Hardness of entropic module-LWE

Lin, Hao; Wang, Mingqiang; Zhuang, Jincheng; Wang, Yang

DOI
10.1016/j.tcs.2024.114553

Publication date
2024

Document Version
Final published version

Published in
Theoretical Computer Science

Theoretical Computer Science 999 (2024) 114553

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Hardness of Entropic Module-LWE ☆

Hao Lin [a,b], Mingqiang Wang [b,d], Jincheng Zhuang [c,*], Yang Wang [b,d]

[a] Faculty of Electrical Engineering, Mathematics and Computer Science, Delft University of Technology, Delft, Netherlands
[b] School of Mathematics, Shandong University, Jinan, China
[c] Quan Cheng Laboratory, Jinan, China
[d] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Jinan, China

ARTICLE INFO

Communicated by G. Yang

Keywords:
Entropic Module-LWE
Binary Module-LWE
Leftover hash lemma

ABSTRACT

The Learning with Errors (LWE) problem is a versatile basis for building various purpose post-quantum schemes. Goldwasser et al. [ISC 2010] initialized the study of a variant of this problem called the Entropic LWE problem, where the LWE secret is generated from a distribution with a certain min-entropy. Brakerski and Döttling recently further extended the study in this field, and first proved the hardness of the Entropic LWE problem with unbounded secret [Eurocrypt 2020], then gave a similar result for the Entropic Ring-LWE problem [TCC 2020].

In this work, we systematically study the hardness of the Entropic Module-LWE problem. Adapting the "lossiness approach" to the module setting, we give lower entropy bounds for the secret distributions that guarantee the hardness of the Entropic Module-LWE problem in both search and decision cases, where results are divided into two settings: bounded and unbounded norm. We also present that our search entropy lower bound in the unbounded case is essentially tight. An application of our bounded result is to deduce the hardness for the Binary Module-LWE problem. One of our central techniques is a new generalized leftover hash lemma over rings, which might be of independent interest.

1. Introduction

The Learning with Errors (LWE) problem, introduced by Regev [29], has been proven to be a versatile basis for constructing cryptography schemes. Among several appealing properties of the LWE problem are its reductions from worst-case lattice problems [20,22,28,29], and its conjectured post-quantum security.

To improve the asymptotic and practical efficiency of LWE-based cryptographic schemes, Lyubashevsky et al. [22] introduced the Ring-LWE problem. To interpolate LWE and Ring-LWE, Brakerski et al. [10,20] introduced the Module-LWE problem. The Module-LWE problem might be able to offer a better level of security than the Ring-LWE problem, while still offering performance advantages over the LWE problem.

The assumption that the LWE and its variants are intractable was used as a basis for various classical applications, such as public key encryption [15,29], key exchange [12,27], identity-based encryption [15], functional encryption [1] and various cutting edge primitives, such as fully homomorphic encryption (FHE) [16] and indistinguishability obfuscation (IO) [18].

☆ This article belongs to Section A: Algorithms, automata, complexity and games, Edited by Paul Spirakis.

* Corresponding author.
E-mail addresses: baronlin001@gmail.com (H. Lin), wangmingqiang@sdu.edu.cn (M. Wang), jchzhuang@gmail.com (J. Zhuang), wyang1114@mail.sdu.edu.cn (Y. Wang).

https://doi.org/10.1016/j.tcs.2024.114553
Received 16 May 2022; Received in revised form 6 October 2023; Accepted 3 April 2024

Available online 8 April 2024

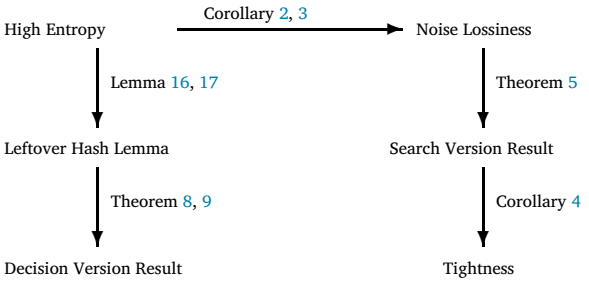

Fig. 1. Outline of our approach for Entropic Module-LWE.

With the rapid development of quantum computers, it is imperative to develop quantum-resistant cryptography schemes. For example, NIST proposed a standardization project, with the aim of selecting quantum-safe schemes for public-key encryption and digital signatures. Currently, the selected final standards Kyber [6] and Dilithium [14] are both based on the Module-LWE problem. Another well-studied KEM scheme Saber relies on the hardness of the Module Learning with Rounding (Module-LWR) problem, which is the definite variant of the Module-LWE problem.

Entropic secrets Motivated to achieve an entropic notion of security that will allow guaranteeing the hardness even if some information about the secret $\mathbf{s}$ is leaked, Goldwasser et al. [17] initiated the study on the hardness of the LWE problem when the secret $\mathbf{s}$ is not chosen uniformly at random. They developed a "noise flooding" method and proved that if $\mathbf{s}$ is sampled from a binary distribution (i.e. supported over $\{0,1\}^n$), then the LWE problem remains hard so long as $\mathbf{s}$ has sufficient entropy. Later, Alwen et al. [4] proved that the LWE problem is hard for bounded secret with sufficient entropy.

Recently, Brakerski and Döttling [9] further extended the study in this setting. They first considered the hardness of the LWE problem with unbounded secrets. By proposing a new approach to deal with the noise ("flooding at the source"), they first got an entropy bound that guarantees the security of the Entropic LWE problem. Besides, their method is also applicable for the bounded case, and yields similar results as [4]. Then they adopted this approach to the ring setting [35], and established the hardness result for the search Entropic Ring-LWE problem. The hardness of the decision Entropic Ring-LWE problem is still an open problem.

Boudgoust et al. [7,19] studied a special Entropic version problem, called Binary Module-LWE. They adapted the method proposed in [17] to the module setting, and showed the hardness of the Binary Module-LWE problem. However, there is no result known for the hardness of the Entropic Module-LWE problem with general secret distribution both in bounded and unbounded cases. In this work, we focus on determining hardness of the Entropic Module-LWE problem.

1.1. Our contributions

We make a systematic study on the hardness of the Entropic Module-LWE problem, and get the hardness results for both search and decision versions. The brief structure of our study is outlined in Fig. 1.

Search version First, we adapt the "flooding at the source" [9] approach to the module setting, and show that the secret distributions with sufficiently high noise lossiness will lead to the hardness of the search Entropic Module-LWE problem. The *noise lossiness* of secret distribution $\mathcal{S}$, denoted by $\nu_\alpha(\mathcal{S})$, is defined to be the conditional smooth min-entropy of a sample from $\mathcal{S}$ conditioned on learning its perturbation by gaussian noise. Formally, $\nu_\alpha(\mathcal{S}) = \tilde{H}_\infty(\mathbf{s} \mid \mathbf{s} + \mathbf{e} \bmod qR^\vee)$ where $\mathbf{e}$ is a gaussian noise with parameter α. Then, we analyze the relation between the *noise-lossiness* and the *min-entropy* of the secret distribution. According to whether there is a bound on the norm of the secret, we distinguish two cases below. By this one can deduce the lower bound for min-entropy of the secret distribution to imply the hardness of Module-LWE in both general case and bounded case, where the bounded case can achieve a better lower bound. Our results can be expressed as the following theorem.

Theorem 1. *Assume that the decision primal Module-LWE problem over ring R with modulus q, dimension k and gaussian noise parameter β is hard. Then the following holds:*

General case: *If secret distribution $\mathcal{S}$ over $(R_q^\vee)^d$ satisfies that:*

$$\widetilde{H}_\infty(\mathcal{S}) \geq nk\log(q) + nd\log\left(\frac{q}{\alpha'}\right) - \frac{d}{2}\log(\Delta_K) + 1 + \omega(\log(\lambda)),$$

where $\frac{q}{\alpha'} \geq \|\tilde{B}_R\| \cdot \sqrt{\frac{\log 4nd}{\pi}}$. Then the search Entropic Module LWE problem with rank d, modulus q, secret distribution $\mathcal{S}$ and gaussian noise parameter $\alpha \approx \alpha'\beta\sqrt{m}$ is hard.

Bounded case: *If secret distribution $\mathcal{S}$ over $(R_q^\vee)^d$ is M-bounded and satisfies that:*

$$\widetilde{H}_\infty(S) \geq nk\log(q) + \sqrt{2\pi nd}\cdot\frac{M}{\alpha'}\log(e) + \omega(\log(\lambda)).$$

Then the search Entropic Module LWE problem with rank d, modulus q, secret distribution $\mathcal{S}$ and gaussian noise parameter $\alpha \approx \alpha'\beta\sqrt{m}$ is also hard.

Our bounded case result directly implies the hardness of the Binary Module-LWE problem, which is a very common variant in applications. For unbounded case, we also show that for general modulus and general min-entropy distributions, this lower bound is tight up to polynomial factors. Besides, during the proof, we introduce a new gaussian decomposition theorem and present the relation between the *noise-lossiness* and the *min-entropy* over module setting, which might be of independent interests.

Decision version Note that, the above theorem only applies to the search version. But the security of many cryptographic schemes depends on the hardness of the decision version. An interesting phenomenon is that, for the Module-LWE problem, we have a search to decision reduction, which means the decision version problem is as hard as the search version. But for the Entropic Module-LWE problem, the hardness of the search version does not always imply the hardness of the decision version. To illustrate this, let us consider a specific setting that the ring R satisfies $qR = \mathfrak{q}_1\mathfrak{q}_2$, where each $N(\mathfrak{q}_i) = q^{n/2}$, $\mathcal{S}$ is a uniform distribution over $(R/\mathfrak{q}_1)^d$ but is 0 mod $\mathfrak{q}_2$, and noise satisfies a gaussian distribution. In this case, the secret distribution has very high min-entropy $\widetilde{H}_\infty(S) = nd\log(q)/2$ which satisfies our requirement, so the search problem is hard. However, in this case, the decision problem is easy. Note that for any Module-LWE sample $(\mathbf{a}, \mathbf{y})$, we have $\langle\mathbf{a}, \mathbf{s}\rangle \bmod \mathfrak{q}_2 = 0$. The adversary can easily solve the decision problem by identifying whether $\mathbf{y} \bmod \mathfrak{q}_2$ is uniform distribution over $R/\mathfrak{q}_2$. Therefore, the hardness of the decision version and the search version problem on these rings are separated.

It is worth noting that the phenomenon described above also exists in the case of plain LWE. However, in the LWE setting, q is usually chosen as a prime, which turns $\mathbb{Z}_q$ into a field, eliminating the aforementioned issue. On the other hand, for the Module-LWE problem, parameters that would make R_q a field are generally not chosen. Therefore, the impact of the aforementioned issue on the Module-LWE problem is more significant.

From the above simple example, we know that the requirement that the secret distribution has high-entropy is obviously not enough for the decision Entropic Module-LWE problem. To deal with the above attacks, the secret distribution needs at least has enough entropy on each prime ideal. Fortunately, we find that this requirement is sufficient. We show that if secret distribution satisfies that for every prime ideal factor $\mathfrak{p}_i | qR$, $\mathbf{s} \bmod \mathfrak{p}_i R^\vee$ has high entropy, then the decision Entropic Module-LWE problem is also hard. To prove this result, we introduce a new leftover hash lemma over module setting, which might be of independent interest. Similar to the search case, the results in the decision version are also divided into two cases, general high entropy case and bounded case, the bounded case can also get a smaller lower bound. The results can be expressed as the following theorem.

Theorem 2. *Assume that the decision primal Module-LWE problem over ring R with prime modulus q, dimension k and gaussian noise parameter β is hard. Assume the decomposition of qR can be expressed as $\prod_i \mathfrak{p}_i^{r_i}$, where each $\mathfrak{p}_i$ is a prime ideal over R. Then the following holds:*

General case: *If secret distribution $\mathcal{S}$ over $(R_q^\vee)^d$ satisfies that:*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \geq nk\log(q+1) + nd\log\left(\frac{q}{\alpha'}\right) - \frac{d}{2}\log(\Delta_K) - 1 + \omega(\log(\lambda)),$$

for any prime ideal $\mathfrak{p}_i$ of qR, where $\frac{q}{\alpha'} \geq \|\tilde{B}_R\| \cdot \sqrt{\frac{\log 4nd}{\pi}}$. Then the decision Entropic Module LWE problem with rank d, modulus q, secret distribution $\mathcal{S}$ and gaussian noise parameter $\alpha \approx \alpha'\beta\sqrt{m}$ is hard.

Bounded case: *If secret distribution $\mathcal{S}$ over $(R_q^\vee)^d$ is M-bounded and satisfies that:*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \geq nk\log(q+1) + \sqrt{2\pi nd}\cdot\frac{M}{\alpha'}\log(e) - 2 + \omega(\log(\lambda))$$

for any prime ideal $\mathfrak{p}_i$ of qR. Then the decision Entropic Module LWE problem with rank d, modulus q, secret distribution $\mathcal{S}$ and gaussian noise parameter $\alpha \approx \alpha'\beta\sqrt{m}$ is also hard.

As an application of this result, we can obtain the hardness of the decision Entropic Ring-LWE problem for some special case secret distribution by combining this theorem and the "modulus switching" technique developed by [2]. The "modulus switching" technique can ensure that the secret keys before and after the switching have the same minimum entropy. However, it introduces an expansion factor for the noise terms, which is related to the maximum norm of the secret keys. Nevertheless, when the noise term is very large, the (Ring-)LWE problem becomes statistically difficult. Therefore, to obtain more meaningful results, we only consider the scenario where the secret key is bounded. In this situation, we can prove that when both $s \bmod qR^\vee$ and $(s - s \bmod qR^\vee)/q$ are bounded, and the entropy of s is sufficiently large, the decision Entropic Ring-LWE problem becomes intractable, where s is a random variable over $R_{q^2}^\vee$. The formal analysis of Entropic Ring-LWE are presented in Section 5.

1.2. Technical overview

Here we provide a technical overview of our main contributions.

Search version At a high level, we prove the hardness of the Entropic Module-LWE problem by adapting the "flooding at the source" approach developed by Brakerski et al. [9] to the module setting. Their proof framework consists of the following 3 steps.

1. Replace A by a lossy matrix $BC + Z$, and replace $\mathbf{e}$ by $F\mathbf{e}_1 + \mathbf{e}_2$;
2. Show that high noise lossiness $\nu_\alpha(S)$ implies the hardness of Entropic LWE;
3. Show that high min-entropy $\tilde{H}_\infty(\mathbf{s})$ implies high noise lossiness.

In the module setting, by the hardness of decision primal Module-LWE assumption (or decision primal Ring-LWE assumption) we can also replace A by $BC + Z$. But since the error term is in $K_{\mathbb{R}}$ and the matrix multiplication in the ring is different from which in $\mathbb{R}^n$, we need to establish a new decomposition theorem for continuous Gaussian distribution on $K_{\mathbb{R}}$ first.

If K is a number field with s_1 real embeddings denoted as $\sigma_1, \cdots, \sigma_{s_1}$ and s_2 pairs complex embeddings denoted as $\sigma_{s_1+1}, \cdots, \sigma_n$, then when F is a fixed matrix in $R^{m\times d}$, $\mathbf{e}_1 \leftarrow (D_{\alpha'}(K_{\mathbb{R}}))^d$ and $\mathbf{e} = F\mathbf{e}_1$, we have $\sigma_i(\mathbf{e})$ and $\sigma_j(\mathbf{e})$ are independent where $i \neq j$ and $|i-j| \neq s_2$. Therefore, we can sample $\mathbf{e}_2$ in blocks and make the random variable $F\mathbf{e}_1 + \mathbf{e}_2$ follow distribution according to $(D_\alpha(K_{\mathbb{R}}))^m$. The details are outlined in Section 3.1.

Step 3 (establishing a relation between min-entropy and noise-lossiness) are portable to the module setting, but we also need to take care of some mathematical subtleties in the ring. The complete analysis and formal statement are presented in Section 4.1.

Decision version In [9], Brakerski et al. proved the hardness of decision Entropic LWE problem when the modulus q is a prime. In this case $\mathbb{Z}_q$ is a field, and they can get a generalized leftover hash lemma. However, for module setting, the requirement that R_q is a field is too harsh. The commonly used ring does not meet this requirement. Therefore, to get the hardness result for the decision Entropic Module-LWE problem, we need to give a variant of leftover hash lemma first.

Our leftover hash lemma consider the case where there is a small amount of leakage of secrets, which states that for some secret distribution $\mathcal{S}$, if for every prime ideal factor $\mathfrak{p}_i | qR$, $\mathbf{s} \bmod \mathfrak{p}_i R^\vee$ has high entropy, then the distribution $(C, C\mathbf{s}, \mathbf{s}+\mathbf{e})$ and $(C, \mathbf{u}, \mathbf{s}+\mathbf{e})$ are statistical indistinguishability. The proof of our leftover hash lemma follows the framework from [21], but has some differences. Because we consider the case that the secret $\mathbf{s}$ is partially leaked $(\mathbf{s}+\mathbf{e})$, we need to use conditional probability in our calculation. As a result, the statistical distance between the two distributions in [21] is controlled by certain collision probability, while in this work it is controlled by certain conditional collision probability. Then we combine the result about the relation between min-entropy and noise-lossiness in Section 3.2 to get the result. For the complete analysis and formal statement of the result, see Section 3.3.

Combining this new lemma, we can adapt the framework in [9] to the module setting and get the hardness result for the decision version problem. The complete analysis and formal statement are presented in Section 4.2.

1.3. Comparison to previous work

Entropic Module-LWE: Following the generalized "closeness to low-rank" approach, Brakerski and Döttling [35] proved that the Ring-LWE problem is hard so long as secret distribution $\mathcal{S}$ has sufficient min-entropy. Their result is established under Decisional Small Polynomial Ratio (DSPR) and Ring-LWE assumption, where DSPR assumption is a mild variant of the NTRU assumption. They determined the hardness of the search version Entropic Ring-LWE problem. The hardness of the decision version Entropic Ring-LWE problem is still open.

Boudgoust et al. [7,19] studied a special Entropic Module-LWE problem, namely Binary Module-LWE. In [7], they adapted the method proposed in [17] to the module setting and use Rényi divergence proved the hardness result for the search version Binary Module-LWE problem. In [19], they adapted the method proposed in [11] to the module setting and showed the hardness result for the decision version Binary Module-LWE problem. These two results are established under the Module-LWE assumption.

Liu et al. [21] studied the definite variant of the Module-LWE problem, namely Module-LWR. They present a search-to-decision reduction for Module-LWR with respect to a special rounding method. As a result, they show that Module-LWR is pseudorandom as long as it is one-way.

Boudgoust et al. [8] recently adapted the proof method from [35] on rings to modules, which uses a sensibly different approach from the one we described above. Their proof is based on an Module-NTRU hardness assumption, while it is based on Module-LWE for us. Although their reduction is rank-preserving, hardness problem they based (Module-NTRU) has very few theoretical hardness results. Besides, their method only shows the entropic hardness of search Module-LWE problem, while our method also provide the entropic hardness of decision Module-LWE problem.

Concretely, in this work, we make the first systematic study on the hardness of the Entropic Module-LWE problem. We get the hardness results for the Entropic Module-LWE problem for both search and decision versions. Each version consists of two cases, where the bounded case has a better lower bound. Our results are established under the Module-LWE assumption (or Ring-LWE assumption). By using "modulus switching" technique, we also get the hardness result for the decision Entropic Ring-LWE problem with some special case secret distribution.

We summarize the results and the achieved parameters in Table 1, which primarily compare the parameters that can be achieved when we assume that the Module-LWE problem with rank k is hard, and secrets are uniformly sampled from a small range $[-\eta, \eta]$.

Table 1
Summary of the results for the Entropic Module-LWE problem.

	Field K	Rank d	Modulus q	Secret $\mathbf{s}$	Variant
[7,19]	Cyclotomic	$\frac{\log q}{\log(2\eta+1)}k$	Prime	$[-\eta,\eta]$	Decision (Search)
[8]	Arbitrary	k	All	$[-nk\log n, nk\log n]$	Search
Ours	Arbitrary	d	All	$[-2^{\frac{k\log q}{d}}, 2^{\frac{k\log q}{d}}]$	Search
Ours	Arbitrary	d	All	Depends on K[a]	Decision

[a] The achievable secret bound depends on the form of the field K.

Leftover hash lemma Most previous ring-based leftover hash lemmas require secret $\mathbf{s}$ to obey some special distribution. Roşca et al. [30] require $\mathbf{s} \leftarrow (D_{R,\alpha})^d$ and Boudgoust et al. [7] require $\mathbf{s} \leftarrow U((R_2^\vee)^d)$. Recently, Liu et al. [21] also proposed a new leftover hash lemma, they show that if $\mathbf{s}$ mod $\mathfrak{p}$ has sufficient entropy for every ideal factor $\mathfrak{p}$, then $C\mathbf{s}$ is indistinguishable from uniform distribution.

The situation we consider is different from theirs. We show that if $\mathbf{s}$ mod $\mathfrak{p}$ has sufficient entropy for every ideal factor $\mathfrak{p}$, then $C\mathbf{s}$ is indistinguishable from uniform distribution even if some auxiliary information $\mathbf{s}+\mathbf{e}$ is leaked. However, in [21], auxiliary information $\mathbf{s}+\mathbf{e}$ is not allowed to be disclosed.

1.4. Paper organization

The remaining of the paper is organized as follows. In Section 2, we present preliminaries and definitions. In Section 3, we prove three probability lemmas over ring. In Section 4, the Entropic Module-LWE problem is formally defined, and the hardness results for both search and decision version are established. In Section 5, we present the hardness results for the decision Entropic Ring-LWE.

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 upper-case letters (A, 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 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 $\bar{z}$. For a matrix X over $\mathbb{R}^{m\times n}$, the spectral norm of matrix is defined by $s_1(X) = \sup_{\mathbf{u}\neq 0} \frac{\|X\mathbf{u}\|_2}{\|\mathbf{u}\|_2}$.

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 $\{\mathbf{b}_1,\cdots,\mathbf{b}_j\}$. We will consider full rank (i.e. $j=n$) lattice. We use the matrix $B=[\mathbf{b}_1,\cdots,\mathbf{b}_n]$ to denote a basis. $\widetilde{B}$ is used to denote the Gram-Schmidt orthogonalization of columns in B (from left to right), $\|B\|$ is the length of the longest vector in ℓ_2 norm of the columns of B and $\|B\|_\infty$ is the length of the longest vector in ℓ_∞ norm of the columns of 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 $v \in K$, multiplication by v is a $\mathbb{Q}$-linear transformation of K into itself, i.e.

$$m_v : K \mapsto K \text{ given by } m_v(x) = vx.$$

The trace of v, denoted by $\mathrm{Tr}(v)$, is defined as the trace of this linear transformation. An element $v \in K$ 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 $\mathbb{T}_{qR^\vee} := K_\mathbb{R}/qR^\vee$. In this paper, we always explicitly assume K be some algebraic number field, R be its ring of integers and $R^\vee$ be the dual of R, unless stated otherwise.

An ideal $\mathcal{I} \subset R$ is a nontrivial additive subgroup that is closed under multiplication by R. An ideal $I \subsetneq R$ is said to be prime if whenever the product $xy \in I$ for elements $x, y \in R$, then at least one of x and y must also belong to I. Two ideal $\mathcal{I},\mathcal{J} \subset R$ are said to be coprime if $\mathcal{I}+\mathcal{J} = R$. A fractional ideal $\mathcal{I} \subset K$ is a set such that $d\mathcal{I} \subset R$ is an integral ideal for some $d \in R$. The product ideal $\mathcal{I}\mathcal{J}$ is the set of all finite sums of terms ab for $a \in \mathcal{I}$, $b \in \mathcal{J}$. Multiplication extends to fractional ideal in an obvious way, and the set of fractional ideals forms a group under multiplication; in particular, every fractional ideal $\mathcal{I}$ has a (multiplicative) inverse ideal, written $\mathcal{I}^{-1}$. The norm of an ideal $\mathcal{I}$ is its index as a subgroup of R, i.e. $N(\mathcal{I}) = |R/\mathcal{I}|$. We have $N(\mathcal{I}\mathcal{J}) = N(\mathcal{I})\cdot N(\mathcal{J})$.

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 $\mathbf{h}_{j+s_2} = \frac{\sqrt{2}\mathbf{i}}{2}(\mathbf{e}_j - \mathbf{e}_{j+s_2})$, where $\mathbf{e}_j \in \mathbb{C}^n$ is the vector with 1 in its j-th coordinate and 0 elsewhere, i is the imaginary number such that $i^2 = -1$. The set $\{\mathbf{h}_j\}_{j\in[n]}$ forms an orthonormal basis of $\mathbb{H}$ as a real vector space. Let $U_H = [\mathbf{h}_1, \mathbf{h}_2, \cdots, \mathbf{h}_n]^\dagger$, we can easily get a field isomorphic $\sigma_H : \mathbb{H} \mapsto \mathbb{R}^n$ where $\sigma_H(\mathbf{x}) = U_H \cdot \mathbf{x}$. 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 $K := \mathbb{Q}(\xi)$ 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 $x \in K$, $\sigma_H(x) = U_H \cdot \sigma_C(x)$.

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 an obvious way, i.e. by embedding each component of R^d into $\mathbb{H}$ separately. For any $\mathbf{x} \in K^d$, define the ℓ_2 norm as $||\mathbf{s}|| = (\sum_{j=1}^d \sum_{i=1}^n |\sigma_i(x_j)|^2)^{1/2}$. It is well known that the dimension of the 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 $\sigma_H(R)$.

For any integer q, we have the following ideal factorization lemma.

Lemma 1. *Let $K = \mathbb{Q}(\alpha)$ be a number field with degree n, where α is an algebraic integer. Moreover if $\gcd(q, [R : \mathbb{Z}[\alpha]]) = 1$, then we have prime ideal decomposition $qR = \prod_{i,j} \mathfrak{p}_{i,j}^{r_{i,j}}$ and $qR^\vee = \prod_{i,j} \mathfrak{p}_{i,j}^{r_{i,j}} R^\vee$.*

Lemma 2 *(Chinese Remainder Theorem [5]). Let $\mathcal{I}$ be a fractional ideal over K, and let $\mathfrak{p}_i$ be pairwise coprime ideals in R, then natural ring homomorphism is an isomorphism: $\mathcal{I}/(\prod_i \mathfrak{p}_i)\mathcal{I} \mapsto \bigoplus_i (\mathcal{I}/\mathfrak{p}_i\mathcal{I})$.*

The following lemma first appeared in [24] and was generalized by Liu et al. in [21] recently. This lemma is the key to prove the generalized leftover hash lemma.

Lemma 3. *Let R be the ring of integers of a number field K, $\mathcal{I}$ be an ideal of R, and $\mathbf{s} = (s_1, \cdots, s_d) \in (R^\vee/\mathcal{I}R^\vee)^d$ be a vector of ring elements. If $\mathbf{a} = (a_1, \cdots, a_d) \in (R/\mathcal{I})^d$ are uniformly random, then $\sum_i a_i \cdot s_i \bmod \mathcal{I}R^\vee$ is uniformly random over the ideal $\langle s_1, \cdots, s_d\rangle/\mathcal{I}R^\vee$. In particular, $\Pr[\sum_i a_i \cdot s_i = 0 \bmod \mathcal{I}R^\vee] = 1/|\langle s_1, \cdots, s_d\rangle/\mathcal{I}R^\vee|$.*

We recall the notion of *maximal belongs* for the vector $\mathbf{s} \in (R^\vee)^d$ in the following, which was first introduced in [21].

Definition 1. Let R be the ring of integers of a number field K, $\mathcal{I}$ be an ideal of R and $R^\vee$ be the dual of R. We say a vector $\mathbf{s} \in (R^\vee)^d$ maximal belongs to a factor $\mathcal{I}$ of qR, abbreviated as $\mathbf{s} \in_{\max} \mathcal{I}R^\vee$, if the following conditions hold:

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

Liu et al. [21] also proved that any possible $\mathbf{s}$ in the range must maximal belong to $\mathcal{J}R^\vee$ for only one ideal factor $\mathcal{J}|qR$, which means $\{\mathbf{s} \in \mathcal{J}R^\vee\}_{\mathcal{J}|qR}$ forms a partition.

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 D, we write $s \leftarrow D$. Also, let $\mathbf{s} = (s_1, \cdots, s_m)^{\mathrm{T}} \leftarrow D^d$ denote the act of sampling each component s_i according to D independently. We also write $\mathrm{Supp}(D)$ to mean the support of the distribution 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 2 *(Statistical distance).* Let X and Y be two discrete probability distributions on a discrete domain $\mathcal{E}$. Their statistical distance is defined as

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

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

Definition 3 *(Min-entropy).* Given a discrete random variable X over $\mathcal{X}$, the min-entropy of X is denoted by

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

Definition 4 *(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

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

We now state a fundamental property of the conditional min-entropy.

Lemma 4 *(Lemma 2.2 in [13]). Let X, Y, Z be random variables, and Y has at most 2^λ possible values, then*

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

Gaussian measures The Gaussian function of parameter α and centre c is defined as $\rho_{\alpha,c}(x) = \exp(-\pi(x-c)^2/\alpha^2)$, and the Gaussian distribution $D_{\alpha,c}$ is the probability distribution whose probability density function is given by $\frac{1}{\alpha}\rho_{\alpha,c}$.

Similarly, for multivariate case, we have the following formal definition. A matrix $\Sigma \in \mathbb{R}^{n\times n}$ is called positive definite, if it holds for every $\mathbf{x} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$ that $\mathbf{x}^T\Sigma\mathbf{x} > 0$. For every positive definite matrix Σ there exists a unique positive definite matrix $\sqrt{\Sigma}$ such that $(\sqrt{\Sigma})^2 = \Sigma$.

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

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

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

Notice that the matrix Σ differs from the standard covariance matrix by a factor of 2π. However, for convenience, we refer to Σ 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 $\Sigma_{ij} = (\alpha_i)^2\delta_{ij}$ and let $\boldsymbol{\alpha} = (\alpha_1, \cdots, \alpha_n)^T$. Then we would write $D_{\boldsymbol{\alpha}}$ to denote the centred Gaussian distribution D_Σ. Furthermore, if $\alpha_1 = \cdots = \alpha_n = \alpha$, we would write D_α 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 $\Sigma \in \mathbb{R}^{n\times n}$ be a positive definite matrix, a sample from D_Σ on $\mathbb{H}$ is given by $\sum_{i\in[n]} x_i\mathbf{h}_i$, where $\mathbf{x} = (x_1, \cdots, x_n)^T \leftarrow D_\Sigma$ over $\mathbb{R}^n$.

We also have discrete Gaussian distributions i.e. normalized distributions defined over some discrete set (typically lattice or lattice coset). The notation for a discrete Gaussian distribution over some n-dimensional lattice Λ and coset vector $\mathbf{u} \in \mathbb{R}^n$ with parameter α is $D_{\Lambda+\mathbf{u},\alpha}$. This distribution has probability mass function $\frac{\rho_\alpha(\mathbf{y})}{\rho_\alpha(\Lambda+\mathbf{u})}$, where $\rho_\alpha(\Lambda+\mathbf{u}) = \sum_{\mathbf{x}\in\Lambda+\mathbf{u}} \rho_\alpha(\mathbf{x})$. For the ring of integers R of a number field K and any $x \in K$, we define $D_{R+x,\alpha}$ 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 $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\Lambda)$ is defined as the smallest $\alpha > 0$ s.t. $\rho_{1/\alpha}(\Lambda^* \setminus \{0\}) \leq \epsilon$.

Lemma 5 *(Lemma 3.1 in [15]). For any $\epsilon > 0$ and n-dimensional lattice Λ with basis B,*

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

Lemma 6 *(Lemma 2.9 in [26]). For any lattice Λ, positive real $\alpha > 0$ and vector $\mathbf{c}$, $\rho_{\alpha,\mathbf{c}}(\Lambda) \leq \rho_\alpha(\Lambda)$.*

Lemma 7 *(Lemma 2.5 in [9]). Let $\alpha_2 > \alpha_1 > 0$. Then it holds for all $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{t} \in \mathbb{R}^n$ that*

$$\rho_{\alpha_1}(\mathbf{x}-\mathbf{t}) \leq \exp\left(\pi\frac{||\mathbf{t}||^2}{\alpha_2^2-\alpha_1^2}\right)\cdot\rho_{\alpha_2}(\mathbf{x}).$$

Moreover, the same holds for the q-periodic Gaussian function, i.e.

$$\rho_{\alpha_1}(\mathbf{x}-\mathbf{t}+q\mathbb{Z}^n) \le \exp\left(\pi\frac{||\mathbf{t}||^2}{\alpha_2^2-\alpha_1^2}\right)\cdot\rho_{\alpha_2}(\mathbf{x}+q\mathbb{Z}^n).$$

Subgaussian Subgaussian distributions are those on $\mathbb{R}$ which have tail dominated by Gaussians [32]. An equivalent formulation is through the moment-generating function of the distribution, this definition is commonly used throughout lattice-based cryptography [25].

Definition 7. A real random variable X is subgaussian with parameter $\alpha \ge 0$ if for all $\beta \in \mathbb{R}$, $E\left(e^{2\pi\beta X}\right) \le e^{\pi\alpha^2\beta^2}$. More generally, we say that a random vector $\mathbf{x} \in \mathbb{R}^n$ is subgaussian with parameter $\alpha \ge 0$ if for all unit vectors $\mathbf{u} \in \mathbb{R}^n$, the random variable $\langle \mathbf{x}, \mathbf{u}\rangle$ is subgaussian with parameter α.

The subgaussian distribution admits the following properties.

Lemma 8 *(Theorem 4.4.5 in [33]). Let $X \in \mathbb{R}^{m\times d}$ be a random matrix with entries drawn independently from a subgaussian distribution with parameter $\alpha \le 0$. Then, there exists some universal constant $C_0 \ge 0$ such that for any $t \ge 0$, with probability at least $1-2e^{-t^2}$ we have $s_1(X) \le C_0\cdot\alpha\cdot(\sqrt{m}+\sqrt{d}+t)$.*

Lemma 9 *(Adapted Lemma 2.8 in [25]). Let $\Lambda \subset \mathbb{R}^n$ be a lattice, then for any $\alpha > 0$, $D_{\Lambda,\alpha}$ is subgaussian with parameter α.*

Noise lossiness The *noise lossiness* of a distribution S measures how information is lost about a sample of S when adding Gaussian noise. It is defined to be the conditional smooth min-entropy of a sample from S conditioned on learning its perturbation by Gaussian noise. This notion was proposed by [9] first.

Definition 8 *(Noise Lossiness).* Let S be a secret distribution over $(R_q^\vee)^d$ and $\mathbf{e} \leftarrow (D_\alpha)^d$ be a gaussian noise. We define the noise-lossiness $\nu_\alpha(S)$ by

$$\nu_\alpha(S) = \widetilde{H}_\infty(\mathbf{s} \mid \mathbf{s}+\mathbf{e} \bmod qR^\vee)$$

where $\mathbf{s} \leftarrow S$.

Lemma 10 *(Adapted from Lemma 5.1 in [9]). Let $\mathbf{s}$ be a random variable over $(R_q^\vee)^d$ with min-entropy $\widetilde{H}_\infty(\mathbf{s})$ and $\mathbf{e} \leftarrow (D_\alpha)^d$. Then it holds that*

$$\nu_\alpha(S) \ge \widetilde{H}_\infty(\mathbf{s}) - \log\left[\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y}-\mathbf{s}^*)d\mathbf{y}\right].$$

Proof. According to calculations, we have

$$\begin{aligned}
\nu_\alpha(S) &= -\log(E_{\mathbf{y}}[\max_{\mathbf{s}^*}\Pr[\mathbf{s}=\mathbf{s}^* \mid \mathbf{s}+\mathbf{e}=\mathbf{y}]]) \\
&= -\log\left(\int_{(\mathbb{T}_{qR^\vee})^d} P_{\mathbf{s}+\mathbf{e}}(\mathbf{y})\cdot\max_{\mathbf{s}^*}\Pr[\mathbf{s}=\mathbf{s}^* \mid \mathbf{s}+\mathbf{e}=\mathbf{y}]d\mathbf{y}\right) \\
&= -\log\left(\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{s},\mathbf{s}+\mathbf{e}}(\mathbf{s}^*,\mathbf{y})d\mathbf{y}\right) \\
&= -\log\left(\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{s}+\mathbf{e}|\mathbf{s}=\mathbf{s}^*}(\mathbf{y})\cdot\Pr[\mathbf{s}=\mathbf{s}^*]d\mathbf{y}\right) \\
&\ge -\log\left(\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{s}+\mathbf{e}|\mathbf{s}=\mathbf{s}^*}(\mathbf{y})\cdot 2^{-\widetilde{H}_\infty(\mathbf{s})}d\mathbf{y}\right) \\
&= \widetilde{H}_\infty(\mathbf{s}) - \log\left[\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y}-\mathbf{s}^*)d\mathbf{y}\right]. \quad \square
\end{aligned}$$

2.3. Module-LWE

The module variant of LWE was first introduced by Brakerski et al. [10], and thoroughly studied by Langlois and Stehlé [20]. The search version problem MLWE(K,d,q,m,χ) is to find $\mathbf{s}\in(R_q^\vee)^d$ given $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$, where $A\leftarrow U((R_q)^{m\times d})$, $\mathbf{s}\leftarrow U((R_q^\vee)^d)$ and $\mathbf{e}\leftarrow\chi^m$. The decisional version problem DMLWE(K,d,q,m,χ) asks to distinguish between the distributions $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$ and $(A,\mathbf{u})$, where A, $\mathbf{s}$ and $\mathbf{e}$ are as in the search version and $\mathbf{u}\leftarrow U((\mathbb{T}_{R^\vee})^m)$. As pointed out by Lyubashevsky et al. [23], 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. [20] showed that DMLWE$(K,d,q,m,D_{R^\vee,\sqrt{2}\alpha})$ is at least as hard as DMLWE(K,d,q,m,D_α) using discretization technique.

Furthermore, Roşca et al. also considered primal form Ring-LWE in [30]. The primal-DRLWE$(K,q,m,D_{R,\alpha})$ problem asks to distinguish between the distributions $(\mathbf{a},\mathbf{a}\cdot\mathbf{s}+\mathbf{e} \bmod qR)$ and $(\mathbf{a},\mathbf{u})$, where $\mathbf{a}\leftarrow U((R_q)^{m\times 1})$, $\mathbf{s}\leftarrow U(R_q)$, $\mathbf{e}\leftarrow(D_{R,\alpha})^m$ and $\mathbf{u}\leftarrow U((R_q)^m)$. In [30] Roşca et al. showed a reduction from Ring-LWE to primal-Ring-LWE with a limited error growth. Later, in [34] 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-Module-LWE. The primal-DMLWE$(K,d,q,m,D_{R,\alpha})$ problem asks to distinguish between the distributions $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR)$ and $(A,\mathbf{u})$, where $A\leftarrow U((R_q)^{m\times d})$, $\mathbf{s}\leftarrow U((R_q)^d)$, $\mathbf{e}\leftarrow(D_{R,\alpha})^m$ and $\mathbf{u}\leftarrow U((R_q)^m)$. By the same way, we can also get the reduction from Module-LWE to primal-Module-LWE.

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

3. Probability lemmas

In this section, we present three results in the probability theory.

1. First, we give a decomposition theorem for Continuous Gaussian on $K_{\mathbb{R}}$ in Section 3.1, which is a generalization of Proposition 3.2 in [9]. This theorem is the key to adapt the proof of the hardness of Entropy LWE to the module setting.
2. Then, we compute the noise lossiness for high-entropy distributions on $K_{\mathbb{R}}$ in Section 3.2. Similar to [9], we will consider two cases: one is for general high-entropy distribution and the other is for bounded high-entropy distribution. We will show that considerable improvements can be achieved when considering bounded case.
3. Finally, we give a generalized leftover hash lemma over rings in Section 3.3. The proof of our leftover hash lemma follows the framework from [21], but has some differences. This theorem will be used to prove the hardness of the decision Entropic Module-LWE problem.

3.1. Gaussian decomposition

In this subsection, we present a new decomposition theorem for continuous Gaussian distribution on $K_{\mathbb{R}}$. Specifically, we show there exists an efficient sampling algorithm $D(F,\alpha,\alpha')$, such that the random variable $\mathbf{e}=F\mathbf{e}_1+\mathbf{e}_2$ follows Gaussian distribution $(D_\alpha(K_{\mathbb{R}}))^m$, where $\mathbf{e}_1\leftarrow(D_{\alpha'}(K_{\mathbb{R}}))^d$, $\mathbf{e}_2\leftarrow D(F,\alpha,\alpha')$ and $F\leftarrow D_{R,\beta}^{m\times d}$.

Assume field K has exactly s_1 real embeddings and s_2 pairs complex embeddings. For any matrix $F=(f_{ij})\in R^{m\times d}$ and any $j\in[s_1]$, we set[1]

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

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

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

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

We are interested in the spectral norm of F^j when $F\leftarrow D_{R,\beta}^{m\times d}$ and give an upper bound in the following lemma.

[1] Here d could be 1, and in this case F would be a vector.

Lemma 11. *Let $F \leftarrow D_{R,\beta}^{m\times d}$, assume for convenience that $m \geq d$. Then with all but 2^{-m} probability it holds that $s_1(F^j) \leq c\beta\sqrt{m}$ for all $j \in [n]$, where c is a global constant.*

Proof. In order to show $s_1(F^j) \leq c\beta\sqrt{m}$, we only need to show that F^j is a random matrix with entries drawn independently from a subgaussian distribution, and then apply Lemma 8. Recall that $F \leftarrow D_{R,\beta}^{m\times d}$ means samples each component f_{kl} according to $D_{R,\beta}$ independently, and $f_{kl} \leftarrow D_{R,\beta}$ means $\sigma_H(f_{kl}) \leftarrow D_{\sigma_H(R),\beta}$, 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, for any $j \in [n]$, the entries of F^j are sampled from the same distribution independently.

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

Thus for any $j \in [n]$, F^j is a random matrix with entries drawn independently from a subgaussian distribution with parameter β. Therefore, by Lemma 8 and set $t = \sqrt{m}$, $c = 3C_0$, we have $s_1(F^j) \leq c\beta\sqrt{m}$ with probability at least $1 - 2e^{-m}$. Finally, we take a union bound over all j and get

$$\Pr[\exists j \in [n] : s_1(F^j) \geq c\beta\sqrt{m})] \leq n \cdot 2e^{-m} \leq 2^{-m}. \quad \square$$

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

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

Theorem 3. *Let $F \in R^{m\times d}$ be a matrix with $s_1(F^j) \leq B$ for any $j \in [n]$. Let $\alpha, \alpha' > 0$ be positive real numbers with $\alpha > \sqrt{2}B \cdot \alpha'$. Let $\mathbf{e}_1 \leftarrow (D_{\alpha'}(K_{\mathbb{R}}))^d$ and $\mathbf{e}_2$ be the random variable in $(K_{\mathbb{R}})^m$ obtained in the following way: for $j \in [s_1]$, set $\mathbf{e}_2^j \leftarrow D_{\sqrt{\Sigma_j}}$ where $\Sigma_j = \alpha^2 I_m - \alpha'^2 F^j (F^j)^{\mathrm{T}}$; for $j \in \{s_1 + 1, \cdots, s_1 + s_2\}$, set $((\mathbf{e}_2^j)^{\mathrm{T}}, (\mathbf{e}_2^{j+s_2})^{\mathrm{T}}) \leftarrow D_{\sqrt{\Sigma_j}}$ where $\Sigma_j = \alpha^2 I_{2m} - \alpha'^2 \widetilde{F}^j (\widetilde{F}^j)^{\mathrm{T}}$. Then the random variable $\mathbf{e} = F\mathbf{e}_1 + \mathbf{e}_2$ follows distribution according to $(D_\alpha(K_{\mathbb{R}}))^m$.*

Proof. We first prove that Σ_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

$$\mathbf{x}^{\mathrm{T}}\Sigma_j\mathbf{x} \geq \alpha^2\|\mathbf{x}\|_2^2 - \alpha'^2 \cdot s_1(F^j)^2\|\mathbf{x}\|_2^2 \geq (\alpha^2 - \alpha'^2 B^2) \cdot \|\mathbf{x}\|_2^2 > 0,$$

as $\alpha \geq \sqrt{2}B \cdot \alpha'$ and $s_1(F^j) = s_1((F^j)^{\mathrm{T}})$.

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

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

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

$$\mathbf{x}^{\mathrm{T}}\Sigma_j\mathbf{x} \geq \alpha^2\|\mathbf{x}\|_2^2 - \alpha'^2 \cdot 2B^2\|\mathbf{x}\|_2^2 > 0.$$

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 $\sigma_H(e_{2i})$ respectively, 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 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

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

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

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

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

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

$$E(\mathbf{e}^j(\mathbf{e}^j)^{\mathrm{T}}) = E(F^j \mathbf{e}_1^j (\mathbf{e}_1^j)^{\mathrm{T}} (F^j)^{\mathrm{T}}) + E(\mathbf{e}_2^j (\mathbf{e}_2^j)^{\mathrm{T}}) = \qquad \alpha'^2 F^j (F^j)^{\mathrm{T}} + \Sigma_j = \alpha^2 I_m.$$

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:

$$E\left[\begin{pmatrix} \mathbf{e}^j \\ \mathbf{e}^{j+s_2} \end{pmatrix} \cdot ((\mathbf{e}^j)^{\mathrm{T}}, (\mathbf{e}^{j+s_2})^{\mathrm{T}})\right] = \alpha'^2 \widetilde{F}^j (\widetilde{F}^j)^{\mathrm{T}} + \Sigma_j = \alpha^2 I_{2m}.$$

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

Remark 1. We find that Brakerski et al. also provided a blockwise Gaussian decomposition theorem (Lemma 5.4) in [35]. Since multiplication over a ring can be converted into multiplication between a matrix and a vector, their result can be regarded as a special case of our result when $d = 1$.

Combining Theorem 3 and Lemma 11, we obtain the following corollary.

Corollary 1. *Let K be a number field with degree n, R be the ring of integers of K. Let $F \leftarrow D_{R,\beta}^{m \times d}$, assume for convenience that $m > d$. Let $\alpha, \alpha' > 0$ with $\alpha > \sqrt{2}c\beta\sqrt{m}\alpha'$. Let $\mathbf{e}_1 \leftarrow (D_{\alpha'}(K_{\mathbb{R}}))^d$ be the random variable in $(K_{\mathbb{R}})^d$. Then with all but 2^{-m} probability there exists an efficient sampling algorithm $D(F, \alpha, \alpha')$, such that the random variable $\mathbf{e} = F\mathbf{e}_1 + \mathbf{e}_2$ is distribution according to $(D_\alpha(K_{\mathbb{R}}))^m$, where $\mathbf{e}_2 \leftarrow D(F, \alpha, \alpha')$.*

3.2. Gaussian noise lossiness

In this subsection, we compute the Gaussian noise lossiness high-entropy distributions over $K_{\mathbb{R}}$. Similar to [9], we will consider two cases: one is general high-entropy distribution and the other is bounded high-entropy distribution. Thanks for Lemma 10, we only need to bound

$$\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y}$$

in the following.

General high entropy secrets In order to get noise lossiness result in general high entropy case, we establish the following lemma first.

Lemma 12. *Let B_R be some known basis of R in $\mathbb{H}$, d, q be integers and α be a parameter for Gaussian with*

$$\frac{q}{\alpha} \geq \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}},$$

then it holds for all $\mathbf{x} \in (K_{\mathbb{R}})^d$ that $\rho_\alpha(\mathbf{x} + (qR^\vee)^d) \leq 2$.

Proof. Since B_R is a basis of R in $\mathbb{H}$, we have $B_{R^d} = I_d \otimes B_R$ is a basis of R^d in $\mathbb{H}^d$. Orthogonalizing from left to right, we can see that $\|\widetilde{B}_{R^d}\|$ is precisely $\|\widetilde{B}_R\|$. By Lemma 5 and set $\epsilon = 1$, we have $\frac{1}{\alpha} \geq \eta_1((\frac{1}{q}R)^d)$. By definition, we obtain $\rho_\alpha((qR^\vee)^d \setminus \{0\}) \leq 1$. Thus, we have $\rho_\alpha((qR^\vee)^d) \leq 2$. And by Lemma 6, we get

$$\rho_\alpha(\mathbf{x} + (qR^\vee)^d) = \rho_{\alpha,\mathbf{x}}((qR^\vee)^d) \leq \rho_\alpha((qR^\vee)^d) \leq 2. \quad \square$$

Now we bound $\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y}$ in the following lemma.

Lemma 13. *Let B_R be some known basis of R in $\mathbb{H}$, d, q be integers and α be a parameter for gaussian with $\frac{q}{\alpha} \geq \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$, then we have*

$$\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y} \leq 2 \cdot \left(\frac{q}{\alpha}\right)^{nd} \cdot \left(\frac{1}{\Delta_K}\right)^{\frac{d}{2}}.$$

Proof. Since $\frac{q}{\alpha} \geq \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$, by Lemma 12, we have $\rho_\alpha(\mathbf{x} + (qR^\vee)^d) \leq 2$. Thus, we have

$$\begin{aligned}
&\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y} \\
=&\frac{1}{\rho_\alpha(\mathbb{R}^{nd})} \int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} \rho_\alpha(\mathbf{y} - \mathbf{s}^* + (qR^\vee)^d) d\mathbf{y} \\
\leq&\frac{1}{\alpha^{nd}} \cdot \int_{(\mathbb{T}_{qR^\vee})^d} 2 d\mathbf{y} = 2 \cdot \left(\frac{q}{\alpha}\right)^{nd} \cdot \left(\frac{1}{\Delta_K}\right)^{\frac{d}{2}}. \quad \square
\end{aligned}$$

By combining Lemma 10 and Lemma 13, we can get the following corollary, which bounds noise lossiness by min-entropy.

Corollary 2 *(General high entropy). Let R be the ring of integers of a field K with degree n, $R^\vee$ be the dual of R and B_R be some known basis of R in $\mathbb{H}$. Let d, q be integers and α be a parameter for gaussian with $\frac{q}{\alpha} \geq \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ then it holds that*

$$\nu_\alpha(\mathbf{s}) \geq \widetilde{H}_\infty(\mathbf{s}) + \frac{d}{2}\log(\Delta_K) - nd\log\left(\frac{q}{\alpha}\right) - 1.$$

Bounded norm secrets We now turn to the case that the secret has bounded norm. We show that considerable improvements can be achieved in this case. We also bound $\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y}$ first.

Lemma 14. *Let d, q be integers and α be a parameter for Gaussian. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ which satisfies $||\mathbf{s}|| \leq M$. Then it holds that*

$$\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y} \leq \exp\left(\sqrt{2\pi nd} \cdot \frac{M}{\alpha}\right).$$

Proof. By Lemma 7, for some $\tilde{\alpha} > \alpha$, we have

$$\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y}$$

$$
\begin{aligned}
&= \frac{1}{\rho_\alpha(\mathbb{R}^{nd})} \int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} \rho_\alpha(\mathbf{y} - \mathbf{s}^* + (qR^\vee)^d) d\mathbf{y} \\
&\le \frac{1}{\rho_\alpha(\mathbb{R}^{nd})} \int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} \exp\left(\pi \frac{||\mathbf{s}^*||^2}{\tilde{\alpha}^2 - \alpha^2}\right) \cdot \rho_{\tilde{\alpha}}(\mathbf{y} + (qR^\vee)^d) d\mathbf{y} \\
&\le \frac{1}{\rho_\alpha(\mathbb{R}^{nd})} \cdot \exp\left(\pi \frac{M^2}{\tilde{\alpha}^2 - \alpha^2}\right) \int_{(\mathbb{T}_{qR^\vee})^d} \rho_{\tilde{\alpha}}(\mathbf{y} + (qR^\vee)^d) d\mathbf{y} \\
&= \frac{\rho_{\tilde{\alpha}}(\mathbb{R}^{nd})}{\rho_\alpha(\mathbb{R}^{nd})} \cdot \exp\left(\pi \frac{M^2}{\tilde{\alpha}^2 - \alpha^2}\right) \\
&= \left(\frac{\tilde{\alpha}}{\alpha}\right)^{nd} \cdot \exp\left(\pi \frac{M^2}{\tilde{\alpha}^2 - \alpha^2}\right).
\end{aligned}
$$

In particular, let $\tilde{\alpha} = \alpha \cdot \sqrt{1+\eta}$ where $\eta = \sqrt{\frac{2\pi}{nd}} \frac{M}{\alpha}$, we have

$$
\begin{aligned}
&\int_{(\mathbb{T}_{qR^\vee})^d} \max_{\mathbf{s}^*} P_{\mathbf{e}}(\mathbf{y} - \mathbf{s}^*) d\mathbf{y} \le (1+\eta)^{\frac{nd}{2}} \cdot \exp\left(\pi \frac{M^2}{\eta \alpha^2}\right) \\
&\le \exp\left(\pi \frac{M^2}{\eta \alpha^2} + \frac{nd\eta}{2}\right) = \exp\left(\sqrt{2\pi nd} \cdot \frac{M}{\alpha}\right). \quad \square
\end{aligned}
$$

By combining Lemma 10 and Lemma 14, we can get the following corollary.

Corollary 3 *(Bounded norm). Let R be the ring of integers of a field K with degree n, $R^\vee$ be the dual of R. Let d, q be integers and α be a parameter for Gaussian. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ which satisfies $||\mathbf{s}|| \le M$. Then it holds that $v_\alpha(\mathbf{s}) \ge \widetilde{H}_\infty(\mathbf{s}) - \sqrt{2\pi nd} \cdot \frac{M}{\alpha} \log(e)$.*

3.3. Leftover hash lemma

Here we show a generalized leftover hash lemma over R_q. We are interested in the case where the noise lossiness of secrets is leaked. Following the framework from [21], we prove a new generalized leftover hash lemma.

In this subsection, all operations are performed on $R_q^\vee$ (i.e. whenever dealing with all operations, they are involved end with a modulo $qR^\vee$ operation), unless stated otherwise. Let $\mathcal{S}$ denote a secret distribution defined on $(R_q^\vee)^d$. For simplicity, we denote distribution $\mathcal{G}$ as

$$\mathcal{G} = \{(C, \mathbf{x}, \mathbf{z}) \,|C \leftarrow U(R_q^{k \times d}), \mathbf{x} = C\mathbf{s}, \mathbf{z} = \mathbf{s} + \mathbf{e} \text{ for } \mathbf{s} \leftarrow \mathcal{S}, \mathbf{e} \leftarrow \chi\},$$

and denote $\mathcal{G}_{\mathbf{z}}$ as the conditional distribution of $(C, \mathbf{x})$ given $\mathbf{z} = \mathbf{s} + \mathbf{e}$.

Similarly, we denote distribution $\mathcal{U}$ as

$$\mathcal{U} = \{(C, \mathbf{x}, \mathbf{z}) \,|C \leftarrow U(R_q^{k \times d}), \mathbf{x} \leftarrow U((R_q^\vee)^k), \mathbf{z} = \mathbf{s} + \mathbf{e} \text{ for } \mathbf{s} \leftarrow \mathcal{S}, \mathbf{e} \leftarrow \chi\},$$

and denote $\mathcal{U}_{\mathbf{z}}$ as the conditional distribution of $(C, \mathbf{x})$ given $\mathbf{z} = \mathbf{s} + \mathbf{e}$. Note that, $\mathcal{U}_{\mathbf{z}}$ is uniform distribution over $R_q^{k \times d} \times (R_q^\vee)^d$. For any distribution D, the collision probability, denoted by $\mathrm{Col}(D)$, represents the probability that two independently sampled samples following (D) are equal.

Our new leftover hash lemma demonstrates that when $\mathcal{S}$ satisfies specific entropy conditions, the statistical distance between $\mathcal{G}$ and $\mathcal{U}$ is negligible. Depending on the splitting of qR, we can attain varying entropy conditions. When qR is low-splitting (meaning it splits into fewer but larger ideals), we are able to achieve smaller parameters. The proof of this lemma starts by constraining the statistical distance between $\mathcal{G}$ and $\mathcal{U}$ with a collision probability. Subsequently, we show that when the entropy of $\mathcal{S}$ is sufficiently high, this collision probability becomes quite small. Now we prove our leftover hash lemma as follows.

Theorem 4. *Let $K = \mathbb{Q}(\xi)$ be a number field with degree n, where ξ is an algebraic integer. Let R be the ring of integers of K and $R^\vee$ be the dual of R. Let q, d, k be positive integers with $d > k$ and $\gcd(q, [R : \mathbb{Z}[\xi]]) = 1$. Let $\mathcal{S}$ be a secret distribution defined on $(R_q^\vee)^d$, χ be a noise distribution over $(K_{\mathbb{R}})^d$ and let $\mathbf{e} \leftarrow \chi$, then we have*

$$\Delta(\mathcal{G}, \mathcal{U}) \le \frac{1}{2} \sqrt{\sum_{\mathcal{J} | qR, \mathcal{J} \ne R} (N(\mathcal{J}))^k \cdot \int_{\mathbf{z}} P_{\mathbf{s}+\mathbf{e}}(\mathbf{z}) \cdot \mathrm{Col}(S_{\mathcal{J}} | \mathbf{z}) d\mathbf{z}},$$

where $\mathrm{Col}(S_{\mathcal{J}} | \mathbf{z})$ is the collision probability of

$$\mathcal{S}_{\mathcal{J}R^\vee} = \{\mathbf{s} \bmod \mathcal{J}R^\vee \mid \mathbf{s} \leftarrow \mathcal{S}\} \text{ given } \mathbf{z} = \mathbf{s} + \mathbf{e}.$$

Proof. By definition, we need to bound $\Delta(\mathcal{G}, \mathcal{U})$. To do this, we first derive an upper bound on the statistical distance between $\mathcal{G}$ and $\mathcal{U}$ in terms of the conditional collision probability $\mathrm{Col}(\mathcal{G}|\mathbf{z})$, where $\mathrm{Col}(\mathcal{G}|\mathbf{z})$ is the collision probability of $\mathcal{G}_{\mathbf{z}}$.

$$\begin{aligned}
\Delta(\mathcal{G}, \mathcal{U}) =& \frac{1}{2} \int_{\mathbf{z}} P_{\mathbf{s}+\mathbf{e}}(\mathbf{z}) \cdot \sum_{(C,\mathbf{x})} |\Pr[(C,\mathbf{x}) \leftarrow \mathcal{G}_{\mathbf{z}}] - \Pr[(C,\mathbf{x}) \leftarrow \mathcal{U}_{\mathbf{z}}]| d\mathbf{z} \\
\le& \frac{1}{2} \int_{\mathbf{z}} P_{\mathbf{s}+\mathbf{e}}(\mathbf{z}) \cdot q^{\frac{nk(d+1)}{2}} \cdot \sqrt{\sum_{(C,\mathbf{x})} (\Pr[(C,\mathbf{x}) \leftarrow \mathcal{G}_{\mathbf{z}}] - \Pr[(C,\mathbf{x}) \leftarrow \mathcal{U}_{\mathbf{z}}])^2} d\mathbf{z} \\
=& \frac{1}{2} \int_{\mathbf{z}} P_{\mathbf{s}+\mathbf{e}}(\mathbf{z}) \cdot \sqrt{q^{nk(d+1)} \cdot \mathrm{Col}(\mathcal{G}|\mathbf{z}) - 1} d\mathbf{z}.
\end{aligned} \tag{1}$$

Next we bound $\mathrm{Col}(\mathcal{G}|\mathbf{z})$ as follows, where probabilities run through two independently copies of $(C, C\mathbf{s}), (C', C'\mathbf{s}') \leftarrow \mathcal{G}_{\mathbf{z}}$.

$$\begin{aligned}
\mathrm{Col}(\mathcal{G}|\mathbf{z}) &= \Pr[(C = C') \wedge (C\mathbf{s} = C'\mathbf{s}') \mid \mathbf{s} + \mathbf{e} = \mathbf{s}' + \mathbf{e}' = \mathbf{z}] \\
&= \frac{1}{q^{ndk}} \cdot \Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \mathbf{s} + \mathbf{e} = \mathbf{s}' + \mathbf{e}' = \mathbf{z}].
\end{aligned} \tag{2}$$

Now we further bound the probability

$$\Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \mathbf{s} + \mathbf{e} = \mathbf{s}' + \mathbf{e}' = \mathbf{z}].$$

We denote $\mathrm{Col}(\mathcal{S}_{\mathcal{J}}|\mathbf{z})$ as the collision probability of $\mathcal{S}_{\mathcal{J}R^\vee}$ given $\mathbf{z} = \mathbf{s} + \mathbf{e}$, where $\mathcal{J}$ is an ideal of R. Obviously, we have

$$\begin{aligned}
\mathrm{Col}(\mathcal{S}_{\mathcal{J}}|\mathbf{z}) &= \Pr[\mathbf{s} - \mathbf{s}' \in \mathcal{J}R^\vee \mid \mathbf{s} + \mathbf{e} = \mathbf{s}' + \mathbf{e}' = \mathbf{z}] \\
&\ge \Pr[\mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee \mid \mathbf{s} + \mathbf{e} = \mathbf{s}' + \mathbf{e}' = \mathbf{z}].
\end{aligned}$$

For simplicity, we use $\clubsuit$ to express the condition $\mathbf{s} + \mathbf{e} = \mathbf{s}' + \mathbf{e}' = \mathbf{z}$ in the following. Since $\{\mathbf{s} \in_{\max} \mathcal{J}R^\vee\}_{\mathcal{J}R^\vee | qR^\vee}$ forms a partition, we have:

$$\begin{aligned}
&\Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \clubsuit] \\
=& \sum_{\mathcal{J}R^\vee | qR^\vee} \Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit] \cdot \Pr[\mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee \mid \clubsuit] \\
\le& \sum_{\mathcal{J}R^\vee | qR^\vee} \Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit] \cdot \mathrm{Col}(\mathcal{S}_{\mathcal{J}}|\mathbf{z}).
\end{aligned} \tag{3}$$

Now we compute $\Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit]$. By Lemma 1, we have $qR = \prod_{i,j} \mathfrak{p}_{i,j}^{r_{i,j}}$ and $qR^\vee = \prod_{i,j} \mathfrak{p}_{i,j}^{r_{i,j}} R^\vee$. Without loss of generality, we let $\mathcal{J} = \prod_{i,j} \mathfrak{p}_{i,j}^{r'_{i,j}}$ with $r'_{i,j} \le r_{i,j}$. By Lemma 2, we have

$$\begin{aligned}
R_q &= R/qR \cong \bigoplus_{i,j} R/\mathfrak{p}_{i,j}^{r_{i,j}}, \\
R_q^\vee &= R^\vee/qR^\vee \cong \bigoplus_{i,j} R^\vee/\mathfrak{p}_{i,j}^{r_{i,j}} R^\vee.
\end{aligned}$$

Thus a random ring element in R_q can be viewed as independently random coordinates in $\{R/\mathfrak{p}_{i,j}^{r_{i,j}}\}_{i,j}$. Therefore, we have:

$$\begin{aligned}
&\Pr[C(\mathbf{s} - \mathbf{s}') = 0 \mid \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit] \\
=& \prod_{i,j} \Pr[C(\mathbf{s} - \mathbf{s}') = 0 \bmod \mathfrak{p}_{i,j}^{r_{i,j}} R^\vee \mid \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit] \\
=& \prod_{i,j} \Pr[C_{i,j}(\mathbf{s} - \mathbf{s}')_{i,j} = 0 \bmod \mathfrak{p}_{i,j}^{r_{i,j}} R^\vee | \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit],
\end{aligned} \tag{4}$$

where $C_{i,j} = C \bmod \mathfrak{p}_{i,j}^{r_{i,j}}$ and $(\mathbf{s} - \mathbf{s}')_{i,j} = (\mathbf{s} - \mathbf{s}') \bmod \mathfrak{p}_{i,j}^{r_{i,j}} R^\vee$.

In [21], Liu et al. proved that the ideal generated by the vector $(\mathbf{s} - \mathbf{s}')_{i,j}$ is $\mathfrak{p}_{i,j}^{r'_{i,j}} R^\vee$ in Claim 5.6. Therefore, by Lemma 3, we have

$$\Pr[C_{i,j}(\mathbf{s} - \mathbf{s}')_{i,j} = 0 \bmod \mathfrak{p}_{i,j}^{r_{i,j}} R^\vee \mid \mathbf{s} - \mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit] = \left(\frac{N(\mathfrak{p}_{i,j}^{r'_{i,j}} R^\vee)}{N(\mathfrak{p}_{i,j}^{r_{i,j}} R^\vee)} \right)^k.$$

Thus, we get

$$\prod_{i,j}\Pr[C_{i,j}(\mathbf{s}-\mathbf{s}')_{i,j}=0 \bmod \mathfrak{p}_{i,j}^{r_{i,j}}R^\vee \mid \mathbf{s}-\mathbf{s}' \in_{\max} \mathcal{J}R^\vee, \clubsuit]$$

$$=\prod_{i,j}\left(\frac{N(\mathfrak{p}_{i,j}^{r'_{i,j}}R^\vee)}{N(\mathfrak{p}_{i,j}^{r_{i,j}}R^\vee)}\right)^k=\left(\frac{N(\prod_{i,j}\mathfrak{p}_{i,j}^{r'_{i,j}}R^\vee)}{N(\prod_{i,j}\mathfrak{p}_{i,j}^{r_{i,j}}R^\vee)}\right)^k$$

$$=\left(\frac{N(\mathcal{J}R^\vee)}{N(qR^\vee)}\right)^k=\frac{(N(\mathcal{J}))^k}{q^{nk}}. \tag{5}$$

Combining the facts $N(R)=1$, $\mathrm{Col}(S_R|\mathbf{z})=1$ and Eqs. (1), (2), (3), (4), (5), we have

$$\begin{aligned}\Delta(\mathcal{G},\mathcal{U}')&\le\frac{1}{2}\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\cdot\sqrt{\sum_{\mathcal{J}|qR,\mathcal{J}\neq R}(N(\mathcal{J}))^k\cdot\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})}d\mathbf{z}\\&\le\frac{1}{2}\sqrt{\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\cdot\sum_{\mathcal{J}|qR,\mathcal{J}\neq R}(N(\mathcal{J}))^k\cdot\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})d\mathbf{z}}\\&=\frac{1}{2}\sqrt{\sum_{\mathcal{J}|qR,\mathcal{J}\neq R}(N(\mathcal{J}))^k\cdot\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\cdot\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})d\mathbf{z}}.\quad\square\end{aligned}$$

Now we bound $\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\cdot\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})d\mathbf{z}$ for any ideal $\mathcal{J}$ in the following lemma.

Lemma 15. *Let q,d,k be positive integers with $d>k$. Let S be a secret distribution defined on $(R_q^\vee)^d$ and χ be a noise distribution over $(K_{\mathbb{R}})^d$ and let $\mathbf{e}\leftarrow\chi$, then we have*

$$\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\cdot\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})d\mathbf{z}\le 2^{-\tilde{H}_\infty(S \bmod \mathcal{J}R^\vee)}\cdot\int_{\mathbf{z}}\max_{\mathbf{s}^*}P_{\mathbf{e}}(\mathbf{z}-\mathbf{s}^*)d\mathbf{z}.$$

Proof. Obviously, we have

$$\begin{aligned}\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})&=\sum_{\mathbf{t}\in(R^\vee/\mathcal{J}R^\vee)^d}\left(\Pr[\mathbf{s}=\mathbf{t} \bmod \mathcal{J}R^\vee \mid \mathbf{s}+\mathbf{e}=\mathbf{z}]\right)^2\\&\le\max_{\mathbf{s}^*}\Pr[\mathbf{s}=\mathbf{s}^* \bmod \mathcal{J}R^\vee \mid \mathbf{s}+\mathbf{e}=\mathbf{z}].\end{aligned}$$

Therefore, we have

$$\begin{aligned}&\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\cdot\mathrm{Col}(S_{\mathcal{J}}|\mathbf{z})d\mathbf{z}\\\le&\int_{\mathbf{z}}P_{\mathbf{s}+\mathbf{e}}(\mathbf{z})\max_{\mathbf{s}^*}\Pr[\mathbf{s}=\mathbf{s}^* \bmod \mathcal{J}R^\vee \mid \mathbf{s}+\mathbf{e}=\mathbf{z}]d\mathbf{z}\\=&\int_{\mathbf{z}}\max_{\mathbf{s}^*}P_{(\mathbf{s}+\mathbf{e},\mathbf{s} \bmod \mathcal{J}R^\vee)}(\mathbf{z},\mathbf{s}^*)d\mathbf{z}\\=&\int_{\mathbf{z}}\max_{\mathbf{s}^*}P_{(\mathbf{s}+\mathbf{e}|\mathbf{s}=\mathbf{s}^* \bmod \mathcal{J}R^\vee)}(\mathbf{z})\cdot\Pr[\mathbf{s}=\mathbf{s}^* \bmod \mathcal{J}R^\vee]d\mathbf{z}\\\le&2^{-\tilde{H}_\infty(S \bmod \mathcal{J}R^\vee)}\cdot\int_{\mathbf{z}}\max_{\mathbf{s}^*}P_{(\mathbf{s}+\mathbf{e}|\mathbf{s}=\mathbf{s}^* \bmod \mathcal{J}R^\vee)}(\mathbf{z})d\mathbf{z}\\\le&2^{-\tilde{H}_\infty(S \bmod \mathcal{J}R^\vee)}\cdot\int_{\mathbf{z}}\max_{\mathbf{s}^*}P_{(\mathbf{s}+\mathbf{e}|\mathbf{s}=\mathbf{s}^*)}(\mathbf{z})d\mathbf{z}\\=&2^{-\tilde{H}_\infty(S \bmod \mathcal{J}R^\vee)}\cdot\int_{\mathbf{z}}\max_{\mathbf{s}^*}P_{\mathbf{e}}(\mathbf{z}-\mathbf{s}^*)d\mathbf{z}.\quad\square\end{aligned}$$

From Theorem 4, Lemma 15, Lemma 13 and Lemma 14, we can derive the following lemmas for two cases: one is for the general high-entropy case and the other is for the bounded norm case.

Lemma 16 *(General case). Let K be some number field with degree n, R be the ring of integers of K and $R^\vee$ be the dual of R. Let d, k be positive integers with $d > k$, q be a prime and $\epsilon \in (0,1)$. Let α be a parameter for gaussian with $\frac{q}{\alpha} \geq \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$ and $\mathbf{e} \leftarrow (D_\alpha(K_\mathbb{R}))^d$ be an noise term. Assume that the decomposition of qR can be expressed as $\prod_i \mathfrak{p}_i^{r_i}$, where each $\mathfrak{p}_i$ is a prime ideal over R. Suppose $\mathbf{s}$ is chosen from some distribution $\mathcal{S}$ over $(R_q^\vee)^d$ such that*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \geq 2\log\left(\frac{1}{\epsilon}\right) + nk\log(q+1) + nd\log\left(\frac{q}{\alpha}\right) - \frac{d}{2}\log(\Delta_K) - 1,$$

for any prime ideal $\mathfrak{p}_i$ of qR. Then we have $\Delta(\mathcal{G}, \mathcal{U}^\vee) \leq \epsilon$.

Proof. By combining Lemma 15 and Lemma 13, for any $\mathcal{J}|qR$ we have

$$\int_{\mathbf{z}} p_{\mathbf{z}}(\mathbf{z}) \cdot \mathrm{Col}(S_{\mathcal{J}}|\mathbf{z}) d\mathbf{z} \leq 2\left(\frac{q}{\alpha}\right)^{nd} \cdot \left(\frac{1}{\Delta_K}\right)^{\frac{d}{2}} \cdot 2^{-\tilde{H}_\infty(\mathcal{S} \bmod \mathcal{J}R^\vee)}.$$

Obviously, we have

$$\tilde{H}_\infty(\mathcal{S} \bmod \mathcal{J}R^\vee) \geq \tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee)$$

for any $\mathfrak{p}_i | \mathcal{J}$. Thus, for any $\mathcal{J}|qR$ we have

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathcal{J}R^\vee) \geq 2\log\left(\frac{1}{\epsilon}\right) + nk\log(q+1) + nd\log\left(\frac{q}{\alpha}\right) - \frac{d}{2}\log(\Delta_K) - 1.$$

Since $qR = \prod_i \mathfrak{p}_i^{r_i}$, we have $\prod_i (\mathfrak{p}_i)^{r_i} = N(qR) = q^n$. And since q is a prime, for any i we have $N(\mathfrak{p}_i) \geq q$ and qR has at most n prime ideals. Thus, we have

$$\sum_{\mathcal{J}|qR} (N(\mathcal{J}))^k \leq \sum_{i=0}^{n} \binom{i}{n} q^{ik} = (q^k+1)^n \leq (q+1)^{nk}.$$

Therefore, we have

$$\Delta(\mathcal{G}, \mathcal{U}^\vee) \leq \frac{1}{2}\sqrt{\sum_{\mathcal{J}|qR, \mathcal{J}\neq R} (N(\mathcal{J}))^k \cdot \int_{\mathbf{z}} p_{\mathbf{z}}(\mathbf{z}) \cdot \mathrm{Col}(S_{\mathcal{J}}|\mathbf{z}) d\mathbf{z}} \leq \epsilon. \quad \square$$

Similarly, for the bounded case, we can get the following lemma.

Lemma 17 *(Bounded case). Let K be some number field with degree n, R be the ring of integers of K and $R^\vee$ be the dual of R. Let d, k be positive integers with $d > k$, q be a prime and $\epsilon \in (0,1)$. Let α be a parameter for gaussian and $\mathbf{e} \leftarrow (D_\alpha(K_\mathbb{R}))^d$ be an noise term. Assume that the decomposition of qR can be expressed as $\prod_i \mathfrak{p}_i^{r_i}$, where each $\mathfrak{p}_i$ is a prime ideal over R. Suppose $\mathbf{s}$ is chosen from some M-bounded distribution $\mathcal{S}$ over $(R_q^\vee)^d$ such that*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \geq 2\log(\frac{1}{\epsilon}) + nk\log(q+1) + \sqrt{2\pi nd}\frac{M}{\alpha}\log e - 2$$

for any prime ideal $\mathfrak{p}_i$ of qR. Then we have $\Delta(\mathcal{G}, \mathcal{U}^\vee) \leq \epsilon$.

Proof. Since $\mathcal{S}$ is a distribution bounded by M, by combining Lemma 15 and Lemma 14, for any $\mathcal{J}|qR$ we have

$$\int_{\mathbf{z}} p_{\mathbf{z}}(\mathbf{z}) \cdot \mathrm{Col}(S_{\mathcal{J}}|\mathbf{z}) d\mathbf{z} \leq \exp\left(\sqrt{2\pi nd} \cdot \frac{M}{\alpha}\right) \cdot 2^{-\tilde{H}_\infty(\mathcal{S} \bmod \mathcal{J}R^\vee)}.$$

Obviously, we have $\tilde{H}_\infty(\mathcal{S} \bmod \mathcal{J}R^\vee) \geq \tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee)$ for any $\mathfrak{p}_i | \mathcal{J}$. Thus, for any $\mathcal{J}|qR$ we have

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathcal{J}R^\vee) \geq 2\log(\frac{1}{\epsilon}) + nk\log(q+1) + \sqrt{2\pi nd}\frac{M}{\alpha}\log e - 2.$$

According to the analysis in Lemma 16, we have $\sum_{\mathcal{J}|qR}(N(\mathcal{J}))^k \leq (q+1)^{nk}$. Therefore, we have

$$\Delta(\mathcal{G}, \mathcal{U}^\vee) \leq \frac{1}{2}\sqrt{\sum_{\mathcal{J}|qR, \mathcal{J}\neq R} (N(\mathcal{J}))^k \cdot \int_{\mathbf{z}} p_{\mathbf{z}}(\mathbf{z}) \cdot \mathrm{Col}(S_{\mathcal{J}}|\mathbf{z}) d\mathbf{z}} \leq \epsilon. \quad \square$$

Remark 2. Note that, in the above lemma we can get smaller parameters when qR does not have a small ideal factor. In the most special case where qR is a field, the best parameters will be obtained. However, in this case number theoretic transform (NTT) [31] algorithm cannot be used in this case, the computational efficiency is the worst. On the other hand, when each $N(\mathfrak{p}_i)$ is very small

then the parameters will be undesirable. For example when qR is completely-splitting, then each coordinate of $\mathbf{s} \bmod \mathfrak{p}_i$ can only provide $\log q$ bits of entropy. In this case, d will be very large. From the perspective of efficiency and security, our lemma suggests using an appropriate q (such that qR only has ideals with large norms) in future Module-LWE applications.

4. Entropic module learning with error

In this section, we give a formal definition for the Entropic Module-LWE problem and then adapt the "flooding at the source" approach from [9] to the module setting to get the first result for the hardness of the Entropic Module-LWE problem. In particular, we present an entropy bound that guarantees the hardness of the Entropic Module-LWE problem. We also adapt the counterexample from [5,9] to the module setting to deduce that our entropy bound is essentially tight for general modulus and general min-entropy distributions.

Specifically, in Section 4.1, we show that high noise lossiness implies the hardness of search Entropic Module-LWE problem. Combining with the result in Section 3.2, we get the entropy bound. In Section 4.2, we show that if for every ideal factor $\mathcal{J}|qR$, $\mathbf{s} \bmod \mathcal{J}$ has high entropy, then we can also get the hardness result of decision Entropic Module-LWE. Finally, we show the tightness of the hardness result for the general high entropy setting in Section 4.3. In the following, we give the formal definition for the Entropic Module-LWE first.

Definition 9 *(Entropic Module-LWE).* Let K be some number field with degree n, R be the ring of integers of K and $R^\vee$ be the dual of R. Let q be a modulus, d be a dimension and m be a sample size. Let χ be an error distribution on $K_\mathbb{R}$ and $\mathcal{S}$ be a secret distribution on $(R_q^\vee)^d$. Let EMLWE$(R,d,q,m,\chi,\mathcal{S})$ be a distribution over $(R_q)^{m\times d} \times (\mathbb{T}_{qR^\vee})^m$ obtained by choosing $A \leftarrow U((R_q)^{m\times d})$, $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{e} \leftarrow \chi^m$, and outputting the pair $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$.

We say search Entropic Module-LWE problem SEMLWE$(R,d,q,m,\chi,\mathcal{S})$ is hard, if it holds for every PPT adversary $\mathcal{A}$ that

$$\Pr[\mathcal{A}(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee) = \mathbf{s}] \le \mathrm{negl}(\lambda),$$

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

We say decision Entropic Module-LWE problem DEMLWE$(R,d,q,m,\chi,\mathcal{S})$ is hard, if it holds for every PPT distinguisher $\mathcal{D}$ that

$$|\Pr[\mathcal{D}(A_1,\mathbf{b}_1)=1] - \Pr[\mathcal{D}(A_2,\mathbf{b}_2)=1]| \le \mathrm{negl}(\lambda),$$

where $(A_1,\mathbf{b}_1) \leftarrow$ EMLWE$(R,d,q,m,\chi,\mathcal{S})$ and $(A_2,\mathbf{b}_2) \leftarrow U((R_q)^{m\times d} \times (\mathbb{T}_{qR^\vee})^m)$.

4.1. Hardness of search Entropic Module-LWE

In this subsection, we only establish the hardness of the search Entropic Module-LWE problem with continuous Gaussian noise. Using discretization technique (see Lyubashevsky et al. [23] for more details) we can get that the search entropic Module-LWE problem with discrete Gaussian noise is also hard. The results are divided into two cases, general high entropy case and bounded case, in which the bounded case can get a smaller lower bound.

Theorem 5. *Let c be the global constant from Corollary 1. Let q,d,m,k be positive integers with $m>n$, $d>k$ and α, β, $\alpha'>0$ with $\alpha > \sqrt{2mc}\beta\alpha'$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution $\mathcal{S}$. Further assume that $\nu_{\alpha'}(\mathcal{S}) \ge nk\log(q) + \omega(\log(\lambda))$. Then search Entropic Module-LWE problem* SEMLWE$(R,d,q,m,D_\alpha,\mathcal{S})$ *is hard, provided that* primal-DMLWE$(R,k,q,D_{R,\beta})$ *is hard.*

Proof. Let $\mathcal{A}$ be a search adversary against SEMLWE$(R,d,q,m,D_\alpha,\mathcal{S})$ and $D(F,\alpha,\alpha')$ be the efficient sampling algorithm from Corollary 1. Consider the following hybrid Module-LWE distributions:

- $\mathcal{H}_0$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $A \leftarrow U((R_q)^{m\times d})$ and $\mathbf{e} \leftarrow D_\alpha(K_\mathbb{R})^m$, and then output $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$;
- $\mathcal{H}_1$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $B \leftarrow U((R_q)^{m\times k})$, $C \leftarrow U((R_q)^{k\times d})$, $F \leftarrow D_{R,\beta}^{m\times d}$, set $A = BC + F \bmod qR$, $\mathbf{e} \leftarrow D_\alpha(K_\mathbb{R})^m$, and output $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$;
- $\mathcal{H}_2$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $B \leftarrow U((R_q)^{m\times k})$, $C \leftarrow U((R_q)^{k\times d})$, $F \leftarrow D_{R,\beta}^{m\times d}$, if there exists $j\in[n]$ s.t. $s_1(F^j) > c\beta\sqrt{m}$ output $\perp$. Else, let $A = BC + F \bmod qR$, $\mathbf{e} \leftarrow D_\alpha(K_\mathbb{R})^m$, and output $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$;
- $\mathcal{H}_3$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $B \leftarrow U((R_q)^{m\times k})$, $C \leftarrow U((R_q)^{k\times d})$, $F \leftarrow D_{R,\beta}^{m\times d}$, if there exists $j\in[n]$ s.t. $s_1(F^j) > c\beta\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e}_1 \leftarrow D_{\alpha'}(K_\mathbb{R})^d$, $\mathbf{e}_2 \leftarrow D(F,\alpha,\alpha')$, and set $A = BC + F \bmod qR$, $\mathbf{e} = \mathbf{F}\mathbf{e}_1 + \mathbf{e}_2$, and then output $(A, A\cdot\mathbf{s}+\mathbf{e} \bmod qR^\vee)$.

First note that $\mathcal{H}_0$ is identical to the SEMLWE$(R,d,q,m,D_\alpha,\mathcal{S})$ experiment. Second, it follows directly by the hardness of primal-DMLWE$(R,k,q,D_{R,\beta})$ that $\mathcal{H}_0$ and $\mathcal{H}_1$ are computationally indistinguishable. Then, if we have for any $j\in[n]$, $s_1(F^j) \le c\beta\sqrt{m}$, $\mathcal{H}_1$ and $\mathcal{H}_2$ are identically distributed. Thus we can bound the statistical distance between $\mathcal{H}_1$ and $\mathcal{H}_2$ by the probability

$$\Pr[\exists j\in[n] : s_1(F^j) \ge c\beta\cdot\sqrt{m})].$$

By Lemma 11, with all but 2^{-m} probability it holds that $s_1(F^j) \le c \cdot \beta \cdot \sqrt{m}$ for all $j \in [n]$. Therefore, the statistical distance between $\mathcal{H}_1$ and $\mathcal{H}_2$ is at most 2^{-m}. Finally, by Corollary 1, we have $\mathcal{H}_2$ and $\mathcal{H}_3$ are identically distributed.

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

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

where $(A, A \cdot \mathbf{s} + \mathbf{e} \bmod qR^\vee) \leftarrow \mathcal{H}_3$. Consequently, by the above we can then argue that the same holds for $(A, A \cdot \mathbf{s} + \mathbf{e} \bmod qR^\vee) \leftarrow \mathcal{H}_0$, which means that the search problem SEMLWE$(R, d, q, m, D_\alpha, S)$ is hard, concluding the proof for the theorem.

To do so, we bound the conditional min-entropy of $\mathbf{s}$ given $(A, \mathbf{y}) \leftarrow \mathcal{H}_3$. Note that we can compute $\mathbf{y} = A \cdot \mathbf{s} + \mathbf{e} \bmod qR^\vee$ given $B \in (R_q)^{m \times k}$, $C\mathbf{s} \bmod qR^\vee$, $F \in R^{m \times d}$, $\mathbf{s} + \mathbf{e}_1 \bmod qR^\vee$ and $\mathbf{e}_2 \in (K_{\mathbb{R}})^m$. 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, we have $C\mathbf{s} \bmod qR^\vee \in (R_q^\vee)^k$ has at most $2^{kn \log q}$ possible values. Then by Lemma 4, we can get the bound:

$$\begin{aligned}
&\widetilde{H}_\infty(\mathbf{s} \mid (A, A \cdot \mathbf{s} + \mathbf{e} \bmod qR^\vee)) \\
&\ge \widetilde{H}_\infty(\mathbf{s} \mid B, C, F, C\mathbf{s} \bmod qR^\vee, \mathbf{s} + \mathbf{e}_1 \bmod qR^\vee, \mathbf{e}_2) \\
&= \widetilde{H}_\infty(\mathbf{s} \mid C, C\mathbf{s} \bmod qR^\vee, \mathbf{s} + \mathbf{e}_1 \bmod qR^\vee) \\
&\ge \widetilde{H}_\infty(\mathbf{s} \mid C, \mathbf{s} + \mathbf{e}_1 \bmod qR^\vee) - nk \log q \\
&= \nu_{\alpha'}(S) - nk \log q.
\end{aligned}$$

Where the first equality follows from the fact that B, F, $\mathbf{e}_2$ are independent of everything else, and the second equality follows from the fact that C is independent of everything else. The second inequality follows from Lemma 4. By assumption we have $\nu_{\alpha'}(S) \ge nk \log(q) + \omega(\log(\lambda))$, it follows that

$$\Pr[\mathcal{A}(A, A \cdot \mathbf{s} + \mathbf{e} \bmod qR^\vee) = \mathbf{s}] \le 2^{-\widetilde{H}_\infty(\mathbf{s} \mid (A, A \cdot \mathbf{s} + \mathbf{e} \bmod qR^\vee))} \le 2^{-\omega(\log(\lambda))},$$

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

By combining Theorem 5, Corollary 2 and Corollary 3, we deduce the following theorems, which present an entropy bound that guarantees the hardness of search Entropic Module-LWE problem in both general case and bounded case.

Theorem 6 *(General high entropy). 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 B_R be some known basis of R in $\mathbb{H}$. Let q, d, m, k be positive integers with $m > n$, $d > k$, β, $\alpha' > 0$ with $\frac{q}{\alpha'} \ge \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ distributed according to some distribution S, with*

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

Furthermore let $\alpha > \sqrt{2mc}\beta\alpha'$, then the search problem SEMLWE$(R, d, q, m, D_\alpha, S)$ *is hard, provided that* primal-DMLWE$(R, k, q, D_{R,\beta})$ *is hard.*

Theorem 7 *(Bounded norm). Let c be the global constant, 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, k be positive integers with $m > n$, $d > k$, $\beta, \alpha' > 0$. Let $\mathbf{s}$ be a M-bounded random variable on $(R_q^\vee)^d$ with*

$$\widetilde{H}_\infty(\mathbf{s}) \ge nk \log(q) + \sqrt{2\pi nd} \cdot \frac{M}{\alpha'} \log(e) + \omega(\log(\lambda)).$$

Furthermore let $\alpha > \sqrt{2mc}\beta\alpha'$, then the search problem SEMLWE$(R, d, q, m, D_\alpha, S)$ *is hard, provided that* primal-DMLWE$(R, k, q, D_{R,\beta})$ *is hard.*

Remark 3. The hardness of primal-DMLWE assumption is used to assert that $BC + F \bmod qR$ is computationally indistinguishable from a uniform matrix. Thus we can set $k = 1$ and use the hardness of Ring-LWE assumption to get the hardness Entropic Module-LWE result.

Binary module LWE Theorem 7 directly implies the hardness of the Binary Module-LWE problem. The Binary Module-LWE problem is a special case of the Entropic Module-LWE problem where the secret is chosen from the $R_2^\vee$. Our method provides an alternative solution for the hardness of the Binary Module-LWE problem. Besides, as a small improvement, the noise ratio in our result is $\sqrt{m}$, smaller than $n^2 d\sqrt{m}$ in [7] and $n^{1.5}\sqrt{d}$ in [19].

For the sake of simplicity, we only consider a particular case, where $K = \mathbb{Q}(\xi)$ is a cyclotomic number field with degree n. In this case, the map taking the coefficient embedding to the canonical embedding is a scaled isometry with scaling factor $\sqrt{n}$. Taking the"power basis" of R given by $1, \xi, \cdots, \xi^{n-1}$, gives us an orthonormal lattice basis of R in the coefficient embedding. Applying the aforementioned scaled isometry, we can find an orthogonal basis in the canonical embedding where each vector has length $\sqrt{n}$. Therefore, in the canonical embedding $\|\tilde{B}_R\| = \sqrt{n}$ when using this basis.

Lemma 18. *Let c be the global constant, R be a cyclotomic rings with degree n and $R^\vee$ be the dual of R. Let q, d, m be positive integers with $m > n$, $d > 11\log q$, β, $\alpha' > 0$. Let $\mathbf{s}$ be a uniform random variable on $(R_2^\vee)^d$. Also let $\alpha > 6c\sqrt{m}\beta$. Then the Binary Module-LWE problem* SEMLWE$(R, d, q, m, D_\alpha, (R_2^\vee)^d)$ *is hard, provided that* primal-DRLWE$(R, q, D_{R,\beta})$ *is hard.*

Proof. Since $\mathbf{s}$ is a uniform random variable on $(R_2^\vee)^d$, we have $\widetilde{H}_\infty(\mathbf{s}) = nd$. Since R is a cyclotomic ring with degree n, we have $R_2^\vee = \frac{1}{n}R_2$. Let $1, \xi, \cdots, \xi^{n-1}$ be the "power basis" of R, for any $s \in R_2^\vee$, we have $s = \frac{1}{n}(a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1})$, where $a_i \in \{0, 1\}$. So we have

$$|\sigma_i(s)| = \frac{1}{n}|\sigma_i(a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1})| \le \frac{1}{n}\sum_{j=1}^{n} a_j|\sigma_j(\xi^j)| = 1.$$

Therefore, we can take $M = \sqrt{nd}$, $k = 1$ and $\alpha' = 4$, then apply Theorem 7 in SEMLWE$(R, d, q, m, D_\alpha, (R_2^\vee)^d)$ to completes this proof. □

Remark 4. In the above lemma, we use $k = 1$ to establish the hardness of the Binary Module-LWE problem from the Ring-LWE problem, because we can get the smallest d in this case. We can also take $k > 1$ to get the hardness of the Binary Module-LWE problem from the Module-LWE problem. In this case d need to satisfy $d > 11k\log q$.

4.2. Hardness of decision Entropic Module-LWE

In this subsection, we will establish the hardness of the decision entropic Module-LWE problem with continuous Gaussian noise. To achieve this, we require secret distribution satisfies that for every prime ideal factor $\mathfrak{p}_i | qR$, $\mathbf{s} \bmod \mathfrak{p}_i R^\vee$ has high entropy. This requirement is not unique to our article, Liu et al. also used it when considering the pseudorandomness of Module-LWR in [21]. In addition, the Binary-MLWE problem also satisfies this requirement. Similar to the search pattern, the results in this subsection are also divided into two cases, general high entropy case and bounded case, the bounded case can also get a smaller lower bound.

Theorem 8 *(Bounded norm). Let c be the global constant from Corollary 1. Let K be some number field with degree n, R be the ring of integers of K and $R^\vee$ be the dual of R. Let d, m, k be positive integers where $m > n$, $d > k$, q be a prime and $\alpha, \alpha', \beta > 0$. Assume that the decomposition of qR can be expressed as $\prod_i \mathfrak{p}_i^{r_i}$, where each $\mathfrak{p}_i$ is a prime ideal over R. Suppose $\mathbf{s}$ is chosen from some M-bounded distribution $\mathcal{S}$ over $(R_q^\vee)^d$ such that*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \ge nk\log(q+1) + \sqrt{2\pi nd}\frac{M}{\alpha'}\log e - 2 + \omega(\log(\lambda))$$

for any prime ideal $\mathfrak{p}_i$ of qR. Let $\alpha > \sqrt{2mc}\beta\alpha'$, then we have decisional problem DEMLWE$(R, d, q, m, D_\alpha, \mathcal{S})$ *is hard, provided* primal-DMLWE$(R, k, q, D_{R,\beta})$ *and* DMLWE(R, k, q, m, D_α) *are hard.*

Proof. Throughout this proof, c is the global constant from Corollary 1 and $D(F, \alpha, \alpha')$ is the efficient sampling algorithm from Corollary 1. We assume $\mathcal{D}$ be a PPT distinguisher which distinguishes DEMLWE$(K, d, q, m, \mathcal{S}, D_\alpha)$ with non-negligible advantage. Consider the following hybrid Module-LWE distributions:

- $\mathcal{H}_0$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $A \leftarrow U((R_q)^{m\times d})$ and $\mathbf{e} \leftarrow D_\alpha(K_\mathbb{R})^m$, and then output $(A, A\cdot\mathbf{s} + \mathbf{e} \bmod qR^\vee)$;
- $\mathcal{H}_3$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $B \leftarrow U((R_q)^{m\times k})$, $C \leftarrow U((R_q)^{k\times d})$, $F \leftarrow D_{R,\beta}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(F^j) > c\beta\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e}_1 \leftarrow D_{\alpha'}(K_\mathbb{R})^d$, $\mathbf{e}_2 \leftarrow D(F, \alpha, \alpha')$, and set $A = BC + F \bmod qR$, $\mathbf{e} = F\mathbf{e}_1 + \mathbf{e}_2$, and then output $(A, A\cdot\mathbf{s} + \mathbf{e} \bmod qR^\vee)$.
- $\mathcal{H}_4$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{s}^* \leftarrow U((R_q^\vee)^d)$, $B \leftarrow U((R_q)^{m\times k})$, $C \leftarrow U((R_q)^{k\times d})$, $F \leftarrow D_{R,\beta}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(F^j) > c\beta\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e}_1 \leftarrow D_{\alpha'}(K_\mathbb{R})^d$, $\mathbf{e}_2 \leftarrow D(F, \alpha, \alpha')$, and set $A = BC + F \bmod qR$, and then output $(A, B\mathbf{s}^* + F(\mathbf{s} + \mathbf{e}_1 \bmod qR^\vee) + \mathbf{e}_2 \bmod qR^\vee)$.
- $\mathcal{H}_5$: Let $\mathbf{s} \leftarrow \mathcal{S}$, $\mathbf{s}^* \leftarrow U((R_q^\vee)^k)$, $B \leftarrow U((R_q)^{m\times k})$, $C \leftarrow U((R_q)^{k\times d})$, $F \leftarrow D_{R,\beta}^{m\times d}$, if there exists $j \in [n]$ s.t. $s_1(F^j) > c\beta\sqrt{m}$ output $\perp$. Otherwise, let $\mathbf{e} \leftarrow D_\alpha(K_\mathbb{R})^m$, set $A = BC + F \bmod qR$, and then output the pair $(A, B\mathbf{s}^* + F\mathbf{s} + \mathbf{e} \bmod qR^\vee)$.

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 Lemma 17. Note that the only difference between $\mathcal{H}_3$ and $\mathcal{H}_4$ is that in $\mathcal{H}_4$ we have replaced $C\mathbf{s}$ by a uniformly random $\mathbf{s}^*$. Moreover, the only other term depending on $\mathbf{s}$ is $\mathbf{s} + \mathbf{e}_1 \bmod qR^\vee$. Consequently, we can bound the statistical distance between $\mathcal{H}_3$ and $\mathcal{H}_4$ by

$$\begin{aligned}\Delta(\mathcal{H}_3; \mathcal{H}_4) \le& \Delta((C, C\mathbf{s}, \mathbf{s} + \mathbf{e}_1 \bmod qR^\vee); (C, \mathbf{s}^*, \mathbf{s} + \mathbf{e}_1 \bmod qR^\vee))\\ =& \Delta(\mathcal{G}, \mathcal{U}) \le 2^{-\omega(\log(\lambda))/2},\end{aligned}$$

which is negligible. The second inequality follows by the Lemma 17.

Next, we claim that $\mathcal{H}_4$ and $\mathcal{H}_5$ are identically distributed. Note that all we did was reversing the decomposition of $\mathbf{e} = F\mathbf{e}_1 + \mathbf{e}_2$. Thus, by the above argument, distinguisher $\mathcal{D}$ also have non-negligible advantage in distinguishing $(A, \mathbf{y})$ from $(A, \mathbf{u})$, where $(A, \mathbf{y}) \leftarrow \mathcal{H}_5$, $(A, \mathbf{u}) \leftarrow U((R_q)^{m\times d} \times (\mathbb{T}_{qR^\vee})^m)$. From such a distinguisher $\mathcal{D}$ we can construct a distinguisher $\mathcal{D}'$ which distinguishes DMLWE(K, k, q, m, D_α) with non-negligible advantage as follows. $\mathcal{D}'$ gets as input $B \in (R_q)^{m\times k}$ and $\mathbf{z} \in (\mathbb{T}_{qR^\vee})^m$, and proceeds as follows:

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

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 $(B, \mathbf{z} = B\mathbf{s}^* + \mathbf{e} \bmod qR^\vee)$, where $B \leftarrow U((R_q)^{m\times k})$, $\mathbf{s}^* \leftarrow U((R_q^\vee)^k)$ and $\mathbf{e} \leftarrow D_r(K_{\mathbb{R}})^m$. Then it holds that

$$\mathbf{y} = \mathbf{z} + F\mathbf{s} \bmod qR^\vee = B\mathbf{s}^* + F\mathbf{s} + \mathbf{e} \bmod qR^\vee.$$

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

On the other hand, if the input of $\mathcal{D}'$ is distributed according to $(B, \mathbf{z})$, where $\mathbf{z} \leftarrow U((\mathbb{T}_{qR^\vee})^m)$. Then it holds that $\mathbf{y} = \mathbf{z} + F\mathbf{s} \bmod qR^\vee$ 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. □

Remark 5. Assuming that qR can be factored into $\prod_i \mathfrak{p}_i^{r_i}$, such that $N(\mathfrak{p}_i) \geq q^{\frac{n}{\varpi}}$ holds for each prime ideal. Then by Theorem 8, the minimum value we can set for d is ϖk.

Now, we provide some parameters to quantify the result of Theorem 8. Let $R = \mathbb{Z}[X]/\langle X^{512} + 1\rangle$, let ϖ be a power of two with $\varpi \leq 512$, let q be a prime with $q - 1 \equiv 2\varpi \pmod{4\varpi}$, and let us fix a primitive 2ϖ-th root of unity ζ in $\mathbb{Z}_q$. Then, the polynomial $X^{512} + 1$ factors into ϖ irreducible polynomials in $\mathbb{Z}_q$, i.e., $X^{512} + 1 \equiv \prod_{i=0}^{\varpi-1}(X^{\frac{512}{\varpi}} - \zeta^{2i+1}) \mod q$. By Chinese remainder theorem, we obtain $\mathcal{R}_q \cong \mathcal{R}_q^0 \times \cdots \times \mathcal{R}_q^{\varpi-1}$ for $\mathcal{R}_q^i = \mathbb{Z}_q[X]/(X^{\frac{512}{\varpi}} - \zeta^{2i+1})$. Assume that the primal-DMLWE$(R, 1, q, D_{R,\beta})$ problem (actually Ring-LWE) is hard and distribution S is $\sqrt{q}$-bounded. In this case, setting $d = 8 \cdot \varpi^2$ is an appropriate choice. Therefore, when qR completely splits, $d = 2^{21}$, which is very large, but when qR splits very little, such as $\varpi = 2$, d can be chosen as 32.

Similarly, by replacing Lemma 17 with Lemma 16 in the above theorem, we can get the following general case theorem. The proof is the same, so we omit here.

Theorem 9 *(General high entropy). Let c be the global constant from Corollary 1. Let K be some number field with degree n, R be the ring of integers of K and $R^\vee$ be the dual of R. Let d, m, k be positive integers with $m > n$, $d > k$, q be a prime and $\alpha, \alpha', \beta > 0$ with $\frac{q}{\alpha} \geq \|\widetilde{B}_R\| \cdot \sqrt{\frac{\log(4nd)}{\pi}}$. Assume that the decomposition of qR can be expressed as $\prod_i \mathfrak{p}_i^{r_i}$, where each $\mathfrak{p}_i$ is a prime ideal over R. Suppose $\mathbf{s}$ is chosen from some distribution S over $(R_q^\vee)^d$ such that*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \geq nk\log(q+1) + nd\log(\frac{q}{\alpha'}) - \frac{d}{2}\log(\Delta_K) - 1 + \omega(\log(\lambda))$$

for any prime ideal $\mathfrak{p}_i$ of qR. Let $\alpha > \sqrt{2mc}\beta\alpha'$, then we have decisional problem DEMLWE$(R, d, q, m, D_\alpha, S)$ *is hard, provided* primal-DMLWE$(R, k, q, D_{R,\beta})$ *and* DMLWE(R, k, q, m, D_α) *are hard.*

Remark 6. Similarly with the search Entropic Module-LWE problem, we can set $k = 1$ here and use the hardness of Ring-LWE assumption to get the hardness of the decision Entropic Module-LWE problem.

4.3. Tightness of the result

In this section, we will show that for general modulus and general min-entropy distributions, our result is tight up to polynomial factors. For sake of simplicity, we also consider the case of cyclotomic rings with degree n.

For a modulus q and a noise parameter α, we will provide an example of a distribution $\mathbf{s}$ with min-entropy at least $nd\log(\frac{q}{\alpha}) - 2\log(\log(\lambda))$, such that SEMLWE$(R, d, q, m, D_\alpha, S)$ is easy. Our counter-example is a natural generalization of the counter example in [5,9].

Lemma 19. *Let R be a cyclotomic rings with degree n and $R^\vee$ be the dual of R. Let $1, \xi, \cdots, \xi^{n-1}$ be the "power basis" of $R^\vee$. Let q be a modulus such that q has a big divisor p. Let d, m be positive integers with $m > n$, $d > 1$ and let χ be a error distribution with $\Pr_{e\leftarrow\chi}[\max_i \mathrm{Tr}(e\xi^i) > B] \leq \delta$ for some (B, δ), where $B \leq \frac{p}{2}$. Define the distribution S to be the uniform distribution on $p \cdot (R_q^\vee)^d$. Then there exists an efficient algorithm $\mathcal{A}$ that solves the search problem* SEMLWE(R, d, q, m, χ, S) *with advantage at least $1 - \delta$.*

Proof. Assume that an element in $(K_{\mathbb{R}})^d$ modulo $pR^\vee$ is represented by the elements in the central residual class. In other word, let $\mathbf{y} = (y_1, \cdots y_m)$ and $\mathbf{z} = \mathbf{y} \bmod pR^\vee$, then we have $|\mathrm{Tr}(z_j\xi^i)| \le \frac{p}{2}$ for any $i \in [n], j \in [m]$. The adversary $\mathcal{A}$ gets as input $(A, \mathbf{y})$ and proceeds as follows:

- Compute $\mathbf{e} \leftarrow \mathbf{y} \bmod pR^\vee$;
- Solve the equation system $\mathbf{A} \cdot \mathbf{s} = \mathbf{y} - \mathbf{e}$ for $\mathbf{s}$, and then output $\mathbf{s}$.

To see that the algorithm $\mathcal{A}$ is correct, note that since R is a cyclotomic rings with degree n, we have $R_q = nR_q^\vee$. Thus, for any $\mathbf{a} \in (R_q)^d, \mathbf{s} \in p \cdot (R_q^\vee)^d$, we have $\mathbf{a} \cdot \mathbf{s} \in p \cdot (R_q^\vee)^d$. Therefore

$$\mathbf{y} \bmod pR^\vee = A \cdot \mathbf{s} + \mathbf{e} \bmod pR^\vee = \mathbf{e}$$

as $B \le \frac{p}{2}$. □

By the above lemma, we deduce the following corollary.

Corollary 4. *Let R be a cyclotomic rings with degree n and $R^\vee$ be the dual of R. There exist moduli q and distribution S over $(R^\vee)^d$ with min-entropy at least $nd\log(\frac{q}{\alpha}) - 2\log(\log(\lambda))$ such that the search problem* SEMLWE$(R, d, q, m, D_\alpha, S)$ *is easy.*

Proof. Note that a gaussian of parameter α is $\log(\lambda)\alpha$ bounded, except with negligible probability and $\sigma_C(1), \sigma_C(\xi), \cdots, \sigma_C(\xi^{n-1})$ is an orthogonal basis on $\mathbb{H}$, we have $\mathrm{Tr}(e\xi^i)$ is also $\log(\lambda)\alpha$ bounded. Moreover, by choosing $p = 2\alpha\log(\lambda)$, the distribution S in Lemma 19 has min-entropy

$$nd\log(q/p) \ge nd\log(\frac{q}{\alpha}) - 2\log(\log(\lambda)).$$

Thus we can apply Lemma 19 to complete this proof. □

5. Entropic ring-LWE

In this section, we show an entropy bound that guarantees the security of the Entropic Ring-LWE problem. The Entropic Ring-LWE is a special Entropic Module-LWE with $d = 1$. We use a different approach than Brakerski et al. [35] to get an essentially same entropy bound for search Entropic Ring-LWE problem in bounded case. The advantage of our method is that we can not only get the hardness for the search Entropic Ring-LWE problem in any number field based on common hardness assumption, but can also get the hardness result for the decision Entropic Ring-LWE problem in some special number fields. To the best of our knowledge, this is the first result for the decision Entropic Ring-LWE problem.

Hardness of E-SRLWE: Brakerski et al. [9] use the generalized "closeness to low-rank" approach to get the first hardness result of the search Entropic Ring-LWE problem. Here, we use another approach to get the hardness of search Entropic Ring-LWE. We only consider continuous gaussian noise here. Using discretization technique, the result holds for the search Entropic Ring-LWE problem with discrete gaussian noise. We show the entropy bound for the search Entropic Ring-LWE problem by combining the result of Albrecht et al. [3] and our Theorem 7.

Lemma 20 *(Adapted from Corollary 3 in [3]). Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R and B_R be some known basis of R in $\mathbb{H}$. Let d, q, m be positive integers and let $\mathbf{G} = (1, q, \cdots, q^{d-1}) \in R^{1\times d}$. Let $\mathbf{s}$ be a random variable on $(R_q^\vee)^d$ according to some distribution S satisfying $\Pr_{\mathbf{s}\leftarrow S}[\max_{i,j} |\sigma_i(s_j)| > B] \le \delta$. Let $\alpha' > 0$, $\epsilon \in (0, 1/2)$, $\tau \ge \|\widetilde{B}_R\| \cdot \sqrt{2\ln(2nd(1+1/\epsilon))/\pi}$ and define $\alpha = \sqrt{\alpha'^2 + (\tau B(mn)^{1/4})^2}$. Suppose there exists a* PPT *algorithm which can solve* ERLWE$(R, q^d, m, \mathbf{G}S, D_\alpha)$ *with probability p, then there is an algorithm solving* E-MLWE$(R, d, q, m, S, D'_\alpha)$ *with probability at least $\frac{(1-\delta)p^2}{2} - (2d+6)\epsilon m - \delta$.*

We now use the above lemma to show the hardness of the Entropic Ring-LWE problem.

Theorem 10. *Let c be the global constant from Corollary 1, R be the ring of integers of degree n, $R^\vee$ be the dual of R and B_R be a basis of R. Let q, m be integers $\alpha, \alpha', \beta > 0$ and $\tau \ge \|\widetilde{B}_R\| \cdot \sqrt{2\ln(4n(1+2^{\omega(\log(\lambda))}))/\pi}$. Let s be a random variable on $(R_{q^2}^\vee)$ with $\|s \bmod qR^\vee\| \le M$, $\|s - (s \bmod qR^\vee)\| \le qM$ and $\widetilde{H}_\infty(s) \ge n\log(q) + 5.5\frac{M\sqrt{n}}{\alpha'}$. Let $\alpha = \sqrt{(\sqrt{2mc}\beta\alpha')^2 + (\tau M(mn)^{1/4})^2}$. Then we have that the search problem* SERLWE(K, q^2, m, S, D_α) *is hard, provided the* primal-DRLWE$(K, q, D_{R,\beta})$ *is hard.*

Proof. Let $\mathbf{G} = (1, q) \in R^{1\times 2}$. Then the map $h_{\mathbf{G}} : (R_q^\vee)^2 \mapsto R_{q^2}^\vee$ given by $h_{\mathbf{G}}(\mathbf{s}) = \mathbf{G}\mathbf{s}$ is a bijection. Thus, for any $\mathbf{s} \in R_{q^2}^\vee$, we denote $\mathbf{G}^{-1}(\mathbf{s})$ be preimage of $\mathbf{s}$. And for any distribution S on $R_{q^2}^\vee$, we denote $\mathbf{G}^{-1}(S)$ be a distribution on $(R_q^\vee)^2$ such that if $\mathbf{s}$ is a random variable according to $\mathbf{G}^{-1}(S)$, then $\mathbf{G}\mathbf{s}$ is a random variable according to S.

Assume there is an adversary $\mathcal{A}$ and a distribution $\mathcal{S}$ such that $\mathcal{A}$ has non-negligible advantage to solve SERLWE$(R, q^2, m, \mathcal{S}, D_\alpha)$, and $\mathcal{S}$ satisfies

$$\|s \bmod qR^\vee\| \le M,\ \|s - (s \bmod qR^\vee)\| \le qM, \qquad \widetilde{H}_\infty(s) \ge n\log(q) + 5.5\frac{M\sqrt{n}}{\alpha'}.$$

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

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

Then by Lemma 20, we can construct a PPT adversary $\mathcal{A}'$ such that $\mathcal{A}'$ solving SEMLWE$(R, 2, q, m, \mathbf{G}^{-1}(\mathcal{S}), D_{\tilde{\alpha}})$ with probability

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

where $\tilde{\alpha} = \sqrt{2mc}\beta\alpha'$. And since $h_{\mathbf{G}}$ is a bijection, we have

$$\widetilde{H}_\infty(\mathbf{G}^{-1}(\mathcal{S})) = \widetilde{H}_\infty(\mathcal{S}) \ge n\log(q) + 5.5\frac{M\sqrt{n}}{q\alpha'}.$$

Thus by Theorem 7, we have the search problem SEMLWE$(R, 2, q, m, \mathcal{S}, D_\alpha)$ is hard, which contradicts to the advantage of $\mathcal{A}'$. This concludes the proof. □

Remark 7. Here, for sake of simplicity, we only use bounded case to get the hardness result for some special secret distribution with modulus q^2. Similar results can be obtained for the Entropic Ring-LWE problem with general secret distribution and modulus q^d.

Hardness of E-DRLWE In this section we will establish the hardness result for the decision version Entropic Ring-LWE problem with continuous gaussian noise. We first give a reduction from the decision Entropic Module-LWE problem to the decision Entropic Ring-LWE problem with a spherical error distribution, and then give the hardness result for the decision Entropic Ring-LWE problem by combining this reduction and our Theorem 8.

Lemma 21. *Let R be the ring of integers of some algebraic number field K of degree n, $R^\vee$ be the dual of R and 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 $\epsilon \in (0, 1/2)$,

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

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.*

The proof of this lemma is obtained by combining the reduction from [2] and a technique (non-spherical error to spherical error) used in [28]. The proof is included in the full version of this paper.

Combining Theorem 8 and Lemma 21, we can get the following theorem. The proof of the following theorem is analogous to Theorem 10.

Theorem 11. *Let c be the global constant from Corollary 1. Let K be some number field with degree n, R be the ring of integers of K and $R^\vee$ be the dual of R. Let d, m, k be positive integers where $m > n$, $d > k$, q be a prime and $\alpha, \alpha', \beta > 0$, and $\tau \ge \|\widetilde{B}_R\| \cdot \sqrt{2\ln(4n(1 + 2^{\omega(\log(\lambda))}))/\pi}$. Assume that the decomposition of qR can be expressed as $\prod_i \mathfrak{p}_i^{r_i}$, where each $\mathfrak{p}_i$ is a prime ideal over R. Let s be a random variable on $(R_{q^2}^\vee)$ distributed according to some distribution $\mathcal{S}$, with $\|s \bmod qR^\vee\| \le M$, $\|s - (s \bmod qR^\vee)\| \le qM$ and*

$$\tilde{H}_\infty(\mathbf{s} \bmod \mathfrak{p}_i R^\vee) \ge nk\log(q+1) + \sqrt{2\pi nd}\frac{M}{\alpha'}\log e - 2 + \omega(\log(\lambda))$$

for any prime ideal $\mathfrak{p}_i$ of qR. Let $r > \sqrt{2}c\sqrt{m}\beta\alpha'$, and $\alpha = \sqrt{r^2 + 4\tau^2 M^2} \cdot (nm/\log(nm))^{1/4}$. Then the decisional problem E-DRLWE$(K, q^2, m, \mathcal{S}, D_\alpha)$ *is hard, provided that* primal-RLWE$(K, q, D_{R,\beta})$ *and* DRLWE(K, q, m, D_r) *are hard.*

Remark 8. Similarly, the hardness results with general secret distribution and modulus q^d can be obtained by the same way.

6. Conclusion

LWE and its variants have been served as the foundation of many post-quantum cryptographic schemes. Module-LWE enjoys the properties of high computational efficiency and feasible concrete parameter selection. Towards establishing the leakage resilience of Module-LWE, we study the hardness of entropic version of Module-LWE. Our results apply to both the search and decision versions, each of which consists of bounded and unbounded norm cases. In terms of techniques, we develop several probability lemmas including a new variant of leftover hash lemma, which might find applications in other scenarios.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

No data was used for the research described in the article.

Acknowledgements

We thank the anonymous reviewers for their helpful suggestions. This work was partially supported by the National Key Research and Development Program of China (No. 2021YFA1000600, No 2021YFB3100200 and No. 2018YFA0704702), the National Natural Science Foundation of China (No. 61832012), the Taishan Scholars Program (No.tsqn202306315), the Open Research Fund of State Key Laboratory of Cryptology (No. MMKFKT202207), Key Research and Development Program of Shandong province (No. 2022CXGC020101) and the Shandong Provincial Natural Science Foundation (No. ZR2022QF039).

References

[1] S. Agrawal, D.M. Freeman, V. Vaikuntanathan, Functional encryption for inner product predicates from learning with errors, in: D.H. Lee, X. Wang (Eds.), ASIACRYPT 2011, in: LNCS, vol. 7073, Springer, 2011, pp. 21–40.
[2] M.R. Albrecht, A. Deo, Large modulus ring-LWE ≥ module-LWE, in: T. Takagi, T. Peyrin (Eds.), ASIACRYPT 2017, in: LNCS, vol. 10624, Springer, 2017, pp. 267–296.
[3] M.R. Albrecht, A. Deo, Large modulus ring-LWE ≥ module-LWE, IACR Cryptol. 2017 (2017) 612, ePrint Arch.
[4] J. Alwen, S. Krenn, K. Pietrzak, D. Wichs, Learning with rounding, revisited - new reduction, properties and applications, in: R. Canetti, J.A. Garay (Eds.), CRYPTO 2013, in: LNCS, vol. 8042, Springer, 2013, pp. 57–74.
[5] M. Bolboceanu, Z. Brakerski, R. Perlman, D. Sharma, Order-LWE and the hardness of ring-LWE with entropic secrets, in: S.D. Galbraith, S. Moriai (Eds.), ASIACRYPT 2019, in: LNCS, vol. 11922, Springer, 2019, pp. 91–120.
[6] J.W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J.M. Schanck, P. Schwabe, G. Seiler, D. Stehlé, CRYSTALS - kyber: a CCA-secure module-lattice-based KEM, in: EuroS&P 2018, IEEE, 2018, pp. 353–367.
[7] K. Boudgoust, C. Jeudy, A. Roux-Langlois, W. Wen, Towards classical hardness of module-LWE: the linear rank case, in: S. Moriai, H. Wang (Eds.), ASIACRYPT 2020, in: LNCS, vol. 12492, Springer, 2020, pp. 289–317.
[8] K. Boudgoust, C. Jeudy, A. Roux-Langlois, W. Wen, Entropic hardness of module-LWE from module-NTRU, in: T. Isobe, S. Sarkar (Eds.), Progress in Cryptology – INDOCRYPT 2022, in: LNCS, vol. 13774, Springer, 2022, pp. 78–99.
[9] Z. Brakerski, N. Döttling, Hardness of LWE on general entropic distributions, in: A. Canteaut, Y. Ishai (Eds.), EUROCRYPT 2020, in: LNCS, vol. 12106, Springer, 2020, pp. 551–575.
[10] Z. Brakerski, C. Gentry, V. Vaikuntanathan, (Leveled) fully homomorphic encryption without bootstrapping, in: S. Goldwasser (Ed.), Innovations in Theoretical Computer Science 2012, Cambridge, MA, USA, January 8-10, 2012, ACM, 2012, pp. 309–325.
[11] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, D. Stehlé, Classical hardness of learning with errors, in: D. Boneh, T. Roughgarden, J. Feigenbaum (Eds.), Symposium on Theory of Computing Conference, STOC 2013, Palo Alto, CA, USA, June 1-4, 2013, ACM, 2013, pp. 575–584.
[12] J. Ding, A simple provably secure key exchange scheme based on the learning with errors problem, IACR Cryptol. 2012 (2012) 688, ePrint Arch.
[13] Y. Dodis, R. Ostrovsky, L. Reyzin, A.D. Smith, Fuzzy extractors: how to generate strong keys from biometrics and other noisy data, SIAM J. Comput. 38 (1) (2008) 97–139.
[14] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, D. Stehlé, CRYSTALS-dilithium: a lattice-based digital signature scheme, IACR Trans. Cryptogr. Hardware Embed. Syst. 2018 (1) (2018) 238–268.
[15] C. Gentry, C. Peikert, V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in: C. Dwork (Ed.), Symposium on Theory of Computing Conference, STOC 2008, Victoria, British Columbia, Canada, May 17-20, 2008, ACM, 2008, pp. 197–206.
[16] C. Gentry, A. Sahai, B. Waters, Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based, in: R. Canetti, J.A. Garay (Eds.), CRYPTO 2013, in: LNCS, vol. 8042, Springer, 2013, pp. 75–92.
[17] S. Goldwasser, Y.T. Kalai, C. Peikert, V. Vaikuntanathan, Robustness of the learning with errors assumption, in: A.C. Yao (Ed.), Innovations in Computer Science, ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010, Tsinghua University Press, 2010, pp. 230–240.
[18] A. Jain, H. Lin, A. Sahai, Indistinguishability obfuscation from well-founded assumptions, in: S. Khuller, V.V. Williams (Eds.), STOC 2021, ACM, 2021, pp. 60–73.
[19] K. Boudgoust, C. Jeudy, A. Roux-Langlois, W. Wen, On the hardness of module-LWE with binary secret, in: K.G. Paterson (Ed.), CT-RSA 2021, in: LNCS, vol. 12704, Springer, 2021, pp. 503–526.
[20] A. Langlois, D. Stehlé, Worst-case to average-case reductions for module lattices, Des. Codes Cryptogr. 75 (3) (2015) 565–599.
[21] F. Liu, Z. Wang, Rounding in the rings, in: D. Micciancio, T. Ristenpart (Eds.), CRYPTO 2020, in: LNCS, vol. 12171, Springer, 2020, pp. 296–326.
[22] V. Lyubashevsky, C. Peikert, O. Regev, On ideal lattices and learning with errors over rings, in: H. Gilbert (Ed.), EUROCRYPT 2010, in: LNCS, vol. 6110, Springer, 2010, pp. 1–23.
[23] V. Lyubashevsky, C. Peikert, O. Regev, A toolkit for ring-LWE cryptography, in: T. Johansson, P.Q. Nguyen (Eds.), EUROCRYPT 2013, in: LNCS, vol. 7881, Springer, 2013, pp. 35–54.

[24] D. Micciancio, Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions, in: Symposium on Foundations of Computer Science, FOCS 2002, Vancouver, BC, Canada, November 16-19, 2002, IEEE Computer Society, 2002, pp. 356–365.
[25] D. Micciancio, C. Peikert, Trapdoors for lattices: simpler, tighter, faster, smaller, in: D. Pointcheval, T. Johansson (Eds.), EUROCRYPT 2012, in: LNCS, vol. 7237, Springer, 2012, pp. 700–718.
[26] D. Micciancio, O. Regev, Worst-case to average-case reductions based on Gaussian measures, in: Symposium on Foundations of Computer Science, FOCS 2004, Rome, Italy, October 17-19, 2004, IEEE Computer Society, 2004, pp. 372–381.
[27] C. Peikert, Public-key cryptosystems from the worst-case shortest vector problem: extended abstract, in: M. Mitzenmacher (Ed.), Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009, ACM, 2009, pp. 333–342.
[28] C. Peikert, O. Regev, N. Stephens-Davidowitz, Pseudorandomness of ring-LWE for any ring and modulus, in: H. Hatami, P. McKenzie, V. King (Eds.), Symposium on Theory of Computing, STOC 2017, Montreal, QC, Canada, June 19-23, 2017, ACM, 2017, pp. 461–473.
[29] O. Regev, On lattices, learning with errors, random linear codes, and cryptography, in: H.N. Gabow, R. Fagin (Eds.), Symposium on Theory of Computing, STOC 2005, Baltimore, MD, USA, May 22-24, 2005, ACM, 2005, pp. 84–93.
[30] M. Roşca, D. Stehlé, A. Wallet, On the ring-LWE and polynomial-LWE problems, in: J.B. Nielsen, V. Rijmen (Eds.), EUROCRYPT 2018, in: LNCS, vol. 10820, Springer, 2018, pp. 146–173.
[31] G. Seiler, Faster AVX2 optimized NTT multiplication for ring-lwe lattice cryptography, IACR Cryptol. 2018 (2018) 39, ePrint Arch.
[32] R. Vershynin, Introduction to the non-asymptotic analysis of random matrices, in: Y.C. Eldar, G. Kutyniok (Eds.), Compressed Sensing, Cambridge University Press, 2012, pp. 210–268.
[33] R. Vershynin, High-Dimensional Probability: An Introduction with Applications in Data Science, vol. 47, Cambridge University Press, 2018.
[34] Y. Wang, M. Wang, CRPSF and NTRU signatures over cyclotomic fields, IACR Cryptol. 2018 (2018) 445, ePrint Arch.
[35] Z. Brakerski, N. Döttling, Lossiness and entropic hardness for ring-LWE, in: R. Pass, K. Pietrzak (Eds.), TCC 2020, in: LNCS, vol. 12550, Springer, 2020, pp. 1–27.