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)

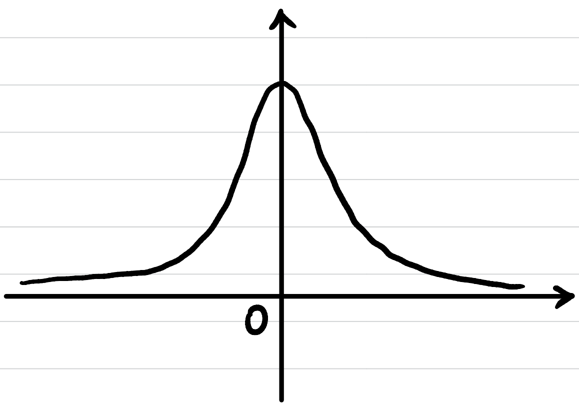
n: security parameter

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

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

χ: distribution over $\mathbb{Z}_q$

(concentrated on "small integers")



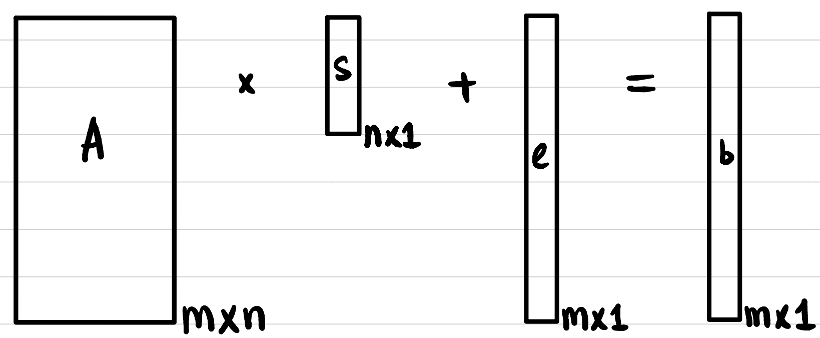
$$\Pr\left[\, |e| > \alpha \cdot q \;\middle|\; e \leftarrow \chi \,\right] \le \mathrm{negl}(n)$$

$\uparrow$

$\alpha \ll 1$

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

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



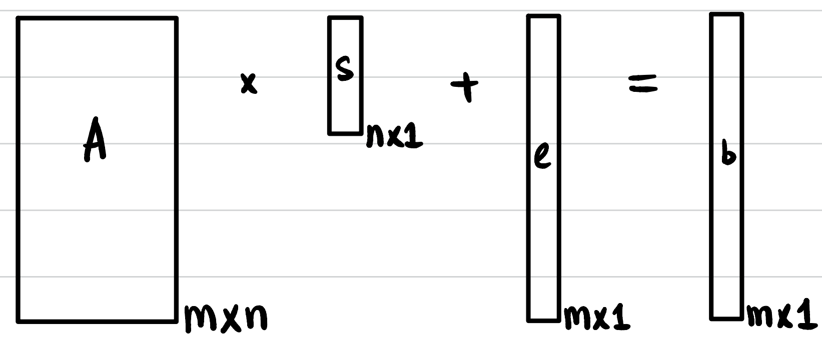
Post-Quantum PKE: Regev Encryption

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

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

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

  $sk = s$

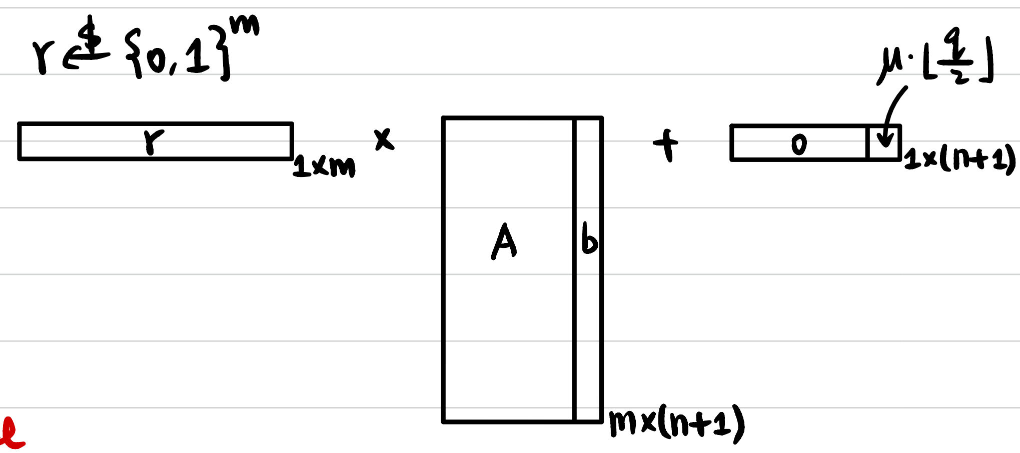


- $\mathrm{Enc}_{pk}(\mu)$: $\mu \in \{0,1\}$

  sample a random $S \subseteq [m]$

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

  i-th row of A



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

  small noise

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

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

Proof Sketch

$\mathcal{H}_0$

$\mathcal{C}$ | $\mathcal{A}$

$$\mathcal{C} \xrightarrow{pk = (A,\ As+e)} \mathcal{A}$$

$$\mathcal{C} \xleftarrow{\mu_0 = 0,\quad \mu_1 = 1} \mathcal{A}$$

$$\mathcal{C} \xrightarrow{c = \left(\sum_{i\in S} A_i,\ \sum_{i\in S} b_i\right)} \mathcal{A}$$

output b'

$\updownarrow$ LWE

$\mathcal{H}_1$

$\mathcal{C}$ | $\mathcal{A}$

$$\mathcal{C} \xrightarrow{pk = (A,\ b')} \mathcal{A}$$

$$\mathcal{C} \xleftarrow{\mu_0 = 0,\quad \mu_1 = 1} \mathcal{A}$$

$$\mathcal{C} \xrightarrow{c = \left(\sum_{i\in S} A_i,\ \sum_{i\in S} b'_i\right)} \mathcal{A}$$

output b'

$\simeq$

$\mathcal{H}_2$

$\mathcal{C}$ | $\mathcal{A}$

$$\mathcal{C} \xrightarrow{pk = (A,\ b')} \mathcal{A}$$

$$\mathcal{C} \xleftarrow{\mu_0 = 0,\quad \mu_1 = 1} \mathcal{A}$$

$$\mathcal{C} \xrightarrow{c = \left(\sum_{i\in S} A_i,\ \sum_{i\in S} b'_i + \lfloor \frac{q}{2} \rfloor\right)} \mathcal{A}$$

output b'

$\updownarrow$ LWE

$\mathcal{H}_3$

$\mathcal{C}$ | $\mathcal{A}$

$$\mathcal{C} \xrightarrow{pk = (A,\ As+e)} \mathcal{A}$$

$$\mathcal{C} \xleftarrow{\mu_0 = 0,\quad \mu_1 = 1} \mathcal{A}$$

$$\mathcal{C} \xrightarrow{c = \left(\sum_{i\in S} A_i,\ \sum_{i\in S} b_i + \lfloor \frac{q}{2} \rfloor\right)} \mathcal{A}$$

output b'

Homomorphic Encryption

So far, encryption schemes:

$$ct \leftarrow Enc(x)$$

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

All-or-Nothing:

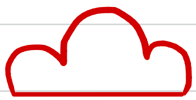
w/ sk $\rightarrow$ x

w/o sk $\rightarrow$ Nothing

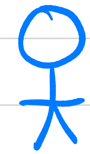
Homomorphic Evaluation:

Application: Outsourcing Storage & Computation

Server



Client



Data x

Key sk

$ct \leftarrow \mathrm{Enc}(x)$

$\xleftarrow{\quad ct \quad}$

$\xleftarrow{\quad f \quad}$

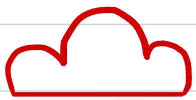
$ct' \leftarrow \mathrm{Eval}(f, ct)$

$\xrightarrow{\quad ct' \quad}$

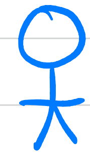
$f(x) \leftarrow \mathrm{Dec}_{sk}(ct')$

Application: Privacy-Preserving Query

Server



Client



Input x

Key sk

$ct \leftarrow Enc(x)$

$\xleftarrow{\quad ct \quad}$

ML/GPT/...

$\downarrow$

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

$\xrightarrow{\quad ct' \quad}$

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

Homomorphic Properties of Encryption Schemes

Multiplicatively Homomorphic

$$\begin{matrix} \mathrm{Enc}(m_1) \searrow \\ \mathrm{Enc}(m_2) \nearrow \end{matrix} \mathrm{Enc}(m_1 \cdot m_2)$$

El Gamal:

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

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

Additively Homomorphic

$$\begin{matrix} \mathrm{Enc}(m_1) \searrow \\ \mathrm{Enc}(m_2) \nearrow \end{matrix} \mathrm{Enc}(m_1 + m_2)$$

Exponential El Gamal:

$$\mathrm{Enc}(m) = (g^{r}, \; h^{r} \cdot g^{m})$$

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

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

Regev:

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

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

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 $\Pi = (\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec}, \mathrm{Eval})$ w.r.t. function family $\mathcal{F}$:
  - $(pk, sk) \leftarrow \mathrm{Gen}(1^n)$
  - $ct \leftarrow \mathrm{Enc}_{pk}(m) \quad m \in \{0,1\}$
  - $m \leftarrow \mathrm{Dec}_{sk}(ct)$
  - $ct_f \leftarrow \mathrm{Eval}(f, ct_1, \cdots, ct_k) \qquad f: \{0,1\}^k \rightarrow \{0,1\}$

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

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

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

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

- **CPA/CCA Security ?**

Missing Requirement ?

Fully Homomorphic Encryption (FHE)

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

- 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?
- 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?

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 $e \ll p$

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

  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: $ct \leftarrow ct_1 \cdot ct_2$

- 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

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

$$\begin{bmatrix} A \end{bmatrix}_{m\times n} \times \begin{bmatrix} s \end{bmatrix}_{n\times 1} + \begin{bmatrix} e \end{bmatrix}_{m\times 1} = \begin{bmatrix} b \end{bmatrix}_{m\times 1}$$

$pk = (A, b)$

$sk = s$

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

sample a random $S \subseteq [m]$

$$c = \Big(\underbrace{\sum_{i\in S} A_i}_{\text{i-th row of } A},\ \big(\sum_{i\in S} b_i\big) + \mu\cdot\lfloor \tfrac{q}{2} \rfloor \Big)$$

$\mathrm{Dec}_{sk}(c)$: $c = \begin{bmatrix} c_1 & | & c_2 \end{bmatrix}$

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

$$\overset{B}{\begin{bmatrix} A & | & -b \end{bmatrix}}_{m\times n} \times \overset{t}{\begin{bmatrix} s \\ 1 \end{bmatrix}}_{n\times 1} = \begin{bmatrix} e \end{bmatrix}_{m\times 1}$$

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

$sk = t_{n\times 1}$

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

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

$$\begin{bmatrix} r \end{bmatrix}_{1\times m} \times \begin{bmatrix} B \end{bmatrix}_{m\times n} + \begin{bmatrix} 0 & | & \mu\cdot\lfloor \tfrac{q}{2} \rfloor \end{bmatrix}_{1\times n}$$

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

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

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)

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

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

How?

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

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

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

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

CPA Security ?

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?

$C_1 + C_2$?

Multiplicative Homomorphism?

$C_1 \cdot C_2$?

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?

$C_1 + C_2$?

Multiplicative Homomorphism?

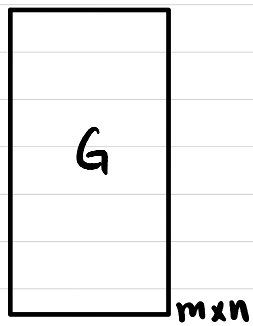
$C_1 \cdot C_2$?

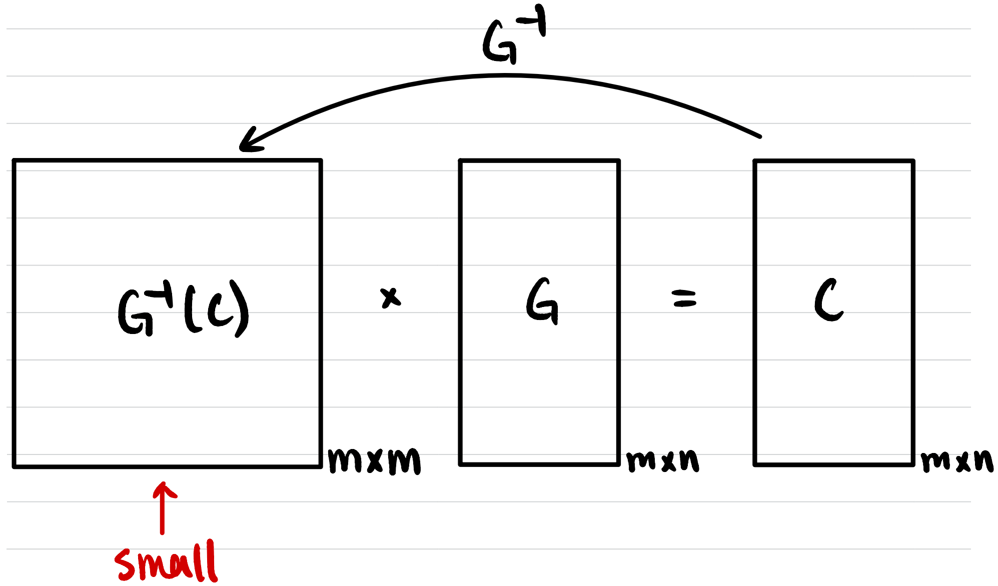
SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattering Gadget:

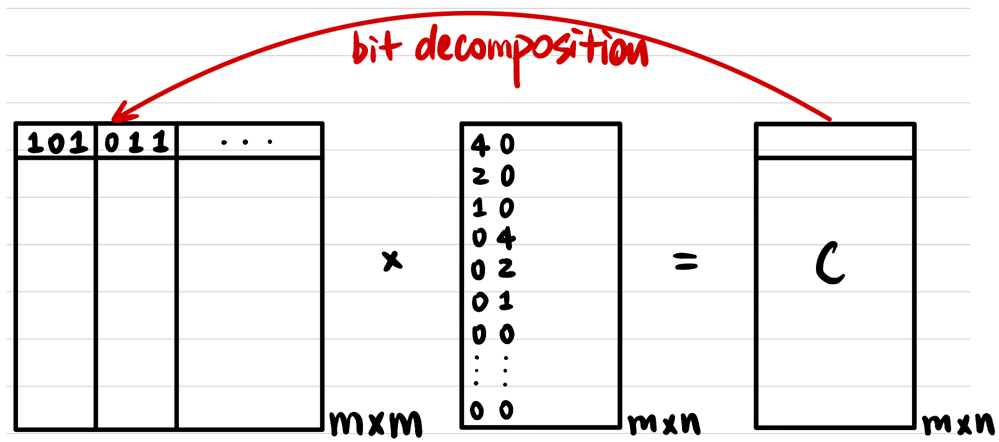
Gadget matrix $G \in \mathbb{Z}_q^{m \times n}$





Inverse transformation

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



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

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

$m = ?$

SWHE from LWE (GSW)

Attempt 2 (secret-key)

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

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

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

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

$$C = C_0 + \mu \cdot \underset{\text{gadget matrix}}{\underset{\uparrow}{G}}$$

$\text{Dec}_{sk}(c)$: $C \cdot \vec{t} = ?$

CPA Security?

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

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

Additive Homomorphism?

$C_1 + C_2$?

Multiplicative Homomorphism?

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

How homomorphic is it?

#MULT ?