# Relating different Polynomial-LWE problems

Madalina Bolboceanu

Bitdefender, Romania

**Abstract.** In this paper we focus on Polynomial Learning with Errors (PLWE). This problem is parametrized by a polynomial and we are interested in relating the hardness of the PLWE$^f$ and PLWE$^h$ problems for different polynomials $f$ and $h$. More precisely, our main result shows that for a fixed monic polynomial $f$, PLWE$^{f\circ g}$ is at least as hard as PLWE$^f$, in both search and decision variants, for any monic polynomial $g$. As a consequence, PLWE$^{\phi_n}$ is harder than PLWE$^f$, for a minimal polynomial $f$ of an algebraic integer from the cyclotomic field $\mathbb{Q}(\zeta_n)$ with specific properties. Moreover, we prove in decision variant that in the case of power-of-2 polynomials, PLWE$^{\phi_n}$ is at least as hard as PLWE$^f$, for a minimal polynomial $f$ of algebraic integers from the $n$th cyclotomic field with weaker specifications than those from the previous result.

**Keywords.** lattice-based cryptography, LWE, PLWE

## 1 Introduction

Lattice-based cryptography is one of the most promising solutions for post-quantum cryptography. One important hard lattice problem which is assumed to remain difficult to solve even with quantum algorithms is Approximate Shortest Vector Problem (ApproxSVP). This problem requires finding a short vector in a lattice, up to an approximation factor. Regev introduced in [Reg05] Learning with Errors (LWE) and gave a quantum reduction from a variant of ApproxSVP to LWE. The goal of its search variant is to find a uniformly sampled vector $\mathbf{s}$ from $\mathbb{Z}_q^n$ from given samples of the form $(\mathbf{A}, \mathbf{A}\cdot\mathbf{s}+\mathbf{e}) \in \mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^n$, where $\mathbf{A}$ is a uniformly sampled matrix from $\mathbb{Z}_q^{m\times n}$ and the noise vector $\mathbf{e}$ is sampled from a discrete Gaussian distribution of small parameter over $\mathbb{Z}^n$. Its decision variant asks you to distinguish such samples for a common secret vector $\mathbf{s}$ from uniform pairs from $\mathbb{Z}_q^{m\times n} \times \mathbb{Z}_q^n$. This problem is a very versatile one, since it enables the design of many advanced cryptographic primitives such as fully homomorphic encryption [GSW13], identity based encryption [ABB10], predicate encryption [GVW15] or key-homomorphic pseudorandom functions [BP14].

The main drawback of the schemes based on LWE is the large size of keys. In order to achieve practical efficiency, algebraic variants of

LWE have been introduced, which use structured matrices. The Polynomial Learning with Errors problem (PLWE) was introduced in [SSTX09] and was initially called Ideal-LWE. It is parametrized by a polynomial $f \in \mathbb{Z}[X]$ and an integer $q \geq 2$ and described in terms of elements from $\mathbb{Z}_q[X]/(f)$. Concretely, its search variant asks you to find a secret polynomial $s$ sampled uniformly from $\mathbb{Z}_q[X]/(f)$, given pairs of the form $(a_i, a_i \cdot s + e_i)$ from $\mathbb{Z}_q[X]/(f) \times \mathbb{R}_q[X]/(f)$, where $a_i$ is sampled uniformly from $\mathbb{Z}_q[X]/(f)$. The coefficient embedding of the noise polynomial $e_i$ follows a Gaussian distribution of small covariance matrix. For a common uniformly sampled $s$, the decision variant consists in distinguishing between such samples and uniform samples from $\mathbb{Z}_q[X]/(f) \times \mathbb{R}_q[X]/(f)$. It may be considered an LWE problem, except that the matrix is not uniform, but instead it is a structured matrix generated by the uniform polynomials $a_i$. Lyubashevsky et al. [LPR10] introduced Ring Learning with Errors (Ring-LWE) which uses number fields instead of polynomials. In this case the error is sampled such that its Minkowski embedding follows a Gaussian distribution. They also gave a reduction from search to decision variants for the case of cyclotomic polynomials, which was further extended for general Galois extensions in [EHL14] and [CLS15]. It has been shown that in the case of power-of-2 cyclotomic polynomials both PLWE and Ring-LWE coincide. Recently, Rosca et al. [RSW18] gave reductions between (search/decision) Ring-LWE and (search/decision) PLWE which incur limited noise growth increases for an exponentially large class of polynomials $f$.

PLWE and RLWE are interesting problems, because their hardness relies on the restriction of ApproxSVP to a special class of so called *ideal lattices*. This restriction is called Ideal-SVP. If Ideal-SVP is assumed to be hard in worst-case, this leads to the PLWE and Ring-LWE instances to be hard. Indeed, Stehlé et al. gave in [SSTX09] a quantum reduction from Ideal-SVP to (search) PLWE$^f$ for power-of-2 cyclotomic polynomials $f$. Later on, Lyubashevsky et al. [LPR10] gave a quantum reduction from Ideal-SVP to (search) Ring-LWE, while Peikert et al. [PRSD17] gave a quantum reduction from Ideal-SVP directly to (decision) Ring-LWE, which works for any number field and modulus. Many provable secure cryptographic applications can be designed from these assumptions, such as key encapsulation mechanisms [ADPS16], [SSZ17] or fully homomorphic encryption schemes [Gen09], [BV11]. It is natural to ask if Approx-SVP is still hard when one restricts only to ideal lattices. One approach to this problem is the one of Cramer et al. [CDPR16] who found a quantum polynomial time algorithm for solving Ideal-SVP for principal ideals

in cyclotomic fields of prime power conductor with $2^{\tilde{O}(\sqrt{n})}$ approximation factor, where $n$ is the degree of the field used. To compare this result with classical algorithms, we mention that the best algorithm for approximating shortest vector with this approximation factor, [SE94], runs in time $2^{\tilde{O}(\sqrt{n})}$, where $n$ is the lattice dimension. Furthermore, Cramer et al. [CDW17] generalized the previous statement by giving a quantum polynomial time algorithm for solving Ideal-SVP for arbitrary ideals in cyclotomic rings. Still, the approximation factor is too large to impact the security of the primitives based on Ring-LWE or PLWE. Until now, there is no reduction from Ring-LWE or PLWE to Ideal-SVP. In terms of hardness, all these attacks show that Ideal-SVP problems for ideal lattices are not the same for all polynomials $f$. The easy instances of Ideal-SVP make the reduction from [SSTX09] vacuous for the corresponding PLWE$^f$ instances. There is a lack of knowledge in finding the polynomial $f$ for which the corresponding PLWE$^f$ problem is the hardest. One may want either to propose a new problem harder than the PLWE$^f$ problem for exponentially many polynomials $f$ or to further study which might be the hardest instances of the PLWE problem.

The first approach was made by Rosca et al. [RSSS17] who proposed Middle Product Learning with Errors (MP-LWE). They gave a reduction from (decision) PLWE$^f$ to (decision) MP-LWE for exponentially many monic polynomials $f$ with bounded expansion factor and constant coefficient coprime with $q$.

**Our contributions.** In this paper we focus on the second approach, namely on finding a polynomial for which the corresponding PLWE problem is at least as hard as many other PLWE problems. Our main result towards this goal is a reduction from PLWE$^f$ to PLWE$^{f\circ g}$ for an arbitrary monic polynomial $g$. This has interesting consequences involving cyclotomic polynomials. As a corollary, we obtain that PLWE$^{\phi_n}$ for the cyclotomic polynomial $\phi_n$ is harder than PLWE$^f$ for all the minimal polynomials $f$ of algebraic integers of the cyclotomic field $\mathbb{Q}(\zeta_n)$ which have specific properties we will mention. We extend this result by showing that, in the case of power-of-2 cyclotomic polynomials $\phi_n$, PLWE$^{\phi_n}$ is at least as hard as PLWE$^f$ for all the minimal polynomials $f$ of algebraic integers of the $n$th cyclotomic field which have weaker properties than those from the previous corollary. All these reductions, excepting the last one, hold in both search and decision variants. The last reduction holds only in decision variant.

**Organization.** Section 2 gives the necessary background regarding the PLWE problem. Section 3 presents the reductions relating the PLWE

problems for different polynomials. In Section 4 we discuss the impact of the main result. In Section 5 we describe some open problems.

## 2 Preliminaries

For a finite set $X$ we denote by $U(X)$ the uniform distribution over $X$. We write $x \leftarrow\!\!\shortmid\ \psi$ when $x$ follows a distribution $\psi$. We write by $[n]$ the set $\{1, 2, \ldots, n\}$. For a matrix $\mathbf{M}$ in $\mathbb{R}^{m \times n}$, we denote by $\|\mathbf{M}\|_F = \sqrt{\sum_{i \in [m]} \sum_{j \in [n]} \mathbf{M}_{i,j}^2}$ the Frobenius norm of $\mathbf{M}$.

### 2.1 Cyclotomic polynomials

The cyclotomic polynomials, especially the power-of-2 cyclotomic ones, have been frequently used in designing cryptographic primitives since their use leads to very efficient solutions, such as homomorphic encryption schemes, [BV11], [BGV11], [GHPS12], or key exchange systems,[ADPS16].

For a positive integer $n$, we denote by $\zeta_n = e^{\frac{2\pi i}{n}}$ an $n$th primitive root. The $n$th cyclotomic polynomial $\phi_n \in \mathbb{Z}[X]$ is the minimal polynomial of $\zeta_n$ over $\mathbb{Q}$ and has as roots all the $n$th primitive roots:

$$\phi_n(X) = \prod_{k \in \mathbb{Z}_n^*} (X - \zeta_n^k).$$

The degree of the cyclotomic polynomial $\phi_n$ is $|\mathbb{Z}_n^*| = \varphi(n)$, where $\varphi$ is the Euler's totient function.

The $n$th cyclotomic field is obtained by adjoining $\zeta_n$ to the rational field $\mathbb{Q}$ (as an abstract element, not as a complex number). There is a natural isomorphism of rings from $\mathbb{Q}[X]/(\phi_n)$ to $\mathbb{Q}(\zeta_n)$, which sends $X$ to $\zeta_n$. This map can be seen as the evaluation map at $\zeta_n$. The ring of algebraic integers of $\mathbb{Q}(\zeta_n)$ is precisely $\mathbb{Z}[\zeta_n]$. This is a $\mathbb{Z}$ module having as basis $\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{\varphi(n)-1}\}$.

We mention here an useful property which relates different cyclotomic polynomials:

**Proposition 2.1. ([LPR13], Fact 2.12)** *Let $n$ be a positive integer and* $\mathrm{rad}(n)$ *the product of all distinct prime divisors of $n$. Then $\phi_n(X) = \phi_{\mathrm{rad}(n)}(X^{n/\mathrm{rad}(n)})$. In particular, if $p$ is a prime and $n$ is a prime power of $p$, then $\phi_n(X) = \phi_p(X^{n/p})$.*

### 2.2 Gaussian distributions

For a symmetric positive definite matrix $\mathbf{\Sigma}$ in $\mathbb{R}^{n\times n}$, we define the Gaussian function on $\mathbb{R}^n$ of covariance matrix $\mathbf{\Sigma}$ as $\rho_{\sqrt{\mathbf{\Sigma}}}(\mathbf{x}) = \exp(-\pi\cdot\mathbf{x}^t\mathbf{\Sigma}^{-1}\mathbf{x})$, where $\mathbf{x}\in\mathbb{R}^n$. When discussing about distributions, we normalize this function $\rho_{\sqrt{\mathbf{\Sigma}}}$ and obtain the (continuous) Gaussian probability distribution $D_{\sqrt{\mathbf{\Sigma}}}$. If $\mathbf{\Sigma} = s^2 I_n$, where $s$ is a positive real number, we simply denote by $\rho_s$ and $D_s$ the Gaussian function and the Gaussian distribution, respectively. It is easy to see that a random vector $\mathbf{x}$ in $\mathbb{R}^n$ follows the Gaussian distribution $D_s$ if and only if its coordinates are independent random variables which follow the Gaussian distribution $D_s$ over $\mathbb{R}$. We will frequently use the fact that if $\mathbf{x}$ is a random vector in $\mathbb{R}^n$ whose distribution is the Gaussian distribution $D_{\sqrt{\mathbf{\Sigma}}}$, then for a matrix $\mathbf{A}$ in $\mathbb{R}^{m\times n}$, the distribution of $\mathbf{A}\cdot\mathbf{x}$ will be the Gaussian distribution $D_{\sqrt{\mathbf{A\Sigma A}^t}}$ over $\mathbb{R}^m$.

### 2.3 The Polynomial Learning with Errors Problem

We now define the problem we study in this paper. Consider a monic polynomial $f$ in $\mathbb{Z}[X]$ and a prime modulus $q$. Denote by $R = \mathbb{Z}[X]/(f)$ and by $R_q = R/qR = \mathbb{Z}_q[X]/(f)$. We use the notation $\mathbb{R}_q := \mathbb{R}/q\mathbb{Z}$.

**Definition 2.1. ($\mathrm{PLWE}^f_{q,\psi}$ distribution).** *For any $s\in R_q$, we define $\mathrm{PLWE}^f_{q,\psi}(s)$ as the distribution over $\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f)$ obtained by sampling $a\hookleftarrow U(R_q)$, by sampling an error polynomial $e\hookleftarrow\psi$ over $\mathbb{R}[X]/(f)$ and by returning $(a, a\cdot s+e \bmod qR)$.*

**Definition 2.2. (The $\mathrm{PLWE}^f$ problem).** *Search $\mathrm{PLWE}^f_{q,\psi}$ consists in finding $s\in\mathbb{Z}_q[X]/(f)$ given an arbitrary number of independent samples from $\mathrm{PLWE}^f_{q,\psi}(s)$, where $s\hookleftarrow U(\mathbb{Z}_q[X]/(f))$. Decision $\mathrm{PLWE}^f_{q,\psi}$ consists in distinguishing between an arbitrary number of independent $\mathrm{PLWE}^f_{q,\psi}(s)$ samples and the same number of independent samples from $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$, with non-negligible probability over the choices of $s\hookleftarrow U(\mathbb{Z}_q[X]/(f))$.*

We will mainly discuss about the decision variant of the $\mathrm{PLWE}^f$ problems where the error polynomial is sampled according to a Gaussian distribution $D_{\alpha q}$, for some $\alpha > 0$. The support of the continuous Gaussian distribution, $\mathbb{R}^n$, is identified with $\mathbb{R}[X]/(f)$, where $n$ is the degree of $f$.

*Remark 2.1.* It suffices to discuss about the PLWE problems for an irreducible polynomial $f$, since if $h|f$, one can find a reduction from $\mathrm{PLWE}^f_{q,\psi}$

to $\mathrm{PLWE}^h_{q,\psi}$. Indeed, the map $\mathbb{Z}[X]/(f) \to \mathbb{Z}[X]/(h), a \to a \bmod h$ is well defined since if $a \equiv \bar{a} \bmod f$, then $f|a - \bar{a}$ and therefore $h|a - \bar{a}$.

## 3 The main result

We consider a fixed monic polynomial $f$ in $\mathbb{Z}[X]$ of degree $m$. Our main result is a reduction from $\mathrm{PLWE}^f$ to $\mathrm{PLWE}^{f\circ g}$, for any arbitrary monic polynomial $g \in \mathbb{Z}[X]$. In order to build intuition for the proof of the main result, we first present a simpler particular case, when $g = X^n$.

### 3.1 An easy particular case

For a positive integer $n$, we denote by $g_n$ the polynomial $X^n$ and by $f_n$ the polynomial $f \circ g_n$. We prove a reduction from (decision) $\mathrm{PLWE}^f_{q,D_{\alpha q}}$ to (decision) $\mathrm{PLWE}^{f_n}_{q,D_{\alpha q}}$, which has a similar but simpler proof as the one of Theorem 3.2, the general case. Unlike the general case, here the error distribution is the same.

We first make some notations: for a ring $R$ (which can be $\mathbb{R}$, $\mathbb{Z}_q$ or $\mathbb{R}_q$) and a monic polynomial $g$ from $\mathbb{Z}[X]$, we consider the maps:

$$\mathcal{F}_{R,g} : (R[X]/(f))^n \to R[X]/(f \circ g),\ \mathcal{F}_{R,g}(c_0, c_1, \ldots, c_{n-1}) = \sum_{i=0}^{n-1} X^i c_i \circ g.$$

We can see that $\mathcal{F}_{R,g}$ is a well defined $R$ linear map of modules, if we consider the input polynomials as a vector obtained by concatenating their vector coefficients.

*Remark 3.1.* For $c_i \in R[X]/(f)$, where $0 \leq i \leq n-1$, we obtain

$$\mathcal{F}_{R,g_n}(c_0, c_1, \ldots, c_{n-1})(X) = \sum_{i=0}^{n-1} X^i c_i \circ g_n(X) = \sum_{i=0}^{n-1} X^i c_i(X^n).$$

Hence the new polynomial has $mn$ coefficients obtained by putting the coefficients of $c_i$ on positions of indices of form $nk+i$, for any $0 \leq i \leq n-1$. We can say that $\mathcal{F}_{R,g_n}$ permutes the coefficients of the input polynomials.

**Theorem 3.1.** *For a monic polynomial $f$ from $\mathbb{Z}[X]$, if $\mathrm{PLWE}^f_{q,D_{\alpha q}}$ is hard given $k+n-1$ samples, then so is $\mathrm{PLWE}^{f_n}_{q,D_{\alpha q}}$ given $k$ samples.*

*Proof.* Assume $\mathcal{B}$ is an algorithm which distinguishes an $\mathrm{PLWE}^{f_n}_{q,D_{\alpha q}}$ distribution from the uniform distribution over $\mathbb{Z}_q[X]/(f_n) \times \mathbb{R}_q[X]/(f_n)$. We construct an algorithm $\mathcal{A}$ which distinguishes an $\mathrm{PLWE}^f_{q,D_{\alpha q}}$ distribution

from the uniform distribution over $\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f)$. $\mathcal{A}$ uses a transformation $T$ which maps $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$ to $U(\mathbb{Z}_q[X]/(f_n)\times\mathbb{R}_q[X]/(f_n))$ and $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$, for a uniform $s$, to $\mathrm{PLWE}^{f_n}_{q,D_{\alpha q}}(\tilde{s})$, where $\tilde{s}$ is uniform and may depend on $s$. This transformation will be described below.

The distinguisher $\mathcal{A}$ draws $n-1$ samples $(a_i^*, b_i^*)$ from the unknown distribution, which may be either $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$, for $s \hookleftarrow \mathbb{Z}_q[X]/(f)$, or $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$. Then it picks $\tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_{n-1} \hookleftarrow U(\mathbb{Z}_q[X]/(f))$. For any query $\mathcal{B}$ makes, $\mathcal{A}$ asks for a fresh sample $(a_j, b_j)$ from the same distribution, where $j \in [k]$, applies $T$ and gives to $\mathcal{B}$ the sample $(\tilde{a}_j, \tilde{b}_j) = T(a_j, b_j)$. When $\mathcal{B}$ ends, $\mathcal{A}$ returns its output.

Assuming $T$ satisfies the specifications stated above, the reduction indeed maps uniform samples to uniform samples and $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$ samples for a uniform $s$ to $\mathrm{PLWE}^{f_n}_{q,D_{\alpha q}}(\tilde{s})$ samples for a uniform $\tilde{s}$ depending on $s$. Hence $\mathcal{A}$ will distinguish with the same probability as $\mathcal{B}$ distinguishes. We describe the map $T$ and prove its stated properties: $T : \mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f) \to \mathbb{Z}_q[X]/(f_n)\times\mathbb{R}_q[X]/(f_n)$, $T(a_j, b_j) = (\tilde{a}_j, \tilde{b}_j)$, where:

$$\tilde{a}_j = \mathcal{F}_{\mathbb{Z}_q, g_n}(a_j, a_1^*, \ldots, a_{n-1}^*) \tag{1}$$

$$\tilde{b}_j = \mathcal{F}_{\mathbb{R}_q, g_n}(b_j, b_1^*, \ldots, b_{n-1}^*) + \tilde{a}_j \cdot \sum_{i\in[n-1]} X^i \tilde{s}_i \circ g_n \tag{2}$$

Since $\mathcal{F}_{\mathbb{Z}_q, g_n}$ and $\mathcal{F}_{\mathbb{R}_q, g_n}$ are well defined, so is $T$.
If $\{(a_j, b_j)\}_{j\in[k]}$ and $\{(a_i^*, b_i^*)\}_{i\in[n-1]}$ are drawn from the uniform distribution, then their coefficients are also uniform. Due to Remark 3.1, $\tilde{a}_j$ and $\mathcal{F}_{\mathbb{R}_q, g_n}(b_j, b_1^*, \ldots, b_{n-1}^*)$ have uniform coefficients. Hence $\{(\tilde{a}_j, \tilde{b}_j)\}_{j\in[k]}$ are from the uniform distribution.
Now suppose that the samples above are drawn from $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$, where $s$ is uniform. Then

$$b_i^* = a_i^* \cdot s + e_i^* \in \mathbb{R}_q[X]/(f), \text{ for any } i \in [n-1] \tag{3}$$

$$b_j = a_j \cdot s + e_j \in \mathbb{R}_q[X]/(f), \text{ for any } j \in [k] \tag{4}$$

where $e_j, e_i^*$'s $\hookleftarrow D_{\alpha q}$ distribution over $\mathbb{R}[X]/(f)$. Notice that:

$$b_i^* \circ g_n = a_i^* \circ g_n \cdot s \circ g_n + e_i^* \circ g_n \in \mathbb{R}_q[X]/(f_n), \text{ for any } i \in [n-1]$$
$$b_j \circ g_n = a_j \circ g_n \cdot s \circ g_n + e_j \circ g_n \in \mathbb{R}_q[X]/(f_n), \text{ for any } j \in [k]$$

Using equations (1), (3) and (4) we obtain from equation (2) the following:

$$\tilde{b}_j = ((a_j \circ g_n \cdot s \circ g_n + e_j \circ g_n) + \tilde{a}_j \cdot \sum_{i\in[n-1]} X^i \tilde{s}_i \circ g_n$$
$$+ \sum_{i\in[n-1]} X^i \left(a_i^* \circ g_n \cdot s \circ g_n + e_i^* \circ g_n\right)$$
$$= \left(a_j \circ g_n + \sum_{i\in[n-1]} X^i a_i^* \circ g_n\right) \cdot s \circ g_n + \left(e_j \circ g_n + \sum_{i\in[n-1]} X^i e_i^* \circ g_n\right)$$
$$+ \tilde{a}_j \sum_{i=1}^{n-1} X^i \tilde{s}_i \circ g_n = \tilde{a}_j \mathcal{F}_{\mathbb{Z}_q,g_n}(s, \tilde{s}_1, \ldots, \tilde{s}_{n-1}) + \mathcal{F}_{\mathbb{R},g_n}(e_j, e_1^*, \ldots, e_{n-1}^*)$$

Denote by

$$\tilde{s} = \mathcal{F}_{\mathbb{Z}_q,g_n}(s, \tilde{s}_1, \ldots, \tilde{s}_{n-1}) \text{ and } \tilde{e}_j = \mathcal{F}_{\mathbb{R},g_n}(e_j, e_1^*, \ldots, e_{n-1}^*),\ j \in [k] \quad (5)$$

We have seen already that $\tilde{a}_j$ is uniform since $a_j, a_i^* \hookleftarrow U(\mathbb{Z}_q[X]/(f))$. As $\tilde{a}_j$, the coefficients of $\tilde{s}$ are obtained by a permutation of the coefficients of $s$ and $\tilde{s}_i$'s. Since $s, \tilde{s}_i$'s $\hookleftarrow U(\mathbb{Z}_q[X](f))$, $\tilde{s}$ is also uniform in $\mathbb{Z}_q[X]/(f_n)$. Similarly, the coefficients of $\tilde{e}_j$ are obtained by a permutation of the coefficients of $e_j$ and $e_i^*$'s , due to the action of $\mathcal{F}_{\mathbb{R},g_n}$ explained in Remark 3.1. Therefore, $\tilde{e}_j$ follows the Gaussian distribution $D_{\alpha q}$ over $\mathbb{R}^{mn}$, viewed as $\mathbb{R}[X]/(f_n)$ since $e_j, e_i^*$'s $\hookleftarrow D_{\alpha q}$ over $\mathbb{R}^m$, viewed as $\mathbb{R}[X]/(f)$. Hence, using equations (5) we get: $\tilde{b}_j = \tilde{a}_j \cdot \tilde{s} + \tilde{e}_j$ in $\mathbb{R}_q[X]/(f_n)$, so $(\tilde{a}_j, \tilde{b}_j)$ is indeed a $\mathrm{PLWE}_{q,D_{\alpha q}}^{f_n}(\tilde{s})$ sample. □

*Remark 3.2.* We mention that the reduction also works for search variants. Indeed if one algorithm $\mathcal{B}$ gets $\tilde{s}$ from $\mathrm{PLWE}_{q,D_{\alpha q}}^{f_n}(\tilde{s})$ samples, then one can construct an algorithm $\mathcal{A}$ who gets $s$ from $\mathrm{PLWE}_{q,D_{\alpha q}}^{f}(s)$ samples using the same transformation as above, since it can get $\tilde{s}$ from $\mathcal{B}$ and therefore $s$ from equation (5), due to the action of $\mathcal{F}_{\mathbb{Z}_q,g_n}$.

### 3.2 The general case

We generalize now Theorem 3.1 by considering an arbitrary monic polynomial $g$ in $\mathbb{Z}[X]$ instead of $g_n$. For this we need to understand better the maps $\mathcal{F}_{R,g}$.

For any monic polynomial $g$ in $\mathbb{Z}[X]$ of degree $n$ and a positive integer $k$, we denote by $\mathbf{T}_g$ the $kn \times kn$ matrix having as columns the vector coefficients of the polynomials

$$1, g, \ldots, g^{k-1}, X, Xg, \ldots, Xg^{k-1}, \ldots, X^{n-1}, X^{n-1}g, \ldots, X^{n-1}g^{k-1}.$$

If the entries are modulo $q$, we denote the obtained matrix by $\mathbf{T}_{g,q}$. From now on, we consider $k$ as the degree of $f$ denoted by $m$, so $\mathbf{T}_g$ is an $mn \times mn$ matrix. For our main result we use the following lemmas:

**Lemma 3.1.** *The maps $\mathcal{F}_{\mathbb{Z}_q,g}$ and $\mathcal{F}_{\mathbb{R}_q,g}$ are both defined by the matrix $\mathbf{T}_{g,q}$ and the map $\mathcal{F}_{\mathbb{R},g}$ is defined by the matrix $\mathbf{T}_g$.*

*Proof.* We only prove for the map $\mathcal{F}_{\mathbb{Z}_q,g}$, since for the other maps the proof is similar. The $\mathbb{Z}_q$ vector spaces, $(\mathbb{Z}_q[X]/(f))^n$ and $\mathbb{Z}_q[X]/(f \circ g)$, have both dimension $mn$, since $f$ and $g$ are monic polynomials of degrees $m$ and $n$, respectively. The columns of the matrix defining $\mathcal{F}_{\mathbb{Z}_q,g}$ are given by the evaluations of this map at the vectors from the canonical basis $\{\mathbf{e}_i\}_{0\leq i\leq mn-1}$, where $\mathbf{e}_i = (0, 0, \ldots, 1, \ldots, 0)$ and its nonzero coordinate is the $i$th coordinate and equal to 1. Equivalently, if $i = mk + r$, for $0 \leq k \leq n-1$ and $0 \leq r \leq m-1$, evaluating at $\mathbf{e}_i$ is the same as evaluating at the polynomials $(c_0, c_1, \ldots, c_{n-1}) = (0, 0, \ldots, X^r, \ldots, 0)$, where $c_k = X^r$ and $c_j = 0$, for $j \neq k$. So $\mathcal{F}_{\mathbb{Z}_q,g}(0, 0, \ldots, X^r, \ldots, 0) = X^k c_k \circ g = X^k g^r$. Then the $(mk + r)$th column of the matrix we look for is the coefficient vector of the polynomial $X^k g^r \bmod q$, hence the $(mk + r)$th column of $\mathbf{T}_{g,q}$. □

**Lemma 3.2.** *The matrix $\mathbf{T}_{g,q}$ is invertible.*

*Proof.* Suppose there exist $A_{k,r} \in \mathbb{Z}_q$, where $0 \leq k \leq n-1$ and $0 \leq r \leq m-1$, such that

$$0 = \sum_{r=0}^{m-1} \sum_{k=0}^{n-1} A_{k,r} X^k g^r = \sum_{r=0}^{m-1} \left( \sum_{k=0}^{n-1} A_{k,r} X^k \right) g^r$$

Since $g$ is a monic polynomial of degree $n$, $g \bmod q$ is still a polynomial of degree $n$, in particular a nonzero polynomial. So we can use divisibility by $g \bmod q$ and get that $g | A_{0,0} + A_{1,0}X + \ldots + A_{n-1,0}X^{n-1}$. It follows that $A_{i,0} = 0$, for any $i$. Dividing by $g$, we get that

$$0 = \sum_{r=1}^{m-1} \left( \sum_{k=0}^{n-1} A_{k,r} X^k \right) g^{r-1}.$$

Inductively, we get all $A_{k,r}$'s are 0. Therefore the polynomials $1, g, \ldots, g^{m-1}$, $X, Xg, \ldots, Xg^{m-1}, \ldots, X^{n-1}, X^{n-1}g, \ldots, X^{n-1}g^{m-1}$ are linearly independent over $\mathbb{Z}_q$, so the matrix $\mathbf{T}_{g,q}$ is invertible. □

*Remark 3.3.* This result also holds if we consider that the leading coefficient of the polynomial $g$ is coprime with $q$.

Using these lemmas, we prove our main result in decision variant.

**Theorem 3.2.** *If $f$ and $g$ are monic polynomials in $\mathbb{Z}[X]$ of degrees $m$ and $n$, respectively, and $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}$ is hard given $k+n-1$ samples, then so is $\mathrm{PLWE}^{f\circ g}_{q,D_{\alpha q\sqrt{\mathbf{T}_g\mathbf{T}_g^t}}}$ given $k$ samples.*

*Proof.* Suppose $\mathcal{B}$ is an algorithm which distinguishes an $\mathrm{PLWE}^{f\circ g}_{q,D_{\alpha q\sqrt{\mathbf{T}_g\mathbf{T}_g^t}}}$ distribution from the uniform distribution over $\mathbb{Z}_q[X]/(f\circ g)\times\mathbb{R}_q[X]/(f\circ g)$. We construct an algorithm $\mathcal{A}$ which distinguishes an $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}$ distribution from the uniform distribution over $\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f)$. $\mathcal{A}$ uses a transformation $T$ which maps $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$ to $U(\mathbb{Z}_q[X]/(f\circ g)\times\mathbb{R}_q[X]/(f\circ g))$ and $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$, for a uniform $s$, to $\mathrm{PLWE}^{f\circ g}_{q,D_{\alpha q\sqrt{\mathbf{T}_g\mathbf{T}_g^t}}}(\tilde{s})$, where $\tilde{s}$ is also uniform and may depend on $s$. This mapping will be described below.

The distinguisher $\mathcal{A}$ draws $n-1$ samples $(a_i^*, b_i^*)$ from the unknown distribution, which may be either $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$, for $s\hookleftarrow\mathbb{Z}_q[X]/(f)$, or $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$. Then it picks $\tilde{s}_1,\tilde{s}_2,\ldots,\tilde{s}_{n-1}\hookleftarrow U(\mathbb{Z}_q[X]/(f))$. Now for any query $\mathcal{B}$ makes, $\mathcal{A}$ asks for a fresh sample $(a_j,b_j)$ from the same distribution, where $j\in[k]$, applies $T$ and gives to $\mathcal{B}$ the sample $(\tilde{a}_j,\tilde{b}_j)=T(a_j,b_j)$. When $\mathcal{B}$ ends, $\mathcal{A}$ returns its output.

Assuming $T$ satisfies the properties stated above, the reduction maps uniform samples to uniform samples and $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$ samples, for a uniform $s$, to $\mathrm{PLWE}^{f\circ g}_{q,D_{\alpha q\sqrt{\mathbf{T}_g\mathbf{T}_g^t}}}(\tilde{s})$ samples, for a uniform $\tilde{s}$ depending on $s$. So $\mathcal{A}$ will distinguish with the same probability as $\mathcal{B}$ does. We define $T$ as follows: $T:\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f)\to\mathbb{Z}_q[X]/(f\circ g)\times\mathbb{R}_q[X]/(f\circ g)$, $T(a_j,b_j)=(\tilde{a}_j,\tilde{b}_j)$, where

$$\tilde{a}_j=\mathcal{F}_{\mathbb{Z}_q,g}(a_j,a_1^*,\ldots,a_{n-1}^*) \tag{6}$$

$$\tilde{b}_j=\mathcal{F}_{\mathbb{R}_q,g}(b_j,b_1^*,\ldots,b_{n-1}^*)+\tilde{a}_j\sum_{i\in[n-1]}X^i\tilde{s}_i\circ g \tag{7}$$

Since $\mathcal{F}_{\mathbb{Z}_q,g}$ and $\mathcal{F}_{\mathbb{R}_q,g}$ are well defined, so is $T$.

We show that $T$ indeed maps $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$ to $U(\mathbb{Z}_q[X]/(f\circ g)\times\mathbb{R}_q[X]/(f\circ g))$ and $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}(s)$ to $\mathrm{PLWE}^{f\circ g}_{q,D_{\alpha q\sqrt{\mathbf{T}_g\mathbf{T}_g^t}}}(\tilde{s})$.

Suppose that $\{(a_j,b_j)\}_{j\in[k]}$ and $\{(a_i^*,b_i^*)\}_{i\in[n-1]}$ are drawn from the uniform distribution. By Lemma 3.2, the matrix $\mathbf{T}_{g,q}$ is invertible, hence

by Lemma 3.1 $\mathcal{F}_{\mathbb{Z}_q,g}$ and $\mathcal{F}_{\mathbb{R}_q,g}$ send uniform distribution to uniform distribution. So $(\tilde{a}_j, \tilde{b}_j)$ is also uniform.

Now suppose that the samples above are drawn from $\text{PLWE}^{f}_{q,D_{\alpha q}}(s)$, where $s \hookleftarrow U(\mathbb{Z}_q[X]/(f))$. Then

$$b_i^* = a_i^* \cdot s + e_i^* \in \mathbb{R}_q[X]/(f), \text{ for any } i \in [n-1] \tag{8}$$
$$b_j = a_j \cdot s + e_j \in \mathbb{R}_q[X]/(f), \text{ for any } j \in [k] \tag{9}$$

where $e_j, e_i^*$'s $\hookleftarrow D_{\alpha q}$ over $\mathbb{R}[X]/(f)$. Notice that:

$$b_i^* \circ g = a_i^* \circ g \cdot s \circ g + e_i^* \circ g \in \mathbb{R}_q[X]/(f \circ g), \text{ for any } i \in [n-1]$$
$$b_j \circ g = a_j \circ g \cdot s \circ g + e_j \circ g \in \mathbb{R}_q[X]/(f \circ g), \text{ for any } j \in [k]$$

Hence from equation (7) we obtain:

$$\begin{aligned}\tilde{b}_j &= b_j \circ g + \sum_{i\in[n-1]} X^i b_i^* \circ g + \tilde{a}_j \sum_{i\in[n-1]} X^i \tilde{s}_i \circ g = ((a_j \cdot s) \circ g + e_j \circ g) \\ &+ \sum_{i\in[n-1]} X^i \left(a_i^* \circ g \cdot s \circ g + e_i^* \circ g\right) + \tilde{a}_j \sum_{i\in[n-1]} X^i \tilde{s}_i \circ g \\ &= \left(a_j \circ g + \sum_{i\in[n-1]} X^i a_i^* \circ g\right) \cdot s \circ g + \left(e_j \circ g + \sum_{i\in[n-1]} X^i e_i^* \circ g\right) \\ &+ \tilde{a}_j \sum_{i\in[n-1]} X^i \tilde{s}_i \circ g = \tilde{a}_j \mathcal{F}_{\mathbb{Z}_q,g}(s, \tilde{s}_1, \ldots, \tilde{s}_{n-1}) + \mathcal{F}_{\mathbb{R},g}(e_j, e_1^*, \ldots, e_{n-1}^*)\end{aligned}$$

where for the second equality we used equations (8) and (9) and for the fourth one the equation (6). Denote by

$$\tilde{s} = \mathcal{F}_{\mathbb{Z}_q,g}(s, \tilde{s}_1, \tilde{s}_2, \ldots, \tilde{s}_{n-1}) \text{ and } \tilde{e}_j = \mathcal{F}_{\mathbb{R},g}(e_j, e_1^*, \ldots, e_{n-1}^*) \tag{10}$$

Notice that $\tilde{a}_j, \tilde{s} \hookleftarrow U(\mathbb{Z}_q[X]/(f \circ g))$ since $a_j, a_i^*$'s, $s, \tilde{s}_i$'s $\hookleftarrow U(\mathbb{Z}_q[X]/(f))$, by the action of $\mathcal{F}_{\mathbb{Z}_q,g}$, described in Lemma 3.1 and Lemma 3.2. Also, $e_j, e_i^*$'s $\hookleftarrow D_{\alpha q}$ over $\mathbb{R}^m$, so the concatenation $\bar{\mathbf{e}}$ of the vector coefficients of these polynomials has $mn$ independent coordinates which follow the Gaussian distribution $D_{\alpha q}$ over $\mathbb{R}$. Hence $\bar{\mathbf{e}} \hookleftarrow D_{\alpha q}$ over $\mathbb{R}^{mn}$. Therefore, by Lemma 3.1 $\tilde{e}_j = \mathcal{F}_{\mathbb{R},g}(\bar{\mathbf{e}}) = \mathbf{T}_g \bar{\mathbf{e}} \hookleftarrow D_{\alpha q \sqrt{\mathbf{T}_g \mathbf{T}_g^t}}$ over $\mathbb{R}^{mn}$. Hence, using equation (10) we get $\tilde{b}_j = \tilde{a}_j \cdot \tilde{s} + \tilde{e}_j$ in $\mathbb{R}_q[X]/(f \circ g)$. Therefore we obtain that $(\tilde{a}_j, \tilde{b}_j)$ is indeed a $\text{PLWE}^{f\circ g}_{q,D_{\alpha q \sqrt{\mathbf{T}_g \mathbf{T}_g^t}}}(\tilde{s})$ sample. □

*Remark 3.4.* As in Remark 3.3, this result also holds when considering $g$, not a monic polynomial, but a polynomial with its leading coefficient coprime with $q$.

*Remark 3.5.* Since the coefficients of $\tilde{e}_j$ from Theorem 3.1 are obtained from a permutation of coefficients of $e_j$, $e_1^*, \ldots, e_{n-1}^*$ as in equation (5), notice that the matrix $\mathbf{T}_{g_n}$ is a permutation matrix. Hence $\mathbf{T}_{g_n}\mathbf{T}_{g_n}^t = \mathbf{I}_{mn}$, so the error distribution of both problems from Theorem 3.1 is the same.

*Remark 3.6.* We mention that the reduction also works for search variants. Indeed if one algorithm $\mathcal{B}$ gets $\tilde{s}$ from $\mathrm{PLWE}_{q,D_{\alpha q}\sqrt{\mathbf{T}_g\mathbf{T}_g^t}}^{f\circ g}(\tilde{s})$ samples, then one can construct an algorithm $\mathcal{A}$ who gets $s$ from $\mathrm{PLWE}_{q,D_{\alpha q}}^{f}(s)$ samples using the same transformation as above, since it can get $\tilde{s}$ from $\mathcal{B}$ and therefore $s$, with the help of equation (10) and of the fact that $\mathcal{F}_{\mathbb{Z}_q,g}$ is an isomorphism of $\mathbb{Z}_q$ vector spaces.

## 4 Impact

Since the cyclotomic polynomials are well studied and used especially in designing cryptographic primitives, we are concerned about the impact of our result regarding the PLWE problems for cyclotomic polynomials.

Using Proposition 2.1 and Theorem 3.1, one can get the following corollaries:

**Corollary 4.1.** *For a positive integer $n$, if $\mathrm{PLWE}_{q,D_{\alpha q}}^{\phi_{\mathrm{rad}(n)}}$ is hard given $k + \frac{n}{\mathrm{rad}(n)} - 1$ samples, then so is $\mathrm{PLWE}_{q,D_{\alpha q}}^{\phi_n}$ given $k$ samples.*

**Corollary 4.2.** *For a prime $p$ and a power of $p$, $n$, if $\mathrm{PLWE}_{q,D_{\alpha q}}^{\phi_p}$ is hard given $k + \frac{n}{p} - 1$ samples, then so is $\mathrm{PLWE}_{q,D_{\alpha q}}^{\phi_n}$ given $k$ samples.*

By Theorem 3.2 we obtain the following corollaries which give an answer to what we were looking for, namely finding a polynomial for which its corresponding PLWE problem is at least as hard as many other PLWE problems. More exactly, in the first corollary we get that the $\mathrm{PLWE}^{\phi_n}$ problem is harder than the $\mathrm{PLWE}^{f}$ problem, for a minimal polynomial $f$ of an algebraic integer with specific properties in the cyclotomic field $\mathbb{Q}(\zeta_n)$. The second corollary generalizes the first one by showing that in the case of power-of-2 cyclotomic polynomials, the $\mathrm{PLWE}^{\phi_n}$ problem is harder than the $\mathrm{PLWE}^{f}$ problem for all the minimal polynomials $f$ of algebraic integers in $\mathbb{Q}(\zeta_n)$ with weaker conditions than those from the previous corollary.

**Corollary 4.3.** *Let $\beta$ be an algebraic integer in the $n$th cyclotomic field $\mathbb{Q}(\zeta_n)$, whose minimal polynomial over $\mathbb{Q}$ is $f_\beta \in \mathbb{Z}[X]$ of degree $m$. Suppose that $\beta = g_\beta(\zeta_n)$, for some $g_\beta \in \mathbb{Z}[X]$ of degree $r$, and $\phi_n = f_\beta \circ g_\beta$.*

*Then if* $\mathrm{PLWE}^{f_\beta}_{q,D_{\alpha q}}$ *is hard given* $k+r-1$ *samples, then* $\mathrm{PLWE}^{\phi_n}_{q,D_{\alpha q\sqrt{\mathbf{T}_{g_\beta}\mathbf{T}^t_{g_\beta}}}}$ *is hard given* $k$ *samples, where* $\mathbf{T}_{g_\beta}$ *is considered as an* $mr \times mr$ *matrix.*

Since $\beta$ is an algebraic integer from $\mathbb{Q}(\zeta_n)$, it belongs to $\mathbb{Z}[\zeta_n]$, so indeed it exists a polynomial $g_\beta \in \mathbb{Z}[X]$ of degree $r$ less than $\varphi(n)$ such that $\beta = g_\beta(\zeta_n)$.

We show now that indeed there exist algebraic integers $\beta$ with the property that $f_\beta \circ g_\beta = \phi_n$: suppose $n = 2^t$. Then $\phi_n(X) = X^{2^{t-1}} + 1$. Consider $\beta = \zeta_n^{2^k} = \zeta_{2^{t-k}}$, for $0 \leq k \leq t$. Then $f_\beta = \phi_{2^{t-k}}$ and $g_\beta = X^{2^k}$. It is easy to see that $\phi_{2^t}(X) = \phi_{2^{t-k}}(X^{2^k})$, hence $\phi_n = f_\beta \circ g_\beta$.

Notice that for $\beta = \zeta_n^{2^k}$, its corresponding $\mathbf{T}_{g_\beta}$ is an $mr \times mr$ matrix where $m = 2^{t-k-1}$ and $r = 2^k$. This matrix has as columns the coefficient vectors of the polynomials

$$1, X^{2^k}, \ldots, X^{2^{t-1}-2^k}, X, X^{1+2^k}, \ldots, X^{2^{t-1}-2^k+1}, \ldots, X^{2^k-1}, \ldots, X^{2^{t-1}-1}.$$

Hence, the matrix $\mathbf{T}_{g_\beta}$ has as column vectors unit vectors. Therefore its Frobenius norm is $\|\mathbf{T}_{g_\beta}\|_F = \sqrt{mr} = 2^{(t-1)/2}$.

We prove now that for a power-of-2 cyclotomic polynomial $\phi_n$, $\mathrm{PLWE}^{\phi_n}$ is at least as hard as $\mathrm{PLWE}^f$ for minimal polynomials $f$ of algebraic integers in the $n$th cyclotomic field $\mathbb{Q}(\zeta_n)$ with weaker conditions as in Corollary 4.3. Notice that the polynomial $g_\beta$ from the same corollary must be monic since $\phi_n = f_\beta \circ g_\beta$ and $\phi_n$ and $f_\beta$ are monic polynomials.

From now on, we consider $\phi_n$ as a power-of-2 cyclotomic polynomial, which is of the form $\phi_n(X) = X^{2^{t-1}} + 1$, for $n = 2^t$. Before proving the result stated previously, we make use of the following notations and lemmas.

For a positive integer $d$ greater than $2^{t-1}$, we consider the matrix $\mathbf{A} \in \mathbb{Z}^{2^{t-1} \times d}$, where for any $1 \leq i \leq 2^{t-1}$ and $1 \leq j \leq d$, the entry $\mathbf{A}_{i,j}$ is $(-1)^k$, if $j = 2^{t-1}k + i$, for $0 \leq k \leq \lfloor \frac{d}{2^{t-1}} \rfloor$, and 0 else. For instance, if $d$ is equal to $2^{t-1}$, the matrix $\mathbf{A}$ is just the $2^{t-1} \times 2^{t-1}$ identity matrix $\mathbf{I}_{2^{t-1}}$. If $d$ is a multiple of $2^{t-1}$, then $\mathbf{A}$ is of the form $\left(\mathbf{I}_{2^{t-1}} - \mathbf{I}_{2^{t-1}} \ldots (-1)^c \mathbf{I}_{2^{t-1}}\right)$, where $c = \frac{d}{2^{t-1}} - 1$. Notice that since its columns are all unit vectors, it follows that $\|\mathbf{A}\|_F = \sqrt{d}$.

For a polynomial $f \in \mathbb{Z}[X]$ of degree $d$ such that $\phi_n$ divides $f$ and a ring $R$ being either $\mathbb{Z}_q$, $\mathbb{R}_q$ or $\mathbb{R}$, we consider the maps:

$$T_{R,f} : R[X]/(f) \to R[X]/(\phi_n),\ T_f(g) = g \bmod \phi_n.$$

Firstly, notice that this map is well defined. Indeed, since if $a \equiv \bar{a} \bmod f$, then $f|a - \bar{a}$, and therefore $\phi_n|a - \bar{a}$. Secondly, if we consider the input polynomial as its coefficient vector, $T_{R,f}$ is an $R$ linear map. Moreover, the following lemma tells us how it acts:

**Lemma 4.1.** *$T_{R,f}$ is an $R$ linear map defined by the $2^{t-1} \times d$ matrix $\mathbf{A}$, where $d$ is the degree of $f$.*

*Proof.* Consider $d - 1 = 2^{t-1} \cdot c + r$, where $0 \leq r \leq 2^{t-1} - 1$. Notice that $X^{2^{t-1}} \equiv -1 \bmod \phi_n$. Hence, $X^{2^{t-1}k+i} \equiv \left(X^{2^{t-1}}\right)^k X^i \equiv (-1)^k X^i \bmod \phi_n$. So $T_{R,f}(X^{2^{t-1}k+i}) = (-1)^k X^i$. Using the linearity of $T_{R,f}$, we obtain for a polynomial $e$ in $R[X]/(f)$ the following:

$$\begin{aligned} T_{R,f}(e) &= \sum_{i=0}^{r}\sum_{k=0}^{c} T_{R,f}(e_{2^{t-1}k+i}X^{2^{t-1}k+i}) + \sum_{i=r+1}^{2^{t-1}-1}\sum_{k=0}^{c-1} T_{R,f}(e_{2^{t-1}k+i}X^{2^{t-1}k+i}) \\ &= \sum_{i=0}^{r}\sum_{k=0}^{c}(-1)^k e_{2^{t-1}k+i}X^i + \sum_{i=r+1}^{2^{t-1}}\sum_{k=0}^{c-1}(-1)^k e_{2^{t-1}k+i}X^i \end{aligned}$$

Therefore the $i$th coefficient of $T_{R,f}(e)$ is $\sum_{k=0}^{c}(-1)^k e_{2^{t-1}k+i}$, if $0 \leq i \leq r$, and $\sum_{k=0}^{c-1}(-1)^k e_{2^{t-1}k+i}$, if $r+1 \leq i \leq 2^{t-1} - 1$. We can easily notice that the coefficient vector of $T_{R,f}$ coincides with the vector $\mathbf{Ae}$, where $\mathbf{e}$ is the coefficient vector of the polynomial $e$. □

By Remark 2.1 we obtain that $\mathrm{PLWE}^{\phi_n}$ is at least as hard as $\mathrm{PLWE}^{f}$ for any multiple $f$ of $\phi_n$. In the next proposition we explore in more detail this reduction in decision variant. This result will be useful in proving our stated corollary.

**Proposition 4.1.** *For a polynomial $f \in \mathbb{Z}[X]$ of degree $d$ such that $\phi_n$ divides $f$, if $\mathrm{PLWE}^{f}_{q,D_{\sqrt{\mathbf{\Sigma}}}}$ is hard given $k$ samples, then $\mathrm{PLWE}^{\phi_n}_{q,D_{\sqrt{\mathbf{A\Sigma A}^t}}}$ is hard given $k$ samples.*

*Proof.* Consider $\mathcal{B}$ an algorithm which distinguishes an $\mathrm{PLWE}^{\phi_n}_{q,D_{\sqrt{\mathbf{A\Sigma A}^t}}}$ distribution from the uniform distribution over $\mathbb{Z}_q[X]/(\phi_n) \times \mathbb{R}_q[X]/(\phi_n)$. We construct an algorithm $\mathcal{A}$ which distinguishes an $\mathrm{PLWE}^{f}_{q,D_{\sqrt{\mathbf{\Sigma}}}}$ distribution from the uniform distribution over $\mathbb{Z}_q[X]/(f) \times \mathbb{R}_q[X]/(f)$. $\mathcal{A}$ uses a

map $T$ which sends $U(\mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f))$ samples to $U(\mathbb{Z}_q[X]/(\phi_n)\times\mathbb{R}_q[X]/(\phi_n))$ samples and $\mathrm{PLWE}^f_{q,D_{\sqrt{\mathbf{\Sigma}}}}(s)$ samples, for a uniform $s$, to $\mathrm{PLWE}^{\phi_n}_{q,D_{\sqrt{\mathbf{A\Sigma A}^t}}}(\tilde{s})$ samples, for a uniform $\tilde{s}$ which depends on $s$.

More precisely, for any query $\mathcal{B}$ makes, $\mathcal{A}$ asks for a sample $(a_i, b_i)$, where $i \in [k]$, from the unknown distribution, which may be either $\mathrm{PLWE}^f_{q,D_{\sqrt{\Sigma}}}(s)$, for a uniform $s$, or $U(\mathbb{Z}_q[X]/(f) \times \mathbb{R}_q[X]/(f))$. Then it applies the transformation $T$ and gives to $\mathcal{B}$ the pair $(\tilde{a}_i, \tilde{b}_i) = T(a_i, b_i)$. When $\mathcal{B}$ ends, $\mathcal{A}$ outputs its return.

If $T$ satisfies the properties stated previously, the reduction indeed maps uniform samples to uniform samples and $\mathrm{PLWE}^f_{q,D_{\sqrt{\mathbf{\Sigma}}}}(s)$ samples, for a uniform $s$, to $\mathrm{PLWE}^{\phi_n}_{q,D_{\sqrt{\mathbf{A\Sigma A}^t}}}(\tilde{s})$ samples, for a uniform $\tilde{s}$ depending on $s$. Therefore, $\mathcal{A}$ will distinguish with the same probability as $\mathcal{B}$ does.

Now we define the map $T$ and prove its properties:

$$T : \mathbb{Z}_q[X]/(f)\times\mathbb{R}_q[X]/(f) \to \mathbb{Z}_q[X]/(\phi_n)\times\mathbb{R}_q[X]/(\phi_n), T = (T_{\mathbb{Z}_q,f}, T_{\mathbb{R}_q,f}).$$

Notice that since $T_{\mathbb{Z}_q,f}$ and $T_{\mathbb{R}_q,f}$ are well defined, so is $T$.

It is clearly that if the samples $\{(a_i, b_i)\}_{i\in[k]}$ are uniform, then their coefficients are also uniform. By the actions of $T_{\mathbb{Z}_q,f}$ and $T_{\mathbb{R}_q,f}$ explained in Lemma 4.1, the coefficients of $T_{\mathbb{Z}_q,f}(a_i)$ and $T_{\mathbb{R}_q,f}(b_i)$ are also uniform. Therefore the samples $\{(\tilde{a}_i, \tilde{b}_i)\}_{i\in[k]}$ are uniform.

If the samples $\{(a_i, b_i)\}_{i\in[k]}$ are $\mathrm{PLWE}^f_{q,D_{\sqrt{\mathbf{\Sigma}}}}(s)$ samples, for a uniform $s$, then $(a_i, b_i) = (a_i, a_i \cdot s + e_i)$, where $e_i \hookleftarrow D_{\sqrt{\mathbf{\Sigma}}}$ over $\mathbb{R}^d$, for any $i \in [k]$. Hence

$$\begin{aligned}(\tilde{a}_i, \tilde{b}_i) &= (a_i \bmod \phi_n, a_i \bmod \phi_n \cdot s \bmod \phi_n + e_i \bmod \phi_n)\\ &= (T_{\mathbb{Z}_q,f}(a_i), T_{\mathbb{Z}_q,f}(a_i) \cdot T_{\mathbb{Z}_q,f}(s) + T_{\mathbb{R},f}(e_i)).\end{aligned}$$

Notice that due to the action of $T_{\mathbb{Z}_q,f}$ described in Lemma 4.1, $a_i \bmod \phi_n$ and $\tilde{s} = s \bmod \phi_n$ are uniform since $a_i$ and $s$ are uniform. Moreover, according to Lemma 4.1, $e_i \bmod \phi_n$ can be considered as the vector $\mathbf{A}\mathbf{e}_i$, where $\mathbf{e}_i$ is the coefficient vector of the polynomial $e_i$. Since $\mathbf{e}_i$ is drawn from the Gaussian distribution $D_{\sqrt{\mathbf{\Sigma}}}$, the distribution of $e_i \bmod \phi_n$ is the Gaussian distribution $D_{\sqrt{\mathbf{A\Sigma A}^t}}$. Therefore $(\tilde{a}_i, \tilde{b}_i)$ is a $\mathrm{PLWE}^{\phi_n}_{q,D_{\sqrt{\mathbf{A\Sigma A}^t}}}(\tilde{s})$ sample, where $\tilde{s} = T_{\mathbb{Z}_q,f}(s)$. □

Using the preliminaries above, we can prove now that for a power-of-2 cyclotomic polynomial $\phi_n$, $\mathrm{PLWE}^{\phi_n}$ is harder than $\mathrm{PLWE}^f$, for a minimal polynomial $f$ of an algebraic integer with a weaker condition as in Corollary 4.3, from $\mathbb{Q}(\zeta_n)$.

**Corollary 4.4.** *Consider $\beta$ an algebraic integer in the nth cyclotomic field $\mathbb{Q}(\zeta_n)$. Let $f_\beta \in \mathbb{Z}[X]$ be its minimal polynomial over $\mathbb{Q}$ of degree $m$. Suppose that $\beta = g_\beta(\zeta_n)$, for some polynomial $g_\beta$ in $\mathbb{Z}[X]$ of degree $s$, and $g_\beta$ is monic. Then if $\mathrm{PLWE}^{f}_{q,D_{\alpha q}}$ is hard given $k + ms - 1$ samples, then $\mathrm{PLWE}^{\phi_n}_{D_{q,\alpha q\sqrt{\mathbf{G}\mathbf{G}^t}}}$ is hard given $k$ samples, where $\mathbf{G}$ is a matrix from $\mathbb{Z}^{2^{t-1}\times ms}$ depending on $\beta$.*

*Proof.* Since $\beta$ is an algebraic integer in $\mathbb{Q}(\zeta_n)$, it belongs to $\mathbb{Z}[\zeta_n]$. Hence it exists and it is unique a polynomial $g_\beta$ in $\mathbb{Z}[X]$ of degree $s$ less than $\varphi(n)$ such that $\beta = g_\beta(\zeta_n)$. By assumption, this polynomial, $g_\beta$, is monic. Denote by $d$ the degree of $f_\beta \circ g_\beta$, which is equal to $ms$.

Since $f_\beta$ is the minimal polynomial of $\beta$, $0 = f_\beta(\beta) = f_\beta(g_\beta(\zeta_n))$. Moreover, since $\phi_n$ is the minimal polynomial of $\zeta_n$, $\phi_n | f_\beta \circ g_\beta$ in $\mathbb{Z}[X]$. By Theorem 3.2, there is a reduction from $\mathrm{PLWE}^{f_\beta}_{q,D_{\alpha q}}$ to $\mathrm{PLWE}^{f_\beta\circ g_\beta}_{q,D_{\alpha q\sqrt{\mathbf{T}_{g_\beta}\mathbf{T}_{g_\beta}^t}}}$, where $\mathbf{T}_{g_\beta}$ is considered as the $d\times d$ matrix. Moreover, by Proposition 4.1, there is a reduction from $\mathrm{PLWE}^{f_\beta\circ g_\beta}_{q,D_{\alpha q\sqrt{\mathbf{T}_{g_\beta}\mathbf{T}_{g_\beta}^t}}}$ to $\mathrm{PLWE}^{\phi_n}_{q,D_{\alpha q\sqrt{\mathbf{A}\mathbf{T}_{g_\beta}\mathbf{T}_{g_\beta}^t\mathbf{A}^t}}}$, where $\mathbf{A}$ is the $2^{t-1}\times d$ matrix described earlier. By letting the matrix $\mathbf{G}$ be $\mathbf{A}\mathbf{T}_{g_\beta}$, the conclusion follows easily. □

*Remark 4.1.* As in Remark 3.3, this corollary also holds for algebraic integers $\beta$ for which their corresponding polynomials $g_\beta$ have their leading coefficients coprime with $q$.

## 5 Open problems

It would be interesting to have a complete characterization of the algebraic integers which have the property stated in Corollary 4.3. Also, since we are concerned about the reductions which give limited noise growth, it would be an interesting question to ask for which such an algebraic integer $\beta$ in the $n$th cyclotomic field its corresponding $\mathbf{T}_{g_\beta}$ matrix has small norm. Moreover, taking into consideration Corollary 4.4, we would also be interested in finding algebraic integers $\beta$ from the $n$th cyclotomic field for which their corresponding matrices $\mathbf{A}\mathbf{T}_{g_\beta}$ have small norm. Another open problem would be to see if Corollary 4.4 holds for any other positive integers $n$ besides the powers of 2. Another interesting problem would be to find a polynomial for which its corresponding PLWE problem is harder than all the other PLWE problems.

**Acknowledgments.** We thank Miruna Rosca and Radu Titiu for helpful discussions. Finally, we thank the anonymous reviewers for comments.

## References

[ABB10] S. Agrawal, D. Boneh, and X. Boyen. Efficient lattice (H)IBE in the standard model. In *Proc. of Eurocrypt'10*, volume 6110 of *LNCS*, pages 553–572, 2010.

[ADPS16] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. Post-quantum key exchange - a new hope. In *USENIX*, page 327343, 2016.

[BGV11] Z. Brakerski, C. Gentry, and V. Vaikuntanathan. Fully homomorphic encryption without bootstrapping. *Cryptology ePrint Archive, Report 2011/277*, 2011.

[BP14] A. Banerjee and C. Peikert. New and improved key-homomorphic pseudorandom functions. In *CRYPTO*, 2014.

[BV11] Z. Brakerski and V. Vaikuntanathan. Fully homomorphic encryption from ring lwe and security for key dependent messages. In *CRYPTO*, 2011.

[CDPR16] R. Cramer, L. Ducas, C. Peikert, and O. Regev. Recovering short generators of principal ideals in cyclotomic rings. In *EUROCRYPT*, 2016.

[CDW17] R. Cramer, L. Ducas, and B. Wesolowski. Short Stickelberger class relations and application to Ideal-SVP. In *EUROCRYPT*, 2017.

[CLS15] H. Chen, K. Lauter, and K. E. Stange. Attacks on search RLWE. 2015. To appear in SIAM Journal on Applied Algebra and Geometry (SIAGA).

[EHL14] K. Eisenträger, S. Hallgren, and K. Lauter. Weak instances of PLWE. In *SAC*, 2014.

[Gen09] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proc. of STOC*, pages 169–178. ACM, 2009.

[GHPS12] C. Gentry, S. Halevi, C. Peikert, and N. P. Smart. Ring switching in BGV-style homomorphic encryption. In *SCN*, 2012.

[GSW13] C. Gentry, A. Sahai, and B. Waters. Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. Cryptology ePrint Archive, Report 2013/340, 2013. `https://eprint.iacr.org/2013/340`.

[GVW15] S. Gorbunov, V. Vaikuntanathan, and H. Wee. Predicate encryption for circuits from lwe. Cryptology ePrint Archive, Report 2015/029, 2015. `https://eprint.iacr.org/2015/029`.

[LPR10] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *JACM, 2013*, 60(6):43, 2010.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. A toolkit for Ring-LWE cryptography. In *EUROCRYPT*, 2013.

[PRSD17] C. Peikert, O. Regev, and N. Stephens-Davidowitz. Pseudorandomness of Ring-LWE for any ring and modulus. In *STOC*, 2017.

[Reg05] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proc. of STOC*, pages 84–93, 2005.

[RSSS17] M. Rosca, A. Sakzad, D. Stehlé, and R. Steinfeld. Middle-product learning with errors. In *CRYPTO*, 2017.

[RSW18] M. Rosca, D. Stehlé, and A. Wallet. On the ring-lwe and polynomial-lwe problems. In *EUROCRYPT*, 2018.

[SE94] C.-P. Schnorr and M. Euchner. Lattice basis reduction: Improved practical algorithms and solving subset sum problems. *Math. Program.*, 66:181–199, 1994.

[SSTX09] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa. Efficient public key encryption based on ideal lattices. In *ASIACRYPT*, 2009.

[SSZ17] R. Steinfeld, A. Sakzad, and R. K. Zhao. Proposal for a NIST Post-Quantum Public-key Encryption and KEM Standard, 2017. `http://users.monash.edu.au/~rste/Titanium_NISTSub.pdf`.