University of Michigan–Ann Arbor

Department of Electrical Engineering and Computer Science

EECS 475 **Introduction to Cryptography**, Winter 2023

Lecture 26: Post-quantum and lattice-based cryptography

April 12, 2023

Lecturer: Mahdi Cheraghchi

Scribe: Yi-Wen Tseng

1 Introduction

In 1994, Peter Shor proposed a quantum algorithm that can factorize integers in polynomial time. The idea behind this algorithm is to use the complex probabilities (quantum weidness). The development of algorithm means that we can use it to break RSA which relies on the hardness of factorizing.

Also, quantum search is weid. Based on Grover's algorithm, we can search in an unstructured array of size N using $O(N)$ operations. In crypto, quantum computers can brute force for a key of length N in time $2^{\frac{N}{2}}$ rather than 2^N. The remedy is to double the key size, so the computational complexity is $O(2^{\frac{2N}{2}}) = O(2^N)$.

Shor's algorithm also computes Discrete log in polynomial time. This means that it can break Diffie-Hellmen, El-Gamal, etc.

Thus, post-quantum cryptography can not rely on the hardness of factoring and discrete log. The older proposal is to rely on the hardness of solving subset sum or hash functions. The more successful proposals rely on **Coding Theory** and **Lattice Theory** instead.

2 Lattice Based Crypto

Idea: Build crypto based on hardness of problems about lattices

Lattice: a periodic, infinite grid in n-dim space $\mathbb{R}^n$. It is generated by n basis vectos in $\mathbb{R}^n$. It is same as vector space, but with integer linear combinations of vectors only.

$$\mathcal{B} = \{b_1, b_2, \ldots, b_n\}$$

$$\mathcal{L}\{\mathcal{B}\} = \{z_1 \cdot b_1 + z_2 \cdot b_2 + z_n \cdot b_n : z_i \in \mathbb{Z}\}$$

in matrix form: $\mathcal{L}\{\mathcal{B}\} = \{B \cdot z : z \in \mathbb{Z}^n\} \subseteq \mathbb{R}^n$

Below is a list of conjectured lattice problems:

1. Shortest Vector Problem (SVP): Given B, find the shortest (or a "very short") nonzero vectr $v \in \mathbb{L}(B)$
2. Decoding (a.k.a Closest Vector or CVP): Given B, and a target point $t \in \mathbb{R}^n$, find teh closest vector in $\mathbb{L}(B)$ to t.
3. Learning With Errors (LWE):

   - Fix n (dimension)
   - Fix $q \approx n^2$

   Pick a secret $s \leftarrow \mathbb{Z}_q^n$, an instance of LWE is to find the secret s in the construction below given n, q, A, b: which is conjectured to be hard.

3 Learning With Errors

3.1 LWE and CVP

LWE is closely related to CVP: $b \approx A \cdot s$ is a target vector close to lattice point $v = A \cdot s$, where A is the lattice basis.

Decision LWE: Given (A, b), distinguish between

1. (A,$b \approx A \cdot s$)
2. (A,b) uniform random

Theorem: LWE search and decision are equivalent under ppt reduction. (each can be solved efficiently iff the other can)

3.2 LWE for Key Exchange

Alice and Bob can agree on a bit in the end.
This can be turned into p.k.e just like turing Diffie-Hellmen to El-Gamal.
To encrypt a bit $m \in \{0, 1\}$, Alice can compute $c \approx r^t \cdot u + m \cdot (\frac{q}{2})$
To recover m: compute $p = c - v^t \cdot s \approx \underbrace{r^t \cdot A \cdot s}_{k_A} + m(\frac{q}{2}) - \underbrace{r^t \cdot A \cdot s}_{k_B} = m(\frac{q}{2})$ can recover m by seeing if p is closer to 0 or $\frac{q}{2}$.

Theorem: This key agreement/PKE is CPA secure assuming LWE decision is hard.