RLWE and PLWE over cyclotomic fields are not equivalent

Applicable Algebra in Engineering, Communication and Computing
https://doi.org/10.1007/s00200-022-00552-9

ORIGINAL PAPER

RLWE and PLWE over cyclotomic fields are not equivalent

Antonio J. Di Scala[1] · **Carlo Sanna**[1] · **Edoardo Signorini**[2]

Received: 21 January 2022 / Revised: 14 March 2022 / Accepted: 30 March 2022

Abstract
We prove that the Ring Learning With Errors (RLWE) and the Polynomial Learning With Errors (PLWE) problems over the cyclotomic field $\mathbb{Q}(\zeta_n)$ are not equivalent. Precisely, we show that reducing one problem to the other increases the noise by a factor that is more than polynomial in n. We do so by providing a lower bound, holding for infinitely many positive integers n, for the condition number of the Vandermonde matrix of the nth cyclotomic polynomial.

Keywords Cyclotomic polynomial · Vandermonde matrix · Condition number · RLWE · PLWE

Mathematics Subject Classification 11C99 · 15A12 · 15B05 · 15B05 · 94A60

1 Introduction

Since the theoretical results of Ajtai [1], lattice-based cryptography has gained increasing interest. Indeed, numerous lattice-based encryption and digital signature schemes, with performance comparable or even superior to that of their number-theoretic counterparts, have been proposed [2, 10, 13, 16]. In particular, because of their presumed resistance against quantum attacks, lattice-based proposals are the most numerous in the final phase of the NIST post-quantum

✉ Carlo Sanna
carlo.sanna@polito.it

Antonio J. Di Scala
antonio.discala@polito.it

Edoardo Signorini
edoardo.signorini@telsy.it

[1] Department of Mathematical Sciences, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy

[2] Telsy S.p.A., Corso Svizzera 185, 10149 Torino, Italy

Published online: 30 April 2022

standardization process, with finalist candidates in both key encapsulation [3, 5, 11] and digital signature schemes [4, 15].

The main building block of lattice-based cryptographic schemes is the Learning With Errors (LWE) problem [19], which, roughly speaking, consists of retrieving a secret vector $s \in \mathbb{Z}_q^n$ from a noisy random sample of matrix products. On the one hand, LWE-based encryption schemes enjoy good computational efficiency and solid theoretical security bases. On the other hand, they require the ciphertexts or the public keys to be nearly quadratic with respect to the security parameters. To overcome this inefficiency, algebraic variants of the LWE problem have been introduced, which consider the problem no longer over $\mathbb{Z}_q$ but over the quotient ring $\mathbb{Z}_q[X]/(f)$, where $f \in \mathbb{Z}_q[X]$ is a monic and irreducible polynomial. The variant known as Polynomial-LWE (PLWE), was first proposed using power-of-two degree cyclotomic polynomials [22]. Later, Lyubashevsky, Peikert, and Regev [18] introduced the Ring-LWE (RLWE) variant over the ring of integers $\mathcal{O}_K$ of a number field $K = \mathbb{Q}(\theta)$ (for surveys on RLWE, see [7, 14]).

The main advantage of RLWE (and of later generalizations such as Module-LWE [17]) is the provable-security link with hard computational problems over (ideal) lattices, as for plain LWE. Nevertheless, most of the concrete constructions of lattice-based schemes, while enjoying the security proofs of RLWE, are expressed in the simpler formalism of PLWE. The latter is in fact preferable in implementations, where the modular arithmetic between polynomials can be efficiently implemented. For these reasons, it is interesting to study for which families of polynomials f the RLWE and PLWE problems are equivalent, that is, every solution of the first problem can be turned in polynomial time into a solution of the second problem, and viceversa, incurring in a noise increase that is polynomial in the degree of f. From a theoretical point of view, the problem of equivalence between RLWE and PLWE was formalized for the first time by Rosca, Stehlé, and Wallet [24], who also explained the relationship between the noise increase and the condition number of a certain Vandermonde matrix associated with f, as detailed below.

More precisely, let $K = \mathbb{Q}(\theta)$ be a monogenic number field of degree m, and let $f \in \mathbb{Z}[X]$ be the minimal polynomial of θ, so that $\mathcal{O}_K \cong \mathbb{Z}[X]/(f)$. The geometric notion of short element derives from a choice of a norm on K by embedding the number field in $\mathbb{C}^m$. On the one hand, RLWE makes use of the *canonical embedding* (or *Minkowski embedding*) σ from K to $\mathbb{C}^m$, where $\sigma_i(\theta)$ $(i = 1, \dots, m)$ are the Galois conjugates of θ. On the other hand, PLWE makes use of the *coefficient embedding*, which maps each $x \in \mathcal{O}_K$ to the vector $(x_0, \dots, x_{m-1}) \in \mathbb{Z}^m$ of its coefficients with respect to the power basis $1, \theta, \dots, \theta^{m-1}$. As a linear map, the canonical embedding σ has a matrix representation $V \in \mathbb{C}^{m \times m}$, so that, for each $x \in \mathcal{O}_K$, we have $\sigma(x) = V \cdot (x_0, \dots, x_{m-1})^\intercal$. For the equivalence between RLWE and PLWE, it is important to determine when, whether $\|x\|$ is small, then so is $\|\sigma(x)\|$, and vice versa. This notion is quantified by V having a small *condition number* $\mathrm{Cond}(V) := \|V\|\|V^{-1}\|$, where $\|V\| := \sqrt{\mathrm{Tr}(V^* V)}$ is the *Frobenius norm* of V, and V^* is the conjugate transpose of V. Precisely, for the equivalence of the RLWE and PLWE problems it must be $\mathrm{Cond}(V) = O(m^r)$ for some constant $r > 0$, depending only on the family of polynomials f.

The equivalence problem can be studied in general for any number field. Although equivalence has been proved for restricted families of polynomials defining number fields [24], the greatest interest arguably concerns cyclotomic fields, which are the most used in cryptographic applications. For cyclotomic fields, the equivalence is well known for the power-of-two case [22] and recently the problem has received more attention both from a theoretical point of view [6, 12] and in practical applications [25]. However, to the best of our knowledge, prior to this work a general result on RLWE and PLWE equivalence for cyclotomic fields was still missing. When $K = \mathbb{Q}(\zeta_n)$ is the nth cyclotomic field, $V_n := V$ is the Vandermonde matrix of the nth cyclotomic polynomial $\boldsymbol{\Phi}_n(X)$, that is,

$$V_n := \begin{pmatrix} 1 & \zeta_{n,0} & \zeta_{n,0}^2 & \cdots & \zeta_{n,0}^{m-1} \\ 1 & \zeta_{n,1} & \zeta_{n,1}^2 & \cdots & \zeta_{n,1}^{m-1} \\ 1 & \zeta_{n,2} & \zeta_{n,2}^2 & \cdots & \zeta_{n,2}^{m-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{n,m-1} & \zeta_{n,m-1}^2 & \cdots & \zeta_{n,m-1}^{m-1} \end{pmatrix},$$

where $\zeta_{n,0}, \ldots, \zeta_{n,m-1}$ are the primitive nth roots of unity, and $m = \varphi(n)$ is the Euler totient function of n. Note that $\boldsymbol{\Phi}_n(X)$ has degree m. If n is a power of 2, then it is easy to show that V_n is a scaled isometry, so that $\mathrm{Cond}(V_n) = m$ and consequently RLWE and PLWE are equivalent. Blanco-Chacón [6] (see also [8, 9]) proved that $\mathrm{Cond}(V_n) = O(n^{r_k})$, where $r_k > 0$ is a constant depending only on the number k of distinct prime factors of n. Therefore, RLWE and PLWE restricted to the positive integers n with a bounded number of prime factors are equivalent. Furthermore, in a previous work [12], the authors gave an explicit formula for the condition number of V_n when n is a prime power or a power of 2 times an odd prime power.

Our main result is the following.

Theorem 1 *There exist infinitely many positive integers n such that*

$$\mathrm{Cond}(V_n) > \exp\left(n^{\log 2/\log\log n}\right)/\sqrt{n}.$$

In particular, for every fixed $r > 0$, *we have that* $\mathrm{Cond}(V_n) \neq O(n^r)$.

As a consequence of Theorem 1 and the previous considerations, one immediately gets the following corollary.

Corollary 1 *RLWE and PLWE over cyclotomic fields are not equivalent.*

Corollary 1 settles the question of the equivalence between RLWE and PLWE over cyclotomic fields by answering it negatively. Therefore, from both a practical and a theoretical point of view, future investigations have to keep in mind that, in general, results on RLWE over cyclotomic fields cannot be translated into results on PLWE over cyclotomic fields, and vice versa, unless further restrictions on the generating polynomials are imposed.

An interesting direction would be to determine the maximal order of $\mathrm{Cond}(V_n)$ and, in particular, if the lower bound of Theorem 1 can be improved significantly. For a plot of the values of $\mathrm{Cond}(V_n)$ up to $n = 10,000$, see Fig. 1. The library used for the calculation of $\mathrm{Cond}(V_n)$ is available in [21].

2 Proof of Theorem 1

Throughout this section, let n be a positive integer and put $m := \varphi(n)$. We write Id_k for the $k \times k$ identity matrix, and we count rows and columns starting from 0, so that the first row or column is the 0th. Furthermore, let

$$W_n := \begin{pmatrix} 1 & \zeta_{n,0} & \zeta_{n,0}^2 & \cdots & \zeta_{n,0}^{mn-1} \\ 1 & \zeta_{n,1} & \zeta_{n,1}^2 & \cdots & \zeta_{n,1}^{mn-1} \\ 1 & \zeta_{n,2} & \zeta_{n,2}^2 & \cdots & \zeta_{n,2}^{mn-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \zeta_{n,m-1} & \zeta_{n,m-1}^2 & \cdots & \zeta_{n,m-1}^{mn-1} \end{pmatrix}$$

be the $m \times mn$ matrix obtained by "continuing" V_n to the right.

Lemma 1 *We have* $W_n W_n^* = mn\mathrm{Id}_m$.

Proof The scalar product of the ith row of W_n and the jth column of W_n^* is equal to

$$\sum_{k=0}^{mn-1} \left(\zeta_{n,i}\overline{\zeta_{n,j}}\right)^k = \begin{cases} mn & \text{if } i = j; \\ 0 & \text{if } i \neq j; \end{cases}$$

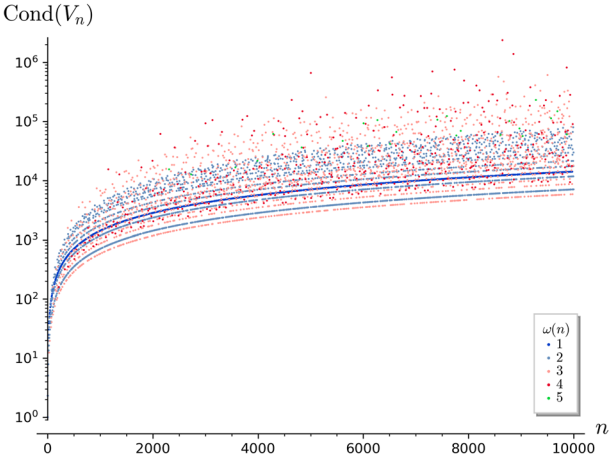

Fig. 1 The condition number of V_n with n squarefree, $1 < n < 10,000$. The data is partitioned according to the number $\omega(n)$ of prime factors of n

where we used the formula for the sum of a geometric progression. The claim follows. □

Let $a_n(j)$ denote the coefficient of X^j in the nth cyclotomic polynomial $\Phi_n(X)$, that is,

$$\Phi_n(X) = \sum_{j=0}^{m} a_n(j) X^j.$$

The study of the coefficients of the cyclotomic polynomials has a very long history, which goes back at least to Gauss. For a survey, see [20]. Let $A(n)$ be the maximum of the absolute values of $a_n(0), \ldots, a_n(m-1)$. We need the following result of Vaughan [23].

Theorem 2 *We have* $A(n) > \exp\left(n^{\log 2/\log\log n}\right)$ *for infinitely many positive integers* n.

Let C_n be the *companion matrix* of $\Phi_n(X)$, which is the $m \times m$ matrix defined as

$$C_n := \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_n(0) \\ 1 & 0 & \cdots & 0 & -a_n(1) \\ 0 & 1 & \cdots & 0 & -a_n(2) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_n(m-1) \end{pmatrix},$$

and let

$$S_n := \left(\mathrm{Id}_m \mid C_n^m \mid C_n^{2m} \mid \cdots \mid C_n^{(n-1)m}\right)$$

be the $m \times mn$ matrix obtained by the juxtaposition of the first n powers of C_n^m.

Lemma 2 *We have* $V_n^{-1} W_n = S_n$.

Proof Let $K := \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field. For each $k \in \{0, \ldots, m-1\}$ we have that $1, \zeta_{n,k}, \zeta_{n,k}^2, \ldots, \zeta_{n,k}^{m-1}$ is a basis of K over $\mathbb{Q}$. Moreover, multiplication by $\zeta_{n,k}$ is a $\mathbb{Q}$-linear map $K \to K$ whose transformation matrix respect to the aforementioned basis is equal to C_n. Therefore, if $z_0, \ldots, z_{m-1} \in K$ satisfy

$$\begin{pmatrix} z_0 \\ z_1 \\ \vdots \\ z_{m-1} \end{pmatrix} = V_n \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix}$$

for some $c_0, \ldots, c_{m-1} \in \mathbb{Q}$, then it follows that

$$\begin{pmatrix} \zeta_{n,0}^{j} z_0 \\ \zeta_{n,1}^{j} z_1 \\ \vdots \\ \zeta_{n,m-1}^{j} z_{m-1} \end{pmatrix} = V_n C_n^j \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{m-1} \end{pmatrix}$$

for every integer $j \geq 0$. Consequently, we have that

$$\begin{pmatrix} \zeta_{n,0}^{j} & \zeta_{n,0}^{j+1} & \cdots & \zeta_{n,0}^{j+m-1} \\ \zeta_{n,1}^{j} & \zeta_{n,1}^{j+1} & \cdots & \zeta_{n,1}^{j+m-1} \\ \vdots & \vdots & \ddots & \vdots \\ \zeta_{n,m-1}^{j} & \zeta_{n,m-1}^{j+1} & \cdots & \zeta_{n,m-1}^{j+m-1} \end{pmatrix} = V_n C_n^j \mathrm{Id}_m = V_n C_n^j, \tag{1}$$

for every integer $j \geq 0$. Therefore, by juxtaposition of (1) for $j = 0, m, 2m, \ldots, (n-1)m$, we obtain that $W_n = V_n S_n$. The claim follows. □

Lemma 3 *We have* $\|V_n^{-1}\|^2 = \frac{1}{mn} \sum_{k=0}^{n-1} \|C_n^{km}\|^2$.

Proof From Lemmas 1 and 2, it follows that

$$mn\|V_n^{-1}\|^2 = mn\mathrm{Tr}\left(V_n^{-1}\left(V_n^{-1}\right)^*\right) = \mathrm{Tr}\left(V_n^{-1} W_n W_n^* \left(V_n^{-1}\right)^*\right) = \mathrm{Tr}(S_n S_n^*).$$

Moreover, by the definition of S_n, we have that

$$\begin{aligned} \mathrm{Tr}(S_n S_n^*) &= \mathrm{Tr}\left(\left(\mathrm{Id}_m \mid C_n^m \mid \cdots \mid C_n^{(n-1)m}\right) \begin{pmatrix} \mathrm{Id}_m \\ (C_n^m)^* \\ \vdots \\ \left(C_n^{(n-1)m}\right)^* \end{pmatrix}\right) \\ &= \sum_{k=0}^{n-1} \mathrm{Tr}\left(C_n^{km}\left(C_n^{km}\right)^*\right) = \sum_{k=0}^{n-1} \|C_n^{km}\|^2, \end{aligned}$$

and the claim follows.

Lemma 4 *Let k be a positive integer and let*

$$C := \begin{pmatrix} 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & c_{k-1} \end{pmatrix} \in \mathbb{C}^{k \times k}.$$

Then, for every integer $j \in [1, k]$, the $(k-j)$th column of C^j is equal to $\begin{pmatrix} c_0 & c_1 & \cdots & c_{k-1} \end{pmatrix}^{\intercal}$.

Proof Actually, a stronger claim holds: For every integer $j \in [1, k]$, the 0th, 1th, ..., $(k-j)$th columns of C^j are equal to the $(j-1)$th, jth, ..., $(k-1)$th columns of C, respectively. This follows easily by induction on j.

We are ready to prove Theorem 1. From Lemmas 3 and 4, it follows that

$$\|V_n^{-1}\|^2 = \frac{1}{mn}\sum_{k=0}^{n-1}\|C_n^{km}\|^2 \geq \frac{1}{mn}\|C_n^m\|^2 \geq \frac{1}{mn}\sum_{j=0}^{m-1}|a_n(j)|^2 \geq \frac{1}{mn}A(n)^2.$$

In turn, this implies that

$$\mathrm{Cond}(V_n) = \|V_n\|\|V_n^{-1}\| = m\|V_n^{-1}\| \geq \sqrt{\frac{m}{n}}A(n) \geq \frac{1}{\sqrt{n}}A(n).$$

As a consequence, Theorem 2 yields that

$$\mathrm{Cond}(V_n) > \exp\left(n^{\log 2/\log\log n}\right)/\sqrt{n},$$

for infinitely many positive integers n. Therefore, for every fixed $r > 0$, we have that

$$\limsup_{n\to+\infty}\frac{\mathrm{Cond}(V_n)}{n^r} = +\infty,$$

so that $\mathrm{Cond}(V_n) \neq O(n^r)$. The proof is complete.

Acknowledgements The authors are members of CrypTO, the group of Cryptography and Number Theory of Politecnico di Torino. A. J. Di Scala and C. Sanna are members of GNSAGA of INdAM. A. J. Di Scala is a member of DISMA Dipartimento di Eccellenza MIUR 2018-2022. E. Signorini is a cryptographer at Telsy S.p.A.

References

1. Ajtai, M.: Generating hard instances of lattice problems. In: Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing, pp. 99–108 (1996)
2. Alkim, E., Ducas, L., Pöppelmann, T., Schwabe, P.: Post-quantum key exchange a new hope. In: 25Th USENIX Security Symposium (USENIX Security 16), pp. 327–343 (2016)
3. Avanzi, R., Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Kyber: Algorithm specifications and supporting documentation, Tech. report
4. Bai, S., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium: Algorithm specifications and supporting documentation, Tech. report, (2021) https://pq-crystals.org/dilithium/data/dilithium-specification-round3-20210208.pdf

5. Basso, A., Bermudo Mera, J.M., D'Anvers, J.-P., Karmakar, A. Roy, S.S., Van Beirendonck, M., Vercauteren, F.: SABER: Algorithm specifications and supporting documentation, Tech. report, (2020), https://www.esat.kuleuven.be/cosic/pqcrypto/saber/files/saberspecround3.pdf
6. Blanco-Chacón, I.: On the RLWE/PLWE equivalence for cyclotomic number fields. Appl. Algebra Eng. Commun. Comput. (2020)
7. Blanco-Chacón, I.: Ring learning with errors: a crossroads between post-quantum cryptography, machine learning and number theory. Irish Math. Soc. Bull. **86**, 17–46 (2020)
8. Blanco-Chacón, I.: RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices. J. Algebra Appl. (2021)
9. Blanco-Chacón , I., López-Hernanz, L.: RLWE/PLWE equivalence for the maximal totally real subextension of the $2^r pq$ -th cyclotomic field, arXiv:2111.13484
10. Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Kyber: A CCA-secure module-lattice-based KEM. In: 2018 IEEE European Symposium on Security and Privacy (EuroS&P), IEEE, pp. 353–367 (2018)
11. Chen, C., Danba, O., Rijneveld, J., Schanck, J.M., Saito, T., Schwabe, P., Whyte, W., Xagawa, K., Yamakawa, T., Zhang, Z.: NTRU: Algorithm specifications and supporting documentation, Tech. report (2020) http://web.archive.org/web/20211110120032/https://ntru.org/release/NIST-PQ-Submission-NTRU-20201016.tar.gz
12. Di Scala, A.J., 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)
13. Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schwabe, P., Seiler, G., Stehlé, D.: CRYSTALS-Dilithium: a lattice-based digital signature scheme. IACR Trans. Cryptograph. Hardw. Embed. Syst. **2018**, 238–268 (2018)
14. Elias, Y., Lauter, K.E., Ozman, E., Stange, K.E.: Ring-LWE cryptography for the number theorist, Directions in Number Theory, Assoc. Women Math. Ser., vol. 3, Springer, Cham, pp. 271–290 (2016)
15. Fouque, P.-A., Hoffstein, J., Kirchner, P., Lyubashevsky, V., Pornin, T., Prest, T., Ricosset, T., Seiler, G., Whyte, W., Zhang, Z.: Falcon: Algorithm specifications and supporting documentation, Tech. report (2020) https://web.archive.org/web/20211215114823/https://falcon-sign.info/falcon.pdf
16. Hülsing, A., Rijneveld, J., Schanck, J., Schwabe, P.: High-speed key encapsulation from NTRU. In: International Conference on Cryptographic Hardware and Embedded Systems. Springer, pp. 232–252 (2017)
17. Langlois, A., Stehlé, D.: Worst-case to average-case reductions for module lattices. Des. Codes Crypt. **75**(3), 565–599 (2015)
18. Lyubashevsky, V., Peikert, C., Regev, O.: Learning with Errors over Rings, Algorithmic Number Theory, vol. 6197, pp. 3–3. Springer, Berlin (2010)
19. Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. J. ACM **56**, 84–93 (2005)
20. Sanna, C.: A survey on coefficients of cyclotomic polynomials. Expo. Math. https://doi.org/10.1016/j.exmath.2022.03.002
21. Signorini, E.: Condition number of cyclotomic Vandermonde matrices, (2022), v1.0.0, GitHub: https://github.com/edoars/cyclovandermonde
22. Stehlé, D., Steinfeld, R., Tanaka, K., Xagawa, K.: Efficient public key encryption based on ideal lattices. In: International Conference on the Theory and Application of Cryptology and Information Security. Springer, pp. 617–635 (2009)
23. Vaughan, R.C.: Bounds for the coefficients of cyclotomic polynomials. Michigan Math. J. **21**(1974), 289–295 (1975)
24. Rosca, M., Stehlé, D., Wallet, A.: On the ring-LWE and polynomial-LWE problems. In: EUROCRYPT 2018-37th Annual International Conference on the Theory and Applications
25. Lyubashevsky, V., Seiler, G.: NTTRU: truly fast NTRU using NTT. TCHES **2019**(3), 180–201 (2019)