Introduction to Cryptography

99 problems and LWE is one

PCMI 2022 - Undergraduate Summer School

We say that Problem A <u>reduces</u> to Problem B if, given a solution to Problem B, we can solve Problem A.

Search LWE (Learning With Errors) Problem

Given a prime q and a positive

---

hold on

Definition: LWE pairs

Given a prime q and a positive integer n

form pairs $(\vec{a}_i, b_i)$ with $\vec{a}_i \in \mathbb{F}_q^n$, $b_i \in \mathbb{F}_q$

in the following way

- the vector $\vec{a}_i$ is chosen uniformly at random from $\mathbb{F}_q^n$

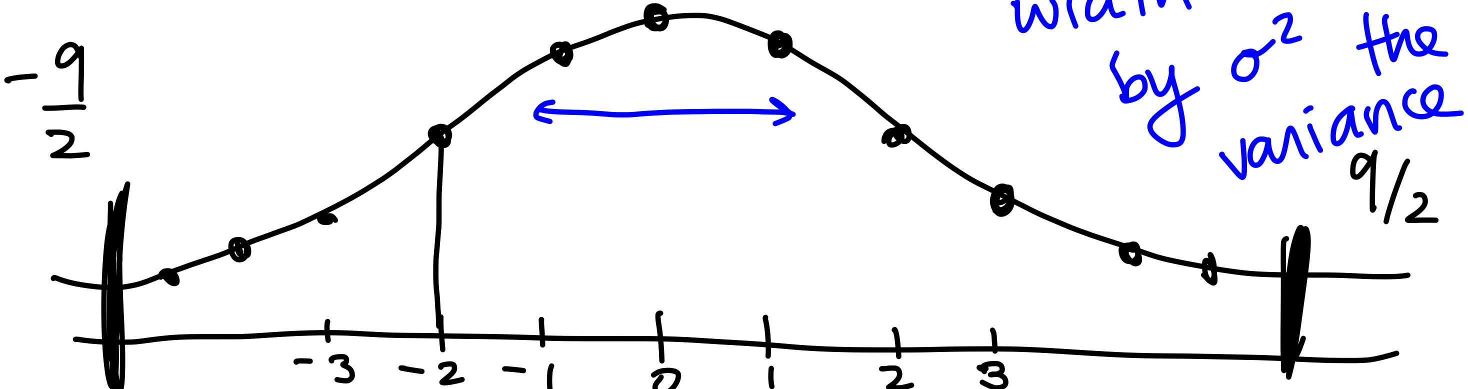
- $b_i = \vec{a}_i \cdot \vec{s} + e_i$ for $\vec{s}$ a fixed element of $\mathbb{F}_q^n$ and e_i a "small" random element of $\mathbb{F}_q$.

χ is the distribution of the e_i's

Pairs like this ⤴ are $LWE_{q,\vec{s},\chi}$ pairs

What is χ, or what is "small":

We usually use χ which is a discrete Gaussian / normal distribution constrained by $-\frac{q}{2} < x < \frac{q}{2}$



width is controlled by σ^2 the variance

LWE pairs: secret $\vec{s}$

Random + small

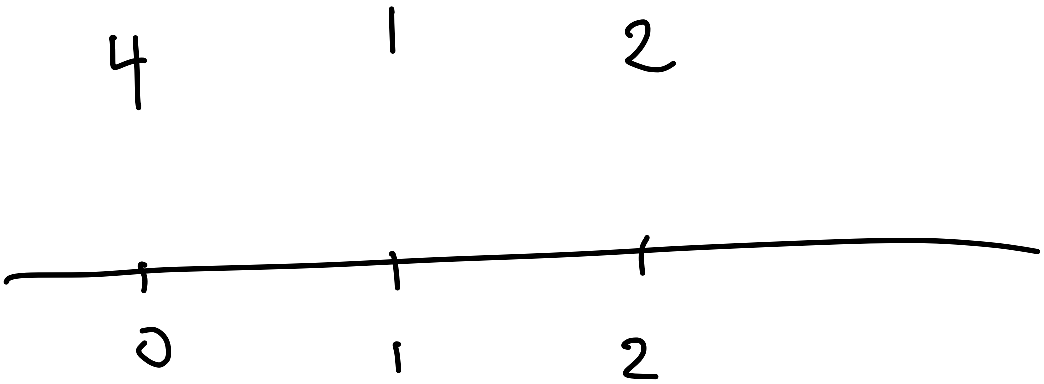
$$(\vec{a}_i, \ b_i = \vec{a}_i \cdot \vec{s} + e_i)$$

Search LWE Problem

Given a certain number of LWE pairs $(\vec{a}_i, b_i)$, find $\vec{s}$.

Decision LWE problem

Given some number of pairs $(\vec{a}_i, b_i)$ determine if they are LWE or if the b_is were chosen at random (separately from the $\vec{a}_i$s)



$$Pr(X=0) = \frac{4}{7}$$

$$Pr(X=1) = \frac{1}{7}$$

$$Pr(X=2) = \frac{2}{7}$$

Theorem:

1. The decision LWE problem reduces (in polynomial time) to the search LWE problem.

2. If q is polynomial in n, the search LWE problem reduces to the decision LWE problem.

1. Given pairs $(\vec{a}_i, b_i)$

put them in the search LWE solver to get $\vec{s}$

Then check if $\vec{a}_i \cdot \vec{s} - b_i$ is distributed like a Gaussian

② Given LWE pairs $(\vec{a}_i, b_i)$

We can check a guess for the first coordinate of $\vec{s}$ in the following way:

Suppose we guess it's $g \in \mathbb{F}_q$

For each i, choose $r_i \in \mathbb{F}_q$ at random and form the pair

$$\Big(\underbrace{\vec{a}_i + (r_i, 0, 0 \ldots 0)}_{\text{new } \vec{a}_i'} \,,\ \underbrace{b_i + g r_i}_{b_i'} \Big)$$

Feed the new pairs in the decision LWE solver

If the pairs are LWE then the guess is correct.

If they are not, guess again.

@home, check why.

$\square$

In 2005, Regev gave a quantum reduction of the "GapSVP" to the search LWE problem.

Later on, Peikert gave a classical reduction of the GapSVP problem for large q ($q \geq 2^{n/2}$) to the search LWE problem.

In 2008, Regev showed that if q is a product of small primes + error is Gaussian, then GapSVP reduces to search LWE.

Definition Short integer solution SIS_β

Fix $\beta > 0$, q prime. Given an $n \times m$ matrix A with entries in $\mathbb{F}_q$ find $\vec{z} \neq 0$, $\vec{z} \in \mathbb{Z}^m$

such that

- $\|\vec{z}\| \leq \beta$
- $A\vec{z} \equiv 0 \mod q$

decision LWE reduces to SIS.

That's all for now!