Lecture 16: Lattice-based cryptography

June 2nd 2020

Logistics:

- HW 5 is out → it's shorter, we promise :)
  - Due June ~~13th~~ 4th !
  - ONE LATE DAY MAXIMUM !!
- As always, anonymous feedback welcome
- Please respond to course feedback on Axess !
  ↳ it's not differentially private :)

Plan: lattice-based cryptography

* Why lattices?
* Learning with errors & Regev encryption
* Worst-case lattice problems (time permitting)

Course overview

Foundations → Cryptanalysis, ECC → zero Knowledge → private computation → **Lattices** (LWE, FHE)

Why study lattice-based crypto?

1) Gives schemes with plausible post-quantum security
   - ↳ factoring, dlog are <u>easy</u> (poly time) on a quantum computer
   - ↳ no known efficient quantum algos for many lattice problems
   - ↳ ongoing standardization effort by NIST

2) New functionalities e.g. FHE
   - ↳ unknown how to build these from other assumptions

3) Nice theoretical consequences
   - ↳ Cryptography based on worst-case hardness
   - ↳ Holy grail: Crypto based on an <u>NP-hard</u> problem

Warmup: solving systems of equations over $\mathbb{Z}_q$

$$
\begin{aligned}
3x_1 + 4x_2 + 1x_3 &= 0 \\
4x_1 + 2x_2 + 6x_3 &= 1 \\
1x_1 + 1x_2 + 1x_3 &= 1
\end{aligned}
\qquad (\text{mod } 7)
$$

Solution: $x_1 = 1, \; x_2 = -1, \; x_3 = 1$

How: Gaussian elimination ! (works for any field)

Matrix notation:

m equations

n unknowns

$$A \in \mathbb{Z}_q^{m \times n} \cdot x \in \mathbb{Z}_q^{n} = b \in \mathbb{Z}_q^{m}$$

Learning with Errors

What if the system is noisy?

$\Rightarrow$ Given A and $Ax + e$ (random noise), can you recover x?

For some choices of parameters & noise, this is:

1) well-defined (x is unique with high probability)

2) Conjectured to be hard!

Some notation:

- We view $\mathbb{Z}_q$ as the integers in the range $\left(-\frac{q}{2}, \frac{q}{2}\right)$ $\rightarrow$ e.g. $\mathbb{Z}_7 = \{-3,-2,-1,0,1,2,3\}$
- for $e \in \mathbb{Z}_q^m$, $\|e\|_\infty = \max_i |e_i|$
- χ_B = B-bounded distribution $\Rightarrow \Pr_{e \leftarrow \chi_B^m}\left[\|e\|_\infty \le B\right] = 1$ (e.g. uniform on $\{-B, \dots, 0, \dots, B\}$)

# of unknowns

# of equations

$LWE(n, m, q, \chi_B)$: (search version)

Let $A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$, $s \xleftarrow{R} \mathbb{Z}_q^{n}$, $e \leftarrow \chi_B^{m}$

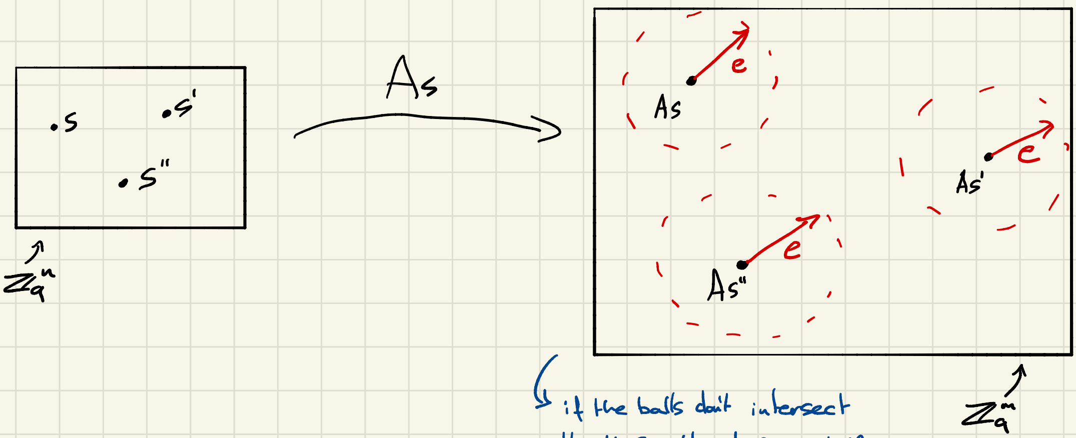
Given $(A, As+e)$ find s' s.t. $\|As' - (As+e)\|_\infty \le B$

↳ s is one possible solution (not necessarily unique)

That's a lot of parameters!

- n = security parameter (more unknowns = harder problem)
- $m = \text{poly}(n)$, $m \gg n$ (overdetermined) (more equations = easier problem)
- $q = \text{poly}(n)$, say $q = O(n^2)$
- $B \ll q$ (smaller noise bound = easier problem)

↳ m, B, q are chosen so that the search LWE problem has a unique solution with high probability



↳ if the balls don't intersect the LWE problem has a unique solution

From search to decision

In crypto, it's often easier to work with decision problems than with search problems.

e.g. DDH vs. CDH

↳ distinguish (g, g^a, g^b, g^{ab}) from (g, g^a, g^b, g^r)

↳ given (g, g^a, g^b) compute g^{ab}

$LWE(n, m, q, \chi_B)$: (decision version)

$$\underbrace{\left\{ (A, As+e) \;\middle|\; \begin{array}{l} A \xleftarrow{R} \mathbb{Z}_q^{m \times n} \\ s \leftarrow \mathbb{Z}_q^n \\ e \leftarrow \chi_B^m \end{array} \right\}}_{D_{LWE}} \qquad \underbrace{\left\{ (A, u) \;\middle|\; \begin{array}{l} A \xleftarrow{R} \mathbb{Z}_q^{m \times n} \\ u \xleftarrow{R} \mathbb{Z}_q^m \end{array} \right\}}_{D_{rand}}$$

Goal: distinguish D_{LWE} from D_{rand}

LWE assumption: $D_{LWE} \approx_c D_{rand}$

↳ Intuition: hard to distinguish vectors "close" to the image of A from random vectors in $\mathbb{Z}_q^m$

this is a small subset of $\mathbb{Z}_q^m$

↳ The search and decision versions of LWE are equally hard!

↳ we believe this isn't the case for DDH/CDH e.g. in pairing groups

Regev encryption (Regev 2005)

A simple "El-Gamal style" public-key cryptosystem from LWE

KeyGen(1^λ):

$$A \xleftarrow{R} \mathbb{Z}_q^{m\times n}$$
$$s \xleftarrow{R} \mathbb{Z}_q^{n}$$
$$e \leftarrow \chi_B^{m}$$
$$b = As + e$$

choose parameters such that $q/4 > mB$

set $sk = s$, $pk = (A, b)$ $\in \mathbb{Z}_q^m$

Encrypt$(pk, x \in \{0,1\})$:

this scheme encrypts a single bit at a time
(this is not very efficient but it gets the main ideas across)

$$r \xleftarrow{R} \{0,1\}^m$$

$$c_0 = r^T A, \quad c_1 = r^T b + \left\lfloor \frac{q}{2} \right\rfloor \cdot x$$

$\lfloor \cdot \rfloor$ rounds down to nearest integer

output $ct = (c_0, c_1) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$

Decrypt(sk, ct): $ct = (c_0, c_1)$

$$\tilde{x} = c_1 - c_0 \cdot s$$

if $|\tilde{x}| < q/4$ output $x = 0$

else output $x = 1$

Correctness:

$$\tilde{x} = c_1 - c_0 \cdot s = r^T b + \lfloor \tfrac{q}{2} \rfloor \cdot x - r^T A s$$
$$= r^T(As+e) + \lfloor \tfrac{q}{2} \rfloor \cdot x - r^T A s$$
$$= \cancel{r^T A s} + r^T e + \lfloor \tfrac{q}{2} \rfloor \cdot x - \cancel{r^T A s}$$
$$= r^T e + \lfloor \tfrac{q}{2} \rfloor \cdot x \rightarrow \text{"noisy" plaintext}$$

we have $e \leftarrow \chi_B^m$ and $r \xleftarrow{R} \{0,1\}^m$ so $|r^T e| \leq mB < q/4$

So if $x = 0$, $|\tilde{x}| < \frac{q}{4}$. If $x = 1$, $|\tilde{x}| > \lfloor \frac{q}{2} \rfloor - \frac{q}{4} \geq \frac{q}{4}$

Security: (sequence of hybrids over the view of the adversary)

real experiment

Hyb_0: $pk = (A, b = As+e)$, $c_0 = r^T A$, $c_1 = r^T b + \lfloor \frac{q}{2} \rfloor \cdot x$

indistinguisable by LWE

Hyb_1: $pk = (A, v \xleftarrow{R} \mathbb{Z}_q^m)$, $c_0 = r^T A$, $c_1 = r^T v + \lfloor \frac{q}{2} \rfloor \cdot x$

statistically indistinguishable using the leftover hash lemma

Hyb_2: $pk = (A, v \xleftarrow{R} \mathbb{Z}_q^m)$, $c_0 \xleftarrow{R} \mathbb{Z}_q^n$, $c_1 \xleftarrow{R} \mathbb{Z}_q$

In Hyb_2, the ciphertext is random and independent of the message x.

Leftover Hash Lemma (simplified version):

- Let $m \geq 2n \log q$
- if $A \xleftarrow{R} \mathbb{Z}_q^{m \times n}$, $x \xleftarrow{R} \{0,1\}^m$, $y \leftarrow \mathbb{Z}_q^n$, then

$$(A, x^T A) \approx_{stat} (A, y)$$

Hard Lattice problems

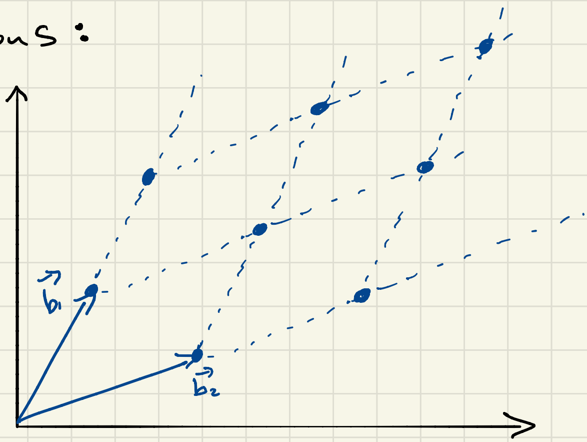
Why is LWE a "lattice" problem?

What's a lattice?

a set of points in $\mathbb{Z}^n$ that are linear combinations of some basis vectors $B = \{\vec{b}_1, \dots, \vec{b}_n\}$

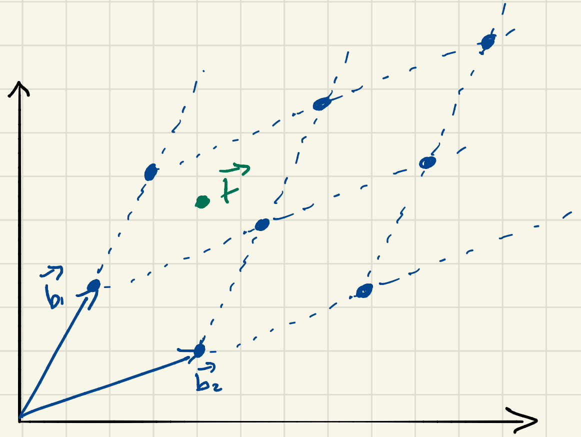
$$\mathcal{L}(B) = \left\{ \sum_{i=1}^{n} a_i \cdot \vec{b}_i \;\middle|\; a_i \in \mathbb{Z} \right\}$$

in 2 dimensions:



The hardness of LWE is related to the hardness of certain problems on lattices

Hard problems on lattices:



1) Shortest vector problem (SVP)

↳ find shortest (e.g. in ℓ_∞ norm) non-zero vector in $\mathcal{L}(B)$

↳ NP-hard !

2) Closest vector problem (CVP)

↳ given $\vec{t} \in \mathbb{Z}^n$, find $\vec{v} \in \mathcal{L}(B)$ that minimizes $\|\vec{t} - \vec{v}\|$

↳ Similarities to search LWE: given $\vec{t} = A\vec{s} + \vec{e}$, find closest point of the form $A\vec{s} \in \mathbb{Z}_q^m$

3) γ-SVP / γ-CVP

↳ solve SVP/CVP approximately (up to a factor $\gamma > 1$)

→ e.g. if shortest vector has norm N, it's sufficient to return a vector of norm $\gamma \cdot N$

* for $\gamma = O(1)$ γ-SVP is NP-hard

* for $\gamma = 2^{o(n)}$, γ-SVP is easy (poly time)

* for $\gamma = \text{poly}(n)$, γ-SVP is conjectured to be hard.

→ even for quantum algos

Moreover, if γ-SVP is hard for some lattice in $\mathbb{Z}^n$, this implies that $LWE(n, m, q, B)$ is also hard (for appropriate m, q, B)

⟹ We can base crypto on the (conjectured) worst-case hardness of a lattice problem.

⟹ Open question: base crypto on an NP-hard problem