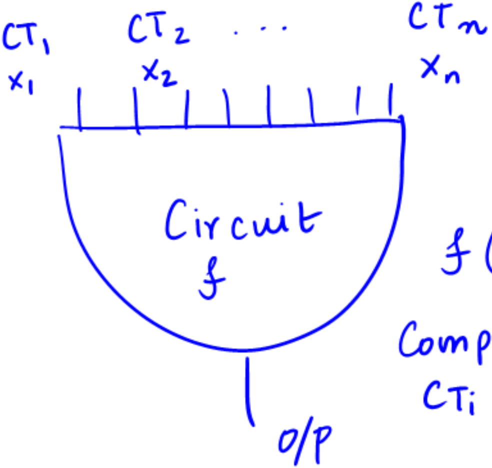
CS6846 – Quantum Algorithms and Cryptography

Fully Homomorphic Encryption

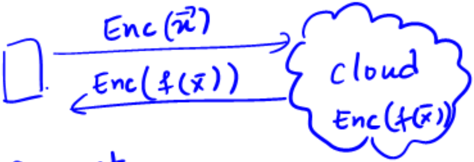
Instructor: Shweta Agrawal, IIT Madras
Email: shweta@cse.iitm.ac.in

Gen09. Computing on Encrypted data.



$f(x_1 \cdots x_n)$

Compute f on CT_i themselves.



$f(\vec{x})$

Decrypt to recover $f(x)$.

Homomorphic Encryption:

Keygen $(1^n) \longrightarrow pk, sk, \underline{evk}$.

Encrypt $(PK, m) \longrightarrow CT$.

Decrypt $(SK, CT) \rightarrow m'$

Eval $(f, CT_1, \ldots, CT_\ell) \rightarrow CT_f$.

Definition (L-homomorphism): A scheme HE is L-homomorphic, if for any depth L arithmetic circuit f, and any set of inputs $m_1 \dots m_\ell$, it holds that:

$$\Pr\Big(\mathrm{Decrypt}\big(sk, \overbrace{\mathrm{Eval}(f, CT_1 \dots CT_\ell, evk)}^{CT_f}\big) \neq f(m_1 \dots m_\ell)\Big) = \mathrm{negl}(n).$$

where $(pk, sk, evk) \leftarrow \mathrm{Keygen}(1^n)$

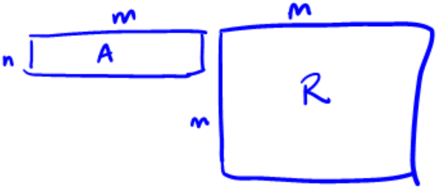
$CT_i \leftarrow \mathrm{Encrypt}(PK, m_i)$.

Compactness: A homomorphic scheme is compact if its ciphertext size is independent of the size of the evaluated function.

Leftover Hash Lemma (ILL '82):

If $A \leftarrow \mathbb{Z}_q^{n \times m}$ where $m \geq 2n \log q$;

and $R \leftarrow \{0,1\}^{m \times m}$, then



$(A, AR) \overset{\text{stat.}}{\approx} (A, \text{uniform})$.

Bit Decomposition: let $x \in \mathbb{Z}_q^n$, let $w_i \in \{0,1\}$ be such that

$$x = \sum_{i=0}^{\lceil \log q \rceil - 1} 2^i w_i \pmod q$$

output $(w_0 \ldots w_{\lceil \log q \rceil - 1})$

The matrix G: Let $g^T = (1, 2, 4 \ldots 2^{k-1} > \frac{q}{2})$

Define $G = \begin{bmatrix} -g^T- & & \\ & -g^T- & \\ & & \ddots \\ & & & -g^T- \end{bmatrix} \in \mathbb{Z}_q^{n \times nk}$.

Powers of 2 matrix.

Define $\underline{\underline{G^{-1}}}$ as follows:

Bit Dec

Lemma: For any $m > n \log q$, $\exists$ a fixed efficiently computable matrix $G \in \mathbb{Z}_q^{n \times m}$ and an efficiently computable function G^{-1} s.t. for any $M \in \mathbb{Z}_q^{n \times m'}$,

$$G^{-1}(M) \in \{0,1\}^{nk \times m'} \quad \text{s.t.}$$

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

Gentry - Sahai - Waters FHE :

Setup$(1^\lambda, 1^d)$: depth. Choose modulus q, matrix dimesions n, m, Choose noise distribution χ, some noise bound B_χ

choose $B \leftarrow \mathbb{Z}_q^{n-1 \times m}$. o/p All this.

Keygen: ① Sample $s \leftarrow \mathbb{Z}_q^{n-1}$.

② output $t = (-s, 1)$. as SK.

③ Let $b = sB + e$ ↳ sampled from χ^m.

④ $PK = A = \begin{bmatrix} B \\ b \end{bmatrix}$

Encrypt (PK, μ) : Sample $R \leftarrow \{0,1\}^{m \times m}$

Compute $C = AR + \mu \cdot G \quad \in \mathbb{Z}_q^{n \times m}$.

Decrypt (SK, CT) : $SK = t = (-s, 1)$.

Define $w = [0, 0 \cdots 0, \lceil q/2 \rceil]$

Compute $v = t \cdot C \cdot G^{-1}(w^T) \in \mathbb{Z}_q$.

Detour : Correctness as PKE

① Note $t \cdot A = (-s, 1)\begin{pmatrix} B \\ b \end{pmatrix} = -sB + b$

$\downarrow$

$sB + e$

$=$ error e.

$tA \approx 0$.

$$t\cdot C = (-s, 1)\cdot(AR + \mu G)$$

$$= \overbrace{\underbrace{tA}_{\text{small}}R}^{\text{"small"}} + \mu\cdot tG \quad \hookrightarrow \text{small}$$

$$\approx \mu t G.$$

$$v = (t\cdot C)\, G^{-1}(w^T)$$

$$= (tC + \underline{\underline{err}})\, \underbrace{\underline{\underline{G^{-1}(w^T)}}}$$

$$\approx t\cdot C\cdot G^{-1}(w^T)$$

$$\approx \mu t G \circ G^{-1}(w^T) = \mu\cdot t\cdot w^T$$

$$= \mu\cdot[-s, 1]\begin{bmatrix}0\\ \vdots\\ q/2\end{bmatrix}$$

$$= \mu\cdot\frac{q}{2} \Rightarrow \text{get } \mu.$$

$\frac{q}{2}m + err.$

$\text{Eval}(f, CT_1 \ldots CT_\ell)$:

$\text{Add}(C_1, C_2)$: $C_1 + C_2$ → $(AR_1 + \mu_1 G) + (AR_2 + \mu_2 G)$

$= A(R_1 + R_2) + (\mu_1 + \mu_2)G$

$= AR_+ + (\mu_1 + \mu_2)G$

Exercise.

$\text{multiply}(\underbrace{C_1}_{n \times m}, \underbrace{C_2}_{n \times m})$:

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

$(n \times m)\ (\underline{m} \times m)$

$t \cdot C_1 G^{-1}(C_2) \overset{\sim}{=} \mu_1 t G G^{-1} C_2$

$\overset{\sim}{=} \mu_1 (t \cdot C_2)$

$\overset{\sim}{=} \mu_1 (\mu_2 t \cdot G)$

$$= (\mu_1 \mu_2)(t \cdot G)$$

Now mult. $G^{-1}(w^T)$, & get

$$(\mu_1 \mu_2)(\underbrace{t}_{(-s,1)}\, G\, \underbrace{G^{-1} w^T}_{\begin{pmatrix} 0 \\ \vdots \\ q/2 \end{pmatrix}})$$

$$\approx \mu_1 \mu_2 \left(\frac{q}{2}\right)$$

Security : $PK = A = \begin{pmatrix} B \\ b = sA + e \end{pmatrix}$

step 1: Replace A by random

$CT = AR + \mu G$

Step 2: LHL says CT random