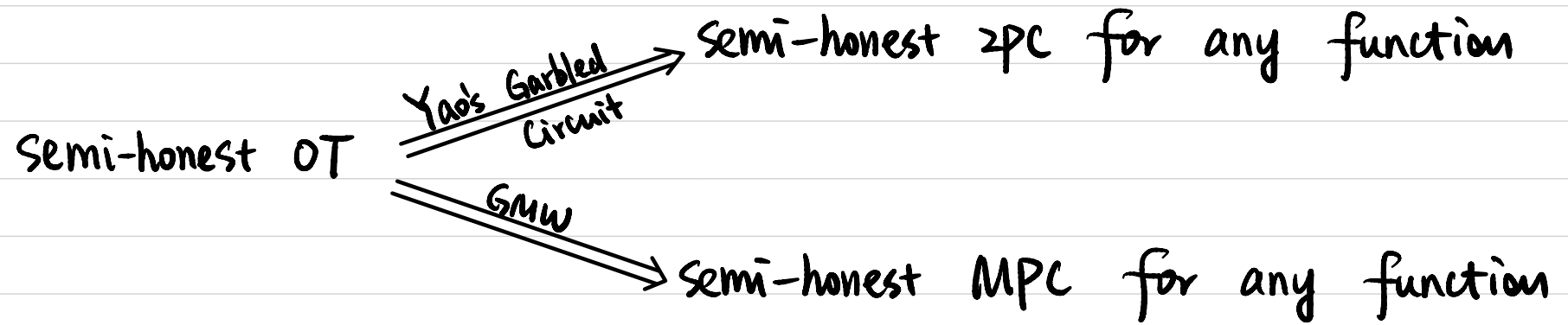


CSCI 1515 Applied Cryptography

This Lecture:

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



Putting it Together: Semi-Honest ZPC

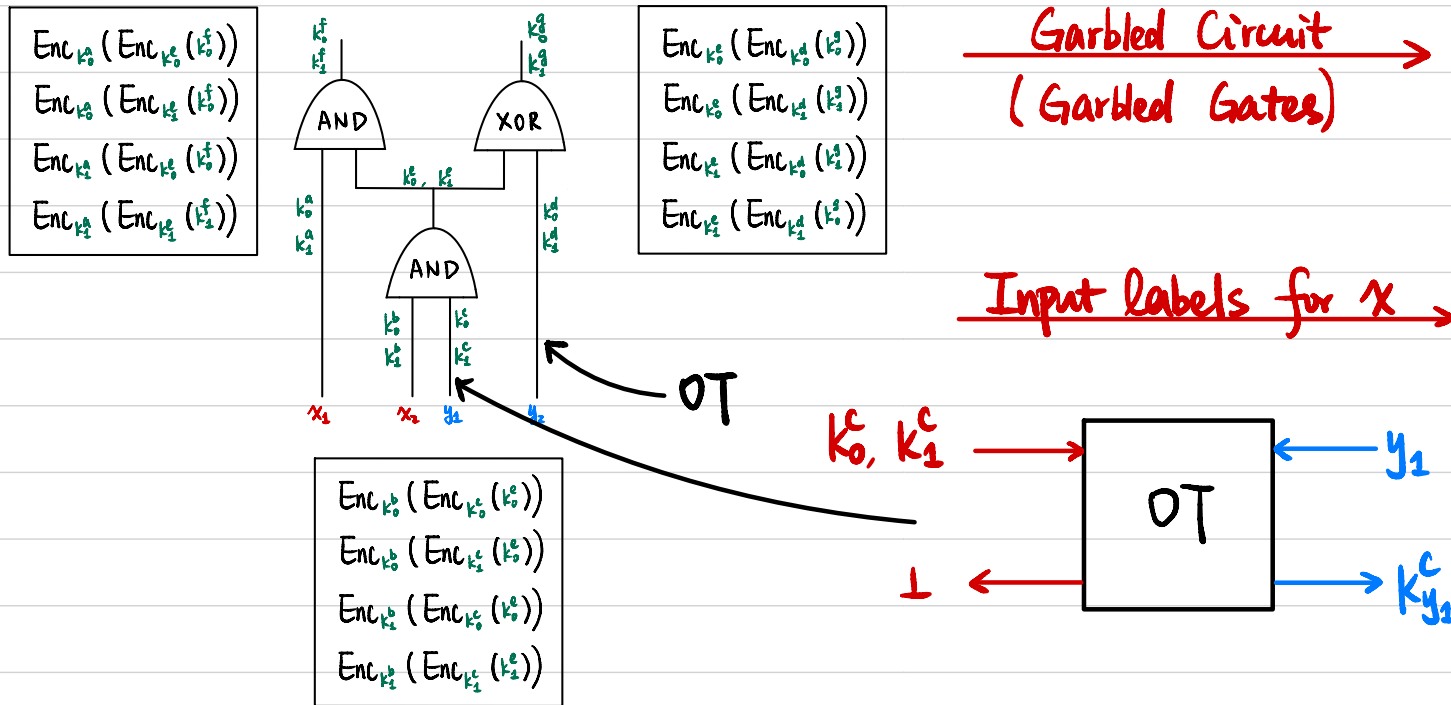
What could go wrong against malicious adversaries?

Alice (Garbler)

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

Bob (Evaluator)

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



• Output labels?

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

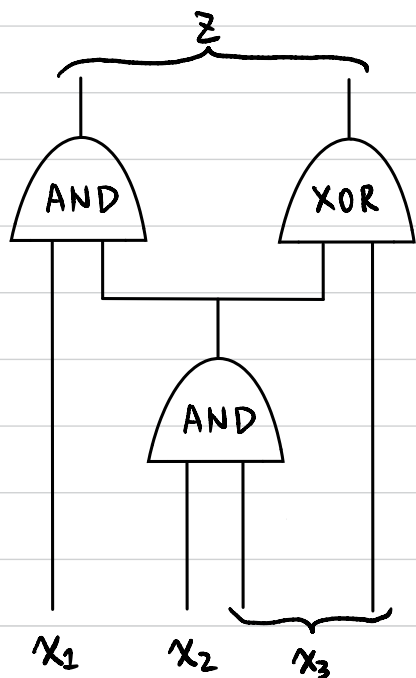
• How to decide which ciphertext to decrypt?

Shuffle {

- $Enc_{k_0^b}(Enc_{k_0^e}(\hat{k}_0^e || \hat{0} \dots \hat{0})) \rightarrow \text{garbage}$
- $Enc_{k_0^b}(Enc_{k_1^e}(k_0^e || 0 \dots 0)) \rightarrow k_0^e || 0 \dots 0$
- $Enc_{k_1^b}(Enc_{k_0^e}(k_0^e || 0 \dots 0)) \rightarrow \text{garbage}$
- $Enc_{k_1^b}(Enc_{k_1^e}(k_1^e || 0 \dots 0)) \rightarrow \text{garbage}$

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:

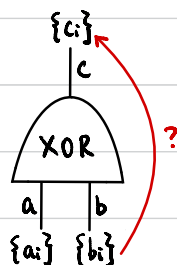
For each input wire w :

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

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

→ Sends v_i^w to party P_i .

XOR gates:

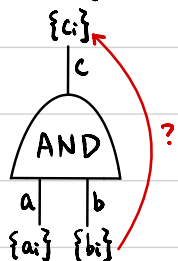


GIVEN: $\bigoplus_{i=1}^n a_i = a$ $\bigoplus_{i=1}^n b_i = b$

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

$c_i = ?$

$$\begin{aligned} a \cdot b &= \left(\sum_{i=1}^n a_i \right) \cdot \left(\sum_{i=1}^n b_i \right) \mod 2 \\ &= \left(\sum_{i=1}^n a_i \cdot b_i \right) + \left(\sum_{i \neq j} a_i \cdot b_j \right) \mod 2 \end{aligned}$$

$\uparrow$ P_i locally $\uparrow$ 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 $t \leq n-1$ (GMW)

Computational Complexity?

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

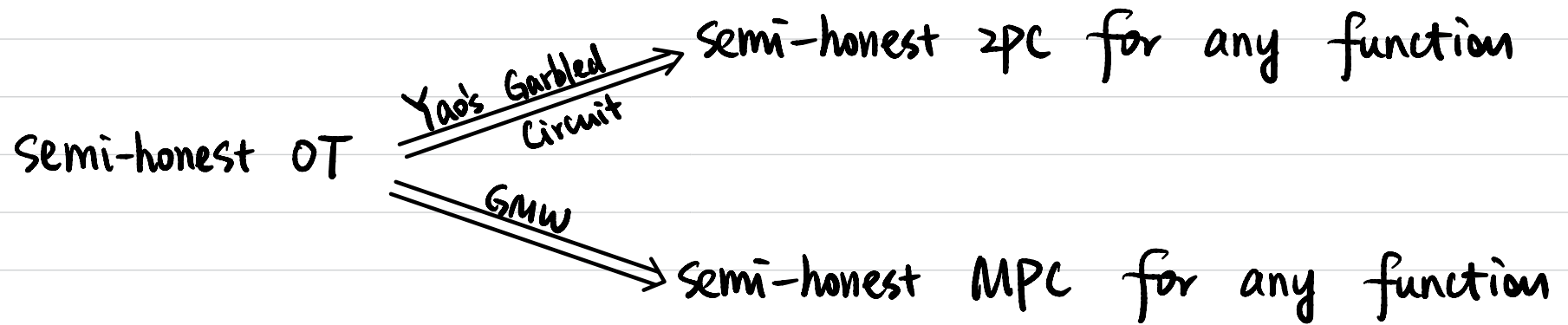
Communication Complexity?

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

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



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 $\cdot n^2$

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.

Step 2: Run semi-honest protocol.

Along with every message, prove in $\mathbb{Z}_k$ 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 Garbled Circuits
(Garbled Gates)

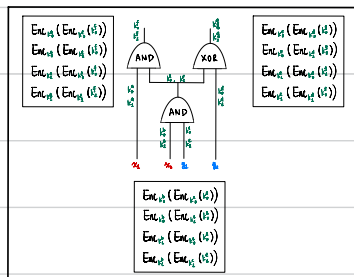
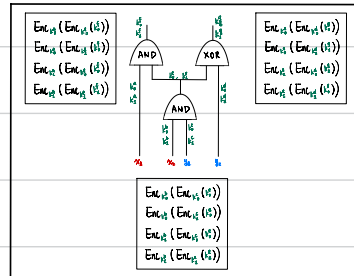
Randomly pick $(\lambda-1)$ of them

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

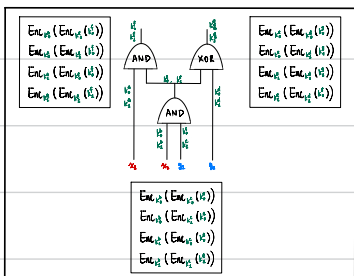
Verify correctness

Continue with the remaining GC

If Alice generated 1 GC incorrectly,
 $\Pr[\text{Alice caught}] = ?$



⋮



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)

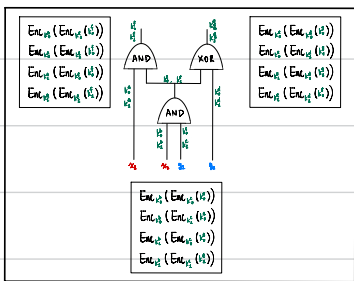
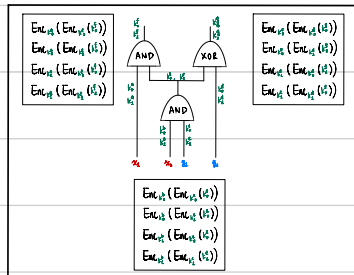
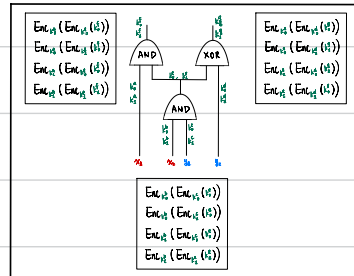
Randomly pick λ of them

Reveal all the labels
for the λ GCs

Verify correctness

Continue with the remaining λ GCs $\Rightarrow$ Take majority

If Alice generated $\geq \frac{\lambda}{2}$ GCs incorrectly,
 $\Pr[\text{Alice caught}] \geq ?$



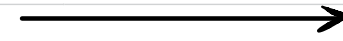
Private Set Intersection (PSI)

Alice



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

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



Bob



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

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

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

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

Private Set Intersection (PSI)

Alice



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

$H(x_1), \dots, H(x_n)$ →

Bob



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

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



$X \cap Y$

Is it (semi-honest) secure?

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

DDH-based PSI

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

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

Alice



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

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

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

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

Is it (semi-honest) secure?

Bob



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

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

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

$$\Downarrow \\ X \cap Y$$

PSI-CA?

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

Alice



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

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

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

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

Bob



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

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

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

$$\downarrow \\ X \cap Y$$

PSI-SUM?

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

Alice



Bob



Input: $X = \{x_1, x_2, \dots, x_n\}$
 $V = \{v_1, v_2, \dots, v_n\}$

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

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

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

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

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