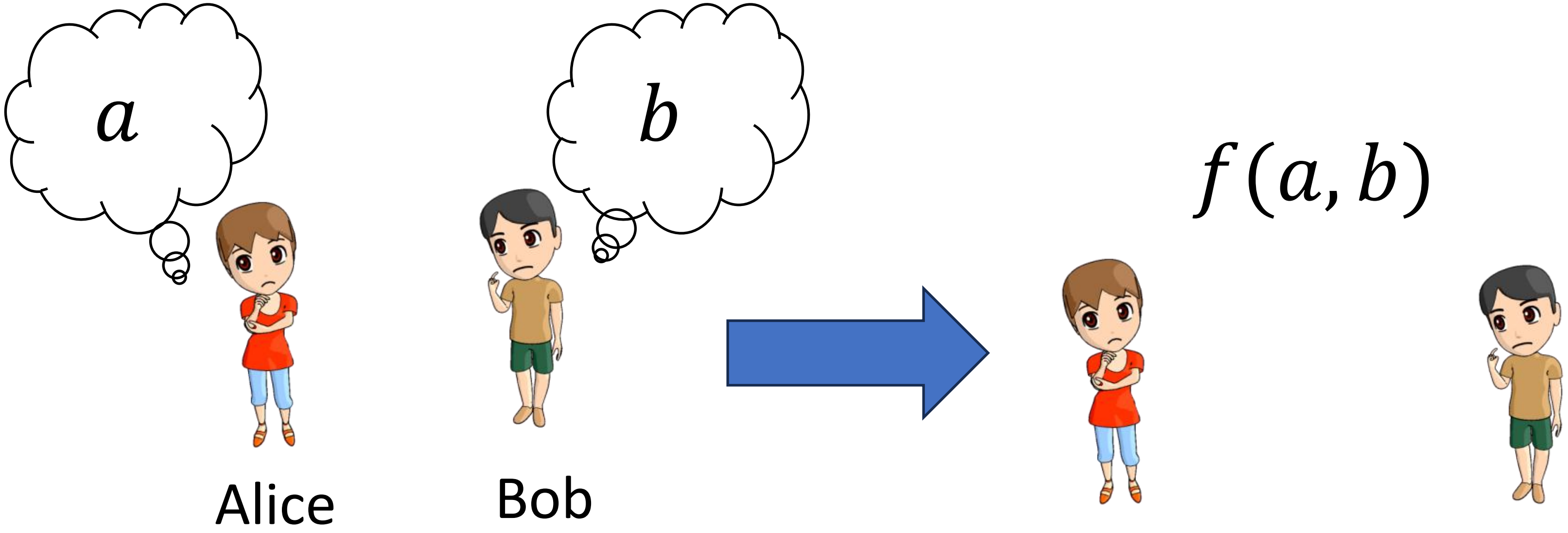
Gakmoro: An Application of Physical Secure Computation to Card Game

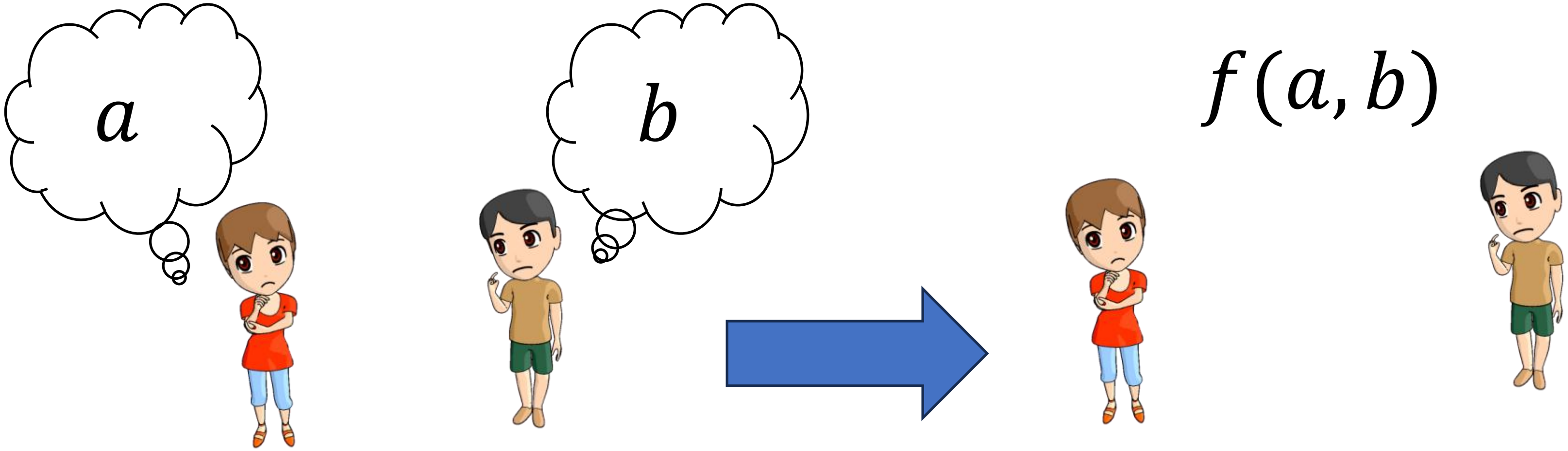
Takaaki Mizuki, Tomoki Kuzuma, Tomoya Hirano, Ririn Oshima, and Momofuku Yasuda

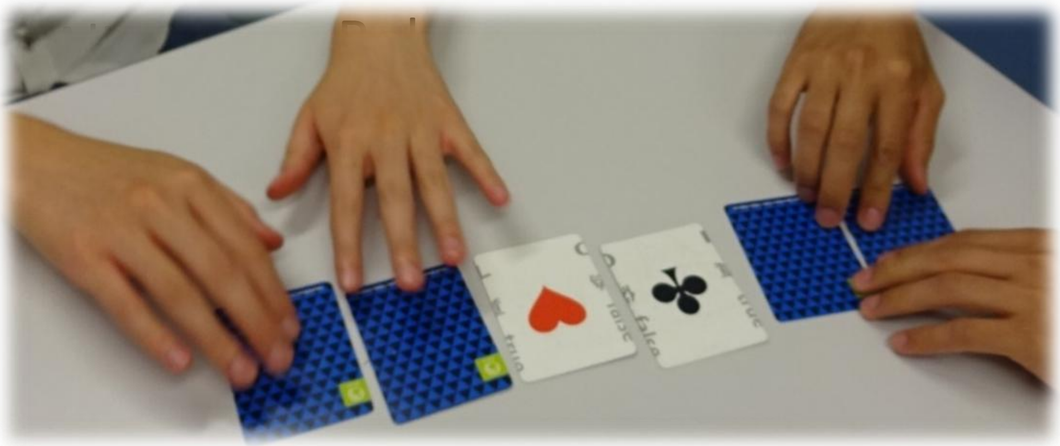
Tohoku University

Gakmoro: An Application of Physical *Secure Computation* to Card Game



Gakmoro: An Application of *Physical* Secure Computation to Card Game

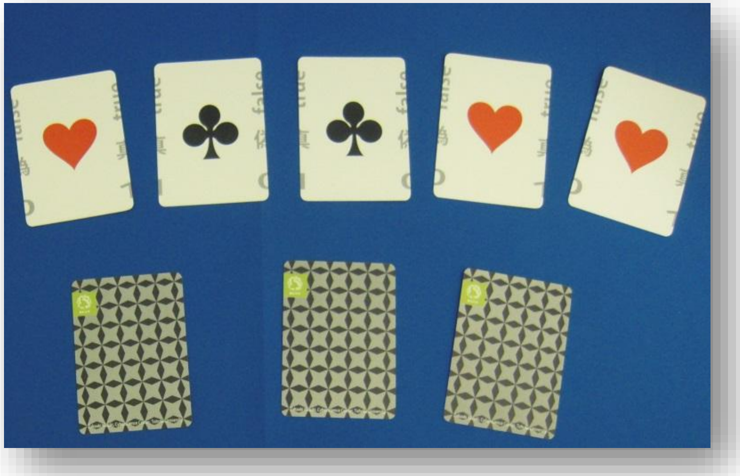




physical deck of cards

Gakmoro: An *Application* of *Physical* Secure Computation to *Card Game*

We create a new card game, named Gakmoro, by making use of card-based cryptography.



How was Gakmoro created?

First-year undergraduate class at Tohoku University, “Introduction to Academic Learning” (2023 Fall Semester)

Teacher: Takaaki Mizuki
Teaching Assistant: Tomoki Kuzuma
Students: Tomoya Hirano, Ririn Oshima, Momofuku Yasuda

Attempting to apply card-based cryptography to creating a card game

Gakmoro, is derived from the Japanese name of the class, “Gakumonron Enshu.”

Table of Contents

Table of Contents

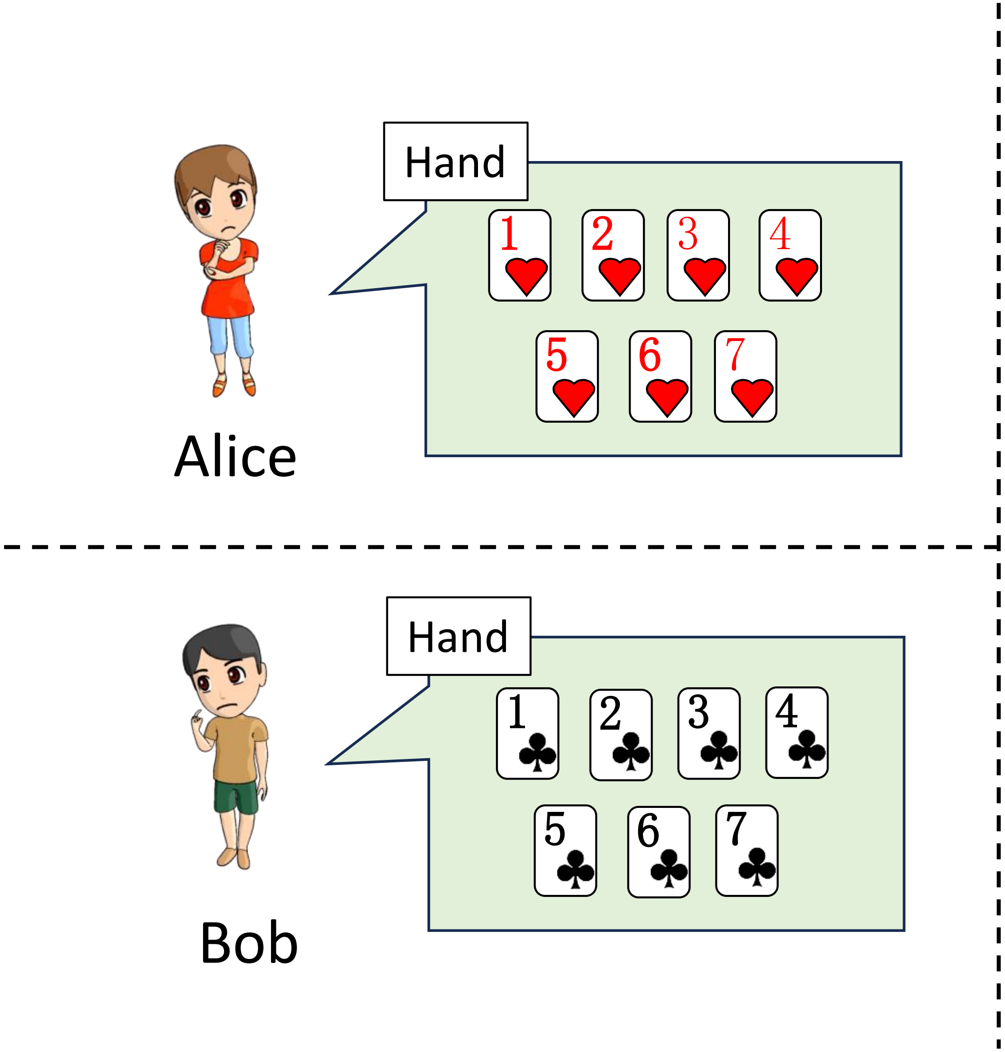
Gakmoro’s Rules

Alice

Dealer

Bob

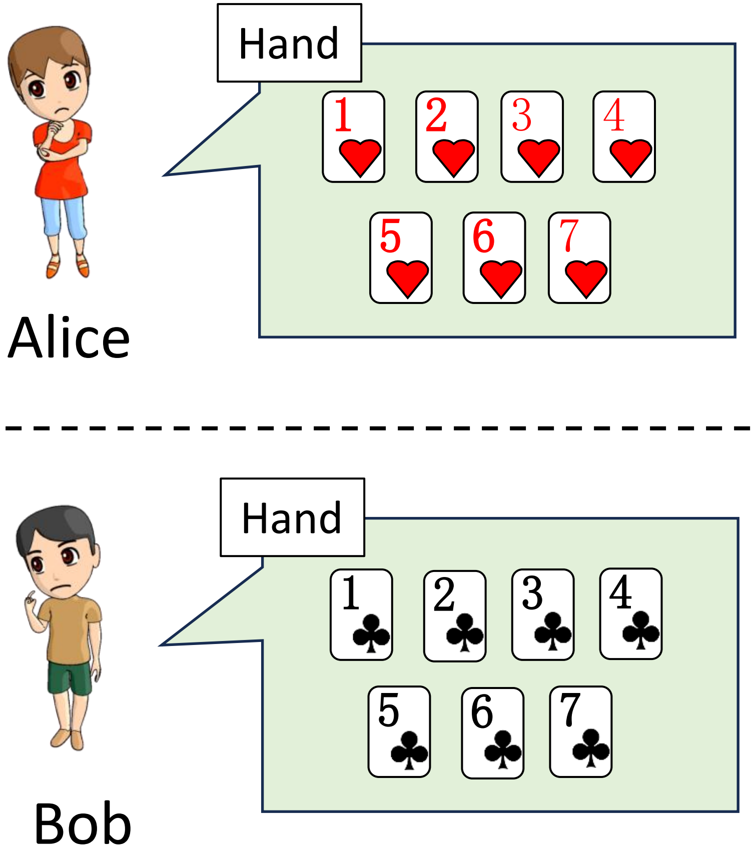
Gakmoro’s Rules



- Each has numbers 1 to 7

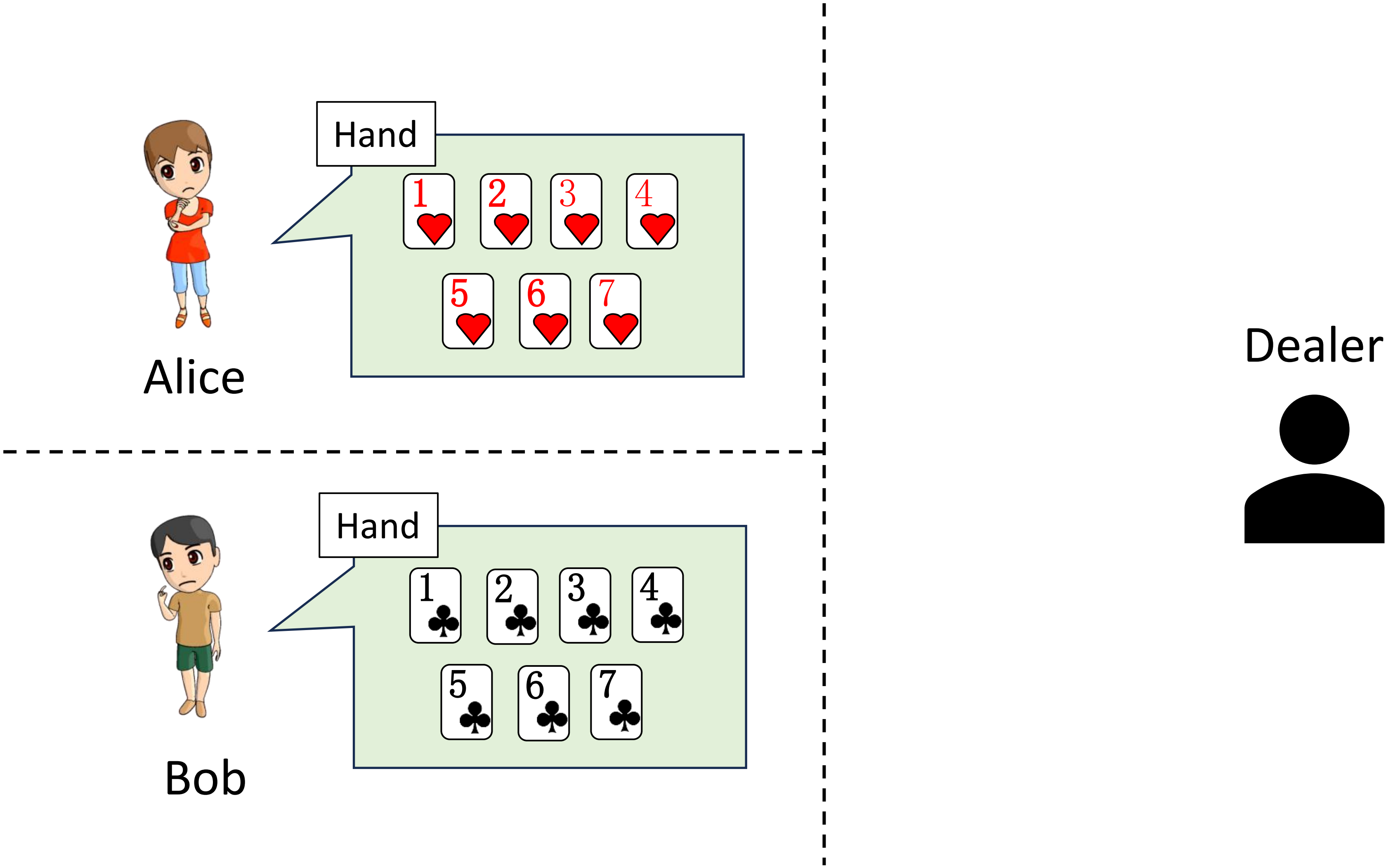
Dealer

Gakmoro’s Rules



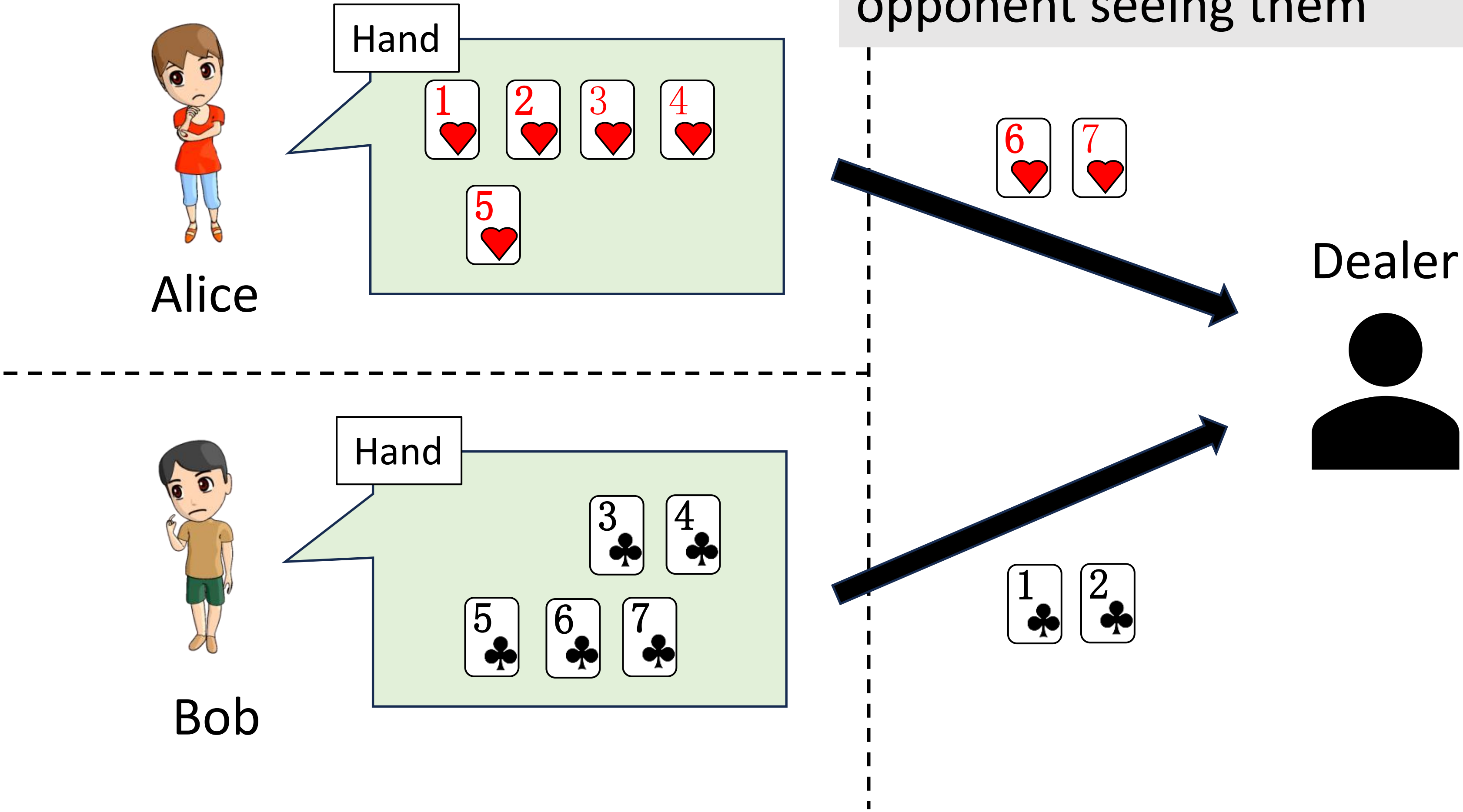
- Each has numbers 1 to 7
- A game consists of up to 3 rounds
- Each secretly chooses 1 to 3 cards to compete based on their total value

Example



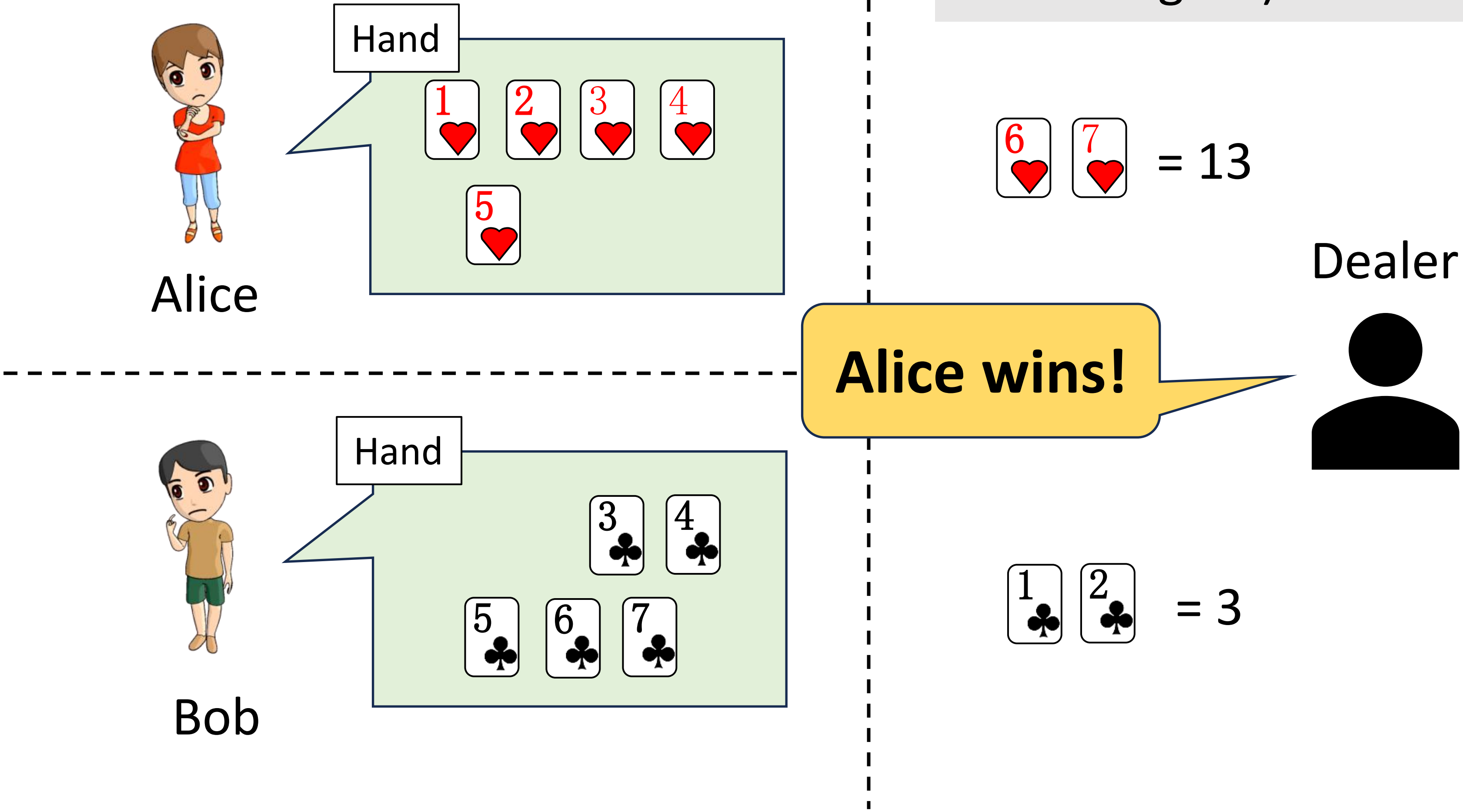
Example: Round 1

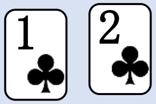
Each submits 1 to 3 cards secretly without the opponent seeing them



Example: Round 1

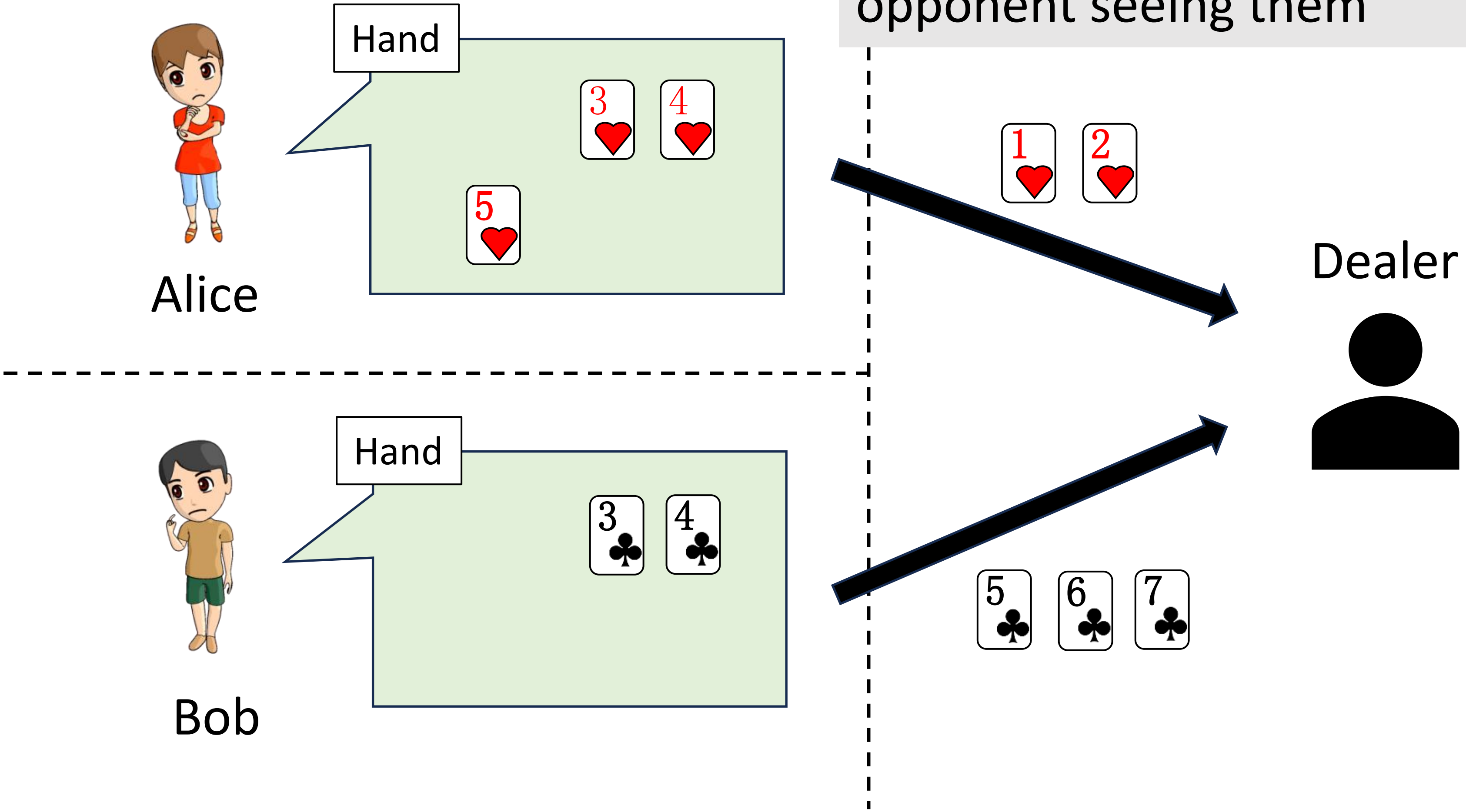
The dealer calculates the sum, and announces only the winner's name (whose total is higher)



	 Alice	 Bob
Round 1		
Round 2		
Round 3		

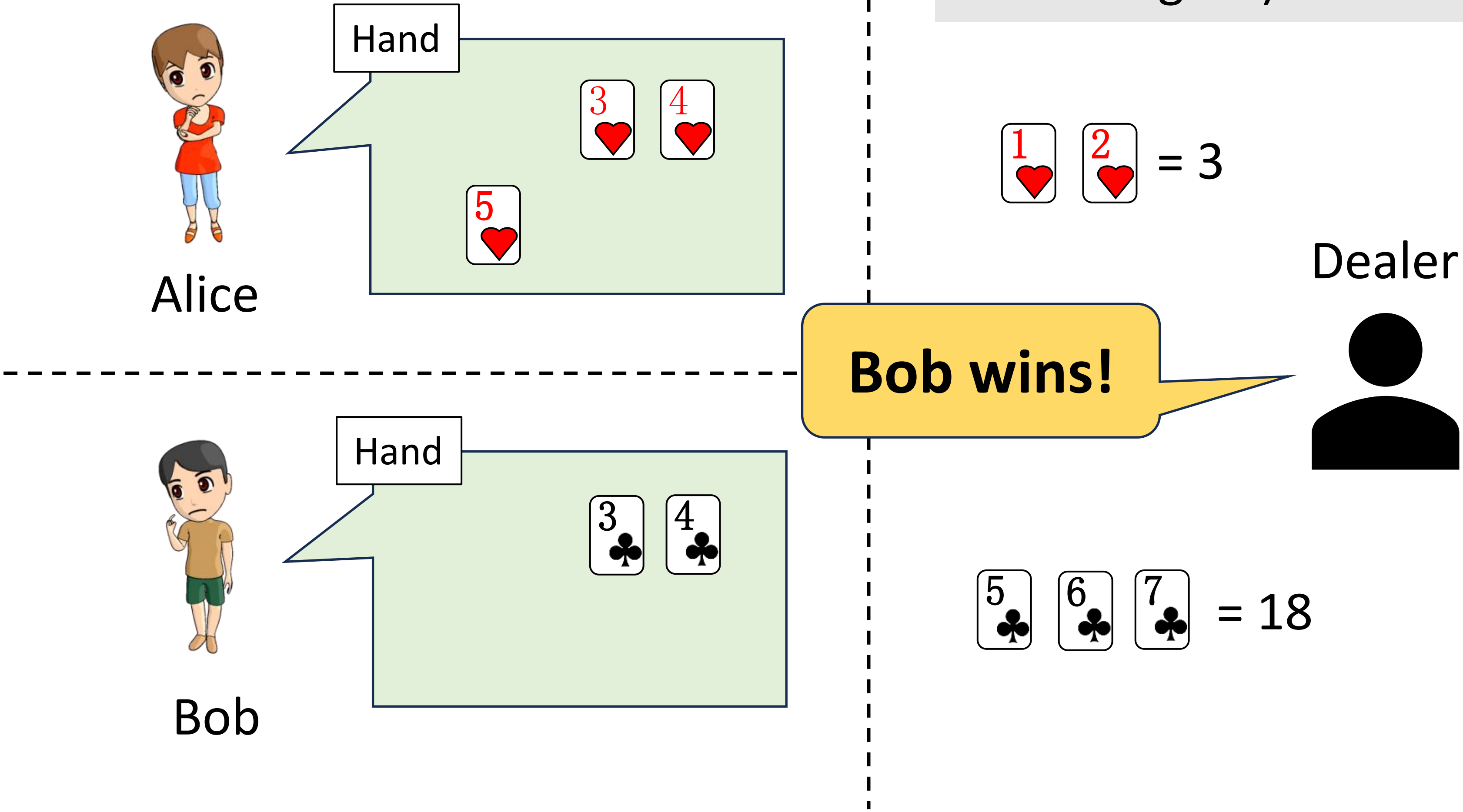
Example: Round 2

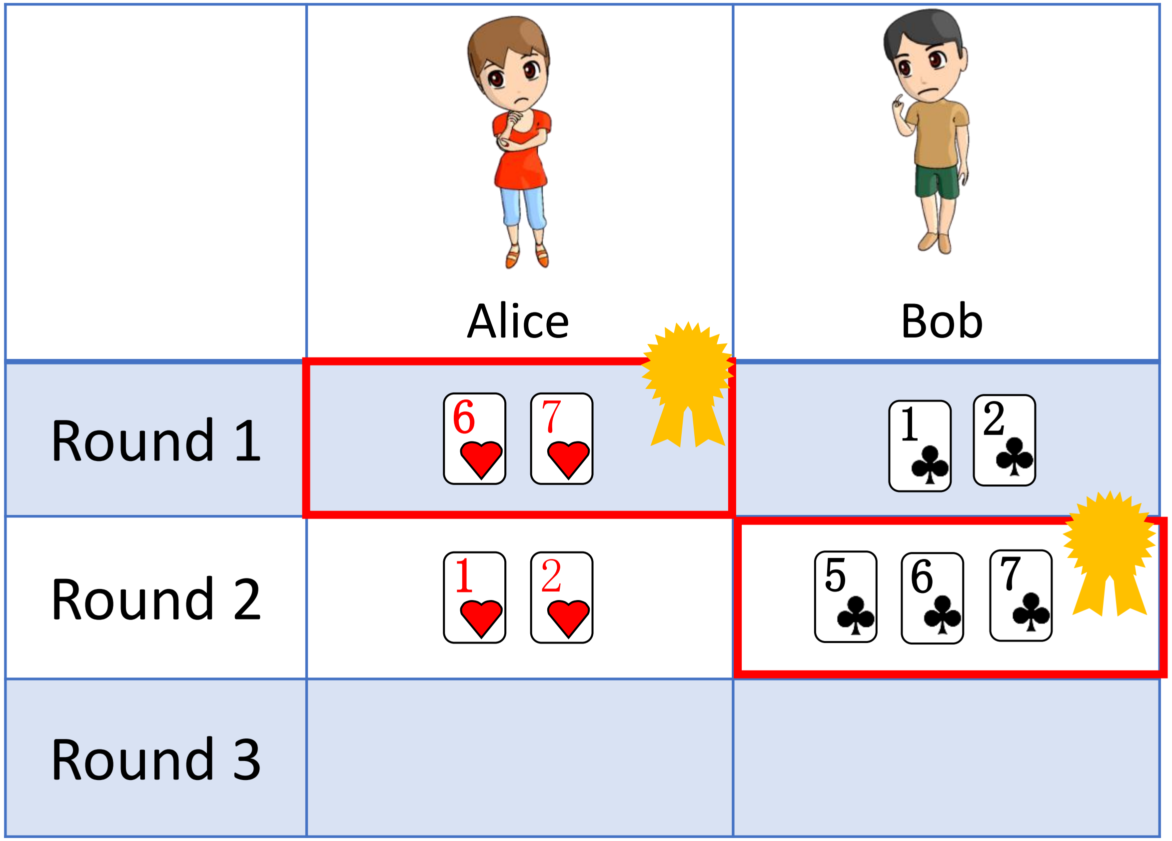
Each submits 1 to 3 cards secretly without the opponent seeing them



Example: Round 2

The dealer calculates the sum, and announces only the winner's name (whose total is higher)

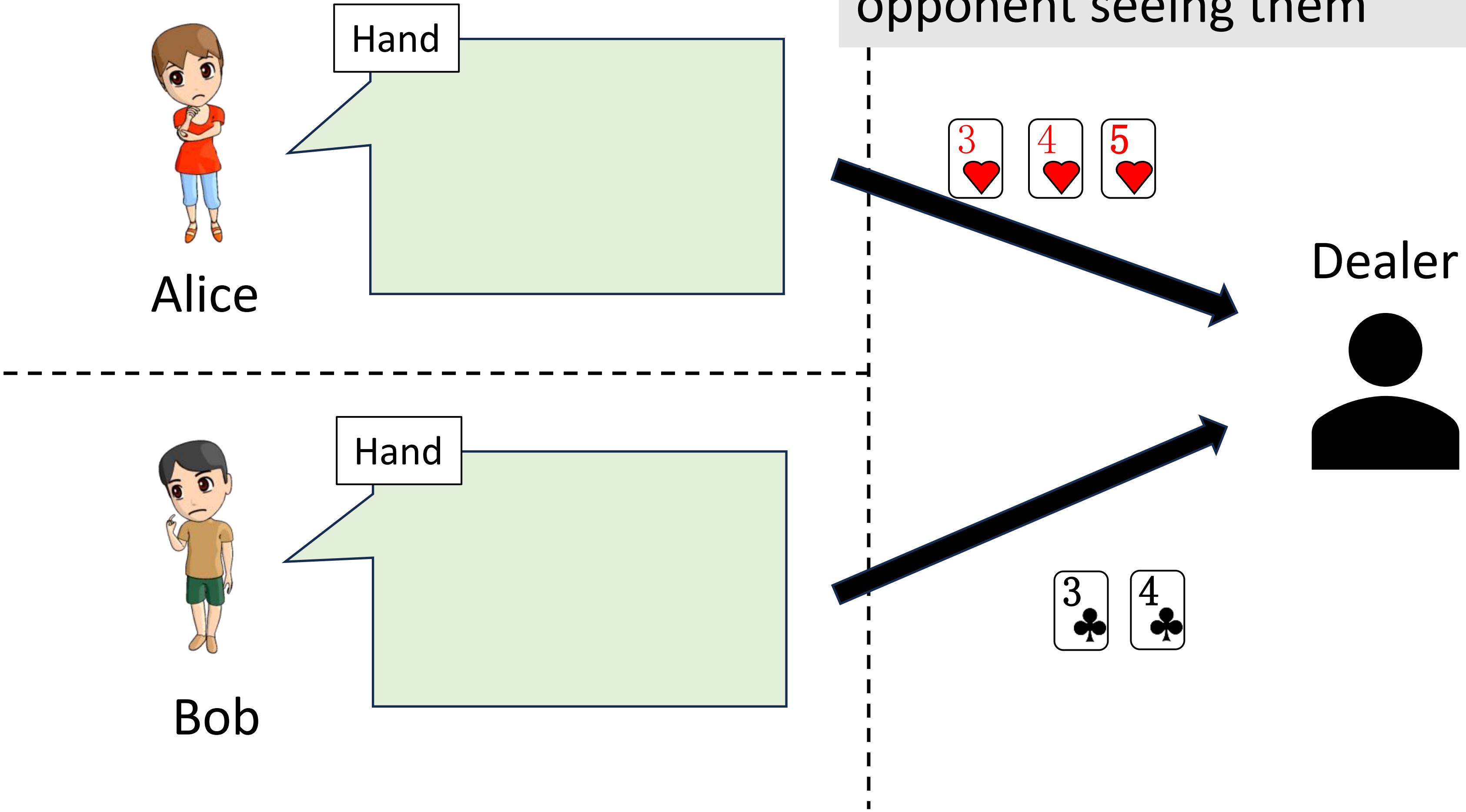




	Alice	Bob
Round 1	6♥ 7♥	1♣ 2♣
Round 2	1♥ 2♥	5♣ 6♣ 7♣
Round 3		

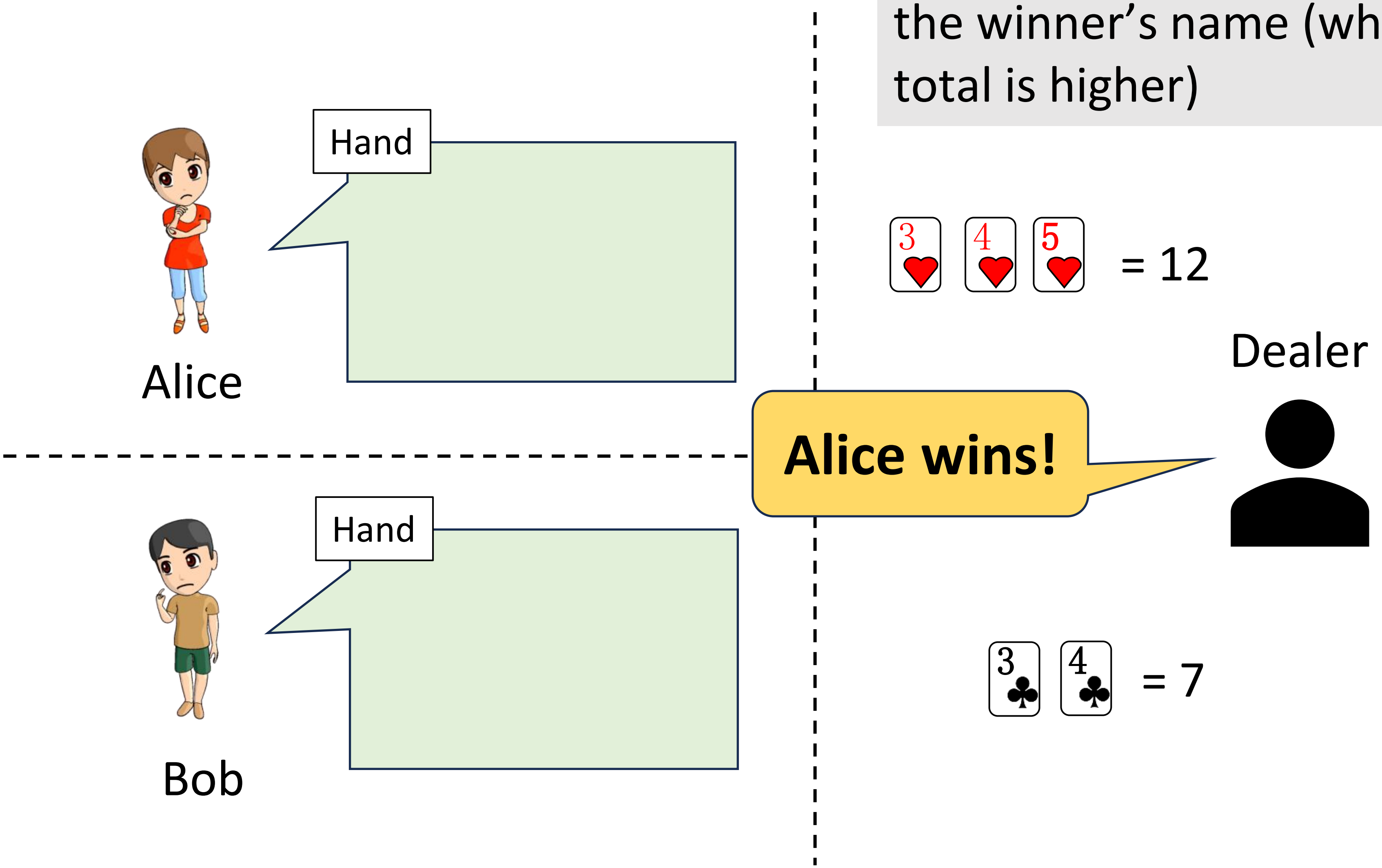
Example: Round 3

Each submits 1 to 3 cards secretly without the opponent seeing them



Example: Round 3

The dealer calculates the sum, and announces only the winner’s name (whose total is higher)



	 Alice	 Bob
Round 1	6♥ 7♥ 🏅	1♣ 2♣
Round 2	1♥ 2♥	5♣ 6♣ 7♣ 🏅
Round 3	3♥ 4♥ 5♥ 🏅	3♣ 4♣

	 Alice	 Bob
Round 1	6♥ 7♥ 🏅	1♣ 2♣
Round 2	1♥ 2♥	5♣ 6♣ 7♣ 🏅
Round 3	3♥ 4♥ 5♥ 🏅	3♣ 4♣

With two wins, Alice is the winner of the game.

Playing Without a Dealer?

The dealer's role in Gakmoro is crucial for maintaining secrecy and ensuring fair play.

The main functions are:

- **Ensuring that each player submits between one and three cards.**
- **Correctly adding the values of the submitted cards.**
- **Announcing only the winner, not the sums or the number of cards played.**

Playing Without a Dealer?

Without a dealer, the game loses its core element of hidden information, which is central to strategic play.

Playing Without a Dealer?

Without a dealer, the game loses its core element of hidden information, which is central to strategic play.

What if there are only two players, making it dificult to find a dealer?

Are there any solutions for playing Gakmoro with just two people?

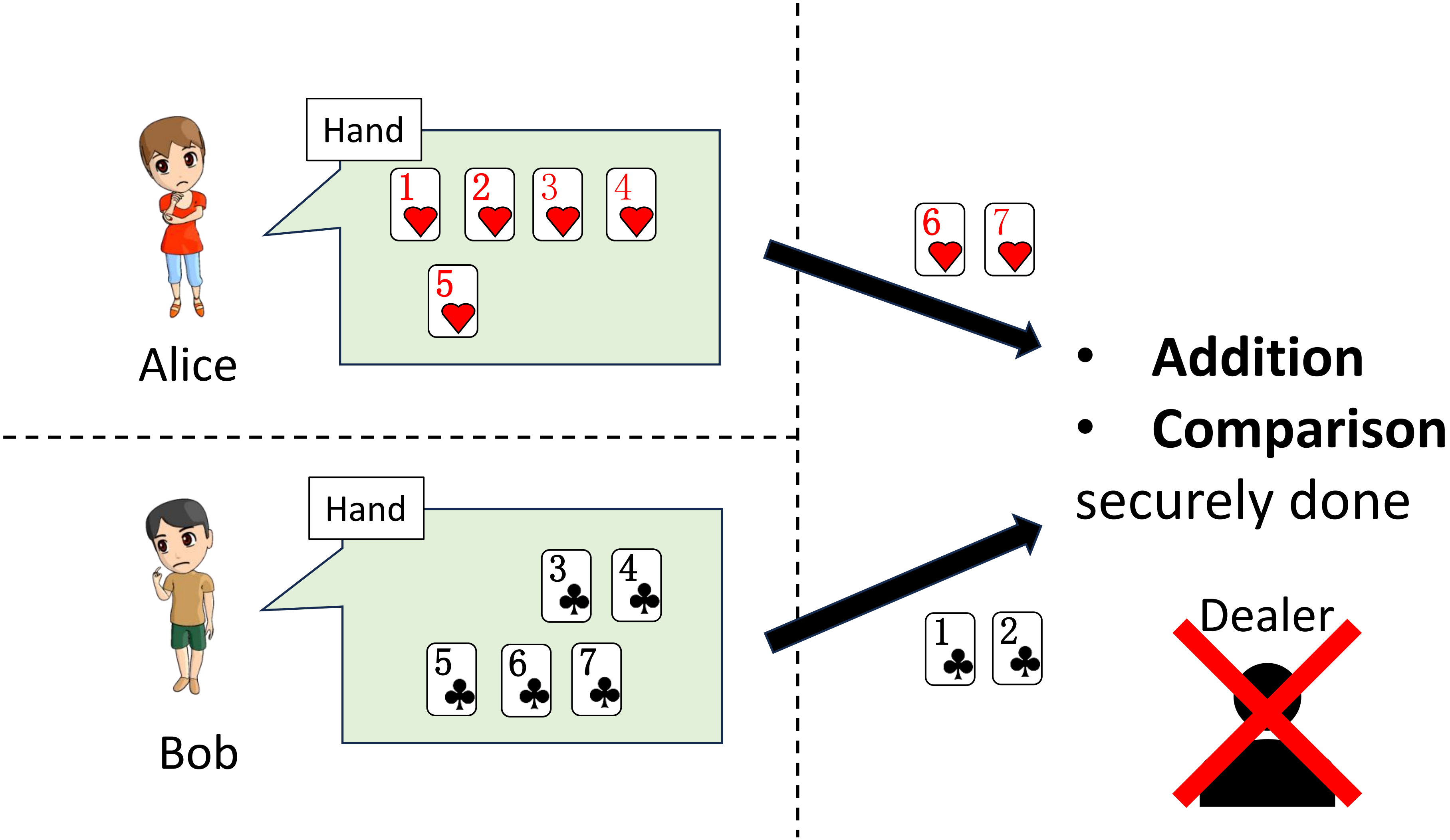
Our contribution

We eliminate the need for a human dealer in Gakmoro by combining existing techniques from **card-based cryptography** and designing a new protocol.

Human dealer

Card-based cryptography

To this end, …



- **Addition**
- **Comparison**

securely done

We use

- **Card-based secure *addition* protocol**
  - ✓ existing one by Ruangwises and Itoh [RI21]
  - ✓ introduce in Section 2

- **Card-based secure *comparison* protocol**
  - ✓ construct in Section 3

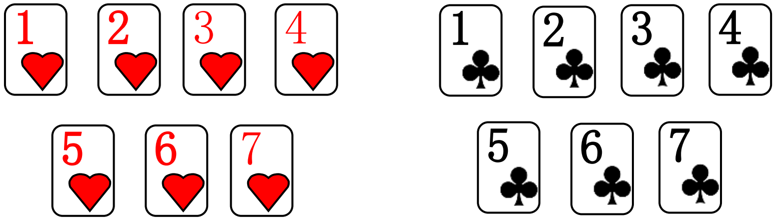
Combining them, we have

- **Gakmoro with secure computation** (Section 4)

[RI21] Suthee Ruangwises and Toshiya Itoh. Securely computing the n-variable equality function with 2n cards. Theor. Comput. Sci.,887:99–110, 2021.

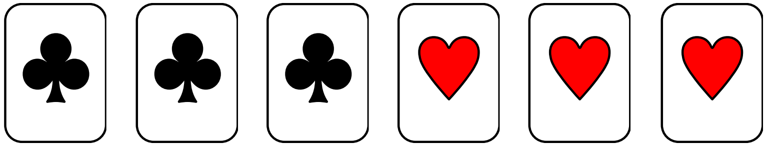
Table of Contents

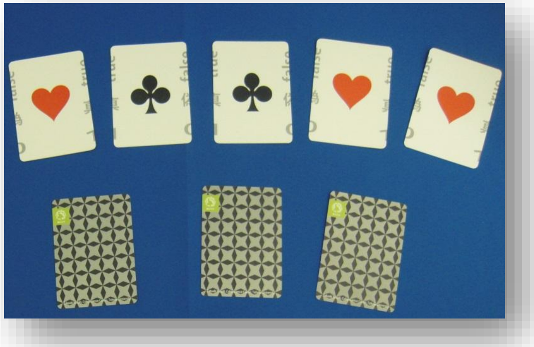
Standard deck of playing cards:



→ not so easy to construct a simple protocol

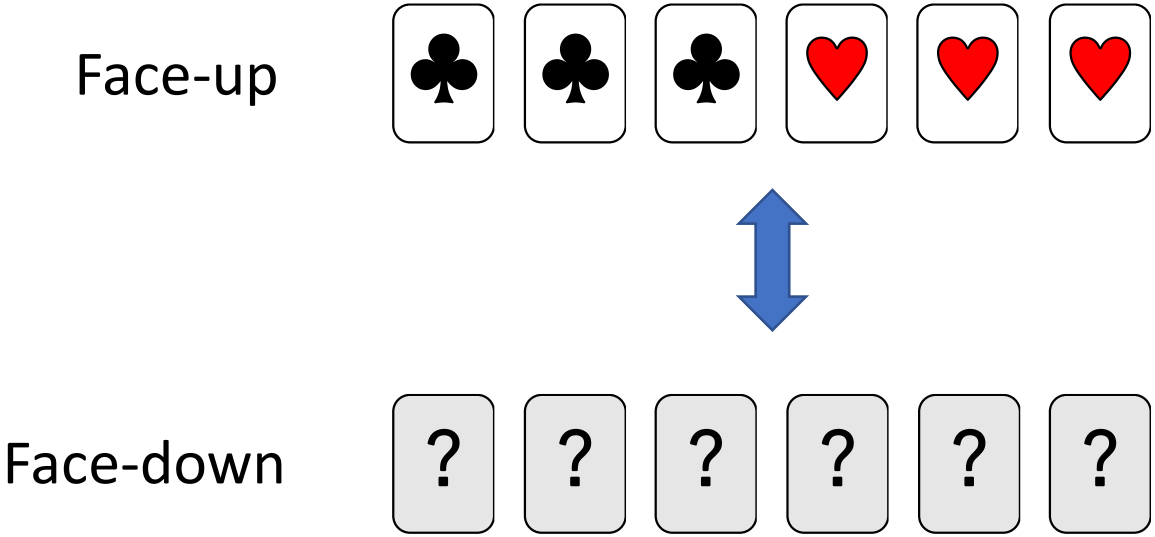
Two-color deck of cards:





→ We use this type of cards

Two-color deck of cards

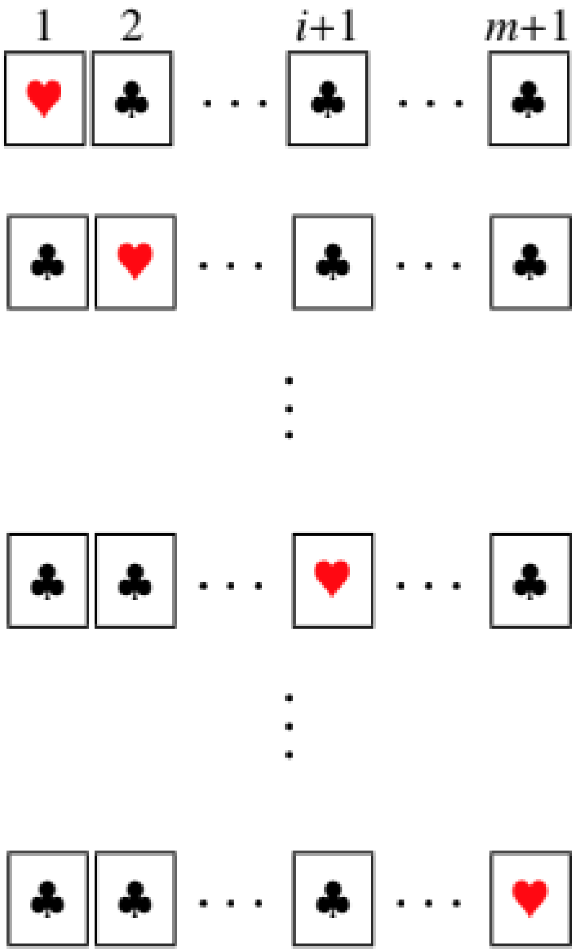


Face-up

Face-down

We need to deal with integers from 1 to 7 as well as their sums

Encoding of integers (between $\mathbf{0}$ and $\boldsymbol{m}$)



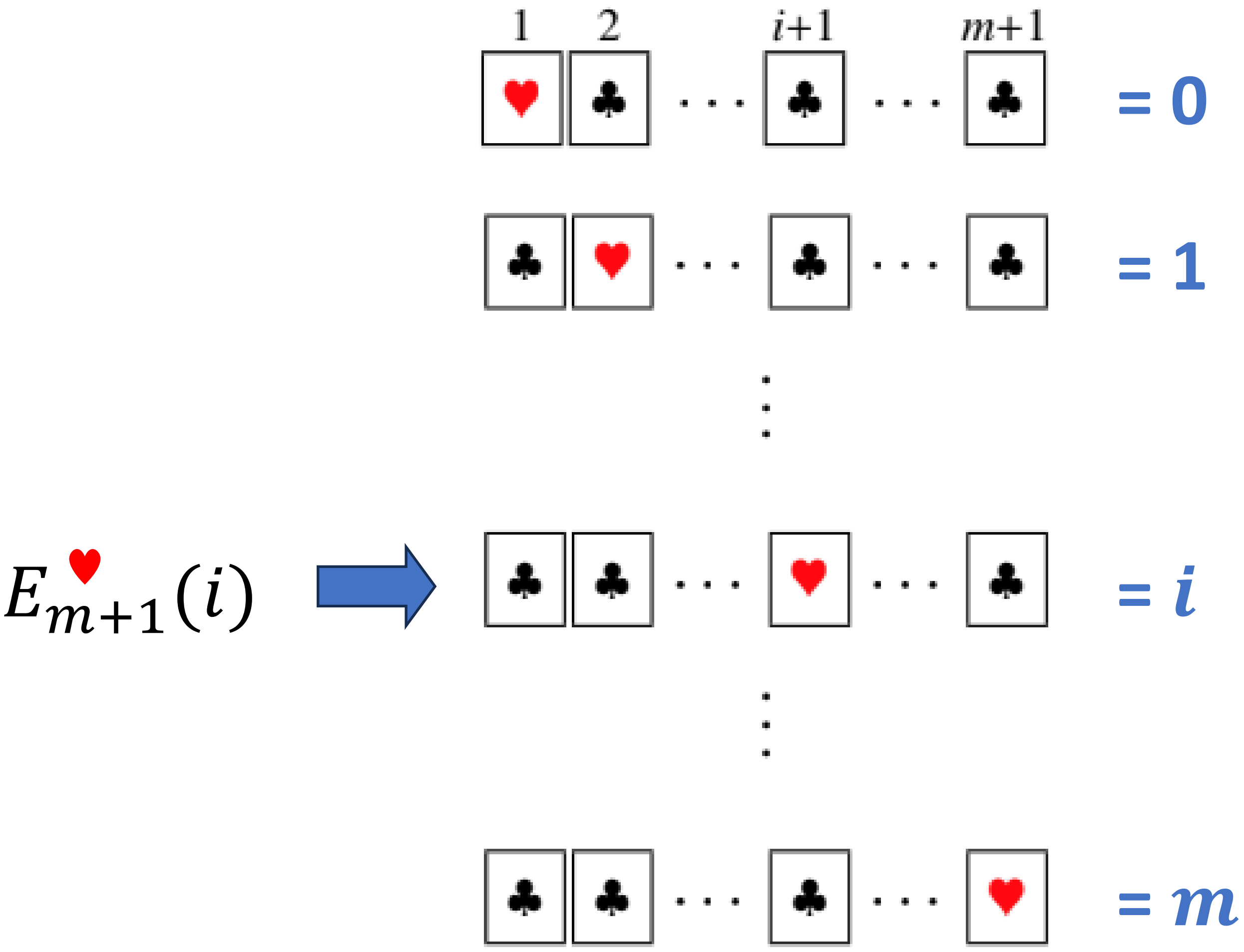
$= 0$

$= 1$

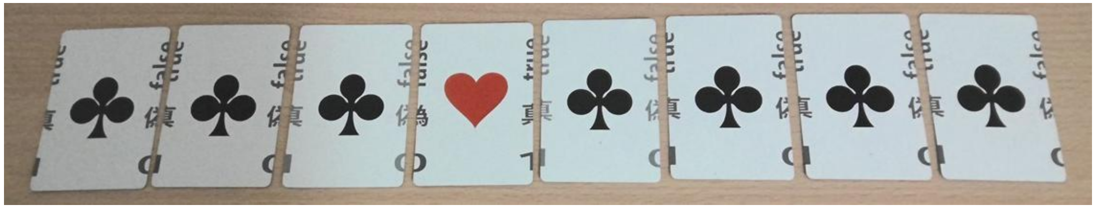
$= \boldsymbol{i}$

$= \boldsymbol{m}$

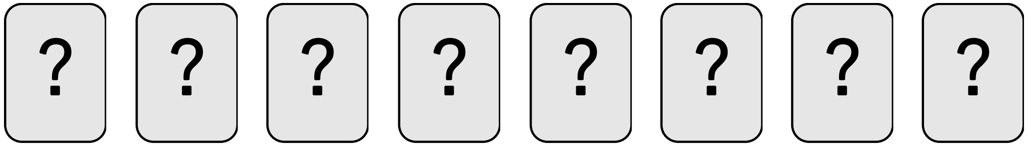
Encoding of integers (between $\mathbf{0}$ and $\boldsymbol{m}$)



Example



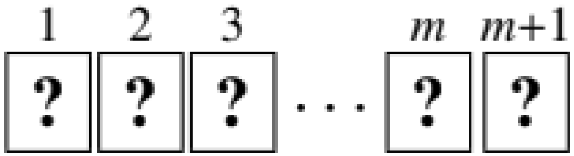
$E_8^{\heartsuit}(3)$:



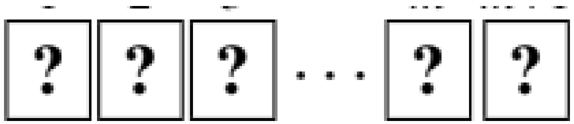
Addition protocol [RI21]

Input

$E^{\heartsuit}_{m+1}(a)$

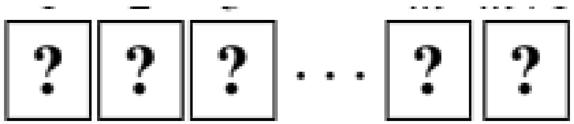


$E^{\heartsuit}_{m+1}(b)$



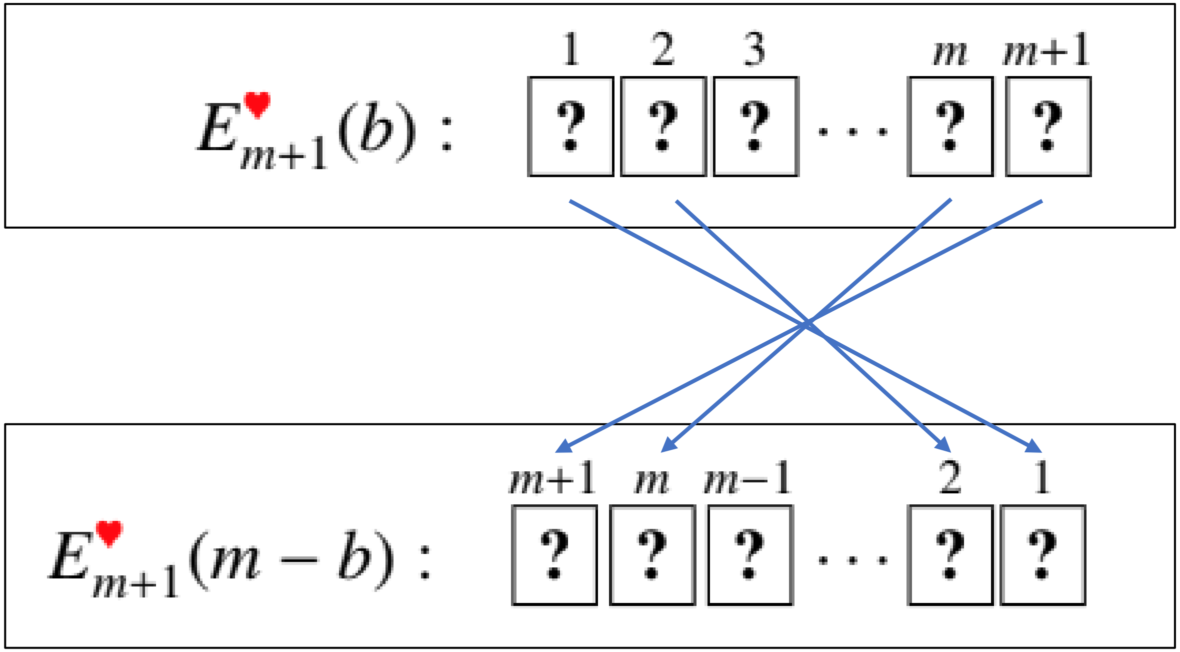
Output

$E^{\heartsuit}_{m+1}(a + b \bmod m + 1)$



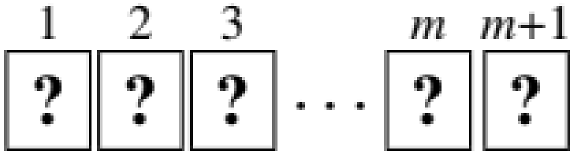
[RI21] Suthee Ruangwises and Toshiya Itoh. Securely computing the n-variable equality function with 2n cards. Theor. Comput. Sci.,887:99–110, 2021.

(1) For $E^{\heartsuit}_{m+1}(b)$, the left and right sides are reversed:

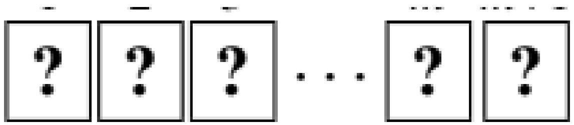


Now we have:

$E^{\heartsuit}_{m+1}(a)$



$E^{\heartsuit}_{m+1}(m-b)$



Idea of adding b to a

$$E(a)\text{: } \overbrace{\clubsuit\clubsuit\clubsuit\clubsuit}^{a\text{ cards}}\heartsuit\clubsuit\clubsuit\clubsuit\clubsuit$$

$$E(m-b)\text{: } \clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\heartsuit\underbrace{\clubsuit\clubsuit}_{b\text{ cards}}$$

Idea

$$E(a)\text{: } \overbrace{\clubsuit\clubsuit\clubsuit\clubsuit}^{a\text{ cards}}\heartsuit\clubsuit\clubsuit\clubsuit\clubsuit$$

$$E(m-b)\text{: } \clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\heartsuit\underbrace{\clubsuit\clubsuit}_{b\text{ cards}}$$

Shift the positions of the two sequences by b to the right:

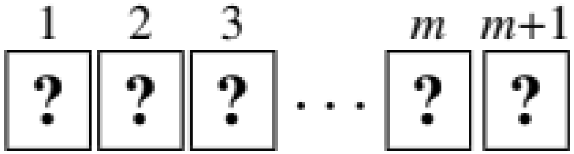
$$E(a+b)\text{: } \clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\heartsuit\clubsuit\clubsuit$$

$$E(m)\text{: } \clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\clubsuit\heartsuit$$

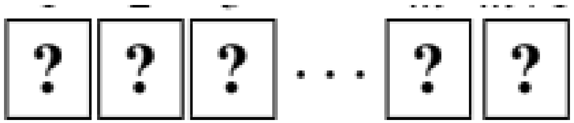
→ It suffices to make ♥ of the second sequence be at the right edge

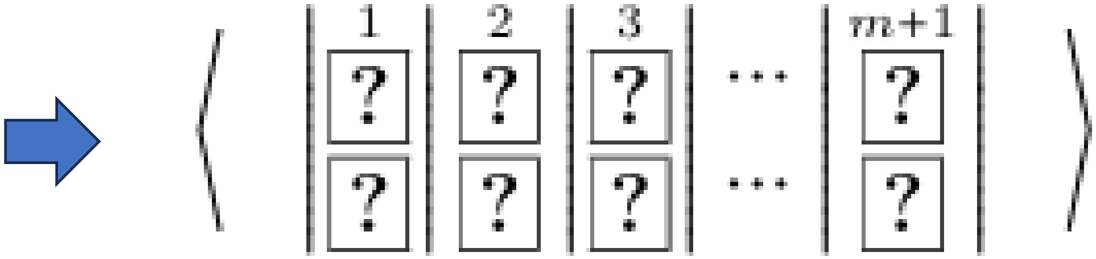
(2) Apply a pile-shifting shuffle:

$E^{\heartsuit}_{m+1}(a)$



$E^{\heartsuit}_{m+1}(m-b)$



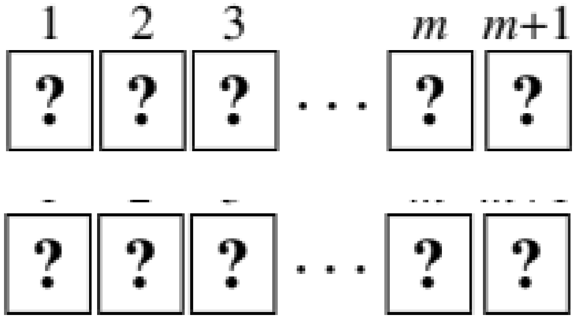


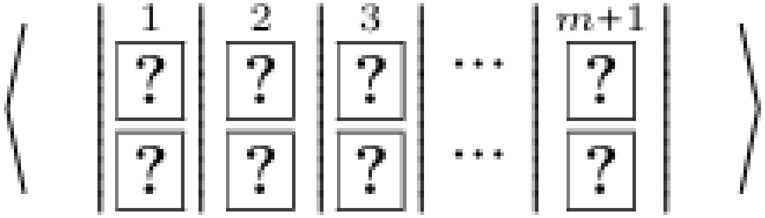
2-card piles are randomly shifted

(2) Apply a pile-shifting shuffle:

$E^{\heartsuit}_{m+1}(a)$

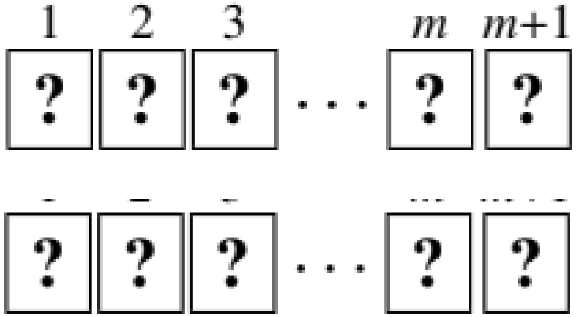
$E^{\heartsuit}_{m+1}(m-b)$





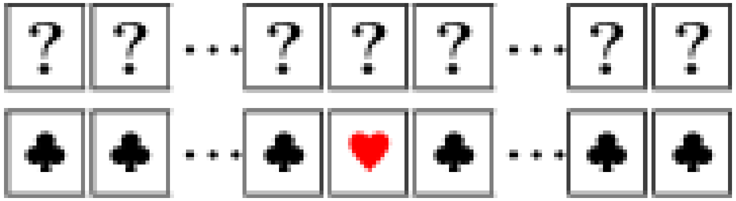
$E^{\heartsuit}_{m+1}(a + r \bmod m+1)$

$E^{\heartsuit}_{m+1}(m - b + r \bmod m+1)$



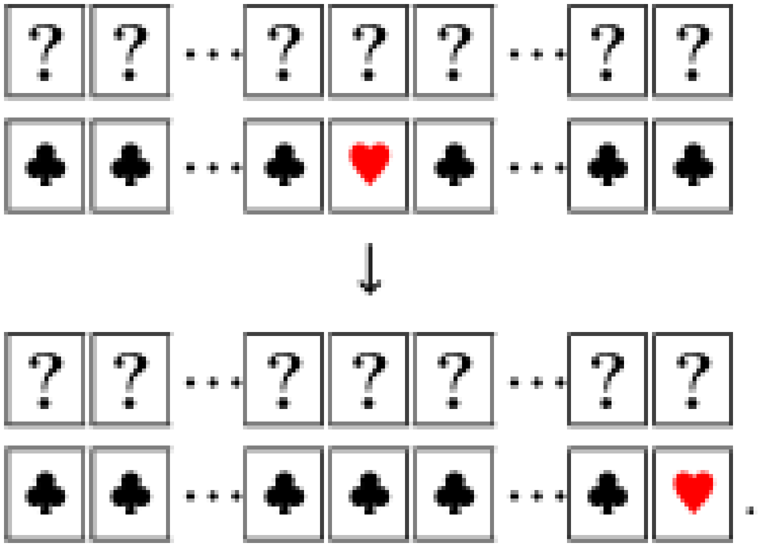
r is random

(3) Turn over all the cards in the bottom row:



$m - b + r$ is revealed
but b is kept secret

Shift the top and bottom cards until ♥ is at the right edge:

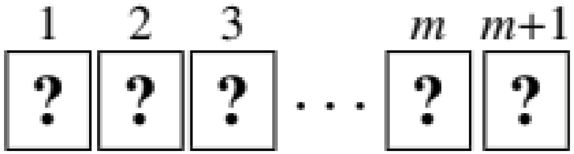


$E^{\heartsuit}_{m+1}(a + b \bmod m + 1)$

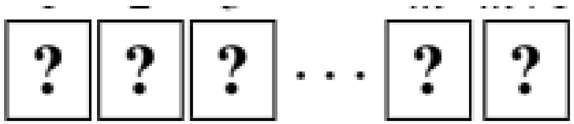
Addition protocol [RI21]

Input

$E^{\heartsuit}_{m+1}(a)$

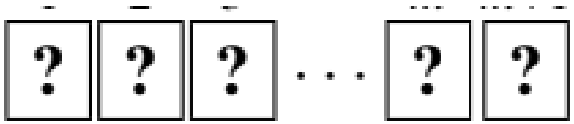


$E^{\heartsuit}_{m+1}(b)$



Output

$E^{\heartsuit}_{m+1}(a + b \bmod m + 1)$



Addition can be done in this way

Gakmoro needs one more, **Comparison**

Table of Contents

Comparison in Gakmoro:

Given a and b, we want to determine whether

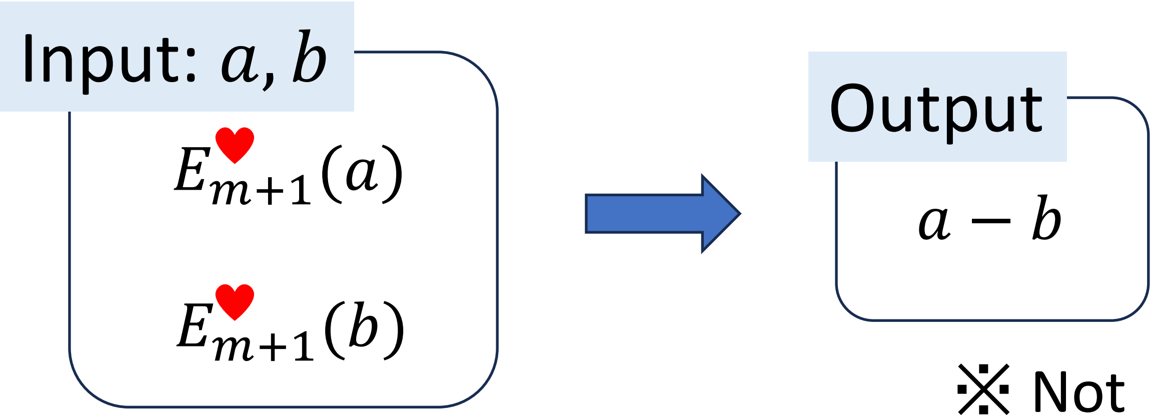
$$\boldsymbol{a > b}$$
$$\boldsymbol{a < b}$$
$$\boldsymbol{a = b}$$

To this end, we will design a **subtraction protocol** producing

$$\boldsymbol{a - b}$$

The sign (positive, negative, or zero) of this determines whether $a > b$, $a < b$, or $a = b$

Subtraction protocol



Input: a, b

$E^{\heartsuit}_{m+1}(a)$

$E^{\heartsuit}_{m+1}(b)$

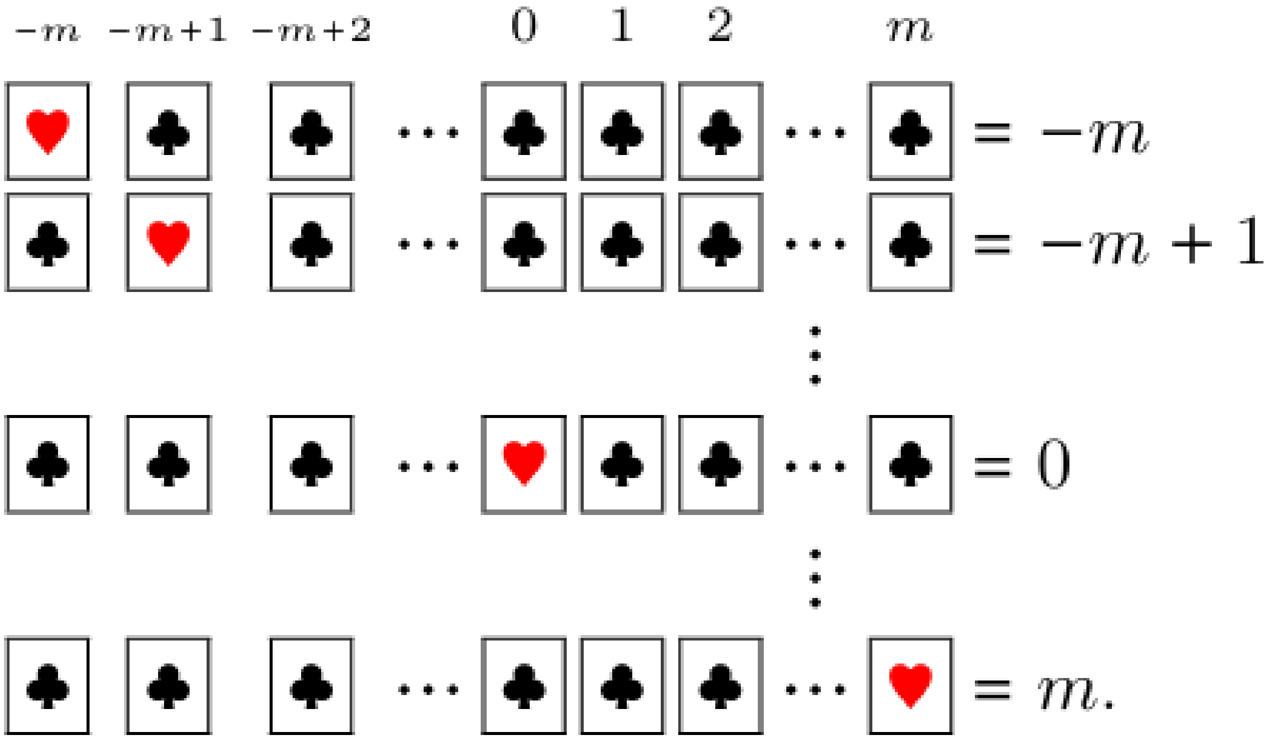
Output

$a - b$

※ Not $a - b \bmod m + 1$

Since we need to deal with negative integers, we extend the encoding a little

Encoding of integers between $-m$ and m



We write $E^{\heartsuit}_{[-m,m]}(i)$

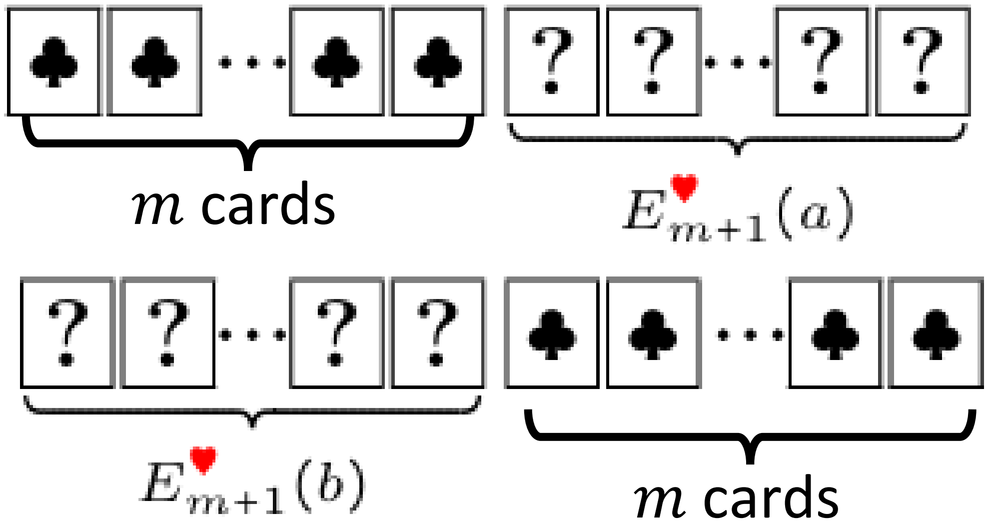
Subtraction protocol

Input: a, b

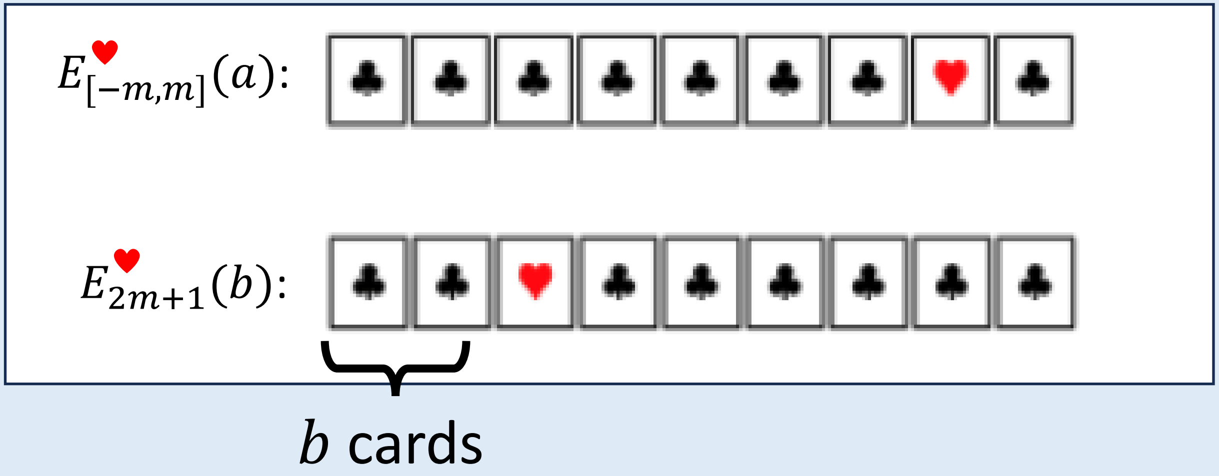
$E^{\heartsuit}_{m+1}(a)$

$E^{\heartsuit}_{m+1}(b)$

(1) Place ♣-cards as follows:



Idea



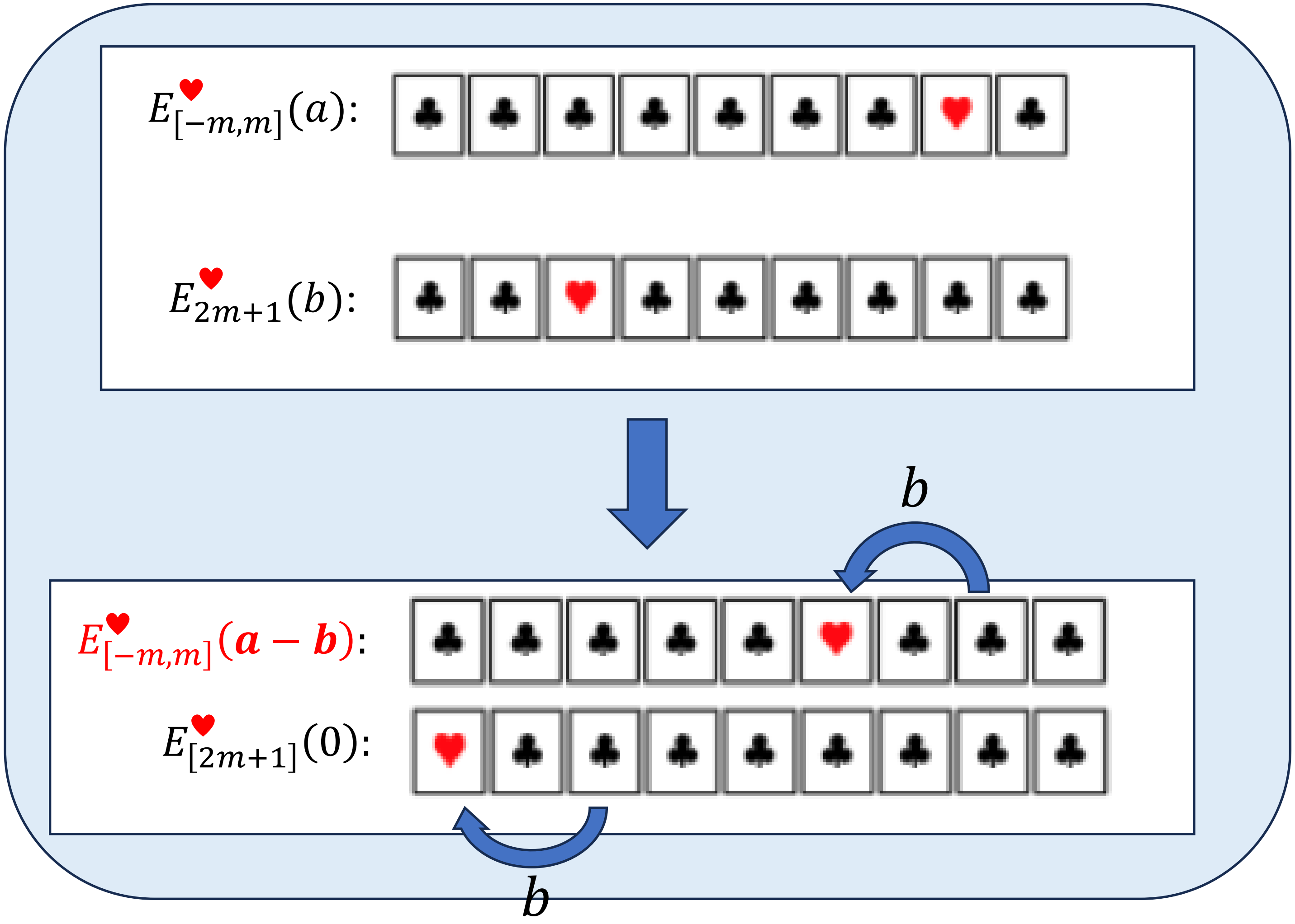
$E^{\heartsuit}_{[-m,m]}(a)$: ♣ ♣ ♣ ♣ ♣ ♣ ♣ ♥ ♣

$E^{\heartsuit}_{2m+1}(b)$: ♣ ♣ ♥ ♣ ♣ ♣ ♣ ♣ ♣

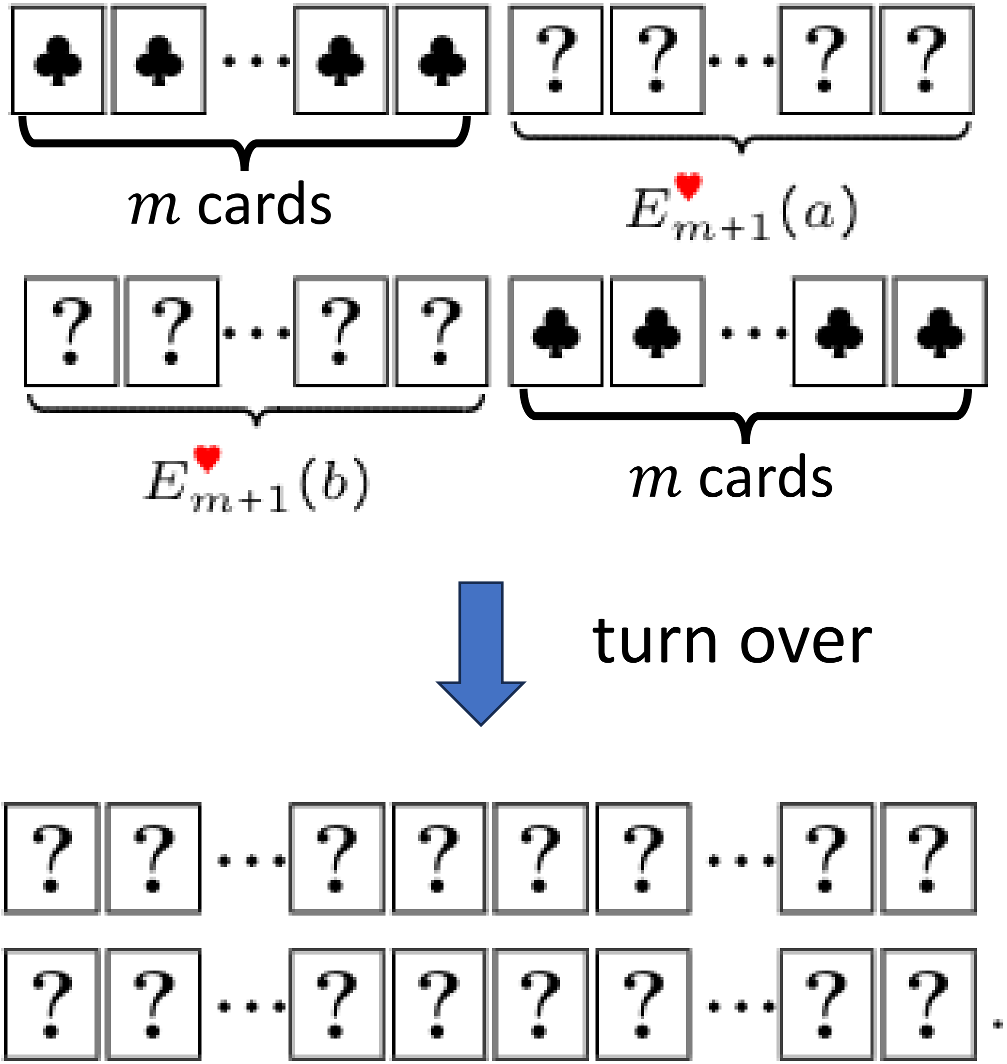
b cards

Idea

Making ♥ of the second sequence be at the left edge yields $\boldsymbol{a-b}$:

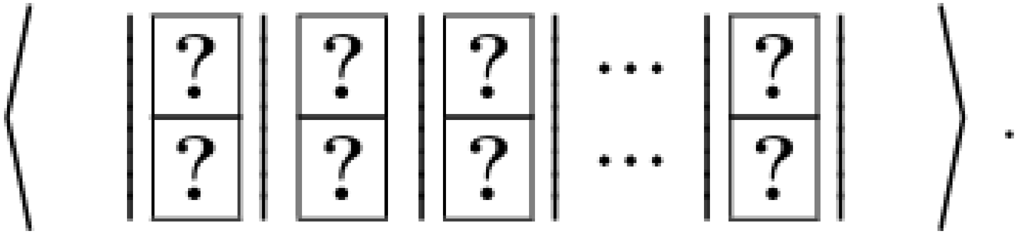


(1) Place ♣-cards as follows:

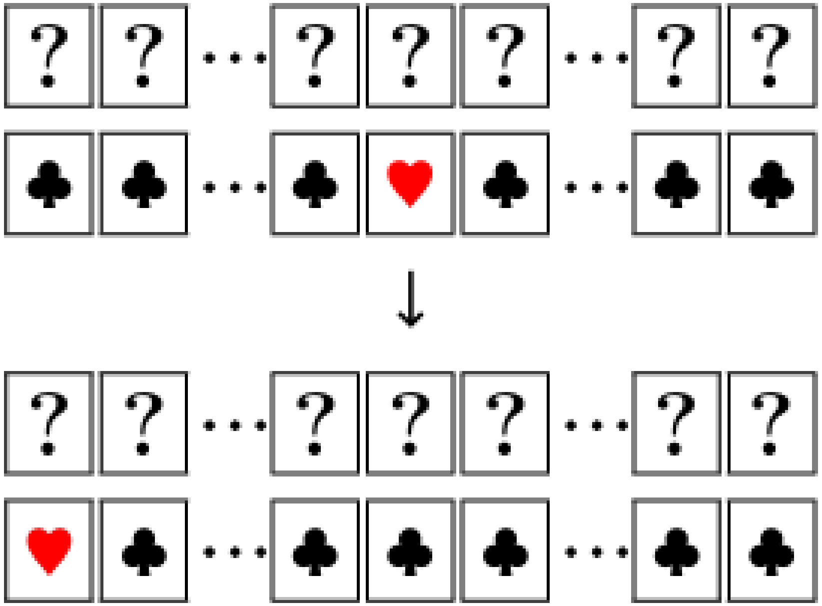


turn over

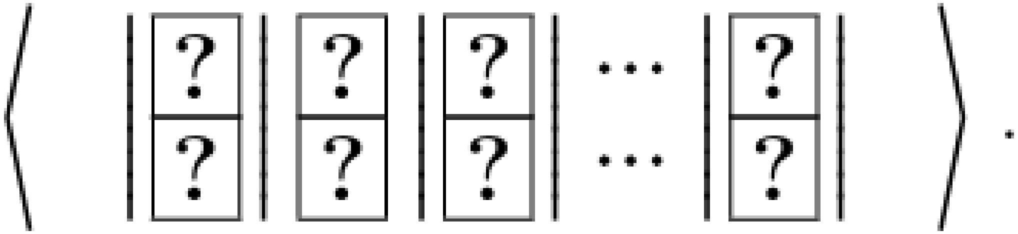
(2) Apply a pile-shifting shuffle:



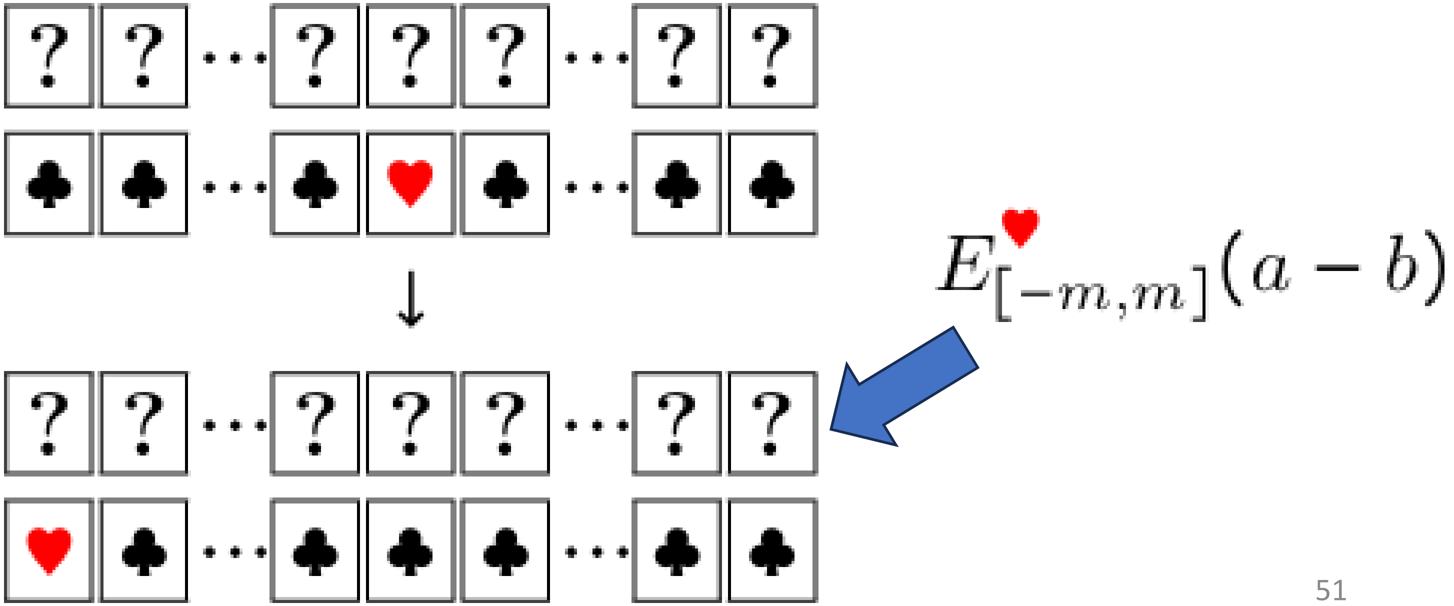
(3) Open the second sequence and shift the two sequences until ♥ is at the left edge:



(2) Apply a pile-shifting shuffle:



(3) Open the second sequence and shift the two sequences until ♥ is at the left edge:



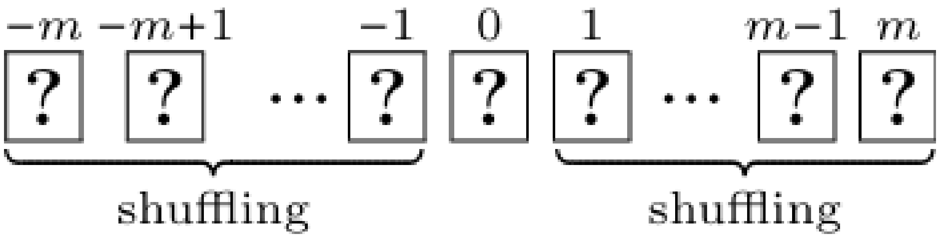
Comparison protocol

Input: $E^{\heartsuit}_{m+1}(a)$ and $E^{\heartsuit}_{m+1}(b)$

(1) By the subtraction protocol, we obtain

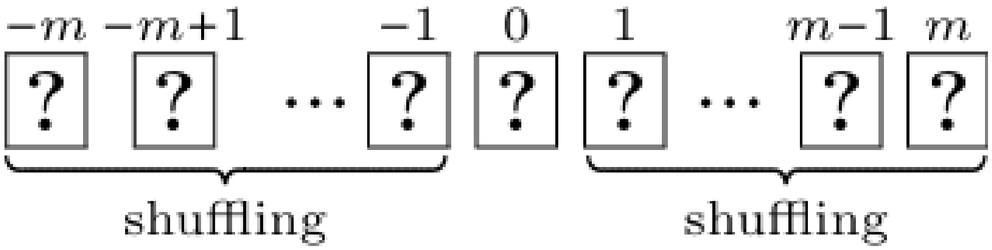
$$E^{\heartsuit}_{[-m,m]}(a-b): \boxed{?}\boxed{?}\cdots\boxed{?}\boxed{?}\boxed{?}\cdots\boxed{?}\boxed{?}$$

(2) Two shuffles are applied:



Comparison protocol

(2) Two shuffles are applied:



(3) Turn over all cards:

- If ♥ appears in the center, then $a = b$;
- If ♥ appears on the left, then $a < b$; and
- If ♥ appears to the right, then $a > b$.

Table of Contents

Remember that in Gakmoro, each player holds 7 cards and submits 1 to 3 cards at every round.

Let us add two cards of value 0 to each player’s hand:

0, **0**, 1, 2, 3, 4, 5, 6, and 7

Then, we can assume that each player, holding 9 cards, submits exactly 3 cards at every round.

Gakmoro with secure computation

(1) Prepare nine bundles for each of Alice and Bob:

$$E_8^{\heartsuit}(0), E_8^{\heartsuit}(0), E_8^{\heartsuit}(1), E_8^{\heartsuit}(2), E_8^{\heartsuit}(3), E_8^{\heartsuit}(4), E_8^{\heartsuit}(5), E_8^{\heartsuit}(6), E_8^{\heartsuit}(7)$$

Alice

$$E_8^{\heartsuit}(0), E_8^{\heartsuit}(0), E_8^{\heartsuit}(1), E_8^{\heartsuit}(2), E_8^{\heartsuit}(3), E_8^{\heartsuit}(4), E_8^{\heartsuit}(5), E_8^{\heartsuit}(6), E_8^{\heartsuit}(7)$$

Bob

Gakmoro with secure computation

(1) Prepare nine bundles for each of Alice and Bob:

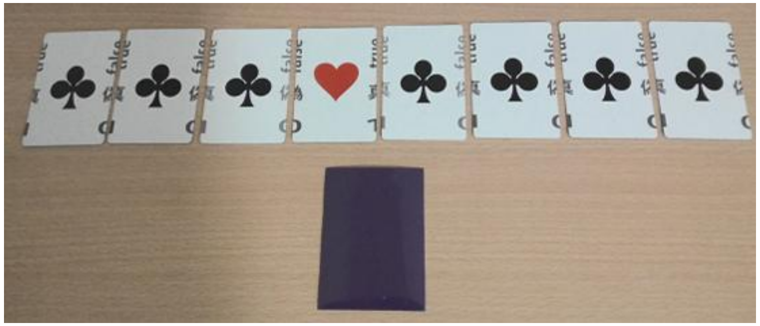
Alice

$E_8^{\heartsuit}(0), E_8^{\heartsuit}(0), E_8^{\heartsuit}(1), E_8^{\heartsuit}(2), E_8^{\heartsuit}(3), E_8^{\heartsuit}(4), E_8^{\heartsuit}(5), E_8^{\heartsuit}(6), E_8^{\heartsuit}(7)$

B

7)

place in a sleeve



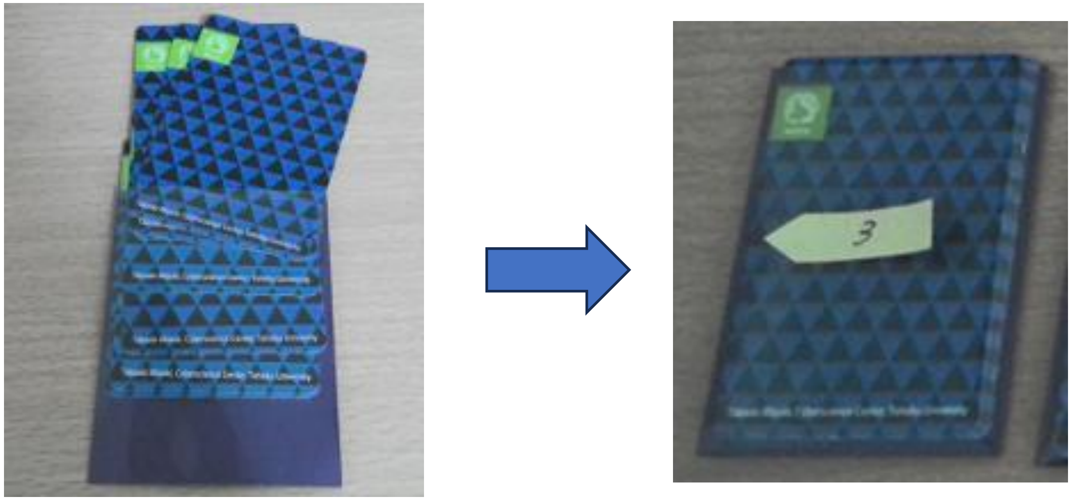
Gakmoro with secure computation

(1) Prepare nine bundles for each of Alice and Bob:

Alice

$$E_8^{\heartsuit}(0), E_8^{\heartsuit}(0), E_8^{\heartsuit}(1), E_8^{\heartsuit}(2), E_8^{\heartsuit}(3), E_8^{\heartsuit}(4), E_8^{\heartsuit}(5), E_8^{\heartsuit}(6), E_8^{\heartsuit}(7)$$

Bob

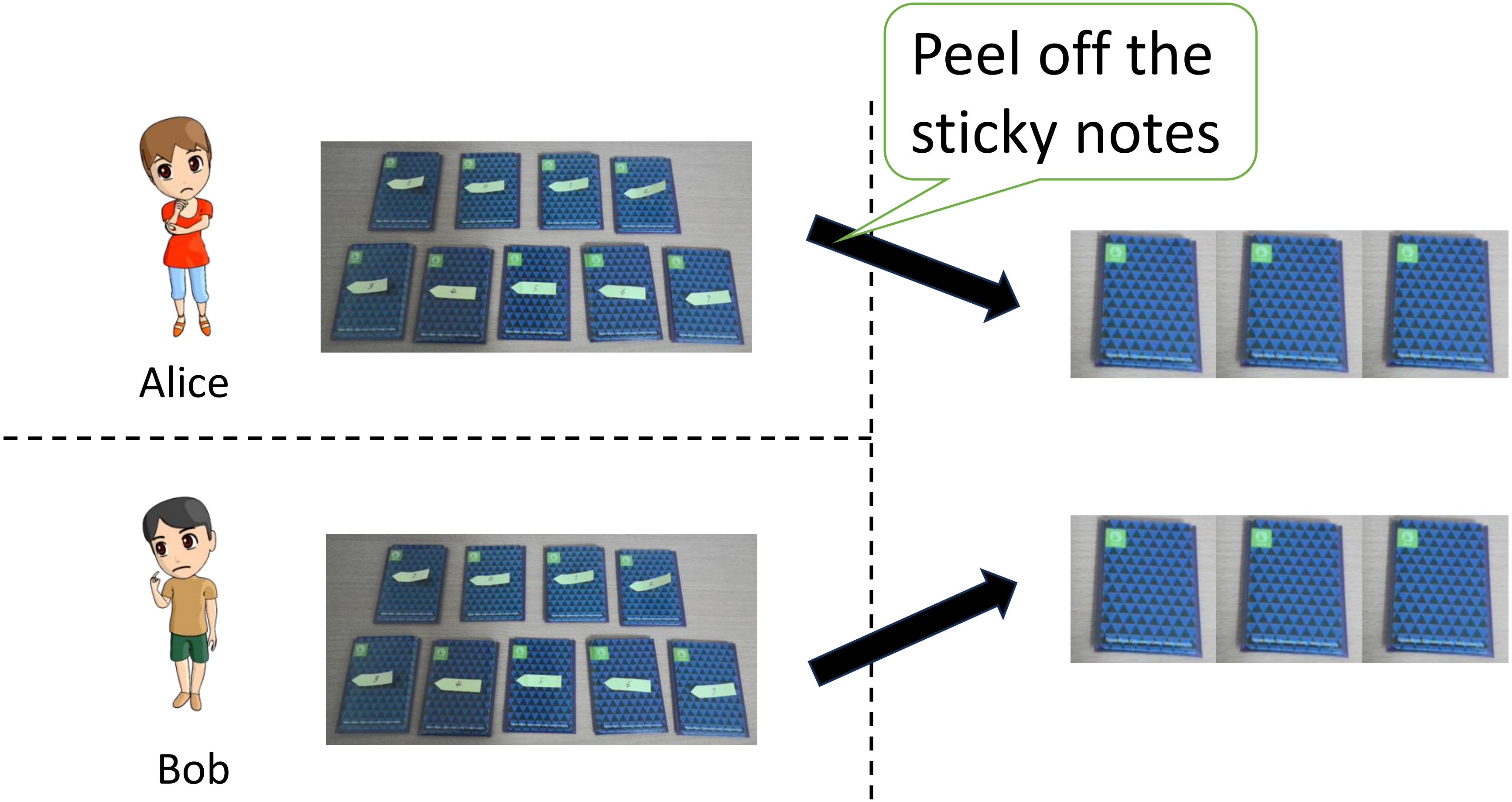


sticky note

“3” is written

- ✓ make up the hand in units of sleeves

(2) Each player chooses 3 bundles from their hand and places them face down on the table:



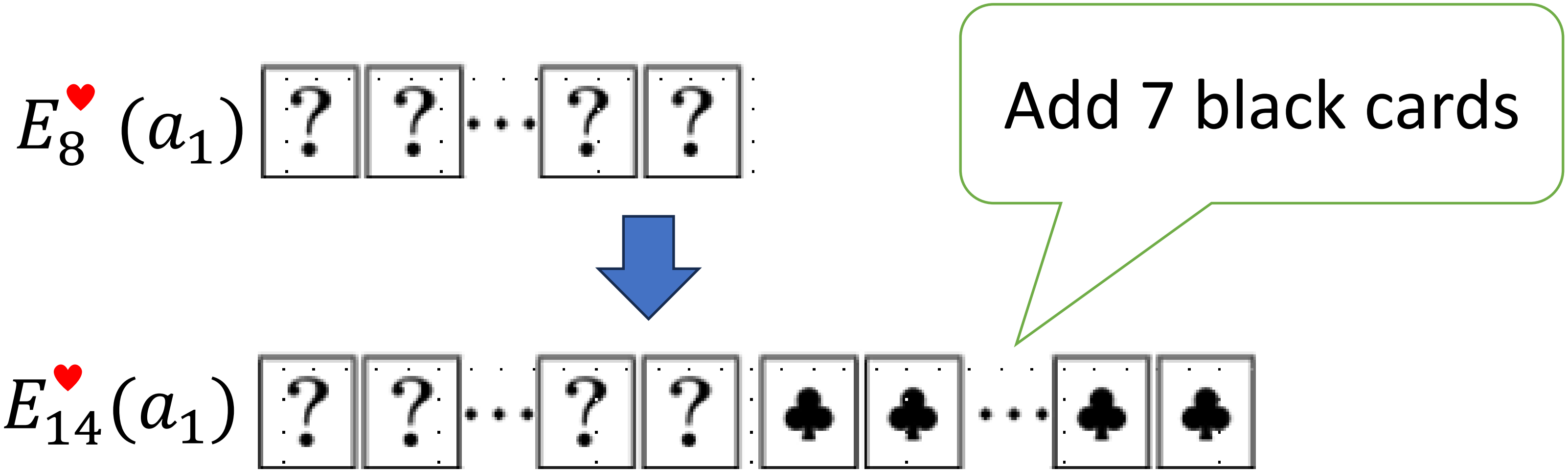
Peel off the sticky notes

Alice

Bob

(3) Apply the addition protocol

$$\underbrace{E_8^{\heartsuit}(a_1)\quad E_8^{\heartsuit}(a_2)}_{a_1+a_2\le 13}\quad E_8^{\heartsuit}(a_3)$$



$E_8^{\heartsuit}(a_1)$? ? ⋯ ? ?

$E_{14}^{\heartsuit}(a_1)$? ? ⋯ ? ? ♣ ♣ ⋯ ♣ ♣

Add 7 black cards

(3) Apply the addition protocol

$$\underbrace{E_8^{\heartsuit}(a_1)\quad E_8^{\heartsuit}(a_2)}\quad E_8^{\heartsuit}(a_3)$$

$\Downarrow$ addition protocol

$$E_{14}^{\heartsuit}(a_1+a_2)$$

(3) Apply the addition protocol

$E_8^{\heartsuit}(a_1)$ $E_8^{\heartsuit}(a_2)$

$E_{14}^{\heartsuit}(a_1 + a_2)$ $E_8^{\heartsuit}(a_3)$

addition protocol

$E_{19}^{\heartsuit}(a_1 + a_2 + a_3)$

(4) Apply the comparison protocol to:

$$E^{\heartsuit}_{19}(a_1 + a_2 + a_3) \quad \text{and} \quad E^{\heartsuit}_{19}(b_1 + b_2 + b_3)$$

to determine who is the winner.

(5) Step (2) to Step (4) are repeated for up to three rounds, with the first player to win two rounds being declared the winner.

Requirements in implementation

- The first addition uses 14 × 2 = 28 cards
- The second addition uses 19 × 2 = 38 cards
- The comparison protocol uses (19 +18) × 2 = 74 cards

The number of required cards and required space are not so small.

→ Further optimization is expected.

Table of Contents

We proposed a new card game called ***Gakmoro***.

We then presented a method that utilizes secure computation to allow two players to enjoy Gakmoro without a dealer.

We have demonstrated that card-based cryptography can increase the flexibility of game play.

Similar recent work: creating virtual players in card games:

- Old Maid (Theory of Computing Systems, 69(1), 2025)
- UNO (this Monday by Ruangwises and Shinagawa)

How about joining this hot research topic?