CSCI 1515 Applied Cryptography

This Lecture:

- Introduction to Fully Homomorphic Encryption
- Somewhat Homomorphic Encryption over Integers
- Post-Quantum Assumption: Learning With Errors

Homomorphic Encryption

So far, encryption schemes:

$$ct \leftarrow Enc(x)$$

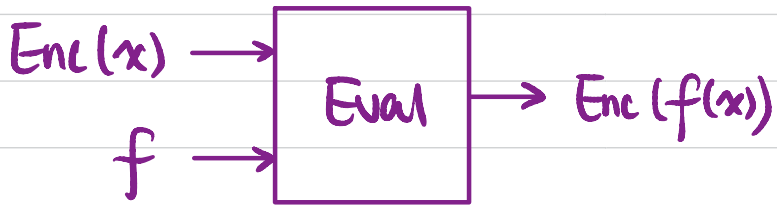
$$x \leftarrow Dec_{sk}(ct)$$

All-or-Nothing:

w/ sk $\rightarrow$ x

w/o sk $\rightarrow$ Nothing

Homomorphic Evaluation:



Fully Homomorphic Encryption (FHE)

$Enc(m_1)$ → $Enc(m_1 + m_2)$ ← $Enc(m_2)$

Additively Homomorphic

↑

Exponential ElGamal / Pallier / Regev

$Enc(m_1)$ → $Enc(m_1 \cdot m_2)$ ← $Enc(m_2)$

Multiplicatively Homomorphic

↑

RSA / ElGamal

Fully Homomorphic: Additively & Multiplicatively Homomorphic

Application: Outsourcing Storage & Computation

Server

Client

Data x

Key sk

$ct \leftarrow Enc(x)$

ct

f

$ct' \leftarrow Eval(f, ct)$

ct'

$f(x) \leftarrow Dec_{sk}(ct')$

Application: Privacy-Preserving Query

Server

Client

Query x

Key sk

$ct \leftarrow Enc(x)$

ct

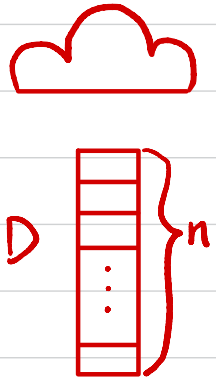
Search / ML / GPT / ...

$ct' \leftarrow Eval(f, ct)$

ct'

$f(x) \leftarrow Dec_{sk}(ct')$

Application: Private Information Retrieval (PIR)



WANT: D[i]

While hiding i against Server

Query i

Key sk

$ct \leftarrow Enc(i)$

ct ←

$ct' \leftarrow Eval(f, ct)$

↑

?

ct' →

$D[i] \leftarrow Dec_{sk}(ct')$

Fully Homomorphic Encryption (FHE)

- **Syntax:** A (public-key) homomorphic encryption scheme $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ w.r.t. function family $\mathcal{F}$:
  - $(pk, sk) \leftarrow \mathsf{Gen}(1^\lambda)$
  - $ct \leftarrow \mathsf{Enc}_{pk}(m) \quad m \in \{0,1\}$
  - $m \leftarrow \mathsf{Dec}_{sk}(ct)$
  - $ct_f \leftarrow \mathsf{Eval}(f, ct_1, \cdots, ct_n) \quad f: \{0,1\}^n \to \{0,1\}$

- **Correctness:** $\forall f \in \mathcal{F}, \quad \forall m_1, m_2, \cdots, m_n \in \{0,1\}$

  $\forall i \in [n], \; ct_i \leftarrow \mathsf{Enc}_{pk}(m_i), \quad ct_f \leftarrow \mathsf{Eval}(f, ct_1, \cdots, ct_n).$

  $\mathsf{Dec}_{sk}(ct_f) = f(m_1, \cdots, m_n)$

- **(CPA) Security:** $(pk, \mathsf{Enc}_{pk}(m_0)) \overset{c}{\approx} (pk, \mathsf{Enc}_{pk}(m_1))$.

- **Compactness:** $|ct_f| \leq$ fixed poly (λ) ← Why do we need this?

  Independent of circuit size of f.

- If $\mathcal{F}$ contains **all** poly-sized Boolean circuits, then Π is **fully** homomorphic.

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from RLWE (BFV)

Step 2: Bootstrapping

SWHE over Integers

Attempt 1 (secret-key)

- secret key: odd number p ← Why odd?
- $\mathrm{Enc}(m)$: $m \in \{0,1\}$
  Sample a random q.
  Output $ct = p \cdot q + m$
  Encryption of 0 is a multiple of p.
- $\mathrm{Dec}(ct)$: $ct \bmod p$
- Eval ADD: $ct \leftarrow ct_1 + ct_2$
  Eval MULT: $ct \leftarrow ct_1 \cdot ct_2$

Why is it homomorphic?

(CPA) Security?

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: $ct \leftarrow ct_1 + ct_2$

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

Why is it homomorphic?

(CPA) Security?

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: $ct \leftarrow ct_1 \cdot ct_2$

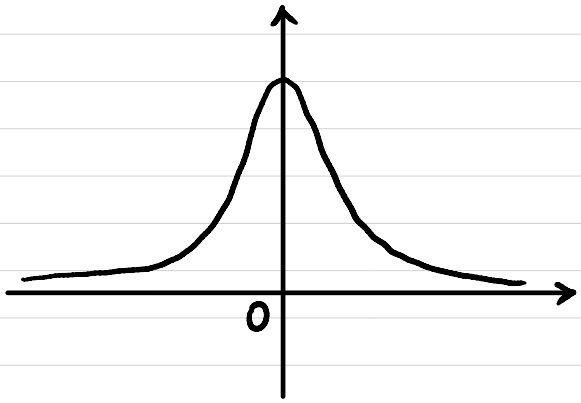
Post-Quantum Assumption: Learning With Errors (LWE)

n: security parameter

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

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

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

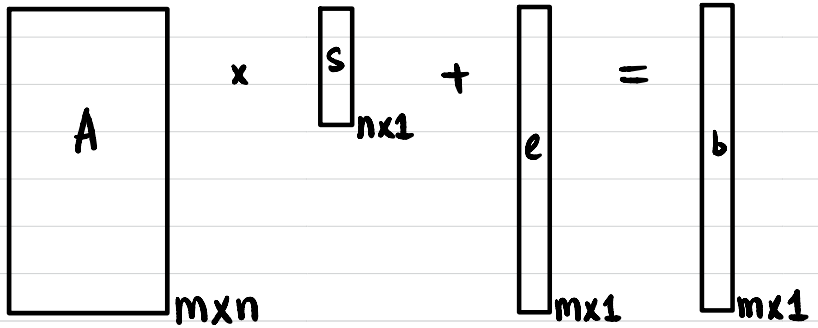


$$\Pr[|e| < \alpha \cdot q \mid e \leftarrow \chi] \simeq 1$$

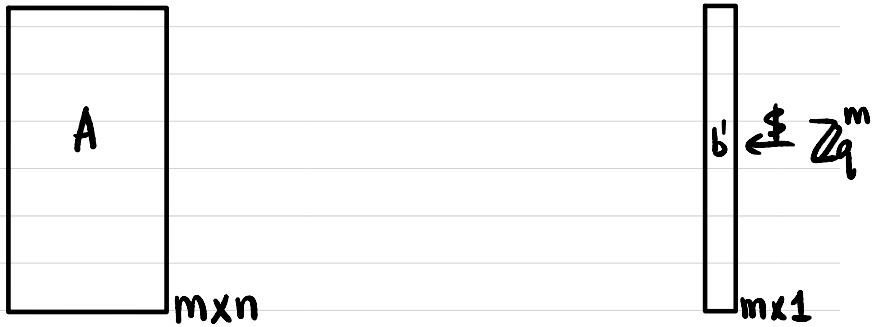
$\alpha \ll 1$

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

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



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



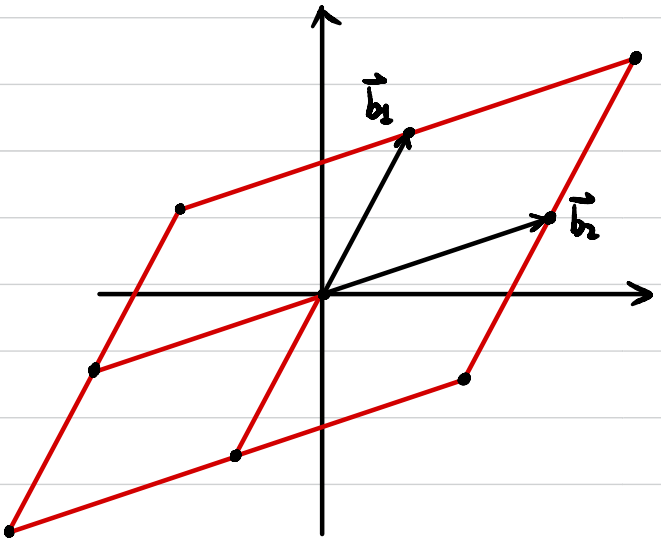
Lattice-Based Crypto

Given a **lattice** of dimension n:

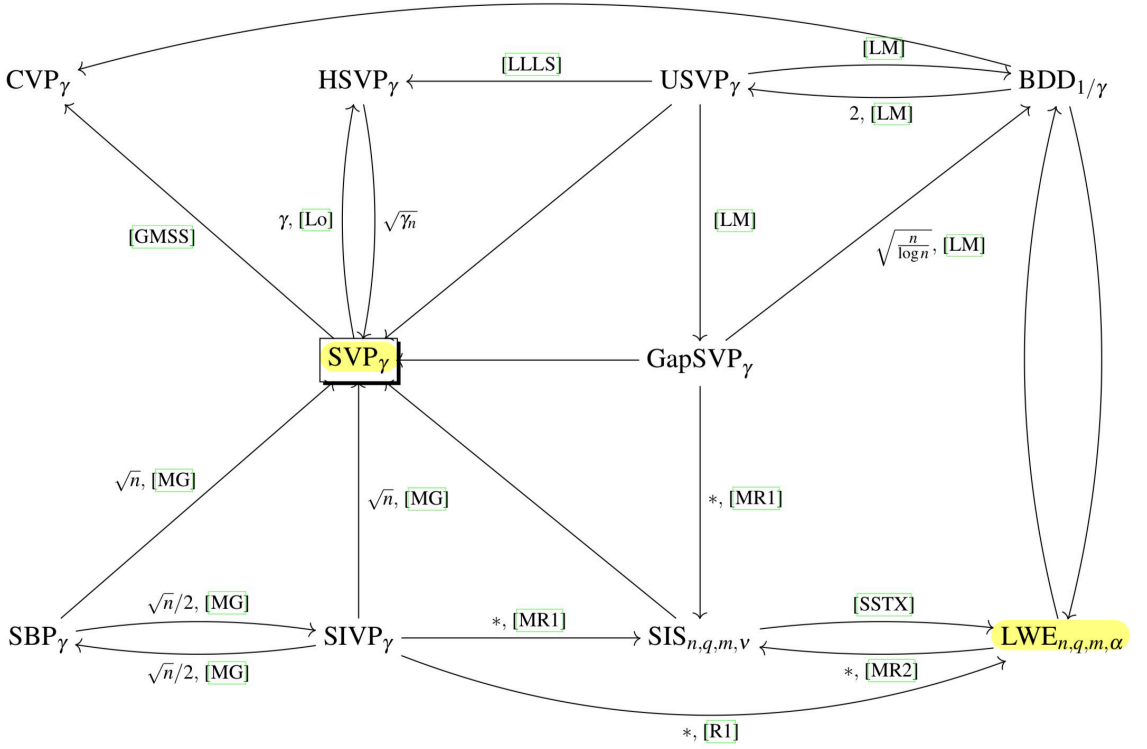
Basis $B = \{ \vec{b}_1, \vec{b}_2, \cdots, \vec{b}_n \}$, linearly independent

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]