Introduction to Cryptography

PCMI 2022 - Undergraduate Summer School

Yesterday: talked about ideas behind FHE

Homework today: "simple cipher" from last week

secret key: p

public key: $x_i = q_i p + r_i$

encr : $c = r_{x_0}(m + \sum x_i + 2r)$

dec : $m \equiv r_p(c) \mod 2$

PLWE: polynomial learning with errors
(variant of RLWE)

K a number field $\qquad \underbrace{[K:\mathbb{Q}]}_{\dim_{\mathbb{Q}} K}=n$

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

We can actually choose $\gamma\in\mathcal{O}_K$ elements with min poly $\in\mathbb{Z}[x]$

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

$\gamma \in K$

We can actually choose $\gamma \in \mathcal{O}_K$

elements with min poly $\in \mathbb{Z}[x]$

If min poly of γ has degree n

$$\gamma^n + b_{n-1}\gamma^{n-1} + \ldots + b_0 = 0$$

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

Example: $K = \mathbb{Q}\left(\frac{\sqrt{2}}{2}\right) = \left\{ a_0 + a_1 \frac{\sqrt{2}}{2} : a_0, a_1 \in \mathbb{Q} \right\}$

$x = \frac{\sqrt{2}}{2} \qquad x^2 = \frac{1}{2} \qquad x^2 - \frac{1}{2} = 0 \qquad 2x^2 - 1 = 0$

So $\frac{\sqrt{2}}{2} \notin \mathcal{O}_K$ but $K = \mathbb{Q}(\sqrt{2})$

and $\sqrt{2} \in \mathcal{O}_K$

Sometimes when we are lucky:

$$\mathcal{O}_K = \mathbb{Z}[\gamma] = \{ a_0 + a_1\gamma + a_2\gamma^2 + \dots + a_{n-1}\gamma^{n-1} : a_i \in \mathbb{Z} \}$$

This is rare, and when it is so, we say that

$\mathcal{O}_K$ is <u>monogenic</u>

For now assume $\mathcal{O}_K$ is monogenic.

LWE pairs $(\vec{a}_i, b_i = \vec{a}_i \cdot \vec{s} + e_i)$

Drawing from the PLWE error distribution:

Fix $\sigma > 0$

e_j

- draw n integers independently at random from a discrete Gaussian with variance σ^2

- Form the "small" element

$$e = e_0 + e_1 \gamma + \ldots + e_{n-1} \gamma^{n-1} \in \mathcal{O}_K$$

Fix a prime $q \in \mathbb{Z}$, consider the quotient ring

$$\mathcal{O}_K / q\mathcal{O}_K =: R_q$$

we know that

$$\mathcal{O}_K / q\mathcal{O}_K = \{ a_0 + a_1 \bar{\gamma} + a_2 \bar{\gamma}^2 + \ldots + a_{n-1} \bar{\gamma}^{n-1} : a_i \in \mathbb{Z}/q\mathbb{Z} \}$$

where $\bar{\gamma}$ is a representative of $\gamma + q\mathcal{O}_K$

To get a small element of R_q

- draw a small $e \in \mathcal{O}_K$
- reduce the coefficients in the polynomial modulo q

A PLWE cipher : K, q, σ all public

$K = \mathbb{Q}(\gamma)$

- key generation:
  - secret key is a random $\boxed{\text{small}}$ $s \in R_q$
  - public key: choose $a \in R_q$ uniformly at random

    $\boxed{\text{small}}$ $e \in R_q$

    publish (a, b) $\quad b = as + e$

- encryption:
  - draw 3 small random elements of R_q, name them r_1, e_1, e_2
  - to send the n bits $m_0, m_1, \ldots, m_{n-1}$ $(m_i \in \{0,1\})$ form

$$m = m_0 + m_1 \bar{\gamma} + \ldots + m_{n-1} \bar{\gamma}^{n-1} \in R_q$$

- send the pair (u, v) where

$u = ar + e_1$

$v = br + e_2 + \left\lfloor \frac{q}{2} \right\rfloor m$

- decryption: compute $v - us = z_0 + z_1 \gamma + \ldots + z_{n-1} \gamma^{n-1}$

Round the coefficients of the polynomial to 0 or $\left\lfloor \frac{q}{2} \right\rfloor$

The security is based on the hardness of the decision RLWE problem

tell apart pairs (a, b) with $b = as + e$

from random pairs (a, b)

Note that here the secret is small not uniformly distributed. Turns out that it doesn't matter.

This relies on search reducing to decision

That’s all for now!