Linear Algebra

n equations in m unknowns

- $n < m$ underdetermined — likely many solutions (space of dim $m-n$ of sol^{n}s)
- $n = m$ critical — likely one solution
- $n > m$ overdetermined — likely no solutions

To solve: Gaussian elimination. $O(n^3)$ field operations $A\vec{x} = b$

$n \times n$ n = dimension

Not: error tolerant

change input slightly ⟶ totally different final output.

Big Picture Idea: "Learning with Errors"

	public key	private key	Hard Problem
$(\mathbb{Z}/p\mathbb{Z})^*$ g primitive root	g^s	s	Given g^s, find s.
E ell. curve $P \in E(\mathbb{F}_p)$	sP	s	Given sP, find s.
Learning with Errors (LWE)	one or several $(\vec{a}, b = \langle \vec{a}, \vec{s} \rangle + e)$ "samples" in $\mathbb{F}_p^n \times \mathbb{F}_p$ ($\langle \cdot, \cdot \rangle$: dot product)	$\vec{s}$	Given (a, b), find $\vec{s}$.

Details: n = dimension, p = prime

$\vec{a}$ = random n-dim^l vector in $\mathbb{F}_p^n$

$\vec{s}$ = short secret vector in $\mathbb{F}_p^n$

e = small "error"

Def^n An $e \in \mathbb{F}_p$ is called "small" if it is in $[-R, R] \subseteq \mathbb{F}_p$

A vector $\vec{s} \in \mathbb{F}_p^n$ is short if its coefficients are small.

Idea: $(\vec{a},\ b = \langle \vec{a}, \vec{s} \rangle)$ is a linear eqⁿ for s, i.e. $\langle \vec{a}, \vec{s} \rangle = b$ (secret)

($\vec{a}$ given, b given)

$$a_1 s_1 + \cdots + a_n s_n = b$$

— Linear eqⁿ's easy to solve:

Given several samples, use Gauss. elimination to find $\vec{s}$.

To make this hard, use $(\vec{a},\ b = \langle \vec{a}, \vec{s} \rangle + e)$ like an approximate linear eqn.

$$a_1 s_1 + \cdots + a_n s_n \approx b.$$

$\Rightarrow$ This is actually $2R+1$ possible linear eqns. (one for each possible e)

Gauss elim. not possible:

If we take n samples $(A\vec{s} = \vec{b})$

then the errors mean Gauss elim. fails.

(Another perspective: there are $(2R+1)^n$ possible systems)

Search LWE Problem.

Given polynomially many samples $(a, b = \langle a, s \rangle + e)$, determine s.

Decision LWE Problem.

Given " " " " or uniformly random samples (a, b)

determine which is the case.

Note: With just one sample, $\exists$ many valid s.

With more, eventually only 1.

(With many random samples, no s.)

Attacks on LWE:

Naive: ① Exhaustively search $s \in \mathbb{F}_p^n$. (Exponential time in n.)

② Exhaustively solve all $(2R+1)^n$ linear systems. (Exponential)
(possibilities for e's in n samples)

Lattice Reduction:

n samples gives a linear system $(A, \vec{b} = A\vec{s} + \vec{e})$.

Define $\Lambda = \{\vec{y} \in \mathbb{Z}^n : \vec{y}^T A \equiv \vec{0} \pmod p\}$.

Find <u>short</u> $\vec{y} \in \Lambda$.

Then $\langle \vec{y}, \vec{b} \rangle = \langle \vec{y}, A\vec{s} + \vec{e} \rangle = \langle \vec{y}, A\vec{s} \rangle + \langle \vec{y}, \vec{e} \rangle$

$= \langle \vec{y}A, \vec{s} \rangle + \langle \vec{y}, \vec{e} \rangle$

$\equiv 0 + \underbrace{\langle \vec{y}, \vec{e} \rangle}_{\text{small}} \pmod p$

If small, then report that samples are well formed.
If not, then report that samples are random.

] Decision LWE

Ring Learning with Errors

p = prime ($p \sim 12289$)

n = dimension = power of 2 ($n \sim 1024$)

"size" of problem: $|\mathbb{F}_p^n| = p^n$. ← vector space of dim n over $\mathbb{F}_p$

$$R_p = \frac{\mathbb{F}_p[X]}{(X^n+1)}$$ ← not irred.

} not a field, but a ring.

Also, as a vector space $R_p \cong \mathbb{F}_p^n$

$a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \to \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$

Private / Public Key pair:

Private: $s \in R_p$ secret

Public: $(a, \; b = as + e) \in R_p \times R_p$

- a: random
- as: mult. as poly's.
- e: small (as a vec.)

This is an instance of LWE:

$$\begin{pmatrix} b_0 \\ \vdots \\ b_{n-1} \end{pmatrix} = \left(A\right) \begin{pmatrix} s_0 \\ \vdots \\ s_{n-1} \end{pmatrix} + \begin{pmatrix} e_0 \\ \vdots \\ e_{n-1} \end{pmatrix}$$ ← 1st sample, ← 2^w samples

multiplication-by-a is a linear transformation

1 RLWE sample = n LWE samples