On the Quantum Equivalence between $S|\text{LWE}\rangle$ 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 $S|\text{LWE}\rangle$ and $C|\text{LWE}\rangle$ 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 $S|\text{LWE}\rangle$ and ISIS. We present the first fully generic reduction from ISIS to $S|\text{LWE}\rangle$, valid even in the presence of errors in the underlying algorithms. We then explore the reverse direction, introducing an inhomogeneous variant of $C|\text{LWE}\rangle$, denoted $IC|\text{LWE}\rangle$, and show that $IC|\text{LWE}\rangle$ reduces to $S|\text{LWE}\rangle$. Finally, we prove that, under certain recoverability conditions, an algorithm for ISIS can be transformed into one for $S|\text{LWE}\rangle$. We instantiate this reverse reduction by tweaking a known algorithm for $(\text{I})\text{SIS}_\infty$ in order to construct a quantum algorithm for $S|\text{LWE}\rangle$ 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 $S|\text{LWE}\rangle$ and ISIS, and we show both their strong connection and 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 Extrapolated 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 $S|\text{LWE}\rangle$ problem, can be significantly easier than the standard LWE problem. They show how to construct polynomial time quantum algorithm for the SIS_∞ for some contrived parameters. At that time, we didn't have corresponding classical algorithms but later works showed efficient classical algorithms for this problem [II24,KOW25].

Using this type of algorithms, Yamakawa and Zhandry [YZ24] provided a first quantum advantage without structure in the Random Oracle Model. They showed that this approach cannot in all generality be "dequantized" as was the previously mentioned algorithm for SIS_∞. This reduction 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 $S|\text{LWE}\rangle$ 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 $S|\text{LWE}\rangle$ using this approach (see [CT24]). Chailloux and Tillich [CT25] provided the first reduction, from ISIS to $S|\text{LWE}\rangle$. This reduction however requires some assumptions on the $S|\text{LWE}\rangle$ 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 $S|\text{LWE}\rangle$ that is robust to errors in the $S|\text{LWE}\rangle$ algorithm?

Also, because of the importance of $S|\text{LWE}\rangle$, recent works directly construct quantum algorithms for $S|\text{LWE}\rangle$. First, a generic quantum algorithm for $S|\text{LWE}\rangle$ was presented in [CHL+25], running in subexponential time and requiring a subexponential number of queries. Then, the authors of [BJK+25] presented a slightly superpolynomial algorithm for $S|\text{LWE}\rangle$ 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 $S|\text{LWE}\rangle$ from algorithms for ISIS? More generally, are the problems $S|\text{LWE}\rangle$ and ISIS equivalent?

Contributions in short. Our work has the following contributions:

1. We provide the first generic reduction from ISIS to $S|\text{LWE}\rangle$ without any condition on the $S|\text{LWE}\rangle$ algorithm, even when it has errors. This improves and generalizes the work of [CT25]. This result is obtained by a slight change in the construction of the ISIS algorithm, as well as a much sharper analysis of the errors in the $S|\text{LWE}\rangle$ algorithm.
2. For the reverse reduction, we show that, given an ISIS algorithm satisfying certain conditions, we can construct an algorithm for the corresponding

$S|\text{LWE}\rangle$ problem, giving a conditional reduction. We require that the output of the ISIS algorithm is uniform over the solutions and that one can recover the internal randomness used from a solution. This reverse reduction is done by introducing an intermediate problem called $IC|\text{LWE}\rangle$, which is the inhomogeneous of the $C|\text{LWE}\rangle$ problem introduced in [CLZ22].

3. The condition on the ISIS algorithm seems quite stringent at first sight and a natural question to ask is whether it can be useful at all. We answer positively, giving examples of ISIS algorithms that satisfy this property. Moreover, we show that we can recover some existing algorithms from [BJK+25] for $S|\text{LWE}\rangle$, using our algorithm for ISIS and our reverse reduction.

Our results clarify the relation between $S|\text{LWE}\rangle$ and ISIS, showing both their strong connection and the remaining barriers to proving full equivalence. We now provide a more formal presentation of our contributions.

1.2 Problems studied

We first informally define some of the problems we consider in this work in order to properly state our contributions. We provide a formal and more in-depth description of these problems and their relation to other lattice-based problems in Section 2.2. The problems in this subsection are all parameterized by a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, and either by an amplitude function $f : \mathbb{Z}_q^m \to \mathbb{C}$ such that $\|f\|_2 = 1$, or by a set $T \subset \mathbb{Z}^m$, where q, n, m are positive integers.

Definition 1 ($\mathbf{ISIS}(\mathbf{A}, T)$). *Given a uniformly random vector $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ as input, the ISIS$(\mathbf{A}, T)$ problem asks to find a vector $\mathbf{x} \in T$ such that $\mathbf{Ax} = \mathbf{y} \mod q$.*

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 them more general. Chen, Liu, and Zhandry introduced variants of the canonical Learning With Errors problem, namely Search-LWE ($S|\text{LWE}\rangle$) and Construct-LWE ($C|\text{LWE}\rangle$).

Definition 2 ($S|\mathbf{LWE}\rangle(\mathbf{A}, f)$). *Given the state $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e}\rangle$ as input, where $\mathbf{s} \leftarrow \mathbb{Z}_q^b$ is a uniformly random secret vector, the $S|LWE\rangle(\mathbf{A}, f)$ problem asks to recover $\mathbf{s}$.*

Definition 3 ($C|\mathbf{LWE}\rangle(\mathbf{A}, f)$). *The $C|LWE\rangle(\mathbf{A}, f)$ problem asks to construct the state*

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

where Z is a normalization factor.

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

Definition 4 ($IC|\mathbf{LWE}\rangle(\mathbf{A}, f)$). *Given a uniformly random vector $\mathbf{y} \leftarrow \mathbb{Z}_q^n$ as input, the $IC|LWE\rangle(\mathbf{A}, f)$ problem asks to construct the unitary $|\mathbf{y}\rangle|\mathbf{0}\rangle \to |\mathbf{y}\rangle|W_{\mathbf{y}}\rangle$, where we define*

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

with normalizing factors $w_{\mathbf{y}}$.

1.3 Contributions

The goal of this paper is to investigate the two-way reduction between ISIS and $S|\text{LWE}\rangle$. A graphical summary of our results is presented in Figure 1. Our first

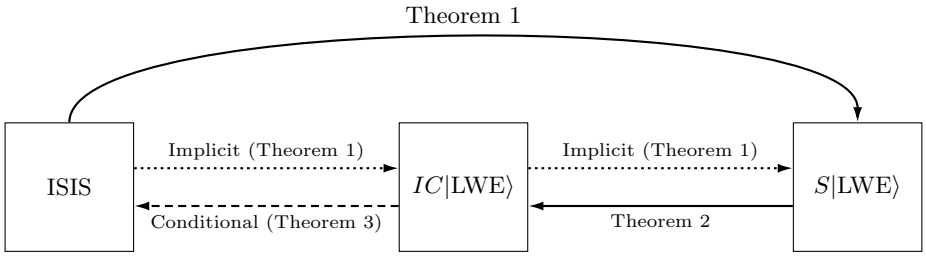

Fig. 1: Table of reductions between the different studied problems. An arrow $A \to B$ means that A reduces to B, or in other terms that an efficient algorithm for problem B can be used to construct an efficient algorithm for problem A.

contribution relates to the forward reduction ISIS $\to S|\text{LWE}\rangle$.

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

This theorem works also when the algorithm solves $S|\text{LWE}\rangle(\mathbf{A}, f)$ with some non-negligible probability p and we also show how to relax the constraint $Supp(\widehat{f}) \subseteq T$. 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 $S|\text{LWE}\rangle(\mathbf{A}, f)$, 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 is to change the error analysis occurring from an error in the $S|\text{LWE}\rangle(\mathbf{A}, f)$ algorithm. We fully take advantage of the fact that we want to solve the inhomogeneous variant $\text{ISIS}(\mathbf{A}, T)$ 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.

The above theorem is very general but a natural question is how to choose the function f and the set T? We provide examples that are standard in the literature. Let ρ_r be the discrete Gaussian distribution on $\mathbb{Z}_q$ of parameter r. The LWE problem is most often defined with the error distribution ρ_r^m, which means the corresponding natural quantum problem is $S|\mathrm{LWE}\rangle(\mathbf{A}, \sqrt{\rho_r^m})$. On the other hand, the most standard setting for ISIS is to consider $T = \{\mathbf{x} \in \mathbb{F}_q^n : \|\mathbf{x}\|_2 \leq l\}$, in which case the corresponding problem is denoted $\mathrm{ISIS}_2(\mathbf{A}, l)$. Applying our theorem with the Gaussian error function and T we can show

Proposition 1. *Let $\mathbf{A} \in \mathbb{F}_q^{n\times m}$ and a real number $r > 0$. If we have an efficient quantum algorithm for $S|LWE\rangle(\mathbf{A}, \sqrt{\rho_r^m})$, then we have an efficient quantum algorithm for $ISIS_2(\mathbf{A}, \sqrt{m}\frac{q}{\sqrt{8\pi}r})$. In particular, if we have an efficient algorithm for $LWE(\mathbf{A}, \rho_r^m)$, then we have an efficient quantum algorithm for $ISIS_2(\mathbf{A}, \sqrt{m}\frac{q}{\sqrt{8\pi}r})$.*

Then, we study the reverse reduction. Our reduction ISIS $\to S|\mathrm{LWE}\rangle$ goes through the intermediate problem which is $IC|\mathrm{LWE}\rangle$. We do not formally write it as a reduction ISIS $\to IC|\mathrm{LWE}\rangle$ and $IC|\mathrm{LWE}\rangle \to S|\mathrm{LWE}\rangle$ 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 $S|\mathrm{LWE}\rangle$ reduces to $IC|\mathrm{LWE}\rangle$.

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

This theorem does not require anything on the algorithm for $IC|\mathrm{LWE}\rangle(\mathbf{A}, f)$, and is robust to errors in the algorithm. One thing to take into account is that the problem $S|\mathrm{LWE}\rangle(\mathbf{A}, f)$ can be intractable 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 $S|\mathrm{LWE}\rangle(\mathbf{A}, f)$ is tractable.

Finally, we investigate the relation between $IC|\mathrm{LWE}\rangle(\mathbf{A}, f)$ and $\mathrm{ISIS}(\mathbf{A}, T)$. Recall that in $IC|\mathrm{LWE}\rangle(\mathbf{A}, f)$, we want to compute the unitary $|\mathbf{y}\rangle|\mathbf{0}\rangle \to |\mathbf{y}\rangle|W_\mathbf{y}\rangle$. We can compute the Fourier transform of $|W_\mathbf{y}\rangle$.

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

where $\Lambda_\mathbf{y}^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{y} \mod q\}$ denotes the q-ary shifted dual lattice associated to $\mathbf{A}$. On the other hand an algorithm for $\mathrm{ISIS}(\mathbf{A}, T)$ 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 $IC|\text{LWE}\rangle \to \text{ISIS}$. More precisely, we introduce the notion of full support randomness-recoverable algorithms, which are randomized classical algorithms from which we can recover the randomness from the solution and that has an output distribution which is uniform over the solutions. We manage to prove the following

Theorem 3 (Informal). *Assume we have an efficient classical algorithm for ISIS$(\mathbf{A}, T)$ which is full support randomness-recoverable, then we have an efficient quantum algorithm for IC$|$LWE$\rangle(\mathbf{A}, f)$, with $\widehat{f} = \mathbb{1}_T$. Using Theorem 2, this means we can also obtain an algorithm for S$|$LWE$\rangle(\mathbf{A}, f)$.*

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 an algorithm of [BJK+25]. This result was phrased in terms of the $\overline{\text{EDCP}}$ problem, which is a variant of the *Extrapolated Dihedral Coset Problem*.

Definition 5 ($\overline{\text{EDCP}}(\mathbf{A}, T)$). *Let q, n, m be positive integers, a set $T \subseteq \mathbb{Z}_q^m$ and a matrix $\mathbf{A} \in \mathbb{F}_q^{n\times m}$. We sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$. Given $|\phi_{\mathbf{s}}\rangle = \frac{1}{\sqrt{|T|}} \sum_{\mathbf{y}\in T} \omega_q^{\mathbf{A}^\mathsf{T}\mathbf{s}\cdot\mathbf{y}} |\mathbf{y}\rangle$, the goal is to recover $\mathbf{s}$*

In [BJK+25], this problem is defined where $T = R^m$ with $R \subseteq \mathbb{Z}_q$. In this case, we can rewrite $|\phi_{\mathbf{s}}\rangle = \bigotimes_{i=1}^m \left(\frac{1}{\sqrt{|R|}} \sum_{j\in R} \omega_q^{j(\mathbf{a}_i\cdot\mathbf{s})} |j\rangle \right)$, where $\mathbf{a}_i$ is the ith line of $\mathbf{A}^\mathsf{T}$.

How is this problem related to our reverse reduction? First notice that $\overline{\text{EDCP}}(\mathbf{A}, T)$ is equivalent to the $S|\text{LWE}\rangle(\mathbf{A}, f)$ problem with $\widehat{f} = \frac{1}{\sqrt{|T|}} \mathbb{1}_T$. Indeed, if we write the states arising in the $S|\text{LWE}\rangle$ problem $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e}) |\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e}\rangle$, we can compute

$$\widehat{|\psi_{\mathbf{s}}\rangle} = \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \omega_q^{\mathbf{A}^\mathsf{T}\mathbf{s}\cdot\mathbf{y}} \left(\frac{1}{\sqrt{q^m}} \sum_{\mathbf{e}\in\mathbb{Z}_q^m} \omega_q^{\mathbf{y}\cdot\mathbf{e}} f(\mathbf{e}) \right) |\mathbf{y}\rangle = \sum_{\mathbf{y}\in\mathbb{Z}_q^m} \omega_q^{\mathbf{A}^\mathsf{T}\mathbf{s}\cdot\mathbf{y}} \widehat{f}(\mathbf{y}) |\mathbf{y}\rangle = |\phi_{\mathbf{s}}\rangle,$$

where $|\phi_{\mathbf{s}}\rangle$ is the state used in $\overline{\text{EDCP}}$. This means we can go from one problem to the other just by applying a quantum Fourier transform on our input state. Our reverse reduction can therefore be naturally restated with this problem

Theorem 4. *Assume we have an efficient classical algorithm for ISIS$(\mathbf{A}, T)$ which is full support randomness recoverable, then we have an efficient quantum algorithm for $\overline{EDCP}(\mathbf{A}, T)$.*

One of the main results of Bai et al. is to prove the following statement

Proposition 2 ([BJK+25]). *For parameters $n, m, q = 2^l$ with $q = \mathsf{poly}(n)$ and $m = 2^{O(\log(n)\log(q))}$, there exists a quantum algorithm for $\overline{EDCP}(\mathbf{A}, \mathbb{Z}_2^m)$ running in time $2^{O(\log(n)\log(q))}$ in the case $\mathbf{A}$ is randomly chosen in $\mathbb{Z}_q^{n\times m}$.*

They also show that the *Extrapolated Dihedral Coset Problem* they consider naturally reduces to $\overline{\text{EDCP}}$. 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 5 (Informal). *One can adapt the classical algorithm for ISIS by Regev to make it randomness-recoverable and full support. Plugging this algorithm into Theorem 4, we can recover Proposition 2.*

1.4 Comparison with Previous Works

As mentioned above, the authors of [CT25] present a reduction from ISIS to $S|\text{LWE}\rangle$ for some class of $S|\text{LWE}\rangle$ solvers. Our result generalizes theirs as it works for all $S|\text{LWE}\rangle$ solvers. Our formulation in terms of $Supp(\widehat{f})$ makes is also very powerful, and this was crucially used in a subsequent work [Cha25] (and adapted to codes) to improve Decoded Quantum Interferometry [JSW+24].

Additionally, in terms of proof techniques, we provide a much sharper analysis of the errors Instead of just adding an error term that depends on the solver's success probability, we use the structure of the error vectors and integrate this in the final success probability. Note that this is done by not going through the quantum sampling problem $IC|\text{LWE}\rangle$ but directly studying the reduction between ISIS and $S|\text{LWE}\rangle$.

Chain of reductions from $S|LWE\rangle$ to ISIS. A natural question is to ask whether reduction from$S|\text{LWE}\rangle$ to ISIS existed in the literature. Such a reduction can actually be obtained from the following chain of reductions: $S|\text{LWE}\rangle \to \text{LWE} \to d\text{LWE} \to \text{SIS} \to \text{ISIS}$. While the $S|\text{LWE}\rangle \to \text{LWE}$ and $\text{SIS} \to \text{ISIS}$ reductions are lossless, the two other ones are lossy, and importantly, this chain is one-way.

The main difference is that our reduction is lossless, in the sense that the matrix $\mathbf{A}$ stays the same throughout the reductions. Moreover, in the regimes where our reverse reduction holds, we can apply the forward and the reverse reduction to recover our original problem, without any losses in the parameters. In this sense, our reverse reduction can be seen as the natural reduction that targets directly $S|\text{LWE}\rangle$. In particular, we couldn't have recovered the results of [BJK+25] if we used the classical reduction instead of our reduction.

1.5 Takeaways and Future Work

Our first contribution is important as it provides what we hope to be the final form of the reduction ISIS $\to S|\text{LWE}\rangle$. 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. As we mentioned, this result was used in [Cha25] to improve on quantum algorithms for 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 $S|\text{LWE}\rangle$ 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 $IC|\text{LWE}\rangle$ is key to understanding the relation between these problems.

Our results could also be used to construct other algorithms for $S|\text{LWE}\rangle$ (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 $S|\text{LWE}\rangle$ could have significant consequences, since there is a reduction LWE $\to S|\text{LWE}\rangle$ shown in [BKSW18]. 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 [BKSW18].

Acknowledgements

We acknowledge funding from the French PEPR integrated projects EPIQ (ANR-22-PETQ-007), PQTLS (ANR-22-PETQ-008) and HQI (ANR-22-PNCQ-0002) all part of plan France 2030. We thank the anonymous reviewers for their insightful comments on our previous submission.

2 Preliminaries

2.1 Notations

For a positive integer q, we write $\mathbb{Z}_q$ for $\mathbb{Z}/q\mathbb{Z}$. We write $\mathbb{Z}_q = \{-\lfloor \frac{q}{2} \rfloor, \ldots, \lfloor \frac{q-1}{2} \rfloor\}$. 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 $\mathbf{A}, \mathbf{H}$. For any function $f : \mathbb{Z}_q^m \to \mathbb{C}$, we define the ℓ_2 norm $\|f\|_2$ of f as $\|f\|_2 = \sum_{\mathbf{x} \in \mathbb{Z}_q^m} |f(\mathbf{x})|^2$.

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. We use the following definition for statistical distance between any two probability distributions represented by their probability mass functions p and q: $\Delta(p,q) = \frac{1}{2}\sum_x |p(x) - q(x)|$.

Definition 6. *Let q, n, m be positive integers 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*

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

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

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

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

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

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

2.2 Definition of computational problems

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

Definition 7 (Short Integer Solution SIS$(\mathbf{A}, \beta)$). *Let q, n, m be positive integers, and β and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. The goal is, given $\mathbf{A}$, to find $\mathbf{x} \in \mathbb{Z}^m \backslash \{\mathbf{0}\}$ such that $\mathbf{A}\mathbf{x} = \mathbf{0} \mod q$ 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 8 (Inhomogeneous Short Integer Solution ISIS$(\mathbf{A}, \beta)$). *Let q, n, m, β be positive integers 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 $\mathbf{A}\mathbf{x} = \mathbf{y} \mod q$ 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 9 (Short Integer Solution SIS$(\mathbf{A}, T)$). *Let q, n, m be positive integers, 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 $\mathbf{x} \in T\backslash\{\mathbf{0}\}$ such that $\mathbf{A}\mathbf{x} = \mathbf{0} \mod q$.*

Definition 10 (Inhomogeneous Short Integer Solution ISIS$(\mathbf{A}, T)$). *Let q, n, m be positive integers, 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 $\mathbf{Ax} = \mathbf{y} \mod q$.*

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 11 (Learning With Errors LWE$(\mathbf{A}, p)$). *Let q, n, m be positive integers, 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 $(\mathbf{A}, \mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e})$, 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 $p = \rho_r^m$ where ρ_r is a discretized Gaussian distribution on $\mathbb{Z}_q$ of parameter r. We now define the variants explicitly introduced in [CLZ22], where the noise is in quantum superposition.

Definition 12 ($S|\mathbf{LWE}\rangle(\mathbf{A}, f)$). *Let q, n, m be positive integers, a function $f : \mathbb{Z}_q^m \to \mathbb{C}$ 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 $|\psi_\mathbf{s}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e}\rangle$, the goal is to recover $\mathbf{s}$.*

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

Definition 13 ($C|\mathbf{LWE}\rangle(\mathbf{A}, f)$). *Let q, n, m be positive integers, a function $f : \mathbb{Z}_q^m \to \mathbb{C}$ 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*

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

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 14 ($IC|\mathbf{LWE}\rangle(\mathbf{A}, f)$). *Let q, n, m be positive integers, a function $f : \mathbb{Z}_q^m \to \mathbb{C}$ such that $\|f\|_2 = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. The goal is to construct the unitary*

$$|\mathbf{y}\rangle|\mathbf{0}\rangle \to |\mathbf{y}\rangle|W_\mathbf{y}\rangle,$$

where we define

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

with normalizing factors $w_\mathbf{y}$.

Remark 1. Defining $IC|\mathrm{LWE}\rangle$ through the construction of *a unitary* instead of an algorithm constructing $|W_\mathbf{y}\rangle$ on input $\mathbf{y}$ might seem an unexpected generalization of the $C|\mathrm{LWE}\rangle$ problem — as the existence of such an algorithm does not imply

the unitary we define, but merely one that satisfies $|\mathbf{y}\rangle|\mathbf{0}\rangle|\mathbf{0}\rangle \to |\mathbf{y}\rangle|W_{\mathbf{y}}\rangle|\phi_{\mathbf{y}}\rangle$ for some garbage state $|\phi_{\mathbf{y}}\rangle$. However, we note that in the special case of $C|\mathrm{LWE}\rangle$, defining the problem through the construction of a unitary or an algorithm is equivalent (in this sense, we do generalize this problem), and that we use $IC|\mathrm{LWE}\rangle$ as an intermediate step in our reduction, and successfully manage to instantiate our final reduction with this condition. Furthermore, defining this problem through a unitary turns out to be crucial in our reduction, as it allows to apply the reverse unitary.

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

The goal of this section is to present some preliminary calculations on the $S|\mathrm{LWE}\rangle, IC|\mathrm{LWE}\rangle$ and ISIS problems. We also provide a discussion on the tractability regime of $S|\mathrm{LWE}\rangle$ 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 $S|\mathrm{LWE}\rangle$ and $IC|\mathrm{LWE}\rangle$ in the Fourier basis.

Proposition 3. *Let q, n, m be positive integers, a function $f : \mathbb{Z}_q^m \to \mathbb{C}$ such that $\|f\|_2 = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. For each $\mathbf{s} \in \mathbb{Z}_q^n$, we define $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\mathsf{T}\mathbf{s}+\mathbf{e}\rangle$. 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

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

Proposition 4. *Let q, n, m be positive integers, a function $f : \mathbb{Z}_q^m \to \mathbb{C}$ such that $\|f\|_2 = 1$ and a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$. For each $\mathbf{y} \in \mathbb{Z}_q^n$, let*

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

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

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

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 $Im(\widehat{f}) \subseteq T$ 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 5.

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

Proof. The first equality 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 6. $\mathbb{E}_{\mathbf{y}}[w_{\mathbf{y}}] = q^n$.

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 $\|f\|_2 = \|\widehat{f}\|_2 = 1$, we immediately have

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

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

Proposition 7. *Let q, m, n be positive integers. Let $f : \mathbb{Z}_q^m \to \mathbb{C}$ such that $\|f\|_2 = 1$ and let $\mathbf{A} \in \mathbb{Z}_q^n$. For each $\mathbf{y} \in \mathbb{Z}_q^n$, let*

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

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 $S|LWE\rangle(\mathbf{A}, f)$ 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 ISIS $\to S|\mathrm{LWE}\rangle$

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

Theorem 1. *Let q, m, n be positive integers, let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and let $f : \mathbb{Z}_q^n \to \mathbb{C}$ with $\|f\|_2 = 1$. Let $T \subseteq \mathbb{Z}_q^m$. Assume that*

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

– *f is quantum samplable in time* Time_{Sampl} *i.e. there is a quantum algorithm running in time* Time_{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*

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

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

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

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

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

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

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

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 $S_{\mathbf{z}} : |\mathbf{x}\rangle \to |\mathbf{x}+\mathbf{z}\rangle$ 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 $|\psi_{\mathbf{t}}\rangle = S_{\mathbf{A}^\intercal(\mathbf{t}-\mathbf{s})}|\psi_{\mathbf{s}}\rangle$. We consider the following algorithm

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

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

2. Apply U on the first two register to obtain

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

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

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

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 $\mathbf{s} \in \mathbb{Z}_q^n$,

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

for some unit vectors $|\widetilde{\psi}_{\mathbf{s},\mathbf{s}'}\rangle$ 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 $|\widetilde{\psi}''_{\mathbf{s},\mathbf{s}'}\rangle = \frac{\gamma_{\mathbf{s},\mathbf{s}'}}{|\gamma_{\mathbf{s},\mathbf{s}'}|} |\widetilde{\psi}'_{\mathbf{s},\mathbf{s}'}\rangle$, we can indeed write

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

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: 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 $f : \mathbb{Z}_q^m \to \mathbb{C}$ such that $\|f\|_2 = 1$. For each $\mathbf{s} \in \mathbb{Z}_q^n$, we write $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\mathsf{T}\mathbf{s}+\mathbf{e}\rangle$. Assume we have an efficiently computable quantum unitary

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

where $\forall \mathbf{s} \in \mathbb{Z}_q^n$, $\gamma_{\mathbf{s},\mathbf{s}} = \sqrt{p}$ and each $\||\widetilde{\psi}_{\mathbf{s},\mathbf{s}'}\rangle\| = 1$. 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 $\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m : \mathbf{A}\mathbf{x} = \mathbf{y} \mod q\}$

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

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

   Here, Ⓐ 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 $\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\omega^{-\mathbf{y}\cdot\mathbf{s}}|\widetilde{\psi}_{\mathbf{s},\mathbf{s}}\rangle|\mathbf{s}\rangle|\mathbf{0}\rangle$.
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

- $\text{Time}_{S|\text{LWE}\rangle}$ be the running time to compute U.
- Time_{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

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

   which corresponds to the initial state by adding a $|\mathbf{0}\rangle$ register and reordering. In ①, we use the fact that $\mathbf{s}\to\mathbf{A}^\mathsf{T}\mathbf{s}$ 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 Time_{Sampl}. In practice, f is chosen such that this state can be computed efficiently. The running time of this is therefore in $O(\text{Time}_{Sampl}+\mathsf{poly}(m,\log(q)))$.
2. In step 3, before the measurement, we have the state

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

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

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: $\frac{1}{\sqrt{q^n}}\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\omega^{-\mathbf{y}\cdot\mathbf{s}}|\widetilde{\psi}_{\mathbf{s},\mathbf{s}}\rangle|\mathbf{s}\rangle|0\rangle$. 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 $S|\mathrm{LWE}\rangle$ algorithm. From there, we conclude that the time required for this algorithm to successfully pass step 3 is

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

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

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

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

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

for some unit vector $|Z_{\mathbf{s}}\rangle$ orthogonal to $|\psi_{\mathbf{s}}\rangle|0\rangle$, 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 $\mathsf{poly}(m,\log(q))$.

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

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

In particular, if $\mathrm{Time}_{S|\mathrm{LWE}\rangle}, \mathrm{Time}_{Sampl}, \frac{1}{p} = \mathsf{poly}(m,\log(q))$ then $\mathrm{Time}_{\mathrm{ISIS}} = \mathsf{poly}(m,\log(q))$. 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

Proof (of Theorem 1). We start from a quantum algorithm for $S|\mathrm{LWE}\rangle(\mathbf{A},f)$ 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 $p'_{\mathbf{y}}$ 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 $p'_{\mathbf{y}} \geq \sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T} |\langle\mathbf{x}|\Xi_{\mathbf{0}}^{\mathbf{y}}\rangle|^2$. We now define the $\{z_{\mathbf{s},\mathbf{x}}\}$ such that $|\widehat{Z_{\mathbf{s}}^0}\rangle = \sum_{\mathbf{x}\in\mathbb{Z}_q^m} z_{\mathbf{s},\mathbf{x}}|\mathbf{x}\rangle$, and have the following lemma.

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

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

Proof. In order to compute $p'_{\mathbf{y}}$, we have to compute $|\Xi_0\rangle$. Using Proposition 3, 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

$$p'_{\mathbf{y}} \geq \sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T} |\langle\mathbf{x}|\Xi_{\mathbf{0}}^{\mathbf{y}}\rangle|^2 = \sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T} \left| \sqrt{q^n p} \widehat{f}(\mathbf{x}) + \sqrt{\frac{1-p}{q^n}} \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \omega^{-\mathbf{y}\cdot\mathbf{s}} z_{\mathbf{s},\mathbf{x}} \right|^2.$$

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

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

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

$$\mathbb{E}_{\mathbf{y}\leftarrow\mathbb{Z}_q^n}\left[\sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T}\left(pq^n|\widehat{f}(\mathbf{x})|^2\right)\right]=p(1-\eta)$$

$$\forall\mathbf{y}\in\mathbb{Z}_q^n,\ \sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T}\left(\frac{1-p}{q^n}\left|\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\omega^{-\mathbf{y}\cdot\mathbf{s}}z_{\mathbf{s},\mathbf{x}}\right|^2\right)\geq 0$$

$$\sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T}\left(2Re\left(\sqrt{p}\sqrt{q^n}\widehat{f}(\mathbf{x})\frac{\sqrt{1-p}}{\sqrt{q^n}}\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\omega^{\mathbf{y}\cdot\mathbf{s}}\overline{z_{\mathbf{s},\mathbf{x}}}\right)\right)=$$

$$2\sqrt{p(1-p)}Re\left(\sum_{\mathbf{x}\in\Lambda_{\mathbf{y}}^{\perp}(\mathbf{A})\cap T,\mathbf{s}\in\mathbb{Z}_q^n}\widehat{f}(\mathbf{x})\omega^{\mathbf{y}\cdot\mathbf{s}}\overline{z_{\mathbf{s},\mathbf{x}}}\right)$$

From there, we write

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

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 $\langle Z^0_{\mathbf{s}}|\psi_{\mathbf{s}}\rangle = \langle \widehat{Z^0_{\mathbf{s}}}|\widehat{\psi_{\mathbf{s}}}\rangle = 0$ 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 $\mathbf{s} \in \mathbb{Z}_q^n$,

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

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

We can now conclude our main proof. We have

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

Plugging this lower bound in the expression above, we obtain

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

which concludes the proof.

We present the instantiation with Gaussian functions (Proposition 1) in Appendix B

5 Reverse direction $S|\mathrm{LWE}\rangle \to IC|\mathrm{LWE}\rangle$

Definition 15. *We say that a unitary U for $IC|LWE\rangle(\mathbf{A}, f)$ has fidelity γ if for all $\mathbf{y} \in \mathbb{Z}_q^n$,*

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

for some unit vectors $|W'_{\mathbf{y}}\rangle$; where $|W_{\mathbf{y}}\rangle = \frac{1}{\sqrt{w_{\mathbf{y}}}} \sum_{\mathbf{s}\in\mathbb{Z}_q^n} \omega^{-\mathbf{y}\cdot\mathbf{s}} \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\mathsf{T}\mathbf{s} + \mathbf{e}\rangle$.

We prove the following theorem

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

- *We have an efficient unitary for $IC|LWE\rangle(\mathbf{A}, f)$ 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*

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

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

Proof. We prove this theorem below in the case where $\varepsilon = \varepsilon' = 0$, and defer the proof for general ε and ε' to Appendix D.

Remember that $|\widehat{\psi_{\mathbf{s}}}\rangle = \frac{1}{q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega^{\mathbf{y}\cdot\mathbf{s}} \sqrt{w_{\mathbf{y}}} |\widehat{W_{\mathbf{y}}}\rangle$ (proposition 5). First apply a QFT to $|\psi_{\mathbf{s}}\rangle$, then apply the function $\mathbf{x} \mapsto \mathbf{A}\mathbf{x}$ in superposition and store the result in a second register. As each $|\widehat{W_{\mathbf{y}}}\rangle$ is a superposition of vectors in $\Lambda_{\mathbf{y}}^\perp(\mathbf{A})$, this yields

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

Now, the existence of an efficient unitary for $IC|\mathrm{LWE}\rangle(\mathbf{A}, f)$ implies the existence of another efficient unitary U mapping $|\mathbf{y}\rangle|\mathbf{0}\rangle$ to $|\mathbf{y}\rangle|\widehat{W_{\mathbf{y}}}\rangle$. Swapping the registers and applying $U^\dagger$ then zeroizes the $|\widehat{W_{\mathbf{y}}}\rangle$ register, allowing us to remove it and leaving only

$$|\phi\rangle \triangleq \frac{1}{q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega^{\mathbf{y}\cdot\mathbf{s}} \sqrt{w_{\mathbf{y}}} |\mathbf{y}\rangle$$

Observe finally that the overlap between $|\phi\rangle$ and $\frac{1}{q^n} \sum_{\mathbf{y}\in\mathbb{Z}_q^n} \omega^{\mathbf{y}\cdot\mathbf{s}} |\mathbf{y}\rangle$ is $\mathbb{E}_{\mathbf{y}} \frac{\sqrt{w_{\mathbf{y}}}}{q^n} = 1$. Thus, applying an inverse QFT on $|\phi\rangle$, and then measuring yields $\mathbf{s}$ with probability 1.

6 Conditional reverse reduction $IC|\mathrm{LWE}\rangle \to \mathrm{ISIS}$

In this last section, we provide another reduction. We show that if we have an algorithm for $\mathrm{ISIS}(\mathbf{A}, f)$ which has a specific form then it can be used to solve $S|\mathrm{LWE}\rangle(\mathbf{A}, f)$. 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 16 (Randomness-Recoverable Algorithm for ISIS). *Let* A *be an algorithm for ISIS*$(\mathbf{A}, T)$*, and denote by* $\mathsf{A}(\mathbf{y}; r)$ *the output of* A *on input* $\mathbf{y}$ *using random tape* $r \in \{0,1\}^\ell$*.* A *is said to be perfectly randomness-recoverable if there is an algorithm* E *satisfying*

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

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

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

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

  where $\Delta(p_{\mathbf{y}}, u_{\mathbf{y}})$ *is the statistical distance between the distribution* $p_{\mathbf{y}}$ *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* $\widehat{f} = \mathbb{1}_T$ *with fidelity* $1 - \varepsilon$ *and time complexity* $\mathsf{poly}(t)$*.*

Remark 2. We do not explicitly say anything about the success probability of the algorithm 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 A in superposition over the first and second registers and store the result in a third register:

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

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

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

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

Let $|W'_{\mathbf{y}}\rangle = \frac{1}{\sqrt{2^\ell}}\mathrm{QFT}_{\mathbb{Z}_q^n}^{-1}\left(\sum_{r\in\{0,1\}^\ell}|\mathsf{A}(\mathbf{y};r)\rangle\right)$. In order to show that we have a quantum algorithm that solves $IC|\mathrm{LWE}\rangle(\mathbf{A}, f)$ 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

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

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 $IC|\mathrm{LWE}\rangle(\mathbf{A}, \mathbb{1}_T)$ with fidelity at least $\mathbb{E}_{\mathbf{y}}[1-\varepsilon_{\mathbf{y}}] = 1-\varepsilon$.

In our work, we only require the above theorem for algorithms which are perfectly randomness recoverable. For sake of completeness, we extend the theorem to setting where the algorithm is almost randomness recoverable in in Appendix C.

7 Specific instantiation of the reverse reduction

In this section, we describe a new algorithm to solve ISIS in a certain range of parameters, and show that, by instantiating our reduction with this solver,

we can recover a recent result from [BJK+25], proving that $S|\mathrm{LWE}\rangle$ is solvable in super-polynomial time when the modulo is a power of two. Interestingly, while [BJK+25] introduced a somehow complex quantum algorithm for this task, involving several layers of preparing, measuring, and combining quantum states, our method is arguably much more straightforward, and "only" involves QFT gates and coherent implementation of classical algorithms. We believe that this hints that the hardness of $S|\mathrm{LWE}\rangle$ mostly lies in the hardness of the underlying ISIS problem.

In this section, we sometimes abuse the notations and write, for $\overline{\mathbf{x}} \in \mathbb{Z}_q^m$, $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$ to denote that the coefficients of $\overline{\mathbf{x}}$ all belong $\{0,1\}$.

7.1 An algorithm for solving ISIS with non-trivial ℓ_∞-norm bounds

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

Proposition 9. *For some parameters $n, m, q = 2^\ell$ with $q = \mathsf{poly}(n)$ 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 describe an efficient ISIS solver algorithm, and show that we can recover the above proposition simply by plugging this algorithm in our reverse reduction.

We start by describing our solver, adapted from the SIS-solver algorithm described in [CLZ22, Appendix A], in a generic way. Recall that instantiating our reduction with a solver requires the solver to be randomness-recoverable. To prove this property, we need to provide more details on how to implement this algorithm — in particular how we sample the vectors. We simply present in this subsection a generic version of the solver, without the aforementioned detailed sampling procedures, and prove its correctness and time-complexity. A complete version of the algorithm, with detailed sampling procedures, is presented them in Section 7.2.

Algorithm 2: ISIS-Solver

Parameters: Positive integers ℓ, n, and w such that $w > cn$ for some constant $c > 1$.

Notations: Let $q = 2^\ell$, and $m = w^\ell$. If $\ell > 1$, let $q' = q/2$, and $m' = m/w$.

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

Output: $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$ such that $\mathbf{A}\overline{\mathbf{x}} = \mathbf{y} \mod q$, and $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$.

Execution of the algorithm (for $\ell = 1$): If $\mathbf{A}$ is not full-rank, abort (*i.e.* return error symbol $\perp$). Otherwise, sample a solution $\mathbf{x}$ to the system $\mathbf{A}\mathbf{x} = \mathbf{y} \mod 2$, and return it.

Execution of the algorithm (for $\ell > 1$):

1. *(Sample $\mathbf{y}$'s shares.)* For $i \in [\![1, m'-1]\!]$, sample $\mathbf{y}_i \leftarrow \mathbb{Z}_2^n$. Let $\mathbf{y}_{m'} \triangleq \mathbf{y} - \sum_{i=1}^{m'-1} \mathbf{y}_i \mod 2$.

2. *(Build block-matrices.)* Let $\mathbf{A}_1, \ldots, \mathbf{A}_{m'}$ be the matrices in $\mathbb{Z}_2^{n \times w}$ such that $\mathbf{A} = [\mathbf{A}_1 | \ldots | \mathbf{A}_{m'}] \mod 2$. If there exists $i \in [\![1, m]\!]$ such that $\mathbf{A}_i$ is not full rank modulo 2, abort (*i.e.* return error symbol $\perp$).

3. *(Sample solution pairs for each block.)* For all $i \in [\![1, m']\!]$, compute two solutions $\mathbf{x}_i^{(1)}$ and $\mathbf{x}_i^{(2)}$ to the equation $\mathbf{A}_i \mathbf{x} = \mathbf{y}_i \mod 2$, such that $\mathbf{x}_i^{(1)} \neq \mathbf{x}_i^{(2)}$. Then, let $\mathbf{x}_i \triangleq \mathbf{x}_i^{(1)}$, and $\mathbf{z}_i \triangleq \mathbf{x}_i^{(2)} - \mathbf{x}_i^{(1)} \mod q$ [a].

4. *(Merge block solutions.)* Let $\mathbf{x} \in \mathbb{Z}_2^m$, and $\mathbf{Z} \in \mathbb{Z}_q^{m \times m'}$ defined as follows:

$$\mathbf{x} \triangleq \begin{pmatrix} \mathbf{x}_1 \\ \hline \vdots \\ \hline \mathbf{x}_{m'} \end{pmatrix} \qquad \mathbf{Z} \triangleq \begin{bmatrix} \mathbf{z}_1 & & & \\ & \mathbf{z}_2 & & \\ & & \ddots & \\ & & & \mathbf{z}_{m'} \end{bmatrix}$$

   where the empty spots in $\mathbf{Z}$ are zeroes. Note that $\mathbf{A}\mathbf{x} = \mathbf{y} \mod 2$, and $\mathbf{A}\mathbf{Z} = \sum_i \mathbf{A}_i \mathbf{z}_i = \mathbf{0} \mod 2$.

5. *(Apply next step of the recursion.)* Let $\mathbf{y}' \triangleq \frac{\mathbf{y} - \mathbf{A}\mathbf{x}}{2} \mod q' \in \mathbb{Z}_{q'}^n$ and $\mathbf{A}' \triangleq \frac{\mathbf{A}\mathbf{Z}}{2} \mod q' \in \mathbb{Z}_{q'}^{n \times m'}$ [b]. Run $\mathsf{ISIS\text{-}Solver}(\mathbf{A}', \mathbf{y}')$ with parameters $(\ell - 1, n)$, and let $\mathbf{x}'$ denote the outcome. If $\mathbf{x} = \perp$, abort (*i.e.* return error symbol $\perp$). Otherwise, return $\overline{\mathbf{x}} = \mathbf{x} + \mathbf{Z}\mathbf{x}' \mod q$.

[a] We emphasize that the $\mathbf{z}_i$'s are defined modulo q and not modulo 2. This turns out to be crucial to enforce the norm constraint.

[b] $\mathbf{y}'$ and $\mathbf{A}'$ are well defined, as $\mathbf{A}\mathbf{x} = \mathbf{y} \mod 2$, and $\mathbf{A}\mathbf{Z} = 0 \mod 2$.

We now prove the correctness and time-complexity of Algorithm 2. We start by proving that Algorithm 2 only aborts with negligible probability over random matrix $\mathbf{A}$ and its internal randomness.

Lemma 3. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$. For all $\mathbf{y} \in \mathbb{Z}_q^n$,*

$$\Pr\left[\mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}) = \perp \,:\, \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}\right] = \mathsf{negl}(n)$$

Proof. Algorithm 2 aborts if any block-matrix is not full-rank. As w is sufficiently larger than n, any block-matrix taken alone is full-rank with probability $1 - \mathsf{negl}(n)$. As one run of the algorithm uses polynomially-many block-matrices, showing that they are all uniformly random and independent is sufficient to prove the proposition by a union bound.

Formally, we prove that when the algorithm is run at level ℓ with a uniformly random matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ as input , then the next-level's matrix $\mathbf{A}' \in \mathbb{Z}_{q'}^{n \times m'}$

produced by the algorithm is also uniformly random, and independent from level-ℓ's block-matrices $(\mathbf{A}_i \mod 2)_i$.

Write first $\mathbf{A} = \mathbf{A}_0 + 2\mathbf{B}$, where $\mathbf{A}_0$ is over $\mathbb{Z}_2$, $\mathbf{B}$ is over $\mathbb{Z}_{q'}$, and the addition and scalar-multiplication are over $\mathbb{Z}_q$. Note that, as $\mathbf{A}$ is uniformly random, and 2 divides q, then $\mathbf{A}_0$ and $\mathbf{B}$ are independent and both uniformly random. For each block i, the corresponding block-matrix is then $(\mathbf{A}_i \mod 2) = \mathbf{A}_{0,i}$. The i-th column $\mathbf{a}'_i$ of the next-level matrix $\mathbf{A}'$ is then defined as

$$\mathbf{a}'_i = \frac{\mathbf{A}_i \mathbf{z}_i}{2} \mod q' = \frac{\mathbf{A}_{0,i} \mathbf{z}_i}{2} + \mathbf{B}_i \mathbf{z}_i \mod q'$$

Now recall that $\mathbf{z}_i$ depends only on $\mathbf{A}_{0,i}$. Hence $\mathbf{B}_i$ is uniformly random, and independent from $\mathbf{A}_{0,i}$ and $\mathbf{z}_i$. As $\mathbf{z}_i$ is non-zero by construction, and each of its coefficients belong to $\{-1, 0, 1\}$, it comes that $\mathbf{a}'_i$ is uniformly random, and independent from $\mathbf{A}_{0,i}$ — and more generally independent from $\mathbf{A}_0$.

Applying this reasoning recursively completes the proof.

We can now proceed with the correctness.

Proposition 10. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$ and $m = w^\ell$. Then, for all $\mathbf{y} \in \mathbb{Z}_q^n$:*

$$\Pr\left[\begin{array}{c} \mathbf{A}\mathbf{x} = \mathbf{y} \mod q \\ \wedge \\ \mathbf{x} \in \mathbb{Z}_2^m \end{array} : \begin{array}{l} \mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m} \\ \mathbf{x} \leftarrow \mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}) \end{array}\right] = 1 - \mathsf{negl}(n)$$

Proof. By Lemma 3, we can safely assume that Algorithm 2 does not abort, as it only changes the probability by a negligible amount. We prove the result by induction on ℓ. When $\ell = 1$, the correctness is immediate. When $\ell > 1$, let $\overline{\mathbf{x}}$ be an output of the algorithm. By construction, $\overline{\mathbf{x}} = \mathbf{x} + \mathbf{Z}\mathbf{x}' \mod q$ where

$$\begin{array}{lll} \mathbf{A}' \triangleq \mathbf{A}\mathbf{Z}/2 \mod q' & \textit{i.e.}\ \mathbf{A}\mathbf{Z} = 2\mathbf{A}' \mod q \\ \mathbf{A}'\mathbf{x}' = \mathbf{y}' \mod q' & \textit{i.e.}\ 2\mathbf{A}'\mathbf{x}' = 2\mathbf{y}' \mod q \\ \mathbf{y}' \triangleq (\mathbf{y} - \mathbf{A}\mathbf{x})/2 \mod q' & \textit{i.e.}\ \mathbf{A}\mathbf{x} = \mathbf{y} - 2\mathbf{y}' \mod q \end{array}$$

where the second line follows by induction hypothesis, as $\mathbf{x}'$ is an output of Algorithm 2 on input $(\mathbf{A}', \mathbf{y}')$. Using these identities, it comes $\mathbf{A}\overline{\mathbf{x}} = \mathbf{A}\mathbf{x} + \mathbf{A}\mathbf{Z}\mathbf{x}' \mod q = \mathbf{A}\mathbf{x} + 2\mathbf{A}'\mathbf{x}' \mod q = \mathbf{A}\mathbf{x} + 2\mathbf{y}' \mod q = \mathbf{y} \mod q$ which concludes the first part of the proof.

It remains to show that $\mathbf{x} \in \mathbb{Z}_2^m$. By induction hypothesis, $\mathbf{x}' \in \mathbb{Z}_2^m$. Furthermore, the block-column structure of $\mathbf{Z}$ enforces $\overline{\mathbf{x}}_i = \mathbf{x}_i + \mathbf{x}'[i] \cdot \mathbf{z}_i$ for all i, where $\mathbf{x}'[i] \in \{0, 1\}$ denotes the i-th coefficient of $\mathbf{x}'$ [1]. Recall that $\mathbf{x}_i$ is defined as the first solution $\mathbf{x}_i^{(1)}$ of the pair $(\mathbf{x}_i^{(1)}, \mathbf{x}_i^{(2)})$ sampled in step 3, and $\mathbf{z}_i$ as $\mathbf{x}_i^{(2)} - \mathbf{x}_i^{(1)}$, where, crucially, the difference is over $\mathbb{Z}_q$. Thus, $\overline{\mathbf{x}}_i \in \left\{\mathbf{x}_i^{(1)}, \mathbf{x}_i^{(2)}\right\}$, which implies $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$, and concludes the proof.

[1] This is as opposed to the notation $\mathbf{x}'_i$ that denotes the i-th *block* of $\mathbf{x}'$.

Proposition 11. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$. Then Algorithm 2 runs in time $2^{O(\log(n)\log(q))}$.*

Proof. This is straightforward, as $m = w^\ell = 2^{O(\log(n)\log(q))}$, and the algorithm consists in less than m blocks, each of them itself consisting in solving 2 linear systems of size $\mathsf{poly}(n)$ over $\mathbb{Z}_2$, which can be done efficiently using Gaussian elimination.

7.2 Randomness recovery

We show in this subsection that Algorithm 2 can be made randomness-recoverable. In order to do that, we present a completed version of this algorithm, in which we explicitely describe how we sample the inhomogeneous and homogeneous solutions at each level. We write the difference between this completed version and Algorithm 2 in blue. This allows us to prove that the algorithm, we considering random tape as an input, is almost bijective, and allows to conclude that it is randomness-recoverable. In the rest of the section, ISIS-Solver denotes this detailed version: Algorithm 3.

Algorithm 3: ISIS-Solver

Parameters: Positive integers ℓ, n, and w such that $w > cn$ for some constant $c > 1$.

Subroutine: A *deterministic* MatExtend procedure that takes a rank-n matrix $\mathbf{A} \in \mathbb{Z}_2^{n\times w}$ as input, as well as an integer $r \in [\![n, w]\!]$, and returns an "extended" matrix $\widetilde{\mathbf{A}} \in \mathbb{Z}_2^{r\times w}$ of rank r, and such that the first n rows of $\widetilde{\mathbf{A}}$ exactly form the matrix $\mathbf{A}$.

Notations: Let $q = 2^\ell$, and $m = w^\ell$. If $\ell > 1$, let $q' = q/2$, and $m' = m/w$.

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

Output: $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$ such that $\mathbf{A}\overline{\mathbf{x}} = \mathbf{y} \mod q$, and $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$.

Execution of the algorithm (for $\ell = 1$): If $\mathbf{A}$ is not full-rank, abort (*i.e.* return error symbol $\perp$ and the random tape). Otherwise, extend $\mathbf{A}$ to the rank-w matrix $\widetilde{\mathbf{A}}$ using MatExtend procedure, then consume $w - n$ bits from the random tape to construct a vector $\mathbf{u} \in \mathbb{Z}_2^{w-n}$, and finally compute and return the only solution $\mathbf{x}$ to the system $\widetilde{\mathbf{A}}\mathbf{x} = (\mathbf{y}\|\mathbf{u})^\mathsf{T} \mod 2$.

Execution of the algorithm (for $\ell > 1$):

1. *(Sample $\mathbf{y}$'s shares.)* For $i \in [\![1, m' - 1]\!]$, consume n bits from the random tape to construct $\mathbf{y}_i \leftarrow \mathbb{Z}_2^n$. Let $\mathbf{y}_{m'} \triangleq \mathbf{y} - \sum_{i=1}^{m'-1} \mathbf{y}_i \mod 2$.

2. *(Build block-matrices.)* Let $\mathbf{A}_1, \ldots, \mathbf{A}_{m'}$ be the matrices in $\mathbb{Z}_2^{n\times w}$ such that $\mathbf{A} = [\mathbf{A}_1|\ldots|\mathbf{A}_{m'}] \mod 2$. If there exists $i \in [\![1, m]\!]$ such that $\mathbf{A}_i$ is

not full rank modulo 2, abort (*i.e.* return error symbol $\perp$ and the random tape).

3. *(Sample solution pairs for each block.)* For all $i \in [\![1, m']\!]$, extend $\mathbf{A}_i$ to a rank-$w-1$ matrix $\widetilde{\mathbf{A}}_i$ using MatExtend procedure, then consume $w-n-1$ bits from the random tape to construct a vector $\mathbf{u}_i \in \mathbb{Z}_2^{w-n-1}$. Compute then the two solutions $\mathbf{x}^{(1)}$ and $\mathbf{x}^{(2)}$ to the equation $\widetilde{\mathbf{A}}_i\mathbf{x} = (\mathbf{y}_i \| \mathbf{u}_i)^\mathsf{T} \mod 2$, such that $\mathbf{x}_i^{(1)} \preccurlyeq \mathbf{x}_i^{(2)}$ in lexicographical order. Then, let $\mathbf{x}_i \triangleq \mathbf{x}_i^{(1)}$, and $\mathbf{z}_i \triangleq \mathbf{x}_i^{(2)} - \mathbf{x}_i^{(1)} \mod q$.

4. *(Merge block solutions.)* Let $\mathbf{x} \in \mathbb{Z}_2^m$, and $\mathbf{Z} \in \mathbb{Z}_q^{m \times m'}$ defined as follows:

$$\mathbf{x} \triangleq \begin{pmatrix} \mathbf{x}_1 \\ \hline \vdots \\ \hline \mathbf{x}_{m'} \end{pmatrix} \qquad \mathbf{Z} \triangleq \begin{bmatrix} \mathbf{z}_1 & & & \\ & \mathbf{z}_2 & & \\ & & \ddots & \\ & & & \mathbf{z}_{m'} \end{bmatrix}$$

where the empty spots in $\mathbf{Z}$ are zeroes. Note that $\mathbf{A}\mathbf{x} = \mathbf{y} \mod 2$, and $\mathbf{A}\mathbf{Z} = \sum_i \mathbf{A}_i\mathbf{z}_i = \mathbf{0} \mod 2$.

5. *(Apply next step of the recursion.)* Let $\mathbf{y}' \triangleq \frac{\mathbf{y}-\mathbf{A}\mathbf{x}}{2} \mod q' \in \mathbb{Z}_{q'}^n$ and $\mathbf{A}' \triangleq \frac{\mathbf{A}\mathbf{Z}}{2} \mod q' \in \mathbb{Z}_{q'}^{n \times m'}$. Run ISIS-Solver$(\mathbf{A}', \mathbf{y}')$ with parameters $(\ell - 1, n)$, and let $\mathbf{x}'$ denote the outcome. If $\mathbf{x}' = \perp$, abort (*i.e.* return error symbol $\perp$ and the random tape). Otherwise, return $\overline{\mathbf{x}} = \mathbf{x} + \mathbf{Z}\mathbf{x}' \mod q$.

Remark 3. We describe an example of an efficient deterministic matrix extension procedure in Appendix E to be used as the MatExtend subroutine.

Remark 4. Note in addition to the detailed sampling, another change in Algorithm 3 is that it now returns its random tape when aborting. An advantage with this formulation is that it ensures that the algorithm is perfectly randomness-recoverable, even when it aborts.

Random tapes notations. We describe the notations we use in this section when discussing Algorithm 3's internal randomness. First note that, at any level $\ell > 1$, Algorithm 2 constructs $m' = w^{\ell-1}$ blocks For each of them but the last one, n bits of randomness are consumed to sample the shares $\mathbf{y}_i$'s. And for each of them, $w - n - 1$ bits of randomness are consumed to sample the solutions. In total, $(m'-1)n + m'(w-n-1) = m'w - m' - n$ are consumed at each level $\ell > 1$, and n are consumed at level 1. We then describe the random tape associated to any level $\ell > 1$ a set of vectors $\left(\{\mathbf{y}_i\}_{i \in [\![1,m'-1]\!]}, \{\mathbf{u}_i\}_{i \in [\![1,m']\!]}\right)$, where $\mathbf{y}_i \in \mathbb{Z}_2^n$, and $\mathbf{u}_i \in \mathbb{Z}_2^{w-n-1}$, and the one associated to level 1 as a vector $\mathbf{u} \in \mathbb{Z}_2^{w-n}$. We denote the whole random tape (for all levels) $\overline{\mathcal{R}}$, and often write $\overline{\mathcal{R}} = \mathcal{R} \| \mathcal{R}'$, where $\mathcal{R}$ denotes the random tape for the current level, and $\mathcal{R}'$ denotes the one

for the next levels. Finally, we write $\mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}; \overline{\mathcal{R}})$ to denote the execution of Algorithm 3 with random tape $\overline{\mathcal{R}}$.

Randomness-recoverability of Algorithm 3. In the following, we state propositions to show that Algorithm 3 is solution-uniform, and randomness-recoverable. We start by showing that any two different random tapes lead to two different solutions (Proposition 12) and that the algorithm is full-support (Proposition 13) in the sense that it can output all possible solutions, which directly implies solution-uniformity. Finally, we prove that our algorithm is randomness-recoverable (Proposition 15).

Proposition 12. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$ and $m = w^\ell$. Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and $\mathbf{y} \in \mathbb{Z}_q^n$. For all pairs $(\overline{\mathcal{R}}_1, \overline{\mathcal{R}}_2)$ of random tapes for $\mathsf{ISIS\text{-}Solver}$, if $\overline{\mathcal{R}}_1 \neq \overline{\mathcal{R}}_2$, then $\mathsf{ISIS\text{-}Solver}(\mathbf{A}, y; \overline{\mathcal{R}}_1) \neq \mathsf{ISIS\text{-}Solver}(\mathbf{A}, y; \overline{\mathcal{R}}_2)$.*

Proof. First note that, if $\mathsf{ISIS\text{-}Solver}$ aborts on $\overline{\mathcal{R}}_1$ (resp. $\overline{\mathcal{R}}_2$), then the proof is immediate, as $\mathsf{ISIS\text{-}Solver}$ then returns $(\perp, \overline{\mathcal{R}}_1)$, (resp. $(\perp, \overline{\mathcal{R}}_2)$). We then focus on the case where none of the random tapes make the algorithm abort, and proceed by induction on ℓ. When $\ell = 1$, the matrix $\widetilde{\mathbf{A}}$ is square and of full-rank, which directly yields a one-to-one mapping between random tapes and solutions, and concludes the proof at this level.

When $\ell > 1$, let $\overline{\mathbf{x}}_1 \leftarrow \mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}; \overline{\mathcal{R}}_1)$, and $\overline{\mathbf{x}}_2 \leftarrow \mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}; \overline{\mathcal{R}}_2)$ for $\overline{\mathcal{R}}_1 \neq \overline{\mathcal{R}}_2$. We prove in the following that $\overline{\mathbf{x}}_1 \neq \overline{\mathbf{x}}_2$. Write $\overline{\mathcal{R}}_1$ as $(\mathcal{R}_1 \| \mathcal{R}'_1)$ and $\overline{\mathcal{R}}_2$ as $(\mathcal{R}_2 \| \mathcal{R}'_2)$, and distinguish two cases:

- Assume first that $\mathcal{R}_1 = \mathcal{R}_2$, and $\mathcal{R}'_1 \neq \mathcal{R}'_2$. Let $(\mathbf{x}_1, \mathbf{Z}_1)$ be the pair of inhomogeneous and homogeneous solutions produced by $\mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}; \overline{\mathcal{R}}_1)$ at level-ℓ, and $\mathbf{x}'_1 \triangleq \mathsf{ISIS\text{-}Solver}(\mathbf{A}', \mathbf{y}'; \mathcal{R}'_1)$. Similarly, let $(\mathbf{x}_2, \mathbf{Z}_2)$ be the pair of inhomogeneous and homogeneous solutions produced by $\mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}; \overline{\mathcal{R}}_2)$ at level-ℓ, and $\mathbf{x}'_2 \triangleq \mathsf{ISIS\text{-}Solver}(\mathbf{A}', \mathbf{y}'; \mathcal{R}'_2)$. Then, by induction hypothesis, we have $\mathbf{x}'_1 - \mathbf{x}'_2$, and by construction, we have $(\mathbf{x}_1, \mathbf{Z}_1) = (\mathbf{x}_2, \mathbf{Z}_2)$. Thus, $\overline{\mathbf{x}}_1 - \overline{\mathbf{x}}_2 = \mathbf{Z}_1(\mathbf{x}'_1 - \mathbf{x}'_2)$. As the kernel of $\mathbf{Z}_1$ is $\{\mathbf{0}\}$, $\overline{\mathbf{x}}_1 \neq \overline{\mathbf{x}}_2$.
- Assume now that $\mathcal{R}_1 \neq \mathcal{R}_2$, and let i be an block index such that $\mathcal{R}_{1,i} \neq \mathcal{R}_{2,i}$. Then, by construction, we have $\mathbf{x}_{1,i} \neq \mathbf{x}_{2,i}$, and $\mathbf{z}_{1,i} \neq \mathbf{z}_{2,i}$. Recall that $\overline{\mathbf{x}}_{1,i} = \mathbf{x}_{1,i} + \mathbf{z}_{1,i}\mathbf{x}'_1[i]$ is a solution to the equation $\widetilde{\mathbf{A}}_i \mathbf{x} = (\mathbf{y}_{1,i} \| \mathbf{u}_{1,i})^\mathsf{T} \mod 2$, and $\overline{\mathbf{x}}_{2,i} = \mathbf{x}_{2,i} + \mathbf{z}_{2,i}\mathbf{x}'_2[i]$ is a solution to the equation $\widetilde{\mathbf{A}}_i \mathbf{x} = (\mathbf{y}_{2,i} \| \mathbf{u}_{2,i})^\mathsf{T} \mod 2$. As $(\mathbf{y}_{1,i} \| \mathbf{u}_{1,i}) \neq (\mathbf{y}_{2,i} \| \mathbf{u}_{2,i})$, it directly comes $\overline{\mathbf{x}}_1 \neq \overline{\mathbf{x}}_2$, which concludes the proof.

Remark 5. Note that this proposition is the reason why we cannot sample each $\mathbf{x}_i$ by extending the block-matrix $\mathbf{A}_i$ to be a square matrix, hence fixing a single solution, and letting $\mathbf{z}_i$ be the difference between the two solutions produced by fixing the first $w - n - 1$ bits of randomness, and letting the last one free. Indeed, this would imply that two random tapes for a level ℓ that differ only on the last bit correspond to the same $\mathbf{z}_i$, and the second case "$\mathcal{R}_1 \neq \mathcal{R}_2$" would not carry over.

The following proposition states that our ISIS solver is full-support with probability almost 1.

Proposition 13. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$ and $m = w^\ell$. Let $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, and $\mathbf{y} \in \mathbb{Z}_q^n$. Then, for all $\overline{\mathbf{x}} \in \mathbb{Z}_q^m$ such that $\mathbf{A}\overline{\mathbf{x}} = \mathbf{y} \mod q$, and $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$.*

$$\Pr[\overline{\mathbf{x}} \in \mathrm{Supp}(\mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}))] = 1 - \mathsf{negl}(n)$$

where the probability is taken over $\mathbf{A} \leftarrow \mathbb{Z}_q^{n \times m}$.

Proof. We proceed by induction on ℓ. When $\ell = 1$, let $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$ such that $\mathbf{A}\overline{\mathbf{x}} = \mathbf{y} \mod 2$. Let $\mathbf{u} \in \mathbb{Z}_2^{w-n}$ such that $(\mathbf{y} \| \mathbf{u})^\mathsf{T} = \widetilde{\mathbf{A}}\overline{\mathbf{x}} \mod 2$, where $\widetilde{\mathbf{A}}$ is the matrix obtained by running the matrix extension $\mathsf{MatExtend}$ on input $\mathbf{A}$. Note that $\widetilde{\mathbf{A}}$ is a square matrix, so $\overline{\mathbf{x}}$ is the only solution of this equation. Thus, running $\mathsf{ISIS\text{-}Solver}$ on $(\mathbf{A}, \mathbf{y})$ with random tape $\mathbf{u}$ either yields $\perp$ if $\mathbf{A}$ is not full-rank, or yields $\overline{\mathbf{x}}$ otherwise. The former case only happens with negligible probability, which concludes the proof at this level.

Consider now a general level $\ell > 1$. Let $\overline{\mathbf{x}} \in \mathbb{Z}_q^m$ such that $\mathbf{A}\overline{\mathbf{x}} = \mathbf{y} \mod q$ and $\overline{\mathbf{x}} \in \mathbb{Z}_2^m$. We want to show that $\overline{\mathbf{x}}$ can be output by our ISIS solver algorithm, that is that $\overline{\mathbf{x}}$ can be written $\overline{\mathbf{x}} = \mathbf{x} + \mathbf{Z}\mathbf{x}'$ where $(\mathbf{x}, \mathbf{Z})$ is a pair of inhomogeneous-homogeneous solutions produced by the algorithm at this level, and $\mathbf{x}'$ is an output of the solver at the next level $\ell - 1$.

For all $i \in \{1, \ldots, m'\}$, let $(\mathbf{y}_i \| \mathbf{u}_i)^\mathsf{T} \triangleq \widetilde{\mathbf{A}}_i \overline{\mathbf{x}}_i \mod 2$, where $\widetilde{\mathbf{A}}_i$ is the extended block-matrix produced by $\mathsf{MatExtend}$. We construct $\mathbf{x}$ and $\mathbf{Z}$ as in algorithm $\mathsf{ISIS\text{-}Solver}$: for all i, let $\mathbf{x}_i \triangleq \mathbf{x}_i^{(1)}$, and $\mathbf{z}_i \triangleq \mathbf{x}_i^{(2)} - \mathbf{x}_i^{(1)}$, where $(\mathbf{x}_i^{(1)}, \mathbf{x}_i^{(2)})$ is the pair, sorted by lexicographical order, of solutions to the equation $\widetilde{\mathbf{A}}_i \overline{\mathbf{x}}_i = (\mathbf{y}_i \| \mathbf{u}_i)^\mathsf{T} \mod 2$ — note that $\overline{\mathbf{x}}_i \in \{\mathbf{x}_i^{(1)}, \mathbf{x}_i^{(2)}\}$ — and let $\mathbf{Z}$ be the corresponding block-columns matrix as defined in algorithm $\mathsf{ISIS\text{-}Solver}$. We then construct $\mathbf{x}'$ as follows: for all i,

$$\mathbf{x}'[i] \triangleq \begin{cases} 0 \text{ if } \mathbf{x}_i^{(1)} = \mathbf{x}_i \\ 1 \text{ otherwise} \end{cases}$$

It directly comes $\overline{\mathbf{x}} = \mathbf{Z}\mathbf{x}' \mod q$. Hence, by setting $\mathbf{A}' \triangleq \mathbf{A}\mathbf{Z}/2 \mod q'$, and $\mathbf{y}' \triangleq (\mathbf{y} - \mathbf{A}\mathbf{x})/2$ as in algorithm $\mathsf{ISIS\text{-}Solver}$, we have $\mathbf{A}'\mathbf{x}' = \mathbf{y}' \mod q'$. By induction hypothesis, this implies that, with probability $1 - \mathsf{negl}(n)$, there exists a random tape $\mathcal{R}'$ such that $\mathbf{x}' = \mathsf{ISIS\text{-}Solver}(\mathbf{A}', \mathbf{y}'; \mathcal{R})$. Thus, by setting $\mathcal{R} \triangleq ((\mathbf{y}_i \| \mathbf{u}_i)^\mathsf{T})_i$, and $\overline{\mathcal{R}} \triangleq \mathcal{R} \| \mathcal{R}'$, it comes $\overline{\mathbf{x}} = \mathsf{ISIS\text{-}Solver}(\mathbf{A}, \mathbf{y}; \overline{\mathcal{R}})$, which concludes the proof.

We can now conclude that our solver is almost solution-uniform.

Proposition 14. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$ and $m = w^\ell$. Let $\mathbf{y} \in \mathbb{Z}_q^n$. Then algorithm $\mathsf{ISIS\text{-}Solver}$ is $\mathsf{negl}(n)$-close to be solution-uniform.*

Proof. The proof immediately follows from propositions 12 and 13.

Proposition 15. *Let n, ℓ, and w be positive integers such that $w > cn$ for some constant $c > 1$, and let $q = 2^\ell$ and $m = w^\ell$. Then, for all $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$, Algorithm 3 is perfectly randomness-recoverable (Definition 16).*

Proof. We show that, given $\mathbf{A}$, $\mathbf{y}$, and any outcome of Algorithm 3, we can efficiently recover the random tape $\overline{\mathcal{R}}$ such that running Algorithm 3 on input $(\mathbf{A}, \mathbf{y})$ with random tape $\overline{\mathcal{R}}$ returns this outcome. With distinguish the following cases:

1. If the outcome is $(\perp, \overline{\mathcal{R}})$, we simply return $\overline{\mathcal{R}}$.
2. Else, if $\ell = 1$, the extended matrix $\widetilde{\mathbf{A}} \in \mathbb{Z}_2^{w \times w}$ produced by $\mathsf{MatExtend}$ procedure is a full-rank square matrix, hence there is a one-to-one mapping between the random tape $\mathcal{R} = \mathbf{u}$ and $\overline{\mathbf{x}}$. In this case, we then simply return $\mathbf{u} \triangleq \widetilde{\mathbf{A}}\overline{\mathbf{x}}$ as the random tape.
3. Else, if $\ell > 1$, the outcome is a solution $\overline{\mathbf{x}} \in \mathbb{Z}_2^{n \times m}$, and, by Proposition 12, there is a single way to write $\overline{\mathbf{x}}$ as $\mathbf{x} + \mathbf{Z}\mathbf{x}' \mod q$. We then recover the random tape $\mathcal{R}$ for this level by letting $(\mathbf{y}_i \| \mathbf{u}_i)^\mathsf{T} \triangleq \widetilde{\mathbf{A}}_i \overline{\mathbf{x}}_i \mod 2$, where $\widetilde{\mathbf{A}}_i$ is the extended matrix obtained when running $\mathsf{MatExtend}$ on $\mathbf{A}_i$, and then $\mathcal{R} \triangleq \{(\mathbf{y})_{i \in [\![1, m'-1]\!]}, (\mathbf{u})_{i \in [\![1, m']\!]}\}$. Then we follow steps 3 and 4 of Algorithm 3 to construct solution pairs $(\mathbf{x}_i, \mathbf{z}_i)$ for all $i \in [\![1, m']\!]$, and then construct $\mathbf{x}$ and $\mathbf{Z}$. Finally, we construct $\mathbf{x}' \in \mathbb{Z}_2^{m'}$ by setting its i-th coefficient to be $\mathbf{x}'[i] = 0$ if $\overline{\mathbf{x}}_i = \mathbf{x}_i$, and $\mathbf{x}'[i] = 1$ otherwise, and run this randomness-recovering procedure on $(\mathbf{A}', \mathbf{y}', \mathbf{x}')$ to get the random-tape $\mathcal{R}'$ of the next levels.

By construction, in all cases, running Algorithm 3 on the recovered random tape yield the expected outcome.

Putting everything together. By Propositions 11, 14 and 15, Algorithm 3 is perfectly randomness-recoverable, $\mathsf{negl}(n)$-solution-uniform, and runs in time $\mathsf{poly}(\log(n)\log(q))$. Then, by Theorems 2 and 3, we recover Proposition 2.

Extending to more general moduli. The correctness of Algorithm 2 naturally extends to general moduli. However, our strategy to make it full-support and randomness recoverable fails when considering moduli that are not powers of two. The reason is that the crux of our proof lies in the fact that at every step of the induction, the partial solution $\overline{\mathbf{x}} = \mathbf{x} + \mathbf{Z}\mathbf{x}' \mod q$ is small, *i.e.* belongs to $\mathbb{Z}_2^m$. To be able to keep it small, we need to find for every block matrix, a vector $\mathbf{z}_i \in \mathbb{Z}_q^m$ such that both (1) $\mathbf{A}_i\mathbf{z}_i = 0 \mod p$ and (2) the solutions of $\mathbf{A}_i\mathbf{x} = \mathbf{y}_i \mod p$ form a line $\{\mathbf{x}_i^{(1)} + \alpha\mathbf{z}_i \mod q \ : \ \alpha \in \mathbb{Z}_p\}$, where $\mathbf{x}_i^{(1)}$ is a fixed solution of this system (e.g. the smallest one, lexicographically-wise).

This is easily doable when $p = 2$, as there are only two such solutions, hence they always form a line. This is however not the case for a general modulo, even another power-of-prime where the prime is not 2. Thus, this strategy fails and it is still unclear to us how to generalize this algorithm with the full-support and randomness recoverability properties for such moduli. Interestingly, as discussed in [BJK+25, Section 4.3], the reason why their algorithm works only for power-of-two moduli is the same as ours.

Comparison with [BJK+25]. The algorithm of [BJK+25] starts with many independent states ($\overline{\text{EDCP}}$ samples), then applies a Kuperberg-like approach, consisting of recursively applying pairing-and-sieving operations which involve partial measurements to gradually build a "target state": a state whose Fourier amplitude concentrates on the secret s. This process is iterative, adaptive, and requires maintaining a large collection of quantum states.

In contrast, our algorithm directly manipulates a single structured quantum state. By applying a QFT, we obtain in one step a state whose support lies on an ISIS-type constraint. Coherently applying the ISIS solver allows us to recover the same type of target state. Our approach directly exploits the algebraic structure of the problem, allowing us to construct this target state in a single global step, and eliminating the need for explicit iterative pairing, sieving, or intermediate measurements.

Another advantage of our approach is that the quantum part of our algorithm is reduced to standard operations (mostly QFT) while the combinatorial complexity is delegated to the ISIS solver. This yields a cleaner and more modular decomposition and highlights the connection with the lattice structure.

Regarding quantum resources however, our approach should not be interpreted as better than the one of [BJK+25]: the overall complexity (time and memory) of [BJK+25] matches ours when using the best known ISIS solver in this regime. In particular, the large memory usage is not eliminated, but rather captured within the ISIS solver.

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 *IACR international workshop on public key cryptography*, 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.

Cha25. André Chailloux. Opi x soft decoders. *arXiv preprint arXiv:2511.22691*, 2025.

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 *Annual international conference on the theory and applications of cryptographic techniques*, 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 Remaud, 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.

II24. Muhammad Imran and Gábor Ivanyos. Efficient quantum algorithms for some instances of the semidirect discrete logarithm problem. *Designs, Codes and Cryptography*, 92(10):2825–2843, 2024.

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.

KOW25. Robin Kothari, Ryan O'Donnell, and Kewen Wu. No exponential quantum speedup for SIS^∞ anymore. *arXiv preprint arXiv:2510.07515*, 2025.

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 $S|\mathrm{LWE}\rangle$

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 $|\psi_{\mathbf{s}}\rangle = \sum_{\mathbf{e}\in\mathbb{Z}_q^m} f(\mathbf{e})|\mathbf{A}^\mathsf{T}\mathbf{s}+\mathbf{e}\rangle$. 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 5, 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 [BKMH97].

B Instantiation of our forward theorem with Gaussian distributions

We directly define the discrete Gaussian probability function.

Definition 17. *Let $r > 0$. We define the Gaussian probability function of parameter σ as follows*

$$\rho_r(x) = \frac{e^{-\frac{\pi x^2}{r^2}}}{\sum_{y\in\mathbb{Z}_q} e^{-\frac{\pi y^2}{r^2}}}.$$

The discrete Gaussian distribution has

Proposition 16. *Let $\sigma > 0$ and let $f = \sqrt{\rho_r(x)}$. We have $\widehat{f} = \sqrt{\rho_{r^*}} + o(1)$, with $r^* = \frac{q}{2r}$. Moreover, for $T = \{\mathbf{x} \in \mathbb{Z}_q^m : \|\mathbf{x}\|_2 \leq \sqrt{m}\frac{q}{\sqrt{8\pi}r}\}$, we have $\sum_{\mathbf{y}\in T} |\widehat{f}(\mathbf{y})|^2 = \Theta(1)$.*

Proof. First notice that f is proportional to $\rho_{\sqrt{2}r}$. The Poisson formula in the continuous setting tells us that the Fourier transform of a Gaussian of parameter r is a Gaussian of parameter $\frac{q}{r}$. This also holds approximately for the discrete Gaussian (see for instance [DFS24], Lemma 4) which tells us $\widehat{f} = \rho_{\frac{q}{\sqrt{2}r}} + o(1) = \sqrt{\rho_{\frac{q}{2r}}} + o(1)$. For the second part, we just use that a vector in $\mathbb{Z}_q^m$ where each coordinate is chosen according to a Gaussian distribution of parameter $\frac{q}{2r}$ has typical 2-norm $\sqrt{m}\frac{q}{\sqrt{8\pi}r}$.

As a direct corollary, using this in Theorem 1, we obtain the following statement

Proposition 17. *Let $r > 0$. If we have an efficient algorithm for $S|LWE\rangle(\mathbf{A}, \sqrt{\rho_r})$, or if we have an efficient algorithm for $LWE(\mathbf{A}, \rho_r)$, then we have an efficient quantum algorithm for $ISIS_2(\mathbf{A}, \sqrt{\frac{qm}{8\pi r}})$.*

C Proof of reverse reduction with almost randomness recoverable algorithms for ISIS

In this section, we extend Theorem 3 to the theorem below

Theorem 4. *Let A be an algorithm for $ISIS(\mathbf{A}, T)$ with time complexity t. Assume the following properties:*

- *A is ε-close to being solution-uniform i.e. if we define $p_{\mathbf{y}}(\mathbf{x}) = \Pr_{\mathbf{r}\leftarrow\{0,1\}^\ell}(\mathsf{A}(\mathbf{y}, \mathbf{r}) = \mathbf{x})$, 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 $p_{\mathbf{y}}$ and the probability function $u_{\mathbf{y}} = \frac{1}{|T\cap\Lambda_{\mathbf{y}}^\perp(\mathbf{A})|}\mathbb{1}_{T\cap\Lambda_{\mathbf{y}}^\perp(\mathbf{A})}$.

– A *is* ε'*-randomness-recoverable; let* E *denote a randomness-extractor for* A *succeeding with probability* $1-\varepsilon'$*. That is, for all* $\mathbf{y} \in \mathbb{Z}_q^n$*,*

$$\Pr\left[\mathsf{E}(\mathbf{y}, \mathsf{A}(\mathbf{y}; r)) = r \,:\, r \leftarrow \{0,1\}^\ell\right] = 1 - \varepsilon'.$$

Then there exists an efficient algorithm solving $IC|LWE\rangle(\mathbf{A}, f)$ *with* $\widehat{f} = \mathbb{1}_T$ *with fidelity* $1 - \varepsilon - \varepsilon'$ *and time complexity* $\mathsf{poly}(t)$*.*

Remark 6. We do not explicitly say anything about the success probability of the algorithm 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 $|\mathbf{y}\rangle$ 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 then A coherently over the first and second registers and store the result in a third register, then swap the second and third registers. The resulting state is

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

Apply now the randomness-extractor E coherently over the first and second registers, and substract the result from the second one; let $|\psi_{\mathbf{y}}\rangle$ denote the resulting state:

$$|\psi_{\mathbf{y}}\rangle = \frac{1}{\sqrt{2^\ell}}|\mathbf{y}\rangle \sum_{r\in\{0,1\}^\ell} |\mathsf{A}(\mathbf{y}; r)\rangle|r - \mathsf{E}(\mathbf{y}, \mathsf{A}(\mathbf{y}; r))\rangle$$

Consider now a state $|\psi'_{\mathbf{y}}\rangle$ constructed in the same way with an "ideal" ISIS-solver A', that is a perfectly solution-uniform and perfectly randomness-recoverable — with corresponding ideal randomness-extractor E' — solver:

$$|\psi'_{\mathbf{y}}\rangle = \frac{1}{\sqrt{2^\ell}}|\mathbf{y}\rangle \sum_{r\in\{0,1\}^\ell} |\mathsf{A}'(\mathbf{y}; r)\rangle|0\rangle$$

where the last register is $|0\rangle$ because the randomness-extractor is perfect. We now discard this last register, and apply an inverse QFT to the second register. By Proposition 4, this yields $|\mathbf{y}\rangle|W_{\mathbf{y}}\rangle$.

It remains to show that, averaged over $\mathbf{y}$, the overlap between $|\psi_{\mathbf{y}}\rangle$ and $|\psi'_{\mathbf{y}}\rangle$ is larger than $1-\varepsilon-\varepsilon'$. We have

$$\begin{aligned}\left|\langle\psi_{\mathbf{y}}|\psi'_{\mathbf{y}}\rangle\right| &= \frac{1}{2^\ell}|\mathbf{y}\rangle \sum_{r,r'\in\{0,1\}^\ell} \langle \mathsf{A}(\mathbf{y};r)|\mathsf{A}'(\mathbf{y};r')\rangle\langle r-\mathsf{E}(\mathbf{y},\mathsf{A}(\mathbf{y};r))|0\rangle \\ &= \frac{1}{2^\ell}|\mathbf{y}\rangle \sum_{r\in\{0,1\}^\ell} \left(\sum_{r'\in\{0,1\}^\ell} \langle \mathsf{A}(\mathbf{y};r)|\mathsf{A}'(\mathbf{y};r')\rangle\right) \langle r-\mathsf{E}(\mathbf{y},\mathsf{A}(\mathbf{y};r))|0\rangle\end{aligned}$$

Now, because A' is perfectly solution-uniform and perfectly randomness-recoverable, there is, for every r, at most a single r' such that $\mathsf{A}(\mathbf{y};r)=\mathsf{A}'(\mathbf{y};r')$. Hence the first overlap $\sum_{r'\in\{0,1\}^\ell}\langle \mathsf{A}(\mathbf{y};r)|\mathsf{A}'(\mathbf{y};r')\rangle$ is 1 if $\mathsf{A}(\mathbf{y};r)\in \Lambda^\perp_{\mathbf{y}}\cap T$, and 0 otherwise. Furthermore, the second overlap $\langle r-\mathsf{E}(\mathbf{y},\mathsf{A}(\mathbf{y};r))|0\rangle$ is 1 if $r=\mathsf{E}(\mathbf{y},\mathsf{A}(\mathbf{y};r))$, and 0 otherwise. It comes

$$\begin{aligned}\left|\langle\psi_{\mathbf{y}}|\psi'_{\mathbf{y}}\rangle\right| &= \Pr_{r\leftarrow\{0,1\}^\ell}\left[\mathsf{A}(\mathbf{y};r)\in\Lambda^\perp_{\mathbf{y}} \wedge \mathsf{E}(\mathsf{A}(\mathbf{y};r))=r\right] \\ &= 1-\Pr_{r\leftarrow\{0,1\}^\ell}\left[\mathsf{A}(\mathbf{y};r)\notin\Lambda^\perp_{\mathbf{y}} \vee \mathsf{E}(\mathsf{A}(\mathbf{y};r))\neq r\right]\end{aligned}$$

By definition of statistical distance, we have $\Pr_{r\leftarrow\{0,1\}^\ell}\left[\mathsf{A}(\mathbf{y};r)\notin\Lambda^\perp_{\mathbf{y}}\right]\leq\epsilon$, and $\Pr_{r\leftarrow\{0,1\}^\ell}[\mathsf{E}(\mathsf{A}(\mathbf{y};r))\neq r]=\epsilon'$ by definition of an ϵ'-randomness-recoverable solver. Applying union bound thus gives us $\left|\langle\psi_{\mathbf{y}}|\psi'_{\mathbf{y}}\rangle\right|\geq 1-\varepsilon-\varepsilon'$ which concludes the proof.

D Proof of Theorem 2

This section will be devoted to the proof of Theorem 2. We first prove the following lemma.

Lemma 4. *The unitary U that for each $\mathbf{y}\in\mathbb{Z}_q^n$ satisfies $U:|W_{\mathbf{y}}\rangle|0\rangle\to|W_{\mathbf{y}}\rangle|\mathbf{y}\rangle$ 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 4:

$$\begin{aligned}|W_{\mathbf{y}}\rangle|0\rangle \xrightarrow{QFT_{\mathbb{Z}_q^m}\otimes I} \frac{q^n}{\sqrt{w_{\mathbf{y}}}}\sum_{\mathbf{x}\in\Lambda^\perp_{\mathbf{y}}(\mathbf{A})}\widehat{f}(\mathbf{x})|\mathbf{x}\rangle|0\rangle \xrightarrow{V_{\mathbf{A}}} \frac{q^n}{\sqrt{w_{\mathbf{y}}}}\sum_{\mathbf{x}\in\Lambda^\perp_{\mathbf{y}}(\mathbf{A})}\widehat{f}(\mathbf{x})|\mathbf{x}\rangle|\mathbf{y}\rangle \\ \xrightarrow{QFT^\dagger_{\mathbb{Z}_q^m}\otimes I} |W_{\mathbf{y}}\rangle|\mathbf{y}\rangle.\end{aligned}$$

We can now prove our theorem

Proof. We start from an efficient unitary U for $IC|\mathrm{LWE}\rangle(\mathbf{A},f)$.

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

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

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

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

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

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

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 5), and apply the unitary from Lemma 4 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

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

where $\gamma_{\mathbf{y}} = |\langle W_{\mathbf{y}} | W'_{\mathbf{y}} \rangle|$. In order to prove this statement, we define $\varepsilon_y = 1 - \sqrt{\frac{w_{\mathbf{y}}}{q^n}}$ 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 $\mathbb{E}_{\mathbf{y}} \left[(1 - \varepsilon_{\mathbf{y}})^2 \right] = 1$ 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 $\mathbb{E}_{\mathbf{y}} \left[\varepsilon'_{\mathbf{y}} \right] = \varepsilon'$
- Each $\gamma_{\mathbf{y}} \in [0, 1]$ so each $\varepsilon'_{\mathbf{y}} \in [0, 1]$ and $\mathbb{E}_{\mathbf{y}} \left[\varepsilon'^2_{\mathbf{y}} \right] \leq \mathbb{E}_{\mathbf{y}} \left[\varepsilon'_{\mathbf{y}} \right] = \varepsilon'$.

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

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

Now, using the Cauchy-Schwarz inequality, we obtain

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

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 $\mathbb{E}_{\mathbf{s}} \left[|\langle \psi'_{\mathbf{s}} | B_{\mathbf{s}} \rangle|^2 \right]$, we get the desired result.

E Matrice Extension Subroutine

We describe in this section an example of a deterministic matrix extension procedure to be used as the MatExtend procedure in Algorithm 3. It takes a rank-n matrix $\mathbf{A} \in \mathbb{Z}_2^{n \times w}$ as input, as well as an integer $r \in [\![n, w]\!]$, and returns an "extended" matrix $\widetilde{\mathbf{A}} \in \mathbb{Z}_2^{r \times w}$ of rank r, and such that the first n rows of $\widetilde{\mathbf{A}}$ exactly form the matrice $\mathbf{A}$.

Procedure (P1) Extend a full rank matrix in $\mathbb{Z}_2^{n \times w}$ to a rank-r matrix in $\mathbb{Z}_2^{r \times w}$ deterministically.

Input: A matrix $\mathbf{A} \in \mathbb{Z}_2^{n \times w}$ of rank n, and an integer $r \in [\![n, w]\!]$.
Output: A matrix $\widetilde{\mathbf{A}} \in \mathbb{Z}_2^{r \times w}$ of rank r, and whose first n rows are $\mathbf{A}$.

Let $\mathbf{e}_i^\top$ be the row vector in $\mathbb{Z}_2^w$ with a 1 at position i and 0 everywhere else.
$\widetilde{\mathbf{A}} \leftarrow \mathbf{A}$
$i \leftarrow 0$
while $\mathrm{rank}(\widetilde{\mathbf{A}}) < r$ **do**
    $\widetilde{\mathbf{A}}' = \left[\begin{array}{c} \widetilde{\mathbf{A}} \\ \hline \mathbf{e}_i^\top \end{array}\right]$ ▷ Append row $\mathbf{e}_i^\top$ to $\widetilde{\mathbf{A}}$
    if $\mathrm{rank}(\widetilde{\mathbf{A}}') > \mathrm{rank}(\widetilde{\mathbf{A}})$ **then**
        $\widetilde{\mathbf{A}} \leftarrow \widetilde{\mathbf{A}}'$
    end if
    $i \leftarrow i + 1$
end while
return $\widetilde{\mathbf{A}}$
