CSCI 1515 Applied Cryptography

This Lecture:

- SWHE over Integers (Continued)
- SWHE from LWE (GSW)

Fully Homomorphic Encryption (FHE)

All poly-sized Boolean circuits

Def A (public-key) homomorphic encryption scheme

$\Pi = (\text{KeyGen}, \text{Enc}, \text{Dec}, \text{Eval})$ w.r.t. function family F:

- $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$
- $ct \leftarrow \text{Enc}_{pk}(m)$ $\quad m \in \{0,1\}$
- $m \leftarrow \text{Dec}_{sk}(ct)$
- $ct_f \leftarrow \text{Eval}(f, ct_1, \cdots, ct_n)$ $\quad f: \{0,1\}^n \to \{0,1\}$

- **Correctness:** $ct_i \leftarrow \text{Enc}_{pk}(m_i)$ $\forall i \in [n]$,

  $\forall f \in F$, $ct_f \leftarrow \text{Eval}(f, ct_1, \cdots, ct_n)$

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

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

- **Compactness:** $|ct_f| \leq$ fixed poly (λ)

  Independent of circuit size of f.

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)
- from RLWE (BFV)

Step 2: Bootstrapping

SWHE over Integers

Attempt 1 (Secret-key)

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

  Sample a random q.

  Output $ct = p \cdot q + m$

  Encryption of 0 is a multiple of p.
- Dec(ct): $ct \bmod p$
- Eval ADD: $ct \leftarrow ct_1 + ct_2$

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

(CPA) Security?

$$\mathrm{GCD}(p \cdot q_1, p \cdot q_2, \cdots) = p$$

SWHE over Integers

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

  Encryption of 0 is small and even modulo p.

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

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

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

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

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

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

$O(e_1+e_2)$

$ct_1 \cdot ct_2 = \cancel{pq_1(pq_2+m_2+2e_2)} + \cancel{m_1 \cdot pq_2} + m_1 \cdot m_2 + m_1 \cdot 2e_2 + \cancel{2e_1 pq_2} + 2e_1 m_2 + 4e_1 e_2$

$O(e_1 \cdot e_2)$

$\Downarrow$

#MULT: $O(\lambda)$

- Approximate GCD Problem:

  Given poly-many $\{x_i = p \cdot q_i + s_i\}$, output p.

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

Best known attacks require 2^λ 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 $ct =$ (random subset sum of x_i'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: $ct \leftarrow ct_1 \cdot ct_2$

How homomorphic is it?

Learning With Errors (LWE) Assumption

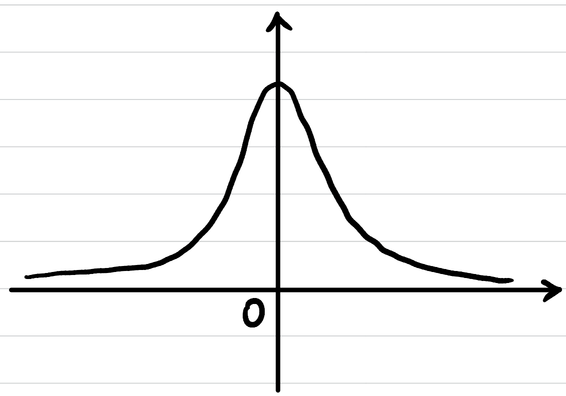
$n \sim$ security parameter

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

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

χ : distribution over $\mathbb{Z}_q$

(concentrated on "small integers")



$$\Pr\left[\,|e| > \underset{\substack{\uparrow \\ \alpha \ll 1}}{\alpha} \cdot q \;\middle|\; e \leftarrow \chi\,\right] \le \mathrm{negl}(n)$$

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

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

$$\underset{m\times n}{\boxed{A}} \times \underset{n\times 1}{\boxed{s}} + \underset{m\times 1}{\boxed{e}} = \underset{m\times 1}{\boxed{b}}$$

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

Learning With Errors (LWE) Assumption

(Lattice-based Crypto)

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

shortest vector problem in lattices

LWE

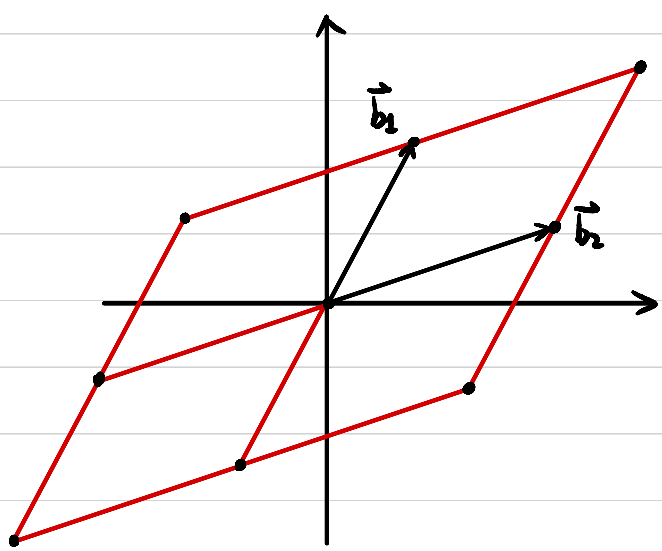
post-quantum secure

Given a lattice of dimension n:

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

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

Find the shortest vector in L.



Regev Encryption from LWE

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

$$\underset{m\times n}{A} \times \underset{n\times 1}{s} + \underset{m\times 1}{e} = \underset{m\times 1}{b}$$

$pk = (A, b)$

$sk = s$

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

sample a random $S \subseteq [m]$

$$c = \left(\sum_{i\in S} A_i ,\ \left(\sum_{i\in S} b_i\right) + \mu \cdot \lfloor \tfrac{q}{2} \rfloor \right)$$

A_i: i-th row of A

$Dec_{sk}(c)$: $c = \boxed{c_1}\boxed{c_2}$

small noise

$$c_2 - \langle c_1, s\rangle = \mu \cdot \lfloor \tfrac{q}{2} \rfloor + \sum_{i\in S} e_i$$

$B = \begin{bmatrix} A & -b \end{bmatrix}, \quad t = \begin{bmatrix} s \\ 1 \end{bmatrix}$

$$\underset{m\times n}{\begin{bmatrix} A & -b \end{bmatrix}} \times \underset{n\times 1}{\begin{bmatrix} s \\ 1 \end{bmatrix}} = \underset{m\times 1}{e}$$

$pk = B_{m\times n}$ $\qquad B\cdot t = \text{Small}$

$sk = t_{n\times 1}$

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

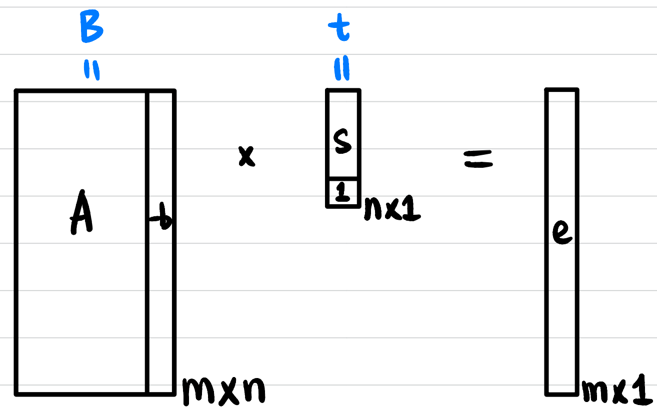
sample $r \xleftarrow{\$} \{0,1\}^m$

$$\underset{1\times m}{r} \qquad \underset{m\times n}{B}$$

$$c = r\cdot B + (0, \cdots, 0, \mu\cdot\lfloor \tfrac{q}{2} \rfloor)$$

$Dec_{sk}(c)$: $\langle c, t\rangle = \mu \cdot \lfloor \tfrac{q}{2} \rfloor + \text{small noise}$

Regev Encryption from LWE



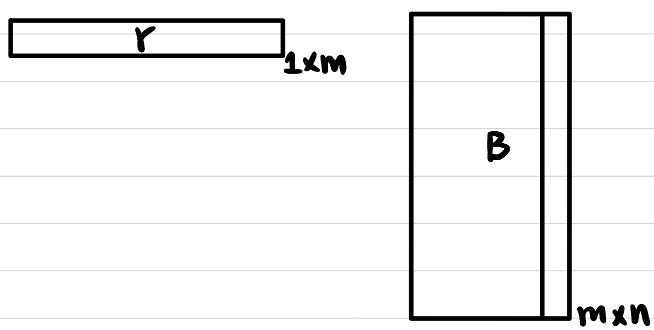
$pk = B_{m\times n}$

$sk = t_{n\times 1}$

$B \cdot t = \text{small}$

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

sample $r \xleftarrow{\$} \{0,1\}^m$



$c = r \cdot B + (0, \cdots, 0, \mu \cdot \lfloor \frac{q}{2} \rfloor)$

$Dec_{sk}(c)$: $\langle c, t\rangle = \mu \cdot \lfloor \frac{q}{2} \rfloor + \text{small noise}$

Homomorphism:

$c_1 = Enc(\mu_1) \qquad \langle c_1, t\rangle = \text{"small"} + \mu_1 \cdot \lfloor \frac{q}{2} \rfloor$

$c_2 = Enc(\mu_2) \qquad \langle c_2, t\rangle = \text{"small"} + \mu_2 \cdot \lfloor \frac{q}{2} \rfloor$

Additive Homomorphism?

$c = c_1 + c_2$

$\langle c, t\rangle = \text{"small"} + (\mu_1 + \mu_2) \cdot \lfloor \frac{q}{2} \rfloor$

Multiplicative Homomorphism?

SWHE from LWE (GSW)

Attempt 1 (secret-key)

$$sk = t_{n\times 1} \qquad \begin{bmatrix} s \\ 1 \end{bmatrix}_{n\times 1}$$

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

How?

Sample $C_0 \in \mathbb{Z}_q^{n\times n}$ s.t. $C_0 \cdot \vec{t} = \text{small}$

$$\begin{bmatrix} C_0 \end{bmatrix}_{n\times n} \times \begin{bmatrix} t \end{bmatrix}_{n\times 1} = \begin{bmatrix} e \end{bmatrix}_{n\times 1}$$

$$\underbrace{C}_{n\times n} = C_0 + \mu \cdot \underbrace{I}_{\text{identity matrix}}$$

$Dec_{sk}(c)$: $c \cdot \vec{t} = (C_0 + \mu \cdot I) \cdot \vec{t} = \vec{e} + \mu \cdot \vec{t}$

SWHE from LWE (GSW)

Attempt 1 (secret-key)

Without Error: $C \cdot \vec{t} = \mu \cdot \vec{t}$

Homomorphism: $C_1 \cdot \vec{t} = \mu_1 \cdot \vec{t}$

$C_2 \cdot \vec{t} = \mu_2 \cdot \vec{t}$

Additive Homomorphism?

$C = C_1 + C_2$

$C \cdot \vec{t} = (C_1 + C_2) \cdot \vec{t} = (\mu_1 + \mu_2) \cdot \vec{t}$

Multiplicative Homomorphism?

$C = C_1 \cdot C_2$

$$\begin{aligned} C \cdot \vec{t} &= (C_1 \cdot C_2) \cdot \vec{t} \\ &= C_1 \cdot (C_2 \cdot \vec{t}) \\ &= C_1 \cdot \mu_2 \cdot \vec{t} \\ &= \mu_2 \cdot (C_1 \cdot \vec{t}) \\ &= \mu_2 \cdot \mu_1 \cdot \vec{t} \end{aligned}$$

With Error: $C \cdot \vec{t} = \mu \cdot \vec{t} + \vec{e}$

Homomorphism: $C_1 \cdot \vec{t} = \mu_1 \cdot \vec{t} + \vec{e}_1$

$C_2 \cdot \vec{t} = \mu_2 \cdot \vec{t} + \vec{e}_2$

Additive Homomorphism?

$C = C_1 + C_2$

$C \cdot \vec{t} = (C_1 + C_2) \cdot \vec{t} = (\mu_1 + \mu_2) \cdot \vec{t} + (\vec{e}_1 + \vec{e}_2)$

Multiplicative Homomorphism?

$C = C_1 \cdot C_2$

$$\begin{aligned} C \cdot \vec{t} &= (C_1 \cdot C_2) \cdot \vec{t} \\ &= C_1 \cdot (C_2 \cdot \vec{t}) \\ &= C_1 \cdot (\mu_2 \cdot \vec{t} + \vec{e}_2) \\ &= \mu_2 \cdot C_1 \cdot \vec{t} + C_1 \cdot \vec{e}_2 \\ &= \mu_2 \cdot (\mu_1 \cdot \vec{t} + \vec{e}_1) + C_1 \cdot \vec{e}_2 \\ &= \mu_2 \cdot \mu_1 \cdot \vec{t} + \mu_2 \cdot \vec{e}_1 + C_1 \cdot \vec{e}_2 \end{aligned}$$

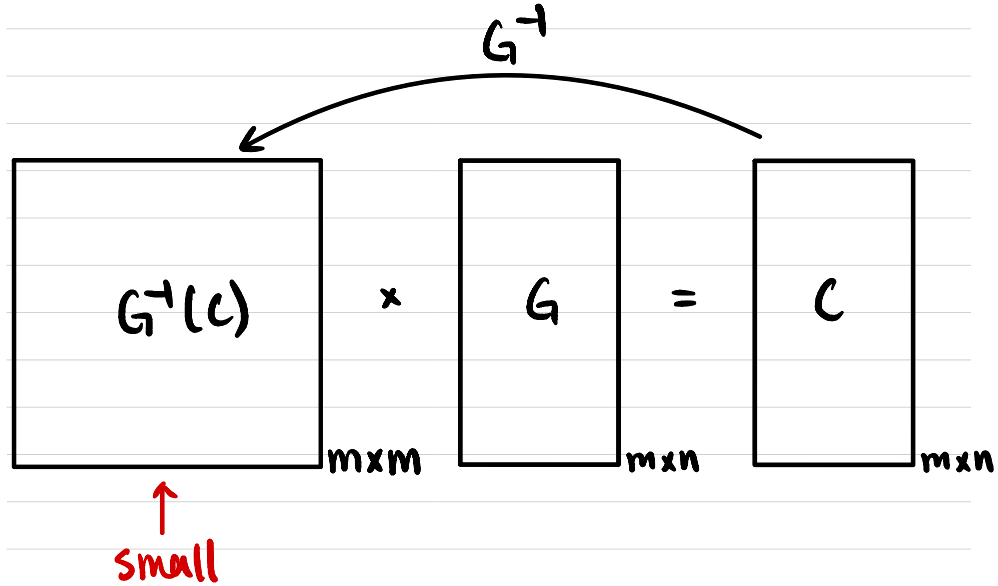
SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattering Gadget:

Gadget matrix $G \in \mathbb{Z}_q^{m \times n}$

$$\boxed{G}_{m \times n}$$

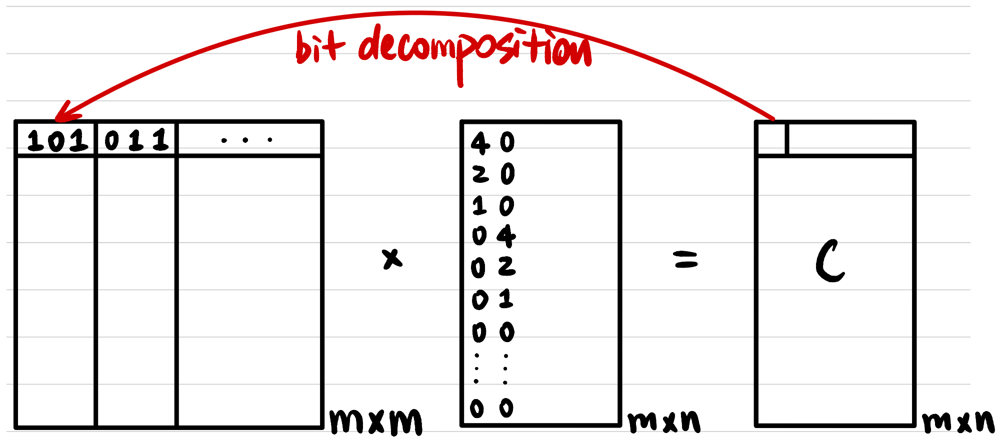


Inverse transformation

$$G^{-1}: \mathbb{Z}_q^{m \times n} \to \mathbb{Z}_q^{m \times m}$$

$$\forall C \in \mathbb{Z}_q^{m \times n}, \quad G^{-1}(C) = \text{small}$$

$$G^{-1}(C) \cdot G = C$$



$m = n \cdot \log q$

SWHE from LWE (GSW)

Attempt 2 (secret-key)

$$sk = t_{n\times 1} \quad \begin{bmatrix} s \\ 1 \end{bmatrix}_{n\times 1}$$

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

Sample $C_0 \in \mathbb{Z}_q^{m\times n}$ s.t. $C_0 \cdot \vec{t} = \text{small}$

$$\begin{bmatrix} C_0 \end{bmatrix}_{m\times n} \times \begin{bmatrix} t \end{bmatrix}_{n\times 1} = \begin{bmatrix} e \end{bmatrix}_{m\times 1}$$

$$C = C_0 + \mu \cdot G$$

↑ gadget matrix

$Dec_{sk}(c)$:

$$C \cdot \vec{t} = (C_0 + \mu \cdot G) \cdot \vec{t}$$
$$= \vec{e} + \mu \cdot (G \cdot \vec{t})$$

Homomorphism:

$$C_1 \cdot \vec{t} = \mu_1 \cdot (G \cdot \vec{t}) + \vec{e_1}$$
$$C_2 \cdot \vec{t} = \mu_2 \cdot (G \cdot \vec{t}) + \vec{e_2}$$

Additive Homomorphism?

$$C = C_1 + C_2 \Rightarrow C \cdot \vec{t} = (\mu_1 + \mu_2) \cdot (G \cdot \vec{t}) + (\vec{e_1} + \vec{e_2})$$

Multiplicative Homomorphism?

$$C = G^{-1}(C_1) \cdot C_2$$

$$\begin{aligned}
C \cdot \vec{t} &= G^{-1}(C_1) \cdot C_2 \cdot \vec{t} \\
&= G^{-1}(C_1) \cdot (\mu_2 \cdot (G \cdot \vec{t}) + \vec{e_2}) \\
&= \mu_2 \cdot G^{-1}(C_1) \cdot G \cdot \vec{t} + G^{-1}(C_1) \cdot \vec{e_2} \\
&= \mu_2 \cdot C_1 \cdot \vec{t} + G^{-1}(C_1) \cdot \vec{e_2} \\
&= \mu_2 \cdot (\mu_1 \cdot (G \cdot \vec{t}) + \vec{e_1}) + G^{-1}(C_1) \cdot \vec{e_2} \\
&= \mu_2 \cdot \mu_1 \cdot (G \cdot \vec{t}) + \mu_2 \cdot \vec{e_1} + G^{-1}(C_1) \cdot \vec{e_2}
\end{aligned}$$

How homomorphic is it?

$$\#\text{MULT} \sim \log_m q$$