Lattice-Based Cryptography, LWE/LWR

Srikar Varadaraj

Columbia University

5/3/2016

Introduction

- What exactly is lattice cryptography?
- Why should we care about it?

Peikert

The use of *apparently* hard problems on point lattices in $\mathbb{R}^n$ as the foundation for secure cryptographic constructions.

What makes Lattice-Crypto Special?

- Conjectured security against *quantum* attacks.

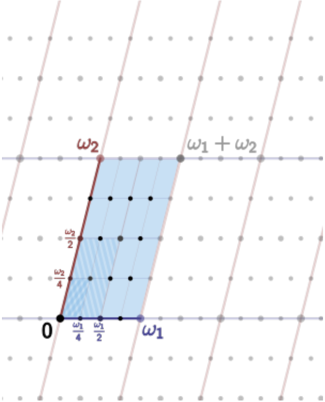
Number-Theoretic cryptography (Diffie-Hellman,RSA) rely on hardness of integer factorization/ discrete-log in groups. But Shor's Quantum Algorithm finds integer factorization in time $O(n)$!

- Ajtai'96 proved that the worst-case hardness of lattice problems implies average-case hardness of certain problems.

What makes Lattice-Crypto Special?

Gentry[*Gen*09*b*, *Gen*09*a*] proposed the first candidate for FHE(Fully Homomorphic Encryption) based on lattices! All further constructions were based on lattices as well.

Lattice: Definition



An $n-$dimensional lattice L is a subset of $\mathbb{R}^n$ which has the structure of:
(1). An additive subgroup $\implies$ $\mathbf{0} \in L$, $-x, x+y \in L\ \forall x, y \in L$.
(2). A discrete set $\implies$ $\forall x \in L$, $\exists$ a neighborhood of x in $\mathbb{R}^n$ such that x is the only point in L contained in the neighborhood.

GapSVP, SVP

We define the minimum distance of a lattice L as the length of the shortest non-zero lattice vector: $\lambda_1(L) = min_{v \in L - \{0\}} ||v||$.
$||v||$ denotes the Euclidean norm. The notion can be generalized by defining $\lambda_i(L)$ as the smallest r such that L has i linearly independent vectors of norm at most r.

GapSVP,SVP

SVP Problem:
Given an arbitrary basis B of an n-dimensional lattice $L = L(B)$, find a non-zero vector $v \in L$ for which $||v|| = \lambda_1(L)$.
SVP$_\gamma$ Problem:
Given a lattice basis B, find a nonzero $v \in L(B)$ such that $0 < ||v|| \leq \gamma\lambda_1(L(B))$. Here $\gamma = \gamma(n) \geq 1$ is a function of dimension n.

GapSVP,SVP

GapSVP$_\gamma$ Problem:
Given a lattice basis B and a positive integer d, output whether $\lambda_1(L(B)) \leq d$ is true or $\lambda_1(L(B)) > d$.
We have the intuitive result: $GapSVP_\lambda \leq SVP_\lambda$ in general.

LPN: Definition

We are provided with samples $(x, f(x))$ where $f(x) \in \{0, 1\}$. However, with some small probability, we are provided with $1 - f(x)$. The idea is to recover the secret if the output is sometimes flipped, or perturbed. Since $f(x)$ has only two possibilities, it represents the parity of a number, since 0 represents $0 \pmod 2$ and 1 represents $1 \pmod 2$.

LPN - Algorithm

For an integer $n \geq 1$ and some real number $\epsilon \geq 0$, we need to find an unknown $s \in \mathbb{Z}_2^n$ if we have a list of equations:
$< s, a_1 > \approx_\epsilon b_1 (mod 2)$

LPN-Algorithm

We can find a set S of $O(n)$ equations such that $\sum_S a_i = (1, 0, ..., 0)$ using Gaussian Elimination. Summing the corresponding values for b_i, gives us a good guess for the first bit of s.
Each b_i is correct with a probability $1 - \epsilon$. We note that this is $\frac{1}{2} + 2^{-\Theta(n)}$. This implies that to get the first bit of s with high probability $(1 - \frac{1}{poly(n)})$, we need to repeat the algorithm $2^{\Theta(n)}$ times.

LPN-Algorithm

Blum et al. provide a subexponential algorithm for the problem. They only use $2^{O(n/log n)}$ equations/time. Best algorithm known today!

LWE: Definition

Let $q = p(n) \leq poly(n)$ be some prime integer (note that in later discussions, we do not have this restriction) and we have a list of equations with error:

$$< s, a_1 > \approx_\chi b_1(modq)$$
$$< s, a_2 > \approx_\chi b_2(modq)$$
$$\vdots$$

$s \in \mathbb{Z}_n^q$ and a_i are chosen independently and uniformly from $\mathbb{Z}_q^n$, $b_i \in \mathbb{Z}_q$. Note that the error now has a distribution specified by $\chi : \mathbb{Z}_q \to \mathbb{R}^+$ on $\mathbb{Z}_q$.
Thus we have:

$$b_i =< s, a_i > +e_i \tag{1}$$

where each e_i is chosen independently according to χ. Now we simply have the problem of learning the secret s given all the equations above with the error added. We denote this problem by $\text{LWE}_{q,\chi}$ as in the paper.

Regev's Result

Let n, p be integers and $\alpha \in (0,1)$ be such that $\alpha p > 2\sqrt(n)$. If there is an efficient algorithm that solves $\mathrm{LWE}_{p,\psi_\alpha}$ then there exists an efficient quantum algorithm that approximates the decision version of the shortest vector problem (GAPSVP) and the shortest independent vectors problem (SIVP) to within $\tilde{O}(n/\alpha)$ in the worst case.

Learning With Rounding (LWR)

Proposed by Banerjee, Peikert, Rosen.
LWR$_{n,q,p}$ **Definition:** We draw independent samples $a_i \in \mathbb{Z}_q^n$ and then round $< a_i, s >$ mod p. We then have to distinguish these rounded inner products from uniform random samples in $\mathbb{Z}_p$. Here $q, p \in \mathbb{N}$.

Discrete Gaussian

The Discrete Gaussian Distribution χ_σ on $\mathbb{Z}_q$ with standard deviation σ : $\chi_\sigma(x)$.

Definition:

For any center $c \in R$, and Gaussian parameter $s \in \mathbb{R}+$, define the discrete Gaussian distribution as:

$$D_{s,c}(x) = \frac{\rho_{s,c}(x)}{\sum_{y=-\infty}^{\infty} \rho_{s,c}(y)} \forall x \in \mathbb{Z}, \tag{2}$$

where ρ denotes the Gaussian function $\rho_{s,c}(x) = e^{-\pi|x-c|^2/s^2}$