SCIENCE CHINA
Information Sciences

• RESEARCH PAPER •

September 2020, Vol. 63 192101:1–192101:13
https://doi.org/10.1007/s11432-018-9788-1

Rényi divergence on learning with errors

Yang TAO[1,2], Han WANG[1,2*] & Rui ZHANG[1,2]

[1] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2] *School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049*, China*

Received 7 August 2018/Revised 31 December 2018/Accepted 14 February 2019/Published online 10 August 2020

Abstract Many lattice-based schemes are built from the hardness of the learning with errors problem, which naturally comes in two flavors: the decision LWE and search LWE. In this paper, we investigate the decision LWE and search LWE by Rényi divergence respectively and obtain the following results: For decision LWE, we apply RD on LWE variants with different error distributions (i.e., center binomial distribution and uniform distribution, which are frequently used in the NIST PQC submissions) and prove the pseudorandomness in theory. As a by-product, we extend the so-called public sampleability property and present an adaptively public sampling property to the application of Rényi divergence on more decision problems. As for search LWE, we improve the classical reduction proof from GapSVP to LWE. Besides, as an independent interest, we also explore the intrinsic relation between the decision problem and search problem.

Keywords Rényi divergence, learning with errors, decision problems, search problems, post-quantum cryptography

Citation Tao Y, Wang H, Zhang R. Rényi divergence on learning with errors. Sci China Inf Sci, 2020, 63(9): 192101, https://doi.org/10.1007/s11432-018-9788-1

1 Introduction

Lattice based crypto and LWE. Lattice-based cryptography has been one of the most promising candidates in the post-quantum cryptography, since it is not known to be affected by any quantum algorithms, e.g., Shor's algorithm. In the recent NIST PQC candidate collections, there are many lattice-based proposals. Among them, most schemes are relied on the learning with errors (LWE) problem which was first introduced by Regev in 2005. In the seminal work of [1], the standard LWE problem can be viewed as decoding random linear codes with discrete Gaussian errors and two versions of LWE — search LWE (SLWE) and decision LWE (DLWE) were defined. Regev gave a quantum reduction from the short independent vectors problem (SIVP) in any lattice to the SLWE and then showed the equivalence between the DLWE and SLWE. However, cryptographic applications based on the plain LWE suffered from the quadratic key size. In order to improve efficiency of the lattice-based schemes, Lyubashesky et al. [2] introduced the ring structure and presented the Ring-LWE (RLWE), which can be proved as hard as SIVP problems in the ideal lattices. Since the algebraic structure may provide the adversaries additional advantage for solving hard problems in the ideal lattice, a more general definition — module-LWE (MLWE) was considered by Langlois and Stehlé [3], which can be viewed as a "tensor product" of the ring to fill the gap between the plain LWE and RLWE.

Up to now, there have been fruitful achievements on cryptographic schemes based on LWE/RLWE/MLWE problems, such as public key encryption [1, 2, 4, 5], fully homomorphic encryption [6, 7], and authenticated key exchange [8, 9]. Hence, LWE problems play a crucial role on the security and performance

[*] Corresponding author (email: wanghan@iie.ac.cn)

Table 1 List of NIST submissions based on LWE with different error distributions

Scheme	Functionality	Hard problem	Error distribution
Kyber [10]	KEM/PKE	MLWE	Center binomial distribution
NewHope [11]	KEM/PKE	RLWE	Center binomial distribution
LAC [12]	KEM/PKE	RLWE	Center binomial distribution
LIMA [13]	KEM/PKE	RLWE	Center binomial distribution
KINDI [14]	KEM/PKE	MLWE	Uniform distribution
Dilithium [15]	Signature	MLWE	Uniform distribution

of such cryptographic schemes. In particular, many NIST candidates even rely on the LWE variants with different error distributions rather than discrete Gaussian distributions. Concretely, in several NIST candidates, in order to avoid the high precise sampling of Gaussian distributions, they choose the efficiently sampleable center binomial distribution or uniform distribution as an approximation of Gaussian errors (see Table 1 [10–15]). However, since the worst-case to average-case reductions of LWE problems are applicable for the standard LWE with Gaussian errors and only the state-of-the-art attacks of such LWE variants are considered, the security reduction of the above LWE variants with different errors is still unclear from the theoretical view.

Rényi divergence on LWE. When analyzing the security proof of cryptographic schemes, it is important to measure the closeness of two different distributions over the same support. In most cases, we use statistical distance to measure the closeness of two distributions due to its probability preserving property. In order to preserve certain probability properties, it is often required the negligible statistical distance between two games of the security proof, which makes the parameters larger and less efficient. To bypass these issues, Lyubashevsky et al. [2] introduced another tool to measure the distance of two distributions, i.e., the so-called Rényi divergence (RD). Unlike the statistical distance behaving as the subtraction of two distributions, RD mainly focuses on the quotient of two distributions. The definition difference may lead us to get a "small" RD while the statistical distance of the same two distributions is quite "large". Thus, Bai et al. [16] improved the security proofs based on search problems, such as signatures and LWE variants' reductions[1]. However, to the best of our knowledge, there is still no effort to apply RD to the reduction from SLWE to the worst-case lattice problems.

On the other hand, as for the decision problems, RD seems not suitable for such problems. The major obstacle is that the advantage of a distinguisher is a substraction of two distributions while RD is the ratio between the given distributions. It is hard to find a lower bound on the substraction of two distributions (details refer to [16]). Thus, a general strategy [16, 17] to apply RD on DLWE is to apply it on the SLWE first and then use its search-to-decision equivalence. However, when adapting to the circumstances where the search-to-decision equivalence seems unclear[2], it is meaningful to apply RD on DLWE directly. Thanks to the public sampleability property, Bai et al. [16] can apply RD on some decision problems with distributions satisfying such property. However, it seems not trivial to verify the public sampleability property for many decision problems, e.g., some DLWE variants with different error distributions, which is frequently used in the NIST submissions and the pseudorandomness of LWE variants is still short of theoretic foundation.

Owing to the significance of LWE problems in the lattice-based cryptography, motivated by the work of Bai et al. [16], we consider the following problem: whether can we analyze the LWE using Rényi divergence?

1.1 Our results

In this paper, we apply RD to the LWE problems. In particular, we consider RD on DLWE and SLWE respectively. In DLWE, we prove the hardness of DLWE variants with different error distributions (i.e., center binomial distribution and uniform distribution) used in many NIST submissions. In SLWE, we

[1] The optimization on reductions in [16] are all reductions between average-case problems.

[2] In the aspect of MLWE, search-to-decision equivalence of [3] is proved just for prime modulus and Gaussian errors. It is unclear for MLWE with other error distributions and non-prime modulus.

can optimize the classical reduction efficiency from SLWE to GapSVP problems [18]. Our contributions are summarized as follows.

First, we focus on DLWE in the module setting where the search-to-decision equivalence is unclear and present a polynomial reduction from DLWE variants to the standard MLWE using RD. Our tool is a modified public sampling property like [16]. It comes from an observation that original public sampleability property seems a bit rigid. Recall that in [16] the decision problem is to distinguish two distributions $D_0(r)$ and $D_1(r)$ given the challenge x. The public sampleability property means there exists a public sampling algorithm S returning samples from $D_0(r)$ with the input $(0, x)$ and samples from $D_1(r)$ with the input $(1, x)$ given $x \leftarrow D_b(r)$ for all (r, b). Bai et al. cleverly utilized the public sampleability property to get samples from $D_0(r)$ and $D_1(r)$, estimated the probability via the Hoeffding bound and linked the advantage with the measure of randomness set r. However, when we regard the error term $\boldsymbol{e}$ of LWE as the randomness, it seems non-trivial to verify the public sampleability property. For simplicity, we take the plain LWE as an example. There are two distributions, i.e., uniform distribution $D_1(\boldsymbol{e}) = \{(\boldsymbol{A}, \boldsymbol{b}) | \boldsymbol{A} \leftarrow \mathbb{Z}_q^{m\times n}, \boldsymbol{b} \leftarrow \mathbb{Z}_q^m\}$ and LWE distribution $D_0(\boldsymbol{e}) = \{(\boldsymbol{A}, \boldsymbol{b} = \boldsymbol{A}\boldsymbol{s}+\boldsymbol{e}) | \boldsymbol{A} \leftarrow \mathbb{Z}_q^{m\times n}, \boldsymbol{s} \leftarrow \mathbb{Z}_q^n, \boldsymbol{e} \leftarrow \chi^m\}$. In general, given a challenge $x = (\boldsymbol{A}, \boldsymbol{b})$, the public sampling algorithm S is defined as $S(0, x) = (\boldsymbol{A}, \boldsymbol{b} + \boldsymbol{A}\boldsymbol{t})$ with $\boldsymbol{t} \leftarrow \mathbb{Z}_q^n$ and $S(1, x) = (\boldsymbol{A}, \boldsymbol{u})$. For $S(0, x)$, when x is from $D_0(\boldsymbol{e})$, the output is from $D_0(\boldsymbol{e})$. However, when x is from D_1, the output is from D_1 (uniform distribution) instead of D_0. Thus, it does not satisfy the public sampleability property.

To overcome the above obstacles, we pose an adaptively public sampling property and apply RD to DLWE variants. Our observation is that when trying to verify distributions satisfying the public sampleability property given an arbitrary sample x, it is not easy to construct a common public sampling algorithm for both distributions. However, it often seems not hard to construct different public sampling algorithms for the different distributions. Actually, it is not necessary to share the same public sampling algorithms for both distributions. Thus, instead of one public sampling algorithm in the public sampleability, we define two public sampling algorithms S_0 and S_1. According to the guess b^* of which distribution the challenge x is from, we adaptively choose the sampling algorithm S_{b^*} and get fresh samples. Following the strategy of [16], we can apply RD to such distinguishing problems and convert a successful distinguisher $\mathcal{A}$ between distributions $D_0(\Phi)$ and $D_1(\Phi)$ to a successful distinguisher $\mathcal{A}'$ between distribution $D_0(\Phi')$ and $D_1(\Phi')$ as long as the RD between Φ and Φ' is bounded by some polynomial. Furthermore, as an application, we can present a reduction from DLWE variants with error distributions of center binomial distribution and uniform distribution to the standard MLWE.

Second, we improve the classical reduction iterations of SLWE problem in [18] from polynomial to constant times. Recall the reduction of [18] is to solve a GapSVP problem using the SLWE oracle. Informally speaking, the reduction first perturbed a lattice point $\boldsymbol{v} \in \Lambda$, then called the closest vector problem (CVP) oracle R on the perturbed point and checked whether R could successfully recover $\boldsymbol{v}$. When the input is a NO instance, R can recover $\boldsymbol{v}$ successfully every time. When the input is a YES instance, $\boldsymbol{v}$ is statistically hidden and R may guess incorrectly with some non-negligible probability. According to such strategy, we apply RD on the YES instances instead of statistical distance and can improve the estimation of the accepting probability in the reduction to a constant. Though our statement is same as [18], our optimization is inspiring to the security guarantee since we can reduce the worst-case lattice problems to SLWE more efficiently.

Third, as an independent interest, inspired by [16], we explore the relation between search problems and decision problems and define a "hidden search problem for $\mathcal{A}$" in every decision problem with distinguisher $\mathcal{A}$. We can link the distinguisher's advantage with the distributions' randomness. In fact, if there are two distributions $D_0(r)$ and $D_1(r)$ distinguished by an adversary $\mathcal{A}$, then we claim there are many bad r bringing such difference of two distributions and an algorithm can be constructed to extract such a bad randomness. Thus, we can convert a successful distinguisher to a solver of hidden search problem. Owing to the compatible application of RD on search problems, such connection between decision problems and search problems indicates the feasibility of RD on decision problems. However, since r may be secret information and such calculation is not trivial, it is still a challenge to analyze RD on decision problems.

1.2 Related work

Takashima and Takayasu [19] tightened the security proof by adaptively choosing the order of RD. Bogdanov et al. [17] proved the noise flooding technique was possible with polynomial modulus by exploiting RD. Recently, Prest [20] applied RD to get tight bounds for distributions that are tailcut or with a bounded relative error, and made an optimization on Gaussian sampling and rejection sampling in BLISS signature scheme [21].

2 Preliminary

Denote the real numbers by $\mathbb{R}$ and integers by $\mathbb{Z}$. For any real number $x \in \mathbb{R}$, let $\lfloor x \rceil$ denote the nearest integer close to x. Denote column vectors over $\mathbb{R}$ with lower-case bold letters (e.g., $\boldsymbol{x}$), and matrices by upper-case bold letters (e.g., $\boldsymbol{A}$). Denote the matrix $[\boldsymbol{A}_1|\boldsymbol{A}_2]$ as the concatenation of the matrix $\boldsymbol{A}_1$ and $\boldsymbol{A}_2$. If S is a set, write $s \leftarrow S$ to denote sampling randomly s from uniform distribution over S. If S is a distribution, write $s \leftarrow S$ to denote sampling s from distribution S. If S is a random algorithm, write $s \leftarrow S$ to denote s is an output of S. A function $\mathrm{negl}(n) : \mathbb{R}_{\geqslant 0} \rightarrow \mathbb{R}_{\geqslant 0}$ is negligible if for arbitrary polynomial $\mathrm{poly}(n)$, sufficiently large n, $\mathrm{negl}(n) < 1/\mathrm{poly}(n)$.

The centered binomial distribution S_η for some positive integer η is defined as follows:

$$\text{Sample } (a_1, \ldots, a_\eta, b_1, \ldots, b_\eta) \leftarrow \{0,1\}^{2\eta} \text{ and output} \sum_{i=1}^{\eta}(a_i - b_i).$$

The statistical distance between two random variables X and Y over a countable set D is denoted as $\Delta(X,Y) = \frac{1}{2}\sum_{w\in D} |\Pr[X = w] - \Pr[Y = w]|$. Let λ denote a security parameter and $\{X_\lambda\}$, $\{Y_\lambda\}$ be ensembles of random variables, we say that $\{X_\lambda\}$ and $\{Y_\lambda\}$ are statistically close if $\Delta(X_\lambda, Y_\lambda)$ is negligible function of λ.

2.1 Lattices and Gaussian measures

In this subsection, we review some facts regarding lattices and Gaussian measures.

Lattices and module lattices. An n-dimension (full-rank) lattice $\Lambda \subseteq \mathbb{R}^n$ is a set of all integer linear combinations of some set of independent basis vectors $\boldsymbol{B} = \{\boldsymbol{b}_1, \ldots, \boldsymbol{b}_n\} \subseteq \mathbb{R}^n$, $\Lambda = \mathcal{L}(\boldsymbol{B}) = \{\sum_{i=1}^n z_i \boldsymbol{b}_i : z_i \in \mathbb{Z}\}$. The minimum distance $\lambda_1(\Lambda)$ of Λ is the length of its shortest nonzero vector: $\lambda_1(\Lambda) = \min_{\boldsymbol{0}\neq\boldsymbol{x}\in\Lambda} \|\boldsymbol{x}\|$. The dual lattice of $\Lambda \subseteq \mathbb{R}^n$ is defined as $\Lambda^* = \{\boldsymbol{x} \in \mathbb{R}^n : \langle \Lambda, \boldsymbol{x}\rangle \subseteq \mathbb{Z}\}$. For integers $n \geqslant 1$, modulus $q \geqslant 2$ and $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$, an m-dimensional lattice is defined as $\Lambda^\perp(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{0} \in \mathbb{Z}_q^n\} \subseteq \mathbb{Z}^m$. For any $\boldsymbol{y}$ in the subgroup of $\mathbb{Z}_q^n$, we also define the coset $\Lambda_{\boldsymbol{y}}^\perp(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{x} = \boldsymbol{y} \mod q\} = \Lambda^\perp(\boldsymbol{A}) + \bar{\boldsymbol{x}}$, where $\bar{\boldsymbol{x}} \in \mathbb{Z}^m$ is an arbitrary solution to $\boldsymbol{A}\bar{\boldsymbol{x}} = \boldsymbol{y}$. For a lattice $\Lambda = \mathcal{L}(\boldsymbol{B})$, let $\widetilde{\boldsymbol{B}}$ denote the Gram-Schmidt orthogonalization of $\boldsymbol{B}$, and $\|\widetilde{\boldsymbol{B}}\|$ is the length of the longest vector in it.

We consider the ring $\mathcal{R} = \mathbb{Z}[x]/(x^n + 1)$ for n a power of 2 and $\mathcal{R}_q = \mathbb{Z}_q[x]/(x^n + 1)$ for q a power of 3. Each element of $\mathcal{R}$ has a polynomial representation of degree $n - 1$ with coefficients in $\mathbb{Z}$. There is a coefficient embedding : $\mathcal{R} \rightarrow \mathbb{Z}^n$, mapping $\phi(\boldsymbol{a}) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in \mathcal{R} \mapsto (a_0, a_1, \ldots, a_{n-1})^t \in \mathbb{Z}^n$. The l_2-norm and l_∞-norm of $\boldsymbol{a}$ are defined as $\|\boldsymbol{a}\| = \sqrt{\sum_i |a_i|^2}$ and $\|\boldsymbol{a}\|_\infty = \max_i |a_i|$ for $\boldsymbol{a} \in \mathcal{R}$ respectively. Besides, we can also view $\mathcal{R}$ as the subring of anti-circulant matrices in $\mathbb{Z}^{n\times n}$ by regarding the element $\boldsymbol{a} \in \mathcal{R}$ as $\mathrm{rot}(\boldsymbol{a}) = [\phi(\boldsymbol{a})|\cdots|\phi(\boldsymbol{a}\boldsymbol{x}^{i-1})|\cdots|\phi(\boldsymbol{a}\boldsymbol{x}^{n-1})]$. If module M is an $\mathcal{R}$-module with rank d, the dimension of corresponding module lattice is dn. For $\forall \boldsymbol{x} = (\boldsymbol{x}_1, \ldots, \boldsymbol{x}_d) \in \mathcal{R}^{1\times d}$, $\mathrm{rot}(\boldsymbol{x}) = [\mathrm{rot}(\boldsymbol{x}_1)|\cdots|\mathrm{rot}(\boldsymbol{x}_d)] \in \mathbb{Z}^{n\times dn}$.

Gaussian measures. Let Λ be a lattice in $\mathbb{Z}^n$. For any vector $\boldsymbol{c} \in \mathbb{R}^n$ and parameter $r > 0$, the n-dimensional Gaussian function $\rho_{r,\boldsymbol{c}} : \mathbb{R}^n \rightarrow (0, 1]$ is defined as $\rho_{r,\boldsymbol{c}}(\boldsymbol{x}) := \exp(-\pi\|\boldsymbol{x} - \boldsymbol{c}\|^2/r^2)$. The discrete Gaussian distribution over Λ with parameter r and center $\boldsymbol{c}$ (abbreviated as $D_{\Lambda,r,\boldsymbol{c}}$) is defined as $\forall \boldsymbol{y} \in \Lambda, D_{\Lambda,r,\boldsymbol{c}}(\boldsymbol{y}) := \frac{\rho_{r,\boldsymbol{c}}(\boldsymbol{y})}{\rho_{r,\boldsymbol{c}}(\Lambda)}$, where $\rho_{r,\boldsymbol{c}}(\Lambda) = \sum_{\boldsymbol{y}\in\Lambda} \rho_{r,\boldsymbol{c}}(\boldsymbol{y})$. When $\boldsymbol{c} = \boldsymbol{0}$, we write $D_{\Lambda,r}$ for short.

Definition 1 ([22])**.** For a lattice Λ and a positive real $\varepsilon > 0$, the smoothing parameter $\eta_\varepsilon(\Lambda)$ is the smallest real $r > 0$ such that $\rho_{1/r}(\Lambda^* \backslash \{\mathbf{0}\}) \leqslant \varepsilon$.

Lemma 1 ([22])**.** For any n-dimensional lattice Λ, we have $\eta_{2^{-n}} \leqslant \frac{\sqrt{n}}{\lambda_1(\Lambda^*)}$.

2.2 Learning with errors assumption

The LWE problem is at least as hard as several lattice problems in the worst case. There are continuous version and discrete version of definitions used in the literature. In this paper, we choose the LWE definition adaptively for convenience.

Plain LWE. For continuous version of LWE, we define the following distribution $A_{\boldsymbol{s},\chi}$, where χ is a distribution over $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and $\boldsymbol{s} \in \mathbb{Z}_q^n$. A sample from the distribution $A_{\boldsymbol{s},\chi}$ is of the form $(\boldsymbol{a}, b) \in \mathbb{Z}_q^n \times \mathbb{T}$ with $b = \frac{\langle \boldsymbol{a},\boldsymbol{s}\rangle}{q} + e \mod 1$, where $\boldsymbol{a}$ is chosen from $\mathbb{Z}_q^n$ uniformly and e is chosen from the distribution χ.

Definition 2 (Continuous version)**.** Let χ be a distribution over $\mathbb{T}$, an integer modulo $q \geqslant 2$. The search version of LWE, denoted as $\mathrm{SLWE}_{n,q,\chi}$, is given m samples from the distribution $A_{\boldsymbol{s},\chi}$ and recover $\boldsymbol{s}$. The decision version of LWE, denoted as $\mathrm{DLWE}_{n,q,\chi}$, is given m pairs of $(\boldsymbol{a}', b') \in \mathbb{Z}_q^n \times \mathbb{T}$ and decide these pairs are from the uniform distribution or $A_{\boldsymbol{s},\chi}$.

Another discrete form of DLWE defined in $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n$ is also common in use, which is equivalent to the continuous version.

Definition 3 (Discrete version)**.** For security parameter λ, let $n = n(\lambda)$ be an integer dimension, let $q = q(\lambda) \geqslant 2$ be an integer, and let $\chi = \chi(\lambda)$ be a distribution over $\mathbb{Z}$. The $\mathrm{DLWE}_{n,q,\chi}$ problem is to distinguish the following two distributions:

$$\{\boldsymbol{A}, \boldsymbol{A}^t\boldsymbol{s} + \boldsymbol{x}\} \text{ and } \{\boldsymbol{A}, \boldsymbol{u}\},$$

where $\boldsymbol{A} \leftarrow \mathbb{Z}_q^{n\times m}$, $\boldsymbol{s} \leftarrow \mathbb{Z}_q^n$, $\boldsymbol{u} \leftarrow \mathbb{Z}_q^m$, and $\boldsymbol{x} \leftarrow \chi^m$.

Corollary 1 ([1, 7, 18, 23, 24])**.** Let $q = q(n)$ be either a prime power $q = p^r$, or a product of co-prime numbers $q = \prod q_i$ such that for all i, $q_i = \mathrm{poly}(n)$, and let $\alpha q \geqslant \sqrt{n}$. If there is an efficient algorithm that solves the (average-case) $\mathrm{DLWE}_{n,q,\alpha}$ problem, then:

- There is an efficient quantum algorithm that solves $\mathrm{GapSVP}_{\widetilde{O}(n/\alpha)}$ (and $\mathrm{SIVP}_{\widetilde{O}(n/\alpha)}$) on any n-dimensional lattice;
- If in addition $q \geqslant \widetilde{O}(2^{n/2})$, there is an efficient classical algorithm for $\mathrm{GapSVP}_{\widetilde{O}(n/\alpha)}$ on any n-dimensional lattice.

Module-LWE. The MLWE is a generalization of the plain LWE and RLWE, whose security is studied in [3]. The MLWE distribution over $\mathcal{R}_q^l \times \mathcal{R}_q$ is the distribution of $(\boldsymbol{a}, \boldsymbol{b})$, where $\boldsymbol{a} \in \mathcal{R}_q^l$ and $\boldsymbol{b} = \boldsymbol{a}^t\boldsymbol{s} + \boldsymbol{e}$ with $\boldsymbol{s} \leftarrow \mathcal{R}_q^l$ and $\boldsymbol{e}$ is sampled from the distribution Ψ. Akin to its counterpart — plain LWE, there are search version and decision version of MLWE problem (denoted as $\mathrm{MLWE}_{n,l,q}(\Psi)$), which are defined as follows.

M-SLWE problem. To find the secret $\boldsymbol{s}$ given the polynomial MLWE samples.

M-DLWE problem. To distinguish the MLWE distribution from uniform distribution $U(\mathcal{R}_q^l \times \mathcal{R}_q)$.

Without confusion, we also denote $\mathrm{MLWE}_{n,m,q}(\Psi)$ as each coefficient of error from distribution Ψ below.

Corollary 2 ([3], Theorem 4.7)**.** Let ε be a negligible function, $\alpha \in (0, 1)$ and $q \geqslant 2$ of known factorization such that $\alpha q > 2\sqrt{l} \cdot \omega(\sqrt{\log n})$. There is a quantum reduction from solving Mod-$\mathrm{GIVP}_\gamma^{\eta_\varepsilon}$ in polynomial time (in the worst case, with high probability) to solving $\text{M-SLWE}_{q,\Psi_{\leqslant\alpha}}$ in polynomial time with non-negligible advantage with $\gamma = \sqrt{8n^2d} \cdot \omega(\sqrt{\log n})/\alpha$.

Assume that q is prime, $q \leqslant \mathrm{poly}(nl)$ and that $q = 1 \mod 2n$. Then there exists a polynomial time reduction from $\text{M-SLWE}_{q,\Psi_{\leqslant\alpha}}$ to $\text{M-DLWE}_{q,\Upsilon_\alpha}$.

2.3 Decision problems and Rényi divergence

In this subsection, we review some useful results of decision problems and RD.

Decision problems. Let Φ, Φ' denote two distributions with $\mathsf{Supp}(\Phi) \subseteq \mathsf{Supp}(\Phi')$, and $D_0(r)$ and $D_1(r)$ denote two distributions determined by some parameter $r \in \mathsf{Supp}(\Phi')$. In this paper, we call r as the randomness and define two decision problems P, P' as follows.

- Problem P. Distinguish whether the input x is sampled from distribution X_0 or X_1, where

$$X_0 = \{x : r \leftarrow \Phi, x \leftarrow D_0(r)\}, \quad X_1 = \{x : r \leftarrow \Phi, x \leftarrow D_1(r)\}.$$

- Problem P'. Distinguish whether the input x is sampled from distribution X_0' or X_1', where

$$X_0' = \{x : r \leftarrow \Phi', x \leftarrow D_0(r)\}, \quad X_1' = \{x : r \leftarrow \Phi', x \leftarrow D_1(r)\}.$$

In general, a successful algorithm $\mathcal{A}$ solving the problem P with a non-negligible advantage $\frac{1}{\mathrm{poly}(n)}$ satisfies $\mathrm{Adv}(\mathcal{A}) = |\Pr[\mathcal{A}(x) = 1|x \leftarrow X_1] - \Pr[\mathcal{A}(x) = 1|x \leftarrow X_0]| \geqslant \frac{1}{\mathrm{poly}(n)}$, where the probability is taken over the choice of x and the randomness of $\mathcal{A}$. Given $r \leftarrow \Phi$ (resp. Φ'), denote $p_0(r)$ and $p_1(r)$ as the (conditional) acceptance probabilities of $\mathcal{A}$ given the input samples from $D_0(r)$ and $D_1(r)$, i.e.,

$$p_0(r) = \Pr[\mathcal{A}(x) = 1|x \leftarrow D_0(r)], \quad p_1(r) = \Pr[\mathcal{A}(x) = 1|x \leftarrow D_1(r)].$$

Rényi divergence. For two distributions P and Q such that $\mathsf{Supp}(P) \subseteq \mathsf{Supp}(Q)$, the Rényi divergence of order a between P and Q is defined as $R_a(P||Q) = (\sum_{x \in \mathsf{Supp}(P)} \frac{P(x)^a}{Q(x)^{a-1}})^{\frac{1}{a-1}}$[3], where $a \in (1, +\infty)$. When $a = 1$, the Rényi divergence is defined as $R_1(P||Q) = \exp(\sum_{x \in \mathsf{Supp}(P)} P(x) \log \frac{P(x)}{Q(x)})$. When $a = +\infty$, the Renyi divergence is defined as $R_\infty(P||Q) = \max_{x \in \mathsf{Supp}(P)} \frac{P(x)}{Q(x)}$.

Lemma 2. Let P and Q be two distributions satisfying $\mathsf{Supp}(P) \subseteq \mathsf{Supp}(Q)$, then for all $a \in [1, +\infty]$, the following holds:

- Logarithm positivity. $R_a(P||Q) \geqslant R_a(P||P) = 1$.
- Data processing inequality. For any function f, denote P^f (resp. Q^f) the distribution by applying the function f to the distribution P (resp. Q). That is $P^f(y) = \sum_{f(x)=y} P(x)$. Then we have for any $a \in [1, +\infty]$, $R_a(P^f||Q^f) \leqslant R_a(P||Q)$.
- Probability preservation. Let $A \subseteq \mathsf{Supp}(P)$ denote an arbitrary event. Then for any $a \in (1, +\infty)$, $Q(A) \cdot R_a(P||Q) \geqslant P(A)^{\frac{a}{a-1}}$. Moreover, we have $Q(A) \cdot R_\infty(P||Q) \geqslant P(A)$.
- Multiplicativity. Suppose P and Q are distributions over the pair (X_1, X_2). Let P_i (resp. Q_i) be the distribution of X_i under P (resp. Q), $i = 1, 2$, and let $P_{2|1}(\cdot|x_1)$ (resp. $Q_{2|1}(\cdot|x_1)$) denote the conditional distribution given the condition that $X_1 = x_1$. Then we have
  - $R_a(P||Q) = R_a(P_1||Q_1) \cdot R_a(P_2||Q_2)$, if X_1, X_2 are independent;
  - $R_a(P||Q) \leqslant R_\infty(P_1||Q_1) \cdot \max_{x_1} R_a(P_{2|1}(\cdot|x_1)||Q_{2|1}(\cdot|x_1))$.

When applying the Rényi divergence on the decision problem of distributions D_0 and D_1, the public sampleability property was considered in [16].

Lemma 3 ([16], Theorem 4.1)**.** Assume that $D_0(\cdot)$ and $D_1(\cdot)$ satisfy the following public sampleability property: there exists a sampling algorithm S with run-time T_S such that for all (r, b), given any sample x from $D_b(r)$:

- $S(0, x)$ outputs a fresh sample distributed as $D_0(r)$ over the randomness of S;
- $S(1, x)$ outputs a fresh sample distributed as $D_1(r)$ over the randomness of S.

Then, given a T-time distinguisher $\mathcal{A}$ for Problem P with advantage ϵ, we can construct a distinguisher $\mathcal{A}'$ for problem P' with run-time and distinguishing advantage respectively bounded from above and below by $O(\frac{1}{\epsilon^2} \log(\frac{R_a(\Phi\|\Phi')}{\epsilon^{a/(a-1)}}) \cdot (T_S + T))$ and $\frac{\epsilon}{4 \cdot R_a(\Phi\|\Phi')} \cdot (\frac{\epsilon}{2})^{\frac{a}{a-1}}$ for any $a \in (1, +\infty]$.

3 Rényi divergence on decision LWE

In this section, we focus on the security of DLWE variants with different error distributions using the analysis of RD. We first introduce a general tool — adaptively public sampling property, broadening the applications of RD on distinguishing problems. Then, as an application, we apply it to our DLWE variants.

[3] Our definition of RD is the exponential of the classical definition [25].

3.1 Adaptively public sampling property

Following the strategy of [16], the high level idea of adaptively public sampling property is to allow an adversary to get fresh samples from distributions D_0 and D_1 with some failure, which only makes negligible impact on the advantage of the decision problem. Concretely, instead of deriving new samples from $D_0(r)$ and $D_1(r)$ with probability 1 as [16], given the challenge $x \leftarrow D_b(r)$ for all (r, b), we define two public sampling algorithms S_0 and S_1 and choose the sampling algorithm S_b adaptively according to the guess of $b \in \{0, 1\}$, which makes the adversary get the fresh samples correctly with probability $\frac{1}{2}$.

Definition 4 (Adaptively public sampling property)**.** We say two distributions $D_0(r)$ and $D_1(r)$ satisfying the adaptively public sampling property, if there exist two probabilistic polynomial time (PPT) sampling algorithms S_0 and S_1 such that for all r, given any sample x from $D_b(r)$:

- For algorithm S_0, it satisfies the following properties:

When $x \leftarrow D_0(r)$, we have

- $S_0(0, x)$ outputs a fresh sample distributed as $\widetilde{D}_0(r)$ over the randomness of S_0;
- $S_0(1, x)$ outputs a fresh sample distributed as $\widetilde{D}_1(r)$ over the randomness of S_0.

When $x \leftarrow D_1(r)$, we have

- $S_0(0, x)$ outputs a fresh sample distributed as U_1 over the randomness of S_0;
- $S_0(1, x)$ outputs a fresh sample distributed as U_2 over the randomness of S_0.

- For algorithm S_1, it satisfies the following properties:

When $x \leftarrow D_0(r)$, we have

- $S_1(0, x)$ outputs a fresh sample distributed as U_3 over the randomness of S_1;
- $S_1(1, x)$ outputs a fresh sample distributed as U_4 over the randomness of S_1.

When $x \leftarrow D_1(r)$, we have

- $S_1(0, x)$ outputs a fresh sample distributed as $\widetilde{D}_0(r)$ over the randomness of S_1;
- $S_1(1, x)$ outputs a fresh sample distributed as $\widetilde{D}_1(r)$ over the randomness of S_1.

For any r, it satisfies $\Delta(D_i, \widetilde{D}_i) < \epsilon_1$ and $\Delta(U_j, U_{j+1}) < \epsilon_1$ with negligible function ϵ_1 for $\forall i \in \{0, 1\}$ and $\forall j \in \{1, 3\}$. The distributions U_1 and U_2 are independent from r, so are U_3 and U_4. Besides, it is hard to distinguish distribution $\widetilde{D}_0$ and U_1 (resp. $\widetilde{D}_0$ and U_3), $\widetilde{D}_1$ and U_2 (resp. $\widetilde{D}_1$ and U_4)[4].

Remark 1. From the definition, our adaptively public sampling property is incompatible with the public sampleability property of [16]. For example, considering the LWE problem $D_0(r) = (\boldsymbol{A}, \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e})$ and $D_1(r) = (\boldsymbol{A}, \boldsymbol{u})$ with randomness $\boldsymbol{A}$, it is easy to verify that satisfies the public sampleability property of [16]. However, it is a bit tricky to satisfy the adaptively public sampling property, unless some constraints are needed as in Theorem 2[5].

On the other hand, when considering LWE problem with error term as randomness, i.e., $D_0(\boldsymbol{e}) = (\boldsymbol{a}, \boldsymbol{b} = \boldsymbol{a}\boldsymbol{s} + \boldsymbol{e})$ with $\boldsymbol{a} \leftarrow \mathcal{R}_q^{1\times m}$, $\boldsymbol{s} \leftarrow \mathcal{R}_q^m$, $D_1(\boldsymbol{e}) = (\boldsymbol{a}, \boldsymbol{u})$ with $\boldsymbol{a} \leftarrow \mathcal{R}_q^{1\times m}$ and $\boldsymbol{u} \leftarrow \mathcal{R}_q$, it is easy to verify the adaptively public sampling property, but hard to verify the public sampleability property. Detailed analysis is mentioned in the introduction and Theorem 2.

Theorem 1. For decision problems P and P', assume that $D_0(\cdot)$ and $D_1(\cdot)$ satisfy the adaptively public sampling property. Then, given a T-time PPT distinguisher $\mathcal{A}$ for problem P with advantage ϵ, we can construct a PPT distinguisher $\mathcal{A}'$ for problem P' with advantage bounded by $\frac{\epsilon}{8\cdot R_a(\Phi\|\Phi')} \cdot (\frac{\epsilon}{8})^{\frac{a}{a-1}} - \frac{1}{2}\epsilon_1$ for any $a \in (1, +\infty]$ with running time at most $O(\frac{1}{\epsilon^2}\log(\frac{R_a(\Phi\|\Phi')}{\epsilon^{\frac{a}{a-1}+1}})(T_S + T))$ where T_S is the upper bound of running time of S_0 and S_1.

Proof. Our proof follows the strategy of [16]. An input x sampled from $D_b(r)$ for some $r \leftarrow \Phi'$ and some unknown $b \in \{0, 1\}$ is given to the distinguisher $\mathcal{A}'$. Denote the output of $\mathcal{A}'$ as the guess of the

[4] This condition is merely to exclude the trivial decision problems. Take $S_0(0, x)$ as an example. Notice that output distribution of $S_0(0, x)$ is either $\widetilde{D}_0(r)$ or U_1 according to the distribution of x. If $\widetilde{D}_0(r)$ and U_1 can be distinguished easily for any r, then $S_0(0, x)$ can distinguish $D_0(r)$ and $D_1(r)$ trivially, which means $S_0(0, x)$ is a trivial distinguisher between $D_0(r)$ and $D_1(r)$ for arbitrary r.

[5] Such D_0 and D_1 satisfy the adaptively public sampling property under the condition of Theorem 2. The public sampling algorithms S_0 and S_1 are defined the same as in Theorem 2.

distribution of x. Then the probability of a successful guess on x is $\frac{1}{2}\Pr[\mathcal{A}'(x)=1|x\leftarrow D_1]+\frac{1}{2}\Pr[\mathcal{A}'(x)=0|x\leftarrow D_0]$.

At first, $\mathcal{A}'$ samples a random coin $b^*\in\{0,1\}$ as the guess of b, and then calls the sampling algorithm S_{b^*} on $(0,x)$ and $(1,x)$. It runs the distinguisher $\mathcal{A}$ on $N=O(\epsilon^{-2}\log(1/\epsilon'))$[6] independent inputs ($\epsilon'$ is defined later) from $S_{b^*}(0,x)$ and $S_{b^*}(1,x)$ and obtains the estimates $\hat{p}_0$ and $\hat{p}_1$ for the acceptance probabilities $p'_0(r)$ and $p'_1(r)$, where $p'_0(r)$ and $p'_1(r)$ are defined as follows:

$$p'_0(r)=\Pr[\mathcal{A}(y)=1|y\leftarrow S_{b^*}(0,x)],\quad p'_1(r)=\Pr[\mathcal{A}(y)=1|y\leftarrow S_{b^*}(1,x)].$$

By the Hoeffding bound, the estimation errors $|\hat{p}_0-p'_0|<\frac{\epsilon}{8}$ and $|\hat{p}_1-p'_1|<\frac{\epsilon}{8}$ hold at most except the probability of ϵ'. Now $\mathcal{A}'$ runs $\mathcal{A}$ as a subroutine and proceeds as follows:

```
if $\hat{p}_1-\hat{p}_0>\frac{\epsilon}{4}+\epsilon_1$
    Output $\mathcal{A}(x)$;
else
    Output a uniformly random bit.
```

Let $p_0(r)$ and $p_1(r)$ denote the acceptance probabilities of $\mathcal{A}$ given the input samples but from $D_0(r)$ and $D_1(r)$, i.e., $p_0(r)=\Pr[\mathcal{A}(x)=1|x\leftarrow D_0(r)]$, $p_1(r)=\Pr[\mathcal{A}(x)=1|x\leftarrow D_1(r)]$.

Assuming $\Pr[\mathcal{A}'(x)=1|x\leftarrow D_1]-\Pr[\mathcal{A}'(x)=1|x\leftarrow D_0]>0$, we analyse the advantage of the distinguisher $\mathcal{A}'$ in two cases.

Case 1. If $\mathcal{A}'$ guesses the value of b correctly, i.e., $b^*=b$, it obtains samples from $\widetilde{D}_0(r)$ and $\widetilde{D}_1(r)$. Then we have

$$p'_0(r)=\Pr[\mathcal{A}(y)=1|y\leftarrow\widetilde{D}_0(r)],\quad p'_1(r)=\Pr[\mathcal{A}(y)=1|y\leftarrow\widetilde{D}_1(r)].$$

Since $\Delta(D_0,\widetilde{D}_0)<\epsilon_1$ and $\Delta(D_1,\widetilde{D}_1)<\epsilon_1$, it follows $|p_0-p'_0|<\epsilon_1$ and $|p_1-p'_1|<\epsilon_1$. Hence, $|\hat{p}_0-p_0|<\frac{\epsilon}{8}+\epsilon_1$ and $|\hat{p}_1-p_1|<\frac{\epsilon}{8}+\epsilon_1$ hold by the triangle inequality, except with the probability ϵ' over the randomness of public sampling algorithm S_{b^*}.

Let $\mathcal{S}'_1=\{r|p_1(r)-p_0(r)\geqslant\frac{\epsilon}{2}+3\epsilon_1\}$, $\mathcal{S}'_2=\{r|-\epsilon_1\leqslant p_1(r)-p_0(r)<\frac{\epsilon}{2}+3\epsilon_1\}$ and $\mathcal{S}'_3=\{r|p_1(r)-p_0(r)<-\epsilon_1\}$. Then:

- If $r\in\mathcal{S}'_1$, we have $\hat{p}_1-\hat{p}_0>\frac{\epsilon}{4}+\epsilon_1$, except with the probability ϵ' over the randomness of S_{b^*}. Therefore, the distinguisher $\mathcal{A}'$ outputs $\mathcal{A}(x)$. Hence, for $b=1$, we have $\Pr[\mathcal{A}'(x)=1|r\in\mathcal{S}'_1]\geqslant\Pr[\mathcal{A}(x)=1|r\in\mathcal{S}'_1]\geqslant(1-\epsilon')p_1(r)\geqslant p_1(r)-\epsilon'$, and for $b=0$, we have $\Pr[\mathcal{A}'(x)=1|r\in\mathcal{S}'_1]=(1-\epsilon')\cdot p_0(r)+\frac{1}{2}\epsilon'\leqslant p_0(r)+\epsilon'$.
- If $r\in\mathcal{S}'_2$, let $u(r)$ denote the probability that $\hat{p}_1-\hat{p}_0>\frac{\epsilon}{4}+\epsilon_1$ over the randomness of S_{b^*}. Then $\mathcal{A}'$ will output what $\mathcal{A}$ returns with probability $u(r)$ and a uniform bit with probability $1-u(r)$. Hence, for $b=1$, we have $\Pr[\mathcal{A}'(x)=1|r\in\mathcal{S}'_2]=u(r)p_1(r)+\frac{1-u(r)}{2}$, and for $b=0$, we have $\Pr[\mathcal{A}'(x)=1|r\in\mathcal{S}'_2]=u(r)p_0(r)+\frac{1-u(r)}{2}$.
- If $r\in\mathcal{S}'_3$, we have $\hat{p}_1-\hat{p}_0<\frac{\epsilon}{4}+\epsilon_1$, except with the probability ϵ' over the randomness of S_{b^*}, and $\mathcal{A}'$ will output a uniform bit. Thus for $b=1$, we have $\Pr[\mathcal{A}'(x)=1|r\in\mathcal{S}'_3]\geqslant(1-\epsilon')\frac{1}{2}\geqslant\frac{1}{2}-\epsilon'$, while for $b=0$, $\Pr[\mathcal{A}'(x)=1|r\in\mathcal{S}'_3]\leqslant(1-\epsilon')\frac{1}{2}+\epsilon'\cdot p_0(r)\leqslant\frac{1}{2}+\epsilon'$.

When $b^*=b$, the advantage $\mathrm{Adv}(\mathcal{A}')$ is as follows:

$$\mathrm{Adv}^{b^*=b}(\mathcal{A}')=\sum_r\{\Phi'(r)(\Pr[\mathcal{A}'(x)=1|x\leftarrow D_1(r),b^*=b]-\Pr[\mathcal{A}'(x)=1|x\leftarrow D_0(r),b^*=b])\}\tag{1}$$

$$\geqslant\sum_{r\in\mathcal{S}'_1}\Phi'(r)(p_1(r)-p_0(r)-2\epsilon')+\sum_{r\in\mathcal{S}'_2}\Phi'(r)u(r)(p_1(r)-p_0(r))-\sum_{r\in\mathcal{S}'_3}\Phi'(r)2\epsilon'\tag{2}$$

$$\geqslant\left(\Phi'(\mathcal{S}'_1)\cdot\frac{\epsilon}{2}+\sum_{r\in\mathcal{S}'_2}\Phi'(r)u(r)\cdot(-\epsilon_1)-2\epsilon'\right)\geqslant\Phi'(\mathcal{S}'_1)\cdot\frac{\epsilon}{2}-\epsilon_1-2\epsilon'.\tag{3}$$

[6] Concretely, $\epsilon'=2\exp(-2N(\frac{\epsilon}{8})^2)$ from the Hoeffding inequality and we get $N=32\epsilon^{-2}\log(2/\epsilon')$.

Case 2. If $\mathcal{A}'$ does not guess the distribution of x correctly, i.e., $b^* \neq b$, it obtains samples from U_i and U_{i+1}, for $i \in \{1,3\}$. Then we have

$$p_0'(r) = \Pr[\mathcal{A}(x) = 1 | x \leftarrow U_i], \quad p_1'(r) = \Pr[\mathcal{A}(x) = 1 | x \leftarrow U_{i+1}].$$

Since the distributions U_i and U_{i+1} are independent of the randomness r, $|p_0'(r) - p_1'(r)| \leqslant \Delta(U_i, U_{i+1}) < \epsilon_1$ satisfies for any r. It follows $|\hat{p}_1 - \hat{p}_0| < \frac{\epsilon}{4} + \epsilon_1$ except the probability ϵ'. Hence, $\mathcal{A}'$ output a uniform bit except the probability ϵ', otherwise $\mathcal{A}'$ returns what $\mathcal{A}$ outputs with probability ϵ'.

Let $\mathcal{S}_1'' = \{r | p_1(r) - p_0(r) \geqslant \frac{\epsilon}{2}\}$, $\mathcal{S}_2'' = \{r | 0 \leqslant p_1(r) - p_0(r) < \frac{\epsilon}{2}\}$ and $\mathcal{S}_3'' = \{r | p_1(r) - p_0(r) < 0\}$. Then, the advantage of $\mathcal{A}'$ is as follows:

$$\mathrm{Adv}^{b^* \neq b}(\mathcal{A}') = \sum_r \{\Phi'(r)(\Pr[\mathcal{A}'(x) = 1 | x \leftarrow D_1(r), b^* \neq b] - \Pr[\mathcal{A}'(x) = 1 | x \leftarrow D_0(r), b^* \neq b])\} \tag{4}$$

$$\geqslant \epsilon' \sum_r \Phi'(r)(p_1(r) - p_0(r)) \geqslant \epsilon' \sum_{r \in \Phi'(\mathcal{S}_3'')} \Phi'(r)(p_1(r) - p_0(r)) \geqslant \epsilon' \cdot (-\Phi'(\mathcal{S}_3'')) \geqslant -\epsilon'. \tag{5}$$

Combining the above two cases, the advantage of $\mathcal{A}'$ is as follows:

$$\mathrm{Adv}(\mathcal{A}') = \sum_r \{\Phi'(r)(\Pr[\mathcal{A}'(x) = 1 | x \leftarrow D_1(r)] - \Pr[\mathcal{A}'(x) = 1 | x \leftarrow D_0(r)])\} \tag{6}$$

$$= \Pr[b = b^*] \cdot \mathrm{Adv}^{b = b^*}(\mathcal{A}') + \Pr[b \neq b^*] \cdot \mathrm{Adv}^{b \neq b^*}(\mathcal{A}') \tag{7}$$

$$\geqslant \frac{1}{2}\Big(\Phi'(\mathcal{S}_1') \cdot \frac{\epsilon}{2} - \epsilon_1 - 3\epsilon'\Big). \tag{8}$$

We claim the set $\mathcal{S}_1'$ has the probability $\Phi(\mathcal{S}_1') \geqslant \frac{\epsilon}{8}$ under the distribution Φ by an averaging argument in Appendix A. By Lemma 2, $\Phi'(\mathcal{S}_1') \geqslant \frac{(\epsilon/8)^{\frac{a}{a-1}}}{R_a(\Phi \| \Phi')}$. Set $\epsilon' = (\epsilon/12) \cdot (\epsilon/8)^{\frac{a}{a-1}} / R_a(\Phi \| \Phi')$, then $\mathrm{Adv}(\mathcal{A}') \geqslant \frac{\epsilon}{8 \cdot R_a(\Phi \| \Phi')} \cdot (\frac{\epsilon}{8})^{\frac{a}{a-1}} - \frac{1}{2}\epsilon_1$.

Remark 2. Our property is a complement to the RD application on decision problems. It seems the public sampleability property is easy to be satisfied for distributions $D_0(r)$ and $D_1(r)$ with the publicly known r. However, when r is confidential, our adaptively public sampling property may be more applicable.

3.2 Application on DLWE

With adaptively public sampling property, we declare that MLWE with error from center binomial distribution or uniform distribution can be as hard as the standard MLWE.

We allow the access to the oracle $\mathcal{O}_x$ explicitly, which returns the instances from the same distribution of x. Concretely, if x is a uniform instance, $\mathcal{O}_x$ returns uniform instances. If x is an LWE instance with secret $\boldsymbol{s}$, $\mathcal{O}_x$ returns fresh LWE instances with the same secret $\boldsymbol{s}$. The following theorem shows that assuming the hardness of the standard MLWE problem with Gaussian error distribution D_α, the variant $\mathrm{MLWE}_{n,m,q}(\chi')$ with error distribution χ' is indistinguishable from the uniform distribution as long as $R_a(\chi' \| D_\alpha)$ is polynomially bounded.

Theorem 2. Let χ' and $\chi = D_{\mathcal{R},\alpha}$ be two error distributions over $\mathcal{R}$ with $\mathsf{Supp}(\chi') \subseteq \mathsf{Supp}(\chi)$. Let $\boldsymbol{a} \leftarrow \mathcal{R}_q^{1 \times m}$, $\boldsymbol{s} \leftarrow \mathcal{R}_q^{m \times 1}$, $m \geqslant 2\lceil \log_2 q \rceil + 2$ and $\alpha \geqslant \omega(\sqrt{\ln nm})$. Then, if there is a PPT distinguisher $\mathcal{A}$ against $\mathrm{MLWE}_{n,m,q}(\chi')$ with advantage ε, there exists a PPT distinguisher $\mathcal{A}'$ against the $\mathrm{MLWE}_{n,m,q}(\chi)$ with the access to oracle $\mathcal{O}_x$ with advantage $\Omega(\frac{\varepsilon^{1+a/(a-1)}}{R_a(\chi' \| \chi)})$ and running time $O(\frac{1}{\epsilon^2} \log(\frac{R_a(\Phi \| \Phi')}{\epsilon^{\frac{a}{a-1}+1}})(T_S + T))$ where T_S is the upper bound of running time of S_0 and S_1, for any $a \in (1, +\infty]$.

In the proof of Theorem 2, it suffices to verify the adaptively public sampling property. Thus, we postpone it in Appendix B.

Corollary 3. Let ϕ be a center binomial distribution, $m \geqslant 2\lceil \log_2 q \rceil + 2$ and $\alpha \geqslant \omega(\sqrt{\ln nm})$. If $R(\phi \| D_{\mathcal{R},\alpha})$ is bounded by some polynomial, then there is a polynomial-time reduction from $\mathrm{MLWE}_{n,m,q}(D_{\mathcal{R},\alpha})$ to $\mathrm{MLWE}_{n,m,q}(\phi)$.

In particular, when the error distribution is uniform distribution in a small interval, we can argue the hardness of MLWE with uniform noise, which can be viewed as an adaptation of Theorem 5.1 in [16] to the module setting.

Corollary 4. Let $m \geqslant 2\lceil \log_2 q \rceil + 2$, $\alpha \geqslant \omega(\sqrt{\ln nm})$ and $\alpha, \beta > 0$ be real numbers with $\beta = \Omega(n\alpha/\log n)$ for positive integers n. Then there is a polynomial-time reduction from $\mathrm{MLWE}_{n,m,q}(D_{\mathcal{R},\alpha})$ to $\mathrm{MLWE}_{n,m,q}(\bar{U}_\beta)$, where $\bar{U}_\beta = \frac{1}{q}\lfloor qU_\beta \rceil$ and U_β is a continuous uniform distribution over $[-\beta, \beta]$.

The proof is similar as Theorem 5.1 in [16] but with RD on decision problems directly, and we put details in Appendix C.

4 Rényi divergence on search LWE

In this section, we improve the classical reduction proof of SLWE in [18]. Our proof strategy is almost the same as [18] but with a different analysis on YES instances using RD. Rather than polynomial times in [18], such crucial analysis results in the constant iterations in the proof.

Definition 5 ([18], Definition 2.5)**.** For functions $\zeta(n) \geqslant \gamma(n) \geqslant 1$, an input to $\mathrm{GapSVP}_{\zeta,\gamma}$ is a pair $(\boldsymbol{B}, d)$, where

- $\boldsymbol{B}$ is a basis of an n-dimensional lattice $\Lambda = \mathcal{L}(\boldsymbol{B})$ for which $\lambda_1(\Lambda) \leqslant \zeta(n)$,
- $\min_i \|\widetilde{\boldsymbol{b}}_i\| \geqslant 1$, and
- $1 \leqslant d \leqslant \frac{\zeta(n)}{\gamma(n)}$.

It is a YES instance if $\lambda_1(\Lambda) \leqslant d$, and a NO instance if $\lambda_1(\Lambda) > \gamma(n) \cdot d$.

Theorem 3. Let $\alpha = \alpha(n) \in (0, 1)$ be a real number and $\gamma = \gamma(n) \geqslant n/(\alpha\sqrt{\log n})$. Let $\zeta = \zeta(n) \geqslant \gamma$ and $q = q(n) \geqslant (\zeta/\sqrt{n}) \cdot \omega(\sqrt{\log n})$. There is a PPT reduction from solving $\mathrm{GapSVP}_{\zeta,\gamma}$ to solving $\mathrm{SLWE}_{n,q,\Phi_\alpha}$ using polynomial samples. Furthermore, the iteration of reduction algorithm is expected to be four times.

Proof. The input $(\boldsymbol{B}, d)$ as an instance of $\mathrm{GapSVP}_{\zeta,\gamma}$ has the properties: $\min\|\widetilde{\boldsymbol{b}}_i\| \geqslant 1$, $\lambda_1(\mathcal{L}(\boldsymbol{B})) \leqslant \zeta$ and $1 \leqslant d \leqslant \zeta/\gamma$. The reduction runs the following procedure four times.

- Sample a point $\boldsymbol{w}$ uniformly at random from the ball $d' \cdot \mathcal{B}_n$, where $\mathcal{B}_n$ is an n-dimensional unit ball and $d' = d \cdot \sqrt{n/(4\log n)}$. Let $\boldsymbol{x} = \boldsymbol{w} \mod \boldsymbol{B}$.
- Given the LWE oracle and sampling oracle D from $D_{\Lambda^*,r}$[7], call the $\mathrm{CVP}_{\alpha q/(\sqrt{2}r)}$ reduction algorithm R of Lemma 3.4 in [1] on the input $(\boldsymbol{B}, \boldsymbol{x})$ with parameter $r = \frac{q\cdot\sqrt{2n}}{\gamma\cdot d}$. Let $\boldsymbol{v}$ be the output of R.

If $\boldsymbol{v} \neq \boldsymbol{x} - \boldsymbol{w}$ in any of the 4 iterations, it outputs YES. Otherwise, output NO.

The analysis of the NO instance is the same as [18]. For completeness, we give a sketch of the proof. We have that $\eta_\epsilon(\Lambda^*) \leqslant \frac{\sqrt{n}}{\gamma\cdot d}$, for $\epsilon(n) = 2^{-n} = \mathrm{negl}(n)$ by Lemma 1. Therefore $r \geqslant \sqrt{2}q \cdot \eta_\epsilon(\Lambda^*)$ as the algorithm R from Lemma 3.4 in [1] required. Moreover, since $\boldsymbol{x} - \boldsymbol{w} \in \Lambda$, the distance from $\boldsymbol{x}$ to Λ is at most $d' = d \cdot \sqrt{\frac{n}{4\log n}} \leqslant \frac{\alpha\gamma d}{\sqrt{4n}} = \frac{\alpha q}{\sqrt{2}r}$. By the definition of d', $\lambda_1(\Lambda) > \gamma \cdot d > 2d'$ and the solution of $\mathrm{CVP}_{\alpha q/(\sqrt{2}r)}$ is unique. The algorithm R outputs $\boldsymbol{v} = \boldsymbol{x} - \boldsymbol{w}$ in each iteration, and our reduction rejects.

Now, we focus on the YES instance, i.e., $(\boldsymbol{B}, d)$ satisfies $\lambda_1(\Lambda) \leqslant d$. The maximum distance between the point on the surface of $\sqrt[n]{9/8}d' \cdot \mathcal{B}_n$ and the point on the surface of $d' \cdot \mathcal{B}_n$ is $\sqrt[n]{9/8}d' + d'$, while the minimum distance between the point on the surface of $\sqrt[n]{9/8}d' \cdot \mathcal{B}_n$ and the point on the surface of $d' \cdot \mathcal{B}_n$ is $\sqrt[n]{9/8}d' - d'$. Thus, $\sqrt[n]{9/8}d' + d' - (\sqrt[n]{9/8}d' - d') = 2d' > 2d > 2\lambda_1(\Lambda)$. Then there exists some integer m, such that $\sqrt[n]{9/8}d' + d' \geqslant m \cdot \lambda_1(\Lambda) \geqslant (\sqrt[n]{9/8}d' - d')$. Thus, there exists at least one point w_0 on the surface of $d' \cdot \mathcal{B}_n$ and one point w'_0 on the surface of the ball $\sqrt[n]{9/8}d' \cdot \mathcal{B}_n$ such that $\boldsymbol{w}_0 - \boldsymbol{w}'_0 = m \cdot \boldsymbol{z}$, where $\boldsymbol{z}$ is the shortest vector in the lattice. Denote the rotation of the ball $\sqrt[n]{9/8}d' \cdot \mathcal{B}_n$ that transforms $\sqrt[n]{9/8}d' \cdot \boldsymbol{w}_0$ to $\boldsymbol{w}'_0$ by T. Suppose $\boldsymbol{w}'$ is the point $T(\sqrt[n]{9/8}\boldsymbol{w})$ where $\boldsymbol{w}$ is chosen uniformly from $d' \cdot \mathcal{B}_n$. Let $\boldsymbol{x}' = \boldsymbol{w}' \mod \boldsymbol{B}$ and invoke R on $\boldsymbol{x}'$. Then $R(\boldsymbol{x}') = \boldsymbol{x}' - \boldsymbol{w}$ is an event. By the probability preserving property, we have that

$$\Pr^2[R(\boldsymbol{x}) - \boldsymbol{x} = -\boldsymbol{w}] \leqslant R_2(\boldsymbol{x}\|\boldsymbol{x}') \cdot \Pr[R(\boldsymbol{x}') - \boldsymbol{x}' = -\boldsymbol{w}] \tag{9}$$

[7] The oracle D can be implemented by Lemma 2.3 in [26] on the reversed dual basis $\boldsymbol{D}$ of $\boldsymbol{B}$.

$$\leqslant R_2(\boldsymbol{w}||\boldsymbol{w}') \cdot \Pr[R(\boldsymbol{x}') - \boldsymbol{x}' + \boldsymbol{w} = 0]. \tag{10}$$

The inequality 10 follows from $R_2(\boldsymbol{x}||\boldsymbol{x}') \leqslant R_2(\boldsymbol{w}||\boldsymbol{w}')$, since $\boldsymbol{x} = \boldsymbol{w} \mod \boldsymbol{B}$ and $\boldsymbol{x}' = \boldsymbol{w}' \mod \boldsymbol{B}$. By the property of RD in Lemma 2, we have

$$\Pr^2[R(\boldsymbol{x}) - \boldsymbol{x} + \boldsymbol{w} = 0] \leqslant R_2(\boldsymbol{w}||\boldsymbol{w}') \cdot \Pr[R(\boldsymbol{x}') - \boldsymbol{x}' + \boldsymbol{w}' = 0]. \tag{11}$$

Invoking the algorithm R on $\boldsymbol{x}'$, it may return $\boldsymbol{x}' - \boldsymbol{w}'$, $\boldsymbol{x}' - \boldsymbol{w}$ or something else. Thus, $\Pr[R(\boldsymbol{x}') - \boldsymbol{x}' + \boldsymbol{w}' = 0] \leqslant 1 - \Pr[R(\boldsymbol{x}') - \boldsymbol{x}' + \boldsymbol{w} = 0]$ and we have

$$\Pr^2[R(\boldsymbol{x}) - \boldsymbol{x} + \boldsymbol{w} = 0] \leqslant R_2(\boldsymbol{w}||\boldsymbol{w}') \cdot (1 - \Pr[R(\boldsymbol{x}') - \boldsymbol{x}' + \boldsymbol{w}' = 0]). \tag{12}$$

Sum the inequalities (11) and (12), we have that $\Pr^2[R(\boldsymbol{x}) = \boldsymbol{x} - \boldsymbol{w}] \leqslant R_2(\boldsymbol{w}||\boldsymbol{w}')/2$. Furthermore,

$$\Pr[R(\boldsymbol{x}) = \boldsymbol{x} - \boldsymbol{w}] \leqslant \sqrt{\big(V\big(\sqrt[n]{9/8}d' \cdot \mathcal{B}_n\big)/V(d' \cdot \mathcal{B}_n)\big)/2} \leqslant \sqrt{9/16}. \tag{13}$$

Since $\Pr[R(\boldsymbol{x}) \neq \boldsymbol{x} - \boldsymbol{w}] = 1 - \Pr[R(\boldsymbol{x}) = \boldsymbol{x} - \boldsymbol{w}] \geqslant 1 - \sqrt{9/16} \geqslant 1/4$, we have $\boldsymbol{v} \neq \boldsymbol{x} - \boldsymbol{w}$ in at least one iteration of the four iterations and the reduction accepts.

Remark 3. Our reduction runs the basic procedure only four times, while [18] needs a large polynomial iterations. Therefore, with access to the $\mathrm{SLWE}_{n,q,\Phi_\alpha}$ solver, the running time of our reduction solving $\mathrm{GapSVP}_{\zeta,\gamma}$ is polynomial times less than that of [18].

5 Links between decision problems and search problems

Motivated by the strategy of [16] and Theorem 1, we explore the relation between search problems and decision problems as an independent interest. In the decision problem, we can extract a search problem—hidden search problem for each distinguisher $\mathcal{A}$.

Definition 6 (Hidden search problem for $\mathcal{A}$)**.** For a decision problem P, we say an algorithm solving a hidden search problem for $\mathcal{A}$ (denoted as $P^{\mathcal{A}}$) if given two distributions X_0 and X_1, we can find a randomness r over which there is a non-negligible difference in acceptance probability on inputs from X_0 versus from X_1, i.e., our goal is to output an r from the set $R = \{r|p_1(r) - p_0(r) \text{ is non-negligible}\}$. If the set R is empty, we output $\perp$.

Proposition 1. If an algorithm $\mathcal{A}$ can solve the decision problem P with the advantage ε and running time T, there exists an algorithm W solving the hidden search problem for $\mathcal{A}$ with probability exponentially close to 1. Besides, the running time of W is upper bounded by $O(\frac{1}{\varepsilon})T$.

Proof. Without loss of generality, we may assume the difference in acceptance probability on inputs from X_1 versus from X_0 is positive. If an algorithm $\mathcal{A}$ can solve the decision problem, there is a non-negligible ε such that $\mathrm{Adv}(\mathcal{A}) = \Pr[\mathcal{A}(x) = 1|x \leftarrow X_1] - \Pr[\mathcal{A}(x) = 1|x \leftarrow X_0] = \varepsilon$.

We divide the randomness domain into three disjoint parts, i.e., $\mathcal{S}_1 = \{r|p_1(r) - p_0(r) \geqslant \frac{3\varepsilon}{4}\}$, $\mathcal{S}_2 = \{r|0 \leqslant p_1(r) - p_0(r) < \frac{3\varepsilon}{4}\}$ and $\mathcal{S}_3 = \{r|p_1(r) - p_0(r) < 0\}$. Define an algorithm W: choose $r \leftarrow \Phi$ and estimate the conditional acceptance probability of $\mathcal{A}$ on X_0 and X_1 by sampling from $D_0(r)$ and $D_1(r)$ several polynomial times. By the Hoeffding bound, we have estimations $\widetilde{p}_0$ and $\widetilde{p}_1$ satisfying $|\widetilde{p}_i - p_i(r)| < \frac{\varepsilon}{8}$, for $i \in \{0, 1\}$ with probability exponentially close to 1. If $\widetilde{p}_1 - \widetilde{p}_0 > \frac{\varepsilon}{2}$, we output r. Otherwise, we repeat the above procedure.

We now prove that W can successfully output an r in the polynomial time. For correctness, the output r has the property $p_1(r) - p_0(r) = p_1 - \widetilde{p}_1 + \widetilde{p}_1 - \widetilde{p}_0 + \widetilde{p}_0 - p_0 > \frac{\varepsilon}{4}$. Notice that as long as $r \in \mathcal{S}_1$, it will be an output, since $\widetilde{p}_1 - \widetilde{p}_0 > \frac{\varepsilon}{2}$. By the average argument, we claim the probability $\Phi(\mathcal{S}_1) \geqslant \frac{\varepsilon}{4}$. Therefore, we can repeat the procedure polynomial times and successfully choose r in $\mathcal{S}_1$ in the expected time $O(\frac{1}{\varepsilon})T$ as an output.

Remark 4. Since RD is appropriate for search problems, Proposition 1 illustrates a method of applying RD on decision problems via analyzing the adversaries' advantage with the measure of r. However, such calculation may need additional properties (e.g., public sampleability or adaptively public sampling property). Thus, applying RD on more decision problems is still an open problem.

6 Conclusion

In this paper, we investigate the security of DLWE and SLWE using RD respectively. As for DLWE, we prove the pseudorandomness of MLWE with different error distributions, especially for center binomial distribution and uniform distribution, which can be viewed as a theoretic support to several NIST submissions. As for SLWE, we optimize the iterations in classical reduction of GapSVP to LWE problem. Furthermore, we find a relation between search problems and decision problems to interpret the feasibility and challenge of RD on decision problems. We leave the extension of RD on more decision problems as our future work.

Acknowledgements This work was supported in part by National Natural Science Foundation of China (Nos. 61772520, 61632020, 61472416, 61802392), Key Research Project of Zhejiang Province (Grant No. 2017C01062), and National Key Research and Development Program of China (Grant No. 2017yfb0802200).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Regev O. On lattices, learning with errors, random linear codes, and cryptography. In: Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, 2005. 84–93

2 Lyubashevsky V, Peikert C, Regev O. On ideal lattices and learning with errors over rings. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco, 2010

3 Langlois A, Stehlé D. Worst-case to average-case reductions for module lattices. Des Codes Cryptogr, 2015, 75: 565–599

4 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Proceedings of the 40th Annual ACM Symposium on Theory of Computing, Victoria, 2008. 197–206

5 Lindner R, Peikert C. Better key sizes (and attacks) for LWE-based encryption. In: Proceedings of Cryptographers' Track at the RSA Conference, San Francisco, 2011. 319–339

6 Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. In: Proceedings of the 52nd Annual Symposium on Foundations of Computer Science, Palm Springs, 2011. 97–106

7 Gentry C, Sahai A, Water B. Homomorphic encryption from learning with errors: conceptually-simpler, asymptotically-faster, attribute-based. In: Proceedings of Annual Cryptology Conference, Santa Barbara, 2013. 75–92

8 Alkim E, Ducas L, Pöppelmann T, et al. Post-quantum key exchange – a new hope. In: Proceedings of the 25th USENIX Security Symposium, Austin, 2016. 327–343

9 Bos J W, Costello C, Ducas L, et al. Frodo: take off the ring! practical, quantum-secure key exchange from LWE. In: Proceedings of the Conference on Computer and Communications Security, Vienna, 2016. 1006–1018

10 Bos J W, Ducas L, Kiltz E, et al. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In: Proceedings of European Symposium on Security and Privacy, London, 2018. 353–367

11 Alkim E, Avanzi R, Bos J, et al. NewHope: alogrithm specifcations and supporting documentation. http://newhopecrypto.org/

12 Lu X H, Liu Y M, Zhang Z F, et al. LAC: practical ring-LWE based public-key encryption with byte-level modulus. 2018. https://eprint.iacr.org/2018/1009.pdf

13 Smart N P, Albrecht M R, Lindell Y, et al. LIMA: a PQC encryption scheme. https://lima-pq.github.io/

14 Bansarkhani R E. KINDI: 20171130 submission. http://kindi-kem.de/

15 Ducas L, Kiltz E, Lepoint T, et al. CRYSTALS-Dilithium: a lattice-based digital signature scheme. IACR Trans Cryptogr Hardw Embed Syst, 2018, 2018: 238–268

16 Bai S, Lepoint T, Roux-Langlois A, et al. Improved security proofs in Lattice-based cryptography: using the Rényi divergence rather than the statistical distance. J Cryptol, 2018, 31: 610–640

17 Bogdanov A, Guo S Y, Masny D, et al. On the hardness of learning with rounding over small modulus. In: Proceedings of Theory of Cryptography, Israel, 2016. 209-224

18 Peikert C. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In: Proceedings of the 41st Annual ACM Symposium on Theory of Computing, Bethesda, 2009. 333–342

19 Takashima K, Takayasu A. Tighter security for efficient lattice cryptography via the rényi divergence of optimized orders. In: Proceedings of International Conference on Provable Security, Kanazawa, 2015. 412–431

20 Prest T. Sharper bounds in lattice-based cryptography using the rényi divergence. In: Proceedings of International Conference on the Theory and Application of Cryptology and Information Security, Hong Kong, 2017. 347–374

21 Ducas L, Durmus A, Lepoint T, et al. Lattice signatures and bimodal gaussians. In: Proceedings of Annual Cryptology Conference, Santa Barbara, 2013. 40–56

22 Micciancio D, Regev O. Worst-case to average-case reductions based on gaussian measures. In: Proceedings of the 45th Symposium on Foundations of Computer Science, Rome, 2004. 372–381

23 Micciancio D, Mol P. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In: Proceedings of Annual Cryptology Conference, Santa Barbara, 2011. 465–484

24 Micciancio D, Peikert C. Trapdoors for lattices: simpler, tighter, faster, smaller. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, 2012. 700–718

25 van Erven T, Harremoes P. Rényi divergence and Kullback-Leibler divergence. IEEE Trans Inform Theory, 2014, 60: 3797–3820

26 Brakerski Z, Langlois A, Peikert C, et al. Classical hardness of learning with errors. In: Proceedings of Symposium on Theory of Computing Conference, Palo Alto, 2013. 575–584