Combining strong secrecy with high efficiency: Equivalence of RLWE and PLWE in lattice-based cryptography

Presenter: Rahinatou Yuh Njah Nchiwo; Supervisor: Camilla Hollanti

Co-authors: Iván Blanco-Chacón, Alberto Pedrouzo Ulloa, Beatriz Barbero-Lucas

Motivation

The rapid development of quantum computers poses a serious threat to many widely used encryption and key exchange systems. To address this, researchers are exploring lattice-based cryptography (LBC), a promising approach for building secure systems that can resist quantum attacks. One practical and efficient method within LBC is Polynomial Learning with Errors (PLWE). Its security is closely related to another well-studied problem, called Ring Learning with Errors (RLWE), which is believed to be hard.

In this work [2], we study the equivalence between PLWE and RLWE for certain number fields [3]. Namely, PLWE provides efficiency, while RLWE provides strong security guarantees. We focus on the condition number of the transformation map linking PLWE to RLWE, which measures how much the noise grows during the transformation. Controlling this growth is crucial for preserving both security and efficiency. For specific cyclotomic fields, we provide improved bounds on this noise growth and also present exact values when using a twisted power basis—helping to maintain the equivalence even in more complex cases.

1. Preliminaries

For K a degree m number field and $\mathcal{O}_K$ its ring of integers, let $R_q = \mathcal{O}_K/q\mathcal{O}_K$, $P_q = \mathbb{Z}_q[x]/(f(x))$ with $f(x)$ monic and irreducible over $\mathbb{Z}[x]$, $q \geq 2$ be prime and χ an error distribution.

Polynomial learning with errors (PLWE) problem

Let a_i and s be uniformly sampled from P_q. Given arbitrary many independent samples of the form $(a_i, b_i = a_i s + e_i) \in P_q \times P_q$, where for each i, e_i is drawn from χ over P_q. Recover the secret s.

Ring learning with errors (RLWE) problem

Let a_i and s be uniformly sampled from R_q. Given arbitrary many independent samples of the form $(a_i, b_i = a_i s + e_i) \in R_q \times R_q$, where for each i, e_i is drawn from χ over R_q. Recover the secret s.

2. Equivalence between RLWE and PLWE

Going from PLWE to RLWE is done via the linear transformation

$$\mathbf{V}_f : \mathbb{Z}[x]/(f(x)) \longrightarrow \sigma_1(\mathcal{O}_K) \times \cdots \times \sigma_m(\mathcal{O}_K)$$

$$\sum_{i=0}^{m-1} a_i x^i \longmapsto \underbrace{\begin{pmatrix} 1 & \theta_1 & \dots & \theta_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \theta_m & \dots & \theta_n^{m-1} \end{pmatrix}}_{\mathbf{V}_f} \begin{pmatrix} a_0 \\ \vdots \\ a_{m-1} \end{pmatrix}.$$

Condition number for Cyclotomic fields

The distortion is measured by the condition number defined as

$$\mathrm{Cond}(\mathbf{V}_f) := ||\mathbf{V}_f||||\mathbf{V}_f^{-1}||.$$

For cyclotomic fields, $f(x) = \Phi_n(x)$, the n^{th} cyclotomic polynomial.

Equivalence. The PLWE and RLWE problems are said to be equivalent if the condition number grows at most polynomially in m.

Proposition 1. Let $n \geq 2$ and $m = \varphi(n)$ and $\omega(n)$ the number of prime factors of the conductor n and rad(n) the product of the prime factors.

a) If $n = p^k$, then $\mathrm{Cond}(\mathbf{V}_{\Phi_n}) \leq 4m^2$.

b) If $n = p^l q^s r^t$, then $\mathrm{Cond}(\mathbf{V}_{\Phi_n}) \leq 4\varphi(\mathrm{rad}(n))^{\omega(n)-1} m^2$.

c) If $n = p^a q^b r^c s^d$, then $\mathrm{Cond}(\mathbf{V}_{\Phi_n}) \leq 4\varphi(\mathrm{rad}(n))^4 m^2$.

d) If $n = p^a q^b r^c s^d t^e$ and then $\mathrm{Cond}(\mathbf{V}_{\Phi_n}) \leq 4\varphi(\mathrm{rad}(n))^7 m^2$.

e) If $n = p^a q^b r^c s^d t^e u^f$, then $\mathrm{Cond}(\mathbf{V}_{\Phi_n}) \leq 4\varphi(\mathrm{rad}(n))^{11} m^2$.

Observation. The condition number grows polynomially in the degree m but depends on $\omega(n)$.

3. Generalizing the result

We state below a general result in [1].

Theorem 1. Let $n \geq 2$ and denote by $A(n)$ the largest coefficient, in absolute value, of $\Phi_n(x)$, $m = \varphi(n)$, and k fixed. If rad(n) $= p_1 \cdots p_k$, then:

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

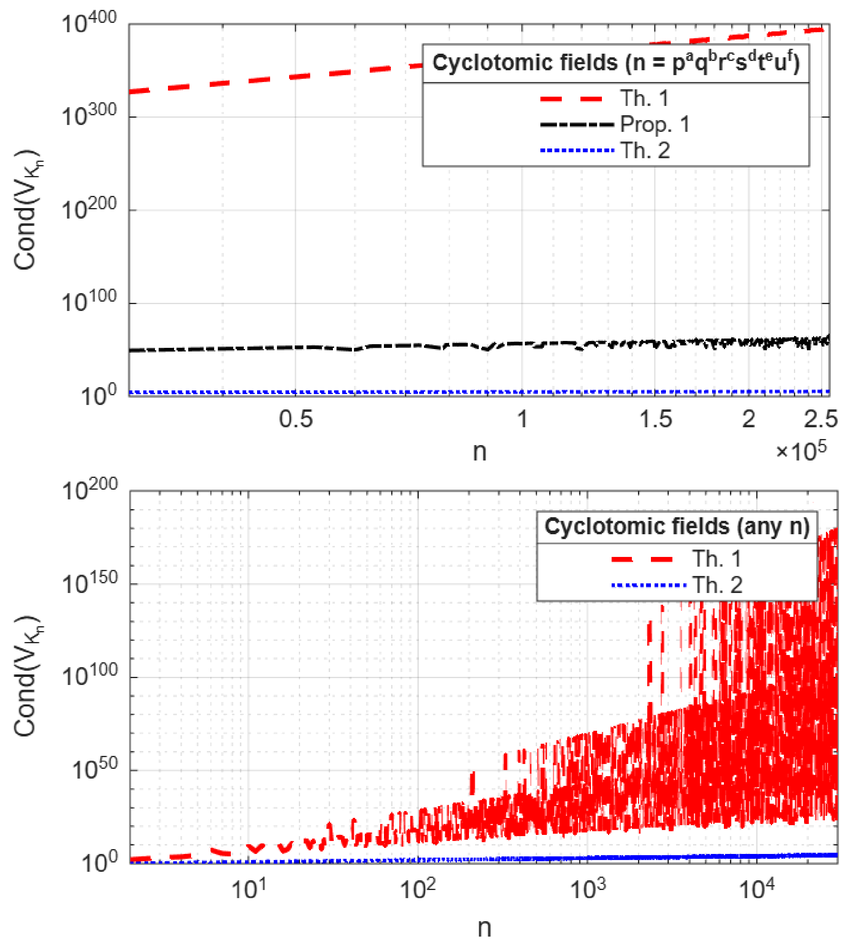
Our result [2] stated below shows that under the twisted basis , the condition number grows polynomially even for the case of conductors divisible by a logarithmically growing number of primes $\omega(n)$.

Theorem 2. For $n = p_1^{k_1} \cdots p_{\omega(n)}^{k_{\omega(n)}}$ we have

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

where TV_{K_n} corresponds to the transformation involving the twisted basis.

4. Analysis



References

[1] Iván Blanco-Chacón. On the RLWE/PLWE equivalence for cyclotomic number fields. *Applicable Algebra in Engineering, Communication and Computing*, 33(1):53–71, 2022.

[2] Iván Blanco-Chacón, Alberto Pedrouzo-Ulloa, Rahinatou Y Njah Nchiwo, and Beatriz Barbero-Lucas. Fast polynomial arithmetic in homomorphic encryption with cyclo-multiquadratic fields. *Cryptography and Communications*, pages 1–35, 2025.

[3] Miruna Rosca, Damien Stehlé, and Alexandre Wallet. On the ring-LWE and polynomial-LWE problems. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 146–173. Springer, 2018.