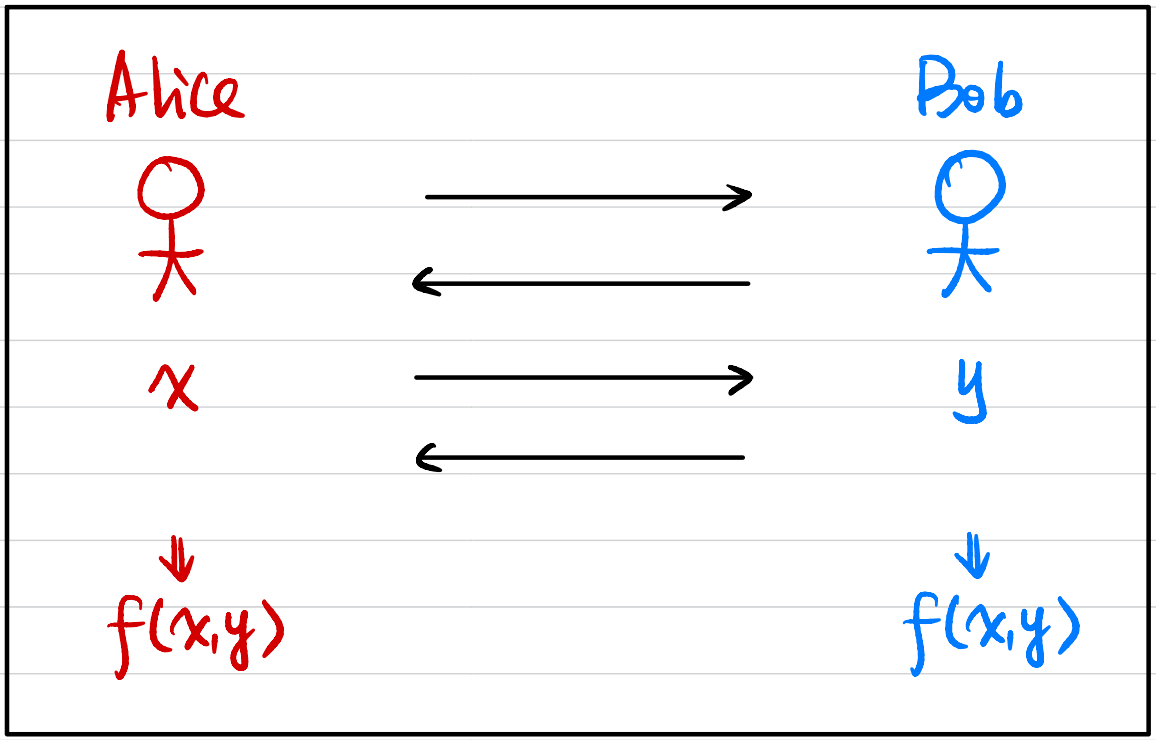
CSCI 1510

This Lecture:

- Definitions of MPC (continued)
- Private Set Intersection
- Oblivious Transfer

Security Against Semi-Honest Adversaries



Alice's view:

$\text{View}_A^{\Pi}(x, y, n) := (x,$ internal random tape $r,$ messages from Bob$)$

Given x, $f(x,y)$, Alice's view can be "simulated".

Security Against Semi-Honest Adversaries

Def (Semi-honest security for 2PC)

Let f be a functionality. We say a protocol Π securely computes f against semi-honest adversaries if $\exists$ PPT algorithms S_A, S_B s.t. $\forall x, y$,

$$\left\{\begin{pmatrix} S_A(1^n, x, f(x,y)) \\ f(x,y) \end{pmatrix}\right\}_{n\in\mathbb{N}} \simeq \left\{\begin{pmatrix} \text{View}_A^{\Pi}(x,y,n) \\ \text{Output}^{\Pi}(x,y,n) \end{pmatrix}\right\}_{n\in\mathbb{N}}$$

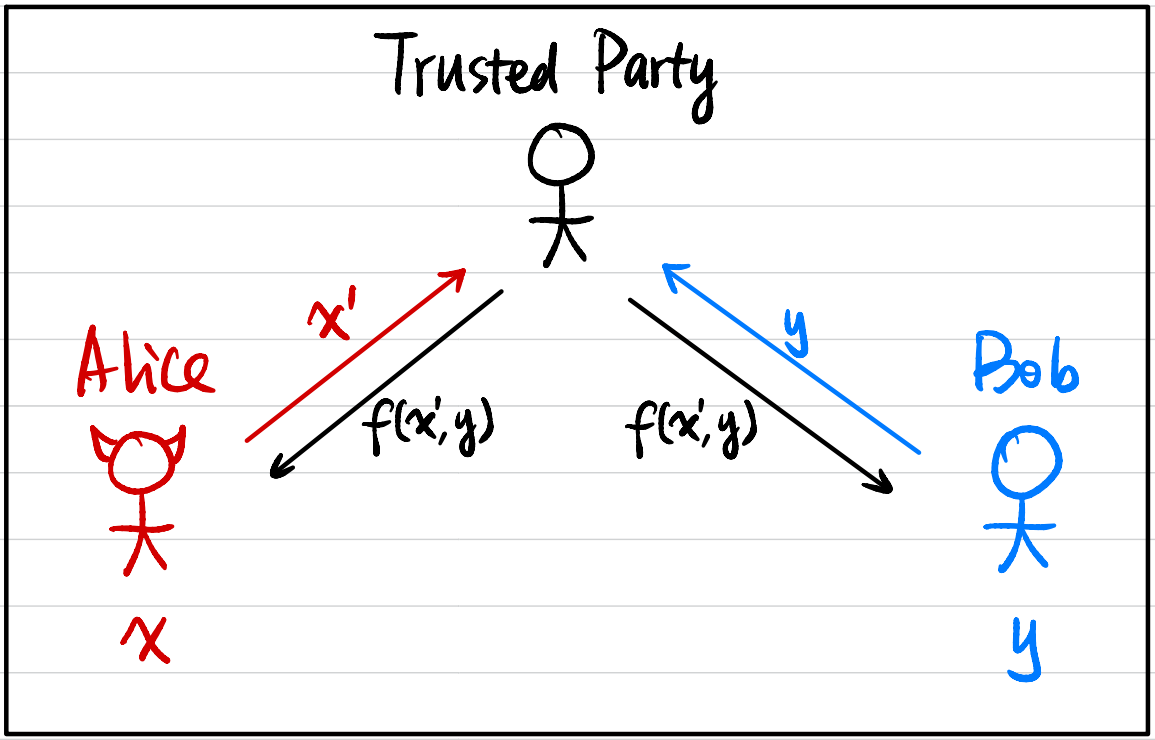
$$\left\{\begin{pmatrix} S_B(1^n, y, f(x,y)) \\ f(x,y) \end{pmatrix}\right\}_{n\in\mathbb{N}} \simeq \left\{\begin{pmatrix} \text{View}_B^{\Pi}(x,y,n) \\ \text{Output}^{\Pi}(x,y,n) \end{pmatrix}\right\}_{n\in\mathbb{N}}$$

perfect / statistical / computational

$\equiv$ $\overset{s}{\simeq}$ $\overset{c}{\simeq}$

Security Against Malicious Adversaries

What's the best we can hope for? (Ideal World)



Security Against Malicious Adversaries (Real / Ideal Paradigm)

Execution in the Real World:

(PPT) adversary $\mathcal{A}$ corrupting party $i \in \{\text{Alice}, \text{Bob}\}$

$$\text{REAL}^{\pi}_{\mathcal{A},i} := \begin{pmatrix} \mathcal{A}\text{'s output} \\ \text{Honest party's output in Real World} \end{pmatrix}$$

Execution in the Ideal World:

PPT adversary $\mathcal{S}$ corrupting party $i \in \{\text{Alice}, \text{Bob}\}$

$$\text{IDEAL}^{f}_{\mathcal{S},i} := \begin{pmatrix} \mathcal{S}\text{'s output} \\ \text{Honest party's output in Ideal World} \end{pmatrix}$$

Def (malicious security for 2PC)

Let f be a functionality. We say a protocol π securely computes f against malicious adversaries if $\forall$ (PPT) $\mathcal{A}$ in the real word, $\exists$ PPT $\mathcal{S}$ in the ideal world s.t. $\forall i \in \{\text{Alice}, \text{Bob}\}$, $\forall x, y$,

$$\left\{\text{REAL}^{\pi}_{\mathcal{A},i}(x, y, n)\right\}_{n \in \mathbb{N}} \simeq \left\{\text{IDEAL}^{f}_{\mathcal{S},i}(x, y, n)\right\}_{n \in \mathbb{N}}$$

Private Set Intersection (PSI)

$|X| = |Y| = n$

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

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

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

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

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

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

Private Set Intersection (PSI)

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

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

$H(x_1), \cdots, H(x_n)$

$x_i \notin X \cap Y$

Dictionary Attack

$f(x, y)$

$f(x, y')$

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

$\Downarrow$

$X \cap Y$

Is it (semi-honest) secure?

Is it possible to achieve 2PC / MPC with 1 round of communication? No!

DDH-based PSI

Cyclic group G of order q with generator g

$H: \{0,1\}^* \to G$

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

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

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

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

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

$\{H(y_1)^{k_B \cdot k_A}, \cdots, H(y_n)^{k_B \cdot k_A}\}$

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

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

$\Downarrow$

$X \cap Y$

$X \cap Y$

$(g^a, g^b, g^{ab}) \overset{c}{\simeq} (g^a, g^b, g^c)$

Thm If DDH is hard in G and H is modeled as a random oracle, then this protocol is semi-honest secure.

$S_A(1^n, X, I = X \cap Y) \rightarrow$ Alice's input X

randomness r

Bob's messages

Alice

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

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

$\{g_1, g_2, \cdots, g_n\} \xleftarrow{\$} G$

$H(x)^{k_A}, \; H(y)^{k_A \cdot k_B}$

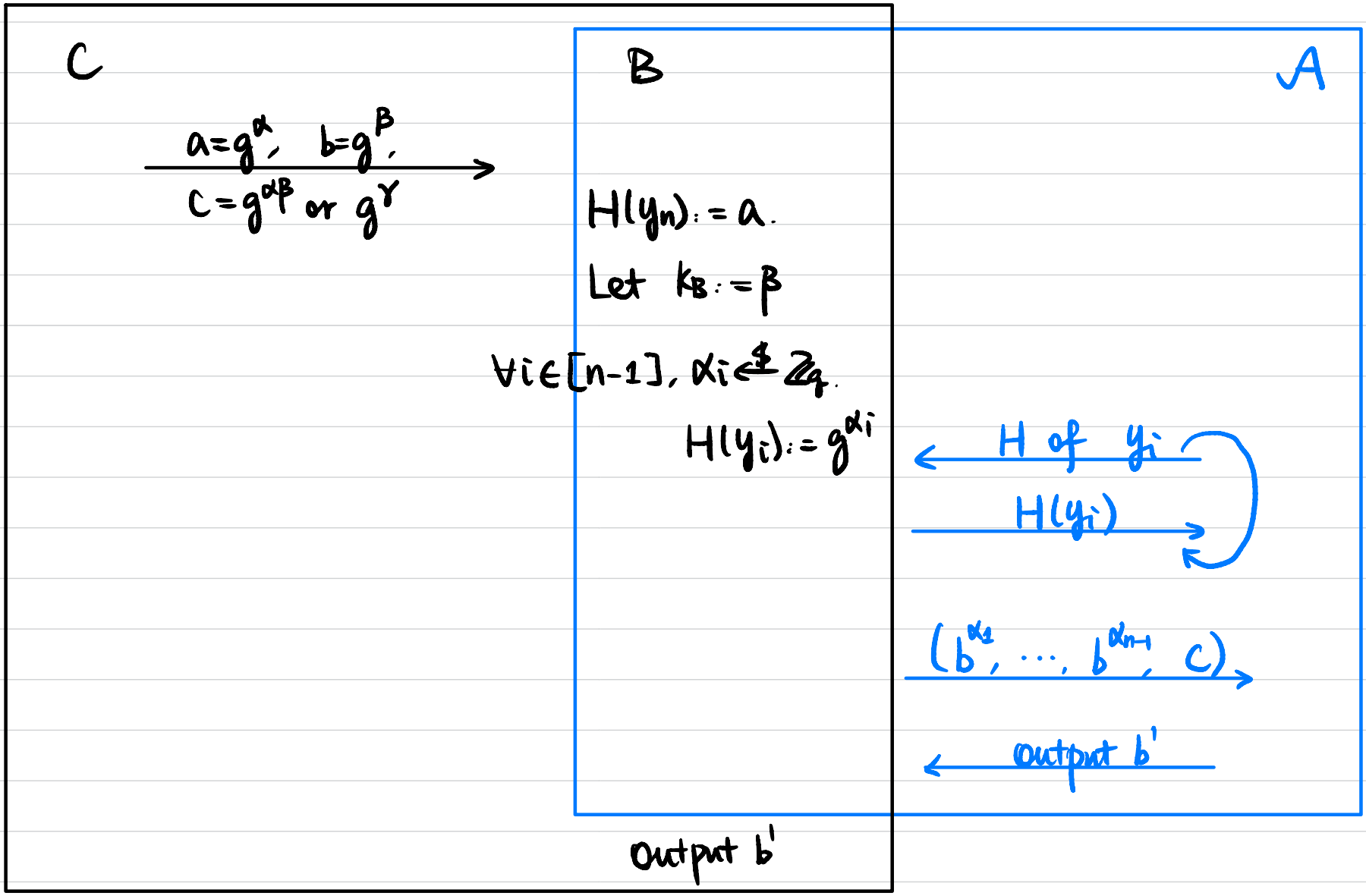
I

$(H(y_1)^{k_B}, \cdots, H(y_n)^{k_B}) \overset{c}{\simeq} (g_1, g_2, \cdots, g_n)$

$$(H(y_1)^{k_B}, \cdots, H(y_n)^{k_B}) \overset{c}{\simeq} (H(y_1)^{k_B}, \cdots, H(y_{n-1})^{k_B}, g_n)$$

Assume $\exists$ PPT A that can distinguish.

We construct PPT B to break DDH in the random oracle model.



Bob's input X ← $S_B(1^n, Y, I = X \cap Y)$

randomness r

Alice's messages

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

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

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

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

$H(I)^{k_A}$ ∪ Random, $H(Y)^{k_A \cdot k_B}$

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

↓

$X \cap Y$

$X \cap Y$

PSI-CA?

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

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

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

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

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

$H(Y)^{k_B} := \{H(y_1)^{k_B}, \cdots, H(y_n)^{k_B}\}$ ←

$H(X)^{k_A}, \{H(Y)^{k_A \cdot k_B}\}_{\text{shuffle}}$ →

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

$\Downarrow$

$|X \cap Y|$

$|X \cap Y|$ ←

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)

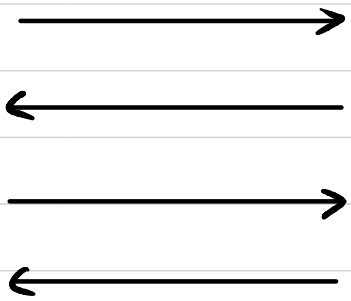
necessary

Oblivious Transfer (OT)

Sender

Receiver

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



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

Output: $\perp$

Output: m_c

Oblivious Transfer (OT)

Cyclic group G of order q with generator g

$H: G \to \{0,1\}^l$

Sender		Receiver
Input: $m_0, m_1 \in \{0,1\}^l$		Input: $c \in \{0,1\}$
$a \xleftarrow{\$} \mathbb{Z}_q$	$\xrightarrow{A = g^a}$	$b \xleftarrow{\$} \mathbb{Z}_q$
	$\xleftarrow{B = g^b \cdot A^c}$	
$k_0 := H(B^a)$ $k_1 := H((\frac{B}{A})^a)$		
	$\xrightarrow{\begin{array}{l} ct_0 := k_0 \oplus m_0 \\ ct_1 := k_1 \oplus m_1 \end{array}}$	
		Output: $m_c := ct_c \oplus H(A^b)$

Thm If CDH is hard in G and H is modeled as a random oracle, then this protocol is semi-honest secure.

$S_A(1^n, (m_0, m_1), \perp)$

Sender

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

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

$A = g^a$ →

← $B \xleftarrow{\$} G$

$k_0 := H(B^a)$

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

$Ct_0 := k_0 \oplus m_0$

$Ct_1 := k_1 \oplus m_1$ →

$S_B(1^n, c, m_c)$

Receiver

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

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

$A = g^a$ →

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

← $B = g^b \cdot A^c$

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

$ct_c := k_c \oplus m_c$

$ct_{1-c} \xleftarrow{\$} \{0,1\}^\ell$ →

Output: $m_c := ct_c \oplus H(A^b)$