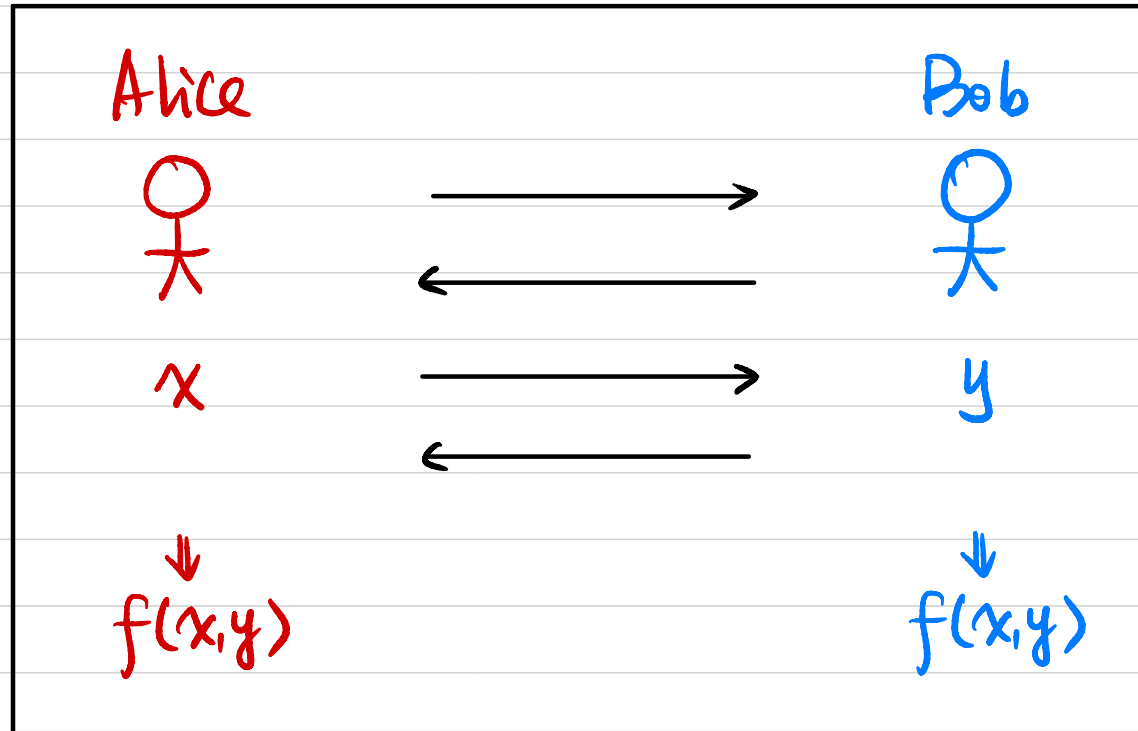


CSCI 1510

This Lecture:

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

Security Against Semi-Honest Adversaries



Alice's view:

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

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

Security Against Semi-Honest Adversaries

Def (Semi-honest security for ZPC)

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. $\forall x, y$,

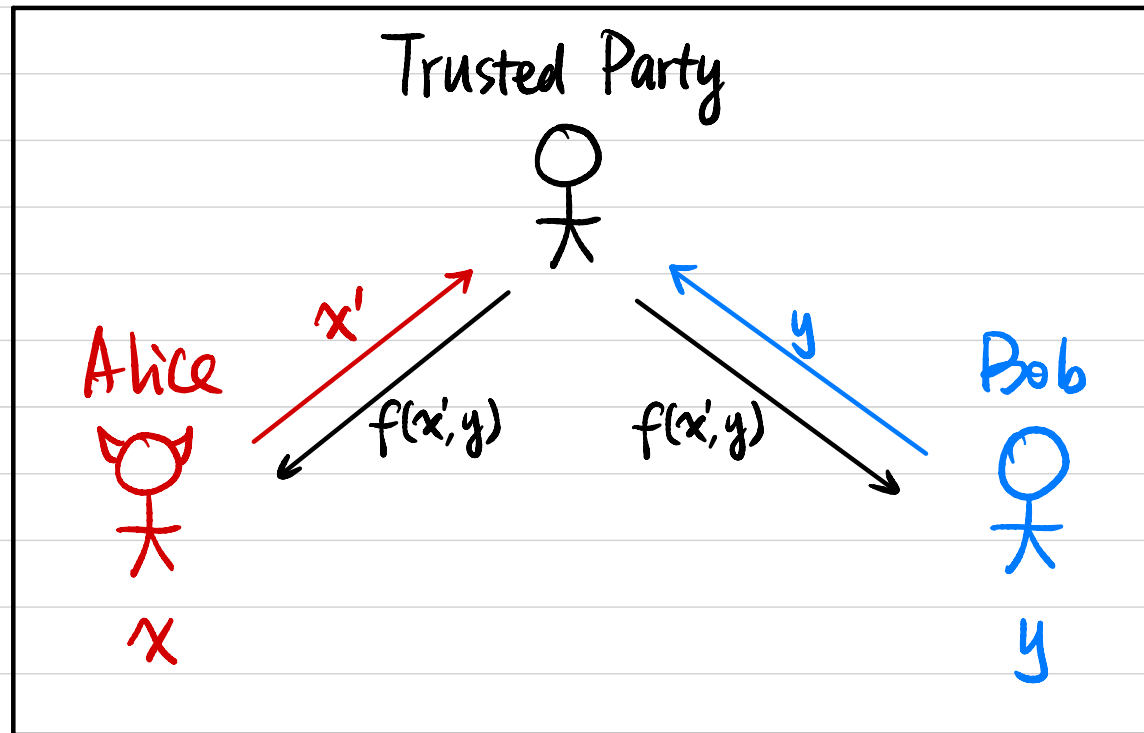
$$\left\{ \begin{pmatrix} S_A(1^n, x, f(x, y)) \\ f(x, y) \end{pmatrix} \right\}_{n \in \mathbb{N}} \approx \left\{ \begin{pmatrix} \text{View}_A^\Pi(x, y, n) \\ \text{Output}^\Pi(x, y, n) \end{pmatrix} \right\}_{n \in \mathbb{N}}$$

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

perfect / statistical / computational
 $\equiv \quad \stackrel{s}{\approx} \quad \stackrel{c}{\approx}$

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 A corrupting party $i \in \{ \text{Alice}, \text{Bob} \}$

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

Execution in the Ideal World:

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

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

Def (malicious security for ZPC)

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

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

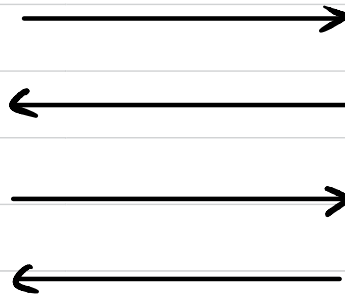
Private Set Intersection (PSI)

Alice



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

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



Bob



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

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

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

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

Private Set Intersection (PSI)

Alice



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

$H(x_1), \dots, H(x_n)$ →

Bob



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

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



$X \cap Y$

Is it (semi-honest) secure?

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

DDH-based PSI

Cyclic group G of order q with generator g

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

Alice



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

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

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

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

$$\leftarrow X \cap Y$$

Bob



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

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

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

$$\Downarrow \\ X \cap Y$$

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

$$S_A(1^n, X, I = X \cap Y)$$

Alice



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

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

← ?

→ $H(X)^{k_A}, H(Y)^{k_A \cdot k_B}$

← ?

$$S_B(1^n, Y, I = X \cap Y)$$

Bob



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

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

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

$\xrightarrow{?}$

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

$\Downarrow$

$\xleftarrow{X \cap Y}$

$X \cap Y$

PSI-CA?

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

Alice



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

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

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

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

$$\leftarrow X \cap Y$$

Bob



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

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

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

$$\Downarrow \\ X \cap Y$$

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



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

Output: $\perp$



Receiver



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

Output: m_c

Oblivious Transfer (OT)

Cyclic group G of order q with generator g
 $H: G \rightarrow \{0,1\}^L$

Sender

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

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

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

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

$$k_0 := H(B^a)$$

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

$$\xrightarrow{\begin{array}{l} ct_0 := k_0 \oplus m_0 \\ ct_1 := k_1 \oplus m_1 \end{array}}$$

Receiver

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

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

Output: ?

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

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

Sender

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

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

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

$$\xleftarrow{?}$$

$$k_0 := H(B^a)$$

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

$$\xrightarrow{\begin{array}{l} ct_0 := k_0 \oplus m_0 \\ ct_1 := k_1 \oplus m_1 \end{array}}$$

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

Receiver

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

→ ?

← $B = g^b \cdot A^c$

→ ?

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

Output: ?