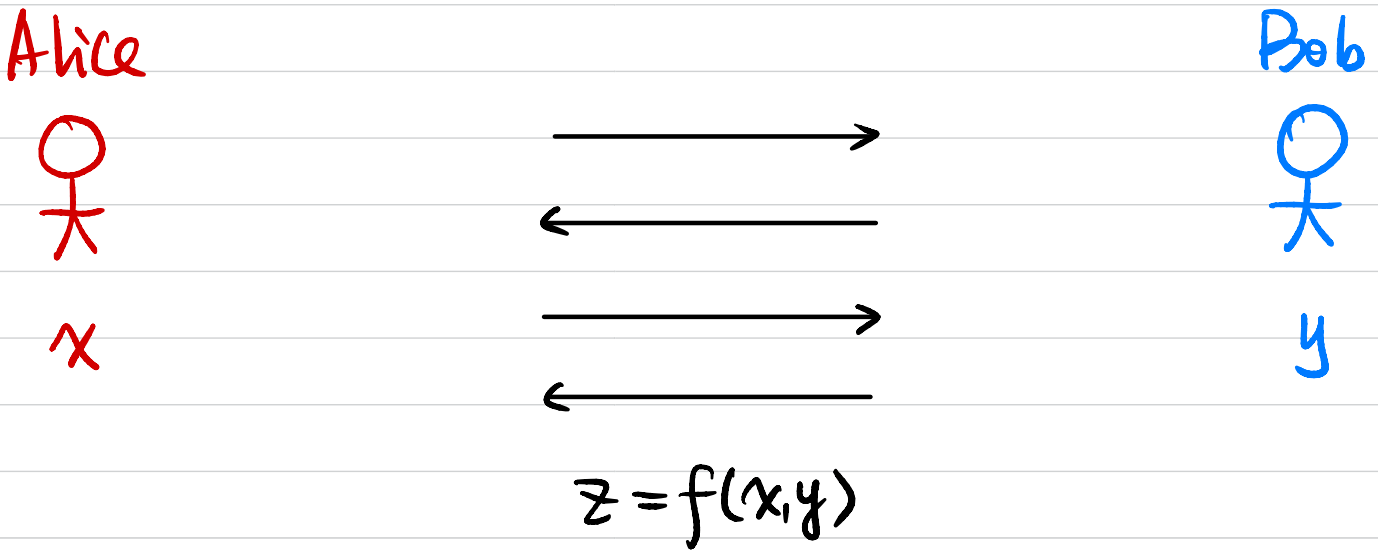
CSCI 1515 Applied Cryptography

This Lecture:

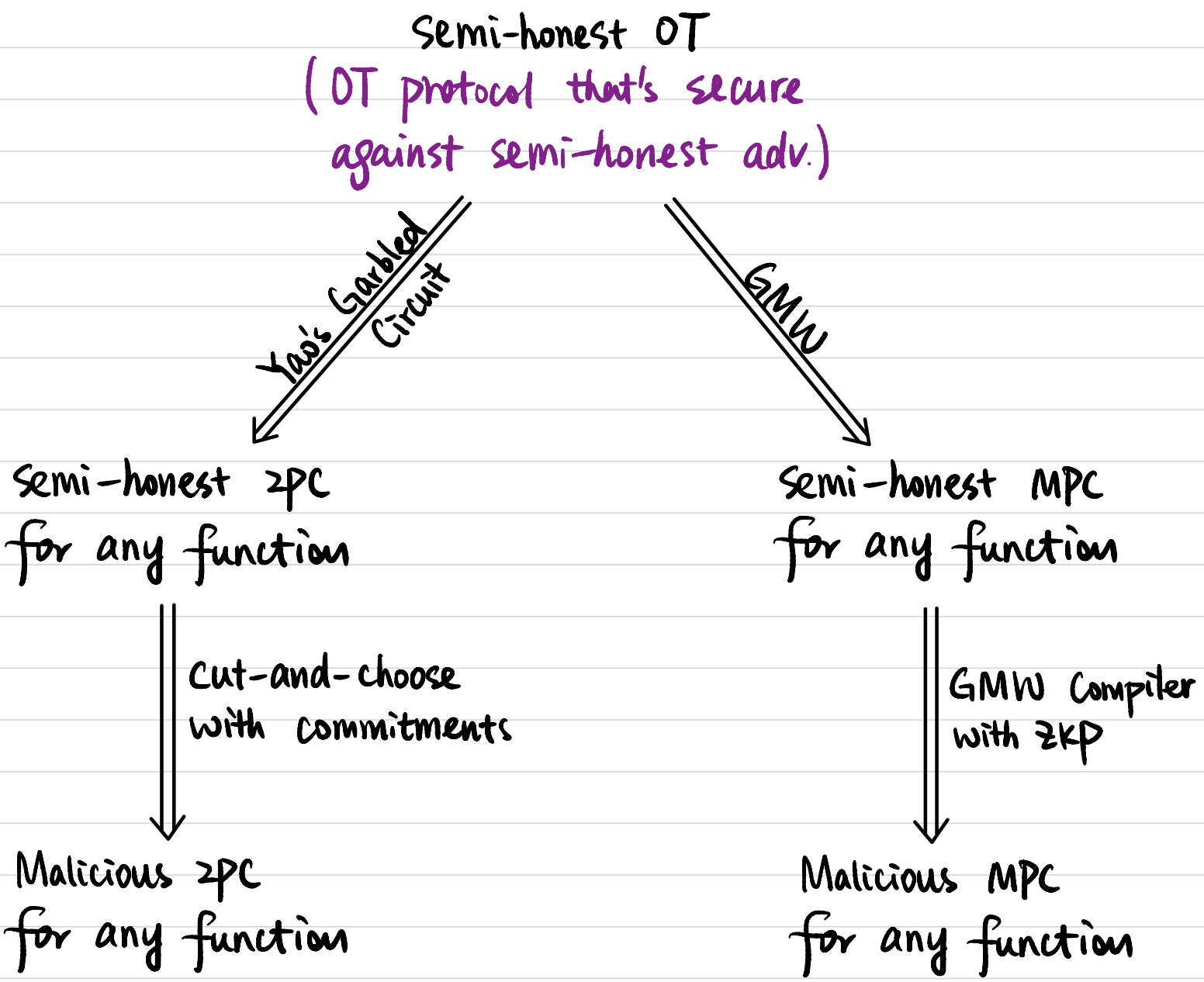
- Yao's Garbled Circuit
- Putting it All Together: Semi-Honest 2PC
- Optimizations of Garbled Circuits

Secure Two-Party Computation (2PC)

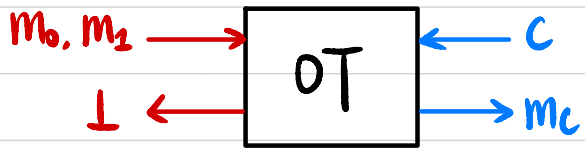


Allowed adversarial behavior:

- **Semi-honest:** Follow the protocol description honestly, but try to extract more information by inspecting transcript.
- **Malicious:** Can deviate arbitrarily from the protocol description.


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:

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

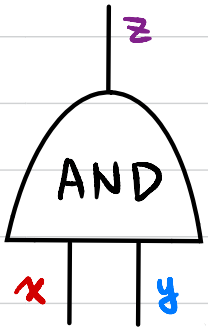
$m_c := Dec_{k_c}(ct_c)$

Example: Private Dating

Alice

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

$f(x,y) = x \wedge y$



Bob

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

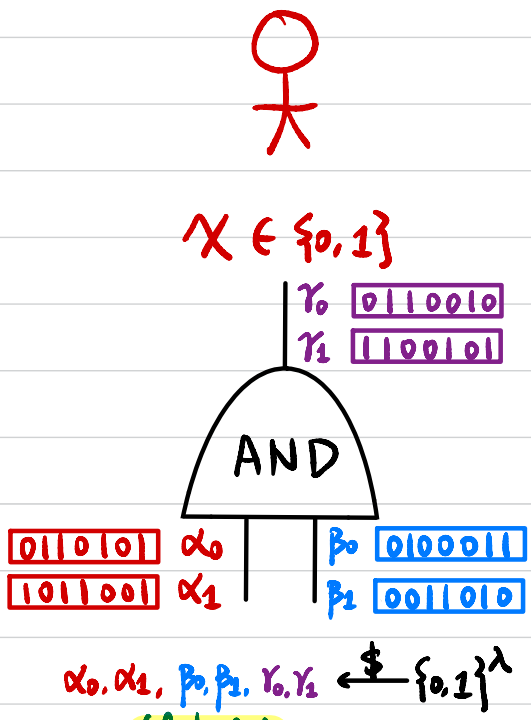
Truth Table:

$x=0$	$y=0$	$\Rightarrow$	$z=0$
$x=0$	$y=1$	$\Rightarrow$	$z=0$
$x=1$	$y=0$	$\Rightarrow$	$z=0$
$x=1$	$y=1$	$\Rightarrow$	$z=1$

Example: Private Dating

Garbler

Evaluator



Garbled Gate

$$\mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_0}(\gamma_0))$$
$$\mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_1}(\gamma_0))$$
$$\mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_0}(\gamma_0))$$
$$\mathrm{Enc}_{\alpha_1}(\mathrm{Enc}_{\beta_1}(\gamma_1))$$

Garbled Truth Table:

α_0 β_0 $\Rightarrow$ γ_0

α_0 β_1 $\Rightarrow$ γ_0

α_1 β_0 $\Rightarrow$ γ_0

α_1 β_1 $\Rightarrow$ γ_1

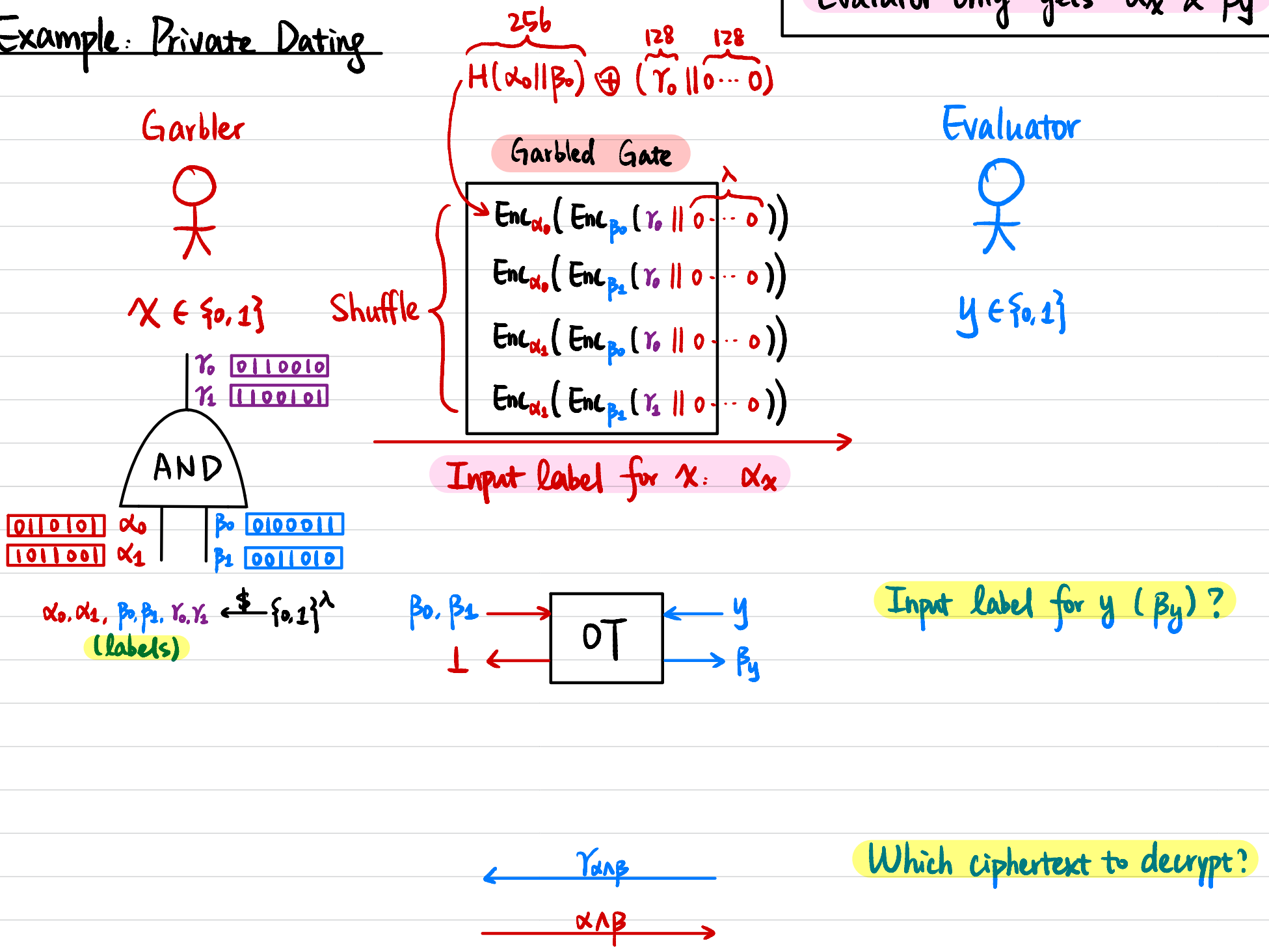
Evalator only gets α_x & β_y

$\Rightarrow$ Which γ label(s)?

$\gamma_{x \wedge y}$

Example: Private Dating

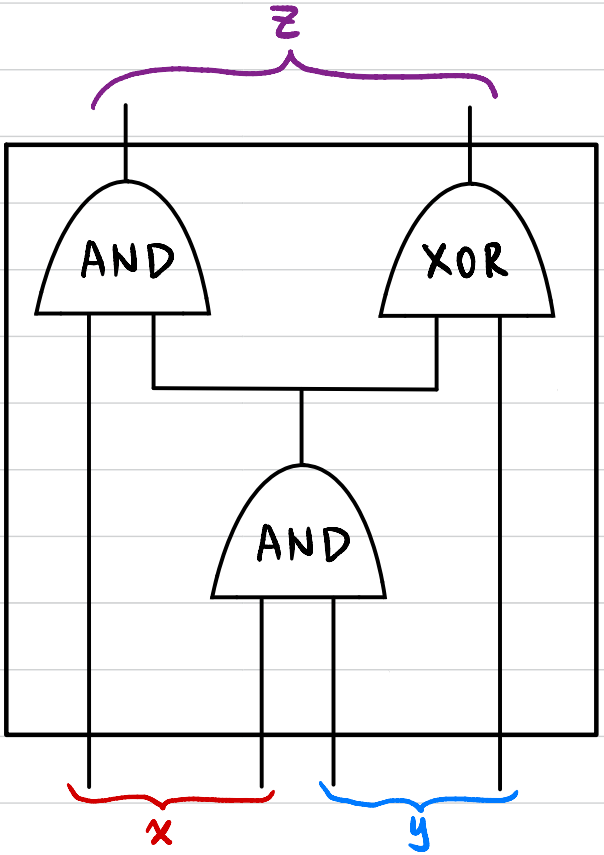
Evalator only gets α_x & β_y



Arbitrary Function → Represent it as a Boolean circuit

Alice

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



Bob

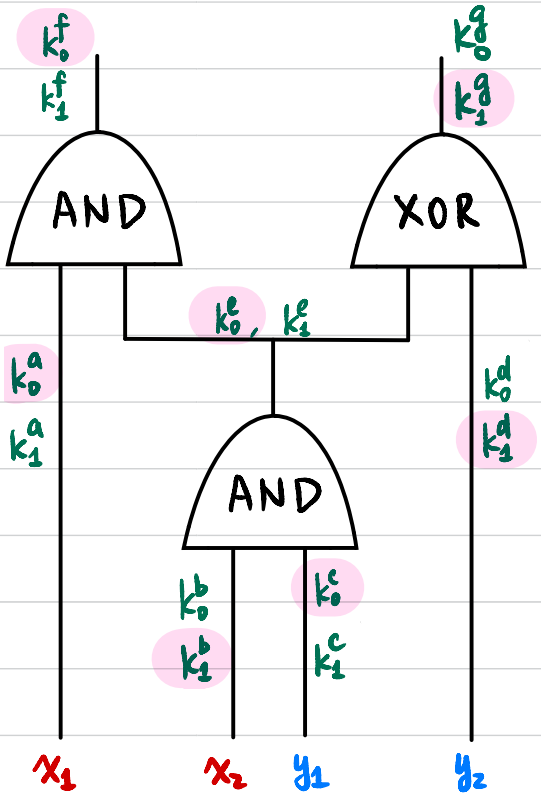
$y \in \{0,1\}^2$

$$z = f(x,y)$$

Yao's Garbled Circuit

Evalator gets one label per wire

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



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

Each label $\xleftarrow{\$} \{0,1\}^\lambda$

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

Secure 2PC

Evalator gets one label per wire

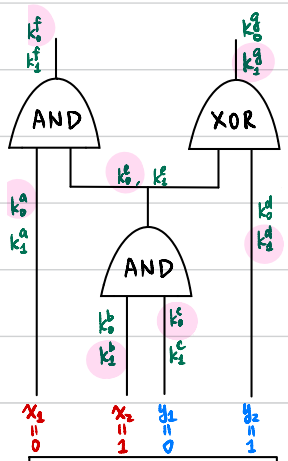
Alice (Garbler)

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

Bob (Evaluator)

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

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



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

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

Garbled Circuit
(Garbled Gates)

Input labels for x

Input labels for y ?

OT

Which ciphertexts to decrypt?

k_0^f, k_1^g

z

Putting it All Together: Semi-Honest 2PC

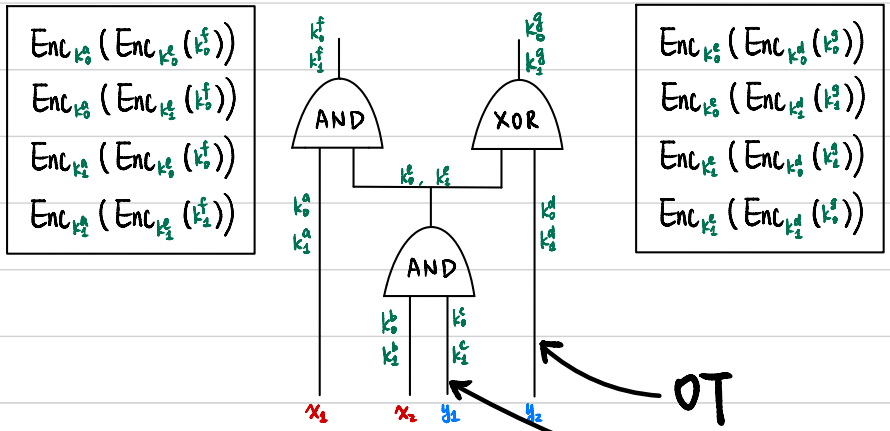
What could go wrong against malicious adversaries?

Alice (Garbler)

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

Bob (Evaluator)

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



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

Shuffle:
- $H(k_0^b \| k_0^c) \oplus (k_0^e \| 0\cdots0)$ → garbage
- $H(k_0^b \| k_1^c) \oplus (k_0^e \| 0\cdots0)$ → garbage
- $H(k_1^b \| k_0^c) \oplus (k_0^e \| 0\cdots0)$ → $k_0^e \| 0\cdots0$
- $H(k_1^b \| k_1^c) \oplus (k_1^e \| 0\cdots0)$ → garbage

(256, 128, 128)

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

Garbled Circuit (Garbled Gates) →

Input labels for x →

k_0^c, k_1^c → OT ← y_1

OT → $k_{y_1}^c$

$\perp$ ←

Input labels for y: OT

← Output labels k^f, k^g

Output z →

Communication cost?

$256 \cdot 4 \cdot |C|$

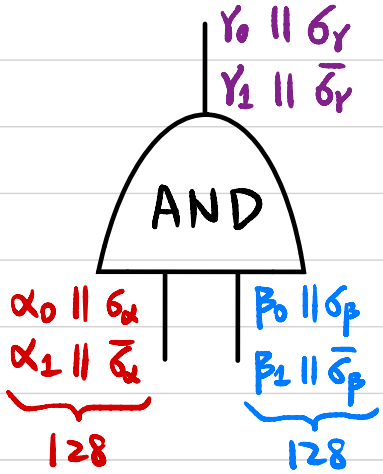
Computation cost?

G&E: $4 \cdot |C|$

Optimization 1: Point-and-Permute

4 · 128 bits / gate

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



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

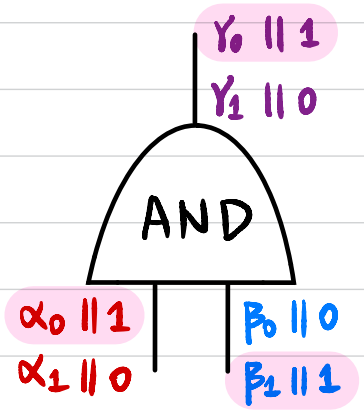
$$\sigma_\alpha \;\; \bar{\sigma}_\beta : \mathrm{Enc}_{\alpha_0}(\mathrm{Enc}_{\beta_1}(Y_0 \| \sigma_\gamma))$$

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

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

Example:

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



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

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

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

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