CIS 700 Lecture 25: Lattice-based cryptography

The first Lattice-based cryptosystems

Ajtai-Dwork: Security of unique SVP
probably broken (Nguyen-Stern)

NTRU (Hoffstein, Pipher, Silverman)
: Works over rings $\mathbb{Z}[X]/X^N-1$
heuristically based on hard ideal lattices

GGH (Goldreich, Goldwasser, Halevi)
: CVP in trapdoor lattices
Broken by Nguyen-Stern

Thm Decisional CVP is NP-complete

Pf CVP in NP: $x \in L(B)$ satisfying $\|x-t\| \le r$ is a witness.

Reduction from subset sum to CVP:

subset sum instance $a_1, \ldots, a_n, s$ $\quad \sum_{i \in A} a_i = S$

CVP instance

$$B = \begin{bmatrix} 2 & & & a_1 \\ & 2 & & a_2 \\ & & \ddots & \vdots \\ & & & 2 \; a_n \end{bmatrix} \} n \qquad t = [1 \; 1 \; 1 \ldots S] \quad (n+1) \qquad r = \sqrt{n}$$

If subset sum yes instance: $\exists$ lattice vector $[0\,2\,0\,0\,2 \ldots S] = v$

$\|v - t\| = \sqrt{n}$

If $\exists x \in L(B)$ $\|t-x\| \le \sqrt{n}$: last n coords even $\Rightarrow \|t-x\| \ge \sqrt{n}$

If $\|t-x\| = \sqrt{n}$ then last coord $= 0$ and other coords 0 or 2

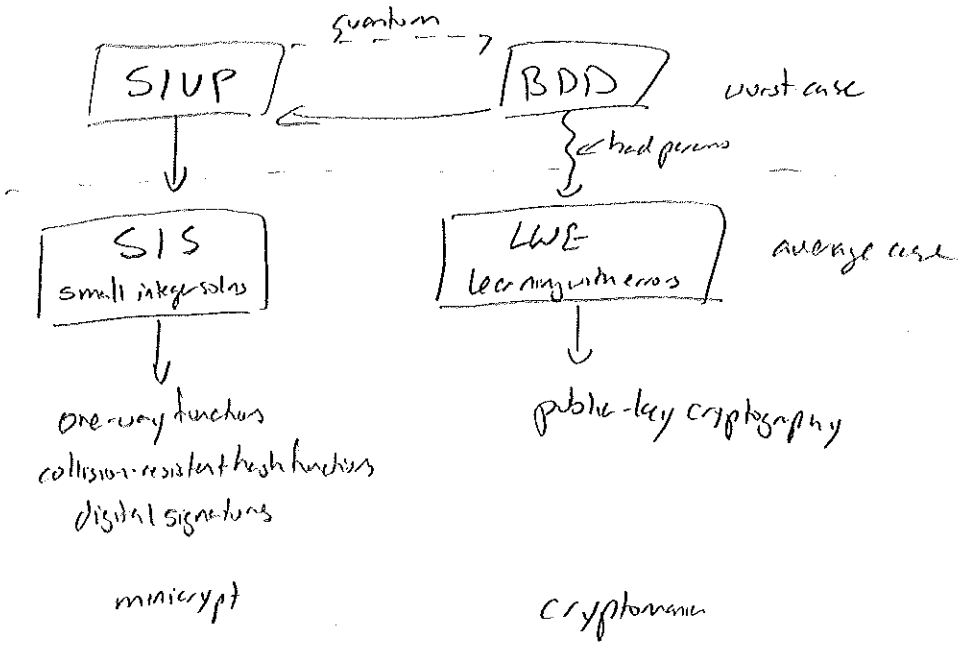
$\Rightarrow x$ is subset sum s/n.

Bounded Distance Decoding

Given B, t s.t. $d(t,B) < \gamma \lambda_1(B)$ find v closest to t.

"Modern" Lattice-Based Cryptography

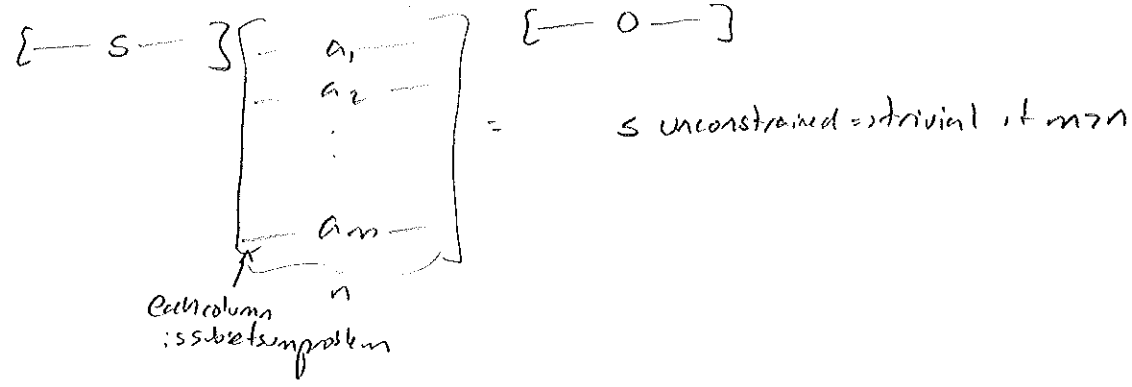
Lyubashevsky



SIS Small Integer Solution

Input: m vectors $a_i \in \mathbb{F}_q^n$

Goal: Find nontrivial $s \in \{0, \pm 1\}^m$ s.t. $sA = 0 \bmod q$



Let $\Lambda_q^\perp(A) = \{y \in \mathbb{Z}^m : yA = 0 \bmod q\}$

- is a lattice
- SIS: find short vector in this lattice
- set $m > \log n$

Collision-resistant hash function from SIS

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

Input $x \in \{0,1\}^m$. $H(x) = xA$

$m > n \log q$ for compression.

Thm H is collision-resistant if SIS hard.

Pf Assume not. Can find x_1, x_2 s.t. $H(x_1) = H(x_2)$

$$[x_1 - x_2] \begin{bmatrix} & A & \end{bmatrix} = [\ 0\ ]$$

$x_1 - x_2 \in \{0, \pm 1\}^m$

Reduction SIVP → SIS

Tool: Gaussian Sampling

Def Gaussian Function

$\rho_{s,c}(x) = e^{-\pi (x-c)^2 / s^2}$

Thm 1 (Micciancio-Regev)

$s > \sqrt{\omega(\log n)} \cdot \lambda_n(L)$ $\Rightarrow \sum_{v \in L} \rho_{sv} = (1 \pm \varepsilon)$ uniform

Thm 2 (Micciancio Regev)

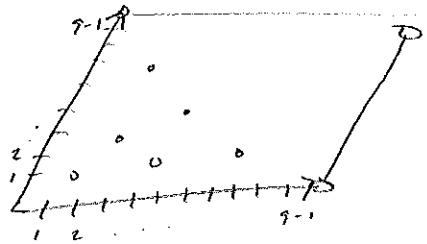
A sample from $\rho_{s,c}$ has distance $\leq s\sqrt{n}$ from c w.p. $1 - 2^{-n}$

Reduction

Input: Basis for L

SIS oracle that works on random instances

Goal: Find a short vector $\in L$.



Algorithm:

1. Sample m points from discrete Gaussian centered at the points.
   $\Rightarrow$ Random SIS instance $\{a_i\}$ uniform by Thm 2 above
2. Input $\{a_i\}$ to SIS oracle.
3. Oracle outputs $\{b_i \in \{-1, 0, +1\}\}$ s.t. $\sum_i a_i b_i = 0 \bmod q$
4. $a_i = v_i + e_i$ (e_i = error, v_i = lattice vector)

$$0 = \sum_i a_i b_i = \sum_i (v_i + e_i) b_i \Rightarrow \sum_i e_i b_i \in L$$

not too large by Thm 1.

Params: $|s| \leq \beta$ $\beta \geq \sqrt{m}$

$m \geq 2n \log q$

o.h.p. every SIS instance has soln. for every point

Thm Reduction works

$q \geq 2\beta\sqrt{n}$

Solving SIS for $|s| \leq \beta \Rightarrow$

solve $2\beta\sqrt{n}$-SIVP

for any n-dimensional lattice.

Learning With Errors (LWE)

Fix s.

Input: m samples $(a_i, b_i = \langle a_i, s \rangle + e_i \bmod q)$

a_i, e_i randomly chosen

Goal: Find s.

$$\begin{bmatrix} — & a_1 & — \\ & \vdots & \\ — & a_m & — \end{bmatrix} \begin{bmatrix} | \\ s \\ | \end{bmatrix} + \begin{bmatrix} e_1 \\ \vdots \\ e_m \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

Generalization of Learning Parity w/ noise from machine learning.

LWE like subset sum (Lyubashevsky)

$c_m \quad \dots \quad c_1$ ← carry bits

$$[— s —] \begin{bmatrix} — & a_1 & — \\ & \vdots & \\ — & a_n & — \end{bmatrix} \} \text{basis}$$

$$[b_m \quad \dots \quad b_1]$$

Subset sum instance $\{a_i\}$

Target b

$s \in \{0,1\}^n$

Transpose:

$$\begin{bmatrix} c_1 \\ \vdots \\ c_m \end{bmatrix} + \begin{bmatrix} — & a_1' & — \\ & \vdots & \\ — & a_n' & — \end{bmatrix} \begin{bmatrix} | \\ s \\ | \end{bmatrix} = \begin{bmatrix} b_1 \\ \vdots \\ b_m \end{bmatrix}$$

replace w/ random errors → LWE

LWE as lattice problem

$L(A) = \{y \in \mathbb{Z}^m : y = As \bmod q \text{ for } s \in \mathbb{Z}^n\}$

LWE: If e_i small, solve CVP on $L(A)$

Decisional LWE:

Distinguish LWE samples from uniform.

Random self-reduction:

Given $(a, b = \langle a, s \rangle + e)$, $(a, b + \langle t, a \rangle) = (a, \langle s+t, a \rangle + e)$ is sample from LWE

$\langle a, s \rangle + e + \langle t, a \rangle$

Reduction from search to decision:

Assume can distinguish LWE dist. from uniform.

For k in $0 \dots q$ do:

1. Sample instances (a, b) from LWE.
2. Map (a, b) to $(a + (r, 0, \dots, 0), b + rk)$

If k correct, will look like LWE sample

incorrect, uniform.

Public-key encryption based on LWE.

Private key: s

Public key: m samples $\{(a_i, b_i = \langle a_i, s\rangle + e_i)\}$ from LWE dist.

Encrypt: Choose random subset S of LWE samples.

$$A_S = \sum_S a_i \qquad B_S = \sum_S b_i$$

$$\underset{b.i.t}{Enc(b)} = \begin{cases} (A_S, B_S) & \text{if } 0 \\ (A_S, B_S + q/2) & \text{if } 1 \end{cases}$$

Decrypt:

$$Dec(A_S, B_S) = \begin{cases} 0 & \text{if } B_S - \langle A_S, s\rangle \approx 0 \\ 1 & \text{if } B_S - \langle A_S, s\rangle \approx \frac{q}{2} \end{cases}$$

Security: Reduction to decision-LWE

Distinguisher for bits distinguishes LWE from random.