- Scribes?
- lecture recording

Homomorphic encryption

$c_1 = Enc_{pk}(m_1)$
$c_2 = Enc_{pk}(m_2)$
} $Enc_{pk}(m_1 + m_2)$

$c = Enc_{pk}(m)$
r
} $Enc_{pk}(r \cdot m)$

El Gamal encryption: $pk: g, h = g^x \qquad g, h \in \mathbb{G}$

$Enc_{pk}(m): (g^r, h^r \cdot g^m)$

$c_1: (g^{r_1}, h^{r_1} \cdot g^{m_1})$
$c_2: (g^{r_2}, h^{r_2} \cdot g^{m_2})$
} $(g^{r_1+r_2}, h^{r_1+r_2} \cdot g^{m_1+m_2})$

$\Downarrow$

$(g^{r_1+r_2+r_3}, h^{r_1+r_2+r_3} \cdot g^{m_1+m_2})$

$P_1(a, b)$ $\qquad$ $P_2(x)$

$pk, Enc_{pk}(x)$ ←

$Enc_{pk}(ax+b)$ →

$ax+b$

Fully homomorphic encryption (FHE)

Secret-Key FHE

KeyGen : output public key pk & private key sk

SK

Enc : $Enc_{pk}(m)$ outputs ciphertext c

$Enc_{sk}(m)$ outputs c

Dec : $Dec_{sk}(c) = m$

Eval : $Eval(pk, \Pi, c_1, \ldots, c_\ell)$ - outputs a ciphertext c

$Eval(\Pi, c_1, \ldots, c_\ell)$ outputs c

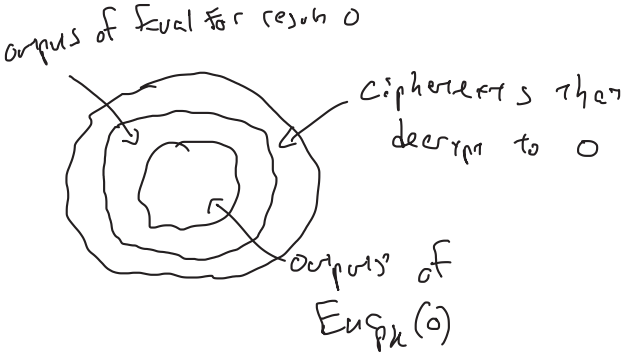
1) For all pk, sk output by KeyGen, and $m \in \{0,1\}$

$$Dec_{sk}(Enc_{pk}(m)) = m$$

2) $\forall$ pk, sk output by KeyGen, & $m_1, \ldots, m_\ell \in \{0,1\}$

$$Dec_{sk}\left(Eval_{pk}(\Pi, Enc_{pk}(m_1), \ldots, Enc_{pk}(m_\ell))\right) = \Pi(m_1, \ldots, m_\ell)$$

may be the case that Eval only supports $\Pi \in \mathcal{C}$



Leveled-FHE - supports circuits of pre-specified depth Σ

FHE is trivial!

$$\mathrm{Eval}_{pk}(\pi, c_1, \ldots, c_\ell) = (\pi, c_1, \ldots, c_\ell)$$

$$\mathrm{Dec}_{sk}(c) = \begin{cases} \text{if } c \text{ is one ciphertext, output } \mathrm{Dec}_{sk}(c) \\ \text{else parse } c = (\pi, c_1, \ldots, c_\ell), \text{ output} \\ \qquad \pi(\mathrm{Dec}_{sk}(c_1), \ldots, \mathrm{Dec}_{sk}(c_\ell)) \end{cases}$$

Additional requirements for FHE

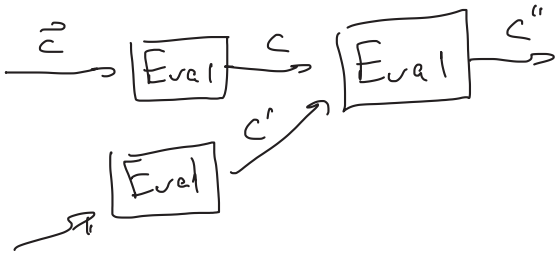
Compactness: c output by Eval should satisfy $|c| \le B(\lambda)$

Circuit privacy: output of Eval should not reveal π

$\exists$ Sim s.t. $\forall \pi$ $\mathrm{Sim}(\vec{b}, \pi(\vec{b})) \approx$

$$\{(pk, sk) \leftarrow \mathrm{KeyGen}(1^\lambda; r);\ \vec{c} \leftarrow \mathrm{Enc}_{pk}(\vec{b}; r');\ c \leftarrow \mathrm{Eval}_{pk}(\pi, \vec{c}) : (r, r', c)\}$$

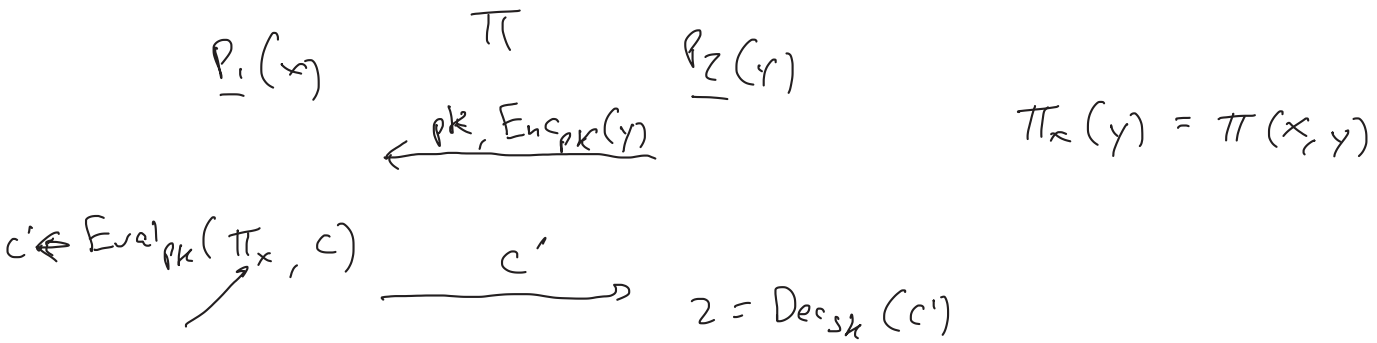
multi-hop: i-hop scheme: sequentially run Eval i times



Strongly homomorphic: output of Eval has the same distribution as outputs of Enc

---

Theorem Compact, ~~multi-hop~~ secret-key FHE $\Rightarrow$ public-key FHE



FHE constructed in two steps:

- Construct leveled-FHE
- use bootstrapping to convert leveled-FHE to FHE

Bootstrapping

Suffices to implement procedure NandEval s.t.

$$Dec_{sk}(NandEval_{pk}(c_1, c_2)) = \underline{Dec_{sk}(c_1)} \text{ NAND } \underline{Dec_{sk}(c_2)}$$

Start w/ leveled-FHE scheme $(KeyGen, Enc, Dec, Eval)$

KeyGen': run KeyGen to get pk, sk

set $c^* \leftarrow Enc_{pk}(sk)$ ← circular security

public key: (pk, c^*)

need $\pi_{c_1,c_2} \in C$

$$NandEval_{pk}(c_1, c_2) = Eval_{pk}(\pi_{c_1,c_2}, c^*)$$

$$= c \quad \{ \text{s.t. } Dec_{sk}(c) = \pi_{c_1,c_2}(sk) = Dec_{sk}(c_1 \text{ NAND } Dec_{sk}(c_2))$$

$$\pi_{c_1,c_2}(s) = \underline{Dec_s(c_1) \text{ NAND } Dec_s(c_2)}$$

GSW leveled FHE scheme

Learning w/ errors assumption

$$A,\ As+e \approx \text{uniform}$$

small coefficients

equivalently: $t = A's + e$

$[A' | t] \cdot \begin{pmatrix} s \\ -1 \end{pmatrix}$ — has small coefficients

(A = $[A' | t]$)

$[s \ -1] \cdot A$ — has small coefficients

---

intuition: encryption of a bit b is a matrix C s.t.

$$s^T \cdot C \approx b \cdot s^T$$

$$s^T \cdot C = b \cdot s^T + \lambda$$

(λ: noise)

addition works ok

C_1, C_2 s.t. $s^T \cdot C_1 = b_1 s^T + \lambda_1$

$s^T \cdot C_2 = b_2 s^T + \lambda_2$

$$\Rightarrow s^T (C_1 + C_2) = (b_1 + b_2) \cdot s^T + \underbrace{\lambda_1 + \lambda_2}_{\text{noise}}$$

multiplication?

$$s^T \cdot (C_1 C_2) = (b_1 s^T + \lambda_1) \cdot C_2$$

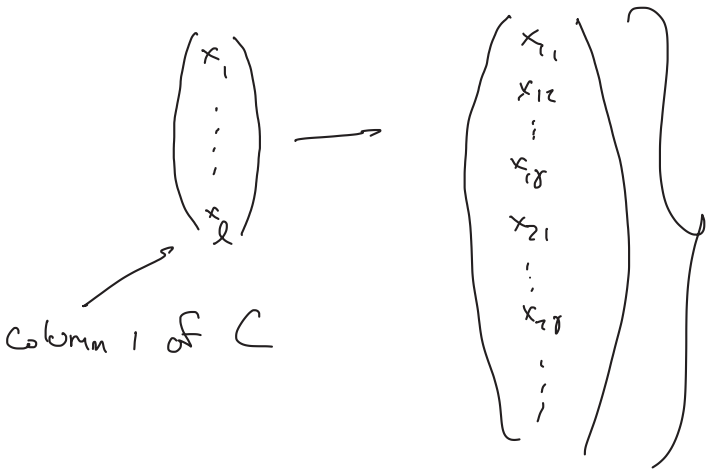
$$= b_1 (b_2 s^T + \lambda_2) + \lambda_1 C_2$$

$$= \underline{b_1 b_2} s^T + \underbrace{b_1 \lambda_2 + \lambda_1 C_2}_{\text{noise}}$$

"flattening gadget"

$G^{-1}(C) \rightarrow$ map coefficients of G_2 to binary rep.

$\gamma = \lceil \log q \rceil$



$\exists\ G$ s.t. $G \cdot G^{-1}(C) = C$

$$G = \begin{bmatrix} 1\ 2\ 4 \cdots 2^{\gamma} & 0 & \cdots & 0 \\ 0 & 1\ 2\ 4 \cdots 2^{\gamma} & & \\ & & \ddots & \end{bmatrix} \begin{pmatrix} x_{11} \\ \vdots \\ x_{1\gamma} \\ \vdots \end{pmatrix} = \begin{bmatrix} x_1 \\ \vdots \\ x_l \end{bmatrix}$$