CSCI 1515 Applied Cryptography

This Lecture:

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

Fully Homomorphic Encryption (FHE)

All poly-sized Boolean circuits

Def A (public-key) homomorphic encryption scheme $\Pi = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Eval})$ w.r.t. function family $\mathcal{F}$:

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

- **Correctness:** $ct_i \leftarrow \mathsf{Enc}_{pk}(m_i) \ \forall i \in [n]$,
  $\forall f \in \mathcal{F}$, $ct_f \leftarrow \mathsf{Eval}(f, ct_1, \cdots, ct_n)$
  $\mathsf{Dec}_{sk}(ct_f) = f(m_1, \cdots, m_n)$
- **(CPA) Security:** $(pk, \mathsf{Enc}_{pk}(m_0)) \overset{c}{\approx} (pk, \mathsf{Enc}_{pk}(m_1))$.
- **Compactness:** $|ct_f| \leq$ fixed poly (λ)
  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?

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

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 $e \ll p$

  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: $ct \leftarrow ct_1 \cdot ct_2$

- 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"

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

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

  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.

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

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

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

How homomorphic is it?

Learning With Errors (LWE) Assumption

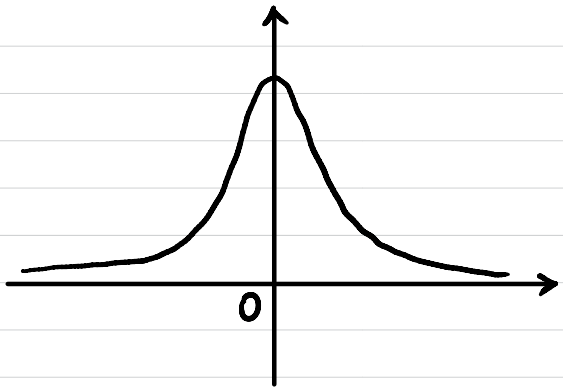
$n \sim$ security parameter

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

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

χ: distribution over $\mathbb{Z}_q$

(concentrated on "small integers")

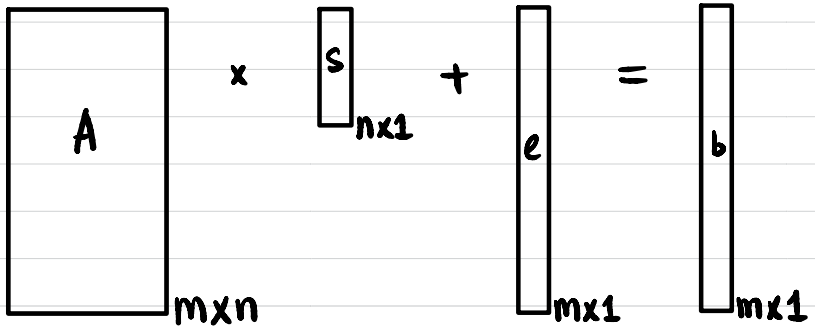


$$\Pr[|e| > \alpha \cdot q \mid e \leftarrow \chi] \leq \text{negl}(n)$$

$\alpha \ll 1$

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

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



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

Learning With Errors (LWE) Assumption

(Lattice-based Crypto)

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

shortest vector problem in lattices

LWE

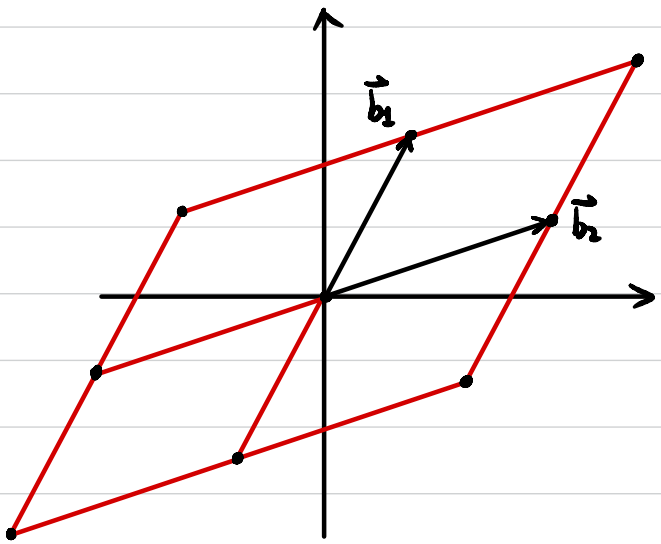
↑ post-quantum secure

Given a lattice of dimension n:

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

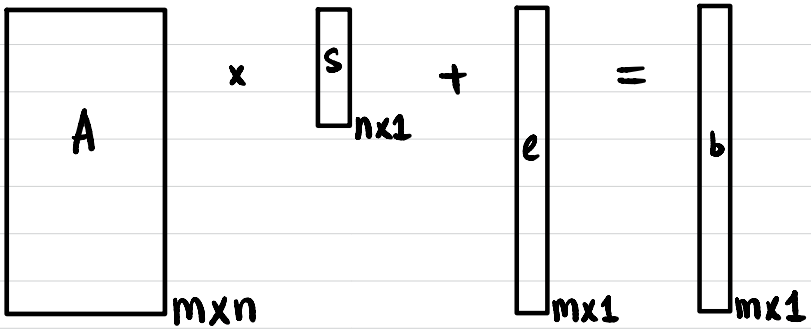
Lattice $L(B) := \{ \sum_{i=1}^{n} \alpha_i \vec{b}_i \mid \alpha_i \in \mathbb{Z} \}$

Find the shortest vector in L.



Regev Encryption from LWE

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



$pk = (A, b)$

$sk = s$

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

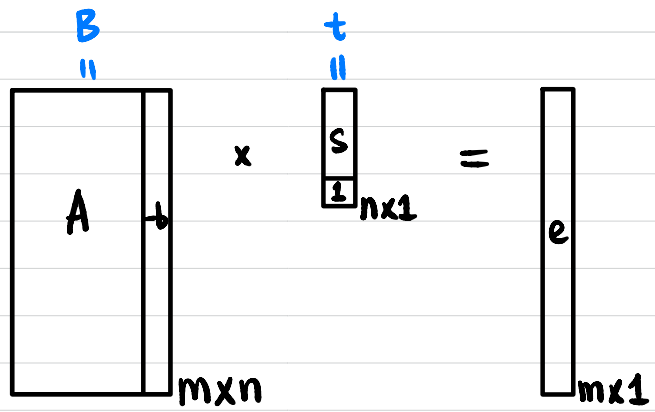
sample a random $S \subseteq [m]$

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

A_i: i-th row of A

$\text{Dec}_{sk}(c)$: $c = [\, c_1 \mid c_2 \,]$

$c_2 - \langle c_1, s \rangle = ?$

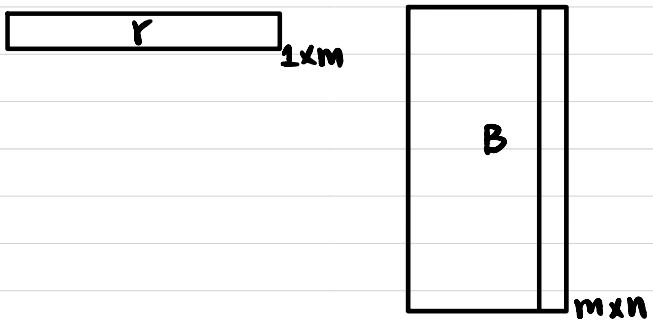


$pk = B_{m \times n}$ $\qquad B \cdot t = \text{Small}$

$sk = t_{n \times 1}$

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

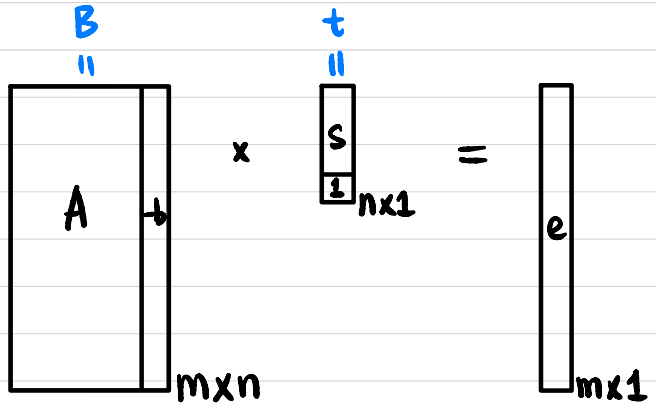
sample $r \xleftarrow{\$} \{0,1\}^m$



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

$\text{Dec}_{sk}(c)$: $\langle c, t \rangle = ?$

Regev Encryption from LWE



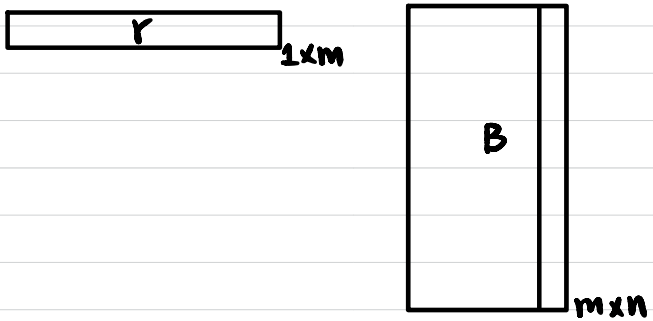
$pk = B_{m \times n}$

$sk = t_{n \times 1}$

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

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

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



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

$Dec_{sk}(c)$: $\langle c, t \rangle = ?$

Homomorphism:

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

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

Additive Homomorphism?

Multiplicative Homomorphism?

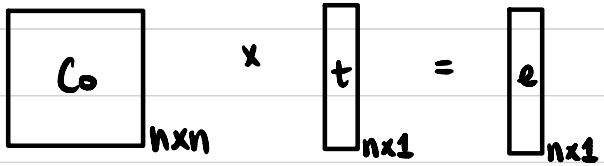
SWHE from LWE (GSW)

Attempt 1 (secret-key)

$sk = t_{nx1}$ 

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

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



$C = C_0 + \mu \cdot I$

C: nxn; I: identity matrix

$Dec_{sk}(c)$: $C \cdot \vec{t} = ?$

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?

Multiplicative Homomorphism?

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?

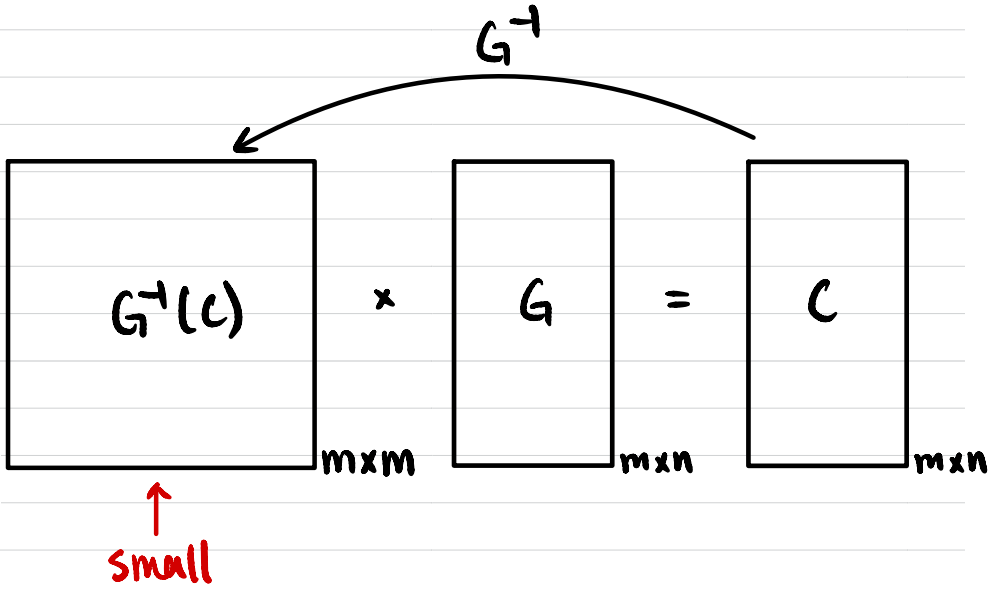
Multiplicative Homomorphism?

SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattering Gadget:

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

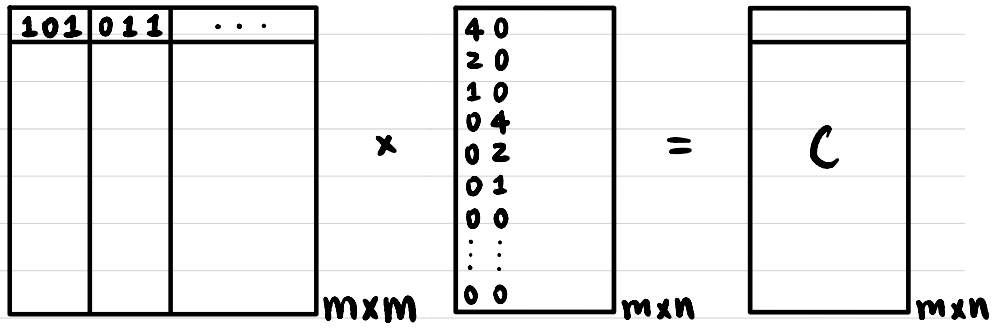


Inverse transformation

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

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

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



m = ?

SWHE from LWE (GSW)

Attempt 2 (secret-key)

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

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

$C_2 \cdot \vec{t} =$

Additive Homomorphism?

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

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

Multiplicative Homomorphism?

$$\underbrace{C_0}_{n\times n} \times \underbrace{t}_{n\times 1} = \underbrace{e}_{n\times 1}$$

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

↑ gadget matrix

$Dec_{sk}(c)$: $C \cdot \vec{t} = ?$

How homomorphic is it?

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

Ciphertext space $R_q \times R_q$

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

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

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

$$sk = s$$

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

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

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

$Dec_{sk}(c)$: $[c_0 + c_1 \cdot s]_q = ?$

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?

Multiplicative Homomorphism?

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:

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

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

$c(s) + c_3 \cdot rlk(s)$?