SMP model, PSM protocols, and their quantum analogues

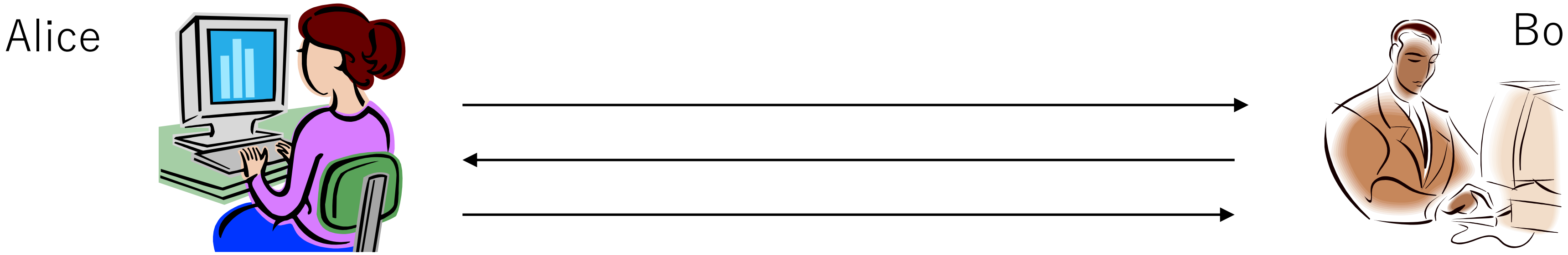
Harumichi Nishimura (Grad. School of Informatics, Nagoya U)
Based on joint work with Akinori Kawachi (Mie U)

June 22, 2021
SUSTech-Nagoya workshop on Quantum Science

Outline

- Setting
  - SMP
  - PSM
- Results
- Open problems

Communication Complexity



Andrew C.-C. Yao

Input: $x \in X$ → Output $f(x, y) \in Z$

Input $y \in Y$ → Output $f(x, y)$

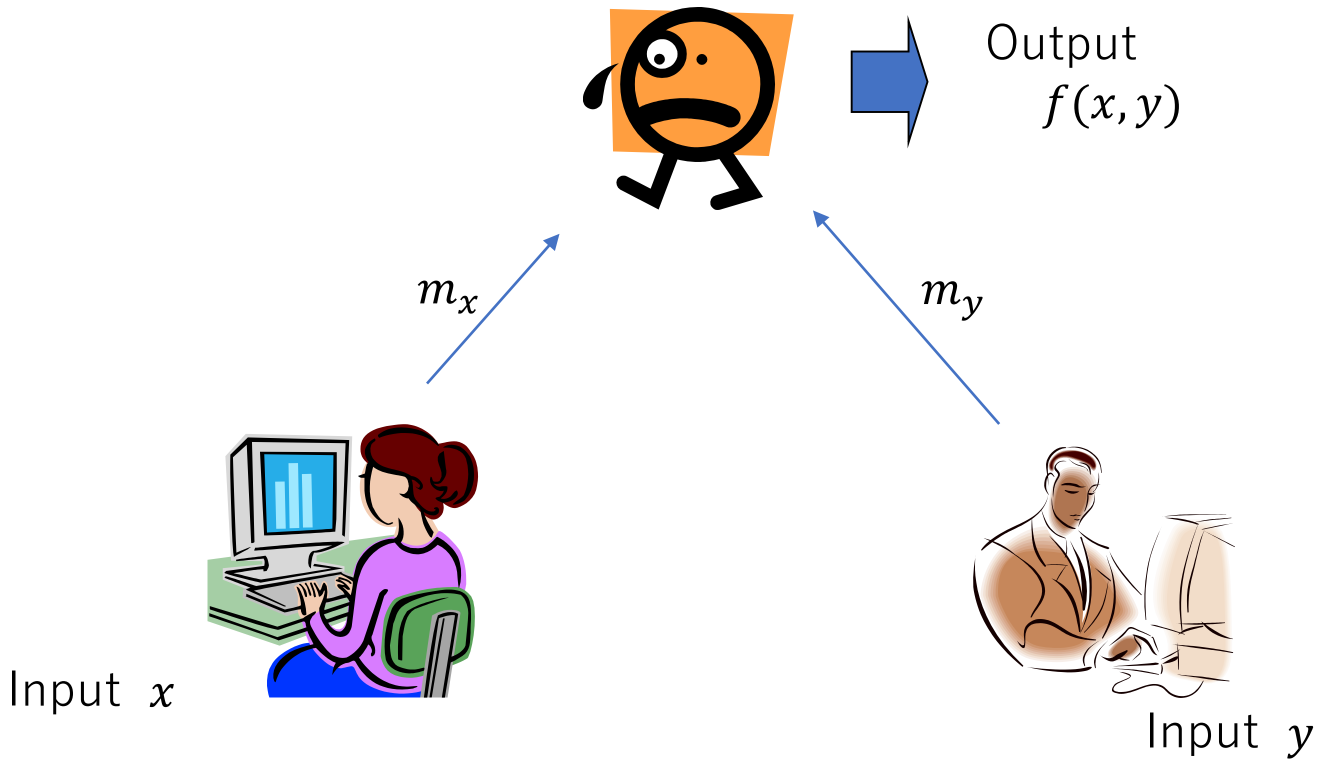
Communication complexity (CC) of $f : X \times Y \to Z$:= the length of bits communicated for computing f in the best communication protocol

- Consider the worst-case on all input pairs (x, y)
- Tool for the lower bound proofs in computational complexity

https://www.kyotoprize.org/en/210618

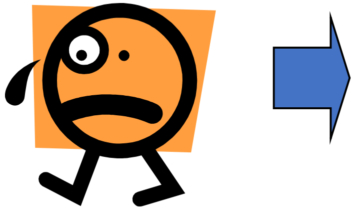
SMP Model

- SMP (Simultaneous Message Passing)
  - Most simplest setting in communication complexity
  - $CC^{smp}(f)$:=CC of f in the SMP model



Example: PARITY

- $CC^{smp}(PARITY_n) = 2$



Output
$PARITY_n(x, y) = \sum_{i=1}^{n}(x_i + y_i) \bmod 2$

m_x

m_y

Input $x = x_1 x_2 \cdots x_n \in \{0,1\}^n$

Input $y = y_1 y_2 \cdots y_n \in \{0,1\}^n$

Example: Equality

- $CC^{smp}(EQ_n) = 2n$
- LB: Reduction to distinguishability

$$EQ_n = \begin{bmatrix} 1 & 0 & & & & & & 0 \\ 0 & 1 & 0 & & & & & \\ & 0 & 1 & & & & & \\ & & & 1 & 0 & & & \\ & & & 0 & 1 & & & \\ & & & & & 1 & 0 & \\ & & & & & 0 & 1 & 0 \\ 0 & 0 & 0 & & & & 0 & 1 \end{bmatrix}$$

m_x $\quad$ $m_{x'}$

Output

$$EQ_n(x,y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$$

m_x $\quad$ m_y

Input $x = x_1 x_2 \cdots x_n \in \{0,1\}^n$ $\quad$ Input $y = y_1 y_2 \cdots y_n \in \{0,1\}^n$

Bounded-Error Setting

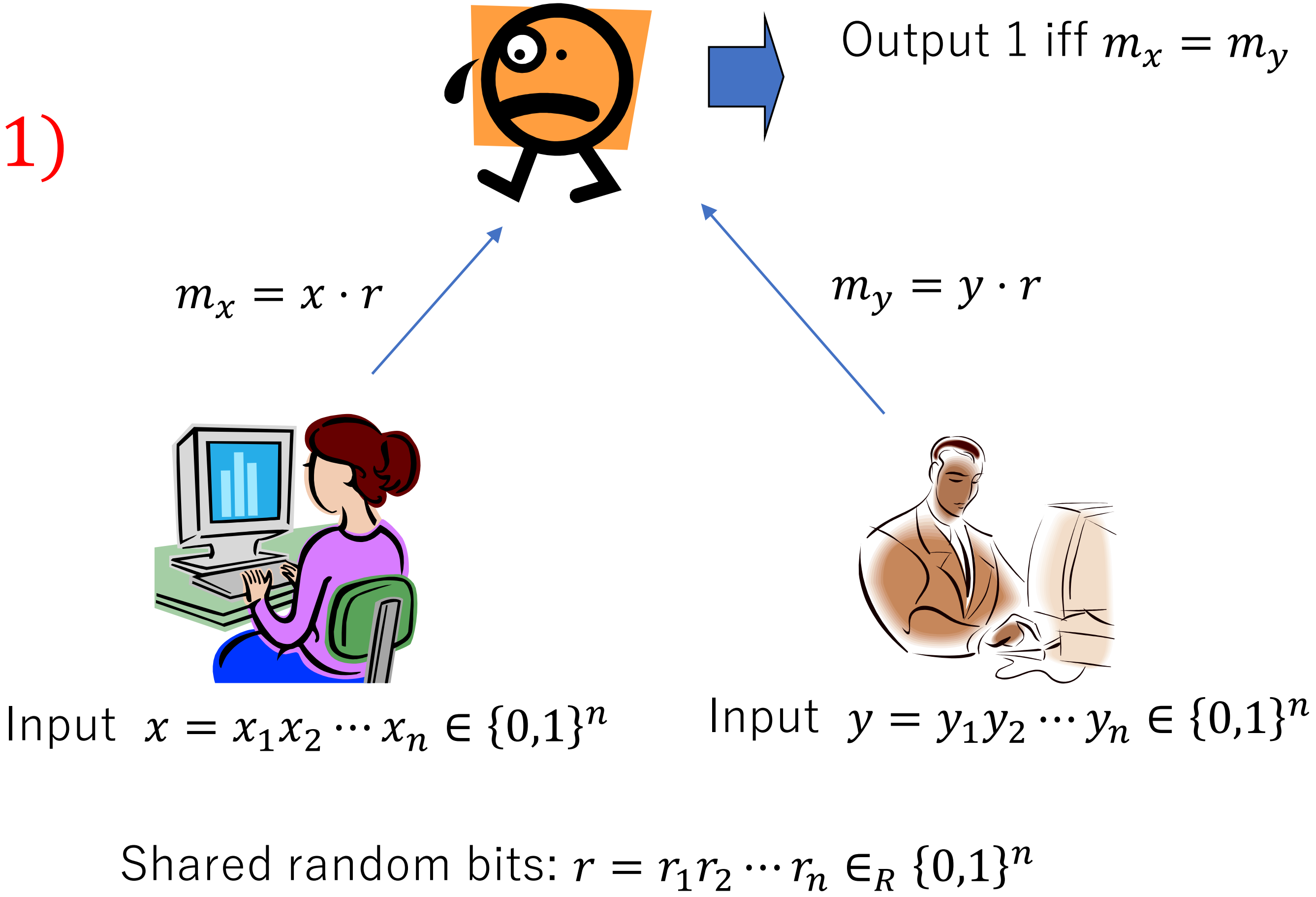
- Alice & Bob may use “randomness” (randomized protocol)
  - Referee do not always need to output the correct answer but needs to do it “with high probability” (say with probability 2/3)
  - $RCC^{smp}(f)$ ≔bounded-error SMP complexity of f
  - For comparison, the case that does not use randomness is called “exact”

Bounded-Error Setting

- Alice & Bob may use randomness (randomized protocol)
  - Referee do not always need to output the correct answer but needs to do it with high probability (say with probability 2/3)
  - $RCC^{smp}(f)$:=bounded-error SMP complexity of f (with private randomness)
- Two types for randomness
  - Private randomness: Alice & Bob (& Referee) must prepare randomness separately
  - Public (shared) randomness: Alice & Bob may share randomness
  - $RCC^{smp,pub}(f)$:=bounded-error SMP complexity of f (with shared randomness)

Example: Equality

- $RCC^{smp,pub}(EQ_n) = O(1)$

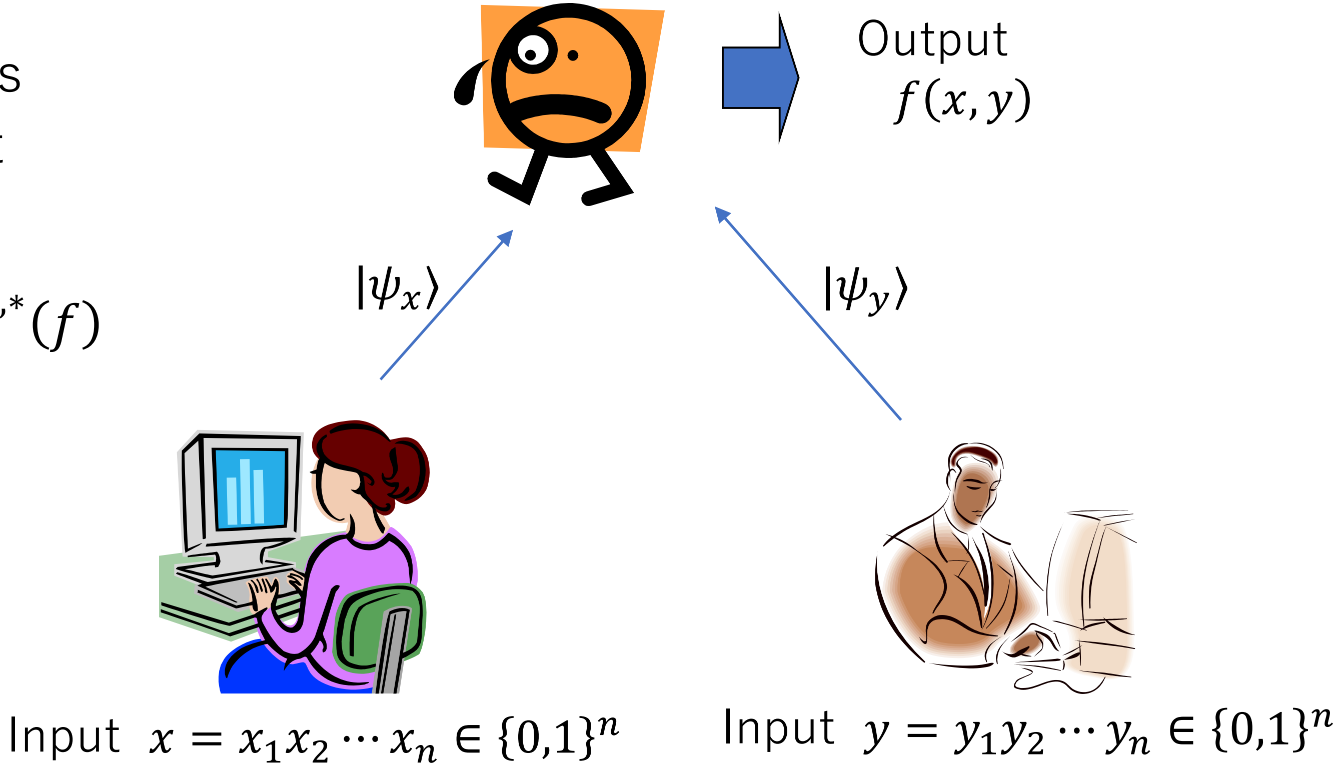


SMP complexity of EQ

- $CC^{smp}(EQ_n) = 2n$
- $RCC^{smp,pub}(EQ_n) = O(1)$
- $RCC^{smp}(EQ_n) = \Theta(\sqrt{n})$ [Amb96,NS96,BK97]

Quantum SMP

- Alice & Bob may send qubits
  - Every party can use quantum computers
- 3 types of bounded-error QSMP
  - $QCC^{smp}(f)$: no shared resource
  - $QCC^{smp,pub}(f)$: shared randomness
  - $QCC^{smp,*}(f)$: shared entanglement
- Exact case
  - $QCC_0^{smp}(f), QCC_0^{smp,pub}(f), QCC_0^{smp,*}(f)$

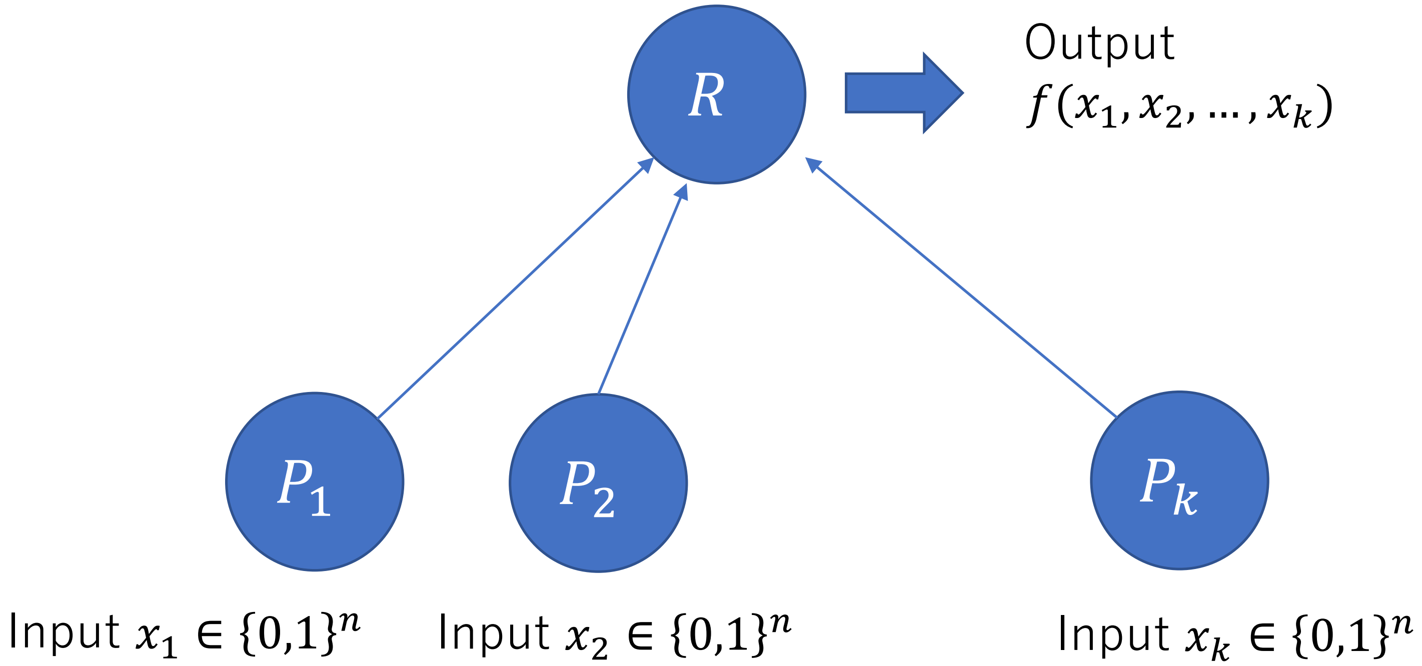


SMP complexity of EQ

- Classical Case
  - $CC^{smp}(EQ_n) = 2n$
  - $RCC^{smp,pub}(EQ_n) = O(1)$
  - $RCC^{smp}(EQ_n) = \Theta(\sqrt{n})$ [Amb96,NS96,BK97]
- Quantum Case
  - $QCC_0^{smp}(EQ_n) = QCC_0^{smp,pub}(EQ_n) = 2n$
  - $QCC_0^{smp,*}(EQ_n) = n$ [HSWCLS05]
  - $QCC^{smp}(EQ_n) = O(\log n)$ [BCWW01]

Extension to Multi-Party Case

- k-party SMP complexity of function $f: (\{0,1\}^n)^k \to \{0,1\}$:= the minimum number of bits sent to the referee R so that R can compute f
- CC of the trivial protocol$=kn$

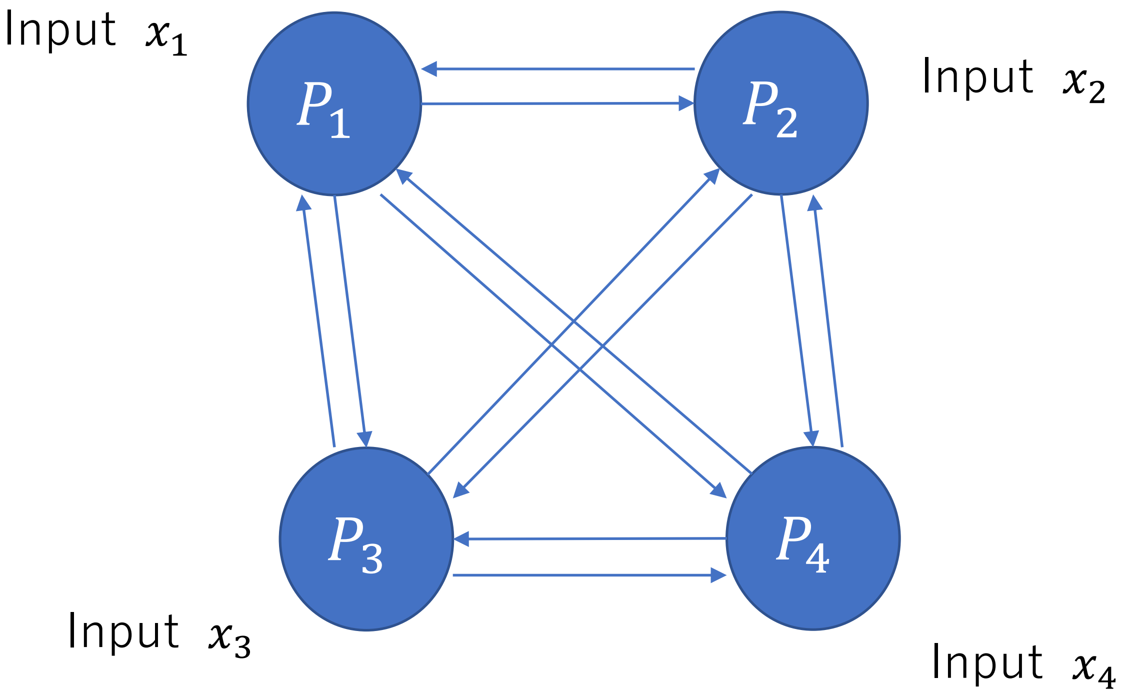


Outline

- Setting
  - SMP
  - PSM
- Results
- Open problems

Multi-Party Computation (MPC)

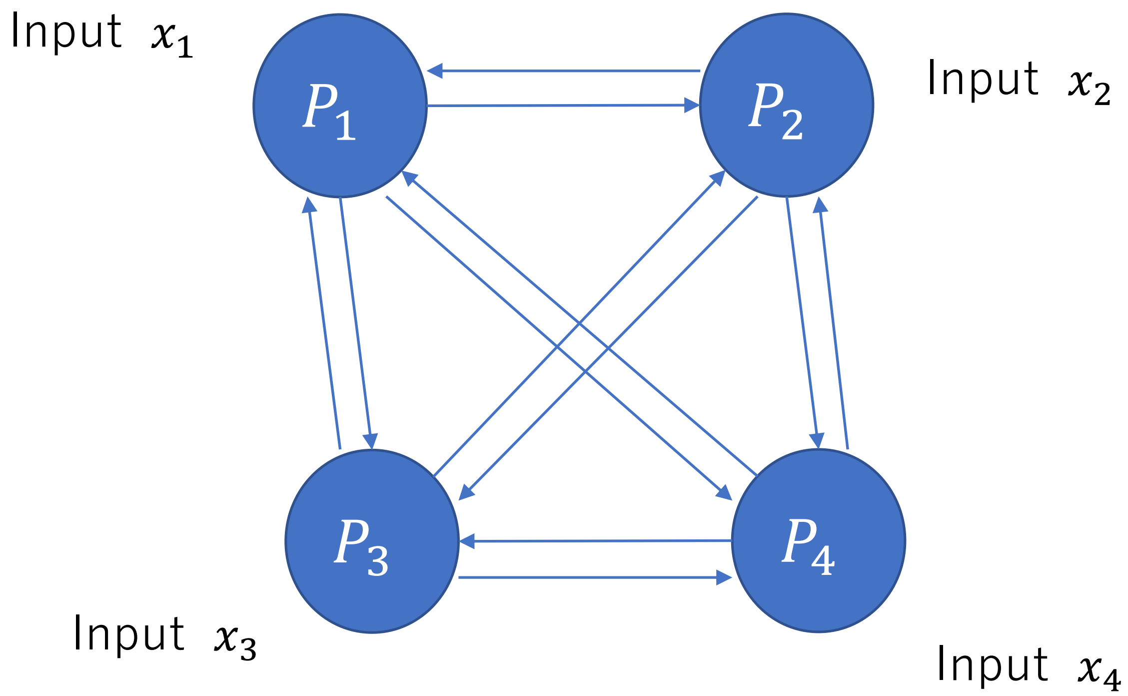
- Jointly computes $f(x_1, x_2, \ldots, x_k)$ with revealing nothing but $f(x_1, x_2, \ldots, x_k)$



Communication Complexity of MPC

- Communication complexity of k-party MPC for function $f: (\{0,1\}^n)^k \rightarrow \{0,1\}$
  := the minimum number of bits sent with one other to implement a MPC for f

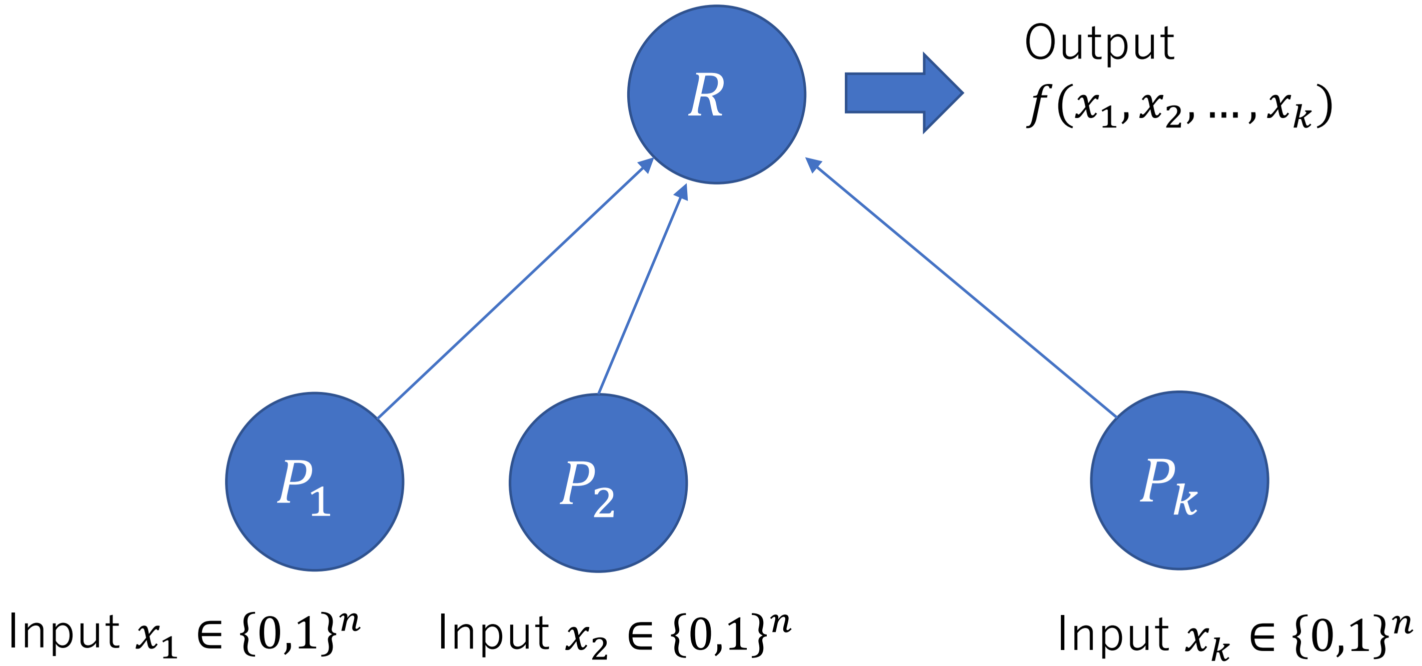
Q. How much is the communication complexity of MPC?



PSM model

- PSM (Private Simultaneous Message)
  - Simplest MPC model [FKN94]; SMP + Security condition

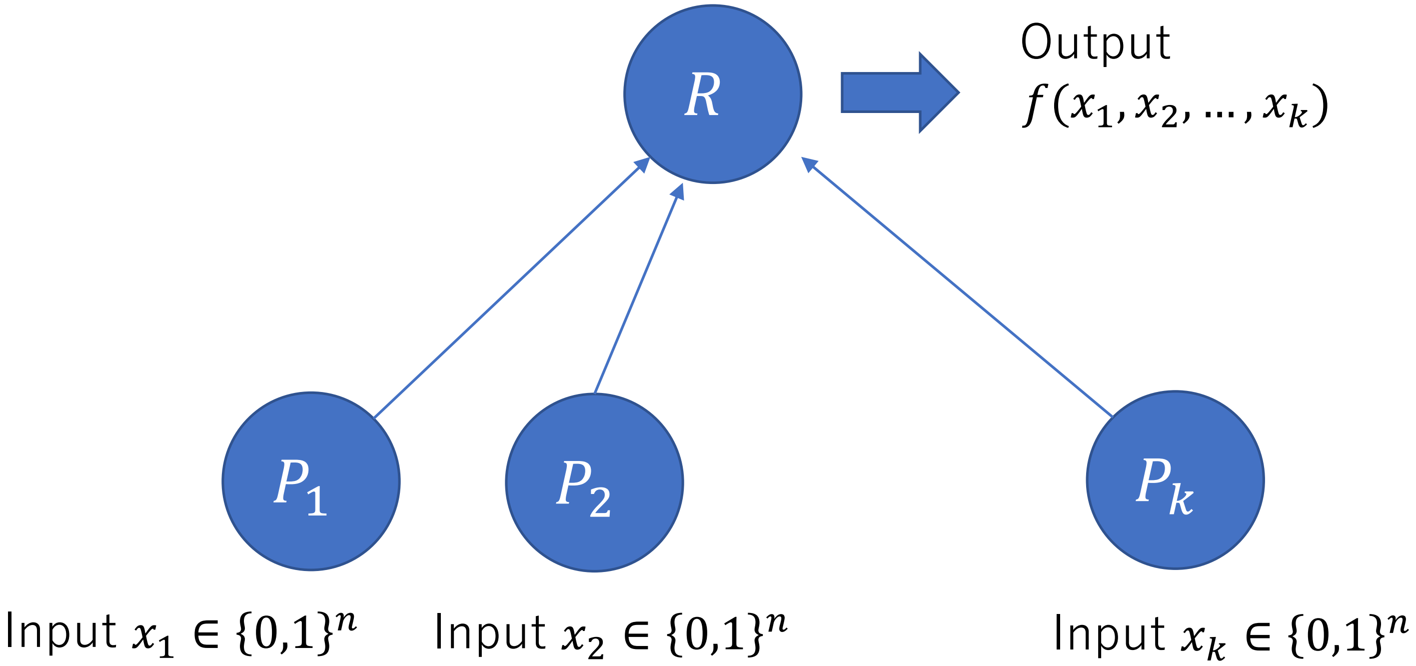
(security) Referee must not learn any information but $f(x_1, x_2, \dots, x_k)$



PSM model

- PSM (Private Simultaneous Message)
  - Simplest MPC model [FKN94]; SMP + Security condition

  (security) Referee must not learn any information but $f(x_1, x_2, \ldots, x_n)$



$$EQ_n = \begin{bmatrix} 1 & 0 & & & & & & 0 \\ 0 & 1 & 0 & & & & & \\ & 0 & 1 & & & & & \\ & & & 1 & 0 & & & \\ & & & 0 & 1 & & & \\ & & & & & 1 & 0 & \\ & & & & & 0 & 1 & 0 \\ 0 & 0 & 0 & & & & 0 & 1 \end{bmatrix} \begin{matrix} \\ \\ \\ m_y \\ m_{y'} \\ \\ \\ \\ \end{matrix}$$

$$\qquad\qquad\qquad m_x \qquad m_{x'}$$

$R(m_x, m_y) = R(m_{x'}, m_{y'}) = 1$

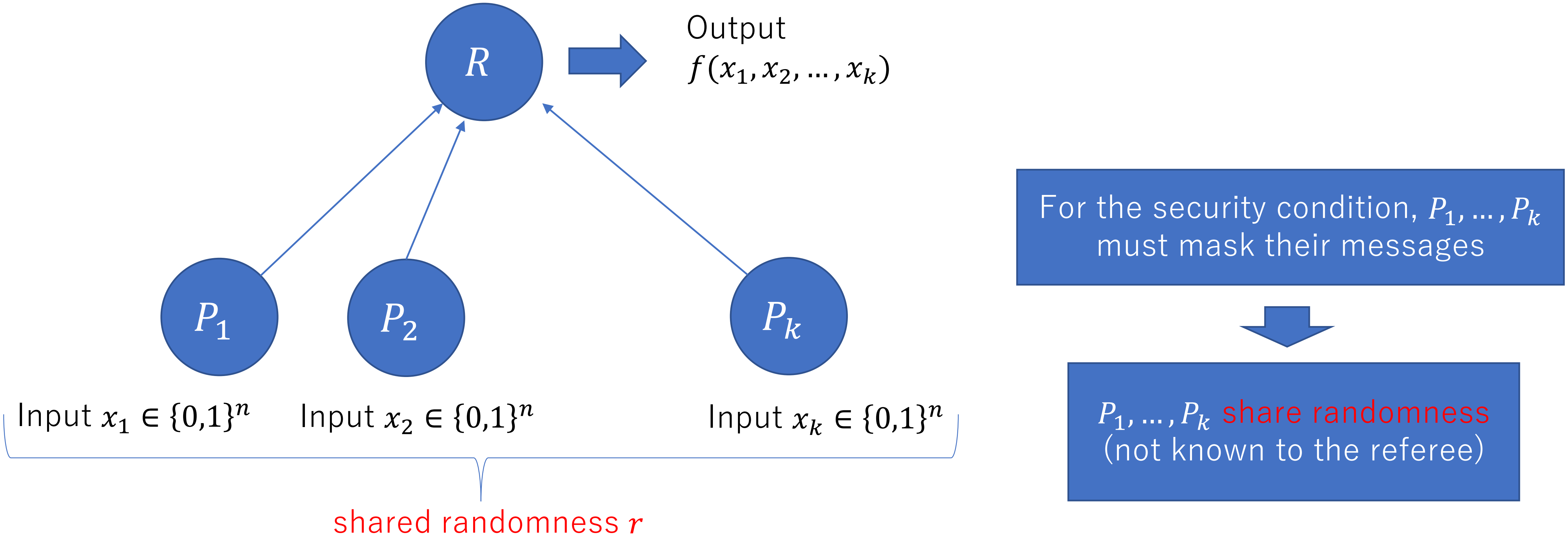
but $(m_x, m_y) \neq (m_{x'}, m_{y'})$

For the security condition, $P_1, \ldots, P_k$ must mask their messages

PSM model

- PSM (Private Simultaneous Message)
  - Simplest MPC model [FKN94]; SMP + Security condition

(security) Referee must not learn any information but $f(x_1, x_2, \ldots, x_n)$

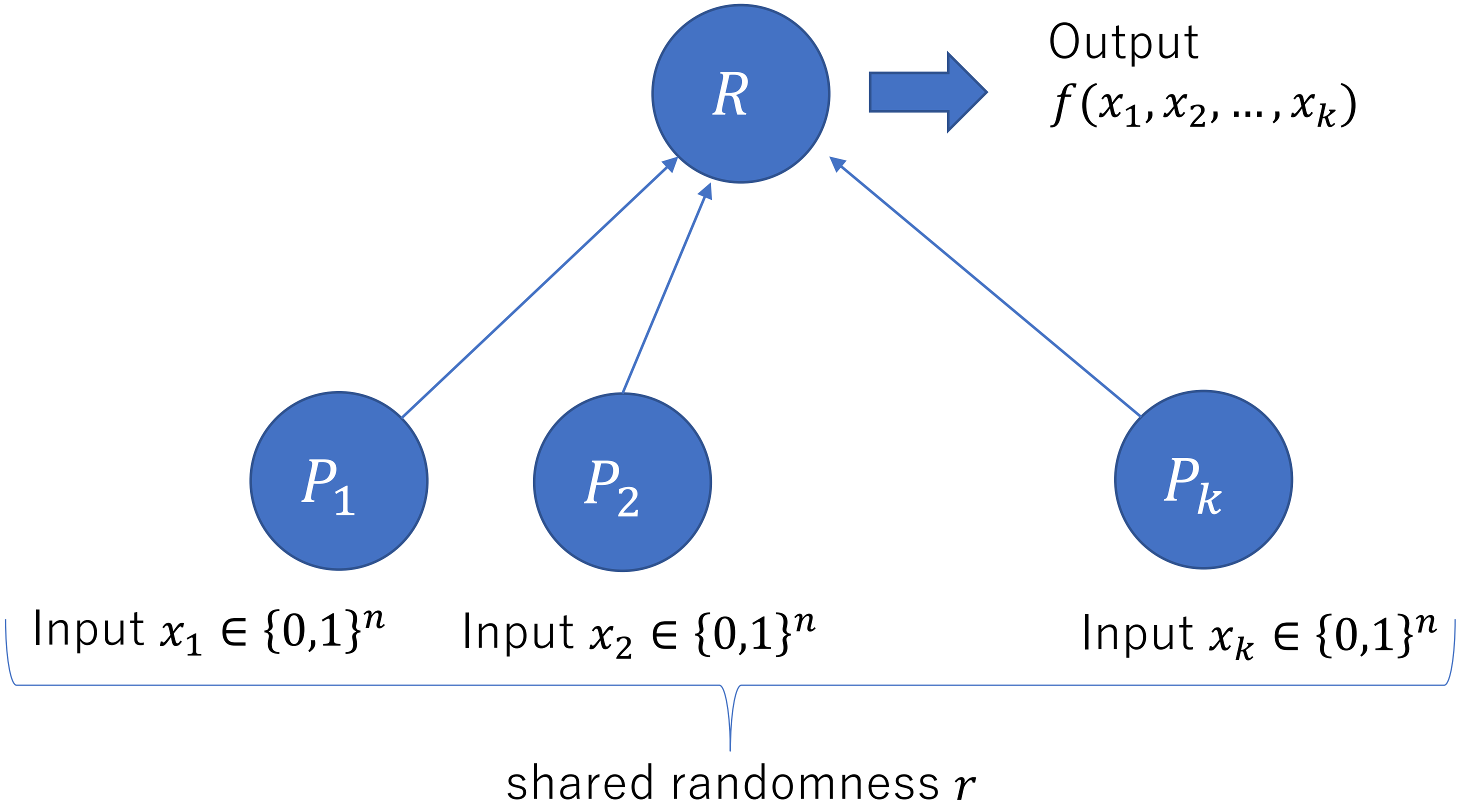


Simulator: Formal definition of Security

- PSM (Private Simultaneous Message)

  (correctness) The output of the referee is $f(x_1, x_2, \ldots, x_k)$

  (security) There is an algorithm (simulator) that given $f(x_1, x_2, \ldots, x_k)$ as input, produces the messages to the referee



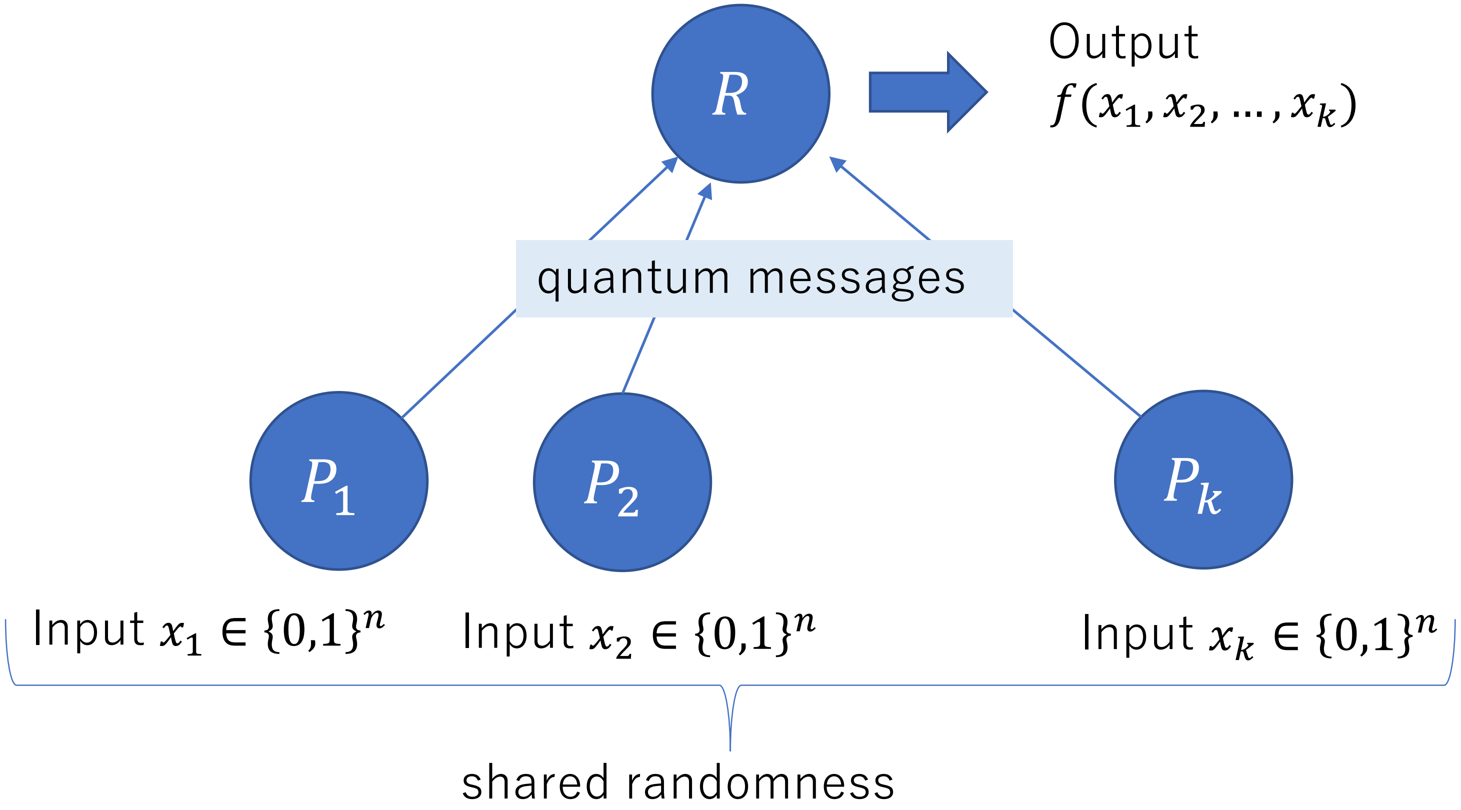
$CC^{psm}(f)$:=CC of PSM for f

PSQM model

- PSQM (Private Simultaneous Quantum Message)

  (correctness) The output of the referee is $f(x_1, x_2, \ldots, x_k)$ (with probability 1)

  (security) There is a quantum algorithm (simulator) that given $f(x_1, x_2, \ldots, x_k)$ as input, produces the quantum messages to the referee



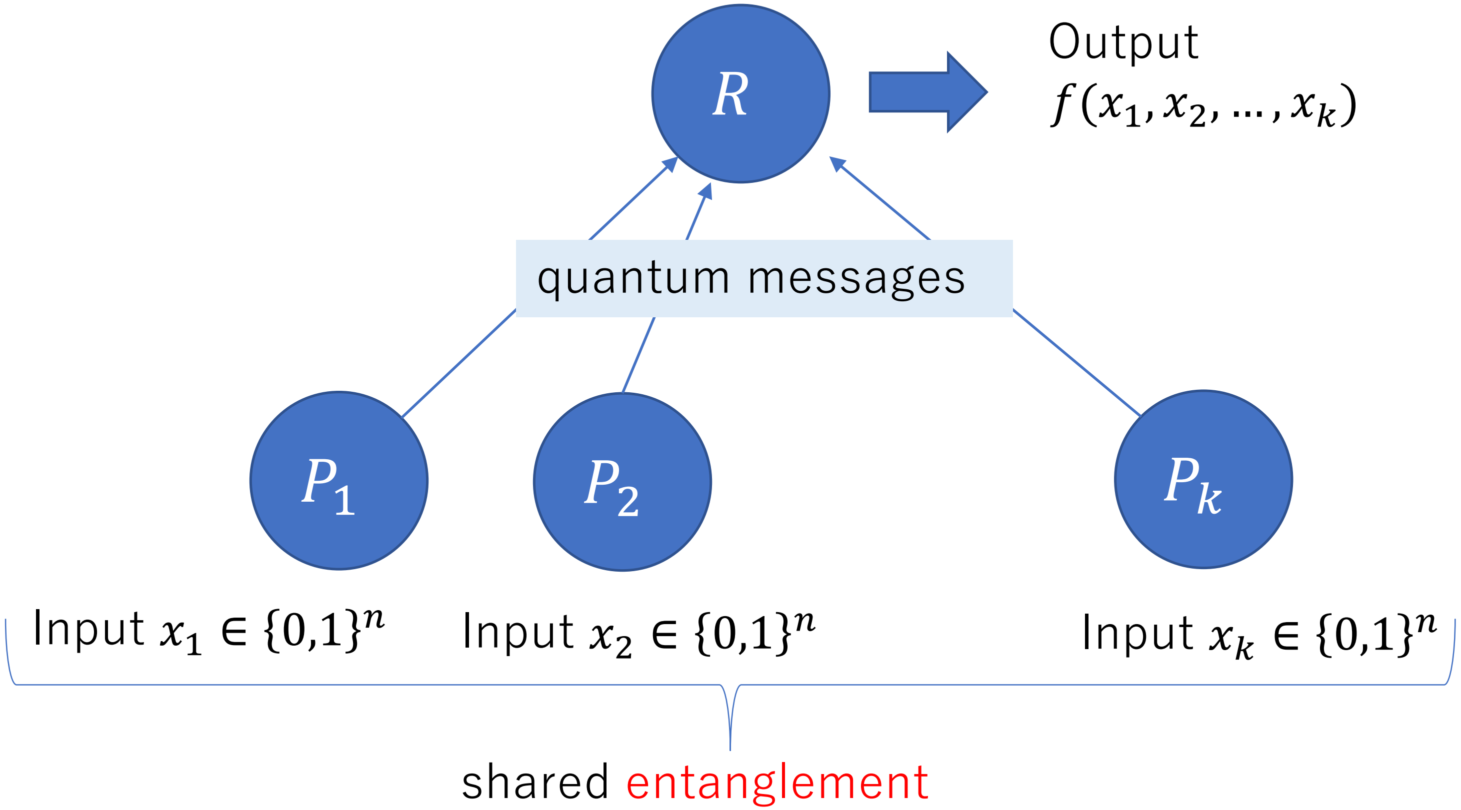
$QCC_0^{psm}(f)$:=CC of PSQM for f

PSQM model with shared entanglement

- PSQM (Private Simultaneous Quantum Message)

  (correctness) The output of the referee is $f(x_1, x_2, \ldots, x_k)$ (with probability 1)

  (security) There is a quantum algorithm (simulator) that given $f(x_1, x_2, \ldots, x_k)$ as input, produces the quantum messages to the referee



$QCC_0^{psm,*}(f)$:=CC of PSQM with shared entanglement for f

Outline

- Setting
  - SMP
  - PSM
- Results
  - Example
  - Known results
  - Our results
- Open problems

Example: PSM for (2-party) Equality

- $EQ_n(x,y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$
- PSM for $EQ_n(x,y)$
  - Identifies n-bit strings with elements in F_{2^n}
  - P_1 & P_2 share random elements $r_1 \in F_{2^n} \setminus \{0\}$ & $r_2 \in F_{2^n}$

1. P_1 and P_2 send $m_1 = r_1 x + r_2$ and $m_2 = r_1 y + r_2$, respectively
2. R outputs 1 iff $m_1 = m_2$

PSM for (2-party) Equality

- $EQ_n(x, y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$
- PSM for $EQ_n(x, y)$
  - Identifies n-bit strings with elements in F_{2^n}
  - P_1 & P_2 share random elements $r_1 \in F_{2^n} \setminus \{0\}$ & $r_2 \in F_{2^n}$

  1. P_1 and P_2 send $m_1 = r_1 x + r_2$ and $m_2 = r_1 y + r_2$, respectively
  2. R outputs 1 iff $m_1 = m_2$
- $CC^{psm}(EQ_n) = 2n$

PSM for (2-party) Equality

(correctness) The output of the referee is $EQ(x, y)$
(security) There is an algorithm (simulator) that given $EQ(x, y)$ as input, produces the messages to the referee

- $EQ_n(x, y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$
- PSM for $EQ_n(x, y)$
  - Identifies n-bit strings with elements in F_{2^n}
  - P_1 & P_2 share random elements $r_1 \in F_{2^n} \setminus \{0\}$ & $r_2 \in F_{2^n}$

1. P_1 and P_2 send $m_1 = r_1 x + r_2$ and $m_2 = r_1 y + r_2$, respectively
2. R outputs 1 iff $m_1 = m_2$

PSM for (2-party) Equality

(correctness) The output of the referee is $EQ(x,y)$
(security) There is an algorithm (simulator) that given $EQ(x,y)$ as input, produces the messages to the referee

- $EQ_n(x,y) = \begin{cases} 1 & (x = y) \\ 0 & (x \neq y) \end{cases}$
- PSM for $EQ_n(x,y)$
  - Identifies n-bit strings with elements in F_{2^n}
  - P_1 & P_2 share random elements $r_1 \in F_{2^n} \setminus \{0\}$ & $r_2 \in F_{2^n}$
  1. P_1 and P_2 send $m_1 = r_1 x + r_2$ and $m_2 = r_1 y + r_2$, respectively
  2. R outputs 1 iff $m_1 = m_2$
- Simulator
  - On input 1: Take $r \in_R F_{2^n}$ and output (r, r)
  - On input 0: Take different r, r' from F_{2^n} uniformly at random and output (r, r')

Results on PSM: Upper bounds

- Feige, Kilian & Naor (1994)
  - Proposal of PSM model
  - 2-party PSM for “any” Boolean function with exponential CC
- Ishai & Kushilevitz (1997)
  - Efficient k-party PSM for any $\#L$ function
- Many other PSM protocols for specific functions

Results on PSM: Lower bounds

- Feige, Kilian & Naor (1994)
  - Proposal of PSM model
  - 2-party PSM for "any" Boolean function with exponential CC
- Ishai & Kushilevitz (1997)
  - Efficient k-party PSM for any $\#L$ function
- Many other PSM protocols for specific functions
- Applebaum, Holenstein, Mishra & Shayevitz (2020)
  - $(3 - o(1))n$ lower bounds of 2-party PSM for $2n$-input random functions
  - If no privacy requirement, trivial upper bound $= 2n$

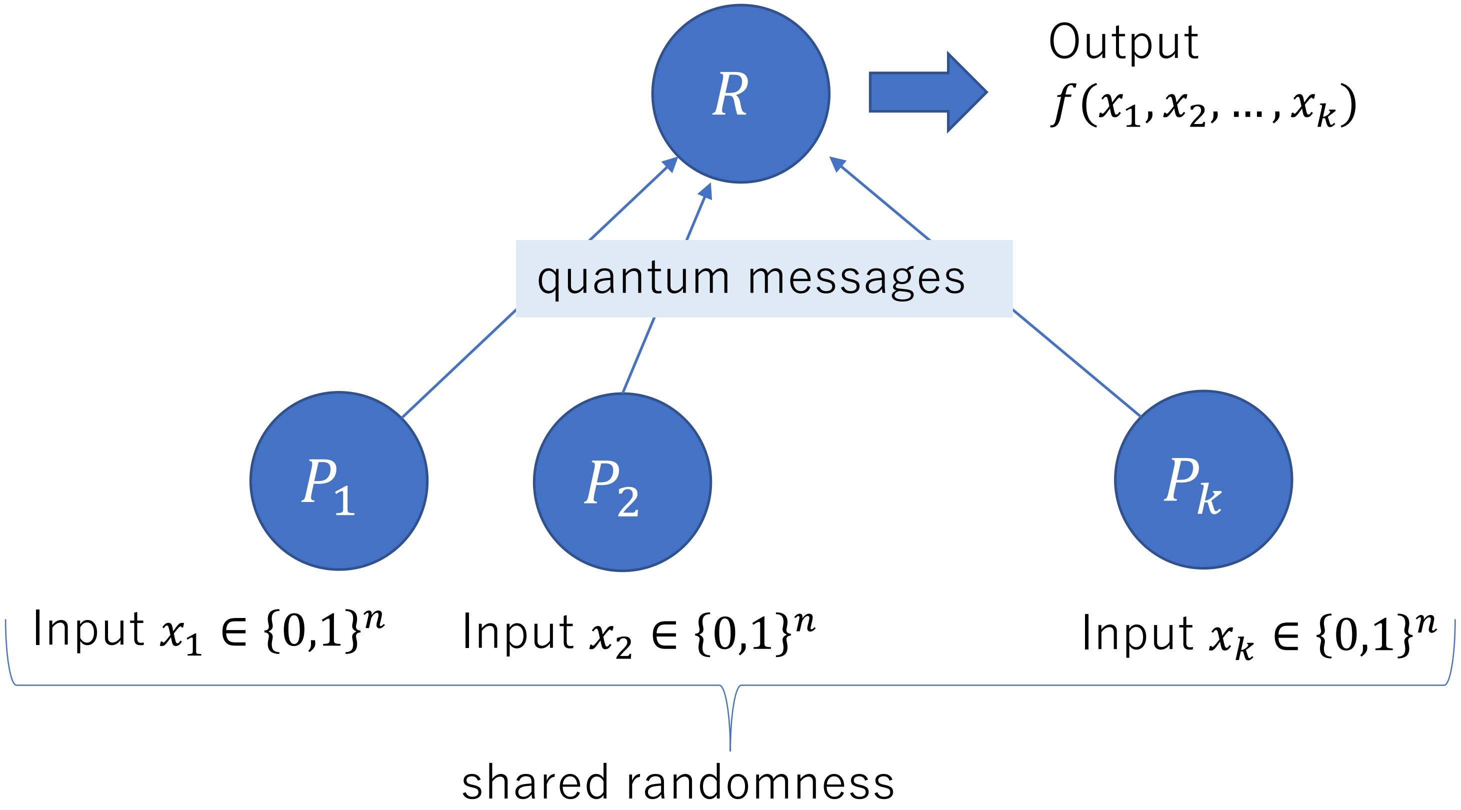
  ➔Implies privacy essentially requires additional communication cost!

Our model: PSQM model

- PSQM (Private Simultaneous Quantum Message)

(correctness) The output of the referee is $f(x_1, x_2, \dots, x_k)$ (with probability 1)

(security) There is a quantum algorithm (simulator) that given $f(x_1, x_2, \dots, x_k)$ as input, produces the quantum messages to the referee



$QCC_0^{psm}(f)$:=CC of PSQM for f

Q. Is there any non-trivial lower bounds?

Our Result (1): 2-party case

- Applebaum, Holenstein, Mishra & Shayevitz (2020)
  - $(3 - o(1))n$ lower bounds of 2-party PSM for $2n$-input random functions
  - If no privacy requirement, trivial upper bound $= 2n$

  ➔Implies privacy essentially requires additional communication cost!

Result 1: For $1 - o(1)$ fraction of functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,
$QCC_0^{psm}(f) \geq (3 - o(1))n$

  - $(3 - o(1))n$ lower bounds of 2-party PSQM for $2n$-input random functions

Our Result (1): 2-party case

- Applebaum, Holenstein, Mishra & Shayevitz (2020)
  - $(3 - o(1))n$ lower bounds of 2-party PSM for $2n$-input random functions
  - If no privacy requirement, trivial upper bound $= 2n$

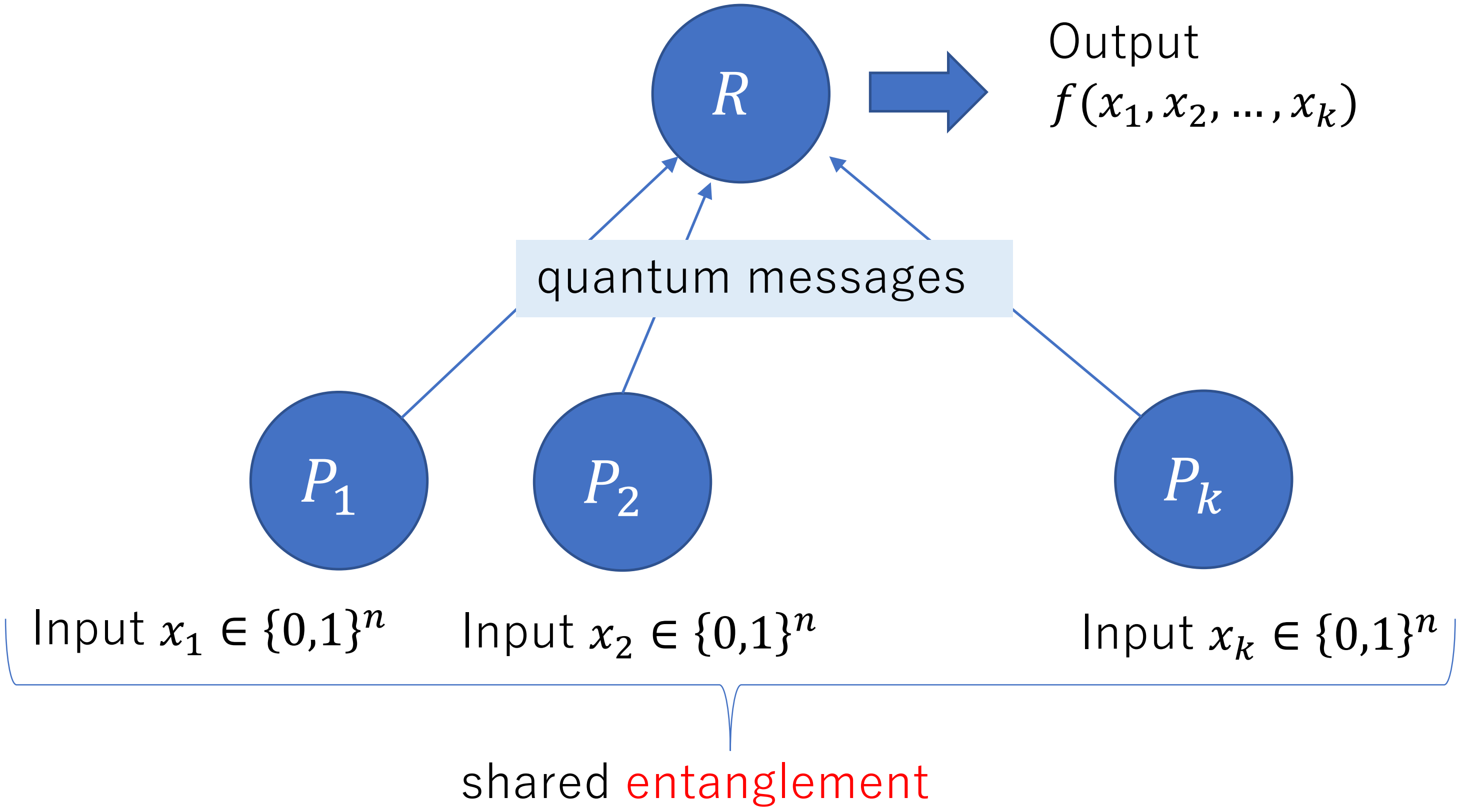
  ➔Implies privacy essentially requires additional communication cost!

Result 1: For $1 - o(1)$ fraction of functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$,
$QCC_0^{psm}(f) \geq (3 - o(1))n$

- $(3 - o(1))n$ lower bounds of 2-party PSQM for $2n$-input random functions
- Quantum extension of the combinatorial argument by Applebaum et al
  - Run the PSM protocol twice, and consider the collision probability $\Pr[m^1 = m^2]$ of the two messages
  - $\Pr[m^1 = m^2] \geq 1/|\text{message domain}|$
  - Analyze an upper bound of $P[m^1 = m^2]$

PSQM model with shared entanglement

- PSQM (Private Simultaneous Quantum Message)
  (correctness) The output of the referee is $f(x_1, x_2, \ldots, x_n)$ (with probability 1)
  (security) There is a quantum algorithm (simulator) that given $f(x_1, x_2, \ldots, x_n)$ as input, produces the quantum messages to the referee



$QCC_0^{psm,*}(f)$:=CC of PSQM with shared entanglement for f

Q. Are $QCC_0^{psm}(f)$ and $QCC_0^{psm,*}(f)$ different?

Shared randomness vs shared entanglement

Q. Are $QCC^{psm}(f)$ and $QCC^{psm,*}(f)$ different?

For SMP model (=PSM with no security);

- There is a relation problem such that $CC^{smp,*}$ is exponentially smaller than $QCC^{smp,pub}$ [GKRW09]
  - ◎Bounded-error result & exponential gap
  - △Not a Boolean function
- There is a partial function such that $CC_0^{smp,*}$ is exponentially smaller than $CC_0^{smp} = CC_0^{smp,pub}$ [BCT99]
  - △Exact case
  - ○Partial Boolean function
  - ◎Exponential gap

Our Result (2): 2-party case

- There is a partial function such that $CC_0^{smp,*}$ is exponentially smaller than $CC_0^{smp} = CC_0^{smp,pub}$ [BCT99]

  △Exact case

  ○Partial Boolean function

  ◎Exponential gap

Result 2: There is a partial function such that $CC_0^{psm,*}$ is exponentially smaller than QCC_0^{smp}

- Uses the function in [BCT99] (distributed Deutsch-Jozsa function)
  - $DJ_n(x,y) = \begin{cases} 1 & (x = y) \\ 0 & (Ham(x,y) = n/2) \end{cases}$
- Adds the security condition
- Shows the quantum SMP complexity lower bound

Shared randomness vs shared entanglement

Q. Are $QCC^{psm}(f)$ and $QCC^{psm,*}(f)$ different?

For SMP model (=PSM with no security);

- There is a relation problem such that $CC^{smp,*}$ is exponentially smaller than $QCC^{smp,pub}$ [GKRW09]
  ◎Bounded-error result & exponential gap
  △Not a Boolean function
- There is a partial function such that $CC_0^{smp,*}$ is exponentially smaller than CC_0^{smp} [BCT99]
  △Exact case
  ○Partial Boolean function
  ◎Exponential gap
- Total function EQ_n has $QCC_0^{smp}(EQ_n) = 2n$ and $QCC_0^{smp,*}(EQ_n) = n$ [HSWCLS05]
  △Exact case
  ◎Total Boolean function
  △Not large gap (but the best known gap for total functions including in the bounded-error setting)

Our Result (3): $\boldsymbol{k}$-party case

- Total function EQ_n has $QCC_0^{smp}(EQ_n) = 2n$ and $QCC_0^{smp,*}(EQ_n) = n$ [HSWCLS05]
  △Exact case
  ◎Total Boolean function
  △Not large gap (but the best known gap for total functions including in the bounded-error setting)

Result 3: A k-party total function $GEQ_n(x_1, x_2, \dots, x_k)$ (where $x_i \in \{0,1\}^n$) has $QCC_0^{psm}(GEQ_n) = kn$ and $QCC_0^{psm,*}(GEQ_n) = \frac{kn}{2}$

- $GEQ_n(x_1, x_2, \dots, x_k) = 1$ iff $\sum_{j=1}^{k} (x_j)_i = 0$ for all $i \in \{1,2,\dots,n\}$
- $GEQ_n(x_1, x_2) = EQ_n(x_1, x_2)$
- Multiparty extension of a protocol for $QCC_0^{smp,*}(EQ_n)$ + security
- Uses the cat state $\frac{1}{\sqrt{2}}(|0^k\rangle + |1^k\rangle)$ for two bits

Simplest case: $n = k = 2$

PSQM protocol for $EQ(x_1, x_2)$

- Shared: $|\Psi^{00}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_2 + |1\rangle_1|1\rangle_2)$ & $r \in F_4$

1. P_j applies X (Z, resp.) on register j iff the 1st (2nd, resp) bit of rx_j is 1
2. P_j sends register j to R
3. R measures registers 1 & 2 in the Bell basis $\left\{\left|\Psi^{ab}\right\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|a\rangle + (-1)^b\left|1\right\rangle|1-a\rangle\right): a, b \in \{0,1\}\right\}$, and the result corresponds to $|\Psi^{00}\rangle$ iff 1 is outputed

1\2	00	01	10	11
00	$|\Psi^{00}\rangle$	$|\Psi^{01}\rangle$	$|\Psi^{10}\rangle$	$|\Psi^{11}\rangle$
01	$|\Psi^{01}\rangle$	$|\Psi^{00}\rangle$	$|\Psi^{11}\rangle$	$|\Psi^{10}\rangle$
10	$|\Psi^{10}\rangle$	$|\Psi^{11}\rangle$	$|\Psi^{00}\rangle$	$|\Psi^{01}\rangle$
11	$|\Psi^{11}\rangle$	$|\Psi^{10}\rangle$	$|\Psi^{01}\rangle$	$|\Psi^{00}\rangle$

Outline

- Setting
  - SMP
  - PSM
- Results
- Open problems

Open Problems (1)

Result 1: For $1 - o(1)$ fraction of functions $f: \{0,1\}^n \times \{0,1\}^n \to \{0,1\}$, $QCC_0^{psm}(f) \geq \big(3 - o(1)\big)n$

OPEN:

- Extension to the shared entanglement case
- Extension to the bounded-error case
- Extension to a relaxed security condition
  - Simulator ⇒ Approximate simulator
  - Shown in the classical case by Applebaum et al. (2020)
- Not well-studied even in the classical case

Open Problems (2)

Result 2: There is a partial function such that $CC_0^{psm,*}$ is exponentially smaller than QCC_0^{smp}

Result 3: A k-party total function $GEQ_n(x_1, x_2, \dots, x_k)$ (where $x_i \in \{0,1\}^n$) has $QCC_0^{psm}(GEQ_n) = kn$ and $QCC_0^{psm,*}(GEQ_n) = \frac{kn}{2}$

OPEN:

- Bounded-error & relaxed security cases
  - ∃ relational problem R [$CC^{psm,*}(R) = O(\log n)$ but $QCC^{psm}(R) = \Omega(\frac{n^{1/3}}{\log n})$] [GKRW09]
- Bigger gaps for total functions (even in the SMP case)

Open Problems (3)

- QCC^{psm} vs CC^{psm}

  Cf. $QCC^{smp}(EQ_n) = O(\log n)$ but $CC^{smp}(EQ_n) = \Theta(\sqrt{n})$
- PSQM for “quantum” problems

THE END