# QUANTUM OBLIVIOUS LWE SAMPLING AND INSECURITY OF STANDARD MODEL LATTICE-BASED SNARKS

THOMAS DEBRIS–ALAZARD [1], POURIA FALLAHPOUR [2], AND DAMIEN STEHLÉ [2,3]

Abstract. The Learning With Errors (LWE) problem asks to find $\mathbf{s}$ from an input of the form $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}) \in (\mathbb{Z}/q\mathbb{Z})^{m\times n} \times (\mathbb{Z}/q\mathbb{Z})^m$, for a vector $\mathbf{e}$ that has small-magnitude entries. In this work, we do not focus on solving LWE but on the task of sampling instances. As these are extremely sparse in their range, it may seem plausible that the only way to proceed is to first create $\mathbf{s}$ and $\mathbf{e}$ and then set $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$. In particular, such an instance sampler knows the solution. This raises the question whether it is possible to obliviously sample $(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e})$, namely, without knowing the underlying $\mathbf{s}$. A variant of the assumption that oblivious LWE sampling is hard has been used in a series of works constructing Succinct Non-interactive Arguments of Knowledge (SNARKs) in the standard model. As the assumption is related to LWE, these SNARKs have been conjectured to be secure in the presence of quantum adversaries.

Our main result is a quantum polynomial-time algorithm that samples well-distributed LWE instances while provably not knowing the solution, under the assumption that LWE is hard. Moreover, the approach works for a vast range of LWE parametrizations, including those used in the above-mentioned SNARKs.

## 1. Introduction

The Learning With Errors (LWE) problem [Reg09] is well-known for its conjectured intractability for quantum algorithms, inherited from the conjectured worst-case hardness of specific problems over Euclidean lattices. It has led to abundant cryptographic constructions that are presumably quantum resistant. For three integers $m \geq n \geq 1$ and $q \geq 2$ as well as a distribution $\chi$ over $\mathbb{Z}/q\mathbb{Z}$ concentrated on values that are small modulo $q$, the search version of LWE with parameters $m, n, q$ and $\chi$ consists in recovering the secret $\mathbf{s}$ from the LWE instance $(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) \in (\mathbb{Z}/q\mathbb{Z})^{m\times n} \times (\mathbb{Z}/q\mathbb{Z})^m$. In the latter, the matrix $\mathbf{A}$ and the vector $\mathbf{s}$ are typically uniformly distributed, and each coefficient of $\mathbf{e}$ is i.i.d. from $\chi$. In this work, we do not focus on solving LWE, but on the task of generating LWE samples. Concretely, we consider algorithms $\mathcal{S}$, which we call LWE samplers, that take as input a uniform matrix $\mathbf{A}$ and output a correctly distributed $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$:

$$\mathcal{S}_{m,n,q,\chi} : \ \mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n} \quad \longrightarrow \quad \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m \ .$$

For parameters of cryptographic interest, a correctly distributed LWE pair $(\mathbf{A}, \mathbf{b})$ admits a unique pair $(\mathbf{s}, \mathbf{e})$ that is much more likely than any other pair to satisfy $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$. This is provided by $m$ being sufficiently large as a function of $n, q$ and $\chi$. In most cases, the dimension $m$ is polynomial in a security parameter $\lambda$ and the modulus $q$ ranges from polynomial to exponential in $\lambda$; the distribution $\chi$ is often set as an integer Gaussian of standard deviation parameter $\sigma \in [\Omega(\sqrt{n}), O(q/\sqrt{n})]$ that is folded modulo $q$, which will be subsequently denoted by $\vartheta_{\sigma,q}$. We have $\vartheta_{\sigma,q}(e) = \sum_{k\in\mathbb{Z}} \exp\left(-|e + qk|^2/\sigma^2\right)$ for all $e \in \mathbb{Z}$, up to a normalization factor. As the correctly formed $\mathbf{b}$'s are extremely sparse in their range (e.g., exponentially so as a function of $\lambda$), the naive approach of sampling a uniform $\mathbf{b}$ and keeping it if it has the correct form is prohibitively expensive. Another major bottleneck with this naive approach is that the distinguishing version of LWE is no easier than its search version (see [Reg09] for small values of $q$ and [Pei09, BLP+13] for large values of $q$). Given this, it could seem that the only way to proceed for a sampler $\mathcal{S}$ is to first create $\mathbf{s}$ and $\mathbf{e}$ and then return $\mathbf{A}\mathbf{s} + \mathbf{e}$. This leads us to the following question:

*Does there exist an efficient algorithm that creates* LWE *samples without knowing the underlying secrets?*

[1] Inria and Laboratoire LIX, École Polytechnique, Palaiseau, France
[3] ENS de Lyon and LIP, Lyon, France
[4] Cryptolab Inc., Lyon, France
*E-mail addresses*: thomas.debris@inria.fr, pouria.fallahpour@ens-lyon.fr, damien.stehle@cryptolab.co.kr.

The obliviousness of the sampler can be formalized by considering an extractor algorithm that takes as inputs the sampler's input and sampler's random coins and outputs the LWE secret of the sampler's output: the LWE sampler is oblivious if no efficient extractor exists. The existence of an oblivious sampler hence implies the hardness of LWE.

Variants of the assumption that no such algorithm exists have been introduced to serve as security foundation of several cryptographic constructions. An early occurrence was [LMSV12], to build a homomorphic encryption scheme with security against chosen ciphertext attacks. The precise algebraic framework was different and led to a quantum polynomial-time attack in [CDPR16], but the usefulness of the assumption can be explained in the LWE context as follows. Assume a ciphertext corresponds to an LWE instance $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ belonging to the ciphertext space $(\mathbb{Z}/q\mathbb{Z})^m$, and that the plaintext of a well-formed ciphertext is a function of $\mathbf{s}$ (the matrix $\mathbf{A}$ is publicly known, and could for example be part of the public key). In the context of chosen-ciphertext security, the attacker is allowed to query a decryption oracle on any element in the ciphertexts space to extract useful information. In the scheme, if the query is not a well-formed ciphertext, the challenger will be able to detect it and reply with a failure symbol. The oblivious sampling hardness assumption ensures that if the adversary makes a decryption query on a well-formed $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, then the reply to the query does not give it anything more than it already knows. The oblivious sampling hardness assumption was used more recently in a series of works building Succinct Non-interactive Arguments of Knowledge (SNARKs) from lattice assumptions [GMNO18, NYI+20, ISW21, SSEK22, CKKK23, GNSV23] in the standard model. In this context, the assumption is typically stated for the knapsack variant of LWE, which asks to recover $\mathbf{e}$ from $\mathbf{B} \in (\mathbb{Z}/q\mathbb{Z})^{(m-n)\times m}$ and $\mathbf{B}\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^{m-n}$ where $\mathbf{B}$ is typically uniform (possibly in a computational indistinguishability sense) and each coefficient of $\mathbf{e}$ is i.i.d. from $\chi$. We refer to [MM11] for reductions between LWE in standard and knapsack forms. As before, we are interested in a regime where there is a single solution. In this formulation, an instance sampler is oblivious if it can create an instance $\mathbf{B}\mathbf{e}$ without knowing the solution $\mathbf{e}$. In the mentioned SNARK constructions, the non-existence of an efficient oblivious sampler is used to provide the knowledge soundness property, i.e., to extract a witness from a prover. As these constructions rely on assumptions related to lattices, they are often conjectured secure even against quantum adversaries.

**Contributions.** Our main contribution is a polynomial-time quantum LWE sampler that we prove oblivious under the assumption that LWE is intractable, under very mild parameter restrictions. We prove the following result.

**Theorem 1.** *Let $m \geq n \geq 1$ and $q \geq 3$ be integers and $\sigma \geq 2$ be a real number. The parameters $m, n, q, \sigma$ are functions of the security parameter $\lambda$ with $m, \log q \leq \mathsf{poly}(\lambda)$ and $q$ prime. Assume that the parameters satisfy the following conditions:*

$$m \geq n\sigma \cdot \omega(\log \lambda) \quad \text{and} \quad 2 \leq \sigma \leq \frac{q}{\sqrt{8m \ln q}} \ .$$

*Then there exists a $\mathsf{poly}(\lambda)$-time quantum oblivious $\mathsf{LWE}_{m,n,q,\vartheta_{\sigma,q}}$ instance sampler, under the assumption that $\mathsf{LWE}_{m,n,q,\vartheta_{\sigma,q}}$ is hard.*

The proof technique and result are quite flexible. For example, the secret $\mathbf{s}$ can have any efficiently sampleable distribution. Also, we will show that obliviousness is preserved through randomized Karp reductions. Then, by using reductions from LWE with a parametrization satisfying the conditions of the statement above to LWE with a second parametrization, we obtain the existence of an efficient quantum oblivious LWE sampler for the second parametrization, under the assumed hardness of LWE for the first parametrization. We can notably throw away superfluous samples (i.e., decrease $m$), take an arbitrary arithmetic shape for $q$ and choose larger values for $\sigma$, by using modulus-dimension switching [BLP+13].

If oblivious LWE sampling is hard classically (which seems to be the case, as far as it is currently known), this gives an exponential quantum speed-up. So far, only very few problems related to lattices admit a quantum polynomial-time algorithm while remaining conjecturally hard for classical algorithms. Notable exceptions include finding a shortest non-zero vector in a lattice

corresponding to a principal ideal in a family of number fields such that the ideal contains an unexpectedly short generator [CDPR16], and finding a mildly short non-zero vector in a lattice corresponding to an (arbitrary) ideal in a family of number fields [CDW21]. These exceptions are restricted to (specific) lattices arising from algebraic number theory.

As a first step, we discuss the notion of oblivious sampling for a quantum algorithm. A prior definition was put forward in [LMZ23]. We propose an alternative definition that, in our opinion, better models what an extractor should be allowed. For the class of quantum algorithms that first perform a unitary and then a measurement, we show that these two definitions are equivalent. Even though our sampler belongs to that specific class of algorithms, we believe that our new definition is valuable as it provides further insight on oblivious sampling.

We then propose a general approach for a quantum oblivious sampling. Namely, we consider quantum algorithms that, given $\mathbf{A}$ as input, first generate a state of the form

$$\sum_{\mathbf{s},\mathbf{e}} \left( \prod_i f(e_i) \right) |\mathbf{A}\mathbf{s}+\mathbf{e}\rangle \ , \tag{1}$$

up to normalization and with $\mathbf{e} = (e_1, \ldots, e_m)^\intercal$, and then measure this state. Here $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is a non-zero complex-valued function, and if there are auxiliary registers, then they are all set to zero. The output is indeed an LWE instance $\mathbf{A}\mathbf{s}+\mathbf{e}$ for the input matrix $\mathbf{A}$. We show that any such quantum algorithm is an oblivious LWE sampler for the error distribution $\chi$ proportional to $|f|^2$ (under the assumption that LWE is hard).

Next, we modify an algorithm from [CLZ22] to obtain a quantum algorithm for generating a state as above, in time polynomial in $m$ and $\log q$, for a uniformly distributed $\mathbf{A}$ and for the folded integer Gaussian distribution $\vartheta_{\sigma,q}$, i.e., with $|f|^2 = \vartheta_{\sigma,q}$.

Finally, we consider the application of our result to the SNARK constructions mentioned above. In particular, this requires to adapt our analysis of the oblivious sampler to matrices $\mathbf{A}$ corresponding to the module version of LWE [BGV12, LS15]. We obtain that the underlying hardness assumption of Linear-Only Vector Encryption does not hold against quantum algorithms. This invalidates the security analyses of several standard model lattice-based SNARKs [GMNO18, NYI+20, ISW21, SSEK22, CKKK23, GNSV23]. We stress that this does not break the constructions themselves. For instance, the authors of [BISW17] mention a different route to analyze their SNARK construction in their Remark 4.9. Their approach is inspired by [BCI+13, Lem. 6.3] and can be applied to some of the constructions mentioned above.

### 1.1. **Technical overview.**

We now go into further detail for each one of the contributions.

#### 1.1.1. *Defining oblivious sampling for quantum algorithms.*

Let us first recall the classical notion of oblivious LWE sampling. Note that the discussion below could be generalized to more problems than LWE, but we focus on LWE for the sake of simplicity. Let $\mathcal{S}$ be an LWE sampler, taking as input a matrix $\mathbf{A}$ and returning a vector $\mathbf{b} = \mathbf{A}\mathbf{s}+\mathbf{e}$. To capture the notion of obliviousness, we consider extractor algorithms that can observe the behaviour of $\mathcal{S}$. More concretely, an extractor $\mathcal{E}$ is an algorithm that has access to the description of $\mathcal{S}$, its input $\mathbf{A}$ and its internal randomness $\rho_{\mathcal{S}}$ (which implies that $\mathcal{E}$ also knows the output $\mathbf{b}$). The extractor can also use random coins $\rho_{\mathcal{E}}$ of its own. Finally, it is requested to output $\mathbf{s}$. We say that $\mathcal{S}$ is an oblivious LWE sampler if no efficient extractor $\mathcal{E}$ succeeds with non-negligible probability over the choice of $\mathbf{A}$, $\rho_{\mathcal{S}}$ and $\rho_{\mathcal{E}}$.

The main difficulty that emerges in the quantum setting stems from measurements. They add inherent randomness to the computation that is not extractable, while classically, the randomness comes from an a priori given random string. In [LMZ23], the authors proposed an adaptation of extractability to the quantum setting that aims at handling this issue. By arguing that any quantum algorithm can be generically transformed into another one that first starts by a unitary transformation and then performs a measurement (possibly not on all its registers), the authors of [LMZ23] consider only such quantum samplers to define extractability. In their definition of extraction, the sampler is first executed until it performs its measurement, and then the measurement outcome and remaining registers are handed over to the extractor. More formally, the

extractor $\mathcal{E}$ is a quantum algorithm that is given as inputs the description of the quantum sampler $\mathcal{S}$, the input matrix $\mathbf{A}$, the output $\mathbf{b} = \mathbf{As} + \mathbf{e}$ and the auxiliary registers of $\mathcal{S}$ (the extractor may also have auxiliary ancillas of its own). Again, we are interested in the existence of efficient samplers of that form that output $\mathbf{s}$ with non-negligible probability. The authors justify as follows that it is a definition that is consistent with the classical setting. It is first observed that unitary algorithms are reversible. In the classical setting, every algorithm can be turned into a reversible one. By having the output of the reversible algorithm, one can find the input which contains the randomness. Therefore, giving the output of the reversible sampler to the extractor is equivalent to giving its input and the randomness to the extractor.

We propose an alternative definition, to allow the extractor to more closely look at the behaviour of the sampler. Indeed, it may seem overly restrictive to forbid the extractor from looking at the sampler's execution itself. Furthermore, the fact that any quantum computation can be converted into a unitary-then-measurement sampler cannot be applied in the extractability context, as it is not a priori excluded that one would be able to extract the secret from the complex form of the algorithm and not from the compiled form and vice-versa. Our definition aims at handling these two limitations of the [LMZ23] definition. The main principle we use is that observing or measuring the execution of a machine (classical or quantum) must not change too much the view that the sampler has of itself. Assume that an extractor is observing a sampler. Let $\rho_{\mathsf{Q}\otimes\mathsf{E}}$ represent the joint state of the sampler $\mathcal{S}$ and the extractor $\mathcal{E}$ at some step of the execution. The extractor might have carried out particular inspections that ended up in entangling its register with that of the sampler, so the state $\rho_{\mathsf{Q}\otimes\mathsf{E}}$ might not be separable. We intuitively expect from a valid extractor that if we trace out its register, the remaining state must be as if the extractor was not inspecting the sampler at all, or as if it was modifying the behaviour of the sampler in a negligible manner. Namely, if $\rho_{\mathsf{Q}}$ was the state of an isolated sampler at a specific step, and $\rho_{\mathsf{Q}\otimes\mathsf{E}}$ is the joint state of the sampler and extractor at the same step, we require that $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}})$ is close to $\rho_{\mathsf{Q}}$ for the trace distance.

We show that these two definitions are equivalent in the case of unitary-then-measurement samplers. However, our definition handles more general samplers, making it easier for the adversary to design an oblivious sampler, and hence providing a stronger notion oblivious sampling hardness. It turns out that our oblivious sampler is of the unitary-then-measurement type, so the definitional discrepancy is not critical to our result. We however believe that our definition provides further insight into the set of operations that an extractor should be allowed to perform.

As an additional contribution on oblivious sampling, we show that obliviousness is preserved under black-box Karp reductions between distributional problems. Let us consider the following scenario in our $\mathsf{LWE}$ setting. Assume that there is a reduction $\mathcal{A}$ from an $\mathsf{LWE}$ variant $\mathsf{LWE}_1$ to another $\mathsf{LWE}$ variant $\mathsf{LWE}_2$ such that $(i)$ an instance of $\mathsf{LWE}_1$ is mapped to an instance of $\mathsf{LWE}_2$ (with appropriate distribution over the randomness of the $\mathsf{LWE}_1$ instance and the random coins of $\mathsf{LWE}_2$) and $(ii)$ a solution to the $\mathsf{LWE}_1$ instance can be obtained from a solution to the $\mathsf{LWE}_2$ instance. Then applying the reduction $\mathcal{A}$ to an oblivious $\mathsf{LWE}_1$ sampler gives an oblivious $\mathsf{LWE}_2$ sampler. In our case, this observation will prove useful to weaken parameter constraints on $\mathsf{LWE}$ for oblivious sampling: we will first obtain an oblivious sampler for some restricted parametrization of $\mathsf{LWE}$ and extend it to more general setups thanks to existing such reductions.

1.1.2. *Reducing oblivious* $\mathsf{LWE}$ *sampling to* $|\mathsf{LWE}\rangle$. Assume we have a (classically) known matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and that we manage to build the quantum state from Equation (1) using a unitary transformation (with possibly auxiliary registers equal to zero). Creating such a state was studied in [SSTX09] and referred to as the $\mathsf{C}|\mathsf{LWE}\rangle$ problem in [CLZ22]. We will refer it as $|\mathsf{LWE}\rangle$, for the sake of simplicity. We show that oblivious $\mathsf{LWE}$ sampling reduces to $|\mathsf{LWE}\rangle$. Intuitively, a measurement of the state above provides an $\mathsf{LWE}$ sample $\mathbf{As} + \mathbf{e}$ for a uniformly distributed $\mathbf{s}$ and a vector $\mathbf{e}$ with distribution $\chi$ proportional to $|f|^2$: there is no reason for a specific $\mathbf{s}$ to be privileged, and this algorithm does not seem to have any additional knowledge about the $\mathsf{LWE}$ solution. We formalize this intuition using the obliviousness sampling definitions discussed above (which coincide here, as we have a unitary-then-measure algorithm). The result also holds if we add non-constant phases for $\mathbf{s}$ (for example to obtain $\mathbf{s}$ that is uniform among those with binary

coordinates). It also allows the parameter $m$ from $|\mathsf{LWE}\rangle$ to be larger than the one we want for oblivious $\mathsf{LWE}$ sampling, as we may throw away the superfluous coordinates without compromising the obliviousness.

We now discuss two existing approaches for solving $|\mathsf{LWE}\rangle$. The first one, derived from the $\mathsf{LWE}$ hardness proof from [Reg09], is to generate the following quantum state

$$\sum_{\mathbf{s},\mathbf{e}} \left( \prod_i f(e_i) \right) |\mathbf{s}\rangle \, |\mathbf{A}\mathbf{s}+\mathbf{e}\rangle \ , \tag{2}$$

up to normalization, and then to uncompute $|\mathbf{s}\rangle$ from $|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$. Generating this state can be done efficiently (possibly under some conditions on $f$) by first creating the superposition over all $\mathbf{s}$ and $\mathbf{e}$ of $|\mathbf{s}\rangle\,|\mathbf{e}\rangle$ with proper amplitudes, and then multiplying the first register by $\mathbf{A}$ to add it to the second one. To remove $\mathbf{s}$, i.e., to replace $\mathbf{s}$ by $\mathbf{0}$ in the first register, the approach from [Reg09] is to recover $\mathbf{s}$ from the second register and subtract it to the first one, by using a quantized $\mathsf{LWE}$ solver. This leads to a reduction from $|\mathsf{LWE}\rangle$ to $\mathsf{LWE}$. Unfortunately, in our context, this is not satisfactory, as $\mathsf{LWE}$ must be assumed difficult for oblivious $\mathsf{LWE}$ sampling to be feasible.

Another approach for solving $|\mathsf{LWE}\rangle$ was recently proposed in [CLZ22, Sec. 5]. The proposed algorithm does not require any oracle for a presumably hard problem, but seems restricted to specific parametrizations of $|\mathsf{LWE}\rangle$, as we discuss below.

- First, it builds the quantum state from Equation (2). It can be rewritten as follows:

$$\begin{aligned} \sum_{\mathbf{s},\mathbf{e}} \bigotimes_{i\leq m} |\mathbf{s}\rangle \, f(e_i) \, |\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i\rangle &= \sum_{\mathbf{s}} |\mathbf{s}\rangle \left( \bigotimes_{i\leq m} \sum_{e_i} f(e_i) \, |\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i\rangle \right) \\ &= \sum_{\mathbf{s}} |\mathbf{s}\rangle \left( \bigotimes_{i\leq m} |\psi_{\langle \mathbf{a}_i, \mathbf{s}\rangle}\rangle \right) \ , \end{aligned}$$

  where $|\psi_k\rangle = \sum_e f(e)\,|k+e\rangle$ for all $k \in \mathbb{Z}/q\mathbb{Z}$ (up to normalization).

- Second, it individually considers all sub-registers $|\psi_{\langle \mathbf{a}_i, \mathbf{s}\rangle}\rangle$ of the $|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle$ register, and performs a measurement for each one of them. For each $i$, the measurement consists in sampling a uniform $k_i \in \mathbb{Z}/q\mathbb{Z}$ and applying a projective measurement with respect to the (normalized) Gram-Schmidt orthogonalization of $|\psi_{k_i+1}\rangle, |\psi_{k_i+2}\rangle, \ldots, |\psi_{k_i-1}\rangle, |\psi_{k_i}\rangle$ (we assume that the $|\psi_j\rangle$'s are linearly independent, and the indices are taken modulo $q$). If the measurement is on the last direction, then $|\psi_{\langle \mathbf{a}_i, \mathbf{s}\rangle}\rangle$ cannot have a component on the span of $|\psi_{k_i+1}\rangle, |\psi_{k_i+2}\rangle, \ldots, |\psi_{k_i-1}\rangle$ and must be equal to $|\psi_{k_i}\rangle$. When successful, the measurement indicates that $\langle \mathbf{a}_i, \mathbf{s}\rangle = k_i \bmod q$.

- Third, sufficiently many successful measurements are collected through the different values of $i$, to obtain many equations of the type $\langle \mathbf{a}_i, \mathbf{s}\rangle = k_i$, where the $\mathbf{a}_i$'s and $k_i$'s are known. This is then fed to a quantized Gaussian elimination algorithm (recall that we are working with a superposition over all $\mathbf{s}$'s). The latter outputs $\mathbf{s}$, which is then subtracted from the first register.

It was proved in [CLZ22] that this algorithm solves $|\mathsf{LWE}\rangle$ in polynomial time, if $m$ and $q$ are polynomial in the security parameter $\lambda$, if a state proportional to $\sum_e f(e)\,|e\rangle$ can be efficiently computed, and if

$$m = \frac{n}{p^{\mathrm{CLZ}}} \cdot \omega(\log \lambda) \quad \text{with} \quad p^{\mathrm{CLZ}} = \frac{\min_x |\widehat{f}(x)|^2}{q} \ .$$

Here, the notation $\widehat{f}$ refers to the Fourier transform over $\mathbb{Z}/q\mathbb{Z}$ of $f$. The quantity $p^{\mathrm{CLZ}}$ corresponds to the probability that an individual measurement of the second step succeeds. This result notably allows to solve $|\mathsf{LWE}\rangle$ (and hence oblivious $\mathsf{LWE}$ sampling) for $q$ polynomial and $\chi$ set as the uniform distribution in an interval $[-B, B] \cap \mathbb{Z}$, for any $B \in \mathbb{Z}$ such that $0 < 2B+1 < q$ and $\gcd(2B+1, q) = 1$. Interestingly, by taking $q = 2$, the result also allows to solve the adaptation of $|\mathsf{LWE}\rangle$ to the decoding problem for uniform binary codes (also known as Learning Parity with

Noise), and to obliviously sample points near codewords for the Bernoulli distribution with an arbitrary Bernoulli parameter in $(0, 1/2)$.

This result has two limitations. First, the lower bound on $m$ and the run-time both grow at least polynomially with $q$ (note that $\min|\widehat{f}| \leq 1$), which prevents us from choosing an exponential $q$. This is in part due to the uniform guess of $\langle \mathbf{a}_i, \mathbf{s}\rangle$ in the measurement, which directly incurs a loss by a factor $q$ in the success probability of each individual measurement. Note that for a fixed standard deviation $\sigma$, LWE becomes no harder as $q$ increases, so that one can expect that it is indeed no easier to obliviously sample LWE instances (intuitively, the easier is the considered problem, the harder it is to obliviously sample instances). Most SNARKs that we consider use an exponential $q$. Second, the quantity $\min|\widehat{f}|$ is extremely small for a wide range of amplitude functions, notably $f = \sqrt{\vartheta_{\sigma,q}}$ up to a normalization factor (recall that $\vartheta_{\sigma,q}$ denotes the folded discrete Gaussian distribution). Indeed, we prove in Lemma 18 that in that case and if $\sigma \geq 1$, we have

$$q \cdot \min|\widehat{f}|^2 \leq 32\sigma \cdot \exp\left(-\min\left(\frac{\pi\sigma^2}{4}, \frac{q^2}{4\sigma^2}\right)\right) .$$

This expression is most often extremely small. For example, for $\sigma = \Omega(\sqrt{n})$ and $q = \Omega(\sqrt{n}\sigma)$, the expression is $2^{-\Omega(n)}$. This prevents from meaningfully using the result for the discrete Gaussian distribution, which is the most common choice of error distribution for LWE.

1.1.3. *Measuring with increased success probability.* The second step of the algorithm from [CLZ22] consists in taking $|\psi_k\rangle$ for an unknown $k \in \mathbb{Z}/q\mathbb{Z}$ as input and returning $k$, i.e., it aims at distinguishing the quantum states $|\psi_0\rangle, \ldots, |\psi_{q-1}\rangle$. One could proceed as follows if the states were orthogonal. Consider the well-defined projective measurement $(\mathbf{E}_i)_i$ defined by $\mathbf{E}_i = |\psi_i\rangle\langle\psi_i|$ for $0 \leq i < q$. Then, if the state $|\psi_k\rangle$ is given, the probability to see $k$ as the outcome is $\langle\psi_k|\mathbf{E}_k^\dagger\mathbf{E}_k|\psi_k\rangle = 1$. In other words, this quantum measurement perfectly distinguishes the quantum states. However, when the $|\psi_k\rangle$'s are not orthogonal (which is our case except for $f$ being 1 in 0 and 0 elsewhere), it is known that there exists no quantum measurement to perfectly distinguish them (see [NC11, Box 2.3]). The measurement from [CLZ22] may output a special symbol $\perp$ representing the "unknown" answer, but it does not make any mistake, in the sense that it never outputs some $\ell \in \mathbb{Z}/q\mathbb{Z}$ different from $k$. Such a process is referred to as unambiguous. This property is important for the subsequent Gaussian elimination step, as it requires all linear equations to be correct. We define the error parameter of the unambiguous measurement as the maximal probability that the measurement outputs $\perp$ over all possible input states:

$$p_\perp = \max_k \langle\psi_k|\mathbf{E}_\perp|\psi_k\rangle ,$$

where $\mathbf{E}_\perp$ corresponds to the outcome $\perp$. The measurement from [CLZ22] satisfies

$$1 - p_\perp^{\mathrm{CLZ}} = p^{\mathrm{CLZ}} = \frac{\min|\widehat{f}|^2}{q} .$$

We propose to change the unambiguous measurement by the positive operator-valued measure (POVM) from [CB98]. It is known to be "optimal" when the $|\psi_i\rangle$'s are symmetric and linearly independent, in the sense that it minimizes the error parameter $p_\perp$ over all possible choice of POVMs. Here, symmetric means that there exists a unitary $\mathbf{U}$ such that $|\psi_i\rangle = \mathbf{U} \cdot |\psi_{i-1 \bmod q}\rangle$ for all $0 \leq i < q$: our states indeed satisfy this property with $\mathbf{U}$ being the mod-$q$ translation operator. The linear independence property may or may not be satisfied, depending on the choice of $f$ (this is a difficulty encountered in other sections of [CLZ22]). The measurement from [CB98] is defined as follows:

$$\forall 0 \leq i < q : \mathbf{E}_i = \alpha \cdot \left|\psi_i^\perp\right\rangle\left\langle\psi_i^\perp\right| \quad \text{and} \quad \mathbf{E}_\perp = \mathbf{I} - \sum_i \mathbf{E}_i ,$$

where $\left|\psi_i^\perp\right\rangle$ is a unit vector orthogonal to all $|\psi_j\rangle$'s for $j \neq i$, for all $0 \leq i < q$. The scalar $\alpha$ is chosen maximal such that the POVM is well-defined, i.e., such that $\mathbf{E}_\perp$ is non-negative: it is the

inverse of the largest eigenvalue of $\sum_i \mathbf{E}_i$. We compute that this measurement leads to:

$$1 - p_{\perp}^{\mathrm{CB}} = \frac{q^2\ \alpha}{\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \left|\widehat{f}(x)\right|^{-2}} = q \cdot \min \left|\widehat{f}\right|^2 \ .$$

Note that the success probability of the measurement is a factor $q^2$ higher than the one from [CLZ22]. By the union bound (and still assuming $q$ prime), with the optimal unambiguous measurement, it suffices to set

$$m = \frac{n}{q \cdot \min |\widehat{f}|^2} \cdot \omega(\log \lambda) \ . \tag{3}$$

1.1.4. *How to implement the measurement in time polynomial in* $\log q$. Compared to the [CLZ22] approach, the quantum distinguishing measurement from [CB98] allows one to choose $m$ smaller by a factor $q^2$ and also to gain a factor $q^2$ in the run-time. But beyond these considerations over the parameter $m$, that we discuss more deeply in Subsection 1.1.5, recall that we are looking for a sampler whose run-time is polynomial in $m$ and $\log q$. We therefore have to efficiently implement the above POVM. Although the measurement was introduced in [CB98], this work does not specify how to efficiently compute it. The POVM components $(\mathbf{E}_j)_{0\leq j<q}$ turn out to be some projections $\left(\left|\psi_j^{\perp}\right\rangle\!\left\langle\psi_i^{\perp}\right|\right)_{0\leq j<q}$. A first approach would be to compute the quantum states $\left|\psi_i^{\perp}\right\rangle$'s, which are given by (here $\omega_q$ refers to a primitive $q$-th root of unity.)

$$\forall j : \left|\psi_j^{\perp}\right\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-jx} \cdot \overline{\widehat{f}(-x)^{-1}}\ |\chi_x\rangle$$

where $N = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} |\widehat{f}(-x)|^{-2}$ and $(|\chi_x\rangle)_{x\in\mathbb{Z}/q\mathbb{Z}}$ denotes the Fourier basis, namely

$$\forall x : |\chi_x\rangle = \frac{1}{\sqrt{q}} \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{xy}\, |y\rangle \ .$$

However, even if one were able to compute these quantum states in polynomial time, there are $q$ of them, making it difficult to obtain a run-time polynomial in $\log q$. One may therefore try to find a way to efficiently compute a unitary sending $|j\rangle\,|0\rangle$ to $|j\rangle\left|\psi_j^{\perp}\right\rangle$ for all $j$. This seems to be a challenging path, as such a unitary would need to implement the POVM. Let us backtrack a little, and try to see how the POVM given by $(\mathbf{E}_j)_{0\leq j<q}$ and $\mathbf{E}_{\perp}$ acts on the $|\psi_j\rangle$'s. First, let us decompose the $|\psi_j\rangle$'s in the Fourier basis:

$$\forall j : |\psi_j\rangle = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x) \cdot \omega_q^{-jx}\ |\chi_x\rangle \ .$$

To correctly identify $|\psi_j\rangle$, we project it according to $\mathbf{E}_j = \left|\psi_j^{\perp}\right\rangle\!\left\langle\psi_j^{\perp}\right|$. This leads to considering the following Hermitian product:

$$\begin{aligned}\left\langle\psi_j^{\perp}\middle|\psi_j\right\rangle &= \frac{1}{\sqrt{Nq^n}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{jx} \cdot \widehat{f}(-x)^{-1} \cdot \widehat{f}(-x) \cdot \omega_q^{-jx} \\ &= \frac{1}{\sqrt{Nq^n}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x)^{-1} \cdot \widehat{f}(-x)\end{aligned}$$

In other words, when projecting $|\psi_j\rangle$ on $\left|\psi_j^{\perp}\right\rangle$, we want to "remove" $\widehat{f}(-x)$ in the amplitudes of $|\psi_j\rangle$ in its Fourier basis decomposition. Therefore, simulating the POVM of [CB98] leads to considering the unitary performing this task, i.e., a unitary $\mathbf{V}$ such that

$$\forall x : |\chi_x\rangle\,|0\rangle \longmapsto \frac{\min|\widehat{f}|}{\widehat{f}(-x)}\,|\chi_x\rangle\,|0\rangle + \sqrt{1 - \left|\frac{\min|\widehat{f}|}{\widehat{f}(-x)}\right|^2}\,|\chi_x\rangle\,|1\rangle$$

(We note that a similar approach was considered in [CT23].) Such a unitary is efficiently computable under the conditions that both $\min|\widehat{f}|$ and $\widehat{f}(-x)$ can be efficiently approximated. Let

us check that $\mathbf{V}$ indeed "simulates" the measurement from [CB98], by computing how it acts on the $|\psi_j\rangle$'s:

$$\begin{aligned}\mathbf{V}\left(|\psi_j\rangle\,|0\rangle\right) &= \mathbf{V}\left(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x)\cdot\omega_q^{-jx}\ |\chi_x\rangle\,|0\rangle\right)\\ &= \sum_{x\in\mathbb{Z}/q\mathbb{Z}}\left(\min|\widehat{f}|\cdot\omega_q^{-jx}\ |\chi_x\rangle\,|0\rangle + \widehat{f}(-x)\cdot\omega_q^{-jx}\cdot\sqrt{1-\left|\frac{\min|\widehat{f}|}{\widehat{f}(-x)}\right|^2}\ |\chi_x\rangle\,|1\rangle\right)\\ &= \sqrt{q}\cdot\min|\widehat{f}|\ |x\rangle\,|0\rangle + \sum_{x\in\mathbb{Z}/q\mathbb{Z}}\widehat{f}(-x)\cdot\omega_q^{-jx}\cdot\sqrt{1-\left|\frac{\min|\widehat{f}|}{\widehat{f}(-x)}\right|^2}\ |\chi_x\rangle\,|1\rangle\end{aligned}$$

In other words, we have (for some quantum state $|\eta_j\rangle$):

$$\mathbf{V}\,|\psi_j\rangle\,|0\rangle = \sqrt{p^{\mathrm{CB}}}\,|j\rangle\,|0\rangle + \sqrt{1-p^{\mathrm{CB}}}\,|\eta_j\rangle\,|1\rangle\ ,$$

where $p^{\mathrm{CB}}$ turns out to be equal to the success probability of the POVM given in [CB98], i.e., $p^{\mathrm{CB}} = 1-p_\perp^{\mathrm{CB}}$. Therefore, by interpreting any quantum state whose last qubit is $|1\rangle$ as $\perp$, applying $\mathbf{V}$ amounts to quantumly recovering $j$ from $|\psi_j\rangle$ with probability $1-p_\perp^{\mathrm{CB}}$.

1.1.5. *Increasing the Fourier coefficients.* At this stage, we have that the modified $|\mathsf{LWE}\rangle$ algorithm is polynomial in $m$ and $\log q$. We also have decreased the feasibility threshold on $m$ from $nq/\min|\widehat{f}|^2\cdot\omega(\log\lambda)$ to $n/(q\cdot\min|\widehat{f}|^2)\cdot\omega(\log\lambda)$. However, as observed in [CLZ22], the quantity $\min|\widehat{f}|^2$ can be extremely low for distributions of interest.

Our last technical ingredient stems from the observation that for the purpose of oblivious $\mathsf{LWE}$ sampling for a distribution $\chi$, we do not need to set $f=\sqrt{\chi}$ but can set $f=\sqrt{\chi}\cdot u$ for any function $u:\mathbb{Z}/q\mathbb{Z}\to\mathbb{C}$ taking values on the unit circle. Indeed, the new phases disappear when we measure the $|\mathsf{LWE}\rangle$ state to obtain the $\mathsf{LWE}$ sample. Interestingly, the phases can greatly help to increase $\min|\widehat{f}|^2$. The astute reader will note that the circuit described above then needs to be updated to account for the phases, but we show that efficiency can be preserved, notably for the function $u$ that we choose. We propose to set $u$ as the sign function:

$$\forall x\in\mathbb{Z}\cap[0,q/2]: u(x)=1 \quad\text{and}\quad \forall x\in\mathbb{Z}\cap(-q/2,0): u(x)=-1\ .$$

Then the following relations hold, for $q$ odd and for all $x\in\mathbb{Z}/q\mathbb{Z}$ viewed as an integer in $(-q/2,q/2]$:

$$\begin{aligned}\widehat{f}(x) &= \frac{1}{\sqrt{q}}\sum_{y\in\mathbb{Z}/q\mathbb{Z}} f(y)\cdot\omega_q^{xy}\\ &= \frac{1}{\sqrt{q}}\sum_{\mathbb{Z}\cap[0,q/2]}\sqrt{\chi(y)}\cdot\omega_q^{xy} - \frac{1}{\sqrt{q}}\sum_{\mathbb{Z}\cap(-q/2,0)}\sqrt{\chi(y)}\cdot\omega_q^{xy}\\ &= \frac{\sqrt{\chi(0)}}{\sqrt{q}} + \frac{1}{\sqrt{q}}\sum_{\mathbb{Z}\cap(0,q/2]}\sqrt{\chi(y)}\cdot(\omega_q^{xy}-\omega_q^{-xy})\ .\end{aligned}$$

Note that the summand is an imaginary number and hence that $\sqrt{\chi(0)/q}$ is the real part of $\widehat{f}(x)$. As a result, we obtain that $\min|\widehat{f}|\geq\sqrt{\chi(0)/q}$. By combining with Equation (3), it suffices to set $m=n/\chi(0)\cdot\omega(\log\lambda)$. For the specific case of the folded integer Gaussian distribution, we have that $\chi(0)\approx 1/\sigma$, leading to an efficient algorithm when $\sigma$ is polynomial in $\lambda$.

We stress that we use both the phases and the improved unambiguous measurement to obtain an efficient algorithm. We already saw that the the improved measurement alone is insufficient. Conversely, if we use the phases and the measurement from [CLZ22], then it seems that we need $m$ to grow as $nq^2/\sigma\cdot\omega(\log\lambda)$, which forbids a run-time polynomial in $\log q$.

1.1.6. *Application to standard model lattice-based SNARKs.* Succinct Non-Interactive Arguments of Knowledge (SNARKs) are cryptographic schemes whose purpose is to prove NP statements with a succinct proof and fast verification, as a function of the statement size. They must satisfy the property of knowledge soundness: informally speaking, if a malicious prover manages to build a proof that passes verification, then one can extract from its description and execution a valid witness for the proved statement. Several candidate SNARKs based on lattices in the standard model [GMNO18, NYI+20, ISW21, SSEK22, CKKK23, GNSV23] assume the hardness of some type of knowledge assumption, i.e., an assumption that formalizes the intuition that an algorithm cannot achieve a given task without knowing a specific information. This intuition is formalized using extractor algorithms. The specific knowledge assumptions used in those schemes are typically defined in terms of LWE-based ciphertexts (also sometimes called encodings) of a symmetric encryption scheme.

To simplify the discussion, we now focus on the constructions from [ISW21, SSEK22, CKKK23]. The discussion can be adapted to the other schemes (see Section 6.4). The corresponding encryption scheme handles plaintexts defined modulo an integer $p$, with ciphertexts that are vectors modulo a much larger integer $q$, such that the scheme enjoys a linear homomorphism property: given $y_1, \ldots, y_m \in \mathbb{Z}/p\mathbb{Z}$ and ciphertexts $\mathbf{ct}_1, \ldots, \mathbf{ct}_m$ decrypting to $a_1, \ldots, a_m$, the vector $\sum_i y_i \mathbf{ct}_i$ decrypts to $\sum y_i a_i$. It is then assumed that the only way to compute a valid ciphertext is to take a linear combination of the available ciphertexts (variants may be used in different schemes). To obtain SNARKs, this is formalized in terms of the existence of an efficient extractor: given the $\mathbf{ct}_i$'s, the description of the algorithm producing a new ciphertext and its internal randomness, some efficient extractor recovers scalars $y_i$'s modulo $p$ such that $\mathbf{ct} = \sum_i y_i \mathbf{ct}_i$.

We observe that the knowledge assumptions involved in those schemes can be expressed in terms of the knapsack version of LWE. The knLWE problem asks to recover $\mathbf{e}$ from the input $(\mathbf{B}, \mathbf{Be})$ where $\mathbf{B}$ is a uniformly chosen matrix from $(\mathbb{Z}/q\mathbb{Z})^{(m-n)\times m}$, for some integers $m > n \geq 1$ and $q \geq 2$. We are in a regime of parameters where $\mathbf{e}$ is uniquely determined from $\mathbf{Be}$, with overwhelming probability over the uniform choice of $\mathbf{B}$. We identify the matrix $\mathbf{B}$ with the matrix $(\mathbf{ct}_1, \ldots, \mathbf{ct}_m)$. Note that it is not uniform, we can pretend it is as it is computationally indistinguishable from uniform under some LWE parametrization. We then argue that the knowledge assumption is quantumly broken, by observing that our witness-oblivious quantum LWE sampler can be turned into a witness-oblivious knLWE sampler by relying on the randomized Karp reduction from LWE to knLWE from [MM11]. As some of the considered schemes rely on algebraic variants of LWE, such as Ring-LWE [SSTX09, LPR10] or Module-LWE [BGV12, LS15], we extend the witness-oblivious LWE sampler to those settings. The analysis extends without difficulty, except for difficulties arising from the fact that the considered rings are not fields.

1.2. **Related works.** Positive and negative results on the possibility of obliviously sampling in the image of a one-way function have been given in [BCPR16]. Even though LWE is a (conjectured) one-way function, this work is incomparable to ours as it considers the situation where the sampler and the extractor are both given some auxiliary input.

From a technical perspective, one of our main ingredients is to replace an unambiguous discrimination measurement used in [CLZ22] by the optimal unambiguous discrimination measurement from [CB98]. This change was also considered recently in [CT23] for linear codes and the Hamming metric, with the objective of obtaining an efficient quantum algorithm to find short non-zero elements in linear codes via the framework given by [CLZ22].

The obliviousness sampling hardness assumption belongs to the family of non-falsifiable assumptions [Nao03, GW11], similar to the knowledge of exponent assumption in the discrete logarithm setting [Dam91]. In the context of succinct non-interactive arguments, such assumptions seem difficult to avoid, as it was proved in [GW11] that falsifiable assumptions must be used to prove security if one resorts to black-box reductions. Using non-falsifiable assumptions makes the cryptanalyst's task more difficult: as the attack cannot be efficiently tested by a challenger, the cryptanalyst is required to prove (or convincingly argue) that the attack works. One way to circumvent this impossibility result is to rely on the random oracle model, which indeed leads to efficient succinct non-interactive arguments [BSCS16]. We stress that our algorithm has an impact

on the quantum security of standard model lattice-based SNARKs, but not on [AFLN23] which relies on the random oracle model. We also stress that our algorithm does not seem applicable to known standard model lattice-based SNARGs, which differ from SNARKs in their definition of soundness.

Beyond those studied in this work, another candidate construction of a standard model lattice-based SNARK was proposed in [ACL+22], but the underlying assumption was broken classically in [WW23].

## 2. Preliminaries

**Notation.** The function ln refers to the logarithm in base e. When the base of the logarithm does not matter, we write log.

We will consider the additive group $\mathbb{Z}/q\mathbb{Z}$ for $q \geq 2$ and may write its elements as

$$\mathbb{Z}/q\mathbb{Z} = \left\{ j \in \mathbb{Z} \ : \ -\frac{q}{2} < j \leq \frac{q}{2} \right\} \ .$$

We define $\omega_q$ as $\exp(2\pi i/q)$. Recall that the discrete Fourier transform of every function $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is defined as follows:

$$\forall x \in \mathbb{Z}/q\mathbb{Z}, \quad \widehat{f}(x) := \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} f(y) \cdot \omega_q^{-xy} \ .$$

For an integer $m$ and a real number $r \geq 0$, we let $\mathrm{B}_m(r)$ denote the ball of $\mathbb{R}^m$ with radius $r$. Vectors are in column notation and are written with bold letters (such as $\mathbf{x}$). Uppercase bold letters are used to denote matrices (such as $\mathbf{A}$). For vectors $\mathbf{a}_1, \ldots, \mathbf{a}_n$, we let $(\mathbf{a}_1 | \ldots | \mathbf{a}_n)$ denote the matrix whose columns are the $\mathbf{a}_i$'s. For any two vectors $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}/q\mathbb{Z})^d$, we define their inner product as

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^{d} x_i y_i \bmod q \ .$$

We define $\omega(\cdot), O(\cdot)$, and $\Omega(\cdot)$ in the usual way. When it is not clear from the context, we use subscripts to clarify the input parameter, for instance $\Omega_\lambda(\cdot)$. We let $\mathsf{poly}(\lambda)$ denote any function which is of order $O(\lambda^a)$ for some constant $a$. Furthermore, the notation $\mathsf{negl}(\lambda)$ refers to a function that is $O(1/\lambda^b)$ for every constant $b > 0$.

We use PPT to denote the usual class of classical Probabilistic Polynomial-Time algorithms.

Sometimes, we will use a subscript to stress the random variable specifying the associated probability space over which the probabilities or expectations are taken. For instance the probability $\mathbb{P}_X(E)$ of the event $E$ is taken over the probability space $\Omega$ with respect to the induced measure by $X$. We let $U(S)$ denote the uniform distribution over $S$. Given any distribution $X$, the distribution $X^{\otimes m}$ is defined as $(X_1, \ldots, X_m)$ where $X_i$'s are independently distributed as $X$. For any two discrete probability distributions $X$ and $Y$ over a set $S$, their statistical distance (also called the total variation distance) is defined as:

$$\Delta(X, Y) := \frac{1}{2} \sum_{s \in S} |\mathbb{P}_X(s) - \mathbb{P}_Y(s)| \ .$$

Let $f : S \to \mathbb{C}$ be a function. We define the function $f^{\otimes d} : S^d \to \mathbb{C}$ as $f^{\otimes d}(x_1, \ldots, x_d) := f(x_1) \cdots f(x_d)$, for all $(x_1, \ldots, x_d) \in S^d$. When the dimension $d$ is clear from the context, we abuse the notation and write $f$ instead of $f^{\otimes d}$. Let $S$ be a finite set and $f : S \to \mathbb{C}$. We say that $f$ is an *amplitude function* if

$$\sum_{x \in S} |f(x)|^2 = 1 \ .$$

We note that $f^{\otimes d}$ is an amplitude function whenever $f$ is an amplitude function.

2.1. **Quantum computations.** We refer the reader to [NC11, Wat18] for introductions on quantum algorithms.

We use the quantum circuit model of computation. A quantum circuit operates on some number of qubits, using one-qubit or two-qubit unitary gates and projective measurements. The measurements are performed in a priori fixed computational basis. The outcome of the last measurement is typically considered as the output of the algorithm. An algorithm may use ancilla qubits, i.e., extra quantum registers initialized to $|0\rangle$. We say that a sequence of quantum circuits $(Q_i)_i$ is QPT if there exists a deterministic polynomial-time algorithm that takes $i$ in unary as input and outputs the description of $Q_i$ with gates and measurements.

**Partial trace.** For our purposes, we need to describe sub-systems of a given "composite" quantum system. This description involves the partial trace. Let $\mathcal{A}$ and $\mathcal{B}$ be two Hilbert spaces with $\{|a\rangle\}_{a\in\mathcal{I}}$ and $\{|b\rangle\}_{b\in\mathcal{J}}$ as their orthonormal bases, respectively. For all $a_1, a_2 \in \mathcal{I}$ and $b_1, b_2 \in \mathcal{J}$, tracing out the register of $\mathcal{B}$ is defined as follows:

$$\mathrm{tr}_{\mathcal{B}}\left(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|\right) := \langle b_1|b_2\rangle\, |a_1\rangle\langle a_2| \ .$$

It is extended by linearity.

**Trace distance.** We will also use the *trace distance* which is defined over two quantum states $\rho, \sigma$ as follows:

$$D_{\mathrm{tr}}\left(\rho,\sigma\right) := \frac{1}{2}\,\mathrm{tr}\left(\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right) \ .$$

For pure quantum states $|\psi\rangle$ and $|\varphi\rangle$, it can be simplified to $\sqrt{1-|\langle\varphi|\psi\rangle|^2}$. The trace distance has the following properties (see [NC11, Th. 9.2]):

- for any joint states $\rho, \sigma$ over $\mathcal{A}\otimes\mathcal{B}$, it holds that $D_{\mathrm{tr}}(\mathrm{tr}_{\mathcal{B}}(\rho), \mathrm{tr}_{\mathcal{B}}(\sigma)) \le D_{\mathrm{tr}}(\rho,\sigma)$;
- for any quantum states $\rho, \sigma, \tau$, it holds that $D_{\mathrm{tr}}(\rho,\sigma) \le D_{\mathrm{tr}}(\rho,\tau) + D_{\mathrm{tr}}(\tau,\sigma)$;
- for any quantum states $\rho, \sigma, \tau$, it holds that $D_{\mathrm{tr}}(\rho\otimes\tau, \sigma\otimes\tau) = D_{\mathrm{tr}}(\rho,\sigma)$;
- for any quantum algorithm $\mathcal{Q}$ and any quantum states $\rho, \sigma$, it holds that $D_{\mathrm{tr}}(\mathcal{Q}(\rho), \mathcal{Q}(\sigma)) \le D_{\mathrm{tr}}(\rho,\sigma)$.

Let $M$ be the set of possible outcomes of a measurement on the above states. Let $X$ and $Y$ be the distributions over $M$ induced by measuring $\rho$ and $\sigma$, respectively. We have:

$$\Delta(X,Y) \ \le \ D_{\mathrm{tr}}(\rho,\sigma) \ . \tag{4}$$

**Quantum Fourier transform (QFT).** The **QFT** over the additive group $\mathbb{Z}/q\mathbb{Z}$, whose characters are $\chi_x : y \mapsto \omega_q^{xy}$ for $x \in \mathbb{Z}/q\mathbb{Z}$, is defined as follows:

$$\forall x \in \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{QFT}\,|x\rangle := \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{xy}\,|y\rangle \ .$$

The quantum states $|\chi_x\rangle := \mathbf{QFT}\,|x\rangle$ for $x \in \mathbb{Z}/q\mathbb{Z}$ are called the *Fourier basis*, whereas the states $|x\rangle$ form the *computational basis*. The following lemma recalls how the computational basis decomposes in the Fourier basis.

**Lemma 1.** *For any $q \ge 2$, it holds that*

$$\forall y \in \mathbb{Z}/q\mathbb{Z}, \quad |y\rangle = \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-yx}\,|\chi_x\rangle \ .$$

*Proof.* We have the following equalities:

$$\begin{aligned}\mathbf{QFT} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-yx} \left|\chi_x\right\rangle &= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-yx} \mathbf{QFT} \left|\chi_x\right\rangle \\ &= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-yx} \frac{1}{\sqrt{q}} \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{xm} \mathbf{QFT} \left|m\right\rangle \\ &= \sum_{m\in\mathbb{Z}/q\mathbb{Z}} \left( \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{x(m-y)} \right) \mathbf{QFT} \left|m\right\rangle \\ &= \sqrt{q}\, \mathbf{QFT} \left|y\right\rangle \ .\end{aligned}$$

The result is obtained by applying $\mathbf{QFT}^{-1}$. □

2.2. **Gaussian distributions.** The Gaussian function centered around $\mathbf{0}$ with the standard deviation parameter $\sigma > 0$ is defined as:

$$\forall \mathbf{x} \in \mathbb{R}^m : \ \rho_\sigma(\mathbf{x}) := \mathrm{e}^{-\pi \frac{\|\mathbf{x}\|^2}{\sigma^2}} \ .$$

where $\|\cdot\|$ denotes the Euclidean norm of $\mathbf{x}$. The following lemma shows the concentration behaviour of $\rho_\sigma$ over lattices.

**Lemma 2** (Adapted from [Ban93, Le. 1.5])**.** *For any $m$-dimensional lattice $\Lambda$ and any real numbers $\sigma > 0$ and $\sigma' \geq \sigma/\sqrt{2\pi}$, it holds that*

$$\rho_\sigma\left(\Lambda \setminus \mathrm{B}_m(\sigma'\sqrt{m})\right) \leq \left( \frac{\sigma'}{\sigma}\ \sqrt{2\pi \mathrm{e}}\ \mathrm{e}^{-\pi \frac{\sigma'^2}{\sigma^2}} \right)^m \rho_\sigma(\Lambda) \ .$$

We have the following inequality.

**Lemma 3.** *For every $\sigma > 0$, we have $\sigma \leq \rho_\sigma(\mathbb{Z}) \leq 1 + \sigma$.*

*Proof.* We have $\rho_\sigma(\mathbb{Z}) \leq 1 + 2\int_0^{+\infty} \rho_\sigma(x)\mathrm{d}x = 1 + \sigma$, by comparing the sum and the integral. Moreover, using the Poisson summation formula, one obtains $\rho_\sigma(\mathbb{Z}) = \sigma \cdot \rho_{1/\sigma}(\mathbb{Z}) \geq \sigma$. □

The discrete Gaussian distribution over $\mathbb{Z}^m$ centered around $\mathbf{0}$ with the standard deviation $\sigma$ is defined as follows:

$$\forall \mathbf{k} \in \mathbb{Z}^m : \ D_{\mathbb{Z}^m,\sigma}(\mathbf{k}) := \frac{\rho_\sigma(\mathbf{k})}{\rho_\sigma(\mathbb{Z}^m)} \ ,$$

where $\rho_\sigma(\mathbb{Z}^m) := \sum_{\mathbf{k}\in\mathbb{Z}^m} \rho_\sigma(\mathbf{k})$. Folding $D_{\mathbb{Z}^m,\sigma}$ modulo an integer $q$ yields the distribution $\vartheta_{\sigma,q}$.

**Definition 1** (Folded Discrete Gaussian Distribution)**.** *Let $q \geq 2$ an integer and $\sigma > 0$ a real number. We define the folded discrete Gaussian distribution over $(\mathbb{Z}/q\mathbb{Z})^m$ with standard deviation $\sigma$ and folding parameter $q$ by its probability mass function $\vartheta_{\sigma,q}$:*

$$\forall \mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^m : \ \vartheta_{\sigma,q}(\mathbf{x}) := \frac{\sum_{\mathbf{k}\in\mathbb{Z}^m} \rho_\sigma(\mathbf{x} + \mathbf{k}q)}{\rho_s(\mathbb{Z}^m)} \ .$$

We note that in all distributions above, the dimension of the input is implicit and can be derived from the context. The distribution $\vartheta_{\sigma,q}$ behaves very closely to $D_{\mathbb{Z}^m,\sigma}$.

**Lemma 4.** *Let $m \geq 1$ and $q \geq 2$ integers and $\sigma > 0$ a real number. Assume that $q \geq 2\sigma\sqrt{m}$. Then for every $\mathbf{x} \in \mathbb{Z}^m \cap (-q/2, q/2]^m$, it holds that*

$$D_{\mathbb{Z}^m,\sigma}(\mathbf{x}) \leq \vartheta_{\sigma,q}(\mathbf{x}) \leq D_{\mathbb{Z}^m,\sigma}(\mathbf{x}) + \mathrm{e}^{-\frac{q^2}{(2\sigma)^2}} \quad \text{and} \quad \sqrt{D_{\mathbb{Z}^m,\sigma}(\mathbf{x})} \leq \sqrt{\vartheta_{\sigma,q}(\mathbf{x})} \leq \sqrt{D_{\mathbb{Z}^m,\sigma}(\mathbf{x})} + \mathrm{e}^{-\frac{q^2}{8\sigma^2}} \ .$$

*Proof.* For $\mathbf{x} \in \mathbb{Z}^m \cap (-q/2, q/2]^m$, we have

$$\begin{aligned}
\sum_{\mathbf{k}\in\mathbb{Z}^m} \rho_\sigma(\mathbf{x}+\mathbf{k}q) &= \rho_\sigma(\mathbf{x}) + \sum_{\mathbf{k}\in\mathbb{Z}^m\setminus\{\mathbf{0}\}} \rho_\sigma(\mathbf{x}+\mathbf{k}q) \\
&\leq \rho_\sigma(\mathbf{x}) + \sum_{\mathbf{k}\in\mathbb{Z}^m:\|\mathbf{k}\|\geq\frac{q}{2}} \rho_\sigma(\mathbf{k}) \\
&\leq \rho_\sigma(\mathbf{x}) + \rho_\sigma\left(\mathbb{Z}^m \setminus \mathrm{B}_m\left(\frac{q}{2}\right)\right) \\
&\leq \rho_\sigma(\mathbf{x}) + \left(\frac{q}{2\sigma\sqrt{m}}\,\sqrt{2\pi\mathrm{e}}\,\mathrm{e}^{-\pi\frac{q^2}{m(2\sigma)^2}}\right)^m \rho_\sigma(\mathbb{Z}^m) \quad \text{(by Lemma 2 with } \sigma' = \frac{q}{2\sqrt{m}}\text{)} \\
&\leq \rho_\sigma(\mathbf{x}) + \left(\mathrm{e}^{-\frac{q^2}{m(2\sigma)^2}}\right)^m \rho_\sigma(\mathbb{Z}^m)\ ,
\end{aligned}$$

where the last inequality follows since for every $x \geq 1$, we have $(1-\pi)x^2 \geq \ln x + \ln\sqrt{2\pi\mathrm{e}}$. This gives the first statement. For the other one, we take the square-root of the last inequality above to obtain:

$$\sqrt{\vartheta_{\sigma,q}(\mathbf{x})} \leq \sqrt{\frac{\rho_\sigma(\mathbf{x}) + \mathrm{e}^{-\frac{q^2}{(2\sigma)^2}}\rho_\sigma(\mathbb{Z}^m)}{\rho_\sigma(\mathbb{Z}^m)}} \leq \sqrt{\frac{\rho_\sigma(\mathbf{x})}{\rho_s(\mathbb{Z}^m)}} + \mathrm{e}^{-\frac{q^2}{8\sigma^2}}\ .$$

This completes the proof. □

2.3. **Learning With Errors.** The LWE problem was introduced by [Reg09]. It can be viewed as a distributional variant of the bounded distance decoding problem over Euclidean lattices (see, e.g., the discussion in [SSTX09]).

**Definition 2** (LWE)**.** *Let $m \geq n \geq 1$ and $q \geq 2$ be integers, and $\chi$ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. The parameters $m, n, q$ and $\chi$ are functions of some security parameter $\lambda$. Let $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ be sampled uniformly and $\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$ be sampled from $\chi^{\otimes m}$. The search $\mathsf{LWE}_{m,n,q,\chi}$ problem is to find $\mathbf{s}$ and $\mathbf{e}$ given the pair $(\mathbf{A}, \mathbf{A}\mathbf{s}+\mathbf{e})$. The vectors $\mathbf{s}$ and $\mathbf{e}$ are respectively called the secret and the noise.*

*Whenever $\chi$ is equal to the folded discrete Gaussian distribution $\vartheta_{\sigma,q}$ for some $\sigma > 0$, we overwrite the notation as $\mathsf{LWE}_{m,n,q,\sigma}$.*

For sufficiently small values of $\sigma$, for example $\sigma = O(q^{(m-n)/m}/\sqrt{\lambda})$, one can show that the valid LWE instances are sparse in $(\mathbb{Z}/q\mathbb{Z})^m$: a uniformly sampled vector $\mathbf{b}$ is unlikely a valid LWE instance.

The quantum hardness of the LWE problem for various distributions of the noise and the secret has been extensively studied (see, e.g., [Reg09, GKPV10, MM11, BLP+13, BD20]) and it is known that LWE is no easier than some conjecturally hard worst-case problems [Reg09].

## 3. Witness Obliviousness

In this section, we are interested in the task of sampling an LWE instance $(\mathbf{A}, \mathbf{b})$, given a matrix $\mathbf{A}$. A direct approach (which follows the definition of the LWE problem) is, using a source of randomness, to produce a secret vector $\mathbf{s}$ and a noise vector $\mathbf{e}$ with appropriate distributions, and then to output $\mathbf{b} = \mathbf{A}\mathbf{s}+\mathbf{e}$. This sampler has a particular property: it itself knows the secret $\mathbf{s}$. In a sense, the LWE problem with the vector $\mathbf{b}$ is not hard for the sampler. In that case, we say that an LWE sampler is *witness-aware*. We are interested in samplers that are not witness-aware, i.e., that are *witness-oblivious*.

Below, we discuss instance samplers and knowledge assumptions with a focus on the LWE problem. We start by splitting our discussion about obliviousness between the classical and quantum settings in Subsections 3.1 and 3.2. Furthermore, we show in Subsection 3.3 how to deduce from a given oblivious sampler another one via reductions. Finally, we show in Subsection 3.4 how to design a quantum oblivious sampler for LWE.

3.1. **Classical Setting.** We begin by the definition of a classical $\mathsf{LWE}$ sampler.

**Definition 3** (Classical $\mathsf{LWE}$ Samplers)**.** *Let $m \geq n \geq 1$ and $q \geq 2$ be integers, and $\chi$ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. The parameters $m, n, q, \chi$ are functions of some security parameter $\lambda$. Let $\mathcal{S}$ be a PPT algorithm that has the following specification:*

*$\mathcal{S}(1^\lambda, \mathbf{A}; r)$: Given as input the security parameter $1^\lambda$ (in unary), the matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ and an auxiliary bit string $r$ of size $\mathsf{poly}(\lambda)$, it returns a pair $(\mathbf{A}, \mathbf{b})$ with $\mathbf{b} \in (\mathbb{Z}/q\mathbb{Z})^m$.*

*We say that $\mathcal{S}$ is a classical $\mathsf{LWE}_{m,n,q,\chi}$ sampler if, for a uniformly distributed input matrix $\mathbf{A}$ and a statistically independent random string $r$, the distribution of $\mathcal{S}(1^\lambda, \mathbf{A}; r)$ is within statistical distance $\mathsf{negl}(\lambda)$ from the distribution of $\mathsf{LWE}_{m,n,q,\chi}$ as given in Definition 2.*

As discussed above, some samplers, during their course of execution, might need to produce the witness in order to be successful, namely they are aware of the witness. Assume that we are given the concrete machine that implements the sampler. If we carefully inspect all steps of the machine, the witness must show up at some point (in an easily recoverable way), which allows us to extract it. We grasp this intuition in the following definition.

**Definition 4** (Witness-Oblivious $\mathsf{LWE}$ Samplers)**.** *Let $m, n, q, \chi, \lambda$ as above. We say that a classical $\mathsf{LWE}_{m,n,q,\chi}$ sampler $\mathcal{S}$ is witness-oblivious if for every PPT extractor $\mathcal{E}$, we have*

$$\mathbb{P}\left(\mathbf{s}' = \mathbf{s} \text{ and } \mathbf{e}' = \mathbf{e} \;\middle|\; \begin{array}{l} \mathbf{A} \leftarrow U\left((\mathbb{Z}/q\mathbb{Z})^{m\times n}\right) \\ r \leftarrow U\left(\{0,1\}^{\mathsf{poly}(\lambda)}\right) \\ (\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e}) \leftarrow \mathcal{S}(1^\lambda, \mathbf{A}; r) \\ (\mathbf{s}', \mathbf{e}') \leftarrow \mathcal{E}\left(1^\lambda, \mathbf{A}, \mathbf{b}, r\right) \end{array}\right) \leq \mathsf{negl}(\lambda) \ ,$$

*where the probability is also taken over the randomness of $\mathcal{E}$.*

This definition implies that given $(\mathbf{A}, \mathbf{b})$, finding a witness is hard for all PPT algorithms.

**Lemma 5.** *Let $m, n, q, \chi, \lambda$ as above. Suppose that there exists a classical witness-oblivious $\mathsf{LWE}_{m,n,q,\chi}$ sampler. Then the $\mathsf{LWE}_{m,n,q,\chi}$ problem is hard for every PPT algorithm; for all PPT algorithm $\mathcal{B}$, we have*

$$\mathbb{P}\left(\mathbf{s}' = \mathbf{s} \text{ and } \mathbf{e}' = \mathbf{e} \;\middle|\; \begin{array}{l} (\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e}) \leftarrow \mathsf{LWE}_{m,n,q,\chi} \\ (\mathbf{s}', \mathbf{e}') \leftarrow \mathcal{B}\left(1^\lambda, \mathbf{A}, \mathbf{b}\right) \end{array}\right) \leq \frac{1}{\mathsf{negl}(\lambda)} \ ,$$

*where the probability is also taken over the randomness of $\mathcal{B}$.*

*Proof.* Let $\mathcal{S}$ denote the witness-oblivious sampler and $\mathcal{B}$ be an arbitrary PPT algorithm. By assumption, if given as input a uniformly distributed matrix $\mathbf{A}$, the output distribution of algorithm $\mathcal{S}$ is within statistical distance $\mathsf{negl}(\lambda)$ from the instance distribution of $\mathsf{LWE}_{m,n,q,\chi}$. Therefore, by properties of the statistical distance, we have:

$$\mathbb{P}\left(\mathbf{s}' = \mathbf{s} \text{ and } \mathbf{e}' = \mathbf{e} \;\middle|\; \begin{array}{l} (\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e}) \leftarrow \mathsf{LWE}_{m,n,q,\chi} \\ (\mathbf{s}', \mathbf{e}') \leftarrow \mathcal{B}\left(1^\lambda, \mathbf{A}, \mathbf{b}\right) \end{array}\right) \leq$$
$$\mathbb{P}\left(\mathbf{s}' = \mathbf{s} \text{ and } \mathbf{e}' = \mathbf{e} \;\middle|\; \begin{array}{l} \mathbf{A} \leftarrow U\left((\mathbb{Z}/q\mathbb{Z})^{m\times n}\right) \\ r \leftarrow U\left(\{0,1\}^{\mathsf{poly}(\lambda)}\right) \\ (\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e}) \leftarrow \mathcal{S}(1^\lambda, \mathbf{A}; r) \\ (\mathbf{s}', \mathbf{e}') \leftarrow \mathcal{B}\left(1^\lambda, \mathbf{A}, \mathbf{b}\right) \end{array}\right) + \mathsf{negl}(\lambda) \ .$$

Define the following PPT algorithm $\mathcal{E}$:

$$\mathcal{E}\left(1^\lambda, \mathbf{A}, \mathbf{b}, r\right) := \mathcal{B}(1^\lambda, \mathbf{A}, \mathbf{b}) \ .$$

Therefore, as $\mathcal{S}$ is a classical witness-oblivious sampler, we have

$$\mathbb{P}\left(\mathbf{s}' = \mathbf{s} \text{ and } \mathbf{e}' = \mathbf{e} \;\middle|\; \begin{array}{l} \mathbf{A} \leftarrow U\left((\mathbb{Z}/q\mathbb{Z})^{m\times n}\right) \\ r \leftarrow U(\{0,1\}^{\mathsf{poly}(\lambda)}) \\ (\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e}) \leftarrow \mathcal{S}(1^\lambda, \mathbf{A}; r) \\ (\mathbf{s}', \mathbf{e}') \leftarrow \mathcal{E}\left(1^\lambda, \mathbf{A}, \mathbf{b}, r\right) \end{array}\right) \leq \mathsf{negl}(\lambda) \ ,$$

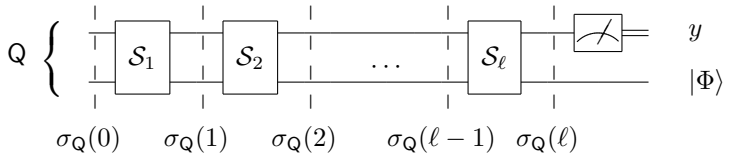


FIGURE 1. The execution of the sampler.

which completes the proof. □

Lemma 5 states that the existence of a witness-oblivious LWE sampler implies the hardness of the LWE problem. We are interested in the converse, i.e., in obtaining an oblivious sampler, under the assumption that LWE is hard.

3.2. **Quantum Setting.** To discuss the post-quantum security of cryptographic schemes, we must migrate to quantum algorithms with appropriate extension of obliviousness. Before going into the details, we need an appropriate definition of quantum samplers.

**Definition 5** (Quantum LWE Samplers)**.** *Let $m \geq n \geq 1$ and $q \geq 2$ be integers, and $\chi$ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. The parameters $m, n, q, \chi$ are functions of some security parameter $\lambda$. Let $\mathcal{S}$ be a QPT algorithm that has the following specification:*

> *$\mathcal{S}\left(1^\lambda, \mathbf{A}, |0\rangle^{\mathsf{poly}(\lambda)}\right)$: Given as input the security parameter $1^\lambda$ (in unary), the matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and a polynomial number of ancillas each initialized to $|0\rangle$ as inputs, it returns a pair $(\mathbf{A}, \mathbf{b})$ with $\mathbf{b} \in (\mathbb{Z}/q\mathbb{Z})^m$.*

*We say that $\mathcal{S}$ is a quantum $\mathsf{LWE}_{m,n,q,\chi}$ sampler if, for a uniformly distributed input matrix $\mathbf{A}$, the distribution of $\mathcal{S}(1^\lambda, \mathbf{A}, |0\rangle^{\mathsf{poly}(\lambda)})$ is within statistical distance $\mathsf{negl}(\lambda)$ from the distribution of $\mathsf{LWE}_{m,n,q,\chi}$ as given in Definition 2.*

The main principle we use to base our obliviousness definition on is that observing or measuring the execution of a machine (be it classical or quantum) must not change the view that the sampler has of itself. Assume that an extractor is observing a sampler. Let $\rho_{\mathsf{Q}\otimes\mathsf{E}}$ represent the joint state of the sampler $\mathcal{S}$ and the extractor $\mathcal{E}$ at some step. The extractor might have carried out particular inspections that ended up in entangling its register with that of the sampler, so the state $\rho_{\mathsf{Q}\otimes\mathsf{E}}$ might not be separable. We intuitively expect from a valid extractor that if we trace out its register, the remaining state must be as if no extractor was inspecting the sampler at all. Namely, if $\rho_{\mathsf{Q}}$ was the state of an isolated sampler at the same step, we require that $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}) = \rho_{\mathsf{Q}}$. We define valid extractors as follows, based on the above discussion, except that we only require that $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}})$ and $\rho_{\mathsf{Q}}$ are close for the trace distance.

**Definition 6.** *Let $\mathsf{Q}$ and $\mathsf{E}$ be two quantum registers initialized to $\tau_{\mathsf{Q}}$ and $\tau_{\mathsf{E}}$ where $\tau_{\mathsf{Q}}$ consists of classical information and ancillas while $\tau_{\mathsf{E}}$ consists of only ancillas. Let $\mathcal{G}$ be the set of one-qubit and two-qubit unitary gates. Let $\mathcal{S}$ be a quantum algorithm operating on register $\mathsf{Q}$ with gates $\mathcal{S}_1, \ldots, \mathcal{S}_\ell$ each of which either belongs to $\mathcal{G}$ or is a measurement in the computational basis. Let $\mathcal{E}$ be a quantum algorithm operating on the joint register $\mathsf{Q}\otimes\mathsf{E}$ with the gates $(\mathcal{E}_{0,j})_{j\leq k(0)}, (\mathcal{E}_{1,j})_{j\leq k(1)}, \ldots, (\mathcal{E}_{\ell+1,j})_{j\leq k(\ell+1)}$ each of which either belongs to $\mathcal{G}$ or is a measurement in the computational basis.*

*In the first scenario, suppose that $\mathcal{S}$ is operating alone on $\mathsf{Q}$. Let $\sigma_{\mathsf{Q}}(i)$ be the density matrix representing the state of $\mathsf{Q}$ just after the $i$-th step of $\mathcal{S}$ for $i \geq 1$ and just before the first step of $\mathcal{S}$ for $i = 0$, as depicted in Figure 1.*

*In the second scenario, suppose that $\mathcal{S}$ and $\mathcal{E}$ are operating jointly on the registers $\mathsf{Q}$ and $\mathsf{E}$ as follows. After the $i$-th step of $\mathcal{S}$ for $i \geq 1$ and before the first step of $\mathcal{S}$ for $i = 0$, algorithm $\mathcal{E}$ is given both registers to perform its operations $(\mathcal{E}_{i,j})_{j\leq k(i)}$ and sends register $\mathsf{Q}$ to $\mathcal{S}$. For every $1 \leq j \leq k(i)$, let $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ denote the joint state of the registers after applying $\mathcal{E}_{i,j}$, and let $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,0)$ denote the state just before applying $\mathcal{E}_i$, as depicted in Figure 2.*

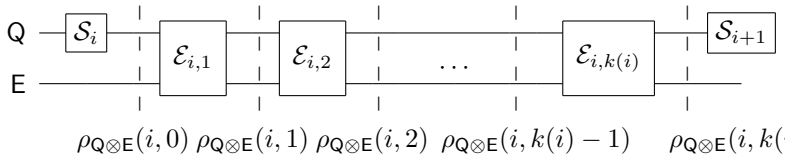


FIGURE 2. The execution of the extractor between Steps $i$ and $i+1$ of the sampler.

*Let $\varepsilon \geq 0$ be a real number. We say that $\mathcal{E}$ is an $\varepsilon$-valid extractor if for every $0 \leq i \leq \ell$ and every $0 \leq j \leq k(i)$, it holds that:*

$$D_{\mathrm{tr}}\left(\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)), \sigma_{\mathsf{Q}}(i)\right) \leq \varepsilon \ . \tag{5}$$

*We say that an extractor is perfect if it is $\varepsilon$-valid for $\varepsilon = 0$. Furthermore, we let $\langle \mathcal{S}, \mathcal{E}\rangle(\tau_{\mathsf{Q}}, \tau_{\mathsf{E}})$ denote the joint output.*

We note that this definition does not assume that $\mathcal{S}$ is a sampler, nor that $\mathcal{S}$ and $\mathcal{E}$ are efficient.

This definition covers all valid extractors in the classical setting. A classical sampler only exploits classical registers. Observing and copying the internal states and the randomness encoded in classical registers is perfectly doable. This translates to the extractor having all the information of internal states and randomness of the sampler. This gives exactly the same information to the extractor as in Definition 4.

**Definition 7** (Witness-Oblivious Quantum Samplers)**.** *Let $m, n, q, \chi, \lambda$ as in Definition 5. We say that a quantum $\mathsf{LWE}_{m,n,q,\chi}$ sampler $\mathcal{S}$ is witness-oblivious if for every $\mathsf{negl}(\lambda)$-valid QPT extractor $\mathcal{E}$, we have*

$$\mathbb{P}\left(\mathbf{s}' = \mathbf{s} \text{ and } \mathbf{e}' = \mathbf{e} \;\middle|\; \begin{array}{l} \mathbf{A} \leftarrow U\left((\mathbb{Z}/q\mathbb{Z})^{m\times n}\right) \\ ((\mathbf{A}, \mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e}), (\mathbf{s}', \mathbf{e}')) \leftarrow \langle \mathcal{S}, \mathcal{E}\rangle\left((1^\lambda, \mathbf{A}, \left|0^{\mathsf{poly}(\lambda)}\right\rangle), \left|0^{\mathsf{poly}(\lambda)}\right\rangle\right) \end{array}\right) \leq \mathsf{negl}(\lambda) \ ,$$

*where the probability is also taken over the measurements of $\mathcal{S}$ and $\mathcal{E}$.*

We note that a statement similar to Lemma 5 holds for quantum witness-oblivious samplers.

**Relation to the definition from [LMZ23].** The authors of [LMZ23] adopted a different approach to define valid extractors. Their definition only deals with unitary algorithms followed by a single final measurement. The sampler is first executed until it performs its final measurement, and then the remaining working register and the measurement outcome are handed over to the extractor. The extractor is not allowed to inspect or observe the sampler during its execution. Using the notations of Figure 1, a valid extractor, in their case, is only given the classical output $y$, and the quantum output $|\Phi\rangle$.

**Definition 8** (Adapted from[LMZ23])**.** *Let $\mathcal{S}$ be a unitary algorithm with a pure initial state and some classical string as input. Assume that $\mathcal{S}$ performs a final measurement in the computational basis over part of its register. A quantum algorithm $\mathcal{E}$ is said to be an LMZ extractor for $\mathcal{S}$ if it operates as follows: in the first phase, the sampler runs its circuit and outputs $|y, \Phi\rangle$ where $y$ is classical and $|\Phi\rangle$ is quantum; in the second phase, the circuit of the extractor runs over $|y, \Phi\rangle$, and possibly extra ancillas, and outputs a classical string.*

We stress that in the definition above, the extractor is not allowed to engage in the first phase: it proceeds *after* the sampler. We show in the following lemma that, when restricted to unitary algorithms with a pure initial state, our definition of perfect extractor is equivalent to the one from [LMZ23].

**Lemma 6.** *Let $\mathsf{Q}$ be a quantum register initialized with some classical string $z$ and with the pure state $|0\rangle_{\mathsf{Q}}$. Let $\mathsf{E}$ be a quantum register with pure initial states $|0\rangle_{\mathsf{E}}$. Let $\mathcal{S}$ be a quantum algorithm operating on $\mathsf{Q}$ by a series of unitary gates followed by a single measurement. Let $\mathcal{E}$ be a QPT*

*$\varepsilon$-valid extractor operating on two registers $\mathsf{Q}$ and $\mathsf{E}$ as per Definition 6. Then, there exists an LMZ extractor $\mathcal{E}'$ (as per Definition 8) that is QPT, and*

$$D_{\mathrm{tr}}\Big(\langle \mathcal{S}, \mathcal{E}\rangle\left((z, |0\rangle_{\mathsf{Q}}), |0\rangle_{\mathsf{E}}\right) \ , \ \mathcal{E}'\left(\mathcal{S}\left(z, |0\rangle_{\mathsf{Q}}\right)\right)\Big) \leq 2\sqrt{2\varepsilon} \ .$$

**Remark 1.** *In the case of quantum* LWE *samplers, the classical string $z$ will be $1^\lambda$ and $\mathbf{A}$.*

**Lemma 7.** *Using notations of Lemma 6, for any $(i,j)$, it holds that*

$$D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j), \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i,j)}\left(|0\rangle\right)\right) \leq 2\sqrt{2\varepsilon} \ ,$$

*where $\mathcal{E}'_{(i,j)}$ is a QPT algorithm given as input a quantum state $|0\rangle$, and implicitly the description of $\mathcal{S}$ and $\mathcal{E}$ as well as the classical string $z$.*

*Proof.* Let us first prove the statement for the perfect-case, i.e., $\varepsilon = 0$. We prove it by induction on $i$. Suppose that the statement holds for $(i-1) \geq 0$ (it clearly holds for $i = 0$ as at this step neither $\mathcal{S}$ nor $\mathcal{E}$ performs any computations). In particular, we have

$$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i-1, k(i-1)) = \sigma_{\mathsf{Q}}(i-1)\otimes\mathcal{E}'_{(i-1,k(i-1))}(|0\rangle) \ .$$

The statement holds for $(i,0)$ by definition, namely,

$$\begin{aligned}\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,0) &= \mathcal{S}_i\sigma_{\mathsf{Q}}(i-1)\otimes\mathcal{E}'_{(i-1,k(i-1))}(|0\rangle)\\ &= \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i-1,k(i-1))}(|0\rangle) \ .\end{aligned}$$

Note that $\mathcal{E}$ is a perfect extractor, therefore according to Definition 6, we have

$$\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)) = \sigma_{\mathsf{Q}}(i) \ .$$

The state $\sigma_{\mathsf{Q}}(i)$ is pure since $\mathcal{S}$ only applies unitaries to $\mathsf{Q}$ which initially contains the pure quantum state $|0\rangle_{\mathsf{Q}}$. Therefore, according to the above equality, $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ is a produce state. Furthermore, it is necessarily given by

$$\sigma_{\mathsf{Q}}(i)\otimes\rho_{\mathsf{E}} \ ,$$

where $\rho_{\mathsf{E}}$ is the quantum state obtained after applying $\mathcal{E}_{i,1},\ldots,\mathcal{E}_{i,j}$ as in Figure 2 on

$$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,0) = \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i-1,k(i-1))}(|0\rangle) \ ,$$

and then tracing out $\mathsf{Q}$. On one hand, $\sigma_{\mathsf{Q}}(i)$ can be computed via $i$ steps of $\mathcal{S}$ given the classical string $z$ and the quantum state $|0\rangle_{\mathsf{Q}}$ where no measurement are performed. Therefore, given the description of $\mathcal{S}$, we can compute a polynomial time unitary $\mathbf{U}$ (the sampler $\mathcal{S}$ is QPT) such that $\sigma_{\mathsf{Q}}(i) = \mathbf{U}|0\rangle$. On the other hand, the quantum state $\rho_{\mathsf{E}\otimes\mathsf{Q}}(i,j)$ is equal, by definition, to

$$\begin{aligned}\rho_{\mathsf{E}\otimes\mathsf{Q}}(i,j) &= \mathcal{E}_{i,j}\ldots\mathcal{E}_{i,1}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,0)\right)\\ &= \mathcal{E}_{i,j}\ldots\mathcal{E}_{i,1}\left(\sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i-1,k(i-1))}(|0\rangle)\right)\\ &= \mathcal{E}_{i,j}\ldots\mathcal{E}_{i,1}\left(\mathbf{U}|0\rangle_{\mathsf{Q}}\otimes\mathcal{E}'_{(i-1,k(i-1))}(|0\rangle)\right) \ .\end{aligned}$$

The algorithm $\mathcal{E}'_{(i,j)}$ computes the above state and then it traces out its first register $\mathsf{Q}$, namely it keeps only the second register $\mathsf{E}$. It shows that the lemma holds when $\varepsilon = 0$ for any $i$ and any $0 \leq j \leq k(i)$. It concludes the proof by induction in this case.

Now suppose that $\varepsilon > 0$. Let us consider the same algorithm $\mathcal{E}'_{(i,j)}$ as above. However, in this case (when keeping the second register) it is not true anymore that, $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j) = \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i,j)}(|0\rangle)$. Indeed, $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j))$ is not a pure state, therefore $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ is not a product state. To handle this case, let us introduce the fidelity $F(\cdot,\cdot)$ between quantum states, i.e., for all quantum states $\rho$ and $\sigma$

$$F(\rho,\sigma) := \mathrm{tr}\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}} \ .$$

By Uhlmann's theorem [NC11, Th. 9.14, Exercise 9.15], there exists some purifications $|\varphi\rangle$ and $|\psi\rangle$ of $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j))$ and $\sigma_{\mathsf{Q}}(i)$, respectively, such that

$$F(\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)), \sigma_{\mathsf{Q}}(i)) = |\langle\varphi|\psi\rangle| \ . \tag{6}$$

Note that by definition: $\mathrm{tr}_{\mathsf{E}}(|\psi\rangle\langle\psi|) = \sigma_{\mathsf{Q}}(i)$ which is a pure state. Therefore $|\psi\rangle$ is a product state, in particular

$$|\psi\rangle = \sigma_{\mathsf{Q}}(i) \otimes \rho \ .$$

By Fuchs-van de Graaf inequalities, [NC11, Eq. 9.110], it holds that

$$\begin{aligned} F(\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)), \sigma_{\mathsf{Q}}(i)) &\geq 1 - D_{\mathrm{tr}}(\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)), \sigma_{\mathsf{Q}}(i)) \\ &\geq 1 - \varepsilon \ . \end{aligned}$$

Therefore, by using Equation (6), we have

$$|\langle\varphi|\psi\rangle| \geq 1 - \varepsilon$$

which implies that

$$D_{\mathrm{tr}}\left(|\varphi\rangle, |\psi\rangle\right) \leq \sqrt{1-(1-\varepsilon)^2} \leq \sqrt{2\varepsilon} \ .$$

The above inequality holds for any purification $|\varphi\rangle$ of $\mathrm{tr}_{\mathsf{E}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)\right)$, in particular for $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ (without loss of generality we can suppose that it is a pure quantum after some purification), namely,

$$D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j), |\psi\rangle\right) \leq \sqrt{1-(1-\varepsilon)^2} \leq \sqrt{2\varepsilon} \ . \tag{7}$$

Recall now that $|\psi\rangle = \sigma_{\mathsf{Q}}(i)\otimes\rho$. In its last step, algorithm $\mathcal{E}'_{(i,j)}(|0\rangle)$ keeps only the second register $\mathsf{E}$ of $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ (it traces out its first register $\mathsf{Q}$). Therefore, by properties of the trace distance,

$$D_{\mathrm{tr}}\left(\rho, \mathcal{E}'_{(i,j)}(|0\rangle)\right) \leq \sqrt{2\varepsilon} \ . \tag{8}$$

By using the triangular inequality,

$$\begin{aligned} D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j), \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i,j)}\left(|0\rangle\right)\right) &\leq D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j), |\psi\rangle\right) + D_{\mathrm{tr}}\left(|\psi\rangle, \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i,j)}\left(|0\rangle\right)\right) \\ &= D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j), |\psi\rangle\right) + D_{\mathrm{tr}}\left(\sigma_{\mathsf{Q}}(i)\otimes\rho, \sigma_{\mathsf{Q}}(i)\otimes\mathcal{E}'_{(i,j)}\left(|0\rangle\right)\right) \\ &= D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j), |\psi\rangle\right) + D_{\mathrm{tr}}\left(\rho, \otimes\mathcal{E}'_{(i,j)}\left(|0\rangle\right)\right) \\ &\leq 2\sqrt{2\varepsilon} \end{aligned}$$

where we used Equations (7) and (8). This completes the proof. □

*Proof of Lemma 6.* Let $\ell$ be the number of steps of the sampler $\mathcal{S}$. Recall that after the $\ell$-th step, the sampler $\mathcal{S}$ measures part of the register $\mathsf{Q}$. According to Lemma 6, we have

$$D_{\mathrm{tr}}\left(\rho_{\mathsf{Q}\otimes\mathsf{E}}(\ell, k(\ell)), \sigma_{\mathsf{Q}}(\ell)\otimes\mathcal{E}'_{\ell,k(\ell)}\left(|0\rangle\right)\right) \leq 2\sqrt{2\varepsilon} \ ,$$

where $\mathcal{E}'_{\ell,k(\ell)}$ is a QPT algorithm that only needs the description of $\mathcal{S}$, $\mathcal{E}$, and the knowledge of the classical string $z$ to run. Therefore, after performing the measurement of $\mathcal{S}$ on $\sigma_{\mathsf{Q}}(\ell)\otimes\mathcal{E}'_{\ell,k(\ell)}\left(|0\rangle\right)$, the post-measurement state is within trace distance $\leq 2\sqrt{2\varepsilon}$ from the post-measurement state after applying the same measurement on $\rho_{\mathsf{Q}\otimes\mathsf{E}}(\ell, k(\ell))$. Let the former be

$$|y, \Phi\rangle \otimes \mathcal{E}'_{\ell,k(\ell)}\left(|0\rangle\right) \ ,$$

where $y$ is classical. To build an LMZ extractor, it suffices to remove the interaction between $\mathcal{E}$ and $\mathcal{S}$. We first run $\mathcal{S}$ once and let it perform its measurement to obtain $|y, \Phi\rangle$. Then, we let $\mathcal{E}$ perform its last steps over $|y, \Phi\rangle \otimes \mathcal{E}'_{\ell,k(\ell)}\left(|0\rangle\right)$. Note that this defines an LMZ extractor since $\mathcal{E}'_{\ell,k(\ell)}\left(|0\rangle\right)$ can be computed in polynomial time and independent of $(i)$ the execution of $\mathcal{S}$ and $(ii)$ its measurement output.

□

3.3. **Obliviousness and black-box reductions.** All definitions of this subsection can be extended to the general class of *distributional problems* as well. Recall that a distributional problem P is a pair $(\mathrm{R}, \mathrm{D})$ where R is an $\mathsf{NP}$ relation and $\mathrm{D} = \{\mathrm{D}_\lambda\}_\lambda$ is a polynomially sampleable ensemble over the instances of R. The problem P asks for finding a witness for an instance that has been sampled according to D. We note that the search $\mathsf{LWE}$ problem belongs to this class.

**Definition 9** (Quantum Samplers)**.** *Let $\lambda$ be the security parameter. Let $\mathrm{P} = (\mathrm{R}, \mathrm{D})$ be a distributional problem. Let $\mathcal{S}$ be a QPT algorithm that has the following specification:*

> *$\mathcal{S}\left(1^\lambda, \tilde{x}, |0\rangle^{\mathsf{poly}(\lambda)}\right)$: Given the parameter $1^\lambda$, a string $\tilde{x}$, and a polynomial number of ancillas initialized to $|0\rangle$ as inputs, it returns a string $x$ of size $\mathsf{poly}(\lambda)$ that has $\tilde{x}$ as a prefix.*

*We say that $\mathcal{S}$ is a quantum* P *sampler if there exists a probability distribution $\{\widetilde{D}_\lambda\}_\lambda$ such that for $\tilde{x}$ sampled from $\widetilde{D}_\lambda$, the distribution of $\mathcal{S}\left(1^\lambda, \tilde{x}, |0\rangle^{\mathsf{poly}(\lambda)}\right)$ is within statistical distance $\mathsf{negl}(\lambda)$ from $\mathrm{D}_\lambda$.*

One can define witness-oblivious samplers by adapting Definition 7. We are interested in preservation of witness-obliviousness under reductions. We begin by recalling the definition of reductions with respect to distributional problems.

**Definition 10.** *A distributional problem $\mathrm{P}_1 = (\mathrm{R}_1, \mathrm{D}_1)$ is randomized Karp-reducible to $\mathrm{P}_2 = (\mathrm{R}_2, \mathrm{D}_2)$ if there exists:*

- *a PPT algorithm $\mathcal{A}$ that maps instances of $\mathrm{P}_1$ to instances of $\mathrm{P}_2$ such that $\mathcal{A}(\mathrm{D}_1)$ is within negligible statistical distance from $\mathrm{D}_2$ over the randomness of $\mathcal{A}$,*
- *a PPT or QPT algorithm $\mathcal{B}$ for $\mathcal{A}$ such that*

$$\forall x_1, y_2 : (\mathcal{A}(x_1; r), y_2) \in \mathrm{R}_2 \implies (x_1, \mathcal{B}(x_1, y_2, r)) \in \mathrm{R}_1 \ ,$$

  *with non-negligible probability over the randomness of $\mathcal{B}$. Note that $\mathcal{B}$ has the randomness $r$ of $\mathcal{A}$ as part of its input (and can use extra randomness).*

The following theorem states that witness-obliviousness is preserved under randomized Karp reductions.

**Lemma 8.** *Let $\mathrm{P}_1$ and $\mathrm{P}_2$ be two distributional problems. Assume that $\mathrm{P}_1$ is randomized Karp-reducible to $\mathrm{P}_2$ with the associated algorithms $\mathcal{A}$ and $\mathcal{B}$. If $\mathcal{S}$ is a quantum witness-oblivious $\mathrm{P}_1$ sampler, then $\mathcal{A}(\mathcal{S})$ is a quantum witness-oblivious $\mathrm{P}_2$ sampler.*

*Proof.* Let $x_1 \leftarrow \mathcal{S}$ and $x_2 \leftarrow \mathcal{A}(x_1; r)$. Suppose that there exists a valid QPT extractor $\mathcal{E}_2$ that finds a witness $y_2$ for the instance $x_2$. One can build a new extractor $\mathcal{E}_1$ for $\mathcal{S}$ as follows. To find a witness for $x_1$, the new extractor $(i)$ collects the randomness $r$ of $\mathcal{A}$, $(ii)$ finds the witness $y_2$ for $x_2$ using $\mathcal{E}_2$, and then $(iii)$ applies $\mathcal{B}(x_1, y_2, r)$. The output of $\mathcal{B}$ is a witness for $x_1$ according to the definition of the randomized Karp reduction. It suffices to note that $\mathcal{B}$ is indeed a valid extractor for $\mathcal{Q}$. □

Note that the $\mathrm{P}_2$ sampler is witness-oblivious under the hardness assumption of $\mathrm{P}_1$. Many classical reductions in the context of lattice problems fall into the above framework.

3.4. **Reducing oblivious $\mathsf{LWE}$ sampling to $|\mathsf{LWE}\rangle$.** We complete this section by providing a general approach to design a quantum witness oblivious sampler via a single unitary and a final measurement. We show that producing $\mathsf{LWE}$ samples in an oblivious manner reduces to synthesizing a quantum state that is a superposition of all $\mathsf{LWE}$ samples, as defined in [CLZ22]. This state synthesis problem is called the $|\mathsf{LWE}\rangle$ problem.

**Definition 11** ($|\mathsf{LWE}\rangle$ State)**.** *Let $m \geq n \geq 1$ and $q \geq 2$ be integers, and $f$ be an amplitude function whose domain is $\mathbb{Z}/q\mathbb{Z}$. The parameters $m, n, q, f$ are functions of some security parameter $\lambda$.*

*For* $\mathbf{A} = (\mathbf{a}_1 | \dots | \mathbf{a}_m)^\mathsf{T} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$*, the* $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ *state is defined as*

$$|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} := \frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^{m} f(e_i) \, |\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q\rangle \ ,$$

*where* $Z_f(\mathbf{A})$ *is the normalization scalar such that* $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ *becomes a unit vector.*

*To simplify notation, when it is clear from the context, we will drop the dependency on* $m, n, q, f$*, and the matrix* $\mathbf{A}$*.*

The normalization term $Z_f(\mathbf{A})$, which guarantees that $|\mathsf{LWE}\rangle$ is a *valid* quantum state, will play an important role. In particular, we will require that $Z_f(\mathbf{A}) \approx q^n$. We will discuss this matter in detail in Section 5, when instantiating our algorithm to the case where $|f|^2$, i.e., the noise distribution of the measured $\mathsf{LWE}$ sample, is a Gaussian distribution.

Constructing this state was studied in [CLZ22] in order to solve the *Short Integer Solution* ($\mathsf{SIS}$) problem with some specific parameters. We note that [CLZ22] neglected the normalization factor $Z_f(\mathbf{A})$ by assuming that it is always equal to $q^n$, see for example [CLZ22, Def. 9 & Cor. 9]. In the general problem of constructing an $|\mathsf{LWE}\rangle$ state, one should take the normalization into account. For instance, it was shown in [DRT23] that this normalization factor should be handled with care when $|f|^2$ concentrates the error weight close to the minimum distance of the spanned linear code.

We also stress that [CLZ22, Def. 9] only allows non-negative real-valued amplitude functions, while we allow complex-valued ones. Although we only use real-valued (but not positive) instantiations of the amplitude function in this work since they are sufficient for our purposes, more choices of the function might have further applications.

**Definition 12** ($|\mathsf{LWE}\rangle$ Problem)**.** *Let* $m, n, q, f, \lambda$ *as in Definition 11. The* $|\mathsf{LWE}\rangle_{m,n,q,f}$ *problem is as follows: given as input a matrix* $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$*, the goal is to build the* $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ *state. More formally, we say that a QPT algorithm* $\mathcal{S}$ *solves* $|\mathsf{LWE}\rangle_{m,n,q,f}$ *if there exists* $M \le \mathsf{poly}(\lambda)$ *such that given* $1^\lambda$*, a uniform* $\mathbf{A}$ *and* $|0\rangle^{m\log q} |0\rangle^M$ *as inputs, algorithm* $\mathcal{S}$ *builds a state within trace distance* $\mathsf{negl}(\lambda)$ *from* $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle^M$*, with probability* $1 - \mathsf{negl}(\lambda)$ *over the randomness of* $\mathbf{A}$ *and its measurements.*

Notice that measuring the $|\mathsf{LWE}\rangle$ state gives the following $m$ $\mathsf{LWE}$-samples:

$$((\mathbf{a}_1, \langle \mathbf{a}_1, \mathbf{s}\rangle + e_1 \bmod q), \dots, (\mathbf{a}_m, \langle \mathbf{a}_m, \mathbf{s}\rangle + e_m \bmod q)) \ ,$$

where the $e_i$'s are i.i.d. with distribution $|f|^2$, while $\mathbf{s}$ is uniform and independent.

In the following theorem, we show that solving $|\mathsf{LWE}\rangle$ using a unitary algorithm provides a witness-oblivious $\mathsf{LWE}$ sampler by measuring the final superposition. We stress that the result holds even if the $|\mathsf{LWE}\rangle$ solver only provides a state that is only approximately equal (in trace distance) to $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle^M$.

**Theorem 2.** *Let* $m, n, q, f, \lambda$ *as in Definition 11. Assume that there exists a unitary QPT algorithm* $\mathcal{S}$ *that solves* $|\mathsf{LWE}\rangle_{m,n,q,f}$ *for some* $M \le \mathsf{poly}(\lambda)$ *number of auxiliary ancillas as input. Then* $\mathcal{S}$ *followed by a measurement in the computational basis is a witness-oblivious quantum* $\mathsf{LWE}_{m,n,q,|f|^2}$ *sampler, assuming the quantum hardness of* $\mathsf{LWE}_{m,n,q,|f|^2}$*.*

*Proof.* Let $\mathsf{Q} = \mathsf{C} \otimes \mathsf{W}$ be the register of $\mathcal{S}$ such that the final measurement is performed upon $\mathsf{C}$ to obtain the classical output and $\mathsf{W}$ is the remaining register. Let $|\psi\rangle$ be the final state of the algorithm $\mathcal{S}$ over $\mathsf{Q}$, right before the measurement. With probability $1 - \mathsf{negl}(\lambda)$ over the uniform choice of $\mathbf{A}$, we have:

$$D_{\mathrm{tr}}\left(|\psi\rangle \, , \ |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle^M\right) \le \mathsf{negl}(\lambda) \ . \tag{9}$$

After applying the measurement, the state $|\psi\rangle$ becomes a mixed state as follows:

$$\sigma_{\mathcal{S}} := \sum_{\mathbf{b}\in(\mathbb{Z}/q\mathbb{Z})^m} p_{\mathbf{b}} \, |\mathbf{b}\rangle\langle\mathbf{b}| \otimes |\phi_{\mathbf{b}}\rangle\langle\phi_{\mathbf{b}}| \ ,$$

where $p_{\mathbf{b}}$ is the probability of observing $\mathbf{b}$ as the outcome, and $|\phi_{\mathbf{b}}\rangle$ is the corresponding state in the working space. After the measurement, the other state becomes:

$$\sigma_{\mathsf{LWE}} := \sum_{\mathbf{b}\in(\mathbb{Z}/q\mathbb{Z})^m} q_{\mathbf{b}} \, |\mathbf{b}\rangle\langle\mathbf{b}| \otimes |\mathbf{0}\rangle\langle\mathbf{0}| \ ,$$

where $\{q_{\mathbf{b}}\}_{\mathbf{b}}$ is the induced distribution of $\mathsf{LWE}_{m,n,q,|f|^2}$ over its support, namely

$$q_{\mathbf{b}} = \mathbb{P}_{\mathbf{s},\mathbf{e}} \left(\mathbf{A}\mathbf{s} + \mathbf{e} = \mathbf{b}\right) \ , \tag{10}$$

where $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ is picked uniformly at random and the $e_i$'s are i.i.d. with distribution $|f|^2$. Using the properties of trace distance, we obtain for a proportion $1 - \mathsf{negl}(\lambda)$ of matrices $\mathbf{A}$:

$$\begin{aligned} D_{\mathrm{tr}}\left(\sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}}\right) &\leq D_{\mathrm{tr}}\left(|\psi\rangle \, , \ |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} \otimes |0\rangle^M\right) \\ &\leq \mathsf{negl}(\lambda) \ , \end{aligned} \tag{11}$$

where in the last line we used Equation (9). Using now Equation (4), we obtain for a proportion $1-\mathsf{negl}(\lambda)$ of matrices $\mathbf{A}$:

$$\Delta\left(\{p_{\mathbf{b}}\}_{\mathbf{b}}, \{q_{\mathbf{b}}\}_{\mathbf{b}}\right) \leq \mathsf{negl}(\lambda) \ .$$

This proves, by using Equation (10), that the sampler $\mathcal{S}$ is a quantum $\mathsf{LWE}$ sampler as stated in Definition 5.

Let us now show that $\mathcal{S}$ followed be a single measurement is a *witness-oblivious* quantum sampler as stated in Definition 7. By assumption, the sampler $\mathcal{S}$ is a unitary algorithm. We first consider the case where the extractor $\mathcal{E}$ is perfect, i.e., $\varepsilon = 0$ in Lemma 6. Therefore, we can suppose that the input of $\mathcal{E}$ is $\sigma_{\mathcal{S}}$.

Suppose that $\mathcal{E}$ is instead given $\sigma_{\mathsf{LWE}}$, namely $|\mathbf{b}\rangle\,|0\rangle^M$ with $\mathbf{b} := \mathbf{A}\mathbf{s} + \mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$ such that it has been picked according to $q_{\mathbf{b}}$ given in Equation (10). In that case, for a uniform choice of matrices $\mathbf{A}$, its probability to output $(\mathbf{s}', \mathbf{e}')$ such that $\mathbf{s}' = \mathbf{s}$ and $\mathbf{e}' = \mathbf{e}$ is $\mathsf{negl}(\lambda)$ as we assumed the quantum hardness of $\mathsf{LWE}_{m,n,q,|f|^2}$. However the extractor is given $\sigma_{\mathcal{S}}$. Using the properties of the trace distance, it holds that for a proportion $1 - \mathsf{negl}(\lambda)$ of matrices $\mathbf{A}$:

$$\begin{aligned} D_{\mathrm{tr}}\Big(\mathcal{E}\left(\sigma_{\mathcal{S}}\right), \mathcal{E}\Big(\sigma_{\mathsf{LWE}}\Big)\Big) &\leq D_{\mathrm{tr}}(\sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}}) \\ &\leq \mathsf{negl}(\lambda) \ . \end{aligned}$$

where in the last line we used Equation (11). This completes the proof in the perfect case, i.e., $\varepsilon = 0$.

Now, suppose that $\mathcal{E}$ is $\mathsf{negl}(\lambda)$-valid extractor. According to Lemma 6, it is given a quantum state a trace distance $2\sqrt{2\mathsf{negl}(\lambda)} = \mathsf{negl}(\lambda)$ from $\sigma_{\mathcal{S}}$. To conclude the proof we proceed as above. □

As a direct application of Theorem 2 and Lemma 8, we obtain that a unitary solver for $|\mathsf{LWE}\rangle_{m,n,q,f}$ gives an witness-oblivious quantum $\mathsf{LWE}_{m',n,q,|f|^2}$ sampler for any integer $m' \in [n, m]$. Indeed, throwing away the superfluous coordinates is a Karp reduction.

## 4. An algorithm for $|\mathsf{LWE}\rangle$

In Subsection 3.4, we have shown that witness-oblivious sampling reduces to the $|\mathsf{LWE}\rangle$ problem (Definition 12). Solving this problem consists in building the $|\mathsf{LWE}\rangle$ state (as per Definition 11). This state is an $m$-fold tensor product where each element corresponds to a single $\mathsf{LWE}$-sample $\langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q$. Like in [CLZ22], our approach to solve the $|\mathsf{LWE}\rangle$ problem singles out each of these elements, analyzes them independently, and finally recombines the results.

**Definition 13** (Coordinate States)**.** *Let $q \geq 2$ and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be an amplitude function. We define the coordinate states as follows:*

$$\forall j \in \mathbb{Z}/q\mathbb{Z}, \quad |\psi_j\rangle := \sum_{e=0}^{q-1} f\left(e\right) |j + e \bmod q\rangle \ .$$

4.1. **Description of the algorithm.** Before going into the details, we briefly explain how our algorithm solves the $|\mathsf{LWE}\rangle$ problem for some arbitrary amplitude function $f$. It proceeds in three general phases that would ideally work as follows.

**Phase A.** First, it builds the following entangled state

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} f^{\otimes m}(\mathbf{e}) \,|\mathbf{s}\rangle\,|\mathbf{A}\mathbf{s}+\mathbf{e}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{j=1}^{m} \left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle \ . \tag{12}$$

The efficiency of this step depends on the specific choice of $f$.

**Phase B.** For each $j$ in parallel, it recovers $\langle \mathbf{a}_j, \mathbf{s}\rangle$ from $\left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle$ with some probability $p$ (independent from $j$). If it fails, the outcome could be thought as special symbol $\perp$. This operation is not allowed to "perturb" $\left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle$: it has to be reversible. We handle this by applying some polynomial-time unitary that maps $\left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle$ to the state

$$\sqrt{p}\,|\langle \mathbf{a}_j, \mathbf{s}\rangle\rangle\,|0\rangle + \sqrt{1-p}\,|a\rangle\,|1\rangle \ ,$$

for some $|a\rangle$ which does not play any role. We interpret any quantum state whose last qubit is $|1\rangle$ as $\perp$. The quality of that step is quantified by the success probability $p$.

**Phase C.** Using the successful coordinates, the algorithm collects some linear equations $\langle \mathbf{a}_j, \mathbf{s}\rangle$ (for known $\mathbf{a}_j$'s). The next step is to recompute $\mathbf{s}$ by Gaussian elimination. This allows to erase it from the content of the first register, i.e., disentangling the state in Equation (12) and solving the $|\mathsf{LWE}\rangle$ problem. However, note that Phase B only enables to recover each $\langle \mathbf{a}_j, \mathbf{s}\rangle$ with some probability $p$. Therefore our approach will work if the number of non-$\perp$ coordinates is no smaller than $n$ in order to expect to have a non-singular linear system to solve, namely if $m = (n + \log\log q)/p \cdot \omega(\log\lambda)$. Therefore, the success probability $p$ considered at Phase B has to be sufficiently large for the purpose of efficiency.

Combining the steps above, one obtains Algorithm 1. Steps 1 to 4 of Algorithm 1 correspond to Phase A above, Steps 5 and 6 correspond to Phase B above, and Steps 7 and 8 correspond to Phase C above.

More details are required to make Steps 2, 6 and 7 explicit. For Step 2, we assume that we can efficiently implement an approximation of the state (see Condition 1 of Theorem 3). A realization for a specific amplitude function $f$ will be discussed in Lemma 17. Step 6 relies on a unitary $\mathbf{V}$ satisfying:

$$\forall x \in \mathbb{Z}/q\mathbb{Z} : \mathbf{V}\left(|\chi_x\rangle\,|0\rangle\right) = |\chi_x\rangle \left(u_x\,|0\rangle + \sqrt{1-|u_x|^2}\,|1\rangle\right) \ , \tag{13}$$

where $u_x$ is an approximation of $(\min|\widehat{f}|)/\widehat{f}(-x)$ (see Condition 2 of Theorem 3). We will explain in Lemma 14 how to implement $\mathbf{V}$. Note that up to the numerical inaccuracy, the unitary $\mathbf{V}$ can be viewed as an implementation of the unambiguous measurement from [CB98] (see Appendix A). Step 7 uses a version of a Gaussian elimination algorithm $\mathcal{A}_{\mathrm{GE}}$ that works as follows when given as input a matrix $\mathbf{A} := (\mathbf{a}_1|\ldots|\mathbf{a}_m)^{\mathsf{T}} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ and $m$ equations $(y_i)_{1\le i\le m}$ where $y_i = \langle \mathbf{a}_i, \mathbf{s}\rangle$ or $y_i = \perp$ (some equations may be erased): it first tests whether the input matrix $\mathbf{A}$ is invertible modulo $q$ (which is not required to be prime); if it is, it then outputs the unique solution $\mathbf{s}$; if it is not, it outputs $\perp$. Algorithm $\mathcal{A}_{\mathrm{GE}}$ is deterministic polynomial-time and has the following properties that will prove useful in our analysis of Algorithm 1:

- it is unambiguous, in the sense that it never outputs an incorrect solution, i.e., it either outputs the valid $\mathbf{s}$ or it fails and outputs $\perp$;
- if $\mathbf{A}$ is sampled uniformly, and the number of non-$\perp$ input $y_i$'s is $(n+\log\log q)\omega(\log\lambda)$ and the indices of the non-$\perp$ input $y_i$'s are chosen independently from $\mathbf{A}$, then $\mathcal{A}_{\mathrm{GE}}$ returns $\perp$ with probability $\mathsf{negl}(\lambda)$ (this can be obtained, e.g., by adapting [BLP+13, Claim 2.13]);

**Algorithm 1** Quantum $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ Solver.

**Parameters:** $m, n, q$ and $f$.
**Input:** $\mathbf{A} := (\mathbf{a}_1|\dots|\mathbf{a}_m)^\intercal \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$.
**Output:** A quantum state $|\varphi\rangle$.

1: Build the state $\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle$.
2: Build the state $\sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^m f(e_i)\,|e_i\rangle$.
3: Consider the joint state of Steps 1 and 2 to get

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^m f(e_i)\,|e_i\rangle \ .$$

4: Apply the quantum unitary $|\mathbf{s},\mathbf{e}\rangle \mapsto |\mathbf{s}, \langle\mathbf{a}_1,\mathbf{s}\rangle + e_1, \dots, \langle\mathbf{a}_m,\mathbf{s}\rangle + e_m\rangle$ to get

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^m f(e_i)\,|\langle\mathbf{a}_i,\mathbf{s}\rangle + e_i\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^m \left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle \ .$$

5: Append one ancilla $|0\rangle$.
6: Apply the unitary $\mathbf{I}\otimes\mathbf{V}^{\otimes m}$ with $\mathbf{V}$ as defined in Equation (13), to obtain

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^m \mathbf{V}\left(\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |0\rangle\right) \ .$$

7: Apply the quantum unambiguous Gaussian elimination as given in Equation (14) to get

$$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}} \left( \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^m \mathbf{V}\left(\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |0\rangle\right) \right) \ .$$

8: Apply $\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}$ and output the resulting quantum state.

- for any fixed $\mathbf{A}$, if the indices of the non-$\perp$ $y_i$'s are chosen randomly and independently from the rest, then the success probability is the same for every $(\mathbf{s}\in\mathbb{Z}/q\mathbb{Z})^n$.

In Algorithm 1, we consider a version of the Gaussian elimination $\mathcal{A}_{\mathrm{GE}}$ that is quantized as follows. For any $(\mathbf{s},\mathbf{x},\mathbf{b}) \in (\mathbb{Z}/q\mathbb{Z})^n \times (\mathbb{Z}/q\mathbb{Z})^m \times \{0,1\}^m$,

$$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}} : |\mathbf{s}\rangle \bigotimes_{i=1}^m |x_i, b_i\rangle \longmapsto \left|\mathbf{s} - \mathcal{A}_{\mathrm{GE}}(\mathbf{A}, (y_i)_{1\le i\le m})\right\rangle \bigotimes_{i=1}^m |x_i, b_i\rangle \ . \tag{14}$$

where $y_i = x_i$ if $b_i = 0$, and $y_i = \perp$ otherwise. To handle the potential output $\perp$ of $\mathcal{A}_{\mathrm{GE}}$, we embed the first quantum register in Equation (14) into $\mathbb{C}^{2q}$ where $(|x\rangle, |\perp\rangle_x)_{x\in\mathbb{Z}/q\mathbb{Z}}$ is the computational basis (for some arbitrary symbols $\perp_x$).

The following theorem gives conditions under which Algorithm 1 solves the $|\mathsf{LWE}\rangle$ problem in time $\mathsf{poly}(\lambda)$.

**Theorem 3.** *Let $m \ge n \ge 1$ and $q \ge 2$ be integers, and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be an amplitude function. The parameters $m, n, q, f$ are functions of some security parameter $\lambda$ with $m, \log q \le \mathsf{poly}(\lambda)$. Assume that the following conditions hold:*

1. *there exists a $\mathsf{poly}(\lambda)$-time algorithm that builds a state within $\mathsf{negl}(\lambda)$ trace distance of the state $\sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e)\,|e\rangle$;*
2. *there exists a $\mathsf{poly}(\lambda)$-time algorithm that, given $x$ as input, outputs $u_x := (\min|\widehat{f}|)/\widehat{f}(-x) + e_{\mathrm{apx}}(x)$ on $\mathsf{poly}(\lambda)$ bits with $\max_x |e_{\mathrm{apx}}(x)| = \mathsf{negl}(\lambda)/\sqrt{q^n}$;*

3. *we have that* $m = (n + \log\log q)/p \cdot \omega(\log\lambda)$, *where* $p := q \cdot \min |\widehat{f}|^2$;
4. *assuming that* $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ *is uniformly distributed, we have*

$$\mathbb{P}_{\mathbf{A}}\left(\left|\frac{Z_f(\mathbf{A})}{q^n} - 1\right| \geq \mathsf{negl}(\lambda)\right) = \mathsf{negl}(\lambda) \ ,$$

*where* $Z_f(\mathbf{A})$ *is the normalization scalar such that* $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ *becomes a unit vector, as per Definition 11.*

*Then Algorithm 1 runs in time* $\mathsf{poly}(\lambda)$ *and, for a proportion* $1 - \mathsf{negl}(\lambda)$ *of matrices* $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, *it outputs a quantum state* $|\varphi\rangle$ *such that*

$$D_{\mathrm{tr}}\left(|\varphi\rangle, |\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle\right) = \mathsf{negl}(\lambda) \ . \tag{15}$$

The first two conditions enable an efficient implementation of Algorithm 1. In Condition 3, the value $p$ refers to the success probability in recovering $j$ from $|\psi_j\rangle$. This condition ensures that $m$ is sufficiently large for the unambiguous Gaussian elimination algorithm to succeed with probability $1 - \mathsf{negl}(\lambda)$. Note that the condition on $m$ and the fact that $m \leq \mathsf{poly}(\lambda)$ imply that we must have $p \geq 1/\mathsf{poly}(\lambda)$. The latter implies that $\widehat{f}(x)$ is non-zero for all $x \in \mathbb{Z}/q\mathbb{Z}$, a condition that is necessary to rely on the measurement from [CB98] and, more concretely, for the unitary $\mathbf{V}$ used in Step 6 of Algorithm 1 to be well-defined (see Condition 3). Still concerning Condition 3, the lower bound on $m$ is to ensure that a uniform $m \times n$ matrix modulo $q$ has an image of size $(\mathbb{Z}/q\mathbb{Z})^n$ with overwhelming probability. If $q$ is prime, this condition can be simplified to $m = n/p \cdot \omega(\log\lambda)$. Finally, Condition 4 intuitively states that the parametrization of $\mathsf{LWE}$ provides a unique solution with overwhelming probability. The last two conditions can be simplified if $q$ is assumed to be prime.

We will first consider the correctness of Algorithm 1 (Lemma 13), and then analyze its runtime (Lemma 15).

4.2. **Correctness.** The purpose of the unitary $\mathbf{V}$ (introduced in Equation (13)) is to recover $\langle \mathbf{a}_i, \mathbf{s}\rangle$ from $|\psi_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\rangle$. More formally, we have the following lemma.

**Lemma 9.** *Using notations of Theorem 3 and with* $\mathbf{V}$ *as defined in Equation (13), we have*

$$\forall j \in \mathbb{Z}/q\mathbb{Z},\ \mathbf{V}\left(|\psi_j\rangle |0\rangle\right) = \sqrt{p}\,|j\rangle |0\rangle + \sqrt{1-p}\,|\eta_j\rangle |1\rangle + |\mathrm{error}_j\rangle \ ,$$

*for some quantum states* $|\eta_j\rangle$ *and* $|\mathrm{error}_j\rangle$ *with* $\max_j \| |\mathrm{error}_j\rangle \| = \mathsf{negl}(\lambda)/\sqrt{q^n}$.

*Proof.* Let us write the $|\psi_j\rangle$'s (Definition 13) in the Fourier basis $(|\chi_x\rangle)_{x\in\mathbb{Z}/q\mathbb{Z}}$. We have, for all $j \in \mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned}
|\psi_j\rangle &= \sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e)\,|j+e \bmod q\rangle \\
&= \frac{1}{\sqrt{q}} \sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e) \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-(j+e)x} |\chi_x\rangle \qquad \text{(by Lemma 1)} \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \left(\frac{1}{\sqrt{q}} \sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e)\,\omega_q^{-xe}\right) \omega_q^{-jx} |\chi_x\rangle \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x)\,\omega_q^{-jx} |\chi_x\rangle \ .
\end{aligned}$$

Therefore, by linearity and definition of $\mathbf{V}$, we have:

$$\begin{aligned}\mathbf{V}\left(|\psi_j\rangle\,|0\rangle\right) &= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x)\omega_q^{-jx}\,\mathbf{V}\left(|\chi_x\rangle\,|0\rangle\right)\\ &= \underbrace{\left(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} u_x\,\widehat{f}(-x)\,\omega_q^{-jx}\,|\chi_x\rangle\right)}_{:=|\psi_{j,0}\rangle}|0\rangle + \underbrace{\left(\sum_{x\in\mathbb{Z}/q\mathbb{Z}} \sqrt{1-|u_x|^2}\,\widehat{f}(-x)\,\omega_q^{-jx}\,|\chi_x\rangle\right)}_{:=|\psi_{j,1}\rangle}|1\rangle\ .\end{aligned}$$

Let us consider $|\psi_{j,0}\rangle$. By definition of $u_x$ and $p$, we have:

$$|\psi_{j,0}\rangle = \underbrace{\sqrt{q}\cdot\min|\widehat{f}|\ \left(\frac{1}{\sqrt{q}}\sum_{x\in\mathbb{Z}/q\mathbb{Z}}\omega_q^{-jx}\,|\chi_x\rangle\right)}_{=\sqrt{p}|j\rangle} + \underbrace{\sum_{x\in\mathbb{Z}/q\mathbb{Z}} e_{\mathrm{apx}}(x)\widehat{f}(-x)\omega_q^{-jx}\,|\chi_x\rangle}_{:=|\mathrm{error}_{j,0}\rangle}\ .$$

Notice that:

$$\|\,|\mathrm{error}\rangle_{j,0}\,\|^2 = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} e_{\mathrm{apx}}(x)^2\,|\widehat{f}(-x)|^2 \le \left(\max_{x\in\mathbb{Z}/q\mathbb{Z}}|e_{\mathrm{apx}}(x)|\right)^2\ .$$

Hence, so far, we have:

$$\mathbf{V}\left(|\psi_j\rangle\,|0\rangle\right) = \sqrt{p}\,|j\rangle\,|0\rangle + |\mathrm{error}_{j,0}\rangle\,|0\rangle + |\psi_{j,1}\rangle\,|1\rangle\ , \tag{16}$$

where $\|\,|\mathrm{error}_{j,0}\rangle\,\| = \mathsf{negl}(\lambda)/\sqrt{q^n}$, by assumption on $\max_x|e_{\mathrm{apx}}(x)|$. Notice that $\mathbf{V}(|\psi_j\rangle\,|0\rangle)$ is a quantum state as $\mathbf{V}$ is unitary. Therefore, we can write

$$|\psi_{j,1}\rangle = \sqrt{1-p}\,|\eta_j\rangle + |\mathrm{error}_{j,1}\rangle\ ,$$

for some quantum states $|\eta_j\rangle$ and $|\mathrm{error}_{j,1}\rangle$ such that $\|\,|\mathrm{error}_{j,1}\rangle\,\| = \mathsf{negl}(\lambda)/\sqrt{q^n}$. Plugging this into Equation (16) gives the result. □

As can be seen from Lemma 9, the transformation $\mathbf{V}$ introduces an error term. It basically comes from the fact that we only assume that we can approximate $(\min|\widehat{f}|)/\widehat{f}(-x)$ (as opposed to exactly computing it). This seems necessary for our subsequent choice of $f$. Ideally, we would analyze the correctness of Algorithm 1 as if we were applying a unitary $\mathbf{W}$ (that we do not know how to implement efficiently) such that

$$\forall j\in\mathbb{Z}/q\mathbb{Z},\quad \mathbf{W}\left(|\psi_j\rangle\,|0\rangle\right) = \sqrt{p}\,|j\rangle\,|0\rangle + \sqrt{1-p}\,|\eta_j\rangle\,|1\rangle\ ,$$

The value $\langle\mathbf{a}_i,\mathbf{s}\rangle$ appears (in superposition) in the first register of $\mathbf{W}(|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\rangle\,|0\rangle)$, for all $i\le m$. Therefore, applying the unitary $\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}$ as in Step 7 to the quantum state

$$\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{s}\rangle\bigotimes_{i=1}^{m}\mathbf{W}\left(|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\rangle\,|0\rangle\right)$$

will allow us to erase $\mathbf{s}$ from the first register. More precisely, we hope that after Step 7, the quantum state

$$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{s}\rangle\bigotimes_{i=1}^{m}\mathbf{W}\,|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\rangle\,|0\rangle\right)$$

will be "close" to the disentangled state

$$\frac{1}{\sqrt{Z_f(\mathbf{A})}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{0}\rangle\bigotimes_{i=1}^{m}\mathbf{W}\,|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\rangle\,|0\rangle\,.$$

Notice now that applying $\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}$, as in Step 8, to the state above does not yield the quantum state $|\mathbf{0}\rangle\,|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}\,|0\rangle$. Instead, this would hold if we were rather applying $\mathbf{I}\otimes\left(\mathbf{W}^\dagger\right)^{\otimes m}$. But we do not know how to implement $\mathbf{W}$ efficiently. In the following two lemmas we show that

applying $\mathbf{V}$ and $\mathbf{V}^\dagger$ lead to quantum states that are close for the trace distance to the case where we would instead apply $\mathbf{W}$ and $\mathbf{W}^\dagger$.

**Lemma 10.** *Using notations of Theorem 3 and letting*

$$|\varphi'\rangle := \left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{s}\rangle\bigotimes_{i=1}^{m}\left(\sqrt{p}\,|\langle\mathbf{a}_i,\mathbf{s}\rangle\rangle\,|0\rangle+\sqrt{1-p}\,\left|\eta_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|1\rangle\right)\right)\quad,\quad(17)$$

*we have*

$$D_{\mathrm{tr}}\left(|\varphi\rangle\,,|\varphi'\rangle\right)=\frac{\mathsf{negl}(\lambda)}{q^{n/4}}\ .$$

*Proof.* Recall that $|\varphi\rangle$ is obtained at the end of Step 8 of Algorithm 1. In particular, we have, thanks to Lemma 9,

$$\begin{aligned}|\varphi\rangle&=\left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{s}\rangle\bigotimes_{i=1}^{m}\mathbf{V}\left(\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|0\rangle\right)\right)\\&=\left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{s}\rangle\bigotimes_{i=1}^{m}\left(\sqrt{p}\,|\langle\mathbf{a}_i,\mathbf{s}\rangle\rangle\,|0\rangle+\sqrt{1-p}\,\left|\eta_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|1\rangle\right.\right.\\&\qquad\left.\left.+\left|\mathrm{error}_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle\right)\right)\ .\end{aligned}$$

Taking the Hermitian product, we obtain:

$$\langle\varphi'|\varphi\rangle=\frac{1}{q^n}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}\prod_{i=1}^{m}\left(1+\sqrt{p}\left\langle\langle\mathbf{a}_i,\mathbf{s}\rangle,0\middle|\mathrm{error}_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle+\sqrt{1-p}\left\langle\eta_{\langle\mathbf{a}_i,\mathbf{s}\rangle},1\middle|\mathrm{error}_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle\right)\ .$$

As $\max_j\left\|\,|\mathrm{error}_j\rangle\,\right\|=\mathsf{negl}(\lambda)/\sqrt{q^n}$, we have that

$$\langle\varphi'|\varphi\rangle=q^{-n}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}\prod_{i\leq m}(1+z_{\mathbf{s},i})$$

for some $z_{\mathbf{s},i}\in\mathbb{C}$ satisfying $\max_{\mathbf{s},i}|z_{\mathbf{s},i}|\leq\mathsf{negl}(\lambda)/\sqrt{q^n}$. Using the fact that $m\leq\mathsf{poly}(\lambda)$, we obtain that $\langle\varphi'|\varphi\rangle=1-\mathsf{negl}(\lambda)/\sqrt{q^n}$. □

**Lemma 11.** *Using notations of Theorem 3 and letting*

$$|\psi'\rangle:=\left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\left(\frac{1}{\sqrt{Z_f(\mathbf{A})}}\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n}|\mathbf{0}\rangle\bigotimes_{i=1}^{m}\left(\sqrt{p}\,|\langle\mathbf{a}_i,\mathbf{s}\rangle\rangle\,|0\rangle+\sqrt{1-p}\,\left|\eta_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|1\rangle\right)\right)\quad(18)$$

*we have*

$$D_{\mathrm{tr}}\left(|\psi'\rangle\,,|\mathbf{0}\rangle\,|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}\,|0\rangle\right)\leq\sqrt{1-\left(1-\sqrt{\frac{q^n}{Z_f(\mathbf{A})}}\,\mathsf{negl}(\lambda)\right)^2}\ .$$

*Proof.* By Definition 11, we have

$$\begin{aligned}
|\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle &= \frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{0}\rangle \bigotimes_{i=1}^{m} \left|\psi_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |0\rangle \\
&= \left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\left(\frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{0}\rangle \bigotimes_{i=1}^{m} \mathbf{V}\left(\left|\psi_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |0\rangle\right)\right) \\
&= \left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\left(\frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{0}\rangle \bigotimes_{i=1}^{m} \left(\sqrt{p}\,|\langle \mathbf{a}_i,\mathbf{s}\rangle\rangle |0\rangle \right.\right. \\
&\qquad \left.\left. + \sqrt{1-p}\left|\eta_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |1\rangle + \left|\mathrm{error}_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle\right)\right) .
\end{aligned}$$

Recall that $\max_j \| |\mathrm{error}_j\rangle \| = \mathsf{negl}(\lambda)/\sqrt{q^n}$ (see Lemma 9). Therefore, we have

$$|\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle = |\psi'\rangle + \left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\left(\frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{0}\rangle |\mathrm{error}_{\mathbf{s}}\rangle\right) ,$$

for some $\mathrm{error}_{\mathbf{s}}$ satisfying $\max_{\mathbf{s}} \| |\mathrm{error}_{\mathbf{s}}\rangle \| \leq m\ \mathsf{negl}(\lambda)/\sqrt{q^n} \leq \mathsf{negl}(\lambda)/\sqrt{q^n}$, since $m = \mathsf{poly}(\lambda)$. We hence obtain that

$$\left\| \left(\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}\right)\left(\frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |0\rangle |\mathrm{error}_{\mathbf{s}}\rangle\right) \right\| \leq \frac{q^n}{\sqrt{Z_f(\mathbf{A})}} \frac{\mathsf{negl}(\lambda)}{\sqrt{q^n}} = \sqrt{\frac{q^n}{Z_f(\mathbf{A})}}\mathsf{negl}(\lambda) ,$$

which completes the proof. □

The following lemma will help us in analyzing the effect of the unitary $\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}$. It considers its application on a state whose second and third registers contain a superposition of solved and undetermined linear equations. It is obtained from (14) by linearity and the fact that $y_i$ in Equation (14) depends only in the last qubit.

**Lemma 12.** *Let $\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}$ be defined as in Equation (14). Let $x_1,\ldots,x_m \in \mathbb{Z}/q\mathbb{Z}$ and $|\eta_1\rangle,\ldots,|\eta_m\rangle$ be some quantum states. We have*

$$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(|\mathbf{s}\rangle \bigotimes_{i=1}^{m}\left(\sqrt{p}\,|x_i\rangle |0\rangle + \sqrt{1-p}\,|\eta_i\rangle |1\rangle\right)\right) = \sum_{\mathbf{y}\in\{x_i,\perp\}^m} |\mathbf{s}-\mathcal{A}_{\mathrm{GE}}(\mathbf{A},\mathbf{y})\rangle \bigotimes_{i=1}^{m} \lambda(y_i)\left|\alpha_{y_i}^{\mathbf{s}}\right\rangle ,$$

*where*

$$\left|\alpha_{y_i}^{\mathbf{s}}\right\rangle := \begin{cases} |x_i\rangle |0\rangle & \text{if } y_i = x_i \\ |\eta_i\rangle |1\rangle & \text{otherwise} \end{cases} \quad \text{and} \quad \lambda(y_i) := \begin{cases} \sqrt{p} & \text{if } y_i = x_i \\ \sqrt{1-p} & \text{otherwise} \end{cases} .$$

We can now show the correctness of Algorithm 1, i.e., that Equation (15) holds.

**Lemma 13.** *Using the notations of Theorem 3, we have, for a proportion $1-\mathsf{negl}(\lambda)$ of matrices $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$:*

$$D_{\mathrm{tr}}\left(|\varphi\rangle, |\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle\right) = \mathsf{negl}(\lambda) .$$

*Proof.* First, by Condition 1 of Theorem 3, we can build the quantum state $\sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e)\,|e\rangle$ up to a trace distance $\mathsf{negl}(\lambda)$. Therefore, when analyzing the trace distance between the output $|\varphi\rangle$ of Algorithm 1 and $|\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle$, we can assume that it is exactly $\sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{j=1}^{m} f(e)\,|e_i\rangle$ that is built at Step 2. Indeed, this only affects the trace distance by an additive $m\mathsf{negl}(\lambda) = \mathsf{negl}(\lambda)$ term (recall that we have $m \leq \mathsf{poly}(\lambda)$).

By Lemmas 10 and 11, and the triangular inequality over the trace distance, we have

$$\begin{aligned} D_{\mathrm{tr}}\Big( |\varphi\rangle, |\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle \Big) \\ &\leq D_{\mathrm{tr}}\left(|\varphi\rangle, |\varphi'\rangle\right) + D_{\mathrm{tr}}\left(|\varphi'\rangle, |\psi'\rangle\right) + D_{\mathrm{tr}}\left(|\psi'\rangle, |\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle\right) \\ &\leq D_{\mathrm{tr}}\left(|\varphi'\rangle, |\psi'\rangle\right) + \frac{\mathsf{negl}(\lambda)}{q^{n/4}} + \sqrt{1 - \left(1 - \frac{q^n}{Z_f(\mathbf{A})}\mathsf{negl}(\lambda)\right)^2} \end{aligned} \tag{19}$$

where $|\varphi'\rangle$ and $|\psi'\rangle$ are respectively defined in Equations (17) and (18). Applying the unitary $\mathbf{I} \otimes \left(\mathbf{V}^\dagger\right)^{\otimes m}$ does not change the trace distance. Therefore, by using the definitions of $|\varphi'\rangle$ and $|\psi'\rangle$, we have

$$D_{\mathrm{tr}}\left(|\varphi'\rangle, |\psi'\rangle\right) = D_{\mathrm{tr}}\left(|\psi\rangle, |\psi_{\mathrm{ideal}}\rangle\right) \tag{20}$$

where

$$|\psi\rangle := \mathbf{U}_{\mathcal{A}_{\mathrm{GE}}} \left( \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \left( \sqrt{p}\,|\langle \mathbf{a}_i, \mathbf{s}\rangle\rangle\,|0\rangle + \sqrt{1-p}\,\left|\eta_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |1\rangle \right) \right)$$

and

$$|\psi_{\mathrm{ideal}}\rangle := \frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{0}\rangle \bigotimes_{i=1}^{m} \left( \sqrt{p}\,|\langle \mathbf{a}_i, \mathbf{s}\rangle\rangle\,|0\rangle + \sqrt{1-p}\,\left|\eta_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |1\rangle \right) .$$

By Lemma 12, we have

$$|\psi\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{y}\in\{\langle \mathbf{a}_i,\mathbf{s}\rangle,\perp\}^m} |\mathbf{s} - \mathcal{A}_{\mathrm{GE}}(\mathbf{A},\mathbf{y})\rangle \bigotimes_{i=1}^{m} \lambda(y_i) \left|\alpha^{\mathbf{s}}_{y_i}\right\rangle$$

where,

$$\left|\alpha^{\mathbf{s}}_{y_i}\right\rangle := \begin{cases} |\langle \mathbf{a}_i,\mathbf{s}\rangle\rangle\,|0\rangle & \text{if } y_i = \langle \mathbf{a}_i,\mathbf{s}\rangle \\ \left|\eta_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |1\rangle & \text{otherwise} \end{cases} \quad \text{and} \quad \lambda(y_i) := \begin{cases} \sqrt{p} & \text{if } y_i = \langle \mathbf{a}_i,\mathbf{s}\rangle \\ \sqrt{1-p} & \text{otherwise} \end{cases} . \tag{21}$$

Similarly, we have

$$|\psi_{\mathrm{ideal}}\rangle = \frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{y}\in\{\langle \mathbf{a}_i,\mathbf{s}\rangle,\perp\}^m} |\mathbf{0}\rangle \bigotimes_{i=1}^{m} \lambda(y_i) \left|\alpha^{\mathbf{s}}_{y_i}\right\rangle .$$

We deduce that

$$\langle\psi_{\mathrm{ideal}}|\psi\rangle = \frac{1}{\sqrt{q^n\ Z_f(\mathbf{A})}} \sum_{\mathbf{s},\mathbf{s}'\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{y}\in\{\langle \mathbf{a}_i,\mathbf{s}\rangle,\perp\}^m} \sum_{\mathbf{y}'\in\{\langle \mathbf{a}_i,\mathbf{s}'\rangle,\perp\}^m} \underbrace{\langle\mathbf{0}|\mathbf{s}' - \mathcal{A}_{\mathrm{GE}}(\mathbf{A},\mathbf{y}')\rangle \prod_{i=1}^{m} \lambda(y_i)\lambda(y'_i) \left\langle \alpha^{\mathbf{s}}_{y_i} \middle| \alpha^{\mathbf{s}'}_{y'_i} \right\rangle}_{:=P_{\mathbf{s},\mathbf{s}',\mathbf{y},\mathbf{y}'}} .$$

Our aim is to show that $P_{\mathbf{s},\mathbf{s}',\mathbf{y},\mathbf{y}'}$ is always equal to 0 except when $\mathbf{s} = \mathbf{s}'$ and $\mathbf{y} = \mathbf{y}'$. First, notice that $P_{\mathbf{s},\mathbf{s}',\mathbf{y},\mathbf{y}'}$ can be non-zero only if the following holds

$$\mathbf{s}' = \mathcal{A}_{\mathrm{GE}}(\mathbf{A},\mathbf{y}') .$$

At this stage, recall that our Gaussian elimination algorithm $\mathcal{A}_{\mathrm{GE}}$ is unambiguous: with the knowledge of $\mathbf{y}'$, it can only output $\mathbf{s}'$ of $\perp$ (but not output another vector). Further, to have $P_{\mathbf{s},\mathbf{s}',\mathbf{y},\mathbf{y}'} \neq 0$, we also need

$$\forall i : \left\langle \alpha^{\mathbf{s}}_{y_i} \middle| \alpha^{\mathbf{s}'}_{y'_i} \right\rangle \neq 0 .$$

Therefore, by definition of the $\left|\alpha^{\mathbf{s}}_{y_i}\right\rangle$'s in Equation (21), it is necessary that for all $i$, we have $y_i = y'_i$. However, the $y'_i$'s uniquely determine $\mathbf{s}'$, therefore $\mathbf{s} = \mathbf{s}'$ in that case. Overall, we obtain that $P_{\mathbf{s},\mathbf{s}',\mathbf{y},\mathbf{y}'} \neq 0$ implies that $\mathbf{s} = \mathbf{s}'$ and $\mathbf{y} = \mathbf{y}'$. Therefore, we obtain

$$\begin{aligned}\langle\psi_{\text{ideal}}|\psi\rangle &= \frac{1}{\sqrt{Z_f(\mathbf{A})\, q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\substack{\mathbf{y}\in(\{\langle\mathbf{a}_j,\mathbf{s}\rangle,\,\perp\})_{j=1}^m:\\ \mathbf{s}=\mathcal{A}_{\mathrm{GE}}(\mathbf{A},\mathbf{y})}} \prod_{i=1}^m \lambda(y_i)^2 \\ &= \sqrt{\frac{q^n}{Z_f(\mathbf{A})}}\, p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A})\ , \end{aligned} \tag{22}$$

where $p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A})$ is the success probability of $\mathcal{A}_{\mathrm{GE}}$ when each of its $m$ equations as input is $\perp$ with probability $1-p$ and $\langle\mathbf{a}_i,\mathbf{s}\rangle$, with probability $p$ (recall that $p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A})$ is independent from $\mathbf{s}$). Now, by Condition 3 of Theorem 3, we have $m = (n+\log\log q)/p \cdot \omega(\log\lambda)$. Therefore, by assumption on algorithm $\mathcal{A}_{\mathrm{GE}}$, except for a $\mathsf{negl}(\lambda)$-proportion of matrices $\mathbf{A}$, we have

$$p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}) = 1 - \mathsf{negl}(\lambda)\ .$$

By using Equations (19), (20) and (22), we deduce that for a proportion $1-\mathsf{negl}(\lambda)$ of matrices $\mathbf{A}$, we have

$$\begin{aligned} D_{\mathrm{tr}}\left(|\varphi\rangle, |\mathbf{0}\rangle\,|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}\,|0\rangle\right) \leq{}& \sqrt{1-\frac{q^n}{Z_f(\mathbf{A})}(1-\mathsf{negl}(\lambda))^2} \\ &+ \frac{\mathsf{negl}(\lambda)}{q^{n/4}} + \sqrt{1-\left(1-\sqrt{\frac{q^n}{Z_f(\mathbf{A})}}\,\mathsf{negl}(\lambda)\right)^2}\ . \end{aligned}$$

To complete the proof, it suffices to use Condition 4 of Theorem 3. □

4.3. **Run-time.** We now focus on the run-time of Algorithm 1. So far, we did not specify how to compute the unitary $\mathbf{V}$. This is the focus of the following lemma.

**Lemma 14.** *Using notations of Theorem 3, we can evaluate a unitary* $\mathbf{V}$ *satisfying Equation* (13) *in time* $\mathsf{poly}(\lambda)$.

*Proof.* Our objective is to implement $\mathbf{V}$ such that

$$\forall x\in\mathbb{Z}/q\mathbb{Z} : \mathbf{V}\left(|\chi_x\rangle\,|0\rangle\right) = |\chi_x\rangle\left(u_x\,|0\rangle + \sqrt{1-|u_x|^2}\,|1\rangle\right)\ .$$

By Condition 2 of Theorem 3, we can efficiently compute $u_x = (\min|\widehat{f}|)/\widehat{f}(-x) + e_{\mathrm{apx}}(x) \in \mathbb{C}$ on $\mathsf{poly}(\lambda)$ bits with $\max_x|e_{\mathrm{apx}}(x)| = \mathsf{negl}(\lambda)/\sqrt{q^n}$. Without loss of generality, we assume that $u_x$ is written as its magnitude and phase $(m_x,\theta_x)$ where $m_x$ and $\theta_x$ have $b = \mathsf{poly}(\lambda)$ bits. As $x\mapsto u_x$ is computable in time $\mathsf{poly}(\lambda)$, we can evaluate a unitary $\mathbf{O}_u$ satisfying the following, in quantum-time $\mathsf{poly}(\lambda)$:

$$\forall x : \mathbf{O}_u\left(|x\rangle\left|0^{2b}\right\rangle\right) = |x\rangle\,|m_x\rangle\,|\theta_x\rangle\ .$$

Now, consider the following two unitaries:

$$\begin{aligned}\mathbf{M} &:= \sum_{y\in\{0,1\}^b} |y\rangle\langle y| \otimes \mathbf{I}_p \otimes \left(\widetilde{y}\,|0\rangle + \sqrt{1-\widetilde{y}^2}\,|1\rangle\right)\langle 0|\ , \\ \mathbf{\Theta} &:= \sum_{z\in\{0,1\}^b} \mathbf{I}_b \otimes |z\rangle\langle z| \otimes \left(\mathrm{e}^{2\pi i\widetilde{z}}\,|0\rangle\langle 0| + |1\rangle\langle 1|\right)\ ,\end{aligned}$$

where $\widetilde{y} = \sum_{i=1}^b y_i/2^i$ and $\widetilde{z} = \sum_{i=1}^b z_i/2^i$. It can be checked that

$$\mathbf{O}_u^\dagger\mathbf{\Theta}\mathbf{M}\mathbf{O}_u\left(|x\rangle\left|0^{2b}\right\rangle|0\rangle\right) = |x\rangle\left|0^{2b}\right\rangle\left(u_x\,|0\rangle + \sqrt{1-|u_x|^2}\,|1\rangle\right)\ .$$

The unitary $\mathbf{M}$ can be implemented with $O(b) = \mathsf{poly}(\lambda)$ unary and binary gates [dW23, Ch. 9, Exercise 7.a]. Furthermore, we have

$$\mathrm{e}^{2\pi i \widetilde{z}} = \prod_{k=1}^{b} \mathrm{e}^{2\pi i 2^{-k} z_k} \ .$$

It shows that one only requires $b = \mathsf{poly}(\lambda)$ controlled gates to implement $\mathbf{\Theta}$. This completes the proof. □

We are now ready to prove that we can run Algorithm 1 in polynomial time.

**Lemma 15.** *Using notations of Theorem 3, Algorithm 1 can be executed in time* $\mathsf{poly}(\lambda)$.

*Proof.* Step 2 of Algorithm 1 can be executed in time $\mathsf{poly}(\lambda)$ by Condition 1 of Theorem 3. All steps except Steps 6, 7 and 8 are readily seen to be computable in time $\mathsf{poly}(\lambda)$ as $m, \log q \leq \mathsf{poly}(\lambda)$. By Lemma 14, Steps 6 and 8 can be executed in time $m\ \mathsf{poly}(\lambda) = \mathsf{poly}(\lambda)$. Finally, Step 7 applies $\mathbf{U}_{\mathrm{GE}}$. This unitary quantizes a $\mathsf{poly}(\lambda)$-time Gaussian elimination algorithm. □

## 5. $|\mathsf{LWE}\rangle$ for the Gaussian distribution and witness-oblivious LWE sampling

Our aim in this section is to construct a witness-oblivious quantum $\mathsf{LWE}_{m,n,q,|f|^2}$ sampler. For this purpose, we use Algorithm 1 with a specific choice of parameter $f$, to obtain the following theorem. The second part of the statement below is obtained by combining the first part and Theorem 2. This proves Theorem 1.

**Theorem 4.** *Let $m \geq n \geq 1$ and $q \geq 3$ be integers and $\sigma \geq 2$ be a real number. The parameters $m, n, q, \sigma$ are functions of the security parameter $\lambda$ with $m, \log q \leq \mathsf{poly}(\lambda)$ and $q$ prime. Assume that the parameters satisfy the following conditions:*

$$m \geq n\sigma \cdot \omega(\log \lambda) \quad \text{and} \quad 2 \leq \sigma \leq \frac{q}{\sqrt{8m \ln q}} \ .$$

*Furthermore, let $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be such that*

$$f(x) := \begin{cases} \sqrt{\vartheta_{\sigma,q}(x)} & \text{if } 0 \leq x \leq \frac{q}{2} \\ -\sqrt{\vartheta_{\sigma,q}(x)} & \text{otherwise} \end{cases} \ .$$

*Then Algorithm 1 runs in time $\mathsf{poly}(\lambda)$ and, for a proportion $1 - \mathsf{negl}(\lambda)$ of matrices $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m \times n}$, it outputs a quantum state $|\varphi\rangle$ such that $D_{\mathrm{tr}}(|\varphi\rangle, |\mathbf{0}\rangle |\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} |0\rangle) = \mathsf{negl}(\lambda)$.*

*In particular, if $\mathsf{LWE}_{m,n,q,\sigma}$ is quantumly hard, then there exists a $\mathsf{poly}(\lambda)$-time quantum witness-oblivious $\mathsf{LWE}_{m,n,q,\sigma}$ sampler.*

Note that Theorem 1 puts some constraints on the arithmetic shape of the modulus $q$, on the number of samples $m$, and on the standard deviation parameter $\sigma$. It would be convenient to allow smaller values of $m$, arbitrary arithmetic shapes for $q$ and superpolynomial values of $\sigma$. Indeed, these are frequent parametrizations of $\mathsf{LWE}$. To reach such values, we can use randomized Karp reductions from $\mathsf{LWE}$ for some parameters to $\mathsf{LWE}$ for other parameters. For instance, we can use Theorem 4 with many samples, and just throw away the superfluous ones. We may also use Theorem 4 with some permitted parameters $n, \sigma, q$ for which $\mathsf{LWE}$ is hard, and then perform modulus-switching or modulus-dimension switching [BLP+13]. As an example, using modulus switching and throwing away superfluous samples, we obtain the following corollary.

**Corollary 1.** *Let $m \geq n \geq 1$ and $q \geq 2$ be integers and $\sigma \geq 2$ be a real number. The parameters $m, n, q, \sigma$ are functions of the security parameter $\lambda$ with $m, \sigma, \log q \leq \mathsf{poly}(\lambda)$. Assume that $\mathsf{LWE}_{m',n,q',\sigma'}$ is hard, where $q' \leq 2q$ is the smallest prime larger than $q$, $\sigma' = \sigma/(n+\lambda) \cdot \Omega_\lambda(1)$ and $m' = \max(m, n\sigma' \cdot \omega(\log \lambda))$. If $2 \leq \sigma' \leq q'/\sqrt{8m' \ln q'}$, then there exists a witness-oblivious $\mathsf{LWE}_{m,n,q,\sigma}$ sampler.*

To prove Theorem 4, we show that the conditions of Theorem 3 are fulfilled for the amplitude function of Theorem 4. This is the purpose of the rest of this section.

5.1. **On Conditions 1 and 2 of Theorem 3.** In the lemmas below, we show that $f$ and $\widehat{f}$ can be approximated with sufficient precision for Conditions 1 and 2 to apply.

**Lemma 16.** *Let $n \geq 1$, $q \geq 3$ integers, $\sigma > 0$ a real number and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ as in Theorem 4. Assume that $n, \sigma = \mathsf{poly}(\lambda)$ and $q = 2^{\mathsf{poly}(\lambda)}$ is odd, where $\lambda$ is security parameter. Then we can compute $u_x = (\min|\widehat{f}|)/\widehat{f}(-x) + e_{\mathrm{apx}}(x)$ on $\mathsf{poly}(\lambda)$ bits with $\max_x |e_{\mathrm{apx}}(x)| = \mathsf{negl}(\lambda)/\sqrt{q^n}$, in classical time $\mathsf{poly}(\lambda)$.*

*Proof.* We show how to approximate $\widehat{f}(x)$ for every $x$ within appropriate accuracy. This also suffices to approximate $\min|\widehat{f}|$ because, by Lemma 19, we have $\min|\widehat{f}| = |\widehat{f}(0)|$. As seen in the proof of Lemma 19, we have, for all $y \in \mathbb{Z}/q\mathbb{Z}$:

$$\widehat{f}(y) = \frac{f(0)}{\sqrt{q}} + i\,\frac{2}{\sqrt{q}} \sum_{x \in \mathbb{Z} \cap (0, q/2)} f(x)\,\sin\frac{2\pi x y}{q}\ .$$

First, note that one can efficiently approximate $f(x)$ on $\mathsf{poly}(\lambda)$ bits and within an absolute error $\mathsf{negl}(\lambda)/\sqrt{q^n}$, by relying on the Gaussian tail bound and summing $\mathsf{poly}(\lambda)$ terms (as $\sigma = \mathsf{poly}(\lambda)$). The quantities $\sin(2\pi xy/q)$ can be similarly approximated, using the Taylor approximation of sin up to degree $\mathsf{poly}(\lambda)$. To approximate $\widehat{f}(y)$, we claim that it suffices to compute the summation above for the summands $x \in \{1, 2, \ldots, \mathsf{poly}(\lambda)\}$. We use the tail bound for the Gaussian distribution. Let $C := \mathsf{poly}(\lambda)\frac{n}{2}\log q \leq \mathsf{poly}(\lambda)$. We have, for all $y \in \mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned}
\left|\sum_{x \in \mathbb{Z} \cap (C, q/2)} \sqrt{\vartheta_{\sigma,q}(x)}\,\sin\frac{2\pi x y}{q}\right| &\leq \sum_{x \in \mathbb{Z} \cap (C, q/2)} \sqrt{\vartheta_{\sigma,q}(x)} \\
&= \frac{1}{\sqrt{\rho_\sigma(\mathbb{Z})}} \sum_{x \in \mathbb{Z} \cap (C, q/2)} \sqrt{\sum_{k \in \mathbb{Z}} \rho_\sigma(x + kq)} \\
&\leq \frac{1}{\sqrt{\rho_\sigma(\mathbb{Z})}} \sum_{x \in \mathbb{Z} \cap (C, q/2)} \sum_{k \in \mathbb{Z}} \rho_{\sqrt{2}\sigma}(x + kq) \\
&\leq \frac{1}{\sqrt{\rho_\sigma(\mathbb{Z})}} \sum_{x \in \mathbb{Z} \setminus [-C, C]} \rho_{\sqrt{2}\sigma}(x) \\
&\leq \frac{\rho_{\sqrt{2}\sigma}(\mathbb{Z})}{\sqrt{\rho_\sigma(\mathbb{Z})}}\,\frac{C}{\sqrt{2\sigma}}\,\sqrt{2\pi \mathrm{e}}\,\mathrm{e}^{-\pi\frac{C^2}{2\sigma^2}} \quad \text{(by Lemma 2)} \\
&\leq \frac{1 + \sqrt{2}\sigma}{\sqrt{\sigma}}\,\frac{C}{\sqrt{2\sigma}}\,\sqrt{2\pi \mathrm{e}}\,\mathrm{e}^{-\pi\frac{C^2}{2\sigma^2}} \quad \text{(by Lemma 3)} \\
&\leq \mathsf{negl}(\lambda)/\sqrt{q^n}\ .
\end{aligned}$$

Finally, we observe that the truncated summation can be computed in time $\mathsf{poly}(\lambda)$. □

**Lemma 17.** *Let $n \geq 1$, $q \geq 3$ integers, $\sigma > 0$ a real number and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ as in Theorem 4. Assume that $n, \sigma = \mathsf{poly}(\lambda)$ and $q = 2^{\mathsf{poly}(\lambda)}$, where $\lambda$ is security parameter. Then we can build the following state in runtime $\mathsf{poly}(\lambda)$ and within error $\mathsf{negl}(\lambda)/\sqrt{q^n}$ in trace distance:*

$$\sum_{x \in \mathbb{Z}/q\mathbb{Z}} f(x)\,|x\rangle\ .$$

*Proof.* Let $C = \mathsf{poly}(\lambda)\frac{n}{2}\log q \leq \mathsf{poly}(\lambda)$. First, we build a state proportional to:

$$\sum_{x \in \mathbb{Z} \cap [-C, C]} \sqrt{\rho_\sigma(x)}\,|x\rangle\ .$$

Thanks to [GR02], such a state can be built in time $\mathsf{poly}(\lambda)$. This state is within trace distance $\mathsf{negl}(\lambda)/\sqrt{q^n}$ (by using the same reasoning as in the proof of Lemma 16) from

$$\sum_{x \in \mathbb{Z}/q\mathbb{Z}} \sqrt{\vartheta_{\sigma,q}}\,|x\rangle\ .$$

To complete the proof, it remains to add a $-1$ phase to the states $|x\rangle$ with $x < 0$. This can be implemented by using a control gate on the appropriate register of $|x\rangle$. □

5.2. **On Condition 3 of Theorem 3.** We now want to show that $q \cdot \min |\widehat{f}|^2$ is $1/\mathsf{poly}(\lambda)$. We first observe that, in most cases, the direct choice of $f_0 = \sqrt{\vartheta_{\sigma,q}}$ does not satisfy this condition. This motivates the introduction of $\pm 1$ phases.

**Lemma 18.** *Let $q \geq 2$ and integer and $\sigma \geq 1$ a real number. Let $f_0 = \sqrt{\vartheta_{\sigma,q}}$. We have:*

$$q \cdot \min |\widehat{f_0}|^2 \leq 32\sigma \cdot \max\left(\mathrm{e}^{-\frac{\pi\sigma^2}{4}}, \mathrm{e}^{-\frac{q^2}{4\sigma^2}}\right) .$$

The proof is deferred to Appendix B. The result shows that, for Condition 3 of Theorem 3 to have a chance to hold, one is required to set the standard deviation parameter $\sigma$ as $O(\sqrt{\log \lambda})$ or such that $q/\sigma = O(\sqrt{\log \lambda})$. Unfortunately, in the first case, the $\mathsf{LWE}_{m,n,q,\sigma}$ problem can be solved efficiently [AG11], whereas the second one is too restrictive to enable cryptographic constructions.

To circumvent the above difficulty, we consider phases. Note that adding phases to $f$ does not have any impact on the measurements and, therefore, after measuring the state, one still obtains an $\mathsf{LWE}$ sample with the same distribution. In the following lemmas, we show that the phases considered in Theorem 4 can sufficiently increase the quantity $q \cdot \min |\widehat{f}|^2$.

**Lemma 19.** *Let $q \geq 2$ an odd integer and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ such that $f(-x) = -f(x)$ for all $x \in \mathbb{Z}/q\mathbb{Z} \setminus \{0\}$. Then we have*

$$q \cdot \min |\widehat{f}|^2 = q \cdot |\widehat{f}(0)| = |f(0)|^2 .$$

*Proof.* The discrete Fourier transform of $f$ is given by

$$\begin{aligned}
\widehat{f}(y) &= \frac{f(0)}{\sqrt{q}} + \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{Z} \cap (0, q/2)} f(x)\, \omega_q^{xy} + \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{Z} \cap (-q/2, 0)} f(x)\, \omega_q^{xy} \\
&= \frac{f(0)}{\sqrt{q}} + \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{Z} \cap (0, q/2)} f(x) \left(\omega_q^{xy} - \omega_q^{-xy}\right) \quad (\text{as } \forall x \neq 0 : f(-x) = -f(x)) \\
&= \frac{f(0)}{\sqrt{q}} + i\, \frac{2}{\sqrt{q}} \sum_{x \in \mathbb{Z} \cap (0, q/2)} f(x)\, \sin \frac{2\pi x y}{q} ,
\end{aligned}$$

for all $y \in \mathbb{Z}/q\mathbb{Z}$. By the triangular inequality, the minimum is reached for $y = 0$. □

We have the following lemma as a special case for the distribution $\vartheta_{\sigma,q}$.

**Lemma 20.** *Let $q \geq 2$ an odd integer, $\sigma > 0$ a real number and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ as in Theorem 4. Then we have*

$$q \cdot \min |\widehat{f}|^2 \geq \frac{1}{1+\sigma} .$$

*Proof.* The statement $f(-x) = -f(x)$ holds for all $x \neq 0$. Therefore, using the positivity of $\vartheta_{\sigma,q}$, we obtain

$$q \cdot \min |\widehat{f}|^2 \geq \vartheta_{\sigma,q}(0) \geq \frac{1}{\rho_\sigma(\mathbb{Z})} .$$

Lemma 3 then gives the result. □

Adding $\pm 1$ phases "exponentially" increases the success probability $p = q \cdot \min |\widehat{f}|^2$, when choosing $|f|^2 = \vartheta_{\sigma,q}$, which allows to fulfill Condition 3 of Theorem 2 under the constraint that $m, \sigma \leq \mathsf{poly}(\lambda)$. This improvement is crucial as otherwise we could not set $m$ (which plays a significant role in the run-time of the algorithm) as some $\mathsf{poly}(\lambda)$.

5.3. **On Condition 4 of Theorem 3.** To instantiate Theorem 3, it now suffices to show that Condition 4 holds. Recall that it involves $Z_f(\mathbf{A})$, which is the normalization scalar ensuring that $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ is unit vector.

**Lemma 21.** *Let $m, n \geq 1, q \geq 2$ integers, $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, $f$ an amplitude function over $\mathbb{Z}/q\mathbb{Z}$, and $Z_f(\mathbf{A})$ as per Definition 11. Then we have:*

$$\left|\frac{Z_f(\mathbf{A})}{q^n} - 1\right| \leq \sum_{\substack{\mathbf{e}\neq\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \ .$$

*Proof.* For every vector $\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$, let $|\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle$ denotes the following state:

$$|\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle := \sum_{\mathbf{x}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{A}\mathbf{x} + \mathbf{e}\rangle \ .$$

(The state is purposefully not normalized.) For two vectors $\mathbf{e}, \mathbf{e}'$, we have

$$\langle \mathrm{Im}(\mathbf{A}) + \mathbf{e}' | \mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle = \begin{cases} q^n & \text{if } \mathbf{e}-\mathbf{e}' \in \mathrm{Im}(\mathbf{A}) \\ 0 & \text{otherwise} \end{cases} \ . \tag{23}$$

Then the $|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f}$ state can be expressed as follows:

$$|\mathsf{LWE}(\mathbf{A})\rangle_{m,n,q,f} = \frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} f(\mathbf{e})\,|\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle \ .$$

Therefore, we have

$$Z_f(\mathbf{A}) = \left\| \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} f(\mathbf{e})\,|\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle \right\|^2 .$$

The above term is equal to:

$$\sum_{\mathbf{e},\mathbf{e}'} f(\mathbf{e})\overline{f(\mathbf{e}')}\,\langle \mathrm{Im}(\mathbf{A}) + \mathbf{e}' | \mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle = q^n \sum_{\substack{\mathbf{e},\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} f(\mathbf{e})\overline{f(\mathbf{e}')} = q^n + q^n \sum_{\substack{\mathbf{e}\neq\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} f(\mathbf{e})\overline{f(\mathbf{e}')} \ ,$$

where we used Equation (23). We obtain:

$$\left|\frac{Z_f(\mathbf{A})}{q^n} - 1\right| = \left| \sum_{\substack{\mathbf{e}\neq\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} f(\mathbf{e})\overline{f(\mathbf{e}')} \right| .$$

The result follows from the triangular inequality. □

We now prove the following lemma.

**Lemma 22.** *Let $m, n \geq 1$ and $q \geq 2$ integers, and $f$ an amplitude function over $\mathbb{Z}/q\mathbb{Z}$. Assume that $q$ is prime. Let $\mathbf{A}$ be sampled uniformly in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and let $Z_f(\mathbf{A})$ be as per Definition 11. Then we have, for any $\delta > 0$:*

$$\mathbb{P}_{\mathbf{A}}\left(\left|\frac{Z_f(\mathbf{A})}{q^n} - 1\right| \geq \delta\right) \leq \frac{\sum_{\mathbf{e}\neq\mathbf{e}'} |f|(\mathbf{e})\cdot|f|(\mathbf{e}')}{\delta\cdot q^{m-n}} \ .$$

*Proof.* We define:

$$S := \sum_{\substack{\mathbf{e}\neq\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \ ,$$

and view it as a random variable over the random choice of $\mathbf{A}$. By Lemma 21, we have that $|Z_f(\mathbf{A})/q^n - 1| \leq S$ holds for all $\mathbf{A}$. Further, by Markov's inequality, one obtains that $\mathbb{P}_{\mathbf{A}}(S \geq \delta) \leq \mathbb{E}_{\mathbf{A}}(S)/\delta$ holds for every $\delta > 0$. Using the linearity of the expectation, one obtains:

$$\begin{aligned}\mathbb{E}_{\mathbf{A}}(S) &= \mathbb{E}_{\mathbf{A}}\left(\sum_{\mathbf{e}\neq\mathbf{e}'} \mathbb{1}_{\mathrm{Im}(\mathbf{A})}(\mathbf{e}-\mathbf{e}')\ |f|(\mathbf{e})\cdot|f|(\mathbf{e}')\right)\\ &= \sum_{\mathbf{e}\neq\mathbf{e}'} \mathbb{P}_{\mathbf{A}}\left(\mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})\right)\ |f|(\mathbf{e})\cdot|f|(\mathbf{e}')\\ &\leq \frac{1}{q^{m-n}}\sum_{\mathbf{e}\neq\mathbf{e}'}|f|(\mathbf{e})\cdot|f|(\mathbf{e}')\ . \end{aligned} \tag{24}$$

The last inequality follows from the union bound (over all elements in the image of $\mathbf{A}$) and the fact that $q$ is prime. □

We are particularly interested in the case where $|f| = \sqrt{\vartheta_{\sigma,q}}$. The following lemma allows us to apply the above result on this particular function.

**Lemma 23.** *Let $m \geq 1$ and $q \geq 2$ integers, and $\sigma$ a real number such that $2 \leq \sigma \leq q/\sqrt{8m\ln q}$. Then we have:*

$$\sum_{\mathbf{e}\neq\mathbf{e}'}\sqrt{\vartheta_{\sigma,q}(\mathbf{e})}\sqrt{\vartheta_{\sigma,q}(\mathbf{e}')} \leq q^{\frac{m}{2}}+1\ .$$

*Proof.* First, note that the summation can be rewritten in the following way:

$$\sum_{\mathbf{e}\neq\mathbf{e}'}\sqrt{\vartheta_{\sigma,q}(\mathbf{e})}\sqrt{\vartheta_{\sigma,q}(\mathbf{e}')} = \Big(\sum_{\mathbf{e}}\sqrt{\vartheta_{\sigma,q}(\mathbf{e})}\Big)^2 - \sum_{\mathbf{e}}\vartheta_{\sigma,q}(\mathbf{e})\ .$$

By positivity of the second term, it suffices to find an upper bound for the first one. We rely on Lemma 4 to approximate $\vartheta_{\sigma,q}$ with $D_{\mathbb{Z}^m,\sigma}$. We have

$$\begin{aligned}\sum_{\mathbf{e}\in\mathbb{Z}^m\cap(-\frac{q}{2},\frac{q}{2}]^m}\sqrt{\vartheta_{\sigma,q}(\mathbf{e})} &\leq \sum_{\mathbf{e}\in\mathbb{Z}^m\cap(-\frac{q}{2},\frac{q}{2}]^m}\left(\sqrt{D_{\mathbb{Z}^m,\sigma}(\mathbf{x})}+\mathrm{e}^{-\frac{q^2}{8\sigma^2}}\right) \quad \text{(by Lemma 4)}\\ &= \sum_{\mathbf{e}\in\mathbb{Z}^m\cap(-\frac{q}{2},\frac{q}{2}]^m}\left(\frac{\rho_{\sqrt{2}\sigma}(\mathbb{Z}^m)}{\sqrt{\rho_\sigma(\mathbb{Z}^m)}}\ D_{\mathbb{Z}^m,\sqrt{2}\sigma}(\mathbf{x})+\mathrm{e}^{-\frac{q^2}{8\sigma^2}}\right)\\ &\leq \frac{\rho_{\sqrt{2}\sigma}(\mathbb{Z}^m)}{\sqrt{\rho_\sigma(\mathbb{Z}^m)}}+q^m\mathrm{e}^{-\frac{q^2}{8\sigma^2}}\\ &\leq \frac{(1+\sqrt{2}\sigma)^m}{\sqrt{\sigma^m}}+q^m\mathrm{e}^{-\frac{q^2}{8\sigma^2}} \quad \text{(by Lemma 3)}\\ &\leq (2\sqrt{\sigma})^m+q^m\mathrm{e}^{-\frac{q^2}{8\sigma^2}}\ .\end{aligned}$$

Since $\sigma \leq q/\sqrt{8m\ln q}$, we have that the last term is $\leq 1$. Finally, note that the same upper bound on $\sigma$ also implies that $2\sqrt{\sigma} \leq \sqrt{q}$. □

We can now conclude, by combining Lemma 22 and Lemma 23 with $\delta = q^{-n}$.

**Lemma 24.** *Let $m \geq n \geq 1$, $q \geq 2$ integers, $\sigma > 0$ a real number and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ as in Theorem 4. Assume that $q$ is prime and $2 \leq \sigma \leq q/\sqrt{8m\ln q}$. Let $\mathbf{A}$ be sampled uniformly from $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and let $Z_f(\mathbf{A})$ as per Definition 11. Then we have*

$$\mathbb{P}_{\mathbf{A}}\left(\left|\frac{Z_f(\mathbf{A})}{q^n}-1\right| \geq q^{-n}\right) \ \leq\ q^{2n-m}(q^{\frac{m}{2}}+1)\ .$$

## 6. On the security of some lattice-based SNARKs

The purpose of this section is to show that the hardness assumptions used in several standard model lattice-based SNARKs [GMNO18, NYI+20, ISW21, SSEK22, CKKK23, GNSV23] are invalid in the context of quantum adversaries.

### 6.1. Module Learning With Errors.

All the SNARK constructions mentioned above can be framed into an algebraic variant of LWE called MLWE, which captures LWE and the Ring Learning With Errors problem (RLWE) [SSTX09, LPR10]. To recall the definition of MLWE and adapt the results on oblivious LWE sampling to MLWE, we first provide some reminders.

Let $d \geq 1$ be a power-of-2 integer. The cyclotomic ring $R$ of degree $d$ is $\mathbb{Z}[x]/\langle x^d+1\rangle$. Each element of $R$ is a polynomial of degree at most $d-1$ with integer coefficients. We let $\phi : R \to \mathbb{Z}^d$ denote the map that sends each element $\sum_{i<d} a_i x^i \in R$ to the vector $(a_0, \ldots, a_{d-1})^\intercal \in \mathbb{Z}^d$. For every element $a \in R$, we define $\mathrm{rot}(a)$ as the matrix whose $i$-th column is $\phi(x^{i-1}a \bmod x^d+1)$, for all $1 \leq i \leq d$. Then we have $\phi(a \cdot b) = \mathrm{rot}(a)\phi(b)$ for all $a, b \in R$. Let $q \geq 2$ be an integer. Both $\phi$ and rot are extended to the quotient ring $R/qR$. Similarly, we extend $\phi$ to $(R/qR)^m$ and rot to $(R/qR)^{m\times n}$ for any integers $m, n \geq 1$.

For a distribution $\chi$ over $\mathbb{Z}/q\mathbb{Z}$, we define $\chi^{\otimes d}$ as the distribution over $R/qR$ obtained by independently sampling each coefficient from $\chi$. The notation is extended to distributions over $(R/qR)^m$ for any $m \geq 1$.

Module Learning With Errors (MLWE) is a variant of LWE introduced and studied in [BGV12, LS15]. It is defined by replacing $\mathbb{Z}/q\mathbb{Z}$ by $R/qR$ in the LWE definition.

**Definition 14** (MLWE). *Let $m \geq n \geq 1, q \geq 2$ be integers, $R$ be a cyclotomic ring of degree a power-of-2 integer $d$ and $\chi$ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. The parameters $m, n, d, q$ and $\chi$ are functions of some security parameter $\lambda$. Let $\mathbf{A} \in (R/qR)^{m\times n}$, $\mathbf{s} \in (R/qR)^n$ be sampled uniformly and $\mathbf{e} \in (R/qR)^m$ be sampled from from $\chi^{\otimes dm}$. The search $\mathsf{MLWE}_{m,n,d,q,\chi}$ problem is to find $\mathbf{s}$ and $\mathbf{e}$ given the pair $(\mathbf{A}, \mathbf{As}+\mathbf{e})$. The vectors $\mathbf{s}$ and $\mathbf{e}$ are respectively called the secret and the noise.*

*Whenever $\chi$ is equal to the folded discrete Gaussian distribution $\vartheta_{\sigma,q}$ for some $\sigma > 0$, we overwrite the notations as $\mathsf{MLWE}_{m,n,d,q,\sigma}$ .*

We now show how Theorem 4 can be extended to MLWE. The MLWE problem can be viewed as a special case of LWE. Concretely, an $\mathsf{MLWE}_{m,n,d,q,\chi}$ instance $(\mathbf{A}, \mathbf{b} = \mathbf{As}+\mathbf{e}) \in (R/qR)^{m\times n} \times (R/qR)^m$ is mapped to the $\mathsf{LWE}_{md,nd,q,\chi}$ instance

$$(\mathrm{rot}(\mathbf{A}), \phi(\mathbf{b}) = \mathrm{rot}(\mathbf{A})\phi(\mathbf{s}) + \phi(\mathbf{e})) \;\in\; (\mathbb{Z}/q\mathbb{Z})^{md\times nd} \times (\mathbb{Z}/q\mathbb{Z})^{md} \; .$$

Our goal is to use Theorem 3 with these specific matrices. By the identity above, one can observe that Conditions 1 and 2 are not impacted by the change from LWE to MLWE. Condition 3 is related to the Gaussian elimination subroutine of Algorithm 1. We note that there is no $q$ such that $R/qR$ is a field (as opposed to $\mathbb{Z}/q\mathbb{Z}$ with $q$). Instead, we choose $q$ prime such that $q = 3 \bmod 8$. In that case, the ring $R/qR$ is isomorphic to $\mathbb{F}_{q^{d/2}} \times \mathbb{F}_{q^{d/2}}$. For $m \geq n \cdot \omega(\log \lambda)$, a uniform $\mathbf{A} \in (R/qR)^{m\times n}$ has a set of $n$ rows that form an invertible matrix, with probability $1 - \mathsf{negl}(\lambda)$. This allows us to adapt the Gaussian elimination subroutine of Algorithm 1 to the module setting. Overall, for such a modulus $q$, Condition 3 is also not impacted by the change from LWE to MLWE.

We now focus on Condition 4, which was proved in Subsection 5.3 to be fulfilled in the LWE case for a specific choice of amplitude function (defined in Theorem 4). We keep the same amplitude function, and adapt Lemma 24 to the module setting.

**Lemma 25.** *Let $m \geq n \geq 1, q \geq 2$ integers, $\sigma > 0$ a real number, $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ as in Theorem 4 and $R$ a cyclotomic ring of degree a power-of-2 integer $d$. Assume that $q$ is prime and satisfies $q = 3 \bmod 8$ and $2 \leq \sigma \leq \sqrt{q/(8m \ln q)}$. Let $\mathbf{A}$ be sampled uniformly from $(R/qR)^{m\times n}$, and let $Z_f(\mathrm{rot}(\mathbf{A}))$ as per Definition 11. Then we have*

$$\mathbb{P}_{\mathbf{A}}\left(\left|\frac{Z_f(\mathrm{rot}(\mathbf{A}))}{q^{nd}} - 1\right| \geq q^{-nd}\right) \;\leq\; q^{(2n-\frac{m}{2})d}(q^{\frac{md}{4}}+1) \; .$$

*Proof.* We follow the proof of Lemma 24 in Subsection 5.3. Lemma 21 applies without any change. For Lemma 22, the only step that needs to be adapted is Equation (24). We have, for $\mathbf{e} \neq \mathbf{e}' \in (R/qR)^m$:

$$\mathbb{P}_{\mathbf{A}}\left(\mathbf{e}-\mathbf{e}' \in \mathrm{Im}(\mathbf{A})\right) \leq q^{dn} \max_{\mathbf{s}\in(R/qR)^n} \mathbb{P}_{\mathbf{A}}\left(\mathbf{e}-\mathbf{e}' = \mathbf{A}\mathbf{s}\right) \ \leq q^{dn} \cdot q^{-\frac{dm}{2}} \ .$$

where we used the union bound in the first inequality and considered only one of the components of $R/qR \simeq \mathbb{F}_{q^{d/2}} \times \mathbb{F}_{q^{d/2}}$ in the second inequality. As a result, the term "$q^{m-n}$" in statement of Lemma 22 is replaced by $q^{(m/2-n)d}$. The proof of Lemma 23 is unchanged, but we strengthen the upper bound on $\sigma$ to $\sigma \leq \sqrt{q/(8m\ln q)}$ to be able to replace the term"$q^{m/2}$" in statement of Lemma 23 by $q^{md/4}$. This completes the proof of Lemma 25. □

Using the above, we obtain the following adaptation of Theorem 4.

**Theorem 5.** *Let $m, n, d, q, R, \sigma, \lambda$ as in Definition 14. Assume that $m, \log q \leq \mathsf{poly}(\lambda)$ and $q$ is prime with $q = 3 \bmod 8$. Assume further that the parameters satisfy the following conditions:*

$$m \geq n\sigma \cdot \omega(\log\lambda) \quad \text{and} \quad 2 \leq \sigma \leq \sqrt{\frac{q}{8m\ln q}} \ .$$

*Then Algorithm 1 runs in time $\mathsf{poly}(\lambda)$ and, for a proportion $1-\mathsf{negl}(\lambda)$ of matrices $\mathbf{A} \in (R/qR)^{m\times n}$, it outputs a quantum state $|\varphi\rangle$ such that $D_{\mathrm{tr}}(|\varphi\rangle, |\mathbf{0}\rangle |\mathsf{LWE}(\mathrm{rot}(\mathbf{A}))\rangle_{q,f} |0\rangle) = \mathsf{negl}(\lambda)$.*

*In particular, if $\mathsf{MLWE}_{m,n,d,q,\sigma}$ is hard, then there exists a $\mathsf{poly}(\lambda)$-time quantum witness-oblivious $\mathsf{MLWE}_{m,n,d,q,\sigma}$ sampler.*

As in the LWE context, we could use Karp reductions from MLWE with one parametrization to MLWE with another parametrization to significantly extend the range of allowed MLWE parametrizations in Theorem 5. We could notably throw away superfluous samples, switch from one modulus to another [LS15] or trade modulus for dimension [AD17].

6.2. **Knapsack MLWE.** We generalize the knapsack variant of LWE from [MM11] to modules.

**Definition 15** (knMLWE)**.** *Let $m, n, d, q, R, \chi$ as in Definition 14. Let $\mathbf{B} \in (R/qR)^{n\times m}$ and $\mathbf{e} \in (R/qR)^m$ be sampled from $\chi^{\otimes dm}$. The search $\mathsf{knMLWE}_{m,n,d,q,\chi}$ problem is to find $\mathbf{e}$ from $(\mathbf{B}, \mathbf{Be})$.*

*Whenever $\chi$ is equal to the folded discrete Gaussian distribution $\vartheta_{\sigma,q}$, we overwrite the notation as $\mathsf{knMLWE}_{m,n,d,q,\sigma}$.*

A Karp reduction from LWE to its knapsack form was given in [MM11, Le. 4.8]. To extend it to modules, one needs to be able to perform linear algebra efficiently and that uniform matrices over $(R/qR)^{m\times(m-n)}$ contain a subset of $m-n$ rows that is invertible with sufficiently high probability. These conditions were already required to obtain Theorem 5, so we can keep the same parameter constraints here. Using Theorem 5 and Lemma 8, we obtain the following result.

**Theorem 6.** *Let $m, n, d, q, R, \sigma, \lambda$ as in Definition 14. Assume that $m, \log q \leq \mathsf{poly}(\lambda)$ and $q$ is prime with $q = 3 \bmod 8$. Assume further that the parameters satisfy the following conditions:*

$$m \geq (m-n)\sigma \cdot \omega(\log\lambda) \quad \text{and} \quad 2 \leq \sigma \leq \sqrt{\frac{q}{8m\ln q}} \ .$$

*Assume that $\mathsf{MLWE}_{m,m-n,d,q,\sigma}$ is hard. Then there exists a $\mathsf{poly}(\lambda)$-time algorithm that produces samples $(\mathbf{B}, \mathbf{Be})$ that are within statistical distance $\mathsf{negl}(\lambda)$ from those obtained by sampling $\mathbf{B}$ uniformly and $\mathbf{e}$ from $\vartheta_{\sigma,q}^{\otimes dm}$, and for which there exists no efficient extractor algorithm that would recover the witness $\mathbf{e}$.*

We discuss some restrictions of Theorem 6. For a large number of columns $m$, the matrix $\mathbf{B}$ must be almost square for the condition $m \geq (m-n)\cdot\omega(\log\lambda)$ to be satisfied. If we are interested in much fewer rows than columns (which is the case in our applications), one may use Theorem 6 with a near-square matrix and then throw away the superfluous rows. This preserves obliviousness.

Another restriction of Theorem 6 is that the modulus $q$ is required to be prime and to satisfy $q = 3 \bmod 8$. However, in most applications, the modulus is not of that form: for example, in [ISW21], the considered moduli are powers of 2. We want to use modulus switching for knMLWE, but there

are two difficulties. First, modulus switching introduces a small rounding error. We make it part of the weight vector $\mathbf{e}$ by putting the matrix $\mathbf{B}$ in canonical form. Second, in our application, the matrix $\mathbf{B}$ is given as input to the instance sampler rather than generated by the sampler itself. For this aspect, we note that the sampler of Theorem 6 satisfies this property: given as input a uniform matrix $\mathbf{B}$, with probability $1 - \mathsf{negl}(\lambda)$, it outputs $\mathbf{Be}$ such that $\mathbf{e}$ is within $\mathsf{negl}(\lambda)$ statistical distance from $\vartheta_{\sigma,q}^{\otimes dm}$.

Algorithm 2 is designed to handle those aspects. Step 1 puts the input matrix in canonical form. Step 4 performs a modulus switch for the non-trivial component $\overline{\mathbf{B}}$ of the canonical form. The new modulus $q'$ is prime and satisfies $q' = 3 \bmod 8$ (note that such primes are frequent). By choice of $\mathbf{E}$ and $\tau$, the resulting matrix $\overline{\mathbf{B}}'$ is within negligible statistical distance from uniform (this may be proved using standard facts on discrete Gaussian distributions, such as done for example in [BLP+13]). Step 6 randomizes to hide the canonical form to obtain a uniform matrix $\overline{\mathbf{B}}$. Step 7 calls the algorithm from Theorem 6 to obtain $\overline{\mathbf{b}} = \overline{\mathbf{B}}\mathbf{e}$ for some unknown $\mathbf{e}$ (as discussed above, the algorithm from Theorem 6 satisfies the property that it outputs a vector for a given matrix, rather than sampling them together). Finally, Step 8 sends $\overline{\mathbf{b}}$ back to $R/qR$.

We can see that the output $\mathbf{b}$ is of the correct form. First, note that we have $\overline{\mathbf{T}}^{-1}\overline{\mathbf{b}} = (\mathbf{I} \mid \overline{\mathbf{B}}')\mathbf{e}$. Rounding from modulus $q'$ to modulus $q$ gives $\frac{q}{q'}(\mathbf{I} \mid \overline{\mathbf{B}}')\mathbf{e} + \mathbf{f}$ for some small-magnitude vector $\mathbf{f}$. Letting $\mathbf{e}_1$ denote the first $n$ entries of $\mathbf{e}$ and $\mathbf{e}_2$ the remaining $m - n$, and using the definition of $\overline{\mathbf{B}}'$, we see that $\frac{q}{q'}(\mathbf{I} \mid \overline{\mathbf{B}}')\mathbf{e} + \mathbf{f}$ is of the form $\overline{\mathbf{B}}\mathbf{e}_2 + \mathbf{g}$ for some small magnitude vector $\mathbf{g}$. This can be rewritten as $(\mathbf{I} \mid \overline{\mathbf{B}})(\mathbf{g}^\intercal | \mathbf{e}_2^\intercal)^\intercal$. Multiplying by $\mathbf{T}$ gives that $\mathbf{b}$ is indeed of the correct form. Further, the transformation preserves obliviousness. Assume by contradiction that an extractor can recover $(\mathbf{g}^\intercal | \mathbf{e}_2^\intercal)^\intercal$. Then it can in particular recover $\mathbf{e}_2$. From $\mathbf{e}_2$, it can recover $\mathbf{e}_1$ as $\mathbf{e}_1 = \overline{\mathbf{T}}^{-1}\overline{\mathbf{b}} - \overline{\mathbf{B}}'\mathbf{e}_2$. This contradicts the fact that the algorithm from Theorem 6 is oblivious.

Finally, let us comment on the failure probability of Step 1 (as $q'$ is prime and satisfies $q' = 3 \bmod 8$, the failure probability of Step 5 is very low). Depending on the arithmetic shape of $q$ and the values of $m$ and $n$, this value could possibly be non-negligible. Fortunately, in all the applications, the number of columns $m$ is orders of magnitude higher than the number of rows $n$, so that, with overwhelming probability, we can find a subset of $n$ columns that is invertible. It then suffices to apply Algorithm 2 after an appropriate reordering of the columns.

**Algorithm 2** Witness-oblivious knMLWE sampler for arbitrary $q$

**Parameters:** $m, n, q, d, \sigma$ and $\lambda$ as in Definition 14.
**Input:** $\mathbf{B} \in (R/qR)^{n \times m}$.
**Output:** A vector $\mathbf{b} \in (R/qR)^n$.

1: Compute a matrix $\mathbf{T}$ such that $\mathbf{TB} = (\mathbf{I} \mid \overline{\mathbf{B}})$. If $\mathbf{T}$ does not exist, then abort.
2: Set $q'$ as the smallest prime larger than $q$ such that $q' = 3 \bmod 8$.
3: Set $\tau := q'/q \cdot \sqrt{\lambda}$.
4: Set $\overline{\mathbf{B}}' := \frac{q'}{q}\overline{\mathbf{B}} + \mathbf{E}$ with each entry of $\mathrm{rot}(\mathbf{E})$ sampled from $D_{\mathbb{Z} - \frac{q'}{q}\mathrm{rot}(\mathbf{B})_{ij}, \tau}$ for all $i, j$.
5: Sample $\overline{\mathbf{T}} \in (R/q'R)^{n \times n}$. If it is not invertible, then abort.
6: Set $\overline{\mathbf{B}} := \overline{\mathbf{T}}(\mathbf{I} \mid \overline{\mathbf{B}}')$.
7: Apply the sampler from Theorem 6 with parameters $m, n, q', d, \sigma$ on $\overline{\mathbf{B}}$ to obtain $\overline{\mathbf{b}} = \overline{\mathbf{B}}\mathbf{e}$.
8: Compute $\mathbf{b} := \mathbf{T}^{-1}\lfloor \frac{q}{q'}(\overline{\mathbf{T}}^{-1}\overline{\mathbf{b}} \bmod q') \rceil \bmod q$.
9: Return $\mathbf{b}$.

6.3. **SNARKs from linear-only vector encryption.** For constructing SNARKs, the authors of [ISW21, SSEK22, CKKK23] adapt the approaches of [BCI+13] and [BISW17] to the LWE setting (the possibility of adaptation to LWE was actually suggested in [BCI+13], see Remark 5.19 therein). They use secret-key vector encryption schemes that are linear-only homomorphic. The plaintexts belong to an $R/pR$-module, whereas the ciphertexts belong to an $R/qR$-module for some integers $q > p \geq 2$ where $R = \mathbb{Z}[x]/\langle x^d + 1 \rangle$ for some power-of-2 degree $d$. Such schemes

allow the players to compute $R/pR$-linear functions of the ciphertexts but no other function than those ones. This is called to the linear-only property.

**Definition 16** (Vector Encryption over Cyclotomic Fields)**.** *Let $\ell, m, n \geq 1$ be integers, $R = \mathbb{Z}[x]/\langle x^d + 1\rangle$ with a power-of-2 degree $d$ $q > p \geq 2$ be integers, and $S$ be a subset of $(R/pR)^m$. All these are functions of the security parameter $\lambda$. A secret-key linearly-homomorphic vector encryption scheme with the message space $(R/pR)^\ell$ and the ciphertext space $(R/qR)^n$ is a tuple of algorithms $\Pi_{\mathsf{Enc}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Add})$ with the following specifications.*

- $\mathsf{Gen}(1^\lambda) \mapsto (\mathsf{pp}, \mathsf{sk})$*: Given the security parameter $\lambda$, it outputs public parameters $\mathsf{pp}$ and a secret key $\mathsf{sk}$;*
- $\mathsf{Enc}(\mathsf{sk}, \mathbf{v}) \mapsto \mathsf{ct}$*: Given the secret key $\mathsf{sk}$ and a vector $\mathbf{v} \in (R/pR)^\ell$, it outputs a ciphertext $\mathbf{ct} \in (R/qR)^n$;*
- $\mathsf{Dec}(\mathsf{sk}, \mathbf{ct}) \mapsto \mathbf{v}/\perp$*: Given the secret key $\mathsf{sk}$ and a ciphertext $\mathbf{ct}$, it outputs a vector $\mathbf{v} \in (R/pR)^\ell$ or a special symbol $\perp$;*
- $\mathsf{Add}(\mathsf{pp}, \{\mathbf{ct}_i\}_i, \{y_i\}_i) \mapsto \mathbf{ct}^*$*: Given the public parameters $\mathsf{pp}$, a collection of ciphertexts $\{\mathbf{ct}_i\}_i$, and a collection of scalars $\{y_i\}_i$ from $R/pR$, it outputs a ciphertext $\mathbf{ct}^*$.*

*Moreover, Algorithm $\mathsf{Add}$ satisfies the following property:*

- *Additive homomorphism with respect to the set $S$: For all security parameters $\lambda$, all vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_m\}$ from $(R/pR)^\ell$, and $(y_1, \ldots, y_m) \in S$, it holds that*

$$\mathbb{P}\left(\mathsf{Dec}(\mathsf{sk}, \mathbf{ct}^*) = \sum_{i=1}^{m} y_i \mathbf{v}_i \;\middle|\; \begin{array}{l} (\mathsf{pp}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathbf{ct}_i \leftarrow \mathsf{Enc}(sk, \mathbf{v}_i) \\ \mathbf{ct}^* \leftarrow \mathsf{Add}(\mathsf{pp}, \{\mathbf{ct}_i\}_i, \{y_i\}_i) \end{array}\right) = 1 - \mathsf{negl}(\lambda) \ .$$

The set $S$ controls the level of homomorphic operations that are allowed. In [ISW21, Th. 3.12], it is showed that the proposed vector encryption scheme allows homomorphic operations with respect to the whole set $(R/pR)^m$ when $q$ is chosen sufficiently large. In [SSEK22, Th. 2], this set is more restricted.

When using lattice problems, the functionality of Definition 16 is obtained as follows. One typically relies on an LWE/MLWE encryption scheme with plaintexts defined modulo $p$. Given ciphertexts $\mathbf{ct}_i$'s, which are vectors modulo $q$, and scalars $y_i$, the $\mathsf{Add}$ algorithm first computes the linear combination $\sum_i y_i \mathbf{ct}_i$ and then possibly adds some large amount of noise (a technique typically referred to as noise flooding or noise smudging) or rounds. These operations can be publicly implemented. In terms of security, the ciphertexts $\mathbf{ct}_i$ are designed to be computationally indistinguishable from uniform, under an appropriate LWE/MLWE parametrization, to ensure the IND-CPA security of the vector encryption scheme. We note that all the schemes we consider follow this blueprint.

In this work, we are particularly interested in the linear-only security property. Note that the adversary is allowed to be a quantum algorithm in the context of post-quantum cryptography. This is taken into account in the following definition.

**Definition 17** (Linear-Only Against Quantum Adversaries)**.** *A vector encryption scheme $\Pi_{\mathsf{Enc}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Add})$ is linear-only if for all QPT algorithms $\mathcal{A}$, there exists a valid QPT extractor $\mathcal{E}$ such that for all security parameters $\lambda$, auxiliary mixed states $\rho$ over $\mathbb{C}^{2^{\mathsf{poly}(\lambda)}}$, and any QPT plaintext generator $\mathcal{M}$, it holds that*

$$\mathbb{P}\left(\mathsf{ExptLinearExt}_{\Pi_{\mathsf{Enc}}, \mathcal{A}, \mathcal{M}, \mathcal{E}, \rho}(1^\lambda) = 1\right) = \mathsf{negl}(\lambda) \ ,$$

*where the experiment $\mathsf{ExptLinearExt}_{\Pi_{\mathsf{Enc}}, \mathcal{A}, \mathcal{M}, \mathcal{E}, \rho}(1^\lambda)$ is defined as follows.*

1. *The challenger samples the public parameters and the secret key $(\mathsf{pp}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$, together with $m$ vectors $(\mathbf{v}_1, \ldots, \mathbf{v}_m) \leftarrow \mathcal{M}(1^\lambda, \mathsf{pp})$. It computes the ciphertexts $\mathbf{ct}_i \leftarrow \mathsf{Enc}(\mathsf{sk}, \mathbf{v}_i)$ for all $i$.*
2. *Then it runs the extraction process with the outputs as follows:*

$$\left((\mathbf{ct}'_1, \ldots, \mathbf{ct}'_k), \mathbf{\Pi}\right) \leftarrow \langle \mathcal{A}, \mathcal{E}\rangle(1^\lambda, |\mathsf{pp}, \mathbf{ct}_1, \ldots, \mathbf{ct}_m\rangle \otimes \rho, |0\rangle) \ .$$

*Let* $\mathbf{V}' = (\mathbf{v}_1|\dots|\mathbf{v}_m)\mathbf{\Pi}$. *The output of the experiment is* 1 *if there exists an* $i \leq m$ *such that* $\mathsf{Dec}(\mathsf{sk}, \mathbf{ct}_i) \neq \perp$ *and* $\mathsf{Dec}(\mathsf{sk}, \mathbf{ct}_i) \neq \mathbf{v}'_i$ *where* $\mathbf{v}'_i$ *is the* $i$*-th column of* $\mathbf{V}'$. *Otherwise, the experiment outputs* 0.

As discussed in [ISW21, Rem. 3.6], the requirement that the extractor must succeed for all auxiliary inputs $\rho$ is too strong. In particular, no polynomial-time extractor exists if $\rho$ is the output of a one-way function that the extractor must invert in order to analyze the behaviour of the sampler. In all cases that we consider, in the classical setting, the auxiliary inputs are sampled as uniform strings. In the quantum setting, such a string can be simulated by Hadamard gates and projective measurements. Therefore, in our applications, we choose $\rho$ to be null.

In Definition 17, the adversary is given $m$ ciphertexts $\mathbf{C} := (\mathbf{ct}_1|\dots|\mathbf{ct}_m) \in (R/qR)^{n\times m}$ and is supposed to output $k$ distinct small linear combinations of these, namely $\mathbf{C}\pi_1, \dots, \mathbf{C}\pi_k$ where $\pi_i \in R^m$ is the $i$-th column of $\mathbf{\Pi}$, with each entry in $(-p/2, p/2]$. It asks the extractor to find the exact value of the matrix $\mathbf{\Pi}$.

We observe that $(\mathbf{C}, \mathbf{C}\pi_i)$ is a $\mathsf{knMLWE}$ instance, for all $i$. In [ISW21], the authors use $\mathsf{MLWE}$ with $d = 2$, whereas much larger degrees are considered in [SSEK22, CKKK23]. In all cases, the $\mathsf{knMLWE}$ number of columns is very large, of the order of $2^{20}$, whereas the number of rows corresponds to $\mathsf{MLWE}$-based ciphertexts is of the order of $2^{12}$. The plaintext modulus $p$ has a bit-size that is much smaller than the one of the ciphertext modulus $q$. The latter may have up to 100 bits in [ISW21].

We attack the linear-only property as follows. Let $\mathbf{C} = (\mathbf{ct}_1|\dots|\mathbf{ct}_m) \in (R/qR)^{n\times m}$ with $\mathbf{ct}_i = \mathsf{Enc}(\mathsf{sk}, \mathbf{v}_i)$ for all $i$. Consider a quantum $\mathsf{knMLWE}$ sampler as in Subsection 6.2. Note that $\mathbf{C}$ is not statistically uniform but only computationally indistinguishable from uniform. This assumption holds for all secret-key encryption schemes used in the considered SNARK constructions. We claim that the sampler is still oblivious in this situation: if an extractor exists for $\mathbf{C}$'s of this form, then we can distinguish $\mathbf{C}$ from uniform (note that one can efficiently verify the validity of the extracted witness). Now, let $\mathbf{Ce}$ be the output of the sampler, with $\mathbf{e} = (e_1, \dots, e_m)^\intercal$ small. It then holds that $e_1\mathbf{ct}_1 + \dots + e_m\mathbf{ct}_m$ decrypts to

$$e_1\mathbf{v}_1 + \dots + e_m\mathbf{v}_m = \mathbf{Ve} \bmod p \ ,$$

as $\Pi_{\mathsf{Enc}}$ is additively-homomorphic modulo $p$. Since $\mathbf{Ce}$ is a hard instance sampled obliviously, extracting $\mathbf{e}$ out of $\mathbf{Ce}$ is not possible for QPT extractors, except with negligible probability. This contradicts Condition 2 of Definition 17.

6.4. **SNARKs from encoding schemes.** In [GGPR13], specific encoding schemes were introduced to build SNARKs from assumptions related to the discrete logarithm problem. Later, the framework was applied to lattices for constructing presumably post-quantum SNARKs [GMNO18, NYI+20, GNSV23]. The constructions in [GMNO18, NYI+20] consider encodings for finite fields, while encodings for rings of the form $R/pR$ are designed. Concretely, the message space is of the form $R/pR$ for some integer $p$ and ring of integers $R$ of a number field, and the codeword space is $(R/qR)^n$ for some integers $n, q > p$. The ring $R$ is usually chosen to be the ring of integers of a power-of-2 cyclotomic field. We recall the definition of encoding schemes, keeping only the parameters and properties that are relevant for our purposes.

**Definition 18** (Encoding Schemes Over Cyclotomic Rings)**.** *Let* $\ell, m, n \geq 1$ *be integers,* $R = \mathbb{Z}[x]/\langle x^d + 1\rangle$ *with a power-of-2 degree* $d$*, and* $q > p \geq 2$ *be integers. All these are functions of the security parameter* $\lambda$*. An* $m$*-linearly-homomorphic encoding scheme with the message space* $R/pR$ *and the codeword space* $C \subseteq (R/qR)^n$ *is a tuple of algorithms* $\Pi_{\mathsf{Ecd}} = (\mathsf{Gen}, \mathsf{Encode}, \mathsf{Eval})$ *with the following specifications.*

- $\mathsf{Gen}(1^\lambda) \mapsto (\mathsf{pp}, \mathsf{sk})$*: Given the security parameter* $\lambda$*, it outputs public parameters* $\mathsf{pp}$ *and a secret key* $\mathsf{sk}$.
- $\mathsf{Encode}(\mathsf{sk}, a) \mapsto \mathbf{cw}$*: Given the secret key* $\mathsf{sk}$ *and a ring element* $a \in R/pR$*, it outputs a codeword* $\mathbf{cw} \in C$ *with the following property: the subsets* $\{C_a \mid a \in R/pR\}$ *partition* $C$ *where* $C_a$ *is the set of all possible encodings of* $a$.

- $\mathsf{Eval}(\mathsf{pp}, \{\mathbf{cw}_1, \ldots, \mathbf{cw}_m\}, \{c_1, \ldots, c_m\}) \mapsto \mathbf{cw}^*$: *Given the public parameters* $\mathsf{pp}$, $m$ *codewords* $\{\mathbf{cw}_1, \ldots, \mathbf{cw}_m\}$, *and* $m$ *scalars* $\{c_1, \ldots, c_m\}$ *in* $R/pR$, *it outputs a codeword* $\mathbf{cw}^*$.

*Moreover, Algorithm* $\mathsf{Eval}$ *satisfies the following property:*

- $m$*-linearly homomorphism: For all* $a_1, \ldots, a_m, c_1, \ldots, c_m \in (R/pR)^m$, *it holds that*

$$\mathbb{P}\left(\mathbf{cw}^* \in C_{\langle \mathbf{a}, \mathbf{c}\rangle} \;\middle|\; \begin{array}{l} (\mathsf{pp}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda) \\ \mathbf{cw}_i \leftarrow \mathsf{Encode}(sk, a_i) \\ \mathbf{cw}^* \leftarrow \mathsf{Eval}(\mathsf{pp}, \{\mathbf{cw}_i\}_i, \{c_i\}_i) \end{array}\right) = 1 - \mathsf{negl}(\lambda) \ .$$

Algorithm $\mathsf{Eval}$ operates within the same framework as Algorithm $\mathsf{Add}$ of Definition 16. Moreover, the encodings are such that the codewords are computationally indistinguishable from random elements in the codeword space.

The $m$-power knowledge of exponent assumption ($m$-PKE) is a generalization of the knowledge of exponent assumption by [Dam91] to encoding schemes. We adapt this assumption to the quantum setting.

**Definition 19** ($m$-PKE Against Quantum Adversaries)**.** *An encoding scheme* $\Pi_{\mathsf{Ecd}} = (\mathsf{Gen}, \mathsf{Encode}, \mathsf{Eval})$ *satisfies* $m$*-PKE assumption for the auxiliary input generator* $\mathcal{Z}$ *if for all QPT algorithms* $\mathcal{A}$, *there exists a valid QPT extractor* $\mathcal{E}$ *such that*

$$\mathbb{P}\left(\mathsf{ExptKnowledgeExt}_{\Pi_{\mathsf{Ecd}}, \mathcal{A}, \mathcal{Z}, \mathcal{E}, k}(1^\lambda) = 1\right) = \mathsf{negl}(\lambda) \ ,$$

*where the experiment* $\mathsf{ExptLinearExt}_{\Pi_{\mathsf{Ecd}}, \mathcal{A}, \mathcal{Z}, \mathcal{E}, k}(1^\lambda)$ *is defined as follows.*

1. *The challenger samples the public parameters and the secret key* $(\mathsf{pp}, \mathsf{sk}) \leftarrow \mathsf{Gen}(1^\lambda)$, *together with* $\alpha$ *and* $s$ *sampled uniformly from* $(R/pR)^\times$ *and a fixed subset of* $(R/pR)^\times$, *respectively. It computes* $\sigma$ *as follows:*

$$\begin{aligned} \sigma := \big(\mathsf{pk}, &\mathsf{Encode}(\mathsf{sk}, 1), \mathsf{Encode}(\mathsf{sk}, s), \ldots, \mathsf{Encode}(\mathsf{sk}, s^m), \\ &\mathsf{Encode}(\mathsf{sk}, \alpha), \mathsf{Encode}(\mathsf{sk}, \alpha s), \ldots, \mathsf{Encode}(\mathsf{sk}, \alpha s^m)\big) \ . \end{aligned}$$

   *It also computes* $z \leftarrow \mathcal{Z}(\sigma)$.

2. *Then it runs the extraction process with the outputs, as follows:*

$$\big((\mathbf{cw}, \mathbf{cw}'), (a_0, \ldots, a_m)\big) \leftarrow \langle \mathcal{A}, \mathcal{E}\rangle(1^\lambda, |\sigma, z\rangle, |0\rangle) \ .$$

   *The output of the experiment is* 1 *if* $\mathbf{cw}' - \alpha\mathbf{cw} \in C_0$ *and* $\mathbf{cw} \notin C_S$ *where* $S = \sum_{i=0}^m a_i s^i$. *Otherwise, the output of the experiment is* 0.

In [GMNO18, NYI+20, GNSV23], it is assumed that $\mathcal{Z}$ is "benign", in the sense that the auxiliary information $z$ is generated with a dependency on $\mathsf{sk}$, $s$ and $\alpha$ that is limited to the extent that it can be generated efficiently from $\sigma$. The extractor is also given the randomness of the adversary. In the quantum setting, we allow the extractor to have auxiliary inputs of the above type, while we omit the randomness of the adversary since it can be simulated by Hadamard gates and projective measurements.

In [GMNO18, NYI+20], the authors use $\mathsf{LWE}$ symmetric encryption (i.e., with $d = 1$) for the encoding scheme. The value of $m$ is of order $2^{15}$, which is significantly larger than the rank of the ciphertext space $n$ (chosen around $2^{10}$). The ciphertext modulus $q$ can be as large as 736 bits, whereas the plaintext modulus $p$ has 32 bits. The authors of [GNSV23] rely on high-degree $\mathsf{MLWE}$, whereas the (module) rank of their ciphertext space is constant.

In Definition 19, the adversary is given $2(m+1)$ encodings of the powers of $s$. We use them to define the following matrix:

$$\mathbf{C} := \left(\begin{array}{c|c|c|c} \mathsf{Encode}(\mathsf{sk}, 1) & \mathsf{Encode}(\mathsf{sk}, s) & \cdots & \mathsf{Encode}(\mathsf{sk}, s^m) \\ \mathsf{Encode}(\mathsf{sk}, \alpha) & \mathsf{Encode}(\mathsf{sk}, \alpha s) & & \mathsf{Encode}(\mathsf{sk}, \alpha s^m) \end{array}\right) \in (R/qR)^{2n \times (m+1)} \ .$$

A small combination $\mathbf{Ce}$ of the columns gives a pair of ciphertext $(\mathbf{cw}, \mathbf{cw}')$ that satisfies $\mathbf{cw} - \alpha\mathbf{cw}' \in C_0$, by the $(m+1)$-linear homomorphism property of the scheme. The vectors $\mathbf{cw}$ and $\mathbf{cw}'$ respectively correspond to the first and second halves of $\mathbf{Ce}$. Note that the auxiliary input $z$ does not help to recover $\mathbf{e}$. It contains codewords of the form $\mathsf{Encode}(\mathsf{sk}, \beta v(s))$ where $v$ is a publicly

known polynomial and $\beta$ is a uniformly sampled element from $R/pR$ that is independent from all other parameters. This does not help the adversary to extract information about the matrix $\mathbf{C}$, as can be shown using a hybrid argument in which one replaces the plaintext $\beta v(s)$ with a garbage plaintext (using the fact that the codewords are indistinguishable from uniform). By adapting the arguments from Subsection 6.3, it can be seen that sampling $\mathbf{Ce}$ obliviously allows to break the security assumption of Definition 19.

Acknowledgments.

The authors are grateful to Dan Boneh, André Chailloux, Omar Fawzi, Alex Grilo, Yuval Ishai, Amit Sahai, Jean-Pierre Tillich and David Wu for insightful discussions. The authors particularly thank Jean-Pierre Tillich and André Chailloux for the reference to the POVM from [CB98] and discussions pertaining to its implementation. The work of Thomas Debris-Alazard was funded by the French Agence Nationale de la Recherche through ANR JCJC COLA (ANR-21-CE39-0011). The authors were supported by the PEPR quantique France 2030 programme (ANR-22-PETQ-0008).

## References


[ACL+22] Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan. Lattice-based SNARKs: Publicly verifiable, preprocessing, and recursively composable. In *CRYPTO*, 2022.

[AD17] Martin R. Albrecht and Amit Deo. Large modulus ring-LWE $\geq$ module-LWE. In *ASIACRYPT*, 2017.

[AFLN23] Martin R. Albrecht, Giacomo Fenzi, Oleksandra Lapiha, and Ngoc Khanh Nguyen. SLAP: Succinct lattice-based polynomial commitments from standard assumptions. 2023. Available at https://eprint.iacr.org/2023/1469.

[AG11] Sanjeev Arora and Rong Ge. New algorithms for learning in presence of errors. In *ICALP*, 2011.

[Ban93] Wojciech Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Math. Ann.*, 1993.

[BCI+13] Nir Bitansky, Alessandro Chiesa, Yuval Ishai, Rafail Ostrovsky, and Omer Paneth. Succinct non-interactive arguments via linear interactive proofs. In *TCC*, 2013.

[BCPR16] Nir Bitansky, Ran Canetti, Omer Paneth, and Alon Rosen. On the existence of extractable one-way functions. *SIAM J. Comput.*, 2016.

[BD20] Zvika Brakerski and Nico Döttling. Hardness of LWE on general entropic distributions. In *EUROCRYPT*, 2020.

[BGV12] Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In *ITCS*, 2012.

[BISW17] Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu. Lattice-based SNARGs and their application to more efficient obfuscation. In *EUROCRYPT*, 2017.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *STOC*, 2013.

[BSCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. Interactive oracle proofs. In *TCC-B*, 2016.

[CB98] Anthony Chefles and Stephen M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A*, 1998.

[CDPR16] Ronald Cramer, Léo Ducas, Chris Peikert, and Oded Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT*, 2016.

[CDW21] Ronald Cramer, Léo Ducas, and Benjamin Wesolowski. Mildly short vectors in cyclotomic ideal lattices in quantum polynomial time. *J. ACM*, 2021.

[CKKK23] Heewon Chung, Dongwoo Kim, Jeong Han Kim, and Jiseung Kim. Amortized efficient zk-SNARK from linear-only RLWE encodings. *J. Comm. Netw.*, 2023.

[CLZ22] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In *EUROCRYPT*, 2022.

[CT23] André Chailloux and Jean-Pierre Tillich. The quantum decoding problem. 2023. Available at https://eprint.iacr.org/2023/1686.

[Dam91] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In *CRYPTO*, 1991.

[DRT23] Thomas Debris-Alazard, Maxime Remaud, and Jean-Pierre Tillich. Quantum reduction of finding short code vectors to the decoding problem. June 2023. arXiv:2106.02747.

[dW23] Ronald de Wolf. Quantum computing: Lecture notes, 2023. Available at https://arxiv.org/abs/1907.09415.

[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct NIZKs without PCPs. In *EUROCRYPT*, 2013.

[GKPV10] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In *ICS*, 2010.

[GMNO18] Rosario Gennaro, Michele Minelli, Anca Nitulescu, and Michele Orrù. Lattice-based ZK-SNARKs from square span programs. In *CCS*, 2018.

[GNSV23] Chaya Ganesh, Anca Nitulescu, and Eduardo Soria-Vazquez. Rinocchio: SNARKs for ring arithmetic. *J. Cryptol.*, 2023.

[GR02] Lov Grover and Terry Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions, 2002. Available at https://arxiv.org/abs/quant-ph/0208112.

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In *STOC*, 2011.

[ISW21] Yuval Ishai, Hang Su, and David J. Wu. Shorter and faster post-quantum designated-verifier zkSNARKs from lattices. In *CCS*, 2021.

[LMSV12] Jake Loftus, Alexander May, Nigel P. Smart, and Frederik Vercauteren. On CCA-secure somewhat homomorphic encryption. In *SAC*, 2012.

[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 *EUROCRYPT*, 2023.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *EUROCRYPT*, 2010.

[LS15] Adeline Langlois and Damien Stehlé. Worst-case to average-case reductions for module lattices. *Des. Codes Cryptogr.*, 2015.

[MM11] Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of LWE search-to-decision reductions. In *CRYPTO*, 2011.

[Nao03] Moni Naor. On cryptographic assumptions and challenges. In *CRYPTO*, 2003.

[NC11] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2011.

[NYI+20] Ken Naganuma, Masayuki Yoshino, Atsuo Inoue, Yukinori Matsuoka, Mineaki Okazaki, and Noboru Kunihiro. Post-quantum zk-SNARK for arithmetic circuits using QAPs. In *AsiaJCIS*, 2020.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *STOC*, 2009.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 2009.

[SSEK22] Ron Steinfeld, Amin Sakzad, Muhammed F. Esgin, and Veronika Kuchta. Private re-randomization for module LWE and applications to quasi-optimal ZK-SNARKs, 2022. Available at https://eprint.iacr.org/2022/1690.

[SSTX09] Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In *ASIACRYPT*, 2009.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[WW23] Hoeteck Wee and David J. Wu. Lattice-based functional commitments: Fast verification and cryptanalysis. In *ASIACRYPT*, 2023.

## Appendix A. Quantum Unambiguous Measurement from [CB98]

A.1. **Positive operator-valued measures.** Positive Operator-Valued Measures (POVM) are defined as follows. They are the most general measurements allowed within quantum information theory.

**Definition 20** (POVM measurements)**.** *A* POVM *is a set* $\{\mathbf{E}_i\}_{i\in\mathcal{I}}$ *of positive operators where* $\mathcal{I}$ *is the set of measurement outcomes and the operators satisfy* $\sum_i \mathbf{E}_i = \mathbf{Id}$*. A measurement upon a quantum state* $|\psi\rangle$ *outputs* $i$ *with probability* $\langle\psi|\,\mathbf{E}_i\,|\psi\rangle$*.*

POVMs are sometimes considered in the following situation: given a set of quantum states $|\psi_1\rangle, \ldots, |\psi_N\rangle$, devise a POVM that when applied over $|\psi_j\rangle$, it either outputs the correct index $j$ or some special symbol $\perp$ representing the "unknown" answer. In other words, the measurement never makes an error when it succeeds to identify the prepared state and we say that it *unambiguously* distinguishes the states $|\psi_j\rangle$'s. The probability of error is defined as the probability that the measurement outputs $\perp$, when it is maximized over all possible input states:

$$p_\perp := \max_k \langle\psi_k|\,\mathbf{E}_\perp\,|\psi_k\rangle$$

where $\mathbf{E}_\perp$ corresponds to the outcome $\perp$.

A.2. **Discrimination of coordinate states.** We now describe the POVM from [CB98], which is known to be optimal to unambiguously distinguish the $|\psi_k\rangle$'s (as given in Definition 13). Namely, it minimizes the error parameter $p_\perp$ over all possible choice of POVMs. This optimality is enabled by the fact that the $|\psi_k\rangle$'s verify the following "symmetry" condition:

$$\forall k \in \mathbf{Z}/q\mathbb{Z}, \quad \mathbf{T}\,|\psi_k\rangle = |\psi_{k+1 \bmod q}\rangle \ ,$$

where $\mathbf{T}$ denotes the translation operator, i.e., $\mathbf{T}\,|a\rangle = |a+1 \bmod q\rangle$ for all $a$, and from the fact that they are linearly independent (which is ensured by $\widehat{f}(x) \neq 0$ for all $x$, as is the case for our instantiation with the folded Gaussian distribution).

**Theorem 7** (Adapted from [CB98])**.** *Let* $q$ *be an integer and* $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ *be an amplitude function such that* $\widehat{f}(y) \neq 0$ *for every* $y \in \mathbb{Z}/q\mathbb{Z}$*. Let*

$$\left|\psi_j^\perp\right\rangle := \frac{1}{\sqrt{N}} \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \overline{\widehat{f}(-y)^{-1}}\ \omega_q^{-jy}\,|\chi_y\rangle\,, \ \text{where}\ \ N := \sum_{y\in\mathbb{Z}/q\mathbb{Z}}^{q-1} |\widehat{f}(y)|^{-2}\ , \tag{25}$$

*and*

$$\forall j \in \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{E}_j := \frac{1}{\lambda_+}\left|\psi_j^\perp\right\rangle\!\left\langle\psi_j^\perp\right|\,, \ \text{and}\ \mathbf{E}_\perp := \mathbf{I} - \sum_{j\in\mathbb{Z}/q\mathbb{Z}} \mathbf{E}_j\ ,$$

*where* $\lambda_+$ *is the maximum eigenvalue of* $\sum_{j\in\mathbb{Z}/q\mathbb{Z}} \left|\psi_j^\perp\right\rangle\!\left\langle\psi_j^\perp\right|$*. Then the set* $\{\mathbf{E}_j\}_{j\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ *is a* POVM *that unambiguously distinguishes the coordinate states with success probability* $p$ *as follows (it is independent of* $j$*):*

$$p = \langle\psi_j|\,\mathbf{E}_j\,|\psi_j\rangle = q \cdot \min_{y\in\mathbb{Z}/q\mathbb{Z}} \left|\widehat{f}(y)\right|^2\ .$$

Representating the coordinate states in the Fourier basis is helpful to approach the problem. The first lemma shows that $\left|\psi_i^\perp\right\rangle$ defined as in Equation (25) is a quantum state orthogonal to all $|\psi_j\rangle$'s where $i \neq j$.

**Lemma 26.** *Using the notations of Theorem 7, we have:*

$$\forall i,j \in \mathbb{Z}/q\mathbb{Z}, \quad \left\langle\psi_i^\perp\middle|\psi_j\right\rangle = \begin{cases} \frac{q}{\sqrt{N}} & \text{if } j = i \\ 0 & \text{otherwise} \end{cases}\ .$$

*Proof.* Let us write the $|\psi_j\rangle$'s in the Fourier basis. We have for all $j \in \mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned}
|\psi_j\rangle &= \sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e)\,|j+e \bmod q\rangle \\
&= \frac{1}{\sqrt{q}} \sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e) \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{-(j+e)x}\,|\chi_x\rangle \quad \text{(by Lemma 1)} \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \left( \frac{1}{\sqrt{q}} \sum_{e\in\mathbb{Z}/q\mathbb{Z}} f(e)\,\omega_q^{-xe} \right) \omega_q^{-jx}\,|\chi_x\rangle \\
&= \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x)\,\omega_q^{-jx}\,|\chi_x\rangle \ .
\end{aligned}$$

We thus have, for all $i \in \mathbb{Z}/q\mathbb{Z}$:

$$\langle\psi_i^\perp|\psi_j\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{x(i-j)} = \begin{cases} \frac{q}{\sqrt{N}} & \text{if } j = i \\ 0 & \text{otherwise} \end{cases} \ .$$

This completes the proof. □

We now consider the maximum eigenvalue $\lambda_+$ of $\sum_{j\in\mathbb{Z}/q\mathbb{Z}} |\psi_j^\perp\rangle\langle\psi_j^\perp|$.

**Lemma 27.** *Using notations of Theorem 7, we have:*

$$\lambda_+ = \frac{q}{N} \frac{1}{\min\limits_{x\in\mathbb{Z}/q\mathbb{Z}} \left|\widehat{f}(x)\right|^2} \ .$$

*Proof.* We have the following equalities:

$$\begin{aligned}
\sum_{j\in\mathbb{Z}/q\mathbb{Z}} |\psi_j^\perp\rangle\langle\psi_j^\perp| &= \frac{1}{N} \sum_{j\in\mathbb{Z}/q\mathbb{Z}} \left( \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \overline{\widehat{f}(-x)^{-1}}\,\omega_q^{-jx}\,|\chi_x\rangle \right) \left( \sum_{y\in\mathbb{Z}/q\mathbb{Z}} \widehat{f}(-y)^{-1}\,\omega_q^{jy}\,\langle\chi_y| \right) \\
&= \frac{1}{N} \sum_{x,y\in\mathbb{Z}/q\mathbb{Z}} \left( \sum_{j\in\mathbb{Z}/q\mathbb{Z}} w_q^{j(y-x)} \right) \overline{\widehat{f}(-x)^{-1}}\,\widehat{f}(-y)^{-1}\ |\chi_x\rangle\langle\chi_y| \\
&= \frac{q}{N} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} |\widehat{f}(-x)|^{-2}\,|\chi_x\rangle\langle\chi_x| \ .
\end{aligned}$$

Therefore, as the $|\chi_x\rangle$'s define an orthonormal basis of the underlying Hilbert space, we obtain

$$\lambda_+ = \frac{q}{N} \frac{1}{\min\limits_{x\in\mathbb{Z}/q\mathbb{Z}} \left|\widehat{f}(x)\right|^2} \ .$$

This completes the proof. □

*Proof of Theorem 7.* The fact that $\{\mathbf{E}_j\}_{j\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ defines a POVM follows from the definition of $\lambda_+$: they are positive operators and sum to the identity.

By Lemma 26, the state $|\psi_i^\perp\rangle$ is orthogonal to $|\psi_j\rangle$ for all $j \neq i$. Therefore, given $|\psi_j\rangle$, the probability to successfully measure $j$ with the POVM $\{\mathbf{E}_i\}_{i\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ is given by

$$p = \langle\psi_j|\,\mathbf{E}_j\,|\psi_j\rangle = \frac{1}{\lambda_+} \left|\langle\psi_j^\perp|\psi_j\rangle\right|^2 = \frac{q^2}{\lambda_+\,N} = q \cdot \min_{y\in\mathbb{Z}/q\mathbb{Z}} \left|\widehat{f}(y)\right|^2 ,$$

where the two last equalities follow from Lemmas 26 and 27. □

## Appendix B. Proof of Lemma 18

Recall that

$$\forall e \in \mathbb{Z} : \vartheta_{\sigma,q}(e) = \frac{1}{\rho_\sigma(\mathbb{Z})} \sum_{k\in\mathbb{Z}} \exp\left(-\frac{|e+qk|^2}{\sigma^2}\right) .$$

Let $A, B : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be defined as follows:

$$\forall y \in \mathbb{Z}/q\mathbb{Z} : A(y) := \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \omega_q^{xy} \left(\sqrt{\vartheta_{\sigma,q}(x)} - \sqrt{D_{\mathbb{Z},\sigma}(x)}\right),$$

$$\forall y \in \mathbb{Z}/q\mathbb{Z} : B(y) := \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \omega_q^{xy} \left(\frac{\sum_{k\in\mathbb{Z}} \rho_{\sqrt{2}\sigma}(x+kq)}{\sqrt{\rho_\sigma(\mathbb{Z})}} - \sqrt{D_{\mathbb{Z},\sigma}(x)}\right).$$

Then, for all $y \in \mathbb{Z}/q\mathbb{Z}$, it holds that

$$\begin{aligned}\widehat{f}_0(y) &= \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{xy} \sqrt{\vartheta_{\sigma,q}(x)} \\ &= \frac{1}{\sqrt{q}} \left(A(y) - B(y) + \sum_{x\in\mathbb{Z}/q\mathbb{Z}} \omega_q^{xy} \frac{\sum_{k\in\mathbb{Z}} \rho_{\sqrt{2}\sigma}(x+kq)}{\sqrt{\rho_\sigma(\mathbb{Z})}}\right).\end{aligned}$$

By the Poisson summation formula, the above term is equal to:

$$\frac{1}{\sqrt{q}}\left(A(y) - B(y) + \sum_{\ell\in\mathbb{Z}} \omega_q^{\ell y} \frac{\rho_{\sqrt{2}\sigma}(\ell)}{\sqrt{\rho_\sigma(\mathbb{Z})}}\right) = \frac{1}{\sqrt{q}}\left(A(y) - B(y) + \frac{\sqrt{2}\sigma}{\sqrt{\rho_\sigma(\mathbb{Z})}} \sum_{\ell\in\mathbb{Z}} \rho_{\frac{1}{\sqrt{2}\sigma}}\left(\ell + \frac{y}{q}\right)\right) . \quad (26)$$

We now find upper bounds for the terms $A(y)$ and $B(y)$ and a lower bound for the remaining term of Equation (26). Using the fact that $\sqrt{\rho_\sigma} = \rho_{\sqrt{2}\sigma}$, we have, for all $y \in \mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned}B(y) &= \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \omega_q^{xy} \left(\frac{\sum_{k\in\mathbb{Z}} \rho_{\sqrt{2}\sigma}(x+kq)}{\sqrt{\rho_\sigma(\mathbb{Z})}} - \sqrt{D_{\mathbb{Z},\sigma}(x)}\right) \\ &= \frac{\rho_{\sqrt{2}\sigma}(\mathbb{Z})}{\sqrt{\rho_\sigma(\mathbb{Z})}} \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \omega_q^{xy} \left(\vartheta_{\sqrt{2}\sigma,q}(x) - D_{\mathbb{Z},\sqrt{2}\sigma}(x)\right).\end{aligned}$$

By the triangular inequality, it follows that

$$\begin{aligned}|B(y)| &\le \frac{\rho_{\sqrt{2}\sigma}(\mathbb{Z})}{\sqrt{\rho_\sigma(\mathbb{Z})}} \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \left(\vartheta_{\sqrt{2}\sigma,q}(x) - D_{\mathbb{Z},\sqrt{2}\sigma}(x)\right) \\ &\le \frac{\rho_{\sqrt{2}\sigma}(\mathbb{Z})}{\sqrt{\rho_\sigma(\mathbb{Z})}}\, q\, \mathrm{e}^{-\frac{q^2}{8\sigma^2}} \quad \text{(by Lemma 4)} .\end{aligned}$$

The use of Lemma 4 requires that $\sigma \le q/2$, which is implied by our assumptions.

We also have, for all $y \in \mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned}|A(y)| &\le \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \left(\sqrt{\vartheta_{\sigma,q}(x)} - \sqrt{D_{\mathbb{Z},\sigma}(x)}\right) \quad \text{(by the triangular inequality)} \\ &\le \sum_{x\in\mathbb{Z}\cap(-q/2,q/2]} \mathrm{e}^{-\frac{q^2}{8\sigma^2}} \quad \text{(by Lemma 4)} \\ &= q\, \mathrm{e}^{-\frac{q^2}{8\sigma^2}} .\end{aligned}$$

Further, for every $y \in \mathbb{Z}$, it holds that

$$\sum_{\ell\in\mathbb{Z}} \rho_{\frac{1}{\sqrt{2}\sigma}}\left(\ell + \frac{y}{q}\right) \ge \mathrm{e}^{-\pi\frac{\sigma^2}{8}} .$$

To see this, note that the sum contains at least one term $\ell + y/q$ that has absolute value $\leq 1/2$.

Going back to Equation (26) and using the triangular inequality, we see that, for all $y \in \mathbb{Z}/q\mathbb{Z}$:

$$\begin{aligned}
|\widehat{f_0}(y)| &\leq \tfrac{1}{\sqrt{q}} \left( \tfrac{\sqrt{2}\sigma}{\sqrt{\rho_\sigma(\mathbb{Z})}} \mathrm{e}^{-\pi \frac{\sigma^2}{8}} + q\ \mathrm{e}^{-\frac{q^2}{8\sigma^2}} + \tfrac{\rho_{\sqrt{2}\sigma}(\mathbb{Z})}{\sqrt{\rho_\sigma(\mathbb{Z})}}\ q\ \mathrm{e}^{-\frac{q^2}{8\sigma^2}} \right) \\
&\leq \tfrac{1}{\sqrt{q}} \left( \sqrt{2\sigma} \mathrm{e}^{-\pi \frac{\sigma^2}{8}} + q\ \mathrm{e}^{-\frac{q^2}{8\sigma^2}} + \tfrac{\sqrt{2}\sigma+1}{\sqrt{\sigma}}\ q\ \mathrm{e}^{-\frac{q^2}{8\sigma^2}} \right) \\
&\leq \tfrac{4\sqrt{\sigma}}{\sqrt{q}} \left( \mathrm{e}^{-\pi \frac{\sigma^2}{8}} + q\ \mathrm{e}^{-\frac{q^2}{8\sigma^2}} \right) ,
\end{aligned}$$

where the second inequality follows from Lemma 3 and the third one from $\sigma \geq 1$. □