Learning With Errors and Extrapolated Dihedral Cosets

Zvika Brakerski[⋆], Elena Kirshanova[⋆⋆], Damien Stehlé[⋆⋆⋆], and Weiqiang Wen[†]

Abstract. The hardness of the learning with errors (LWE) problem is one of the most fruitful resources of modern cryptography. In particular, it is one of the most prominent candidates for secure post-quantum cryptography. Understanding its quantum complexity is therefore an important goal.

We show that under quantum polynomial time reductions, LWE is equivalent to a relaxed version of the dihedral coset problem (DCP), which we call extrapolated DCP (eDCP). The extent of extrapolation varies with the LWE noise rate. By considering different extents of extrapolation, our result generalizes Regev's famous proof that if DCP is in BQP (quantum poly-time) then so is LWE (FOCS 02). We also discuss a connection between eDCP and Childs and Van Dam's algorithm for generalized hidden shift problems (SODA 07).

Our result implies that a BQP solution for LWE might not require the full power of solving DCP, but rather only a solution for its relaxed version, eDCP, which could be easier.

1 Introduction

The Learning With Errors problem $\mathrm{LWE}_{n,q,\alpha}$ with parameters $n, q \in \mathbb{Z}$ and $\alpha \in (0,1)$ consists in finding a vector $\mathbf{s} \in \mathbb{Z}_q^n$ from arbitrarily many samples $(\mathbf{a}_i, \langle \mathbf{a}_i, \mathbf{s}\rangle + e_i) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\mathbf{a}_i$ is uniformly sampled in $\mathbb{Z}_q^n$ and e_i is sampled from $\mathcal{D}_{\mathbb{Z},\alpha q}$, the discrete Gaussian distribution of standard deviation parameter αq (i.e., the distribution such that $\mathcal{D}_{\mathbb{Z},\alpha q}(k) \sim \exp(-\pi k^2/(\alpha q)^2)$ for all $k \in \mathbb{Z}$). Since its introduction by Regev [28, 29], LWE has served as a security foundation for numerous cryptographic primitives (see e.g. an overview in [24]). The cryptographic attractiveness of LWE stems from two particularly

[⋆] Weizmann Institute of Science, zvika.brakerski@weizmann.ac.il. Supported by the Israel Science Foundation (Grant No. 468/14) and Binational Science Foundation (Grants No. 2016726, 2014276) and ERC Project 756482 REACT.

[⋆⋆] ENS de Lyon and Laboratoire LIP (U. Lyon, CNRS, ENS de Lyon, INRIA, UCBL), elena.kirshanova@ens-lyon.fr. Supported by ERC Starting Grant ERC-2013-StG-335086-LATTAC.

[⋆⋆⋆] ENS de Lyon and Laboratoire LIP (U. Lyon, CNRS, ENS de Lyon, INRIA, UCBL), damien.stehle@ens-lyon.fr. Supported by ERC Starting Grant ERC-2013-StG-335086-LATTAC.

[†] ENS de Lyon and Laboratoire LIP (U. Lyon, CNRS, ENS de Lyon, INRIA, UCBL), weiqiang.wen@ens-lyon.fr. Supported by ERC Starting Grant ERC-2013-StG-335086-LATTAC.

desirable properties. First, its algebraic simplicity enables the design of primitives with advanced functionalities, such as fully homomorphic encryption [8], attribute-based encryption for all circuits [14] and (single key) functional encryption [13]. Second, LWE is conjectured hard even in the context of quantum computations, making it one of the most appealing candidate security foundations for post-quantum cryptography [5]. Current quantum algorithms for LWE do not outperform classical ones, but it is not clear whether this is inherent (for example, it is known that LWE is *easier* than the Dihedral Coset Problem under polynomial-time reductions, see below). In this work, we characterize the quantum hardness of LWE under polynomial-time reductions and show that it is computationally equivalent (up to small parameter losses) to a quantum problem closely related to the aforementioned Dihedral Coset Problem.

LWE*, Lattices and the Dihedral Coset Problem.* LWE is tightly connected to worst-case approximation problems over Euclidean lattices. In particular, LWE is an (average-case) instance of the Bounded Distance Decoding problem (BDD) (see, e.g., [21, Section 5.4]), but is also known to be as hard as *worst-case* BDD (with some polynomial loss in parameters) [29]. BDD is the problem of finding the closest lattice vector to a given target point which is promised to be very close to the lattice (formally, closer than λ_1/γ where λ_1 is the length of the shortest non-zero vector). Classical and quantum connections between BDD and other problems such as SIVP, GapSVP, uSVP are also known [7, 20, 23, 29].

Regev [25, 27] showed that uSVP, and therefore also BDD and LWE, are no harder to solve than the quantumly-defined Dihedral Coset Problem (DCP). An instance of $\mathrm{DCP}_{N,\ell}$, for integer parameters N and ℓ, consists of ℓ quantum registers in superposition $|0, x_k\rangle + |1, x_k + s\rangle$, with a common $s \in \mathbb{Z}_N$ and random and independent $x_k \in \mathbb{Z}_N$ for $k \in [\ell]$. The goal is to find s (information theoretically $\ell = \mathcal{O}(\log N)$ is sufficient for this task [10]). We note that Regev considered a variant with unbounded number of registers, but where a fraction of them is faulty (a faulty state is of the form $|b, x_k\rangle$ for arbitrary $b \in \{0, 1\}, x_k \in \mathbb{Z}_N$). In our work, we assume a non-faulty formulation of DCP.

Still, it is quite possible that DCP is in fact much harder to solve than LWE. The best known algorithm for DCP, due to Kuperberg [17], runs in time $2^{\mathcal{O}(\log \ell + \log N/\log \ell)}$ which does not improve upon classical methods for solving LWE. Other variants of the problem were explored in [10, 11], and of particular relevance to this work is a "vector" variant of the problem where $\mathbb{Z}_N$ is replaced with $\mathbb{Z}_q^n$ (i.e. s and x_k are now vectors). These problems behave similarly to DCP with $N = q^n$.

Finally, Regev showed that DCP can be solved given efficient algorithms for the subset-sum problem (which is classically defined), however in a regime of parameters that appears harder to solve than LWE itself.

Extrapolated DCP. The focus of this work is a generalization of the DCP problem, i.e. rather than considering registers containing $|0, x_k\rangle + |1, x_k + s\rangle$, we allow (1) x_i's and s be n-dimensional vectors, and (2) other than non-uniform distribution for amplitudes. We name this problem Extrapolated DCP (EDCP) as its input registers has more extrapolated states. To be more precise, $\mathrm{EDCP}^{\ell}_{n,N,f}$, with parameters three integers n, N, ℓ and a function $f : \mathbb{Z} \mapsto \mathbb{C}$ with $\sum_{j\in\mathbb{Z}} j \cdot |f(j)|^2 < +\infty$, consists in recovering $\mathbf{s} \in \mathbb{Z}_N^n$ from the following ℓ states over $\mathbb{Z} \times \mathbb{Z}_N^n$:

$$\left\{ \frac{1}{\sqrt{\sum_{j\in\mathbb{Z}} |f(j)|^2}} \cdot \sum_{j\in\mathbb{Z}} f(j) \left| j, \mathbf{x}_k + j \cdot \mathbf{s} \right\rangle \right\}_{k\leq\ell} ,$$

where the $\mathbf{x}_k$'s are arbitrary in $\mathbb{Z}_N^n$.[1] Note that DCP is the special case of EDCP for $n = 1$ and f being the indicator function of $\{0, 1\}$.

In [9], Childs and van Dam consider a special case of EDCP where f is the indicator function of $\{0, \ldots, M-1\}$ for some integer M, which we will refer to as uniform EDCP (or, $\text{U-EDCP}^{\ell}_{n,N,M}$).

Our Main Result. We show that up to polynomial loss in parameters, U-EDCP is equivalent to LWE. Thus we provide a formulation of the hardness assumption underlying lattice-based cryptography in terms of the (generalized) Dihedral Coset Problem.

Theorem 1 (Informal). *There exists a quantum polynomial-time reduction from* $\mathrm{LWE}_{n,q,\alpha}$ *to* $\text{U-EDCP}^{\ell}_{n,N,M}$*, with* $N = q$*,* $\ell = \mathrm{poly}(n \log q)$ *and* $M = \frac{\mathrm{poly}(n \log q)}{\alpha}$*. Conversely, there exists a polynomial-time reduction from* U-EDCP *to* LWE *with the same parameter relationships, up to* $\mathrm{poly}(n \log q)$ *factors.*

Our proof crucially relies on a special case of EDCP where f is a Gaussian weight function with standard deviation parameter r. We call this problem Gaussian EDCP (G-EDCP). We show that G-EDCP and U-EDCP are equivalent up to small parameter losses.

EDCP is analogous to LWE in many aspects. The decisional version of LWE (dLWE) asks to distinguish between LWE samples and random samples of the form $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$ where both components are chosen uniformly at random. Similarly, we also consider the decisional version of EDCP, denoted by dEDCP. In $\mathrm{dEDCP}_{n,N,f}$, we are asked to distinguish between an EDCP state and a state of the form

$$|j\rangle \left|\mathbf{x} \bmod N\right\rangle ,$$

where j is distributed according to the function $|f|^2$, and $\mathbf{x} \in \mathbb{Z}_N^n$ is uniformly chosen. EDCP enjoys a reduction between its search and decisional variants via LWE.

Related work. In [9], Childs and van Dam show that $\text{U-EDCP}^{\ell}_{1,N,M}$ reduces to the problem of finding all the solutions $\mathbf{b} \in \{0, \ldots, M-1\}^k$ to the equation $\langle \mathbf{b}, \mathbf{x} \rangle = w \bmod N$, where $\mathbf{x}$ and w are given and uniformly random modulo N. They interpret this as an integer linear program and use lattice reduction, within Lenstra's algorithm [19], to solve it. This leads to a polynomial-time

[1] Note that the assumption on f implies, via Markov's inequality, that one may restrict the sum to a finite index set and obtain a superposition which remains within negligible ℓ_2 distance from the countable superposition above.

algorithm for U-EDCP$^{\ell}_{1,N,M}$ when $M = \lfloor N^{1/k} \rfloor$ and $\ell \geq k$, for any $k \geq 3$. Interestingly, finding small solutions to the equation $\langle \mathbf{b}, \mathbf{x} \rangle = w \bmod N$ is a special case of the Inhomogeneous Small Integer Solution problem [12] (ISIS), which consists in finding a small-norm $\mathbf{x}$ such that $\mathbf{B}\mathbf{x} = \mathbf{w} \bmod q$, with $\mathbf{B} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{w} \in \mathbb{Z}_q^n$ uniform (where q, n, m are integer parameters). A reduction from the homogeneous SIS (i.e., with $\mathbf{w} = \mathbf{0}$ and $\mathbf{x} \neq \mathbf{0}$) to LWE was provided in [31]. It does not seem possible to derive from it a reduction from EDCP to LWE via the Childs and van Dam variant of ISIS, most notably because the reduction from [31] does not provide a way to compute all ISIS solutions within a box $\{0, 1, \ldots, M-1\}^k$.

It is not hard to see that, at least so long as M is polynomial, a solution to DCP implies a solution to EDCP$^{\ell}_{n,N,M}$. Therefore our result implies [25] as a special case. On the other extreme, our result also subsumes [9] since the LLL algorithm [18] can be used to solve LWE$_{n,q,\alpha}$ in polynomial time when $1/\alpha$ and q are $2^{\Theta(n)}$, which implies a polynomial-time algorithm for EDCP for $M = 2^{\Theta(\sqrt{n \log N})}$, significantly improving Childs and van Dam's $M = 2^{\varepsilon n \log N}$.

Finally, we observe that the LWE to U-EDCP reduction (and the uSVP to DCP reduction from [27]) can be adapted to a uSVP to U-EDCP reduction, as explained below. Combining this adaptation with the reduction from U-EDCP to LWE (via G-EDCP) provides a novel quantum reduction from worst-case lattice problems to LWE. However, it does not seem to have advantages compared to [29].

1.1 Technical overview

As mentioned above, the hardness of LWE is essentially invariant so long as $n \log q$ is preserved, and therefore we restrict our attention in this overview to the one-dimensional setting. A crucial ingredient in our reduction is a weighted version of EDCP, denoted by G-EDCP and quantified by a Gaussian weight function $f_r(j) =\rho_r(j) = \exp(-\pi j^2/r^2)$, for some standard deviation parameter r. We refer to this problem as Gaussian EDCP (G-EDCP).

Reducing G-EDCP *to* LWE. Given an G-EDCP state as input, our reduction efficiently transforms it into a classical LWE sample with constant success probability. Thus, making only one query to the LWE oracle, we are able to solve G-EDCP. More precisely, the reduction input consists of a normalized state corresponding to $\sum_{j \in \mathbb{Z}_N} \rho_r(j) \left|j\right\rangle \left|x + j \cdot s \bmod N\right\rangle$, for some integers $r \ll N$. One can think of N as the LWE modulus and of r as the standard deviation parameter of the LWE error.

Our first step is to apply a quantum Fourier transform over $\mathbb{Z}_N$ to the second register. This gives us a quantum superposition of the form:

$$\sum_{a \in \mathbb{Z}_N} \sum_{j \in \mathbb{Z}_N} \omega_N^{a \cdot (x + j \cdot s)} \cdot \rho_r(j) \left|j\right\rangle \left|a\right\rangle .$$

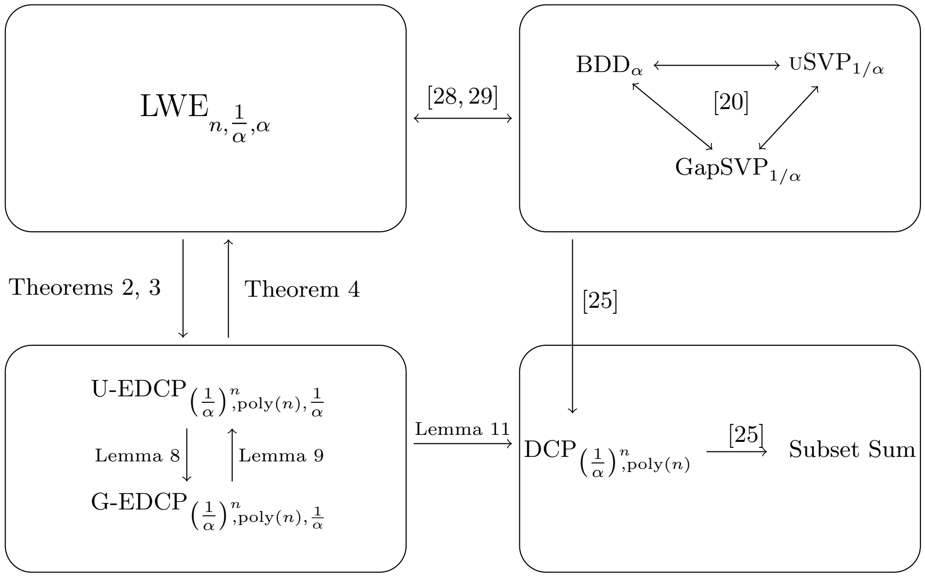

$\mathrm{LWE}_{n,\frac{1}{\alpha},\alpha}$
[28, 29]
BDD_{α}
$\mathrm{uSVP}_{1/\alpha}$
[20]
$\mathrm{GapSVP}_{1/\alpha}$
Theorems 2, 3
Theorem 4
[25]
$\text{U-EDCP}_{\left(\frac{1}{\alpha}\right)^n,\mathrm{poly}(n),\frac{1}{\alpha}}$
Lemma 8
Lemma 9
$\text{G-EDCP}_{\left(\frac{1}{\alpha}\right)^n,\mathrm{poly}(n),\frac{1}{\alpha}}$
Lemma 11
$\mathrm{DCP}_{\left(\frac{1}{\alpha}\right)^n,\mathrm{poly}(n)}$
[25]
Subset Sum

Fig. 1: Graph of reductions between the LWE problem (upper-left), worst-case lattice problems (upper-right), combinatorial problems (lower-right) and the Extrapolated Dihedral Coset problems (lower-left). Parameters α are given up to poly(n)-factors, where n is the dimension of the LWE problem. The same n stands for the lattice-dimension considered in problems of the upper-right corner. The subset-sum problem stated in the lower-right corner is of density ≈ 1 (in particular, the expected number of solutions is constant).

where $\omega_N = \exp(2i\pi/N)$. We then measure the second register and obtain a value $\widehat{a} \in \mathbb{Z}_N$. This leaves us with the state:

$$\sum_{j\in\mathbb{Z}_N} \omega_N^{j\cdot\widehat{a}\cdot s} \cdot \rho_r(j)\, |j\rangle\, |\widehat{a}\rangle\,.$$

Note that $\widehat{a}$ is uniformly random over $\mathbb{Z}_N$, which at the end serves as the first component of LWE sample. The exponent of relative phase in current state has a form similar to the second component of LWE sample but without noise. Now we can benefit from the first register, which stores a superposition corresponding to a Gaussian distribution over $\mathbb{Z}_N$ with standard deviation r. Applying a second quantum Fourier transform over $\mathbb{Z}_N$ to the first register gives us a quantum superposition of the form:

$$\sum_{b\in\mathbb{Z}_N}\sum_{j\in\mathbb{Z}_N} \omega_N^{j\cdot(\widehat{a}\cdot s+b)} \cdot \rho_r(j)\, |b\rangle\,.$$

Now the second component of the LWE sample $\widehat{a}\cdot s + b$ is stored in the phase (up to a factor j). Omitting the exponentially small Gaussian tail, we assume the summation for j is taken over the integers. An application of the Poisson summation formula transfers $\widehat{a}\cdot s + b$ into a shift of the Gaussian distribution defined over $\mathbb{Z}$. In other words, the received state is exponentially close to the superposition:

$$\sum_{e\in\mathbb{Z}_N} \rho_{1/r}\left(\frac{e}{N}\right) |-\widehat{a}\cdot s + e\rangle\,.$$

Once we measure the state above, we obtain a value $-\widehat{a}\cdot s+e$, where $e \hookleftarrow \mathcal{D}_{\mathbb{Z},N/r}$. Together with already known $\widehat{a}$, this gives us an LWE sample:

$$(-\widehat{a}, -\widehat{a}\cdot s + e)\,.$$

In case the input state is of the form $|j\rangle\, |x \bmod N\rangle$, where j is distributed according to the function ρ_r^2, and $x \in \mathbb{Z}_N$ is uniformly chosen (the decisional case), the reduction outlined above outputs a uniform random pair (a, b) from $\mathbb{Z}_N \times \mathbb{Z}_N$. This gives a reduction from decisional version of G-EDCP to decisional version of LWE.

Reducing LWE *to* G-EDCP. Our reduction from LWE to G-EDCP follows the general design of Regev's reduction from uSVP to DCP [27], with several twists that enable simplifications and improvements. We note that this reduction is folklore,[2] although we could not find it described explicitly.

First, the use of LWE rather than uSVP allows us to avoid Regev's initial sub-reduction from uSVP to BDD, as LWE is a randomized variant of BDD. Indeed, if we consider m samples $(a_i, a_i \cdot s + e_i)$ from $\mathrm{LWE}_{n,q,\alpha}$, then we have a BDD

[2] `https://groups.google.com/d/msg/cryptanalytic-algorithms/uhr6gGrVkIk/XxEv4uvEBwAJ`

instance for the lattice $\varLambda = \mathbf{A}\mathbb{Z}_q + q\mathbb{Z}^m$ and the target vector $\mathbf{t} = \mathbf{b} + \mathbf{e} \in \mathbb{Z}^m$ with $\mathbf{b} \in \varLambda$ satisfying $\mathbf{b} = \mathbf{A} \cdot s \bmod q$.

As Regev's, our reduction proceeds by subdividing the ambient space $\mathbb{R}^m$ with a coarse grid, setting the cell width between $\|\mathbf{e}\|$ and $\lambda_1(\varLambda)$. We map each point $\mathbf{y} \in \mathbb{R}^m$ to a cell $\phi(\mathbf{y})$. By choice of the cell width, we have $\phi(\mathbf{c}_1) \neq \phi(\mathbf{c}_2)$ for any $\mathbf{c}_1 \neq \mathbf{c}_2$ in $\varLambda$. Also for any $\mathbf{c} \in \mathbb{R}^m$, the vectors $\mathbf{c}$ and $\mathbf{c}+\mathbf{e}$ are most likely mapped to the same cell, as $\mathbf{e}$ is short. This intuition fails if a border between two cells falls close to $\mathbf{c}$. This (rare but non-negligibly so) event is the source of the limitation on the number ℓ of DCP/EDCP states produced by the reduction. The space subdivision by a grid is illustrated in Figure 2.

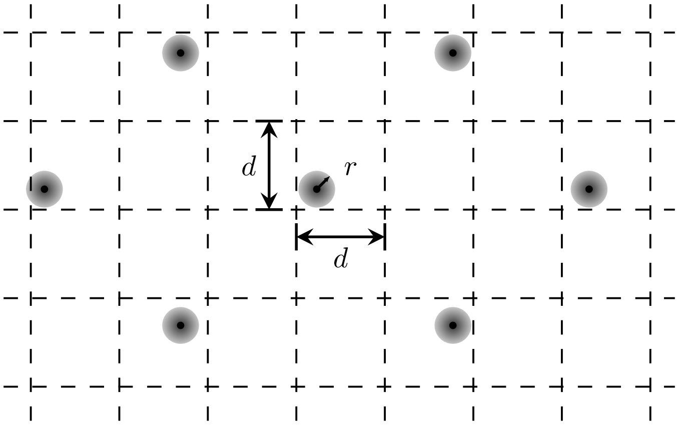


Fig. 2: A visualization of the space subdivision. Each radially shaded disk has width r, the upper bound of the error $\|\mathbf{e}\|$. Each cell has width d, chosen to be between $\|\mathbf{e}\|$ and $\lambda_1(L)/\sqrt{m}$. Note that the grid intersects the left-most disk, potentially leading to an error in the reduction.

Regev's reduction and ours differ in the way the grid is used to create the DCP/EDCP states. Let us first briefly recall the core of Regev's reduction. Let $\mathbf{B} = (\mathbf{b}_1, \ldots, \mathbf{b}_m)$ be a basis of $\varLambda$ and subtract an appropriate combination of the $\mathbf{b}_i$'s from $\mathbf{t}$ to get $\mathbf{t}'$ so that the coordinates $\mathbf{x}'$ of the closest vector $\mathbf{b}' \in \varLambda$ to $\mathbf{t}'$with respect to the $\mathbf{b}_i$'s are $\leq 2^m$ (this may be achieved using LLL [18] and Babai's nearest plane algorithm [1]). The first step is the creation of a superposition

$$\sum_{\substack{\mathbf{x}\in\mathbb{Z}^m\\ \|\mathbf{x}\|_\infty \leq 2^{2m}}} \left(|0, \mathbf{x}, \phi(\mathbf{B}\mathbf{x})\rangle + |1, \mathbf{x}, \phi(\mathbf{B}\mathbf{x} - \mathbf{t}')\rangle\right) =$$

$$|0\rangle \sum_{\substack{\mathbf{x}\in\mathbb{Z}^m\\ \|\mathbf{x}\|_\infty \leq 2^{2m}}} |\mathbf{x}, \phi(\mathbf{B}\mathbf{x})\rangle + |1\rangle \sum_{\substack{\mathbf{x}\in\mathbb{Z}^m\\ \|\mathbf{x}+\mathbf{x}'\|_\infty \leq 2^{2m}}} |\mathbf{x} + \mathbf{x}', \phi(\mathbf{B}\mathbf{x} - \mathbf{e})\rangle\,,$$

where the equality holds by a change of variable. By measuring the last register, with overwhelming probability this collapses to $|0\rangle |\mathbf{x}_k\rangle + |1\rangle |\mathbf{x}_k + \mathbf{x}'\rangle$, which corresponds to an m-dimensional DCP input state with modulus $2^{\mathcal{O}(m)}$. The whole process can be repeated multiple times using the same input vector $\mathbf{t}$, and results in different $\mathbf{x}_k$'s but a common $\mathbf{x}'$. Each iteration may fail because of an ill-placed cell delimitation, or if $\mathbf{x}_k + \mathbf{x}'$ has a coordinate whose magnitude is larger than 2^{2m}. This leads to a bounded number of correct DCP input states. Finally, m-dimensional DCP can be reduced to 1-dimensional DCP, with a significant modulus increase: the resulting modulus N is $2^{\mathcal{O}(m^2)}$.

Instead of using a superposition based on the coordinates with respect to a basis, we exploit the special form of $\Lambda = \mathbf{a}\mathbb{Z}_q + q\mathbb{Z}^m$ (w.l.o.g., assume 1-dimensional LWE, [7]). We start with the following superposition:

$$\sum_{x \in \mathbb{Z}_q} |0, x, \phi(\mathbf{a}x)\rangle + |1, x, \phi(\mathbf{a}x - \mathbf{t})\rangle = |0\rangle \sum_{x \in \mathbb{Z}_q} |x, \phi(\mathbf{a}x)\rangle + |1\rangle \sum_{x \in \mathbb{Z}_q} |x + s, \phi(\mathbf{a}x - \mathbf{e})\rangle \,.$$

We then measure the last register (classically known and omitted) and hopefully obtain a superposition $|0\rangle |x\rangle + |1\rangle |x + s\rangle$. This approach has several notable advantages. First, by using a grid over the torus $\mathbb{R}^m/q\mathbb{R}^m$, the only source of failure is the position of the cell delimitation (coordinates cannot spill over, they wrap around). Second, we directly end up with a DCP state, not a vectorial variant thereof. Third, and most importantly, the DCP modulus N is only q and not $2^{\mathcal{O}(m^2)}$. Note that m should be set as $\Omega(\log q)$ for s to be uniquely determined by the LWE samples. This improvement results in a much tighter reduction.

The improvement stems from the use of a small modulus q rather than large integer coordinates. It is possible to obtain such a small DCP modulus while starting from BDD (rather than LWE), by modifying Regev's reduction as follows. One may first reduce BDD to a variant thereof that asks to find the coordinates of the BDD solution modulo a small modulus q rather than over the integers. Such a reduction is presented in [29, Lemma 3.5]. One may then reduce this BDD variant to DCP as we proceed for LWE. Note that this transformation makes the BDD to DCP reduction from [27] iterative: the DCP oracle is called several times, and the input of an oracle call depends on the output of the previous oracle calls. This is akin to the phenomenon described in the *open questions* paragraph from [7].

A further difference between our reduction and the one from [27] is that we consider larger multiples of s in the input superposition to obtain a state of the form $\sum_j \rho_r(j) |j\rangle |x + js\rangle$, with $r \approx 1/\alpha$ (up to polynomial factors). This does not lead to any extra complication, but leads us to G-EDCP rather than DCP, which we crucially need to allow for a converse reduction. We conjecture that G-EDCP is strictly easier than DCP.

As Regev [26], we can also improve the resulting deviation parameter r of G-EDCP by a factor of $\sqrt{m}$ using balls' intersections rather than cube separation. We consider intersections of balls drawn around $\mathbf{a} \cdot s$ and its noisy shifts. The radius R of each ball is set to be the largest value such that the balls arising from different s (and their shifts) do not intersect. We are interested in the intersection area the balls drawn around $\pm s, \pm 2s$, etc. Following Regev [26], this area is large enough to guarantee that once we measure, we hit a point from the intersection of all the balls (see grey areas in Figure 3).

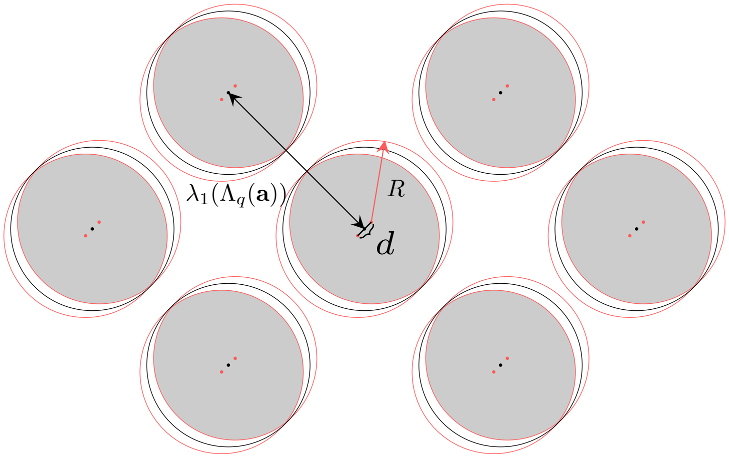


Fig. 3: A visualization of the balls' intersections. The lattice points (black dots) are of distance first minimum of lattice $\mathbf{a}\mathbb{Z}_q + q\mathbb{Z}$ to each other. The distance between the two furtherst shifts $\|j\mathbf{e}\|$ (red dots) has an upper bound, denoted by d. Each ball has a radius R chosen to be (approximately) $\lambda_1(\Lambda_q(\mathbf{a}))/2$, where $\Lambda_q(\mathbf{a}) = \mathbf{a}\mathbb{Z}_q + q\mathbb{Z}$. Note that once the shaded gray area is measured, the reduction succeeds in outputting an G-EDCP sample. For the reduction to work with a constant success probability, the shaded area has to have a large enough proportion compared to the volume of the balls.

The same algorithm provides a reduction from dLWE to dG-EDCP. Given a random sample $(\mathbf{a}, \mathbf{b}) \in \mathbb{Z}_q^m \times \mathbb{Z}_q^m$, it suffices to show that all the balls centered at $\mathbf{a}s + j\mathbf{b}$ for $s \in \mathbb{Z}_q$ and $j \in \mathbb{Z}$, do not intersect with each other. All the points considered above form the lattice $(\mathbf{a}|\mathbf{b})\mathbb{Z}_q + q\mathbb{Z}$, We argue analogously using the upper-bound on the minima of this lattice. As a result, the superposition collapses exactly to one of the balls, which gives a random sample of dG-EDCP.

1.2 Open problems

Towards an alternative reduction from EDCP *to* LWE. In [9], Childs and van Dam obtain a state of the form

$$\sum_{a \in \mathbb{Z}_N} \sum_{\substack{\mathbf{j} \in \{0,\ldots,M-1\}^\ell \\ \langle \mathbf{j}, \mathbf{y} \rangle = a \bmod N}} \omega_N^{a \cdot s} |\mathbf{j}\rangle \, .$$

for some uniform $\mathbf{y} \in \mathbb{Z}_N^\ell$. Note the uniform distribution of weights for $\mathbf{j}$. To recover s, the authors use the Pretty Good Measurement technique from [16] as was done in [2, 3] for similar problems. Implementing this general technique to this particular setup requires the construction of a POVM with operators corresponding to superpositions of *all* the $\mathbf{j}$'s in $\{0, \ldots, M-1\}^\ell$ such that $\langle \mathbf{j}, \mathbf{y} \rangle = a \bmod N$. As we already mentioned, a unitary operator that realizes such a POVM, uses a lattice-reduction technique as its main subroutine and, hence, works efficiently only for large values of M.

The question we do not address here is the interpretation of the POVM technique (and, possibly, a different reduction to LWE) for Gaussian-weighted superpositions. It might be simpler to obtain Gaussian $\mathbf{j}$'s rather than uniform from a cube, and hence it is possible that such a technique may lead to an improved reduction to LWE.

Hardness of EDCP *with more input states.* We show in this work that LWE and U-EDCP are computationally equivalent up to small parameter losses, when the number of U-EDCP states ℓ is polynomial. In these reductions, the U-EDCP bound M is within a polynomial factor of the LWE noise rate $1/\alpha$. When more states are available, U-EDCP is likely to become easier. For instance, with $M = 2$, the best known algorithms when ℓ is polynomially bounded are exponential. Oppositely, Kuperberg's algorithm [17] runs in time $2^{\widetilde{O}(\sqrt{\log N})}$ when $\ell = 2^{\widetilde{O}(\sqrt{\log N})}$. This suggests that there may be a U-EDCP self-reduction allowing to trade ℓ for M: Is it possible to reduce $\mathrm{EDCP}_{N,\ell,M}$ to $\mathrm{EDCP}_{N,\ell',M'}$ with $\ell' \leq \ell$, while allowing for $M' \geq M$?

2 Prerequisites

Notations. We use lower case bold letters to denote vectors and upper case bold to denote matrices. For a vector $\mathbf{x}$, we let $\|\mathbf{x}\|_\infty$ denote its ℓ_∞ norm and $\|\mathbf{x}\|$ denote its ℓ_2 norm. We let $\mathbb{Z}_N$ denote the cyclic group $\{0, 1, \cdots, N-1\}$ with addition modulo N. We assume we can compute with real numbers. All the arguments are valid if a sufficiently accurate approximation is used instead. For a distribution D, the notation $x \hookleftarrow D$ means that x is sampled from D. For a set S, we let $x \hookleftarrow S$ denote that x is a uniformly random element from S.

For any $r > 0$, we let $\rho_r(\mathbf{x})$ denote $\exp(-\pi\|\mathbf{x}\|^2/r^2)$, where $\mathbf{x} \in \mathbb{R}^n$ for a positive integer n. We let $\mathcal{D}_{\mathbb{Z},r}$ denote a Gaussian distribution over the integers with density function proportional to $\rho_r(\cdot)$. We let $\mathcal{D}_{\varLambda,r,\mathbf{c}}$ denote the Gaussian distribution over the n-dimensional lattice $\varLambda$ (for a positive integer n), with standard deviation parameter $r \in \mathbb{R}$ and center $\mathbf{c} \in \mathbb{R}^n$. If $\mathbf{c} = \mathbf{0}$, we omit it. We let $\mathcal{B}_n(\mathbf{c}, R)$ denote the n-dimensional Euclidean ball of radius R centered at $\mathbf{c} \in \mathbb{R}^n$ and $\mathcal{B}_n$ denotes the n-dimensional Euclidean unit ball centered at $\mathbf{0}$. We use ω_N as a short-hand for $\exp(2\pi i/N)$.

For a lattice $\varLambda$ with a basis $\mathbf{B}$, the parallelepiped $\mathcal{P}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} : 0 \leq x_i \leq 1\}$ is a fundamental domain of $\varLambda$. We let $\lambda_1(\varLambda)$ (resp. $\lambda_1^\infty(\varLambda)$) denote the ℓ_2-norm (ℓ_∞-norm) of a shortest vector of $\varLambda$. We let $\varLambda^\star = \{\mathbf{y} \in \mathbb{R}^n : \forall \mathbf{x} \in \varLambda, \langle \mathbf{x}, \mathbf{y} \rangle \in \mathbb{Z}\}$

$$\begin{tikzcd}
 & \mathrm{LWE}^{m}_{\substack{n,q,\alpha<1/(rm\ell q^{n/m}) \\ n,q,\alpha<1/(r\sqrt{m}\ell q^{n/m})}} \arrow[d, "\text{Theorems 2, 3}"] & & \\
\mathrm{EDCP}^{\ell\kappa^{1.5}}_{n,q,\sqrt{\kappa}r} \arrow[r, "\text{Lemma 9}"] \arrow[rrd, "\text{Lemma 10}"'] & \mathrm{EDCP}^{\ell}_{n,q,r} \arrow[r, "\text{Lemma 8}"] \arrow[rrd, "\text{Lemma 11}"'] \arrow[dd, "\text{Theorem 4}"] & \mathrm{EDCP}^{\ell/\kappa}_{n,q,r} \arrow[r, "\text{Lemma 10}"] & \mathrm{DCP}^{\ell/(\kappa^2 r)}_{q} \\
 & & \mathrm{EDCP}^{\ell}_{n,q,r} & \mathrm{DCP}^{\ell/(\kappa^2 \log r)}_{q} \\
 & \mathrm{LWE}^{\ell}_{1,q,\alpha>1/r} & &
\end{tikzcd}$$

Fig. 4: Graph of reductions between the extrapolated Dihedral Coset Problem instantiated with uniform distribution over $\{0, 1, \ldots, r-1\}$ (the first and the third problems from the left) and ℓ-sample Gaussian EDCP with parameter r (the middle problem). We assume all the parameters n (the dimension), q (the modulus) and r are functions of a common parameter κ. The most relevant choice of such a relation one can keep in mind is when n, ℓ, q and r are poly(κ). One can trace the losses in the parameters (with respect to the number of samples ℓ and to r) once we move from one problem to another. Notice that some reductions may be performed in two ways. For example, using the self-reducibility property of EDCP (Lemma 10), we can bypass Gaussian EDCP and have a more sample-efficient reduction from EDCP with large r to an EDCP with smaller r. Similarly, Gaussian EDCP can be reduced to DCP either directly (Lemma 11) or via uniform EDCP.
The two central reductions that show equivalence between LWE and EDCP problems are on the vertical line. As for EDCP, the LWE parameters n, q, and α are functions of κ. We present two reductions from LWE to EDCP, the stronger one gives a tighter result for the error-parameter by a factor of $\sqrt{m}$.

denote the dual of a lattice Λ. We define the smoothing parameter $\eta_\varepsilon(\Lambda)$ as be the smallest r such that $\rho_{1/r}(\Lambda^\star\backslash\{\mathbf{0}\}) \leq \varepsilon$ for an n-dimensional lattice Λ and positive $\varepsilon > 0$.

For $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$, we define two lattices $\Lambda_q(\mathbf{A}) = \{\mathbf{Ax} \bmod q \colon \mathbf{x} \in \mathbb{Z}_q^n\}$ and $\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}_q^n \text{ s.t. } \mathbf{Ay} = \mathbf{0} \bmod q\}$.

We introduce a variable κ to relate all the parameters involved in the definitions below. Namely, n, q, etc. are actually functions in κ: $n(\kappa)$, $q(\kappa)$. We omit the variable κ for clarity.

Definition 1 (Search LWE). *Given a parameter κ, the input to the search* $\mathrm{LWE}^m_{n,q,\chi}$ *with dimension $n \geq 1$, modulus $q \geq 2$ and distribution χ over $\mathbb{Z}$, consists of $m \geq n$ many samples of the form $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, with $\mathbf{a} \hookleftarrow \mathbb{Z}_q^n$, $b = \langle \mathbf{a}, \mathbf{s}\rangle + e$ and $e \hookleftarrow \chi$, where $s \in \mathbb{Z}_q^n$ is uniformly chosen. We say that an algorithm solves the search* $\mathrm{LWE}^m_{n,q,\chi}$ *if it outputs* $\mathbf{s}$ *with probability* $\mathrm{poly}(1/(n \log q))$ *in time* $\mathrm{poly}(n \log q)$.

Definition 2 (Decision LWE). *Given a parameter κ, the decisional* $\mathrm{LWE}^m_{n,q,\chi}$ *with dimension $n \geq 1$, modulus $q \geq 2$ and distribution χ over $\mathbb{Z}$, asks to distinguish between $m \geq n$ many* LWE *samples and random samples of the form $(\mathbf{a}, b) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$, with $\mathbf{a} \hookleftarrow \mathbb{Z}_q^n$, $b \hookleftarrow \mathbb{Z}_q$. We say that an algorithm solves the decisional* $\mathrm{LWE}^m_{n,q,\chi}$ *if it succeeds in distinguishing with probability* $\mathrm{poly}(1/(n \log q))$ *in time* $\mathrm{poly}(n \log q)$.

We let $\mathrm{LWE}^m_{n,q,\alpha}$ (resp. $\mathrm{dLWE}^m_{n,q,\alpha}$) denote search (resp. decisional) LWE problem with m samples of dimension n, modulus q, error distributed as $\mathcal{D}_{\mathbb{Z},\alpha q}$.

Definition 3 (Dihedral Coset Problem). *Given a parameter κ, the input to the* DCP^ℓ_N *with modulus N consists of ℓ states. Each state is of the form (normalization is omitted)*

$$|0\rangle |x\rangle \ + \ |1\rangle |(x+s) \bmod N\rangle , \tag{1}$$

stored on $1 + \lceil \log_2 N \rceil$ qubits, where $x \in \mathbb{Z}_N$ is arbitrary and $s \in \mathbb{Z}_N$ is fixed throughout all the states. We say that an algorithm solves DCP^ℓ_N *if it outputs s with probability* $\mathrm{poly}(1/\log N)$ *in time* $\mathrm{poly}(\log N)$.

Note that Regev in [25] defines the Dihedral Coset problem slightly differently. Namely, he introduces a failure parameter $f(\kappa)$, and with probability $\leq 1/(\log N(\kappa)^{f(\kappa)})$, we have a state of the form $|b\rangle |x\rangle$ for arbitrary $b \in \{0,1\}^n$ and $x \in \mathbb{Z}_N$. Such a state does not contain any information on s. Our definition takes 0 for the failure parameter. Conversely, Regev's definition is our Def. 3 with a reduced number of input states.

Now we define the problem which can be viewed as an extension of DCP. Analogous to LWE, it has two versions: search and decisional.

Definition 4 (Search Extrapolated Dihedral Coset Problem). *Given a parameter κ, the input to the search Extrapolated Dihedral Coset Problem*

($\mathrm{EDCP}^{\ell}_{n,N,D}$*) with dimension* n*, modulus* N *and a discrete distribution* D*, consists of* ℓ *input states of the form (normalization is omitted)*

$$\sum_{j \in \mathrm{supp}(D)} D(j) \left| j \right\rangle \left| (\mathbf{x} + j \cdot \mathbf{s}) \bmod N \right\rangle , \tag{2}$$

where $\mathbf{x} \in \mathbb{Z}_N^n$ *is arbitrary and* $\mathbf{s} \in \mathbb{Z}_N^n$ *is fixed for all* ℓ *states. We say that an algorithm solves search* $\mathrm{EDCP}^{\ell}_{n,N,D}$ *if it outputs* $\mathbf{s}$ *with probability* $\mathrm{poly}(1/(n \log N))$ *in time* $\mathrm{poly}(n \log N)$*.*

Definition 5 (Decisional Extrapolated Dihedral Coset Problem). *Given a parameter* κ*, the decisional Extrapolated Dihedral Coset Problem* ($\mathrm{dEDCP}^{\ell}_{n,N,D}$) *with modulus* N *and a discrete distribution* D*, asks to distinguish between* ℓ *many* EDCP *samples and* ℓ *many random samples of the form*

$$\left| j_k \right\rangle \left| \mathbf{x}_k \bmod N \right\rangle , \tag{3}$$

where $j_k \hookleftarrow D^2$ *and* $\mathbf{x}_k \in \mathbb{Z}_N^n$ *is uniformly chosen for* $1 \leq k \leq \ell$*. We say that an algorithm solves* $\mathrm{dEDCP}^{\ell}_{n,N,D}$ *if it distinguishes the two cases with probability* $\mathrm{poly}(1/(n \log N))$ *in time* $\mathrm{poly}(n \log N)$*.*

Different choices of D give rise to different instantiations of EDCP. The two interesting ones are: (1) D is uniform over $\mathbb{Z}_M$ for some $M \in \mathbb{Z}$, which we further denote as U-$\mathrm{EDCP}^{\ell}_{n,N,M}$ and (2) D is Gaussian $\mathcal{D}_{\mathbb{Z},r}$, which we further denote as G-$\mathrm{EDCP}^{\ell}_{n,N,r}$. The former, named the generalized hidden shift problem, was already considered in [9]. The latter is central in our reductions. Correspondingly, we call the decisional version of G-EDCP by dG-EDCP.

Gaussian distribution on lattices. In the following, we recall some important properties of discrete Gaussian distribution.

Lemma 1. *For any* $\kappa, r > 0$*, we have* $\rho_r(\mathbb{Z} \backslash [-\sqrt{\kappa} r, \sqrt{\kappa} r]) < 2^{-\Omega(\kappa)} \rho_r(\mathbb{Z})$*.*

A proof can be found in Appendix A in the full version [6].

From Lemma 1, we can see that the tail of Gaussian distribution has only negligible proportion compared to the whole sum. We use this fact within a quantum superposition state. For a quantum superposition state with Gaussian amplitudes, the superposition corresponding to Gaussian distribution over full lattice and the one without Gaussian tail have exponentially small ℓ_2 distance.

Lemma 2 ([4, Lemma 1.5(ii)]). *For any* n*-dimensional lattice* Λ *and* $\mathbf{u} \in \mathbb{R}^n$*, it holds that*

$$\rho_r(\Lambda + \mathbf{u} \backslash \mathcal{B}(\mathbf{0}, \sqrt{n} r)) < 2^{-\Omega(n)} \rho_r(\Lambda).$$

Lemma 3 (Poisson Summation Formula). *For any* n*-dimensional lattice* Λ *and vector* $\mathbf{u} \in \mathbb{R}^n$*, it holds that*

$$\rho_r(\Lambda + \mathbf{u}) = \det(\Lambda^{\star}) \cdot r^n \cdot \sum_{\mathbf{x} \in \Lambda^{\star}} e^{2\pi i \langle \mathbf{x}, \mathbf{u} \rangle} \rho_{1/r}(\mathbf{x}).$$

The following Lemma is originally due to Grover-Rudolph [15] and was adapted to Gaussian distribution in [29].

Lemma 4 (Adapted from [29, Lemma 3.12]). *Given a parameter κ and an integer r, there exists an efficient quantum algorithm that outputs a state that is within ℓ_2 distance $2^{-\Omega(\kappa)}$ of the normalized state corresponding to*

$$\sum_{x \in \mathbb{Z}} \rho_r(x) \left| x \right\rangle .$$

The following two lemmata are well-known facts about lower-bounds on minimum of q-ary lattices.

Lemma 5. *Given a uniformly chosen matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ for some positive integers q, m and n such that $m \geq n$, then we have $\lambda_1^{\infty}(\Lambda_q(\mathbf{A})) \geq q^{(m-n)/m}/2$ and $\lambda_1^{\infty}(\Lambda_q^{\perp}(\mathbf{A})) \geq q^{n/m}/2$ both with probability $1 - 2^{-m}$.*

Lemma 6. *Given a uniformly chosen matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$ for some positive integer q, m and n such that $m \geq n$, then we have $\lambda_1(\Lambda_q(\mathbf{A})) \geq \min\{q, \frac{\sqrt{m}q^{(m-n)/m}}{2\sqrt{2\pi e}}\}$ with probability $1 - 2^{-m}$.*

Reductions between EDCP *variants.* In the following, we show that the EDCP problem is analogue to the LWE problem in many aspects: (1) Gaussian-EDCP (G-EDCP$^{\ell'}_{n,N,r}$) and uniform-EDCP (U-EDCP$^{\ell}_{n,N,M}$) are equivalent, up to small parameter losses; (2) EDCP enjoys the self-reduction property as we show in Lemma 10. The main ingredient in both proofs is quantum rejection sampling due to Ozols et al. [22].

Lemma 7 ([22, Sec. 4]). *There is a quantum rejection sampling algorithm, which given as input*

$$\sum_{k=1}^{n} \pi_k \left| k \right\rangle \left| \eta_k \right\rangle ,$$

for some probability π_k, outputs

$$\frac{1}{\|\mathbf{p}\|} \sum_{k=1}^{n} p_k \left| k \right\rangle \left| \eta_k \right\rangle .$$

for some $p_k \leq \pi_k$, with probability $\|\mathbf{p}\|^2 = \sum_{k=1}^{n} p_k^2$.

Lemma 8 (G-EDCP $\leq$ U-EDCP). *Let N, n and ℓ be integers greater than 1, r be any real number, and let $M = c \cdot r$ for some constant c such that M is an integer. Then there is a probabilistic reduction with run-time polynomial in κ, from* G-EDCP$^{\ell}_{n,N,r}$ *to* U-EDCP$^{\mathcal{O}(\ell/\kappa)}_{n,N,M}$.

Proof. We are given as input G-EDCP$^{\ell}_{n,N,r}$ states:

$$\left\{ \sum_{j \in \mathbb{Z}} \rho_r(j) \left| j \right\rangle \left| (\mathbf{x}_k + j \cdot \mathbf{s}) \bmod N \right\rangle \right\}_{k \leq \ell} .$$

Our aim is to find $\mathbf{s}$, given access to a U-EDCP$^{\mathcal{O}(\ell/\kappa)}_{n,N,cr}$ oracle for some constant c.

For each G-EDCP$_{n,N,r}$ sample, we proceed as follows. We let $sign(x)$ to denote the sign of x, its output is either 1 (for '$+$') or 0 (for '$-$'). We first compute the sign of the first register and store it in a new register:

$$\sum_{j\in\mathbb{Z}} \rho_r(j) \left|j\right\rangle \left|(\mathbf{x}+j\cdot\mathbf{s}) \bmod N\right\rangle \left|sign(j)\right\rangle .$$

Second, we measure the third register. Note that we observe 1 with probability at least 1/2, independently over all k's. If the observed value is 0, we discard the state. From states with the observed value 1, we obtain (up to normalization):

$$\sum_{j\in\mathbb{Z}_+} \rho_r(j) \left|j\right\rangle \left|(\mathbf{x}+j\cdot\mathbf{s}) \bmod N\right\rangle .$$

Using quantum rejection sampling (Lemma 7), we transform a G-EDCP$_{N,\ell,r}$ state into a U-EDCP$_{n,N,M}$ state of the form

$$\sum_{j\in[0,M-1]} \left|j\right\rangle \left|(\mathbf{x}+j\cdot\mathbf{s}) \bmod N\right\rangle$$

with probability $\Omega(M\rho_r^2(c\cdot r)/r) = \Omega(1)$.

We repeat the above procedure until we obtain $\mathcal{O}(\ell/\kappa)$ many U-EDCP$_{n,N,M}$ states, which happens with probability $\geq 1-2^{-\Omega(\kappa)}$. We call the U-EDCP$^{\mathcal{O}(\ell/\kappa)}_{n,N,M}$ oracle to recover the secret $\mathbf{s}$ as the solution for the input G-EDCP$^{\ell}_{n,N,r}$ instance.

Lemma 9 (U-EDCP $\leq$ G-EDCP)**.** *Let N, M, n and ℓ be integers greater than 1, r be any real number, such that $M = \sqrt{\kappa}\cdot r = \mathrm{poly}(\kappa)$ is an integer. Then there is a probabilistic reduction with run-time polynomial in κ, from* U-EDCP$^{\ell}_{n,N,M}$ *to* G-EDCP$^{\mathcal{O}(\ell/\kappa^{1.5})}_{n,N,r}$.

Proof. We are given as input ℓ many U-EDCP$^{\ell}_{n,N,M}$ states:

$$\left\{ \sum_{j\in[0,M-1]} \left|j\right\rangle \left|(\mathbf{x}+j\cdot\mathbf{s}) \bmod N\right\rangle \right\}_{k\leq\ell} .$$

Our aim is to find $\mathbf{s}$, given access to a G-EDCP$^{\mathcal{O}(\ell/\kappa^{1.5})}_{n,N,r}$ oracle where $r = M/\sqrt{\kappa}$.

For each U-EDCP$_{n,N,M}$ state we proceed as follows. First, we symmetrize the uniform distribution by applying the function $f(x) = x - \lfloor (M-1)/2 \rfloor$ to the first register:

$$\sum_{j\in[0,M-1]} \left|j-\lfloor (M-1)/2\rfloor\right\rangle \left|(\mathbf{x}+j\cdot\mathbf{s}) \bmod N\right\rangle = \sum_{j'\in\left[-\lfloor \frac{M-1}{2}\rfloor, \lceil \frac{M-1}{2}\rceil\right]} \left|j'\right\rangle \left|(\mathbf{x}'+j'\cdot\mathbf{s}) \bmod N\right\rangle ,$$

where $j' = j - \lfloor (M-1)/2 \rfloor$, $\mathbf{x}' = \mathbf{x} + \lceil (M-1)/2 \rceil \cdot \mathbf{s}$.

Using rejection sampling (Lemma 7), with probability $\Omega(r/M) = \Omega(1/\sqrt{\kappa})$ we transform each U-EDCP$_{n,N,\lceil \frac{M-1}{2} \rceil}$ state into a G-EDCP$_{n,N,r}$ state:

$$\sum_{j' \in \left[-\lfloor \frac{M-1}{2} \rfloor, \lceil \frac{M-1}{2} \rceil\right]} \rho_r(j') \left|j'\right\rangle \left|(\mathbf{x}' + j' \cdot \mathbf{s}) \bmod N\right\rangle .$$

According to Lemma 1, the latter is within the ℓ_2 distance of $2^{-\Omega(\kappa)}$ away from the state

$$\sum_{j' \in \mathbb{Z}} \rho_r(j') \left|j'\right\rangle \left|(\mathbf{x}' + j' \cdot \mathbf{s}) \bmod N\right\rangle .$$

We repeat the above procedure until we obtain $\mathcal{O}(\ell/\kappa^{1.5})$ many G-EDCP$_{n,N,r}$ states, which happens with probability $\geq 1 - 2^{-\Omega(\kappa)}$. Then we can use the G-EDCP$^{\mathcal{O}(\ell/\kappa^{1.5})}_{n,N,r}$ oracle to recover the secret $\mathbf{s}$ as the solution to U-EDCP$^{\ell}_{n,N,M}$.

Next, we show the self-reducibility property for EDCP. We refer the reader to Appendix B in the full version [6] for the proof.

Lemma 10 (EDCP **self-reduction).** *Let $N, n,$ and ℓ be integers greater than 1, r_1 and r_2 be such that $r_1 > r_2$ and $r_1/r_2 = \mathcal{O}(\kappa^c)$ for any constant c. Then there is a probabilistic reduction with run-time polynomial in κ, from* G-EDCP$^{\ell}_{n,N,r_1}$ *(resp.* U-EDCP$^{\ell}_{n,N,r_1}$*) to* G-EDCP$^{\mathcal{O}(\ell/\kappa^{c+1})}_{n,N,r_2}$ *(resp.* U-EDCP$^{\mathcal{O}(\ell/\kappa^{c+1})}_{n,N,r_2}$*).*

In the following, we give a reduction from Gaussian-EDCP to DCP. Thus uniform-EDCP can also be reduced to DCP in two ways: either via self-reduction, or via Gaussian-EDCP as the next lemma shows. This result is especially interesting when the parameter r (or M for the uniform-EDCP) is super-polynomially large, as in this case, Lemma 10 cannot be applied. Lemma below works with 1-dimensional EDCP. This is without loss of generality as we can combine our main result (equivalence of LWE and EDCP) with the result of Brakerski et al. [7] (equivalence of LWE$_{n,q,\alpha}$ and LWE$_{1,q^n,\alpha}$).

Lemma 11 (Gaussian-EDCP **to** DCP**).** *Let N and ℓ be arbitrary integers. Then there is a probabilistic reduction with run-time polynomial in κ, from* G-EDCP$^{\ell}_{1,N,r}$ *to* DCP$^{\mathcal{O}(\ell/(\log r \cdot \kappa^2))}_{N}$ *if $r \geq 3\log N$, and from* G-EDCP$^{\ell}_{1,N,r}$ *to* DCP$^{\mathcal{O}(\ell/(r \cdot \kappa))}_{N}$ *otherwise.*

Proof. We are given as input ℓ many G-EDCP$_{1,N,r}$ states:

$$\left\{ \sum_{j \in \mathbb{Z}} \rho_r(j) \left|j\right\rangle \left|(x_k + j \cdot s) \bmod N\right\rangle \right\}_{k \leq \ell} .$$

We show how to find s if we are given access to a DCP$^{\mathcal{O}(\ell/(r \cdot \kappa))}_{N}$ oracle for $r < 3\log N$, and a DCP$^{\mathcal{O}(\ell/(\log r \cdot \kappa^2))}_{N}$ oracle otherwise.

• Case $r \geq 3\log N$.

According to Lemma 8, we can transform ℓ many G-EDCP$_{1,N,r}$ states into ℓ/κ many U-EDCP$_{1,N,M'}$ states with $M' = 2c \cdot r + 1$ for some constant c losing a factor of κ samples. Assume we obtain ℓ/κ many U-EDCP$_{1,N,M'}$ samples. For each such state, we symmetrize the interval $[0, M']$ as in the proof of Lemma 9. Then we receive a uniform distribution over $[-M, M]$ for $M = (M'-1)/2$. We compute the absolute value of the first register and store it in a new register:

$$\sum_{j \in [-M,M]} |j\rangle \, |(\hat{x}_k + j \cdot s) \bmod N\rangle \, ||j|\rangle \,, \tag{4}$$

where $\hat{x}_k = x_k - M \cdot s$. We measure the third register and denote the observed value by v_k.

We make use of the two well-known facts from number theory. For proofs, the reader may consult [30, Chapter 5]. First, there exist more than $M/\log M$ many primes that are smaller than M. Second, N has at most $2\log N/\log\log N$ prime factors. Thus there are at least $M/\log M - 2\log N/\log\log N$ many numbers smaller than M that are co-prime with all prime factors of N.

From the above, with probability $\Omega(1/\log M) = \Omega(1/\log r)$, the observed value v_k is non-zero and co-prime with N. If this is not the case, we discard the state. Otherwise, we obtain (up to normalization):

$$|-v_k\rangle \, |(\hat{x}_k - v_k \cdot s) \bmod N\rangle + |v_k\rangle \, |(\hat{x}_k + v_k \cdot s) \bmod N\rangle \,.$$

We multiply the value in the second register by $v_k^{-1} \bmod N$:

$$|-v_k\rangle \, |(x'_k - s) \bmod N\rangle + |v_k\rangle \, |(x'_k + s) \bmod N\rangle \,,$$

where $x'_k = \hat{x}_k \cdot v_k^{-1}$.

Let $\bar{x}_k = x'_k - s \bmod N$ and $\bar{s} = 2 \cdot s \bmod N$. Rewrite the above state as:

$$|-v_k\rangle \, |\bar{x}_k\rangle + |v_k\rangle \, |(\bar{x}_k + \bar{s}) \bmod N\rangle \,.$$

As we know v_k classically, we uncompute the first register and obtain a DCP state:

$$|0\rangle \, |\bar{x}_k\rangle + |1\rangle \, |(\bar{x}_k + \bar{s}) \bmod N\rangle \,. \tag{5}$$

We repeat the above procedure until we obtain $\mathcal{O}(\ell/(\log r \cdot \kappa^2))$ many DCP$_N$ states with probability $\geq 1 - 2^{-\Omega(\kappa)}$.

- Case that $r < 3\log N$.

The first steps are identical to the proof for the case $r \geq 3\log N$: Compute the absolute value of the first register to get a state as in (4) and measure the third register. Denote the observed value by v_k. Now we keep only those states, for which $v_k = 1$ was observed. Otherwise, we do not use the state. In case $v_k = 1$, we can easily transform the result to the state given in (5) analogously to the proof for $r \geq 3\log N$.

Now we show that $v_k = 1$ occurs with probability $\Omega(1/r)$ independently over all k's. Indeed,

$$\Pr[v_k = 1] = \frac{\rho_r(1)^2 + \rho_r(-1)^2}{\sum_{j \in \mathbb{Z}} \rho_r(j)^2} \geq \frac{2 \cdot \rho_r(1)^2}{\int_{\mathbb{R}} \rho_r(x)^2 \mathrm{d}x + 1} = \frac{2 \cdot \exp(-\frac{2\pi}{r^2})}{\frac{r}{\sqrt{2}} + 1} = \Omega\Big(\frac{1}{r}\Big).$$

We repeat the above procedure until we obtain $\mathcal{O}(\ell/(r\cdot\kappa))$ many DCP_N states, which happens with probability $\geq 1-2^{-\Omega(\kappa)}$.

In both cases considered in this lemma, we can use the $\mathrm{DCP}_N^{\mathcal{O}(\ell/(r\cdot\kappa))}$ oracle and get the secret $\bar{s}$. There are at most 2 possible values s such that $\bar{s}=2s \bmod N$: if there are 2 possibilities, we uniformly choose either, which decreases the success probability by at most a factor of 2.

3 Reduction from LWE to EDCP

In this section, we reduce $\mathrm{LWE}_{n,q,\alpha}^m$ to $\text{G-EDCP}_{n,q,r}^{\ell}$, where $r\approx 1/\alpha$ up to a factor of $\mathrm{poly}(n\log q)$. Analogous to Regev's reductions from uSVP to DCP, we present two versions of the reduction from LWE to G-EDCP. The second one is tighter with respect to the parameter losses. At the end of the section we show that using the same algorithm, one can reduce the decisional version of LWE to the decisional version of EDCP (see Def. 5).

3.1 First reduction: using cube separation

The main result of this section is the following theorem.

Theorem 2 (LWE $\leq$ EDCP)**.** *Let (n,q,α) be* LWE *parameters and (n,q,r) be* EDCP *parameters. Given $m=n\log q=\Omega(\kappa)$ many $\mathrm{LWE}_{n,q,\alpha}$ samples, there exists a probabilistic quantum reduction, with run-time polynomial in κ, from $\mathrm{LWE}_{n,q,\alpha}^m$ to $\text{G-EDCP}_{n,q,r}^{\ell}$, where $r<1/(32m\kappa\alpha\ell q^{n/m})$.*

The main step of our reduction is to partition the ambient space $\mathbb{R}^m$ with an appropriately chosen grid (cubes). This is analogous to Regev's reduction from uSVP to DCP [25]. Lemma 12 shows how we choose the width of the cell in our grid. Figure 2 gives a 2-dimensional example of such a grid.

Lemma 12. *For a constant $c\geq 8$, a matrix $\mathbf{A}\in\mathbb{Z}_q^{m\times n}$ is randomly chosen for integers q, n, $m=n\log q$, and $k\geq m$, consider a function*

$$g:(x_1,\cdots,x_m)\to(\lfloor x_1/z-w_1 \bmod \bar{q}\rfloor,\cdots,\lfloor x_m/z-w_m \bmod \bar{q}\rfloor),$$

where $z=q/c$ and $z\in[1/c,1/2]\cdot\lambda_1^\infty(\Lambda_q(\mathbf{A}))$, $w_1,\ldots,w_m$ are uniformly chosen from $[0,1)$, and $\bar{q}=q/z$. Then for any $\mathbf{x}\in\mathbb{Z}_q^n$, we have the following two statements.

- *For any $\mathbf{u}=\mathbf{A}\mathbf{x}+\mathbf{e}_1,\mathbf{v}=\mathbf{A}\mathbf{x}+\mathbf{e}_2$ where $\|\mathbf{e}_1\|_\infty,\|\mathbf{e}_2\|_\infty\leq\lambda_1^\infty(\Lambda_q(\mathbf{A}))/(2ck)$, with probability $(1-1/k)^m$, over the randomness of $w_1,\cdots,w_m$, we have $g(\mathbf{u})=g(\mathbf{v})$.*
- *For any $\mathbf{u}=\mathbf{A}\mathbf{x}+\mathbf{e}_1,\mathbf{v}=\mathbf{A}\widehat{\mathbf{x}}+\mathbf{e}_2$, where $\|\mathbf{e}_1\|_\infty,\|\mathbf{e}_2\|_\infty\leq\lambda_1^\infty(\Lambda_q(\mathbf{A}))/(2ck)$ and $\mathbf{x}\neq\widehat{\mathbf{x}}\in\mathbb{Z}_q^n$, we have $g(\mathbf{u})\neq g(\mathbf{v})$.*

Proof. • Proof for the first claim.

Write $\mathbf{u}=\mathbf{A}\mathbf{x}+\mathbf{e}_1 \bmod q$ and $\mathbf{v}=\mathbf{A}\mathbf{x}+\mathbf{e}_2 \bmod q$ for some $\mathbf{x}\in\mathbb{Z}_q^n$ and $\|\mathbf{e}_1\|_\infty,\|\mathbf{e}_2\|_\infty\leq\lambda_1^\infty(\Lambda_q(\mathbf{A}))/(2ck)$.

Let DIFF denote the event that $g(\mathbf{u}) \neq g(\mathbf{v})$, and, for all $i \leq m$, let DIFF_i denote the event that the i^{th} coordinates of $g(\mathbf{u})$ and $g(\mathbf{v})$ differ. Since we choose $w_1, \ldots, w_m$ independently and uniformly from $[0,1)$, we can consider each of m dimension separately and view each $e_{1,i}/z + w_i$ and $e_{2,i}/z + w_i$ as random 1-dim. real points inside an interval of length 1. We have

$$\Pr_{w_i}[\text{DIFF}_i] = \frac{|e_{1,i} - e_{2,i}|}{z} \leq \frac{z/k}{z} = \frac{1}{k},$$

where the inequality follows from the lower-bound on z. This implies

$$\Pr_{\mathbf{w}}[\text{NO DIFF}] = \prod_{i \leq m} \left(1 - \Pr_{w_i}[\text{DIFF}_i]\right) \geq \left(1 - \frac{1}{k}\right)^m .$$

- Proof for the second claim.

Write $\mathbf{u} = \mathbf{A}\mathbf{x} + \mathbf{e}_1 \bmod q$ and $\mathbf{v} = \mathbf{A}\widehat{\mathbf{x}} + \mathbf{e}_2 \bmod q$ for $\mathbf{x} \neq \widehat{\mathbf{x}} \in \mathbb{Z}_q^n$ and $\|\mathbf{e}_1\|_\infty, \|\mathbf{e}_2\|_\infty \leq \lambda_1^\infty(\Lambda_q(\mathbf{A}))/(2ck)$. Then we have

$$g(\mathbf{u}) = \left\lfloor \frac{1}{z} \cdot (\mathbf{A}\mathbf{x}) + \frac{1}{z} \cdot \mathbf{e}_1 + \mathbf{w} \bmod \bar{q} \right\rfloor,$$
$$g(\mathbf{v}) = \left\lfloor \frac{1}{z} \cdot (\mathbf{A}\widehat{\mathbf{x}}) + \frac{1}{z} \cdot \mathbf{e}_2 + \mathbf{w} \bmod \bar{q} \right\rfloor.$$

Now we show that $g(\mathbf{u})$ and $g(\mathbf{v})$ differ in at least 1 coordinate. This is the case if the arguments of the floor function differ by 1 in at least one coordinate, i.e., $\|\frac{1}{z}\mathbf{A} \cdot (\mathbf{x} - \hat{\mathbf{x}}) + \frac{1}{z}(\mathbf{e}_1 - \mathbf{e}_2) \bmod \bar{q}\|_\infty \geq 1$.

Assume the contrary is the case. Note that due to our choice of $\mathbf{e}_i$ and $\bar{q}$, $\|\frac{1}{z}(\mathbf{e}_1 - \mathbf{e}_2) \bmod \bar{q}\|_\infty$ is either at most $1/k$ or at least $\bar{q} - 1/k$. Either way we have $\|\frac{1}{z}\mathbf{A}(\mathbf{x} - \hat{\mathbf{x}}) \bmod \bar{q}\|_\infty < 1 + 1/k$ or $\|\frac{1}{z}\mathbf{A}(\mathbf{x} - \hat{\mathbf{x}}) \bmod \bar{q}\|_\infty > \bar{q} - 1 + 1/k$. Due to the bounds on z and c, the former case is equivalent to

$$\|\mathbf{A}(\mathbf{x} - \hat{\mathbf{x}}) \bmod \bar{q}\|_\infty < z + z/k \leq \lambda_1^\infty(\Lambda_{\bar{q}}(\mathbf{A}))\left(\tfrac{1}{2} + \tfrac{1}{2k}\right) \leq \lambda_1^\infty(\Lambda_{\bar{q}}(\mathbf{A})).$$

Hence, we have just found a vector in the lattice $\Lambda_{\bar{q}}(\mathbf{A})$ shorter than the minimum of the lattice. In the latter case when $\|\frac{1}{z}\mathbf{A} \cdot (\mathbf{x} - \hat{\mathbf{x}}) \bmod \bar{q}\|_\infty > \bar{q} - 1/k + 1$, we obtain the same contradiction by noticing that $\Lambda_{\bar{q}}$ contains $\bar{q}$-ary vectors.

Proof (of Theorem 2). Assume we are given an $\text{LWE}^m_{n,q,\alpha}$ instance $(\mathbf{A}, \mathbf{b}_0)$ with $\mathbf{b}_0 = \mathbf{A} \cdot \mathbf{s}_0 + \mathbf{e}_0 \bmod q$. Our aim is to find $\mathbf{s}_0$ given access to a $\text{G-EDCP}^\ell_{n,q,r}$ oracle.

We first prepare a necessary number of registers in the state $|0\rangle$ and transform them to the state of the form (normalization omitted)

$$\sum_{\mathbf{s} \in \mathbb{Z}_q^n} |0\rangle\, |\mathbf{s}\rangle\, |0\rangle\, . \tag{6}$$

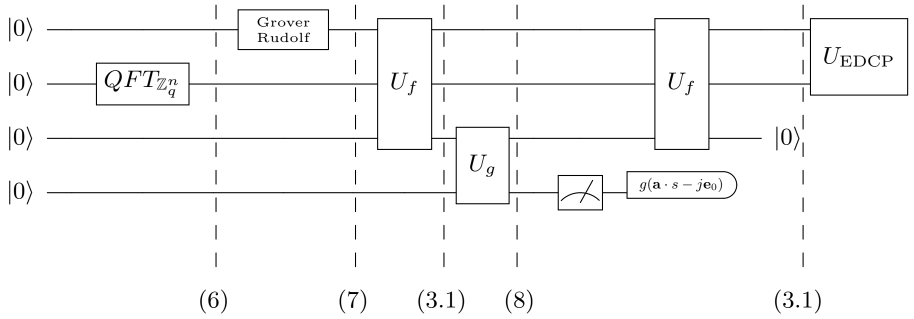


Fig. 5: Quantum circuit for our reduction LWE $\leq$ EDCP. All the global phases are omitted. The input registers are assumed to have the required number of qubits. Function f is defined as $U_f \left|j\right\rangle \left|s\right\rangle \left|0\right\rangle \rightarrow \left|j\right\rangle \left|\mathbf{s}\right\rangle \left|\mathbf{A}\mathbf{s} - j\mathbf{b} \bmod q\right\rangle$. Function U_g is the embedding of function g described in Lemma 12, i.e. $U_g \left|\mathbf{x}\right\rangle \left|0\right\rangle \rightarrow \left|\mathbf{x}\right\rangle \left|\lfloor \mathbf{x}/z - \mathbf{w} \bmod \bar{q}\rceil\right\rangle$ for appropriately chosen $z, \mathbf{w}, \bar{q}$.

We use Lemma 4 to obtain a state within ℓ_2 distance of $2^{-\Omega(\kappa)}$ away from

$$\sum_{\mathbf{s}\in\mathbb{Z}_q^n}\Big(\sum_{j\in\mathbb{Z}}\rho_r(j)\left|j\right\rangle\Big)\left|\mathbf{s}\right\rangle\left|0\right\rangle. \tag{7}$$

According to Lemma 1, the state above is within ℓ_2 distance of $2^{-\Omega(\kappa)}$ away from[3]

$$\sum_{\substack{\mathbf{s}\in\mathbb{Z}_q^n\\ j\in\mathbb{Z}\cap[-\sqrt{\kappa}\cdot r,\sqrt{\kappa}\cdot r]}}\rho_r(j)\left|j\right\rangle\left|\mathbf{s}\right\rangle\left|0\right\rangle.$$

We evaluate the function $f(j,\mathbf{s}) \mapsto \mathbf{A}\mathbf{s} - j\cdot\mathbf{b} \bmod q$ and store the result in the third register. The next equality follows from a change of variable on s

$$\sum_{\substack{\mathbf{s}\in\mathbb{Z}_q^n\\ j\in\mathbb{Z}\cap[-\sqrt{\kappa}\cdot r,\sqrt{\kappa}\cdot r]}}\rho_r(j)\left|j\right\rangle\left|\mathbf{s}\right\rangle\left|\mathbf{A}\mathbf{s} - j\cdot\mathbf{A}\mathbf{s}_0 - j\mathbf{e}_0\right\rangle = \sum_{\substack{\mathbf{s}\in\mathbb{Z}_q^n\\ j\in\mathbb{Z}\cap[-\sqrt{\kappa}\cdot r,\sqrt{\kappa}\cdot r]}}\rho_r(j)\left|j\right\rangle\left|\mathbf{s}+j\mathbf{s}_0\right\rangle\left|\mathbf{A}\mathbf{s} - j\mathbf{e}_0\right\rangle.$$

Sample $w_1,\ldots,w_m$ uniformly from $[0,1)$. Set $z = q/c$ for some constant $c \geq 8$, thus we have $z \in [1/c, 1/2]\cdot\lambda_1^\infty(\Lambda_q(\mathbf{A}))$, where the upper bound holds with probability $1 - 2^{-m} = 1 - 2^{-\Omega(\kappa)}$ (see Lemmata 5).

For $\mathbf{x} \in \mathbb{Z}_q^m$, we define

$$g(\mathbf{x}) = (\lfloor (x_1/z - w_1) \bmod \bar{q}\rceil, \ldots, \lfloor (x_m/z - w_m) \bmod \bar{q}\rceil),$$

[3] Here we cut the tail of the Gaussian distribution on the first register. Otherwise, a measurement that follows leads to a state mixed with noisy vectors from different lattice points with large (unbounded) noise. However, it has ℓ_2 distance exponentially close to the state we consider in the current algorithm.

where $\bar{q} = q/z = c$. We evaluate the function g on the third register and store the result on a new register. We obtain

$$\sum_{\substack{\mathbf{s}\in\mathbb{Z}_q^n \\ j\in\mathbb{Z}\cap[-\sqrt{\kappa}\cdot r,\sqrt{\kappa}\cdot r]}} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\cdot\mathbf{s}_0\rangle\,|\mathbf{A}\mathbf{s}-j\cdot\mathbf{e}_0\rangle\,|g(\mathbf{A}\mathbf{s}-j\cdot\mathbf{e}_0)\rangle\,. \tag{8}$$

We measure the fourth register and do not consider it further. According to Lemma 1, we have $\|\mathbf{e}_0\|_\infty \leq \sqrt{\kappa}\alpha q$ with probability $\geq 1-2^{-\Omega(m)} = 1-2^{-\Omega(\kappa)}$. Recall that $r < 1/(32m\ell\kappa\alpha q^{n/m}) \leq 1/(4ck\kappa\alpha q^{n/m})$ for $c = 8$ and $k = m\ell$. Therefore, we have $\|\sqrt{\kappa}r\cdot\mathbf{e}_0\|_\infty \leq \lambda_1^\infty(\Lambda_q(\mathbf{A}))/(2ck)$. Then by Lemma 12, we obtain

$$\sum_{j\in\mathbb{Z}\cap[-\sqrt{\kappa}\cdot r,\sqrt{\kappa}\cdot r]} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\cdot\mathbf{s}_0\rangle\,|\mathbf{A}\mathbf{s}-j\cdot\mathbf{e}_0\rangle$$

for some $\mathbf{s}\in\mathbb{Z}_q^n$, with probability $(1-1/k)^m$ over the randomness of $\mathbf{A}$ and $w_1,\cdots,w_m$.

Finally, we evaluate the function $(j,\mathbf{s},\mathbf{b}) \mapsto \mathbf{b}-\mathbf{A}\mathbf{s}+j\cdot\mathbf{b}_0$ on the first three registers, which gives $\mathbf{0}$. Discarding this $\mathbf{0}$-register, the state is of the form

$$\sum_{j\in\mathbb{Z}\cap[-\sqrt{\kappa}\cdot r,\sqrt{\kappa}\cdot r]} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\cdot\mathbf{s}_0\rangle\,.$$

According to Lemma 1, the above state is within ℓ_2 distance of $2^{-\Omega(\kappa)}$ away from

$$\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{s}+j\cdot\mathbf{s}_0\rangle\,.$$

We repeat the above procedure ℓ times, and with probability $(1-\frac{1}{k})^{m\ell}$, we obtain ℓ many G-EDCP$^\ell_{n,q,r}$ states

$$\left\{\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{x}_k+j\cdot\mathbf{s}_0\rangle\right\}_{k\leq\ell},$$

where $\mathbf{x}_k\in\mathbb{Z}_q^n$.

Now we can call the G-EDCP$^\ell_{n,q,r}$ oracle with the above states as input and obtain $\mathbf{s}_0$ as output of the oracle.

3.2 An improved reduction: using balls' intersection

Here we give an improved reduction from LWE to EDCP. Following the idea of Regev ([25][Section 3.3]), instead of separating the ambient space $\mathbb{Z}^m$ by cubes, we consider intersections of balls drawn around the points $\mathbf{A}\mathbf{s}$ and its shifts. Note that with this reduction we improve the upper-bound on r essentially by the factor of $\sqrt{m}$.

Theorem 3 (LWE $\leq$ EDCP)**.** *Let* (n, q, α) *be* LWE *parameters and* (n, q, r) *be* EDCP *parameters. Given* $m = \Omega(\kappa)$ *many* $\mathrm{LWE}_{n,q,\alpha}$ *samples, there exists a quantum reduction, with run-time polynomial in* κ*, from* $\mathrm{LWE}^m_{n,q,\alpha}$ *to* $\text{G-EDCP}^{\ell}_{n,q,r}$*, where* $r < 1/(6\sqrt{2\pi e}\sqrt{m\kappa}\ell\alpha q^{n/m})$*.*

We give an intuitive idea of how the reduction works. All the necessary lemmata and the full proof are given in Appendix B in the full version [6].

Informally, the reduction works as follows. Given an LWE instance $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s}_0 + \mathbf{e}_0) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, for each $\mathbf{s} \in \mathbb{Z}_q^n$, we consider (in a superposition over all such $\mathbf{s}$) a lattice point $\mathbf{A}\mathbf{s}$ together with its small shifts of $\mathbf{A}\mathbf{s} - j\mathbf{e}_0$, where j's are drawn from a small interval symmetric around 0. So far this is exactly what we did in the first (weaker) reduction. Note that we receive a configuration of points in $\mathbb{Z}_q^m$ as depicted in Figure 3. Note that contrary to Regev's reduction, where there is only one shift (i.e., the DCP case), our extrapolated version considers poly(κ) shifts thus leading us to the EDCP case.

Let us fix some $\mathbf{A}\mathbf{s}$ together with its shifts. Draw a ball around each shift of a maximal radius R such that there is no intersection between the shifts coming from different lattice points, i.e. there is no j, j' s.t. $\mathcal{B}(\mathbf{A}\mathbf{s} - j\mathbf{e}_0, R) \cap \mathcal{B}(\mathbf{A}\mathbf{s}' - j'\mathbf{e}_0, R) \neq \emptyset$ for any two $\mathbf{s}, \mathbf{s}'$ such that $\mathbf{s} \neq \mathbf{s}'$. To satisfy this condition, we can take R almost as large as the first minimum of the lattice $\Lambda_q(\mathbf{A})$ (again, see Figure 3). With such an R, due to the fact that the shifts are small, the intersection of the balls drawn around the shifts is large enough (see Lemma 13 in Appendix B of the full version [6]). Hence, once we measure the register that 'stores' our balls, the resulting state collapses (with large enough probability) to a superposition of some $\mathbf{A}\mathbf{s}$ for *one* $\mathbf{s}$ and all its shifts. Informally, the higher this probability is, the tighter the parameters achieved by the reduction.

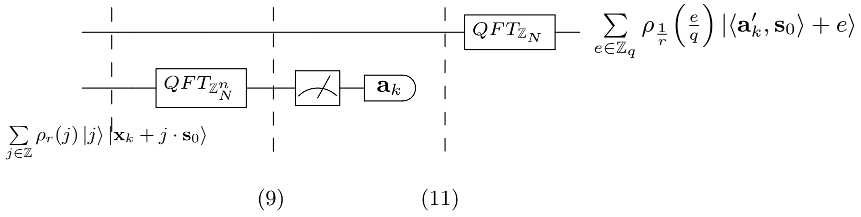
3.3 Reduction from dLWE to dEDCP

As a corollary to the above theorem, we show that the decisional LWE can be reduced to decisional EDCP. In fact, to establish the reduction, we use the same algorithm as for Theorem 3 (a weaker reduction given in Theorem 2 will work as well). Recall that in the proof, starting from an EDCP sample, we obtain an LWE sample with non-negligible probability. Corollary 1 below shows that in case we are given a tuple $(\mathbf{A}, \mathbf{b})$ drawn uniformly at random from $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^m$, the procedure described in Theorem 3 outputs a state of the form $|j\rangle\, |\mathbf{x} \bmod N\rangle$, a uniform counterpart to EDCP in the sense of Definition 5. A proof of the following corollary is given in Appendix B of the full version [6].

Corollary 1 (dLWE $\leq$ dEDCP)**.** *Let* (n, q, α) *be valid* dLWE *parameters and* (n, q, r) *be valid* dEDCP *parameters. Given* $m = \Omega(\kappa)$ *many* $\mathrm{LWE}_{n,q,\alpha}$ *samples, there exists a quantum reduction, with run-time polynomial in* κ*, from* $\mathrm{LWE}^m_{n,q,\alpha}$ *to* $\text{G-EDCP}^{\ell}_{n,q,r}$*, where* $r < 1/(6\sqrt{2\pi e}\sqrt{m\kappa}\ell\alpha q^{(n+1)/m})$*.*

4 Reduction from EDCP to LWE

In this section, we reduce G-EDCP$^{\ell}_{n,N,r}$ to LWE$^{\ell}_{n,N,\alpha}$, where $r \approx 1/\alpha$ up to a factor of poly$(n \log N)$. Combined with the result of the previous section, this gives us equivalence between the two problems: LWE and EDCP, for both search and decisional variants.



$QFT_{\mathbb{Z}_N}$
$\sum_{e\in\mathbb{Z}_q} \rho_{\frac{1}{r}}\left(\frac{e}{q}\right) |\langle \mathbf{a}'_k, \mathbf{s}_0\rangle + e\rangle$
$QFT_{\mathbb{Z}_N^n}$
$\mathbf{a}_k$
$\sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{x}_k + j\cdot\mathbf{s}_0\rangle$
(9)
(11)

Fig. 6: Reduction from G-EDCP to LWE

Theorem 4 (EDCP $\leq$ LWE)**.** *Let (n, N, r) be valid* EDCP *parameters and (n, N, α) with $r = \Omega(\sqrt{\kappa})$ be valid* LWE *parameters. Given $\ell = \Omega(\kappa)$ many* G-EDCP$_{n,N,r}$ *samples, there exists a quantum reduction, with run-time polynomial in κ, from* G-EDCP$^{\ell}_{n,N,r}$ *to* LWE$^{\ell}_{n,N,\alpha}$*, where $\alpha = 1/r$.*

Proof. Assume we are given ℓ many EDCP$_{n,N,r}$ instances

$$\left\{ \sum_{j\in\mathbb{Z}} \rho_r(j)\,|j\rangle\,|\mathbf{x}_k + j\cdot\mathbf{s}_0 \bmod N\rangle \right\}_{k\in[\ell]} .$$

Our aim is to find $\mathbf{s}_0$ given access to an LWE$^{\ell}_{n,N,\alpha}$ oracle.

For each input state, the quantum Fourier transform over $\mathbb{Z}_N^n$ is applied to the second register, which yields (without loss of generality, consider the k^{th} sample)

$$\sum_{\mathbf{a}\in\mathbb{Z}_N^n} \sum_{j\in\mathbb{Z}} \omega_N^{\langle \mathbf{a}, (\mathbf{x}_k + j\cdot\mathbf{s}_0)\rangle} \cdot \rho_r(j)\,|j\rangle\,|\mathbf{a}\rangle . \tag{9}$$

Then we measure the second register and let $\mathbf{a}_k$ denote the observed value. Note that each element of $\mathbb{Z}_N^n$ is measured with probability $1/N^n$ and that the distributions for different k's are independent. Omitting the global phase of each state, we obtain

$$\sum_{j\in\mathbb{Z}} \omega_N^{\langle \mathbf{a}_k, (j\cdot\mathbf{s}_0)\rangle} \cdot \rho_r(j)\,|j\rangle\,|\mathbf{a}_k\rangle . \tag{10}$$

We omit the second register as we know each $\mathbf{a}_k$ classically. Since $N \gg r$, from Lemma 1 it follows that the resulting state is within ℓ_2 distance of $2^{-\Omega(\kappa)}$ away from the state (note the change in the range for j)

$$\sum_{j\in\mathbb{Z}_N} \omega_N^{j\cdot\langle \mathbf{a}_k, \mathbf{s}_0\rangle} \cdot \rho_r(j)\,|j\rangle . \tag{11}$$

For each such an input state, the quantum Fourier transform over $\mathbb{Z}_N$ yields

$$\sum_{b\in\mathbb{Z}_N}\sum_{j\in\mathbb{Z}_N}\omega_N^{j\cdot(\langle\mathbf{a}_k,\mathbf{s}_0\rangle+b)}\cdot\rho_r(j)\,|b\rangle\,. \tag{12}$$

Once again we use Lemma 1 to argue that the state above is within ℓ_2 distance of $2^{-\Omega(\kappa)}$ away from the state

$$\sum_{b\in\mathbb{Z}_N}\sum_{j\in\mathbb{Z}}\omega_N^{j\cdot(\langle\mathbf{a}_k,\mathbf{s}_0\rangle+b)}\cdot\rho_r(j)\,|b\rangle\,.$$

Using the Poisson summation formula (Lemma 3) and changing the summation variable to $e\leftarrow N\cdot j+\langle\mathbf{a}_k,\mathbf{s}_0\rangle+b$, the above state can be rewritten as

$$\sum_{b\in\mathbb{Z}_N}\sum_{j\in\mathbb{Z}}\rho_{1/r}\Big(j+\frac{\langle\mathbf{a}_k,\mathbf{s}_0\rangle+b}{N}\Big)\,|b\rangle=\sum_{e\in\mathbb{Z}}\rho_{1/r}\Big(\frac{e}{N}\Big)\,|\langle\mathbf{a}'_k,\mathbf{s}_0\rangle+e \bmod N\rangle$$

where $\mathbf{a}'_k=-\mathbf{a}_k \bmod N$. Since $r=\Omega(\sqrt{\kappa})$, we can apply Lemma 1 to the above state (for a scaled $\mathbb{Z}$-lattice), and instead of the above state, consider the state that is within a $2^{-\Omega(\kappa)}$ ℓ_2-distance from it, namely:

$$\sum_{e\in\mathbb{Z}_N}\rho_{1/r}\Big(\frac{e}{N}\Big)\,|\langle\mathbf{a}'_k,\mathbf{s}_0\rangle+e\rangle\,. \tag{13}$$

Once we measure the state above, we obtain an LWE sample

$$(\mathbf{a}'_k,\langle\mathbf{a}'_k,\mathbf{s}_0\rangle+e_k)\,,$$

where $e_k\hookleftarrow\mathcal{D}_{\mathbb{Z},N/r}$.

Now we can call the $\mathrm{LWE}_{n,N,\alpha}$ oracle for $\alpha=1/r$ with the above states as input and obtain $\mathbf{s}_0$ as output of the oracle.

4.1 Reduction from dEDCP to dLWE

Similar to the previous section where as a corollary we show that dLWE can be reduced to dEDCP, we finish this section by a reverse reduction. Again we use exactly the same reduction algorithm as for the search versions (see Figure 6). Thus it remains to show that we can obtain a uniform random sample $(\mathbf{a},b)\in\mathbb{Z}_N^n\times\mathbb{Z}_N$ given as input a state of the form $|j\rangle\,|\mathbf{x} \bmod N\rangle$.

Corollary 2 **(dEDCP $\leq$ dLWE).** *Let (n,N,r) be valid* dG-EDCP *parameters and (n,N,α) be valid* dLWE *parameters. Given $\ell=\Omega(\kappa)$ many* $\mathrm{EDCP}_{n,N,r}$ *samples, there exists a quantum reduction, with run-time polynomial in κ, from* $\text{dG-EDCP}^{\ell}_{n,N,r}$ *to* $\mathrm{dLWE}^{\ell}_{n,N,\alpha}$*, where $\alpha=1/r$.*

Proof. Assume we are given ℓ many samples of $\mathrm{EDCP}_{n,N,r}$ either of the form

$$\left\{\sum_{j\in\mathbb{Z}}\rho_r(j)\,|j\rangle\,|\mathbf{x}_k+j\cdot\mathbf{s}_0\rangle \bmod N\right\}_{k\in[\ell]}$$

or of the form

$$\{|j_k\rangle\,|\mathbf{x}_k \bmod N\rangle\}_{k\in[\ell]}\,,$$

where $j_k \hookleftarrow \mathcal{D}^2_{\mathbb{Z},r}$ and $\mathbf{x}_k \in \mathbb{Z}_N^n$ is uniform. Our aim is to distinguish between the above two forms given access to a $\mathrm{dLWE}_{n,N,\alpha}$ oracle.

As explained above, we assume that random samples of EDCP are given. For each input state, after the quantum Fourier transform over $\mathbb{Z}_N^n$ on the second register, we obtain

$$\sum_{a\in\mathbb{Z}_N^n} \omega_N^{\langle \mathbf{x}_k,\mathbf{a}\rangle}\,|j_k\rangle\,|\mathbf{a}\rangle\,.$$

Then we measure the second register and let $\mathbf{a}_k$ denote the observed value. Note that each element of $\mathbb{Z}_N^n$ is measured with probability $1/N^n$ and that the distributions for different k's are independent. Up to a global phase, we have

$$|j_k\rangle\,|\mathbf{a}_k\rangle\,.$$

We omit the second register which is known to us. According to Lemma 1, with probability $1-2^{-\Omega(\kappa)}$, the value stored in the first register is in the range $[-\lfloor N/2\rfloor, \lceil N/2\rceil - 1]$. Applying QFT over $\mathbb{Z}_N$ to the first register, we obtain

$$\sum_{b\in\mathbb{Z}_N} \omega_N^{j_k\cdot b}\,|b\rangle\,.$$

Once we measure the state above and let b_k denote the observed value. Note that each element of $\mathbb{Z}_N$ is measured with probability $1/N$ and that the distributions for different k's are independent. We obtain a sample

$$(\mathbf{a}_k, b_k)\,,$$

where $(\mathbf{a}_k, b_k)$ are uniformly random from $\mathbb{Z}_N^n \times \mathbb{Z}_N$.

References

1. L. Babai. On Lovász lattice reduction and the nearest lattice point problem. *Combinatorica*, 6:1–13, 1986.
2. D. Bacon, A. M. Childs, and W. van Dam. From optimal measurement to efficient quantum algorithms for the hidden subgroup problem over semidirect product groups. In *Proc. or FOCS*, pages 469–478. IEEE Computer Society Press, 2005.
3. D. Bacon, A. M. Childs, and W. van Dam. Optimal measurements for the dihedral hidden subgroup problem. *Chicago J. Theor. Comput. Sci.*, 2006.
4. W. Banaszczyk. New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen*, 296(4):625–635, 1993.
5. D. J. Bernstein, J. Buchmann, and E. Dahmen. *Post Quantum Cryptography.* Springer, 1st edition, 2008.
6. Z. Brakerski, E. Kirshanova, D. Stehlé, and Wen W. Learning with errors and extrapolated dihedral cosets. *CoRR*, abs/1710.08223, 2017.
7. Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé. Classical hardness of learning with errors. In *Proc. of STOC*, pages 575–584. ACM, 2013.

8. Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proc. of FOCS*, pages 97–106. IEEE Computer Society Press, 2011.
9. A. M. Childs and W. van Dam. Quantum algorithm for a generalized hidden shift problem. In *Proc. of SODA*, pages 1225–1232. SIAM, 2007.
10. M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In *Proc. of STACS*, volume 1563 of *LNCS*, pages 478–487. Springer, 1999.
11. K. Friedl, G. Ivanyos, F. Magniez, M. Santha, and P. Sen. Hidden translation and translating coset in quantum computing. *SIAM J. Comput*, 43(1):1–24, 2014.
12. C. Gentry, C. Peikert, and V. Vaikuntanathan. Trapdoors for hard lattices and new cryptographic constructions. In *Proc. of STOC*, pages 197–206. ACM, 2008. Full version available at `http://eprint.iacr.org/2007/432.pdf`.
13. S. Goldwasser, Y. T. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich. Reusable garbled circuits and succinct functional encryption. In *Proc. of STOC*, pages 555–564. ACM, 2013.
14. S. Gorbunov, V. Vaikuntanathan, and H. Wee. Attribute-based encryption for circuits. In *Proc. of STOC*, pages 545–554. ACM, 2013.
15. L. Grover and T. Rudolph. Creating superpositions that correspond to efficiently integrable probability distributions, 2002. Draft. Available at `https://arxiv.org/pdf/quant-ph/0208112v1`.
16. P. Hausladen and W. K. Wootters. A pretty good measurement for distinguishing quantum states. *Journal of Modern Optics*, 41(12):2385–2390, 1994.
17. G. Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput*, 35(1):170–188, 2005.
18. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann*, 261:515–534, 1982.
19. H. W. Lenstra, Jr. Integer programming with a fixed number of variables. *Mathematics of Operations Research*, 8(4):538–548, 1983.
20. V. Lyubashevsky and D. Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In *Proc. of CRYPTO*, pages 577–594, 2009.
21. D. Micciancio and O. Regev. Lattice-based cryptography. In *Post-Quantum Cryptography, D. J. Bernstein, J. Buchmann, E. Dahmen (Eds)*, pages 147–191. Springer, 2009.
22. M. Ozols, M. Roetteler, and J. Roland. Quantum rejection sampling. *ACM Trans. Comput. Theory*, 5(3):11:1–11:33, August 2013.
23. C. Peikert. Public-key cryptosystems from the worst-case shortest vector problem. In *Proc. of STOC*, pages 333–342. ACM, 2009.
24. C. Peikert. A decade of lattice cryptography. *Foundations and Trends in Theoretical Computer Science*, 10(4):283–424, 2016.
25. O. Regev. Quantum computation and lattice problems. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, pages 520–529. IEEE Computer Society, 2002.
26. O. Regev. New lattice-based cryptographic constructions. *J. ACM*, 51(6):899–942, 2004.
27. O. Regev. Quantum computation and lattice problems. *SIAM J. Comput*, 33(3):738–760, 2004.
28. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of STOC*, pages 84–93. ACM, 2005.

29. O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), 2009.
30. Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, New York, NY, USA, 2005.
31. D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *Proc. of ASIACRYPT*, volume 5912 of *LNCS*, pages 617–635. Springer, 2009.