Lecture 16: Lattice-based Cryptography

June 2nd 2020
Logistics:

• HW 5 is out  • Due June 10th
  • ONE LATE DAY MAXIMUM

• As always, anonymous feedback welcome

• Please respond to course feedback on Axess

Plan: lattice-based cryptography

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

Why study lattice-based crypto?

1) Gives schemes with plausible post-quantum security
   - Factoring, DLog are easy (polynomial) on a quantum computer
   - No known efficient quantum algs for many lattice problems
   - Ongoing standardization effort by NIST

2) New functionalities e.g.
   - LWE, 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 NP-hard problem
Warmup: solving systems of equations over $\mathbb{Z}_q$

\[ \begin{align*}
3x_1 + 4x_2 + 1x_3 &= 0 \\
4x_1 + 2x_2 + 6x_3 &= 1 \\
1x_1 + 1x_2 + 1x_3 &= 1 \\
\end{align*} \quad \text{(mod 7)} \]

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

How: Gaussian elimination \( \checkmark \) (works for any field)

Matrix notation:

\[ \begin{align*}
A \in \mathbb{Z}_q^{m \times n} \cdot x \in \mathbb{Z}_q^n &= b \in \mathbb{Z}_q^n
\end{align*} \]
Learning with Errors

What if the system is noisy?

\( \Rightarrow \) Given \( A \) and \( Ax + e \), 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 \((-\frac{q}{2}, \frac{q}{2})\)
- For \( e \in \mathbb{Z}_q^m \), \( \|e\|_\infty = \max |e_i| \)
- \( X_B = B\text{-bounded distribution} \Rightarrow \Pr_{e \sim X_B} [\|e\|_\infty \leq B] = 1 \)

\( \rightarrow \) eg. \( \mathbb{Z}_3 = \{\pm 3, \pm 2, \pm 1, 0, 1, 2, 3\} \)

eg uniform on \( -3, -2, \ldots, 0, \ldots, 3 \)
LWE(\(n, m, q, x_B\)): (search version)

Let \(A \leftarrow Z_q^{m \times n}\), \(s \leftarrow Z_q^n\), \(e \leftarrow X_B^n\)

Given \((A, As + e)\) find \(s'\) such that \(|As' - (As + e)|_2 \leq B\)

\(\Rightarrow s\) is one possible solution (not necessarily unique)

That’s a lot of parameters!

- \(n = \) security parameter (more unknowns = harder problem)
- \(m = \text{poly}(n), m \gg n\) (over-determined) (more equations = easier problem)
- \(q = \text{poly}(n), \) say \(q = d n^3\)
- \(B \ll q\) (smaller noise bound = easier problem)

\(\Rightarrow m, B, q\) are chosen so that the search LWE problem has a unique solution with high probability
From search to decision

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

E.g. **DDH** vs. **CDH**

- **DDH**: Given \((g, g^a, g^b)\), compute \(g^{ab}\)
- **CDH**: Given \((g, g^a, g^b)\), compute \(g^{ab}\)

\[ \text{LWE}(u, m, q, X_b): \text{ (decision version)} \]

\[
\begin{align*}
\left\{ (A, As+E) \right\} & \rightarrow \begin{cases} 
A \leftarrow \mathbb{Z}_q^{m \times n} \\
E \leftarrow \mathbb{Z}_q^n \\
e \leftarrow \mathbb{Z}_q^n
\end{cases} \\
\text{Dlwe} & \rightarrow \begin{cases} 
A \leftarrow \mathbb{Z}_q^{m \times n} \\
U \leftarrow \mathbb{Z}_q^n
\end{cases} \\
\text{Drand} &
\end{align*}
\]

Goal: distinguish \text{Dlwe} from \text{Drand}

**LWE assumption**: \text{Dlwe} \neq \text{Drand}

Intuition: hard to distinguish vectors "close" to the image of \(A\) from random vectors in \(\mathbb{Z}_q^n\)

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

**Key Gen(1^k):**

\[
\begin{align*}
A & \leftarrow \mathbb{Z}_q^{m \times n} \\
s & \leftarrow \mathbb{Z}_q^* \\
e & \leftarrow X_{\mathbb{Z}_q^*} \\
b & = As + e \\
end{align*}
\]

\{ choose parameters such that \( q/4 > mB \) \}

set \( sk = s \), \( pk = (A, b) \)

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

\[
\begin{align*}
c_0 & \leftarrow \mathbb{Z}_q^{m} \\
r & \leftarrow \mathbb{Z}_q^{m} \quad \left( \text{rounds down to nearest integer} \right) \\
c_0 = r^TA, \quad c_1 = r^Tb + \left\lfloor \frac{q}{2} \right\rfloor \cdot x \\
end{align*}
\]

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

**Decrypt (sk, ct):**

\[
\begin{align*}
x & = c_1 - c_0 \cdot s \\
if \ |x| < q/4 & \text{ output } x = 0 \\
else & \text{ output } x = 1
\end{align*}
\]
Correctness:

\[
\tilde{x} = c_1 - c_0 \cdot s = r^T b + L_{\frac{q}{3}} \cdot x - r^T As
\]
\[
= r^T (As e) + L_{\frac{q}{3}} \cdot x - r^T As
\]
\[
= r^T As + r^T e + L_{\frac{q}{3}} \cdot x - r^T As
\]
\[= r^T e + L_{\frac{q}{3}} \cdot x \rightarrow "noisy" \text{ plaintext}
\]

We have \( e \leftarrow \chi^m \) and \( r \leftarrow \chi^{0,13^m} \) so \( |r^T e| \leq mB < q/4 \)

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

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

<table>
<thead>
<tr>
<th>experiment</th>
<th>( H_{ybo} ): ( pk = (A, b = A \cdot x e) ), ( c_0 = r^T A ), ( c_1 = r^T b + L_{\frac{q}{3}} \cdot x )</th>
</tr>
</thead>
<tbody>
<tr>
<td>indistinguishable</td>
<td>( H_{yb1} ): ( pk = (A, v \leftarrow Z_q^m) ), ( c_0 = r^T A ), ( c_1 = r^T v + L_{\frac{q}{3}} \cdot x )</td>
</tr>
<tr>
<td>statistically indistinguishable</td>
<td>( H_{yb2} ): ( pk = (A, v \leftarrow Z_q^m) ), ( c_0 \leftarrow Z_q^m ), ( c_1 \leftarrow Z_q )</td>
</tr>
</tbody>
</table>

In \( H_{yb2} \), the ciphertext is random and independent of the message \( x \).

Leftover Hash Lemma (simplified version):

- Let \( m \geq 2n \log q \)
- If \( A \leftarrow Z_q^{mn}, x \leftarrow \xi_0,13^m, y \leftarrow Z_q^m \), then \((A, x^T A) \nleftrightarrow (A, y)\)
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 $B = \{b_1, \ldots, b_n\}$

$L(B) = \{ \sum_{i=1}^{n} a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \}$

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 $\|\cdot\|_\infty$ norm) non-zero vector in $\mathbb{L}(B)$
   - $\leftrightarrow$ NP-hard

2) **Closest vector problem (CVP)**
   - Given $\mathbf{f} \in \mathbb{Z}^n$, find $\mathbf{v} \in \mathbb{L}(B)$ that minimizes $\|\mathbf{f} - \mathbf{v}\|$
   - $\leftrightarrow$ Similarities to search LWE: given $\mathbf{f} = \mathbf{h}_s + \mathbf{e}$, find closest point of the form $\mathbf{h}_s' \in \mathbb{Z}^n$

3) **$\gamma$-SVP / $\gamma$-CVP**
   - Solve SVP/CVP approximately (up to a factor $\gamma > 1$)

   * for $\gamma = O(1)$, $\gamma$-SVP is NP-hard
   * for $\gamma = 2^{\omega(n)}$, $\gamma$-SVP is easy (polynomial time)
   * for $\gamma = \text{poly}(n)$, $\gamma$-SVP is conjectured to be hard.

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

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

$\Rightarrow$ Open question: base crypto on an NP-hard problem