

CSCI 1515 Applied Cryptography

This Lecture:

- Feasibility Results of MPC
- Yao's Garbled Circuits and Optimizations

Secure Two-Party Computation (2PC)

Alice



x

Bob

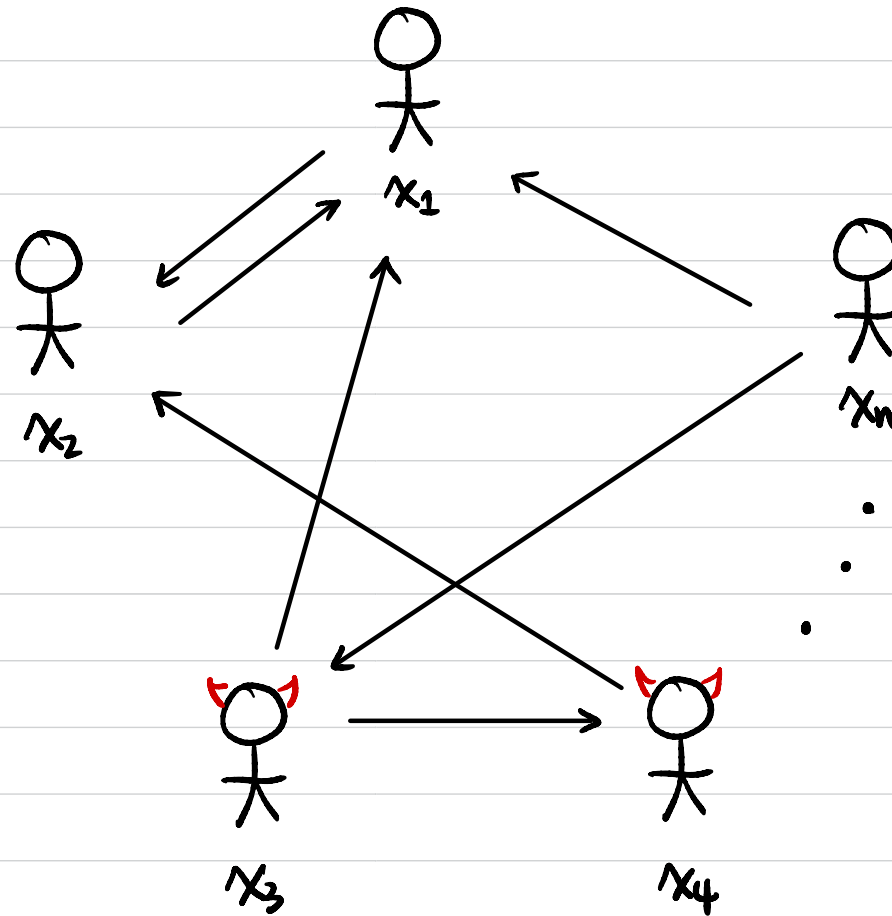


y



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

Secure Multi-Party Computation (MPC)



$$z = f(x_1, \dots, x_n)$$

Setting

- n parties $P_1, P_2, \dots, P_n$
with private inputs $x_1, x_2, \dots, x_n$
- Jointly compute $f(x_1, x_2, \dots, x_n)$
- Communication:
Authenticated secure point-to-point channels between each pair (P_i, P_j)
(Sometimes also assume broadcast channel)
- The adversary can "corrupt" a subset of the parties
(e.g. at most t parties)

General Security Properties

- **Correctness:** The function is computed correctly.
- **Privacy:** Only the output is revealed.
- **Independence of Inputs:** Parties cannot choose inputs depending on others' inputs.
- **Security with Abort:** Adversary may "abort" the protocol.
(preventing honest parties from receiving the output)
- **Fairness:** If one party receives output, then all receive output.
- **Guaranteed Output Delivery (GOD):** Honest parties always receive output.

Adversary's Power

Allowed adversarial behavior:

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

Adversary's Computing Power:

- Unbounded computing power $\Rightarrow$ Information-Theoretic (IT) Security
- PPT bounded $\Rightarrow$ Computational Security

Feasibility Results

Computational Security:

Semi-honest Oblivious Transfer (OT)



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

corrupted parties



malicious MPC for any function with $t < n$

Information-Theoretic (IT) Security:

semi-honest/malicious MPC for any function with $t < n/2$

(honest majority)



necessary

Oblivious Transfer (OT)

Sender



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

Output: $\perp$

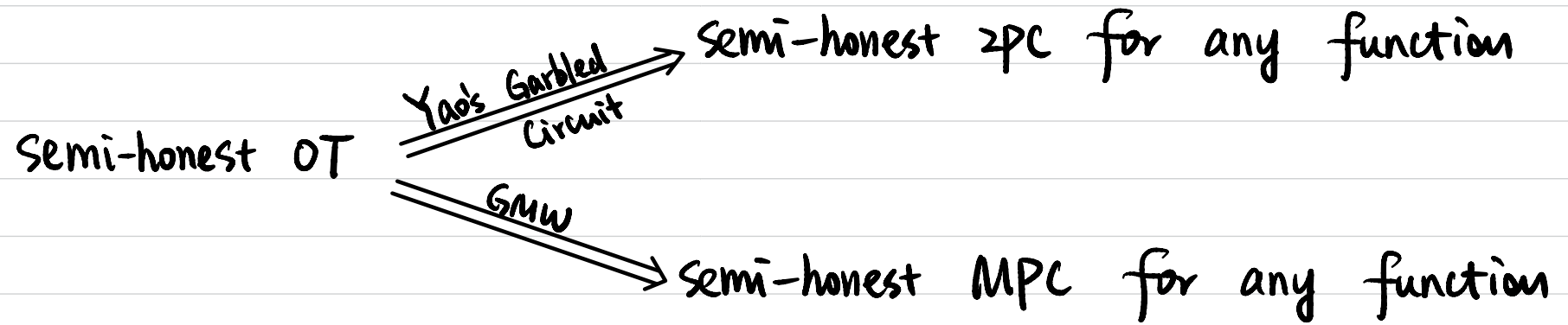


Receiver



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

Output: m_b



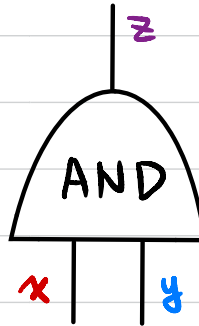
Example: Private Dating

Alice



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

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



Bob



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

Truth Table:

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

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

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

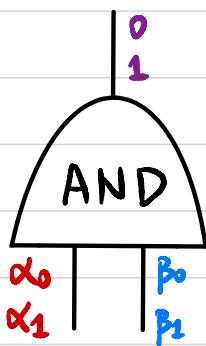
$$x=1 \quad y=1 \Rightarrow z=1$$

Example: Private Dating

Alice



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



$\alpha_0, \alpha_1, \beta_0, \beta_1 \xleftarrow{\$} \{0, 1\}^\lambda$
(labels)

$\text{Enc}_{\alpha_0}(\text{Enc}_{\beta_0}(0))$
$\text{Enc}_{\alpha_0}(\text{Enc}_{\beta_1}(0))$
$\text{Enc}_{\alpha_1}(\text{Enc}_{\beta_0}(0))$
$\text{Enc}_{\alpha_1}(\text{Enc}_{\beta_1}(1))$

Garbled Gate

Bob



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

Garbled Truth Table:

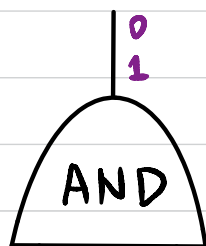
α_0	β_0	$\Rightarrow$	0
α_0	β_1	$\Rightarrow$	0
α_1	β_0	$\Rightarrow$	0
α_1	β_1	$\Rightarrow$	1

Example: Private Dating

Alice

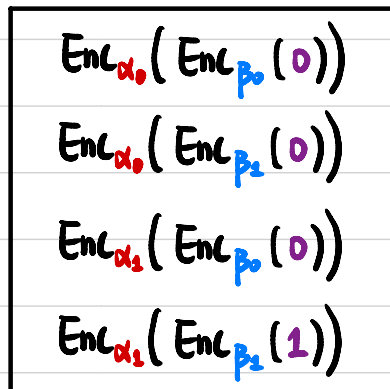


$x \in \{0, 1\}$



α_0
 α_1 β_0
 β_1

$\alpha_0, \alpha_1, \beta_0, \beta_1 \xleftarrow{\$} \{0, 1\}^\lambda$
(labels)



Input label for x : α_x

Bob



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

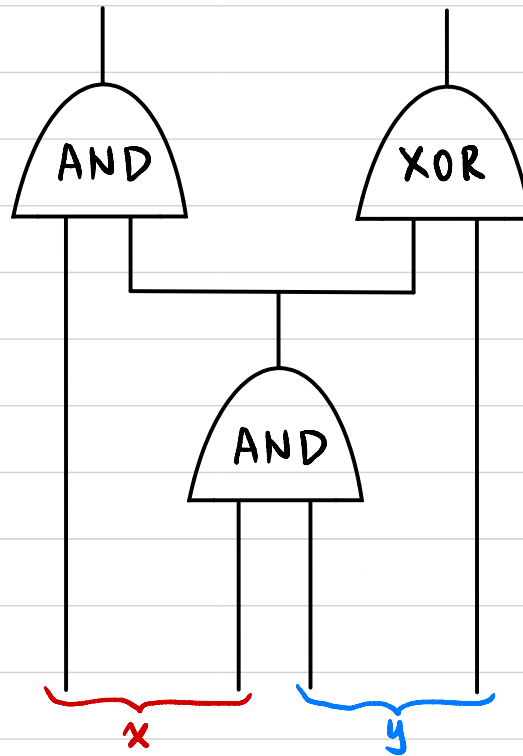
Input label for y ?

Arbitrary Function $\rightarrow$ Represent it as a Boolean circuit

Alice



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



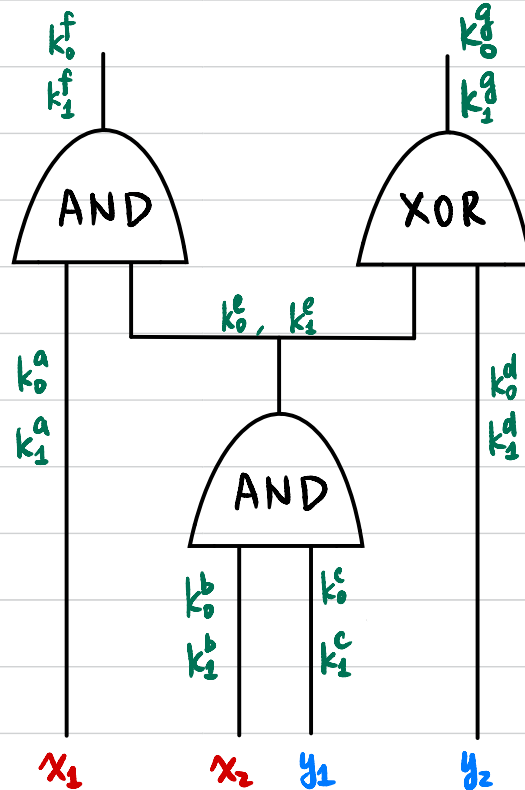
Bob



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

Yao's Garbled Circuit

$$\begin{aligned} & \text{Enc}_{k_0^a} (\text{Enc}_{k_0^e} (k_0^f)) \\ & \text{Enc}_{k_0^a} (\text{Enc}_{k_2^e} (k_0^f)) \\ & \text{Enc}_{k_1^a} (\text{Enc}_{k_0^e} (k_0^f)) \\ & \text{Enc}_{k_1^a} (\text{Enc}_{k_1^e} (k_1^f)) \end{aligned}$$



$$\begin{aligned} & \text{Enc}_{k_0^e} (\text{Enc}_{k_0^d} (k_0^g)) \\ & \text{Enc}_{k_0^e} (\text{Enc}_{k_2^d} (k_1^g)) \\ & \text{Enc}_{k_1^e} (\text{Enc}_{k_0^d} (k_1^g)) \\ & \text{Enc}_{k_1^e} (\text{Enc}_{k_1^d} (k_0^g)) \end{aligned}$$

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

$$\begin{aligned} & \text{Enc}_{k_0^b} (\text{Enc}_{k_0^c} (k_0^e)) \\ & \text{Enc}_{k_0^b} (\text{Enc}_{k_2^c} (k_0^e)) \\ & \text{Enc}_{k_1^b} (\text{Enc}_{k_0^c} (k_0^e)) \\ & \text{Enc}_{k_1^b} (\text{Enc}_{k_1^c} (k_1^e)) \end{aligned}$$

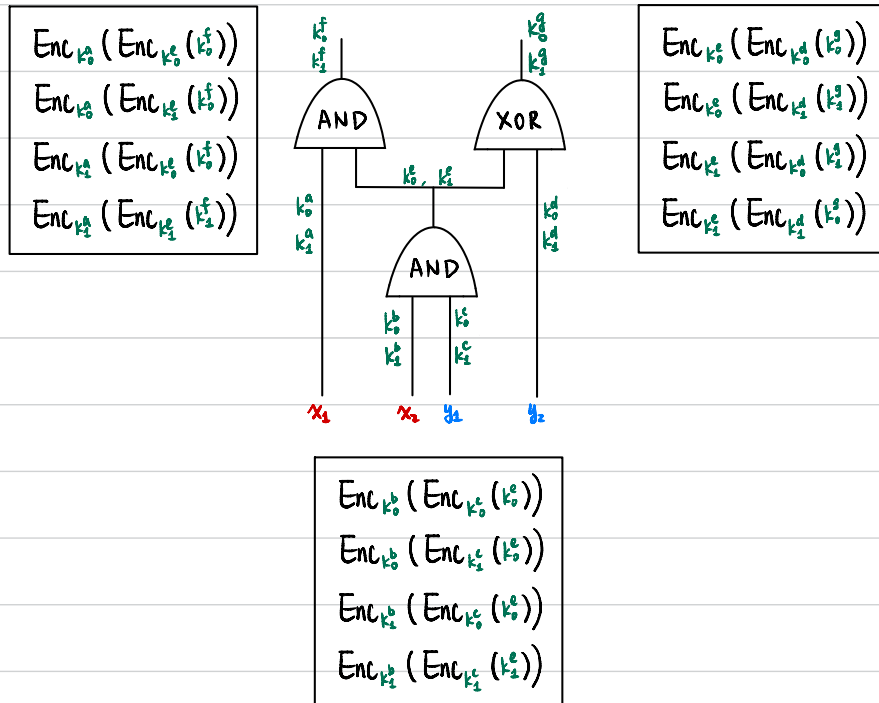
Secure 2PC

Alice (Garbler)

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

Bob (Evaluator)

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



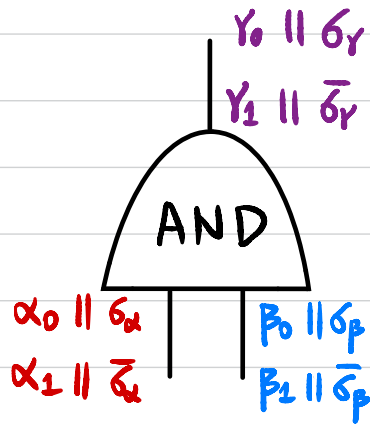
Garbled Circuit
(Garbled Gates) →

Input labels for x →

Input labels for y ?

- Output labels?
- How to decide which ciphertext to decrypt?

Optimization 1: Point-and-Permute



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

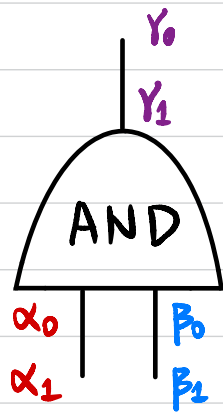
$$\sigma_\alpha \quad \sigma_\beta : \text{Enc}_{\alpha_0}(\text{Enc}_{\beta_0}(Y_0 \parallel \sigma_Y))$$

$$\sigma_\alpha \quad \bar{\sigma}_\beta : \text{Enc}_{\alpha_0}(\text{Enc}_{\beta_1}(Y_0 \parallel \sigma_Y))$$

$$\bar{\sigma}_\alpha \quad \sigma_\beta : \text{Enc}_{\alpha_1}(\text{Enc}_{\beta_0}(Y_0 \parallel \sigma_Y))$$

$$\bar{\sigma}_\alpha \quad \bar{\sigma}_\beta : \text{Enc}_{\alpha_1}(\text{Enc}_{\beta_1}(Y_1 \parallel \bar{\sigma}_Y))$$

Optimization 2: Row Reduction



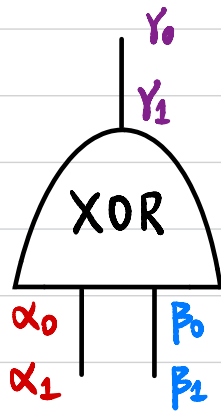
$$H(\alpha_0 \parallel \beta_0) \oplus \gamma_0$$

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

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

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

Optimization 3: Free XOR



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

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

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

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

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

Other Optimizations:

- Half-gates : 2λ bits per AND gate + free XOR
- Slicing-and-dicing : $\sim 1.5\lambda$ bits per AND gate + free XOR