Research Article

Hardness of Module-LWE with Semiuniform Seeds from Module-NTRU

Wenjuan Jia,1,2 Jiang Zhang,2, and Baocang Wang1,3

1School of Telecommunications Engineering, Xidian University, Xi’an, Shaanxi 710071, China
2State Key Laboratory of Cryptology, P.O. Box 5159, Beijing 100878, China
3State Key Laboratory of Integrated Service Networks, Xidian University, Xi’an, Shaanxi 710071, China

Correspondence should be addressed to Wenjuan Jia; 18368910175@163.com

Received 31 May 2023; Revised 8 July 2023; Accepted 18 August 2023; Published 23 October 2023

Academic Editor: Youwen Zhu

Copyright © 2023 Wenjuan Jia et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The module learning with errors (MLWE) problem has attracted significant attention and has been widely used in building a multitude of lattice-based cryptographic primitives. The hardness of the MLWE problem has been established for several variants, but most of the known results require the seed distribution (i.e., the distribution of matrix A) to be the uniform distribution. In this paper, we show that under the Module-N-th degree Truncated polynomial Ring Units (NTRU) (MNTRU) assumption, the search MLWE problem can still be hard for some distributions that are not (even computationally indistinguishable from) the uniform distribution. Specifically, we show that if the seed distribution is a semiuniform distribution (namely, the seed distribution can be publicly derived from and has a “small difference” to the uniform distribution), then for appropriate settings of parameters, the search MLWE problem is hard under the MNTRU assumption. Moreover, we also show that under the appropriate settings of parameters, the search learning with errors over rings problem with semiuniform seeds can still be hard under the NTRU assumption due to our results for the search MLWE problem with semiuniform seeds being rank-preserving.

1. Introduction

Lattice-based cryptography has triggered significant attention in the last few decades because of its specific algebraic structures. The learning with errors (LWE) problem was first introduced by Regev [1] in the groundbreaking paper in 2005 and has been proven to be a versatile ingredient for lattice-based cryptography. For positive integers \(q \geq 2\), let \(q\) be the seed distribution over \(\mathbb{Z}_q\), \(\delta\) be the secret distribution over \(\mathbb{Z}_q^n\), and \(\chi\) be the noise distribution over \(\mathbb{Z}_q\) (or \(\mathbb{Z}\)). The search LWE problem \((\mathcal{D}, \delta, \chi, m)\)-LWE\(_n\) in matrix form asks an algorithm to recover the secret \(s \in \mathbb{Z}_q^n\) from the LWE samples \((A, y = As + e \mod q)\) for some \(A \leftarrow \mathcal{D}, s \leftarrow \delta,\) and \(e \leftarrow \chi^m\), whereas the decision LWE problem \((\mathcal{D}, \delta, \chi, m)\)-DLWE\(_n\) asks to distinguish between \((A, y = As + e \mod q)\) and \((A, u)\), where \(u\) is an uniform random vector over \((\mathbb{T}_q)^m\) (or \(\mathbb{Z}_q^m\)) and \(\mathbb{T}_q\) is the \(q\)-scaled of the real torus. Denote by \(U(S)\) the uniform distribution over some set \(S\) and by \(D_\alpha\) the continuous Gaussian distribution with parameter \(\alpha > 0\) over \(\mathbb{R}\). Under the specific settings of parameters, the works by Regev [1], Brakerski et al. [2], and Peikert [3] has established the quantum and classical reductions from some standard worst-case lattice problems, such as the gap shortest vector problem (GapSVP) and the shortest independent vector problem (SIVP), to the LWE problem \((U(\mathbb{Z}_q^{m\times n}), U(\mathbb{Z}_q^m), D_\alpha, m)\)-LWE\(_n\). The LWE problem is extensively served as a security foundation for a remarkable number and variety of lattice-based cryptographic primitives [1, 3–12] since its introduced.

All of the LWE-based primitives however are not usually efficient enough due to their key sizes and computation times are at least quadratic in the security parameter. To improve the intrinsic inefficiency of LWE-based schemes, LWE over rings (RLWE) [13–15], LWE over modules (module learning with error; MLWE) [6, 16], and the learning with rounding (LWR) problem and its algebraically structured variants [17–19] were introduced and studied. The RLWE problem uses a more algebraic setting instead of working over integers, and it generally offers an improve in efficiency over the...
LWE problem. It has been shown in [13, 14] that the RLWE problem is at least as hard as some standard worst-case ideal-lattice problems, such as SVP and SIVP restricted to ideal-lattices (Ideal-SVP and Ideal-SIVP). Nevertheless, contrary to the case of general lattices, the works by Cramer et al. [20, 21] showed that some lattice problems, such as GapSVP, are actually easy on the ideal lattices. Therefore, the MLWE problem was proposed to address the drawbacks both in LWE and RLWE, and it might be able to offer a better level of security than the RLWE problem while still offering performance advantages over the LWE problem [22, 23].

Formally, for positive integers \(d, m, n\) and modulus \(q \geq 2\), let \(R\) be the ring of integers of an \(n\)-degree number field \(K\). Define \(K_R = K \otimes_K R\), \(\mathcal{T}_q R = K_R / (qR)\), \(R_q = R / (qR)\), and \(R_q^\vee = R^\vee / (qR^\vee)\). Let \(D\) be the seed distribution over \(R_q^\text{mod}\), \(\mathcal{S}\) be the secret distribution over \((R_q^\vee)^d\) and \(\chi\) be the noise distribution over \(K_R\) (or \(R\)). The search MLWE problem \((D, \mathcal{S}, qR, m) - \text{MLWE}_{K,d,n,q}\) asks an algorithm to output the secret \(s \in (R_q^\vee)^d\) (we note that the MLWE problem in which the secret \(s\) is chosen from \(R_q^\vee\) is also called the primal-MLWE problem, and that the MLWE problem in which the secret \(s\) is chosen from \((R_q^\vee)^d\) is also called the dual-MLWE problem [24]) from the MLWE samples \((A, y = As + e \mod qR^\vee)\) for some \(A \in \mathcal{D}\), \(s \in \mathcal{S}\), and \(e \sim \mathcal{P}_n\), whereas the decision MLWE problem \((D, \mathcal{S}, \chi, m) - \text{MLWE}_{K,d,n,q}\) asks to distinguish between \((A, As + e \mod qR^\vee)\) and \((A, u)\), where \(u \sim U(\mathbb{Z}_q^m)\). Notice that the RLWE problem \((D, \mathcal{S}, \chi, m) - \text{RLWE}_{K,d,n,q}\) can be seen as a special case of the MLWE problem \((D, \mathcal{S}, \chi, m) - \text{MLWE}_{K,d,n,q}\) with the rank \(d = 1\). Similarly to LWE, for appropriate settings of parameters, the MLWE problem also enjoys the quantum and classical worst-case to average-case reductions from some standard module–lattice problems such as GIVP (which is a generalized version of SIVP) and GapSVP restricted to module–lattices (Module-GIVP and Module-GapSVP) [16, 25, 26]. In this present work, we only consider the MLWE problem with secret \(s\) lies in \(R_q^\vee\) instead of \((R_q^\vee)^d\).

Since the introduction of MLWE, it has attracted significant attention and has been widely used in building a plethora of lattice-based cryptographic constructions. For example, two of four postquantum algorithms selected by NIST (https://csrc.nist.gov/news/2022/pqc-candidates-to-be-standardized-and-round-4) for postquantum cryptography (PQC) standardization are MLWE based—the signature scheme CRYSTALS–Dilithium [27] and the public-key encryption/key encapsulation mechanism CRYSTALS–Kyber [28]. We notice that most results [16, 22, 26–32] only consider the MLWE problem with seed distribution that is other a uniform distribution or computationally indistinguishable from the uniform distribution [32]. However, as far as we know, no results can apply to the MLWE problem with seed distribution that is not (even computationally indistinguishable from) the uniform distribution. This raises a natural question: Is the RLWMLWE problem still hard when the seed distribution is not (even computationally indistinguishable from) the uniform distribution?

1.1. Our Results. In the present work, we concentrate on the search R/MLWE problem and answer the above question affirmatively. Particularly, we consider a special class of distributions which we call semiuniform distribution (informally, a distribution is called a semiuniform distribution if it can be derived from and has a "small difference" to the uniform distribution), and show that under the specific settings of parameters, the search MLWE problem with semiuniform seeds is as hard as the Module-N-th degree Truncated polynomial Ring Units (NTRU) (henceforth MNTRU) problem as long as the secret distribution \(\mathcal{S}\) has sufficiently large min-entropy. Due to the results for the search MLWE problem with semiuniform seeds are rank-preserving, we also show that for the appropriate settings of parameters, the search RLWE problem with semiuniform seeds can still be hard under the NTRU assumption. Before giving our results for the search R/MLWE with semiuniform seeds, we first define some necessary notations.

Formally, a matrix distribution \(\mathcal{M}\) is known as a \(\eta\)-semiuniform distribution over some finite set \(R^\text{mod}\) if there exists a set of distributions \(\{\phi_U\}_{U \in R^\text{mod}}\) such that for any randomly chosen matrices \(M \leftarrow \mathcal{M}, U \leftarrow U(R^\text{mod})\), \(E_U \leftarrow \phi_U\), we have that 1) \(M\) is statistically close to \(U - E_U\); and 2) the spectral norm of \(E_U\) is upper bounded by \(\eta\). Moreover, let \(\phi\) be a distribution over \(R, (G, F) \leftarrow \phi^\text{mod} \times \phi^\text{mod}\) conditioned on \(G\) is invertible in \(R_q\), and let \(G^{-1}_q\) be the \(R_q\)-inverse of \(G\). The MNTRU problem \((\phi, m) - \text{MNTRU}_{R,d,n,q}\) is to distinguish between \(F \cdot G^{-1}_q \mod qR\) and \(U \leftarrow U(R_q^\text{mod})\). And the NTRU problem with \(m\) samples \((\phi, m) - \text{NTRU}_{R,d,n,q}\) can be seen as a special case of the MNTRU problem \((\phi, m) - \text{MNTRU}_{R,d,n,q}\) with \(d = 1\). We have the following informal theorems for the search R/MLWE problem with semiuniform seeds (see Sections 4 and 5 for the formal results).

**Theorem 1** (Informal). Let \(\mathcal{D}\) be a \(\eta\)-semiuniform distribution over \(R^\text{mod}\) and \(\mathcal{S}\) be a secret distribution over \(R_q^\vee\). Assume that the Gaussian parameter \(\beta\) is large enough and that the problem \((D, \mathcal{S}, qR, m) - \text{MLWE}_{K,d,n,q}\) is hard. Then the search MLWE problem \((D, \mathcal{S}, \mathcal{D}_q, qR, m) - \text{MLWE}_{K,d,n,q}\) is hard, provided that the distribution \(\mathcal{S}\) has sufficiently large min-entropy and the Gaussian parameter \(\alpha\) is large enough.

**Theorem 2** (Informal). Let \(\mathcal{D}\) be a \(\eta\)-semiuniform distribution over \(R^\text{mod}\) and \(\mathcal{S}\) be a secret distribution over \(R_q^\vee\). Assume that the Gaussian parameter \(\beta\) is large enough and that the problem \((D, \mathcal{S}, \mathcal{D}_q, qR, m) - \text{MLWE}_{K,d,n,q}\) is hard. Then the search RLWE problem \((\mathcal{D}, \mathcal{S}, \mathcal{D}_q, qR, m) - \text{RLWE}_{K,d,n,q}\) is hard, provided that the secret distribution \(\mathcal{S}\) has sufficiently large min-entropy and Gaussian parameter \(\alpha\) is large enough.

1.2. Technical Overview. We will sketch the main ideas behind our results in the following and the techniques used in this paper followed the ones used by Boudgoust et al.
(1) We first convert the goal of this paper, namely proving the hardness of the search MLWE problem with semiuniform seeds under the MNTRU assumption, into proving the hardness of the Str-LWE problem with str-semiuniform seeds under the Str-NTRU assumption, see Section 3 for details.

(2) We then define a sometimes lossy pseudorandom distribution, as introduced by Boudgoust et al. [30, 33] and Brakerski and Döttling [34], and give explicit conditions for the existence of a sometimes lossy pseudorandom distribution \( \mathcal{Y} \), see Theorem 3.

(3) Combining with Lemma 9 (which shows that the existence of a sometimes lossy pseudorandom distribution implies the hardness of Str-LWE with str-semiuniform seeds), we then prove that under specific settings of parameters, the Str-LWE problem with str-semiuniform seeds is hard provided that the Str-NTRU problem is hard.

For the item (1) mentioned before, we first define two nonalgebraic form problems, namely the structured LWE (Str-LWE) and structured NTRU (Str-NTRU) problems as defined by Boudgoust et al. [30, 33], and define the structured semiuniform distribution (str-semiuniform for short). Formally, let \( d, m, n, q \geq 2 \) be positive integers. Let \( \mathcal{D}, \mathcal{S}, \) and \( \mathcal{X} \) be the seed, secret and noise distributions over \( \mathbb{Z}_q^{dn}, \mathbb{Z}_q^{mn}, \) and \( \mathbb{R}^n \), respectively. Let \( \mathcal{X} \) be a distribution of matrices over \( \mathbb{Z}_q^{mn}, \) and \( \Phi \) be a distribution of matrices over \( GL(dn: \mathbb{Z}, q) \times \mathbb{Z}^{\mathit{maxdn}}, \) where \( GL(dn: \mathbb{Z}, q) \) is the set of matrices in \( \mathbb{Z}^{dn} \) that are invertible in \( \mathbb{Z}_q \). The Str-LWE problem \( (\mathcal{D}, \mathcal{S}, \mathcal{X}, m) - \text{Str-LWE}_{d,n,q} \) asks an algorithm to output the secret \( s \in \mathbb{Z}_q^d \) given matrix \( A \leftarrow \mathcal{D} \) and “noisy” vector \( y = As + e \mod q \) for some \( s \leftarrow \mathcal{S} \) and \( e \leftarrow \mathcal{X}^m \). Moreover, the Str-NTRU problem \( (\Phi, \mathcal{X}, m) - \text{Str-NTRU}_{d,n,q} \) is to distinguish between \( F_q^{-1} \mod q \) and \( U \leftarrow \mathcal{X}^m \), where \( (G, F) \leftarrow \Phi \) and \( G_q^{-1} \) be the \( \mathbb{Z}_q \)-inverse of \( G \mod q \). Note that as shown by Boudgoust et al. [30, 33], we use the name Str-NTRU only because it is to MNTRU what Str-LWE is to MLWE, and NTRU should not be interpreted as if there exists an unstructured version of NTRU due to it already being a structured problem. Finally, a matrix distribution \( \mathcal{M} \) is known as a \( \eta \)-str-semiuniform distribution over \( \mathbb{Z}_q^{\mathit{maxdn}} \) if there exists a set of distributions \( \{ \phi_U \}_{U \in \mathbb{Z}_q^{\mathit{maxdn}}} \) such that for any randomly chosen matrices \( M \leftarrow \mathcal{M}, U \leftarrow \mathcal{X}^m \), and \( E_U \leftarrow \phi_U \), we have that (1) \( M \) is statistically close to \( U - E_U \); and (2) the spectral norm of \( E_U \) is upper bounded by \( \eta \).

Define \( \mathcal{X} = \mathbb{M}_R(U(R_q^{\mathit{mod}})) \), then we can convert the MNTRU problem \( (\Phi, m) - \text{MNTRU}_{d,n,q} \) to the Str-NTRU problem \( (\Phi, \mathcal{X}, m) - \text{Str-NTRU}_{d,n,q} \) via embedding the algebraic setting into vectors and matrices over the integers or the reals, where \( \mathbb{M}_R \) is defined in Section 2.1 and \( \Phi \) is a distribution over \( R \), see Remark 1 for more detail. Similarly, let \( B_q \) be the inverse of a known basis of the ideal lattice \( \sigma_H(R) \), where \( \sigma_H(\cdot) \) is a map from some \( n \)-degree number field \( K \) to \( \mathbb{R}^n \) given in Section 2.1. We can also convert the MLWE problem with semiuniform seeds \( (\mathcal{D}, \mathcal{S}, D_{\mathit{K}_0}, a, m) - \text{MLWE}_{K_0,d,n,q} \) to the Str-LWE problem with str-semiuniform seeds \( (\mathcal{D}, \mathcal{S}, D_{\mathit{A}_q}, m) - \text{Str-LWE}_{d,n,q} \) (see Lemma 7 for more details), where \( D_0 \) is the seed distribution over \( R_0 \), \( \mathcal{S}_0 \) is the secret distribution over \( R_0 \), \( \mathcal{D} = \mathbb{M}_R(\mathcal{D}_0) \), \( \mathcal{S} = \mathcal{S}_0(\mathcal{S}_0) \), and \( D_{\mathit{A}_q} = \psi(D_{\mathit{A}_q}) \).

As alluded to before, the goal of this paper is then converted in proving the hardness of the Str-LWE problem \( (\mathcal{D}, \mathcal{S}, D_{\mathit{A}_q}, m) - \text{Str-LWE}_{d,n,q} \) provided that the Str-NTRU problem \( (\Phi, \mathcal{X}, m) - \text{Str-NTRU}_{d,n,q} \) is hard.

For the item (2) noted above, we first consider a special class of distributions which we call sometimes lossy pseudorandom distribution (adapted from Boudgoust et al. [30, 33]). Formally, a distribution \( \mathcal{Y} \) is known as a sometimes lossy pseudorandom distribution for \( (\mathcal{D}, \mathcal{S}, \mathcal{X}) \) if there exists \( \kappa = \omega(\log(\lambda)) \) and \( \nu \geq 1/\poly(\lambda) \) such that (1) (Pseudorandomness) \( \mathcal{Y} \) is computationally indistinguishable from \( \mathcal{D} \), and (2) (Sometimes Lossiness) \( Pr_{A \leftarrow \mathcal{Y}}(H_{\nu}^c(s, A, As + e \mod q) \geq k) \geq \nu \), where \( H_{\nu}^c \) is the \( \nu \)-smooth average conditional min-entropy given in Section 2.2. Therefore, it suffices to prove the existence of a sometimes lossy pseudorandom distribution \( \mathcal{Y} \) since the existence of \( \mathcal{Y} \) implies the hardness of the Str-LWE problem with str-semiuniform seeds (Lemma 9). For the sake of convenience, we will omit “\( \mod q \)” from the expression in the following.

Recall that the distribution \( \mathcal{X} = \mathbb{M}_R(U(R_q^{\mathit{mod}})) \), by the assumption that \( \mathcal{D} \) is a \( \eta \)-str-semiuniform distribution over \( \mathbb{Z}_q^{\mathit{maxdn}} \), there exists a set of distributions \( \{ \phi_U \}_{U \in \mathbb{Z}_q^{\mathit{maxdn}}} \) such that the following two distributions are statistically close:

\[
\{ A : A \leftarrow \mathcal{D} \}, \quad \{ A = U - E_U : U \leftarrow \mathcal{X}, E_U \leftarrow \phi_U \}. \tag{1}
\]

Moreover, if the Str-NTRU problem \( (\Phi, \mathcal{X}, m) - \text{Str-NTRU}_{d,n,q} \) is hard, then we can replace the matrix \( U \) from the Str-LWE instance \( (U - E_U, y = (U - E_U)s + e) \) by the Str-NTRU instance \( F_q^{-1} \), where \( \Phi \) is a distribution over \( GL(dn: \mathbb{Z}, q) \times \mathbb{Z}_q^{\mathit{maxdn}}, (G, F) \leftarrow \Phi, \) and \( G_q^{-1} \in \mathbb{Z}_q^{\mathit{maxdn}} \) is the \( \mathbb{Z}_q \)-inverse of \( G \mod q \). Thus, the following two distributions are computationally indistinguishable:
\[
\begin{align*}
(A = U - E_U; U \leftarrow \mathcal{X}, E_U \leftarrow \phi_U), \\
A = U - E_U; U = FG_0^{-1}, (G, F) \leftarrow \Phi, E_U \leftarrow \phi'_U.
\end{align*}
\] (2)

That is to say, if we define the distribution \( \mathcal{Y} \) as the distribution of \( U - E_U \) with \( U = FG_0^{-1} \), then the pseudorandomness property holds for the distribution \( \mathcal{Y} \) by the above analysis. Next, we will show that the sometimes lossiness property also holds for \( \mathcal{Y} \) defined above.

We now can rewrite \( y = As + e = (U - E_U)s + e = (FG_0^{-1} - E_U)s + e = FG_0^{-1}s - E_0s + e \), where \( s \leftarrow S \) and \( e \leftarrow D_{\alpha}^m \). Assume that the spectral norms of \( F'(G)^{-1} \) and \( G' \) are, respectively, upper bounded by \( s_1 \) and \( s_2 \) with probability at least \( \nu \geq 1/\text{poly}(\lambda) \) over the choice of \((G, F)\), where
\[
G = B_{\mathbb{F}_q^m}^{-1}GB_{\rho}, \quad F = B_{\mathbb{F}_q^m}FB_{\rho}, \quad \text{and} \quad B_{\rho} = I_1 \otimes B_{\rho} \text{ for any positive integer } k.
\]

By the property of spectral norm, we have that the spectral norm of \( B_{\mathbb{F}_q^m}^{-1}FG_0^{-1} - E_U \) is upper bounded by \( s_1 + \eta_0 \), where \( \eta_0 \) is the upper bound of the spectral norm of \( s (B_{\mathbb{F}_q^m}^{-1}E_1B_{\rho}) \) and \( G^{-1} \in Q^{\text{mod } d} \) is the \( Q \)-inverse of \( G \).

Set \( a_1 = 2^{3/2}a_0 \), we have \( a_1 \geq a_1(s_1 + \eta_0) \) by the assumption that \( a \geq 2^{3/2}a_1(s_1 + \eta_0) \). By the property of continuous Gaussians (Lemma 2), we have that there exists a distribution \( \mathcal{Y} \) over \( \mathbb{R}^m \) such that the random variable \( e = (FG_0^{-1} - E_U)e_1 + e' \), where \( e_1 \leftarrow D_{\alpha}^m \), and \( e' \leftarrow \mathcal{Y} \) is distributed according to \( D_{\alpha}^m \). We then have the following two distributions are identical:

\[
\begin{align*}
\{ y = FG_0^{-1}s - E_0s + e : e \leftarrow D_{\alpha}^m \}, \\
y = F(G_0^{-1}s + G^{-1}e_1) - E_U(s + e_1) + e_1 : e_1 \leftarrow D_{\alpha}^m, e' \leftarrow \mathcal{Y}.
\end{align*}
\] (3)

Moreover, we can describe \( e' \) using \( dn \log(s_2) \)-bit since \( e'_s \) is only depends on the lattice coset \( e_0 \mod \Lambda(G) \).

Finally, from above analysis, we know that \( a_0 = a_1/\sqrt{2} > \eta_1 \). Then by the property of discrete Gaussian to continuous Gaussian (see Lemma 5), we have that \( s + e_1 \) and \( s + e_0 \) are \( 8\epsilon \)-close, where \( e_0 \leftarrow D_{\alpha}^m \).

Therefore, we have \( H_2(s_0^e(s + e_1) + G^{-1}e_1, s + e_1) \geq H_\infty(s_0^e(s + e_1) + G^{-1}e_1, s + e_1) \geq o(\log(\lambda)) \) with probability at least \( \nu \). It follows that the sometimes lossiness property also holds for the distribution \( \mathcal{Y} \). Thus, combining with the pseudorandomness property of \( \mathcal{Y} \), the distribution \( \mathcal{Y} \) is a sometimes lossy pseudorandom distribution.

As alluded to before, we know that the sometimes lossiness means that going from \( s \) to \( (U - E_U)s + e \) with \( U = FG_0^{-1} \) loses enough information on \( s \) with nonnegligible probability over the choice of \( F, G, \) and \( E_U \) so that it is hard to recover \( s \). Hence the sometimes lossiness implies the hardness of the Str-LWE problem with \( A = U - E_U \) instead of being str-semiuniform \( A \). Combining with the pseudorandomness property, it then yields the hardness of the Str-LWE problem with \( A - \mathcal{D} \). Finally, in Section 5, we construct the distributions \( \Phi \) as defined by Boudgoust et al. [30, 33] and \( \phi'_U \) that satisfy the required conditions in Theorem 3, and give the main results for this paper.

2. Preliminaries

We use \( \lambda \) to denote the security parameter and \([n]\) to denote the discrete set \([1, \ldots, n]\) for any positive integer \( n \). A function \( f(x) \) is known as negligible if for every positive \( c \) and all sufficiently large \( x \) it holds that \( f(x) < 1/x^c \), and we use \( \negl(\cdot) \) to denote an unspecified negligible function. A probability \( p \) is known as overwhelming if \( 1 - p \) is negligible. We use bold lower case letters (e.g., \( a \)) to denote column vectors, bold capital letters (e.g., \( A \)) to denote matrices, \( I_n \) to denote the identity matrix of size \( n \times n \), italic capital letters (e.g., \( S \)) to denote sets, and calligraphic capital letters (e.g., \( \mathcal{D} \)) to denote probability distributions. Denote by \( (\cdot)^T \) (resp., \( (\cdot) \)) the transpose (resp., Hermitian) of a vector or matrix, and by \( \bar{x} \) the complex conjugate of \( x \in \mathbb{C} \). Denote \( U(S) \) by the uniform distribution over a set \( S, x \leftarrow \mathcal{D} \) by sampling an element \( x \) according to a distribution \( \mathcal{D} \), and \( x = (x_1, \ldots, x_m)^T \leftarrow \mathcal{D}^m \) by sampling each component \( x_i \) according to \( \mathcal{D} \) independently. For two discrete random variables \( X \) and \( Y \) over a common countable support \( S \), the statistical distance between \( X \) and \( Y \) is defined by \( \Delta(X, Y) = 1/2 \sum_{x \in S} |\Pr[X = x] - \Pr[Y = x]| \). We use \( \approx \) to denote “statistically close”. Denote by \( P_X(\cdot) \) the probability density of the continuous random variable \( X \). We write PPT as shorthand for probabilistic polynomial time.

Denote by \( \mathbb{Z}_q \) the the quotient ring \( \mathbb{Z}/(q\mathbb{Z}) \), by \( T_q \) the real torus \( \mathbb{R}/(q\mathbb{Z}) \), and by \( \text{diag}(x) \) the diagonal matrix whose diagonal entries are the entries of \( x \in \mathbb{C}^n \). For positive integers \( n, q \), we denote by \( GL(n; \mathbb{Z}/q\mathbb{Z}) \) (resp., \( GL(n, \mathbb{Z}, q) \)) the set of matrices (resp., elements) in \( \mathbb{Z}^{nxn} \) (resp., \( \mathbb{Z} \)) that are
invertible in $\mathbb{Z}_q$. The $\ell_2$-norm and $\ell_\infty$-norm of some vector $x \in \mathbb{C}^n$ is defined by $\|x\|_2 = \sqrt{\sum_{i=1}^{n} |x_i|^2}$ and $\|x\|_\infty = \max_{i=1}^{n} |x_i|$, respectively. For any matrix $A = (a_1, \ldots, a_n) \in \mathbb{C}^{m \times n}$, we use $\|A\|$ to denote the length of a matrix, which is the norm of its longest column, namely $\|A\| = \max_{i=1}^{m} \|a_i\|$. Recall that the singular values $\sigma_i(A)$ of $A$ are the square roots of the eigenvalues of $AA^*$. The number of nonzero singular values of $A$ equals the rank of $A$.

The spectral norm $s(A)$ of a matrix $A \in \mathbb{C}^{m \times n}$ is defined by $s(A) = \max_{x \in \mathbb{C}^m, \|x\|=1} \|Ax\|_2 \|x\|_2$, which corresponds to the largest singular value of $A$. A lattice $\Lambda$ in $\mathbb{R}^n$ is an additive discrete subgroup of $\mathbb{R}^n$ and each rank-$n$ (full rank) lattice $\Lambda \subseteq \mathbb{R}^n$ can be generated by a basis $B = (b_1, \ldots, b_n) \in \mathbb{R}^{m \times n}$, i.e., $\Lambda = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in \mathbb{Z} \text{ for } i \in [n] \right\}$. The dual lattice $\Lambda^*$ of $\Lambda \subseteq \mathbb{R}^n$ is defined as $\Lambda^* = \{ y \in \mathbb{R}^n : \langle x, y \rangle \in \mathbb{Z} \}$.

### 2.1. Algebraic Number Theory

#### 2.1.1. The Space $\mathbb{H}$

There are exactly $n = t_1 + 2t_2$ field homomorphisms $\sigma_i : K \to \mathbb{C}$ that map $\zeta$ to each of the distinct roots of the polynomial $f$ for a number field $K = \mathbb{Q}(\zeta)$ of degree $n$, where $i \in [n]$, and the polynomial $f$ is the defining polynomial of the algebraic number $\zeta$. Let $\sigma_1, \ldots, \sigma_n$ be the real embeddings (namely the embeddings that map $\zeta$ to one of the real roots of $f$) and $\sigma_{t_1+1}, \ldots, \sigma_{n}$ be complex ones. It is known that for polynomial $f \in \mathbb{Q}(x)$, the complex roots come in conjugate pairs via the fundamental theorem of algebra, so too do the complex embeddings. Then we have $\sigma_{t_1+t_2+j} = \overline{\sigma_{t_1+j}}$ for any $j \in [t_2]$. Define the space $\mathbb{H} = \{ (x_1, \ldots, x_n) \in \mathbb{R}^{n} \times \mathbb{C}^{2t_2} : x_{t_1+t_2+j} = x_{t_1+j}, \forall j \in [t_2] \} \subseteq \mathbb{C}^n$. Then $\mathbb{H}$ equipped with the inner product induced by $\mathbb{C}^n$ is isomorphic to $\mathbb{R}^n$ via the map $x \to U_n^* x$, where $U_n = (h_1, \ldots, h_n)$ with $h_j = e_j$ for $j \in [t_1], h_1 = \sqrt{-1}/\sqrt{2}(e_1 + e_{t_2+1})$ and $h_{t_1+t_2+1} = \sqrt{-1}/\sqrt{2}(e_1 - e_{t_2+1})$ for $j \in [t_1+1, \ldots, t_1+t_2]$, and $e_j \in \mathbb{R}^n$ is the vector with $1$ in its $j$th coordinate and $0$ elsewhere.

#### 2.1.2. Coefficient and Canonical Embeddings

Any $n$-degree number field $K = \mathbb{Q}(\zeta)$ can be seen as an $n$-dimension $\mathbb{Q}$-vector space with basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$. Thus every $x \in K$ can be written as $x = \sum_{i=0}^{n-1} x_i \zeta^i$ with $x_i \in \mathbb{Q}$. The coefficient embedding is the isomorphism $\tau : K \to \mathbb{Q}^n$ that maps every $x \in K$ to its coefficient vector $\tau(x) = (x_0, \ldots, x_{n-1})^T \in \mathbb{Q}^n$. For simplicity, we denote by $r(x)$ the component $x_k$ of $\tau(x)$ for $k \in [n]$. The canonical embedding is the field homomorphism $\sigma_c : K \to \mathbb{H}$ defined as $\sigma_c(x) = (\sigma_1(x), \ldots, \sigma_n(x))^T$, and the addition and multiplication of vectors are both performed component-wise. We notice that an element in $K_R$ can be uniquely identified in $\mathbb{R}^n$ under the isomorphic $\sigma_{H}(\cdot) : K_R \to \mathbb{R}^n$ defined by $\sigma_{H}(x) = \sum_{i=1}^{n} \cdot \cdot \cdot \sigma_i(x)^T$ for any $x \in K_R$. For any vector $x = (x_1, \ldots, x_{t_2})^T \in \mathbb{R}^{t_2}$, we define $\sigma_{H}(x) = (\sigma_1(x_1), \ldots, \sigma_{t_1+t_2}(x_{t_2}))^T \in \mathbb{R}^d$ and similarly for $\tau(x)$ and $\sigma_{H}(x)$. It is known that the coefficients embedding $\tau(x)$ and canonical embedding $\sigma_c(x)$ of $x$ are linked through the Vandermonde matrix $V$ of the roots of the minimal polynomial $f$ for any $x \in K$. That is to say, let $\sigma_i(x) = (a_1, a_2, \ldots, a_n)^T$, then we have $\sigma_c(x) = V \cdot \tau(x)$ for all $x \in K$, where $V = (v_1, \ldots, v_n)^T$ with $v_i = (1, a_i, \ldots, a_i^{d-1})^T$.

For all $x \in K$, the field trace $Tr: K \to \mathbb{Q}$ of $K$ is defined by $Tr(x) = \sum_{i=1}^{n} \sigma_i(x)$ and the field norm $N: K \to \mathbb{Q}$ of $K$ is defined by $N(x) = \prod_{i=1}^{n} \sigma_i(x)$. The dual $R^*$ of $R$ is defined as $R^* = \{ x \in K : Tr(xr) \subseteq \mathbb{Z} \}$. For an $n$-degree number field $K = \mathbb{Q}(\zeta)$, if the power basis $\{1, \zeta, \ldots, \zeta^{n-1}\}$ is an integral basis of $R$, such as cyclotomic number field, then the (absolute) discriminant $\Delta_K$ of $K$ is equal to $(\det(V))^2$. Particularly, we have $\Delta_K \leq n^n$ for general cyclotomic number field $K$ and $\Delta_K = n^n$ for the power-of-two cyclotomic number field $K$. We now define the field tensor product $K_R = K \otimes_{\mathbb{R}} \mathbb{C}$, the torus $\mathbb{T}_g = K_R / (q \mathbb{T})$, and the quotient ring $R_g = R / (q \mathbb{T})$ for some modulus $q$. The coefficient embedding $\tau$ and canonical embedding $\sigma_c$ can be extended to $K_R$, which yields an isomorphism from $K_R$ to $\mathbb{R}^n$ and from $K_R$ to $\mathbb{H}$, respectively. Similarly, the trace $Tr$ and the norm $N$ can also be extended to $K_R$.

#### 2.1.3. Ideals and Modules

An (integral) ideal $\mathcal{I} \subseteq R$ is a nontrivial additive subgroup that is closed under multiplication by $R$, i.e., $r \cdot x \in \mathcal{I}$ for all $(r, x) \in R \times \mathcal{I}$. A fractional ideal $\mathcal{I} \subseteq R$ is a set such that $d \mathcal{I} \subseteq R$ is an integral ideal for some nonzero $d \in R$. Any fractional ideal $\mathcal{I} \subseteq R$ with $\mathbb{Z}$-basis $\{b_1, \ldots, b_n\} \subseteq \mathcal{I}$ embeds into a rank-$n$ lattice $\sigma_{H}(\mathcal{I}) \subseteq \mathbb{R}^n$ with basis $\{\sigma_{H}(b_1), \ldots, \sigma_{H}(b_n)\} \subseteq \sigma_{H}(\mathcal{I})$, which is called ideal lattice. An $R$-module $M \subseteq \mathbb{R}^d$ is a set such that it is closed under addition by $M$ and under multiplication by $R$, where the positive integer $d$ is known as the module rank. If there exists a finite family $\{b_1, \ldots, b_n\}$ of vectors in $K^d$ such that $M = \bigoplus R \cdot b_i$, then $M$ is a finitely generated module. For any finitely generated $R$-module $M \subseteq \mathbb{R}^d$, $M$ embeds into a module lattice $\sigma_{H}(\mathcal{I}) \subseteq \mathbb{R}^n$ (as the map $\sigma_{H}(\mathcal{I})$ is an embedding from $K^d$ to $\mathbb{R}^n$).

#### 2.1.4. Multiplication Matrices

By using the fact by Lyubashevsky et al. [13], the multiplication of elements in $K$ (or $K_R$) is mapped to coordinate-wise multiplication in $\mathbb{H}$: for any $x, y \in K$, $\sigma_c(xy) = \{\sigma_c(x), \ldots, \sigma_c(y)\} = \{\sigma_c(x) \cdot \sigma_c(y)\}$. The multiplication of elements in $K$ or $K_R$ is mapped to coordinate-wise multiplication in $\mathbb{H}$.
Hadamard product (i.e., a coordinate-wise multiplication). It can be further converted to a matrix-vector multiplication as shown by Boudgoust et al. [30, 33]. To be precise, in the canonical embedding setting, we have \( \sigma_c(xy) = \sigma_c(x) \otimes \sigma_c(y) = \text{diag}(\sigma_c(x) \cdot \sigma_c(y)) \) for any \( x, y \in K \). Thus the multiplication matrix in the canonical embedding setting can be defined as \( M_{\sigma_c}(x) = \text{diag}(\sigma_c(x)) \). Moreover, the multiplication matrix corresponding to \( \sigma_H \) can be expressed as \( M_{\sigma_H}(x) = U_H^t M_{\sigma_c}(x) U_H = U_H^t \text{diag}(\sigma_c(x)) U_H \). In the coefficient embedding setting, we also have \( \tau(xy) = M_{\tau}(x) \cdot \tau(y) \), but the expression of \( M_{\tau}(x) \) is more complicated. In detail, \( M_{\tau}(x) = \sum_{i=0}^{n-1} r_k(x) C_i \) where \( C_i \) is the companion matrix of the minimal polynomial \( f \) (see Lemma 2.2 from Boudgoust et al. [31] in more detail). For any matrix \( A = (a_y)_{\mathbb{C}[\alpha_i][j][d] \in K_{\text{mod}}} \), we define the block matrix \( M_{\sigma_c}(A) = \begin{bmatrix} M_{\sigma_c}(a_{00}) & \cdots & M_{\sigma_c}(a_{0n}) \\ \vdots & \ddots & \vdots \\ M_{\sigma_c}(a_{n0}) & \cdots & M_{\sigma_c}(a_{nn}) \end{bmatrix} \) and similarly for \( M_{\sigma_H}(A) \) and \( M_{\tau}(A) \). Note that \( M_{\sigma_c}, M_{\sigma_H}, \) and \( M_{\tau} \) are homomorphisms.

As shown by Boudgoust et al. [30, 33], for a ring of integers \( R \) of an algebraic number field \( K \), let \( L_R \) be a basis of the ideal lattice \( \sigma_H(R) \) and \( B_R = L_R^{-1} \). We can map \( R \) to \( \mathbb{Z}^n \) via \( B_R \cdot \sigma_H \) since any lattice element can be represented by \( L_R \) for some \( a \in \mathbb{Z}^n \). Thus the associated multiplication matrix can be expressed as \( M_{\sigma_H}(x) = B_R M_{\sigma_c}(x) B_R^{-1} = B_R U_H^t \text{diag}(\sigma_c(x)) B_R U_H \). We note that the distribution \( D_{B,c} \) depends only on matrix \( \Sigma = BB^t \) and not on any specific choice of the square root \( B \). Sometimes we also use \( D_{\Sigma,\rho} \) to refer to the Gaussian distribution with covariance matrix \( \Sigma \) in this paper. We typically omit \( c \) when it equals to 0, and denote \( D_{\Sigma,B} \) if the matrix \( B \) is a diagonal matrix (namely, \( B = \text{diag}(r) \) for some \( r = (r_1, \ldots, r_n)^T \) with \( r_i > 0 \)). We also denote \( D_{\Sigma,B} \) by \( D_r \) if \( r_i = \ldots = r_n = r \). In an \( n \)-dimensional lattice \( \Lambda \) and \( t \in \mathbb{R}^n \), we define the discrete Gaussian distribution \( D_{\Lambda+t,B,c}(x) = \rho_{B,c}(x)/\rho_{B,c}(A+t) = \rho_{B,c}(x)/\sum_{y \in \Lambda+t} \rho_{B,c}(y) \) for all \( x \in \Lambda + t \). A sample \( x \in \mathbb{Z}_\Sigma \) from the distribution \( D_{\Lambda+t,B,c} \) is obtained by first sampling each component of \( \sigma_H(x) \in \mathbb{R}^n \) from \( D_r \) over \( \mathbb{R} \) (i.e., \( \sigma_H(x) \sim (D_r)^n \)) and then outputting \( x \) by applying the inverse of \( \sigma_H \). Similarly, a sample \( x \in R \) from the distribution \( D_{\Lambda,t,B,c} \) is obtained by first sampling \( \sigma_H(x) \) from \( D_{\sigma_H(R),t,B,c} \) and then outputting \( x \) by applying the inverse of \( \sigma_H \).

2.3. Blockwise Gaussian Decomposition and Gaussian Convolution. We first recall that the definition of noise lossiness and that the bounds on the noise lossiness gave by Brakerski and Döttling [38] for general secret distributions and distributions over bounded secrets. And then we review some lemmata generalized by Boudgoust et al. [30, 33] that will be instrumental to prove our main theorem.

Definition 1 (Noise lossiness [38]). Let \( B \in \mathbb{R}^{dx \times dn} \) be a non-singular matrix and \( q \geq 2 \) be a modulus. For any distribution \( \mathcal{D} \) over \( \mathbb{Z}_q^d \), and real \( \alpha > 0 \), the noise lossiness \( \nu_{\mathcal{D},B}(\alpha) \) of \( \mathcal{D} \) is defined as \( \nu_{\mathcal{D},B}(\alpha) = \nu_{\mathcal{D},B}(s) = -\log(\Pr_{s \leftarrow \mathcal{D}}[\mathcal{D}(s) = s]) \), where \( s \leftarrow \mathcal{D} \). \( e \leftarrow D_{\mathcal{D},B} \). and \( \mathcal{D}(s) \) is the optimal maximal likelihood decoder for \( s \), namely \( \mathcal{D}(s) = \text{arg max}_{s \in \mathcal{D}} \Pr_{s \leftarrow \mathcal{D}}[s = s] \).

Lemma 1 (Adapted from [38], Lemmas 5.2 and 5.4). Let \( d, n \) and \( q \geq 2 \) be the positive integers, \( \alpha > 0 \) be a Gaussian parameter, and let \( \mathcal{D} \) be a secret distribution over \( \mathbb{Z}_q^d \). Assume that \( \frac{q^2}{\alpha^2} \geq \log(4dn)/\pi \), then it holds that \( \int_{s} \max_{x} \Pr_{x \leftarrow D_{\mathcal{D}}}[y = s + \mathcal{D}(s)]dy \leq 2 \cdot \frac{d^\frac{d}{2}}{\alpha^d} \). Moreover, assume that \( \mathcal{D} \) is \( B \)-bounded, i.e., \( \|s\|_2 \leq B \) for some \( B > 0 \) and \( s \leftarrow \mathcal{D} \), then it holds that \( \int_{s} \max_{x} \Pr_{x \leftarrow D_{\mathcal{D}}}[y = s + \mathcal{D}(s)]dy \leq \exp(\sqrt{2\pi dn \cdot B/\alpha}) \).
Lemma 2 (Blockwise Gaussian Decomposition [30, 33], Lemma 4.1). Let \( d, m, n \) be positive integers, \( F = (F_{ij})_{i \in [n], j \in [d]} \) be a random block matrix where each block \( F_{ij} \in \mathbb{R}^{m \times dn} \) be split with spectral norm upper bound \( s \). Let \( a, b \in \mathbb{R}^d \). Then it holds that the marginal distribution of \( X_{ab} \) is within statistical distance \( 8e \) to \( D_{ab} \). It still holds if \( X_{ab} \) is sample-
from the continuous Gaussian \( D_{ab} \).

Lemma 3 (Gaussian Convolution [39], Theorem 3.1). Let \( \Sigma_1, \Sigma_2 > 0 \) be two positive definite matrices such that \( \Sigma = \Sigma_1 + \Sigma_2 \). Let \( A_1, A_2 \) be two lattices such that \( \sqrt{\Sigma_1} \eta = \eta \chi \) and \( \sqrt{\Sigma_2} \eta = \eta \chi \), respectively. Let \( A_1 \) be the seed, secret and noise distributions over \( \mathbb{Z}_n \) be the ring of integers of an \( n \)-degree number field \( K \), and \( Y \) be the distribution over error distributions on \( K \). Let \( \mathcal{D}, \mathcal{S}, \text{ and } \chi \leftarrow Y \) be the seed, secret, and noise distributions over \( R_{q_{\text{mod}}}^*, R_{q_{\text{mod}}}^* \) and \( K_2 \), respectively. We say that the search MLWE problem \( (\mathcal{D}, \mathcal{S}, \chi, m) \)-MLWE is hard, if it holds for every PPT distinguisher \( \mathcal{A} \) that

\[
\Pr[\mathcal{A}(1^d, \mathcal{A}, \mathcal{S} + e \text{ mod } qR) = \mathbb{1}] \leq \text{negl}(\lambda),
\]

where \( \mathbb{A} \leftarrow \mathcal{D}, s \leftarrow \mathcal{S}, \text{ and } e \leftarrow \chi^m \).

Definition 3 (Module-NTRU). Let \( \lambda \) be the security parameter, \( d, m, n \) be positive integers, and \( R \) be the ring of integers of an \( n \)-degree number field \( K \), and \( Y \) be the distribution over error distributions on \( K \). Let \( \mathcal{D}, \mathcal{S}, \text{ and } \chi \leftarrow Y \) be the seed, secret, and noise distributions over \( R_{q_{\text{mod}}}^*, R_{q_{\text{mod}}}^* \) and \( K_2 \), respectively. We say that the search MLWE problem \( (\mathcal{D}, \mathcal{S}, \chi, m) \)-MLWE is hard, if it holds for every PPT distinguisher \( \mathcal{A} \) that

\[
\Pr[\mathcal{A}(1^d, \mathcal{A}, \mathcal{S} + e \text{ mod } qR) = \mathbb{1}] \leq \text{negl}(\lambda),
\]

Definition 4 (Structured LWE). Let \( \lambda \) be the security parameter, \( d, m, n \) be positive integers, and \( R \) be the distribution over error distributions on \( \mathbb{R}^n \). Let \( \mathcal{D}, \mathcal{S}, \text{ and } \chi \leftarrow Y \) be the seed, secret, and noise distributions over \( R_{q_{\text{mod}}}^*, R_{q_{\text{mod}}}^* \) and \( \mathbb{R}^n \), respectively. We say that the search MLWE problem \( (\mathcal{D}, \mathcal{S}, \chi, m) \)-MLWE is (standard) hard, if it holds for every PPT distinguisher \( \mathcal{A} \) that

\[
\Pr[\mathcal{A}(1^d, \mathcal{A}, \mathcal{S} + e \text{ mod } qR) = \mathbb{1}] \leq \text{negl}(\lambda),
\]

where \( \mathbb{A} \leftarrow \mathcal{D}, s \leftarrow \mathcal{S}, \text{ and } e \leftarrow \chi^m \).

3. Module-LWE, Module-NTRU, and Structured LWE

The MLWE problem was first introduced by Brakerski et al. [6] and studied at length by Langlois and Stébé [16]. Within this work, we will consider the MLWE problem with secret \( s \) lies in \( R_q \) rather than \( \left( R_q^m \right)^d \). Moreover, the NTRU problem was introduced by Hoffstein et al. [40] and it is a core computational assumption in public-key cryptography. For positive integers \( d, m, n, \) and \( q \geq 2 \), we will consider the MLWE problem with secret \( s \) lies in \( R_q \) rather than \( \left( R_q^m \right)^d \). In the following, let \( \text{Pr} \) denote the probability of an event. Let \( A, \mathcal{S}, \text{ and } \mathcal{D} \) be the seed, secret, and noise distributions over \( R_{q_{\text{mod}}}^*, R_{q_{\text{mod}}}^* \), and \( \mathbb{R}_n \), respectively. We say that the search MLWE problem \( (\mathcal{D}, \mathcal{S}, \chi, m) \)-MLWE is (standard) hard, if it holds for every PPT distinguisher \( \mathcal{A} \) that

\[
\Pr[\mathcal{A}(1^d, \mathcal{A}, \mathcal{S} + e \text{ mod } qR) = \mathbb{1}] \leq \text{negl}(\lambda),
\]
Remark 1. Assume that $\mathcal{X} = \mathbb{M}_R(U(R^{m_{\text{cord}}}))$ is the distribution over $\mathbb{Z}_q^{m \times d}$ and define the mapping $\psi = B_R \cdot \sigma_H$, where $B_R$ is the inverse of the known basis of lattice $\sigma_H(R)$. Let $\delta_0$ and $\chi_0$ be the secret and noise distributions over $R_q^d$ and $R_q^d$, respectively. Define $\delta = \psi(\delta_0)$ and $\chi = \psi(\chi_0)$. The works by Boudgoust et al. [30, 33] showed that the MLE problem $\left(U(R^{m_{\text{cord}}}), \delta_0, \chi_0, m\right)$-MLWE is equivalent to the MLE problem $\left(R_q^{m_{\text{cord}}}, \delta, X, \chi, m\right)$-MLWE. Assume that $\Phi$ is a distribution over $R$, and the distribution $\Phi$ over $GL(dn; \mathbb{Z}, q) \times \mathbb{Z}_q^{m \times d}$ is obtained by sampling $\left(\mathbb{M}_R, \mathbb{M}_R(F)\right)$. The works by Boudgoust et al. [30, 33] also showed that the MNTRU problem $\left(\Phi, X, m\right)$-MNTRU is equivalent to the Stn-NTRU problem $\left(\Phi, X, m\right)$-Stn-NTRU.

Definition 5 (Structured NTRU). Let $\lambda$ be the security parameter, $d, m, n$ and $q \geq 2$ be positive integers. Let $\mathcal{X}$ be a distribution of matrices over $\mathbb{Z}_q^{m \times d}$, $\Phi$ be a distribution over $GL(dn; \mathbb{Z}, q) \times \mathbb{Z}_q^{m \times d}$, $(G, F) \sim \Phi$, and $G_{q}^{-1}$ be the $\mathbb{Z}_q$-inverse of $G$ mod $q$. We say that the Str-NTRU problem $(\Phi, \mathcal{X}, m)$-Str-NTRU is hard, if it holds for every PPT distinguisher $\mathcal{B}$ that

$$\Pr[\mathcal{B}(1^d, FG_{q}^{-1}) = 1] - \Pr[\mathcal{B}(1^d, U) = 1] \leq \negl(\lambda),$$

where $U \leftarrow \mathcal{X}$.

For our interest, we now give the formal definitions of the uniform distribution over $R_q^{m_{\text{cord}}}$ and the structured semisemigroup distribution over $\mathbb{Z}_q^{m \times d}$, and then we prove that the MLWE problem with semisemigroup seeds is equivalent to the Stn-LWE problem with semisemigroup seeds.

Definition 7 ($\eta$-Semigroup Distribution). Let $d, m, n$, and $q \geq 2$ be positive integers and $R$ be the ring of integers of an $n$-degree number field $K$. For any real $\eta > 0$, we say that a matrix distribution $\mathcal{M}$ is an $\eta$-semigroup distribution over $R_q^{m_{\text{cord}}}$ if there exists a set of distributions $\{\phi_U\}_{U \in R_q^{m_{\text{cord}}}}$ such that for any randomly chosen matrices $M \leftarrow \mathcal{M}$, $U \leftarrow U(R_q^{m_{\text{cord}}})$, $E_U \leftarrow \phi_U$, we have that

1. $M$ is statistically close to $U - E_U$; and
2. the spectral norm of $E_U$ is upper bounded by $\eta$ with overwhelming probability over the random choices of $U$ and $E_U$.

Definition 8 (Structured $\eta$-Semigroup Distribution). Let $d, m, n$, and $q \geq 2$ be positive integers and $\mathcal{X}$ be a distribution over $\mathbb{Z}_q^{m \times d}$. For any real $\eta > 0$, we say that a matrix distribution $\mathcal{M}$ is an $\eta$-structured semigroup distribution over $\mathbb{Z}_q^{m \times d}$ if there exists a set of distributions $\{\phi_U\}_{U \in R_q^{m_{\text{cord}}}}$ such that for any randomly chosen matrices $M \leftarrow \mathcal{M}$, $U \leftarrow \mathcal{X}$, and $E_U \leftarrow \phi_U$, we have that

1. $M$ is statistically close to $U - E_U$; and
2. the spectral norm of $E_U$ is upper bounded by $\eta$ with overwhelming probability over the random choices of $U$ and $E_U$.

We define the spectral norm $s(E)$ of a matrix $E = (e_{ij})_{i \in [m], j \in [d]} \in R_q^{m_{\text{cord}}}$ as the spectral norm $s(E_{\text{core}})$ of a matrix $E_{\text{core}} \in \mathbb{Q}^{m \times d}$ which is obtained by replacing each element $e_{ij} \in R$ with the transpose of its coefficient embedding $\tau(e_{ij}) \in \mathbb{Q}^{n}$. Note that we can also define the spectral norm of matrix $E$ as the spectral norm $s(E_{\text{can}})$ of a matrix $E_{\text{can}} \in \mathbb{C}^{m \times d}$ which is obtained by replacing each element $e_{ij} \in R$ with the transpose of its canonical embedding $\sigma_{C}(e_{ij}) \in \mathbb{C}^{n}$. In this paper, we use the former, namely $s(E) = s(E_{\text{can}})$.

Notice that the works by Boudgoust et al. [30, 33] and Brakerski and Döttling [34] showed that standard hardness implies mild hardness, and that mild hardness also implies standard hardness for an unbounded number of samples. Although the later holds for an unbounded number of samples (which is not always realistic), we fortunately can generate unbounded number of samples from a fixed number of samples using statistical rerandomization procedures given by Boudgoust et al. [30, 33] and Brakerski and Döttling [34].
of degree $n$, then $s(E_{\text{can}}) \leq \sqrt{n}s(E_{\text{can}})$, $s(M_{\sigma_{t}}(E)) \leq \sqrt{n}s(E_{\text{can}})$, and $s(E_{\text{can}}) \leq \sqrt{n}s(E_{\text{can}})$.

Proof. Define the block matrix $J$ of size $m \times mn$ as follows:

$$
J = \begin{pmatrix}
1 & 0 & \cdots & 0 \\
0 & 1 & \cdots & 0 \\
\vdots & \vdots & \ddots & \vdots \\
0 & 0 & \cdots & 1 \\
\end{pmatrix},
$$

(9)

where $I$ and $0$ are the all-ones and all-zeros row vector of size $n$, respectively. Then we have $J \cdot M_{\sigma_{t}}(E) = E_{\text{can}}$. Moreover, we can calculate $s(J)$ via the definition of the spectral norm, i.e., $s(J) = \sqrt{n}$. Thus using the fact that the spectral norm is submultiplicative, we have that $s(E_{\text{can}}) = s(J \cdot M_{\sigma_{t}}(E)) = s(J) \cdot s(M_{\sigma_{t}}(E)) = \sqrt{n}s(E_{\text{can}})$.

Recall that $M_{\sigma_{t}}(E)$ is the block matrix of size $mn \times dn$ whose each block is the diagonal matrix $\text{diag}(\sigma_{t}(e_{j}))$ of size $n \times n$ for $(i, j) \in [m] \times [d]$. Namely, the matrix $M_{\sigma_{t}}(E)$ can be seen as an $m \times d$ matrix with blocks of size $n \times n$. We then can get an $n \times n$ matrix with blocks of size $m \times d$ by permuting the rows and columns of the matrix $M_{\sigma_{t}}(E)$ to end up with a matrix of size $n \times n$ with blocks of size $m \times d$ only on the diagonal. As shown in the proof of Lemma 2.3 by Boudgoust et al. [31], we define the following permutation $\phi_{k}$ of $[kn]$ for any positive integer $k$. For all $i \in [kn]$, let $i = 1 + k_{1}^{(i)} + n \cdot k_{2}^{(i)}$ with $k_{1}^{(i)} \in [0, \ldots, n - 1]$ and $k_{2}^{(i)} \in [0, \ldots, k - 1]$. Then, define $\phi_{k}(v) = 1 + k_{2}^{(v)} + k \cdot k_{1}^{(v)}$. This is a well-defined permutation based on the uniqueness of the Euclidean division. We can then define the associated permutation matrix $P_{\phi_{k}} = [\delta_{i, \phi_{k}(i)}]_{i \in [kn], j \in [kn]} \in \mathbb{R}^{kn \times kn}$, where $\delta_{i, j}$ is the Kronecker symbol which equals 1 if $i = \phi_{k}(j)$ and 0 otherwise. Then by defining two permutation matrices $P = P_{\phi_{k}} \in \mathbb{R}^{mn \times mn}$ and $Q = P_{\phi_{k}} \in \mathbb{R}^{dn \times dn}$, we have that

$$
P \cdot M_{\sigma_{t}}(E) \cdot Q = \begin{pmatrix}
\sigma_{1}(E) \\
\vdots \\
\sigma_{n}(E)
\end{pmatrix} : = \hat{E} \in \mathbb{C}^{mn \times dn},
$$

(10)

Thus we have that $s(M_{\sigma_{t}}(E)) = s(\hat{E})$ as permutation matrices $P, Q$ are unitary and the unitary matrix preserves the spectral norm.

Recall that

$$
V = \begin{pmatrix}
1 & a_{1} & \cdots & a_{n}^{n-1} \\
1 & a_{2} & \cdots & a_{n}^{n-2} \\
\vdots & \vdots & \ddots & \vdots \\
1 & a_{n} & \cdots & a_{n}^{n-1}
\end{pmatrix} = \begin{pmatrix}
v_{1}^{T} \\
v_{2}^{T} \\
\vdots \\
v_{n}^{T}
\end{pmatrix} \in \mathbb{C}^{n \times n},
$$

(11)

is the Vandermonde matrix of the roots of the minimal polynomial $f$, where $(a_{k})_{k \in [n]}$ is the $n$ distinct roots of $f$.

Define $Z_{k} = I_{d} \otimes v_{k} \in \mathbb{C}^{d \times dn}$ for $k \in [n]$, we have that

$$
\hat{E} = \begin{pmatrix}
E_{\text{can}} Z_{1} \\
\vdots \\
E_{\text{can}} Z_{n}
\end{pmatrix}
$$

(12)

since the canonical embedding and coefficient embedding of each element in $K$ can be linked via the matrix $V$ (see Section 2.1). We then get that the set of singular values of the diagonal matrix $Z := \text{diag}(Z_{1}, \ldots, Z_{n})$ is equal to the union of the set of singular values of matrices $Z_{1}, \ldots, Z_{n}$. Thus, we have that $s(Z) = \max_{k \in [n]} s(Z_{k})$.

As shown in the proof of Lemma 5.7 by Peikert and Pepin [42], let $\alpha = \max_{k \in [n]} |\alpha_{k}| \geq 1$ be the maximum magnitude of all roots of $f$. As $\alpha_{k} = g(a_{k})$ for $k \in [n]$, we have $\alpha_{k} \leq \alpha \cdot A$ by the triangle inequality, thus $\alpha_{k}^{n} \leq A$. Therefore, we have $s(Z_{k}) = ||v_{k}||_{2} \leq \sqrt{n}A^{n} \leq \sqrt{n}A^{n}(1 - \frac{1}{n})$ for all $k \in [n]$, and $s(M_{\sigma_{t}}(E)) = s(\hat{E}) \leq s(E_{\text{can}}) s(Z) \leq \sqrt{n}A^{n}(1 - \frac{1}{n}) s(E_{\text{can}})$.

Finally, combining $s(E_{\text{can}}) \leq \sqrt{n}s(M_{\sigma_{t}}(E))$ with $s(M_{\sigma_{t}}(E)) \leq \sqrt{n}A^{n}(1 - \frac{1}{n}) s(E_{\text{can}})$, we have $s(E_{\text{can}}) \leq \sqrt{n}A^{n}(1 - \frac{1}{n}) s(E_{\text{can}})$.

Alternatively, since the canonical embedding and coefficient embedding of each element in $K$ can be linked via the matrix $V$, we have $E_{\text{can}} = E_{\text{can}} \cdot (I_{d} \otimes V^{T})$. Hence, we also get that $s(E_{\text{can}}) \leq s(E_{\text{can}}) s(V) \leq nA^{n}(1 - \frac{1}{n}) \leq nA^{n}(1 - \frac{1}{n}) s(E_{\text{can}})$ as $s(V) \leq n \max_{i \in [n], j \in [n]} |v_{j}^{(i)}| \leq n A^{n}(1 - \frac{1}{n})$, where $v_{j}^{(i)}$ is an element in the $i$th row and $j$th column of matrix $V$.

Moreover, if $K$ is a cyclotomic number field of degree $n$, then $\alpha = 1$, $s(Z) = ||v_{k}||_{2} = \sqrt{n}$ and $s(V) \leq n$. Therefore, we have that $s(M_{\sigma_{t}}(E)) \leq \sqrt{n}A^{n}(1 - \frac{1}{n})$ and $s(E_{\text{can}}) \leq \sqrt{n}A^{n}(1 - \frac{1}{n})$.

Lemma 7. Let $d, m, n, t$ and $q \geq 2$ be positive integers, $R$ be the ring of integers of an $n$-degree number field $K$, $B_{\text{can}}$ be the inverse of a known basis of ideal lattice $\sigma_{t}(R)$, and $\mathcal{X} = M_{\text{can}}(U(R_{\text{mod}}))$ be the distribution over $Z_{\text{mod}}$, where $\sigma_{t}$ and $M_{\text{can}}$ are defined in Section 2.1. Let $D_{\theta_{0}}, \theta_{0}$ and $\chi$ be the seed, and secret and noise distributions over $Z$, respectively. Define $\mathcal{Q} = M_{\text{can}}(D_{\theta_{0}})$, $\theta = B_{\text{can}} \cdot \sigma_{t}(\theta_{0})$, and $\chi = B_{\text{can}} \cdot \sigma_{t}(\chi_{0})$. Then we have that the MLWE problem with $\eta$-semiuniform seeds $(\mathcal{Q}, \theta_{0}, \chi_{0}, m)$-MLWE$_{K,n,q}$ is equivalent to the Str-LWE problem with $\eta$-str-semiuniform seeds $(\mathcal{Q}, \theta_{0}, \chi_{0}, m)$-Str-LWE$_{K,n,q}$ where $\eta' = \eta^{\sqrt{n}A^{n}(1 - \frac{1}{n})}$, $s(B_{\text{can}}) \cdot s(\hat{B}_{\text{can}})$ and $A$ is defined as in Lemma 6.

Proof. By Remark 1, it suffices to show that $D_{\theta_{0}}$ can be transformed into a str-semiuniform distribution $\mathcal{Q}$ by applying ring homomorphism $M_{\text{can}}$. For the $\eta$-semiuniform seed distribution $D_{\theta_{0}}$ over $R_{\text{mod}}$, we have $A_{\text{can}}(U - E_{\text{can}})$ and $s(E_{\text{can}}) \leq \eta$ by Definition 7, where $A_{\text{can}} \leftarrow D_{\theta_{0}}, U \leftarrow U(R_{\text{mod}})$, and $E_{\text{can}} \leftarrow \phi_{\text{U}}$.

Then, we have $M_{\text{can}}(A_{\text{can}}, U - E_{\text{can}}) = M_{\text{can}}(U) - M_{\text{can}}(E_{\text{can}})$.
due to statistical closeness is preserved by any function, and $M_{qR}(E_U) = (B_{R^q}^{-1} (I_q \otimes U_{qR})) M_{qR} (E_U) (B_{R^q}^{-1} (I_q \otimes U_{qR}))^{-1}$. Since $M_{qR}(U)$ is distributed according to $X = M_{qR}(U(R_q^{mod}))$ for $U \leftarrow U(R_q^{mod})$, $M_{qR}(E_U)$ is distributed according to $M_{qR} (\phi_U)$, and $s(M_{qR}(E_U)) \leq s(B_{R^q}) \cdot s(M_{qR} (E_U)) \cdot s(B_{R^q}^{-1}) \leq \eta \sqrt{n} A^{n/(n-1)} \cdot s(B_{R^q}) \cdot s(B_{R^q}^{-1})$, where the first inequality follows from the facts that the spectral norm is submultiplicative and that the unitary matrix $U_R$ preserves the spectral norm, and the second inequality follows from Lemma 6. Therefore, the $\eta$-semiuniform seed distribution $\mathcal{D}_0$ over $R_q^{mod}$ can be transformed into the $\eta \sqrt{n} A^{n/(n-1)} \cdot s(B_{R^q}) \cdot s(B_{R^q}^{-1})$-str-semiuniform seed distribution $\mathcal{D} = M_{qR}(\mathcal{D}_0)$ over $Z_q^{mod}$. The other direction simply consists in using the inverse mapping of $M_{qR}$ since $M_{qR}$ is an invertible mapping. This completes the proof.

Denoted by $[x]$ the closest integer to $x \in \mathbb{R}$. For any positive integers $p, q$, define the modulus switching function $[ \cdot ]_{q \rightarrow p}: \mathbb{Z}_q \rightarrow \mathbb{Z}_p$ which maps $x \in \mathbb{Z}_q$ to $[x]_{q \rightarrow p} = \lfloor x/q \rfloor \cdot x \mod p$. Note that this modulus switching function can be naturally extended to matrices, vectors as well as ring elements via a component/coefficient-wise way. For better understanding the semiuniform distribution $\phi_U$ over $R_q^{mod}$, we give an example for it and give the upper bound of the spectral norm of $E_U \leftarrow \phi_U$.

Definition 9. Let $d, m, n$ be the positive integers, $p, q$ be moduli, $K = \mathbb{Q}(\xi)$ be a number field of degree $n$ and $R$ be its ring of integers. We define the distribution $\phi_U$ over $R_q^{mod}$ as follows: choose $U \leftarrow U(R_q^{mod})$; compute $U = [U]_{q \rightarrow p}$ and $U' = [U]_{p \rightarrow q}$; output $E_U = U - U'$. 

Lemma 8. Let $d, m, n$ be the positive integers, $p, q$ be moduli, $K$ be a number field of degree $n$, and $R$ be its ring of integers. Let the distribution $\phi_U$ be defined as Definition 9. Then it holds that $s(E_U) \leq \lfloor q/2p \rfloor \cdot \sqrt{d}mn$.

Proof. Recall that the spectral norm $s(E)$ of vector $E = (e_j)_{j \in [m], j \in [d]} \in \mathbb{R}^{mod}$ is defined as the spectral norm $s(E_{e_{\text{ord}}})$ of a matrix $E_{e_{\text{ord}}} \in \mathbb{Q}^{mod}$ which is obtained by replacing each element $e_j \in R$ with the transpose of its coefficient embedding $e_{j_{\text{ord}}} \in \mathbb{Q}^{n}$. From Definition 9, we know that the absolute value of each coefficient of $E_U$ is upper bounded by $\lfloor q/2p \rfloor$ for $E_U \leftarrow \phi_U$. This is because $U = p/q \cdot U + E_U \mod p$ for some $E_U$, where the absolute value of each coefficient of $E_U$ is upper bounded by $1/2$, and $U' = U = [p/q \cdot U + E_U]_{p \rightarrow q} = U = [q/p E_U']$. Thus we have that $s(E_U) \leq \lfloor q/2p \rfloor \cdot \sqrt{d}mn$. This completes the proof.

Remark 2. Let $\mathcal{D}$ be the rounded uniform seed distribution over $R_q^{mod}$ which is obtained by first sampling $U \leftarrow U(R_q^{mod})$ and $E_U \leftarrow \phi_U$, and then outputting $U - E_U$. It is easy to check that $\mathcal{D}$ is a $\eta$-semiuniform distribution with $\eta = \lfloor q/2p \rfloor \cdot \sqrt{d}mn$.

We now review and adapt the notion of sometimes lossy pseudorandom distribution defined by Boudgout et al. [30, 33] in the following.

Definition 10 (Adapted from Boudgout et al. [30, 33], Definition 7). Let $\lambda$ be the security parameter, $d, m, n$ and $q \geq 2$ be positive integers, and $\eta, \epsilon > 0$ be reals. Let $\mathcal{Y}$ be a distribution over $Z_q^{mod}$, $\mathcal{D}$ be a $\eta$-str-semiuniform distribution over $Z_q^{mod}$, $\mathcal{S}$ be a secret distribution over $Z_q$, and $\mathcal{X}$ be a noise distributions over $\mathbb{R}^n$. We say that $\mathcal{Y}$ is a sometimes lossy pseudorandom distribution for $(\mathcal{D}, \mathcal{S}, \mathcal{X})$ if there exists $\epsilon = o(\log(\lambda))$ and $\nu \geq 1/\text{poly}(\lambda)$ such that the following properties hold

(1) Pseudorandomness: $\mathcal{Y}$ is computationally indistinguishable from $\mathcal{D}$,

(2) Sometimes Lossiness: $\Pr_{\lambda \leftarrow \mathcal{Y}} [H_{\mathcal{S}}(\mathcal{S}|A, \mathcal{S} + e \mod q) \geq k] \geq \nu$, where $s \leftarrow \mathcal{S}$ and $e \leftarrow \mathcal{X}^m$.

4. Structured LWE with Str-Semiuniform Seeds

In this section, we first adapt Theorem 2 by Boudgout et al. [30, 33] to state that the existence of a sometimes lossy pseudorandom distribution implies the mild hardness of the structured LWE with str-semiuniform seeds. The proof of Lemma 9 is similar to that of Theorem 2 by Boudgout et al. [30, 33], and we omit it in this work due to the limitation of space. We then give sufficient conditions to construct such distribution. In the following, we will omit “mod $q$” from the expression for convenience.

Lemma 9 (Adapted from Boudgout et al. [30, 33], Theorem 2). Let $\lambda$ be the security parameter, $d, m, n$ and $q \geq 2$ be positive integers, and $\eta, \epsilon > 0$ be reals. Let $R$ be the ring of integers of an $n$-degree number field $K$, $B_k$ be the inverse of some known basis of lattice $\sigma_{H}(R)$, and define $B_{p,k} = I_q \otimes B_k$ for any positive integer $k$. Let $\mathcal{D}$ be a $\eta$-str-semiuniform distribution over $Z_q^{mod}$, $\mathcal{S}$ be a secret distribution over $Z_q$, and $\mathcal{X}$ be an error distribution supported over $\mathbb{R}^n$. We assume that all the distributions are efficiently sampleable. If the distribution $\mathcal{Y}$ is a sometimes lossy pseudorandom distribution for $(\mathcal{D}, \mathcal{S}, \mathcal{X})$, then the Str-LWE problem $(\mathcal{D}, \mathcal{S}, \mathcal{X}, \mathcal{M})$-Str-LWE is mildly hard.

Theorem 3. Let $\lambda$ be the security parameter, $d, m, n$ and $q \geq 2$ be positive integers, and $\alpha, \chi, \epsilon_1, \chi_2, \eta_0 > 0$ be reals. Let $R$ be the ring of integers of an $n$-degree number field $K$, $B_k$ be the inverse of some known basis of lattice $\sigma_{H}(R)$, and define $B_{p,k} = I_q \otimes B_k$ for any positive integer $k$. Let $\mathcal{D}$ be a $\eta$-str-semiuniform distribution over $Z_q^{mod}$, $\mathcal{S}$ be a secret distribution over $Z_q$, and $\mathcal{X}$ be a distribution over $GL(dn: \mathbb{Z}, q) \times Z_q^{mod}$. For $G \in GL(dn: \mathbb{Z}, q)$, let $G^{-1} \in \mathbb{Q}^{dn}$ be the $\mathbb{Q}$-inverse of $G$, and $G_0 + \mathcal{H}^{mod} = \mathbb{Z}_q$ be the $\mathbb{Z}_q$-inverse of $G$ mod $q$. Let $F = \lfloor F_{ij} (i,j) \in [m][d] \rfloor$ be the block matrix with
block $F_i \in \mathbb{Z}^{m \times n}$. Define the matrices $G' = B_{G'}^{-1}GB_{G'}$ and $F' = B_{F'}^{-1}FB_{F'}$. Assume that if $(G, F) \leftarrow \Phi$ then $s(F(G')^{-1}) \leq s_1$ and $s(G') \leq s_2$ with probability at least $\nu \geq 1/\text{poly}(\lambda)$ over the choice of $(G, F)$. Define the distribution $\mathcal{Y}$ over $\mathbb{Z}_q^{\text{maxdet}}$ by $U - E_U$, where $U = F_{q_1}G_1 \bmod q$ and $E_U \leftarrow \phi_U$ over the random choice of $(G, F) \leftarrow \Phi$, and $\phi_U$ is a distribution over $\mathbb{Z}_q^{\text{maxdet}}$. Let $s(B_{x_i}^T F_{x_i} B_{x_i}) \leq \eta_0$ with overwhelming probability over the random choices of $U$ and $E_U$, and let $a_0 > s_2 \cdot \eta_0 \cdot (\lambda B_{x_i}^T)$ and $\alpha \geq 2^{3/2}a_0 \cdot (s_1 + \eta_0)$. Further assume that $H_\infty(s) \geq \sum_{i=0}^{\lambda} \log \left( \max_{s' \in S} P_{q_i}(y_i - s^* + q\mathbb{Z}^{dn})dy_i \right) + \alpha \log(\lambda)$ for $s \leftarrow \Delta$. Then $\mathcal{Y}$ is a sometimes lossy pseudorandom distribution for $(D, S, D_{ab_k})$ provided that the problem $(\Phi, \mathcal{X}, m)$-Str-NTRU_{d,n,q} is hard.

**Proof.** We followed the methods of Brakerski and Döttling [34] and Boudgoust et al. [30, 33]. Let the distribution $\mathcal{X} = M_{G_k}(U(R_q^{\text{maxdet}}))$, where $M_{G_k}(\cdot)$ is defined in Section 2.1. Consider the following hybrid Str-LWE distributions.

(i) $\mathcal{X}_1$:
- $s \leftarrow \mathcal{D}$
- $A \leftarrow D_{ab_k}$
- $e \leftarrow D_{ab_k}$
- Output $(A, A_s + e)$

(ii) $\mathcal{X}_2$:
- $s \leftarrow \mathcal{D}$
- $U \leftarrow \mathcal{X}$
- $E_U \leftarrow \mathcal{X}$
- if $s(E_U) > \eta_0$, output $\bot$
- $A = U - E_U$
- $e \leftarrow D_{ab_k}$
- Output $(A, A_s + e)$

(iii) $\mathcal{X}_3$:
- $s \leftarrow \mathcal{D}$
- $(G, F) \leftarrow \Phi$
- $U = F_G^{-1}$
- $E_U \leftarrow \phi_U$
- if $s(E_U) > \eta_0$ output $\bot$
- $A = U - E_U$
- $e \leftarrow D_{ab_k}$
- Output $(A, A_s + e)$

We first notice that $\mathcal{X}_1$ is identical to the $(\mathcal{D}, S', D_{ab_k}, m)$-Str-LWE_{d,n,q} experiment. By the assumption that $\mathcal{D}$ is a $\eta$-str-semiuniform distribution over $\mathbb{Z}_q^{\text{maxdet}}$, there exists a set of distributions $\{\phi_U\}_{U \in \mathbb{Z}_q^{\text{maxdet}}}$ such that for any randomly chosen matrix $A \leftarrow \mathcal{D}$, $U \leftarrow \mathcal{X}$, and $E_U \leftarrow \phi_U$, we have that (1) $A$ is statistically close to $U - E_U$, and (2) $s(E_U) \leq \eta$ with overwhelming probability over the random choices of $U$ and $E_U$. Thus, we have that $\mathcal{X}_1$ and $\mathcal{X}_2$ are statistically close.

Next, under the assumption that the problem $(\Phi, \mathcal{X}, m)$-Str-NTRU_{d,n,q} is hard, we have that the matrices $U \leftarrow \mathcal{X}$ and $F_{G_q}^{-1}$ are computationally indistinguishable, where $\Phi$ is a distribution over $GL(dn : \mathbb{Z}_q) \times \mathbb{Z}_q^{\text{maxdet}}$, $(G, F) \leftarrow \Phi$, and $G_{q_1} \in \mathbb{Z}_q^{\text{maxdet}}$ is the $\mathbb{Z}_q$-inverse of $G \bmod q$. Thus $\mathcal{X}_2$ and $\mathcal{X}_3$ are computationally indistinguishable.

From the above analysis, we have that $\mathcal{X}_1$ and $\mathcal{X}_3$ are computationally indistinguishable, provided that the problem $(\Phi, \mathcal{X}, m)$-Str-NTRU_{d,n,q} is hard. Thus, define the distribution $\mathcal{Y}$ over $\mathbb{Z}_q^{\text{maxdet}}$ as $U - E_U$, where $U = F_{G_q}^{-1}$ and $E_U \leftarrow \phi_U$ for $(G, F) \leftarrow \Phi$ and $G_{q_1} \in \mathbb{Z}_q^{\text{maxdet}}$ is the $\mathbb{Z}_q$-inverse of $G \bmod q$. We have that the distributions $D$ and $\mathcal{Y}$ are computationally indistinguishable, that is to say, the pseudorandomness property holds for the distribution $\mathcal{Y}$. To complete the proof, we now show that the sometimes lossiness property also holds for the distribution $\mathcal{Y}$ defined as above.

Fix a secret distribution $\mathcal{D}$ and let $s \leftarrow \mathcal{D}$. Since $G' = B_{G'}^{-1}GB_{G'}$, $F' = B_{F'}^{-1}FB_{F'}$, $s(F(G')^{-1}) \leq s_1$, and $s(B_{x_i}^T F_{x_i} B_{x_i}) \leq \eta_0$. We have $F(G')^{-1} = B_{F'}^{-1}(F(G')^{-1})B_{F'}$, and $s(B_{x_i}^T (F(G')^{-1} - B_{F'}^{-1} F_{x_i} B_{F'})) \leq s(F(G')^{-1} - B_{F'}^{-1} F_{x_i} B_{F'})) \leq \eta_1 + \eta_0$.

Now set $\alpha_1 = 2^{3/2}a_0$, by the assumption that $\alpha \geq 2^{3/2}a_0(\eta_1 + \eta_0)$, we have $\alpha \geq \alpha_1(\eta_1 + \eta_0)$. It holds by Lemma 2 that there exists a distribution $\mathcal{Y}$ over $\mathbb{Z}_q^{\text{maxdet}}$ such that we can equivalently sample $e \leftarrow D_{ab_k} - D_{ab_k}$ by $e = (\lambda G_1^{-1} - E_U)e_1 + e'$, where $e_1 = D_{ab_k} - D_{ab_k}$ and $e' \sim \mathcal{Y}$. Accordingly, given $G_{q_1}^{-1}s + G^{-1}e_1$, $s + e_1$, and $e' \sim \mathcal{Y}_q$, as well as the (fixed) matrices $F \in \mathbb{Z}_q^{\text{maxdet}}$, $G \in GL(dn : \mathbb{Z}_q)$, and $E_U \in \mathbb{Z}_q^{\text{maxdet}}$, we can compute $y = As + e$ as follows:

\[
y = As + e = (U - E_U)s + e = (FG_q^{-1} - E_U)s + e = (FG_q^{-1} - E_U)s + (FG_q^{-1} - E_U)e_1 + e' = F(G_q^{-1}s + G^{-1}e_1) - E_U(s + e_1) + e'.
\]

Then we can bound

\[
\tilde{H}_\infty(s|A, A_s + e) \geq H_\infty(s|G_{q_1}^{-1}s + G^{-1}e_1, s + e_1, e') = \tilde{H}_\infty(s|G_{q_1}^{-1}s + G^{-1}e_1, s + e_1),
\]

where the inequality follows from the fact that conditional entropy is nonincreasing when conditioning on more information, and the equality follows from the fact that $F, G, E_U$, and $e'_1$ are independent of $s$ and $e'_1$.

Set $\alpha_2 = \alpha_1/\sqrt{2} = 2a_0$ and $e_2 \leftarrow D_{\lambda(G)} a_{G, B_{G'}}$ be a discrete Gaussian distribution over lattice $\Lambda(G)$. By the assumption that $a_0 > \tilde{\eta}_1$, we have $\alpha_2 > 2\tilde{\eta}_1 \cdot \Lambda(B_{G'}^{-1}) > \sqrt{2} \tilde{\eta}_1 \cdot \Lambda(B_{G'}^{-1})$. Thus it holds by Lemma 4 that
Multiplying $G^{-1}_q s + G^{-1} e_1$ by $G$ preserves the entropy due to $G^{-1}_q$ is the $Z_q$-inverse of $G$ mod $q$ and $G^{-1}$ is the $\mathbb{Q}$-inverse of $G$, then we have

$$\bar{H}_\infty(s|G^{-1}_q s + G^{-1} e_1, s + e_1) \geq \bar{H}_\infty(s|G^{-1}_q s + G^{-1} e_2, s + e_1).$$  \hspace{1cm} (15)$$

where the inequality follows from the fact that conditional entropy is nonincreasing when conditioning on more information. Since $e'_3 \leftarrow D_{k(G)} - c_3 \mu_{s \Lambda'}$, $e'_3$ is only depends on the lattice coset $e_3 \mod \Lambda(G)$. We then have

$$\bar{H}_\infty(s|s + e_3, e'_3, s + e_1) \geq \bar{H}_\infty(s|s + e_3, s + e_1) - \bar{H}_\infty(e'_3)$$

$$\geq \bar{H}_\infty(s|s + e_3, s + e_1) - dn \cdot \log(s(G')).$$  \hspace{1cm} (18)$$

where the first inequality follows from the entropy chain rule, and the second inequality follows from $\frac{\log |Z_q|!}{\log (s(G'))}$ (using the Hadamard's inequality). Last, we have $\alpha_3/\sqrt{2} = \alpha_0 > \eta_\epsilon \Lambda(B_{R'}^{-1})$. Thus, it holds by Lemma 5 that

$$\bar{H}_{\infty}(s|s + e_3, s + e_1) \geq \bar{H}_\infty(s + e_0, s + e_1),$$  \hspace{1cm} (19)$$

where $e_0 \leftarrow D_{\alpha_0} \mu_{d'}$. Combining the Equations (14)–(19), we get

$$\bar{H}_{\infty}(s|A, As + e) \geq \bar{H}_\infty(s|s + e_0, s + e_1) - dn \cdot \log(s(G'))$$

$$\geq \bar{H}_\infty(s + e_0, s + e_1) - dn \cdot \log(s_2),$$  \hspace{1cm} (20)$$

where the last inequality follows from the assumption that $s(G') \leq s_2$. We now compute

\begin{align*}
\bar{H}_\infty(s|s + e_0 q, s + e_1) &= -\log \left( \sum_{y_0, y_1} \max_{s' \in S} \Pr_{s, e_0, e_1} [s = s' | s + e_0 = y_0, s + e_1 = y_1] \right) \\
&= -\log \left( \int \int P(s + e_0, s + e_1) \cdot \max_{s' \in S} \Pr_{s, e_0, e_1} [s = s' | s + e_0 = y_0, s + e_1 = y_1] dy_0 dy_1 \right) \\
&= -\log \left( \int \max_{s'} P(s + e_0, s + e_1) (s', y_0, y_1) dy_0 dy_1 \right) \\
&= -\log \left( \int \max_{s'} P(s + e_0, s + e_1 = s) (y_0, y_1) \cdot \Pr_{s} [s = s'] dy_0 dy_1 \right) \\
&\geq \bar{H}_\infty(s) - \log \left( \int \int \max_{s'} P(s + e_0, e_1) (y_0, y_1) \cdot \Pr_{s} [s = s'] /\leq 2^{-\delta(s,0)} dy_0 dy_1 \right) \\
&= \bar{H}_\infty(s) - \log \left( \prod_{i=0}^{\infty} \max_{y_i, s'} P(e_0, y_i | s' = s + q^i \mu_{s'}) dy_0 dy_1 \right) \\
&= \bar{H}_\infty(s) - \sum_{i=0}^{\infty} \log \left( \int \max_{y_i, s'} P(e_0, y_i | s' = s + q^i \mu_{s'}) dy_i \right). \hspace{1cm} (21)\end{align*}
with the Equations (20) and (21), we have that \( \tilde{H}_\infty(s)A, As + e \geq o(\log(\lambda)) \) with probability at least \( \nu \geq \text{poly}(\lambda) \). That is to say, the sometimes lossiness property holds for distribution \( \mathcal{Y} \). This completes the proof. \( \square \)

Combining Lemma 9 with Theorem 3, we have the following corollary.

**Corollary 1.** The problem \( (\mathcal{D}, \mathcal{S}, D_{\mathcal{A}}, m)\)-Str-LWE\(_{d,n,q}\) is mildly hard if the conditions of Theorem 3 are satisfied.

### 5. Instantiation for Semiuniform R/MLWE Problem

In this section, we first review the result by Boudgoust et al. [30, 33] which gave the density of \( g \leftarrow D_{\mathcal{R}, \beta} \) that are invertible module \( q\mathcal{R} \) and the definition of the distribution \( \Phi \), and then we define the distribution \( \Phi_\mathcal{U} \) over \( \mathbb{Z}_q^{\text{mod}} \). Finally, we give the instantiation for the search R/MLWE problem.

**Lemma 10** (Adapted from Boudgoust et al. [30, 33], Theorem 4). Let \( K \) be the \( \nu \) th cyclotomic number field of degree \( n = \varphi(n) \) and \( \mathcal{R} \) be its ring of integers, where \( \varphi(\cdot) \) is the Euler’s totient function. Let integer \( d \geq 1 \) and \( q > 2n \) be a prime satisfying \( q = 1 \mod n \). Assume that \( \beta \geq 2^{1/(2d-1)} \cdot (\Delta_n \cdot q^{-d/(d-1)(2d-1)})^{1/n} \). Then \( \Pr_{G \leftarrow D_{\mathcal{R}, \beta}^{\text{mod}}}[G \notin GL(d; R, q)] \leq 2n/q + \text{negl}(n) \).

**Definition 11** (Boudgoust et al. [30, 33], Definition 8). Let \( d, m, n, q \geq 2 \) be positive integers, \( m \) be the ring of integers of an \( n \)-degree number field \( K \), and \( \mathcal{R} \) be the ring of integers of a Gaussian parameter. We define the distribution \( \Phi \) as follows: choose \( G \leftarrow D_{\mathcal{R}, \beta}^{\text{mod}} \) such that \( G \in GL(d; R, q) \); choose \( F \leftarrow D_{\mathcal{R}, \beta}^{\text{mod}} \); output \( \langle \mathcal{M}_R(G), \mathcal{M}_R(F) \rangle \).

**Remark 3.** The works by Boudgoust et al. [30, 33] showed that Lemma 10 still holds for any number field \( K \) and for any unramified prime \( q > 2n \), and that \( \Phi \) is efficiently sampleable if \( \beta \) is large enough, where \( \beta \) depends on the splitting behavior of modulus \( q \). Particularly, if \( q = 1 \mod \nu \) for the \( \nu \)th cyclotomic field, then \( q \mathcal{R} \) fully splits into the product of \( n \) distinct prime ideals of norm \( q \) and \( \Delta_n \leq n^c \). Thus we can choose \( \beta = \Theta(n) \) and have a nonnegligible probability that a sample from \( D_{\mathcal{R}, \beta}^{\text{mod}} \) is also in \( GL(d; R, q) \) for a fully split prime \( q \) in cyclotomic field \( K \). The works by Boudgoust et al. [30, 33] and Brakerski and Döttling [34] also provided another distribution \( \Phi \) that is different from the distribution defined in Definition 11 to highlight the tradeoff between the underlying hardness assumptions and the parameters. In this paper, we do not focus on the different distribution defined by Boudgoust et al. [30, 33] and Brakerski and Döttling [34] and defer readers by Boudgoust et al. [30, 33] and Brakerski and Döttling [34] for more details.

**Lemma 11** (Boudgoust et al. [30, 33], Lemma 8). Let \( d, m, n \) be the positive integers, \( q \geq 2 \) be a modulus, and \( \beta \in \mathbb{R}^+ \) be a Gaussian parameter. Let \( \mathcal{R} \) be the ring of integers of an \( n \)-degree number filed \( K \). Let \( \langle \mathcal{M}_R(G), \mathcal{M}_R(F) \rangle \leftarrow \Phi \), where the distribution \( \Phi \) is defined as in Definition 11. It holds that

\[
\begin{align*}
&\Pr\left( \exists (\mathcal{M}_R(G), \mathcal{M}_R(F)) \right) \\
\leq d\beta(\log(\log(\lambda))) &\leq d\beta(\log(\log(\lambda)))
\end{align*}
\]

\((22)\)

\( \square \)

Combining Lemma 9 with Theorem 3, we have the following corollary.

**Corollary 1.** The problem \( (\mathcal{D}, \mathcal{S}, D_{\mathcal{A}}, m)\)-Str-LWE\(_{d,n,q}\) is mildly hard if the conditions of Theorem 3 are satisfied.
the MLWE problem with the rounded uniform seed distribution $\mathcal{D}$ is equivalent to the Str-LWE problem with str-semiuniform seed distribution $M_{R,K}(\mathcal{D})$ via a specific connection between the distributions by Lemma 7. Hence, we have the following theorem by combining Lemmas 11 and 12 with Corollary 1.

**Theorem 4.** Let $d$, $m$, $n$, $t$ be the positive integers with $t < n$, $p$, $q$ be moduli, $\alpha$, $\alpha_0 > 0$ be reals, and $\beta \in \mathbb{R}^+$ be a Gaussian parameter such that $D_{GL(B,R,q),\beta}$ is efficiently sampleable. Let $R$ be the ring of integers of an $n$-degree number filed $K$, and $B_0$ be the inverse of the basis of lattice $\sigma_{H}(R)$. Let $\mathcal{D}$ be the rounded uniform seed distribution over $\mathbb{R}^n_{mod}$ defined as in Remark 2, $\delta'$ be a secret distribution over $R_{n}^{d}$, and define $\delta'' = \mathbf{B}_R \cdot \sigma_{H}(\delta')$. Let $\alpha_0 > d\beta \log(n) \cdot \eta_{\epsilon}(R^t)$ and $\alpha \geq 2^{3/2} n \sqrt{dn} \alpha_0 \cdot (\sqrt{dn} \log(n) + \lceil \log(q/2p) \rceil \cdot A_{\eta_{\epsilon}(\log(\lambda))}$, where $A$ is defined as in Lemma 6. Further assume that $H_\infty(\delta') \geq \sum_{s=0}^{n} \log \left( \prod_{i=1}^{n} \max_{r < s'} \mathbf{p}_e(y_i - s + \sqrt{q} \mathbf{e}_{n}) \right) + dn \log(n) + o(\log(\lambda))$ for $\delta' \rightarrow \delta''$. Then the search MLWE problem $(\mathcal{D}, \delta', D_{\mathbb{K}_{a}, \eta_{\epsilon}(R^t)})$-MLWE$_{K,d,n,q}$ is mildly hard, provided that the MNTRU problem $(D_{R,\beta,m})$-MNTRU$_{R,d,n,q}$ is hard.

We can choose $B_R = (U_{n}^{T}, V)^{-1}$ which yields $\mathbf{B}_R \cdot \sigma_{H} = \tau$ in cyclotomic number field $K$ as discussed in Section 2.1. We then know that $\|s\|_2 = \|B_R \cdot \sigma_{H}(s)\|_2 = \|s\|_2 \leq \sqrt{dn} \cdot (r - 1) = B$ for $s \leftarrow \delta'$ and $s' \leftarrow \delta''$, where $\delta'$ is supported on $R_{n}^{d}$ for some positive integer $r \geq 2$. Note that distributions $\delta'$ and $\delta''$ have the same entropy due to $\tau$ is a bijection, and $\alpha_1 = 2^{3/2} \alpha_0$ (see the proof of Theorem 3). Combining with Lemmas 1 and 10 and Theorem 4, we have the following corollary for cyclotomic number field $K = \mathbb{Q}(\zeta)$.

**Corollary 2.** Let $R$ be the ring of integers of the $n$th cyclotomic number filed $K$ of degree $n = \phi(n)$, and $B_0$ be the inverse of the basis of lattice $\sigma_{H}(R)$. Let $d$, $m$, $n$, $t$ be positive integers, modulus $q > 2n$ be a prime satisfying $q = 1 \mod n$, $\alpha_0 > 0$ be reals, and Gaussian parameter $\beta > 2n$. Let $\mathcal{D}$ be the rounded uniform seed distribution over $\mathbb{R}^n_{mod}$ defined as in Remark 2, $\delta'$ be a secret distribution over $R_{n}^{d}$, and define $\delta'' = \tau(\delta')$. Let $\alpha \geq 2^{3/2} n \sqrt{dn} \alpha_0 \cdot (\sqrt{dn} \log(n) + \lceil \log(q/2p) \rceil \cdot A_{\eta_{\epsilon}(\log(\lambda))}$, where $A$ is defined as in Lemma 6. Further assume that for $d\beta \log(n) \cdot \eta_{\epsilon}(R^t)<\alpha_0 \leq 2^{3/2} q \cdot \sqrt{\pi} / \log(4dn)$, it holds that $H_\infty(\delta') \geq 2dn \log(q/\alpha_0) + dn \log(d\beta \log(n)) - \frac{3}{2} dn + o(\log(\lambda))$.

Then the search MLWE problem $(\mathcal{D}, \delta', D_{\mathbb{K}_{a}, \eta_{\epsilon}(R^t)})$-MLWE$_{K,d,n,q}$ is mildly hard, provided that the MNTRU problem $(D_{R,\beta,m})$-MNTRU$_{R,d,n,q}$ is hard.

Furthermore, if $\delta'$ is supported on $R_{n}^{d}$ for some positive integer $r \geq 2$, and for $\alpha_0 > d\beta \log(n) \cdot \eta_{\epsilon}(R^t)$ it holds that $H_\infty(\delta') \geq \sqrt{2\pi} \cdot \left( 1 + 2^{-3/2} \cdot (r - 1) - \log(\epsilon) \right) \cdot \log(\lambda)$

Then the conclusion is also holds.

Since the above definitions and results for MLWE problem can still be hold for the rank $d = 1$, we have the following theorem and corollary for the computational RLWE problem $(\mathcal{D}, \delta', D_{\mathbb{K}_{a}, \eta_{\epsilon}(R^t)})$-RLWE$_{K,d,n,q}$.

**Theorem 5.** Let $m$, $n$, $t$ be the positive integers with $t < n$, $p$, $q$ be moduli, $\alpha$, $\alpha_0 > 0$ be reals, and $\beta \in \mathbb{R}^+$ be a Gaussian parameter such that $D_{GL(B,R,q),\beta}$ is efficiently sampleable. Let $R$ be the ring of integers of an $n$-degree number filed $K$, and $B_0$ be the inverse of the basis of lattice $\sigma_{H}(R)$. Let $\mathcal{D}$ be the rounded uniform seed distribution over $\mathbb{R}^n_{mod}$ defined as in Remark 2, $\delta'$ be a secret distribution over $R_{n}^{d}$, and define $\delta'' = \mathbf{B}_R \cdot \sigma_{H}(\delta')$. Let $\alpha_0 > \beta \log(n) \cdot \eta_{\epsilon}(R)$ and $\alpha \geq 2^{3/2} n \sqrt{dn} \alpha_0 \cdot (\sqrt{dn} \log(n) + \lceil \log(q/2p) \rceil \cdot A_{\eta_{\epsilon}(\log(\lambda))}$, where $A$ is defined as in Lemma 6. Further assume that $H_\infty(\delta') \geq \sum_{s=0}^{n} \log \left( \prod_{i=1}^{n} \max_{r < s'} \mathbf{p}_e(y_i - s + \sqrt{q} \mathbf{e}_{n}) \right) + n \log(\beta \log(n)) + o(\log(\lambda))$ for $\delta' \rightarrow \delta''$. Then the search RLWE problem $(\mathcal{D}, \delta', D_{\mathbb{K}_{a}, \eta_{\epsilon}(R^t)})$-RLWE$_{K,d,n,q}$ is mildly hard, provided that the NTRU problem $(D_{R,\beta,m})$-NTRU$_{R,d,n,q}$ is hard.

**Corollary 3.** Let $R$ be the ring of integers of the $n$th cyclotomic number filed $K$ of degree $n = \phi(n)$, and $B_0$ be the inverse of the basis of lattice $\sigma_{H}(R)$. Let $m$, $n$, $t$ be positive integers, modulus $q > 2n$ be a prime satisfying $q = 1 \mod n$, $\alpha_0 > 0$ be reals, and Gaussian parameter $\beta > 2n$. Let $\mathcal{D}$ be the rounded uniform seed distribution over $\mathbb{R}^n_{mod}$ defined as in Remark 2, $\delta'$ be a secret distribution over $R_{n}^{d}$, and define $\delta'' = \tau(\delta')$. Let $\alpha \geq 2^{3/2} n \sqrt{dn} \alpha_0 \cdot (\sqrt{dn} \log(n) + \lceil \log(q/2p) \rceil \cdot A_{\eta_{\epsilon}(\log(\lambda))}$, where $A$ is defined as in Lemma 6. Further assume that for $\beta \log(n) \cdot \eta_{\epsilon}(R^t)<\alpha_0 \leq 2^{-3/2} q \cdot \sqrt{\pi} / \log(4dn)$, it holds that $H_\infty(\delta') \geq 2n \log(q/\alpha_0) + n \log(\beta \log(n)) - \frac{3}{2} n + o(\log(\lambda))$.

Then the search RLWE problem $(\mathcal{D}, \delta', D_{\mathbb{K}_{a}, \eta_{\epsilon}(R^t)})$-RLWE$_{K,d,n,q}$ is mildly hard, provided that the NTRU problem $(D_{R,\beta,m})$-NTRU$_{R,d,n,q}$ is hard.

Furthermore, if $\delta'$ is supported on $R_{n}^{d}$ for some positive integer $r \geq 2$, and for $\alpha_0 > \beta \log(n) \cdot \eta_{\epsilon}(R)$ it holds that
6. Conclusion and Discussion

In this paper, we gave the formalized definition of the semiuniform distribution. By considering the semiuniform seed distributions such as the rounded uniform distribution, we showed that under specific parameter constraints, the search MLWE problem with semiuniform seeds is as hard as the MNTRU problem as long as the secret distribution has sufficiently large min-entropy. Moreover, due to our results for the search MLWE problem with semiuniform seeds are rank-preserving, we also showed that for the appropriate settings of secret and noise distributions, the search RLWE problem with semiuniform seeds can still be hard under the NTRU assumption. Note that we only proved the search R/MLWE problem with semiuniform seeds are hard under the NTRU/MNTRU assumption in this work, and we leave it as an open problem to prove the decision variants of our problems. One possibility would be to find a search-to-decision reduction for the search R/MLWE problem with semiuniform seeds to prove the decision variants of our problems (note that existing search-to-decision reductions for R/MLWE, e.g., Langlois and Stehlé [16], does not work for nonuniform seeds). We also note that for a special case where the quotient ring \( R_q \) decomposes into a “CRT representation,” the work by Bolboceanu et al. [43] provided a polynomial time reduction from the decisional Bounded Distance Decoding on a Hidden Lattice (HLBDD, namely, a decision variant of BDD problem in which BDD is to be solved on an ideal lattice which is sampled from a large family of ideals) to the decision RLWE problem with a \( k \)-wise independent secret distribution, provided that the standard decision RLWE problem is hard. More precisely, Bolboceanu et al. [43] first exhibited a polynomial time reduction from HLBDD to the decision RLWE problem with single sample using the “noise swallowing” technique (informally, a discrete Gaussian distribution with super-polynomial Gaussian parameter will “eat up” any random variable with polynomial amplitude), and then exhibited a polynomial time reduction from the decision RLWE problem with single sample to the decision RLWE problem with polynomially many samples using a rerandomization technique [35] and the noise swallowing technique. However, the rerandomization technique by Lyubashevsky et al. [35] does not directly work for the decision RLWE problem with semiuniform seeds, and we leave it as an interesting open problem.

Data Availability

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Conflicts of Interest

The authors declare that they have no conflict of interest to this work.

Authors’ Contributions

Wenjuan Jia and Jiang Zhang contributed in formal analysis; Wenjuan Jia contributed in the investigation and writing—original draft; Wenjuan Jia, Baocang Wang, and Jiang Zhang contributed in writing—review and editing; Jiang Zhang contributed in the conceptualization.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China (Grant Nos. 62272362 and U19B2021).

References


