Lecture 27 Lattices ctd.

Recall

SVP shortest vector problem

CVP closest vector problem

Babai's Algorithm for CVP

Write $w = t_1 v_1 + \cdots + t_n v_n \notin L$

where $t_i \in \mathbb{R}$.

$v_{closest} = \text{round}(t_1) v_1 + \cdots + \text{round}(t_n) v_n$.

Only works if basis is close enough to orthogonal. How do we measure?

Recall

Prop $\det(L) = \left(\det(\langle v_i, v_j \rangle)\right)^{1/2}$.

Prop (Hadamard's inequality)

$\det(L) \leq \|v_1\| \cdots \|v_n\|$ w/ equality iff $v_1, \ldots, v_n$ orthogonal.

Def Hadamard's ratio for $\{v_1, \ldots, v_n\}$ is:

$$\left(\frac{\det(L)}{\|v_1\| \cdots \|v_n\|}\right)^{1/n} \leq 1.$$

$H \in (0,1]$, $H = 1 \iff$ orthogonal.

GGH Cryptosystem

Goldreich – Goldwasser – Halevi

Based on CVP.

Alice

Choose a good basis $v_1, \dots, v_n \in \mathbb{R}^m$ — private key

$\mathcal{H} \sim 1$.

Compute a bad basis $w_1, \dots, w_n$ of L by

$$(w_1 \dots w_n) = (v_1 \dots v_n) U$$

— public key.

$U \in GL_n(\mathbb{Z})$.

Publish $(w_1 \dots w_n)$.

Bob Plaintext $m = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \in \mathbb{F}_2^n$.

Choose random "short" vector $r \in \mathbb{R}^m$

ciphertext $c = \sum_{i=1}^{n} m_i w_i + r \notin L$.

Alice Compute $v_{closest}$ w/ Babai's algorithm:

① decompose $c = \sum a_i v_i$

② $v_{closest} = \sum \text{round}(a_i) v_i$

③ $= \sum m_i w_i$.

⇝ get message.

Disadvantages

- very large keys ~128Kb to be secure
- floats are confusing.

Example

Alice $v_1 = \begin{pmatrix} 6 \\ -1 \end{pmatrix}$ $v_2 = \begin{pmatrix} 5 \\ 29 \end{pmatrix}$ Private key

$v_1 \cdot v_2 = 1$ $\quad \gamma = \dfrac{6 \cdot 29 + 5}{\|v_1\| \, \|v_2\|} = 0.999992$

$$(w_1 \; w_2) = (v_1 v_2) U$$

$$= \begin{pmatrix} 6 & 5 \\ -1 & 29 \end{pmatrix} \begin{pmatrix} 3 & 7 \\ 2 & 8 \end{pmatrix} = \begin{pmatrix} 28 & 67 \\ 55 & 138 \end{pmatrix}$$

$\gamma(w_1, w_2) = 0.1288 \ll 1.$

Bob $m = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad r = \begin{pmatrix} 1 \\ -3 \end{pmatrix}$

$$C = m_1 w_1 + m_2 v_2 + r$$

$$= \begin{pmatrix} 28 \\ 55 \end{pmatrix} + \begin{pmatrix} 1 \\ -3 \end{pmatrix} = \begin{pmatrix} 29 \\ 52 \end{pmatrix}$$

Alice $\begin{pmatrix} 29 \\ 52 \end{pmatrix} = 3.25 \begin{pmatrix} 6 \\ -1 \end{pmatrix} + 1.91 \begin{pmatrix} 5 \\ 29 \end{pmatrix}$

$\Rightarrow \quad v_{closest} = 3\begin{pmatrix} 6 \\ -1 \end{pmatrix} + 2\begin{pmatrix} 5 \\ 29 \end{pmatrix}$

$= \begin{pmatrix} 28 \\ 55 \end{pmatrix}$

$= 1 \cdot w_1 + 0 \cdot w_2.$