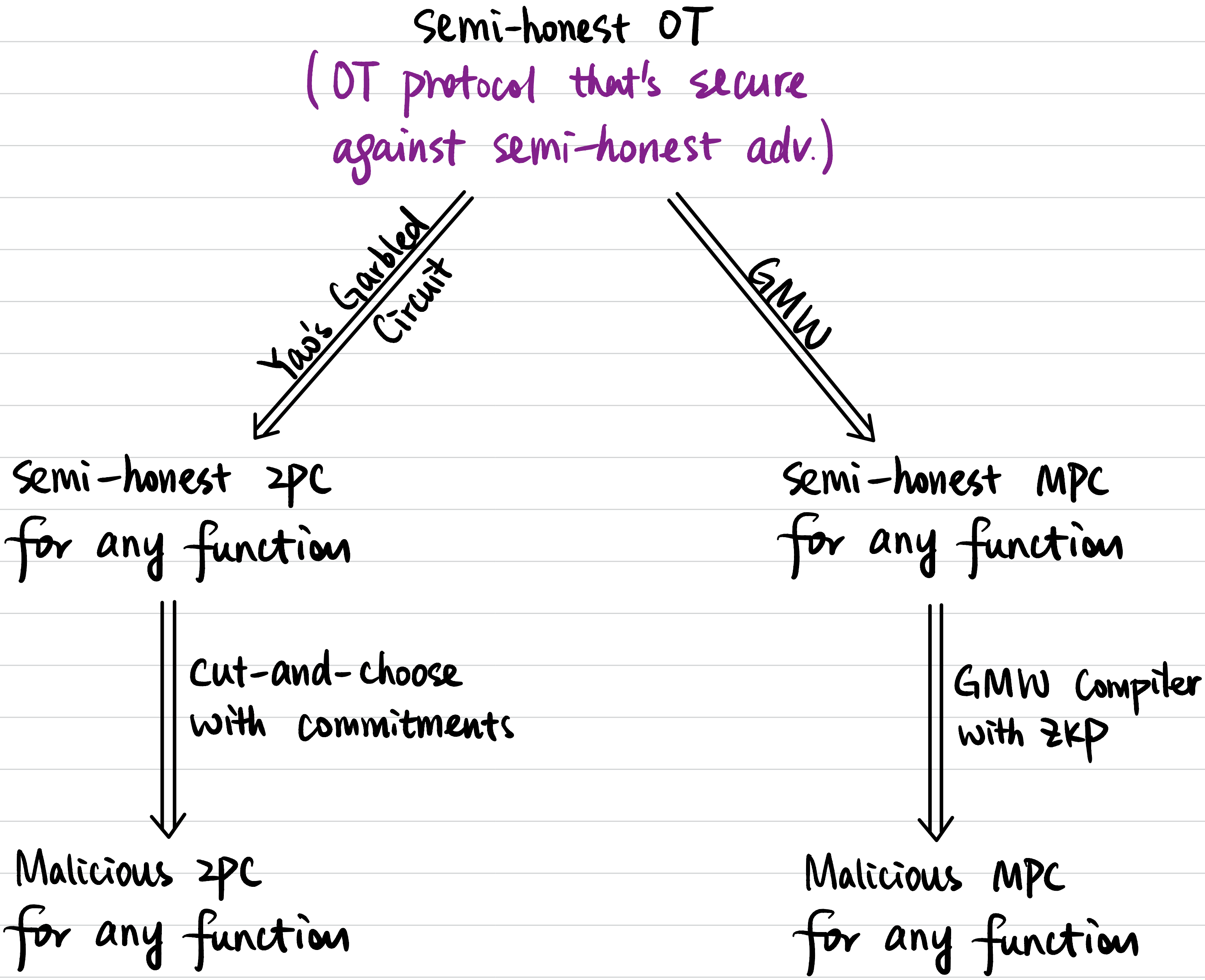
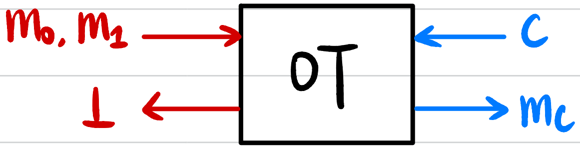
CSCI 1515 Applied Cryptography

This Lecture:

- Putting it All Together: Semi-Honest 2PC
- Optimizations of Garbled Circuits
- Cut-and-Choose for Garbled Circuits
- Private Set Intersection


Semi-honest OT
(OT protocol that's secure against semi-honest adv.)
Yao's Garbled Circuit
GMW
Semi-honest 2PC for any function
Semi-honest MPC for any function
Cut-and-choose with commitments
GMW Compiler with ZKP
Malicious 2PC for any function
Malicious MPC for any function

Oblivious Transfer (OT)



Sender

Receiver

Input: $m_0, m_1 \in \{0,1\}^\ell$

Input: $c \in \{0,1\}$

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

$$\xrightarrow{A = g^a}$$

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

$$\xleftarrow{B = g^b \cdot A^c}$$

$k_0 := H(B^a)$

$k_1 := H((\frac{B}{A})^a)$

$$\xrightarrow[ct_1 \leftarrow Enc_{k_1}(m_1)]{ct_0 \leftarrow Enc_{k_0}(m_0)}$$

Output:

$k_c := H(A^b) = H(g^{ab})$

$m_c := Dec_{k_c}(ct_c)$

Putting it All Together: Semi-Honest 2PC

What could go wrong against malicious adversaries?

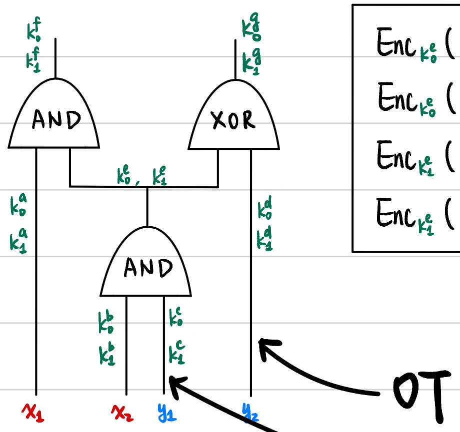
Alice (Garbler)

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

Bob (Evaluator)

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

$\mathrm{Enc}_{k_0^a}(\mathrm{Enc}_{k_0^e}(k_0^f))$
$\mathrm{Enc}_{k_0^a}(\mathrm{Enc}_{k_1^e}(k_0^f))$
$\mathrm{Enc}_{k_1^a}(\mathrm{Enc}_{k_0^e}(k_0^f))$
$\mathrm{Enc}_{k_1^a}(\mathrm{Enc}_{k_1^e}(k_1^f))$



$\mathrm{Enc}_{k_0^e}(\mathrm{Enc}_{k_0^d}(k_0^g))$
$\mathrm{Enc}_{k_0^e}(\mathrm{Enc}_{k_1^d}(k_1^g))$
$\mathrm{Enc}_{k_1^e}(\mathrm{Enc}_{k_0^d}(k_1^g))$
$\mathrm{Enc}_{k_1^e}(\mathrm{Enc}_{k_1^d}(k_0^g))$

$\mathrm{Enc}_{k_0^b}(\mathrm{Enc}_{k_0^c}(k_0^e))$
$\mathrm{Enc}_{k_0^b}(\mathrm{Enc}_{k_1^c}(k_0^e))$
$\mathrm{Enc}_{k_1^b}(\mathrm{Enc}_{k_0^c}(k_0^e))$
$\mathrm{Enc}_{k_1^b}(\mathrm{Enc}_{k_1^c}(k_1^e))$

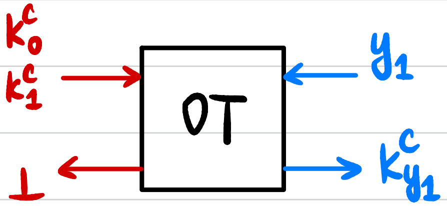
Shuffle

$H(k_0^b \| k_0^c) \oplus (k_0^e \| 0 \cdots 0)$ → garbage
$H(k_0^b \| k_1^c) \oplus (k_0^e \| 0 \cdots 0)$ → garbage
$H(k_1^b \| k_0^c) \oplus (k_0^e \| 0 \cdots 0)$ → $k_0^e \| 0 \cdots 0$
$\underbrace{H(k_1^b \| k_1^c)}_{256} \oplus (\underbrace{k_1^e}_{128} \| \underbrace{0 \cdots 0}_{128})$ → garbage

Garbled Circuit (Garbled Gates) →

Input labels for x →

Input labels for y: OT



← Output labels k^f, k^g

Output z →

Communication cost?

$4 \cdot 256 \cdot |C|$ bits

Computation cost?

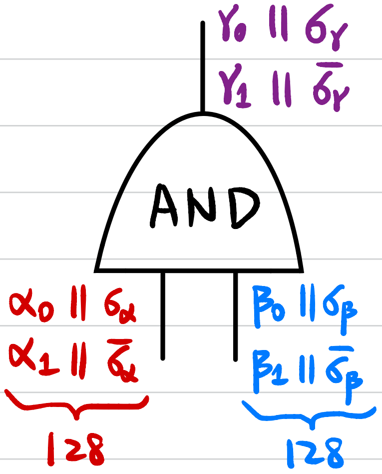
$4 \cdot |C|$

Optimization 1: Point-and-Permute

$4 \cdot 128$ bits / gate

$\sigma_\alpha, \sigma_\beta, \sigma_\gamma \xleftarrow{\$} \{0,1\}$

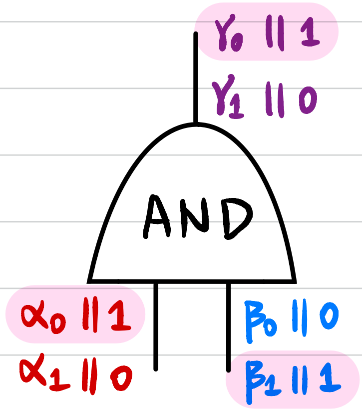
(signal bits)



σ_α	σ_β	:	$\text{Enc}_{\alpha_0}(\text{Enc}_{\beta_0}(\overbrace{\gamma_0}^{127} \| \overbrace{\sigma_\gamma}^{1}))$
σ_α	$\bar{\sigma}_\beta$	:	$\text{Enc}_{\alpha_0}(\text{Enc}_{\beta_1}(\gamma_0 \| \sigma_\gamma))$
$\bar{\sigma}_\alpha$	σ_β	:	$\text{Enc}_{\alpha_1}(\text{Enc}_{\beta_0}(\gamma_0 \| \sigma_\gamma))$
$\bar{\sigma}_\alpha$	$\bar{\sigma}_\beta$	:	$\text{Enc}_{\alpha_1}(\text{Enc}_{\beta_1}(\gamma_1 \| \bar{\sigma}_\gamma))$

Example:

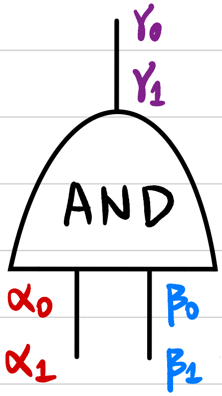
$\sigma_\alpha = 1 \quad \sigma_\beta = 0 \quad \sigma_\gamma = 1$



0	0	:	$\text{Enc}_{\alpha_1}(\text{Enc}_{\beta_0}(\gamma_0 \| 1))$
0	1	:	$\text{Enc}_{\alpha_1}(\text{Enc}_{\beta_1}(\gamma_1 \| 0))$
1	0	:	$\text{Enc}_{\alpha_0}(\text{Enc}_{\beta_0}(\gamma_0 \| 1))$
1	1	:	$\text{Enc}_{\alpha_0}(\text{Enc}_{\beta_1}(\gamma_0 \| 1))$

Optimization 2: Row Reduction

3 · 128 bits/gate



~~$H(\alpha_0 \| \beta_0) \oplus \gamma_0$~~ $:= 0$ $\gamma_0 := H(\alpha_0 \| \beta_0)$

$H(\alpha_0 \| \beta_1) \oplus \gamma_0$

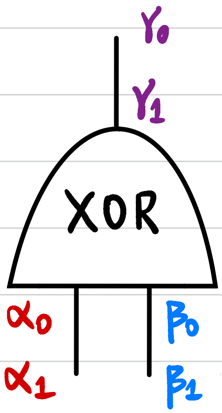
$H(\alpha_1 \| \beta_0) \oplus \gamma_0$

$H(\alpha_1 \| \beta_1) \oplus \gamma_1$

↑

Random Oracle

Optimization 3: Free XOR



hidden to evaluator

Sample a global $\Delta \xleftarrow{\$} \{0,1\}^\lambda$

$\alpha_1 := \alpha_0 \oplus \Delta$

$\beta_1 := \beta_0 \oplus \Delta$

$\gamma_1 := \gamma_0 \oplus \Delta$

$\gamma_0 := \alpha_0 \oplus \beta_0$

Other Optimizations:

- Half-gates : 2λ bits per AND gate + free XOR
- Three halves: $\sim 1.5\lambda$ bits per AND gate + free XOR

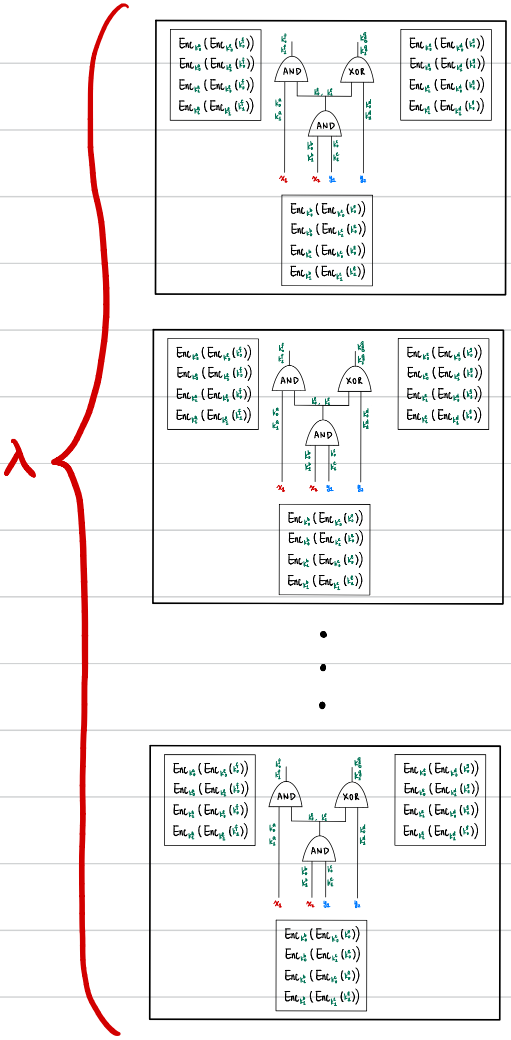
Cut-and-Choose for Garbled Circuits

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,

$\Pr[\text{Alice passes verification}] = ?$

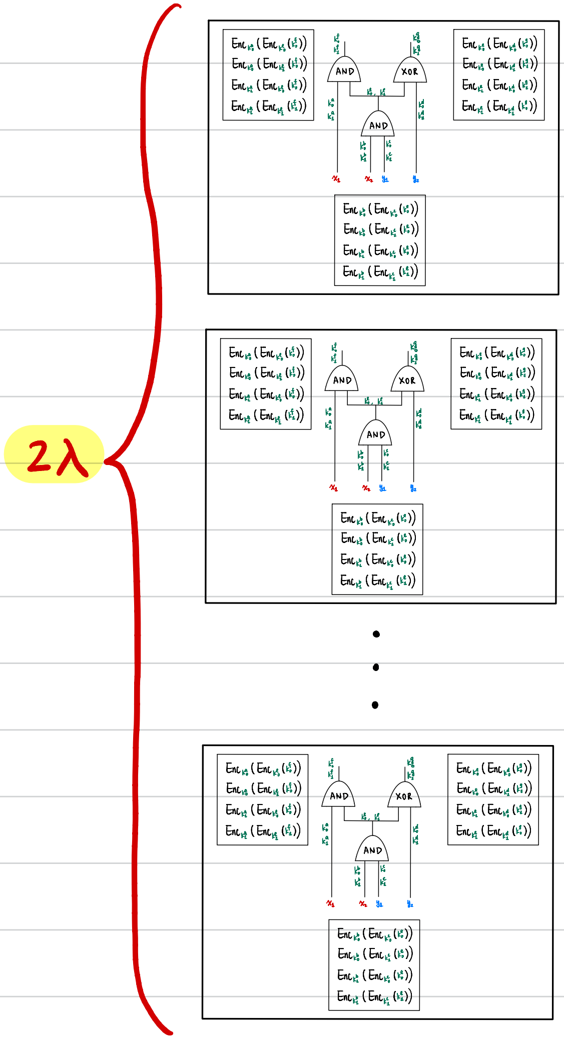
Cut-and-Choose for Garbled Circuits

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 →

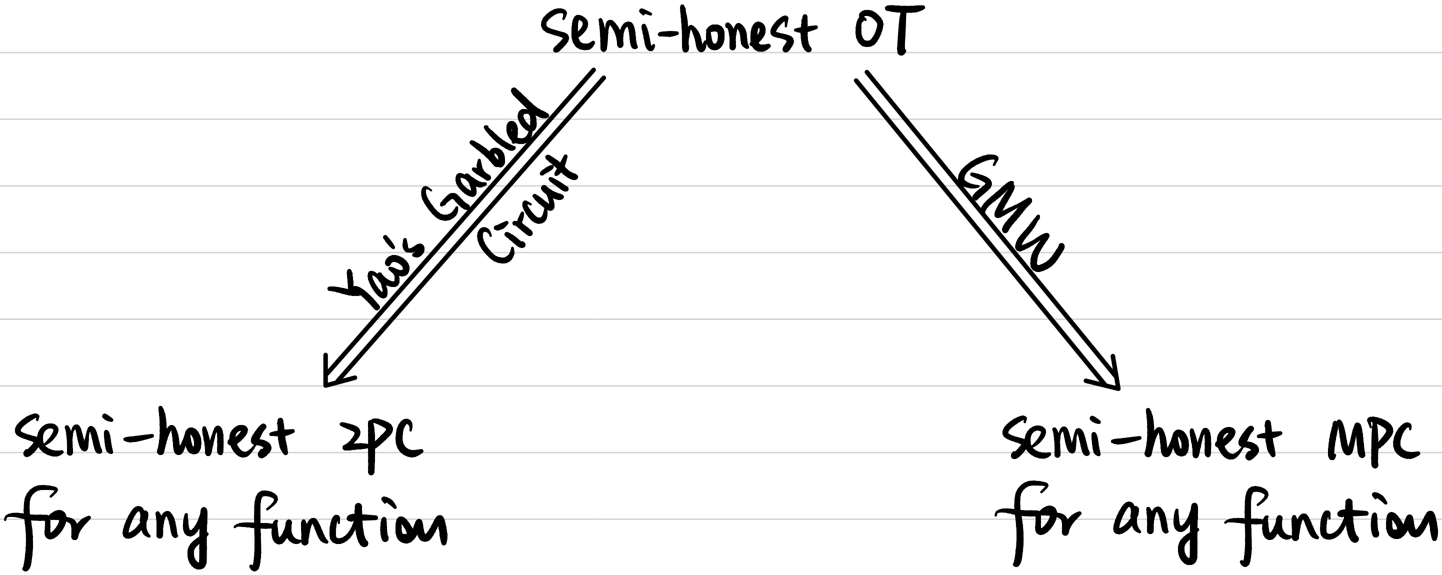
Verify correctness

↓

Continue with the remaining λ GCs ⇒ Take majority

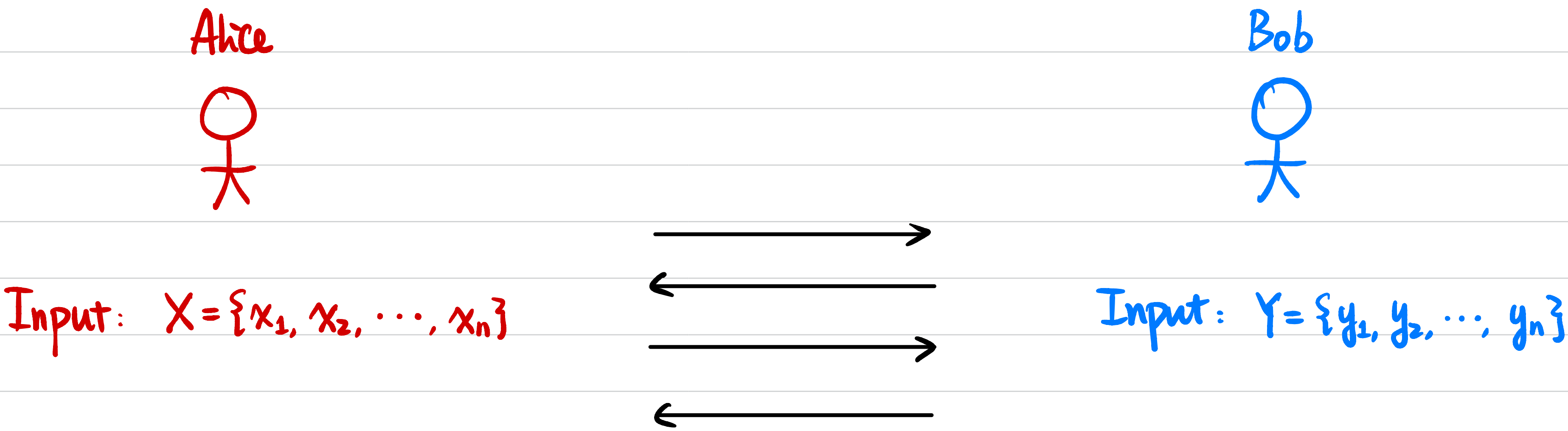
If Alice generated $\geq \frac{\lambda}{2}$ GCs incorrectly,

Pr[Alice passes all verification] ≤ ?



How to compare?

Private Set Intersection (PSI)



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

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

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

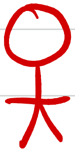
PSI-CA: $f(X, Y) = |X \cap Y|$

Applications:

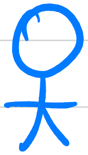
- Password Breach Alert (Chrome, Edge, Firefox, iOS keychain, $\cdots$)
- Ads Conversion Measurement (Google)
- Privacy-Preserving Inventory Matching (J.P. Morgan)
- Private Database Joins

Private Set Intersection (PSI)

Alice



Bob



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

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

$$\xrightarrow{H(x_1), \cdots, H(x_n)}$$

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

$$\Downarrow$$

$$X \cap Y$$

Is it (semi-honest) secure?

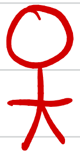
Is it possible to achieve 2PC / MPC with 1 round of communication?

DDH-based PSI

Cyclic group $\mathbb{G}$ of order q with generator g, where DDH holds.

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

Alice



Bob

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

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

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

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

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

$$\xrightarrow{\quad H(X)^a,\ H(Y)^{a \cdot b} \quad}$$

$$H(X)^{a \cdot b} \cap H(Y)^{a \cdot b}$$

$$\Downarrow$$

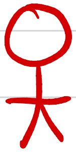
$$X \cap Y$$

Is it (semi-honest) secure?

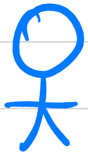
PSI-CA ?

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

Alice



Bob



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

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

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

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

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

$$\xrightarrow{H(X)^a,\ H(Y)^{a \cdot b}}$$

$$H(X)^{a \cdot b} \cap H(Y)^{a \cdot b}$$

$$\Downarrow$$

$$X \cap Y$$