

CSCI 1515 Applied Cryptography

This Lecture:

- Post-Quantum Assumption : Learning With Errors (Continued)
- Regev Encryption
- SWHE from RLWE (BFV)

Post-Quantum Assumption: Learning With Errors (LWE)

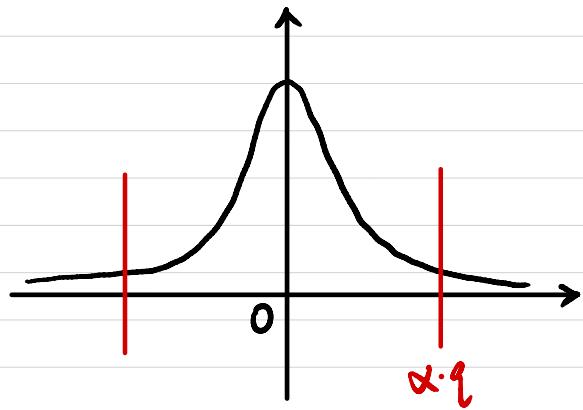
n : security parameter

$$q \sim 2^{n^t}$$

$$m = \Omega(n \log q)$$

χ : distribution over \mathbb{Z}_q

(concentrated on "small integers")



$$\Pr[|e| < \alpha \cdot q \mid e \in \chi] \approx 1$$

\uparrow
 $\alpha \ll 1$

LWE $[n, m, q, \chi]$:

$$A \in \mathbb{Z}_q^{m \times n} \quad s \in \mathbb{Z}_q^n \quad e \in \chi^m$$

$$\begin{array}{c|c|c|c|c} A & \times & s_{n \times 1} & + & e_{m \times 1} \\ \hline m \times n & & & & m \times 1 \\ \hline & & & & \end{array} = \begin{array}{|c|c|c|c} b & & & \\ \hline m \times 1 & & & \end{array}$$

$$(A, b = As + e) \stackrel{\epsilon}{\sim} (A, b' \in \mathbb{Z}_q^m)$$

$$\begin{array}{c|c} A & \\ \hline m \times n & \end{array}$$

$$\begin{array}{|c|c} b' & \in \mathbb{Z}_q^m \\ \hline m \times 1 & \end{array}$$

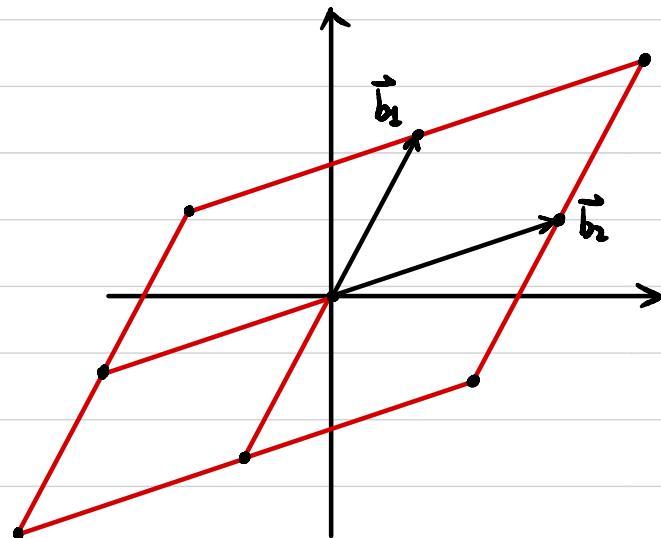
Lattice-Based Crypto

Given a lattice of dimension n :

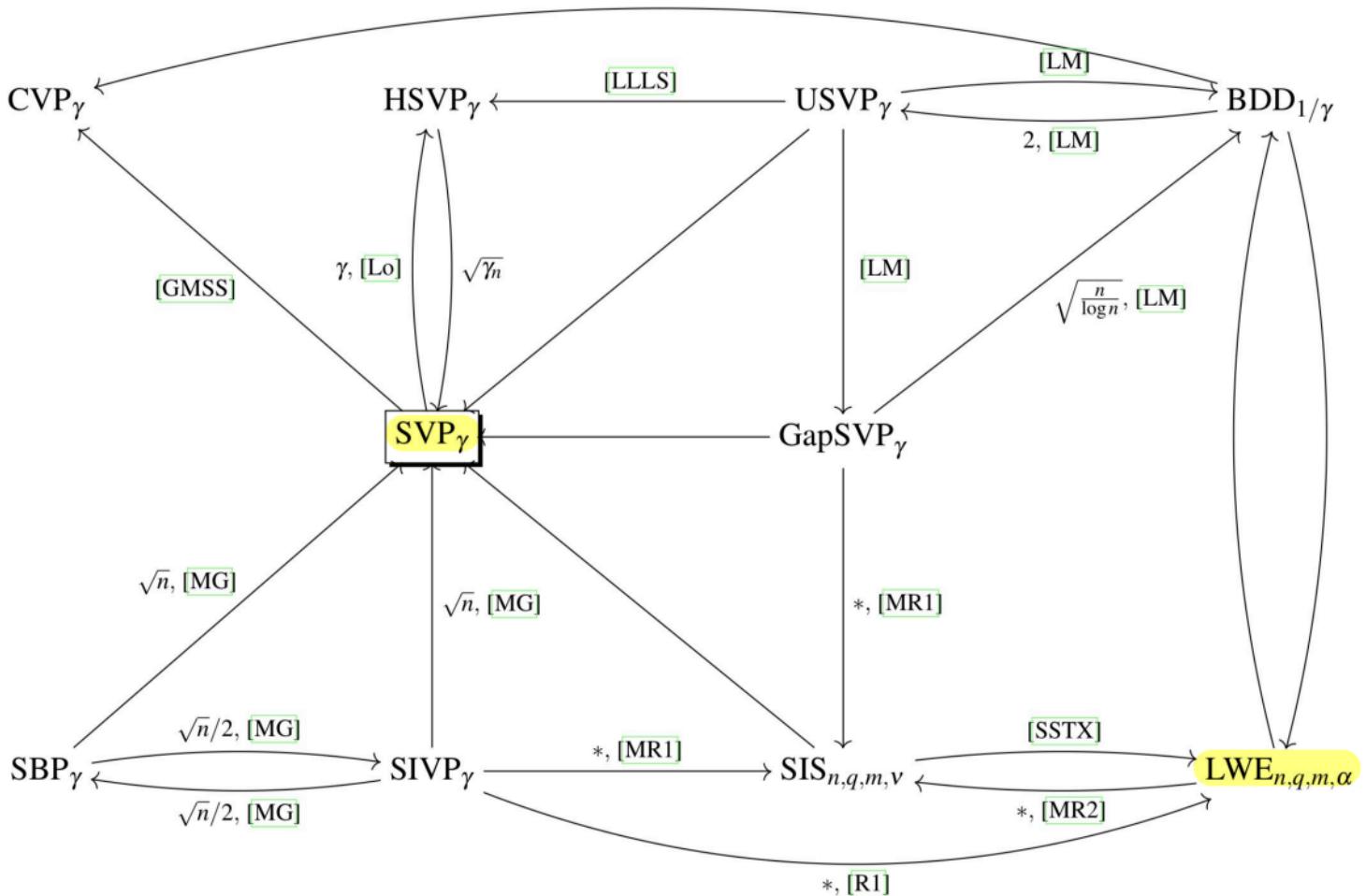
Basis $B = \{\vec{b}_1, \vec{b}_2, \dots, \vec{b}_n\}$, linearly independent

Lattice $L(B) := \left\{ \sum_{i=1}^n \alpha_i \vec{b}_i \mid \alpha_i \in \mathbb{Z} \right\}$

Shortest Vector Problem (SVP): Find the shortest vector in L .



worst-case hardness $\xrightarrow{\text{reduce}}$ average-case hardness



Post-Quantum Encryption: Regev

- $\text{Gen}(1^n)$:

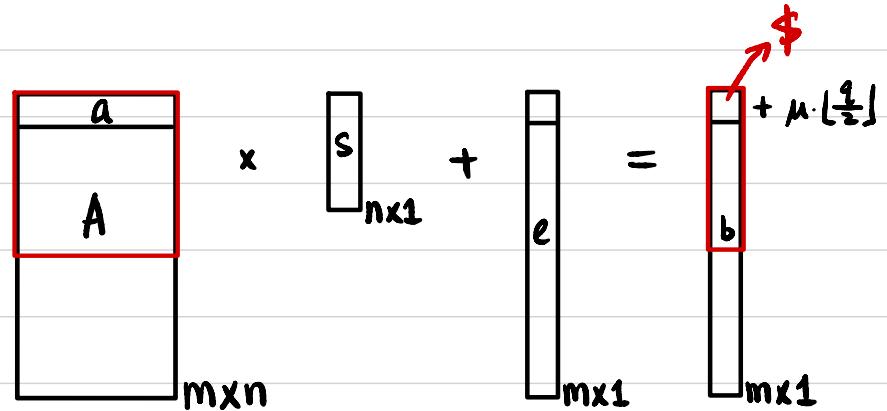
$$\vec{s} \leftarrow \mathbb{Z}_q^n$$

Output $\text{sk} = \vec{s}$

- $\text{Enc}_{\text{sk}}(\mu)$: $\mu \in \{0, 1\}$

$$\vec{a} \leftarrow \mathbb{Z}_q^n \quad e \leftarrow X$$

$$c = (\vec{a}, \langle \vec{a}, \vec{s} \rangle + e + \mu \cdot \lfloor \frac{q}{2} \rfloor)$$



- $\text{Dec}_{\text{sk}}(c)$: $c = \boxed{a} \mid \boxed{z}$

$$z - \langle \vec{a}, \vec{s} \rangle = e + \mu \cdot \lfloor \frac{q}{2} \rfloor$$

(CPA) Security?

Additive Homomorphism?

$$c_1 = (\vec{a}_1, \langle \vec{a}_1, \vec{s} \rangle + e_1 + \mu_1 \cdot \lfloor \frac{q}{2} \rfloor)$$

$$c_2 = (\vec{a}_2, \langle \vec{a}_2, \vec{s} \rangle + e_2 + \mu_2 \cdot \lfloor \frac{q}{2} \rfloor)$$

$$\rightarrow (\vec{a}_1 + \vec{a}_2, \langle \vec{a}_1 + \vec{a}_2, \vec{s} \rangle + (e_1 + e_2) + (\mu_1 + \mu_2) \cdot \lfloor \frac{q}{2} \rfloor)$$

Public-Key?

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from RLWE (BFV)

Step 2: Bootstrapping

Ring LWE (RLWE) Assumption

Polynomial ring $R = \mathbb{Z}[x] / (x^m + 1)$

$m = 2^k$

polynomials with integer coefficients modulo $(x^m + 1)$

$R_q = \mathbb{Z}_q[x] / (x^m + 1)$

polynomials with integer coefficients modulo q and $(x^m + 1)$

Def A ring is a set R with two binary operations $+$, \cdot satisfying:

① R is an abelian group under " $+$:

- $\forall a, b \in R, a+b \in R$
- $\forall a, b, c \in R, (a+b)+c = a+(b+c)$
- $\exists 0 \in R$ s.t. $\forall a \in R, a+0=a$
- $\forall a \in R, \exists -a \in R$ s.t. $a+(-a)=0$.
- $\forall a, b \in R, a+b=b+a$

② R is a monoid under " \cdot :

- $\forall a, b \in R, a \cdot b \in R$
- $\forall a, b, c \in R, (a \cdot b) \cdot c = a \cdot (b \cdot c)$
- $\exists 1 \in R$ s.t. $\forall a \in R, a \cdot 1 = 1 \cdot a = a$.

③ " \cdot " is distributive w.r.t. " $+$:

- $\forall a, b, c \in R, a \cdot (b+c) = a \cdot b + a \cdot c$
- $\forall a, b, c \in R, (a+b) \cdot c = a \cdot c + b \cdot c$

Ring LWE (RLWE) Assumption

Polynomial ring $R = \mathbb{Z}[x] / (x^m + 1)$

$$R_q = \mathbb{Z}_q[x] / (x^m + 1)$$

polynomials with integer coefficients modulo $(x^m + 1)$

χ : "noise" distribution over R

$$a \in R_q \quad s \in R_q \text{ (or } s \in \chi\text{)} \quad e \in \chi$$

$$(a, [a \cdot s + e]_q) \stackrel{\sim}{=} (a, b \in R_q)$$

SWHE from RLWE (BFV)

Plaintext space $R_t = \mathbb{Z}_t[x] / (x^m + 1)$

Ciphertext space $R_q \times R_q$

$$\Delta := \left\lfloor \frac{q}{t} \right\rfloor \quad t \ll q$$

$a \leftarrow R_q \quad s \leftarrow X \quad e \leftarrow X$

$$pk = \left([-(a \cdot s + e)]_q, a \right)$$

sk = s

$\text{Enc}_{pk}(m) : m \in R_t$

Sample $u, e_1, e_2 \leftarrow X$

$$c = \left([pk_0 \cdot u + e_1 + \Delta \cdot m]_q, [pk_1 \cdot u + e_2]_q \right)$$

$\text{Dec}_{sk}(c) : [c_0 + c_1 \cdot s]_q = [-(a \cdot s + e) \cdot u + e_1 + \Delta \cdot m + (a \cdot u + e_2) \cdot s]_q$
 $= [\Delta \cdot m + \text{error}]_q$

SWHE from RLWE (BFV)

$$[C(s)]_q = c_0 + c_1 \cdot s = \Delta \cdot m + e$$

Homomorphism: $[C^{(1)}(s)]_q = \Delta \cdot m_1 + e_1$

$$[C^{(2)}(s)]_q = \Delta \cdot m_2 + e_2$$

Additive Homomorphism?

$$[C^{(1)}(s) + C^{(2)}(s)]_q = [\Delta \cdot (m_1 + m_2) + e_1 + e_2]_q$$

Multiplicative Homomorphism?

$$\begin{aligned} C(s) &= C^{(1)}(s) \cdot C^{(2)}(s) \\ &= (\Delta \cdot m_1 + e_1 + \alpha_1 \cdot q) \cdot (\Delta \cdot m_2 + e_2 + \alpha_2 \cdot q) \\ &= \underline{\Delta^2 \cdot m_1 m_2 + \Delta m_1 e_2 + \Delta m_1 \cdot \alpha_2 q + e_1 \cdot \Delta m_2 + e_1 e_2 + e_1 \alpha_2 q + \alpha_1 q \cdot \Delta m_2 + \alpha_1 q \cdot e_2 + \alpha_1 \alpha_2 q^2} \end{aligned}$$

WANT: $\Delta \cdot m_1 m_2 + \text{small}$

$$\Delta = \left\lfloor \frac{q}{t} \right\rfloor$$

SWHE from RLWE (BFV)

$$[C(s)]_q = c_0 + c_1 \cdot s + c_2 \cdot s^2 = \Delta \cdot m + e$$

\downarrow

$$[c'(s)]_q = c'_0 + c'_1 \cdot s = \Delta \cdot m + e$$

Relinearization:

$$\text{Relinearization key: } \text{rlk} = \left([-(a \cdot s + e + s^2)]_q, a \right)$$

$$[\text{rlk}(s)]_q = -s^2 + \text{small}$$

$$C(s) + c_2 \cdot \text{rlk}(s) = c_0 + c_1 \cdot s + \cancel{c_2 \cdot s^2} + c_2 \cdot (-s^2 + \text{small})$$

\uparrow
 $\sum \text{rlk}_i(s) \cdot c_2[i]$

\uparrow
large

$$\text{rlk}_i = \left([-(a \cdot s + e + z^i \cdot s^2)]_q, a \right)$$

$$[\text{rlk}_i(s)]_q = -z^i \cdot s^2 + \text{small}$$