

CSCI 1515 Applied Cryptography

This Lecture:

- Private Information Retrieval
- Bootstrapping SWHE to FHE
- Secure Hardware: Intel SGX, HSM

Fully Homomorphic Encryption (FHE)

$$\begin{array}{l} \text{Enc}(m_1) \\ \text{Enc}(m_2) \end{array} \begin{array}{c} \searrow \\ \nearrow \end{array} \text{Enc}(m_1 + m_2)$$

Additively Homomorphic

$$\begin{array}{l} \text{Enc}(m_1) \\ \text{Enc}(m_2) \end{array} \begin{array}{c} \searrow \\ \nearrow \end{array} \text{Enc}(m_1 \cdot m_2)$$

Multiplicatively Homomorphic

$$\begin{array}{c} c \\ \text{Enc}(m) \end{array} \begin{array}{c} \searrow \\ \nearrow \end{array} \text{Enc}(c \cdot m)$$

Homomorphic Scalar Multiplication

FHE Constructions

Step 1: Somewhat Homomorphic Encryption (SWHE)

- over Integers
- from RLWE (BFV)

Step 2: Bootstrapping

Application: Privacy-Preserving Query

Server



Client



Query x

Key sk

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

ct

Search / ML / GPT / ...



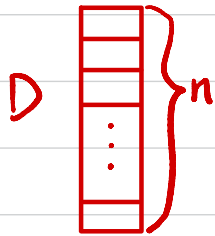
$ct' \leftarrow \text{Eval}(f, ct)$

ct'

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

Application: Private Information Retrieval (PIR)

Server



Client



WANT: $D[i]$

While hiding i against Server

Query i

Key sk

$ct \leftarrow \text{Enc}(i)$

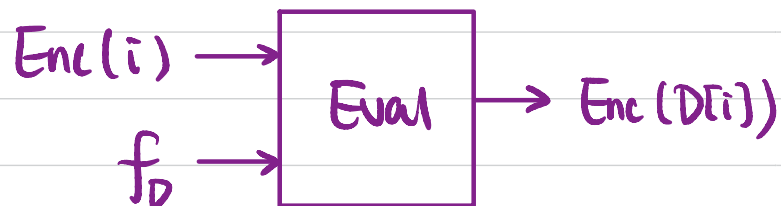
$\xleftarrow{ct}$

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

$\uparrow$
 $f_D(i) = D[i]$

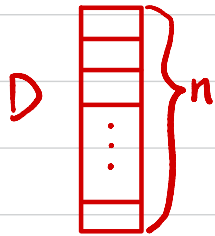
$\xrightarrow{ct'}$

$D[i] \leftarrow \text{Dec}_{sk}(ct')$



Private Information Retrieval (PIR)

Server



Client



WANT: $D[i]$

While hiding i against Server

Trivial Solution:

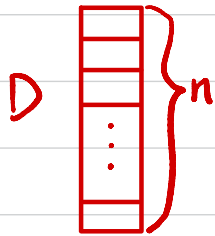


Communication complexity $O(n)$

Goal: Communication complexity $o(n)$

Private Information Retrieval (PIR)

Server



Homomorphic
Scalar Mult

$$ct' \leftarrow \sum_{i=1}^n D[i] \cdot ct_i$$

Homomorphic Add

Client



$$ct_1 \leftarrow \text{Enc}(0)$$

$\vdots$

$$ct_{i-1} \leftarrow \text{Enc}(0)$$

$$ct_i \leftarrow \text{Enc}(1)$$

$$ct_{i+1} \leftarrow \text{Enc}(0)$$

$\vdots$

$$\leftarrow ct_n \leftarrow \text{Enc}(0)$$

WANT: $D[i]$

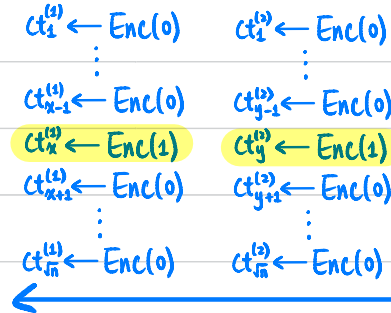
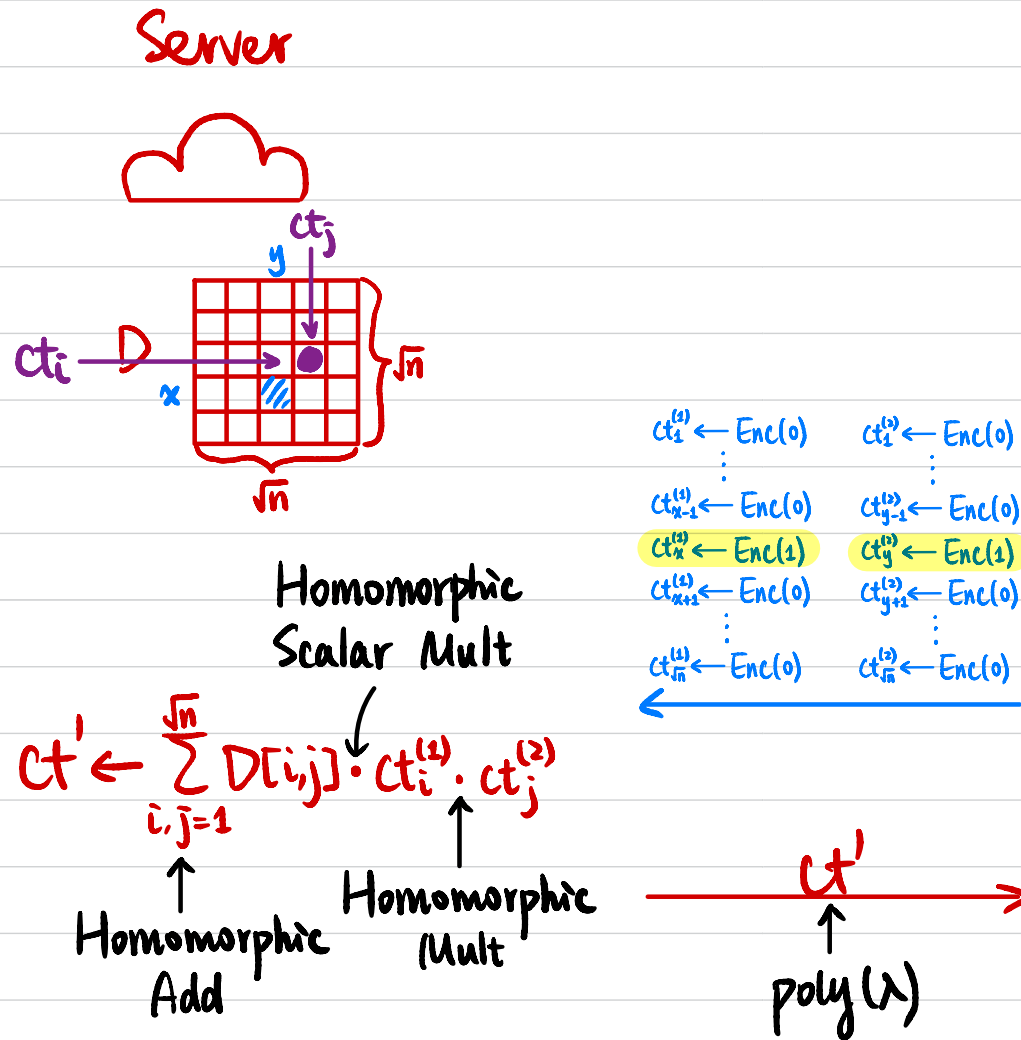
While hiding i against Server

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

$\uparrow$
 $\text{poly}(\lambda)$

$$D[i] = \text{Dec}(ct')$$

Private Information Retrieval (PIR)



$$D[x, y] = \text{Dec}(ct')$$

Extend to dimension d ?

Homomorphic Mult = ?

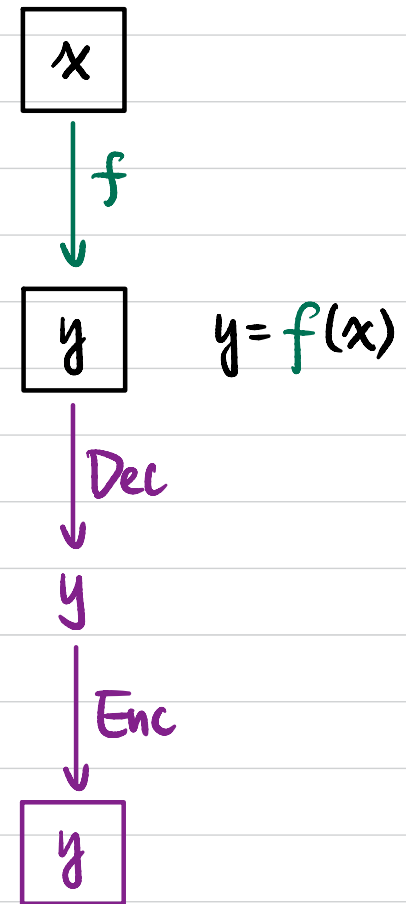
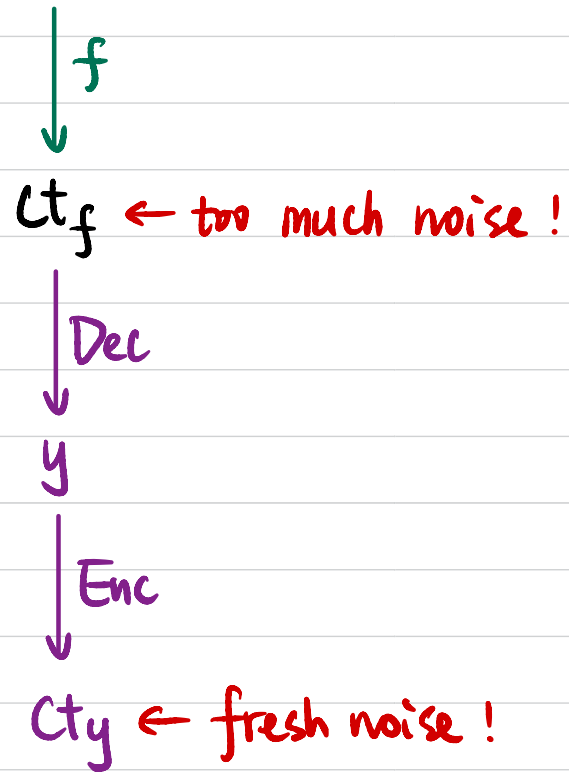
Homomorphic Scalar Mult = ?

Homomorphic Add = ?

Communication = ?

Step 2: Bootstrapping

$ct_1 \quad ct_2 \quad \dots \quad ct_n$



Leveled FHE

(pk_1, sk_1) ct_1 ct_2 $\dots$ ct_n $\boxed{x}_{pk_1}$

too much noise ! $\rightarrow$ ct_f $\boxed{y}_{pk_1}$

||

1001011 ... 0

l

Enc_{pk_2}

$ct_1^{(2)}$

$ct_2^{(2)}$

...

$ct_l^{(2)}$

sk_1

||

01101 ... 1

k

Enc_{pk_2}

$\tilde{ct}_1^{(2)}$

...

$\tilde{ct}_k^{(2)}$

sk_1

pk_2

(pk_2, sk_2)

$\boxed{y}_{pk_1}$

pk_2

$\boxed{\boxed{y}_{pk_1}}_{pk_2}$

sk_1

pk_2

$f' = Dec(sk_1, ct_f)$

$ct_{f'} = Enc_{pk_2}(y)$ $\boxed{y}_{pk_2}$

One more operation ADD & MULT

Step 2: Bootstrapping

Leveled FHE: $pk_1, pk_2, pk_3, \dots, pk_n$
 $Enc_{pk_2}(sk_1) \quad Enc_{pk_3}(sk_2) \quad \dots \quad Enc_{pk_n}(sk_{n-1})$

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

"circular secure" assumption

Outsourcing Computation by FHE

Server



ct

f



Memory



cpu



Public
Eval

← ct, f

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

→ ct'

Client



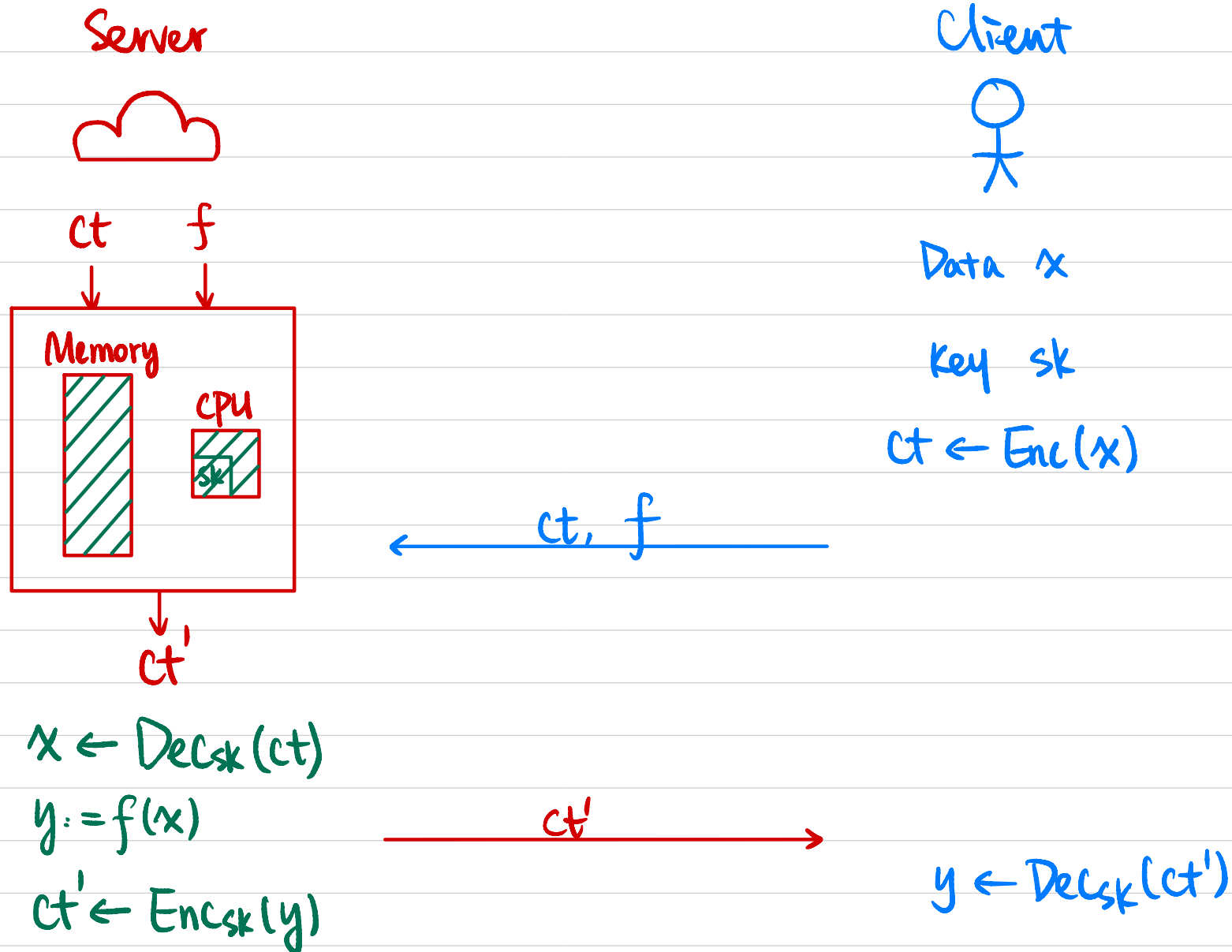
Data x

Key sk

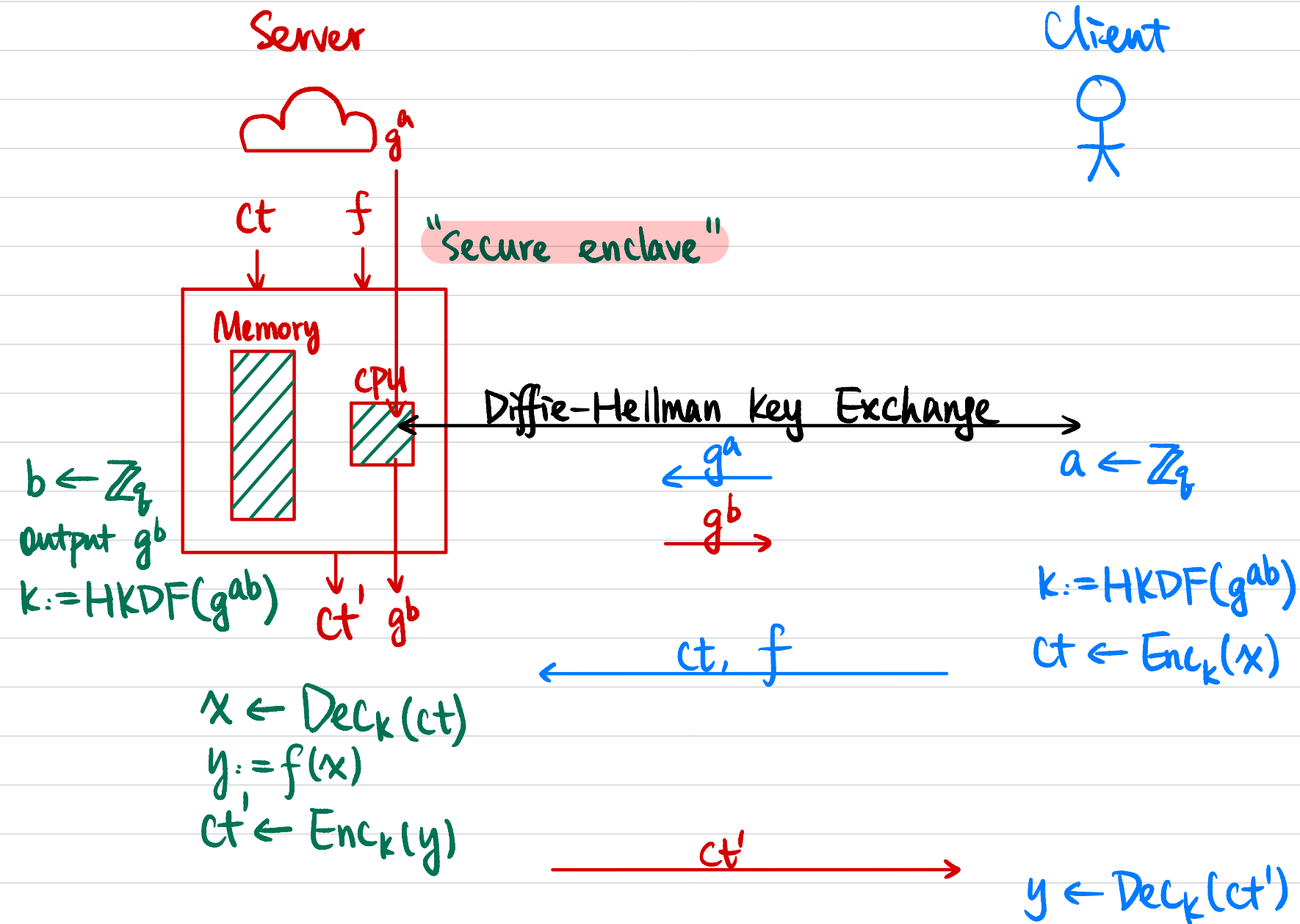
$ct \leftarrow \text{Enc}(x)$

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

Outsourcing Computation by Secure Hardware

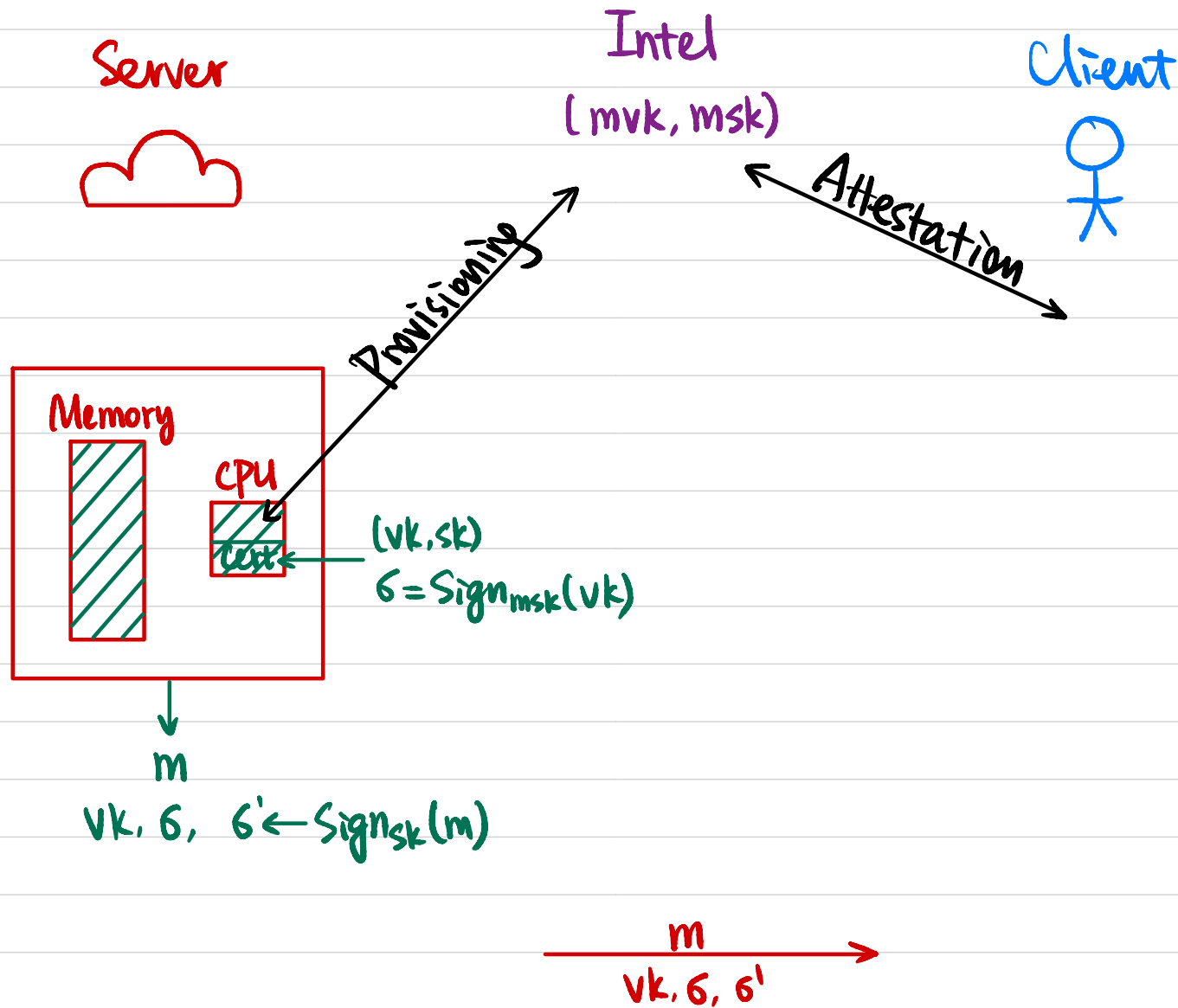


Intel Software Guard Extension (SGX)



What could go wrong?

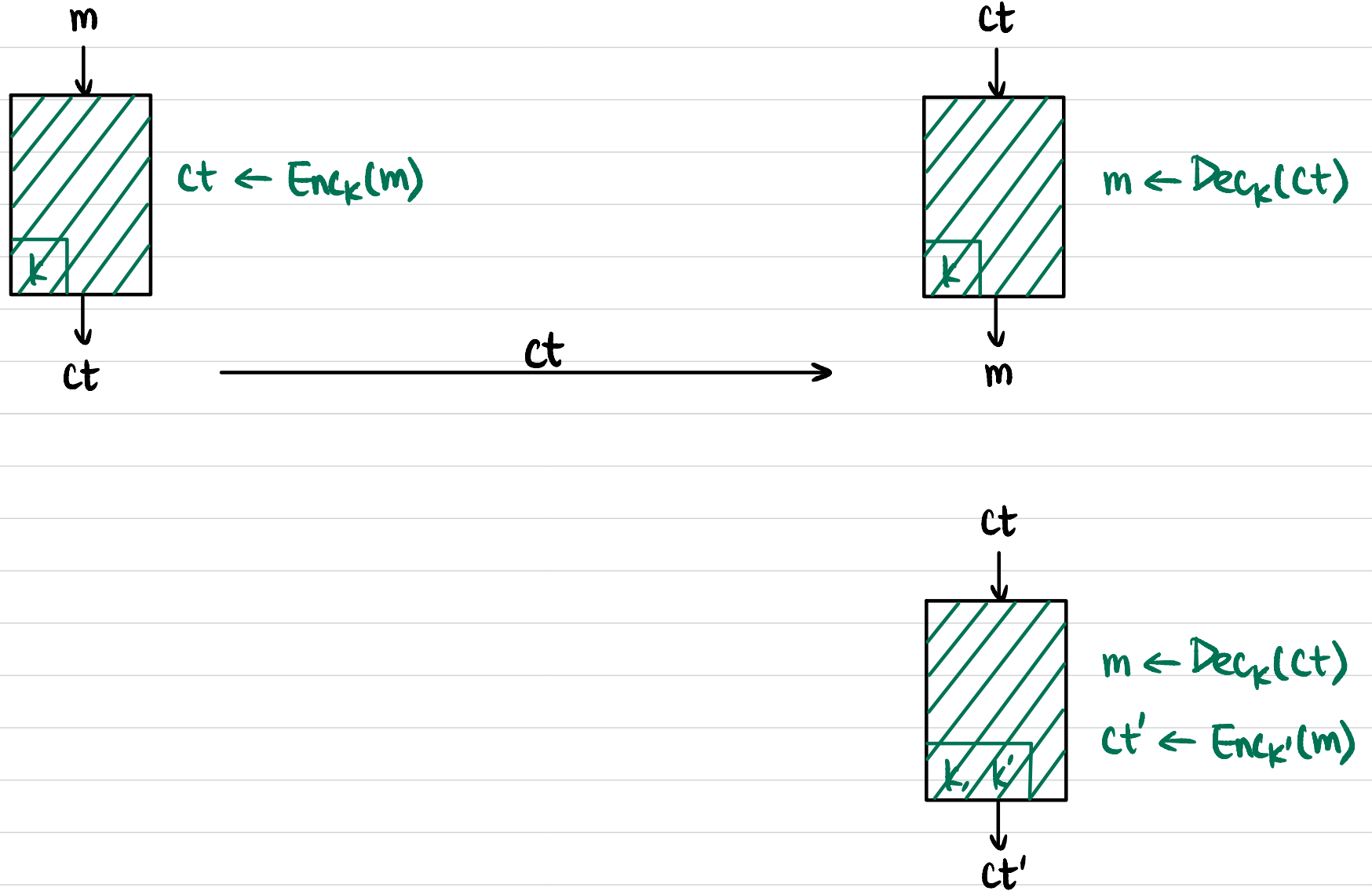
Intel Software Guard Extension (SGX)



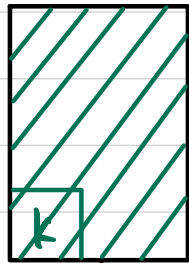
Constraints & Attacks

- Trust in hardware
- Trust in Intel
- Limited memory size: 128 MB
- Replay attacks
- Side-channel attacks : memory access pattern
 - ↳ fix: Oblivious RAM (ORAM)
 - overhead $\Theta(\log N)$

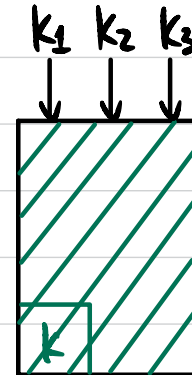
Hardware Secure Module (HSM)



Key Agreement



Sample k_1, k_2, k_3 s.t.
 $k_1 \oplus k_2 \oplus k_3 = K$



$K := k_1 \oplus k_2 \oplus k_3$

