LWE Public-key schemes

Tuesday, November 28, 2023 5:28 PM

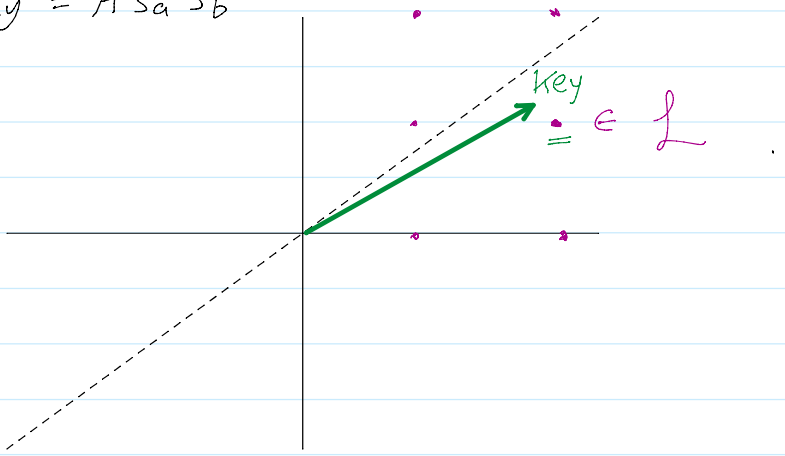
Recall: LWE

1] Key Exchange Protocol (using LWE)

	Alice	Bob
① Alice and Bob agree on A	① A	A
② Alice chooses random secret s_a, Bob chooses " " s_b	② s_a	s_b
③	③ $As_a + e_a$ → x	$As_b + e_b$ → y
④	④ Key: $(As_b + e_b)\, s_a = As_b \cdot s_a + e_b \cdot s_a$	Key: $(As_a + e_a) \cdot s_b = As_a \cdot s_b + e_a \cdot s_b$
	$\Rightarrow$ Key $= As_a \cdot s_b + e$	

⑤ Use a probabilistic algorithm to remove the error.

$\Rightarrow$ Shared key $= As_a s_b$



2] LWE Public-key cryptosystem

Setup:

① Alice and Bob choose a random public $m \times n$ matrix A in $\mathbb{Z}_q^{m \times n}$

$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \end{bmatrix}$

① Alice and Bob choose a random public $m \times n$ matrix A in $\mathbb{Z}_q^{m \times n}$

② Alice chooses a private binary vector $\vec{x} \in \mathbb{Z}_2^m$ and computes public $\vec{u} = A\vec{x}$ (public-key)

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & \\ \vdots & & & \\ a_{m1} & \cdots & \cdots & a_{mn} \end{bmatrix}$$

$\vec{u} = A$

Encryption

① Bob chooses random secret $\vec{s}$ and private error vectors $\vec{e_1}$ and $\vec{e_2}$

② To send a message $M = (d_1 d_2 \cdots d_k)_2$

$\vec{b_1} = A\vec{s} + \vec{e_1}$

$\vec{b_2} = \vec{s} \cdot \vec{u} + \vec{e_2} + d_i \cdot (\frac{q}{2})$; $d_i \in \{0,1\}$, $\vec{e} << \frac{q}{4}$

Decryption

① to finds if d_i was 1 or 0 :

Alice computes:

$$\vec{b_1} \cdot \vec{x} = (A\vec{s} + \vec{e_1})\vec{x} = \vec{s} \cdot \vec{u} + \vec{e_1} \cdot \vec{x}$$

$$\vec{b_2} - \vec{b_1}\vec{x} = \vec{s} \cdot \vec{u} + \vec{e_2} + d_i (\frac{q}{2}) - \vec{s} \cdot \vec{u} + \vec{e_1} \cdot \vec{x}$$

$$(e_2 - \vec{e_1} \cdot \vec{x}) + d_i(\frac{q}{2})$$

($e_2 - \vec{e_1} \cdot \vec{x}$: very small; $d_i(\frac{q}{2})$: only small if $d_i = 0$)

If $\vec{b_2} - \vec{b_1}\vec{x}$ is small then $d_i = 0$

Else, $d_i = 1$

3] Note.

The hardness of this cryptosyste is based on the hardness of LWE (and CVP)