Lecture 5

Tuesday, September 10, 2024 7:13 PM

Medium

$B_{bad} = \{\begin{pmatrix}6\\14\end{pmatrix}, \begin{pmatrix}3\\8\end{pmatrix}\}$

give V & L

v

$L = a\begin{pmatrix}6\\14\end{pmatrix} + b\begin{pmatrix}3\\8\end{pmatrix} = \begin{pmatrix}11.6\\4.2\end{pmatrix}$

$6a + 3b = 11.6$

$14a + 8b = 4.2$ Solve for a & b

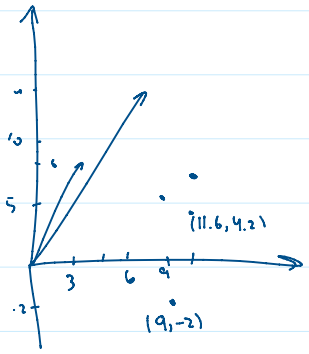
$a = 13.4, b = -22.9$

$a \approx 13, b = -23$

$a \approx 14, b = -23$

by sub a & b in L

$13\begin{pmatrix}6\\14\end{pmatrix} + -23\begin{pmatrix}3\\8\end{pmatrix} = \begin{pmatrix}9\\-2\end{pmatrix}$ $\begin{pmatrix}15\\12\end{pmatrix}$



$B_{good} = \{\begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\}$

give $v = \begin{pmatrix}11.6\\4.2\end{pmatrix}$ $a\begin{pmatrix}3\\0\end{pmatrix} + b\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}11.6\\4.2\end{pmatrix}$

$3a + 0 = 11.6 \rightarrow a = 3.86 \rightarrow a = 4$

$0 + 2b = 4.2 \rightarrow b = 2.1 \rightarrow b = 2$

$4\begin{pmatrix}3\\0\end{pmatrix} + 2\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}12\\4\end{pmatrix}$

Naïve Cryptosystem

Key

Pk in $B_{bad} = \{\begin{pmatrix}6\\14\end{pmatrix}, \begin{pmatrix}3\\8\end{pmatrix}\}$

Sk in $B_{good} = \{\begin{pmatrix}3\\0\end{pmatrix}, \begin{pmatrix}0\\2\end{pmatrix}\}$

Enc

$(h, i) = (14, -24)$

1) $14\begin{pmatrix}6\\14\end{pmatrix} - 24\begin{pmatrix}3\\8\end{pmatrix} = \begin{pmatrix}12\\4\end{pmatrix}$

2) $\vec{e} = \begin{pmatrix}-0.4\\0.2\end{pmatrix}$

3) $\begin{pmatrix}12\\4\end{pmatrix} + \vec{e} = \begin{pmatrix}11.6\\4.2\end{pmatrix}$

Dec

1) $a\begin{pmatrix}3\\0\end{pmatrix} + b\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}11.6\\4.2\end{pmatrix}$

2) $4\begin{pmatrix}3\\0\end{pmatrix} + 2\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}12\\4\end{pmatrix}$

3) $a\begin{pmatrix}6\\14\end{pmatrix}+b\begin{pmatrix}3\\8\end{pmatrix}=\begin{pmatrix}12\\4\end{pmatrix}$

$a=14,\ b=-24$

Learning with Error (LWE)

Given:

a random matrix A

a secret vector s

and an error vector e

all are defined $\mathbb{Z}_q$

$$As+e=b$$

$Ax=b$

$x=A^{-1}b$

Regev's LWE-based Cryptosystem (2005)

$As+e=b$

given A & b, it is easy to solve s?

Key gen

Secret key: a random secret vector $s\in\mathbb{Z}_q^n$

Public key: a random matrix $A\in\mathbb{Z}_q^{m\times n}$ and compute $b=As+e$ where $\vec{e}$ is small error vec

Pk is (A,b)

Sk is s

Enc

To enc. a bit $\hat{b}$, Alice

1) Chooses a random binary vector x

2) $c_1=A^T x \bmod q$

~~$c_2=b^T x+\hat{b}\lfloor q/2\rfloor \bmod q$~~ $c_2=b^T x+\hat{b}\lfloor q/2\rfloor \bmod q$

Ciphertext (c_1,c_2)

Dec Bob knows s

$\Delta=c_2-c_1^T s \bmod q$

$=b\lfloor q/2\rfloor \bmod q$

if Δ is closer to $q/2$, $b=1$; other $b=0$

Ex

$q=7,\ n=3,\ m=3$

Omark

Ex

$q=7, n=3, m=3$

Regevs

Key generation

- sk $s \in \mathbb{Z}_7^3 = [1,2,3]$
- pk is (A,b) where $A \in \mathbb{Z}_7^{3\times 3}$ and $b = As + e \bmod 7$, where $e \in \mathbb{R}^3 \bmod 1$ $e \in [0,1)$

but we will take $e \in \mathbb{Z}_7^3$, $e = [1,0,2]$

let $A = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 0 & 6 \\ 5 & 2 & 1 \end{bmatrix}$, $b = \begin{bmatrix} 2 & 1 & 3 \\ 4 & 0 & 6 \\ 5 & 2 & 1 \end{bmatrix} \times \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} = \begin{bmatrix} 13 \\ 22 \\ 12 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix} \bmod 7$

$b = \begin{bmatrix} 14 \\ 22 \\ 14 \end{bmatrix} \bmod 7 = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix}$

pk is $\left(\begin{bmatrix} 2 & 1 & 3 \\ 4 & 0 & 6 \\ 5 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \right)$ & sk is $\begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix}$

Encrypt

- To encrypt a bit $\bar{b} = 1$, choose a random binary vector $x \in \{0,1\}^3$, say $x = \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix}$
- Compute $c_1 = A^T x \bmod q = \begin{bmatrix} 2 & 4 & 5 \\ 1 & 0 & 2 \\ 3 & 6 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \bmod 7 = \begin{bmatrix} 7 \\ 3 \\ 4 \end{bmatrix} \bmod 7 = \begin{bmatrix} 0 \\ 3 \\ 4 \end{bmatrix}$
- Compute $c_2 = b^T \cdot x + \lfloor q/2 \rfloor \cdot \bar{b} \bmod 7 = [0\ 1\ 0] \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} + \lfloor 7/2 \rfloor \cdot 1 \bmod 7$

$= 0 + 4 \bmod 7 = 4$ ~~3~~

Alice sends $\left(\begin{bmatrix} 0 \\ 3 \\ 4 \end{bmatrix}, 4 \right)$

Decrypt

$\Delta = c_2 - c_1^T \cdot s \bmod q$

$c_1^T \cdot s \bmod 7 = [0\ 3\ 4] \begin{bmatrix} 1 \\ 2 \\ 3 \end{bmatrix} \bmod 7 = 18$

$\Delta = (4 - 18) \bmod 7 = (-14) \bmod 7 = 0$ ~~6~~

Since Δ is closer to 0 ~~3~~ then $\bar{b} = 0$ ~~1~~