

On the Quantum Equivalence between $S|LWE\rangle$ and ISIS

André Chailloux and Paul Hermouet

Inria de Paris, COSMIQ team

`andre.chailloux@inria.fr`

`paul.hermouet@inria.fr`

Abstract. Chen, Liu, and Zhandry [CLZ22] introduced the problems $S|LWE\rangle$ and $C|LWE\rangle$ as quantum analogues of the Learning with Errors problem, designed to construct quantum algorithms for the Inhomogeneous Short Integer Solution (ISIS) problem. Several later works have used this framework for constructing new quantum algorithms in specific cases. However, the general relation between all these problems is still unknown.

In this paper, we investigate the equivalence between $S|LWE\rangle$ and ISIS. We present the first fully generic reduction from ISIS to $S|LWE\rangle$, valid even in the presence of errors in the underlying algorithms. We then explore the reverse direction, introducing an inhomogeneous variant of $C|LWE\rangle$, denoted $IC|LWE\rangle$, and show that $IC|LWE\rangle$ reduces to $S|LWE\rangle$. Finally, we prove that, under certain recoverability conditions, an algorithm for ISIS can be transformed into one for $S|LWE\rangle$. We instantiate this reverse reduction by tweaking a known algorithm for (I)SIS_∞ in order to construct quantum algorithm for $S|LWE\rangle$ when the alphabet size q is a small power of 2, recovering some results of Bai et al. [BJK⁺25]. Our results thus clarify the landscape of reductions between $S|LWE\rangle$ and ISIS, and we show both their strong connection as well as the remaining barriers for showing full equivalence.

1 Introduction

1.1 Context

A cornerstone of lattice-based cryptography is Regev’s reduction [Reg05], which is a quantum reduction between some lattice-based problems related to the *Short Integer Solution* (SIS) problem and the *Learning With Errors* (LWE) problem. This is a quantum reduction that uses a (classical or quantum) algorithm for LWE in order to create a superposition of noisy lattice points and then measuring in the Fourier basis to obtain a short dual lattice point.

As noted in [SSTX09], we actually need to solve an easier problem than LWE, since the error can be in quantum superposition. This creates strong links between this problem and the *Dihedral Coset Problem*. This was actually first explicitly used by Brakerski, Kirshanova, Stehlé and Wen [BKSW18] where they extend this reduction and introduce the Extended Dihedral Coset Problem.

A few years later, Chen Liu and Zhandry [CLZ22] revisited this reduction for algorithmic purposes. They show that in some regimes, the LWE problem with errors in quantum superposition, which they call the $S|LWE\rangle$ problem, can be significantly easier than the standard LWE problem. They show how to construct polynomial time quantum algorithm for the SIS_∞ for some parameters. While these parameters are still very far from those used in lattice-based cryptography, this result shows the very promising nature of this family of algorithms.

This framework has then been successfully used. Yamakawa and Zhandry [YZ24] provided a first quantum advantage without structure in the Random Oracle Model, and was used in a somewhat different context to construct quantum oblivious sampling [DFS24]. This approach has also been extended to the setting of linear codes [DRT23, CT24], as well as structured codes in order to obtain a quantum advantage [JSW⁺24, CT25]. All of these results use an algorithm for $S|LWE\rangle$ to construct an algorithm for SIS or ISIS and perform an ad hoc analysis of this reduction. Note that we cannot have a generic reduction from SIS to $S|LWE\rangle$ using this approach (see [CT24]). However, Chailloux and Tillich [CT25] provided the first generic reduction, but from ISIS to $S|LWE\rangle$. This reduction does however have some assumptions on the $S|LWE\rangle$ algorithm, which are satisfied by classical algorithms but not necessarily by quantum algorithms. A first natural question arises.

Question 1. Is it possible to have a fully general reduction from ISIS to $S|LWE\rangle$ that is robust to errors in the decoder?

Also, because of the importance of $S|LWE\rangle$, recent works directly construct quantum algorithms for $S|LWE\rangle$. First, a generic quantum algorithm for $S|LWE\rangle$ was presented in [CHL⁺25], running in subexponential time and requiring a subexponential of queries. Then, the authors of [BJK⁺25] presented a slightly superpolynomial algorithm for $S|LWE\rangle$ in the case where the alphabet size q is a small power of 2. These results both use variants of the quantum Kuperberg sieve [Kup13] for the Dihedral Coset Problem. When looking at these algorithms more carefully, one can notice that they are actually very similar to known classical algorithm for ISIS and this raises the following natural question

Question 2. Is there a way to construct algorithms for $S|LWE\rangle$ from algorithms for ISIS? More generally, are the problems $S|LWE\rangle$ and ISIS equivalent?

1.2 Problems studied

In order to present our results, we first formally define some of the problems we consider in this work in order to properly state our contributions. We provide a more in-depth description of these problems and their relation to other lattice-based problems in Section 2.2.

Definition 1 (Inhomogeneous Short Integer Solution $ISIS(\mathbf{A}, T)$). Let positive integers q, n, m , a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $T \subseteq \mathbb{Z}^m$. We sample $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ and the goal is, given $(\mathbf{A}, \mathbf{y})$ and T , to find $\mathbf{x} \in T$ such that $\mathbf{Ax} = \mathbf{y} \pmod{q}$.

This problem is usually defined for matrices $\mathbf{A}$ chosen at random and the set T chosen as $\{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\|_2 \leq \beta\}$ for a parameter β . Our results will hold for any choice of matrices and of set T , which makes our results more general. Chen, Liu, and Zhandry introduced variants of the canonical Learning With Errors problem, namely Search-LWE ($S|LWE\rangle$) and Construct-LWE ($C|LWE\rangle$).

Definition 2. $S|LWE\rangle(\mathbf{A}, f)$.

Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\|_2 = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$. Given $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle$, the goal is to recover $\mathbf{s}$.

Definition 3. $C|LWE\rangle(\mathbf{A}, f)$.

Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\|_2 = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. The goal is to construct the unit vector

$$|W\rangle = \frac{1}{\sqrt{Z}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle,$$

where Z is a normalization factor.

In this work, we also introduce an inhomogeneous variant of the Construct LWE problem.

Definition 4. $IC|LWE\rangle(\mathbf{A}, f)$.

Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We sample $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ and the goal is to construct the unit vector

$$|W_{\mathbf{y}}\rangle = \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{-\mathbf{y} \cdot \mathbf{s}} f(\mathbf{e})|\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle,$$

where $w_{\mathbf{y}}$ is a normalization factor and $\omega = e^{\frac{2i\pi}{q}}$.

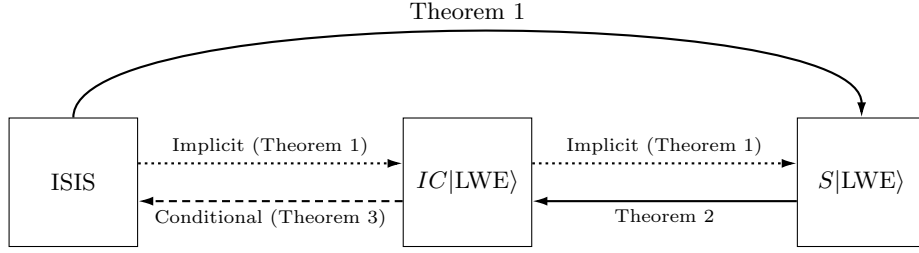


Fig. 1: Table of reductions between the different studied problems. An arrow $A \rightarrow B$ means that A reduces to B , or in other terms that an efficient algorithm for problem B can be used to construct an efficient algorithm for problem A .

1.3 Contributions

The goal of this paper is to investigate the two-way reduction between ISIS and $S|LWE$. A graphical summary of our results is presented in figure 1. Our first contribution relates to the forward reduction $ISIS \rightarrow S|LWE$.

Theorem 1 (Informal). *If we have an efficient algorithm solving $S|LWE(\mathbf{A}, f)$ with $Im(\hat{f}) \subseteq T$, then we can construct an efficient algorithm for $ISIS(\mathbf{A}, T)$.*

This theorem works also when the algorithm solves $S|LWE(\mathbf{A}, f)$ with some non-negligible probability p and we also show how to relax the constraint $Im(\hat{f}) \subseteq T$. The only requirement — which appears in all the works using this reduction — is that the state $\sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$ is efficiently sampleable.

In order to prove this result, we start from the reduction of [CT25] and make a few notable changes. Our main goal was to ensure the reduction of [CT25] holds for any quantum algorithm solving $S|LWE(\mathbf{A}, f)$, since several applications actually use a full quantum algorithm here. First, we change slightly the way the algorithm works in order to be used with quantum algorithms. Our main contribution then it to change the error analysis occurring from an error in the $S|LWE(\mathbf{A}, f)$ algorithm. We fully take advantage of the fact that we want solve the inhomogeneous variant $ISIS(\mathbf{A}, T)$ in order to perform a tighter analysis. Another thing to note is that we rephrase this reduction in terms of lattice problems while [CT25] phrases the reduction in terms of coding problems. There is a straightforward correspondence between the two but our formulation makes it easier to relate with existing work on the subject.

We can directly apply this theorem with standard lattice-based parameters. Informally, if we consider a discrete Gaussian on $\mathbb{Z}_q$ with standard deviation σ , which we denote χ_σ , then an algorithm for solving $S|LWE(\mathbf{A}, \chi_\sigma^m)$ for a randomly chosen matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ can be used to solve $ISIS(\mathbf{A}, T)$ with $T = \{\mathbf{x} \in \mathbb{F}_q^n : \|\mathbf{x}\|_2 \leq \frac{q\sqrt{m}}{\sigma}\}$ at least for $\sigma \ll q$. This is directly implied by our theorem, since $\widehat{\chi_\sigma} \approx \chi_{\frac{q}{\sigma}}$ and the distribution $\chi_{\frac{q}{\sigma}}^m$ is highly concentrated around

words of norm $\sqrt{m} \frac{q}{\sigma}$.

Then, we study the reverse reduction. To the best of our knowledge, no results were known on this direction before our work. Interestingly, the reduction $\text{ISIS} \rightarrow S|\text{LWE}\rangle$ actually goes through the intermediate problem which is $IC|\text{LWE}\rangle$. We do not formally write it as a reduction $\text{ISIS} \rightarrow IC|\text{LWE}\rangle$ and $IC|\text{LWE}\rangle \rightarrow S|\text{LWE}\rangle$ because it would induce a loss in some of the parameters but our Theorem 1 actually implicitly uses this route. Our first result for the reverse reduction is that $S|\text{LWE}\rangle$ reduces to $IC|\text{LWE}\rangle$

Theorem 2 (informal). *If we have an efficient quantum algorithm that solves $IC|\text{LWE}\rangle(\mathbf{A}, f)$ then we have an efficient quantum algorithm for $S|\text{LWE}\rangle(\mathbf{A}, f)$.*

This theorem does not require anything on the algorithm for $IC|\text{LWE}\rangle(\mathbf{A}, f)$, and is robust to errors in the algorithm. One thing to take into account is that the problem $S|\text{LWE}\rangle(\mathbf{A}, f)$ can be impossible from an information theoretic point of view for certain choices of f . We explicit this regime and show that our theorem holds for any f such that the problem $S|\text{LWE}\rangle(\mathbf{A}, f)$ is tractable from an information theoretic point of view.

Finally, we investigate the relation between $IC|\text{LWE}\rangle(\mathbf{A}, f)$ and $\text{ISIS}(\mathbf{A}, T)$. Recall that in $IC|\text{LWE}\rangle(\mathbf{A}, f)$, we want to compute the state $|W_{\mathbf{y}}\rangle$ for a random $\mathbf{y} \in \mathbb{Z}_q$. We can compute the Fourier transform of this state and obtain the state

$$|\widehat{W_{\mathbf{y}}}\rangle \sim \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})} \widehat{f}(\mathbf{x})|\mathbf{x}\rangle,$$

where $\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}^{\top} \mathbf{x} = \mathbf{y} \bmod q\}$ denotes the q -ary shifted dual lattice associated to $\mathbf{A}$. On the other hand an algorithm for $\text{ISIS}(\mathbf{A}, T)$ outputs a string $\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) \cap T$, so if we take $\widehat{f} = \mathbb{1}_T$, the two problems look quite similar. Unfortunately, even from an algorithm that outputs a uniformly random element of $\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) \cap T$, it is not clear how to construct the state $|\widehat{W_{\mathbf{y}}}\rangle$.

Under some condition on the algorithm used for ISIS , we can prove the missing part of the reduction, namely that $IC|\text{LWE}\rangle \rightarrow \text{ISIS}$. More precisely, we introduce the notion of randomness recoverable algorithms, which are randomized classical algorithms from which we can recover the randomness from the solution. We manage to prove the following

Theorem 3 (Informal). *Assume we have an efficient classical algorithm for $\text{ISIS}(\mathbf{A}, T)$ which is randomness recoverable, then we can have an efficient quantum algorithm for $IC|\text{LWE}\rangle(\mathbf{A}, f)$, with $\widehat{f} = \mathbb{1}_T$.*

Notice that using Theorem 2, this means we can also obtain an algorithm for $S|\text{LWE}\rangle(\mathbf{A}, f)$. The formal theorem actually also requires that the output distribution of the algorithm closely matches the uniform distribution over the set of solutions.

While these conditions on the algorithm for ISIS seem very strict and potentially unachievable for real algorithms, we show that this is not the case. Our final

contribution is to show how to recover (and extend) an algorithm of [BJK⁺25] for $S|LWE\rangle$ in the case q is a small power of two. This result was phrased in terms of the $\overline{\text{EDCP}}$ problem and we rephrase it in terms of the $S|LWE\rangle$ problem.

Proposition 1 ([BJK⁺25]). *For some parameters $n, m, q = 2^l$ with $q = \text{poly}(n)$ and $m = 2^{O(\log(n) \log(q))}$, there exists an algorithm for $S|LWE\rangle(\mathbf{A}, f)$ in the case $\mathbf{A}$ is randomly chosen in $\mathbb{Z}_q^{n \times m}$ and f is the function such that $\hat{f} = \mathbb{1}_{\mathbb{Z}_2^m}$.*

The quantum algorithm used to prove this proposition is a Kuperberg style algorithm but strongly leverages on the fact that q is a small power of 2, with ideas that were already developed by Bonnetain and Naya-Plasencia [BN18] in a somewhat different context.

When looking at this algorithm carefully, this quantum algorithm also strongly resembles a classical algorithm for SIS_∞ in the same parameter regime (by replacing n with $m - n$). This algorithm was presented in [CLZ22, Appendix A of the ArXiv version], and attributed to Regev. A natural question therefore becomes whether this algorithm can be used in our reverse reduction.

We show that it is actually possible to modify this classical algorithm to the case of ISIS and such that it satisfies all the requirements of Theorem 3.

Theorem 4 (Informal). *One can adapt the classical algorithm for ISIS by Regev to make it randomness recoverable. Plugging this algorithm into Theorems 2 and 3, we can recover Proposition 1.*

1.4 Takeaways and Future Work

Our first contribution is important as it provides what we hope to be the final form of the reduction $\text{ISIS} \rightarrow S|LWE\rangle$. A natural direction for future work is to extend this reduction to codes, which we believe will help address open questions related to the *Decoded Quantum Interferometry* framework. In particular, we hope to leverage this reduction to directly apply the soft decoders introduced in [CT25] to the Optimal Polynomial Intersection Problem (*OPI*), as originally defined by [JSW⁺24].

From a conceptual standpoint, the reverse reduction is new. This is the first time there is an (even conditional) tight reduction between these two problems. It shows that one cannot fundamentally improve this framework based on Regev’s reduction if we restrict ourselves to $S|LWE\rangle$ and ISIS. When the reduction was phrased between ISIS and LWE, such a reverse reduction could not be envisioned. Moreover, we showed that the intermediate problem $IC|LWE\rangle$ is key to understanding the relation between these problems.

Our results could also be used to construct other algorithms for $S|LWE\rangle$ (or equivalently $\overline{\text{EDCP}}$ defined in [BJK⁺25]). We have already recovered some of these results showing that the randomness-recoverability conditions are achievable. It would be interesting to explore other algorithms, such as the one by Chen et al. [CHL⁺25], and investigate whether they fit into our framework. Finally, finding new algorithms for $S|LWE\rangle$ could have significant consequences, since there is

a reduction $\text{LWE} \rightarrow S|\text{LWE}\rangle$ shown in [BKS18]. While our reverse reduction has some limitations, it nevertheless paves the way for many potential new algorithms for $S|\text{LWE}\rangle$, obtained via known algorithms for ISIS-type problems and incorporated into the reduction of [BKS18].

2 Preliminaries

2.1 Notations

For a positive integer q , we write $\mathbb{Z}_q$ for $\mathbb{Z}/q\mathbb{Z}$. We write $\mathbb{Z}_q = \{-\lfloor \frac{q}{2} \rfloor, \dots, \lfloor \frac{q-1}{2} \rfloor\}$. Vectors with elements in $\mathbb{Z}_q$ will be denoted with bold small letters such as $\mathbf{x}, \mathbf{y}$ and matrices with elements in $\mathbb{Z}_q$ will be denoted with capital bold letters such as $\mathbf{A}, \mathbf{H}$.

The canonical q -th root of unity is denoted $\omega_q = e^{2i\pi/q}$. We will consider only roots of unity ω_q for the alphabet size q and will usually omit the subscript q .

For any probability distribution D , we write $x \leftarrow D$ to indicate that x is sampled according to D . We abuse the notation and write $x \leftarrow S$ for any set S to indicate that x is sampled uniformly from S .

Definition 5. Let positive integers q, n, m and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. For each $\mathbf{y} \in \mathbb{Z}_q^n$, we define the shifted dual lattice

$$\Lambda_{\mathbf{y}}^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}^\top \mathbf{x} = \mathbf{y} \pmod{q}\}.$$

Fourier Transform and Quantum Fourier Transform For a function $f : \mathbb{Z}_q \rightarrow \mathbb{C}$, we define its Fourier transform

$$\hat{f}(x) = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{Z}_q} \omega^{xy} f(y).$$

We extend this definition to functions $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ and denote the Fourier transform of f as $\hat{f}(\mathbf{x}) = \frac{1}{\sqrt{q^m}} \sum_{\mathbf{y} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot \mathbf{y}} f(\mathbf{y})$. The Quantum Fourier Transform on $\mathbb{Z}_q$ is the unitary operations

$$QFT_{\mathbb{Z}_q}(|x\rangle) = |\hat{x}\rangle = \frac{1}{\sqrt{q}} \sum_{y \in \mathbb{Z}_q} \omega^{xy} |y\rangle.$$

Again, it is extended to a unitary acting on $\mathbb{Z}_q^m$ as follows: $QFT_{\mathbb{Z}_q^m}(|\mathbf{x}\rangle) = |\hat{\mathbf{x}}\rangle = \frac{1}{\sqrt{q^m}} \sum_{\mathbf{y} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot \mathbf{y}} |\mathbf{y}\rangle$. We omit the subscript and simply write QFT when clear from the context.

2.2 Definition

The Short Integer Solution problem is one of the cornerstones of lattice-based cryptography.

Definition 6 (Short Integer Solution SIS($\mathbf{A}, \beta$)). Let positive integers q, n, m , and β and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. The goal is, given $\mathbf{A}$, to find $\mathbf{x} \in \mathbb{Z}^m \setminus \{\mathbf{0}\}$ such that $\mathbf{Ax} = \mathbf{0} \pmod{q}$ and $\|\mathbf{x}\|_2 \leq \beta$.

The above problem is usually defined for a uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ but is also defined for structured matrices and/or with other norms such as the infinity norm. This problem also has what is called an inhomogeneous variant

Definition 7 (Inhomogeneous Short Integer Solution ISIS($\mathbf{A}, \beta$)). Let positive integers q, n, m, β and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We sample $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ and the goal is, given $(\mathbf{A}, \mathbf{y})$, to find $\mathbf{x} \in \mathbb{Z}^m$ such that $\mathbf{Ax} = \mathbf{y} \pmod{q}$ and $\|\mathbf{x}\|_2 \leq \beta$.

We generalize these definitions by replacing the condition $\|\mathbf{x}\|_2 \leq \beta$ with the condition $\mathbf{x} \in T$ for a given set T .

Definition 8 (Short Integer Solution SIS($\mathbf{A}, T$)). Let positive integers q, n, m , a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $T \subseteq \mathbb{Z}^m$. The goal is, given $\mathbf{A}$ and T , to find $\mathbf{x} \in T \setminus \{\mathbf{0}\}$ such that $\mathbf{Ax} = \mathbf{0} \pmod{q}$.

Definition 9 (Inhomogeneous Short Integer Solution ISIS($\mathbf{A}, T$)). Let positive integers q, n, m , a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $T \subseteq \mathbb{Z}^m$. We sample $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ and the goal is, given $(\mathbf{A}, \mathbf{y})$ and T , to find $\mathbf{x} \in T$ such that $\mathbf{Ax} = \mathbf{y} \pmod{q}$.

We now define a general form of the Learning with errors problem, for an alphabet size q , dimension n and number of samples m .

Definition 10 (Learning With Errors LWE($\mathbf{A}, p$)). Let positive integers q, n, m , a probability distribution p on $\mathbb{Z}_q^m$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and $\mathbf{e} \leftarrow p$. Given $(\mathbf{A}, \mathbf{A}^\top \mathbf{s} + \mathbf{e})$, the goal is to recover $\mathbf{s}$.

This problem is commonly studied in the case where $\mathbf{A}$ is uniformly chosen in $\mathbb{Z}_q^{n \times m}$ and $p = \chi^m$ where χ is a discretized Gaussian distribution on $\mathbb{Z}_q$. We now define the variants explicitly introduced in [CLZ22], where the noise is in quantum superposition.

Definition 11. $S|\text{LWE}\rangle(\mathbf{A}, f)$.

Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$. Given $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle$, the goal is to recover $\mathbf{s}$.

Notice that by measuring $|\psi_{\mathbf{s}}\rangle$, one can recover a random $\mathbf{A}^\top \mathbf{s} + \mathbf{e}$ for $\mathbf{e} \leftarrow |f|^2$. This immediately implies that $S|\text{LWE}\rangle(\mathbf{A}, f)$ is easier than $\text{LWE}(\mathbf{A}, |f|^2)$.

Definition 12. $C|\text{LWE}\rangle(\mathbf{A}, f)$.

Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. The goal is to construct the unit vector

$$|W\rangle = \frac{1}{\sqrt{Z}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle,$$

where Z is a normalization factor.

In this work, we introduce an inhomogeneous variant of this problem, which will be useful for our reductions.

Definition 13. $IC|LWE\rangle(\mathbf{A}, f)$.

Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. We sample $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ and the goal is to construct the unit vector

$$|W_{\mathbf{y}}\rangle = \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{-\mathbf{y} \cdot \mathbf{s}} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle,$$

where $w_{\mathbf{y}}$ is a normalization factor.

3 Preliminary calculations around $S|LWE\rangle$ and $IC|LWE\rangle$ and tractability results

The goal of this section is to present some preliminary calculations on the $S|LWE\rangle$, $IC|LWE\rangle$ and ISIS problems. We also provide a discussion on the tractability regime of $S|LWE\rangle$ from an information theoretic view, which is a direct generalization of results in [CT24].

3.1 Preliminary calculations

An important calculation will be to write the states $|\psi_{\mathbf{s}}\rangle$ and $|W_{\mathbf{y}}\rangle$ appearing respectively in $S|LWE\rangle$ and $IC|LWE\rangle$ in the Fourier basis.

Proposition 2. Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. For each $\mathbf{s} \in \mathbb{Z}_q^n$, we define $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle$. We have

$$|\widehat{\psi_{\mathbf{s}}}\rangle = \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle.$$

Proof. We write

$$\begin{aligned} |\widehat{\psi_{\mathbf{s}}}\rangle &= \frac{1}{\sqrt{q^m}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot (\mathbf{A}^\top \mathbf{s} + \mathbf{e})} f(\mathbf{e}) |\mathbf{x}\rangle \\ &= \frac{1}{\sqrt{q^m}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot \mathbf{A}^\top \mathbf{s}} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot \mathbf{e}} f(\mathbf{e}) |\mathbf{x}\rangle \\ &= \frac{1}{\sqrt{q^m}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \omega^{\mathbf{A} \mathbf{x} \cdot \mathbf{s}} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot \mathbf{e}} f(\mathbf{e}) |\mathbf{x}\rangle \\ &= \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \omega^{\mathbf{A} \mathbf{x} \cdot \mathbf{s}} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle \\ &= \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle \end{aligned}$$

Proposition 3. Let positive integers q, n, m , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. For each $\mathbf{y} \in \mathbb{Z}_q^n$, let

$$|W_{\mathbf{y}}\rangle = \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{-\mathbf{y} \cdot \mathbf{s}} f(\mathbf{e}) |\mathbf{A}^T \mathbf{s} + \mathbf{e}\rangle.$$

Then $|\widehat{W_{\mathbf{y}}}\rangle = \frac{q^n}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle$.

Proof. We write

$$\begin{aligned} |\widehat{W_{\mathbf{y}}}\rangle &= \frac{1}{\sqrt{q^m}} \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot (\mathbf{A}^T \mathbf{s} + \mathbf{e})} \omega^{-\mathbf{y} \cdot \mathbf{s}} f(\mathbf{e}) |\mathbf{x}\rangle \\ &= \frac{1}{\sqrt{q^m}} \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{\mathbf{x} \cdot \mathbf{A}^T \mathbf{s} - \mathbf{y} \cdot \mathbf{s}} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} \omega^{\mathbf{x} \cdot \mathbf{e}} f(\mathbf{e}) |\mathbf{x}\rangle \\ &= \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{(\mathbf{A}\mathbf{x} - \mathbf{y}) \cdot \mathbf{s}} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle \\ &= \frac{q^n}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle \end{aligned}$$

where in the last equality follows from the identity $\sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{(\mathbf{A}\mathbf{x} - \mathbf{y}) \cdot \mathbf{s}} = 0$ if $\mathbf{A}\mathbf{x} - \mathbf{y} \neq 0$, and q^n otherwise.

This proposition shows in particular that if one can construct the state $|W_{\mathbf{y}}\rangle$ for any $\mathbf{y} \in \mathbb{Z}_q^n$ with $\text{Im}(\widehat{f}) \subseteq T$ then one can solve the ISIS($\mathbf{A}, T$) by applying a Quantum Fourier Transform on $|W_{\mathbf{y}}\rangle$ and measuring the resulting state in the computational basis. Also, this proposition directly implies that the $|W_{\mathbf{y}}\rangle$ are pairwise orthogonal.

Finally, we present relations between these states.

Proposition 4.

$$\begin{aligned} \forall \mathbf{y} \in \mathbb{Z}_q^n, \quad |W_{\mathbf{y}}\rangle &= \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} |\psi_{\mathbf{s}}\rangle \\ \forall \mathbf{s} \in \mathbb{Z}_q^n, \quad |\psi_{\mathbf{s}}\rangle &= \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sqrt{w_{\mathbf{y}}} |W_{\mathbf{y}}\rangle \end{aligned}$$

Proof. The first inequality comes directly from the definitions of $|W_{\mathbf{y}}\rangle$ and $|\psi_{\mathbf{s}}\rangle$. For the second equality, the above two propositions immediately imply that

$$|\widehat{\psi_{\mathbf{s}}}\rangle = \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \frac{\sqrt{w_{\mathbf{y}}}}{q_n} |\widehat{W_{\mathbf{y}}}\rangle,$$

which gives the result by performing an inverse Quantum Fourier Transform on each side of the equality.

Finally, we give a proposition related to the norms $w_{\mathbf{y}}$.

Proposition 5. $\mathbb{E}_{\mathbf{y}}[w_{\mathbf{y}}] = q^n$.

Proof. Because $|\widehat{W}_{\mathbf{y}}\rangle$ is a unit vector, we have

$$w_{\mathbf{y}} = q^{2n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})} |\widehat{f}(\mathbf{x})|^2.$$

Since $\|f\| = \|\widehat{f}\| = 1$, we immediately have

$$\frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} w_{\mathbf{y}} = q^n \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})} |\widehat{f}(\mathbf{x})|^2 = q^n \sum_{\mathbf{x} \in \mathbb{Z}_q^n} |\widehat{f}(\mathbf{x})|^2 = q^n.$$

3.2 Tractability bound for $S|\text{LWE}\rangle(\mathbf{A}, f)$

Proposition 6. Let q, m, n be positive integers. Let $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ such that $\|f\| = 1$ and let $\mathbf{A} \in \mathbb{Z}_q^n$. For each $\mathbf{y} \in \mathbb{Z}_q^n$, let

$$|W_{\mathbf{y}}\rangle = \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{e} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} f(\mathbf{e}) |\mathbf{A}^T \mathbf{s} + \mathbf{e}\rangle,$$

where $w_{\mathbf{y}}$ is a normalizing factor so that $|W_{\mathbf{y}}\rangle$ are unit vectors. The maximum probability p_{max} that a (potentially unbounded) quantum algorithm has of solving $S|\text{LWE}\rangle(\mathbf{A}, f)$ is

$$p_{max} = \left(\mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} \left[\sqrt{\frac{w_{\mathbf{y}}}{q^n}} \right] \right)^2.$$

Proof. This is proven by analyzing the Pretty Good Measurement on the states $|\psi_{\mathbf{s}}\rangle$, which turns out to be optimal for this family of states and then reusing the analysis of [CT24]. For completeness, we formally prove this proposition in Appendix A.

This proposition explains why the term $\mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} \left[\sqrt{\frac{w_{\mathbf{y}}}{q^n}} \right]$ appears in some of our reductions.

4 The forward direction $\text{ISIS} \rightarrow S|\text{LWE}\rangle$

Our first result is to prove the general forward reduction $\text{ISIS} \rightarrow S|\text{LWE}\rangle$.

Theorem 1. Let positive integers q, m, n , let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and let $f : \mathbb{Z}_q^n \rightarrow \mathbb{C}$ with $\|f\| = 1$. Let $T \subseteq \mathbb{Z}_q^n$. Assume that

- There exists a quantum algorithm that solves $S|\text{LWE}\rangle(\mathbf{A}, f)$ in time $\text{Time}_{S|\text{LWE}\rangle}$ and succeeds with probability p .
- $\sum_{\mathbf{x} \in T} |\widehat{f}(\mathbf{x})|^2 = 1 - \eta$.

- f is quantum samplable in time $\text{Time}_{\text{Sampl}}$ i.e. there is a quantum algorithm running in time $\text{Time}_{\text{Sampl}}$ that constructs the state $\sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$.

Then there exists a quantum algorithm that solves $\text{ISIS}(\mathbf{A}, T)$, that succeeds with probability at least $p(1 - \eta) - 2\sqrt{p(1 - p)}\eta$ and runs in time

$$\text{Time}_{\text{ISIS}} = O\left(\frac{1}{p} (\text{Time}_{S|\text{LWE}} + \text{Time}_{\text{Sampl}}) + \text{poly}(m, \log(q))\right).$$

The remainder of this section is devoted to the proof of this theorem.

4.1 Characterization of quantum algorithms for $S|\text{LWE}\rangle$

A quantum algorithm for $S|\text{LWE}\rangle(\mathbf{A}, f)$ can be described by a unitary U (that depends on $\mathbf{A}$ and f) such that for all $\mathbf{s} \in \mathbb{Z}_q^n$,

$$U|\psi_{\mathbf{s}}\rangle|0\rangle = \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma_{\mathbf{s}, \mathbf{s}'} |\mathbf{s}'\rangle |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle, \text{ for some unit vectors } |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle \text{ and } \gamma_{\mathbf{s}, \mathbf{s}'} \in \mathbb{C},$$

and the result is obtained by measuring the first register. The success probability of this algorithm for each $\mathbf{s}$ is $p_{\mathbf{s}} = |\gamma_{\mathbf{s}, \mathbf{s}}|^2$ and the overall success probability is $p = \frac{1}{q^n} \sum_{\mathbf{s}} |\gamma_{\mathbf{s}, \mathbf{s}}|^2$. We first prove that any such quantum algorithm can be symmetrized in the sense that each $\gamma_{\mathbf{s}, \mathbf{s}}$ is equal to $\sqrt{p}$.

Proposition 7. *Let $\mathcal{A}$ be an efficient quantum algorithm for $S|\text{LWE}\rangle(\mathbf{A}, f)$ that succeeds with probability p . There exists an efficiently computable unitary U such that for all $\mathbf{s} \in \mathbb{Z}_q^n$,*

$$U|\psi_{\mathbf{s}}\rangle|0\rangle = \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma'_{\mathbf{s}, \mathbf{s}'} |\mathbf{s}'\rangle |\tilde{\psi}''_{\mathbf{s}, \mathbf{s}'}\rangle, \text{ for some unit vectors } |\tilde{\psi}''_{\mathbf{s}, \mathbf{s}'}\rangle \text{ and each } \gamma'_{\mathbf{s}, \mathbf{s}} = \sqrt{p}.$$

Proof. The idea is to use the symmetries inherent to the states $|\psi_{\mathbf{s}}\rangle$. We present a first algorithm that succeeds with probability p for each input state $|\psi_{\mathbf{s}}\rangle$. Consider the shift unitaries $S_{\mathbf{z}} : |\mathbf{x}\rangle \rightarrow |\mathbf{x} + \mathbf{z}\rangle$ for $\mathbf{x}, \mathbf{z} \in \mathbb{Z}_q^m$ which are efficiently computable. Notice that $\forall \mathbf{s}, \mathbf{t} \in \mathbb{Z}_q^n$, we have $|\psi_{\mathbf{t}}\rangle = S_{\mathbf{A}^\top(\mathbf{t} - \mathbf{s})} |\psi_{\mathbf{s}}\rangle$. We consider the following algorithm

1. Given input $|\psi_{\mathbf{s}}\rangle$, construct

$$|\Omega_1\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{t} \in \mathbb{Z}_q^n} S_{\mathbf{A}^\top \mathbf{t}} |\psi_{\mathbf{s}}\rangle |0\rangle |\mathbf{t}\rangle = \sum_{\mathbf{t} \in \mathbb{Z}_q^n} |\psi_{\mathbf{s} + \mathbf{t}}\rangle |0\rangle |\mathbf{t}\rangle.$$

2. Apply U on the first two register to obtain

$$|\Omega_2\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{t} \in \mathbb{Z}_q^n} \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma_{\mathbf{s} + \mathbf{t}, \mathbf{s}'} |\mathbf{s}'\rangle |\tilde{\psi}_{\mathbf{s} + \mathbf{t}, \mathbf{s}'}\rangle |\mathbf{t}\rangle.$$

3. We subtract the value from the third register in the first register to obtain

$$\begin{aligned} |\Omega_3\rangle &= \frac{1}{\sqrt{q^n}} \sum_{\mathbf{t} \in \mathbb{Z}_q^n} \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma_{\mathbf{s}+\mathbf{t}, \mathbf{s}'} |\mathbf{s}' - \mathbf{t}\rangle |\tilde{\psi}_{\mathbf{s}+\mathbf{t}, \mathbf{s}'}\rangle |\mathbf{t}\rangle \\ &= \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \sum_{\mathbf{t} \in \mathbb{Z}_q^n} \gamma_{\mathbf{s}+\mathbf{t}, \mathbf{s}'+\mathbf{t}} |\mathbf{s}'\rangle |\tilde{\psi}_{\mathbf{s}+\mathbf{t}, \mathbf{s}'+\mathbf{t}}\rangle |\mathbf{t}\rangle \end{aligned}$$

If we measure the first register, we obtain $\mathbf{s}$ with probability $\frac{1}{q^n} \sum_{\mathbf{t}} |\gamma_{\mathbf{s}+\mathbf{t}, \mathbf{s}+\mathbf{t}}|^2 = p$ which is independent of $\mathbf{s}$. If we perform the above algorithm fully coherently, we obtain a quantum unitary U' such that for all $\mathbf{s} \in \mathbb{Z}_q^n$,

$$U' |\psi_{\mathbf{s}}\rangle |0\rangle = \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma'_{\mathbf{s}, \mathbf{s}'} |\mathbf{s}'\rangle |\tilde{\psi}'_{\mathbf{s}, \mathbf{s}'}\rangle$$

for some unit vectors $|\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle$ and each $|\gamma'_{\mathbf{s}, \mathbf{s}}| = \sqrt{p}$. In order to conclude, we just have to put the potential phases of $\gamma'_{\mathbf{s}, \mathbf{s}}$ into the second register so if we define $|\tilde{\psi}''_{\mathbf{s}, \mathbf{s}'}\rangle = \frac{\gamma_{\mathbf{s}, \mathbf{s}'}}{|\gamma_{\mathbf{s}, \mathbf{s}'}|} |\tilde{\psi}'_{\mathbf{s}, \mathbf{s}'}\rangle$, we can indeed write

$$U' |\psi_{\mathbf{s}}\rangle |0\rangle = \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma'_{\mathbf{s}, \mathbf{s}'} |\mathbf{s}'\rangle |\tilde{\psi}''_{\mathbf{s}, \mathbf{s}'}\rangle \quad \text{with each } \gamma'_{\mathbf{s}, \mathbf{s}} = \sqrt{p}.$$

4.2 The main algorithm

Presentation of the main algorithm We present now a detailed description of our algorithm. We slightly modify the way it is presented in the literature in order to make the proofs easier.

Algorithm 1: Algorithm 1: Quantum algorithm based on Regev's reduction for ISIS

Input: We start from a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. Let $T \subseteq \mathbb{Z}^m$ and $f : \mathbb{F}_q^n \rightarrow \mathbb{C}$ such that $\|f\|_2 = 1$. For each $\mathbf{s} \in \mathbb{Z}_q^n$, we write $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^T \mathbf{s} + \mathbf{e}\rangle$. Assume we have an efficiently computable quantum unitary

$$U |\psi_{\mathbf{s}}\rangle |0\rangle = \sum_{\mathbf{s}' \in \mathbb{F}_q^k} \gamma_{\mathbf{s}, \mathbf{s}'} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle |\mathbf{s}'\rangle$$

where $\forall \mathbf{s} \in \mathbb{F}_q^k$, $\gamma_{\mathbf{s}, \mathbf{s}} = \sqrt{p}$ and each $\|\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\| = 1$. Finally, we are given a random $\mathbf{y} \in \mathbb{Z}_q^n$.

Goal: Find $\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T$, where $\Lambda_{\mathbf{y}}^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{y} \pmod{q}\}$

Execution of the algorithm:

1. First construct the state $\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} |\psi_{\mathbf{s}}\rangle |0\rangle |\mathbf{s}\rangle$ (See Section 4.2).
2. Perform the operation

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} |\psi_{\mathbf{s}}\rangle |0\rangle |\mathbf{s}\rangle \xrightarrow{\textcircled{A}} \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}, \mathbf{s}' \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} \gamma_{\mathbf{s}, \mathbf{s}'} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle |\mathbf{s}'\rangle |\mathbf{s} - \mathbf{s}'\rangle$$

Here, $\textcircled{A}$ is done by applying U on the first two registers and then subtracting the value of the second register in the third register.

3. Measure the third register. If we do not obtain $\mathbf{0}$, start again from step 1. Otherwise, we obtain the state $\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}}\rangle |\mathbf{s}\rangle |\mathbf{0}\rangle$.
4. Discard the third register and apply $U^\dagger$ on the first two registers. The resulting state is

$$|\Phi_{\mathbf{y}}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{p} |\psi_{\mathbf{s}}\rangle |\mathbf{0}\rangle + \omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{1-p} |Z_{\mathbf{s}}\rangle$$

for unit vectors $|Z_{\mathbf{s}}\rangle \perp |\psi_{\mathbf{s}}\rangle |\mathbf{0}\rangle$.

5. We apply a Quantum Fourier Transform on the first register and measure in the computational basis. Output the outcome of the measurement.

First analysis and running time of the algorithm We first provide some details over each step of the algorithm and on the running time. Let

- $\text{Time}_{S|\text{LWE}}$ be the running time to compute U .
- $\text{Time}_{\text{Sampl}}$ be the running time to quantum sample f , *i.e.* to construct the state $\sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{e}\rangle$.

1. The initialization step of the algorithm can be done as follows

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} |\mathbf{s}\rangle \otimes \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{e}\rangle \xrightarrow{\textcircled{1}} \sum_{\substack{\mathbf{s} \in \mathbb{Z}_q^n \\ \mathbf{e} \in \mathbb{Z}_q^m}} f(\mathbf{e}) |\mathbf{s}\rangle |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle = \sum_{\mathbf{s} \in \mathbb{Z}_q^n} |\mathbf{s}\rangle |\psi_{\mathbf{s}}\rangle,$$

which corresponds to the initial state by adding a $|\mathbf{0}\rangle$ register and reordering. In $\textcircled{1}$, we use the fact that $\mathbf{s} \rightarrow \mathbf{A}^\top \mathbf{s}$ is easily computable and apply this operation coherently. We then need to compute $\sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{e}\rangle$ which takes some time $\text{Time}_{\text{Sampl}}$. In practice, f is chosen such that this state can be computed efficiently. The running time of this is therefore in $O(\text{Time}_{\text{Sampl}} + \text{poly}(m, \log(q)))$.

2. In step 3, before the measurement, we have the state

$$\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s}, \mathbf{s}' \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} \gamma_{\mathbf{s}, \mathbf{s}'} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle |\mathbf{s}'\rangle |\mathbf{s} - \mathbf{s}'\rangle =$$

$$\frac{1}{\sqrt{q^n}} \left(\sum_{\mathbf{s}} \omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{p} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}}\rangle |\mathbf{s}\rangle |\mathbf{0}\rangle + \sum_{\mathbf{s}, \mathbf{s}' \neq \mathbf{s}} \omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{1-p} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle |\mathbf{s}'\rangle |\mathbf{s} - \mathbf{s}'\rangle \right).$$

which means that we successfully measure $\mathbf{0}$ in the last register with probability p and that conditioned on this outcome, the resulting state is the following: $\frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}}\rangle |\mathbf{s}\rangle |\mathbf{0}\rangle$. We therefore have to repeat steps 1 to 3 $O(\frac{1}{p})$ times. Moreover, step 2 requires to compute U , which takes time Time_U which is the running time of the $S|\text{LWE}\rangle$ algorithm. From there, we conclude that the time required for this algorithm to successfully pass step 3 is

$$O\left(\frac{1}{p} (\text{Time}_{S|\text{LWE}} + \text{Time}_{\text{Sampl}} + \text{poly}(m, \log(q)))\right).$$

3. In order to obtain $|\phi_{\mathbf{y}}\rangle$ in the end of step 4, we start from $U|\psi_{\mathbf{s}}\rangle|\mathbf{0}\rangle = \sum_{\mathbf{s}' \in \mathbb{Z}_q^n} \gamma_{\mathbf{s}, \mathbf{s}'} |\tilde{\psi}_{\mathbf{s}, \mathbf{s}'}\rangle |\mathbf{s}'\rangle$ which implies

$$\langle \psi_{\mathbf{s}} | \langle \mathbf{0} | \cdot U^\dagger \left(|\tilde{\psi}_{\mathbf{s}, \mathbf{s}}\rangle |\mathbf{s}\rangle \right) = \langle \tilde{\psi}_{\mathbf{s}, \mathbf{s}} | \langle \mathbf{s} | \cdot U(|\psi_{\mathbf{s}}\rangle |\mathbf{0}\rangle) = \gamma_{\mathbf{s}, \mathbf{s}} = \sqrt{p}.$$

This means that for each $\mathbf{s} \in \mathbb{Z}_q^n$, we can indeed write

$$U^\dagger(|\tilde{\psi}_{\mathbf{s}, \mathbf{s}}\rangle |\mathbf{s}\rangle) = \sqrt{p} |\psi_{\mathbf{s}}\rangle |\mathbf{0}\rangle + \sqrt{1-p} |Z_{\mathbf{s}}\rangle,$$

for some unit vector $|Z_{\mathbf{s}}\rangle$ orthogonal to $|\psi_{\mathbf{s}}\rangle |\mathbf{0}\rangle$, which justifies step 4 of the algorithm. Finally, in step 5, we have to perform m quantum Fourier transforms in $\mathbb{Z}_q$ and measure, which takes time $\text{poly}(m, \log(q))$.

From this analysis, we can conclude that the total running time of the algorithm satisfies

$$\text{Time}_{\text{ISIS}} = O\left(\frac{1}{p} (\text{Time}_{S|\text{LWE}} + \text{Time}_{\text{Sampl}} + \text{poly}(m, \log(q)))\right).$$

In particular, if $\text{Time}_{S|\text{LWE}}, \text{Time}_{\text{Sampl}}, \frac{1}{p} = \text{poly}(m, \log(q))$ then $\text{Time}_{\text{ISIS}} = \text{poly}(m, \log(q))$. The trickier part will be to argue about the success probability of the algorithm, which is the goal of the following section.

4.3 Proof of the main theorem

We are ready to prove our main theorem of this section, which we restate below.

Theorem 1. *Let positive integers q, m, n , let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and let $f : \mathbb{Z}_q^n \rightarrow \mathbb{C}$ with $\|f\| = 1$. Let $T \subseteq \mathbb{Z}_q^n$ such that $\text{Im}(f) \subseteq T$. Assume that*

- There exists a quantum algorithm that solves the $S|LWE\rangle(\mathbf{A}, f)$ problem in time $\text{Time}_{S|LWE\rangle}$ and succeeds with probability p .
- $\sum_{\mathbf{x} \in T} |\widehat{f}(\mathbf{x})|^2 = 1 - \eta$.
- f is quantum samplable in time $\text{Time}_{\text{Sampl}}$ i.e. there is a quantum algorithm running in time $\text{Time}_{\text{Sampl}}$ that constructs the state $\sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{e}\rangle$.

Then there exists a quantum algorithm that solves $ISIS(\mathbf{A}, T)$, that succeeds with probability at least $p(1 - \eta) - 2\sqrt{p(1 - p)}\eta$ and runs in time

$$\text{Time}_{ISIS} = O\left(\frac{1}{p} (\text{Time}_{S|LWE\rangle} + \text{Time}_{\text{Sampl}}) + \text{poly}(m, \log(q))\right).$$

Proof. We start from a quantum algorithm for $S|LWE\rangle(\mathbf{A}, f)$ and we consider the algorithm described in Section 4.2. The running time of the algorithm has been discussed in the previous section so we just need to prove the success probability. We fix $\mathbf{y} \in \mathbb{Z}_q^n$, and let p'_y be the probability that the algorithm outputs an element $\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T$ given this $\mathbf{y}$.

Consider the state $|Z_{\mathbf{s}}\rangle$ defined in step 4 of the Algorithm. We write

$$|Z_{\mathbf{s}}\rangle = |Z_{\mathbf{s}}^0\rangle|\mathbf{0}\rangle + \sum_{\mathbf{v} \neq \mathbf{0}} |Z_{\mathbf{s}}^{\mathbf{v}}\rangle|\mathbf{v}\rangle,$$

with in particular $\| |Z_{\mathbf{s}}^0\rangle \| \leq 1$. Recall that $|Z_{\mathbf{s}}\rangle$ is orthogonal to $|\psi_{\mathbf{s}}\rangle|\mathbf{0}\rangle$ which implies that $|Z_{\mathbf{s}}^0\rangle$ is orthogonal to $|\psi_{\mathbf{s}}\rangle$. At step 5 of the algorithm before the final measurement, we have the state

$$|\Omega^{\mathbf{y}}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \left(\omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{p} |\widehat{\psi}_{\mathbf{s}}\rangle |\mathbf{0}\rangle + \omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{1 - p} |\widehat{Z}_{\mathbf{s}}^0\rangle |\mathbf{0}\rangle + \sum_{\mathbf{v} \neq \mathbf{0}} |\widehat{Z}_{\mathbf{s}}^{\mathbf{v}}\rangle |\mathbf{v}\rangle \right)$$

Now, let us define

$$|\Xi_0^{\mathbf{y}}\rangle \triangleq \frac{1}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \left(\omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{p} |\widehat{\psi}_{\mathbf{s}}\rangle + \omega^{-\mathbf{y} \cdot \mathbf{s}} \sqrt{1 - p} |\widehat{Z}_{\mathbf{s}}^0\rangle \right),$$

so that $|\Omega^{\mathbf{y}}\rangle = |\Xi_0^{\mathbf{y}}\rangle|\mathbf{0}\rangle + \sum_{\mathbf{v} \neq \mathbf{0}} |\widehat{Z}_{\mathbf{s}}^{\mathbf{v}}\rangle|\mathbf{v}\rangle$. Since we only measure the first register and we succeed when we have an element of $\Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T$, we have $p'_y \geq \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} |\langle \mathbf{x} | \Xi_0^{\mathbf{y}} \rangle|^2$. We now define the $\{z_{\mathbf{s}, \mathbf{x}}\}$ such that $|\widehat{Z}_{\mathbf{s}}^0\rangle = \sum_{\mathbf{x} \in \mathbb{Z}_q^n} z_{\mathbf{s}, \mathbf{x}} |\mathbf{x}\rangle$, and have the following lemma.

Lemma 1. For each $\mathbf{y} \in \mathbb{Z}_q^n$,

$$p'_y \geq \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} \left| \sqrt{p} \sqrt{q^n} \widehat{f}(\mathbf{x}) + \frac{\sqrt{1 - p}}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{s} \cdot \mathbf{y}} z_{\mathbf{s}, \mathbf{x}} \right|^2.$$

Proof. In order to compute p'_y , we have to compute $|\Xi_0\rangle$. Using Proposition 2, and the identity $\sum_{\mathbf{y}' \in \mathbb{Z}_q^n} \omega^{(\mathbf{y}' - \mathbf{y}) \cdot \mathbf{s}} = 0$ if $\mathbf{y}' \neq \mathbf{y}$, and q^n otherwise, we have

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} |\widehat{\psi}_{\mathbf{s}}\rangle = \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sum_{\mathbf{y}' \in \mathbb{Z}_q^n} \omega^{(\mathbf{y}' - \mathbf{y}) \cdot \mathbf{s}} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}'}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle = q^n \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle.$$

From there, we have

$$|\Xi_0\rangle = \sqrt{q^n p} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x}) |\mathbf{x}\rangle + \sqrt{\frac{1-p}{q^n}} \sum_{\mathbf{x} \in \mathbb{Z}_q^m} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} z_{\mathbf{s}, \mathbf{x}} |\mathbf{x}\rangle.$$

The algorithm computes this state and measures in the computational basis. The probability to output an element of $\Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T$ is therefore

$$p'_y \geq \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} |\langle \mathbf{x} | \Xi_0 \rangle|^2 = \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} \left| \sqrt{q^n p} \widehat{f}(\mathbf{x}) + \sqrt{\frac{1-p}{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} z_{\mathbf{s}, \mathbf{x}} \right|^2.$$

We can now go continue the proof of our theorem. We write

$$\begin{aligned} p'_y &\geq \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} \left| \sqrt{p} \sqrt{q^n} \widehat{f}(\mathbf{x}) + \frac{\sqrt{1-p}}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} z_{\mathbf{s}, \mathbf{x}} \right|^2 \\ &= \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} \left[pq^n |\widehat{f}(\mathbf{x})|^2 + \frac{1-p}{q^n} \left| \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} z_{\mathbf{s}, \mathbf{x}} \right|^2 \right. \\ &\quad \left. + 2Re \left(\sqrt{p} \sqrt{q^n} \widehat{f}(\mathbf{x}) \frac{\sqrt{1-p}}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right) \right] \end{aligned}$$

where we used $|a+b|^2 = (a+b)(\bar{a}+\bar{b}) = |a|^2 + |b|^2 + 2Re(ab)$. We now bound each term separately. We first write

$$\begin{aligned} &\mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} \left[\sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} (pq^n |\widehat{f}(\mathbf{x})|^2) \right] = p(1-\eta) \\ &\forall \mathbf{y} \in \mathbb{Z}_q^n, \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} \left(\frac{1-p}{q^n} \left| \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} z_{\mathbf{s}, \mathbf{x}} \right|^2 \right) \geq 0 \\ &\sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} \left(2Re \left(\sqrt{p} \sqrt{q^n} \widehat{f}(\mathbf{x}) \frac{\sqrt{1-p}}{\sqrt{q^n}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right) \right) = 2\sqrt{p(1-p)} Re \left(\sum_{\substack{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T \\ \mathbf{s} \in \mathbb{Z}_q^n}} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right) \end{aligned}$$

From there, we write

$$\mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} [p'_{\mathbf{y}}] \geq p(1 - \eta) + 2\sqrt{p(1 - p)} \mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} \left[\operatorname{Re} \left(\sum_{\substack{\mathbf{x} \in \Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}) \cap T \\ \mathbf{s} \in \mathbb{Z}_q^n}} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right) \right]$$

In order to conclude, prove the following lemma

Lemma 2.

$$\forall \mathbf{s} \in \mathbb{Z}_q^n, \left| \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) \cap T} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right| \leq \sqrt{\eta}.$$

Proof. We start from the equality $\langle Z_{\mathbf{s}}^0 | \psi_{\mathbf{s}} \rangle = \langle \widehat{Z}_{\mathbf{s}}^0 | \widehat{\psi}_{\mathbf{s}} \rangle = 0$ for each $\mathbf{s} \in \mathbb{Z}_q^n$, which can be rewritten

$$\forall \mathbf{s} \in \mathbb{Z}_q^n, \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})} \omega^{\mathbf{y} \cdot \mathbf{s}} \widehat{f}(\mathbf{y}) \overline{z_{\mathbf{s}, \mathbf{x}}} = 0$$

This implies that for each $\mathbf{s} \in \mathbb{Z}_q^n$,

$$\begin{aligned} \left| \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) \cap T} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right| &= \left| \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) \cap \overline{T}} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right| \\ &= \left| \sum_{\mathbf{x} \in \overline{T}} \widehat{f}(\mathbf{x}) \omega^{\mathbf{A}^{\top} \mathbf{x} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right| \\ &\leq \sqrt{\sum_{\mathbf{x} \in \overline{T}} |\widehat{f}(\mathbf{x}) \omega^{\mathbf{A}^{\top} \mathbf{x} \cdot \mathbf{s}}|^2} \sqrt{\sum_{\mathbf{y} \in \overline{T}} \overline{z_{\mathbf{s}, \mathbf{x}}}} \\ &\leq \sqrt{\eta} \sqrt{1} = \sqrt{\eta}, \end{aligned}$$

where we used the fact that the $|\widehat{Z}_{\mathbf{s}}^0\rangle$ have norm at most 1.

We can now conclude our main proof. We have

$$\begin{aligned} \mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} \left[\operatorname{Re} \left(\sum_{\substack{\mathbf{x} \in \Lambda_{\mathbf{u}}^{\perp}(\mathbf{A}) \cap T \\ \mathbf{s} \in \mathbb{Z}_q^n}} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right) \right] &= \frac{1}{q^n} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \operatorname{re} \left(\sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right) \\ &\geq -\frac{1}{q^n} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \left| \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})} \widehat{f}(\mathbf{x}) \omega^{\mathbf{y} \cdot \mathbf{s}} \overline{z_{\mathbf{s}, \mathbf{x}}} \right| \\ &\geq -\frac{1}{q^n} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \sqrt{\eta} \\ &= -\sqrt{\eta} \end{aligned}$$

Plugging this lower bound in the expression above, we obtain

$$\mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} [p'_\mathbf{y}] \geq p(1 - \eta) - 2\sqrt{p(1 - p)\eta}$$

which concludes the proof.

5 Reverse direction $S|\text{LWE}\rangle \rightarrow IC|\text{LWE}\rangle$

Definition 14. We say that a quantum algorithm for $IC|\text{LWE}\rangle(\mathbf{A}, f)$ has fidelity γ and is clean if it can be described as a unitary such that

$$\forall \mathbf{y} \in \mathbb{Z}_q^n, U|\mathbf{y}\rangle|0\rangle = |\mathbf{y}\rangle|W'_\mathbf{y}\rangle \quad \text{with } \mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} [|\langle W'_\mathbf{y} | W_\mathbf{y} \rangle|] = \gamma,$$

for some unit vectors $|W'_\mathbf{y}\rangle$; where $|W_\mathbf{y}\rangle = \frac{1}{\sqrt{w_\mathbf{y}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{y} \cdot \mathbf{s}} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle$.

Lemma 3. The unitary U that for each $\mathbf{y} \in \mathbb{Z}_q^n$ satisfies $U : |W_\mathbf{y}\rangle|0\rangle \rightarrow |W_\mathbf{y}\rangle|\mathbf{y}\rangle$ is efficiently computable.

Proof. Let $V_\mathbf{A}$ be the quantum unitary satisfying $V_\mathbf{A}|\mathbf{x}\rangle|0\rangle = |\mathbf{x}\rangle|\mathbf{A}\mathbf{x}\rangle$. We perform the following operations, using the expressions of $|\widehat{W}_\mathbf{y}\rangle$ from Proposition 3:

$$|W_\mathbf{y}\rangle|0\rangle \xrightarrow{QFT_{\mathbb{Z}_q^m} \otimes I} q^n \sum_{\mathbf{x} \in \Lambda_\mathbf{y}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x})|\mathbf{x}\rangle|0\rangle \xrightarrow{V_\mathbf{A}} q^n \sum_{\mathbf{x} \in \Lambda_\mathbf{y}^\perp(\mathbf{A})} \widehat{f}(\mathbf{x})|\mathbf{x}\rangle|\mathbf{y}\rangle \xrightarrow{QFT_{\mathbb{Z}_q^m}^\dagger \otimes I} |W_\mathbf{y}\rangle|\mathbf{y}\rangle.$$

We can now prove our main theorem

Theorem 2. Let positive integers q, m, n , a function $f : \mathbb{Z}_q^m \rightarrow \mathbb{C}$ and $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$. If:

- We have a clean (see Definition 14) efficient quantum algorithm that solves $IC|\text{LWE}\rangle(\mathbf{A}, f)$ with fidelity $\gamma = 1 - \varepsilon'$.
- $\mathbb{E}_\mathbf{y} \left[\sqrt{\frac{w_\mathbf{y}}{q^n}} \right] = 1 - \varepsilon$, where $w_\mathbf{y}$ is the normalization factor so that

$$|W_\mathbf{y}\rangle = \frac{1}{\sqrt{w_\mathbf{y}}} \sum_{\mathbf{s} \in \mathbb{Z}_q^n} \omega^{-\mathbf{s} \cdot \mathbf{y}} \sum_{\mathbf{e} \in \mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle \quad \text{is a unit vector.}$$

Then one can construct an efficient quantum algorithm that solves $S|\text{LWE}\rangle(\mathbf{A}, f)$ that succeeds with probability $\left(1 - \varepsilon - \varepsilon' - 2\sqrt{\varepsilon\varepsilon'}\right)^2$.

Proof. We start from an efficient clean quantum algorithm for $IC|\text{LWE}\rangle(\mathbf{A}, f)$. Let U be the efficient unitary such that

$$\forall \mathbf{y} \in \mathbb{Z}_q^n, U|\mathbf{y}\rangle|0\rangle = |\mathbf{y}\rangle|W'_\mathbf{y}\rangle \quad \text{with } \mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} [|\langle W'_\mathbf{y} | W_\mathbf{y} \rangle|] = \gamma = 1 - \varepsilon'.$$

For each $\mathbf{s} \in \mathbb{Z}_q^n$, we define

$$|B_{\mathbf{s}}\rangle = \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{s} \cdot \mathbf{y}} |\widetilde{W}_{\mathbf{y}}\rangle |\mathbf{y}\rangle.$$

The $|B_{\mathbf{s}}\rangle$ are pairwise orthogonal unit vectors. Using U , one can efficiently construct the unitary $|\mathbf{s}\rangle|0\rangle \rightarrow |B_{\mathbf{s}}\rangle$. Indeed, we can write

$$|\mathbf{s}\rangle|0\rangle \xrightarrow{QFT \otimes I} \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} |\mathbf{y}\rangle|0\rangle \xrightarrow{U} \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} |\mathbf{y}\rangle |\widetilde{W}_{\mathbf{y}}\rangle \xrightarrow{SWAP} |B_{\mathbf{s}}\rangle$$

In particular, we can efficiently measure in the basis $|B_{\mathbf{s}}\rangle$. We now present our algorithm for $S[\text{LWE}](\mathbf{A}, f)$.

1. Start from $|\psi_{\mathbf{s}}\rangle = \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sqrt{w_{\mathbf{y}}} |W_{\mathbf{y}}\rangle$ (see Proposition 4), and apply the unitary from Lemma 3 to obtain the state

$$|\psi'_{\mathbf{s}}\rangle = \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sqrt{w_{\mathbf{y}}} |W_{\mathbf{y}}\rangle |\mathbf{y}\rangle.$$

2. Measure this state in the basis $\{|B_{\mathbf{s}}\rangle\}$ and output the result.

The success probability of this algorithm is $\mathbb{E}_{\mathbf{s} \leftarrow \mathbb{Z}_q^n} |\langle \psi'_{\mathbf{s}} | B_{\mathbf{s}} \rangle|^2$. We compute

$$|\langle \psi'_{\mathbf{s}} | B_{\mathbf{s}} \rangle| = \frac{1}{q^n} \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sqrt{w_{\mathbf{y}}} \gamma_{\mathbf{y}} = \mathbb{E}_{\mathbf{y}} \left[\sqrt{\frac{w_{\mathbf{y}}}{q^n}} \gamma_{\mathbf{y}} \right].$$

In order to prove this statement, we define $\varepsilon_{\mathbf{y}} = 1 - \sqrt{\frac{w_{\mathbf{y}}}{q^n}}$ and $\varepsilon'_{\mathbf{y}} = 1 - \gamma_{\mathbf{y}}$. Let us now recap what we know about these variables.

- $\mathbb{E}_{\mathbf{y}} \left[\sqrt{\frac{w_{\mathbf{y}}}{q^n}} \right] = (1 - \varepsilon)$ hence $\mathbb{E}_{\mathbf{y}} [\varepsilon_{\mathbf{y}}] = \varepsilon$.
- $\mathbb{E}_{\mathbf{y}} \left[\frac{w_{\mathbf{y}}}{q^n} \right] = 1$ which can be rewritten $\mathbb{E}_{\mathbf{y}} [(1 - \varepsilon_{\mathbf{y}})^2] = 1$ which implies $\mathbb{E}_{\mathbf{y}} [\varepsilon_{\mathbf{y}}^2] = 2\mathbb{E}_{\mathbf{y}} [\varepsilon_{\mathbf{y}}] = 2\varepsilon$.
- $\mathbb{E}_{\mathbf{y}} [\gamma_{\mathbf{y}}] = \gamma$ so $\mathbb{E}_{\mathbf{y}} [\varepsilon'_{\mathbf{y}}] = \varepsilon'$
- Each $\gamma_{\mathbf{y}} \in [0, 1]$ so each $\varepsilon'_{\mathbf{y}} \in [0, 1]$ and $\mathbb{E}_{\mathbf{y}} [\varepsilon'^2_{\mathbf{y}}] \leq \mathbb{E}_{\mathbf{y}} [\varepsilon'_{\mathbf{y}}] = \varepsilon'$.

We can now compute the success probability of this algorithm. We write

$$|\langle \psi'_{\mathbf{s}} | B_{\mathbf{s}} \rangle| = \mathbb{E}_{\mathbf{y}} \left[\sqrt{\frac{w_{\mathbf{y}}}{q^n}} \gamma_{\mathbf{y}} \right] = \mathbb{E}_{\mathbf{y}} [(1 - \varepsilon_{\mathbf{y}})(1 - \varepsilon'_{\mathbf{y}})] = 1 - \varepsilon - \varepsilon' + \mathbb{E}_{\mathbf{y}} [\varepsilon_{\mathbf{y}} \varepsilon'_{\mathbf{y}}]$$

Now, using the Cauchy-Schwarz inequality, we obtain

$$|\mathbb{E}_{\mathbf{y}} [\varepsilon_{\mathbf{y}} \varepsilon'_{\mathbf{y}}]| \leq \sqrt{\mathbb{E}_{\mathbf{y}} [\varepsilon_{\mathbf{y}}^2]} \sqrt{\mathbb{E}_{\mathbf{y}} [\varepsilon'^2_{\mathbf{y}}]} \leq \sqrt{2\varepsilon\varepsilon'}$$

Plugging this in the above, we obtain that for each $\mathbf{s}$, $|\langle \psi'_{\mathbf{s}} | B_{\mathbf{s}} \rangle| \geq 1 - \varepsilon - \varepsilon' - 2\sqrt{\varepsilon\varepsilon'}$. Since the success probability is $\mathbb{E}_{\mathbf{s}} [|\langle \psi'_{\mathbf{s}} | B_{\mathbf{s}} \rangle|^2]$, we get the desired result.

Remark: The extra register $|0^l\rangle$ is actually a useful softening of the clean condition. In the next section, this will correspond to the randomness register which can be almost perfectly erased.

6 Conditional reverse reduction $IC|LWE\rangle \rightarrow ISIS$

In this last section, we provide another reduction. We show that if we have an algorithm for $ISIS(\mathbf{A}, f)$ which has a specific form then it can be used to solve $S|LWE\rangle(\mathbf{A}, f)$. We start by introducing the definition of a randomness recoverable algorithm. This is a random algorithm whose random tape value can be recovered given the corresponding output.

Definition 15 (Randomness Recoverable Algorithm for ISIS). *Let $\mathcal{A}$ be an algorithm for $ISIS(\mathbf{A}, T)$, and denote by $\mathcal{A}(\mathbf{y}; r)$ the output of $\mathcal{A}$ on input $\mathbf{y}$ using random tape $r \in \{0, 1\}^\ell$. $\mathcal{A}$ is said to be perfectly randomness recoverable if there is an algorithm $\mathcal{R}$ satisfying*

$$\forall r \in \{0, 1\}^\ell, \forall \mathbf{y} \in \mathbb{Z}_q^n, \mathcal{R}(\mathbf{y}, \mathcal{A}(\mathbf{y}; r)) = r.$$

Theorem 3. *Let $\mathcal{A}$ be an algorithm for $ISIS(\mathbf{A}, T)$ with time complexity t . Assume the following properties:*

- $\mathcal{A}$ is perfectly randomness recoverable;
- $\mathcal{A}$ is ε -close to being solution-uniform i.e. if we define $p_y(x) = \Pr_{\mathbf{r} \leftarrow \{0, 1\}^\ell} (\mathcal{A}(\mathbf{y}, \mathbf{r}) = \mathbf{x})$, we have

$$\Delta(p_{\mathbf{y}}, u_{\mathbf{y}}) = \varepsilon_{\mathbf{y}} \quad \text{and} \quad \mathbb{E}_{\mathbf{y} \leftarrow \mathbb{Z}_q^n} [\varepsilon_{\mathbf{y}}] = \varepsilon,$$

where $\Delta(p_{\mathbf{y}}, u_{\mathbf{y}})$ is the statistical distance between the distribution p_y and the probability function $u_{\mathbf{y}} = \frac{1}{|T \cap \Lambda_{\mathbf{y}}^\perp(\mathbf{A})|} \mathbb{1}_{T \cap \Lambda_{\mathbf{y}}^\perp(\mathbf{A})}$.

Then there exists an efficient algorithm solving $IC|LWE\rangle(\mathbf{A}, f)$ with $\hat{f} = \mathbb{1}_T$ with fidelity $1 - \varepsilon$ and time complexity $\text{poly}(t)$.

Remark: We don't explicitly say anything about the success probability of the algorithm $\mathcal{A}$. However, the fact that it is ε -close to being solution-uniform implies that with a uniformly random choice of randomness r , the algorithm outputs a valid solution (i.e. $\in T \cap \Lambda_{\mathbf{y}}^\perp(\mathbf{A})$) with probability at least $1 - \varepsilon$ on average on $\mathbf{y}$.

Proof. We show that there is an efficient process mapping $|\mathbf{y}\rangle|0\rangle$ to $|\mathbf{y}\rangle|W_{\mathbf{y}}\rangle$ for all $\mathbf{y} \in \mathbb{Z}_q^n$. Start with $|y\rangle$ as first register, then prepare a uniform superposition of $r \in \{0, 1\}^\ell$ in the second register:

$$\frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \sum_{r \in \{0, 1\}^\ell} |r\rangle$$

Apply $\mathcal{A}$ in superposition over the first and second registers and store the result in a third register:

$$\frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \sum_{r \in \{0, 1\}^\ell} |r\rangle |\mathcal{A}(\mathbf{y}; r)\rangle$$

From $\mathcal{R}$, we have access to the quantum unitary $U_{\mathcal{R}}$ mapping $|\mathbf{y}\rangle|\mathcal{A}(\mathbf{y}; r)\rangle|0\rangle$ to $|\mathbf{y}\rangle|\mathcal{A}(\mathbf{y}; r)\rangle|r\rangle$ for any $r \in \{0, 1\}^l$. We then perform the following operations.

$$\begin{aligned}
& \frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \sum_{r \in \{0, 1\}^\ell} |r\rangle |\mathcal{A}(\mathbf{y}; r)\rangle \xrightarrow{SWAP} \frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \sum_{r \in \{0, 1\}^\ell} |\mathcal{A}(\mathbf{y}; r)\rangle |r\rangle \\
& \xrightarrow{U_{\mathcal{R}}^\dagger} \frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \sum_{r \in \{0, 1\}^\ell} |\mathcal{A}(\mathbf{y}; r)\rangle |0\rangle \\
& \xrightarrow{\text{discard}} \frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \sum_{r \in \{0, 1\}^\ell} |\mathcal{A}(\mathbf{y}; r)\rangle \\
& \xrightarrow{\text{inverse QFT}} \frac{1}{\sqrt{2^\ell}} |\mathbf{y}\rangle \otimes \text{QFT}_{\mathbb{Z}_q^n}^{-1} \left(\sum_{r \in \{0, 1\}^\ell} |\mathcal{A}(\mathbf{y}; r)\rangle \right)
\end{aligned}$$

For this final step, one has to be careful because we do not necessarily restrict the outputs of $\mathcal{A}(\mathbf{y}; r)$ to elements of $\mathbb{Z}_q^n$. For example, we will consider algorithms which sometimes outputs Abort. We extend the operation $\text{QFT}_{\mathbb{Z}_q^n}^{-1}$ so that it applies the identity to elements outside of $\mathbb{Z}_q^n$.

Let $|W'_{\mathbf{y}}\rangle = \frac{1}{\sqrt{2^\ell}} \text{QFT}_{\mathbb{Z}_q^n}^{-1} \left(\sum_{r \in \{0, 1\}^\ell} |\mathcal{A}(\mathbf{y}; r)\rangle \right)$. In order to show that we have a quantum algorithm that solves $IC|LWE\rangle(\mathbf{A}, f)$ with fidelity $1 - \varepsilon$, we need to compute the inner products $|\langle W_{\mathbf{y}} | W'_{\mathbf{y}} \rangle| = |\langle \widehat{W}_{\mathbf{y}} | \widehat{W}'_{\mathbf{y}} \rangle|$. Since we have $\widehat{f} \sim \mathbb{1}_T$, we know that

$$\begin{aligned}
|\widehat{W}_{\mathbf{y}}\rangle &= \frac{1}{\sqrt{|\Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T|}} \sum_{\mathbf{x} \in \Lambda_{\mathbf{y}}^\perp(\mathbf{A}) \cap T} |\mathbf{x}\rangle \\
|\widehat{W}'_{\mathbf{y}}\rangle &= \frac{1}{\sqrt{2^\ell}} \sum_{r \in \{0, 1\}^\ell} |\mathcal{A}(\mathbf{y}; r)\rangle
\end{aligned}$$

We then obtain

$$|\langle \widehat{W}_{\mathbf{y}} | \widehat{W}'_{\mathbf{y}} \rangle| = \sum_{\mathbf{x}} \sqrt{p_{\mathbf{y}}(\mathbf{x}) u_{\mathbf{y}}(\mathbf{x})} = F(p_{\mathbf{y}}, u_{\mathbf{y}}),$$

Where F is the fidelity between the two probability functions. By the Fuchs-van de Graaf inequality [FvdG99], we have $F(p_{\mathbf{y}}, u_{\mathbf{y}}) \geq 1 - \Delta(p_{\mathbf{y}}, u_{\mathbf{y}}) = 1 - \varepsilon_{\mathbf{y}}$. From there, we can conclude that this algorithm solves $IC|LWE\rangle(\mathbf{A}, \mathbb{1}_T)$ with fidelity at least $\mathbb{E}_{\mathbf{y}} [1 - \varepsilon_{\mathbf{y}}] = 1 - \varepsilon$.

7 Specific instantiation of the reverse reduction

We first recall one of the results of [BJK⁺25].

Proposition 8. *For some parameters $n, m, q = 2^l$ with $q = \text{poly}(n)$ and $m = 2^{O(\log(n) \log(q))}$, there exists an algorithm for $S|LWE\rangle(\mathbf{A}, f)$ in the case $\mathbf{A}$ is randomly chosen in $\mathbb{Z}_q^{n \times m}$ and f is the function such that $\widehat{f} = \mathbb{1}_{\mathbb{Z}_2^m}$.*

In this section, we show how to recover the above proposition using our reverse reduction. We tweak this classical algorithm by Regev to make it randomness recoverable. We will use natural notations for merging matrices. $(\mathbf{A}|\mathbf{B})$ will corresponds to the matrix $\mathbf{B}$ added to right of matrix $\mathbf{A}$ and $\begin{pmatrix} \mathbf{A} \\ \mathbf{B} \end{pmatrix}$ will corresponds to the matrix $\mathbf{B}$ added at the bottom of matrix $\mathbf{A}$. For the case of vectors, since we are using column vectors, the notation $(\mathbf{x}||\mathbf{y})$ for vectors $\mathbf{x}, \mathbf{y}$ will actually corresponds to the vector $\begin{pmatrix} \mathbf{x} \\ \mathbf{y} \end{pmatrix}$. We can now describe our algorithm.

Algorithm 2: ISIS Solver $\mathcal{A}_1$

Parameters: Positive integers l, n . Fix $q = 2^l$ and $m = (2n + 1)^l$.

Inputs: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{y} \in \mathbb{Z}_q^n$.

Output: $\mathbf{x}_F \in \mathbb{Z}_2^m$ such that $\mathbf{A}\mathbf{x}_F = \mathbf{y}$, where the operations are in $\mathbb{Z}_q$.

Execution of the algorithm:

1. If $l = 1$, output a solution $\mathbf{x}_F$ using $n + 1$ bits of randomness and procedure (P2). Otherwise:
2. **Sample $\mathbf{y}$'s shares:** Let $m' = \frac{m}{2n+1} = (2n+1)^{l-1}$. Sample $\mathbf{y}_1, \dots, \mathbf{y}_{m'}$ each from $\mathbb{Z}_2^n$ such that $\sum_{i=1}^{m'} \mathbf{y}_i = (\mathbf{y} \bmod 2)$. To do this, sample random strings $\mathbf{y}_1, \dots, \mathbf{y}_{m'-1} \in \mathbb{Z}_2^n$ and choose $\mathbf{y}_{m'}$ according to the above equality.
3. **Build matrix blocks:** Let $\mathbf{A}_1, \dots, \mathbf{A}_{m'}$ be the matrices in $\mathbb{Z}_2^{n \times (2n+1)}$ such that $\mathbf{A} = [\mathbf{A}_1 | \dots | \mathbf{A}_{m'}] \bmod 2$. If there exists $i \in \llbracket 1, m' \rrbracket$ such that $\mathbf{A}_i$ is not of full rank, Abort.
4. **Extend matrices $\mathbf{A}_i$ to full rank matrices** $\in \mathbb{Z}_2^{2n \times (2n+1)}$. We extend each matrix $\mathbf{A}_i$ into a matrix $\tilde{\mathbf{A}}_i \in \mathbb{Z}_2^{2n \times (2n+1)}$ using the deterministic procedure (P1) described below.
5. **Find solutions for each block:** For all $i \in \llbracket 1, m' \rrbracket$, sample $\mathbf{u}_i \leftarrow \mathbb{Z}_2^n$ and let $\mathbf{t}_i = (\mathbf{y}_i || \mathbf{u}_i)$. Let $\mathbf{x}_i^{(1)}$ and $\mathbf{x}_i^{(2)}$ be the two vectors in $\mathbb{Z}_2^{2n+1}$ such that $\tilde{\mathbf{A}}_i \mathbf{x}_i^{(1)} = \tilde{\mathbf{A}}_i \mathbf{x}_i^{(2)} = \mathbf{u}_i \bmod 2$. This implies in particular $\mathbf{A}_i \mathbf{x}_i^{(1)} = \mathbf{A}_i \mathbf{x}_i^{(2)} = \mathbf{y}_i \bmod 2$.
6. **Merge block solutions:** We order these solutions such that $\mathbf{x}_i^{(1)} \preccurlyeq \mathbf{x}_i^{(2)}$ in lexicographical order. For each $\mathbf{i} \in \llbracket 1, m' \rrbracket$, we define $\mathbf{x}_i = \mathbf{x}_i^{(1)}$ and $\mathbf{z}_i = \mathbf{x}_i^{(2)} - \mathbf{x}_i^{(1)} \bmod 2$. Let $\mathbf{x} \triangleq [\mathbf{x}_1 || \dots || \mathbf{x}_{m'}] \in \mathbb{Z}_2^m$, and $\mathbf{Z} \in \mathbb{Z}_2^{m \times m'}$ defined as follows:

$$\mathbf{Z} \triangleq \begin{bmatrix} \mathbf{z}_1 & & & \\ & \mathbf{z}_2 & & \\ & & \ddots & \\ & & & \mathbf{z}_{m'} \end{bmatrix}$$

where the empty spots are zeroes.

7. **Recursion:** Let $\mathbf{y}' = \frac{\mathbf{y} - \mathbf{A}\mathbf{x}}{2} \in \mathbb{Z}_{q/2}^n$ and $\mathbf{A}' = \frac{\mathbf{A}\mathbf{Z}}{2} \in \mathbb{Z}_{q/2}^{n \times m'}$. Use the algorithm $\mathcal{A}_1$ with parameters $(l-1), n$ on input $\mathbf{A}', \mathbf{y}'$, to obtain $\mathbf{x}' \in \mathbb{Z}_2^{m'}$ such that $\mathbf{A}'\mathbf{x}' = \mathbf{y}' \pmod{2}$.
8. **Return** $\mathbf{x}_F = \mathbf{x} + \mathbf{Z}\mathbf{x}' \pmod{q}$.

Procedures (P1) and (P2) are presented on the next page. In the above algorithm, the randomness is generated on the fly. We show in Proposition 11 that the amount of randomness used in the algorithm is $m - nl$ when the algorithm doesn't abort. We now reformulate the above algorithm in terms of an algorithm that has its randomness as part of the input.

Algorithm 3: ISIS Solver $\mathcal{A}$

Inputs: $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, $\mathbf{y} \in \mathbb{Z}_q^n$, $\mathbf{r} \in \{0, 1\}^{m-nl}$.

Execution of the algorithm: run $\mathcal{A}_1(\mathbf{A}, \mathbf{y})$ above. When some random bits are chosen in $\mathcal{A}_1$ take the next available bits in $\mathbf{r}$. If at some point, algorithm $\mathcal{A}_1$ aborts, output $(\perp, \mathbf{r})$. Otherwise, output what $\mathcal{A}_1$ outputs.

An advantage with this formulation is that when the algorithm aborts, we also output the randomness. This will ensure that the algorithm is perfectly randomness recoverable, even when it aborts.

Procedure (P1). Extending a full rank matrix in $\mathbb{Z}_2^{n \times (2n+1)}$ to a full rank matrix in $\mathbb{Z}_2^{2n \times (2n+1)}$ deterministically

Input: $\mathbf{A} \in \mathbb{Z}_2^{n \times (2n+1)}$ of full rank n

Output: $\tilde{\mathbf{A}} \in \mathbb{Z}_2^{2n \times (2n+1)}$ of full rank $2n$

- 1: Let $\mathbf{e}_i^\top$ be the row vector in $\mathbb{Z}_2^{2n+1}$ with a 1 at position i and 0 elsewhere
 - 2: $\tilde{\mathbf{A}} \leftarrow \mathbf{A}$
 - 3: $i \leftarrow 0$
 - 4: **while** $\text{rank}(\tilde{\mathbf{A}}) < 2n$ **do**
 - 5: $\tilde{\mathbf{A}}' = \begin{bmatrix} \tilde{\mathbf{A}} \\ \mathbf{e}_i^\top \end{bmatrix}$ $\triangleright$ Append row $\mathbf{e}_i^\top$ to $\tilde{\mathbf{A}}$
 - 6: **if** $\text{rank}(\tilde{\mathbf{A}}') > \text{rank}(\tilde{\mathbf{A}})$ **then**
 - 7: $\tilde{\mathbf{A}} \leftarrow \tilde{\mathbf{A}}'$
 - 8: **end if**
 - 9: $i \leftarrow i + 1$
 - 10: **end while**
 - 11: **return** $\tilde{\mathbf{A}}$
-

Procedure (P2).

Input: $\mathbf{A} \in \mathbb{Z}_2^{n \times (2n+1)}$ of full rank n , a vector $\mathbf{y} \in \mathbb{Z}_2^n$.

Output: $\mathbf{x}_F \in \mathbb{Z}_2^{2n+1}$ such that $\mathbf{A}\mathbf{x}_F = \mathbf{y}$.

- 1: Construct deterministically a matrix $\mathbf{B} \in \mathbb{Z}_2^{(n+1) \times (2n+1)}$ such that $\begin{bmatrix} \mathbf{A} \\ \mathbf{B} \end{bmatrix}$ is of full rank $2n+1$. This can be done by adapting Procedure (P1) to the case where we want a matrix of rank $(2n+1)$ instead of $2n$.
- 2: Choose a random string $\mathbf{u} \in \mathbb{F}_2^{n+1}$.
- 3: With Gaussian elimination, find the unique vector $\mathbf{x}_F \in \mathbb{F}_2^{2n+1}$ such that

$$\begin{bmatrix} \mathbf{A} \\ \mathbf{B} \end{bmatrix} \mathbf{x}_F = \begin{pmatrix} \mathbf{y} \\ \mathbf{u} \end{pmatrix}.$$

- 4: **return** $\mathbf{x}_F$.
-

We now prove several properties of our algorithm $\mathcal{A}_1$ which will help us showing that the above algorithm $\mathcal{A}$ is perfectly randomness recoverable and ε -solution-uniform with $\varepsilon = \text{negl}(n)$.

Proposition 9. *If Algorithm $\mathcal{A}_1$ does not abort, then it always outputs a valid solution.*

Proof. We prove the result by induction on l . If $l = 1$, this is clear from Procedure (P2). We now prove the result for general l . Let $\mathbf{x}_F = \mathbf{x} + \mathbf{Z}\mathbf{x}'$ be a solution that the algorithm outputs. By induction, we have that $\mathbf{A}'\mathbf{x}' = \mathbf{y}'$.

We first show that $\mathbf{x}_F \in \mathbb{Z}_2^m$. Writing $\mathbf{x}' = (x'_1, \dots, x'_{m'})$ where each $x'_i \in \mathbb{Z}_2$, it comes

$$\mathbf{x}_F = (\mathbf{x}_1 + x'_1 \mathbf{z}_1 \parallel \mathbf{x}_2 + x'_2 \mathbf{z}_2 \parallel \dots \parallel \mathbf{x}_{m'} + x'_{m'} \mathbf{z}_{m'}).$$

Each $\mathbf{x}_i = \mathbf{x}_i^{(1)}$ and $\mathbf{x}_i + \mathbf{z}_i = \mathbf{x}_i^{(2)} \in \mathbb{Z}_2^{2n+1}$. Since each $x'_i \in \mathbb{Z}_2$, we conclude that each $\mathbf{x}_i + x'_i \mathbf{z}_i \in \mathbb{Z}_2^{2n+1}$ and $\mathbf{x}_F \in \mathbb{Z}_2^m$. Regarding the linear constraint, we write

$$\mathbf{A}\mathbf{x}_F = \mathbf{A}\mathbf{x} + \mathbf{A}\mathbf{Z}\mathbf{x}' = \mathbf{A}\mathbf{x} + 2\mathbf{A}'\mathbf{x}' = \mathbf{A}\mathbf{x} + 2\mathbf{y}' = \mathbf{A}\mathbf{x} + (\mathbf{y} - \mathbf{A}\mathbf{x}) = \mathbf{y}.$$

Proposition 10. *For a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, Algorithm $\mathcal{A}_1$ aborts with probability $\text{negl}(n)$.*

Proof. The above algorithm aborts if one the matrices $\mathbf{A}_i \in \mathbb{Z}_2^{n \times (2n+1)}$ is not of full rank n . Since these matrices are randomly chosen, this happens with probability at most $2^{-\Theta(n)} = \text{negl}(n)$ for each matrix. Then, by a union bound, the probability that this happens for a matrix is $m \cdot 2^{-\Theta(n)} = \text{negl}(n)$ since we consider $q = \text{poly}(n)$ and $m = 2^{O(\log(n) \log(q))}$. When the rank conditions are satisfied, each $\tilde{\mathbf{A}}_i \in \mathbb{Z}_2^{2n \times (2n+1)}$ is exactly of rank $2n$ so there will be exactly two (different) solutions $\mathbf{x}_i^{(1)}$ and $\mathbf{x}_i^{(2)}$ at step 5 and the algorithm succeeds.

Finally, we have to argue about the recursive steps. We have $\mathbf{A}' = \frac{\mathbf{A}\mathbf{Z}}{2}$, where the $\mathbf{z}_i$ are randomly chosen such that in particular $\mathbf{A}\mathbf{Z} \bmod 2 = \mathbf{0}$. Using the

fact that the $\mathbf{A}_i$ are random matrices, the matrices $\mathbf{A}' \in \mathbb{F}_2^{n \times m'}$ will also behave as random matrices hence the algorithm will abort with negligible probability in the subproblem as well.

Proposition 11. *Algorithm $\mathcal{A}_1$ requires $m - \ln$ bits of randomness.*

Proof. Fix a parameter n and let R_l be the number of bits of randomness used in the algorithm that depends on the parameter l . First, we have $R_1 = n + 1$ from Procedure (P2).

In the case $l > 1$, we look at the randomness required at each step. Step 2 requires $n(m' - 1)$ bits of randomness as we need to randomly generate $\mathbf{y}_1, \dots, \mathbf{y}_{m'-1}$ and then compute $\mathbf{y}_{m'}$ from these values and $\mathbf{y}$. Step 4 requires sampling the $\mathbf{u}_i$ which requires nm' bits of randomness. Finally, we need to generate the randomness related to the instance with parameters n and $l - 1$. Therefore, we have

$$\forall l \geq 2, R_l = n(2m' - 1) + R_{l-1} \quad \text{and} \quad R_1 = n + 1.$$

We can therefore write $R_l - R_{l-1} = n(2(2n + 1)^{l-1} - 1)$ when $l \geq 2$. Solving this recurrence, we obtain

$$\begin{aligned} R_l &= 2n \sum_{i=1}^{l-1} (2n + 1)^i - n(l - 1) + R_1 \\ &= 2n \frac{(2n + 1)^l - (2n + 1)}{(2n + 1) - 1} - n(l - 1) + (n + 1) \\ &= (2n + 1)^l - (2n + 1) + (2n + 1) - \ln \\ &= (2n + 1)^l - \ln, \end{aligned}$$

which concludes the proof using $m = (2n + 1)^l$.

Proposition 12. *Two different choices of randomness give two different solutions in $\mathcal{A}$*

Proof. If the two choices of randomness r and r' correspond to an abort outcome, then the outcomes in $\mathcal{A}$ are respectively $(\perp, r)$ and $(\perp, r')$ which are different.

Consider a run of the algorithm with these two different random strings in the case there are no aborts. If the randomness differs in the choice of the shares $\mathbf{y}_i$ or of the $\mathbf{u}_i$, then there is a different $\mathbf{t}_i = (\mathbf{y}_i, \mathbf{u}_i)$. Notice that for each $i \in \llbracket 1, m' \rrbracket$, $\tilde{\mathbf{A}}_i \mathbf{z}_i = \mathbf{0}$. If we write $\tilde{\mathbf{A}} = [\tilde{\mathbf{A}}_1 \parallel \dots \parallel \tilde{\mathbf{A}}_{m'}]$, then this implies that $\tilde{\mathbf{A}} \mathbf{Z} = [\mathbf{0}]$.

From there, we obtain that

$$(\tilde{\mathbf{A}}_i (\mathbf{x}_F)_i \mod 2) = (\tilde{\mathbf{A}}_i \mathbf{x}_i) = \begin{pmatrix} \mathbf{y}_i \\ \mathbf{u}_i \end{pmatrix},$$

which implies that a difference in $\mathbf{y}_i$ or $\mathbf{u}_i$ leads to a different solution $\mathbf{x}_F$.

The other possibility is that the randomness is the same at this level but the randomness differs for the subproblem. We apply recursively the same argument and for final case $l = 1$, two different choices of randomness $\mathbf{u}$ immediately give different solutions $\mathbf{x}_F$ (see Procedure (P2)).

Proposition 13. *Algorithm $\mathcal{A}$ is perfectly randomness recoverable.*

Proof. We start from input $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{y} \in \mathbb{Z}_q^n$ as well as a solution $\mathbf{x}_F \in \mathbb{Z}_q^m$. If $m = (2n + 1)$ and $q = 2$ (which corresponds to $l = 1$), we can recover the $n + 1$ bits of randomness by computing

$$\begin{bmatrix} \mathbf{A} \\ \mathbf{B} \end{bmatrix} \mathbf{x}_F = \begin{pmatrix} \mathbf{y} \\ \mathbf{u} \end{pmatrix},$$

where $\mathbf{B}$ is the matrix constructed in procedure (P2) and $\mathbf{u} = u_1, \dots, u_{n+1}$ are the random bits we extract.

We now consider the main case. As in the algorithm, we construct the matrices $\tilde{\mathbf{A}}_i$. We know that

$$(\tilde{\mathbf{A}}_i \mathbf{x}_F \mod 2) = (\tilde{\mathbf{A}}_i \mathbf{x}) = \begin{pmatrix} \mathbf{y}_i \\ \mathbf{u}_i \end{pmatrix},$$

which means we can recover all the $\mathbf{y}_i$ and $\mathbf{u}_i$. Recall that the $\mathbf{y}_1, \dots, \mathbf{y}_{m'-1} \in \mathbb{Z}_2^n$ correspond to the randomness and then $\mathbf{y}_{m'} = \mathbf{y} \mod 2 - \sum_{i=1}^{m'-1} \mathbf{y}_i$. On the other hand, all the $\mathbf{u}_i \in \mathbb{Z}_2^n$ are chosen uniformly at random. This corresponds therefore to $(m' - 1)n + m'n = 2m'n - n$ bits of randomness.

From these random values $\mathbf{y}_i$ and $\mathbf{u}_i$, we can perform steps 5 and 6 of the protocol to construct all the $\mathbf{x}_i$ and $\mathbf{z}_i$. From there, we can recreate the instance $(\mathbf{A}', \mathbf{y}')$ as well as the string $\mathbf{Z}\mathbf{x}' = \mathbf{x}_F - \mathbf{A}\mathbf{x}$. Finally, since each $\mathbf{z}_i$ is never the $\mathbf{0}$ vector (because the two solutions $\mathbf{x}_i^{(1)}$ and $\mathbf{x}_i^{(2)}$ are always distinct), one can always perfectly $\mathbf{x}'$ from $\mathbf{Z}\mathbf{x}'$. With access to the new instance $(\mathbf{A}', \mathbf{y}')$ as well as the solutions $\mathbf{x}'$, we can apply our randomness recovering algorithm recursively to conclude.

The randomness recovering algorithm succeeds when all the iterations of the algorithm succeed *i.e.* there is no abort. On the other hand, if we start from an output $(\perp, r)$ then one can trivially recover the randomness r . We therefore have that the algorithm succeeds wp. 1.

Proposition 14. *Algorithm $\mathcal{A}$ is ε -close to being solution-uniform with $\varepsilon = \text{negl}(n)$.*

Proof. This can be seen as a direct consequence of our randomness recoverable algorithm $\mathcal{R}$. If we apply this algorithm on a random solution $\mathbf{x}_F \in \mathbb{Z}_2^m \cap \Lambda_{\mathbf{y}}^\perp(\mathbf{A})$, then the same analysis shows that it aborts only with negligible probability. But because we always have $\mathcal{A}(\mathbf{y}, r) \neq \mathcal{A}(\mathbf{y}, r')$ when $r \neq r'$, we have that the set $\{\mathcal{A}(\mathbf{y}, r)\}$ hits a $1 - \text{negl}(n)$ fraction of the solution set $\mathbb{Z}_2^m \cap \Lambda_{\mathbf{y}}^\perp(\mathbf{A})$ which gives the result.

Putting everything together. From Propositions 13 and 14, we have that algorithm $\mathcal{A}$ is perfectly randomness recoverable and is ε solution-uniform with $\varepsilon = \text{negl}(n)$. Moreover, this algorithm runs in time $O(m) = 2^{O(\log(n) \log(q))}$. By applying Theorem 3 and then Theorem 2 we recover Proposition 1.

References

- BJK⁺25. Shi Bai, Hansraj Jangir, Elena Kirshanova, Tran Ngo, and William Youmans. A quasi-polynomial time algorithm for the extrapolated dihedral coset problem over power-of-two moduli. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 416–448, Cham, 2025. Springer Nature Switzerland.
- BKMH97. Masahi Ban, Keiko Kurokawa, Rei Momose, and Osamu Hirota. Optimum measurements for discrimination among symmetric quantum states and parameter estimation. *International Journal of Theoretical Physics*, 36(6):1269–1288, 1997.
- BKSW18. Zvika Brakerski, Elena Kirshanova, Damien Stehlé, and Weiqiang Wen. Learning with errors and extrapolated dihedral cosets. In *Public-Key Cryptography – PKC 2018*, volume 10770 of *Lecture Notes in Computer Science*, pages 702–727. Springer, 2018.
- BN18. Xavier Bonnetain and María Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 560–592, Cham, 2018. Springer International Publishing.
- CHL⁺25. Yilei Chen, Zihan Hu, Qipeng Liu, Han Luo, and Yaxin Tu. Lwe with quantum amplitudes: Algorithm, hardness, and oblivious sampling. In Yael Tauman Kalai and Seny F. Kamara, editors, *Advances in Cryptology – CRYPTO 2025*, pages 513–544, Cham, 2025. Springer Nature Switzerland.
- CLZ22. Yilei Chen, Qipeng Liu, and Mark Zhandry. Quantum algorithms for variants of average-case lattice problems via filtering. In Orr Dunkelman and Stefan Dziembowski, editors, *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III*, volume 13277 of *LNCS*, pages 372–401. Springer, 2022.
- CT24. André Chailloux and Jean-Pierre Tillich. The quantum decoding problem. In *Theory of Quantum Computation, Communication and Cryptography, TQC 2024, September 9-13, 2024, Okinawa, Japan*, volume 310 of *LIPIcs*, pages 6:1–6:14, 2024.
- CT25. André Chailloux and Jean-Pierre Tillich. Quantum advantage from soft decoders. In *Proceedings of the 57th Annual ACM Symposium on Theory of Computing*, STOC ’25, page 738–749, New York, NY, USA, 2025. Association for Computing Machinery.
- DFS24. Thomas Debris-Alazard, Pouria Fallahpour, and Damien Stehlé. Quantum oblivious LWE sampling and insecurity of standard model lattice-based snarks. In Bojan Mohar, Igor Shinkar, and Ryan O’Donnell, editors, *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pages 423–434. ACM, 2024.
- DRT23. Thomas Debris-Alazard, Maxime Rémard, and Jean-Pierre Tillich. Quantum reduction of finding short code vectors to the decoding problem. *IEEE Trans. Inform. Theory*, November 2023. in press, see also arXiv:2106.02747 (v2).
- FvdG99. C.A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.

- JSW⁺24. Stephen P. Jordan, Noah Shutty, Mary Wootters, Adam Zalcman, Alexander Schmidhuber, Robbie King, Sergei V. Isakov, and Ryan Babbush. Optimization by decoded quantum interferometry, 2024.
- Kup13. Greg Kuperberg. Another Subexponential-time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. In Simone Severini and Fernando Brandao, editors, *8th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2013)*, volume 22 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20–34, Dagstuhl, Germany, 2013. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.
- Reg05. Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing*, STOC '05, page 84–93, New York, NY, USA, 2005. Association for Computing Machinery.
- SSTX09. Damien Stehlé, Ron Steinfeld, Keisuke Tanaka, and Keita Xagawa. Efficient public key encryption based on ideal lattices. In Mitsuru Matsui, editor, *Advances in Cryptology – ASIACRYPT 2009*, pages 617–635, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.
- YZ24. Takashi Yamakawa and Mark Zhandry. Verifiable quantum advantage without structure. *J. ACM*, 71(3):20, 2024.

A Tractability of $S|LWE\rangle$

We essentially reproduce (with elements in $\mathbb{Z}_q$ instead of $\mathbb{F}_q$), the argument of [CT24]. We consider the set of states $\{|\widehat{\psi}_{\mathbf{s}}\rangle\}_{\mathbf{s} \in \mathbb{Z}_q^n}$ with $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e} \in \mathbb{Z}_q^n} f(\mathbf{e}) |\mathbf{A}^\top \mathbf{s} + \mathbf{e}\rangle$. The associated *Pretty Good Measurement* is the POVM $\{M_{\mathbf{s}}\}$ with

$$M_{\mathbf{s}} = \rho^{-1/2} |\widehat{\psi}_{\mathbf{s}}\rangle \langle \widehat{\psi}_{\mathbf{s}}| \rho^{-1/2}, \quad \text{with } \rho = \sum_{\mathbf{s}} |\widehat{\psi}_{\mathbf{s}}\rangle \langle \widehat{\psi}_{\mathbf{s}}|.$$

From Proposition 4, we have that $|\psi_{\mathbf{s}}\rangle = \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sqrt{w_{\mathbf{y}}} |W_{\mathbf{y}}\rangle$, from which we can write

$$|\psi_{\mathbf{s}}\rangle \langle \psi_{\mathbf{s}}| = \frac{1}{q^{2n}} \sum_{\mathbf{y}, \mathbf{y}' \in \mathbb{Z}_q^n} \sqrt{w_{\mathbf{y}} w_{\mathbf{y}'}} \omega^{\mathbf{s} \cdot (\mathbf{y} - \mathbf{y}')} |W_{\mathbf{y}}\rangle \langle W_{\mathbf{y}}|$$

and

$$\begin{aligned} \rho &= \sum_{\mathbf{s}} |\psi_{\mathbf{s}}\rangle \langle \psi_{\mathbf{s}}| \\ &= \frac{1}{q^{2n}} \sum_{\mathbf{y}, \mathbf{y}' \in \mathbb{Z}_q^n} \sqrt{w_{\mathbf{y}} w_{\mathbf{y}'}} \sum_{\mathbf{s}} \omega^{\mathbf{s} \cdot (\mathbf{y} - \mathbf{y}')} |W_{\mathbf{y}}\rangle \langle W_{\mathbf{y}'}| \\ &= \frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} w_{\mathbf{y}} |W_{\mathbf{y}}\rangle \langle W_{\mathbf{y}}| \end{aligned}$$

Since the $|W_{\mathbf{y}}\rangle$ are pairwise orthogonal and of norm 1, we have $\rho^{-1/2} = \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sqrt{\frac{q^n}{w_{\mathbf{y}}}} |W_{\mathbf{y}}\rangle \langle W_{\mathbf{y}}|$. Now, we write

$$\begin{aligned} \rho^{-1/2} \cdot |\widehat{\psi}_{\mathbf{s}}\rangle &= \left(\sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sqrt{\frac{q^n}{w_{\mathbf{y}}}} |W_{\mathbf{y}}\rangle \langle W_{\mathbf{y}}| \right) \cdot \left(\frac{1}{q^n} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} \sqrt{w_{\mathbf{y}}} |W_{\mathbf{y}}\rangle \right) \\ &= \frac{1}{\sqrt{q^n}} \sum_{\mathbf{y} \in \mathbb{Z}_q^n} \omega^{\mathbf{y} \cdot \mathbf{s}} |W_{\mathbf{y}}\rangle \triangleq |Y_{\mathbf{s}}\rangle \end{aligned}$$

where $|Y_{\mathbf{s}}\rangle$ is a pure unit vector. By definition, we then have that $M_{\mathbf{s}} = |Y_{\mathbf{s}}\rangle \langle Y_{\mathbf{s}}|$. The probability that the Pretty Good Measurement succeeds is then

$$p_{PGM} = E_{\mathbf{s}} |\langle \psi_{\mathbf{s}} | Y_{\mathbf{s}} \rangle|^2 = \frac{1}{q^{3n}} \left(\sum_{\mathbf{y} \in \mathbb{Z}_q^n} \sqrt{w_{\mathbf{y}}} \right)^2 = \left(\mathbb{E}_{\mathbf{y} \in \mathbb{Z}_q^n} \left[\sqrt{\frac{w_{\mathbf{y}}}{q^n}} \right] \right)^2$$

Finally, we know that this measurement is optimal for distinguishing between the states $|\psi_{\mathbf{s}}\rangle$ due to the symmetric nature of this set of states [BKM97].