Module Learning With Errors and Structured Extrapolated Dihedral Cosets

Weiqiang Wen and Jinwei Zheng

Telecom Paris, Institute Polytechnique de Paris, Palaiseau 91120, France
{weiqiang.wen,jinwei.zheng}@telecom-paris.fr

Abstract. The Module Learning With Errors (MLWE) problem is the fundamental hardness assumption underlying the key encapsulation and signature schemes ML-KEM and ML-DSA, which have been selected by NIST for post-quantum cryptography standardization. Understanding its quantum hardness is crucial for assessing the security of these standardized schemes.

Inspired by the equivalence between LWE and Extrapolated Dihedral Cosets Problem (EDCP) in [Brakerski, Kirshanova, Stehlé and Wen, PKC 2018], we show that the MLWE problem is as hard as a structured variant of the EDCP, which we refer to as the Integer Polynomial Module EDCP (IP-M-EDCP). This extension from EDCP to IP-M-EDCP relies crucially on the algebraic structure of the ring underlying MLWE: the extrapolation depends not only on the noise rate, but also on the ring's degree. In fact, an IP-M-EDCP state forms a superposition over an exponential (in ring degree) number of possibilities. Our equivalence result holds for MLWE defined over power-of-two cyclotomic rings with constant module rank, a setting of particular relevance in cryptographic applications. Moreover, we present a reduction from IP-M-EDCP to EDCP. Therefore, to analyze the quantum hardness of MLWE, it may be advantageous to study IP-M-EDCP, which might be easier than EDCP.

Keywords: Module Learning with Errors · Extrapolated Dihedral Cosets · Quantum Hardness.

© IACR 2026. This article is the full revision of the version to be published by Springer-Verlag in the proceedings of CRYPTO 2026.

Table of Contents

1 Introduction . . . 3
2 Technical Overview . . . 6
2.1 Reduction from P-MLWE to IP-M-EDCP . . . 8
2.2 Reduction from IP-M-EDCP to P-MLWE . . . 10
2.3 Increasing the Number of Samples . . . 12
2.4 Reduction from IP-M-EDCP to EDCP . . . 13
2.5 Open Problems . . . 14
3 Preliminaries . . . 14
3.1 Lattices . . . 15
3.2 Algebraic Number Theory . . . 16
3.3 Rényi Divergence . . . 18
3.4 Gaussian and Discrete Gaussian Distributions . . . 19
3.5 Module Learning with Errors Problems . . . 22
3.6 Properties about the Connections between $\mathbb{Z}_{f(q)}$ and $\mathbb{Z}_q[x]/f$ . . . 23
3.7 Quantum Computation . . . 25
3.8 Extrapolated Dihedral Cosets Problems . . . 27
4 Reduction from IP-M-EDCP to P-MLWE . . . 28
4.1 Reduction from G-IP-M-EDCP to *q-adic* IP-MLWE . . . 29
4.2 Reduction from *q-adic* IP-MLWE with discrete Gaussian errors to *q-adic* IP-MLWE with errors from $D + U$ . . . 30
4.3 Reduction from *q-adic* IP-MLWE to P-MLWE . . . 32
4.4 Main Theorem . . . 35
5 Reduction from P-MLWE to stEDCP . . . 38
5.1 Amplification of the Sample Number . . . 38
5.2 Reduction from MLWE to G-IP-M-EDCP . . . 42
6 Reduction from IP-M-EDCP to EDCP . . . 45
A Supplementary Materials for Failure of the Reduction from P-MLWE to M-EDCP . . . 49
B Supplementary Materials for Preliminaries . . . 50
B.1 Missing Proofs for Gaussian and Discrete Gaussian Distribution . . . 50
B.2 Transformations between LWE with Continuous Gaussian Distribution and Discrete Gaussian Distribution . . . 57
B.3 Transformations between MLWE and P-MLWE . . . 58
B.4 More Properties about the Connections between $\mathbb{Z}_{f(q)}$ and $\mathbb{Z}_q[x]/f$ . . . 61
B.5 Equivalence between LWE and EDCP . . . 63
C Supplementary Materials for Reduction from G-IP-M-EDCP to MLWE . . . 64
C.1 Trace Distance Needed in the Proof of Lemma 25 . . . 64
C.2 Computation of the Carries . . . 66
C.3 Proof of Lemma 26 . . . 68
C.4 Proof of Lemma 27 . . . 71
D Supplementary Materials for Reduction from MLWE to G-IP-M-EDCP . . . 79
D.1 Invertible Submatrix in the Matrix $\mathbf{A}(x) \in (\mathcal{O}_K/q\mathcal{O}_K)^{m\times n}$ . . . 79
D.2 Regularity Lemma . . . 79
D.3 Statistical Distance Between $\mathbf{A}(q) \bmod f(q)$ and $U(\mathbb{Z}_{f(q)}^{m\times n})$ . . . 80
D.4 The Size of Error Terms . . . 81
D.5 Reduction for any module rank n . . . 82
E Supplementary Materials for the reduction from IP-M-EDCP to EDCP . . . 84

1 Introduction

The Learning with Errors (LWE) problem was first introduced by Regev in [Reg05,Reg09]. The $\mathsf{LWE}_{q,\alpha}^{m,n}$ with parameters $m, n, q \in \mathbb{Z}$ and $\alpha \in (0,1)$ involves recovering a secret vector $\mathbf{s} \in \mathbb{Z}_q^n$, given m samples of the form $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \bmod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\mathbf{a}_i$ is randomly chosen from $\mathbb{Z}_q^n$ and e_i is sampled from $\mathcal{D}_{\mathbb{Z},\alpha q}$, which is the discrete Gaussian distribution with standard deviation parameter αq (i.e., $\mathcal{D}_{\mathbb{Z},\alpha q}(x) \sim \exp(\pi x^2/(\alpha q)^2)$ for all $x \in \mathbb{Z}$).

In [Reg05], Regev provided a reduction from the LWE problem to the Dihedral Coset Problem (DCP), which involves recovering a hidden shift s given multiple samples of the quantum state $\{|0, x_i\rangle + |1, x_i + s\rangle\}_{i \leqslant m}$ for some integer m. However, the existence of a reduction in the inverse direction remains an open question. Later, in [BKSW18], Brakerski et al introduced the Extrapolated Dihedral Coset Problem (EDCP). An instance of $\mathsf{EDCP}_{q,\phi}^{m,n}$, for integer parameters m, n and q, and a function $\phi : \mathbb{Z} \mapsto \mathbb{C}$, consists of m quantum states:

$$\left\{ \sum_{j \in \mathbb{Z}} \phi(j) \, |j, \mathbf{x}_i + j \cdot \mathbf{s} \bmod q\rangle \right\}_{i \leqslant m}, \tag{1}$$

where $\mathbf{x}_i$'s are random and independent in $\mathbb{Z}_q^n$, and $\mathbf{s} \in \mathbb{Z}_q^n$. Given such instance, EDCP asks to recover the secret $\mathbf{s}$. When $\phi(j) = \sqrt{\mathcal{D}_{\mathbb{Z},r}(j)}$, we denote the problem as $\mathsf{G\text{-}EDCP}_{q,\phi}^{m,n}$, which is proved to be equivalent to LWE with discrete Gaussian errors. To date, no subexponential-time quantum algorithm in n is known for solving EDCP with parameters enabling a reduction from LWE, supporting the post-quantum hardness of LWE-based cryptography.

However, the application of LWE introduces significant communication overhead, posing efficiency challenges. To address this issue, Stehlé et al and Lyubashevsky et al introduced the Polynomial Learning with Errors (PLWE) problem in [SSTX09] and Ring Learning with Errors (RLWE) problem in [LPR10], respectively. The PLWE problem denoted by $\mathsf{PLWE}_{q,r,f}^{m}$ is defined for integer parameters m and q, a number $\alpha \in (0,1)$, and a polynomial f of degree d, as recovering the secret $s \in \mathbb{Z}_q[x]/f(x)$ from the given samples: $(\mathbf{a}, \mathbf{a}s + \mathbf{e}) \in (\mathbb{Z}_q[x]/f)^m \times (\mathbb{Z}_q[x]/f)^m$, where $\mathbf{a}$ is randomly chosen from $U((\mathbb{Z}_q[x]/f)^m)$ and the coefficient vector of each entry of $\mathbf{e}$ is selected from $\mathcal{D}_{\mathbb{Z}^d,\alpha q}$ (i.e., $\mathcal{D}_{\mathbb{Z}^d,\alpha q}(\mathbf{x}) \sim \exp(\pi \|\mathbf{x}\|^2/(\alpha q)^2)$ for all $x \in \mathbb{Z}^d$). The RLWE problem denoted by $\mathsf{RLWE}_{q,\alpha,f}^{m}$ is defined for parameters $m, q \in \mathbb{Z}$ and a polynomial f, as recovering the secret $s \in \mathcal{O}_K$ from the given samples: $(\mathbf{a}, \mathbf{a}s + \mathbf{e}) \in (\mathcal{O}_K/q\mathcal{O}_K)^m \times (\mathcal{O}_K/q\mathcal{O}_K)^m$, where $K = \mathbb{Q}[x]/f$ is a number field with $\mathcal{O}_K$ as its ring of integers, $\mathbf{a}$ is chosen from $U((\mathcal{O}_K/q\mathcal{O}_K)^m)$, each entry of $\mathbf{e}$ is selected from the discrete Gaussian distribution[0] over $\mathcal{O}_K$ with deviation parameter αq. In [RSW18], Roşca et al showed that RLWE is as hard as PLWE for a large family of rings. When the vector $\mathbf{a}$ is generalized to a matrix $\mathbf{A} \in (\mathcal{O}_K/q\mathcal{O}_K)^{m \times n}$ and the secret s is extended to a vector $\mathbf{s} \in (\mathcal{O}_K/q\mathcal{O}_K)^n$ for $n \geqslant 1$, the problem becomes the

[0] In fact, an embedding to the real space is involved for sampling a ring element according to Gaussian distribution. We omit it here for simplicity.

Module LWE ($\mathsf{MLWE}^{m,n}_{q,\alpha,f}$) problem, which is introduced in [BGV12] and later extensively studied in [LS15]. A polynomial variant of this, referred to as Polynomial MLWE ($\mathsf{P\text{-}MLWE}^{m,n}_{q,\alpha,f}$), can also be defined analogously. MLWE offers more flexibility than RLWE in parameter selection, making it a leading choice for the building of post-quantum key encapsulation and signature schemes, such as in ML-KEM [BDK+18] and ML-DSA [DKL+18].

There is a common concern that MLWE might be easier than LWE due to the algebraic structure of MLWE. Existing algorithms for solving LWE or EDCP have not yet exploited the algebraic structure of the ring $\mathcal{O}_K$. This raises the following key question:

- ⋆ Is there a quantum problem that is potentially easier than EDCP yet still equivalent to the MLWE problem?

Since MLWE and RLWE are structured variants of LWE, the corresponding variants of EDCP should also reflect the underlying ring structure. We denote this kind of EDCP as structured EDCP (stEDCP).

A natural candidate is obtained by considering a ring analogue of EDCP. Since EDCP is as hard as LWE for suitable parameters, one may replace the integers in (1) with elements of the polynomial ring $\mathbb{Z}[x]/f$. This leads to quantum states of the form

$$\sum\nolimits_{c\in\mathbb{Z}[x]/f} \phi'(c)\,|c\rangle\,|\mathbf{x}+c\cdot\mathbf{s} \bmod (q,f)\rangle\,, \tag{2}$$

where $\phi'(c)$ denotes the weight assigned to c by the discrete Gaussian distribution $D_{\mathbb{Z}^d,r}$ on its coefficient vector, and $\mathbf{x},\mathbf{s}\in(\mathbb{Z}_q[x]/f)^n$. We refer to this variant of stEDCP as Module-EDCP, denoted by M-EDCP. When the secret vector $\mathbf{s}(x)$ has dimension 1, we further refer to it as Ring-EDCP, denoted by R-EDCP.

However, following the framework of [BKSW18] to reduce MLWE to M-EDCP appears to require a heuristic assumption; see the Supplementary Material A for a detailed discussion. Therefore, we seek an alternative variant of stEDCP that admits a provable equivalence with MLWE.

Our solution to this issue is inspired by the Integer Polynomial LWE (IPLWE) problem, which is introduced in [Gu19] and formally studied in [DSSS21]. In particular, in the latter work, it is shown that the IPLWE problem is equivalent to the PLWE problem. Moreover, this result can be naturally generalized to establish an equivalence between P-MLWE and Integer P-MLWE (IP-MLWE). More precisely, an IP-MLWE sample is of the form $(\mathbf{A},\mathbf{As}+\mathbf{e} \bmod f(q))\in\mathbb{Z}^{m\times n}_{f(q)}\times\mathbb{Z}^{m}_{f(q)}$ with $f(x)$ as the defining polynomial of some ring of degree d, where $\mathbf{A}$ is randomly chosen from $U(\mathbb{Z}^{m\times n}_{f(q)})$ and each entry of $\mathbf{e}$ is defined by first sampling a polynomial whose coefficient vector is sampled from a discrete Gaussian distribution and then evaluating this polynomial at $x=q$.

Similarly, we consider an integer version of M-EDCP problem with sample of the form:

$$\sum\nolimits_{c\in\mathbb{Z}[x]/f} \phi(c)\,|c\rangle\,|\mathbf{x}+c(q)\cdot\mathbf{s} \bmod f(q)\rangle\,, \tag{3}$$

where both $\mathbf{x},\mathbf{s}\in\mathbb{Z}_{f(q)}$.

Compared to the state in (2), in the second register, all operations are now defined over $\mathbb{Z}_{f(q)}$. We refer to the problem of recovering the secret $\mathbf{s}$ from samples of such quantum states as Integer Polynomial Module EDCP, denoted by IP-M-EDCP. When the secret has dimension 1, we refer to the resulting problem as Integer Polynomial EDCP, denoted by IP-EDCP. The main contribution of this paper is to establish an equivalence between MLWE and IP-M-EDCP.

Our Results. To explore this question, we introduce a structured variant of EDCP, denoted as IP-M-EDCP, which, to the best of our knowledge, has not been previously considered. The $\mathsf{IP\text{-}M\text{-}EDCP}^{m,n}_{q,\varphi,f}$, with parameters $m, n, q \in \mathbb{Z}$, a polynomial f of degree d and a function $\varphi : \mathbb{Z}^d \mapsto \mathbb{C}$ admitting the expression[1] $\varphi(\mathbf{c}) = \prod_{i \leqslant d} \varphi_i(c_i)$ with $\sum_{c_i \in \mathbb{Z}} c_i \cdot |\varphi_i(c_i)|^2 < +\infty$ for each $i \leqslant d$, consists in recovering $\mathbf{s} \in \mathbb{Z}^n_{f(q)}$ from the following m states:

$$\left\{ \frac{1}{\sqrt{\sum_{\mathbf{c} \in \mathbb{Z}^d} |\varphi(\mathbf{c})|^2}} \cdot \sum_{\mathbf{c} \in \mathbb{Z}^d} \varphi(\mathbf{c}) \, |\mathbf{c}\rangle \, |\mathbf{x}_i + \langle \mathbf{c}, \mathbf{z} \rangle \cdot \mathbf{s} \bmod f(q)\rangle \right\}_{i \leqslant m}, \tag{4}$$

where $\mathbf{x}_i$'s are arbitrary in $\mathbb{Z}^n_{f(q)}$, and $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$. If we let $c(x)$ be a polynomial with coefficient vector $\mathbf{c}$, then the inner product $\langle \mathbf{c}, \mathbf{z} \rangle$ can be naturally interpreted as the evaluation $c(q)$. We adhere to the form in Equation (4) as it is more naturally adapted to the proof of equivalence to MLWE. A natural computational problem associated with this quantum state is the following: given a sufficient number of such quantum states, asks to recover the secret vector $\mathbf{s}$. We refer to this problem as the structured Extrapolated Dihedral Cosets Problem (IP-M-EDCP). When $\varphi(\mathbf{c}) = \sqrt{\mathcal{D}_{\mathbb{Z}^d, r}(\mathbf{c})}$ for some positive number r, the problem is denoted by $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{m,n}_{q,r,f}$. In case of $d = 1$, IP-M-EDCP is exactly EDCP. However, we emphasize that for $d > 1$, the IP-M-EDCP sample, as a quantum superposition, encodes exponentially (in d) more possibilities than its EDCP counterpart. Our main result can be informally stated as below.

Theorem 1 (Informal). *Given a cyclotomic polynomial $f = x^d + 1$ of power-of-2 degree d, there is an equivalence (under quantum polynomial-time) between $\mathsf{MLWE}^{m,n}_{q,\alpha,f}$ and $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{\overline{m},n}_{q,r,f}$, with $n = \mathcal{O}(1)$, $q = \mathsf{poly}(d)$, $m = \mathcal{O}(\log(q))$, $\overline{m} = \mathsf{poly}(d)$ and $r = \mathsf{poly}(nd \log q)/\alpha$.*

The restrictions to power-of-2 cyclotomic polynomials and logarithmic ranks are required only to derive the equivalence. In fact, each reduction direction can be established under weaker conditions. For the reduction from MLWE to IP-M-EDCP, it suffices to assume that $f(x) = x^d + g(x)$ with $\deg(g) \leqslant d/2$, if polynomially many MLWE samples are available. For the reverse reduction, we require $f(x) = x^d - C$ for a constant C and can only reduce to MLWE with $\mathcal{O}(\log q)$ samples. Therefore, to close the reduction chain, a sample amplification result for MLWE is further required, which is currently known only for cyclotomic rings.

[1] Under this assumption, one may restrict the sum to a finite set and the superposition can still have a negligible ℓ_2 distance from the superposition above.

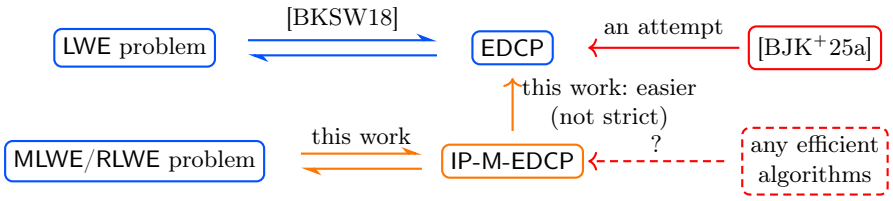

Fig. 1. The overview of our results in this work

Since EDCP can be viewed as a quantum analogue of LWE, in this work we show that IP-M-EDCP can similarly be regarded as a quantum analogue of MLWE. Notably, when $f(x) = x$, this quantum state is exactly an EDCP state. This naturally leads to the question of how IP-M-EDCP relates to EDCP.

Theorem 2 (Informal). *There exists a quantum polynomial-time reduction from* G-IP-M-EDCP$^{m,n}_{q,r,f}$ *to* G-EDCP$^{m,n}_{q,r}$.

As shown in Figure 1, this result implies that IP-M-EDCP could be easier than EDCP. Recently, we have seen an attempt in [Che24] to solve LWE via solving (a variant of) EDCP. Furthermore, A quasi-polynomial-time quantum algorithm for the EDCP problem is proposed in [BJK+25a]. Our findings motivate further cryptanalytic study of the newly introduced IP-M-EDCP problem.

Roadmap. The remainder of the paper is organized as follows. In Section 2, we provide a technical overview of our main results. In Section 4, we present a reduction from IP-M-EDCP to MLWE, and in Section 5, we establish the reduction in the reverse direction. Section 6 shows that IP-M-EDCP is no harder than EDCP.

2 Technical Overview

As introduced in Section 1, our work is inspired by IP-MLWE problem, which is as hard as P-MLWE. To facilitate the presentation, we first recall two important maps used to bridge P-MLWE and IP-MLWE. defined in [DSSS21]. The first map $\mathsf{Eval}_q^{(f)}(P(x)) = \mathsf{Eval}_q(P(x)) \bmod f(q)$ is used to transform P-LWE to its integer version, where $\mathsf{Eval}_q(P(x))$ takes an element $P(x)$ from $\mathbb{Z}_q[x]/f(x)$ as input, evaluates it at $x = q$. In the following, we first define the centered q-ary decomposition of an integer $a \in \mathbb{Z}$. For $q > 2$ and $a \in \mathbb{Z}$, for every $0 \leqslant i \leqslant \lceil \log_q a \rceil$, we define $a_i := (a - \sum_{j<i} a_j q^j)/q^i \bmod q$, and $\mathbf{a} = (a_0, a_1, \ldots, a_{d-1})^T$ as the centered q-ary decomposition of a. For any integer a such that its centered q-ary decomposition $\mathbf{a}$ has an ℓ_∞ norm (e.g., ℓ_∞ norm of $\mathbf{x}$ is $\|\mathbf{x}\|_\infty = \max_i |x_i|$) significantly smaller than q, we will call this integer *segmented* and each component a_i of its decomposition vector as its *segment*. Actually, $\mathsf{Eval}_q^{(f)}$ behaves similarly to a ring homomorphism, up to small deviations (refer to Supplementary Material B.4 for details).

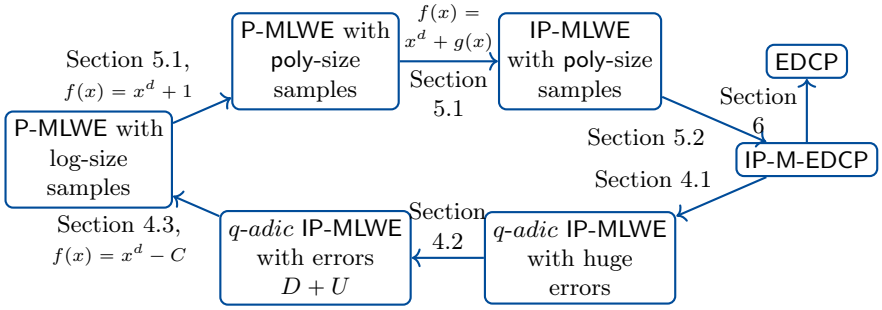

Fig. 2. The outline of our reductions

(I) For any $a(x), b(x) \in \mathbb{Z}_q[x]/f$, we have $\mathsf{Eval}_q^{(f)}(a(x) + b(x)) = a(q) + b(q) + c_r(q) \bmod f(q)$, where $c_r(q)$ is *segmented*;

(II) For any $a(x), b(x) \in \mathbb{Z}_q[x]/f$ such that either $a(x)$ or $b(x)$ has small coefficients, then $\mathsf{Eval}_q^{(f)}(a(x) \cdot b(x) \bmod f(x)) = a(q) \cdot b(q) + c_r(q) \bmod f(q)$, where $c_r(q)$ is *segmented*.

The second map $\Phi_q^{(f)}(a) = \Phi_q(a) \bmod (q, f(x))$ gives the reverse transformation, where $\Phi_q(a)$ takes an element a from $\mathbb{Z}_{f(q)}$ as input, performs a centered q-ary decomposition on it, and outputs a polynomial whose coefficient vector equals to the decomposition vector. As shown in [DSSS21], this mapping behaves similarly to a ring homomorphism, up to small deviations.

(I) for any $a, b \in \mathbb{Z}_{f(q)}$, we have $\Phi_q^{(f)}(a + b \bmod f(q)) = (\Phi_q^{(f)}(a) + \Phi_q^{(f)}(b) \bmod f(x)) + c_r(x)$, where carries $c_r(x)$ has small coefficients;

(II) for any $a, b \in \mathbb{Z}_{f(q)}$ such that either $\Phi_q^{(f)}(a)$ or $\Phi_q^{(f)}(b)$ has small coefficients, then $\Phi_q^{(f)}(a \cdot b \bmod f(q)) = (\Phi_q^{(f)}(a) \cdot \Phi_q^{(f)}(b) \bmod f(x)) + c_r(x)$, where the carries $c_r(x)$ has small coefficients.

Throughout the paper, we will also consider the natural generalization of these two maps with input as matrix. Concretely, given $\mathbf{P}(x) \in (\mathbb{Z}_q[x]/f(x))^{m \times n}$ and $\mathbf{A} \in (\mathbb{Z}_{f(q)})^{m \times n}$, we define $\mathsf{Eval}_q^{(f)}(\mathbf{P}(x)) = (\mathsf{Eval}_q^{(f)}(P_{i,j}(x)))_{i \leqslant m, j \leqslant n}$ and $\Phi_q^{(f)}(\mathbf{A}) = (\Phi_q^{(f)}(A_{i,j}))_{i \leqslant m, j \leqslant n}$.

In [RSW18], the authors establish the equivalence between the RLWE problem and the PLWE problem for a broad class of underlying polynomials. This result naturally extends to an equivalence between the MLWE and P-MLWE problems; see Supplementary Material B.3 for details. Therefore, in this work we restrict our attention to reductions between the P-MLWE and IP-M-EDCP problems.

We provide an overview of our results in Figure 2. First, in Subsections 2.1 to 2.3, we present the reductions between P-MLWE and IP-M-EDCP. Then, in Subsection 2.4, we show the reduction from IP-M-EDCP to EDCP.

2.1 Reduction from P-MLWE to IP-M-EDCP

We begin with the reduction from P-MLWE to IP-M-EDCP, which helps to illustrate the design rationale behind IP-M-EDCP. First, we transform P-MLWE into its integer version with the map $\mathsf{Eval}_q^{(f)}$.

Given a P-MLWE instance of the form $(\mathbf{A}(x), \mathbf{A}(x)\mathbf{s}(x) + \mathbf{e}(x) \bmod f(x))$, where both $\mathbf{s}(x)$ and $\mathbf{e}(x)$ have small coefficients, it follows that

$$\begin{aligned}&(\mathsf{Eval}_q^{(f)}(\mathbf{A}(x)), \mathsf{Eval}_q^{(f)}(\mathbf{A}(x)\mathbf{s}(x) + \mathbf{e}(x) \bmod f(x)))\\ =&(\mathbf{A}(q) \bmod f(q), \mathbf{A}(q)\mathbf{s}(q) + \mathbf{e}(q) + \mathbf{c}_r \bmod f(q)),\end{aligned} \tag{5}$$

where we have $\mathbf{c}_r = \mathsf{Eval}_q^{(f)}(\mathbf{c}_r(x))$ for a polynomial vector $\mathbf{c}_r(x)$ such that its each component polynomial has small coefficients. For simplicity, we let $\widehat{\mathbf{A}} = \mathbf{A}(q) \bmod f(q)$, $\widehat{\mathbf{s}} = \mathbf{s}(q) \bmod f(q)$ and $\widehat{\mathbf{e}} = \mathbf{e}(q) + \mathbf{c}_r \bmod f(q)$. Notice that for $\mathbf{A}(x) \hookleftarrow U((\mathbb{Z}_q[x]/f(x))^{m\times n})$, the distribution of $\mathbf{A}(q) \bmod f(q)$ should be statistically close to uniform in the case of $f = x^d + g$, where g is a polynomial with degree $\leqslant d/2$. Therefore, we will always focus on this case and assume $\widehat{\mathbf{A}}$ to be uniformly random in $U(\mathbb{Z}_{f(q)}^{m\times n})$ in the following.

Now, we are ready to start our quantum transformation. First, we prepare the quantum state $\sum_{\mathbf{c}\in\mathbb{Z}^d}\sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n}\rho_r(\mathbf{c})\,|\mathbf{c}\rangle\,|\mathbf{x}\rangle$[2]. With the instance $(\widehat{\mathbf{A}}, \widehat{\mathbf{A}}\widehat{\mathbf{s}} + \widehat{\mathbf{e}} \bmod f(q))$ we evaluate the function $F(\mathbf{c}, \mathbf{x}) = \widehat{\mathbf{A}}\mathbf{x} - \langle\mathbf{c}, \mathbf{z}\rangle(\widehat{\mathbf{A}}\widehat{\mathbf{s}} + \widehat{\mathbf{e}}) \bmod f(q)$ and store the result in the third register (with κ as the security parameter):

$$\sum_{\mathbf{c}\in\mathbb{Z}^d\bigcap[-r\sqrt{\kappa},r\sqrt{\kappa}]^d}\sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n}\rho_r(\mathbf{c})\,|\mathbf{c}\rangle\,|\mathbf{x}\rangle\,|\widehat{\mathbf{A}}\mathbf{x} - \langle\mathbf{c}, \mathbf{z}\rangle(\widehat{\mathbf{A}}\widehat{\mathbf{s}} + \widehat{\mathbf{e}}) \bmod f(q)\rangle\,. \tag{6}$$

Then we replace $\mathbf{x}$ with $\mathbf{x} + \langle\mathbf{c}, \mathbf{z}\rangle \cdot \widehat{\mathbf{s}} \bmod f(q)$, and get the quantum state:

$$\sum_{\mathbf{c}\in\mathbb{Z}^d\bigcap[-r\sqrt{\kappa},r\sqrt{\kappa}]^d}\sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n}\rho_r(\mathbf{c})\,|\mathbf{c}\rangle\,|\mathbf{x} + \langle\mathbf{c}, \mathbf{z}\rangle\widehat{\mathbf{s}}\rangle\,|\widehat{\mathbf{A}}\mathbf{x} - \langle\mathbf{c}, \mathbf{z}\rangle\widehat{\mathbf{e}} \bmod f(q)\rangle\,. \tag{7}$$

Before moving to the next step, we need to show that the term $\langle\mathbf{c}, \mathbf{z}\rangle\widehat{\mathbf{e}} \bmod f(q)$ in the third register remains small compared to $f(q)$ for all (exponentially many) choices of $\mathbf{c}$. This will eventually lead us to a IP-M-EDCP superposition with exponentially many possibilities.

We let $c(x)$ denote the polynomial with coefficient vector $\mathbf{c}$, hence we have $\langle\mathbf{c}, \mathbf{z}\rangle \bmod f(q) = \mathsf{Eval}_q^{(f)}(c(x))$. Recall that $\widehat{\mathbf{e}} = \mathbf{e}(q) + \mathbf{c}(q) \bmod f(q)$ and each component $\widehat{e}_i$ is *segmented*. We denote $\widehat{e}_i(x)$ as the polynomial whose coefficient vector is the q-ary decomposition of $\widehat{e}_i$. Then $c(x)\widehat{e}_i(x) \bmod f(x)$ for each $i \leqslant d$ has relatively small coefficients. Due to the approximate ring homomorphism property of $\mathsf{Eval}_q^{(f)}$, $\mathsf{Eval}_q^{(f)}\,(c(x)\widehat{e}_i(x) \bmod f(x))$ is equal to the product of $\langle\mathbf{c}, \mathbf{z}\rangle$ and i-th entry of $\widehat{\mathbf{e}}$ up to some additive *segmented* carries $\widehat{c}_{r,i}$. As a result, the term $\langle\mathbf{c}, \mathbf{z}\rangle \cdot \widehat{\mathbf{e}} \bmod f(q)$ will also be *segmented*. We denote the (ℓ_∞-norm) bound

[2] In the following part of this paper, we omit normalization factors of quantum states for convenience.

of its *segments* by $\widetilde{B}$, so that $\|\langle \mathbf{c}, \mathbf{z}\rangle \cdot \hat{\mathbf{e}} \bmod f(q)\|_\infty \leqslant \widetilde{B} \cdot (q^d - 1)/(q-1)$. It is important to note that without the specific structure of $\hat{\mathbf{e}}$, multiplying by $\langle \mathbf{c}, \mathbf{z}\rangle$ over the ring $\mathbb{Z}_{f(q)}$ could result in an error term with an unbounded ℓ_∞ norm.

Now given a fixed $\mathbf{x}$, all points $\widehat{\mathbf{A}}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}}$ for all $\mathbf{c}$'s in the specified domain are somewhat close to each other. In the next step, we will subdivide the space $\mathbb{R}^m$ such that all these points can fall into the same cell with $1 - 1/k$ probability for some polynomially large $k = \mathsf{poly}(\kappa)$ with security parameter κ. To achieve this, we further require that $\|\langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}} \bmod f(q)\|_\infty$ is smaller than $\lambda_1^\infty(\Lambda_{f(q)}(\widehat{\mathbf{A}}))/k$, where $\lambda_1^\infty(\Lambda_{f(q)}(\widehat{\mathbf{A}}))$ denotes the first minimum of the lattice $\Lambda_{f(q)}(\widehat{\mathbf{A}}) = \widehat{\mathbf{A}}\mathbb{Z}^n + f(q)\mathbb{Z}^m$. As illustrated in Figure 3, we let the red points denote all possible values in the third register of the above state. As done in prior works [Reg04a,BKSW18], we then subdivide the space $\mathbb{R}^m$ into cells of length d_{cell}, which is between $\|\langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}} \bmod f(q)\|_\infty$ and $\lambda_1^\infty(\Lambda_{f(q)}(\widehat{\mathbf{A}}))$. Define ϕ as the mapping that assigns each $\mathbf{y} \in \mathbb{R}^m$ to a cell $\phi(\mathbf{y})$. One can observe that there exist some targeting values $\mathbf{x}$'s, the mapping $\phi(\widehat{\mathbf{A}}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}})$ results in the same cell for all $\mathbf{c}$'s. Additionally, for any $\mathbf{x}_1 \neq \mathbf{x}_2$, we have $\phi(\widehat{\mathbf{A}}\mathbf{x}_1) \neq \phi(\widehat{\mathbf{A}}\mathbf{x}_2)$. Concretely, we apply the map ϕ on the input value in the third register and store the result in the fourth register, yielding the following quantum state:

$$\sum_{\substack{\mathbf{c}\in\mathbb{Z}^d \bigcap [-r\sqrt{\kappa}, r\sqrt{\kappa}]^d \\ \mathbf{x}\in\mathbb{Z}^n_{f(q)}}} \rho_r(\mathbf{c}) \left|\mathbf{c}\right\rangle \left|\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s}'\right\rangle \left|\widehat{\mathbf{A}}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}}\right\rangle \left|\phi(\widehat{\mathbf{A}}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}})\right\rangle . \quad (8)$$

Measuring the fourth register ensures that $\mathbf{x}$ is determined. Once this fixed $\mathbf{x}$ happens (with non-negligible probability) to be one of the aforementioned targeting values, all possibilities $\mathbf{c}$'s will remain. As a result, all possible values for a same $\mathbf{x}$ in the third register (as a full cluster of red points inside one cell in Figure 3) will be kept[3]. When the resulting $\mathbf{x}$ lies outside the set of targeting values, the reduction fails. This event restricts the number of IP-M-EDCP samples obtained in this reduction.

Last, using the instance $(\widehat{\mathbf{A}}, \widehat{\mathbf{A}}\hat{\mathbf{s}} + \hat{\mathbf{e}} \bmod f(q))$ along with the values in the first and second registers, we can effectively zeroize the third register. Consequently, we obtain a quantum state that is negligibly close in trace distance to the IP-M-EDCP quantum state. Note that, this reduction holds for MLWE with any rank.

There is one remaining subtlety in bounding $\|\langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}} \bmod f(q)\|_\infty$ by the first minimum $\lambda_1^\infty(\Lambda_{f(q)}(\widehat{\mathbf{A}}))$. Recall that $\|\langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}} \bmod f(q)\|_\infty \leqslant \widetilde{B}(q^d - 1)/(q-1)$. Meanwhile, $\lambda_1^\infty(\Lambda_{f(q)}(\widehat{\mathbf{A}}))$ has a lower bound of $f(q)^{\frac{m-n}{m}}/2$ with overwhelming probability (refer to Lemma 1). Thus, to guarantee that $\|\langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}} \bmod f(q)\|_\infty$ is

[3] As shown in Figure 3, the errors $\langle \mathbf{c}, \mathbf{z}\rangle \hat{\mathbf{e}}$ may appear in multiple directions. In [Reg04a,BKSW18], one could use sphere intersection as a cap to improve the one with box separation by a factor of $\sqrt{m}$. However, in our case, the intersection is not a cap. Approximating this intersection by a sphere will not lead to any improvement.

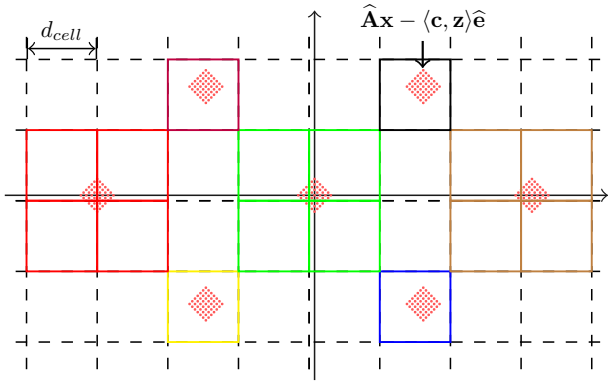

Fig. 3. Illustration of subdivision of the ambient space of dimension 2

smaller than $\lambda_1^{\infty}(\Lambda_{f(q)}(\widehat{\mathbf{A}}))$, it is necessary to have $m \geqslant \mathcal{O}((nd \log q)/(\log(q/\widetilde{B})))$. However, as shown in the next subsection, one can only obtain $m = \mathcal{O}(\log d)$ many MLWE samples in the reverse reduction, which is not sufficient for the forward direction. Our approach to address this gap is presented in Subsection 2.3.

2.2 Reduction from IP-M-EDCP to P-MLWE

To complete the picture, we present the reverse reduction, ensuring that we are not reducing P-MLWE to a strictly harder problem. We thus show that the two problems are, in fact, equivalent. Specifically, we explain the reduction from IP-M-EDCP to P-MLWE in three steps.

First Step: from IP-M-EDCP to q-*adic* IP-MLWE. In [BKSW18], the authors employed the quantum Fourier transform to establish a connection between the EDCP and LWE problems. Inspired by this approach, we also aim to utilize the quantum Fourier transform to construct an integer variant of MLWE from IP-M-EDCP. Specifically, this work focuses on the q-adic IP-MLWE problem, in which one is given multiple samples of the form $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle \cdot \mathbf{z} + \mathbf{e} \bmod f(q)) \in \left(\mathbb{Z}_{f(q)}\right)^n \times \left(\mathbb{Z}_{f(q)}\right)^d$, where $\mathbf{z} = (1, q, q^2, \ldots, q^{d-1})^{\top}$, and the goal is to recover the secret $\mathbf{s}$.

Given a quantum state $\sum_{\mathbf{c} \in \mathbb{Z}_{f(q)}^d} \rho_{\sqrt{2}r}(\mathbf{c}) \left|\mathbf{c}\right\rangle \left|\mathbf{x} + \langle \mathbf{z}, \mathbf{c} \rangle \cdot \mathbf{s} \bmod f(q)\right\rangle$, whose trace distance from the quantum state $\sum_{\mathbf{c} \in \mathbb{Z}^d} \rho_{\sqrt{2}r}(\mathbf{c}) \left|\mathbf{c}\right\rangle \left|\mathbf{x} + \langle \mathbf{z}, \mathbf{c} \rangle \cdot \mathbf{s} \bmod f(q)\right\rangle$ is negligible, we apply a quantum Fourier transform over $\mathbb{Z}_{f(q)}$ to the second register and get a quantum state of the form:

$$\sum_{\mathbf{a} \in \mathbb{Z}_{f(q)}^n} \sum_{\mathbf{c} \in \mathbb{Z}_{f(q)}^d} \rho_{\sqrt{2}r}(\mathbf{c}) \omega_{f(q)}^{\langle \mathbf{a}, \mathbf{x} + \langle \mathbf{c}, \mathbf{z} \rangle \mathbf{s} \rangle} |\mathbf{c}\rangle |\mathbf{a}\rangle,$$

where $\omega_{f(q)} = \exp(2\pi\sqrt{-1}/f(q))$. Since the quantum Fourier transform can be implemented as a quantum circuit consisting of only $\Theta\left((\log f(q))^2\right)$ Hadamard gates and controlled phase shift gates, which is polynomial in d. We then measure the second register and obtain a value $\widetilde{\mathbf{a}}$. This leaves us with the quantum

state $\sum_{\mathbf{c}\in\mathbb{Z}^d_{f(q)}} \rho_{\sqrt{2}r}(\mathbf{c})\omega_{f(q)}^{\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\langle\mathbf{c},\mathbf{z}\rangle}|\mathbf{c}\rangle$. Note that $\widetilde{\mathbf{a}}$ is uniformly random over $\mathbb{Z}^n_{f(q)}$. Applying a second quantum Fourier transform over $\mathbb{Z}^d_{f(q)}$ to the first register gives us a quantum state of the form:

$$\sum\nolimits_{\mathbf{b}\in\mathbb{Z}^d_{f(q)}} \sum\nolimits_{\mathbf{c}\in\mathbb{Z}^d_{f(q)}} \rho_{\sqrt{2}r}(\mathbf{c})\omega_{f(q)}^{\langle\mathbf{c},\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{b}\rangle}|\mathbf{b}\rangle. \tag{9}$$

Omitting the exponentially small Gaussian tails, we get a quantum state as follows: $\sum_{\mathbf{b}\in\mathbb{Z}^d_{f(q)}} \sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_{\sqrt{2}r}(\mathbf{c})\omega_{f(q)}^{\langle\mathbf{c},\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{b}\rangle}|\mathbf{b}\rangle$. An application of the Poisson summation formula transfers $\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{b}$ into a shift of the Gaussian distribution over $\mathbb{Z}^d$. In other words, we get a quantum state as follows:

$$\sum_{\mathbf{b}\in\mathbb{Z}^d_{f(q)}} \sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_{\frac{1}{\sqrt{2}r}}(\mathbf{c}+\frac{\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{b}}{f(q)})|\mathbf{c}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}^d} \rho_{f(q)/(\sqrt{2}r)}(\mathbf{e})|\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{e} \bmod f(q)\rangle. \tag{10}$$

By measuring the first register, we obtain a sample of the form $(\widetilde{\mathbf{a}},\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{e} \bmod f(q))$, where the error term $\mathbf{e}$ follows the distribution $D_{\mathbb{Z}^d,f(q)/(\sqrt{2}r)}$.

Second Step: from q-*adic* IP-MLWE with large errors to q-*adic* IP-MLWE with errors $D+U$. Before we move to the next step, we need to make a finer analysis on the errors of q-*adic* IP-MLWE samples. In particular, we analyze the distribution of the least significant $(d-1)\lceil\log q\rceil$ bits and higher-order bits of each entry in $\mathbf{e}$ separately.

First, we consider the least significant $(d-1)\lceil\log q\rceil$ bits of each entry in $\mathbf{e}$, where $\mathbf{e}\sim D_{\mathbb{Z}^d,f(q)/(\sqrt{2}r)}$, and ignore the higher-order bits. When the standard deviation parameter $f(q)/(\sqrt{2}r)$ is larger than smoothing parameter of $q^{d-1}\mathbb{Z}^d$, the statistical distance between the distribution of $\mathbf{e} \bmod q^{d-1}\mathbb{Z}^d$ and the uniform distribution $U(\mathbb{Z}^d_{q^{d-1}})$ is negligible[4]. For any polynomially large r, this condition can always be satisfied by enlarging q. Next, we focus on the higher-order bits, i.e., the distribution of $\lfloor\mathbf{e}/q^{d-1}\rceil$, and ignore other bits. While its statistical distance from $D_{\mathbb{Z}^d,f(q)/(\sqrt{2}rq^{d-1})}$ is not necessarily small, their Rényi divergence remains bounded (refer to Lemma 12).

In fact, we cannot treat the errors as the sum of two independent components, because the least significant $(d-1)\lceil\log q\rceil$ bits and higher-order bits are correlated. However, the observation above still motivates us to approximate the error term $\mathbf{e}$ with $\mathbf{e}'=q^{d-1}\mathbf{e}_1+\mathbf{e}_2$ as shown in Figure 4 , where $\mathbf{e}_1\sim D_{\mathbb{Z}^d,f(q)/(\sqrt{2}rq^{d-1})}$, and $\mathbf{e}_2\sim U(\mathbb{Z}^d_{q^{d-1}})$ is a uniform random vector over $\mathbb{Z}^d_{q^{d-1}}$. Indeed, the Rényi divergence between the distributions of $\mathbf{e}$ and $\mathbf{e}'$ remains polynomially bounded (refer to Lemma 14). This ensures that if an algorithm can recover $\mathbf{s}$ from $(\mathbf{a},\langle\mathbf{a},\mathbf{s}\rangle\mathbf{z}+\mathbf{e}' \bmod f(q))$ with a non-negligible advantage, it can also recover $\mathbf{s}$ from $(\mathbf{a},\langle\mathbf{a},\mathbf{s}\rangle\mathbf{z}+\mathbf{e} \bmod f(q))$ with a smaller non-negligible advantage.

Third Step: from q-*adic* IP-MLWE with errors $D+U$ to P-MLWE. Our goal is to extract P-MLWE samples from IP-MLWE samples. Now we are in the

[4] Refer to Definition 1 for the smoothing parameter. For example, when $f(q)/(\sqrt{2}r)\geqslant q^{d-1}\sqrt{\kappa}$, the statistical distance is at most $2^{-\kappa}$ for security parameter κ.

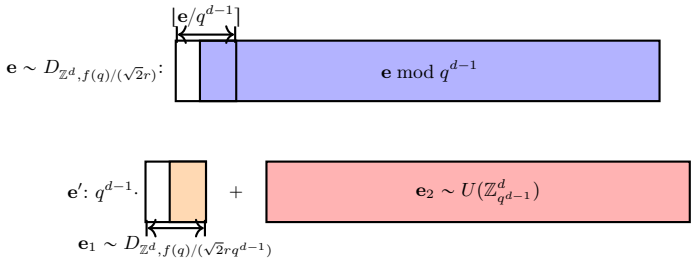

Fig. 4. Illustration of the difference between $\mathbf{e}$ and $\mathbf{e}'$

case that the least significant $(d-1)\lceil \log q \rceil$ bits of each entry in $\mathbf{e}'$ mod $f(q)$ are uniformly random, therefore, it suffices to focus on the information carried by the most significant $\lceil \log q \rceil$ bits of each entry in the vector $\mathbf{b} = \langle \mathbf{a}, \mathbf{s} \rangle \cdot \mathbf{z} + \mathbf{e}'$ mod $f(q)$.

For each $i \in \{0, 1, \ldots, d-1\}$, we have $\Phi_q^{(f)}(b_i) = \langle \Phi_q^{(f)}(\mathbf{a}), \Phi_q^{(f)}(\mathbf{s}) \rangle x^i + \Phi_q^{(f)}(e'_i) + \widetilde{c}_i(x) \bmod f(x)$, where the carry term $\widetilde{c}_i(x)$ has a coefficient vector of small infinity norm. The $(d-1)$-th coefficient of $\Phi_q^{(f)}(e'_i)$ follows the distribution $D_{\mathbb{Z}, f(q)/(\sqrt{2}rq^{d-1})}$. Extracting these coefficients for all i and combining them yields a new polynomial.

More precisely, for $f(x) = x^d - C$, we obtain $\sum_{i=0}^{d-1} \Phi_q^{(f)}(b_{d-1-i})_{d-1} x^i = \langle \Phi_q^{(f)}(\mathbf{a}), \Phi_q^{(f)}(\mathbf{s}) \rangle + \overline{e}'(x) + \overline{c}(x) \bmod f(x)$, where $\overline{c}(x)$ has small-norm coefficients and $\overline{e}'(x) \sim D_{\mathbb{Z}[x]/f, f(q)/(\sqrt{2}rq^{d-1})}$. Although additional carries appear, the resulting instance remains close to a P-MLWE instance in Rényi divergence for $m = \mathcal{O}(\log d)$, which necessitates restricting to constant module rank n.

However, we note that $m = \mathcal{O}(\log d)$ P-MLWE samples are insufficient for the reduction from P-MLWE to IP-M-EDCP. We address this issue in the next subsection. Since the sample-amplification technique we rely on requires the underlying polynomial $f(x)$ to be cyclotomic, we formalize this step in the main body of the paper by restricting to $f(x) = x^d + 1$, where d is a power of 2.

2.3 Increasing the Number of Samples

We recall that the reduction from the IP-M-EDCP problem to P-MLWE requires $m = \mathcal{O}(\log d)$ samples, whereas generating IP-M-EDCP quantum states requires $m = \omega((\log q \cdot dn)/(\log(q/\widetilde{B})))$ P-MLWE samples. Hence, an additional step is required before carrying out the procedure described in Section 2.1.

Our technique for addressing this gap requires the underlying polynomial f to define a cyclotomic ring, a requirement that will be justified later. Moreover, since the reduction from IP-M-EDCP to P-MLWE restricts $f(x)$ to be of the form $x^d - C$ for some constant C, we specialize to the polynomial $f(x) = x^d + 1$ with d a power of 2 in order to complete the reduction chain. In this case, the ring of integers $\mathcal{O}_K$ coincides with the integer polynomial ring $\mathbb{Z}[x]/f(x)$.

Starting from a P-MLWE instance of the form $(\mathbf{A}(x), \mathbf{A}(x)\mathbf{s}(x) + \mathbf{e}(x)) \in (\mathbb{Z}_q[x]/f(x))^{m\times n} \times (\mathbb{Z}_q[x]/f(x))^m$, where $m = \mathcal{O}(\log d)$, we aim to increase the number of samples.

Since $\mathbf{A}(x)$ is randomly selected from $(\mathcal{O}_K/q\mathcal{O}_K)^{m\times n}$, when $m \geqslant n$, $\mathbf{A}(x)$ is a full column-rank matrix with overwhelming probability under specific selection of q (refer to Lemma 48). By performing a series of row interchange operations, we can transform a full column-rank $\mathbf{A}(x)$ into the form

$$\begin{pmatrix} \mathbf{I}_n \\ \mathbf{A}_2(x)\mathbf{A}_1(x)^{-1} \end{pmatrix} \cdot \mathbf{A}_1(x).$$

Thus, without loss of generality, we assume that $\mathbf{A}(x)$ is already in this form.

Using the regularity lemma (refer to Lemma 49), if we left-multiply the matrix $\begin{pmatrix} \mathbf{I}_n \\ \mathbf{A}_2(x)\mathbf{A}_1(x)^{-1} \end{pmatrix}$ by a vector sampled from the discrete Gaussian distribution over $\mathcal{O}_K$, the resulting vector is statistically close to a uniformly random vector.

Now, consider a matrix $\mathbf{E}(x) \in (\mathcal{O}_K/q\mathcal{O}_K)^{m'\times m}$ whose entries are independently drawn from a discrete Gaussian distribution over $\mathcal{O}_K$. By construction, $\mathbf{A}'(x) = \mathbf{E}(x)\mathbf{A}(x)$ remains statistically close to a uniformly random matrix. Therefore, left-multiplying the original P-MLWE instance by $\mathbf{E}(x)$ yields a new P-MLWE-like instance with m' samples and slightly larger but still small errors $\mathbf{e}'(x)$. Notably, the new error $\mathbf{e}'(x)$ is correlated to $\mathbf{A}'(x) = \mathbf{E}(x)\mathbf{A}(x)$. However, dependence will not pose an issue because the reduction relies solely on the randomness of $\mathbf{A}'(x)$ and smallness of $\mathbf{e}'(x)$.

By choosing $m' \gg \mathcal{O}\left(\log(q) \cdot dn/\log(q/\widetilde{B})\right)$, the P-MLWE-like instance would be sufficient to generate the IP-M-EDCP instance.

2.4 Reduction from IP-M-EDCP to EDCP

Given an IP-M-EDCP state, our goal is to transform it into an EDCP state with the same modulus. For the sake of simplicity, we consider the case of $n = 1$, where we are given a quantum state of the form $\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_r |\mathbf{c}\rangle |x + \langle \mathbf{c}, \mathbf{z}\rangle \cdot s \bmod f(q)\rangle$ with $x, s \in \mathbb{Z}_{f(q)}$ and $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$. Our first step is to measure the last $d-1$ components $c_1, \ldots, c_{d-1}$ of $\mathbf{c}$ in the first register. Then we get the state $\sum_{c_0\in\mathbb{Z}} \rho_r |c_0\rangle |(x + (\sum_{i=1}^{d-1} c_i q^i) \cdot s \bmod f(q)) + c_0 \cdot s \bmod f(q)\rangle$, where the value in the second register can be rewritten as $x' + c_0 \cdot s \bmod f(q)$ with $x' = x + (\sum_{i=1}^{d-1} c_i q^i) \cdot s \bmod f(q)$. This resulting state is exactly an EDCP state with the same modulus $f(q)$.

In fact, a dimension-modulus switching can be applied to the EDCP problem. Specifically, we reduce an instance of EDCP with modulus $f(q)$ to a standard instance with modulus q. We first reduce the 1-dimensional EDCP problem with modulus $f(q)$ to a 1-dimensional LWE instance with the same modulus, using the reduction from [BKSW18]. Next, applying the dimension-modulus switching technique from [BLP+13], we can reduce this problem to an LWE problem with

dimension $\mathcal{O}(d \log q)$ and modulus q. Finally, as shown in [BKSW18], one can reduce the latter LWE problem to an EDCP problem with the same dimension and modulus. We remark that there is an alternative reduction. Concretely, we first reduce IP-M-EDCP to MLWE, which can then be reduced to approximate Shortest Vector Problem (SVP) with $\mathcal{O}(d \log q)$ dimension. The latter one can be reduced to LWE, which reduces to EDCP at the end.

2.5 Open Problems

Our reduction between MLWE and IP-M-EDCP has heavily relied on the Rényi divergence, which is particularly suitable for the search variants but does not naturally extend to decision variants. A possible workaround is to first establish an equivalence between search and decision variants of IP-M-EDCP, then combine this with the known equivalence for MLWE, as well as our results, to bridge the decision variants. Additionally, the use of Rényi divergence restricts the result to MLWE with constant module rank. It remains an interesting question to achieve such reductions without relying on Rényi divergence.

Our transformation from MLWE, if given sufficient samples, to IP-M-EDCP works for a large family of rings (refer to Supplementary Material D.5). However, due to the requirement of having the cyclotomic structure assumed in the sample amplification procedure, the equivalence only holds for cyclotomic polynomials with power-of-two index. Extending our results to accommodate a broader class of polynomial rings remains a research direction for future work.

Our reduction from IP-M-EDCP to EDCP, suggests that IP-M-EDCP may be an easier problem. Therefore, it seems interesting to ask whether there exists an algorithm that solves IP-M-EDCP asymptotically faster than EDCP. More ambitiously, can such an improvement be leveraged to solve MLWE via IP-M-EDCP more efficiently than by existing algorithms? One potential approach is to adapt Kuperberg's algorithms [Kup05,Kup11] to IP-M-EDCP. Then, it would also be good to investigate whether the algorithm of Bai et al [BJK+25a] for solving EDCP can be adapted to solve IP-M-EDCP with lower time or sample complexity.

3 Preliminaries

Let q be a positive integer. Let $[n] = \{0, 1, \ldots, n-1\}$. Let the representation set of $\mathbb{Z}_q$ be $(-q/2, q/2] \bigcap \mathbb{Z}$. For any vector $\mathbf{x}$ in $\mathbb{C}^n$, we let $\|\mathbf{x}\|_\infty$ denote its infinity norm and $\|\mathbf{x}\|_p$ denote its ℓ_p-norm for any integer $p \geqslant 1$. Furthermore, for a polynomial $c(x) \in \mathbb{C}[x]$, we denote $\|c(x)\|_p = \|\mathbf{c}\|_p$, where $\mathbf{c}$ is the coefficient vector of $c(x)$. Moreover, for a linear operator from $\mathbb{C}^n$ to $\mathbb{C}^m$, which can be written as a matrix $\mathbf{A} \in \mathbb{C}^{m \times n}$, we can also define the p-norm of $\mathbf{A}$ as $\|\mathbf{A}\|_p = \max_{\mathbf{x} \in \mathbb{C}^n \setminus \{0\}} \|\mathbf{A}\mathbf{x}\|_p / \|\mathbf{x}\|_p$. When $p = 2$, we omit the subscript p in the notation.We let $\mathsf{det}(\mathbf{A})$ denote the determinant of a square matrix $\mathbf{A}$. Let $\mathsf{poly}(\kappa)$ denote a polynomial in κ (i.e., $\mathsf{poly}(\kappa) = \mathcal{O}(\kappa^c)$ for some constant c). We let $\mathbf{I}_d$ denote the $d \times d$ identity matrix. Let $U(\mathcal{S})$ denote the uniform distribution over

the set $\mathcal{S}$. We use $u \hookleftarrow \mathcal{D}$ to denote sampling an element u from the distribution $\mathcal{D}$. Last, we let $\Delta(\mathcal{P}, \mathcal{Q}) = \frac{1}{2}\sum_{x\in\mathcal{X}} |\mathcal{P}(x) - \mathcal{Q}(x)|$ denote the statistical distance between the two distributions $\mathcal{P}$ and $\mathcal{Q}$ defined over the same domain $\mathcal{X}$.

3.1 Lattices

We begin by reviewing the basic notions of lattices for this work. Let $\mathbf{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subset \mathbb{R}^m$, where $n \leqslant m$, consist of n linearly independent vectors. The n-dimensional lattice generated by the basis $\mathbf{B}$ is denoted by:

$$\Lambda(\mathbf{B}) = \left\{\mathbf{x} = \sum\nolimits_{i\in[n]} c_i\mathbf{b}_i \mid \forall i \in [n], c_i \in \mathbb{Z}\right\}.$$

We let $\Lambda^* = \{\mathbf{y} \in \mathsf{span}(\Lambda) \mid \forall \mathbf{x} \in \mathcal{L}, \langle \mathbf{x}, \mathbf{y}\rangle \in \mathbb{Z}\}$ denote the dual of a lattice Λ with basis $\mathbf{B}$, where $\mathsf{span}(\Lambda) = \{y = \sum_{i\in[n]} a_i\mathbf{b}_i, a_i \in \mathbb{R}\}$. Then we define the smoothing parameter.

Definition 1 (Smoothing Parameter). *For any $\varepsilon > 0$ and a lattice Λ, we define the smoothing parameter of Λ with parameter ε as the smallest s such that $\rho_{1/s}(\Lambda^*\backslash\{0\}) \leqslant \varepsilon$ and denote it by $\eta_\varepsilon(\Lambda)$*

We provide more relevant tools about lattices. For a full-rank lattice $\mathcal{L}(\mathbf{B})$, we denote $\mathcal{P}(\mathbf{B}) = \mathbb{R}^m \bmod \mathcal{L}(\mathbf{B})$. The first minima of lattice are defined as follows.

Definition 2. *Let Λ be a lattice of rank n in the vector space $\mathbb{R}^m$, where $n \leqslant m$. For $i \in \{1, \ldots, n\}$ we define the i-th successive minimum as*

$$\lambda_i(\Lambda) = \inf\{r|\mathsf{dim}(\mathsf{span}(\Lambda \cap \overline{B}(0, r))) \geqslant i\},$$

where $\overline{B}(0, r) = \{\mathbf{x} \in \mathbb{R}^n \mid \|\mathbf{x}\| \leqslant r\}$ is the closed ball if radius r around 0. Furthermore, for different norm $\|\cdot\|$, $\lambda_i(\Lambda)$'s are different. Particularly, we denote $\lambda_i^\infty(\Lambda)$ as the i-th successive minimum corresponding to the infinity-norm $\|\cdot\|_\infty$.

Then, we introduce the following q-ary lattice that is widely known to be underlying the LWE problem.

Definition 3. *Let q be a positive integer and $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, we define*

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m | \exists \mathbf{x} \in \mathbb{Z}^n \ s.t.\ \mathbf{A}\mathbf{x} = \mathbf{y} \bmod q\}.$$

We also recall a lower bound of the first minimum of this lattice for infinity norm.

Lemma 1 ([BKSW18, Lemma 6]). *Given a uniformly chosen matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$ for some positive integer q, m, n such that $m \geqslant n$, we have $\lambda_1^\infty(\Lambda_q(\mathbf{A})) \geqslant \frac{q^{\frac{m-n}{m}}}{2}$ with probability at least $1 - 2^{-m}$.*

At the end of this subsection, we briefly recall some properties of matrix norms. The following lemma establishes the relations between the ℓ_1-norm, ℓ_2-norm, and ℓ_∞-norm of a matrix.

Lemma 2 ([GVL13, Section 2.3.2]). *Let* $\mathbf{A} \in \mathbb{R}^{m\times n}$. *Then we have*

$$\frac{1}{\sqrt{n}}\|\mathbf{A}\|_\infty \leqslant \|\mathbf{A}\|_2 \leqslant \frac{1}{\sqrt{m}}\|\mathbf{A}\|_\infty;$$
$$\frac{1}{\sqrt{m}}\|\mathbf{A}\|_1 \leqslant \|\mathbf{A}\|_2 \leqslant \frac{1}{\sqrt{n}}\|\mathbf{A}\|_1.$$

3.2 Algebraic Number Theory

Let $\mathbb{Q}[x]$ denote the ring of univariate polynomials with rational coefficients. For a monic irreducible polynomial $f \in \mathbb{Q}[x]$, the quotient ring $\mathbb{Q}[x]/(f)$ forms a number field, i.e., a finite field extension of $\mathbb{Q}$. In the remainder of this paper, we assume that the degree of f, which equals the extension degree $[\mathbb{Q}[x]/(f) : \mathbb{Q}]$, is d. In particular, given an irreducible polynomial f in $\mathbb{Q}[x]$, there exists an algebraic number $\xi \in \mathbb{C}$ such that $\mathbb{Q}[x]/(f) \cong \mathbb{Q}(\xi)$, where ξ is a root of f and x corresponds to ξ under this isomorphism. Let $K = \mathbb{Q}(\xi)$ denote the number field generated by ξ. Denote by $\mathcal{O}_K$ the ring of integers of K, and let $R = \mathbb{Z}[\xi] = \mathbb{Z}[x]/(f)$. It holds that $R \subseteq \mathcal{O}_K$. An ideal of a ring R is defined as follows.

Definition 4. *We let* $\mathcal{I}$ *denote an ideal of ring* R, *which satisfies the following conditions:*

1) $\mathcal{I} \subseteq R$ *is a additive subgroup of* R;
2) for any $a \in R$, $a \cdot \mathcal{I} \subseteq \mathcal{I}$ *and* $\mathcal{I} \cdot a \subseteq \mathcal{I}$.

According to the definition, it is obvious that $\mathcal{I}$ is an R-module. A **fractional R-ideal** $\mathcal{I}$ is an R-module contained in K such that for some $a \in K^\times$, $a\mathcal{I} \subseteq R$. A fractional R-ideal is said to be invertible if there exists a fractional R-ideal $\mathcal{J}$ such that $\mathcal{I}\mathcal{J} = R$. In this case, the inverse is $\mathcal{I}^{-1} = \{x \in K : x\mathcal{I} \subseteq R\}$. Every $\mathcal{O}_K$-ideal is invertible.

For an R-ideal $\mathcal{I}$, the **norm of** $\mathcal{I}$ is defined as $N_R(\mathcal{I}) = |R/\mathcal{I}|$, and we will omit the subscript when $R = \mathcal{O}_K$. It satisfies $N_R(\mathcal{I}\mathcal{J}) = N_R(\mathcal{I})N_R(\mathcal{J})$ for every R-ideals $\mathcal{I}$, $\mathcal{J}$.

For any $a \in K$, we denote $\phi_a : K \longrightarrow K$ the $\mathbb{Q}$-linear endomorphism on K defined by the multipication by a, when K is seen as a $\mathbb{Q}$-linear space. Hence we define **the trace of** a **over** K $Tr_K(a)$ by $Tr_K(\phi_a)$.

The **dual of a fractional R-ideal** $\mathcal{I}$ is $\mathcal{I}^\vee = \{\alpha \in K : Tr_K(\alpha\mathcal{I}) \subseteq \mathbb{Z}\}$ and this is still a fractional R-ideal. We have $\mathcal{I}\mathcal{I}^\vee = R^\vee$ and $\mathcal{I}^{\vee\vee} = \mathcal{I}$. Directly, $\mathcal{I}^\vee = \mathcal{I}^{-1}R^\vee$ when $\mathcal{I}$ is invertible. **The discriminant of the number field** K is defined as $\Delta_K = \mathcal{N}((\mathcal{O}_K^\vee)^{-1})$ and this is a invariant of the number field K.

Since K is a d-extension over $\mathbb{Q}$, there are d different homomorphic embeddings σ_i, $i \in [d] : K \mapsto \mathbb{C}$, satisfying that $\sigma_i|_{\mathbb{Q}} = id_{\mathbb{Q}}$. Without loss of generality, assume that we have the first t_1 real embeddings and the last $2t_2$ complex embeddings such that $t_1 + 2t_2 = d$. Moreover, for any $a \in K$, assume that $\sigma_{t_1+t_2+j}(a) = \overline{\sigma_{t_1+j}(a)}$. We define $\mathbb{H} \subseteq \mathbb{C}^d$ as $\mathbb{H} = \{\mathbf{x} \in \mathbb{R}^{t_1} \times \mathbb{C}^{2t_2} : \forall j \in$

$[t_2]$, $x_{t_1+t_2+j} = \overline{x_{t_1+j}}\}$. It is straightforward to verify that $\mathbb{H}$ is a d-dimensional $\mathbb{R}$-linear space with orthonormal basis given by the columns of $\mathbf{U}_{\mathbb{H}}$, where

$$\mathbf{U}_{\mathbb{H}} = \frac{1}{\sqrt{2}} \begin{bmatrix} \sqrt{2}\mathbf{I}_{t_1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I}_{t_2} & i\mathbf{I}_{t_2} \\ \mathbf{0} & \mathbf{I}_{t_2} & -i\mathbf{I}_{t_2} \end{bmatrix}.$$

Now we are ready to define the canonical embedding.

Definition 5 (Canonical Embedding). *The Canonical embedding σ is defined as a map from $K_{\mathbb{R}}$ to $\mathbb{H}$, which maps $a \in K_{\mathbb{R}}$ to $\sigma(a) = (\sigma_0(a), \ldots, \sigma_{d-1}(a))$.*

A number field K of extension index d can be considered as a free d-dimensional $\mathbb{Q}$-module with basis $\{1, \xi, \xi^2 \ldots \xi^{d-1}\}$. Let $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$, thus K can be considered as a subset of $K_{\mathbb{R}}$. It is a d-dimension $\mathbb{R}$-linear space with basis $\{1, \xi, \xi^2 \ldots \xi^{d-1}\}$. Now we are ready to define the coefficient embedding.

Definition 6 (Coefficient Embedding). *The coefficient embedding is defined as a map τ from $K_{\mathbb{R}}$ to $\mathbb{R}^d$, which maps $a \in K_{\mathbb{R}}$ to $\tau(a) = (a_0, a_1, \ldots, a_{d-1})^\top$, which are the unique coefficients such that $a = \sum_{i=0}^{d-1} a_i \xi^i$.*

We define the rotation matrix of an element $a \in K_{\mathbb{R}}$ as

$$\mathsf{rot}(a) = (\tau(a)^\top, \tau(\xi a)^\top, \tau(\xi^2 a)^\top, \ldots \tau(\xi^{d-1} a)^\top)^\top.$$

Furthermore, for any element $a \in K_{\mathbb{R}}$, we define the matrix:

$$\mathcal{M}(a) = \left(\tau\left((\xi^{d-1+j-i} a)_{d-1}\right)\right)_{i \in [d], j \in [d]},$$

where the entry in the i-th row and j-th column is $\tau\left((\xi^{d-1+j-i} a)_{d-1}\right)$.

Hence we can map $K_{\mathbb{R}}$ to $\mathbb{R}^d$ with $\sigma_{\mathbb{H}} = \mathbf{U}_{\mathbb{H}}^{\dagger} \sigma$. We extend the embeddings to the matrices in $K_{\mathbb{R}}^{m \times n}$ in the natural way by concatenating the embedding vectors of each item, i.e., for any $\mathbf{A} = (a_{i,j})_{i \in [m], j \in [n]}$, $\tau(\mathbf{A}) = (\tau(a_{i,j}))_{i \in [m], j \in [n]}$ and similarly for σ, $\sigma_{\mathbb{H}}$ and rot.

Actually, we can use a Vandemonde matrix to bridge coefficient embedding and canonical embedding: for $\forall a \in K_{\mathbb{R}}$, $\sigma(a) = \mathbf{V}_K \tau(a)$, where

$$\mathbf{V}_K = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{d-1} \\ \vdots & \vdots & & \vdots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix}.$$

Let $\mathbf{V}_K$ be a Vandermonde matrix. In this paper, we specifically consider the field $K = \mathbb{Q}[x]/(x^d - C)$. Regarding the norm of the Vandermonde matrix over $K = \mathbb{Q}[x]/(x^d - C)$, where C is a constant, we recall the results in the following lemma, which are presented in Section 4.2 of [RSW18].

Lemma 3 ([RSW18, Section 4.2 restated]). *Let d be a positive integer. Let K be the field $\mathbb{Q}[x]/f$, where $f = x^d - C$ and C is a constant, then $\|\mathbf{V}_K\|_2 \leqslant d|C|$ and $\|\mathbf{V}_K^{-1}\|_2 \leqslant \sqrt{d}$.*

It is obvious that $\tau : K_{\mathbb{R}} \longrightarrow \mathbb{R}^d$ is a bijection, and the matrices $\mathbf{U}_{\mathbb{H}}$ and $\mathbf{V}_K$ are invertible, the maps σ and $\sigma_{\mathbb{H}}$ are bijections. In general, τ, σ and $\sigma_{\mathbb{H}}$ over $K_{\mathbb{R}}^{m\times n}$ are also bijections.

In addition, the expansion factor of a polynomial $f \in \mathbb{Z}[x]$ is required in our analysis.

Definition 7 (Expansion Factor). *For $q \geqslant 2$ and $f \in \mathbb{Z}[x]$ of degree d, the expansion factor of the polynomial f is defined as: $EF(f) := \max_{g\in\mathbb{Z}^{<2d-1}[x]\setminus\{0\}}\{\|g \bmod f\|_\infty/\|g\|_\infty\}$.*

In the remainder of this paper, we require the polynomial f to satisfy the condition $EF(f) \leqslant \mathsf{poly}(d)$, where $EF(f)$ denotes the expansion factor of f. Polynomials satisfying this condition are known to exist. Specifically, let $f = x^d + g$, where $\deg(g) \leqslant d/2$ and $|g|_\infty \leqslant \mathsf{poly}(d)$. Lyubashevsky et al [LM06] showed that such polynomials admit a polynomially bounded expansion factor.

3.3 Rényi Divergence

Rényi divergence is widely used in information theory. Recently, it has also found applications in lattice-based cryptography [LPSS14,BLL+15,BLRL+18]. In this work, we consider scenarios where two distributions are not statistically close, yet their Rényi divergence remains bounded by a polynomial in the security parameter.

Definition 8. *Let P and Q be two discrete distributions satisfying $supp(P) \subseteq supp(Q)$. The Rényi divergences of orders 2 and ∞ are defined as below:*

$$R(P\|Q) := \sum_{x\in\mathsf{supp}(P)} \frac{P(x)^2}{Q(x)} \text{ and } R_\infty(P\|Q) := \max_{x\in\mathsf{supp}(P)} \frac{P(x)}{Q(x)}.$$

We also recall some important properties of Rényi divergence, which will be extensively used throughout this paper. We use the statement in [DSSS21].

Lemma 4 ([DSSS21, Lemma 1]). *Let P and Q be two discrete distributions such that $supp(P) \subseteq supp(Q)$. The following properties hold:*

* ***Log Positivity**: $R(P\|Q) \geqslant R(P\|P) = 1$.*
* ***Data Processing Inequality**: $R(P^f\|Q^f) \leqslant R(P\|Q)$ for any function f, where X^f denotes the distribution of $f(x)$ when sampling $x \hookleftarrow X$.*
* ***Multiplicativity**: Let P and Q be two distributions of a pair of random variables X_1 and X_2. P_i and Q_i denote the marginal distribution of X_i under P and Q respectively. In general, we have $R(P\|Q) \leqslant R_\infty(P_1\|Q_1) \cdot \max_{x_1\in supp(P_1)} R((P_2|x_1)\|(Q_2|x_1))$. If X_1 and X_2 are independent, $R(P\|Q) = R(P_1\|Q_1)R(P_2\|Q_2)$.*
* ***Probability Preservation**: $E \subseteq supp(Q)$ is an arbitrary event. Then, $Q(E) \geqslant P(E)^2/R(P\|Q)$.*

3.4 Gaussian and Discrete Gaussian Distributions

We now recall several important properties of the Gaussian distribution. Let Σ be a full-rank, symmetric, positive definite matrix in $\mathbb{R}^{n\times n}$. The n-dimensional Gaussian function with covariance matrix Σ and center $\mathbf{c} \in \mathbb{R}^n$ is defined as $\rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x}) = \exp(-\pi \cdot (\mathbf{x}-\mathbf{c})^T \Sigma^{-1}(\mathbf{x}-\mathbf{c}))$, for any $\mathbf{x} \in \mathbb{R}^n$. In particular, if Σ is a diagonal matrix with all diagonal entries equal to r^2, then the function simplifies to $\rho_{r,\mathbf{c}}(\mathbf{x}) = \exp(-\pi \cdot \|\mathbf{x}-\mathbf{c}\|^2/r^2)$. Furthermore, if the center $\mathbf{c} = \mathbf{0}$, we denote the function as $\rho_r(\mathbf{x}) = \exp(-\pi \cdot \|\mathbf{x}\|^2/r^2)$.

Based on the Gaussian function $\rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x}) = \exp\left(-\pi \cdot (\mathbf{x}-\mathbf{c})^\top \Sigma^{-1}(\mathbf{x}-\mathbf{c})\right)$, the corresponding Gaussian (or normal) distribution is defined as follows.

Definition 9. *Let $\mathbb{R}^n$ be the Euclidean space, and let Σ be a positive definite matrix in $\mathbb{R}^{n\times n}$. The Gaussian (or normal) distribution $\mathcal{N}_{\sqrt{\Sigma},\mathbf{c}}$ over $\mathbb{R}^n$ with center $\mathbf{c} \in \mathbb{R}^n$ and covariance matrix Σ is defined by the density function:*

$$p(\mathbf{x},\mathbf{c},\Sigma) = \rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x})/\mathsf{det}(\Sigma)^{\frac{1}{2}}$$

In practice, the discrete Gaussian distribution is typically used in place of the continuous one. Its formal definition is given below.

Definition 10. *For a full-rank, symmetric, positive definite $n\times n$ matrix Σ, and Λ a n-dimension full-rank lattice, we define the n-dimension discrete Gaussian distribution over a lattice coset $\Lambda + \mathbf{v}$, $D_{\Lambda+\mathbf{v},\sqrt{\Sigma},\mathbf{c}}$ by*

$$\forall x \in \Lambda + \mathbf{v}: \quad D_{\Lambda+\mathbf{v},\sqrt{\Sigma},\mathbf{c}}(\mathbf{x}) = \rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x})/\rho_{\sqrt{\Sigma},\mathbf{c}}(\Lambda+\mathbf{v}),$$

where $\rho_{\sqrt{\Sigma},\mathbf{c}}(\Lambda+\mathbf{v}) = \sum_{\mathbf{x}\in\Lambda+\mathbf{v}} \rho_{\sqrt{\Sigma},\mathbf{c}}(\mathbf{x})$.

In [BJRLW23], the authors extend the notion of Gaussian distributions from $K_\mathbb{R}$ to the product space $K_\mathbb{R}^n$. Since the canonical embedding σ induces a bijection between $K_\mathbb{R}^n$ and $\mathbb{R}^{nd}$, the discrete Gaussian distribution over $K_\mathbb{R}^n$ can be naturally defined via this embedding as follows.

Definition 11. *Let Σ be a full-rank, symmetric, positive definite matrix in $\mathbb{R}^{nd\times nd}$, and let $\mathcal{M}$ be an R-submodule of $K_\mathbb{R}^n$. For a coset representative $\mathbf{v} \in K_\mathbb{R}^n/\mathcal{M}$ and a center $\mathbf{c} \in K_\mathbb{R}^n$, we define the discrete Gaussian distribution over $K_\mathbb{R}^n$ as follows: First, sample $\mathbf{x} \hookleftarrow D_{\sigma(\mathbf{v}+\mathcal{M}),\sqrt{\Sigma},\sigma(\mathbf{c})}$ over $\mathbb{R}^{nd}$, where σ is the canonical embedding. Then, map $\mathbf{x}$ back to $K_\mathbb{R}^n$ via σ^{-1} to obtain a sample from the discrete Gaussian distribution over $K_\mathbb{R}^n$. We denote the distribution by $D^{\mathbb{H}^n}_{\mathbf{v}+\mathcal{M},\sqrt{\Sigma},\mathbf{c}}$ over $K_\mathbb{R}^n$. We can omit the subscript when $\mathcal{M} = \mathcal{O}_K^n$. Similarly, we can define $\mathcal{N}^{\mathbb{H}^n}_{\sqrt{\Sigma},\mathbf{c}}$ over the space $\mathbb{H}^n$.*

Besides the canonical embedding approach, we may alternatively define discrete Gaussian distributions via the coefficient embedding. For a vector of polynomials $\mathbf{a} \in (\mathbb{R}[x]/(f))^n \cong K_\mathbb{R}^n$, let τ denote the coefficient embedding, which maps $\mathbf{a}$ to $\tau(\mathbf{a}) \in \mathbb{R}^{nd}$. Since τ is a bijection, if we write $\mathbf{x} \hookleftarrow \psi$ for some distribution ψ over $\mathbb{R}^{nd}$, and $\mathbf{x} \in K_\mathbb{R}^n$, we mean that we first sample $\overline{\mathbf{x}} \hookleftarrow \psi$ in $\mathbb{R}^{nd}$, and

then set $\mathbf{x} = \tau^{-1}(\overline{\mathbf{x}})$. In this way, we can also define discrete Gaussian distributions over $K_{\mathbb{R}}^n$ by considering the Gaussian distribution over the concatenated coefficient vectors of polynomials in $\mathbb{R}[x]/(f)$. When we write $e(x) \hookleftarrow D_{\mathbb{Z}[x]/f,\sqrt{\Sigma}}$, we refer to sampling the coefficient vector of $e(x)$ from the discrete Gaussian distribution $D_{\mathbb{Z}^d,\sqrt{\Sigma}}$.

Since in this paper we only consider the infinity norm of the error terms, the notation $D_{\mathbb{Z}^d,\sqrt{\Sigma},B}$ (resp. $D_{\mathbb{Z}[x]/f,\sqrt{\Sigma},B}$) denotes the distribution restricted to vectors (resp. polynomials) whose each entry (resp. coefficient) are bounded in absolute value by B.

Next, we recall the Poisson Summation Formula, a useful tool for analyzing the distance between distributions.

Lemma 5 (Poisson Summation Formula). *For any n-dimensional lattice Λ and any function $f : \mathbb{R}^n \to \mathbb{C}$, it holds that $f(\Lambda) = \det(\Lambda^*)\hat{f}(\Lambda^*)$, where $\hat{f}$ is the Fourier transform of f. Specially, for $f(\mathbf{x}) = \rho_r(\mathbf{x} + \mathbf{u})$ for any $\mathbf{u} \in \mathbb{R}^n$, it holds that*

$$\rho_r(\Lambda + \mathbf{u}) = \mathsf{det}(\Lambda^*) \cdot r^n \cdot \sum\nolimits_{\mathbf{x}\in\Lambda^*} \exp(2\pi\sqrt{-1}\langle \mathbf{x}, \mathbf{u}\rangle) \cdot \rho_{1/r}(\mathbf{x}).$$

Intuitively, the probability of sampling a point far from the center of a discrete Gaussian distribution decays rapidly. To formalize this intuition, we recall the following tail bounds for the discrete Gaussian distribution.

Lemma 6 ([PR06, Lem. 1]). *For any n-dimensional lattice Λ, $\mathbf{c} \in \mathsf{span}(\Lambda)$, a positive real number $\varepsilon > 0$, and $r \geqslant 2\eta_\varepsilon(\Lambda)$, and for every $\mathbf{x} \in \Lambda$, we have*

$$D_{\Lambda,r,\mathbf{c}}(\mathbf{x}) \leqslant \frac{1+\varepsilon}{1-\varepsilon} \cdot 2^{-n}.$$

The following lemma implies that the tail of the discrete Gaussian distribution constitutes only a negligible proportion of the total summation. A complete proof can be found in [BKSW18, Lemma 1]. We restate the lemma here.

Lemma 7 ([BKSW18, Lemma 1]). *For any $\kappa, r > 0$, the summation of the Gaussian function satisfies $\rho_r(\mathbb{Z}\backslash[-\sqrt{\kappa}r, \sqrt{\kappa}r]) \leqslant 2^{-\Omega(\kappa)}\rho_r(\mathbb{Z})$.*

In the more general case, the summation outside a sufficiently large Euclidean ball remains negligible. We state the lemma as follows.

Lemma 8 ([Ban93, Lemma 1.5(i)]). *Let $\mathcal{B}_n$ denote the Euclidean unit ball. Then for any lattice Λ and any $r > 0$, $\rho_r(\Lambda\backslash\sqrt{n}r\mathcal{B}_n) < 2^{-2n} \cdot \rho_r(\Lambda)$.*

From Lemma 7, it follows that the summation outside a sufficiently large cube remains negligible. We state the corollary as follows.

Corollary 1. *For any $\kappa, r > 0$, $n = \mathcal{O}(\kappa)$ a positive integer, $B \geqslant \sqrt{\kappa}r$, we have $\rho_r(\mathbb{Z}^n)(1-2^{-\omega(\log(\kappa))}) \leqslant \rho_r(\mathbb{Z}^n)(1-n2^{-\Omega(B^2/r^2)}) \leqslant \rho_r\left((\mathbb{Z}\cap[-B,B])^n\right) \leqslant \rho_r(\mathbb{Z}^n)$, and $1/\rho_r(\mathbb{Z}^n) \leqslant 1/\rho_r\left((\mathbb{Z}\cap[-B,B])^n\right) \leqslant (1+2^{-\omega(\log(\kappa))})/\rho_r(\mathbb{Z}^n)$.*

Proof.

$$\frac{\rho_r\left((\mathbb{Z}\cap[-B,B])^n\right)}{\rho_r(\mathbb{Z}^n)}=\left(\frac{\rho_r\left(\mathbb{Z}\cap[-B,B]\right)}{\rho_r(\mathbb{Z})}\right)^n$$
$$\geqslant(1-2^{-\Omega(B^2/r^2)})^n\geqslant 1-n2^{-\Omega(B^2/r^2)}\geqslant 1-2^{-\omega(\log(\kappa)}.$$

The result follows directly. □

In the following, we recall some useful lemmata concerning the density function of the discrete Gaussian distribution.

Lemma 9 ([Reg09, Claim 3.8]). *For any lattice Λ, $\mathbf{c}\in\mathbb{R}^n$, and $r\geqslant\eta_\varepsilon(\Lambda)$,*

$$\rho_r(\Lambda+\mathbf{c})\in[1-\varepsilon,1+\varepsilon]\cdot r^n\mathsf{det}(\Lambda^*).$$

Lemma 9 directly implies the following two lemmata. One can refer to Supplementary Material B.1 for complete proofs of these two lemmas.

Lemma 10. *Assume that $r_1,r_2\geqslant\eta_\varepsilon(\Lambda)$, and $\varepsilon\leqslant 1/3$*

$$\frac{\rho_{r_1}(\Lambda)}{\rho_{r_2}(\Lambda)}\in\left[\frac{1-\varepsilon}{1+\varepsilon},\frac{1+\varepsilon}{1-\varepsilon}\right]\cdot\left(\frac{r_1}{r_2}\right)^n\subseteq[1-3\varepsilon,1+3\varepsilon]\cdot\left(\frac{r_1}{r_2}\right)^n.$$

Lemma 11. *For any $\mathbf{c}\in\mathbb{R}^n$, $r\geqslant\eta_\varepsilon(\Lambda)$ and $\varepsilon\leqslant 1/3$,*

$$\rho_r(\Lambda+\mathbf{c})\in\left[\frac{1-\varepsilon}{1+\varepsilon},\frac{1+\varepsilon}{1-\varepsilon}\right]\cdot\rho_r(\Lambda)\subseteq[1-3\varepsilon,1+3\varepsilon]\cdot\rho_r(\Lambda).$$

Finally, we introduce a new distribution $D^{Sum}_{\mathbb{Z}^n,r,G}$ as shown below.

Definition 12. *In the integer lattice $\mathbb{Z}^n$, given a positive integer G, we define the following particular sum of discrete Gaussian as:*

$$D^{Sum,G}_{\mathbb{Z}^n,r}(\mathbf{v})=\sum_{\mathbf{x}\in\mathcal{C}(\mathbf{v},\frac{1}{2}G)\bigcap\mathbb{Z}^n}D_{\mathbb{Z}^n,r}(\mathbf{x}),$$

where $\mathcal{C}(\mathbf{v},\frac{1}{2}G)$ is the cube $((-\frac{1}{2}+v_0)G,(\frac{1}{2}+v_0)G]\times\cdots\times((-\frac{1}{2}+v_{n-1})G,(\frac{1}{2}+v_{n-1})G]$.

We next demonstrate that, for a suitable choice of r and G, the Rényi divergence $R(D_{\mathbb{Z}^n,\frac{r}{G}}\|D^{\mathrm{Sum},G}_{\mathbb{Z}^n,r})$ can be bounded polynomially in n.

Lemma 12. *For positive numbers $r,G>0$, $\varepsilon>0$, and $r,\frac{r}{G}\geqslant\eta_\varepsilon(\mathbb{Z}^n)$, the Rényi divergence $R(D_{\mathbb{Z}^n,\frac{r}{G}}\|D^{Sum,G}_{\mathbb{Z}^n,r})$ has an upper bound $(1+3\varepsilon)^2\exp\left((5Gn)/(2r)\right)$. Furthermore, if $r\geqslant\omega(Gn)$, this Rényi divergence has a polynomial-sized upper bound.*

We also require the following lemma, adapted from [MR07, Lemma 4.1]. One can refer to Supplementary Material B.1 for complete proof.

Lemma 13 ([MR07, Lemma 4.1] adapted). *For any $r > 0$, $\mathbf{c} \in \mathbb{R}^n$, and lattice $\mathcal{L}(\mathbf{B}) \subseteq \mathbb{Z}^n$ with $\mathbf{B}$ a basis, the statistical distance between $D_{\mathbb{Z}^n,r,\mathbf{c}} \bmod \mathcal{L}(\mathbf{B})$ and the uniform distribution $U(\mathbb{Z}^n/\mathcal{L}(\mathbf{B}))$ is at most $\frac{r^n}{2\rho_{r,\mathbf{c}}(\mathbb{Z}^n)}\left(\rho_{\frac{1}{r}}(\mathcal{L}(\mathbf{B}^*)) - 1\right) + \frac{1}{2}\left|\frac{r^n}{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} - 1\right|$. In particular, for any $\varepsilon > 0$ and any $r \geqslant \eta_\varepsilon(\mathbf{B})$, the statistical distance is at most $\frac{\varepsilon}{1-\varepsilon}$.*

Then we derive the last Rényi divergence. From Lemma 13 above, it is not surprising that the difference between the distribution $G \cdot D^{Sum,G}_{\mathbb{Z}^n,r} + U(\mathbb{Z}^n_G)$ and the distribution $D_{\mathbb{Z}^n,r}$ can be bounded. We formally compute the Rényi divergence between these two distributions below. One can refer to Lemma B.1 for complete proof.

Lemma 14. *Let κ be the security parameter, $n = \mathsf{poly}(\kappa)$, r be a positive number satisfying $r \geqslant \eta_\varepsilon(\mathbb{Z}^n)$ and G be a positive integer such that $\frac{r}{G} \geqslant \eta_\varepsilon(\mathbb{Z}^n)$, where $\varepsilon = 2^{-\omega(\log(\kappa))}$. We have:*

$$R(G \cdot D^{Sum,G}_{\mathbb{Z}^n,r} + U(\mathbb{Z}^n_G) \| D_{\mathbb{Z}^n,r}) \leqslant (1+3\varepsilon)^2 \exp\left((9nG)/(2r)\right).$$

Last, we state the tail bound of discrete Gaussian distribution applied in this paper (refer to Supplementary Material B.1 for proof).

Lemma 15. *For any κ, $r > 0$, n a positive integer, $B \geqslant \sqrt{\kappa} r$, the statistical distance satisfies $\Delta(D_{\mathbb{Z}^n,r,B}, D_{\mathbb{Z}^n,r}) \leqslant n \cdot 2^{-\Omega(B^2/r^2)} \leqslant n \cdot 2^{-\Omega(\kappa)}$.*

Additional properties of the discrete Gaussian distribution used in this paper are provided in Supplementary Material B.1.

3.5 Module Learning with Errors Problems

In the subsection, we present the Module Learning with Errors (MLWE) problem, along with its polynomial variant, referred to as Polynomial-MLWE (P-MLWE).

Definition 13 (MLWE and P-MLWE Distribution). *For K a number field with extension index d, Σ a full-rank, positive definite $d \times d$ matrix and $q \geqslant 2$ an positive integer,*

* MLWE ***distribution*** $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},\varphi,f}$*: For $\mathbf{s} \in (\mathcal{O}_K/q\mathcal{O}_K)^n$, the $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},\varphi,f}$ distribution over $(\mathcal{O}_K/q\mathcal{O}_K)^{m\times n} \times (K_{\mathbb{R}}/q\mathcal{O}_K^\vee)^m$ is obtained by sampling $\mathbf{A} \hookleftarrow U((\mathcal{O}_K/q\mathcal{O}_K)^{m\times n})$ and $\mathbf{e} \hookleftarrow \varphi$, where $supp(\varphi) \subset K^m_{\mathbb{R}}$, and returning the pair $(\mathbf{A}, \mathbf{A}\cdot\mathbf{s}+\mathbf{e})$. When $\mathbf{e} \hookleftarrow (D^{\mathbb{H}}_{\mathcal{O}_K,\sqrt{\Sigma}})^m$ (resp. $\Sigma = r^2\mathbf{I}_d$), the distribution will be rewritten as $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},\sqrt{\Sigma},f}$ (resp. $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},r,f}$).*
* P-MLWE ***distribution*** $\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},\varphi,f}$*: For $\mathbf{s} \in (\mathbb{Z}_q[x]/(f))^n$, the P-MLWE distribution over $(\mathbb{Z}_q[x]/(f))^{m\times n} \times (\mathbb{R}_q[x]/(f))^m$ is obtained by sampling $\mathbf{A} \hookleftarrow U((\mathbb{Z}_q[x]/(f))^{m\times n})$ and $\mathbf{e} \hookleftarrow \varphi$, where $supp(\varphi) \subset K^m_{\mathbb{R}}$, and returning the pair $(\mathbf{A}, \mathbf{A}\cdot\mathbf{s}+\mathbf{e})$. When $\mathbf{e} \hookleftarrow (D_{\mathbb{Z}[x]/f,\sqrt{\Sigma}})^m$ (resp. $\Sigma = r^2\mathbf{I}_d$), the distribution can be rewritten as $\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},\sqrt{\Sigma},f}$ (resp. $\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},r,f}$). Furthermore, if the magnitude of each coefficient of e_i, has a bound B, the distribution will be written as $\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},(r,B),f}$.*

With the above distributions, we now define the MLWE and P-MLWE problems, focusing on their search variants.

Definition 14 (Search $\mathsf{MLWE}^{m,n}_{q,\chi,\varphi,f}$ (resp. $\mathsf{P\text{-}MLWE}^{m,n}_{q,\chi',\varphi',f}$) problem). *For integers m, n, select a secret $\mathbf{s} \hookleftarrow \chi$ (where χ is over $(\mathcal{O}_K/q\mathcal{O}_K)^n$ (resp. select a secret $\mathbf{s} \hookleftarrow \chi'$ where χ' is over $(\mathbb{Z}_q[x]/(f))^n$)). Then, sample $(\mathbf{A}, \mathbf{b}) \hookleftarrow \mathsf{MLWE}^{m,n} q, \mathbf{s}, \varphi, f$ (resp. $(\mathbf{A}, \mathbf{b}) \hookleftarrow \mathsf{P\text{-}MLWE}^{m,n} q, \mathbf{s}, \varphi', f$) and output it to the adversary. The adversary is asked to recover $\mathbf{s} \in (\mathcal{O}_K/q\mathcal{O}_K)^n$ (or $\mathbf{s} \in (\mathbb{Z}_q[x]/(f))^n$). If $\mathbf{s} \hookleftarrow (D^{\mathbb{H}}_{\mathcal{O}_K,\sqrt{\Sigma}})^n$ (resp. $\mathbf{s} \hookleftarrow \left(D_{\mathbb{Z}[x]/f,\sqrt{\Sigma'}}\right)^n$), we denote this problem as Search $\mathsf{MLWE}^{m,n}_{q,\sqrt{\Sigma},\varphi,f}$ (resp. $\mathsf{P\text{-}MLWE}^{m,n}_{q,\sqrt{\Sigma'},\varphi',f}$).*

In particular, when $n = 1$, the $\mathsf{MLWE}^{m,n}_{q,\chi,\varphi,f}$ problem becomes the Ring LWE ($\mathsf{RLWE}^{m}_{q,\chi,\varphi,f}$) problem as defined in [LPR10], and the $\mathsf{P\text{-}MLWE}^{m,n}_{q,\chi',\varphi',f}$ problem becomes the Polynomial LWE ($\mathsf{PLWE}^{m}_{q,\chi',\varphi',f}$) problem as introduced in [SSTX09]. Furthermore, when $f(x) = x$, this reduces to the LWE problem in [Reg05], denoted as $\mathsf{LWE}^{m,n}_{q,\chi,\varphi}$.

3.6 Properties about the Connections between $\mathbb{Z}_{f(q)}$ and $\mathbb{Z}_q[x]/f$

In this section, we review some useful properties of the maps between $\mathbb{Z}_{f(q)}$ and $\mathbb{Z}_q[x]/f$ given in [DSSS21], which are required in this work. We first recall the integer range $I_{f,q}$ as defined in [DSSS21].

Definition 15. *Let $q > 2$ and f a monic and irreducible polynomial of degree d in $\mathbb{Z}[x]$, We define:*

$$I_{f,q} = \begin{cases} \left(\frac{q}{2}\frac{q^d-1}{q-1} - f(q), \frac{q}{2}\frac{q^d-1}{q-1}\right] & \text{if } q \text{ even and } q\frac{q^d-1}{q-1} \geqslant f(q) \geqslant q^d, \\ \left(-\frac{q-2}{2}\frac{q^d-1}{q-1}, f(q) - \frac{q-2}{2}\frac{q^d-1}{q-1}\right] & \text{if } q \text{ even and } q^d > f(q) > (q-2)\frac{q^d-1}{q-1}, \\ (-f(q)/2, f(q)/2] & \text{otherwise.} \end{cases}$$

In this paper, we use the integers in $I_{f,q} \subseteq \mathbb{Z}$ as the representatives of elements in the ring $\mathbb{Z}_{f(q)}$. To avoid ambiguity, when we write $a \in \mathbb{Z}_{f(q)}$, we mean that $a \in I_{f,q}$.

Next, we introduce the decomposition of an integer together with two important maps, $\Phi^{(f)}_q$ and $\mathsf{Eval}^{(f)}_q$.

Definition 16 (Centered q-ary decomposition of an integer). *For $q > 2$ and $a \in \mathbb{Z}$, for every $0 \leqslant i \leqslant \lceil \log_q a \rceil$, we define $a_i := \frac{a - \sum_{j<i} a_j q^j}{q^i} \bmod q$, and $\mathbf{a} = (a_0, a_1, \ldots, a_{d-1})^T$ as the centered q-ary decomposition of a.*

Based on this integer decomposition, we define a conversion between the integer ring $\mathbb{Z}$ and the polynomial ring $\mathbb{Z}_q[x]$, as well as between the modular ring $\mathbb{Z}_{f(q)}$ and the quotient ring $\mathbb{Z}_q[x]/(f)$.

Definition 17. *For $q > 2$, we have the map Φ_q, mapping $\forall a \in \mathbb{Z}$ to $\sum_{i=0}^{\lceil \log_q a \rceil} a_i x^i$, where a_i is defined in Definition 16; and its inverse map Eval_q, mapping $\forall P(x) \in \mathbb{Z}_q[x]$ to $P(q) \in \mathbb{Z}$.*

When we consider the conversion between the set $\mathbb{Z}_{f(q)}$ of integers modulo $f(q)$ and the integer polynomial ring $\mathbb{Z}_q[x]/(f)$, we have $\Phi_q^{(f)}(a) = \Phi_q(a) \bmod (q, f(x))$ for any $a \in \mathbb{Z}_{f(q)}$ and $\mathsf{Eval}_q^{(f)}(P(x)) = \mathsf{Eval}_q(P(x)) \bmod f(q) \in I_{f,q}$ for any $P(x) \in \mathbb{Z}_q[x]/f$.

It is clear that neither $\Phi_q^{(f)}$ nor Φ_q is a ring-homomorphism, i.e., carries arise when performing addition and multiplication. To be more precise, let $c_f^{(a)}(a,b) = \Phi_q^{(f)}(a+b) - \Phi_q^{(f)}(a) - \Phi_q^{(f)}(b) \bmod f$ and $c_f^{(m)}(a,b) = \Phi_q^{(f)}(a \cdot b) - \Phi_q^{(f)}(a) \cdot \Phi_q^{(f)}(b) \bmod f$. Similarly, let $c^{(a)}(a,b) \bmod q = \Phi_q(a+b) - \Phi_q(a) - \Phi_q(b) \bmod q$ and $c^{(m)}(a,b) \bmod q = \Phi_q(a \cdot b) - \Phi_q(a) \cdot \Phi_q(b) \bmod q$. In fact, what we are concerned with is not the exact values of the carries but rather an upper bound on their norm. In [DSSS21], Devevey et al gave the following bound of $c^{(a)}(a,b)$ and $c^{(m)}(a,b)$ that we require.

Lemma 16 ([DSSS21, Lemma 3]). *For $q > 2$, $a, b \in \mathbb{Z}$, let $q' = \lfloor (q-1)/2 \rceil$. We have:*

$$\|c^{(a)}(a,b)\|_\infty \leqslant 1, \text{ and}$$
$$\|c^{(m)}(a,b)\|_\infty \leqslant \frac{q + q' + \min(\|\Phi_q(a)\|_\infty \cdot \|\Phi_q(b)\|_1, \|\Phi_q(b)\|_\infty \cdot \|\Phi_q(a)\|_1)}{q-1}.$$

Both $c_f^{(a)}(a,b)$ and $c_f^{(m)}(a,b)$ can be computed based on $c^{(a)}(a,b)$ and $c^{(m)}(a,b)$ as follows.

Lemma 17 ([DSSS21, Lemma 7]). *For $q > 2$ and $a, b \in I_{f,q}$, where $f \in \mathbb{Z}[x]$ is a monic and irreducible polynomial whose coefficients in $(-q/2, q/2)$, we have:*

* ***Addition carries**: for some $\delta_0, \delta_1 \in \{-1, 0, 1\}$,*

$$c_f^{(a)}(a,b) = c^{(a)}(a,b) + c^{(a)}(a+b, \delta_0 f(q)) + (\delta_0 + \delta_1 + a_m + b_m) f.$$

  a_m, b_m here is the same as the ones in Definition 16 and in this case, we have $a_m, b_m \in \{-1, 0, 1\}$.
* ***Multiplication carries**:*

$$c_f^{(m)}(a,b) = c^{(m)}(a,b) + c^{(m)}(-\delta, f(q)) + c^{(a)}(a \cdot b, -\delta f(q)) \bmod f,$$

  where $\delta = \lfloor (a \cdot b - (a \cdot b \bmod f(q)))/f(q) \rceil$.

In addition to the properties of carries, we are also interested in the injectivity and surjectivity of $\Phi_q^{(f)}$ and $\mathsf{Eval}_q^{(f)}$. Furthermore, although these maps are not bijective, but they are close to being bijections.

Lemma 18 ([DSSS21, Lemma 4]). *For $q > 2$ and $f \in \mathbb{Z}[x]$ a monic and irreducible polynomial whose coefficients in the range $(-q/2, q/2)$, we have the following two cases:*

* *If* $f(q) \geqslant q^d$*, for any* $P \in \mathbb{Z}_q[x]/f$*,* $\Phi_q^{(f)}(\mathsf{Eval}_q^{(f)}(P)) = P$*, hence* $\Phi_q^{(f)}$ *is surjective and* $\mathsf{Eval}_q^{(f)}$ *is injective.*
* *If* $f(q) < q^d$*, for any* $a \in I_{f,q}$*,* $\mathsf{Eval}_q^{(f)}(\Phi_q^{(f)}(a)) = a \bmod f(q)$*, hence* $\Phi_q^{(f)}$ *is injective and* $\mathsf{Eval}_q^{(f)}$ *is surjective.*

In [DSSS21], Devevey et al also consider the numbers of predecessors of the surjection $\mathsf{Eval}_q^{(f)}$ when $f(q) < q^d$ and $\Phi_q^{(f)}$ when $f(q) \geqslant q^d$. We will also make use of these properties as shown below.

Lemma 19 ([DSSS21, Lemma 5 and Lemma 6]).

1) ***(Surjectivity of the evaluation, when*** $f(q) < q^d$***).*** *Let* $q > 2$ *and* $f \in \mathbb{Z}[x]$ *be a monic and irreducible polynomial of degree* d *such that* $f(q) < q^d$ *and whose coefficients belong to* $(-\frac{q}{2}, \frac{q}{2})$*. Then for any* $a \in \mathbb{Z}_{f(q)}$*, there exist at most* 2 *polynomials* $P, Q \in \mathbb{Z}[x]/f(x)$ *such that* $P(q) \bmod f(q) = Q(q) \bmod f(q) = a$*. When evaluating* P *in* q*, the coefficients of* P *are taken in* $(-\frac{q}{2}, \frac{q}{2}]$*.*
2) ***(Surjectivity of the map*** $\Phi_q^{(f)}$***, when*** $f(q) \geqslant q^d$***).*** *Let* $q > 2$ *and* $f \in \mathbb{Z}[x]$ *be a monic polynomial of degree* d *such that* $f(q) \geqslant q^d$ *and whose coefficients belong to* $(-\frac{q}{2}, \frac{q}{2})$*. For any* $P \in \mathbb{Z}_q[x]/f$*, there exist at most* 3 *integers* $a, b, c \in \mathbb{Z}_{f(q)}$ *such that* $P = \Phi_q^{(f)}(a) = \Phi_q^{(f)}(b) = \Phi_q^{(f)}(c)$*. Remember that when applying* $\Phi_q^{(f)}$ *on* a*, the representative of* a *is taken in* $I_{f,q}$*.*

At the end of this subsection, we define the integer version of MLWE (IP-MLWE) as a generalization of IPLWE defined in [DSSS21] to the module setting.

Definition 18. IP-MLWE *distribution* $\mathsf{IP\text{-}MLWE}_{q,\mathbf{s},\varphi,f}^{m,n}$*: Let* f *a monic and irreducible polynomial of degree* d*. Let* q, m, n *be positive integers. Let* φ *be a distribution over* $\mathbb{Z}[x]/f$*. The distribution* $\mathsf{IP\text{-}MLWE}_{q,\mathbf{s},\varphi,f}^{m,n}$ *over* $\mathbb{Z}_{f(q)}^{m\times n} \times \mathbb{Z}_{f(q)}^{m}$ *is obtained as follows: For a fixed* $\mathbf{s} \in \mathbb{Z}_{f(q)}^n$*, sample* $\mathbf{A} \hookleftarrow U\left(\mathbb{Z}_{f(q)}^{m\times n}\right)$*, sample the error term* $\mathbf{e} \hookleftarrow \left(\mathsf{Eval}_q^{(f)}(\varphi)\right)^m$ *and output the pair* $(\mathbf{A}, \mathbf{As} + \mathbf{e} \bmod f(q))$*. When* $n = 1$*, this distribution is called the* IPLWE *distribution.*

Definition 19. *Search version of* IP-MLWE *problem: We inherit the parameter settings in Definition 18.* $\mathcal{S}$ *is a distribution over* $\mathbb{Z}_{f(q)}^n$*. Select* $\mathbf{s} \hookleftarrow \mathcal{S}$*, select* $(\mathbf{A}, \mathbf{As} + \mathbf{e} \bmod f(q)) \hookleftarrow \mathsf{IP\text{-}MLWE}_{q,\mathbf{s},\varphi,f}^{m,n}$ *and output the pair. The adversary tries to find the secret* $\mathbf{s}$*. We denote this problem as* $\mathsf{IP\text{-}MLWE}_{q,\mathcal{S},\varphi,f}^{m,n}$*. When* $n = 1$*, this problem is called the* IPLWE *problem.*

For more properties about the connections between $\mathbb{Z}_{f(q)}$ and $\mathbb{Z}_q[x]/f$, one can refer to Supplementary Material B.4.

3.7 Quantum Computation

In this section, we first recall the well known *Quantum Fourier Transforms*. In the standard mathematical notation, the discrete Fourier transform takes as

input a vector of complex numbers $x_0, \ldots, x_{N-1}$ where N is a fixed parameter representing the length of the vector. It outputs the transformed data, a vector of complex numbers $y_0, \ldots, y_{N-1}$, defined by

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi\sqrt{-1}jk/N}.$$

The quantum Fourier transform is essentially the same transformation, though its conventional notation differs slightly. The quantum Fourier transform on an orthonormal basis $|0\rangle, \ldots, |N-1\rangle$ is defined as a linear operator that acts on the basis states as follows.

$$|j\rangle \to \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi\sqrt{-1}jk/N} |k\rangle.$$

We also recall the the complexity of quantum Fourier transform.

Lemma 20 ([NC10, Section 5.1] adapted). *For an orthonormal quantum state basis $|0\rangle, \ldots, |N-1\rangle$, there exists an algorithm for performing the quantum Fourier transform with $\Theta((\log(N))^2)$ quantum gates.*

Next, we recall a result about sampling quantum superposition state with Gaussian-distributed amplitudes.

Lemma 21 ([BKSW18, Lemma 4]). *Given a parameter κ and a deviation parameter r, there exists a polynomial-time (in κ) algorithm generating a state within l_2 distance $2^{-\Omega(\kappa)}$ of the normalized state corresponding to $\sum_{x\in\mathbb{Z}} \rho_r(x)|x\rangle$ Furthermore, a state with in ℓ_2 distance $2^{-\Omega(\kappa)}$ of the normalized state corresponding to $\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_r(\mathbf{c})|\mathbf{c}\rangle$ can also be outputted by a polynomial-time (in κ) quantum algorithm, where $d \leqslant \mathsf{poly}(\kappa)$.*

Quantum measurement extracts the transmitted information from quantum states, hence it plays an important role in quantum computation. Sometimes the positive-operator valued measure (POVM) is more efficient of obtaining information. We give the definition of POVM below.

Definition 20 (Positive-Operator Valued Measure). *In a POVM measurement, the measurement operator system $\{Q_i\}_{i\in M}$ over some Hilbert space H, where M is an alphabet set of all possible outcomes of the measurement, gave the properties:*

1) *Q_i is Hermitian: $Q_i = Q_i^\dagger$;*
2) *Q_i is positive semi-definite: For any quantum state $|\psi\rangle$ on this Hilbert space H, $\langle\psi| Q_i |\psi\rangle \geqslant 0$;*
3) *$\{Q_i\}_{i\in M}$ forms a resolution of the identity on the space H: $\sum_{i\in M} Q_i = \mathbf{I}_H$, where $\mathbf{I}_H$ is the identity operator over Hilbert space H.*

The trace distance is used to measure the difference between two quantum states. It can be seen as an adaptation of the statistical distance in the quantum setting. The formal definition is given below.

Definition 21 (Trace Distance). *Let $|\psi\rangle, |\varphi\rangle$ be two quantum states on some Hilbert space H. The trace distance between these two quantum states is defined as:*

$$\Delta_{tr}(|\psi\rangle, |\phi\rangle) = \frac{1}{2} Tr\left(\sqrt{(|\psi\rangle\langle\psi| - |\varphi\rangle\langle\varphi|)^2}\right),$$

where $Tr(\cdot)$ is the trace of linear operators.

According to the definition, the trace distance preserved under unitary transformations, and we state it formally in the following lemma.

Lemma 22. *Let $|\psi\rangle, |\varphi\rangle$ be two quantum states on some Hilbert space H. Let U be a unitary transformation, then $\Delta_{tr}(U|\psi\rangle, U|\phi\rangle) = \Delta_{tr}(|\psi\rangle, |\phi\rangle)$.*

Then we consider the trace distance after applying a POVM measurement. Actually, the trace distance between two states after the POVM measurement is not larger than the original one. This is given in the following lemma.

Lemma 23 ([NC10, Theorem 9.1]). *Let $|\psi\rangle, |\varphi\rangle$ be two quantum states on Hilbert space H, and $\{Q_i\}_{i\in M}$ is a POVM measurement operator system. Then for any $i \in M$, we have:*

$$\Delta_{tr}(|\psi\rangle, |\varphi\rangle) = \max_{i\in M} \Delta_{tr}(Q_i|\psi\rangle, Q_i|\varphi\rangle).$$

Now we give the analogue of Lemma 15 under trace distance.

Lemma 24. *Let κ, r be positive numbers and n be a positive integer. Let $|\psi\rangle = \sum_{\mathbf{x}\in\mathbb{Z}} \sqrt{D_{\mathbb{Z}^d,r}(\mathbf{x})}|\mathbf{x}\rangle$ and $|\varphi\rangle = \sum_{\mathbf{x}\in(\mathbb{Z}\cap[-\sqrt{\kappa}r,\sqrt{\kappa}r])^n} \sqrt{D_{\mathbb{Z}^n,r,\sqrt{\kappa}r}(\mathbf{x})}|\mathbf{x}\rangle$. Then the trace distance of these two quantum states satisfies: $\Delta_{tr}(|\psi\rangle, |\varphi\rangle) \leqslant n \cdot 2^{-\Omega(\kappa)}$.*

Proof.

$$\begin{aligned}\Delta_{tr}(|\psi\rangle, |\varphi\rangle) &= \frac{1}{2} Tr\left(\left|\sum_{\mathbf{x}\in\mathbb{Z}^n} (D_{\mathbb{Z}^n,r,\sqrt{\kappa}r}(\mathbf{x}) - D_{\mathbb{Z}^n,r}(\mathbf{x}))|\mathbf{x}\rangle\langle\mathbf{x}|\right|\right) \\ =&\frac{1}{2}\sum_{\mathbf{x}\in\mathbb{Z}^n} \left|D_{\mathbb{Z}^n,r,\sqrt{\kappa}r}(\mathbf{x}) - D_{\mathbb{Z}^n,r}(\mathbf{x})\right| = \Delta(D_{\mathbb{Z}^n,r}, D_{\mathbb{Z}^n,r,\sqrt{\kappa}r}).\end{aligned}$$

The result follows directly according to Lemma 15. □

3.8 Extrapolated Dihedral Cosets Problems

In this subsection, we define the search variant of the *Integer Polynomial Module* EDCP (denoted as IP-M-EDCP), which generalizes the standard EDCP problem.

Definition 22 (Search IP-M-EDCP$^{m,n}_{q,\chi,\mathcal{D},f}$). *Let m, n be two positive integers, f a degree-d polynomial, $q > 2$ a positive integer, χ a distribution over $(\mathbb{Z}_{f(q)})^n$,*

and φ a function from $\mathbb{Z}^d$ to $\mathbb{C}$ with support $supp(\varphi)$. Let $\mathbf{s} \hookleftarrow \chi$ be a secret vector. Given m quantum samples of the following form:

$$\left\{\sum_{\mathbf{c}_i \in supp(\varphi)} \varphi(\mathbf{c}_i)|\mathbf{c}_i\rangle|\mathbf{x}_i + \langle \mathbf{z}, \mathbf{c}_i\rangle \cdot \mathbf{s} \bmod f(q)\rangle\right\}_{i\in[m]},$$

where $\mathbf{z} = (1, q, \ldots, q^{d-1})$, and in each sample, the vectors $\mathbf{x}_i$'s are drawn independently and uniformly from $(\mathbb{Z}_{f(q)})^n$. The goal is to recover the secret $\mathbf{s} \in (\mathbb{Z}_{f(q)})^n$.

For a fixed secret $\mathbf{s}$, we refer to the m quantum samples as an instance of $\mathsf{IP\text{-}M\text{-}EDCP}^{m,n}_{q,\mathbf{s},\varphi,f}$. Furthermore, when $\varphi(\mathbf{c}) = \sqrt{D_{\mathbb{Z}^n,r}(\mathbf{c})}$ for some standard deviation parameter r, we denote the problem as Search $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{m,n}_{q,\chi,r,f}$.

When $f = x$, this problem is exactly the EDCP problem defined in [BKSW18].

In Supplementary Material B.5, we recall the equivalence between EDCP and LWE problems in [BKSW18].

4 Reduction from IP-M-EDCP to P-MLWE

Due to the equivalence between the MLWE and P-MLWE problems for a broad class of underlying polynomials (see Supplementary Material B.3), we restrict our attention to reductions between P-MLWE and IP-M-EDCP in this work. Moreover, if we aim to complete the reduction chain, then the limitations of our technique naturally restrict the choice of the underlying polynomial to a class for which the MLWE–P-MLWE equivalence already holds.

We begin with a reduction from IP-M-EDCP to MLWE. In this section, we show that given a G-stEDCP instance, one can efficiently construct a corresponding instance of P-MLWE. Our construction relies on an intermediate problem, referred to as the q-adic Integer Polynomial MLWE problem (q-adic IP-MLWE). We formally define its associated sample distribution and search variant below.

Definition 23 (q-adic IP-MLWE distribution). *Let $f(x)$ be a monic and irreducible polynomial over the ring $\mathbb{Z}[x]$ with degree d, and let m, n be positive integers and r a positive real number. We define the q-adic IP-MLWE distribution $\mathcal{F}^{m,n}_{q,\mathbf{s},\chi,f}$: for a secret $\mathbf{s} \in \mathbb{Z}^n_{f(q)}$, select $\mathbf{A} \hookleftarrow U(\mathbb{Z}^{m\times n}_{f(q)})$, and for i-th row $\mathbf{A}_i$ of the matrix $\mathbf{A}$, select $\mathbf{e}_i \hookleftarrow \chi$, where χ is a distribution over $\mathbb{Z}^d$, compute $\mathbf{b}_i = \langle \mathbf{A}_i, \mathbf{s}\rangle \mathbf{z} + \mathbf{e}_i \bmod f(q)$, where $\mathbf{z} = (1, q, q^2 \ldots, q^{d-1})^\top$. Output $(\mathbf{A}, \{\mathbf{b}_i\}_{i\in[m]})$. When $\chi = D_{\mathbb{Z}^d,r,B}$, this distribution can be denoted as $\mathcal{F}^{m,n}_{q,\mathbf{s},(r,B),f}$.*

Then we define the search problem corresponding to the distribution above.

Definition 24 (Search q-adic IP-MLWE problem). *Let $f(x)$ be a monic and irreducible polynomial over ring $\mathbb{Z}[x]$ of degree d. Let m, n, q be positive integers and r a positive number. Let ψ be a distribution over $\mathbb{Z}^n_{f(q)}$. The search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\psi,\chi,f}$ problem is defined as: for a secret $\mathbf{s} \hookleftarrow \psi$, select $(\mathbf{A}, \{\mathbf{b}_i\}_{i\in[m]}) \hookleftarrow \mathcal{F}^{m,n}_{q,\mathbf{s},\chi,f}$, find the secret $\mathbf{s}$.*

The reduction proceeds in three steps, detailed in the following three subsections and summarized in the fourth.

4.1 Reduction from G-IP-M-EDCP to *q-adic* IP-MLWE

In this subsection, we present a polynomial-time algorithm that transforms a G-IP-M-EDCP instance into a *q-adic* IP-MLWE instance.

Lemma 25. *Let κ be the security parameter. Let $q = \mathsf{poly}(\kappa)$ be a positive integer, and let m, n be positive integers. Let f be a monic and irreducible polynomial of degree $d = \mathsf{poly}(\kappa)$ with coefficients in the range $\left(-\frac{q}{2}, \frac{q}{2}\right)$. Let $r_\alpha = \mathsf{poly}(\kappa)$. Let ψ be the distribution of secret $\mathbf{s}$ over $\mathbb{Z}_{f(q)}^n$. There is a reduction from Search $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}_{q,\psi,r_\alpha,f}^{m,n}$ to Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\psi,f(q)/(2r_\alpha),f}^{m,n}$. Furthermore, if a polynomial-time algorithm $\mathcal{A}$ solves the Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\psi,f(q)/(2r_\alpha),f}^{m,n}$ problem with advantage δ_α, then there exists an algorithm that solves the Search $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}_{q,\psi,r_\alpha,f}^{m,n}$ problem with advantage $\delta_\alpha - 2^{-\omega(\log \kappa)}$ in polynomial time.*

Proof. We are given m quantum states of the form $|\phi_1\rangle = \sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s} \bmod f(q)\rangle \in H_1 \otimes H_2$, where $\mathbf{c} \in \mathbb{Z}^d$, $\mathbf{x}, \mathbf{s} \in \mathbb{Z}_{f(q)}^n$ and $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$, and the first register is on the space H_1, the second register is on the space H_2. When $\mathbf{s}$ is selected from the distribution ψ, this represents an instance of the $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}_{q,\psi,r_\alpha,f}^{m,n}$ problem. In this proof, we will demonstrate how to derive a *q-adic* IP-MLWE instance from the quantum state described above. We denote $|\phi_1'\rangle = \sum_{\mathbf{c}\in\mathbb{Z}_{f(q)}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s} \bmod f(q)\rangle$. Throughout the reduction, the secret $\mathbf{s}$ remains unchanged, so its distribution is preserved. The reduction is completed by repeating the following process m times.

First, we apply the quantum Fourier transform[5] over $\mathbb{Z}_{f(q)}^n$ to the second register, which we denote as $I_{H_1} \otimes U_{\mathsf{QFT},H_2}$, where I_{H_1} is the identity operator on H_1 and U_{QFT,H_2} is the QFT operator on H_2. This is a polynomial-time algorithm, as established by Lemma 20 in Section 3.7, yielding:

$$|\phi_2\rangle = I_{H_1} \otimes U_{QFT,H_2} |\phi_1\rangle = \sum_{\mathbf{a}\in\mathbb{Z}_{f(q)}^n} \sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c}) \omega_{f(q)}^{\langle \mathbf{a}, \mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s}\rangle} |\mathbf{c}\rangle|\mathbf{a}\rangle.$$

Next, we measure the second register, and let $\widetilde{\mathbf{a}} \in \mathbb{Z}_{f(q)}^n$ denote the observed value. We denote this measurement operator as $I_{H_1} \otimes |\widetilde{\mathbf{a}}\rangle\langle\widetilde{\mathbf{a}}|$, which is an element of the POVM measurement system $\{I_{H_1} \otimes |\mathbf{a}\rangle\langle\mathbf{a}|\}_{\mathbf{a}\in\mathbb{Z}_{f(q)}^n}$. As a result, the quantum state becomes: $|\phi_3\rangle = (I_{H_1} \otimes |\widetilde{\mathbf{a}}\rangle\langle\widetilde{\mathbf{a}}|)\,|\phi_2\rangle = \sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c}) \omega_{f(q)}^{\langle \widetilde{\mathbf{a}}, \mathbf{s}\rangle\langle \mathbf{c}, \mathbf{z}\rangle} |\mathbf{c}\rangle$. Let $|\phi_3'\rangle = \sum_{\mathbf{c}\in\mathbb{Z}_{f(q)}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c}) \omega_{f(q)}^{\langle \widetilde{\mathbf{a}}, \mathbf{s}\rangle\langle \mathbf{c}, \mathbf{z}\rangle} |\mathbf{c}\rangle$. Then the trace distance[6] satisfies:

$$\Delta_{tr}(|\phi_3\rangle, |\phi_3'\rangle) \leqslant \Delta_{tr}(|\phi_1\rangle, |\phi_1'\rangle) = \Delta_{tr}\Big(\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c})\,|\mathbf{c}\rangle, \sum_{\mathbf{c}\in\mathbb{Z}_{f(q)}^d} \rho_{\sqrt{2}r_\alpha}(\mathbf{c})\,|\mathbf{c}\rangle\Big) \tag{11}$$

The first inequality follows from Lemma 22 and Lemma 23, while the second equality is a direct consequence of Lemma 22. Moreover, by Lemma 24, the third trace distance in formula (11) is bounded above by $2^{-\omega(\log \kappa)}$. All these lemmas are provided in Section 3.7.

[5] Quantum Fourier Transform is formally defined in Section 3.7.
[6] Trace distance is formally defined in Section 3.7.

Applying quantum Fourier transform U_{QFT,H_1} to the first register of $|\phi_3'\rangle$ yields: $|\phi_4'\rangle = U_{\mathsf{QFT},H_1}|\phi_3'\rangle = \sum_{\mathbf{b}\in\mathbb{Z}_{f(q)}^d}\sum_{\mathbf{c}\in\mathbb{Z}_{f(q)}^d}\rho_{\sqrt{2}r_\alpha}(\mathbf{c})\omega_{f(q)}^{\langle\mathbf{c},\langle\tilde{\mathbf{a}},\mathbf{s}\rangle\cdot\mathbf{z}+\mathbf{b}\rangle}|\mathbf{b}\rangle$.

We denote $|\phi_4\rangle = \sum_{\mathbf{b}\in\mathbb{Z}_{f(q)}^d}\sum_{\mathbf{c}\in\mathbb{Z}^d}\rho_{\sqrt{2}r_\alpha}(\mathbf{c})\omega_{f(q)}^{\langle\mathbf{c},\langle\tilde{\mathbf{a}},\mathbf{s}\rangle\cdot\mathbf{z}+\mathbf{b}\rangle}|\mathbf{b}\rangle$. By Lemma 45 in Supplementary Material C.1, trace distance admits the following upper bound:

$$\Delta_{tr}(|\phi_4\rangle,|\phi_4'\rangle) \leqslant d^3\cdot 2^{-\Omega(f(q)^2/r_\alpha^2)}/(f(q)^d r_\alpha^d) < 2^{-\omega(\log(\kappa))}.$$

By the Poisson summation formula (refer to Lemma 5 in Section 3.4) and a change of variable from $\mathbf{c}$ to $\mathbf{e} = f(q)\mathbf{c} + \langle\tilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z} + \mathbf{b}$ in $|\phi_4\rangle$, it can be rewritten as:

$$\sum_{\mathbf{b}\in\mathbb{Z}_{f(q)}^d}\sum_{\mathbf{c}\in\mathbb{Z}^d}\rho_{\frac{1}{\sqrt{2}r_\alpha}}(\mathbf{c}+\frac{\langle\tilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{b}}{f(q)})|\mathbf{b}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}^d}\rho_{\frac{f(q)}{\sqrt{2}r_\alpha}}(\mathbf{e})|\langle\tilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\mathbf{e} \bmod f(q)\rangle.$$

Finally, we measure the state and obtain a sample of the form $(\tilde{\mathbf{a}},\langle\tilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z}+\tilde{\mathbf{e}} \bmod f(q))$, where $\tilde{\mathbf{e}}$ is drawn from the distribution $D_{\mathbb{Z}^d,\frac{f(q)}{2r_\alpha}}$. This precisely constitutes a valid sample for the q-adic IP-MLWE problem, thereby completing the proof of the lemma. The loss of the advantage is at most the sum of the aforementioned trace distances, which is $2^{-\omega(\log(\kappa))}$. □

4.2 Reduction from *q-adic* IP-MLWE with discrete Gaussian errors to *q-adic* IP-MLWE with errors from $D+U$

Our next objective is to extract P-MLWE samples. To this end, we first reduce the Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\chi,r_\beta,f}$ problem to the Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\chi,D+U,f}$ problem, where the noise distribution is $D+U = q^{d-1}D_{\mathbb{Z}^d,r_\beta/q^{d-1}} + U(\mathbb{Z}_{q^{d-1}}^d)$, for some sufficiently large parameter r_β. The following lemma relies on the fact that the Rényi divergence between $D+U$ and $D_{\mathbb{Z}^d,r_\beta}$ admits a polynomial upper bound.

Lemma 26. *Let κ be the security parameter, q,m,n be positive integers, such that $q=\mathsf{poly}(\kappa)$, $m\leqslant\mathsf{poly}(\kappa)$, f a monic and irreducible polynomial of degree $d=\mathsf{poly}(\kappa)$ with coefficients in the range of $(-\frac{q}{2},\frac{q}{2})$, and r_β a positive number such that $\frac{r_\beta}{q^{d-1}}\geqslant\omega(dm)\geqslant\sqrt{d}\geqslant\eta_\varepsilon(\mathbb{Z}^d)$, where $\varepsilon=2^{-\omega(\log(\kappa))}$, there exists a polynomial-time algorithm that reduces Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\chi,r_\beta,f}^{m,n}$ problem to Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\chi,D+U,f}^{m,n}$ problem, where $D+U=q^{d-1}D_{\mathbb{Z}^d,r_\beta/q^{d-1}}+U(\mathbb{Z}_{q^{d-1}}^d)$. Furthermore, if there exists a polynomial-time algorithm that can solve Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\chi,D+U,f}^{m,n}$ problem with advantage δ_β, then there exists a polynomial-time algorithm that solves Search q-adic $\mathsf{IP\text{-}MLWE}_{q,\chi,r_\beta,f}^{m,n}$ with the advantage at least δ_β' satisfying $\delta_\beta'\geqslant\delta_\beta^4/\left((1+3\varepsilon)^{6m}\cdot\exp\left((19dmq^{d-1})/(2r_\beta)\right)\right)\geqslant\delta_\beta^4/\mathsf{poly}(\kappa)$. Particularly, we consider the case $n=\mathcal{O}(1)$. Let $d=\mathcal{O}(\kappa)$, $m=\mathcal{O}(\log(\kappa))$, $q=\mathsf{poly}(d)$, $r_\beta\geqslant\mathcal{O}(q^{d-1}d\log(\kappa)^{3/2})$. It is easy to verify that the advantage satisfies $\delta_\beta'\geqslant\delta_\beta^4/\mathsf{poly}(\kappa)$.*

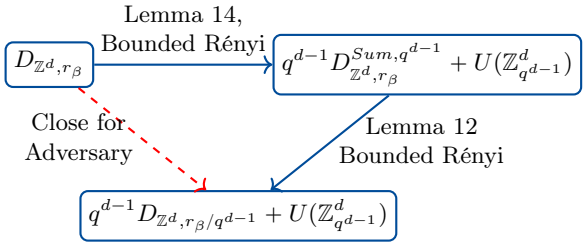

Fig. 5. Main idea of the proof of Lemma 26.

Due to space constraints, we defer the proof to Supplementary Material C.3. We roughly sketch the proof below.

The only difference between the q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,r_\beta,f}$ problem and the q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,D+U,f}$ problem lies in the distribution of the error terms. Consequently, our analysis focuses on the difference between the distributions $D_{\mathbb{Z}^d,r_\beta}$ and $q^{d-1}D_{\mathbb{Z}^d,r_\beta/q^{d-1}} + U(\mathbb{Z}^d_{q^{d-1}})$. We show the main idea of this paper in Figure 26.

We introduce the distribution $q^{d-1}D^{\mathrm{Sum},q^{d-1}}_{\mathbb{Z}^d,r_\beta} + U(\mathbb{Z}^d_{q^{d-1}})$ as an intermediate distribution, where $D^{\mathrm{Sum},q^{d-1}}_{\mathbb{Z}^d,r_\beta}$ denotes the distribution of $\lfloor \mathbf{x}/q^{d-1} \rceil$ for $\mathbf{x} \hookleftarrow D_{\mathbb{Z}^d,r_\beta}$. By Lemma 14 in Section 3.4, we have

$$R\left(q^{d-1}D^{\mathrm{Sum},q^{d-1}}_{\mathbb{Z}^d,r_\beta} + U(\mathbb{Z}^d_{q^{d-1}}) \| D_{\mathbb{Z}^d,r_\beta}\right) \leqslant (1+3\varepsilon)^2 \exp(\mathcal{O}(dq^{d-1}/r_\beta)),$$

where ε is the same as that in the statement of the lemma.

It follows that the Rényi divergence between a single sample of q-adic $\mathsf{IP\text{-}MLWE}$ with error drawn from $D_{\mathbb{Z}^d,r_\beta}$ and one with error drawn from $q^{d-1}D^{\mathrm{Sum},q^{d-1}}_{\mathbb{Z}^d,r_\beta} + U(\mathbb{Z}^d_{q^{d-1}})$ is bounded by the same quantity. By multiplicativity, the Rényi divergence between m samples from the two distributions is bounded by $(1+3\varepsilon)^{2m}\exp(\mathcal{O}(dmq^{d-1}/r_\beta))$.

Therefore, any adversary that solves the Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,D^{\mathrm{Sum}}+U,f}$ problem with advantage δ_2 also solves the Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,r_\beta,f}$ problem with advantage $\delta_1 \geqslant \delta_2^2/\left((1+3\varepsilon)^{2m}\exp(\mathcal{O}(dmq^{d-1}/r_\beta))\right)$.

Moreover, by Lemma 12 in Section 3.4, we have

$$R(q^{d-1}D_{\mathbb{Z}^d,r_\beta/q^{d-1}} + U(\mathbb{Z}^d_{q^{d-1}}) \| q^{d-1}D^{\mathrm{Sum},q^{d-1}}_{\mathbb{Z}^d,r_\beta} + U(\mathbb{Z}^d_{q^{d-1}})) \leqslant (1+3\varepsilon)^2\exp(\mathcal{O}(dq^{d-1}/r_\beta)).$$

By the same argument as above, any adversary that solves the Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,D+U,f}$ problem with advantage δ_3 also solves the Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,D^{\mathrm{Sum}}+U,f}$ problem with advantage

$$\delta_2 \geqslant \delta_3^2/\left((1+3\varepsilon)^{2m}\exp\left(\mathcal{O}\left(\left(dmq^{d-1}\right)/r_\beta\right)\right)\right).$$

Therefore, it follows that $\delta_1 \geqslant \delta_3^4/(1+3\varepsilon)^{6m}\exp\left(\mathcal{O}(dmq^{d-1}/r_\beta)\right)$. Setting $m \leqslant \mathsf{poly}(\kappa)$, we have $(1+3\varepsilon)^{6m} = \mathcal{O}(1)$. Moreover, if $r_\beta/q^{d-1} \geqslant \omega(dm)$, then

$\exp(\mathcal{O}(dmq^{d-1}/r_\beta)) \leqslant \exp(1/\omega(1))$. Hence, it follows that $\delta_1 \geqslant \delta_3^4/\mathsf{poly}(\kappa)$, which implies the result.

4.3 Reduction from *q-adic* IP-MLWE to P-MLWE

Now, we are ready to extract the classical P-MLWE samples with error distribution $D_{\mathbb{Z}^d, r_\beta/q^{d-1}}$ from the *q-adic* IP-MLWE samples with error distribution $q^{d-1} \cdot D_{\mathbb{Z}^d, r_\beta/q^{d-1}} + U(\mathbb{Z}^d_{q^{d-1}})$.

Lemma 27. *Let κ be the security parameter. Let $q = \mathsf{poly}(\kappa)$, and $f = x^d + 1$ with degree $d = \mathsf{poly}(\kappa)$ a power of 2. Let m, n be two positive integers such that $m = \mathcal{O}(\log(\kappa))$ and $n = \mathcal{O}(1)$. Let r_γ, r' be two numbers satisfying $r_\gamma \geqslant \omega\left((r'\sqrt{\kappa}n^2 + nd)\sqrt{dm}\right)$, $\frac{q}{r_\gamma\sqrt{\kappa}} = \mathsf{poly}(\kappa)$, $\frac{q}{r'\sqrt{\kappa}} = \mathsf{poly}(\kappa)$. There exists a reduction from Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ to Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',r_\gamma,f}$, where $D + U = q^{d-1}D_{\mathbb{Z}^d,r_\gamma} + U(\mathbb{Z}^d_{q^{d-1}})$, and $D_{r'}(q)$ denotes the distribution of the secret $\mathbf{s}$ obtained by first sampling $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r'})^n$ and then setting $\mathbf{s} = \mathbf{s}(q) \bmod f(q)$. Furthermore, if there exists a polynomial-time adversary $\mathcal{A}$ that solves Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',r_\gamma,f}$ with advantage δ_γ, there exists a polynomial-time adversary $\mathcal{A}'$ for Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ with advantage $\delta'_\gamma \geqslant \delta_\gamma^2/\left((2e^2)^m \exp\left((2\pi dm\tilde{c}^2_{max})/r^2_\gamma\right)\right) - 2^{-\omega(\log(\kappa))} \geqslant \delta_\gamma^2/\mathsf{poly}(\kappa)$, where $c_{max} = \left(3r'\sqrt{\kappa}n^2\right) + 18n + 11/2$.*

In particular, we consider the case where $n = \mathcal{O}(1)$. Let $m = \mathcal{O}(\log\kappa)$, $q = \mathsf{poly}(d)$, and $r' = \mathcal{O}(\kappa)$. In this setting, $c_{\max} = \mathcal{O}(\kappa^{5/2})$. Furthermore, let $r_\gamma \geqslant \mathcal{O}(\kappa^3 \log\kappa)$. Then it is easy to verify that the advantage satisfies $\delta'_\gamma \geqslant \delta^2_\gamma/\mathsf{poly}(\kappa)$.

Due to the restriction of the space, we provide only a proof sketch. The full proof is given in Lemma 47 and Corollary 4 in Supplementary Material C.4.

For simplicity of exposition, we focus on the case $n = 1$ to illustrate how to extract P-MLWE samples from IP-MLWE samples. Suppose we are given an IP-RLWE instance of the form $(a, as\mathbf{z} + \mathbf{e}' \bmod f(q))$, where $a, s \in \mathbb{Z}_{f(q)}$, $\Phi_q^{(f)}(s)$ has small coefficients and $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$. Using the properties of the mapping $\Phi_q^{(f)}$ introduced earlier, for all $i \in [d]$, we have $\Phi_q^{(f)}(asq^i + e'_i) = \Phi_q^{(f)}(a) \cdot \Phi_q^{(f)}(s) \cdot x^i + \Phi_q^{(f)}(e'_i) \bmod f(x) + \tilde{c}_i(x)$, where the carry term $\tilde{c}_i(x)$ has small coefficients.

We denote the coefficient vector of $\Phi_q^{(f)}(a)$ as $\overline{\mathbf{a}} = (\overline{a}_0, \ldots, \overline{a}_{d-1})^\top$, the one of $\Phi_q^{(f)}(s)$ as $\overline{\mathbf{s}} = (\overline{s}_0, \ldots, \overline{s}_{d-1})^\top$, the one of $\Phi_q^{(f)}(e'_i)$ as $\overline{\mathbf{e}}'_i = (\overline{e}'_{i,0}, \ldots, \overline{e}'_{i,d-1})^\top$ and the one of $\tilde{c}_i(x)$ as $\overline{\mathbf{c}}_i = (\overline{c}_{i,0}, \ldots, \overline{c}_{i,d-1})^\top$. Suppose $f(x) = x^d - C$, where C is a constant, the coefficient vector of $\Phi_q^{(f)}(a \cdot s \cdot q^i + e'_i)$ can be written as

$$\begin{bmatrix} C\overline{a}_{d-i} & C\overline{a}_{d-i-1} & \ldots & C^2\overline{a}_{d-i+1} \\ C\overline{a}_{d-i+1} & C\overline{a}_{d-i} & \ldots & C^2\overline{a}_{d-i+2} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{a}_{d-i-1} & \overline{a}_{d-i-2} & \ldots & C\overline{a}_{d-i} \end{bmatrix} \cdot \begin{bmatrix} \overline{s}_0 \\ \overline{s}_1 \\ \vdots \\ \overline{s}_{d-1} \end{bmatrix} + \begin{bmatrix} \overline{e}'_{i,0} \\ \overline{e}'_{i,1} \\ \vdots \\ \overline{e}'_{i,d-1} \end{bmatrix} + \begin{bmatrix} \overline{c}_{i,0} \\ \overline{c}_{i,1} \\ \vdots \\ \overline{c}_{i,d-1} \end{bmatrix}. \quad (12)$$

For each i, we extract the coefficient of x^{d-1} from $\Phi_q^{(f)}(a \cdot s \cdot q^i + e'_i)$, which we use red and blue (for denoting the fixed $\bar{\mathbf{s}}$) to highlight in (12) and concatenate these coefficients into a single vector, resulting in a d-dimensional vector of the form:

$$\underbrace{\begin{bmatrix} \bar{a}_0 & C\bar{a}_{d-1} & \dots & C\bar{a}_1 \\ \bar{a}_1 & \bar{a}_0 & \dots & C\bar{a}_2 \\ \vdots & \vdots & \ddots & \vdots \\ \bar{a}_{d-1} & \bar{a}_{d-2} & \dots & \bar{a}_0 \end{bmatrix}}_{\mathbf{A}'} \cdot \begin{bmatrix} \bar{s}_0 \\ \bar{s}_1 \\ \vdots \\ \bar{s}_{d-1} \end{bmatrix} + \begin{bmatrix} \bar{e}'_{d-1,d-1} \\ \bar{e}'_{d-2,d-1} \\ \vdots \\ \bar{e}'_{0,d-1} \end{bmatrix} + \begin{bmatrix} \bar{c}_{d-1,d-1} \\ \bar{c}_{d-2,d-1} \\ \vdots \\ \bar{c}_{0,d-1} \end{bmatrix}.$$

In this case ($f(x) = x^d - C$), the first matrix $\mathbf{A}'$ happens to be exactly the multiplication matrix of $\Phi_q^{(f)}(a)$. To the best of our knowledge, we only know that when $f(x) = x^d - C$ for some constant C, the matrix $\mathbf{A}'$ remains a multiplication matrix for some element in $\mathbb{Z}_q[x]/f$ after concatenation.

Since the sample-amplification technique employed in the next section requires $f(x)$ to be cyclotomic, we therefore restrict our attention to $f(x) = x^d + 1$ with d a power of 2.

When considering the case $n > 1$, starting from the integer sample $(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle \mathbf{z} + \mathbf{e} \bmod f(q))$, we can extract a polynomial sample of the following form:

$$(\mathbf{a}'(x) = \Phi_q^{(f)}(\mathbf{a}),\ b'(x) = \langle \Phi_q^{(f)}(\mathbf{a}), \Phi_q^{(f)}(\mathbf{s}) \rangle + \bar{e}'(x) + \bar{c}(x)). \tag{13}$$

For convenience, we denote $\mathbf{s}(x) = \Phi_q^{(f)}(\mathbf{s})$, whose distribution is statistically close to $(D_{\mathbb{Z}[x]/f,r'})^n$. Moreover, we can show that $\bar{e}'(x)$ follows the distribution statistically close to $D_{\mathbb{Z}[x]/f,r_\gamma}$, while the distribution of $\bar{c}(x)$ depends on $\Phi_q^{(f)}(\mathbf{a})$, $\mathbf{s}(x)$, and $b'(x)$. To keep the exposition in the main text concise, we treat the distributions of $\mathbf{s}(x)$ and $\bar{e}'(x)$ as discrete Gaussian distributions. In the detailed proof in Supplementary Material C.4, we instead use discrete Gaussian distributions as intermediate distributions in order to ensure full rigor.

If the distribution of m samples of the form (13) has bounded Rényi divergence from that of $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',r_\gamma,f}$, then any efficient algorithm for $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',r_\gamma,f}$ can recover the secret $\mathbf{s}(x)$ from these m samples with non-negligible advantage. Hence, it suffices to bound this Rényi divergence, denoted by R_1.

For a fixed $\mathbf{s}(x)$, we denote the distribution of m samples of the form (13) by $\mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},r_\gamma,f}$. By the multiplicativity property of Rényi divergence shown in Lemma 4 in Section 3.3, we have

$$\begin{aligned} R_1 &\leqslant R_\infty((D_{\mathbb{Z}[x]/f,r'})^n \| (D_{\mathbb{Z}[x]/f,r'})^n) \cdot \max_{\mathbf{s}(x)\in\mathbb{Z}[x]/f} R(\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s}(x),r_\gamma,f} \| \mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},r_\gamma,f}) \\ &\leqslant \max_{\mathbf{s}(x)\in\mathbb{Z}[x]/f} R(\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s}(x),r_\gamma,f} \| \mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},r_\gamma,f}) \\ &= \left(\max_{\mathbf{s}(x)\in\mathbb{Z}[x]/f} R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s}(x),r_\gamma,f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f})\right)^m. \end{aligned}$$

Hence we focus on finding the upper bound of $R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s}(x),r_\gamma,f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f})$. By definition, this Rényi divergence can be written as

$$R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},r_\gamma,f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f}) = \sum_{\substack{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n, \\ Q(x)\in\mathbb{Z}_q[x]/f}} R_{term}(\mathbf{P}(x), Q(x)), \tag{14}$$

where

$$\begin{aligned}&R_{term}(\mathbf{P}(x),Q(x))\\ =&\frac{\Pr_{\substack{\mathbf{a}(x)\hookleftarrow U((\mathbb{Z}_q[x]/f)^n)\\ e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma}}}\left(\mathbf{a}(x)=\mathbf{P}(x),\langle\mathbf{a}(x),\mathbf{s}(x)\rangle+e(x)\bmod f(x)=Q(x)\right)^2}{\Pr_{(\mathbf{a}'(x),b'(x))\hookleftarrow\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f}}\left(\mathbf{a}'(x)=\mathbf{P}(x),b'(x)=Q(x)\right)}.\end{aligned}\tag{15}$$

Considering the denominator of formula (15), we can prove that

$$\begin{aligned}&\Pr_{(\mathbf{a}'(x),b'(x))\hookleftarrow\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f}}\left(\mathbf{a}'(x)=\mathbf{P}(x),b'(x)=Q(x)\right)\\ \geqslant&\Pr_{\overline{e}'(x)\hookleftarrow D_{\mathbb{Z}[x]/f(x),r_\gamma}}\left(\overline{e}'(x)=Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle-\overline{c}(x)\right)/(f(q))^n.\end{aligned}$$

On the other hand,considering the numerator of the formula (15), we have

$$\begin{aligned}&\Pr_{\substack{\mathbf{a}(x)\hookleftarrow U((\mathbb{Z}_q[x]/f)^n)\\ e(x)\hookleftarrow D_{\mathbb{Z}[x]/f(x),r_\gamma}}}\left(\mathbf{a}(x)=\mathbf{P}(x),\langle\mathbf{a}(x),\mathbf{s}(x)\rangle+e(x)\bmod f(x)=Q(x)\right)\\ =&\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f(x),r_\gamma}}\left(e(x)=Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle\bmod f(x)\right)/q^{nd}.\end{aligned}$$

Therefore, $R_{\text{term}}(\mathbf{P}(x),Q(x))$ can be upper bounded by

$$\frac{f(q)^n}{q^{2nd}}\frac{\Pr\limits_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f(x),r_\gamma}}\left(e(x)=Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle\bmod f(x)\right)^2}{\Pr_{\overline{e}'(x)\hookleftarrow D_{\mathbb{Z}[x]/f(x),r_\gamma}}\left(\overline{e}'(x)=Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle-\overline{c}(x)\right)}.\tag{16}$$

Let $\overline{e}^*(x)=Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle \bmod (q,f(x))$. Replacing $Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle \bmod (q,f(x))$ with $\overline{e}^*(x)$, the expression in (16) can be rewritten as

$$\begin{aligned}\frac{f(q)^n}{q^{2nd}}\frac{(D_{\mathbb{Z}[x]/f(x),r_\gamma}(\overline{e}^*(x)))^2}{D_{\mathbb{Z}[x]/f(x),r_\gamma}(\overline{e}^*(x)-\overline{c}(x))}=&\frac{f(q)^n}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\frac{\exp(-2\pi\|\overline{\mathbf{e}}^*\|^2/r_\gamma^2)}{\exp(-\pi\|\overline{\mathbf{e}}^*-\overline{\mathbf{c}}\|^2/r_\gamma^2)}\\ =&\frac{f(q)^n}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\frac{\exp(-\pi\|\overline{\mathbf{e}}^*+\overline{\mathbf{c}}\|^2/r_\gamma^2)}{\exp(-2\pi\|\overline{\mathbf{c}}\|^2/r_\gamma^2)}.\end{aligned}$$

Here, $\overline{\mathbf{e}}^*$ and $\overline{\mathbf{c}}$ denote the coefficient vectors of $\overline{e}^*(x)$ and $\overline{c}(x)$, respectively.

Since $Q(x)=\overline{e}^*(x)+\langle\mathbf{P}(x),\mathbf{s}(x)\rangle \bmod (q,f(x))$, we have $R_{term}(\mathbf{P}(x),Q(x))=R_{term}(\mathbf{P}(x),\overline{e}^*(x)+\langle\mathbf{P}(x),\mathbf{s}(x)\rangle \bmod (q,f(x)))$ can be considered as a function only depends on $\mathbf{P}(x)$ and $\overline{e}^*(x)$. Furthermore, for a fixed $\mathbf{P}(x)$, one $Q(x)$ corresponds to unique $\overline{e}^*(x)$. Hence the Rényi divergence can be refomulated as

$$\begin{aligned}&R(\mathsf{P}\text{-}\mathsf{MLWE}^{1,n}_{q,\mathbf{s}(x),r_\gamma,f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f})\\ =&\sum_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n}\Big(\sum_{Q(x)\in\mathbb{Z}_q[x]/f}R_{term}(\mathbf{P}(x),Q(x))\Big)\\ =&\sum_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n}\Big(\sum_{\overline{e}^*(x)\in\mathbb{Z}_q[x]/f}R_{term}\left(\mathbf{P}(x),\overline{e}^*(x)+\langle\mathbf{P}(x),\mathbf{s}(x)\rangle\bmod f(x)\right)\Big).\end{aligned}\tag{17}$$

Then we can bound this Rényi divergence from above as follows:

$$\begin{aligned}&R(\mathsf{P}\text{-}\mathsf{MLWE}^{1,n}_{q,\mathbf{s}(x),r_\gamma,f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f})\\ \leqslant&\sum\nolimits_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n}\Big(\sum\nolimits_{\overline{\mathbf{e}}^*\in\mathbb{Z}_q^d}\frac{f(q)^n}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\frac{\exp(-\pi\|\overline{\mathbf{e}}^*+\overline{\mathbf{c}}\|^2/r_\gamma^2)}{\exp(-2\pi\|\overline{\mathbf{c}}\|^2/r_\gamma^2)}\Big).\end{aligned}\tag{18}$$

By Lemma 46 in Supplementary Material C.2, we have $\|\overline{\mathbf{c}}\|_\infty \leqslant 3r\sqrt{\kappa}n^2 + 18n + 11/2$, denoted as c_{max}. Moreover, $\overline{\mathbf{c}}$ can be decomposed as the sum $\overline{\mathbf{c}}_{(I)} + \overline{\mathbf{c}}_{(II)}$, where $\overline{\mathbf{c}}_{(I)}$ satisfies $\|\overline{\mathbf{c}}_{(I)}\|_\infty \leqslant 6$, while $\overline{\mathbf{c}}_{(II)}$ only depends on $\mathbf{P}(x)$. Therefore, for a fixed $\mathbf{P}(x)$, we have

$$\sum_{\overline{\mathbf{e}}^* \in \mathbb{Z}_q^d} \frac{f(q)^n}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)} \frac{\exp(-\pi\|\overline{\mathbf{e}}^* + \overline{\mathbf{c}}\|^2/r_\gamma^2)}{\exp(-2\pi\|\overline{\mathbf{c}}\|^2/r_\gamma^2)} \leqslant \frac{(q^d+1)^n \cdot \exp\left(\frac{2\pi d}{r_\gamma^2} c_{max}^2\right)}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)} \sum_{\overline{\mathbf{e}}^* \in \mathbb{Z}^d} \rho_{r_\gamma}(\overline{\mathbf{e}}^* + \overline{\mathbf{c}}). \tag{19}$$

Moreover, we can compute that

$$\textstyle\sum_{\overline{\mathbf{e}}^* \in \mathbb{Z}^d} \rho_{r_\gamma}(\overline{\mathbf{e}}^* + \overline{\mathbf{c}}) = \prod_{i\in[d]} \Big(\sum_{\overline{e}_i^* \in \mathbb{Z}} \rho_{r_\gamma}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i}) \Big),$$

where $\overline{e}_i^*$, $\overline{c}_{(I),i}$, and $\overline{c}_{(II),i}$ denote the i-th entries of $\overline{\mathbf{e}}^*$, $\overline{\mathbf{c}}_{(I)}$, and $\overline{\mathbf{c}}_{(II)}$, respectively. The summation of $\overline{e}_i^*$ over $\mathbb{Z}$ can be bounded as

$$\begin{aligned} &\sum_{\overline{e}_i^* \in \mathbb{Z}} \rho_{r_\gamma}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i}) \leqslant 2\|\overline{\mathbf{c}}_{(I)}\|_\infty + \rho_{r_\gamma}(\mathbb{Z} + \overline{c}_{(II),i}) \\ \leqslant &12 + \rho_{r_\gamma}(\mathbb{Z} + \overline{c}_{(II),i}) \approx 12 + \rho_{r_\gamma}(\mathbb{Z}), \end{aligned} \tag{20}$$

where the first inequality follows from monotonicity, and the second inequality follows from the upper bound on $\|\overline{\mathbf{c}}_{(I)}\|_\infty$. Therefore, the expression in (19) can be approximately bounded as

$$\frac{(q^d+1)\cdot\exp\left(\frac{2\pi d c_{\max}^2}{r_\gamma^2}\right)}{q^{2nd}} \cdot \left(\frac{12 + \rho_{r_\gamma}(\mathbb{Z})}{\rho_{r_\gamma}(\mathbb{Z})}\right)^d \approx \frac{(q^d+1)\cdot\exp\left(\frac{2\pi d c_{\max}^2}{r_\gamma^2}\right)}{q^{2nd}} \cdot (1 + 12/r_\gamma)^d, \tag{21}$$

where, when $r_\gamma \geqslant 12d$, we have $(1 + 12/r_\gamma)^d \leqslant e$. Hence,

$$\begin{aligned} &R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s}(x),r_\gamma,f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f}) \lesssim \sum_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f(x))^n} \frac{e\cdot(q^d+1)^n\cdot\exp\left(\frac{2\pi d c_{\max}^2}{r_\gamma^2}\right)}{q^{2nd}} \\ &= \left(q^{nd}\cdot e\cdot(q^d+1)^n\cdot\exp\big((2\pi d c_{\max}^2)/r_\gamma^2\big)\right) \Big/ q^{2nd} \leqslant e^2\cdot\exp\big((2\pi d c_{\max}^2)/r_\gamma^2\big), \end{aligned}$$

where the last inequality holds since $q^d > n$, which implies $(1 + 1/q^d)^n \leqslant e$. Compared with the upper bound in Lemma 47 in Supplementary Material C.4, the upper bound above differs by a constant factor C, which arises from the approximations used in (20) and (21). Accounting for this constant factor, the Rényi divergence R_1 can be upper bounded by $(Ce^2)^m \cdot \exp\big((2\pi m d c_{\max}^2)/r_\gamma^2\big)$. Setting $m = \mathcal{O}(\log\kappa)$ and assuming $r_\gamma \geqslant \omega(\sqrt{md}\cdot c_{\max})$, it follows that R_1 is polynomially bounded.

4.4 Main Theorem

By combining all lemmas in this section, we establish a reduction from the IP-M-EDCP problem to the P-MLWE problem.

Theorem 3. *Let κ be the security parameter. Let $q = \mathsf{poly}(\kappa)$, and $f = x^d + 1$ with $d = \mathsf{poly}(\kappa)$ a power of 2. Let m, n be two positive integers such that $m = \mathcal{O}(\log(\kappa))$ and $n = \mathcal{O}(1)$ and r, r' two numbers satisfying $\frac{q}{r'\sqrt{\kappa}} = \mathsf{poly}(\kappa)$, $q/r \geqslant \omega\big(\max\{(r'\sqrt{\kappa}n^2 + nd)\sqrt{dm}, dm\}\big)$. There is a polynomial-time quantum reduction from Search $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{m,n}_{q,D_{r'}(q),r,f}$ to Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',\frac{f(q)}{2rq^{d-1}},f}$, where $D_{r'}(q)$ denotes the distribution of the secret $\mathbf{s}$ obtained by first sampling $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r'})^n$ and then setting $\mathbf{s} = \mathbf{s}(q) \bmod f(q)$. If there is a polynomial-time adversary that can solve Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',\frac{q^d+1}{2rq^{d-1}},f}$ with advantage δ, then there is a polynomial-time adversary against Search $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{m,n}_{q,D_{r'}(q),r,f}$ with advantage:*

$$\delta' \geqslant \delta^8 / \left(64(2e^2)^{4m} \exp\left(\frac{32\pi dmr^2 q^{2(d-1)} c_{max}^2}{(q^d+1)^2} + \frac{19dmrq^{d-1}}{q^d+1}\right)\right) \geqslant \delta^8/\mathsf{poly}(\kappa),$$

where $c_{max} = 3r'\sqrt{\kappa}n^2 + 18n + 11/2$. Particularly, we consider the case $n = \mathcal{O}(1)$. Let $d = \mathcal{O}(\kappa)$, $m = \mathcal{O}(\log(\kappa))$, $r' = \mathcal{O}(\kappa)$, $r = \mathcal{O}(\kappa)$. Let $q \geqslant \mathcal{O}(\kappa^4 \log(\kappa))$. Then it is easy to verify that the advantage satisfies $\delta' \geqslant \delta^8/\mathsf{poly}(\kappa)$.

Proof. We prove this theorem by reducing the $\mathsf{G\text{-}stEDCP}$ (**Problem 1**) to $\mathsf{P\text{-}MLWE}$ (**Problem 4**) as shown below.

* **Problem 1.** Search $\mathsf{G\text{-}stEDCP}^{m,n}_{q,D_{r'}(q),r,f}$, where $D_{r'}(q)$ denotes the distribution that selects $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r'})^n$ and outputs $\mathbf{s}(q) \bmod f(q)$.
* **Problem 2.** Search *q-adic* $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D'_r(q),\frac{f(q)}{2r},f}$ problem.

Lemma 25 in Section 4.1 shows that if there is a polynomial-time adversary for solving Search *q-adic* $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),\frac{f(q)}{2r},f}$ problem with non-negligible advantage δ_2, there exists a polynomial-time adversary for Search $\mathsf{G\text{-}stEDCP}^{m,n}_{q,D_{r'}(q),r,f}$ with advantage $\delta = \delta_1 \geqslant \delta_2 - 2^{-\omega(\log(\kappa))}$.

* **Problem 3.** Search *q-adic* $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ problem, where $D + U = q^{d-1}D_{\mathbb{Z}^d,\frac{q^d+1}{2rq^{d-1}}} + U(\mathbb{Z}^d_{q^{d-1}})$.

Lemma 26 in Section 4.2 shows that, under the condition

$$\frac{q^d+1}{2rq^{d-1}} \geqslant \omega(dm) \geqslant \sqrt{d} \geqslant \eta_\varepsilon(\mathbb{Z}^d),$$

where $\varepsilon = 2^{-\omega(\log(\kappa))}$, if there exists a polynomial-time algorithm that solves the Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ problem with non-negligible advantage δ_3, then this algorithm can be used to solve the Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),\frac{q^d+1}{2r},f}$ problem with advantage

$$\delta_2 \geqslant \frac{\delta_3^4}{(1+3\varepsilon)^{6m}\exp\left(\frac{19dmrq^{d-1}}{q^d+1}\right)} \geqslant \frac{\delta_3^4}{2\cdot\exp\left(\frac{19dmrq^{d-1}}{q^d+1}\right)},$$

where the second inequality holds because $(1+3\varepsilon)^{6m} = (1+3\varepsilon)^{\frac{1}{3\varepsilon}\cdot 3\varepsilon\cdot 6m} \leqslant e^{3\varepsilon\cdot 6m} = e^{2^{-\omega(\log(\kappa))}} \leqslant 2$.

The above condition is guaranteed by the parameter requirement in the statement of the theorem, namely $q/r \geqslant \omega\big(\max\{(r'\sqrt{\kappa}n^2+nd)\sqrt{dm},\, dm\}\big)$.

* **Problem 4.** Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',\frac{q^d+1}{2rq^{d-1}},f}$ problem.

Lemma 27 in Section 4.3 shows that if there exists a polynomial-time adversary against Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',\frac{q^d+1}{2rq^{d-1}},f}$ with advantage δ_4, there exists a polynomial-time adversary against Search *q-adic* $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ with advantage:

$$\begin{aligned}\delta_3 &\geqslant \frac{\delta_4^2}{(2e^2)^m \exp\left((8\pi dmr^2q^{2(d-1)}c_{max}^2)/(q^d+1)^2\right)} - 2^{-\omega(\log(\kappa))}\\ &\geqslant \frac{\delta_4^2}{2(2e^2)^m \exp\left((8\pi dmr^2q^{2(d-1)}c_{max}^2)/(q^d+1)^2\right)},\end{aligned}$$

where $c_{max} = 3r'\sqrt{\kappa}n^2 + 18n + 11/2$.

To conclude, there exists a reduction from Search $\mathsf{G\text{-}stEDCP}^{m,n}_{q,D_{r'}(q),r,f}$ to the problem Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',\frac{q^d+1}{2rq^{d-1}},f}$. If there exists a polynomial-time adversary against Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',\frac{q^d+1}{2rq^{d-1}},f}$ with advantage δ, there exists polynomial-time adversary against Search $\mathsf{G\text{-}stEDCP}^{m,n}_{q,D_{r'}(q),r,f}$ with advantage:

$$\begin{aligned}\delta' &\geqslant \frac{\delta^8}{32(2e^2)^{4m}\cdot\exp\left(\frac{32\pi dmr^2q^{2(d-1)}c_{max}^2}{(q^d+1)^2} + \frac{19dmrq^{d-1}}{q^d+1}\right)} - 2^{-\omega(\log(\kappa))}\\ &\geqslant \frac{\delta^8}{64(2e^2)^{4m}\cdot\exp\left(\frac{32\pi dmr^2q^{2(d-1)}c_{max}^2}{(q^d+1)^2} + \frac{19dmrq^{d-1}}{q^d+1}\right)}\\ &= \frac{\delta^8}{64(2e^2)^{4m}\cdot\exp\left(\frac{32\pi dmr^2q^{2(d-1)}c_{max}^2}{(q^d+1)^2} + \frac{19dmrq^{d-1}}{q^d+1}\right)}\end{aligned}$$

According to our parameter selection, we have

$$q/r \geqslant \omega\left(\max\{r'\sqrt{\kappa}n^2+nd)\sqrt{dm}, dm\}\right)$$

and $m = \mathcal{O}(\log(\kappa))$, hence $\exp\big(\frac{32\pi dmr^2q^{2(d-1)}c_{max}^2}{(q^d+1)^2} + \frac{19dmrq^{d-1}}{q^d+1}\big) \leqslant \exp(1/\omega(1))$ and $(2e^2)^{4m} = \mathsf{poly}(\kappa)$. We have $\delta' \geqslant \delta^8/\mathsf{poly}(\kappa)$ and the result follows.

In particular, let $n = \mathcal{O}(1)$, $m = \mathcal{O}(\log\kappa)$, $r' = \mathcal{O}(\kappa)$, and $r = \mathcal{O}(\kappa)$. In this case, we obtain $c_{\max} = \mathcal{O}(\kappa^{5/2}) + \mathcal{O}(1) = \mathcal{O}(\kappa^{5/2})$ and $(2e^2)^{4m} = \mathsf{poly}(\kappa)$. Furthermore, by setting $q \geqslant \mathcal{O}(\kappa^4\log\kappa)$, we have:

$$q/r \;\geqslant\; \mathcal{O}(\kappa^3\log\kappa) \;\geqslant\; \omega\Big(\max\{\mathcal{O}(\kappa^3\sqrt{\log\kappa}), \mathcal{O}(\kappa\log\kappa)\}\Big) \;=\; \omega(\kappa^3\sqrt{\log\kappa}).$$

Hence,

$$\exp\left(\frac{32\pi dmr^2q^{2(d-1)}c_{\max}^2}{f(q)^2}+\frac{19dmrq^{d-1}}{f(q)}\right)$$
$$\leqslant \exp\left(\frac{\kappa^6\log\kappa}{\omega(\kappa^6\log\kappa)}+\frac{\kappa\log\kappa}{\omega(\kappa^3\sqrt{\log\kappa})}\right)=\exp\big(1/\omega(1)\big).$$

This implies that $\delta' \geqslant \delta^8/\mathsf{poly}(\kappa)$. □

The subsequent reduction from P-MLWE to MLWE generalizes canonically the reduction from PLWE to RLWE in [RSW18], which can be found in Supplementary Material B.3. For a defining polynomial f of the form x^d+1, the loss in error width incurred in the final reduction is bounded by $\sqrt{d}$.

5 Reduction from P-MLWE to stEDCP

As shown in Supplementary Material B.3, under an appropriate choice of the underlying number field, the MLWE problem is as hard as the P-MLWE problem. Hence, it suffices to establish a reduction from P-MLWE to IP-M-EDCP.

To this end, we adapt the technique of [BKSW18] to generate IP-M-EDCP samples. Following [DSSS21], we map P-MLWE samples to IP-MLWE-like samples by evaluating each polynomial at $x = q$, which is applied independently to each sample and hence preserves the sample count. These IP-MLWE-like samples then form the basis for constructing IP-M-EDCP samples, as described in Section 5.2.

Theorem 3 in Section 4 shows that, due to inherent limitations of the underlying technique, the reduction from IP-M-EDCP to P-MLWE (or MLWE) produces only $\mathcal{O}(\log\kappa)$ samples. However, as discussed in the technical overview in Section 2.3, the application of the technique of [BKSW18], detailed in Section 5.2, requires $\mathsf{poly}(\kappa)$ many IP-MLWE-like samples.

Therefore, it is necessary to increase the number of available P-MLWE samples from $\mathcal{O}(\log(\kappa))$ to $\mathsf{poly}(\kappa)$ before mapping the resulting instance to an IP-MLWE-like instance. We formalize this sample amplification step in Lemma 28, stated in Section 5.1.

5.1 Amplification of the Sample Number

To increase the number of samples, we rely on the well-known Regularity Lemma of [LPR13], which applies to cyclotomic rings. Since the reduction from IP-M-EDCP to P-MLWE requires the underlying polynomial to be of the form x^d-C for a constant integer C, in our setting we further restrict the polynomial to $f(x) = x^d+1$ with d a power of 2 to meet both requirements. In this case, the ring of integers of $\mathbb{Q}[x]/f$, denoted by $\mathcal{O}_K$, satisfies $\mathcal{O}_K = \mathbb{Z}[x]/f$. Therefore, the Regularity Lemma applies directly to the ring $\mathbb{Z}[x]/f$.

The technique has already been sketched in the technical overview in Section 2.3, and we omit the repetition here. We formalize the transformation from a P-MLWE instance with $\mathcal{O}(\log\kappa)$ samples to an IP-MLWE-like instance with $\mathsf{poly}(\kappa)$ samples in the following lemma.

Lemma 28. *Let κ be the security parameter. Let $f(x) = x^d + 1$ be an irreducible cyclotomic polynomial with $d = \mathsf{poly}(\kappa)$ a power of 2, $K = \mathbb{Q}[x]/f$ a number field and $\mathcal{O}_K$ its ring of integer. Let $q = \mathsf{poly}(\kappa)$ be an unramified prime in $\mathcal{O}_K$, which splits into $\mathfrak{p}_i$'s so that $\min_{i\in[k]} \mathcal{N}(\mathfrak{p}_i) \geqslant (nd)^{\omega(1/(m-n+1))}$. Let m, n be two positive integers satisfying $m = \mathcal{O}(\log(\kappa))$ and $n = \mathcal{O}(1)$. Let $m' = \mathsf{poly}(\kappa)$ be a positive integer. Let r_1, r_1' be two positive number satisfying $r_1, r_1' \geqslant \sqrt{d} \geqslant \eta_\varepsilon(\mathbb{Z}^d)$, where $\varepsilon = 2^{-\omega(\log(\kappa))}$. Let r_2 be a positive number such that $r_2 \geqslant 2d \cdot q^{\frac{n}{m}+\frac{2}{dm}}$. For a secret $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r_1'})^n$, consider $(\mathbf{A}(x), \mathbf{A}(x)\mathbf{s}(x)+\mathbf{e}(x) \bmod (q, f(x))) \hookleftarrow \mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},r_1,f}$, then there exists a polynomial-time algorithm that transforms the* P-MLWE *instance above to the* IP-MLWE*-like instance $(\widetilde{\mathbf{A}}', \widetilde{\mathbf{b}}' = \widetilde{\mathbf{A}}'\widetilde{\mathbf{s}} + \mathbf{e}'') \in \mathbb{Z}^{m'\times n}_{f(q)} \times \mathbb{Z}^{m'}_{f(q)}$, which satisfies the following conditions:*

1) *The distribution of $\widetilde{\mathbf{A}}'$ is close to $U(\mathbb{Z}^{m'\times n}_{f(q)})$ with statistical distance at most $2^{-\omega(\log(\kappa))}$;*
2) *The infinity norm of the error vector $\mathbf{e}''$ satisfies $\|\mathbf{e}''\|_\infty \leqslant c'_{max}\frac{q^d-1}{q-1}$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$. Here $c'_{max} = 2 + c_{max} + 2mr_1r_2d^2\sqrt{\kappa}$, where $c_{max} = 3r_1'\sqrt{\kappa}\cdot n^2 + 18n + 11/2$.*
3) *The distribution of the secret $\widetilde{\mathbf{s}}$ is statistically close to $D_{r_1'}(q)$ within distance $2^{-\omega(\log(\kappa))}$, where $D_{r_1'}(q)$ is obtained by sampling $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r_1'})^n$ and outputting $\mathsf{Eval}^{(f)}_q(\mathbf{s}(x) \bmod (q, f(x)))$.*

Proof.

Given an P-MLWE instance $(\mathbf{A}(x), \mathbf{b}(x) = \mathbf{A}(x)\mathbf{s}(x) + \mathbf{e}(x) \bmod q)$, we proceed as follows to obtain an IP-MLWE-like instance.

Since $f(x) = x^d + 1$ and d is a power of 2, the ring $\mathcal{O}_K$ is the ring of integers of the $2d$-th cyclotomic number field, and we have $\mathcal{O}_K = \mathbb{Z}[x]/f$. Under this setting, the Regularity Lemma stated in Supplementary Material D.2 applies directly to the ring $\mathbb{Z}_q[x]/f$.

By Lemma 48 in Supplementary Material D.1, for a uniformly random matrix $\mathbf{A}(x) \in (\mathbb{Z}_q[x]/f)^{m\times n}$ with $m \geqslant n$, the probability that $\mathbf{A}(x)$ contains an invertible submatrix of rank n is at least $1 - 2^{-\omega(\log(nd))} \geqslant 1 - 2^{-\omega(\log\kappa)}$.

Conditioned on this event, we sample $\mathbf{E}(x) \hookleftarrow (D^{\mathbb{H}}_{\mathcal{O}_K,r_2})^{m'\times m}$ and left-multiply both components of the MLWE instance by $\mathbf{E}(x)$. This yields the new instance $(\mathbf{E}(x)\mathbf{A}(x) \bmod q\mathcal{O}_K, \mathbf{E}(x)\mathbf{A}(x)\mathbf{s}(x) + \mathbf{E}(x)\mathbf{e}(x) \bmod q)$. For convenience, we denote the resulting instance by $(\mathbf{A}'(x), \mathbf{b}'(x) = \mathbf{A}'(x)\mathbf{s}(x) + \mathbf{e}'(x) \bmod q) \in (\mathbb{Z}_q[x]/f)^{m'\times n} \times (\mathbb{Z}_q[x]/f)^{m'}$, where $\mathbf{A}'(x) = \mathbf{E}(x)\mathbf{A}(x) \bmod q \in (\mathbb{Z}_q[x]/f)^{m'\times n}$ and $\mathbf{e}'(x) = \mathbf{E}(x)\mathbf{e}(x) \in (\mathbb{Z}[x]/f)^{m'}$.

By Corollary 6 in Supplementary Material D.2, the distribution of $\mathbf{A}'(x) \bmod q$ is statistically close to uniform distribution $U((\mathbb{Z}_q[x]/f)^{m'\times n})$, with statistical distance at most $2^{-\Omega(d)}$.

We now consider the upper bound of the infinity norm of each entry of the error terms.

First, the upper bound of the 1-norm of each entry of $\mathbf{E}(x)$, namely the polynomials $E_{i_1,i_2}(x)$. We have $\|E_{i_1,i_2}(x)\|_1 \leqslant \|\mathbf{V}_K^{-1}\|_1 \cdot \|\sigma(E_{i_1,i_2}(x))\|_1$. By Lemma 8,

$\|\sigma(E_{i_1,i_2}(x))\| \leqslant r_2\sqrt{d}$ with probability at least $(1-2^{-\omega(\log(\kappa))})$, and hence with probability at least $(1-2^{-\omega(\log(\kappa))})$, we have:

$$\|\sigma(E_{i_1,i_2}(x))\|_1 \leqslant \sqrt{d}\,\|\sigma(E_{i_1,i_2}(x))\| \leqslant r_2 d,$$

where the first inequality follows from the relation between ℓ_1-norm and ℓ_2-norm. Moreover, since $\|\mathbf{V}_K^{-1}\|_1 \leqslant \sqrt{d}\|\mathbf{V}_K^{-1}\| \leqslant d$ by the inequality between matrix norms (presented in Lemma 2 in Section 3.1), it follows that $\|E_{i_1,i_2}(x)\|_1 \leqslant r_2 d^2$. Secondly, for each entry of $\mathbf{e}(x)$, namely $e_{i_2}(x)$, we obtain $\|e_{i_2}(x)\|_\infty \leqslant r_1\sqrt{\kappa}$ with probability at least $1-2^{-\omega(\log(\kappa))}$.

With the above preparation, we bound the infinity norm of each entry of $\mathbf{e}'(x) = \mathbf{E}(x)\mathbf{e}(x)$. For any entry $e'_{i_1}(x)$, we have

$$e'_{i_1}(x) = \sum_{i_2\in[m]} E_{i_1,i_2}(x)\, e_{i_2}(x),$$

and hence its infinity norm can be bounded as follows:

$$\begin{aligned}
&\|e'_{i_1}(x)\|_\infty = \|\textstyle\sum_{i_2\in[m]} E_{i_1,i_2}(x)e_{i_2}(x)\|_\infty \\
\leqslant &\textstyle\sum_{i_2\in[m]} \|E_{i_1,i_2}(x)\cdot e_{i_2}(x)\|_\infty \\
\leqslant &\textstyle\sum_{i_2\in[m]} EF(f)\|E_{i_1,i_2}(x)\|_1 \cdot \|e_{i_2}(x)\|_\infty.
\end{aligned}$$

Since $f = x^d+1$, we have $EF(f) \leqslant 2$. Combining this with the analysis above, it follows that $\|e'_{i_1}(x)\|_\infty \leqslant 2m\, r_1 r_2\, d^2\sqrt{\kappa}$ with probability at least $1-2^{-\omega(\log(\kappa))}$.

We then apply the map $\mathsf{Eval}_q^{(f)}$ to transform the polynomial instance into an integer instance. Let

$$(\widetilde{\mathbf{A}}', \widetilde{\mathbf{b}}') = \left(\mathsf{Eval}_q^{(f)}(\mathbf{A}'(x)),\ \mathsf{Eval}_q^{(f)}\big(\mathbf{A}'(x)\mathbf{s}(x) + \mathbf{e}'(x) \bmod (q, f(x))\big)\right).$$

Since $f(x) = x^d + 1$ and hence $f(q) > q^d$, by Lemma 18 in Section 3.6, we can rewrite $\mathbf{A}'(x)\mathbf{s}(x) + \mathbf{e}'(x) \bmod (q, f(x))$ as

$$\begin{aligned}
&\Phi_q^{(f)}(\mathbf{A}'(q) \bmod f(q)) \cdot \Phi_q^{(f)}(\mathbf{s}(q) \bmod f(q)) + \Phi_q^{(f)}(\mathbf{e}'(q) \bmod f(q)) \\
= &\Phi_q^{(f)}\big(\mathbf{A}'(q)\mathbf{s}(q) + \mathbf{e}'(q) \bmod f(q)\big) + \mathbf{c}'(\mathbf{A}'(x), \mathbf{e}'(x)),
\end{aligned}$$

where $\mathbf{c}'(\mathbf{A}'(x), \mathbf{e}'(x))$ is a carry term. We next bound the infinity norm of $\mathbf{c}'(\mathbf{A}'(x), \mathbf{e}'(x))$. According to Lemma 46 in Supplementary Material C.2, together with $EF(f) \leqslant 2$ and the bound on the infinity norm of each entry of $\mathbf{s}(x)$, we obtain for each entry of $\mathbf{c}'(\mathbf{A}'(x), \mathbf{e}'(x))$, the infinite norm can be upper bounded as $3r'_1\sqrt{\kappa}\cdot n^2 + 18n + 11/2$ with probability at least $1-2^{-\omega(\log(\kappa))}$, and we denote it as c_{max}.

Moreover, for $\mathbf{A}'_i(x)$, the i-th row of the matrix $\mathbf{A}'(x)$, we have:

$$\begin{aligned}
&\mathsf{Eval}_q^{(f)}\left(\langle \mathbf{A}'_i(x), \mathbf{s}(x)\rangle + e'_i(x) \bmod f(x)\right) \\
=&\mathsf{Eval}_q^{(f)}\left(\Phi_q^{(f)}(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q)) + c'_i(\mathbf{A}'(x), \mathbf{e}(x)) \bmod q\right) \\
=&\mathsf{Eval}_q^{(f)}\left(\Phi_q^{(f)}(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q)) + c'_i(\mathbf{A}'(x), \mathbf{e}'(x)) + q\sum_{j=0}^{d-1}\delta_j x^j\right),
\end{aligned}$$

where

$$\delta_j = \lfloor \frac{\Phi_q^{(f)}(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))_j + c'_i(\mathbf{A}'(x), \mathbf{e}'(x))_j}{q} \rceil \in \{0, \pm 1\},$$

$c'_i(\mathbf{A}'(x), \mathbf{e}'(x))$ is the i-th entry of $\mathbf{c}'(\mathbf{A}'(x), \mathbf{e}'(x))$ and $\Phi_q^{(f)}(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))_j$ is the j-th coefficient of $\Phi_q^{(f)}(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))$, while $c'_i(\mathbf{A}'(x), \mathbf{e}'(x))_j$ is the j-th coefficient of polynomial $c'_i(\mathbf{A}'(x), \mathbf{e}'(x))$. Continuing the computation, we have:

$$\begin{aligned}
&\mathsf{Eval}_q^{(f)}(\langle \mathbf{A}'_i(x), \mathbf{s}(x)\rangle + e'_i(x) \bmod f(x)) \\
=&\mathsf{Eval}_q^{(f)}\Big(\Phi_q(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q)) + \delta' f(x) + c'_i(\mathbf{A}', \mathbf{e}') + q\sum_{j=0}^{d-1}(\delta_j + \delta'_j)x^j\Big) \\
=&\Phi_q(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))(q) + \delta' f(q) \\
&+ c'_i(\mathbf{A}'(x), \mathbf{e}'(x))(q) + \sum_{j=0}^{d-1}\left(\delta_{j-1} + \delta'_{j-1}\right) q^j \bmod f(q) \\
=&\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q) + c'_i(\mathbf{A}'(x), \mathbf{e}'(x))(q) + \sum_{j=0}^{d-1}\left(\delta_{j-1} + \delta'_{j-1}\right) q^j \bmod f(q) \\
=&\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) + c'_i(\mathbf{A}'(x), \mathbf{e}'(x))(q) + \sum_{j=0}^{d-1}\left(\delta_{j-1} + \delta'_{j-1}\right) q^j \bmod f(q),
\end{aligned}$$

which is subject to the relations $\delta' = \left\lfloor \frac{\Phi_q(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))}{f(x)} \right\rceil \in \{0, \pm 1\}$, $\delta_{-1} = -\delta_{d-1}$, $\delta'_j = \left\lfloor \frac{\Phi_q(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))_j + \delta' f_j}{q} \right\rceil \in \{0, \pm 1\}$, and $\delta'_{-1} = -\delta'_{d-1}$. Here the integer $\Phi_q(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))_j$ denotes the j-th coefficient of the polynomial $\Phi_q(\langle \mathbf{A}'_i(q), \mathbf{s}(q)\rangle + e'_i(q) \bmod f(q))$, and f_j denotes the j-th coefficient of $f(x)$.

We consider the summation

$$e''_i = e'_i(q) + c'_i(\mathbf{A}'(x), \mathbf{e}'(x))(q) + \sum_{j=0}^{d-1}(\delta_{j-1} + \delta'_{j-1})q^j.$$

According to the upper bounds established earlier in the proof, the absolute value of e''_i satisfies

$$|e''_i| \leqslant \left(2 + c_{\max} + 2mr_1r_2d^2\sqrt{\kappa}\right)\frac{q^d - 1}{q - 1}$$

with probability at least $1 - 2^{-\omega(\log(\kappa))}$. Moreover, the coefficients of the polynomial $\Phi_q^{(f)}\left(e'_i(q) + c'_i(\mathbf{A}', \mathbf{e}')(q) + \sum_{j=0}^{d-1}\delta_{j-1}q^j\right)$ are bounded above by $2 + c_{\max} + 2mr_1r_2d^2\sqrt{\kappa}$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$. We denote this upper bound by $c'_{\max}$. Let $\mathbf{e}'' = (e''_0, \ldots, e''_{m'-1})^\top$, and we obtain an instance $\left(\widetilde{\mathbf{A}}', \widetilde{\mathbf{b}}'\right) =$

$\left(\widetilde{\mathbf{A}}', \widetilde{\mathbf{A}}' \cdot \widetilde{\mathbf{s}} + \mathbf{e}'' \bmod f(q)\right)$ where $\widetilde{\mathbf{s}} = \mathbf{s}(q) \bmod f(q)$. We next show that this is precisely the instance required in the statement of the lemma.

According to the upper bound on $|e_i''|$, the condition in item 2) is satisfied. Moreover, since $\widetilde{\mathbf{s}} = \mathbf{s}(q) \bmod f(q)$, the condition in item 3) is also satisfied.

As to the item 1), we define the following two distributions:

$$\mathcal{D}_1 = \left\{ \widetilde{\mathbf{A}}_1 \in \mathbb{Z}_{f(q)}^{m' \times n} \;\middle|\; \begin{array}{l} \widetilde{\mathbf{A}}_1 = \mathsf{Eval}_q^{(f)}(\mathbf{E}(x)\mathbf{A}(x) \bmod (q, f(x))), \\ \mathbf{E}(x) \hookleftarrow (D_{\mathcal{O}_K, r_2}^{\mathbb{H}})^{m' \times m}, \;\; \mathbf{A}(x) \xleftarrow{\$} U((\mathbb{Z}_q[x]/f(x))^{m \times n}) \end{array} \right\},$$

$$\mathcal{D}_2 = \left\{ \widetilde{\mathbf{A}}_2 \in \mathbb{Z}_{f(q)}^{m' \times n} \middle| \widetilde{\mathbf{A}}_2 = \mathbf{A}'(q) \bmod f(q), \mathbf{A}'(x) \xleftarrow{\$} U\left((\mathbb{Z}_q[x]/f)^{m' \times n}\right) \right\}.$$

By Corollary 6 in Supplemenatry Material D.2, the statistical distance between $\mathcal{D}_1$ and $\mathcal{D}_2$ can be bounded as below: $\Delta(\mathcal{D}_1, \mathcal{D}_2) \leqslant 2^{-\omega(\log(\kappa))}$. While the statistical distance between $\mathcal{D}_2$ and $U(\mathbb{Z}_{f(q)}^{m' \times n})$ is at most $2^{-\omega(\log(\kappa))}$ due to Corollary 7 in Supplementary Material D.3. Then we have:

$$\begin{aligned} \Delta\left(\mathcal{D}_1, U(\mathbb{Z}_{f(q)}^{m' \times m})\right) \leqslant & \Delta\left(\mathcal{D}_1, \mathcal{D}_2\right) + \Delta\left(\mathcal{D}_2, U(\mathbb{Z}_{f(q)}^{m' \times m})\right) \\ \leqslant & 2^{-\omega(\log(\kappa))} + 2^{-\omega(\log(\kappa))} \leqslant 2^{-\omega(\log(\kappa))}. \end{aligned}$$

This completes the proof of the item 1). □

5.2 Reduction from MLWE to G-IP-M-EDCP

To complete the reduction from MLWE to IP-M-EDCP, we also rely on the subdivision map defined in [BKSW18]. The following lemma formally defines the mapping ϕ, as previously mentioned in Section 2.1.

Lemma 29 ([BKSW18, Lemma 12]). *For a constant $C \geqslant 8$, a matrix $\mathbf{A} \in \mathbb{Z}_{q'}^{m \times n}$ is randomly chosen for integers q', n, m, and $k \geqslant m$, consider a function*[7]

$$g : (x_0, \ldots x_{m-1}) \mapsto \left(\lfloor (x_0/z) - w_0 \bmod \bar{q}' \rfloor, \ldots \lfloor (x_{m-1}/z) - w_{m-1} \bmod \bar{q}' \rfloor\right),$$

where $z = q/c$ and $z \in \left[\frac{1}{c}, \frac{1}{2}\right] \cdot \lambda_1^{\infty}(\Lambda_{q'}(\mathbf{A}))$, $w_0, \ldots w_{m-1}$ are uniformly chosen from $[0, 1)$, and $\bar{q}' = q/z$. Then for any $x \in \mathbb{Z}_{q'}^n$, we have the following two statements:

1) *For any $\mathbf{u} = \mathbf{A}\mathbf{x} + \mathbf{e}$, $\mathbf{v} = \mathbf{A}\mathbf{x} + \mathbf{e}_2$ where $\|\mathbf{e}_1\|_\infty$, $\|\mathbf{e}_2\|_\infty \leqslant \lambda_1^{\infty}(\Lambda_{q'}(\mathbf{A}))/(2kC)$, with probability $(1 - 1/k)^m$, over randomness of $w_0, \ldots, w_{m-1}$, we have $g(\mathbf{u}) = g(\mathbf{v})$;*
2) *For any $\mathbf{u} = \mathbf{A}\mathbf{x} + \mathbf{e}_1$, $v = \mathbf{A}\hat{\mathbf{x}} + \mathbf{e}_2$, where $\|\mathbf{e}_1\|_\infty$, $\|\mathbf{e}_2\|_\infty \leqslant \lambda_1^{\infty}(\Lambda_{q'}(\mathbf{A}))/(2kC)$ and $\mathbf{x} \neq \hat{\mathbf{x}} \in \mathbb{Z}_q^n$, we have $g(\mathbf{u}) \neq g(\mathbf{v})$.*

[7] The w_i's in the following function is randomized once, and randomized classically, and that "applying the map g" means also to select the values w_i's.

As discussed above, amplifying the number of samples introduces a dependency between the error term and the other components, which is not the case for the standard IP-MLWE samples. To address this, the following lemma introduces a more general oracle which poses restriction mainly on the smallness of the error term, which are satisfied by the IP-MLWE-like instance described earlier. Consequently, the result presented below is slightly more general than the standard reduction from IP-MLWE to IP-M-EDCP.

Lemma 30. *Let κ be the security parameter, and let $C \geqslant 8$ be a constant, m', n two positive integers, where $m' \leqslant \mathsf{poly}(\kappa)$. Let f be an irreducible and monic polynomial of degree d over the ring $\mathbb{Z}[x]$. Let $q = \mathsf{poly}(\kappa)$ be a positive integer and $f(q) \geqslant q^d$. Let χ be the distribution of secret $\mathbf{s}$ over $\mathbb{Z}_{f(q)}^n$. Let r be a positive number, l a positive integer and $k = m'l$. Given an oracle: for $\mathbf{s} \hookleftarrow \chi$ fixed, choose $\mathbf{A} \hookleftarrow U(\mathbb{Z}_{f(q)}^{m' \times n})$, $\mathbf{e} \hookleftarrow \varphi_{\mathbf{A}}$, where $\varphi_{\mathbf{A}}$ can be any distribution of $\mathbf{e}$ correlated (or not) to the distribution of matrix $\mathbf{A}$, which satisfies $\|\Phi_q^{(f)}(\mathbf{e})\|_\infty \leqslant B$ and $\|\mathbf{e}\|_\infty \in \left(-\frac{q}{2}\frac{q^d-1}{q-1}, \frac{q}{2}\frac{q^d-1}{q-1}\right]$, and outputs $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \bmod f(q))$. Let the parameters satisfy the following condition:*

$$\left(3 + r\sqrt{\kappa}Bd\left(EF(f) + 2/q\right)\right) \cdot (q^d - 1)/(q-1) \leqslant f(q)^{\frac{m'-n}{m'}}/(4kC).$$

There is a polynomial-time quantum algorithm with inputs the instance $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \bmod f(q))$ from the above oracle and outputs G-IP-M-EDCP instance

$$\left\{\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}'_i + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s} \bmod f(q)\rangle\right\}_{i\in[l]}$$

with probability at least $1/e$, where $\mathbf{x}'_i$'s are unknown and $\mathbf{s}$ is the same as the secret in the input.

Proof. At the beginning of the reduction, we are given an input of form $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \bmod f(q))$ as specified in the lemma. First, We prepare a state: $\sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n} |0\rangle|\mathbf{x}\rangle|0\rangle$. Then, according to Lemma 21 in Section 3.7, we produce a quantum state within trace distance $2^{-\Omega(\kappa)}$ of the following quantum state:

$$\sum_{\mathbf{c}\in\mathbb{Z}^d} \sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}\rangle|0\rangle. \tag{22}$$

Then by Lemma 24 in Section 3.7, the trace distance between the above state and the following one is at most $2^{-\omega(\log(\kappa))}$:

$$\sum_{\mathbf{c}\in\mathbb{Z}^d \bigcap [-r\sqrt{\kappa}, r\sqrt{\kappa}]^d} \sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}\rangle|0\rangle \tag{23}$$

We apply the function $f(\mathbf{c}, \mathbf{x}) = \mathbf{A}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle(\mathbf{A}\mathbf{s} + \mathbf{e}) \bmod f(q)$ on the first two registers and store the result in the third register:

$$\begin{aligned}
&\sum_{\mathbf{c}\in\mathbb{Z}^d \bigcap (-r\sqrt{\kappa}, r\sqrt{\kappa}]^d} \sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}\rangle|\mathbf{A}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle(\mathbf{A}\mathbf{s} + \mathbf{e}) \bmod f(q)\rangle \\
= &\sum_{\mathbf{c}\in\mathbb{Z}^d \bigcap (-r\sqrt{\kappa}, r\sqrt{\kappa}]^d} \sum_{\mathbf{x}\in\mathbb{Z}_{f(q)}^n} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle \cdot \mathbf{s} \bmod f(q)\rangle|\mathbf{A}\mathbf{x} - \langle \mathbf{c}, \mathbf{z}\rangle \cdot \mathbf{e} \bmod f(q)\rangle
\end{aligned}$$

Given $\|\Phi_q^{(f)}(\mathbf{e})\|_\infty \leqslant B$, according to Lemma 51 in Supplementary Material D.4, we have

$$\|\langle \mathbf{c}, \mathbf{z}\rangle \mathbf{e} \bmod f(q)\|_\infty \leqslant \left(3 + r\sqrt{\kappa} B d \left(EF(f) + 2/q\right)\right) \cdot (q^d - 1)/(q-1).$$

We set $\mathbf{e}_{tot} = \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{e} \bmod f(q)$. Next, we apply the map g (as defined in Lemma 29) to the third register and store the output in the fourth register:

$$\sum_{\substack{\mathbf{c}\in\mathbb{Z}^d \bigcap (-r\sqrt{\kappa}, r\sqrt{\kappa}]^d \\ \mathbf{x}\in\mathbb{Z}_{f(q)}^n}} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle \cdot \mathbf{s}\rangle|\mathbf{A}\mathbf{x} - \mathbf{e}_{tot} \bmod f(q)\rangle|g(\mathbf{A}\mathbf{x} - \mathbf{e}_{tot} \bmod f(q))\rangle. \tag{24}$$

Due to our parameter settings, the following condition in formula (25) holds, and thus we can apply Lemma 29.

$$\|\langle \mathbf{c}, \mathbf{z}\rangle \mathbf{e} \bmod f(q)\|_\infty \leqslant \left(3 + r\sqrt{\kappa} B d \left(EF(f) + \frac{2}{q}\right)\right) \frac{q^d - 1}{q-1} \leqslant \frac{f(q)^{\frac{m'-n}{m'}}}{4kC}. \tag{25}$$

We now measure the last register in (24). By Lemma 29, this yields the following quantum state with probability at least $(1 - 1/k)^{m'}$:

$$\sum\nolimits_{\mathbf{c}\in\mathbb{Z}^d \bigcap (-r\sqrt{\kappa}, r\sqrt{\kappa}]^d} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}' + \langle \mathbf{c}, \mathbf{z}\rangle \cdot \mathbf{s}\rangle|\mathbf{A}\mathbf{x}' - \mathbf{e}_{tot} \bmod f(q)\rangle.$$

We evaluate the function $(\mathbf{c}, \mathbf{x}, \mathbf{b}) \mapsto \mathbf{b} - \mathbf{A}\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle(\mathbf{A}\mathbf{s} + \mathbf{e})$ to zeroize the third register, obtaining $\sum_{\mathbf{c}\in\mathbb{Z}^d \cap (-r\sqrt{\kappa}, r\sqrt{\kappa}]^d} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}' + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s}\rangle$. By Lemma 24 in Section 3.7, the trace distance between this state and

$$\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}' + \langle \mathbf{c}, \mathbf{z}\rangle \mathbf{s}\rangle$$

is at most $2^{-\omega(\log(\kappa))}$. The claim follows. □

By combining Lemma 28 and Lemma 30, we arrive at the following main theorem.

Theorem 4. *Let κ be the security parameter, and let $C \geqslant 8$ be a constant. Let $f(x) = x^d + 1$ be an irreducible cyclotomic polynomial with $d = \mathsf{poly}(\kappa)$ a power of 2, $K = \mathbb{Q}[x]/f$ be the corresponding number field, and $\mathcal{O}_K$ its ring of integers. Let $q = \mathsf{poly}(\kappa)$ be an unramified prime integer that splits into prime ideals $\mathfrak{p}_i$ such that $\min_{i\in[k]} \mathcal{N}(\mathfrak{p}_i) \geqslant (nd)^{\omega(1/(m-n+1))}$. Let m, n be positive integers satisfying $m = \mathcal{O}(\log(\kappa))$ and $n = \mathcal{O}(1)$. Let l be a positive integer. Let r_1, r_1' be two positive integers satisfying $r_1, r_1' \geqslant \sqrt{d} \geqslant \eta_\varepsilon(\mathbb{Z}^d)$, where $\varepsilon = 2^{-\omega(\log(\kappa))}$. Let r_2 be a positive number such that $r_2 \geqslant 2d \cdot q^{\frac{n}{m} + \frac{2}{dm}}$, let $m' = \mathsf{poly}(\kappa)$, and let r be a positive number such that*

$$\left(3 + r\sqrt{\kappa} c'_{max} d \left(\sqrt{2} + 2/q\right)\right) \cdot (q^d - 1) \Big/ (q-1) \leqslant f(q)^{\frac{m'-n}{m'}} / (4m'lC),$$

where $c'_{max} = 2 + c_{max} + 2mr_1r_2d^2\sqrt{\kappa}$, $c_{max} = 3r_1'\sqrt{\kappa} \cdot n^2 + 18n + 11/2$.

Then there exists a polynomial-time reduction from $\mathsf{P\text{-}MLWE}^{m,n}_{q,r'_1,r_1,f}$ *problem to* $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{l,n}_{q,D_{r'_1}(q),r,f}$*, where* $D_{r'_1}(q)$ *denotes the distribution selecting the polynomial vector* $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r'_1})^n$ *and outputting* $\mathsf{Eval}^{(f)}_q(\mathbf{s}(x) \bmod (q, f(x)))$.

Proof. For a secret $\mathbf{s} \hookleftarrow (D_{\mathbb{Z}[x]/f,r'_1})^n$, we are given an instance $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e} \bmod (q, f(x))) \hookleftarrow \mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},r_1,f}$. According to Lemma 28, with probability at least $1-2^{-\omega(\log(\kappa))}$, there exists a polynomial-time algorithm that transforms the given instance to the instance $(\widetilde{\mathbf{A}}', \widetilde{\mathbf{b}}' = \widetilde{\mathbf{A}}'\widetilde{\mathbf{s}}' + \mathbf{e}'' \bmod f(q)) \in \mathbb{Z}^{m'\times n}_{f(q)} \times \mathbb{Z}^{m'}_{f(q)}$, where the distribution of $\widetilde{\mathbf{A}}'$ is close to $U(\mathbb{Z}^{m'\times n}_{f(q)})$ with statistical distance at most $2^{-\omega(\log(\kappa))}$, the distribution of $\mathbf{e}''$ is correlated to the distribution of the matrix $\widetilde{\mathbf{A}}'$, with the property that $\|\Phi^{(f)}_q(\mathbf{e}'')\|_\infty \leqslant c'_{max}$ and $\|\mathbf{e}''\|_\infty \leqslant c'_{max}\frac{q^d-1}{q-1}$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$. Furthermore, according to the distribution of $\mathbf{s}$, the distribution of $\widetilde{\mathbf{s}}$ is close to $D_{r'}(q)$ by a statistical distance at most $2^{-\omega(\log(\kappa))}$. The conditions above satisfy the requirements for applying Lemma 30. Therefore, by providing the instance $(\widetilde{\mathbf{A}}', \widetilde{\mathbf{b}}' = \widetilde{\mathbf{A}}'\widetilde{\mathbf{s}} + \mathbf{e}'' \bmod f(q))$ to the reduction algorithm in Lemma 30, with probability at least $1/e$, this algorithm can output l quantum states and each one has a trace distance at most $2^{-\omega(\log(\kappa))}$ from the quantum state below:

$$\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_r(\mathbf{c})|\mathbf{c}\rangle|\mathbf{x}' + \langle \mathbf{c}, \mathbf{z}\rangle\widetilde{\mathbf{s}} \bmod f(q)\rangle, \tag{26}$$

The polynomial-time reduction from search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r'_1,r_1,f}$ problem to search $\mathsf{G\text{-}stEDCP}^{l,n}_{q,D_{r'_1}(q),r,f}$ follows. □

For readers interested in the reduction from MLWE to IP-M-EDCP, we also provide a more general result that removes the restrictions on the sample size and the module rank of the MLWE instance. In Supplementary Material D.5, we present a reduction from MLWE with sufficiently many samples (e.g., $\mathcal{O}(n \log q)$ samples for module rank n) to IP-M-EDCP, which moreover applies to a broader class of underlying rings.

6 Reduction from IP-M-EDCP to EDCP

In the following theorem, we first reduce from IP-M-EDCP to EDCP with same (exponentially large) modulus. Then we present how we can further reduce the latter problem to the standard one with polynomially large modulus.

Theorem 5. *Let* κ *be the security parameter;* f *be a monic and irreducible polynomial with degree* d*;* m, n, q *be positive integers and* $r > 0$*. There exists a polynomial-time reduction from* $\mathsf{G\text{-}IP\text{-}M\text{-}EDCP}^{m,n}_{q,U(\mathbb{Z}^n_{f(q)}),r,f}$ *to* $\mathsf{G\text{-}EDCP}^{m,n}_{f(q),U(\mathbb{Z}^n_{f(q)}),r}$.

Proof. Given an IP-M-EDCP quantum state $\sum_{\mathbf{c}\in\mathbb{Z}^d} \rho_r(\mathbf{c})\,|\mathbf{c}\rangle\,|\mathbf{x} + \langle \mathbf{c}, \mathbf{z}\rangle\mathbf{s} \bmod f(q)\rangle$, where $\mathbf{c} = (c_0, \ldots, c_{d-1})^\top$, measure $c_1, \ldots, c_{d-1}$ and denote $\bar{c} = \sum_{i=1}^{d-1} q^i c_i$ and

get the following quantum state:

$$\sum_{c_0 \in \mathbb{Z}} \rho_r(c_0) \left| c_0 \right\rangle \left| \mathbf{x} + \bar{c}\mathbf{s} + c_0 \mathbf{s} \bmod f(q) \right\rangle . \tag{27}$$

Let $\mathbf{x} + \bar{c}\mathbf{s} = \mathbf{x}'$, then the quantum state in (27) is an EDCP state. □

In the reduction above, starting from IP-M-EDCP, we can reduce to the EDCP problem with dimension n and modulus $f(q)$. Then, one can reduce this EDCP problem to LWE with dimension n and modulus $f(q)$ as shown in [BKSW18]. Using the dimension-modulus switching technique introduced in [BLP+13], the latter problem can be reduced to LWE with dimension $\mathcal{O}(nd \log q)$ and modulus q. Finally, we can apply the LWE to EDCP reduction, which preserves both dimension and modulus. Therefore, we can eventually reduce IP-M-EDCP to the more classical EDCP with polynomially large modulus. We refer to Supplementary Material E for details.

Acknowledgments

We thank the anonymous reviewers for their helpful feedback. This work was supported by the HELO ANR grant (ANR-24-CE48-4293) and the European Union's Horizon Europe research and innovation programme under the project "Quantum Secure Networks Partnership" (QSNP, No. 101114043).

References

ACF+15. Martin R Albrecht, Carlos Cid, Jean-Charles Faugere, Robert Fitzpatrick, and Ludovic Perret. On the complexity of the bkw algorithm on lwe. Designs, Codes and Cryptography, 74(2):325–354, 2015.

Ban93. Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. Math. Ann., 296:625–635, 1993.

BD20. Zvika Brakerski and Nico Döttling. Lossiness and entropic hardness for ring-LWE. In TCC, pages 1–27. Springer, 2020.

BDK+18. Joppe Bos, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Vadim Lyubashevsky, John M Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM. In EuroS&P, pages 353–367. IEEE, 2018.

BGV12. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In ITCS, pages 309–325, 2012.

BJK+25a. Shi Bai, Hansraj Jangir, Elena Kirshanova, Tran Ngo, and William Youmans. A quasi-polynomial time algorithm for the extrapolated dihedral coset problem over power-of-two moduli. In CRYPTO, 2025.

BJK+25b. Shi Bai, Hansraj Jangir, Elena Kirshanova, Tran Ngo, and William Youmans. A quasi-polynomial time algorithm for the extrapolated dihedral coset problem over power-of-two moduli. Cryptology ePrint Archive, 2025.

BJRLW23. Katharina Boudgoust, Corentin Jeudy, Adeline Roux-Langlois, and Weiqiang Wen. On the hardness of module learning with errors with short distributions. J. Cryptol., 36(1):1, 2023.

BKSW18. Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen. Learning with errors and extrapolated dihedral cosets. In PKC, pages 702–727. Springer, 2018.

BLL+15. Shi Bai, Adeline Langlois, Tancrede Lepoint, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance. In ASIACRYPT, pages 3–24, 2015.

BLP+13. Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In STOC, pages 575–584, 2013.

BLRL+18. Shi Bai, Tancrède Lepoint, Adeline Roux-Langlois, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. Improved security proofs in lattice-based cryptography: using the Rényi divergence rather than the statistical distance. J. Cryptol., 31:610–640, 2018.

BV11. Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In CRYPTO, pages 505–524. Springer, 2011.

Che24. Yilei Chen. Quantum algorithms for lattice problems. Cryptology ePrint Archive, Paper 2024/555, 2024.

Con24. Keith Conrad. The conductor ideal of an order. Expository paper. url: https://kconrad. math. uconn. edu/blurbs/gradnumthy/conductor. pdf, 1(1):2–2, 2024.

DKL+18. Léo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, and Damien Stehlé. CRYSTALS-Dilithium: A lattice-based digital signature scheme. CHES, 2018(1):238–268, 2018.

DSSS21. Julien Devevey, Amin Sakzad, Damien Stehlé, and Ron Steinfeld. On the integer polynomial learning with errors problem. In PKC, pages 184–214. Springer, 2021.

Erd32. Paul Erdos. Beweis eines satzes von tschebyschef. Acta Sci. Math., 5:194–198, 1932.

GMPW20. Nicholas Genise, Daniele Micciancio, Chris Peikert, and Michael Walter. Improved discrete gaussian and subgaussian analysis for lattice cryptography. In PKC, pages 623–651. Springer, 2020.

GPV08. Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In STOC, pages 197–206, 2008.

Gu19. Chunsheng Gu. Integer version of ring-LWE and its applications. In SocialSec, pages 110–122. Springer, 2019.

GVL13. Gene H Golub and Charles F Van Loan. Matrix computations. JHU press, 2013.

HLS18. Andreas Hülsing, Tanja Lange, and Kit Smeets. Rounded gaussians: fast and secure constant-time sampling for lattice-based crypto. In PKC, pages 728–757. Springer, 2018.

Joh70. Charles Royal Johnson. Positive definite matrices. The American Mathematical Monthly, 77(3):259–264, 1970.

Kup05. Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. SIAM J. Comput., 35(1):170–188, 2005.

Kup11. Greg Kuperberg. Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. arXiv preprint arXiv:1112.3333, 2011.

LM06. Vadim Lyubashevsky and Daniele Micciancio. Generalized compact knapsacks are collision resistant. In ICALP, pages 144–155. Springer, 2006.

LPR10. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In EUROCRYPT, pages 1–23. Springer, 2010.

LPR13. Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-LWE cryptography. In EUROCRYPT, pages 35–54. Springer, 2013.

LPSS14. San Ling, Duong Hieu Phan, Damien Stehlé, and Ron Steinfeld. Hardness of k-LWE and applications in traitor tracing. In CRYPTO, pages 315–334, 2014.

LS15. Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr., 75(3):565–599, 2015.

May15. James Maynard. Small gaps between primes. Ann. Math., pages 383–413, 2015.

MR07. Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. SIAM J. Comput., 37(1):267–302, 2007.

NC10. Michael A Nielsen and Isaac L Chuang. Quantum computation and quantum information. Cambridge university press, 2010.

Pei09. Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In STOC, pages 333–342, 2009.

Pei10. Chris Peikert. An efficient and parallel gaussian sampler for lattices. In CRYPTO, pages 80–97. Springer, 2010.

PR06. Chris Peikert and Alon Rosen. Efficient collision-resistant hashing from worst-case assumptions on cyclic lattices. In TCC, pages 145–166. Springer, 2006.

Ram19. Srinivasa Ramanujan. A proof of Bertrand's postulate. J. Indian Math. Soc., 11(181-182):27, 1919.

Reg04a. Oded Regev. Quantum computation and lattice problems. SIAM J. Comput., 33(3):738–760, 2004.

Reg04b. Oded Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space. arXiv preprint quant-ph/0406151, 2004.

Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. STOC, pages 84–93, 2005.

Reg09. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. J. ACM, 56(6):1–40, 2009.

RSW18. Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. In EUROCRYPT, pages 146–173. Springer, 2018.

SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In ASIACRYPT, pages 617–635. Springer, 2009.

Supplementary Materials

A Supplementary Materials for Failure of the Reduction from P-MLWE to M-EDCP

We first recall the process in [BKSW18]. First, generate the quantum state of the form

$$\sum_{j\in\mathbb{Z}}\sum_{\mathbf{x}\in\mathbb{Z}^n}\rho_r(j)\,|j\rangle\,|\mathbf{x}\rangle\,. \tag{28}$$

Then with the LWE instance $(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e} \bmod q)$, We can generate the quantum state as follows:

$$\sum_{j\in\mathbb{Z}}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\rho_r(j)\,|j\rangle\,|\mathbf{x}\rangle\,|\mathbf{A}(\mathbf{x}-j\cdot\mathbf{s})-j\cdot\mathbf{e} \bmod q\rangle\,.$$

Then replaceing $\mathbf{x}$ with $\mathbf{x}-j\cdot\mathbf{s}$, and we can get the quantum state of the form:

$$\sum_{j\in\mathbb{Z}}\sum_{\mathbf{x}\in\mathbb{Z}_q^n}\rho_r(j)\,|j\rangle\,|\mathbf{x}+j\cdot\mathbf{s} \bmod q\rangle\,|\mathbf{A}\mathbf{x}-j\cdot\mathbf{e} \bmod q\rangle\,.$$

The next step is to discretize the ambient space by a coarse cell decomposition. More precisely, we divide the space into cells of width d_{cell} and define $\phi(\mathbf{y})$ maps $\mathbf{y}$ into the cell containing $\mathbf{y}$. This map is illustrated in Figure 6. Intuitively, ϕ forgets the exact position of a point and only records the coarse cell to which it belongs.

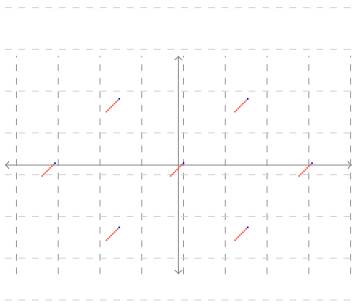

Fig. 6. Illustration of the cell decomposition used in the reduction from LWE to EDCP.

The cell width is chosen between the size of the shifted error and the minimum distance of the q-ary lattice, namely $\|j\cdot\mathbf{e}\|_\infty < d_{\mathsf{cell}} < \lambda_1^\infty(\Lambda_q(\mathbf{A}))$. This guarantees the two properties needed for the reduction. First, since $j\mathbf{e}$ is small compared with the cell width, the two points $\mathbf{A}\mathbf{x}$ and $\mathbf{A}\mathbf{x}-j\cdot\mathbf{e}$ are mapped to the same cell with high probability, namely $\phi(\mathbf{A}\mathbf{x})=\phi(\mathbf{A}\mathbf{x}-j\mathbf{e})$. Second, since

the cell width is smaller than the minimum ℓ_∞-distance between distinct points of $\Lambda_q(\mathbf{A})$, different lattice points are mapped to different cells. After coherently computing the cell label, the state becomes

$$\sum_{\substack{j\in\mathbb{Z}\\ \mathbf{x}\in\mathbb{Z}^n}} \rho_r(j)\,|j\rangle\,|\mathbf{x}+j\cdot\mathbf{s}\rangle\,|\mathbf{A}\mathbf{x}-j\cdot\mathbf{e}\rangle\,|\phi(\mathbf{A}\mathbf{x}-j\cdot\mathbf{e})\rangle\,.$$

Measuring the last register fixes the cell label and thereby erases the fine information contained in the third register. Conditioned on the good event that the perturbation $j\mathbf{e}$ does not cross a cell boundary, the remaining state is therefore an EDCP-type state with hidden shift $\mathbf{s}$ and Gaussian weights $\rho_r(j)$.

Then, if we try to follow the framework recalled above to give a reduction from P-MLWE to M-EDCP, a natural first attempt is to replace the integer elements in the LWE-to-EDCP reduction by ring elements. Namely, instead of starting from quantum states of the form (28), we consider the state

$$\sum_{\substack{j(x)\in\mathbb{Z}[x]/f(x)\\ \mathbf{s}'(x)\in(\mathbb{Z}_q[x]/f(x))^n}} \rho_r(j(x))\,|j(x)\rangle\,|\mathbf{s}'(x)\rangle\,, \tag{29}$$

where $\rho_r(j(x))$ means that the coefficient vector of $j(x)$ is sampled according to a discrete Gaussian distribution with deviation parameter r. Throughout, ring elements are stored in the computational basis via their coefficient-vector representation.

Given a P-MLWE instance $(\mathbf{A}(x), \mathbf{A}(x)\mathbf{s}(x)+\mathbf{e}(x)) \in (\mathbb{Z}_q[x]/f(x))^{m\times n} \times (\mathbb{Z}_q[x]/f(x))^m$, one could formally repeat the procedure of [BKSW18]. After the corresponding variable substitution, this gives a quantum state of the form

$$\sum_{\substack{j(x)\in\mathbb{Z}[x]/f(x)\\ \mathbf{s}'(x)\in(\mathbb{Z}_q[x]/f(x))^n}} \rho_r(j(x))\,|j(x)\rangle\,|\mathbf{s}'(x)+j(x)\cdot\mathbf{s}(x)\rangle\,|\mathbf{A}(x)\mathbf{s}'(x)-j(x)\cdot\mathbf{e}(x)\rangle\,.$$

Similarly to the procedure in [BKSW18], the next step is to define an analogous coarse cell map ϕ. This requires a cell decomposition of the coefficient-embedded ambient space $\mathbb{R}^{mn}$. In order for the cell map to separate distinct lattice points while being insensitive to the error perturbation, a suitable lower bound on $\lambda_1^\infty(\Lambda_q(\mathsf{rot}(\mathbf{A}(x))))$[8] is needed. However, although heuristic estimates for such quantities are widely used in lattice cryptanalysis [ACF+15], a provable lower bound of the required form does not seem to be available in the literature, to the best of our knowledge. Therefore, this direct adaptation of the LWE-to-EDCP reduction cannot be justified as it stands, and we need a different approach to obtain the desired reduction.

B Supplementary Materials for Preliminaries

B.1 Missing Proofs for Gaussian and Discrete Gaussian Distribution

The following part is the proof of Lemma 10.

[8] The map $\mathsf{rot}(\cdot)$ is defined in Section 3.2.

Proof. [of Lemma 10.] By Lemma 9, it's easy to get that

$$\frac{\rho_{r_1}(\Lambda)}{\rho_{r_2}(\Lambda)} \in \left[\frac{1-\varepsilon}{1+\varepsilon}, \frac{1+\varepsilon}{1-\varepsilon}\right] \cdot \left(\frac{r_1}{r_2}\right)^n.$$

By Taylor series of $1/(1-\varepsilon)$ at 0,

$$(1+\varepsilon)/(1-\varepsilon) = 1 + 2\varepsilon + 2\sum_{i=2}^{+\infty} \varepsilon^i = 1 + 2\varepsilon + \frac{2\varepsilon^2}{1-\varepsilon}.$$

When $\varepsilon \leqslant 1/3$, $(2\varepsilon^2)/(1-\varepsilon) \leqslant \varepsilon$. Hence $(1+\varepsilon)/(1-\varepsilon) \leqslant 1+3\varepsilon$.

On the other side, by Taylor series of $1/(1+\varepsilon)$ at 0,

$$(1-\varepsilon)/(1+\varepsilon) = 1 + \sum_{i=1}^{+\infty}(-\varepsilon)^i + \sum_{i=1}^{+\infty}(-\varepsilon)^i = 1 - 2\varepsilon + \varepsilon^2/(1+\varepsilon) \geqslant 1 - 3\varepsilon.$$

The result follows. □

The following part is the proof of Lemma 11.

Proof. [of Lemma 11.] By Lemma 10, it's easy to get that

$$\frac{\rho_r(\Lambda + \mathbf{c})}{\rho_r(\Lambda)} \in \left[\frac{1-\varepsilon}{1+\varepsilon}, \frac{1+\varepsilon}{1-\varepsilon}\right].$$

By Taylor series of $1/(1-\varepsilon)$ at 0,

$$(1+\varepsilon)/(1-\varepsilon) = 1 + 2\varepsilon + 2\sum_{i=2}^{+\infty} \varepsilon^i = 1 + 2\varepsilon + \frac{2\varepsilon^2}{1-\varepsilon}.$$

When $\varepsilon \leqslant 1/3$, $(2\varepsilon^2)/(1-\varepsilon) \leqslant \varepsilon$. Hence $(1+\varepsilon)/(1-\varepsilon) \leqslant 1+3\varepsilon$.

On the other side, by Taylor series of $1/(1+\varepsilon)$ at 0,

$$(1-\varepsilon)/(1+\varepsilon) = 1 + \sum_{i=1}^{+\infty}(-\varepsilon)^i + \sum_{i=1}^{+\infty}(-\varepsilon)^i = 1 - 2\varepsilon + \varepsilon^2/(1+\varepsilon) \geqslant 1 - 3\varepsilon.$$

The result follows. □

Prior to presenting the proofs, we introduce an auxiliary tool that will be employed in its proof.

Lemma 31. *Let n be a positive integer. Let $r > 0$. For any $\mathbf{x}, \mathbf{c} \in \mathbb{R}^n$, we have $\rho_r(\mathbf{x})^2/\rho_r(\mathbf{x}+\mathbf{c}) = \rho_r(\mathbf{x}-\mathbf{c})/\rho_r(\sqrt{2}\mathbf{c})$.*

Proof. By definition of the function ρ_r, we have:

$$\begin{aligned}
&\rho_r(\mathbf{x})^2/\rho_r(\mathbf{x}+\mathbf{c}) \\
=&\frac{\exp(-2\pi\|\mathbf{x}\|^2/r^2)}{\exp(-\pi\|\mathbf{x}+\mathbf{c}\|^2/r^2)} = \exp(-\pi(2\|\mathbf{x}\|^2 - \|\mathbf{x}+\mathbf{c}\|^2)/r^2) \\
=&\exp(-\pi(\|\mathbf{x}\|^2 - 2\langle\mathbf{x},\mathbf{c}\rangle - \|\mathbf{c}\|^2)/r^2) = \exp(-\pi(\|\mathbf{x}\|^2 - 2\langle\mathbf{x},\mathbf{c}\rangle + \|\mathbf{c}\|^2 - 2\|\mathbf{c}\|^2)/r^2) \\
=&\frac{\exp(-\pi\|\mathbf{x}-\mathbf{c}\|^2/r^2)}{\exp(-\pi\|\sqrt{2}\mathbf{c}\|^2/r^2)} = \rho_r(\mathbf{x}-\mathbf{c})/\rho_r(\sqrt{2}\mathbf{c}).
\end{aligned}$$

The result follows. □

The following part is the proof of Lemma 12.

Proof. [of Lemma 12] We have:

$$\begin{aligned}
R(D_{\mathbb{Z}^n,r/G}\|D^{Sum,G}_{\mathbb{Z}^n,r}) &= \sum_{\mathbf{v}\in\mathbb{Z}^n}\frac{\Pr_{x\hookleftarrow D_{\mathbb{Z}^n,r/G}}(\mathbf{x}=\mathbf{v})^2}{\Pr_{\mathbf{x}'\hookleftarrow D^{Sum,G}_{\mathbb{Z}^n,r}}(\mathbf{x}'=\mathbf{v})}\\
&= \sum_{\mathbf{v}\in\mathbb{Z}^n}\frac{\left(\frac{\rho_{r/G}(\mathbf{v})}{\rho_{r/G}(\mathbb{Z}^n)}\right)^2}{\prod_{i=0}^{n-1}\left(\sum_{x_i\in\left((v_i-\frac{1}{2})G,\,(v_i+\frac{1}{2})G\right]\cap\mathbb{Z}}\rho_r(x_i)\right)/\rho_r(\mathbb{Z})}\\
&= \frac{\rho_r(\mathbb{Z}^n)}{\rho_{\frac{r}{G}}(\mathbb{Z}^n)^2}\sum_{\mathbf{v}\in\mathbb{Z}^n}\frac{\left(\rho_{r/G}(\mathbf{v})\right)^2}{\prod_{i=0}^{n-1}\left(\sum_{x_i\in\left((v_i-\frac{1}{2})G,\,(v_i+\frac{1}{2})G\right]\cap\mathbb{Z}}\rho_r(x_i)\right)}.
\end{aligned}$$

According to the Lemma 10 in this subsection of Supplementary Materials, it follows that

$$\begin{aligned}
&R(D_{\mathbb{Z}^n,r/G}\|D^{Sum,G}_{\mathbb{Z}^n,r})\\
\in& G^n\frac{[1-3\varepsilon,1+3\varepsilon]}{\rho_{r/G}(\mathbb{Z}^n)}\sum_{\mathbf{v}\in\mathbb{Z}^n}\frac{\left(\rho_{r/G}(\mathbf{v})\right)^2}{\prod_{i=0}^{n-1}\left(\sum_{x_i\in\left((v_i-\frac{1}{2})G,\,(v_i+\frac{1}{2})G\right]\cap\mathbb{Z}}\rho_r(x_i)\right)}.
\end{aligned}$$

Considering the summation in the above formula, we obtain:

$$\begin{aligned}
&\sum_{\mathbf{v}\in\mathbb{Z}^n}\frac{\left(\rho_{r/G}(\mathbf{v})\right)^2}{\prod_{i=0}^{n-1}\left(\sum_{x_i\in\left((v_i-\frac{1}{2})G,\,(v_i+\frac{1}{2})G\right]\cap\mathbb{Z}}\rho_r(x_i)\right)}\\
=&\sum_{\mathbf{v}\in\mathbb{Z}^n}\prod_{i=0}^{n-1}\frac{\left(\rho_{r/G}(v_i)\right)^2}{\left(\sum_{x_i\in\left((v_i-\frac{1}{2})G,\,(v_i+\frac{1}{2})G\right]\cap\mathbb{Z}}\rho_r(x_i)\right)}\\
=&\prod_{i=0}^{n-1}\sum_{v_i\in\mathbb{Z}}\frac{\left(\rho_{r/G}(v_i)\right)^2}{\left(\sum_{x_i\in\left((v_i-\frac{1}{2})G,\,(v_i+\frac{1}{2})G\right]\cap\mathbb{Z}}\rho_r(x_i)\right)}.
\end{aligned}$$

We analysis the summation in three cases. For $v_i = 0$, we have:

$$\frac{\left(\rho_{r/G}(v_i)\right)^2}{\left(\sum_{x_i\in((v_i-1/2)G,\,(v_i+1/2)G]\cap\mathbb{Z}}\rho_r(x_i)\right)}\leqslant\frac{1}{G\cdot\rho_r(G/2)}=\frac{1}{G\cdot\rho_{r/G}(1/2)};$$

for $v_i < 0$, we have:

$$\begin{aligned}
&\frac{\left(\rho_{r/G}(v_i)\right)^2}{\left(\sum_{x_i\in((v_i-1/2)G,\,(v_i+1/2)G]\cap\mathbb{Z}}\rho_r(x_i)\right)}\leqslant\frac{\left(\rho_{r/G}(v_i)\right)^2}{G\cdot\rho_r((v_i-1/2)\cdot G)}\\
=&\frac{\left(\rho_{r/G}(v_i)\right)^2}{G\cdot\rho_{r/G}(v_i-1/2)}=\frac{\rho_{r/G}(v_i+1/2)}{G\cdot\rho_{r/G}(1/\sqrt{2})},
\end{aligned}$$

where the first inequality follows from the monotonicity of ρ_r, and the last equality from Lemma 31 in this subsection of Supplementary Materials.

Similarly, for $v_i > 0$, we have:

$$\frac{\left(\rho_{r/G}(v_i)\right)^2}{\left(\sum_{x_i\in((v_i-1/2)G,\,(v_i+1/2)G]\cap\mathbb{Z}}\rho_r(x_i)\right)} \leqslant \frac{\left(\rho_{r/G}(v_i)\right)^2}{G\cdot\rho_r((v_i+1/2)\cdot G)}$$
$$=\frac{\left(\rho_{r/G}(v_i)\right)^2}{G\cdot\rho_{r/G}(v_i+1/2)} = \frac{\rho_{r/G}(v_i-1/2)}{G\cdot\rho_{r/G}(1/\sqrt{2})},$$

where the first inequality follows from the monotonicity of ρ_r, and the last equality from Lemma 31 in this subsection of Supplementary Materials.

Therefore, the Rényi divergence is bounded as follows.

$$\begin{aligned}
&R(D_{\mathbb{Z}^n,\frac{r}{G}}\|D^{Sum,G}_{\mathbb{Z}^n,r})\\
\leqslant&\frac{1+3\varepsilon}{\rho_{\frac{r}{G}}(\mathbb{Z}^n)}\prod_{i=0}^{n-1}\left(\frac{1}{\rho_{\frac{r}{G}}(1/2)}+\sum_{v_i<0}\frac{\rho_{\frac{r}{G}}(v_i)^2}{\rho_{\frac{r}{G}}(v_i-1/2)}+\sum_{v_i>0}\frac{\rho_{\frac{r}{G}}(v_i)^2}{\rho_{\frac{r}{G}}(v_i+1/2)}\right)\\
=&\frac{1+3\varepsilon}{\rho_{\frac{r}{G}}(\mathbb{Z}^n)}\prod_{i=0}^{n-1}\left(\frac{1}{\rho_{\frac{r}{G}}(1/2)}+\sum_{v_i<0}\frac{\rho_{\frac{r}{G}}(v_i+1/2)}{\rho_{\frac{r}{G}}(1/\sqrt{2})}+\sum_{v_i>0}\frac{\rho_{\frac{r}{G}}(v_i-1/2)}{\rho_{\frac{r}{G}}(1/\sqrt{2})}\right)\\
=&\frac{1+3\varepsilon}{\rho_{\frac{r}{G}}(\mathbb{Z}^n)\rho_{\frac{r}{G}}\left(1/\sqrt{2}\right)^n}\prod_{i=0}^{n-1}\Big(\frac{\rho_{\frac{r}{G}}\left(1/\sqrt{2}\right)}{\rho_{\frac{r}{G}}(1/2)}+\sum_{v_i<0}\rho_{\frac{r}{G}}(v_i+1/2)+\sum_{v_i>0}\rho_{\frac{r}{G}}(v_i-1/2)\Big).
\end{aligned}\tag{30}$$

Due to $\rho_{r/G}(1/\sqrt{2})^n = \rho_{r/G}\left(\sqrt{n}/\sqrt{2}\right)$ and

$$\frac{\rho_{\frac{r}{G}}(1/\sqrt{2})}{\rho_{\frac{r}{G}}(1/2)} = \frac{\exp\left(-\pi\left(1/\sqrt{2}\right)^2/(r/G)^2\right)}{\exp\left(-\pi\left(1/2\right)^2/(r/G)^2\right)} = \exp\left(-\pi\left(1/2\right)^2/(r/G)^2\right) = \rho_{\frac{r}{G}}(1/2),$$

the last two lines in the formula (30) is equal to

$$\frac{1+3\varepsilon}{\rho_{\frac{r}{G}}(\mathbb{Z}^n)\rho_{\frac{r}{G}}\left(\sqrt{n}/\sqrt{2}\right)}\prod_{i=0}^{n-1}\left(\rho_{\frac{r}{G}}(1/2)+\sum_{v_i<0}\rho_{\frac{r}{G}}(v_i+1/2)+\sum_{v_i>0}\rho_{\frac{r}{G}}(v_i-1/2)\right).$$

Then we consider the summation

$$\begin{aligned}
&\prod_{i\in[n]}\left(\rho_{\frac{r}{G}}(1/2)+\sum_{v_i<0}\rho_{\frac{r}{G}}(v_i+1/2)+\sum_{v_i>0}\rho_{\frac{r}{G}}(v_i-1/2)\right)\leqslant\left(1+\rho_{\frac{r}{G}}(\mathbb{Z}+1/2)\right)^n\\
\leqslant&(1+(1+\varepsilon)\cdot r/G)^n=(r/G)^n\cdot\left(1+\frac{\varepsilon\cdot(r/G)+1}{r/G}\right)^{\frac{r/G}{\varepsilon\cdot(r/G)+1}\cdot\frac{\varepsilon\cdot(r/G)+1}{r/G}\cdot n}\\
\leqslant&\left(\frac{r}{G}\right)^n\exp\left(\frac{2Gn}{r}\right).
\end{aligned}$$

Therefore, the Rényi Divergence can be bounded as follows:

$$\begin{aligned}
R(D_{\mathbb{Z}^n,\frac{r}{G}}\|D^{Sum,G}_{\mathbb{Z}^n,r})\leqslant&\frac{(1+3\varepsilon)\cdot(r/G)^n\cdot\exp((2Gn)/r)}{(1-\varepsilon)(r/G)^n\rho_{\frac{r}{G}}\left(\sqrt{n}/\sqrt{2}\right)}\\
\leqslant&(1+3\varepsilon)^2\exp\left(\frac{2Gn}{r}+\frac{\pi nG^2}{2r^2}\right)\leqslant(1+3\varepsilon)^2\exp\left(\frac{5Gn}{2r}\right).
\end{aligned}$$

The result follows directly. □

The following part is the proof of Lemma 13.

Proof. [of Lemma 13.] $\mathcal{L}(\mathbf{B})$ is a full rank lattice over $\mathbb{R}^n$. We denote the distribution $D_{\mathbb{Z}^n,r,\mathbf{c}}$ mod $\mathcal{L}(\mathbf{B})$ as Y. For any $\mathbf{x} \in \mathbb{Z}^n \bigcap \mathcal{P}(\mathbf{B})$,

$$Y(\mathbf{x}) = \frac{1}{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \sum_{\mathbf{y}\in\mathcal{L}(\mathbf{B})} \rho_{r,\mathbf{c}}(\mathbf{x}+\mathbf{y}) = \frac{\rho_{r,\mathbf{c}-\mathbf{x}}(\mathcal{L}(\mathbf{B}))}{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)}.$$

Applying Fourier transform, we have:

$$Y(\mathbf{x}) = \frac{\mathsf{det}(\mathcal{L}(\mathbf{B}^*)) \cdot r^n}{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \sum\nolimits_{\mathbf{w}\in\mathcal{L}(\mathbf{B}^*)} e^{2\pi\sqrt{-1}\langle \mathbf{x}-\mathbf{c},\mathbf{w}\rangle} \rho_{\frac{1}{r}}(\mathbf{w}).$$

Therefore, the statistical distance can be computed as:

$$\begin{aligned}
&\Delta(Y,U) = \frac{1}{2}\sum\nolimits_{x\in\mathcal{P}(\mathbf{B})\bigcap\mathbb{Z}^n} |Y(\mathbf{x}) - U(\mathbf{x})| \\
=&\frac{1}{2} \sum_{x\in\mathcal{P}(\mathbf{B})\bigcap\mathbb{Z}^n} \left| \frac{\mathsf{det}(\mathcal{L}(\mathbf{B}^*)) \cdot r^n}{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \sum_{\mathbf{w}\in\mathcal{L}(\mathbf{B}^*)} e^{2\pi\sqrt{-1}\langle \mathbf{x}-\mathbf{c},\mathbf{w}\rangle} \rho_{\frac{1}{r}}(\mathbf{w}) - \frac{1}{\mathsf{det}(\mathcal{L}(\mathbf{B}))} \right| \\
\leqslant&\frac{r^n}{2\mathsf{det}(\mathbf{B})\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \left(\sum_{\mathbf{x}\in\mathcal{P}(\mathbf{B})\bigcap\mathbb{Z}^n} \left| \sum_{w\in\mathcal{L}(\mathbf{B}^*)\setminus\{\mathbf{0}\}} e^{2\pi\sqrt{-1}\langle \mathbf{x}-\mathbf{c},\mathbf{w}\rangle} \rho_{\frac{1}{r}}(\mathbf{w}) \right| + \left| 1 - \frac{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)}{r^n} \right| \right) \\
\leqslant&\frac{r^n}{2\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \left(\max_{x\in\mathcal{P}(\mathbf{B})\bigcap\mathbb{Z}^n} \left| \sum_{w\in\mathcal{L}(\mathbf{B}^*)\setminus\{\mathbf{0}\}} e^{2\pi\sqrt{-1}\langle \mathbf{x}-\mathbf{c},\mathbf{w}\rangle} \rho_{\frac{1}{r}}(\mathbf{w}) \right| + \left| 1 - \frac{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)}{r^n} \right| \right) \\
\leqslant&\frac{r^n}{2\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \left(\rho_{\frac{1}{r}}\left(\mathcal{L}(\mathbf{B}^*)\setminus\{\mathbf{0}\}\right) + \left| 1 - \frac{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)}{r^n} \right| \right) \\
=&\frac{r^n}{2\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \left(\rho_{\frac{1}{r}}\left(\mathcal{L}(\mathbf{B}^*)\right) - 1 + \left| 1 - \frac{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)}{r^n} \right| \right) \\
=&\frac{r^n}{2\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} \left(\rho_{\frac{1}{r}}\left(\mathcal{L}(\mathbf{B}^*)\right) - 1 \right) + \frac{1}{2} \left| \frac{r^n}{\rho_{r,\mathbf{c}}(\mathbb{Z}^n)} - 1 \right|
\end{aligned}$$

The result follows directly. □

The following part is the proof of Lemma 14.

Proof. [of Lemma 14.] By the definition, we have:

$$R(G\cdot D_{\mathbb{Z}^n,r}^{Sum,G} + U(\mathbb{Z}_G^n) \| D_{\mathbb{Z}^n,r}) = \sum_{\substack{\mathbf{x}'\in\mathbb{Z}^n \\ \mathbf{x}''\in\mathbb{Z}_G^n}} \frac{\Pr\limits_{\substack{\mathbf{x}_2^{(1)}\hookleftarrow D_{\mathbb{Z}^n,r}^{Sum,G} \\ \mathbf{x}_2^{(2)}\hookleftarrow U(\mathbb{Z}_G^n)}} \left(\mathbf{x}_2^{(1)} = \mathbf{x}', \mathbf{x}_2^{(2)} = \mathbf{x}''\right)^2}{\Pr\limits_{x_1\hookleftarrow D_{\mathbb{Z}^n,r}} \left(\left\lfloor \frac{\mathbf{x}_1}{G} \right\rceil = \mathbf{x}', \mathbf{x}_1 \bmod G = \mathbf{x}''\right)}.$$

Let $\mathbf{x} = G\cdot\mathbf{x}' + \mathbf{x}'' \in \mathbb{Z}^n$. Then the formula can be rewritten as follows:

$$R(G\cdot D_{\mathbb{Z}^n,r}^{Sum,G} + U(\mathbb{Z}_G^n) \| D_{\mathbb{Z}^n,r}) = \sum\nolimits_{\mathbf{x}\in\mathbb{Z}^n} \frac{(D_{\mathbb{Z}^n,r}^{Sum,G}(\lfloor \frac{\mathbf{x}}{G} \rceil) \cdot \frac{1}{G^n})^2}{D_{\mathbb{Z}^n,r}(\mathbf{x})}.$$

By definition, the formula expands as follows:

$$\begin{aligned}
&R(G\cdot D^{Sum,G}_{\mathbb{Z}^n,r}+U(\mathbb{Z}_G^n)\|D_{\mathbb{Z}^n,r})\\
=&\frac{1}{\rho_r(\mathbb{Z}^n)}\sum\nolimits_{\mathbf{x}\in\mathbb{Z}^n}\frac{\prod_{i=0}^{n-1}\left(\sum\limits_{(\lfloor\frac{x_i}{G}\rceil-\frac{1}{2})G<v_i\leqslant(\lfloor\frac{x_i}{G}\rceil+\frac{1}{2})G}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{G^{2n}\cdot\exp\left(-\frac{\pi}{r^2}\|\mathbf{x}\|^2\right)}\\
=&\frac{1}{G^{2n}\rho_r(\mathbb{Z}^n)}\prod\nolimits_{i=0}^{n-1}\sum\nolimits_{x_i\in\mathbb{Z}}\frac{\left(\sum\limits_{(\lfloor\frac{x_i}{G}\rceil-\frac{1}{2})G<v_i\leqslant(\lfloor\frac{x_i}{G}\rceil+\frac{1}{2})G}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}.
\end{aligned}$$

Considering the summation over x_i in the above formula, we obtain:

$$\begin{aligned}
&\sum\nolimits_{x_i\in\mathbb{Z}}\frac{\left(\sum\limits_{(\lfloor x_i/G\rceil-1/2)G<v_i\leqslant(\lfloor x_i/G\rceil+1/2)G}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\\
=&\sum\nolimits_{\lfloor x_i/G\rceil=0}\frac{\left(\sum\limits_{-G/2<v_i\leqslant G/2}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\\
&+\sum\nolimits_{j<0}\sum\nolimits_{\lfloor x_i/G\rceil=j}\frac{\left(\sum\limits_{(\lfloor x_i/G\rceil-1/2)G<v_i\leqslant(\lfloor x_i/G\rceil+1/2)G}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\\
&+\sum\nolimits_{j>0}\sum\nolimits_{\lfloor x_i/G\rceil=j}\frac{\left(\sum\limits_{(\lfloor x_i/G\rceil-1/2)G<v_i\leqslant(\lfloor x_i/G\rceil+1/2)G}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}.
\end{aligned}$$

By monotonicity, we have the following upper bounds for the three cases, $j=0$, $j<0$ and $j>0$. When $j=0$, we have:

$$\sum\nolimits_{\lfloor\frac{x_i}{G}\rceil=0}\frac{\left(\sum\limits_{-G/2<v_i\leqslant G/2}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\leqslant\sum\nolimits_{\lfloor\frac{x_i}{G}\rceil=0}\frac{G^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\leqslant\frac{G^3}{\exp\left(-\frac{\pi G^2}{4r^2}\right)};$$

when $j<0$, we obtain:

$$\begin{aligned}
&\sum\nolimits_{j<0}\sum\nolimits_{\lfloor\frac{x_i}{G}\rceil=j}\frac{\left(\sum\limits_{(j-1/2)G<v_i\leqslant(j+1/2)G}\exp\left(-\frac{\pi}{r^2}v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\\
\leqslant&\sum\nolimits_{j<0}\sum\nolimits_{\lfloor\frac{x_i}{G}\rceil=j}\frac{G^2\cdot\exp\left(-\frac{2\pi G^2}{r^2}(j+1/2)^2\right)}{\exp\left(-\frac{\pi}{r^2}x_i^2\right)}\leqslant\sum_{j<0}\frac{G^3\cdot\exp\left(-\frac{2\pi G^2}{r^2}(j+1/2)^2\right)}{\exp\left(-\frac{\pi G^2}{r^2}(j-1/2)^2\right)};
\end{aligned}$$

and when $j > 0$, we obtain:

$$\sum_{j>0}\sum_{\lfloor \frac{x_i}{G} \rfloor = j} \frac{\left(\sum\limits_{(j-1/2)G < v_i \leqslant (j+1/2)G} \exp\left(-\frac{\pi}{r^2} v_i^2\right)\right)^2}{\exp\left(-\frac{\pi}{r^2} x_i^2\right)}$$
$$\leqslant \sum_{j>0}\sum_{\lfloor \frac{x_i}{G} \rfloor = j} \frac{G^2 \cdot \exp\left(-\frac{2\pi G^2}{r^2}\left(j-1/2\right)^2\right)}{\exp\left(-\frac{\pi}{r^2} x_i^2\right)} \leqslant \sum_{j<0} \frac{G^3 \cdot \exp\left(-\frac{2\pi G^2}{r^2}\left(j-1/2\right)^2\right)}{\exp\left(-\frac{\pi G^2}{r^2}\left(j+1/2\right)^2\right)}.$$

Therefore, the Rényi divergence admits the following upper bound:

$$R(G \cdot D^{Sum,G}_{\mathbb{Z}^n,r} + U(\mathbb{Z}^n_G) \| D_{\mathbb{Z}^n,r}) \leqslant \frac{G^{3n}}{G^{2n}\rho_r(\mathbb{Z}^n)} \prod_{i=0}^{n-1} \left(\frac{1}{\exp\left(-\frac{\pi G^2}{4r^2}\right)} \right.$$
$$\left. + \sum_{j<0} \frac{\exp\left(-\frac{2\pi G^2}{r^2}\left(j+1/2\right)^2\right)}{\exp\left(-\frac{\pi G^2}{r^2}\left(j-1/2\right)^2\right)} + \sum_{j>0} \frac{\exp\left(-\frac{2\pi G^2}{r^2}\left(j-1/2\right)^2\right)}{\exp\left(-\frac{\pi G^2}{r^2}\left(j+1/2\right)^2\right)} \right).$$

Simplifying the above formula using Lemma 31 in this subsection yields:

$$R(G \cdot D^{Sum,G}_{\mathbb{Z}^n,r} + U(\mathbb{Z}^n_G) \| D_{\mathbb{Z}^n,r}) \leqslant \frac{G^n}{\rho_r(\mathbb{Z}^n)} \prod_{i=0}^{n-1} \left(\exp\left(\frac{\pi G^2}{4r^2}\right) \right.$$
$$\left. + \sum_{j<0} \exp\left(-\frac{\pi G^2}{r^2}\left(j+3/2\right)^2 + \frac{2\pi G^2}{r^2}\right) + \sum_{j>0} \exp\left(-\frac{\pi G^2}{r^2}\left(j-3/2\right)^2 + \frac{2\pi G^2}{r^2}\right) \right)$$
$$\leqslant \frac{G^n}{\rho_r(\mathbb{Z}^n)} \prod_{i=0}^{n-1} \left(\exp\left(\frac{\pi G^2}{4r^2}\right) + \sum_{j<0} \exp\left(-\frac{\pi G^2}{r^2}\left(j+3/2\right)^2 + \frac{5\pi G^2}{2r^2}\right) \right.$$
$$\left. + \sum_{j>0} \exp\left(-\frac{\pi G^2}{r^2}\left(j-3/2\right)^2 + \frac{5\pi G^2}{2r^2}\right) \right)$$
$$= \frac{G^n}{\rho_r(\mathbb{Z}^n)} \exp\left(\frac{5\pi n G^2}{2r^2}\right) \prod_{i=0}^{n-1} \left(\exp\left(-\frac{9\pi G^2}{4r^2}\right) \right.$$
$$\left. + \sum_{j<0} \exp\left(-\frac{\pi G^2}{r^2}\left(j+3/2\right)^2\right) + \sum_{j>0} \exp\left(-\frac{\pi G^2}{r^2}\left(j-3/2\right)^2\right) \right).$$

We consider the following summation:

$$\prod_{i=0}^{n-1} \left(\exp\left(-\frac{9\pi G^2}{4r^2}\right) + \sum_{j<0} \exp\left(-\frac{\pi G^2}{r^2}\left(j+3/2\right)^2\right) + \sum_{j>0} \exp\left(-\frac{\pi G^2}{r^2}\left(j-3/2\right)^2\right) \right)$$
$$\leqslant (3 + \rho_{\frac{r}{G}}(\mathbb{Z}+1/2))^n \leqslant (\frac{r}{G})^n \cdot \left(\frac{3+\varepsilon\cdot\frac{r}{G}}{r/G}+1\right)^{\frac{r/G}{3+\varepsilon\cdot(r/G)}\cdot\frac{3+\varepsilon\cdot(r/G)}{r/G}\cdot n} \leqslant (\frac{r}{G})^n \cdot \exp\left(\frac{4nG}{r}\right).$$

Therefore, the Rényi Divergence can be bounded as follows:

$$R(G \cdot D^{Sum,G}_{\mathbb{Z}^n,r} + U(\mathbb{Z}^n_G) \| D_{\mathbb{Z}^n,r}) \leqslant (1+3\varepsilon) \cdot \frac{G^n (r/G)^n \cdot \exp\left((4nG)/r\right)}{\rho_r(\mathbb{Z}^n)} \exp\left(\frac{5\pi n G^2}{2r^2}\right)$$
$$\leqslant (1+3\varepsilon) \cdot \frac{G^n (r/G)^n}{r^n \cdot (1-\varepsilon)} \exp\left(\frac{5\pi n G^2}{2r^2} + \frac{4nG}{r}\right) \leqslant (1+3\varepsilon)^2 \exp\left(\frac{9nG}{2r}\right).$$

Furthermore, if $\frac{r}{G} \geqslant \omega(n)$, this Rényi divergence has a polynomial-sized bound. □

In order to prove Lemma 15, we define $D^{j-}_{\mathbb{Z}^n,r,B}$ for $j \in [n+1]$ as the distribution over $\mathbb{Z}^n$ where, for $\mathbf{x} \in \mathbb{Z}^n$, the first j coordinates x_i (for $0 \leqslant i < j$) are sampled from $D_{\mathbb{Z},r,B}$, and the remaining coordinates x_i (for $i \geqslant j$) are sampled from $D_{\mathbb{Z},r}$. In particular, we have $D^{0-}_{\mathbb{Z}^n,r,B} = D_{\mathbb{Z}^n,r}$ and $D^{n-}_{\mathbb{Z}^n,r,B} = D_{\mathbb{Z}^n,r,B}$. We also denote the support set by $\mathcal{S}^{j-}_B := \mathsf{supp}(D^{j-}_{\mathbb{Z}^n,r,B})$. Using this notation, we now present the proof of Lemma 15.

Proof. First, we have:

$$\Delta(D_{\mathbb{Z}^n,r,B}, D_{\mathbb{Z}^n,r}) \leqslant \sum_{j\in[n]} \Delta(D^{j-}_{\mathbb{Z}^n,r,B}, D^{(j+1)-}_{\mathbb{Z}^n,r,B}).$$

Then for each $j \in [n]$, we have:

$$\begin{aligned}
&\Delta(D^{j-}_{\mathbb{Z}^n,r,B}, D^{(j+1)-}_{\mathbb{Z}^n,r,B}) \\
=&\frac{1}{2}\sum_{\mathbf{x}\in\mathcal{S}^{(j+1)-}_B}\left|\frac{\rho_r(\mathbf{x})}{\rho_r(\mathbb{Z}\cap[-B,B])^j\rho_r(\mathbb{Z})^{n-j}} - \frac{\rho_r(\mathbf{x})}{\rho_r(\mathbb{Z}\cap[-B,B])^{j+1}\rho_r(\mathbb{Z})^{n-j-1}}\right| \\
&+\frac{1}{2}\sum_{\mathbf{x}\in\mathcal{S}^{j-}_B\setminus\mathcal{S}^{(j+1)-}_B}\left|\frac{\rho_r(\mathbf{x})}{\rho_r(\mathbb{Z}\cap[-B,B])^{j+1}\rho_r(\mathbb{Z})^{n-j-1}}\right| \\
=&\frac{1}{2}\left(\sum_{\mathbf{x}\in\mathcal{S}^{(j+1)-}_B}\rho_r(\mathbf{x})\right)\cdot\frac{\rho_r(\mathbb{Z}\setminus[-B,B])}{\rho_r(\mathbb{Z}\cap[-B,B])^{j+1}\rho_r(\mathbb{Z})^{n-j}} \\
&+\frac{1}{2}\frac{\rho_r(\mathbb{Z}\setminus[-B,B])\cdot\rho_r(\mathbb{Z}\cap[-B,B])^j\rho_r(\mathbb{Z})^{n-j-1}}{\rho_r(\mathbb{Z}\cap[-B,B])^{j+1}\rho_r(\mathbb{Z})^{n-j-1}} \\
\leqslant&2^{-\Omega(B^2/r^2)}/2 + \frac{2^{-\Omega(B^2/r^2)}}{2(1-2^{-\Omega(B^2/r^2)})} = 2^{-\Omega(B^2/r^2)} \leqslant 2^{-\Omega(\kappa)}.
\end{aligned}$$

Therefore, the result follows directly. □

B.2 Transformations between LWE with Continuous Gaussian Distribution and Discrete Gaussian Distribution

In this subsection, we recall the equivalence between LWE with a continuous Gaussian distribution and LWE with a discrete Gaussian distribution.

Lemma 32 ([Reg09, Claim 3.9]). *Let Λ be a lattice, let $\mathbf{u} \in \mathbb{R}^n$ be any vector, let $r, s > 0$ be two real numbers, and let t denote $\sqrt{r^2+s^2}$. Assume that $rs/t \geqslant \eta_\varepsilon(\Lambda)$ for some $\varepsilon < \frac{1}{2}$. Consider the continuous distribution Y on $\mathbb{R}^n$ obtained by sampling from $D_{\Lambda+\mathbf{u},r}$ and then adding a noise vector taken from $\mathcal{N}_s$. Then the statistical distance between Y and $\mathcal{N}_t$ is at most 4ε.*

This yields the following canonical corollary with respect to vector-form errors.

Corollary 2. *For the lattice $\mathbb{Z}^n$, let Σ a positive definite matrix which can be decomposed as $\Sigma = \mathbf{U}^\top \mathbf{D}_\Sigma \mathbf{U}$, where $\mathbf{D}_\Sigma$ is the diagonal matrix $diag(\lambda_i^2)$ and let Σ' be the positive definite matrix such that $\Sigma' = \mathbf{U}^\top \mathbf{D}'_{\Sigma'} \mathbf{U}$, where $\mathbf{D}'_{\Sigma'}$ is the diagonal matrix $diag(\lambda_i'^2)$ satisfying $\frac{\lambda'_i \lambda_i}{\lambda_i^2 + \lambda_i'^2} \geqslant \eta_\varepsilon(\mathbf{U}_i \mathbb{Z})$ for $i \in [n]$ and some $\varepsilon \leqslant \frac{1}{2^n}$, where $\mathbf{U}_i$ is the i-th column of $\mathbf{U}$. Then the statistical distance between $D_{\mathbb{Z}^n, \sqrt{\Sigma}} + \mathcal{N}_{\sqrt{\Sigma'}}$ and $\mathcal{N}_{\sqrt{\Sigma + \Sigma'}}$ is at most $\frac{4n}{2^n}$.*

Based on Lemma 32, it is clear that, given an LWE instance of form $(\mathbf{A}, \mathbf{b})$ with discrete Gaussian error vector $\mathbf{e}$, adding to $\mathbf{b}$ an error vector $\mathbf{e}'$ selected from continuous Gaussian distribution with an appropriate parameter yields a new LWE instance $(\mathbf{A}, \mathbf{b} + \mathbf{e}')$ with continuous Gaussian error $\mathbf{e} + \mathbf{e}'$. Building on Corollary 2, we can have a same reduction for $\mathsf{P\text{-}MLWE}$. To better illustrate the loss incurred in the application of Lemma 32, consider the setting where the parameter $r = \omega(\log n)$. By choosing $s = r$, we obtain a constant multiplicative loss factor of $\sqrt{2}$ (e.g., $t = \sqrt{2}s$), while still ensuring that the statistical distance $\epsilon = 2^{-\omega(\log n)}$ remains negligible.

For the reduction of the reverse direction, we recall the following lemma.

Lemma 33 ([Pei10, Theorem 3.1]). *Let $\Sigma_1, \Sigma_2 > 0$ be two $n \times n$ positive definite matrices, with $\Sigma = \Sigma_1 + \Sigma_2 > 0$ and $\Sigma_3^{-1} = \Sigma_1^{-1} + \Sigma_2^{-1} > 0$. Let Λ_1, Λ_2 be lattices satisfying $\lambda^{max}_{\sqrt{\Sigma_1}} \geqslant \eta_\varepsilon(\Lambda_1)$ and $\lambda^{max}_{\sqrt{\Sigma_3}} \geqslant \eta_\varepsilon(\Lambda_2)$ for some $\varepsilon \leqslant \frac{1}{2}$. Let $\mathbf{v}_1, \mathbf{v}_2 \in \mathbb{R}^n$ be arbitrary. Consider the following probabilistic experiment: Choose $\mathbf{x}_2 \hookleftarrow D_{\Lambda_2 + \mathbf{v}_2, \sqrt{\Sigma_2}}$, then choose $\mathbf{x}_1 \hookleftarrow \mathbf{x}_2 + D_{\Lambda_1 + \mathbf{v}_1 - \mathbf{x}_2, \sqrt{\Sigma_1}}$. The marginal distribution of $\mathbf{x}_1$ is within statistical distance 8ε of $D_{\Lambda_1 + \mathbf{v}_1, \sqrt{\Sigma}}$.*

Consider the following probabilistic experiment: Choose $\mathbf{x}_2 \hookleftarrow \mathcal{N}_{\sqrt{\Sigma_2}}$, then choose $\mathbf{x}_1 \hookleftarrow D_{\Lambda_1 + \mathbf{v}_1 - \mathbf{x}_2, \sqrt{\Sigma_1}}$. The marginal distribution of $\mathbf{x}_1$ is within statistical distance 2ε of $D_{\Lambda_1 + \mathbf{v}_1, \sqrt{\Sigma}}$.

Therefore, given an LWE instance with continuous Gaussian error vector $(\mathbf{A}, \mathbf{b} = \mathbf{As} + \mathbf{e})$, sample $\mathbf{e}'$ from $D_{\mathbb{Z}^m - (\mathbf{As} + \mathbf{e}), \sqrt{\Sigma'}} = D_{\mathbb{Z}^m - \mathbf{e}, \sqrt{\Sigma'}}$ and add it to $\mathbf{b}$, we have $\mathbf{b}' = \mathbf{As} + \mathbf{e} + \mathbf{e}'$ with $\mathbf{e} + \mathbf{e}' \approx_{8\varepsilon} D_{\mathbb{Z}^m, \sqrt{\Sigma'}}$ according to Lemma 33.

B.3 Transformations between MLWE and P-MLWE

To set the stage, we introduce the concept of an order in K and its conductor.

Definition 25 (Order in K). *An order in $\mathbf{K}$ is a number ring $\mathcal{O}$ which is a finite index subring of $\mathcal{O}_K$. In other words, $[\mathcal{O}_K : \mathcal{O}]$ is finite.*

In particular, the number ring $\mathbb{Z}[x]/f(x)$ is also an order of $\mathcal{O}_K$.

Definition 26 (Conductor of an order $\mathcal{O}$). *The conductor of an order $\mathcal{O}$ is defined as the set $\mathcal{C}_\mathcal{O} = \{x \in K : x\mathcal{O}_K \subseteq \mathcal{O}\}$. It is contained in the order $\mathcal{O}$ and it is both an $\mathcal{O}_K$-ideal and an $\mathcal{O}$-ideal.*

Then we introduce an important lemma about conductor.

Lemma 34 ([RSW18, Lemma 2.2]). *Let $\mathcal{O}$ be an order in K and $\mathcal{I}$ and $\mathcal{I}$ an $\mathcal{O}_K$-ideal coprime to the conductor $\mathcal{C}_\mathcal{O}$. Then the inclusions $\mathcal{C}_\mathcal{O} \subset \mathcal{O}$ and $\mathcal{C}_\mathcal{O} \subset \mathcal{O}_K$ induce isomorphisms $\mathcal{C}_\mathcal{O}/\mathcal{I} \cap \mathcal{C}_\mathcal{O} \simeq \mathcal{O}/\mathcal{O} \cap \mathcal{I}$ and $\mathcal{C}_\mathcal{O}/\mathcal{I} \cap \mathcal{C}_\mathcal{O} \simeq \mathcal{O}_K/\mathcal{I}$.*

Lemma 35 ([Con24, Corollary 3.10]). *Let $\mathcal{O}$ be an order of K and $\beta \in \mathcal{O}$ such that $\beta\mathcal{O}_K$ is comprime to $\mathcal{C}_\mathcal{O}$. Then $\beta\mathcal{O}_K \cap \mathcal{O} = \beta\mathcal{O}$.*

The following lemma provides a method for constructing an isomorphism from $\mathcal{O}_K/q\mathcal{O}_K$ to $\mathbb{Z}_q[x]/f(x)$.

Lemma 36 ([LPR10, Lemma 2.14]). *Let $\mathcal{I}$ and $\mathcal{J}$ be two $\mathcal{O}_K$-ideals. Let $t \in \mathcal{I}$ such that the ideals $t \cdot \mathcal{I}^{-1}$ and $\mathcal{J}$ are coprime and let $\mathcal{I}'$ be any fractional $\mathcal{O}_K$-ideal. Then the function $\theta_t : \mathcal{I}' \to \mathcal{I}'$ defined as $\theta_t(a) = t \cdot a$ induces an $\mathcal{O}_K$-module isomorphism from $\mathcal{I}'/\mathcal{J}\mathcal{I}'$ to $\mathcal{I}\mathcal{I}'/\mathcal{I}\mathcal{J}\mathcal{I}'$.*

Finally, we restate an observation in [RSW18], which can help us understand the error distribution easily.

Lemma 37 ([RSW18, Observation at p.12, restated]). *Let $t \in K_\mathbb{R}$. Let Σ be a positive definite $n \times n$ matrix. Suppose e follows the distribution $\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma}}$, then $t \cdot e$ follows the distribution $\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma'}}$, where $\Sigma' = \mathrm{diag}(|\sigma_i(t)|) \cdot \Sigma \cdot \mathrm{diag}(|\sigma_i(t)|)$.*

Proof. For any $a \in K_\mathbb{R}$, we have $\sigma_\mathbb{H}(tx) = U^\dagger_\mathbb{H} \cdot \sigma(tx) = U^\dagger_\mathbb{H} \cdot \sigma(t) \cdot \sigma(a) = U^\dagger_\mathbb{H}\sigma(t)U_\mathbb{H} \cdot \sigma_\mathbb{H}(a)$. Since $U^\dagger_\mathbb{H}\sigma(t)U_\mathbb{H} = \mathrm{diag}(|\sigma_i(t)|)$, which is a diagonal matrix with diagonal entries $|\sigma_i(t)|$, $i \in [n]$. The result follows. □

In order to reduce MLWE to P-MLWE, we need to recall the following lemmata, which show that there exists an efficient algorithm to sample some particular t with small ℓ_2 norm coefficient vector for this transformation.

Lemma 38 ([RSW18, Corollary 3.2]). *Let $\mathcal{I}$ be an integral $\mathcal{O}_K$-ideal with extension index d. Let $q \geqslant \max(2d, 2^{16} \cdot \Delta_K^{\frac{8}{d}})$ be a prime rational integer and $\mathfrak{p}_k$ a prime factor of $q\mathcal{O}_K$ with largest norm. We define:*

$$r_t = \begin{cases} q^{\frac{1}{2}} \cdot (\mathcal{N}(\mathcal{I})\Delta_K)^{\frac{1}{d}} & \text{if } \mathcal{N}(\mathfrak{p}_k) \geqslant q^{\frac{5d}{8}}, \\ q^{\frac{3}{4}} \cdot (\mathcal{N}(\mathcal{I})\Delta_K)^{\frac{1}{d}} & \text{else.} \end{cases}$$

Then, for sufficiently large d, we have:

$$\Pr_{t \hookleftarrow D_{\mathcal{I}, r_t}} (t\mathcal{I}^{-1} + q\mathcal{O}_K = \mathcal{O}_K) \geqslant \frac{1}{2}.$$

Lemma 39. *Assume all parameters inherits from the Lemma 38, input a positive integer m, run the following algorithm 1, then with probability at least $1 - \left(\frac{1}{2}\right)^m$, the algorithm outputs $t \in \mathcal{I}$ such that $t\mathcal{I}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$.*

Algorithm 1 Sampling an invertible element modulo q

Input: $m > 0$
while m>0 **do**
  $t \hookleftarrow D^{\mathbb{H}}_{\mathcal{I},r_t}$
  if $t\mathcal{I}^{-1} + q\mathcal{O}_K = \mathcal{O}_K$ **then**
    Output: t.
    Abort.
  end if
  $m--$
end while
Abort.

Building upon the above lemma, by choosing a sufficiently large $m = O(\kappa)$, where κ denotes the security parameter, we can obtain the desired t except with negligible probability. Then, as shown in [RSW18], it is sufficient to perform the transformation with such a t.

Lemma 40 ([RSW18, Theorem 4.2]). *Assume that $q\mathcal{O}_K + \mathcal{C}_{\mathbb{Z}[x]/f} = \mathcal{O}_K$. Let Σ be a full-rank positive definite $d \times d$ matrix and $s \in \mathcal{O}_K/q\mathcal{O}_K$. Let $t \in \mathcal{C}_{\mathbb{Z}[x]/f}$ such that $t\mathcal{C}^{-1}_{\mathbb{Z}[x]/f} + q\mathcal{O}_K = \mathcal{O}_K$. Then the map $(a, b) \mapsto (t \cdot a, t^2 \cdot b)$ transforms $\mathsf{RLWE}_{q,s,\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma}},f}$ to $\mathsf{PLWE}_{q,ts,\mathcal{N}_{\sqrt{\Sigma'}},f}$, where $\Sigma' = \mathbf{V}_K^\top(\mathbf{U}_{\mathbb{H}}^\top)^{-1}\operatorname{diag}(|\sigma_i(t)|^2) \cdot \Sigma \cdot \operatorname{diag}(|\sigma_i(t)|^2)\mathbf{U}_{\mathbb{H}}^{-1}\mathbf{V}_K$. Furthermore, the natural inclusion $\mathbb{Z}[x]/(f) \to \mathcal{O}_K$ canonically induces a map that transforms $\mathsf{PLWE}_{q,\mathbf{s},\mathcal{N}_{\sqrt{\Sigma}},f}$ to $\mathsf{RLWE}_{q,\mathbf{s},\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma'}},f}$, where $\overline{\Sigma}' = \mathbf{U}_{\mathbb{H}}^\top(\mathbf{V}_K^\top)^{-1}\overline{\Sigma}\mathbf{V}_K^{-1}\mathbf{U}_{\mathbb{H}}$.*

The transformation in Lemma 40 can maintain relatively short errors due to the discrete Gaussian sampling in Lemma 38. Beyond this, for the matrix space, the map

$$\begin{aligned}\theta_t : (\mathcal{O}_K/q\mathcal{O}_K)^{m\times n} &\longrightarrow (\mathbb{Z}_q[x]/f)^{m\times n}\\ \mathbf{A} &\longmapsto t\mathbf{A}\end{aligned}$$

is also a bijection for $\forall m, n \in \mathbb{Z}$. Similarly, in the proof of [RSW18, Theorem 4.2], Roşca et al pointed out that $t^2\mathcal{C}^{-1}_{\mathbb{Z}[x]/f} + q\mathcal{O}_K = \mathcal{O}_K$, which also indicates that the map from $\mathbf{b}$ to $t^2\mathbf{b}$ induces an isomorphism over vector space. Hence Lemma 40 can be canonically adapted to module version.

Corollary 3. *Assume that $q\mathcal{O}_K + \mathcal{C}_{\mathbb{Z}[x]/f} = \mathcal{O}_K$. Let Σ be a full-rank positive definite $d \times d$ matrix and $\mathbf{s}(x) \in (\mathcal{O}_K/q\mathcal{O}_K)^n$. Let $t \in \mathcal{C}_{\mathbb{Z}[x]/f}$ such that $t\mathcal{C}^{-1}_{\mathbb{Z}[x]/f} + q\mathcal{O}_K = \mathcal{O}_K$. The map $(\mathbf{A}, \mathbf{b}) \mapsto (t \cdot \mathbf{A}, t^2 \cdot \mathbf{b})$ transforms $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},(\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma}})^m,f}$ to $\mathsf{P\text{-}MLWE}^{m,n}_{q,ts,\mathcal{N}^m_{\sqrt{\Sigma'}},f}$, where $\Sigma' = \mathbf{V}_K^\top(\mathbf{U}_{\mathbb{H}}^\top)^{-1}\operatorname{diag}(|\sigma_i(t)|^2)\Sigma\operatorname{diag}(|\sigma_i(t)|^2)\mathbf{U}_{\mathbb{H}}^{-1}\mathbf{V}_K$.*

Furthermore, the natural inclusion $\mathbb{Z}[x]/f \to \mathcal{O}_K$ induces a map that transforms $\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},\mathcal{N}^m_{\sqrt{\Sigma}},f}$ instance to $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},(N^{\mathbb{H}}_{\sqrt{\Sigma'}})^m,f}$ instance, where $\overline{\Sigma}' = \mathbf{U}_{\mathbb{H}}^\top(\mathbf{V}_K^\top)^{-1}\overline{\Sigma}\mathbf{V}_K^{-1}\mathbf{U}_{\mathbb{H}}$.

Proof. Let $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e})$ be an $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},\mathcal{N}^{\mathbb{H}^m}_{\mathbf{I}_m\otimes\sqrt{\Sigma}},f}$ instance. Let $\mathbf{A}' = t \cdot \mathbf{A}$ and $\mathbf{b}' = t^2 \cdot \mathbf{b} = \mathbf{A}' \cdot (t \cdot \mathbf{s}) + \mathbf{e}' \bmod (q, f(x))$ with $\mathbf{e}' = t^2 \cdot \mathbf{e}$. Then each component of $\mathbf{A}'$ is independently and uniformly distributed in $\mathcal{C}_{\mathbb{Z}/f(x)}/q\mathcal{C}_{\mathbb{Z}/f(x)}$ according to Lemma 36 for $\mathcal{I} = \mathcal{C}_{\mathbb{Z}[x]/f}$, $\mathcal{J} = q\mathcal{O}_K$ and $\mathcal{I}' = \mathcal{O}_K$. Hence $\mathbf{A}'$ is also uniformly distributed in $(\mathbb{Z}_q[x]/f(x))^{m\times n}$ by applying Lemma 34 and Lemma 35 in this subsection. The noise follows the claimed distribution according to Lemma 37 and the coordinate transformation between coefficient embedding and canonical embedding. The fact that $t \cdot \mathbf{s} \in \mathbb{Z}_q[x]/f(x)$ completes the proof that $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},(\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma}})^m,f}$ is mapped to $\mathsf{P\text{-}MLWE}^{m,n}_{q,ts,\mathcal{N}^m_{\sqrt{\Sigma'}},f}$.

We now turn to the reverse direction. We denote the inclusion homomorphism from $\mathcal{C}_{\mathbb{Z}[x]/f(x)}$ to $\mathcal{O}_K$ as ν_1, the inclusion homomorphism from $\mathcal{C}_{\mathbb{Z}[x]/f(x)}$ to $\mathbb{Z}[x]/f(x)$ as ν_2 and the inclusion homomorphism from $\mathbb{Z}[x]/f(x)$ to $\mathcal{O}_K$ as ν_3. We have $\nu_1 = \nu_3 \circ \nu_2$. Due to Lemma 34 in this subsection, the homomorphism from $\mathcal{C}_{\mathbb{Z}[x]/f(x)}$ to $\mathcal{O}_K/q\mathcal{O}_K$ induced by ν_1 is surjective, and we denote it as π_1. We also denote the homomorphism from $\mathbb{Z}[x]/f(x)$ to $\mathcal{O}_K/q\mathcal{O}_K$ induced by ν_3 as π_3. We also have $\pi_1 = \pi_3 \circ \nu_2$. Since π_1 is surjective, then π_3 must be surjective. Additionaly, the homomorphism π_3 canonically induces a homomorphism from $(\mathbb{Z}[x]/f(x))/q\mathcal{O}_K \cap (\mathbb{Z}[x]/f(x)) = \mathbb{Z}_q[x]/f(x)$ to $\mathcal{O}_K/q\mathcal{O}_K$, which we denote it as π_3'. Due to Lemma 34, $|\mathbb{Z}_q[x]/f(x)| = |\mathcal{O}_K/q\mathcal{O}_K|$. Hence π_3' is an isomorphism. Furthermore, π_3' is canonically induced by the inclusion from $\mathbb{Z}[x]/f(x)$ to $\mathcal{O}_K$. This implies that a $\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},\mathcal{N}^m_{\sqrt{\Sigma}},f}$ instance can be directly transformed into a $\mathsf{MLWE}^{m,n}_{q,\mathbf{s},(\mathcal{N}^{\mathbb{H}}_{\sqrt{\Sigma'}})^m,f}$ instance by inclusion, and the distribution of the error terms remains unchanged up to a coordinate transformation. □

In [RSW18], Roşca et al showed that for $f = x^d - C$, where C is a constant, we have $\|\mathbf{V}_K\|_2 \leqslant |C|d$ and $\|\mathbf{V}_K^{-1}\|_2 \leqslant \sqrt{d}$. In this case, the transformations between RLWE and PLWE ensure that the error terms remain small. Furthermore, for defining polynomial f of the form $x^n + x \cdot P(x) - a$, where $\deg(P) < n/2$ and a is a prime satisfying $a \geqslant 25 \cdot |P|_1^2$ and $a \leqslant \mathsf{poly}(d)$, they showed that the same property holds. These results can be naturally extended to the transformation between MLWE and $\mathsf{P\text{-}MLWE}$.

B.4 More Properties about the Connections between $\mathbb{Z}_{f(q)}$ and $\mathbb{Z}_q[x]/f$

Lemma 41. *Let $q > 2$ and $a(x), b(x) \in \mathbb{Z}_q[x]/f$ where $f \in \mathbb{Z}[x]$ is a monic and irreducible polynomial of degree d whose coefficients in the range $(-q/2, q/2)$, and $f(q) \geqslant q^d$, $\|f\|_\infty$ is bounded by a constant, we have:*

- *Addition carries: for any $a(x), b(x) \in \mathbb{Z}_q[x]/f(x)$, there exists an addition carries $c^{(a)}_{Eval}(a(x), b(x)) \bmod f(q) = \mathsf{Eval}^{(f)}_q(a(x) + b(x) \bmod (q, f(x))) - (a(q) + b(q)) \bmod f(q)$ such that $\left\|\Phi^{(f)}_q(c^{(a)}_{Eval}(a(x), b(x)))\right\|_\infty \leqslant 7 + 2\|f\|_\infty$;*
- *Multiplication carries: for any $a(x) \in \mathbb{Z}_q[x]/f(x)$, and for $b(x) \in \mathbb{Z}_q[x]/f(x)$ such that $\|b(x)\|_\infty \leqslant B$, where $B \ll q$, there exists a multiplication car-*

ries $c^{(m)}_{Eval}(a(x),b(x)) \bmod f(q) = \mathsf{Eval}^{(f)}_q(a(x)\cdot b(x) \bmod (q, f(x))) - (a(q)\cdot b(q)) \bmod f(q)$ *such that* $\left\|\Phi^{(f)}_q(c^{(m)}_{Eval}(a(x),b(x)))\right\|_\infty \leqslant 9 + 4\|f\|_\infty + 2B$.

Proof. First, we compute the addition carries:

$$\begin{aligned}
&\mathsf{Eval}^{(f)}_q(a(x)+b(x) \bmod f(x))\\
=&\mathsf{Eval}^{(f)}_q\left(\Phi^{(f)}_q(a(q)+b(q) \bmod f(q)) - c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q)) \bmod q\right)\\
=&\mathsf{Eval}^{(f)}_q\big(\Phi^{(f)}_q(a(q)+b(q) \bmod f(q))\\
&- c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q)) + q\textstyle\sum_{j=0}^{d-1}\delta_j x^j\big),
\end{aligned}$$

where $\delta_j = \lfloor \frac{\Phi^{(f)}_q(a(q)+b(q) \bmod f(q))_j + (-c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q)))_j}{q} \rceil \in \{0, \pm 1\}$. Continuing the computation, we have:

$$\begin{aligned}
&\mathsf{Eval}^{(f)}_q(a(x)+b(x) \bmod f(x))\\
=&\Big(\Phi_q(a(q)+b(q) \bmod f(q)) - c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q))\\
&+ \delta' f(x) + q\textstyle\sum_{j=0}^{d-1}\left(\delta_j + \delta'_j\right)x^j\Big)(q) \bmod f(q)\\
=&\Phi_q(a(q)+b(q) \bmod f(q))(q) + \delta' f(q) - c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q))(q)\\
&+ \textstyle\sum_{j=1}^{d}\left(\delta_{j-1} + \delta'_{j-1}\right)q^j \bmod f(q)\\
=&a(q)+b(q) - c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q))(q) + \textstyle\sum_{j=1}^{d}\left(\delta_{j-1} + \delta'_{j-1}\right)q^j \bmod f(q)
\end{aligned}$$

where $\delta' = \lfloor \frac{\Phi_q(a(q)+b(q) \bmod f(q))}{f(x)} \rceil$, $\delta'_j = \lfloor \frac{\Phi_q(a(q)+b(q) \bmod f(q))_j + \delta' f_j}{q} \rceil$.

We denote that $c^{(a)}_{Eval}(a(x),b(x)) = -c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q))(q) + \sum_{j=1}^{d}\left(\delta_{j-1} + \delta'_{j-1}\right)q^j \bmod f(q)$. Then we have $\|\Phi^{(f)}_q(c^{(a)}_{Eval}(a(x),b(x)))\|_\infty \leqslant \| - c^{(a)}_f(a(q) \bmod f(q), b(q) \bmod f(q))\|_\infty + \max_{j\in\{0,\ldots,d-2\}}|\delta_j| + \max_{j\in\{0,\ldots,d-2\}}|\delta_j| + (\delta_{d-1} + \delta'_{d-1})\|f\|_\infty \leqslant 7 + 2\|f\|_\infty$.

Then we compute the multiplication carries:

$$\begin{aligned}
&\mathsf{Eval}^{(f)}_q(a(x)\cdot b(x) \bmod f(x))\\
=&\mathsf{Eval}^{(f)}_q\left(\Phi^{(f)}_q(a(q)\cdot b(q) \bmod f(q)) - c^{(m)}_f(a(q) \bmod f(q), b(q) \bmod f(q)) \bmod q\right)\\
=&\mathsf{Eval}^{(f)}_q\Big(\Phi^{(f)}_q(a(q)\cdot b(q) \bmod f(q))\\
&- c^{(m)}_f(a(q) \bmod f(q), b(q) \bmod f(q)) + q\textstyle\sum_{j=0}^{d-1}\delta_j x^j\Big),
\end{aligned}$$

where $\delta_j = \lfloor \frac{\Phi^{(f)}_q(a(q)\cdot b(q) \bmod f(q))_j + (-c^{(m)}_f(a(q) \bmod f(q), b(q) \bmod f(q)))_j}{q} \rceil \in \{0, \pm 1\}$. Continuing the computation, we have:

$$
\begin{aligned}
&\mathsf{Eval}_q^{(f)}(a(x)\cdot b(x) \bmod f(x))\\
=&\Big(\Phi_q(a(q)\cdot b(q) \bmod f(q)) + \delta' f(x) - c_f^{(m)}(a(q) \bmod f(q), b(q) \bmod f(q))\\
&+ q\sum_{j=0}^{d-1}\left(\delta_j + \delta'_j\right)x^j\Big)(q) \bmod f(q)\\
=&\Phi_q(a(q)\cdot b(q) \bmod f(q))(q) + \delta' f(q) - c_f^{(m)}(a(q) \bmod f(q), b(q) \bmod f(q))(q)\\
&+ \sum_{j=0}^{d}\left(\delta_{j-1} + \delta'_{j-1}\right)q^j \bmod f(q)\\
=&a(q)\cdot b(q) - c_f^{(m)}(a(q) \bmod f(q), b(q) \bmod f(q))(q) + \sum_{j=0}^{d}\left(\delta_{j-1} + \delta'_{j-1}\right)q^j \bmod f(q)
\end{aligned}
$$

where $\delta' = \lfloor \frac{\Phi_q(a(q)\cdot b(q) \bmod f(q))}{f(x)} \rceil$, $\delta'_j = \lfloor \frac{\Phi_q(a(q)\cdot b(q) \bmod f(q))_j + \delta' f_j}{q} \rceil$.

We denote that $c_{Eval}^{(m)}(a(x), b(x)) = -c_f^{(m)}(a(q) \bmod f(q), b(q) \bmod f(q))(q) + \sum_{j=1}^{d}\left(\delta_{j-1} + \delta'_{j-1}\right)q^j \bmod f(q)$. Then we have $\|\Phi_q^{(f)}(c_{Eval}^{(m)}(a(x), b(x)))\|_\infty \leqslant \| - c_f^{(m)}(a(q) \bmod f(q), b(q) \bmod f(q))\|_\infty + \max_{j\in\{0,\ldots,d-2\}}|\delta_j| + \max_{j\in\{0,\ldots,d-2\}}|\delta_j| + (\delta_{d-1} + \delta'_{d-1})\|f\|_\infty \leqslant 9 + 4\|f\|_\infty + 2B$. □

Intuitively, for an interval in $I_{f,q}$ close to the origin, $\Phi_q^{(f)}$ is a bijection over this interval. More precisely, we establish this result in the following lemma.

Lemma 42. *Let κ be the security parameter. For $q = \mathsf{poly}(\kappa)$ a positive integer, $f(x)$ a monic and irreducible polynomial over $\mathbb{Z}[x]$ with degree $d = \mathsf{poly}(\kappa)$ and B a positive number satisfying $q \geqslant \omega(1)\cdot B$, let $\mathcal{I}_B = \left\{a \in I_{f,q}, \left|\lfloor \frac{a}{q^{d-1}} \rceil\right| \leqslant B\right\}$ and $\mathcal{P}_B = \{a(x) \in \mathbb{Z}_q/f(x), \|a_{d-1}\| \leqslant B\}$. $\Phi_q^{(f)}\Big|_{\mathcal{I}_B}$ is a bijection from $\mathcal{I}_B$ to $\mathcal{P}_B$ and its inverse map is $\mathsf{Eval}_q^{(f)}\Big|_{\mathcal{P}_B}$.*

Proof. For each $a \in \mathcal{I}_B$, $\Phi_q^{(f)}(a) \in \mathcal{P}_B$. If there exists another $a' \in \mathcal{I}_B$ such that $a' \neq a$ and $\Phi_q^{(f)}(a) = \Phi_q^{(f)}(a')$, it means that $\Phi_q(a') = \Phi_q(a) + \delta f(x)$ where $\delta \neq 0$ is an integer. In this case, $B \geqslant \left|\lfloor \frac{a}{q^{d-1}} \rceil\right| \geqslant |\delta| q - \frac{q}{2} \geqslant B\cdot\omega(1)$, which is a contradiction. Hence $\Phi_q^{(f)}\Big|_{\mathcal{I}_B}$ is injective. Furthermore, $\#\mathcal{I}_B = \#\mathcal{P}_B$, $\Phi_q^{(f)}\Big|_{\mathcal{I}_B}$ is a bijective. One can check that $\Phi_q^{(f)}\Big|_{\mathcal{I}_B} \circ \mathsf{Eval}_q^{(f)}\Big|_{\mathcal{P}_B}$ is an identity map and the result follows. □

B.5 Equivalence between LWE and EDCP

We recall the equivalence between LWE and G-EDCP in [BKSW18]. These results will be used to show a dimension-modulus switching for EDCP in Supplementary Material E.

Lemma 43 ([BKSW18, Theorem 2]). *Let κ be the security parameter. Let n, m, q be positive integers such that $m \geqslant n\log q$. Let $\alpha < 1$ be a positive number. Let $r < 1/(32m\kappa\alpha q^{n/m})$ be a positive integer. Let $l = \mathsf{poly}(\kappa)$ be a positive*

integer. Let $\mathcal{S}$ be a distribution over $\mathbb{Z}_q^n$. There exists a probabilistic quantum reduction with run-time polynomial in κ, from $\mathsf{LWE}_{q,\mathcal{S},\alpha q}^{m,n}$ to $\mathsf{G\text{-}EDCP}_{q,\mathcal{S},r}^{l,n}$.

Lemma 44 ([BKSW18, Theorem 4]). *Let κ be security parameter. Let n, m, q be positive integers. Let $r = \Omega(\sqrt{\kappa})$ be a positive number. Let $\mathcal{S}$ be a distribution over $\mathbb{Z}_q^n$. There exists a quantum reduction, with run-time polynomial in κ, from $\mathsf{G\text{-}EDCP}_{q,\mathcal{S},r}^{m,n}$ to $\mathsf{LWE}_{q,\mathcal{S},\frac{q}{2r}}^{m,n}$.*

C Supplementary Materials for Reduction from G-IP-M-EDCP to MLWE

C.1 Trace Distance Needed in the Proof of Lemma 25

Lemma 45. *Let κ be the security parameter. Let q, n, r be positive integers satisfying $q \geqslant \sqrt{\kappa} r$ and $r \geqslant \sqrt{n} \geqslant \eta_\varepsilon(\mathbb{Z}^n)$, where $\varepsilon \leqslant 2^{-\omega(\log(\kappa))}$. Let $\mathbf{a} \in \mathbb{Z}_q^n$ be a fixed vector. Given the following two quantum states:*

$$|\psi_1\rangle = \frac{1}{\sqrt{S_1}} \sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_1(\mathbf{b}) |\mathbf{b}\rangle \text{ and } |\psi_2\rangle = \frac{1}{\sqrt{S_2}} \sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_2(\mathbf{b}) |\mathbf{b}\rangle,$$

where we have $D_1(\mathbf{b}) = \sum_{\mathbf{c}\in\mathbb{Z}_q^n} \rho_r(\mathbf{c}) \omega_q^{\langle \mathbf{c}, \mathbf{a}+\mathbf{b}\rangle}$, $D_2(\mathbf{b}) = \sum_{\mathbf{c}\in\mathbb{Z}^n} \rho_r(\mathbf{c}) \omega_q^{\langle \mathbf{c}, \mathbf{a}+\mathbf{b}\rangle}$, $S_1 = \sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_1(\mathbf{b}) \overline{D_1(\mathbf{b})}$ and $S_2 = \sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_2(\mathbf{b}) \overline{D_2(\mathbf{b})}$, the trace distance between $|\psi_1\rangle$ and $|\psi_2\rangle$ satisfies $\Delta_{tr}(|\psi_1\rangle, |\psi_2\rangle) \leqslant n^3 \cdot 2^{-\Omega(q^2/r^2)}/(q^n r^n)$.

Proof. First, $D_2(\mathbf{b})$ is a positive real number according to Poisson summation formula in Lemma 5. Therefore, we have $S_2 = \sum_{\mathbf{b}\in\mathbb{Z}^n} (D_2(\mathbf{b}))^2$.

For a fixed $\mathbf{b}$, let $D_1(\mathbf{b}) = D_2(\mathbf{b}) + \delta(\mathbf{b})$, where

$$\delta(\mathbf{b}) = \sum_{\mathbf{c}\in\mathbb{Z}^n \setminus (\mathbb{Z}\cap(-q/2, q/2])^n} \rho_r(\mathbf{c}) \omega_q^{\langle \mathbf{c}, \mathbf{a}+\mathbf{b}\rangle},$$

and $\omega_q = \exp(2\pi\sqrt{-1}/q)$. Then the norm of $\delta(\mathbf{b})$ can be bounded as follows:

$$\begin{aligned} |\delta(\mathbf{b})| &\leqslant \sum_{\mathbf{c}\in\mathbb{Z}^n \setminus (\mathbb{Z}\cap(-q/2, q/2])^n} |\rho_r(\mathbf{c}) \omega_q^{\langle \mathbf{c}, \mathbf{a}+\mathbf{b}\rangle}| \\ &= \sum_{\mathbf{c}\in\mathbb{Z}^n \setminus (\mathbb{Z}\cap(-q/2, q/2])^n} \rho_r(\mathbf{c}) \leqslant n \cdot 2^{-\Omega(q^2/r^2)}, \end{aligned}$$

where the second inequality holds due to Corollary 1 in Section 3.4. Then,

$$\begin{aligned} S_1 = |S_1| &= \left| \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(D_2(\mathbf{b})^2 + \delta(\mathbf{b}) D_2(\mathbf{b}) + \overline{\delta(\mathbf{b})} D_2(\mathbf{b}) + |\delta(\mathbf{b})|^2 \right) \right| \\ &\leqslant \left| \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(D_2(\mathbf{b})^2 \right) \right| + \left| \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(\delta(\mathbf{b}) D_2(\mathbf{b}) + \overline{\delta(\mathbf{b})} D_2(\mathbf{b}) + |\delta(\mathbf{b})|^2 \right) \right| \\ &\leqslant S_2 + \sum_{\mathbf{b}\in\mathbb{Z}_q^n} |\delta(\mathbf{b})| \left(2 D_2(\mathbf{b}) + |\delta(\mathbf{b})| \right) \\ &\leqslant S_2 + n \cdot 2^{-\Omega(q^2/r^2)} \cdot \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(2 D_2(\mathbf{b}) + n \cdot 2^{-\Omega(q^2/r^2)} \right). \end{aligned}$$

Due to Lemma 9 in Section 3.4,

$$D_2(\mathbf{b}) = |D_2(\mathbf{b})| \leqslant \sum_{\mathbf{c}\in\mathbb{Z}^n} \rho_r(\mathbf{c}) \leqslant (1+\varepsilon)r^n,$$

hence $S_1 \leqslant S_2 + n \cdot r^n \cdot 2^{-\Omega(q^2/r^2)}$. On the other side,

$$\begin{aligned}
S_2 = |S_2| =& \left|\sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(|D_1(\mathbf{b})|^2 - \delta(\mathbf{b})\overline{D_1(\mathbf{b})} - \overline{\delta(\mathbf{b})}D_1(\mathbf{b}) + |\delta(\mathbf{b})|^2\right)\right| \\
\leqslant& \left|\sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(|D_1(\mathbf{b})|^2\right)\right| + \left|\sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(\delta(\mathbf{b})\overline{D_1(\mathbf{b})} + \overline{\delta(\mathbf{b})}D_1(\mathbf{b}) - |\delta(\mathbf{b})|^2\right)\right| \\
\leqslant& S_1 + \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(|\delta(\mathbf{b})| \cdot |D_1(\mathbf{b})| + |\delta(\mathbf{b})| \cdot |D_1(\mathbf{b})| + |\delta(\mathbf{b})|^2\right) \\
\leqslant& S_1 + \sum_{\mathbf{b}\in\mathbb{Z}_q^n} |\delta(\mathbf{b})| \left(2(D_2(\mathbf{b}) + |\delta(\mathbf{b})|) + |\delta(\mathbf{b})|\right) \\
\leqslant& S_1 + n \cdot 2^{-\Omega(q^2/r^2)} \cdot \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(2D_2(\mathbf{b}) + 3n \cdot 2^{-\Omega(q^2/r^2)}\right) \\
\leqslant& S_1 + n \cdot r^n \cdot 2^{-\Omega(q^2/r^2)}.
\end{aligned}$$

Therefore, $|S_1 - S_2| \leqslant n \cdot r^n \cdot 2^{-\Omega(q^2/r^2)}$. Then we consider the trace distance:

$$\begin{aligned}
\Delta_{tr}(|\psi_1\rangle, |\psi_2\rangle) =& \frac{1}{2} \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left|\frac{D_1(\mathbf{b})\overline{D_1(\mathbf{b})}}{S_1} - \frac{D_2(\mathbf{b})\overline{D_2(\mathbf{b})}}{S_2}\right| \\
=& \frac{1}{2} \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left|\frac{S_2 D_1(\mathbf{b}) \cdot \overline{D_1(\mathbf{b})} - S_1(D_1(\mathbf{b}) - \delta(\mathbf{b}))(\overline{D_1(\mathbf{b})} - \overline{\delta(\mathbf{b})})}{S_1 S_2}\right| \\
=& \frac{1}{2} \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left|\frac{(S_2 - S_1)D_1(\mathbf{b})\overline{D_1(\mathbf{b})} + S_1(\delta(\mathbf{b})\overline{D_1(\mathbf{b})} + \overline{\delta(\mathbf{b})}D_1(\mathbf{b})) - S_1|\delta(\mathbf{b})|^2}{S_1 S_2}\right| \\
\leqslant& \frac{1}{2} \sum_{\mathbf{b}\in\mathbb{Z}_q^n} \left(\frac{|S_2 - S_1|D_1(\mathbf{b})\overline{D_1(\mathbf{b})}}{S_1 S_2} + \frac{\left|(\delta(\mathbf{b})\overline{D_1(\mathbf{b})} + \overline{\delta(\mathbf{b})}D_1(\mathbf{b})) - |\delta(\mathbf{b})|^2\right|}{S_2}\right) \\
\leqslant& \frac{|S_2 - S_1|}{2S_2} + \frac{1}{2}\sum_{\mathbf{b}\in\mathbb{Z}_q^n} \frac{2|\delta(\mathbf{b})|D_2(\mathbf{b}) + |\delta(\mathbf{b})|^2}{S_2} \\
\leqslant& \frac{|S_2 - S_1|}{2S_2} + \max_{\mathbf{b}\in\mathbb{Z}_q^n}\{|\delta(\mathbf{b})|\} \cdot \frac{\sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_2(\mathbf{b})}{S_2} + \frac{\sum_{\mathbf{b}\in\mathbb{Z}_q^n} |\delta(\mathbf{b})|^2}{2S_2}.
\end{aligned}$$

Now we consider the lower bound of S_2:

$$\begin{aligned}
S_2 =& \sum_{\mathbf{b}\in\mathbb{Z}_q^n} (D_2(\mathbf{b}))^2 \geqslant \frac{1}{n}\left(\sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_2(\mathbf{b})\right)^2 \\
=& \frac{1}{n}\left(\sum_{\mathbf{b}\in\mathbb{Z}_q^n} r^n \cdot \rho_{1/r}\left(\mathbb{Z}^n + \frac{\mathbf{a}+\mathbf{b}}{q}\right)\right)^2 \geqslant \frac{r^{2n}q^{2n}}{n},
\end{aligned}$$

where the first inequality holds due to mean inequality, the second equality is derived from the Poisson summation formula and the last inequality holds due to $\rho_{1/r}\left(\mathbb{Z}^n + (\mathbf{a}+\mathbf{b})/q\right) \geqslant \rho_{1/r}(\mathbf{0}) \geqslant 1$. With the inequality above, we also have

$$\frac{\sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_2(\mathbf{b})}{S_2} \leqslant \frac{n}{\sum_{\mathbf{b}\in\mathbb{Z}_q^n} D_2(\mathbf{b})} \leqslant \frac{n}{r^n q^n}.$$

Therefore, we have:

$$\begin{aligned}\Delta_{tr}(|\psi_1\rangle, |\psi_2\rangle) \leqslant & \frac{n^2 \cdot 2^{-\Omega(q^2/r^2)}}{q^{2n} r^n} + \frac{n^2 \cdot 2^{-\Omega(q^2/r^2)}}{q^n r^n} + \frac{n^3 \cdot 2^{-\Omega(2q^2/r^2)}}{2q^n r^{2n}} \\ \leqslant & \frac{n^3 \cdot 2^{-\Omega(q^2/r^2)}}{q^n r^n}.\end{aligned}$$

The result follows. □

C.2 Computation of the Carries

As a preparatory step for the proof of reduction from stEDCP to MLWE, we first derive the following upper bounds for several carries.

Lemma 46. *For a secret $\mathbf{s}(x) \in (\mathbb{Z}_q[x]/f)^n$ satisfying $\|s_i(x)\|_\infty \leqslant B$, $i \in [n]$, any $\mathbf{a} \in (\mathbb{Z}_{f(q)})^n$ and any $b \in \mathbb{Z}_{f(q)}$, we denote the polynomial $c_i^{**}(\mathbf{a}, b)(x) = \Phi_q^{(f)}\left(\langle \mathbf{a}, \mathbf{s}\rangle q^i + b \bmod f(q)\right) - \left(\langle \Phi_q^{(f)}(\mathbf{a}), \Phi_q^{(f)}(\mathbf{s})\rangle \cdot x^i + \Phi_q^{(f)}(b) \bmod f(x)\right)$, $i \in [d]$. We denote $c_{i,(I)}^{**} = c_f^{(a)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q), b)$ and $c_{i,(II)}^{**} = c_i^{**}(\mathbf{a}, b) - c_{i,(I)}^{**}$ and we have:*

1) *We have $\|c_{i,(I)}^{**}\|_\infty \leqslant 2 + 4\|f\|_\infty$, and note that $c_{i,(I)}^{**}$ depends on b;*
2) *We have $\|c_{i,(II)}^{**}\|_\infty \leqslant \left(\frac{3B}{2}n^2 + (7 + \|f\|_1)n - 2\right) EF(f) + \frac{7}{2}$, and note that $c_{i,(II)}^{**}$ is independent of b;*
3) *$\|c_i^{**}(\mathbf{a}, b)\|_\infty \leqslant \left(\frac{3B}{2}n^2 + (7 + \|f\|_1)n - 2\right) EF(f) + \frac{11}{2} + 4\|f\|_\infty$.*

Proof. First, we have:

$$\begin{aligned}&\Phi_q^{(f)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i + b \bmod f(q)) \\ =&\Phi_q^{(f)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q)) + \Phi_q^{(f)}(b) + c_f^{(a)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q), b \bmod f(q)) \\ =&\left(\Phi_q^{(f)}(\langle \mathbf{a}, \mathbf{s}\rangle \bmod f(q))\Phi_q^{(f)}(q^i) \bmod f(x)\right) + \Phi_q^{(f)}(b) \\ &+ c_f^{(m)}(\langle \mathbf{a}, \mathbf{s}\rangle \bmod f(q), q^i) + c_f^{(a)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q), b \bmod f(q)).\end{aligned} \tag{31}$$

Since $\Phi_q^{(f)}(q^i)$ can be replaced by x^i directly, we have:

$$\begin{aligned}(31) =&\Big(\left(\langle \Phi_q^{(f)}(\mathbf{a}), \Phi_q^{(f)}(\mathbf{s})\rangle \bmod f(x)\right) + \sum_{l=1}^{n} c_f^{(m)}(a_l, s_l) \\ &+ \sum_{k=1}^{n-1} c_f^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q), a_{n-k+1}s_{n-k+1} \bmod f(q))\Big) x^i \bmod f(x) \\ &+ \Phi_q^{(f)}(b) + c_f^{(m)}(\langle \mathbf{a}, \mathbf{s}\rangle \bmod f(q), q^i) + c_f^{(a)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q), b \bmod f(q)).\end{aligned} \tag{32}$$

Therefore, the carries are:

$$\begin{aligned}c_i^{**}(\mathbf{a}, b)(x) = &\left(\sum_{k=1}^{n-1} c_f^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q), a_{n-k+1}s_{n-k+1} \bmod f(q))\right) x^i \bmod f(x) \\ &+ \left(\sum_{l=1}^{n} c_f^{(m)}(a_l, s_l)\right) x^i \bmod f(x) + c_f^{(m)}(\langle \mathbf{a}, \mathbf{s}\rangle \bmod f(q), q^i) \\ &+ c_f^{(a)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q), b \bmod f(q)).\end{aligned}$$

Since $c^{**}_{i,(I)} = c_f^{(a)}(\langle \mathbf{a}, \mathbf{s}\rangle q^i \bmod f(q), b)$, then we have:

$$\begin{aligned}
&c^{**}_{i,(II)} = c_i^{**}(\mathbf{a}, b)(x) - c^{**}_{i,(I)} \\
&= \left(\sum_{k=1}^{n-1} c_f^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q), a_{n-k+1}s_{n-k+1} \bmod f(q))\right) x^i \bmod f(x) \\
&\quad + \left(\sum_{l=1}^{n} c_f^{(m)}(a_l, s_l)\right) x^i \bmod f(x) + c_f^{(m)}(\langle \mathbf{a}, \mathbf{s}\rangle \bmod f(q), q^i).
\end{aligned}$$

From the expression of $c^{**}_{i,(II)}$, we obtain that $c^{**}_{i,(II)}$ is independent of b. We rewrite $c^{**}_{i,(II)}$ as $c^{*}_{i,1} + c^{*}_{i,2}$, where

$$\begin{aligned}
&c^{*}_{i,1}(x) \\
&= \left(\sum_{k=1}^{n-1} c_f^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q), a_{n-k+1}s_{n-k+1} \bmod f(q))\right) x^i \bmod f(x) \\
&= \left(\sum_{k=1}^{n-1} c^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q), a_{n-k+1}s_{n-k+1} \bmod f(q))\right) x^i \bmod f(x) \\
&\quad + \left(\sum_{k=1}^{n-1} c^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q) + a_{n-k+1}s_{n-k+1} \bmod f(q), \delta_{i,0} f(q))\right) x^i \bmod f(x),
\end{aligned}$$

where $\delta_{i,0} \in \{-1, 0, 1\}$ and

$$\begin{aligned}
c^{*}_{i,2}(x) &= \left(\sum_{l=1}^{n} c_f^{(m)}(a_l, s_l)\right) x^i \bmod f(x) \\
&= \left(\sum_{l=1}^{n} c^{(m)}(a_l, s_l)\right) x^i \bmod f(x) + \left(\sum_{l=1}^{n} c^{(m)}(-\delta'_l, f(q))\right) x^i \bmod f(x) \\
&\quad + \left(\sum_{l=1}^{n} c^{(a)}(a_l s_l, -\delta'_l f(q))\right) x^i \bmod f(x),
\end{aligned}$$

where $\delta'_l = \lfloor \frac{a_l s_l - (a_l s_l \bmod f(q))}{f(q)} \rfloor$.

Then we compute the upper bound of the infinity norms of these two terms above as:

$$\begin{aligned}
\|c^{*}_{i,1}\|_\infty \leqslant & EF(f) \cdot \left\| \sum_{k=1}^{n-1} c^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q), a_{n-k+1}s_{n-k+1} \bmod f(q)) \right\|_\infty \\
& + EF(f) \cdot \left\| \sum_{k=1}^{n-1} c^{(a)}(\sum_{j=1}^{n-k} a_j s_j \bmod f(q) + a_{n-k+1}s_{n-k+1} \bmod f(q), \delta_{i,0} f(q)) \right\|_\infty \\
\leqslant & (n-1)EF(f) + (n-1)EF(f) \leqslant 2(n-1)EF(f),
\end{aligned}$$

where the second inequality holds due to Lemma 16 in Section 3.6, and

$$\begin{aligned}
\|c^{*}_{i,2}\|_\infty \leqslant & EF(f) \cdot \left\| \sum_{l=1}^{n} c^{(m)}(a_l, s_l) \right\|_\infty + EF(f) \cdot \left\| \sum_{l=1}^{n} c^{(m)}(-\delta'_l, f(q)) \right\|_\infty \\
& + EF(f) \cdot \left\| \sum_{l=1}^{n} c^{(a)}(a_l s_l, -\delta'_l f(q)) \right\|_\infty \\
\leqslant & n\frac{q + \lfloor \frac{q-1}{2} \rfloor + qnB}{q-1} EF(f) + n\frac{q + \lfloor \frac{q-1}{2} \rfloor + q\|f\|_1}{q-1} EF(f) + nEF(f) \\
\leqslant & nEF(f)(5 + \frac{3}{2}(nB + \|f\|_1)),
\end{aligned}$$

where the second inequality holds due to Lemma 16. According to Lemma 16 and Lemma 17 in Section 3.6, $\left\|c^{**}_{i,(I)}\right\|_\infty \leqslant 2 + 4\|f\|_\infty$. Then we consider the infinity bound of $c^{**}_{i,(II)}$:

$$\left\|c^{**}_{i,(II)}\right\|_\infty \leqslant \|c^{*}_{i,1}\|_\infty + \|c^{*}_{i,2}\|_\infty \leqslant \left(\frac{3B}{2}n^2 + (7 + \|f\|_1)n - 2\right) EF(f) + \frac{7}{2}.$$

Therefore the infinite norm of $c^{**}_i(\mathbf{a}, b)(x)$ can also be bounded as follows.

$$\begin{aligned}\|c^{**}_i(\mathbf{a}, b)\|_\infty \leqslant & \|c^{**}_{i,(I)}\|_\infty + \|c^{**}_{i,(II)}\|_\infty \\ \leqslant & \left(\frac{3B}{2}n^2 + (7 + \|f\|_1)n - 2\right) EF(f) + \frac{11}{2} + 4\|f\|_\infty.\end{aligned}$$

The result follows. □

C.3 Proof of Lemma 26

Proof. To prove this lemma, we first fix a secret. We then apply a hybrid argument and analyze the Rényi divergence between the distributions arising from different hybrids.

Hybrid 1. For a $\mathbf{s} \hookleftarrow \chi$, the oracle selects and outputs at most m samples of the form $(\mathbf{a}, \mathbf{b} = \langle \mathbf{a}, \mathbf{s}\rangle \mathbf{z} + \mathbf{e} \bmod f(q)) \in \mathbb{Z}^n_{f(q)} \times \mathbb{Z}^d_{f(q)}$, where $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$, $\mathbf{a} \hookleftarrow U(\mathbb{Z}^n_{f(q)})$, and $\mathbf{e} \hookleftarrow D_{\mathbb{Z}^d, r_\beta}$. The adversary is asked to recover the secret $\mathbf{s}$.

In this hybrid argument, the instance corresponds exactly to the distribution provided to the adversary in the Search *q-adic* $\mathsf{IP\text{-}MLWE}^{m,n}_{q,\chi,r_\beta,f}$ problem.

Hybrid 2. For a $\mathbf{s} \hookleftarrow \chi$, the oracle selects and outputs at most m samples of the form $(\mathbf{a}, \mathbf{b} = \langle \mathbf{a}, \mathbf{s}\rangle \mathbf{z} + \mathbf{e} \bmod f(q)) \in \mathbb{Z}^n_{f(q)} \times \mathbb{Z}^d_{f(q)}$, where $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$, $\mathbf{a} \hookleftarrow U(\mathbb{Z}^n_{f(q)})$, and $\mathbf{e} \hookleftarrow q^{d-1} D^{Sum, q^{d-1}}_{\mathbb{Z}^d, r_\beta} + U(\mathbb{Z}^d_{q^{d-1}})$. The adversary is asked to recover the secret $\mathbf{s}$.

The only difference between **Hybrid 1** and **Hybrid 2** is the distributions of the errors $\mathbf{e}$'s. We compute the Rényi divergence as follows. We first fix the secret $\mathbf{s}$. Let $\mathcal{D}_1$ denote the distribution of one sample with secret $\mathbf{s}$ in **Hybrid 1** and $\mathcal{D}_2$ denote the distribution of one sample with secret $\mathbf{s}$ in **Hybrid 2**, then we have:

$$R(\mathcal{D}_2 \| \mathcal{D}_1) = \sum_{\substack{\tilde{\mathbf{a}} \in \mathbb{Z}^n_{f(q)} \\ \tilde{\mathbf{b}} \in \mathbb{Z}^d_{f(q)}}} \frac{\Pr\limits_{\substack{\mathbf{a} \hookleftarrow U(\mathbb{Z}^n_{f(q)}) \\ \mathbf{e} \hookleftarrow D^{Sum} + U}} (\mathbf{a} = \tilde{\mathbf{a}}, \langle \mathbf{a}, \mathbf{s}\rangle \mathbf{z} + \mathbf{e} = \tilde{\mathbf{b}})^2}{\Pr\limits_{\substack{\mathbf{a}' \hookleftarrow U(\mathbb{Z}^n_{f(q)}) \\ \mathbf{e}' \hookleftarrow D_{\mathbb{Z}^d, r_\beta}}} (\mathbf{a}' = \tilde{\mathbf{a}}, \langle \mathbf{a}', \mathbf{s}\rangle \mathbf{z} + \mathbf{e}' = \tilde{\mathbf{b}})},$$

where $D^{Sum}+U$ is the simplification of $q^{d-1}\cdot D^{Sum,q^{d-1}}_{\mathbb{Z}^d,r_\beta}+U(\mathbb{Z}^d_{q^{d-1}})$. Continuing the computation, we obtain:

$$\begin{aligned}R(\mathcal{D}_2\|\mathcal{D}_1)=&\sum_{\substack{\widetilde{\mathbf{a}}\in\mathbb{Z}^n_{f(q)}\\ \widetilde{\mathbf{b}}\in\mathbb{Z}^d_{f(q)}}}\frac{\frac{1}{f(q)^{2n}}\Pr\limits_{\mathbf{e}\hookleftarrow D^{Sum}+U}(\mathbf{e}=\widetilde{\mathbf{b}}-\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z})^2}{\frac{1}{f(q)^n}\Pr\limits_{\mathbf{e}'\hookleftarrow D_{\mathbb{Z}^d,r_\beta}}(\mathbf{e}'=\widetilde{\mathbf{b}}-\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z})}\\ =&f(q)^n\cdot\sum_{\widetilde{\mathbf{e}}\in\mathbb{Z}^d_{f(q)}}\frac{\Pr\limits_{\mathbf{e}\hookleftarrow D^{Sum}+U}(\mathbf{e}=\widetilde{\mathbf{e}})^2}{f(q)^n\Pr\limits_{\mathbf{e}'\hookleftarrow D_{\mathbb{Z}^d,r_\beta}}(\mathbf{e}'=\widetilde{\mathbf{e}})}.\end{aligned}$$

The second equality holds because for each fixed $\widetilde{\mathbf{a}}$,

$$\sum_{\widetilde{\mathbf{b}}\in\mathbb{Z}^d_{f(q)}}\frac{\frac{1}{f(q)^{2n}}\Pr\limits_{\mathbf{e}\hookleftarrow D^{Sum}+U}(\mathbf{e}=\widetilde{\mathbf{b}}-\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z})^2}{\frac{1}{f(q)^n}\Pr\limits_{\mathbf{e}'\hookleftarrow D_{\mathbb{Z}^d,r_\beta}}(\mathbf{e}'=\widetilde{\mathbf{b}}-\langle\widetilde{\mathbf{a}},\mathbf{s}\rangle\mathbf{z})}$$

can be rewritten as

$$\sum\nolimits_{\widetilde{\mathbf{e}}\in\mathbb{Z}^d_{f(q)}}\frac{\Pr_{\mathbf{e}\hookleftarrow D^{Sum}+U}(\mathbf{e}=\widetilde{\mathbf{e}})^2}{f(q)^n\Pr_{\mathbf{e}'\hookleftarrow D_{\mathbb{Z}^d,r_\beta}}(\mathbf{e}'=\widetilde{\mathbf{e}})}.$$

Therefore, the above Rényi divergence can be upper bounded as:

$$\begin{aligned}R(\mathcal{D}_2\|\mathcal{D}_1)=&\sum\nolimits_{\widetilde{\mathbf{e}}\in\mathbb{Z}^d_{f(q)}}\frac{\Pr_{\mathbf{e}\hookleftarrow D^{Sum}+U}(\mathbf{e}=\widetilde{\mathbf{e}})^2}{\Pr_{\mathbf{e}'\hookleftarrow D_{\mathbb{Z}^d,r_\beta}}(\mathbf{e}'=\widetilde{\mathbf{e}})}\\ =&R(q^{d-1}\cdot D^{Sum,q^{d-1}}_{\mathbb{Z}^d,r_\beta}+U(\mathbb{Z}^d_{q^{d-1}})\|D_{\mathbb{Z}^d,r_\beta})\\ \leqslant&(1+3\varepsilon)^2\exp\left((9dq^{(d-1)})/(2r_\beta)\right),\end{aligned}$$

where the last inequality refers to Lemma 14 in Section 3.4 by replacing G in Lemma 14 with q^{d-1}. Therefore, when we consider m samples with fixed secret $\mathbf{s}$, the Rényi Divergence, which is denoted as $R_{2,1}$, has an upper bound:

$$R_{2,1}\leqslant(1+3\varepsilon)^{2m}\exp\left((9dmq^{(d-1)})/(2r_\beta)\right).$$

Then we take the randomness of the secret $\mathbf{s}$ into account. Since the distributions of the secrets in **Hybrid 1** and **Hybrid 2** are identical, $R_\infty(\chi\|\chi)=1$, and the Rényi Divergence between m samples in **Hybrid 1** and m samples in **Hybrid 2**, which is denoted as $R'_{2,1}$, also has an upper bound as follows.

$$R'_{2,1}\leqslant R_\infty(\chi\|\chi)\cdot R_{2,1}\leqslant(1+3\varepsilon)^{2m}\exp\left((9dmq^{(d-1)})/(2r_\beta)\right).$$

Therefore, if there exists a polynomial-time adversary who can recover the secret from m samples in **Hybrid 2** with advantage $\delta_{\beta,2}$, then this adversary can also recover the secret from m samples in **Hybrid 1** with advantage:

$$\delta'_\beta\geqslant\delta^2_{\beta,2}/\left((1+3\varepsilon)^{2m}\exp\left((9dmq^{(d-1)})/(2r_\beta)\right)\right).$$

Hybrid 3. For a fixed $\mathbf{s}$, the oracle selects and outputs at most m samples of the form $(\mathbf{a}, \mathbf{b} = \langle \mathbf{a}, \mathbf{s} \rangle \mathbf{z} + \mathbf{e} \bmod f(q)) \in \mathbb{Z}_{f(q)}^n \times \mathbb{Z}_{f(q)}^d$, where $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$, $\mathbf{a} \hookleftarrow U(\mathbb{Z}_{f(q)}^n)$, and $e \hookleftarrow q^{d-1} D_{\mathbb{Z}^d, r_\beta/q^{d-1}} + U(\mathbb{Z}_{q^{d-1}}^d)$.

In this hybrid argument, the distribution of the instance is the same as the distribution of the instance in Search q-*adic* $\mathsf{IP\text{-}MLWE}_{q,\chi,D+U,f}^{m,n}$.

For a fixed secret $\mathbf{s}$, we denote the distribution of one sample with fixed secret $\mathbf{s}$ in **Hybrid 2** as $\mathcal{D}_2$ and the distribution of one sample with fixed secret $\mathbf{s}$ in **Hybrid 3** as $\mathcal{D}_3$. Then we can compute the following Rényi divergence:

$$R(\mathcal{D}_3 \| \mathcal{D}_2) = \sum_{\substack{\widetilde{\mathbf{a}} \in \mathbb{Z}_{f(q)}^n \\ \widetilde{\mathbf{b}} \in \mathbb{Z}_{f(q)}^d}} \frac{\Pr_{\substack{\mathbf{a} \hookleftarrow U(\mathbb{Z}_{f(q)}^n) \\ \mathbf{e} \hookleftarrow D+U}} (\mathbf{a} = \widetilde{\mathbf{a}}, \langle \mathbf{a}, \mathbf{s} \rangle \mathbf{z} + \mathbf{e} = \widetilde{\mathbf{b}})^2}{\Pr_{\substack{\mathbf{a}' \hookleftarrow U(\mathbb{Z}_{f(q)}^n) \\ \mathbf{e}' \hookleftarrow D^{Sum}+U}} (\mathbf{a}' = \widetilde{\mathbf{a}}, \langle \mathbf{a}', \mathbf{s} \rangle \mathbf{z} + \mathbf{e}' = \widetilde{\mathbf{b}})},$$

where $D + U$ is the simplification of $q^{d-1} D_{\mathbb{Z}^d, r_\beta/q^{d-1}} + U(\mathbb{Z}_{q^{d-1}}^d)$ and $D^{Sum} + U$ is the simplification of $q^{d-1} D_{\mathbb{Z}^d, r_\beta}^{Sum, q^{d-1}} + U(\mathbb{Z}_{q^{d-1}}^d)$. We have:

$$\begin{aligned}
R(\mathcal{D}_3 \| \mathcal{D}_2) =& \sum_{\substack{\widetilde{\mathbf{a}} \in \mathbb{Z}_{f(q)}^n \\ \widetilde{\mathbf{b}} \in \mathbb{Z}_{f(q)}^d}} \frac{\frac{1}{f(q)^{2n}} \Pr_{\mathbf{e} \hookleftarrow D+U} (\mathbf{e} = \widetilde{\mathbf{b}} - \langle \widetilde{\mathbf{a}}, \mathbf{s} \rangle \mathbf{z})^2}{\frac{1}{f(q)^n} \Pr_{\mathbf{e}' \hookleftarrow D^{Sum}+U} (\mathbf{e}' = \widetilde{\mathbf{b}} - \langle \widetilde{\mathbf{a}}, \mathbf{s} \rangle \mathbf{z})} \\
=& f(q)^n \cdot \sum_{\widetilde{\mathbf{e}} \in \mathbb{Z}_{f(q)}^d} \frac{\Pr_{\mathbf{e} \hookleftarrow D+U} (\mathbf{e} = \widetilde{\mathbf{e}})^2}{f(q)^n \Pr_{\mathbf{e}' \hookleftarrow D^{Sum}+U} (\mathbf{e}' = \widetilde{\mathbf{e}})} \\
=& \sum_{\widetilde{\mathbf{e}} \in \mathbb{Z}_{f(q)}^d} \frac{\Pr_{\mathbf{e} \hookleftarrow D+U} (\mathbf{e} = \widetilde{\mathbf{e}})^2}{\Pr_{\mathbf{e}' \hookleftarrow D^{Sum}+U} (\mathbf{e}' = \widetilde{\mathbf{e}})} \\
=& R(D_{\mathbb{Z}^d, r_\beta/q^{d-1}} \| D_{\mathbb{Z}^d, r_\beta}^{Sum, q^{d-1}}) \leqslant (1 + 3\varepsilon)^2 \exp\left((5dq^{d-1}) / (2r_\beta) \right),
\end{aligned}$$

where the last inequality relies on the Lemma 12 in Section 3.4. Therefore, when we consider m samples with fixed secret $\mathbf{s}$, the Rényi Divergence, which is denoted as $R_{3,2}$ has an upper bound

$$R_{3,2} \leqslant (1 + 3\varepsilon)^{2m} \exp\left((5dmq^{d-1}) / (2r_\beta) \right).$$

Then we take the randomness of the secret $\mathbf{s}$ into consider. Since the distributions of the secrets in **Hybrid 2** and **Hybrid 3** are identical, $R_\infty(\chi \| \chi) = 1$, and the Rényi Divergence between m samples in **Hybrid 2** and m samples in **Hybrid 3**, which is denoted as $R'_{3,2}$, also has an upper bound as follows.

$$R'_{3,2} \leqslant R_\infty(\chi \| \chi) \cdot R_{3,2} \leqslant (1 + 3\varepsilon)^{2m} \exp\left((5dmq^{d-1}) / (2r_\beta) \right).$$

Therefore, if there exists a polynomial-time adversary who can recover the secret from m samples in **Hybrid 3** with advantage δ'_β, then this adversary can also recover the secret from m samples in **Hybrid 2** with advantage:

$$\delta_{\beta,2} \geqslant \frac{(\delta_\beta)^2}{(1 + 3\varepsilon)^{2m} \exp\left((5dmq^{d-1}) / (2r_\beta) \right)}.$$

In general, we have:

$$\delta'_\beta \geqslant \delta_\beta^4 / \left((1+3\varepsilon)^{6m} \exp\left((19dmq^{d-1})/(2r_\beta)\right)\right).$$

Since $r_\beta/q^{d-1} \geqslant \omega(dm)$, it follows that $\exp\left(19dmq^{d-1}/(2r_\beta)\right) \leqslant \exp(1/\omega(1))$. Moreover, as $\varepsilon \leqslant 2^{-\omega(\log(\kappa))}$ and $m \leqslant \mathsf{poly}(\kappa)$, we have $(1+3\varepsilon)^{6m} = (1+3\varepsilon)^{\frac{1}{3\varepsilon}\cdot 3\varepsilon\cdot 6m} \leqslant e^{3\varepsilon\cdot 6m} = e^{2^{-\omega(\log(\kappa))}} = \mathcal{O}(1)$. Therefore, the claim follows immediately.

In particular, if we set $n = \mathcal{O}(1)$, $d = \mathcal{O}(\kappa)$, $m = \mathcal{O}(\log(\kappa))$, $q = \mathsf{poly}(d)$, $r_\beta \geqslant \mathcal{O}(q^{d-1} d \log(\kappa)^{3/2})$, $\exp\left(19dmq^{d-1}/(2r_\beta)\right) \leqslant \exp\left(\mathcal{O}(1/\log(\kappa)^{1/2})\right)$ and $(1+3\varepsilon)^{6m} \leqslant \mathsf{poly}(\kappa)$. This implies that $\delta'_\beta \geqslant \delta_\beta^4/\mathsf{poly}(\kappa)$. □

C.4 Proof of Lemma 27

In this subsection, we study the reduction from the q-adic IP-MLWE problem to the P-MLWE problem. To realize this reduction, given a q-adic IP-MLWE instance, we need to map it into an instance of polynomial vectors. In this paper, we mainly consider the case $f(x) = x^d + 1$ with d a power of 2.

For convenience in stating lemmas and proofs, we define the following distribution.

Definition 27. *Let q, m, n, d be positive integers, and let $r_\gamma, B > 0$. Let $f(x)$ be a monic irreducible polynomial of degree d such that $f(q) > q^d$. For a fixed $\mathbf{s}(x) \in \mathbb{Z}_q[x]/f$, the distribution $\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,B),f}$ is defined by sampling $(\mathbf{a}, \mathbf{b} = \langle \mathbf{a}, \mathbf{s}\rangle \mathbf{z} + \mathbf{e}) \hookleftarrow \mathcal{F}^{1,n}_{q,\mathbf{s}(q),D+U,f}$[9] and outputting*

$$\left(\mathsf{rot}^{-1} \circ \mathcal{M}\big(\Phi_q^{(f)}(\mathbf{a})\big),\ \sum_{i=0}^{d-1} \Phi_q^{(f)}(b_{d-1-i})_{d-1} x^i\right),$$

where $\mathbf{z} = (1, q, \ldots, q^{d-1})^\top$, $D+U = q^{d-1} D_{\mathbb{Z}^d, r_\gamma, B} + U(\mathbb{Z}^d_{q^{d-1}})$ and $\Phi_q^{(f)}(b_{d-1-i})_{d-1}$ is the $(d-1)$-th coefficient of the polynomial $\Phi_q^{(f)}(b_{d-1-i})$. Here, $\mathsf{rot}^{-1} \circ \mathcal{M}\left(\Phi_q^{(f)}(\mathbf{a})\right)$ means computing $\mathsf{rot}^{-1} \circ \mathcal{M}\left(\Phi_q^{(f)}(a_i)\right)$ for each $i \in [n]$ and concatenating the resulting polynomials into a column vector in order.

If we repeat this sampling m times for the same secret $\mathbf{s}(x)$ and output all samples as one instance, we denote the resulting distribution as $\mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},(r_\gamma,B),f}$.

Since $f(q) = q^d + 1 > q^d$, the map $\Phi_q^{(f)}$ is surjective and $\mathsf{Eval}_q^{(f)}$ is injective, which guarantees that the above distribution is well-defined. Based on this distribution, we proceed to the following lemma.

Lemma 47. *Let κ be the security parameter. For $q = \mathsf{poly}(\kappa)$ a positive integer, $f(x) = x^d + 1$ with d a power of 2, n a positive integer such that $q \geqslant n+1$, r', r_γ two positive numbers satisfying $r_\gamma \geqslant \eta_\varepsilon(\mathbb{Z}^d)$ where $\varepsilon = 2^{-\omega(\log(\kappa))}$, $r_\gamma \geqslant$*

[9] The distribution is formally defined in Definition 23 at the beginning of Section 4.

$\omega\left(2(r'\sqrt{\kappa}n^2+nd)\sqrt{d}\right)$ *and* $q/r_\gamma = \mathsf{poly}(\kappa)$*, we choose* $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r',r'\sqrt{\kappa}})^n$*. Then for this fixed* $\mathbf{s}(x)$*, we have the Rényi divergence*

$$R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}),f}) \leqslant 2\exp\left(\frac{2\pi d c_{max}^2}{r_\gamma^2}+2\right) \leqslant \mathsf{poly}(\kappa),$$

where $c_{max} = 3r'\sqrt{\kappa}n^2 + 18n + 11/2$*.*

Proof. In this case, $\Phi_q^{(f)}$ is surjective and $\mathsf{Eval}_q^{(f)}$ is injective, and the Rényi divergence can be written as follows:

$$R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}),f}) = \sum_{\substack{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n \\ Q(x)\in\mathsf{supp}_{\mathbf{P}(\mathbf{x})}}} R_{term}(\mathbf{P}(x),Q(x)), \tag{33}$$

where

$$\begin{aligned} &R_{term}(\mathbf{P}(x),Q(x)) \\ =&\frac{\Pr\limits_{\substack{\mathbf{a}(x)\hookleftarrow U((\mathbb{Z}_q[x]/f)^n) \\ e(x)\hookleftarrow D_{\mathbb{Z}[x]/(f(x)),r_\gamma,r_\gamma\sqrt{\kappa}}}} \left(\mathbf{a}(x)=\mathbf{P}(x),\langle\mathbf{a}(x),\mathbf{s}(x)\rangle+e(x) \bmod f(x)=Q(x)\right)^2}{\Pr\limits_{\substack{(\mathbf{a}',\mathbf{b}')\hookleftarrow \\ \mathcal{F}^{1,n}_{\mathbf{s}(q),q,D+U,f}}} \left(\mathsf{rot}^{-1}\circ\mathcal{M}\left(\Phi_q^{(f)}(\mathbf{a}')\right)=\mathbf{P}(x),\sum_{i=0}^{d-1}\Phi_q^{(f)}(b'_{d-1-i})_{d-1}x^i=Q(x)\right)}, \end{aligned} \tag{34}$$

$D+U$ follows the definition in the lemma and $\mathsf{supp}_{\mathbf{P}(x)}$ is the support set of $Q(x)$ corresponding to $\mathbf{P}(x)$. In other words, for each $\mathbf{P}(x)$ and given $\mathbf{s}(x)$, we have:

$$\mathsf{supp}_{\mathbf{P}(x)} = \left\{ Q(x) = \langle\mathbf{P}(x),\mathbf{s}(x)\rangle + e(x) \bmod f(q) \middle|\, \mathbf{e}(x) \hookleftarrow D_{\mathbb{Z}[x]/(f(x)),r_\gamma,r_\gamma\sqrt{\kappa}} \right\}.$$

We first consider the denominator of (34). By the definition of the map $\mathcal{M}(\cdot)$, when $f = x^d+1$, $\mathcal{M}(\cdot)$ satisfies $\mathcal{M}(\Phi_q^{(f)}(\mathbf{a}')) = \mathsf{rot}(\Phi_q^{(f)}(\mathbf{a}'))$. In the following part of this proof we will replace $\mathsf{rot}^{-1}\circ\mathcal{M}\left(\Phi_q^{(f)}(\mathbf{a}')\right)$ with $\Phi_q^{(f)}(\mathbf{a}')$.

In Equation (34), we have the probability:

$$\begin{aligned} &\Pr_{(\mathbf{a}',\mathbf{b}')\hookleftarrow\mathcal{F}^{1,n}_{\mathbf{s}(q),q,D+U,f}}\left(\Phi_q^{(f)}(\mathbf{a}')=\mathbf{P}(x),\sum_{i=0}^{d-1}\Phi_q^{(f)}(b'_{d-1-i})_{d-1}x^i=Q(x)\right) \\ =&\sum\nolimits_{\mathbf{a}':\Phi_q^{(f)}(\mathbf{a}')=\mathbf{P}(x)}\left(\Pr\left(\Phi_q^{(f)}(\mathbf{a}')=\mathbf{P}(x)\right)\right. \\ &\left.\times\Pr_{\mathbf{e}'\hookleftarrow D+U}\left(\sum_{i=0}^{d-1}\Phi_q^{(f)}(b'_{d-1-i})_{d-1}x^i=Q(x)\middle|\,\Phi_q^{(f)}(\mathbf{a}')=\mathbf{P}(x)\right)\right). \end{aligned} \tag{35}$$

We now explain the presence of the summation over $\mathbf{a}'$. As noted at the beginning of the proof, $\Phi_q^{(f)}$ is surjective; therefore, multiple $\mathbf{a}'$'s may satisfy $\Phi_q^{(f)}(\mathbf{a}') = \mathbf{P}(x)$. We set $\mathbf{a}'_{\mathbf{P}} = \mathsf{Eval}_q^{(f)}(\mathbf{P}(x))$. Then $\mathbf{a}' = \mathbf{a}'_{\mathbf{P}}$ implies $\Phi_q^{(f)}(\mathbf{a}') = \Phi_q^{(f)}(\mathbf{a}'_{\mathbf{P}}) = \Phi_q^{(f)}(\mathsf{Eval}_q^{(f)}(\mathbf{P}(x))) = \mathbf{P}(x)$ due to Lemma 18 in Section 3.6. Therefore we obtain:

$$
\begin{aligned}
(35) &\geqslant \Pr_{\mathbf{a}' \hookleftarrow U(\mathbb{Z}_{f(q)}^n)}(\mathbf{a}' = \mathbf{a}'_{\mathbb{P}}) \Pr_{\mathbf{e}' \hookleftarrow D+U} \left(\sum_{i=0}^{d-1} \Phi_q^{(f)}(b'_{d-1-i})_{d-1} x^i = Q(x) \middle| \mathbf{a}' = \mathbf{a}'_{\mathbf{P}} \right), \\
&= \Pr_{\mathbf{e}' \hookleftarrow D+U} \left(\sum_{i=0}^{d-1} \Phi_q^{(f)}(b'_{d-1-i})_{d-1} x^i = Q(x) \middle| \mathbf{a}' = \mathbf{a}'_{\mathbf{P}} \right) \Big/ f(q)^n.
\end{aligned} \tag{36}
$$

We next consider the polynomial $Q(x) = \sum_{i=0}^{d-1} \Phi_q^{(f)}(b'_{d-1-i})_{d-1} x^i$. Here $\mathbf{b}' = \langle \mathbf{a}'_{\mathbf{P}}, \mathbf{s}(q) \rangle \mathbf{z} + \mathbf{e}'$, where $\mathbf{e}' = q^{d-1}\mathbf{e}'_{(1)} + \mathbf{e}'_{(2)}$ with $\mathbf{e}'_{(1)} \hookleftarrow D_{\mathbb{Z}^d, r_\gamma, r_\gamma\sqrt{\kappa}+c_{\max}}$ and $\mathbf{e}'_{(2)} \hookleftarrow U(\mathbb{Z}_{q^{d-1}}^d)$. By Lemma 46 in Supplementary Material C.2, we obtain:

$$
\begin{aligned}
&\Phi_q^{(f)}(b_{d-1-i} - \langle \mathbf{a}'_{\mathbf{P}}, \mathbf{s}(q) \rangle q^{d-1-i}) = \Phi_q^{(f)}(e'_{d-1-i}) \\
=&\Phi_q^{(f)}(b'_{d-1-i}) + \langle \Phi_q^{(f)}(\mathbf{a}'_{\mathbf{P}}), \Phi_q^{(f)}(-\mathbf{s}(q)) \rangle x^{d-1-i} + c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i}) \bmod (q, f(x)) \\
=&\Phi_q^{(f)}(b'_{d-1-i}) - \langle \mathbf{P}(x), \mathbf{s}(x) \rangle x^{d-1-i} + c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i}) \bmod (q, f(x))
\end{aligned}
$$

for some carry term $c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i})$. By Lemma 46 in Supplementary Material C.2, the term $c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i})$ admits a decomposition $c^{**}_{d-1-i,(I)}(x) + c^{**}_{d-1-i,(II)}(x)$, where $c^{**}_{d-1-i,(I)}(x)$ satisfies $\|c^{**}_{d-1-i,(I)}(x)\|_\infty \leqslant 6$, while $c^{**}_{d-1-i,(II)}(x)$ is independent of b'_{d-1-i} and satisfies $\|c^{**}_{d-1-i,(II)}(x)\|_\infty \leqslant 3r'\sqrt{\kappa}n^2 + 18n - \frac{1}{2}$.

It directly follows that

$$
\Phi_q^{(f)}(b'_{d-1-i}) = \langle \mathbf{P}(x), \mathbf{s}(x) \rangle x^{d-1-i} + \Phi_q^{(f)}(e'_{d-1-i}) - c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i}) \bmod (q, f(x)).
$$

By definition, the $(d-1)$-th coefficient of $\langle \mathbf{P}(x), \mathbf{s}(x) \rangle x^{d-1-i} \bmod (q, f(x))$ coincides with the i-th coefficient of $\langle \mathbf{P}(x), \mathbf{s}(x) \rangle \bmod (q, f(x))$. Moreover, the $(d-1)$-th coefficient of $\Phi_q^{(f)}(e'_{d-1-i})$ equals the $(d-1-i)$-th entry of $\mathbf{e}'_{(1)}$, which is distributed according to $D_{\mathbb{Z}, r_\gamma, r_\gamma\sqrt{\kappa}+c_{\max}}$.

With the analysis above, we can rewrite $Q(x) = \sum_{i=0}^{d-1} \Phi_q^{(f)}(b'_{d-1-i})_{d-1} x^i \bmod f(x)$ as:

$$
Q(x) = \langle \mathbf{P}(x), \mathbf{s}(x) \rangle + \overline{e}'(x) + \overline{c}(x) \bmod f(x),
$$

where $\overline{e}'(x)$ is the polynomial whose i-th coefficient equals the $(d-1)$-th coefficient of $\Phi_q^{(f)}(e'_{d-1-i})$, and $\overline{c}(x)$ is the polynomial whose i-th coefficient is given by the $(d-1)$-th coefficient of $-c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i})$. By the properties of $\Phi_q^{(f)}(e'_{d-1-i})$ for all $i \in [d-1]$, the polynomial $\overline{e}'(x)$ follows the distribution $D_{\mathbb{Z}[x]/f, r_\gamma, r_\gamma\sqrt{\kappa}+c_{max}}$. By the properties of $c^{**}_{d-1-i}(\mathbf{a}'_{\mathbf{P}}, b'_{d-1-i})$ for all $i \in [d-1]$, the polynomial $\overline{c}(x)$ can be decomposed as $\overline{c}_{(I)}(x) + \overline{c}_{(II)}(x)$. Here, $\overline{c}_{(I)}(x)$ satisfies $\|\overline{c}_{(I)}(x)\|_\infty \leqslant 6$, while $\overline{c}_{(II)}(x)$ is independent of $Q(x)$ and satisfies $\|\overline{c}_{(II)}(x)\|_\infty \leqslant 3r'\sqrt{\kappa}n^2 + 18n - \frac{1}{2}$. In the other word, given a fixed $\mathbf{P}(x)$, $\overline{c}_{(II)}(x)$ is fixed. Then the inequality in (36) can be rewritten as follows:

$$
(35) \geqslant \Pr_{\overline{e}'(x) \hookleftarrow D_{\mathbb{Z}[x]/f, r_\gamma, r_\gamma\sqrt{\kappa}+c_{max}}} (\langle \mathbf{P}(x), \mathbf{s}(x) \rangle + \overline{e}'(x) + \overline{c}(x) \bmod f(x) = Q(x)) \Big/ f(q)^n.
$$

On the other side, the numerator of (34) can be written as follows:

$$
\begin{aligned}
&\Pr_{\substack{\mathbf{a}(x)\hookleftarrow U((\mathbb{Z}_q[x]/f)^n)\\ e(x)\hookleftarrow D_{\mathbb{Z}[x]/(f(x)),r_\gamma,r_\gamma\sqrt{\kappa}}}}(\mathbf{a}(x)=\mathbf{P}(x),\langle\mathbf{a}(x),\mathbf{s}(x)\rangle+e(x) \bmod f(x)=Q(x))\\
=&\Pr_{\mathbf{a}(x)\hookleftarrow U((\mathbb{Z}_q[x]/f)^n)}(\mathbf{a}(x)=\mathbf{P}(x))\\
&\times\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}}}(\langle\mathbf{P}(x),\mathbf{s}(x)\rangle+e(x) \bmod f(x)=Q(x))\\
=&\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}}}(\langle\mathbf{P}(x),\mathbf{s}(x)\rangle+e(x) \bmod f(x)=Q(x))\Big/q^{nd}.
\end{aligned}
$$

Therefore, $R_{term}(\mathbf{P}(x),Q(x))$ can be upper bounded as follows:

$$
\begin{aligned}
&R_{term}(\mathbf{P}(x),Q(x))\\
\leqslant&\frac{\left(\frac{1}{q^{nd}}\right)^2\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}}}(\langle\mathbf{P}(x),\mathbf{s}(x)\rangle+e(x) \bmod f(x)=Q(x))^2}{\frac{1}{f(q)^n}\Pr_{\overline{e}'(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}}}(\langle\mathbf{P}(x),\mathbf{s}(x)\rangle+\overline{e}'(x)+\overline{c}(x) \bmod f(x)=Q(x))}\\
=&\frac{f(q)^n}{q^{2nd}}\frac{\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}}}(\langle\mathbf{P}(x),\mathbf{s}(x)\rangle+e(x) \bmod f(x)=Q(x))^2}{\Pr_{\overline{e}'(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}}}(\langle\mathbf{P}(x),\mathbf{s}(x)\rangle+\overline{e}'(x)+\overline{c}(x) \bmod f(x)=Q(x))}.
\end{aligned}
\tag{37}
$$

We make the following change of variables: let $\overline{e}^*(x)=Q(x)-\langle\mathbf{P}(x),\mathbf{s}(x)\rangle \bmod (q,f(x))$. For fixed $\mathbf{P}(x)$ and $Q(x)$, $\overline{e}^*(x)$ is fixed as well. Therefore, the upper bound in formula (37) can be rewritten as follows:

$$
\begin{aligned}
&\frac{f(q)^n}{q^{2nd}}\frac{\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}}}\left(e(x)=\overline{e}^*(x)\right)^2}{\Pr_{\overline{e}'(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}}}\left(\overline{e}'(x)+\overline{c}(x)=\overline{e}^*(x)\right)}\\
=&\frac{f(q)^n}{q^{2nd}}\frac{\Pr_{e(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}}}\left(e(x)=\overline{e}^*(x)\right)^2}{\Pr_{\overline{e}'(x)\hookleftarrow D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}}}\left(\overline{e}'(x)+\overline{c}_{(I)}(x)+\overline{c}_{(II)}(x)=\overline{e}^*(x)\right)}\\
=&\frac{f(q)^n}{q^{2nd}}\frac{D_{\mathbb{Z}^n,r_\gamma,r_\gamma\sqrt{\kappa}}(\overline{\mathbf{e}}^*)^2}{D_{\mathbb{Z}^n,r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}}\left(\overline{\mathbf{e}}^*-\overline{\mathbf{c}}_{(I)}-\overline{\mathbf{c}}_{(II)}\right)}\\
=&\frac{f(q)^n\rho_{r_\gamma}\left(\mathbb{Z}^d\cap(-r_\gamma\sqrt{\kappa}-c_{max},r_\gamma\sqrt{\kappa}+c_{max}]^d\right)}{q^{2nd}\rho_{r_\gamma}\left(\mathbb{Z}^d\cap(-r_\gamma\sqrt{\kappa},r_\gamma\sqrt{\kappa}]^d\right)^2}\cdot\frac{\exp\left(-\frac{2\pi}{r_\gamma^2}\|\overline{\mathbf{e}}^*\|^2\right)}{\exp\left(-\frac{\pi}{r_\gamma^2}\|\overline{\mathbf{e}}^*-\overline{\mathbf{c}}_{(I)}-\overline{\mathbf{c}}_{(II)}\|^2\right)},
\end{aligned}
\tag{38}
$$

where $\overline{\mathbf{e}}^*$, $\overline{\mathbf{c}}_{(I)}$ and $\overline{\mathbf{c}}_{(II)}$ are the coefficient vectors of $\overline{e}^*(x)$, $\overline{c}_{(I)}(x)$ and $\overline{c}_{(II)}(x)$. Since for a fixed $\mathbf{P}(x)$, $\overline{c}_{(II)}(x)$ is fixed, then $\overline{\mathbf{c}}_{(II)}$ is fixed under a fixed $\mathbf{P}(x)$.

By Corollary 1 (Section 3.4), the formula (38) can be bounded from above by

$$\frac{f(q)^n(1+2^{-\omega(\log(\kappa))})}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\cdot\frac{\exp\left(-\frac{2\pi}{r_\gamma^2}\|\overline{\mathbf{e}}^*\|^2\right)}{\exp\left(-\frac{\pi}{r_\gamma^2}\|\overline{\mathbf{e}}^*-\overline{\mathbf{c}}_{(I)}-\overline{\mathbf{c}}_{(II)}\|^2\right)}.$$

By Lemma 31 in Supplementary Material B.1, the above upper bound on $R_{\text{term}}(\mathbf{P}(x),Q(x))$ can be rewritten as follows:

$$\frac{f(q)^n(1+2^{-\omega(\log(\kappa))})}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\cdot\frac{\exp\left(-\frac{\pi}{r_\gamma^2}\left\|\overline{\mathbf{e}}^*+\overline{\mathbf{c}}_{(I)}+\overline{\mathbf{c}}_{(II)}\right\|^2\right)}{\exp\left(-\frac{2\pi}{r_\gamma^2}\left\|\overline{\mathbf{c}}_{(I)})+\overline{\mathbf{c}}_{(II)})\right\|^2\right)}.$$

Then we go back to formula (33) and consider the upper bound of Rényi divergence $R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}),f})$. We have:

$$R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s}(x),r_\gamma,f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f})=\sum_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n}\Big(\sum_{Q(x)\in\mathsf{supp}_{\mathbf{P}(x)}}R_{term}(\mathbf{P}(x),Q(x))\Big)$$

$$=\sum_{\mathbf{P}(x)\in(\mathbb{Z}[x]/f)^n}\Big(\sum_{\substack{\overline{e}^*(x)\in\mathbb{Z}_q[x]/f,\\ \|\overline{e}^*(x)\|_\infty\leqslant r_\gamma\sqrt{\kappa}}}R_{term}(\mathbf{P}(x),\overline{e}^*(x)+\langle\mathbf{P}(x),\mathbf{s}(x)\rangle \bmod (q,f(x)))\Big)$$

$$\leqslant\frac{f(q)^n(1+2^{-\omega(\log(\kappa))})}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\sum_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n}\left(\sum_{\overline{\mathbf{e}}^*\in\mathbb{Z}^d}\frac{\exp\left(-\frac{\pi}{r_\gamma^2}\left\|\overline{\mathbf{e}}^*+\overline{\mathbf{c}}_{(I)}+\overline{\mathbf{c}}_{(II)}\right\|^2\right)}{\exp\left(-\frac{2\pi}{r_\gamma^2}\left\|\overline{\mathbf{c}}_{(I)})+\overline{\mathbf{c}}_{(II)})\right\|^2\right)}\right).$$

According to Lemma 46 in Supplementary Material C.2, $\|\overline{\mathbf{c}}_{(I)}+\overline{\mathbf{c}}_{(II)}\|_\infty\leqslant 3r'\sqrt{\kappa}n^2+18n+\frac{11}{2}$. The right hand of this inequality is exactly c_{max} in the statement of this lemma, and it follows that

$$1\Big/\exp\left(-\frac{2\pi}{r_\gamma^2}\left\|\overline{\mathbf{c}}_{(I)}+\overline{\mathbf{c}}_{(II)}\right\|^2\right)\leqslant\exp\left(\frac{2\pi d}{r_\gamma^2}c_{max}^2\right).$$

Therefore, we have:

$$\begin{aligned}&R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f}\|\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}),f})\\ \leqslant&\frac{f(q)^n(1+2^{-\omega(\log(\kappa))})}{q^{2nd}\rho_{r_\gamma}(\mathbb{Z}^d)}\cdot\exp\left(\frac{2\pi d}{r_\gamma^2}c_{max}^2\right)\\ &\times\sum_{\mathbf{P}(x)\in(\mathbb{Z}_q[x]/f)^n}\sum_{\overline{\mathbf{e}}^*\in\mathbb{Z}^d}\exp\left(-\frac{\pi}{r_\gamma^2}\left\|\overline{\mathbf{e}}^*+\left(\overline{\mathbf{c}}_{(I)}+\overline{\mathbf{c}}_{(II)}\right)\right\|^2\right),\end{aligned}$$

where $c_{max}=3r'\sqrt{\kappa}n^2+18n+\frac{11}{2}$. For a fixed $\mathbf{P}(x)$, in other words, given $\overline{\mathbf{c}}_{(II)}$ fixed, we compute the following summation:

$$\sum_{\mathbf{e}\in\mathbb{Z}^d}\exp\left(-\frac{\pi}{r_\gamma^2}\left\|\overline{\mathbf{e}}^*+\left(\overline{\mathbf{c}}_{(I)}+\overline{\mathbf{c}}_{(II)}\right)\right\|^2\right)=\prod_{i=0}^{d-1}\sum_{\overline{e}_i^*\in\mathbb{Z}}\exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^*+\overline{c}_{(I),i}+\overline{c}_{(II),i})^2\right).\tag{39}$$

By Lemma 46, we have $|\overline{c}_{(I),i}| \leqslant 2 + 4\|f\|_\infty = 6$. Therefore, for each $\overline{e}_i^* > -\overline{c}_{(II),i} + 6$, we have:

$$\exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i})^2\right) \leqslant \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* - 6 + \overline{c}_{(II),i})^2\right),$$

while for each $\overline{e}_i^* < -\overline{c}_{(II),i} - 6$, we have:

$$\exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i})^2\right) \leqslant \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + 6 + \overline{c}_{(II),i})^2\right).$$

Therefore, considering the summation over $\overline{e}_i^*$ in formula (39), we have:

$$\begin{aligned}
&\sum_{\overline{e}_i^* \in \mathbb{Z}} \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i})^2\right) \\
\leqslant &\sum_{\overline{e}_i^* \in \mathbb{Z} \cap [-\overline{c}_{(II),i} - 6, -\overline{c}_{(II),i} + 6]} \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i})^2\right) \\
&+ \sum_{\overline{e}_i^* \in \mathbb{Z} \cap (-\overline{c}_{(II),i} + 6, +\infty)} \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* - 6 + \overline{c}_{(II),i})^2\right) \\
&+ \sum_{\overline{e}_i^* \in \mathbb{Z} \cap (-\infty, -\overline{c}_{(II),i} - 6)} \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + 6 + \overline{c}_{(II),i})^2\right).
\end{aligned} \tag{40}$$

Since the sum of the last two terms in formula (40) is smaller than $\rho_{r_\gamma}(\mathbb{Z} + \overline{c}_{(II),i})$, which can be readily obtained via a variable substitution, we conclude that

$$\sum_{e_i \in \mathbb{Z}} \exp\left(-\frac{\pi}{r_\gamma^2}(\overline{e}_i^* + \overline{c}_{(I),i} + \overline{c}_{(II),i})^2\right) \leqslant 12 + \rho_{r_\gamma}\left(\mathbb{Z} + \overline{c}_{(II),i}\right).$$

Returning to formula (39), we deduce that:

$$\begin{aligned}
&\sum\nolimits_{\mathbf{e} \in \mathbb{Z}^d} \exp\left(-\frac{\pi}{r_\gamma^2}\left\|\overline{\mathbf{e}}^* + \left(\overline{\mathbf{c}}_{(I)} + \overline{\mathbf{c}}_{(II)}\right)\right\|^2\right) \\
\leqslant &\prod\nolimits_{i=0}^{d-1}\left(12 + \rho_{r_\gamma}(\mathbb{Z} + \overline{c}_{(II),i})\right).
\end{aligned} \tag{41}$$

Furthermore, we have the following inequality:

$$\frac{\left(12 + \rho_{r_\gamma}(\mathbb{Z} + \overline{c}_{(II),i})\right)^d}{\rho_{r_\gamma}(\mathbb{Z}^d)} \leqslant \left(12/\rho_{r_\gamma}(\mathbb{Z}) + 1 + 3\varepsilon\right)^d = \left(\frac{12 + 3\varepsilon \cdot \rho_{r_\gamma}(\mathbb{Z})}{\rho_{r_\gamma}(\mathbb{Z})} + 1\right)^d,$$

where $\varepsilon = 2^{-\omega(\log \kappa)}$ denotes the parameter associated with the smoothing parameter $\eta_\varepsilon(\mathbb{Z})$, and the inequality follows from Lemma 11 in Section 3.4. By Lemma 9 in Section 3.4, we have:

$$3\varepsilon \cdot \rho_{r_\gamma}(\mathbb{Z}) \leqslant 3\varepsilon(1+\varepsilon) \cdot r_\gamma = 2^{-\omega(\log(\kappa))},$$

hence we have:

$$\frac{\left(12+\rho_{r_\gamma}(\mathbb{Z}+\overline{c}_{(II),i})\right)^d}{\rho_{r_\gamma}(\mathbb{Z}^d)} \leqslant \left(\frac{13}{\rho_{r_\gamma}(\mathbb{Z})}+1\right)^d$$
$$\leqslant \left(\frac{13}{r_\gamma(1-\varepsilon)}+1\right)^d \leqslant \left(\frac{14}{r_\gamma}+1\right)^d,$$

where the second inequality follows from Lemma 9 in Section 3.4. Therefore, when $r_\gamma \geqslant 14d$, the formula above has an upper bound e. Hence we have:

$$R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}),f})$$
$$\leqslant \frac{2f(q)^n \cdot e \cdot q^{nd}}{q^{2nd}} \exp\left(\frac{2\pi d}{r_\gamma^2}c_{max}^2\right) = \frac{2ef(q)^n}{q^{nd}} \exp\left(\frac{2\pi d}{r_\gamma^2}c_{max}^2\right).$$

For the term $f(q)^n/q^{nd}$, we have:

$$\frac{f(q)^n}{q^{nd}} = \frac{(q^d+1)^n}{q^{nd}} = \left(\frac{1}{q^d}+1\right)^n \leqslant e, \tag{42}$$

where the last inequality holds because $q^d > n$. This allows us to bound the Rényi divergence as follows:

$$R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}+c_{max}),f}) \leqslant 2e^2 \exp\left(\frac{2\pi d}{r_\gamma^2}c_{max}^2\right).$$

When $r_\gamma \geqslant \omega(\sqrt{d}\cdot c_{max})$, $\exp\left(2\pi d \cdot c_{max}^2/r_\gamma^2\right) \leqslant \exp(1/\omega(1))$. According to our parameter selection, this condition is satisfied, and the desired result follows. □

Corollary 4. *Let κ be the security parameter. Let $q = \mathsf{poly}(\kappa)$ be a positive integer, $f = x^d + 1$ with d a power of 2. Let $m = \mathcal{O}(\log(\kappa))$, an integer $n = \mathcal{O}(1)$. Let r', r_γ be two positive numbers satisfying $r_\gamma \geqslant \eta_\varepsilon(\mathbb{Z}^d)$ where $\varepsilon = 2^{-\omega(\log(\kappa))}$, $r_\gamma \geqslant \omega\left((r'\sqrt{\kappa}n^2+nd)\sqrt{dm}\right)$ and $\frac{q}{r_\gamma\sqrt{\kappa}} = \mathsf{poly}(\kappa)$, $\frac{q}{r'\sqrt{\kappa}} = \mathsf{poly}(\kappa)$. There exists a polynomial-time reduction from Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ problem to Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',r_\gamma,f}$ problem, where $D_{r'}(q)$ denotes the distribution that samples the secret $\mathbf{s}(x) \hookleftarrow \left(D_{\mathbb{Z}[x]/f,\,r'}\right)^n$ and outputs $\mathsf{Eval}_q^{(f)}(\mathbf{s}(x))$, $D + U = q^{d-1}D_{\mathbb{Z}^d,r_\gamma} + U(\mathbb{Z}^d_{q^{d-1}})$. If there is a poly-time adversary for solving Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,r',r_\gamma,f}$ problem with advantage $\delta_{\gamma,3}$, then there exists a polynomial time adversary for solving Search q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r'}(q),D+U,f}$ problem with the advantage $\delta_{\gamma,2}$ being at least*

$$\delta_{\gamma,3}^2/\left((2e^2)^m \exp\left(2\pi dmc_{max}^2/r_\gamma^2\right)\right) - 2^{-\omega(\log(\kappa))},$$

where $c_{max} = 3r'\sqrt{\kappa}n^2 + 18n + 11/2$.

Proof. In order to connect with the preceding result, we now consider the reduction from the Search q-*adic* $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r',r'\sqrt{\kappa}}(q),D'+U,f}$ problem to the

Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,(r',r'\sqrt{\kappa}),(r_\gamma,r_\gamma\sqrt{\kappa}),f}$ problem. Here, $D_{r',r'\sqrt{\kappa}}(q)$ denotes the distribution that samples the secret $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r',r'\sqrt{\kappa}})^n$ and outputs $\mathbf{s}(q)$ mod $f(q)$, while $D' + U = q^{d-1} D_{\mathbb{Z}^d, r_\gamma, r_\gamma + c_{\max}} + U(\mathbb{Z}^d_{q^{d-1}})$. On the other hand, in the Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,(r',r'\sqrt{\kappa}),(r_\gamma,r_\gamma\sqrt{\kappa}),f}$ problem, the secret terms and error terms are drawn from $(D_{\mathbb{Z}[x]/f,r',r'\sqrt{\kappa}})^n$ and $(D_{\mathbb{Z}[x]/f,r_\gamma,r_\gamma+c_{\max}})^m$, respectively.

Compared with the reduction in the statement of this corollary, the difference lies in replacing the discrete Gaussian distribution with its bounded variant. By Lemma 15 in Section 3.4, the loss in advantage caused by this replacement is at most $2^{-\omega(\log(\kappa))}$.

We consider the Rényi divergence for a fixed secret $\mathbf{s}$. Let us denote the distribution consisting of m samples from $\mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f}$ by $\mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},r_\gamma,f}$. Relying on Lemma 47 in this subsection, we then obtain:

$$\begin{aligned} & R(\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f} \| \mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},r_\gamma,f}) \\ =& R(\mathsf{P\text{-}MLWE}^{1,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f} \| \mathcal{D}\text{-}\mathsf{con}^{1,n}_{q,\mathbf{s},r_\gamma,f})^m \\ \leqslant & (2e^2)^m \exp\left(\frac{2\pi d m c^2_{max}}{r^2_\gamma}\right). \end{aligned}$$

Since for each $\mathbf{s}(x) \hookleftarrow \left(D_{\mathbb{Z}[x]/f,r',r'\sqrt{\kappa}}\right)^n$, we have $\Phi^{(f)}_q\left(\mathsf{Eval}^{(f)}_q(\mathbf{s}(x))\right) = \mathbf{s}(x)$ by Lemma 42 in Supplementary Material B.4, it follows that

$$R_\infty\left((D_{\mathbb{Z}[x]/f,r',r'\sqrt{\kappa}})^n \,\|\, \Phi^{(f)}_q(D_{r',r'\sqrt{\kappa}}(q))\right) = 1,$$

where $\Phi^{(f)}_q(D_{r',r'\sqrt{\kappa}}(q))$ denotes the distribution that selects $\mathbf{s} \hookleftarrow D_{r',r'\sqrt{\kappa}}(q)$ and outputs $\Phi^{(f)}_q(\mathbf{s})$.

With the above preparations, we can analyze the Rényi divergence accounting for the randomness of the secret $\mathbf{s}$, denoted by R_1. By Lemma 4 in Section 3.3, it can be bounded as:

$$\begin{aligned} R_1 \leqslant & R_\infty\left((D_{\mathbb{Z}[x]/f,r',r'\sqrt{\kappa}})^n \,\|\, \Phi^{(f)}_q(D_{r',r'\sqrt{\kappa}}(q))\right) \\ & \cdot \max_{\mathbf{s}} R(\mathsf{P\text{-}MLWE}^{m,n}_{q,\mathbf{s},(r_\gamma,r_\gamma\sqrt{\kappa}),f} \| \mathcal{D}\text{-}\mathsf{con}^{m,n}_{q,\mathbf{s},r_\gamma,f}) \\ \leqslant & (2e^2)^m \exp\left(2\pi d m c^2_{max}/r^2_\gamma\right). \end{aligned} \tag{43}$$

Given an q-adic $\mathsf{IP\text{-}MLWE}$ instance, we first transform it into a $\mathcal{D}\text{-}\mathsf{con}$ instance and provide this instance to the adversary for Search $\mathsf{P\text{-}MLWE}^{m,n}_{q,(r',r'\sqrt{\kappa}),(r_\gamma,r_\gamma\sqrt{\kappa}),f}$. Suppose the adversary achieves an advantage of at least $\delta_{\gamma,2}$. Then, by formula (43), we can recover the secret with an advantage of at least

$$\frac{\delta^2_{\gamma,2}}{(2e^2)^m \exp\left(2\pi d m c^2_{\max}/r^2_\gamma\right)}.$$

When $r_\gamma \geqslant \omega(\sqrt{dm} \cdot c_{max})$, $m \leqslant \mathcal{O}(\log(\kappa))$, we have $\exp\left(2\pi m d \cdot c^2_{max}/r^2_\gamma\right) \leqslant \exp(1/\omega(1))$ and $(2e^2)^m \leqslant \mathsf{poly}(\kappa)$. According to our parameter selection, this condition is satisfied. Therefore, the secret of a q-adic $\mathsf{IP\text{-}MLWE}^{m,n}_{q,D_{r',r'\sqrt{\kappa}}(q),D+U,f}$ instance can also be recovered immediately, and the result follows. □

D Supplementary Materials for Reduction from MLWE to G-IP-M-EDCP

D.1 Invertible Submatrix in the Matrix $\mathbf{A}(x) \in (\mathcal{O}_K/q\mathcal{O}_K)^{m\times n}$

We begin by recalling the probability that a random matrix $\mathbf{A}$, defined over a ring of integers, contains an invertible submatrix.

Lemma 48 ([BJRLW23, Lemma 2.6]). *Let K be a number field, whose extension index over $\mathbb{Q}$ is d, and $\mathcal{O}_K$ be its ring of integers. Let q be a prime integer that is unramified in $\mathcal{O}_K$ which splits as $\langle q\rangle = \prod_{i\in[k]}\mathfrak{p}_i$, where $k \leqslant d$ is the number of all prime ideals split from q. Let $m \geqslant n$ be two integers. It holds*

$$\Pr_{\mathbf{A}(x)\xleftarrow{\$}U((\mathcal{O}_K/q\mathcal{O}_K)^{n\times m})}(\mathbf{A}(x)\cdot(\mathcal{O}_K/q\mathcal{O}_K)^m = (\mathcal{O}_K/q\mathcal{O}_K)^n) \geqslant \prod_{l=0}^{n-1}\prod_{i\in[k]}\left(1-\frac{1}{\mathcal{N}(\mathfrak{p}_i)^{m-l}}\right).$$

The following conclusion is claimed in [BJRLW23] without a proof. For completeness, we provide a detailed proof here.

Corollary 5. *Let K be a number field, whose extension index over $\mathbb{Q}$ is d, and $\mathcal{O}_K$ be its ring of integers. Let q be a prime integer that is unramified in $\mathcal{O}_K$ which splits as $\langle q\rangle = \prod_{i\in[k]}\mathfrak{p}_i$, where $k \leqslant d$ is the number of all prime ideals above q. Let $m \geqslant n$ be two integers. If q splits into only high-norm ideal factors so that $\min_{i\in[k]}\mathcal{N}(\mathfrak{p}_i) \geqslant (nd)^{\omega(1/(m-n+1))}$, the probability satisfies*

$$\Pr_{\mathbf{A}(x)\xleftarrow{\$}U((\mathcal{O}_K/q\mathcal{O}_K)^{n\times m})}(\mathbf{A}(x)\cdot(\mathcal{O}_K/q\mathcal{O}_K)^m = (\mathcal{O}_K/q\mathcal{O}_K)^n) \geqslant 1-2^{-\omega(\log(nd))}.$$

Proof. We have:

$$\begin{aligned}\prod_{l=0}^{n-1}\prod_{i\in[k]}\left(1-\frac{1}{\mathcal{N}(\mathfrak{p}_i)^{m-l}}\right) &\geqslant \prod_{i\in[k]}\left(1-\frac{1}{\mathcal{N}(\mathfrak{p}_i)^{m-n+1}}\right)^n\\ &\geqslant \left(1-\frac{1}{(nd)^{\omega(1)}}\right)^{nd} \geqslant \frac{1}{e^{(nd)/(nd)^{\omega(1)}}}.\end{aligned}$$

Due to Taylor series of e^x, $e^{(nd)/(nd)^{\omega(1)}} = 1+(nd)/(nd)^{\omega(1)}+o((nd)/(nd)^{\omega(1)})$. Therefore, $1-(1/e)^{(nd)/(nd)^{\omega(1)}} = (nd)/(nd)^{\omega(1)}+o((nd)/(nd)^{\omega(1)}) = 2^{-\omega(\log(nd))}$. The result follows. □

D.2 Regularity Lemma

We first recall the following regularity result over rings.

Lemma 49 ([LPR13, Corollary 7.5]). *Let $\mathcal{O}_K$ be the ring of integer in the d'-th cyclotomic number field K of degree d, and $q \geqslant 2$ an integer. For positive integer $n < m \leqslant \mathsf{poly}(n)$, let $\mathbf{A}(x) = (\mathbf{I}_n|\,\mathbf{A}'(x))$, where $\mathbf{A}'(x) \hookleftarrow U((\mathcal{O}_K/q\mathcal{O}_K)^{n\times(m-n)})$, $\mathbf{e}(x) \hookleftarrow (D^{\mathbb{H}}_{\mathcal{O}_K,r})^m$ where $r \geqslant 2d\cdot q^{\frac{n}{m}+\frac{2}{dm}}$, with probability $1-2^{-\Omega(d)}$ over the choice of $\mathbf{A}'(x)$, we have:*

$$\Delta((\mathbf{A}(x),\mathbf{A}(x)\mathbf{e}(x)),(\mathbf{A}(x),U((\mathcal{O}_K/q\mathcal{O}_K)^n))) \leqslant 2^{-\Omega(d)}.$$

With Lemma 48 and 49, we can get the following corollary.

Corollary 6. *Let $\mathcal{O}_K$ be the ring of integer in the d'-th cyclotomic number field K of degree d. Let m, n be positive integers such that $n < m \leqslant \mathsf{poly}(n)$ and $m' > 1$ be any positive integer. Let $q \geqslant 2$ a prime that is unramified over the ring $\mathcal{O}_K$,which splits into $\mathfrak{p}_i$'s so that $\min_{i\in[k]} \mathcal{N}(\mathfrak{p}_i) \geqslant (nd)^{\omega(1/(m-n+1))}$. The following two distributions have statistical distance $\Delta(\mathcal{D}_1, \mathcal{D}_2) \leqslant 2^{-\Omega(d)}$:*

$$\mathcal{D}_1 = \left\{ (\mathbf{A}(x), \mathbf{E}(x)\mathbf{A}(x)) \,\middle|\, \mathbf{A}(x) \xleftarrow{\$} U\left((\mathcal{O}_K/q\mathcal{O}_K)^{m\times n}\right), \mathbf{E}(x) \hookleftarrow (D^{\mathbb{H}}_{\mathcal{O}_K,r})^{m\times m'} \right\},$$
$$\mathcal{D}_2 = \left\{ (\mathbf{A}(x), \mathbf{B}(x)) \,\middle|\, \mathbf{A}(x) \xleftarrow{\$} U\left((\mathcal{O}_K/q\mathcal{O}_K)^{m\times n}\right), \mathbf{B} \xleftarrow{\$} U((\mathcal{O}_K/q\mathcal{O}_K)^{m'\times n}) \right\}.$$

Proof. By the choice of q and Corollary 5 in Supplementary Material D.1, if $\mathbf{A}(x) \xleftarrow{\$} U((\mathcal{O}_K/q\mathcal{O}_K)^{m\times n})$, then with probability at least $1 - 2^{-\omega(\log(nd))}$ over the randomness of $\mathbf{A}(x)$, we have $(\mathcal{O}_K/q\mathcal{O}_K)^m \cdot \mathbf{A}(x) = (\mathcal{O}_K/q\mathcal{O}_K)^n$. Assuming $\mathbf{A}(x)$ satisfies this condition, there exists a row-permutation matrix $\mathbf{U}$ such that $\mathbf{UA}(x)$ can be written as:

$$\mathbf{UA} = \begin{pmatrix} \mathbf{A}_1(x) \\ \mathbf{A}_2(x) \end{pmatrix} = \begin{pmatrix} \mathbf{I}_n \\ \mathbf{A}_2(x)\mathbf{A}_1^{-1}(x) \end{pmatrix} \cdot \mathbf{A}_1(x),$$

where $\mathbf{A}_1(x)$ is invertible. Hence $\mathbf{E}(x)\mathbf{A}(x) = \mathbf{E}(x)\mathbf{U}^{-1}\mathbf{UA}(x)$, where $\mathbf{U}^{-1}$ is a column permutation matrix. Thus, $\mathbf{E}(x)\mathbf{U}^{-1}$ also follows the distribution $(D^{\mathbb{H}}_{\mathcal{O}_K,r})^{m\times m'}$. Therefore, by Lemma 49 in this subsection, the result follows. □

D.3 Statistical Distance Between $\mathbf{A}(q)$ mod $f(q)$ and $U(\mathbb{Z}^{m\times n}_{f(q)})$

Lemma 50. *Let q, m, n be positive integers. Let $f(x) = x^d + g(x)$ be a irreducible and monic polynomial over $\mathbb{Z}[x]$ of degree d. We denote $D_{\mathsf{Eval,Mat}} := \{A(q) \bmod f(q) \mid A(x) \hookleftarrow U((\mathbb{Z}_q[x]/f(x))^{m\times n})\}$. Then we have $\Delta(U(\mathbb{Z}^{m\times n}_{f(q)}), D_{\mathsf{Eval,Mat}}) \leqslant mn \cdot |g(q)| \min\{1/f(q), 1/q^d\}$.*

Proof. We only need to analyze the statistical distance between the uniform distribution over $\mathbb{Z}_{f(q)}$, denoted by $U(\mathbb{Z}_{f(q)})$, and the distribution $D_{\mathsf{Eval}} := \{a(q) \bmod f(q) \mid a(x) \hookleftarrow U(\mathbb{Z}_q[x]/f(x))\}$. The statistical distance between the matrix distributions $U(\mathbb{Z}^{m\times n}_{f(q)})$ and $D_{\mathsf{Eval,Mat}}$ can then be bounded by

$$\Delta(U(\mathbb{Z}^{m\times n}_{f(q)}), D_{\mathsf{Eval,Mat}}) \leqslant mn \cdot \Delta(U(\mathbb{Z}_{f(q)}), D_{\mathsf{Eval}}).$$

When $f(q) > q^d$, $\mathsf{Eval}^{(f)}_q$ is injective, therefore, we have:

$$\begin{aligned}\Delta(U(\mathbb{Z}_{f(q)}, D_{\mathsf{Eval}})) =& \frac{1}{2}\left(q^d \cdot \left|\frac{1}{f(q)} - \frac{1}{q^d}\right| + (f(q) - q^d) \cdot \frac{1}{f(q)}\right) \\ =& 1 - \frac{q^d}{f(q)} = \frac{g(q)}{f(q)}.\end{aligned}$$

When $f(q) \leqslant q^d$, $\mathsf{Eval}^{(f)}_q$ is surjective, by Lemma 19, there are at most two polynomials whose evaluations over q are equal. In the distribution D_{Eval}, there

exist $q^d - f(q)$ values with probability $2/q^d$, while each of the other $2f(q) - q^d$ values appears with probability $1/q^d$. Therefore, we have:

$$\begin{aligned}\Delta(U(\mathbb{Z}_{f(q)}, D_{\mathsf{Eval}})) =& \frac{1}{2}\left((2f(q)-q^d)\cdot\left|\frac{1}{f(q)}-\frac{1}{q^d}\right| + (q^d - f(q))\cdot\left|\frac{2}{q^d}-\frac{1}{f(q)}\right|\right)\\ =& \frac{(2f(q)-q^d)\cdot(q^d-f(q))}{f(q)\cdot q^d} = 3 - \frac{q^{2d}+2(q^d+g(q))\cdot f(q)}{q^d\cdot f(q)}\\ =& 1 - \frac{q^{2d}+2g(q)f(q)}{q^d f(q)} = 1 - \frac{q^{2d}+2g(q)f(q)}{q^d\cdot(q^d+g(q))} = -\frac{g(q)}{q^d}.\end{aligned}$$

Therefore $\Delta(U(\mathbb{Z}_{f(q)}^{m\times n}), D_{\mathsf{Eval},\mathsf{Mat}}) \leqslant mn\cdot|g(q)|\min\left\{\frac{1}{f(q)}, \frac{1}{q^d}\right\}$. □

This Lemma implies the following Corollary directly.

Corollary 7. *Let q, m, n be positive integers. Let $f(x) = x^d + g(x)$ be a irreducible and monic polynomial over $\mathbb{Z}[x]$ of degree d. We denote $D_{\mathsf{Eval},\mathsf{Mat}} := \{A(q) \bmod f(q) \mid A(x) \hookleftarrow U((\mathbb{Z}_q[x]/f(x))^{m\times n})\}$. Additionally, let κ be the security parameter, $m \leqslant \mathsf{poly}(\kappa)$, $n \leqslant \mathsf{poly}(\kappa)$, $d = \mathcal{O}(\kappa)$ and $q = \mathsf{poly}(d)$. When the degree of $g(x)$ is less than $d/2$, the statistical distance satisfies*

$$\Delta(U(\mathbb{Z}_{f(q)}^{m\times n}), D_{\mathsf{Eval},\mathsf{Mat}}) \leqslant 2^{-\omega(\log(\kappa))}.$$

D.4 The Size of Error Terms

Building on Lemma 17, we provide an upper bound for $c(q)\cdot c'(q)$, where both $c(x)$ and $c'(x)$ are two polynomials with bounded infinity norm of coefficient vectors.

Lemma 51. *Let κ be the security parameter, $q = \mathsf{poly}(\kappa)$ a positive integer, f a monic and irreducible polynomial of degree d with coefficients in the range $(-\frac{q}{2}, \frac{q}{2})$, B, B' two positive numbers satisfying $q/(BB'd\cdot EF(f)) \geqslant \mathsf{poly}(\kappa)$. Given two polynomial $c(x)$, $c'(x)$ such that $\|c(x)\|_\infty \leqslant B$, $\|c'(x)\|_\infty \leqslant B'$, we have:*

$$|c(q)c'(q) \bmod f(q)| \leqslant \left(3 + BB'd\left(EF(f) + \frac{2}{q}\right)\right)\frac{q^d-1}{q-1}.$$

Proof. Map $c(q)c'(q) \bmod f(q)$ to the ring $\mathbb{Z}_q[x]/(f(x))$ through $\Phi_q^{(f)}$, and it shows that:

$$\Phi_q^{(f)}(c(q)c'(q) \bmod f(q)) = \Phi_q^{(f)}(c(q))\Phi_q^{(f)}(c'(q)) + c_f^{(m)}(c(q), c'(q)) \bmod f(x).$$

Since $\frac{q}{B} \geqslant poly(\kappa)$ and $\frac{q}{B'} \geqslant poly(\kappa)$, $\Phi_q^{(f)}(c(q)) = c(x)$ and $\Phi_q^{(f)}(c'(q)) = c'(x)$. $\|c(x)c'(x)\|_\infty \leqslant BB'd\cdot EF(f)$ and the results follows directly according to Lemma 17. □

D.5 Reduction for any module rank n

In the main body of our results, we restrict the number of samples to $\mathcal{O}(\log(\kappa))$ so that the reductions form a closed loop; in this case, the module rank must be limited to $\mathcal{O}(1)$. However, this restriction is not necessary for the MLWE to stEDCP reduction if sufficiently many MLWE samples are available. In this subsection, we present a reduction from the MLWE problem with a sufficiently large number of samples to the stEDCP problem. Under this setting, sample amplification is no longer required, and the module rank n can exceed $\mathcal{O}(1)$. Moreover, this enables the reduction to hold over a broader class of rings.

In the following lemma, we show how to transform a P-MLWE instance into an IP-MLWE-like instance. Together with the transformation between MLWE and P-MLWE in Supplementary Material B.3, and the algorithm presented in Lemma 30 in Section 5.2, this yields a reduction from MLWE to stEDCP with a larger number of samples and over a broader class of rings.

Lemma 52. *Let κ be the security parameter, and let q, m, n, d be positive integers such that $d = \mathsf{poly}(\kappa)$, $q = \mathsf{poly}(\kappa)$ and $m \geqslant \mathcal{O}(n\log(q))$. Let $f(x) = x^d + g(x)$ be an irreducible cyclotomic polynomial with $\deg(g(x)) \leqslant d/2$, satisfying $f(q) \geqslant q^d$. Define $K = \mathbb{Q}[x]/f$ to be the corresponding number field, and let $\mathcal{O}_K$ denote its ring of integers.*

Consider a randomly chosen $\mathsf{P\text{-}MLWE}^{m,n}_{q,r'_1,r_1,f}$ instance of the form

$$\big(\mathbf{A}(x),\, \mathbf{A}(x)\mathbf{s}(x) + \mathbf{e}(x) \bmod (q, f(x))\big) \in (\mathbb{Z}_q[x]/f)^{m\times n} \times (\mathbb{Z}_q[x]/f)^m.$$

With probability at least $1 - 2^{-\omega(\log(\kappa))}$, there exists a polynomial-time algorithm that transforms this instance into an IP-MLWE-like instance

$$\big(\widetilde{\mathbf{A}},\, \widetilde{\mathbf{A}}\widetilde{\mathbf{s}} + \widetilde{\mathbf{e}} \bmod f(q)\big) \in (\mathbb{Z}_{f(q)})^{m\times n} \times (\mathbb{Z}_{f(q)})^m,$$

which satisfies the following condition:

1) *The distribution of $\widetilde{\mathbf{A}}$ is statistically close to $U(\mathbb{Z}^{m\times n}_{f(q)})$ with distance at most $2^{-\omega(\log(\kappa))}$;*
2) *The infinity norm of the error vector $\widetilde{\mathbf{e}}$ satisfies $\|\widetilde{\mathbf{e}}\|_\infty \leqslant c'_{max}(q^d-1)/(q-1)$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$, where $c'_{max} = 2 + c_{\max} + r_1\sqrt{\kappa}$, $c_{max} = \big((3r'_1\sqrt{\kappa}n^2)/2 + (7 + \|f\|_1)n - 2\big)\, EF(f) + 11/2 + 4\|f\|_\infty$. Moreover, for each entry of $\widetilde{\mathbf{e}}$, namely $\widetilde{e}_i$, $\|\Phi^{(f)}_q(\widetilde{e}_i)\|_\infty \leqslant c'_{max}$;*
3) *The distribution of the secret $\widetilde{\mathbf{s}}$ is statistically close to $D_{r'_1}(q)$ with distance at most $2^{-\omega(\log(\kappa))}$, where $D_{r'_1}(q)$ denotes the distribution selecting $\mathbf{s}(x) \hookleftarrow (D_{\mathbb{Z}[x]/f,r'_1})^n$ and outputting $\mathbf{s}(q) \bmod f(q)$.*

Proof. First, by Corollary 1 in Supplementary Material B.1, each entry of $\mathbf{s}(x)$, namely $s_i(x)$ for $i \in [n]$, is bounded as $\|s_i(x)\|_\infty \leqslant r'_1\sqrt{\kappa}$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$. Similarly, for each entry of $\mathbf{e}(x)$, namely $e_j(x)$ for $j \in [m]$, is bounded as $\|e_j(x)\|_\infty \leqslant r_1\sqrt{\kappa}$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$.

Since $f(x)$ satisfies $f(q) \geqslant q^d$, by Lemma 18 in Section 3.6, we can rewrite $\mathbf{A}(x)\mathbf{s}(x) + \mathbf{e}(x) \bmod (q, f(x))$ as

$$\begin{aligned}&\Phi_q^{(f)}(\mathbf{A}(q) \bmod f(q)) \cdot \Phi_q^{(f)}(\mathbf{s}(q) \bmod f(q)) + \Phi_q^{(f)}(\mathbf{e}(q) \bmod f(q))\\ =\ &\Phi_q^{(f)}\big(\mathbf{A}(q)\mathbf{s}(q) + \mathbf{e}(q) \bmod f(q)\big) + \mathbf{c}(\mathbf{A}(x), \mathbf{e}(x)),\end{aligned}$$

where $\mathbf{c}(\mathbf{A}(x), \mathbf{e}(x))$ is a carry term. By Lemma 46 in Supplementary Material C.2 and the bound on $\|\mathbf{s}(x)\|_\infty$, each entry of $\mathbf{c}(\mathbf{A}(x), \mathbf{e}(x))$ is bounded in infinity norm by

$$\big((3r_1'\sqrt{\kappa}n^2)/2 + (7 + \|f\|_1)n - 2\big)\, EF(f) + 11/2 + 4\|f\|_\infty,$$

with probability at least $1 - 2^{-\omega(\log(\kappa))}$. We denote this bound by $c_{\max}$.

Moreover, for $\mathbf{A}_i(x)$, the i-th row of the matrix $\mathbf{A}(x)$, we have:

$$\begin{aligned}&\mathsf{Eval}_q^{(f)}\left(\langle \mathbf{A}_i(x), \mathbf{s}(x)\rangle + e_i(x) \bmod f(x)\right)\\ =&\mathsf{Eval}_q^{(f)}\left(\Phi_q^{(f)}(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q)) + c_i(\mathbf{A}(x), \mathbf{e}(x)) \bmod q\right)\\ =&\mathsf{Eval}_q^{(f)}\left(\Phi_q^{(f)}(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q)) + c_i(\mathbf{A}(x), \mathbf{e}(x)) + q\textstyle\sum_{j=0}^{d-1}\delta_j x^j\right),\end{aligned}$$

where $\delta_j = \left\lfloor \Phi_q^{(f)}(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))_j + c_i(\mathbf{A}(x), \mathbf{e}(x))_j/q \right\rceil \in \{0, \pm 1\}$. Here, $c_i(\mathbf{A}(x), \mathbf{e}(x))$ denotes the i-th entry of $\mathbf{c}(\mathbf{A}(x), \mathbf{e}(x))$, $\Phi_q^{(f)}(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))_j$ is the j-th coefficient of $\Phi_q^{(f)}(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))$, $c_i(\mathbf{A}(x), \mathbf{e}(x))_j$ is the j-th coefficient of the polynomial $c_i(\mathbf{A}(x), \mathbf{e}(x))$. Continuing the computation, we obtain:

$$\begin{aligned}&\mathsf{Eval}_q^{(f)}(\langle \mathbf{A}_i(x), \mathbf{s}(x)\rangle + e_i(x) \bmod f(x))\\ =&\mathsf{Eval}_q^{(f)}\Big(\Phi_q(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q)) + \delta' f(x) + c_i(\mathbf{A}, \mathbf{e}) + q\textstyle\sum_{j=0}^{d-1}(\delta_j + \delta_j')x^j\Big)\\ =&\Phi_q(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))(q) + \delta' f(q)\\ &+ c_i(\mathbf{A}(x), \mathbf{e}(x))(q) + \textstyle\sum_{j=0}^{d-1}\left(\delta_{j-1} + \delta_{j-1}'\right) q^j \bmod f(q)\\ =&\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q) + c_i(\mathbf{A}(x), \mathbf{e}(x))(q) + \textstyle\sum_{j=0}^{d-1}\left(\delta_{j-1} + \delta_{j-1}'\right) q^j \bmod f(q)\\ =&\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) + c_i(\mathbf{A}(x), \mathbf{e}(x))(q) + \textstyle\sum_{j=0}^{d-1}\left(\delta_{j-1} + \delta_{j-1}'\right) q^j \bmod f(q),\end{aligned}$$

which is subject to the relations $\delta' = \left\lfloor \frac{\Phi_q(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))}{f(x)} \right\rceil \in \{0, \pm 1\}$, $\delta_{-1} = -\delta_{d-1}$, $\delta_j' = \left\lfloor \frac{\Phi_q(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))_j + \delta' f_j}{q} \right\rceil \in \{0, \pm 1\}$, and $\delta_{-1}' = -\delta_{d-1}'$. Here the integer $\Phi_q(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))_j$ denotes the j-th coefficient of the polynomial $\Phi_q(\langle \mathbf{A}_i(q), \mathbf{s}(q)\rangle + e_i(q) \bmod f(q))$, and f_j denotes the j-th coefficient of $f(x)$.

We denote $\widetilde{\mathbf{A}} = \mathbf{A}(q) \bmod f(q)$, $\widetilde{\mathbf{s}} = \mathbf{s}(q) \bmod f(q)$. Then the term 1) is satisfied due to Corollary 7 in Supplementary Material D.3, and term 3) is satisfied canonically. Then we consider the second condition. We consider the summation

$$\widetilde{e}_i = e_i(q) + c_i(\mathbf{A}(x), \mathbf{e}(x))(q) + \textstyle\sum_{j=0}^{d-1}(\delta_{j-1} + \delta_{j-1}')q^j,$$

and denote $\widetilde{\mathbf{e}}$ be the vector whose i-th entry is $\widetilde{e}_i$.

According to the upper bounds established earlier in the proof, the absolute value of $\widetilde{e}_i$ satisfies $|\widetilde{e}_i| \leqslant (2 + c_{\max} + r_1\sqrt{\kappa})\,(q^d - 1)/(q-1)$ with probability at least $1 - 2^{-\omega(\log(\kappa))}$. Moreover, the coefficients of the polynomial $\Phi_q^{(f)}\left(e_i(q) + c_i(\mathbf{A}(x), \mathbf{e}(x))(q) + \sum_{j=0}^{d-1} \delta_{j-1} q^j\right)$ are bounded above by $2 + c_{\max} + r_1\sqrt{\kappa}$. Therefore, the second term is satisfied. □

E Supplementary Materials for the reduction from IP-M-EDCP to EDCP

In this section, in order to reduce stEDCP to the more classical EDCP with polynomially large modulus, we present an addition result for EDCP about trading modulus for dimension. We first recall some necessary prior definitions and results.

In Definition 9, we define the Gaussian distribution. We adopt the following notation for Gaussian distributions with unspecified standard deviation.

Definition 28. *Let r be the deviation parameter. For the Gaussian distribution on $\mathbb{R}^n$ with some unknown deviation parameter which is smaller than r, we denote this distribution as $\mathcal{N}_{\leqslant r}$. Furthermore, if the errors in the* LWE *problem are selected from this distribution, we can denote it as* $\mathsf{LWE}^{m,n}_{q,\mathcal{S},\mathcal{N}_{\leqslant r}}$.

In the following, we recall the reduction from standard LWE with secret from $U(\mathbb{Z}_q^k)$ to its variants with secret from Gaussian distribution with small width and uniformly random distribution $U(\{0,1\}^n)$, respectively.

Lemma 53 ([BLP+13, Lemma 2.12]). *Let $q \geqslant 25$, $n, m \geqslant 1$, $\varepsilon \leqslant 1/2$ and $\alpha \geqslant \sqrt{\ln(2n(1+1/\varepsilon)/\pi)}/q$. There is an efficient reduction from* $\mathsf{LWE}^{m,n}_{q,U(\mathbb{Z}_q^n),\mathcal{N}_{\alpha q}}$ *to* $\mathsf{LWE}^{m',n}_{q,D_{\mathbb{Z}^n,\sqrt{2}\alpha q},\mathcal{N}_{\alpha q}}$ *where $m' = m - (16n + 4\ln\ln q)$.*

Lemma 54 ([BLP+13, Theorem 4.1]). *Let $k, q \geqslant 1$ and $m \geqslant n \geqslant 1$ be integers, and let $\varepsilon \in (0, 1/2)$, $\alpha, \delta > 0$, be such that $n \geqslant (k+1)\log q + 2\log(1/\delta)$, $\alpha \geqslant \sqrt{\ln(2n(1+1/\varepsilon))/\pi}/q$. There exist three reductions from* $\mathsf{LWE}^{m,k}_{q,U(\mathbb{Z}_q^k),\mathcal{N}_{\alpha q}}$ *to* $\mathsf{LWE}^{m,n}_{q,U(\{0,1\}^n),\mathcal{N}_{\leqslant\sqrt{10n}\alpha q}}$*, such that for any algorithm for the latter problem with advantage ζ, at least one of the reductions produces an algorithm for the former problem with advantage at least*

$$(\zeta - \delta)/(3m) - 41\varepsilon/2 - \sum\nolimits_{p|q,p \text{ is prime}} p^{-k-1}.$$

Then, from the bounded secret variant of LWE, one can reduce its modulus to a moderate size as stated below.

Lemma 55 ([BLP+13, Corollary 3.2]). *For any $m, n \geqslant 1$, $q \geqslant q' \geqslant 1$, (B, δ)-bounded distribution $\mathcal{D}$ over $\mathbb{Z}^n$, $\alpha, \beta > 0$ and $\varepsilon \in (0, 1/2)$ such that*

$$\beta^2 \geqslant \alpha^2 + (4/\pi)\ln(2n(1+1/\varepsilon)) \cdot (B/q')^2,$$

there is an efficient reduction from $\mathsf{LWE}^{m,n}_{q,\mathcal{D},\mathcal{N}_{\leqslant\alpha q}}$ *to* $\mathsf{LWE}^{m,n}_{q',\mathcal{D},\mathcal{N}_{\leqslant\beta q'}}$ *that reduce the advantage by at most* $\delta + 14\varepsilon m$. *A distribution is said to be* (B,δ)*-bounded if for* $\mathbf{e} \hookleftarrow \mathcal{D}$, *it holds that* $\Pr[|\mathbf{e}|_2 > B] \leqslant \delta$.

To fix the parameter for the error distribution, we also require the following result.

Lemma 56 ([Reg05, Lemma 3.7]). *Let* $\mathcal{A}$ *be an algorithm for* $\mathsf{LWE}^{m,n}_{q,U(\mathbb{Z}_q^n),\mathcal{N}_{\alpha q}}$ *with advantage at least* $\varepsilon > 0$. *There exists an algorithm* $\mathcal{B}$ *for* $\mathsf{LWE}^{m',n}_{q,U(\mathbb{Z}_q^n),\mathcal{N}_{\leqslant\alpha q}}$ *using oracle access to* $\mathcal{A}$ *with advantage at least* $1/3$, *where both* m' *and its running time are* $\mathsf{poly}(m, 1/\varepsilon, n, \log q)$.

We also rely on the existence of a prime number inside interval $(n, 2n-2)$ for any $n > 3$.

Lemma 57 ([Ram19,Erd32]). *For any integer* $n > 3$, *there exists at least one prime number* p *such that* $n < p < 2n - 2$.

Now we state our main result for reducing the modulus as follows.

Lemma 58. *Let* κ *be the security parameter. Let* f *of degree* d *be a monic and irreducible polynomial with coefficients in the range* $(-q/2, q/2)$. *Let* m, n, m', n', q *be positive integers such that* $n' \geqslant (n+1)d\lceil\log q\rceil + 2\kappa$, $m' = m - (16n + 4\lceil\ln\ln(f(q))\rceil) \geqslant n'\log q$. *Let* $l = \mathsf{poly}(\kappa)$. *Let* β', r', r *be positive such that* $\beta' \geqslant (10890n^2\kappa^2n')/(\pi^2r^4) + (4\kappa)/(\pi q)$, $r' \leqslant 1/(32\sqrt{2}m\kappa\beta' l q^{n'/m})$. *There exists a reduction from* $\mathsf{G\text{-}EDCP}^{m,n}_{f(q),U(\mathbb{Z}^n_{f(q)}),r}$ *to* $\mathsf{G\text{-}EDCP}^{l,n'}_{q,U(\mathbb{Z}_q^{n'}),r'}$ *in polynomial time.*

Proof. Starting from $\mathsf{G\text{-}EDCP}^{m,n}_{f(q),U(\mathbb{Z}^n_{f(q)}),r}$, by Lemma 44, one can first reduce it to $\mathsf{LWE}^{m,n}_{f(q),U(\mathbb{Z}^n_{f(q)}),f(q)/2r}$. Then by Lemma 32, the latter one can be reduced to $\mathsf{LWE}^{m,n}_{f(q),U(\mathbb{Z}^n_{f(q)}),\mathcal{N}_{f(q)/(\sqrt{2}r)}}$ by adding an error term selected from $\mathcal{N}_{f(q)/(\sqrt{2}r)}$.

According to Lemma 53, we can reduce from $\mathsf{LWE}^{m,n}_{f(q),U(\mathbb{Z}^n_{f(q)}),\mathcal{N}_{f(q)/(\sqrt{2}r)}}$ to $\mathsf{LWE}^{m',n}_{f(q),D_{\mathbb{Z}^n,f(q)/r},\mathcal{N}_{f(q)/(\sqrt{2}r)}}$ with $m' = m - (16n + 4\lceil\ln\ln(f(q))\rceil)$. Let q' be the largest prime smaller than $f(q)$. By Lemma 57, we have $q' > f(q)/2$. From the last problem, by Lemma 55, there is a reduction to $\mathsf{LWE}^{m',n}_{q',D_{\mathbb{Z}^n,f(q)/r},\mathcal{N}_{\leqslant\beta q'}}$, where

$$\beta \geqslant 1/(2r^2) + (32n\kappa)/(\pi r^2).$$

The distribution $\mathcal{N}_{\leqslant\beta q'}$ follows the Definition 28. Then by Lemma 56 with proper parameters, there exists an efficient reduction from $\mathsf{LWE}^{m',n}_{q',D_{\mathbb{Z}^n,f(q)/r},\mathcal{N}_{\leqslant\beta q'}}$ to $\mathsf{LWE}^{m',n}_{q',D_{\mathbb{Z}^n,f(q)/r},\mathcal{N}_{\beta q'}}$, and the latter problem can further be efficiently reduced to $\mathsf{LWE}^{m',n}_{q',U(\mathbb{Z}^n_{q'}),\mathcal{N}_{\beta q'}}$ according to self re-randomization by adding a random secret chosen from $U(\mathbb{Z}^n_{q'})$.

To continue, from the $\mathsf{LWE}^{m',n}_{q',U(\mathbb{Z}^n_{q'}),\mathcal{N}_{\beta q'}}$ problem, by Lemma 54, we can reduce it to $\mathsf{LWE}^{m',n'}_{q',U(\{0,1\}^{n'}),\mathcal{N}_{\leqslant\sqrt{10n'}\beta q'}}$, where $n' \geqslant (n+1)\log q' + 2\kappa$. According to Lemma 56, the latter problem can be reduced to $\mathsf{LWE}^{m',n'}_{q',U(\{0,1\}^{n'}),\mathcal{N}_{\sqrt{10n'}\beta q'}}$.

Now we can apply Lemma 55 to switch the modulus from q', which is still exponentially large, to a polynomial-sized modulus q. Concretely, we reduce $\mathsf{LWE}^{m',n'}_{q',U(\{0,1\}^{n'}),\mathcal{N}_{\sqrt{10n'}\beta q'}}$ to $\mathsf{LWE}^{m',n'}_{q,U(\{0,1\}^{n'}),\mathcal{N}_{\leqslant\beta' q}}$, where

$$\beta' \geqslant 10n'\beta^2 + (4\kappa)/(\pi q) \geqslant (10890n^2\kappa^2 n')/(\pi^2 r^4) + (4\kappa)/(\pi q).$$

The latter problem can be reduced to $\mathsf{LWE}^{m',n'}_{q,U(\mathbb{Z}_q^{n'}),\mathcal{N}_{\beta' q}}$ according to self re-randomization by adding a random secret chosen from $U(\mathbb{Z}_q^{n'})$. Then we can reduce $\mathsf{LWE}^{m',n'}_{q,U(\mathbb{Z}_q^{n'}),\mathcal{N}_{\beta' q}}$ to $\mathsf{LWE}^{m',n'}_{q,U(\mathbb{Z}_q^{n'}),\sqrt{2}\beta' q}$ according to Lemma 33. Finally, by Lemma 43, the latter problem can be reduced to $\mathsf{G\text{-}EDCP}^{l,n'}_{q,U(\mathbb{Z}_q^{n'}),r'}$, where $l = \mathsf{poly}(\kappa)$ and $r' \leqslant 1/(32\sqrt{2}m'\kappa\beta' l q^{n'/m'})$. □