Discrete Gaussians Modulo Sub-Lattices: New Leftover Hash Lemmas for Discrete Gaussians

Haoxiang Jin[1], Feng-Hao Liu[2], Zhedong Wang[1], Dawu Gu[1]

[1] Shanghai Jiao Tong University, Shanghai, China.
{iniesta8, wzdstill, dwgu}@sjtu.edu.cn,
[2] Washington State University, Pullman, WA, USA. feng-hao.liu@wsu.edu.

Abstract. The Leftover Hash Lemma (LHL) is a powerful tool for extracting randomness from an entropic distribution, with numerous applications in cryptography. LHLs for discrete Gaussians have been explored in both integer settings by Gentry et al. (GPV, STOC'08) and algebraic ring settings by Lyubashevsky et al. (LPR, Eurocrypt'13). However, the existing LHLs for discrete Gaussians have two main limitations: they require the Gaussian parameter to be larger than certain smoothing parameters, and they cannot handle cases where fixed and arbitrary information is leaked.

In this work, we present new LHLs for discrete Gaussians in both integer and ring settings. Our results show that the Gaussian parameter can be improved by a factor of $\omega(\sqrt{\log \lambda})$ and $O(\sqrt{N})$ compared to the regularity lemmas of GPV and LPR, respectively, under similar parameter choices such as the dimension and ring. Furthermore, our new LHLs can be applied to leaked discrete Gaussians, and the result can be used to establish asymptotic hardness of the extended MLWE assumptions, addressing an open question in recent works by Lyubashevsky et al. (LNP, Crypto'22)[3]. Our central techniques involve new fine-grained analyses of the min-entropy in discrete Gaussians modulo sublattices, and should be independent of interest.

Keywords: Leftover Hash Lemma, Discrete Gaussian Distribution, Min-Entropy, Extended-MLWE

1 Introduction

The Leftover Hash Lemma (LHL) [6, 24] is a crucial tool in cryptography, stating that universal hash functions are effective good randomness extractors, i.e., $(\mathcal{H}, \mathcal{H}(\boldsymbol{x})) \approx (U, U)$ where $\mathcal{H}$ is a random function in the universal hash family, U is the uniform distribution, and $\boldsymbol{x}$ is from some distribution with sufficient min-entropy. In lattice-based cryptography, a significant instance is the matrix-vector multiplication form, where the expression becomes $(\mathbf{A}, \mathbf{A} \cdot \boldsymbol{x})$ for random matrix

[3] The extended MLWE assumption is also considered by the original version of the work dPEK+ [15] by del Pino et al, and the recent version of dPEK+ [16] that removes this assumption is accepted by Crypto'24.

$\mathbf{A} \leftarrow \mathcal{M}^{n\times m}$ and entropic $\boldsymbol{x}$. In the integer lattice case, $\mathcal{M} = \mathbb{Z}_q$ can be easily shown that the matrix-vector multiplication in $\mathbb{Z}_q$ serves as the universal hash family, thereby enabling randomness extraction. In the ideal lattice case where $\mathcal{M} = R_q$ for some ring R, proving randomness extraction remains feasible but requires more sophisticated analyses [26,30,33,34,49,50]. This matrix-vector form is particularly important in many lattice-based analyses, including the Regev and Dual-Regev encryption schemes [20,46], and other various advanced designs and analyses [1–3,7,8,17,21,30].

Our Focus: LHL for Discrete Gaussians. In this work, we focus on an important case where $\boldsymbol{x}$ comes from the discrete Gaussian distribution, which has been used in the analysis of Dual-Regev encryption scheme for the integer lattice case [20] and the ring case [33]. However, the existing analyses of LHLs in these two cases post some stronger requirements on the Gaussian width (standard deviation) and cannot be used to analyze the *leakage* case, i.e., the case where some part of $\boldsymbol{x}$ is leaked.

Large Gaussian width has two main disadvantages. Firstly, it will increase the storage and memory requirements. Considering the correctness of lattice-based constructions, which relies on the error-correcting techniques, the ratio of the modulus q to the Gaussian width σ must surpass a certain function of other parameters like dimensions. Hence a larger Gaussian width implies a larger modulus size, which in turn increases the storage bits of each element. Secondly, large Gaussian width increases the time required for discrete Gaussian sampling. Discrete Gaussian sampling for large standard deviation typically requires base sampler for some small and fixed standard deviation, followed by the techniques of Gaussian convolutions [40] or reject sampling [23] to construct discrete Gaussian with large width. In contrast, Gaussian sampling with small width can be implemented from table-based approach, which requires much less time than those advanced techniques, and smaller width implies smaller size of tables. Moreover, it is not clear whether the security of the cryptosystems degrades smoothly with leakage, as the prior analyses of leakage-resilience [3, 21] do not apply. Our goal is to remove the strong requirements on the Gaussian, and prove LHL of the most general form for discrete Gaussians.

Limitations in Existing Works. Before we present our results, we overview currently the best known analyses and then identify their limitations.

- For the integer lattice case, the GPV [20] showed that for all but negligible fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and for discrete Gaussian $\boldsymbol{x} \in \mathbb{Z}_q^m$ with parameter $\sigma \geq \eta_\epsilon(\mathbf{\Lambda}^\perp(\mathbf{A})) = \omega(\sqrt{\log m})$ where $\eta_\epsilon(\mathbf{\Lambda}^\perp(\mathbf{A}))$ is the smoothing parameter of lattice $\mathbf{\Lambda}^\perp(\mathbf{A})$, the distribution of $\mathbf{A}\cdot\boldsymbol{x}$ is statistically close to the uniform distribution. By applying a union bound argument, this analysis implies an LHL for uniformly random $\mathbf{A}$.
- For the ideal lattice case, the work [33] showed that the marginal distribution of $b_0 + \sum_{i=1}^{m-1} b_i a_i$ is statistically close to uniformly random distribution over R_q, where R is a cyclotomic ring of degree N, $\{b_i\}_{i=0}^{m-1}$ are independently

chosen from the discrete Gaussian distribution on R and $\{a_i\}_{i=0}^{m-1}$ are chosen uniformly at random and independently from R_q. This result also requires the Gaussian parameter of b_i, namely σ to be greater than $\eta_\epsilon(\mathbf{\Lambda}^\perp(\boldsymbol{a})) = \Omega(n \cdot q^{2/m})$ for $\boldsymbol{a} = (1, a_1, \cdots, a_{m-1})$.

Clearly we can see that the two LHLs mentioned above require σ to be greater than some smoothing parameters, and this seems necessary if we require the marginal distribution $\mathbf{A} \cdot \boldsymbol{x}$ to be close to uniform *for all but negligible* fraction of matrices $\mathbf{A}$'s. However, in the setting of LHL where $\mathbf{A}$ is uniformly at random and we consider the joint distribution of $(\mathbf{A}, \mathbf{A} \cdot \boldsymbol{x})$, this requirement on σ might become removable, i.e., $\sigma = O(1)$ can be sufficient to imply randomness extraction. To illustrate this intuition, we consider the case of a uniform binary vector, i.e., $\boldsymbol{x} \leftarrow \{0,1\}^m$. If m is sufficiently large, e.g., $m = O(n \log q)$, then the existing LHL [6, 24] implies $(\mathbf{A}, \mathbf{A} \cdot \boldsymbol{x}) \approx (U, U)$. Since a discrete Gaussian with parameter $O(1)$ (for sufficiently large constants) should have more than 1 bit entropy, it would be unsatisfactory that the current LHLs [20, 33] cannot analyze this case. Additionally, the above Gaussian LHLs are not applicable when $\boldsymbol{x}$ has been somewhat leaked, even for arbitrary 1-bit leakage, whereas the general LHL [24] preserves randomness extraction as long as $\boldsymbol{x}$ has entropy $O(n \log q) + \ell$ where ℓ is the number of leaked bits. This presents another unsatisfactory gap.

To address these, this work aims to answer the following main questions:

(**Main Questions:**) (1) Can we derive a leftover hash lemma for the discrete Gaussian over lattice without the dependency of $\sigma \geq \eta_\epsilon(\mathbf{\Lambda}^\perp(\mathbf{A}))$ or $\sigma \geq \eta_\epsilon(\mathbf{\Lambda}^\perp(\boldsymbol{a}))$? (2) Can the leftover hash lemma handle arbitrarily bounded leakage?

1.1 Our Contributions

This work answers the above two questions affirmatively with the following three major contributions.

Contribution 1. First we propose two approaches to compute the exact min-entropy of discrete Gaussians modulo a sub-lattice. The follow theorem is a combination of our two approaches:

Theorem 1.1 *Let $\mathbf{\Lambda}, \mathbf{\Lambda}'$ be n-dimensional full-rank lattices such that $\mathbf{\Lambda}' \subseteq \mathbf{\Lambda}$. Let $\mathbf{B} \in \mathbb{R}^{n \times n}$ be a basis of $\mathbf{\Lambda}$ and $\mathbf{B} \cdot \mathbf{T}$ be a basis of $\mathbf{\Lambda}'$ for some nonsingular upper or lower triangular matrix $\mathbf{T} \in \mathbb{Z}^{n \times n}$ with positive diagonal elements $(t_i)_{i \in [n]}$. Let $\varepsilon \in (0,1)$, positive definite matrix $\mathbf{\Sigma} \in \mathbb{R}^{n \times n}$ be a positive definite matrix, and $\mathbf{c} \in \mathbb{R}^n$ be any center. Define the random variable $\mathcal{S} := D_{\mathbf{\Lambda}, \sqrt{\mathbf{\Sigma}}, \mathbf{c}} \bmod \mathbf{\Lambda}'$.*

First, for $\sigma = 1/\|\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{B}\|_2$, we have

$$2^{H_\infty(\mathcal{S})} \geq \begin{cases} \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{c}') \cdot \prod_{i=1}^{n} \rho_\sigma(\mathbb{Z}_{t_i}) & \text{if } \sqrt{\mathbf{\Sigma}} > 0 \\ \frac{1-\varepsilon}{1+\varepsilon} \cdot \prod_{i=1}^{n} \rho_\sigma(\mathbb{Z}_{t_i}) & \text{if } \sqrt{\mathbf{\Sigma}} \geq \eta_\varepsilon(\mathbf{\Lambda}) \end{cases}.$$

where $\mathbf{c}' = \boldsymbol{c} \bmod \boldsymbol{\Lambda}$.

Furthermore, we have

$$H_\infty(\mathcal{S}) \geq \begin{cases} \log \frac{\det \boldsymbol{\Lambda}'}{\det \boldsymbol{\Lambda}} - \log \frac{1+\varepsilon}{1-\varepsilon}, & \text{if } \sqrt{\boldsymbol{\Sigma}} \geq \eta_\varepsilon(\boldsymbol{\Lambda}'); \\ \log \frac{\det \boldsymbol{\Lambda}'}{\det \boldsymbol{\Lambda}} - n \log \left(\eta_\varepsilon \left(\sqrt{\boldsymbol{\Sigma}}^{-1} \boldsymbol{\Lambda}' \right) \right) - \log \frac{1+\varepsilon}{1-\varepsilon} & \text{if } \eta_\varepsilon(\boldsymbol{\Lambda}) \leq \sqrt{\boldsymbol{\Sigma}} < \eta_\varepsilon(\boldsymbol{\Lambda}'). \end{cases}$$

It should be noted that the inequality "$H_\infty(\mathcal{S}) \geq \log \frac{\det \boldsymbol{\Lambda}'}{\det \boldsymbol{\Lambda}} - \log \frac{1+\varepsilon}{1-\varepsilon}$ if $\sqrt{\boldsymbol{\Sigma}} \geq \eta_\varepsilon(\boldsymbol{\Lambda}')$" can be implicitly derived in the celebrated Gaussian smoothing lemmas [38, Lemma 4.1] and [20, Corollary 2.8], though the smoothing lemmas themselves directly only tell us about the *smooth min-entropy*[4] of $\mathcal{S}$, i.e. $H_\infty^\varepsilon(\mathcal{S}) = \log \frac{\det \boldsymbol{\Lambda}'}{\det \boldsymbol{\Lambda}}$. In order to make Theorem 1.1 a more complete lattice toolbox related to discrete Gaussians, we write it down here without claiming any new contributions on this statement.

Through our new approaches, we derive a series of new entropy lower bounds of discrete Gaussian modulo sublattices by substituting lattice tuples $(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}')$ with some useful and specific choices, such as integer lattice pair $(\mathbb{Z}^n, q\mathbb{Z}^n)$, ideal lattice pair $(R, \mathfrak{q})$ and q-ary lattice pair $(\boldsymbol{\Lambda}_q^\perp(\mathbf{A}), q\mathbb{Z}^m)$ for some $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.

It should be noted that one might consider and easily to compute the so-called *smooth min-entropy* for some certain pairs of $(\boldsymbol{\Lambda}, \boldsymbol{\Lambda}')$. The *smooth min-entropy*, however, has the following three limitations:

1. When the modulus q is a composite number, the smooth entropy is unlikely helpful, unless we set other constraint on the distribution of $\boldsymbol{x}$;
2. Some previous works [7, Lemma 5.4] require the exact min-entropy instead of smooth min-entropy;
3. Indeed, we have a general lower bound for the exact entropy $H_\infty(\boldsymbol{x})$ given by a function of ε and the ε-smooth min-entropy $H_\infty^\varepsilon(\boldsymbol{x})$, which was applied in [45, Lemma 3.8]. Nevertheless, this lower bound has very bad performance.

For more details, please refer to Section 3.

An interesting case is the ideal lattice setting, which plays a crucial role of the improvements of our new leftover hash lemma over regularity lemma from [33]. We demonstrate that

Lemma 1.2 (Ideal Lattice) *Let R be a ring of integers with degree N, q be a prime number and $\mathfrak{q}$ be an ideal factor of qR with norm $\mathcal{N}(\mathfrak{q}) = q^t$, $\mathcal{S} := D_{R,\sigma}^{\mathsf{coeff}} \bmod \mathfrak{q}$ be the Gaussian distribution over coefficient lattice of R modulo $\mathfrak{q}$, and $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4t)}}$. Then we have $H_\infty(\mathcal{S}) \geq t \log \sigma - 1$.*

These lower bounds are the keys to our improved LHLs, and they might provide new insight on the randomness of discrete Gaussian modulo sub-lattices. Thus, we believe that our new methods and lower bounds can be of independent interests.

[4] A random variable X has ϵ-smooth min-entropy at least k, denoted by $H_\infty^\epsilon(X) \geq k$, if there exists some variable X' such that $\Delta(X, X') \leq \epsilon$ and $H_\infty(X') \geq k$.

Contribution 2. Based on the results in Contribution 1 and further technical optimizations, we derive two new LHLs in the integer and ideal lattice settings.

For the case of integer lattice, by using the standard LHL [6] with Theorem 1.1 in the integer setting, we are able to achieve Theorem 1.3. Since the min-entropy of discrete Gaussian distribution over $\mathbb{Z}$ modulo $q\mathbb{Z}$ was studied in [35, Lemma 2.5] and applying their estimation to the standard LHL can also achieve a similar theorem, we do not claim any new result in Theorem 1.1, but write it here and compare with GPV regularity lemma [20] in order to illustrate that leftover hashing can be better than smoothing in integer settings.

Theorem 1.3 (LHL for Discrete Gaussian over Integer Lattice) *Let $q = q_1 q_2$ be a product of two primes, $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and $\boldsymbol{x} \leftarrow D_{\mathbb{Z}^m,\sigma} \bmod q$, $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{\min\{q_1,q_2\}}{\sqrt{\ln(4m)}}$, and $m \log \sigma \geq 2\log(1/\varepsilon) + n \log q$, then $\mathsf{SD}\left((\mathbf{A}, \mathbf{A}\cdot \boldsymbol{x}), U\right) \leq \varepsilon$.*

Here we only consider the case of composite q, and omit the prime modulus case. The reason is that when q is a prime and $q/\sigma > \omega(\log \lambda)$, the smooth entropy of $\boldsymbol{x}$ can be derived via $D_{\mathbb{Z}^n,\sigma}(\mathbf{0}) = 1/\rho_\sigma(\mathbb{Z}^n)$ as we discussed previously, and then apply the leftover hash lemma to $D_{\mathbb{Z}^n,\sigma}$ to obtain the regularity lemma for $D_{\mathbb{Z}^n,\sigma} \bmod q$. However, as we claimed previously, the smooth entropy based analysis might not work for the case of composite q. Alternatively, we can obtain the LHL above based on the exact min-entropy lower bound in our contribution 1. Without loss of generality, we only consider the simplest case that q has only two prime factors, and believe it can be generalized to any other composite case.

This new LHL provides a flexible trade-off between the Gaussian parameter and dimension. Additionally, it can be modified slightly to achieve the leakage-resilience, assuming the conditional entropy given leakage still satisfies $m \log \sigma \geq 2\log(1/\varepsilon) + n \log q$. Compared with the GPV analysis [20], our LHL can save the Gaussian parameter at least by a factor of $\omega(\sqrt{\log \lambda})$ under the same dimension, i.e., [20] requires $m \geq 2n \log q$ and $\sigma \geq \omega(\sqrt{\log m})$.

We note that the Gaussian parameter σ in [20] needs to be greater than the smoothing parameter for other purpose besides the LHL. In particular, they need to sample from the discrete Gaussian distribution over a lattice, and σ is implicitly greater than the smoothing parameter (ref to Lemma 4.2 in [20]). However, our result above indeed improves the parameters of GPV's result without considering other purposes.

The following theorem is the case of the discrete Gaussian over ideal lattice under coefficient-embedding, which is the main focus of this paper.

Theorem 1.4 (LHL for Discrete Gaussian over Ideal Lattice) *Let R be a cyclotomic ring of integers, q be a prime number, $qR = \mathfrak{q}_1^e \mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$ be the ideal factorization of qR such that $\mathcal{N}(\mathfrak{q}_i) = q^f$ and $N = efg$. Let $\mathcal{S} = (D_{R,\sigma}^{\mathsf{coeff}})^m$ be the discrete Gaussian over the coefficients with parameter $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4m)}}$ and $mf \log \sigma \geq 2\log(1/\varepsilon) + nf \log q + \log g + m$. Then we have $\mathsf{SD}\left((\mathbf{A}, \mathbf{A}\cdot \boldsymbol{x}), U\right) \leq \varepsilon$, where $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$ and $\boldsymbol{x} \leftarrow \mathcal{S}$.*

Our LHL over ideal lattice provides a flexible trade-off between the Gaussian parameter, the module rank and the norm of the ideal factor. Similar to the first LHL, we can use the conditional entropy to analyze the case of leakage. Compared with the result in [33], our second LHL can save the Gaussian parameter at least by a factor of $\sqrt{N}$ (N is the ring dimension) under the same ring and module rank, i.e., [33] requires $m \log \frac{\sigma}{2\sqrt{N}} \geq (n + \frac{2}{N}) \log q$ and $m \geq n + \omega(\log \lambda)$ (refer more details to Lemma 2.14 and Corollary 2).

Our new LHLs are applicable to the case $\sigma = O(1)$ as long as the dimension m is sufficiently large, and can be used to analyze leakage scenarios using techniques of conditional entropy [3,7,30]. To the best of our knowledge, these are the first results without dependencies on the smoothing parameters when we consider the LHL scenario. Thus, we can answer the two main questions affirmatively.

Contribution 3. We identify an important application for proving asymptotic hardness of the extended module LWE, namely ExtMLWE, used as the main security foundation in the recent works by Lyubashevsky et al. [31] and del Pino et al. [15]. However, these prior works were not able to establish a security reduction, thus leaving the hardness of ExtMLWE as pure assumption. Particularly, our Theorem 1.4 serves as the key that leads to the following reduction, showing hardness of ExtMLWE based on the more well-studied module LWE, i.e., MLWE:

Theorem 1.5 (Asymptotic Hardness of ExtMLWE, Informal) *Assume that* MLWE *(for appropriate parameters) is hard. Then the* ExtMLWE *problem (for appropriate parameters) is also hard.*

This result enhances our confidence of their constructions [15,31], resolving an open problem in these works.

1.2 Technical Overview

We provide a technical overview of our main contributions. To start with, in order to show LHLs for discrete Gaussian over integer and ring, we rely on the standard randomness extraction approach, i.e., extracting enough randomness from the source with sufficient entropy. Thus, we need firstly determine the min-entropy of a discrete Gaussian, particularly, the min-entropy of discrete Gaussian modulo a sub-lattice, as it requires that the source mod every factor of modulus q or ideal qR has sufficient entropy for the case of arbitrary q or qR [27,30,35]. Regretfully, there is currently no literature that has explicitly calculate such lower bound. Therefore, our first technique task is to calculate the min-entropy lower bound of discrete Gaussian modulo sub-lattice.

Min-Entropy of Discrete Gaussian modulo Sub-Lattice

Let $\mathbf{\Lambda}$ and $\mathbf{\Lambda}'$ be full-rank lattices in $\mathbb{R}^n$ such that $\mathbf{\Lambda}'$ is a sub-lattice of $\mathbf{\Lambda}$. Our goal in this paper is to find an explicit lower bound for the min-entropy of the modular distribution $\mathcal{X} = (D_{\mathbf{\Lambda},\mathbf{\Sigma},\mathbf{c}} \bmod \mathbf{\Lambda}')$ for some specific but commonly used lattices $\mathbf{\Lambda}$ and $\mathbf{\Lambda}'$, for example, $\mathbf{\Lambda} = \mathbb{Z}^n$ & $\mathbf{\Lambda}' = q\mathbb{Z}^n$ for some modulus q, or $\mathbf{\Lambda} = \mathcal{O}_K$ and $\mathbf{\Lambda}' = \mathfrak{q}$ for some number field K and its $\mathcal{O}_K$-ideal $\mathfrak{q}$. To this end, we propose two approaches to evaluate the lower bound of $\mathcal{X}'s$ min-entropy.

Here is our first general approach. For simplicity, we begin with $\mathbf{\Sigma} = \sigma^2 \mathbf{I}_n$ and $\boldsymbol{c} = \mathbf{0}^n$ for some spherical gaussian with parameter $\sigma > 0$. From the definition of min-entropy, we have

$$2^{H_\infty\left(D_{\mathbf{\Lambda},\sigma} \bmod \mathbf{\Lambda}'\right)} = \frac{\rho_\sigma(\mathbf{\Lambda})}{\max\limits_{\boldsymbol{x}\in\mathbf{\Lambda}} \rho_\sigma(\mathbf{\Lambda}'+\boldsymbol{x})} \geq \frac{\rho_\sigma(\mathbf{\Lambda})}{\rho_\sigma(\mathbf{\Lambda}')} \tag{1}$$

$$= \sum_{\boldsymbol{x}\in\mathbf{\Lambda}/\mathbf{\Lambda}'} \frac{\rho_\sigma(\mathbf{\Lambda}'+\boldsymbol{x})}{\rho_\sigma(\mathbf{\Lambda}')} \geq \sum_{\boldsymbol{x}\in\mathbf{\Lambda}/\mathbf{\Lambda}'} \rho_\sigma(\boldsymbol{x}), \tag{2}$$

where $\mathbf{\Lambda}/\mathbf{\Lambda}'$ is the quotient group $\mathbf{\Lambda} \bmod \mathbf{\Lambda}'$ and $\boldsymbol{x}$ traverses one representative vector of each coset in $\mathbf{\Lambda}/\mathbf{\Lambda}'$. Inequalities (1) and (2) are owed to the gaussian inequality $\rho_\sigma(\mathcal{L})\cdot\rho_\sigma(\boldsymbol{v}) \leq \rho_\sigma(\mathcal{L}+\boldsymbol{v}) \leq \rho_\sigma(\mathcal{L})$ for all full-rank lattice $\mathcal{L}$ and vector $\boldsymbol{v} \in \mathbb{R}^n$ (see lemma 2.3). For a single coset $\boldsymbol{v} + \mathbf{\Lambda}' \in \mathbf{\Lambda}/\mathbf{\Lambda}'$, the representative element $\boldsymbol{x}$ of $\boldsymbol{v} + \mathbf{\Lambda}' \in \mathbf{\Lambda}/\mathbf{\Lambda}'$ is not unique, and we wish its norm to be as small as possible in order to make the Gaussian $\rho_\sigma(\boldsymbol{x})$ reach its maximum among $\boldsymbol{x} \in \boldsymbol{v} + \mathbf{\Lambda}'$. Hence our goal can be reduced to first finding a low-norm representative of each coset in the quotient group $\mathbf{\Lambda}/\mathbf{\Lambda}'$ and second estimating a lower bound of $\rho_\sigma(\mathbf{\Lambda}/\mathbf{\Lambda}')$.

To this end, we apply the *Hermite Normal Form Decomposition* [19], which tells us that every nonsingular integer matrix can be transformed to an integer upper triangular matrix via elementary column operations. For general pairs of n-dim full-rank lattice $\mathbf{\Lambda} = \mathcal{L}(\mathbf{B})$ and its full-rank sub-lattice $\mathbf{\Lambda}' = \mathcal{L}(\mathbf{B}')$ such that $\mathbf{B}' = \mathbf{B}\cdot\mathbf{M}$ for some nonsingular integer matrix $\mathbf{M} \in \mathbb{Z}^{n\times n}$, we can decompose $\mathbf{M}$ to $\mathbf{M} = \mathbf{TP}$ for an upper triangular matrix $\mathbf{T} \in \mathbb{Z}^{n\times n}$ with diagonal elements $(t_i)_{i\in[n]}$ and a unimodular matrix $\mathbf{P}$. Then $\mathbf{B}\cdot\mathbf{T}$ can also be a basis of $\mathbf{\Lambda}'$. Then we can rewrite the quotient group as[5]

$$\mathbf{\Lambda}/\mathbf{\Lambda}' = \mathbf{B}\cdot(\mathbb{Z}^n/\mathbf{T}\cdot\mathbb{Z}^n) = \mathbf{B}\cdot\{\boldsymbol{t} + \mathbf{T}\cdot\mathbb{Z}^n \mid \boldsymbol{t} \in (\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top\}.$$

Therefore, we successfully find explicit coset representatives of $\mathbf{\Lambda}/\mathbf{\Lambda}'$ to be $\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top$, yielding that

$$2^{H_\infty\left(D_{\mathbf{\Lambda},\sigma} \bmod \mathbf{\Lambda}'\right)} \geq \rho_\sigma(\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top)$$
$$= \rho_{\sigma/\|\mathbf{B}\|_2}((\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top) = \prod_{i=1}^n \rho_{\sigma/\|\mathbf{B}\|_2}(\mathbb{Z}_{t_i}).$$

We further consider the case of ideal lattices, i.e. $\mathbf{\Lambda} = R$ and $\mathbf{\Lambda}' = \mathcal{I}$, where $R = \mathcal{O}_K$ is the ring of integers of a number field $K = \mathbb{Q}[\zeta]$, and $\mathcal{I}$ is an R-ideal. It's a problem to identify a proper structure of $R/\mathcal{I}$ for general R and $\mathcal{I}$. If $\mathcal{I}$ is a prime ideal factor of qR with norm $N(\mathcal{I}) = q^f$ where q is a prime number, then $\mathcal{I}$ is generated by two elements, i.e. $\mathcal{I} = \langle q, F_\mathcal{I}(\zeta)\rangle$ for some f-degree polynomial $F_\mathcal{I}$ with integer coefficients, by Dedekind theorem. From this approach, a question is raised whether there exist similar properties for more general ideal $\mathcal{I}$? Our new

[5] We define the set $\mathbb{Z}_q$ to be integers in $(-q/2, q/2]$ for modulus $q \geq 2$.

observation is that we can extend Dedekind theorem to every ideal factor $\mathcal{I}$ of qR where q is a prime number and $\mathcal{N}(\mathcal{I}) = q^t$ for $1 \le t \le N$, such that $\mathcal{I} = \langle q, F_{\mathcal{I}}(\zeta)\rangle$ for some t-degree integer-coefficient polynomial $F_{\mathcal{I}}$. This shows that each coset of $R/\mathcal{I}$ has a representative $\sum_{i=0}^{t-1} a_i\zeta^i$ for some $a_i \in \mathbb{Z}_q$, indicating that the quotient ring $R/\mathcal{I}$ is isomorphic to $\mathbb{Z}_q^t \times \{0\}^{N-t}$ via the coefficient embedding mapping ϕ. Let $D_{R,\sigma}^{\mathsf{coeff}}$ denote the discrete Gaussian distribution sampling from the coefficient lattice $\phi(R)$ with parameter σ. Therefore, we can obtain a lower bound for the min-entropy of the distribution $D_{R,\sigma}^{\mathsf{coeff}} \bmod \mathcal{I}$:

$$\begin{aligned} H_\infty\left(D_{R,\sigma}^{\mathsf{coeff}} \bmod \mathcal{I}\right) &\ge \log\left(\rho_\sigma^{\mathsf{coeff}}(R/\mathcal{I})\right) = \log\left(\rho_\sigma(\phi(R)/\phi(\mathcal{I}))\right) \\ &\ge \log\left(\rho_\sigma(\mathbb{Z}_q^t)\right) \approx t\log\sigma. \end{aligned}$$

Our second approach is inspired by a lemma from Lyubashevsky, Peikert and Regev [33, Claim 7.1], which stated that for any n-dimensional lattice $\mathbf{\Lambda}$ and $\varepsilon, \sigma > 0$, we have

$$\rho_{1/\sigma}(\mathbf{\Lambda}) \le (1+\varepsilon)\cdot \max\{1, \eta_\varepsilon(\mathbf{\Lambda}^\vee)/\sigma\}^n.$$

Let $\mathcal{X} = (D_{\mathbf{\Lambda},\sigma,\boldsymbol{c}} \bmod \mathbf{\Lambda}')$ for some full rank n-dimensional lattices $\mathbf{\Lambda}$ and $\mathbf{\Lambda}' \subseteq \mathbf{\Lambda}$. Since $H_\infty(\mathcal{X}) = -\log\left(\max_{\boldsymbol{x}\in\mathbf{\Lambda}} \frac{\rho_\sigma(\mathbf{\Lambda}'+\boldsymbol{x}-\boldsymbol{c})}{\rho_\sigma(\mathbf{\Lambda}-\boldsymbol{c})}\right)$ From the properties of smoothing parameter and the lemma above, for $\sigma \ge \eta_\varepsilon(\mathbf{\Lambda})$, we can compute that

$$\begin{aligned} \rho_\sigma(\mathbf{\Lambda}'+\boldsymbol{x}-\boldsymbol{c}) &\le \rho_\sigma(\mathbf{\Lambda}') = \frac{\sigma^n}{\det\mathbf{\Lambda}'}\cdot\rho_{1/\sigma}((\mathbf{\Lambda}')^\vee) \le \frac{\sigma^n}{\det\mathbf{\Lambda}'}\cdot(1+\varepsilon)\cdot\max\{1,\eta_\varepsilon(\mathbf{\Lambda}')/\sigma\}^n \\ \rho_\sigma(\mathbf{\Lambda}-\boldsymbol{c}) &\ge (1-\varepsilon)\cdot\frac{\sigma^n}{\det\mathbf{\Lambda}}, \end{aligned}$$

Therefore, we have

$$H_\infty(\mathcal{X}) \ge \log\frac{\det\mathbf{\Lambda}'}{\det\mathbf{\Lambda}} - n\log\left(\max\{1,\eta_\varepsilon(\mathbf{\Lambda}')/\sigma\}\right) - \log\frac{1+\varepsilon}{1-\varepsilon}$$

It should be noted that (1) this min-entropy result is consistent with the smoothing lemma from [38, Lemma 4.1] and [20, Corollary 2.8], since for $\sigma \ge \eta_\varepsilon(\mathbf{\Lambda}')$, we have $H_\infty(\mathcal{X}) \ge \log\frac{\det\mathbf{\Lambda}'}{\det\mathbf{\Lambda}} - \log\frac{1+\varepsilon}{1-\varepsilon}$ which almost reaches the full min-entropy of $\mathbf{\Lambda}/\mathbf{\Lambda}'$ and this lower bound can improve several previous analyses such as [45, Lemma 3.8]; (2) Many cases are fit in our second approach. We take the q-ary case $\mathbf{\Lambda} = \mathbf{\Lambda}^\perp(\mathbf{A})$ and $\mathbf{\Lambda}' = q\mathbb{Z}^m$ for some $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and the ring case $\mathbf{\Lambda} = \sigma(R)$ and $\mathbf{\Lambda}' = \sigma(\mathfrak{q})$ for some ring of integers R and its ideal $\mathfrak{q}$ as two examples. Please refer more details to Corollary 8 and Corollary 9.

Improving LHL of Discrete Gaussian over Ideal Lattice

Based on our new min-entropy lower bound of discrete Gaussian mod q-ary lattice, we can obtain a LHL for discrete Gaussian over integer lattice by combining the standard LHL. For the case of discrete Gaussian over ideal lattice, we can derive a LHL with more tight parameters compared with directly applying Corollary 5.7 in [30]. In order to illustrate our new insight, we start with a recap of the proof strategy of Corollary 5.7 in [30].

The proof in [30] is based on the basic *algebraic leftover hash lemma* in [30], which says that

$$\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \boldsymbol{s}), (\mathbf{A}, \boldsymbol{u})) \leq \frac{1}{2}\sqrt{\sum_{\mathfrak{q}|qR} \mathcal{N}(\mathfrak{q})^n \cdot \mathsf{Col}(\mathcal{S} \bmod \mathfrak{q}) - 1}, \tag{3}$$

where $\mathbf{A} \leftarrow U(R_q^{n\times m})$ and $\boldsymbol{u} \leftarrow U(R_q^m)$ are sampled uniformly at random, and $\mathcal{S}$ is a distribution over R_q^m and has sufficient entropy modulo each ideal factor $\mathfrak{q}$. It needs to further upper bound the term $\sum_{\mathfrak{q}|qR} \mathcal{N}(\mathfrak{q})^n \cdot \mathsf{Col}(\mathcal{S} \bmod \mathfrak{q})$ via the min-entropy of $\mathcal{S} \bmod \mathfrak{q}$. Their strategy is to directly upper bound $\mathsf{Col}(\mathcal{S} \bmod \mathfrak{q})$ by the worst case, i.e., $\mathsf{Col}(\mathcal{S} \bmod \mathfrak{q}) \leq 1/2^{H_\infty(\mathcal{S} \bmod \mathfrak{q})} \leq \frac{1}{2^e}$ for any ideal $\mathfrak{q}|qR$, and then upper bound $\frac{1}{2^e} \cdot \sum_{\mathfrak{q}|qR} \mathcal{N}(\mathfrak{q})^n \leq \frac{q^{2nN}}{2^e}$. Therefore, they require the min-entropy of $\mathcal{S} \bmod \mathfrak{q}$ greater than $nN \log q$. This constraint will produce quite large Gaussian parameters if the ideal qR is splitted into many R-ideals.

Our new insight is a more tight upper bound of the term $\sum_{\mathfrak{q}|qR} \mathcal{N}(\mathfrak{q})^n \cdot \mathsf{Col}(\mathcal{S} \bmod \mathfrak{q})$, which only requires q^n/σ^m to be negligible. We observe that if the min-entropy lower bound of $\mathcal{S} \bmod \mathfrak{q}$ has somewhat linear relationship with t for $N(\mathfrak{q}) = q^t$, then we can obtain a more tight upper bound of $\sum_{\mathfrak{q}|qR} \mathcal{N}(\mathfrak{q})^n \cdot \mathsf{Col}(\mathcal{S} \bmod \mathfrak{q})$. Take a simple case of q unramified over R and qR full-splitting ($qR = \mathfrak{q}_1 \cdots \mathfrak{q}_N$ and every prime ideal factor $\mathfrak{q}$ of qR has norm q) as an example. We can upper bound $\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \boldsymbol{s}), (\mathbf{A}, \boldsymbol{u}))$ as follows:

$$\begin{aligned}
&\mathsf{SD}((\mathbf{A}, \mathbf{A} \cdot \boldsymbol{s}),\, (\mathbf{A}, \boldsymbol{u})) && (4)\\
\leq\ & \frac{1}{2}\sqrt{\sum_{\mathfrak{q}|qR} \mathcal{N}(\mathfrak{q})^n \cdot \mathsf{Col}\left((D_{R,\sigma}^{\mathsf{coeff}})^m \bmod \mathfrak{q}\right) - 1} \\
=\ & \frac{1}{2}\sqrt{\sum_{i_1,\cdots,i_N \in \{0,1\}} \mathcal{N}(\mathfrak{q}_1^{i_1} \cdots \mathfrak{q}_N^{i_N})^n \cdot \mathsf{Col}\left((D_{R,\sigma}^{\mathsf{coeff}})^m \bmod \mathfrak{q}_1^{i_1} \cdots \mathfrak{q}_N^{i_N}\right) - 1} \\
\leq\ & \frac{1}{2}\sqrt{\sum_{i_1,\cdots,i_N \in \{0,1\}} q^{n(i_1 + \cdots i_N)} \cdot 2^{-(i_1+\cdots i_N)m\log\sigma} - 1} && (5)\\
=\ & \frac{1}{2}\sqrt{\left(\sum_{i_1 \in \{0,1\}} \left(\frac{q^n}{\sigma^m}\right)^{i_1}\right) \cdots \left(\sum_{i_N \in \{0,1\}} \left(\frac{q^n}{\sigma^m}\right)^{i_N}\right) - 1} \ (\text{let } \varepsilon = \frac{q^n}{\sigma^m}) \\
=\ & \frac{1}{2}\sqrt{(1+\varepsilon)^N - 1} \leq \sqrt{N\varepsilon}
\end{aligned}$$

where $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$, $\boldsymbol{s} \leftarrow (D_{R,\sigma}^{\mathsf{coeff}})^m$ and $\boldsymbol{u} \xleftarrow{\$} R_q^n$. Inequality (5) is due to the fact that collision probability is less than or equal to the maximal probability of a random variable. This result implies that if $m \log \sigma \geq n \log q + \omega(\log \lambda)$, the statistical distance between $(\mathbf{A}, \mathbf{A} \cdot \boldsymbol{s})$ and uniform random is negligible.

From our new proof of LHL for discrete Gaussian over ideal lattice, we propose a strategy for how to use the algebraic leftover hash lemma even if qR is splitting into many prime ideals. For certain distribution $\mathcal{S}$, the goal is to find a linear function $f(x) = a \cdot x - \delta$ s.t. for each ideal factor $\mathfrak{q}$ of qR with norm $\mathcal{N}(\mathfrak{q}) = q^t$, $H_\infty(\mathcal{S} \bmod \mathfrak{q}) \geq f(t)$. We refer more details to lemma 5.3.

2 Preliminary

Notations Let λ denote the security parameter. For an integer n, let $[n]$ denote the set $\{1, ..., n\}$. We use bold lowercase letters (e.g. $\boldsymbol{a}$) to denote vectors and bold capital letters (e.g. $\mathbf{A}$) to denote matrices. We write $\mathbf{e} = \exp(1)$ as the natural constant. For a positive integer $q \geq 2$, let $\mathbb{Z}_q$ be the ring of integers modulo q where each number is located in $(-q/2, q/2]$. For any $c \in (-1/2, 1/2]$, let $\mathbb{Z}_q + c = (\mathbb{Z} + c) \cap (-q/2, q/2]$ (note that whether q is odd or even, this set has size q). For a distribution on a set X, we write $x \stackrel{\$}{\leftarrow} X$ to denote the operation of sampling a random x according to X. For distributions X, Y, we let $\mathsf{SD}(X, Y)$ denote their statistical distance. We write $X \stackrel{s}{\approx} Y$ or $X \stackrel{c}{\approx} Y$ to denote statistical closeness or computational indistinguishability, respectively. We use $\mathsf{negl}(\lambda)$ to denote the set of all negligible functions $\mu(\lambda) = \lambda^{-\omega(1)}$. We write $r\mathcal{B}_n^p$ as the n-dimensional unit ball with radius r related to p-th norm, i.e. $r\mathcal{B}_n^p = \{\boldsymbol{x} \in \mathbb{R}^n \mid \|\boldsymbol{x}\|_p \leq r\}$ for $p \in [1, \infty]$ and $r > 0$.

A unimodular matrix $\mathbf{U} \in \mathbb{Z}^{n \times n}$ satisfies $\det \mathbf{U} = \pm 1$; in particular, $\mathbf{U}^{-1} \in \mathbb{Z}^{n \times n}$ is also a unimodular matrix. The spectual norm of a matrix $\mathbf{X} \in \mathbb{R}^{n \times k}$ is its largest singular value $s_1(\mathbf{X})$. The length of a matrix $\mathbf{X}$ is the norm of its longest column $\|\mathbf{X}\| = \max_i \|\boldsymbol{x}_i\|$. For any (ordered) set $\mathbf{S} = \{\boldsymbol{s}_1, \cdots, \boldsymbol{s}_n\} \subseteq \mathbb{R}^n$ of linearly independent vectors, let $\widetilde{\mathbf{S}} = \{\widetilde{\boldsymbol{s}_1}, \cdots, \widetilde{\boldsymbol{s}_n}\}$ denote its Gram-Schmidt orthogonalization [20].

The *min-entropy* of a random variable X is $H_\infty(X) \stackrel{\text{def}}{=} -\log(\max_x \Pr[X = x])$, which measures the maximal probability of elements in X. The *conditional min-entropy* of X conditioned on Z is $H_\infty(X \mid Z) \stackrel{\text{def}}{=} -\log(\mathbb{E}_{z \leftarrow Z}[\max_x \Pr[X = x \mid Z = z]])$, which measures the best guess for X given a correlated random variable Z. The following lemma says that the min-entropy drops by at most ℓ bits if conditioning on ℓ bits of information.

Lemma 2.1 ([18]) *Let X, Y, Z be arbitrary (correlated) random variables where the support of Z is of size at most 2^ℓ. Then $H_\infty(X \mid Y, Z) \geq H_\infty(X \mid Y) - \ell$.*

2.1 Lattices

A lattice $\mathbf{\Lambda} \subset \mathbb{R}^n$ is the set of all integer linear combinations of t linearly independent basis vectors $\mathbf{B} = (\boldsymbol{b}_1, \cdots, \boldsymbol{b}_t) \in \mathbb{R}^{n \times t}$, i.e., $\mathbf{\Lambda} = \mathbf{B} \cdot \mathbb{Z}^t$. We call t the rank of the lattice. If $t = n$, we call $\mathbf{\Lambda}$ a full-rank lattice.

A lattice is a discrete additive subgroup of $\mathbf{R}^n$. For sub-lattice $\mathbf{\Lambda}' \subseteq \mathbf{\Lambda}$, the quotient group $\mathbf{\Lambda}/\mathbf{\Lambda}'$ is well-defined as the additive group of distinct cosets $\boldsymbol{v} + \mathbf{\Lambda}'$ for $\boldsymbol{v} \in \mathbf{\Lambda}$. The vector $\boldsymbol{v}$ is called the coset representative of $\boldsymbol{v} + \mathbf{\Lambda}'$.

The length of the shortest non-zero vector in L_p norm of a lattice $\mathbf{\Lambda}$ is denoted as $\lambda_1^p(\mathbf{\Lambda}) := \min_{\boldsymbol{x}\in\mathbf{\Lambda}/\{0\}} \|\boldsymbol{x}\|_p$. The dual lattice of $\mathbf{\Lambda}$ is defined as $\mathbf{\Lambda}^\vee := \{\boldsymbol{y} \in \mathbb{R}^n \mid \langle \boldsymbol{y}, \mathbf{\Lambda}\rangle \subseteq \mathbb{Z}\}$, i.e., the set of all vectors that have integer inner product with all lattice vectors in $\mathbf{\Lambda}$. It is easy to see that $(\mathbf{\Lambda}^\vee)^\vee = \mathbf{\Lambda}$. For a lattice $\mathbf{\Lambda}$ and its one set of basis $\mathbf{B} \in \mathbb{R}^{n\times n}$, the set $\mathcal{P}(\mathbf{B}) := \mathbf{B} \cdot [-1/2, 1/2)^n$ is called the fundamental parallelepiped defined by the basis. For a point $\boldsymbol{c} \in \mathbb{R}^n$, we write $\boldsymbol{c}' := \boldsymbol{c} \bmod \mathcal{P}(\mathbf{B})$ for the unique element $\boldsymbol{c}'$ s.t. $\boldsymbol{c} = \boldsymbol{c}' + \boldsymbol{x}$ for some lattice point $\boldsymbol{x} \in \mathbf{\Lambda}$. Equivalently, if $\boldsymbol{c} = \mathbf{B} \cdot \boldsymbol{v}$ for $\boldsymbol{v} \in \mathbb{R}^n$, then $\boldsymbol{c} \bmod \mathcal{P}(\mathbf{B}) = \mathbf{B} \cdot (\boldsymbol{x} - \lfloor \boldsymbol{x} \rceil)$. A set of linearly independent vectors $\boldsymbol{y}_1, \cdots, \boldsymbol{y}_k \in \mathbf{\Lambda}$ is primitive with respect to $\mathbf{\Lambda}$ if $\forall \boldsymbol{t} \in \mathbb{R}^k$, $(\boldsymbol{y}_1, \cdots, \boldsymbol{y}_k) \cdot \boldsymbol{t} \in \mathbf{\Lambda}$ iff $\boldsymbol{t} \in \mathbb{Z}^k$. We have the following basis extension theorem in lattices:

Lemma 2.2 (Theorem 7 in [13]) *Let $\mathbf{\Lambda} \subset \mathbb{R}^n$ be a $k \geq 1$ dimensional lattice. Given $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_i \in \mathbf{\Lambda}$ primitive with respect to $\mathbf{\Lambda}$, there exists $\boldsymbol{b}_{i+1}, \cdots, \boldsymbol{b}_k \in \mathbf{\Lambda}$ such that the extension $\boldsymbol{b}_1, \cdots, \boldsymbol{b}_k$ is a basis of $\mathbf{\Lambda}$.*

Let $\mathbf{A} \in \mathbb{Z}^{n\times m}$ for some positive integers n, m and we define two lattices given by $\mathbf{A}$,

$$\begin{aligned}\mathbf{\Lambda}(\mathbf{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{y} = \mathbf{A}^\top \cdot \boldsymbol{s} \text{ for some } \boldsymbol{s} \in \mathbb{Z}^n\}\\ \mathbf{\Lambda}^\perp(\mathbf{A}) &= \{\boldsymbol{e} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \boldsymbol{e} = 0\},\end{aligned}$$

and two q-ary lattices given by $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ for some positive modulus q:

$$\begin{aligned}\mathbf{\Lambda}_q(\mathbf{A}) &= \{\boldsymbol{y} \in \mathbb{Z}^m \mid \boldsymbol{y} = \mathbf{A}^\top \cdot \boldsymbol{s} \mod q \text{ for some } \boldsymbol{s} \in \mathbb{Z}_q^n\}\\ \mathbf{\Lambda}_q^\perp(\mathbf{A}) &= \{\boldsymbol{e} \in \mathbb{Z}^m \mid \mathbf{A} \cdot \boldsymbol{e} = 0 \mod q\}.\end{aligned}$$

2.2 Gaussian Distribution

We define the Gaussian function on $\mathbb{R}^n$ with Gaussian parameter $\sigma > 0$ centered at $\boldsymbol{c} \in \mathbb{R}^n$ as $\rho_{\sigma,\boldsymbol{c}} : \mathbb{R}^n \to (0, 1]$:

$$\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \exp(-\pi\|\boldsymbol{x} - \boldsymbol{c}\|^2/\sigma^2).$$

We define the discrete Gaussian distribution on a n-dimensional full rank lattices $\mathbf{\Lambda}$ centered at $\boldsymbol{c} \in \mathbb{R}^n$ with Gaussian parameter $\sigma > 0$ as $D_{\mathbf{\Lambda},\sigma,\boldsymbol{c}} : \mathbf{\Lambda} \to (0, 1]$:

$$D_{\mathbf{\Lambda},\sigma,\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\mathbf{\Lambda})}.$$

The subscripts σ and $\boldsymbol{c}$ are taken to be 1 and $\mathbf{0}$ respectively when omitted. We denote $D_{\mathbf{\Lambda},\sigma,\boldsymbol{c},\leq r}$ as the truncated Gaussian distribution by sampling $\boldsymbol{x} \leftarrow D_{\mathbf{\Lambda},\sigma,\boldsymbol{c}}$, rejecting if $\|\boldsymbol{x}\| > r$, and sampling $\boldsymbol{x}$ again until success and outputing $\boldsymbol{x}$. Truncated Gaussian density is defined as:

$$D_{\mathbf{\Lambda},\sigma,\boldsymbol{c},\leq r}(\boldsymbol{x}) = \begin{cases} \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\mathbf{\Lambda}\cap r\mathcal{B}_n^2)}, & \text{if } \|\boldsymbol{x}\| \leq r;\\ 0, & \text{if } \|\boldsymbol{x}\| > r.\end{cases}$$

For a positive definite matrix $\mathbf{\Sigma}$, we define the non-spherical Gaussian function on $\mathbb{R}^n$ centered at $\boldsymbol{c} \in \mathbb{R}^n$ with matrix parameter $\sqrt{\mathbf{\Sigma}}$ as

$$\rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\boldsymbol{x}) = \exp\left(-\pi(\boldsymbol{x}-\boldsymbol{c})^\top \mathbf{\Sigma}^{-1}(\boldsymbol{x}-\boldsymbol{c})\right) = \exp\left(-\pi \left\| \sqrt{\mathbf{\Sigma}}^{-1}(\boldsymbol{x}-\boldsymbol{c}) \right\|^2\right).$$

For a positive definite matrix $\mathbf{\Sigma}$, we define the discrete Gaussian distribution on a n-dimensional full rank lattices $\mathbf{\Lambda}$ centered at $\boldsymbol{c} \in \mathbb{R}^n$ with matrix parameter $\sqrt{\mathbf{\Sigma}}$ as $D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}} : \mathbf{\Lambda} \to (0,1]$:

$$D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\boldsymbol{x}) = \frac{\rho_{\sigma,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{\sigma,\boldsymbol{c}}(\mathbf{\Lambda})}.$$

Lemma 2.3 ([14], Lemma 3) *For a full rank lattice $\mathbf{\Lambda} \subseteq \mathbb{R}^n$, $\sigma > 0$ and $\boldsymbol{c} \in \mathbb{R}^n$, we have*

$$\rho_\sigma(\mathbf{\Lambda}) \cdot \rho_\sigma(\boldsymbol{c}) \leq \rho_{\sigma,\boldsymbol{c}}(\mathbf{\Lambda}) \leq \rho_\sigma(\mathbf{\Lambda}).$$

We take $\sigma = 1$, $\mathbf{\Lambda} \leftarrow \sqrt{\mathbf{\Sigma}}^{-1}\mathbf{\Lambda}$ and $\boldsymbol{c} \leftarrow \sqrt{\mathbf{\Sigma}}^{-1}\boldsymbol{c}$ in lemma 2.3 to obtain the generalized corollary:

Corollary 1. *For a full rank lattice $\mathbf{\Lambda} \subseteq \mathbb{R}^n$, positive definite matrix $\mathbf{\Sigma} \in \mathbb{R}^{n\times n}$ and $\boldsymbol{c} \in \mathbb{R}^n$, we have*

$$\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}) \cdot \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{c}) \leq \rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda}) \leq \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}).$$

The following two tail bounds by Banaszczyk are useful when dealing with truncated Gaussian sums.

Lemma 2.4 ([5], Lemma 2.8) *For any n-dimensional lattice $\mathbf{\Lambda}$ and radius $r \geq \sqrt{n/2\pi}$,*

$$\frac{\rho(\mathbf{\Lambda} \backslash r\mathcal{B}_n^2)}{\rho(\mathbf{\Lambda})} < \left(\frac{2\pi \mathrm{e}}{n}\right)^{n/2} r^n \exp(-\pi r^2).$$

Lemma 2.5 ([5], Lemma 2.10) *For any n-dimensional lattice $\mathbf{\Lambda}$, center $\boldsymbol{v} \in \mathbb{R}^n$ and radius $r > 0$,*

$$\frac{\rho((\mathbf{\Lambda} - \boldsymbol{v}) \backslash r\mathcal{B}_n^\infty)}{\rho(\mathbf{\Lambda})} < 2n \cdot \exp(-\pi r^2).$$

2.3 Smoothing Parameter

We will recall the definition of smoothing parameter and its useful properties from [20, 38, 41].

Definition 2.6 (Smoothing Parameter [38]) *For lattice $\mathbf{\Lambda} \subseteq \mathbb{R}^n$ and any $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\mathbf{\Lambda})$ is the smallest real $s > 0$ such that $\rho_{1/s}(\mathbf{\Lambda}^\vee) \leq 1 + \varepsilon$. For an invertible matrix $\mathbf{B} \in \mathbb{R}^{n\times n}$, we say that $\eta_\varepsilon(\mathbf{\Lambda}) \leq \mathbf{B}$ if $\eta_\varepsilon(\mathbf{B}^{-1}\mathbf{\Lambda}) \leq 1$.*

Lemma 2.7 (Generalization of Corollary 2.8 [20]) *Let $\mathbf{\Lambda}, \mathbf{\Lambda}'$ be n-dimensional lattices with $\mathbf{\Lambda}' \subseteq \mathbf{\Lambda}$. For any $\varepsilon \in (0, 1/2)$, $\sqrt{\mathbf{\Sigma}} \geq \eta_\varepsilon(\mathbf{\Lambda}')$ and $\boldsymbol{c} \in \mathbb{R}^n$, we have*

$$\mathsf{SD}(D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}} \bmod \mathbf{\Lambda}, U(\mathbf{\Lambda} \bmod \mathbf{\Lambda}')) \leq 2\varepsilon.$$

Lemma 2.8 (Lemma 3.5 [41]) *For any $p \in [1, \infty]$, any n-dimensional lattice $\mathbf{\Lambda}$, and any $\varepsilon > 0$,*

$$\eta_\varepsilon(\mathbf{\Lambda}) \leq \frac{\sqrt{\ln(2n(1+1/\varepsilon))/\pi}}{\lambda_1^\infty(\mathbf{\Lambda}^\vee)} \leq \frac{n^{1/p} \cdot \sqrt{\ln(2n(1+1/\varepsilon))/\pi}}{\lambda_1^p(\mathbf{\Lambda}^\vee)}.$$

Lemma 2.9 (Lemma 3.1 [20]) *For any n-dimensional lattice $\mathbf{\Lambda}$, any basis $\mathbf{B}$ of $\mathbf{\Lambda}$, and any $\varepsilon > 0$,*

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

Lemma 2.10 (Implicit in Lemma 4.4 [38]) *Let $\mathbf{\Lambda}$ be an n-dimensional lattice. For any $\varepsilon > 0$, positive definite matrix $\mathbf{\Sigma}$ such that $\sqrt{\mathbf{\Sigma}} \geq \eta_\varepsilon(\mathbf{\Lambda})$ and $\boldsymbol{c} \in \mathbb{R}^n$, we have*

$$\frac{\sqrt{\det \mathbf{\Sigma}}}{\det(\mathbf{\Lambda})} \leq \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}) \leq (1+\varepsilon) \cdot \frac{\sqrt{\det \mathbf{\Sigma}}}{\det(\mathbf{\Lambda})},$$
$$(1-\varepsilon) \cdot \frac{\sqrt{\det \mathbf{\Sigma}}}{\det(\mathbf{\Lambda})} \leq \rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda}) \leq (1+\varepsilon) \cdot \frac{\sqrt{\det \mathbf{\Sigma}}}{\det(\mathbf{\Lambda})}.$$

Lemma 2.11 (Claim 7.1 [33]) *For any n-dimensional lattice $\mathbf{\Lambda}$ and $\varepsilon, \sigma > 0$,*

$$\rho_{1/\sigma}(\mathbf{\Lambda}) \leq (1+\varepsilon) \cdot \max\left\{1, \left(\frac{\eta_\varepsilon(\mathbf{\Lambda}^\vee)}{\sigma}\right)^n\right\}.$$

Lemma 2.12 (Adapted from Corollary 5.4 in [20] and Lemma 18 in [10]) *Let $q \geq 2$ and $m \geq 2n \log q$. For all but at most $q^{-0.16n}$ fraction of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, we have $\lambda_1^\infty(\mathbf{\Lambda}_q(\mathbf{A})) \geq q/4$. For such $\mathbf{A}$ and any $\sigma \geq 4\sqrt{\ln(2m(1+\frac{1}{\varepsilon}))/\pi}$, the statistical distance between the marginal distribution of $\boldsymbol{u} = \mathbf{A}\boldsymbol{s}$ and $U(\mathbb{Z}_q^n)$ is within 2ε.*

Gaussians over Ideal Lattices

We will describe the discrete gaussian distributions over fractional ideal $\mathcal{I}$ under coefficient embedding $\phi : K \to \mathbb{Q}$ and canonical embedding $\sigma : K \to H$. For more detailed introductions to algebraic number theory, please refer to Appendix

For any positive definite matrix $\mathbf{\Sigma}$ and element $t \in K_\mathbb{R}$, we define the discrete Gaussian over coefficient lattice as $D^{\mathsf{coeff}}_{\mathcal{I},\sqrt{\mathbf{\Sigma}},t}$ (respectively, $D^{\mathsf{coeff}}_{\mathcal{I},\sqrt{\mathbf{\Sigma}},t,\leq r}$) to be a discrete Gaussian (respectively, truncated gaussian) distribution on coefficients, by taking the coefficients as a lattice in $\mathbb{R}^n$, i.e. sampling $\phi(a) \leftarrow D_{\phi(\mathcal{I}),\sqrt{\mathbf{\Sigma}},\phi(t)}$ (respectively, $D_{\phi(\mathcal{I}),\sqrt{\mathbf{\Sigma}},\phi(t),\leq r}$) and output a. We define $D^{\mathsf{coeff}}_{K_\mathbb{R},\sqrt{\mathbf{\Sigma}},t}$ to be a continuous Gaussian over $K_\mathbb{R}$ where we sample Gaussian vector in the coefficient space, and the probability density function is defined as $D^{\mathsf{coeff}}_{K_\mathbb{R},\sqrt{\mathbf{\Sigma}},t}(a) = D_{\mathbb{R}^N,\sqrt{\mathbf{\Sigma}},\phi(t)}(\phi(a))$.

We also define the discrete Gaussian over canonical lattice by $D_{\mathcal{I},\sqrt{\mathbf{\Sigma}},t}(a) = D_{\sigma(\mathcal{I}),\sqrt{\mathbf{\Sigma}},\sigma(t)}(\sigma(a))$ and $D_{\mathcal{I},\sqrt{\mathbf{\Sigma}},t,\leq r}(a) = D_{\sigma(\mathcal{I}),\sqrt{\mathbf{\Sigma}},\sigma(t),\leq r}(\sigma(a))$ for all $a \in \mathcal{I}$ to be the gaussian distribution and truncated gaussian distribution on canonical embedding. Similarly, we define the continuous Gaussian over canonical space by $D_{K_{\mathbb{R}},\sqrt{\mathbf{\Sigma}},t}(a) = D_{H,\sqrt{\mathbf{\Sigma}},\sigma(t)}(\sigma(a))$

Since there exists a direct linear map from $\phi(a)$ to $\sigma(a)$ by $\sigma(a) = \mathbf{V}_f\phi(x)$ for all $x \in K$, we have $D_{\mathcal{I},\mathbf{V}_f\sqrt{\mathbf{\Sigma}},t}(a) = D^{\mathsf{coeff}}_{\mathcal{I},\sqrt{\mathbf{\Sigma}},t}(a)$ for all $a \in K$. Particularly, if K is M-th cyclotomic number field where M is a prime number or power of 2, $D_{\mathcal{I},\sqrt{N}\sigma,t}(a) = D^{\mathsf{coeff}}_{\mathcal{I},\sigma,t}(a)$ and $D_{\mathcal{I},\sqrt{N}\sigma,t,\leq\sqrt{N}r}(a) = D^{\mathsf{coeff}}_{\mathcal{I},\sigma,t,\leq r}(a)$ for all $a \in \mathcal{I}$ and $r > 0$ (i.e. for spherical gaussian, the gaussian parameter in canonical embedding is $\sqrt{N}$ times of the gaussian parameter in coefficient embedding).

With the definition of discrete Gaussian over ideal lattice, we need the following regularity lemma from [33] to show the advantage of our new regularity lemma. It is worth to note that the discrete Gaussian distribution in their regularity lemma is sampled over the canonical lattice $\sigma(R)$ with respect to Gaussian parameter σ.

Lemma 2.13 (Corollary 7.5 [33]) *Let $K = \mathbb{Q}[\zeta]$ be the M-th cyclotomic field with degree $N = \varphi(M)$. Let $\sigma > 2N \cdot q^{\frac{n}{m}+\frac{2}{mN}}$ be a Gaussian parameter. Let n, m, q be lattice parameters. Assume that $\mathbf{A} = [\mathbf{I}_n \mid \bar{\mathbf{A}}] \in R_q^{n\times m}$ where $\bar{\mathbf{A}} \xleftarrow{\$} R_q^{n\times(m-n)}$. With probability $1 - 2^{-\Omega(N)}$ over the choice of $\bar{\mathbf{A}}$, the distribution of $\mathbf{A}\boldsymbol{s} \in R_q^n$ where $\boldsymbol{s} \leftarrow (D_{R,\sigma})^m$ is within statistical distance $2^{-\Omega(N)}$ of $U(R_q^n)$.*

Micciancio and Suhl proposed a transformation from a LWE instance to a Knapsack instance [39, Lemma 20]. We can generalize it to ring case, where the function maps $([\mathbf{I}_n \mid \bar{\mathbf{A}}], [\mathbf{I}_n \mid \bar{\mathbf{A}}]\cdot\boldsymbol{s}) \in R_q^{n\times m}\times R_q^n$ to $(\mathbf{A}', \mathbf{A}'\cdot\boldsymbol{s}) \in R_q^{n\times m}\times R_q^n$, and $([\mathbf{I}_n \mid \bar{\mathbf{A}}], \boldsymbol{b})$ to $(\mathbf{A}', \boldsymbol{b}')$ such that $(\bar{\mathbf{A}}, \boldsymbol{b})$, $(\mathbf{A}', \boldsymbol{b}')$ are closed uniform distribution respectively and $\boldsymbol{s} \leftarrow (D_{R,\sigma})^m$, as long as there exists n columns of $\mathbf{A}'$ that form an invertible matrix in $R_q^{n\times n}$ overwhelmingly. We apply the technique from Jin et al. [25, Theorem 5.2] to show that the constraint $m \geq n+\omega(\log\lambda)$ is sufficient for the overwhelming probability of the existence of an invertible sub-matrix from $R_q^{n\times m}$, and we put the proof to Appendix B.1:

Lemma 2.14 *Let $K = \mathbb{Q}[\zeta]$ be the M-th cyclotomic field with degree $N = \varphi(M)$. Let m, n, q be lattice parameters such that $q \geq 2N$ is a prime number and $m \geq n$. With all but at most 2^{n-m} probability, for $\mathbf{A}' \xleftarrow{\$} R_q^{n\times m}$, there exists n columns of $\mathbf{A}'$ that form an invertible matrix in $R_q^{n\times n}$.*

Therefore, with the lemma 2.14, we can obtain the following corollary, which modifies the public matrix $\mathbf{A}$ from $[\mathbf{I}_n \mid U(R_q^{n\times(m-n)})]$ to $U(R_q^{n\times m})$. This corollary will serve for a fair comparison with our new regularity lemma in Corollary 11.

Corollary 2. *Let λ be the security parameter. Let $K = \mathbb{Q}[\zeta]$ be the M-th cyclotomic field with degree $N = \varphi(M)$. Let m, n, q be lattice parameters such that $q \geq 2N$ is a prime and $m \geq n + \omega(\log\lambda)$. Let $\sigma > 2N \cdot q^{\frac{n}{m}+\frac{2}{mN}}$ be a*

Gaussian parameter. Let the prime ideal factorization of qR be $qR = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_g$ where $\mathcal{N}(\mathfrak{q}_i) = q^f$ and $fg = n$. With probability $1 - \mathsf{negl}(\lambda)$ over the choice of $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$, the distribution of $\mathbf{A}\boldsymbol{s} \in R_q^n$ where $\boldsymbol{s} \leftarrow (D_{R,\sigma})^m$ is within statistical distance $2^{-\Omega(N)}$ of $U(R_q^n)$.

3 General Limitations of Smooth Min-Entropy

Smooth min-entropy was first introduced by Renner and Wolf [47], which intuitively says that a distribution has high smooth min-entropy if it is statistically close to a distribution with high exact min-entropy.

Definition 3.1 (Smooth Min-Entropy) *We say that a random variable X has ε-smooth min-entropy at least k, denoted by $H_\infty^\varepsilon(X) \geq k$, if there exists some random variable X' such that $\mathsf{SD}(X, X') \leq \varepsilon$ and $H_\infty(X') \geq k$.*

For the sake of illustrating that computing exact min-entropy is necessary, we list three limitations of smooth entropy in the following remarks:

Remark 3.2 *As we introduced in the introduction, a lattice-structured leftover hash lemma (in integer settings) is to state that $(\mathbf{A}, \mathbf{A}\cdot\boldsymbol{x}) \overset{\varepsilon}{\approx} (\mathbf{A}, \boldsymbol{u})$ for $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$, $\boldsymbol{u} \xleftarrow{\$} \mathbb{Z}_q^n$ and $\boldsymbol{x} \leftarrow \mathcal{X}$ for some distribution $\mathcal{X}$ with support $\mathbb{Z}_q^m$.*

When q is a prime, the smooth entropy is quite useful in the following way: If we have $H_\infty^{\varepsilon_1}(\mathcal{X}) \geq k$ for some $\varepsilon_1 > 0$, then there exists a random variable $\mathcal{X}'$ such that $H_\infty(\mathcal{X}') \geq k$. For $\boldsymbol{x}' \leftarrow \mathcal{X}'$, we can apply the leftover hash lemma to derive that $(\mathbf{A}, \mathbf{A}\cdot\boldsymbol{x}') \overset{\varepsilon_2}{\approx} (\mathbf{A}, \boldsymbol{u})$ for some $\varepsilon_2 > 0$. In the end, we can get $(\mathbf{A}, \mathbf{A}\cdot\boldsymbol{x}) \overset{\varepsilon_1+\varepsilon_2}{\approx} (\mathbf{A}, \boldsymbol{u})$.

When q is a composite number, the application of leftover hash lemma is more complicated, which requires $(\mathcal{X} \bmod p)$ has enough min-entropy for all $p \mid q$. if we only have preconditions that $H_\infty^\varepsilon(\mathcal{X} \bmod p) \geq k$ such that $(\mathcal{X} \bmod p) \overset{\varepsilon}{\approx} \mathcal{X}_p'$ and $H_\infty(\mathcal{X}_p') \geq k$ for some distribution $\mathcal{X}_p'$, and we still want to apply the leftover hash lemma to prove the uniformity of $(\mathbf{A}, \mathbf{A}\cdot\boldsymbol{x})$, we need to find a random variable $\mathcal{X}'$ such that $H_\infty(\mathcal{X}' \bmod p)$ for all $p \mid q$ is known. However, these preconditions does not guarantee the existence of such $\mathcal{X}'$ since $\mathcal{X}_q' \bmod p$ is unlikely the same as $\mathcal{X}_p'$. Therefore, in the case of composite q, we should be more careful when applying the leftover hash lemma, let alone the ring case R_q.

Remark 3.3 *In some previous works, the exact min-entropy is required. Brakerski and Döttling [7] proposed a reduction from the standard LWE to LWE with entropic secrets. In the case where the secret has bounded norm [7, Lemma 5.4], they required the secret $\boldsymbol{s}$ to be totally bounded, instead of being overwhelmingly bounded. Therefore, when dealing with the bounded case, we need to find the exact min-entropy of the totally bounded distribution. For example, if we would like to take the discrete Gaussian as the secret distribution while discrete Gaussian is not totally bounded but overwhelmingly bounded, then we must first change the discrete Gaussian to a truncated discrete Gaussian, and then apply the bounded* *case of [7] to the truncated one, which requires the exact min-entropy of the truncated distribution. For more details of the exact min-entropy of truncated discrete Gaussian and its application in bounded case of entropic LWE's hardness, please refer to Corollary 7 and Lemma 6.4.*

Remark 3.4 *For a distribution D, there exists a natural and general lower bound of the exact min-entropy $H_\infty(D)$, which can be formulated by a function of ε and the smooth min-entropy $H^\varepsilon_\infty(D) = k$ such that $H_\infty(D') = k$ and $D \overset{\varepsilon}{\approx} D'$ in the following way:*

$$H_\infty(D) = -\log\left(\max_{\boldsymbol{x}} D(\boldsymbol{x})\right) \geq -\log\left(\max_{\boldsymbol{x}} D'(\boldsymbol{x}) + 2\varepsilon\right) = -\log\left(2^{-k} + 2\varepsilon\right).$$

Thus, the natural lower bound depends on both k and ε. If $\varepsilon \gg 2^{-k}$, this lower bound has very bad performance since $-\log\left(2^{-k} + 2\varepsilon\right)$ is far less than k. For example, $\varepsilon = 2^{-n}$ is an ideal setting asymptotically, however, if we have $k = n \log q$, then $H_\infty(D)$ can be only lower bounded by $n - 1$, which loses too much min-entropy compared to $k = n \log q$. Therefore, computing the min-entropy of a distribution by its smooth min-entropy has unavoidable demerits.

4 Min-Entropy of Discrete Gaussian Modulo a Sub-Lattice

In this section, we propose two approaches to compute the lower bound of min-entropy of discrete Gaussian modulo a sub-lattice. The first approach does not depend on the smoothing parameter and its intuitive idea has been discussed in techinical overview. The second approach utilizes the smoothing parameter, which serves as a supplement to our first approach.

4.1 First Approach

Before presenting our theorem of the first approach, we start with *Hermite Normal Form Decomposition.* The following lemma is mainly taken from [19], which illustrates that any square integer matrix $\mathbf{M}$ can be factorized to a integer upper triangular matrix $\mathbf{T} \in \mathbb{Z}^{n\times n}$, followed by a unimodular matrix $\mathbf{P} \in \mathbb{Z}^{n\times n}$, i.e., $\mathbf{M} = \mathbf{TP}$. In fact, [19] proves a stronger result that if we set other constraints on the upper triangular matrix $\mathbf{T}$, then the decomposition is unique. We do not claim any new results in lemma 4.1, but give a simple proof based on the basis extension theorem in lattices, which only requires the existence of such decomposition and the uniqueness of $\mathbf{T}$'s diagonal elements except for signs.

Lemma 4.1 (Hermite Normal Form Decomposition [19]) *Let $n \geq 1$ be the matrix dimension. For any invertible integer matrix $\mathbf{M} = (m_{kj})_{k,j\in[n]} \in \mathbb{Z}^{n\times n}$, there exists a unimodular matrix $\mathbf{P} \in \mathbb{Z}^{n\times n}$ such that $\mathbf{T} = \mathbf{MP}$ is an upper triangular matrix and there exists an efficient algorithm to get such $\mathbf{P}$. Moreover, regardless the choice of $\mathbf{P}$, the sequence and the absolute values of the diagonal entries $\mathbf{T}_{ii}$ for $i \in [n]$ are invariant.*

Proof. We will find the matrix $\mathbf{P} = \begin{pmatrix} \boldsymbol{p}_1 \ \boldsymbol{p}_2 \cdots \boldsymbol{p}_n \end{pmatrix}$ by determining $\boldsymbol{p}_1, \boldsymbol{p}_2, \cdots, \boldsymbol{p}_n \in \mathbb{Z}^n$ successively.

For the matrix $\mathbf{M} \in \mathbb{Z}^{n\times n}$, we define $\mathbf{M}_i \in \mathbb{Z}^{(n-i)\times n}$ as the matrix altered from $\mathbf{M}$ by deleting the upper i rows for $0 \le i \le n$. Then we obtain a sequence of lattices:

$$\{\mathbf{0}^n\} = \mathbf{\Lambda}^{\perp}(\mathbf{M}_0) \subsetneq \mathbf{\Lambda}^{\perp}(\mathbf{M}_1) \subsetneq \cdots \subsetneq \mathbf{\Lambda}^{\perp}(\mathbf{M}_{n-1}) \subsetneq \mathbf{\Lambda}^{\perp}(\mathbf{M}_n) = \mathbb{Z}^n$$

where $\dim \mathbf{\Lambda}^{\perp}(\mathbf{M}_i) = i$ for all i.

We notice that the requirements on $\mathbf{P}$ can be translated to two conditions:

1. The requirement that $\mathbf{MP}$ is an integer upper triangular matrix, is equivalent to the condition that $\boldsymbol{p}_i \in \mathbf{\Lambda}^{\perp}(\mathbf{M}_i)$ for all $i \in [n]$;
2. The requirement that $\det \mathbf{P} = \pm 1$, is equivalent to the condition that $\mathbf{P}$ is a basis of $\mathbb{Z}^n$.

We state that for any $1 \le i < j \le n$, any basis of $\mathbf{\Lambda}^{\perp}(\mathbf{M}_i)$ is primitive with respect to $\mathbf{\Lambda}^{\perp}(\mathbf{M}_j)$. Otherwise, if for some basis $\mathbf{M}'_i \in \mathbb{Z}^{n\times i}$ of $\mathbf{\Lambda}^{\perp}(\mathbf{M}_i)$, there exists a non-integer vector $\boldsymbol{t} \in \mathbb{R}^i$ such that $\mathbf{M}'_i \cdot \boldsymbol{t} \in \mathbf{\Lambda}^{\perp}(\mathbf{M}_j) \subset \mathbb{Z}^n$, then due to $\mathbf{M}_i \cdot (\mathbf{M}'_i \cdot \boldsymbol{t}) = \mathbf{0}^i$, we have $\mathbf{M}'_i \cdot \boldsymbol{t} \in \mathbf{\Lambda}^{\perp}(\mathbf{M}_i)$, contradicting to the definition of lattice basis.

From the basis extension theorem in lemma 2.2, we can successively pick $\boldsymbol{p}_i$, such that $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_i$ is a basis of $\mathbf{\Lambda}^{\perp}(\mathbf{M}_i)$ conditioned on $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_{i-1}$ is a basis of $\mathbf{\Lambda}^{\perp}(\mathbf{M}_{i-1})$. By Gaussian elimination algorithm, we can finish this step efficiently (with time in $\mathsf{poly}(n)$). Therefore, the choice of $\mathbf{P}$ satisfies the two conditions above, which completes the proof of existence.

Suppose there exist two invertible integer upper triangular matrices $\mathbf{T} = (t_{ij})_{i,j\in[n]}, \mathbf{T}' = (t'_{ij})_{i,j\in[n]} \in \mathbb{Z}^{n\times n}$ such that $|t_{ii}| \neq |t'_{ii}|$ for some $i \in [n]$, and there exists a unimodular matrix $\mathbf{U} \in \mathbb{Z}^{n\times n}$ such that $\mathbf{T} = \mathbf{T}'\mathbf{U}$. Since $\mathbf{T}'^{-1}$ is an upper triangular matrix with diagonal entries to be $(\mathbf{T}'^{-1})_{ii} = 1/t'_{ii}$ for all $i \in [n]$, then $\mathbf{U} = \mathbf{T}'^{-1}\mathbf{T}$ is also an upper triangular matrix with diagonal entries to be $\mathbf{U}_{ii} = t_{ii}/t'_{ii} \in \mathbb{Z}$ for all $i \in [n]$. From the same arguments $t'_{ii}/t_{ii} \in \mathbb{Z}$ for all $i \in [n]$, yielding a contradiction to $|t'_{ii}| \neq |t_{ii}|$ for some $i \in [n]$. This completes the proof of invariance of diagonal parts. □

Hermite Normal Form Decomposition gives us a way to characterize the relationship between a full-rank lattice $\mathbf{\Lambda} = \mathbf{B} \cdot \mathbb{Z}^{n\times n}$ and its full-rank sub-lattice $\mathbf{\Lambda}' = \mathbf{B} \cdot \mathbf{M} \cdot \mathbb{Z}^n$ where $\mathbf{B} \in \mathbb{R}^{n\times n}$ is a basis of $\mathbf{\Lambda}$ and $\mathbf{M} \in \mathbb{Z}^{n\times n}$ is some nonsingular matrix. Because the basis $\mathbf{B}$ multiplied with any unimodular matrix $\mathbf{P}$ can still be the basis of the same lattice, we can rewrite the sublattice $\mathbf{\Lambda}'$ as $\mathbf{\Lambda}' = \mathbf{B} \cdot \mathbf{T} \cdot \mathbb{Z}^n$ for some nonsingular upper triangular matrix $\mathbf{T} \in \mathbb{Z}^{n\times n}$. The following corollary gives us explicit coset representatives of $\mathbf{\Lambda}/\mathbf{\Lambda}'$, which is useful for our estimation of the min-entropy of discrete Gaussian distribution over $\mathbf{\Lambda}$ modulo $\mathbf{\Lambda}'$ for a general lattice pair $(\mathbf{\Lambda}, \mathbf{\Lambda}')$.

Corollary 3. *Let $n \ge 1$ be the lattice dimension. Let $\mathbf{\Lambda} \subset \mathbb{R}^n$ be a full-rank lattice with basis $\mathbf{B} \in \mathbb{R}^{n\times n}$. For any full-rank sub-lattice $\mathbf{\Lambda}' \subseteq \mathbf{\Lambda}$, there exist* *some integer upper triangular matrix* $\mathbf{T} \in \mathbb{Z}^{n\times n}$ *with invariant diagonal entries* $t_1, t_2, \cdots, t_n > 0$ *such that the basis of* $\mathbf{\Lambda}'$ *is* $\mathbf{B}\cdot\mathbf{T}$. *Moreover, a coset representative of the quotient group* $\mathbf{\Lambda}/\mathbf{\Lambda}'$ *is* $\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\mathbb{Z}_{t_2}\times\cdots\times\mathbb{Z}_{t_n})^\top$.

Proof. The existence of the integer upper triangular matrix $\mathbf{T}$ follows lemma 4.1. If some diagonal elements of $\mathbf{T}$ are not positive, we can multiply a diagonal matrix with elements ± 1 to the right side of $\mathbf{T}$ and transform the negative elements to its absolute values while keeping $\mathbf{T}$ to be an upper triangular matrix. The uniqueness of diagonal elements of $\mathbf{T}$ also follows lemma 4.1.

If there exist non-zero vector $\boldsymbol{y}\in(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top$ such that $\mathbf{B}\cdot\boldsymbol{y}\in\mathbf{\Lambda}'$, we will find some $\boldsymbol{x}=(x_i)_{i\in[n]}\in\mathbb{Z}^n$ such that $\mathbf{B}\cdot\boldsymbol{y}=\mathbf{B}\cdot\mathbf{T}\cdot\boldsymbol{x}$, yielding $\boldsymbol{y}=\mathbf{T}\cdot\boldsymbol{x}$. In order to satisfy this linear system of equations, we can apply the induction on i to prove that $x_{n-i}=0$ for $i=0,\cdots,n-1$ due to the upper triangular property of $\mathbf{T}$. Therefore, there do not exist two different vectors from $\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\mathbb{Z}_{t_2}\times\cdots\times\mathbb{Z}_{t_n})^\top$ in the same coset of $\mathbf{\Lambda}/\mathbf{\Lambda}'$. Moreover, we have

$$|\mathbf{\Lambda}/\mathbf{\Lambda}'| = \frac{\det\mathbf{\Lambda}'}{\det\mathbf{\Lambda}} = \frac{\det(\mathbf{B}\cdot\mathbf{T})}{\det\mathbf{B}} = \det\mathbf{T} = \prod_{i=1}^n t_i = \left|\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\mathbb{Z}_{t_2}\times\cdots\times\mathbb{Z}_{t_n})^\top\right|,$$

which shows that a set of coset representatives of $\mathbf{\Lambda}/\mathbf{\Lambda}'$ is exactly $\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})$. □

Here, we present the main theorem of our first approach.

Theorem 4.2 *Let* $\mathbf{\Lambda}, \mathbf{\Lambda}'$ *be* n*-dimensional full rank lattices such that* $\mathbf{\Lambda}'\subseteq\mathbf{\Lambda}$. *Let* $\mathbf{B}\in\mathbb{R}^{n\times n}$ *be a basis of* $\mathbf{\Lambda}$ *and* $\mathbf{B}\cdot\mathbf{T}$ *be the basis of* $\mathbf{\Lambda}'$ *for an upper triangular matrix* $\mathbf{T}\in\mathbb{Z}^{n\times n}$ *with positive diagonal entries* $(t_i)_{i\in[n]}$. *For any* $\varepsilon\in(0,1)$, *any positive definite matrix* $\mathbf{\Sigma}\in\mathbb{R}^{n\times n}$, $\boldsymbol{c}\in\mathbb{R}^n$ *and* $\boldsymbol{c}'=\boldsymbol{c} \bmod \mathbf{\Lambda}$, *let* $\sigma=\frac{1}{s_1(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{B})}$, *we have*

$$2^{H_\infty(D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}} \bmod \mathbf{\Lambda}')} \geq \begin{cases} \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{c}')\cdot\prod_{i=1}^n \rho_\sigma(\mathbb{Z}_{t_i}) & \text{if } \sqrt{\mathbf{\Sigma}}>0 \\ \frac{1-\varepsilon}{1+\varepsilon}\cdot\prod_{i=1}^n\rho_\sigma(\mathbb{Z}_{t_i}) & \text{if } \sqrt{\mathbf{\Sigma}}\geq\eta_\varepsilon(\mathbf{\Lambda}) \end{cases}.$$

Proof. Notice that $\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}-\boldsymbol{c})=\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}-\boldsymbol{c}')$. From corollary 1, we have

$$\begin{aligned} H_\infty(D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}} \bmod \mathbf{\Lambda}') &= -\log\left(\max_{\boldsymbol{x}\in\mathbf{\Lambda}}\frac{D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda}'+\boldsymbol{x})}{D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda})}\right) \\ &= -\log\left(\frac{\max_{\boldsymbol{x}\in\mathbf{\Lambda}}\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}'+\boldsymbol{x}-\boldsymbol{c})}{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}-\boldsymbol{c})}\right) \\ &\geq -\log\left(\frac{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}')}{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}-\boldsymbol{c}')}\right) \end{aligned}$$

Therefore, we obtain that

$$2^{H_\infty(D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\mathbf{c}} \bmod \mathbf{\Lambda}')} \geq \frac{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda} - \boldsymbol{c}')}{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}')} \geq \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{c}') \cdot \frac{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda})}{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}')} \tag{6}$$

$$= \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{c}') \cdot \frac{\sum_{\boldsymbol{x}\in\mathbf{\Lambda}/\mathbf{\Lambda}'} \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}' + \boldsymbol{x})}{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}')}$$

$$\geq \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{c}') \cdot \sum_{\boldsymbol{x}\in\mathbf{\Lambda}/\mathbf{\Lambda}'} \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{x}).$$

From corollary 3, a coset representative set of $\mathbf{\Lambda}/\mathbf{\Lambda}'$ is $\mathbf{B} \cdot (\mathbb{Z}_{t_1} \times \cdots \mathbb{Z}_{t_n})^\top$, then we can estimate the term $\sum_{\boldsymbol{x}\in\mathbf{\Lambda}/\mathbf{\Lambda}'} \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{x})$ as follows:

$$\sum_{\boldsymbol{x}\in\mathbf{\Lambda}/\mathbf{\Lambda}'} \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{x}) \geq \sum_{\boldsymbol{x}\in\mathbf{B}\cdot(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top} \rho_{\sqrt{\mathbf{\Sigma}}}(\boldsymbol{x})$$

$$\geq \sum_{\boldsymbol{y}\in(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top} \rho\left(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{B}\boldsymbol{y}\right)$$

$$\geq \sum_{\boldsymbol{y}\in(\mathbb{Z}_{t_1}\times\cdots\times\mathbb{Z}_{t_n})^\top} \rho_\sigma(\boldsymbol{y}) = \prod_{i=1}^{n} \rho_\sigma(\mathbb{Z}_{t_i}),$$

which completes the first part of he proof. For the part $\sqrt{\mathbf{\Sigma}} \geq \eta_\varepsilon(\mathbf{\Lambda})$, from the definition of smoothing parameter and possion summation formular, we have $\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda} - \boldsymbol{c}') \geq \frac{1-\varepsilon}{1+\varepsilon} \cdot \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda})$, which completes the second part of the proof. □

Next, we give a way to compute the lower bound of $\rho_\sigma(\mathbb{Z}_q)$ for any Gaussian parameter $\sigma > 0$ and modulus $q \geq 2$.

Claim 4.3 *Let $\sigma > 0$ be a Gaussian parameter and $q \geq 2$ be a modulus. We have*

$$\rho_\sigma(\mathbb{Z}_q) \geq \begin{cases} \sigma/2, & \text{if } \sigma \leq \frac{\sqrt{\pi}}{2\sqrt{\ln 4}} \cdot q; \\ q/4, & \text{if } \sigma > \frac{\sqrt{\pi}}{2\sqrt{\ln 4}} \cdot q. \end{cases}$$

For dimension $n \geq 1$, we have

$$\rho_\sigma(\mathbb{Z}_q^n) \geq \sigma^n/2, \qquad \text{if } \sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4n)}}.$$

Proof. For any $\delta > 0$, $\mathbb{Z}_q$ covers all integer points in the ball $(q/2 - \varepsilon)\mathcal{B}_1^\infty = [-(q/2-\delta), q/2-\delta]$, then we have

$$\rho_\sigma(\mathbb{Z}_q) \geq \rho\left(\frac{1}{\sigma} \cdot \mathbb{Z} \cap \frac{q/2-\delta}{\sigma} \cdot \mathcal{B}_1^\infty\right)$$

$$= \rho_\sigma(\mathbb{Z}) - \rho\left(\frac{1}{\sigma} \cdot \mathbb{Z} \setminus \frac{q/2-\delta}{\sigma} \cdot \mathcal{B}_1^\infty\right)$$

$$> \rho_\sigma(\mathbb{Z}) \cdot \left(1 - 2\exp(-\pi(q/2-\delta)^2/\sigma^2)\right) \tag{7}$$

$$> \sigma \cdot (1 - 2\exp(-\pi(q/2-\delta)^2/\sigma^2))$$

where the inequality (7) is from Lemma 2.5. The previous inequality holds for every $\delta > 0$ and because of the continuity, we have

$$\rho_\sigma(\mathbb{Z}_q) > \rho_\sigma(\mathbb{Z}) \cdot (1 - 2\exp(-\pi q^2/4\sigma^2)).$$

For $\sigma \leq \frac{\sqrt{\pi}}{2\sqrt{\ln 4}} \cdot q$, we have

$$\rho_\sigma(\mathbb{Z}_q) > \sigma \cdot \rho_{1/\sigma}(\mathbb{Z}) \cdot (1 - 2\exp(-\pi q^2/4\sigma^2)) > \sigma/2.$$

For $\sigma \geq \frac{\sqrt{\pi}}{2\sqrt{\ln 4}} \cdot q$, we have that for all $x \in \mathbb{Z}_q$, $\rho_\sigma(x) \geq \rho_\sigma(q/2) \geq 1/4$, then

$$\rho_\sigma(\mathbb{Z}_q) \geq q \cdot \rho_\sigma(q/2) \geq q/4.$$

The case for dimension n and Gaussian parameter $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4n)}}$, is similar to the case for dimension 1. □

Remark 4.4 *Lemma 4.1, Corollary 3 and Theorem 4.2 still hold if we change the* upper triangular matrix *to the* lower triangular matrix *in their descriptions. In details, every nonsingular integer matrix* $\mathbf{M} \in \mathbb{Z}^{n\times n}$ *can be decomposed to a lower triangular matrix* $\mathbf{T}$ *multiplied with a unimodular matrix* $\mathbf{P}$*, and the diagonal elements of* $\mathbf{T}$ *are invariant except for signs. The ways to find coset representatives of the quotient group* $\mathbf{\Lambda}/\mathbf{\Lambda}'$ *and estimate the min-entropy of discrete Gaussian over* $\mathbf{\Lambda}$ *modulo* $\mathbf{\Lambda}'$ *remain the same.*

Following corollaries are two examples of applying our first approach (theorem 4.2) to specific lattice pairs $(\mathbb{Z}^n, q\mathbb{Z}^n)$ and $(\mathbf{\Lambda}_q^\perp(\mathbf{g}_k), q\mathbb{Z}^n)$ with modulus q, $k = \lceil \log q \rceil$ and gadget vector $\mathbf{g}_k = (1, 2, \cdots, 2^{k-1})^\top$.

Corollary 4. *Let* n, q *be lattice parameters and* $\sigma > 0$ *be a Gaussian parameter. Let* $\boldsymbol{c} \in \mathbb{R}^n$ *be any point. Define random variable* $\mathcal{S} := D_{\mathbb{Z}_q^n,\sigma,\mathbf{c}} \bmod q$*, and if* $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4n)}}$*, for any* $\varepsilon \in (0,1)$*, we have*

$$H_\infty(\mathcal{S}) \geq \begin{cases} n\log\sigma - 1 & \text{if } 0 < \sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4n)}} \text{ and } \mathbf{c} \in \mathbb{Z}^n; \\ n\log\sigma - 1 - \log\frac{1+\varepsilon}{1-\varepsilon} & \text{if } \eta_\varepsilon(\mathbb{Z}^n) \leq \sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4n)}}. \end{cases}$$

Proof. We take $\mathbf{\Lambda} = \mathbb{Z}^n$ with basis $\mathbf{B} = \mathbf{I}_n$, and $\mathbf{\Lambda}' = q\mathbb{Z}^n$ with basis $q\mathbf{I}_n$, and the corresponding upper triangular matrix $\mathbf{T} = q\mathbf{I}_n$ in the setting of theorem 4.2. Since $\rho_\sigma(\mathbb{Z}_q)^n = \rho_\sigma(\mathbb{Z}_q^n)$, we combine claim 4.3 and theorem 4.2 to complete the proof of Corollary 4. □

Corollary 5. *Let* $q \geq 2$ *be a positive modulus and* $k = \lceil \log q \rceil$*. Let* $\varepsilon \in (0,1)$*. Let* $\mathbf{g}_k = (1, 2, \cdots, 2^{k-1})^\top$ *be the gadget vector. Define the random variable* $\mathcal{S} := D_{\mathbf{\Lambda}_q^\perp(\mathbf{g}_k),\sigma,\mathbf{c}} \bmod q$ *for some* $\boldsymbol{c} \in \mathbb{R}^k$*.*

If $q = 2^k$*, we have*

$$H_\infty(\mathcal{S}) \geq \begin{cases} k\log\frac{\sigma}{3} - 1 & \text{if } 0 < \sigma \leq \frac{3\sqrt{\pi}}{4} \cdot \frac{q}{\sqrt{\ln(4k)}} \text{ and } \mathbf{c} = \mathbf{0}^k; \\ k\log\frac{\sigma}{3} - 1 - \log\frac{1+\varepsilon}{1-\varepsilon} & \text{if } 2\sqrt{\ln(2k(1+\frac{1}{\varepsilon}))/\pi} \leq \sigma \leq \frac{3\sqrt{\pi}}{4} \cdot \frac{q}{\sqrt{\ln(4k)}}. \end{cases}$$

If $2^{k-1} < q < 2^k$ *and* q *is an odd number, we have*

$$H_\infty(\mathcal{S}) \geq \begin{cases} (k-1)\log \frac{\sigma}{2\max\{\sqrt{5},\sqrt{k}\}} - 1 & \textit{if } 0 < \sigma \leq \frac{\max\{\sqrt{5},\sqrt{k}\}\cdot\sqrt{\pi}q}{\sqrt{\ln(4(k-1))}} \textit{ and } \mathbf{c} = \mathbf{0}^k; \\ (k-1)\log \frac{\sigma}{2\max\{\sqrt{5},\sqrt{k}\}} - 1 - \log\frac{1+\varepsilon}{1-\varepsilon} & \textit{if } \sqrt{5\ln(2k(1+\frac{1}{\varepsilon}))/\pi} \leq \sigma \leq \frac{\max\{\sqrt{5},\sqrt{k}\}\cdot\sqrt{\pi}q}{\sqrt{\ln(4(k-1))}}. \end{cases}$$

Proof. We first show the proof for the case $q = 2^k$. In [36], Micciancio and Peikert computes a short basis of $\mathbf{\Lambda}_q^\perp(\mathbf{g}_k)$, which is

$$\mathbf{B}_q = \begin{pmatrix} 2 & & & & \\ -1 & 2 & & & \\ & -1 & \ddots & & \\ & & & 2 & \\ & & & -1 & 2 \end{pmatrix} \in \mathbb{Z}^{k\times k}$$

with norm $s_1(\mathbf{B}_q) \leq 3$ and $\|\widetilde{\mathbf{B}_q}\| = 2$. Consider the lower triangular matrix

$$\mathbf{T}_q = \begin{pmatrix} 2^{k-1} & & & & \\ 2^{k-2} & 2^{k-1} & & & \\ \vdots & \vdots & \ddots & & \\ 2 & 4 & \cdots & 2^{k-1} & \\ 1 & 2 & \cdots & 2^{k-2} & 2^{k-1} \end{pmatrix} \in \mathbb{Z}^{k\times k}.$$

We can verify that $\mathbf{B}_q \cdot \mathbf{T}_q = 2^k \cdot \mathbf{I}_k$ which is a basis of $q\mathbb{Z}^k$. Hence $\mathbf{T}_q$ is our desired lower triangular matrix in the transition from $\mathbf{\Lambda}_q^\perp(\mathbf{g}_k)$ to $q\mathbb{Z}^k$ with k diagonal entries all $2^{k-1} = q/2$. From theorem 4.2, we have

$$2^{H_\infty(\mathcal{S})} \geq \begin{cases} \rho_{\frac{\sigma}{3}}\left(\mathbb{Z}_{\frac{q}{2}}\right)^k & \text{if } \mathbf{c} = \mathbf{0}^k; \\ \frac{1-\varepsilon}{1+\varepsilon}\cdot\rho_{\frac{\sigma}{3}}\left(\mathbb{Z}_{\frac{q}{2}}\right)^k & \text{if } \sigma \geq \eta_\varepsilon(\mathbf{\Lambda}_q^\perp(\mathbf{g}_k)). \end{cases}$$

This, together with Claim 4.3 and Lemma 2.9, completes the proof for $q = 2^k$.

We then show the proof for the case odd $q \in (2^{k-1}, 2^k)$. Let $q = \sum_{i=0}^{k-1} 2^i q_i$ be the binary decomposition of q for $q_i \in \{0,1\}$ and $i = 0, \cdots, k-1$. From [36], a short basis of $\mathbf{\Lambda}_q^\perp(\mathbf{g}_k)$ is

$$\mathbf{B}_q = \begin{pmatrix} 2 & & & & q_0 \\ -1 & 2 & & & q_1 \\ & -1 & \ddots & & \vdots \\ & & & 2 & q_{k-2} \\ & & & -1 & q_{k-1} \end{pmatrix} \in \mathbb{Z}^{k\times k}$$

with norm $s_1(\mathbf{B}_q) \leq 2\max\{\sqrt{5},\sqrt{k}\}$, $\|\widetilde{\mathbf{B}_q}\| \leq \sqrt{5}$ and $\det\mathbf{B}_q = q$. Consider the lower triangular matrix

$$\mathbf{T}_q = \begin{pmatrix} 1 & & & & & \\ -2\lfloor\frac{q}{2^2}\rfloor & q & & & & \\ -2\lfloor\frac{q}{2^3}\rfloor & & q & & & \\ \vdots & & & \ddots & & \\ -2\lfloor\frac{q}{2^{k-1}}\rfloor & & & & q & \\ -2 & & & & & q \end{pmatrix} \in \mathbb{Z}^{k\times k}.$$

We can verify that every entry of $\mathbf{B}_q \cdot \mathbf{T}_q$ is divided evenly by q, indicating that $(\mathbf{B}_q \cdot \mathbf{T}_q) \cdot \mathbb{Z}^k \subseteq q\mathbb{Z}^k$. Moreover, $\det(\mathbf{B}_q \cdot \mathbf{T}_q) = \det \mathbf{B}_q \cdot \det \mathbf{T}_q = q \cdot q^{k-1} = q^k = \det(q\mathbb{Z}^k)$ which shows that $(\mathbf{B}_q \cdot \mathbf{T}_q) \cdot \mathbb{Z}^k = q\mathbb{Z}^k$, i.e., $\mathbf{B}_q \cdot \mathbf{T}_q$ is a basis of $q\mathbb{Z}^k$. Therefore $\mathbf{T}_q$ is our target lower triangular matrix with diagonal elements 1 and $k-1$ number of q. From Theorem 4.2, we have

$$2^{H_\infty(\mathcal{S})} \geq \begin{cases} \rho_{\frac{\sigma}{s_1(\mathbf{B}_q)}}(\mathbb{Z}_q)^{k-1} & \text{if } \boldsymbol{c} = \mathbf{0}^k; \\ \frac{1-\varepsilon}{1+\varepsilon} \cdot \rho_{\frac{\sigma}{s_1(\mathbf{B}_q)}}(\mathbb{Z}_q)^{k-1} & \text{if } \sigma \geq \eta_\varepsilon(\mathbf{\Lambda}_q^\perp(\mathbf{g}_k)). \end{cases}$$

This, together with Claim 4.3 and Lemma 2.9, completes the proof for odd q. □

Discrete Gaussians modulo Ideal $\mathfrak{q}$ under Coefficient Embeddings

Here we apply our Theorem 4.2 to ideal lattices, where the crux is how to get a proper and short representatives for the elements in the quotient ring $R \bmod \mathfrak{q}$.

First, we will prove an generalized lemma of the basic Dedekind theorem (referred to lemma A.1). Dedekind theorem shows the generators of each prime ideals, and in the next lemma, we will show that for each ideal factor $\mathcal{I} \mid q\mathcal{O}_K$ with norm $\mathcal{N} = q^t$, there exists a t-degree polynomial $f_\mathcal{I} \in \mathbb{Z}_q[x]$ such that $\mathcal{I} = \langle q, f_\mathcal{I}(\zeta) \rangle$, which presents an explicit representation for every ideal factor $\mathcal{I} \mid q\mathcal{O}_K$.

Lemma 4.5 *Let $K = \mathbb{Q}(\zeta)$ be a number field for $\zeta \in \mathcal{O}_K$, and $F(x)$ be the minimal polynomial of ζ in $\mathbb{Z}[x]$. For any prime q, the ideal $q\mathcal{O}_K$ factors into prime ideals as $\langle q \rangle = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$, where $\mathcal{N}(\mathfrak{q}_i) = q^{f_i}$ for $f_i = [\mathcal{O}_K/\mathfrak{q}_i : \mathbb{Z}_q]$, and $N = \sum_{i=1}^g e_i f_i$.*

Moreover if q does not divide the index of $[\mathcal{O}_K : \mathbb{Z}[\zeta]]$, then we have further structures as following. We can express $F(x) = f_1(x)^{e_1} \dots f_g(x)^{e_g} \mod q$, where each $f_i(x)$ is a monic irreducible polynomial in $\mathbb{Z}_q[x]$. Then, for any integers $k_i \in [e_i]$ where $i \in [d]$, we have $\prod_{i=1}^d \mathfrak{q}_i^{k_i} = \left\langle q,\ \prod_{i=1}^d f_i(\zeta)^{k_i} \right\rangle$.

Proof. Let ideal $\mathcal{I} = \prod_{i=1}^d \mathfrak{q}_i^{k_i}$ and $\mathcal{J} = \left\langle q, \prod_{i=1}^d f_i(\zeta)^{k_i} \right\rangle$. We prove this lemma by double inclusion and start with $\mathcal{J} \subseteq \mathcal{I}$. Obviously, $\prod_{i=1}^d f_i(\zeta)^{k_i} \in \mathcal{I}$. Since $\mathcal{I} \mid \langle q \rangle$, we have $q \in \langle q \rangle \subseteq \mathcal{I}$, which completes the first inclusion.

For all $qx_i + f_i(\zeta)^{k_i} y_i \in \mathfrak{q}_i$, we can write their product $\prod_{i=1}^d (qx_i + f_i(\zeta)^{k_i} y_i)$ in the form of $qx + (\prod_{i=1}^d f_i(\zeta)^{k_i})y \in \mathcal{J}$, which indicates that $\mathcal{I} \subseteq \mathcal{J}$. □

With this extended Dedekind theorem, we obtain the following theorem of min-entropy of discrete gaussian distribution over modular ideal lattice, here the discrete gaussian is defined over the coefficient lattice $\phi(R)$.

Corollary 6. *Let $K = \mathbb{Q}(\zeta)$ be a number field with minimal polynomial f of degree N. Let $q = \mathsf{poly}(\lambda)$ be a prime number such that $\gcd(q, [R : \mathbb{Z}[\zeta]]) = 1$, and $\mathfrak{q} \neq R$ be a factor of qR with norm $\mathcal{N}(\mathfrak{q}) = q^t$ for some $1 \leq t \leq N$. Let $\sigma > 0$ be a gaussian parameter. Let $c \in K$ and $\mathcal{S} := D_{R,\sigma,c}^{\mathsf{coeff}} \bmod \mathfrak{q}$ be the gaussian* *distribution over coefficient lattice of R modulo $\mathfrak{q}$ centered at $c \in K_{\mathbb{R}}$. For any $\varepsilon \in (0,1)$, we have*

$$H_\infty(\mathcal{S}) \geq \begin{cases} t\log\sigma - 1 & \text{if } 0 < \sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4t)}} \text{ and } c \in R, \\ t\log\sigma - 1 - \log\frac{1+\varepsilon}{1-\varepsilon} & \text{if } \eta_\varepsilon(\mathbb{Z}^N) \leq \sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4t)}}. \end{cases}$$

Proof. From lemma 4.5, there exists a t-degree monic polynomial $f(x) \in \mathbb{Z}_p[x]$ such that $\mathfrak{q} = \langle q, f(\zeta)\rangle$. This form of ideal indicates that we can write the cosets of the quotient ring $R/\mathfrak{q}$ as $\sum_{i=0}^{t-1} a_i\zeta^i + \mathfrak{q}$ for $a_i \in \mathbb{Z}_q$. Hence, we can take the representative vector in $\phi(R) \bmod \phi(\mathfrak{q})$ as $\mathbb{Z}_q^t \times \{0\}^{N-t}$. Besides, from $\mathbb{Z}^N \subseteq \phi(R)$, we have $\eta_\varepsilon(\phi(R)) \leq \eta_\varepsilon(\mathbb{Z}^N)$.

This, together with Theorem 4.2, allows us to obtain

$$\sum_{x \in R \bmod \mathfrak{q}} \rho_\sigma^{\mathsf{coeff}}(x) \geq \sum_{\boldsymbol{x} \in \mathbb{Z}_q^t} \rho_\sigma(\boldsymbol{x}) \geq \sigma^t/2$$

where the last inequality is from claim 4.3, which completes the proof. □

Remark 4.6 *Corollary 6 holds for every number field $K = \mathbb{Q}(\zeta)$. However, its performance is better in the case of small $[R : \mathbb{Z}[\zeta]]$. The reason is that if $[R : \mathbb{Z}[\zeta]]$ is far more than 1, then R contains elements with shorter length than all elements from $\mathbb{Z}[\zeta]$. Our choice of the representative elements of $R \bmod \mathfrak{q}$ is the set of $\sum_{i=0}^{t-1} a_i\zeta^i$ for $a_i \in \mathbb{Z}_q$, which are totally contained in $\mathbb{Z}[\zeta]$. Therefore, if $[R : \mathbb{Z}[\zeta]] > 1$, such coset representatives seems to be in a bad quality since there are more possible shorter elements in R which are not chosen as representatives, yielding a bad estimation of our min-entropy. Fortunately, the most commonly used number field is the cyclotomic number field which satisfies $R = \mathbb{Z}[\zeta]$.*

While sometimes we need a truncated version of discrete gaussian distribution in lattice primitive constructions, here we give a lower bound for the min-entropy of truncated discrete gaussian distribution.

Corollary 7. *Let $K = \mathbb{Q}(\zeta)$ be a number field with minimal polynomial f of degree N. Let $q = \mathsf{poly}(\lambda)$ be a prime number such that $\gcd(q, [R : \mathbb{Z}[\zeta]]) = 1$, and $\mathfrak{q} \neq R$ be a factor of qR with norm $\mathcal{N}(\mathfrak{q}) = q^t$ for some $1 \leq t \leq N$. Let $\sigma > 0$ be a gaussian parameter. Let $\mathcal{S} := D^{\mathsf{coeff}}_{R,\sigma,\leq\sigma\sqrt{N}} \bmod \mathfrak{q}$ be the gaussian distribution over coefficient lattice of R modulo $\mathfrak{q}$. If $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4t)}}$, we have $H_\infty(\mathcal{S}) \geq t\log\sigma - 1 - \mathbf{e}^{-N}$.*

Proof. Apply $\boldsymbol{\Lambda} = \phi(R)$ and bound $r = \sqrt{N}$ in lemma 2.4, we have

$$\begin{aligned} \frac{\rho_\sigma(\boldsymbol{\Lambda} \cap \sigma r\mathcal{B}_N^2)}{\rho_\sigma(\boldsymbol{\Lambda})} &= \frac{\rho(\frac{\boldsymbol{\Lambda}}{\sigma} \cap r\mathcal{B}_N^2)}{\rho(\frac{\boldsymbol{\Lambda}}{\sigma})} = 1 - \frac{\rho(\frac{\boldsymbol{\Lambda}}{\sigma} \setminus r\mathcal{B}_N^2)}{\rho(\frac{\boldsymbol{\Lambda}}{\sigma})} \\ &> 1 - (2\pi\mathbf{e})^{N/2} \cdot \mathbf{e}^{-\pi N} > 1 - \mathbf{e}^{-1.7N}. \end{aligned}$$

From lemma 2.3, we have

$$\max_{a\in R}\rho_\sigma(\phi(a+\mathfrak{q})\cap\sigma r\mathcal{B}_N^2)\le\max_{a\in R}\rho_\sigma(\phi(a+\mathfrak{q}))\le\rho_\sigma(\phi(\mathfrak{q}))=\rho_\sigma^{\mathsf{coeff}}(\mathfrak{q})$$

Then, we can bound the min-entropy:

$$\begin{aligned}2^{H_\infty(\mathcal{S})}&=\frac{\rho_\sigma(\phi(R)\cap\sigma r\mathcal{B}_N^2)}{\max_{a\in R}\rho_\sigma(\phi(a+\mathfrak{q})\cap\sigma r\mathcal{B}_N^2)}\\&\ge(1-\mathbf{e}^{-1.7N})\cdot\frac{\rho_\sigma^{\mathsf{coeff}}(R)}{\rho_\sigma^{\mathsf{coeff}}(\mathfrak{q})}.\end{aligned}$$

Furthermore, we have $\log(1-\mathbf{e}^{-1.7N})\ge-\mathbf{e}^{-N}$ from the fact $\log(1+x)\ge 2x$ for $\frac{1}{2\ln 2}-1\le x\le 0$. The rest computation is the same as proof of corollary 6. □

4.2 Second Approach

We will utilize another approach to obtain a lower bound for the min-entropy of discrete Gaussian distribution modulo sub-lattice, which relies on the properties of smoothing parameter. The following theorem can be applied to any lattices $\mathbf{\Lambda}$ and $\mathbf{\Lambda}'$ as long as the Gaussian parameter $\sigma\ge\eta_\varepsilon(\mathbf{\Lambda})$.

Theorem 4.7 *Let $\mathbf{\Lambda}$ be a n-dimensional full-rank lattice and $\mathbf{\Lambda}'\subseteq\mathbf{\Lambda}$ be a full-rank sub-lattice. For any $\varepsilon\in(0,1)$ and positive definite matrix $\mathbf{\Sigma}$ such that $\eta_\varepsilon(\mathbf{\Lambda})\le\sqrt{\mathbf{\Sigma}}$, define the random variable $\mathcal{S}:=D_{\mathbf{\Lambda},\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}\bmod\mathbf{\Lambda}'$, we have*

$$H_\infty(\mathcal{S})\ge\begin{cases}\log\frac{\det\mathbf{\Lambda}'}{\det\mathbf{\Lambda}}-\log\frac{1+\varepsilon}{1-\varepsilon}, & \text{if } \sqrt{\mathbf{\Sigma}}\ge\eta_\varepsilon(\mathbf{\Lambda}');\\ \log\frac{\det\mathbf{\Lambda}'}{\det\mathbf{\Lambda}}-n\log\left(\eta_\varepsilon\left(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{\Lambda}'\right)\right)-\log\frac{1+\varepsilon}{1-\varepsilon} & \text{if } \eta_\varepsilon(\mathbf{\Lambda})\le\sqrt{\mathbf{\Sigma}}<\eta_\varepsilon(\mathbf{\Lambda}').\end{cases}$$

Proof. From corollary 1, lemma 2.10 and lemma 2.11, for any $\boldsymbol{x}\in\mathbf{\Lambda}$,

$$\begin{aligned}\rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda}'+\boldsymbol{x})\le\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{\Lambda}')&=\rho\left(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{\Lambda}'\right)\\&=\frac{\sqrt{\det\mathbf{\Sigma}}}{\det\mathbf{\Lambda}'}\cdot\rho\left(\left(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{\Lambda}'\right)^\vee\right)\\&\le\frac{\sqrt{\det\mathbf{\Sigma}}}{\det\mathbf{\Lambda}'}\cdot(1+\varepsilon)\cdot\max\left\{1,\left(\eta_\varepsilon\left(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{\Lambda}'\right)\right)^n\right\}.\end{aligned}$$

From lemma 2.10 and $\sqrt{\mathbf{\Sigma}}\ge\eta_\varepsilon(\mathbf{\Lambda})$, $\rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda})\ge(1-\varepsilon)\cdot\frac{\sqrt{\det\mathbf{\Sigma}}}{\det\mathbf{\Lambda}}$, then we can compute that

$$\begin{aligned}2^{-H_\infty(\mathcal{S})}&=\max_{\boldsymbol{x}\in\mathbf{\Lambda}}\frac{\rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda}'+\boldsymbol{x})}{\rho_{\sqrt{\mathbf{\Sigma}},\boldsymbol{c}}(\mathbf{\Lambda})}\\&\le\frac{1+\varepsilon}{1-\varepsilon}\cdot\frac{\det\mathbf{\Lambda}}{\det\mathbf{\Lambda}'}\cdot\max\left\{1,\eta_\varepsilon\left(\sqrt{\mathbf{\Sigma}}^{-1}\mathbf{\Lambda}'\right)^n\right\}\end{aligned}$$

which completes the proof. □

Discrete Gaussians over q-ary Lattices modulo q

In some lattice-based primitives, the discrete Gaussian distributions are sampled over a q-ary lattice [20, 36]. In the following corollary, we give an estimation of the lower bound for the (shifted) discrete Gaussians over a q-ary lattice $\mathbf{\Lambda}^{\perp}(\mathbf{A})$ for most $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.

Corollary 8. *Let n, m, q be lattice parameters such that $m \geq 2n \log q$ and q is a prime. Then for all but at most 2^{-n} fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, for any $\boldsymbol{c} \in \mathbb{R}_q^m$, define the random variable $\mathcal{S} = D_{\mathbf{\Lambda}_q^{\perp}(\mathbf{A}),\sigma,\mathbf{c}}$, we have*

$$H_\infty(\mathcal{S}) \geq \begin{cases} (m-n)\log q - \log \frac{1+\varepsilon}{1-\varepsilon} & \text{if } \sigma > q\cdot\eta \\ m\log(\sigma/\eta) - n\log q - \log\frac{1+\varepsilon}{1-\varepsilon} & \text{if } 4\eta \leq \sigma \leq q\cdot\eta, \end{cases}$$

where $\eta = \sqrt{\ln(2m(1+1/\varepsilon))/\pi}$ for some $\varepsilon \in (0,1)$.

Proof. By Lemma 2.12, for all but at most 2^{-n} fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we have $\eta_\varepsilon(\mathbf{\Lambda}_q^{\perp}(\mathbf{A})) \leq 4\eta$, and for such $\mathbf{A}$, $\det\left(\mathbf{\Lambda}_q^{\perp}(\mathbf{A})\right) = q^n$ since the columns of $\mathbf{A}$ generate $\mathbb{Z}_q^n$.

From the proof in Theorem 4.7, we have

$$\begin{aligned} 2^{-H_\infty(\mathcal{S})} &\leq \frac{1+\varepsilon}{1-\varepsilon}\cdot\frac{\det(\mathbf{\Lambda}^{\perp}(\mathbf{A}))}{\det(q\mathbb{Z}^m)}\cdot\max\left\{1, \left(\frac{q\cdot\eta_\varepsilon(\mathbb{Z}^m)}{\sigma}\right)^m\right\} \\ &\leq \frac{1+\varepsilon}{1-\varepsilon}\cdot q^{n-m}\cdot\max\left\{1,\left(\frac{q\cdot\eta}{\sigma}\right)^m\right\}, \end{aligned}$$

which completes the proof. □

Discrete Gaussians modulo Ideal $\mathcal{I}$ under Canonical Embeddings

Based on several existing estimations [41, 43, 44] of smoothing parameters in ideal lattices, we can get a lower bound for min-entropy of discrete Gaussians over ideal lattices modulo any R-ideal $\mathcal{I}$, where the discrete Gaussian is defined according to the canonical lattice $\sigma(R)$. The following lemma gives upper and lower bounds on the minimal distance of an ideal lattice.

Lemma 4.8 ([44]) *For any fractional ideal $\mathcal{I}$ in a number field K of degree N,*

$$\sqrt{N}\cdot(\mathcal{N}(\mathcal{I}))^{1/N} \leq \lambda_1^{(2)}(\mathcal{I}) \leq \sqrt{N}\cdot(\mathcal{N}(\mathcal{I}))^{1/N}\cdot\sqrt{\Delta_K^{1/N}}.$$

This lemma, together with our second approach in theorem 4.7, allows us to obtain a lower bound of $H_\infty(D_{R,\sigma,c} \bmod \mathcal{I})$.

Corollary 9. *Let $K = \mathbb{Q}(\zeta)$ be a number field with degree N. Let $\mathcal{I} \subseteq R$ be an R-ideal. Let $\sigma > 0$ be a gaussian parameter and $c \in R$ be a Gaussian center. Let $\mathcal{S} := D_{R,\sigma,c} \bmod \mathcal{I}$ be the discrete Gaussian over canonical lattice of R modulo $\mathcal{I}$. Let $\eta = \sqrt{\ln(2N(1+1/\varepsilon))/\pi}$, we have*

$$H_\infty(\mathcal{S}) \geq \begin{cases} \log\mathcal{N}(\mathcal{I}) - \log\frac{1+\varepsilon}{1-\varepsilon}, & \text{if } \sigma \geq \eta\cdot(\mathcal{N}(\mathcal{I})\Delta_K)^{1/N}; \\ N\log(\sigma/\eta) - \log\Delta_K - \log\frac{1+\varepsilon}{1-\varepsilon}, & \text{if } \eta\cdot\Delta_K^{1/N} \leq \sigma \leq \eta\cdot(\mathcal{N}(\mathcal{I})\Delta_K)^{1/N}. \end{cases}$$

Proof. By lemma 2.8, lemma 4.8 and the fact $\mathcal{N}(\mathcal{I}^\vee) = \mathcal{N}(\mathcal{I}^{-1})\mathcal{N}(R^\vee) = (\mathcal{N}(\mathcal{I})\Delta_K)^{-1}$, we have 0

$$\eta_\varepsilon(\mathcal{I}) \leq \frac{\sqrt{N \ln(2N(1+1/\varepsilon))/\pi}}{\lambda_1^{(2)}(\mathcal{I}^\vee)} \leq \sqrt{\ln(2N(1+1/\varepsilon))/\pi} \cdot (\mathcal{N}(\mathcal{I})\Delta_K)^{1/N}.$$

Next, from theorem 4.7, the fact $\det R = \sqrt{\Delta_K}$ and $\det \mathcal{I} = \mathcal{N}(\mathcal{I}) \cdot \sqrt{\Delta_K}$

$$\begin{aligned}
2^{-H_\infty(\mathcal{S})} &\leq \frac{1+\varepsilon}{1-\varepsilon} \cdot \frac{1}{\mathcal{N}(\mathcal{I})} \cdot \max\left\{1, \left(\frac{\eta_\varepsilon(\mathcal{I})}{\sigma}\right)^N\right\} \\
&\leq \frac{1+\varepsilon}{1-\varepsilon} \cdot \frac{1}{\mathcal{N}(\mathcal{I})} \cdot \max\left\{1, \left(\frac{\sqrt{\ln(2N(1+1/\varepsilon))/\pi} \cdot (\mathcal{N}(\mathcal{I})\Delta_K)^{1/N}}{\sigma}\right)^N\right\}
\end{aligned}$$

which completes the proof. □

5 New Leftover Hash Lemma for Discrete Gaussians

Different from the proof approach of regularity lemma in [20,33,49,50], we compute our regularity lemma through algebraic leftover hash lemma [30, Theorem 5.5] and our new lower bounds of the min-entropy of discrete Gaussians. We first recall the algebraic leftover hash lemma over a number field K in [30].

Lemma 5.1 (Generalization of Theorem 5.5 [30]) *Let $K = \mathbb{Q}[\zeta]$ be a number field and $R = \mathcal{O}_K$ be its ring of integers. Let $q \geq 2$ be any integer modulus and $n, m \geq 1$ be dimension parameters. Let $(\mathcal{S}, \mathsf{aux})$ be correlated random variables with $\mathcal{S}$ over R^m. Let $D_0 = (U(R_q^{n\times m} \times R_q^n), \mathsf{aux})$ be the uniform distribution with auxiliary information, and D_1 be the distribution of $(\mathbf{A}, \mathbf{A}\boldsymbol{x}, \mathsf{aux})$ by sampling $\mathbf{A} \overset{\$}{\leftarrow} R_q^{n\times m}$ and $\boldsymbol{x} \leftarrow \mathcal{S}_q$. Then*

$$\mathsf{SD}(D_0, D_1) \leq \frac{1}{2}\sqrt{\sum_{\mathfrak{q}|\langle q\rangle} \mathcal{N}(\mathfrak{q})^n \cdot \mathsf{Col}(\mathcal{S}_\mathfrak{q} \mid \mathsf{aux}) - 1},$$

where $\mathcal{S}_\mathfrak{q} = \mathcal{S} \bmod \mathfrak{q}$ and $\mathsf{Col}(\mathcal{S}_\mathfrak{q} \mid \mathsf{aux})$ is the collision probability of $\mathcal{S}_\mathfrak{q}$ conditioned on aux.

The algebraic leftover hash lemma implies the commonly used integer lattice version if we take the ring of integers R to be $\mathbb{Z}$ and each ideal factor $\mathfrak{q}$ to be integer factor of q. Thus, we can obtain the following LHL for discrete Gaussians over integer lattice $\mathbb{Z}^m$. As we stated in the Contribution section, we do not state any new results on Corollary 10, which can be obtained via a similar min-entropy result from [35, Lemma 2.5] and the standard LHL. To the best of our knowledge, no one have ever written down this leftover hash lemma over discrete Gaussian distribution in integer settings explicitly, so we write it down here as a toy example, and compare it with GPV regularity lemma in Remark 5.2.

Corollary 10. *Let $q = q_1 q_2$ be a product of two primes $q_1, q_2 = \mathsf{poly}(\lambda)$ and $n, m \geq 1$ be lattice parameters. Let $D_0 = U(\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n)$ be the uniform distribution, and D_1 be the distribution of $(\mathbf{A}, \mathbf{A}\boldsymbol{x})$ by sampling $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ and $\boldsymbol{x} \leftarrow D_{\mathbb{Z},\sigma}^m \bmod q$. Let $\sigma > 0$ be gaussian parameter such that $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{\min\{q_1,q_2\}}{\sqrt{\ln(4m)}}$. Then for all $\varepsilon > 0$ such that $m \log \sigma \geq 2\log(1/\varepsilon) + n \log q$, we have $\mathsf{SD}(D_0, D_1) \leq \varepsilon$.*

Proof. Take the ring of integers R to be $\mathbb{Z}$ and secret distribution $\mathcal{S}$ to be $D_{\mathbb{Z},\sigma}^m$ in lemma 5.1, we have

$$
\begin{aligned}
\mathsf{SD}(D_0, D_1) &\leq \frac{1}{2}\sqrt{q_1^n \cdot \mathsf{Col}(D_{\mathbb{Z},\sigma}^m \bmod q_1) + q_2^n \cdot \mathsf{Col}(D_{\mathbb{Z},\sigma}^m \bmod q_2) + q^n \cdot \mathsf{Col}(D_{\mathbb{Z},\sigma}^m \bmod q)} \\
&\leq \frac{1}{2}\sqrt{q_1^n \cdot 2^{-H_\infty(D_{\mathbb{Z},\sigma}^m \bmod q_1)} + q_2^n \cdot 2^{-H_\infty(D_{\mathbb{Z},\sigma}^m \bmod q_2)} + q^n \cdot 2^{-H_\infty(D_{\mathbb{Z},\sigma}^m \bmod q)}} \\
&\leq \frac{1}{2}\sqrt{(q_1^n + q_2^n + q^n) \cdot 2^{-m\log\sigma + 1}} \qquad (8) \\
&\leq \sqrt{q^n \cdot 2^{-m\log\sigma}} \leq \varepsilon,
\end{aligned}
$$

where (8) comes from corollary 4. □

Remark 5.2 (Comparison with Corollary 5.4 in [20]) *The regularity lemma in [20] only proves the case for $m \geq 2n\log q$ and $\sigma \geq \omega(\sqrt{\log m})$. For a fair comparison and based on techniques from [20], we can make modifications to their statement, which appears at lemma 2.12. Consider the LHL scenario ($\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ is chosen uniformly at random), lemma 2.12 requires $\sigma \geq 2q^{\frac{n}{m}} \cdot \sqrt{\ln(2m(1+1/\varepsilon))/\pi}$ while the requirement of our corollary 10 is $\sigma > q^{\frac{n}{m}} \cdot \left(\frac{1}{\varepsilon}\right)^{\frac{1}{m}}$. Both requirements have the factor $q^{\frac{n}{m}}$. For a negligible distance $\varepsilon = 2^{-\omega(\log\lambda)}$, our regularity lemma can save the Gaussian parameter by a factor $\omega(\sqrt{\log\lambda})$.*

The following lemma is our new strategy for a fine-grained analysis of algebraic leftover hash lemma.

Theorem 5.3 *Let K be M-th cyclotomic field with degree $N = \varphi(M)$, and $q, n, m \geq 1$ be lattice parameters with q prime. Let $qR = \mathfrak{q}_1^e \mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$ be the ideal factorization of qR such that $\mathcal{N}(\mathfrak{q}_i) = q^f$ and $N = efg$. Let $(\mathcal{S}, \mathsf{aux})$ be correlated random variables with $\mathcal{S}$ over R^m, such that for all ideal factor $\mathfrak{q} \mid \langle q\rangle$ with $N(\mathfrak{q}) = q^t$ and $\mathfrak{q} \neq R$, such that $H_\infty(\mathcal{S}_\mathfrak{q} \mid \mathsf{aux}) \geq mt\log\sigma - \delta$ for some $\sigma, \delta > 0$. Let $D_0 = (U(R_q^{n\times m} \times R_q^n), \mathsf{aux})$ be the uniform distribution with auxiliary information, and D_1 be the distribution of $(\mathbf{A}, \mathbf{A}\boldsymbol{x}, \mathsf{aux})$ by sampling $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$ and $\boldsymbol{x} \leftarrow \mathcal{S}_\mathfrak{q}$. For any positive $\varepsilon < 2^{(\delta-1)/2}$, if $mf\log\sigma \geq 2\log(1/\varepsilon) + nf\log q + \log g + \delta$, we have $\mathsf{SD}(D_0, D_1) \leq \varepsilon$.*

Proof. Let $\theta = \frac{q^{nf}}{\sigma^{mf}} \leq \varepsilon^2/(2^\delta \cdot g) \leq 1/2g$.

By the properties of entropy, $\mathsf{Col}(\mathcal{S}_\mathfrak{q} \mid \mathsf{aux}) \le 2^{-H_\infty(\mathcal{S}_\mathfrak{q}|\mathsf{aux})} \le 2^\delta \cdot \sigma^{mt}$ for every $\mathcal{N}(\mathfrak{q}) = q^t$, and the fact $\mathcal{N}(R)\mathsf{Col}(\mathcal{S}_R \mid \mathsf{aux}) = 1$, then we compute that

$$\begin{aligned}
\sum_{\mathfrak{q}|\langle q\rangle} \mathcal{N}(\mathfrak{q})^n \mathsf{Col}(\mathcal{S}_\mathfrak{q} \mid \mathsf{aux}) - 1 &\le 2^\delta \cdot \left(\sum_{0\le i_1,\cdots,i_g\le e} \frac{\mathcal{N}(\mathfrak{q}_1^{i_1}\cdots\mathfrak{q}_1^{i_g})^n}{\sigma^{mf(i_1+\cdots+i_g)}} - 1 \right) \\
&= 2^\delta \cdot \left(\sum_{0\le i_1,\cdots,i_g\le e} \frac{q^{nf(i_1+\cdots+i_g)}}{\sigma^{mf(i_1+\cdots+i_g)}} - 1 \right) \\
&= 2^\delta \cdot \left(\left(\sum_{i=0}^{e} \theta^i \right)^g - 1 \right) = 2^\delta \left(\left(\frac{1-\theta^{e+1}}{1-\theta} \right)^g - 1 \right) \\
&< 2^\delta \cdot ((1+2\theta)^g - 1) \le 2^{\delta+2} \cdot g \cdot \theta.
\end{aligned}$$

The last two inequalities hold due to $1/(1-x) \le 1+2x$ for all $x \in (0, 1/2)$, and $(1+x)^g \le 1 + 2gx$ for all $x \le 1/g$, respectively. Therefore, it together with lemma 5.1, allows us to obtain $\mathsf{SD}(D_0, D_1) \le \varepsilon$, which completes the proof. □

We can take discrete Gaussians as an example whose lower bound of min-entropy matches the form of theorem 5.3.

Corollary 11. *Adopt notations in lemma 5.3. Take $\mathcal{S} = (D^{\mathsf{coeff}}_{R,\sigma})^m$ for $\sigma > 0$ and $\mathsf{aux} = \emptyset$. For any $\varepsilon \in (0, \frac{1}{\sqrt{2}})$, if the following condition holds,*

– $\sigma \le \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4m)}}$ *and* $mf \log \sigma \ge 2\log(1/\varepsilon) + nf \log q + \log g + m$*;*

we have $\mathsf{SD}(D_0, D_1) \le \varepsilon$*.*

The regularity lemma in [33] is presented in Lemma 2.13. The Gaussian parameter in their regularity lemma is related to the discrete Gaussian over canonical lattice $\sigma(R)$, while ours is with respect to coefficient lattice $\phi(R) = \mathbb{Z}^N$, hence comparing in the case that M is a power of two is a fair choice. In the following remark, the secret $\boldsymbol{s}$ is sampled from $(D^{\mathsf{coeff}}_{R,\sigma})^m$.

Remark 5.4 (Comparison with Corollary 7.5 in [33]) *The regularity lemma in [33] requires the public matrix $\mathbf{A}$ to be a concatenation of an identity matrix $\mathbf{I}_n$ and a matrix $\bar{\mathbf{A}}^{n\times m}$, while our regularity lemma requires the public matrix to be uniformly at random, which is more suitable for the LHL scenarios. The constraint of their Gaussian parameter is $m \log \frac{\sigma}{2\sqrt{N}} > \left(n + \frac{2}{N}\right) \log q$ which implicitly requires $\sigma > 2\sqrt{N}$. Let $\varepsilon = \mathsf{negl}(\lambda)$, then as long as $mf \ge 2\log\frac{1}{\varepsilon} = \omega(\log\lambda)$, our Gaussian parameter σ is saved by at least a factor of $2\sqrt{N}$ under the same R, module rank n, m and prime modulus q. Unlike [33], our regularity lemma cannot set the parameters m, n, f as all constants, but this is a necessary lower bound for the uniformity over a prime ideal $\mathfrak{q}$, which has been proved in [33]. We make modifications to the regularity lemma in [33] and get Corollary 2, where the public matrix is uniform at random, which also requires $m \ge n + \omega(\log\lambda)$.*

6 Hardness: MLWE in Hermite Normal Form with Linear Leakage

In this section, we will show that the decision version of MLWE is hard, even after leaking a number of $\log q$-bit linear terms correlated to the coefficients of the secret and the error. Called as extended MLWE assumption, this sort of MLWE assumption has been used in several lattice-based primitives [15, 31], while its hardness has not been established on vanilla MLWE assumption or worst-case lattice problems to our best knowledge. We restrict the choice of number field $K = \mathbb{Q}[x]/(x^N + 1)$ to be M-th cyclotomic number field where M is a power of two, $N = \varphi(M) = M/2$ is the degree and its ring of integers $R = \mathbb{Z}[x]/(x^N + 1)$.

We first recall the definition of extended MLWE assumption from [15]. Apart from [15], our definition and reduction do not have restrictions on the choice of matrix $\mathbf{M} \in \mathbb{Z}_q^{k\times N\cdot(n+m)}$.

Definition 6.1 (ExtMLWE) *Let λ be a security parameter, $n, m, q \geq 1$ be lattice parameters and χ be an error distribution over R_q. Let $k \geq 1$ be the number of linearly leakaged terms. For any matrix $\mathbf{M} \in \mathbb{Z}_q^{k\times N\cdot(n+m)}$, we say that $\mathsf{ExtMLWE}_{\chi,\mathbf{M}}^{n,m,q}$ is hard, if it holds for every PPT distinguisher $\mathcal{A}$ that*

$$\left|\Pr\left[\mathcal{A}\left(1^\lambda, \mathbf{A}, \mathbf{A}\boldsymbol{s}+\boldsymbol{e}, \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)=1\right] - \Pr\left[\mathcal{A}\left(1^\lambda, \mathbf{A}, \boldsymbol{u}, \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)=1\right]\right| \leq \mathsf{negl}(\lambda),$$

where $\mathbf{A} \xleftarrow{\$} R_q^{m\times n}$, $\boldsymbol{s} \xleftarrow{\$} \chi^n$, $\boldsymbol{e} \leftarrow \chi^m$, $\boldsymbol{u} \xleftarrow{\$} R_q^m$ and $\phi : R_q^{n+m} \to \mathbb{Z}_q^{N\cdot(n+m)}$ is the coefficient embedding map.

Next, we will define the entropic MLWE with extra $k \log q$ bits of linear leakage assumption, denoted as ent-MLWE-LL, which is generalized from the LWE assumption with entropic secret distribution [?, 7]. The purpose of defining this sort of assumption is that we need a medium MLWE problem in which both secret $\boldsymbol{s}$ and $\boldsymbol{e}$ are chosen from discrete Gaussian distributions but with different Gaussian parameters. It is also worth to note that ExtMLWE is a kind of ent-MLWE-LL where each entry of secret and error follows the same distribution over R_q.

Definition 6.2 (ent-MLWE with Linear Leakage) *Let λ be a security parameter, $n, m, q \geq 1$ be lattice parameters, $\mathcal{S}$ be an entropic secret distribution over R_q^n and χ be an error distribution over R_q. Let $k \geq 1$ be the number of linearly leakaged terms. For any matrix $\mathbf{M} \in \mathbb{Z}_q^{k\times N\cdot(n+m)}$, we say that $\mathsf{ent\text{-}MLWE\text{-}LL}_{\mathcal{S},\chi}^{n,m,q,\mathbf{M}}$ is hard, if it holds for every PPT distinguisher $\mathcal{A}$ that*

$$\left|\Pr\left[\mathcal{A}\left(1^\lambda, \mathbf{A}, \mathbf{A}\boldsymbol{s}+\boldsymbol{e}, \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)=1\right] - \Pr\left[\mathcal{A}\left(1^\lambda, \mathbf{A}, \boldsymbol{u}, \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)=1\right]\right| \leq \mathsf{negl}(\lambda),$$

where $\mathbf{A} \xleftarrow{\$} R_q^{m\times n}$, $\boldsymbol{s} \xleftarrow{\$} \mathcal{S}$, $\boldsymbol{e} \leftarrow \chi^m$, $\boldsymbol{u} \xleftarrow{\$} R_q^m$. and $\phi : R_q^{n+m} \to \mathbb{Z}_q^{N\cdot(n+m)}$ is the coefficient embedding map.

The following is the main theorem of this section. It gives a reduction from the vanilla MLWE assumption to the extended MLWE assumption. This established an asymptotic hardness of extended MLWE assumption for any prime modulus q.

Theorem 6.3 *Let λ be a security parameter. Let $n, \ell, m, q = \mathsf{poly}(\lambda)$ be lattice parameters such that q is a prime and $qR = \mathfrak{q}_1^e \cdots \mathfrak{q}_g^e$ is the ideal factorization of qR where $\mathcal{N}(\mathfrak{q}_i) = q^f$ for each $i \in [g]$ and $N = efg$. Let k be a positive integer and $\mathbf{M} \in \mathbb{Z}_q^{k \times N\cdot(n+m)}$ be any matrix related to linear leakage. Let $\sigma, \sigma', \beta, \gamma > 0$ be Gaussian parameters and $\chi = D_{R,\gamma}^{\mathsf{coeff}}$ be a discrete Gaussian distribution over R. If the parameters satisfy the following constraints:*

- $\sigma < \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4N)}}$, $\sqrt{\gamma^2 - \sigma^2} \geq \omega(\sqrt{\log \lambda})$;
- $\gamma \geq \sqrt{\left(C_0 \beta \sigma' \sqrt{2N}\left(\sqrt{m} + \sqrt{n} + \sqrt{\lambda}\right)\right)^2 + \omega(\log \lambda)}$ *for a global constant* $C_0 \leq 1$;
- $nf \log \sigma \geq ((\ell+1)f + k)\log q + \log g + \sqrt{2\pi}\log \mathbf{e} \cdot Nn \cdot \frac{\sigma}{\sigma'} + n(\boldsymbol{e}^{-N} + 1) + \omega(\log \lambda)$;

then there exists a PPT *reduction from $\mathsf{MLWE}_{\ell, m-1, q, D_{R,\beta}^{\mathsf{coeff}}}$ to $\mathsf{ExtMLWE}_{\chi, \mathbf{M}}^{n,m,q}$.*

The proof of theorem 6.3 is obtained by combining two reductions, as described in lemma 6.4 and lemma 6.5.

The proof of lemma 6.4 is mainly adapted from the lossy framework in [3, Theorem 4.1]. We also apply the noisy lossiness framework in [7] to compute the remaining entropy of the secret $\boldsymbol{s}$. It is worth to note that we cannot apply the framework of [3, 7] to directly prove the hardness of ExtMLWE assumption based on MLWE assumption, due to the requirement that Gaussian parameter of the error $\boldsymbol{e}$ needs to be larger than the bound of secret $\boldsymbol{s}$, which is closely related to the Gaussian width of $\boldsymbol{s}$. Therefore, in lemma 6.4, with the hardness of MLWE, we prove the hardness of MLWE where the secret $\boldsymbol{s}$ and error $\boldsymbol{e}$ are chosen from discrete Gaussians with different parameters. In lemma 6.5, thanks to the linearity of both $\mathbf{A}\boldsymbol{s} + \boldsymbol{e}$ and the $k \log q$ bits of leakage, we utilize the *sum of discrete Gaussians* lemma from [37] to give a reduction from our medium MLWE assumption to the extended MLWE assumption. We put the proof to Appendix B.2.

Lemma 6.4 ($\mathsf{MLWE}_{\ell,m-1,q,D_{R,\beta}^{\mathsf{coeff}}}$ to ent-MLWE-LL$_{(D_{R,\sigma}^{\mathsf{coeff}})^n, D_{R,\gamma}^{\mathsf{coeff}}}^{n,m,q,\mathbf{M}}$) *Let λ be a security parameter. Let $n, m, \ell, q \geq 1$ be* LWE *parameters such that q is a prime number, and the ideal factorization of qR is $qR = \mathfrak{q}_1^e \mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$ such that $\mathcal{N}(\mathfrak{q}_j) = f$ for $j \in [g]$ and $N = efg$. Let $\sigma, \sigma', \beta, \gamma$ be Gaussian parameters such that $\sigma < \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4N)}}$ and $\gamma \geq \sqrt{\left(C_0 \beta \sigma' \sqrt{2N}\left(\sqrt{m} + \sqrt{n} + \sqrt{\lambda}\right)\right)^2 + \omega(\log \lambda)}$ for a global constant $C_0 \leq 1$. Let k be a positive integer and $\mathbf{M} \in \mathbb{Z}_q^{k \times N\cdot(n+m)}$ be any matrix related to linear leakage. If the parameters satisfy the following constraint:*

$$nf \log \sigma \geq ((\ell+1)f + k)\log q + \log g + \sqrt{2\pi}\log \mathbf{e} \cdot Nn \cdot \frac{\sigma}{\sigma'} + n(\boldsymbol{e}^{-N} + 1) + \omega(\log \lambda)$$

then $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$ *is hard under the assumptions that* $\mathsf{MLWE}_{\ell,m-1,q,D^{\mathsf{coeff}}_{R,\beta}}$ *is hard.*

Lemma 6.5 ($\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$ to $\mathsf{ExtMLWE}^{n,m,q}_{D^{\mathsf{coeff}}_{R,\gamma},\mathbf{M}}$) *Let* $n, m, q \geq 1$ *be* LWE *parameters and* $\sigma, \gamma > 0$ *be two Gaussian parameters s.t.* $\sigma \geq \sqrt{2}\eta_\varepsilon(\mathbb{Z}^{nN})$ *and* $\sqrt{\gamma^2 - \sigma^2} \geq \sqrt{2}\eta_\varepsilon(\mathbb{Z}^{nN})$ *for some* $\varepsilon = \mathsf{negl}(\lambda)$*. For any positive integer* k *and any matrix* $\mathbf{M} \in \mathbb{Z}_q^{k \times N \cdot (n+m)}$*, there exists a* PPT *reduction from* $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$ *to* $\mathsf{ExtMLWE}^{n,m,q}_{D^{\mathsf{coeff}}_{R,\gamma},\mathbf{M}}$.

References

1. P. Abla, F.-H. Liu, H. Wang, and Z. Wang. Ring-based identity based encryption - asymptotically shorter MPK and tighter security. In K. Nissim and B. Waters, editors, *TCC 2021, Part III*, volume 13044 of *LNCS*, pages 157–187. Springer, Cham, Nov. 2021.
2. A. Akavia, S. Goldwasser, and V. Vaikuntanathan. Simultaneous hardcore bits and cryptography against memory attacks. In O. Reingold, editor, *TCC 2009*, volume 5444 of *LNCS*, pages 474–495. Springer, Berlin, Heidelberg, Mar. 2009.
3. J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs. Learning with rounding, revisited - new reduction, properties and applications. In Canetti and Garay [9], pages 57–74.
4. B. Applebaum, D. Cash, C. Peikert, and A. Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In S. Halevi, editor, *CRYPTO 2009*, volume 5677 of *LNCS*, pages 595–618. Springer, Berlin, Heidelberg, Aug. 2009.
5. W. Banaszczyk. Inequalities for convex bodies and polar reciprocal lattices inrn. *Discrete Comput. Geom.*, 13(2):217–231, dec 1995.
6. B. Barak, Y. Dodis, H. Krawczyk, O. Pereira, K. Pietrzak, F.-X. Standaert, and Y. Yu. Leftover hash lemma, revisited. In Rogaway [48], pages 1–20.
7. Z. Brakerski and N. Döttling. Hardness of LWE on general entropic distributions. In A. Canteaut and Y. Ishai, editors, *EUROCRYPT 2020, Part II*, volume 12106 of *LNCS*, pages 551–575. Springer, Cham, May 2020.
8. Z. Brakerski and N. Döttling. Lossiness and entropic hardness for ring-LWE. In R. Pass and K. Pietrzak, editors, *TCC 2020, Part I*, volume 12550 of *LNCS*, pages 1–27. Springer, Cham, Nov. 2020.
9. R. Canetti and J. A. Garay, editors. *CRYPTO 2013, Part I*, volume 8042 of *LNCS*. Springer, Berlin, Heidelberg, Aug. 2013.
10. Y. Chen, Z. Hu, Q. Liu, H. Luo, and Y. Tu. On the hardness of $\mathsf{S}|\mathsf{LWE}\rangle$ with gaussian and other amplitudes. Cryptology ePrint Archive, Report 2023/1498, 2023.
11. K. Conrad. The different ideal. Expository papers. Available at: `https://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf`.
12. K. Conrad. Factoring ideals after dedekind. Expository papers/Lecture notes. Available at: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/dedekindf.pdf`.
13. D. Dadush and L. Ducas. Introduction, 2018. Intro to Lattice Algs and Crypto, Lecture notes. Available at: `https://homepages.cwi.nl/~dadush/teaching/lattices-2018/notes/lecture-1.pdf`, last accessed 10 Apr 2024.

14. D. Dadush and L. Ducas. Periodic gaussian, discrete gaussian and transference, 2018. Intro to Lattice Algs and Crypto, Lecture notes. Available at: `https://homepages.cwi.nl/~dadush/teaching/lattices-2018/notes/lecture-7.pdf`, last accessed 10 Apr 2024.
15. R. del Pino, T. Espitau, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, M. Rossi, and M.-J. Saarinen. Raccoon. Technical report, National Institute of Standards and Technology, 2023. Available at : `https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/round-1/spec-files/raccoon-spec-web.pdf`.
16. R. del Pino, S. Katsumata, T. Prest, and M. Rossi. Raccoon: A masking-friendly signature proven in the probing model. In L. Reyzin and D. Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 409–444. Springer, Cham, Aug. 2024.
17. Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan. Public-key encryption schemes with auxiliary inputs. In D. Micciancio, editor, *TCC 2010*, volume 5978 of *LNCS*, pages 361–381. Springer, Berlin, Heidelberg, Feb. 2010.
18. Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith. Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. *SIAM Journal on Computing*, 38(1):97–139, 2008.
19. P. D. Domich, R. Kannan, and L. E. Trotter. Hermite normal form computation using modulo determinant arithmetic. *Mathematics of Operations Research*, 12(1):50–59, 1987.
20. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In R. E. Ladner and C. Dwork, editors, *40th ACM STOC*, pages 197–206. ACM Press, May 2008.
21. S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan. Robustness of the learning with errors assumption. In A. C.-C. Yao, editor, *ICS 2010*, pages 230–240. Tsinghua University Press, Jan. 2010.
22. S. Han, S. Liu, Z. Wang, and D. Gu. Almost tight multi-user security under adaptive corruptions from LWE in the standard model. In H. Handschuh and A. Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 682–715. Springer, Cham, Aug. 2023.
23. J. Howe, T. Prest, T. Ricosset, and M. Rossi. Isochronous gaussian sampling: From inception to implementation. In J. Ding and J.-P. Tillich, editors, *Post-Quantum Cryptography - 11th International Conference, PQCrypto 2020*, pages 53–71. Springer, Cham, 2020.
24. R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions (extended abstracts). In *21st ACM STOC*, pages 12–24. ACM Press, May 1989.
25. H. Jin, F.-H. Liu, Z. Wang, Y. Yu, and D. Gu. Revisiting the robustness of (r/m)LWR under polynomial moduli with applications to lattice-based compact SO-CCA security. Cryptology ePrint Archive, Paper 2024/1696, 2024.
26. S. Katsumata and S. Yamada. Partitioning via non-linear polynomial functions: More compact IBEs from ideal lattices and bilinear maps. In J. H. Cheon and T. Takagi, editors, *ASIACRYPT 2016, Part II*, volume 10032 of *LNCS*, pages 682–712. Springer, Berlin, Heidelberg, Dec. 2016.
27. Q. Lai, F.-H. Liu, and Z. Wang. Almost tight security in lattices with polynomial moduli - PRF, IBE, all-but-many LTF, and more. In A. Kiayias, M. Kohlweiss, P. Wallden, and V. Zikas, editors, *PKC 2020, Part I*, volume 12110 of *LNCS*, pages 652–681. Springer, Cham, May 2020.

28. A. Langlois and D. Stehlé. Worst-case to average-case reductions for module lattices. *DCC*, 75(3):565–599, 2015.
29. H. Lin, M. Wang, J. Zhuang, and Y. Wang. Hardness of entropic module-lwe. *Theor. Comput. Sci.*, 999(C), July 2024.
30. F.-H. Liu and Z. Wang. Rounding in the rings. In D. Micciancio and T. Ristenpart, editors, *CRYPTO 2020, Part II*, volume 12171 of *LNCS*, pages 296–326. Springer, Cham, Aug. 2020.
31. V. Lyubashevsky, N. K. Nguyen, and M. Plançon. Lattice-based zero-knowledge proofs and applications: Shorter, simpler, and more general. In Y. Dodis and T. Shrimpton, editors, *CRYPTO 2022, Part II*, volume 13508 of *LNCS*, pages 71–101. Springer, Cham, Aug. 2022.
32. V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. In H. Gilbert, editor, *EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, Berlin, Heidelberg, May / June 2010.
33. V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for ring-LWE cryptography. In T. Johansson and P. Q. Nguyen, editors, *EUROCRYPT 2013*, volume 7881 of *LNCS*, pages 35–54. Springer, Berlin, Heidelberg, May 2013.
34. D. Micciancio. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions from worst-case complexity assumptions. In *43rd FOCS*, pages 356–365. IEEE Computer Society Press, Nov. 2002.
35. D. Micciancio and P. Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In Rogaway [48], pages 465–484.
36. D. Micciancio and C. Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In D. Pointcheval and T. Johansson, editors, *EUROCRYPT 2012*, volume 7237 of *LNCS*, pages 700–718. Springer, Berlin, Heidelberg, Apr. 2012.
37. D. Micciancio and C. Peikert. Hardness of SIS and LWE with small parameters. In Canetti and Garay [9], pages 21–39.
38. D. Micciancio and O. Regev. Worst-case to average-case reductions based on Gaussian measures. In *45th FOCS*, pages 372–381. IEEE Computer Society Press, Oct. 2004.
39. D. Micciancio and A. Suhl. Simulation-secure threshold PKE from LWE with polynomial modulus. Cryptology ePrint Archive, Report 2023/1728, 2023.
40. D. Micciancio and M. Walter. Gaussian sampling over the integers: Efficient, generic, constant-time. In J. Katz and H. Shacham, editors, *CRYPTO 2017, Part II*, volume 10402 of *LNCS*, pages 455–485. Springer, Cham, Aug. 2017.
41. C. Peikert. Limits on the hardness of lattice problems in lp norms. In *Twenty-Second Annual IEEE Conference on Computational Complexity (CCC'07)*, pages 333–346, 2007.
42. C. Peikert. An efficient and parallel Gaussian sampler for lattices. In T. Rabin, editor, *CRYPTO 2010*, volume 6223 of *LNCS*, pages 80–97. Springer, Berlin, Heidelberg, Aug. 2010.
43. C. Peikert and A. Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In S. Halevi and T. Rabin, editors, *TCC 2006*, volume 3876 of *LNCS*, pages 145–166. Springer, Berlin, Heidelberg, Mar. 2006.
44. C. Peikert and A. Rosen. Lattices that admit logarithmic worst-case to average-case connection factors. In D. S. Johnson and U. Feige, editors, *39th ACM STOC*, pages 478–487. ACM Press, June 2007.
45. R. D. Pino, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, and M.-J. O. Saarinen. Threshold raccoon: Practical threshold signatures from standard lattice assumptions. In M. Joye and G. Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 219–248. Springer, Cham, May 2024.

46. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In H. N. Gabow and R. Fagin, editors, *37th ACM STOC*, pages 84–93. ACM Press, May 2005.
47. R. Renner and S. Wolf. Smooth rényi entropy and applications. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, pages 233–, 2004.
48. P. Rogaway, editor. *CRYPTO 2011*, volume 6841 of *LNCS*. Springer, Berlin, Heidelberg, Aug. 2011.
49. M. Rosca, D. Stehlé, and A. Wallet. On the ring-LWE and polynomial-LWE problems. In J. B. Nielsen and V. Rijmen, editors, *EUROCRYPT 2018, Part I*, volume 10820 of *LNCS*, pages 146–173. Springer, Cham, Apr. / May 2018.
50. D. Stehlé and R. Steinfeld. Making NTRU as secure as worst-case problems over ideal lattices. In K. G. Paterson, editor, *EUROCRYPT 2011*, volume 6632 of *LNCS*, pages 27–47. Springer, Berlin, Heidelberg, May 2011.
51. W. Stein. A brief introduction to classical and adelic algrbraic number theory, 2004. `https://wstein.org/129/ant/ant.pdf`, last accessed 16 Otc 2024.

Appendix

A Missing Definitions

A.1 Algebraic Number Theory Background

Algebraic number theory is the study of number fields. Below we present the requisite concepts and notations used in this paper. More backgrounds and complete proofs can be found in any introductory book on the subject, e.g., [11, 51].

The Space H

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

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

As described in the work [32], we can equip H with norms, which would naturally define norms of elements in a number field or ideal lattice via an embedding that maps field elements into H. We will present more details next.

It is not hard to verify that H equipped with the inner product induced by $\mathbb{C}^N$, is isomorphic to $\mathbb{R}^N$ as an inner product space. This can be seen via the orthonormal basis $\{\boldsymbol{h}_i\}_{i\in[n]}$ defined as: for $j \in [N]$, let $\boldsymbol{e}_i \in \mathbb{C}^N$ be the vector with 1 in its jth coordinate, and 0 elsewhere; then for $j \in [s_1]$, we define $\boldsymbol{h}_j = \boldsymbol{e}_j \in \mathbb{C}^N$, and for $s_1 < j \leq s_1 + s_2$ we take $\boldsymbol{h}_j = \frac{1}{\sqrt{2}}(\boldsymbol{e}_j + \boldsymbol{e}_{j+s_2})$ and $\boldsymbol{h}_{j+s_2} = \frac{1}{\sqrt{-2}}(\boldsymbol{e}_j - \boldsymbol{e}_{j+s_2})$.

We can equip H with the ℓ_2 and ℓ_∞ norms induced on it from $\mathbb{C}^N$. Namely, for $\boldsymbol{x} \in H$ we have $\|\boldsymbol{x}\|_2 = \sum_i (|x_i|^2)^{1/2} = \sqrt{\langle \boldsymbol{x}, \boldsymbol{x} \rangle}$ and $\|\boldsymbol{x}\|_\infty = \max_i |x_i|$. ℓ_p norms can be defined similarly.

Number Fields and Their Geometry

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

The elements in K can be viewed as $(N-1)$-degree polynomials in $\mathbb{Q}[x]$, so we can consider a natural coefficient embedding of K to $\mathbb{Q}^N$. We define the *coefficient embedding* $\phi : K \to \mathbb{Q}^N$ by mapping $x = \sum_{i=0}^{N-1} x_i \zeta^i$ to $(x_0, x_1, \cdots, x_{N-1})^\top$. For any $x \in K$, we define the coefficient 2-norm of x is $\|x\|_{\mathsf{coeff}} = \|\phi(x)\|$. We extend the definition of coefficient embedding to the map from K^ℓ to $\mathbb{Q}^{\ell N}$ by embedding each field element K as a vector in $\mathbb{Q}^N$.

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

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

By identifying elements of K and their canonical embeddings on H, we can define the norms on K. For any $x \in K$ and any $p \in [1, \infty]$, the ℓ_p norm of x is simply $\|x\|_p = \|\sigma(x)\|_p$. Then we have that $\|xy\|_p \leq \|x\|_\infty \cdot \|y\|_p \leq \|x\|_p \cdot \|y\|_p$, for any $x, y \in K$ and $p \in [1, \infty]$. We omit the subscript p if $p = 2$.

Let $\mathbf{V}_f = (\zeta_i^{j-1})_{i,j\in[n]}$ be the *Vandermonde Matrix* of the polynomial f, where ζ_i are N distinct roots of f. $\mathbf{V}_f$ represents a linear transformation from coefficient embedding to canonical embedding, i.e. for all $x \in K$, $\sigma(x) = \mathbf{V}_f \phi(x)$. Particularly, if $K = \mathbb{Q}[x]/(x^N + 1)$ is the M-th cyclotomic field with M power of 2, then $\mathbf{V}_f/\sqrt{N}$ is a unitary matrix, indicating that $\|x\| = \sqrt{N} \cdot \|x\|_{\mathsf{coeff}}$.

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

Ring of Integers and Ideals

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

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

An ideal $\mathfrak{p} \subsetneq \mathcal{O}_K$ is *prime* if $ab \in \mathfrak{p}$ for some $a, b \in \mathcal{O}_K$, then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ (or both). In $\mathcal{O}_K$, an ideal $\mathfrak{p}$ is prime if and only if it is maximal, which implies that the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field of order $\mathcal{N}(\mathfrak{p})$. An ideal $\mathcal{I}$ is called to *divide* ideal $\mathcal{J}$, which is written as $\mathcal{I} \mid \mathcal{J}$, if there exists another ideal $\mathcal{H} \in \mathcal{O}_K$ such that $\mathcal{J} = \mathcal{H}\mathcal{I}$. Two ideal $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}_K$ are *coprime* if $\mathcal{I} + \mathcal{J} = \mathcal{O}_K$.

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

Duality

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

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

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

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

Ideal Lattices

Recall that a fractional ideal $\mathcal{I}$ of $\mathcal{O}_K$ has a $\mathbb{Z}$-basis $\mathbf{B} = \{b_1, \cdots, b_N\}$. Therefore, under the canonical embedding σ, the ideal yields a full-rank lattice $\sigma(\mathcal{I})$ have basis $\{\sigma(b_1), \cdots, \sigma(b_N)\} \subset H$. For convenience, we often identify an ideal with its embedded lattice, and then speak of several fundamental properties of the lattice, e.g., the minimal distance $\lambda_1(\mathcal{I})$ of an ideal, etc.

The *discriminant* Δ_K of a number field K is defined to be the square of the fundamental volume of $\sigma(\mathcal{O}_K)$, the lattice of the embedded ring of integers. Equivalently, $\Delta_K = |\det(\text{Tr}(b_i \cdot b_j))|$ where $b_1, \cdots b_N$ is any integer basis of $\mathcal{O}_K$. Consequently, the fundamental volume of any ideal lattice $\sigma(\mathcal{I})$ is $\mathcal{N}(\mathcal{I}) \cdot \sqrt{\Delta_K}$. The discriminant of the M-th cyclotomic number field $K = \mathbb{Q}(\zeta_M)$ of degree $N = \varphi(M)$ is known to be $\Delta_K = M^N / (\prod_{p|M} p^{N/(p-1)}) \leq N^N$, where the product in the denominator runs over all primes p dividing M.

Prime Splitting

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

Lemma A.1 (Dedekind [12]) *Let $K = \mathbb{Q}(\zeta)$ be a number field for $\zeta \in \mathcal{O}_K$, and $F(x)$ be the minimal polynomial of ζ in $\mathbb{Z}[x]$. For any prime p, the ideal*

$p\mathcal{O}_K$ factors into prime ideals as $\langle q \rangle = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_g^{e_g}$, where $\mathcal{N}(\mathfrak{q}_i) = q^{f_i}$ for $f_i = [\mathcal{O}_K/\mathfrak{q}_i : \mathbb{Z}_q]$, and $N = \sum_{i=1}^{g} e_i f_i$.

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

For each $\mathfrak{q}_i$, we have $\mathfrak{q}_i \mid q\mathcal{O}_K$, which can be written as $\mathfrak{q}_i \mid \langle q \rangle$, and call $\mathfrak{q}_i$ a factor of $\langle q \rangle$.

Cyclotomic Number fields

Here we list some useful facts about cyclotomic number fields and we can refer more details to [32, 51].

Let $q \in \mathbb{Z}$ be any integer prime numbers and the factorization of ideal $\langle q \rangle = qR$ is as follows. Let $q' = q^h$ $(h \geq 0)$ be the largest power of q that divides m, let $e = \varphi(q')$ and let f be the multiplicative order of q modulo m/q'. Then $\langle q \rangle = \mathfrak{q}_1^e \mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$, where $\mathfrak{q}_i$ are $g = N/(ef)$ distinct prime ideals of each norm q^f. Furthermore, these prime ideals are in the form $\mathfrak{q}_i = \langle q, f_i(\zeta) \rangle$, where $\Phi_m(x) = f_1(x)^e f_2(x)^e \cdots f_g(x)^e$ is the factorization of the cyclotomic polynomial $\Phi_m(x)$ into f-degree monic irreducible polynomials $f_i(x)$ in $\mathbb{Z}_q[x]$.

A.2 Ring\Module Learning with Errors

We recall the definition of ring and module learning with errors problem and their various forms.

Definition A.2 (RLWE [32]) *Let $K = \mathbb{Q}(\zeta)$ be a number field with degree N and R be its ring of integers. Decision* RLWE *problem with lattice parameters $m, q \geq 2$, and an error distribution χ such that $\mathsf{Supp}(\chi) \subseteq R_q$ denoted as $\mathsf{RLWE}_{m,q,\chi}$ is defined as follows. We say that $\mathsf{RLWE}_{m,q,\chi}$ is hard, if it holds for every* PPT *distinguisher $\mathcal{A}$ that*

$$\left|\Pr[\mathcal{A}(1^\lambda, \boldsymbol{a}, \boldsymbol{a} \cdot s + \boldsymbol{e}) = 1] - \Pr[\mathcal{A}(1^\lambda, \boldsymbol{a}, \boldsymbol{u}) = 1]\right| \leq \mathsf{negl}(\lambda),$$

where $\boldsymbol{a} \stackrel{\$}{\leftarrow} R_q^m$, $s \stackrel{\$}{\leftarrow} R_q$, $\boldsymbol{e} \leftarrow \chi^m$ and $\boldsymbol{u} \stackrel{\$}{\leftarrow} R_q^m$.

Definition A.3 (MLWE [28]) *Let $K = \mathbb{Q}(\zeta)$ be a number field with degree N and R be its ring of integers. Decision* MLWE *problem with lattice parameters $n \geq 1, m, q \geq 2$, and an error distribution χ over R_q or $K_\mathbb{R} \bmod qR$ denoted as $\mathsf{MLWE}_{n,m,q,\chi}$ is defined as follows. We say that $\mathsf{MLWE}_{n,m,q,\chi}$ is hard, if it holds for every* PPT *distinguisher $\mathcal{A}$ that*

$$\left|\Pr[\mathcal{A}(1^\lambda, \mathbf{A}, \mathbf{A}\boldsymbol{s} + \boldsymbol{e}) = 1] - \Pr[\mathcal{A}(1^\lambda, \mathbf{A}, \boldsymbol{u} + \boldsymbol{e}) = 1]\right| \leq \mathsf{negl}(\lambda),$$

where $\mathbf{A} \stackrel{\$}{\leftarrow} R_q^{m \times n}$, $\boldsymbol{s} \stackrel{\$}{\leftarrow} R_q^n$, $\boldsymbol{e} \leftarrow \chi^m$ and $\boldsymbol{u} \stackrel{\$}{\leftarrow} R_q^m$.

We notice that the latter two types MLWE problems defined above are the so-called "Hermite Normal Form" version, which can be easily reduced to the standard MLWE via the approach in [4]. For standard MLWE, it is known to be at least as hard as certain standard lattice problems over ideal lattice in the worst case [28]. It should be pointed out that RLWE is the special case of $n = 1$.

B Missing Proofs

B.1 Proof of Lemma 2.14

Lemma B.1 *Let $K = \mathbb{Q}[\zeta]$ be the M-th cyclotomic field with degree $N = \varphi(M)$. Let m, n, q be lattice parameters such that $q \geq 2N$ is a prime and $m \geq n$. With all but 2^{n-m} probability, for $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$, there exists n columns of $\mathbf{A}$ that form an invertible matrix in $R_q^{n\times n}$.*

Proof. Denote P as the probability that there exists n columns of $\mathbf{A}$ that form an invertible matrix in $R_q^{n\times n}$ of $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$.

Let $qR = \mathfrak{q}_1\mathfrak{q}_2\cdots\mathfrak{q}_g$ be prime ideal factorization of the ideal qR where each $\mathfrak{q}_j$ is prime ideal with norm $\mathcal{N}(\mathfrak{q}_j) = q^f$ such that $N = fg$. Let $\{\mathbf{u}_i\}_{1\leq i\leq n}$ be vectors from R_q^n. For $1 \leq i \leq n$, denote E_i as the event that $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_i \in (R_q^n)^*$ and $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_i$ are linearly independent in R_q^n. We define E_i^j as the event that $\mathbf{u}_1, \mathbf{u}_2, \cdots, \mathbf{u}_i \in (R/\mathfrak{q}_j)^*$ and these vectors are linearly independent in $(R/\mathfrak{q}_j)^*$ for $1 \leq j \leq g$. Our next goal is to compute $\Pr_{\mathbf{u}_i}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]$ for all i where the probability is taken from $\mathbf{u}_i \xleftarrow{\$} R_q^n$. We have the following claim.

Claim B.2 $\Pr_{\mathbf{u}_i}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] = \left(1 - q^{-(n-i+1)f}\right)^g$.

Proof. First, we can get a lower bound for each $\Pr_{\mathbf{u}_i}[\mathsf{E}_i^j \mid \mathsf{E}_{i-1}^j]$ where the probability is taken from $\mathbf{u}_i \xleftarrow{\$} R/\mathfrak{q}_j$. For all $1 \leq j \leq k$,

$$\begin{aligned}\Pr_{\mathbf{u}_i\xleftarrow{\$}(R/\mathfrak{q}_j)^n}[\mathsf{E}_i^j \mid \mathsf{E}_{i-1}^j] &= \Pr_{\mathbf{u}_i\xleftarrow{\$}(R/\mathfrak{q}_j)^n}[\mathbf{u}_i \notin \mathsf{span}\{\mathbf{u}_1, \cdots, \mathbf{u}_{i-1}\} \mid \mathsf{E}_{i-1}^j] \\ &= 1 - \Pr_{\mathbf{u}_i\xleftarrow{\$}(R/\mathfrak{q}_j)^n}[\mathbf{u}_i \in \mathsf{span}\{\mathbf{u}_1, \cdots, \mathbf{u}_{i-1}\} \mid \mathsf{E}_{i-1}^j] \\ &= 1 - q^{-(n-i+1)f},\end{aligned}$$

where the last equality holds because $(R/\mathfrak{q}_j)$ is a q^f-sized field.

Since the k random variables ($\mathbf{u}_i \bmod \mathfrak{q}_j$) for $j \in [k]$ is mutually independent when $\mathbf{u}_i \xleftarrow{\$} R_q^n$, we observe that for all $1 \leq i \leq n$,

$$\Pr_{\mathbf{u}_i\xleftarrow{\$}R_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] = \prod_{j=1}^{g} \Pr_{\mathbf{u}_i\xleftarrow{\$}(R/\mathfrak{q}_j)^n}[\mathsf{E}_i^j \mid \mathsf{E}_{i-1}^j] = \left(1 - q^{-(n-i+1)f}\right)^g.$$

□

In claim B.2, we already present a lower bound of probability for each event E_i conditioned on E_{i-1} under the choice $\mathbf{u}_i \xleftarrow{\$} R_q^n$. In order to utilize these lower bounds to compute the probability of existence of a invertible sub-matrix in $\mathbf{A} \xleftarrow{\$} R_q^{n\times m}$, we construct an event with same combinatorial meaning.

Let $\{\mathbf{v}_i\}_{i\in[n]}$ be vectors from $\mathbb{Z}_2^n$. For $1 \le i \le n$, we denote F_i as the event that $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_i$ are linearly independent in $\mathbb{Z}_2^n$, and we find that $\Pr_{\mathbf{v}_i \xleftarrow{\$} \mathbb{Z}_2^n}[\mathsf{F}_i \mid \mathsf{F}_{i-1}]$ exactly matches the lower bound of $\Pr_{\mathbf{u}_i \xleftarrow{\$} \mathbb{Z}_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]$ in claim B.2:

$$\begin{aligned}\Pr_{\mathbf{u}_i \xleftarrow{\$} R_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}] &= \left(1 - q^{-(n-i+1)f}\right)^g \ge 1 - N\cdot q^{-(n-i+1)} \\ &\ge 1 - 2^{-(n-i+1)} = \Pr_{\mathbf{v}_i \xleftarrow{\$} \mathbb{Z}_2^n}[\mathsf{F}_i \mid \mathsf{F}_{i-1}]. \qquad (9)\end{aligned}$$

Let $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n\times m}$ (respectively $\mathbf{F} \xleftarrow{\$} \mathbb{Z}_2^{n\times m}$), which contains m independent samples from R_q^n (respectively $\mathbb{Z}_2^n$). We can view the process of picking n linearly independent column vectors of $\mathbf{A}$ (respectively $\mathbf{F}$) as tossing irregular coins, where each sample (column vector) represents a toss round and head denotes that a sample vector meets the criteria based on chosen samples. To be detailed, during the process of picking linearly independent vectors from $\mathbf{A}$ (respectively $\mathbf{F}$), the probability of flipping a coin with a head outcome based on $i-1$ heads is $\Pr_{\mathbf{u}_i \xleftarrow{\$} R_q^n}[\mathsf{E}_i \mid \mathsf{E}_{i-1}]$ (respectively $\Pr_{\mathbf{v}_i \xleftarrow{\$} \mathbb{Z}_2^n}[\mathsf{F}_i \mid \mathsf{F}_{i-1}]$). It should be noted that, these two scenes have the same number of samples (both m), same target number (both n), and same tossing coins settings (probability of a head is based on the number of existing heads). From the inequality (9), the probability of tossing a coin with a head outcome conditioned on $(i-1)$ existing heads in case of $\mathbf{A}$ is greater than or equal to probability in case $\mathbf{F}$ for all $i \le n$. Therefore, we can obtain that the probability of n heads in $\mathbf{A}$ is greater than or equal to the probability in $\mathbf{F}$, i.e. P can be lower bounded by the probability of $U(\mathbb{Z}_2^{n\times m})$ to be non-singular:

$$P \ge \Pr_{\mathbf{F} \xleftarrow{\$} \mathbb{Z}_2^{n\times m}}[\mathbf{F} \text{ is non-singular}].$$

Since $\mathbb{Z}_2$ is a field, $\mathbf{F}$ is non-singular iff $\mathbf{F}$ has column rank n iff $\mathbf{F}$ has full row rank n, we have

$$\begin{aligned}P &\ge \Pr_{\mathbf{F}_1 \xleftarrow{\$} \mathbb{Z}_2^{n\times m}}[\mathbf{F} \text{ is non-singular}] \\ &= \left(1 - 2^{-m}\right)\left(1 - 2^{-(m-1)}\right)\cdots\left(1 - 2^{-(m-n+1)}\right) > 1 - 2^{n-m},\end{aligned}$$

which completes the proof. □

In the following lemmas, the number field $K = \mathbb{Q}[x]/(x^N + 1)$ is the M-th cyclotomic number field with M being a power of 2 and $N = M/2$. $R =$

$\mathbb{Z}[x]/(x^N+1)$ is the M-th cyclotomic ring of integers and $K_{\mathbb{R}} = \mathbb{R}[x]/(x^N+1)$ is the field tensor product of K and $\mathbb{R}$.

B.2 Proof of Lemma 6.4

Lemma B.3 ($\mathsf{MLWE}_{\ell,m-1,q,D^{\mathsf{coeff}}_{R,\beta}}$ to $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n,D^{\mathsf{coeff}}_{R,\gamma}}$) *Let λ be a security parameter. Let $n,m,\ell,q \geq 1$ be* LWE *parameters such that q is a prime number, and the ideal factorization of qR is $qR = \mathfrak{q}_1^e\mathfrak{q}_2^e \cdots \mathfrak{q}_g^e$ such that $\mathcal{N}(\mathfrak{q}_j) = q^f$ for $j \in [g]$ and $N = efg$. Let $\sigma, \sigma', \beta, \gamma$ be Gaussian parameters such that $\sigma \leq \frac{\sqrt{\pi}}{2} \cdot \frac{q}{\sqrt{\ln(4N)}}$ and $\gamma \geq \sqrt{\left(C_0\beta\sigma'\sqrt{2N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})\right)^2 + \omega(\log\lambda)}$ for a global constant $C_0 \leq 1$. Let k be a positive integer and $\mathbf{M} \in \mathbb{Z}_q^{k\times N\cdot(n+m)}$ be any matrix related to linear leakage. If the parameters satisfy the following constraint:*

$$nf\log\sigma \geq ((\ell+1)f+k)\log q + \log g + \sqrt{2\pi}\log \mathbf{e}\cdot Nn \cdot \frac{\sigma}{\sigma'} + n(\boldsymbol{e}^{-N}+1) + \omega(\log\lambda)$$

then $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n,D^{\mathsf{coeff}}_{R,\gamma}}$ *is hard under the assumption that* $\mathsf{MLWE}_{\ell,m-1,q,D^{\mathsf{coeff}}_{R,\beta}}$ *is hard.*

For the proof of B.3, we need the following four lemmas, which are adapted from [7, 29, 42].

Lemma B.4 intuitively says that the spectral norm of a matrix, in which each entry is independently sampled from a discrete Gaussian distribution, is bounded overwhelmingly. In lemma B.4, we keep the flexible parameter t of [29]'s lemma 8 in the proof of [29]'s lemma 11. Lemma B.5 is the Gaussian decomposition lemma over algebraic ring. Lemma B.6 gives us a lower bound of the ring-based *noisy lossiness*, i.e. the entropy of $\boldsymbol{s}$ conditioned on $\boldsymbol{s}+\boldsymbol{e}$ in the algebraic ring setting with bounded $\boldsymbol{s}$. Lemma B.7 is Peikert's efficient transformation from continuous Gaussian to discrete Gaussian [42].

Lemma B.4 (Cyclotomic Case of Lemma 11 in [29]) *Let m,n be lattice parameters and β be a Gaussian parameter. Sample $\mathbf{F} \leftarrow (D^{\mathsf{coeff}}_{R,\beta})^{m\times n}$. With all but $2N\cdot\mathbf{e}^{-t^2}$ probability, it holds that $\forall j \in [n]$, $s_1(\sigma_j(\mathbf{F})) \leq C_0 \cdot \beta\sqrt{N}\cdot(\sqrt{m}+\sqrt{n}+t)$ for some global constant $C_0 \leq 1$ and flexible parameter t.*

Lemma B.5 (Cyclotomic Case of Theorem 3 in [29]) *Let $\mathbf{F} \in R^{m\times n}$ be a matrix with $s_1(\sigma_j(\mathbf{F})) \leq B$ for any $j \in [N]$. Let $\gamma, \sigma' > 0$ be Gaussian parameters such that $\gamma > \sqrt{2}B\sigma'$. Let $\boldsymbol{e}^{(1)} \leftarrow (D^{\mathsf{coeff}}_{K_{\mathbb{R}},\sigma'})^n$. There exists a sampling algorithm $\mathsf{Samp}(\mathbf{F},\gamma,\sigma')$ which outputs $\boldsymbol{e}^{(2)} \in K^m_{\mathbb{R}}$ such that the random variable $\boldsymbol{e} = \mathbf{F}\boldsymbol{e}^{(1)} + \boldsymbol{e}^{(2)}$ follows $(D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma})^m$.*

Lemma B.6 (Corollary 3 in [29]) *Let n,q be lattice parameters. Let σ' be a Gaussian parameter and $\mathcal{S}$ be a distribution over R^n s.t. for all $\boldsymbol{s}' \in \mathsf{Supp}(\mathcal{S})$, $\|\boldsymbol{s}'\| \leq r$. For all ideal factor $\mathfrak{q} \mid qR$, $H_\infty(\boldsymbol{s}' \bmod \mathfrak{q} \mid \boldsymbol{s}'+\boldsymbol{e}') \geq H_\infty(\boldsymbol{s}' \bmod \mathfrak{q} \mid) - \sqrt{2\pi Nn}\cdot\frac{r}{\sigma'\sqrt{N}}\cdot\log(\mathbf{e})$, where $\boldsymbol{s}' \leftarrow \mathcal{S}$ and $\boldsymbol{e}' \leftarrow (D^{\mathsf{coeff}}_{K_{\mathbb{R}},\sigma'})^n$.*

Lemma B.7 (Particular Case of Theorem 3.1 [42]) *Let γ_1 and γ_2 be Gaussian parameters such that $\gamma_1, \gamma_2 \geq \sqrt{2}\eta_\varepsilon(\mathbb{Z})$ for some $\varepsilon \leq 1/2$. Consider the distribution (x_1, x_2) where $x_2 \leftarrow D_{\gamma_2}$ and $x_1 \leftarrow x_2 + D_{\mathbb{Z}-x_2,\gamma_1}$. The marginal distribution of x_1 is within statistical distance 2ε of $D_{\mathbb{Z},\sqrt{\gamma_1^2+\gamma_2^2}}$.*

In an asymptotic setting, if $\gamma_1, \gamma_2 \geq \omega(\sqrt{\log \lambda})$, the marginal distribution of x_1 is statistically close to $D_{\mathbb{Z},\sqrt{\sigma_1^2+\sigma_2^2}}$.

Then we can come to the proof of lemma B.3. The structure of proof of lemma B.3 is similar to the proofs of [3, Theorem 4.1], [22, Theorem 3]. In each step, apart from keeping one LWE sample $(\mathbf{a}, \langle \mathbf{a}, \boldsymbol{s}\rangle + e)$, we change the public matrix to a lossy matrix with its LWE samples $(\mathbf{B}\cdot\mathbf{C}+\mathbf{F}, (\mathbf{B}\cdot\mathbf{C}+\mathbf{F})\boldsymbol{s}+\boldsymbol{e})$ where $\mathbf{B} \in R_q^{(m-1)\times\ell}$ and $\mathbf{C} \in R_q^{\ell\times n}$ with $\ell \ll n$ based on the multi-secret $\mathsf{MLWE}_{\ell,m-1,q,\chi}$ assumption. Then we use the Gaussian decomposition lemma B.5 and compute the remaining entropy in $\boldsymbol{s}$. Next, we apply our new regularity lemma on discrete Gaussians over algebraic ring with leakage to illustrate the uniform randomness of the extractor $\langle \mathbf{a}, \boldsymbol{s}\rangle$. Afterwards, we change the lossy matrix $\mathbf{B}\cdot\mathbf{C}+\mathbf{F}$ back to a uniform one. In each step, we change one inner product $\langle \mathbf{a}, \boldsymbol{s}\rangle$ to $U(R_q)$. After m steps, we can change m LWE samples to m uniform samples.

It should be noted that the entropic hardness of LWE for bounded secret distribution in [3, Definition B.1] requires the secret and auxiliary $(\boldsymbol{s}, \mathsf{aux})$ is independent from the public matrix $\mathbf{A}$ and the error $\boldsymbol{e}$, while we need the auxiliary leakage to be correlated with both $\boldsymbol{s}$ and $\boldsymbol{e}$. These do not have a confilict, thanks to the fact that the linear leakage $\mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e})$ only has $k\log q$ bits of information and we detailedly describe that random variables can be sampled from the disturbance $\boldsymbol{s}+\boldsymbol{e}'$ and the linear leakage $\mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e})$, which is referred to claim B.11.

Proof (Lemma B.3). Let $\gamma_1 = C_0\beta\sqrt{2N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, then $\gamma \geq \sqrt{\gamma_1^2+\gamma_2^2}$ where $\gamma_2 = \omega(\sqrt{\log\lambda})$. We begin by defining a sequence of hybrid MLWE distributions in which the error is sampled from continuous Gaussian distribution $D^{\mathsf{coeff}}_{K_\mathbb{R},\gamma_1}$. Hyb_m, Hyb_0 and for $i = m-1, \cdots, 0$, $\mathsf{Hyb}_{i,0}, \cdots$, $\mathsf{Hyb}_{i,8}$ are defined as follows.

- Hyb_m: Sample $\mathbf{A} \xleftarrow{\$} R_q^{m\times n}$, $\boldsymbol{s} \leftarrow (D^{\mathsf{coeff}}_{R,\sigma})^n$ and $\boldsymbol{e} \leftarrow (D^{\mathsf{coeff}}_{R,\gamma})^m$.
  Output $(\mathbf{A}, \mathbf{A}\boldsymbol{s}+\boldsymbol{e}, \mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e}))$.
- Hyb_{-1}: Sample $\mathbf{A} \xleftarrow{\$} R_q^{m\times n}$, $\boldsymbol{s} \leftarrow (D^{\mathsf{coeff}}_{R,\sigma})^n$, $\boldsymbol{e} \leftarrow (D^{\mathsf{coeff}}_{R,\gamma})^m$ and $\boldsymbol{u} \xleftarrow{\$} R_q^m$.
  Output $(\mathbf{A}, \boldsymbol{u}+\boldsymbol{e}, \mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e}))$.
- $\mathsf{Hyb}_{i,0}$:
  Sample $\mathbf{A}_i' \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$, and $\mathbf{A}_i'' \xleftarrow{\$} R_q^{i\times n}$.
  Sample $\boldsymbol{s} \leftarrow \left(D^{\mathsf{coeff}}_{R,\sigma}\right)^n$, $\boldsymbol{e}_i' \leftarrow \left(D^{\mathsf{coeff}}_{K_\mathbb{R},\gamma_1}\right)^{m-i-1}$, $e_i' \leftarrow D^{\mathsf{coeff}}_{K_\mathbb{R},\gamma_1}$, and $\boldsymbol{e}_i'' \leftarrow \left(D^{\mathsf{coeff}}_{K_\mathbb{R},\gamma_1}\right)^i$. Let $\boldsymbol{e}_1 \in K_\mathbb{R}^m$ be the concatenation of $\boldsymbol{e}_i'$, e_i and $\boldsymbol{e}_i''$.
  Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D^{\mathsf{coeff}}_{R^m-\boldsymbol{e}_1,\gamma_2}$.
  Sample $\boldsymbol{u}_i' \xleftarrow{\$} R_q^{m-i-1}$.

Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \mathbf{A}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ \langle \mathbf{a}_i, \boldsymbol{s} \rangle + e_i \\ \mathbf{A}''_i \boldsymbol{s} + \boldsymbol{e}''_i \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

– $\mathsf{Hyb}_{i,1}$:

Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$.

Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times \ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell \times n}$ and $\mathbf{F}_i \leftarrow \left(D_{R,\beta}^{\mathsf{coeff}}\right)^{i\times n}$.

Sample $\boldsymbol{s} \leftarrow \left(D_{R,\sigma}^{\mathsf{coeff}}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^{m-i-1}$, $e_i \leftarrow D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}$, and $\boldsymbol{e}''_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^i$. Let $\boldsymbol{e}_1 \in K_\mathbb{R}^m$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\boldsymbol{e}''_i$.

Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D_{R^m - \boldsymbol{e}_1,\gamma_2}^{\mathsf{coeff}}$.

Sample $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$.

Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ \langle \mathbf{a}_i, \boldsymbol{s} \rangle + e_i \\ \tilde{\mathbf{A}}''_i \boldsymbol{s} + \boldsymbol{e}''_i \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

– $\mathsf{Hyb}_{i,2}$:

Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$.

Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times \ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell \times n}$ and $\mathbf{F}_i \leftarrow \left(D_{R,\beta}^{\mathsf{coeff}}\right)^{i\times n}$.

If there exists $j \in [N]$ s.t. $s_1(\sigma_j(\mathbf{F}_i)) > C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, output $\perp$.

Sample $\boldsymbol{s} \leftarrow \left(D_{R,\sigma}^{\mathsf{coeff}}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^{m-i-1}$, $e_i \leftarrow D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}$, and $\boldsymbol{e}''_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^i$. Let $\boldsymbol{e}_1 \in K_\mathbb{R}^m$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\boldsymbol{e}''_i$.

Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D_{R^m - \boldsymbol{e}_1,\gamma_2}^{\mathsf{coeff}}$.

Sample $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$.

Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ \langle \mathbf{a}_i, \boldsymbol{s} \rangle + e_i \\ \tilde{\mathbf{A}}''_i \boldsymbol{s} + \boldsymbol{e}''_i \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

– $\mathsf{Hyb}_{i,3}$:

Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$.

Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times \ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell \times n}$ and $\mathbf{F}_i \leftarrow \left(D_{R,\beta}^{\mathsf{coeff}}\right)^{i\times n}$.

If there exists $j \in [N]$ s.t. $s_1(\sigma_j(\mathbf{F}_i)) > C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, output $\perp$.

Sample $\boldsymbol{s} \leftarrow \left(D_{R,\sigma}^{\mathsf{coeff}}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^{m-i-1}$, $e_i \leftarrow D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}$. Sample $\tilde{\boldsymbol{e}}''_i \leftarrow \mathbf{F}_i \cdot \boldsymbol{e}_i^{(1)} + \boldsymbol{e}_i^{(2)}$ where $\boldsymbol{e}_i^{(1)} \leftarrow (D_{K_\mathbb{R},\sigma'}^{\mathsf{coeff}})^n$ and $\boldsymbol{e}_i^{(2)} \leftarrow \mathsf{Samp}(\mathbf{F}_i, \gamma_1, \sigma')$. Let $\boldsymbol{e}_1 \in K_\mathbb{R}^m$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\tilde{\boldsymbol{e}}''_i$.

Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D_{R^m - \boldsymbol{e}_1,\gamma_2}^{\mathsf{coeff}}$.

Sample $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$.
Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ \langle \mathbf{a}_i, \boldsymbol{s} \rangle + e_i \\ \mathbf{B}_i \cdot \mathbf{C}_i \cdot \boldsymbol{s} + \mathbf{F}_i \cdot (\boldsymbol{s} + \boldsymbol{e}_i^{(1)}) + \boldsymbol{e}_i^{(2)} \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

- $\mathsf{Hyb}_{i,4}$:

  Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$.
  Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times\ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell\times n}$ and $\mathbf{F}_i \leftarrow \left(D_{R,\beta}^{\mathsf{coeff}}\right)^{i\times n}$.
  If there exists $j \in [N]$ s.t. $s_1(\sigma_j(\mathbf{F}_i)) > C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, output $\perp$.
  Sample $\boldsymbol{s} \leftarrow \left(D_{R,\sigma}^{\mathsf{coeff}}\right)^n$, $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$, $\boldsymbol{e}'_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^{m-i-1}$, $e_i \leftarrow D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}$.
  Sample $\tilde{\boldsymbol{e}}''_i \leftarrow \mathbf{F}_i \cdot \boldsymbol{e}_i^{(1)} + \boldsymbol{e}_i^{(2)}$ where $\boldsymbol{e}_i^{(1)} \leftarrow (D_{K_\mathbb{R},\sigma'}^{\mathsf{coeff}})^n$ and $\boldsymbol{e}_i^{(2)} \leftarrow \mathsf{Samp}(\mathbf{F}_i, \gamma_1, \sigma')$.
  Let $\boldsymbol{e}_1 \in K_\mathbb{R}^m$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\tilde{\boldsymbol{e}}''_i$.
  Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D_{R^m - \boldsymbol{e}_1,\gamma_2}^{\mathsf{coeff}}$.
  Sample $u_i \xleftarrow{\$} R_q$.
  Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ u_i + e_i \\ \mathbf{B}_i \cdot \boldsymbol{s}^* + \mathbf{F}_i \cdot (\boldsymbol{s} + \boldsymbol{e}_i^{(1)}) + \boldsymbol{e}_i^{(2)} \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

- $\mathsf{Hyb}_{i,5}$:

  Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$.
  Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times\ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell\times n}$ and $\mathbf{F}_i \leftarrow \left(D_{R,\beta}^{\mathsf{coeff}}\right)^{i\times n}$.
  If there exists $j \in [N]$ s.t. $s_1(\sigma_j(\mathbf{F}_i)) > C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, output $\perp$.
  Sample $\boldsymbol{s} \leftarrow \left(D_{R,\sigma}^{\mathsf{coeff}}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}\right)^{m-i-1}$, $e_i \leftarrow D_{K_\mathbb{R},\gamma_1}^{\mathsf{coeff}}$. Sample $\tilde{\boldsymbol{e}}''_i \leftarrow \mathbf{F}_i \cdot \boldsymbol{e}_i^{(1)} + \boldsymbol{e}_i^{(2)}$ where $\boldsymbol{e}_i^{(1)} \leftarrow (D_{K_\mathbb{R},\sigma'}^{\mathsf{coeff}})^n$ and $\boldsymbol{e}_i^{(2)} \leftarrow \mathsf{Samp}(\mathbf{F}_i, \gamma_1, \sigma')$. Let $\boldsymbol{e}_1 \in K_\mathbb{R}^m$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\boldsymbol{e}''_i$.
  Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D_{R^m - \boldsymbol{e}_1,\gamma_2}^{\mathsf{coeff}}$.
  Sample $u_i \xleftarrow{\$} R_q$ and $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$.
  Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ u_i + e_i \\ \mathbf{B}_i \cdot \mathbf{C}_i \cdot \boldsymbol{s} + \mathbf{F}_i \cdot (\boldsymbol{s} + \boldsymbol{e}_i^{(1)}) + \boldsymbol{e}_i^{(2)} \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

- $\mathsf{Hyb}_{i,6}$:

  Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$.
  Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times\ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell\times n}$ and $\mathbf{F}_i \leftarrow \left(D_{R,\beta}^{\mathsf{coeff}}\right)^{i\times n}$.
  If there exists $j \in [N]$ s.t. $s_1(\sigma_j(\mathbf{F}_i)) > C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, output $\perp$.

Sample $\boldsymbol{s} \leftarrow \left(D^{\mathsf{coeff}}_{R,\sigma}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}\right)^{m-i-1}$, $e_i \leftarrow D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}$ and $\boldsymbol{e}''_i \leftarrow \left(D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}\right)^i$. Let $\boldsymbol{e}_1 \in K^m_{\mathbb{R}}$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\boldsymbol{e}''_i$.
Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D^{\mathsf{coeff}}_{R^m - \boldsymbol{e}_1,\gamma_2}$.
Sample $u_i \xleftarrow{\$} R_q$ and $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$.
Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ u_i + e_i \\ \tilde{\mathbf{A}}''_i \boldsymbol{s} + \boldsymbol{e}''_i \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

– $\mathsf{Hyb}_{i,7}$:
Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, and $\mathbf{a}_i \xleftarrow{\$} R_q^n$.
Sample $\tilde{\mathbf{A}}''_i \leftarrow \mathbf{B}_i \cdot \mathbf{C}_i + \mathbf{F}_i$ s.t. $\mathbf{B}_i \xleftarrow{\$} R_q^{i\times\ell}$, $\mathbf{C}_i \xleftarrow{\$} R_q^{\ell\times n}$ and $\mathbf{F}_i \leftarrow \left(D^{\mathsf{coeff}}_{R,\beta}\right)^{i\times n}$.
Sample $\boldsymbol{s} \leftarrow \left(D^{\mathsf{coeff}}_{R,\sigma}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}\right)^{m-i-1}$, $e_i \leftarrow D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}$ and $\boldsymbol{e}''_i \leftarrow \left(D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}\right)^i$. Let $\boldsymbol{e}_1 \in K^m_{\mathbb{R}}$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\boldsymbol{e}''_i$.
Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D^{\mathsf{coeff}}_{R^m - \boldsymbol{e}_1,\gamma_2}$.
Sample $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$, and $u_i \xleftarrow{\$} R_q$.
Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \tilde{\mathbf{A}}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ u_i + e_i \\ \tilde{\mathbf{A}}''_i \boldsymbol{s} + \boldsymbol{e}''_i \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

– $\mathsf{Hyb}_{i,8}$:
Sample $\mathbf{A}'_i \xleftarrow{\$} R_q^{(m-i-1)\times n}$, $\mathbf{a}_i \xleftarrow{\$} R_q^n$, and $\mathbf{A}''_i \xleftarrow{\$} R_q^{i\times n}$.
Sample $\boldsymbol{s} \leftarrow \left(D^{\mathsf{coeff}}_{R,\sigma}\right)^n$, $\boldsymbol{e}'_i \leftarrow \left(D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}\right)^{m-i-1}$, $e_i \leftarrow D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1}$, and $\boldsymbol{e}''_i \leftarrow (D^{\mathsf{coeff}}_{K_{\mathbb{R}},\gamma_1})^i$. Let $\boldsymbol{e}_1 \in K^m_{\mathbb{R}}$ be the concatenation of $\boldsymbol{e}'_i$, e_i and $\boldsymbol{e}''_i$.
Sample $\boldsymbol{e} \leftarrow \boldsymbol{e}_1 + \boldsymbol{e}_2$ where $\boldsymbol{e}_2 \leftarrow D^{\mathsf{coeff}}_{R^m - \boldsymbol{e}_1,\gamma_2}$.
Sample $\boldsymbol{u}'_i \xleftarrow{\$} R_q^{m-i-1}$, and $u_i \xleftarrow{\$} R_q$.
Output

$$\left(\begin{bmatrix} \mathbf{A}'_i \\ \mathbf{a}_i^\top \\ \mathbf{A}''_i \end{bmatrix}, \begin{bmatrix} \boldsymbol{u}'_i + \boldsymbol{e}'_i \\ u_i + e_i \\ \mathbf{A}''_i \boldsymbol{s} + \boldsymbol{e}''_i \end{bmatrix} + \boldsymbol{e}_2, \mathbf{M} \cdot \phi \begin{pmatrix} \boldsymbol{s} \\ \boldsymbol{e} \end{pmatrix} \right).$$

Hyb_m is the distribution of MLWE samples with linear leakage in the ent-MLWE-LL assumption, and Hyb_{-1} is the uniform distribution with linear leakage. We now show that each pair of adjacent hybrid distributions are statistically or computationally indistinguishable.

Claim B.8 *If $\gamma_1, \gamma_2 \geq \omega(\sqrt{\log \lambda})$, we have $\mathsf{Hyb}_m \overset{s}{\approx} \mathsf{Hyb}_{m-1,0}$ and $\mathsf{Hyb}_{-1} \overset{s}{\approx} \mathsf{Hyb}_{0,8}$.*

Proof. We first rewrite the distribution of $\mathsf{Hyb}_{m-1,0}$ as $(\mathbf{A}, \mathbf{A}\boldsymbol{s}+\boldsymbol{e}, \mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e}))$ where $\mathbf{A} \xleftarrow{\$} R_q^{m\times n}$, $\boldsymbol{s} \leftarrow (D_{R,\sigma}^{\mathsf{coeff}})^n$, $\boldsymbol{e}_1 \leftarrow (D_{K_{\mathbb{R}},\gamma_1}^{\mathsf{coeff}})^m$, $\boldsymbol{e}_2 \leftarrow D_{R^m-\boldsymbol{e}_1,\gamma_2}^{\mathsf{coeff}}$ and $\boldsymbol{e} \leftarrow \boldsymbol{e}_1+\boldsymbol{e}_2$. The difference between $\mathsf{Hyb}_{m-1,0}$ and Hyb_m is the distribution of the error $\boldsymbol{e}$. Since $(D_{K_{\mathbb{R}},\gamma_1}^{\mathsf{coeff}})^m$ $(D_{R^m-\boldsymbol{e}_1}^{\mathsf{coeff}},\gamma_2$, respectively) essentially samples each coefficient of each polynomial in $\boldsymbol{e}_1$ ($\boldsymbol{e}_2$, respectively) from D_{γ_1} ($D_{\mathbb{Z}-e_{i,j},\gamma_2}$ for $i\in[N]$ and $j\in[m]$, respectively), we can apply lemma B.7 to each coefficient of $\boldsymbol{e}$, and conclude that $\mathsf{Hyb}_m \overset{s}{\approx} \mathsf{Hyb}_{m-1,0}$.

From a similar argument, we have $\mathsf{Hyb}_{-1} \overset{s}{\approx} \mathsf{Hyb}_{0,8}$. □

Claim B.9 *For every $i = m-1,\cdots,1$, under the $\mathsf{MLWE}_{\ell,i,q,D_{R,\beta}^{\mathsf{coeff}}}$ assumption, we have $\mathsf{Hyb}_{i,0} \overset{c}{\approx} \mathsf{Hyb}_{i,1}$ and $\mathsf{Hyb}_{i,7} \overset{c}{\approx} \mathsf{Hyb}_{i,8}$.*

Proof. The transition from $\mathsf{Hyb}_{i,0}$ (respectively, $\mathsf{Hyb}_{i,8}$) to $\mathsf{Hyb}_{i,1}$ (respectively, $\mathsf{Hyb}_{i,7}$) is changing the uniform sampler to lossy sampler [3, 7, 21], which is computationally indistinguishable under the MLWE assumptions. □

Claim B.10 *For every $i = m-1,\cdots,1$, we have $\mathsf{SD}(\mathsf{Hyb}_{i,1},\mathsf{Hyb}_{i,2}) \le N\mathbf{e}^{-\lambda}$ and $\mathsf{SD}(\mathsf{Hyb}_{i,6},\mathsf{Hyb}_{i,7}) \le N\mathbf{e}^{-\lambda}$.*

Proof. The difference between $\mathsf{Hyb}_{i,1}$ and $\mathsf{Hyb}_{i,2}$ is that $\mathsf{Hyb}_{i,2}$ aborts when $\sigma_j(\mathbf{F}_i) \ge C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$ for some $j\in[N]$. Take $t=\sqrt{\lambda}$ in lemma B.4, the probability that the abortion occurs is less than $N\mathbf{e}^{-\lambda}$. Therefore,

$$\mathsf{SD}(\mathsf{Hyb}_{i,1},\mathsf{Hyb}_{i,2}) \le \Pr_{\mathbf{F}_i}\left[\exists j\in[N],\, s_1(\sigma_j(\mathbf{F}_i)) \ge C_0\beta\sqrt{N}\left(\sqrt{m}+\sqrt{n}+\sqrt{\lambda}\right)\right] \le N\mathbf{e}^{-\lambda}.$$

The claim $\mathsf{SD}(\mathsf{Hyb}_{i,6},\mathsf{Hyb}_{i,7}) \le N\mathbf{e}^{-\lambda}$ follows by a similar argument. □

Claim B.11 *If $\gamma_1 \ge C_0\beta\sigma'\sqrt{2N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$, we have $\mathsf{Hyb}_{i,2}\equiv\mathsf{Hyb}_{i,3}$ and $\mathsf{Hyb}_{i,5}\equiv\mathsf{Hyb}_{i,6}$.*

Proof. The difference between $\mathsf{Hyb}_{i,2}$ (respectively, $\mathsf{Hyb}_{i,5}$) and $\mathsf{Hyb}_{i,3}$ (respectively, $\mathsf{Hyb}_{i,6}$) is the way of sampling error vector $\boldsymbol{e}_i''$. Take $B = C_0\beta\sqrt{N}(\sqrt{m}+\sqrt{n}+\sqrt{\lambda})$ in lemma B.5, this claim holds. □

Claim B.12 *If $nf\log\sigma \ge ((\ell+1)f+k)\log q + \log g + n(\mathbf{e}^{-N}+1) + \sqrt{2\pi}\log\mathbf{e}\cdot Nn\cdot\frac{\sigma}{\sigma'} + \omega(\log\lambda)$, we have $\mathsf{Hyb}_{i,4} \overset{s}{\approx} \mathsf{Hyb}_{i,5}$, $\mathsf{Hyb}_{i,5} \overset{s}{\approx} \mathsf{Hyb}_{i,6}$.*

Proof. The difference between $\mathsf{Hyb}_{i,3}$ and $\mathsf{Hyb}_{i,4}$ is that we change $\mathbf{a}_i^\top\boldsymbol{s}$ and $\mathbf{C}_i\boldsymbol{s}$ to uniform u_i and $\boldsymbol{s}^*$ resepctively. We will apply our new regularity lemma on discrete Gaussians to show that

$$\underbrace{\left(\begin{bmatrix}\mathbf{a}_i^\top\\ \mathbf{C}_i\end{bmatrix},\, \begin{bmatrix}\mathbf{a}_i^\top\\ \mathbf{C}_i\end{bmatrix}\cdot\boldsymbol{s},\, \boldsymbol{s}+\boldsymbol{e}_i^{(1)},\, \mathbf{A}_i',\, \boldsymbol{u}_i',\, \mathbf{B}_i,\, \mathbf{F}_i,\, \boldsymbol{e}_i^{(2)},\, \boldsymbol{e}_i',\, e_i,\, \boldsymbol{e}_2,\, \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)}_{D_0}$$

$$\overset{s}{\approx} \underbrace{\left(\begin{bmatrix}\mathbf{a}_i^\top\\ \mathbf{C}_i\end{bmatrix},\, \begin{bmatrix}u_i\\ \boldsymbol{s}^*\end{bmatrix},\, \boldsymbol{s}+\boldsymbol{e}_i^{(1)},\, \mathbf{A}_i',\, \boldsymbol{u}_i',\, \mathbf{B}_i,\, \mathbf{F}_i,\, \boldsymbol{e}_i^{(2)},\, \boldsymbol{e}_i',\, e_i,\, \boldsymbol{e}_2,\, \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)}_{D_1}. \quad (10)$$

Since the constraint in lemma B.6 requires the secret $\boldsymbol{s}$ to be totally bounded while discrete Gaussian distribution does not satisfy it, despite being bounded with overwhelming probability. First, we define two medium distributions D_2 and D_3. D_2 (D_3, respectively) is the same as D_0 (D_1, respectively) except that $\boldsymbol{s}$ is changed to $\boldsymbol{s}'$ where $\boldsymbol{s}'$ is sampled from a truncated discrete Gaussian distribution $(D^{\mathsf{coeff}}_{R,\sigma,\leq\sigma\sqrt{N}})^n$. From the tail bound in lemma 2.4, the statistical distance between D_0 (D_0, respectively) to D_2 (D_3, respectively) is no more than $n\cdot\mathbf{e}^{-N}/2$, which is negligible.

Next we would like to show that

$$\underbrace{\left(\begin{bmatrix}\mathbf{a}_i^\top\\ \mathbf{C}_i\end{bmatrix},\ \begin{bmatrix}\mathbf{a}_i^\top\\ \mathbf{C}_i\end{bmatrix}\cdot\boldsymbol{s}',\ \boldsymbol{s}'+\boldsymbol{e}_i^{(1)},\ \mathbf{A}_i',\ \boldsymbol{u}_i',\ \mathbf{B}_i,\ \mathbf{F}_i,\ \boldsymbol{e}_i^{(2)},\ \boldsymbol{e}_i',\ e_i,\ \boldsymbol{e}_2,\ \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)}_{D_2}$$

$$\overset{s}{\approx}\underbrace{\left(\begin{bmatrix}\mathbf{a}_i^\top\\ \mathbf{C}_i\end{bmatrix},\ \begin{bmatrix}u_i\\ \boldsymbol{s}^*\end{bmatrix},\ \boldsymbol{s}'+\boldsymbol{e}_i^{(1)},\ \mathbf{A}_i',\ \boldsymbol{u}_i',\ \mathbf{B}_i,\ \mathbf{F}_i,\ \boldsymbol{e}_i^{(2)},\ \boldsymbol{e}_i',\ e_i,\ \boldsymbol{e}_2,\ \mathbf{M}\cdot\phi\begin{pmatrix}\boldsymbol{s}\\ \boldsymbol{e}\end{pmatrix}\right)}_{D_3}.$$

For every ideal factor $\mathfrak{q}$ of qR with norm $\mathcal{N}(\mathfrak{q})=q^t$, the remaining min-entropy of $\boldsymbol{s}' \bmod \mathfrak{q}$ conditioned on the auxiliaries is computed as follows.

$$\begin{aligned}
&H_\infty(\boldsymbol{s}' \bmod \mathfrak{q} \mid \boldsymbol{s}'+\boldsymbol{e}_i^{(1)}, \mathbf{A}_i', \boldsymbol{u}_i', \mathbf{B}_i, \mathbf{F}_i, \boldsymbol{e}_i^{(2)}, \boldsymbol{e}_i', e_i, \boldsymbol{e}_2, \mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e}))\\
&\geq H_\infty(\boldsymbol{s}' \bmod \mathfrak{q} \mid \boldsymbol{s}'+\boldsymbol{e}_i^{(1)}, \mathbf{A}_i', \boldsymbol{u}_i', \mathbf{B}_i, \mathbf{F}_i, \boldsymbol{e}_i^{(2)}, \boldsymbol{e}_i', e_i, \boldsymbol{e}_2) - k\log q \qquad (11)\\
&\geq H_\infty(\boldsymbol{s}' \bmod \mathfrak{q} \mid \boldsymbol{s}'+\boldsymbol{e}_i^{(1)}, \mathbf{A}_i', \boldsymbol{u}_i', \mathbf{B}_i, \mathbf{F}_i, \boldsymbol{e}_i^{(2)}, \boldsymbol{e}_i', e_i) - k\log q \qquad (12)\\
&= H_\infty(\boldsymbol{s}' \bmod \mathfrak{q} \mid \boldsymbol{s}'+\boldsymbol{e}_i^{(1)}) - k\log q \qquad (13)\\
&\geq H_\infty(\boldsymbol{s}' \bmod \mathfrak{q}) - k\log q - \sqrt{2\pi}\log\mathbf{e}\cdot Nn\cdot\frac{\sigma}{\sigma'} \qquad (14)\\
&\geq nt\log\sigma - n(\boldsymbol{e}^{-N}+1) - k\log q - \sqrt{2\pi}\log\mathbf{e}\cdot Nn\cdot\frac{\sigma}{\sigma'}. \qquad (15)
\end{aligned}$$

Inequality (11) is directly from lemma 2.1 since the linear leakage $\mathbf{M}\cdot\phi(\boldsymbol{s},\boldsymbol{e})\in\mathbb{Z}_q^k$ has $k\log q$ bits of information. In equality (12), we discard the term $\boldsymbol{e}_2$, since its distribution $D_{R^m-\boldsymbol{e}_1,\gamma_2}$ only depends on the fractional part of $\boldsymbol{e}_1$. This allows us to rewritten it as

$$D^{\mathsf{coeff}}_{R^m-\boldsymbol{e}_1,\gamma_2} = D^{\mathsf{coeff}}_{R^m,\gamma_2,\boldsymbol{b}} - \boldsymbol{b} \qquad \text{where} \qquad \boldsymbol{b} = \begin{bmatrix}\boldsymbol{e}_i'\\ e_i\\ \mathbf{F}_i\cdot(\boldsymbol{s}+\boldsymbol{e}_i^{(1)})+\boldsymbol{e}_i^{(2)}\end{bmatrix}\in K_{\mathbb{R}}^m$$

which depends on $\boldsymbol{e}_i'$, e_i, $\mathbf{F}_i$, $(\boldsymbol{s}+\boldsymbol{e}_i^{(1)})$ and $\boldsymbol{e}_i^{(2)}$. In equality (13), we use the fact that random variables $\mathbf{B}_i, \mathbf{F}_i, \boldsymbol{e}_i^{(2)}, \boldsymbol{e}_i', e_i$ are all independent from $\boldsymbol{s}'$ and $\boldsymbol{e}_i^{(1)}$. The 2-norm bound of canonical embedding of $(D^{\mathsf{coeff}}_{R,\sigma,\leq\sigma\sqrt{N}})^n$ is $r=\sigma\sqrt{nN}\cdot\sqrt{N}=\sigma N\sqrt{n}$. Hence from lemma B.6, the inequality (14) holds. By corollary 7 and the constraint $\sigma\leq\sqrt{\frac{q-1}{2}}$, the inequality (15) holds.

At last, we take the flexible leakage parameter δ to be $\delta = n\mathbf{e}^{-N}+k\log q+\sqrt{2\pi}\log\mathbf{e}\cdot Nn\cdot\frac{\sigma}{\sigma'}$ in lemma 5.3, and from the condition

$$nf\log\sigma \geq (\ell+1)f\log q + \log g + \delta + \omega(\log\lambda),$$

we have $D_2 \overset{s}{\approx} D_3$, which shows that $D_0 \overset{s}{\approx} D_1$ by hybrid bridges of D_2 and D_3. This completes the proof of $\mathsf{Hyb}_{i,4} \overset{s}{\approx} \mathsf{Hyb}_{i,5}$.

Proof of $\mathsf{Hyb}_{i,5} \overset{s}{\approx} \mathsf{Hyb}_{i,6}$ follows a similar argument, which we omit here. □

Since $\mathsf{Hyb}_{i,8}$ and $\mathsf{Hyb}_{i-1,0}$ are identical distributions for all $i = m-1, \cdots, 1$, we conclude that $\mathsf{Hyb}_m \overset{c}{\approx} \mathsf{Hyb}_{-1}$.

□

B.3 Proof of Lemma 6.5

Lemma B.13 (ent-MLWE-LL$^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$ to ent-MLWE-LL$^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\gamma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$) *Let $n, m, q = \mathsf{poly}(\lambda)$ be* LWE *parameters and $\sigma, \gamma > 0$ be two Gaussian parameters s.t. $\sigma \geq \sqrt{2}\eta_\varepsilon(\mathbb{Z}^{nN})$ and $\sqrt{\gamma^2 - \sigma^2} \geq \sqrt{2}\eta_\varepsilon(\mathbb{Z}^{nN})$ for some $\varepsilon = \mathsf{negl}(\lambda)$. For any positive integer k and any $\boldsymbol{z} = (\boldsymbol{z}_i)_{i\in[k]} \in R_q^{k(n+m)}$, there exists a* PPT *reduction from* ent-MLWE-LL$^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$ *to* ent-MLWE-LL$^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\gamma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$.

To prove lemma B.13, we need the following lemma that intuitively says the sum of discrete Gaussian distributions is statistically close to a discrete Gaussian distribution if each Gaussian parameter is greater than or equal to the smoothing parameter.

Lemma B.14 (Particular Case of Theorem 3.3 [37]) *Let $\mathbf{\Lambda}$ be an n-dimensional lattice and $\sigma_1, \sigma_2 \geq \sqrt{2}\eta_\varepsilon(\mathbf{\Lambda})$. Let $\boldsymbol{y}_i$ be independent vectors with distributions $D_{\mathbf{\Lambda},\sigma_i}$ for $i = 1, 2$ respectively. Then the distribution of $\boldsymbol{y} = \boldsymbol{y}_1 + \boldsymbol{y}_2$ is statistical close to $D_{\mathbf{\Lambda},\sqrt{\sigma_1^2+\sigma_2^2}}$.*

Proof (Lemma B.13). Assume that $\boldsymbol{z}, \boldsymbol{c}$ are fixed and public. We describe below an efficient randomized mapping $\phi : R_q^{m\times n} \times R_q^m \times \mathbb{Z}_q^k \to R_q^{m\times n} \times R_q^m \times \mathbb{Z}_q^k$. For input a tuple $(\mathbf{A}, \boldsymbol{b}, L)$, first sample $\boldsymbol{s}' \leftarrow (D^{\mathsf{coeff}}_{R,\sqrt{\gamma^2-\sigma^2}})^n$ and output $(\mathbf{A}, \boldsymbol{b} + \mathbf{A}\boldsymbol{s}', L + \mathbf{M}\cdot\phi(\boldsymbol{s}', 0^m))$ where $\boldsymbol{s}' \| 0^m \in \mathbb{R}^{n+m}$ is the vector $\boldsymbol{s}'$ padded by m zeros.

Due to the linearity of the leakage, the reduction maps the leakage part from $\mathbf{M}\cdot\phi(\boldsymbol{s}, \boldsymbol{e})$ where $\boldsymbol{s} \leftarrow (D^{\mathsf{coeff}}_{R,\sigma})^n$ and $\boldsymbol{e} \leftarrow (D^{\mathsf{coeff}}_{R,\gamma})^m$, to $\mathbf{M}\cdot\phi(\boldsymbol{s}+\boldsymbol{s}', \boldsymbol{e})$ where $\boldsymbol{s}' \leftarrow (D^{\mathsf{coeff}}_{R,\sqrt{\gamma^2-\sigma^2}})^n$. Take $\mathbf{\Lambda} = \mathbb{Z}^{nN}$ in lemma 5.4, we get that $D_{\mathbb{Z}^{nN},\sigma} + D_{\mathbb{Z}^{nN},\sqrt{\gamma^2-\sigma^2}} \overset{s}{\approx} D_{\mathbb{Z}^{nN},\gamma}$. Since the samplings of $\boldsymbol{s}$ and $\boldsymbol{s}'$ are taking the coefficient vector of each entry in $\boldsymbol{s}$ and $\boldsymbol{s}'$ as a gaussian vector from $\mathbb{Z}^N$, we can interpret $\boldsymbol{s} + \boldsymbol{s}'$ as a random variable $\mathsf{negl}(\lambda)$-close to $(D^{\mathsf{coeff}}_{R,\gamma})^n$.

In detail, if the input is MLWE samples with linear leakage in the problem ent-MLWE-LL$^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$, i.e.

$$(\mathbf{A}, \mathbf{A}\boldsymbol{s} + \boldsymbol{e}, \mathbf{M}\cdot\phi(\boldsymbol{s}, \boldsymbol{e}))_{\mathbf{A}\overset{\$}{\leftarrow} R_q^{m\times n},\, \boldsymbol{s}\leftarrow(D^{\mathsf{coeff}}_{R,\sigma})^n,\, \boldsymbol{e}\leftarrow(D^{\mathsf{coeff}}_{R,\gamma})^m},$$

then the output of ϕ follows the distribution

$$(\mathbf{A}, \mathbf{A}(\boldsymbol{s}+\boldsymbol{s}') + \boldsymbol{e}, \mathbf{M}\cdot\phi(\boldsymbol{s}+\boldsymbol{s}', \boldsymbol{e}))_{\mathbf{A}\overset{\$}{\leftarrow} R_q^{m\times n}, \boldsymbol{s}\leftarrow(D^{\mathsf{coeff}}_{R,\sigma})^n, \boldsymbol{s}'\leftarrow(D^{\mathsf{coeff}}_{R,\sqrt{\gamma^2-\sigma^2}})^n, \boldsymbol{e}\leftarrow(D^{\mathsf{coeff}}_{R,\gamma})^m}.$$

which is statistically closed to the MLWE sample with linear leakage in the problem $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\gamma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$.

Similarly, if the input is uniform samples with linear leakage in the problem $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\sigma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$, i.e.

$$(\mathbf{A}, \boldsymbol{u}, \mathbf{M} \cdot \phi(\boldsymbol{s}, \boldsymbol{e}))_{\mathbf{A} \xleftarrow{\$} R_q^{m \times n},\, \boldsymbol{s} \leftarrow (D^{\mathsf{coeff}}_{R,\sigma})^n,\, \boldsymbol{e} \leftarrow (D^{\mathsf{coeff}}_{R,\gamma})^m, \boldsymbol{u} \xleftarrow{\$} R_q^m},$$

then the output of ϕ follows the distribution

$$(\mathbf{A}, \boldsymbol{u} + \mathbf{A}\boldsymbol{s}', \mathbf{M} \cdot \phi(\boldsymbol{s} + \boldsymbol{s}', \boldsymbol{e}))_{\mathbf{A} \xleftarrow{\$} R_q^{m \times n}, \boldsymbol{s} \leftarrow (D^{\mathsf{coeff}}_{R,\sigma})^n, \boldsymbol{s}' \leftarrow (D^{\mathsf{coeff}}_{R,\sqrt{\gamma^2 - \sigma^2}})^n, \boldsymbol{e} \leftarrow (D^{\mathsf{coeff}}_{R,\gamma})^m, \boldsymbol{u} \xleftarrow{\$} R_q^m}.$$

which is statistically closed to the uniform sample with linear leakage in the problem $\mathsf{ent\text{-}MLWE\text{-}LL}^{n,m,q,\mathbf{M}}_{(D^{\mathsf{coeff}}_{R,\gamma})^n, D^{\mathsf{coeff}}_{R,\gamma}}$ due to the one time pad property and lemma B.14. □