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

Attempt 2 (secret-key)

- secret key: odd number p
- $\mathrm{Enc}(m)$: $m \in \{0,1\}$

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

  Output $ct = p \cdot q + m + 2e$

  Encryption of 0 is small and even modulo p.

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

$ct_1 = p \cdot q_1 + m_1 + 2e_1$

$ct_2 = p \cdot q_2 + m_2 + 2e_2$

Why is it homomorphic?

$ct_1 + ct_2 = p \cdot (q_1 + q_2) + (m_1 + m_2) + 2(e_1 + e_2)$

(CPA) Security?

$ct_1 \cdot ct_2 = p \cdot (\cdots) + 2 \cdot (\cdots) + m_1 \cdot m_2$

How homomorphic is it?

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

  $\{x_i = p \cdot q_i + 2e_i\}_{i \in [\lambda]}$

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

  Sample a random $e \ll p$

  Output $ct = (\text{random subset sum of } x_i\text{'s}) + m + 2e$

  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: $ct \leftarrow ct_1 \cdot ct_2$

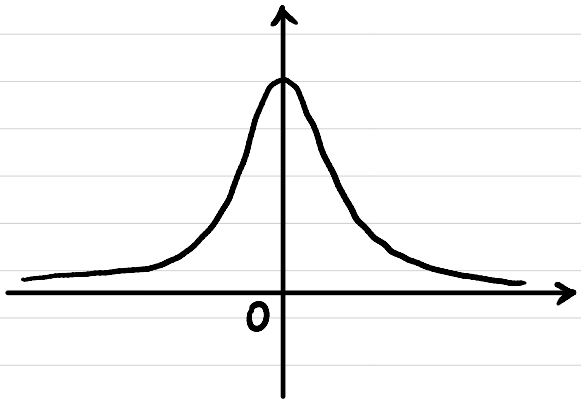
Post-Quantum Assumption: Learning With Errors (LWE)

n: security parameter

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

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

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

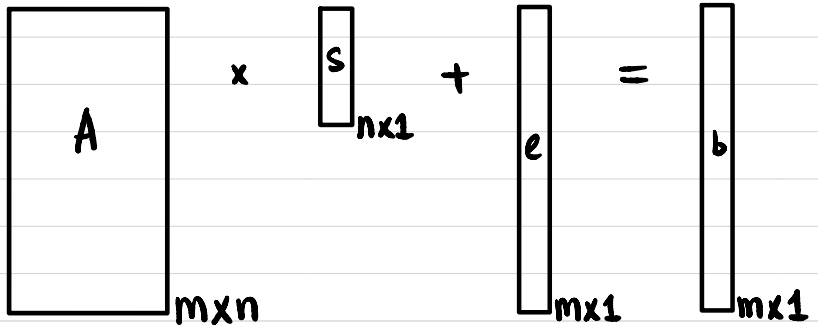


$$\Pr[|e| < \alpha \cdot q \mid e \leftarrow \chi] \simeq 1$$

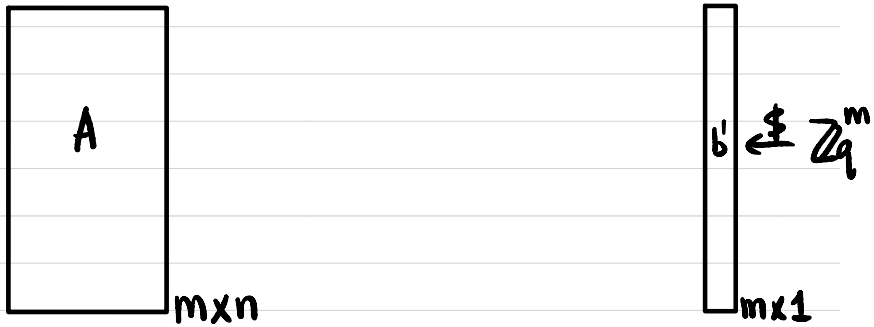
$\alpha \ll 1$

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

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



$$(A,\ b = As + e) \overset{c}{\simeq} (A,\ b' \xleftarrow{\$} \mathbb{Z}_q^m)$$



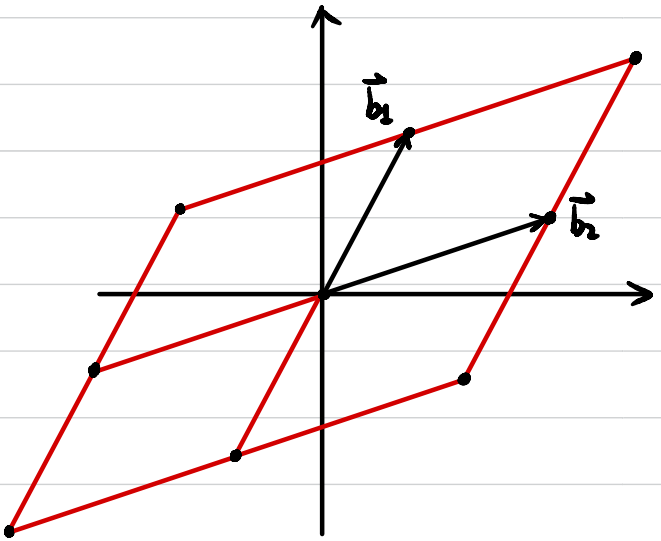
Lattice-Based Crypto

Given a **lattice** of dimension n:

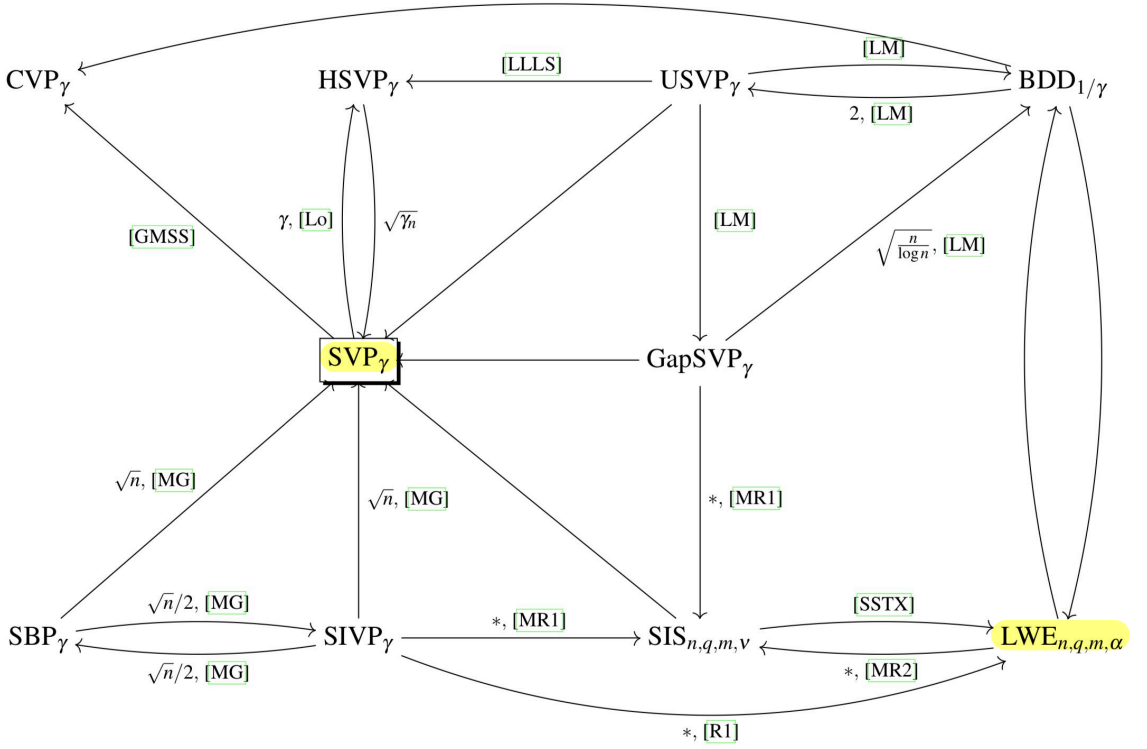
Basis $B = \{ \vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n \}$, linearly independent

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


CVP_γ
HSVP_γ
[LLLS]
USVP_γ
[LM]
2, [LM]
$\mathrm{BDD}_{1/\gamma}$
[GMSS]
γ, [Lo]
$\sqrt{\gamma_n}$
[LM]
$\sqrt{\frac{n}{\log n}}$, [LM]
SVP_γ
GapSVP_γ
$\sqrt{n}$, [MG]
$\sqrt{n}$, [MG]
$*$, [MR1]
$\sqrt{n}/2$, [MG]
$\sqrt{n}/2$, [MG]
SBP_γ
SIVP_γ
$*$, [MR1]
$\mathrm{SIS}_{n,q,m,\nu}$
[SSTX]
$*$, [MR2]
$\mathrm{LWE}_{n,q,m,\alpha}$
$*$, [R1]

Post-Quantum Encryption: Regev

- $Gen(1^n)$:

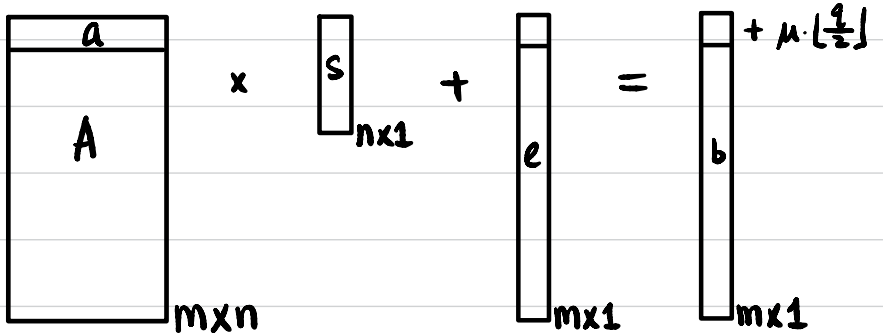
  $\vec{s} \xleftarrow{\$} \mathbb{Z}_q^n$

  Output $sk = \vec{s}$

- $Enc_{sk}(\mu)$: $\mu \in \{0,1\}$

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

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



- $Dec_{sk}(c)$: $c =$ [a | z]

  $z - \langle \vec{a}, \vec{s} \rangle = ?$

(CPA) Security?

Additive Homomorphism?

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

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

Public-key?

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 $R = \mathbb{Z}[x] / (x^m + 1)$ where $m = 2^k$

↑ 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

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

$$(a,\ [a \cdot s + e]_q) \overset{c}{\simeq} (a,\ b \xleftarrow{\$} R_q)$$

SWHE from RLWE (BFV)

Plaintext space $R_t = \mathbb{Z}_t[x]/(x^m+1)$ $\quad \Delta := \lfloor \frac{q}{t} \rfloor$ $\quad t \ll q$

Ciphertext space $R_q \times R_q$

Gen:

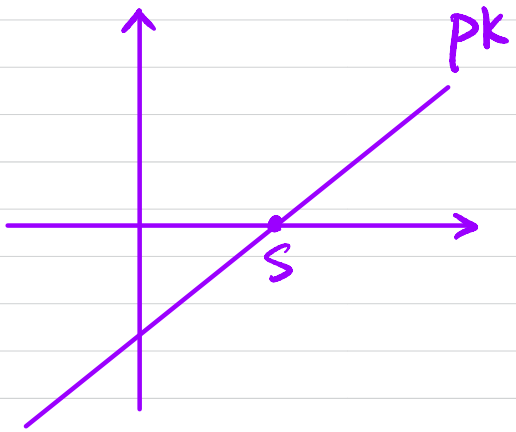
Sample $a \xleftarrow{\$} R_q$ $\quad s, e \leftarrow \chi$

$sk = s$

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

$= (pk_0, pk_1)$

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



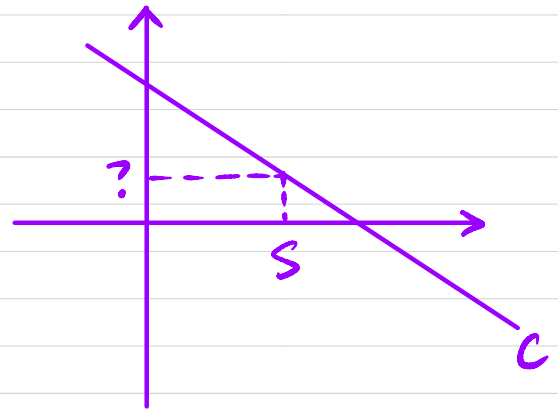
$Enc_{pk}(m)$: $m \in R_t$

Sample $u, e_1, e_2 \leftarrow \chi$

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

$= (c_0, c_1)$

$[c(s)]_q = c_0 + c_1 \cdot s \simeq ?$



$Dec_{sk}(c)$?

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?