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 $v \notin L$ $\quad v$

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

$6a+3b = 11.6$

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

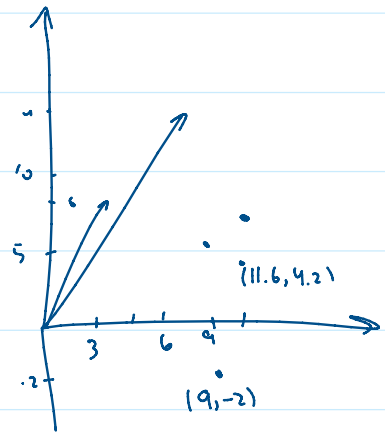
$a = 13.4, b = -22.9$

$a \approx 13, b = -23$

$a = 14, b = -23$

by sub a & b in L

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



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

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

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

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

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

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

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 $\mathbb{Z}_q$

$$As + e = b$$

$$Ax = b$$

$$x = A^{-1}b$$

$$a\begin{pmatrix}3\\0\end{pmatrix} + b\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}14\\6\end{pmatrix}$$

$$\begin{pmatrix}3 & 0\\0 & 2\end{pmatrix}\begin{pmatrix}a\\b\end{pmatrix} + \begin{pmatrix}e_1\\e_2\end{pmatrix} = \begin{pmatrix}14\\6\end{pmatrix}$$

$$Ax = b$$

Regev's LWE-based Cryptosystem

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 vector

Pk is (A, b)

Sk is s

Enc

To enc. a bit b, Alice

1) Chooses a random binary vector x

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

$c_2 = b^T x + b\lfloor q/2 \rceil \bmod q$

Ciphertext (c_1, c_2)

Dec Bob knows s

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

$\Delta = b\lfloor q/2 \rceil \bmod q$

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