COS 597A: Quantum Cryptography — Princeton University
Lecture 9 (October 10, 2018)
Lecturer: Mark Zhandry — Scribe: Barak Nehoran

Notes for Lecture 9

1 Lattice Cryptography (Part 2)

Last time, we saw the **shortest integer solution** problem:

Definition 1. SIS_{nmqb}*: given random* $A \in \mathbb{Z}_q^{n\times m}$*,* $m \gg n$*,* $b \ll q$
find x *s.t.*

- $0 < |x| \le b$
- $A \cdot x = 0 \mod q$

This is a special case of SVP_γ for

$$\Lambda_q^\perp(A) = \{x \in \mathbb{Z}^m : A \cdot x = 0 \mod q\}$$

There exists a proof (not covered here) that this special case is as hard as the hardest cases.

2 Learning With Errors (LWE)

Learning with errors is another problem related to SIS.

Definition 2. $\mathsf{LWE}_{nmq\chi}$*: given random* $A \in \mathbb{Z}_q^{n\times m}$*, and* $v \in \mathbb{Z}_q^m$ *sampled as*

- *pick random* $s \in \mathbb{Z}_q^n$
- *pick random* $e \leftarrow \chi^m$
- *set* $u^\top = s^\top A + e^\top \mod q$

The two versions of LWE are:

Search*: Find* s

Decision*: distinguish* u *from random vector*

This is a special case of CVP_γ for

$$\Lambda_q(A) = \left\{x \in \mathbb{Z}^m : x = A^\top s \mod q \text{ for some } s\right\}$$

the lattice spanned by the rows of A and $(q,0,0,\dots),(0,q,0,\dots),\dots,(0,0,0,\dots,q)$

3 Public Key Encryption from LWE

pk: $A, u \leftarrow \mathsf{LWE}_{nmq\chi}$

sk: s

$\mathsf{Enc}(pk, m)$:

- choose a random $x \in \{0,1\}^m$
- output $c_0 = A \cdot x$, $c_1 = u \cdot x + f(m) \mod q$

$\mathsf{Dec}(sk, (c_0, c_1))$:

- $c_1 - s^\top c_0 = \left(s^\top A + e^\top\right) \cdot x + f(m) - s^\top Ax \mod q = f(m) + e^\top x \mod q$

Need $f(m)$ invertible even under small errors

$$f(m) = m \cdot \left\lceil \frac{q}{2} \right\rfloor \qquad m \in \{0,1\}$$

4 Security Proof

Proof. Suppose pk is sampled uniformly in $\mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^m$

Fact: $\binom{A}{u} \cdot x \approx$ uniform in $\mathbb{Z}_q^{(n+1)}$ if $m \gg n \log q$

Entropy of x is m.

Entropy of random $\mathbb{Z}_q^{(n+1)}$ is $(n+1)\log q$.

This is true even given A, u.

Apply this to cyphertext:

$$\begin{matrix} c_0 = A \cdot x \\ c_1 = u \cdot x + f(m) \end{matrix} \approx \text{ random}$$

so this completely hides m.

For decisional LWE, the adversary can't tell if pk is honest or random. This can be used to reduce LWE to the encryption scheme. (If the encryption scheme can be broken by the adversary, use the adversary to solve decisional LWE.)

$\square$

5 Dual Scheme

pk: $A \in \mathbb{Z}_q^{n \times m}$

sk: $x \in \{0,1\}^m$ s.t. $A \cdot x = 0 \mod q$

choose x first then choose A

Fact: $A \approx$ random

Let's consider encrypting just a single bit, b (though this can be extended to any message).

$\mathsf{Enc}(pk, b)$:

- if $b = 0$: choose u random in $\mathbb{Z}_q^m$
- if $b = 1$: choose $u^\top = s^\top A + e^\top$ as in LWE for random s, and short e

$\mathsf{Dec}(sk, c)$: $c^\top \cdot x$

- if $b = 0$: $u^\top \cdot x =$ random in $\mathbb{Z}_q^m$
- if $b = 1$: $s^\top A \cdot x + e^\top \cdot x = e^\top \cdot x \mod q$, which is small

(**Note**: in practice, use $u = s^\top A + e^\top + f(m)$, where $f(m) = m \cdot \lceil \frac{q}{2} \rfloor$)

Breaking the Dual Scheme allows solving decisional LWE.

Futher, a SIS solution allows breaking the Dual Scheme.

So a SIS solution implies a decisional LWE solution.

Finally, using a quantum computer a search LWE solution leads to a SIS solution.

6 Search LWE $\Rightarrow$ SIS

Setup:

- **Goal 1**: given A, we want to find a SIS solution using an algorithm for search LWE
- **Goal 2**: construct the state

  $$|\psi\rangle \propto \sum_{\substack{x \in \mathbb{Z}_q^m \text{ s.t.} \\ A \cdot x = 0 \mod q}} \chi_\sigma(x)|x\rangle$$

  where $\chi_\sigma(x)$ is discrete Gaussian weighting.
- **Goal 3**: construct the state

  $$|\varphi\rangle \propto \sum_{s,e} \chi_{q/\sigma}(e)|s^\top A + e^\top\rangle$$

Observation 1: Measuring from Goal 2 solves Goal 1.

Observation 2: Applying the multidimensional Quantum Fourier Transform, mod q, to Goal 3 solves Goal 2.

Proof.

- QFT of $\sum \chi_\sigma(x)|x\rangle \approx \sum_e \chi_{q/\sigma}(e)|e\rangle$
- QFT of $\sum_{x \in \mathbb{Z}_q^m \text{ s.t. } A \cdot x = 0 \mod q} |x\rangle \to \sum_{x \in \mathbb{Z}_q^n} |s^\top A \mod q\rangle$
- multiplication before Fourier Transform is equivalent to convolution after the Fourier Transform. That is

  $$\sum_x \alpha_x \beta_x |x\rangle \to \sum_{y,z} \hat{\alpha}_y \hat{\beta}_z |y + z\rangle$$

- Now, let $\alpha_x = \begin{cases} 1, & \text{if } A \cdot x = 0 \mod q \\ 0, & \text{otherwise} \end{cases}$ and let $\beta_x = \chi_\sigma(x)$

□

So solving Goal 1 reduces to solving Goal 3.

6.1 Solving Goal 3

1. construct $\sum_{s,e} \chi_{q/\sigma}|s, e\rangle$
2. compute $|s, e\rangle \to |s, e\rangle|s^\top A + e^\top \bmod q\rangle$

$$\sum_{s,e} \chi_{q/\sigma}(e)|s, e, s^\top A + e^\top \bmod q\rangle$$

3. uncompute e

$$\sum_{s,e} \chi_{q/\sigma}(e)|s, s^\top A + e^\top \bmod q\rangle$$

4. use LWE solver to uncompute s

$$\sum_{s,e} \chi_{q/\sigma}(e)|s^\top A + e^\top \bmod q\rangle$$

and we're done!