International Journal of Software and Informatics, ISSN 1673-7288
http://www.ijsi.org, ijsi@iscas.ac.cn, +86-10-62661048
IJSI, 2025, 15(4): 401–417, doi: 10.21655/ijsi.1673-7288.00356

International Journal of Software and Informatics

Research Article

Tighter Reductions of LWE Problems with Semi-uniform Seeds

Yang Wang (王洋)[1,2], Mingqiang Wang (王明强)[1]

[1] (School of Mathematics, Shandong University, Jinan 250100, China)
[2] (State Key Laboratory of Cryptology, Beijing 100878, China)
Corresponding author: Mingqiang Wang, wangmingqiang@sdu.edu.cn

Abstract In certain designs and applications of practical lattice-based cryptography, the use of a specialized variant of LWE problems, where the public matrix is sampled from a non-uniform distribution, is required to establish the security of the corresponding cryptographic schemes. Recently, the formal definition of LWE problems with semi-uniform seeds was introduced by the community, in which the hardness of Euclidean, ideal, and module lattice-based LWE problems with semi-uniform seeds was proved through reduction approach similar to those employed in the hardness proofs of entropic LWE problems. However, known reduction introduces significant losses in the Gaussian error parameters and lattice dimensions. Moreover, additional non-standard assumptions are required to demonstrate the hardness of LWE problems with semi-uniform seeds over rings. In this paper, a tighter reduction is proposed for LWE problems with semi-uniform seeds by incorporating modified techniques from the hardness proofs of Hint-LWE problems. The proposed reduction is unaffected by the algebraic structure of the underlying problems and can be uniformly applied to Euclidean, ideal, and module lattice-based LWE problems with semi-uniform seeds. The hardness of these LWE problems can be established based on standard LWE assumptions without the need for any additional non-standard assumption. Furthermore, the dimension of corresponding LWE problems remains unchanged, and the reduction introduces only minimal losses in Gaussian error parameters.

Keywords lattice-based cryptography; reductions of lattice-based problems; LWE problems with semi-uniform seeds; Hint-LWE problem; discrete Gaussian distribution

Citation Wang Y, Wang MQ. Tighter reductions of LWE problems with semi-uniform seeds, *International Journal of Software and Informatics*, 2025, 15(4): 401–417. http://www.ijsi.org/1673-7288/356.htm

The learning with errors (LWE) problem over Euclidean lattices[1] and its algebraic variants—the ring/module LWE problems[2, 3]—represent the most widely used class of average-case computationally hard problems in lattice-based cryptography. Nearly all known cryptographic primitives can be constructed based on the Euclidean/ring/module LWE problems, or their appropriately defined variants. Studies on practical variants of the LWE problems can

This is the English version of the Chinese article "半均匀 LWE 问题的紧致归约. 软件学报, 2025, 36(10): 4405–4416. doi: 10.13328/j.cnki.jos.007388"
Funding items: National Key Research and Development Program of China (2021YFB3100200); Stable Support Project of National Key Laboratory of Security Communication (2024, WD202402); Open Project of State Key Laboratory of Cryptography (MMKFKT202207); Natural Science Foundation of Shandong Province (ZR2022QF039)
Received 2024-06-25; Revised 2024-09-05; Accepted 2024-12-30; IJSI published online 2025-12-30

be broadly categorized into three classes (a more detailed discussion can be found in Ref. [4]). The first class investigates the hardness of the LWE problems when the secret or the error follows more general distributions (e.g., the binary distribution on $\{0,1\}$, uniform distribution over small intervals $[-\alpha,\alpha]$, or the entropic LWE problems)[5–9]. The second class studies the hardness of the LWE problems when partial information about the secret or error is leaked, leading to the so-called Hint-LWE problems[5, 10–15]. The third class examines the hardness of the LWE problem instances where the public matrix is drawn from a non-uniform distribution, referred to as the non-uniform LWE problems[4, 16–18].

Recently, Jia *et al.*[4, 17, 18] systematically investigated the hardness of a specific type of non-uniform LWE problem, namely the semi-uniform LWE (SU-LWE) problem. They provided a formal definition of the SU-LWE problem and established hardness results for the SU-LWE counterparts over Euclidean, ideal, or module lattices by employing a reduction strategy analogous to that used in proving the hardness of the entropic LWE problem. Taking Euclidean lattices as an example, a distribution $\mathcal{D}$ over $\mathbb{Z}_q^{m\times d}$ is called an η-semi-uniform distribution if there is a family of efficiently sampleable distributions $\{\phi_U\}_{U\in\mathbb{Z}_q^{m\times d}}$ in $\mathbb{Z}^{m\times d}$, such that the output distribution of the sampling process $\{U+E_U : U \hookleftarrow \mathrm{U}(\mathbb{Z}_q^{m\times d}), E_U \hookleftarrow \phi_U\}$ is statistically indistinguishable from $\mathcal{D}$, and with probability close to 1, the spectral norm of E_U does not exceed η. In this paper, the discrete Gaussian distribution is generally denoted by D. When no confusion arises, in order to emphasize the public matrix in the SU-LWE problem, we use $\mathcal{D}$ to represent the distribution that the public matrix A follows in the corresponding LWE problem. Correspondingly, the decision version of the non-uniform LWE problem, denoted as $\mathrm{DLWE}^d_{\mathbb{Z},m,q,\chi_1}(\chi_2;\mathcal{D})$, can be defined as the task of distinguishing between the following two distributions:

(1) $\{(A, A\cdot \boldsymbol{s}+\boldsymbol{e} \bmod q\mathbb{Z}) : A\hookleftarrow \mathcal{D}, \boldsymbol{s}\hookleftarrow \chi_2, \boldsymbol{e}\hookleftarrow\chi_1\}$;

(2) $\{(A,\boldsymbol{u}) : A\hookleftarrow\mathcal{D}, \boldsymbol{u}\hookleftarrow \mathrm{U}(\mathbb{Z}_q^m)\}$.

It is noteworthy that for any $U\in\mathbb{Z}_q^{m\times d}$, if a specific constant function $E_U = \left\lfloor \frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot U\right\rceil\right\rceil - U$ is chosen for ϕ_U, the corresponding SU-LWE problem reduces to distinguishing the following distributions:

(1) $\left\{\left(\left\lfloor \frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot A\right\rceil\right\rceil, \left\lfloor \frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot A\right\rceil\right\rceil\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\mathbb{Z}\right) : A\hookleftarrow \mathrm{U}(\mathbb{Z}_q^{m\times d}), \boldsymbol{s}\hookleftarrow\chi_2,\right.$ $\left.\boldsymbol{e}\hookleftarrow\chi_1\right\}$;

(2) $\left\{\left(\left\lfloor \frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot A\right\rceil\right\rceil, \boldsymbol{u}\right) : A\hookleftarrow \mathrm{U}(\mathbb{Z}_q^{m\times d}), \boldsymbol{u}\hookleftarrow \mathrm{U}(\mathbb{Z}_q^m)\right\}$.

It is worth noting that from A, $\left\lfloor \frac{q}{p}\cdot\left\lfloor\frac{p}{q}\cdot A\right\rceil\right\rceil$ can be easily computed. Through a specific type of SU-LWE problem discussed here, the IND-CPA (indistinguishability under chosen-plaintext attack) security of the underlying public-key encryption scheme used by Kyber, a candidate algorithm from the first round of the NIST (National Institute of Standards and Technology) post-quantum competition, can be proven[19, 20]. In other words, it can be demonstrated that efficient public-key encryption schemes designed using the LP (Lindner-Peikert) framework[21] with a compressed public key also satisfy IND-CPA security. Previously, due to the lack of a strict reduction from the corresponding non-uniform LWE problem to the standard LWE problem, the Kyber design team removed the public key compression technique from the scheme starting from the second round of the NIST competition[22–24], which resulted in increased communication bandwidth for the corresponding scheme. In practical applications, this specific type of SU-LWE problem can be combined with techniques like key consensus to design highly efficient lattice-based cryptographic schemes[25–29].

The existing reduction results for the hardness of the SU-LWE problems apply to general secret distributions (i.e., the reduction only requires that the distribution of the secret $\boldsymbol{s}$ has sufficient entropy under certain conditions, and the specific form of the distribution that secret $\boldsymbol{s}$ follows can be arbitrary). Because it adopts a reduction approach similar to that used for proving the hardness of the entropic LWE problems, the known reductions for the SU-LWE problems incur significant losses in terms of dimension and Gaussian parameter[4, 17, 18]. Specifically, proving the hardness of a d-dimensional SU-LWE problem relies on the hardness of a standard LWE problem of dimension $\tilde{d}$ ($d = \mathrm{O}(\tilde{d} \cdot \log q)$). Furthermore, for a general η-semi-uniform distribution $\mathcal{D}$, the loss in the Gaussian error parameter during the reduction is dependent on the number of samples (particularly, when the number of samples is $\mathrm{poly}(\lambda)$, the expansion factor for the error parameter is relatively large). Additionally, when proving the hardness of the SU-LWE problem or the search variant of the SU-LWE problem over rings, it is necessary to introduce an extra, relatively non-standard hardness assumption, namely a certain decisional version of the NTRU problem.

In practice, the LWE problem with secret/error distributions following a discrete Gaussian distribution is commonly employed for the design of cryptographic protocols or the discussion of hardness reductions. A question is whether a tighter reduction for the non-uniform LWE problem can be provided specifically for the case of discrete Gaussian distributions. This is the primary starting point and research motivation of this paper.

In this paper, we generalize the techniques used in the study of Hint-LWE problem hardness and apply them to the investigation of SU-LWE problem hardness, presenting a tighter reduction method for the hardness of the SU-LWE problems. The reduction method employed in this paper is largely independent of algebraic structure limitations and can be uniformly applied to SU-LWE problems defined over Euclidean, ideal, or module lattices. Specifically, our reduction approach offers the following advantages.

(1) The reduction result is dimension-preserving, i.e., the hardness of a d-dimensional SU-LWE problem can be based solely on the hardness of a d-dimensional standard LWE problem.

(2) The loss in the Gaussian parameter during the reduction is small, and the Gaussian parameter in the reduction for a general η-semi-uniform distribution $\mathcal{D}$ is independent of the number of samples, that is, the hardness of a d-dimensional SU-LWE problem with Gaussian parameter σ can be guaranteed by the hardness of a d-dimensional standard LWE problem with Gaussian parameter $\mathrm{O}(\eta \cdot \sigma)$.

In this paper, we will introduce a brief overview of the research status concerning non-uniform LWE problems in Section 1. We present the necessary background knowledge, including (ideal/module) lattices, Gaussian distributions, definitions used in the (semi-uniform) LWE problem, and some useful lemmas in Section 2. We introduce the main reduction of this paper and provide a brief comparison of our reduction results with known results in Section 3 and conclude in Section 4.

1 Related Work on Non-uniform LWE Problems

In the initial LWE problem, the public matrix is typically sampled from a random uniform distribution, i.e., $A \hookleftarrow \mathrm{U}(\mathbb{Z}_q^{m \times d})$. In the study of some known variants of the LWE problem, it is often necessary to replace A with a so-called "Lossy" form (i.e., $A = B \cdot C + E$, using LWE samples with multiple secrets) for analysis[6–8]. Generally, the distribution corresponding to $A = B \cdot C + E$ is not statistically indistinguishable from the uniform distribution. However, under the computational assumption that the corresponding LWE problem is hard, it can be proven that this specific "non-uniform" LWE problem is also hard. In this paper, a non-uniform LWE problem refers to an LWE instance where the distribution $\mathcal{D}$ from which the public matrix A is sampled is not statistically or computationally indistinguishable from $\mathrm{U}(\mathbb{Z}_q^{m\times d})$.

To the best of our knowledge, excluding LWE problems where A is a specific circulant matrix[30] (in such cases, the coefficients of A are chosen uniformly over certain rings), Boneh *et al.*[16] were the first to discuss the hardness of non-uniform LWE problems. They proved that when the distribution $\mathcal{D}$ of the public matrix A is: (1) a discrete Gaussian distribution over $\mathbb{Z}^d$ with appropriate parameters; (2) the uniform distribution over $\{0,1\}^k$ for sufficiently large k; (3) the uniform distribution over certain sufficiently large linear subspaces of $\mathbb{Z}^d$, the hardness of the corresponding non-uniform LWE problem can be guaranteed by the hardness of the standard LWE problem. Furthermore, the "continuous LWE problem" proposed by Bruna *et al.*[31] involves a public matrix A sampled from an appropriate continuous Gaussian distribution. Gupte *et al.*[32] also proved that, under appropriate parameter conditions, the hardness of such problems can be reduced to that of the standard LWE problem.

However, the aforementioned types of non-uniform LWE problems are not suitable for certain lattice-based cryptographic applications (e.g., encryption/key encapsulation mechanism (KEM) schemes designed using public key compression techniques[25–29]). Recently, Jia *et al.*[4, 17, 18] formally defined the SU-LWE problem. Employing a reduction strategy akin to that used for proving the hardness of the entropic LWE problem and utilizing tools such as Renyi divergence and regularity lemmas for lattices (e.g., the leftover hash lemma), they demonstrated the hardness of appropriately parameterized SU-LWE problems in Euclidean, ideal, or module lattices.

2 Basic Knowledge

In this section, we will introduce the notation and present the concepts, definitions, and some lemmas that will be frequently used in the subsequent discussion.

The symbols $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ denote the sets of integers, rational numbers, and real numbers, respectively. For a given positive integer $q \in \mathbb{Z}$, define $\mathbb{Z}_q := \mathbb{Z}/q\cdot\mathbb{Z}$, and use the symbol $[q]$ denotes the set $\{1, 2, \ldots, q\}$. Unless otherwise specified, the representatives of cosets in $\mathbb{Z}_q$ are taken from the set $\left[-\frac{q}{2}, \frac{q}{2}\right) \cap \mathbb{Z}$. Bold lowercase letters (e.g., $\boldsymbol{x}$) denote vectors, and italic uppercase letters (e.g., A) denote matrices or sets. Unless specified, vectors are treated as column vectors by default; the symbol A^{T} denotes the transpose of matrix A (vectors are considered as special matrices); the symbol I_d denotes the $d\times d$ identity matrix. For a vector $\boldsymbol{x} = (x_1, \ldots, x_d)^{\mathrm{T}} \in \mathbb{R}^d$, we define $\|\boldsymbol{x}\| := \sum_{i=1}^d x_i^2$, $\|\boldsymbol{x}\|_1 := \sum_{i=1}^d |x_i|$, $\|\boldsymbol{x}\|_\infty := \max_{i\in[d]} |x_i|$. For a matrix $A \in \mathbb{R}^{d\times d}$, the symbol $\mathfrak{s}_k(A)$, where $k \in [d]$, denotes the d distinct singular values of matrix A. We assume singular values are ordered such that $\mathfrak{s}_d(A) \leq \ldots \leq \mathfrak{s}_2(A) \leq \mathfrak{s}_1(A)$, where $\mathfrak{s}_1(A)$ is the spectral norm of A. For a finite set S, $\mathrm{U}(S)$ denotes the uniform distribution over S. For a probability distribution $\mathcal{D}$, the notation $x \hookleftarrow \mathcal{D}$ indicates that the random variable x is sampled from $\mathcal{D}$. The statistical distance $\Delta(\mathcal{D}_1, \mathcal{D}_2)$ between two discrete probability distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ over a set S is defined as $\Delta(\mathcal{D}_1, \mathcal{D}_2) := \frac{1}{2}\cdot\sum_{a\in S} |\Pr_{x\hookleftarrow\mathcal{D}_1}[x=a] - \Pr_{y\hookleftarrow\mathcal{D}_2}[y=a]|$. The symbol λ denotes the security parameter. A function $f(\lambda)$ is said to be negligible if for every constant $c > 0$, there exists λ_0 such that for all $\lambda \geq \lambda_0$, $f(\lambda) \leq \frac{1}{\lambda^c}$ holds. When the specific form of the function does not affect our discussion, we generally use the symbol $negl(\lambda)$ to represent (one or several different) negligible functions. If $\Delta(\mathcal{D}_1, \mathcal{D}_2) \le negl(\lambda)$, and then the distributions $\mathcal{D}_1$ and $\mathcal{D}_2$ are said to be statistically close/indistinguishable.

2.1 Lattices and discrete Gaussian distributions

In this paper, we discuss only full-rank integer lattices. More precisely, a d-dimensional Euclidean lattice $\mathit{\Lambda} := \mathcal{L}(B)$ discussed herein can be written in the form $\mathbb{Z} \cdot \boldsymbol{b}_1 + \ldots + \mathbb{Z} \cdot \boldsymbol{b}_d$, where $B := (\boldsymbol{b}_1|\ldots|\boldsymbol{b}_d) \in \mathbb{Z}^{d\times d}$ and d is an arbitrary positive integer. The dual lattice $\mathit{\Lambda}^*$ of $\mathit{\Lambda}$ is defined as $\mathit{\Lambda}^* := \{\boldsymbol{x} \in \mathbb{R}^d : <\boldsymbol{x}, \boldsymbol{y}> \in \mathbb{Z}, \forall \boldsymbol{y} \in \mathit{\Lambda}\}$. We are also concerned with special ideal/module lattices. To simplify the discussion, we fix a positive integer $n = 2^{\hat{n}}$ and consider the specific cyclotomic field $\mathcal{K} := \mathbb{Q}[x]/(x^n + 1)$ and its ring of integers $\mathcal{R} := \mathbb{Z}[x]/(x^n + 1)$ (it is worth noting that, using an analysis similar to that in this paper, our conclusions can be generalized to general algebraic number fields). For a polynomial $a = a_0 + a_1 \cdot x + \ldots + a_{n-1} \cdot x^{n-1}$ in $\mathcal{R}$, we use the coefficient embedding σ_{coef} to embed it into $\mathbb{Z}^n$, i.e., $\sigma_{\text{coef}}(a) := (a_0, \ldots, a_{n-1})^{\mathrm{T}}$. Note that the multiplication of two elements in $\mathcal{R}$ can be represented as matrix-vector multiplication. For given $a = a_0 + a_1 \cdot x + \ldots + a_{n-1} \cdot x^{n-1}$ and $b = b_0 + b_1 \cdot x + \ldots + b_{n-1} \cdot x^{n-1}$, a simple calculation shows that $\sigma_{\text{coef}}(a \cdot b) = M_{\text{coef}}(a) \cdot \sigma_{\text{coef}}(b) = M_{\text{coef}}(b) \cdot \sigma_{\text{coef}}(a)$, where

$$M_{\text{coef}}(a) := \begin{pmatrix} a_0 & -a_{n-1} & -a_{n-2} & \cdots & -a_1 \\ a_1 & a_0 & -a_{n-1} & \cdots & -a_2 \\ a_2 & a_1 & a_0 & \cdots & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{pmatrix}$$

It is easy to see that for any ideal $\mathcal{J}$ of $\mathcal{R}$, $\sigma_{\text{coef}}(\mathcal{J})$ forms a full-rank lattice.

For any given positive real $s \in \mathbb{R}$ and vector $\boldsymbol{c} \in \mathbb{R}^d$, the d-dimensional Gaussian function with parameter s and center $\boldsymbol{c}$ is defined as $\rho_{s,\boldsymbol{c}}(\boldsymbol{x}) := \mathrm{e}^{-\pi \cdot \frac{\|\boldsymbol{x}-\boldsymbol{c}\|^2}{s^2}}$. Correspondingly, the probability density function of the d-dimensional continuous Gaussian distribution $D_{s,\boldsymbol{c}}$ is $\frac{1}{s^d} \cdot \rho_{s,\boldsymbol{c}}(\boldsymbol{x}), \boldsymbol{x} \in \mathbb{R}^d$. This Gaussian distribution can be restricted to any lattice (or discrete set) $\mathit{\Lambda}$. The corresponding discrete Gaussian distribution $D_{\mathit{\Lambda},s,\boldsymbol{c}}$ has the probability mass function $\frac{\rho_{s,\boldsymbol{c}}(\boldsymbol{x})}{\rho_{s,\boldsymbol{c}}(\mathit{\Lambda})}, \boldsymbol{x} \in \mathit{\Lambda}$, where $\rho_{s,\boldsymbol{c}}(\mathit{\Lambda}) := \sum_{\boldsymbol{x}\in\mathit{\Lambda}} \rho_{s,\boldsymbol{c}}(\boldsymbol{x})$. When $\boldsymbol{c} = 0$ or $s = 1$, the corresponding subscript is omitted from the notation, e.g., $\rho_s(\boldsymbol{x})$, $\rho(\boldsymbol{x})$. Given any non-singular matrix $B \in \mathbb{R}^{d\times d}$, the matrix $\Sigma := B \cdot B^{\mathrm{T}}$ is a real symmetric positive definite matrix (denoted as $\Sigma > 0$). Define $\rho_B(\boldsymbol{x}) := \rho(B^{-1} \cdot \boldsymbol{x}) = \mathrm{e}^{-\pi \cdot \boldsymbol{x}^{\mathrm{T}} \cdot \Sigma^{-1} \cdot \boldsymbol{x}}$. Note that the value of $\rho_B(\boldsymbol{x})$ depends only on Σ and $\boldsymbol{x}$, so we denote $\rho_{\sqrt{\Sigma}}(\boldsymbol{x}) := \rho_B(\boldsymbol{x})$. To simplify the discussion, $\sqrt{\Sigma}$ here is chosen as the Cholesky decomposition of Σ (i.e., satisfying $\Sigma = \sqrt{\Sigma} \cdot \sqrt{\Sigma}^{\mathrm{T}}$, where $\sqrt{\Sigma}$ is a lower triangular matrix). In fact, taking $\sqrt{\Sigma}$ to be any matrix B satisfying $\Sigma = B \cdot B^{\mathrm{T}}$ does not affect the subsequent discussion. For two real symmetric positive definite matrices A and B, if $A - B$ is also real symmetric positive definite, we write $A > B$.

When discussing within $\mathcal{R}$, we use the notation $f \hookleftarrow D_{\mathcal{R},s}$ to indicate that the coefficients of the polynomial f are independently sampled from the 1-dimensional discrete Gaussian distribution $D_{\mathbb{Z},s}$ with parameter s. Since $(D_{\mathbb{Z},s})^d = D_{\mathbb{Z}^d,s}$, $f \hookleftarrow D_{\mathcal{R},s}$ is equivalent to the vector of coefficients of f following the distribution $D_{\mathbb{Z}^n,s}$, i.e., $\sigma_{\text{coef}}(f) \hookleftarrow D_{\mathbb{Z}^n,s}$. In particular, we have $D_{\mathcal{R}^d,s} = D_{\mathbb{Z}^{n\cdot d},s}$. Suppose $\varepsilon > 0$ is a positive real number. For any d-dimensional lattice $\mathit{\Lambda}$, the smoothing parameter $\eta_\varepsilon(\mathit{\Lambda})$ (related to ε) is defined as $\min_{s>0} \{s : \rho_{1/s}(\mathit{\Lambda}^*\backslash\{0\}) \le \varepsilon\}$. Similarly, for any real symmetric positive definite matrix

$\Sigma > 0$, if $\eta_\varepsilon(\sqrt{\Sigma}^{-1} \cdot \Lambda) \le 1$ holds, we write $\sqrt{\Sigma} \ge \eta_\varepsilon(\Lambda)$. By definition, the condition $\eta_\varepsilon(\sqrt{\Sigma}^{-1} \cdot \Lambda) \le 1$ is equivalent to $\rho(\sqrt{\Sigma}^{\mathrm{T}} \cdot \Lambda^*\backslash\{0\}) = \rho_{\sqrt{\Sigma}^{-1}}(\Lambda^*\backslash\{0\}) \le 0$. In the subsequent discussion, we will need the following lemmas[1, 8, 10, 33–35].

Lemma 1. The following facts hold.

(1) Assume Σ is a real symmetric positive definite matrix, Λ is a lattice, and $\varepsilon \in \left(0, \frac{1}{2}\right)$. If $\mathfrak{s}_1(\Sigma) \le \eta_\varepsilon(\Lambda)^{-2}$, then $\sqrt{\Sigma} \ge \eta_\varepsilon(\Lambda)$ holds.

(2) For the d-dimensional lattice $\mathbb{Z}^d$, there exists a negligible $\varepsilon = \varepsilon(\lambda)$ such that $\eta_\varepsilon(\mathbb{Z}^d) \le \omega(\sqrt{\log d})$.

(3) Given a basis B for a d-dimensional lattice $\Lambda = \mathcal{L}(B)$ and a real number $r = \omega(\sqrt{\log d})$, for any vector $\boldsymbol{c} \in \mathbb{R}^d$ and any real symmetric positive definite matrix Σ satisfying $\Sigma > r^2 \cdot B \cdot B^{\mathrm{T}}$, there exists a polynomial-time sampling algorithm (using B) that samples from a distribution statistically close to $D_{\Lambda,\sqrt{\Sigma},\boldsymbol{c}}$.

Note that under the σ_{coef} embedding, $\mathcal{R}$ corresponds to $\mathbb{Z}^n$. According to Lemma 1, for any vector $\boldsymbol{c} \in \mathbb{R}^{n\cdot d}$ and any real symmetric positive definite matrix Σ satisfying $\Sigma > \omega(\sqrt{\log n \cdot d})$, we can efficiently sample from a distribution statistically indistinguishable from $D_{\mathcal{R}^d,\sqrt{\Sigma},\boldsymbol{c}}$.

Lemma 2. Assume $\varepsilon \in \left(0, \dfrac{1}{2}\right)$, Σ_1, Σ_2 are real symmetric positive definite matrices, $\Sigma_3^{-1} := \Sigma_2^{-1} + \Sigma_2^{-1}$, and $\sqrt{\Sigma_3} \ge \eta_\varepsilon(\mathbb{Z}^d)$. Then, for any vector $\boldsymbol{c} \in \mathbb{R}^d$, the statistical distance between the distribution $\{\boldsymbol{x}_1 + \boldsymbol{x}_2 : \boldsymbol{x}_1 \hookleftarrow D_{\mathbb{Z}^d,\sqrt{\Sigma_1}}, \boldsymbol{x}_2 \hookleftarrow D_{\mathbb{Z}^d,\sqrt{\Sigma_2},\boldsymbol{c}}\}$ and $D_{\mathbb{Z}^d,\sqrt{\Sigma_1+\Sigma_2},\boldsymbol{c}}$ is at most $2 \cdot \varepsilon$.

Using Lemma 2, we can decompose a discrete Gaussian distribution into the sum of two discrete Gaussian distributions with appropriate parameters.

2.2 LWE problems

The LWE problem was first introduced by Regev[1] and is currently the most widely used average-case hard lattice problem in lattice-based cryptography design.

In this paper, we use the symbol $\mathfrak{R}$ to denote the ring $\mathbb{Z}$ or $\mathcal{R}$ (the ring of integers in a cyclotomic field) and define $\mathfrak{R}_q := \mathfrak{R}/q \cdot \mathfrak{R}$. Under the coefficient embedding σ_{coef}, the addition and multiplication of elements in $\mathcal{R}$ can be represented using vector addition in $\mathbb{Z}^n$ and matrix-vector multiplication, respectively. Note that σ_{coef} can be trivially extended to vectors or matrices whose elements belong to $\mathcal{R}$. For convenience of discussion, the action of σ_{coef} on $\mathbb{Z}$ is defined as the identity map. Thus, σ_{coef} can be viewed as a $\mathbb{Z}$-module homomorphism on $\mathfrak{R}$, or as a $\mathbb{Z}_q$-module homomorphism on $\mathfrak{R}_q$.

For positive integers m, d, q, a probability distribution χ_1 over $\mathfrak{R}^m$, a probability distribution χ_2 over $\mathfrak{R}^d$, and a probability distribution $\mathcal{D}$ over $\mathfrak{R}_q^{m\times d}$, the decision version of the LWE problem related to the ring $\mathfrak{R}$ (denoted as $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$) is defined as follows: distinguish the distribution $(A, A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R})$ from the distribution $(A, \boldsymbol{u})$. Here, $A \hookleftarrow \mathcal{D}$, $\boldsymbol{s} \hookleftarrow \chi_2$, $\boldsymbol{e} \hookleftarrow \chi_1$, and $\boldsymbol{u} \hookleftarrow \mathrm{U}(\mathfrak{R}_q^m)$. Note that the parameter m in this definition corresponds to the number of samples in the LWE instance; $\mathcal{D}$ is the distribution of the public matrix; and χ_1 and χ_2 are the distributions for the error vector and the secret vector, respectively. For ease of discussion later, when a sample is of the form $(A, A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R})$, we say the sample is drawn from the distribution of the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ problem. For any (quantum) probabilistic polynomial-time adversary $\mathfrak{A}$, its advantage in solving the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ problem is defined as:

$$\mathrm{Adv}_{\mathfrak{A}}(\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})) := |\Pr[\mathfrak{A}(A, A\cdot\boldsymbol{s}+\boldsymbol{e} \bmod q\cdot\mathfrak{R}) = 1] - \Pr[\mathfrak{A}(A,\boldsymbol{u}) = 1]|$$

When $\mathfrak{R} = \mathbb{Z}$, the aforementioned decision version of the LWE problem corresponds to the LWE problem over Euclidean lattices. In this case, the parameter d represents the dimension of the corresponding lattice. When $\mathfrak{R} = \mathcal{R}$ (the ring of integers in a cyclotomic field), the aforementioned decision version of the LWE problem corresponds to the respective LWE problem defined over cyclotomic fields with power-of-two degree, which are the most used in practice. Here, the dimension of the corresponding lattice is $n \cdot d$. When $d = 1$, it corresponds to the ring LWE problem, whereas when $d \geq 2$, it corresponds to the module LWE problem.

Generally, the public matrix in the LWE problem follows the uniform distribution $\mathcal{D} = \mathrm{U}(\mathfrak{R}_q^{m\times d})$. When $\mathcal{D} \neq \mathrm{U}(\mathfrak{R}_q^{m\times d})$, we refer to the corresponding LWE problem as a non-uniform LWE problem. In this paper, we focus on a special class of non-uniform LWE problems called the SU-LWE problem, where $\mathcal{D}$ is an η-semi-uniform distribution defined as follows[4, 17, 18].

Definition 1. Let m, d be positive integers. For any positive real number $\eta > 0$, we say that a distribution $\mathcal{D}$ over $\mathfrak{R}_q^{m\times d}$ is an η-semi-uniform distribution if there exists a family of efficiently sampleable probability distributions $\{\phi_U\}_{U\in\mathfrak{R}^{m\times d}}$ over $\mathfrak{R}^{m\times d}$ such that for any randomly sampled $A \hookleftarrow \mathcal{D}$, $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, and $E_U \hookleftarrow \phi_U$, the following two conditions hold:

(1) The random variable A is statistically indistinguishable from $U + E_U \bmod q \cdot \mathfrak{R}$.

(2) $\Pr_{U\hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d}), E_U \hookleftarrow \phi_U}[\mathfrak{s}_1(\sigma_c(E_U)) \leq \eta] \geq 1 - \mathit{negl}(\lambda)$.

3 Research on Hardness of SU-LWE Problems

This section presents a tighter reduction method related to the hardness of the SU-LWE problem. Before giving the specific reduction, we require the following key lemma. The proof technique for Lemma 3 is similar to the method used in Ref. [10].

Lemma 3. Let σ_1, σ_2 be positive real numbers, $\tilde{m}, \tilde{n}$ be positive integers, and $F \in \mathbb{Z}^{\tilde{m}\times\tilde{n}}$ be an arbitrary matrix such that the matrix $\Sigma_0 := \left(\frac{1}{\sigma_1^2} \cdot I_{\tilde{n}} + \frac{1}{\sigma_2^2} \cdot F^{\mathrm{T}} \cdot F\right)^{-1}$ exists. Then the following two sampling procedures output identical distributions:

(1) Firstly take samples $\boldsymbol{s} \hookleftarrow D_{\mathbb{Z}^{\tilde{n}},\sigma_1}$ and $\boldsymbol{e} \hookleftarrow D_{\mathbb{Z}^{\tilde{m}},\sigma_2}$, then compute $\boldsymbol{z} = F \cdot \boldsymbol{s} + \boldsymbol{e}$, and finally output $(\boldsymbol{s}, \boldsymbol{z}) \in \mathbb{Z}^{\tilde{n}} \times \mathbb{Z}^{\tilde{m}}$;

(2) Firstly take samples $\boldsymbol{s} \hookleftarrow D_{\mathbb{Z}^{\tilde{n}},\sigma_1}$ and $\boldsymbol{e} \hookleftarrow D_{\mathbb{Z}^{\tilde{m}},\sigma_2}$, then compute $\boldsymbol{z} = F \cdot \boldsymbol{s} + \boldsymbol{e}$ and $\boldsymbol{c} = \frac{1}{\sigma_2^2} \cdot \Sigma_0 \cdot F^{\mathrm{T}} \cdot \boldsymbol{z}$; subsequently sample $\tilde{\boldsymbol{s}} \hookleftarrow D_{\mathbb{Z}^{\tilde{n}},\sqrt{\Sigma_0},\boldsymbol{c}}$; finally output $(\tilde{\boldsymbol{s}}, \boldsymbol{z}) \in \mathbb{Z}^{\tilde{n}} \times \mathbb{Z}^{\tilde{m}}$.

Proof: Denote the random variable output by the first procedure as $\boldsymbol{x}$ and that output by the second procedure as $\boldsymbol{y}$. Note that for any $(\boldsymbol{v}, \boldsymbol{w}) \in \mathbb{Z}^{\tilde{n}} \times \mathbb{Z}^{\tilde{m}}$,

$$\Pr[\boldsymbol{x} = \boldsymbol{v} \wedge \boldsymbol{y} = \boldsymbol{w}] = \Pr[\boldsymbol{y} = \boldsymbol{w}] \cdot \Pr[\boldsymbol{x} = \boldsymbol{v} | \boldsymbol{y} = \boldsymbol{w}]$$

Also, in both sampling procedures, $\Pr[\boldsymbol{y} = \boldsymbol{w}] = \Pr[\boldsymbol{z}{=}F \cdot \boldsymbol{s} + \boldsymbol{e} = \boldsymbol{w}]$ is identical. Therefore, to prove that the final output distributions of the two sampling procedures are identical, it suffices to prove that in sampling procedure (1), the conditional distribution of $\boldsymbol{s}$, given $F\cdot\boldsymbol{s}+\boldsymbol{e}$, is $D_{\mathbb{Z}^{\tilde{n}},\sqrt{\Sigma_0},\boldsymbol{c}}$.

To this end, take any $(\boldsymbol{v}, \boldsymbol{w}) \in \mathbb{Z}^{\tilde{n}} \times \mathbb{Z}^{\tilde{m}}$. In sampling procedure (1), we have:

$$\Pr[\boldsymbol{x} = \boldsymbol{v} \wedge \boldsymbol{y} = \boldsymbol{w}] = \Pr\left[\boldsymbol{s} = \boldsymbol{v} \wedge F \cdot \boldsymbol{s} + \boldsymbol{e} = \boldsymbol{w}\right] = \Pr[\boldsymbol{s} = \boldsymbol{v} \wedge \boldsymbol{e} = \boldsymbol{w} - F \cdot \boldsymbol{v}]$$

$$= \frac{1}{\rho_{\sigma_1}(\mathbb{Z}^{\tilde{n}}) \cdot \rho_{\sigma_2}(\mathbb{Z}^{\tilde{m}})} \cdot \mathrm{e}^{-\pi\left(\frac{1}{\sigma_1^2}\cdot \boldsymbol{v}^{\mathrm{T}}\cdot \boldsymbol{v} + \frac{1}{\sigma_2^2}\cdot(\boldsymbol{w}-F\cdot\boldsymbol{v})^{\mathrm{T}}\cdot(\boldsymbol{w}-F\cdot\boldsymbol{v})\right)}$$

$$= \frac{1}{\rho_{\sigma_1}(\mathbb{Z}^{\tilde{n}}) \cdot \rho_{\sigma_2}(\mathbb{Z}^{\tilde{m}})} \cdot \mathrm{e}^{-\pi\left((\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c}) - \boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c} + \frac{1}{{\sigma_2}^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}$$

Here, we have used the condition $\Sigma_0^{-1} = \Sigma_0^{-T}$. Noting that

$$\Pr[\boldsymbol{y}=\boldsymbol{w}] = \Pr[\boldsymbol{z}=\boldsymbol{w}] = \sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}} \Pr[\boldsymbol{s}=\boldsymbol{a}]\cdot\Pr[\boldsymbol{e}=\boldsymbol{w}-F\cdot\boldsymbol{s}|\boldsymbol{s}=\boldsymbol{a}]$$

$$= \frac{1}{\rho_{\sigma_1}(\mathbb{Z}^{\tilde{n}}) \cdot \rho_{\sigma_2}(\mathbb{Z}^{\tilde{m}})} \cdot \sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}} \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}} \cdot \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}$$

We can obtain:

$$\Pr[\boldsymbol{x}=\boldsymbol{v}|\boldsymbol{y}=\boldsymbol{w}] = \Pr[\boldsymbol{s}=\boldsymbol{v}|\boldsymbol{z}=\boldsymbol{w}] = \frac{\Pr[\boldsymbol{s}=\boldsymbol{v}\wedge\boldsymbol{z}=\boldsymbol{w}]}{\Pr[\boldsymbol{z}=\boldsymbol{w}]}$$

$$= \frac{\mathrm{e}^{-\pi\left(-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{{\sigma_2}^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}}{\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}} \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}} \cdot \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}} \cdot \mathrm{e}^{-\pi\cdot(\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})}$$

Because $\dfrac{\mathrm{e}^{-\pi\left(-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{{\sigma_2}^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}}{\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}} \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}} \cdot \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}}$ is independent of $\boldsymbol{v}$, and the probability identity $\sum_{\boldsymbol{v}\in\mathbb{Z}^{\tilde{n}}} \Pr[\boldsymbol{s}=\boldsymbol{v}|\boldsymbol{z}=\boldsymbol{w}] = 1$ holds, we have:

$$\frac{\mathrm{e}^{-\pi\left(-\boldsymbol{c}^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot\boldsymbol{c}+\frac{1}{\sigma_2^2}\boldsymbol{w}^{\mathrm{T}}\cdot\boldsymbol{w}\right)}}{\sum_{\boldsymbol{a}\in\mathbb{Z}^{\tilde{n}}} \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{a}\|^2}{\sigma_1^2}} \cdot \mathrm{e}^{-\pi\cdot\frac{\|\boldsymbol{w}-F\cdot\boldsymbol{a}\|^2}{\sigma_2^2}}} = \left(\sum_{\boldsymbol{v}\in\mathbb{Z}^{\tilde{n}}} \mathrm{e}^{-\pi\cdot(\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})}\right)^{-1} = \frac{1}{\rho_{\sqrt{\Sigma_0},\boldsymbol{c}}(\mathbb{Z}^{\tilde{n}})}$$

Therefore,

$$\Pr[\boldsymbol{s}=\boldsymbol{v}|\boldsymbol{z}=\boldsymbol{w}] = \frac{1}{\rho_{\sqrt{\Sigma_0},\boldsymbol{c}}(\mathbb{Z}^{\tilde{n}})} \cdot \mathrm{e}^{-\pi\cdot(\boldsymbol{v}-\boldsymbol{c})^{\mathrm{T}}\cdot\Sigma_0^{-1}\cdot(\boldsymbol{v}-\boldsymbol{c})}$$

That is to say, given $\boldsymbol{z} = F\cdot\boldsymbol{s}+\boldsymbol{e} = \boldsymbol{w}$, the conditional distribution of $\boldsymbol{s}$ is $D_{\mathbb{Z}^{\tilde{n}},\sqrt{\Sigma_0},\boldsymbol{c}}$.
□

3.1 Reduction for SU-LWE problems

The main theorem of this paper is as follows.

Theorem 1. Let $\varepsilon = negl(\lambda)$ be a negligible function, m, q, d be positive integers, and $\mathcal{D}$ be an η-semi-uniform distribution over $\mathfrak{R}_q^{m\times d}$. Let positive real numbers $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \gamma \geq \omega(\max\{\sqrt{\log m\cdot n}, \sqrt{\log d\cdot n}\})$ satisfy the conditions $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}} \geq \eta_\varepsilon(\mathfrak{R}^m)$, $\sigma_1 = \sqrt{\gamma^2+\sigma_3^2}$, and $\dfrac{1}{\sigma_2^2} + \dfrac{\eta^2}{\gamma^2} < \dfrac{1}{2\cdot\sigma_4^2}$. Define $\chi_1 = D_{\mathfrak{R}^m,\sigma_1}$, $\chi_2 = D_{\mathfrak{R}^d,\sigma_2}$, $\chi_3 = D_{\mathfrak{R}^m,\sigma_3}$, and $\chi_4 = D_{\mathfrak{R}^d,\sigma_4}$. If there exists a (quantum) probabilistic polynomial-time adversary $\mathfrak{A}$ that can solve the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ problem with probability δ, then there exists a (quantum) probabilistic polynomial-time adversary $\mathfrak{B}$ that can solve the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_3}(\chi_4;\mathrm{U}(\mathfrak{R}_q^{m\times d}))$ problem with probability $\delta - negl(\lambda)$.

Proof: By assumption, $\mathcal{D}$ is an η-semi-uniform distribution over $\mathfrak{R}_q^{m\times d}$. From Definition 1, there exists a family of efficiently sampleable probability distributions $\{\phi_U\}_{U\in\mathfrak{R}^{m\times d}}$ over $\mathfrak{R}^{m\times d}$ such that for any randomly sampled $A \hookleftarrow \mathcal{D}$, $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, and $E_U \hookleftarrow \phi_U$, the random variable A is statistically indistinguishable from $U + E_U \bmod q\cdot\mathfrak{R}$. Furthermore, $\Pr_{U\hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d}), E_U\hookleftarrow\phi_U}[\mathfrak{s}_1(\sigma_c(E_U)) \le \eta] \ge 1 - negl(\lambda)$.

For any (quantum) probabilistic polynomial-time adversary $\mathfrak{A}$, we define a sequence of distinguishing games Game_i, and define $p_i := \Pr_{\mathrm{Game}_i}[\mathfrak{A}(A,\boldsymbol{b}) = 1]$, where $i \in [6]$, $(A,\boldsymbol{b}) \in \mathfrak{R}_q^{m\times d} \times \mathfrak{R}_q^m$.

- Game_1: Take samples $A \hookleftarrow \mathcal{D}$, $\boldsymbol{s} \hookleftarrow \chi_2$, $\boldsymbol{e} \hookleftarrow \chi_1$; compute $\boldsymbol{b} = A\cdot\boldsymbol{s} + \boldsymbol{e} \bmod q\cdot\mathfrak{R}$; finally output $(A,\boldsymbol{b}) \in \mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

  Note that the output sample $(A,\boldsymbol{b})$ in Game_1 is the original distribution of the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}(\chi_2;\mathcal{D})$ problem.
- Game_2: Take samples $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $E_U \hookleftarrow \phi_U$, $\boldsymbol{s} \hookleftarrow \chi_2$, $\boldsymbol{e} \hookleftarrow \chi_1$; if $\mathfrak{s}_1(\sigma_c(E_U)) > \eta$, output $\perp$ (indicating a sampling error, game terminates); otherwise, compute $A = U + E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{b} = A\cdot\boldsymbol{s} + \boldsymbol{e} \bmod q\cdot\mathfrak{R}$; finally output $(A,\boldsymbol{b}) \in \mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

  According to Definition 1, the probability of outputting $\perp$ in Game_2 is negligible. When Game_2 outputs $(A,\boldsymbol{b})$ normally, the A output in Game_2 is statistically indistinguishable from the A output in Game_1. Therefore, we have $|p_1 - p_2| \le negl(\lambda)$.
- Game_3: Take samples $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $E_U \hookleftarrow \phi_U$, $\boldsymbol{s} \hookleftarrow \chi_2$; if $\mathfrak{s}_1(\sigma_c(E_U)) > \eta$, output $\perp$; otherwise, continue sampling $\boldsymbol{e}_1 \hookleftarrow D_{\mathfrak{R}^m,\gamma}$, $\boldsymbol{e}_2 \hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$; then compute $\boldsymbol{z} = E_U\cdot\boldsymbol{s} + \boldsymbol{e}_1$, $A = U + E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{b} = U\cdot\boldsymbol{s} + \boldsymbol{z} + \boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$; finally output $(A,\boldsymbol{b}) \in \mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

  Let $N = m$, $\tilde{N} = d$ when $\mathfrak{R} = \mathbb{Z}$; and $N = m\cdot n$, $\tilde{N} = n\cdot d$ when $\mathfrak{R} = \mathcal{R}$. If we set $\Sigma_1 := \gamma^2\cdot I_N$, $\Sigma_2 := \sigma_3^2\cdot I_N$, and take $\Sigma_3 := \dfrac{\gamma^2\cdot\sigma_3^2}{\gamma^2+\sigma_3^2}\cdot I_N$, then based on the assumption $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}} \ge \eta_\varepsilon(\mathfrak{R}^m) = \eta_\varepsilon(\mathbb{Z}^N)$ and Lemma 2, the statistical distance between the probability distribution $D_{\mathfrak{R}^m,\gamma} + D_{\mathfrak{R}^m,\sigma_3}$ and the distribution $D_{\mathfrak{R}^m,\sqrt{\gamma^2+\sigma_3^2}} = \chi_1$ is at most $2\cdot\varepsilon$. In Game_3, we have:

$$\begin{aligned}\boldsymbol{b} &= U\cdot\boldsymbol{s} + \boldsymbol{z} + \boldsymbol{e}_2 \bmod q\cdot\mathfrak{R} = U\cdot\boldsymbol{s} + E_U\cdot\boldsymbol{s} + \boldsymbol{e}_1 + \boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}\\ &= (U+E_U)\cdot\boldsymbol{s} + (\boldsymbol{e}_1+\boldsymbol{e}_2) \bmod q\cdot\mathfrak{R} = A\cdot\boldsymbol{s} + (\boldsymbol{e}_1+\boldsymbol{e}_2) \bmod q\cdot\mathfrak{R}\end{aligned}$$

  Therefore, from the above analysis, we get $|p_2 - p_3| \le negl(\lambda)$.
- Game_4: Take samples $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $E_U \hookleftarrow \phi_U$, $\boldsymbol{s} \hookleftarrow \chi_2$; if $\mathfrak{s}_1(\sigma_c(E_U)) > \eta$, output $\perp$; otherwise, continue sampling $\boldsymbol{e}_1 \hookleftarrow D_{\mathfrak{R}^m,\gamma}$, $\boldsymbol{e}_2 \hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$; then compute $A = U + E_U \bmod q\cdot\mathfrak{R}$, $\boldsymbol{z} = E_U\cdot\boldsymbol{s} + \boldsymbol{e}_1$, and take $\Sigma_0 := \left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}} + \dfrac{1}{\gamma^2}\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\sigma_c(E_U)\right)^{-1}$, $\boldsymbol{c} = \frac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$; subsequently sample $\tilde{\boldsymbol{s}} \hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0},\boldsymbol{c}}$, and use the pair $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ to compute $\boldsymbol{b} = U\cdot\tilde{\boldsymbol{s}} + \boldsymbol{z} + \boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$; finally output $(A,\boldsymbol{b}) \in \mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

  We firstly analyze whether the distributions required in Game_4 can be sampled efficiently. Note that $\Sigma_0^{-1} = \dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}} + \dfrac{1}{\gamma^2}\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\sigma_c(E_U)$. Based on the parameter choices, we have $\mathfrak{s}_1(\Sigma_0^{-1}) \le \dfrac{1}{\sigma_2^2} + \dfrac{\eta^2}{\gamma^2} < \dfrac{1}{2\cdot\sigma_4^2}$. Therefore, we get $\mathfrak{s}_{\tilde{N}}(\Sigma_0) > 2\cdot\sigma_4^2$, implying $\Sigma_0 > \sigma_4^2\cdot I_{\tilde{N}}$. By Lemma 1 and our parameter condition $\sigma_4 \ge \omega(\sqrt{\log n\cdot d})$, we can efficiently sample $\tilde{s}$ from a distribution statistically indistinguishable from $D_{\mathfrak{R}^d,\sqrt{\Sigma_0},\boldsymbol{c}}$. When all distributions can be efficiently sampled, the only difference between Game_3 and Game_4 lies in the pairs $(\boldsymbol{s},\boldsymbol{z})$ and $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ used to compute $\boldsymbol{b}$. According to Lemma 3, under our parameter choices, the distributions of $(\boldsymbol{s},\boldsymbol{z})$ and $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ are statistically indistinguishable. Therefore, we have $|p_3-p_4|\le negl(\lambda)$.

- Game_5: Take samples $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $E_U \hookleftarrow \phi_U$, $\boldsymbol{s} \hookleftarrow \chi_2$; if $\mathfrak{s}_1(\sigma_c(E_U))>\eta$, output $\perp$; otherwise, continue sampling $\boldsymbol{e}_1 \hookleftarrow D_{\mathfrak{R}^m,\gamma}$, $\boldsymbol{e}_2 \hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$; then $\Sigma_0 := \left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\sigma_c(E_U)\right)^{-1}$, $\boldsymbol{c}=\dfrac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$; subsequently sample $\boldsymbol{s}_1 \hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$ and $\boldsymbol{s}_2 \hookleftarrow D_{\mathfrak{R}^d,\sigma_4}$ and compute $\tilde{\boldsymbol{s}}=\boldsymbol{s}_1+\boldsymbol{s}_2 \bmod q\cdot\mathfrak{R}$; then use the pair $(\tilde{\boldsymbol{s}},\boldsymbol{z})$ to compute $\boldsymbol{b}=U\cdot\tilde{\boldsymbol{s}}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$; finally output $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

  We have already known $\mathfrak{s}_{\tilde{N}}(\Sigma_0) > 2\cdot\sigma_4^2$, so $\mathfrak{s}_{\tilde{N}}(\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}})>\sigma_4^2$. According to Lemma 1 and our parameter choices, we can efficiently sample from a distribution statistically close to $D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$. Now, if we set $\Sigma_1^{-1}=\frac{1}{\sigma_4^2}\cdot I_{\tilde{N}}$, $\Sigma_2^{-1}=(\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}})^{-1}$, and let $\Sigma_3^{-1}=\Sigma_1^{-1}+\Sigma_2^{-1}$, a simple calculation shows that $\mathfrak{s}_1(\Sigma_3^{-1})\le\dfrac{1}{\sigma_4^2}+\mathfrak{s}_1(\Sigma_2^{-1})<\dfrac{2}{\sigma_4^2}\le(\eta_\varepsilon(\mathfrak{R}^d))^{-2}$ holds. By Lemma 1, $\sqrt{\Sigma_3}\ge\eta_\varepsilon(\mathfrak{R}^d)$. Then, according to Lemma 2, the statistical distance between the distribution $D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}+D_{\mathfrak{R}^d,\sigma_4}$ and the distribution $D_{\mathfrak{R}^d,\sqrt{\Sigma_0},\boldsymbol{c}}$ is at most $2\cdot\varepsilon$, meaning the distributions of $\tilde{\boldsymbol{s}}$ in Game_4 and Game_5 are statistically indistinguishable. Thus, we get $|p_4-p_5|\le\mathrm{negl}(\lambda)$.

- Game_6: Take samples $U \hookleftarrow \mathrm{U}(\mathfrak{R}_q^{m\times d})$, $E_U \hookleftarrow \phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$, and $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$; if $\mathfrak{s}_1(\sigma_c(E_U))>\eta$, output $\perp$; otherwise compute $A=U+E_U \bmod q\cdot\mathfrak{R}$ and $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$; let $\Sigma_0 := \left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\sigma_c(E_U)\right)^{-1}$, $\boldsymbol{c}=\dfrac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$; subsequently sample $\boldsymbol{s}_1\hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$ and $\boldsymbol{u}\hookleftarrow U(\mathfrak{R}_q^m)$; compute $\boldsymbol{b}=U\cdot\boldsymbol{s}_1+\boldsymbol{z}+\boldsymbol{u} \bmod q\cdot\mathfrak{R}$; finally output $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

  In Game_6, since $\boldsymbol{u}$ is independently and randomly sampled from $\mathrm{U}(\mathfrak{R}_q^m)$, we have $\boldsymbol{b}\hookleftarrow\mathrm{U}(\mathfrak{R}_q^m)$. By the property of the η-semi-uniform distribution, the distribution of A is statistically indistinguishable from $\mathcal{D}$. By assumption, $\mathfrak{A}$ can solve $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_1}$ $(\chi_2;\mathcal{D})$ problem with probability δ. Therefore, we obtain $|p_1-p_6|\ge\delta-negl(\lambda)$. Combining the analysis from Game_1 to Game_5, we have $|p_5-p_6|\ge\delta-negl(\lambda)$. Note that in Game_5, $\boldsymbol{b}=U\cdot\tilde{\boldsymbol{s}}+\boldsymbol{z}+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}=U\cdot\boldsymbol{s}_1+\boldsymbol{z}+U\cdot\boldsymbol{s}_2+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$.

Now, we can use adversary $\mathfrak{A}$'s capability to construct an adversary $\mathfrak{B}$ for solving the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_3}$ $(\chi_4;\mathrm{U}(\mathfrak{R}_q^{m\times d}))$ problem. Suppose adversary $\mathfrak{B}$ receives a sample $(U,\tilde{\boldsymbol{b}})$, where either $U\hookleftarrow\mathrm{U}(\mathfrak{R}_q^{m\times d})$, $\boldsymbol{s}_2\hookleftarrow D_{\mathfrak{R}^d,\sigma_4}$, $\boldsymbol{e}_2\hookleftarrow D_{\mathfrak{R}^m,\sigma_3}$, $\tilde{\boldsymbol{b}}=U\cdot\boldsymbol{s}_2+\boldsymbol{e}_2 \bmod q\cdot\mathfrak{R}$ or $U\hookleftarrow\mathrm{U}(\mathfrak{R}_q^{m\times d})$, $\tilde{\boldsymbol{b}}\hookleftarrow\mathrm{U}(\mathfrak{R}_q^m)$, then $\mathfrak{B}$ performs the following operations:

(1) Take samples $E_U\hookleftarrow\phi_U$, $\boldsymbol{s}\hookleftarrow\chi_2$; if $\mathfrak{s}_1(\sigma_c(E_U))>\eta$, output $\perp$; otherwise, continue sampling $\boldsymbol{e}_1\hookleftarrow D_{\mathfrak{R}^m,\gamma}$;

(2) Compute $A=U+E_U \bmod q\cdot\mathfrak{R}$ and $\boldsymbol{z}=E_U\cdot\boldsymbol{s}+\boldsymbol{e}_1$, then take $\Sigma_0 := \left(\dfrac{1}{\sigma_2^2}\cdot I_{\tilde{N}}+\dfrac{1}{\gamma^2}\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\sigma_c(E_U)\right)^{-1}$, $\boldsymbol{c}=\dfrac{1}{\gamma^2}\cdot\Sigma_0\cdot\sigma_c(E_U)^{\mathrm{T}}\cdot\boldsymbol{z}$;

(3) Take samples $\boldsymbol{s}_1\hookleftarrow D_{\mathfrak{R}^d,\sqrt{\Sigma_0-\sigma_4^2\cdot I_{\tilde{N}}},\boldsymbol{c}}$, then compute $\boldsymbol{b}=U\cdot\boldsymbol{s}_1+\boldsymbol{z}+\tilde{\boldsymbol{b}} \bmod q\cdot\mathfrak{R}$;

(4) Output $(A,\boldsymbol{b})\in\mathfrak{R}_q^{m\times d}\times\mathfrak{R}_q^m$ to $\mathfrak{A}$.

Finally, $\mathfrak{B}$ outputs whatever $\mathfrak{A}$ outputs.

Clearly, based on our parameter choices, the operations of $\mathfrak{B}$ above can be completed in probabilistic polynomial time. Now, consider the probability that the constructed adversary $\mathfrak{B}$ successfully solves the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_3}$ $(\chi_4; \mathrm{U}(\mathfrak{R}_q^{m\times d}))$ problem. It is easy to see that when $(U, \tilde{\boldsymbol{b}})$ comes from the uniform distribution, the distribution of the sample $(A, \boldsymbol{b})$ given by $\mathfrak{B}$ to $\mathfrak{A}$ is identical to the output distribution of Game_6. Otherwise, the distribution of $(A, \boldsymbol{b})$ given by $\mathfrak{B}$ to $\mathfrak{A}$ is identical to the output distribution of Game_5. Therefore,

$$\mathrm{Adv}_{\mathfrak{B}}(\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_3}(\chi_4; \mathrm{U}(\mathfrak{R}_q^{m\times d}))) = |p_5 - p_6| \geq \delta - negl(\lambda)$$

□

Note that the condition $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \gamma \geq \omega(\max\{\sqrt{\log m \cdot n}, \sqrt{\log d \cdot n}\})$ in Theorem 1 is for a unified analysis over $\mathfrak{R}$. When $\mathfrak{R} = \mathbb{Z}$, the corresponding condition can be changed to $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \gamma \geq \omega(\max\{\sqrt{\log m}, \sqrt{\log d}\})$. We provide some brief explanations for the parameter conditions chosen in Theorem 1. The conditions $\frac{\gamma \cdot \sigma_3}{\sqrt{\gamma^2 + \sigma_3^2}} \geq \eta_\varepsilon(\mathfrak{R}^m)$ and $\sigma_1 = \sqrt{\gamma^2 + \sigma_3^2}$ ensure that during the transition from Game_2 to Game_3, we can decompose the original error $\boldsymbol{e}$ in Game_2. The condition $\frac{1}{\sigma_2^2} + \frac{\eta^2}{\gamma^2} < \frac{1}{2 \cdot \sigma_4^2}$ ensures that we can apply the key Lemma 3. Essentially, the condition $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \gamma \geq \omega(\max\{\sqrt{\log m \cdot n}, \sqrt{\log d \cdot n}\})$ guarantees that the corresponding discrete Gaussian distributions in the proof can be sampled efficiently. Meanwhile, this condition, combined with the condition $\frac{1}{\sigma_2^2} + \frac{\eta^2}{\gamma^2} < \frac{1}{2 \cdot \sigma_4^2}$, guarantees that during the transition from Game_4 to Game_5, the original error $\boldsymbol{s}$ in Game_4 can be decomposed. The resulting distribution form of Game_5 (and subsequently Game_6) is exactly as desired, which greatly facilitates the construction of a probabilistic polynomial-time algorithm (reduction) to embed an instance of the $\mathrm{DLWE}^d_{\mathfrak{R},m,q,\chi_3}$ $(\chi_4; \mathrm{U}(\mathfrak{R}_q^{m\times d}))$ problem.

3.2 Comparative analysis with known results

Utilizing Theorem 1, we can obtain hardness results for the SU-LWE problem over Euclidean, ring, or module lattices. In this subsection, for any integer $x \in \mathbb{Z}$, the symbol $\lfloor x \rfloor$ denotes the largest integer not exceeding x, and we define $\lfloor x \rceil := \lfloor x + \frac{1}{2} \rfloor$. The corresponding rounding notation can be trivially extended to vectors (polynomials) or matrices.

When $\mathfrak{R} = \mathbb{Z}$, we obtain a hardness reduction for the SU-LWE problem corresponding to d-dimensional Euclidean lattices.

Corollary 1. Let $\varepsilon = negl(\lambda)$ be a negligible function, m, q, d be positive integers, and $\mathcal{D}$ be an η-semi-uniform distribution over $\mathbb{Z}_q^{m\times d}$. Let positive real numbers $\sigma_1, \sigma_2, \sigma_3, \sigma_4, \gamma \geq \sqrt{2} \cdot \omega(\max\{\sqrt{\log m}, \sqrt{\log d}\})$ satisfy the conditions $\frac{\gamma \cdot \sigma_3}{\sqrt{\gamma^2 + \sigma_3^2}} \geq \eta_\varepsilon(\mathbb{Z}^m)$, $\sigma_1 = \sqrt{\gamma^2 + \sigma_3^2}$, and $\frac{1}{\sigma_2^2} + \frac{\eta^2}{\gamma^2} < \frac{1}{2 \cdot \sigma_4^2}$. Define $\chi_1 = D_{\mathbb{Z}^m,\sigma_1}$, $\chi_2 = D_{\mathbb{Z}^d,\sigma_2}$, $\chi_3 = D_{\mathbb{Z}^m,\sigma_3}$, and $\chi_4 = D_{\mathbb{Z}^d,\sigma_4}$. If there exists a (quantum) probabilistic polynomial-time adversary $\mathfrak{A}$ that can solve the $\mathrm{DLWE}^d_{\mathbb{Z},m,q,\chi_1}$ $(\chi_2; \mathcal{D})$ problem with probability δ, then there exists a (quantum) probabilistic polynomial-time adversary $\mathfrak{B}$ that can solve the $\mathrm{DLWE}^d_{\mathbb{Z},m,q,\chi_3}$ $(\chi_4; \mathrm{U}(\mathbb{Z}_q^{m\times d}))$ problem with probability $\delta - negl(\lambda)$.

If we choose $\sigma_2 = 2\sqrt{2} \cdot \sigma_4$ and $\gamma = 2\sqrt{2} \cdot \sigma_4 \cdot \eta$, then $\frac{1}{\sigma_2^2} + \frac{\eta^2}{\gamma^2} = \frac{1}{4 \cdot \sigma_4^2} <$

$\dfrac{1}{2\cdot\sigma_4^2}$. By Lemma 1, $\eta_\varepsilon(\mathbb{Z}^m) \le \omega(\sqrt{\log m})$. Furthermore, $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}} = \dfrac{\gamma}{\sqrt{1+\left(\frac{\gamma}{\sigma_3}\right)^2}} = \dfrac{\sigma_3}{\sqrt{1+\left(\frac{\sigma_3}{\gamma}\right)^2}}$. Under the above parameter settings, when $\sigma_3, \gamma \ge \sqrt{2}\cdot\omega(\sqrt{\log m})$, the inequality $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}} \ge \eta_\varepsilon(\mathbb{Z}^m)$ always holds.

Note that $\sigma_1 = \sqrt{\gamma^2+\sigma_3^2}$, therefore, when selecting parameters $\sigma_3 = \sigma_4 =: \sigma$, the standard $\mathrm{DLWE}^d_{\mathbb{Z},m,q,D_{\mathbb{Z}^m,\sigma}}$ $(D_{\mathbb{Z}^d,\sigma}; \mathrm{U}(\mathbb{Z}_q^{m\times d}))$ problem can be reduced to the semi-uniform $\mathrm{DLWE}^d_{\mathbb{Z},m,q,\chi_1}$ $(\chi_2; \mathcal{D})$ problem where the public matrix follows an arbitrary η-semi-uniform distribution $\mathcal{D}$. Here, $\chi_1 = D_{\mathbb{Z}^m,\sigma_1}$, $\sigma_1 = O(\eta\cdot\sigma)$ and $\chi_2 = D_{\mathbb{Z}^d,\sigma_2}$, $\sigma_2 = O(\sigma)$.

It is worth noting that, disregarding polynomial sample size, the magnitude of the Gaussian parameter for the error distribution $\boldsymbol{e}$ determines the hardness of the corresponding LWE problem (e.g., using the method from Ref. [36], an LWE problem with a secret sampled from a uniform distribution can be reduced to an LWE problem with a secret sampled from a discrete Gaussian distribution with the same parameter as the error, i.e., the so-called normal form LWE problem; and the LWE problem with a uniformly distributed secret is the hardest among problems under equivalent conditions). Therefore, here we only illustrate the case where $\sigma_3 = \sigma_4$ here.

Compared with the reduction result in Ref. [4], our reduction is dimension-preserving (it maintains the lattice dimension d), whereas the reduction in Ref. [4] relies on the hardness of a corresponding lower-dimensional LWE problem. Simultaneously, in our reduction result, the asymptotic loss in the error parameter between the two problems is η, independent of the number of samples. However, the asymptotic loss in the error parameter in the reduction of Ref [4] depends on the number of samples (approximately $\sigma_1 = \tilde{\mathrm{O}}(\sqrt{m}\cdot\sigma+\eta)$). It is important to note that our reduction result is limited to the case where the secret/error follows a discrete Gaussian distribution and is only applicable to the reduction for the decision version of the LWE problem. In contrast, the reduction in Ref. [4] applies to both search and decision versions. However, for the decision version of the corresponding problem, Ref. [4] requires additional restrictions, such as q being prime or the secret $\boldsymbol{s}$ being drawn from a binary distribution over $\{0,1\}$ with sufficient entropy under specific conditions.

Let $0 < p \le q$ be positive integers. For any matrix $U \in \mathbb{Z}_q^{m\times d}$, we can define a fixed function $E_U = \left\lfloor \dfrac{q}{p}\cdot\left\lfloor\dfrac{p}{q}\cdot U\right\rceil\right\rceil - U$. For any $x\in\mathbb{Z}_q$, a simple calculation shows that $\left|x - \left\lfloor\dfrac{q}{p}\cdot\left\lfloor\dfrac{p}{q}\cdot x\right\rceil\right\rceil\right| \le \left\lfloor\frac{q}{2p}\right\rceil$. Therefore, we have $\mathfrak{s}_1(E_U) \le \sqrt{m\cdot d}\cdot\left\lfloor\dfrac{q}{2p}\right\rceil$. Define the distribution $\mathcal{D}_{p,q,m,d}$ as: Sample $U\in\mathbb{Z}_q^{m\times d}$, output $\left\lfloor\dfrac{q}{p}\cdot\left\lfloor\dfrac{p}{q}\cdot U\right\rceil\right\rceil$. Then $\mathcal{D}_{p,q,m,d}$ is a specific $\sqrt{m\cdot d}\cdot\left\lfloor\dfrac{q}{2p}\right\rceil$ -semi-uniform distribution. The conclusions discussed above can be naturally applied to the SU-LWE problem corresponding to $\mathcal{D}_{p,q,m,d}$.

When $\mathfrak{R} = \mathcal{R}$, we obtain a hardness reduction for the corresponding decision version of the ring/module SU-LWE problem.

Corollary 2. Let $\varepsilon = negl(\lambda)$ be a negligible function, m, q, d be positive integers, and $\mathcal{D}$ be an η-semi-uniform distribution over $\mathcal{R}_q^{m\times d}$. Let positive real numbers $\sigma_1,\sigma_2,\sigma_3,\sigma_4,\gamma \ge \sqrt{2}\cdot\omega(\max\{\sqrt{\log m\cdot n}, \sqrt{\log d\cdot n}\})$ satisfy the conditions $\dfrac{\gamma\cdot\sigma_3}{\sqrt{\gamma^2+\sigma_3^2}} \ge \eta_\varepsilon(\mathcal{R}^m)$, $\sigma_1 =$

$\sqrt{\gamma^2+\sigma_3^2}$, and $\dfrac{1}{\sigma_2^2}+\dfrac{\eta^2}{\gamma^2}<\dfrac{1}{2\cdot\sigma_4^2}$. Define $\chi_1=D_{\mathcal{R}^m,\sigma_1}$, $\chi_2=D_{\mathcal{R}^d,\sigma_2}$, $\chi_3=D_{\mathcal{R}^m,\sigma_3}$, and $\chi_4=D_{\mathcal{R}^d,\sigma_4}$. If there exists a (quantum) probabilistic polynomial-time adversary $\mathfrak{A}$ that can solve the $\mathrm{DLWE}^d_{\mathcal{R},m,q,\chi_1}$ $(\chi_2;\mathcal{D})$ problem with probability δ, then there exists a (quantum) probabilistic polynomial-time adversary $\mathfrak{B}$ that can solve the $\mathrm{DLWE}^d_{\mathcal{R},m,q,\chi_3}$ $(\chi_4;U(\mathcal{R}_q^{m\times d}))$ problem with probability $\delta-negl(\lambda)$.

Similar to the parameter analysis for the SU-LWE problem over Euclidean lattices, it can be deduced that, when selecting parameters $\sigma_3=\sigma_4=:\sigma$, the standard $\mathrm{DLWE}^d_{\mathcal{R},m,q,D_{\mathcal{R}^m,\sigma}}$ $(D_{\mathcal{R}^d,\sigma};\mathrm{U}(\mathcal{R}_q^{m\times d}))$ problem can be reduced to the semi-uniform $\mathrm{DLWE}^d_{\mathcal{R},m,q,\chi_1}$ $(\chi_2;\mathcal{D})$ problem where the public matrix follows an arbitrary η-semi-uniform distribution $\mathcal{D}$. Here, $\chi_1=D_{\mathcal{R}^m,\sigma_1}$, $\sigma_1=\mathrm{O}(\eta\cdot\sigma)$ and $\chi_2=D_{\mathcal{R}^d,\sigma_2}$, $\sigma_2=\mathrm{O}(\sigma)$.

Note that when $d=1$, the above result corresponds to the hardness reduction for the SU-LWE problem over rings. Unlike the conclusion in Ref. [17], we can reduce the standard ring LWE problem to the corresponding ring SU-LWE problem without requiring additional hardness assumptions (such as specific forms of the decisional small polynomial ratio (DSPR) assumption, which corresponds to a decisional version of the NTRU assumption). When $d\geq 2$, compared to the result in Ref. [4], asymptotically, the loss in our error parameter reduction is only η, independent of other parameters. Particularly, our reduction is also dimension-preserving (it maintains the lattice dimension/rank d) and does not rely on the hardness of lower-dimensional (more precisely, lower-rank) module LWE problems as in Refs. [4, 17, 18].

The distribution $\mathcal{D}_{p,q,m,d}$ is defined as: Take sample $U\in\mathcal{R}_q^{m\times d}$, output $\left\lfloor\dfrac{q}{p}\cdot\left\lfloor\dfrac{p}{q}\cdot U\right\rceil\right\rceil$. A simple calculation shows that $\mathcal{D}_{p,q,m,d}$ is a specific $n\cdot\sqrt{m\cdot d}\cdot\left\lceil\dfrac{q}{2p}\right\rceil$-semi-uniform distribution. Using the module SU-LWE problem corresponding to distribution $\mathcal{D}_{p,q,m,d}$, one can prove that when employing a public key compression design method similar to that used in the NIST Round 1 candidate Kyber, the underlying encryption scheme also satisfies IND-CPA security. A concrete scheme construction is as follows. Since the proof of IND-CPA security for related schemes is standard, we only provide a general explanation; detailed proofs can be found in Refs. [4, 25–29].

- $\mathrm{KeyGen}(1^\lambda)$: Given the security parameter λ, the key generation algorithm samples $A\hookleftarrow\mathrm{U}(\mathcal{R}_q^{d\times d})$, $\boldsymbol{s}\hookleftarrow D_{\mathcal{R}^d,\sigma_2}$, $\boldsymbol{e}\hookleftarrow D_{\mathcal{R}^d,\sigma_1}$. It computes $\boldsymbol{b}=A\cdot\boldsymbol{s}+\boldsymbol{e}$ and returns the public key $pk=(A,\left\lfloor\dfrac{p}{q}\cdot\boldsymbol{b}\right\rceil)$ and the secret key $sk=\boldsymbol{s}$.
- $\mathrm{Enc}(pk,m)$: Assume $pk=(A,\left\lfloor\dfrac{p}{q}\cdot\boldsymbol{b}\right\rceil)$. To encrypt a message $\sigma_c(m)\in\{0,1\}^n$, the encryption algorithm first computes $\tilde{\boldsymbol{b}}=\left\lfloor\dfrac{q}{p}\cdot\left\lfloor\dfrac{p}{q}\cdot\boldsymbol{b}\right\rceil\right\rceil$. Then, it takes samples $\boldsymbol{r}\hookleftarrow D_{\mathcal{R}^d,\sigma_2}$, $\boldsymbol{e}_1\hookleftarrow D_{\mathcal{R}^d,\sigma_2}$, $e_2\hookleftarrow D_{\mathcal{R},\sigma_1}$, and computes $\boldsymbol{c}_1=A^{\mathrm{T}}\cdot\boldsymbol{r}+\boldsymbol{e}_1$ and $c_2=\tilde{\boldsymbol{b}}^{\mathrm{T}}\cdot\boldsymbol{r}+e_2$. Finally, it outputs the ciphertext $ct=(\boldsymbol{c}_1,c_2)$.
- $\mathrm{Dec}(sk,ct)$: Assume $ct=(\boldsymbol{c}_1,c_2)$, $sk=\boldsymbol{s}$. The decryption algorithm computes and returns $m=\left\lfloor\dfrac{2}{q}\cdot(c_2-\boldsymbol{s}^{\mathrm{T}}\cdot\boldsymbol{c}_1)\right\rceil$.

A simple calculation shows that, for appropriately chosen parameters, the above scheme can decrypt correctly. To prove the IND-CPA security of the scheme, the decisional version of the LWE assumption needs to be used twice. The first time is to replace $(A,\boldsymbol{b})$ with a uniformly random $(A,\boldsymbol{u})$, using the assumption that the $\mathrm{DLWE}^d_{\mathcal{R},d,q,D_{\mathcal{R}^d,\sigma_1}}$ $(D_{\mathcal{R}^d,\sigma_2};\mathrm{U}(\mathcal{R}_q^{d\times d}))$

problem is hard. The second time is to replace the ciphertext with uniformly random elements, where replacing the ciphertext $\boldsymbol{c}_1$ still uses the assumption that the $\mathrm{DLWE}^d_{\mathcal{R},d,q,D_{\mathcal{R}^d,\sigma_1}}$ $(D_{\mathcal{R}^d,\sigma_2};\mathrm{U}(\mathcal{R}_q^{d\times d}))$ problem is hard. However, replacing the ciphertext c_2 requires the hardness assumption of the $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}$ $(D_{\mathcal{R}^d,\sigma_2};\mathcal{D}_{p,q,1,d})$ problem. Here, $\mathcal{D}_{p,q,1,d}$ corresponds to the distribution: Sample $\boldsymbol{u} \hookleftarrow \mathrm{U}(\mathcal{R}_q^d)$, output $\left\lfloor \frac{q}{p} \cdot \left\lfloor \frac{p}{q} \cdot \boldsymbol{u} \right\rceil \right\rceil$. Note that the distribution $\mathcal{D}_{p,q,1,d}$ is an $n\cdot\sqrt{d}\cdot\left\lfloor \frac{q}{2p} \right\rceil$-semi-uniform distribution. Using the reduction result of this paper, the hardness of the $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}$ $(D_{\mathcal{R}^d,\sigma_2};\mathcal{D}_{p,q,1,d})$ problem can be guaranteed by the hardness of the $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma}}$ $(D_{\mathcal{R}^d,\sigma};\mathrm{U}(\mathcal{R}_q^d))$ problem. The corresponding parameter relationship is $\sigma_1 = \mathrm{O}\left(n\cdot\sqrt{d}\cdot\left\lfloor \frac{q}{2p} \right\rceil\cdot\sigma\right)$, $\sigma_2 = \mathrm{O}(\sigma)$. To balance decryption error rate and security strength, the bit difference between parameters p and q is generally $\mathrm{O}(1)$. Using the empirical estimation from Ref. [27], the hardness of an asymmetric LWE problem is roughly equivalent to that of a symmetric LWE problem with an error parameter of about $\sqrt{\sigma_1\cdot\sigma_2} = \mathrm{O}(n^{\frac{1}{2}}\cdot d^{\frac{1}{4}})\cdot\sigma$. Therefore, when applying the reduction result of this paper to public key encryption schemes designed using the Kyber-like compressed public key method, the corresponding theoretical reduction loss is about $\mathrm{O}(n^{\frac{1}{2}}\cdot d^{\frac{1}{4}})$. It is worth noting that our reduction method imposes very few restrictions on the parameter d (and q). One can choose $d=\mathrm{O}(1)$, in which case the corresponding theoretical reduction loss is about $\mathrm{O}(n^{\frac{1}{2}})$.

We use theorem in Section 5.2 of Ref. [4] to estimate the theoretical reduction loss for the IND-CPA security of the public key encryption scheme designed as above. In this case, the hardness of the $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}$ $(D_{\mathcal{R}^d,\sigma_2};\mathcal{D}_{p,q,1,d})$ problem can be guaranteed by the hardness of the $\mathrm{DLWE}^k_{\mathcal{R},1,q,D_{\mathcal{R},\sigma}}$ $(\mathrm{U}(\mathcal{R}_q^k);\mathrm{U}(\mathcal{R}_q^k))$ problem and the $\mathrm{DLWE}^d_{\mathcal{R},1,q,D_{\mathcal{R},\sigma_1}}$ $(\mathrm{U}(\mathcal{R}_q^d);\mathrm{U}(\mathcal{R}_q^d))$ problem. Here, $\sigma_1 = \mathrm{O}\left(n\cdot\sqrt{d}\cdot\left\lfloor \frac{q}{2p} \right\rceil\cdot\sigma+\sigma^2\right)$. If we also choose $\sigma_2 = \mathrm{O}(\sigma)$, then based on the properties of discrete Gaussian distributions and roughly estimating the entropy inequality condition in Ref. [4], the rank d of the corresponding module LWE problem should satisfy $d \geq \mathrm{O}(k\cdot\log q+\log n+\omega(\log\lambda))$ (note that this condition should hold even if $D_{\mathcal{R}^d,\sigma_2}$ is replaced by a random uniform distribution). Therefore, strictly speaking, the reduction result of Ref. [4] is not applicable to the case $d=\mathrm{O}(1)$. Furthermore, the reduction result of Ref. [4] imposes additional restrictions on the parameter q and the secret distribution. For example, it requires q to be a prime with good splitting properties and requires the distribution of the secret modulo each prime ideal of $q\mathcal{R}$ to have sufficiently large entropy. With these restrictions, the reduction result of Ref. [4] becomes even more limited.

4 Summary

In this paper, we refined techniques from the study of Hint-LWE related problems and applied them to the investigation of the SU-LWE problem, presenting a simpler and tighter hardness reduction for non-uniform LWE problems. Specifically, the reduction method introduced here is largely independent of the underlying algebraic structure and can be uniformly applied to reductions for the SU-LWE problem defined over Euclidean, ring, or module lattices. Compared with known reduction results for the SU-LWE problem, our reduction is dimension-preserving for the corresponding LWE problem and incurs a smaller reduction loss. This loss, reflected in the Gaussian parameter of the error distribution in the corresponding LWE problem, is independent of conditions such as the number of samples. When applying our reduction to the ring LWE problems, the corresponding method can establish the hardness of the non-uniform ring LWE problems based on the standard ring LWE problem, without requiring additional (and relatively non-standard) hardness assumptions such as DSPR.

References

[1] Regev O. On lattices, learning with errors, random linear codes, and cryptography. Proc. of the 37th Annual ACM SIGACT Symp. on Theory of Computing. Baltimore: ACM, 2005. 84–93. [doi: 10.1145/1060590.1060603]

[2] Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: Gilbert H, ed. Proc. of the 29th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. French: Springer, 2010. 1–23. [doi: 10.1007/978-3-642-13190-5_1]

[3] Langlois A, Stehlé D. Worst-case to average-case reductions for module lattices. Designs, Codes and Cryptography, 2015, 75(3): 565–599. [doi: 10.1007/s10623-014-9938-4]

[4] Jia WJ, Zhang J, Xiang BW, Wang BC. Hardness of (M)LWE with semi-uniform seeds. Theoretical Computer Science, 2024, 994: 114481. [doi: 10.1016/j.tcs.2024.114481]

[5] Brakerski Z, Langlois A, Peikert C, Regev O, Stehlé D. Classical hardness of learning with errors. Proc. of the 45th Annual ACM Symp. on Theory of Computing. Palo Alto: ACM, 2005. 575–584. [doi: 10.1145/2488608.2488680]

[6] Goldwasser S, Kalai YT, Peikert C, Vaikuntanathan V. Robustness of the learning with errors assumption. Innovations in Computer Science—ICS 2010. Beijing: Tsinghua University Press, 2010. 230–240.

[7] Micciancio D. On the hardness of learning with errors with binary secrets. Theory of Computing, 2018, 14: 13. [doi: 10.4086/toc.2018.v014a013]

[8] Brakerski Z, Döttling N. Hardness of LWE on general entropic distributions. In: Canteaut A, Ishai Y, eds. Proc. of the 39th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Zagreb: Springer, 2020. 551–575. [doi: 10.1007/978-3-030-45724-2_19]

[9] Boudgoust K, Jeudy C, Roux-Langlois A, Wen WQ. On the hardness of module learning with errors with short distributions. Journal of Cryptology, 2023, 36(1): 1. [doi: 10.1007/s00145-022-09441-3]

[10] Kim D, Lee D, Seo J, Song Y. Toward practical lattice-based proof of knowledge from Hint-MLWE. In: Handschuh H, Lysyanskaya A, eds. Proc. of the 43rd Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO 2023). Santa Barbara: Springer, 2023. 549–580. [doi: 10.1007/978-3-031-38554-4_18]

[11] Dottling N, Kolonelos D, Lai RWF, Lin CW, Malavolta G, Rahimi A. Efficient laconic cryptography from learning with errors. In: Hazay C, Stam M, eds. Proc. of the 42nd Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Lyon: Springer, 2023. 417–446. [doi: 10.1007/978-3-031-30620-4_14]

[12] Agrawal S, Libert B, Stehlé D. Fully secure functional encryption for inner products, from standard assumptions. In: Robshaw M, Katz J, eds. Proc. of the 36th Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO 2016). Santa Barbara: Springer, 2023. 333–362. [doi: 10.1007/978-3-662-53015-3_12]

[13] Mera JMB, Karmakar A, Marc T, Soleimanian A. Efficient lattice-based inner-product functional encryption. In: Hanaoka G, Shikata J, Watanabe Y, eds. Proc. of the 25th IACR Int'l Conf. on Practice and Theory of Public-key Cryptography. Springer, 2022. 163–193. [doi: 10.1007/978-3-030-97131-1_6]

[14] Alperin-Sheriff J, Peikert C. Circular and KDM security for identity-based encryption. In: Fischlin M, Buchmann J, Manulis M, eds. Proc. of the 15th Int'l Conf. on Practice and Theory in Public Key Cryptography. Darmstadt: Springer, 2012. 334–352. [doi: 10.1007/978-3-642-30057-8_20]

[15] O'Neill A, Peikert C, Waters B. Bi-deniable public-key encryption. In: Rogaway P, ed. Proc. of the 31st Annual Cryptology Conf. on Advances in Cryptology (CRYPTO 2011). Santa Barbara: Springer, 2011. 525–542. [doi: 10.1007/978-3-642-22792-9_30]

[16] Boneh D, Lewi K, Montgomery H, Raghunathan A. Key homomorphic PRFs and their applications.

In: Canetti R, Garay JA, eds. Proc. of the 33rd Annual Cryptology Conf. on Advances in Cryptology. Santa Barbara: Springer, 2013. 410–428. [doi: 10.1007/978-3-642-40041-4_23]

[17] Jia WJ, Zhang J, Wang BC. Hardness of module-LWE with semiuniform seeds from module-NTRU. IET Information Security, 2023, 2023: 2969432. [doi: 10.1049/2023/2969432]

[18] Jia WJ, Wang BC. Hardness of (Semiuniform) MLWE with short distributions using the Rényi divergence. IET Information Security, 2023, 2023: 2104380. [doi: 10.1049/2023/2104380]

[19] National Institute of Standards and Technology. Post-quantum cryptography—Round 1 submissions. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-1-submissions

[20] Bos J, Ducas L, Kiltz E, Lepoint T, Lyubashevsky V, Schanck JM, Schwabe P, Seiler G, Stehle D. CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. Proc. of the 2018 IEEE European Symp. on Security and Privacy (EuroS&P). London: IEEE, 2018. 353–367. [doi: 10.1109/EuroSP.2018.00032]

[21] Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Kiayias A, ed. Topics in Cryptology—CT-RSA 2011. Berlin, Heidelberg: Springer, 2011. 319–339. [doi: 10.1007/978-3-642-19074-2_21]

[22] National Institute of Standards and Technology. Post-quantum cryptography—Round 2 submissions. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-2-submissions

[23] National Institute of Standards and Technology. Post-quantum cryptography—Round 3 submissions. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions

[24] National Institute of Standards and Technology. Post-quantum cryptography—Selected algorithms 2022. 2024. https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[25] Jin ZZ, Zhao YL. Optimal key consensus in presence of noise. arXiv: 1611.06150, 2017.

[26] Jin ZZ, Zhao YL. Generic and practical key establishment from lattice. In: Deng RH, Gauthier-Umana V, Ochoa M, Yung M, eds. Proc. of the 17th Int'l Conf. on Applied Cryptography and Network Security. Bogota: Springer, 2019. 302–322. [doi: 10.1007/978-3-030-21568-2_15]

[27] Zhang J, Yu Y, Fan SQ, Zhang ZF, Yang K. Tweaking the asymmetry of asymmetric-key cryptography on lattices: KEMs and signatures of smaller sizes. In: Kiayias A, Kohlweiss M, Wallden P, Zikas V, eds. Proc. of the 23rd IACR Int'l Conf. on Practice and Theory of Public-key Cryptography. Edinburgh: Springer, 2020. 37–65. [doi: 10.1007/978-3-030-45388-6_2]

[28] Chinese Association for Cryptologic Research. Public key algorithms selected to the second round competition of national cryptographic algorithm competitions. 2020 (in Chinese). http://sfjs.cacrnet.org.cn/site/term/list_77_1.html

[29] Chinese Association for Cryptologic Research. Announcement of the selection results of the national cryptographic algorithm competition. 2020 (in Chinese). https://www.cacrnet.org.cn/site/content/854.html

[30] Micciancio D. Generalized compact knapsacks, cyclic lattices, and efficient one-way functions. Computational Complexity, 2007, 16(4): 365–411. [doi: 10.1007/s00037-007-0234-9]

[31] Bruna J, Regev O, Song MJ, Tang Y. Continuous LWE. Proc. of the 53rd Annual ACM SIGACT Symp. on Theory of Computing. ACM, 2021. 694–707. [doi: 10.1145/3406325.3451000]

[32] Gupte A, Vafa N, Vaikuntanathan V. Continuous LWE is as hard as LWE & applications to learning Gaussian mixtures. Proc. of the 63rd IEEE Annual Symp. on Foundations of Computer Science. Denver: IEEE, 2022. 1162–1173. [doi: 10.1109/FOCS54457.2022.00112]

[33] Peikert C. An efficient and parallel Gaussian sampler for lattices. In: Rabin T, ed. Proc. of the 30th Annual Cryptology Conf. on Advances in Cryptology (CRYPTO 2010). Santa Barbara: Springer, 2010. 80–97. [doi: 10.1007/978-3-642-14623-7_5]

[34] Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. Proc. of the 40th Annual ACM Symp. on Theory of Computing. Victoria: ACM, 2008. 197–206. [doi: 10.1145/1374376.1374407]

[35] Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. SIAM Journal on Computing, 2007, 37(1): 267–302. [doi: 10.1137/S0097539705447360]

[36] Applebaum B, Cash D, Peikert C, Sahai A. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In: Halevi S, ed. Proc. of the 29th Annual Int'l Cryptology Conf. on Advances in Cryptology (CRYPTO 2009). Santa Barbara: Springer, 2009. 595–618. [doi: 10.1007/978-3-642-03356-8_35]

Yang Wang, Ph.D., assistant professor. His research interests include lattice-based cryptography, quantum information, and quantum computing.

Mingqiang Wang, Ph.D., professor, doctoral supervisor. His research interests include analysis and design of public-key cryptographic algorithms, elliptic curves, lattice-based cryptography, quantum information, and quantum computing.