Introduction to Cryptography

PCMI 2022 - Undergraduate Summer School

K a number field, deg n $/\mathbb{Q}$

Then there are n different maps $K \hookrightarrow \mathbb{C}$

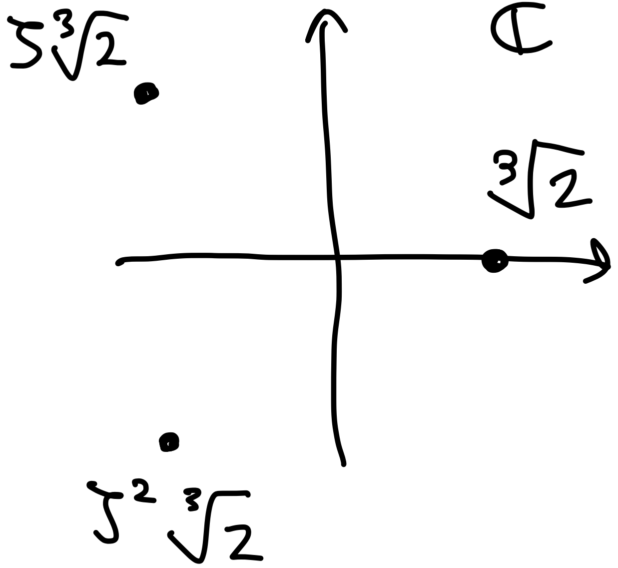
that respect $+, \times$

If $K = \mathbb{Q}(\gamma)$ min poly of γ is $f(x) \in \mathbb{Q}[x]$

then the n embeddings are

$$\left.\begin{aligned} \gamma &\longmapsto \alpha_1 \\ &\longmapsto \alpha_2 \\ &\longmapsto \vdots \\ &\longmapsto \alpha_n \end{aligned}\right\} \text{ the } n \text{ distinct roots of } f$$

Ex: $K = \mathbb{Q}(\gamma)$ $\quad \gamma^3 = 2$



3 embeddings into $\mathbb{C}$:

$$\sigma_1 : \gamma \longmapsto \sqrt[3]{2}$$

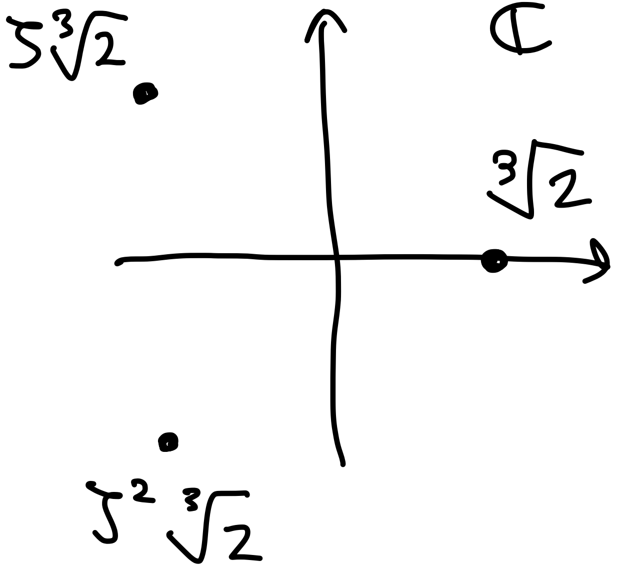
ζ is a primitive third root of unity

Since $\sigma_1(1) = 1$, it implies that $\sigma_1(a) = a \quad \forall a \in \mathbb{Q}$

If $\alpha \in K$, $\alpha = a_0 + a_1\gamma + a_2\gamma^2$,

then $\sigma_1(\alpha) = a_0 + a_1\sigma_1(\gamma) + a_2\sigma_1(\gamma)^2$

Ex: $K = \mathbb{Q}(\gamma)$ $\quad \gamma^3 = 2$



3 embeddings into $\mathbb{C}$:

"real" embedding

$\sigma_1 : \gamma \longmapsto \sqrt[3]{2}$

Since $\sigma_1(\gamma) \in \mathbb{R}$ then $\sigma_1(K) \subseteq \mathbb{R}$

$\tau_1 : \gamma \longmapsto \zeta\sqrt[3]{2}$

$\tau_2 : \gamma \longmapsto \zeta^2\sqrt[3]{2}$

complex embeddings

$\tau_2 = \overline{\tau_1}$ complex conjugate of τ_1

In general if deg of K is n

K will have s_1 real embeddings

s_2 pairs of complex embeddings

then $n = s_1 + 2s_2$

From now on, fix the embeddings $K \hookrightarrow \mathbb{C}$

$$\underbrace{\sigma_1, \sigma_2 \dots, \sigma_{s_1}}_{\text{real embeddings}},\ \underbrace{\tau_1, \tau_2 \dots, \tau_{s_2}}_{\text{a rep from each cx conj pair}},\ \overline{\tau}_1, \overline{\tau}_2, \dots \overline{\tau}_{s_2}$$

The <u>canonical embedding</u> of $\sigma : K \hookrightarrow \mathbb{R}^n$ is given by

$$\begin{array}{l} K \\ \ni \\ \alpha \longmapsto \big(\sigma_1(\alpha), \sigma_2(\alpha), \dots, \sigma_{s_1}(\alpha), \sqrt{2}\,\mathrm{Re}(\tau_1(\alpha)), \sqrt{2}\,\mathrm{Im}(\tau_1(\alpha)), \\ \qquad \dots, \sqrt{2}\,\mathrm{Re}(\tau_{s_2}(\alpha)), \sqrt{2}\,\mathrm{Im}(\tau_{s_2}(\alpha))\big) \end{array}$$

$$\mathbb{R}^{s_1} \times \mathbb{C}^{s_2}$$

Super fun: If R is the ring of integers of K

$(R = \mathcal{O}_K)$

then $\sigma(R) \subseteq \mathbb{R}^n$ is a lattice

$R = \mathbb{Z} + \alpha_1 \mathbb{Z} + \dots + \alpha_{n-1} \mathbb{Z}$

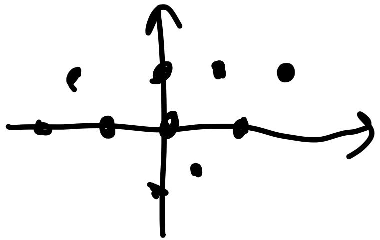
Difference between PLWE and RLWE is how the errors are drawn

In PLWE $\alpha \in R$, $\alpha = \boxed{a_0} + \boxed{a_1}\gamma + \dots + \boxed{a_{n-1}}\gamma^{n-1}$

$a_i \in \mathbb{Z}$

draw the coefficient a_i at random

In RLWE, we use a Gaussian on the lattice



ERROR distributions

Def: A continuous Gaussian on $\mathbb{R}^n$ is a random variable with probability distribution function $\qquad \|\vec{x}\| = \sqrt{x_1^2 + \ldots + x_n^2}$

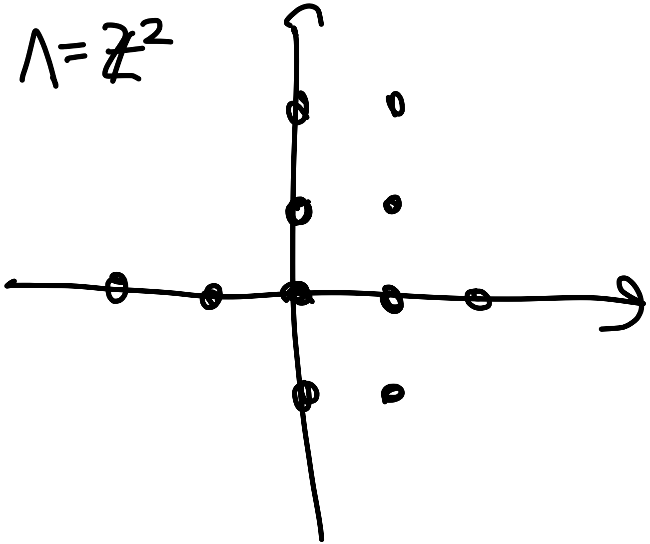
$$D_\sigma(\vec{x}) = \frac{1}{(2\pi\sigma^2)^{n/2}} \exp\left(\frac{-\|\vec{x}\|}{2\sigma^2} \right)$$

Def: A discretization of a Gaussian to a lattice coset $\vec{v} + \Lambda$ for $\vec{v} \in \mathbb{R}^n$, $\Lambda \subseteq \mathbb{R}^n$ is drawn in the following way,

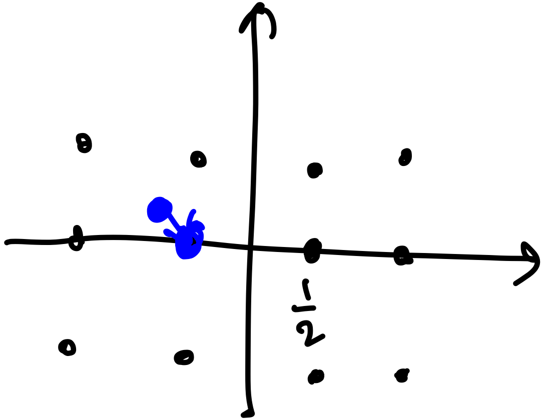
1- first draw $\vec{x}$ from a cts Gaussian

2- "round" to an element of $\vec{v} + \Lambda$ that is "not too far"

$\Lambda = \mathbb{Z}^2$



$(\frac{1}{2}, 0) + \Lambda$



Key generation

$\vec{a}\cdot\vec{x} = x_0$

Public: $K, R, n, p \in \mathbb{Z}$ prime, $l \geq 2$, $r > 0$, $\sigma > 0$

$q \in \mathbb{Z}$ another prime

- $(a_0 = -1, a_1, \ldots, a_{l-1})$ $\quad a_i \in R/qR$ uniformly at random
- $(x_0, x_1, \ldots, x_{l-1}, x_l = 1)$ $\quad x_i$ "small" integer (Gaussian with s.d. r)
- $a_l = -\sum_{i=0}^{l-1} x_i a_i$

secret key $\vec{x} = (x_1, \ldots, x_l), x_0$

public key $\vec{a} = (a_1, \ldots, a_l)$

Encryption: plaintext $\mu \in R/pR$

- Draw errors $e_0, e_1, \ldots, e_{\ell-1}$ from a Gaussian discretized to pR

- Draw e_ℓ from a Gaussian discretized to $\mu + pR$

Ciphertext: $\vec{c} = e_0 \vec{a} + \vec{e}$ mod qR $\quad \vec{e} = (e_1, \ldots, e_\ell)$

Decryption:

First compute $\bar{d} = \vec{c} \cdot \vec{x} \in R/qR$

Take a "good" basis (almost orthonormal) $\{b_i\}$ of R

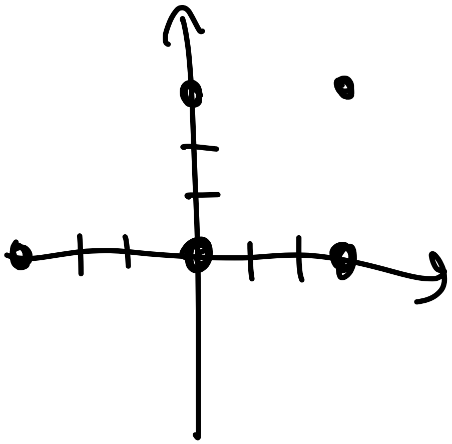
Then $\bar{d} = \sum \bar{d}_i \bar{b}_i$ $\quad$ $\bar{b}_i \equiv b_i \bmod qR$

$\bar{d}_i \in \mathbb{Z}/q\mathbb{Z}$

Lift $\bar{d}_i$ to an integer $-\frac{q}{2} \leq d_i < \frac{q}{2}$

Then $d = \sum d_i b_i \in R$ and $d \equiv \mu \bmod pR$ with high prob.

$3\mathbb{Z}^2$



That’s all for now!