Cryptography and Communications (2025) 17:741–775
https://doi.org/10.1007/s12095-024-00771-6

RESEARCH

Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields

Iván Blanco-Chacón[1,3] · Alberto Pedrouzo-Ulloa[2] · Rahinatou Y. Njah Nchiwo[3] · Beatriz Barbero-Lucas[4]

Received: 23 April 2024 / Accepted: 22 December 2024 / Published online: 30 January 2025
© The Author(s) 2025

Abstract
We discuss the advantages and limitations of cyclotomic fields to have fast polynomial arithmetic within homomorphic encryption, and show how these limitations can be overcome by replacing cyclotomic fields by a family that we refer to as cyclo-multiquadratic. This family is of particular interest due to its arithmetic efficiency properties and to the fact that the Polynomial Learning with Errors (PLWE) and Ring Learning with Errors (RLWE) problems are equivalent for it. Likewise, we provide exact expressions for the condition number for any cyclotomic field, but under what we call the twisted power basis. As a tool for our result, we obtain refined polynomial upper bounds for the condition number of cyclotomic fields with up to 6 different primes dividing the conductor. From a more practical side, we also show that for this family, swapping between NTT (Number Theoretic Transform) and coefficient representations can be achieved at least twice faster than for the usual cyclotomic family.

Keywords Ring Learning with Errors · Polynomial Learning with Errors · Condition Number · Cyclotomic polynomials · Homomorphic Encryption · Number Theoretic Transforms

Mathematics Subject Classification (2010) 11T71 · 94A60 · 11Y16

Iván Blanco-Chacón and Alberto Pedrouzo-Ulloa contributed equally to this work.

✉ Iván Blanco-Chacón
ivan.blancoc@uah.es

✉ Alberto Pedrouzo-Ulloa
apedrouzo@gts.uvigo.es

✉ Rahinatou Y. Njah Nchiwo
rahinatou.njahepousenchiwo@aalto.fi

✉ Beatriz Barbero-Lucas
beatriz.barberolucas@ucdconnect.ie

1 Departament of Physics and Mathematics, University of Alcalá, Alcalá, Spain

2 atlanTTic, Universidade de Vigo, Vigo 36310, Galicia, Spain

3 Department of Mathematics and Systems Analysis, Aalto University, Espoo, Finland

4 School of Mathematics and Statistics, University College Dublin, Dublin, Ireland

1 Introduction and motivation

Lattices have become a fundamental tool for the construction of modern and efficient cryptographic primitives. Notably, they bring about several relevant properties; firstly, from a theoretical perspective, lattice-based cryptographic primitives admit quantum polynomial reductions from worst-case to average-case supposedly hard lattice problems, which typically correspond to approximating within polynomial factors the Shortest Vector Problem (SVP) or Closest Vector Problem (CVP) over general lattices, or even over the more structured class of ideal lattices. Despite the fact that the precise theoretical hardness of all these worst-case assumptions is not well established yet, confidence on its difficulty has been gained during the last years by the fact that there are already numerous works studying their concrete bit security [1], and there are also related theoretical results proving that SVP for general lattices and with small approximation factors is NP-hard [2, 3]. Secondly, lattice-based primitives are easier to implement and require, in general, much smaller key sizes than other post-quantum proposals.

At this point, it is worth mentioning that comparing to more traditional quantum-vulnerable cryptographic assumptions (*e.g.,* hardness of integer factorisation for RSA and the discrete logarithm problem for Diffie-Hellman), lattice-based primitives introduce a non-negligible size overhead on both the encrypted data and the keys. Even so, in return they are usually simple, efficient and highly parallelizable, while also comparing favourably with the use of post-quantum assumptions. Actually, the success caused by their benefits is confirmed by the fact that, out of the four proposals selected in the NIST Post-Quantum Cryptography Standardization Process, three are lattice-based (see [4]). Moreover, this category has been keeping the largest number of surviving candidates along all the previous rounds. For instance, in the third round, 5 out of 7 finalists were based on structured lattice assumptions; being also the only hardness assumption keeping surviving representatives for digital signatures, Public-Key Cryptography (PKE) and Key Encapsulation Mechanisms (KEM).

Finally, not only they appear as a strong substitute for conventional cryptographic primitives, but also they have shown to be very flexible, having been used to construct a wide variety of new exciting applications, *e.g.,* Fully Homomorphic Encryption (FHE), Functional Encryption (FE), Attribute-based Encryption (ABE), etc. In particular, if we pay attention to the state-of-the-art of FHE, lattice-related assumptions are nowadays the main building block backing up its security; *e.g.,* in the Homomorphic Encryption (HE) standardization process all included designs rely on the use of lattices. (see [5]).

1.1 The family of Learning with Errors and its equivalence between variants

While the aim in lattice-based cryptography is to ground security in the hardness of the previously mentioned worst-case lattice problems, alternative average-case assumptions are often considered to build cryptographic primitives. In this case, the objective is to make use of the assumptions which better fit the needs of practical cryptographic constructions. Among them, the most prominent example is the Learning with Errors problem (LWE [6]). It has become the preferred one due to its versatility and strong security guarantees by possessing a reduction from approximate SVP over general lattices. However, applications based on LWE present a quadratic overhead with respect to the considered security parameter [7].

As a means to effectively address this limitation, Lyubashevsky *et al.* [7] introduced a variant called Ring Learning with Errors (RLWE) which, contrarily to LWE, is based on the

hardness of worst-case problems over ideal lattices. RLWE has proven to be more practical than LWE, removing its quadratic overhead and, consequently, enabling a noteworthy reduction in the size of public keys and the ciphertext-to-plaintext size ratio. Alternatively, the Module-LWE problem (MLWE [8, 9]) was introduced as a bridge between LWE and RLWE, enabling for more (resp. less) efficient constructions than LWE (resp. RLWE), but having a reduction from problems over less structured lattices (*i.e.,* module lattices) than ideal lattices.

In general, the wide variety of structured and unstructured lattice assumptions, together with their dependency on many interrelated parameters, makes the analysis of the concrete security of lattice constructions a very relevant topic (see [10] and [1]).

1.2 PLWE and conditions for polynomial equivalence with RLWE

To make the present work self-contained, we recall next the definitions of the RLWE and the PLWE problems we will work with, as well as the notion of both problems being equivalent.

For a number field K, let us denote by $\mathcal{O}_K$ its ring of integers. Let q be a rational prime and let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial. Denote further $\mathcal{O}_f = \mathbb{Z}[x]/(f(x))$. If the polynomial $f(x)$ is understood or not entirely relevant for the discussion, we will just write $\mathcal{O}$ instead of $\mathcal{O}_f$.

Definition 1.1 (The RLWE/PLWE problem) Let χ be a discrete random variable with values in $\mathcal{O}_K/q\mathcal{O}_K$ (resp. in $\mathcal{O}/q\mathcal{O}$). The RLWE (resp. PLWE) problem for χ is defined as follows:

For an element $s \in \mathcal{O}_K/q\mathcal{O}_K$ (resp. $\mathcal{O}/q\mathcal{O}$) chosen uniformly at random,[1] a RLWE sample (resp. a PLWE sample) is a pair $(a, as + e)$ where a is sampled uniformly at random from $\mathcal{O}_K/q\mathcal{O}_K$ (resp. from $\mathcal{O}/q\mathcal{O}$) and e is sampled from the distribution χ. The RLWE (resp. PLWE) distribution is the probability distribution whose support is the set of all possible RLWE (resp. PLWE samples) and its probability function is that induced from the uniform and from the χ distributions in their respective sets.

The RLWE (resp. PLWE) problem consists in giving an adversary access to arbitrarily many samples of the RLWE (resp. PLWE) distribution and asking the adversary to recover s with non-negligible advantage.

Remark 1.2 First, it is worthy to mention that the random variables χ used to define both problems are discretized versions of multivariate centred Gaussian distributions (for details see [13, Section 2]). Second, Definition 1.1 is the definition of RLWE/PLWE in *search version*. Moreover, the original definition for the RLWE distribution in [13] is built upon the image by the canonical embedding of $\mathcal{O}_K^\vee$, the dual of the ring of integers $\mathcal{O}_K$. However, as proved in [14], this dual-based definition is equivalent to the non-dual one we provide here. We are using this version as starting point, as, being equivalent to the dual one, it is more suitable for our arguments. Moreover, we refer the reader to [13] for the *decisional version* of the problem.

In [15], a polynomial time reduction is given from worst case SVP over ideal lattices to the PLWE problem for power-of-two cyclotomic fields. Later, in [13] ideal-SVP polynomial

[1] Note that several different choices for the distribution of s (*i.e.,* the secret key distribution) are commonly used in practice, particularly in homomorphic encryption. These choices include the error distribution χ itself, ternary and binary distributions over $\mathcal{O}_K/q\mathcal{O}_K$ (resp. $\mathcal{O}/q\mathcal{O}$), as well as distributions that produce sparse elements from $\mathcal{O}_K/q\mathcal{O}_K$ (resp. $\mathcal{O}/q\mathcal{O}$). For more details on the distributions typically used for s in homomorphic encryption, we refer the reader to [11, 12].

time reduction was established for RLWE over cyclotomic fields under flexible conditions on the security parameters and further, in [16] the polynomial reduction was extended to non-cyclotomic Galois number fields building on the same number-theoretical kind of arguments as in [13].

While the RLWE problem is formulated in terms of the ring of integers $\mathcal{O}_K$ of an algebraic number field K, the use of more concrete ring structures is usually more suitable for cryptographic implementations. In particular, the PLWE problem provides a very convenient choice supporting efficient arithmetic [15, 17].

A natural and important question which arises with PLWE is to understand under which conditions it is equivalent to RLWE, in particular in the case where K is the splitting field of $f(x)$ and hence $\mathcal{O}_K$ is isomorphic (by evaluation at a root) to a sub-order in the ring $\mathbb{Z}[x]/(f(x))$. More formally, following [14], [18] and [19] we recall the notion of equivalence:

Definition 1.3 (Equivalence) For a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$, denote by K its splitting field. We say that the RLWE and PLWE problems are equivalent if there exists an algorithm which takes any RLWE sample into a PLWE sample and viceversa in probabilistic polynomial time in the degree of K, incurring in a noise increase which is also polynomial in the degree of K. Following [14], the noise increase caused by the change of embeddings (coefficient embedding in the quotient ring and evaluation followed by canonical embedding in the ring of integers) is measured by the condition number of the corresponding matrix. We will develop this in more detail in Subsection 3.1.

Notice that even if the quotient rings $\mathbb{Z}[x]/(f(x))$ and $\mathcal{O}_K$ were isomorphic (*i.e.,* when K is monogenic), the problems might not be equivalent. Indeed, evaluation at a root of $f(x)$ followed by the canonical embedding takes PLWE samples to RLWE samples in polynomial time using, for instance, Horner's polynomial evaluation and as for the reverse algorithm, solving the corresponding Vandermonde system by Gaussian elimination takes about n^3 operations where n is the degree of K. However, the noise distribution on the canonical embedding size might be so twisted after evaluation that an admissible PLWE sample might be taken into a non-admissible RLWE sample if the noise gets amplified beyond a certain threshold.

The term *admissible* refers here to the fact that decryption reverses encryption. Hence, this algorithm must cause a distortion into the error distribution which is, at most, also polynomial in the degree of the underlying number field.

For those PLWE instantiations where there is an affirmative answer for this equivalence, RLWE hardness results straightforwardly apply to the corresponding PLWE-based implementation. Although it is known [20] that this equivalence holds for the widely used case of PLWE under $\mathbb{Z}[x]/(x^m+1)$ (with m a power-of-two) and RLWE under power-of-two cyclotomic fields,[2] it has been recently shown that the same relation does not hold in general for arbitrary cyclotomic number fields [21]. Additionally, a series of works [14, 18–20, 22] have explored in detail this relation for different types of number fields and quotient polynomial rings: (1) In [14] the authors show their equivalence for an ad hoc family of polynomials, (2) for the cyclotomic scenario there are some positive results showing the equivalence if

[2] The transformation between RLWE and PLWE samples is a scaled isometry for power-of-two cyclotomic number fields.

the number of distinct primes dividing the conductor[3] is kept uniformly bounded [18], and finally, (3) there are also positive results for a family of finite abelian $\mathbb{Q}$-extensions [19, 23].

Main objectives Consequently, *a better understanding of the required conditions for the equivalence between PLWE and RLWE* is not only an interesting research topic by itself, but also turns out to be fundamental to provide a wider catalogue of PLWE instantiations for the designers of cryptographic implementations. *This corresponds to the first objective of this work*.

Our second goal addresses the study of the polynomial multiplication, a building block affecting the speed of cryptographic primitives based on RLWE and, specifically, its use in homomorphic encryption. In particular, we discuss to what extent the broadly used Residue Number System representation (definition given in the next Section 2) interferes with the RLWE-PLWE equivalence for most of families of number fields used to back homomorphic encryption primitives. As a way to overcome this tradeoff, we propose the use of a new family of number fields which we have baptised as *cyclo-multiquadratic*. It is worth remarking that, while cyclo-multiquadratics can enhance the performance of this underlying building block, it also comes with limitations. We elaborate more on the possible tradeoffs in following sections.

1.3 Our contributions

First, we give refined polynomial upper bounds for the condition number of the Vandermonde matrix corresponding to the RLWE-to-PLWE transformation for cyclotomic number fields with up to 6 primes dividing the conductor. These bounds are much sharper than the general one given in [18, Thm. 3.10] and extend the results of Section 4 therein. The proof of these bounds has been postponed to the appendix, to ease the reading of our work.

Second, in Thm. 3.16 we give an exact formula for the condition number of the RLWE-to-PLWE transformation for any cyclotomic number field, but where the usual power basis is replaced by the twisted power basis,[4] and justify why this basis is preferable to the usual one in homomorphic encryption applications. Furthermore, we compare the condition number for different cyclotomic fields with our predicted bounds. We consider conductors up to 10^6, divisible by up to 6 different primes and with general conductors of that magnitude (Fig. 2).

Third, we introduce cyclo-multiquadratic number fields and justify why they are interesting as a tool to grant RLWE/PLWE equivalence, while also providing arithmetic efficiency when applying the Residue Number System representation. In particular, we prove in Prop. 4.4 and Cor. 4.5 that, under very general assumptions on the parameters set, RLWE and PLWE are equivalent for this family with at most a sub-quadratic noise increase under the twisted power basis embedding. We note that, despite this efficiency improvement, the noise increase remains slightly higher than that of the widely considered case of power-of-two cyclotomics. We elaborate further on this comparison in Section 2.

Finally, in Subsection 4.1 we introduce and justify a hybrid embedding (usual power basis on the multiquadratic part twisted by the usual power basis in the cyclotomic side), and

[3] The conductor of the n-th cyclotomic field is n. In the present work we will not use this notion for other number fields.

[4] The formal definition of the twisted basis can be found in Definition 3.10. It is worth noting that it is also referred to as the powerful basis in the literature [7].

likewise we prove RLWE/PLWE equivalence in Thm. 4.6 by using the sharper bounds for the condition number mentioned in the first paragraph.

1.4 Organisation of our work

In Section 2 we revise the Residue Number System (RNS) representation and how this tool serves to speed up the arithmetic in relevant polynomial rings. Likewise, we also discuss the need for modern HE schemes to swap between representations, and how this causes a logarithmic increase in the computational complexity. A natural question which arises is whether there exists a more efficient representation, a question answered in [24, 25] by the second author in the affirmative for the family of the so called *multiquadratic* number fields. We recall that, however, for this family the RLWE and PLWE problems are not equivalent, being this the reason for which we introduce a new family: the cyclo-multiquadratric number fields.

In Section 3 we recall some algebraic number theoretical tools to make the paper self-contained. In particular, we discuss the Kronecker product in some detail, as we will make use of it in a decisive manner. We also introduce the twisted power basis, discuss several results on the equivalence on cyclotomic number fields and show, with the help of the Kronecker product, that if we replace the usual power basis by the twisted power basis, the cyclotomic ring of integers admits a lattice structure for which RLWE and PLWE become equivalent for arbitrary degree.

In Section 4 we study the arithmetic of cyclo-multiquadratic number fields and show the equivalence of the RLWE and PLWE problems for this family, as well as we discuss how it keeps the computational efficiency. Finally, in the Appendix we give the proof of several sharp bounds for the condition number of cyclotomic fields whose conductor is divisible by at most six different primes, a result which we use in Section 4.

2 Homomorphic encryption and cyclo-multiquadratic fields

The majority of the efficiency improvements that PLWE brings about are strongly related to the algebraic structure of the used quotient polynomial ring $R = \mathbb{Z}[x]/(f(x))$. The most common choice is to have $f(x) = \Phi_n(x)$, the n-th cyclotomic polynomial. For the sake of exposition, we will simplify here things a little bit and consider that PLWE-based ciphertexts are composed of an unknown number of polynomial elements belonging to the ring $R_q = \mathbb{F}_q[x]/\Phi_n(x)$. Instead of making use of the coefficient representation, an adequate selection of the ciphertext modulus q makes $\Phi_n(x)$ to split into linear factors,[5] which enables us to use the Chinese Remainder Theorem (CRT) as a means to efficiently operate with polynomials. While polynomial multiplication with the coefficient representation presents an asymptotic cost of $\mathcal{O}(\phi(n)\log\phi(n))$, this cost is reduced to $\mathcal{O}(\phi(n))$ under a CRT representation; hence being linear in the degree of the involved polynomials [7]. Consequently, as PLWE-based primitives usually require to deal with a relatively high degree of the underlying number field, this alternative representation is widely used because it reduces the effect of the logarithmic factor in each polynomial multiplication.

This CRT tool is useful to speed up any type of PLWE-based primitive and, in particular, it results to be fundamental to accelerate homomorphic encryption. In this scenario, the CRT

[5] In particular, $\Phi_n(x)$ decomposes into $\phi(n)$ distinct linear factors over $\mathbb{F}_q[x]$ if and only if $q \equiv 1 \pmod{n}$.

is not only applied at the "ciphertext" layer by choosing an adequate modulo q, but also at the "plaintext" layer where an adequate plaintext modulo allows to batch several integers (usually refered as "slots") in only one encryption (as many as $\phi(n)$ slots per ciphertext). In addition to reducing cipher expansion with respect to plaintext size, this CRT isomorphism enables Single Instruction, Multiple Data (SIMD) operations directly over encrypted integer vectors [26]. Many of the most recent libraries dealing with homomorphic cryptography, such as TFHE-rs [6] and TFHE [27], HElib [28], Lattigo [29], NFLlib [30], PALISADE [7] (currently updated and included inside the OpenFHE library [31]) and SEAL [32] take advantage of different variants of this tool to optimize polynomial operations. Specifically, the BFV implementation of HElib and PALISADE uses a double-CRT representation and works over general cyclotomic number fields. This representation applies a first CRT to split the cyclotomic polynomial, and a second CRT over $\mathbb{F}_q$ to factor the coefficients of the polynomials depending on the prime-power-decomposition of the modulus q. The rest of implementations are specialized for power-of-two cyclotomic fields: (1) Libraries implementing the FHEW/TFHE [33, 34] scheme usually make use of a Discrete Fourier Transform (DFT) representation by means of efficient Fast Fourier Transform (FFT) computations over complex numbers. (2) BFV and CKKS implementations [35, 36] with $f(x) = x^m + 1$ make use of a CRT–NTT representation (where NTT stands for Number Theoretic Transform), in which a CRT is applied over all coefficients in $\mathbb{F}_q$, while a negacyclic NTT is applied to split $f(x)$ in linear factors. See Fig. 1 for a toy example of this representation.[8]

Hence we see that the quotient polynomial ring $\mathbb{Z}_q[x]/(x^m + 1)$ is the preferred choice by current libraries, as it enables efficient implementations of polynomial operations through previously computing fast radix[9] algorithms of the DFT and NTT [30, 39]. Also important, polynomial operations over the plaintext ring naturally correspond to basic blocks in practical signal processing applications [40–42], comprising, among others, linear convolutions, filtering, and linear transforms.

2.1 Non-polynomial operations and RNS representation

In the community of computer arithmetic, the CRT representation described above is also referred to as Residue Number System (RNS). The benefits of staying in the CRT-NTT representation are not only asymptotic. The factorization into several terms produced by the CRT over $\mathbb{F}_q$ enables to fit the computation flow into the underlying machine word, with the consequent improvement on practical performance.

Unfortunately, the current state-of-the-art in HE, represented by schemes as CKKS and BFV, also makes an intensive use of other non-polynomial operations which are not entirely compatible with the CRT–NTT representation. One clear example is the case of coefficient rounding/rescaling, which is usually performed at the end of each ciphertext multiplication.

While there are several strategies to apply this rounding while staying in the first CRT decomposition [35, 36], currently there are no equivalent results for its negacyclic NTT counterpart. This means that whenever we execute a non-polynomial operation over each

[6] TFHE-rs: Pure Rust implementation of the TFHE scheme for boolean and integers FHE arithmetics, https://github.com/zama-ai/tfhe-rs.

[7] PALISADE Homomorphic Encryption Software Library, https://palisade-crypto.org/.

[8] In Fig. 1, the Hadamard product between vectors $\boldsymbol{a}$ and $\boldsymbol{b}$ is denoted as $\boldsymbol{a} \circ \boldsymbol{b}$. Example extracted from [37].

[9] For a DFT/NTT of composite size, radix-type algorithms recursively express the transform in terms of a series of DFTs/NTTs of smaller size. The term radix here usually refers to the smallest factor considered in the recursive decompositions [38].

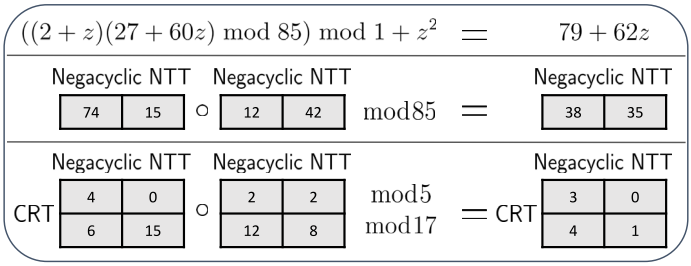


Fig. 1 Toy example of the CRT-NTT representation

polynomial coefficient, we have to swap between NTT and coefficient-wise representations, which presents an asymptotic cost of $\mathcal{O}(m \log m)$ elementary multiplications and $\mathcal{O}(m \log m)$ elementary additions by means of efficient FFT-type algorithms.

2.2 Efficient conversion between coefficient and CRT–NTT representation

The inherent logarithm increase in computational cost which appears when swapping between CRT-NTT (or double-CRT) and coefficient representations is already contemplated in [43], where the authors pose the question of *whether there is a more compact representation that can be converted to double-CRT in linear time.*

Interestingly, this question can be answered in the affirmative for a concrete family of non-cyclotomic number fields, coined in [24, 25] as multiquadratic number fields. Those works show how the convolution property displayed by these rings is compatible with a particular NTT transform, whose shape is related to a number theoretic version of the Walsh-Hadamard Transform (WHT). This transform can be very efficiently computed with a variant of the Fast Walsh-Hadamard transform algorithm (FWHT), which requires a total of $\mathcal{O}(m \log m)$ elementary additions but only $\mathcal{O}(m)$ elementary multiplications. Consequently, by substituting the polynomial ring $R = \mathbb{Z}[x]/(x^m + 1)$ by the ring $R = \mathbb{Z}[x_1, ..., x_r]/(x_1^2 + d_1, \ldots, x_r^2 + d_r)$ in the PLWE formulation (with $m = 2^r$), we can now take advantage of the different algebraic structure introduced by these multiquadratic rings. In practice, this means that we can swap between NTT and coefficient representations in linear time with respect to the number of elementary multiplications.

The benefits of this structure do not only amount to providing more efficient polynomial arithmetic [24], but it also introduces interesting improvements for homomorphic slot manipulation by adding new strategies and storage/computation tradeoffs for relinearization and linear matrix operations. All these benefits build on the natural hypercube structure of its group of automorphisms, which is the direct product $\underbrace{(\mathbb{Z}_2, +) \times \cdots \times (\mathbb{Z}_2, +)}_{r}$, where $m = 2^r$ is the dimension of the corresponding multivariate number field. Contrarily, the hypercube structure considered in other works dealing with cyclotomic number fields [44–46] relies on the group $\mathbb{Z}_m^*/(p)$, where extra homomorphic operations are required to address "bad" dimensions [28]. These are dimensions where more than one automorphism is needed to rotate their slots.[10]

[10] HElib distinguishes between two types of "bad" dimensions: those referred to as "bad" and those called "very bad." The difference lies in the degree of perturbation that the application of automorphisms causes to the slots of the dimension. We refer the reader to [28] for further details.

2.3 Another non-cyclotomic family: Cyclo-multiquadratic fields

The reduction from worst-case ideal lattice problems to RLWE [16] also applies to multiquadratic number fields, namely, those of the form $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r})$, whenever an adequate choice of $\{d_1, \ldots, d_r\}$ parameters is made [25]. Hence, we can efficiently swap between polynomial coefficients and CRT–NTT representations with linear multiplicative complexity, while still backing up security on the hardness of RLWE, and consequently, answering in the affirmative the question posed in [43] regarding swapping "double-CRT" representations in linear time.

Delving now into its RLWE-PLWE relation, here we observe how the RLWE and PLWE problems defined, respectively, over multivariate number fields $\mathbb{Q}(\sqrt{d_1}, \ldots, \sqrt{d_r})$ and multivariate quotient polynomial rings $R = \mathbb{Z}[x_1, ..., x_r]/(x_1^2+d_1, \ldots, x_r^2+d_r)$ are not equivalent in the sense we informally stated previously. Actually, *the algorithm transforming RLWE samples into PLWE samples and vice versa does not cause a polynomial distortion in the error distribution, but instead quasi-polynomial*. In view of this, one last objective of this work is to explore related number field families where (1) the RLWE-PLWE equivalence still holds, and (2) the swapping between CRT–NTT representations is still more efficient than in the widespread cyclotomic case.

To this aim, we explore a non-cyclotomic family of number fields defined as the compositum of cyclotomic and multiquadratic fields [25] (see Section 4), which we refer to as cyclo-multiquadratic number fields in the present work. We find particular instantiations of this family which satisfy the RLWE/PLWE equivalence while still providing better concrete efficiency than cyclotomics when swapping between double-CRT representations. Unfortunately, it does seem to be the case that, *to have "polynomial" RLWE/PLWE equivalence, we have to resign to have asymptotic linear complexity in the double-CRT transformation*. We elaborate more on these tradeoffs next.

Tradeoff for hybrid cyclo-multiquadratic rings Our work suggests the existence of different concrete practical tradeoffs between the (1) "polynomial/quasi-polynomial" RLWE-PLWE equivalence and (2) "quasi-linear/linear" complexity for the double-CRT transform applied to all polynomial elements in cyclo-multiquadratic rings. For example, some simple parameters' choices already give more efficient double-CRT transforms than cyclotomic rings. This is done by decomposing m, the total field dimension, in terms of both its multiquadratic and cyclotomic subfields[11] as $m = m_{cyclo}m_{mult} = m^{1/l}m^{1-1/l}$, where the parameter l controls the relative dimensions provided by each subfield.

It can be seen that, in the above expression, for $l = \log m$ we have linear multiplicative complexity $\mathcal{O}(m)$, while for $l = \sqrt{\log m}$, we have $\mathcal{O}(m\sqrt{\log m})$ multiplicative complexity (see Appendix B.1 for further details). This complexity is obtained by combining the use of FFT-type and FWHT-type algorithms for, respectively, the cyclotomic and multiquadratic subfield dimensions. Unfortunately, only a quasi-polynomial RLWE/PLWE equivalence remains in both cases. We refer the reader to Appendix B.1 for a detailed explanation of the complexity of this algorithm and the PLWE-RLWE equivalence for this choice of parameters.

On the contrary, Section 4 shows that, by means of Prop. 4.4, sub-quadratic RLWE–PLWE equivalence can be achieved for cyclo-multiquadratic rings if $m_{cyclo} = 2^u$ and $m_{mult} = 2^r$ with $u = r^{1+1/l}$ for fixed $l \geq 2$. Also, by allowing a more generic conductor on the cyclotomic

[11] Here m_{cyclo} is the dimension of the cyclotomic subfield, and m_{mult} is the dimension of the multiquadratic subfield.

side, we can still grant a polynomial condition number, with moderately low degree, as we prove in the last subsection (see Thm. 4.6). If we compare again cyclo-multiquadratic rings with the case of cyclotomics, the multiplicative complexity of the double-CRT transform approaches an improvement by a factor of $\frac{r+r^{1+1/l}}{r^{1+1/l}}$, while still keeping the RLWE-PLWE polynomial equivalence. In short, whenever we work with large enough r, but in a range where we still have $l \gg r$ for this choice of parameters (or more precisely, $r^{1/l}$ is close enough to 1), swapping between representations can be achieved approximately twice faster (*i.e.,* with a constant improvement by a factor of 2). It is also worth mentioning that, if we define $m_{mult} = 2^{cr}$ for a fixed constant $c \geq 1$, then, whenever we work in the range $l \gg r$ with large enough r, the swapping between representations is approximately $c+1$ times faster. We refer the reader to Appendix B.2 for a detailed description of the achievable improvements in terms of c, r and l.

Some remarks in the practical impact of cyclo-multiquadratics The previous claimed efficiency improvements require further clarifications from our side. First, we note that while the improvement factor of $c+1$ is achieved with $l \gg r$ and large enough r, a wider range of values, even with $l \approx r$ and $c = 2$, can still give reasonable improvements in the multiplicative complexity. To see this, we delve into the improvement given by the exact expression for the cost ratio[12] from Appendix B.2.1:

$$\mathsf{Mult}_{\mathsf{CostRatio}}(2^{r^{1+1/r}}, 2^{2r}) \geq 1 + \frac{2}{r^{\frac{1}{r}}} - \frac{3}{r^{1+\frac{1}{r}}},$$

for which if we select $l \approx r$ such that $\log m = \lceil r(2+r^{\frac{1}{r}}) \rceil$, and choose some practical values for m as for example $\{2048, 16384, 131072\}$, then we get an improvement in the multiplicative complexity of respectively $\approx \{1.69, 1.88, 2.01\}$. We refer the reader to Appendix B.2 for more details on the influence of c, r and l on the cost ratio.

Second, although it is clear that this type of rings introduces some theoretical improvements in the multiplicative complexity of polynomial operations, in practice they can also present a higher noise expansion factor after ciphertext multiplication. Consequently, to homomorphically evaluate a circuit with the same multiplicative depth, the modulo q considered in the polynomial coefficients of ciphertexts built with cyclo-multiquadratics will be bigger than those built with only power-of-two cyclotomics. These tradeoffs were already discussed with specific parameters for the extreme case of the non-dual ring version of multiquadrics and low-depth circuits in [24]. Delving into the concrete complexity of FFT algorithms, the computational cost of current FFT-based NTTs with power-of-two cyclotomics [47] consists of $\frac{m}{2}\log_2 m$ elemental multiplications and $m \log_2 m$ elemental additions. In contrast, multiquadratic rings [25] eliminate the logarithmic component in the number of multiplications, resulting in a total of m elemental multiplications and $m \log_2 m$ elemental additions. Therefore, the *cyclo-multiquadratic rings presented in our work precisely allow to explore hybrid intermediate parameterizations achieving a smaller modulo q than multiquadratics and a faster arithmetic efficiency than cyclotomics*.

In particular, for the parameter choices previously discussed (see Cor. 4.5) and by combining FFT-type and FWHT-type algorithms (see Appendix B.1), we can swap representations in cyclo-multiquadratics with a total cost that approximates $\frac{m}{2(c+1)}\log_2 m$ elemental multiplications and $m \log_2 m$ elemental additions. This is achieved for a range of field dimensions m where, for a large enough r, we have $r^{1/l} \approx 1$, and where c controls the relative size of

[12] We have considered here that the multiplicative cost of the FFT for cyclotomics is $\mathsf{Mult}_{\mathsf{FFT}}(m) = m \log_2 m$. See Appendix B.1 for further details.

the multiquadratic component. Thus, although all cyclotomics, multiquadratics, and cyclo-multiquadratics require the same number of additions, we obtain a constant improvement in the multiplicative complexity when compared to cyclotomics. It is important to mention that if the cost of additions is comparable to the cost of multiplications, the $m \log_2 m$ elemental additions dominate the total cost, and the improvement is significantly reduced.

From a theoretical point of view, lower bounds of $\mathcal{O}(m)$ linear multiplicative complexity [38] are known for the case of FFTs over complex and real numbers (*i.e.,* DFT computation). Although we could not find a concrete calculation of the complexity regarding the number of additions, they grow very rapidly and become excessive even for very small values of m (*e.g.,* $m = 32$ for the case of real numbers [48]). This is due to the fact that these solutions reduce the number of multiplications by implementing rational constants through additions, a method that does not seem applicable to the NTT over finite rings, as we are not aware of any algorithm that can compute NTTs with $\mathcal{O}(m)$ multiplicative complexity. Regarding the additive complexity, no FFT algorithm has managed to reduce the number of additions below $m \log_2 m$ [38].

Finally, while an exhaustive analysis of the concrete impact of applying cyclo-multiquadratics in current homomorphic constructions and libraries goes beyond the scope of this work, we briefly list here the factors we believe are the most relevant regarding its practical performance:

- *Number of swapping between representations*: When the number of swappings (NTT/INTT transforms) required by implementations is high, a slight increase in error noise is not the most significant factor affecting efficiency performance.
- *Hardware architecture*: These rings help to minimize the number of elemental multiplications, which is particularly beneficial when such multiplications are considerably more expensive than additions.

As we can see, not only these factors are challenging to adequately characterize, but they also depend heavily on the type of application and hardware under which homomorphic encryption is used. In future work we intend to study in detail the influence of these factors on the concrete tradeoffs and performance offered by cyclo-multiquadratics, by also comparing with current libraries and constructions.

3 Algebraic background

For a field extension L/F, denote as usual by $\mathrm{Gal}(L/F)$ the corresponding Galois group, namely, the group of field automorphisms of L which fix F.

Two field extensions L/F and M/F are said to be linearly disjoint if $L \cap M = F$. In that case, denoting by LM the compositum of both extensions, it is well known that

$$Gal(LM/F) \cong Gal(L/F) \times Gal(M/F). \tag{3.1}$$

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 θ. The evaluation-at-θ map is a field $\mathbb{Q}$-isomorphism $\mathbb{Q}[x]/(f(x)) \cong K$.

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

The extension $K/\mathbb{Q}$ is said to be Galois if K is the splitting field of $f(x)$. Denoting by s_1 the number of real embeddings, *i.e.,* those whose image is contained in $\mathbb{R}$, and by s_2 the number of pairs of complex non-real embeddings, one has $n = s_1 + 2s_2$.

For $z \in \mathbb{C}$, denote by z^* its complex conjugate. We will make use of the metric space

$$\Lambda_n := \left\{ (x_1, ..., x_n) \in \mathbb{R}^{s_1} \times \mathbb{C}^{2s_2} \middle| \begin{matrix} x_{s_1+i} = x^*_{s_1+s_2+i} \\ \text{for } 1 \leq i \leq s_2 \end{matrix} \right\},$$

endowed with the inner product induced by the usual one in $\mathbb{C}^n$.

Definition 3.1 The canonical embedding $\sigma_K : K \to \Lambda_n$ is the ring monomorphism defined as:

$$\sigma_K(x) := (\sigma_1(x), ..., \sigma_n(x)),$$

where the addition and product on the left are those of the field K and on the right are defined componentwise. When K is clear from the context we will write σ instead of σ_K.

By a lattice in Λ_n, we will understand, as usual, a pair (L, ι) where L is a finitely generated and torsion free group and $\iota : L \hookrightarrow \Lambda_n$ is a group monomorphism. We will only deal with full rank lattices, namely, those whose rank is precisely n.

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. We will assume that K is monogenic, namely, that $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some $\theta \in K$. It is well known (see for instance [49]) that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, thus for each ideal $I \subseteq \mathcal{O}_K$ the pair (I, σ) is a full rank lattice in Λ_n.

Definition 3.2 An ideal lattice is a lattice (L, ι) such that $\iota(L) = \eta(I)$ for I an ideal of a ring R and $\eta : R \hookrightarrow \Lambda_n$ a ring monomorphism (the product in Λ_n being defined componentwise).

Denoting $\mathcal{O} := \mathbb{Z}[x]/(f(x))$, we can embed this ring as a lattice into $\mathbb{R}^n$ in a different manner:

Definition 3.3 The coordinate embedding of $\mathcal{O}$ is

$$\begin{matrix} \sigma_{C,K} : \mathcal{O} \to \mathbb{R}^n \\ \sum_{i=0}^{n-1} a_i \overline{x}^i \mapsto (a_0, a_1, ..., a_{n-1}), \end{matrix}$$

where $\overline{x}$ denotes the class of x modulo $f(x)$. When K is clear from the context we will write σ_C instead of $\sigma_{C,K}$.

The evaluation at θ map composed with the canonical embedding V_f transforms the lattice $(\mathcal{O}, \sigma_C)$ to the lattice $(\mathcal{O}_K, \sigma)$:

$$\begin{matrix} V_f : \mathcal{O} \to & \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_n(\mathcal{O}_K) \\ \sum_{i=0}^{n-1} a_i \overline{x}^i \mapsto & \begin{pmatrix} 1 & \theta_1 & \cdots & \theta_1^{n-1} \\ 1 & \theta_2 & \cdots & \theta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_n & \cdots & \theta_n^{n-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}, \end{matrix}$$

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

We will also deal with a third embedding, more suitable for certain applications: the twisted coordinate embedding, which we present next.

Suppose that $f(x)$ and $g(x)$ are two irreducible monic polynomials with integer coefficients of degrees n and m respectively and with no common roots. Denote by $K_f \cong \mathbb{Q}[x]/(f(x))$ and $K_g \cong \mathbb{Q}[x]/(g(x))$ their corresponding splitting fields, which we assume

monogenic, so that $\mathcal{O}_{K_f} \cong \mathbb{Z}[x]/(f(x))$ and $\mathcal{O}_{K_g} \cong \mathbb{Z}[x]/(g(x))$. Denoting by K_{fg} the compositum $K_f K_g$, we have:

$$\begin{aligned}\mathbb{Z}[x, y]/(f(x), g(y)) &\cong \mathbb{Z}[x]/(f(x)) \otimes_{\mathbb{Z}} \mathbb{Z}[y]/(g(y)) \\ &\cong \left\{ \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} a_{i,j} \overline{x}^i \overline{y}^j, a_{i,j} \in \mathbb{Z} \right\}, \end{aligned} \tag{3.2}$$

where $\overline{x}$ and $\overline{y}$ are, respectively, the class of x modulo $f(x)$ and the class of y modulo $g(y)$.

Definition 3.4 The twisted coordinate embedding of $\mathbb{Z}[x, y]/(f(x), g(y))$ is

$$\begin{aligned}\sigma_{T,K} : \mathbb{Z}[x, y]/(f(x), g(y)) &\to \mathbb{R}^{nm} \\ \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} a_{i,j} \overline{x}^i \overline{y}^j &\mapsto (a_{i,j})_{i,j=0}^{n,m}. \end{aligned}$$

3.1 The condition number and the Kronecker product

For a matrix $A \in \mathrm{M}_n(\mathbb{C})$, denote by $||A||$ its Frobenius norm, namely, $||A|| = \sqrt{Tr(AA^*)}$, where A^* is the transposed conjugated matrix of A and Tr denotes the matrix trace.

Definition 3.5 For a matrix $A \in \mathrm{GL}_n(\mathbb{C})$, the condition number of A is defined as

$$\mathrm{Cond}(A) := ||A||||A^{-1}||,$$

where $||A||$ is the Frobenius norm of A (see [19] Subsection 2.3 for more details).

The condition number of V_f measures the noise amplification caused by sending PLWE samples to RLWE samples and vice-versa. For further clarification on the requirements that must be applied to the condition number to ensure the equivalence between the PLWE and RLWE problems, we refer the reader to Subsection 1.2, particularly to Definition 1.3.

Definition 3.6 For two matrices $A = (a_{ij})_{i,j=1}^{m,n} \in \mathrm{M}_{m\times n}(\mathbb{C})$ and $B = (b_{ij})_{i,j=1}^{p,q} \in \mathrm{M}_{p\times q}(\mathbb{C})$ the Kronecker product $A \otimes B$ is the $\mathrm{M}_{pm\times qn}(\mathbb{C})$ block matrix

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix}.$$

A standard computation shows that if A, B, C, and D are matrices such that the products AC and BD are defined, then

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD). \tag{3.3}$$

As a consequence we have:

Lemma 3.7 *Given square matrices $A \in M_p(\mathbb{C})$ and $B \in M_q(\mathbb{C})$, the matrix $A \otimes B$ is invertible if and only if A and B are invertible and in this case:*

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}.$$

The next lemma is proved in a straightforward manner and shows that the Kronecker product also behaves nicely with respect to the Frobenius norm

Lemma 3.8 *Given $A \in M_p(\mathbb{C})$ and $B \in M_q(\mathbb{C})$, we have:*

$$||A \otimes B|| = ||A||||B||.$$

As a corollary, the Kronecker product satisfies the following property with respect to the condition number:

Corollary 3.9 *Given $A \in GL_p(\mathbb{C})$ and $B \in GL_q(\mathbb{C})$, we have:*

$$\mathrm{Cond}(A \otimes B) = \mathrm{Cond}(A)\mathrm{Cond}(B).$$

Proof First, from Lemma 3.8 we have:

$$||A \otimes B|| = ||A||||B||.$$

Secondly, from Lemma 3.7 we have:

$$||(A \otimes B)^{-1}|| = ||A^{-1} \otimes B^{-1}|| = ||A^{-1}||||B^{-1}||,$$

hence the result follows. □

3.2 Cyclotomic fields. First facts.

For $n \geq 2$, let us denote by $\Phi_n(x)$ the n-th cyclotomic polynomial, namely, the minimal polynomial of a primitive n-th root of unity ζ_n. As well known, its degree is $m := \phi(n)$, where ϕ is Euler's totient function, namely, $\phi(n)$ is the number of positive integers coprime to n and less than or equal to n. For $n = p_1^{k_1} \ldots p_r^{k_r}$, denote $\mathrm{rad}(n) := p_1 \ldots p_r$ and $\omega(n) := r$, the number of different prime divisors of n. Let us denote by K_n the n-th cyclotomic field, namely, the splitting field of $\Phi_n(x)$, and by $\mathcal{O}_{K_n}$ its ring of integers. It is also well known that $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta_n]$. The cyclotomic extension $K_n/\mathbb{Q}$ is Galois and its Galois group is

$$Gal(K_n/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* .$$

Moreover, since the extensions $K_{p_1^{k_1}}/\mathbb{Q}$,...,$K_{p_r^{k_r}}/\mathbb{Q}$ are linearly disjoint, from (3.1) we have

$$\mathrm{Gal}(K_n/\mathbb{Q}) \cong \mathrm{Gal}(K_{p_1^{k_1}}/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(K_{p_r^{k_r}}/\mathbb{Q}). \tag{3.4}$$

For K_n and K_m with n and m coprime, write $N = \phi(n)$ and $M = \phi(m)$ so that $K_n = \mathbb{Q}(\zeta_n)$ and $K_m = \mathbb{Q}(\zeta_m)$. Let $\{\zeta_{n,i}\}_{i=1}^N$ be the set of the N conjugated primitive n-th roots of unity, which is a $\mathbb{Q}$-basis of K_n and $\{\zeta_{m,i}\}_{i=1}^M$ the set of the M conjugated primitive m-th roots of unity, which analogously is a $\mathbb{Q}$-basis of K_m.

On the other hand, the set $\{1, \zeta_n, ..., \zeta_n^{N-1}\}$ is also a $\mathbb{Q}$-basis of K_n and the set $\{1, \zeta_m, ..., \zeta_m^{M-1}\}$ is also a $\mathbb{Q}$-basis of K_m and since the extensions are linearly disjoint, the set $\{\zeta_n^i \zeta_m^j\}_{i,j=0}^{N-1,M-1}$ is a $\mathbb{Q}$-basis of $K_n K_m = K_{nm}/\mathbb{Q}$.

Definition 3.10 The twisted basis of K_{nm} (also called *powerful basis* [7]) is the basis $\{\zeta_n^i \zeta_m^j\}_{i,j=0}^{N-1,M-1}$. Notice that this basis is different to the usual power basis $\{(\zeta_n \zeta_m)^k\}_{k=0}^{NM-1}$.

Lemma 3.11 *The twisted basis of K_{nm} is also a $\mathbb{Z}$-basis of $\mathcal{O}_{K_{nm}}$.*

Proof Clearly $\zeta_n \zeta_m \in \mathbb{Z}[\zeta_n^i \zeta_m^j]$ hence $\mathcal{O}_{K_{nm}} \subseteq \mathbb{Z}[\zeta_n^i \zeta_m^j]$. Now, $\zeta_n = \zeta_{nm}^m$ and $\zeta_m = \zeta_{nm}^n$ hence $\zeta_n, \zeta_m \in K_{nm}$. Hence, $\zeta_n^i \zeta_m^j \in K_{nm}$ for every i and j. Since these elements are algebraic integers the result follows. □

Now, due to (3.1), we have

$$\mathrm{Gal}(K_n K_m/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^*, \tag{3.5}$$

where an element $[i, j]$ of the right hand side of (3.5) acts on $K_n K_m$ as $[i, j](\zeta_n \zeta_m) := \zeta_n^i \zeta_m^j$.

Definition 3.12 Denote $V_{K_n} = \left(\zeta_{n,i}^l\right)_{1\le i,l+1\le N}$ and $V_{K_m} = \left(\zeta_{m,j}^k\right)_{1\le j,k+1\le N}$. The twisted Vandermonde matrix for the extension K_{nm} is

$$TV_{K_{nm}} := V_{K_n} \otimes V_{K_m}.$$

Notice that V_{K_n} corresponds to the change from the coordinate-to-canonical embedding of K_n and analogously with V_{K_m}. Hence the twisted Vandermonde matrix $TV_{K_{nm}}$ corresponds to the change from the twisted coordinate embedding-to-canonical embedding of K_{nm} with respect to the twisted basis of K_{nm}.

3.3 Condition numbers of cyclotomic fields

The investigation of the condition number of the Vandermonde matrices attached to cyclotomic fields has been the study of a good number of articles in the R/P-LWE literature. First of all, it is straightforward to check that for power of two conductor, the Vandermonde matrix is a scaled isometry. In [20], the authors deal with the case of conductor p and $2p$ with p prime. Recently, the following result gives a closed formula for the case of conductor $2^k p^l$:

Theorem 3.13 *([50], Thm. 3.2) Let $n = p^k$, where p is any prime number and k is a positive integer, or $n = 2^k p^l$, where $p > 2$ is prime and k and l are positive integers. Denote by V_{Φ_n} the Vandermonde matrix corresponding to the coordinate to canonical embedding transformation for O_{K_n}. Then*

$$\mathrm{Cond}(V_{K_n}) = \phi(n)\sqrt{2\left(1 - \frac{1}{p}\right)}.$$

Moving to a conductor which is the product of more primes is not at all a straightforward task. For instance, in [18] the author gives the asymptotic upper bound:

Theorem 3.14 *([18] Thm. 3.10) Let $n \ge 2$ and denote by $A(n)$ the largest coefficient, in absolute value, of $\Phi_n(x)$. Denote $m = \phi(n)$ as usual. If $\mathrm{rad}(n) = p_1 \ldots p_k$, then:*

$$\mathrm{Cond}(V_{\Phi_n}) \le 2\,\mathrm{rad}(n) n^{2^k+k+2} A(n).$$

In particular, if we restrict to families of conductors (a) divisible for at most k primes (k fixed) and (b) if we can grant that $A(n)$ grows polynomially in n, then the condition number grows polynomially for this family. In particular, [18] gives a much more refined formula for conductors divisible by up to three primes. We have extended this formula for products of up to six primes. We give the statement next and postpone the proof for the Appendix A:

Proposition 3.15 *For $n \ge 2$ and $m := \phi(n)$, the following upper-bounds hold for the condition number of V_{Φ_n}:*

a) If $n = p^k$, then

$$\mathrm{Cond}(V_{\Phi_n}) \le 4m^2.$$

b) If $n = p^l q^s r^t$ *with* $l, s, t \geq 0$, *denoting by* ε *the number of primes diving* n *with positive power, then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^{\varepsilon-1} m^2.$$

c) If $n = p^a q^b r^c s^d$, *then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^4 m^2.$$

d) If $n = p^a q^b r^c s^d t^e$ *and* $m = \phi(n)$, *then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^7 m^2.$$

e) If $n = p^a q^b r^c s^d t^e u^f$, *then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^{11} m^2.$$

The results provided in Prop. 3.15 are particularly useful for defining secure parameters in practical applications, such as those relying on the HElib library [44, 51], which operates with quotient cyclotomic rings under the power basis and where n is the product of several prime powers. For example, HElib is used in several practical applications that work with n composed of up to three primes, including homomorphic building of logistic regression models [52] and the homomorphic execution of AES encryption/decryption circuits [53]. Any improvement in the bounds provided in Prop. 3.15 would have immediate implications for the choice of tighter cyclotomic PLWE-based cryptosystem parameters. However, things are much easier if we replace the usual power basis by the twisted basis. In this case, we are changing, first, the usual coordinate embedding by the twisted coordinate embedding and second, even if the image of the transformation is again the canonical embedding of the ring of integers, the basis is again different. Even so, as we pointed out, for many applications it is preferable to work under the twisted canonical embedding instead of the usual canonical embedding. In particular, we have:

Theorem 3.16 *For* $n = p_1^{k_1} \ldots p_r^{k_r}$ *we have*

$$\mathrm{Cond}(TV_{K_n}) = \phi(n)\sqrt{2}^r \sqrt{\prod_{i=1}^{r}\left(1 - \frac{1}{p_i}\right)}.$$

Proof Since the $K_{p_i^{k_i}}$ are linearly disjoint, from (3.4) we have

$$TV_{K_n} = V_{p_1^{k_1}} \otimes \cdots \otimes V_{p_r^{k_r}},$$

From Corollary 3.9 we have

$$\mathrm{Cond}(TV_{K_n}) = \mathrm{Cond}(V_{p_1^{k_1}}) \cdots \mathrm{Cond}(V_{p_r^{k_r}}).$$

The result now follows from Theorem 3.13. □

Contrariwise to the case of Theorem 3.14, where we needed to impose a constant number of primes dividing the conductor, we can see by Theorem 3.16 that, if we work with PLWE under the twisted basis, the condition number grows polynomially even for the case of conductors divisible by a growing number of primes. Consequently, choices of n where $r = \mathcal{O}(\log n)$ give still the equivalence of RLWE/PLWE under the twisted basis. Nevertheless, even though we can obtain an exact expression for the condition number of cyclotomics under the twisted basis, many applications still utilize the power basis and/or both [28]. This highlights the

importance of obtaining sufficiently tight upper bounds for the condition number under both the power and twisted bases, not only in cyclotomics but also in the more general cases discussed in Section 4 for the proposed cyclo-multiquadratics (see Cor. 4.5 and Thm. 4.6).

As far as we currently know, we could only find in [28] some related numerical bounds for both cyclotomic power and twisted basis. Their results focus on the infinity norm of the linear transformation from RLWE to PLWE, for which they provide some empirical results for the power basis with up to 5 primes dividing n. For the aim of exposition of our results, we have compared in several figures all the expressions and upper bounds for the condition number from Thm 3.14, Prop. 3.15 and Thm 3.16.[13] Figures 2a, 2c, 2d, 2e, 2f, 2g compare all provided expressions,[14] but each figure specifically considers a different number of primes dividing the conductor: Fig. 2a considers 1 prime, Fig. 2c considers 2 primes, Fig. 2d considers 3 primes, Fig. 2e considers 4 primes, Fig. 2f considers 5 primes and Fig. 2g considers 6 primes. Then, Fig. 2b represents the particular case of $n = 2^l p^d$ by comparing the expressions from Thm. 3.14, Prop. 3.15 and Thm. 3.16 with the closed formula from Theorem 3.13. Finally, Fig. 2h compares the condition number without any restriction for n, by considering the expressions for power (from Thm. 3.14) and twisted basis (from Thm. 3.16).

Note that all figures are log-log plots, so polynomial functions appear approximately as linear functions in which the slope is equal to the maximum degree of the polynomial. Then, it is easy to see how, for Figures 2a, 2b 2c, 2d, 2e, 2f, 2g, in which the number of primes dividing n is keep constant, the refined upper bounds from Prop. 3.15 grow much slower than the ones from Thm. 3.14. In all these cases, the analogous expression for the twisted basis given in Thm. 3.16 is the slowest, by growing approximately linear in n.

In general, this difference among expressions increases when we have a higher number of different primes dividing n, and finally, it becomes more evident in Fig. 2h, where we do not fix the number of primes. For this more general case, the upper bound for the usual power basis from Thm. 3.14 presents a double exponential in the number of primes, and hence, it grows considerably faster than the expression for the twisted basis given in Thm. 3.16.

4 Cyclo-multiquadratic fields

A multiquadratic field is a number field of the form $\mathbb{Q}(\sqrt{d_1}, ..., \sqrt{d_r})$ with $d_i \in \mathbb{Z}$ square-free. In this section we will deal with totally real multiquadratic fields, namely, $d_i \geq 2$ for $1 \leq i \leq r$. We are interested in the interplay between cyclotomic and totally real multiquadratic fields. In particular, let $n \geq 2$ be fixed and let us take r different primes $p_1, p_2, ..., p_r$ such that $p_i \nmid n$ for each i. Denote $K := K_n(\sqrt{p_1}, ..., \sqrt{p_r})$.

Proposition 4.1 *For the extensions $K_n/\mathbb{Q}$ and $K/\mathbb{Q}$, we have*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(K_n/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}) \times \ldots \times \mathrm{Gal}(\mathbb{Q}(\sqrt{p_r})/\mathbb{Q}).$$

Proof First, we observe that the extensions $K_n/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}$ are linearly disjoint: otherwise it would be $K_n \cap \mathbb{Q}(\sqrt{p_1}) = \mathbb{Q}(\sqrt{p_1})$ hence $\mathbb{Q}(\sqrt{p_1}) \subseteq K_n$. In that case, the prime p_1, which ramifies in $\mathbb{Q}(\sqrt{p_1})$, would ramify in K_n, which is a contradiction since $p_1 \nmid n$. The

[13] Note that, for Thm. 3.14, we represent the upper bound for $\mathrm{Cond}(V_{\Phi_n})$ divided by $A(n)$, *i.e.,* $\mathrm{Cond}(V_{\Phi_n})/A(n)$. It is actually a lower bound of the expression given for $\mathrm{Cond}(V_{\Phi_n})$ in that theorem.

[14] The used code is publicly available at https://github.com/apedrouzoulloa/cyclomultiquadratic.

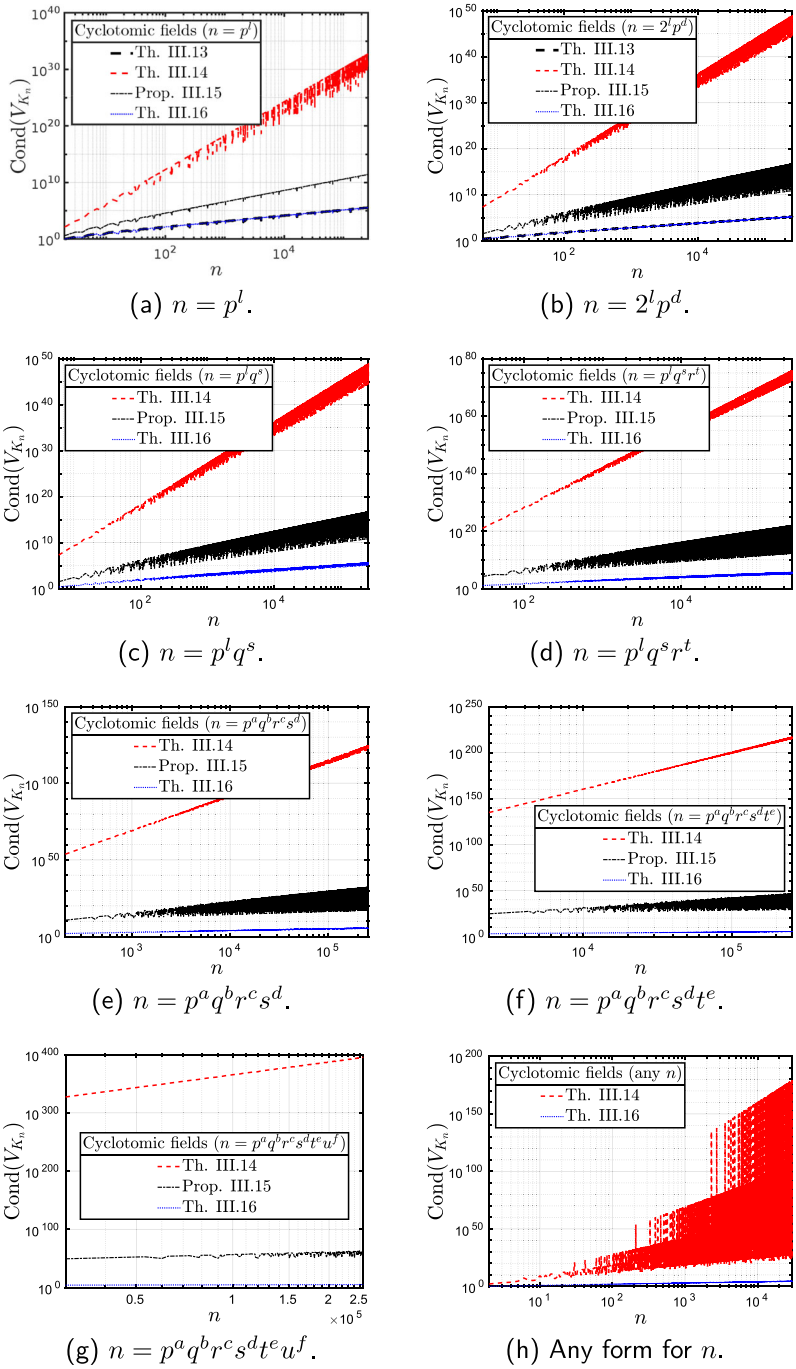


Fig. 2 Condition number of cyclotomic fields in terms of (1) different forms for n, and (2) use of conventional power basis or twisted basis

same argument applies to the extensions $K_n\mathbb{Q}(\sqrt{p_1})/\mathbb{Q}(\sqrt{p_1})$ and $\mathbb{Q}(\sqrt{p_1},\sqrt{p_2})/\mathbb{Q}(\sqrt{p_1})$ to show that they are linearly disjoint, and the statement for arbitrary $r > 1$ follows by induction. Finally, by using (3.1) the result holds. □

Double-CRT with cyclo-multiquadratic rings Our focus in this section is to discuss the conditions for the equivalence between RLWE and PLWE for this family of fields. This equivalence is described in terms of zero characteristic rings, which is why arithmetic modulo q is not explicitly considered in the main results of this section (Cor. 4.5 and Thm. 4.6). However, returning to our discussion in Section 2 about efficient polynomial arithmetic, double-CRT is always possible for cyclo-multiquadratic rings. In general, we need a chain of prime moduli $q'_1,\ldots,q'_L$ such that $q = \prod_i q'_i$, although for simplicity, we first assume that q is prime in our explanation.

Unlike the cyclotomic rings discussed in Section 2, where we work with polynomial rings of the form $\mathbb{Z}_q[x]/\Phi_n(x)$, in the case of cyclo-multiquadratics, we consider a multivariate polynomial quotient ring of the form $R_q = \mathbb{Z}_q[x_0,x_1,\ldots,x_r]/(\Phi_n(x_0),x_1^2-p_1,\ldots,x_r^2-p_r)$. In addition to the coefficient representation, cyclo-multiquadratic rings also support a CRT representation [25] if the prime modulus q makes each factor $\Phi_n(x_0), x_1^2-p_1,\ldots,x_r^2-p_r$ split into linear factors. Specifically, q must satisfy several simultaneous conditions:

- $\Phi_n(x_0)$ splits if $q \equiv 1 \pmod n$.
- For all i, $x_i^2 - p_i$ splits if p_i is a quadratic residue modulo q.

To verify the latter condition, we can use the Legendre symbol, which is defined for an odd prime q as $\left(\frac{p_i}{q}\right) = p_i^{\frac{q-1}{2}} \bmod q$. In summary, besides $q \equiv 1 \pmod n$ (as is required for cyclotomic rings), the double-CRT representation for cyclo-multiquadratic rings also requires $\left(\frac{p_i}{q}\right) = 1$ for all i. Finally, in the more general case where q is the product of several primes q'_j, we require that, for all i and j, $n \equiv 1 \pmod{q'_j}$ and $\left(\frac{p_i}{q'_j}\right) = 1$.

Condition number for cyclo-multiquadratics To alleviate notation, from now on, and unless stated otherwise, by the notation $\otimes$ we will understand the usual tensor product $\otimes_{\mathbb{Z}}$. Denote, as in the previous section, $\mathcal{O}_n = \mathbb{Z}[x]/(\Phi_n(x))$ and set $\mathcal{O}_{\sqrt{p_i}} := \mathbb{Z}[x]/(q_i(x))$, where $q_i(x)$ is the minimal polynomial of $\sqrt{p_i}$, namely, $q_i(x) = x^2 - p_i$ if $p_i \equiv 2,3 \pmod 4$ and $q_i(x) = x^2 - x + \frac{1-p_i}{4}$, the minimal polynomial of $\frac{1+\sqrt{p_i}}{2}$ otherwise. Recall that for a quadratic number field $\mathbb{Q}(\sqrt{d})$, where d is square-free, its ring of integers is given by $\mathbb{Z}[\varepsilon_d]$. Here, $\varepsilon_d = \sqrt{d}$ when $d \neq 1 \pmod 4$, and $\varepsilon_d = \frac{1+\sqrt{d}}{2}$ otherwise, as shown in [49, Thm. 3.3]. Since we need to distinguish between these two cases in the computation of condition numbers below, let us instead denote

$$\varepsilon_i = \begin{cases} \sqrt{p_i} & \text{if } p_i \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{p_i}}{2} & \text{if } p_i \equiv 1 \pmod 4. \end{cases}$$

Setting $\mathcal{O} := \mathbb{Z}[x]/(\Phi_n(x)) \otimes \mathbb{Z}[x]/(q_1(x)) \otimes \cdots \otimes \mathbb{Z}[x]/(q_r(x))$, we have:

Lemma 4.2 *Succesive evaluations at ζ_n, $\varepsilon_1,\ldots\varepsilon_r$ yield an isomorphism*

$$\mathcal{O} \cong \mathcal{O}_K.$$

Proof Denote by $\mathcal{O}_{K_n}$ the ring of integers of K_n and notice that $\mathcal{O}_{\sqrt{p_i}}$ isomorphic to the ring of integers of $\mathbb{Q}(\sqrt{p_i})$. Since the respective evaluation maps are isomorphisms between the

quotient rings and the corresponding ring of integers and since all these are free $\mathbb{Z}$-modules, succesive evaluations at ζ_n, ε_1,...ε_r give an isomorphism

$$\mathcal{O} \cong \mathcal{O}_{K_n} \otimes \mathcal{O}_{\sqrt{p_i}} \otimes \cdots \otimes \mathcal{O}_{\sqrt{p_r}}.$$

Moreover, since the extensions are linearly disjoint and the gcd of all the discriminants is 1, by [54, Thm. 4.26] we have

$$\mathcal{O}_{K_n} \otimes \mathcal{O}_{\sqrt{p_i}} \otimes \cdots \otimes \mathcal{O}_{\sqrt{p_r}} \cong \mathcal{O}_K.$$

□

Hence, by Prop. 4.1 the twisted coordinate embedding reads as:

$$\begin{aligned} \sigma_{T,K} : \mathcal{O} &\to \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_{2^r m}(\mathcal{O}_K) \\ \sum_{i=0}^{2^r m-1} a_i \overline{x}^i &\mapsto TV_K \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^r m-1} \end{pmatrix}, \end{aligned} \tag{4.1}$$

where, as in the previous section

$$TV_K := TV_{K_n} \otimes V_{p_1} \otimes ... \otimes V_{p_r},$$

with

$$V_{p_i} = \begin{cases} \begin{pmatrix} 1 & \sqrt{p_i} \\ 1 & -\sqrt{p_i} \end{pmatrix} \text{ if } p_i \equiv 2, 3 \pmod 4 \\ \begin{pmatrix} 1 & \frac{1+\sqrt{p_i}}{2} \\ 1 & \frac{1-\sqrt{p_i}}{2} \end{pmatrix} \text{ if } p_i \equiv 1 \pmod 4. \end{cases}$$

Hence, we have:

$$\mathrm{Cond}(V_{p_i}) = \begin{cases} \sqrt{p_i} + \frac{1}{\sqrt{p_i}} \text{ if } p_i \equiv 2, 3 \pmod 4 \\ \frac{5}{2\sqrt{p_i}} + \frac{\sqrt{p_i}}{2} \text{ if } p_i \equiv 1 \pmod 4. \end{cases} \tag{4.2}$$

The following upper bound follows directly from (4.2):

Corollary 4.3 *For each prime number $p \geq 2$, it holds*

$$\mathrm{Cond}(V_p) \leq 2 + \sqrt{p}.$$

Hence, as a direct consequence of Corollary 3.9 and Theorem 3.13, we have:

Proposition 4.4 *With notation as above:*

$$\mathrm{Cond}(TV_K) \leq \phi(n) 2^{\frac{\omega(n)}{2}} \prod_{i=1}^{r} \left(2 + \sqrt{p_i}\right).$$

We can hence conclude that

Corollary 4.5 *For $n \geq e^e$ we have*

$$\mathrm{Cond}(TV_K) \leq \phi(n) n^{\alpha} \prod_{i=1}^{r} \left(2 + \sqrt{p_i}\right) \text{ with } \alpha = 0.2076.$$

Proof In [55, Thm. 11 pag. 369], it is proved that for $n \geq 3$ it holds

$$\omega(n) \leq 1.3841 \frac{\log(n)}{\log\log(n)}.$$

The result follows from this upper bound and from Proposition 4.4. □

Now, the idea is to choose n and the primes $p_1,...,p_r$ in such a way that

$$\mathrm{Cond}(TV_K) = O((m2^r)^k), \text{ with } m = \phi(n), \tag{4.3}$$

and with uniformly upper bounded (and *small*) k, say $0 \leq k \leq 4$, so that for suitable large enough choices of n and r we can grant that the distortion caused by the RLWE-PLWE correspondence is polynomial in the degree of the number field, which is a sort of balance between noise and security. We need to recall, first, the straightforward inequality

$$n \leq 2\phi(n)^2, \text{ for each } n \geq 1.$$

Actually, if $n = 2^a m$ with $a \neq 1$, then $n \leq \phi(n)^2$.

For (4.3) to hold, it is enough that we can grant that in the large

$$(1+2\alpha)\log(m) + \sum_{i=1}^{r} \log\left(2+\sqrt{p_i}\right) \cong k(\log(m) + r\log(2)),$$

or equivalently

$$k = \lim_{m,r\to\infty} \frac{(1+2\alpha)\log(m) + \sum_{i=1}^{r} \log\left(2+\sqrt{p_i}\right)}{\log(m) + r\log(2)}, \tag{4.4}$$

whenever this limit exists.

If, for instance, we take the popular choice $n = 2^{u+1}$ and $p_i =$ the i-th prime (with $i > 1$), the right hand side of (4.4), before taking limit, can be upper bounded by

$$\frac{(1+2\alpha)u\log(2) + r\log\left(2+\sqrt{p_r}\right)}{u\log(2) + r\log(2)} \tag{4.5}$$

Since, by the Prime Number Theorem, a reasonable approximation for the r-th prime is $p_r \cong r\log(r)$, for u and r large enough, (4.5) can be fairly approximated by

$$\frac{(1+2\alpha)u\log(2) + r\log(2+\sqrt{r\log(r)})}{u\log(2) + r\log(2)}.$$

Moreover, if in addition $u\log(2) \gg r\log(2+\sqrt{r\log(r)})$, namely, if

$$\lim_{u,r\to\infty} \frac{u\log(2)}{r\log(2+\sqrt{r\log(r)})} = \infty,$$

then we have:

$$k \leq 1 + 2\alpha = 1.4152.$$

For instance, if $u \sim r^{1+1/l}$ for fixed $l \geq 2$, then we obtain a sub-quadratic upper-bound for the condition number.

Some extra remarks on the condition number and double-CRT To obtain the upper bounds in Cor. 4.5 (and also in Thm. 4.6 for Subsection 4.1) for the condition number of cyclo-multiquadratics, we consider its ring of integers $\mathcal{O}_K$ (see Lemma 4.2). However, it is

important to mention that $\mathcal{O}_K$ does not, in general, have the same form as the one used for the existence of the double-CRT in $R_q = \mathbb{Z}_q[x_0, x_1, \ldots, x_r]/(\Phi_n(x_0), x_1^2 - p_1, \ldots, x_r^2 - p_r)$.

Some quotients $q_i(x_i)$ of $\mathcal{O}_K$ take the form $q_i(x_i) = x_i^2 - x_i + \frac{1-p_i}{4}$ if $p_i \equiv 1 \pmod 4$. Following [25], in this situation, we must simply apply a map from $\mathcal{O}_K$ to R_q, where for all x_i such that $p_i \equiv 1 \pmod 4$:

- Substitute $x_i \to \frac{x_i+1}{2}$ in the two polynomial elements of the PLWE sample $(a, b = as + e) \in \mathcal{O}_K^2$.
- Multiply both polynomial elements of the PLWE sample by 2.

As a result, we obtain transformed PLWE samples $(\tilde{a}, \tilde{b}) \in R_q^2$. The transformation applied to each x_i such that $p_i \equiv 1 \pmod 4$ can also be seen as a multiplication by the matrix $M = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}$, with $\mathrm{Cond}(M) = 3$. Thus, we have $\mathrm{Cond}(M^{-1} V_{p_i}) \leq 3 \left(\frac{5}{2\sqrt{p_i}} + \frac{\sqrt{p_i}}{2} \right)$. The use of the double-CRT when the number field has primes $p_i \equiv 1 \pmod 4$ implies that the term $\sqrt{p_i}$ in the upper bound given in Cor. 4.3 is multiplied by $\frac{3}{2}$. Since this increase in the upper bound does not affect the results obtained in Cor. 4.5 and Thm. 4.6, which still hold in this case, we have preferred not to account for this constant factor in the exposition for simplicity.

4.1 A hybrid embedding

Setting as before $K = K_n \mathbb{Q}(\sqrt{p_1}) \cdots \mathbb{Q}(\sqrt{p_r})$, observe that, in the previous subsection, we have evaluated the elements of the multivariate quotient ring at the powerful basis on the cyclotomic side, at the generators of the quadratic fields on the multiquadratic side and then, we have applied the canonical embedding. We recall that this approach allows us to obtain a sub-quadratic condition number. However, if the conductor n of the cyclotomic part is divisible by several primes, the ring of integers of the cyclotomic field is isomorphic to the quotient ring $\mathbb{Z}[x]/(\Phi_n(x))$ but also to a multivariate quotient polynomial ring (Lemma 3.11 together with (3.2)).

Hence, if the coordinates of the samples are given with respect to the usual power basis instead of the powerful basis, it is the Vandermonde matrix V_{K_n} the one whose condition number we must upper bound, as the transformation between PLWE and RLWE is, in this case, evaluation at the usual power basis on the cyclotomic side, evaluation at the generators of the quadratic fields on the multiquadratic side and followed by the canonical embedding.

Namely, the corresponding embedding for the whole cyclo-multiquadratic field would be

$$\begin{aligned} \sigma'_{T,K} : \mathcal{O} &\to \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_{2^r m}(\mathcal{O}_K) \\ \sum_{i=0}^{2^r m-1} a_i \overline{x}^i &\mapsto TV'_K \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^r m-1} \end{pmatrix}, \end{aligned} \tag{4.6}$$

where now

$$TV'_K = V_{K_n} \otimes V_{p_1} \otimes \ldots \otimes V_{p_r}.$$

In the context of cyclotomic rings where the conductor n is divisible by several primes, PLWE samples under the powerful basis (see Thm. 3.16) typically exhibit a significantly smaller condition number compared to PLWE samples under the power basis (see Prop. 3.15). This raises the question of the relevance and utility of providing in this section upper bounds

and conducting analyses under the cyclotomic power basis, as opposed to exclusively using the powerful basis. While some works, such as [56], which focuses on an implementation of CKKS with a conductor composed of two primes, consider only the cyclotomic powerful basis, it is important to recognize that certain HE libraries make use of both basis depending on the specific algorithm being executed. For instance, in the BGV implementation of HElib [28], the power basis is employed during modulus switching, key switching, and encryption, whereas the powerful basis is used in other operations such as decryption.

Thus, in practice, it may also be valuable to consider the power basis when working with the cyclotomic part K_n of the proposed cyclo-multiquadratic rings in K.

Denoting by $c(n)$ the condition number of K_n, we have that

$$\mathrm{Cond}(TV'_K) \leq c(n) \prod_{i=1}^{r} \left(2 + \sqrt{p_i}\right)$$

As in the previous subsection, we will choose $p_i =$ the i-th prime number, where we do not explicitly exclude the $\omega(n)$ primes p_i that divide n because this does not significantly affect the approximation used for the size of the primes. In this case, if we want

$$\mathrm{Cond}(TV'_K) = O((m2^r)^k), \tag{4.7}$$

we need to have

$$k = \limsup_{m,r\to\infty} \frac{\log(c(n)) + \sum_{i=1}^{r} \log\left(2 + \sqrt{p_i}\right)}{\log(m) + r\log(2)}, \tag{4.8}$$

As we have pointed out in the previous section, in [21] it is shown that $c(n)$ is not polynomial for general $n \geq 2$. However, if we stick to a conductor divisible by a bounded number of primes, we can grant that $c(n)$ essentially grows polynomially with $\mathrm{rad}(n)$.

Next, we will assume that $\omega(n) \leq 6$ and will use Proposition 3.15 to give an explicit formula for (4.8) to grant (4.7).

First, assume that $\omega(n) \leq 3$. Then, the right hand side of the equality (4.8), before taking limit, is upper bounded by

$$\frac{\log(4) + 2\log(m) + (\omega(n) - 1)\log(\phi(\mathrm{rad}(n)))}{\log(m) + r\log(2)} + \frac{r\log\left(2 + \sqrt{r\log(r)}\right)}{\log(m) + r\log(2)}. \tag{4.9}$$

As in the previous subsection, we impose that

$$r\log(\sqrt{r\log(r)}) \ll \log(m),$$

namely, that $\lim_{r,m\to\infty} \frac{r\log(\sqrt{r\log(r)})}{\log(m)} = 0$.

If $\omega(n) = 1$, the upper limit of (4.9) is indeed the limit and we have

$$k = \lim_{r,m\to\infty} \frac{\log(4) + 2\log(m)}{\log(m) + r\log(2)} + \frac{(\omega(n) - 1)\log(\phi(\mathrm{rad}(n))) + r\log\left(2 + \sqrt{r\log(r)}\right)}{\log(m) + r\log(2)} = 2.$$

If $1 < \omega(n) \leq 3$, we observe that $\frac{\log(\phi(\mathrm{rad}(n))}{\log(m)} \leq 1$, but the limit of this expression may not exist in general. However, it is still true that $\limsup_{n\to\infty} \frac{\log(\phi(\mathrm{rad}(n))}{\log(m)} = 1$. Hence

$$k = \limsup_{r,m\to\infty} \frac{\log(4) + 2\log(m)}{\log(m) + r\log(2)} + \frac{(\omega(n) - 1)\log(\phi(\mathrm{rad}(n))) + r\log\left(2 + \sqrt{r\log(r)}\right)}{\log(m) + r\log(2)} \leq 4.$$

For $\omega(n) = 4$, we have

$$k = \limsup_{r,m\to\infty} \frac{\log(4) + 2\log(m) + 4\log(\phi(\mathrm{rad}(n)))}{\log(m) + r\log(2)} + \frac{r\log\left(\sqrt{2 + r\log(r)}\right)}{\log(m) + r\log(2)} \leq 6,$$

and for $\omega(n) = 5$ we obtain

$$k = \limsup_{r,m\to\infty} \frac{\log(4) + 2\log(m) + 7\log(\phi(\mathrm{rad}(n)))}{\log(m) + r\log(2)} + \frac{r\log\left(\sqrt{2 + r\log(r)}\right)}{\log(m) + r\log(2)} \leq 9.$$

Finally, for $\omega(n) = 6$ we obtain

$$k = \limsup_{r,m\to\infty} \frac{\log(4) + 2\log(m) + 11\log(\phi(\mathrm{rad}(n)))}{\log(m) + r\log(2)} + \frac{r\log\left(\sqrt{2 + r\log(r)}\right)}{\log(m) + r\log(2)} \leq 13.$$

Altogether, we have proved the following:

Theorem 4.6 *Let $K = K_n\mathbb{Q}(\sqrt{p_1}, \cdots, \sqrt{p_r})$ with p_r =the r-th prime and $m = \phi(n)$. Assume that we choose n and r such that $\lim_{r,m\to\infty} \frac{r\log(\sqrt{r\log(r)})}{\log(m)} = 0$. Then, we have:*

- *If $\omega(n) \leq 3$, then*
$$\mathrm{Cond}(TV'_K) = O((2^r m)^{2+\omega(n)-1}).$$
- *If $\omega(n) = 4$, then*
$$\mathrm{Cond}(TV'_K) = O((2^r m)^6).$$
- *If $\omega(n) = 5$, then*
$$\mathrm{Cond}(TV'_K) = O((2^r m)^9).$$
- *If $\omega(n) = 6$, then*
$$\mathrm{Cond}(TV'_K) = O((2^r m)^{13}).$$

The results from Thm. 4.6 and Prop. 3.15 enable a fair comparison of the condition numbers obtained for cyclotomics and cyclo-multiquadratics that follow our parameters' indications. By fixing the same equivalent field dimension for both cases, we observe that the incorporation of the multiquadratic part does not substantially increase the condition number. Moreover, although at first glance the results provided in Cor. 4.5 and Thm. 4.6 seem to indicate that it is always better to work under the twisted basis for the cyclotomic part of cyclo-multiquadratic rings, we remind the reader that several practical applications in homomorphic encryption (HE) based on PLWE with cyclotomics utilize both the cyclotomic power and powerful basis [52, 53]. Both applications are implemented in the HElib library [44, 51], which employs either basis depending on the specific step executed within the HE primitive. We note, however, that HElib [43] employs a more general notion of the basis, considering n-th cyclotomic fields where n decomposes into pairwise coprime integers. In contrast, our work with the twisted basis focuses on decomposing n into different prime powers, enabling a more detailed analysis of the condition number. Still, it is worth mentioning that Definition 3.10 provides a formulation of the twisted basis that accommodates this more general context, bridging the gap between these two approaches.

Some discussions on the impact of cyclo-multiquadratics Once we have introduced our two main results on the condition number for cyclo-multiquadratics in Cor. 4.5 and Thm. 4.6,

we return to the discussion in Section 2 regarding the practical efficiency improvements introduced by cyclo-multiquadratics.

In general, we observe that these rings can provide a constant improvement in the multiplicative computational cost when swapping between NTT and coefficient representations. Nevertheless, as noted in Cor. 4.5, these rings also produce a slight increase in noise distortion compared to the cyclotomic counterparts with the same field dimension. Due to this increase, maintaining RLWE worst-case hardness, according to the invulnerability condition stated in [57], requires adding extra noise to the PLWE samples. In practice, this implies selecting a larger modulus q, which could reduce the efficiency gains discussed in Section 2.

As previously discussed in the comparison between the cyclotomic power and powerful basis, the HElib library makes use of both in different steps of the BGV implementation [28]. Moreover, several practical applications implemented with the BGV scheme of HElib consider cyclotomics with an order n that is the product of three distinct primes [52, 53], for which Prop. 3.15 shows that the condition number grows as a polynomial of degree 4. In contrast, as demonstrated in Cor. 4.5 and Thm. 4.6, the inclusion of the multiquadratic part in cyclo-multiquadratics results in a much smaller increase in the condition number, even remaining sub-quadratic in the total field dimension for the case discussed in Cor. 4.5.

Thus, although the required modulus q would be slightly larger than in the ideal scenario with power-of-two cyclotomics, the noise distortion remains significantly smaller than that produced in the general cyclotomic rings currently implemented in practical applications. This high-level analysis seems to indicate that, despite the need for a larger modulus q, the benefits of cyclo-multiquadratics would remain. Nevertheless, we emphasize that this analysis is qualitative, and a more detailed study is needed, as many factors can influence its practical efficiency (see Subsection 2.3), which is beyond the scope of this work.

For more concrete examples of the increase in q caused by only multiquadratics, we refer to [24], where an additive homomorphic scheme based on RLWE is instantiated. Despite requiring larger ciphertexts compared to RLWE with power-of-2 cyclotomics, the scheme still achieved improved efficiency for its primitives. The solutions proposed in Cor. 4.5 and Thm. 4.6 aim precisely to find a middle ground, producing smaller ciphertexts than in the multiquadratic case while still improving the efficiency of the basic building blocks.

5 Conclusions

We have started discussing in Sections 1 and 2 why the CRT is useful to speed up homomorphic encryption. In most applications, CRT is applied both on plaintexts and ciphertexts, hence enabling SIMD operations directly over encrypted integer vectors. We have also pointed out how several widely used homomorphic schemes, such as CKKS and BFV, use other non-polynomial operations, like coefficient rounding/rescaling, which are not entirely compatible with the CRT–NTT representation. Because of this, when running a non-polynomial operation, one has to swap between NTT and coefficient-wise representations, which presents an asymptotic cost of $\mathcal{O}(m \log m)$ elementary multiplications. This led us to address the question whether or not there is a more compact representation that can be converted to double-CRT in linear time.

We recall previous investigation of the second author, where the multiquadratic family was introduced, answering that question in an affirmative manner. However, a new difficulty appears in this setting since the RLWE and PLWE problems for multiquadratic fields are not

equivalent, which led us to introduce the cyclo-multiquadratic family studied in the present work.

For this family, we have proved that (a) we have RLWE–PLWE equivalence if we consider the twisted power basis in the cyclotomic part, for every choice of conductor, and (b) we have equivalence under the hybrid embedding if the conductor of the cyclotomic part is divisible for up to 6 different primes. As an auxiliary tool, we have obtained refined bounds for the condition number of cyclotomic Vandermonde matrices which are much sharper than existing ones, by making use of recent results in analytic number theory.

As a result, we have shown that our family of cyclo-multiquadratic fields speeds up the efficient swapping between NTT and CRT representations by a factor of at least two under the twisted power basis while keeping the RLWE–PLWE equivalence.

Finally, we discussed how a fair and exhaustive evaluation of the concrete efficiency offered by these rings in current libraries is not straightforward. In future work, we intend to explore in detail the existing tradeoffs and determine for which range of concrete parameters and applications, cyclo-multiquadratics could yield practical improvements in current constructions. Furthermore, it would be interesting to investigate, as a future research direction, how the noise tolerance in HElib might be improved by replacing the power basis with the twisted basis.

Appendix Proof of proposition 3.15

Here we give the proof of Proposition 3.15 for the cases $\omega(n) = 4$, 5 and 6 (the cases $\omega(n) \leq 3$ are dealt with in [18] Theorems 4.1, 4.3 and 4.6). Denote $m := \phi(n)$ for $n \geq 2$ and $k := \omega(n)$.For $n \geq 2$, if $n = p_1^{r_1} \cdots p_k^{r_k}$ is its prime factorisation, denote $\mathrm{rad}(n) := p_1 \cdots p_k$.

First of all, observe that for $n \geq 2$ we have that $n \leq 2\phi(n)^2$. Actually, if $n = 2^a m$ with $a \neq 1$, indeed $n \leq \phi(n)^2$.

We will need the following facts about cyclotomic polynomials, whose proof can be found in [58] Chapter 2:

Proposition A.1 *Let $n = pr$ with p prime and $p \nmid r$.Then*

$$\Phi_n(x) = \frac{\Phi_r(x^p)}{\Phi_r(x)}.$$

In addition, if we write $n = p_1^{r_1} \cdots p_l^{r_l}$ with $p_1, \cdots, p_l$ different primes, then

$$\Phi_n(x) = \Phi_{\mathrm{rad}(n)}(x^{\frac{n}{\mathrm{rad}(n)}}).$$

To bound the condition number in the aforementioned cases, notice first that since $||V_{\Phi_n}|| = m$, we only need to upper bound $||V_{\Phi_n}^{-1}||$. To start with, we recall the following result:

Lemma A.1 ([14], Section 4.2) Notations as before, it holds

$$V_{\Phi_n}^{-1} = (w_{ij})$$

with

$$w_{ij} = (-1)^{m-i} \frac{e_{m-i}(\bar{\zeta}_j)}{\prod_{k \neq j}(\zeta_j - \zeta_k)}, \tag{A1}$$

where e_{m-i} is the elementary symmetric polynomial of degree $m - i$ in $m - 1$ variables and $\bar{\zeta}_j = (\zeta_1, \zeta_2, \ldots, \zeta_{j-1}, \zeta_{j+1}, \ldots, \zeta_m)$.

For $n \geq 2$, denote by $A(n)$ the maximum of all the coefficients in absolute value of the cyclotomic polynomial $\Phi_n(x)$. Next, we will use the following result to upper bound the entries of $V_{\Phi_n}^{-1}$:

Proposition A.2 ([18] Proposition 3.7) *For $n \geq 2$, the following upper bound is valid:*

$$|w_{ij}| \leq \mathrm{rad}(n) \frac{A(n)+1}{|\Phi'_{\mathrm{rad}(n)}(\zeta_j^{n/\mathrm{rad}(n)})|}. \tag{A2}$$

In [18] Section 4, the author uses some classical upper upper bounds for $A(n)$, namely, for $\omega(n) \leq 2$, it is well know that $A(n) \leq 1$ while for $\omega(n) = 3$, say, $\mathrm{rad}(n) = pqr$ with $p < q < r$, it holds that $A(n) \leq p-1$. However, for $\omega(n) > 3$ things become more complicated and there is no hope for a general polynomial asymptotic expression for $A(n)$, indeed, Erdös proved that that there exist infinitely many n such that $A(n) \geq e^{e^{\log(2)\log(n)/\log(\log(n))}}$. We can, nevertheless, upper bound the condition number for, at least, $\omega(n) \leq 6$, taking advantage of the following recent result:

Theorem A.4 ([59] Theorem 4) *For any $n \geq 2$, we have:*

- *If $n = pqrst$ with $p < q < r < s < t$, then*

$$A(n) \leq \frac{135 p^7 q^3 r}{512}.$$

- *If $n = pqrstu$ with $p < q < r < s < t < u$, then*

$$A(n) \leq \frac{18225 p^{15} q^7 r^3 s}{262144}.$$

We will also need the following result to lower bound the denominators in Proposition A2:

Lemma A.5 For $4 \leq k \leq 6$ we have

$$\frac{1}{|\phi'_n(\zeta_n)|} \leq 2m^{k-3}.$$

Proof We give the proof for $k = 4$, as the argument is analogue for the rest of cases. So, suppose that $n = pqrs$ with $p < q < r < s$. Using Proposition A.1 we have:

$$\begin{aligned} |\phi'(\zeta_n)| &= \frac{s|\phi'_{pqr}(\zeta_n^s)|}{|\phi_{pqr}(\zeta_n)|} \\ &= \frac{sr|\phi'_{pq}(\zeta_n^{rs})|}{|\phi_{pqr}(\zeta_n)||\phi_{pq}(\zeta_n^s)|} \\ &= \frac{pqrs}{|\phi_{pqr}(\zeta_n)||\phi_{pq}(\zeta_n^s)||\phi_p(\zeta_n^{rs})|\zeta_n^{qrs}-1|}, \end{aligned}$$

hence

$$\begin{aligned} \frac{1}{|\phi'_n(\zeta_n)|} &\leq \frac{2(p-1)^3(q-1)^2(r-1)}{pqrs} \\ &\leq \frac{2(p-1)^2(q-1)}{s} \\ &\leq 2m. \end{aligned}$$

□

A.1 Case $k = 4$

We start by observing that for $m = pqrs$, we have (see [59], pag. 1) $A(m) \leq p(p-1)(pq-1)$ for $p < q < r < s$. Secondly, for any $n \geq 2$, since $\Phi_n(x) = \Phi_{\mathrm{rad}(n)}(x^{n/\mathrm{rad}(n)})$, we have that if $k = 4$, then $A(n) = A(\mathrm{rad}(n)) \leq p(p-1)(pq-1)$ too.

Theorem A.6 *If $m = p^a q^b r^c s^d$, then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^4 m^2.$$

Proof First, we use Prop. A2 to obtain

$$|w_{ij}| \leq pqrs \frac{A(pqrs)+1}{|\Phi'_{pqrs}(\zeta_{pqrs})|}.$$

Now, using Lemma A.5, we get

$$\begin{aligned} |w_{ij}| &\leq 2p^2qrs\phi(\mathrm{rad}(n))(p-1)(pq-1) \\ &\leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^2 \\ &\leq 4\phi(\mathrm{rad}(n))^4. \end{aligned}$$

Thus, we have $||V_{\Phi_n}^{-1}|| \leq 4m\phi(\mathrm{rad}(n))^4$ and the result follows.

A.2 Case $k = 5$

In this case, the result is as follows:

Theorem A.7 *Let $n = p^a q^b r^c s^d t^e$ and $m = \phi(n)$ and $p < q < r < s < t$. Then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^7 m^2.$$

Proof We have, as in the previous case, by using Proposition A2 and Lemma A.5:

$$|w_{ij}| \leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^2(A(\mathrm{rad}(n))+1).$$

Now, by using Theorem A.4, we obtain

$$\begin{aligned} |w_{ij}| &\leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^2 p^7 q^3 r \\ &\leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^2 (q-1)^5 (r-1)^3 (s-1)^3, \end{aligned}$$

which is upper bounded by $2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^5$. Again, since $\mathrm{rad}(n) \leq 2\phi(\mathrm{rad}(n))^2$ the result follows. □

A.3 Case $k = 6$

Finally, for $\omega(n) = 6$ we have:

Theorem A.8 *Let $n = p^a q^b r^c s^d t^e u^f$ and $m = \phi(n)$ and $p < q < r < s < t < u$. Then*

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4m^2\phi(\mathrm{rad}(n))^{11}.$$

Proof As in the previous cases, Proposition A2 and Lemma A.5 give

$$|w_{ij}| \leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^3(A(\mathrm{rad}(n))+1).$$

Now, by using Theorem A.4, we obtain

$$\begin{aligned}|w_{ij}| &\leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^3 p^{15}q^7r^3s\\ &\leq 2\,\mathrm{rad}(n)\phi(\mathrm{rad}(n))^3(q-1)^{15}(r-1)^7(s-1)^3(t-1),\end{aligned}$$

which can be upper bounded as

$$\begin{aligned}|w_{ij}| &\leq 2\phi(\mathrm{rad}(n))^9\,\mathrm{rad}(n)\\ &\leq 4\phi(\mathrm{rad}(n))^{11},\end{aligned}$$

hence

$$\mathrm{Cond}(V_{\Phi_n}) \leq 4\phi(\mathrm{rad}(n))^{11}m^2.$$

□

Notice that if $n = 2^a m$ with $a \neq 1$, then $n \leq \phi(n)^2$ and the upper bounds for the condition number will be $2\phi(\mathrm{rad}(n))^k m^2$ with $k = 4, 7, 11$.

Appendix B HFTs with cyclo-multiquadratic rings

B.1 A combination of FFT and FWHT algorithms for cyclo-multiquadratics

Following the notation indicated in Section 2, we decompose the total field dimension m into the product of the dimensions of both its multiquadratic and cyclotomic subfields as $m = m_{cyclo} \cdot m_{mult} = m^{1/l} \cdot m^{1-1/l}$. The parameter l is used to control the relative dimensions of each subfield, adjusting the balance between cyclotomic and multiquadratic components. For the case of pure cyclotomics (*i.e.,* $m = m_{cyclo}$), an NTT computed by means of FFT algorithms can be run with a cost of $\mathcal{O}(m \log_2 m)$ elemental operations [47]. It is worth noting that, while the number of additions is usually neglected, the best FFT algorithms require a total of $\mathsf{Add}_{\mathsf{FFT}}(m) = m \log_2 m$ additions and $\mathsf{Mult}_{\mathsf{FFT}}(m) = A \cdot m \log_2 m$ multiplications. The constant A accounts for discrepancies in hidden terms and differences across FFT algorithm families.

In order to calculate the analogous multiplicative cost for cyclo-multiquadratics (denoted for size $m = m_{cyclo} \cdot m_{mult}$ as $\mathsf{Mult}_{\mathsf{HFT}}(m_{cyclo}, m_{mult})$, *i.e.,* we call it Hybrid Fast Transform due to its use of both FFTs and FWHTs), we represent the polynomial elements in $R_q = \mathbb{Z}_q[x_0, x_1, \ldots, x_r]/(\Phi_n(x_0), x_1^2 - p_1, \ldots, x_r^2 - p_r)$ as bidimensional arrays, with the length of each dimension corresponding to the degree of each subfield. This allows the application of multidimensional DFT algorithms: first, we compute a sequence of m/m_{cyclo} FFTs over the cyclotomic dimension, followed by m/m_{mult} generalized FWHTs over the multiquadratic dimension.

Let the multiplicative cost of the generalized FWHT [25] of size m_{mult} be denoted as $\mathsf{Mult}_{\mathsf{FWHT}}(m_{mult}) = m_{mult}$. The total multiplicative cost is then given by:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{HFT}}(m_{cyclo}, m_{mult}) &= m_{mult} \cdot \mathsf{Mult}_{\mathsf{FFT}}(m_{cyclo}) + m_{cyclo} \cdot \mathsf{Mult}_{\mathsf{FWHT}}(m_{mult}) \\ &= \frac{m}{m_{cyclo}} \cdot A \cdot m_{cyclo} \log_2 m_{cyclo} + \frac{m}{m_{mult}} \cdot m_{mult} \\ &= m \cdot A \cdot \log_2 m_{cyclo} + m \\ &= m \cdot (1 + A \cdot \log_2 m_{cyclo}).\end{aligned}$$

Therefore, we can calculate the ratio between the cost of FFT-type transforms in cyclotomics and HFT-type transforms in cyclo-multiquadratics as:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &= \frac{\mathsf{Mult}_{\mathsf{FFT}}(m)}{\mathsf{Mult}_{\mathsf{HFT}}(m_{cyclo}, m_{mult})} \\ &= \frac{A \cdot \log_2 m}{1 + A \cdot \log_2 m_{cyclo}} \\ &= \frac{\log_2 m}{1/A + \log_2 m^{1/l}} \\ &= \frac{\log_2 m}{1/A + \frac{\log_2 m}{l}}.\end{aligned}$$

From the above expression, we can see that when $l = \frac{A \cdot \log_2 m}{A-1}$, the ratio $\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult})$ is given by:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &= \frac{\log_2 m}{1/A + \frac{(A-1) \cdot \log_2 m}{A \cdot \log_2 m}} \\ &= \log_2 m.\end{aligned}$$

From this result, we can deduce that $\mathsf{Mult}_{\mathsf{FFT}}(m)$ is $\mathcal{O}(\log_2 m)$ times larger than $\mathsf{Mult}_{\mathsf{HFT}}(m_{cyclo}, m_{mult})$ when $l = \mathcal{O}(\log m)$. Similarly, when $l = \sqrt{\log_2 m}$, we can follow similar steps and see that the ratio is approximately:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &= \frac{\log_2 m}{1/A + \frac{\log_2 m}{l}} \\ &= \frac{\log_2 m}{1/A + \sqrt{\log_2 m}} \\ &\approx \frac{\log_2 m}{\sqrt{\log_2 m}} \\ &\approx \sqrt{\log_2 m}.\end{aligned}$$

Thus, we deduce that the cost $\mathsf{Mult}_{\mathsf{FFT}}(m)$ is $\mathcal{O}(\sqrt{\log_2 m})$ times larger than $\mathsf{Mult}_{\mathsf{HFT}}(m_{cyclo}, m_{mult})$.

Finally, observe that in both cases, $m_{mult} = m^{1-1/l} = m^{\frac{l-1}{l}}$, and for large enough l, the cyclotomic subfield dimension becomes negligible, causing the multiquadratic dimension to dominate such that the PLWE-RLWE equivalence no longer holds.

B.2 Reduction of multiplicative complexity under PLWE-RLWE equivalence

Following again the notation indicated in Section 2, and building on one of our results detailed in the proof of Cor. 4.5, we can make different choices for the relative sizes of the cyclotomic and multiquadratic subfield dimensions. In particular, letting $m_{cyclo} = 2^u$ and $m_{mult} = 2^{cr}$ (where $u = r^{1+1/l}$, and we have fixed $c \geq 1$ and $l \geq 2$ as constants) allows for PLWE-RLWE equivalence with a sub-quadratic noise increase (see Section 4). If we revisit the multiplicative cost ratio between cyclotomic and cyclo-multiquadratic rings for this particular choice of m_{cyclo} and m_{mult}, we obtain the following expression:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &= \frac{A \cdot \log_2 m}{1 + A \cdot \log_2 m_{cyclo}} \\ &= \frac{A \cdot (u + cr)}{1 + A \cdot u}.\end{aligned}$$

By considering $r^{1/l} \approx 1$, which implies that we work within a range of intermediate values for r where l is still sufficiently large compared to r, we obtain $u = r^{1+1/l} \approx r$. This allows us to obtain the following upper bound approximation:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &\approx \frac{A \cdot (1 + c)r}{1 + A \cdot r} \\ &\lessapprox \frac{A \cdot (1 + c)r}{A \cdot r} \\ &\lessapprox 1 + c,\end{aligned}$$

which indicates that, under the assumption $\frac{A\cdot(1+c)r}{1+A\cdot r} \approx \frac{A\cdot(1+c)\cdot r}{A\cdot r}$ (holding whenever $A \cdot r$ is large enough), we achieve a constant improvement by a factor of $c + 1$ in the number of multiplications. As the constant factor A is removed, this improvement is independent of the specific FFT algorithm being used.

To derive an approximate lower bound for $\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult})$, we can utilize the fact that $\frac{x}{x+1} \geq \frac{x-1}{x}$ for $x \geq 1$, and apply it recursively $c + 1$ times, yielding:

$$\begin{aligned}\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &\approx \frac{A \cdot (1 + c) \cdot r}{1 + A \cdot r} \\ &\approx \frac{A \cdot r}{1 + A \cdot r} + \frac{c \cdot A \cdot r}{1 + A \cdot r} \\ &\gtrapprox \frac{A \cdot r - 1}{A \cdot r} + \frac{c \cdot A \cdot r}{1 + A \cdot r} \\ &\gtrapprox 1 - \frac{1}{A \cdot r} + \frac{c \cdot A \cdot r}{1 + A \cdot r} \\ &\gtrapprox (c + 1) - \frac{c + 1}{A \cdot r}.\end{aligned}$$

In summary, we observe that, in general, as r grows but remains small enough relative to l, $\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult})$ approaches the approximate upper bound $c + 1$, with $c \geq 1$. However, further analysis is needed to determine the maximum value of c that still yields an effective efficiency improvement for practical values of the field degree m.

B.2.1 General expression for $\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult})$

In the previous section, we made use of several assumptions regarding the relation between r and l. However, we can obtain an exact lower bound for $\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult})$ without the need to work in the range of intermediate values for r where $r^{1/l} \approx 1$. To do this, we again resort to the fact that $\frac{x}{x+1} \geq \frac{x-1}{x}$ for $x \geq 1$, and define $d = 1/l$ for simplicity in notation, yielding the following lower bound:

$$
\begin{aligned}
\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult}) &= \frac{A \cdot (u + cr)}{1 + A \cdot u} \\
&= \frac{A \cdot (r^{1+d} + cr)}{1 + A \cdot r^{1+d}} \\
&= \frac{A \cdot c \cdot r}{1 + A \cdot r^{1+d}} + \frac{A \cdot r^{1+d}}{1 + A \cdot r^{1+d}} \\
&= \frac{A \cdot r}{1 + A \cdot r^{1+d}} + \frac{A \cdot (c-1) \cdot r}{1 + A \cdot r^{1+d}} + \frac{A \cdot r^{1+d}}{1 + A \cdot r^{1+d}} \\
&\geq \frac{A \cdot r - 1}{A \cdot r^{1+d}} + \frac{A \cdot (c-1) \cdot r}{1 + A \cdot r^{1+d}} + \frac{A \cdot r^{1+d}}{1 + A \cdot r^{1+d}} \\
&\geq \frac{A \cdot r}{A \cdot r^{1+d}} - \frac{1}{A \cdot r^{1+d}} + \frac{A \cdot (c-1) \cdot r}{1 + A \cdot r^{1+d}} + \frac{A \cdot r^{1+d}}{1 + A \cdot r^{1+d}} \\
&\geq \frac{1}{r^d} - \frac{1}{A \cdot r^{1+d}} + \frac{A \cdot (c-1) \cdot r}{1 + A \cdot r^{1+d}} + \frac{A \cdot r^{1+d}}{1 + A \cdot r^{1+d}} \\
&\geq \frac{c}{r^d} - \frac{c}{A \cdot r^{1+d}} + \frac{A \cdot r^{1+d} - 1}{A \cdot r^{1+d}} \\
&\geq \frac{c}{r^d} - \frac{c}{A \cdot r^{1+d}} + 1 - \frac{1}{A \cdot r^{1+d}} \\
&\geq 1 + \frac{c}{r^d} - \frac{c+1}{A \cdot r^{1+d}}.
\end{aligned}
$$

This expression provides a much better understanding of the adequate values for c, $l = 1/d$, and r which maximize $\mathsf{Mult}_{\mathsf{CostRatio}}(m_{cyclo}, m_{mult})$. Generally, we need r values small enough compared to l, but larger than c to minimize the effect of the term being subtracted.

Acknowledgements I. Blanco-Chacón is partially supported by the grants MTM2016-79400-P (Spanish Ministry of Science and Innovation), CCG20/IA-057 (University of Alcalá), and PID2019-104855RBI00/AEI/10.13039/501100011033 (Spanish Ministry of Science and Innovation). Part of the work has been completed as a visiting professor at Aalto University School of Science. A. Pedrouzo-Ulloa is partially supported by the European Union's Horizon Europe Framework Programme for Research and Innovation Action under project TRUMPET (proj. no. 101070038), by the European Regional Development Fund (FEDER) and Xunta de Galicia under project "Grupos de Referencia Competitiva" (ED431C 2021/47), and by FEDER and MCIN/AEI under project FELDSPAR (TED2021-130624B-C21). Part of the work has been completed as a visiting researcher at CEA-List, Université Paris-Saclay, and at the Universitat Politècnica de Catalunya (UPC), being funded by the European Union "NextGenerationEU/PRTR" under TRUFFLES and by means of a Margarita Salas grant of the Universidade de Vigo. R. Y. Njah Nchiwo is supported in part by a PhD scholarship by the Magnus Ehrnrooth Foundation, Finland, in part by Academy of Finland, grant 351271 (P.I. Camilla Hollanti) and in part by MATINE, Finnish Ministry of Defence, grant #2500M-0147 (P.I. PI Camilla Hollanti). B. Barbero-Lucas is partially supported by the grant CCG20/IA-057.

Funding Open Access funding provided thanks to the CRUE-CSIC agreement with Springer Nature. Funded by the European Union. Views and opinions expressed are however those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. The authors would like to thank Camilla Hollanti and Raúl Durán-Díaz for helpful

discussion and thorough reading of several versions of our work. Likewise, I. Blanco-Chacón would like to thank Aalto SCI for inviting him as a visiting professor for the year 2023–2024. Finally, we would like to thank the anonymous reviewers and the editor for their valuable feedback, which greatly contributed to improving the quality of this manuscript.

Data Availability The data and code used to generate the figures in this paper are publicly available in the following GitHub repository: https://github.com/apedrouzoulloa/cyclomultiquadratic. This repository contains the code used for the analysis and figure generation. The repository is publicly accessible for review and use.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Albrecht, M.R., Player, R., Scott, S.: On the concrete hardness of learning with errors. J. Math. Cryptol. **9**(3), 169–203 (2015)
2. Micciancio, D.: The shortest vector in a lattice is hard to approximate to within some constant. SIAM J. Comput. **30**(6), 2008–2035 (2000)
3. Khot, S.: Hardness of approximating the shortest vector problem in lattices. J. ACM. **52**(5), 789–808 (2005)
4. NIST Post-Quantum Cryptography Standardization, Round 3 Submissions. https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/round-3-submissions
5. Homomorphic Encryption Standardization. https://homomorphicencryption.org/
6. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM. **56**(6), 34–13440 (2009)
7. Lyubashevsky, V., Peikert, C., Regev, O.: A toolkit for ring-lwe cryptography. In: Advances in Cryptology - EUROCRYPT 2013. Lecture Notes in Computer Science, vol. 7881, pp. 35–54. Springer, Berlin, Heidelberg (2013)
8. Brakerski, Z., Gentry, C., Vaikuntanathan, V.: (leveled) fully homomorphic encryption without bootstrapping. ACM Trans. Comput. Theory. **6**(3), 13–11336 (2014)
9. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Cryptogr. **75**(3), 565–599 (2015)
10. Bolboceanu, M., Brakerski, Z., Sharma, D.: On algebraic embedding for unstructured lattices. IACR Cryptol. ePrint Arch., 53 (2021)
11. Albrecht, M., Chase, M., Chen, H., Ding, J., Goldwasser, S., Gorbunov, S., Halevi, S., Hoffstein, J., Laine, K., Lauter, K., Lokam, S., Micciancio, D., Moody, D., Morrison, T., Sahai, A., Vaikuntanathan, V.: Homomorphic Encryption Standard. Cryptology ePrint Archive, Paper 2019/939 (2019). https://eprint.iacr.org/2019/939
12. Bossuat, J.-P., Cammarota, R., Chillotti, I., Curtis, B.R., Dai, W., Gong, H., Hales, E., Kim, D., Kumara, B., Lee, C., Lu, X., Maple, C., Pedrouzo-Ulloa, A., Player, R., Polyakov, Y., Lopez, L.A.R., Song, Y., Yhee, D.: Security Guidelines for Implementing Homomorphic Encryption. Cryptology ePrint Archive, Paper 2024/463 (2024). https://eprint.iacr.org/2024/463
13. Lyubashevsky, V., Peikert, C., Regev, O.: On ideal lattices and learning with errors over rings. In: Advances in Cryptology - EUROCRYPT 2010. Lecture Notes in Computer Science, vol. 6110, pp. 1–23. Springer, Berlin, Heidelberg (2010)
14. Rosca, M., Stehlé, D., Wallet, A.: On the ring-lwe and polynomial-lwe problems. In: Advances in Cryptology - EUROCRYPT 2018–37th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science, vol. 10820, pp. 146–173. Springer, Cham (2018)
15. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: Advances in Cryptology - ASIACRYPT. Lecture Notes in Computer Science, vol. 5912, pp. 617–635. Springer, Berlin, Heidelberg (2009)

16. Peikert, C., Regev, O., Stephens-Davidowitz, N.: Pseudorandomness of ring-lwe for any ring and modulus. In: ACM SIGACT Symposium on Theory of Computing. STOC 2017, pp. 461–473. ACM, New York, NY, USA (2017)
17. Brakerski, Z., Vaikuntanathan, V.: Fully homomorphic encryption from ring-lwe and security for key dependent messages. In: Advances in Cryptology - CRYPTO. Lecture Notes in Computer Science, vol. 6841, pp. 505–524. Springer, Berlin, Heidelberg (2011)
18. Blanco-Chacón, I.: On the RLWE/PLWE equivalence for cyclotomic number fields. Appl. Algebra Eng. Commun. Comput. **33**(1), 53–71 (2022)
19. Blanco-Chacón, I.: RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices. J. Algebra Appli. **21**(11), 2250218 (2022)
20. Ducas, L., Durmus, A.: Ring-lwe in polynomial rings. In: Public Key Cryptography - PKC 2012–15th International Conference on Practice and Theory in Public Key Cryptography. Lecture Notes in Computer Science, vol. 7293, pp. 34–51. Springer, Berlin, Heidelberg (2012)
21. Scala, A.J.D., Sanna, C., Signorini, E.: Rlwe and plwe over cyclotomic fields are not equivalent. Applicable Algebra in Engineering, Communication and Computing (2022)
22. Bolboceanu, M.: Relating different polynomial-lwe problems. In: SecITC 2018. Lecture Notes in Computer Science, vol. 11359, pp. 492–503. Springer, Cham (2018)
23. Blanco-Chacón, I., López-Hernanz, L.: RLWE/PLWE equivalence for the maximal totally real subextension of the 2^{rpq}-th cyclotomic field. Adv. Math. Commun. (2022)
24. Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Gama, N., Georgieva, M., Perez-Gonzalez, F.: Multi-quadratic rings and walsh-hadamard transforms for oblivious linear function evaluation. 2020 IEEE International Workshop on Information Forensics and Security, WIFS 2020. (2020)
25. Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Gama, N., Georgieva, M., Pérez-González, F.: Revisiting multivariate ring learning with errors and its applications on lattice-based cryptography. Math. **9**(8) (2021)
26. Smart, N.P., Vercauteren, F.: Fully homomorphic SIMD operations. Des. Codes Cryptogr. **71**(1), 57–81 (2014)
27. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: TFHE: Fast Fully Homomorphic Encryption Library. https://tfhe.github.io/tfhe/ (2016)
28. Halevi, S., Shoup, V.: Design and implementation of helib: a homomorphic encryption library. IACR Cryptol. ePrint Arch., 1481 (2020)
29. Mouchet, C., Bossuat, J.-P., Troncoso-Pastoriza, J., Hubaux, J.: Lattigo: a multiparty homomorphic encryption library in go. In: WAHC (2020)
30. Aguilar-Melchor, C., Barrier, J., Guelton, S., Guinet, A., Killijian, M.-O., Lepoint, T.: NFLlib: NTT-Based Fast Lattice Library, pp. 341–356. Springer, Cham (2016)
31. Badawi, A.A., Bates, J., Bergamaschi, F., Cousins, D.B., Erabelli, S., Genise, N., Halevi, S., Hunt, H., Kim, A., Lee, Y., Liu, Z., Micciancio, D., Quah, I., Polyakov, Y., Saraswathy, R.V., Rohloff, K., Saylor, J., Suponitsky, D., Triplett, M., Vaikuntanathan, V., Zucca, V.: Openfhe: Open-source fully homomorphic encryption library. In: Proceedings of the 10th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, Los Angeles, CA, USA, 7 November 2022, pp. 53–63. ACM, New York, NY, USA (2022)
32. Microsoft SEAL (release 4.1). https://github.com/Microsoft/SEAL. Microsoft Research, Redmond, WA. (2023)
33. Ducas, L., Micciancio, D.: FHEW: bootstrapping homomorphic encryption in less than a second. In: Advances in Cryptology - EUROCRYPT 2015. Lecture Notes in Computer Science, vol. 9056, pp. 617–640. Springer, Berlin, Heidelberg (2015)
34. Chillotti, I., Gama, N., Georgieva, M., Izabachène, M.: TFHE: fast fully homomorphic encryption over the torus. J. Cryptol. **33**(1), 34–91 (2020)
35. Bajard, J., Eynard, J., Hasan, M.A., Zucca, V.: A full RNS variant of FV like somewhat homomorphic encryption schemes. In: Selected Areas in Cryptography - SAC. Lecture Notes in Computer Science, vol. 10532, pp. 423–442. Springer, Cham (2016)
36. Halevi, S., Polyakov, Y., Shoup, V.: An improved RNS variant of the BFV homomorphic encryption scheme. In: Topics in Cryptology - CT-RSA 2019. Lecture Notes in Computer Science, vol. 11405, pp. 83–105. Springer, Cham (2019)
37. Pedrouzo-Ulloa, A.: Multiquadratic rings and oblivious linear function evaluation. TEMat monográficos. **2**, 83–86 (2021)
38. Duhamel, P., Vetterli, M.: Fast fourier transforms: A tutorial review and a state of the art. Signal Process. **19**(4), 259–299 (1990)
39. Harvey, D.: Faster arithmetic for number-theoretic transforms. J. Symb. Comput. **60**, 113–119 (2014)
40. Nussbaumer, H.J.: Fast Fourier Transform and Convolution Algorithms. Springer, Berlin, Heidelberg (1982)

41. Bianchi, T., Piva, A., Barni, M.: Composite Signal Representation for Fast and Storage-Efficient Processing of Encrypted Signals. IEEE Trans. Inf. Forensic. Secur. **5**(1), 180–187 (2010)
42. Pedrouzo-Ulloa, A., Troncoso-Pastoriza, J.R., Pérez-González, F.: Number theoretic transforms for secure signal processing. IEEE Trans. Inf. Forensic. Secur. **12**(5), 1125–1140 (2017)
43. Halevi, S., Shoup, V.: Bootstrapping for helib. J. Cryptol. **34**(1), 7 (2021)
44. Halevi, S., Shoup, V.: Faster homomorphic linear transformations in helib. In: Advances in Cryptology - CRYPTO 2018. Lecture Notes in Computer Science, vol. 10991, pp. 93–120. Springer, Cham (2018)
45. Cheon, J.H., Choe, H., Lee, D., Son, Y.: Faster linear transformations in HElib, revisited. IEEE Access. **7**, 50595–50604 (2019)
46. Han, K., Hhan, M., Cheon, J.H.: Improved homomorphic discrete fourier transforms and FHE bootstrapping. IEEE Access. **7**, 57361–57370 (2019)
47. Chiu, S., Parhi, K.K.: Long polynomial modular multiplication using low-complexity number theoretic transform [lecture notes]. IEEE Signal Process. Mag. **41**(1), 92–102 (2024)
48. Heideman, M.T., Burrus, C.S.: On the number of multiplications necessary to compute a length-2^ndft. IEEE Trans. Acoust. Speech Signal Process. **34**(1), 91–95 (1986)
49. Stewart, I.N., Tall., D.O.: Algebraic Number Theory (Second Edition). Chapman and Hall/CRC Press, New York (1987)
50. Scala, A.J.D., Sanna, C., Signorini, E.: On the condition number of the vandermonde matrix of the nth cyclotomic polynomial. J. Math. Cryptol. **15**(1), 174–178 (2021)
51. Halevi, S., Shoup, V.: Algorithms in helib. In: Advances in Cryptology - CRYPTO 2014. Lecture Notes in Computer Science, vol. 8616, pp. 554–571. Springer, Berlin, Heidelberg (2014)
52. Crawford, J.L.H., Gentry, C., Halevi, S., Platt, D., Shoup, V.: Doing real work with FHE: the case of logistic regression. In: Proceedings of the 6th Workshop on Encrypted Computing & Applied Homomorphic Cryptography, WAHC@CCS 2018, Toronto, ON, Canada, October 19, pp. 1–12. ACM (2018)
53. Gentry, C., Halevi, S., Smart, N.P.: Homomorphic evaluation of the AES circuit. In: Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings. Lecture Notes in Computer Science, vol. 7417, pp. 850–867. Springer, Berlin, Heidelberg (2012)
54. Narkiewicz, W.: Elementary and Analytic Theory of Algebraic Numbers. Springer, Berlin, Heidelberg (2004)
55. Robin, G.: Estimation de la fonction de tchebychef θ sur le k-iéme nombre premier et grandes valeurs de la fonction $\omega(n)$ nombre de diviseurs premiers de n. Acta Arithmetica. **42**(4), 367–389 (1983)
56. Jang, J., Lee, Y., Kim, A., Na, B., Yhee, D., Lee, B., Cheon, J.H., Yoon, S.: Privacy-preserving deep sequential model with matrix homomorphic encryption. In: ASIA CCS '22: ACM Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May 2022 - 3 June 2022, pp. 377–391. ACM, New York, NY, USA (2022)
57. Peikert, C.: How (not) to instantiate ring-lwe. In: Security and Cryptography for Networks - 10th International Conference, SCN 2016, Amalfi, Italy, August 31 - September 2, 2016, Proceedings. Lecture Notes in Computer Science, vol. 9841, pp. 411–430. Springer, Cham (2016)
58. Washington, L.C.: Introduction to Cyclotomic Fields. Springer, New York, NY (1997)
59. Bzdega, B.: On the height of cyclotomic polynomials. Acta Arithmetica. **152**, 349–359 (2010)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.