CSCI 1510

This Lecture:

- Somewhat Homomorphic Encryption from LWE (GSW)
- Bootstrapping SWHE to FHE
- Program Obfuscation

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE) from LWE (GSW)

Step 2: Bootstrapping

Post-Quantum Assumption: Learning With Errors (LWE)

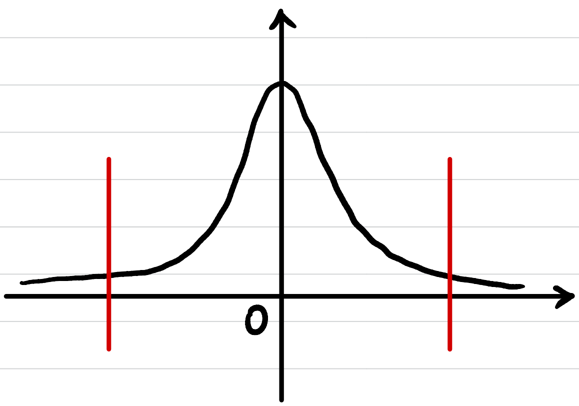
n: security parameter

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

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

χ: distribution over $\mathbb{Z}_q$

(concentrated on "small integers")

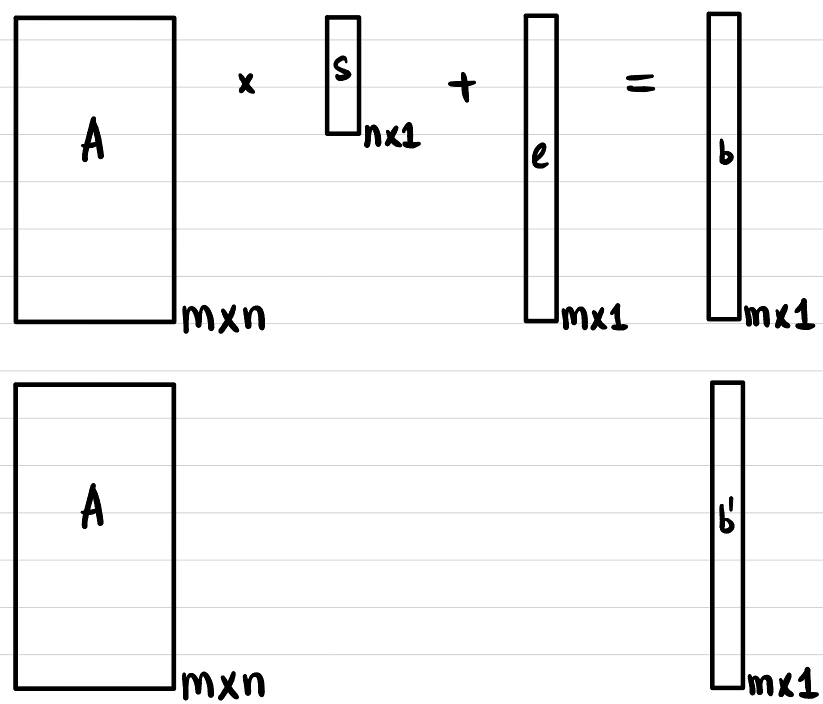


$$\Pr\left[\,|e| > \alpha \cdot q \;\middle|\; e \leftarrow \chi\,\right] \le \mathrm{negl}(n)$$

$\alpha \ll 1$

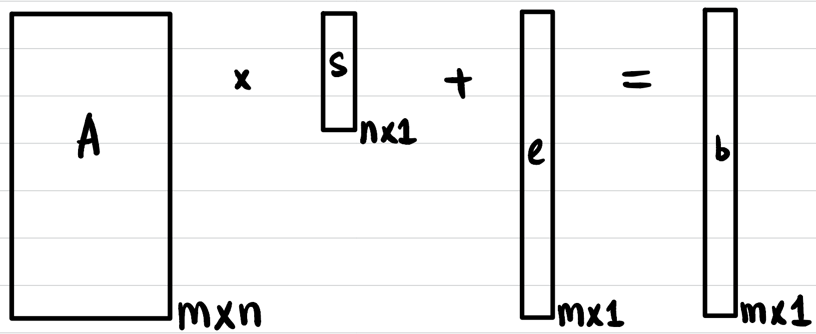
Def We say the decisional $\mathrm{LWE}_{n,m,q,\chi}$ problem is (quantum) hard if $\forall$ (quantum) PPT $\mathcal{A}$, $\exists$ negligible function $\varepsilon(\cdot)$ s.t.

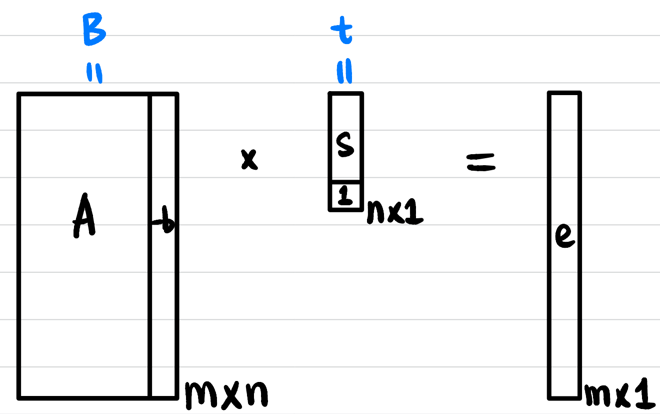
$$\left| \Pr\left[\begin{array}{l} A \xleftarrow{\$} \mathbb{Z}_q^{m\times n} \\ s \xleftarrow{\$} \mathbb{Z}_q^{n} \\ e \leftarrow \chi^m \end{array} : \mathcal{A}(A, [As+e \bmod q]) = 1 \right] - \Pr\left[\begin{array}{l} A \xleftarrow{\$} \mathbb{Z}_q^{m\times n} \\ b' \xleftarrow{\$} \mathbb{Z}_q^{m}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



Regev Encryption from LWE

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





$pk = (A, b)$

$sk = s$

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

$sk = t_{n\times 1}$

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

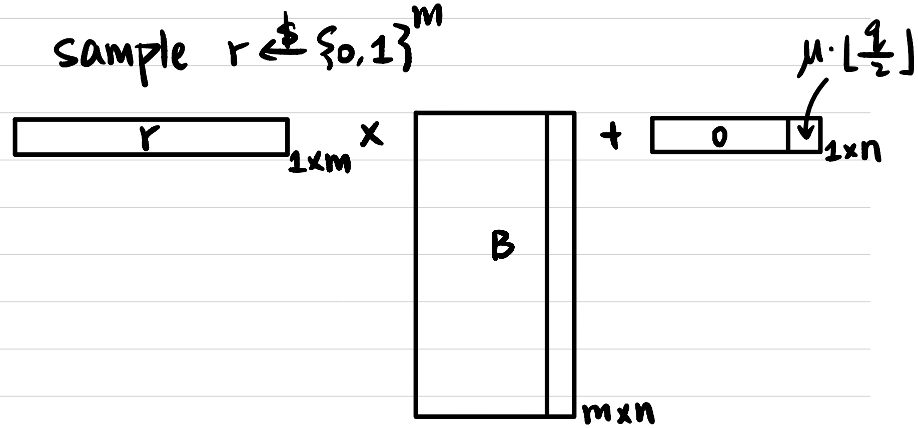
sample a random $S \subseteq [m]$

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

i-th row of A

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

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



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

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

small noise

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

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

Regev Encryption from LWE

Homomorphism:

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

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

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)

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

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

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

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

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

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

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?

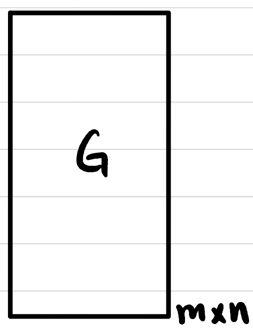
$C_1 \cdot C_2$?

SWHE from LWE (GSW)

Attempt 2 (secret-key)

Flattering Gadget:

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

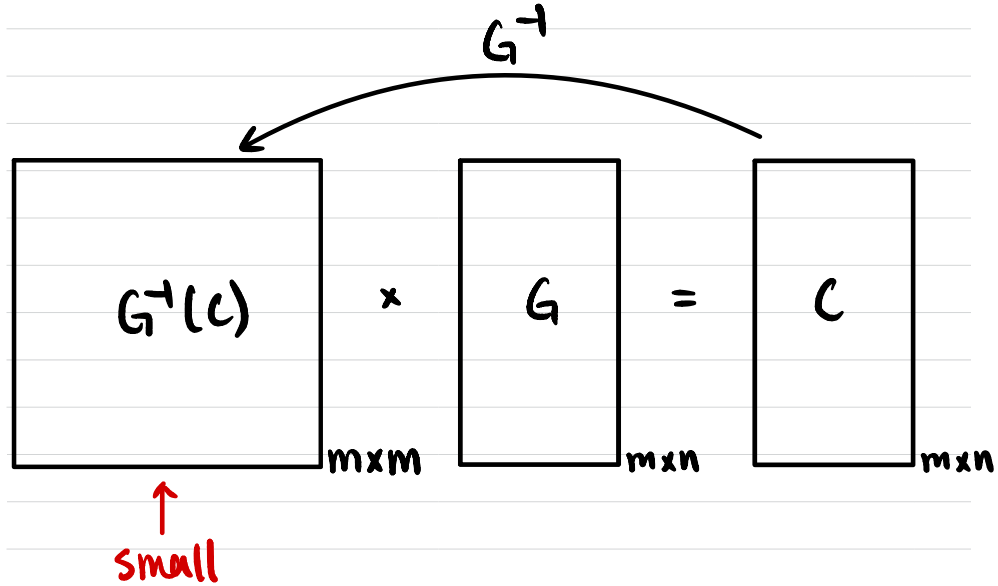


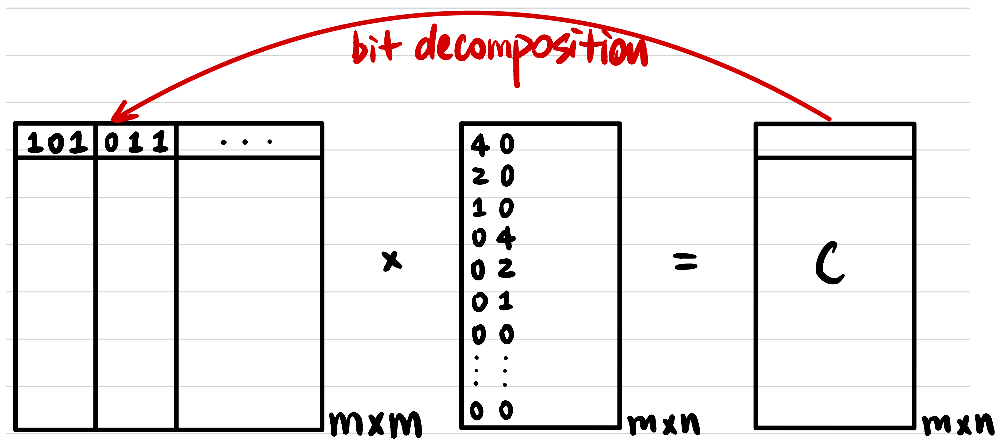
Inverse transformation

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

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

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





SWHE from LWE (GSW)

Attempt 2 (secret-key)

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

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

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

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

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

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

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 ?

SWHE from LWE (GSW)

Attempt 3 (public-key)

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

public key: "encryptions of 0"

$$\left\{ C_0^i \in \mathbb{Z}_q^{m\times n} \;\middle|\; C_0^i \cdot \vec{t} = \text{small} \right\}_{i\in[n]}$$

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

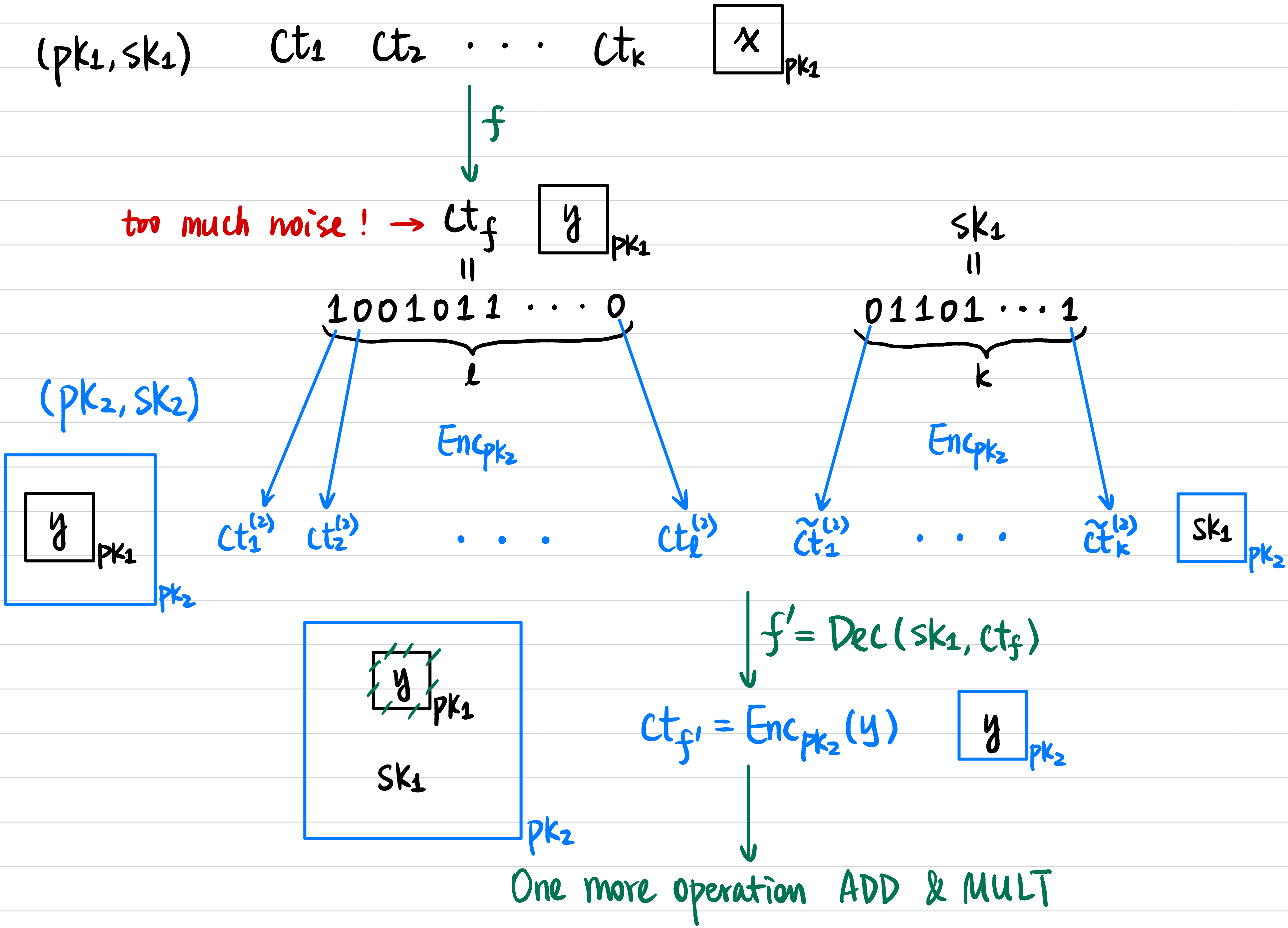
$$C = (\text{random subset sum of } C_0^i\text{'s}) + \mu \cdot G$$

gadget matrix

Step 2: Bootstrapping

$$
\begin{tikzcd}
ct_1 \quad ct_2 \quad \cdots \quad ct_k \arrow[d, "f"] & & \boxed{x} \arrow[d, "f"] \\
ct_f \leftarrow \text{too much noise!} \arrow[d, "\mathrm{Dec}"] & & \boxed{y} \arrow[d, "\mathrm{Dec}"] & y = f(x) \\
y \arrow[d, "\mathrm{Enc}"] & & y \arrow[d, "\mathrm{Enc}"] \\
ct_y \leftarrow \text{fresh noise!} & & \boxed{y}
\end{tikzcd}
$$

Leveled FHE



(pk1, sk1)
ct1 ct2 . . . ctk
x
pk1
f
too much noise ! → ctf
y
pk1
=
1001011 . . . 0
ℓ
sk1
=
01101 . . . 1
k
(pk2, sk2)
y
pk1
pk2
Encpk2
ct1(2) ct2(2) . . . ctℓ(2)
Encpk2
c̃t1(2) . . . c̃tk(2)
sk1
pk2
y
pk1
sk1
pk2
f′ = Dec(sk1, ctf)
ctf′ = Encpk2(y)
y
pk2
One more operation ADD & MULT

Step 2: Bootstrapping

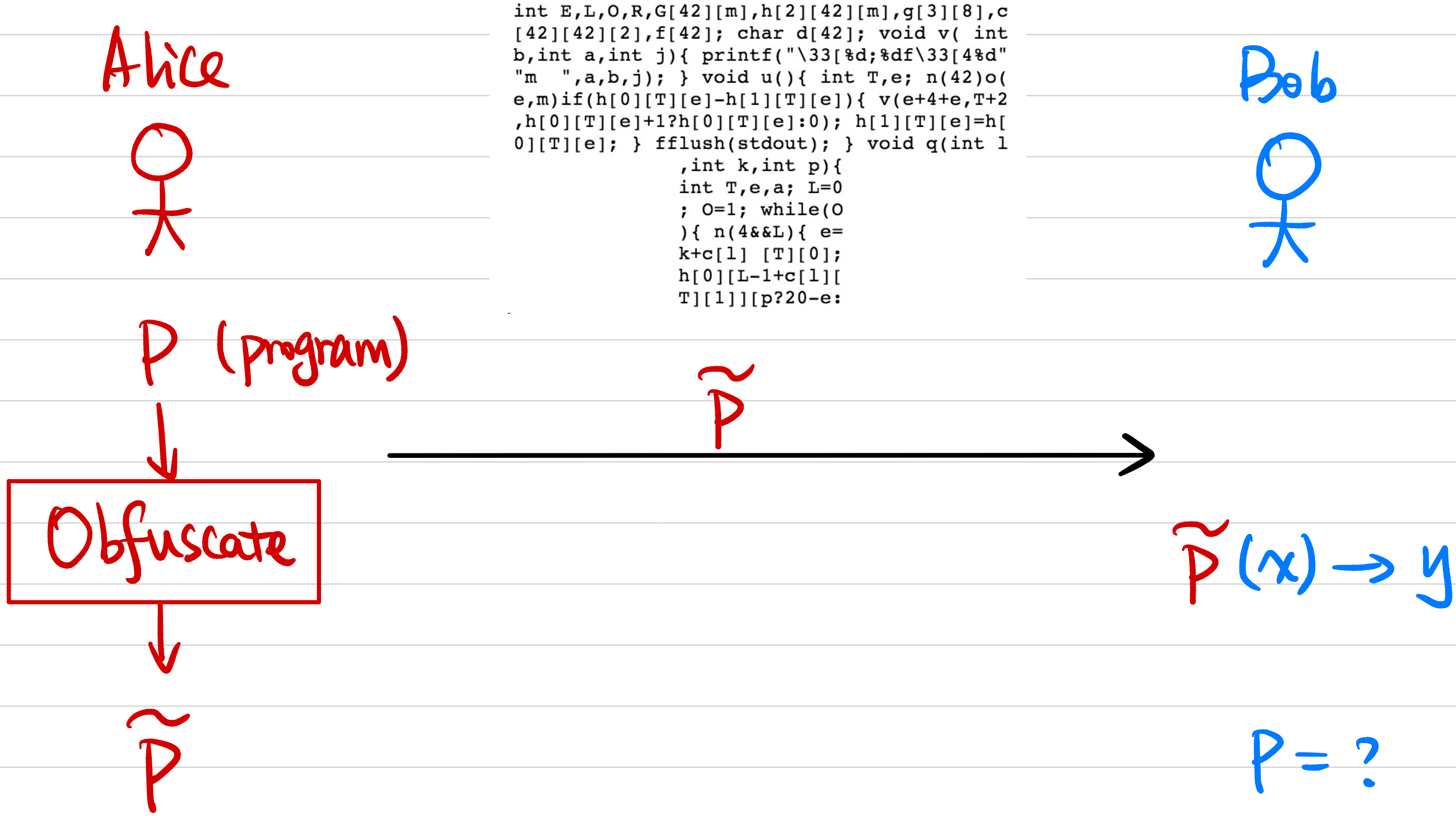
Leveled FHE: pk_1, pk_2, pk_3, . . . , pk_n

$Enc_{pk_2}(sk_1)$ $Enc_{pk_3}(sk_2)$ $Enc_{pk_n}(sk_{n-1})$

FHE: pk, $Enc_{pk}(sk)$

"circular secure" assumption

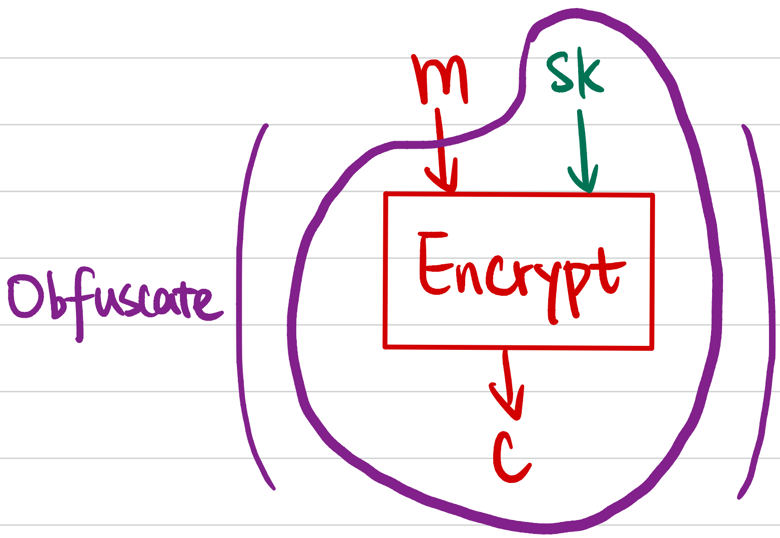
Program Obfuscation

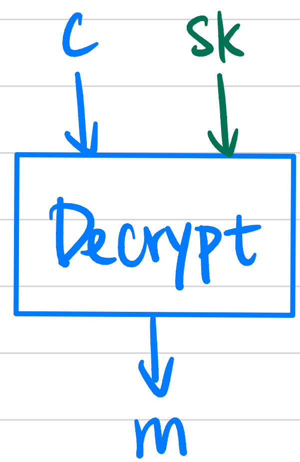



```
int E,L,O,R,G[42][m],h[2][42][m],g[3][8],c
[42][42][2],f[42]; char d[42]; void v( int
b,int a,int j){ printf("\33[%d;%df\33[4%d"
"m  ",a,b,j); } void u(){ int T,e; n(42)o(
e,m)if(h[0][T][e]-h[1][T][e]){ v(e+4+e,T+2
,h[0][T][e]+1?h[0][T][e]:0); h[1][T][e]=h[
0][T][e]; } fflush(stdout); } void q(int l
               ,int k,int p){
               int T,e,a; L=0
               ; O=1; while(O
               ){ n(4&&L){ e=
               k+c[l] [T][0];
               h[0][L-1+c[l][
               T][1]][p?20-e:
```

Goal: Make the program "unintelligible" without affecting its functionality.

Symmetric-Key to Public-Key



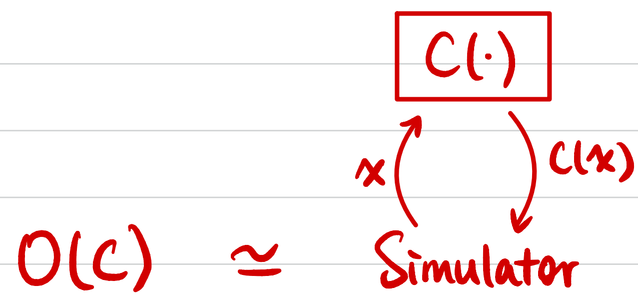


Formal Definition: Virtual Black Box (VBB)

Obfuscator O: $\quad C \xrightarrow{O} O(C)$

- **Functionality:** $O(C)$ computes the same function as C.
- **Polynomial Slowdown:** $|O(C)| \leq \text{poly}(n) \cdot |C|$
- **Security (Virtual Black Box):**

  $\forall$ PPT A, $\exists$ PPT S, s.t. $\forall C$, $\quad A(O(C)) \overset{c}{\simeq} S^{C(\cdot)}(1^{|C|})$.



Thm VBB obfuscator for all poly-sized circuits is impossible to achieve.

Formal Definition: Indistinguishability Obfuscation (iO)

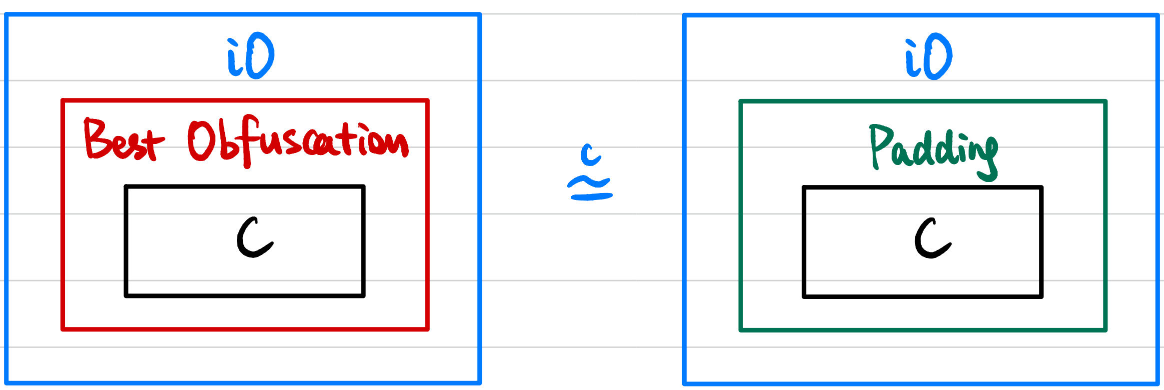
Obfuscator O: $C \xrightarrow{O} O(C)$

- **Functionality:** $O(C)$ computes the same function as C.
- **Polynomial Slowdown:** $|O(C)| \leq poly(n) \cdot |C|$
- **Security (indistinguishability obfuscation):**

  If C_0 & C_1 compute the same function and $|C_0| = |C_1|$,

  then $O(C_0) \overset{c}{\approx} O(C_1)$

- **Best Possible Obfuscation**



Is it possible?

- 2001: Notion introduced
- 2013: Fist "candidate" construction from multilinear maps
- 2013-2020: Attack, fixes, new constructions from new assumptions
- 2020: New construction from well-founded assumptions

PKE from iO

Let $G: \{0,1\}^n \to \{0,1\}^{2n}$ be a length-doubling PRG.

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

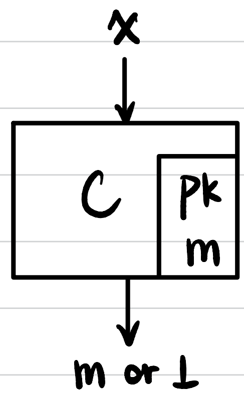
  $sk \xleftarrow{\$} \{0,1\}^n$

  $pk := G(sk)$

- $\mathrm{Enc}_{pk}(m)$:

  $$C_{pk,m}(x) := \begin{cases} m & \text{if } G(x) = pk \\ \perp & \text{otherwise} \end{cases}$$

  Output $c \leftarrow iO(C_{pk,m})$



- $\mathrm{Dec}_{sk}(c)$: ?

<u>Thm</u> If G is a PRG and $iO(\cdot)$ is an idistinguishability obfuscator, then this PKE scheme is CPA-secure.