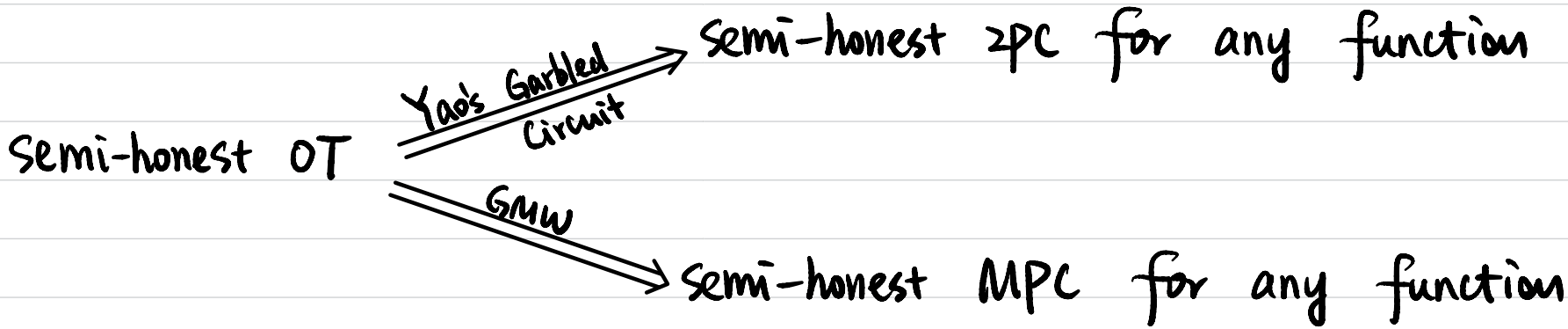
CSCI 1515 Applied Cryptography

This Lecture:

- GMW Compiler: Malicious MPC for Any Funtion
- Cut-and-Choose: Malicious 2PC for Any Funtion
- Private Set Intersection (PSI)


semi-honest OT
Yao's Garbled Circuit
semi-honest 2PC for any function
GMW
semi-honest MPC for any function

Putting it Together: Semi-Honest 2PC

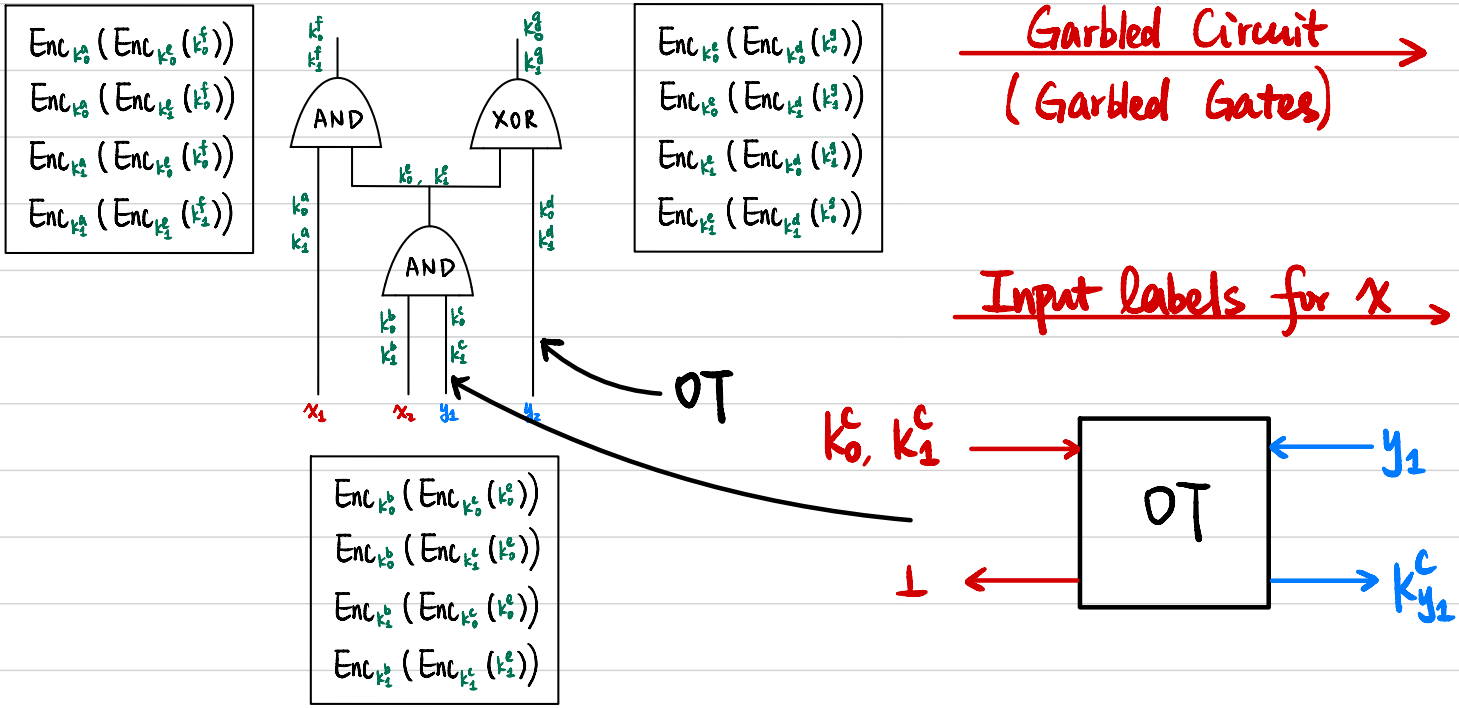
What could go wrong against malicious adversaries?

Alice (Garbler)

$x \in \{0,1\}^2$

Bob (Evaluator)

$y \in \{0,1\}^2$



Garbled Circuit (Garbled Gates)

Input labels for x

Input labels for y?

- Output labels?

  Evaluator sends k^f, k^g back to garbler

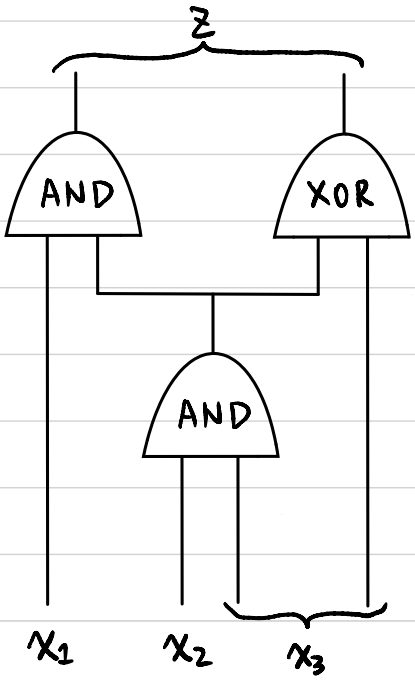
- How to decide which ciphertext to decrypt?

Shuffle

- $\mathrm{Enc}_{k_0^b}(\mathrm{Enc}_{k_0^c}(k_0^e \| \overbrace{0 \cdots 0}^{\lambda}))$ → garbage
- $\mathrm{Enc}_{k_0^b}(\mathrm{Enc}_{k_1^c}(k_0^e \| 0 \cdots 0))$ → $k_0^e \| 0 \cdots 0$
- $\mathrm{Enc}_{k_1^b}(\mathrm{Enc}_{k_0^c}(k_0^e \| 0 \cdots 0))$ → garbage
- $\mathrm{Enc}_{k_1^b}(\mathrm{Enc}_{k_1^c}(k_1^e \| 0 \cdots 0))$ → garbage

2λ

MPC for any function with $t \leq n-1$ (GMW)



Each party P_i holds a random share $v_i^w \in \{0,1\}$ s.t. $\bigoplus_{i=1}^{n} v_i^w = v^w$

Inputs:

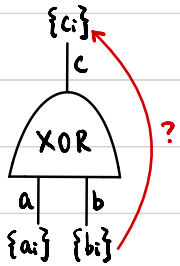
For each input wire w:

If it's from party P_k with input value $v^w \in \{0,1\}$.

P_k randomly samples $v_i^w \xleftarrow{\$} \{0,1\}$ s.t. $\bigoplus_{i=1}^{n} v_i^w = v^w$

↳ Sends v_i^w to party P_i.

XOR gates:

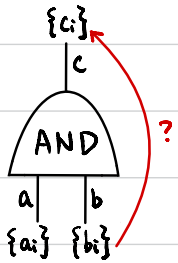


GIVEN: $\bigoplus_{i=1}^{n} a_i = a$ $\bigoplus_{i=1}^{n} b_i = b$

WANT: $\{c_i\}$ s.t. $\bigoplus_{i=1}^{n} c_i = c = a \oplus b$

$c_i = a_i \oplus b_i$

AND gates:



GIVEN: $\bigoplus_{i=1}^{n} a_i = a$ $\bigoplus_{i=1}^{n} b_i = b$

WANT: $\{c_i\}$ s.t. $\bigoplus_{i=1}^{n} c_i = c = a \cdot b$

$c_i = ?$

$$a \cdot b = \left(\sum_{i=1}^{n} a_i\right) \cdot \left(\sum_{i=1}^{n} b_i\right) \mod 2$$

$$= \left(\sum_{i=1}^{n} a_i \cdot b_i\right) + \left(\sum_{i \neq j} a_i \cdot b_j\right) \mod 2$$

P_i locally — Reshare

Outputs:

For each output wire w:

Each party P_i holds a random share $v_i^w \in \{0,1\}$

↳ Sends v_i^w to all parties

Each party computes the value $v^w = \bigoplus_{i=1}^{n} v_i^w$

MPC for any function with $t \le n-1$ (GMW)

Yao:

Computational Complexity?

$O(\#\text{AND} \cdot n)$ for each party

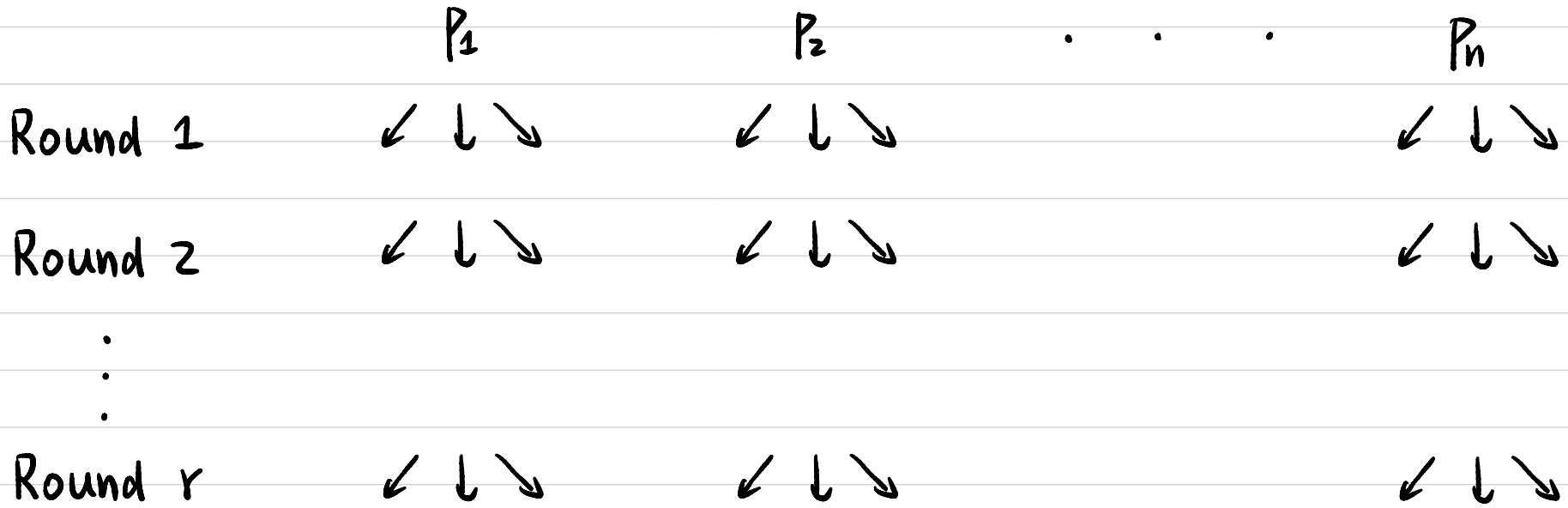
$O(\#\text{inputs})$ OTs + $O(\#\text{AND})$ AES

Communication Complexity?

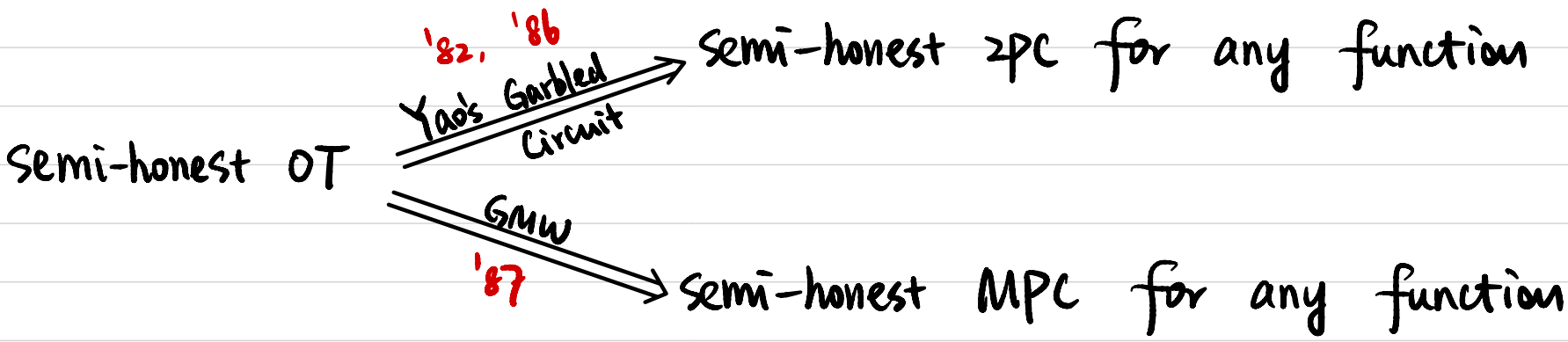
$O(\#\text{AND} \cdot n^2)$ in total

$O(\#\text{inputs} + \#\text{AND})$

Round Complexity? $O(\text{depth of AND gates})$ $O(1)$



What could go wrong against malicious adversaries?



How to compare ?

Yao's Garbled Circuit	Goldreich-Micali-Wigderson
+ malicious security lower overhead	
+ # OTs : # inputs	- # OTs : #AND · n^2
+ O(1) rounds of communication	- O(depth of AND gates)
- only 2PC	+ Any # of parties
- only Boolean circuits	+ Extendable to arithmetic circuits $\mathbb{Z}_2 \to \mathbb{Z}_p$

Feasibility Results

Computational Security:

Semi-honest Oblivious Transfer (OT)

semi-honest MPC for any function with $t<n$

malicious MPC for any function with $t<n$

GMW Compiler

Given a semi-honest protocol:

Once inputs & randomness are fixed, protocol is **deterministic**.

Step 1: Each party P_i commits to its input x_i & randomness r_i to be used in the semi-honest protocol.

x_i: x_i'

r_i: $\bigoplus_{j=1}^{n} r_i^j$

$r_i := H(\text{messages} \| \underbrace{\text{seed}}_{\lambda})$

Step 2: Run semi-honest protocol.

Along with every message, prove in ZK that the message is computed correctly (based on its input, randomness, transcript so far)

Cut-and-Choose for Garbled Circuits

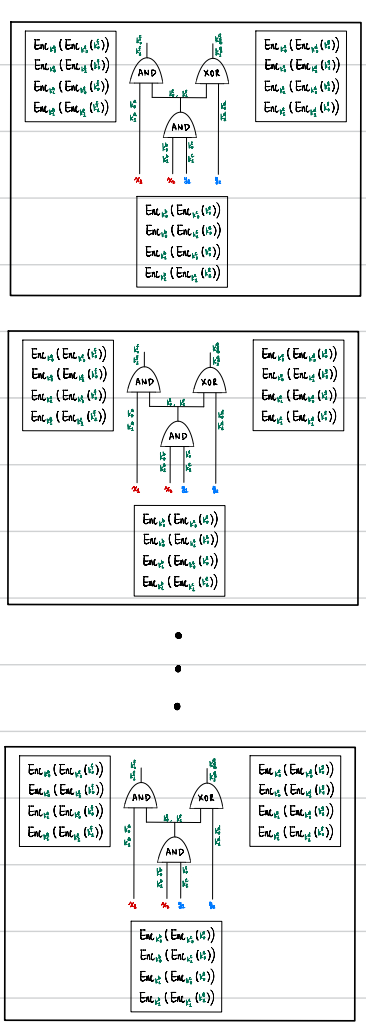
Alice (Garbler)

$x \in \{0,1\}^2$

Bob (Evaluator)

$y \in \{0,1\}^2$

λ



λ Garbled Circuits (Garbled Gates) →

← Randomly pick $(\lambda-1)$ of them

Reveal all the labels for the $(\lambda-1)$ GCs →

Verify correctness

↓

Continue with the remaining GC

If Alice generated 1 GC incorrectly,

$\Pr[\text{Alice caught}] = 1 - \frac{1}{\lambda}$

↑

WANT: negligible

Cut-and-Choose for Garbled Circuits

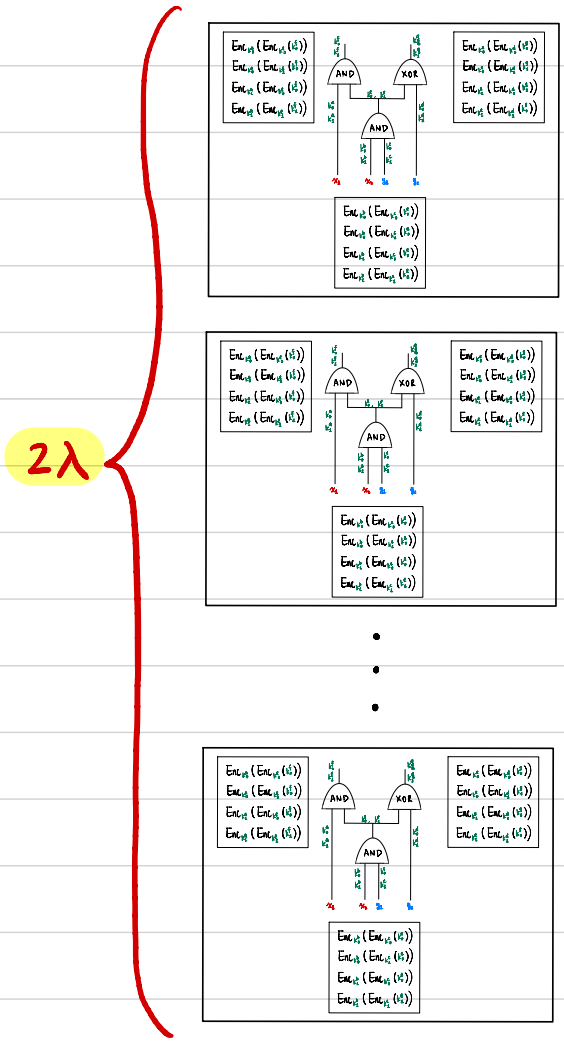
Alice (Garbler)

$x \in \{0,1\}^2$

Bob (Evaluator)

$y \in \{0,1\}^2$

2λ Garbled Circuits (Garbled Gates) →



← Randomly pick λ of them

Reveal all the labels for the λ GCs →

Verify correctness

↓

Continue with the remaining λ GCs ⇒ Take majority

If Alice generated $\geq \frac{\lambda}{2}$ GCs incorrectly,

$\Pr[\text{Alice caught}] \geq 1 - \text{negl}.$

$$\Pr[\text{Alice passed}] = \frac{2\lambda - \frac{\lambda}{2}}{2\lambda} \cdot \frac{2\lambda - \frac{\lambda}{2} - 1}{2\lambda - 1} \cdots \frac{\frac{\lambda}{2} + 1}{\lambda + 1} \leq \left(\frac{3}{4}\right)^{\lambda}$$

Private Set Intersection (PSI)

Input: $X = \{x_1, x_2, \cdots, x_n\}$

$V = \{v_1, v_2, \cdots, v_n\}$

Input: $Y = \{y_1, y_2, \cdots, y_n\}$

PSI: $f(X, Y) = X \cap Y$

PSI-CA: $f(X, Y) = |X \cap Y|$

PSI-SUM: $f((X, V), Y) = |X \cap Y|, \sum_{i : x_i \in Y} v_i$

Private Set Intersection (PSI)

Input: $X = \{x_1, x_2, \cdots, x_n\}$

Input: $Y = \{y_1, y_2, \cdots, y_n\}$

$H(x_1), \cdots, H(x_n)$ →

$H(y_1), \cdots, H(y_n)$

⇓

$X \cap Y$

$x' \in X$?

$H(x')$ ←

Is it (semi-honest) secure?

No! Dictionary Attack

Is it possible to achieve 2PC / MPC with 1 round of communication?

No! It allows Bob to learn $f(x, y)$ on any y.

DDH-based PSI

Cyclic group G of order q with generator g, where DDH holds.

$H: \{0,1\}^* \to G$ (modeled as Random Oracle)

Input: $X = \{x_1, x_2, \cdots, x_n\}$

$k_A \xleftarrow{\$} \mathbb{Z}_q$

Input: $Y = \{y_1, y_2, \cdots, y_n\}$

$k_B \xleftarrow{\$} \mathbb{Z}_q$

$\leftarrow \quad H(Y)^{k_B} := \{H(y_1)^{k_B}, \cdots, H(y_n)^{k_B}\}$

$H(X)^{k_A}, \quad H(Y)^{k_A \cdot k_B} \quad \rightarrow$

$H(X)^{k_A \cdot k_B} \cap H(Y)^{k_A \cdot k_B}$

$\Downarrow$

$X \cap Y$

$x' \in X ?$

$H(x')^{k_A} ?$

Is it (semi-honest) secure?

PSI-CA?

PSI-CA: $f(X,Y) = |X \cap Y|$

Input: $X = \{x_1, x_2, \cdots, x_n\}$

$k_A \xleftarrow{\$} \mathbb{Z}_q$

Input: $Y = \{y_1, y_2, \cdots, y_n\}$

$k_B \xleftarrow{\$} \mathbb{Z}_q$

$$\xleftarrow{H(Y)^{k_B} := \{H(y_1)^{k_B}, \cdots, H(y_n)^{k_B}\}}$$

$$\xrightarrow{H(X)^{k_A}, \{H(Y)^{k_A \cdot k_B}\}}$$

Shuffle

$H(X)^{k_A \cdot k_B} \cap H(Y)^{k_A \cdot k_B}$

$\downarrow$

$|X \cap Y|$

PSI-SUM?

PSI-SUM: $f((X, V), Y) = |X \cap Y|, \sum_{i : x_i \in Y} v_i$

Input: $X = \{x_1, x_2, \cdots, x_n\}$

$V = \{v_1, v_2, \cdots, v_n\}$

Input: $Y = \{y_1, y_2, \cdots, y_n\}$

$k_A \xleftarrow{\$} \mathbb{Z}_q$

$k_B \xleftarrow{\$} \mathbb{Z}_q$

$\leftarrow H(Y)^{k_B} := \{H(y_1)^{k_B}, \cdots, H(y_n)^{k_B}\}$

$H(x)^{k_A}, \; H(Y)^{k_A \cdot k_B} \rightarrow$