Introduction to Cryptography

Today's homework should be ready soon!
(just got sent to printing)

PCMI 2022 - Undergraduate Summer School

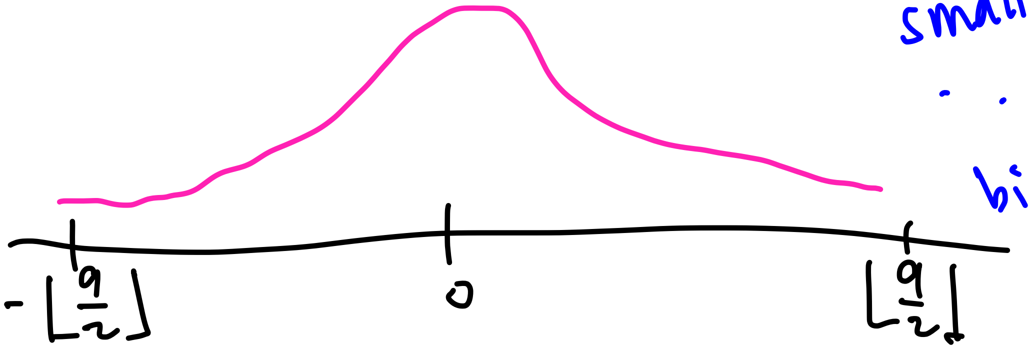
Recall an LWE pair looks like

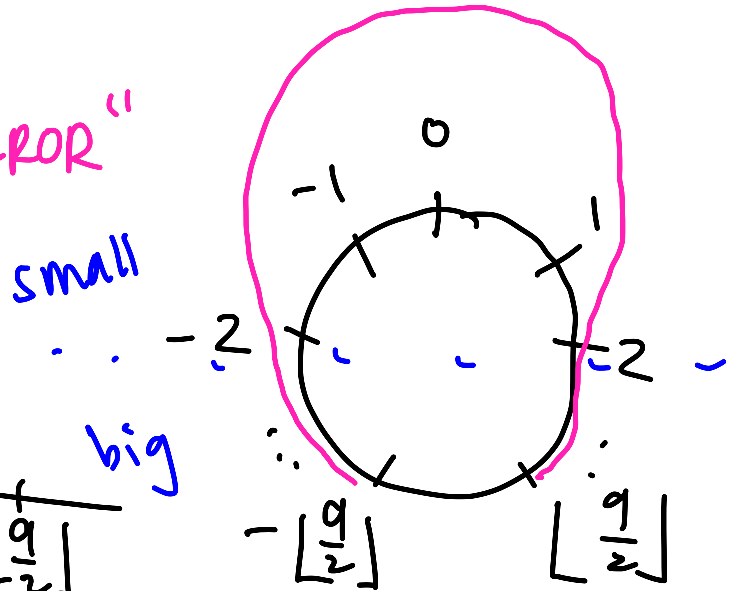
$(\vec{a}_i, b_i)$

- $\vec{a}_i \in \mathbb{F}_q^n$ q prime integer, odd

- $b_i = \vec{a}_i \cdot \vec{s} + e_i \quad \in \mathbb{F}_q$

$\leftarrow$ "small error"





Regev's LWE cipher, fix n, prime q, σ^2 variance

Key generation

- choose random $\vec{s} \in \mathbb{F}_q^n$, this is the private key
- choose random $\vec{a}_i \in \mathbb{F}_q^n$, errors $e_i \in \mathbb{F}_q$

  uniformly ... chosen from a Gaussian with variance σ^2

- public key are the LWE pairs

$$(\vec{a}_i,\ b_i = \vec{a}_i \cdot \vec{s} + e_i) \qquad i = 1, \ldots, m$$

Regev in 2005 suggested for fixed n

- $n^2 \le q \le 2n^2$
- $m = (1+\varepsilon)(n+1)\log q$ for any $\varepsilon > 0$
- $\sigma = \dfrac{q}{\sqrt{2\pi n}\,(\log n)^2}$

Regev LWE encryption

- Choose a random subset $T \subseteq \{1, \ldots, m\}$
- Compute $\vec{a} = \sum_{i \in T} \vec{a}_i$
- To send $x=0$, $b = \sum_{i \in T} b_i$

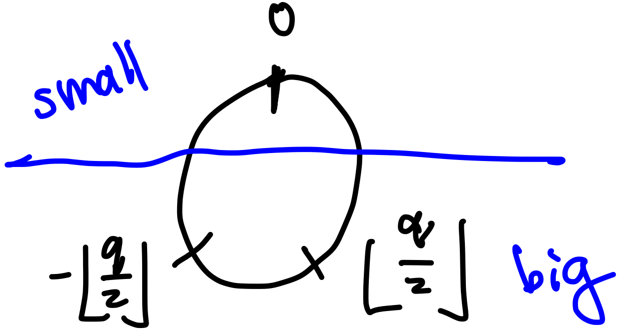
  To send $x=1$, $b = \sum_{i \in T} b_i + \left\lfloor \frac{q}{2} \right\rfloor$ ← biggest number
- Send $(\vec{a}, b)$

Regev LWE decryption

Compute $\vec{a} \cdot \vec{s} - b = \begin{cases} \sum_{i \in T} e_i & \text{if } x=0 \\ \sum_{i \in T} e_i + \lfloor \frac{q}{2} \rfloor & \text{if } x=1 \end{cases}$

With high probability, $x=0$ if $\vec{a} \cdot \vec{s} - b$ is "small"

$x=1$ if $\vec{a} \cdot \vec{s} - b$ is "big"



Next week

- Monday: Fully homomorphic encryption (FHE)
- Tuesday | Thursday: Ring LWE
- Friday: Cryptography in the real world

Algebraic number theory background for RLWE

- A <u>number field</u> K is a field containing $\mathbb{Q}$ and such that $\underbrace{\dim_{\mathbb{Q}} K = n}$ $< \infty$

  K satisfies properties of a vector space / $\mathbb{Q}$

- The number n is called the <u>degree</u> of K

- $\alpha \in K$

degree of K over $\mathbb{Q}$

consider $\{1, \alpha, \alpha^2, \alpha^3, \dots, \alpha^n\}$

This is n+1 elements in a vector space of dim n, so there must be a relation

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \dots + a_1 \alpha + a_0 = 0$$

for $a_i \in \mathbb{Q}$

$f(x) = a_n x^n + \dots + a_0$ then $f(\alpha) = 0$

- From the fact that α satisfies a polynomial of degree $\leq n$ with coeffs in $\mathbb{Q}$, we can get that there is a unique monic irreducible polynomial $p \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$.

only trivial factorization over $\mathbb{Q}$

$a_n = 1$, leading coefficient

This unique poly is the minimal polynomial of α.

- Inside of K, take the set of elements α such that the minimal polynomial of α has coefficients in $\mathbb{Z}$. This set is a ring, we call it the <u>ring of integers</u> of K

Ex: $\frac{1+\sqrt{-5}}{2}$ is an "integer"

$\frac{1}{2} \in K$ root of $2x-1$ or $x-\frac{1}{2}$

So $\mathbb{Z} \subseteq \mathcal{O}_K$

← ring of integers
"mathcal O sub K"

Example: $K = \mathbb{Q}(i) = \{a+bi, \ a,b \in \mathbb{Q}, \ i^2=-1\}$

$\mathcal{O}_K = \mathbb{Z}[i] = \{a+bi, \ a,b \in \mathbb{Z}, \ i^2=-1\}$

Primitive element theorem (adapted)

If K is a number field of degree n, then there is $\gamma \in K$ such that

$$K = \mathbb{Q}(\gamma) = \{ a_0 + a_1\gamma + a_2\gamma^2 + \ldots + a_{n-1}\gamma^{n-1} : a_i \in \mathbb{Q} \}$$

We call γ a primitive element, and the minimal polynomial of γ has degree n in this case.

Suppose that $K = \mathbb{Q}(\gamma)$ is a number field of degree n, then there are n injective ring homomorphisms

$$K \hookrightarrow \mathbb{C} \quad \leftarrow \text{complex numbers}$$

$$\begin{aligned}
\gamma &\longmapsto \gamma_1 \\
\gamma &\longmapsto \gamma_2 \\
&\vdots \\
\gamma &\longmapsto \gamma_n
\end{aligned}
\Bigg\} \quad \gamma_1, \ldots, \gamma_n \text{ are the } n \text{ roots of the minimal polynomial of } \gamma$$

Example $K = \mathbb{Q}(\alpha)$ with $\alpha^2 - 2 = 0$

$$\begin{aligned} K &\hookrightarrow \mathbb{R} \subseteq \mathbb{C} \\ \alpha &\longmapsto \sqrt{2} \end{aligned}$$

$$\alpha \longmapsto -\sqrt{2}$$

That’s all for now!