RLWE/PLWE equivalence for cyclotomic extensions and subextensions

Iván Blanco Chacón
Department of Mathematics, School of Science
Universidad de Alcalá de Henares
ivan.blancoc@uah.es

***Abstract*—We report on our recent proofs of the equivalence between the Ring Learning With Errors and Polynomial Learning With Errors problems in the settings of a) cyclotomic number fields and b) their maximal totally real subextensions for the $2p$ conductor case (p odd prime). We discuss future extensions of our results and possible applications in practical scenarios such as fully homomorphic encryption in network/cloud distributed environments, like in the areas of health data processing or e/i-voting schemes in distributed wireless networks.**

***Keywords*—Ring Learning With Errors, Polynomial Learning With Errors, Homomorphic Encryption, Cyclotomic Fields.**

I. RLWE and PLWE. Definitions and facts

A. Motivation

The third round of the last NIST call confirms the lattice-based proposals as the strongest contenders (https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions). Within this category, RLWE/PLWE keeps the largest number of surviving proposals. These numbers, along with the ease-to-implement of most RLWE/PLWE-based primitives, their small key sizes (in comparison with code-based and multivariate-based proposals) and the fact of being a natural tool for fully homomorphic encryption support the enormous interest in this topic from practical and theoretical points of view.

A theoretical open problem is the relation between both versions: RLWE, formulated in terms of rings of algebraic integers and PLWE, in terms of rings of polynomials. The natural ring isomorphism deforms the error distributions and nothing prevents an exponential noise increase. In [9], polynomial equivalence was first shown for an ad-hoc family of polynomials. However, it is the cyclotomic family the most interesting for cryptography, for which until now, such equivalence was an open question apart from the power-of-two degree and some particular cases ([4]). In [2], we proved the equivalence if the number of primes dividing the conductor is fixed.

A strong reason to pursue such equivalence is that security reduction proofs are usually carried out using RLWE (cf. [8] Theorem 4.1), whilst a smart handling of quotient polynomial rings yields extremely efficient algorithms (by a delicate use of Toom or Karatsuba polynomial multiplication method or NTT-variants), making PLWE proner to computer implementations. For instance, NTRU-Prime requires 28682 cycles on one core of an Intel Haswell CPU for polynomial multiplication in their recommended ring $\mathbb{F}_{4591}[x]/(x^{761}-x-1)$, at a postquantum security level of 128 bits, outperforming the range of 150000 cycles required for ECC schemes.

This communication is a summary of our recent works [2] and [3], with an account of our further lines of research on the topic, aligned with our projects *CloudWall* (Cloud-enabled Resiliency Framework for HealthCare IT Infrastructures), and *UCeNet*, in particular in their area of security and resilience of critical infrastructures.

B. Algebraic number fields

An algebraic number field is a field extension $K=\mathbb{Q}(\theta)/\mathbb{Q}$ of some finite degree m, where θ satisfies $f(\theta)=0$ for $f(x)\in\mathbb{Q}[x]$ monic and irreducible. In particular, K is an m-dimensional $\mathbb{Q}$-vector space and the set $\{1,\theta,...,\theta^{m-1}\}$ is a $\mathbb{Q}$-basis of K. Notice that evaluation at θ yields a field isomorphism $K\cong\mathbb{Q}[x]/f(x)$ fixing $\mathbb{Q}$.

A number field $K=\mathbb{Q}(\theta)$ of degree m has exactly m field $\mathbb{Q}$-embeddings, which we denote $\sigma_i : K\to\overline{\mathbb{Q}}$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$.

The canonical embedding $\sigma : K\to\mathbb{R}^{s_1}\times\mathbb{C}^{2s_2}$ is defined as $\sigma(x):=(\sigma_1(x),...,\sigma_m(x))$ where $m=s_1+2s_2$.

An algebraic integer is an element of $\overline{\mathbb{Q}}$ whose minimal polynomial over $\mathbb{Q}$ has integer coefficients and we denote by $\mathcal{O}_K\subset K$ the set of all algebraic integers in K. This set forms a ring under addition and multiplication in K ([11], Theorem 2.9). Moreover, $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n ([11]), i.e., a full rank lattice.[1] Moreover, for each ideal $I\subseteq\mathcal{O}_K$, the canonical embedding provides a (full rank) sublattice of $\mathcal{O}_K$ for which multiplication and addition are preserved component-wise. This is not true for the coordinate embedding: e.g. for any $l\geq 2$, multiplying by x in the ring $\mathbb{Z}[x]/(x^{2^l}+1)$ is equivalent to shifting the coordinates and negate the independent term. This is a strong reason to prefer working with the canonical embedding rather than with the coordinate embedding.

C. Cyclotomic fields

Let $n>1$ be an integer. The set of primitive n-th roots of unity $\{\zeta_k=exp(2\pi i)k/n, 1\leq k\leq n \text{ coprime to } n\}$ is a multiplicative group of order $m:=\phi(n)$[2]. The n-th cyclotomic polynomial is

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

This polynomial is irreducible over $\mathbb{Z}[x]$ and $K_n:=\mathbb{Q}(\zeta)$ for each $\zeta=\zeta_k$ is an algebraic number field of degree m

[1] By a full rank lattice we understand here a finitely generated abelian subgroup Λ of $\mathbb{R}^n$ of rank n.

[2] The letter m will be used for the degree of the number field considered in each section and is not to be confused, in the cyclotomic case, with the order of the root of unity, for which the letter n is reserved.

independent of k. It can be proved ([11] Chap 3) that $\mathcal{O}_{K_n} = \mathbb{Z}[\zeta]$.

Setting $\psi_k = \zeta_k + \zeta_k^{-1} = 2\cos\left(\frac{2k\pi}{n}\right)$, denote $K_n^+ := \mathbb{Q}(\psi)$. This is the maximal totally real subextension of K_n (it does not depend on k) and its degree $m = \phi(n)/2$. Moreover (cf. [12] Ch. 1), one has that $\mathcal{O}_{K_n^+} = \mathbb{Z}[\zeta + \zeta^{-1}]$. Denote by $\Phi_n^+(x)$ the minimal polynomial of ψ_k.

D. Ring/Polynomial Learning With Errors

The next definitions apply for any number field, but we are only interested in the cases $K = K_n$ and K_n^+ in this work. Denote by $\mathcal{O}_K$ the ring of integers of K and assume that $\mathcal{O}_K = \mathbb{Z}[\theta]$ for some θ (i.e. suppose that K is monogenic) and set $\mathcal{O} := \mathbb{Z}[x]/(f(x))$, where $f(x)$ stands for the minimal polynomial of θ.

Definition I.1 (The RLWE/PLWE problem)**.** *Let q be a prime and let χ be a 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. $\mathcal{O}/q\mathcal{O}$), if an adversary (for which s is secret) is given access to arbitrarily many samples $\{(a_i, a_i s + e_i)\}_{i\geq 1}$ of the RLWE (resp. PLWE) distribution, where for each $i \geq 1$, a_i is uniformly chosen at random and e_i is sampled from χ, the adversary must recover s with non-negligible advantage.*

Definition I.2. *We say that RLWE and PLWE are equivalent for a number field K if every solution for the first can be turned in polynomial time into a solution for the second (and viceversa), incurring in a noise increase which is polynomial in the degree of K.*

E. Distortion between embeddings

As lattices, $\mathbb{Z}[x]/(\Phi_n(x))$ is endowed with the coordinate embedding while $\mathbb{Z}[\zeta]$ is endowed with the canonical embedding, and the evaluation-at-θ map causes a distortion between the noise distributions. Explicitly, the transformation between the embeddings defined by evaluation at ζ

$$V_{\Phi_n} : \mathbb{Z}[x]/(\Phi_n(x)) \rightarrow \sigma_1(\mathcal{O}_{K_n}) \times \cdots \times \sigma_m(\mathcal{O}_{K_n}) \tag{I.1}$$

maps the polynomial $\sum_{i=0}^{m-1} a_i \overline{x}^i$ to the vector

$$\begin{pmatrix} 1 & \zeta_1 & \cdots & \zeta_1^{m-1} \\ 1 & \zeta_2 & \cdots & \zeta_2^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_m & \cdots & \zeta_m^{m-1} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix}$$

where $\overline{x}$ is the class of x modulo $\Phi_n(x)$. Namely, the transformation V_{Φ_n} is given by a Vandermonde matrix acting on the coordinates.

As justified in [9], the noise growth caused by V_{Φ_n} will remain *controlled* whenever $||V_{\Phi_n}||$ and $||V_{\Phi_n}^{-1}||$ remain so and a reasonable measure of how both quantities are controlled is given by the condition number of V_{Φ_n}, defined as follows:

Definition I.3. *The condition number of an invertible matrix $A \in \mathrm{M}_n(\mathbb{C})$ is defined as Cond$(A) := ||A||||A^{-1}||$ where $||\ \ ||$ denotes the Frobenius norm, but this is not essential, as all matrix norms are equivalent.*

Hence the problem of the equivalence is reduced to show that $\mathrm{Cond}(V_{\Phi_n}) = O(n^r)$ for some constant r independent of n. The difficulty is that Vandermonde matrices tend to be very ill conditioned: for instance, Vandermonde matrices with positive nodes are exponentially conditioned ([6]). In particular, if $n > 4$ and n is even, we have that $\mathrm{Cond}(V_{K_n^+}) > 2^{\phi(n)/2-1}$.

II. Main results

Let ζ, ψ, K_n, K_n^+, $\mathcal{O}_{K_n}$, $\Phi_n(x)$ and $\Phi_n(x)^+$ be as in Section I.

A. Equivalence for the cyclotomic case

Definition II.1. *For $n \geq 3$, denote by $A(n)$ the maximum coefficient of $\Phi_n(x)$ in absolute value. If $n = p_1^{r_1}...p_s^{r_s}$, ($p_i \neq p_j$ if $i \neq j$) denote $rad(n) = p_1...p_s$. Notice that $A(n) = A(rad(n))$.*

If $n = 2^k$ for some $k > 2$, one can easily show that the map V_{Φ_n} is a scaled isommetry and $\mathrm{Cond}(V_{\Phi_n}) = 2^{k-1}$ ([10]), hence we will assume that $rad(n) \neq 2$. Our main result is as follows:

Theorem II.2 ([2] Thm. 3.10)**.** *Let $k \geq 1$ be fixed. If rad$(n) = p_1...p_k$, then*

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

The keys of the proof are: 1) as in [9], we start with an expression of the entries in $V_{\Phi_n}^{-1}$ as quotients of symmetric polynomials in the n-th primitive roots, 2) a bound for $A(n)$ due to Bateman ([1]) which is polynomial in m once k is fixed; some surgery on this bound allows to control the numerators, and 3) the observation that $A(n) = A(rad(n))$, which simplifies the treatment of the denominators. When $k \leq 3$, we can refine our bound as follows:

Theorem II.3 ([2], Thms. 4.1, 4,3 and 4.6)**.** *For $n \geq 1$ and $m = \phi(n)$, the following bounds hold for the condition number of cyclotomic polynomial $\Phi_n(x)$:*

a) *If $n = p^k$ then* $\mathrm{Cond}(V_{\Phi_n}) \leq 4(p-1)m$.
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* $\mathrm{Cond}(V_{\Phi_n}) \leq 2\phi(rad(n)m^2$.

B. Equivalence for the maximal totally real cyclotomic subextension

The Kronecker-Weber theorem states that every abelian $\mathbb{Q}$-extension is a subextension of a cyclotomic extension, hence, a natural extension (towards the general abelian case) of our above theorems 2.2 and 2.3 would be a result establishing the equivalence for nontrivial subextensions of cyclotomic number fields. In [3] we have addressed this question for K_n^+ for $n = 4p$ with p an arbitrary prime, while the general case is still under study.

A first consideration is that one can pass from a PLWE-sample to a RLWE-sample by Gaussian elimination in $O(m^3)$-time via the transformation matrix $V_{K_n^+}$, but the problem is that the norm of the noise gets amplified by an exponential factor. Our strategy in [3] consists in replacing the matrix $V_{K_n^+}$ by a so-called quasi-Vandermonde matrix $QV_{K_n^+,\{p_i(x)\}_{i=0}^{m-1}} = \left(p_i(\psi_{k_j})\right)_{i,j=0}^{m-1}$, where $\psi_k := 2\cos\left(\frac{2k\pi}{n}\right)$

with k coprime to n, and where $p_i(x) \in \mathbb{Z}[x]$ has degree i. The following result is easy to prove (see [3] Prop. 3.1) and our starting point:

Proposition II.4. *For any $\{p_i(x)\}_{i=0}^{m-1} \subseteq \mathbb{Z}[x]$ with $deg(p_i(x)) = i$, the matrix $QV_{K_n^+,\{p_i(x)\}_{i=0}^{m-1}}$ is invertible.*

The requirement that $p_i(x) \in \mathbb{Z}[x]$ is needed to ensure that $QV_{K_n^+}$ maps (isomorphically) $\mathbb{Z}[x]/\Phi_n^+(x)$ onto $\sigma(\mathcal{O}_{K_n^+})$. But we need to choose the polynomials in such a way that $\mathrm{Cond}(QV_{K_n^+})$ is polynomial in m, whenever this is possible. This is attainedif we use, for instance, the Tchebychev family:

Definition II.5. *The family of Tchebychev polynomials of the first kind is defined any of the following equivalent properties:*

a) $T_n(x) = \cos(n\arccos(x))$.
b) $T_0(x) = 1, T_1(x) = x$ *and* $T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$ *for* $n \geq 2$.

The reason why our approach solves our problem is the following result:

Proposition II.6 ([7], Cor. 1)**.** *For each $N > 2$, let $x_k^{(N)} = \cos\left(\frac{2k-1}{2N}\pi\right)$. Denote $V_N = (T_i(x_k^{(N)})_{i,k-1=0}^{N}$. Then, $\mathrm{Cond}(V_N)$ is polynomial in N.*

Assume that $N = p$ prime. We notice that Prop. II.6 works by evaluating the Tchebychev family at $\frac{1}{2}\psi_1$ and their conjugates, rather than at the generator of $\mathcal{O}_{K_{2p}^+}$. We overcome this problem by writing $T_i(x_k^{(p)}) = Q_i(2x_k^{(p)})$ where $Q_i(x) := T_i(\frac{1}{2}x)$, and $2x_k^{(p)} = \psi_k$. The following fact has a straightforward proof by induction:

Lemma II.7. *For $n \geq 1$, we can write $Q_n(x) = \frac{1}{2}a_n(x)$, where $a_n(x) \in \mathbb{Z}[x]$.*

Since for each $A \in GL_n(\mathbb{C})$ and $\lambda \in \mathbb{C}^*$ it is $||\lambda A|| = |\lambda|||A||$, it also holds $\mathrm{Cond}(\lambda A) = \mathrm{Cond}(A)$, hence the matrix $Q_{4p} := \left(a_i(2x_k^{(p)})\right)_{i,k-1=0}^{p-1}$ is also polynomially conditioned, namely:

$$\mathrm{Cond}(Q_{4p}) \leq p(p+1). \qquad \text{(II.1)}$$

Next, we observe that we have to restrict the nodes only to those with $2k+1$ coprime with p. Now, by the very definition we have $T_i(x_{\frac{p-1}{2}}^{(p)}) = \cos\left(\frac{i\pi}{2}\right) \in \{0, \pm 1\}$ for $0 \leq i \leq p-1$ and since permutation of two rows does not affect the condition number, we still denote by Q_{4p} the result of permuting the first and $\frac{p-1}{2}$-th rows.

The next step is to eliminate all the elements in the first row using $a_0(x_1^{(p)})$ as pivot, obtaining $M_{4p} = Q_{4p}R$, where R is an upper triangular elementary matrix:

$$M_{4p} = \begin{pmatrix} 1 & O \\ \mathbf{a} & N_{4p} \end{pmatrix}$$

with $O \in M_{1\times p-1}(\mathbb{R})$ and $\mathbf{a} \in M_{p-1\times 1}(\mathbb{R})$. The matrix which solves our problem is $N_{4p} = (b_i(2\psi_k))$ with $1 \leq p-1$ and $k (\in \mathbb{Z}/p\mathbb{Z})^*$, where according to the fact that elimination has been performed just by summing all the columns with the first one multiplied by 0 or ± 1, we have $b_i(x) \in \mathbb{Z}[x]$. So we need to check that N_{4p} is polynomial in its size: $p-1$. To see this, first we notice that $||N_{4p}|| \leq ||M_{4p}||$. Secondly:

Proposition II.8. *With the previous notations we have that $||N_{4p}^{-1}||$ is polynomial in its size.*

Proof. First, since M_{4p} is invertible, so is N_{4p} and we can write:

$$M_{4p}^{-1} = \begin{pmatrix} 1 & O \\ \mathbf{b} & N_{4p}^{-1} \end{pmatrix}$$

where $N_{4p}\mathbf{b} = -\mathbf{a}$, and hence $||N_{4p}^{-1}|| \leq ||M_{4p}^{-1}||$, as desired. □

All told, we put together our previous analysis in the following satement, which shows the RLWE/PLWE equivalence for K_{2p}^+:

Theorem II.9. *There exists a matrix $N_{4p} \in M_{p-1}(\mathcal{O}_{K_{2p}^+})$, polynomially conditioned in its size such that the map*

$$\begin{array}{ccc} \mathbb{Z}[x]/\Phi_{2p}^+(x) & \rightarrow & \sigma_1((\mathcal{O}_{K_{2p}^+}) \times ...\sigma_{p-1}((\mathcal{O}_{K_{2p}^+}) \\ \boldsymbol{u} & \mapsto & N_{4p}\boldsymbol{u} \end{array}$$

provides a lattice (and ring) isomorphism inducing a polynomial noise increase between the RLWE and the PLWE distributions.

III. Conclusions, ongoing and further research

As stated in the introduction, the arithmetic of polynomial quotient rings is much faster to implement and to use in cryptographic settings than its number field counterpart. This is important in settings as network distributed scenarios accessed with devices with limited computation resources or memory. If in addition, these scenarios are assumed to support homomorphic encryption, PLWE is likely one of the most promising solutions, if the ring is chosen carefully. But apart from cyclotomic settings, there are no general security reduction proofs for schemes attached to general rings of integers. Here is where RLWE/PLWE-equivalence plays a role, since the security reduction is well established for most (Galois) number fields (cf. for instance [8] Thm 4.1).

In [2], we proved the equivalence of RLWE and PLWE for cyclotomic number fields, in the sense that for any fixed number of primes dividing the conductor, for any degree n, the problems RLWE and PLWE for the cyclotomic field K_n are polynomially equivalent. In [3] we prove the same result for the maximal totally real subextension K_{4p}^+ of K_{4p}. This is a first step to tackle the general abelian case.

In the totally real case, we have restricted ourselves to the $2p$ conductor case because it is unclear how to upper-bound the term $||V_n^{-1}||$ for general n. The number of elementary operations increases very fast in n and we cannot control the joint norm of non-permutation row operations at the moment. Several empirical examples lead us to think that the task is doable (but cumbersome), leaving it for further work.

The application that we have in mind in our project *CloudWall* is a) to formally grant and b) practically provide security to the action of the nodes to refrain the advance of malware, to which end it is important to control the error-increase in the different layers of the homomorphic encryption by choosing a suitable ring (tentatively cyclotomic or maximal totally real). Our current research towards this aim is to exploit certain subgroups of cyclotomic units to locally reshape the geometry of the noise distribution. On the other hand, in our project UCeNet, the clearest application of our work is to back the security of the implementation of homomorphic encryption in distributed e/i-voting, again, by a suitable choice of a polynomial ring, either cyclotomic or maximal totally real. The reader is referred to [5] for a detailed exposition of LWE in e-voting, which is the starting point of the PLWE-based scheme we are developing for UCeNet.

Acknowledgements

Partially supported by the projects PID2019-104855RB-I00/AEI /10.13039/501100011033 of the Spanish Ministry of Science and Innovation, and UCeNet CM/JIN/2019-031 of the Comunidad de Madrid and University of Alcalá.

References

[1] P.T. Bateman: On the size of the coefficients of the cyclotomic polynomial.*Seminaire de Théorie des Nombres de Bordeaux, 11* (28) (1982) 1–18.

[2] I. Blanco-Chacón. On the RLWE/PLWE equivalence for cyclotomic number fields. To appear in *Applicable Algebra in Engineering, Communications and Computing*, 2020 (available in arxiv: https://arxiv.org/abs/2001.10891)

[3] I. Blanco-Chacón. RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices (submitted) https://arxiv.org/abs/2006.16354

[4] L. Ducas, A. Durmus. Ring-LWE in polynomial rings. In PKC, 2012.

[5] I. Chillotti, N. Gama, M. Georgieva, M. Izabachene. A homomorphic LWE-Based e-voting scheme. In *PQCrypto 2016*, pp. 245–265 (2016).

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

[7] M. Kuian, L. Reichel, S. Shiyanovskii: Optimally conditioned Vandermonde-like matrices. SIAM J. Matr. Anal. Appl., 40 (4) (2019) pp. 1399–1424.

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

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

[10] D. N. Stehle, R. Steinfeld, K. Tanaka, K. Xagawa. Efficient public key encryption based on ideal lattices. In *Advances in Cryptology ASIACRYPT 2009.* 617–635 (2009).

[11] I. Stewart. *Algebraic number theory and Fermat's last theorem.* AK Peters Ltd, 2002.

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