CS 4501-6501 Topics in Cryptography	2015/02/09
Lecture 8	
Lecturer: Mohammad Mahmoody	*Scribe: Dasith Gunawardhana*

1 Overview

- Previous lecture: Private-key encryption from LWE
- Today: Public-key encryption from LWE using leftover hash lemma

2 Private-Key Encryption (Regev's) Review

- Secret key: Vector s with components in $\mathbb{Z}_q^n$
- LWE tells us it is hard to distinguish $(a, \langle a, s\rangle + e)$ vs. (random)
  - e is noise
- Encryption:
  - Encrypt $b \in \{0, 1\}$ as $(a, \langle a, s\rangle + e + b \cdot (\frac{q+1}{2}))$
  - Can flip from 0 to 1 by adding or subtracting $\frac{q+1}{2}$
  - a is a random element of $\mathbb{Z}_q^n$

3 Public-Key Encryption

3.1 General Idea

- Publish $\begin{bmatrix} c_0^1 & c_0^2 & \dots & c_0^k \\ c_1^1 & c_1^2 & \dots & c_1^k \end{bmatrix}$ as public key, where c_0^i and c_1^i are ciphertexts encrypting 0 and 1 respectively
- To encrypt, choose a random subset of the matrix

3.2 Applying the General Idea to Regev's

- Private key, s, is the same
- Public key: $A' = (A, b) = \begin{bmatrix} \vec{a}_1 & b_1 \\ \vec{a}_2 & b_2 \\ \vdots & \vdots \\ \vec{a}_m & b_m \end{bmatrix} = (A = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix}), b$
  - Matrix of encryptions of 0, where each row is a random sample of the secret keyspace

- Each $\vec{a}_i$ is a vector of n elements

- $b = A \cdot s + \vec{e}$
  - $\vec{e}$ is a vector of noise

3.3 Encrypting 0

- Idea: Choose a random subset of the rows and add them
- Let R be a Boolean vector in $\{0, 1\}^m$
- $\text{Enc}(0) = R \times A'$
  - Has dimension $n + 1$, has the form (c, b)

3.4 Encrypting 1

- Encrypt 0 to get (c, b) then change b to $b + \frac{q+1}{2}$

3.5 Proof of Security

- Leftmost case is encrypting 0, rightmost is encrypting 1, we will show that an adversary cannot tell them apart

World 0	Imaginary 0	Imaginary 1	World 1
Public key: $[A, b] = A'$	Choose A' completely at random	A' is completely at random	Public key: $[A, b] = A'$
Cipher for 0: RA'	RA'	RA' with the last component shifted	Cipher for 1: (RA' = cipher for 0) with the last component shifted

- **Lemma 1:** World 0 is indistinguishable from Imaginary 0.
  If some adversary ADV can tell apart the two worlds, then there exists some ADV' which can solve LWE.

- **Lemma 2:** No efficient adversary can distinguish World 1 from Imaginary 1.
  Subtract $\frac{q}{2}$ then reduce to **Lemma 1**

- **Lemma 3:** No ADV can tell apart Imaginary 0 from Imaginary 1 by more than 2^{-k} probability if $m >> 2k + (n + 1) \log_2 q$
  - **Statistical Distance:** The statistical distance $\Delta(X, Y)$ between random variables X and Y is defined as:

$$\Delta(X, Y) = \frac{1}{2} \sum_{\alpha} | \Pr[X = \alpha] - \Pr[Y = \alpha] |$$

α is any possible value of X or Y.

- **Main Lemma about Statistical Distance:** The statistical distance $\Delta(X, Y) = \varepsilon$ iff there exists an adversary who can distinguish samples from X from samples from Y by advantage ε.

- **Lemma 3' (implies Lemma 3):** The distribution of (A', RA') is statistically close to (A', U) ($\Delta((A', RA'), (A', U)) \leq 2^{-k}$) if $m \geq 2k + n \log_2 q$.
  $q \leq$ poly(n) and $m \leq \; O(n)$
  - **Leftover Hash Lemma:** Let $Ex : R \times A' \to x$ be a function such that:
    * $x \in \mid \mathbf{Z}_p^n \mid = 2^{n \log p}$
    * Randomness of $R = m \geq 2k + n \log q$
    * For any $R_1 \neq R_2$ the distribution of $Ex((R_1, A), (R_2, A)) \equiv (U, U')$. A is the same in both, and U and U' are independent.

    Then the distribution of (A', x) is statistically close to (A, U) i.e. $\Delta((A', x), (A, U)) \leq 2^{-k}$ U is over the range of x.

    The function Ex is a called a **strong extractor**.

  The Lemma states that a public key and a ciphertext looks like a public key and a uniform random vector.

3.6 Summary

- We now have a public-key encryption scheme based on LWE that allows addition.

References

Regev, O.: On lattices, learning with errors, random linear codes, and cryptography. In STOC 2005 (2005) 8493.