On the Hardness of $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian and Other Amplitudes

Yilei Chen* Zihan Hu† Qipeng Liu‡ Han Luo§ Yaxin Tu¶

October 1, 2023

Abstract

The learning with errors problem (LWE) is one of the most important building blocks for post-quantum cryptography. To better understand the quantum hardness of LWE, it is crucial to explore quantum variants of LWE, show quantum algorithms for those variants, or prove they are as hard as standard LWE.

To this end, Chen, Liu, and Zhandry [Eurocrypt 2022] define the $\mathsf{S}|\mathsf{LWE}\rangle$ problem, which encodes the error of LWE samples into quantum amplitudes. They then show efficient quantum algorithms for $\mathsf{S}|\mathsf{LWE}\rangle$ with a few interesting amplitudes. However, the hardness of the most interesting amplitude, Gaussian, was not addressed by Chen et al., or only known for some restricted settings (for example, when the number of $\mathsf{S}|\mathsf{LWE}\rangle$ samples is very small, it is well known that $\mathsf{S}|\mathsf{LWE}\rangle$ is as hard as standard LWE).

In this paper, we show new hardness and algorithms for $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian and other amplitudes. Our main results are

1. There exist quantum reductions from standard LWE or worst-case GapSVP to $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude with *unknown* phase, and arbitrarily many $\mathsf{S}|\mathsf{LWE}\rangle$ samples.
2. There is a $2^{\widetilde{O}(\sqrt{n})}$-time algorithm for $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude with *known* phase, given $2^{\widetilde{O}(\sqrt{n})}$ many quantum samples. The algorithm is modified from Kuperberg's sieve, and in fact works for more general amplitudes as long as the amplitudes and phases are completely *known*.

One way of interpreting our result is: to show a sub-exponential time quantum algorithm for standard LWE, all we need is to handle *phases* in $\mathsf{S}|\mathsf{LWE}\rangle$ amplitudes better, either in the algorithm or the reduction.

*IIIS, Tsinghua University; Shanghai Artificial Intelligence Laboratory; and Shanghai Qi Zhi Institute. chenyilei@mail.tsinghua.edu.cn. chenyilei.ra@gmail.com. Supported by Tsinghua University startup funding.

†IIIS, Tsinghua University huzihan423@gmail.com.

‡UC San Diego qipengliu0@gmail.com. The work was initiated while Qipeng Liu was a postdoc researcher in Simons Insititute, supported in part by the Simons Institute for the Theory of Computing, through a Quantum Postdoctoral Fellowship and by the DARPA SIEVE-VESPA grant No.HR00112020023.

§IIIS, Tsinghua University luohan23@mails.tsinghua.edu.cn.

¶Department of Computer Science, Princeton University yaxin.tu@princeton.edu. The work was initiated while Yaxin Tu was in IIIS, Tsinghua University.

Contents

1 Introduction

The learning with errors problem asks to learn a secret vector given many noisy linear samples.

Definition 1.1 (Learning with errors (LWE) [Reg09]). *Let n, m, q be positive integers. Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector. The search LWE problem $\mathsf{LWE}_{n,m,q,\alpha}$ asks to find the secret $\mathbf{s}$ given access to an oracle that outputs $\mathbf{a}_i$, $\langle \mathbf{s}, \mathbf{a}_i \rangle + e_i \pmod q$ on its i^{th} query, for $i = 1, \cdots, m$. Here each $\mathbf{a}_i$ is a uniformly random vector in $\mathbb{Z}_q^n$, and each error term e_i is sampled from the Gaussian distribution over $\mathbb{Z}$ with standard deviation $\alpha q/\sqrt{2\pi}$.*

The LWE problem is extremely versatile, leading to advanced encryption schemes such as fully homomorphic encryptions [Gen09, BV11, Mah18]. It is also shown by Regev to be quantumly as hard as the approximate short vector problems for all lattices [Reg09]. LWE and lattice problems in general (e.g. [HPS98, Reg09]) are also popular candidates for the NIST post-quantum cryptography standardization, due to their conjectured hardness against quantum computers. In fact, the fastest quantum and classical algorithms for LWE all run in $2^{\Omega(n)}$ time. However, the conjectured quantum hardness of lattice problem is still lacking solid evidences. Finding quantum algorithms for lattice problems has therefore been a major open problem in the area of quantum computation and cryptography in the past decade.

One way of exploring the quantum power for solving LWE is to consider the quantum variants of LWE, by encoding quantum states into the LWE problem (henceforth, we refer to the original LWE problem as "classical LWE" or "standard LWE" to distinct them from the quantum variant mentioned below). To this end, Chen, Liu, and Zhandry [CLZ22] define the following variant of LWE.

Definition 1.2 (Solve $|\mathsf{LWE}\rangle$, $\mathsf{S}|\mathsf{LWE}\rangle$). *Let n, m, q be positive integers. Let f be a function from $\mathbb{Z}_q$ to $\mathbb{C}$. Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector. The problem $\mathsf{S}|\mathsf{LWE}\rangle_{n,m,q,f}$ asks to find $\mathbf{s}$ given access to an oracle that outputs independent samples $\mathbf{a}_i$, $\sum_{e_i \in \mathbb{Z}_q} f(e_i) | \langle \mathbf{s}, \mathbf{a}_i \rangle + e_i \bmod q \rangle$ on its i^{th} query, for $i = 1, \cdots, m$. Here each $\mathbf{a}_i$ is a uniformly random vector in $\mathbb{Z}_q^n$.*

Chen, Liu, and Zhandry [CLZ22] then show a quantum filtering technique to solve $\mathsf{S}|\mathsf{LWE}\rangle$ when the DFT of the error amplitude is non-negligible everywhere over $\mathbb{Z}_q$. Two interesting error amplitudes covered by their result are the bounded uniform amplitude and Laplacian amplitude. In particular, the classical LWE problem with bounded uniform error distribution is proven to be as hard as worst-case lattice problems [DM13, MP13]. Thus, their work gives a strong indication that $\mathsf{S}|\mathsf{LWE}\rangle$ is easier than classical LWE for certain error distributions.

However, the most interesting amplitude, Gaussian, was not addressed in [CLZ22]. For classical LWE, Gaussian distribution is the default error distribution since Regev [Reg09] shows a quantum reduction from worst-case lattice problems to LWE with Gaussian error, given *arbitrarily* many LWE samples. Interestingly, it was implicitly shown in [SSTX09] and [BKSW18] that $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude is as hard as standard LWE when the number of samples is *very small*. But if we are given *arbitrarily* many samples, is the $\mathsf{S}|\mathsf{LWE}\rangle$ problem with Gaussian amplitude still hard?

Not only did the understanding $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude shed light on our knowledge of the standard LWE, but it was also considered a bedrock on which interesting quantum protocols can be based, especially unclonable cryptography. The idea was first initially by Zhandry [Zha19]

Error Amplitude	# Samples	Algorithm or Hardness	Reference
Gaussian	Few	As hard as LWE or approx-GapSVP	[SSTX09] [BKSW18]
Gaussian with unknown phase	Arbitrary	As hard as LWE or approx-GapSVP	Sections 3,4
Gaussian	$2^{\tilde{O}(\sqrt{n})}$	$2^{\tilde{O}(\sqrt{n})}$-time quantum algorithm	Section 5
Known with wide DFT	$\mathsf{poly}(n)$	$\mathsf{poly}(n)$-time quantum algorithm	[CLZ22]

Table 1: Hardness of $\mathsf{S}|\mathsf{LWE}\rangle$ with different error amplitudes

for a potential approach to construct a very powerful cryptographic primitive called quantum lightning, while its concrete and secure instantiation still remains unknown. After that, Khesin, Lu, and Shor proposed another lightning construction [KLS22] based on $\mathsf{S}|\mathsf{LWE}\rangle$ but later was broken by Liu, Montgomery, and Zhandry [LMZ23]. Poremba [Por23], and Ananth, Poremba, and Vaikuntanathan [APV23] build certifiable deletion based on $\mathsf{S}|\mathsf{LWE}\rangle$, basing on certain conjectured security. If $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude was not secure, then all schemes mentioned before may not even have semantic security, let alone its unclonability.

1.1 Main results

In this paper, we show new quantum algorithms and hardness results for $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian and other amplitudes.

Our first result is a sub-exponential time quantum algorithm for solving $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude, given sub-exponentially many $\mathsf{S}|\mathsf{LWE}\rangle$ samples. The algorithm combines Kuperberg's sieve [Kup05] and quantum rejection sampling [ORR13]. In fact, it works for a more general amplitude f as long as the discrete Fourier transform of f has two non-negligible points (the DFT of Gaussian certainly has two non-negligible points).

Theorem 1.3 (Theorem 5.1, informal)**.** *Let $f : \mathbb{Z} \to \mathbb{C}$ be a known, normalized error amplitude function for $\mathsf{S}|\mathsf{LWE}\rangle$ such that for the DFT_q of f, denoted by g, there exists two distinct values $j_1, j_2 \in \mathbb{Z}_q$ such that $\gcd(j_1 - j_2, q) = 1$ and $|g(j_1)|, |g(j_2)| \geq 2^{-\sqrt{n}\log q}$, and $g(j_1), g(j_2)$ are computable in time $2^{\Theta(\sqrt{n}\log q)}$.*

Then there exists a quantum algorithm that, given $m = 2^{\Theta(\sqrt{n}\log q)}$ samples of $\mathsf{S}|\mathsf{LWE}\rangle$ with amplitude f, finds the secret within a time complexity of $2^{\Theta(\sqrt{n}\log q)}$.

Readers may wonder whether Theorem 1.3 leads to sub-exponential time quantum algorithms for classical LWE. To address this question, let us recall the quantum reduction from GapSVP and SIVP to classical LWE with Gaussian error distribution due to Regev [Reg09]. This reduction works even given *arbitrarily many* classical LWE samples. One would (reasonably?) hope that the reduction can be modified to a quantum reduction from worst-case lattice problems to $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude.

However, we are only able to modify Regev's reduction into a quantum reduction from worst-case lattice problem to $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian amplitude with *unknown* phase, with arbitrarily many $\mathsf{S}|\mathsf{LWE}\rangle$ samples. Before stating our main theorem, let us first introduce the definition of $\mathsf{S}|\mathsf{LWE}\rangle$ with phase.

Definition 1.4 ($\mathsf{S|LWE}\rangle^{\mathsf{phase}}$)**.** *Let n, m, q be LWE parameters. Define the following components: (1) an amplitude function $f : \mathsf{supp}(f) \to \mathbb{R}$; (2) a mapping $\theta : \mathsf{supp}(\theta) \to \mathbb{R}$ for the phase term; (3) a distribution D_θ over the set $\mathsf{supp}(\theta)$.*

We say a quantum algorithm solves $\mathsf{S|LWE}\rangle^{\mathsf{phase}}_{n,m,q,f,\theta,D_\theta}$, if for any hidden vector $\mathbf{s} \in \mathbb{Z}_q^n$, when provided with m samples of

$$\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n), \quad \mathbf{y} \leftarrow D_\theta, \quad \sum_{e \in \mathsf{supp}(f)} f(e) \exp(2\pi \mathrm{i} \cdot e\theta(\mathbf{y})) |(\langle \mathbf{a}, \mathbf{s} \rangle + e) \bmod q\rangle,$$

the algorithm outputs $\mathbf{s}$ with probability at least $1 - 2^{-\Omega(n)}$.

On the first pass of the definition, readers can think of $\mathbf{y}$ as some auxiliary information. The phase term $\theta(\mathbf{y})$ is a function of $\mathbf{y}$. As it is defined, the function θ may or may not be efficiently computable (it is not efficiently computable in our result). So we can think of $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ as a variant of $\mathsf{S|LWE}\rangle$ with a phase term in the amplitude.

Theorem 1.5 (Theorem 4.2, informal)**.** *Let $q = q(n) > 10n$ be an integer of at most $\mathsf{poly}(n)$ bits, $\alpha \in (0, \frac{1}{5\sqrt{n}})$ such that $\alpha q > 2\sqrt{n}$. Suppose there exists quantum algorithms that solve $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ where the amplitude $f(e) := \exp\left(-\pi \frac{e^2}{(\alpha q)^2}\right)$, the phase θ is not efficiently computable, with $m = 2^{o(n)}$ samples and in time complexity T. Then there exists a quantum algorithm that solves GapSVP_γ and SIVP_γ, where $\gamma \in \tilde{O}(n/\alpha)$, in time $\mathsf{poly}(n, m, T)$.*

The informal statement above omits the distribution of the unknown phase term $\theta(\mathbf{y})$ and some other details. All those details can be found in the statement of Theorem 4.2. Morally, Theorem 4.2 says there is a quantum reduction from worst-case lattice problems to $\mathsf{S|LWE}\rangle$ with Gaussian amplitude with unknown phase (the distribution of the unknown phase is known though), with arbitrarily many $\mathsf{S|LWE}\rangle$ samples.

We also provide a quantum reduction directly from classical LWE to $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ in Theorem 3.4. This reduction goes through the (extrapolated) dihedral coset problem, originally used in [Reg02, BKSW18]. It achieves worse parameters compared to Theorem 4.2, but is much simpler to describe. For more details we refer the readers to Section 3. Although the result appears to be qualitatively similar as Theorem 4.2, as it also says $\mathsf{S|LWE}\rangle$ with Gaussian amplitude with unknown phase is as hard as classical LWE; the reduction itself is very different, therefore it might offer a different approach for potential improvements.

Overall, we reduce worst-case lattice problems, or classical LWE, to $\mathsf{S|LWE}\rangle$ with unknown phase. Readers may wonder what prevents us from removing the unknown phase in our reductions. However, the reasons are rather technical and entangled with the details of our algorithms, so we refer readers to the main body for discussions therein.

In Table 1 we summarize the old and new algorithms and hardness results for $\mathsf{S|LWE}\rangle$. In Figure 1 we provide some examples of interesting amplitudes addressed in our paper or previous papers.

Future directions. Our main results provide two possibilities of getting a sub-exponential time quantum algorithm for standard LWE via $\mathsf{S|LWE}\rangle$. (1) Changing our reductions to get *known*

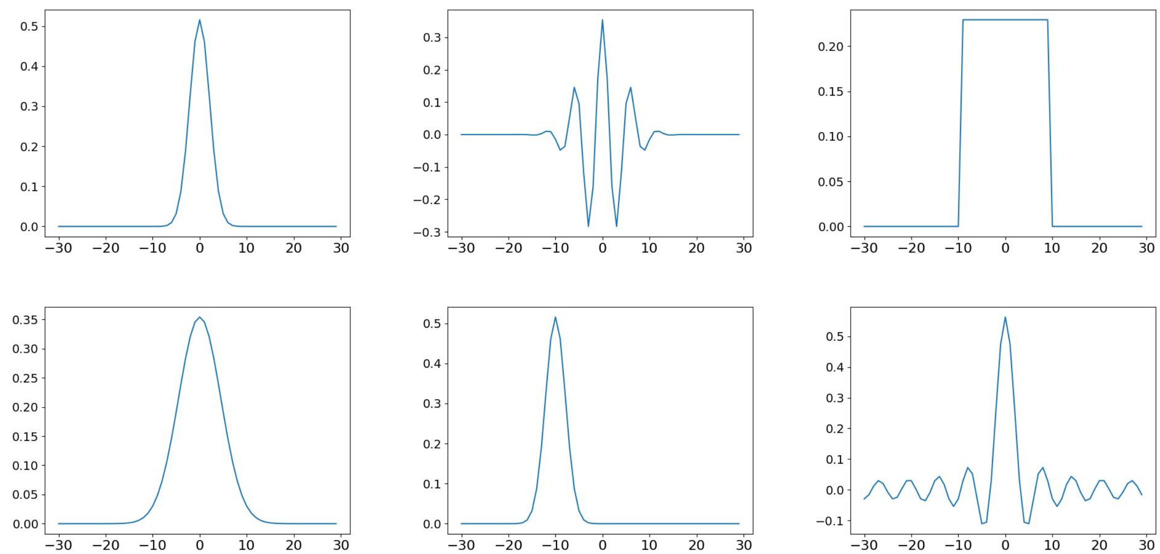


Figure 1: Interesting $\mathsf{S|LWE}\rangle$ error amplitudes (top) and their discrete Fourier transforms (bottom). All pictures are depicting the real parts of the functions. The x-axis is the input (from -30 to 29, all examples are given over $\mathbb{Z}_{60}$). The y-axis is the amplitude. Three pictures on the top from left to right are: (1) Gaussian, where our sub-exponential algorithm applies; (2) Gaussian with some phase, where our reductions apply when the phase (or the center of the DFT) is unknown; (3) bounded uniform distribution, where the algorithm in [CLZ22] applies.

phases, or (2) further modify Kuperberg's algorithm to handle unknown phases. While we have not accomplished those tasks in our paper (we really hope we have done so!), we cannot rule out the possibility either.

Organization. The rest of this paper is organized as follows. In Section 2 we provide the background of quantum computation and lattice problems. In Section 3 we provide the reduction from classical LWE to $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ via extrapolated DCP. In Section 4 we provide the reduction from worst-case lattice problem to $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ via quantizing Regev's reduction. We choose to present the reduction from classical LWE to $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ via extrapolated DCP first, since this reduction is relatively easier to follow. In Section 5 we provide our sub-exponential time quantum algorithm for $\mathsf{S|LWE}\rangle$ with completely known amplitude. Section 3, Section 4, Section 5 are in fact self-contained and independent, containing their own overview if necessary, so readers can start from any section without reading the others.

2 Preliminaries

Notations and terminology. Let $\mathbb{C}, \mathbb{R}, \mathbb{Z}, \mathbb{N}$ be the set of complex numbers, real numbers, integers and natural numbers (non-negative integers). Denote $\mathbb{Z}/q\mathbb{Z}$ by $\mathbb{Z}_q$. By default we represent the elements of $\mathbb{Z}_q$ by elements in $(-q/2, q/2] \cap \mathbb{Z}$. For any integer $q \geq 2$, let $\omega_q = e^{2\pi \mathrm{i}/q}$ denote the primitive q-th root of unity. The rounding operation $\lfloor a \rceil : \mathbb{R} \to \mathbb{Z}$ rounds a real number a to its nearest integer. For positive integer q the rounding operation $\lfloor a \rceil_q : \mathbb{R} \to q\mathbb{Z}$ rounds a real number a to its nearest integer which is a multiple of q. For $n \in \mathbb{N}$, let $[n] := \{1, 2, \cdots, n\}$.

A vector in $\mathbb{R}^n$ (represented in column form by default) is written as a bold lower-case letter, e.g. $\mathbf{v}$. For a vector $\mathbf{v}$, the i^{th} component of $\mathbf{v}$ will be denoted by v_i. A matrix is written as a bold capital letter, e.g. $\mathbf{A}$. The i^{th} column vector of $\mathbf{A}$ is denoted $\mathbf{a}_i$.

For $x \in \mathbb{R}$ and $q \in \mathbb{N}^+$, let $x \bmod q$ be the unique real number $z \in (-q/2, q/2]$ such that $x - z$ is a multiple of q. For a vector $\mathbf{v} \in \mathbb{R}^n$, we do mod coordinate-wise, i.e. the i^{th} coordinate of $\mathbf{v} \bmod q$ is given by $v_i \bmod q$. To avoid ambiguity, we give mod lower precedence than addition/subtraction. For example, $\mathbf{a} + \mathbf{b} \bmod q$ means $(\mathbf{a} + \mathbf{b}) \bmod q$.

The length of a vector is the ℓ_p-norm $\|\mathbf{v}\|_p := (\sum v_i^p)^{1/p}$, or the infinity norm given by its largest entry $\|\mathbf{v}\|_\infty := \max_i\{|v_i|\}$. The ℓ_p norm of a matrix is the norm of its longest column: $\|\mathbf{A}\|_p := \max_i \|\mathbf{a}_i\|_p$. By default we use ℓ_2-norm unless explicitly mentioned. Let $\mathbf{x} \in \mathbb{C}^n$, then $\|\mathbf{x}\|_\infty \le \|\mathbf{x}\|_2 \le \|\mathbf{x}\|_1$. Let B_p^n denote the open unit ball in $\mathbb{R}^n$ in the ℓ_p norm.

When a variable v is drawn uniformly random from the set S we denote as $v \leftarrow \mathcal{U}(S)$. When a function f is applied on a set S, it means $f(S) := \sum_{x \in S} f(x)$.

Definition 2.1 (Statistical distance). *For two distributions over $\mathbb{R}^n$ with probability density functions f_1 and f_2, we define the statistical distance between them as*

$$D(f_1, f_2) = \frac{1}{2} \int_{\mathbb{R}^n} |f_1(\mathbf{x}) - f_2(\mathbf{x})| d\mathbf{x}.$$

We say two distributions (respectively, quantum states) are ϵ-close to each other if their statistical distance (respectively, trace distance by default) is at most ϵ. We say two pure (unnormalized) states $|\phi\rangle$ and $|\psi\rangle$ are ϵ-close in ℓ_2 distance if $\||\phi\rangle - |\psi\rangle\| \le \epsilon \min(\||\phi\rangle\|, \||\psi\rangle\|)$.

Fourier transform. The Fourier transform of a function $h : \mathbb{R}^n \to \mathbb{C}$ is defined to be

$$\hat{h}(\mathbf{w}) = \int_{\mathbb{R}^n} h(\mathbf{x}) \exp(-2\pi \mathrm{i} \langle \mathbf{x}, \mathbf{w} \rangle) d\mathbf{x}.$$

Define the convolution of two functions as $f * g(\mathbf{y}) = \int_{\mathbb{R}^n} f(\mathbf{x}) g(\mathbf{y} - \mathbf{x}) d\mathbf{x}$. Then $\widehat{f * g} = \hat{f} \cdot \hat{g}$ and $\widehat{f \cdot g} = \hat{f} * \hat{g}$.

We recall some formulas about Fourier transform (cf. [Gra08, P.100, Proposition 2.2.11]). If h is defined by $h(\mathbf{x}) = g(\mathbf{x} + \mathbf{v})$ for some function $g : \mathbb{R}^n \to \mathbb{C}$ and vector $\mathbf{v} \in \mathbb{R}^n$, then

$$\hat{h}(\mathbf{w}) = \hat{g}(\mathbf{w}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w} \rangle). \tag{1}$$

If h is defined by $h(\mathbf{x}) = g(\mathbf{x}) \exp(2\pi i \langle \mathbf{x}, \mathbf{v} \rangle)$ for some function $g : \mathbb{R}^n \to \mathbb{C}$ and vector $\mathbf{v} \in \mathbb{R}^n$, then

$$\hat{h}(\mathbf{w}) = \hat{g}(\mathbf{w} - \mathbf{v}). \tag{2}$$

As a corollary of Eqns. (1) and (2), if h is defined by $h(\mathbf{x}) = f(\mathbf{x} + \mathbf{v}) \exp(2\pi i \langle \mathbf{x}, \mathbf{z} \rangle)$ for some function $f : \mathbb{R}^n \to \mathbb{C}$ and vectors $\mathbf{v}$, $\mathbf{z} \in \mathbb{R}^n$, then we define $g(\mathbf{x}) := f(\mathbf{x} + \mathbf{v})$, so $h(\mathbf{x}) = g(\mathbf{x}) \exp(2\pi i \langle \mathbf{x}, \mathbf{z} \rangle)$. Therefore $\hat{g}(\mathbf{w}) = \hat{f}(\mathbf{w}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w} \rangle)$, and

$$\hat{h}(\mathbf{w}) = \hat{g}(\mathbf{w} - \mathbf{z}) = \hat{f}(\mathbf{w} - \mathbf{z}) \cdot \exp(2\pi i \langle \mathbf{v}, \mathbf{w} - \mathbf{z} \rangle).$$

2.1 Lattices

An n-dimensional lattice $\mathcal{L}$ of rank $k \le n$ is a discrete additive subgroup of $\mathbb{R}^n$. Given k linearly independent basis vectors $\mathbf{B} = \{\mathbf{b}_1, \cdots, \mathbf{b}_k \in \mathbb{R}^n\}$, the lattice generated by $\mathbf{B}$ is

$$\mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{b}_1, \cdots, \mathbf{b}_k) = \left\{ \sum_{i=1}^{k} x_i \cdot \mathbf{b}_i, x_i \in \mathbb{Z} \right\}.$$

By default we work with full-rank lattices unless explicitly mentioned.

The minimum distance $\lambda_1(\mathcal{L})$ of a lattice $\mathcal{L}$ is the length (in the ℓ_2 norm by default) of its shortest nonzero vector: $\lambda_1(\mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L} \setminus \{\mathbf{0}\}} \|\mathbf{x}\|$. More generally, the i^{th} successive minimum $\lambda_i(\mathcal{L})$ is the smallest radius r such that $\mathcal{L}$ contains i linearly independent vectors of norm at most r. We write λ_1^p note the minimum distance measured in the ℓ_p norm.

For a point $\mathbf{y} \in \mathbb{R}^n$, its distance to $\mathcal{L}$ is given by $\mathrm{dist}(\mathbf{y}, \mathcal{L}) = \min_{\mathbf{x} \in \mathcal{L}} \{\|\mathbf{y} - \mathbf{x}\|\}$. Define "the ball around lattice" as $B_{\mathcal{L}}(r) = \{\mathbf{x} \in \mathbb{R}^n : \mathrm{dist}(\mathbf{x}, \mathcal{L}) < r\}$. For $\mathbf{y} \in B_{\mathcal{L}}(\lambda_1(\mathcal{L})/2)$, the (unique) closest vector to $\mathbf{y}$ in $\mathcal{L}$ is given by $\kappa_{\mathcal{L}}(\mathbf{y}) = \mathrm{argmin}_{\mathbf{x} \in \mathcal{L}} \{\|\mathbf{y} - \mathbf{x}\|\}$. For convenience, we omit the $\lambda_1(\mathcal{L})/2$ term and define $B_{\mathcal{L}}$ as $B_{\mathcal{L}}(\lambda_1(\mathcal{L})/2)$, over which $\kappa_{\mathcal{L}}$ is uniquely defined.

The dual of a lattice $\mathcal{L} \in \mathbb{R}^n$ is defined as

$$\mathcal{L}^* := \{\mathbf{y} \in \mathbb{R}^n : \langle \mathbf{y}, \mathbf{x} \rangle \in \mathbb{Z} \text{ for all } \mathbf{x} \in \mathcal{L}\}.$$

If $\mathbf{B}$ is a basis of a full-rank lattice $\mathcal{L}$, then $\mathbf{B}^{-T}$ is a basis of $\mathcal{L}^*$. The determinant of a full-rank lattice $\mathcal{L}(\mathbf{B})$ is $\det(\mathcal{L}(\mathbf{B})) = |\det(\mathbf{B})|$.

Lemma 2.2 (Poisson Summation Formula)**.** *For any lattice $\mathcal{L}$ and any Schwartz function $f : \mathbb{R}^n \to \mathbb{C}$, we have $f(\mathcal{L}) = \det(\mathcal{L}^*) \hat{f}(\mathcal{L}^*)$.*

Gaussians and lattices. For any $s > 0$, define the Gaussian function on $\mathbb{R}^n$ with parameter s following the convention in [MR07]

$$\forall \mathbf{x} \in \mathbb{R}^n, \ \rho_s(\mathbf{x}) = \exp(-\pi \|\mathbf{x}\|^2 / s^2).$$

For any $\mathbf{c} \in \mathbb{R}^n$, define $\rho_{s,\mathbf{c}}(\mathbf{x}) := \rho_s(\mathbf{x} - \mathbf{c})$. The subscripts s and $\mathbf{c}$ are taken to be 1 and $\mathbf{0}$ (respectively) when omitted. Note that the standard deviation of ρ_s is $s/\sqrt{2\pi}$. The Fourier transform for Gaussian satisfies $\hat{\rho_s} = s^n \rho_{1/s}$. From Poisson summation formula we have $\rho_s(\mathcal{L}) = s^n \cdot \det(\mathcal{L}^*) \cdot \rho_{1/s}(\mathcal{L}^*)$.

For a full-rank, symmetric, positive definite $n \times n$ matrix $\mathbf{\Sigma}$, define the Gaussian function on $\mathbb{R}^n$ with parameter $\sqrt{\mathbf{\Sigma}}$ following the convention in [MP12]

$$\forall \mathbf{x} \in \mathbb{R}^n, \ \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{x}) = \exp(-\pi \cdot \mathbf{x}^T \mathbf{\Sigma}^{-1} \mathbf{x}).$$

For any $\mathbf{c} \in \mathbb{R}^n$, real $s > 0$, and n-dimensional lattice $\mathcal{L}$, define the discrete Gaussian distribution $D_{\mathcal{L}+\mathbf{c},s}$ as

$$\forall \mathbf{x} \in \mathcal{L} + \mathbf{c}, \ D_{\mathcal{L}+\mathbf{c},s}(\mathbf{x}) = \frac{\rho_s(\mathbf{x})}{\rho_s(\mathcal{L} + \mathbf{c})}.$$

Similarly, for a full-rank, symmetric, positive definite $n \times n$ matrix $\mathbf{\Sigma}$, define the discrete Gaussian distribution $D_{\mathcal{L}+\mathbf{c},\sqrt{\mathbf{\Sigma}}}$ as

$$\forall \mathbf{x} \in \mathcal{L}+\mathbf{c},\ D_{\mathcal{L}+\mathbf{c},\sqrt{\mathbf{\Sigma}}}(\mathbf{x}) = \frac{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{x})}{\rho_{\sqrt{\mathbf{\Sigma}}}(\mathcal{L}+\mathbf{c})}.$$

The following Gaussian tail bound over lattices is due to Banaszczyk.

Lemma 2.3 (Lemma 1.5 of [Ban93])**.** *For any n-dimensional lattice $\mathcal{L}$, and $r \geq \frac{1}{\sqrt{2\pi}}$, $\mathbf{c} \in \mathbb{R}^n$,*

$$\begin{aligned} &\rho(\mathcal{L} \setminus B^n(r\sqrt{n})) < \left(r\sqrt{2\pi e} \cdot e^{-\pi r^2}\right)^n \rho(\mathcal{L}), \\ &\rho((\mathcal{L}-\mathbf{c}) \setminus B^n(r\sqrt{n})) < 2\left(r\sqrt{2\pi e} \cdot e^{-\pi r^2}\right)^n \rho(\mathcal{L}). \end{aligned} \tag{3}$$

As a direct corollary, for $r > \frac{C}{\sqrt{2\pi}}\alpha\sqrt{n}$ with $C > 1$ be a constant, we have that

$$\rho_\alpha((\mathcal{L}-\mathbf{c}) \setminus B^n(r)) < 2^{-\Omega(n)}\rho_\alpha(\mathcal{L}).$$

Lemma 2.4 (Claim 8.1 [RS17])**.** *For any $n \geq 1$, $s > 0$,*

$$s^n(1+2e^{-\pi s^2})^n \leq \rho_s(\mathbb{Z}^n) \leq s^n(1+(2+1/s)e^{-\pi s^2})^n.$$

Smoothing parameter. We recall the definition of smoothing parameter for Gaussian over lattices and some useful facts.

Definition 2.5 (Smoothing parameter [MR07])**.** *For any lattice $\mathcal{L}$ and positive real $\epsilon > 0$, the smoothing parameter $\eta_\epsilon(\mathcal{L})$ is the smallest real $s > 0$ such that $\rho_{1/s}(\mathcal{L}^* \setminus \{\mathbf{0}\}) \leq \epsilon$.*

Lemma 2.6 ([MR07])**.** *For any n-dimensional lattice $\mathcal{L}$, and any real $\epsilon > 0$,*

$$\eta_\epsilon(\mathcal{L}) \leq \lambda_n(\mathcal{L}) \cdot \sqrt{\ln(2n(1+1/\epsilon))/\pi}.$$

Lemma 2.7 ([Reg09])**.** *For any n-dimensional lattice $\mathcal{L}$, and any real $\epsilon > 0$,*

$$\eta_\epsilon(\mathcal{L}) \geq \sqrt{\frac{\ln 1/\epsilon}{\pi}}\frac{1}{\lambda_1(\mathcal{L}^*)}.$$

Lemma 2.8 (Claim 3.8 of [Reg09])**.** *For any n-dimensional lattice $\mathcal{L}$, $\mathbf{c} \in \mathbb{R}^n$, $\epsilon > 0$, and $r \geq \eta_\epsilon(\mathcal{L})$*

$$\rho_r(\mathcal{L}+\mathbf{c}) \in r^n \det(\mathcal{L}^*)(1 \pm \epsilon).$$

q-ary lattices. Given $n < m \in \mathbb{N}$ and a modulus $q \geq 2$, for $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, define q-ary lattices as

$$\begin{aligned} \mathcal{L}_q(\mathbf{A}) &= \left\{\mathbf{x} \in \mathbb{Z}^m : \exists \mathbf{s} \in \mathbb{Z}^n \text{ such that } \mathbf{x} = \mathbf{A}^T \cdot \mathbf{s} + q\mathbb{Z}^m\right\}; \\ \mathcal{L}_q^\perp(\mathbf{A}) &= \left\{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\cdot\mathbf{x} = \mathbf{0} \pmod q\right\}. \end{aligned}$$

Those two lattices are dual of each other up to a factor of q, i.e., $\mathcal{L}_q(\mathbf{A}) = q \cdot \mathcal{L}_q^\perp(\mathbf{A})^*$.

Lemma 2.9. *Let $q \geq 2, m \geq 2n \log_2 q$, then for all but at most $q^{-0.16n}$ fraction of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, we have*

$$\lambda_1^\infty(\mathcal{L}_q(\mathbf{A})) \geq \frac{q}{4}.$$

Proof. The lemma is proven when q is a prime in [GPV08, Lemma 5.3]. Here we extend the proof to a general q.

For any fixed non-zero $\mathbf{s} \in \mathbb{Z}_q^n$, wlog assuming s_1 is a non-zero entry of $\mathbf{s}$. Then for any $\mathbf{a} \in \mathbb{Z}_q^n$, $y := \langle \mathbf{a}, \mathbf{s}\rangle \mod q$ can be written as $y = s_1 a_1 + v \mod q$ for some $v \in \mathbb{Z}_q$. We observe that for any $q \in \mathbb{N}$, for any $v \in \mathbb{Z}_q$, for any non-zero $s_1 \in \mathbb{Z}_q$,

$$\Pr_{a_1 \in \mathbb{Z}_q}[\ s_1 a_1 + v \bmod q \in (-q/4, q/4) \cap \mathbb{Z}\ ] \leq 2/3,$$

where the equality holds when $q \in 3^k \cdot \mathbb{N}$ for some $k \geq 1$, $s_1 \in (q/3)\cdot \mathbb{Z}/q\mathbb{Z}$, $s_1 \neq 0$, and for some $v \in \mathbb{Z}_q$ (for example, when $q = 15$, $s_1 = 5$, and $v = 2$).

Therefore, over the randomness of $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the probability that $\mathbf{A}^T\mathbf{s} = \mathbf{y} \bmod q$ for some $\mathbf{y} \in \mathbb{Z}^m$ such that $\|\mathbf{y}\|_\infty < q/4$ is at most $(2/3)^m \leq (3/2)^{-2n\log_2 q} \leq q^{-1.16n}$. Applying a union bound over all $\mathbf{s} \in \mathbb{Z}_q^n$ completes the proof of Lemma 2.9. □

Lattice problems. We have formally defined the LWE, $\mathsf{S|LWE}\rangle$, and $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$ problems in the introduction. Now let us recall the definitions for other lattice problems.

The shortest vector problem (SVP) asks to find a lattice vector of length λ_1. More generally, let $\gamma(n) \geq 1$ be an approximation factor, we consider the approximation version of SVP and its close variants.

Definition 2.10 (Approximate SVP)**.** *Given a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L}$, the SVP_γ problem asks to output a non-zero lattice vector $\mathbf{Bx}$, $\mathbf{x} \in \mathbb{Z}^n \setminus \{\mathbf{0}\}$, such that $\|\mathbf{Bx}\| \leq \gamma(n)\cdot\lambda_1(\mathcal{L})$.*

Definition 2.11 (GapSVP)**.** *Given a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L}$ and a number $d > 0$, the GapSVP_γ problem asks to decide whether $\lambda_1(\mathcal{L}) \leq d$ or $\lambda_1(\mathcal{L}) > d \cdot \gamma(n)$.*

Definition 2.12 (Shortest independent vector problem (SIVP))**.** *Given a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L}$, the SIVP_γ problem asks to output a set of n linearly independent vectors of length at most $\gamma(n)\cdot\lambda_n(\mathcal{L})$.*

Definition 2.13 (Discrete Gaussian Sampling Problem (DGS))**.** *Given a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L}$ and a parameter $s > 0$, the DGS_s problem asks to output a vector whose distribution is statistically close to $D_{\mathcal{L},s}$.*

Definition 2.14 (Quantum Discrete Gaussian Sampling Problem ($|\mathsf{DGS}\rangle$))**.** *Given a basis $\mathbf{B}$ of an n-dimensional lattice $\mathcal{L}$ and a parameter $s > 0$, the $|\mathsf{DGS}\rangle_s$ problem asks to output a quantum state that is $2^{-\Omega(n)}$-close to $\sum_{\mathbf{v}\in\mathcal{L}} \rho_s(\mathbf{v})|\mathbf{v}\rangle$ in trace distance.*

If a quantum algorithm solves $|\mathsf{DGS}\rangle_s$, then it immediately solves $\mathsf{DGS}_{s/\sqrt{2}}$ by simply measuring the quantum state. Let us also recall the relationships among DGS, GapSVP, and SIVP.

Lemma 2.15 (Lemma 3.20 of [Reg09])**.** *For any $\gamma = \gamma(n) \geq 1$, there exists a polynomial time reduction from* $\mathsf{GapSVP}_{100\sqrt{n}\gamma}$ *for* $\mathcal{L}$ *to* $\mathsf{DGS}_{\sqrt{n}\gamma/\lambda_1(\mathcal{L}^*)}$ *for* $\mathcal{L}^*$*.*

Lemma 2.16 (Lemma 3.17 of [Reg09])**.** *For any $\gamma > \omega(\sqrt{\log n})$, there exists a polynomial time reduction from* $\mathsf{SIVP}_{2\sqrt{n}\gamma}$ *for* $\mathcal{L}$ *to* $\mathsf{DGS}_{\gamma\lambda_n(\mathcal{L})}$ *for* $\mathcal{L}$*.*

2.2 Quantum computation

We assume readers are familiar with the basic concepts of quantum computation. All the quantum background we need in this paper are available in standard textbooks of quantum computation, e.g., [NC16]. When writing a quantum state such as $\sum_{x\in S} f(x)|x\rangle$, we typically omit the normalization factor except when needed.

The trace distance between two quantum states ρ and σ is defined as $\delta(\rho,\sigma) := \frac{1}{2}\operatorname{tr}|\rho-\sigma|$. Note that when ρ and σ commute they are diagonal in the same basis,

$$\rho = \sum_i r_i |i\rangle\langle i|, \quad \sigma = \sum_i s_i |i\rangle\langle i|,$$

for some orthonormal basis $|i\rangle$, then $\delta(\rho,\sigma) = \frac{1}{2}\operatorname{tr}|\sum_i (r_i - s_i)|i\rangle\langle i|| = \frac{1}{2}\sum_i |r_i - s_i|$.

The trace distance is preserved under unitary transformations, and is contractive under trace-preserving operations.

Lemma 2.17. *Let $|\phi\rangle$, $|\psi\rangle$ be un-normalized vectors s.t. $\||\phi\rangle\| \geq \mu$ and $\||\phi\rangle - |\psi\rangle\| \leq \epsilon$. Then*

$$\delta\left(\frac{1}{\||\phi\rangle\|}|\phi\rangle, \frac{1}{\||\psi\rangle\|}|\psi\rangle\right) = \sqrt{1 - \left(\frac{|\langle\phi|\psi\rangle|}{\||\phi\rangle\|\||\psi\rangle\|}\right)^2} \leq O\left(\sqrt{\frac{\epsilon}{\mu}}\right).$$

Lemma 2.18 (Gentle measurement [Win99])**.** *Let ρ be a quantum state and let $(\mathbf{\Pi}, \mathbf{I} - \mathbf{\Pi})$ be a two-outcome projective measurement such that $\operatorname{tr}(\mathbf{\Pi}\rho) \geq 1-\epsilon$. Let $\rho' = \frac{\mathbf{\Pi}\rho\mathbf{\Pi}}{\operatorname{tr}(\mathbf{\Pi}\rho)}$ be the state after applying the measurement and post-selecting on getting the first outcome. Then $\delta(\rho,\rho') \leq 2\sqrt{\epsilon}$.*

We need the following lemma about the trace distance between discrete Gaussian states.

Lemma 2.19. *When $q > 2\sqrt{n}\max(\beta_1,\beta_2)$ and $R \geq \frac{2\sqrt{n}}{\min(\beta_1,\beta_2)}$, the trace distance between*

$$|\phi_1\rangle = \sum_{e\in\mathbb{Z}_{qR}/R} \rho_{\beta_1}(e)|e\rangle \qquad \text{and} \qquad |\phi_2\rangle = \sum_{e\in\mathbb{Z}_{qR}/R} \rho_{\beta_2}(e)|e\rangle$$

is at most $\sqrt{\frac{(\beta_1-\beta_2)^2}{\beta_1^2+\beta_2^2}}(1+2^{-\Omega(n)})$.

Proof.

$$\begin{aligned}\frac{\langle\phi_1|\phi_2\rangle}{\||\phi_1\rangle\|\||\phi_2\rangle\|} &= \sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\frac{\beta_1\beta_2}{\sqrt{\beta_1^2+\beta_2^2}}}(e)\Big/\sqrt{\sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\beta_1/\sqrt{2}}(e)\sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\beta_2/\sqrt{2}}(e)}\\ &= \sum_{e\in\mathbb{Z}/R}\rho_{\frac{\beta_1\beta_2}{\sqrt{\beta_1^2+\beta_2^2}}}(e)\Big/\sqrt{\sum_{e\in\mathbb{Z}/R}\rho_{\beta_1/\sqrt{2}}(e)\sum_{e\in\mathbb{Z}/R}\rho_{\beta_2/\sqrt{2}}(e)}\,(1+2^{-\Omega(n)})\\ &= \frac{\beta_1\beta_2}{\sqrt{\beta_1^2+\beta_2^2}}\cdot\frac{\sqrt{2}}{\sqrt{\beta_1\beta_2}}\sum_{e\in R\mathbb{Z}}\rho_{\frac{\sqrt{\beta_1^2+\beta_2^2}}{\beta_1\beta_2}}(e)\Big/\sqrt{\sum_{e\in R\mathbb{Z}}\rho_{\sqrt{2}/\beta_1}(e)\sum_{e\in R\mathbb{Z}}\rho_{\sqrt{2}/\beta_2}(e)}\,(1+2^{-\Omega(n)})\\ &= \frac{\sqrt{2\beta_1\beta_2}}{\sqrt{\beta_1^2+\beta_2^2}}(1+2^{-\Omega(n)}),\end{aligned}$$

where we use the Poisson summation formula and Banaszczyk's tail bound.

So their trace distance is at most

$$\sqrt{1-\left(\frac{|\langle\phi_1|\phi_2\rangle|}{\||\phi_1\rangle\|\||\phi_2\rangle\|}\right)^2}\le\sqrt{\frac{(\beta_1-\beta_2)^2}{\beta_1^2+\beta_2^2}}(1+2^{-\Omega(n)}).$$ □

We use the following quantum algorithms:

Lemma 2.20 (Quantum Fourier Transform (QFT) [Kit95])**.** *Let $q\ge 2$ be an integer. The following unitary operator QFT_q can be implemented by $\mathsf{poly}(\log q)$ elementary quantum gates. When QFT_q is applied on a quantum state $|\phi\rangle := \sum_{x\in\mathbb{Z}_q} f(x)|x\rangle$, we have*

$$\mathsf{QFT}_q|\phi\rangle=\sum_{y\in\mathbb{Z}_q}\sum_{x\in\mathbb{Z}_q}\frac{1}{\sqrt{q}}\cdot e^{-2\pi\mathrm{i}\cdot xy/q}\cdot f(x)|y\rangle.$$

We use the following lemma [ORR13] to change the amplitude of a state.

Lemma 2.21 (Quantum rejection sampling)**.** *Let $f: D\to\mathbb{C}$ be a normalized amplitude of some quantum state $|\phi_f\rangle := \sum_{x\in D} f(x)|x\rangle$. Let $\gamma: D\to[0,1]$ be a polynomial time computable function. There is a quantum algorithm that takes as input $|\phi_f\rangle$, outputs a state $\sum_{x\in D}\frac{1}{\sqrt{M}}\gamma(x)f(x)|x\rangle$ with probability M where $M=\sum_{x\in D}\gamma^2(x)|f(x)|^2$.*

In this paper we are interested in preparing the Gaussian state $|\sigma_{n,R}\rangle := \sum_{\mathbf{x}\in\mathbb{Z}^n\cap B^n(R\sqrt{n})}\rho_R(\mathbf{x})|\mathbf{x}\rangle$ for some radius $R\le 2^{\mathsf{poly}(n)}$. Given Lemma 2.3, there is a $2^{-\Omega(n)}$ mass in the tail of $\rho_R(\mathbf{x})$ outside $B^n(R\sqrt{n})$. This means for any integer $P\in(2R\sqrt{n},2^{\mathsf{poly}(n)})$, $|\sigma_{n,R}\rangle$ is $2^{-\Omega(n)}$ close to $\sum_{\mathbf{x}\in\mathbb{Z}_P^n}\rho_R(\mathbf{x})|\mathbf{x}\rangle$. This also means we can prepare $|\sigma_{n,R}\rangle$ by generating n independent samples of one-dimensional Gaussian state $|\sigma_{1,R}\rangle$, which can be done efficiently using [GR02].

Lemma 2.22 (Gaussian state preparation)**.** *Let $n,R\in\mathbb{N}$ such that $1\le R\le 2^{n^c}$ for some constant $c\ge 0$. Then we can create a $\mathsf{poly}(n)$ size unitary U that maps $|\mathbf{0}\rangle$ to a state within trace distance $2^{-\Omega(n)}$ from $|\sigma_{n,R}\rangle$ with $2n\lceil n^c\cdot\log n\rceil$ qubits.*

3 Reduction via Extrapolated DCP

In this section, we show how to obtain a quantum reduction from classical LWE to $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$ with Gaussian amplitude. Our reduction goes through the Extrapolated Dihedral Coset problem (EDCP), derived from a modification of the reduction by Regev [Reg04] and Brakerski et al. [BKSW18]. Our reduction consists of two steps:

Step 1 Given a classical LWE instance, our quantum reduction first generates an Extrapolated DCP state with amplitudes following a Gaussian distribution centered at an unknown value. More precisely, we establish the following theorem:

Theorem 3.1. *Let $n, m, q \in \mathbb{N}^+$, $\alpha, \beta, \gamma \in \mathbb{R}^+$ satisfy $m \geq n \log q$, $\alpha = \Omega(\sqrt{n})$, $\alpha\gamma\sqrt{m} < \beta < \frac{q}{16\sqrt{m \log \beta}}$. There exists a $\mathsf{poly}(n)$ time quantum algorithm that, given a classical LWE instance $\mathsf{LWE}_{n,m,q,\gamma} = (\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$, generates, with probability $1 - 2^{-\Omega(n)}$, a vector $\mathbf{y} \in \mathbb{Z}_q^m \cap B_{\mathcal{L}_q(\mathbf{A})}$ and an Extrapolated DCP state of form*

$$|\mathsf{EDCP}\rangle = \sum_{j \in \mathbb{Z}_q} \rho_\sigma(j - c)|j\rangle|(\mathbf{v} + j \cdot \mathbf{s}) \bmod q\rangle, \tag{4}$$

where

1. *the vector $\mathbf{v}$ is chosen uniformly at random from $\mathbb{Z}_q^n$ and is unknown.*
2. *the Gaussian width $\sigma = \frac{\alpha\beta}{\sqrt{\alpha^2\|\mathbf{e}\|^2 + \beta^2}}$.*
3. *the vector $\mathbf{y}$ is sampled by first sampling $\mathbf{x} \in \mathbb{Z}^m \cap B^m(\lambda_1(\mathcal{L}_q(\mathbf{A}))/2)$ with probability proportional to $\Pr(\mathbf{x}) \propto \rho_{\beta\sqrt{\mathbf{\Sigma}/2}}(\mathbf{x})$ where $\mathbf{\Sigma} = \mathbf{I}_m + \frac{\alpha^2}{\beta^2}\mathbf{e}\mathbf{e}^T$, then outputting $\mathbf{y} = (\mathbf{A}^T\mathbf{v} + \mathbf{x}) \bmod q$.*
3. *the center $c = -\frac{\alpha^2\langle \mathbf{x}, \mathbf{e}\rangle}{\alpha^2\|\mathbf{e}\|^2 + \beta^2}$ (we don't know how to efficiently compute c with success probability $1 - 2^{-\Omega(n)}$ since we don't know $\mathbf{x}$ and $\mathbf{e}$; we can guess c correctly with non-negligible probability, but the event of guessing correctly is not efficiently checkable).*

Step 2 Given an Extrapolated DCP state with amplitudes following a Gaussian distribution centered at an unknown value, we adapt the quantum reduction proposed by Brakerski et al. [BKSW18] to transform it to an $\mathsf{S}|\mathsf{LWE}\rangle$ instance. The resulting $\mathsf{S}|\mathsf{LWE}\rangle$ instance will have amplitudes represented as a Gaussian distribution multiplied by an unknown phase term. More precisely, we establish the following theorem:

Theorem 3.2. *There exists an efficient quantum algorithm that, given an Extrapolated DCP state of form as Equation (4), generates an $\mathsf{S}|\mathsf{LWE}\rangle$ state of form*

$$\mathsf{S}|\mathsf{LWE}\rangle = \sum_{e \in \mathbb{Z}} \rho_{q/\sigma}(e) \exp(2\pi \mathrm{i} \cdot ce/q)|(\langle \mathbf{a}, \mathbf{s}\rangle + e) \bmod q\rangle \tag{5}$$

along with a known vector $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$. Here the parameters σ, c correspond to those mentioned in Theorem 3.1.

In the remaining part of this section, we will provide the detailed proofs for Theorem 3.1 and Theorem 3.2. By combining these two theorems, we achieve a quantum reduction from classical LWE to $\mathsf{S|LWE}\rangle$, whose amplitude is represented as a Gaussian distribution multiplied by an unknown phase term. This establishes that solving the classical LWE problem is as hard as solving the quantum variant $\mathsf{S|LWE}\rangle$ with an "unknown phase". Formally, we define our special parameters and functions, and propose the main theorem for this section here:

Definition 3.3. *Let $n, m, q \in \mathbb{N}^+$, $\alpha, \beta, \gamma \in \mathbb{R}^+$ satisfy $m \geq n \log q$, $\alpha = \Omega(\sqrt{n})$, $\alpha\gamma\sqrt{m} < \beta < \frac{q}{16\sqrt{m \log \beta}}$. Given a classical LWE instance $\mathsf{LWE}_{n,m,q,\gamma} = (\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$, we define:*

1. *A family of functions $\{f_E : \mathbb{Z} \to \mathbb{R}\}_{E \in \mathbb{N}}$ with $f_E(e) = \rho_{q/\sigma(E)}(e)$ where $\sigma(E) = \frac{\alpha\beta}{\sqrt{\alpha^2 E + \beta^2}}$ is known given E, α, β.*
2. *A distribution $D_{\theta,\mathbf{e}}(\mathbf{y})$ over $\mathbb{Z}_q^m \cap B_{\mathcal{L}_q(\mathbf{A})}$ given by $\Pr(\mathbf{y}) \propto \rho_{\beta\sqrt{\mathbf{\Sigma}/2}}(\mathbf{y}')$ where $\mathbf{\Sigma} = \mathbf{I}_m + \frac{\alpha^2}{\beta^2}\mathbf{e}\mathbf{e}^T$ and $\mathbf{y}' = \mathbf{y} - \kappa_{\mathcal{L}_q(\mathbf{A})}(\mathbf{y})$.*
3. *A family of functions $\{\theta_{E,\mathbf{e}} : \mathbb{Z}_q^m \cap B_{\mathcal{L}_q(\mathbf{A})} \to \mathbb{R}\}_{E \in \mathbb{N}}$ with $\theta_{E,\mathbf{e}}(\mathbf{y}) = -\frac{\alpha^2 \langle \mathbf{y}', \mathbf{e} \rangle}{q(\alpha^2 E + \beta^2)}$ (This family of functions is not efficiently computable when assuming classcial LWE is hard).*

Theorem 3.4 (Main theorem, from LWE to $\mathsf{S|LWE}\rangle^{\mathsf{phase}}$)**.** *Following the parameters defined in Definition 3.3. Given a classical LWE sample $(\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$, assuming there exists quantum algorithms that can solve $\mathsf{S|LWE}\rangle^{\mathsf{phase}}_{n,\ell,q,f_E,\theta_{E,\mathbf{e}},D_{\theta,\mathbf{e}}}$ for all $E \in \{1, 2, \cdots, \lceil \gamma^2 m \rceil\}$, with $\ell = 2^{o(n)}$ and time complexity $T = 2^{o(n)}$, then there exists a quantum algorithm capable of solving for the secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ from the LWE instance $(\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$, with success probability $1 - 2^{-\Omega(n)}$ and time complexity $O((T + \ell \cdot \mathsf{poly}(n, q)) \cdot \gamma^2 m)$.*

Remark 3.5. *A typical setting of parameters is to let $\gamma \geq 2\sqrt{n}$ and $m \in \Omega(n \log q)$, then the smallest modulus q can be $q = \widetilde{\Theta}(\beta\sqrt{m}) = \widetilde{\Theta}(n^2)$.*

Proof. We proceed to address the classical LWE instance $(\mathbf{A}, \mathbf{A}^T\mathbf{s} + \mathbf{e})$ as follows:

1. Enumerate $E \in \{1, 2, \cdots, \lceil \gamma^2 m \rceil\}$ to make a guess for $\|\mathbf{e}\|^2$.
2. Apply Theorem 3.1 and Theorem 3.2 ℓ times to generate ℓ instances of $\mathsf{S|LWE}\rangle$ in the form of Equation (5).
3. Utilize the quantum algorithm in the assumption for $\mathsf{S|LWE}\rangle^{\mathsf{phase}}_{n,\ell,q,f_E,\theta_{E,\mathbf{e}},D_{\theta,\mathbf{e}}}$, with those ℓ $\mathsf{S|LWE}\rangle$ instances as input, to derive a solution $\mathbf{s}'$.
4. Employ any verification algorithm (e.g., as proposed by Regev [Reg09, Lemma 3.6]) to ascertain whether $\mathbf{s}' = \mathbf{s}$. If this condition holds, output $\mathbf{s}'$ and conclude the process.

It can be easily verified that this algorithm operates with a runtime of $O((T + \ell \cdot \mathsf{poly}(q, n)) \cdot \gamma^2 m)$. Furthermore, as indicated in Theorem 3.1, the probability of successfully generating ℓ $\mathsf{S|LWE}\rangle$ states in step 2 is exponentially close to 1. Thus, when $E = \|\mathbf{e}\|^2$ (i.e., when we guess E correctly), the probability that the solution $\mathbf{s}' = \mathbf{s}$ is exponentially close to 1. Consequently, the aforementioned algorithm achieves success probability exponentially close to 1. ∎

3.1 Reduce classical LWE to Extrapolated DCP

Our quantum reduction from classical LWE to Extrapolated DCP follows the general design of Regev's reduction [Reg04] and the reduction proposed by Brakerski et al. [BKSW18]. In these reductions, the Euclidean space $\mathbb{R}^n$ is divided into grids, with each grid cell having a width that lies between the length of the error vector $\|\mathbf{e}\|$ and the length of the shortest vector in the lattice $\lambda_1(\mathcal{L}_q(\mathbf{A}))$. The key observation is that when randomly selecting a vector $\mathbf{x} \in \mathbb{R}^n$, the vectors $\mathbf{x}, \mathbf{x}+\mathbf{e}, \cdots, \mathbf{x}+k\cdot\mathbf{e}$ will be in the same grid cell with high probability, creating a superposition in the quantum world.

We modify the reductions in [Reg04, BKSW18] by introducing Gaussian balls around all lattice points in $\mathcal{L}_q(\mathbf{A})$, where the radius of each ball is a quantity smaller then the length of shortest vector in the lattice $\lambda_1(\mathcal{L}_q(\mathbf{A}))$. Note that the reductions in [Reg04, BKSW18] use Euclidean balls or cubes.

Here we give the detailed proof of Theorem 3.1.

Proof of Theorem 3.1. Following the parameters defined in Theorem 3.1. Relying on both Lemma 2.9 and Banaszczyk's tail bound from Lemma 2.3, we make the assumptions that $\lambda_1(\mathcal{L}_q(\mathbf{A})) \geq \frac{q}{4}$ and $\|\mathbf{e}\| < \gamma\sqrt{m}$ for the remainder of this proof; these assumptions hold with probability $1 - 2^{-\Omega(n)}$. Our quantum reduction from classical LWE to Extrapolated DCP works as follows (for simplicity, we omit the normalization factors):

1. We start by preparing the superposition using the Gaussian state sampler (see Lemma 2.22)
$$\sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)|j\rangle \sum_{\mathbf{v}\in\mathbb{Z}_q^n} |\mathbf{v}\rangle \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\beta(\mathbf{x})|\mathbf{x}\rangle.$$

2. We apply a unitary to compute $(j, \mathbf{v}, \mathbf{x}) \to (\mathbf{A}^T\mathbf{v} - j\cdot(\mathbf{A}^T\mathbf{s}+\mathbf{e}) + \mathbf{x}) \bmod q$ on the third register, obtaining the state
$$\sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)|j\rangle \sum_{\mathbf{v}\in\mathbb{Z}_q^n} |\mathbf{v}\rangle \sum_{\mathbf{x}\in\mathbb{Z}_q^m} \rho_\beta(\mathbf{x})|(\mathbf{A}^T\mathbf{v} - j\cdot(\mathbf{A}^T\mathbf{s}+\mathbf{e}) + \mathbf{x}) \bmod q\rangle. \tag{6}$$

   This state approximates, with an error of $1 - 2^{-\Omega(n)}$, the same state structure with the only difference being the range of $\mathbf{x}$ in the summation, which is now $\mathbb{Z}^m$ rather than $\mathbb{Z}_q^m$. By expressing $\mathbf{A}^T\mathbf{v} - j\cdot(\mathbf{A}^T\mathbf{s}+\mathbf{e}) + \mathbf{x}$ as $\mathbf{A}^T(\mathbf{v} - j\cdot\mathbf{s}) + (\mathbf{x} - j\cdot\mathbf{e})$, we perform a change of variables $\mathbf{v} \leftarrow (\mathbf{v} + j\cdot\mathbf{s}) \bmod q$ and $\mathbf{x} \leftarrow \mathbf{x} + j\cdot\mathbf{e}$, yields that the state of form Equation (6) is $2^{-\Omega(n)}$-close to the state
$$\sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)|j\rangle \sum_{\mathbf{v}\in\mathbb{Z}_q^n} |(\mathbf{v} + j\cdot\mathbf{s}) \bmod q\rangle \sum_{\mathbf{x}\in\mathbb{Z}^m} \rho_\beta(\mathbf{x} + j\cdot\mathbf{e})|(\mathbf{A}^T\mathbf{v} + \mathbf{x}) \bmod q\rangle. \tag{7}$$

   To proceed, we need the following lemma to guarantee that each vector in the support of the third register $\mathbf{y} := \mathbf{A}^T\mathbf{v} + \mathbf{x} \bmod q$ corresponds to a unique $\mathbf{x}$, in order to match with the target of Theorem 3.1 and to simplify later analyses. The proof of this lemma is deferred to Appendix A.2.

Lemma 3.6. *Assume that* $(\beta\sqrt{m}+\alpha\gamma m)\sqrt{\log\beta} < \lambda_1(\mathcal{L}_q(\mathbf{A}))/2$ *and* $\beta > \sqrt{m}$*, then the state in Equation (7) is* $2^{-\Omega(n)}$*-close to the state*

$$\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)|j\rangle\sum_{\mathbf{v}\in\mathbb{Z}_q^n}|(\mathbf{v}+j\cdot\mathbf{s}) \bmod q\rangle \sum_{\substack{\mathbf{x}\in\mathbb{Z}^m,\\ \|\mathbf{x}\|<\lambda_1(\mathcal{L}_q(\mathbf{A}))/2}}\rho_\beta(\mathbf{x}+j\cdot\mathbf{e})|(\mathbf{A}^T\mathbf{v}+\mathbf{x}) \bmod q\rangle. \quad (8)$$

Under the condition of Theorem 3.1, $(\beta\sqrt{m}+\alpha\gamma m)\sqrt{\log\beta} < 2\beta\sqrt{m\log\beta} < q/8 < \lambda_1(\mathcal{L}_q(\mathbf{A}))/2$ and $\beta > \alpha\gamma\sqrt{m} > \sqrt{m}$, so the state in Equation (7) is $2^{-\Omega(n)}$-close to the state in Equation (8), which can be rewritten as follows

$$\sum_{\substack{\mathbf{v}\in\mathbb{Z}_q^n,\mathbf{x}\in\mathbb{Z}^m,\\ \|\mathbf{x}\|<\lambda_1(\mathcal{L}_q(\mathbf{A}))/2}}\left(\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)\rho_\beta(\mathbf{x}+j\cdot\mathbf{e})|j\rangle|(\mathbf{v}+j\cdot\mathbf{s}) \bmod q\rangle\right)|(\mathbf{A}^T\mathbf{v}+\mathbf{x}) \bmod q\rangle \quad (9)$$

3. We measure the state in Equation (9) on the third register and denote the result as $\mathbf{y} = (\mathbf{A}^T\mathbf{v}+\mathbf{x}) \bmod q$ (note that we have $\|\mathbf{x}\| < \lambda_1(\mathcal{L}_q(\mathbf{A}))/2$, so the vectors $\mathbf{v}$ and $\mathbf{x}$ are both unique), then the remaining state on the first two registers is

$$\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)\rho_\beta(\mathbf{x}+j\cdot\mathbf{e})|j\rangle|(\mathbf{v}+j\cdot\mathbf{s}) \bmod q\rangle.$$

The amplitude of this state is computed as follows

$$\begin{aligned}\rho_\alpha(j)\rho_\beta(\mathbf{x}+j\cdot\mathbf{e}) &= \exp\left[-\pi\left(\frac{j^2}{\alpha^2}+\frac{j^2\|\mathbf{e}\|^2+2j\langle\mathbf{x},\mathbf{e}\rangle+\|\mathbf{x}\|^2}{\beta^2}\right)\right]\\ &\propto \exp\left[-\pi\left(\frac{(\alpha^2\|\mathbf{e}\|^2+\beta^2)j^2+2j\alpha^2\langle\mathbf{x},\mathbf{e}\rangle}{\alpha^2\beta^2}\right)\right]\\ &\propto \rho_\sigma(j-c),\end{aligned}$$

where the Gaussian width $\sigma = \frac{\alpha\beta}{\sqrt{\alpha^2\|\mathbf{e}\|^2+\beta^2}} \in (\alpha/\sqrt{2},\alpha)$ and the center $c = -\frac{\alpha^2\langle\mathbf{x},\mathbf{e}\rangle}{\alpha^2\|\mathbf{e}\|^2+\beta^2}$. Unfortunately, the center c remains unknown because we have no knowledge of $\mathbf{x}$ other than that it is the error term in the LWE sample $\mathbf{y} = (\mathbf{A}^T\mathbf{v}+\mathbf{x}) \bmod q$. The analysis of the distribution of $\mathbf{y}$ and c is deferred to Section 3.3.

It's evident that in the state of Equation (8), the amplitude for every $\mathbf{v}\in\mathbb{Z}_q^n$ is the same, which implies that the distribution of the vector $\mathbf{v}$ is uniformly random. This completes the proof. □

Remark 3.7. *It seems that our reduction bears similarities to the reduction from classical LWE to G-EDCP (Extrapolated DCP with amplitudes following a Gaussian distribution) proposed by Brakerski et al. [BKSW18]. However, our reduction, compared to both Regev's reduction and Brakerski et al.'s reduction, exhibits superior success probability. In the previous reductions, the failure probability is inverse-polynomial, leading to the reduction of classical LWE to only polynomially many (Extrapolated) DCP states. In contrast, our reduction achieves* $1-2^{-\Omega(n)}$ *success probability, allowing for the construction of sub-exponentially many Extrapolated DCP states without failure, the cost is introducing an unknown center in the Gaussian distribution of the amplitude. This novel approach offers the potential for creating sub-exponential time quantum algorithms for the standard LWE problem.*

3.2 Reduce Extrapolated DCP to $\mathsf{S|LWE\rangle}$

The second step of our quantum reduction from classical LWE to $\mathsf{S|LWE\rangle^{phase}}$ involves reducing the obtained Extrapolated DCP states to $\mathsf{S|LWE\rangle^{phase}}$. This step is an adaptation of the reduction from G-EDCP to LWE proposed by Brakerski et al. [BKSW18]. We give the detailed proof of Theorem 3.2 here.

Proof of Theorem 3.2. Suppose we are given an Extrapolated DCP state with the form as Equation (4). Our quantum reduction works as follows (for simplicity, we omit the normalization factors):

1. Apply Quantum Fourier Transformation on $\mathbb{Z}_q^n$ for the second register, obtaining the state

$$\sum_{\mathbf{a}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}_q}\omega_q^{\langle\mathbf{a},\mathbf{v}+j\cdot\mathbf{s}\rangle}\rho_\sigma(j-c)|j\rangle|\mathbf{a}\rangle.$$

2. Measure the second register to get a particular measurement result $\hat{\mathbf{a}}$, which is randomly chosen from $\mathbb{Z}_q^n$ with a uniform distribution. By omitting the global phase term $\omega_q^{\langle\hat{\mathbf{a}},\mathbf{v}\rangle}$, the remaining state is

$$\sum_{j\in\mathbb{Z}_q}\omega_q^{\langle\hat{\mathbf{a}},j\cdot\mathbf{s}\rangle}\rho_\sigma(j-c)|j\rangle.$$

3. Apply another Quantum Fourier Transformation on $\mathbb{Z}_q$ and incorporate Gaussian tails of j again, obtaining a state $2^{-\Omega(n)}$-close to the state

$$\sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}}\omega_q^{j(\langle\hat{\mathbf{a}},\mathbf{s}\rangle+b)}\rho_\sigma(j-c)|b\rangle.$$

4. Use the Poisson summation formula on the amplitude and change the summation variable to $e\leftarrow\langle\hat{\mathbf{a}},\mathbf{s}\rangle+b-q\cdot j$, this state can be rewritten as

$$\begin{aligned}&\sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}}\omega_q^{j(\langle\hat{\mathbf{a}},\mathbf{s}\rangle+b)}\rho_\sigma(j-c)|b\rangle\\ =&\sum_{b\in\mathbb{Z}_q}\sum_{j\in\mathbb{Z}}\sigma\rho_{1/\sigma}\left(j-\frac{\langle\hat{\mathbf{a}},\mathbf{s}\rangle+b}{q}\right)\cdot\exp\left(-2\pi\mathrm{i}\cdot c\left(j-\frac{\langle\hat{\mathbf{a}},\mathbf{s}\rangle+b}{q}\right)\right)|b\rangle\\ \propto&\sum_{e\in\mathbb{Z}}\rho_{q/\sigma}(e)\cdot\exp(2\pi\mathrm{i}\cdot ce/q)|(\langle-\hat{\mathbf{a}},\mathbf{s}\rangle+e)\bmod q\rangle\end{aligned}$$

Finally, this state along with the classical vector $-\hat{\mathbf{a}}$ will be the output $\mathsf{S|LWE\rangle^{phase}}$ instance of our quantum reduction. □

3.3 The distribution of unknown center

For additional technical insights, we present a more detailed analysis of the distribution of center c in the Extrapolated DCP states (see Equation (4)) we get. To achieve this, we begin by examining the distribution of $\mathbf{x}$ after measurement on the third register of the state given in Equation (9). It is evident that the probability of obtaining a specific vector $\mathbf{x}$ is proportional to

$$\begin{aligned}\Pr(\mathbf{x}) &\propto \sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)^2 \rho_\beta(\mathbf{x}+j\cdot\mathbf{e})^2 \\ &\approx \sum_{j\in\mathbb{Z}} \rho_\alpha(j)^2 \rho_\beta(\mathbf{x}+j\cdot\mathbf{e})^2 \\ &= \sum_{j\in\mathbb{Z}} \exp\left[-2\pi\left(\frac{j^2}{\alpha^2}+\frac{j^2\|\mathbf{e}\|^2+2j\langle\mathbf{x},\mathbf{e}\rangle+\|\mathbf{x}\|^2}{\beta^2}\right)\right] \\ &= \sum_{j\in\mathbb{Z}} \rho_{\sigma/\sqrt{2}}(j-c)\cdot\exp\left[-2\pi\left(\frac{\|\mathbf{x}\|^2}{\beta^2}-\frac{\alpha^2\langle\mathbf{x},\mathbf{e}\rangle^2}{\beta^2(\alpha^2\|\mathbf{e}\|^2+\beta^2)}\right)\right].\end{aligned}$$

We observe that $\sigma = \frac{\alpha\beta}{\sqrt{\alpha^2\|\mathbf{e}\|^2+\beta^2}} > \frac{\alpha}{\sqrt{2}} = \Omega(\sqrt{n})$, which implies that almost all of the weight of $\rho_{\sqrt{2}/\sigma}$ is concentrated at $\rho_{\sqrt{2}/\sigma}(0)$ with exponentially small weight elsewhere. Using the Poisson summation formula, we get that

$$\sum_{j\in\mathbb{Z}} \rho_{\sigma/\sqrt{2}}(j-c) = \sum_{j\in\mathbb{Z}} \frac{\sigma}{\sqrt{2}}\rho_{\sqrt{2}/\sigma}(j)\cdot\exp(-2\pi\mathrm{i}\cdot cj) \in \frac{\sigma}{\sqrt{2}}(1\pm 2^{-\Omega(n)}).$$

Let us denote $\mathbf{\Sigma} = \left(\mathbf{I}_m - \frac{\alpha^2}{\alpha^2\|\mathbf{e}\|^2+\beta^2}\mathbf{e}\mathbf{e}^T\right)^{-1} = \mathbf{I}_m + \frac{\alpha^2}{\beta^2}\mathbf{e}\mathbf{e}^T$, the remaining term can be written as

$$\begin{aligned}\exp\left[-2\pi\left(\frac{\|\mathbf{x}\|^2}{\beta^2}-\frac{\alpha^2\langle\mathbf{x},\mathbf{e}\rangle^2}{\beta^2(\alpha^2\|\mathbf{e}\|^2+\beta^2)}\right)\right] &= \exp\left[-2\pi\cdot\frac{1}{\beta^2}(\mathbf{x})^T\left(\mathbf{I}_m-\frac{\alpha^2}{\alpha^2\|\mathbf{e}\|^2+\beta^2}\mathbf{e}\mathbf{e}^T\right)\mathbf{x}\right] \\ &= \exp\left[-2\pi\cdot\frac{1}{\beta^2}(\mathbf{x})^T\mathbf{\Sigma}^{-1}\mathbf{x}\right] \\ &= \rho_{\beta\sqrt{\mathbf{\Sigma}/2}}(\mathbf{x}).\end{aligned}$$

This means that the distribution of $\mathbf{x}$ follows the discrete Gaussian distribution with center $\mathbf{0}$ and covariance matrix $\beta^2\mathbf{\Sigma}/2$. Correspondingly, the distribution of $\mathbf{y}\in\mathbb{Z}_q^m\cap B_{\mathcal{L}_q(\mathbf{A})}$ is given by $\Pr(\mathbf{y}) = \rho_{\beta\sqrt{\mathbf{\Sigma}/2}}(\mathbf{x})$.

To derive the distribution of the unknown center $c = \frac{\alpha^2\langle\mathbf{x},\mathbf{e}\rangle}{\alpha^2\|\mathbf{e}\|^2+\beta^2}$, we emphasize that the probability of every entry in $\mathbf{e}$ having a greatest common divisor of 1 is exponentially close to 1, and the distribution of $\mathbf{x}$ is smooth enough to be treated as a continuous Gaussian distribution since the eigenvector of $\beta^2\mathbf{\Sigma}/2$ are $\beta^2/2$ and $(\beta^2+\alpha^2\|\mathbf{e}\|^2)/2$. So the distribution of the unknown center c can be approximated by the discrete Gaussian distribution with minimum step $\frac{\alpha^2}{\alpha^2\|\mathbf{e}\|^2+\beta^2}$, center 0 and variance

$$\sigma_c^2 = \left(\frac{\alpha^2}{\alpha^2\|\mathbf{e}\|^2+\beta^2}\right)^2\cdot\mathbf{e}^T\left(\beta^2\mathbf{\Sigma}/2\right)\mathbf{e} = \frac{\alpha^4\|\mathbf{e}\|^2}{2(\alpha^2\|\mathbf{e}\|^2+\beta^2)}.$$

In conclusion, we propose the following statement for the distribution of the unknown center in the Extrapolated DCP states:

Theorem 3.8. *The distribution of c in Equation (4) of Theorem 3.1 approximately follows the discrete Gaussian distribution $D_{\frac{\alpha^2}{\alpha^2\|\mathbf{e}\|^2+\beta^2}\mathbb{Z},\sigma_c}$ where $\sigma_c = \frac{\alpha^2\|\mathbf{e}\|}{\sqrt{2(\alpha^2\|\mathbf{e}\|^2+\beta^2)}}$.*

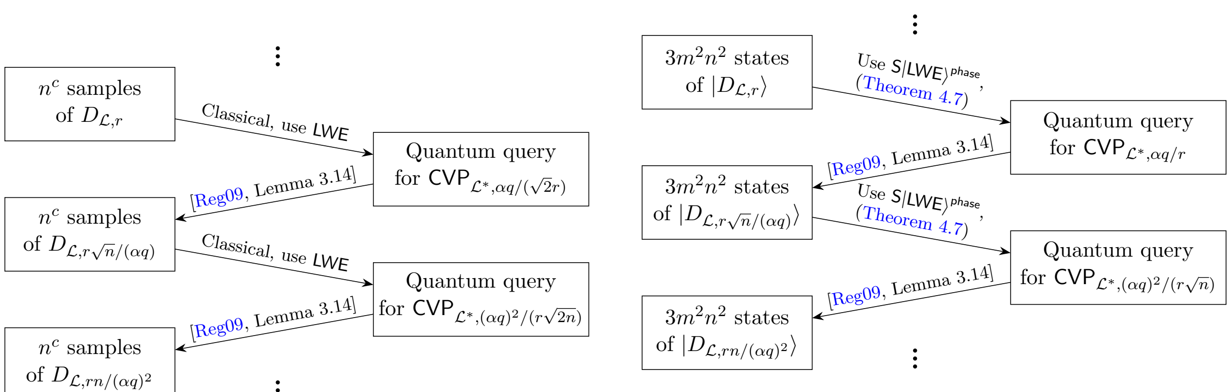
Remark 3.9. *As readers may notice, the Gaussian width σ of j and the Gaussian width σ_c of c (the center of the distribution of j) satisfy $\sigma_c = \frac{\alpha\|\mathbf{e}\|}{\sqrt{2}\beta}\sigma$. In our settings, if we assume $\beta \gg \alpha \cdot \|\mathbf{e}\|$, then the distribution of j is a discrete Gaussian distribution with a small shift. However, this shift is non-negligible, preventing our $\mathsf{S}|\mathsf{LWE}\rangle$-like state from being exponentially close to a $\mathsf{S}|\mathsf{LWE}\rangle$ state without unknown phase.*

4 Reduction via Quantizing Regev's Iterative Reduction

In this section, we show how to reduce from the problem of generating discrete Gaussian states ($|\mathsf{DGS}\rangle$, Definition 2.14) to a variant of $\mathsf{S}|\mathsf{LWE}\rangle$ with an unknown phase term on the amplitude ($\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$), by modifying Regev's iterative reduction [Reg09] from the problem of generating discrete Gaussian samples (DGS, Definition 2.13) to LWE. Combined with the known reductions from GapSVP and SIVP to DGS in Lemma 2.15 and Lemma 2.16, it gives a quantum reduction from $\mathsf{GapSVP}_{\tilde{O}(n^{1.5})}$ and $\mathsf{SIVP}_{\tilde{O}(n^{1.5})}$ to $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$.

4.1 Overview of our reduction

As in [Reg09], our proof is iterative. We start from generating discrete Gaussian states with exponentially large widths (discrete Gaussian samples with exponentially large widths in Regev's reduction; both can be done efficiently). Then, each iteration produces discrete Gaussian states (samples) with smaller widths. Repeating the iteration for polynomial number of times gives the discrete Gaussian states (samples) for the $|\mathsf{DGS}\rangle$ (DGS) problem. We illustrate Regev's reduction in Figure 2a, aligned with our reduction in Figure 2b, and then explain with more details.



(a) Two iterations in Regev's reduction [Reg09].

(b) Two iterations in our reduction that quantizes Regev's reduction.

Figure 2: The correspondence between Regev's reduction (from DGS to LWE) and our reduction (from $|\mathsf{DGS}\rangle$ to $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$).

In order to quantize Regev's iterative reduction, we focus on quantizing the only classical step in the reduction – solving CVP. Roughly speaking, given a CVP instance $\mathbf{x}$, Regev [Reg09] utilizes LWE oracle to solve CVP by feeding it with samples $\mathbf{a} := \mathcal{L}^{-1}\mathbf{v} \bmod q$ and $\langle \mathbf{x}, \mathbf{v}\rangle \bmod q$ where $\mathbf{v} \leftarrow D_{\mathcal{L},r}$, which are close to the LWE sample $\mathbf{a}$ and $\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod q$ where $\mathbf{s} = (\mathcal{L}^*)^{-1}\kappa_{\mathcal{L}^*}(\mathbf{x}) \bmod q$ and e is sampled from the Gaussian distribution. To quantize this step, a natural idea is to replace the classical $\mathbf{v}$ with a superposition state of Gaussian samples $\sum_{\mathbf{v}\in\mathcal{L}} \rho_r(\mathbf{v})|\mathbf{v}\rangle$, measure $\mathbf{a} = \mathcal{L}^{-1}\mathbf{v} \bmod q$, and compute $\langle \mathbf{x}, \mathbf{v}\rangle \bmod q$ in another register, hoping that the register contains an $\mathsf{S}|\mathsf{LWE}\rangle$ state. However, we should be careful to make sure that the $\mathbf{v}$ register does not collapse to a classical $\mathbf{v}$. Our solution is to measure the $\mathbf{v}$ register in Fourier basis, which can ensure that each $\mathbf{v} \in q\mathcal{L} + \mathcal{L}\mathbf{a}$ appears in the amplitude of the $\langle \mathbf{x}, \mathbf{v}\rangle$ register. But it also inevitably introduces a phase term that we are unable to compute efficiently from the measurement results. The above discussion ignores the Gaussian distribution to smooth the error distribution. More details can be found in Section 4.2.

The above described reduction leads us to requiring an $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$ oracle with specific parameter. We first formally define our special parameters and functions, and propose the main theorem for this section here:

Definition 4.1. *Let $\mathcal{L}$ be an n-dimensional integer lattice. Given parameters $q, R \in \mathbb{N}^+$ such that $R \in 2^{\mathsf{poly}(n)}$, $\alpha, r \in \mathbb{R}$ and a vector $\mathbf{x} \in \mathbb{R}^n$ such that* $\mathrm{dist}(\mathbf{x}, \mathcal{L}^*) \le \lambda_1(\mathcal{L}^*)/2$, *we define*

1. *An amplitude function $f : \mathbb{Z}_{qR}/R \to \mathbb{R}$ with $f(e) = \rho_{\sqrt{2}\alpha q}(e)$ which is completely known.*
2. *A family of distribution $D_\theta^{(r,\mathbf{x})}$ over $\mathbb{Z}_R^n \cap R \cdot B_{(q\mathcal{L})^*}$ parameterized by $(r, \mathbf{x})$ and given by* $\Pr(\mathbf{y}) \propto \rho_{\sqrt{\mathbf{\Sigma}/2}}(\mathbf{z}(\mathbf{y}))$ *where $\mathbf{\Sigma} := \frac{\mathbf{I}}{r^2} + \frac{\mathbf{x}'\mathbf{x}'^T}{2\alpha^2q^2 - r^2\|\mathbf{x}'\|^2}$, $\mathbf{x}' := \mathbf{x} - \kappa_{\mathcal{L}^*}(\mathbf{x})$ and $\mathbf{z}(\mathbf{y}) := \mathbf{y}/R - \kappa_{(q\mathcal{L})^*}(\mathbf{y}/R)$.*
3. *A family of phase function $\theta^{(r,\mathbf{x})} : \mathbb{Z}_R^n \cap R \cdot B_{(q\mathcal{L})^*} \to \mathbb{R}$ parameterized by $(r, \mathbf{x})$ with $\theta^{(r,\mathbf{x})}(\mathbf{y}) = \frac{r^2\langle \mathbf{x}', \mathbf{z}(\mathbf{y})\rangle}{2\alpha^2q^2}$, where $\mathbf{x}' = \mathbf{x} - \kappa_{\mathcal{L}^*}(\mathbf{x})$ and $\mathbf{z}(\mathbf{y}) = \mathbf{y}/R - \kappa_{(q\mathcal{L})^*}(\mathbf{y}/R)$. This function is not known to be efficiently computable since it requires to solve approximate* CVP.

Theorem 4.2 (Main theorem, from $|\mathsf{DGS}\rangle$ to $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$)**.** *Let $\mathcal{L}$ be an n-dimensional integer lattice. Let $\epsilon = \epsilon(n)$ be a negligible function such that $\epsilon(n) < 2^{-n}$, $q = q(n) > 10n$ be an integer of at most $\mathsf{poly}(n)$ bits, $\alpha \in (0, \frac{1}{5\sqrt{n}})$ such that $\alpha q > 2\sqrt{n}$, $R = R(n)$ be an exponentially large integer such that $R > \max\{2^{2n+2}n\lambda_n(\mathcal{L})^2, \frac{2^{4n+1}\sqrt{2}n\lambda_n(\mathcal{L}^*)\lambda_n(\mathcal{L})}{\alpha q}, 2^{3n}\lambda_n(\mathcal{L}^*)\}$. Let $r_0 > 4\sqrt{n}\eta_\epsilon(\mathcal{L})/\alpha$ be the width parameter of the $|\mathsf{DGS}\rangle$ problem.*

Assume there exists quantum algorithms that can solve $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}_{n,m,q,f,\theta^{(r,\mathbf{x})},D_\theta^{(r,\mathbf{x})}}$ for any choice of pair $(r, \mathbf{x})$ such that $\alpha q r_0/\sqrt{n} < r < 2^{2n}\sqrt{2}\lambda_n(\mathcal{L})$, $\mathbf{x} \in \mathcal{L}^*/R$ and $\mathrm{dist}(\mathbf{x}, \mathcal{L}^*) \le \alpha q/r$, with $m = 2^{o(n)}$ samples and in time complexity T. Then there exists a quantum algorithm that can generate a state that is $2^{-\Omega(n)}$-close to the discrete Gaussian state $|D_{\mathcal{L},r_0}\rangle = \sum_{\mathbf{v}\in\mathcal{L}} \rho_{r_0}(\mathbf{v})|\mathbf{v}\rangle$ in time complexity $O((m^4 + m^3T)\mathsf{poly}(n))$.

Then the $|\mathsf{DGS}\rangle$ problem is easily reduced to either GapSVP or SIVP. The connection to GapSVP and SIVP is a Corollary of Theorem 4.2 and Lemmas 2.6, 2.7, 2.15, and 2.16.

Corollary 4.3. *Under the same assumption used in Theorem 4.2, there exists quantum algorithms for solving GapSVP_γ and SIVP_γ for $\gamma \in \tilde{O}(n/\alpha)$ in time complexity* $\mathsf{poly}(n, m, T)$.

Remark 4.4. *Readers may think the assumption of Theorem 4.2 looks too strong because the family of phase functions* $\{\theta^{(r,\mathbf{x})}\}$ *is a very large family. However, we know the absolute value of* $\theta^{(r,\mathbf{x})}(\mathbf{y})$ *is small with high probability, when* $(r,\mathbf{x})$ *follows the setting in Theorem 4.2 and* $\mathbf{y}$ *is sampled from the corresponding distribution* $D_\theta^{(r,\mathbf{x})}$*. This is because when* $\mathbf{y} \leftarrow D_\theta^{(r,\mathbf{x})}$, $\mathbf{z}(\mathbf{y}) = \mathbf{y}/R - \kappa_{(q\mathcal{L})^*}(\mathbf{y}/R)$ *follows the distribution* $\rho_{\sqrt{\mathbf{\Sigma}/2}}(\mathbf{z}(\mathbf{y}))$ *over support* $\mathbb{Z}_R^n/R \cap B_{(q\mathcal{L})^*}$ *and thus has* ℓ_2 *norm at most* $\frac{\sqrt{n}\alpha q}{r\sqrt{2\alpha^2q^2-r^2\|\mathbf{x}'\|^2}}$ *with* $1-2^{-\Omega(n)}$ *probability. Then* $\left|\theta^{(r,\mathbf{x})}(\mathbf{y})\right| \le \frac{\sqrt{n}}{2\alpha q}$ *with* $1-2^{-\Omega(n)}$ *probability. As our algorithm in Section 5 can solve the problem in sub-exponential time if* $\theta^{(r,\mathbf{x})}(\mathbf{y})$ *is always zero, there might be a way to solve the problem when* $\theta^{(r,\mathbf{x})}(\mathbf{y})$ *is close to zero.*

In what follows, we will display the idea of our proof for Theorem 4.2, which will be an expansion of the proof idea described earlier with Figure 2. As is described before, our proof is iterative. We start from generating discrete Gaussian states with exponentially large widths. Then, equipped with an $\mathsf{S|LWE\rangle^{phase}}$ solver, we iteratively generate discrete Gaussian states with smaller widths in each step. Repeating the iterative step for polynomial number of times gives the discrete Gaussian states we desired. Formally, our initialization and iterative steps are:

Theorem 4.5 (The initialization step, [Reg09, Lemma 3.12])**.** *There exists an efficient quantum algorithm that given any* n*-dimensional integer lattice* $\mathcal{L}$ *and width* $r > 2^{2n}\sqrt{2}\lambda_n(\mathcal{L})$*, output a state that is* $2^{-\Omega(n)}$*-close to the state* $|D_{\mathcal{L},r}\rangle = \sum_{\mathbf{v}\in\mathcal{L}} \rho_r(\mathbf{v})$.

Theorem 4.6 (The iterative step)**.** *Let* $\mathcal{L}$ *be an* n*-dimensional integer lattice,* $q > 2$ *be an integer. Define the parameters* $\epsilon \in (0, 2^{-n})$, $\alpha \in (0, \frac{1}{5\sqrt{n}})$, $r > 4q\eta_\epsilon(\mathcal{L})$*, and a precision parameter* $R > \max\{2\sqrt{n}r\sqrt{\log r}, \frac{2\sqrt{n}}{\alpha q}, \frac{2^{2n+1}nr\lambda_n(\mathcal{L}^*)}{\alpha q}, 2^{3n}\lambda_n(\mathcal{L}^*)\}$ *as an integer.*

Assume that there exists a quantum algorithm that solves $\mathsf{S|LWE\rangle}^{\mathsf{phase}}_{n,m,q,f,\theta^{(r,\mathbf{x})},D_\theta^{(r,\mathbf{x})}}$ *for any* $\mathbf{x} \in \mathcal{L}^*/R$ *with* $\mathrm{dist}(\mathbf{x},\mathcal{L}^*) < \alpha q/r$ *in time complexity* T*. Then there exists a quantum algorithm that, given* $3m^2n^2$ *discrete Gaussian states* $|D_{\mathcal{L},r}\rangle = \sum_{\mathbf{v}\in\mathcal{L}}\rho_r(\mathbf{v})|\mathbf{v}\rangle$*, produces* $3m^2n^2$ *discrete Gaussian states that are* $2^{-\Omega(n)}$*-close to* $|D_{\mathcal{L},r\sqrt{n}/\alpha q}\rangle$*, in time complexity* $O((m^4+m^3T)\mathsf{poly}(n))$.

The iterative step consists of two steps:

Step 1 Given a CVP instance, we can use a collection of discrete Gaussian states $|D_{\mathcal{L},r}\rangle$ to construct an $\mathsf{S|LWE\rangle^{phase}}$ instance. Solving the $\mathsf{S|LWE\rangle^{phase}}$ instance will in return solve the CVP problem. More precisely, we show the following theorem:

Theorem 4.7. *Let* $\mathcal{L}$ *be an* n*-dimensional integer lattice, define the parameters* $\epsilon \in (0, 2^{-n})$, $\alpha \in (0, \frac{1}{5\sqrt{n}})$, $r > 4q\eta_\epsilon(\mathcal{L})$*, and a precision parameter* $R > \max\{2\sqrt{n}r\sqrt{\log r}, \frac{2\sqrt{n}}{\alpha q}, \frac{2^{2n+1}nr\lambda_n(\mathcal{L}^*)}{\alpha q}\}$ *as an integer.*

Assume that there exists an quantum algorithm that solves $\mathsf{S|LWE\rangle}^{\mathsf{phase}}_{n,m,q,f,\theta^{(r,\mathbf{x})},D_\theta^{(r,\mathbf{x})}}$ *for any* $\mathbf{x} \in \mathcal{L}^*/R$ *with* $\mathrm{dist}(\mathbf{x},\mathcal{L}^*) < \alpha q/r$ *in time complexity* T*. Then there exists a quantum algorithm that, given* $3m^2n^2$ *discrete Gaussian states* $|D_{\mathcal{L},r}\rangle = \sum_{\mathbf{v}\in\mathcal{L}}\rho_r(\mathbf{v})|\mathbf{v}\rangle$*, answers quantum query to* $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ *on the support* $\mathcal{L}^*/R$ *(denoted by* $|\mathbf{x},\mathbf{y}\rangle \to |\mathbf{x},\mathbf{y}+\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle$ *with* $\mathbf{x}\in\mathcal{L}^*/R$ *such that* $\mathrm{dist}(\mathbf{x},\mathcal{L}^*) \le \alpha q/r$*) up to exponentially small error, with exponentially small disturbance to the states* $|D_{\mathcal{L},r}\rangle$*, and in time* $O((m^2+mT)\mathsf{poly}(n))$.

Step 2 (Same as the quantum step in Regev's reduction) A query to the CVP oracle can help to generate a discrete Gaussian state with a smaller width. More precisely:

Theorem 4.8 ([Reg09, Lemma 3.14])**.** *There exists an efficient quantum algorithm that, given any n-dimensional lattice $\mathcal{L}$, a number $d < \lambda_1(\mathcal{L}^*)/2$ and an integer $R > 2^{3n}\lambda_n(\mathcal{L}^*)$, outputs $|D_{\mathcal{L},\sqrt{n}/d}\rangle = \sum_{\mathbf{v}\in\mathcal{L}} \rho_{\sqrt{n}/d}(\mathbf{v})|\mathbf{v}\rangle$, with only one quantum query on the second register of state*

$$\sum_{\mathbf{x}\in\mathcal{L}^*/R, \|\mathbf{x}\|\le d} \rho_{d/\sqrt{n}}(\mathbf{x})|\mathbf{x}, \mathbf{x} \bmod \mathcal{P}(\mathcal{L}^*)\rangle,$$

to the $\mathsf{CVP}_{\mathcal{L}^*,d}$ oracle, which is on the support $\mathcal{L}^*/R$.

The full picture of the proof for the main reduction Theorem 4.2 is illustrated in Figure 3. The proof starts with the initial step (Theorem 4.5) then applies the iterative step (Theorem 4.6)

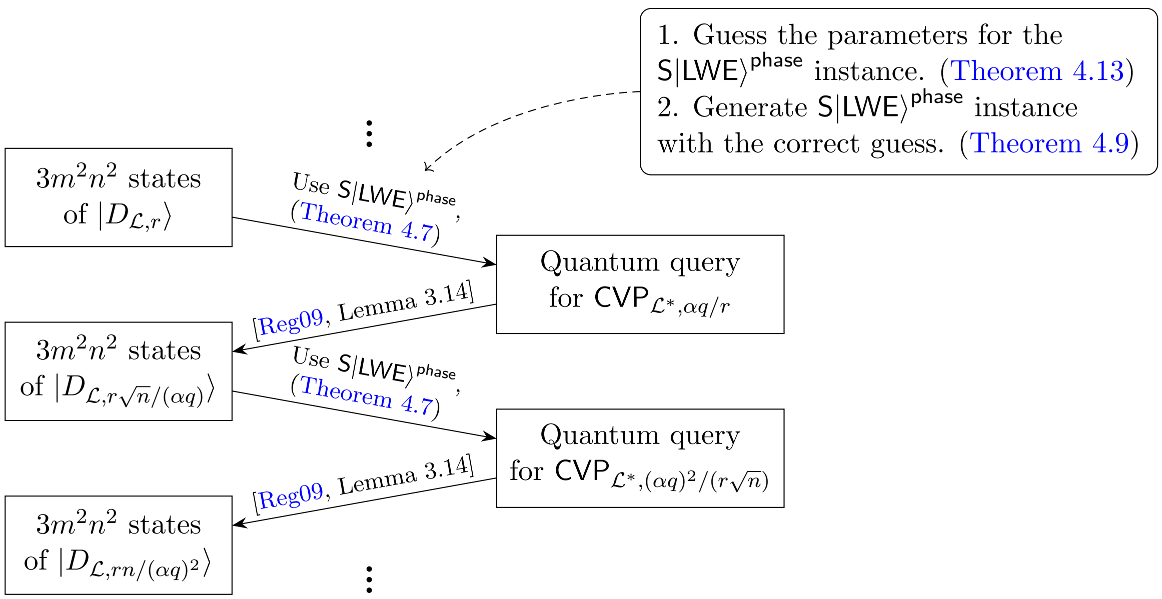


Figure 3: Illustration of two iterations of the reduction algorithm.

for $\mathsf{poly}(n)$ times. The iterative step consists of two parts, first the construction of CVP oracle (Theorem 4.7) with the help of discrete Gaussian states from the previous iteration and the help of an $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$ solver, and then the generation of a narrower discrete Gaussian state through one query to the CVP oracle (Theorem 4.8). Since the discrete Gaussian states generated in the previous iteration are only disturbed by an exponentially small amount upon each query of the CVP oracle, we can reuse them for $3m^2n^2$ times to construct $3m^2n^2$ narrower discrete Gaussian states for use of the next iteration.

It is left to prove Theorem 4.7, to which the remainder of this section will be devoted. To prove it, we start by generating an $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$ instance but with an unknown Gaussian width, instead of the fixed and known width $\sqrt{2}\alpha q$ in the $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$ solver, as displayed in Theorem 4.9 in Section 4.2. We then address and resolve the issue of the unknown width in order to solve the CVP instance using the $\mathsf{S}|\mathsf{LWE}\rangle^{\mathsf{phase}}$ oracle, in the proof of Theorem 4.13 in Section 4.3. Finally, we note that the procedure in Theorem 4.13 answers the CVP quantum query with $1 - 2^{-\Omega(n)}$ probability. Therefore using the idea of gentle measurement, we can answer each CVP quantum query with exponentially small disturbance to the states $|D_{\mathcal{L},r}\rangle$, as discussed in Section 4.4.

4.2 Generating the $\mathsf{S|LWE\rangle^{phase}}$ samples

In this subsection, we show how to create the $\mathsf{S|LWE\rangle^{phase}}$ instance for Theorem 4.7 but with an unknown Gaussian width. Given a $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ instance, the idea is to replace the classical Gaussian samples from $D_{\mathcal{L},r}$ in [Reg09] (that helps to produce the LWE instance) with a superposition state of Gaussian samples $|D_{\mathcal{L},r}\rangle := \sum_{\mathbf{v}\in\mathcal{L}} \rho_r(\mathbf{v})|\mathbf{v}\rangle$ that helps to produce the $\mathsf{S|LWE\rangle^{phase}}$ instance.

Theorem 4.9. *Let $\mathcal{L}$ be an n-dimensional integer lattice, define the parameters $\epsilon \in (0, 2^{-n})$, $\alpha \in (0, \frac{1}{5\sqrt{n}})$, $\sigma \in [\alpha q, \sqrt{2}\alpha q]$, $r > 4q\eta_\epsilon(\mathcal{L})$, and a precision parameter $R > 2\sqrt{n}r\sqrt{\log r}$ as an integer. Given a $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ instance $\mathbf{x} \in \mathcal{L}^*/R$ and a state $|D_{\mathcal{L},r}\rangle$ as input, there exists an efficient quantum algorithm that generates a random vector $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ and a state $2^{-\Omega(n)}$-close to the following state*

$$\gamma_t^{\mathbf{a}} = \sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}} \rho_{\sqrt{\mathbf{\Sigma}/2}}(\mathbf{z}(\mathbf{y}))|\mathbf{y}\rangle\langle\mathbf{y}| \otimes |\psi_t^{\mathbf{a},\mathbf{y}}\rangle\langle\psi_t^{\mathbf{a},\mathbf{y}}|$$

where $t = \sqrt{\sigma^2 + r^2\|\mathbf{x}'\|^2}$, $\mathbf{s} = (\mathcal{L}^*)^{-1}\kappa_{\mathcal{L}^*}(\mathbf{x}) \bmod q$, $\mathbf{x}' = \mathbf{x} - \kappa_{\mathcal{L}^*}(\mathbf{x})$, $\mathbf{z}(\mathbf{y}) = \mathbf{y}/R - \kappa_{(q\mathcal{L})^*}(\mathbf{y}/R)$, $\mathbf{\Sigma} = \frac{\mathbf{I}_n}{r^2} + \frac{\mathbf{x}'\mathbf{x}'^T}{\sigma^2}$, and the state $|\psi_t^{\mathbf{a},\mathbf{y}}\rangle$ is an $\mathsf{S|LWE\rangle}$-like state

$$|\psi_t^{\mathbf{a},\mathbf{y}}\rangle := \sum_{u\in\mathbb{Z}_{qR}/R} \rho_t(u)\exp\left(2\pi\mathrm{i}\cdot u\frac{r^2\langle\mathbf{x}',\mathbf{z}(\mathbf{y})\rangle}{t^2}\right)|\langle\mathbf{s},\mathbf{a}\rangle + u \bmod q\rangle. \quad (10)$$

Proof. From now on, when it is clear from the context, we use $\mathbf{z}$ to denote the value $\mathbf{z}(\mathbf{y})$, which actually depends on $\mathbf{y}$.

Here is the procedure of our quantum algorithm. For simplicity, we ignore the normalization factors when writing down superposition states.

1. Prepare the initial state

$$|D_{\mathcal{L},r}\rangle \otimes \sum_{e\in\mathbb{Z}_{qR}/R} \rho_\sigma(e)|e\rangle,$$

which is $2^{-\Omega(n)}$-close to $\sum_{\mathbf{v}\in\mathcal{L},\|\mathbf{v}\|\le\sqrt{n}r} \rho_r(\mathbf{v})|\mathbf{v}\rangle \otimes \sum_{e\in\mathbb{Z}_{qR}/R} \rho_\sigma(e)|e\rangle$ by Banaszczyk's Gaussian tail bound.

2. Measure $\mathbf{a} := \mathcal{L}^{-1}\mathbf{v} \bmod q$ to get an outcome $\mathbf{a}$ and a result state $2^{-\Omega(n)}$-close to

$$\sum_{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\|\mathbf{v}\|\le\sqrt{n}r} \rho_r(\mathbf{v})|\mathbf{v}\rangle \otimes \sum_{e\in\mathbb{Z}_{qR}/R} \rho_\sigma(e)|e\rangle$$

According to Lemma 2.8, when $r/\sqrt{2} > q\eta_\epsilon(\mathcal{L})$, the distribution of $\mathbf{a}$ is $2^{-\Omega(n)}$-close to uniform.

3. Apply a unitary to add the inner product $\langle \mathbf{x}, \mathbf{v} \rangle \bmod q$ to the last register[1] and get

$$\sum_{\mathbf{v} \in q\mathcal{L}+\mathcal{L}\mathbf{a}, \|\mathbf{v}\| \leq \sqrt{n}r} \rho_r(\mathbf{v}) |\mathbf{v}\rangle \otimes \sum_{e \in \mathbb{Z}_{qR}/R} \rho_\sigma(e) | \langle \mathbf{s}, \mathbf{a} \rangle + \langle \mathbf{x}', \mathbf{v} \rangle + e \bmod q \rangle. \tag{11}$$

Note that since we assumed $\mathbf{x} \in \mathcal{L}^*/R$, the second register always has its value in $\mathbb{Z}_{qR}/R$.

Intuitively, since $u := \langle \mathbf{x}', \mathbf{v} \rangle + e \leq \alpha q \sqrt{n} + \sigma \sqrt{n} < q/2$ with high probability and $R > 2\sqrt{n}r$, Equation (11) should be $2^{-\Omega(n)}$-close to the following state displayed in Equation (12). The proof is deferred to Appendix A.3.

Lemma 4.10. *Suppose that $q/2 > \alpha q \sqrt{n} + \sigma \sqrt{n}$, $R > 2\sqrt{n}r\sqrt{\log r}$ and $r > \sqrt{2}q\eta_\epsilon(\mathcal{L})$ for $\epsilon < 2^{-n}$, then the state in Equation (11) is $2^{-\Omega(n)}$-close to the state*

$$\sum_{\mathbf{v} \in q\mathcal{L}+\mathcal{L}\mathbf{a}} \rho_r(\mathbf{v}) |\mathbf{v} \bmod R\rangle \otimes \sum_{u \in \mathbb{Z}_{qR}/R} \rho_\sigma(u - \langle \mathbf{x}', \mathbf{v} \rangle) | \langle \mathbf{s}, \mathbf{a} \rangle + u \bmod q \rangle. \tag{12}$$

By the assumption that $\sigma \leq \sqrt{2}\alpha q$, we have that $\alpha q \sqrt{n} + \sigma \sqrt{n} \leq (1+\sqrt{2})\alpha q \sqrt{n} < q/2$. Therefore, according to the lemma mentioned above, we can obtain a state that is $2^{-\Omega(n)}$-close to the state displayed in Equation (12).

4. Recall that $\omega_q = e^{2\pi i/q}$. Applying QFT_R to the first register, we can get a state $2^{-\Omega(n)}$-close to

$$\sum_{\mathbf{y} \in \mathbb{Z}_R^n} \sum_{\mathbf{v} \in q\mathcal{L}+\mathcal{L}\mathbf{a}} \rho_r(\mathbf{v}) \cdot \omega_R^{\langle \mathbf{v}, \mathbf{y} \rangle} |\mathbf{y}\rangle \otimes \sum_{u \in \mathbb{Z}_{qR}/R} \rho_\sigma(u - \langle \mathbf{x}', \mathbf{v} \rangle) | \langle \mathbf{s}, \mathbf{a} \rangle + u \bmod q \rangle. \tag{13}$$

We show that the state in Equation (13) is $2^{-\Omega(n)}$-close to the following state displayed in Equation (14). The proof is deferred to Appendix A.4.

Lemma 4.11. *Suppose that $\epsilon < 2^{-n}, R > 2\sqrt{n}r\sqrt{\log r}, r > 4q\eta_\epsilon(\mathcal{L})$ and $\sigma \geq \alpha q$, then the state in Equation (13) is $2^{-\Omega(n)}$-close to the state*

$$\begin{aligned} &\sum_{\mathbf{y} \in \mathbb{Z}_R^n \cap R \cdot B_{(q\mathcal{L})^*}} \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{z}) \exp\left(2\pi i \left\langle \mathcal{L}\mathbf{a}, \kappa_{(q\mathcal{L})^*}(\mathbf{y}/R) \right\rangle\right) |\mathbf{y}\rangle \\ &\qquad \otimes \sum_{u \in \mathbb{Z}_{qR}/R} \rho_t(u) \exp\left(2\pi i \cdot u \frac{r^2 \langle \mathbf{x}', \mathbf{z} \rangle}{t^2}\right) | \langle \mathbf{s}, \mathbf{a} \rangle + u \bmod q \rangle, \end{aligned} \tag{14}$$

where $t, \mathbf{s}, \mathbf{z}, \mathbf{\Sigma}$ are specified in Theorem 4.9.

By the assumption that $\sigma \in [\alpha q, \sqrt{2}\alpha q]$, we have that $\alpha q \sqrt{n} + \sigma \sqrt{n} < (1+\sqrt{2})\alpha q \sqrt{n} < (1+\sqrt{2})q/5 < q/2$. Therefore, according to Lemma 4.11, we can obtain a state that is $2^{-\Omega(n)}$-close to the state (recall the definition of $|\psi_t^{\mathbf{a},\mathbf{y}}\rangle$ in Equation (10))

$$\sum_{\mathbf{y} \in \mathbb{Z}_R^n \cap R \cdot B_{(q\mathcal{L})^*}} \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{z}) \exp\left(2\pi i \left\langle \mathcal{L}\mathbf{a}, \kappa_{(q\mathcal{L})^*}(\mathbf{y}/R) \right\rangle\right) |\mathbf{y}\rangle \otimes |\psi_t^{\mathbf{a},\mathbf{y}}\rangle$$

[1] More precisely, this step can be done by computing $\langle \mathbf{x}, \mathbf{v} \rangle \bmod q$ in another register, applying unitary U that maps $|x, y\rangle$ to $|x, x+y \bmod q\rangle$ for every $x, y \in \mathbb{Z}_q$ to compute $(e + \langle \mathbf{x}, \mathbf{v} \rangle) \bmod q = (\langle \mathbf{s}, \mathbf{a} \rangle + \langle \mathbf{x}', \mathbf{v} \rangle + e) \bmod q$, and then uncomputing $\langle \mathbf{x}, \mathbf{v} \rangle \bmod q$.

5. Measure the first register to get a state $2^{-\Omega(n)}$-close to the state $\gamma_t^{\mathbf{a}}$.

Finally, combining the measurement result $\mathbf{a}$ from step 2 and the state $\gamma_t^{\mathbf{a}}$ from step 5 gives the desired sample. □

Remark 4.12. *An important caveat is that we should not discard the* $\mathbf{y}$ *register and hope we can solve the problem given only* $\mathbf{a}$ *and the* $\mathsf{S|LWE\rangle}$*-like state* $|\psi^{\mathbf{a},\mathbf{y}}_{\sqrt{2}\alpha q}\rangle$ *whose error amplitude is Gaussian with a small phase, because such a solver is so strong that it solves* LWE *directly. This is because such a solver utilizes no information about* $\mathbf{y}$ *(the seed that generates* θ*). So it should output* $\mathbf{s}$ *given samples* $\mathbf{a}$ *and the second register after step 3 (Note that in the actual procedure the solver is given the second register after step 5, but step 4 and step 5 are both local operations acting on the first register, which should not influence the state of the second register). This leads to an algorithm that outputs* $\mathbf{s}$ *given samples* $(\mathbf{a}, \langle \mathbf{s}, \mathbf{a}\rangle + e \bmod q)$ *where* $\mathbf{a} \leftarrow \mathcal{U}_{\mathbb{Z}_q^n}$ *and* $e = \langle \mathbf{x}', \mathbf{v}\rangle$ *for* $\mathbf{v}$ *distributed according to* $D_{q\mathcal{L}+\mathcal{L}\mathbf{a}, r/\sqrt{2}}$ *and a fixed vector* $\|\mathbf{x}'\| \le \frac{\alpha q}{r}$*. As the distribution of* e *is close to a Gaussian distribution, this will give a surprising method to solve* LWE*.*

This also explains why we describe the auxiliary information $\mathbf{y}$ *carefully in Definition 1.4 and Definition 4.1 instead of discarding* $\mathbf{y}$ *and strengthening the solver in Theorem 4.2 to solve* $\mathsf{S|LWE\rangle}^{\mathsf{phase}}_{n,m,q,f,\theta,D}$ *for any unknown* θ *such that* $|\theta| \le \frac{\sqrt{n}}{2\alpha q}$ *(see Remark 4.4) and an arbitrary distribution* D*.*

Given that we must use the information of $\mathbf{y}$*, one may hope to compute* $\mathbf{z}(\mathbf{y})$ *to learn something about the phase* $\theta^{(r,\mathbf{x})}(\mathbf{y}) = \frac{r^2\langle \mathbf{x}', \mathbf{z}(\mathbf{y})\rangle}{2\alpha^2 q^2}$*. However,* $\mathbf{z}(\mathbf{y})$ *has* ℓ_2 *norm roughly* $\frac{\sqrt{n}}{r}$ *(see Remark 4.4). So computing* $\mathbf{z}(\mathbf{y})$ *from* $\mathbf{y}$ *is a* $\mathsf{CVP}_{\mathcal{L}^*, \frac{q\sqrt{n}}{r}}$ *instance, which is even harder than the goal of this iteration (a quantum query to* $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$*). How to utilize* $\mathbf{y}$ *requires more attempts and is an important step towards our ultimate goal of solving standard* LWE *efficiently.*

4.3 Dealing with the unknown Gaussian width

Now that we know how to generate $(\mathbf{a}, \gamma_t^{\mathbf{a}})$ which resembles an $\mathsf{S|LWE\rangle}^{\mathsf{phase}}$ instance. However, the $\mathsf{S|LWE\rangle}^{\mathsf{phase}}$ solver requires instances with an error distribution of the fixed width $\sqrt{2}\alpha q$. To bridge this gap, we experiment with different values of σ to obtain a suitable width that is sufficiently close to $\sqrt{2}\alpha q$. Equipped with the $\mathsf{S|LWE\rangle}^{\mathsf{phase}}$ solver, we can in turn solve the CVP problem. We realize this idea in the proof of the following theorem:

Theorem 4.13. *Let* $\mathcal{L}$ *be an* n*-dimensional integer lattice, define the parameters* $\epsilon \in (0, 2^{-n})$*,* $\alpha \in (0, \frac{1}{5\sqrt{n}})$*,* $r > 4q\eta_\epsilon(\mathcal{L})$*, and a precision parameter* $R > \max\{2\sqrt{n}r\sqrt{\log r}, \frac{2\sqrt{n}}{\alpha q}\}$ *as an integer.*

Assume that there exists a quantum algorithm $\mathcal{A}$ *that, given* m *samples of independently uniformly random vector* $\mathbf{a} \in \mathbb{Z}_q^n$ *and state* $\gamma^{\mathbf{a}}_{\sqrt{2}\alpha q}$*, solves the secret vector* $\mathbf{s}$ *in time complexity* T*. Then there exists a quantum algorithm that, given a* $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ *instance* $\mathbf{x} \in \mathcal{L}^*/R$ *and* $3m^2 n$ *states* $|D_{\mathcal{L},r}\rangle$ *as input, outputs* $\mathbf{s} = (\mathcal{L}^*)^{-1}\kappa_{\mathcal{L}^*}(\mathbf{x}) \bmod q$ *with probability* $1 - 2^{-\Omega(n)}$ *in time* $O((m^2 + mT)\mathsf{poly}(n))$*.*

Proof. Let $\sigma' = \sqrt{2\alpha^2 q^2 - r^2\|\mathbf{x}'\|^2}$ and $\sigma_i = \alpha q\left(1 + (\sqrt{2}-1)\frac{i}{2m}\right), t_i = \sqrt{\sigma_i^2 + r^2\|\mathbf{x}'\|^2}$ for $i =$

$0, 1, \cdots, 2m$. In this condition, we have $\sigma_i \in [\alpha q, \sqrt{2}\alpha q]$. Since $r\|\mathbf{x}'\| < \alpha q$, there must exist an index $0 \leq j < 2m$ such that $\sigma_j < \sigma' \leq \sigma_{j+1}$.

Then σ_j is a suitable value of σ to generate samples for the quantum algorithm $\mathcal{A}$. Formally,

Lemma 4.14. *The quantum algorithm $\mathcal{A}$ can solve $\mathbf{s}$ with probability at least $1/2$, when given m independent samples of vector $\mathbf{a} \in \mathbb{Z}_q^n$ and state $\gamma_{t_j}^{\mathbf{a}}$.*

Before the proof of the lemma, let's first show how to construct a CVP algorithm based on the lemma. Here is the procedure of our quantum algorithm.

1. (Generate classical LWE samples for verification of the solution) Apply Theorem 4.9 to n states $|D_{\mathcal{L},r}\rangle$ with $\sigma = \sigma_0$ to obtain n samples of vectors $\mathbf{a} \in \mathbb{Z}_q^n$ and states $\gamma_{t_0}^{\mathbf{a}}$. Then, measure the second register of $\gamma_{t_0}^{\mathbf{a}}$ to obtain n classical LWE samples of the form $\langle \mathbf{a}, \mathbf{s}\rangle + u \bmod q$.
2. Enumerate σ from the set $\{\sigma_i : i \in \{0, 1, \cdots, 2m-1\}\}$.
3. For each $\sigma = \sigma_i$, apply Theorem 4.9 to mn states $|D_{\mathcal{L},r}\rangle$ to obtain mn samples of vectors $\mathbf{a} \in \mathbb{Z}_q^n$ and states $\gamma_{t_i}^{\mathbf{a}}$ with a precision of $1 - 2^{-\Omega(n)}$.
4. Utilize the quantum algorithm $\mathcal{A}$ on a group of m samples of vectors $\mathbf{a} \in \mathbb{Z}_q^n$ and states $\gamma_{t_i}^{\mathbf{a}}$ to derive a solution $\mathbf{s}'$.
5. Employ any verification process (e.g., as proposed by Regev in [Reg09, Lemma 3.6]) with the assistance of the n classical LWE samples obtained in step 1 to check whether $\mathbf{s}' = \mathbf{s}$. If this condition holds, output $\mathbf{s}'$ and conclude the process.

This procedure will use a maximum of $2m^2n + n < 3m^2n$ samples of $|D_{\mathcal{L},r}\rangle$ and operates with a time complexity of $O((m^2 + mT)\mathsf{poly}(n))$. Moreover, it will output the correct $\mathbf{s}$ with a probability of at least $1 - 2^{-\Omega(n)}$ when $\sigma = \sigma_j$, by Lemma 4.14. □

Lemma 4.14 follows from the fact that $\gamma_{t_j}^{\mathbf{a}}$ is close to $\gamma_{\sqrt{2}\alpha q}^{\mathbf{a}}$ as t_j is close to $\sqrt{2}\alpha q$. For completeness, let's provide the formal proof here.

Proof of Lemma 4.14. We label the m samples to be $\{(\mathbf{a}_i, \gamma_{t_j}^{\mathbf{a}_i})\}_{i\in[m]}$. By assumption, the quantum algorithm $\mathcal{A}$ can solve $\mathbf{s}$ with probability at least $1-2^{-\Omega(n)}$, when given m samples $\{(\mathbf{a}_i, \gamma_{\sqrt{2}\alpha q}^{\mathbf{a}_i})\}_{i\in[m]}$.

The trace distance between the states in these two different types of samples is given by

$$\begin{aligned}
\delta\left(\bigotimes_{i=1}^{m}\gamma_{t_j}^{\mathbf{a}_i},\bigotimes_{i=1}^{m}\gamma_{\sqrt{2}\alpha q}^{\mathbf{a}_i}\right) &\le \sum_{i=1}^{m}\delta\left(\gamma_{t_j}^{\mathbf{a}_i},\gamma_{\sqrt{2}\alpha q}^{\mathbf{a}_i}\right)\\
&\le \sum_{i=1}^{m}\delta\left(|D_{q\mathcal{L}+\mathcal{L}\mathbf{a}_i,r}\rangle\sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\sigma_j}(e)|e\rangle,|D_{q\mathcal{L}+\mathcal{L}\mathbf{a}_i,r}\rangle\sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\sigma'}(e)|e\rangle\right)+2^{-\Omega(n)}\\
&= \sum_{i=1}^{m}\delta\left(\sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\sigma_j}(e)|e\rangle,\sum_{e\in\mathbb{Z}_{qR}/R}\rho_{\sigma'}(e)|e\rangle\right)+2^{-\Omega(n)}\\
&\le_{(*)} m\sqrt{\frac{(\sigma'-\sigma_j)^2}{\sigma_j^2+\sigma'^2}}(1+2^{-\Omega(n)})+2^{-\Omega(n)}\\
&\le m\cdot\sqrt{\frac{(\alpha q/(2m))^2}{2(\alpha q)^2}}(1+2^{-\Omega(n)})+2^{-\Omega(n)}\\
&\le \frac{1}{2\sqrt{2}}+2^{-\Omega(n)}
\end{aligned}$$

where $(*)$ is according to Lemma 2.19 and $\sigma_j,\sigma'\in[\alpha q,\sqrt{2}\alpha q), R>\frac{2\sqrt{n}}{\alpha q}$.

Therefore, the quantum algorithm $\mathcal{A}$ will output $\mathbf{s}$ when given $\{(\mathbf{a}_i,\gamma_{t_j}^{\mathbf{a}_i})\}_{i\in[m]}$ with probability at least

$$1-\frac{1}{2\sqrt{2}}-2^{-\Omega(n)}>\frac{1}{2}.$$ □

One last gap between Theorem 4.13 and the theorem we need to prove (Theorem 4.7) is that, in Theorem 4.13 the algorithm only outputs $\mathbf{s}=(\mathcal{L}^*)^{-1}\kappa_{\mathcal{L}^*}(\mathbf{x}) \bmod q$, which answers a modulo version of $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ for instance $\mathbf{x}\in\mathcal{L}^*/R$. However, as [Reg09] shows, CVP is efficiently reducible to its modulo version, which closes this final gap. Formally,

Theorem 4.15 ([Reg09, a slight modification of Lemma 3.5])**.** *Let $\mathcal{L}$ be an n-dimensional integer lattice, define distance parameter $d\in(0,\lambda_1(\mathcal{L})/2)$, and integers $q>2, R>\frac{2^{2n+1}n\lambda_n(\mathcal{L})}{d}$. Assume there exists an algorithm $\mathcal{A}$ that, on input $\mathbf{x}\in\mathcal{L}/R$ with the guarantee $\mathrm{dist}(\mathbf{x},\mathcal{L})\le d$, outputs $\mathbf{s}=\mathcal{L}^{-1}\kappa_{\mathcal{L}}(\mathbf{x}) \bmod q$ with probability $1-2^{-\Omega(n)}$, then there exists a polynomial-time algorithm that, on input $\mathbf{x}\in\mathcal{L}/R$ with guarantee $\mathrm{dist}(\mathbf{x},\mathcal{L})\le d$, outputs $\kappa_{\mathcal{L}}(\mathbf{x})$ with probability $1-2^{-\Omega(n)}$ using at most n calls to $\mathcal{A}$.*

Proof. It is merely the same as the proof of Lemma 3.5 in [Reg09], but with a slight modification. Compute a sequence $\mathbf{x}_1,\mathbf{x}_2,\cdots$ where $\mathbf{x}_1$ is the input $\mathbf{x}$ and $\mathbf{x}_{i+1}$ is given by the following: for $\mathbf{x}_i\in\mathcal{L}/R$, call $\mathcal{A}$ to compute $\mathbf{s}_i=\mathcal{L}^{-1}\kappa_{\mathcal{L}}(\mathbf{x}_i) \bmod q$, and then compute $\mathbf{y}_i:=(\mathbf{x}_i-\mathcal{L}\mathbf{s}_i)/q$. Now that $\mathbf{y}_i\in\mathcal{L}/(Rq)$ and $\mathrm{dist}(\mathbf{y}_i,\mathcal{L})=\mathrm{dist}(\mathbf{x}_i,\mathcal{L})/q$, we can apply Babai's nearest plane algorithm [Bab86] to find a point $\mathbf{x}_{i+1}\in\mathcal{L}/R$ such that $\mathrm{dist}(\mathbf{x}_{i+1},\mathbf{y}_i)\le 2^n\mathrm{dist}(\mathbf{y}_i,\mathcal{L}/R)\le 2^{n-1}n\lambda_n(\mathcal{L}/R)<d/2^{n+2}$. Then $\mathrm{dist}(\mathbf{x}_{i+1},\mathcal{L})\le\mathrm{dist}(\mathbf{y}_i,\mathcal{L})+\mathrm{dist}(\mathbf{x}_{i+1},\mathbf{y}_i)<\mathrm{dist}(\mathbf{x}_i,\mathcal{L})/q+d/2^{n+2}$.

Thus $\mathrm{dist}(\mathbf{x}_i,\mathcal{L})\le\frac{1}{q^{i-1}}(\mathrm{dist}(\mathbf{x}_1,\mathcal{L})-dq/(2^{n+2}(q-1)))+dq/(2^{n+2}(q-1))\le\frac{d}{q^{i-1}}+\frac{d}{2^{n+1}}$. Then $\kappa_{\mathcal{L}}(\mathbf{x}_{i+1})=\kappa_{\mathcal{L}}(\mathbf{y}_i)$ because $\mathrm{dist}(\mathbf{y}_i,\mathcal{L})+\mathrm{dist}(\mathbf{x}_{i+1},\mathbf{y}_i)<\mathrm{dist}(\mathbf{x}_i,\mathcal{L})/q+d/2^{n+2}<d<\lambda_1(\mathcal{L})/2$.

After n steps, we have a point $\mathbf{x}_{n+1}$ such that $\mathrm{dist}(\mathbf{x}_{n+1}, \mathcal{L}) \le \frac{d}{q^n} + \frac{d}{2^{n+1}} < \frac{d}{2^n}$. Hence we can apply Babai's nearest plane algorithm [Bab86] to recover $\kappa_{\mathcal{L}}(\mathbf{x}_{n+1})$.

Note that $\kappa_{\mathcal{L}}(\mathbf{x}_i) = q\kappa_{\mathcal{L}}(\mathbf{y}_i) + \mathcal{L}\mathbf{s}_i = q\kappa_{\mathcal{L}}(\mathbf{x}_{i+1}) + \mathcal{L}\mathbf{s}_i$. We can recover $\kappa_{\mathcal{L}}(\mathbf{x}_1)$ step by step. Notice that each call to $\mathcal{A}$ has failure probability $2^{-\Omega(n)}$ and we use n calls to $\mathcal{A}$, so our algorithm has failure probability at most $2^{-\Omega(n)}$, which completes the proof. $\square$

As a direct corollary of Theorem 4.13 and Theorem 4.15, we can reduce CVP to $\mathsf{S|LWE\rangle}^{\mathsf{phase}}$ given a sufficient number of states $|D_{\mathcal{L},r}\rangle$. Formally,

Corollary 4.16. *Let $\mathcal{L}$ be an n-dimensional integer lattice, define the parameters $\epsilon \in (0, 2^{-n})$, $\alpha \in (0, \frac{1}{5\sqrt{n}})$, $r > 4q\eta_\epsilon(\mathcal{L})$, and a precision parameter $R > \max\{2\sqrt{n}r\sqrt{\log r}, \frac{2\sqrt{n}}{\alpha q}, \frac{2^{2n+1}nr\lambda_n(\mathcal{L}^*)}{\alpha q}\}$ as an integer. Assume that there exists a quantum algorithm $\mathcal{A}$ that, given m samples of uniformly random vector $\mathbf{a} \in \mathbb{Z}_q^n$ and state $\gamma^{\mathbf{a}}_{\sqrt{2}\alpha q}$, solves the secret vector $\mathbf{s}$ in time complexity T. Then there exists an algorithm that given a $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ instance $\mathbf{x} \in \mathcal{L}^*/R$ and $3m^2n^2$ states $|D_{\mathcal{L},r}\rangle$ as input, outputs $\kappa_{\mathcal{L}^*}(\mathbf{x})$ with probability $1 - 2^{-\Omega(n)}$ in time $O((m^2 + mT)\mathsf{poly}(n))$.*

4.4 Answering the quantum CVP query with small disturbance on $|D_{\mathcal{L},r}\rangle$

We are now ready to conclude the proof of Theorem 4.7. Corollary 4.16 provides a method to answer classical queries for $\mathsf{CVP}_{\mathcal{L}^*,\alpha q/r}$ on instance $\mathbf{x} \in \mathcal{L}^*/R$ with $1 - 2^{-\Omega(n)}$ probability. By deferred measurement principle and gentle measurement principle, we expect that it can help us to answer quantum query $|\mathbf{x}, \mathbf{y}\rangle \to |\mathbf{x}, \mathbf{y} + \kappa_{\mathcal{L}^*}(\mathbf{x})\rangle$ with $\mathrm{dist}(\mathbf{x}, \mathcal{L}^*) \le \alpha q/r$, using $3m^2n^2$ states $|D_{\mathcal{L},r}\rangle$ while introducing only an exponentially small disturbance on them. However, it is important to note that the gentle measurement principle is primarily suitable for producing measurement results (which is classical) rather than answering quantum query. Therefore, we shall provide a formal proof for using gentle measurement principle to answer quantum query:

Proof of Theorem 4.7. The existence of the quantum algorithm $\mathcal{A}$ in Corollary 4.16 is a direct consequence of the assumption that a quantum algorithm can solve the $\mathsf{S|LWE\rangle}^{\mathsf{phase}}_{n,m,q,f,\theta^{(r,\mathbf{x})},D_\theta^{(r,\mathbf{x})}}$ problem. Specifically, let's recall the expression

$$\gamma^{\mathbf{a}}_{\sqrt{2}\alpha q} = \sum_{\mathbf{y} \in \mathbb{Z}_R^n \cap R \cdot B_{(q\mathcal{L})^*}} \rho_{\sqrt{\mathbf{\Sigma}/2}}(\mathbf{z}(\mathbf{y}))|\mathbf{y}\rangle\langle\mathbf{y}| \otimes |\psi^{\mathbf{a},\mathbf{y}}_{\sqrt{2}\alpha q}\rangle\langle\psi^{\mathbf{a},\mathbf{y}}_{\sqrt{2}\alpha q}|.$$

The quantum algorithm $\mathcal{A}$ proceeds by first measuring the result of $|\mathbf{y}\rangle$ to obtain a specific $\mathbf{y}$ and an $\mathsf{S|LWE\rangle}$ state $|\psi^{\mathbf{a},\mathbf{y}}_{\sqrt{2}\alpha q}\rangle$. The parameters and functions of this state corresponds to the parameters and functions defined in Definition 4.1. Subsequently, $\mathcal{A}$ applies the $\mathsf{S|LWE\rangle}^{\mathsf{phase}}_{n,m,q,f,\theta^{(r,\mathbf{x})},D_\theta^{(r,\mathbf{x})}}$ solver to compute $\mathbf{s}$.

We defer all the measurements in the algorithm in Corollary 4.16 including those in the $\mathsf{S|LWE\rangle}^{\mathsf{phase}}$ solver $\mathcal{A}$ to obtain a unitary $U : |\mathbf{x}\rangle|D_{\mathcal{L},r}\rangle^{\otimes(3m^2n^2)}|0^{\mathsf{Aux}}\rangle \to |\mathbf{x}\rangle|\phi_{\mathbf{x}}\rangle$, where the first register of $|\phi_{\mathbf{x}}\rangle$ contains the solution $\kappa_{\mathcal{L}^*}(\mathbf{x})$, and the size of U is $O((m^2 + mT)\mathsf{poly}(n))$. As the algorithm in Corollary 4.16 outputs $\kappa_{\mathcal{L}^*}(\mathbf{x})$ with probability at least $1 - 2^{-\Omega(n)}$ whenever $\mathrm{dist}(\mathbf{x}, \mathcal{L}^*) \le \alpha q/r$ and $\mathbf{x} \in \mathcal{L}^*/R$, by gentle measurement principle [Win99], there exists state

$|\phi_{\mathbf{x}}^{\mathsf{Aux}}\rangle$ such that the state $|\phi_{\mathbf{x}}\rangle$ is $2^{-\Omega(n)}$-close to the state $|\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle|\phi_{\mathbf{x}}^{\mathsf{Aux}}\rangle$ in ℓ_2-norm. Our quantum algorithm answers the query $|\mathbf{x},\mathbf{y}\rangle \to |\mathbf{x},\mathbf{y}+\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle$ with $\mathrm{dist}(\mathbf{x},\mathcal{L}^*) \le \alpha q/r$ using the following procedure:

1. Prepare the initial state
$$|\mathbf{x},\mathbf{y}\rangle|D_{\mathcal{L},r}\rangle^{\otimes\left(3m^2n^2\right)}|0^{\mathsf{Aux}}\rangle.$$
2. Apply U to the registers containing $|\mathbf{x}\rangle|D_{\mathcal{L},r}\rangle^{\otimes(3m^2n^2)}|0^{\mathsf{Aux}}\rangle$ to get a state $2^{-\Omega(n)}$-close to the state
$$|\mathbf{x},\mathbf{y}\rangle|\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle|\phi_{\mathbf{x}}^{\mathsf{Aux}}\rangle$$
in ℓ_2-norm.
3. Apply a unitary to add the value of $\kappa_{\mathcal{L}^*}(\mathbf{x})$ to $\mathbf{y}$ to get a state $2^{-\Omega(n)}$-close to the state
$$|\mathbf{x},\mathbf{y}+\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle|\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle|\phi_{\mathbf{x}}^{\mathsf{Aux}}\rangle$$
in ℓ_2-norm.
4. Apply $U^\dagger$ to the registers containing $|\mathbf{x}\rangle|\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle|\phi_{\mathbf{x}}^{\mathsf{Aux}}\rangle$ to get a state $2^{-\Omega(n)}$-close to the state
$$|\mathbf{x},\mathbf{y}+\kappa_{\mathcal{L}^*}(\mathbf{x})\rangle|D_{\mathcal{L},r}\rangle^{\otimes\left(3m^2n^2\right)}|0^{\mathsf{Aux}}\rangle$$
in ℓ_2-norm.

Therefore, we can answer the quantum query up to exponentially small error with exponentially small disturbance on the states $|D_{\mathcal{L},r}\rangle$ in time $O((m^2+mT)\mathsf{poly}(n))$, which ends up the proof of Theorem 4.7. □

5 Quantum Sub-exponential Time Algorithm for $\mathsf{S|LWE\rangle}$

In this section, we provide a quantum sub-exponential time algorithm designed to solve $\mathsf{S|LWE\rangle}$ instances with specific amplitudes. More precisely, we consider scenarios where the discrete Fourier transform of these amplitudes exhibits a $2^{-\sqrt{n}\log q}$ mass on two distinct points. Our approach is built upon two key steps: (1) generate a DCP state for each quantum $\mathsf{S|LWE\rangle}$ sample, resulting in a sub-exponential collection of DCP states; (2) employ the Kuperberg sieve technique [Kup05] on the DCP states to successfully recover the secret vector. Formally, We state the main theorem of this section as follows:

Theorem 5.1 (Main theorem)**.** *Assuming the existence of an algorithm that, given the normalized amplitude function $f:\mathbb{Z}\to\mathbb{C}$ of any $\mathsf{S|LWE\rangle}$ state, identifies two distinct points j_1 and j_2 from $\mathbb{Z}_q$ with $\gcd(j_1-j_2,q)=1$ and computes $\mathsf{DFT}_q(f)$ (the discrete Fourier transform of f, defined as $\mathsf{DFT}_q(f)(j)=\frac{1}{\sqrt{q}}\sum_{e\in\mathbb{Z}} f(e)\omega_q^{je}$ for $j\in\mathbb{Z}_q$) on these points in time $2^{O(\sqrt{n}\log q)}$, subject to the condition that $|\mathsf{DFT}_q(f)(j_1)|$ and $|\mathsf{DFT}_q(f)(j_2)|$ are both greater than $2^{-\sqrt{n}\log q}$.*

Under these assumptions, there exists a quantum algorithm that, given $\ell = 2^{\Theta(\sqrt{n}\log q)}$ samples of vector $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ and $\mathsf{S}|\mathsf{LWE}\rangle$ state of form

$$\mathsf{S}|\mathsf{LWE}\rangle = \sum_{e\in\mathbb{Z}} f(e)|\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod q\rangle,$$

solves the secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ within a time complexity of $2^{\Theta(\sqrt{n}\log q)}$.

To prove Theorem 5.1, we begin by introducing the Kuperberg sieve algorithm [Kup05].

Lemma 5.2 (Kuperberg sieve)**.** *Let $\mathbf{s} \in \mathbb{Z}_q^n$ be a secret vector. There exists a quantum algorithm that given $\ell^* = 2^{\Theta(\sqrt{n}\log q)}$ samples of*

$$\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n), \quad |\psi_{\mathbf{a}}\rangle = |0\rangle + \omega_q^{\langle \mathbf{a},\mathbf{s}\rangle}|1\rangle,$$

finds out the secret vector $\mathbf{s}$ in time $2^{\Theta(\sqrt{n}\log q)}$.

Now we present the proof of Theorem 5.1 here.

Proof of Theorem 5.1. Suppose we have $\ell = \ell^* \cdot 2^{4\sqrt{n}\log q} = 2^{\Theta(\sqrt{n}\log q)}$ instances of $\mathsf{S}|\mathsf{LWE}\rangle$ states. Our quantum algorithm proceeds as follows:

1. Apply QFT to any $\mathsf{S}|\mathsf{LWE}\rangle$ state, resulting in the state

$$\mathsf{QFT}_q \cdot \mathsf{S}|\mathsf{LWE}\rangle = \frac{1}{\sqrt{q}} \sum_{j\in\mathbb{Z}_q}\sum_{e\in\mathbb{Z}} f(e)\omega_q^{j(\langle \mathbf{a},\mathbf{s}\rangle + e)}|j\rangle = \sum_{j\in\mathbb{Z}_q} \omega_q^{\langle j\cdot\mathbf{a},\mathbf{s}\rangle}\mathsf{DFT}_q(f)(j)|j\rangle,$$

2. Identify two distinct points $j_1, j_2 \in \mathbb{Z}_q$ where $\mathsf{DFT}_q(f)(j_1)$ and $\mathsf{DFT}_q(f)(j_2)$ are both computable and have norms greater than $2^{-\sqrt{n}\log q}$. Define $\gamma(j) : \mathbb{Z}_q \to [0,1]$ as

$$\gamma(j) = \frac{\min\{|\mathsf{DFT}_q(f)(j_1)|, |\mathsf{DFT}_q(f)(j_2)|\}}{|\mathsf{DFT}_q(f)(j)|} \text{ for } j = j_1, j_2$$

and $\gamma(j) = 0$ otherwise, apply quantum rejection sampling (Lemma 2.21) to obtain the state

$$\frac{\mathsf{DFT}_q(f)(j_1)}{|\mathsf{DFT}_q(f)(j_1)|}\omega_q^{\langle j_1\cdot\mathbf{a},\mathbf{s}\rangle}|j_1\rangle + \frac{\mathsf{DFT}_q(f)(j_2)}{|\mathsf{DFT}_q(f)(j_2)|}\omega_q^{\langle j_2\cdot\mathbf{a},\mathbf{s}\rangle}|j_2\rangle, \tag{15}$$

with probability

$$M = \sum_{j\in\mathbb{Z}_q} \gamma^2(j)|f(j)|^2 = 2(\min\{|\mathsf{DFT}_q(f)(j_1)|, |\mathsf{DFT}_q(f)(j_2)|\})^2 > 2^{-2\sqrt{n}\log q}.$$

3. For the states that have been successfully transformed to Equation (15), apply a unitary operation

$$U : |j_1\rangle \to \frac{\overline{\mathsf{DFT}_q(f)(j_1)}}{|\mathsf{DFT}_q(f)(j_1)|}|0\rangle, |j_2\rangle \to \frac{\overline{\mathsf{DFT}_q(f)(j_2)}}{|\mathsf{DFT}_q(f)(j_2)|}|1\rangle,$$

this results in the state

$$|\psi_{(j_2-j_1)\mathbf{a}}\rangle = |0\rangle + \omega_q^{\langle (j_2-j_1)\mathbf{a},\mathbf{s}\rangle}|1\rangle,$$

where $(j_2 - j_1)\mathbf{a}$ is a known vector in $\mathbb{Z}_q^n$ that is uniformly random by the assumption that $\gcd(j_1 - j_2, q) = 1$.

4. Select ℓ^* such states obtained in step 3 and apply the Kuperberg sieve algorithm to recover the secret vector $\mathbf{s} \in \mathbb{Z}_q^n$.

It is evident that transforming any $\mathsf{S}|\mathsf{LWE}\rangle$ state to a DCP-like state requires a time complexity of $2^{O(\sqrt{n}\log q)}$. Therefore, the run time of our quantum algorithm is constrained by both the quantity of $\mathsf{S}|\mathsf{LWE}\rangle$ states and the application of the Kuperberg sieve, which both exhibit a complexity of $2^{\Theta(\sqrt{n}\log q)}$. In step 2, the count of states successfully transformed to Equation (15) will be at least $M^2\ell = \ell^*$ with a probability exponentially close to 1. This concludes the proof. □

Corollary 5.3. *Suppose m, n, q are LWE parameters. There exists a quantum algorithm that, given $2^{\Theta(\sqrt{n}\log q)}$ samples of vector $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$ and $\mathsf{S}|\mathsf{LWE}\rangle$ state of form*

$$\mathsf{S}|\mathsf{LWE}\rangle = \sum_{e\in\mathbb{Z}} \rho_\sigma(e)\exp(2\pi \mathrm{i}\cdot ce/q)|\langle \mathbf{a}, \mathbf{s}\rangle + e \bmod q\rangle,$$

where the Gaussian width σ satisfies $\sigma = \Omega(\sqrt{n}), \sigma \leq q$, and c is an arbitrary known number that can be different for different samples, solves the secret vector $\mathbf{s} \in \mathbb{Z}_q^n$ within a time complexity of $2^{\Theta(\sqrt{n}\log q)}$.

Proof. Let us define

$$N = \sum_{e\in\mathbb{Z}} \rho_\sigma^2(e) = \sum_{e\in\mathbb{Z}} \frac{\sigma}{\sqrt{2}}\rho_{\sqrt{2}/\sigma}(e) \approx \frac{\sigma}{\sqrt{2}},$$

where the final approximation holds under the assumption that $\sigma = \Omega(n)$. In this case, the summation of $\rho_{\sqrt{2}/\sigma}$ the summation of $\rho_{\sqrt{2}/\sigma}$ is concentrated at $\rho_{\sqrt{2}/\sigma}(0)$, with exponentially small weight elsewhere.

In the given problem scenario, it becomes evident that

$$f(e) = \frac{1}{\sqrt{N}}\rho_\sigma(e)\exp(2\pi\mathrm{i}\cdot ce/q),$$

thus

$$\begin{aligned}
\mathsf{DFT}_q(f)(j) &= \frac{1}{\sqrt{qN}}\sum_{e\in\mathbb{Z}}\rho_\sigma(e)\exp(2\pi\mathrm{i}\cdot(j+c)e/q) \\
&=_{(*)} \frac{1}{\sqrt{qN}}\sum_{e\in\mathbb{Z}}\sigma\rho_{1/\sigma}\left(e - \frac{j+c}{q}\right) \\
&\approx_{(**)} \frac{1}{\sqrt{qN}}\sigma\rho_{1/\sigma}\left(\left\lfloor\frac{j+c}{q}\right\rceil - \frac{j+c}{q}\right) \\
&= \frac{1}{\sqrt{qN}}\rho_{q/\sigma}(j+c-\lfloor j+c\rceil_q),
\end{aligned}$$

here $(*)$ is from the Poisson summation formula, $(**)$ holds due to the initial assumption that $\sigma = \Omega(\sqrt{n})$. In this case, the summation $\sum_{j\in\mathbb{Z}_q}\rho_{1/\sigma}\left(e - \frac{j+c}{q}\right)$ is concentrated at $\rho_{1/\sigma}\left(\left\lfloor\frac{j+c}{q}\right\rceil - \frac{j+c}{q}\right)$, with exponentially small weight elsewhere.

Define $j_1 = \lfloor -c \rfloor \bmod q, j_2 = (\lfloor -c \rfloor + 1) \bmod q$, we can establish that $|j + c - \lfloor j + c \rceil_q| \leq 1$ holds for both $j = j_1$ and $j = j_2$. This implies that

$$|\mathsf{DFT}_q(f)(j)| \geq \sqrt{\frac{\sqrt{2}}{q\sigma}} \rho_{q/\sigma}(1)(1 - 2^{-\Omega(n)}) \geq \sqrt{\frac{\sqrt{2}}{q^2}} e^{-\pi}(1 - 2^{-\Omega(n)}) \gg 2^{-\sqrt{n}\log q},$$

for both $j = j_1, j_2$.

As a result, we can deduce the validity of the original statement by straightforwardly applying Theorem 5.1. □

Remark 5.4. *Readers may be curious about why our sub-exponential algorithm cannot handle* $\mathsf{S}|\mathsf{LWE}\rangle$ *instances with an unknown phase, similar to the* $\mathsf{S}|\mathsf{LWE}\rangle$ *states we obtain from the reductions discussed in previous sections. Informally speaking, when the phase term of* $\mathsf{S}|\mathsf{LWE}\rangle$ *samples is unknown, we can only obtain a DCP-like state with varying weights in the superposition. Although the ratio of weights on* $|0\rangle$ *and* $|1\rangle$ *can be bounded by an inverse polynomial, this ratio tends to become extremely large during the sieving step of Kuperberg's algorithm. As a result, the final state collapses into either* $|0\rangle$ *or* $|1\rangle$*, and the information about* $\mathbf{s}$ *is entirely lost.*

References

[APV23] Prabhanjan Ananth, Alexander Poremba, and Vinod Vaikuntanathan. Revocable cryptography from learning with errors. *arXiv preprint arXiv:2302.14860*, 2023. 2

[Bab86] László Babai. On lovász' lattice reduction and the nearest lattice point problem. *Comb.*, 6(1):1–13, 1986. 25, 26

[Ban93] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(1):625–635, 1993. 7

[BKSW18] Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen. Learning with errors and extrapolated dihedral cosets. In *Public Key Cryptography (2)*, volume 10770 of *Lecture Notes in Computer Science*, pages 702–727. Springer, 2018. 1, 2, 3, 11, 13, 14, 15

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *IEEE 52nd Annual Symposium on Foundations of Computer Science, FOCS 2011, Palm Springs, CA, USA, October 22-25, 2011*, pages 97–106, 2011. 1

[CLZ22] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In *EUROCRYPT (3)*, volume 13277 of *Lecture Notes in Computer Science*, pages 372–401. Springer, 2022. 1, 2, 4

[DM13] Nico Döttling and Jörn Müller-Quade. Lossy codes and a new variant of the learning-with-errors problem. In *EUROCRYPT*, volume 7881 of *Lecture Notes in Computer Science*, pages 18–34. Springer, 2013. 1

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, pages 169–178. ACM, 2009. 1

[GPV08] Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *STOC*, pages 197–206, 2008. 8

[GR02] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions. *arXiv preprint quant-ph/0208112*, 2002. 10

[Gra08] Loukas Grafakos. *Classical fourier analysis*. Springer, 2008. 5

[HPS98] Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. NTRU: A ring-based public key cryptosystem. In *ANTS*, volume 1423 of *Lecture Notes in Computer Science*, pages 267–288. Springer, 1998. 1

[Kit95] Alexei Y. Kitaev. Quantum measurements and the abelian stabilizer problem. 1995. 10

[KLS22] Andrey Boris Khesin, Jonathan Z Lu, and Peter W Shor. Publicly verifiable quantum money from random lattices. *arXiv preprint arXiv:2207.13135*, 2022. 2

[Kup05] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005. 2, 27, 28

[LMZ23] Jiahui Liu, Hart Montgomery, and Mark Zhandry. Another round of breaking and making quantum money: How to not build it from lattices, and more. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 611–638. Springer, 2023. 2

[Mah18] Urmila Mahadev. Classical homomorphic encryption for quantum circuits. In *FOCS*, pages 332–338. IEEE Computer Society, 2018. 1

[MP12] Daniele Micciancio and Chris Peikert. Trapdoors for lattices: Simpler, tighter, faster, smaller. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 700–718, 2012. 6

[MP13] Daniele Micciancio and Chris Peikert. Hardness of SIS and LWE with small parameters. In *CRYPTO (1)*, volume 8042 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2013. 1

[MR07] Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on Gaussian measure. *SIAM Journal on Computing*, 37(1):267–302, 2007. 6, 7

[NC16] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information (10th Anniversary edition)*. Cambridge University Press, 2016. 9

[ORR13] Maris Ozols, Martin Roetteler, and Jérémie Roland. Quantum rejection sampling. *ACM Transactions on Computation Theory (TOCT)*, 5(3):1–33, 2013. 2, 10

[Por23] Alexander Poremba. Quantum proofs of deletion for learning with errors. In *ITCS*, volume 251 of *LIPIcs*, pages 90:1–90:14. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023. 2

[Reg02] Oded Regev. Quantum computation and lattice problems. In *FOCS*, pages 520–529. IEEE Computer Society, 2002. 3

[Reg04] Oded Regev. Quantum computation and lattice problems. *SIAM J. Comput.*, 33(3):738–760, 2004. 11, 13

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, 2009. 1, 2, 7, 9, 12, 17, 18, 19, 20, 21, 24, 25

[RS17] Oded Regev and Noah Stephens-Davidowitz. A reverse minkowski theorem. In *STOC*, pages 941–953. ACM, 2017. 7

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In *Advances in Cryptology - ASIACRYPT 2009, 15th International Conference on the Theory and Application of Cryptology and Information Security, Tokyo, Japan, December 6-10, 2009. Proceedings*, pages 617–635, 2009. 1, 2

[Win99] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999. 9, 26

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In *EUROCRYPT (3)*, volume 11478 of *Lecture Notes in Computer Science*, pages 408–438. Springer, 2019. 1

A Appendix

A.1 Upper bounds on Gaussian tails

Lemma A.1. *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice, $\mathbf{u} \in \mathbb{R}^n$ be a fixed vector, $\epsilon \in (0,1)$ be a small error parameter, σ be a positive real number with $\sigma > 2\eta_\epsilon(\mathcal{L})$. Then we have*

$$\sum_{\mathbf{x} \in \mathcal{L}^*} \rho_{1/\sigma}(\mathbf{x} - \mathbf{u}) < \rho_{1/\sigma}(\mathbf{u} - \kappa_{\mathcal{L}^*}(\mathbf{u})) + \epsilon.$$

If $\mathbf{u}$'s closest vectors in $\mathcal{L}^*$ are not unique, then $\kappa_{\mathcal{L}^*}(\mathbf{u})$ can be an arbitrary one of the closest vectors.

Proof. It suffices to prove that

$$\sum_{\mathbf{x} \in \mathcal{L}^* \setminus \{\kappa_{\mathcal{L}^*}(\mathbf{u})\}} \rho_{1/\sigma}(\mathbf{x} - \mathbf{u}) < \epsilon.$$

For any $\mathbf{x} \in \mathcal{L}^*$, we have that

$$\begin{aligned}
\|\mathbf{x}-\mathbf{u}\|^2 &\geq \frac{1}{2}\left(\|\mathbf{x}-\mathbf{u}\|^2 + \|\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}\|^2\right) \qquad \text{(by the definition of } \kappa_{\mathcal{L}^*}(\mathbf{u})) \\
&\geq \frac{1}{4}\left(\|\mathbf{x}-\mathbf{u}\| + \|\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}\|\right)^2 \\
&\geq \frac{1}{4}\|\mathbf{x}-\mathbf{u}-(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u})\|^2 \qquad \text{(triangle inequality)} \\
&= \frac{1}{4}\|\mathbf{x}-\kappa_{\mathcal{L}^*}(\mathbf{u})\|^2,
\end{aligned}$$

so

$$\begin{aligned}
\sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\kappa_{\mathcal{L}^*}(\mathbf{u})\}} \rho_{1/\sigma}(\mathbf{x}-\mathbf{u}) &\leq \sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\kappa_{\mathcal{L}^*}(\mathbf{u})\}} \rho_{2/\sigma}(\mathbf{x}-\kappa_{\mathcal{L}^*}(\mathbf{u})) \\
&= \sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\mathbf{0}\}} \rho_{2/\sigma}(\mathbf{x}) \\
&< \epsilon,
\end{aligned}$$

as desired. □

Lemma A.2. *Let $\mathcal{L} \subseteq \mathbb{R}^n$ be a lattice, $\mathbf{u} \in \mathbb{R}^n$ be a fixed vector, $\epsilon \in (0,1)$ be a small error parameter, σ be a positive real number with $\sigma > 2\sqrt{2}\eta_\epsilon(\mathcal{L})$. Then we have*

$$\sum_{\mathbf{x}\in\mathcal{L}^*} \rho_{1/\sigma}(\mathbf{x}-\mathbf{u}) < \rho_{1/\sigma}(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}) + \epsilon \cdot \rho_{\sqrt{2}/\sigma}(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}).$$

If $\mathbf{u}$'s closest vectors in $\mathcal{L}^*$ are not unique, then $\kappa_{\mathcal{L}^*}(\mathbf{u})$ can be an arbitrary one of the closest vectors.

Proof. It suffices to prove that

$$\sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\kappa_{\mathcal{L}^*}(\mathbf{u})\}} \rho_{1/\sigma}(\mathbf{x}-\mathbf{u}) < \epsilon \cdot \rho_{\sqrt{2}/\sigma}(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}).$$

For any $\mathbf{x} \in \mathcal{L}^*$, we have that

$$\begin{aligned}
\|\mathbf{x}-\mathbf{u}\|^2 - \frac{1}{2}\|\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}\|^2 &\geq \frac{1}{4}\left(\|\mathbf{x}-\mathbf{u}\|^2 + \|\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}\|^2\right) \qquad \text{(by the definition of } \kappa_{\mathcal{L}^*}(\mathbf{u})) \\
&\geq \frac{1}{8}\left(\|\mathbf{x}-\mathbf{u}\| + \|\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}\|\right)^2 \\
&\geq \frac{1}{8}\|\mathbf{x}-\mathbf{u}-(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u})\|^2 \qquad \text{(triangle inequality)} \\
&= \frac{1}{8}\|\mathbf{x}-\kappa_{\mathcal{L}^*}(\mathbf{u})\|^2,
\end{aligned}$$

so

$$\begin{aligned}
\sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\kappa_{\mathcal{L}^*}(\mathbf{u})\}} \rho_{1/\sigma}(\mathbf{x}-\mathbf{u}) &\leq \rho_{\sqrt{2}/\sigma}(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}) \sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\kappa_{\mathcal{L}^*}(\mathbf{u})\}} \rho_{2\sqrt{2}/\sigma}(\mathbf{x}-\kappa_{\mathcal{L}^*}(\mathbf{u})) \\
&= \rho_{\sqrt{2}/\sigma}(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}) \sum_{\mathbf{x}\in\mathcal{L}^*\setminus\{\mathbf{0}\}} \rho_{2\sqrt{2}/\sigma}(\mathbf{x}) \\
&< \epsilon \cdot \rho_{\sqrt{2}/\sigma}(\kappa_{\mathcal{L}^*}(\mathbf{u})-\mathbf{u}),
\end{aligned}$$

as desired. □

A.2 Proof of Lemma 3.6

Proof of Lemma 3.6. Denote the (unnormalized) state in Equation (7) as $|\Phi\rangle$, and the (unnormailized) state in Equation (8) as $|\Phi'\rangle$. Then we have

$$\begin{aligned}
\||\Phi\rangle - |\Phi'\rangle\|^2 &= \sum_{\mathbf{v}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)^2\left\|\sum_{\substack{\mathbf{x}\in\mathbb{Z}^m,\\ \|\mathbf{x}\|\geq\lambda_1(\mathcal{L}_q(\mathbf{A}))/2}}\rho_\beta(\mathbf{x}+j\cdot\mathbf{e})|(\mathbf{A}^T\mathbf{v}+\mathbf{x}) \bmod q\rangle\right\|^2\\
&\leq_{(1)} q^n\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)^2\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}^m,\\ \|\mathbf{x}\|\geq\lambda_1(\mathcal{L}_q(\mathbf{A}))/2}}\rho_\beta(\mathbf{x}+j\cdot\mathbf{e})\right)^2\\
&\leq_{(2)} q^n\sum_{\substack{j\in\mathbb{Z}_q,\\ |j|<\alpha\sqrt{m\log\beta}}}\rho_\alpha(j)^2\left(\sum_{\substack{\mathbf{x}\in\mathbb{Z}^m,\\ \|\mathbf{x}\|\geq\beta\sqrt{m\log\beta}}}\rho_\beta(\mathbf{x})\right)^2 + q^n\sum_{\substack{j\in\mathbb{Z}_q,\\ |j|\geq\alpha\sqrt{m\log\beta}}}\rho_\alpha(j)^2\left(\sum_{\mathbf{x}\in\mathbb{Z}^m}\rho_\beta(\mathbf{x})\right)^2,
\end{aligned}$$

where in (1) we absorb the summation over $\mathbf{v}\in\mathbb{Z}_q^n$ in q^n, and use the fact that ρ is non-negative; in (2), the first term uses the following: when $\|\mathbf{x}\|\geq\lambda_1(\mathcal{L}_q(\mathbf{A}))/2$ and $|j|<\alpha\sqrt{m\log\beta}$, we have $\|\mathbf{x}+j\cdot\mathbf{e}\|>\lambda_1(\mathcal{L}_q(\mathbf{A}))/2-\alpha\sqrt{m\log\beta}\cdot\gamma\sqrt{m}>\beta\sqrt{m\log\beta}$, the second term uses for any $\mathbf{c}\in\mathbb{R}^n$, $\sum_{\mathbf{x}\in\mathbb{Z}^m}\rho_\beta(\mathbf{x}+\mathbf{c})\leq\sum_{\mathbf{x}\in\mathbb{Z}^m}\rho_\beta(\mathbf{x})$.

From Banaszczyk's tail bound (see Lemma 2.3), we have that

$$\sum_{\substack{\mathbf{x}\in\mathbb{Z}^m,\\ \|\mathbf{x}\|\geq\beta\sqrt{m\log\beta}}}\rho_\beta(\mathbf{x})<\beta^{-3m}\sum_{\mathbf{x}\in\mathbb{Z}^m}\rho_\beta(\mathbf{x}),\qquad \sum_{\substack{j\in\mathbb{Z}_q,\\ |j|\geq\alpha\sqrt{m\log\beta}}}\rho_{\alpha/\sqrt{2}}(j)<\beta^{-6m}\sum_{j\in\mathbb{Z}_q}\rho_{\alpha/\sqrt{2}}(j).$$

Notice that $\beta>\sqrt{m}$, so from Lemma 2.4, $\sum_{\mathbf{x}\in\mathbb{Z}^m}\rho_\beta(\mathbf{x})<(1+2^{-\Omega(m)})\beta^m$. Therefore,

$$\begin{aligned}
\||\Phi\rangle - |\Phi'\rangle\|^2 &< 2q^n\beta^{-6m}\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)^2\left(\sum_{\mathbf{x}\in\mathbb{Z}^m}\rho_\beta(\mathbf{x})\right)^2\\
&< 2(1+2^{-\Omega(n)})q^n\beta^{-4m}\sum_{j\in\mathbb{Z}_q}\rho_\alpha(j)^2
\end{aligned}$$

On the other hand, notice that from Lemma 2.4, $\sum_{\mathbf{x}\in\mathbb{Z}^m} \rho_{\beta/\sqrt{2}}(\mathbf{x}) > (\beta/\sqrt{2})^m$, we have that

$$\begin{aligned}\||\Phi\rangle\|^2 &\geq \sum_{\mathbf{v}\in\mathbb{Z}_q^n}\sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)^2 \sum_{\mathbf{x}\in\mathbb{Z}^m} \rho_\beta(\mathbf{x}+j\cdot\mathbf{e})^2 \\ &= q^n \sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)^2 \sum_{\mathbf{x}\in\mathbb{Z}^m} \rho_\beta(\mathbf{x})^2 \\ &> q^n \left(\frac{\beta}{\sqrt{2}}\right)^m \sum_{j\in\mathbb{Z}_q} \rho_\alpha(j)^2\end{aligned}$$

Hence, we get that $\frac{\||\Phi\rangle - |\Phi'\rangle\|^2}{\||\Phi\rangle\|^2} < 2^{-\Omega(n)}$, this implies that $|\Phi\rangle$ and $|\Phi'\rangle$ are $2^{-\Omega(n)}$-close to each other, by Lemma 2.17, as desired. □

A.3 Proof of Lemma 4.10

Proof of Lemma 4.10. For any vector $\mathbf{v} \in q\mathcal{L} + \mathcal{L}\mathbf{a}$ such that $\|\mathbf{v}\| \leq \sqrt{n}r$, as $q/2 > \sigma\sqrt{n}$, the state

$$\sum_{e\in\mathbb{Z}_{qR}/R} \rho_\sigma(e)|\langle \mathbf{s},\mathbf{a}\rangle + \langle \mathbf{x}',\mathbf{v}\rangle + e \bmod q\rangle \tag{16}$$

is $2^{-\Omega(n)}$-close to the state

$$\sum_{e\in[-\sigma\sqrt{n},\sigma\sqrt{n}]\cap(\mathbb{Z}/R)} \rho_\sigma(e)|\langle \mathbf{s},\mathbf{a}\rangle + \langle \mathbf{x}',\mathbf{v}\rangle + e \bmod q\rangle$$

in ℓ_2 norm by Banaszczyk's tail bound (see Lemma 2.3), which is $2^{-\Omega(n)}$-close to the state

$$\sum_{e\in\mathbb{Z}_{qR}/R-\langle\mathbf{x}',\mathbf{v}\rangle} \rho_\sigma(e)|\langle \mathbf{s},\mathbf{a}\rangle + \langle \mathbf{x}',\mathbf{v}\rangle + e \bmod q\rangle$$

in ℓ_2 norm due to Banaszczyk's tail bound and the fact that $|\langle\mathbf{x}',\mathbf{v}\rangle| \leq \frac{\alpha q}{r}\cdot\sqrt{n}r < q/2 - \sigma\sqrt{n}$, which implies $[-\sigma\sqrt{n},\sigma\sqrt{n}]\cap(\mathbb{Z}/R) \subseteq \mathbb{Z}_{qR}/R - \langle\mathbf{x}',\mathbf{v}\rangle$.

We can perform a change of variable $u \leftarrow \langle\mathbf{x}',\mathbf{v}\rangle + e$ to write the last state as

$$\sum_{u\in\mathbb{Z}_{qR}/R} \rho_\sigma(u - \langle\mathbf{x}',\mathbf{v}\rangle)|\langle \mathbf{s},\mathbf{a}\rangle + u \bmod q\rangle. \tag{17}$$

Observe that Equation (16) and Equation (17) are $2^{-\Omega(n)}$-close to each other in ℓ_2 norm for every $\mathbf{v} \in q\mathcal{L} + \mathcal{L}\mathbf{a}$ such that $\|\mathbf{v}\| \leq \sqrt{n}r$. Therefore, the given state

$$\sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|\leq\sqrt{n}r}} \rho_r(\mathbf{v})|\mathbf{v}\rangle \otimes \sum_{e\in\mathbb{Z}_{qR}/R} \rho_\sigma(e)|\langle \mathbf{s},\mathbf{a}\rangle + \langle \mathbf{x}',\mathbf{v}\rangle + e \bmod q\rangle$$

is $2^{-\Omega(n)}$-close to the state

$$\sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|\leq\sqrt{n}r}} \rho_r(\mathbf{v})|\mathbf{v}\rangle \otimes \sum_{u\in\mathbb{Z}_{qR}/R} \rho_\sigma(u - \langle\mathbf{x}',\mathbf{v}\rangle)|\langle \mathbf{s},\mathbf{a}\rangle + u \bmod q\rangle,$$

which is $2^{-\Omega(n)}$-close to the state

$$|\Phi\rangle := \sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|<R/2}} \rho_r(\mathbf{v})|\mathbf{v}\rangle \otimes \sum_{u\in\mathbb{Z}_{qR}/R} \rho_\sigma(u-\langle\mathbf{x}',\mathbf{v}\rangle)|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle$$

by Banaszczyk's tail bound.

It remains to prove that $|\Phi\rangle$ is $2^{-\Omega(n)}$-close to

$$|\Phi'\rangle := \sum_{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a}} \rho_r(\mathbf{v})|\mathbf{v} \bmod R\rangle \otimes \sum_{u\in\mathbb{Z}_{qR}/R} \rho_\sigma(u-\langle\mathbf{x}',\mathbf{v}\rangle)|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle.$$

The proof is similar to the proof of Lemma 3.6. We first give an upper bound for $\||\Phi\rangle-|\Phi'\rangle\|^2$:

$$\begin{aligned}
\||\Phi\rangle-|\Phi'\rangle\|^2 &\le_{(1)} \left(\sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|\ge R/2}} \rho_r(\mathbf{v}) \left\| |\mathbf{v} \bmod R\rangle \otimes \sum_{u\in\mathbb{Z}_{qR}/R} \rho_\sigma(u-\langle\mathbf{x}',\mathbf{v}\rangle)|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle \right\|\right)^2 \\
&\le_{(2)} \left(\sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|>\sqrt{n}r\sqrt{\log r}}} \rho_r(\mathbf{v}) \sqrt{\sum_{u\in\mathbb{Z}_{qR}/R} \rho_\sigma(u-\langle\mathbf{x}',\mathbf{v}\rangle)^2}\right)^2 \\
&\le_{(3)} r^{-6n}\left(\sum_{u\in\mathbb{Z}/R}\rho_\sigma(u)^2\right)\left(\sum_{\mathbf{v}\in q\mathcal{L}}\rho_r(\mathbf{v})\right)^2 \\
&\le_{(4)} r^{-4n}\left(\sum_{u\in\mathbb{Z}/R}\rho_\sigma(u)^2\right)\det((q\mathcal{L})^*)^2(1+2^{-\Omega(n)})
\end{aligned}$$

where (1) is due to triangle inequality, (2) uses that $R/2>\sqrt{n}r\sqrt{\log r}$, (3) is due to Banaszczyk's tail bound, and (4) is due to Lemma 2.8 and $r\ge\eta_\epsilon(q\mathcal{L})$ for $\epsilon<2^{-n}$.

On the other hand, notice that

$$\begin{aligned}
\||\Phi\rangle\|^2 &\ge \sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|\le\sqrt{n}r}} \rho_r(\mathbf{v})^2 \sum_{u\in\mathbb{Z}_{qR}/R}\rho_\sigma(u-\langle\mathbf{x}',\mathbf{v}\rangle)^2 \\
&\ge_{(1)} (1-2^{-\Omega(n)})\sum_{\substack{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a},\\ \|\mathbf{v}\|\le\sqrt{n}r}} \rho_r(\mathbf{v})^2 \sum_{u\in\mathbb{Z}/R}\rho_\sigma(u)^2 \\
&\ge_{(2)} (1-2^{-\Omega(n)})(r/\sqrt{2})^n\det((q\mathcal{L})^*)\sum_{u\in\mathbb{Z}/R}\rho_\sigma(u)^2
\end{aligned}$$

where (1) is due to Banaszczyk's tail bound and the fact that $\sigma\sqrt{n}<q/2-|\langle\mathbf{x}',\mathbf{v}\rangle|$ when $\|\mathbf{v}\|\le\sqrt{n}r$, and (2) is due to Banaszczyk's tail bound, Lemma 2.8 and $r/\sqrt{2}\ge\eta_\epsilon(q\mathcal{L})$ for $\epsilon<2^{-n}$.

Hence, we have that $\frac{\||\Phi\rangle-|\Phi'\rangle\|^2}{\||\Phi\rangle\|^2}<2^{-\Omega(n)}$, this implies that $|\Phi\rangle$ and $|\Phi'\rangle$ are $2^{-\Omega(n)}$-close to each other, by Lemma 2.17, as desired.

□

A.4 Proof of Lemma 4.11

Proof of Lemma 4.11. The amplitude of $|\mathbf{y}\rangle|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle$ in the given state (Equation (13)) is

$$\sum_{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a}}\rho_r(\mathbf{v})\rho_\sigma(u-\langle\mathbf{x}',\mathbf{v}\rangle)\omega_R^{\langle\mathbf{v},\mathbf{y}\rangle}=\rho_t(u)\sum_{\mathbf{v}\in q\mathcal{L}+\mathcal{L}\mathbf{a}}\rho_{\sqrt{\mathbf{\Sigma}^{-1}}}\left(\mathbf{v}-\frac{r^2u}{t^2}\mathbf{x}'\right)\omega_R^{\langle\mathbf{v},\mathbf{y}\rangle}$$
$$\propto\rho_t(u)\sum_{\mathbf{w}\in(q\mathcal{L})^*-\mathbf{y}/R}\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{w})\exp\left(2\pi\mathrm{i}\left\langle\mathcal{L}\mathbf{a}-\frac{r^2u}{t^2}\mathbf{x}',\mathbf{w}\right\rangle\right)\omega_R^{\langle\mathcal{L}\mathbf{a},\mathbf{y}\rangle},$$

where $t=\sqrt{\sigma^2+r^2\|\mathbf{x}'\|^2}\in[\sigma,\sqrt{2}\sigma)$, matrix $\mathbf{\Sigma}=\frac{\mathbf{I}_n}{r^2}+\frac{\mathbf{x}'\mathbf{x}'^T}{\sigma^2}$ with eigenvalues $1/r^2,(t/r\sigma)^2$, and we use the Poisson Summation Formula to compute the last equality. We define the amplitude as a function

$$\phi(\mathbf{y},u):=\rho_t(u)\sum_{\mathbf{w}\in(q\mathcal{L})^*-\mathbf{y}/R}\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{w})\exp\left(2\pi\mathrm{i}\left\langle\mathcal{L}\mathbf{a}-\frac{r^2u}{t^2}\mathbf{x}',\mathbf{w}\right\rangle\right)\omega_R^{\langle\mathcal{L}\mathbf{a},\mathbf{y}\rangle}.$$

Meanwhile, for $\mathbf{y}/R\in B_{(q\mathcal{L})^*}$, we define another amplitude function $\phi'(\mathbf{y},u)$ as

$$\phi'(\mathbf{y},u):=\rho_t(u)\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{z})\exp\left(2\pi\mathrm{i}\left\langle\mathcal{L}\mathbf{a}-\frac{r^2u}{t^2}\mathbf{x}',-\mathbf{z}\right\rangle\right)\omega_R^{\langle\mathcal{L}\mathbf{a},\mathbf{y}\rangle},$$

where we recall that $\mathbf{z}=\mathbf{z}(\mathbf{y})=\mathbf{y}/R-\kappa_{(q\mathcal{L})^*}(\mathbf{y}/R)$. $\phi'(\mathbf{y},u)$ is the leading term in $\phi(\mathbf{y},u)$, as we will implicitly show below.

We prove that the following (unnormalized) states

$$|\Phi\rangle:=\sum_{\mathbf{y}\in\mathbb{Z}_R^n}\sum_{u\in\mathbb{Z}_{qR}/R}\phi(\mathbf{y},u)|\mathbf{y}\rangle|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle\quad\text{(the given state)}$$
$$|\Phi'\rangle:=\sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}}\sum_{u\in\mathbb{Z}_{qR}/R}\phi'(\mathbf{y},u)|\mathbf{y}\rangle|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle\quad\text{(the target state in Equation (14))}$$

are $2^{-\Omega(n)}$-close to each other. To prove it, we need in addition the following (unnormalized) state

$$|\Phi''\rangle:=\sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}}\sum_{u\in\mathbb{Z}_{qR}/R}\phi(\mathbf{y},u)|\mathbf{y}\rangle|\langle\mathbf{s},\mathbf{a}\rangle+u \bmod q\rangle.$$

Let's begin by establishing upper bounds for both $\||\Phi''\rangle-|\Phi'\rangle\|^2$ and $\||\Phi\rangle-|\Phi''\rangle\|^2$. The first term is relatively simpler to bound: for any $\epsilon<2^{-n}$, according to Lemma A.2 and the assumption that $\frac{r\sigma}{t}>\frac{r}{\sqrt{2}}>2\sqrt{2}\eta_\epsilon(q\mathcal{L})$, we get that

$$\begin{aligned}\||\Phi''\rangle-|\Phi'\rangle\|^2&=\sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}}\sum_{u\in\mathbb{Z}_{qR}/R}\left|\phi(\mathbf{y},u)-\phi'(\mathbf{y},u)\right|^2\\&\le\sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}}\sum_{u\in\mathbb{Z}_{qR}/R}\left(\rho_t(u)\sum_{\mathbf{w}\in(q\mathcal{L})^*\setminus\{\mathbf{0}\}}\rho_{t/r\sigma}(\mathbf{w}-\mathbf{z})\right)^2\qquad(18)\\&<\epsilon^2\sum_{u\in\mathbb{Z}_{qR}/R}\rho_t(u)^2\sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}}\rho_{t/r\sigma}(\mathbf{z}).\end{aligned}$$

To establish an upper bound for the latter term $\||\Phi\rangle - |\Phi''\rangle\|^2$, according to Lemma A.2 and the fact that $\frac{r\sigma}{t} > 2\sqrt{2}\eta_\epsilon(q\mathcal{L})$, we get that for $\mathbf{y} \in \mathbb{Z}_R^n \setminus R \cdot B_{(q\mathcal{L})^*}$,

$$\begin{aligned}\sum_{\mathbf{w}\in(q\mathcal{L})^*-\mathbf{y}/R} \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{w}) &\leq \sum_{\mathbf{w}\in(q\mathcal{L})^*-\mathbf{y}/R} \rho_{t/r\sigma}(\mathbf{w}) \\ &\leq \exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{(t/r\sigma)^2}\right) + \epsilon \cdot \exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{2(t/r\sigma)^2}\right) \\ &\leq \exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{2(t/r\sigma)^2}\right)\left(\exp\left(-\pi\frac{(\lambda_1((q\mathcal{L})^*)/2)^2}{4/r^2}\right) + \epsilon\right) \\ &\leq 2^{-n+1}\exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{2(t/r\sigma)^2}\right)\end{aligned}$$

where the last inequality holds since $\lambda_1((q\mathcal{L})^*) \geq \sqrt{\frac{n\ln 2}{\pi}} \cdot \frac{1}{q\eta_\epsilon(\mathcal{L})} \geq \sqrt{\frac{n\ln 2}{\pi}} \cdot \frac{4}{r}$ by Lemma 2.7. Therefore,

$$\begin{aligned}\||\Phi\rangle - |\Phi''\rangle\|^2 &= \sum_{\mathbf{y}\in\mathbb{Z}_R^n\setminus R\cdot B_{(q\mathcal{L})^*}} \sum_{u\in\mathbb{Z}_{qR}/R} |\phi(\mathbf{y},u)|^2 \\ &\leq \sum_{u\in\mathbb{Z}_{qR}/R} \rho_t(u)^2 \sum_{\mathbf{y}\in\mathbb{Z}_R^n\setminus R\cdot B_{(q\mathcal{L})^*}} \left(\sum_{\mathbf{w}\in(q\mathcal{L})^*-\mathbf{y}/R} \rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{w})\right)^2 \\ &\leq 2^{-2n+2} \sum_{u\in\mathbb{Z}_{qR}/R} \rho_t(u)^2 \sum_{\mathbf{y}\in\mathbb{Z}_R^n\setminus R\cdot B_{(q\mathcal{L})^*}} \exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{(t/r\sigma)^2}\right).\end{aligned} \tag{19}$$

Combine the two upper bounds in Equation (18) and Equation (19), we get that

$$\begin{aligned}\||\Phi\rangle - |\Phi'\rangle\|^2 &\leq 2\||\Phi\rangle - |\Phi''\rangle\|^2 + 2\||\Phi''\rangle - |\Phi'\rangle\|^2 \\ &\leq 2^{-2n+3} \sum_{u\in\mathbb{Z}_{qR}/R} \rho_t(u)^2 \sum_{\mathbf{y}\in\mathbb{Z}_R^n} \exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{(t/r\sigma)^2}\right).\end{aligned} \tag{20}$$

On the other hand, we can compute that

$$\begin{aligned}\||\Phi'\rangle\|^2 &= \sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}} \sum_{u\in\mathbb{Z}_{qR}/R} \left|\phi'(\mathbf{y},u)\right|^2 \\ &\geq \sum_{u\in\mathbb{Z}_{qR}/R} \rho_t(u)^2 \sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}} \exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{(1/\sqrt{2}r)^2}\right).\end{aligned} \tag{21}$$

Combining with the bounds in Equation (20), we get that

$$\frac{\||\Phi\rangle - |\Phi'\rangle\|^2}{\||\Phi'\rangle\|^2} \leq 2^{-2n+3}\frac{\sum_{\mathbf{y}\in\mathbb{Z}_R^n}\exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{(t/r\sigma)^2}\right)}{\sum_{\mathbf{y}\in\mathbb{Z}_R^n\cap R\cdot B_{(q\mathcal{L})^*}}\exp\left(-\pi\frac{\mathrm{dist}(\mathbf{y}/R,(q\mathcal{L})^*)^2}{(1/\sqrt{2}r)^2}\right)}. \tag{22}$$

Now let's establish an upper bound on the ratio between the two summations on the right-hand side of the above inequality. We accomplish this through the following steps:

1. Expanding the support of $\mathbf{y}$. Given our assumption that $\mathcal{L}$ is an integer lattice, we have $(q\mathcal{L})^* + \mathbf{k} = (q\mathcal{L})^*$ for any $\mathbf{k} \in \mathbb{Z}^n$. Consequently, $\mathrm{dist}((\mathbf{y} - R\mathbf{k})/R, (q\mathcal{L})^*) = \mathrm{dist}(\mathbf{y}/R, (q\mathcal{L})^* + \mathbf{k}) = \mathrm{dist}(\mathbf{y}/R, (q\mathcal{L})^*)$. Therefore, we can expand the support of $\mathbf{y}$ from $\mathbb{Z}_R^n$ to $\mathbb{Z}_{RN}^n$ for any $N \in \mathbb{N}_+$, which is a combination of N^n hypercubes, each in the form $\mathbb{Z}_R^n + R\mathbf{k}$, i.e.

$$\frac{\||\Phi\rangle - |\Phi'\rangle\|^2}{\||\Phi'\rangle\|^2} \leq 2^{-2n+3} \lim_{N \to +\infty} \frac{\sum_{\mathbf{y} \in \mathbb{Z}_{RN}^n} \exp\left(-\pi \frac{\mathrm{dist}(\mathbf{y}/R, (q\mathcal{L})^*)^2}{(t/r\sigma)^2}\right)}{\sum_{\mathbf{y} \in \mathbb{Z}_{RN}^n \cap R \cdot B_{(q\mathcal{L})^*}} \exp\left(-\pi \frac{\mathrm{dist}(\mathbf{y}/R, (q\mathcal{L})^*)^2}{(1/\sqrt{2}r)^2}\right)}.$$

2. Bound the numerator and denominator as N approaches infinity. Assume that N is a sufficiently large integer, and denote $\ell_{\max} = \max_{\mathbf{y} \in \mathbb{R}^n} \mathrm{dist}(\mathbf{y}, (q\mathcal{L})^*) < +\infty$. For the numerator, when considering $\mathbf{y} \in \mathbb{Z}_{RN}^n$, the closest vector from $\mathbf{y}/R$ to the lattice $(q\mathcal{L})^*$ will have ℓ_∞ norm at most $RN/2 + \ell_{\max}$. Thus

$$\sum_{\mathbf{y} \in \mathbb{Z}_{RN}^n} \exp\left(-\pi \frac{\mathrm{dist}(\mathbf{y}/R, (q\mathcal{L})^*)^2}{(t/r\sigma)^2}\right) \leq \sum_{\substack{\mathbf{u} \in (q\mathcal{L})^*, \\ \|\mathbf{u}\|_\infty \leq RN/2 + \ell_{\max}}} \sum_{\mathbf{y} \in \mathbb{Z}^n} \rho_{t/r\sigma}(\mathbf{y}/R - \mathbf{u}).$$

Similarly, for the denominator, when considering $\mathbf{u} \in (q\mathcal{L})^*$ with ℓ_∞ norm at most $RN/2 - \ell_{\max}$, the vectors $\mathbf{y} \in \mathbb{Z}^n \cap R \cdot B_{(q\mathcal{L})^*}$ for which the closest vector to $(q\mathcal{L})^*$ is $\mathbf{u}$ will certainly have an ℓ_∞ norm at most $RN/2$. Thus

$$\begin{aligned}
&\sum_{\mathbf{y} \in \mathbb{Z}_{RN}^n \cap R \cdot B_{(q\mathcal{L})^*}} \exp\left(-\pi \frac{\mathrm{dist}(\mathbf{y}/R, (q\mathcal{L})^*)^2}{(1/\sqrt{2}r)^2}\right) \\
\geq &\sum_{\substack{\mathbf{u} \in (q\mathcal{L})^*, \\ \|\mathbf{u}\|_\infty \leq RN/2 - \ell_{\max}}} \sum_{\substack{\mathbf{y} \in \mathbb{Z}^n, \\ \|\mathbf{y}/R - \mathbf{u}\| < \lambda_1((q\mathcal{L})^*)/2}} \rho_{1/\sqrt{2}r}(\mathbf{y}/R - \mathbf{u}) \\
\geq &\sum_{\substack{\mathbf{u} \in (q\mathcal{L})^*, \\ \|\mathbf{u}\|_\infty \leq RN/2 - \ell_{\max}}} \left(\sum_{\mathbf{y} \in \mathbb{Z}^n} \rho_{1/\sqrt{2}r}(\mathbf{y}/R - \mathbf{u}) - 2^{-\Omega(n)} \rho_{1/\sqrt{2}r}(\mathbb{Z}^n/R)\right),
\end{aligned}$$

where the final inequality is based on Banaszczyk's tail bound (Lemma 2.3), with the guarantee that $\lambda_1((q\mathcal{L})^*)/2 > \sqrt{\frac{n \ln 2}{\pi}} \cdot \frac{2}{r} > \frac{2}{\sqrt{2\pi}} \cdot \frac{1}{\sqrt{2}r} \sqrt{n}$.

According to Lemma 2.6, it follows that $\eta_{2^{-n}}(\mathbb{Z}^n/R) \leq \frac{1}{R} \cdot \sqrt{\frac{2n}{\pi}} < \frac{1}{\sqrt{2}r} < \frac{t}{r\sigma}$. Therefore, by using Lemma 2.8, we can conclude that

$$\sum_{\mathbf{y} \in \mathbb{Z}^n} \rho_{t/r\sigma}(\mathbf{y}/R - \mathbf{u}) \leq (1 + 2^{-\Omega(n)}) \cdot R^n \cdot (t/r\sigma)^n,$$

$$\sum_{\mathbf{y} \in \mathbb{Z}^n} \rho_{1/\sqrt{2}r}(\mathbf{y}/R - \mathbf{u}) - 2^{-\Omega(n)} \rho_{1/\sqrt{2}r}(\mathbb{Z}^n/R) \geq (1 - 2^{-\Omega(n)}) \cdot R^n \cdot (1/\sqrt{2}r)^n.$$

3. Establish an upper bound for the right hand side of Equation (22). By combining the inequalities in the previous step, we obtain that

$$
\begin{aligned}
\frac{\||\Phi\rangle - |\Phi'\rangle\|^2}{\||\Phi'\rangle\|^2} &\le 2^{-2n+3}(1+2^{-\Omega(n)}) \cdot (\sqrt{2}t/\sigma)^n \cdot \lim_{N\to+\infty} \frac{\#\{\mathbf{u} \in (q\mathcal{L})^* : \|\mathbf{u}\|_\infty \le RN/2 + \ell_{\max}\}}{\#\{\mathbf{u} \in (q\mathcal{L})^* : \|\mathbf{u}\|_\infty \le RN/2 - \ell_{\max}\}} \\
&\le 2^{-n+3}(1+2^{-\Omega(n)}) \cdot \lim_{N\to+\infty} \frac{\#\{\mathbf{u} \in (q\mathcal{L})^* : \|\mathbf{u}\|_\infty \le RN/2 + \ell_{\max}\}}{\#\{\mathbf{u} \in (q\mathcal{L})^* : \|\mathbf{u}\|_\infty \le RN/2 - \ell_{\max}\}} \\
&= 2^{-n+3}(1+2^{-\Omega(n)}) \cdot \lim_{N\to+\infty} \frac{(RN/2+\ell_{\max})^n}{(RN/2-\ell_{\max})^n} \\
&= 2^{-n+3}(1+2^{-\Omega(n)}).
\end{aligned}
$$

Consequently, we can infer that the provided state $|\Phi\rangle$ is $2^{-\Omega(n)}$-close to $|\Phi'\rangle$, according to Lemma 2.17, as desired. □