Card-Based Protocols Imply PSM Protocols

Kazumasa Shinagawa (Ibaraki Univ. / AIST)
Koji Nuida (Kyushu Univ. / AIST)

Secure Computation

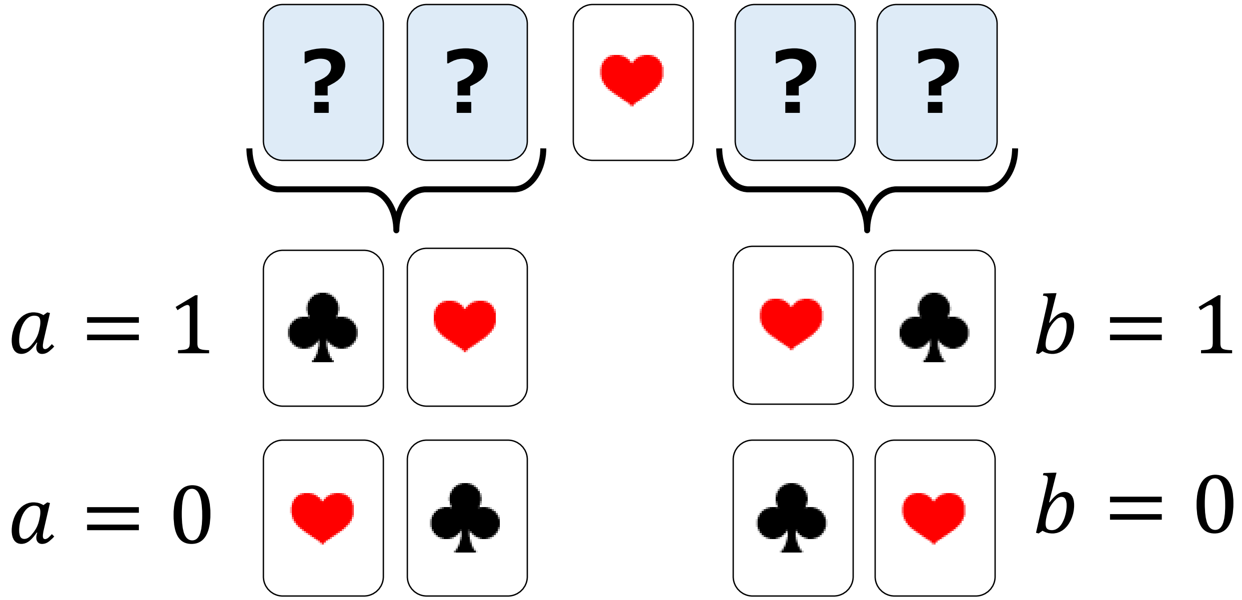
- **Secure computation** is a cryptographic technique to compute a function $f(x_1, \dots, x_n)$ hiding $x_1, \dots, x_n$ as much as possible

- Secure computation for the AND function $a \wedge b$
  - Alice and Bob have a private input $a, b \in \{0,1\}$, respectively
  - They wish to compute $a \wedge b$ hiding a, b as much as possible

- This can be done by using a **deck of physical cards**

Five-Card Trick (1/3)

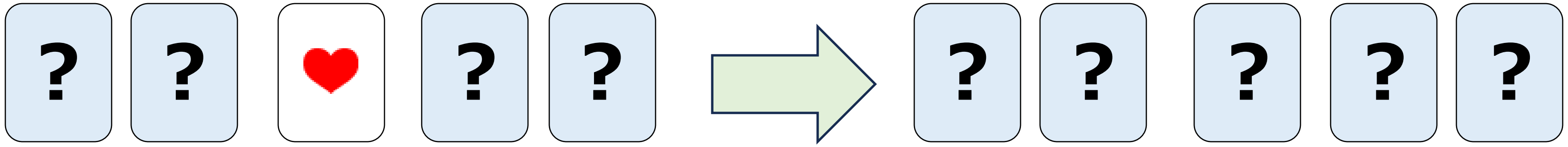
1. Alice and Bob place face-down cards as follows:



B. den Boer, More Efficient Match-Making and Satisfiability The Five Card Trick, EUROCRYPT 1989.

Five-Card Trick (2/3)

2. Turn over the center card.

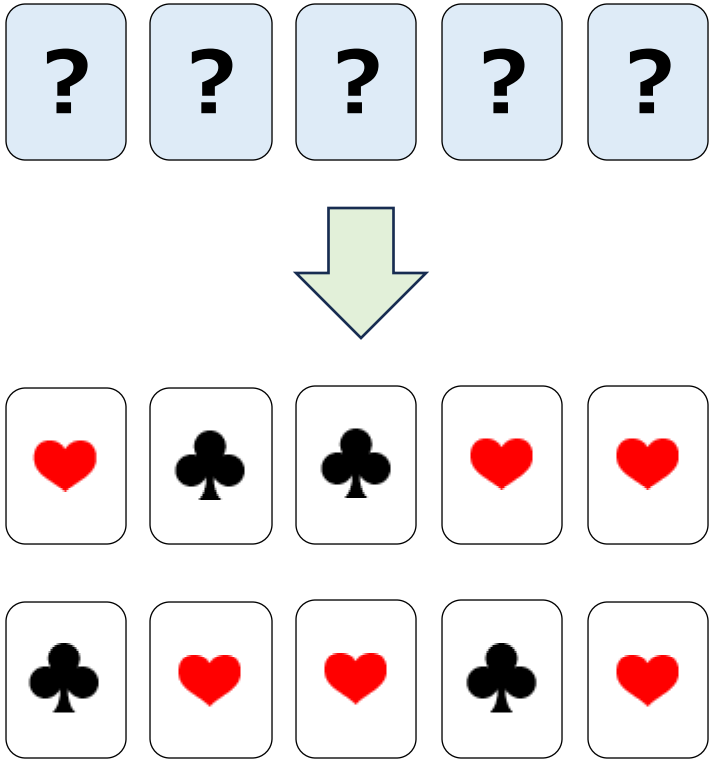


3. Apply a random shift of the sequence.

B. den Boer, More Efficient Match-Making and Satisfiability The Five Card Trick, EUROCRYPT 1989.

Five-Card Trick (3/3)

4. Open all cards.



Three consecutive ♥s $a \wedge b = 1$

Otherwise $a \wedge b = 0$

B. den Boer, More Efficient Match-Making and Satisfiability The Five Card Trick, EUROCRYPT 1989.

Correctness and Security of Five-Card Trick

- The input sequences just after Step 1 are as follows:

$(a,b)=(0,0)$	$(a,b)=(0,1)$	$(a,b)=(1,0)$	$(a,b)=(1,1)$
♥ ♣ ♥ ♣ ♥	♥ ♣ ♥ ♥ ♣	♣ ♥ ♥ ♣ ♥	♣ ♥ ♥ ♥ ♣

- Only the case of $(1,1)$ has consecutive three hearts (Correctness)
- Other three patterns are cyclically equal (Security)

Card-Based Cryptography

- Card-based cryptography is secure computation using cards
  - The first paper is published at EUROCRYPT 1989
  - Since then, more than 200 papers have been published

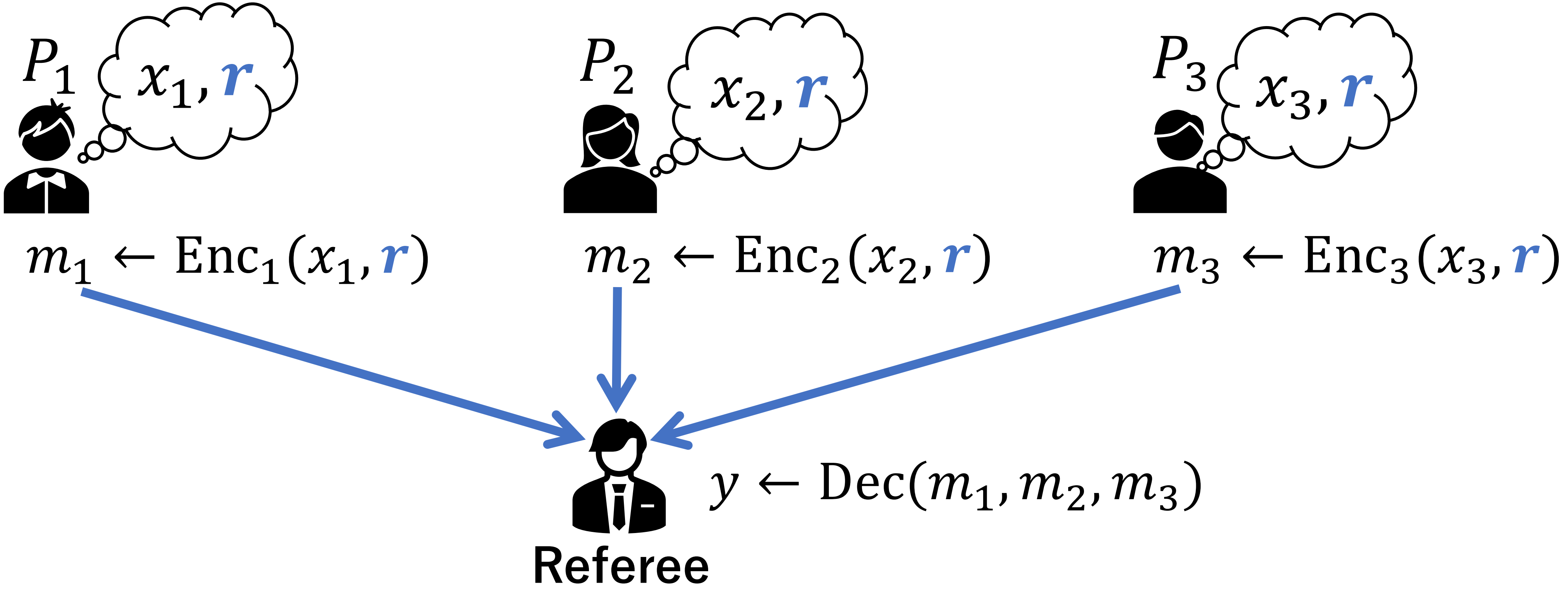
- Due to its good visualization, it is used for education

- However, no relationship between card-based cryptography and other conventional cryptography is found

Our Contribution

- The first generic conversion from card-based protocols to **private simultaneous messages (PSM) protocols**
- Given a card-based protocol for $f: \{0,1\}^n \to \{0,1\}$ opening t cards, we obtain a PSM protocol with t-bit communication per party
- Applications
  - A new method to construct PSM protocols
  - Lower bounds for card-based protocols from those for PSM protocols

Private Simultaneous Messages (PSM)



- **Correctness**: Referee obtains $y = f(x_1, x_2, x_3)$ correctly
- **Security**: Referee learns nothing about x_i beyond $f(x_1, x_2, x_3)$

Our Contribution

- The first generic conversion from card-based protocols to **private simultaneous messages (PSM) protocols**

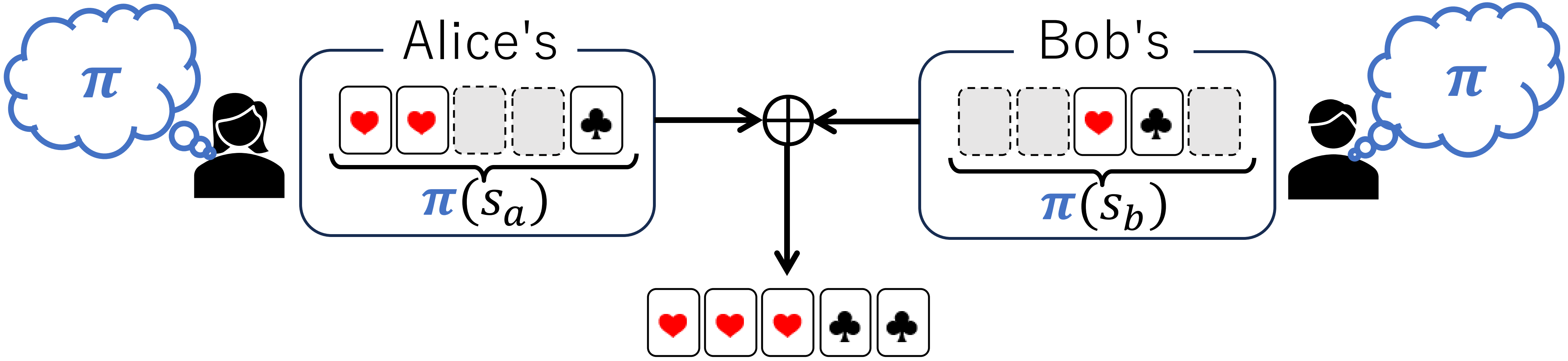
- Given a card-based protocol for $f: \{0,1\}^n \to \{0,1\}$ opening t cards, we obtain a PSM protocol with t-bit communication per party

- Applications
  - A new method to construct PSM protocols
  - Lower bounds for card-based protocols from those for PSM protocols

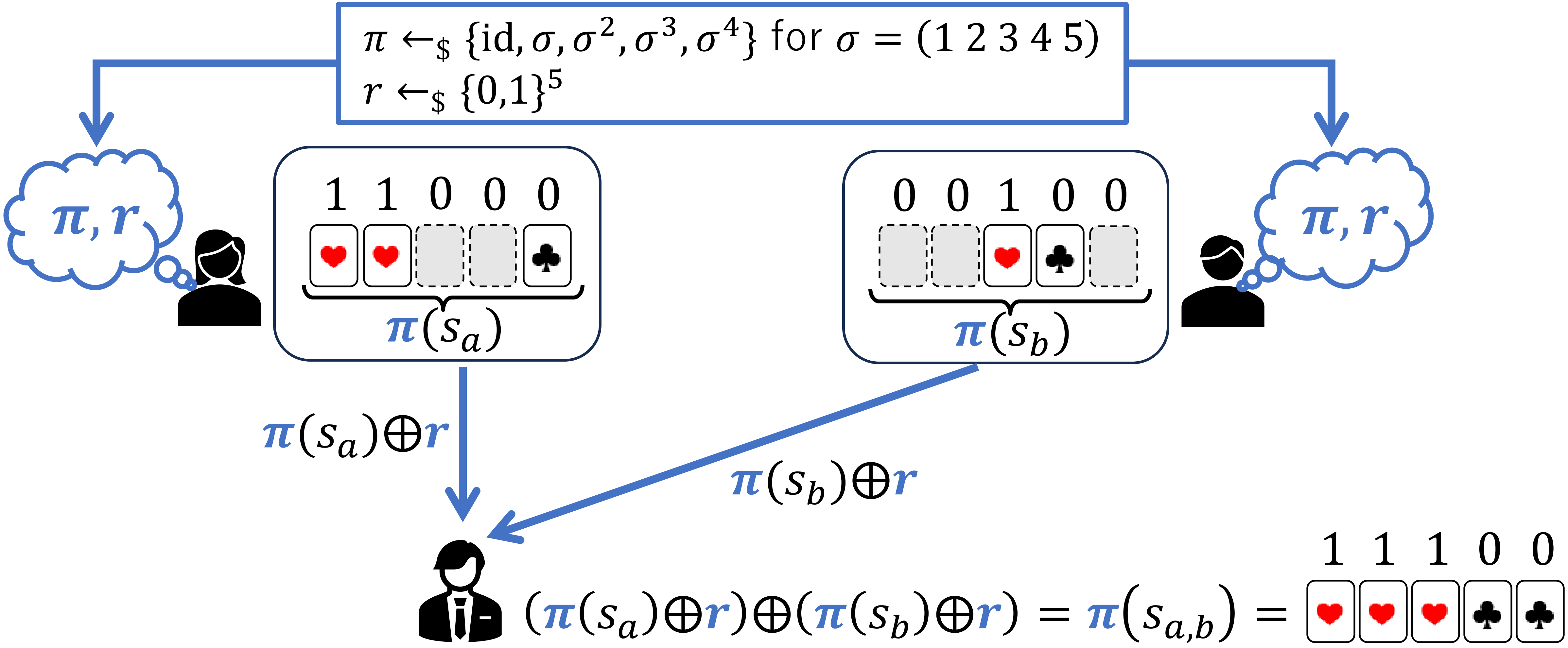
Conversion from Card to PSM

Our Idea for Constructing PSM Protocols

- Set a random permutation π of shuffle as a **common randomness**
- Alice and Bob send $\pi(s_a)$ and $\pi(s_b)$ as messages, whose sum is equal to the opened symbols of the five-card trick

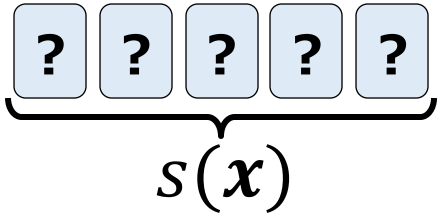


PSM Protocol from Five-Card Trick

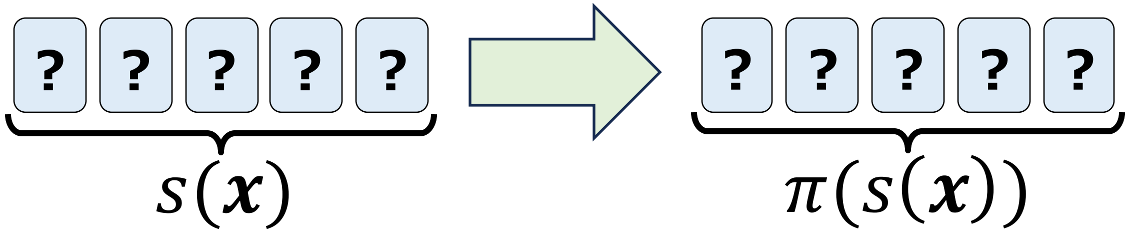


Single-shuffle Full-open (SF) Protocols

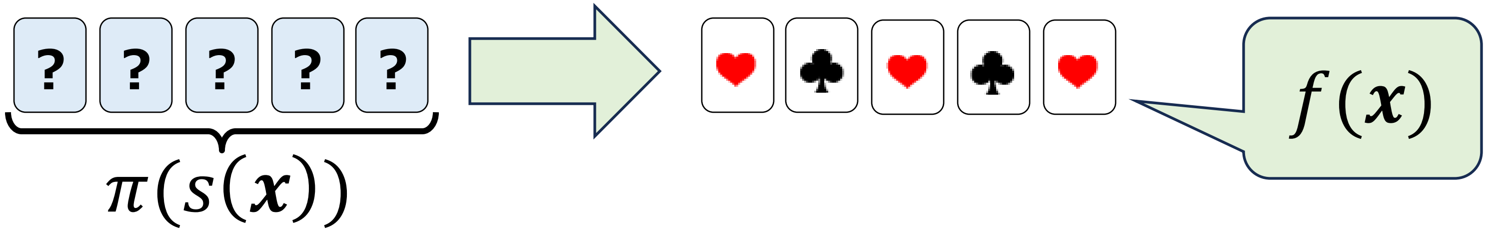
1. Place a card-sequence $s(\boldsymbol{x})$ with input $\boldsymbol{x} = (x_1, x_2, \dots, x_n)$



2. Apply a permutation π from $\Pi \subseteq S_k$ uniformly at random



3. All cards are opened, and the output value is determined



Main Result

Theorem

Given any SF protocol for $f(x_1, \ldots, x_n)$ with k cards,
then we have a PSM protocol for f with k-bit message per party

- Lower bounds on SF protocols is obtained from those on PSM
- The state-of-the-art PSM protocol for $f: \{0,1\}^k \times \{0,1\}^k \rightarrow \{0,1\}$ requires $O(2^{k/2})$-bit message
- Assume its optimality, any SF protocol requires $\Omega(2^{k/2})$ cards

Our Result for General Case

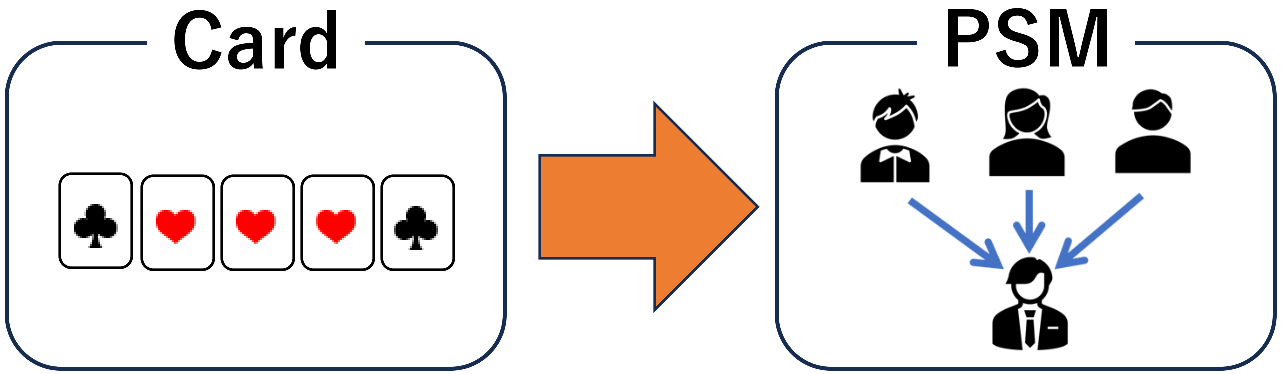
Theorem

Given any finite-runtime card-protocol for f **opening k cards**, then we have a PSM protocol for f with k-bit message per party

- k = (# of opened cards in all possible branches of the protocol)
- The finite-runtimeness is important to make k finite
- Assuming PSM-lower-bounds, we obtain card-lower-bounds

Conclusion

- A generic conversion from card-based to PSM protocols



- Future work
  - Can we obtain more efficient conversion?
  - Can we find other relations to conventional cryptography?