\mathrm{T}}\boldsymbol{\Sigma}_j\mathbf{x} \geq r^2\|\mathbf{x}\|_2^2 - r_1^2 \cdot 2\eta^2\|\mathbf{x}\|_2^2 > 0.$$

Since we have $(K_{\mathbb{R}})^m \cong \mathbb{R}^{mn}$, $\sigma_H(\mathbf{e}_1), \sigma_H(\mathbf{e}_2)$ are independent Gaussian vectors, and therefore $\sigma_H(\mathbf{e})$ is also a Gaussian vector. Since $\sigma_H(\mathbf{e}_1), \sigma_H(\mathbf{e}_2)$ have expectation 0, then so does $\sigma_H(\mathbf{e})$.

Now let us calculate the covariance matrix for $\sigma_H(\mathbf{e})$. We use $\sigma_{H_j}(e_i)$, $\sigma_{H_j}(e_{1i})$ and $\sigma_{H_j}(e_{2i})$ to denote the j-th component of $\sigma_H(e_i)$, $\sigma_H(e_{1i})$ and $\sigma_H(e_{2i})$ separately, where e_i, e_{1i} and e_{2i} is the i-th coordinate of $\mathbf{e}$, $\mathbf{e}_1$ and $\mathbf{e}_2$ separately, and we use f_{kl}^j to denote the entry that appears in the k-th row and l-th column of matrix $\mathbf{F}^j$. Since $e_i = \sum_{k=1}^d f_{ik}e_{1k} + e_{2i}$, for any $j \in [s_1]$ we have

$$\sigma_{H_j}(e_i) = \sum_{k=1}^d f_{ik}^j \sigma_{H_j}(e_{1k}) + \sigma_{H_j}(e_{2i}).$$

For any $j \in \{s_1+1, \cdots, s_1+s_2\}$ we have

$$\begin{aligned}\sigma_{H_j}(e_i) &= \sqrt{2}\mathrm{Re}[\sum_{k=1}^d \sigma_j(f_{ik})\sigma_j(e_{1k}) + \sigma_j(e_{2i})] \\ &= \frac{1}{\sqrt{2}}\sum_{k=1}^d [f_{ik}^j \sigma_{H_j}(e_{1k}) - f_{ik}^{j+s_2}\sigma_{H_{j+s_2}}(e_{1k})] + \sigma_{H_j}(e_{2i}), \\ \sigma_{H_{j+s_2}}(e_i) &= \sqrt{2}\mathrm{Im}[\sum_{k=1}^d \sigma_j(f_{ik})\sigma_j(e_{1k}) + \sigma_j(e_{2i})] \\ &= \frac{1}{\sqrt{2}}\sum_{k=1}^d [f_{ik}^j \sigma_{H_{j+s_2}}(e_{1k}) + f_{ik}^{j+s_2}\sigma_{H_j}(e_{1k})] + \sigma_{H_{j+s_2}}(e_{2i}).\end{aligned}$$

Therefore, according to the sampling method of $\mathbf{e}_1$ and $\mathbf{e}_2$, we have for any $j \in [s_1]$, $j' \in [n]$ which satisfies $j' \neq j$, and any $i, i' \in [m]$, we have $\sigma_{H_j}(e_i)$ and $\sigma_{H_{j'}}(e_{i'})$ are independent. For any $j \in \{s_1+1, \cdots, s_1+s_2\}$, any $j' \in [n]$ which satisfies $j' \neq j, j' \neq j+s_2$, and any $i, i' \in [m]$, we have $\sigma_{H_j}(e_i)$ and $\sigma_{H_{j'}}(e_{i'})$ are independent. For any $j \in \{s_1+s_2+1, \cdots, n\}$, any $j' \in [n]$ which satisfies $j' \neq j, j' \neq j-s_2$, and any $i, i' \in [m]$, we have $\sigma_{H_j}(e_i)$ and $\sigma_{H_{j'}}(e_{i'})$ are independent.

And by a direct calculation, for any $j \in [s_1]$, we have $\mathbf{e}^j = \mathbf{F}^j\mathbf{e}_1^j + \mathbf{e}_2^j$; for any $j \in \{s_1+1, \cdots, s_1+s_2\}$, we have

$$\begin{pmatrix} \mathbf{e}^j \\ \mathbf{e}^{j+s_2} \end{pmatrix} = \frac{\sqrt{2}}{2} \begin{pmatrix} \mathbf{F}^j & -\mathbf{F}^{j+s_2} \\ \mathbf{F}^{j+s_2} & \mathbf{F}^j \end{pmatrix} \begin{pmatrix} \mathbf{e}_1^j \\ \mathbf{e}_1^{j+s_2} \end{pmatrix} + \begin{pmatrix} \mathbf{e}_2^j \\ \mathbf{e}_2^{j+s_2} \end{pmatrix}.$$

Therefore, for any $j \in [s_1]$, the covariance matrix of $\mathbf{e}^j$ is:

$$E(\mathbf{e}^j(\mathbf{e}^j)^{\mathrm{T}}) = E(\mathbf{F}^j\mathbf{e}_1^j(\mathbf{e}_1^j)^{\mathrm{T}}(\mathbf{F}^j)^{\mathrm{T}}) + E(\mathbf{e}_2^j(\mathbf{e}_2^j)^{\mathrm{T}}) = r_1^2\mathbf{F}^j(\mathbf{F}^j)^{\mathrm{T}} + \mathbf{\Sigma}_j = r^2\mathbf{I}_m.$$

Likewise, for any $j \in \{s_1+1, \cdots, s_1+s_2\}$, the covariance matrix of $\begin{pmatrix} \mathbf{e}^j \\ \mathbf{e}^{j+s_2} \end{pmatrix}$ is:

$$E\left[\begin{pmatrix} \mathbf{e}^j \\ \mathbf{e}^{j+s_2} \end{pmatrix} \cdot ((\mathbf{e}^j)^{\mathrm{T}}, (\mathbf{e}^{j+s_2})^{\mathrm{T}})\right] = r_1^2\widetilde{\mathbf{F}}^j(\widetilde{\mathbf{F}}^j)^{\mathrm{T}} + \mathbf{\Sigma}_j = r^2\mathbf{I}_{2m}.$$

Consequently, $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$ is the distribution according to $(D_r(K_{\mathbb{R}}))^m$. □

By combining Theorem 3 and Lemma 10, we can easily obtain the following corollary.

Corollary 1. *Let C be a global constant, K be a number field, R be a ring of integers of K. Let $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, assume for convenience that $m > d$. Let $r, r_1 > 0$ be positive real numbers which satisfies that $r > \sqrt{2}C \cdot r_1 \cdot \gamma \cdot \sqrt{m}$. Let $\mathbf{e}_1 \leftarrow (D_{r_1}(K_{\mathbb{R}}))^d$ be the random variable in $(K_{\mathbb{R}})^d$. If for any $j \in [n]$, we have $s_1(\mathbf{F}^j) \le C\gamma\sqrt{m}$, then there exists an efficient sampling algorithm $D(\mathbf{F}, r, r_1)$, such that the random variable $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$ is distribution according to $(D_r(K_{\mathbb{R}}))^m$, where $\mathbf{e}_2 \leftarrow D(\mathbf{F}, r, r_1)$.*

4 Entropic Module Learning With Error

In this section we give the definition of Entropic Module Learning With Error problem (E-MLWE) first, we consider dual forms because this form is the most widely used in practice. Then to prove the hardness of E-MLWE, we show a reduction from primal-DMLWE problem to E-MLWE problem and a reduction from primal-DMLWE problem to E-DMLWE problem. Finally, we compute the noise lossiness for general high min-entropy distributions over $K_{\mathbb{R}}$. Our proof follows the proof structure of Brakerski et al. [BD20].

4.1 Definition of the Entropic M-LWE

Definition 10 (Entropic M-LWE). *Let K be some number field with degree $n = \mathrm{poly}(\lambda)$, R be the ring of integers of K and $R^\vee$ be the dual of R. Let $q = q(\lambda)$ be a modulus, $d = d(\lambda)$ be a dimension and $m = \mathrm{poly}(\lambda)$ be a sample size. Let χ be an error distribution on $K_{\mathbb{R}}$ and $\mathcal{S} = \mathcal{S}(\lambda, K, d, q, m)$ be a secrets distributions on $(R_q^\vee)^d$. Let $\mathrm{MLWE}_{K,d,q,m,\chi}(\mathcal{S})$ be the distribution over $(R_q)^{m\times d} \times (\mathbb{T}_{R^\vee})^m$*

obtained by choosing $\mathbf{A} \leftarrow U((R_q)^{m\times d})$, $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{e} \leftarrow \chi^m$, *and outputting the pair* $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$.

We say that the search problem E-MLWE$(K, d, q, m, \mathcal{S}, \chi)$ *is hard, if it holds for every* PPT *adversary* $\mathcal{A}$ *that*

$$\Pr[\mathcal{A}(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee) = \mathbf{s}] \leq \mathrm{negl}(\lambda),$$

where $\mathbf{A} \leftarrow U((R_q)^{m\times d})$, $\mathbf{s} \leftarrow \mathcal{S}$ *and* $\mathbf{e} \leftarrow \chi^m$.

Likewise, we say that the decisional problem E-DMLWE$(K, d, q, m, \mathcal{S}, \chi)$ *is hard, if it holds for every* PPT *distinguisher* $\mathcal{D}$ *that*

$$|\Pr[\mathcal{D}(\mathbf{A}_1, \mathbf{b}_1) = 1] - \Pr[\mathcal{D}(\mathbf{A}_2, \mathbf{b}_2) = 1]| \leq \mathrm{negl}(\lambda),$$

where $(\mathbf{A}_1, \mathbf{b}_1) \leftarrow \mathrm{MLWE}_{K,d,q,m,\chi}(\mathcal{S})$ *and* $(\mathbf{A}_2, \mathbf{b}_2) \leftarrow U((R_q)^{m\times d} \times (\mathbb{T}_{R^\vee})^m)$.

4.2 Hardness of E-MLWE

In this section we will establish the hardness of entropic search MLWE with continuous gaussian noise. Using discretization technique, see Lyubashevsky et al. [LPR13] for more details, we can easily get that entropic search MLWE with discrete gaussian noise is also hard.

Theorem 4. *Let* C *be the global constant from Corollary 1. Let* R *be the ring of integers of some algebraic number field* K *of degree* n *and* $R^\vee$ *be the dual of* R. *Let* q, d, m *be positive integers where* $m > d > 1$ *and* r, γ, $r_1 > 0$. *Let* $\mathbf{s}$ *be a random variable on* $(R_q^\vee)^d$ *distributed according to some distribution* $\mathcal{S}$, $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ *be an error term. Let* $r > \sqrt{2}C\sqrt{m}\gamma r_1$. *Further assume that*

$$\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee) \geq nk\log(q) + \omega(\log(\lambda)).$$

Then the search problem E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DMLWE$(K, k, q, D_{R,\gamma})$ *is hard.*

Proof. Let $\mathcal{A}$ be a search adversary against E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$. Throughout this proof, C is the global constant from Corollary 1, $D(\mathbf{F}, r, r_1)$ is the efficient sampling algorithm from Corollary 1. Consider the following hybrid MLWE distributions:

- $\mathcal{H}_0$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{A} \leftarrow U((R_q)^{m\times d})$ and $\mathbf{e} \leftarrow D_r(K_\mathbb{R})^m$, and then output $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$;
- $\mathcal{H}_1$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, set $\mathbf{A} = \mathbf{BC} + \mathbf{F} \bmod qR$, $\mathbf{e} \leftarrow D_r(K_\mathbb{R})^m$, and output $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$;
- $\mathcal{H}_2$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(\mathbf{F}^j) > C\gamma\sqrt{m}$ output $\perp$. Else, let $\mathbf{A} = \mathbf{BC} + \mathbf{F} \bmod qR$, $\mathbf{e} \leftarrow D_r(K_\mathbb{R})^m$, and output $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$;

– $\mathcal{H}_3$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(\mathbf{F}^j) > C\gamma\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e}_1 \leftarrow D_{r_1}(K_{\mathbb{R}})^d$, $\mathbf{e}_2 \leftarrow D(\mathbf{F}, r, r_1)$, and set $\mathbf{A} = \mathbf{BC} + \mathbf{F} \bmod qR$, $\mathbf{e} = \mathbf{Fe}_1 + \mathbf{e}_2$, and then output $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$.

First note that $\mathcal{H}_0$ is identical to the E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ experiment. Second, it follows directly by the hardness of primal-DMLWE$(K, k, q, D_{R,\gamma})$ that $\mathcal{H}_0$ and $\mathcal{H}_1$ are computationally indistinguishable. Then, if we have for any $j \in [n]$, $s_1(\mathbf{F}^j) \le C\gamma\sqrt{m}$, $\mathcal{H}_1$ and $\mathcal{H}_2$ are identically distributed. Thus we can bound the statistical distance between $\mathcal{H}_1$ and $\mathcal{H}_2$ by $\Pr[\exists j \in [n] : s_1(\mathbf{F}^j) \ge C\gamma\cdot\sqrt{m})]$. By Lemma 10, we have with all but 2^{-m} probability it holds that $s_1(\mathbf{F}^j) \le C\cdot\gamma\cdot\sqrt{m}$ for all $j \in [n]$. Therefore, the statistical distance between $\mathcal{H}_1$ and $\mathcal{H}_2$ is at most 2^{-m}. Finally, we claim that $\mathcal{H}_2$ and $\mathcal{H}_3$ are identically distributed by Corollary 1.

We now show that for any search adversary $\mathcal{A}$, we have

$$\Pr[\mathcal{A}(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee) = \mathbf{s}] < \mathrm{negl}(\lambda),$$

where $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee) \leftarrow \mathcal{H}_3$. Consequently, by the above we can then argue that the same holds for $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee) \leftarrow \mathcal{H}_0$, which means that the search problem E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ is hard, concluding the proof for the theorem. To do so, we will bound the conditional min-entropy of $\mathbf{s}$ given $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee) \leftarrow \mathcal{H}_3$. We can compute $\mathbf{y} = \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee$ given $\mathbf{B} \in (R_q)^{m\times k}$, $\mathbf{Cs} \bmod qR^\vee \in (R_q^\vee)^k$, $\mathbf{F} \in R^{m\times d}$, $\frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee$ and $\mathbf{e}_2 \in (K_{\mathbb{R}})^m$. Since we have

$$\frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee = \frac{1}{q}\mathbf{B}\cdot(\mathbf{Cs} \bmod qR^\vee) + \mathbf{F}\cdot(\frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee) + \mathbf{e}_2 \bmod R^\vee.$$

And since $R^\vee$ is a free $\mathbb{Z}$-module of rank n, $R_q^\vee$ is a free $\mathbb{Z}_q$-module of rank n. Consequently, $\mathbf{Cs} \bmod qR^\vee \in (R_q^\vee)^k$ has at most $2^{kn\log q}$ possible values. Then by Lemma 1, we can get the bound:

$$\begin{aligned}
&\widetilde{H}_\infty(\mathbf{s} \mid (\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)) \\
&\ge \widetilde{H}_\infty(\mathbf{s} \mid \mathbf{B}, \mathbf{C}, \mathbf{F}, \mathbf{Cs} \bmod qR^\vee, \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee, \mathbf{e}_2) \\
&= \widetilde{H}_\infty(\mathbf{s} \mid \mathbf{C}, \mathbf{Cs} \bmod qR^\vee, \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee) \\
&\ge \widetilde{H}_\infty(\mathbf{s} \mid \mathbf{C}, \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee) - nk\log q \\
&= \widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee) - nk\log q.
\end{aligned}$$

Where the first equality follows from the fact that $\mathbf{B}$, $\mathbf{F}$, $\mathbf{e}_2$ are independent of everything else, and the second equality follows from the fact that $\mathbf{C}$ is independent of everything else. The second inequality follows from Lemma 1. By

assumption we have

$$\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee) \geq nk\log(q) + \omega(\log(\lambda)),$$

it follows that

$$\begin{aligned}\Pr[\mathcal{A}(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee) = \mathbf{s}] &\leq 2^{-\widetilde{H}_\infty(\mathbf{s}|(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s})+\mathbf{e} \bmod R^\vee))} \\ &\leq 2^{-\widetilde{H}_\infty(\mathbf{s}|\frac{\mathbf{s}}{q}+\mathbf{e_1} \bmod R^\vee)+nk\log q} \\ &\leq 2^{-\omega(\log(\lambda))},\end{aligned}$$

which is negligible. This concludes the proof of the theorem. □

The hardness of primal-DMLWE assumption is only used to asserts that $\mathbf{BC} + \mathbf{F} \bmod qR$ is computationally indistinguishable from a uniform matrix. Thus we can also use the hardness of primal-DRLWE assumption to get the similar result. The proof of the following corollary is analogous, and we describe the proof in full version of this paper.

Corollary 2. *Let C be the global constant from Corollary 1. Let R be the ring of integers of some algebraic number field K of degree n and $R^\vee$ be the dual of R. Let q, d, m be positive integers where $m > d > 1$ and r, γ, $r_1 > 0$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution $\mathcal{S}$, $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ be an error term. Let $r > \sqrt{2}C\sqrt{m}\gamma r_1$. Further assume that*

$$\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee) \geq n\log(q) + \omega(\log(\lambda)).$$

Then the search problem E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DRLWE$(K, q, D_{R,\gamma})$ *is hard.*

4.3 Hardness of E-DMLWE

In this section we will establish the hardness of entropic decision MLWE with continuous gaussian noise. Using discretization technique, we can also easily get that entropic decision MLWE with discrete gaussian noise is also hard.

Theorem 5. *Let C be the global constant from Corollary 1. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K and $R^\vee$ be the dual of R. Let q be a prime such that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, d, m be positive integers where $m > d > 1$ and r, γ, $r_1 > 0$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution $\mathcal{S}$, $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ be an error term. Let $r > \sqrt{2}C\sqrt{m}\gamma r_1$. Further assume that*

$$\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee) \geq nk\log(q) + \omega(\log(\lambda)).$$

Then the decisional problem E-DMLWE$(K, d, q, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DMLWE$(K, k, q, D_{R,\gamma})$ *and* DMLWE(K, k, q, m, D_r) *are hard.*

Proof. Throughout this proof, C is the global constant from Corollary 1 and $D(\mathbf{F}, r, r_1)$ is the efficient sampling algorithm from Corollary 1. We assume $\mathcal{D}$ be a PPT distinguisher which distinguishes E-DMLWE$(K, d, q, m, \mathcal{S}, D_r)$ with non-negligible advantage. Consider the following hybrid MLWE distributions:

- $\mathcal{H}_0$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{A} \leftarrow U((R_q)^{m\times d})$ and $\mathbf{e} \leftarrow D_r(K_{\mathbb{R}})^m$, and then output $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$;
- $\mathcal{H}_3$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(\mathbf{F}^j) > C\gamma\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e}_1 \leftarrow D_{r_1}(K_{\mathbb{R}})^d$, $\mathbf{e}_2 \leftarrow D(\mathbf{F}, r, r_1)$, and set $\mathbf{A} = \mathbf{BC} + \mathbf{F} \bmod qR$, $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$, and then output $(\mathbf{A}, \frac{1}{q}(\mathbf{A}\cdot\mathbf{s}) + \mathbf{e} \bmod R^\vee)$.
- $\mathcal{H}_4$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{s}^* \leftarrow U((R_q^\vee)^d)$, $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(\mathbf{F}^j) > C\gamma\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e}_1 \leftarrow D_{r_1}(K_{\mathbb{R}})^d$, $\mathbf{e}_2 \leftarrow D(\mathbf{F}, r, r_1)$, and set $\mathbf{A} = \mathbf{BC} + \mathbf{F} \bmod qR$, and then output $(\mathbf{A}, \frac{1}{q}\mathbf{B}\mathbf{s}^* + \mathbf{F}(\frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee) + \mathbf{e}_2 \bmod R^\vee)$.
- $\mathcal{H}_5$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{s}^* \leftarrow U((R_q^\vee)^k)$, $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(\mathbf{F}^j) > C\gamma\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e} \leftarrow D_r(K_{\mathbb{R}})^m$, set $\mathbf{A} = \mathbf{BC} + \mathbf{F} \bmod qR$, and then output the pair $(\mathbf{A}, \frac{1}{q}(\mathbf{B}\mathbf{s}^* + \mathbf{F}\mathbf{s}) + \mathbf{e} \bmod R^\vee)$.

First, we have $\mathcal{H}_0$ and $\mathcal{H}_3$ are computationally indistinguishable by the proof in Theorem 5. Then, we will show that $\mathcal{H}_3$ and $\mathcal{H}_4$ are statistically close via the Theorem 2. Note that the only difference between $\mathcal{H}_3$ and $\mathcal{H}_4$ is that in $\mathcal{H}_4$ we have replaced $\mathbf{Cs}$ by a uniformly random $\mathbf{s}^*$. Moreover, the only other term depending on $\mathbf{s}$ is $\frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee$. Consequently, we can bound the statistical distance between $\mathcal{H}_3$ and $\mathcal{H}_4$ by

$$\begin{aligned}
\Delta(\mathcal{H}_3; \mathcal{H}_4) &\le \Delta((\mathbf{C}, \mathbf{Cs}, \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee); (\mathbf{C}, \mathbf{s}^*, \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee)) \\
&\le \frac{1}{2}\sqrt{q^{nk} \cdot 2^{-\widetilde{H}_\infty(\mathbf{s} | \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee)}} \\
&\le \frac{1}{2}\sqrt{2^{nk\cdot\log(q)} \cdot 2^{-(nk\cdot\log(q) + \omega(\log(\lambda)))}} \\
&= 2^{-\omega(\log(\lambda))},
\end{aligned}$$

which is negligible. The second inequality follows by the Theorem 2. Note that we can apply the leftover hash lemma whenever $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$.

Next, we claim that $\mathcal{H}_4$ and $\mathcal{H}_5$ are identically distributed. To see this, note that all we did was reversing the decomposition of $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$.

Thus, by the above argument, distinguisher $\mathcal{D}$ also have non-negligible advantage in distinguishing $(\mathbf{A}, \mathbf{y})$ from $(\mathbf{A}, \mathbf{u})$, where $(\mathbf{A}, \mathbf{y}) \leftarrow \mathcal{H}_5$, $\mathbf{u} \leftarrow (\mathbb{T}_{R^\vee})^m$. From such a distinguisher $\mathcal{D}$ we can construct a distinguisher $\mathcal{D}'$ which distinguishes DMLWE(K, k, q, m, D_r) with non-negligible advantage as follows. $\mathcal{D}'$ gets as input $\mathbf{B} \in (R_q)^{m\times k}$ and $\mathbf{z} \in (\mathbb{T}_{R^\vee})^m$, and proceeds as follows:

– Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{C} \leftarrow U((R_q)^{k\times d})$, $\mathbf{F} \leftarrow D_{R,\gamma}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(\mathbf{F}^j) > C\gamma\sqrt{m}$ output $\perp$. Otherwise, set $\mathbf{A} = \mathbf{BC}+\mathbf{F} \bmod qR$, $\mathbf{y} = \mathbf{z}+\frac{1}{q}\mathbf{Fs} \bmod R^\vee$, and then output $\mathcal{D}(\mathbf{A}, \mathbf{y})$.

We claim that $\mathcal{D}'$ has the same advantage as $\mathcal{D}$. First consider the case that the input of $\mathcal{D}'$ is a pair of the form $(\mathbf{B}, \mathbf{z} = \frac{1}{q}\mathbf{Bs}^* + \mathbf{e} \bmod R^\vee)$, where $\mathbf{B} \leftarrow U((R_q)^{m\times k})$, $\mathbf{s}^* \leftarrow U((R_q^\vee)^k)$ and $\mathbf{e} \leftarrow D_r(K_\mathbb{R})^m$. Then it holds that

$$\mathbf{y} = \mathbf{z} + \frac{1}{q}\mathbf{Fs} \bmod R^\vee = \frac{1}{q}(\mathbf{Bs}^* + \mathbf{Fs}) + \mathbf{e} \bmod R^\vee.$$

Thus, $(\mathbf{A}, \mathbf{y})$ is distributed according to $\mathcal{H}_5$.

On the other hand, if the input of $\mathcal{D}'$ is distributed according to $(\mathbf{B}, \mathbf{z})$, where $\mathbf{z} \leftarrow U((\mathbb{T}_{R^\vee})^m)$. Then it holds that $\mathbf{y} = \mathbf{z} + \frac{1}{q}\mathbf{Fs} \bmod R^\vee$ is also a uniformly random variable.

Therefore, $\mathcal{D}'$ has the same advantage as $\mathcal{D}$, which contradicts the hardness of DMLWE(K, k, q, m, D_r). This concludes the proof. □

By the same way, we can also get a reduction from primal-DRLWE problem to E-DMLWE problem.

Corollary 3. *Let C be the global constant from Corollary 1. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K and $R^\vee$ be the dual of R. Let q be a prime such that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, d, m be positive integers where $m > d > 1$ and r, γ, $r_1 > 0$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution $\mathcal{S}$, $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ be an error term. Let $r > \sqrt{2}C\sqrt{m}\gamma r_1$. Further assume that*

$$\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee) \geq n\log(q) + \omega(\log(\lambda)).$$

Then the decisional problem E-DMLWE$(K, d, q, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DRLWE$(K, q, D_{R,\gamma})$ *and* DRLWE(K, q, m, D_r) *are hard.*

4.4 Noise-Lossiness for Gaussian

In this section, we will compute the gaussian noise lossiness for general high-entropy distributions over $K_\mathbb{R}$.

Lemma 11. *Let R be the ring of integers of a field K with degree n, $R^\vee$ be the dual of R and $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$. Let d, q be integers and r_1 be a parameter for gaussian with $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$, then it holds for all $\mathbf{x} \in (K_\mathbb{R})^d$ that $\rho_{r_1}(\mathbf{x} + (R^\vee)^d) \leq 2$.*

Proof. Since $\mathbf{B}_R$ is a basis of R in $\mathbb{H}$, we have $\mathbf{B}_{R^d} = \mathbf{I}_d \otimes \mathbf{B}_R$ is a basis of R^d in $\mathbb{H}^d$. Orthogonalizing from left to right, we can see that $\|\widetilde{\mathbf{B}}_{R^d}\|$ is precisely $\|\widetilde{\mathbf{B}}_R\|$.

By Lemma 3, and set $\epsilon = 1$, we have $\frac{1}{r_1} \geq \eta_1(R^d)$. By definition, we obtain $\rho_{r_1}((R^\vee)^d \setminus \{0\}) \leq 1$. Thus, we have $\rho_{r_1}((R^\vee)^d) \leq 2$. And by Lemma 4, we get

$$\rho_{r_1}(\mathbf{x} + (R^\vee)^d) = \rho_{r_1,\mathbf{x}}((R^\vee)^d) \leq \rho_{r_1}((R^\vee)^d) \leq 2.$$

□

Theorem 6. *Let R be the ring of integers of a field K with degree n, $R^\vee$ be the dual of R and $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$. Let d, q be integers and r_1 be a parameter for gaussian with $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ and $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$. Then it holds that*

$$\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee) \geq \widetilde{H}_\infty(\mathbf{s}) - nd\log(\frac{1}{r_1}) + \frac{d}{2}\log(\Delta_K) - 1.$$

Proof. Since $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$, by Lemma 11, we have $\rho_{r_1}(\mathbf{x} + (R^\vee)^d) \leq 2$. Let $\mathbf{y} = \frac{\mathbf{s}}{q} + \mathbf{e}_1 \bmod R^\vee$ be a random variable over $(\mathbb{T}_{R^\vee})^d$, then we have

$$\begin{aligned}\int_{\mathbf{y}} \max_{\mathbf{s}^*} p_{\mathbf{e}_1}(\mathbf{y} - \frac{\mathbf{s}^*}{q} + (R^\vee)^d)d\mathbf{y} &= \frac{1}{\rho_{r_1}(\mathbb{R}^{nd})}\int_{\mathbf{y}} \max_{\mathbf{s}^*} \rho_{r_1}(\mathbf{y} - \frac{\mathbf{s}^*}{q} + (R^\vee)^d)d\mathbf{y} \\ &\leq \frac{1}{r_1^{nd}} \cdot \int_{\mathbf{y}} 2d\mathbf{y} = 2 \cdot (\frac{1}{r_1})^{nd} \cdot (\frac{1}{\Delta_K})^{\frac{d}{2}}.\end{aligned}$$

Therefore, by Lemma 2, we have

$$\begin{aligned}\widetilde{H}_\infty(\mathbf{s} \mid \frac{\mathbf{s}}{q} + \mathbf{e_1} \bmod R^\vee) &\geq \widetilde{H}_\infty(\mathbf{s}) - \log(\int_{\mathbf{y}} \max_{\mathbf{s}^*} p_{\mathbf{e}_1}(\mathbf{y} - \frac{\mathbf{s}^*}{q} + (R^\vee)^d)d\mathbf{y}) \\ &\geq \widetilde{H}_\infty(\mathbf{s}) - nd\log(\frac{1}{r_1}) + \frac{d}{2}\log(\Delta_K) - 1.\end{aligned}$$

□

By combining Theorem 4 and Theorem 6, we can easily obtain the following corollary.

Corollary 4. *Let C be the global constant from Corollary 1. Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R and $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$. Let q, d, m be positive integers with $m > d > 1$ and r, γ, $r_1 > 0$. Let $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ be an error term with $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$ and $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution $\mathcal{S}$, with*

$$\widetilde{H}_\infty(\mathbf{s}) \geq nk\log(q) + nd\log(\frac{1}{r_1}) - \frac{d}{2}\log(\Delta_K) + \omega(\log(\lambda)).$$

Let $r > \sqrt{2}C\sqrt{m}\gamma r_1$. Then the search problem E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DMLWE$(K, k, q, D_{R,\gamma})$ *is hard.*

By combining Theorem 5 and Theorem 6, we can easily obtain the following corollary.

Corollary 5. *Let C be the global constant from Corollary 1. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K, $R^\vee$ be the dual of R and $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$. Let q be a prime such that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, d, m be positive integers where $m > d > 1$ and r, γ, $r_1 > 0$. Let $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ be an error term with $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$ and $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution $\mathcal{S}$, with*

$$\widetilde{H}_\infty(\mathbf{s}) \geq nk\log(q) + nd\log(\frac{1}{r_1}) - \frac{d}{2}\log(\Delta_K) + \omega(\log(\lambda)).$$

Let $r > \sqrt{2}C\sqrt{m}\gamma r_1$. Then the decisional problem E-DMLWE$(K, d, q, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DMLWE$(K, k, q, D_{R,\gamma})$ *and* DMLWE(K, k, q, m, D_r) *are hard.*

5 Entropic Ring Learning With Error

In this section we give the definition of Entropic Ring Learning With Error problem (E-RLWE) first, we alos consider dual forms. Then to prove the hardness of E-RLWE, we show a reduction from E-MLWE problem to E-RLWE problem and a reduction from E-DMLWE problem to E-DRLWE problem. Our proof follows the proof structure of Albrecht et al. [AD17].

5.1 Definition of the Entropic R-LWE

Definition 11 (Entropic R-LWE). *Let K be some number field with degree $n = \text{poly}(\lambda)$, R be the ring of integers of K and $R^\vee$ be the dual of R. Let $q = q(\lambda)$ be a modulus, $m = \text{poly}(\lambda)$ be a sample size. Let χ be an error distribution on $K_\mathbb{R}$ and $\mathcal{S} = \mathcal{S}(\lambda, K, q, m)$ be a secrets distribution on $R_q^\vee$. Let* $\text{RLWE}_{K,q,m,\chi}(\mathcal{S})$ *be the distribution over $(R_q)^m \times (\mathbb{T}_{R^\vee})^m$ obtained by choosing $\mathbf{a} \leftarrow U((R_q)^m)$, $s \leftarrow \mathcal{S}$, $\mathbf{e} \leftarrow \chi^m$, and outputting the pair $(\mathbf{a}, \frac{1}{q}(\mathbf{a} \cdot s) + \mathbf{e} \bmod R^\vee)$.*

We say that the search problem E-RLWE$(K, q, m, \mathcal{S}, \chi)$ *is hard, if it holds for every* PPT *adversary $\mathcal{A}$ that*

$$\Pr[\mathcal{A}(\mathbf{a}, \frac{1}{q}(\mathbf{a} \cdot s) + \mathbf{e} \bmod R^\vee) = s] \leq \text{negl}(\lambda),$$

where $\mathbf{a} \leftarrow U((R_q)^m)$, $s \leftarrow \mathcal{S}$ and $\mathbf{e} \leftarrow \chi^m$.

Likewise, we say that the decisional problem E-DRLWE$(K, q, m, \mathcal{S}, \chi)$ *is hard, if it holds for every* PPT *distinguisher $\mathcal{D}$ that*

$$|\Pr[\mathcal{D}(\mathbf{a}_1, \mathbf{b}_1) = 1] - \Pr[\mathcal{D}(\mathbf{a}_2, \mathbf{b}_2) = 1]| \leq \text{negl}(\lambda),$$

where $(\mathbf{a}_1, \mathbf{b}_1) \leftarrow \text{RLWE}_{K,q,m,\chi}(\mathcal{S})$ and $(\mathbf{a}_2, \mathbf{b}_2) \leftarrow U((R_q)^m \times (\mathbb{T}_{R^\vee})^m)$.

5.2 Hardness of E-RLWE

In this section we will establish the hardness of entropic search RLWE with continuous gaussian noise. Using discretization technique, we can also easily get that entropic search RLWE with discrete gaussian noise is also hard. We will first recall a lemma in [AD17], and then show the hardness of E-RLWE problem.

Lemma 12 (Adapted from Corollary 3 in [AD17]). *Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R and $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$. Let d, q be positive integers, and $\mathbf{G} = (1, q, \cdots, q^{d-1}) \in R^{1\times d}$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ according to some distribution $\mathcal{S}$ satisfying $\Pr_{\mathbf{s}\leftarrow\mathcal{S}}[\max_{i,j} |\sigma_i(s_j)| > B] = 0$. Also take any $r > 0$, any $\epsilon \in (0, 1/2)$, $\tau \geq \frac{1}{q}\|\widetilde{B}_R\| \cdot \sqrt{2\ln(2nd(1+1/\epsilon))/\pi}$, and define $r' = \sqrt{r^2 + (\tau B(mn)^{1/4})^2}$. Suppose there exists a* PPT *algorithm which can solve* E-RLWE$(K, q^d, m, \mathbf{G}\mathcal{S}, D_{r'})$ *with probability p. Then there is a* PPT *algorithm solving* E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ *with probability at least $\frac{p^2}{2} - (2d+6)\epsilon m$.*

We now use the above lemma to show the hardness of E-RLWE problem.

Theorem 7. *Let C be the global constant from Corollary 1. Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R, $\mathbf{B}_R$ be some known basis of R and $\mathbf{B}_{R^\vee}$ be some known basis of $R^\vee$ in $\mathbb{H}$. Let q, d, m be positive integers with $m > d > 1$, r, γ, $r_1 > 0$ and*

$$\tau \geq \frac{1}{q}\|\widetilde{B}_R\| \cdot \sqrt{2\ln(2nd(1+2^{\omega(\log(\lambda))}))/\pi}.$$

Let $\mathbf{e}_1 \leftarrow D_{r_1}(K_\mathbb{R})^d$ be an error term with $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$ and $\mathbf{s}$ be a random variable on $(R_{q^d}^\vee)$ distributed according to some distribution $\mathcal{S}$, with

$$\widetilde{H}_\infty(\mathbf{s}) \geq nk\log(q) + nd\log(\frac{1}{r_1}) - \frac{d}{2}\log(\Delta_K) + \omega(\log(\lambda)).$$

Let $r' > \sqrt{2}C\sqrt{m}\gamma r_1$, and set $r^2 = r'^2 + (\tau nq\|\mathbf{B}_{R^\vee}\|_\infty (mn)^{1/4})^2$. Then we have that the search problem E-RLWE$(K, q^d, m, \mathcal{S}, D_r)$ *is hard, provided the* primal-DMLWE$(K, k, q, D_{R,\gamma})$ *is hard.*

Proof. Let $\mathbf{G} = (1, q, \cdots, q^{d-1}) \in R^{1\times d}$. Then we can easily find that the map $h_\mathbf{G} : (R_q^\vee)^d \mapsto R_{q^d}^\vee$ given by $h_\mathbf{G}(\mathbf{s}) = \mathbf{G}\mathbf{s}$ is a bijection. Thus, for any $s \in R_{q^d}^\vee$, we denote $\mathbf{G}^{-1}(s)$ be preimage of s. And for any distribution $\mathcal{S}$ on $R_{q^d}^\vee$, we denote $\mathbf{G}^{-1}(\mathcal{S})$ be a distribution on $(R_q^\vee)^d$ such that if $\mathbf{s}$ is a random variable according to $\mathbf{G}^{-1}(\mathcal{S})$, then $\mathbf{G}\mathbf{s}$ is a random variable according to $\mathcal{S}$.

Assume there is an adversary $\mathcal{A}$ and a distribution $\mathcal{S}$ such that $\mathcal{A}$ has non-negligible advantage to solve E-RLWE$(K, q^d, m, \mathcal{S}, D_r)$, and $\mathcal{S}$ satisfies

$$\widetilde{H}_\infty(\mathbf{s}) \geq nk\log(q) + nd\log(\frac{1}{r_1}) - \frac{d}{2}\log(\Delta_K) + \omega(\log(\lambda)).$$

Then since $\mathbf{G}^{-1}(\mathcal{S})$ is a distribution on $(R_q^\vee)^d$, we have

$$\Pr_{\mathbf{s}\leftarrow\mathbf{G}^{-1}(\mathcal{S})}[\max_{i,j}|\sigma_i(s_j)| > nq\|\mathbf{B}_{R^\vee}\|_\infty] = 0.$$

Then by Lemma 12, we can construct a PPT adversary $\mathcal{A}'$ such that $\mathcal{A}'$ solving E-MLWE$(K, d, q, m, \mathbf{G}^{-1}(\mathcal{S}), D_{r'})$ with probability

$$\mathrm{Adv}(\mathcal{A}') \geq \frac{(\mathrm{Adv}(\mathcal{A}))^2}{2} - (2d+6)m \cdot 2^{-\omega(\log(\lambda))}.$$

And since $h_{\mathbf{G}}$ is a bijection, we have

$$\widetilde{H}_\infty(\mathbf{G}^{-1}(\mathcal{S})) = \widetilde{H}_\infty(\mathcal{S}) \geq nk\log(q) + nd\log(\frac{1}{r_1}) - \frac{d}{2}\log(\Delta_K) + \omega(\log(\lambda)).$$

Thus by Corollary 4, we have the search problem E-MLWE$(K, d, q, m, \mathcal{S}, D_r)$ is hard, which contradicts to the advantage of $\mathcal{A}'$. This concludes the proof. □

5.3 Hardness of E-DRLWE

In this section we will establish the hardness of entropic decision RLWE with continuous gaussian noise. Using discretization technique, we can also easily get that entropic decision RLWE with discrete gaussian noise is also hard. We will first recall some lemmas, then prove a reduction from E-DMLWE problem to E-DRLWE problem, and finally show the hardness of E-RLWE problem.

Lemma 13 (Adapted from Theorem 1 in [AD17]). *Let R be the ring of integers of some algebraic number field K of degree n, let d, q, be positive integers, $\epsilon \in (0, \frac{1}{2})$, and $\mathbf{G} \in R^{1\times d}$. Also, fix $\mathbf{s} = (s_1, \cdots, s_d) \in (R^\vee)^d$. Further, let $\mathbf{B}_\Lambda$ be some known basis of the lattice $\Lambda = \frac{1}{q^d}\mathbf{G}^{\mathrm{T}}R + R^d$ (in $\mathbb{H}^d$), $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$ and*

$$\tau \geq \max(\|\widetilde{\mathbf{B}}_\Lambda\|, \frac{1}{q}\|\widetilde{\mathbf{B}}_R\|) \cdot \sqrt{\frac{2\ln(2nd(1+1/\epsilon))}{\pi}}.$$

There exists an efficient probabilistic mapping $\mathcal{F} : (R_q)^d \times \mathbb{T}_{R^\vee} \mapsto R_{q^d} \times \mathbb{T}_{R^\vee}$ such that:

1. *The output distribution given uniform input $\mathcal{F}(U((R_q)^d \times \mathbb{T}_{R^\vee}))$ is within statistical distance 4ϵ of the uniform distribution over $R_{q^d} \times \mathbb{T}_{R^\vee}$.*
2. *Let $B = \max_{i,j}|\sigma_i(s_j)|$, the distribution of $\mathcal{F}(\mathbf{a}_1, \mathbf{a}_1^{\mathrm{T}} \cdot \mathbf{s} + e_1 \bmod R^\vee)$ is within statistical distance $(2d+6)\epsilon$ of $(a_2, a_2 \cdot \mathbf{G}\mathbf{s} + e_2 \bmod R^\vee)$, where $\mathbf{a}_1 \leftarrow U((R_q)^d)$, $e_1 \leftarrow D_r$ and $a_2 \leftarrow U(R_{q^d})$, $e_2 \leftarrow D_{\mathbf{r}'}$ with $(\mathbf{r}'_i)^2 = r^2 + \tau^2(\beta^2 + \sum_{j=1}^d |\sigma_i(s_j)|^2)$ for any β satisfying $\beta^2 \geq B^2 d$.*

Lemma 14 (Claim 7.1 in [PRS17]). *Let $r_1, \cdots, r_n \in \mathbb{R}^+$ and $s_1, \cdots, s_n \in \mathbb{R}^+$ be such that for all i, $|s_i/r_i - 1| < \sqrt{\log n/n}$. Then any set $A \subset \mathbb{R}^n$ whose measure under the Gaussian distribution $D_{r_1} \times \cdots \times D_{r_n}$ is non-negligible, also has non-negligible measure under $D_{s_1} \times \cdots \times D_{s_n}$.*

We now show a reduction from E-DMLWE to E-DMLWE with a spherical error distribution. Our proof follows the proof structure of Peikert et al. [PRS17].

Lemma 15. *Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R and $\mathcal{S}$ be a distribution on $R_q^\vee$. Then, there is a randomized polynomial-time algorithm that given any $\eta > 0$ and $m \geq 1$, as well as an oracle that solves* E-DRLWE$(K, q, m, \mathcal{S}, D_r)$ *given only m samples, where $r = \eta(nm/\log(nm))^{1/4}$, solves* E-DRLWE$(K, q, m, \mathcal{S}, D_{\mathbf{r}'})$ *for any (possibly unknown) $\mathbf{r}'$ satisfying that all r_i' are in $[0, \eta]$.*

Proof. For $e_1, \cdots, e_m \in \mathbb{T}$, consider the transformation mapping m samples $(a_i, b_i)_{i=1}^m$ to $(a_i, b_i + e_i)_{i=1}^m$. Then it is easy to see that for all secrets distribution $\mathcal{S}$ on $R_q^\vee$, error distribution χ and $\widetilde{\mathbf{r}}$, if we sample from $\mathrm{RLWE}_{K,q,m,\chi}(S)$ and apply this transformation with $e_1, \cdots, e_m \in \mathbb{T}$ chosen independently from $D_{\widetilde{\mathbf{r}}}$, then the output distribution is $\mathrm{RLWE}_{K,q,m,\chi+D_{\widetilde{\mathbf{r}}}}(S)$.

The reduction repeats the following reduction a polynomial number of times. Choose $e_1, \cdots, e_m$ independently from D_r. Then estimate the acceptance probability of the oracle on the following two input distributions: the first is obtained by applying the above transformation with $e_1, \cdots, e_m$ to our input samples; the second is the uniform distribution $(R_q \times \mathbb{T})^m$. If in any of these polynomial number of attempts, a non-negligible difference is observed between the two acceptance probabilities, output "non-uniform"; otherwise output "uniform".

Notice that if our input distribution is uniform, then in each of the attempts, the two distributions on which we estimate the oracle's acceptance probability are exactly the same, hence we output "uniform" with overwhelming probability. Assume that our input distribution is $\mathrm{RLWE}_{K,q,m,D_{\mathbf{r}'}}(S)$ for some $\mathbf{r}'$ satisfying that all r_i' are in $[0, \alpha]$. Let $B(e_1, \cdots, e_m)$ be the distribution on m pairs that our reduction uses as input to the oracle. Define the vector $\widetilde{\mathbf{r}}$ with coordinates $\widetilde{r}_j = r - r_j$ so that $D_{\mathbf{r}'} + D_{\widetilde{\mathbf{r}}} = D_r$. By our observation above, the distribution of $B(e_1, \cdots, e_m)$ over $e_1, \cdots, e_m \leftarrow D_{\widetilde{\mathbf{r}}}$ is $\mathrm{RLWE}_{K,q,m,\chi+D_{\widetilde{\mathbf{r}}}}(S)$. Let T be the set of all tuples $(e_1, \cdots, e_m)$ for which the oracle has a non-negligible difference in acceptance probability on $B(e_1, \cdots, e_l)$ and on the unifrom distribution. By assumption, the measure of T under $D_{\widetilde{\mathbf{r}}}$ is non-negligible. Therefore by Lemma 14, we have the measure of T under $(D_r)^m$ is also non-negligible , and we are done. □

We now use the above lemma to show a reduction from E-DMLWE problem to E-DRLWE problem.

Lemma 16. *Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R and $\mathbf{B}_R$ be some known basis of R in $\mathbb{H}$. Let d, q be positive integers, and $\mathbf{G} = (1, q, \cdots, q^{d-1}) \in R^{1\times d}$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ according to some distribution $\mathcal{S}$ satisfying*

$$\Pr_{\mathbf{s}\leftarrow\mathcal{S}}[\max_{i,j} |\sigma_i(s_j)| > B] = 0.$$

Also take any $r > 0$, any $\epsilon \in (0, 1/2)$,

$$\tau \geq \frac{1}{q}\|\widetilde{B}_R\| \cdot \sqrt{2\ln(2nd(1 + 2^{\omega(\log(\lambda))}))/\pi},$$

and define $r' = \sqrt{r^2 + 2\tau^2 B^2 d} \cdot (nm/\log(nm))^{1/4}$. *Suppose there exists a* PPT *algorithm solving* E-DRLWE$(K, q^d, m, \mathbf{G}\mathcal{S}, D_{r'})$ *with non-negligible probability, then there is a* PPT *algorithm solving* E-DMLWE$(K, d, q, m, \mathcal{S}, D_r)$ *with non-negligible probability.*

Proof. When we gets as input $(\mathbf{A}, \mathbf{b}) \in (R_q)^{m\times d} \times (\mathbb{T}_{R^\vee})^m$, we use the transformation in Lemma 13 to our input samples and get $(\mathbf{a}', \mathbf{b}') \in (R_{q^d})^m \times (\mathbb{T}_{R^\vee})^m$. Then repeats the following a polynomial number of times. Estimate the acceptance probability of the oracle on the following two input distributions: the first is obtained by applying transformation in Lemma 14 with $e_1, \cdots, e_m$ to $(\mathbf{a}', \mathbf{b}')$; the second is the uniform distribution $(R_{q^d})^m \times (\mathbb{T}_{R^\vee})^m$. If in any of these polynomial number of attempts, a non-negligible difference is observed between the two acceptance probabilities, output "non-uniform"; otherwise output "uniform".

Notice that if input distribution is $\mathrm{MLWE}_{K,d,q,m,D_r}(\mathcal{S})$, then by Lemma 13, the distribution of $(\mathbf{a}', \mathbf{b}')$ is $\mathrm{RLWE}_{K,q^d,m,D_{\mathbf{r}'}}(\mathcal{S})$, where $r_i' \in [0, \sqrt{r^2 + 2\tau^2 B^2 d}]$; if our input distribution is uniform, then $(\mathbf{a}', \mathbf{b}')$ is also uniform. Therefore by Lemma 15, we can solving E-DMLWE$(K, d, q, m, \mathcal{S}, D_r)$ with non-negligible probability. □

By combining Corollary 5 and Lemma 16, we can get the following theorem. The proof of the following theorem is analogous to Theorem 7 and we describe the proof in full version of this paper.

Theorem 8. *Let C be the global constant from Corollary 1. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n, where α is an algebraic integer, $f(x)$ be the minimum polynomial of α over $\mathbb{Q}$. Let R be the ring of integers of K, $R^\vee$ be the dual of R, $\mathbf{B}_R$ be some known basis of R and $\mathbf{B}_{R^\vee}$ be some known basis of $R^\vee$ in $\mathbb{H}$. Let q be a prime such that $f(x)$ is an irreducible polynomial in $\mathbb{Z}_q[x]$, d, m be positive integers with $m > d > 1$, r, γ, $r_1 > 0$ and*

$$\tau \geq \frac{1}{q}\|\widetilde{B}_R\| \cdot \sqrt{2\ln(2nd(1 + 2^{\omega(\log(\lambda))}))/\pi}.$$

Let $\mathbf{e}_1 \leftarrow D_{r_1}(K_{\mathbb{R}})^d$ be an error term with $\frac{1}{r_1} \geq \|\widetilde{\mathbf{B}}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$ and $\mathbf{s}$ be a random variable on $(R^\vee_{q^d})$ distributed according to some distribution $\mathcal{S}$, with

$$\widetilde{H}_\infty(\mathbf{s}) \geq nk\log(q) + nd\log(\frac{1}{r_1}) - \frac{d}{2}\log(\Delta_K) + \omega(\log(\lambda)).$$

Let $r' > \sqrt{2}C\sqrt{m}\gamma r_1$, and $r = \sqrt{r'^2 + 2\tau^2 n^2 q^2 \|\mathbf{B}_{R^\vee}\|_\infty^2 d} \cdot (nm/\log(nm))^{1/4}$ Then the decisional problem E-DRLWE$(K, q^d, m, \mathcal{S}, D_r)$ *is hard, provided that* primal-DMLWE$(K, k, q, D_{R,\gamma})$ *and* DMLWE$(K, k, q, m, D_{r'})$ *are hard.*

References

ACP+09. Applebaum, B., Cash, D., Peikert, C., Sahai, A. (2009, August). Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In Annual International Cryptology Conference (pp. 595-618). Springer, Berlin, Heidelberg.

AD17. Albrecht, M. R., Deo, A. (2017, December). Large Modulus Ring-LWE ≥ Module-LWE. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 267-296). Springer, Cham.

AW04. Alaca, Ş., Williams, K. S. (2004). Introductory algebraic number theory. Cambridge: Cambridge University Press.

BBP+19. Bolboceanu, M., Brakerski, Z., Perlman, R., Sharma, D. (2019, December). Order-lwe and the hardness of ring-lwe with entropic secrets. In International Conference on the Theory and Application of Cryptology and Information Security (pp. 91-120). Springer, Cham.

BD20. Brakerski, Z., Döttling, N. (2020, May). Hardness of LWE on General Entropic Distributions. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 551-575). Springer, Cham.

BDK+18. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., Stehlé, D. (2018, April). CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In 2018 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 353-367). IEEE.

BLP+13. Brakerski, Z., Langlois, A., Peikert, C., Regev, O., Stehlé, D.(2013). Classical hardness of learning with errors. In: Proceedings of the forty-fifth annual ACM symposium on Theory of computing (pp. 575-584).

BGV12. Brakerski, Z., Gentry, C., Vaikuntanathan, V.(2014). (Leveled) fully homomorphic encryption without bootstrapping. ACM Transactions on Computation Theory (TOCT), 6(3), 1-36.

Coh13. Cohen, H. (2013). A course in computational algebraic number theory (Vol. 138). Springer Science & Business Media.

DOR+08. Dodis, Y., Ostrovsky, R., Reyzin, L., Smith, A. (2008). Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. SIAM journal on computing, 38(1), 97-139.

GKP+10. Goldwasser, S., Kalai, Y. T., Peikert, C., Vaikuntanathan, V. (2010). Robustness of the learning with errors assumption.

GPV08. Gentry, C., Peikert, C., Vaikuntanathan, V.(2008). Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the fortieth annual ACM symposium on Theory of computing (pp. 197-206).

HPS98. Hoffstein, J., Pipher, J., Silverman, J. H. (1998, June). NTRU: A ring-based public key cryptosystem. In International Algorithmic Number Theory Symposium (pp. 267-288). Springer, Berlin, Heidelberg.

LPR10. Lyubashevsky, V., Peikert, C., Regev, O.(2010). On ideal lattices and learning with errors over rings. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 1-23). Springer, Berlin, Heidelberg.

LPR13. Lyubashevsky, V., Peikert, C., Regev, O. (2013). A toolkit for ring-LWE cryptography. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 35-54). Springer, Berlin, Heidelberg.

LS15. Langlois, A., Stehlé, D. (2015). Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 75(3), 565-599.

Mic02. Micciancio, D. (2002, November). Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings. (pp. 356-365). IEEE.

MP12. Micciancio, D., Peikert, C. (2012, April). Trapdoors for lattices: Simpler, tighter, faster, smaller. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 700-718). Springer, Berlin, Heidelberg.

MR07. Micciancio, D., Regev, O. (2007). Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 37(1), 267-302.

Reg05. Regev, O. (2005, May). On lattices, learning with errors, random linear codes, and cryptography. In Proceedings of the thirty-seventh annual ACM symposium on Theory of computing (pp. 84-93).

PRS17. Peikert, C., Regev, O., Stephens-Davidowitz, N. (2017, June). Pseudorandomness of ring-LWE for any ring and modulus. In Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (pp. 461-473).

RSW18. Rosca, M., Stehlé, D., Wallet, A. (2018, April). On the ring-LWE and polynomial-LWE problems. In Annual International Conference on the Theory and Applications of Cryptographic Techniques (pp. 146-173). Springer, Cham.

Ver10. Vershynin, R. (2010). Introduction to the non-asymptotic analysis of random matrices. arXiv preprint arXiv:1011.3027.

Ver18. Vershynin, R. (2018). High-dimensional probability: An introduction with applications in data science (Vol. 47). Cambridge university press.

WW18. Wang, Y., Wang, M. (2018). CRPSF and NTRU Signatures over cyclotomic fields. IACR Cryptol. ePrint Arch., 2018, 445.