

# Cyclotomic Cosets: Hidden Subgroup and Quantum Sieving Algorithm for Prime-Power Moduli

Mathias Boucher, Pierre-Alain Fouque, and Yixin Shen

Univ Rennes, Inria, CNRS, IRISA, Rennes, France

**Abstract.** The Learning With Errors (LWE) problem is a fundamental assumption in post-quantum cryptography. Regev established a quantum reduction from LWE to the Dihedral Coset Problem (DCP). Later, Brakerski et al. introduced the Extrapolated Dihedral Coset Problem (EDCP), proving its equivalence to LWE. However, unlike DCP, EDCP no longer admits a coset structure. This limits the direct application of techniques for hidden subgroup problems.

In this work, we introduce the Cyclotomic Coset Problem (CCP), a cyclotomic generalization of DCP that preserves an exact hidden-subgroup structure. Let  $\zeta_p$  be a primitive  $p$ -th root of unity, let  $\pi = \zeta_p - 1$ , and write  $q = p^t$  and  $L = t(p - 1)$ . We work over  $R_q = \mathbb{Z}_q[\zeta_p] \cong \mathbb{Z}[\zeta_p]/(\pi^L)$ , where the isomorphism follows from the total ramification identity  $(p) = (\pi)^{p-1}$ . We exploit the resulting  $\pi$ -adic ideal chain to construct a quantum sieve that successively reduces phase states modulo  $\pi^L, \pi^{L-1}, \dots, \pi$ . For every fixed prime  $p$  and modulus  $q = p^t$ , our algorithm solves the CCP in time and sample complexity  $2^{O_p(\log n \log q)}$ , using polynomial quantum space. The sieve also applies to uniform EDCP and Gaussian  $S$ [LWE], yielding quasi-polynomial time algorithms for all the above problems when  $q = \text{poly}(n)$ . This extends the power-of-two EDCP sieve of Bai et al. (CRYPTO 2025) to a cyclotomic setting.

However, we emphasize that our result does not, by itself, yield a quasi-polynomial-time algorithm for standard LWE, because the currently known reduction produces only a limited number of approximate CCP states.

**Keywords:** Learning With Errors, Dihedral Coset Problem, Extrapolated Dihedral Coset Problem, Hidden Subgroup Problem, Cyclotomic Rings, Kuperberg’s algorithm.

## 1 Introduction

The Learning With Errors problem (LWE), introduced by Regev in [16], is a cornerstone of post-quantum cryptography. In its search form, LWE asks to recover a secret vector  $\mathbf{s} \in \mathbb{Z}_q^n$  from noisy linear equations

$$b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \bmod q,$$

where the vectors  $\mathbf{a}_i$  are uniform in  $\mathbb{Z}_q^n$  and the errors  $e_i$  are sampled from a prescribed narrow distribution. The importance of LWE stems both from its versatility in cryptographic constructions and from quantum worst-case-to-average-case reductions relating it to fundamental lattice problems [16,17].

Quantum coset problems provide another perspective on the complexity of lattice problems. In earlier work, Regev established a connection between unique shortest-vector problems and the Dihedral Hidden Subgroup Problem [13]. Its coset-state formulation, known as the Dihedral Coset Problem (DCP), asks to recover a secret  $\mathbf{s} \in \mathbb{Z}_q^n$  from states of the form

$$\frac{1}{\sqrt{2}} (|0\rangle |\mathbf{x}\rangle + |1\rangle |\mathbf{x} + \mathbf{s}\rangle),$$

where  $\mathbf{x} \in \mathbb{Z}_q^n$  is uniformly random. DCP is particularly appealing because its input states are exact coset states of order-two subgroups of a generalized dihedral group.

Childs and van Dam considered in [8] the generalized hidden shift problem. It consists in finding a hidden shift  $s \in \mathbb{Z}_q$  given quantum samples of the form

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle |x_i + js\rangle$$

for randomly chosen  $x_i \in \mathbb{Z}_q$  and an integer  $M$ . They provided an efficient quantum algorithm based on "pretty good measurement" when  $M$  is large with respect to  $q$  ( $M = q^\epsilon$  for a constant  $\epsilon$ ).

Brakerski, Kirshanova, Stehlé, and Wen subsequently introduced the Extrapolated Dihedral Coset Problem (EDCP) [5]. In EDCP, the DCP state is replaced by

$$\sum_j f(j) |j\rangle |\mathbf{x} + j\mathbf{s}\rangle$$

for a prescribed amplitude function  $f$ . They proved that suitable Gaussian and uniform variants of EDCP are equivalent to LWE under quantum polynomial-time reductions, up to parameter losses. This equivalence provides a useful quantum formulation of the computational content of LWE. However, except in particular cases, the set of translations

$$\{(j\mathbf{s}, j) : j \in \text{supp}(f)\}$$

does not form a subgroup. General EDCP states therefore do not retain the exact hidden-subgroup structure of DCP.

Closely related quantum formulations arise by encoding the LWE error distribution in the amplitudes of a quantum state. In the  $S$  |LWE> problem introduced by Chen, Liu, and Zhandry [7], one is given uniformly random vectors  $\mathbf{a}_i \in \mathbb{Z}_q^n$ , together with quantum states of the following form

$$\sum_{e \in \mathbb{Z}_q} f(e) |\langle \mathbf{a}_i, \mathbf{s} \rangle + e \bmod q \rangle,$$

and the objective is again to recover  $\mathbf{s}$ . Applying a quantum Fourier transform moves the secret into a phase and produces states closely related to phase formulations of EDCP.

*Quantum sieving.* DCP admits subexponential-time quantum algorithms due to Kuperberg [11,12,9] and Regev [15]. At a high level, these algorithms first transform coset states into phase-states of the form  $1/\sqrt{2}(|0\rangle + \omega_q^{\langle \mathbf{y}, \mathbf{s} \rangle} |1\rangle)$ , with a label  $\mathbf{y}$  which is uniform and known. They then repeatedly combine phase-states whose labels agree on selected blocks, thereby producing new states with increasingly divisible labels. The process eventually isolates enough information to recover the secret.

Recently, Bai, Jangir, Kirshanova, Ngo, and Youmans developed a quasi-polynomial-time quantum algorithm for EDCP over power-of-two moduli [2] inspired by the "Simon-meets-Kuperberg" algorithm of Bonnetain and Naya-Plasencia [4]. Their algorithm uses a quasi-polynomial number of quantum samples and polynomial quantum space. It also yields a quasi-polynomial-time algorithm for Gaussian- $S$  [LWE] over power-of-two moduli. The algorithm exploits the following sequence of ideals:

$$\mathbb{Z}_{2^t} \supset 2\mathbb{Z}_{2^t} \supset \cdots \supset 2^{t-1}\mathbb{Z}_{2^t},$$

combining binary phase states to increase the regularity of their labels one level at a time. Chailloux and Hermouet [6] recovered the same result using a reduction from  $S$  [LWE] to the Inhomogeneous Short Integer Solution problem (ISIS). Although using a different technique, they encountered the same bottleneck as in [2] when trying to generalize the result to other prime-power moduli.

Hidden-shift problems such as DCP can be viewed as hidden-subgroup problems. Thus, in parallel with [2], Imran and Ivanyos [10] generalized the "Simon-meets-Kuperberg" algorithm [4] to a particular class of groups, namely nilpotent groups. These are groups for which there exists a subgroup chain allowing us to use the same sieving techniques as in the case where we have the 2-adic chain mentioned in the paragraph just above.

However, Imran and Ivanyos' result cannot be directly applied to EDCP, since it does not have the structure of a hidden subgroup; nor can it be applied to a DCP with parameters  $(n, q)$  for  $q$  that is not a power of two, as stated in the following exercise in Rotman [18, Exercise 5.41]:

*The dihedral group of order  $2q$  is nilpotent if and only if  $q$  is a power of two.*

One might therefore ask whether there exists a specific nilpotent group that can be related to EDCP and DCP for any prime power  $q$ . This is what motivates the introduction of a new coset problem, which we have named the Cyclotomic Coset Problem.

We emphasize that our algorithms are not a direct application of Imran and Ivanyos [10]. The exact algorithm of Imran and Ivanyos assumes access to a unitary  $U$  implementing state preparation and to its inverse  $U^{-1}$ . In our model, the input consists only of independent quantum samples: neither the preparation circuit nor its inverse is available. Their exact theorem therefore does not apply directly. Moreover, the nilpotency class  $t(p-1)$  of our cyclotomic group  $G_{n,q,p} := R_q^n \rtimes \mathbb{F}_p$  need not be constant. We instead use their zero-sum algorithm and describe the quantum state transformations explicitly, accounting for sample consumption and working space.

### 1.1 Cyclotomic Coset

Let  $p$  be a prime, let  $q = p^t$ , and let  $\zeta_p$  be a primitive  $p$ -th root of unity. We consider the cyclotomic ring  $R_q := \mathbb{Z}_q[\zeta_p]$ . Multiplication by  $\zeta_p$  defines an action of the additive group  $\mathbb{F}_p$  on  $R_q$ . This allows us to define the semidirect product  $G_{n,q,p} := R_q^n \rtimes \mathbb{F}_p$  with multiplication

$$(\mathbf{x}, j)(\mathbf{y}, k) = (\mathbf{x} + \zeta_p^j \mathbf{y}, j + k).$$

Consequently, for every  $\mathbf{s} \in R_q^n$ , the set

$$H_{\mathbf{s}} := \{(\lambda_j \mathbf{s}, j) : j \in \mathbb{F}_p\}, \quad \text{with } \lambda_j = \sum_{i=0}^{j-1} \zeta_p^i,$$

is a subgroup of  $G_{n,q,p}$ . Equivalently, it is the cyclic subgroup generated by  $(\mathbf{s}, 1)$ . The subgroup order follows from the identity

$$\lambda_p = 1 + \zeta_p + \cdots + \zeta_p^{p-1} = 0$$

shows that  $H_{\mathbf{s}}$  has order  $p$ . A left coset of  $H_{\mathbf{s}}$  gives rise to the quantum state

$$|\phi_{\mathbf{x}, \mathbf{s}}\rangle = \frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} |j\rangle |\mathbf{x} + \lambda_j \mathbf{s}\rangle,$$

where  $\mathbf{x} \in R_q^n$  is uniformly random. We define the Cyclotomic Coset Problem (CCP) as the problem of recovering  $\mathbf{s}$  from independent states of this form.

When  $p = 2$ , we have

$$\zeta_2 = -1, \quad \lambda_0 = 0, \quad \lambda_1 = 1,$$

and  $R_q = \mathbb{Z}_q$ . Hence CCP specializes exactly to DCP.

We show that  $G_{n,q,p}$  is a nilpotent group, in Lemma 2 and the associated hidden subgroup problem is close to a generalized hidden-shift problem.

Note that our version of (CCP) assumes that the secret  $\mathbf{s}$  is contained in  $\mathbb{Z}_q^n$ , a restricted subset of  $R_q^n$ . This choice is justified by the introduction of a cyclotomic version of LWE (CyLWE), which also requires a restricted secret.

## 1.2 Organization and contributions

Our work makes several contributions towards the study of coset problems over cyclotomic rings and their quantum algorithms.

- We first introduce new computational problems over cyclotomic rings, namely CyLWE and CCP, which can be viewed as analogues of LWE and DCP, respectively. We establish equivalences between these problems when  $p$  is constant.
- We define a quantum Fourier transform over cyclotomic rings, which allows us to give a rigorous definition of phase-state samples over such rings, in analogy with Kuperberg’s phase states.
- We construct a sieving algorithm for CCP that exploits these new phase-state samples. Our algorithm can be viewed as a specific instance of the framework introduced by Imran and Ivanyos [10].
- We show that, for a certain range of parameters, our algorithm solves uniform EDCP and  $S$  [LWE] in quasi-polynomial time, given a quasi-polynomial number of samples. This generalizes the results of [2] from power-of-two moduli to a broader setting.

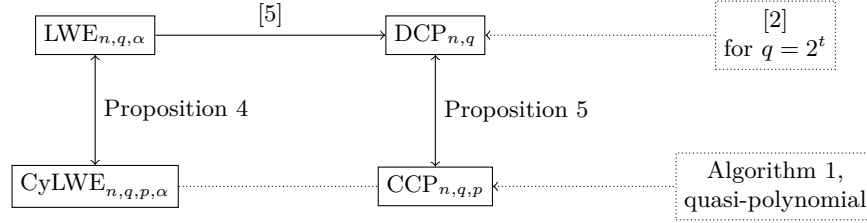


**Fig. 1.** Overview representing the different contributions of the paper. Note that we are considering an  $n$ -dimensional version of DCP. Moreover, [2] shows that there exists a reduction from  $\text{EDCP}_{n,q,M}$  to  $\text{DCP}_{n,q}$ .

## 2 Preliminaries

*Asymptotic notations.* We define the notations  $O(\cdot)$ ,  $\Omega(\cdot)$ ,  $\text{poly}(\cdot)$  in the standard way, with respect to the dimension  $n$  of the lattice and the security parameter  $\kappa$ . We say a function  $f : \mathbb{N} \rightarrow (0, 1]$  is negligible if for all positive polynomials  $p(\cdot)$  there exists an integer  $N$  such that,  $\forall n > N, f(n) < 1/p(n)$ . We say a positive function is quasipolynomial if it is upper bounded by  $2^{O(\log^c n)}$  for some constant  $c \geq 1$ .

### 2.1 Cyclotomic ring

We introduce the notation and definitions associated with the cyclotomic ring used throughout the paper. Let  $p$  be a prime number and let  $q = p^t$  with  $t \geq 1$ .

We denote by  $\zeta_p$  a primitive  $p$ -th root of unity, and define the cyclotomic field  $K = \mathbb{Q}[\zeta_p]$  as an extension of  $\mathbb{Q}$  generated by  $\zeta_p$ . Equivalently, the cyclotomic field can be viewed as the quotient  $\mathbb{Q}[X]/(\Phi_p(X))$  where  $\Phi_p(X) := 1 + X + \dots + X^{p-1}$  is the  $p$ -th cyclotomic polynomial. Hence we denote  $R := \mathbb{Z}[\zeta_p]$  the ring of integers of  $K$ . We write  $R_q = R/qR$ . We can view  $R_q$  as  $\mathbb{Z}_q[\zeta_p] = \mathbb{Z}_q[X]/(\Phi_p(X))$ , a cyclotomic extension of  $\mathbb{Z}_q$ . This allows us to represent elements of  $R_q$  by their coefficients with respect to the basis  $(1, \zeta_p, \dots, \zeta_p^{p-2})$ ,

$$\iota : \mathbb{Z}_q^{p-1} \rightarrow R_q, \quad (x_0, \dots, x_{p-2}) \mapsto \sum_{i=0}^{p-2} x_i \zeta_p^i$$

and we can state that  $\iota$  is an isomorphism of  $\mathbb{Z}_q$ -modules.

Using the same arguments as in the previous paragraph, one can show that  $R := \mathbb{Z}[\zeta_p]$  and  $\mathbb{Z}^{p-1}$  are isomorphic as  $\mathbb{Z}$ -modules. This directly induces a notion of distance on the cyclotomic ring. Indeed, for  $e \in \mathbb{Z}[\zeta_p]$ , we use the slight abuse of notation  $\|e\|_2$  to denote the  $\ell_2$ -norm of its representation in  $\mathbb{Z}^{p-1}$  with respect to the basis  $(1, \zeta_p, \dots, \zeta_p^{p-2})$ .

Finally, we denote by  $\langle \cdot, \cdot \rangle$  the symmetric bilinear form on  $R_q^n$  such that, for  $\mathbf{x} = (x_1, \dots, x_n)$  and  $\mathbf{y} = (y_1, \dots, y_n)$  in  $R_q^n$ , we have

$$\langle \mathbf{x}, \mathbf{y} \rangle := \sum_{i=1}^n x_i y_i.$$

*$\pi$ -decomposition.* The element  $\pi = \zeta_p - 1$  is a prime element of  $R$ , and there exists  $u_0 \in R^\times$  invertible such that

$$p = u_0 \pi^{p-1},$$

and therefore  $q = u_0^t \pi^L$  with  $L = t(p-1)$ , we say that  $p$  is ramified. Consequently, the two quotient rings are canonically isomorphic:

$$R_q = R/qR \cong R/\pi^L R.$$

For this reason, we will sometimes use the abusive notation  $R_L$  to talk about  $R_{\pi^L}$ . We have  $|R_k| = p^k$ : multiplication by  $\pi^{k-1}$  identifies  $R/\pi R$  with  $\pi^{k-1}R/\pi^k R$ , so each successive quotient has  $p$  elements. This will allow us to consider intermediate quotient rings that would be difficult to represent without the  $\pi$ -decomposition:

$$R_q = R_L \rightarrow R_{L-1} \rightarrow \dots \rightarrow R_1 = \mathbb{F}_p.$$

*Field trace.* The field trace corresponds to the linear map  $\text{Tr} : K \rightarrow \mathbb{Q}$ . More precisely, suppose  $K/\mathbb{Q}$  is a Galois extension and let  $x$  be an element of  $K$ . Then the trace of  $x$  is the sum of all Galois conjugates of  $x$ :

$$\text{Tr}(x) = \sum_{\sigma \in \text{Gal}(K/\mathbb{Q})} \sigma(x).$$

Let  $K = \mathbb{Q}(\zeta_p)$  be a cyclotomic extension of  $\mathbb{Q}$ . The trace is the linear map from  $K$  to  $\mathbb{Q}$  such that

$$\mathrm{Tr}(1) = p - 1, \quad \mathrm{Tr}(\zeta_p^k) = -1 \quad \text{for all } 1 \leq k \leq p - 1.$$

This follows from the fact that  $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_u \in \mathrm{Aut}(K) : \sigma_u(\zeta_p) = \zeta_p^u, u \in \mathbb{F}_p^\times\}$ . We immediately see that  $\mathrm{Tr}(1) = p - 1$ . For  $1 \leq k \leq p - 1$ , we obtain

$$\mathrm{Tr}(\zeta_p^k) = \sum_{u \in \mathbb{F}_p^\times} \sigma_u(\zeta_p^k) = \zeta_p + \cdots + \zeta_p^{p-1} = -1.$$

## 2.2 Lattices and cyclotomic lattices

*Discrete gaussian distribution.* For any  $r > 0$  and  $p > 2$ , we define the Gaussian function  $\rho_r(x) := \exp(-\pi\|x\|_2^2/r^2)$  for  $x \in \mathbb{R}^n$ . For  $x \in R_q^n$ , we also use the abusive notation  $\rho_r(x)$  to denote the quantity  $\rho_r(\iota(x))$  with  $\iota(x) \in \mathbb{R}^{n(p-1)}$ . For an  $n$ -dimensional lattice  $\Lambda$ , we write  $D_{\Lambda,r}$  for the discrete Gaussian distribution over  $\Lambda$  with density proportional to  $\rho_r(\cdot)$ . For the coefficient lattice  $\mathbb{Z}^{n(p-1)}$ , the Gaussian weight factors over coordinates, so the resulting distribution is a product of independent one-dimensional discrete Gaussians [1]. This factorization is not asserted for arbitrary lattices. We also extend the definition of Gaussian distribution to  $R^n$  by considering its injection in  $\mathbb{R}^{n(p-1)}$  related to the basis  $(1, \zeta_p, \dots, \zeta_p^{p-2})$ .

The tails of a Gaussian distribution are negligible compared to its central mass.

**Lemma 1 ([3], Lemma 1.5).** *For any  $n$ -dimensional lattice  $\Lambda$  and  $r > 0$ ,*

$$\rho_r(\Lambda \setminus B_n(0, \sqrt{n}r)) < 2^{-\Omega(n)} \rho_r(\Lambda).$$

Note that this result holds for cyclotomic sublattices of  $R^n$  using their coefficient embedding in  $\mathbb{R}^{n(p-1)}$ .

## 2.3 The cyclotomic group

Let  $p$  be a prime number and  $q = p^t$  a power of  $p$ . We call  $\zeta_p$  a primitive  $p$ -th root of unity and denote the cyclotomic ring by  $R_q := \mathbb{Z}_q[\zeta_p]$ , and we fix a dimension  $n \geq 1$ . We are interested here in the group

$$G_{n,q,p} = R_q^n \rtimes \mathbb{F}_p.$$

This is the group  $(R_q^n \rtimes \mathbb{F}_p, \star)$  where the product  $\star$  satisfies:

$$(\mathbf{x}_1, j_1) \star (\mathbf{x}_2, j_2) := (\mathbf{x}_1 + \zeta_p^{j_1} \mathbf{x}_2, j_1 + j_2), \text{ for } \mathbf{x}_1, \mathbf{x}_2 \in R_q^n \text{ and } j_1, j_2 \in \mathbb{Z}_p$$

One can verify that the internal composition law  $\star$  indeed defines a group structure on  $G_{n,q,p}$ .

*Nilpotent group.* Let  $G$  be a group. Let  $A$  and  $B$  be two subgroups of  $G$ ; we denote by  $[A, B]$  the subgroup generated by the commutator  $[a, b] := aba^{-1}b^{-1}$  with  $a$  in  $A$  and  $b$  in  $B$ . We call the lower central series the sequence of subgroups  $C^k(G)$  defined for every positive integer  $k$  by  $C^1(G) = G$  and  $C^{k+1}(G) = [G, C^k(G)]$ . We say that  $G$  is *nilpotent* if there exists an integer  $k$  such that  $C^k(G) = \{e\}$  (the trivial group). Moreover, the nilpotency class of  $G$  is the smallest integer  $k$  such that  $C^{k+1}(G) = \{e\}$ . The lemma below allows us to state that the cyclotomic group is a nilpotent group.

**Lemma 2.** *Let  $p$  be a prime,  $q = p^t$  with  $t \geq 1$ , and let  $n \geq 1$  be a dimension. The cyclotomic group  $G_{n,q,p}$  is a nilpotent group, of nilpotency class  $t(p-1)$ .*

*Proof.* Let  $G = R_q^n \rtimes \mathbb{F}_p$  and  $L = t(p-1)$ . We shall show by induction that, for every integer  $k \geq 2$ ,  $C^k(G) = \pi^{k-1}R_q^n \rtimes \{0\}$ . In the case  $k = 2$ , we have for  $(\mathbf{x}_1, j_1), (\mathbf{x}_2, j_2) \in G$ :

$$[(\mathbf{x}_1, j_1), (\mathbf{x}_2, j_2)] = ((1 - \zeta_p^{j_2})\mathbf{x}_1 + (\zeta_p^{j_1} - 1)\mathbf{x}_2, 0).$$

Since  $1 - \zeta_p^j = -\pi(1 + \zeta_p + \dots + \zeta_p^{j-1})$ , we obtain  $C^2(G) \subseteq \pi R_q^n \rtimes \{0\}$ . Conversely, for every  $\mathbf{x} \in R_q^n$ ,

$$[(0, 1), (\mathbf{x}, 0)] = (\pi\mathbf{x}, 0), \tag{1}$$

hence  $C^2(G) = \pi R_q^n \rtimes \{0\}$ . Now suppose that, for some  $k \geq 2$ ,  $C^k(G) = \pi^{k-1}R_q^n \rtimes \{0\}$ . Commuting an element of this subgroup with any element of  $G$  multiplies its vector by  $\zeta_p^j - 1$ , so  $C^{k+1}(G) \subseteq \pi^k R_q^n \rtimes \{0\}$ . Equation (1), applied to  $\mathbf{x} \in \pi^{k-1}R_q^n$ , proves the reverse inclusion.

Finally,  $(q) = (\pi^L)$  gives  $\pi^L R_q^n = 0$  and  $\pi^{L-1}R_q^n \neq 0$ . Therefore  $C^{L+1}(G) = \{e\}$  and, for  $L \geq 2$ ,  $C^L(G) \neq \{e\}$ . If  $L = 1$ ,  $G$  is nontrivial and abelian. In both cases its nilpotency class is exactly  $L = t(p-1)$ .  $\square$

## 2.4 Computational problems

*Learning with errors problems.* We introduce a variable  $\kappa$  to relate all the parameters involved in the definition below. Indeed,  $n, q, p$  are functions of  $\kappa$ , but we omit the variable  $\kappa$  for clarity.

**Definition 1 (Search LWE, [16]).** *Let  $p$  be a prime,  $q = p^t$ ,  $n$  be a positive integer, and  $\alpha > 0$ . Fix a secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . Given  $\ell$  samples of the form*

$$(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q),$$

*with  $\mathbf{a} \leftarrow \mathcal{U}(\mathbb{Z}_q^n)$  and  $e \leftarrow D_{\mathbb{Z}, \alpha q}$ , denoted by  $\text{LWE}_{n,q,\alpha}^\ell$ , the search LWE problem, asks to recover  $\mathbf{s} \in \mathbb{Z}_q^n$ .*

We now introduce a version of LWE on the cyclotomic ring called CyLWE. The rational-secret restriction and the coefficient error distribution distinguish this problem from the usual Ring-LWE (RLWE) setting discussed in [19]. For fixed  $p$ , the ring degree is the constant  $p-1$ , and  $n$  is an independent vector dimension. In common RLWE parameter families, the ring degree grows with the security parameter.

**Definition 2 (Cyclotomic LWE).** Let  $p$  be a prime,  $q = p^t$ ,  $n$  be a positive integer, and  $\alpha > 0$ . Fix a secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . Consider  $\ell$  samples of the form

$$(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + e \bmod q),$$

with  $\mathbf{a} \leftarrow \mathcal{U}(R_q^n)$  and  $e \leftarrow D_{R, \alpha q}$ . The cyclotomic LWE problem, denoted by  $\text{CyLWE}_{n,q,p,\alpha}^\ell$ , asks to recover  $\mathbf{s} \in \mathbb{Z}_q^n$ , given  $\ell$  samples.

*Hidden subgroup problem.*

**Definition 3 (Hidden Subgroup Problem).** Let  $G$  be a finite group and  $X$  a finite set. Fix  $H$  a hidden subgroup of  $G$ . Given a function  $f : G \rightarrow X$  that hides  $H$  (i.e.,  $f(g) = f(g')$  if and only if  $gH = g'H$ ), provided by means of an oracle using  $O(\log |G| + \log |X|)$  bits, the Hidden Subgroup Problem (HSP) asks to recover a generating set of  $H$ .

In practice, the oracle used in the HSP is assumed to be the existence of a quantum gate  $U_f$  such that  $|g\rangle |0\rangle \mapsto |g\rangle |f(g)\rangle$ . A quantum use of this gate is as follows. First, this consists of generating a quantum superposition of the elements of  $G$  and computing  $f$  in a second register by means of  $U_f$ .

$$\frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |0\rangle \rightarrow \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle |f(g)\rangle.$$

The second register is then measured. By the hiding promise, the preimage of an output  $x \in X$  of  $f$  can be viewed as a left coset of  $H$ , i.e., there exists  $g_0 \in G$  such that  $f^{-1}\{x\} = g_0H$ . The resulting state is therefore

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_0h\rangle.$$

Thus, a quantum instance that is solved in place of the classical instance of the HSP is stated as follows.

**Definition 4 (Coset Problem).** Let  $G$  be a group and  $H$  a hidden subgroup. Consider samples of the form

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |g_ih\rangle,$$

with the  $g_i$  drawn independently and uniformly from  $G$ . Given a certain number of samples from  $G$ , the Coset Problem asks to recover a subset generating  $H$ .

For hidden subgroups generated by  $(\mathbf{s}, 1)$ , this gives the dihedral coset problem over  $\mathbb{Z}_q^n \rtimes_{-1} \mathbb{Z}_2$ , and the cyclotomic coset problem over  $G_{n,q,p}$ , respectively.

*Coset problems.* We now introduce two quantum hidden-shift problems over finite rings, namely the Dihedral Coset Problem and its cyclotomic generalization. Initially, the dihedral coset problem was stated over  $\mathbb{Z}_q$ , but [9] discusses the DCP over  $\mathbb{Z}_q^n$ . We have therefore chosen to state it directly over  $\mathbb{Z}_q^n$  too.

**Definition 5 (Dihedral Coset Problem).** *Let  $p$  be a prime,  $q = p^t$  with  $t \geq 1$ , and  $n \geq 1$ . Fix a secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . Consider quantum samples  $\{|\phi_k\rangle\}_{k=0}^{\ell-1}$  of the form*

$$|\phi_k\rangle = \frac{1}{\sqrt{2}} (|0\rangle |\mathbf{x}_k\rangle + |1\rangle |\mathbf{x}_k + \mathbf{s}\rangle),$$

where the  $\mathbf{x}_k$  are independent uniform elements of  $\mathbb{Z}_q^n$ . The Dihedral Coset Problem over  $\mathbb{Z}_q^n$ , denoted by  $\text{DCP}_{n,q,p}^\ell$ , asks to recover  $\mathbf{s} \in \mathbb{Z}_q^n$ , given  $\ell$  samples.

**Definition 6 (Cyclotomic Coset Problem).** *Let  $p$  be a prime,  $q = p^t$  with  $t \geq 1$ , and  $n \geq 1$ . Fix a secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . We identify  $\mathbf{s} \in \mathbb{Z}_q^n$  with its coordinatewise constant embedding in  $R_q^n$ . Consider quantum samples  $\{|\phi_k\rangle\}_{k=0}^{\ell-1}$  of the form*

$$|\phi_k\rangle = \frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} |j\rangle |\mathbf{x}_k + \lambda_j \mathbf{s} \bmod q\rangle,$$

where  $\lambda_0 = 0$ ,  $\lambda_j = \sum_{i=0}^{j-1} \zeta_p^i$  for  $1 \leq j < p$ , and the  $\mathbf{x}_k$  are independent uniform elements of  $R_q^n$ . The Cyclotomic Coset Problem, denoted by  $\text{CCP}_{n,q,p}^\ell$ , asks to recover  $\mathbf{s} \in \mathbb{Z}_q^n$ , given  $\ell$  samples.

These problems are closely related to the EDCP introduced in [5]; for  $p = 2$ , CCP is DCP and hence uniform EDCP with two branches. Furthermore, it is clear that these two problems are specific variants of the Coset Problem. For DCP, the ambient group is the generalized dihedral group, while CCP uses  $G_{n,q,p}$ . Indeed,  $\lambda_{j+k} = \lambda_j + \zeta_p^j \lambda_k$  (indices modulo  $p$ ), so  $(\mathbf{s}, 1)^j = (\lambda_j \mathbf{s}, j)$  and  $H_{\mathbf{s}} = \langle (\mathbf{s}, 1) \rangle$  has order  $p$ . The left coset  $(\mathbf{x}, 0)H_{\mathbf{s}}$  gives exactly the stated CCP state after swapping registers.

## 2.5 Quantum Fourier Transform

We briefly recall the definition of the Quantum Fourier Transform and its efficient implementation as a quantum circuit.

**Definition 7 (Quantum Fourier Transform).** *Let  $N \geq 1$  be an integer and let  $\mathcal{H}_N$  be the  $N$ -dimensional Hilbert space spanned by the computational basis  $|0\rangle, \dots, |N-1\rangle$ . The Quantum Fourier Transform (QFT) over  $\mathbb{Z}_N$  is the unitary operator  $\text{QFT}_N$  defined on the computational basis states by*

$$\text{QFT}_N(|x\rangle) = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i xy/N} |y\rangle, \quad \forall x \in \{0, \dots, N-1\},$$

and extended to arbitrary states by linearity.

**Lemma 3 ([20], Implementation of the QFT).** *Let  $N \geq 2$  and  $0 < \varepsilon < 1$ . The quantum Fourier transform  $\text{QFT}_N$  admits a circuit approximation with operator-norm error at most  $\varepsilon$  using  $\text{poly}(\log N, \log(1/\varepsilon))$  elementary gates from a fixed universal gate set. When  $N$  is a power of a fixed prime, its ideal radix expansion uses  $O(\log^2 N)$  constant-dimensional Fourier and controlled-phase gates.*

### 3 Quantum Fourier Transform over cyclotomic rings

In this section, we define the quantum Fourier transform (QFT) on  $R_L = R/\pi^L R$  and provide an efficient construction of it. We then introduce phase-states, which are quantum states directly obtained from CCP samples using the QFT and which will be useful for designing a sieving algorithm.

#### 3.1 The duality in $R_L$

In this part, we provide an explicit description of the dual of  $R_L$  and its characters, using the field trace. The characters are indexed by the elements of  $R_L$  and satisfy several useful properties.

**Lemma 4.** *Fix  $K = \mathbb{Q}(\zeta_p)$  and let  $L$  be a positive integer. The map*

$$B_L : R_L \times R_L \rightarrow \mathbb{Q}/\mathbb{Z}, \quad B_L(x, y) := \text{Tr} \left( \frac{xy}{p\pi^{L-1}} \right) \bmod \mathbb{Z}$$

*is a non-degenerate symmetric  $\mathbb{Z}$ -bilinear form.*

*Proof.* Let  $(\zeta_p^i)_{0 \leq i \leq p-2}$  be the canonical basis of  $R$ . We can show that the family  $(e_j)_{0 \leq j \leq p-2}$  of  $R$  defined by

$$e_j := \frac{\zeta_p^{p-j} - \zeta_p}{\pi} = \zeta_p \sum_{k=0}^{p-j-2} \zeta_p^k, \quad 0 \leq j \leq p-2,$$

is also a basis of  $R$ :  $e_0 = -1$ , and  $e_j - e_{j+1} = \zeta_p^{p-j-1}$  for  $0 \leq j < p-2$ , so these elements generate the basis  $1, \zeta_p, \dots, \zeta_p^{p-2}$ . For  $0 \leq i, j \leq p-2$  we have  $\text{Tr} \left( \frac{\pi}{p} \zeta_p^i e_j \right) = \delta_{i,j}$ . In other words,  $((\pi/p)e_j)_{0 \leq j \leq p-2}$  is the trace-dual basis of  $(\zeta_p^i)_{0 \leq i \leq p-2}$ . This allows us to show, for  $x, y \in R$ , that

$$\text{Tr} \left( \frac{xy}{p\pi^{L-1}} \right) \in \mathbb{Z} \text{ for all } y \in R \iff x \in \pi^L R, \quad (2)$$

because the trace-dual lattice is  $R^\vee = (\pi/p)R$ , and the left-hand condition is equivalent to  $x/(p\pi^{L-1}) \in R^\vee$ .

The map  $B_L$  is well defined: changing either lift by an element of  $\pi^L R$  changes the trace by an element of  $\text{Tr}((\pi/p)R) \subseteq \mathbb{Z}$ . It is symmetric and  $\mathbb{Z}$ -bilinear, and non-degeneracy follows from (2).  $\square$

Thanks to this lemma, one can easily define the dual of  $R_L$ , by indexing the characters by the elements of  $R_L$ .

**Proposition 1 (Duality).** *The map below is an isomorphism:*

$$\Phi_L : R/\pi^L R \rightarrow \text{Hom}((R/\pi^L R, +), \mathbb{C}^\times), \quad y \mapsto \chi_y,$$

where  $\chi_y : x \mapsto \exp\left(2i\pi \text{Tr}\left(\frac{xy}{p\pi^{L-1}}\right)\right)$ . For  $y \in R/\pi^L R$ , we call character of  $(R_L, +)$ , the map  $\chi_y : R_L \rightarrow \mathbb{C}^\times$ .

*Proof.* Since the field trace is linear,  $\Phi_L$  is a group homomorphism. It remains to show that  $\Phi_L$  is a bijection. Because  $B_L$  from Lemma 4 is non-degenerate,  $\Phi_L$  is injective. Moreover,  $(R_L, +)$  is a finite group, so it has the same cardinality as its dual. In other words,

$$|R_L| = |\text{Hom}((R_L, +), \mathbb{C}^\times)|.$$

Hence,  $\Phi_L$  is an injection between groups of the same cardinality, so it is an isomorphism.  $\square$

Several useful properties of characters follow from this definition.

**Proposition 2 (Properties of the Characters).** *Let  $x, y, a, b$  be elements of  $R_L$ , let  $\lambda \in R$ , and let  $\sigma_u \in \text{Gal}(K/\mathbb{Q})$  with  $u \in \mathbb{F}_p^\times$ . The characters of  $(R_L, +)$  have the properties listed below.*

1. (Group homomorphism)

$$\chi_y(a + b) = \chi_y(a)\chi_y(b);$$

2. (Symmetry)

$$\chi_y(\lambda x) = \chi_1(\lambda xy) = \chi_x(\lambda y);$$

3. (Orthogonality of characters)

$$\frac{1}{p^L} \sum_{y \in R/\pi^L R} \chi_y(x) = \delta_{0,x};$$

4. (Stability under the Galois group)

We have

$$\chi_y(x) = \chi_{\sigma_u(y)}(\pi^{L-1}\sigma_u(x/\pi^{L-1})),$$

where  $\pi^{L-1}\sigma_u(x/\pi^{L-1}) \equiv u^{1-L}x \pmod{\pi R}$ ;

5. (Characters of  $R_{L-1}$ )

For  $L \geq 2$ , the character  $\chi_{\pi y} : R_L \rightarrow \mathbb{C}^\times$  induces a character on  $R_{L-1}$ .

*Proof.* We prove the above properties one by one.

– Properties 1 and 2 follow directly from the definition of  $\Phi_L$  in Proposition 1.

- The orthogonality of characters holds trivially when  $x = 0$ . Suppose  $x$  is not zero. Then there exists  $z \in R_L$  such that  $\chi_z(x) \neq 1$ . Reindexing the character sum gives

$$\begin{aligned} \frac{1}{p^L} \sum_{y \in R_L} \chi_y(x) &= \frac{1}{p^L} \sum_{y \in R_L} \chi_{y+z}(x) \\ &= \chi_z(x) \left( \frac{1}{p^L} \sum_{y \in R_L} \chi_y(x) \right), \end{aligned}$$

which shows that the sum is zero.

- The stability under Galois automorphisms follows from the corresponding stability of the field trace. Let  $x, y \in R_L$ . Since  $\text{Tr} \circ \sigma = \text{Tr}$  for every  $\sigma \in \text{Gal}(K/\mathbb{Q})$ , the exponent of the character satisfies

$$\begin{aligned} \text{Tr} \left( \frac{xy}{p\pi^{L-1}} \right) &= \text{Tr} \left( \sigma_u \left( \frac{xy}{p\pi^{L-1}} \right) \right) \\ &= \text{Tr} \left( \frac{1}{p\pi^{L-1}} \left[ \pi^{L-1} \sigma_u \left( \frac{x}{\pi^{L-1}} \right) \right] \sigma_u(y) \right). \end{aligned}$$

Moreover, we note that  $\sigma_u(\pi)/\pi \equiv u \pmod{\pi R}$ , hence  $(\pi/\sigma_u(\pi))^{L-1} \equiv u^{1-L} \pmod{\pi R}$  and  $\sigma_u(x) \equiv x \pmod{\pi R}$ , which concludes the proof of this property.

- Finally, the definition of  $\Phi_L$  in Proposition 1 gives

$$\chi_{\pi y}(x) = \exp \left( 2i\pi \text{Tr} \left( \frac{x\pi y}{p\pi^{L-1}} \right) \right) = \exp \left( 2i\pi \text{Tr} \left( \frac{xy}{p\pi^{L-2}} \right) \right),$$

which corresponds to the image of a character of  $R_{L-1}$ .  $\square$

In particular, the concept of characters allows us to define the Fourier transform on  $R_L$  and thus to correctly define its quantum Fourier transform.

### 3.2 Construction of the Quantum Fourier Transform

For odd  $p$ , the Fourier transform over Galois rings in [21] does not directly cover the present ramified ring. Indeed,

$$\Phi_p(X) = (X - 1)^{p-1} \pmod{p}.$$

We therefore use the trace-dual pairing above. Its Fourier transform can be implemented using ordinary abelian Fourier transforms and a change of coordinates.

**Definition 8 (Quantum Fourier Transform over  $R_L$ ).** *Let  $p$  be a prime and  $L \geq 1$ . We define the quantum Fourier transform (QFT) over  $R_L$  as the linear operator specified by*

$$\text{QFT}_{R_L}(|x\rangle) := \frac{1}{\sqrt{p^L}} \sum_{y \in R_L} \chi_y(x) |y\rangle.$$

for each  $x \in R_L$ , and extend to all quantum states by linearity. Orthogonality of characters proves that this map is unitary.

We extend this quantum Fourier transform to  $R_L^n$  by performing the unitary  $\text{QFT}_{R_L}$  coordinatewise. In other words, we can consider characters on  $R_L^n$  such that for  $\mathbf{x}, \mathbf{y} \in R_L^n$  we have,

$$\chi_{\mathbf{y}}(\mathbf{x}) = \prod_{i=1}^n \chi_{y_i}(x_i) = \exp \left( 2i\pi \text{Tr} \left( \frac{\langle \mathbf{x}, \mathbf{y} \rangle}{p\pi^{L-1}} \right) \right).$$

Note that when  $L = 1$ , we have  $R_1 \cong \mathbb{F}_p$ , and  $B_1(x, y) = -xy/p \bmod \mathbb{Z}$ . Thus this QFT is the inverse of the positive-sign quantum Fourier transform over  $\mathbb{F}_p$  introduced in Section 2.5.

**Proposition 3.** *For fixed  $p$  and  $L = t(p-1)$ , the quantum Fourier transform over  $R_L$  admits an implementation to error  $\varepsilon$  in time  $\text{poly}_p(t, \log(1/\varepsilon))$ .*

*Proof.* We first recall that  $R_L = R_q$  when  $L = (p-1)t$ , and that  $R_q \cong \mathbb{Z}_q^{p-1}$ . Hence, if we let  $\iota : \mathbb{Z}_q^{p-1} \rightarrow R_q$  denote such an isomorphism, the map

$$\overline{B}_L : \mathbb{Z}_q^{p-1} \times \mathbb{Z}_q^{p-1} \rightarrow \mathbb{Q}/\mathbb{Z}, \quad \overline{B}_L(\mathbf{x}, \mathbf{y}) := B_L(\iota(\mathbf{x}), \iota(\mathbf{y})),$$

is a non-degenerate symmetric bilinear form. Consequently, there exists a matrix  $\mathbf{D} \in \mathbb{Z}_q^{(p-1) \times (p-1)}$  such that

$$\overline{B}_L(\mathbf{x}, \mathbf{y}) = \frac{1}{q}(\mathbf{x}^T \mathbf{D} \mathbf{y}), \quad \text{for all } \mathbf{x}, \mathbf{y} \in \mathbb{Z}_q^{p-1}.$$

In the power basis we take  $D_{ij} = qB_L(\zeta_p^i, \zeta_p^j) \bmod q$ ; these entries are integers modulo  $q$  since  $qR_L = 0$ . They are computable by rational arithmetic in  $K$  in polynomial time in  $t$  for fixed  $p$ . Non-degeneracy makes  $\mathbf{D}$  invertible, and symmetry gives  $\mathbf{D}^T = \mathbf{D}$ . Therefore, the unitary  $\mathcal{U}_{\mathbf{D}} : |\mathbf{x}\rangle \mapsto |\mathbf{D}\mathbf{x}\rangle$  admits an efficient implementation, as does the quantum Fourier transform over  $\mathbb{Z}_q^{p-1}$ . The resulting composition acts as follows:

$$\begin{aligned} \text{QFT}_{\mathbb{Z}_q^{p-1}} \circ \mathcal{U}_{\mathbf{D}}(|\mathbf{x}\rangle) &= \text{QFT}_{\mathbb{Z}_q^{p-1}}(|\mathbf{D}\mathbf{x}\rangle) \\ &= \frac{1}{\sqrt{q^{p-1}}} \sum_{\mathbf{y} \in \mathbb{Z}_q^{p-1}} \exp\left(\frac{2i\pi}{q} \mathbf{x}^T \mathbf{D} \mathbf{y}\right) |\mathbf{y}\rangle \\ &= \text{QFT}_{R_L}(|\mathbf{x}\rangle), \end{aligned}$$

which concludes the proof.  $\square$

### 3.3 Phase-state Problem

In the spirit of Kuperberg's algorithm, the quantum Fourier transform on the ring  $R_L$  allows us to transform a CCP sample into a quantum state in which the information about the secret is encoded in the phase of the state. We therefore define a new problem, the phase-state problem (PSP), which consists in recovering the secret  $\mathbf{s}$  from such phase-state samples.

**Definition 9 (Phase-States Problem).** Let  $n$  and  $L$  be positive integers, and let  $p$  be a prime. Fix a secret  $\mathbf{s} \in R_L^n$ . Suppose we are given  $\ell$  phase-state samples of the form  $(\mathbf{y}_i, |\psi_{\mathbf{y}_i}\rangle)$ , where

$$\mathbf{y}_i \leftarrow \mathcal{U}(R_L^n), \quad |\psi_{\mathbf{y}_i}\rangle = \frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} \chi_{\mathbf{y}_i}(\lambda_j \mathbf{s}) |j\rangle.$$

The labels  $\mathbf{y}_i$  are independent. The phase-state problem, denoted  $\text{PSP}_{n,L,p}^\ell$ , asks to recover the secret  $\mathbf{s}$ .

**Lemma 5.** Let  $n$  be a positive integer, let  $p$  be a prime, and let  $q = p^t$  be a power of  $p$ . Fix  $L := t(p-1)$ . Then  $\text{CCP}_{n,q,p}$  reduces to  $\text{PSP}_{n,L,p}$ .

*Proof.* It is enough to show that one can build a phase-state sample from a CCP sample involving the same secret  $\mathbf{s}$ . A phase-state sample  $(\mathbf{y}_i, |\psi_{\mathbf{y}_i}\rangle)$  with  $\mathbf{y}_i \leftarrow \mathcal{U}(R_L^n)$  is obtained from a CCP state  $|\phi_{\mathbf{x}}\rangle$  by applying a quantum Fourier transform over  $R_q^n \cong R_L^n$  to the second register. Indeed,

$$\begin{aligned} (\text{id}_{\mathbb{F}_p} \otimes \text{QFT}_{R_q}^{\otimes n})(|\phi_{\mathbf{x}}\rangle) &= p^{-(Ln+1)/2} \sum_{j \in \mathbb{F}_p} |j\rangle \sum_{\mathbf{y} \in R_L^n} \chi_{\mathbf{y}}(\mathbf{x} + \lambda_j \mathbf{s}) |\mathbf{y}\rangle \\ &= p^{-(Ln+1)/2} \sum_{\mathbf{y} \in R_L^n} \chi_{\mathbf{y}}(\mathbf{x}) \left( \sum_{j \in \mathbb{F}_p} \chi_{\mathbf{y}}(\lambda_j \mathbf{s}) |j\rangle \right) |\mathbf{y}\rangle \\ &= p^{-Ln/2} \sum_{\mathbf{y} \in R_L^n} \chi_{\mathbf{y}}(\mathbf{x}) |\psi_{\mathbf{y}}\rangle |\mathbf{y}\rangle. \end{aligned}$$

Measuring the second register yields each  $\mathbf{y}$  with probability  $p^{-Ln}$ , independently of  $\mathbf{x}$ . Its remaining factor  $\chi_{\mathbf{y}}(\mathbf{x})$  is a global phase. Independent input samples therefore give independent uniform labels.  $\square$

## 4 A practical algorithm for solving the CCP

In 2023, Imran and Ivanyos [10] showed that there exists a quantum algorithm solving the hidden subgroup problem for nilpotent groups. They further point out that solving the hidden-shift problem via the "Simon-meets-Kuperberg" algorithm [4] is a special case of their algorithm applied to the dihedral group.

**Theorem 1 ([10], Theorem 1.).** Let  $G$  be a nilpotent group of bounded nilpotency class such that the prime factors of  $|G|$  are constant. Assuming there exists a black box allowing a unique encoding of the elements via  $\ell$ -bit strings, there exists an exact quantum algorithm that solves the hidden-shift problem for  $G$  using  $\text{poly}(\ell)$  operations and  $\text{poly}(\log |G|)$  calls to the hidden subgroup problem oracle.

Since, by Lemma 2, the cyclotomic group  $G_{n,q,p}$  is nilpotent, its nilpotency class is bounded by  $\log(q)(p-1)$ , and its cardinality is a power of  $p$ , Theorem 1

highlights an algorithm for solving the HSP for the cyclotomic group, i.e., a potential algorithm for solving CCP.

Nevertheless, some points need to be qualified. For applications in public key cryptography, we are interested in asymptotic results with respect to the dimension  $n$  and the modulus  $q$  of the problem. In this setting, the nilpotency class of the cyclotomic group is no longer constant. Moreover, the complexity studied is not a complexity tied to the number of oracle calls, but rather a time and space complexity. Indeed, the exact algorithm of Imran and Iyanyos assumes access to a unitary  $U$  implementing state preparation and to its inverse  $U^{-1}$ . In our model, the input consists only of independent quantum samples: neither the preparation circuit nor its inverse is available. For these reasons, we have decided to present the algorithm of Imran and Iyanyos [10] within the framework of CCP.

It is worth mentioning that this connection was not immediately apparent to us. During our work on CCP, we independently arrived at an approach closely related to the algorithm of Imran and Iyanyos, before becoming aware of their work. The algorithm we had been developing can be viewed as an instance of their more general framework. We therefore present it here not as a new algorithm, but as a reformulation and specialization of their result to the cyclotomic setting, with particular emphasis on its concrete time and space complexity.

In this section, we present an algorithm for solving CCP in quasi-polynomial time using a quasi-polynomial number of samples. Combined with Proposition 5, this yields a quasi-polynomial-time algorithm for DCP with arbitrary prime-power moduli. Our result generalizes the result of [2].

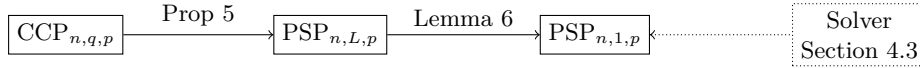


**Fig. 2.** Overview of the CCP solver. The core idea is to reduce CCP to a phase-state problem and then perform sieving steps iteratively in order to obtain phase states from which information about the secret can be extracted.

#### 4.1 Solver for the easy instance of $\text{PSP}_{n,1,p}$

Suppose we have a phase-state sample  $(\mathbf{y}, |\psi_{\mathbf{y}}\rangle)$  for an instance of  $\text{PSP}_{n,1,p}$  such that  $\mathbf{y} \neq 0$ . Since  $R_1 = \mathbb{F}_p$ , we have  $j \in R_1$ , and the quantum state has the form

$$\begin{aligned}
 \frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} \chi_{\mathbf{y}}(\lambda_j \mathbf{s}) |j\rangle &= \frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} \chi_{\mathbf{s}}(\lambda_j \mathbf{y}) |j\rangle \\
 &= \frac{1}{\sqrt{p}} \sum_{j \in R_1} \chi_j(\langle \mathbf{y}, \mathbf{s} \rangle) |j\rangle \\
 &= \text{QFT}_{R_1}(|\langle \mathbf{y}, \mathbf{s} \rangle \bmod p\rangle).
 \end{aligned}$$

By measuring the phase state in its Fourier basis, we can recover  $\langle \mathbf{y}, \mathbf{s} \rangle$ . Hence, if we have access to  $n$  phase-state samples  $(\mathbf{y}_i, |\psi_{\mathbf{y}_i}\rangle)$ , with constant probability the  $\mathbf{y}_i$  are linearly independent, we can then recover  $\mathbf{s} \bmod p$ .

Hence, the goal is to reduce to this simple case using Lemma 6.

## 4.2 Sieving step

**Lemma 6 (from  $\text{PSP}_{n,L,p}$  to  $\text{PSP}_{n,L-1,p}$ ).** *Let  $n$  and  $L$  be positive integers, with  $L \geq 2$ . There exists a quantum algorithm which, given  $r$  samples from  $\text{PSP}_{n,L,p}$  denoted by  $(\mathbf{y}_i, |\psi_{\mathbf{y}_i}\rangle)_{i=1}^r$  with  $\mathbf{y}_i$  in  $R_L^n$  satisfying  $\sum_{i=1}^r \mathbf{y}_i = 0 \bmod \pi R$ , is able to produce a sample from  $\text{PSP}_{n,L-1,p}$ .*

*Proof.* Suppose that we have access to  $r$  samples from  $\text{PSP}_{n,L,p}$ , which we denote by  $(\mathbf{y}_i, |\psi_{\mathbf{y}_i}\rangle)_{i=1}^r$ . The following operations reduce the level by one.

1. We begin with the tensor product of the input states:

$$\bigotimes_{i=1}^r |\psi_{\mathbf{y}_i}\rangle = \frac{1}{\sqrt{p^r}} \sum_{(j_1, \dots, j_r) \in \mathbb{F}_p^r} \chi_{\mathbf{s}} \left( \sum_{i=1}^r \mathbf{y}_i \lambda_{j_i} \right) |j_1\rangle \dots |j_r\rangle.$$

2. For every  $i \geq 2$ , we perform the label change  $j_i \mapsto j_i - j_1$  in order to introduce a dependence on  $j_1$  in each register. This gives explicitly the following state:

$$\frac{1}{\sqrt{p^r}} \sum_{(j_1, \dots, j_r) \in \mathbb{F}_p^r} \chi_{\mathbf{s}} \left( \sum_{i=1}^r \mathbf{y}_i \lambda_{j_i} \right) |j_1\rangle |j_2 - j_1\rangle \dots |j_r - j_1\rangle$$

3. We then measure the last  $r-1$  registers. Suppose that the output of the  $i$ -th register is  $x_i \in \mathbb{F}_p$ . Fix  $x_1 = 0$  and denote the free variable  $j_1$  by  $j$ . In this case, the remaining state is:

$$\frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} \chi_{\mathbf{s}} \left( \sum_{i=1}^r \mathbf{y}_i \lambda_{x_i + j} \right) |j\rangle.$$

Using the property  $\lambda_{x_i + j} = \lambda_{x_i} + \zeta_p^{x_i} \lambda_j$ , it follows that the remaining state is proportional to the state

$$\frac{1}{\sqrt{p}} \sum_{j \in \mathbb{F}_p} \chi_{\mathbf{s}} \left( \sum_{i=1}^r \mathbf{y}_i \zeta_p^{x_i} \lambda_j \right) |j\rangle.$$

We claim that the resulting state indeed corresponds to a  $\text{PSP}_{n,L-1,p}$ .

To this end, it suffices to observe that:

$$\sum_{i=1}^r \mathbf{y}_i \zeta_p^{x_i} = \sum_{i=1}^r \mathbf{y}_i \bmod \pi R^n = 0 \bmod \pi R^n.$$

Therefore, there exists  $\mathbf{y}' \in R_{L-1}^n$  such that  $\sum_{i=1}^r \mathbf{y}_i \zeta_p^{x_i} = \pi \mathbf{y}'$ . The resulting state is thus of the form  $(\mathbf{y}', |\psi_{\mathbf{y}'}\rangle)$ , a sample from  $\text{PSP}_{n,L-1,p}$ .  $\square$

In order to properly use the above lemma, it is necessary to efficiently find such a sequence  $\mathbf{y}_i$  of vectors whose sum is zero modulo  $\pi R^n$ . The following theorem provides the required zero-sum search algorithm:

**Theorem 2 ([10], Theorem 2).** *There exists a deterministic algorithm which, given a sequence of size  $S(n, p) = p^{O(p \log^2 p)} n^{O(p \log p)}$  of vectors in  $\mathbb{F}_p^n$ , is able to find a subsequence whose sum is zero in time  $\text{poly}(S(n, p))$ .*

Observing that  $R_1^n = \mathbb{F}_p^n$ , it suffices to apply the theorem to a sequence of size  $S(n, p)$  of  $\bar{\mathbf{y}}_i$  corresponding to the reduction modulo  $\pi$  of the labels of the  $\text{PSP}_{n,L,p}$  samples of the form  $(\mathbf{y}_i, |\psi_{\mathbf{y}_i}\rangle)$ .

**Lemma 7 (Uniform output labels).** *Let  $S = S(n, p) \geq 2$  be an integer threshold for Theorem 2. Given  $S$  independent uniform labels in  $R_L^n$ , select the nonempty zero-sum subsequence using only their residues modulo  $\pi$ , and apply Lemma 6. The output label is uniform in  $R_{L-1}^n$ .*

*Proof.* Condition on the residues of all labels, choose fixed lifts  $\mathbf{r}_i$ , and write  $\mathbf{y}_i = \mathbf{r}_i + \pi \mathbf{z}_i$ . The vectors  $\mathbf{z}_i$  are independent and uniform in  $R_{L-1}^n$ . The selected index set  $I$  is now fixed. The measured differences  $x_i$  are independent of the full labels by the preceding proof, so conditioning on them does not change the distribution of the  $\mathbf{z}_i$ . The output label is

$$\mathbf{y}' = \mathbf{c} + \sum_{i \in I} \zeta_p^{x_i} \mathbf{z}_i, \quad \mathbf{c} = \frac{\sum_{i \in I} \zeta_p^{x_i} \mathbf{r}_i}{\pi} \in R_{L-1}^n.$$

The division is well defined because the numerator is divisible by  $\pi$ . Since  $I$  is nonempty and every  $\zeta_p^{x_i}$  is a unit, conditioning also on all but one of the  $\mathbf{z}_i$  leaves  $\mathbf{y}'$  uniform.  $\square$

### 4.3 Description of the sieving algorithm

The sieving algorithm introduces lists  $\mathcal{L}_0, \dots, \mathcal{L}_{L-1}$  such that, for every  $i$ ,  $\mathcal{L}_i$  contains samples associated with  $\text{PSP}_{n,L-i,p}$ . The main idea is to move from one level to the next by grouping in buckets of size  $S(n, p)$ , then applying the algorithm from Theorem 2 to find a zero-sum sequence, and doing the procedure described in Lemma 6. Once the final stage is reached, we obtain a list  $\mathcal{L}_{L-1}$  consisting of samples from  $\text{PSP}_{n,1,p}$ , from which we can easily recover  $\mathbf{s}_0 = \mathbf{s} \pmod{p}$ . Once the secret modulo  $p$  has been recovered, we can reduce  $\text{CCP}_{n,q,p}$  to an instance of  $\text{CCP}_{n,q/p,p}$  with secret  $(\mathbf{s} - \mathbf{s}_0)/p$  and repeat the same procedure until  $\mathbf{s}$  is fully recovered.

The algorithm is presented as follows.

The analysis of Algorithm 1 shows that it runs in quasi-polynomial time when  $q = \text{poly}(n)$ . This can be summarized by the following theorem.

**Theorem 3 (Quasi-Polynomial Algorithm for CCP).** *Let  $n$  and  $\ell$  be non-negative integers, let  $p$  be a prime, and let  $q$  be a power of  $p$ . When  $\ell = 2^{\Omega(\log n \log q)}$ , Algorithm 1 solves  $\text{CCP}_{n,q,p}^\ell$  with constant success probability in time  $2^{O(\log n \log q)}$  using  $\text{poly}(n)$  quantum space.*

---

**Algorithm 1** CCP solver

---

**Input:**  $\ell$  CCP samples of a secret  $\mathbf{s} \in \mathbb{Z}_q^n$

**Output:** The secret  $\mathbf{s} \in \mathbb{Z}_q^n$  of the CCP instance

- 1: Build  $\ell$  phase-state samples from the  $\ell$  CCP samples, involving the same secret  $\mathbf{s} \in \mathbb{Z}_q^n$ .
  - 2: Regroup the phase-state samples into families of  $S(n, p)$  elements and apply the algorithm from Theorem 2 to each to get zero-sum sequences.
  - 3: Apply Lemma 6 to obtain, on average,  $\ell' \geq \ell \cdot \frac{1}{S(n, p)}$  phase-state samples associated with  $\text{PSP}_{n, L-1, p}$  with secret  $\mathbf{s} \bmod \pi^{L-1} R$ .
  - 4: Repeat Step 2 until obtaining, on average,  $\ell \cdot (\frac{1}{S(n, p)})^{L-1}$  samples of  $\text{PSP}_{n, 1, p}$ .
  - 5: Deduce  $\mathbf{s} \bmod p$  from this easy instance of  $\text{PSP}_{n, 1, p}$ .
  - 6: Repeat the previous steps for an instance of  $\text{CCP}_{1, q/p, p}$  with secret  $\mathbf{s}_0 = \mathbf{s} \bmod (q/p)$ , until the entire secret  $\mathbf{s} \in \mathbb{Z}_q^n$  is recovered.
- 

*Proof.* The first round (Steps 1–2–3–4) of the algorithm dominates the subsequent ones, and a total of  $\log(q)$  rounds are performed. The overall complexity is therefore determined by the complexity of the first round.

The goal is to find a lower bound on the size of the first list  $\mathcal{L}_0$  that ensures we have enough elements at level  $\mathcal{L}_{L-1}$  to allow us to recover  $\mathbf{s} \bmod p$ . To do this, we note that at each reduction step, we obtain

$$|\mathcal{L}_{i+1}| \leq S(n, p)^{-1} |\mathcal{L}_i|$$

By applying this inequality  $L - 1$  times, we obtain

$$|\mathcal{L}_{L-1}| \leq S(n, p)^{-L+1} |\mathcal{L}_0|.$$

On the other hand, we must ensure that there are sufficiently many elements at the final level to recover  $\mathbf{s} \bmod p$ . By Section 7.1, we know that  $O(n)$  phase-states from  $\text{PSP}_{n, 1, p}$  are sufficient to recover  $\mathbf{s} \bmod p$ .

$$|\mathcal{L}_{L-1}| \geq \text{poly}(n)$$

Combining these conditions on  $|\mathcal{L}_{L-1}|$ , we obtain

$$\text{poly}(n) \geq S(n, p)^{-L+1} |\mathcal{L}_0| \Rightarrow |\mathcal{L}_0| \geq (S(n, p))^L \text{poly}(n).$$

Thus, this justifies that the number of samples required is  $\ell = 2^{\Omega(\log n \log q)}$ , and it follows directly that the algorithm runs in  $2^{O(\log n \log q)}$  time. The quantum space follows Regev's construction [14].  $\square$

## 5 Equivalences between classical and cyclotomic problems

### 5.1 Between LWE and CyLWE

The following proposition establishes a correspondence between search  $\text{LWE}_{n, q, \alpha}$  and cyclotomic  $\text{CyLWE}_{n, q, p, \alpha}$ . Indeed, by showing that one can efficiently construct a sample of one problem from samples of the other, and vice versa, we can directly justify the equivalence between the two problems.

**Proposition 4.** *Let  $p$  be a prime number,  $q$  be a power of  $p$ ,  $\alpha > 0$  be a scalar, and  $n$  be an integer. There exists an algorithm that, given  $p - 1$  samples of  $\text{LWE}_{n,q,\alpha}$ , produces a sample of  $\text{CyLWE}_{n,q,p,\alpha}$  involving the same secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . Conversely, given a sample of  $\text{CyLWE}_{n,q,p,\alpha}$ , there exists an algorithm that outputs  $p - 1$  samples of  $\text{LWE}_{n,q,\alpha}$ .*

*Proof.* We first establish the forward direction. Suppose we are given an instance of classical  $\text{LWE}_{n,q,\alpha}$  with secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . Take  $(p - 1)$  LWE samples  $\{(\mathbf{a}_i, b_i)\}_{i=0}^{p-2}$  and form the following coefficient expansions:

$$\mathbf{a}' := \sum_{i=0}^{p-2} a_i \zeta_p^i, \quad b' := \sum_{i=0}^{p-2} b_i \zeta_p^i \pmod{q} = \langle \mathbf{a}', \mathbf{s} \rangle + e' \pmod{q}$$

The pair  $(\mathbf{a}', b')$  is an instance of  $\text{CyLWE}$  with secret  $\mathbf{s}_0 \in \mathbb{Z}_q^n$  and error  $e' = \sum_{i=0}^{p-2} e_i \zeta_p^i$ , where  $e_i$  denotes the error term in the sample  $(\mathbf{a}_i, b_i)$ . This error follows a distribution over  $R^n$  proportional to

$$\prod_{i=0}^{p-2} \rho_{\alpha q}(e_i) = \rho_{\alpha q}((e_0, \dots, e_{p-2})) = \rho_{\alpha q}(e'),$$

since the Gaussian weight factorize over coordinates,  $D_{\mathbb{Z}[\zeta_p], \alpha}$  coincides with the product of  $p - 1$  independent one-dimensional discrete Gaussian.

Conversely, suppose we have a sample of  $\text{CyLWE}_{n,q,p,\alpha}$  noted  $(\mathbf{a}, b)$ . We can decompose  $\mathbf{a}$  and  $b$  into the basis  $(1, \zeta_p, \dots, \zeta_p^{p-2})$  such that

$$\mathbf{a} = \sum_{i=0}^{p-2} \mathbf{a}_i \zeta_p^i, \quad b = \sum_{i=0}^{p-2} b_i \zeta_p^i \pmod{q} = \sum_{i=0}^{p-2} (\langle \mathbf{a}_i, \mathbf{s} \rangle + e_i) \zeta_p^i \pmod{q},$$

where  $b_i = \langle \mathbf{a}_i, \mathbf{s} \rangle + e_i \pmod{q}$  with  $e_i \leftarrow D_{\mathbb{Z}, \alpha q}$ . This yields  $(p - 1)$  samples of LWE with secret  $\mathbf{s}$ .  $\square$

The introduction of  $\text{CyLWE}$  in the paper and its connection to LWE is extremely important to us, because it is what allowed us to fully understand how to link a classical problem to a problem on cyclotomic rings. Among other things, this is what enabled us to establish that the CCP secret must indeed be contained within the restricted space  $\mathbb{Z}_q^n$  and not within  $R_q^n$ . All other reductions, like *Proposition 5* and *Lemma 10*, are inspired by the philosophy of the proof described above, which considers the group isomorphism  $\mathbb{Z}_q^{p-1}$  to  $R_q$ .

## 5.2 Between DCP and CCP

The proof of the equivalence between DCP and CCP follows the same approach as the one used for the equivalence between LWE and  $\text{CyLWE}$ . Namely, we show that samples associated with one problem can be efficiently constructed from samples of the other problem, while preserving the same secret.

**Proposition 5.** *Given  $(p-1)$  samples of  $\text{DCP}_{n,q,p}$ , there exists a quantum algorithm that produces a  $\text{CCP}_{n,q,p}$  sample with probability  $p/2^{p-1}$ . Conversely, given a sample of  $\text{CCP}_{n,q,p}$ , there exists a quantum algorithm that outputs a  $\text{DCP}_{n,q}$  sample with probability  $2/p$ . Both direction involving the same secret.*

*Proof.* Let  $f : \mathbb{Z}_q^{n \times (p-1)} \rightarrow R_q^n$  denote the bijection defined, for a matrix  $\mathbf{X} = (\mathbf{x}_0 \mid \cdots \mid \mathbf{x}_{p-2}) \in \mathbb{Z}_q^{n \times (p-1)}$ , by

$$f(\mathbf{X}) := \sum_{i=0}^{p-2} \mathbf{x}_i \zeta_p^i.$$

We begin the first reduction by collecting  $(p-1)$  samples of  $\text{DCP}_{n,q,p}$  of the form

$$|\phi_i\rangle \propto \sum_{j \in \{0,1\}} |j\rangle |\mathbf{x}_i + j\mathbf{s} \bmod q\rangle.$$

Taking their tensor product and rearranging the registers gives the following expression for their joint state:

$$\begin{aligned} \bigotimes_{i=0}^{p-2} |\phi_i\rangle &= \sum_{(j_0, \dots, j_{p-2}) \in \mathbb{F}_2^{p-1}} |j_0\rangle |\mathbf{x}_0 + j_0\mathbf{s}\rangle \cdots |j_{p-2}\rangle |\mathbf{x}_{p-2} + j_{p-2}\mathbf{s}\rangle \\ &= \sum_{\mathbf{J} \in \mathbb{F}_2^{p-1}} |\mathbf{J}\rangle |\mathbf{X} + \mathbf{M}_{\mathbf{J}, \mathbf{s}}\rangle, \end{aligned}$$

with  $\mathbf{X} = (\mathbf{x}_0 \mid \cdots \mid \mathbf{x}_{p-2}) \in \mathbb{Z}_q^{n \times (p-1)}$  and  $\mathbf{M}_{\mathbf{J}, \mathbf{s}} = (j_0\mathbf{s} \mid \cdots \mid j_{p-2}\mathbf{s}) \in \mathbb{Z}_q^{n \times (p-1)}$ . We then apply  $f$  to the second register, obtaining

$$\sum_{\mathbf{J} \in \mathbb{F}_2^{p-1}} |\mathbf{J}\rangle |f(\mathbf{X} + \mathbf{M}_{\mathbf{J}, \mathbf{s}})\rangle = \sum_{\mathbf{J} \in \mathbb{F}_2^{p-1}} |\mathbf{J}\rangle |\mathbf{x} + \sum_{i \in \text{supp}(\mathbf{J})} \zeta_p^i \mathbf{s}\rangle,$$

where  $\mathbf{x} = \sum_{i=0}^{p-2} \mathbf{x}_i \zeta_p^i$  and  $\text{supp}(\mathbf{J}) = \{0 \leq i \leq p-2 \mid J_i \neq 0\}$ . This state is close to a  $\text{CCP}_{n,q,p}$  state. Indeed, a  $\text{CCP}_{n,q,p}$  state corresponds to the uniform superposition indexed by vectors  $\mathbf{J}$  in the subset

$$S = \{\mathbf{J}_j \in \mathbb{F}_2^{p-1} \mid j \in \mathbb{F}_p, (\mathbf{J}_j)_i = \mathbf{1}_{\{0, \dots, j-1\}}(i)\}.$$

Hence, by computing in an auxiliary register  $\mathbf{J} \mapsto \mathbf{1}_S(\mathbf{J})$  and measuring it, we obtain the output 1 with probability  $p/2^{p-1}$ . The remaining state corresponds to a superposition over  $S$  from which we can convert to a  $\text{CCP}_{n,q,p}$  state:

$$\sum_{\mathbf{J}_j \in S} |\mathbf{J}_j\rangle |\mathbf{x} + \sum_{i=0}^{j-1} \zeta_p^i \mathbf{s}\rangle \rightarrow \sum_{j \in \mathbb{F}_p} |j\rangle |\mathbf{x} + \sum_{i=0}^{j-1} \zeta_p^i \mathbf{s}\rangle.$$

Conversely, suppose we are given a  $\text{CCP}_{n,q,p}$  sample and we want to compute a  $\text{DCP}_{n,q}$  sample. We measure the two outcome projector onto the first register

subspace spanned by  $|0\rangle$  and  $|1\rangle$  and its orthogonal complement. With probability  $2/p$ , we get:

$$\frac{1}{\sqrt{2}}(|0\rangle|\mathbf{x}\rangle + |1\rangle|\mathbf{x} + \mathbf{s}\rangle).$$

We write  $\mathbf{x} = \sum_{i=0}^{p-2} x_i \zeta_p^i$  and apply the coefficient bijection  $f^{-1}$  to the second register. Since  $\mathbf{s} \in R_q^n$  has only a constant coefficient (it's the coordinatewise constant embedding of an element of  $\mathbb{Z}_q^n$  in  $R_q^n$ ), the state factors exactly as

$$\frac{|0\rangle|\mathbf{x}_0\rangle + |1\rangle|\mathbf{x}_0 + \mathbf{s}\rangle}{\sqrt{2}} \otimes |\mathbf{x}_1, \dots, \mathbf{x}_{p-2}\rangle$$

We can discard the last registers and get a DCP state.  $\square$

### 5.3 A potential direct reduction from CyLWE to CCP?

We believe it is possible to construct a direct reduction from CyLWE to CCP, analogous to Regev's reduction from LWE to DCP [14].

Informally, the idea is that given a CyLWE  $(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}) \in R_q^{m \times n} \times R_q^m$ , for a secret  $\mathbf{s} \in \mathbb{Z}_q^n$ , we consider a superposition on the  $q$ -ary cyclotomic lattice:

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in R_q^m \mid \mathbf{y} = \mathbf{A}\mathbf{x} \pmod{q}, \mathbf{x} \in R_q^n\},$$

which is shifted by a vector  $\lambda_j \mathbf{e}$ , where  $j$  is in  $\mathbb{F}_p$ . Given assumptions about the minimum distance of the  $q$ -ary lattice, the shift is very small compared to the minimum distance, and we can remove the error using cube-separation or ball-intersection techniques, as in [5].

However, for all of this to work, we obviously need results on the topology of random  $q$ -ary lattice, which we do not claim to have. Furthermore, such a reduction would improve only very slightly upon a reduction consisting of moving from CyLWE to LWE, then from LWE to DCP via [14], and finally from DCP to CCP.

## 6 Impact and discussions

In this section, we discuss the impact of Algorithm 1 on other, more extensively studied computational problems such as EDCP or  $S|\text{LWE}\rangle$ . This allows us to conclude that a quasi-polynomial-time algorithm exists when  $q$  is a power of a fixed prime  $p$ .

### 6.1 On the Extrapolated Dihedral Coset Problem.

**Definition 10 (Search Extrapolated Dihedral Coset Problem [5]).** *Let a parameter  $n$  be a dimension,  $q \geq 2$  be a modulus and  $M, \ell$  be positive integers. The uniform search Extrapolated Dihedral Coset Problem ( $\text{U-EDCP}_{n,q,M}^\ell$ ) consists of  $\ell$  input states of the form*

$$\frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} |j\rangle |\mathbf{x}_i + j\mathbf{s} \pmod{q}\rangle, \quad \text{for } i = 0 \dots \ell,$$

where  $\mathbf{x}_i \in \mathbb{Z}_q^n$  are sampled uniformly, and asks to recover the secret  $\mathbf{s} \in \mathbb{Z}_q^n$ .

**Lemma 8 ([9], Lemma 10).** *Let  $n, q, \ell, M, M'$  be integers greater than 1 and  $M \geq M'$ . There exists a probabilistic polynomial-time quantum reduction from  $\text{U-EDCP}_{n,q,M}^\ell$  to  $\text{U-EDCP}_{n,q,M'}^\ell$  that succeeds with a constant success probability.*

**Theorem 4.** *Let  $n, q, \ell, M$ , be integers greater than 1 and  $q$  be any prime-power. There exists a quantum algorithm that solves  $\text{U-EDCP}_{n,q,M}^\ell$  in time  $2^{O(\log n \log q)}$  using  $\text{poly}(n)$  quantum space, when  $\ell = 2^{\Omega(\log n \log q)}$ .*

*Proof.* The proof follows Lemma 8 in order to get  $\text{U-EDCP}_{n,q,2}^{\ell'}$  with  $\ell' = O(\ell)$ , then apply Proposition 5 to reduce to a  $\text{CCP}_{n,q,p}^{O(\ell')}$  and use the CCP solver in Algorithm 1.  $\square$

## 6.2 An algorithm for Gaussian $S|\text{LWE}\rangle$

In this section, we present a quasi-polynomial-time algorithm that solves the Gaussian  $S|\text{LWE}\rangle$  problem, based on the algorithm for solving CCP in Section 4. We thus generalize the procedure in [2] for this problem to any modulus  $q = p^t$ , where  $p$  is a constant prime. To do this, we first provide a definition of the Gaussian  $S|\text{LWE}\rangle$  problem and of  $\overline{\text{U-EDCP}}$ . This second problem will allow us to bridge the gap between  $S|\text{LWE}\rangle$  and PSP, defined in Section 3, to which we will be able to apply the procedure in Algorithm 1.

**Definition 11 (Gaussian  $S|\text{LWE}\rangle$ ).** *Given parameters  $\ell, n, q$  and a scalar  $r > 0$ , Gaussian  $S|\text{LWE}\rangle$  consists of  $\ell$  samples  $(\mathbf{a}_i, |\varphi_i\rangle)$  such that:*

$$\mathbf{a}_i \leftarrow \mathcal{U}(\mathbb{Z}_q^n), \quad |\varphi_i\rangle \propto \sum_{e \in \mathbb{Z}} \rho_r(e) |\langle \mathbf{a}_i, \mathbf{s} \rangle + e\rangle,$$

and asks to recover the secret  $\mathbf{s} \in \mathbb{Z}_q^n$ .

**Definition 12 ( $\overline{\text{U-EDCP}}$ ).** *Let a parameter  $n$  be a dimension,  $q \geq 2$  be a modulus and  $M, \ell$  be positive integers. The  $\overline{\text{U-EDCP}}$  consists of  $\ell$  samples of the following form:*

$$\mathbf{y}_k \leftarrow \mathcal{U}(\mathbb{Z}_q^n), \quad |\psi_{\mathbf{y}_k}\rangle = \frac{1}{\sqrt{M}} \sum_{j=0}^{M-1} \omega_q^{j \langle \mathbf{y}_k, \mathbf{s} \rangle} |j\rangle,$$

with  $\omega_q = \exp\left(\frac{2\sqrt{-1}\pi}{q}\right)$  and asks to recover the secret  $\mathbf{s} \in \mathbb{Z}_q^n$ .

Next, we recall in Lemma 9 the reduction that allows us to obtain  $\overline{\text{U-EDCP}}_{n,q,M}^{O(\ell)}$  samples from Gaussian  $S|\text{LWE}\rangle$  samples.

**Lemma 9 (from  $S|\text{LWE}\rangle$  to  $\overline{\text{U-EDCP}}$ , [2], Lemma 15 and 16).** *Let  $\kappa$  be the security parameter,  $\ell = \omega(\kappa)$  and  $n, q = \text{poly}(\kappa)$  be positive integers. Let  $r = \Omega(\sqrt{\kappa})$  and  $q/r = \Omega(\sqrt{\kappa})$ . There exists a quantum polynomial-time reduction from  $S|\text{LWE}\rangle_{n,q,r}^\ell$  to  $\overline{\text{U-EDCP}}_{n,q,M}^{O(\ell)}$ , where  $M = c \cdot r$  for some constant  $c$ , and succeeds with overwhelming probability.*

The next lemma converts these inputs into cyclotomic phase states.

**Lemma 10 (from  $\overline{\text{U-EDCP}}$  to PSP).** *Let  $n, q, M, p$  be integers greater than 1, with  $p$  prime and  $q = p^t$ . There exists a quantum algorithm that given a constant number of samples  $\overline{\text{U-EDCP}}_{n,q,q}$ , outputs  $\text{PSP}_{n,L,p}$  samples, with  $L = (p-1) \log q$ , involving the same secret  $\mathbf{s} \in \mathbb{Z}_q^n$  with constant probability.*

*Proof.* We describe the successive steps that allow us to obtain phase-state samples from states of the following form. We omit normalization factors in the intermediate expressions below.

$$|\phi_i\rangle \propto \sum_{x_i \in \mathbb{Z}_q} \omega_q^{x_i \langle \mathbf{y}_i, \mathbf{s} \rangle} |x_i\rangle, \quad \text{for } i = 0 \dots p-2,$$

with known labels  $\mathbf{y}_i$ .

1. We begin by entangling the  $p-1$  states to obtain the following state:

$$\begin{aligned} \bigotimes_{i=0}^{p-2} |\phi_i\rangle &= \sum_{(\mathbf{x}_0, \dots, \mathbf{x}_{p-2}) \in \{0, \dots, M-1\}^{p-1}} \omega_q^{\sum_{i=0}^{p-2} x_i \langle \mathbf{y}_i, \mathbf{s} \rangle} |\mathbf{x}_1\rangle \dots |\mathbf{x}_{p-2}\rangle \\ &= \sum_{\mathbf{x} \in \{0, \dots, M-1\}^{p-1}} \omega_q^{\mathbf{x}^T \mathbf{v}} |\mathbf{x}\rangle, \end{aligned}$$

where  $\mathbf{v} \in \mathbb{Z}_q^{p-1}$  is such that its  $i$ -th coordinate is  $v_i = \langle \mathbf{y}_i, \mathbf{s} \rangle$ .

2. Let  $\mathbf{D} \in \mathbb{Z}_q^{(p-1) \times (p-1)}$  be the invertible matrix associated with the bilinear form  $B_L$  from Proposition 3 with  $L = t(p-1)$ . By noting  $\mathbf{v}' = \mathbf{D}^{-1}\mathbf{v}$ , in other words there exists  $(\mathbf{y}'_i)_{i=0}^{p-2}$  such that  $\mathbf{v}'_i = \langle \mathbf{y}'_i, \mathbf{s} \rangle$  for  $0 \leq i \leq p-2$ . We have

$$\sum_{\mathbf{x} \in \{0, \dots, M-1\}^{p-1}} \omega_q^{\mathbf{x}^T \mathbf{D}\mathbf{v}'} |\mathbf{x}\rangle = \sum_{\mathbf{x} \in \iota(\{0, \dots, M-1\}^{p-1})} \chi_{\mathbf{x}}(\iota(\mathbf{v}')) |\mathbf{x}\rangle$$

where  $\iota : \mathbb{Z}_q^{p-1} \rightarrow R_q$  is the injection with respect to the basis  $(1, \zeta_p, \dots, \zeta_p^{p-2})$ . Moreover,  $\iota(\mathbf{v}') = \sum_{i=0}^{p-2} \zeta_p^i \langle \mathbf{y}'_i, \mathbf{s} \rangle = \langle \mathbf{y}', \mathbf{s} \rangle$ , where  $\mathbf{y}' = \sum_{i=0}^{p-2} \zeta_p^i \mathbf{y}'_i$ . Note that  $\mathbf{y}'$  follows a uniform distribution on  $\iota(\{0, \dots, M-1\}^{p-1})$  by invertibility of the coordinate transformation. We obtain

$$\chi_{\mathbf{x}}(\iota(\mathbf{v})) = \exp \left( 2i\pi \text{Tr} \left( \frac{\langle \mathbf{x}\mathbf{y}', \mathbf{s} \rangle}{p\pi^{L-1}} \right) \right) = \chi_{\mathbf{s}}(\mathbf{x}\mathbf{y}').$$

The resulting state at the end of this operation is therefore

$$\sum_{\mathbf{x} \in \iota(\{0, \dots, M-1\}^{p-1})} \chi_{\mathbf{s}}(\mathbf{x}\mathbf{y}') |\mathbf{x}\rangle.$$

3. The idea is now to move from a superposition over  $\mathbf{x} \in \iota(\{0, \dots, M-1\}^{p-1})$  to a superposition over  $E := \{\lambda_j\}_{j \in \mathbb{F}_p}$  and thereby obtain a PSP sample. To this end, we will use the intermediate superposition  $\iota(\{0, 1\}^{p-1})$ . We therefore compute in an auxiliary register the function  $\mathbf{x} \mapsto \lfloor \iota^{-1}(\mathbf{x})/2 \rfloor$ , which we measure directly. Let  $\mathbf{k} \in \mathbb{Z}_q^{p-1}$  denote the output, and suppose that  $\mathbf{k} \in \{0, \dots, (M-1)/2\}^{p-1}$  this happens with probability bounded below by a positive constant when  $M$  is large (otherwise, we discard the resulting state and restart from the beginning). The remaining state has support in the following translated set:

$$\iota(\mathbf{k}) + \iota(\{0, 1\}^{p-1}) \subset \iota(\{0, \dots, M-1\}^{p-1}),$$

that is,

$$\sum_{\mathbf{x} \in \iota(\{0, 1\}^{p-1})} \chi_{\mathbf{s}}((\mathbf{x} - \iota(\mathbf{k}))\mathbf{y}') |\mathbf{x}\rangle \propto \sum_{\mathbf{x} \in \iota(\{0, 1\}^{p-1})} \chi_{\mathbf{s}}(\mathbf{x}\mathbf{y}') |\mathbf{x}\rangle.$$

4. Finally, it suffices to compute the function  $\mathbf{x} \mapsto \mathbf{1}_E(\mathbf{x})$  in a new auxiliary register. After measurement, there is a constant probability  $p/2^{p-1}$  of obtaining the desired output 1 and thus obtaining a PSP state with label  $\mathbf{y}'$  and with respect to the same secret  $\mathbf{s} \in \mathbb{Z}_q^{p-1}$ .  $\square$

Observe that this lemma provides an alternative way to prove the existence of a quasi-polynomial-time algorithm for uniform EDCP without having to resort to a reduction to DCP.

**Theorem 5.** *Let  $\kappa$  be the security parameter and  $n, q = \text{poly}(\kappa)$  be integers, where  $q = p^t$  is a power of a fixed prime  $p$ . Let  $r = \Omega(\sqrt{\kappa})$  and  $q/r = \Omega(\sqrt{\kappa})$ . There exists a quantum algorithm that solves  $S|\text{LWE}\rangle_{n,q,r}^\ell$  in time  $2^{O(\log^2 n)}$  using  $\text{poly}(n)$  quantum space, when  $\ell = 2^{\Omega(\log^2 n)}$ .*

*Proof.* Start by applying Lemma 9 to obtain  $O(\ell)$   $\overline{\text{U-EDCP}}$  samples, then applying Lemma 10 to get  $O(\ell)$  phase-state sample involving the same secret  $\mathbf{s} \in \mathbb{Z}_q^n$ . Then it remains to apply the procedure from Algorithm 1 to recover  $\mathbf{s}$  from a quasi-polynomial number of phase-state samples.  $\square$

Note that the Lemma 10, which is used to prove the existence of an algorithm for the Gaussian  $S|\text{LWE}\rangle$ , is specific to our paper. Indeed, to the best of our knowledge,  $S|\text{LWE}\rangle$  is not a hidden subgroup problem. We therefore would not have been able to obtain such an algorithm had we not defined a quantum Fourier transform on  $R_q$  and had we not explicitly specified the phase-state samples.

*Non-impact on Learning with Errors.* Since this result generalizes the algorithm in [2], we obtain the same conclusion regarding the security of LWE. Indeed, the sieving algorithm requires too many CCP samples, and the reduction from LWE to DCP places an upper bound on the number of samples that is smaller than the number of samples required to solve the problem.

## References

1. Aggarwal, D., Regev, O.: A Note on Discrete Gaussian Combinations of Lattice Vectors (Aug 2013), <https://arxiv.org/abs/1308.2405v2>
2. Bai, S., Jangir, H., Kirshanova, E., Ngo, T., Youmans, W.: A Quasi-polynomial Time Algorithm for the Extrapolated Dihedral Coset Problem over Power-of-Two Moduli. In: Kalai, Y.T., Kamara, S.F. (eds.) *Advances in Cryptology - CRYPTO 2025 - 45th Annual International Cryptology Conference*, Santa Barbara, CA, USA, August 17-21, 2025, Proceedings, Part II. pp. 416–448. *Lecture Notes in Computer Science*, Springer (2025). [https://doi.org/10.1007/978-3-032-01878-6\\_14](https://doi.org/10.1007/978-3-032-01878-6_14), [https://doi.org/10.1007/978-3-032-01878-6\\_14](https://doi.org/10.1007/978-3-032-01878-6_14)
3. Banaszczyk, W.: New bounds in some transference theorems in the geometry of numbers. *Mathematische Annalen* **296**(1), 625–635 (Dec 1993). <https://doi.org/10.1007/BF01445125>, <https://doi.org/10.1007/BF01445125>
4. Bonnetain, X., Naya-Plasencia, M.: Hidden Shift Quantum Cryptanalysis and Implications (2018), <https://eprint.iacr.org/2018/432>, publication info: Preprint. MINOR revision.
5. Brakerski, Z., Kirshanova, E., Stehlé, D., Wen, W.: Learning with Errors and Extrapolated Dihedral Cosets. In: Abdalla, M., Dahab, R. (eds.) *Public-Key Cryptography - PKC 2018 - 21st IACR International Conference on Practice and Theory of Public-Key Cryptography*, Rio de Janeiro, Brazil, March 25-29, 2018, Proceedings, Part II. pp. 702–727. *Lecture Notes in Computer Science*, Springer (2018). [https://doi.org/10.1007/978-3-319-76581-5\\_24](https://doi.org/10.1007/978-3-319-76581-5_24), [https://doi.org/10.1007/978-3-319-76581-5\\_24](https://doi.org/10.1007/978-3-319-76581-5_24)
6. Chailloux, A., Hermouet, P.: On the quantum equivalence between  $s|LWE\rangle$  and ISIS. *Cryptology ePrint Archive*, Paper 2025/1857 (2025), <https://eprint.iacr.org/2025/1857>
7. Chen, Y., Liu, Q., Zhandry, M.: Quantum algorithms for variants of average-case lattice problems via filtering. In: Dunkelman, O., Dziembowski, S. (eds.) *Advances in Cryptology - EUROCRYPT 2022 - 41st Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III. *Lecture Notes in Computer Science*, vol. 13277, pp. 372–401. Springer (2022). [https://doi.org/10.1007/978-3-031-07082-2\\_14](https://doi.org/10.1007/978-3-031-07082-2_14), [https://doi.org/10.1007/978-3-031-07082-2\\_14](https://doi.org/10.1007/978-3-031-07082-2_14)
8. Childs, A.M., van Dam, W.: Quantum algorithm for a generalized hidden shift problem. In: *Proceedings of the Eighteenth Annual ACM-SIAM Symposium on Discrete Algorithms*. p. 1225–1232. *SODA '07*, Society for Industrial and Applied Mathematics, USA (2007)
9. Doliskani, J.: Efficient Quantum Public-Key Encryption From Learning With Errors (2020), <https://eprint.iacr.org/2020/1557>, publication info: Preprint. MINOR revision.
10. Imran, M., Ivanyos, G.: Zero sum subsequences and hidden subgroups. *Quant. Inf. Proc.* **23**(1), 14 (2024). <https://doi.org/10.1007/s11128-023-04228-2>
11. Kuperberg, G.: A Subexponential-Time Quantum Algorithm for the Dihedral Hidden Subgroup Problem. *SIAM Journal on Computing* **35**(1), 170–188 (2005). <https://doi.org/10.1137/S0097539703436345>, <https://doi.org/10.1137/S0097539703436345>, [\\_eprint: https://doi.org/10.1137/S0097539703436345](https://doi.org/10.1137/S0097539703436345)
12. Kuperberg, G.: Another subexponential-time quantum algorithm for the dihedral hidden subgroup problem. In: Severini, S., Brandão, F.G.S.L. (eds.) *8th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC*

- 2013, Guelph, Canada, May 21-23, 2013. LIPIcs, vol. 22, pp. 20–34. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2013). <https://doi.org/10.4230/LIPICS.TQC.2013.20>, <https://doi.org/10.4230/LIPICS.TQC.2013.20>
13. Regev, O.: Quantum computation and lattice problems. In: 43rd Symposium on Foundations of Computer Science, FOCS 2002, Vancouver, BC, Canada, November 16-19, 2002, Proceedings. pp. 520–529. IEEE Computer Society (2002). <https://doi.org/10.1109/SFCS.2002.1181976>, <https://doi.org/10.1109/SFCS.2002.1181976>
  14. Regev, O.: Quantum Computation and Lattice Problems. SIAM J. Comput. **33**(3), 738–760 (2004). <https://doi.org/10.1137/S0097539703440678>, <https://doi.org/10.1137/S0097539703440678>
  15. Regev, O.: A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space (Jun 2004), <https://arxiv.org/abs/quant-ph/0406151v1>
  16. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In: Gabow, H.N., Fagin, R. (eds.) Proceedings of the 37th Annual ACM Symposium on Theory of Computing, Baltimore, MD, USA, May 22-24, 2005. pp. 84–93. ACM (2005). <https://doi.org/10.1145/1060590.1060603>, <https://doi.org/10.1145/1060590.1060603>
  17. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**(6), 34:1–34:40 (2009). <https://doi.org/10.1145/1568318.1568324>, <https://doi.org/10.1145/1568318.1568324>
  18. Rotman, J.: An Introduction to the Theory of Groups. Graduate Texts in Mathematics, Springer New York (1999), <https://books.google.fr/books?id=vb9kUfHqQigC>
  19. Wen, W., Zheng, J.: Module Learning With Errors and Structured Extrapolated Dihedral Cosets (2026), <https://eprint.iacr.org/2026/155>, publication info: Preprint.
  20. de Wolf, R.: Quantum computing: Lecture notes (2026), <https://arxiv.org/abs/1907.09415>
  21. Zhang, Y.: Quantum Fourier Transform Over Galois Rings (Apr 2009). <https://doi.org/10.48550/arXiv.0904.2560>, <http://arxiv.org/abs/0904.2560>, arXiv:0904.2560 [quant-ph]