On the R/P-LWE equivalence for cyclotomic subextensions and cryptoanalytic implications

Iván Blanco Chacón

University of Alcalá

04/04/2022

Summary

- Motivation
- The RLWE and PLWE cryptosystems
- RLWE/PLWE equivalence: the cyclotomic case
- RLWE/PLWE equivalence: the maximal totally real subextension
- Some cryptoanalysis

Motivation: NIST figures (Third round, April 2022)

Category	Number of candidates
Code-based	3
Lattice-based	6
Multivariate-based	2
Elliptic curve-based	1
Hash-based/other	2

Table: NIST Round 3 finalists.

Motivation: Lattice-based cryptography

Based on the unfeasibility (proved or conjectural) of different problems dealing with lattices:
Shortest Vector Problem and Closest Vector Problem: proved NP hard over the class of arbitray algebraic lattices (if no extra structure is assumed)

- NTRU (Hoffstein, Piffer, Silverman 1996): arithmetic on $\mathbb{Z}[x]/(x^n - 1)$.
- LWE (Regev 2005): linear algebra in $\mathbb{Z}^n$ (fixed one basis)
- PLWE (Stehlé, 2009): lattices attached to quotient polynomial rings.
- RLWE (Lyubashevsky, Peikert, Regev, 2010): lattices attached to number fields.

Motivation: Lattices (definitions and examples)

Definition

A lattice is (Λ, ρ) where Λ is a torsion free finitely generated abelian group and $\rho : \Lambda \to \mathbb{R}^n$ is a group monomorphism. We say that Λ has full rank if its rank is n.

- Example 1: $\Lambda = \mathbb{Z}^n$, $\rho =$inclusion in $\mathbb{R}^n$.
- Example 2: K number field of degree $n = r + 2s$, r real embeddings, s pairs of complex embeddings, $\Lambda = O_K$ ring of integers, $\rho : \Lambda \to \mathbb{R}^r \times \mathbb{C}^{2s}$, the canonical embedding.
- Example 3: $\Lambda = \mathbb{Z}[x]/(f(x))$ with $f(x) \in \mathbb{Z}[x]$ monic irreducible of degree n, $\rho\left(\sum_{k=0}^{n-1} a_k x^k\right) = (a_0, \ldots, a_{n-1})$ (coefficient embedding).

The RLWE cryptosystem: foundations

K number field of degree n, O_K ring of integers.

Definition (Ring Learning With Errors oracles)

Let q be prime, $s \in O_K/qO_K$, χ a O_K/qO_K-valued random variable. A RLWE-oracle is an algorithm $A_{s,\chi}$ which:

- samples $a \in O_K/qO_K$ (uniformly) and samples e from χ.
- returns $(a, as + e) \in O_K/qO_K \times O_K/qO_K$.

Definition (The RLWE problem)

- Search version: Given $A_{s,\chi}$, the adversary must recover s by having access to arbitrarily many samples.
- Decisional version: Given $A = A_{s,\chi}$ or uniform, the adversary must decide whether $A = A_{s,\chi}$ or uniform by having access to arbitrarily many samples.

The RLWE cryptosystem: definition (Lyubashevsky, Peikert, Regev 2009)

q prime, χ is an O_K/qO_K-valued Gaussian, covariance matrix bounded entry-wise by $\alpha n^{1/4}$, $\alpha < \sqrt{\frac{log(n)}{n}}$.

1. Key generation: choose $a \in O_K/qO_K$ uniformly at random and choose s, e sampled from χ. The secret key will be s and the public key will be the pair $(a, b = as + e)$.
2. Encryption: take a plaintext z consisting of a stream of bits and regard it as a polynomial in O_K/qO_K, mapping each bit to a coefficient, say, $z \in R_q$. Choose r, e_1, e_2 sampled from χ. Set $u = ar + e_1$ and $v = br + e_2 + \lfloor \frac{q}{2} \rfloor z$.
3. Decryption: Perform $v - us = er + e_2 - e_1 s + \lfloor \frac{q}{2} \rfloor z$ and round the coefficients either to zero or to $\lfloor \frac{q}{2} \rfloor$, whichever is closest mod q.

The RLWE cryptosystem: discussion

Theorem (Lyubashevsky, Peikert, Regev)

The PLWE cryptosystem is correct (i.e. decryption undoes encryption) and pseudorandom.

Theorem (Lyubashevsky et al for K cyclotomic, Rosca et al for Galois number fields 2017)

There exists a quantum polynomial reduction from γ-SVP over ideal lattices to decision RLWE.

BUT...

γ-SVP is not proved to be NP-hard for that γ, and even less when restricted to the class of ideal lattices on number fields. Empirical evidence suggests so, but still...

The PLWE problem

Instead of working with O_K, use a polynomial ring $R_q = \mathbb{F}_q[x]/(f(x))$, $f(x) \in \mathbb{F}_q$ monic irreducible.
The distribution χ now should take values on R_q.
The learning problem with these choices is called PLWE (Polynomial Learning With Errors)
Why using PLWE instead of RLWE? Because it is easier to implement on a computer.
PLWE and RLWE are not always equivalent:

- The field may not be monogenic: i.e. $O_K \neq \mathbb{Z}[\alpha]$ (in general, the latter is an order in the former)
- Even if monogenic, for RLWE, O_K is endowed with the Minkowski embedding, $\mathbb{Z}[x]/(f(x))$ with the coefficient embedding and the isomorphism distort the distribution.
- For cyclotomics of 2-power degree, the isomorphism is a scaled isometry, so both problems are equivalent.

RLWE/PLWE equivalence

Assume K monogenic from now on.
We study the equivalence between *RLWE*, attached to $\mathbb{Z}[\alpha]$ with Galois embedding, and PLWE, attached to $\mathbb{Z}[x]$, and the coordinate embedding.
For $g(x) = \sum_{i=0}^{n-1} a_i x^i$, consider the map $\mathbb{Z}[x]/(f(x)) \to \mathbb{Z}[\alpha]$, the last identified with its Galois image:

$$(a_0, \ldots, a_{n-1}) \mapsto (\sum_{i=0}^{n-1} a_i \sigma_1(\alpha)^i, \ldots, \sum_{i=0}^{n-1} a_i \sigma_n(\alpha)^i),$$

The transformation is given by multiplication with the Vandermonde matrix $V_f := (\sigma_k(\alpha)^j))$. Hence, the problems are equivalent if the distortion caused by the matrix is poynomial in n.
Want: to study $||V_f||||V_f^{-1}||$, where $||A|| := \sqrt{Tr(A^* A)}$.

RLWE/PLWE equivalence: the cyclotomic case

The n-th cyclotomic polynomial:

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

Properties:
$\Phi_n(x)$ is irreducible of degree $\phi(n)$.
$K_n := \mathbb{Q}(\zeta)$ is monogenic and Galois.
$\mathcal{O}_{K_n} = \mathbb{Z}[\zeta] \cong \mathbb{Z}[x]/(\Phi_n(x))$, but the embeddings may be very different.
Goal: to bound the condition number V_{Φ_n}.

RLWE/PLWE equivalence: the cyclotomic case

For $m = p_1^{e_1} \dots p_k^{e_k}$, denote $rad(n) = p_1 \dots p_k$.
If $\Phi_n(x) = \sum_{i=0}^{\phi(n)} c_i x^i$, denote $A(n) = \max_{i=0}^{\phi(n)} \{|c_i|\}$.

Theorem (B. 2020)

Notations as before. Let $k > 1$ be fixed and $rad(n) = p_1 \dots p_k$. Then

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

Idea of proof:

- Write the entries in $V_{\Phi_n}^{-1}$ as quotients of symmetric polynomials in the n-th primitive roots (Rosca-Stehlé-Wallet, 2016).
- Use a bound for $A(n)$ due to Bateman which is polynomial in m once k is fixed.
- Some nasty bounds for the numerators.

RLWE/PLWE equivalence: the cyclotomic case. Sharper bounds

Theorem (B. 2020)

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 $Cond(V_{\Phi_n}) \leq 4(p-1)m$.*

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

Key inputs: classical bounds for $A(n)$ due to Bang (1895) for 2 primes. Bloom (1968) for 3 primes. Erdös for 4 primes and maybe 5.

RLWE/PLWE equivalence: the general bound

Theorem (Barbero, B., Njah, 2021)

- *If* $m = p^a q^b r^c s^d$, *then* $Cond(V_{\Phi_n}) \leq 2\phi(rad(n))^3 m^2$.
- *If* $n = p^a q^b r^c s^d t^e$ *and* $m = \phi(n)$, *then* $Cond(V_{\Phi_n}) \leq 2\phi(rad(n))^6 m^2$.
- *If* $n = p^a q^b r^c s^d t^e u^f$, *then* $Cond(V_{\Phi_n}) \leq 2m\phi(rad(n))^5$.

But finally, the question has been closed for general n:

Theorem (Sanna, di Scala, Signorini, 2022)

There exist infinitely many $n \geq 2$ *such that*

$$Cond(V_n) \geq exp\left(n^{\frac{log(2)}{loglog(n)}}\right) / \sqrt{n}.$$

Hence, for each $r \geq 1$, $Cond(V_n) \neq O(n^r)$. *Consequently, RLWE and PLWE are not equivalent for general* $n \geq 2$.

RLWE/PLWE equivalence: the maximal totally real cyclotomic subextension

$K_n^+ =$ maximal totally real subfield of $K_n = \mathbb{Q}(\zeta)$, the n-th cyclotomic field.
$K_n^+ = \mathbb{Q}(\psi_n)$ with $\psi_n = \zeta_n + \zeta_n^{-1} = 2cos\left(\frac{2\pi}{n}\right)$
$\mathcal{O}_{K_n^+} = \mathbb{Z}(\psi_n)$, i.e. K_n^+ is monogenic (and Galois).
Denote $\Phi_n^+(x)$ the minimal polynomial of ψ_n
Question: Is RLWE equivalent to PLWE for K_n^+?
Absence of noice: Gaussian elimination sends PLWE-samples to RLWE-samples in $O(m^3)$-time via the transformation matrix.
$V_{K_n^+}$ exponentially amplifies the noise (real nodes, hence exponential condition number, Gautschi).

RLWE/PLWE equivalence: the maximal totally real cyclotomic subextension

Assume $n = 4p$, p prime.

Definition

Tchebychev polynomials

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 $n \geq 2$.

Proposition (Kuian, 2005)

Let $x_k^{(N)} = \cos\left(\frac{2k-1}{2N}\pi\right)$. *Denote* $V_N = \left(T_i(x_k^{(N)})\right)_{i,k-1=0}^{N}$. *Then,* $\mathrm{Cond}(V_N)$ *is polynomial in* N.

Write $T_i(x_k^{(p)}) = Q_i(2x_k^{(p)})$,

RLWE/PLWE equivalence: the maximal totally real cyclotomic subextension

Lemma

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

Denote: $Q_{4p} := \left(a_i(2x_k^{(p)})\right)_{i,k-1=0}^{p-1}$.

$$\mathrm{Cond}(Q_{4p}) \leq p(p+1). \tag{0.1}$$

Restrict the nodes only to those with $2k+1$ coprime with p.
$T_i(x_{\frac{p-1}{2}}^{(p)}) = \cos\left(\frac{i\pi}{2}\right) \in \{0, \pm 1\}$ for $0 \leq i \leq p-1$

RLWE/PLWE equivalence: the maximal totally real cyclotomic subextension

Still denote by Q_{4p} the result of permuting the first and $\frac{p-1}{2}$-th rows.
Eliminate first row, obtain $M_{4p} = Q_{4p}R$:

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

Theorem (B. 2020)

$Cond(N_{4p}) = O(p^4)$ and the map

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

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

RLWE/PLWE equivalence: the maximal totally real cyclotomic subextension

Recently, we have proved:

Theorem (B.-López-Hernanz 2021)

For $r \geq 2$, p and q primes (or 1), then $Cond(N_{2^r pq}) = O((2^r pq)^4)$ and the map

$$\begin{array}{rcl} \Psi : \mathbb{Z}[x]/\Phi_{2p}^{+}(x) & \to & \sigma_1((\mathcal{O}_{K^+_{2^r pq}}) \times \ldots \sigma_{2^{r-2}(p-1)(q-1)}((\mathcal{O}_{K^+_{2^r pq}}) \\ \mathbf{u} & \mapsto & N_{4p}\mathbf{u} \end{array}$$

is a lattice (and ring) monomorphism. The image is a sublattice of (explicit) finite index λ and the map

$$x \mapsto \Psi(\lambda x)$$

has also condition number $O((2^r pq)^4)$. Consequently, R/P-LWE are equivalent.

Why K_n^+?: cryptoanalysis

Theorem (Elias, Lauter et al., 2016)

If K satisfies the following six conditions, there is a polynomial time attack to the search version of the associated RLWE scheme:

1. $K = \mathbb{Q}(\beta)$ *is Galois of degree* n.
2. *The ideal* (q) *splits totally in* $\mathcal{O}_K$.
3. K *is monogenic, i.e,* $\mathcal{O}_K = \mathbb{Z}[\beta]$.
4. $Cond(V_f) = O(n^r)$, r *fixed,* f *minimal poly of* β.
5. $f(1) \equiv 0 \pmod{q}$.
6. *The prime* q *can be chosen suitably large.*

Can relax $f(1) = 0 \pmod{q}$ to $f(\theta) = 0$ with θ of *small order* or of *small residue* mod q.

Why K_n^+?: cryptoanalysis

$\alpha = \pm 1$ is never a cyclotomic root of Φ_n if $(n, q) = 1$.

Example (Durán, 2021)

For $\Phi_{61}(x)$, $\alpha = 2$ is a root modulo $q = 2305843009213693951$ and for $\sigma = 0.4$, Lauter's attack holds. Same with $\Phi_{85}(x)$, $\alpha = 2$, $q = 9520972806333758431$ and $\sigma = 0.1$.

Fact: $\Phi_n(x) := \Phi_n^+(x + x^{-1})x^{\frac{\phi(n)}{2}}$.

Fact: $\Phi_{2^r k}^+(x) = \frac{\Phi_k^+(u_{2^r}(x))}{\Phi_k^+(u_{2^{r-1}}(x))}$, $u_n(x) := 2t_n(x/2)$.

Proposition (B., López-Hernanz, 2021)

For $r \geq 2$ and $k \geq 3$ odd, we have, mod q:

$$\Phi_{2^r}^+(1) = \pm 1; \quad \Phi_{2^r}^+(2) = 2; \quad \Phi_{2^r k}^+(1) = \Phi_{2^r k}^+(2) = 1.$$

GRAZIE PER L'ATTENZIONE!!