CSCI 1510

- Post-Quantum PKE from LWE Assumption (Continued)
- Homomorphic Encryption
- Somewhat Homomorphic Encryption over Integers
- SWHE from LWE (GSW)

ANNOUNCEMENT: Mid-semester survey (for extra credit)

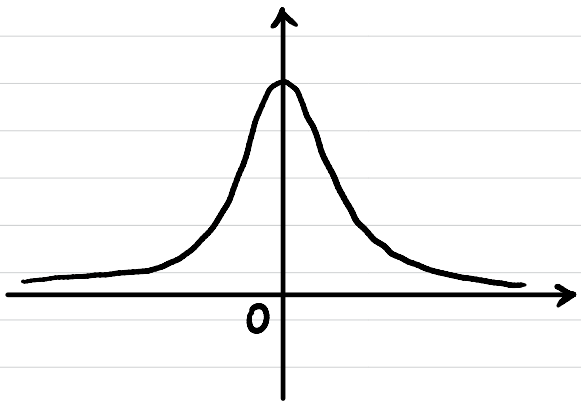
Post-Quantum Assumption: Learning With Errors (LWE)

n: security parameter

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

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

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

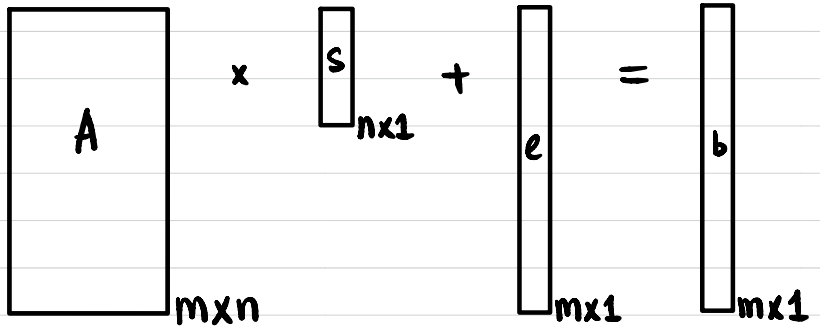


$$\Pr[|e| > \alpha \cdot q \mid e \leftarrow \chi] \leq \text{negl}(n)$$

$\alpha \ll 1$

Def We say the decisional $\text{LWE}_{n,m,q,\chi}$ problem is (quantum) hard if $\forall$ (quantum) PPT $\mathcal{A}$, $\exists$ negligible function $\epsilon(\cdot)$ s.t.

$$\left| \Pr\left[\begin{matrix} A \xleftarrow{\$} \mathbb{Z}_q^{m \times n} \\ s \xleftarrow{\$} \mathbb{Z}_q^n \\ e \leftarrow \chi^m \end{matrix} : \mathcal{A}(A, [As + e \bmod q]) = 1 \right] - \Pr\left[\begin{matrix} A \xleftarrow{\$} \mathbb{Z}_q^{m \times n} \\ b' \xleftarrow{\$} \mathbb{Z}_q^m \end{matrix} : \mathcal{A}(A, b') = 1 \right] \right| \leq \epsilon(n).$$



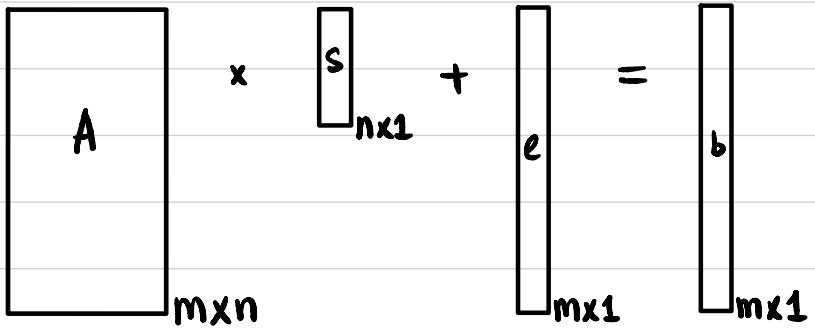
Post-Quantum PKE: Regev Encryption

- $\mathrm{Gen}(1^n)$:

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

  $pk = (A, b = As + e \bmod q)$

  $sk = s$

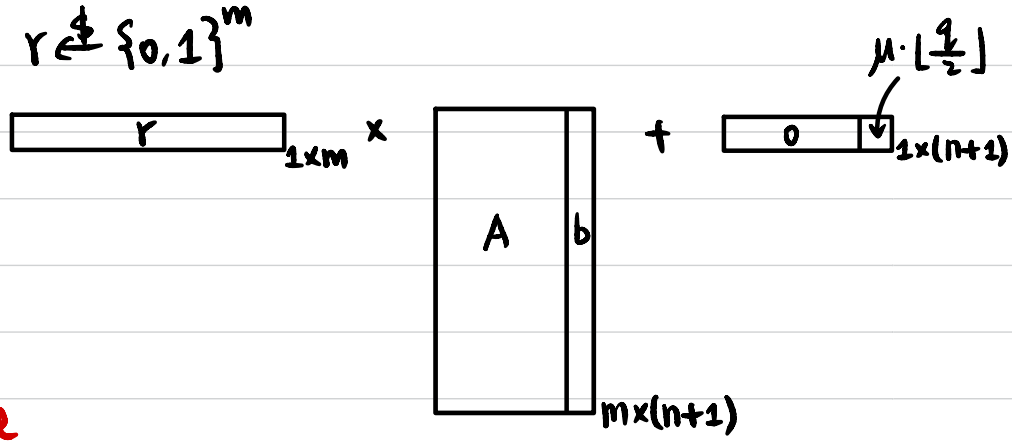


- $\mathrm{Enc}_{pk}(\mu)$: $\mu \in \{0,1\}$

  sample a random $S \subseteq [m]$

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

  A_i: i-th row of A

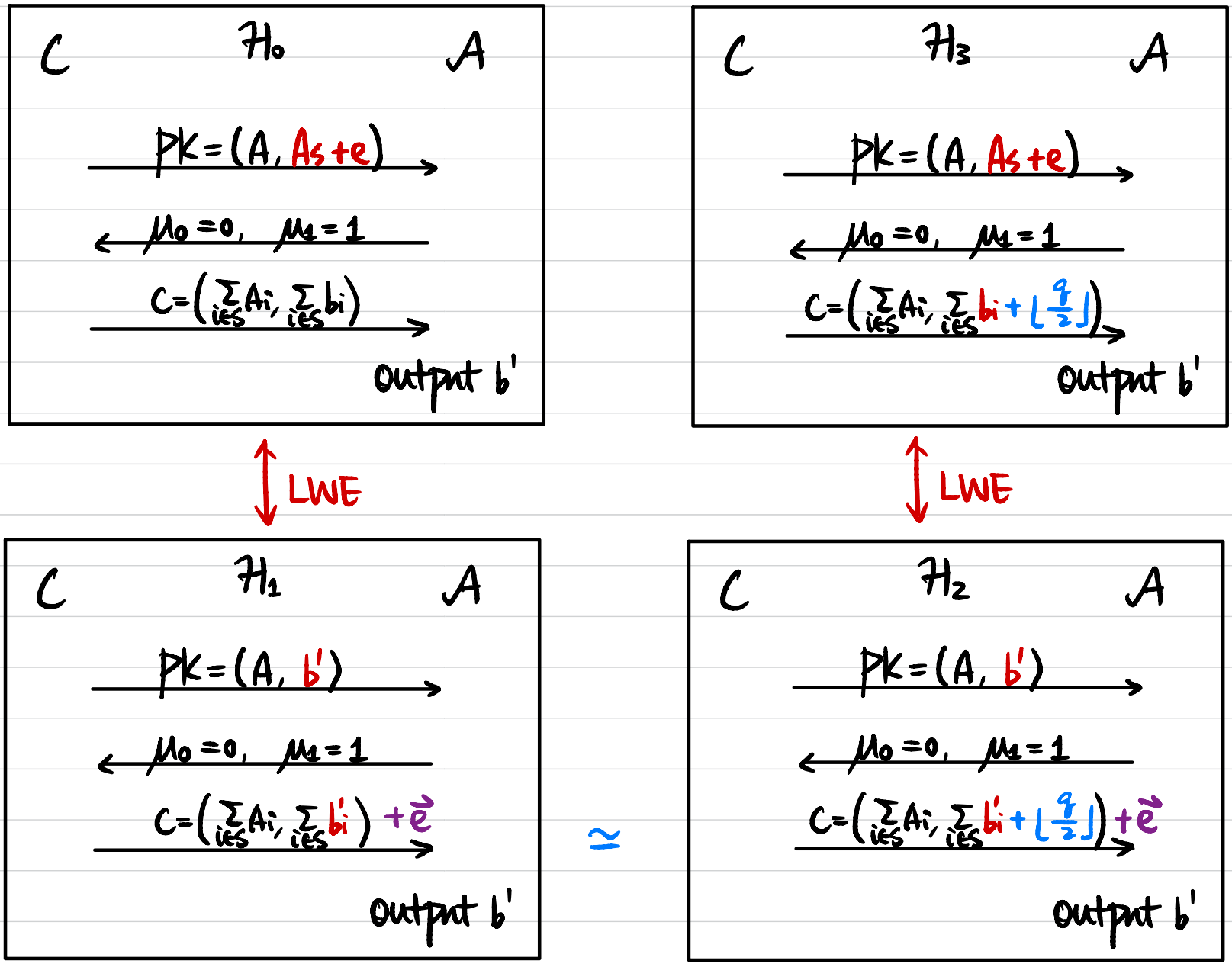


- $\mathrm{Dec}_{sk}(c)$: $c = [c_1 \mid c_2]$

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

Thm If $\mathrm{LWE}_{n,m,q,\chi}$ is (quantum) hard, then Regev encryption is (post-quantum) CPA-secure.

Proof Sketch



Homomorphic Encryption

So far, encryption schemes:

$$ct \leftarrow Enc(x)$$

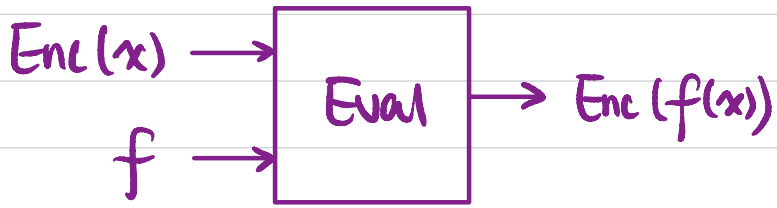
$$x \leftarrow Dec_{sk}(ct)$$

All-or-Nothing:

w/ sk $\rightarrow$ x

w/o sk $\rightarrow$ Nothing

Homomorphic Evaluation:



Application: Outsourcing Storage & Computation

Data x

Key sk

$ct \leftarrow Enc(x)$

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

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

Application: Privacy-Preserving Query

Server

Client

Input x

Key sk

$ct \leftarrow Enc(x)$

ct

$ML/GPT/\cdots$

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

ct'

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

Homomorphic Properties of Encryption Schemes

Multiplicatively Homomorphic

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

Additively Homomorphic

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

El Gamal:

$C_1 = (g^{r_1},\ h^{r_1} \cdot m_1)$

$C_2 = (g^{r_2},\ h^{r_2} \cdot m_2)$

$\Downarrow$

$(g^{r_1+r_2},\ h^{r_1+r_2} \cdot (m_1 \cdot m_2))$

Exponential El Gamal:

$Enc(m) = (g^r,\ h^r \cdot g^m)$

$C_1 = (g^{r_1},\ h^{r_1} \cdot g^{m_1})$

$C_2 = (g^{r_2},\ h^{r_2} \cdot g^{m_2})$

$\Rightarrow (g^{r_1+r_2},\ h^{r_1+r_2} \cdot g^{m_1+m_2})$

Regev:

$C_1 = (r_1^T \cdot A,\ r_1^T \cdot b + \mu_1 \cdot \lfloor \frac{q}{2} \rfloor)$

$C_2 = (r_2^T \cdot A,\ r_2^T \cdot b + \mu_2 \cdot \lfloor \frac{q}{2} \rfloor)$

$\Downarrow$

$((r_1+r_2)^T \cdot A,\ (r_1+r_2)^T \cdot b + (\mu_1+\mu_2) \cdot \lfloor \frac{q}{2} \rfloor)$

Fully Homomorphic: Additively & Multiplicatively Homomorphic

Is it possible?

- Question was asked back in 1978
- Big breakthough in 2009 (Gentry)
  - Complicated construction
  - Non-standard assumptions
- By now: much simpler constructions from standard assumptions.

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 $\mathcal{F}$:
  - $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
  - $ct \leftarrow \mathsf{Enc}_{pk}(m) \quad m \in \{0,1\}$
  - $m \leftarrow \mathsf{Dec}_{sk}(ct)$
  - $ct_f \leftarrow \mathsf{Eval}(f, ct_1, \cdots, ct_k) \quad f: \{0,1\}^k \to \{0,1\}$

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

$$\Pr[\mathsf{Dec}_{sk}(ct_f) = f(m_1, \cdots, m_k)] \geq 1 - \mathsf{negl}(n)$$

where $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$, $ct_i \leftarrow \mathsf{Enc}_{pk}(m_i) \quad \forall i \in [k]$,

$ct_f \leftarrow \mathsf{Eval}(f, ct_1, \cdots, ct_k)$.

Impossible!

- **CPA/CCA Security?**

Missing Requirement?

$|ct_f| \leq$ fixed $\mathrm{poly}(n)$

Independent of circuit size of f.

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 $\mathcal{F}$:
  - $(pk, sk) \leftarrow \mathsf{Gen}(1^n)$
  - $ct \leftarrow \mathsf{Enc}_{pk}(m) \quad m \in \{0,1\}$
  - $m \leftarrow \mathsf{Dec}_{sk}(ct)$
  - $ct_f \leftarrow \mathsf{Eval}(f, ct_1, \cdots, ct_k) \quad f: \{0,1\}^k \to \{0,1\}$

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

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from LWE (GSW)

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: $ct \leftarrow ct_1 \cdot ct_2$

CPA Security? No!

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

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

Best known attacks require 2^n time.

SWHE over Integers

Attempt 3 (public-key)

- secret key: odd number p

  public key: "encryptions of 0"

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

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

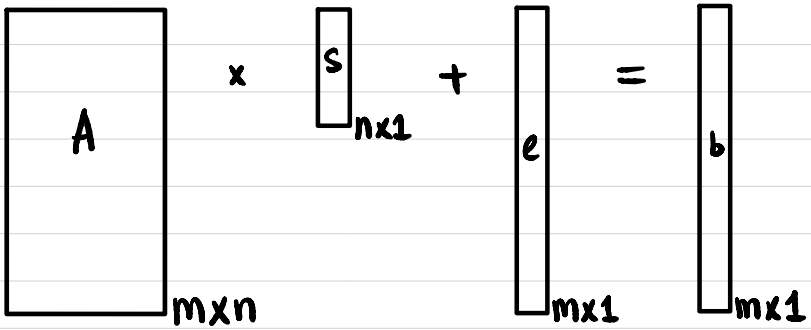
- Eval ADD: $ct \leftarrow ct_1 + ct_2$

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

How homomorphic is it?

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 $S \subseteq [m]$

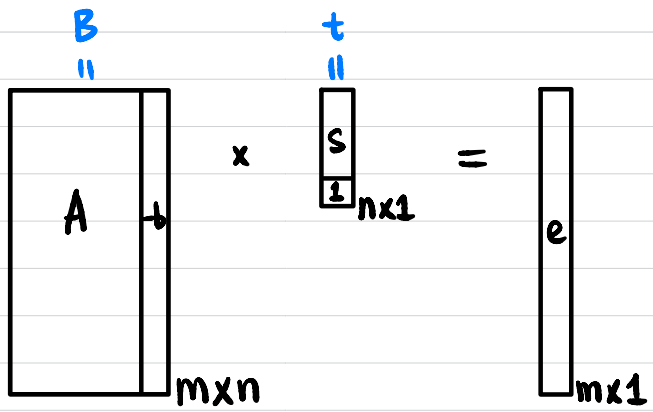
$$c = \left(\sum_{i \in S} A_i \,,\ \left(\sum_{i \in S} b_i \right) + \mu \cdot \left\lfloor \frac{q}{2} \right\rfloor \right)$$

A_i: i-th row of A

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

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

($\sum_{i \in S} e_i$: small noise)

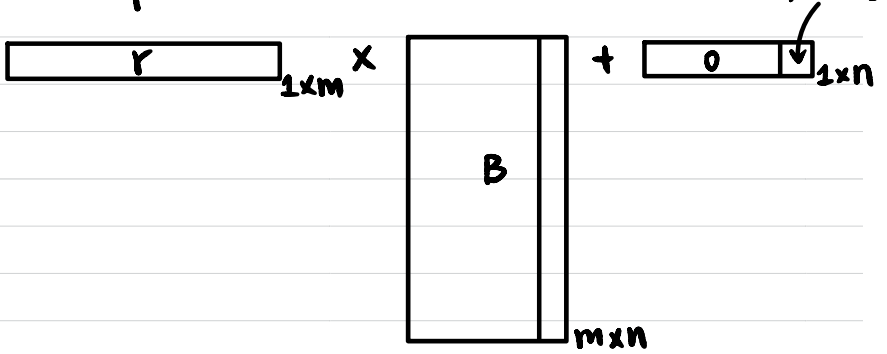


$pk = B_{m \times n}$ $\quad B \cdot t = \text{small}$

$sk = t_{n \times 1}$

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

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



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

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

Regev Encryption from LWE

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?

$c = c_1 + c_2$

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

Multiplicative Homomorphism?

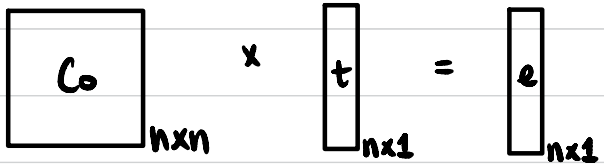
SWHE from LWE (GSW)

Attempt 1 (secret-key)

$sk = t_{n\times 1}$ 

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

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: $n \times n$; I: identity matrix

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

CPA Security?

SWHE from LWE (GSW)

Attempt 1 (secret-key)

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

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

Homomorphism:

$c_1 \cdot \vec{t} = \mu_1 \cdot \vec{t}$

$c_2 \cdot \vec{t} = \mu_2 \cdot \vec{t}$

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?

$$c = c_1 + c_2$$

$$c \cdot \vec{t} = (c_1 + c_2) \cdot \vec{t} = (\mu_1 + \mu_2) \cdot \vec{t}$$

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?

$$c = c_1 \cdot c_2$$

$$\begin{aligned} c \cdot \vec{t} &= (c_1 \cdot c_2) \cdot \vec{t} \\ &= c_1 \cdot (c_2 \cdot \vec{t}) \\ &= c_1 \cdot \mu_2 \cdot \vec{t} \\ &= \mu_2 \cdot (c_1 \cdot \vec{t}) \\ &= \mu_2 \cdot \mu_1 \cdot \vec{t} \end{aligned}$$

Multiplicative Homomorphism?

$$c = c_1 \cdot c_2$$

$$\begin{aligned} c \cdot \vec{t} &= (c_1 \cdot c_2) \cdot \vec{t} \\ &= c_1 \cdot (c_2 \cdot \vec{t}) \\ &= c_1 \cdot (\mu_2 \cdot \vec{t} + \vec{e}_2) \\ &= \mu_2 \cdot c_1 \cdot \vec{t} + c_1 \cdot \vec{e}_2 \\ &= \mu_2 \cdot (\mu_1 \cdot \vec{t} + \vec{e}_1) + c_1 \cdot \vec{e}_2 \\ &= \mu_2 \cdot \mu_1 \cdot \vec{t} + \mu_2 \cdot \vec{e}_1 + c_1 \cdot \vec{e}_2 \end{aligned}$$