RLWE/PLWE EQUIVALENCE FOR THE MAXIMAL TOTALLY REAL SUBEXTENSION OF THE $2^{pq}$-TH CYCLOTOmic FIELD.

IVÁN BLANCO CHACÓN AND LORENA LÓPEZ-HERNANZ

1. INTRODUCTION

Lattice-based cryptography is one of the most efficient alternatives for the standardisation of postquantum cryptography. Indeed, the majority of surviving proposals in the third round of the NIST public contest belongs to this category. Its strengths are, first, the ease to implement, and second, the fact that no attack has been found (apart from some weak instances of parameters which can be avoided) which significantly outperforms brute force. Moreover, several theoretical results seem to support a provable hardness guarantee. These results consist on the reduction of several versions of the Shortest Vector Problem for lattices to two of the problems which back lattice-based cryptography: the Learning With Errors Problem (where the reduction comes from the class of general lattices) and the Ring Learning With Errors Problem (where the reduction comes from the subclass of ideal lattices). Despite the fact that the hardness of the precise lattice problems which reduce to the mentioned cryptographic problems has not been established yet, a promising number of hits has been reached, at least in the category of general lattices ([13], [10]). Other feature which makes lattice-based primitives preferable to other approaches is the required size of the secret and public keys to ensure a given security level, far below multivariate-based and code-based contenders. The reader is referred to https://www.safecrypto.eu/pqclounge/ for a detailed description of the remaining proposals and the history of the contest along all the rounds.

Within lattice-based cryptography, the Learning With Errors Problem (LWE from now on), the Ring Learning With Errors Problem (RLWE from now on) and the Polynomial Learning With Errors Problem (PLWE from now on) hold a prominent position. The first was introduced in [15], the second in [12] and the third in [18]. In general, PLWE is more suitable for implementations due to the very efficient arithmetic algorithms available for polynomial rings while the majority of security reduction proofs have been established for RLWE. Moreover, at the time of writing and apart from [5] and those against sheer LWE, there are no direct attacks against RLWE, while a number of theoretical attacks have been produced against PLWE under some general assumptions (see, for instance [8], [14]). Hence, it seems natural to ask for the relation and mutual dependence of RLWE and PLWE and this is the goal of the present article, which is an extension of [3] and answers a question raised therein by the first author.

First author partially supported by MTM2016-79400-P, CCG20/IA-057, CM/JIN/2019-031 and PID2019-104855RB-00/ AEI/10.13039/501100011033.; second author, by PID2019-105621 GB-I00.
In [16], the authors develop the notion of equivalence between RLWE and PLWE in their several versions; namely, both problems are said to be equivalent if there exists an algorithm which transforms admissible RLWE-samples into admissible PLWE-samples and vice versa with a complexity of polynomial order in the rank of the lattice (i.e. the degree of the underlying number field). The word admissible means that the algorithm must make the error distribution to incur at most in a distortion which, again, is polynomial in the rank of the lattice. Moreover, the authors justify why the right measure of this distortion is the condition number of the matrix defining the lattice transformation and study the equivalence for an ad hoc family of polynomials.

The usual (and natural) lattice transformation in [16] is nothing else but left multiplication by a Vandermonde matrix attached to the Galois conjugates of a primitive element of the underlying number field and Vandermonde matrices tend to be very ill-conditioned apart from some ad hoc cases. In the cyclotomic scenario, which is the most dealt with in practical cryptographic primitives, the problem is now reasonably well understood (cf. [6], [2], [17]).

However, a seek for more flexibility, as justified in [14] and in [16], calls for a good understanding of both problems in more general number fields. To our knowledge, the first study of RLWE/PLWE equivalence for a family of non-cyclotomic number fields apart from [16] is [3]. In that work, the first author establishes the RLWE/PLWE equivalence for the maximal totally real subextension of the cyclotomic field \( \mathbb{Q}(\zeta_{4p}) \) (with \( p \) arbitrary prime) and justifies why the approach based on the evaluation map at an integral primitive element is deemed to fail due to an exponential lower bound for the condition number of the Vandermonde matrix with real symmetric nodes due to Gautschi [9]). The main contribution of [3] is the replacement of the Vandermonde matrix by a quasi-Vandermonde matrix attached to the family of Tchebycheff polynomials up to degree \( p - 1 \) and the roots of the \( p \)-th Tchebycheff polynomials. These matrices are known to be optimally conditioned and to present a good number of amenable properties due to the orthogonality of the Tchebycheff family.

In the present article we generalize the main result of [3]. Namely, we will prove the following result:

**Theorem 1.1.** Let \( p \) and \( q \) be different odd prime numbers and let \( r \geq 2 \). For \( k = 1 \), \( k = p \) and \( k = pq \), the RLWE and the PLWE problems are equivalent for the maximal totally real subextension of the \( 2^r k \)-th cyclotomic field.

We have structured our presentation in four sections in the following manner:

Section 2 is a summary of algebraic generalities and notations whose aim is to make our article self-contained. Section 3 recalls the RLWE and PLWE problems and the formal definition of equivalence and provides a summary of previous results on the equivalence of the R/P-LWE Problems. Subsection 3.4 points out an advantage of using the family \( K_{2^r k} \) (the totally real subextension of the \( 2^r k \)-th cyclotomic field) from a cryptoanalytical point of view: we prove that this family is immune against one of the attacks described in [8], whereas cyclotomic fields are not (or at least not in a provable manner).
Section 4 is the core of the paper and proves Theorem 1.1. The main ingredient is the analysis of how the condition number behaves under several elementary operations performed in a quasi-Vandermonde matrix attached to the Galois-conjugates of the natural primitive element of the extension.

We thank our colleague Raúl Durán for a careful reading and discussion of our work and for providing us with Example 3.7.

## 2. Algebraic setup

**Definition 2.1.** A lattice is a pair \((\Lambda, \phi)\) where \(\Lambda\) is a finitely generated and torsion-free abelian group and \(\phi : \Lambda \rightarrow \mathbb{R}^N\) is a group monomorphism for some \(N\). When \(N\) equals the rank of \(\Lambda\) we will say that \(\Lambda\) has full rank. All our lattices will be full rank unless stated otherwise.

### 2.1. Number fields and ideal lattices.

For any field extension \(L/F\), \(\text{Gal}(L/F)\) denotes the Galois group of the extension, i.e. the group of field automorphisms of \(L\) which fix \(F\).

Let \(K = \mathbb{Q}(\theta)\) be an algebraic number field of degree \(n\) and let \(f(x) \in \mathbb{Q}[x]\) be the minimal polynomial of \(\theta\). In particular, \(K\) is a \(\mathbb{Q}\)-vector space of dimension \(n\) and the set \(\{1, \theta, ..., \theta^{n-1}\}\) is a \(\mathbb{Q}\)-basis. The evaluation-at-\(\theta\) map is a field \(\mathbb{Q}\)-isomorphism \(\mathbb{Q}[x]/(f(x)) \cong K\).

The field \(K\) is furnished with \(n\) field \(\mathbb{Q}\)-embeddings \(\sigma_i : K \rightarrow \overline{\mathbb{Q}}\), with \(1 \leq i \leq n\) and \(\overline{\mathbb{Q}}\) a fixed algebraic closure of \(\mathbb{Q}\). Each of these morphisms is fully determined by its image at \(\theta\), namely \(\sigma_i(\theta) = \theta_i\), where \(\{\theta_1 := \theta, \theta_2, ..., \theta_n\}\) are the roots of \(f\) (namely, the Galois conjugates of \(\theta\)).

The extension \(K/\mathbb{Q}\) (or just the field \(K\)) is said to be Galois if \(K\) is the splitting field of \(f\). This is equivalent to saying that the embeddings \(\sigma_i\) are indeed automorphisms of \(K\), hence \(\text{Gal}(K/\mathbb{Q}) = \{\sigma_1 = \text{Id}, \sigma_2, ..., \sigma_n\}\).

Setting \(s_1\) as the number of real embeddings, i.e. those whose image is contained in \(\mathbb{R}\), and \(s_2\) as the number of complex non-real embeddings, one has \(n = s_1 + 2s_2\).

**Definition 2.2.** The canonical embedding \(\sigma_K : K \rightarrow \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2}\) is defined as:

\[
\sigma_K(x) := (\sigma_1(x), ..., \sigma_n(x)).
\]

The field \(K\) is said to be totally real in case \(s_2 = 0\). When \(K\) is clear from the context we will simply write \(\sigma\) instead of \(\sigma_K\).

Recall that an algebraic integer is an element of \(\overline{\mathbb{Q}}\) whose minimal polynomial belongs to \(\mathbb{Z}[x]\). The set \(\mathcal{O}_K\) of algebraic integers in \(K\) is a ring: the ring of integers of \(K\).

It is also well known (see for instance [19]) that \(\mathcal{O}_K\) is a free \(\mathbb{Z}\)-module of rank \(n\), thus for each ideal \(I \subseteq \mathcal{O}_K\) its image \(\sigma(I)\) is a lattice in the space

\[
\Lambda_n := \{(x_1, ..., x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} : x_{s_1+i} = \overline{x}_{s_1+s_2+i} \text{ for } 1 \leq i \leq s_2\}.
\]
Notice that when $K$ is totally real we have $\Lambda_n = \mathbb{R}^n$.

**Definition 2.3.** A lattice $(\Lambda, \phi)$ is said to be an ideal lattice if there exists a number field $K$ and an ideal $I \subseteq \mathcal{O}_K$ such that $\sigma(I) = \phi(\Lambda)$.

Of great relevance in cryptography is the obvious observation that every ideal lattice is endowed with an extra ring structure inherited from that in $\mathcal{O}_K$.

**Definition 2.4.** The field $K$ is said to be monogenic if $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in K$. We will assume that all our fields are monogenic.

The canonical embedding is one of the two main characters in our story, whose interplay is the object of our study. The second character is presented next:

**Definition 2.5.** The coordinate embedding of $\mathcal{O}_K$ is

$$\sigma_{C,K} : \mathcal{O}_K = \mathbb{Z}[\theta] \to \mathbb{R}^n$$

$$a_0 + a_1\theta + ... + a_{n-1}\theta^{n-1} \mapsto (a_0, a_1, ..., a_{n-1})$$

When $K$ is clear from the context we will write $\sigma_C$ instead of $\sigma_{C,K}$. It is worthwhile to mention that multiplication and addition are preserved component-wise by the canonical embedding while, in general, only addition is respected by the coordinate embedding.

### 2.2. The cyclotomic field and its maximal totally real subextension.

For an integer $n > 1$ denote by $\mathbb{Z}_n^*$ the group of multiplicative units in the ring $\mathbb{Z}_n$. The set of primitive $n$-th roots of unity (those of the form $\zeta_k = \exp(2\pi ik/n)$ with $(k, n) = 1$) is a multiplicative group of order $m = \phi(n)$, where $\phi$ stands for Euler’s totient function. The $n$-th cyclotomic polynomial is

$$\Phi_n(x) = \prod_{k \in \mathbb{Z}_n^*} (x - \zeta_k)$$

This polynomial is irreducible in $\mathbb{Z}[x]$ and setting $\zeta = \zeta_k$ for any $k \in \mathbb{Z}_n^*$, the number field $K_n = \mathbb{Q}(\zeta)$ is the splitting field of $\Phi_n(x)$, hence it is Galois of degree $m$. In this paper we study the maximal totally real subextension of $K_n$, denoted $K_n^+$, whose degree is $\phi(n)/2$. As $K_n$, the field $K_n^+$ is Galois and monogenic (see [20, Chapter 2]), namely:

$$\mathcal{O}_{K_n^+} = \mathbb{Z}[\psi_k],$$

with $\psi_k = \zeta_k^n + \zeta_n^{-k} = 2 \cos\left(\frac{2\pi k}{n}\right)$ for each $k \in \mathbb{Z}_n^*/\{\pm 1\}$. We denote by $\Phi_n^+$ the minimal polynomial of $\psi_k$.

### 3. The R/P-LWE problems and the notion of equivalence

With the same notations as before, denote $\mathcal{O} = \mathbb{Z}[x]/(f(x))$, where $f(x)$ is the minimal polynomial of an integer element $\theta$. As seen in the previous section, the ring $\mathcal{O}$ has a lattice structure in $\mathbb{R}^m$, where $m$ is the degree of $f$, via the coordinate embedding.
Definition 3.1 (The search RLWE/PLWE problem). Let \( q = r(n) \) be a prime, with \( r[x] \in \mathbb{R}[x] \), let \( \chi \) be a discrete Gaussian distribution (cf. [12, Section 2.2]) with values in \( \mathcal{O}_K/q\mathcal{O}_K \) (resp. in \( \mathcal{O}/q\mathcal{O} \)). The RLWE (resp. PLWE) problem for \( \chi \) is stated as follows:

For a secret element \( s \in \mathcal{O}_K/q\mathcal{O}_K \) (resp. \( \mathcal{O}/q\mathcal{O} \)) chosen uniformly at random, if an adversary for whom \( s \) is unknown is given access to arbitrarily many samples \( \{(a_i, a_is + \epsilon_i)\}_{i \geq 1} \) of the RLWE (resp. PLWE) distribution, where for each \( i \geq 1 \), \( a_i \) is uniformly chosen at random and \( \epsilon_i \) is sampled from \( \chi \), this adversary is asked to guess \( s \) with non-negligible advantage.

From now on, by RLWE/PLWE problem we will refer to the search RLWE/PLWE problem. It is a very natural question to wonder what is the relation between the RLWE and the PLWE problems, what we discuss next.

3.1. The condition number. In [16], the authors define the notion of equivalence between RLWE and PLWE. In [2] this equivalence is proved for cyclotomic fields under the hypothesis of fixing (or upper bounding) the number of prime divisors of the conductor, and in [3] we have proved the equivalence for the maximal totally real subextension \( K_{4p}^+ \) of the cyclotomic field \( K_4 \), for \( p \) arbitrary prime.

Definition 3.2. For a monogenic Galois number field \( \mathbb{K} = \mathbb{Q}(\theta) \) of degree \( n \geq 2 \), the problems RLWE and PLWE are said to be equivalent if each one of them reduces to the other one in polynomial time and with a polynomial noise increase. This means that there exists an algorithm which transfers RLWE-samples into PLWE-samples (and vice versa) with complexity \( O(n^r) \) with \( r \) independent of \( n \) and this algorithm amplifies the noise by a factor which is also polynomial in \( n \).

As before, let \( f(x) \in \mathbb{Z}[x] \) denote the minimal polynomial of \( \theta \) and \( \theta_1 := \theta, \theta_2, \ldots, \theta_n \) the Galois conjugates of \( \theta \). The evaluation-at-\( \theta \) map \( V_f \) transforms the lattice \( (\mathcal{O}, \sigma_C) \) in the lattice \( (\mathcal{O}_K, \sigma) \):

\[
V_f : \mathcal{O} \to \mathcal{O}_K^n = \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_n(\mathcal{O}_K)
\]

\[
\sum_{i=0}^{n-1} a_i x \mapsto \begin{pmatrix}
1 & \theta_1 & \cdots & \theta_1^{n-1} \\
1 & \theta_2 & \cdots & \theta_2^{n-1} \\
\vdots & \vdots & \ddots & \vdots \\
1 & \theta_n & \cdots & \theta_n^{n-1}
\end{pmatrix}
\begin{pmatrix}
a_0 \\
a_1 \\
\vdots \\
a_{n-1}
\end{pmatrix},
\]

namely, \( V_f \) is given by a Vandermonde matrix left-multiplying the vector of coordinates.

As justified in [16] and later in [2], [3] and [17], the idea of noise increase can be formally captured by means of the condition number, defined in terms of the Frobenius norm:

Definition 3.3. For a square matrix \( A = (a_{ij}) \in \mathcal{M}_r(\mathbb{C}) \), the Frobenius norm of \( A \) is

\[
\|A\| := \sqrt{\text{Tr}(AA^\ast)} = \sqrt{\sum_{i=1}^{r} \sum_{j=1}^{r} |a_{i,j}|^2}.
\]
where $\text{Tr}$ stands for the trace map and $A^*$ is the conjugated-transpose of $A$. The condition number of $A$ is defined as

$$\text{Cond}(A) := \|A\|\|A^{-1}\|.$$ 

The condition number satisfies the following properties:

**Proposition 3.4.** For any $A, B \in \text{GL}_r(\mathbb{C})$ it holds:

- The condition number is invariant by scalar multiplication, namely, for each $\lambda \in \mathbb{C}^*$ it is $\|A\| = |\lambda|\|A\|$ and $\text{Cond}(\lambda A) = \text{Cond}(A)$.
- The condition number satisfies $\text{Cond}(A) = \text{Cond}(A^{-1})$.
- The Frobenius norm and hence the condition number are submultiplicative, namely: $\text{Cond}(AB) \leq \text{Cond}(A)\text{Cond}(B)$.

The condition number captures the idea of noise increase caused by the transformation between the lattices $(\mathcal{O}, \sigma_C)$ and $(\mathcal{O}_K, \sigma)$. Indeed, as proved in [2], for the cyclotomic field $K_n$, where the transformation is expressed in terms of the Vandermonde matrix $V_{\Phi_n}$, the condition number $\text{Cond}(V_{\Phi_n})$ is polynomial in $n$ if the number of primes dividing $n$ is fixed. However, this is not the case for $K_{4p}$, what led us to replace the map $V_{\Phi_n}$ by another lattice isomorphism which we proved to be polynomially conditioned in [3]. We will recall this second approach in Section 4.

3.2. **In praise of the family $\Phi_{2^r}^{+}(x)$.** Despite the fact that both R/PLWE problems are strongly believed to be computationally intractable, several ad hoc weak instances have been found and dealt with in a number of recent papers ([8], [7], [5], [14]). As [14] points out, these vulnerable instantiations have not been proposed for practical applications, as they do not satisfy the hypotheses of the worst-case hardness theorems which back the R/PLWE cryptosystem proposed in [12]. However, quoting [14] again, these ad hoc constructions serve to raise the following questions:

- How close are these insecure instantiations to those which enjoy worst-case hardness?
- Can we identify from these instantiations any feature which make some number fields more secure than others for R/P-LWE?
- How can we evaluate other instantiations that may not be backed by worst-case hardness theorems?

We close this section pointing out a reason to be interested, from a cryptographic point of view, in the family $\Phi_{2^r}^{+}(x)$, with $r \geq 2$ and $k$ odd: we will show that $\Phi_{2^r}^{+}(x)$ is not vulnerable to one of the attacks described in [8], an attack for which cyclotomic polynomials are not immune, in principle.

The attack has several steps: it starts with a distinguisher attack on PLWE which is transferred to a distinguisher attack against RLWE if RLWE and PLWE are equivalent for the underlying number field. Then, the decissional RLWE attack is turned into a search attack if two additional hypotheses are satisfied, but we will not enter into it here.
Soon after [8], in [5] the authors gave a direct attack on RLWE without passing by PLWE, by using the $\chi^2$ statistical test. The attack works for several general cyclotomic fields of non-power-of-two degree, but it does not seem to be any way to apply this attack to our family $\Phi_{2^m}(x)$. These attacks also justify the study of other number fields, other than cyclotomics, to instantiate R/PLWE.

The hypotheses for the attack described in [8] to be effective are as follows:

**Theorem 3.5** ([8, 7]). Let $K = \mathbb{Q}(\beta)$ be a number field of degree $n$ where $\beta \in \mathcal{O}_K$ and let $q$ be an odd prime. Suppose that the pair $(K, q)$ satisfies the following conditions:

1. $K$ is Galoisian of degree $n$.
2. The ideal $(q)$ is totally split in $\mathcal{O}_K$.
3. $K$ is monogenic.
4. The transformation between the canonical embedding of $K$ and the power basis representation of $K$ is given by a scaled orthogonal matrix.
5. If $f$ is the minimal polynomial of $\beta$, then:
   5.1 either $f(1) \equiv 0 \pmod{q}$,
   5.2 or $f(\alpha) \equiv 0 \pmod{q}$ for $\alpha \in \mathbb{F}_q$ of small order modulo $q$,
   5.3 or $f(\alpha) \equiv 0 \pmod{q}$ for $\alpha \in \mathbb{F}_q$ of small residue modulo $q$.
6. The prime $q$ is large enough, namely, $q > n^2$.

Then, there is a polynomial-time attack to the search RLWE problem for $(K, q)$.

We will not describe the attack here, but we mention that the first two conditions provide the RLWE search-to-decision reduction. The third and fourth conditions are sufficient to grant the RLWE-to-PLWE equivalence, namely, that both problems reduce to each other in polynomial time and with a polynomial error rate distortion (see [16, Section 4]). However, to grant this equivalence, as discussed in [7], it is enough that, when passing from the coordinate to the canonical embedding, the noise increase is polynomial in the degree of the underlying number field, and this noise increase is well accounted for by the condition number of the corresponding matrix.

Moreover, as we justified in [3, Remark 2.8], to grant the RLWE-to-PLWE equivalence it is not necessary to impose that the transformation between both embeddings is the natural one given by the Vandermonde matrix, and for the setting dealt with there, we replaced it by another one, given by a quasi-Vandermonde matrix attached to a subfamily of Tchebycheff polynomials of the first kind.

Finally, the last two conditions are the key to construct the attack on PLWE. Cyclotomic fields are protected against Condition [5.1]: it is well-known that if $n$ is not a prime power then $\Phi_n(1) = 1$, and if $n = q^r$ with $q$ prime then $\Phi_n(1) = q$. Therefore, $\Phi(1) \not\equiv 0 \pmod{q}$ unless $n = q^r$ for some $r \geq 1$.

Moreover, cyclotomic fields are also protected against Condition [5.2] for $\alpha \in \mathbb{F}_q$ of order 2, namely for $\alpha = -1$. Indeed (see for instance [4, Lemma 7]) $\Phi_n(-1) = 0$ if $n = 2$, $\Phi_n(-1) = p$ if $n = 2p^r$, with $p$ prime and $r \geq 1$ and $\Phi_n(-1) = 1$ otherwise.
It is not clear what can be said, in general, about roots of $\Phi_n(x)$ of order higher than 2 (but still small), although some partial results have been obtained by the authors in a still ongoing work.

What about Condition [5.3] for the cyclotomic setting? Let $\alpha$ be a root of $\Phi_n(x)$ modulo $q$. Assume that the error distribution is Gaussian, namely, $N(0, \sigma)$ with $\sigma$ chosen in a certain way to grant the ideal-lattice-SVP-to-RLWE reduction and a certain security level (a value of $\sigma \approx 8$ is proposed in [7]). Denote by $U$ the event that a sample $(a(x), b(x))$ is taken from the uniform distribution in $\mathcal{O}/q\mathcal{O} \times \mathcal{O}/q\mathcal{O}$ and by $G$ the event that the sample is taken from the PLWE distribution. Denote by $E$ the event that $b(\alpha) - ga(\alpha) \mod q$ belongs to the interval $[-q/4, q/4)$ for some guess $g \in \mathbb{F}_q$. In this case (see [7, p. 10]) we have:

$$p(E|G) = 1$$

and since $p(E|U) = 1/2$, then, assuming that samples can be taken from the uniform distribution and from the PLWE distribution with the same probability, it follows that the probability that for some guess $g$ we have $b(\alpha) - ga(\alpha) \in [-q/4, q/4)$ is $3/4$. This probability grants an overwhelming probability of success of the attack.

The authors justify that a condition for this to happen is that

$$(3.1) \quad \frac{\alpha^{2n} - 1}{\alpha - 1} \leq \frac{q^2}{64\sigma^2},$$

but even if equation $(3.1)$ does not hold, for several choices of the parameters the attack may work with probability beyond $1/2$:

**Examples 3.6** ([8]). For $n = 2^6$, $q \approx 2^{60}$ and $\sigma \approx 8$, and $\alpha = 2 \pmod q$ the authors conclude that their attack works with probability about 0.56 for any irreducible polynomial (not necessarily cyclotomic) of degree $2^6$ with $\alpha = 2$ as a root modulo $q$.

For $\sigma$ large enough, there is not much hope for equation $(3.1)$ to hold for $\alpha = 2$, and even less for $\alpha > 2$. For smaller values of $\sigma$, however, the inequality may work for not too large values of $q$. The following examples have been found with the aid of Maple:

**Examples 3.7.** For the cyclotomic polynomial $\Phi_{61}(x)$, $\alpha = 2$ is a root modulo $q = 2305843009213693951$. For these values, equation $(3.1)$ is satisfied for $\sigma = 0.4$. Likewise, for the cyclotomic polynomial $\Phi_{85}(x)$, $\alpha = 2$ is a root modulo $q = 9520972806333758431$. For these values, $(3.1)$ is again satisfied for $\sigma = 0.1$.

**Remark 3.8.** As the first author proved in [2], denoting by $\omega(n)$ the number of different primes dividing $n$, for every $M > 0$, if $\omega(n) \leq M$, the condition number of the Vandermonde matrix $V_{\Phi_n}$ is polynomial in $\phi(n)$. Hence, the problems RLWE and PLWE are equivalent for the class of cyclotomic fields $K_n$ if $\omega(n)$ is upper bounded by a fixed value. In particular, both problems are equivalent and hence RLWE is also immune to the attack for $\alpha = \pm 1$ for these fields.

Now, if we replace the cyclotomic polynomial $\Phi_n(x)$ by the polynomial $\Phi_n^+(x)$, at least in the case $n = 2^r k$, with $r \geq 2$ and $k \geq 1$ odd, we can grant not only that $\alpha = \pm 1$ are...
never roots modulo any odd prime $q$, but also that $\alpha = \pm 2$ is never a root modulo $q$, making the family $\Phi_{2r,k}^+(x)$ immune against Condition $[5.1]$, against Condition $[5.2]$ for order 2, namely for $\alpha = -1$, and against Condition $[5.3]$ for $\alpha = 2$.

Since $4 \mid 2^r k$, the polynomial $\Phi_{2r,k}^+(x)$ is even (see $[1]$ Proposition 2.5]), and hence it is enough to check our claims for $\alpha = 1, 2$.

**Proposition 3.9.** For $\Phi_{2r,k}^+(x)$, with $r \geq 2$ and $k \geq 3$ odd, we have
$$\Phi_{2r}^+(1) = \pm 1; \quad \Phi_{2r}^+(2) = 2; \quad \Phi_{2r,k}^+(1) = \Phi_{2r,k}^+(2) = 1.$$

**Proof.** Using $[1]$ Theorem 2.6], we have that $\Phi_{2r}^+(x) = u_{2r-2}(x)$ and, if $k \geq 3$,
$$\Phi_{2r,k}^+(x) = \frac{\Phi_{2r}^+(u_{2r}(x))}{\Phi_{2r}^+(u_{2r-1}(x))},$$
where $u_n(x) := 2t_n(x/2)$, being $t_n(x)$ the $n$-th Tchebycheff polynomial of the first kind. Since $u_1(x) = x$, $u_2(x) = x^2 - 1$ and $u_j(u_l(x)) = u_{jl}(x)$ for all $j, l \geq 0$, we obtain that $u_{2r}(1) = -1$ for all $n \geq 1$ and $u_1(1) = 1$, so $\Phi_{2r}^+(1) = 1$ if $r = 2$, $\Phi_{2r}^+(1) = -1$ if $r \geq 3$ and $\Phi_{2r,k}^+(1) = 1$. To see that $\Phi_{2r,k}^+(2) = 2$ and $\Phi_{2r,k}^+(2) = 1$ we can use the same argument, taking into account that $u_n(2) = 2$ for all $n \geq 1$ (see $[1]$ Corollary 2.4). We can also give the following alternative proof: for each $n \geq 1$, consider the rational expression
$$r_n(x) := \Phi_{2r}^+(x + x^{-1})x^{\frac{\phi(n)}{2}}.$$
Since $x + x^{-1} = x^{-1}(x^2 + 1)$, we see that $r_n(x)$ is a polynomial with integer coefficients. Moreover, since $\Phi_{2r}^+(\zeta_n + \zeta_n^{-1}) = 0$, then $r_n(x)$ vanishes at $\zeta_n$ and hence $\Phi_n(x) \mid r_n(x)$. Since the degree of $r_n(x)$ is precisely $\phi(n)$, then $r_n(x) = \Phi_n(x)$ up to a non-zero rational scalar. Moreover, is is easy to see that this scalar factor is the leading coefficient of $\Phi_n^+(x)$, which is 1. Hence $\Phi_{2r,k}^+(2) = \Phi_{2r,k}^+(1)$, which is equal to 2 if $k = 1$ and equal to 1 if $k \geq 3$.

Hence, if for $K_{2r,k}^+$ both RLWE and PLWE are equivalent, then also the RLWE problem will be immune against this attack based on the roots $\alpha = \pm 1, \pm 2$ for any odd prime $q$, while $K_{2r,k}$ is only provably immune against the attack based on $\alpha = \pm 1$. The goal of the rest of our article is to prove the equivalence between both problems in the sense of Definition 3.2 for $k = 1$, $k = p$ and $k = pq$, with $p$ and $q$ arbitrary odd primes and $p \neq q$.

4. The polynomial equivalence in the $2^r pq$ maximal totally real cyclotomic subextension

Here we establish the equivalence of the RLWE and PLWE problems for the family $\Phi_{2r,k}^+(x)$ in the generalised framework described in $[3]$ for $k = 1$, $k = p$ and $k = pq$. The starting point of our approach there and also here is the family of Tchebycheff polynomials of the first kind:
**Definition 4.1.** The family of Tchebycheff polynomials of the first kind is defined by any of the following equivalent properties:

a) \( t_i(x) = \cos(i \arccos(x)) \) for \( i \geq 0 \).

b) \( t_0(x) = 1, t_1(x) = x \) and \( t_i(x) = 2xt_{i-1}(x) - t_{i-2}(x) \) for \( i \geq 2 \).

Set, for \( i \geq 0 \), \( u_i(x) = 2t_i(x/2) \). An easy induction argument shows that \( u_i(x) \in \mathbb{Z}[x] \) for each \( i \geq 0 \). By an iterated application of the identity for the cosine of the sum of two angles, it is easy to show the following property:

\[
t_{i+j}(x) + t_{|i-j|}(x) = 2t_i(x)t_j(x),
\]

which yields the following identity:

\[
u_{i+j}(x) + u_{|i-j|}(x) = u_i(x)u_j(x)
\]

for any \( i, j \geq 0 \).

For \( n \geq 1 \) such that \( 4 \mid n \), set \( N = n/4 \) and denote

\[
V_N = (u_i(\psi_{2k-1}))_{0 \leq i \leq n-1},
\]

where \( \psi_{2k-1} = 2 \cos \left( \frac{2\pi(2k-1)}{n} \right) \). Using [11, Theorem 1] it was shown in [3, Proposition 3.4] that

\[
\text{Cond}(V_N) \leq N(N+1).
\]

### 4.1. Main result.

4.1.1. \textit{Case \( n = 2^r \).} Assume that \( n = 2^r \), with \( r \geq 2 \) so that \( N = 2^{r-2} = \deg(K_{2^r}^+) \). In this case, \( \Phi_n^+(x) \) is the minimal polynomial of \( \psi_1 = 2 \cos \left( \frac{\pi}{2^{r+1}} \right) \), whose Galois conjugates are all the nodes \( \psi_{2k-1} \) with \( 1 \leq k \leq 2^{r-2} \). Hence the matrix \( V_N \) already provides the polynomially conditioned lattice monomorphism from \((\mathcal{O}, \sigma_C)\) to \((\mathcal{O}_{K_i^+}, \sigma)\). Since the image of \( V_N \) is a finite order sublattice of \((\mathcal{O}_{K_i^+}, \sigma)\), multiplying by this index and composing with \( V_N^{-1} \) provides a polynomially conditioned monomorphism from \((\mathcal{O}_{K_i^+}, \sigma)\) to \((\mathcal{O}, \sigma_C)\). This will be discussed in Theorem 4.14 which applies to the three cases under study, namely \( n = 2^r \), \( n = 2^rp \) and \( n = 2^rpq \).

4.1.2. \textit{Case \( n = 2^rp \).} Assume that \( n = 2^rp \), with \( p \) an odd prime number, so \( N = 2^{r-2}p \) and \( m = \deg(K_{2^r}^{+p}) = 2^{r-2}(p-1) \). Since we are looking for a polynomially conditioned lattice isomorphism between \((\mathcal{O}, \sigma_C)\) and \((\mathcal{O}_{K_i^+}, \sigma)\), we need to exclude from \( V_N \) the \( N - m = 2^{r-2}p \) rows corresponding to the values \( \psi_{2k-1} \) such that \( (2k-1, p) \neq 1 \), i.e. the nodes of the form

\[
\psi_{jp} = 2 \cos \left( \frac{j \pi}{2^{r-1}} \right),
\]

and we also need to extract \( 2^{r-2} \) columns so that the remaining \( m \times m \) matrix is invertible. This is equivalent to multiplying \( V_N \) by a suitable matrix \( A \) obtaining

\[
V_N A = \begin{pmatrix} V_{N-m} & O \\ C & R_m \end{pmatrix},
\]
where $O$ is the $(N - m) \times m$ zero matrix, $V_{N-m}$ is a square matrix of dimension $N - m$, $C$ is an $m \times (N - m)$ matrix and $R_m$ is a square invertible matrix of size $m$ with entries in $\mathcal{O}_{K^+_m}$. If $A$ is polynomially conditioned, as we will prove, so will be $R_m$.

We begin with a permutation of the rows of $V_N$ so that those $2r^{-2}$ rows corresponding to the nodes $\psi_{jp}$ are in the first positions. For simplicity, we still denote this matrix by $V_N$, which clearly has the same condition number as before.

The strategy, as in [3], will be to perform certain transformations on the columns of $V_N$ such that the $(N - m) \times m$ upper-right submatrix of $V_N$ becomes the zero matrix and to control the condition number of the matrix which contains all the elementary column operations. Write $V_N = [C_0, C_1, \ldots, C_{N-1}]$, where $C_i$ is the $(i + 1)$-th column of $V_N$. Observe that $u_{2r^{-2}}(\psi_{jp}) = 0$ for all $j$, so the first $N - m$ entries of the column $C_{2r^{-2}}$ are zero. We perform the following transformations: for each $l$ with $1 \leq l \leq 2r^{-2}(p - 1) - 1$, we replace the column $C_{2r^{-2} + l}$ by the sum

$$C_{2r^{-2} + l} + C_{[2r^{-2} - l]}$$

This transformation is equivalent to multiplying $V_N$ on the right by the matrix

$$A = \begin{pmatrix} I_{N-m} & K \\ O & L_m \end{pmatrix},$$

where $I_{N-m}$ is the identity matrix of dimension $N - m$, $K$ is a $(N - m) \times m$ matrix whose columns are zero except for the $k$-th ones, with $2 \leq k \leq 2r^{-1}$, all of which have one entry equal to 1 and the rest of them equal to 0, and $L_m$ is matrix whose $k$-diagonals are zero except for $k = 0$ and $k = 2r^{-1}$ (where by $k$-diagonal of a square matrix $(a_{ij})$ we mean the diagonal whose terms are the entries of the form $a_{i,i+k}$, both of which are constant and equal to 1).

By relation (4.1), after this transformation the term corresponding to the node $\psi_{2k-1}$ in the new column $C_{2r^{-2} + l}$ is the value at $\psi_{2k-1}$ of $u_{2r^{-2}} u_l$, so it is zero on $\psi_{jp}$. Regarding the condition number of $A$, we have that

**Proposition 4.2.**

$$\text{Cond}(A) < \sqrt{3m(5m^2 + 2m)}.$$

**Proof.** Since that matrix $A$ has only $N + 2r^{-1} - 1 + m - 2r^{-1} = N + m - 1$ non-zero terms, all of them equal to 1, and $N < 2m$, we have

$$\|A\|^2 < 3m.$$

The inverse of $A$ is given by

$$A^{-1} = \begin{pmatrix} I_{N-m} - KL_m^{-1} \\ O & L_m^{-1} \end{pmatrix}.$$ 

The matrix $L_m^{-1}$ has $k$-diagonal equal to zero except if $k = j2r^{-1}$, for $j \geq 0$, in which case the diagonal is constant and equal to $(-1)^j$. Therefore, the entries of $KL_m^{-1}$ are all
bounded in absolute value by 2, and
\[ \| A^{-1} \|^2 < N + 4(N - m)m + \frac{m(m - 1)}{2} < 5m^2 + 2m, \]
which shows the bound for the condition number of \( A \).

4.1.3. Case \( n = 2^r pq \). Assume that \( n = 2^r pq \), with \( p, q \) odd prime numbers and \( p < q \), so \( N = 2^{r-2}pq \) and \( m = \deg(K_{2^r pq}^+) = 2^{r-2}(p - 1)(q - 1) \). In this case, we need to exclude from \( V_N \) the \( N - m = 2^{r-2}(p + q - 1) \) rows corresponding to the values \( \psi_{2k-1} \) such that \( (2k - 1, pq) \neq 1 \), i.e. the nodes of the form
\[ \psi_{jp} = 2 \cos \left( \frac{j \pi}{2r - 1 q} \right) \quad \text{and} \quad \psi_{jq} = 2 \cos \left( \frac{j \pi}{2r - 1 p} \right), \]
with \( j \) odd such that \( jp \leq 2N - 1 \) and \( jq \leq 2N - 1 \) and we also need to extract \( N - m \) columns so that the remaining \( m \times m \) matrix is invertible.

As in the previous case, we begin with a permutation of the rows of \( V_N \) so that those \( N - m \) rows corresponding to the nodes \( \psi_{jp} \) and \( \psi_{jq} \) are in the first positions, and we still denote this matrix by \( V_N \).

We will use the following fact:

**Lemma 4.3.** Notations as before, we have that \( u_{2^{r-2}q}(\psi_{jp}) = 0 \) for all \( j \), and
\[ \sum_{k=1}^{\frac{p-1}{2}} (-1)^{k+1} u_{2^{r-1}k}(\psi_{jq}) = 1 \]
for all \( j \) such that \( p \nmid j \).

**Proof.** The first identity is clear. For the second one, we use Lagrange trigonometric identity:
\[ \sum_{k=1}^{M} \cos(k\theta) = -\frac{1}{2} + \frac{\sin((M + 1/2)\theta)}{2\sin(\theta/2)}, \]
for any \( M \geq 1 \) and any \( 0 < \theta < 2\pi \).

Notice that the identity remains true for any \( \theta \) which is not an integer multiple of \( 2\pi \). Hence, taking \( M = (p - 1)/2 \) and \( \theta = (j + p)\pi/p \) (which is not a multiple of \( 2\pi \) since \( p \nmid j \)), we have:
\[ \sum_{k=1}^{\frac{p-1}{2}} (-1)^{k+1} \cos \left( \frac{k \pi j}{p} \right) = -\sum_{k=1}^{\frac{p-1}{2}} \cos \left( \frac{k \pi j}{p} + k \pi \right) = \frac{1}{2} - \frac{\sin((j + p)\pi/(2p))}{2\sin((j + p)\pi/(2p))} = \frac{1}{2} \]
since \( j \) and \( p \) are odd. Therefore,
\[ \sum_{k=1}^{\frac{p-1}{2}} (-1)^{k+1} u_{2^{r-1}k}(\psi_{jq}) = 2 \sum_{k=1}^{\frac{p-1}{2}} (-1)^{k+1} \cos \left( \frac{k \pi j}{p} \right) = 1. \]
Write \( V_N = [C_0, C_1, \ldots, C_{N-1}] \), where \( C_i \) is the \((i+1)\)-th column of \( V_N \). We perform the following transformations: for each \( l \) with \( 0 \leq l \leq m-1 \), we replace the column \( C_{2^{r-2}(q+p-1)+l} \) by the sum

\[
(4.3) \quad \sum_{j=1}^{n-1} (-1)^{j+1} \left[ C_{2^{r-2}(q+p-(2j-1))} + C_{2^{r-2}(q-p+(2j-1))} \right] + (-1)^{\frac{n+3}{2}} C_{2^{r-2}q} \quad \text{if } l = 0,
\]

and by the sum

\[
(4.4) \quad \sum_{j=1}^{n-1} (-1)^{j+1} \left[ C_{2^{r-2}(q+p-(2j-1))} + C_{2^{r-2}(q-p+(2j-1))} \right] + C_{2^{r-2}(q+p-(2j-1))} + C_{2^{r-2}(q-p-(2j-1))} \right] + (-1)^{\frac{n+3}{2}} \left[ C_{2^{r-2}q+l} + C_{2^{r-2}(q-l)} \right] \quad \text{if } l \geq 1.
\]

This transformation is equivalent to multiplying \( V_N \) on the right by the matrix

\[
A = \left( \begin{array}{cc} I_{N-m} & K \\ O & L_m \end{array} \right),
\]

where \( I_{N-m} \) is the identity matrix, \( K \) is a \((N-m) \times m\) matrix and \( L_m \) is an upper triangular matrix whose main diagonal is the identity.

By relation (4.1), after this transformation the term corresponding to the node \( \psi_{2k-1} \) in the new column \( C_{2^{r-2}(q+p-1)+l} \) is the value at \( \psi_{2k-1} \) of

\[
u_{2^{r-2}q} \left[ \sum_{j=1}^{n-1} (-1)^{j+1} u_{2^{r-2}q \cdot (2j-1)} + (-1)^{\frac{n+3}{2}} u_{2^{r-2}q} \right] = (-1)^{\frac{n+3}{2}} \nu_{2^{r-2}q} \sum_{j=1}^{n-1} (-1)^{j+1} u_{2^{r-2}q} - 1
\]

in case \( l = 0 \), or

\[
\nu_{2^{r-2}q} \left[ \sum_{j=1}^{n-1} (-1)^{j+1} \left( u_{2^{r-2}(p-(2j-1))} + u_{2^{r-2}(p-(2j-1))} \right) + (-1)^{\frac{n+3}{2}} u_l \right]
\]

\[
= \nu_{2^{r-2}q} u_l \left[ \sum_{j=1}^{n-1} (-1)^{j+1} u_{2^{r-2}(p-(2j-1))} + (-1)^{\frac{n+3}{2}} \right]
\]

\[
= (-1)^{\frac{n+3}{2}} \nu_{2^{r-2}q} u_l \left[ \sum_{j=1}^{n-1} (-1)^{j+1} u_{2^{r-2}q} - 1 \right],
\]

in case \( l \geq 1 \), so by Lemma 4.3 it is zero on \( \psi_{jq} \) and \( \psi_{jm} \).

We have the following result for the blocks \( K \) and \( L_m \) of the matrix \( A \):

**Lemma 4.4.** The matrix \( K \) has entries in \( \{0, \pm 1, \pm 2\} \), and the matrix \( L_m \) is a Toeplitz matrix whose \( k \)-diagonal is equal to \((-1)^j\) if \( k = j2^{r-1} \) for \( 0 \leq j \leq p-1 \), is equal to \((-1)^{j+1}\) if \( k = j2^{r-1} \) with \( q \leq j \leq q + p - 1 \) and is equal to 0 otherwise.
Proof. The condition on the entries of $K$ is clear for the first column, whose non-zero entries are in fact $\pm 1$, since the columns that appear in the sum (4.3) are all different. For the other columns of $K$, observe that for all $1 \leq i, j \leq (p-1)/2$ we have

\[(4.5) \quad 2^{r-2}(q + p - (2i - 1)) + l > 2^{r-2}q + l > 2^{r-2}(q - p + (2j - 1)) + l > l.
\]

Moreover, for all $1 \leq j \leq (p-1)/2$ we have that

- If $l \leq 2^{r-2}q$ then $|2^{r-2}(q + p - (2j - 1)) - l| > |2^{r-2}q - l|$ and either
  \[|2^{r-2}(q + p - (2j - 1)) - l| < l \quad \text{or} \quad |2^{r-2}(q + p - (2j - 1)) - l| < |2^{r-2}q - l|;\]
- If $l > 2^{r-2}q$ then $l > |2^{r-2}(q - p + (2j - 1)) - l| > |2^{r-2}q - l|$. 

These relations, together with (4.5), imply that each column in the sum (4.4) appears at most twice, and the statement on the entries of $K$ is proved.

To show the statement for $L_m$, note that for each $l \geq 1$ an index $k \geq 2^{r-2}(q + p - 1)$ in the sum (4.4) can only be of the form $|2^{r-2}(q - p + (2j - 1)) - l|$ if $l > 2^{r-2}(q - p + (2j - 1))$ (otherwise those terms are less than $2^{r-2}(q - 2)$), can only be of the form $|2^{r-2}(q - p - (2j - 1)) - l|$ if $l > 2^{r-2}(q + p - (2j - 1))$ (otherwise those terms are less than $2^{r-2}(q + 2) < 2^{r-2}(q + p - 1)$) and can only be of the form $|2^{r-2}q - l|$ if $l > 2^{r-2}q$ (otherwise those terms are less than $2^{r-2}q$). In this case, for all $1 \leq i, j \leq (p-1)/2$ we have

\[l - 2^{r-2}(q - p + (2i - 1)) > l - 2^{r-2}q > l - 2^{r-2}(q + p - (2j - 1)).\]

This relation, together with (4.5), shows that each column $C_k$ with $k \geq 2^{r-2}(q + p - 1)$ appears at most once in the sum (4.4). Observe that the maximum index that appears in the sum (4.4) among the terms of the form $2^{r-2}(q + p - (2j - 1)) + l$, $2^{r-2}q + l$ and $2^{r-2}(q - p + (2j - 1)) + l$ is $2^{r-2}(q + p - 1) + l$ and the minimum is $2^{r-2}(q - p + 1) + l$, so those terms range the $k$-diagonals for $0 \leq k \leq 2^{r-1}(p - 1)$; the difference between two consecutive terms, which appear with opposite sign in the sum (4.4), is $2^{r-1}$, so the statement for the diagonals of the form $2^{r-1}j$ with $0 \leq j \leq p-1$ follows. Analogously, the maximum index that appears in the sum (4.4) among the terms of the form $l - 2^{r-2}(q - p + (2j - 1))$, $l - 2^{r-2}q$ and $l - 2^{r-2}(q + p - (2j - 1))$ is $l - 2^{r-2}(q - p + 1)$ and the minimum is $l - 2^{r-2}(q + p - 1)$, so those terms range the $k$-diagonals for $2^{r-1}q \leq k \leq 2^{r-1}(q + p - 1)$, and the statement for the columns of the form $2^{r-1}j$ with $q \leq j \leq q + p - 1$ follows as in the previous case.

As for the condition number, we have:

**Proposition 4.5.** With notations as before,

\[\text{Cond}(A) < \sqrt{(5m^2 + 2m)(4m^4 + m^2 + 2m)}.\]
Proof. By Lemma 4.4, since the non-zero entries of $K$ are bounded in absolute value by 2 and the non-zero entries in $L_m$ are bounded in absolute value by 1, we have

$$\|A\|^2 \leq N + 4(N - m)m + \frac{m(m - 1)}{2}.$$ 

Since

$$\frac{N}{m} = \frac{p}{p - 1} \frac{q}{q - 1} < 2$$

we obtain $\|A\|^2 < 5m^2 + 2m$. On the other hand,

$$A^{-1} = \begin{pmatrix} I_{N-m} - KL_m^{-1} \\ 0 \quad L_m^{-1} \end{pmatrix}.$$

Since $L_m$ is an upper triangular Toeplitz matrix, if we denote $r(x) = 1 + \sum_{j=1}^{m-1} a_j x^j$, where $a_j$ is the entry of the $j$-diagonal of $L_m$, the inverse of $L_m$, which is also an upper triangular Toeplitz matrix, has $k$-diagonal equal to $b_k$, where $s(x) = \sum_{k \geq 0} b_k x^k$ is the formal series such that $r(x)s(x) = 1$. Denote $t = 2^{-1}$. If $p = 3$, then $(p-1)t \leq m-1 < qt$, so by Lemma 4.4 we have that $r(x) = 1 - x^t + x^{2t}$. Since $r(x)(1 + x^t) = 1 + x^{3t}$, then

$$s(x) = (1 + x^t)(1 + x^{3t})^{-1} = (1 + x^t) \sum_{i \geq 0} (-1)^i x^{3it}$$

and the non-zero diagonals of $L_m^{-1}$ are ±1. If $p \geq 5$ then $(q + p - 1)t \leq m - 1$, since

$$\frac{(q + p - 1)t}{m} = \frac{2(q + p - 1)}{(p - 1)(q - 1)} \leq \frac{2(q + 4)}{4(q - 1)} < 1.$$ 

Then, by Lemma 4.4 we have that

$$r(x) = 1 - x^t + x^{2t} - x^{3t} + \ldots + x^{(p-1)t} + x^{qt} - x^{(q+1)t} + x^{(q+2)t} - x^{(q+3)t} + \ldots + x^{(q+p-1)t}.$$ 

Since $r(x)(1 + x^t) = 1 + x^{pt} + x^{qt} + x^{(p+q)t} = (1 + x^{pt})(1 + x^{qt})$, then

$$s(x) = (1 + x^t)(1 + x^{pt})^{-1}(1 + x^{qt})^{-1} = (1 + x^t) \sum_{i,j \geq 0} (-1)^{i+j} x^{(ip+jq)t}.$$ 

Note that if $ip + jq = kp + lq + 1$ for some $i, j, k, l \geq 0$, then $i + j$ and $k + l$ have opposite parity, so the coefficient of $x^{(ip+jq)t}$ in the series $s(x)$ is zero; moreover, $ip + jq = kp + lq$ with $(i, j) \neq (k, l)$ can only hold if $ip + jq \geq pq$, so $(ip + jq)t \geq m$. This implies that the non-zero diagonals of $L_m^{-1}$ can only be ±1. Therefore the entries of $-KL_m^{-1}$ are bounded in absolute value by 2$m$. Then,

$$\|A^{-1}\|^2 \leq N + 4m^2(N - m)m + \frac{m(m - 1)}{2} < 4m^4 + m^2 + 2m$$

and the bound for the condition number follows. \qed
4.1.4. Conclusion. Putting together the cases $n = 2^r$, $n = 2^rq$ and $n = 2^rpq$, due to Proposition 3.4 from equation (4.2) and Propositions 4.2 and 4.5 we obtain

\[
\text{Cond}(V_N) \leq m(m+1) \quad \text{if } n = 2^r
\]

\[
\text{Cond}(V_N A) \leq 2m(2m+1)\sqrt{3m(5m^2 + 2m)} \quad \text{if } n = 2^rp
\]

\[
\text{Cond}(V_N A) \leq 2m(2m+1)\sqrt{(5m^2 + 2m)(4m^4 + m^2 + 2m)} \quad \text{if } n = 2^rpq.
\]

Let us write

\[
V_N A = \begin{pmatrix} V_{N-m} & O \\ C & R_m \end{pmatrix},
\]

where $V_{N-m}$ is the principal minor of $V_N$ of order $N-m$, which is invertible, $C$ is an $m \times (N-m)$ matrix and $R_m \in M_{m \times (N-m)}(O_{K_n^{2r-pq}})$ is invertible (since $V_N$ is so). The reason why the entries of $R_m$ belong to $O_{K_n^{2r-pq}}$ is that they are linear combinations of the entries of $V_N$ with coefficients 0, ±1, ±2. Hence, it is also immediate that

\[
\|R_m\| \leq \|V_N A\|.
\]

Now, the inverse of $V_N A$ exists and is:

\[
(V_N A)^{-1} = \begin{pmatrix} V_{N-m}^{-1} & O \\ -R_m^{-1}CV_{N-m}^{-1} & R_m^{-1} \end{pmatrix},
\]

hence

\[
\|R_m^{-1}\| \leq \|(V_N A)^{-1}\|.
\]

The previous inequalities imply that

\[
\text{Cond}(R_m) \leq \text{Cond}(V_N A).
\]

We are now in position to prove our main result:

**Theorem 4.6.** Let $p$ and $q$ be different odd prime numbers and let $r \geq 2$. For $n = 2^r$, $n = 2^rp$ and $n = 2^rpq$, the RL WE and the PL WE problems are equivalent for the ring of integers $O_{K_n^{2r-pq}}$ of $K_n^{2r-pq}$.

**Proof.** Setting as before $n = 2^r pq$ (the other cases are analogous), the map

\[
\Psi : O \rightarrow \sigma(O_{K_n^{2r-pq}})
\]

\[
\mathbf{u} \mapsto R_m \mathbf{u}
\]

is a well defined monomorphism of lattices, since $R_m \in M_{m \times (N-m)}(O_{K_n^{2r-pq}})$ and it is invertible. Moreover, as established above, the condition number of $R_m$ is $O(20m^5)$. This provides a polynomial reduction from PLWE to RLWE incurring into a distortion which is polynomial in $m$.

The map $\Psi$ is not necessarily surjective since we can only grant that $\Psi(O)$ is a sublattice of $\sigma(O_{K_n^{2r-pq}})$ but since $\Psi$ is injective (because $R_m$ is invertible), the ranks of $\Psi(O)$ and $\sigma(O_{K_n^{2r-pq}})$ coincide. In particular, the image $\Psi(O)$ is a sublattice of $\sigma(O_{K_n^{2r-pq}})$ of finite index.
Indeed, as it was shown in section 4.1.3, there exist polynomials $p_j(x) \in \mathbb{Z}[x]$, for $0 \leq j \leq m - 1$, of different degrees such that each row of the matrix $R_m$ is of the form $(p_0(\psi_1), p_1(\psi_1), \ldots, p_{m-1}(\psi_1))$ for some odd $l$ coprime with $p$ and $q$. Moreover, the polynomials $p_j$ are of the form

$$p_0(x) = a(x); \quad p_j(x) = a(x)u_j(x) \text{ for } 1 \leq j \leq m - 1,$$

where

$$a(x) = (-1)^{\frac{j+1}{2}} u_{2r-2q}(x) \left[ \sum_{i=1}^{r} (-1)^{i+1} u_{2r-1i}(x) - 1 \right].$$

Note that $a(x)$ is a polynomial of degree $N - m$ and its roots are exactly the $N - m$ nodes $\psi_{jp}$ and $\psi_{jq}$, with $j$ odd, so $a(\psi_1) \neq 0$ for every odd $l$ coprime with $p$ and $q$. Consequently, the elements $\{p_0(\psi_1), p_2(\psi_1), \ldots, p_{m-1}(\psi_1)\}$ are linearly independent over $\mathbb{Z}$, since otherwise the elements $\{1, u_1(\psi_1), \ldots, u_{m-1}(\psi_1)\}$ would be linearly dependent, which is clearly not the case, as $\deg(u_i(x)) = i$ and $\deg(K_{2r\cdot pq}^+) = m$.

Hence, for $0 \leq i \leq m - 1$, taking into account that the minimal polynomial of $\psi_1$ has degree $m$, we can write $p_i(\psi_1) := \sum_{j=0}^{m-1} a_{i,j} \psi_1^j$ so that the matrix

$$P = (a_{ij})_{0 \leq i,j \leq m-1}$$

contains the coordinates (with respect to the power basis of $O_{K_{2r\cdot pq}^+}$) of the elements $\{p_0(\psi_1), p_1(\psi_1), \ldots, p_{m-1}(\psi_1)\}$, which are a $\mathbb{Z}$-basis of a sublattice $\Lambda$ of $O_{K_{2r\cdot pq}^+}$ of the same rank and hence of finite index $\lambda := |\det(P)|$ (see [19] Theorem 1.17).

Now, pushing forward this inclusion by the canonical embedding $\sigma$, which is in particular a lattice isomorphism over its image, we observe that $\Psi(O) = \sigma(\Lambda)$ is a sublattice of $\sigma(O_{K_{2r\cdot pq}^+})$ of the same index $\lambda$.

Hence, for each $u \in \sigma(O_{K_{2r\cdot pq}^+})$, one has that $\lambda u \in \Psi(O)$ and the map

$$\Psi^{-1} \circ [\lambda]: \sigma(O_{K_{2r\cdot pq}^+}) \to O \quad u \mapsto R_m^{-1}(\lambda u)$$

provides a polynomial reduction from RLWE to PLWE incurring into a distortion which is, since homotheties have condition number 1, polynomial in $m$. \qed

### References

[1] K. Alan Loper, N. J. Werner. Resultants of minimal polynomials of maximal real cyclotomic extensions. *Journal of Number Theory*, 158 (2016) 298–315.

[2] I. Blanco-Chacón. On the RLWE/PLWE equivalence for cyclotomic number fields. *Applicable Algebra in Engineering, Communications and Computing*, 2020 (DOI: https://doi.org/10.1007/s00200-020-00433-z)
18 IVÁN BLANCO CHACÓN AND LORENA LÓPEZ-HERNANZ

[3] I. Blanco-Chacón. RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices. *Journal of Algebra and its Applications*, 2021 (DOI: https://doi.org/10.1142/S0219498822502188)

[4] B. Bzdęga, A. Herrera-Poyatos, P. Moree. Cyclotomic polynomials at roots of unity. *Acta Arithmetica*, 184 no. 3 (2018) 215–230.

[5] H. Chen, K. Lauter, K. E. Stange. Attacks on the Search RLWE Problem with Small Errors. *SIAM Journal on Applied Algebra and Geometry*, (1), 2017, 665–682.

[6] L. Ducas, A. Durmus. Ring-LWE in polynomial rings. In: Fischlin M., Buchmann J., Manulis M. (eds) Public Key Cryptography. PKC 2012. *Lecture Notes in Computer Science*, vol 7293 (2012). Springer, Berlin, Heidelberg.

[7] K. Eisenträger, S. Hallgren, K. Lauter: Weak Instances of PLWE. In: JouxA., Youssef A. (eds) Selected Areas in Cryptography–SAC 2014. *Lecture Notes in Computer Science*, vol 8781 (2014). Springer.

[8] Y. Elias, K. Lauter, E. Ozman, K. Stange. Ring-LWE cryptography for the number theorist. In: E. Eischen, L. Long, R. Pries, K. Stange (eds) *Directions in Number Theory*. Association for Women in Mathematics Series, vol 3. Springer 2016.

[9] W. Gautschi, G. Inglese. Lower bounds for the condition number of Vandermonde matrices. *Numerische Mathematik*, 52 (1988), 241–250.

[10] S. Khoth. Hardness of approximating the shortest vector problem in lattices. *Journal of the ACM*, 52 (2005), no. 5, 789–808.

[11] M. Kuian, L. Reichel, S. Shiyanyovskii. Optimally conditioned Vandermonde-like matrices. *SIAM Journal on Matrix Analysis and Application*, 40 (4) (2019) pp. 1399–1424.

[12] V. Lyubashevsky, C. Peikert, O. Regev. On ideal lattices and learning with errors over rings. In: Gilbert H. (eds) Advances in Cryptology–EUROCRYPT 2010. *Lecture Notes in Computer Science*, 6110. Springer.

[13] D. Micciancio. The shortest vector in a lattice is hard to approximate to within some constant. In Proc. 39th Annual IEEE Symposium on Foundations of Computer Science, 1998.

[14] C. Peikert. How (not) to instantiate ring-RLWE. In: Zikas, V.; de Prisco, R. (eds.) SCN 2016, LNCS vol 9841, pags. 411–430 (2016) Springer.

[15] O. Regev. On lattices, learning with errors, random linear codes and cryptography. *Journal of the ACM*, 56 (6), 2009.

[16] M. Rosca, D. Stehlé, A. Wallet. On the Ring-LWE and Polynomial-LWE Problems. In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2018. *Lecture Notes in Computer Science*, vol 10820 (2018). Springer, Cham.

[17] A. J. Di Scala, C. Sanna, E. Signorini: On the condition number of the Vandermonde matrix of the nth cyclotomic polynomial. *Journal of Mathematical Cryptology*, vol. 15, no. 1 (2021), 174–178.

[18] D. Stehlé, R. Steinfeld, K. Tanaka, K. Xagawa. Efficient Public Key Encryption Based on Ideal Lattices. In: Matsui M. (eds) Advances in Cryptology–ASIACRYPT 2009. *Lecture Notes in Computer Science*, vol 5912 (2009). Springer, Berlin, Heidelberg.

[19] I.N. Stewart and D.O. Tall. *Algebraic Number Theory (Second Edition)*. Chapman and Hall/CRC Press, 1987.

[20] L.C. Washington. *Introduction to cyclotomic fields*. Springer GTM, 1997.

Departamento de Física y Matemáticas, Universidad de Alcalá, España

Email address: ivan.blancoc@uah.es; lorena.lopezh@uah.es