Exact Coset Sampling for Quantum Lattice Algorithms

Yifan Zhang

yifanzhangresearch@gmail.com

January 11, 2026

Abstract

We revisit the post-processing phase of Chen's Karst-wave quantum lattice algorithm [Chen, 2024] in the Learning with Errors (LWE) parameter regime. Conditioned on a transcript E, the post-Step 7 coordinate state on $(\mathbb{Z}_M)^n$ is supported on an affine grid line

$$\{\, j\Delta + \boldsymbol{v}^*(E) + M_2\boldsymbol{k} \bmod M : j \in \mathbb{Z},\ \boldsymbol{k} \in \mathcal{K}\,\},$$

with $\Delta = 2D^2\mathbf{b}$, $M = 2M_2 = 2D^2Q$, and Q odd. The amplitudes include a quadratic Karst-wave chirp $\omega_Q^{-j^2}$ and an unknown run-dependent offset $\boldsymbol{v}^*(E)$. We show that Chen's Steps 8-9 can be replaced by a single exact post-processing routine: measure the deterministic residue $\tau := X_1 \bmod D^2$, obtain the run-local class $v_{1,Q} := v_1^*(E) \bmod Q$ as explicit side information in our access model, apply a $v_{1,Q}$-dependent diagonal quadratic phase on X_1 to cancel the chirp, and then apply $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the coordinate registers. The routine never needs the full offset $\boldsymbol{v}^*(E)$. Under Additional Conditions AC1-AC5 on the front end, a measured Fourier outcome $\boldsymbol{u} \in \mathbb{Z}_M^n$ satisfies the resonance $\langle \mathbf{b}, \boldsymbol{u}\rangle \equiv 0 \pmod{Q}$ with probability $1 - \mathrm{negl}(n)$. Moreover, conditioned on resonance, the reduced outcome $\boldsymbol{u} \bmod Q$ is *exactly* uniform on the dual hyperplane $H = \{\boldsymbol{v} \in \mathbb{Z}_Q^n : \langle \mathbf{b}, \boldsymbol{v}\rangle \equiv 0 \pmod{Q}\}$.

1 Introduction

Fourier sampling quantum algorithms for lattice problems prepare a structured superposition, and a Fourier transform then reveals modular linear structure [Regev, 2004, 2009]. Chen's windowed quantum Fourier transform (QFT) with complex Gaussian windows [Chen, 2024] fits this pattern. The n coordinate registers of the post-Step 7 state $|\widetilde{\varphi}_7\rangle$ live in $\mathbb{Z}_M$, with $M = 2M_2$. The one-shot routine in Algorithm 1 performs the run-local phase correction described below and then applies $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ directly to these registers. The post-Step 7 state has affine support

$$|\widetilde{\varphi}_7\rangle = \sum_{j\in\mathbb{Z}} \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_E(j,\boldsymbol{k})\, \omega_Q^{-j^2}\, i^{\|\boldsymbol{k}\|^2}\ |\mathbf{X}(j) + M_2\boldsymbol{k}\rangle_M\,, \tag{1.1}$$

for an outcome-dependent amplitude profile $\alpha_E(j,\boldsymbol{k})$ and an index set $\mathcal{K} \subseteq \{0\} \times \{0,1\}^{n-1}$ that comes from the grid-state construction. When it is clear from context, we suppress the transcript index E. The phase factor $i^{\|\boldsymbol{k}\|^2}$ comes from Chen's grid-state preparation procedure. We view the coordinate values as elements of $(\mathbb{Z}_M)^n$ throughout. Accordingly, $\mathbf{X}(j) := 2D^2 j\,\mathbf{b} + \boldsymbol{v}^*$ is interpreted componentwise modulo M, and $\boldsymbol{k}$ records the M_2-shift term $M_2\boldsymbol{k}$. Reducing the coordinate registers modulo M_2 eliminates this shift and yields the affine congruence $\mathbf{X}(j) \equiv 2D^2 j\,\mathbf{b} + \boldsymbol{v}^* \pmod{M_2}$ used in Additional Condition AC1.

The additional factor $\omega_Q^{-j^2} = \exp(-2\pi i j^2/Q)$ is the Karst-wave chirp. Step 9† removes it using only the first coordinate register and the run-local residue $v_{1,Q} = v_1^*(E) \bmod Q$ promised by Additional Condition AC4. We denote the chirp-free state obtained after this run-local phase correction by $|\varphi_7\rangle$; it satisfies

$$|\varphi_7\rangle = \sum_{j\in\mathbb{Z}} \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_E(j,\boldsymbol{k})\, i^{\|\boldsymbol{k}\|^2}\ |\mathbf{X}(j) + M_2\boldsymbol{k}\rangle_M\,. \tag{1.2}$$

Additional Condition AC4 isolates the only extra access needed to cancel the Karst-wave chirp using only the first coordinate register: after measuring the deterministic residue $\tau := X_1 \bmod D^2$, the post-processing must obtain the run-local class $v_{1,Q} := v_1^*(E) \bmod Q$. This information is *not* implied by AC1 alone; in our access model, it is provided as a short run-local gauge value. If the gauge value is available coherently inside the preparation, one can compile a canonical-gauge variant with $\lambda(E) = 0$ (Proposition 2.3), in which case $v_{1,Q} = \mathrm{ctr}(\tau) \bmod Q$. Under Additional Condition AC1, the first coordinate satisfies the precise congruence

$$X_1(j) \equiv -2D^2 j + v_1^*(E) \pmod{M_2}$$

for every j in the effective window. Write $\Delta := 2D^2\mathbf{b}$ and recall $M = 2M_2 = 2D^2Q$. Since $D^2, Q \mid M$, reducing any physical basis value $x \in \mathbb{Z}_M$ modulo D^2 or Q is unambiguous. In particular,

$$X_1 \bmod D^2 \equiv v_1^* \bmod D^2, \qquad (X_1 \bmod Q) - v_{1,Q} \equiv -2D^2 j \pmod{Q},$$

where under AC4 the post-processing computes $v_{1,Q} = v_1^*(E) \bmod Q$ from $\tau = X_1 \bmod D^2$ together with the run-local gauge value.

In Chen's post-processing, one ultimately outputs non-zero Fourier samples in $\mathbb{Z}_{M_2}^n$ (with $M_2 = M/2$) whose reduction modulo $Q = M/(2D^2)$ satisfies a homogeneous dual relation. In our direct-QFT variant, we instead measure $\boldsymbol{u} \in \mathbb{Z}_M^n$ and store only the reduction $\boldsymbol{u}_Q := \boldsymbol{u} \bmod Q$. In either view, the goal is to obtain non-zero vectors satisfying

$$\langle \mathbf{b}, \boldsymbol{u}\rangle \equiv 0 \pmod{Q}, \tag{1.3}$$

where $Q := \frac{M}{2D^2}$ is an odd integer. The short vector $\mathbf{b} = (b_1, \ldots, b_n) \in \mathbb{Z}^n$ stores the hidden data and satisfies the normalization $b_1 = -1$. The offset $\boldsymbol{v}^*$ is unknown and can change from run to run. The algorithm then collects $O(n)$ such samples and solves the resulting linear system modulo Q to recover $\mathbf{b} \bmod Q$ and hence the hidden data vector.

Chen's published Steps 8-9 enforce relations of the form Equation (1.3) via additional offset-handling and a domain-extension mechanism that is tailored to a particular parameterization. Step 9† provides an alternative post-processing designed for an access model in which the affine offset $\boldsymbol{v}^*(E)$ may vary across runs and no special factorization of Q is assumed. It uses only the affine structure $\mathbf{X}(j) = j\Delta + \boldsymbol{v}^*$ with $\Delta = 2D^2\mathbf{b}$, the normalization $b_1 = -1$, a run-local chirp cancellation acting on X_1 (Additional Condition AC4), and a direct $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ on the coordinate registers. Under Additional Condition AC5, the resulting outcomes satisfy $\langle \mathbf{b}, \boldsymbol{u}\rangle \equiv 0 \pmod{Q}$ except with negligible failure probability.

When we instantiate the front end with the q-ary lattice $L_q^{\perp}(\mathbf{A})$ from Chen [2024], the new Step $9^{\dagger}$ recovers the planted shortest vector $\mathbf{b} = [-1, 2p_1 s^{\top}, 2p_1 e^{\top}]^{\top}$ and hence the LWE secret s and error e in the chosen-secret regime considered there. Combined with the classical reductions of Chen [2024], this yields a quantum algorithm for standard LWE in the same parameter regime, conditional on Additional Conditions AC1-AC5.

2 Background and Access Model

Notations. Let $q \in \mathbb{N}$ and write $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$ with representatives in $(-\frac{q}{2}, \frac{q}{2}]$. Vectors are written in bold. We use $\langle \cdot, \cdot \rangle$ for the inner product. For $T \in \mathbb{N}$ we write $\omega_T := \exp(2\pi i/T)$. The *physical* coordinate registers live in $\mathbb{Z}_M^n$, where

$$M := 2M_2 = 2D^2Q, \qquad M_2 := D^2Q.$$

We will repeatedly reduce physical basis values $x \in \mathbb{Z}_M$ modulo M_2, D^2, or Q. Since $D^2, Q \mid M_2 \mid M$, the canonical reduction maps

$$\mathbb{Z}_M \to \mathbb{Z}_{M_2}, \qquad \mathbb{Z}_M \to \mathbb{Z}_{D^2}, \qquad \mathbb{Z}_M \to \mathbb{Z}_Q$$

are well-defined ring homomorphisms.

Modular inner products. For $\boldsymbol{a} \in \mathbb{Z}^n$ and $\boldsymbol{u} \in (\mathbb{Z}_M)^n$ we write

$$\langle \boldsymbol{a}, \boldsymbol{u} \rangle \bmod Q \;:=\; \sum_{i=1}^{n} (a_i \bmod Q) \cdot (u_i \bmod Q) \;\in\; \mathbb{Z}_Q.$$

When we write $\langle \boldsymbol{a}, \boldsymbol{u} \rangle \equiv 0 \pmod{Q}$, this is the intended meaning.

Representative conventions. We use the standard representatives in $\{0, \ldots, M-1\}$ for $\mathbb{Z}_M$. All coordinate-register kets $|\cdot\rangle_M$ are labelled by elements of $\mathbb{Z}_M$ in these representatives. We also routinely identify $t \in \mathbb{Z}_T$ with its representative in $\{0, \ldots, T-1\}$ when evaluating phases ω_T^t. When we refer to reductions modulo M_2, D^2, or Q, we always mean the canonical ring homomorphisms from $\mathbb{Z}_M$.

We write

$$0 \,|\, \mathbb{Z}^{n-1} := \{0\} \times \mathbb{Z}^{n-1}.$$

We also use

$$0 \,|\, \{0,1\}^{n-1} := \{0\} \times \{0,1\}^{n-1}.$$

Since $M_2 = M/2$, the basis shift $M_2\boldsymbol{k} \bmod M$ depends only on $\boldsymbol{k} \bmod 2$ (because $M_2(\boldsymbol{k} + 2\boldsymbol{e}_i) \equiv M_2\boldsymbol{k} \pmod{M}$), and the phase $i^{\|\boldsymbol{k}\|^2}$ depends only on $\boldsymbol{k} \bmod 2$. Accordingly, throughout we fix $\mathcal{K} \subseteq 0 \,|\, \{0,1\}^{n-1}$ as a set of parity representatives. Whenever the front end naturally produces a sum over a larger grid index set (e.g. $\boldsymbol{k} \in 0 \,|\, \mathbb{Z}^{n-1}$ as in Chen's expression), we implicitly *group* all terms with the same parity class $\boldsymbol{k} \bmod 2$ into a single coefficient. Thus, restricting to $\mathcal{K}$ incurs no loss of generality: any dependence on $\boldsymbol{k} + 2\mathbb{Z}^{n-1}$ is absorbed into the amplitudes $\alpha_E(j, \boldsymbol{k})$.

The physical coordinate block in Chen's Step 7 lives in $\mathbb{Z}_M$ with $M = 2M_2$. When this helps to avoid confusion, we write the reduction modulo M with a subscript $_M$. For a coordinate slice we write $\boldsymbol{x}_{[2..n]} := (x_2, \ldots, x_n)$. Set $\Delta := 2D^2\,\mathbf{b} \in \mathbb{Z}^n$.

We use $\mathrm{poly}(\cdot)$ for an unspecified fixed polynomial and $\mathrm{negl}(n)$ for a negligible function of n. In the intended LWE instantiation (Definition 2.1) we have $Q = \mathrm{poly}(n)$, hence $Q^{-(n-1)} = \mathrm{negl}(n)$.

Idealized unitaries vs. circuit precision. For clarity, we treat $\mathrm{QFT}_{\mathbb{Z}_M}$ and the controlled root-of-unity phases used in the chirp correction (AC4) as exact unitaries. In a standard uniform gate set, these operations can be implemented to precision $2^{-\operatorname{poly}(n)}$, which perturbs all output distributions by at most $\operatorname{negl}(n)$ in total variation distance. We suppress this approximation issue throughout, since it does not affect any of the modular-algebraic arguments. See, e.g., standard treatments of approximate QFT and fault-tolerant synthesis [Nielsen and Chuang, 2010].

Finally, we write $\operatorname{ctr} : \mathbb{Z}_{D^2} \to \mathbb{Z}$ for the centered lift: for $\tau \in \mathbb{Z}_{D^2}$, $\operatorname{ctr}(\tau)$ is the unique integer in $(-D^2/2, D^2/2]$ that is congruent to τ modulo D^2. We use $\operatorname{ctr}(\tau)$ as a canonical integer representative when converting $\tau = X_1 \bmod D^2$ into arithmetic in $\mathbb{Z}_Q$.

At the frontier right before Step 8, and for fixed outcomes E, Lemma 2.8 gives $\mathbf{X}(j) \equiv j\boldsymbol{\Delta} + \boldsymbol{v}^*$ (mod M_2) for every j in the effective window.

Parameter identification from Chen [2024]. In Chen's notation, $M = 2(t^2+u^2)$ and $x = D\mathbf{b}$, where $\mathbf{b}$ is the short vector from the LWE-to-lattice reduction (Eq. (12) in Chen [2024]). We follow this identification. Chen's Step 9 defines a relabelled vector $\mathbf{b}^*$. Our post-processing never uses $\mathbf{b}^*$. We keep all formulas in terms of $\mathbf{b}$ instead.

Under Chen's parameter constraints, the quantity $M/(2D^2)$ is an odd integer. We write

$$Q := \frac{M}{2D^2}, \qquad M_2 := \frac{M}{2} = D^2 Q.$$

In Chen's concrete instantiation, Q happens to admit a factorization into pairwise coprime odd factors, the new Step $9^\dagger$ does not use this extra structure and only relies on Q being odd.

Chen uses the letter P for a large loop modulus with $P \approx M^2/2$. We keep this convention and reserve P only for that modulus.

Index domain vs. first coordinate. The preparation uses a loop index j. This index is the discrete time variable of the Karst wave and appears in Chen [2024] as a summation index. It runs over the large modulus P. We denote the register by $J \in \mathbb{Z}_P$.

The first coordinate satisfies

$$X_1 \equiv 2D^2 j\, b_1 + v_1^* \pmod{M_2}.$$

In Chen's setup, v_1^* depends on the measurement outcomes $(y', z', h^\star)$. The experiment cannot be reset in a controlled way to obtain the same outcomes and the same v^*. So we cannot query the state preparation on chosen basis inputs j and then compute $\mathbf{X}(j)$ either classically or into an extra register. We must work with the single quantum state $|\varphi_7\rangle$ that a successful run outputs.

Parameter re-tuning. As in Chen [2024] we run a classical outer loop over polynomially many candidates for $\|\mathbf{b}\|^2$ and, for each guess, set

$$Q = (c{+}1)\|\mathbf{b}\|^2, \qquad M = 2D^2 Q, \qquad M_2 = D^2 Q.$$

The scaling parameter D can then be chosen (odd, $\gcd(D, Q) = 1$, and $\operatorname{poly}(n)$-bounded) to satisfy the geometric separation requirement of the Karst-wave front end (Condition C.6 of Chen [2024]). The only additional analytic requirement used by Step $9^\dagger$ is the one-dimensional spectral concentration property recorded in Additional Condition AC5, which is achieved in Chen's complex-Gaussian regime once the loop-envelope width satisfies $\sigma_J \gtrsim Q \log n$ (Remark 2.5). All subsequent correctness statements are conditional on the existence of a re-tuned front-end configuration satisfying Definition 2.1 and Additional Conditions AC1-AC5.

Definition 2.1 (Re-tuned Karst-wave configuration)**.** Take LWE parameters (ℓ, m, q, β) in the regime of Chen [2024] and set $n := 1 + \ell + m$. Let $L_q^{\perp}(\mathbf{A})$, the planted shortest vector $\mathbf{b}$, and the integers $(p_\eta)_\eta = (p_1, \ldots, p_\kappa)$ be as in Section 3.2 of Chen [2024]. We assume $\kappa \geq 2$ and $\kappa - 1 \leq \ell$, so that the $(\kappa - 1)$ chosen secret coordinates fit in the ℓ-dimensional secret. A *re-tuned Karst-wave configuration* is any choice of front-end parameters

$$(c, D, r, s, t, u, P, M, Q)$$

that satisfies the following properties.

(R1) The integers $p_1, \ldots, p_\kappa$ are odd and pairwise coprime. They control the chosen-secret embedding and the parsing of $\mathbf{b}$ in the LWE extraction step, but they do not impose any algebraic constraint on Q. Fix an integer $c = c(n) \in 4\mathbb{Z}$ (typically $c = \Theta(\log^6 n)$ in Chen-style instantiations) and set

$$Q := (c{+}1)\|\mathbf{b}\|^2.$$

In the chosen-secret LWE embedding of [Chen, 2024], $\mathbf{b} = [-1, 2p_1 s^\top, 2p_1 e^\top]^\top$ has one odd coordinate and all remaining coordinates even, hence $\|\mathbf{b}\|^2 \equiv 1 \pmod 4$. Since $c \in 4\mathbb{Z}$, this makes $Q = (c{+}1)\|\mathbf{b}\|^2$ automatically odd. We also require that Q satisfies

$$\|\mathbf{b}\|_\infty \leq 2p_1\beta \log n < Q/2,$$

so that $\mathbf{b} \bmod Q$ uniquely determines $\mathbf{b}$ by centered lifting.

(R2) Choose an odd scaling parameter D that is coprime to Q and polynomially bounded in n (for concreteness, one may take the smallest odd integer at least $32 \log^2 n$ with $\gcd(D, Q) = 1$). Define

$$u^2 := \|D\mathbf{b}\|^2 = D^2\|\mathbf{b}\|^2, \qquad t^2 := c\, u^2,$$

and set the Karst-wave moduli

$$M := 2(t^2 + u^2) = 2D^2 Q, \qquad M_2 := M/2 = D^2 Q, \qquad P := M(t^2 + u^2) = \frac{M^2}{2}.$$

Then $2D^2$ is a unit modulo Q.

(R3) Choose $r, s > 0$ so that Chen's Karst-wave constraints C.5-C.7 hold, and the resulting geometric width parameter

$$\sigma_{\text{geom}} := \frac{rs^2 t}{u\sqrt{r^4 + s^4}}$$

obeys $2 \log n < \sigma_{\text{geom}} < D/(4 \log n)$. Chen's analysis shows that such choices exist with all parameters bounded by $\text{poly}(n)$; we fix one such choice.

(R4) For the resulting complex-Gaussian front end, let σ_J denote the standard deviation of the one-dimensional envelope $\alpha_E(j)$ along the loop index j. We restrict to parameter choices satisfying

$$\sigma_J \geq C_{\text{spec}}\, Q \log n$$

for some fixed absolute constant $C_{\text{spec}} > 0$. A lower bound of this form keeps the spectral leakage in Additional Condition AC5 bounded by $\exp(-\Omega(\log^2 n))$. In contrast, the geometric width parameter σ_{geom} in (R3) controls the *within-ball* width of each extracted Gaussian ball in coordinate space; these are distinct quantities in Chen's regime.

When we refer to Chen's front end with re-tuned parameters below, we mean an outcome-conditioned circuit family compiled with a fixed choice of parameters that satisfies (R1)-(R4).

2.1 Front-end properties and additional conditions

We now record the structural properties and spectral conditions that the re-tuned front end must satisfy. These conditions allow the LWE solver in Step $9^\dagger$ to work in the exact sampling regime.

AC1. After modulus splitting and center extraction (Steps 5-7 of Chen [2024]) and just before the Step 8 gadget, conditioned on any fixed transcript E the post-Step 7 coordinate block is supported on

$$\left\{\, j\Delta + \boldsymbol{v}^*(E) + M_2\boldsymbol{k} \bmod M : j \in \mathbb{Z},\ \boldsymbol{k} \in \mathcal{K} \,\right\},$$

for some index set $\mathcal{K} \subseteq 0\,|\,\{0,1\}^{n-1}$, where $\Delta = 2D^2\mathbf{b}$ and the offset $\boldsymbol{v}^*(E) \in (\mathbb{Z}_M)^n$ depends on E but not on j. As above, $\mathcal{K}$ is a choice of parity representatives; any larger grid index domain can be reduced to this form by regrouping all terms with the same $\boldsymbol{k}$ mod 2 into a single amplitude. Reducing modulo M_2 eliminates the $M_2\boldsymbol{k}$ term and yields the affine congruence

$$\mathbf{X}(j) \equiv 2D^2 j\,\mathbf{b} + \boldsymbol{v}^*(E) \pmod{M_2}.$$

This matches the offset-coherence invariant of Chen's deferred-measurement front end (Lemma 2.8). In particular, since $k_1 = 0$ for all $\boldsymbol{k} \in \mathcal{K}$ and $b_1 = -1$, the first coordinate satisfies

$$X_1 \equiv -2D^2 j + v_1^* \pmod{M_2}, \qquad X_1 \bmod D^2 \equiv v_1^* \bmod D^2.$$

AC2. We assume throughout that Q is an odd integer. The post-processing in Step $9^\dagger$ works for an arbitrary composite modulus Q. Whenever we invert a residue class, we only do so modulo a modulus that is guaranteed to be coprime to that residue. In particular, we do not require Q to factor in any prescribed way, and the integers $(p_\eta)_\eta$ from the LWE-to-lattice reduction play no role in the algebraic structure of Q.

AC3. We keep the scaling regime of Chen [2024]. The parameter D is odd, coprime to Q, and we define

$$M := 2D^2 Q, \qquad M_2 := M/2 = D^2 Q.$$

Since Q is odd (AC2) and $\gcd(D, Q) = 1$, we have $\gcd(2D^2, Q) = 1$, so $2D^2$ is a unit modulo Q. All divisions by D^2 or $2D^2$ that appear in the post-processing should be read as multiplications by the corresponding inverses in $\mathbb{Z}_Q$; we never perform integer division by D^2 or $2D^2$ in $\mathbb{Z}$. For the first coordinate, this gives

$$X_1 \equiv 2D^2 j b_1 + v_1^* \equiv -2D^2 j + v_1^* \pmod{M_2},$$

so that reduction modulo D^2 kills the j-dependent term:

$$X_1 \bmod D^2 \equiv v_1^* \bmod D^2.$$

AC4. *Run-local chirp cancellation from the first coordinate.* The post-Step 7 amplitudes contain the quadratic chirp $\omega_Q^{-j^2}$ in the loop index j. Fix a transcript E. By AC1 and $b_1 = -1$, for every j in the effective window,

$$X_1 \equiv -2D^2 j + v_1^*(E) \pmod{M_2}, \qquad M_2 = D^2 Q.$$

Since $k_1 = 0$ for all $\boldsymbol{k} \in \mathcal{K}$, reducing modulo D^2 removes the j-term on every branch:

$$\tau := X_1 \bmod D^2 \equiv v_1^*(E) \bmod D^2.$$

Thus τ is deterministic conditioned on E; measuring it does not disturb the coherent superposition over j and $\boldsymbol{k}$. Let $\bar{v}_1 := \mathrm{ctr}(\tau) \in (-D^2/2, D^2/2]$.

Side information. We assume the preparation oracle also returns, as classical side information, either the residue

$$v_{1,Q} := v_1^*(E) \bmod Q \in \mathbb{Z}_Q,$$

or equivalently a "high-order" gauge value $\lambda(E) \in \mathbb{Z}_Q$ satisfying $v_1^*(E) \equiv \bar{v}_1 + \lambda(E)D^2 \pmod{M_2}$, so that $v_{1,Q} = (\bar{v}_1 + \lambda(E)D^2) \bmod Q$. (See Proposition 2.3 for a canonical-gauge compilation where $\lambda(E) = 0$.)

Chirp-cancellation unitary. Define $\mathrm{inv} := (-2D^2)^{-1} \in \mathbb{Z}_Q$, which exists by AC2-AC3. For each basis value $x \in \mathbb{Z}_M$ of X_1, write $x_Q := x \bmod Q$ and define

$$j(x) \;:=\; \mathrm{inv} \cdot \big((x_Q - v_{1,Q}) \bmod Q\big) \in \mathbb{Z}_Q.$$

We apply the diagonal unitary $U_{\mathrm{corr}}^{(v_{1,Q})}$ on X_1,

$$|x\rangle_{X_1} \longmapsto \omega_Q^{j(x)^2}\, |x\rangle_{X_1},$$

implemented by reversible arithmetic that computes $j(x)$, applies the phase, and uncomputes. On a branch with loop label j we have $(X_1 \bmod Q) - v_{1,Q} \equiv -2D^2 j \pmod{Q}$, hence $j(X_1) \equiv j \pmod{Q}$ and $j(X_1)^2 \equiv j^2 \pmod{Q}$. Therefore $U_{\mathrm{corr}}^{(v_{1,Q})}$ cancels $\omega_Q^{-j^2}$ on every branch and yields the chirp-free state $|\varphi_7\rangle$ in Equation (1.2). All arithmetic in the definition of $j(x)$ and in the square $j(x)^2$ is in $\mathbb{Z}_Q$; in particular, the phase exponent is reduced modulo Q.

AC5. For the rephased chirp-free state of AC4 and a fixed transcript E, define for $\boldsymbol{u} \in \mathbb{Z}_M^n$

$$S_E(\boldsymbol{u}) \;:=\; \sum_{j \in \mathbb{Z}} \sum_{\boldsymbol{k} \in \mathcal{K}} \alpha_E(j, \boldsymbol{k})\, i^{\|\boldsymbol{k}\|^2}\, \omega_M^{j\langle \boldsymbol{u}, \Delta\rangle + M_2 \langle \boldsymbol{u}, \boldsymbol{k}\rangle}.$$

Up to the $\boldsymbol{u}$-dependent global phase $\omega_M^{\langle \boldsymbol{u}, \boldsymbol{v}^*\rangle}$, $S_E(\boldsymbol{u})$ is the unnormalized Fourier amplitude of $|\boldsymbol{u}\rangle$ obtained after applying $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the coordinate registers of $|\varphi_7\rangle$.

We view the loop index $j \in \mathbb{Z}_P$ as embedded in $\mathbb{Z}$. We extend $\alpha_E(j, \boldsymbol{k})$ by zero outside an interval $\{|j| \le J_{\max}\}$. The effective window satisfies $J_{\max} = \mathrm{poly}(Q \log n) \ll P$ in the Karst-wave regime below; in particular, we assume $J_{\max} < P/2$ so that the embedding of $j \in \mathbb{Z}_P$ into integers is unambiguous on the support of the state. The infinite sum above then matches, up to negligible error, the finite sum that appears in Chen's state.

As in Chen's Karst-wave front end, we assume that conditioned on E, the amplitudes factor across the loop index and the grid label:

$$\alpha_E(j, \boldsymbol{k}) = \alpha_E(j)\, \beta_E(\boldsymbol{k}).$$

Define the one-dimensional Fourier transform of the loop envelope

$$\widehat{\alpha}_E(\theta) := \sum_{j \in \mathbb{Z}} \alpha_E(j)\, e^{2\pi i j \theta}.$$

A transcript E is called *good* if the off-resonant Fourier mass on the Q-point grid $\{t/Q : t \in \mathbb{Z}_Q\}$ is negligible:

$$\sum_{t \in \mathbb{Z}_Q \setminus \{0\}} \left|\widehat{\alpha}_E(t/Q)\right|^2 \leq \mathrm{negl}(n) \cdot \sum_{t \in \mathbb{Z}_Q} \left|\widehat{\alpha}_E(t/Q)\right|^2. \tag{2.1}$$

We assume that a transcript drawn from the front end is good except with probability $\mathrm{negl}(n)$ over the front-end randomness.

Reliability of the additional conditions. Additional Conditions AC2-AC3 are enforced directly by Definition 2.1. Additional Condition AC1 is the standard offset-coherence invariant of Chen's deferred-measurement front end (Lemma 2.8). Additional Condition AC4 is the only genuinely new access-model requirement used by Step $9^\dagger$: it asks for run-local access to $v_{1,Q}(E)$ (equivalently, to a gauge value $\lambda(E)$) so that the quadratic chirp can be cancelled using only X_1. This information is not implied by AC1 and is treated as explicit side information returned by the oracle; if the gauge value is available coherently inside the preparation, one can also compile a canonical gauge via an E-controlled basis translation on X_1 (Proposition 2.3). Finally, Additional Condition AC5 follows from the complex discrete-Gaussian Karst-wave envelope once $\sigma_J \geq C_{\mathrm{spec}} Q \log n$ (Proposition 2.6).

Lemma 2.2 (Uniformity modulo Q on the dual hyperplane)**.** Assume AC1-AC4 and fix any transcript E. Let μ_E be the distribution of $\boldsymbol{u} \in \mathbb{Z}_M^n$ obtained by applying $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the coordinate registers of $|\varphi_7\rangle$ (after the correction in AC4) and measuring. Define the resonance event and dual hyperplane

$$R := \{\boldsymbol{u} \in \mathbb{Z}_M^n : \langle \mathbf{b}, \boldsymbol{u} \rangle \equiv 0 \pmod{Q}\}, \qquad H := \{\boldsymbol{v} \in \mathbb{Z}_Q^n : \langle \mathbf{b}, \boldsymbol{v} \rangle \equiv 0 \pmod{Q}\}.$$

If $\Pr_{\mu_E}[R] > 0$, then conditioned on R the reduced outcome $\boldsymbol{u} \bmod Q \in \mathbb{Z}_Q^n$ is exactly uniform on H. In particular, $\Pr[\boldsymbol{u} \bmod Q = \mathbf{0} \mid R] = 1/|H| = Q^{-(n-1)}$.

Proof. Fix E. Apply $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the chirp-free state (1.2). For each $\boldsymbol{u} \in \mathbb{Z}_M^n$, the unnormalized amplitude equals

$$\omega_M^{\langle \boldsymbol{u}, \boldsymbol{v}^* \rangle} \cdot \sum_{j \in \mathbb{Z}} \sum_{\boldsymbol{k} \in \mathcal{K}} \alpha_E(j, \boldsymbol{k})\, i^{\|\boldsymbol{k}\|^2}\, \omega_M^{j\langle \boldsymbol{u}, \Delta \rangle + M_2 \langle \boldsymbol{u}, \boldsymbol{k} \rangle},$$

so the outcome probabilities are proportional to the squared magnitude of the inner sum.

Because $M_2 = M/2$, we have $\omega_M^{M_2 \langle \boldsymbol{u}, \boldsymbol{k} \rangle} = (-1)^{\langle \boldsymbol{u}, \boldsymbol{k} \rangle}$, which depends only on the parity pattern of $\boldsymbol{u}_{[2..n]}$ since $k_1 = 0$ for all $\boldsymbol{k} \in \mathcal{K}$. Let $\boldsymbol{u}_Q := \boldsymbol{u} \bmod Q \in \mathbb{Z}_Q^n$ and set $t(\boldsymbol{u}) := \langle \mathbf{b}, \boldsymbol{u}_Q \rangle \in \mathbb{Z}_Q$. We can reduce $\boldsymbol{u}$ modulo Q inside the phase because of the special form of Δ. Write $\boldsymbol{u} = \boldsymbol{u}_Q + Q\boldsymbol{t}$ with $\boldsymbol{t} \in \mathbb{Z}^n$ coordinatewise. Since $\Delta = 2D^2\mathbf{b}$ and $M = 2D^2 Q$, we have

$$\langle Q\boldsymbol{t}, \Delta \rangle = Q \cdot 2D^2 \langle \boldsymbol{t}, \mathbf{b} \rangle = M \cdot \langle \boldsymbol{t}, \mathbf{b} \rangle \in M\mathbb{Z},$$

so $\omega_M^{j\langle Q\boldsymbol{t},\Delta\rangle} = 1$ for all integers j. Therefore

$$\omega_M^{j\langle \boldsymbol{u},\Delta\rangle} = \omega_M^{j\langle \boldsymbol{u}_Q,\Delta\rangle} = \exp\left(2\pi i\, j\, \frac{t(\boldsymbol{u})}{Q}\right).$$

On the event R we have $t(\boldsymbol{u}) = 0$, hence $\omega_M^{j\langle \boldsymbol{u},\Delta\rangle} = 1$ for all j. Therefore, conditioned on R, the outcome probabilities depend on $\boldsymbol{u}$ only through the parity pattern of $\boldsymbol{u}_{[2..n]}$.

Now fix any $\boldsymbol{v} \in H$. The fibre $F_{\boldsymbol{v}} := \{\boldsymbol{u} \in \mathbb{Z}_M^n : \boldsymbol{u} \bmod Q = \boldsymbol{v}\}$ consists of the vectors $\boldsymbol{u} = \boldsymbol{v} + Q\boldsymbol{t}$ with $\boldsymbol{t} \in \mathbb{Z}_{M/Q}^n = \mathbb{Z}_{2D^2}^n$. Since Q is odd, as $\boldsymbol{t}$ ranges over $\mathbb{Z}_{2D^2}^n$ the parity pattern of $(\boldsymbol{v} + Q\boldsymbol{t})_{[2..n]}$ is exactly uniform over $\{0,1\}^{n-1}$, independently of $\boldsymbol{v}$. Hence, each parity pattern occurs in $F_{\boldsymbol{v}}$ with the same multiplicity for every $\boldsymbol{v} \in H$, and since the conditional probabilities depend only on this parity pattern, $\mu_E[F_{\boldsymbol{v}} \mid R]$ is constant over $\boldsymbol{v} \in H$. This proves uniformity of $\boldsymbol{u} \bmod Q$ on H conditioned on R. Finally, because $b_1 = -1$ is a unit in $\mathbb{Z}_Q$, $|H| = Q^{n-1}$, so $\Pr[\boldsymbol{u} \bmod Q = \mathbf{0} \mid R] = Q^{-(n-1)}$. $\square$

Proposition 2.3 (Gauge side information and canonical-gauge compilation)**.** Assume AC1 and suppose the state-preparation procedure is given as an explicit circuit (or oracle) that outputs the coordinate registers together with a classical side-information register E from which the gauge parameter $\lambda(E) \in \mathbb{Z}_Q$ of AC4 (equivalently, $v_{1,Q} = v_1^*(E) \bmod Q$) can be obtained. Then Additional Condition AC4 holds: the post-processing can compute $v_{1,Q}$ for the current run and implement the chirp-cancellation unitary on X_1. Moreover, if E is available coherently during the preparation, one can compile the preparation by appending an E-controlled basis translation on X_1 by $-\lambda(E)D^2$ (modulo M) so that the resulting state satisfies the canonical gauge $\lambda(E) = 0$. If the preparation is a black-box state oracle that outputs only the coordinate registers and does not expose $\lambda(E)$ (or $v_1^*(E) \bmod Q$) as side information, then AC4 becomes an additional oracle promise and is not implied by AC1 alone.

Proof. Fix a transcript E. By AC1 we have $X_1 \equiv -2D^2 j + v_1^*(E) \pmod{M_2}$ with $M_2 = D^2 Q$. Let $\tau(E) := v_1^*(E) \bmod D^2$ and let $\bar{v}_1 := \mathrm{ctr}(\tau(E)) \in (-D^2/2, D^2/2]$. Because $D^2 \mid M_2$, there exists a unique $\lambda(E) \in \mathbb{Z}_Q$ such that $v_1^*(E) \equiv \bar{v}_1 + \lambda(E)D^2 \pmod{M_2}$. By assumption, the post-processing can obtain $\lambda(E)$ (or directly $v_{1,Q}$) from the side-information register E, and hence can recover the needed residue $v_{1,Q} = v_1^*(E) \bmod Q = (\bar{v}_1 + \lambda(E)D^2) \bmod Q$ and implement the chirp correction of AC4. If one prefers to avoid carrying $\lambda(E)$ into the post-processing, one can instead compile the preparation itself: inside the preparation unitary (where E is available coherently), apply the controlled basis translation $|x\rangle_{X_1} \mapsto |x - \lambda(E)D^2 \bmod M\rangle_{X_1}$. This map is a permutation of the computational basis of X_1 and hence unitary. It leaves $\tau = X_1 \bmod D^2$ invariant, and it replaces the offset representative by $\bar{v}_1$, enforcing $\lambda(E) = 0$. $\square$

Lemma 2.4 (Center-referenced chirp cancellation)**.** Assume AC1-AC4. Then the procedure in AC4 defines, for each run-local residue $v_{1,Q} = v_1^*(E) \bmod Q$ (obtainable from τ and/or transcript side information), a unitary $U_{\mathrm{corr}}^{(v_{1,Q})}$ on the first coordinate register such that $|\varphi_7\rangle := U_{\mathrm{corr}}^{(v_{1,Q})}|\widetilde{\varphi}_7\rangle$ has the form Equation (1.2). The quadratic chirp $e^{-2\pi i j^2/Q}$ in the loop index is removed on every branch.

Proof. Under AC1, we have $X_1 \equiv -2D^2 j + v_1^* \pmod{M_2}$ with v_1^* independent of j. Conditioned on the transcript E, the measurement of $\tau := X_1 \bmod D^2$ is deterministic and yields $\tau \equiv v_1^* \bmod D^2$ on every branch. By AC4, the post-processing obtains $v_{1,Q} = v_1^*(E) \bmod Q$, hence $(X_1 \bmod Q) - v_{1,Q} \equiv -2D^2 j \pmod{Q}$ on every branch. The reversible computation of $j(X_1)$ in AC4 is well-defined modulo Q by AC2-AC3. For $x = X_1$ on a branch with loop label j we have $j(X_1) \equiv j \pmod{Q}$. The unitary

U_{corr} multiplies that branch by $\exp(2\pi i j^2/Q)$. It cancels the original chirp $e^{-2\pi i j^2/Q}$. The map is diagonal in the computational basis of X_1. Hence, it is unitary. $\square$

Remark 2.5 (Justification of Additional Condition AC5)**.** Additional Condition AC5 isolates the only additional front-end property used by Step 9†: spectral concentration of the one-dimensional Karst-wave envelope on the Q-point grid, with dominant mass at the single resonant frequency $t = 0$.

In Chen's Karst-wave front end, conditioned on a transcript E, the post-Step 7 amplitudes factor as $\alpha_E(j, \boldsymbol{k}) = \alpha_E(j)\beta_E(\boldsymbol{k})$ (see Eq. (35) in Chen [2024]). After chirp cancellation (Additional Condition AC4), the Fourier amplitude at $\boldsymbol{u} \in \mathbb{Z}_M^n$ factorizes as

$$S_E(\boldsymbol{u}) = \widehat{\alpha}_E(t(\boldsymbol{u})/Q) \cdot G_E(\boldsymbol{u}),$$

where $G_E(\boldsymbol{u})$ collects the grid contribution. Here we write

$$t(\boldsymbol{u}) \ := \ \langle \mathbf{b}, \boldsymbol{u} \rangle \bmod Q \ \in \ \mathbb{Z}_Q,$$

and identify $t(\boldsymbol{u})$ with its standard representative in $\{0, \dots, Q-1\}$ when used as an argument of $\widehat{\alpha}_E(\cdot)$ on $[0, 1)$. Taking the envelope width $\sigma_J \gtrsim Q \log n$ yields $|\widehat{\alpha}_E(t/Q)| \le \exp(-\Omega(\log^2 n)) \cdot |\widehat{\alpha}_E(0)|$ for all integers $t \not\equiv 0 \pmod{Q}$ by standard Poisson-summation / discrete-Gaussian Fourier-decay estimates [Micciancio and Regev, 2007, Peikert, 2010, Regev, 2010]. Since $\sum_{t \in \mathbb{Z}_Q} |\widehat{\alpha}_E(t/Q)|^2 \ge |\widehat{\alpha}_E(0)|^2$, this implies the leakage bound Equation (2.1).

A time shift $j \mapsto j - j_0$ multiplies $\widehat{\alpha}_E(\theta)$ by a unit-modulus factor and does not affect its magnitude. In contrast, a nontrivial linear phase $\alpha_E(j) \mapsto \alpha_E(j) e^{2\pi i \nu j}$ shifts the spectrum $\widehat{\alpha}_E(\theta) \mapsto \widehat{\alpha}_E(\theta + \nu)$ and can move the dominant residue class away from $t = 0$ on the grid $\{t/Q\}$. In our setting, if the post-processing were to *ignore* the gauge term $\lambda(E)D^2$ and use $v_{1,Q} = \bar{v}_1 \bmod Q$ in place of the correct value $v_{1,Q} = (\bar{v}_1 + \lambda(E)D^2) \bmod Q$, then the chirp-cancellation unitary would leave a residual linear phase $\omega_Q^{-\lambda(E)j}$ (up to a global constant) on the loop index j. This would shift the dominant residue class away from $t = 0$ on the Q-point grid. Additional Condition AC4 (or canonical-gauge compilation) rules out this mismatch by requiring the *exact* run-local residue $v_{1,Q}$.

No additional near-uniformity assumption is needed for the *reduced* samples: Lemma 2.2 shows that conditioned on $\langle \mathbf{b}, \boldsymbol{u} \rangle \equiv 0 \pmod{Q}$, the reduction $\boldsymbol{u} \bmod Q$ is exactly uniform on the dual hyperplane H, and $\Pr[\boldsymbol{u} \bmod Q = \mathbf{0} \mid \langle \mathbf{b}, \boldsymbol{u} \rangle \equiv 0] = 1/|H| = Q^{-(n-1)}$.

Proposition 2.6 (Spectral concentration for the re-tuned Karst wave)**.** For the complex-Gaussian Karst-wave front end of Chen [2024] (where, conditioned on a transcript E, the post-Step 7 amplitudes factor as $\alpha_E(j, \boldsymbol{k}) = \alpha_E(j)\beta_E(\boldsymbol{k})$), instantiated with any re-tuned configuration that satisfies Definition 2.1, Additional Condition AC5 holds.

Proof. Under Chen's Karst-wave analysis, conditioned on a transcript E the loop envelope $\alpha_E(j)$ is a discrete Gaussian of width σ_J, and the factorization $\alpha_E(j, \boldsymbol{k}) = \alpha_E(j)\beta_E(\boldsymbol{k})$ holds. An integer shift in j does not affect $|\widehat{\alpha}_E(\cdot)|$. Any additional run-dependent linear phase on the $1/Q$ grid would shift the dominant residue class away from $t = 0$; in our setting, this corresponds to using an incorrect $v_{1,Q}$ in the chirp correction, which AC4 rules out by supplying the run-local gauge value. Thus, it suffices to bound the centered discrete-Gaussian prototype $g_\sigma(j) := \exp(-\pi j^2/\sigma^2)$. Its Fourier series satisfies the Poisson-summation identity (see, e.g., [Micciancio and Regev, 2007])

$$\sum_{j \in \mathbb{Z}} g_\sigma(j)\, e^{2\pi i j \theta} = \sigma \sum_{m \in \mathbb{Z}} \exp\bigl(-\pi \sigma^2 (\theta - m)^2\bigr).$$

Evaluating at $\theta = t/Q$, for any integer $t \not\equiv 0 \pmod{Q}$ let $m^\star \in \mathbb{Z}$ be a nearest integer to t/Q (so $m^\star \in \{0,1\}$). Then $|t/Q - m^\star| \geq 1/Q$, hence the dominant Gaussian term in the Poisson sum is at most $\sigma \exp(-\pi\sigma^2/Q^2)$, and all other terms are smaller by an additional factor $\exp(-\Omega(\sigma^2))$. Consequently, for some absolute constant $c_0 > 0$,

$$|\widehat{\alpha}_E(t/Q)| \leq |\widehat{\alpha}_E(0)| \cdot \exp\Big(-c_0 \cdot (\sigma_J/Q)^2\Big) \quad \text{for all } t \not\equiv 0 \pmod{Q},$$

up to negligible truncation error from the effective window. With $\sigma_J \geq C_{\mathrm{spec}} Q \log n$ (Definition 2.1), this gives $|\widehat{\alpha}_E(t/Q)| \leq |\widehat{\alpha}_E(0)| \exp(-\Omega(\log^2 n))$. Since $Q = \mathrm{poly}(n)$ in the re-tuned regime, summing the squared bound over the $(Q-1)$ nonzero residues yields

$$\sum_{t \in \mathbb{Z}_Q \setminus \{0\}} |\widehat{\alpha}_E(t/Q)|^2 \leq (Q-1)\exp(-\Omega(\log^2 n)) \cdot |\widehat{\alpha}_E(0)|^2.$$

Using $\sum_{t \in \mathbb{Z}_Q} |\widehat{\alpha}_E(t/Q)|^2 \geq |\widehat{\alpha}_E(0)|^2$ proves Equation (2.1). $\square$

2.2 Access model

Definition 2.7 (Access model)**.** We assume circuit-level quantum access to an outcome-conditioned state-preparation procedure that, on each invocation, outputs one copy of the post-Step 7 state $|\widetilde{\varphi}_7\rangle$ on coordinate registers $X \in (\mathbb{Z}_M)^n$, together with a classical side-information register E that may include Chen's measured strings and, for AC4, a short run-local *gauge* value sufficient to obtain the residue $v_{1,Q} := v_1^*(E) \bmod Q$ (equivalently, $\lambda(E) \in \mathbb{Z}_Q$). We treat E as a *classical* output register (i.e., returned in the computational basis). Equivalently, the oracle may measure E before returning it. This ensures that reading E and any deterministic function of E is compatible with maintaining coherence over the loop index j and grid label $\boldsymbol{k}$ in $|\widetilde{\varphi}_7\rangle$. We do not assume this gauge value is derivable from the Step 7 coordinate registers alone; it is treated as explicit side information returned by the oracle, and since it is fixed conditioned on E it can be measured without disturbing the superposition over j and $\boldsymbol{k}$. As a special case, if the known preparation circuit is compiled into the canonical gauge $\lambda(E) = 0$ (Proposition 2.3), then $v_1^*(E) \bmod Q$ can be recovered from $\tau = X_1 \bmod D^2$ alone and no explicit transcript access is needed for chirp cancellation.

For each invocation there exists a transcript E such that, conditioned on E, the reduced state on X satisfies Additional Condition AC1 with offset $\boldsymbol{v}^*(E)$ and amplitudes $\alpha_E(j, \boldsymbol{k})$. Across invocations, the transcript is re-sampled, so the offset $\boldsymbol{v}^*(E)$ may change from run to run and cannot be forced to repeat.

The post-processing is allowed to apply any quantum circuit of size $\mathrm{poly}(n)$ to the output registers, including arithmetic in $\mathbb{Z}_M$ and $\mathbb{Z}_Q$, intermediate measurements, and $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$. We do *not* assume the ability to query the preparation on chosen basis inputs j, to classically compute the full offset $\boldsymbol{v}^*(E)$, or to obtain two copies of $|\widetilde{\varphi}_7\rangle$ with the same offset.

In this model, an algorithm acts on the superposition directly. The offset $\boldsymbol{v}^*(E)$ depends on the run-specific outcomes E and behaves like a one-time pad on the coordinate values in the computational basis. Step $9^\dagger$ shows that this offset turns into a harmless phase pattern after a Fourier transform. We can then sample from the dual lattice without ever learning $\boldsymbol{\Delta}$ or $\boldsymbol{v}^*$ as explicit classical data.

Lemma 2.8 (Offset coherence)**.** In the deferred-measurement unitary of Chen [2024], take the program point just before Step 8 and after modulus splitting and center extraction (Steps 5-7). For each fixed transcript E, the post-Step 7 coordinate block in $(\mathbb{Z}_M)^n$ is supported on

$$\left\{\, j\Delta + \boldsymbol{v}^*(E) + M_2\boldsymbol{k} \bmod M : j \in \mathbb{Z},\ \boldsymbol{k} \in \mathcal{K} \,\right\},$$

for some index set $\mathcal{K} \subseteq 0\,|\,\{0,1\}^{n-1}$, where $\Delta = 2D^2\mathbf{b}$ and the offset $\boldsymbol{v}^*(E) \in (\mathbb{Z}_M)^n$ depends on E but not on j. Reducing modulo M_2 eliminates the $M_2\boldsymbol{k}$ term and yields

$$\mathbf{X}(j) \equiv 2D^2 j\,\mathbf{b} + \boldsymbol{v}^*(E) \pmod{M_2}.$$

Proof. This is immediate from Chen's post-Step 7 computational-basis form: the basis values are $2Dj\,\boldsymbol{x} + \boldsymbol{v}' + \frac{M}{2}\boldsymbol{k} \bmod M$ with $\boldsymbol{k} \in 0\,|\,\mathbb{Z}^{n-1}$ and $\boldsymbol{x} = D\mathbf{b}$. Since $M_2 = M/2$, only $\boldsymbol{k} \bmod 2$ affects $\frac{M}{2}\boldsymbol{k} \bmod M$ (and the phase $i^{\|\boldsymbol{k}\|^2}$), so one may fix $\boldsymbol{k} \in 0\,|\,\{0,1\}^{n-1}$ as representatives. Substituting $\boldsymbol{x} = D\mathbf{b}$ gives $2Dj\,\boldsymbol{x} = 2D^2 j\,\mathbf{b} = j\Delta$ with $\Delta = 2D^2\mathbf{b}$, and writing $\boldsymbol{v}^*(E) := \boldsymbol{v}' \bmod M$ yields the claimed support in $(\mathbb{Z}_M)^n$. Reducing modulo $M_2 = M/2$ eliminates the $M_2\boldsymbol{k}$ term, giving $\mathbf{X}(j) \equiv 2D^2 j\,\mathbf{b} + \boldsymbol{v}^*(E) \pmod{M_2}$. $\square$

Algorithm 1 STEP9DAGGERSAMPLE: chirp correction and direct Fourier sampling

Input: Parameters (D, M, Q) and $\mathrm{inv} := (-2D^2)^{-1} \in \mathbb{Z}_Q$.
Oracle: One copy of $|\widetilde{\varphi}_7\rangle$ on coordinate registers $X \in (\mathbb{Z}_M)^n$ and side information sufficient to obtain $v_{1,Q} := v_1^*(E) \bmod Q$ (Definition 2.7).
Output: A reduced sample $\boldsymbol{u}_Q \in \mathbb{Z}_Q^n$ (possibly $\mathbf{0}$).
Query the state-preparation oracle to obtain $|\widetilde{\varphi}_7\rangle$ on X and run-local side information E (including the gauge value needed for AC4).
Measure $\tau \leftarrow X_1 \bmod D^2$ and set $\bar{v}_1 \leftarrow \mathrm{ctr}(\tau)$ ▷ Deterministic conditioned on E (AC1); needed only if E encodes $\lambda(E)$.
Using $(E, \bar{v}_1)$, compute the run-local residue $v_{1,Q} := v_1^*(E) \bmod Q$ as in AC4:
  either read $v_{1,Q}$ directly from E, or read $\lambda(E) \in \mathbb{Z}_Q$ from E and set $v_{1,Q} \leftarrow (\bar{v}_1 + \lambda(E)D^2) \bmod Q$.
Apply the diagonal unitary $U_{\mathrm{corr}}^{(v_{1,Q})}$ on X_1 as defined in AC4 (using inv).
Apply $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to X and measure $\boldsymbol{u} \in \mathbb{Z}_M^n$.
return $\boldsymbol{u}_Q \leftarrow \boldsymbol{u} \bmod Q$.

3 The new Step $9^{\dagger}$

Algorithm 2 Step $9^{\dagger}$

Input: A chosen-secret LWE instance $(\mathbf{U}, \mathbf{t})$ as in Chen [2024] over modulus q (equivalently, the lattice $L_q^{\perp}(\mathbf{A})$ with $\mathbf{A} = [2p_1\mathbf{t} \mid \mathbf{U}^{\top} \mid \mathbf{I}_m]$), together with public parameters $(q, \beta, p_1, \ldots, p_\kappa)$.
Oracle: State-preparation access to $|\widetilde{\varphi}_7\rangle$ as in Definition 2.7.
Parameters: A re-tuned Karst-wave configuration $(c, D, r, s, t, u, P, M, Q)$ as in Definition 2.1 (chosen for the current norm guess; see Remark 3.1).
Output: Either the LWE secret s and error e, or FAIL (meaning the current norm guess is rejected).
Let $\ell \leftarrow$ the number of rows of $\mathbf{U}$ and $m \leftarrow$ the number of columns of $\mathbf{U}$; set $n \leftarrow 1 + \ell + m$.
Fix absolute constants $C_{\text{rank}} > 1$, $C_{\text{try}} \geq 1$, and $C_{\text{samp}} \geq 1$.
Set the target sample count $N \leftarrow \lceil C_{\text{rank}}(n-1) \rceil$ and the batch budget $T_{\max} \leftarrow \lceil C_{\text{try}} n \rceil$.
Set a per-batch oracle-call cap $B_{\max} \leftarrow \lceil C_{\text{samp}} \cdot N \rceil$.
Precompute $\text{inv} := (-2D^2)^{-1} \in \mathbb{Z}_Q$ ▷ Exists by AC2-AC3. Used inside AC4.
for trial $= 1$ **to** $T_{\max}$ **do**
  Initialize $\mathcal{S} \leftarrow \emptyset$ and calls $\leftarrow 0$.
  while $|\mathcal{S}| < N$ **and** calls $< B_{\max}$ **do**
    calls $\leftarrow$ calls $+ 1$.
    $\boldsymbol{u}_Q \leftarrow$ STEP9DAGGERSAMPLE(D, M, Q, inv) ▷ Algorithm 1.
    if $\boldsymbol{u}_Q \neq \mathbf{0}$ **then**
      Append $\boldsymbol{u}_Q$ as a row of $\mathcal{S}$.
    end if
  end while
  if $|\mathcal{S}| < N$ **then**
    continue ▷ Sampling cap exceeded (wrong guess or atypical transcript).
  end if
  $\mathbf{b}_Q \leftarrow$ RECOVERBMODQ$(\mathcal{S}, Q)$ ▷ Algorithm 4.
  if $\mathbf{b}_Q =$ FAIL **then**
    continue
  end if
  $(s, e) \leftarrow$ EXTRACTANDVERIFYLWE$(\mathbf{b}_Q, \mathbf{U}, \mathbf{t}, q, \beta, p_1, \ldots, p_\kappa)$ ▷ Algorithm 3.
  if $(s, e) \neq$ FAIL **then**
    return (s, e)
  end if
end for
return FAIL

Algorithm 3 ExtractAndVerifyLWE: parse and certify (s, e)

Input: $\mathbf{b}_Q \in \mathbb{Z}_Q^n$, a chosen-secret LWE instance $(\mathbf{U}, \mathbf{t})$ with $\mathbf{U} \in \mathbb{Z}_q^{\ell \times m}$ and $\mathbf{t} \in \mathbb{Z}_q^m$, and public parameters $(q, \beta, p_1, \ldots, p_\kappa)$.
Output: The LWE secret s and error e, or FAIL.
Let $\ell \leftarrow$ the number of rows of $\mathbf{U}$ and $m \leftarrow$ the number of columns of $\mathbf{U}$; set $n \leftarrow 1 + \ell + m$.
(Fail if $\kappa - 1 > \ell$.) ▷ Chosen-secret prefix must fit in the ℓ-dimensional secret.
Lift $\mathbf{b}_Q$ coordinate-wise to $\mathbf{b} \in (-Q/2, Q/2]^n \cap \mathbb{Z}^n$.
if $b_1 \neq -1$ as an integer **then**
    return FAIL
end if
for $i = 2$ **to** n **do**
    if $2p_1 \nmid b_i$ in $\mathbb{Z}$ **then**
        return FAIL
    end if
end for
for $i = 2$ **to** κ **do**
    if $b_i \neq 2p_1 p_i$ in $\mathbb{Z}$ **then**
        return FAIL
    end if
end for
Parse $\mathbf{b} = [-1,\, 2p_1 s^\top,\, 2p_1 e^\top]^\top$ with $s \in \mathbb{Z}^\ell$ and $e \in \mathbb{Z}^m$, and recover s, e by integer division by $2p_1$.
Check shortness (e.g. $\|s\|_\infty, \|e\|_\infty \le \beta \log n$) and any promised norm bounds for $\|\mathbf{b}\|$ from the lattice analysis.
if $\mathbf{U}^\top s + e \not\equiv \mathbf{t} \pmod{q}$ **then**
    return FAIL
end if
return (s, e).

Algorithm 4 RecoverBModQ: solve for $\mathbf{b}$ mod Q from dual samples

Input: A matrix $\mathcal{S} \in (\mathbb{Z}_Q)^{N \times n}$ whose rows are nonzero samples $\boldsymbol{u}_Q$.
Output: $\mathbf{b}_Q = \mathbf{b} \bmod Q$, or FAIL.
Let $W \in (\mathbb{Z}_Q)^{N \times (n-1)}$ be the submatrix of $\mathcal{S}$ consisting of columns $2..n$, and let $\boldsymbol{y} \in (\mathbb{Z}_Q)^N$ be column 1 of $\mathcal{S}$.
Solve $W\boldsymbol{z} \equiv \boldsymbol{y} \pmod{Q}$ and test uniqueness (e.g. via Smith normal form [Kannan and Bachem, 1979]).
if no solution exists **or** the solution is not unique **then**
    return FAIL
end if
Let $\boldsymbol{z}$ be the unique solution and set $\mathbf{b}_Q \leftarrow [-1, \boldsymbol{z}^\top]^\top \in \mathbb{Z}_Q^n$.
return $\mathbf{b}_Q$.

Remark 3.1 (Classical guessing loop for the norm)**.** As in Chen [2024], the small modulus is chosen as $Q = (c{+}1)\|\mathbf{b}\|^2$, where $\mathbf{b}$ is the unknown unique shortest vector of $L_q^\perp(\mathbf{A})$. We run a classical outer loop over all polynomially many candidates B_{guess} for $\|\mathbf{b}\|^2$. For each guess we set $Q \leftarrow (c+1)B_{\text{guess}}$, choose an odd D with $\gcd(D, Q) = 1$, derive $M = 2D^2Q$ (hence $M_2 = D^2Q$), and complete the remaining Karst-wave parameters as in Definition 2.1. We then execute Algorithm 2 for this guess.

Only the correct guess yields dual samples supported on the hyperplane $\langle \mathbf{b}, \boldsymbol{u}\rangle \equiv 0 \pmod{Q}$ and passes the explicit verification in Algorithm 3, except with negligible probability. To keep rejection for incorrect guesses polynomial-time, Algorithm 2 uses a fixed trial budget $T_{\max} = \text{poly}(n)$ and a per-trial sampling cap $B_{\max} = \text{poly}(n)$, returning FAIL if no verified solution is found within budget.

Remark 3.2 (Instantiation for LWE)**.** For the q-ary lattice $L_q^{\perp}(\mathbf{A})$ in Chen [2024], the promised unique shortest vector has the form

$$\mathbf{b} = [-1,\, 2p_1 s^{\top},\, 2p_1 e^{\top}]^{\top} \in \mathbb{Z}^n,$$

where s is the LWE secret and e is the error vector. Because $\|\mathbf{b}\|_\infty \leq 2p_1\beta \log n < Q/2$ in the parameter regime of interest, the reduction map $\mathbf{b} \mapsto \mathbf{b} \bmod Q$ is injective on the centered cube that contains the true shortest vector. Therefore, once Algorithm 2 recovers $\mathbf{b} \bmod Q$, the canonical lift to $(-Q/2, Q/2]^n$ recovers $\mathbf{b}$ as an integer vector. Dividing the last $n-1$ coordinates by $2p_1$ (after checking divisibility) yields s and e, and the check $\mathbf{U}^{\mathsf{T}} s + e \equiv \mathbf{t} \pmod{q}$ certifies correctness (equivalently, $\mathbf{A}\mathbf{b} \equiv 0 \pmod{q}$).

Fourier sampling. We apply $\text{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the coordinate register block and then measure $\boldsymbol{u} \in \mathbb{Z}_M^n$ (Algorithm 1). The outcome distribution is analyzed in the next part.

3.1 Correctness under Additional Conditions

Lemma 3.3 (Dual sampling via direct QFT)**.** Assume AC1-AC5 and let $|\varphi_7\rangle$ be the chirp-free state from Lemma 2.4. Fix a good measurement transcript E in the sense of Additional Condition AC5 and write the conditional state as

$$|\varphi_7\rangle = \sum_{j\in\mathbb{Z}} \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_E(j, \boldsymbol{k})\, i^{\|\boldsymbol{k}\|^2}\ |j\Delta + \boldsymbol{v}^* + M_2\boldsymbol{k} \bmod M\rangle\,,$$

where $\Delta = 2D^2\mathbf{b}$ and $M_2 = M/2$. After applying $\text{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the coordinate registers and measuring $\boldsymbol{u} \in \mathbb{Z}_M^n$, we have

$$\Pr\big[\langle \mathbf{b}, \boldsymbol{u}\rangle \equiv 0 \pmod{Q}\big] \geq 1 - \text{negl}(n).$$

Moreover, by Lemma 2.2, conditioned on the event $\langle \mathbf{b}, \boldsymbol{u}\rangle \equiv 0 \pmod{Q}$ the reduced outcome $\boldsymbol{u} \bmod Q$ is exactly uniform on the dual hyperplane H, hence $\Pr[\boldsymbol{u} \bmod Q = \mathbf{0}] \leq Q^{-(n-1)} + \text{negl}(n)$.

Proof of Lemma 3.3. Fix E. Apply $\text{QFT}_{\mathbb{Z}_M}^{\otimes n}$ to the chirp-free state Equation (1.2). For each $\boldsymbol{u} \in \mathbb{Z}_M^n$, the unnormalized amplitude equals

$$\omega_M^{\langle \boldsymbol{u}, \boldsymbol{v}^*\rangle} \cdot \sum_{j\in\mathbb{Z}} \sum_{\boldsymbol{k}\in\mathcal{K}} \alpha_E(j, \boldsymbol{k})\, i^{\|\boldsymbol{k}\|^2}\, \omega_M^{j\langle \boldsymbol{u}, \Delta\rangle + M_2\langle \boldsymbol{u}, \boldsymbol{k}\rangle},$$

so the outcome probabilities are proportional to the squared magnitude of the inner sum.

By AC5, conditioned on E the coefficients factor as $\alpha_E(j,\boldsymbol{k}) = \alpha_E(j)\beta_E(\boldsymbol{k})$. Using $M_2 = M/2$ we have $\omega_M^{M_2\langle \boldsymbol{u},\boldsymbol{k}\rangle} = (-1)^{\langle \boldsymbol{u},\boldsymbol{k}\rangle}$, and since $k_1 = 0$ this depends only on the parity pattern of $\boldsymbol{u}_{[2..n]}$. Moreover $M = 2D^2Q$ and $\Delta = 2D^2\mathbf{b}$, hence

$$\omega_M^{j\langle \boldsymbol{u},\Delta\rangle} = \exp\!\left(2\pi i\, j\, \frac{t(\boldsymbol{u})}{Q}\right),$$

where $t(\boldsymbol{u}) := \langle \mathbf{b}, \boldsymbol{u}\rangle \bmod Q \in \mathbb{Z}_Q$ and we identify $t(\boldsymbol{u})$ with its representative in $\{0,\dots,Q-1\}$ when used inside the exponential. Equivalently, if we write $\boldsymbol{u} = \boldsymbol{u}_Q + Q\boldsymbol{t}$ with $\boldsymbol{u}_Q = \boldsymbol{u} \bmod Q$, then $\langle \boldsymbol{u},\Delta\rangle - \langle \boldsymbol{u}_Q,\Delta\rangle = \langle Q\boldsymbol{t}, 2D^2\mathbf{b}\rangle \in M\mathbb{Z}$, so $\omega_M^{j\langle \boldsymbol{u},\Delta\rangle} = \omega_M^{j\langle \boldsymbol{u}_Q,\Delta\rangle}$ for all integers j. Therefore $S_E(\boldsymbol{u})$ factorizes as

$$S_E(\boldsymbol{u}) = \Big(\sum_{j\in\mathbb{Z}} \alpha_E(j)\, e^{2\pi i j\, t(\boldsymbol{u})/Q}\Big)\cdot\Big(\sum_{\boldsymbol{k}\in\mathcal{K}} \beta_E(\boldsymbol{k})\, i^{\|\boldsymbol{k}\|^2}\, (-1)^{\langle \boldsymbol{u},\boldsymbol{k}\rangle}\Big) = \widehat{\alpha}_E(t(\boldsymbol{u})/Q)\cdot G_E(\boldsymbol{u}),$$

where $G_E(\boldsymbol{u})$ depends only on the parity pattern of $\boldsymbol{u}_{[2..n]}$. For notational clarity, write $t(\boldsymbol{u}) := \langle \mathbf{b},\boldsymbol{u}\rangle \bmod Q \in \mathbb{Z}_Q$ and view $t(\boldsymbol{u})$ in $\{0,\dots,Q-1\}$ when used as an argument of $\widehat{\alpha}_E(\cdot)$. Then the envelope factor above is $\widehat{\alpha}_E(t(\boldsymbol{u})/Q)$.

Thus

$$\Pr[\boldsymbol{u}] \;\propto\; |S_E(\boldsymbol{u})|^2 = |\widehat{\alpha}_E(t(\boldsymbol{u})/Q)|^2 \cdot |G_E(\boldsymbol{u})|^2.$$

For each residue $t \in \mathbb{Z}_Q$, let

$$T_t := \{\boldsymbol{u} \in \mathbb{Z}_M^n : \langle \mathbf{b},\boldsymbol{u}\rangle \equiv t \pmod{Q}\}.$$

Because $b_1 = -1$ is a unit in $\mathbb{Z}_Q$, for every fixed $\boldsymbol{u}_{[2..n]} \in \mathbb{Z}_M^{n-1}$ and every t there are exactly $M/Q = 2D^2$ values of $u_1 \in \mathbb{Z}_M$ such that $\boldsymbol{u} \in T_t$. Since $G_E(\boldsymbol{u})$ does not depend on u_1, the total grid mass $\sum_{\boldsymbol{u}\in T_t} |G_E(\boldsymbol{u})|^2$ is the same for every t. Hence, the total probability mass of T_t is proportional to $|\widehat{\alpha}_E(t/Q)|^2$, up to negligible truncation error.

By the leakage bound Equation (2.1) (good transcript) and this proportionality, the total off-resonant probability mass satisfies

$$\sum_{t\neq 0} \Pr[T_t] = \frac{\sum_{t\neq 0} |\widehat{\alpha}_E(t/Q)|^2}{\sum_{t\in\mathbb{Z}_Q} |\widehat{\alpha}_E(t/Q)|^2} \le \mathrm{negl}(n),$$

so

$$\Pr\big[\langle \mathbf{b},\boldsymbol{u}\rangle \equiv 0 \pmod{Q}\big] \ge 1 - \mathrm{negl}(n).$$

Finally, conditioned on this resonance event, Lemma 2.2 gives exact uniformity of $\boldsymbol{u} \bmod Q$ on H, and in particular $\Pr[\boldsymbol{u} \bmod Q = \mathbf{0}] \le Q^{-(n-1)} + \mathrm{negl}(n)$. □

Theorem 3.4 (Step 9† is correct)**.** Assume AC1-AC5 and run Algorithm 2 in the correct iteration of the outer norm-guessing loop. Each accepted sample $\boldsymbol{u}_Q \in \mathbb{Z}_Q^n$ appended to $\mathcal{S}$ by Algorithm 2 is non-zero by construction and satisfies

$$\langle \mathbf{b}, \boldsymbol{u}_Q\rangle \equiv 0 \pmod{Q}$$

except with probability $\mathrm{negl}(n)$ over the choice of a good transcript and the internal randomness of the measurements. Solving the resulting linear system modulo Q recovers $\mathbf{b} \bmod Q$ and hence $\mathbf{b}$ as an integer vector. The LWE secret and error are then extracted and verified in polynomial time with overwhelming probability.

Proof. By Additional Condition AC5, a transcript drawn from the front end is good except with probability $\mathrm{negl}(n)$. Algorithm 2 makes only $\mathrm{poly}(n)$ oracle calls, so by a union bound we may condition on the event that all invocations are good, losing at most a negligible term in the overall success probability.

In each oracle call within Algorithm 2, the sampling primitive STEP9DAGGERSAMPLE (Algorithm 1) measures $\tau = X_1 \bmod D^2$, obtains the run-local residue $v_{1,Q} = v_1^*(E) \bmod Q$ from run-local side information (AC4), and applies the diagonal gate $U_{\mathrm{corr}}^{(v_{1,Q})}$. Lemma 2.4 shows that this removes the quadratic chirp and produces the chirp-free state $|\varphi_7\rangle$ assumed in AC5.

Applying $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ and measuring yields $\boldsymbol{u} \in \mathbb{Z}_M^n$. Lemma 3.3 implies that $\langle \mathbf{b}, \boldsymbol{u} \rangle \equiv 0 \pmod{Q}$ except with probability $\mathrm{negl}(n)$, and Lemma 2.2 implies that, conditioned on this resonance event, $\boldsymbol{u} \bmod Q$ is exactly uniform on $H = \{\boldsymbol{v} \in \mathbb{Z}_Q^n : \langle \mathbf{b}, \boldsymbol{v} \rangle \equiv 0 \pmod{Q}\}$. In particular, $\Pr[\boldsymbol{u} \bmod Q = \mathbf{0}] \leq Q^{-(n-1)} + \mathrm{negl}(n)$, so the rejection step $\boldsymbol{u}_Q \neq \mathbf{0}$ fails only negligibly often. A union bound over the $N = O(n)$ accepted samples in a batch implies that, with probability $1 - \mathrm{negl}(n)$, every accepted $\boldsymbol{u}_Q$ satisfies $\langle \mathbf{b}, \boldsymbol{u}_Q \rangle \equiv 0 \pmod{Q}$.

Fix such a successful batch. Because $b_1 = -1$ is a unit in $\mathbb{Z}_Q$, the projection $H \to \mathbb{Z}_Q^{n-1}$ given by $\boldsymbol{u} \mapsto \boldsymbol{u}_{[2..n]}$ is a bijection. Moreover, on H the only vector with $\boldsymbol{u}_{[2..n]} = \mathbf{0}$ is $\boldsymbol{u} = \mathbf{0}$ (because $-u_1 \equiv 0$ then forces $u_1 \equiv 0$), so rejecting $\boldsymbol{u}_Q = \mathbf{0}$ is equivalent to rejecting $\boldsymbol{u}_{Q,[2..n]} = \mathbf{0}$. Hence, the accepted vectors $\boldsymbol{u}_{Q,[2..n]}$ are i.i.d. (up to a negligible statistical error from the rare off-resonant outputs) uniform over $\mathbb{Z}_Q^{n-1} \setminus \{\mathbf{0}\}$. Let $W \in \mathbb{Z}_Q^{N \times (n-1)}$ be the matrix with these rows and let $\boldsymbol{y}$ be the vector of first coordinates. Then the true unknown $\mathbf{b}_{[2..n]} \bmod Q$ satisfies $W\mathbf{b}_{[2..n]} \equiv \boldsymbol{y} \pmod{Q}$.

With overwhelming probability W is injective as a map $(\mathbb{Z}_Q)^{n-1} \to (\mathbb{Z}_Q)^N$. Because $Q = \mathrm{poly}(n)$, the number of distinct prime divisors of Q is at most $\log_2 Q = O(\log n)$, so a union bound over $p \mid Q$ preserves a negligible overall failure probability. Indeed, for any prime $p \mid Q$, the reduction $W \bmod p$ is (up to a negligible error from excluding the all-zero row) an i.i.d. uniform random matrix over the field $\mathbb{Z}_p$ with $N \geq C_{\mathrm{rank}}(n-1)$ rows, and standard rank bounds give $\Pr[\mathrm{rank}_{\mathbb{Z}_p}(W \bmod p) < n-1] \leq p^{-\Omega(n)}$. If $\mathrm{rank}_{\mathbb{Z}_p}(W \bmod p) = n-1$ and $W\boldsymbol{z} \equiv \mathbf{0} \pmod{p^e}$, then reducing modulo p gives $\boldsymbol{z} \equiv \mathbf{0} \pmod{p}$; writing $\boldsymbol{z} = p\boldsymbol{z}_1$ and iterating shows $\boldsymbol{z} \equiv \mathbf{0} \pmod{p^e}$, so $\ker(W \bmod p^e) = \{\mathbf{0}\}$. By the Chinese remainder theorem, $\ker(W \bmod Q) = \{\mathbf{0}\}$. Therefore the system has a unique solution $\boldsymbol{z} \in \mathbb{Z}_Q^{n-1}$, which Algorithm 4 computes and uses to set $\mathbf{b}_Q = [-1, \boldsymbol{z}^\top]^\top = \mathbf{b} \bmod Q$.

Finally, the bound $\|\mathbf{b}\|_\infty < Q/2$ from (R1) makes the centered lift from $\mathbb{Z}_Q^n$ to $(-Q/2, Q/2]^n$ injective on the relevant region, so lifting $\mathbf{b}_Q$ recovers $\mathbf{b}$ as an integer vector. The subsequent divisibility, planted-prefix, shortness, and LWE-consistency checks (Algorithm 3) succeed for the correct guess and reject incorrect guesses, as in Chen [2024]. ☐

Corollary 3.5 (Conditional quantum algorithm for LWE)**.** Assume the LWE-to-lattice reduction and the unique-shortest-vector promise for $L_q^\perp(\mathbf{A})$ from Chen [2024]. If the corresponding front end can be compiled in a re-tuned configuration satisfying Additional Conditions AC1-AC5, then Algorithm 2 solves the chosen-secret LWE instance encoded by $L_q^\perp(\mathbf{A})$ in quantum polynomial time with overwhelming probability. Via the classical reductions of Chen [2024], this yields a quantum algorithm for standard LWE in the same parameter regime, conditional on AC1-AC5.

4 Related Work

Lattice-based cryptography is rooted in worst-case hardness frameworks such as Ajtai's construction of hard lattice instances [Ajtai, 1996] and subsequent worst-case-to-average-case reductions based on Gaussian measure [Micciancio and Regev, 2007]. Regev introduced LWE and gave quantum worst-case reductions from lattice problems such as GapSVP and SIVP to LWE [Regev, 2009]. Subsequent work clarified parameter tradeoffs and established classical hardness in a range of regimes [Peikert, 2009, Brakerski et al., 2013]. These reductions underpin a broad ecosystem of cryptographic constructions, including trapdoors for hard lattices [Gentry et al., 2008] and fully homomorphic encryption [Gentry, 2009].

For context, the fastest known worst-case SVP algorithms are classical and typically rely on sieving and/or discrete Gaussians, starting from the sieve of Ajtai-Kumar-Sivakumar [Ajtai et al., 2001] and later practical refinements [Nguyen and Vidick, 2008], and including the $2^{n+o(n)}$-time discrete-Gaussian algorithm of Aggarwal et al. [2015]. Discrete Gaussian sampling is also a central technical tool in lattice algorithms more broadly; efficient lattice Gaussian samplers were developed, for example, by Peikert [Peikert, 2010].

On the quantum side, lattice algorithms are often organized around preparing structured coset- or line-supported superpositions and extracting information via Fourier sampling. A canonical early connection is Regev's reduction from unique-SVP to the dihedral hidden subgroup problem (DHSP) via coset sampling [Regev, 2004], together with subexponential-time algorithms for DHSP such as Kuperberg's sieve [Kuperberg, 2005]. Related dihedral-coset models have since appeared in lattice settings, e.g., the extrapolated dihedral coset problem (EDCP), which is closely connected to LWE [Brakerski et al., 2018].

On the average-case state side, Chen, Liu, and Zhandry introduced a filtering framework for decoding hidden linear structure from LWE-like quantum states and used it to obtain polynomial-time quantum algorithms for several average-case variants, including EDCP in certain regimes [Chen et al., 2022]. Subsequent work has studied both algorithms and hardness barriers for quantum LWE-state families with structured (e.g., Gaussian) amplitudes and linear/quadratic phase terms [Chen et al., 2025].

Chen's Karst-wave construction [Chen, 2024] is an instance of this Fourier-sampling template with amplitude engineering via complex-Gaussian windowing, yielding a post-processing state supported on a shifted grid line whose amplitudes include a quadratic chirp in the loop index. Chen's published post-processing (Steps 8-9) exploits additional arithmetic structure to handle the unknown shift and chirp. The present work isolates an explicit access-model promise that suffices for exact post-processing in the LWE regime: run-local access to $v_{1,Q} := v_1^*(E) \bmod Q$ (AC4), enabling single-coordinate chirp cancellation followed by a direct $\mathrm{QFT}_{\mathbb{Z}_M}^{\otimes n}$ without learning the full offset $\boldsymbol{v}^*(E)$.

5 Conclusion

In this work, we present a new Step $9^\dagger$, which turns unknown offsets into harmless phase patterns. Under explicit front-end conditions on the Karst wave window, it yields modular linear relations from direct Fourier sampling on the coordinate registers. We instantiate this step with the parameters and the lattice $L_q^\perp(\mathbf{A})$ from Chen [2024]. In the access model of Section 2.2, such a construction gives a direct path from a superposition with support $\{j\Delta + \boldsymbol{v}^*\}$ to samples from the dual lattice. Under these assumptions, we obtain a quantum algorithm that solves the chosen-secret LWE problem of Chen [2024] in almost the same parameter regime as in that work.

Acknowledgments

We are grateful to all who provided constructive discussions and helpful feedback. The author used AI-enabled tools solely for English grammar and clarity suggestions in non-technical prose. All technical ideas, proofs, and results are the author's own work.

References

Divesh Aggarwal, Daniel Dadush, Oded Regev, and Noah Stephens-Davidowitz. Solving the shortest vector problem in 2^n time using discrete gaussian sampling. In *Proceedings of the forty-seventh annual ACM symposium on Theory of computing*, pages 733–742, 2015.

Miklós Ajtai. Generating hard instances of lattice problems. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 99–108, 1996.

Miklós Ajtai, Ravi Kumar, and Dandapani Sivakumar. A sieve algorithm for the shortest lattice vector problem. In *Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 601–610, 2001.

Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the forty-fifth annual ACM symposium on Theory of computing*, pages 575–584, 2013.

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.

Yilei Chen. Quantum algorithms for lattice problems. *Cryptology ePrint Archive*, 2024.

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.

Yilei Chen, Zihan Hu, Qipeng Liu, Han Luo, and Yaxin Tu. Lwe with quantum amplitudes: algorithm, hardness, and oblivious sampling. In *Annual International Cryptology Conference*, pages 513–544. Springer, 2025.

Craig Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 169–178, 2009.

Craig Gentry, Chris Peikert, and Vinod Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proceedings of the fortieth annual ACM symposium on Theory of computing*, pages 197–206, 2008.

Ravindran Kannan and Achim Bachem. Polynomial algorithms for computing the smith and hermite normal forms of an integer matrix. *siam Journal on Computing*, 8(4):499–507, 1979.

Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM Journal on Computing*, 35(1):170–188, 2005.

Daniele Micciancio and Oded Regev. Worst-case to average-case reductions based on gaussian measures. *SIAM journal on computing*, 37(1):267–302, 2007.

Phong Q Nguyen and Thomas Vidick. Sieve algorithms for the shortest vector problem are practical. *Journal of Mathematical Cryptology*, 2(2):181–207, 2008.

Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proceedings of the forty-first annual ACM symposium on Theory of computing*, pages 333–342, 2009.

Chris Peikert. An efficient and parallel gaussian sampler for lattices. In *Annual Cryptology Conference*, pages 80–97. Springer, 2010.

Oded Regev. Quantum computation and lattice problems. *SIAM Journal on Computing*, 33(3): 738–760, 2004.

Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *Journal of the ACM (JACM)*, 56(6):1–40, 2009.

Oded Regev. The learning with errors problem. *Invited survey in CCC*, 7(30):11, 2010.