Post-Quantum Cryptography

Tuesday, November 7, 2023 5:39 PM

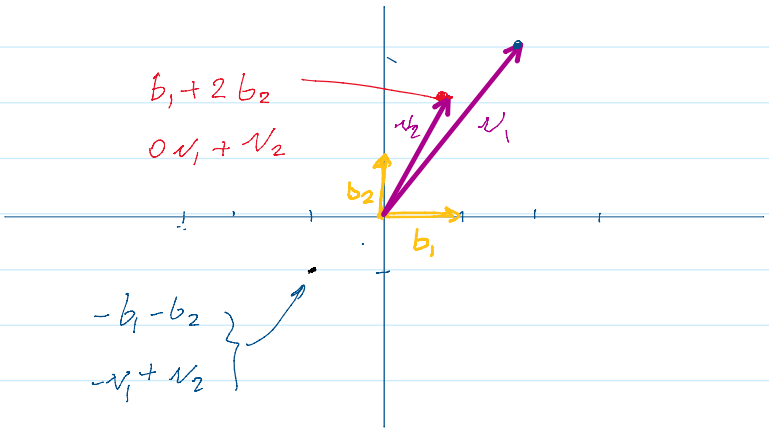
Recall: $\mathcal{L}(b_1, b_2, \ldots, b_n)$

Let $B = \begin{bmatrix} | & | & & | \\ b_1 & b_2 & \cdots & b_n \\ | & | & & | \end{bmatrix}$ } m

Then $\mathcal{L}(B) = \{Bx \mid x \in \mathbb{Z}^n\}$ | $\mathcal{L} = \underset{m \times n}{[B]} \times \underset{n \times 1}{[x]} = \underset{m \times 1}{[v]}$

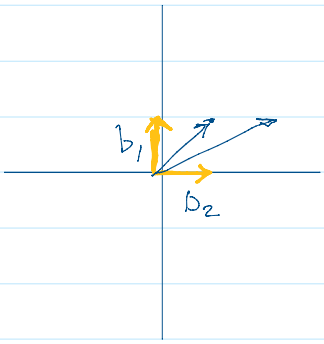
1] Note: same lattice can have different basis

e.g. $B_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and $B_2 = \begin{pmatrix} 2 & 1 \\ 3 & 2 \end{pmatrix}$ for $\mathbb{Z}^2$



2] Exer:

$B_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $B_4 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$



Is $\mathcal{L}(B_3) = \mathcal{L}(B_4)$?

3] Def^n. Given n linearly independent vectors $b_1, b_2, \ldots, b_n \in \mathbb{R}^m$

the span is defind as:

$$\mathcal{S}(b_1, b_2, \dots, b_n) = \left\{ \sum_{i=1}^{n} x_i b_i \;\middle|\; x_i \in \mathbb{R} \right\}$$

Note: $\mathcal{L}(b_1, b_2, \dots, b_n) \subset \mathcal{S}(b_1, b_2, \dots, b_n)$

4] Def^{n}. A matrix $U \in \mathbb{Z}^{n \times n}$ is unimodular if $\det(U) = \pm 1$

e.g. $U_1 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \Rightarrow \det = 2 \cdot 1 - 1 \cdot 1 = 1$

$\therefore U_1$ is unimodular

$U_2 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow \det = 2 \cdot 0 - 1 \cdot 1 = -1$

$\therefore U_2$ is unimodular.

5] Prop. if U is unimodular, then so is U^{-1}

6] Thm. Given two full rank bases $B_1, B_2 \in \mathbb{R}^{n \times n}$

Then $\mathcal{L}(B_1) = \mathcal{L}(B_2)$ iff $\exists$ a unimodular matrix U such that $B_1 \cdot U = B_2$

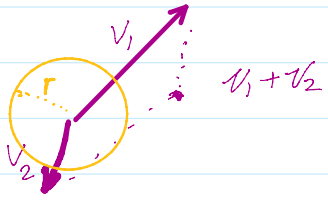
7] Post-Quantum Cryptography:

1. Quantum computers will break most of public-key crypto systems, such as: RSA, Diffie-Hellman, ElGamal.
2. We need new methods that can resist quantum attacks.
3. These methods include:
   - lattice-based cryptography.
   - Learning with error.
   - hash-based cryptography.
   - code-base

- hash - based cryptography.
- code - base crypto.

8] Lattice computational problems.

① Short Vector Problem (SVP) [optimization]
Given a Lattice $\mathcal{L}(B)$, find the shortest non-zero vector in $\mathcal{L}(B)$



[decision]

Decesion SVP : Is there any vector shorter than r?

② Closest Vector Problem (CVP)
Given a basis of $\mathcal{L}$ and $v \notin \mathcal{L}$, find the closest vector in $\mathcal{L}$ to v.

9] Learning with Error (LWE)

① In LWE, we use:
a random matrix A
a secret vector s
and an error vector e
all are defined in $\mathbb{Z}_q$

e.g. $\mathbb{Z}_{13}$

A : 7×4, $\vec{s}$: 4×1 $\vec{v} = A \cdot s$: 7×1

$$\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix} \times \begin{bmatrix} 6 \\ 9 \\ 11 \\ 11 \end{bmatrix} = \begin{bmatrix} -2+9+4+6 \\ 4+6+8-10 \\ \\ \\ \\ \\ \\ \end{bmatrix} = \begin{bmatrix} 4 \\ 8 \\ 1 \\ 10 \\ 4 \\ 12 \\ 9 \end{bmatrix}$$

(HW)

② Given A and As, the secret s can be found easily using Gaussian elimination.

③ Introducing error will make it hard to solve.

$\vec{v} = A \cdot \vec{s} + \vec{e}$ here e is an error vector (small entries)

e.g.

$$\underset{A}{\begin{bmatrix} 4 & 1 & 11 & 10 \\ 5 & 5 & 9 & 5 \\ 3 & 9 & 0 & 10 \\ 1 & 3 & 3 & 2 \\ 12 & 7 & 3 & 4 \\ 6 & 5 & 11 & 4 \\ 3 & 3 & 5 & 0 \end{bmatrix}} \times \underset{s}{\begin{bmatrix} 6 \\ 9 \\ 11 \\ 11 \end{bmatrix}} + \underset{e}{\begin{bmatrix} 0 \\ -1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}} = \underset{v = As + e}{\begin{bmatrix} 4 \\ 7 \\ 2 \\ 11 \\ 5 \\ 10 \\ 9 \end{bmatrix}}$$