OBLIVIOUS LWE SAMPLING IN QUANTUM POLYNOMIAL TIME

THOMAS DEBRIS–ALAZARD [1,2], POURIA FALLAHPOUR [3], AND DAMIEN STEHLÉ [3,4]

Abstract. XXX

1. Introduction

The Learning With Errors (LWE) problem [Reg09] is well-known for its conjectured intractability for quantum algorithms, inherited from the worst-case hardness of 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 χ 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 χ consists in recovering the secret $\mathbf{s}$ from the LWE instance $(\mathbf{A}, \mathbf{As}+\mathbf{e}) \in (\mathbb{Z}/q\mathbb{Z})^{m\times n} \times (\mathbb{Z}/q\mathbb{Z})^m$. 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 χ. 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 $\mathbf{b} = \mathbf{As} + \mathbf{e}$:

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

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 $\mathbf{b} = \mathbf{As} + \mathbf{e}$. This is provided by m being sufficiently large as a function of n, q and χ. Informally, the correct $\mathbf{b}$'s are extremely sparse in their range. The naive approach of sampling a uniform $\mathbf{b}$ and keeping it if it has the correct form is therefore 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 $\mathbf{As} + \mathbf{e}$. This leads us to the following question:

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

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 occurence 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 sample $\mathbf{b} = \mathbf{As} + \mathbf{e}$ belonging to the ciphertext space $(\mathbb{Z}/q\mathbb{Z})^m$, and that the plaintext of a well-formed ciphertext is a function of $\mathbf{s}$. 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 $\mathbf{b} = \mathbf{As} + \mathbf{e}$, 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 Short Non-interactive Arguments of Knowledge (SNARKs) from lattice assumptions [BISW18, GMNO18, ISW21, ACL+22, SSEK22, CKKK23, CLM23, GNSV23]. 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 $\mathbf{eB} \in (\mathbb{Z}/q\mathbb{Z})^{m-n}$ where $\mathbf{B}$ is typically uniform and each coefficient of $\mathbf{e}$ is i.i.d. from χ. 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 $\mathbf{eB}$ 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 is oblivious under the assumption that LWE is intractable. Under the assumption that oblivious LWE sampling is hard classically, 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]. All 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 definition was put forward in [LMZ23]. We propose an alternative definition that, in our opinion, better models what an extractor could be allowed to do. 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

$$\sum_{\mathbf{s},\mathbf{e}} f(\mathbf{e})^2 \left|\mathbf{As}+\mathbf{e}\right\rangle \ ,$$

up to normalization, and then measure it. Here f is a complex-valued function f, and if there are auxiliary registers, then they are all set to 0. The output is indeed an LWE sample $\mathbf{As}+\mathbf{e}$ for the intput matrix $\mathbf{A}$. We show that any such quantum algorithm is an oblivious LWE sampler for the error distribution proportional to $|f(\cdot)|^2$ (under the assumption that LWE is hard).

Next, we modify the 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 discrete integer Gaussian distribution, i.e., with $|f(\mathbf{e})|^2 = \sum_{\mathbf{k}\in\mathbb{Z}^m} \exp\big(-\|\mathbf{e}+q\mathbf{k}\|^2/\sigma^2\big)$ for any $\mathbf{e} \in \mathbb{Z}^m$ and up to a normlization factor. Our result requires that the standard deviation parameter σ satisfies $\sigma \geq \mathit{TOBECOMPLETED}$.

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 assumptions do not hold against quantum algorithms. For TO BE COMPLETED, we also provide cryptanalyses against the schemes. As a result, these constructions should not be considered as post-quantum.

1.1. **Technical overview.**

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

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 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 $\mathbf{b} = \mathbf{As}+\mathbf{e}$. 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 $\mathcal{A}$, 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 necessarily 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 measures 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 final measurement (on all registers)[1], and then the measurement outcome 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 $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$ and the measurement of 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 seems 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 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 no extractor was inspecting the sampler at all. Namely, if ρ_{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 $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}) = \rho_{\mathsf{Q}}$.

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 definition 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 LWE setting. Assume that there is a reduction $\mathcal{A}$ from an LWE variant LWE_1 to another LWE variant LWE_2 such that (i) an instance of LWE_1 is mapped to an instance of LWE_2 (with appropriate distribution over the randomness of the LWE_1 instance and the random coins of LWE_2, and (ii) a solution to the LWE_1 instance can be obtained from a solution to the LWE_2 instance. Then applying the reduction $\mathcal{A}$ to an oblivious LWE_1 sampler gives an oblivious LWE_2 sampler. In our case, this observation will prove useful to weaken parameter constraints on LWE for

[1] **[Pouria : it does not necessary perform the measurement on all registers. it might have quantum ouput that should also be given to the extractor.]**

oblivious sampling: we will first obtain an oblivious sampler for some restricted parametrization of LWE and extend it to more general setups thanks to existing such reductions.

1.1.2. *A general approach to oblivious* LWE *sampling:* $|\mathsf{LWE}\rangle$. Bibliography: CLZ21 (and previous works), the new paper, old papers: Regev + SSTX + BKSW

Failure 1: Regev

Failure 2: CLZ (mauvaise mesure mais il y a un cote intrinseque, Arora-Ge)

1.1.3. *Warm-up: solving* $|\mathsf{LPN}\rangle$. JP+A: change la mesure pour un POVM, dans le but de trouver des vecteurs cours dans le code dual. Mais echec a la zone facile.

Dans notre cas, on s'en fout de SIS, et on peut ajouter des phases.

1.1.4. *An efficient* $|\mathsf{LWE}\rangle$ *algorithm.* On reutilise les deux idees : un bon POVM (mais ca suffit, le fhat est tout moisi), et des phases.

1.1.5. *Application to lattice-based SNARKs.*

2. Preliminaries

General notations. The notation $x \overset{\text{def}}{=} y$ means that x is defined to be equal to y. Given a finite set $\mathcal{S}$, we let $|\mathcal{S}|$ denote its cardinality. We distinguish an ordered set of elements a_i's by writing $(a_i)_i$ instead of $\{a_i\}_i$. For a and b integers with $a \leq b$, we let $[\![a,b]\!]$ denote the set of integers $\{a, a+1, \cdots, b\}$. For every $x \in \mathbb{R}$, its floor $\lfloor x \rfloor$ is the largest integer smaller than or equal to x, and its ceil $\lceil x \rceil$ is the smallest integer larger than or equal to x. We define $\mathbb{N}$ as the set of natural numbers $\{1, 2, 3, \cdots\}$. We let $\mathrm{B}_m(r)$ denote the m-dimensional ball with radius r. We will often consider the additive group $\mathbb{Z}/q\mathbb{Z}$ and write its elements as

$$\mathbb{Z}/q\mathbb{Z} = \left\{ j \; : \; -\lceil \frac{q}{2} \rceil \leq j \leq \lfloor \frac{q}{2} \rfloor \right\}.$$

For any integer $q \geq 2$, the canonical q-th root of unity will be denoted ω_q, namely

$$\omega_q \overset{\text{def}}{=} e^{\frac{2\pi i}{q}}.$$

Vectors are in column notation and they will be written with bold letters (such as $\mathbf{x}$). Uppercase bold letters are used to denote matrices (such as $\mathbf{A}$). When it is necessary, we use a subscript to denote the dimension of a matrix, for instance $\mathbf{A}_{m \times n}$, and whenever $m = n$, we simply write $\mathbf{A}_n$. For two vectors $\mathbf{x}$ and $\mathbf{y}$, we let $(\mathbf{x} \mid \mathbf{y})$ denote the horizontal concatenation of columns $\mathbf{x}$ and $\mathbf{y}$. For every two vectors $\mathbf{x}, \mathbf{y} \in (\mathbb{Z}/q\mathbb{Z})^d$, we define their inner product as

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

We define the Euclidean norm of $\mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^d$ as,

$$\|\mathbf{x}\| \overset{\text{def}}{=} \sqrt{\sum_{i=1}^{d} \min(x_i, q - x_i)^2}. \tag{1}$$

For real-valued functions defined over $\mathbb{R}$ or $\mathbb{N}$, we define $o(\cdot), \omega(\cdot), O(\cdot)$ 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 $\Omega_n(\cdot)$. We let $\mathsf{poly}(n)$ denote any function which is of order $O(n^a)$ for some constant a. Furthermore, $\mathsf{negl}(n)$ will be defined as any function being of order $O(1/n^b)$ for every constant $b > 0$.

We let $\mathsf{Desc}(M)$ denote the binary description of the algorithm M in some arbitrary computational model. The exact choice of the model is irrelevant to our purposes, but it can be assumed that we use (quantum) circuit model of computation. 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 Ω 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 $(X_1, \cdots, X_m)$ 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:

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

Let $f : S \to \mathbb{C}$ be a function. We define the function $f^{\otimes d} : S^d \to \mathbb{C}$ over the tuple $(x_1, \cdots, x_d)$ to be

$$f^{\otimes d}(x_1, \cdots, x_d) \overset{\text{def}}{=} f(x_1) \cdots f(x_d).$$

When the dimension d is clear from the context, we abuse the notation and write f instead of any tensor power $f^{\otimes d}$.

2.1. **Quantum Computation.** All the necessary material about quantum computation can be found in [NC11, Wat18]. However, we will cover some here, for the sake of convenience.

Quantum algorithms. A quantum algorithm is a series of unitary operators and projective measurements that is allowed to use ancilla registers and trace out some of its registers during the execution. Usually the outcome of the last measurement is considered as the output of the algorithm.

A uniform quantum polynomial-time algorithm is a BQP Turing machine defined as in [BV97, Def 8.1]. We let QPT denote all such algorithms. Equivalently, one can always use the following model of computation.

Definition 1 (Universal Gates)**.** *A finite set of* 1*-qubit or* 2*-qubit elements* $\mathcal{G}$ *of* $SU(2)$ *is said to be universal if for any unitary* $\mathbf{U} \in SU(d)$ *and any* $\varepsilon > 0$*, there exists* $\mathbf{G}_t, \mathbf{G}_{t-1}, \cdots, \mathbf{G}_1 \in \mathcal{G}$*, such that*

$$\|\mathbf{U} - \widetilde{\mathbf{G}_t}\widetilde{\mathbf{G}_{t-1}} \cdots \widetilde{\mathbf{G}_1}\| \leq \varepsilon,$$

where $\widetilde{\mathbf{G}}$ *is the canonical extension of* $\mathbf{G} \in SU(2)$ *to* $SU(d)$*, and* $\|\mathbf{A}\| = \max_{\mathbf{v}} \frac{\|\mathbf{A}\mathbf{v}\|}{\|\mathbf{v}\|}$ *is the spectral norm.*

Let $\mathcal{G}$ be a fixed universal set of gates. Every algorithm can be approximated by $\mathcal{G}$ as above and the measurements in the computational basis, within negligible distance with respect to $\log(\dim(\mathcal{H}))$ where $\mathcal{H}$ is the working space of the algorithm. Given a algorithm in $\mathcal{G}$, its runtime is defined as the number of its gates plus the number of measurements in the computational basis. The following theorem establishes the robustness of the runtime definition for BQP machines. In other words, the asymptotics of the runtime is independent from the choice of $\mathcal{G}$.

Lemma 1 (Solovay-Kitaev Theorem)**.** *If* $\mathcal{G}$ *is a universal set of gates that is closed under inverse (for every* $\mathbf{G} \in \mathcal{G}$*, we have* $\mathbf{G}^{-1} \in \mathcal{G}$*), then for every unitary* $\mathbf{U} \in SU(2)$ *there exists* $\mathbf{G}_t, \mathbf{G}_{t-1}, \cdots, \mathbf{G}_1 \in \mathcal{G}$ *such that*

$$\|\mathbf{U} - \mathbf{G}_t\mathbf{G}_{t-1} \cdots \mathbf{G}_1\| \leq \varepsilon, \text{ and } t = O(\log^2 \frac{1}{\varepsilon}).$$

As a consequence of this theorem, any quantum algorithm with k constant-qubit unitries can be apprximated within error ε using $O(k \log^c(k/\varepsilon))$ gates in $\mathcal{G}$. Therefore, one can verify that every BQP machine can be approximated within negligible distance using only polynomial number of gates. We say that a QPT algorithm is *unitary* if it only applies unitary gates during the execution followed by a single final measurement determining its output.

Positive Operator-Valued Measure (POVM) and quantum state discrimination. An operator $\mathbf{A}$ is said to be Hermitian if there exists a finite orthonormal basis $\{|i\rangle\}_i$, and real numbers $\{\lambda_i\}_i$ such that

$$\mathbf{A} = \sum_i \lambda_i |i\rangle\langle i|.$$

Given a function $f : \mathbb{R} \to \mathbb{R}$, the operator $f(\mathbf{A})$ is defined as $f(\mathbf{A}) = \sum_i f(\lambda_i) |i\rangle\langle i|$. Positive operators are Hermitian operators with non-negative λ_i's.

Positive Operator-Valued Measures (POVM) quantum measurements allowed within quantum information theory. They are defined as follows.

Definition 2 (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* $\sum_i \mathbf{E}_i = \mathbf{Id}$*. Performing a measurement upon a quantum state* $|\psi\rangle$*, outputs* i *with probability* $\langle\psi|\,\mathbf{E}_i\,|\psi\rangle$*.*

The problem of distinguishing quantum states is defined as follows. Given a set of quantum states $|\psi_1\rangle, \cdots, |\psi_N\rangle$, devise a quantum measurement such that when applied over $|\psi_j\rangle$, it outputs the correct index j. One can proceed as follows when the states form an orthonormal set. Consider the well-defined projective measurement $\mathbf{E}_i \overset{\text{def}}{=} |\psi_i\rangle\langle\psi_i|$ for $1 \leq i \leq N$. Then, if the state $|\psi_j\rangle$ is given, the probability to see j as the outcome is $\langle\psi_j|\,\mathbf{E}_j^\dagger \mathbf{E}_j\,|\psi_j\rangle = 1$. In other words, the above quantum measurement perfectly distinguishes the quantum states. However, when the $|\psi_j\rangle$'s are not orthonormal, it is known that there exists no quantum measurement to perfectly distinguish them (see [NC11, Box 2.3]). Yet, it is still possible to distinguish them *unambiguously.* By this, we mean that it is possible to design a quantum measurement such that, given $|\psi_j\rangle$, it either outputs 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. The probability of error is defined as the maximal probability that the measurement outputs $\perp$ over all possible input states:

$$p_{\text{error}} \overset{\text{def}}{=} \max_j \langle\psi_j|\,\mathbf{E}_\perp\,|\psi_j\rangle\,,$$

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

Later, for our main result, we will use the POVM given in [CB98]. It is known to be "optimal" when the $|\psi_i\rangle$'s are linearly independent and satisfy some symmetric property. By optimal, we mean that it has the smallest p_{error} over all possible choice of POVMs.

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:

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

It is extended by linearity.

Trace distance. We will also use the *trace distance* which is defined over two quantum states ρ, σ as follows:

$$D_{\text{tr}}\left(\rho,\sigma\right) \overset{\text{def}}{=} \frac{1}{2}\operatorname{tr}\left(\sqrt{(\rho-\sigma)^\dagger(\rho-\sigma)}\right).$$

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 [NC11, Theorem 9.2]:

- For any joint states ρ, σ over $\mathcal{A}\otimes\mathcal{B}$, it holds that $D_{\text{tr}}(\operatorname{tr}_{\mathcal{B}}(\rho), \operatorname{tr}_{\mathcal{B}}(\sigma)) \leq D_{\text{tr}}(\rho,\sigma)$;
- For any quantum states ρ, σ, τ, it holds that $D_{\text{tr}}(\rho,\sigma) \leq D_{\text{tr}}(\rho,\tau) + D_{\text{tr}}(\tau,\sigma)$;
- For any quantum states ρ, σ, τ, it holds that $D_{\text{tr}}(\rho\otimes\tau, \sigma\otimes\tau) = D_{\text{tr}}(\rho,\sigma)$;
- For any quantum algorithm $\mathcal{Q}$ and any quantum states ρ, σ, it holds that $D_{\text{tr}}(\mathcal{Q}(\rho), \mathcal{Q}(\sigma)) \leq D_{\text{tr}}(\rho,\sigma)$.

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 ρ and σ, respectively. We have:

$$\Delta(X,Y) \leq D_{\text{tr}}(\rho,\sigma). \tag{2}$$

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:

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

The quantum states of the form

$$|\chi_x\rangle \overset{\text{def}}{=} \mathbf{QFT}\,|x\rangle$$

are called the *Fourier basis* (or dual of the *computational basis* $(|x\rangle)_{x\in\mathbb{Z}/q\mathbb{Z}}$).

The computational basis decomposes in the Fourier basis as shown in the following lemma.

Lemma 2. *It holds that*

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

Proof. We have the following equalities:

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

The proof is completed by applying $\mathbf{QFT}^{-1}$. □

The $\mathbf{QFT}$ is intimately connected to its "classical" counterpart: the discrete Fourier transform. Recall that the discrete Fourier transform of every function $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is defined as follows:

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

One can verify that for every function $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$, the following holds:

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

There is difference in runtime between classical and quantum Fourier transforms. The classical Fourier transform can be carried out in $O(q\log q)$, while the $\mathbf{QFT}$ takes only $O(\log q)$ steps.

We will use the simplified version of Poisson summation formula as follows.

Lemma 3 (Poisson Summation Formula)**.** *Let $f : \mathbb{R} \to \mathbb{R}$ be a function. It holds that*

$$\sum_{x\in\mathbb{Z}} e^{2\pi i x y} f(x) = \sum_{x\in\mathbb{Z}} \widehat{f}(x+y).$$

Amplitude function. The following definition characterizes the least condition of a function to be allowed to appear in the amplitudes of a quantum state.

Definition 3 (Amplitude Function)**.** *Let S be a 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.

One can efficiently build a quantum state for particular set of amplitudes using the following lemma.

Lemma 4 ([GR02])**.** *Let X be a random variable over $\mathbb{R}$ such that for every $a \le b \in \mathbb{R}$, the quantity $\mathbb{P}_X\,(a \le x \le b)$ is computable in constant time. Then one can build*

$$\sum_{s\in S} \sqrt{\frac{\mathbb{P}_X(s)}{\mathbb{P}_X(S)}}\,|s\rangle\,,$$

in $\mathsf{poly}(\log(|S|))$ *steps.*

2.2. **Algebraic Number Theory.** We recall some algebraic number theory background. The reader who is not interested in the cryptographic applications of our main theorem discussed in Section 6 can safely skip this part.

Let R be a ring. An ideal $\mathfrak{a}$ of R is an additive group that is closed under multiplication with the elements of R. The product of every two ideals $\mathfrak{a}$ and $\mathfrak{b}$ defined as below is also an ideal:

$$\mathfrak{a}\mathfrak{b} \overset{\text{def}}{=} \{ab \mid a \in \mathfrak{a}, b \in \mathfrak{b}\}.$$

A proper ideal $\mathfrak{p} \subset R$ is said to be prime if for every $ab \in R$ such that $ab \in \mathfrak{p}$ it holds that either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are coprime if $\mathfrak{a} + \mathfrak{b} = R$. A maximal ideal $\mathfrak{a}$ is the one such that $R/\mathfrak{a}$ is a field.

Lemma 5 (Chinese Remainder Theorem (CRT))**.** *Let R be a ring and $\{\mathfrak{a}_1, \cdots, \mathfrak{a}_k\}$ be a collection of pairwise coprime ideals. Then we have*

$$R/(\mathfrak{a}_1 \cdots \mathfrak{a}_k) \simeq R/\mathfrak{a}_1 \times \cdots \times R/\mathfrak{a}_k$$

Number fields. A number field $K \overset{\text{def}}{=} \mathbb{Q}(\zeta)$ is an algebraic extension obtained by adjoining an algebraic number ζ to $\mathbb{Q}$. The degree of the number field is the rank of $\mathbb{Q}(\zeta)$ as a $\mathbb{Q}$-vector space. The ring of integers R of K is the set of all its algebraic integers. It is known that R is a *Dedekind* domain. Therefore, every prime ideal of R is also maximal. We have the following property about the ideals of R.

Lemma 6 ([NS13, Theorem 3.3])**.** *Every ideal $\mathfrak{a}$ of a ring of integers R except $\{0\}$ and R admits a unique prime factorization up to the orders of the factors.*

Every number field admits an integral basis, namely there exists elements $\{\alpha_1, \cdots, \alpha_d\} \subset R$ such that for all $x \in R$ there exist unique integers $x_1, \cdots, x_d$ such that we have

$$x = x_1\alpha_1 + \cdots + x_d\alpha_d.$$

Finding such a basis is not always efficient, but in this work we consider that it is given[2]. If such a basis exits, it would also be a basis for the number field which implies that d must be the degree of the extension.

We will be working with the following isomorphisms.

Definition 4. *Let $K \overset{def}{=} \mathbb{Q}(\zeta)$ be a degree d extension, R be its ring of integers, and q be an integer. We define the map $\phi : R \to \mathbb{Z}^d$ as follows:*

$$\forall x \in R: \ \phi(x) \overset{def}{=} (x_0, x_1, \cdots, x_{d-1}),$$

where the x_i's are the coefficients in an integral basis $\{\alpha_1, \cdots, \alpha_d\}$. We call ϕ the coefficient embedding.

Furthermore, for every $y \in R$, we define the map $\mathrm{T}_y : R \to R$ as follows:

$$\forall x \in R: \ \mathrm{T}_y(x) \overset{def}{=} yx.$$

We abuse the notation and also denote the modular variants of these maps over the domain R/qR by the same symbols. Note that the co-domains of ϕ and T_y over R/qR are $(\mathbb{Z}/q\mathbb{Z})^d$ and R/qR, respectively.

We have the following properties of ϕ and T_y based on the above discussion.

Lemma 7. *Let $K \overset{def}{=} \mathbb{Q}(\zeta)$ be a degree d extension, R be its ring of integers, and q be an integer. Then the coefficient embedding is an isomorphism. Furthermore, for every $y \in R/qR$, the matrix representation of T_y in a basis $\{\alpha_1, \cdots, \alpha_d\}$ belongs to $(\mathbb{Z}/q\mathbb{Z})^{d\times d}$.*

To sample elements from R/qR, we will consider the following type of distributions.

[2] In cryptographic applications, one only considers number fields for which such a basis is efficiently computable.

Definition 5 (Element-Wise i.i.d. Distribution)**.** *Let χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. A distribution over R/qR is called element-wise i.i.d. according to χ if $x \in R/qR$ is sampled as $\phi^{-1}(x_1, \cdots, x_d)$ where all the x_i's are independently distributed according χ over $\mathbb{Z}/q\mathbb{Z}$, and ϕ is the coefficient embedding of the number field.*

Cyclotomic number fields are used in cryptographic applications more than the others. In particular, all cases of cryptographic schemes that we discuss in Section 6 are of this type. We recall the definition here. We refer the reader to [NS13] for more details.

Definition 6 (Cyclotomic Fields)**.** *Let $n \geq 1$ be an integer. The n-th cyclotomic polynomial $\Phi_n(x)$ is defined as follows:*

$$\Phi_n(x) = \prod_{\substack{1 \leq k \leq n \\ \gcd(k,n)=1}} (x - \omega_n^k).$$

Then n-th cyclotomic field is the field extension $\mathbb{Q}(\omega_n) \simeq \mathbb{Q}[x]/\langle \Phi_n(x) \rangle$.

The degree of the n-th cyclotomic field is $\varphi(n)$ where φ is the Euler totient function. Its ring of integers is $\mathbb{Z}[\omega_n]$. The set $\{1, \omega_n, \omega_n^2, \cdots, \omega_n^{\varphi(n)-1}\}$ form an integral basis for the field.

Lemma 8. *Let q be an integer, then linear algebra is efficient over matrices with elements in $\mathbb{Z}[\omega_n]/q\mathbb{Z}[\omega_n]$.*

Proof. Let $q = p_1^{\alpha_1}, \cdots, p_k^{\alpha_k}$ be the prime decomposition of q in $\mathbb{Z}$. The ideals $\langle p_i^{\alpha_i} \rangle$ and $\langle p_j^{\alpha_j} \rangle$ are co-prime in $\mathbb{Z}[\omega_n]$ since there exists $a, b \in \mathbb{Z} \subset \mathbb{Z}[\omega_n]$ such that $ap_i^{\alpha_i} + bp_j^{\alpha_j} = 1$. Therefore, with the CRT, we obtain

$$\mathbb{Z}[\omega_n]/q\mathbb{Z}[\omega_n] \simeq \prod_i \mathbb{Z}[\omega_n]/\langle p_i^{\alpha_i} \rangle.$$

[Pouria : TODO: this is a Galois ring. Smith normal form of Galois ring. then linear system of equations.] □

2.3. **Lattices.** A lattice Λ is a discrete subgroup of $\mathbb{R}^m$. One can always find a basis $\mathbf{B} = (\mathbf{b}_1 \mid \cdots \mid \mathbf{b}_n)$ with $n \leq m$ of linearly independent vectors such that Λ is the integer combination of $\{\mathbf{b}_i\}_i$. In other words, we have $\Lambda = \mathbf{B}\mathbb{Z}^n$. The choice of basis is not unique. In fact, for every unimodular matrix $\mathbf{U}$ the two bases $\mathbf{B}$ and $\mathbf{BU}$ define the same lattice. When $n = m$, we say that the lattice is full-rank. An important computational problem over lattices is the *shortest vector problem* which asks to find a shortest non-zero vector, with respect to the ℓ_2 norm, in Λ given a basis $\mathbf{B}$. We let $\lambda_1(\Lambda)$ denote the ℓ_2 norm of such a vector in lattice Λ. The q-array lattices for an integer q are those lattices which are periodic modulo $q\mathbb{Z}^m$. A particular q-array lattice of interest is the following one:

$$\Lambda_q(\mathbf{A}) = \mathbf{A}(\mathbb{Z}/q\mathbb{Z})^n + q\mathbb{Z}^m = \{\mathbf{As} + q\mathbf{k} \mid \mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n, \mathbf{k} \in \mathbb{Z}^m\},$$

where $\mathbf{A}$ is a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m \times n}$. Let R be a ring of integers for some number field K with degree d. We also consider the module variant of the above definition as follows:

$$\Lambda_q(\mathbf{A}) = \mathbf{A}(R/qR)^n + qR^m = \{\mathbf{As} + q\mathbf{k} \mid \mathbf{s} \in (R/qR)^n, \mathbf{k} \in R^m\},$$

where $\mathbf{A}$ is an element of $(R/qR)^{m \times n}$. Note that $\Lambda_q(\mathbf{A}) \subseteq R^m$ is indeed a lattice by representing R^m as elements of $\mathbb{Z}^{md}$ with the coefficient embedding of the field.

2.4. **Probabilities.** The Gaussian measure centered around $\mathbf{0}$ with the standard deviation $s > 0$ is defined as:

$$\forall \mathbf{x} \in \mathbb{R}^m, \quad \rho_s(\mathbf{x}) \stackrel{\text{def}}{=} e^{-\pi \frac{\|\mathbf{x}\|^2}{s^2}}.$$

The following lemma shows the concentration behaviour of ρ_s over lattices.

Lemma 9 (Adapted from [Ban93, Lemma 1.5])**.** *For any m-dimensional lattice Λ, and any positive real numbers $s, r \geq \frac{s}{\sqrt{2\pi}}$, it holds that*

$$\rho_s\left(\Lambda \setminus \mathrm{B}_m(r\sqrt{m})\right) \leq \left(\frac{r}{s}\,\sqrt{2\pi e}\; e^{-\pi r^2/s^2}\right)^m \rho_s(\Lambda).$$

We also have the following inequality.

Lemma 10. *For every $s > 0$, we have $s \leq \rho_s(\mathbb{Z}) \leq 1 + s$.*

Proof. We have

$$\begin{aligned}\rho_s(\mathbb{Z}) &\leq 1 + 2\int_0^{+\infty} \rho_s(x)\ dx \\ &= 1 + s,\end{aligned}$$

where we used a comparison between the sum and the integral. Moreover, using the Poisson summation formula, one obtains

$$\rho_s(\mathbb{Z}) \geq s\ \rho_{\frac{1}{s}}(\mathbb{Z}) \geq s.$$

□

We let D_s denote the continuous Gaussian distribution over $\mathbb{R}^m$ centered around $\mathbf{0}$ with the standard deviation s that is defined as follows:

$$\forall \mathbf{x} \in \mathbb{R}^m,\ D_s(\mathbf{x}) = \frac{1}{s^m}\rho_s(\mathbf{x}).$$

The following ensemble of distributions will be used in the modulus switching lemma 34.

Definition 7. *For every $s > 0$, we let $\Psi_{\leq s}$ be the ensemble of the probability distributions $\{D_t\}_{t \leq s}$.*

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

$$\forall \mathbf{k} \in \mathbb{Z}^m,\ D_{\mathbb{Z}^m,s}(\mathbf{k}) = \frac{D_s(\mathbf{k})}{D_s(\mathbb{Z}^m)},$$

where $D_s(\mathbb{Z}^m) = \sum_{\mathbf{k}\in\mathbb{Z}^m} D_s(\mathbf{k})$.

Folding $D_{\mathbb{Z}^m,s}$ modulo an integer q yields the following probability distribution.

Definition 8 (Folded Discrete Gaussian Distribution)**.** *Let $s > 0$. We define the folded discrete Gaussian distribution over $(\mathbb{Z}/q\mathbb{Z})^m$ with standard deviation s by its probability mass function ϑ_s:*

$$\forall \mathbf{x} \in [\![-\lceil\frac{q}{2}\rceil, \lfloor\frac{q}{2}\rfloor]\!]^m :\ \vartheta_s(\mathbf{x}) \overset{def}{=} \frac{\sum_{\mathbf{k}\in\mathbb{Z}^m} \rho_s(\mathbf{x} + \mathbf{k}q)}{\rho_s(\mathbb{Z}^m)}\quad ,$$

where $\rho_s(\mathbb{Z}^d) = \sum_{\mathbf{k}\in\mathbb{Z}^m} \rho_s(\mathbf{k})$.

We note that in all distributions above, the dimension of the input is implicit and can be derived from the context.

The distribution ϑ_s behaves very closely to $D_{\mathbb{Z},s}$.

Lemma 11. *Let $q \geq 2$ be a positive integer and $s > 0$ be a real number such that $q \geq \frac{2s}{\sqrt{2\pi}}$. Then for every x in $\{-\lceil\frac{q}{2}\rceil, \cdots, \lfloor\frac{q}{2}\rfloor\}$, it holds that*

$$D_{\mathbb{Z},s}(x) \leq \vartheta_s(x) \leq D_{\mathbb{Z},s}(x) + e^{-2q^2/s^2},\ \text{and}\ \sqrt{\vartheta_s(x)} \leq \sqrt{D_{\mathbb{Z},s}(x)} + e^{-q^2/s^2}.$$

Proof. First, note that

$$\vartheta_s(x) = \frac{\sum_{k\in\mathbb{Z}} \rho_s(x + kq)}{\rho_s(\mathbb{Z})}\quad .$$

We have

$$\begin{aligned}\sum_{k\in\mathbb{Z}} \rho_s(x + kq) &= \rho_s(x) + \sum_{k\in\mathbb{Z}\setminus\{0\}} \rho_s(x + kq) \\ &\leq \rho_s(x) + \sum_{\ell\in\mathbb{Z}:|\ell|\geq\lceil q/2\rceil} \rho_s(\ell) \\ &\leq \rho_s(x) + \frac{q}{2s}\ \sqrt{2\pi e}\ e^{-\pi q^2/(2s)^2}\rho_s(\mathbb{Z}) \quad \text{(by Lemma 10)} \\ &\leq \rho_s(x) + e^{-2q^2/s^2}\rho_s(\mathbb{Z}),\end{aligned}$$

where the last inequality follows since for every $x \in \mathbb{R}$, we have $8x^2 \geq \ln x + \ln \sqrt{2\pi e}$. This completes the first inequality. For the other one, we obtain

$$\begin{aligned}\sqrt{\vartheta_s(x)} &\leq \sqrt{\frac{\rho_s(x) + e^{-2q^2/s^2}\rho_s(\mathbb{Z})}{\rho_s(\mathbb{Z})}} \\ &\leq \sqrt{\frac{\rho_s(x)}{\rho_s(\mathbb{Z})}} + e^{-q^2/s^2}.\end{aligned}$$

□

The last lemma extends to higher dimensions as follows.

Lemma 12. *Let $m \geq 1, q \geq 2$ be positive integers and $s > 0$ be a real number such that $q \geq \frac{2s\sqrt{m}}{\sqrt{2\pi}}$. The following statement holds.*

$$\forall \mathbf{x} \in [\![-\lceil \frac{q}{2} \rceil, \lfloor \frac{q}{2} \rfloor]\!]^m : \sqrt{D_{\mathbb{Z}^m,s}}(\mathbf{x}) \leq \sqrt{\vartheta_s}(\mathbf{x}) \leq \sqrt{D_{\mathbb{Z}^m,s}}(\mathbf{x}) + e^{-q^2/(ms^2)}.$$

Proof. The proof is similar to that of Lemma 12 using the fact that for every vector $\mathbf{x}$, we have $\rho_s(\mathbf{x}) = \prod_i \rho_s(x_i)$. □

Lemma 13. *TODO: Lemme for modulus switching.*

We have the following lemma regarding the embedding of ϑ in the amplitudes of a quantum satate.

Corollary 1. *Let $s > 0$ be a real number. Then one can build the following state with runtime complexity* $\mathsf{poly}(\log q)$*:*

$$\sum_{i \in [\![-\lceil \frac{q}{2} \rceil, \lfloor \frac{q}{2} \rfloor]\!]} \sqrt{\vartheta_s(i)} \left| i \right\rangle .$$

Proof. Since ϑ_s well approximates $D_{\mathbb{Z},s}$, the statement holds according to Lemma 5. □

2.5. **Learning With Errors.** The LWE problem can be viewed as a lattice problem. It was first introduced by [Reg09].

Definition 9 (LWE Problem)**.** *Let n, m, q be integers and $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$. Let χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. Let $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$ be sampled uniformly and $\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$ be sampled from $\chi^{\otimes m}$.*

The search $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ problem is defined as: 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 χ is equal to the folded discrete Gaussian distribution $\vartheta_{\alpha q}$, we overwrite the notation as $\mathsf{LWE}_{q,\alpha}(\mathbf{A})$.

Let $\lambda_1(\mathbf{A})$ be the norm of a shortest non-zero vector in $\Lambda_q(\mathbf{A})$ with respect to the ℓ_2 norm. We note that if the distribution of the noise $\chi^{\otimes m}$ is not concentrated in a ball with radius $\lambda_1(\mathbf{A})/2$, then it is likely that the LWE instance can be decoded into two different secrets. To avoid such issues, we always assume that

$$\mathbb{P}_{\mathbf{A},\chi^{\otimes m}}\left(\|\mathbf{e}\|_2 \geq \frac{\lambda_1(\mathbf{A})}{2}\right) = \mathsf{negl}(n). \tag{3}$$

With the condition above, in the language of lattices, the LWE problem asks for finding the unique[3] closest point in $\Lambda_q(\mathbf{A})$ to $\mathbf{As} + \mathbf{e}$.

The quantum hardness of the LWE problem for various distributions of the noise and the secret has been extensively studied [Reg09, GKPV10, MM11, BLP+13] and it is known that LWE is harder than some hard worst-case problems [Reg09]. We mention one of the central assumptions in this context below.

[3] It is unique with probability $1 - \mathsf{negl}(n)$.

Assumption 1 (Quantum Hardness of LWE)**.** *Let m, n, q be integers, $\alpha \in (0,1)$, and $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ sampled uniformly. If α is non-negligible in n and $\alpha q \geq 2\sqrt{n}$, then no QPT algorithm can solve the $\mathsf{LWE}_{q,\alpha}(\mathbf{A})$ problem with non-negligible probability.*

2.6. Module Learning with Errors.

Some structured variants of LWE have been studied in the literature, such as in [SSTX09, LPR10, LS15]. Instead of choosing the matrix $\mathbf{A}$ uniformly, one might choose it with some particular structure. The rationale of this approach is, roughly speaking, to define LWE instances that allow more efficient algorithms in the cryptographic case studies.

The module LWE problem (MLWE) is a variant of LWE in which the matrix $\mathbf{A}$ is chosen uniformly at random in $(R/qR)^{m\times n}$. For the sake of simplicity, we always assume that each coefficient of the error distribution over R/qR is element-wise i.i.d.

Definition 10 (MLWE Problem)**.** *Let n, m, q, d be integers. Let K be a number field with degree d and R be its ring of integers. Let $\mathbf{A}$ be a matrix in $(R/qR)^{m\times n}$. Let $\chi^{\otimes d}$[4] be an element-wise i.i.d. distribution over R/qR. Let $\mathbf{s} \in (R/qR)^n$ be sampled uniformly and $\mathbf{e} \in (R/qR)^m$ from $\chi^{\otimes dm}$.*

The search $\mathsf{MLWE}_{d,q,\chi}(\mathbf{A})$ problem is defined as follows: 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 χ is equal to the folded discrete Gaussian distribution $\vartheta_{\alpha q}$, we overwrite the notation as $\mathsf{MLWE}_{d,q,\alpha}(\mathbf{A})$.

We impose the same restriction on the distribution of the matrix $\mathbf{A}$ and the noise as in LWE. Let $\lambda_1(\mathbf{A})$ be the norm of a shortest vector in $\Lambda_q(\mathbf{A})$ with respect to the ℓ_2 norm. We implicitly assume that

$$\mathbb{P}_{\mathbf{A},\chi^{\otimes dm}}\left(\|\mathbf{e}\|_2 \geq \frac{\lambda_1(\mathbf{A})}{2}\right) = \mathsf{negl}(n). \tag{4}$$

The MLWE problem is conjectured to be hard for certain sets of parameters (see [SSTX09, LPR10, LS15] for more details).

Assumption 2 (Quantum Hardness of MLWE)**.** *Let n, m, q, d be integers. Let K be a number field with degree d and R be its ring of integers. Let $\mathbf{A} \in (R/qR)^{m\times n}$ be sampled uniformly. If α is non-negligible in n and $\alpha q \geq 2\sqrt{d}\,\omega(\sqrt{\log n})$ [5], then no QPT algorithm can solve the $\mathsf{MLWE}_{d,q,\alpha}(\mathbf{A})$ problem with non-negligible probability.*

MLWE is a particular case of LWE. The MLWE problem can be viewed as a special case of LWE as follows. For every $x \in R/qR$, we have $\phi(x) \in (\mathbb{Z}/q\mathbb{Z})^d$ where d is the degree of the number field. Furthermore, the coefficient embedding of the product xy for every $x, y \in (R/qR)$ is

$$\phi(xy) = \widetilde{\mathrm{T}_x}\left(\phi(y)\right),$$

where $\widetilde{\mathrm{T}_x} \in (\mathbb{Z}/q\mathbb{Z})^{d\times d}$ is the matrix representation of T_x in the integral basis of the field. Therefore, one can transform each sample $\langle \mathbf{a}, \mathbf{s}\rangle + e$ of MLWE to d samples of LWE as follows.

$$\langle \mathbf{a}, \mathbf{s}\rangle + e \mapsto \left(\sum_{i=1}^{n} \widetilde{\mathrm{T}_{a_i}}\left(\phi(s_i)\right)\right) + \phi(e) = \begin{pmatrix} \widetilde{\mathrm{T}_{a_1}} & \widetilde{\mathrm{T}_{a_2}} & \cdots & \widetilde{\mathrm{T}_{a_n}} \end{pmatrix} \begin{pmatrix} \phi(s_1) \\ \phi(s_2) \\ \vdots \\ \phi(s_n) \end{pmatrix} + \phi(e).$$

The map $\mathrm{T}_{\mathbb{Z}}$ defined below determines the shape of $\mathbf{A} \in (R/qR)^{m\times n}$ after the above transform.

Definition 11. *Let R be a ring of integers of a number field with degree d, and q be an integer. We define $T_{\mathbb{Z}} : (R/qR)^{m\times n} \to (\mathbb{Z}/q\mathbb{Z})^{md\times nd}$ as follows.*

$$\forall \mathbf{A} = (a_{ij})_{i,j} \in (R/qR)^{m\times n} : \ \mathrm{T}_{\mathbb{Z}}(\mathbf{A}) = \left(\widetilde{\mathrm{T}_{a_{ij}}}\right)_{i,j},$$

where $\widetilde{\mathrm{T}_{a_{ij}}} \in (\mathbb{Z}/q\mathbb{Z})^{d\times d}$ is the matrix representation of $\mathrm{T}_{a_{ij}}$ in an integral basis of the ring.

[4] **[Pouria : @Thomas:in the notation $\mathsf{MLWE}_{d,q,\chi}(\mathbf{A})$, distribution χ has its support in $\mathbb{Z}/q\mathbb{Z}$. It simplifies things later when it is defined like that. If I remove tensor here, then it ruins that notation.]**

[5] **[Pouria : @Damien: I think this is the correct condition as in Theorem 4.7 of LS15]**

One must note that this process blows up the dimensions of the matrix $\mathbf{A}$ from $m\times n$ to $md\times nd$, which has to be taken into account in the statements.

The noise distribution of MLWE is also changed by the above transform. As highlighted in Definition 10, the distribution χ is element-wise i.i.d. Thus, for every $e \in R/qR$, its probability to be picked satisfies

$$\prod_{i}^{d} \mathbb{P}_{\chi}\left(\phi(e)_i\right).$$

This means that the distribution of the noise in the d samples of LWE obtained by the above transform is $\chi^{\otimes d}$.

Overall, we have

$$\mathsf{MLWE}_{d,q,\chi}\left(\mathbf{A}\right) = \mathsf{LWE}_{q,\chi}(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})). \tag{5}$$

2.7. **Random Matrices.** The following lemma deals with the probability of a random matrix to be full-rank.

Lemma 14. *Let $n, m \geq n+1$ be integers, q be a prime integer, and $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ be chosen uniformly. Then the probability of $\mathbf{A}$ being full-rank is at most $1 - p^{n+1-m}$.*

We also need the following lemma.

Lemma 15. *Let $m \geq n$ be integers, q be a prime integer, $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ be a uniformly chosen full-rank matrix, and $\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$ be a non-zero vector. Then, we have*

$$\mathbb{P}_{\mathbf{A}}\left(\exists \mathbf{x}: \ \mathbf{A}\mathbf{x} = \mathbf{e}\right) \leq q^{n-m}.$$

Proof. Consider the Hermite normal form of $\mathbf{A}$ as follows:

$$\mathbf{A}\mathbf{U} = \begin{pmatrix} \mathbf{I}_{n\times n} \\ \mathbf{H}_{(m-n)\times n} \end{pmatrix}.$$

Let $\mathbf{V}_{(m-n)\times(m-n)}$ uniformly chosen unimodular matrix, and $\mathbf{B}$ be $\mathbf{V}\begin{pmatrix}\mathbf{H} & -\mathbf{I}_{(m-n)\times(m-n)}\end{pmatrix}$. It holds that $\mathbf{B}\mathbf{A} = \mathbf{0}$, and $\mathbf{B}$ is also a uniform full-rank matrix. One can verify that

$$\{\mathbf{A}\mathbf{x} \mid \mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n\} = \{\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m \mid \mathbf{B}\mathbf{e} = \mathbf{0}\}.$$

Therefore we have

$$\begin{aligned}\mathbb{P}_{\mathbf{A}}\left(\exists \mathbf{x}: \ \mathbf{A}\mathbf{x} = \mathbf{e}\right) &= \mathbb{P}_{\mathbf{B}}\left(\mathbf{B}\mathbf{e} = \mathbf{0}\right) \\ &= \prod_{i=1}^{m-n} \mathbb{P}_{\mathbf{b}_i}\left(\langle \mathbf{b}_i, \mathbf{e}\rangle = 0\right) \\ &= (\frac{1}{q})^{m-n}.\end{aligned}$$

□

The following lemma shows that one can efficiently find a representation of kernels of matrices over ring of integers.

Lemma 16. *Let K be a cyclotomic field with degree d and R be its ring of integers. Let $n, q, m \geq n + \omega(n)$ be integers. The following statements hold:*

- *Let $\mathbf{A}$ be a matrix that is sampled uniformly from $(R/qR)^{m\times n}$ and M be defined as follows:*

  $$M \overset{def}{=} \{\mathbf{x} \in (R/qR)^m \mid \mathbf{x}^\top \mathbf{A} = \mathbf{0} \bmod q\}.$$

  Then the rank of M is $m - n$ with probability $1 - \mathsf{negl}(n)$, and in this case, one can find a matrix $\mathbf{B} \in (R/qR)^{(m-n)\times n}$ such that its rows generate M.
- *Let $\mathbf{B}$ be sampled uniformly from $(R/qR)^{(m-n)\times n}$ and N be defined as follows:*

  $$N \overset{def}{=} \{\mathbf{y} \in (R/qR)^m \mid \mathbf{B}\mathbf{y} = \mathbf{0} \bmod q\}.$$

  Then the rank of N is n with probability $1 - \mathsf{negl}(n)$, and in this case, one can find a matrix $\mathbf{A} \in (R/qR)^{m\times n}$ such that its columns generate N.

Furthermore, both of these algorithms require $\mathsf{poly}(n, m, \log q)$ *steps.*

Proof. The statements follow by Lemma **??** □

3. Witness Awareness and Obliviousness

In this section we are interested in the ways that given a matrix $\mathbf{A}$, one can sample an LWE instance $(\mathbf{A}, \mathbf{b})$. A natural way (as in the definition of the LWE problem) is the following: the sampler, using a source of randomness, produces a secret vector $\mathbf{s}$ and a noise vector $\mathbf{e}$ with given distributions. Then it outputs $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$. 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.*

Various *knowledge assumptions* are implicitly used in security proofs of several lattice-based cryptographic schemes, such as *Succint Non-Interactive Arguments of Knowledge* (SNARKs), for example [LMSV12, GMNO18, ISW21, GNSV23, ACL$^+$22, SSEK22, CKKK23, CLM23]. All of them can be viewed as special cases of the following general statement: any LWE sampler is witness-aware. In particular, in the case of SNARKs, the adversary plays the role of the sampler and it wins in the security game if it produces an LWE instance in a way that it does not know the secret itself. We call this property as *witness obliviousness.*

For post-quantum security, the adversary (the sampler) can be a quantum algorithm. Therefore, the quantum version of the knowledge assumption must be put at stake.

In this section, we analyze instance samplers and knowledge assumptions with the focus on the LWE problem. We start by splitting our discussion about obliviousness between classical and quantum settings in Subsections 3.1 and 3.2. All our discussions also hold for MLWE by using Equation (5). Indeed, in each definitions, lemmas and assumptions the matrix $\mathbf{A}$ is fixed without any assumption on its shape. Furthermore, we show in Subsection 3.3 how to deduce from a given oblivious sampler another one via reductions. Ultimately, 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 the classical LWE sampler.

Definition 12 (Classical LWE Samplers)**.** *Let n, m, q be integers which are some functions of the security parameter λ, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. Let $\mathcal{S}$ be a PPT algorithm that has the following specification:*

> $\mathcal{S}(\mathbf{A}; r)$*: Given as input a matrix $\mathbf{A}$ and an independent randomness r, it returns an instance $(\mathbf{A}, \mathbf{b} \overset{def}{=} \mathbf{A}\mathbf{s} + \mathbf{e})$ with $\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n$, and $\mathbf{e} \in (\mathbb{Z}/q\mathbb{Z})^m$.*

We say that $\mathcal{S}$ is a classical $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler, if the distribution of $(\mathbf{A}, \mathbf{b})$ is at most $\mathsf{negl}(\lambda)$-far with respect to the statistical distance from the instance distribution of $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ as given in Definition 9.

As discussed earlier, 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, which allows us to extract it. We grasp this intuition in the following definition.

Definition 13 (Witness-Aware LWE Samplers)**.** *Let n, m, q be integers which are some functions of the security parameter λ, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. We say that a classical $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler $\mathcal{S}$ is witness-aware if there exists a PPT extractor $\mathcal{E}$ such that*

$$\mathbb{P}\left(\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \;\middle|\; \begin{array}{l} r \leftarrow U\left(\{0,1\}^{\mathsf{poly}(\lambda)}\right) \\ (\mathbf{A}, \mathbf{b}) \leftarrow \mathcal{S}(\mathbf{A}; r) \\ (\mathbf{s}, \mathbf{e}) \leftarrow \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), (\mathbf{A}, \mathbf{b}), r\right) \end{array} \right) \geq \frac{1}{\mathsf{poly}(\lambda)},$$

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

Finally, we are able to define witness-oblivious samplers. We request the sampler to be resistant against any sort of inspection by polynomial-time extractors.

Definition 14 (Witness-Oblivious LWE Samplers)**.** *Let n, m, q be integers which are some functions of the security parameter λ, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$.*

We say that a classical $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ *sampler* $\mathcal{S}$ *is witness-oblivious if for every PPT extractor* $\mathcal{E}$*, we have*

$$\mathbb{P}\left(\mathbf{b}=\mathbf{A}\mathbf{s}+\mathbf{e}\;\middle|\;\begin{array}{l} r\leftarrow U\left(\{0,1\}^{\mathsf{poly}(\lambda)}\right)\\ (\mathbf{A},\mathbf{b})\leftarrow\mathcal{S}(\mathbf{A};r)\\ (\mathbf{s},\mathbf{e})\leftarrow\mathcal{E}\left(\mathsf{Desc}(\mathcal{S}),(\mathbf{A},\mathbf{b}),r\right)\end{array}\right)\leq\mathsf{negl}(\lambda),$$

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

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

Lemma 17. *Let* q *be an integer with is function of the security parameter* λ *and* χ *be a distribution over* $\mathbb{Z}/q\mathbb{Z}$*. Suppose that there exists a classical witness-oblivious* $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ *sampler. Then the* $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ *problem is hard for every PPT algorithm; for all PPT algorithm* $\mathcal{B}$*, we have*

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

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

Proof. Let $\mathcal{S}$ denote the witness-oblivious sampler, and $\mathcal{B}$ be a PPT algorithm. By assumption, the algorithm $\mathcal{S}$ is a classical witness-oblivious $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler (see Definition 12). Its output distribution is at most $\mathsf{negl}(\lambda)$-far from the instance distribution of $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ with respect to the statistical distance. Therefore,

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

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

$$\mathcal{E}\left(\mathsf{Desc}(\mathcal{S}),(\mathbf{A},\mathbf{b}),r\right)\stackrel{\text{def}}{=}\mathcal{B}(\mathbf{A},\mathbf{b}).$$

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

$$\mathbb{P}\left(\mathbf{b}=\mathbf{A}\mathbf{s}+\mathbf{e}\;\middle|\;\begin{array}{l} r\leftarrow U(\{0,1\}^{\mathsf{poly}(\lambda)})\\ (\mathbf{A},\mathbf{b})\leftarrow\mathcal{S}(\mathbf{A};r)\\ (\mathbf{s},\mathbf{e})\leftarrow\mathcal{E}\left(\mathsf{Desc}(\mathcal{S}),(\mathbf{A},\mathbf{b}),r\right)\end{array}\right)\leq\mathsf{negl}(\lambda),$$

which completes the proof. □

The reason that we explicitly isolated the matrix $\mathbf{A}$ as part of the input to the sampler is that, in some cases, the matrix $\mathbf{A}$ could be sampled according to an adversarially chosen distribution. This might indeed affect the awareness or obliviousness of the sampler as shown in the above lemma. For each obliviousness result, we must resort to a hardness assumption that is compatible with the distribution of $(\mathbf{A},\mathbf{b})$. In other words, the very minimal requirement for obliviousness is that the outcome instance of the sampler must be hard enough for polynomial-time solvers, otherwise finding the witness $(\mathbf{s},\mathbf{e})$ would be efficiently doable which contradicts our intuition of obliviousness. To satisfy the hardness requirement, the LWE instance must be sampled from a proper regime of distributions such as those explained in [Reg09, SSTX09, LPR10, LS15].

One could also be interested in the converse: assuming the hardness of the LWE problem, can one sample hard instances obliviously? It is conjectured that the converse does not hold.

Assumption 3 (Classical LWE Knowledge Assumption)**.** *Let* n,m,q *be integers,* $\mathbf{A}$ *be a matrix in* $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$*, and* χ *be a distribution over* $\mathbb{Z}/q\mathbb{Z}$*. Then any classical* $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ *sampler* $\mathcal{S}$ *is witness-aware.*

To break the above assumption, it is sufficient to show that there exists a classical witness-oblivious $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler. As mentioned, we are not aware of any such algorithm.

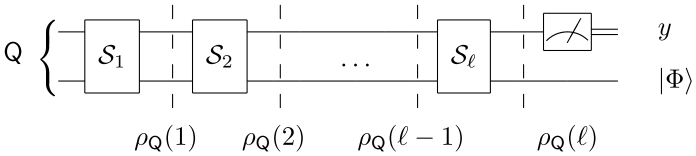

FIGURE 1. The execution of the sampler.

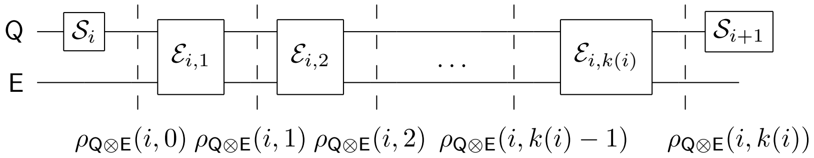
Q
E
$\mathcal{S}_i$
$\mathcal{E}_{i,1}$
$\mathcal{E}_{i,2}$
$\mathcal{E}_{i,k(i)}$
$\mathcal{S}_{i+1}$
$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,0)$
$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,1)$
$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,2)$
$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,k(i)-1)$
$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,k(i))$

FIGURE 2. The interaction of the extractor and the sampler at Step i.

3.2. **Quantum Setting.** To discuss the post-quantum security of cryptographic schemes, in particular lattice-based SNARKs, we must migrate to quantum algorithms with appropriate extensions of awareness and obliviousness. Before going into the details, we need an appropriate definition of quantum samplers.

Definition 15 (Quantum LWE Samplers)**.** *Let n, m, q be integers which are some functions of the security parameter λ, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$. Let χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$, and $\mathcal{S}$ be a QPT algorithm that has the following specification:*

> $\mathcal{S}\left(1^\lambda, |\mathbf{A}\rangle\right)$*: Given as input the parameter 1^λ, the matrix $\mathbf{A}$, and polynomial number of ancillas as inputs, it returns an instance $(\mathbf{A}, \mathbf{b})$ where $\mathbf{b} \in (\mathbb{Z}/q\mathbb{Z})^m$.*

We say that $\mathcal{S}$ is a quantum $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler, if the distribution of $(\mathbf{A}, \mathbf{b})$ is at most $\mathsf{negl}(\lambda)$-far with respect to the statistical distance from the instance distribution of $\mathsf{LWE}_{q,\chi}(\mathbf{A})$.

The main principle we use to base our definition on is that observing or measuring the execution of a machine (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 ρ_{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.

Definition 16. *Let Q and E be two quantum registers, and $\mathcal{G}$ be a universal set of gates. Let $\mathcal{S}$ be a quantum algorithm operating on register Q with the set of gates $\mathcal{S}_1, \cdots, \mathcal{S}_\ell$ 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 set of gates $\mathcal{E}_1, \cdots, \mathcal{E}_{\ell+1}$ such that each $\mathcal{E}_i$ is a series of gates in $\mathcal{G}$ and measurements in the computational basis. In one scenario, suppose that $\mathcal{S}$ is operating alone on Q. Let $\rho_{\mathsf{Q}}(i)$ be the density matrix representing the state of Q exactly after the i-th step of $\mathcal{S}$ as in Figure 1. In another scenario, suppose that $\mathcal{S}$ and $\mathcal{E}$ are operating jointly on both registers Q and E as follows. After the i-th step of $\mathcal{S}$, algorithm $\mathcal{E}$ is given both registers to perform its operation $\mathcal{E}_i$ and sends register Q to $\mathcal{S}$. Assume that $\mathcal{E}_i = \mathcal{E}_{i,1}\mathcal{E}_{i,2}\cdots\mathcal{E}_{i,k(i)}$ for some function k. For every $1 \le j \le k(i)$, 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 exactly before applying $\mathcal{E}_i$ as in Figure 2.*

We say that $\mathcal{E}$ is a valid extractor if for every $1 \le i \le \ell$ and every $0 \le j \le k(i)$, it holds that:

$$\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)) = \rho_{\mathsf{Q}}(i). \tag{6}$$

We assume that $\mathcal{E}$ is also given $\mathsf{Desc}(\mathcal{S})$ *as input. Furthermore, we let* $\langle \mathcal{S}, \mathcal{E} \rangle_{\mathrm{ext}}(1^\lambda, \sigma_{\mathsf{Q}}, \sigma_{\mathsf{E}})$ *denote the joint output when both* Q *and* E *have been initiated by* σ_{Q} *and* σ_{E} *of size* $\mathsf{poly}(\lambda)$*, respectively.*

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 given in Definitions 13 and 14.

The condition in Equation (6) can be relaxed by requiring $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j))$ to be within $\mathsf{negl}(\ell)$ trace norm from $\rho_{\mathsf{Q}}(i)$. This statistical indistinguishability of the states provides a stronger notion of extraction. If the number of gates is ℓ, the extractor changes the outcome distribution of the sampler by at most ℓ $\mathsf{negl}(\ell)$ which remains negligible in ℓ. In the case where σ_{Q} is efficiently constructible and the sampler only applies unitary gates, then one can replace statistical indistinguishability by computational indistinguishability without any cost since they are equivalent. This is because the distinguisher can always rewind to the initial state and check whether it is equal to σ_{Q} or not. Our sampler for LWE is of this type and therefore remains oblivious even in this strong computational extraction setting.

[Pouria : Another argument why this is a good definition: In the black-box setting, an extractor can perform measurements or unitaries that (almost) commute with all the gates of the sampler, see https://arxiv.org/abs/2103.03085 as an example of online extraction in the QROM. The intuition that we have about not changing the circuit of the sampler is kind of close to saying that we should behave with the gates of the sampler as black-boxes. Of course we know their description, but in the course of execution (somehow corresponds to the online phase of the mentioned paper), we shouldn't change them. The good thing about our definition is that it also covers the extractors which (almost) commute with the gates of the sampler.]

Relation to other definitions. Liu *et al.* [LMZ23] adopted a different approach. Their definition only deals with unitary algorithms followed by a single final measurement. In their definition of extraction [LMZ23, Assumption 2], 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, the extractor is only given the description of the gates $\mathcal{S}_1, \cdots, \mathcal{S}_\ell$, the classical output y, and the quantum output $|\Phi\rangle$. The authors justify that it is a definition that is consistent with the classical setting, as follows. It is first observed that unitary algorithms are reversible. In the classical setting, every machine can be turned into a reversible one. By having the output of the reversible machine, 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. For this reason, samplers (classical or quantum) are restricted to reversible ones and so the definition from [LMZ23] is consistent in the classical and quantum settings. We show in the following lemma that our definition covers the one from [LMZ23] when restricted to unitary algorithms.

Lemma 18. *Let* Q *and* E *be two quantum registers. Let* $\mathcal{S}$ *be a quantum algorithm operating on* Q *by a series of unitary gates followed by a single measurement. Let* $\mathcal{E}$ *be a valid extractor operating on two registers* Q *and* E *as per Definition 16. Then* $\mathcal{E}$ *has only access to the description of* $\mathcal{S}$*, its output, and its remaining working state. In other words, there exists a QPT extractor* $\mathcal{E}'$ *such that*

$$\langle \mathcal{S}, \mathcal{E} \rangle_{\mathrm{ext}}(1^\lambda, \sigma_{\mathsf{Q}}, \sigma_{\mathsf{E}}) = \mathcal{E}'\left(1^\lambda, \mathsf{Desc}(\mathcal{S}), \mathcal{S}\left(\sigma_{\mathsf{Q}}\right), \sigma_{\mathsf{E}}\right).$$

Proof. See Appendix A.1. □

Definition 16 provides a solid basis to extend awareness and obliviousness as per Definitions 13 and 14 to quantum samplers. We begin by witness-awareness.

Definition 17 (Witness-Aware Quantum LWE Samplers)**.** *Let n, m, q be integers which are some functions of the security parameter λ, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. We say that a quantum $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler $\mathcal{S}$ is witness-aware if there exists a valid QPT extractor $\mathcal{E}$ such that*

$$\mathbb{P}\left(\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \;\middle|\; ((\mathbf{A}, \mathbf{b}), (\mathbf{s}, \mathbf{e})) \leftarrow \langle \mathcal{S}, \mathcal{E}\rangle_{\text{ext}}\left(1^\lambda, \left|\mathbf{A}, 0^{\mathsf{poly}(\lambda)}\right\rangle, \left|0^{\mathsf{poly}(\lambda)}\right\rangle\right)\right) \geq \frac{1}{\mathsf{poly}(\lambda)},$$

where the probability is taken over the measurements of $\mathcal{E}$.

The witness-obliviousness of quantum samplers is defined by negating the above definition.

Definition 18 (Witness-Oblivious Quantum Samplers)**.** *Let n, m, q be integers, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. We say that a quantum $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler $\mathcal{S}$ is witness-oblivious if for every valid QPT extractor $\mathcal{E}$*

$$\mathbb{P}\left(\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \;\middle|\; ((\mathbf{A}, \mathbf{b}), (\mathbf{s}, \mathbf{e})) \leftarrow \langle \mathcal{S}, \mathcal{E}\rangle_{\text{ext}}\left(1^\lambda, \left|\mathbf{A}, 0^{\mathsf{poly}(\lambda)}\right\rangle, \left|0^{\mathsf{poly}(\lambda)}\right\rangle\right)\right) \leq \mathsf{negl}(\lambda),$$

where the probability is taken over the measurements of $\mathcal{E}$.

We note that a statement similar to Lemma 18 holds for quantum witness-oblivious samplers. Assumption 3 only deals with classical samplers. In the quantum adversarial setting, it is more appropriate to study the case wherein the sampler could also be a quantum algorithm. We extend the definition as follows.

Assumption 4 (Quantum LWE Knowledge Assumption)**.** *Let n, m, q be integers, $\mathbf{A}$ be a matrix in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and χ be a distribution over $\mathbb{Z}/q\mathbb{Z}$. Then any quantum $\mathsf{LWE}_{q,\chi}(\mathbf{A})$ sampler $\mathcal{S}$ is witness-aware.*

In Section 4 , we show how to break this assumption but for some particular parameters α and q for which LWE is conjectured to be quantumly hard. However, these parameters are not those considered in SNARKs that we aim to break quantumly. It is therefore natural to wonder whether an oblivious sampler can be extended to cover larger regimes of parameters. In the following subsection we answer positively by showing how oblivious samplers behave under black-box reductions.

3.3. **Obliviousness Under Black-Box Reductions.**

All definitions of this section can be extended to the general class of *distributional problems* as well. Recall that a distributional problem P is a pair (R, D) where R is an NP relation and $\mathrm{D} = \{\mathrm{D}_\lambda\}_{\lambda\in\mathbb{N}}$ 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 LWE problem belongs to this class.

Definition 19 (Quantum Samplers)**.** *Let n be an integer and $\tilde{x} \in \{0,1\}^*$ such that $|\tilde{x}| \leq \lambda$. Let $\mathrm{P} = (\mathrm{R}, \mathrm{D})$ be a distributional problem. Let $\mathcal{S}$ be a QPT algorithm that has the following specification:*

> $\mathcal{S}\left(1^\lambda, |\tilde{x}\rangle\right)$: *it takes the parameter 1^λ, a string $\tilde{x}$, and polynomial number of ancillas as inputs, and returns a string x of size λ that has $\tilde{x}$ as substring.*

We say that $\mathcal{S}$ is a quantum P sampler, if the distribution of x is at most $\mathsf{negl}(\lambda)$-far from D_λ with respect to the statistical distance.

One can define witness-aware and witness-oblivious samplers similarly as Subsections 3.1 and 3.2.

We study the conditions under which the composition of algorithms with the witness-oblivious samplers remain oblivious. We begin by defining a set of algorithms as below. We will show later that they behave well in terms of obliviousness.

Definition 20. *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* P_1 *to instances of* P_2 *such that* $\mathcal{A}(\mathrm{D}_1)$ *is within negligible statistical distance from* D_2 *over the randomness of* $\mathcal{A}$*,*
- *a uniform polynomial-time (classical or quantum) algorithm* $\mathcal{B}$ *for* $\mathcal{A}$ *such that*

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

with non-negligible probability over the randomness of $\mathcal{B}$*. Note that* $\mathcal{B}$ *takes the randomness of* $\mathcal{A}$ *as input.*

The following theorem explains how one can come up with new witness-oblivious samplers by composing a given witness-oblivious sampler with randomized Karp reductions.

Lemma 19. *Let* P_1 *and* P_2 *be two distributional problems, and* P_1 *be randomized Karp-reducible to* P_2 *with the associated algorithms* $\mathcal{A}$ *and* $\mathcal{B}$*. If* $\mathcal{S}$ *is a witness-oblivious quantum* P_1 *sampler, then* $\mathcal{A}(\mathcal{S})$ *is a witness-oblivious quantum* P_2 *sampler.*

Proof. Let $x_1 \leftarrow \mathcal{S}$ and $x_2 \leftarrow \mathcal{A}(x_1)$. Suppose that there exists a valid QPT extractor $\mathcal{E}_2$ that finds a witness 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 $\mathcal{B}(x_2, y_2, r)$. The output of $\mathcal{B}$ is a witness for x_1 according to the definition of the randomized Karp reduction. One can conclude by noting that $\mathcal{B}$ is indeed a valid extractor for $\mathcal{Q}$. □

Note that the P_2 sampler is witness-oblivious under the hardness assumption of P_1. In some applications, the distribution of the P_2 is fixed and one would like to change the distribution of P_1 so that after applying the reduction, we obtain the fixed distribution. This generally changes the assumption to the hardness of P_1 with the tweaked distribution which does not necessarily hold. Many classical reductions in the context of lattice problems fall into the above framework.

3.4. Solving the $|\mathsf{LWE}\rangle$ Problem for Obliviously Sampling LWE Instances.

We conclude this section by showing how to design a quantum witness oblivious sampler via a single unitary. We show that producing LWE samples in an oblivious manner reduces to synthesizing a quantum state that is a superposition of all LWE samples as defined in [CLZ21]. We call this particular state synthesis problem as $|\mathsf{LWE}\rangle$ problem. It relies on building the following quantum state,

Definition 21 ($|\mathsf{LWE}\rangle$ State)**.** *Let* m, n, q *be integers which are some functions of the security parameter* λ*, and* $\mathbf{A} \overset{def}{=} (\mathbf{a}_1 | \cdots | \mathbf{a}_m)^\top \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$*. Let* f *be an amplitude function whose domain is* $\mathbb{Z}/q\mathbb{Z}$*. The* $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$*-state is defined as*

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

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

To simplify notation, when it is clear from the context, we will drop the dependency on m, n, q*, the error amplitude* 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 $Z_f(\mathbf{A}) \approx q^n$. We will discuss this matter in detail in Subsection **??** when instantiating our algorithm to the case where $|f|^2$, i.e., the noise distribution involved in LWE, is a Gaussian distribution.

Constructing this state was studied in [CLZ21] in order to solve the *Short Integer Solution (SIS)* problem with some particular parameters. We note that [CLZ21] neglected the normalization factor $Z_f(\mathbf{A})$ by assuming that it is always equal to q^n, see for example [CLZ21, Definition 9] and the discussion afterwards in particular [CLZ21, Corollary 9]. However, this is a minor issue since for the parameters choses in [CLZ21], the statement $Z_f(\mathbf{A}) \approx q^n$ holds with overwhelming probability. In the general problem of constructing an $|\mathsf{LWE}\rangle$ state, one should take the normalization into account as we will discuss in Subsection **??**. We must also highlight that [CLZ21, Definition 9] only allows non-negative real-valued amplitude functions, while we allow complex-valued ones.

Although we only use real-valued instantiations of the amplitude function in this work since they are sufficient for our purposes, more choices of the function might have further applications.

Problem 1 ($|\mathsf{LWE}\rangle$ Problem)**.** *Let m, n, q be integers which are some functions of the security parameter λ. For every matrix $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and an amplitude function f over $\mathbb{Z}/q\mathbb{Z}$, the problem of synthesizing the $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$ state is defined as follows:*

- *Input:* $\mathbf{A} \overset{def}{=} \left(\mathbf{a}_1^\top | \cdots | \mathbf{a}_m^\top\right) \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ *and* f*,*
- *Output: the* $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$*-state*

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

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

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

where the e_i's are independently distributed according to the distribution $|f|^2$ while $\mathbf{s}$ has been picked uniformly at random.

In the following theorem, we show that solving the $|\mathsf{LWE}\rangle$ problem using only unitary algorithms can be turned into a witness-oblivious LWE sampler by measuring the final superposition. We assume an algorithm that solves the $|\mathsf{LWE}\rangle$ problem approximately and not perfectly. Such an approximation is sufficient for obtaining the result.

Theorem 1. *Let m, n, q, M be integers which are some functions of the security parameter λ, and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be an amplitude function. Assume that there exists a unitary QPT algorithm $\mathcal{S}$ that, given $\mathbf{A}$ and f as inputs, outputs a quantum state which is at most $\mathsf{negl}(\lambda)$-far from $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f} \otimes |0\rangle^M$ in trace distance.*

Then $\mathcal{S}$ followed by a measurement in the computational basis is a witness-oblivious quantum $\mathsf{LWE}_{q,|f|^2}(\mathbf{A})$ sampler, assuming the quantum hardness of $\mathsf{LWE}_{q,|f|^2}(\mathbf{A})$.

Proof. By assumption, the sampler $\mathcal{S}$ is a sequence of unitary algorithms followed by a single measurement. We can assume that the input of the extractor is the description of the sampler together with its produced sample and its remaining work space, as explained in Lemma 19.

Let $\mathcal{M}$ be the Hilbert space upon which $\mathcal{S}$ performs its measurement, and $\mathcal{W}$ be its remaining working space. Let $|\psi\rangle$ be the final state of the algorithm $\mathcal{S}$ over $\mathcal{H} \otimes \mathcal{W}$, right before the measurement. We have:

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

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

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

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

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

where $q_{\mathbf{x}}$ is the probability of observing $\mathbf{x}$ after sampling an $\mathsf{LWE}_{q,|f|^2}(\mathbf{A})$ instance. Using the properties of trace distance, we obtain:

$$D_{\text{tr}}\left(\text{tr}_{\mathcal{W}}(\sigma_{\mathcal{S}}), \text{tr}_{\mathcal{W}}(\sigma_{\mathsf{LWE}})\right) \le D_{\text{tr}}\left(\sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}}\right) \le D_{\text{tr}}\left(|\psi\rangle \, , \ |\mathsf{LWE}(\mathbf{A})\rangle_{q,f} \otimes |0\rangle^M \right) \le \mathsf{negl}(\lambda).$$

According to the property of the trace distance in Equation (2), we obtain

$$\Delta(\{p_{\mathbf{x}}\}_{\mathbf{x}}, \{q_{\mathbf{x}}\}_{\mathbf{x}}) \le D_{\text{tr}}\left(\text{tr}_{\mathcal{W}}(\sigma_{\mathcal{S}}), \text{tr}_{\mathcal{W}}(\sigma_{\mathsf{LWE}})\right) \le \mathsf{negl}(\lambda).$$

This proves that the sampler $\mathcal{S}$ is a quantum LWE sampler as stated in Definition 15. Let us now show that it is a witness-oblivious quantum samplers according to Definition 18. Let $\mathcal{E}$ be a valid extractor for $\mathcal{S}$. Using the properties of the trace distance, it holds that

$$\begin{aligned}
D_{\mathrm{tr}}\Big(\mathrm{tr}_{\mathcal{W}}\left(\sigma_{\mathcal{S}}\right) \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathcal{S}}\right), \left(\mathrm{tr}_{\mathcal{W}}\left(\sigma_{\mathsf{LWE}}\right) \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathsf{LWE}}\right) \Big) \\
&\leq D_{\mathrm{tr}}\Big(\sigma_{\mathcal{S}} \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathcal{S}}\right), \left(\sigma_{\mathsf{LWE}} \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathsf{LWE}}\right) \Big) \\
&\leq D_{\mathrm{tr}}\Big(\sigma_{\mathcal{S}} \otimes \sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}} \otimes \sigma_{\mathsf{LWE}} \Big) \\
&\leq D_{\mathrm{tr}}(\sigma_{\mathcal{S}} \otimes \sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}} \otimes \sigma_{\mathcal{S}}) + D_{\mathrm{tr}}(\sigma_{\mathsf{LWE}} \otimes \sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}} \otimes \sigma_{\mathsf{LWE}}) \\
&= 2 D_{\mathrm{tr}}(\sigma_{\mathcal{S}}, \sigma_{\mathsf{LWE}}) \\
&\leq \mathsf{negl}(\lambda).
\end{aligned}$$

Let Π_{LWE} be the projection to the subspace

$$\mathrm{span}\big(\{ |\mathbf{b}\rangle \otimes |\mathbf{s}, \mathbf{e}\rangle \ \mid \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \} \big).$$

When applied to a quantum state, the projection Π_{LWE} checks whether the second register contains the secret of the LWE instance in the first register or not. Such a projection is not efficiently implementable if the LWE problem is hard. However, it is useful for expressing the success probability of the extractor as follows:

$$\| \Pi_{\mathsf{LWE}} \big(\mathrm{tr}_{\mathcal{W}}\left(\sigma_{\mathcal{S}}\right) \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathcal{S}}\right) \big) \|^2.$$

Therefore, the bound above implies that

$$\| \Pi_{\mathsf{LWE}} \big(\mathrm{tr}_{\mathcal{W}}\left(\sigma_{\mathcal{S}}\right) \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathcal{S}}\right) \big) \|^2 \leq \| \Pi_{\mathsf{LWE}} \big(\mathrm{tr}_{\mathcal{W}}\left(\sigma_{\mathsf{LWE}}\right) \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathsf{LWE}}\right) \big) \|^2 + \mathsf{negl}(\lambda).$$

Assuming the quantum hardness of $\mathsf{LWE}_{q,|f|^2}(\mathbf{A})$, we have

$$\| \Pi_{\mathsf{LWE}} \big(\mathrm{tr}_{\mathcal{W}}\left(\sigma_{\mathsf{LWE}}\right) \otimes \mathcal{E}\left(\mathsf{Desc}(\mathcal{S}), \sigma_{\mathsf{LWE}}\right) \big) \|^2 = \mathsf{negl}(\lambda),$$

since otherwise $\mathcal{E}$ would be an efficient solver for LWE. Plugging this in the above inequality completes the proof. □

We note that if $\mathbf{A}$ has been sampled uniformly and $|f|^2$ is $\vartheta_{\alpha q}$, the hardness of $\mathsf{LWE}_{q,|f|^2}(\mathbf{A})$ becomes Assumption 1. Consequently, Assumption 3 would be false. Therefore, to break Assumption 3, it suffices to solve the $|\mathsf{LWE}\rangle$ problem for LWE instantiations. However, in the following section we first design an algorithm to solve $|\mathsf{LWE}\rangle$ for an arbitrary amplitude function f and a for almost all matrices $\mathbf{A}$. We will show that our algorithm is polynomial-time under mild assumptions of f, roughly speaking that good a enough approximation over $\widehat{f}$ can be efficiently computed. Then will instantiate our algorithm to the case where f is such that $|f|^2 = \vartheta_{\alpha q}$, in particular we will show that it verifies assumptions for our algorithm to be polynomial-time.

4. Witness-Oblivious Sampler for LWE

In Subsection 3.4 we have shown that a witness-oblivious sampler reduces to solve the $|\mathsf{LWE}\rangle$ problem (see Problem 1). Solving this problem reduces to build the $|\mathsf{LWE}\rangle$ state (see Definition 21) and one may notice that it consists of an m-fold tensor product where each element is a single sample of LWE. Our approach to solve the $|\mathsf{LWE}\rangle$ problem is to single out each of these elements and analyze them independently.

Definition 22 (Coordinate States)**.** *Let q be an integer which is function of the security parameter λ and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be an amplitude function. We define the coordinate states as follows:*

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

4.1. **Solving the $|\mathsf{LWE}\rangle$ Problem for General Amplitudes.** Before going into the details, we would like to briefly explain how our algorithm solves the $|\mathsf{LWE}\rangle$ problem for some arbitrary amplitude f. It proceeds in three steps as follows.

Step 1. First, it builds the following entangled state

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} f^{\otimes m}(\mathbf{e}) |\mathbf{s}\rangle |\mathbf{A}\mathbf{s}+\mathbf{e}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \left|\psi_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle . \tag{7}$$

Step 2. Recover $\langle \mathbf{a}_j, \mathbf{s}\rangle$ with probability p or fail otherwise (in the case of failure the outcome is $\perp$) for each coordinate state $\left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle$. However, this operation is not allowed to "perturb" $\left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle$, it has to be reversible. We avoid this issue by applying some polynomial time unitary that basically maps $\left|\psi_{\langle \mathbf{a}_j,\mathbf{s}\rangle}\right\rangle$ to,

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

and we interpret any quantum states whose last qubit is $|1\rangle$ as $\perp$.

Step 3. Having some linear equations $\langle \mathbf{a}_j, \mathbf{s}\rangle$'s, the next step of the algorithm is to recompute $\mathbf{s}$; enabling us to erase it from the content of the first register, *i.e.,* disentangling the state and solving the $|\mathsf{LWE}\rangle$ problem. However, notice that Step 2 only enables to recover $\langle \mathbf{a}_j, \mathbf{s}\rangle$ with some probability p. Therefore our approach will work if the number of non-$\perp$ coordinates is greater than n in order to hope a non-singular system to solve, namely if

$$mp = n\left(1 + \Omega_n(1)\right).$$

It puts some constraints on the parameters, in particular the number of registers m has to be greater than n/p. Therefore p has to be large enough to ensure polynomial time quantum algorithm. But as we will see it imposes $|\widehat{f}|$ to be flat enough.

By putting everything together, one obtains Algorithm 2. Theorem 3 shows that Algorithm 2 solves the $|\mathsf{LWE}\rangle$ problem in time $\mathsf{poly}(\lambda)$. However some assumptions have to be done.

Theorem 2. *Let m, n be integers and q be a prime integer which are functions of the security parameter λ, and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be an amplitude function such that,*

(1) for all $x \in \mathbb{Z}/q\mathbb{Z}$, $\widehat{f}(x) \neq 0$,

(2) we can compute, $x \mapsto \frac{\min|\widehat{f}|}{\widehat{f}(-x)} + e_{\text{apx}}(x)$ with $e_{\text{apx}} = 2^{-\Omega(\lambda)}$ independently of x, in classical time $\mathsf{poly}(\lambda)$,

(3) we have,

$$\frac{1}{p} = \mathsf{poly}(\lambda) \quad \text{where } p \overset{def}{=} q \min|\widehat{f}|^2.$$

Then Algorithm 2 has running 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

$$D_{\text{tr}}\left(|\varphi\rangle, |\mathsf{LWE}(\mathbf{A})\rangle_{q,f} \otimes |0\rangle\right) = 1 - \mathsf{negl}(\lambda).$$

Crucial steps of Algorithms 2 are Instructions 6 and 7. In the following lemmas we analyze them. In particular it relies on the following unitaries,

(1) XXX

(2) XXX

XXX

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

```
Input: $\mathbf{A} \overset{\text{def}}{=} (\mathbf{a}_1|\cdots|\mathbf{a}_m)^\top \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ and $f$.
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 $|\mathbf{s},\mathbf{e}\rangle \mapsto |\mathbf{s}, \langle\mathbf{a}_1,\mathbf{s}\rangle + e_1, \cdots, \langle\mathbf{a}_m,\mathbf{s}\rangle + e_m\rangle$ to get
     $$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^m f(e_i)\,|\langle\mathbf{a},\mathbf{s}\rangle + e_i\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^m \left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle.$$
5: Append one ancilla $|0\rangle$.
6: Apply the unitary $\mathbf{I}\otimes\mathbf{U}^{\otimes m}$ (where $\mathbf{U}$ is defined in Proposition 1) to obtain
     $$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^m \mathbf{U}\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|0\rangle\,.$$
7: Apply an unambiguous Gaussian elimination algorithm $\mathcal{A}_{\mathrm{GE}}$ (as per Definition 23) in superposition to the $m$-fold tensor product state to find the value of $\mathbf{s}$ and subtract it from the first register, namely apply $\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}$ as given in Equation (14):
     $$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^m \mathbf{U}\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|0\rangle\right).$$
8: Apply $\mathbf{I}\otimes\left(\mathbf{U}^\dagger\right)^{\otimes m}$ and output the resulting quantum state.
```

One of the subroutines of our algorithm for solving the $|\mathsf{LWE}\rangle$ problem is the ability, given $|\psi_j\rangle$ for an unknown index j, to either successfully finds j, or aborts in case of failure. To this aim we will use the decomposition of the $|\psi_j\rangle$'s in the Fourier basis.

Lemma 20. *Using notations of Definition 22, we have:*

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

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

$$\begin{aligned}
|\psi_j\rangle &= \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f\,(e)\,|j+e \bmod q\rangle \\
&= \frac{1}{\sqrt{q}} \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f\,(e) \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \omega_q^{-(j+e)x}\,|\chi_x\rangle \quad \text{(by Lemma 2)} \\
&= \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{1}{\sqrt{q}} \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f\,(e)\,\omega_q^{-xe} \right) \omega_q^{-jx}\,|\chi_x\rangle \\
&= \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \widehat{f}\,(-x)\,\omega_q^{-jx}\,|\chi_x\rangle\,.
\end{aligned}$$

□

According to this lemma, the $|\psi_j\rangle$'s are orthogonal quantum states if $\widehat{f}$ is a constant function. In other words, if $\widehat{f}$ is constant, then with certainty we can recover j given $|\psi_j\rangle$ as we aim. However, in our case we cannot afford this assumption as $|f|^2$ is the noise distribution involved in LWE. But this discussion motivates to introduce the unitary that basically multiplies amplitudes by $1/\widehat{f}(x)$ in the Fourier basis.

Proposition 1. *Let $f : \mathbb{Z}/\mathbb{Z} \to \mathbb{C}$ be an amplitude function such that for all $x \in \mathbb{Z}/q\mathbb{Z}$,*

$$\widehat{f}(x) \neq 0,$$

Let $\mathbf{U}$ be the following unitary operator,

$$\forall x \in \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{U}\,|\chi_x\rangle\,|0\rangle = |\chi_x\rangle \left(u_x\,|0\rangle + \sqrt{1-|u_x|^2}\,|1\rangle \right) \tag{8}$$

where u_x is a $\mathsf{poly}(\lambda)$-bits integer such that,

$$\forall x \in \mathbb{Z}/q\mathbb{Z}, \quad u_x \overset{def}{=} \frac{\min|\widehat{f}|}{\widehat{f}(-x)} + e_{\text{apx}}(x)$$

with $e_{\text{apx}}(x) = 2^{-\Omega(\lambda)}$ independently of x. Then,

$$\forall j \in \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{U}\,|\psi_j\rangle\,|0\rangle = \sqrt{p_{\text{succ}}}\,|j\rangle\,|0\rangle + \sqrt{1-p_{\text{suc}}}\,|a\rangle\,|1\rangle + |\text{error}\rangle$$

where $|a\rangle$ is an arbitrary quantum state and,

$$p_{\text{succ}} \overset{def}{=} q\,\min|\widehat{f}|^2 \quad ; \quad \|\text{error}\| = 2^{-\Omega(n)}.$$

Proof. By definition,

$$\begin{aligned}
\mathbf{U}\,|\psi_j\rangle\,|0\rangle &= \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \mathbf{U}\,\widehat{f}(-x)\omega_q^{-jx}\,|\chi_x\rangle\,|0\rangle \\
&= \underbrace{\left(\sum_{x \in \mathbb{Z}/q\mathbb{Z}} u_x\,\widehat{f}(-x)\,\omega_q^{-jx}\,|\chi_x\rangle \right)}_{\overset{\text{def}}{=}|\varphi\rangle} |0\rangle + \underbrace{\left(\sum_{x \in \mathbb{Z}/q\mathbb{Z}} \sqrt{1-|u_x|^2}\,\widehat{f}(-x)\,\omega_q^{-jx}\,|\chi_x\rangle \right)}_{|\psi\rangle} |1\rangle
\end{aligned}$$

Let us compute $|\varphi\rangle$, by definition of u_x,

$$\begin{aligned}|\varphi\rangle &= \sqrt{q}\min|\widehat{f}|\left(\frac{1}{\sqrt{q}}\sum_{x\in\mathbb{Z}/q\mathbb{Z}}\omega_q^{-jx}|\chi_x\rangle\right)+\sum_{x\in\mathbb{Z}/q\mathbb{Z}}e_{\mathrm{apx}}(x)\widehat{f}(-x)\omega_q^{-jx}|\chi_x\rangle\\ &= \sqrt{p_{\mathrm{succ}}}\,|j\rangle + |\mathrm{error}_1\rangle\end{aligned}$$

Notice that,

$$\|\,|\mathrm{error}\rangle_1\,\|^2 = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} e_{\mathrm{apx}}(x)^2\;|\widehat{f}(-x)|^2 = \sum_{x\in\mathbb{Z}/q\mathbb{Z}} 2^{-\Omega(\lambda)}\;|\widehat{f}(-x)|^2 = 2^{-\Omega(\lambda)}$$

where we used that by assumption $e_{\mathrm{apx}}(x) = 2^{-\Omega(\lambda)}$. Therefore,

$$\mathbf{U}\,|\psi_j\rangle\,|0\rangle = \sqrt{p_{\mathrm{succ}}}\,|j\rangle\,|0\rangle + |\mathrm{error}_1\rangle\,|0\rangle + |\psi\rangle\,|1\rangle \tag{9}$$

Notice that $\mathbf{U}\,|\psi_j\rangle\,|0\rangle$ has to be a quantum state as $\mathbf{U}$ is unitary. Furthermore, $\|\,|\mathrm{error}_1\rangle\,\| = 2^{-\Omega(\lambda)}$. Therefore,

$$|\psi\rangle\,|1\rangle = \sqrt{1-p_{\mathrm{succ}}}\,|a\rangle\,|1\rangle + |\mathrm{error}_2\rangle\,|1\rangle$$

for some quantum state $|a\rangle$ and with $\|\,|\mathrm{error}_2\rangle\,\| = 2^{-\Omega(\lambda)}$. Plugging this into Equation (9) concludes the proof. □

Remark 1. ***[Thomas : relation to* [CB98]*]***

This proposition shows that $\mathbf{U}$

Lemma 21. *Using notations of Proposition 1, suppose furthermore that it exists a classical algorithm computing*

$$x \mapsto u_x$$

in time $\mathsf{poly}(\lambda)$. *Then we can run* $\mathbf{U}$ *in time* $\mathsf{poly}(\lambda)$.

Proof. By assumption $u_x \in \mathbb{C}$ has $\mathsf{poly}(\lambda)$-bits. Without loss of generality we can suppose that u_x is written as (m_x, θ_x) where m_x and θ_x are $p = \mathsf{poly}(\lambda)$-bits integers corresponding to its magnitude and phase, respectively. As $x \mapsto u_x$ is computable in time $\mathsf{poly}(\lambda)$, we can compute the following unitary in quantum-time $\mathsf{poly}(\lambda)$,

$$\mathbf{O}_u : |x\rangle\,\left|0^{2p}\right\rangle \mapsto |x\rangle\,|m_x\rangle\,|\theta_x\rangle$$

Consider now the following two unitaries:

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

where $\widetilde{y} = \sum_{i=1}^{p} y_i/2^i$ and $\widetilde{z} = \sum_{i=1}^{p} z_i/2^i$. One can verify that

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

Unitary $\mathbf{M}$ can be implemented with $O(p)$ number of gates [dW23, Ch. 9, Exercise 7.a]. Furthermore,

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

It shows that one only requires p controlled gates to implement $\boldsymbol{\Theta}$. This completes the proof. □

Algorithm 2 will crucially use this unitary as subroutine to solve LWE but also the following variant of Gaussian elimination.

Definition 23 (Unambiguous Gaussian Elimination)**.** *An unambiguous Gaussian elimination is defined as a classical algorithm $\mathcal{A}_{\mathrm{GE}}$ that solves the following problem by performing a Gaussian elimination:*

- *Input:* $\mathbf{A} \stackrel{\text{def}}{=} \left(\mathbf{a}_1^\top|\cdots|\mathbf{a}_m^\top\right) \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ *and* $(y_i)_{1\leq i\leq m}$ *where* $y_i = \langle \mathbf{a}_i, \mathbf{s}\rangle$ *or* $y_i = \perp$,

- *Output:* $\mathbf{s}$ *or* $\perp$.

We define $p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}, p)$ *as being the success probability of* $\mathcal{A}_{\mathrm{GE}}$*:*

$$p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}, p) \overset{def}{=} \mathbb{P}_{\mathbf{y}}\left(\mathcal{A}_{\mathrm{GE}}(\mathbf{A}, \mathbf{y}) = \mathbf{s}\right) \tag{10}$$

when the coordinates of $\mathbf{y}$ *are independently distributed as follows:*

$$\mathbb{P}\left(y_i = \langle \mathbf{a}_i, \mathbf{s}\rangle\right) = p \quad \textit{and} \quad \mathbb{P}\left(y_i = \perp\right) = 1 - p.$$

The unambiguity of $\mathcal{A}_{\mathrm{GE}}$, meaning that it outputs $\perp$ in the case of failure, will be required for our application (see the proof of Theorem 3 in Appendix A.2).

Notice that if the number of non-$\perp$ coordinates, for example $y_i = \langle \mathbf{a}_i, \mathbf{s}\rangle$, is greater than n, namely

$$mp = n\left(1 + \Omega_n(1)\right),$$

then $\mathcal{A}_{\mathrm{GE}}$ is reduced to solving an overdetermined linear system to recover $\mathbf{s}$. Therefore, the algorithm will be successful as soon as the underlying linear system has full rank. In our application, we will consider matrices $\mathbf{A}$ (for instance uniform matrices) for which the above holds with a probability exponentially close to 1, namely:

$$p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}, p) = 1 - q^{-\Omega(n)}.$$

4.2. **Solving the $|\mathsf{LWE}\rangle$ Problem for General Amplitudes.** Before going into the details, we would like to briefly explain how one can efficiently solve the $|\mathsf{LWE}\rangle$ problem. Let $\{\mathbf{E}_i\}_{i\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ be an unambiguous POVM for coordinate states, and $\mathcal{A}_{\mathrm{GE}}$ be an unambiguous Gaussian elimiation subroutine. The algorithm proceeds in three steps as follows.

1) First, it builds the following entangled state

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} f^{\otimes m}(\mathbf{e})\,|\mathbf{s}\rangle\,|\mathbf{A}\mathbf{s} + \mathbf{e}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \left|\psi_{\langle \mathbf{a}_i, \mathbf{s}\rangle}\right\rangle. \tag{11}$$

2) By applying the given POVM $\{\mathbf{E}_i\}_{i\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ over each coordinate state $\left|\psi_{\langle \mathbf{a}_j, \mathbf{s}\rangle}\right\rangle$, the algorithm would recover $\langle \mathbf{a}_j, \mathbf{s}\rangle$ with probability p or fail otherwise (in the case of failure the outcome is $\perp$). However, applying such a quantum measurement would disturb the state $\left|\psi_{\langle \mathbf{a}_j, \mathbf{s}\rangle}\right\rangle$ which would not necessarily be reversible. We avoid this issue by not applying the measurement, but emulating the behaviour of the measurement in a Hilbert space of greater dimension.

3) Having some linear equations $\langle \mathbf{a}_j, \mathbf{s}\rangle$'s, the next step of the algorithm is to recompute $\mathbf{s}$; enabling us to erase it from the content of the first register, *i.e.*, disentangling the state and solving the $|\mathsf{LWE}\rangle$ problem. To do so, the algorithm uses the unambiguous Gaussian elimination in superposition.

By putting everything together, one obtains Algorithm 2.

Theorem 3 shows that Algorithm 2 solves the $|\mathsf{LWE}\rangle$ problem.

Theorem 3. *Let* m, n, q *be integers,* $p \in [0, 1]$*,* $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ *be an amplitude function,* T_f *be a runtime upper bound on a single evaluation of* f*, and* $\mathbf{A}$ *be a matrix in* $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$*. Let* $\mathcal{A}_{\mathrm{GE}}$ *be an unambiguous Gaussian elimination algorithm as per Definition 23, and* $\{\mathbf{E}_i\}_{i\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ *be an unambiguous rank-one* POVM *for coordinate states as per Definition* **??** *with success probability* p *and runtime* $T_{\mathbf{E}}$*.*

Algorithm 2 Quantum $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$ Solver.

```
Input: $\mathbf{A} \overset{\text{def}}{=} (\mathbf{a}_1|\cdots|\mathbf{a}_m)^\top \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ and $f$.
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 $|\mathbf{s},\mathbf{e}\rangle \mapsto |\mathbf{s}, \langle\mathbf{a}_1,\mathbf{s}\rangle + e_1, \cdots, \langle\mathbf{a}_m,\mathbf{s}\rangle + e_m\rangle$ to get
     $$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^{m} f(e_i)\,|\langle\mathbf{a},\mathbf{s}\rangle + e_i\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle .$$
5: Append $m$ ancillas $|0\rangle \in \mathbb{C}^{q+1}$ (whose computational basis is $(|i\rangle)_{i\in[\![0,q-1]\!]\cup\{\perp\}}$).
6: Apply the unitary $\mathbf{I}\otimes\mathbf{V}^{\otimes m}$ (where $\mathbf{V}$ is defined in Equation (13)) to obtain
     $$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \mathbf{V}\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |0\rangle .$$
7: Apply an unambiguous Gaussian elimination algorithm $\mathcal{A}_{\mathrm{GE}}$ (as per Definition 23) in superposition to the $m$-fold tensor product state to find the value of $\mathbf{s}$ and subtract it from the first register, namely apply $\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}$ as given in Equation (14):
     $$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}\left(\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \mathbf{V}\left|\psi_{\langle\mathbf{a}_i,\mathbf{s}\rangle}\right\rangle |0\rangle\right) .$$
8: Apply $\mathbf{I}\otimes\left(\mathbf{V}^\dagger\right)^{\otimes m}$ and output the resulting quantum state.
```

Then Algorithm 2 has running time $\mathsf{poly}\left(m, q, T_{\mathbf{E}}, T_f\right)$ [6] *and outputs a quantum state* $|\varphi\rangle$ *such that*

$$D_{\mathrm{tr}}\left(|\varphi\rangle\,, |\mathsf{LWE}(\mathbf{A})\rangle_{q,f} \otimes |0\rangle^{\otimes m\log(q+1)}\right) = \sqrt{1 - \frac{q^n}{Z_f(\mathbf{A})}\, p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A},p)^2}\ .$$

We use this theorem to obtain an efficient witness-oblivious $\mathsf{LWE}_{q,|f|^2}(\mathbf{A})$ sampler. Note that Algorithm 2 is unitary. It paves the way for applying Theorem 1. To do so, we need the trace distance above, between the outcome of the algorithm and $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$, to be negligible, and the runtime of the algorithm to be polynomial. In particular, it is sufficient if we have the following conditions:

(1) The probability $p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A},p)$ is overwhelming. Note that it depends on the distribution of $\mathbf{A}$ and the success probability of the POVM. If mp is sufficiently large, for instance

$$mp = n\big(1 + \Omega_n(1)\big), \tag{12}$$

and $\mathbf{A}$ is full-rank, then $\mathcal{A}_{\mathrm{GE}}$ succeeds with probability $1 - q^{\Omega(n)}$.

(2) The quantity $Z_f(\mathbf{A})$ is not much larger than q^n. We note that it depends on the distribution of $\mathbf{A}$, and the amplitude function f.

[6] **[Pouria : @thomas: you say I put mT_E instead of m, T_E? If yes, what is the issue of the current one?]**

To deal with (1), we exhibit a POVM in Subsection 4.3 whose success probability is given by

$$p = q \cdot \min \left| \widehat{f} \right|^2 ,$$

where f corresponds to the amplitude of errors in the $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$ state. Its runtime is polynomial in q and T_f. For typical cryptographic applications, we choose f such that $|f|^2$ is a folded discrete Gaussian distribution $\vartheta_{\alpha q}$ where α is non-negligible in n and $\alpha q \geq 2\sqrt{n}$. One might naturally choose f as $\sqrt{\vartheta_{\alpha q}}$. But choosing such a function f leads to (as shown in Lemma 27)

$$p = q \cdot \min \left| \widehat{f} \right|^2 = O\left(e^{-\pi \alpha^2 q^2} \right) .$$

Therefore, a direct application of Theorem 3 with the POVM of Subsection 4.3 gives a not so interesting result; for mp to be sufficiently large as in Equation (12), one requires an exponentially large m. In particular, it implies an exponential time algorithm as a function of q (note that the parameter α cannot be too small otherwise the considered LWE problem becomes easy). We will be fixing this issue in Subsection 4.4. To briefly discuss the idea, we note that adding phases into the amplitudes f does not change the distribution of the measurement: the outcome of measuring $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$ only depends on $|f|^2$. Using this idea, we show how to add the phases to the function f above to get a success probability p of order $\approx 1/(\alpha q)$ in Corollary 2. Therefore, the parameters of the LWE problem would need to satisfy a weaker condition $m/n \approx \alpha q$ to imply Equation (12).

Once (1) is handled, we will deal with (2) in Subsection 4.5. The normalization factor $Z_f(\mathbf{A})$ is a function of f and $\mathbf{A}$. So far, we only assumed that $\mathbf{A}$ belongs to $(\mathbb{Z}/q\mathbb{Z})^{m \times n}$. We will show that $Z_f(\mathbf{A}) \leq q^n + 1$ with overwhelming probability when $\mathbf{A}$ is picked uniformly and q is prime.

In [CLZ21], the authors also propose a generic algorithm to construct an $|\mathsf{LWE}\rangle$ state based on a "filtering out" technique. Their approach can be seen as a variant of Algorithm 2 where the POVM is replaced by a projective measurement.

Outline of the proof of Theorem 3. After constructing the quantum state given in Equation (11), Algorithm 2 performs the POVM $\{\mathbf{E}_i\}_{i \in (\mathbb{Z}/q\mathbb{Z}) \cup \perp}$ on its last m registers to obtain some of the values of $\langle \mathbf{a}_i, \mathbf{s} \rangle$'s. Then, by performing a Gaussian elimination, it recovers $\mathbf{s}$. However, the information given by the $\langle \mathbf{a}_i, \mathbf{s} \rangle$'s has to be exploited quantumly. To achieve this, we use the interpretation of a POVM as a projective measurement in a higher-dimensional space. More precisely, we will use the following unitary $\mathbf{V}$:

$$\mathbf{V} : |\psi\rangle |0\rangle \longmapsto \sum_{i=0}^{q-1} \sqrt{\mathbf{E}_i} |\psi\rangle |i\rangle + \sqrt{\mathbf{E}_\perp} |\psi\rangle |\perp\rangle , \tag{13}$$

where $|0\rangle$ is the ancilla state in $\mathbb{C}^{q+1}$ whose orthonormal basis is $\{|i\rangle\}_{i \in (\mathbb{Z}/q\mathbb{Z}) \cup \{\perp\}}$. We note that if the POVM is computable in time $T_{\mathbf{E}}$, then one can construct this unitary in time $\mathsf{poly}(T_{\mathbf{E}})$ as discussed in [vAG18, Section 4.1].

Lemma 22. *Using the notations above, we have*

$$\forall i \in \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{V} |\psi_i\rangle |0\rangle = \sqrt{p} |\varphi_i\rangle |i\rangle + \sqrt{1-p} |\varphi_{i,\perp}\rangle |\perp\rangle ,$$

for some quantum states $\{|\varphi_i\rangle , |\varphi_{i,\perp}\rangle\}_{i \in \mathbb{Z}/q\mathbb{Z}}$.

Proof. See Appendix A.2. □

According to this lemma, the values $\langle \mathbf{a}_i, \mathbf{s} \rangle$ appear in the second register of $\mathbf{V} \left| \psi_{\langle \mathbf{a}_i, \mathbf{s} \rangle} \right\rangle |0\rangle$. Therefore, performing an unambiguous Gaussian elimination $\mathcal{A}_{\mathrm{GE}}$ (as given in Definition 23), namely applying the unitary

$$\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}} : \ |\mathbf{s}\rangle |\varphi\rangle |\mathbf{y}\rangle \mapsto |\mathbf{s} - \mathcal{A}_{\mathrm{GE}}(\mathbf{A}, \mathbf{y})\rangle |\varphi\rangle |\mathbf{y}\rangle \tag{14}$$

to the quantum state

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

will allow us to erase $\mathbf{s}$ from the first register. Recall that the success probability of $\mathcal{A}_{\mathrm{GE}}(\mathbf{A}, \mathbf{y})$ is $p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}, p)$. Hence, after applying the unitary $\mathbf{U}_{\mathcal{A}_{\mathrm{GE}}}$, one will obtain a quantum state

$$|\psi\rangle \stackrel{\text{def}}{=} \mathbf{U}_{\mathcal{A}_{\mathrm{GE}}} \left(\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n} |\mathbf{s}\rangle \bigotimes_{i=1}^{m} \mathbf{V} \left|\psi_{\langle \mathbf{a}_i, \mathbf{s}\rangle}\right\rangle |0\rangle \right) \tag{15}$$

that is close with respect to the trace distance to the disentangled state

$$|\psi_{\mathrm{ideal}}\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{Z_f(\mathbf{A})}} \sum_{\mathbf{s} \in (\mathbb{Z}/q\mathbb{Z})^n} |0\rangle \bigotimes_{i=1}^{m} \mathbf{V} \left|\psi_{\langle \mathbf{a}_i, \mathbf{s}\rangle}\right\rangle |0\rangle . \tag{16}$$

Note that applying $\mathbf{I} \otimes \mathbf{V}^{\dagger} \otimes \mathbf{I}$ to the state above yields

$$|\mathsf{LWE}(\mathbf{A})\rangle_{q,|f|^2} \otimes |0\rangle^{\otimes m \log(q+1)} .$$

Lemma 23. *Using the notations of Theorem 3, we have*

$$D_{\mathrm{tr}}\left(|\psi\rangle, |\psi_{\mathrm{ideal}}\rangle\right) \leq \sqrt{1 - \frac{q^n}{Z_f(\mathbf{A})}\, p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}, p)^2}.$$

Proof. See Appendix A.2. □

Proof of Theorem 3. In Step 7 of Algorithm 2, the quantum state can be described as in Equation (15). To complete the proof, it suffices to apply Lemma 24. Concerning the running time, note that preparing the superposition of all vectors in $(\mathbb{Z}/q\mathbb{Z})^m$ costs $O(m \log^2 q)$ steps using quantum Fourier transform. Preparing the quantum state whose amplitudes are chosen according to the function f is doable in time $O(\sqrt{q}\, T_f)$. We must apply the unitary $\mathbf{V}$ to each component of the m-fold tensor product which costs $O(mT_{\mathbf{E}})$. At the end, the unambiguous Gaussian elimination runs in time $O(m^3)$. □

4.3. **Unambiguous Discrimination of Coordinate States.** As outlined previously, one ingredient for Algorithm 2 for successfully solving the $|\mathsf{LWE}\rangle$ problem is a POVM that unambiguously distinguishes coordinate states. We will use the POVM given in [CB98]. In particular, when applied to a set of states with a symmetrical property, the success probability is "maximal" over all possible measurements. The symmetrical condition is that there exists a unitary $\mathbf{T}$ such that

$$\forall j \in \mathbb{Z}/q\mathbb{Z} : \ \mathbf{T}\,|\psi_j\rangle = |\psi_{j+1 \bmod q}\rangle . \tag{17}$$

One can verify that the *translation* unitary satisfies above statement for coordinate states. We provide the POVM in the following theorem.

Theorem 4. *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 T_f be an upper bound for each evaluation of f. Let*

$$\left|\psi_j^{\perp}\right\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{N}} \sum_{y \in \mathbb{Z}/q\mathbb{Z}} \overline{\widehat{f}(-y)^{-1}}\, \omega_q^{-jy} \,|\chi_y\rangle\,, \text{ where } N \stackrel{\text{def}}{=} \sum_{y \in \mathbb{Z}/q\mathbb{Z}}^{q-1} |\widehat{f}(y)|^{-2}, \tag{18}$$

and

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

where λ_+ is the maximum eigenvalue of $\sum_{j \in \mathbb{Z}/q\mathbb{Z}} \left|\psi_j^{\perp}\middle\rangle\middle\langle\psi_j^{\perp}\right|$. Then the set $\{\mathbf{E}_j\}_{j \in (\mathbb{Z}/q\mathbb{Z}) \cup \{\perp\}}$ is a POVM *that unambiguously distinguishes the coordinate states (as given in Definition 22) with success probability p as follows:*

$$p = q \cdot \min_{y \in \mathbb{Z}/q\mathbb{Z}} \left|\widehat{f}(y)\right|^2 .$$

Furthermore, this is the maximal success probability over all possible POVMs, and one can construct it in time $\mathsf{poly}(q, T_f)$.

We require the following lemmas. Representating the coordinate states in the Fourier basis is helpful to approach the problem. The first lemma is an implication of this. It shows that $\left|\psi_i^\perp\right\rangle$ defined as in Equation (18) is a quantum state orthogonal to all $|\psi_j\rangle$'s where $i \neq j$.

Lemma 24. *Using the notations of Theorem 4, we have:*

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

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

$$\begin{aligned} |\psi_j\rangle &= \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f(e) \, |j + e \bmod q\rangle \\ &= \frac{1}{\sqrt{q}} \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f(e) \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \omega_q^{-(j+e)x} \, |\chi_x\rangle \quad \text{(by Lemma 2)} \\ &= \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \left(\frac{1}{\sqrt{q}} \sum_{e \in \mathbb{Z}/q\mathbb{Z}} f(e) \, \omega_q^{-xe} \right) \omega_q^{-jx} \, |\chi_x\rangle \\ &= \sum_{x \in \mathbb{Z}/q\mathbb{Z}} \widehat{f}(-x) \, \omega_q^{-jx} \, |\chi_x\rangle \, . \end{aligned}$$

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

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

This completes the proof. □

The second lemma is concerned with the maximum eigenvalue λ_+ of $\sum_{j \in \mathbb{Z}/q\mathbb{Z}} \left|\psi_j^\perp\middle\rangle\!\middle\langle\psi_j^\perp\right|$.

Lemma 25. *Using notations of Theorem 4, 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:

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

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

By Lemma 25, the state $\left|\psi_i^\perp\right\rangle$ 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

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

where the two last equalities follow from Lemmas 25 and 26.

For performing the POVM, one must build the unitary $\mathbf{W}$ that maps $|0\rangle$ to $\left|\psi_j^\perp\right\rangle$. To do so, we first classically compute the Fourier of f, reciprocate the result to obtain $1/\widehat{f}$, and compute the Fourier of $1/\widehat{f}$ in $\mathsf{poly}(q, T_f)$ time. This is the amplitudes of $\left|\psi_j^\perp\right\rangle$. Then according to Lemma 4, one can perfectly build $\mathbf{W}$ and thus perform the projection in $\mathsf{poly}(q, T_f)$ time. □

4.4. **Instantiation with the Gaussian Distribution.** In Subsection 4.3, we showed that the probability of success for our POVM is

$$q\cdot \min\left|\widehat{f}\right|^2 ,$$

where $|f|^2$ is the error amplitude in $|\mathsf{LWE}(\mathbf{A})\rangle_{q,f}$. In our applications, we are interested in the case where $|f|^2$ is a folded Gaussian distribution modulo q, i.e.,the distribution $\vartheta_{\alpha q}$ from Definition 8. A natural choice for f is $\sqrt{\vartheta_{\alpha q}}$ wherein the above minimum is given by the following proposition.

Lemma 26. *Let n be an integer, $q = \Omega(n)$, and $\alpha = O(1/\sqrt{q})$. Let $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be such that*

$$f \overset{def}{=} \sqrt{\vartheta_{\alpha q}},$$

Then, we have

$$q\cdot \min|\widehat{f}|^2 = O\left(e^{-\pi\alpha^2 q^2}\right) .$$

Proof. See Appendix A.3. □

Therefore, the success probability p of the POVM in Section 4.3 for the function f chosen as above is exponentially small in the standard deviation αq. Recall that one condition for the successful termination of Algorithm 2 is

$$mp = (1+\Omega_n(1))n,$$

The result above shows that, for this condition holds, one would require an exponentially large m for the particular choice of f in the discussion above. It is thus not efficient to solve the $|\mathsf{LWE}\rangle$ problem. However, one may notice that adding some phases to f does not have any measurement effect with respect to the same basis, and therefore after measuring the state, one still obtains an LWE sample with the same distribution. In the following theorem, we show how to choose these phases in order to sufficiently increase the success probability $q\cdot\min|\widehat{f}|^2$ of the POVM.

Theorem 5. *Let q be an integer and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be such that for all $x \in \mathbb{Z}/q\mathbb{Z}$ it holds that $f(-x) = -f(x)$. Then we have*

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

Proof. The discrete Fourier transform of f is given by,

$$\begin{aligned}\widehat{f}(y) &= \frac{1}{\sqrt{q}}\sum_{x\in[\![0,\lfloor\frac{q}{2}\rfloor]\!]} f(x)\,\omega_q^{xy} - \frac{1}{\sqrt{q}}\sum_{x\in[\![-\lceil\frac{q}{2}\rceil,-1]\!]} f(x)\,\omega_q^{xy}\\ &= \frac{f(0)}{\sqrt{q}} + \frac{1}{\sqrt{q}}\sum_{x\in[\![1,\lfloor\frac{q}{2}\rfloor]\!]} f(x)\left(\omega_q^{xy} - \omega_q^{-xy}\right) \quad \text{(we used that } f(-x) = -f(x))\\ &= \frac{f(0)}{\sqrt{q}} + i\,\frac{2}{\sqrt{q}}\sum_{x\in[\![1,\lfloor\frac{q}{2}\rfloor]\!]} f(x)\,\sin\frac{2\pi xy}{q} .\end{aligned}$$

The theorem follows by taking the norm squared of $\widehat{f}(y)$. □

We have the following corollary as a special case for the distribution $\vartheta_{\alpha q}$.

Corollary 2. *Let $\alpha \in (0,1)$, q be an integer and $f : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be such that*

$$f(x) \overset{def}{=} \begin{cases} \sqrt{\vartheta_{\alpha q}(x)} & \textit{if } 0 \leq x \leq \lfloor \frac{q}{2} \rfloor, \\ -\sqrt{\vartheta_{\alpha q}(x)} & \textit{otherwise.} \end{cases}$$

Then we have

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

Proof. Note that $f(-x) = -f(x)$. Therefore, using the positivity of $\vartheta_{\alpha q}$, we obtain

$$q \cdot \min |\widehat{f}|^2 \geq \vartheta_{\alpha q}(0) \geq \rho_{\alpha q}(\mathbb{Z})^{-1}. \tag{19}$$

We complete the proof by noting that Lemma 11 implies $\rho_{\alpha q}(\mathbb{Z})^{-1} \geq \frac{1}{1+\alpha q}$. □

Adding -1 phases "exponentially" increases the success probability of the POVM which allows us to choose m (the number of LWE samples) in Theorem 1 to be of order $\Omega(n\alpha q)$ as required in Equation (12). This improvement is crucial as m roughly determines the time complexity of the algorithm for obliviously producing LWE samples. However, in some practical cases, such as those of Section 6, αq is superpolynomially large: typically we have $\alpha q = \sqrt{q}$ where q is itself chosen to be exponentially large with respect to n. In other words, what we have just presented seems to be insufficient in this setting as it requires m to be exponentially large. Hopefully, we will show in Section 5.2 that we can extend it to other regimes of parameters of LWE using self-reductions of LWE.

4.5. About the Normalization Factor $Z_f(\mathbf{A})$.

For a matrix $\mathbf{A}$ in $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, recall that $Z_f(\mathbf{A})$ is the norm of the following vector.

$$\sum_{\mathbf{s}\in(\mathbb{Z}/q\mathbb{Z})^n} \sum_{\mathbf{e}\in(\mathbb{Z}/q\mathbb{Z})^m} \bigotimes_{i=1}^{m} f(e_i) \left| \langle \mathbf{a}_i, \mathbf{s}\rangle + e_i \bmod q \right\rangle . \tag{20}$$

The quantitiy of this variable directly affects the success probability of Algorithm 2 as shown in Theorem 3. We discussed earlier, that for our purposes, it suffices to have $Z_f(\mathbf{A}) \leq q^n + 1$ with overwhelming probability when $\mathbf{A}$ is sampled uniformly. In particular, when f is instantiated such that $|f| = \sqrt{\vartheta_{\alpha q}}$, this condition imposes an upper bound on the quantity of α. We will determine how large α can be chosen with respect to this condition.

Recall that image of $\mathbf{A}(\mathbb{Z}/q\mathbb{Z})^{m\times n}$ is defined as follows:

$$\mathrm{Im}(\mathbf{A}) \overset{\text{def}}{=} \{\mathbf{A}\mathbf{x} \mid \mathbf{x} \in (\mathbb{Z}/q\mathbb{Z})^n\} \subseteq (\mathbb{Z}/q\mathbb{Z})^m.$$

We begin by relating $Z_f(\mathbf{A})$ to the image of $\mathbf{A}$ and the function $|f|$.

Lemma 27. *Let n, m, q be integers, $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$, f be an amplitude funtion, and $Z_f(\mathbf{A})$ be defined as above. Then we have:*

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

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:

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

One can verify that for two vectors $\mathbf{e}, \mathbf{e}'$, we have

$$\langle \mathrm{Im}(\mathbf{A}) + \mathbf{e}' | \mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle = \begin{cases} q^n & \text{if } \mathbf{e} - \mathbf{e}' \in \mathrm{Im}(\mathbf{A}), \\ 0 & \text{otherwise.} \end{cases} \tag{21}$$

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

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

Therefore, we have

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

The above term is equal to:

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

where we used Equation (21).

On the other hand, we have the following inequalities.

$$\begin{aligned} Z_f(\mathbf{A}) = |Z_f(\mathbf{A})| &= \Bigg|q^n \sum_{\mathbf{e},\mathbf{e}':\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} f(\mathbf{e})\overline{f(\mathbf{e}')}\Bigg| \\ &\le q^n \sum_{\mathbf{e},\mathbf{e}':\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} |f(\mathbf{e})|\cdot|f(\mathbf{e}')| \quad \text{(by triangle inequality)} \\ &= q^n \sum_{\mathbf{e},\mathbf{e}':\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} |f|(\mathbf{e})\cdot|f|(\mathbf{e}'). \end{aligned}$$

□

Let $\mathbf{A}\in(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and λ_1 be the norm of a shortest non-zero vector $\mathbf{x}$ with respect to the ℓ_2 norm of the following lattice:

$$\Lambda_q(\mathbf{A}) = \mathbf{A}(\mathbb{Z}/q\mathbb{Z})^n + q\mathbb{Z}^m.$$

Consider the following representation of $\mathbb{Z}/q\mathbb{Z}$:

$$\mathbb{Z}/q\mathbb{Z} = \Big\{ j \ :\ -\lceil \tfrac{q}{2}\rceil \le j \le \lfloor \tfrac{q}{2}\rfloor \Big\}\,.$$

Every element of $\mathrm{Im}(\mathbf{A})$ belongs to $\Lambda_q(\mathbf{A})$ with respect to the above representation. Moreover, if $\mathbf{y}\in\mathrm{Im}(\mathbf{A})$, then it holds that $\|\mathbf{y}\|\ge\|\mathbf{x}\|_{\ell_2}$ where the norm of $\mathbf{y}$ is defined as in Equation (1). Therefore, the quantity of $Z_f(\mathbf{A})$ depends on how wide is $|f|$ with respect to λ_1. For example, if $|f|$ vanishes beyond $\lambda_1/2$, then we have

$$\begin{aligned} Z_f(\mathbf{A}) \ &\le\ q^n \sum_{\mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \\ &=\ q^n \sum_{\mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})\setminus\{\mathbf{0}\}} |f|(\mathbf{e})\cdot|f|(\mathbf{e}')\ +\ q^n \\ &\le\ q^n \sum_{\|\mathbf{e}-\mathbf{e}'\|\ge\lambda_1} |f|(\mathbf{e})\cdot|f|(\mathbf{e}')\ +\ q^n \\ &=\ q^n. \end{aligned}$$

By developing this intuition, one can bound the quantity $Z_f(\mathbf{A})$ over q-ary lattices. However, we proceed by another approach which gives much better bounds on the width of $|f|$. Let $|f| = \sqrt{\vartheta_{\alpha q}}$, and $\mathbf{A}\in(\mathbb{Z}/q\mathbb{Z})^{m\times n}$ be chosen uniformly. In particular, we show that α can be as large as $1/(m\sqrt{\ln q})$.

The downfall of this approach is that we can only use it for the case of plain LWE problem when the modulus q is prime. For the non-prime modulus or the MLWE problem we will proceed in the way discussed above.

LWE case. We begin by the following lemma. A version appeared in [DRT21].

Lemma 28. *Let $n, m \geq n+1$ be integers, q be a prime integer, $\mathbf{A}$ be sampled uniformly from $(\mathbb{Z}/q\mathbb{Z})^{m\times n}$, and f be an amplitude function over $\mathbb{Z}/q\mathbb{Z}$. Let $Z_f(\mathbf{A})$ be defined as above. Then we have*

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

for every $\delta > 0$.

Proof. In Lemma 28, we showed that

$$\begin{aligned} Z_f(\mathbf{A}) = |Z_f(\mathbf{A})| &= \left| q^n \sum_{\mathbf{e},\mathbf{e}':\ \mathbf{e}-\mathbf{e}'\in \mathrm{Im}(\mathbf{A})} f(\mathbf{e})\overline{f(\mathbf{e}')} \right| \\ &\leq q^n \sum_{\mathbf{e},\mathbf{e}':\ \mathbf{e}-\mathbf{e}'\in \mathrm{Im}(\mathbf{A})} |f(\mathbf{e})|\cdot|f(\mathbf{e}')| \quad \text{(by triangle inequality)} \\ &= q^n \sum_{\mathbf{e},\mathbf{e}':\ \mathbf{e}-\mathbf{e}'\in \mathrm{Im}(\mathbf{A})} |f|(\mathbf{e})\cdot|f|(\mathbf{e}'). \end{aligned}$$

It holds that

$$\mathbb{P}_{\mathbf{A}}\left(Z_{|f|}(\mathbf{A}) \geq (1+\delta)q^n\right) \ \leq\ \mathbb{P}_{\mathbf{A}}\left(Z_{|f|}(\mathbf{A}) \geq (1+\delta)q^n \mid \mathbf{A} \text{ full-rank }\right) + \mathbb{P}(\mathbf{A} \text{ not full-rank }).$$

The probability of $\mathbf{A}$ not being full-rank is at most q^{n+1-m} according to Lemma 15. From now on, we assume that $\mathbf{A}$ is full-rank.

Let S be defined as follows:

$$S \stackrel{\text{def}}{=} \sum_{\substack{\mathbf{e}\neq\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \ .$$

The random variable S has positive values, then by Markov's inequality, one obtains

$$\begin{aligned} \mathbb{P}_{\mathbf{A}}\left(Z_{|f|}(\mathbf{A}) \geq (1+\delta)q^n\right) &= \mathbb{P}_{\mathbf{A}}\left(S \geq \delta\right) \\ &\leq \frac{1}{\delta}\,\mathbb{E}_{\mathbf{A}}(S), \end{aligned}$$

for every $\delta > 0$. Using the linearity of the expectation function, one can compute the expectation in the right hand side as follows.

$$\begin{aligned} \mathbb{E}_{\mathbf{A}}(S) &= \mathbb{E}_{\mathbf{A}}\left(\sum_{\substack{\mathbf{e}\neq\mathbf{e}' \\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})}} |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \right) \\ &= \mathbb{E}_{\mathbf{A}}\left(\sum_{\mathbf{e}\neq\mathbf{e}'} \mathbb{1}_{\mathrm{Im}(\mathbf{A})}(\mathbf{e}-\mathbf{e}')\ |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \right) \\ &= \sum_{\mathbf{e}\neq\mathbf{e}'} \mathbb{P}_{\mathbf{A}}\left(\mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})\right)\ |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \\ &= \frac{1}{q^{m-n}} \sum_{\mathbf{e}\neq\mathbf{e}'} |f|(\mathbf{e})\cdot|f|(\mathbf{e}') \quad \text{(by Lemma 16)}. \end{aligned}$$

This completes the proof. □

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

Lemma 29. *Let $m \geq n \geq 2$ and q be positive integers, and α be a real number such that $0 < \alpha \leq \frac{1}{m\sqrt{\ln q}}$. Then we have:*

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

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

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

It suffices to bound the quadratic term. With Lemma 13, one can approximate $\vartheta_{\alpha q}$ using $D_{\mathbb{Z}^m, \alpha q}$. We obtain

$$\begin{aligned}
\sum_{\mathbf{e} \in [\![-\lceil \frac{q}{2} \rceil, \lfloor \frac{q}{2} \rfloor]\!]^m} \sqrt{\vartheta_{\alpha q}(\mathbf{e})} &\leq \sum_{\mathbf{e} \in [\![-\lceil \frac{q}{2} \rceil, \lfloor \frac{q}{2} \rfloor]\!]^m} \sqrt{D_{\mathbb{Z}^m, \alpha q}(\mathbf{x}) + e^{-1/(m\alpha^2)}} \quad \text{(by Lemma 13)} \\
&= \sum_{\mathbf{e} \in [\![-\lceil \frac{q}{2} \rceil, \lfloor \frac{q}{2} \rfloor]\!]^m} \frac{\rho_{\sqrt{2}\alpha q}(\mathbb{Z}^m)}{\sqrt{\rho_{\alpha q}(\mathbb{Z}^m)}} D_{\mathbb{Z}^m, \sqrt{2}\alpha q}(\mathbf{x}) + e^{-1/(m\alpha^2)} \\
&\leq \frac{\rho_{\sqrt{2}\alpha q}(\mathbb{Z}^m)}{\sqrt{\rho_{\alpha q}(\mathbb{Z}^m)}} + q^m e^{-1/(m\alpha^2)} \\
&\leq \frac{(1+\sqrt{2}\alpha q)^m}{(\sqrt{\alpha q})^m} + q^m e^{-1/(m\alpha^2)} \quad \text{(by Lemma 11)} \\
&\leq (2\sqrt{\alpha q})^m + q^m \; e^{-1/(m\alpha^2)}. \qquad (22)
\end{aligned}$$

Since $\alpha \leq \frac{1}{m\sqrt{\ln q}}$, we have $q^m \; e^{-1/(m\alpha^2)} \leq 1$. Furthermore, the same bound for α implies that $2\sqrt{\alpha q} \leq \sqrt{q}$, which completes the proof. □

We finally obtain the following theorem.

Theorem 6. *Let $m \geq n+1 \geq 3$ be integers, q be a prime integer, and α be a real number such that $0 < \alpha \leq \frac{1}{m\sqrt{\ln q}}$. Let $\mathbf{A}$ be sampled uniformly from $(\mathbb{Z}/q\mathbb{Z})^{m \times n}$, f be an amplitude function over $\mathbb{Z}/q\mathbb{Z}$ as per Corollary 2, and $Z_f(\mathbf{A})$ be defined as in Equation (20). Then we have*

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

Proof. It suffices to use Lemma 30 and 29 with $\delta = q^{-n}$. □

MLWE case. We first briefly explain the idea. Recall that Lemma **??** states that $Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))$ is equal to the norm of the following vector:

$$\sum_{\mathbf{s} \in (R/qR)^n} \sum_{\mathbf{e} \in (R/qR)^m} \bigotimes_{i=1}^{m} f^{\otimes d}(e_i) \left| \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \bmod q \right\rangle. \qquad (23)$$

Let R be the cyclotomic ring of integers with degree d. Let $|f| = \sqrt{\vartheta_{\alpha q}}$, and $\mathbf{A} = (I_{n \times n} \mid \overline{\mathbf{A}})^\top \in (R/qR)^{m \times n}$ where $\overline{\mathbf{A}}$ is sampled uniformly. We calculate the quantity $Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))$, by relating it to the norm of a shortest vector in $\Lambda_q(\mathbf{A})$, namely λ_1 of:

$$\Lambda_q(\mathbf{A}) = \mathbf{A}(R/qR)^n + qR^m.$$

Then one can use the regularity lemma [LPR13, Theorem 7.4] to obtain an approximation of λ_1 in the case of cyclotomic fields.

Lemma 30. *Let K be a number field with degree d, and R be its ring of integers. Let n, m, q be integers, $\mathbf{A} \in (R/qR)^{m \times n}$, f be an amplitude funtion, and $Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))$ be defined as above. If*

$$\sum_{\substack{\mathbf{e} \in (R/qR)^m \\ \|\mathbf{e}\| \geq \lambda_1/2}} |f|(\mathbf{e}) = \delta(n),$$

for some negligible function δ, then we have

$$Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})) \le q^{nd}\big(1 + 2\delta(n)\big).$$

Proof. The proof is similar as in Lemma 28, but we explain it for the sake of completeness. Let $\mathrm{Im}(\mathbf{A})$ be the image of $\mathbf{A}$ in $(R/qR)^m$. For every vector $\mathbf{e} \in (R/qR)^m$, let $|\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle$ denotes the following state:

$$|\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle \overset{\text{def}}{=} \sum_{\mathbf{x}\in(R/qR)^n} |\mathbf{A}\mathbf{x} + \mathbf{e}\rangle \,.$$

One can verify that for two vectors $\mathbf{e}, \mathbf{e}'$, we have

$$\langle \mathrm{Im}(\mathbf{A}) + \mathbf{e}' | \mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle = \begin{cases} q^{nd} & \text{if } \mathbf{e} - \mathbf{e}' \in \mathrm{Im}(\mathbf{A}), \\ 0 & \text{Otherwise.} \end{cases} \tag{24}$$

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

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

Therefore, we have

$$Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})) = \Big\| \sum_{\mathbf{e}\in(R/qR)^m} f(\mathbf{e})\, |\mathrm{Im}(\mathbf{A}) + \mathbf{e}\rangle \Big\|^2.$$

The above term is equal to:

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

where we used Equation (24).

On the other hand, we have the following inequalities.

$$\begin{aligned} Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})) = |Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))| &= \Big| q^{nd} \sum_{\mathbf{e},\mathbf{e}' :\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} f(\mathbf{e})\overline{f(\mathbf{e}')} \Big| \\ &\le q^{nd} \sum_{\mathbf{e},\mathbf{e}' :\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} |f(\mathbf{e})| \cdot |f(\mathbf{e}')| \quad \text{(by triangle inequality)} \\ &= q^{nd} \sum_{\mathbf{e},\mathbf{e}' :\ \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} |f|(\mathbf{e}) \cdot |f|(\mathbf{e}') \\ &= Z_{|f|}(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})). \end{aligned}$$

Therefore, it suffices to show that $Z_{|f|}(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})) \le q^{nd}\big(1 + \delta(n)\big)$. It holds that

$$\begin{aligned} \frac{Z_{|f|}(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))}{q^{nd}} &= \sum_{\mathbf{e},\mathbf{e}' : \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})} |f|(\mathbf{e}) \cdot |f|(\mathbf{e}') \\ &= \sum_{\mathbf{e}=\mathbf{e}'} |f|(\mathbf{e}) \cdot |f|(\mathbf{e}') + \sum_{\mathbf{e},\mathbf{e}' : \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})\setminus\{\mathbf{0}\}} |f|(\mathbf{e}) \cdot |f|(\mathbf{e}') \\ &= 1 + \sum_{\mathbf{e},\mathbf{e}' : \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})\setminus\{\mathbf{0}\}} |f|(\mathbf{e}) \cdot |f|(\mathbf{e}'). \end{aligned}$$

If $\mathbf{e} - \mathbf{e}' \in \mathrm{Im}(\mathbf{A}) \setminus \{\mathbf{0}\}$, then $\|\mathbf{e} + \mathbf{e}'\| \ge \lambda_1$ which means either $\|\mathbf{e}\| \ge \lambda_1/2$ or $\|\mathbf{e}'\| \ge \lambda_1/2$. Note that, for every $\mathbf{x} \in (R/qR)^m$, we have $|f|(\mathbf{x}) \le 1$. Therefore, we obtain

$$\sum_{\mathbf{e},\mathbf{e}' : \mathbf{e}-\mathbf{e}'\in\mathrm{Im}(\mathbf{A})\setminus\{\mathbf{0}\}} |f|(\mathbf{e}) \cdot |f|(\mathbf{e}') \le 2 \sum_{\|\mathbf{e}\|\ge\lambda_1/2} |f|(\mathbf{e}) = 2\delta(n).$$

□

One can see this lemma as an amplitude version of unique decoding because the concentration is treated with respect to the absolute value of amplitudes. In the following, we consider an almost uniform matrix $\mathbf{A}$ and the folded discrete Gaussian distribution.

Lemma 31. *Let K be a cyclotomic number field with degree d, and R be its ring of integers. Let $m \geq n$ and q be positive integers, and α be a real number. Let $\mathbf{A} = (I_{n\times n} \mid \overline{\mathbf{A}})^\top \in (R/qR)^{m\times n}$ be a matrix where $\overline{\mathbf{A}}$ is sampled uniformly, and λ_1 be the random variable that corresponds to the norm of a shortest non-zero vector of $\Lambda_q(\mathbf{A})$. If*

$$0 < \alpha \leq \min\left(\frac{1}{2\sqrt{2md}\; dq^{n/m+2/(md)}}, \frac{1}{md\sqrt{2\ln q}}\right),$$

then we have

$$\sum_{\substack{\mathbf{e}\in(R/qR)^m \\ \|\mathbf{e}\|\geq\lambda_1/2}} \sqrt{\vartheta_{\alpha q}(\mathbf{e})} = \mathsf{negl}(md).$$

Proof. We proceed by representing the elements of R/qR in $(\mathbb{Z}/q\mathbb{Z})^d$ with the coefficient embedding of the number field. We have

$$\begin{aligned}\sum_{\substack{\mathbf{e}\in[\![-\lceil\frac{q}{2}\rceil,\lfloor\frac{q}{2}\rfloor]\!]^{md} \\ \|\mathbf{e}\|\geq\lambda_1/2}} \sqrt{\vartheta_{\alpha q}(\mathbf{e})} &\leq \sum_{\substack{\mathbf{e}\in[\![-\lceil\frac{q}{2}\rceil,\lfloor\frac{q}{2}\rfloor]\!]^{m} \\ \|\mathbf{e}\|\geq\lambda_1/2}} \sqrt{D_{\mathbb{Z}^{md},\alpha q}(\mathbf{e})} + e^{-1/(md\alpha^2)} \quad \text{(by Lemma 13)} \\ &\leq \frac{1}{\sqrt{\rho_{\alpha q}(\mathbb{Z}^{md})}}\; \rho_{\sqrt{2}\alpha q}(\mathbb{Z}^{md}\setminus \mathrm{B}_{md}(\lambda_1)) + q^{md}e^{-1/(md\alpha^2)}, \qquad (25)\end{aligned}$$

where $\mathrm{B}_{md}(\lambda_1)$ is the ball with radius λ_1 in $\mathbb{R}^{md}$. Note that since $\alpha \leq \frac{1}{md\sqrt{2\ln q}}$, then we have $q^{md}e^{-1/(md\alpha^2)} = \mathsf{negl}(md)$. Furthermore, we have $\rho_{\alpha q}(\mathbb{Z}^{md}) \geq 1$. Hence, it suffices to show that the following term is negligible:

$$\rho_{\sqrt{2}\alpha q}(\mathbb{Z}^{md}\setminus \mathrm{B}_{md}(\lambda_1)).$$

According to [LPR13, Theorem 7.4], we have

$$\mathbb{E}_{\mathbf{A}}\left(\rho_{\frac{q}{s}}(\Lambda_q(\mathbf{A}))\right) = \mathbb{E}_{\mathbf{A}}\left(\rho_{1/s}(\frac{1}{q}\;\Lambda_q(\mathbf{A}))\right) \leq 1 + 2^{-\Omega(n)}$$

whenever $s > 2d\; q^{n/m+2/dm}$, and so by Markov's inequality we obtain

$$\rho_{\frac{q}{s}}\left(\Lambda_q(\mathbf{A})\right) \leq 1 + 2^{-\Omega(n)}$$

except with probability at most $2^{-\Omega(n)}$. It implies that $\lambda_1 \geq \frac{q}{s}\,\sqrt{md}$ except with probability at most $2^{-\Omega(n)}$. Therefore, when $\sqrt{2}\alpha q\,\sqrt{md} \leq \frac{q}{2d\;q^{n/m+2/(dm)}}$, it holds that

$$\rho_{\sqrt{2}\alpha q}\left(\mathbb{Z}^{md}\setminus \mathrm{B}_{md}(\lambda_1)\right) \;\leq\; \rho_{\sqrt{2}\alpha q}\left(\mathbb{Z}^{md}\setminus \mathrm{B}_{md}(\frac{q}{s}\sqrt{md}\;)\right) + 2^{-\Omega(n)} \;\leq\; \mathsf{negl}(md) + 2^{-\Omega(n)},$$

where we used Lemma 10. This completes the proof. □

The following theorem is a direct consequence of the lemmas above.

Theorem 7. *Let K be a cyclotomic number field with degree d, and R be its ring of integers. Let $m \geq n \geq 2$ and q be positive integers, and α be a real number. Let $\mathbf{A} = (I_{n\times n} \mid \overline{\mathbf{A}})^\top \in (R/qR)^{m\times n}$ be a matrix where $\overline{\mathbf{A}}$ is sampled uniformly, f be an amplitude function over $\mathbb{Z}/q\mathbb{Z}$ as per Corollary 2, and $Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))$ be defined as in Equation (23). If*

$$0 < \alpha \leq \min\left(\frac{1}{2\sqrt{2md}\; dq^{n/m+2/(md)}}, \frac{1}{md\sqrt{2\ln q}}\right),$$

then there exists a negligible function $\delta(n)$ such that

$$\mathbb{P}_{\mathbf{A}}\left(Z_f(\mathrm{T}_{\mathbb{Z}}(\mathbf{A})) \geq q^{nd}(1+\delta(n))\right) = \mathsf{negl}(n)$$

The above theorem also covers the LWE problem when the number field is $\mathbb{Q}$. It gives another variant of Theorem 6, when the modulus is not prime.

Corollary 3. *Let $m \geq n \geq 2$ and q be positive integers, and α be a real number. Let $\mathbf{A} = (I_{n\times n} \mid \overline{\mathbf{A}})^\top \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$ be a matrix where $\overline{\mathbf{A}}$ is sampled uniformly, f be an amplitude function over $\mathbb{Z}/q\mathbb{Z}$ as per Corollary 2, and $Z_f(\mathbf{A})$ be defined as in Equation (20). If*

$$0 < \alpha \leq \min\left(\frac{1}{2\sqrt{2m}\; q^{(n+2)/m}}, \frac{1}{m\sqrt{2\ln q}}\right),$$

then there exists a negligible function $\delta(n)$ such that

$$\mathbb{P}_{\mathbf{A}}\left(Z_f(\mathbf{A}) \geq q^n(1+\delta(n))\right) = \mathsf{negl}(n).$$

4.6. Concrete Witness-Oblivious Sampler for (M)LWE.

As mentioned earlier, in this subsection, we use all the results demonstrated above to obtain an explicit witness-oblivious LWE sampler. We note that all the ingredients in Subsections 4.3, 4.4, and 4.5 were necessary in order to obtain a regime of parameters that is practical in the context of cryptography.

Theorem 8. *Let $n \geq 2$ be an integer, $m = \gamma n$ be an integer for some constant γ, q be a prime number such that $\omega(n) \leq q \leq \mathsf{poly}(n)$, and α be a real number such that $\frac{2\sqrt{n}}{q} \leq \alpha \leq \frac{1}{m\sqrt{\ln q}}$.*

If $\gamma \geq 1 + \alpha q$, then under Assumption 1, there exists a witness-oblivious $\mathsf{LWE}_{q,\alpha}(\mathbf{A})$ sampler for all but negligible[7] fraction of matrices $\mathbf{A} \in (\mathbb{Z}/q\mathbb{Z})^{m\times n}$.

Proof. We show that Algorihtm 2 with the input $\mathbf{A}$ and the amplitude function f defined as per Corollary 2 is a witness-oblivious sampler.

Let $\{\mathbf{E}_i\}_{i\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ be the POVM as per Definition **??** with success probability p. Theorem 3 states that Algorithm 2 successfully outputs a quantum state $|\varphi\rangle$, such that

$$D_{\text{tr}}\left(|\varphi\rangle, |\mathsf{LWE}(\mathbf{A})\rangle_{q,f}\right) = \sqrt{1 - \frac{q^n}{Z_f(\mathbf{A})}\, p_{\mathcal{A}_{\text{GE}}}(\mathbf{A},p)^2}\ ,$$

where $p_{\mathcal{A}_{\text{GE}}}(\mathbf{A},p)^2$ is defined in Definition 23. If the success probability p of the POVM satisfies $mp = n(1+\Omega_n(1))$, and the matrix $\mathbf{A}$ is full-rank, then we have

$$p_{\mathcal{A}_{\text{GE}}}(\mathbf{A},p)^2 = 1 - q^{-\Omega(n)}.$$

We note that the matrix $\mathbf{A}$ is full-rank for all but negligible fraction of matrices. Furthermore, the quantity of p satisfies $mp = n(1+\Omega_n(1))$ due to Corollary 2 since we have chosen $\gamma \geq (1+\alpha q)$. Therefore, the above condition holds. On the other hand, Theorem 6 asserts that $Z_f(\mathbf{A})$ is not greater than $q^n + 1$ with overwhelming probability when $\alpha \leq \frac{1}{m\sqrt{\ln q}}$. By putting these two upper bounds together, we deduce that the trace distance is bounded by $\mathsf{negl}(n)$. We also note that the condition $\alpha q \geq 2\sqrt{n}$ is required for Assumption 1. Finally, it suffices to apply Theorem 1 to complete the proof. □

Note that This result shows that under the quantum hardness assumption of LWE, the quantum knowledge assumption of LWE, i.e.,Assumption 4, is false.

A similar result can be obtained for MLWE problem.

Theorem 9. *Let K be the cyclotomic number field with degree d, and R be the ring of integers. Let $n \geq 2$ and q be positive integers, $m = \gamma n$ be an integer for some constant γ, and α be a real number such that*

$$\frac{2\sqrt{d}\;\omega(\sqrt{\log n})}{q} \leq \alpha \leq \min\left(\frac{1}{2\sqrt{2md}\; dq^{n/m+2/(md)}}, \frac{1}{md\sqrt{2\ln q}}\right).$$

Let $\mathbf{A} = (I_{n\times n} \mid \overline{\mathbf{A}})^\top$ be a matrix in $(R/qR)^{m\times n}$.

If $\gamma \geq 1+\alpha q$, then under Assumption 2, there exists a witness-oblivious $\mathsf{LWE}_{q,\alpha}(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))$ sampler for all but negligible[8] fraction of matrices $\overline{\mathbf{A}} \in (R/qR)^{(m-n)\times n}$.

Proof. The proof is similar to that of Theorem 8. □

[7] with repsect to n

[8] with repsect to nd

4.7. **Other Variants of** (M)LWE. **[Pouria : We don't need modulus switching anymore, to obtain lwe with large modulus and large s.d., we only need to add some large noise.]** In Section **??**, we exhibited witness-oblivious quantum LWE and MLWE samplers (see Theorem 8, 9). However, the required conditions of our algorithm put some limitations on the parameters of the samplers. In particular, the standard deviation αq must be polynomially large in n. One might also be curious about the LWE regime of parameters where the modulus q and the standard deviation αq are exponentially large in n. By Assumption 1, as long as $\alpha q \geq 2\sqrt{n}$, the instance is hard for polynomial-time algorithms. The following theorem shows that our result extends to this regime of LWE parameters.

Theorem 10. *Let K be the cyclotomic number field with the power-of-two degree d, and R be the ring of integers. Let $n \geq 2$ be an integer, $m \geq 2n$ be an integer of order $\mathsf{poly}(n)$, q be an integer, and $\beta \in (d^{3/4} \frac{1}{\mathsf{poly}(n)}, 1)$*[9] *be a real number.*

Then under Assumption 2, there exists a witness-oblivious $\mathsf{LWE}_{q,\beta}(\mathrm{T}_{\mathbb{Z}}(\mathbf{A}))$ sampler for all but negligible[10] *fraction of matrices $A \in (R/qR)^{m\times n}$.*

Note that the parameters are less restricted compared to Theorem 8. In particular, the modulus is allowed to be any integer of any order.

The proof of this theorem requires the following lemma. The original version of this lemma is concerned about decision variant of MLWE and thus uses a particular distribution Υ_s. Since we need its search variant, we restrict the statement to the continuous Gaussian distribution $\Psi_{\leq s}$. One can verify that the proof is similar.

Lemma 32 (Adapted from [LS15, Theorem 4.8])**.** *Let K be the cyclotomic number field with the power-of-two degree d, and R be its ring of integers. Let $n \geq 2$ be an integer, m be an integer of order $\mathsf{poly}(n)$, $p, q \in [\![2, 2^{(nd)^{O(1)}}]\!]$ be integers, and $\alpha, \beta > 0$ be a real numbers such that*

$$\beta \geq \alpha \;\max(1, \frac{p}{q})\; d^{1/4}(nd)^{1/2}\;\omega(\log nd),\;\textit{and}\;\alpha p \geq \omega\left(\sqrt{\log nd/d}\right) \tag{26}$$

Then there exists a PPT reduction as follows:

$$\mathsf{MLWE}_{d,p,\Psi_{\leq \alpha p}}(\mathbf{B}) \leq \mathsf{MLWE}_{d,q,\Psi_{\leq \beta q}}(\mathbf{A})\,.$$

where the reduction maps uniform $\mathbf{B} \in (R/qR)^{(m+n)\times n}$ to $\mathbf{A} \in (R/qR)^{m\times n}$ that is within negligible[11] *statistical distance from uniform distribution over $(R/qR)^{m\times n}$. Moreover, the loss in the advantage is negligible in nd, too.*

Proof of Theorem 10. **[Pouria : TODO: We first add some continuous Gaussian to $\vartheta_{\alpha q}$ to becomes ind. from $\Psi_{s'}$. Then apply the lemma. Then round the result and show that the rounded distribution is within negligible statistical distance from $\vartheta_{\beta q}$.]**

Plugging in this reduction and Theorem 8 into Lemma 33 concludes the theorem. □

A variant of Theorem 10 is the following result for LWE.

Corollary 4. *Let $n \geq 2$ be an integer, $m \geq 2n$ be an integer of order $\mathsf{poly}(n)$, q be an integer, and $\beta \in (\frac{1}{\mathsf{poly}(n)}, 1)$*[12] *be a real number.*

Then under Assumption 1, there exists a witness-oblivious $\mathsf{LWE}_{q,\beta}(\mathbf{A})$ sampler for all but negligible[13] *fraction of matrices $A \in (R/qR)^{m\times n}$.*

Proof. The theorem follows by noting that $\mathbb{Q}$ is the cyclotomic field of degree 1. □

[9] **[Pouria : check the parameters again]**

[10] with repsect to nd

[11] with respect to nd

[12] **[Pouria : check the parameters again]**

[13] with repsect to n

5. Breaking the Security of Lattice-Based SNARKs

Succint Non-Interactive Arguments of Knowledges (SNARKs) are cryptographic schemes whose purpose is to prove some NP statement with a relatively short proof compared to the witness. Ideally, the proof size is poly-logarithmic in the size of the statement. The prover is always a PPT algorithm that could potentially cheat. The security property guarantees that the prover cannot cheat unless with a negligible probability. The formal syntax and properties are recalled in the Appendix B.

In a paper, Gentry and Wichs [GW11] showed that no SNARK can be proved to be secure under the black-box reductions using only *falsifiable assumptions*, which left the possibility for studying candidate constructions only based on non-falsifiable assumptions. In the recent years, there have been several constructions proposed for post-quantum security in the literature such as XXX most of which rely on lattices. Here, we are only interested in those that are based on lattice knowledge assumptions. In particular, we will discuss [GMNO18, ISW21, GNSV23, SSEK22, ACL$^+$22, CLM23].

TODO: Explain that surprisingly, although they claim post-quantum security, they only consider PPT adversaries against the knowledge assumptions such as linear-only or knowledge MISIS.

5.1. Linear-Only Vector Encryption.

For constructing SNARKs, the authors of [BCI$^+$13, ISW21, SSEK22] use secret-key vector encryption schemes that are *linear-only* homomorphic, the messages belong to an R/pR-module, and the ciphertexts belong to an R/qR-module for some $p < q$. Such schemes allow the players to compute R/pR-linear functions of the ciphertexts but not any function beyond those. In particular, the two papers [ISW21, SSEK22] use MLWE-based encryption with cyclotomic fields of power of two. We will show how their instantiation together with the linear-only property would translate to lattice knowlege assumptions.

Definition 24 (Vector Encryption over Cyclotomic Fields)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter, $\ell = \ell(\lambda), m = m(\lambda), q = q(\lambda)$ and $p = p(\lambda)$ be integers such that $p \ll q$, and $K = \mathbb{Q}[x]/\langle x^d + 1\rangle$ where $d = d(\lambda)$ is a power of two. Let R be the ring of integers of K. A secret-key linearly-homomorphic vector encryption with the message space $(R/pR)^\ell$ and the ciphertext space $(R/qR)^m$ is a tuple of algorithms $\Pi_{\mathsf{Enc}} = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Add})$ such that*

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

Moreover, Algorithm Add *satisfies the following property:*

- *Linearly homomorphism: TODO*

Encryption schemes might satisfy various properties such as correctness and security. Within the scope of this work, we are particulary interested in the linear-only 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 25 (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 $\lambda \in \mathbb{N}$, auxiliary mixed states ρ 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* $(\mathbf{v}_1, \cdots, \mathbf{v}_m) \leftarrow \mathcal{M}(1^\lambda, \mathsf{pp})$*. It computes the ciphertexts* $(\mathbf{ct}_1, \cdots, \mathbf{ct}_m) \leftarrow \mathsf{Enc}(\mathsf{sk}, \{\mathbf{v}_i\}_i)$*.*

(2) *Then it runs the extraction process with the outputs as follows:*

$$\big((\mathbf{ct}'_1, \cdots, \mathbf{ct}'_k), \mathbf{\Pi}\big) \leftarrow \langle \mathcal{A}, \mathcal{E}\rangle_{\mathsf{ext}}(1^\lambda, |\mathsf{pp}, \mathbf{ct}_1, \cdots, \mathbf{ct}_m\rangle \otimes \rho, |\mathsf{pp}, \mathbf{ct}_1, \cdots, \mathbf{ct}_m\rangle \otimes \rho).$$

Let $\mathbf{V}' = (\mathbf{v}_1 \mid \cdots \mid \mathbf{v}_m)\mathbf{\Pi}$*. The output of the experiment is* 1 *if there exists an* $1 \leq i \leq m$ *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*.*

TODO: discussion about the auxiliary input is null or a classical uniform string.

In Definition 27, the adversary is given a couple of ciphertexts $\mathbf{C} \overset{\text{def}}{=} (\mathbf{ct}_1, ..., \mathbf{ct}_m) \in (R/qR)^{\ell\times m}$ and is supposed to output k different small linear combinations of them, namely $\mathbf{C}\pi_1, \mathbf{C}\pi_2, \cdots, \mathbf{C}\pi_k$ where $\pi_i \in (R/pR)^m$ is the i-th column of $\mathbf{\Pi}$. It asks the extractor to find the exact value of the matrix $\mathbf{\Pi}$. We note that the vector $\mathbf{C}\pi_i$ has the same form as the *knapsack* form of MLWE.

The $\mathsf{knapsackLWE}$ problem was introduced in [MM11]. We recall its general module version.

Definition 26 ($\mathsf{knapsackMLWE}$ Problem)**.** *Let* n, m, q, d *be integers with* $m > n$*. Let* K *be a number field with degree* d *and* R *be its ring of integers. Let* $\mathbf{A}$ *be a matrix in* $(R/qR)^{(m-n)\times m}$*. Let* $\chi^{\otimes d}$ *be an element-wise i.i.d. distribution over* R/qR*. The search* $\mathsf{knapsackMLWE}_{d,q,\chi}(\mathbf{A})$ *problem with parameters asks to recover* $\mathbf{e}$ *from* $(\mathbf{A}, \mathbf{Ae})$*, where* $\mathbf{e} \leftarrow \chi^{\otimes m}$*.*

They also showed a reduction from LWE to $\mathsf{knapsackLWE}$ which can also be extended to the module setting as follows.

Lemma 33. *Let* n, m, q, d *be integers with* $m > n$*. Let* K *be a number field with degree* d *and* R *be its ring of integers. Let* $\mathbf{A}$ *be a matrix in* $(R/qR)^{m\times n}$*. Let* $\chi^{\otimes d}$ *be an element-wise i.i.d. distribution over* R/qR*. Then, there exists a classical polynomial-time reduction from* $\mathsf{MLWE}_{d,q,\chi}(\mathbf{A})$ *to* $\mathsf{knapsackMLWE}_{d,q,\chi}(\mathbf{A}^\perp)$ *where* $\mathbf{A}^\perp$ *is a basis for the left kernel of* $\mathbf{A}$*.*

Proof. We note that one can find a basis for the left kernel of $\mathbf{A}$, in $\mathsf{poly}(n, m, \log q)$ steps as in Lemma 17. By multiplying it with a unimodular matrix, the result would be a uniform matrix $\mathbf{A}^\perp$. Then by multiplying $\mathbf{A}^\perp$ with the MLWE instance $\mathbf{b} = \mathbf{As} + \mathbf{e}$, we obtain a valid $\mathsf{knapsackMLWE}$ instance. □

As a consequnce of Lemma 33, if we use the witness-oblivious $\mathsf{MLWE}_{d,q,\chi}(\mathbf{A})$ sampler in Theorem **??**, we obtain a witness-oblivious $\mathsf{knapsackMLWE}_{d,q,\chi}(\mathbf{A}^\perp)$ sampler.

In the following theorem, we show that how obliviously sampling a $\mathsf{knapsackMLWE}$ instace would break the linear-only property.

Theorem 11. *If* Π_{Enc} *is a secret-key linearly-homomorphic vector encryption scheme with the ciphertext space* $(R/qR)^\ell$ *where* q *is* $\mathsf{poly}(\ell)$*, and that its ciphertexts are indistinguishable from random elements of the ciphertext space, then* Π_{Enc} *is not linear-only against quantum adversaries.*

Proof. Let $\mathbf{C} = (\mathbf{ct}_1 \mid ... \mid \mathbf{ct}_m) \in (R/qR)^{\ell\times m}$. We build a witness-oblivious $\mathsf{knapsackMLWE}_{d,q,\chi}(\mathbf{C})$ sampler where χ is a distribution over $[\![-\lceil \frac{p}{2}\rceil, \lfloor \frac{p}{2}\rfloor]\!]$ which will be determined later. Let $\mathbf{Ce}$ be its instance. Then we have

$$e_1\mathbf{ct}_1 + \cdots + e_m\mathbf{ct}_m = \mathsf{Enc}(\mathsf{sk}, e_1\mathbf{v}_1 + \cdots + e_m\mathbf{v}_m) = \mathsf{Enc}(\mathsf{sk}, \mathbf{Ve}),$$

where $\mathbf{V} = (\mathbf{v}_1 \mid \cdots \mid \mathbf{v}_m)$. Therefore, since $\mathbf{Ce}$ is sampled obliviously, extracting $\mathbf{e}$ out of $\mathbf{Ve}$, even by knowing the secret key sk, is not possible for all QPT extractors unless with negligible probability. This contradicts Condition 2 of Definition 27 which completes the theorem.

To obliviously sample an $\mathsf{knapsackMLWE}_{d,q,\chi}(\mathbf{C})$ instance, we proceed as follows. The matrix $\mathbf{C}$ is computationally indistinguishable from a uniformly chosen matrix. Therefore, its right kernel has rank $m - \ell$ with probability $1 - \mathsf{negl}(\ell)$ since otherwise, by using the algorithm in Lemma 17, one can distinguish $\mathbf{C}$ from the uniform matrix in polynomial-time. Let $\mathbf{D} \in (R/qR)^{m\times(m-\ell)}$ be a generator set for the right kernel of $\mathbf{C}$ as in Lemma 17. Let α be a positive real number such that

$$\frac{2\sqrt{d}\;\omega(\sqrt{\log n})}{q} \leq \alpha < \min\left(\frac{p}{q}, \frac{1}{2\sqrt{2d}\;q^{n/m+2/md}}, \frac{1}{md\sqrt{2\ln q}}\right).$$

Such an alpha exists due to the constraints of the parameters. Let $M \gg (m-\ell)(1+\alpha q)$ be an integer, and $\mathbf{A} = (\mathbf{I} \mid \mathbf{DU}) \in (R/qR)^{M\times(m-\ell)}$ where $\mathbf{U} \in (R/qR)^{(m-\ell)\times(m-\ell)}$ is a uniform unimodular matrix. According to Theorem 9, one can obliviously sample an $\mathsf{MLWE}_{d,q,\alpha}(\mathbf{A})$ instance $(\mathbf{A}, \mathbf{As}+\mathbf{e}')$. We then throw out the first $M-m$ rows of $(\mathbf{A}, \mathbf{As}+\mathbf{e}')$ to obtain $(\mathbf{DU}, \mathbf{DU}+\mathbf{e})$. We note that the new instance remains oblivious according to Lemma 33. Finally, by multiplying the instance with $\mathbf{C}$ on the left, we obtain

$$\mathbf{C}(\mathbf{DU}+\mathbf{e}) = \mathbf{Ce}.$$

This is an $\mathsf{knapsackMLWE}_{d,q,\alpha}(\mathbf{C})$ instance which is oblivious according to Lemma 33. We note that the distribution of the noise is ϑ_α which has its support in $[\![-\lceil \frac{p}{2}\rceil, \lfloor \frac{p}{2}\rfloor]\!]$. This completes the proof.

□

5.2. **Knowledge k-M-ISIS and vSIS Assumptions.** In [ACL⁺22], the authors propose the knowledge k-M-ISIS assumption (Definition 26 in the paper) and analyze some aspects of it. We note that the authors of [ACL⁺22] only consider PPT adversaries. Here, we adapt their definition to the quantum setting.

Definition 27 (Knowledge k-M-ISIS Assumption Against Quantum Adversaries)**.** *Let λ be the security parameter, $\ell = \ell(\lambda), \eta = \eta(\lambda), q = q(\lambda)$ be integers, and $\alpha^*, \beta^*, \gamma^* \geq 1$ be real numbers. Let $K = \mathbb{Q}[x]/\langle x^d+1\rangle$ where $d = d(\lambda)$ is a power of two, and R be its ring of integers.*

Let $\mathbf{x} \overset{def}{=} (x_1, \cdots, x_w)$, and $\mathcal{G} \subset R[\mathbf{x}]$ be a set of Laurent monomials whose size is k. Let $\mathcal{T} \in (R/qR)^\eta$ be such that, for any $\mathbf{t} = (t_1, \cdots, t_\eta) \in \mathcal{T}$, it holds that

$$\langle t_1, \cdots, t_\eta\rangle = R/qR, \text{ and } \frac{|\langle \mathbf{t}\rangle|}{|(R/qR)^\eta|} = \mathsf{negl}(\lambda).$$

For any $g \in \mathcal{G}$, $\mathbf{A} \in (R/qR)^{\eta\times\ell}$, $\mathbf{t} \in \mathcal{T}$, and $\mathbf{v} \in ((R/qR)^\times)^w$, we let the set of short vectors $D_{g,\mathbf{A},\mathbf{t},\mathbf{v}}$ be defined as follows:

$$\{\mathbf{u}_g \in R^\ell \mid \mathbf{A}\mathbf{u}_g = g(\mathbf{v})\mathbf{t} \bmod q \wedge \|\mathbf{u}_g\| \leq \gamma^*\}.$$

The knowledge k-M-ISIS assumption states that for all QPT algorithms $\mathcal{A}$, there exists a valid QPT extractor $\mathcal{E}$ such that for all security parameters $\lambda \in \mathbb{N}$, it holds that

$$\mathbb{P}\left(\mathsf{ExptKnowledgeExt}_{\mathsf{pp}m\mathcal{A},\mathcal{E}}(1^\lambda) = 1\right) = \mathsf{negl}(\lambda),$$

where the experiment $\mathsf{ExptKnowledgeExt}_{\mathsf{pp}m\mathcal{A},\mathcal{E}}(1^\lambda)$ is defined as follows:

(1) The challenger samples matrix $\mathbf{A} \in (R/qR)^{\eta\times\ell}$, $\mathbf{t} \in \mathcal{T}$, and $\mathbf{v} \in ((R/qR)^\times)^w$, uniformly. For every Laurent polynomial $g \in \mathcal{G}$, it samples a short vector $\mathbf{u}_g$ uniformly from $D_{g,\mathbf{A},\mathbf{t},\mathbf{v}}$.

(2) Then it runs the extraction process with the outputs as follows:

$$\left((c, \mathbf{u}), \{x_g\}_{g\in\mathcal{G}}\right) \leftarrow \langle \mathcal{A}, \mathcal{E}\rangle_{\mathsf{ext}}\left(1^\lambda, |\mathsf{pp}, \mathbf{A}, \mathbf{t}, \mathbf{v}, \{\mathbf{u}_g\}_{g\in\mathcal{G}}\rangle, |\mathsf{pp}, \mathbf{A}, \mathbf{t}, \mathbf{v}, \{\mathbf{u}_g\}_{g\in\mathcal{G}}\rangle\right).$$

The output of the experiment is 1 if

$$\mathbf{Au} = c\mathbf{t} \bmod q, \text{ and } 0 < \|\mathbf{u}\| \leq \beta^*,$$

and c is not a short linear combination of $\{g(\mathbf{v})\}_{g\in\mathcal{G}}$ as follows:

$$c = \sum_{g\in\mathcal{G}} x_g g(\mathbf{v}), \text{ and } \|\mathbf{x}_\mathcal{G}\| \leq \alpha^*,$$

where $\mathbf{x}_\mathcal{G}$ is a vector whose elements are x_g's. Otherwise, the output of the experiment is 0.

We have the following result.

Theorem 12. *Let $\mathbf{U} \in (R/qR)^{\ell \times k}$ denote the vertical concatenation of $(\mathbf{u}_g)_{g \in \mathcal{G}}$'s, and $\alpha = \alpha^*/\sqrt{k}$. Then Assumption 29 does not hold if $\mathsf{knapsackMLWE}_{d,q,\alpha}(\mathbf{U})$ is hard for all QPT adveraries.*

Proof. We show how to obliviously sample an $\mathsf{knapsackMLWE}_{d,q,\alpha}(\mathbf{U})$ instance $\mathbf{Ue}$. This completes the proof since $\|\mathbf{e}\| \leq \alpha^*$ □

5.3. **Encoding Schemes.** The *encoding schemes* were first introduced by [GGPR13] in order to build group-based SNARKs. Later, the authors of [GMNO18, **?**] applied the same framework using lattice-based encoding schemes for constructing post-quantum secure SNARKs. We recall the definition of encoding schemes. We only keep the relevent parameters and properties of the scheme.

Definition 28 (Encoding Schemes)**.** *Let $\lambda \in \mathbb{N}$ be the security parameter, $d = d(\lambda), p = p(\lambda), q = (\lambda)$ be an integers. A d-linearly-homomorphic encoding scheme with the message space $\mathbb{Z}/p\mathbb{Z}$ and the codeword space $C \subseteq \mathbb{Z}/q\mathbb{Z}$ is a tuple of algorithms $\Pi_{\mathsf{Encod}} = (\mathsf{Gen}, \mathsf{Encod}, \mathsf{Eval})$ such that*

- $\mathsf{Gen}(1^\lambda) \to (\mathsf{pp}, \mathsf{sk})$*: Given the security parameter λ, it outputs the public parameters* pp *and the secret key* sk.
- $\mathsf{Encod}(sk, a) \to \mathsf{cw}$*: Given the secret key* sk *and a field element $a \in \mathbb{F}$, it outputs a codeword* $\mathsf{cw} \in C$ *with the following property: the subsets $\{C_a \mid a \in \mathbb{F}\}$ partition C where C_a is the set of all possible encodings of a.*
- $\mathsf{Eval}(\mathsf{pp}, \{\mathsf{cw}_1, \cdots, \mathsf{cw}_d\}, \{c_1, \cdots, c_d\}) \to \mathsf{cw}^*$*: Given the public parameters* pp*, d codewords $\{\mathsf{cw}_1, \cdots, \mathsf{cw}_d\}$, and d scalars $\{c_1, \cdots, c_d\}$, it outputs a codeword cw^*.*

Moreover, Algorithm Eval *satisfies the following property:*

- *d-Linearly homomorphism: TODO*

In the real instantiation of the scheme the message space must be a finite field which requires p to be prime. But we note that this is irrelevent to the approach that we are taking here.

The d-power knowledge of exponent assumption (d-PKE) is the generalization of the knowledge of exponent assumption by [Dam92] to the encoding schemes. We adapt this assumption into the quantum setting.

Definition 29 (d-PKE Against Quantum Adversaries)**.** *An encoding scheme $\Pi_{\mathsf{Encod}} = (\mathsf{Gen}, \mathsf{Encod}, \mathsf{Eval})$ satisfies d-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 for all security parameters $\lambda \in \mathbb{N}$, it holds that*

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

where the experiment $\mathsf{ExptLinearExt}_{\Pi_{\mathsf{Encod}},\mathcal{A},\mathcal{Z},\mathcal{E},d}(1^\lambda)$ 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 uniform $\alpha, s \leftarrow \mathbb{F}^\times$. It computes σ as follows:*

$$\sigma \leftarrow \left(\mathsf{pk}, \mathsf{Encod}(1), \mathsf{Encod}(s), \cdots, \mathsf{Encod}(s^d), \mathsf{Encod}(\alpha), \mathsf{Encod}(\alpha s), \cdots, \mathsf{Encod}(\alpha s^d)\right).$$

It also computs $z \leftarrow Z(\sigma)$.

(2) *Then it runs the extraction process with the outputs as follows:*

$$\left((\mathsf{cw}, \mathsf{cw}'), (a_0, \cdots, a_d)\right) \leftarrow \langle \mathcal{A}, \mathcal{E} \rangle_{\mathsf{ext}}(1^\lambda, |\sigma, z\rangle, |\sigma, z\rangle).$$

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

TODO: a discussion about $\mathcal{Z}$ that is either null or a uniform string.

The following theorem shows how to break d-PKE assumption for all encoding schemes.

Theorem 13. *If Π_{Encod} is a d-linearly-homomorphic encoding scheme that its codewords are indistinguishable from random elements of the codeword space, then d-PKE assumption does not hold relative to Π_{Encod}.*

Proof. Let $\mathbf{C} \in (\mathbb{Z}/q\mathbb{Z})^{1\times d}$ b a matrix as follows:

$$\mathbf{C} \overset{\text{def}}{=} (\mathsf{Encod}(1) \mid \mathsf{Encod}(s) \mid \cdots \mid \mathsf{Encod}(s^d)).$$

If one can build a witness-oblivious $\mathsf{knapsackMLWE}_{d,q,\chi}(\mathbf{C})$ sampler for some arbitrary distribution χ, the d-PKE does not hold for this scheme. The rest of the proof is exactly similar to that of Theorem 11. □

[Pouria : I think we should also thank Omar and Alex Grilo (he mentioned that the extraction condition can be replaced by computational indistinguishability)]

Acknowledgments.

The authors are grateful to André Chailloux and Jean-Pierre Tillich for many insightful discussions. 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) and the ANR JCJC COLA grant (ANR-21-CE39-0011).

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.

[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, Omer Paneth, and Rafail Ostrovsky. Succinct non-interactive arguments via linear interactive proofs. In Amit Sahai, editor, *Theory of Cryptography*, pages 315–333, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

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

[BISW18] Dan Boneh, Yuval Ishai, Amit Sahai, and David J. Wu. Quasi-optimal SNARGs via linear multi-prover interactive proofs. In *EUROCRYPT*, 2018.

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

[BV97] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26(5):1411–1473, 1997.

[CB98] Anthony Chefles and Stephen M. Barnett. Optimum unambiguous discrimination between linearly independent symmetric states. *Physics Letters A*, 250(4-6):223–229, Dec 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. *Journal of Communications and Networks*, 2023.

[CLM23] Valerio Cini, Russell W. F. Lai, and Giulio Malavolta. Lattice-based succinct arguments from vanishing polynomials. In *CRYPTO*, 2023.

[CLZ21] Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering, 2021. arXiv:2108.11015.

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

[Dam92] Ivan Damgård. Towards practical public key systems secure against chosen ciphertext attacks. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 445–456, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.

[DRT21] Thomas Debris-Alazard, Maxime Remaud, and Jean-Pierre Tillich. Quantum reduction of finding short code vectors to the decoding problem. *IACR Cryptol. ePrint Arch.*, 2021.

[dW23] Ronald de Wolf. Quantum computing: Lecture notes, 2023.

[GGPR13] Rosario Gennaro, Craig Gentry, Bryan Parno, and Mariana Raykova. Quadratic span programs and succinct nizks without pcps. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 626–645, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[GKPV10] Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, and Vinod Vaikuntanathan. Robustness of the learning with errors assumption. In Andrew Chi-Chih Yao, editor, *Innovations in Computer Science - ICS 2010, Tsinghua University, Beijing, China, January 5-7, 2010. Proceedings*, pages 230–240. Tsinghua University Press, 2010.

[GMF21] Naixu Guo, Kosuke Mitarai, and Keisuke Fujii. Nonlinear transformation of complex amplitudes via quantum singular value transformation, 2021.

[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.

[GSLW19] András Gilyén, Yuan Su, Guang Hao Low, and Nathan Wiebe. Quantum singular value transformation and beyond: Exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, STOC 2019, page 193–204, New York, NY, USA, 2019. Association for Computing Machinery.

[GW11] Craig Gentry and Daniel Wichs. Separating succinct non-interactive arguments from all falsifiable assumptions. In *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing*, STOC '11, page 99–108, New York, NY, USA, 2011. Association for Computing Machinery.

[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 Henri Gilbert, editor, *Advances in Cryptology – EUROCRYPT 2010*, pages 1–23, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[LPR13] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. A toolkit for ring-lwe cryptography. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology – EUROCRYPT 2013*, pages 35–54, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

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

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

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

[Nie99] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83:436–439, Jul 1999.

[NS13] J. Neukirch and N. Schappacher. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2013.

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

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

[RR23] Arthur G. Rattew and Patrick Rebentrost. Non-Linear Transformations of Quantum Amplitudes: Exponential Improvement, Generalization, and Applications. *arXiv e-prints*, page arXiv:2309.09839, September 2023.

[SSEK22] Ron Steinfeld, Amin Sakzad, Muhammed F. Esgin, and Veronika Kuchta. Private re-randomization for module LWE and applications to quasi-optimal ZK-SNARKs. Cryptology ePrint Archive, Paper 2022/1690, 2022. 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.

[vAG18] Joran van Apeldoorn and András Gilyén. Improvements in quantum sdp-solving with applications. In *International Colloquium on Automata, Languages and Programming*, 2018.

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

Appendix A. Deffered Material

We provide deffered material of the main body of the paper in this section.

A.1. **Additional Material for Section 3.** We explain the proof of Lemma 19.

The class of operations over bipartite states known as *Local Operations and Classical Communications (LOCC) paradigm* is defined as follows. We refer to [Wat18, Section 6] for more details.

Definition 30. *Let $|\psi\rangle$ be a pure bipartite state over the Hilbert space $\mathcal{A} \otimes \mathcal{B}$ such that Alice owns the $\mathcal{A}$ part and Bob owns the other. We say that a quantum computation over the bipartite state $|\psi\rangle$ is LOCC if it can be performed by repeating the following ordered steps:*

(1) Alice applies local operations over $\mathcal{A}$;
(2) Alice communicates classical information to Bob;
(3) Bob applies local operations over $\mathcal{B}$;
(4) Bob communicates classical information to Alice.

One can decompose joint quantum states into product states as follows.

Definition 31 (Schmidt Decomposition)**.** *Let $\mathcal{A}$ and $\mathcal{B}$ be two Hilbert spaces of dimensions n and m, respectively, such that $m \geq n$. Then for every pure state $|\psi\rangle$ in $\mathcal{A} \otimes \mathcal{B}$, there exist orthonormal bases $\{|\alpha_i\rangle\}_{1\leq i\leq n}$ and $\{|\beta_j\rangle\}_{1\leq j\leq m}$ for $\mathcal{A}$ and $\mathcal{B}$, and unique (up to ordering) non-negative real numbers $\{\lambda_j\}_{1\leq j\leq m}$ such that*

$$|\psi\rangle = \sum_{j=1}^{m} \lambda_j |\alpha_j\rangle |\beta_j\rangle .$$

Moreover, the seqeuence $(\lambda_j)_j$, when ordered decreasingly, is said to be the Schdmidt coefficients of $|\psi\rangle$.

The following lemma categorizes LOCC operations.

Lemma 34 (Nielsen's Theorem, [Nie99])**.** *Let $|\psi\rangle$ and $|\varphi\rangle$ be pure states in a product Hilbert space $\mathcal{A} \otimes \mathcal{B}$. Assume that Alice owns the $\mathcal{A}$ part of $|\psi\rangle$ and Bob owns the $\mathcal{B}$ part. Let $\lambda = (\lambda_i)_i$ and $\mu = (\mu_i)_i$ be the Schmidt decomposition of $|\psi\rangle$ and $|\varphi\rangle$, respectively. Then, Alice and Bob can transform $|\psi\rangle$ to $|\varphi\rangle$ within LOCC paradigm if and only if, for every index n, we have*

$$\sum_{i=0}^{n} \lambda_i \leq \sum_{i=0}^{n} \mu_i .$$

Proof of Lemma 19. We first show that $\mathcal{E}$ only performs local operations on E during the course of $\mathcal{S}$'s execution. Without loss of generality, one can assume that $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$, as in Definition 16, is a pure state since one can always purify it with extra registers and obtain a new extractor that is pure. Fix i and j, and consider the Schmidt decomposition of $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ as follows:

$$\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j) = \left(\sum_{s\in\mathcal{J}} \lambda_s |\alpha_s\rangle_{\mathsf{Q}} |\beta_s\rangle_{\mathsf{E}}\right)\left(\sum_{s'\in\mathcal{J}} \overline{\lambda_{s'}} \langle\alpha_{s'}|_{\mathsf{Q}} \langle\beta_{s'}|_{\mathsf{E}}\right),$$

where the $|\alpha_s\rangle$'s and $|\beta_s\rangle$'s are orthonormal states. We trace out register E:

$$\begin{aligned}
\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)) &= \mathrm{tr}_{\mathsf{E}}\left(\sum_{s\in\mathcal{J}} \lambda_s |\alpha_s\rangle_{\mathsf{Q}} |\beta_s\rangle_{\mathsf{E}} \sum_{s'\in\mathcal{J}} \overline{\lambda'_s} \langle\alpha'_s|_{\mathsf{Q}} \langle\beta'_s|_{\mathsf{E}}\right) \\
&= \sum_{s,s'\in\mathcal{J}} \lambda_s\overline{\lambda_{s'}}\, \mathrm{tr}_{\mathsf{E}}\left(|\alpha_s\rangle\langle\alpha_{s'}|_{\mathsf{Q}} \otimes |\beta_s\rangle\langle\beta_{s'}|_{\mathsf{E}}\right) \\
&= \sum_{s,s'\in\mathcal{J}} \lambda_s\overline{\lambda_{s'}} \langle\beta_s|\beta_{s'}\rangle_{\mathsf{E}}\; |\alpha_s\rangle\langle\alpha_{s'}|_{\mathsf{Q}} \\
&= \sum_{s\in\mathcal{J}} |\lambda_s|^2 |\alpha_s\rangle\langle\alpha_s|_{\mathsf{Q}} ,
\end{aligned}$$

where in the last equality we used that the quantum states $|\beta_s\rangle_{\mathsf{E}}$'s, which are involved in the Schmidt decomposition, are orthonormal.

Notice now that $\mathcal{E}$ is a valid extractor, therefore according to Definition 16, we have

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

The state $\rho_{\mathsf{Q}}(i)$ is pure since $\mathcal{S}$ only applies unitaries to Q. Therefore, according to the above equality, the remaining state after tracing out must be a pure state, i.e., $|\mathcal{J}| = 1$. It implies that $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$ has Schmidt number one and is therefore separable.

The statement above holds for every $1 \leq i \leq \ell$ and every $0 \leq j \leq k(i)$ (k is defined in Definitin 16), and thus the bipartite states $\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)$'s are all separable. Therefore, their Schmidt coefficients are of the form $(1,0,0,\cdots)$. By applying Lemma 36 to these states, one obtains that the operations by $\mathcal{S}$ and $\mathcal{E}$ over $\mathsf{Q}\otimes\mathsf{E}$ must be either local (either an operation only over Q or an operation only over E) or in the form of classical communication between the two. Note that $\mathcal{S}$ always performs locally over Q. Suppose that $\mathcal{E}$ has applied a non-local operation in the form of a classical communication. Since $\mathcal{S}$ is unitary and does not perform a measurement during the execution, then $\mathcal{E}$ must have performed the measurement by itself to obtain the classical information. On the other hand, this measurement does not change the state of Q based on the constraint $\mathrm{tr}_{\mathsf{E}}(\rho_{\mathsf{Q}\otimes\mathsf{E}}(i,j)) = \rho_{\mathsf{Q}}(i)$. Hence, this register must have contained only classical information with respect to the measurement. Recall that the description of Q is also given to $\mathcal{E}$ beforehand. This means that $\mathcal{E}$ could obtain this classical information by simulating the execution of $\mathcal{S}$ locally by itself. This completes the lemma. □

A.2. **Additional Material for Section 4.2.** In this subsection we prove Lemmas 23 and 24 stated in Section 4.2.

Lemma 23. *Using the notations above, we have*

$$\forall i \in \mathbb{Z}/q\mathbb{Z}, \quad \mathbf{V}\,|\psi_i\rangle\,|0\rangle = \sqrt{p}\,|\varphi_i\rangle\,|i\rangle + \sqrt{1-p}\,|\varphi_{i,\perp}\rangle\,|\perp\rangle\,,$$

for some quantum states $\{|\varphi_i\rangle\,, |\varphi_{i,\perp}\rangle\}_{i\in\mathbb{Z}/q\mathbb{Z}}$.

Proof. Recall that $\{\mathbf{E}_j\}_{j\in(\mathbb{Z}/q\mathbb{Z})\cup\{\perp\}}$ is a POVM. In particular, we have

$$\mathbf{E}_\perp + \sum_{j\in\mathbb{Z}/q\mathbb{Z}} \mathbf{E}_j = \mathbf{Id}.$$

Furthermore, this measurement unambiguously distinguishes coordinate states: it satisfies Equations (**??**) and (**??**). Therefore, we have $\mathbf{E}_j\,|\psi_i\rangle = \mathbf{0}$ when $i \neq j$ and (independently of j),

$$p = \langle\psi_j|\,\mathbf{E}_j\,|\psi_j\rangle = \frac{1}{\lambda_+}\left|\langle\psi_j|\psi_j^\perp\rangle\right|^2. \tag{27}$$

By definition, we also have

$$\forall j \in \mathbb{Z}/q\mathbb{Z}, \quad \sqrt{\mathbf{E}_j} = \frac{1}{\sqrt{\lambda_+}}\;|\psi_j^\perp\rangle\langle\psi_j^\perp|\,.$$

We deduce that

$$\begin{aligned}\mathbf{V}\,|\psi_i\rangle\,|0\rangle &= \frac{1}{\sqrt{\lambda_+}}\,\langle\psi_i^\perp|\psi_i\rangle\,|\psi_i^\perp\rangle\,|i\rangle + \frac{1}{\sqrt{\lambda_+}}\sqrt{\mathbf{E}_\perp}\,|\psi_i\rangle\,|\perp\rangle \\ &= \sqrt{p}\;\underbrace{e^{ia}\,|\psi_i^\perp\rangle}_{|\varphi_i\rangle}|i\rangle + \sqrt{1-p}\;\underbrace{e^{ib}\sqrt{\mathbf{E}_\perp}\,|\psi_i\rangle}_{|\varphi_{i,\perp}\rangle}|\perp\rangle\end{aligned}$$

for some $a, b \in \mathbb{R}$. In the last equality, we used Equation (27). □

Lemma 24. *Using the notations of Theorem 3, we have*

$$D_{\mathrm{tr}}\left(|\psi\rangle\,, |\psi_{\mathrm{ideal}}\rangle\right) \leq \sqrt{1 - \frac{q^n}{Z_f(\mathbf{A})}\;p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A}, p)^2}.$$

Proof. First notice that according to Lemma 23, it holds that

$$\begin{aligned}\bigotimes_{i=1}^{m} \mathbf{V}\left|\psi_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|0\rangle &= \bigotimes_{i=1}^{m}\left(\sqrt{p}\left|\varphi_{\langle \mathbf{a}_i,\mathbf{s}\rangle}\right\rangle|\langle \mathbf{a}_i,\mathbf{s}\rangle\rangle + \sqrt{1-p}\left|\varphi_{\langle \mathbf{a}_i,\mathbf{s}\rangle,\perp}\right\rangle|\perp\rangle\right)\\ &= \sum_{\mathbf{y}\in(\{\langle \mathbf{a}_j,\mathbf{s}\rangle,\ \perp\})_{j=1}^{m}} \bigotimes_{i=1}^{m} \lambda(y_i)\left|\varphi_{h(y_i)}\right\rangle|y_i\rangle\end{aligned}$$

where,

$$\lambda(y_i) \overset{\text{def}}{=} \begin{cases}\sqrt{p} & \text{if } y_i = \langle \mathbf{a}_i,\mathbf{s}\rangle,\\ \sqrt{1-p} & \text{otherwise.}\end{cases} \quad \text{and} \quad h_{\mathbf{s}}(y_i) \overset{\text{def}}{=} \begin{cases}\langle \mathbf{a}_i,\mathbf{s}\rangle & \text{if } y_i = \langle \mathbf{a}_i,\mathbf{s}\rangle,\\ \langle \mathbf{a}_i,\mathbf{s}\rangle,\perp & \text{otherwise.}\end{cases} \tag{28}$$

Therefore, using Equations (15) and (16), we obtain

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

and

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

We have:

$$\begin{aligned}\langle\psi_{\text{ideal}}|\psi\rangle = \frac{1}{\sqrt{q^n\ Z_f(\mathbf{A})}} &\sum_{\mathbf{s},\mathbf{s}'\in(\mathbb{Z}/q\mathbb{Z})^n}\ \sum_{\mathbf{y}\in(\{\langle \mathbf{a}_j,\mathbf{s}\rangle,\ \perp\})_{j=1}^{m}}\ \sum_{\mathbf{y}'\in(\{\langle \mathbf{a}_j,\mathbf{s}'\rangle,\ \perp\})_{j=1}^{m}}\\ &\underbrace{\langle \mathbf{0}|\mathbf{s}'-\mathcal{A}_{\mathrm{GE}}(\mathbf{A},\mathbf{y}')\rangle \prod_{i=1}^{m} \lambda(y_i)\lambda(y_i')\left\langle\varphi_{h_{\mathbf{s}}(y_i)}\middle|\varphi_{h_{\mathbf{s}}(y_i')}\right\rangle\langle y_i|y_i'\rangle\,.}_{P}\end{aligned} \tag{29}$$

Our aim is to show that P is always equal to 0 except when $\mathbf{s}=\mathbf{s}'$ and $\mathbf{y}=\mathbf{y}'$. First, notice that

$$\langle y_i|y_i'\rangle = \begin{cases}1 & \text{if } y_i = y_i',\\ 0 & \text{otherwise.}\end{cases}$$

We deduce that $\mathbf{y}=\mathbf{y}'$, otherwise $P=0$. Furthermore, the quantity P will be non-zero if also the following holds

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

But recall that $\mathcal{A}_{\mathrm{GE}}$ is a unambiguous Gaussian elimination (see Definition 23): with the knowledge of the $y_i' = \langle \mathbf{a}_i,\mathbf{s}'\rangle \neq \perp$, it uniquely determines $\mathbf{s}'$. Therefore, as $\mathbf{y}=\mathbf{y}'$, we necessarily have $\mathbf{s}=\mathbf{s}'$. It implies that $h_{\mathbf{s}}(y_i) = h_{\mathbf{s}}(y_i')$ (see Equation (28)), even when $y_i = \perp$. Therefore, we have

$$\left\langle\varphi_{h_{\mathbf{s}}(y_i)}\middle|\varphi_{h_{\mathbf{s}}(y_i')}\right\rangle = 1.$$

We finally deduce that P in Equation (29) is necessarily equal to 0 except when $\mathbf{s}=\mathbf{s}'$ and $\mathbf{y}=\mathbf{y}'$. Therefore, we obtain

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

where $p_{\mathcal{A}_{\mathrm{GE}}}(\mathbf{A})$ is the success probability of $\mathcal{A}_{\mathrm{GE}}$ when its equations as inputs are $\perp$ with probability $1-p$ and $\langle \mathbf{a}_i,\mathbf{s}\rangle$, with probability p. To complete the proof, it suffices to use the definition of the trace distance. □

A.3. **Additional Material for Section 4.4.** In this subsection, we prove Lemma 27.

Proof of Lemma 27. Let $A, B : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ be defined as follows:

$$\begin{aligned} A(y) &\stackrel{\text{def}}{=} \sum_{x \in [\![-\lceil q/2 \rceil, \lfloor q/2 \rfloor]\!]} \omega_q^{xy} \left(\sqrt{\vartheta_{\alpha q}(x)} - \sqrt{D_{\mathbb{Z},\alpha q}(x)} \right), \\ B(y) &\stackrel{\text{def}}{=} \sum_{x \in [\![-\lceil q/2 \rceil, \lfloor q/2 \rfloor]\!]} \omega_q^{xy} \left(\frac{\sum_{k \in \mathbb{Z}} \rho_{\sqrt{2}\alpha q}(x+kq)}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}} - \sqrt{D_{\mathbb{Z},\alpha q}(x)} \right). \end{aligned}$$

Then, it holds that

$$\begin{aligned} \widehat{f}(y) &= \frac{1}{\sqrt{q}} \sum_{x \in [\![-\lceil q/2 \rceil, \lfloor q/2 \rfloor]\!]} \omega_q^{xy} \sqrt{\vartheta_{\alpha q}(x)} \\ &= \frac{1}{\sqrt{q}} \left(\sum_{x \in [\![-\lceil q/2 \rceil, \lfloor q/2 \rfloor]\!]} \omega_q^{xy} \frac{\sum_{k \in \mathbb{Z}} \rho_{\sqrt{2}\alpha q}(x+kq)}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}} + A(y) - B(y) \right), \end{aligned}$$

where we used the fact that $\sqrt{\rho_{\alpha q}} = \rho_{\sqrt{2}\alpha q}$. Following the Poisson summation formula, the above term is equal to:

$$\frac{1}{\sqrt{q}} \Big(\sum_{\ell \in \mathbb{Z}} \omega_q^{\ell y} \frac{\rho_{\sqrt{2}\alpha q}(\ell)}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}} + A(y) - B(y) \Big) = \frac{1}{\sqrt{q}} \Big(\sum_{\ell \in \mathbb{Z}} \frac{\sqrt{2}\alpha q}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}} \rho_{1/(\sqrt{2}\alpha q)} \big(\ell + \frac{y}{q}\big) + A(y) - B(y) \Big) \quad (30)$$

Lemma 35. *Using the notations above, if $\alpha \leq \frac{\pi}{2}$, then we have $|A(y)| + |B(y)| \leq 4\sqrt{\alpha q}\, q\, e^{-1/\alpha^2}$.*

Proof. Using the fact that $\sqrt{\rho_s} = \rho_{\sqrt{2}s}$, we have

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

It follows that

$$\begin{aligned} |B(y)| &\leq \frac{\rho_{\sqrt{2}\alpha q}(\mathbb{Z})}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}} \sum_{x \in [\![-\lceil q/2 \rceil, \lfloor q/2 \rfloor]\!]} \left(\vartheta_{\sqrt{2}\alpha q}(x) - D_{\mathbb{Z},\sqrt{2}\alpha q}(x) \right) \quad \text{(by the triangle inequality)} \\ &\leq \frac{\rho_{\sqrt{2}\alpha q}(\mathbb{Z})}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}}\, q\, e^{-1/\alpha^2} \quad \text{(by Lemma 12)} \\ &\leq 2\sqrt{\alpha q}\, q\, e^{-1/\alpha^2} \quad \text{(by Lemma 11).} \end{aligned}$$

Note that the condition $\alpha \leq \frac{\pi}{2}$ is required to apply Lemma 10.

On the other hand, we have

$$\begin{aligned}
|A(y)| &= \left| \sum_{x\in[\![-\lceil q/2\rceil,\lfloor q/2\rfloor]\!]} \omega_q^{xy} \left(\sqrt{\vartheta_{\alpha q}(x)} - \sqrt{D_{\mathbb{Z},\alpha q}(x)}\right) \right| \\
&\le \sum_{x\in[\![-\lceil q/2\rceil,\lfloor q/2\rfloor]\!]} \left(\sqrt{\vartheta_{\alpha q}(x)} - \sqrt{D_{\mathbb{Z},\alpha q}(x)}\right) \quad \text{(by the triangle inequality)} \\
&\le \sum_{x\in[\![-\lceil q/2\rceil,\lfloor q/2\rfloor]\!]} e^{-1/\alpha^2} \quad \text{(by Lemma 12)} \\
&= q\, e^{-1/\alpha^2}.
\end{aligned}$$

One can conclude by adding the two terms. □

Lemma 36. *For every $y \in \mathbb{Z}$, it holds that* $\sum_{\ell\in\mathbb{Z}} \rho_{1/(\sqrt{2}\alpha q)}\big(\ell + \frac{y}{q}\big) \ge e^{-\pi\alpha^2 q^2/2}$.

Proof. The minimum occurs when $y/q = 1/2$. **[Pouria : TODO]** □

Using the bounds above, as long as $\alpha = O(1/\sqrt{q})$, in Equation (30), the summation asymptotically dominates the quantity $|A(y)| + |B(y)|$ for every $y \in \mathbb{Z}$. More precisely, we have

$$\begin{aligned}
|A(y)| + |B(y)| &\le 4\sqrt{\alpha q}\; q\; e^{-1/\alpha^2} \\
&= o\left(4\sqrt{\alpha q}\; q\; e^{-\pi\alpha^2 q^2/2}\right) \\
&= o\left(\sum_{\ell\in\mathbb{Z}} \frac{\sqrt{2}\alpha q}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}}\; \rho_{1/(\sqrt{2}\alpha q)}\big(\ell + \frac{y}{q}\big)\right)
\end{aligned}$$

Recall that Equation (30) is equal to $|\hat{f}(y)|$, therefore we obtain

$$\min_y \left|\widehat{f}(y)\right|^2 = O\Big(\frac{\alpha\sqrt{2q}}{\sqrt{\rho_{\alpha q}(\mathbb{Z})}}\; e^{-\pi\alpha^2 q^2/2}\Big)^2.$$

The lemma follows by noting that

$$\rho_{\alpha q}(\mathbb{Z}) = \alpha q \cdot \rho_{\alpha q}(\mathbb{Z}) \ge \alpha q,$$

where we used Poisson summation formula. □

Appendix B. Elementary Materials for SNARKs

Email address: thomas.debris@inria.fr

Email address: pouria.fallahpour@ens-lyon.fr

Email address: damien.stehle@ens-lyon.fr

[1] Inria

[2] Laboratoire LIX, École Polytechnique, Palaiseau, France

[3] ENS de Lyon, Lyon, France

[4] Cryptolab Inc., Lyon, France