Post-Quantum Cryptography

Wednesday, April 21, 2021 4:48 PM

Recall: Lattices $\mathcal{L}(B)$

1] Def^n. Given n linearly independent vectors $b_1, b_2, \dots, b_n \in \mathbb{R}^m$, their span is defined as

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

2] Note: $\mathcal{L}$ vs. $\mathcal{S}$:

for lattice, we take the integer linear combination

for the span, we take the linear combination with real coefficients.

This is crucial power of lattices

i.e. $\mathcal{L}(b_1, b_2, \dots, b_n) \subset \mathcal{S}(b_1, b_2, \dots, b_n)$

3] 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

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

5] 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 s.t. $B_1 U = B_2$

Proof: see p-5 of the handout.

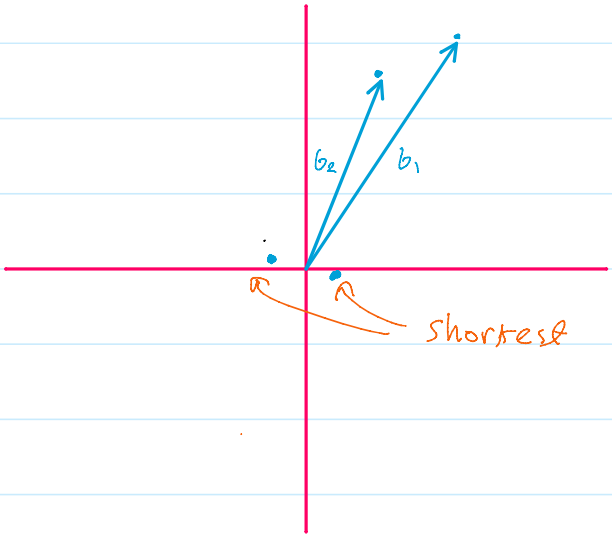
6] Post-Quantum Cryptography

- Quantum computers will crack most public-key methods, like RSA, D.H., ElGamal.
- We need new methods that define hard problems which will not be cracked by quantum computers.
- These methods include:
  1. Lattice-based Cryptography
  2. Learning with error
  3. hash-based signature.

7] Lattice Computational problem

① Shortest Vector Problem (SVP)

Given a Lattice $\mathcal{L}(B)$, find the shortest non-zero vector in $\mathcal{L}(B)$.



② Closest Vector Problem (CVP)

Given a basis of $\mathcal{L}$ and a $v \notin \mathcal{L}$, find the closest vector in $\mathcal{L}$ to v.

8] Learning With Error (LWE)

① In LWE, we use:

a random matrix A,

a secret matrix S,

and an error matrix e,

all defined in $\mathbb{Z}_n$

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

A : 7×4 , S : 4×1 AS : 7×1

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

② Given A and As, the secret S can be found easily using Gaussion elimination.

③ Introducing error will make it hard to solve.

$A \times s + e$

e.g.

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

9] Ring LWE

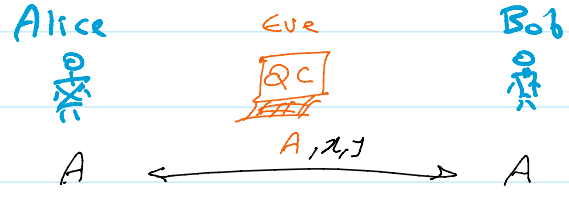
uses polynomials with coefficients from $\mathbb{Z}_n$

e.g. $\mathbb{Z}_{13}[x] / (x^4+1)$

$$A: \quad 4 + 1x + 11x^2 + 10x^3$$
$$s: \quad 6 + 9x + 11x^2 + 11x^3$$
$$e: \quad 0 - 1x + 1x^2 + 1x^3$$
$$= \quad 10 + 5x + 10x^2 + 7x^3$$

10] KE protocol using LWE

① Alice and Bob agree on random matrix A



matrix A

② Alice chooses random secret s_a

Bob chooses random secret s_b

③ A computes $A s_a + e_a$

B Computes $A s_b + e_b$

where e_a and e_b are error matrices

④ A compute: key = $s_a \cdot y$

$= s_a (A s_b + e_b)$

B computes: key = $s_b \cdot x$

$= s_b (A s_a + e_a)$

⑤ use probabilistic encryption to remove errors

shared key = $A s_a s_b = A s_b s_a$