

CSCI 1515 Applied Cryptography

This Lecture:

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

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers

- from RLWE (BFV)

Step 2: Bootstrapping

SWHE over Integers

$$p \sim 2^{O(\lambda^2)}, \quad q_i \sim 2^{O(\lambda^5)}, \quad e_i \sim 2^{O(\lambda)}$$

Attempt 2 (Secret-key)

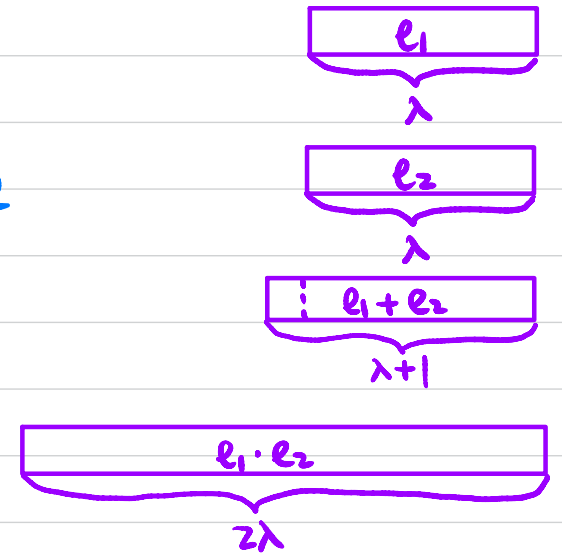
- secret key: odd number p

- Enc(m): $m \in \{0, 1\}$

Sample a random q . Sample a random $e \ll p$ noise

Output $ct = p \cdot q + m + ze$

Encryption of 0 is small and even modulo p .



- Dec(ct): $[ct \bmod p] \bmod 2$

- Eval ADD: $ct \leftarrow ct_1 + ct_2$ (ADD mod 2) ← XOR

- Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$ (MULT mod 2) ← AND

$$ct_1 = p \cdot q_1 + m_1 + ze_1$$

$$ct_2 = p \cdot q_2 + m_2 + ze_2$$

Why is it homomorphic?

$$ct_1 + ct_2 = p \cdot (q_1 + q_2) + (m_1 + m_2) + z(e_1 + e_2)$$

(CPA) Security?

$$ct_1 \cdot ct_2 = p \cdot (\dots) + z \cdot (\dots) + m_1 \cdot m_2$$

$$= p \cdot (q_1 q_2 \cdot p + q_1 m_2 + q_2 m_1 + z e_1 + z e_2)$$

$$+ z(e_1 m_2 + e_2 m_1 + z e_1 e_2) + m_1 \cdot m_2$$

How homomorphic is it?

$O(\lambda)$ MULT/AND

Approximate GCD Problem

Given polynomially many $\{x_i = p \cdot q_i + s_i\}$, find p .

Example parameters:

$$p \sim 2^{O(\lambda^2)}, \quad q_i \sim 2^{O(\lambda^5)}, \quad s_i \sim 2^{O(\lambda)}$$

Best known algorithms take $\sim 2^\lambda$ time

SWHE over Integers

Attempt 3 (public-key)

- secret key: odd number p

public key: "encryptions of 0" ← generic

$$\{x_i = p \cdot q_i + z e_i\}_{i \in [\lambda]}$$

- Enc(m): $m \in \{0, 1\}$

Sample a random $e \ll p$

Output $ct = (\text{random subset sum of } x_i\text{'s}) + m + ze$

Encryption of 0 is small and even modulo p .

- Dec(ct): $[ct \bmod p] \bmod 2$

- Eval ADD: $ct \leftarrow ct_1 + ct_2$

Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

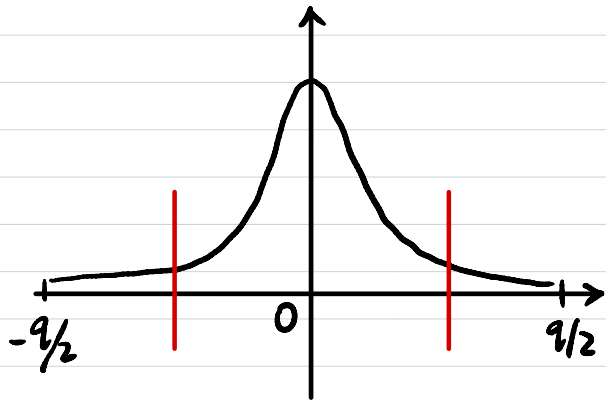
Post-Quantum Assumption: Learning With Errors (LWE)

n : security parameter

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

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

χ : distribution over \mathbb{Z}_q
(concentrated on "small integers")



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

↑
 $\alpha \ll 1$

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

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

$$\begin{matrix} \boxed{A} & \times & \boxed{s} & + & \boxed{e} & = & \boxed{b} \\ & & \text{nx1} & & \text{mx1} & & \text{mx1} \\ & & & & & & \text{mxn} \end{matrix}$$

$$(A, b = As + e) \stackrel{c}{\approx} (A, b' \leftarrow \mathbb{Z}_q^m)$$

$$\begin{matrix} \boxed{A} & & \boxed{b'} \\ & & \leftarrow \mathbb{Z}_q^m \\ & & \text{mx1} \\ & & \text{mxn} \end{matrix}$$

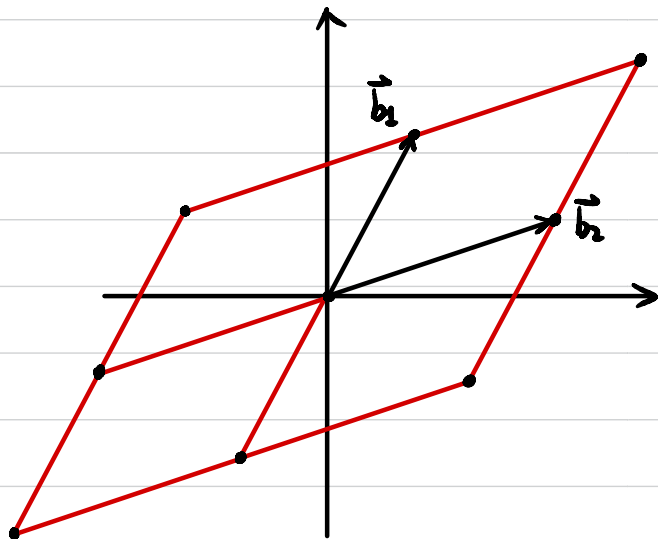
Lattice-Based Crypto

Given a **lattice** of dimension n :

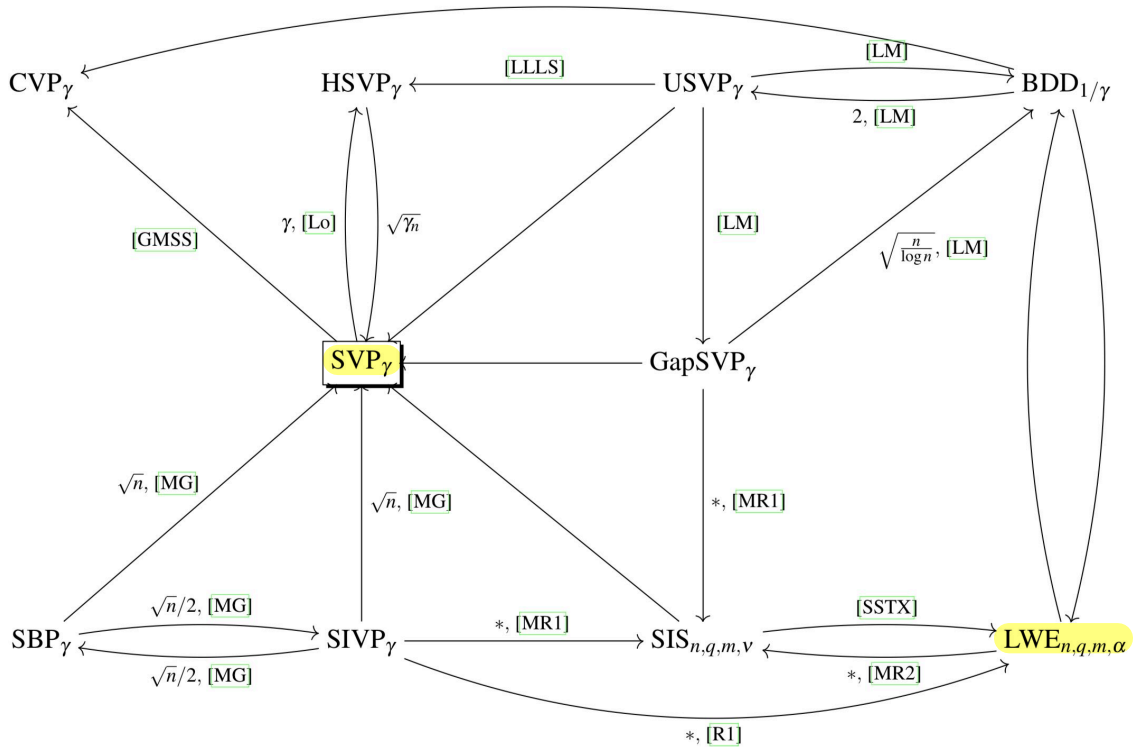
Basis $B = \{ \vec{b}_1, \vec{b}_2, \dots, \vec{b}_n \}$, linearly independent

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

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



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



Post-Quantum Encryption: Regev

• Gen(1^n):

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

Output $sk = \vec{s}$

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

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

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

n : security parameter
 $q \sim 2^{n^\epsilon}$
 $m = \Omega(n \log q)$
 \mathcal{X} : distribution over \mathbb{Z}_q
(concentrated on "small integers")

$$\begin{matrix} a \\ \hline A \\ \hline \end{matrix}_{m \times n} \times \begin{matrix} s \\ \hline \end{matrix}_{n \times 1} + \begin{matrix} e \\ \hline \end{matrix}_{m \times 1} = \begin{matrix} a \\ \hline b \\ \hline \end{matrix}_{m \times 1} + \mu \cdot \lfloor \frac{q}{2} \rfloor$$

• Dec $_{sk}(c)$: $c = \begin{bmatrix} a \\ \hline z \end{bmatrix}$

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

(CPA) Security?

Additive Homomorphism?

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

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

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

Public-Key?

Ring LWE (RLWE) Assumption

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

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

$m = 2^k$

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

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

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

χ : "noise" distribution over R

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

$$(a, [a \cdot s + e]_q) \stackrel{c}{\approx} (a, b \leftarrow R_q)$$

SWHE from RLWE (BFV)

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

Ciphertext space $R_q \times R_q$

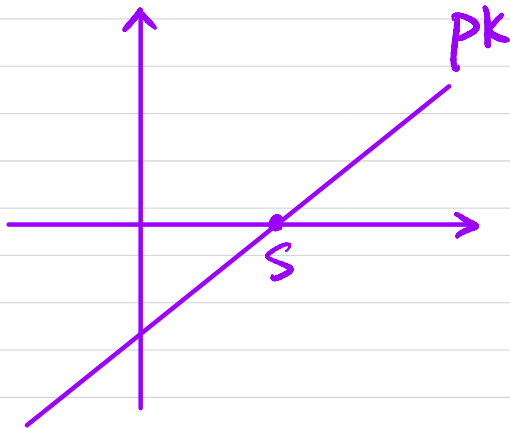
Gen:

Sample $a \leftarrow \mathbb{Z}_q$, $s, e \leftarrow \mathcal{X}$

$sk = s$

$pk = ([-(a \cdot s + e)]_q, a)$
 $= (pk_0, pk_1)$

$$[pk(s)]_q = pk_0 + pk_1 \cdot s = e \approx 0$$



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

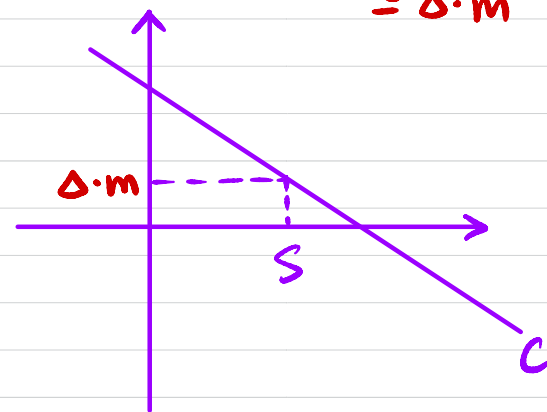
Enc_{pk}(m): $m \in R_t$

Sample $u, e_1, e_2 \leftarrow \mathcal{X}$

$c = ([pk_0 \cdot u + e_1 + \Delta \cdot m]_q,$
 $[pk_1 \cdot u + e_2]_q)$
 $= (c_0, c_1)$

$$[c(s)]_q = c_0 + c_1 \cdot s = -e \cdot u + e_1 + e_2 \cdot s + \Delta \cdot m$$

$\approx \Delta \cdot m$



Dec_{sk}(c) ? $c_0 + c_1 \cdot s \rightarrow \Delta \cdot m + \text{error}$

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?

Multiplicative Homomorphism?

