Fast Multiplication and the PLWE-RLWE Equivalence

Efe İzbudak
`ephemer4l@liberior.org`

November 13, 2024

Notation and distribution

Definition (RLWE distribution)

Let K be a number field and $\mathcal{O}_K$ be its ring of integers. For rational prime q, $s \in R_q = \mathcal{O}_K / q\mathcal{O}_K$ and error distribution χ on R_q the RLWE distribution $\mathcal{A}_{s,\chi}$ is given by

$$\mathcal{A}_{s,\chi} = \left\{ (a, b) \in R_q \times R_q \;\middle|\; \begin{array}{l} a \leftarrow U(R_q), \\ e \leftarrow \chi, \\ b = a \cdot s + e \mod q \end{array} \right\}$$

That is, the joint probability distribution of random variables **a** and **b** is given by

$$\mathbb{P}_{s,\chi}(a_0, b_0) = \mathbb{P}[\mathbf{a} = a_0]\mathbb{P}[\mathbf{b} = b_0 \mid \mathbf{a} = a_0] = \mathbb{P}_{s,\chi}(a_0, b_0) = \frac{1}{|R_q|}\bar{\chi}(b - a_0 s)$$

where $\bar{\chi}(e') = \sum_{\substack{e \in R \\ e \mod q = e'}} \chi(e)$

RLWE Problems

Definition (Decision RLWE)

Given m independent samples $(a_i, b_i) \in R_q \times R_q$, $i \in \{1, \dots, m\}$ determine whether these samples are

(i) from $\mathcal{A}_{s,\chi}$ for some fixed s

(ii) from the uniform distribution on $R_q \times R_q$

Definition (Search RLWE)

Given m samples $(a_i, b_i) \in \mathcal{D}_{s,\chi}$, $i \in \{1, \dots, m\}$, where $s \leftarrow U(R_q)$, find s.

Remark

Decision RLWE is the problem that we base our cryptosystems on.

Hardness of RLWE

Theorem ([LPR10], informal)

For $m = poly(n)$, the cyclotomic ring R of degree n over $\mathbb{Z}$ and appropriate choices of modulus q and error distribution χ of error rate $\alpha < 1$, solving the $RLWE_{q,\chi,m}$ problem is at least as hard as quantumly solving the SVP_γ problem on arbitrary ideal lattices in R for $\gamma = poly(n)/\alpha$.

Worst case approx-SVP inR
on ideal lattices in R $\leqslant$ *search RLWE* $\leqslant$ *decision RLWE*

(quantum,
any $R = \mathcal{O}_K$)

(classical,
cyclotomic R)

Hardness of RLWE

Theorem ([PRS17], informal)

Let K be any number field of degree n and $R = \mathcal{O}_K$ be its ring of integers. For large enough modulus q and appropriate choice of error distribution χ of error rate $\alpha < 1$, solving the $\mathrm{RLWE}_{q,\chi,m}$ problem is at least as hard as quantumly solving the SVP_γ problem on arbitrary ideal lattices in R for $\gamma = \max\{\eta(\mathcal{I}) \cdot \sqrt{2}/\alpha \cdot \omega(1), \sqrt{2n}/\lambda_1(\mathcal{I}^\vee)\}$.

Worst case approx-SVP on ideal lattices in R $\leqslant$ *decision RLWE*

(quantum, any $R = \mathcal{O}_K$*)*

Definition of PLWE

Definition (PLWE Distribution)

Let $f(x)$ be a monic irreducible polynomial in $\mathbb{Z}[x]$. Denote by $\mathcal{O}_f$ the quotient ring $\mathbb{Z}[x]/(f(x))$ and set $R_q = \mathcal{O}_f/q\mathcal{O}_f$. For $s \in R$ and χ an error distribution over R, the PLWE distribution $\mathcal{B}_{s,\chi}$ is given by

$$\mathcal{B}_{s,\chi} = \left\{ (a, b) \in R_q \times R_q \;\middle|\; \begin{array}{l} a \leftarrow U(R_q), \\ e \leftarrow \chi, \\ b = a \cdot s + e \mod q \end{array} \right\}$$

PLWE Problems

Definition (Decision PLWE)

Given m independent samples $(a_i, b_i) \in R_q \times R_q$, $i \in \{1, \dots, m\}$ determine whether these samples are

(i) from $\mathcal{B}_{s,\chi}$ for some fixed s

(ii) from the uniform distribution on $R_q \times R_q$

Definition (Search PLWE)

Given m samples $(a_i, b_i) \in \mathcal{B}_{s,\chi}$, $i \in \{1, \dots, m\}$, where $s \leftarrow U(R_q)$, find s.

Why look for new fields?

Theorem ([Eli+16], [BDS24], informal)

If the polynomial $f(x)$ has a root α of small order and small residue in a field extension of $\mathbb{F}_q$ the decision PLWE problem can be solved in polynomial time.

Theorem ([CDW17])

Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$ where K is a cyclotomic number field of prime power conductor. Assuming GRH, there exists a quantum polynomial time algorithm which returns an element $v \in \mathfrak{a}$ with

$$\|v\|_{Euc} \leqslant N\mathfrak{a}^{1/n} exp(O(\sqrt{n}))$$

Why Maximal Totally Real Subfields of Cyclotomic Fields?

Theorem ([BL24], [Bla22b], informal)

The small root attacks for $\alpha = \pm 2$ and $\alpha = \pm 1$ are ineffective when the irreducible polynomial $f(x)$ is defined over the maximal totally real subextension of the cyclotomic field.

Remark

The ring of integers of a maximal totally real subextension of a cyclotomic field is not in general an ideal of the ring of integers of the cyclotomic field.

Discrete Cosine Transform

Definition (DCT)

Let $N \in \mathbb{Z}^+$ and $a(k)$ a finite real sequence of N elements. The non-scaled type-III DCT of $a(k)$ is th sequence

$$a(\hat{j}) = \frac{a(0)}{2} + \sum_{i=1}^{N-1} a(i) \cos\left(\frac{2\pi(2j+1)i}{4N}\right), \quad 0 \leqslant j \leqslant N-1.$$

The "inverse" transform is called the type-II DCT and is given by

$$a'(j) = \sum_{i=0}^{N-1} a(i) cos\left(\frac{2\pi(2i+1)j}{4N}\right), \quad 0 \leqslant j \leqslant N-1.$$

Matrix representations

The DCT and inverse DCT transforms have the matrix representations

$$DCT(\mathbf{a}) = C_N S_N^{-1}\mathbf{a}$$
$$IDCT(\mathbf{a}) = C_N^T\mathbf{a}$$

where

$$(C_N)_{ij} = \cos\left(\frac{2\pi(2i+1)j}{4N}\right) \quad \text{for } i,j = 0,1,\ldots,N-1$$

and

$$S_N = \begin{bmatrix} 2 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}.$$

"Inverse" relation

Lemma

For any real finite sequence $a(k)$, $k = 0, 1, \ldots, N-1$, we have

$$IDCT(DCT(\mathbf{a})) = \frac{N}{2}\mathbf{a}$$

or in matrix notation

$$C_N^T C_N S_N^{-1} = \frac{N}{2} I$$

Idea of proof.

Column sums of C_N are 0. $\square$

Setup

Condition number

Definition (Condition number)

Let $A \in \mathrm{GL}(\mathbb{C})$ be an invertible matrix with complex entries. The condition number of A is given by

$$\kappa_F(A) = ||A||_F ||A^{-1}||_F$$

where $|| \cdot ||_F$ is the Frobenius norm, i,e,

$$||A||_F^2 = \mathrm{Tr}(A^* A)$$

Setup

Condition number

Lemma

The condition number of the cosine matrix C_N is

$$\kappa_F(C_N)^2 = \|C_N\|_F^2 \|C_N^{-1}\|_F^2 = N^2 + \frac{N-1}{2} = O(N^2)$$

and in particular we have

$$\|C_N\|_F^2 = N + \frac{N(N-1)}{2}$$
$$\|C_N^{-1}\|_F^2 = \frac{2N-1}{N}$$

Idea of proof.

Follows from the previous lemma directly. $\square$

Setup

Previous results

Theorem ([DD12], informal)

RLWE and PLWE problems are equivalent for conductor $2^k p$ or $2^k pq$ where p, q are primes with $q < p$.

Theorem ([RSW18], informal)

RLWE and PLWE problems are equivalent for family of polynomials $f_{na}(x) = x^n - a$, $n \geqslant 2$, $a \geqslant 1$ and for family of polynomials $f_{n,\epsilon_0,\epsilon_1} = x^n + \epsilon_1 x + \epsilon_0$ for $\epsilon_i = \pm 1$.

Theorem ([Bla22a], informal)

RLWE and PLWE problems are equivalent for cyclotomic fields if the conductor is divisible by a bounded number of primes.

Setup

Chebyshev polynomials

Definition (Chebyshev polynomials)

The polynomials given recursively by

$$T_0(x) = 1$$
$$T_1(x) = x$$
$$T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$$

are called Chebyshev polynomials. We define modified Chebyshev polynomials by

$$V_i(x) = 2T_i(x/2) \text{ for } i \geqslant 1$$

Setup

Structure of the maximal real subfield

- Let $\psi_n = \zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$ so $\mathbb{Q}(\psi_n) = \mathbb{Q}(\zeta_n)^+$ is the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_n)$ and the ring of integers of $\mathbb{Q}(\psi_n)$ is $\mathbb{Z}[\psi_n] \cong Z[x]/(\Psi_n(x))$ where $\Psi_n(x)$ is the minimal polynomial of ψ_n of degree ϕ_n
- The modified Chebyshev polynomials V_i, $i \in \{1, \ldots, m-1\}$ where $m = \phi(n)/2$ form a $\mathbb{Z}$-basis of $\mathbb{Z}[x]/(\Psi_n(x))$.
- For the conductor $n = 2^r3^s$ we have $m = \phi(n)/2 = 2^{r-1}3^{s-1}$.
- For the equivalence it is enough to show that the Minkowski embedding $\mathcal{M}\colon \mathbb{Z}[x]/(\Psi_n(x)) \to \mathbb{R}^m$ which is given by

$$a_0V_0(x) + a_1V_1(x) + \cdots + a_{m-1}V_{m-1}(x) \mapsto M(a_0, a_1, \ldots, a_{m-1})^T$$

is “well-behaved”.

"Well-behaved" embedding

Matrix M

We say that the embedding is "well-behaved" if M is well-conditioned. That is. if the condition number of M is bounded by some polynomial in n. The matrix M is given explicitly by

$$M = \begin{bmatrix} 1 & 2\cos\left(\frac{2\pi}{n}\right) & 2\cos\left(\frac{2\pi\cdot 2}{n}\right) & \dots & 2\cos\left(\frac{2\pi(m-1)}{n}\right) \\ 1 & 2\cos\left(\frac{2\pi\sigma}{n}\right) & 2\cos\left(\frac{2\pi\sigma\cdot 2}{n}\right) & \dots & 2\cos\left(\frac{2\pi\sigma(m-1)}{n}\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2\cos\left(\frac{2\pi(n/2-1)}{n}\right) & 2\cos\left(\frac{2\pi\cdot 2(n/2-1)}{n}\right) & \dots & 2\cos\left(\frac{2\pi(m-1)(n/2-1)}{n}\right) \end{bmatrix},$$

where $\sigma \in \{1, 2, \dots, n/2\}$ and $(\sigma, n) = 1$.

"Well-behaved" embedding

Matrix V

Of course, M is well-conditioned if and only if the matrix V given by

$$V = \begin{bmatrix} 1 & \cos\left(\frac{2\pi}{n}\right) & \cos\left(\frac{2\pi\cdot 2}{n}\right) & \dots & \cos\left(\frac{2\pi(m-1)}{n}\right) \\ 1 & \cos\left(\frac{2\pi\sigma}{n}\right) & \cos\left(\frac{2\pi\sigma\cdot 2}{n}\right) & \dots & \cos\left(\frac{2\pi\sigma(m-1)}{n}\right) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \cos\left(\frac{2\pi(n/2-1)}{n}\right) & \cos\left(\frac{2\pi\cdot 2(n/2-1)}{n}\right) & \dots & \cos\left(\frac{2\pi(m-1)(n/2-1)}{n}\right) \end{bmatrix},$$

is well-conditioned.

Main theorem

Theorem (RLWE-PLWE equivalence)

Let $r \geqslant 3$, $s \geqslant 1$ and $n = 2^r3^s$. Then PLWE and RLWE problems are equivalent for the maximal real subextension of the n-th cyclotomic field.

Idea of proof.

Realize V as a submatrix of C_N for $n = 4N = 2^r3^s$, that is, $N = 3m/2$. Norm of V is bounded by the norm of C_N. Lower-triangularize to get a bound for the norm of the inverse. $\square$

Fast multiplication

Let p be a polynomial of degree $\leqslant N-1$ in $\mathbb{Z}[x]/(\Psi_n(x))$. Then represent p as

$$p(x) = \sum_{i=0}^{N-1} a_i V_i(x)$$

Define DCT($p(x)$)=DCT($\mathbf{a}$) where $\mathbf{a}$ is the column coefficient matrix of p. Then for

$$x_j = 2\cos\left(\frac{2\pi(2j+1)}{4N}\right), j = 0, 1, \ldots, N-1$$

we have

$$\hat{\mathbf{p}} = 2DCT(p(x))$$

where $\hat{\mathbf{p}} = (p(x_0), p(x_1), \ldots, \ldots, p(x_{N-1}))^T$.

Fast multiplication

Now let $p(x), q(x) \in \mathbb{Z}[x]$ and $r(x) = p(x)q(x)$. Then the vector evaluations satisfy

$$\hat{\mathbf{r}} = \hat{\mathbf{p}} \odot \hat{\mathbf{q}}$$

the calculation of the coefficient vector of r is then done by

$$\frac{4}{N} IDCT(DCT(p(x)) \odot DCT(q(x)))$$

The overall complexity of computing the DCT and IDCT matrices is $O(N \log N)$ via [Kok97].

Fast Basis Change in $\mathbb{Z}[x]/(\Psi_n(x))$

Theorem ([Pan98])

Any polynomial of degree at most $N-1$ can be evaluated on the Chebyshev nodes x_j, $j = 0, \ldots, N-1$ in $O(N \log N)$ operations.

Theorem

Interpolation to a polynomial of a degree at most $N-1$ on the Chebyshev node set can e performed with $O(N \log N)$ complexity.

Lemma

Given a polynomial of degree less than or equal to $m-1$, the complexity of the change of basis between the power basis $\{1, x, \ldots, x^{m-1}\}$ and $\{V_0(x), V_1(x), \ldots, V_{m-1}(x)\}$ is $O(m \log m)$.

Polynomial multiplication

Theorem

Given two polynomials $a, s \in \mathbb{Z}[x]/(\Psi_n(x))$ in the power basis, their product as can be computed with complexity $O(n \log n)$.

References I

I. Blanco-Chacón, R. Durán-Díaz, and R. M. Sanchéz-Ledesma.
"A Generalized Approach to Root-based Attacks towards PLWE."
In: Submitted (2024).

I. Blanco-Chacón and L. López-Hernanz.
"RLWE/PLWE equivalence for the maximal totally real subextension of the $2^r pq$-th cyclotomic field."
In: *Advances in Mathematics of Communications* 18.5 (2024), pp. 1343–1363.

I. Blanco-Chacón.
"On the RLWE/PLWE equivalence for cyclotomic number fields."
In: *Appl. Algebra Eng., Commun. Comput.* 33.1 (2022), pp. 53–71.

References II

I. Blanco-Chacón.
"RLWE/PLWE equivalence for totally real cyclotomic subextensions via quasi-Vandermonde matrices."
In: *Journal of Algebra and Its Applications* 21.11 (2022).

R. Cramer, L. Ducas, and B. Wesolowski.
"Mildly Short Vectors in Cyclotomic Ideal Lattices in Quantum Polynomial Time."
In: *Journal of the ACM (JACM)* 58.2 (2021), pp. 1–26.

L. Ducas and A. Durmus.
"Ring-LWE in Polynomial Rings."
In: *Public Key Cryptography – PKC 2012. PKC 2012. Lecture Notes in Computer Science*, vol. 7293. Springer, 2012.

References III

- Y. Elias, K. Lauter, E. Ozman, and K. Stange.
  "Ring-LWE Cryptography for the Number Theorist."
  In: vol. 3. Springer Cham, Sept. 2016, pp. 271–290.
- C. W. Kok.
  "Fast algorithm for computing discrete cosine transform."
  In: *IEEE Transactions on Signal Processing* 45.3 (1997), pp. 757–760.
- Vadim Lyubashevsky, Chris Peikert, and Oded Regev, *On ideal lattices and learning with errors over rings*, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 1–23, 2010.
- V. Y. Pan, "New fast algorithms for polynomial interpolation and evaluation on the Chebyshev node set," *Computers & Mathematics with Applications*, vol. 35, no. 3, pp. 125–129, 1998.

References IV

Chris Peikert, Oded Regev, and Noah Stephens-Davidowitz, *Pseudorandomness of ring-LWE for any ring and modulus*, Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC), ACM, pp. 461–473, 2017.

M. Rosca, D. Stehlé, and A. Wallet.
“On the Ring-LWE and Polynomial-LWE Problems.”
In: *Advances in Cryptology – EUROCRYPT 2018*. Springer International Publishing, 2018, pp. 146–173.