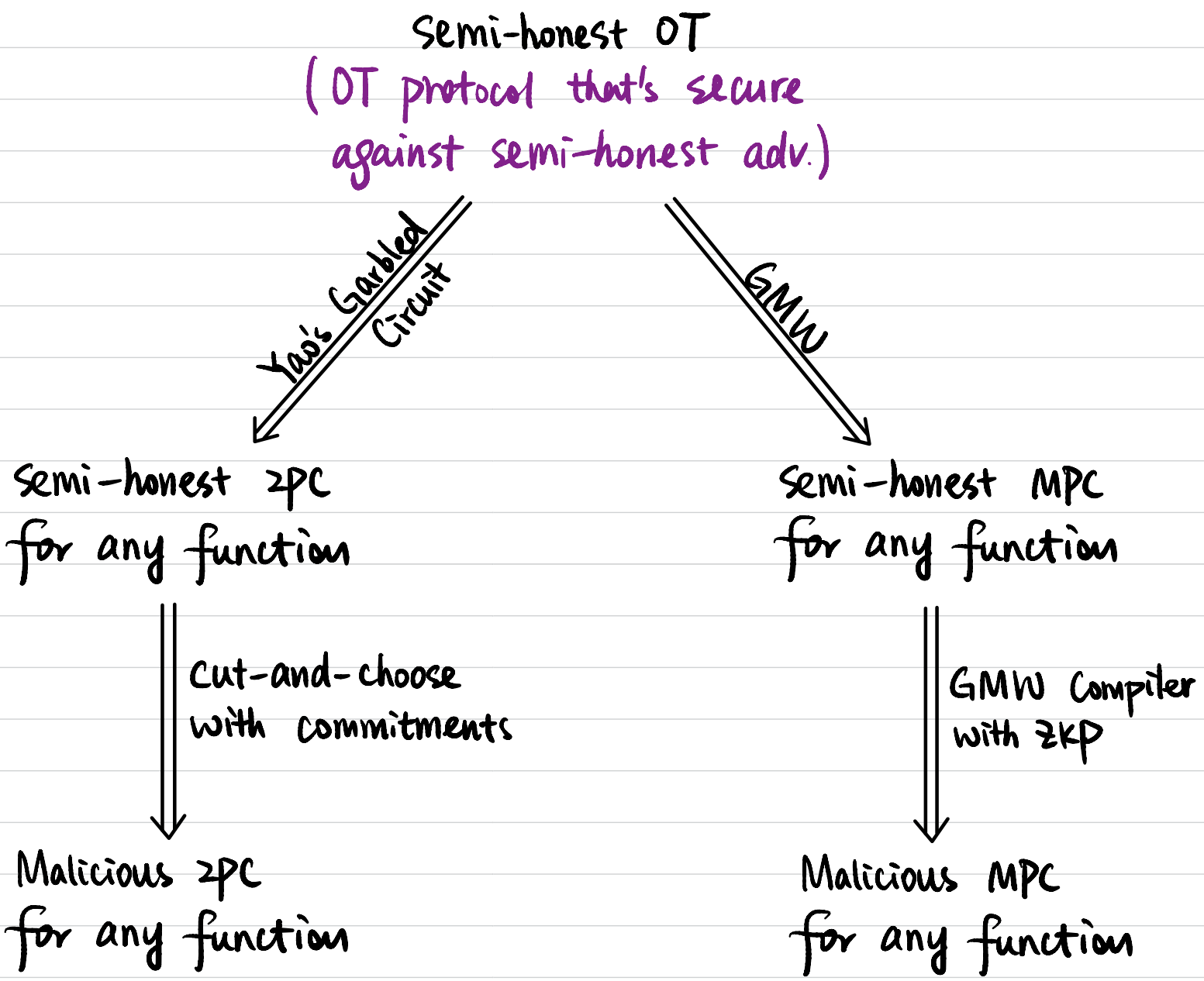
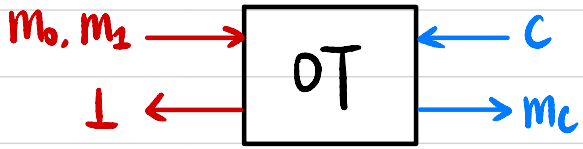
CSCI 1515 Applied Cryptography

This Lecture:

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


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

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

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

$A = g^a$ →

← $B = g^b \cdot A^c$

$k_0 := H(B^a)$

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

$ct_0 \leftarrow Enc_{k_0}(m_0)$
$ct_1 \leftarrow Enc_{k_1}(m_1)$ →

Receiver

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

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

Output:

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

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

Putting it All Together: Semi-Honest 2PC

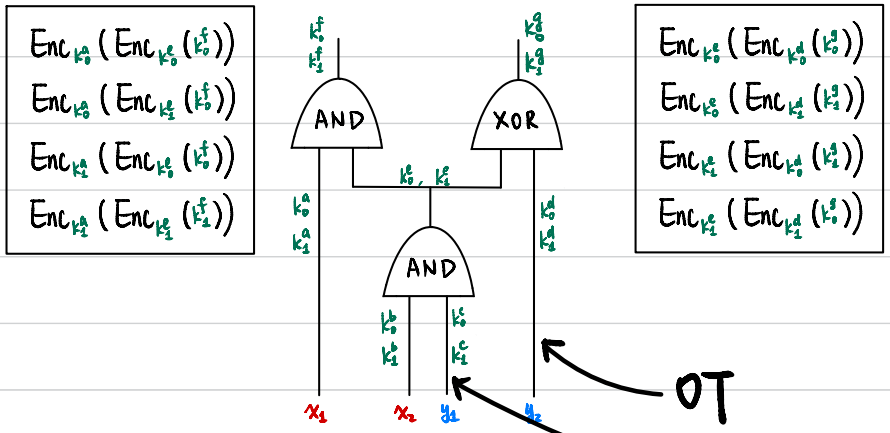
What could go wrong against malicious adversaries?

Alice (Garbler)

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

Bob (Evaluator)

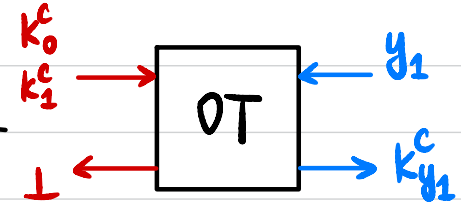
$y \in \{0,1\}^2$



Garbled Circuit (Garbled Gates)

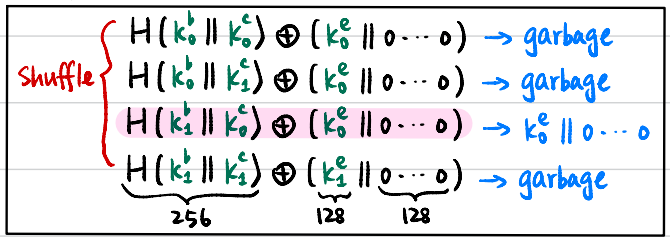
Input labels for x

Input labels for y: OT



Output labels k^f, k^g

Output z



Communication cost?

$4 \cdot 256 \cdot |c|$ bits

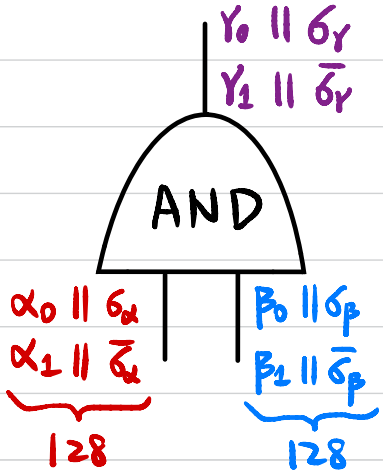
Computation cost?

$4 \cdot |c|$

Optimization 1: Point-and-Permute

4 · 128 bits / gate

$\sigma_\alpha, \sigma_\beta, \sigma_\gamma \xleftarrow{\$} \{0,1\}$
(signal bits)



$$\sigma_\alpha \;\; \sigma_\beta : \mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_0}(\overbrace{Y_0}^{127} \| \overbrace{\sigma_\gamma}^{1}))$$

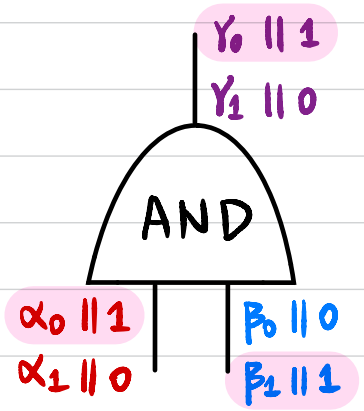
$$\sigma_\alpha \;\; \bar{\sigma}_\beta : \mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_1}(Y_0 \| \sigma_\gamma))$$

$$\bar{\sigma}_\alpha \;\; \sigma_\beta : \mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_0}(Y_0 \| \sigma_\gamma))$$

$$\bar{\sigma}_\alpha \;\; \bar{\sigma}_\beta : \mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_1}(Y_1 \| \bar{\sigma}_\gamma))$$

Example:

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



$$0 \;\; 0 : \mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_0}(Y_0 \| 1))$$

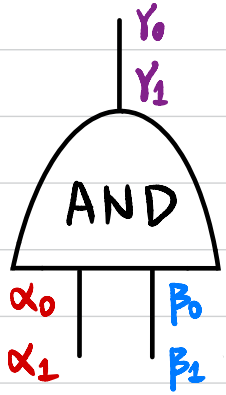
$$0 \;\; 1 : \mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_1}(Y_1 \| 0))$$

$$1 \;\; 0 : \mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_0}(Y_0 \| 1))$$

$$1 \;\; 1 : \mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_1}(Y_0 \| 1))$$

Optimization 2: Row Reduction

3 · 128 bits/gate



$$\cancel{H(\alpha_0 \| \beta_0) \oplus Y_0} := 0$$

$$H(\alpha_0 \| \beta_1) \oplus Y_0$$

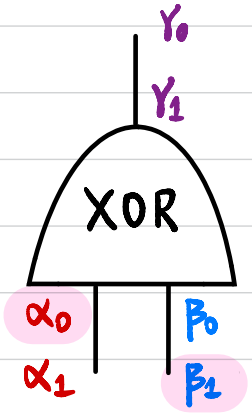
$$H(\alpha_1 \| \beta_0) \oplus Y_0$$

$$H(\alpha_1 \| \beta_1) \oplus Y_1$$

↑ Random Oracle

$$Y_0 := H(\alpha_0 \| \beta_0)$$

Optimization 3: Free XOR



hidden to evaluator

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

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

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

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

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

$$\begin{aligned} &\alpha_0 \oplus \beta_1 \\ &= \alpha_0 \oplus (\beta_0 \oplus \Delta) \\ &= (\alpha_0 \oplus \beta_0) \oplus \Delta \\ &= \gamma_0 \oplus \Delta \\ &= \gamma_1 \end{aligned}$$

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

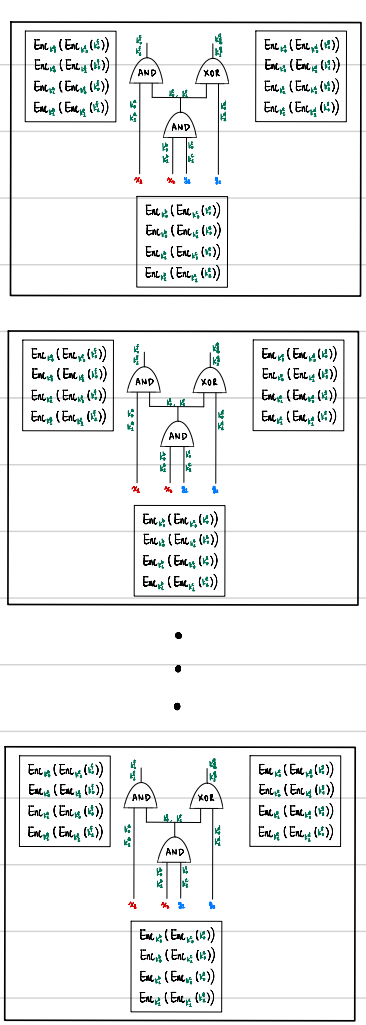
Alice (Garbler)

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

Bob (Evaluator)

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

λ



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,

$\Pr[\text{Alice passes verification}] = \frac{1}{\lambda}$

Cut-and-Choose for Garbled Circuits



$\frac{\lambda}{2}$ bad $\frac{3\lambda}{2}$ good

$\leq \left(\frac{3}{4}\right)^{\lambda}$

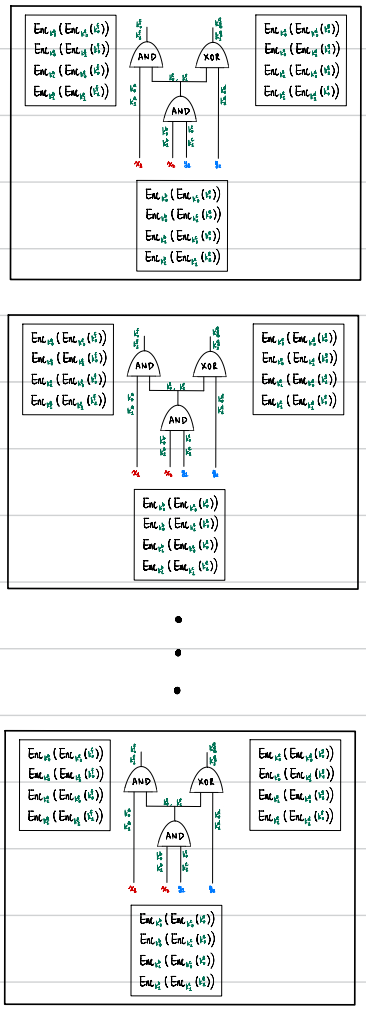
Alice (Garbler)

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

Bob (Evaluator)

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

2λ



2λ Garbled Circuits (Garbled Gates) →

← Randomly pick λ of them

Reveal all the labels for the λ GCs →

Verify correctness

"selective abort"

↓

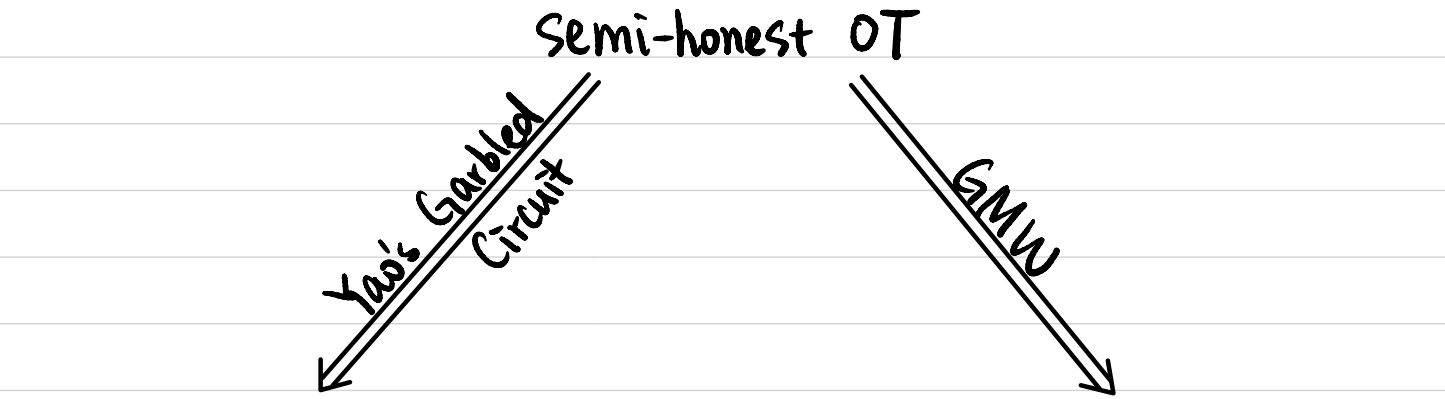
Continue with the remaining λ GCs ⇒ Take majority

Why?

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

$$\Pr[\text{Alice passes all verification}] \leq \frac{\binom{3\lambda/2}{\lambda}}{\binom{2\lambda}{\lambda}} = \frac{\frac{(3\lambda/2)!}{\lambda!\,(\lambda/2)!}}{\frac{(2\lambda)!}{\lambda!\,\lambda!}}$$

$$= \frac{\lambda \cdot (\lambda-1) \cdots (\frac{\lambda}{2}+1)}{(2\lambda)\cdot(2\lambda-1)\cdots(\frac{3\lambda}{2}+1)} \leq \left(\frac{1}{2}\right)^{\lambda/2}$$



How to compare?

Round:	+ O(1)	- O(depth of AND gates)
Circuit:	- Only Boolean	+ Also works for arithmetic