Lattice-Based Foundations of Homomorphic Encryption

Efe İzbudak
ephemer4l@liberior.org

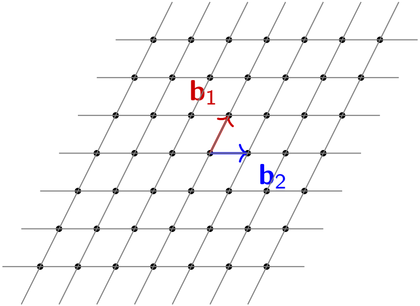
December 25, 2024

Integer Lattices

Definitions

Definition (Lattices)

Let $a_1, a_2, \ldots, a_\ell$ be linearly independent vectors in $\mathbb{R}^n$. Then the free $\mathbb{Z}-$module $\mathcal{L}$ generated by these vectors is called a **lattice** of rank ℓ. We say that $\mathcal{L}$ is a full-rank lattice if $\ell = n$



$\mathbf{b}_1 = (1/2, 1)$

$\mathbf{b}_2 = (1, 0)$

Integer Lattices

Definitions

Definition (Dual Lattice)

Let $\mathcal{L}$ be a lattice in $\mathbb{R}^n$. The **dual** of lattice $\mathcal{L}$ is given by

$$\mathcal{L}^* = \mathrm{Hom}_{\mathrm{Ab}}(\mathcal{L}, \mathbb{Z}) = \{w \in span(\mathcal{L}) \mid \langle w, \mathcal{L} \rangle \subset \mathbb{Z}\}$$

Example

(a) The dual of $\mathbb{Z}^n$ is $\mathbb{Z}^n$.

(b) The dual of $2\mathbb{Z} \oplus \mathbb{Z}$ is $\frac{1}{2}\mathbb{Z} \oplus \mathbb{Z}$.

(c) The dual of $\{x \in \mathbb{Z}^n \mid \sum_i x_i = 0 \mod 2\}$ is $\mathbb{Z}^n + \left(\frac{1}{2}, \frac{1}{2}, \ldots, \frac{1}{2}\right)$.

Integer Lattices

Hard problems [Pei15]

Definition (λ_i)

The value $\lambda_i(\mathcal{L}) \in \mathbb{R}$, called the **ith successive minimum**, gives the smallest $r \in \mathbb{R}$ such that $\mathcal{L}$ contains i linearly independent vectors of ℓ^2 norm not exceeding r.

Definition (SVP)

Given an arbitrary basis $\mathcal{B}$ of lattice $\mathcal{L}$, find a shortest nonzero lattice vector, i.e., $v \in \mathcal{L}$ such that $\lambda_1(\mathcal{L}) = \|v\|$.

Definition (Approx-SVP$_\gamma$)

Given a basis $\mathcal{B}$ of $n-$dimensional lattice $\mathcal{L}$, find a nonzero vector $v \in \mathcal{L}$ such that $\|v\| \leqslant \gamma(n) \cdot \lambda_1(\mathcal{L})$.

Integer lattices

Hard problems [Pei15]

Definition (GapSVP$_\gamma$)

Given basis $\mathcal{B}$ of lattice $\mathcal{L}$, where either $\lambda_1(\mathcal{L}) \leqslant 1$ or $\lambda_1(\mathcal{L}) > \gamma(n)$ determine which is the case.

Definition (SIVP$_\gamma$)

Given a basis $\mathcal{B}$ of a full-rank $n-$dimensional lattice $\mathcal{L}$ output a set $\{s_1, s_2, \ldots, s_n\} \subset \mathcal{L}$ of independent vectors such that $||s_i|| \leqslant \lambda_n(\mathcal{L})$ for $i \in [n]$.

Definition (BDD$_\gamma$)

Given basis $\mathcal{B}$ and target point $t \in \mathbb{R}^n$ with $||t - \mathcal{L}|| < d = \lambda_1(\mathcal{L})/2\gamma(n)$, find the unique lattice vector $v \in \mathcal{L}$ with $||t - v|| < d$.

Integer Lattices

Algorithms and complexity

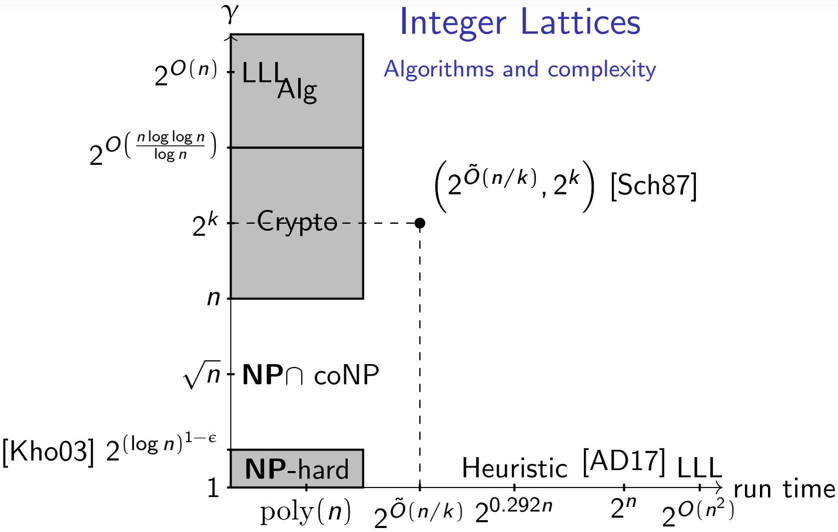


Figure: Complexity of SVP, inspired by [Vai24]

Integer Lattices

Algorithms and complexity

Definition (Sieving, informal, [Ste20])

1. Get a large list S of vectors. ($|S| >> 2^n$)

Integer Lattices

Algorithms and complexity

Definition (Sieving, informal, [Ste20])

1. Get a large list S of vectors. ($|S| >> 2^n$)
2. Find the differences of close vectors and add them to S (threshold depends on the algorithm)

Integer Lattices

Algorithms and complexity

Definition (Sieving, informal, [Ste20])

1. Get a large list S of vectors. ($|S| >> 2^n$)
2. Find the differences of close vectors and add them to S (threshold depends on the algorithm)
3. Update S and remove long vectors (above some threshold)

Integer Lattices

Algorithms and complexity

Definition (Sieving, informal, [Ste20])

1. Get a large list S of vectors. ($|S| >> 2^n$)
2. Find the differences of close vectors and add them to S (threshold depends on the algorithm)
3. Update S and remove long vectors (above some threshold)
4. Stop when a vector with norm close to $\sqrt{\frac{n}{2\pi e}}(\det(\mathcal{L}))^{\frac{1}{n}}$ is found.

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.
2. Modify the basis such that $||b_1|| \leqslant ||b_2||$, $||b_2|| \leqslant ||b_2 \pm b_1||$

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.
2. Modify the basis such that $||b_1|| \leqslant ||b_2||$, $||b_2|| \leqslant ||b_2 \pm b_1||$

$$\begin{bmatrix} 101 & 5 \\ 20 & 1 \end{bmatrix}$$

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.
2. Modify the basis such that $||b_1|| \leqslant ||b_2||$, $||b_2|| \leqslant ||b_2 \pm b_1||$

$$\begin{bmatrix} 101 & 5 \\ 20 & 1 \end{bmatrix} \xrightarrow{\text{swap}} \begin{bmatrix} 5 & 101 \\ 1 & 20 \end{bmatrix}$$

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.
2. Modify the basis such that $||b_1|| \leqslant ||b_2||$, $||b_2|| \leqslant ||b_2 \pm b_1||$

$$\begin{bmatrix} 101 & 5 \\ 20 & 1 \end{bmatrix} \xrightarrow{\text{swap}} \begin{bmatrix} 5 & 101 \\ 1 & 20 \end{bmatrix} \xrightarrow{\text{reduce}} \begin{bmatrix} 5 & 1 \\ 1 & 0 \end{bmatrix}$$

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.
2. Modify the basis such that $||b_1|| \leqslant ||b_2||$, $||b_2|| \leqslant ||b_2 \pm b_1||$

$$\begin{bmatrix} 101 & 5 \\ 20 & 1 \end{bmatrix} \xrightarrow{\text{swap}} \begin{bmatrix} 5 & 101 \\ 1 & 20 \end{bmatrix} \xrightarrow{\text{reduce}} \begin{bmatrix} 5 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{\text{swap}} \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix}$$

Integer Lattices

Algorithms and complexity

Example (Simplified LLL in $\mathbb{Z}^2$, [Ste20])

1. Consider a lattice $\mathcal{L}$ generated by $b_1 = (101, 20)$ and $b_2 = (5, 1)$.
2. Modify the basis such that $||b_1|| \leqslant ||b_2||$, $||b_2|| \leqslant ||b_2 \pm b_1||$

$$\begin{bmatrix} 101 & 5 \\ 20 & 1 \end{bmatrix} \xrightarrow{\text{swap}} \begin{bmatrix} 5 & 101 \\ 1 & 20 \end{bmatrix} \xrightarrow{\text{reduce}} \begin{bmatrix} 5 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{\text{swap}} \begin{bmatrix} 1 & 5 \\ 0 & 1 \end{bmatrix} \xrightarrow{\text{reduce}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

3. $(1, 0)$ is our solution to the SVP problem.

Integer Lattices

Algorithms and complexity

We instead consider the conditions

1. $||b_1||^2 \leqslant ||\tilde{b_2}||^2 + \mu^2 ||b_1||^2$
2. $|\mu| \leqslant 1/2$

where $\tilde{b_2}$ is the Gram-Schmidt vector attained from $b_2 = \mu \cdot b_1 + \tilde{b_2}$.

Integer Lattices

Algorithms and complexity

We instead consider the conditions

1. $||b_1||^2 \leqslant ||\tilde{b_2}||^2 + \mu^2||b_1||^2$
2. $|\mu| \leqslant 1/2$

where $\tilde{b_2}$ is the Gram-Schmidt vector attained from $b_2 = \mu \cdot b_1 + \tilde{b_2}$.

Note that

1. $\det(\mathcal{L}) = ||b_1|| \cdot ||\tilde{b_2}||$

Integer Lattices

Algorithms and complexity

We instead consider the conditions

1. $||b_1||^2 \leqslant ||\tilde{b_2}||^2 + \mu^2 ||b_1||^2$
2. $|\mu| \leqslant 1/2$

where $\tilde{b_2}$ is the Gram-Schmidt vector attained from $b_2 = \mu \cdot b_1 + \tilde{b_2}$.

Note that

1. $\det(\mathcal{L}) = ||b_1|| \cdot ||\tilde{b_2}||$
2. $\min\{||b_1||, ||\tilde{b_2}||\} \leqslant \lambda_1(\mathcal{L}) \leqslant ||b_1||$

Integer Lattices

Algorithms and complexity

We instead consider the conditions

1. $||b_1||^2 \leqslant ||\tilde{b_2}||^2 + \mu^2 ||b_1||^2$
2. $|\mu| \leqslant 1/2$

where $\tilde{b_2}$ is the Gram-Schmidt vector attained from $b_2 = \mu \cdot b_1 + \tilde{b_2}$.

Note that

1. $\det(\mathcal{L}) = ||b_1|| \cdot ||\tilde{b_2}||$
2. $\min\{||b_1||, ||\tilde{b_2}||\} \leqslant \lambda_1(\mathcal{L}) \leqslant ||b_1||$

$$\implies ||b_1|| \leqslant \sqrt{4/3} \cdot ||\tilde{b_2}||$$

Integer Lattices

Algorithms and complexity

We instead consider the conditions

1. $||b_1||^2 \leqslant ||\tilde{b_2}||^2 + \mu^2 ||b_1||^2$
2. $|\mu| \leqslant 1/2$

where $\tilde{b_2}$ is the Gram-Schmidt vector attained from $b_2 = \mu \cdot b_1 + \tilde{b_2}$.

Note that

1. $\det(\mathcal{L}) = ||b_1|| \cdot ||\tilde{b_2}||$
2. $\min\{||b_1||, ||\tilde{b_2}||\} \leqslant \lambda_1(\mathcal{L}) \leqslant ||b_1||$

$$\implies ||b_1|| \leqslant \sqrt{4/3} \cdot ||\tilde{b_2}||$$
$$\implies ||b_1|| \leqslant \sqrt{4/3} \cdot \lambda_1(\mathcal{L})$$

Integer Lattices

Algorithms and complexity

Definition (LLL Algorithm, [Ste20])

(i) $\delta \cdot ||\tilde{b}_i|| \leqslant ||\tilde{b_{i+1}}||^2 + \mu_{i,i+1}^2 \cdot ||\tilde{b}_i||^2$

(ii) $|\mu_{i,j}| \leqslant 1/2$

1. If (ii) is not satisfied, reduce.
2. If (i) is not satisfied, swap b_i and b_{i+1}
3. Repeat until both are satisfied.

Remark

This algorithm solves $\sqrt{(4/3)^n}$—SVP in polynomial time.

Integer Lattices

Discrete Gaussians

Definition (Elliptic Gaussian)

We say that a random variable X has the continuous **elliptic N-dimensional Guassian distribution** of mean zero and covariance matrix Σ if it has probability density function

$$\rho_{\mathbf{r}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^N \det(\Sigma)}} \exp\left(-\frac{1}{2}\mathbf{x}^{\mathrm{T}}\Sigma^{-1}\mathbf{x}\right)$$

Integer Lattices

Discrete Gaussians

Definition (Elliptic Gaussian)

We say that a random variable X has the continuous **elliptic N-dimensional Guassian distribution** of mean zero and covariance matrix Σ if it has probability density function

$$\rho_{\mathbf{r}}(\mathbf{x}) = \frac{1}{\sqrt{(2\pi)^N \det(\Sigma)}} \exp\left(-\frac{1}{2}\mathbf{x}^{\mathrm{T}}\Sigma^{-1}\mathbf{x}\right)$$

Definition (Discrete Gaussian)

Let $\mathcal{L}$ be a full-rank lattice in $\mathbb{R}^N$. We say that the discrete random variable X supported on $\mathcal{L}$ is a **discrete elliptic Gaussian random variable** if it has the probability distribution

$$\Pr[X = \mathbf{x}] = \frac{\rho_{\mathbf{r}}(\mathbf{x})}{\rho_{\mathbf{r}}(\mathcal{L})} \text{ for all } \mathbf{x} \in \mathcal{L}.$$

Learning with errors

Distribution and problems

Definition (LWE distribution)

For a vector $s \in \mathbb{Z}_q^n$, the LWE distribution $\mathcal{A}_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is induced by the process

$$a \leftarrow U(\mathbb{Z}_q^n), \quad e \leftarrow \chi, \quad b = \langle s, a \rangle + e, \quad \text{output } (a, b).$$

where $U(\mathbb{Z}_q^n)$ is the uniform distribution on $\mathbb{Z}_q^n$ and χ is the error distribution.

Definition (Search-LWE$_{n,q,\chi,m}$)

Given m linearly independent samples from $\mathcal{A}_{s,\chi}$, find s.

Definition (Decision-LWE$_{n,q,\chi,m}$)

Given m linearly independent vectors from $\mathbb{Z}_q^n \times \mathbb{Z}$, determine whether they are uniformly distributed or sampled from some $\mathcal{A}_{s,\chi}$ for uniformly random $s \in \mathbb{Z}_q^n$.

Learning with errors

Reformulation of GapSVP [Pei15]

Definition (GapSVP$_{\zeta,\gamma}$)

Given a basis $\mathcal{B}$ of lattice $\mathcal{L}$ and real number d with

(a) $\lambda_1(\mathcal{L}) \leqslant \zeta(n)$.

(b) $\min_i \|\tilde{b}_i\| \geqslant 1$ where $\tilde{b}_i$ is the Gram-Schmidt orthogonalized version of $b_i \in \mathcal{B}$

(c) $1 \geqslant d \geqslant \zeta(n)/\gamma(n)$

determine whether $\lambda_1(\mathcal{L}) \leqslant d$ or $\lambda_1(\mathcal{L}) > \gamma(n) \cdot d$.

Learning with errors

Reformulation of GapSVP

Remark

1. $\min_i \|\tilde{b}_i\| \geqslant 1$ *implies* $\lambda_1(\mathcal{L}) \geqslant 1$ *and this is without loss of generality by scaling* $\mathcal{B}$.
2. $1 \geqslant d \geqslant \zeta(n)/\gamma(n)$ *is without loss of generality because the instance is trivially solvable when* d *lies outside of the range.*
3. *For* $\zeta(n) \geqslant 2^{(n-1)/2}$ *the* $GapSVP_{\zeta,\gamma}$ *problem is equivalent to the* $GapSVP_{\gamma}$ *since we can use the LLL algorithm to find another basis with*

$$\lambda_1(\mathcal{L}) \leqslant \|b_1\| \leqslant 2^{(n-1)/2} \cdot \min_i \|\tilde{b}_i\|$$

Learning with errors

Hardness

Theorem ([Reg05])

For any $m = \mathrm{poly}(n)$, any modulus $q \leqslant 2^{\mathrm{poly}(n)}$ and any discretized Gaussian error distribution χ of parameter α where $\alpha q \geqslant 2\sqrt{n}$ and $0 < \alpha < 1$, solving the Decision-LWE$_{n,q,\chi,m}$ problem is at least as hard as quantumly solving GapSVP$_\gamma$ and SIVP$_\gamma$ on arbitrary $n-$dimensional lattices, for some $\gamma = \tilde{\mathcal{O}}(n/\alpha)$.

Learning with errors

Hardness

Theorem ([Reg05])

For any $m = \mathrm{poly}(n)$, *any modulus* $q \leqslant 2^{\mathrm{poly}(n)}$ *and any discretized Gaussian error distribution* χ *of parameter* α *where* $\alpha q \geqslant 2\sqrt{n}$ *and* $0 < \alpha < 1$, *solving the Decision-LWE*$_{n,q,\chi,m}$ *problem is at least as hard as quantumly solving GapSVP*$_\gamma$ *and SIVP*$_\gamma$ *on arbitrary* $n-$*dimensional lattices, for some* $\gamma = \tilde{\mathcal{O}}(n/\alpha)$.

Theorem ([Pei09])

Let $\alpha = \alpha(n) \in (0, 1)$ *and* $\gamma = \gamma(n) \geqslant n/(\alpha\sqrt{\log n})$. *Suppose* $\zeta = \zeta(n) \geqslant \gamma$ *and* $q = q(n) \geqslant (\zeta/\sqrt{n}) \cdot \omega(\sqrt{\log n})$. *Then there exists a (classic) probabilistic polynomial-time reduction from solving GapSVP*$_{\zeta,\gamma}$ *in the worst case (with overwhelming probability) to solving Search-LWE*$_{n,q,\chi_\alpha,m}$.

Learning with errors

Shortcomings

1. Large key sizes (public key size increases with $\mathcal{O}(n^2 \log q)$)
2. Slow multiplication (Lacking in FFT-like algorithms)

Interlude on ideal lattices

Definition (Ideal lattice)

An ideal lattice is in integer lattice $\mathcal{L}(\mathcal{B}) \subset \mathbb{Z}^n$ corresponding to some ideal of $\mathcal{R} = \mathbb{Z}[x]/(f)$ where f is irreducible, monic, and of degree n.

Example

Consider $\mathcal{R} = \mathbb{Z}[x]/(1+x^2)$ which can be embedded into $\mathbb{C}^2$ via the Minkowski canonical embedding.

$$\begin{aligned} \sigma\colon \mathcal{R} &\to \mathbb{C}^2 \\ 1 &\mapsto (1,1) \\ x &\mapsto (i,-i) \end{aligned}$$

Then the vectors $(1,0,1,0), (0,1,0,-1)$ generate an ideal lattice in $\mathbb{R}^4$.

Return of the Discrete Gaussian

Discrete Gaussians on Ideal Lattices

Remark

Note that if we embed $\mathcal{R}$ into $\mathbb{R}^N$ using the coefficient embedding σ_{coeff} then $\sigma_{coeff}(\mathcal{R})$ is an ideal lattice. Moreover, if X is a discrete Gaussian random variable with values in $\sigma_{coeff}(\mathcal{R})$ then we can define the random variable X_q of finite support consisting of the reductions of the values of X modulo q. More explicitly,

$$\Pr[X_q = \mathbf{x}] = \sum_{\substack{\mathbf{z} \in \sigma_{coeff}(\mathcal{R}) \\ \mathbf{z} \equiv \mathbf{x} \mod q}} \frac{\rho_{\mathbf{r}}(\mathbf{z})}{\rho_{\mathbf{r}}(\sigma_{\text{coeff}}(\mathcal{R}_q))} \text{ for all } \mathbf{x} \in \sigma_{coeff}(\mathcal{R}_q).$$

where $\rho_{\mathbf{r}}$ is the probability density function of the discrete Gaussian.

Ring Learning with Errors

Distribution and problems

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

$$a \leftarrow U(R_q), \quad e \leftarrow \chi, \quad b = as + e, \quad \text{output } (a, b).$$

That is, the joint probability distribution of random variables $\mathbf{a}$ and $\mathbf{b}$ 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 $\bar{\chi}(e') = \sum_{\substack{e \in R \\ e \mod q = e'}} \chi(e)$

Ring Learning with Errors

Distribution and problems [RSW18]

Definition (Decision RLWE)

Given m independent samples $(a_i, b_i) \in R_q \times R_q$, $i \in \{1, \ldots, m\}$ 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 $(a_i, b_i) \in \mathcal{D}_{s,\chi}$, $i \in \{1, \ldots, m\}$, 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 in R 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*

$\uparrow$

(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

$$a \leftarrow U(R_q), \quad e \leftarrow \chi, \quad b = a \cdot s + e, \quad \text{return } (a, b)$$

PLWE Problems

Definition (Decision PLWE)

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

Some attacks on PLWE

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.

Some attacks on PLWE

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

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

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.

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.

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1+X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathrm{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathrm{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)

Security: (c_1, c_0) is an RLWE sample (essentially).

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathrm{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)
  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathrm{Dec}_s(c(S))$: get short $d \in R$ such that $d = c(s) \mod q$. Output $d \mod 2$.

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathrm{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)
  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathrm{Dec}_s(c(S))$: get short $d \in R$ such that $d = c(s) \mod q$. Output $d \mod 2$.
- $\mathrm{EvalAdd}(c, c') = (c + c')(S)$, $\quad \mathrm{EvalMul}(c, c') = (c \cdot c')(S)$.
  Decryption works if $e + e'$, $e \cdot e'$ are "short enough".

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1+X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathrm{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)
  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathrm{Dec}_s(c(S))$: get short $d \in R$ such that $d = c(s) \mod q$. Output $d \mod 2$.
- $\mathrm{EvalAdd}(c, c') = (c + c')(S)$, $\quad \mathrm{EvalMul}(c, c') = (c \cdot c')(S)$.
  Decryption works if $e + e'$, $e \cdot e'$ are "short enough".
- Many mults $\implies$ large power of expansion factor

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathsf{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

  $$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)
  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathsf{Dec}_s(c(S))$: get short $d \in R$ such that $d = c(s) \mod q$. Output $d \mod 2$.
- $\mathrm{EvalAdd}(c, c') = (c + c')(S)$, $\quad \mathrm{EvalMul}(c, c') = (c \cdot c')(S)$.
  Decryption works if $e + e'$, $e \cdot e'$ are "short enough".
- Many mults $\implies$ large power of expansion factor $\implies$ tiny error rate

Example Application: Homomorphic Encryption [BV11a]

- $R = \mathbb{Z}[X]/(1 + X^{2^k})$, $\quad R_q = R/qR$. Symmetric key $s \leftarrow R_q$.
- $\mathrm{Enc}_s(m \in R_2)$: choose a "short" $e \in R$ such that $e = m \mod 2$. Let

$$c_1 \leftarrow R_q \quad \text{and} \quad c_0 = -c_1 \cdot s + e \in R_q$$

  and output $c(S) = c_0 + c_1 S \in R_q[S]$. (Notice: $c(s) = e \mod q$.)
  Security: (c_1, c_0) is an RLWE sample (essentially).
- $\mathrm{Dec}_s(c(S))$: get short $d \in R$ such that $d = c(s) \mod q$. Output $d \mod 2$.
- $\mathrm{EvalAdd}(c, c') = (c + c')(S)$, $\quad \mathrm{EvalMul}(c, c') = (c \cdot c')(S)$.
  Decryption works if $e + e'$, $e \cdot e'$ are "short enough".
- Many mults $\implies$ large power of expansion factor $\implies$ tiny error rate α $\implies$ big parameters!

References I

D. Aggarwal and N. Stephens-Davidowitz,
"Just Take the Average! An Embarrassingly Simple 2^n-Time Algorithm for SVP (and CVP),"
In: *arXiv preprint arXiv:1709.01535*, 2017. [Online]. Available: https://arxiv.org/abs/1709.01535.

I. Blanco-Chacón, R. Durán-Díaz, and R. M. Sanchéz-Ledesma.
"A Generalized Approach to Root-based Attacks towards PLWE."
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.

References II

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

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).

Z. Brakerski and V. Vaikuntanathan,
"Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages,"
In: *Advances in Cryptology - CRYPTO 2011*, vol. 6841 of *Lecture Notes in Computer Science*, P. Rogaway, Ed. Springer, 2011, pp. 505–524. DOI: https://doi.org/10.1007/978-3-642-22792-9_29.

References III

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.

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.

S. Khot.
Hardness of approximating the shortest vector problem in lattices.
In: J. ACM, 52(5):789– 808, 2005. Preliminary version in FOCS 2003.

References IV

V. Lyubashevsky, C. Peikert, and O. Regev,
On ideal lattices and learning with errors over rings,
In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 1–23, 2010.

O. Regev,
On Lattices, Learning with Errors, Random Linear Codes, and Cryptography,
In: arXiv:2401.03703, 2024. Available at:
https://arxiv.org/abs/2401.03703.

C. Peikert, O. Regev, and N. Stephens-Davidowitz,
Pseudorandomness of ring-LWE for any ring and modulus,
In: Proceedings of the 49th Annual ACM SIGACT Symposium on Theory of Computing (STOC), ACM, pp. 461–473, 2017.

References V

C. Peikert.
Public-key cryptosystems from the worst-case shortest vector problem.
In *Proceedings of the 41st Annual ACM Symposium on Theory of Computing (STOC)*, pages 333–342, Bethesda, MD, 2009. ACM.

C. Peikert,
A Decade of Lattice Cryptography,
In: IACR Cryptology ePrint Archive, Report 2015/939, 2015, pp. 22–27. Available at `https://eprint.iacr.org/2015/939`.

N. Stephens-Davidowitz,
Algorithms for lattice problems.
January 2020
At: Simons Institute Lattices: Geometry, Algorithms, and Hardness,

References VI

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.

C. P. Schnorr.
A hierarchy of polynomial time lattice basis reduction algorithms.
In: Theor. Comput. Sci., 53:201–224, 1987.

V. Vaikuntanathan,
Lecture notes,
Fall 2024
Advanced Topics in Cryptography: From Lattices to Program Obfuscation