An Application of Secure Computation to Tagiron

Koichi Koizumi National Institute of Technology, Fukushima College

Takaaki Mizuki Cyberscience Center, Tohoku University

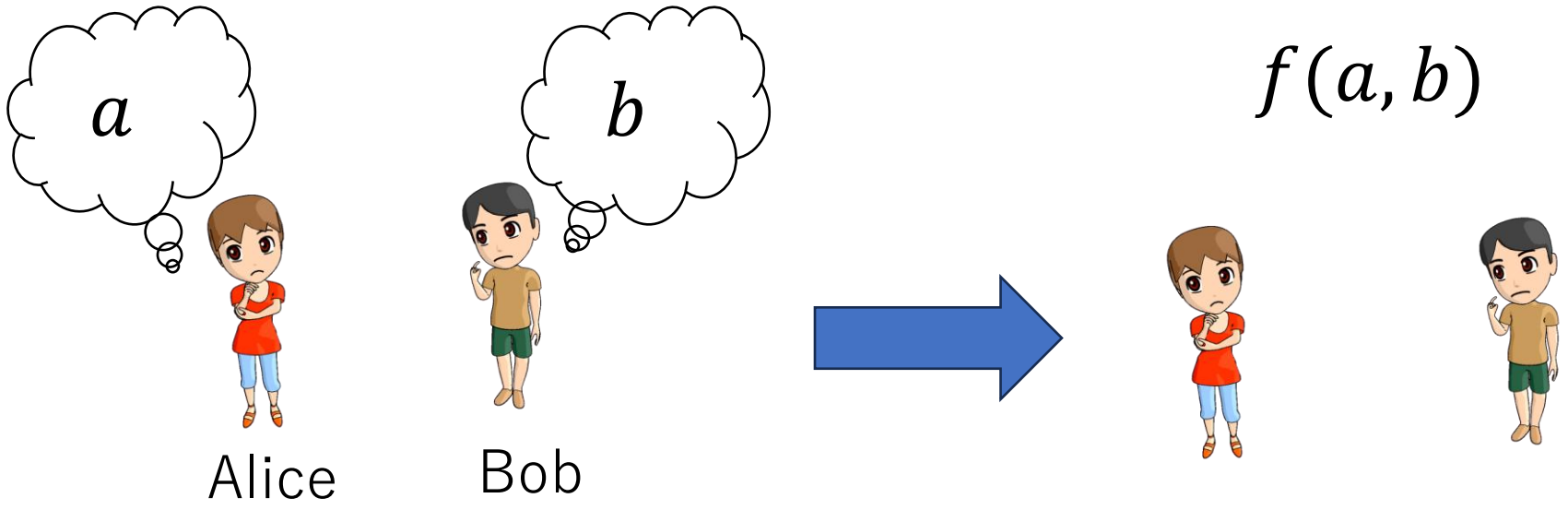
ACG 2025

An Application of Secure Computation to *Tagiron*

A logic-based deduction game

Tagiron by JELLY JELLY GAMES (https://jelly2games.com/tagiron)

An Application of ***Secure Computation*** to Tagiron



Cryptographic technique enabling players to know only the value of a function without leaking information about inputs

An *Application* of Secure Computation to Tagiron

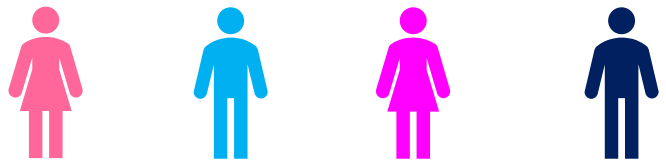
We apply secure computation to enhancing gameplay of Tagiron.

Table of Contents

Table of Contents

Tagiron (a.k.a. Break the Code)

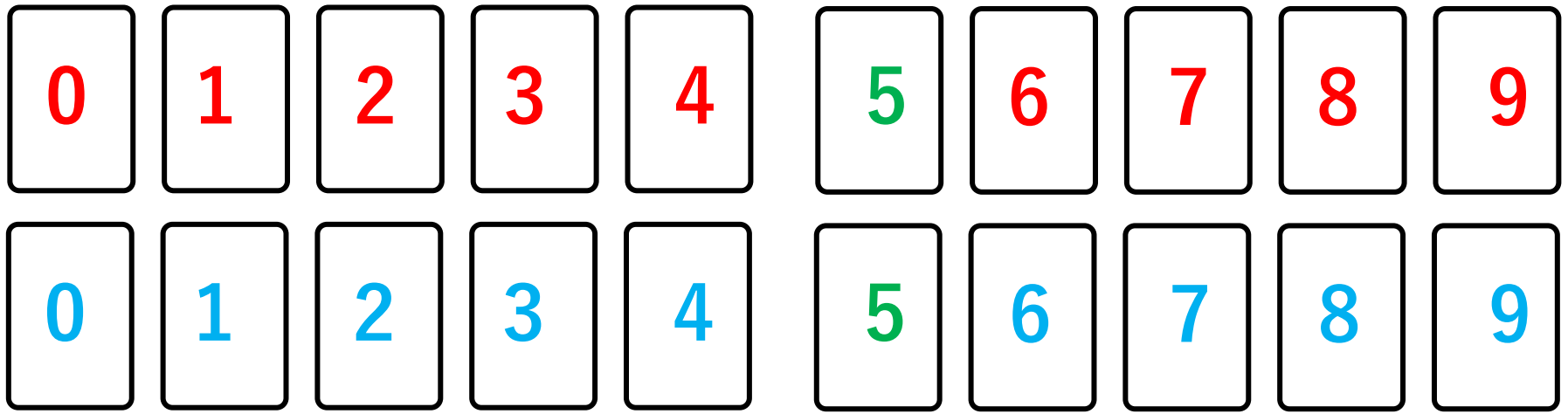
- A popular logic-based deduction game invented by Ryohei Kurahashi.
- The game is played with 2 to 4 players, but we focus on the *4-player* version.



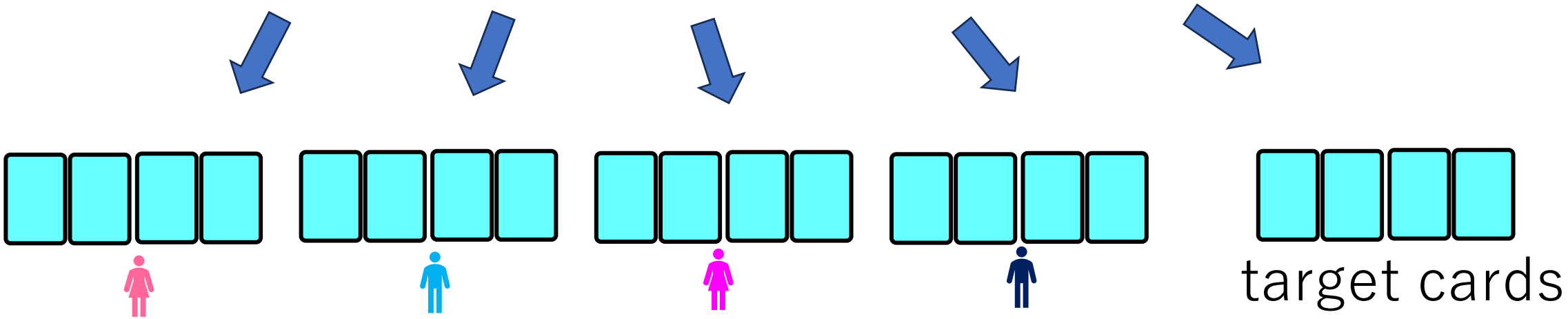
- There are 20 Tagiron cards (small tiles).

20 Tagiron cards (small tiles)

- Has a number from 0 to 9 and a color of red, blue, or green

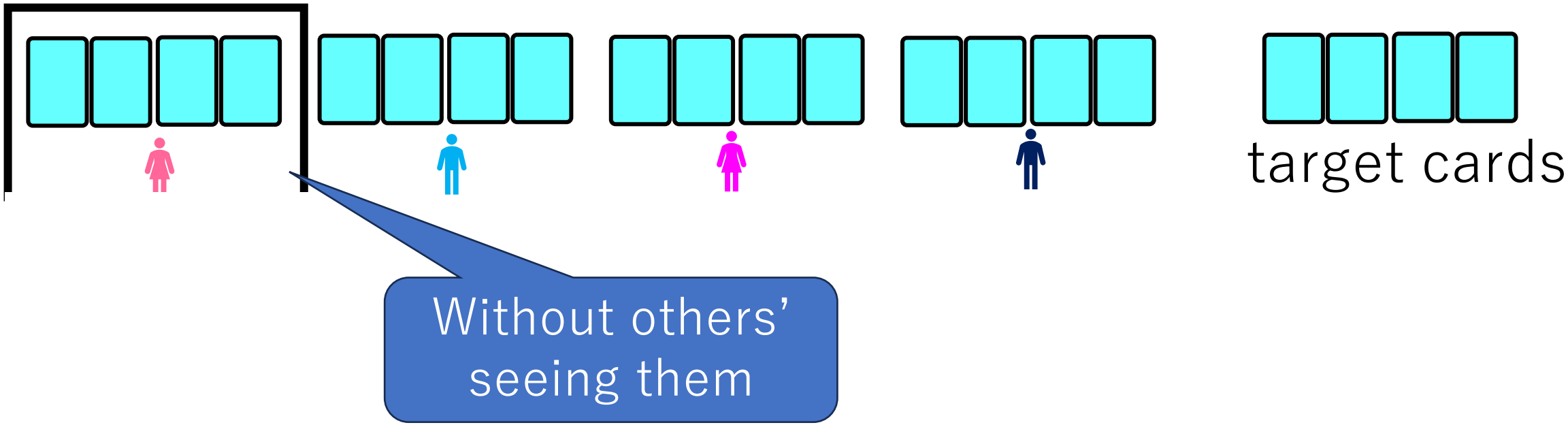


The 20 Tagiron cards are shuffled and distributed:

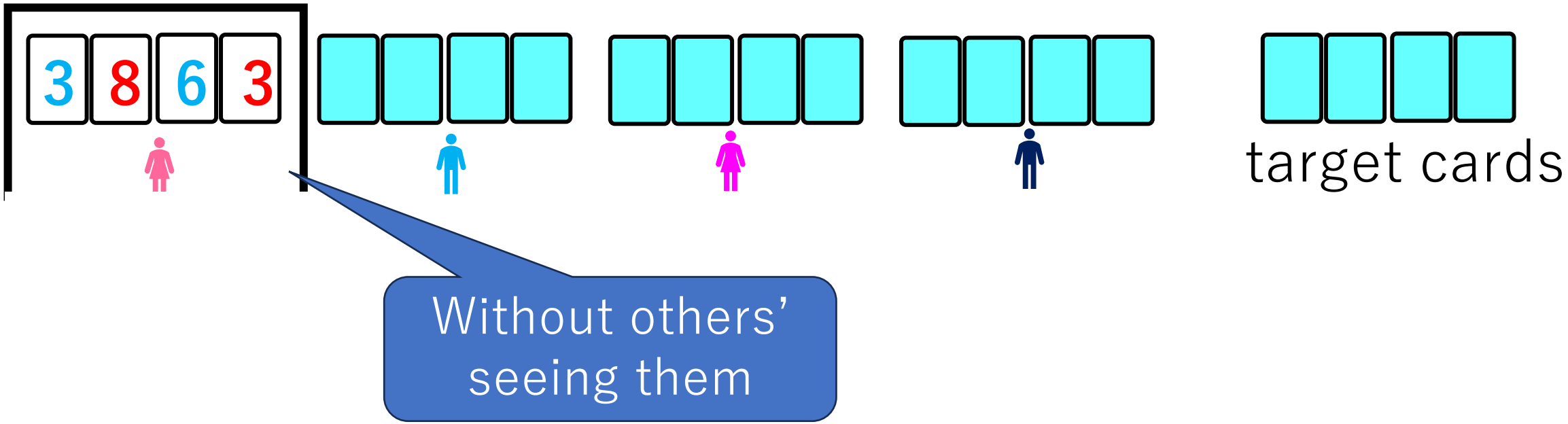


- Each player receives 4 cards.
- The remaining 4 cards become the target to deduce.

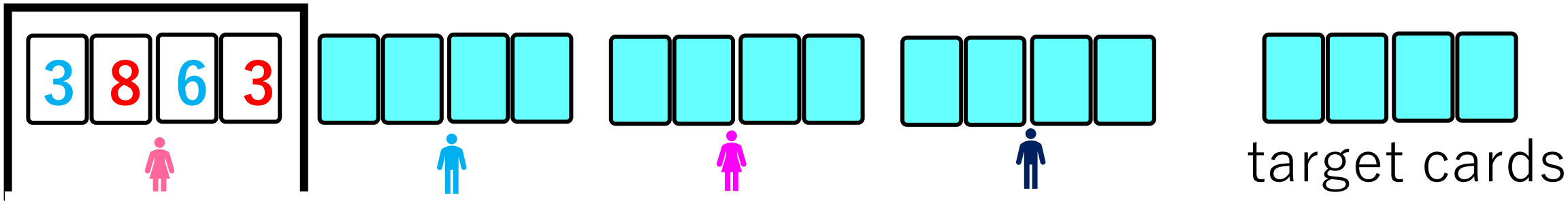
- Each player secretly looks at their 4 cards



・Each player secretly looks at their 4 cards

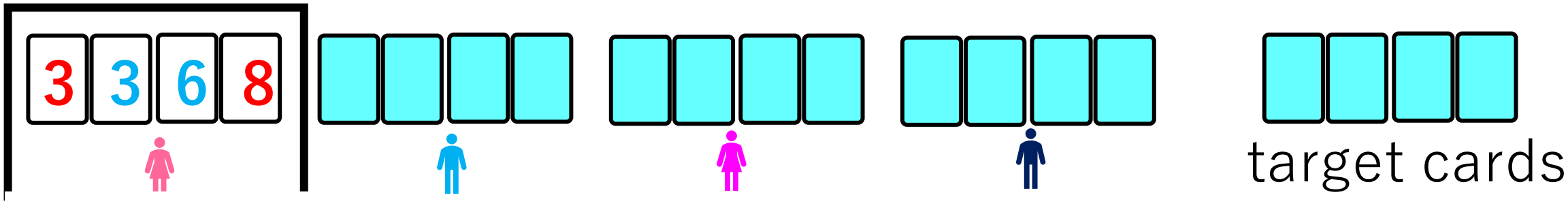


- Each player secretly looks at their 4 cards
- Sort the 4 cards in ascending order from left to right



red < **blue**

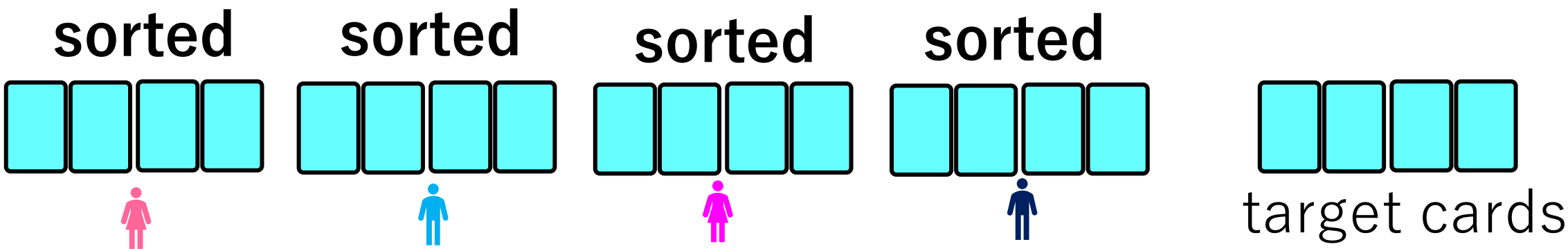
- Each player secretly looks at their 4 cards
- Sort the 4 cards in ascending order from left to right



sorted

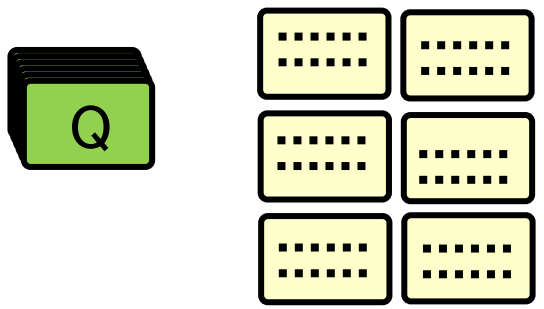
red < **blue**

- Each player secretly looks at their 4 cards
- Sort the 4 cards in ascending order from left to right

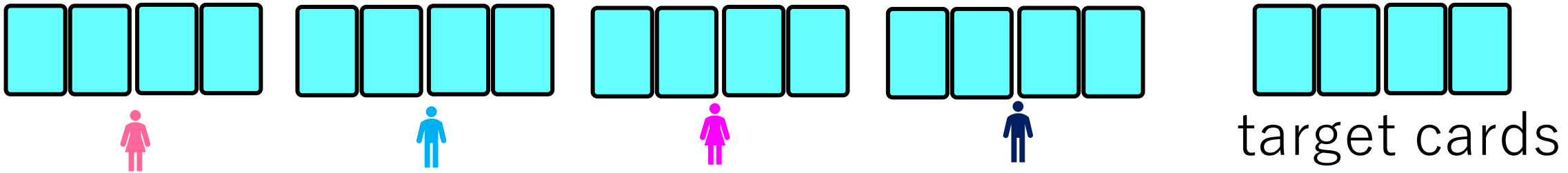


red < **blue**

19 **question cards** are shuffled and 6 of them are revealed

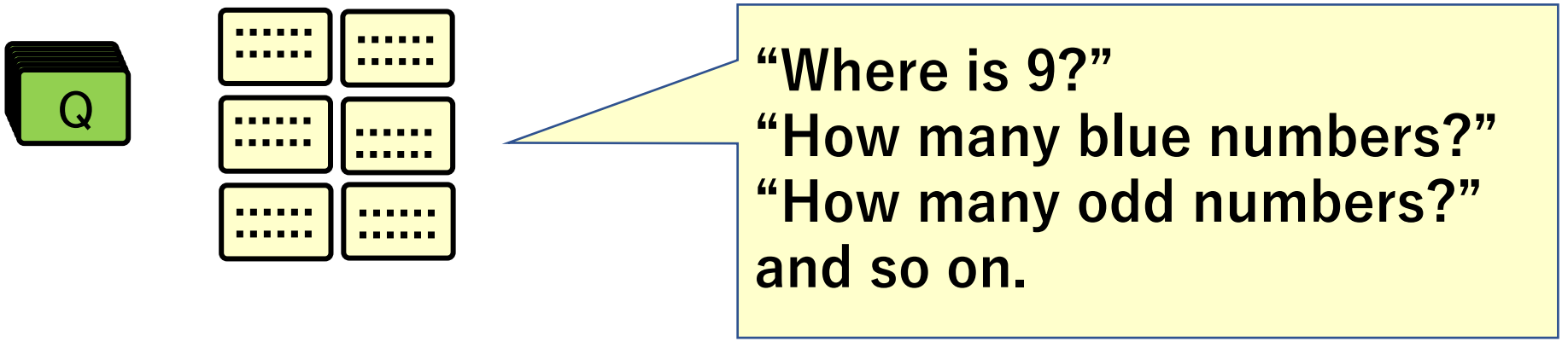


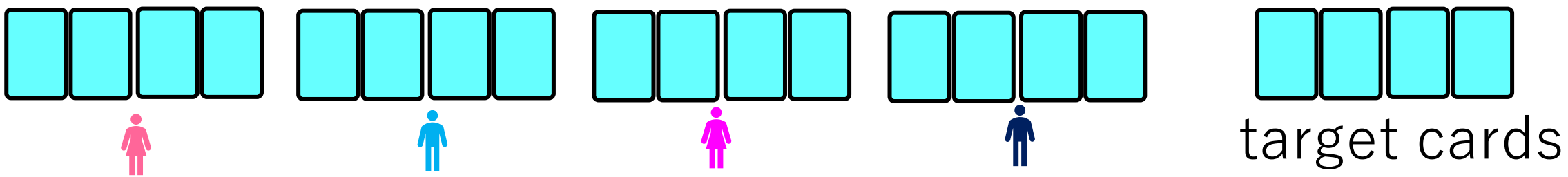
“Where is 9?”
“How many blue numbers?”
“How many odd numbers?”
and so on.



Players take turns:

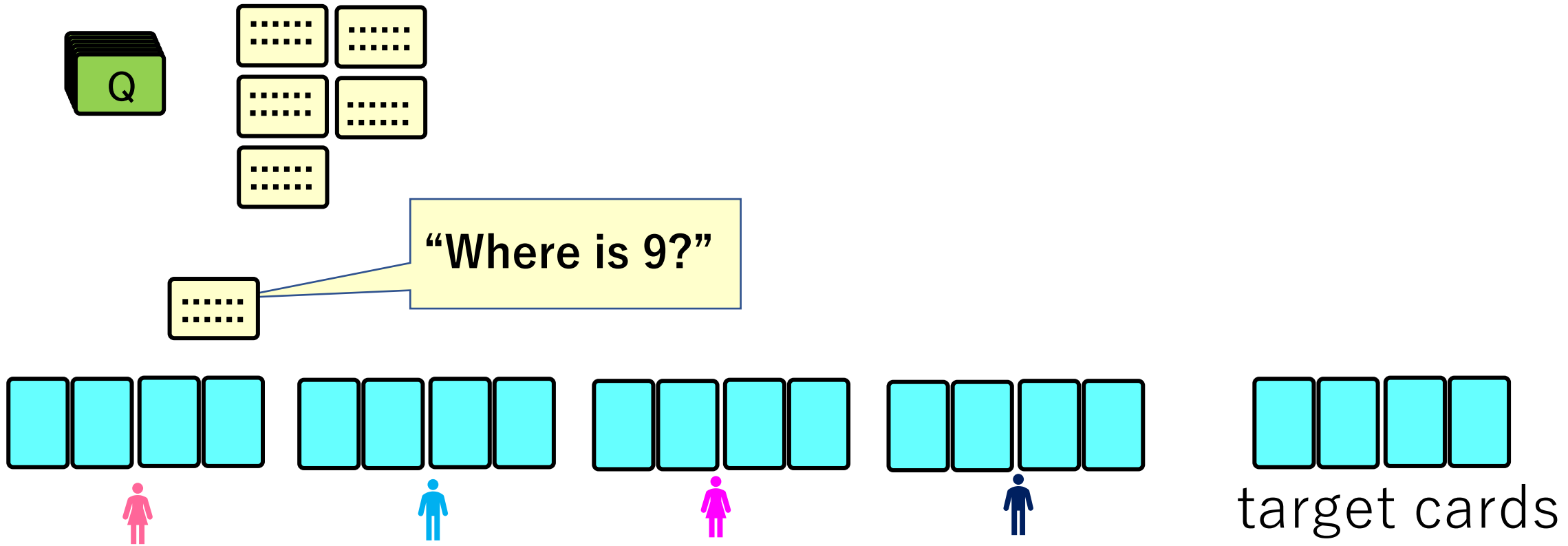
1. A player chooses one question card and asks a question.
2. All players answer the question honestly.
3. A new question card is revealed from the deck.





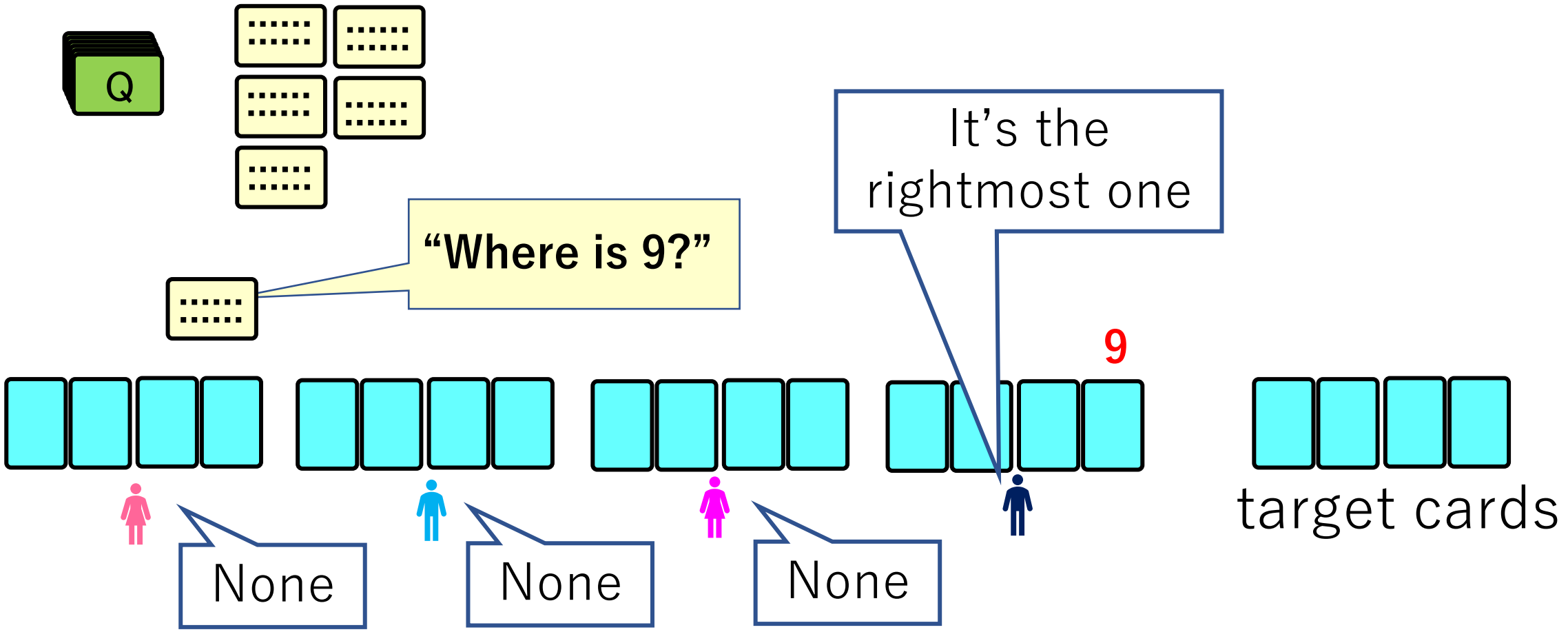
Players take turns:

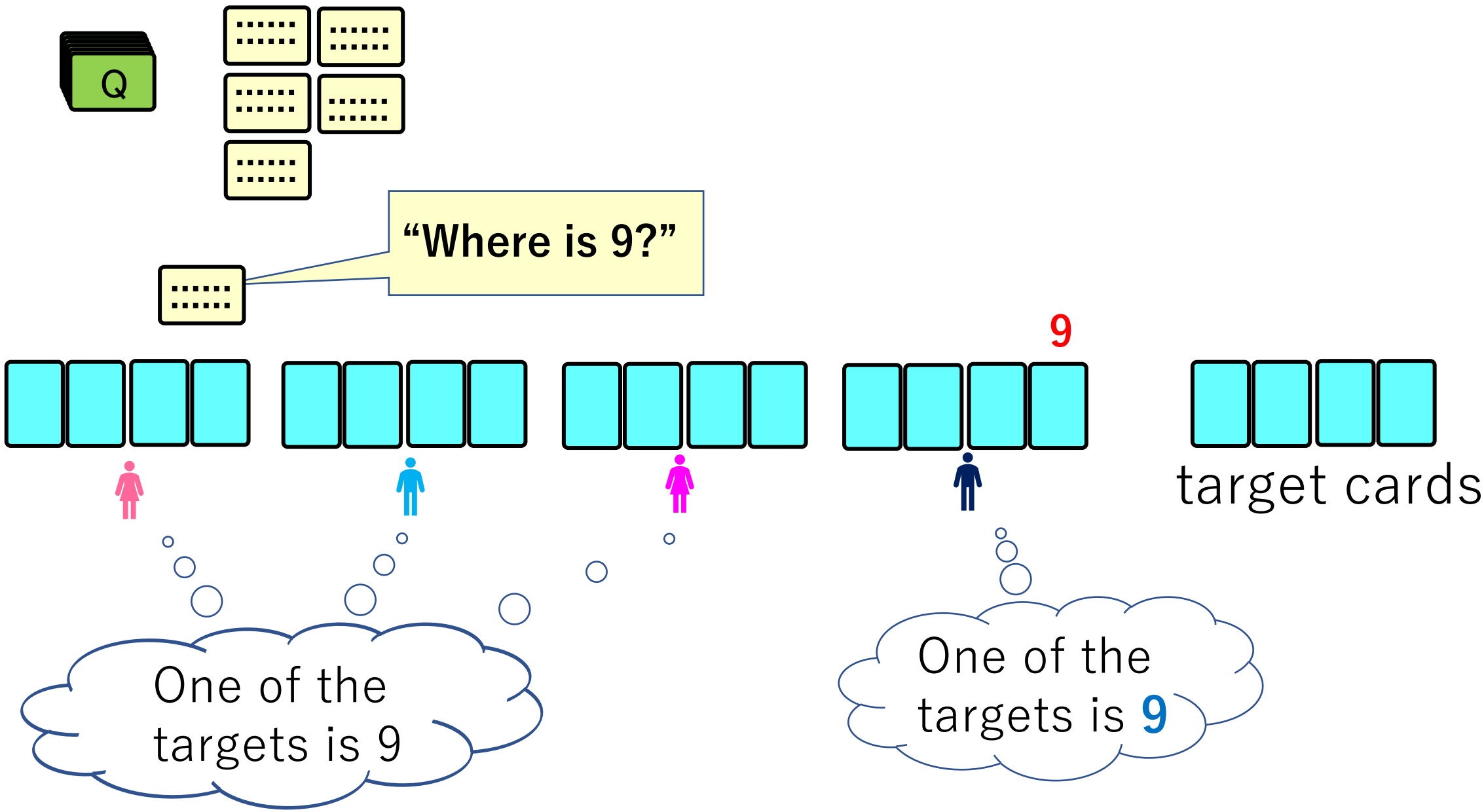
1. A player chooses one question card and asks a question.
2. All players answer the question honestly.
3. A new question card is revealed from the deck.



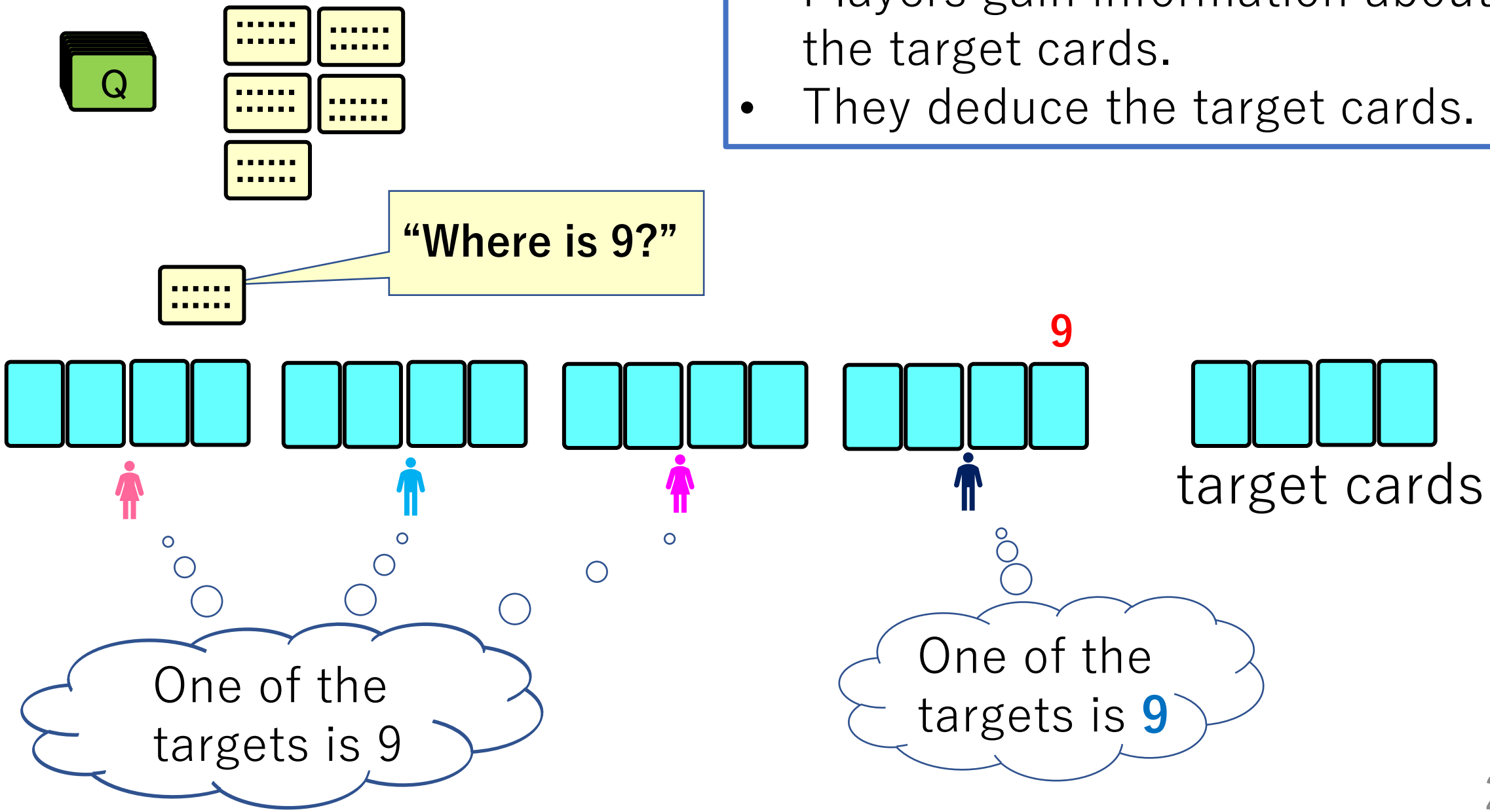
Players take turns:

1. A player chooses one question card and asks a question.
2. All players answer the question honestly.
3. A new question card is revealed from the deck.

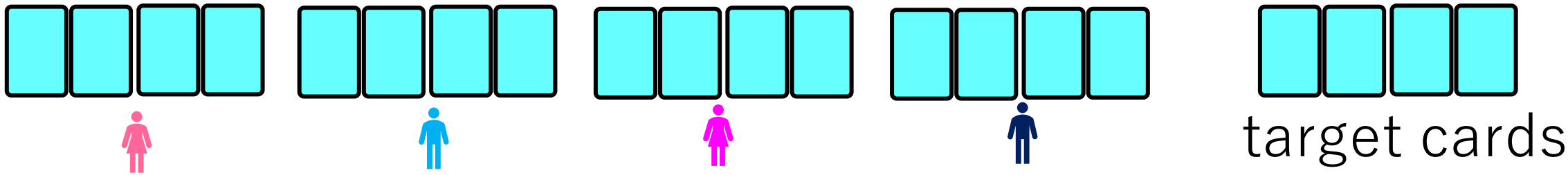



Q
“Where is 9?”
9
target cards
One of the targets is 9
One of the targets is 9

- Players gain information about the target cards.
- They deduce the target cards.

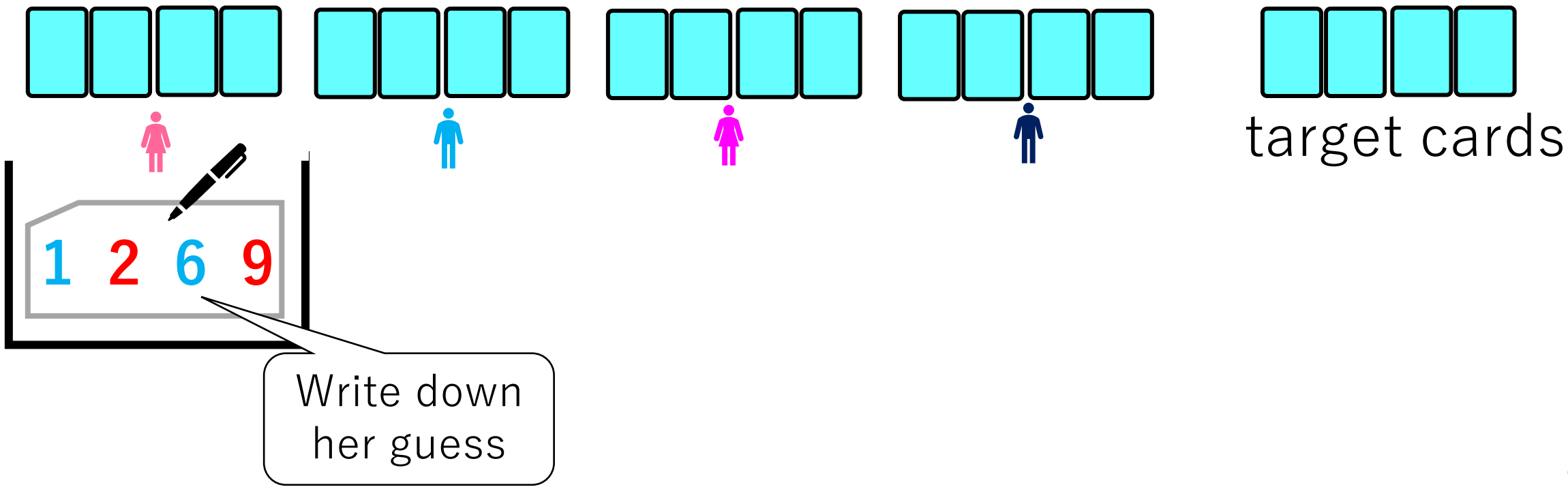


Each player can make a ***challenge*** anytime, but only once.



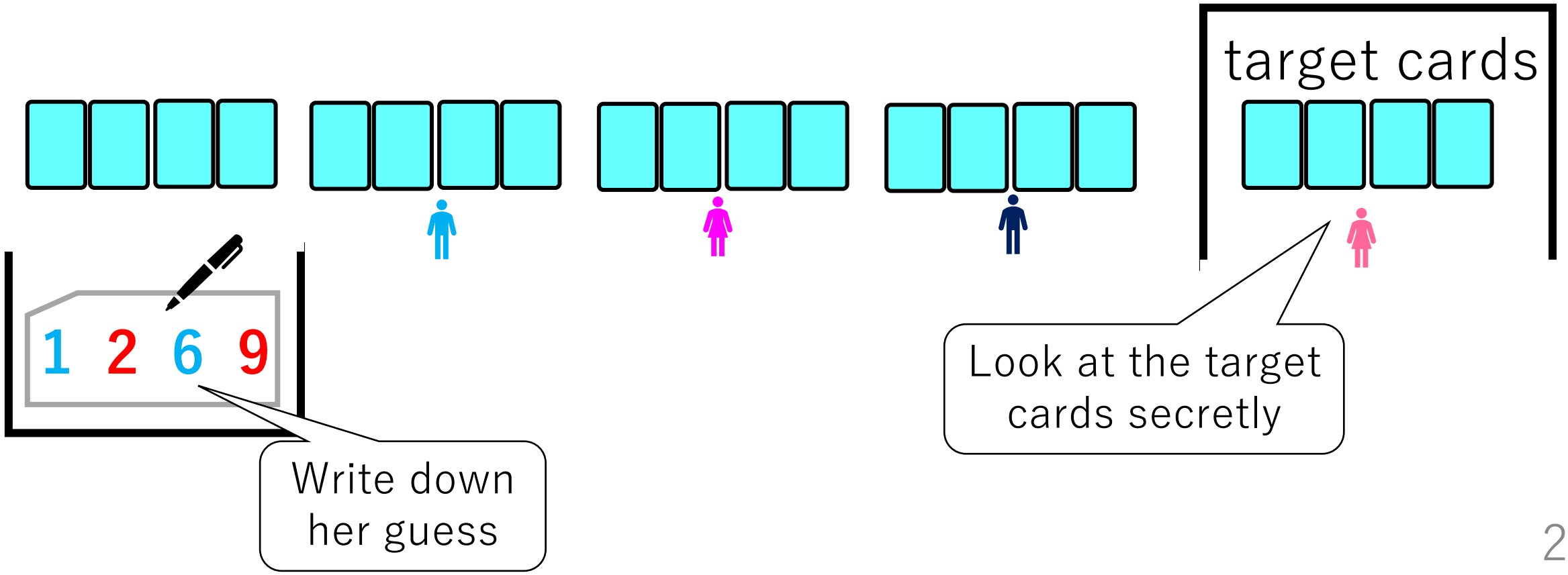
Each player can make a ***challenge*** anytime, but only once.

- The player who challenges writes down their guess.



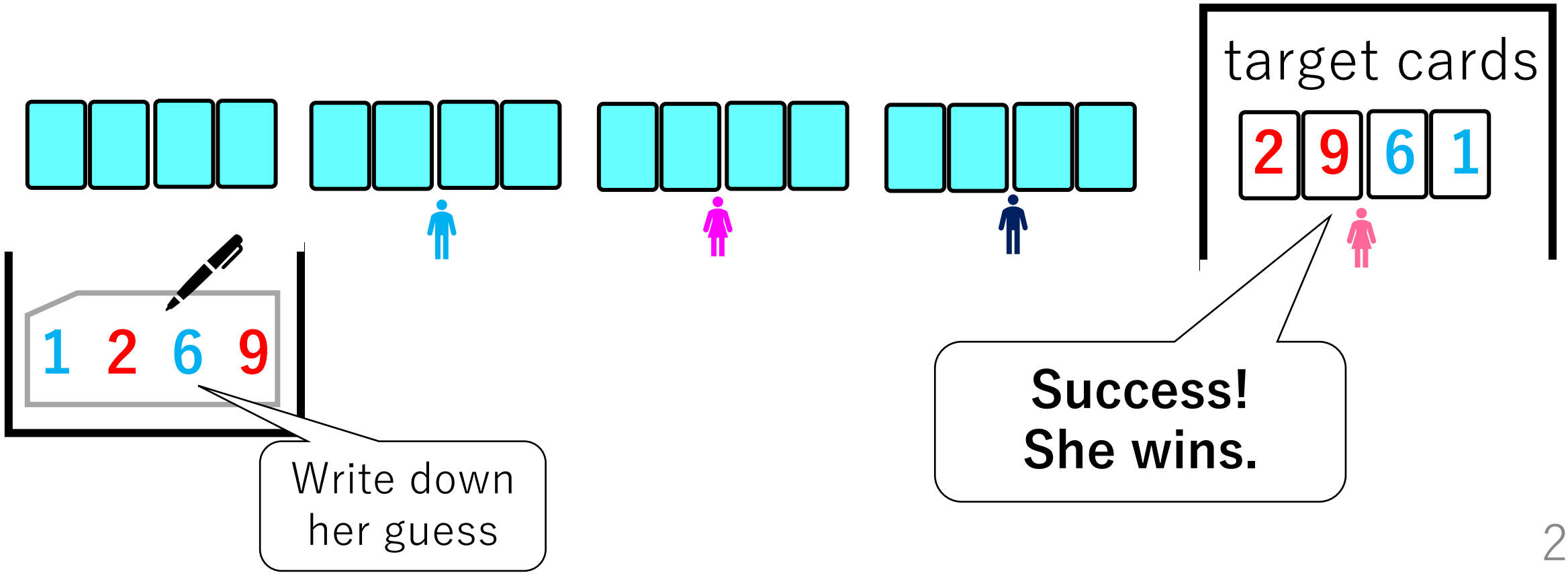
Each player can make a ***challenge*** anytime, but only once.

- The player who challenges writes down their guess.
- The player **looks at the four face-down target cards** secretly.



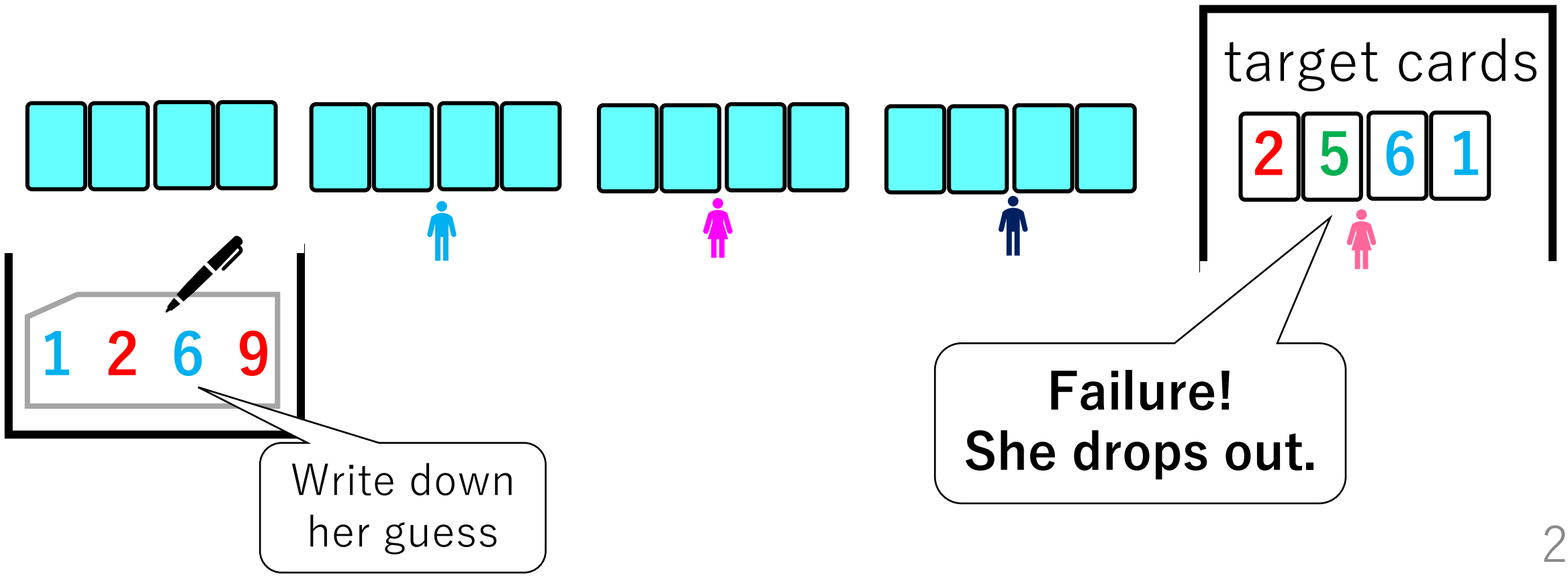
Each player can make a ***challenge*** anytime, but only once.

- The player who challenges writes down their guess.
- The player **looks at the four face-down target cards** secretly.



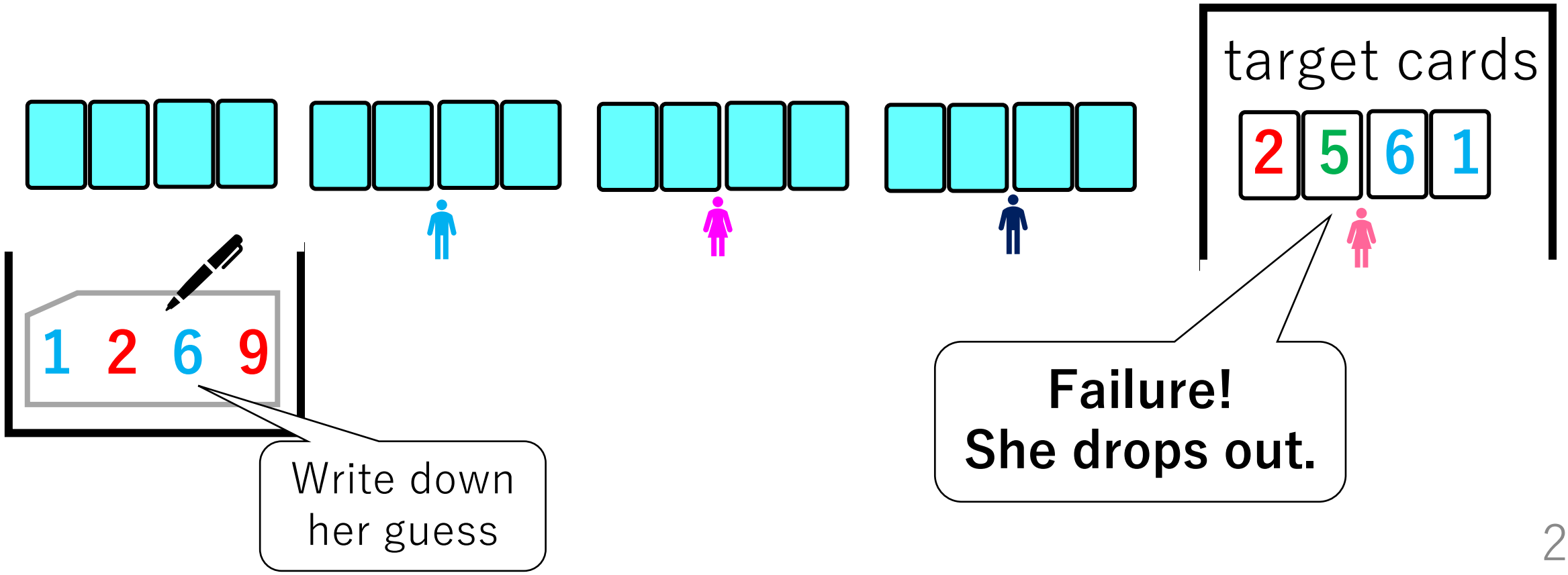
Each player can make a ***challenge*** anytime, but ***only once***.

- The player who challenges writes down their guess.
- The player **looks at the four face-down target cards** secretly.



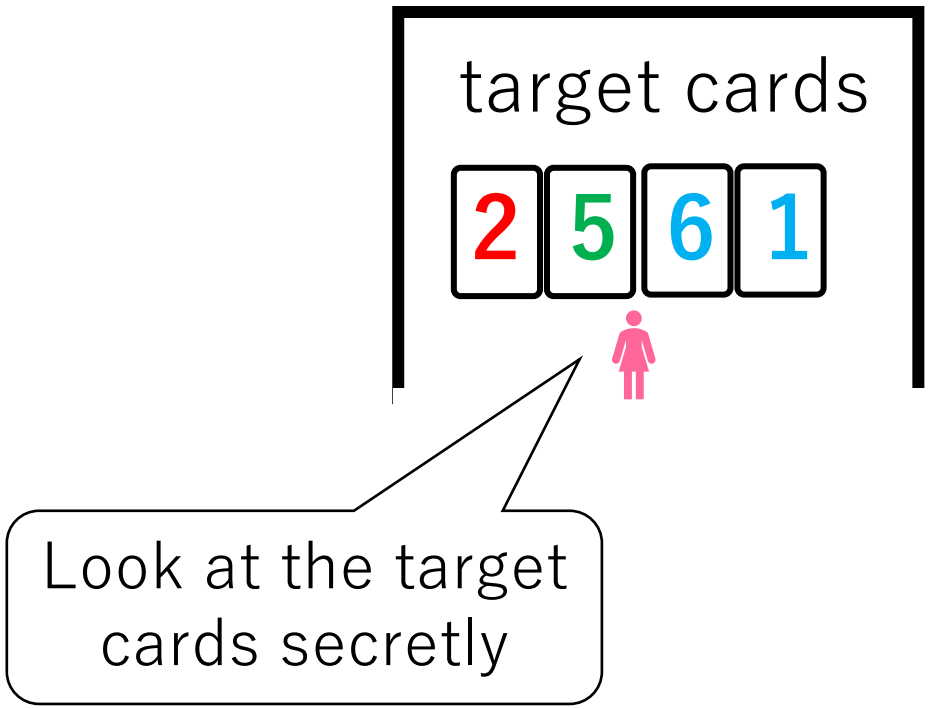
If player's guess is wrong, he or she is eliminated from the game.

This is because looking at the target cards makes him/her gain complete knowledge about the target cards.

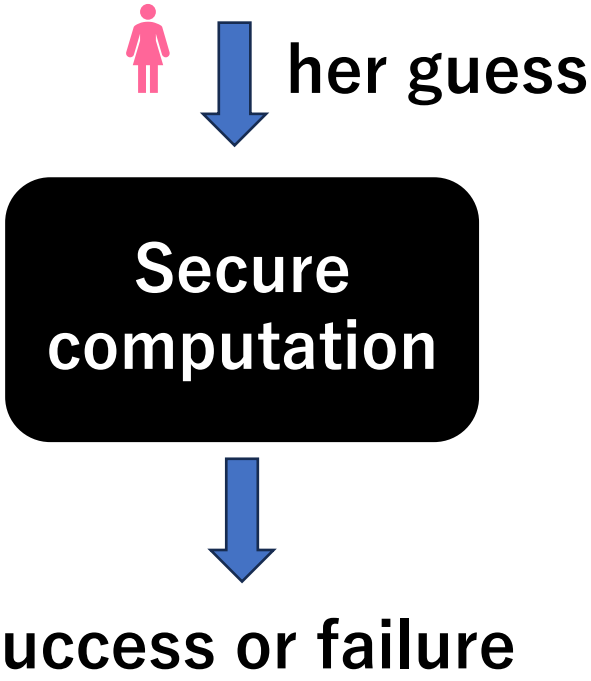


In this study, we explore an ***alternative challenge mechanism***.

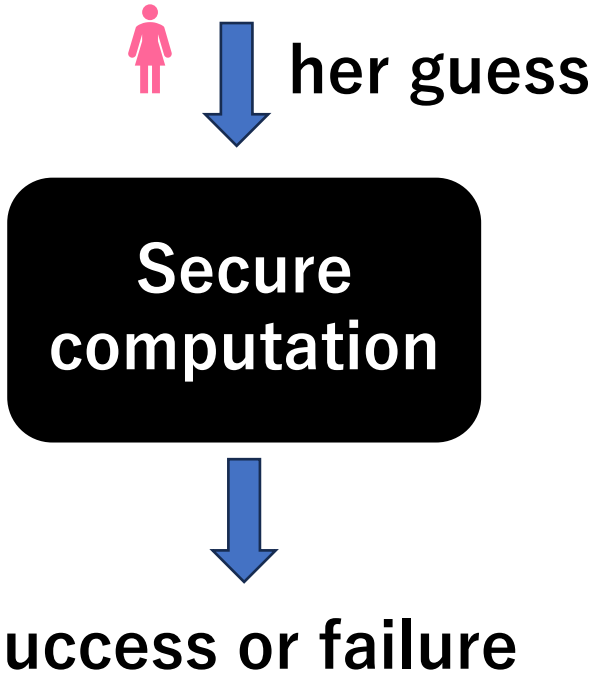
Original



Our method



Our method



A player who fails a challenge only learns that their guess is incorrect, allowing him/her to continue playing.

Our method

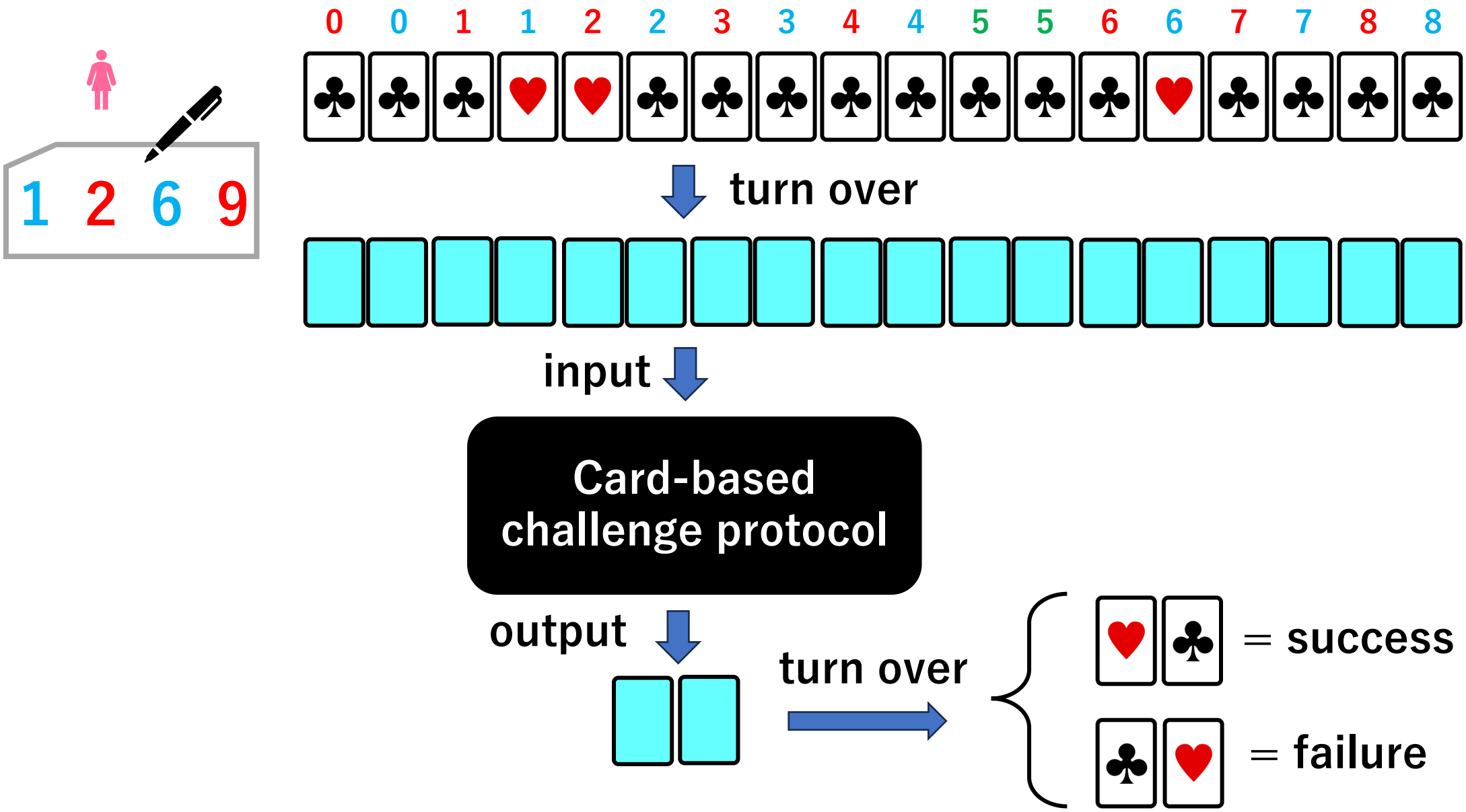
her guess

Secure computation

We use card-based cryptography

success or failure

Our challenge mechanism



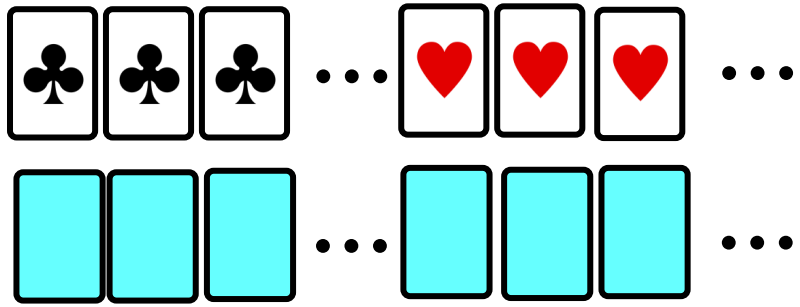
Our contribution

By using **card-based cryptography**, we propose a method for securely **determining whether a challenge succeeds or not** without leaking any information (more than necessary).

This provides new game variations of Tagiron; for example, a version could allow players **up to two challenges**, creating new strategic possibilities.

Table of Contents

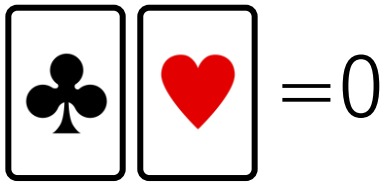
Card-based cryptography



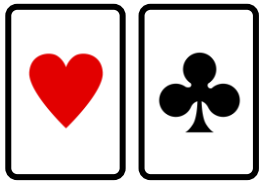
face-up

face-down

Encoding:

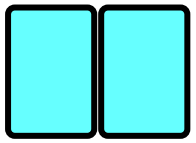


$=0$



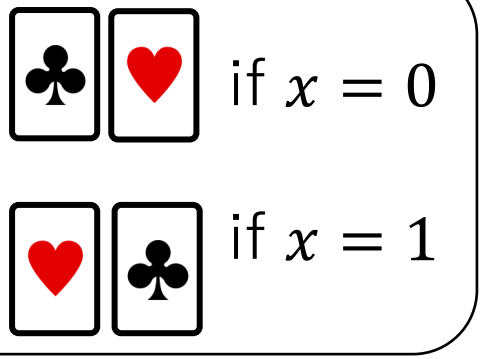
$=1$

Commitment to $x \in \{0,1\}$:



x

Face down



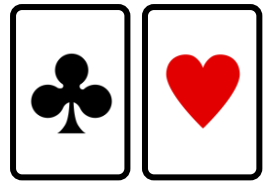
if $x = 0$

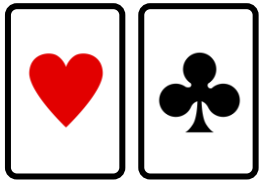
if $x = 1$

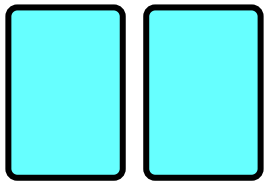
Card-based AND protocol

We want to obtain a commitment to the AND value without leaking any information. How?

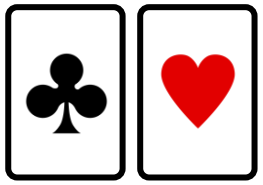
AND protocol [MS09]


=0

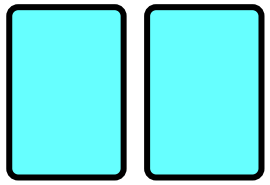

=1



x_1



0

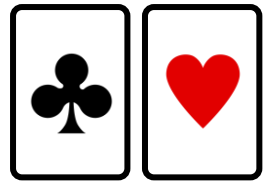


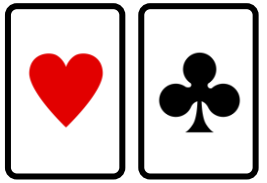
x_2

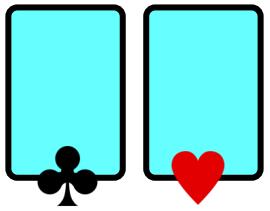
$$x_1 \wedge x_2 = \begin{cases} 0, & x_1 = 0 \\ x_2, & x_1 = 1 \end{cases}$$

[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

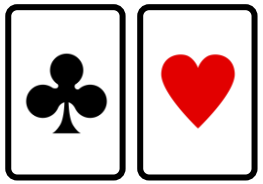
AND protocol [MS09]


=0

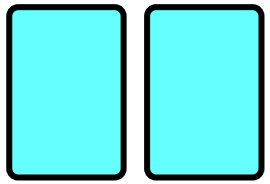

=1



x_1



0

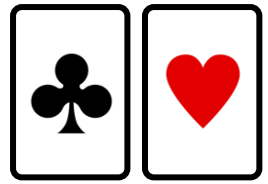


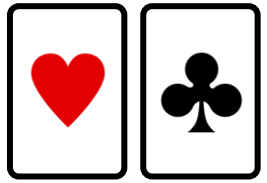
x_2

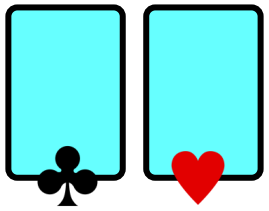
$$x_1 \wedge x_2 = \begin{cases} 0, & x_1 = 0 \\ x_2, & x_1 = 1 \end{cases}$$

[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

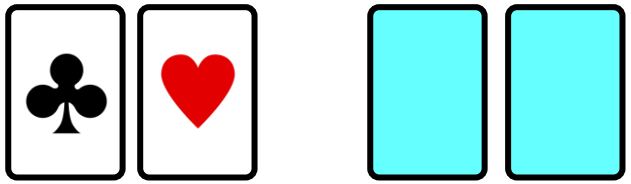
AND protocol [MS09]


=0


=1



x_1



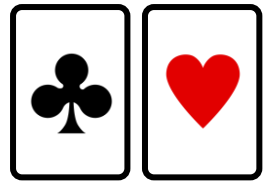
0 x_2

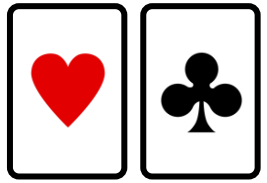
$x_1 \wedge x_2$

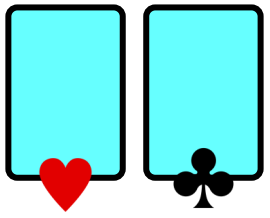
$$x_1 \wedge x_2 = \begin{cases} 0, & x_1 = 0 \\ x_2, & x_1 = 1 \end{cases}$$

[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

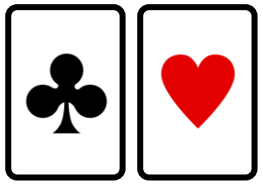
AND protocol [MS09]


=0

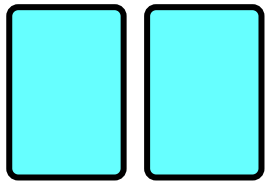

=1



x_1



0



x_2

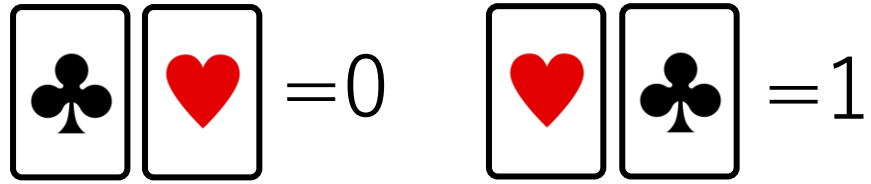
$$x_1 \wedge x_2 = \begin{cases} 0, & x_1 = 0 \\ x_2, & x_1 = 1 \end{cases}$$

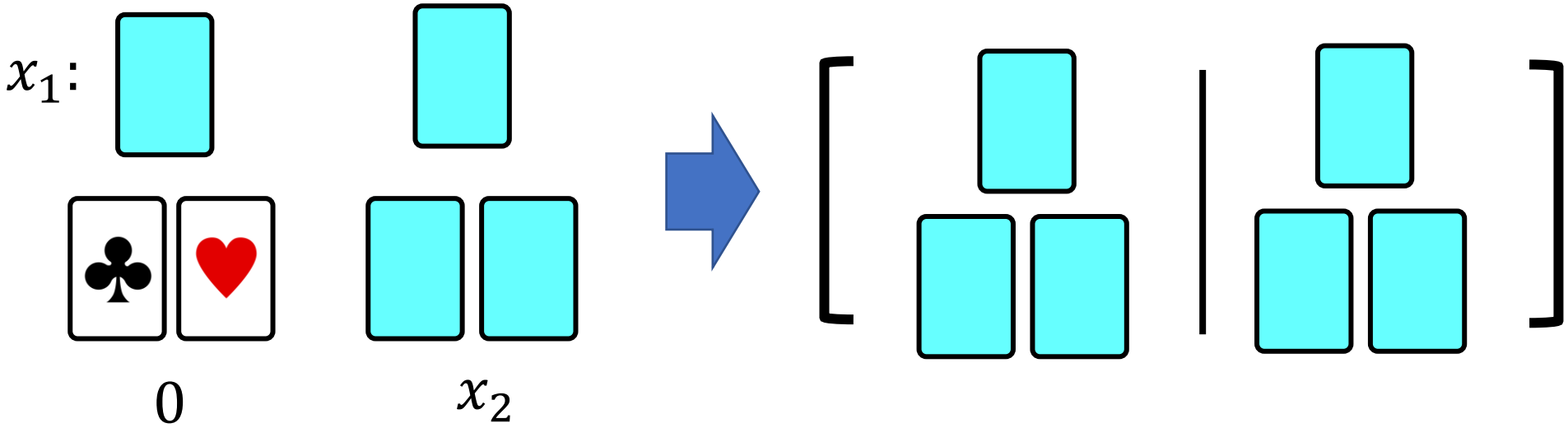
$x_1 \wedge x_2$ is always below 

$x_1 \wedge x_2$

[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

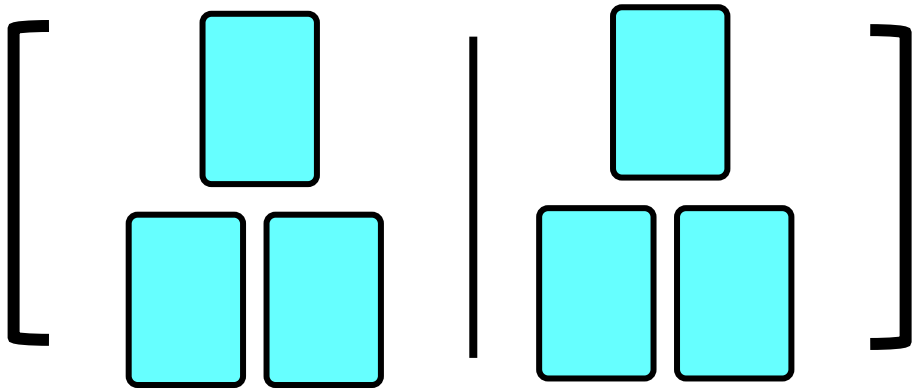
AND protocol [MS09]



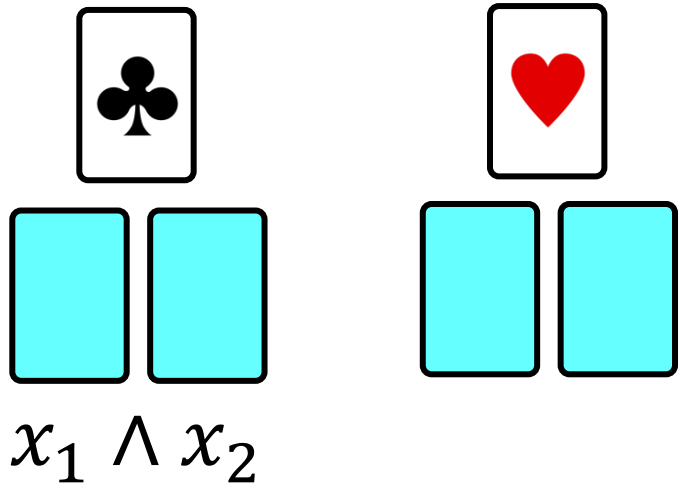


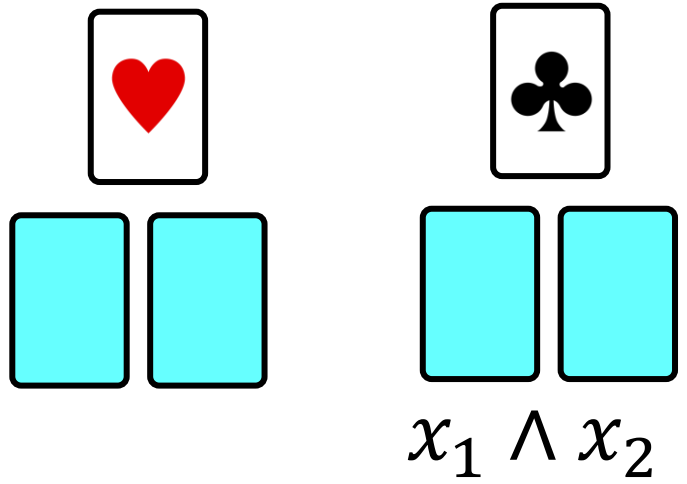
[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

AND protocol [MS09]



Open top cards

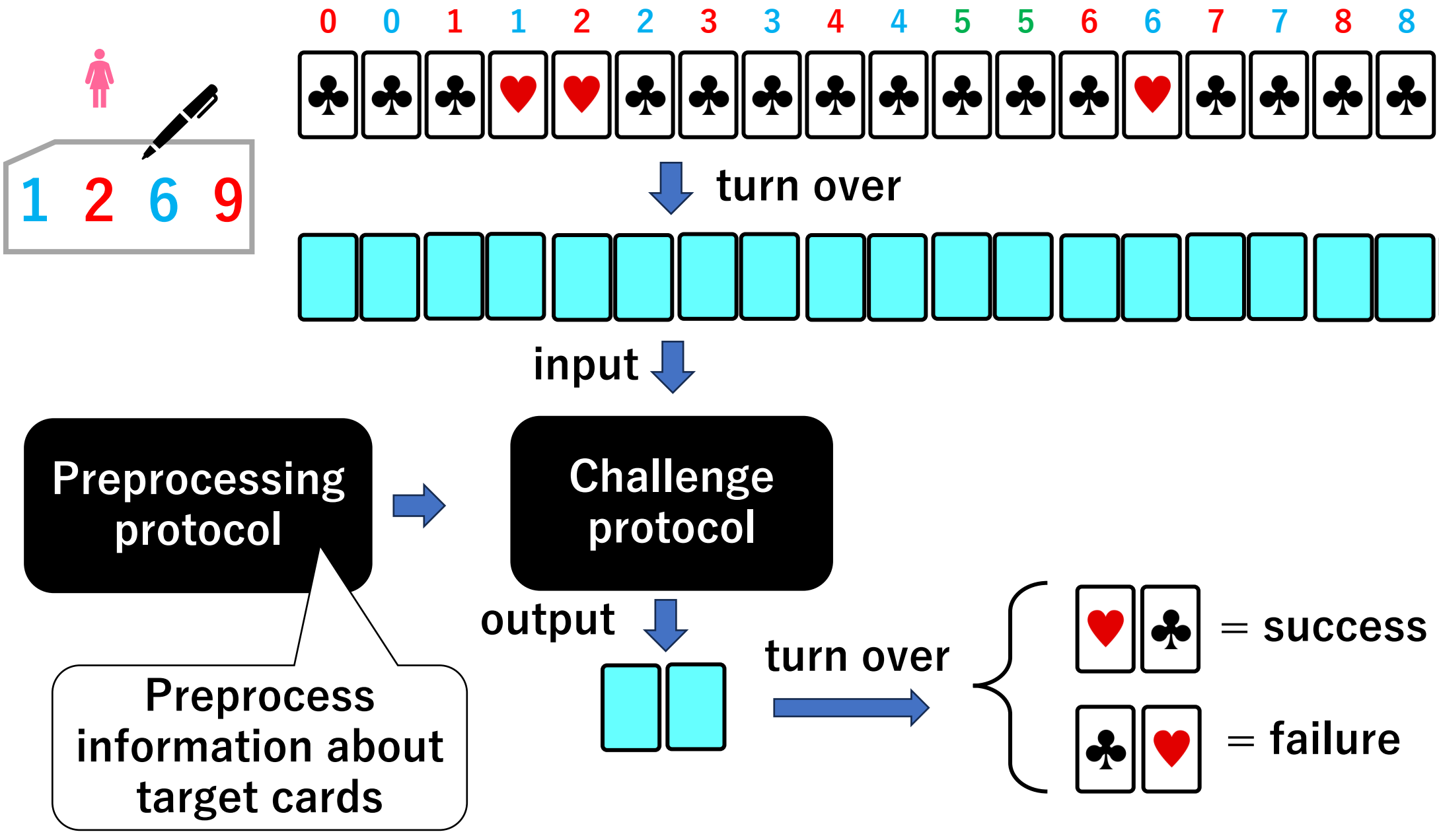




[MS09] Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR, Frontiers in Algorithmics, volume 5598 of LNCS, pages 358–369, Berlin, Heidelberg, 2009. Springer.

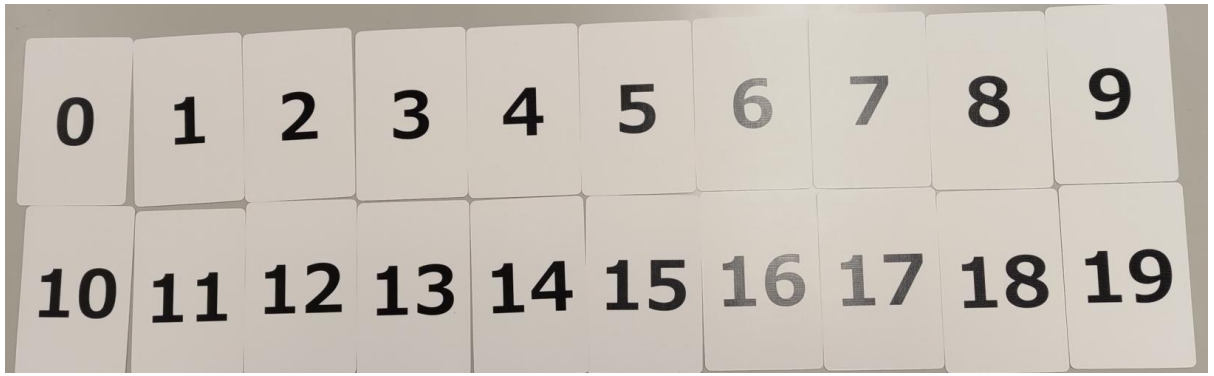
Table of Contents

Our method


0 0 1 1 2 2 3 3 4 4 5 5 6 6 7 7 8 8 9 9
1 2 6 9
turn over
input
Preprocessing protocol
Challenge protocol
Preprocess information about target cards
output
turn over
= success
= failure

Tagiron cards

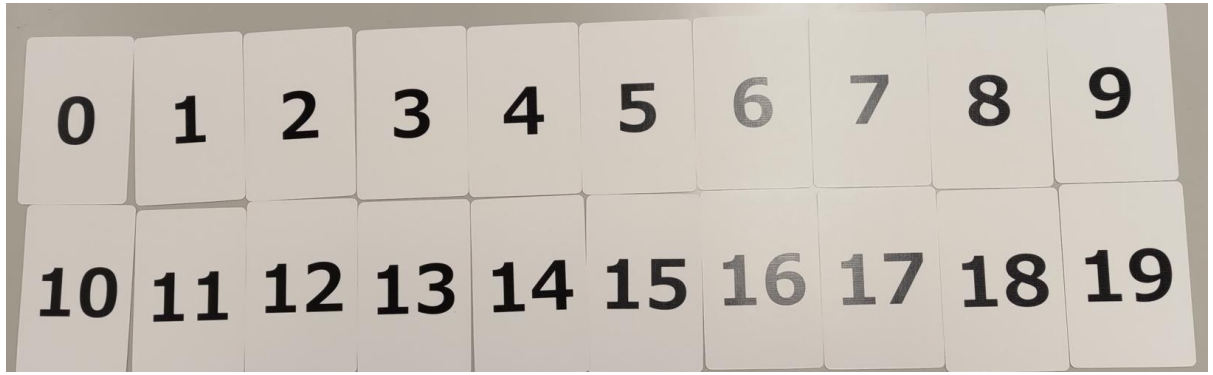
Number cards

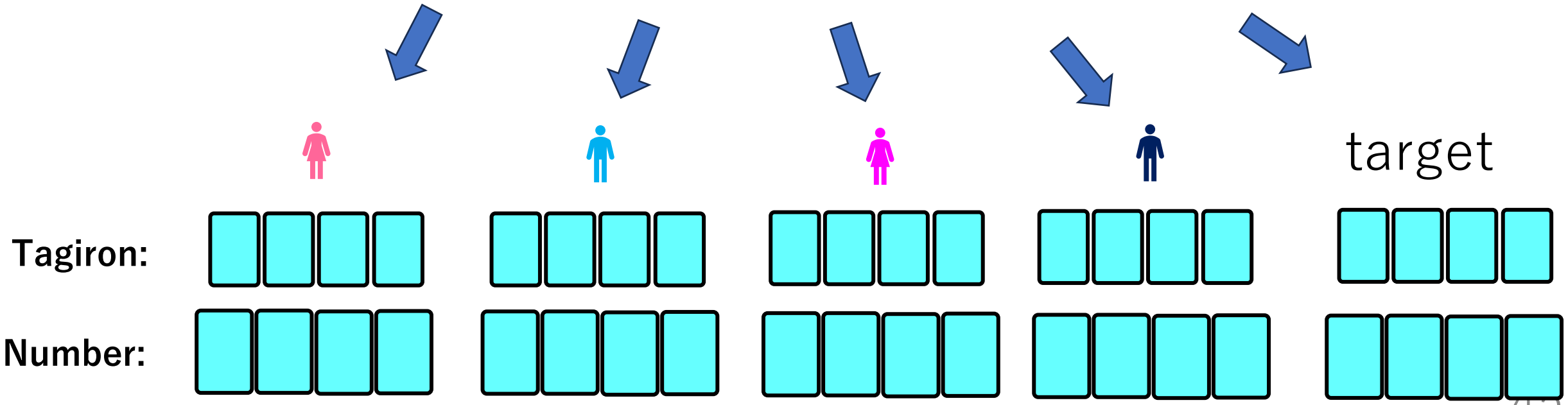


Correspondence

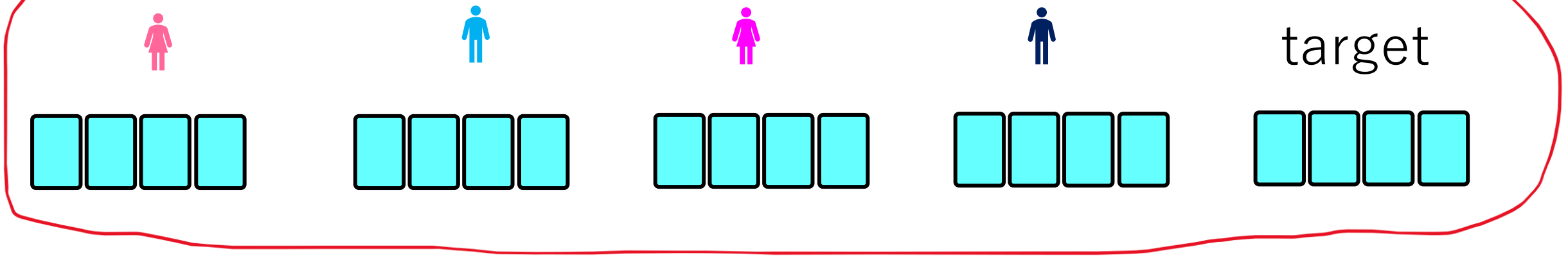
0	0	1	1	2	2	3	3	4	4	5	5	6	6	7	7	8	8	9	9
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

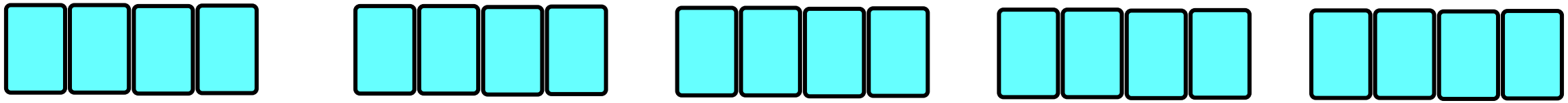
Tagiron cards along with number cards are distributed:





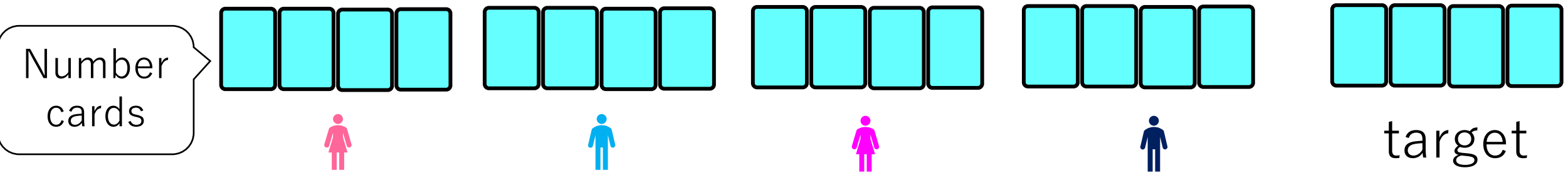
Tagiron cards are used as in a normal game:



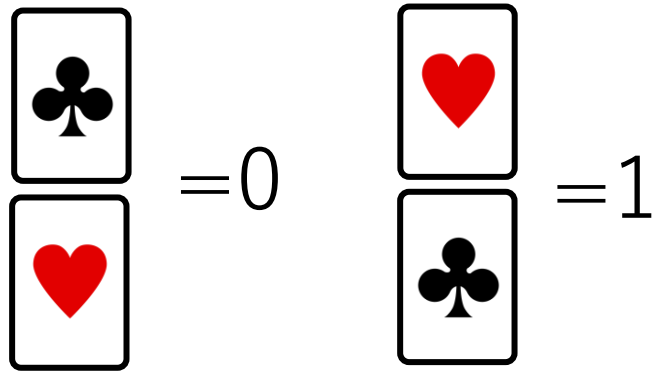


Number cards are used in the preprocessing protocol and challenge protocol

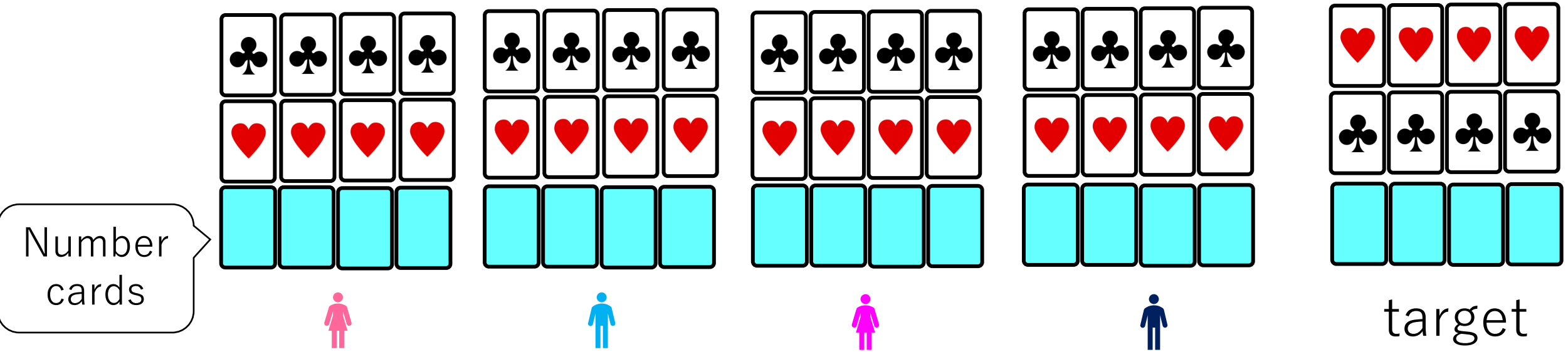
Preprocessing protocol



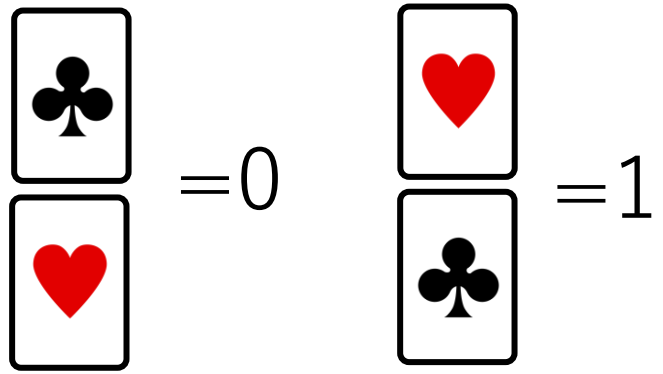
Preprocessing protocol



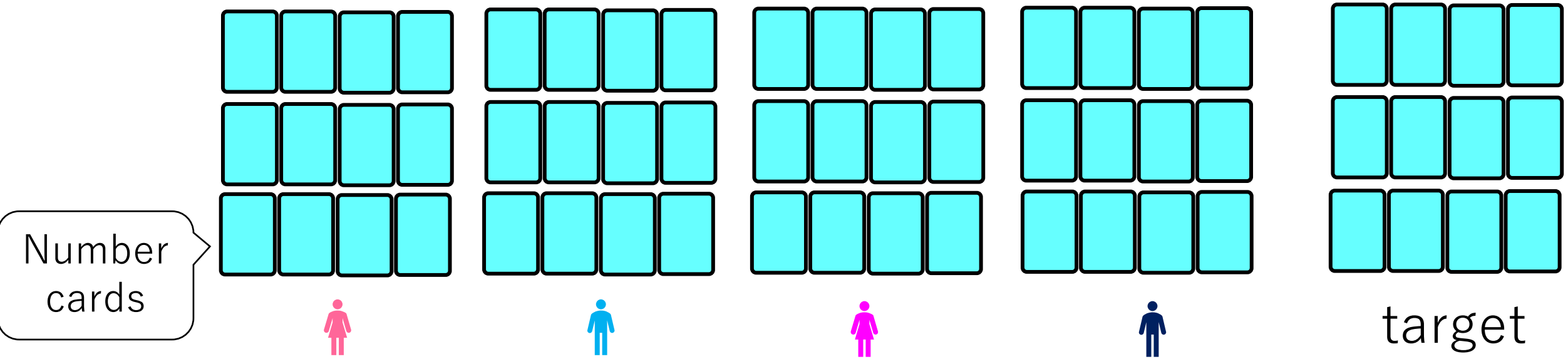
Place 0 above players' cards, and 1 above the target cards:



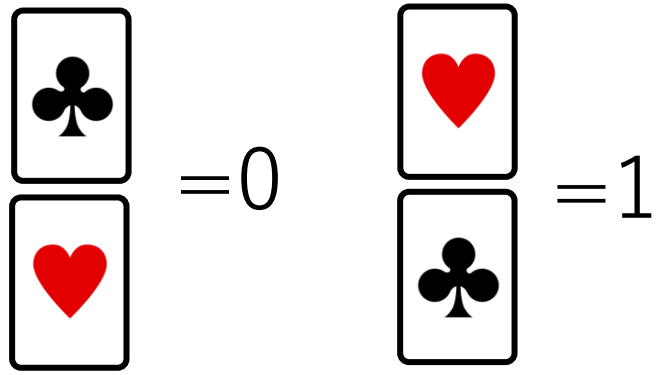
Preprocessing protocol



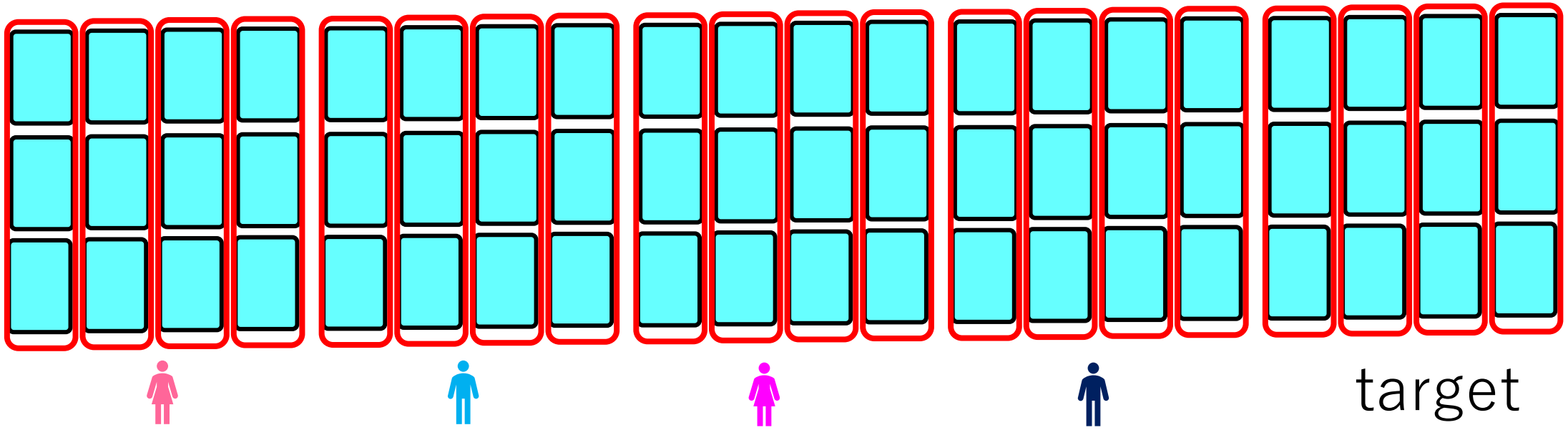
Turn over all face-up cards:



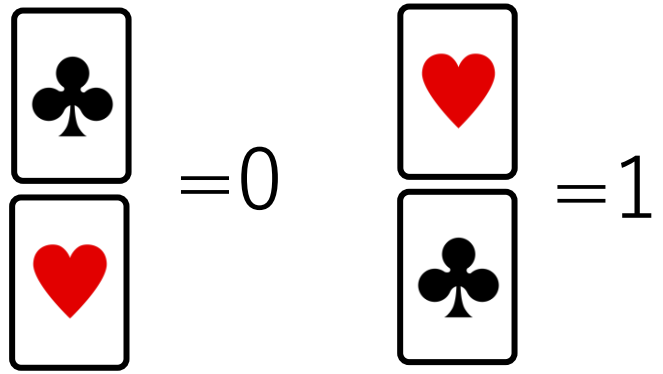
Preprocessing protocol



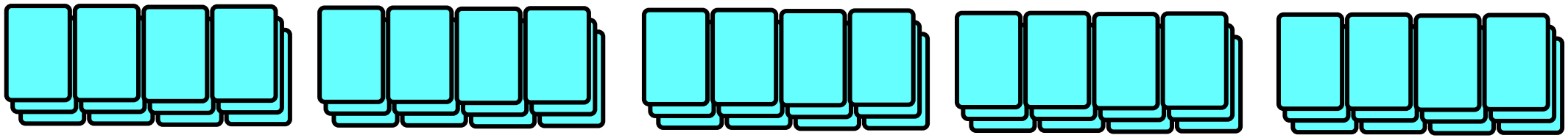
Make 3-card piles:



Preprocessing protocol



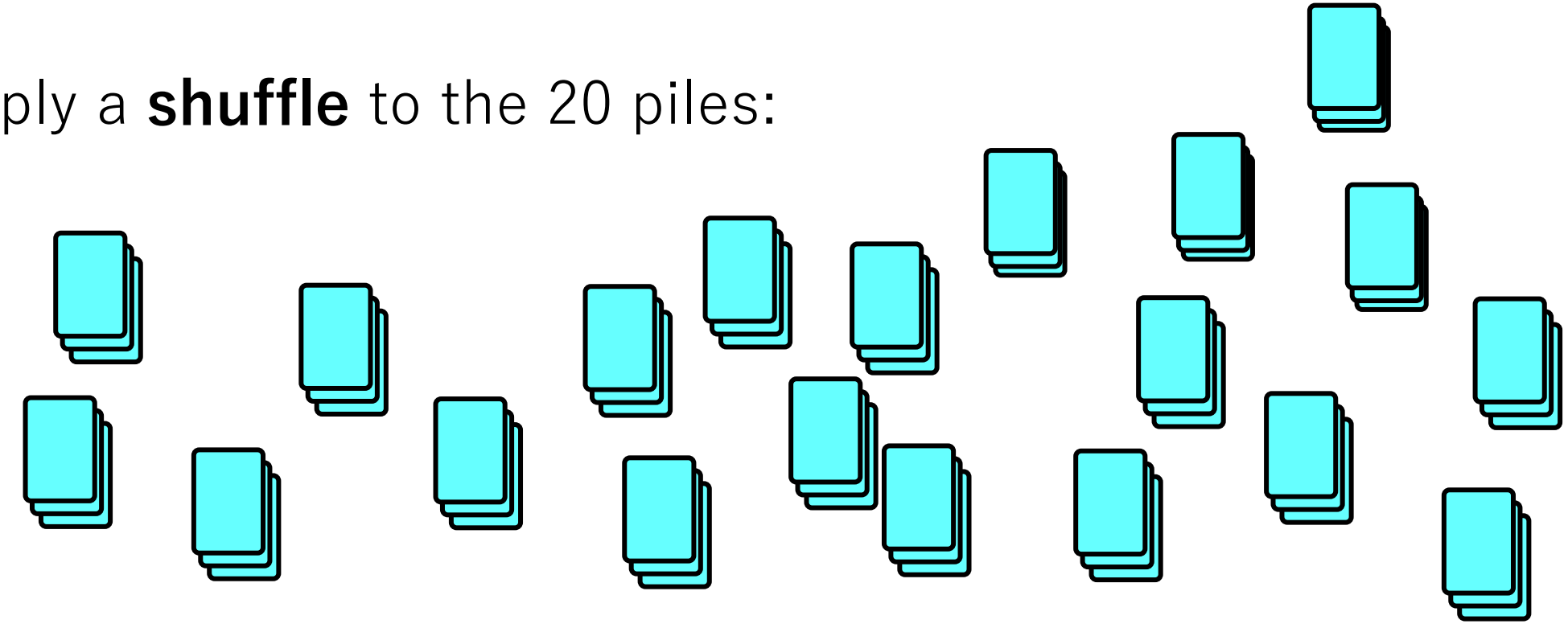
Make 3-card piles:



target

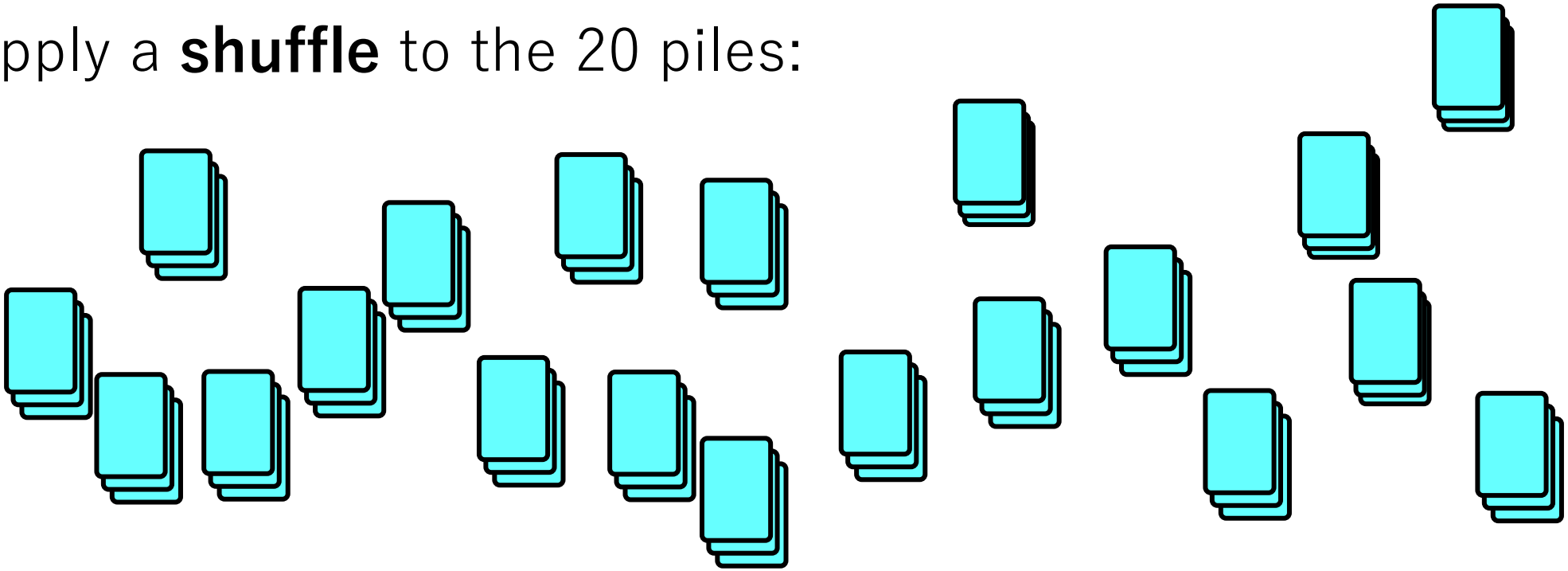
Preprocessing protocol

Apply a **shuffle** to the 20 piles:



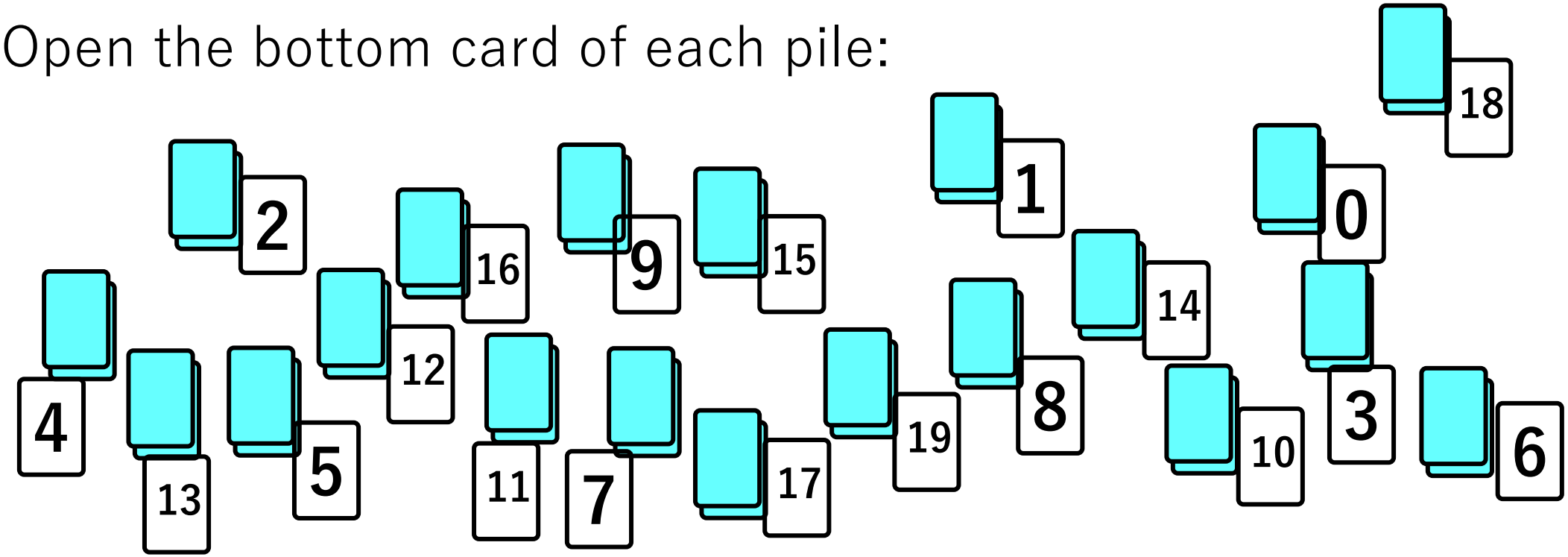
Preprocessing protocol

Apply a **shuffle** to the 20 piles:



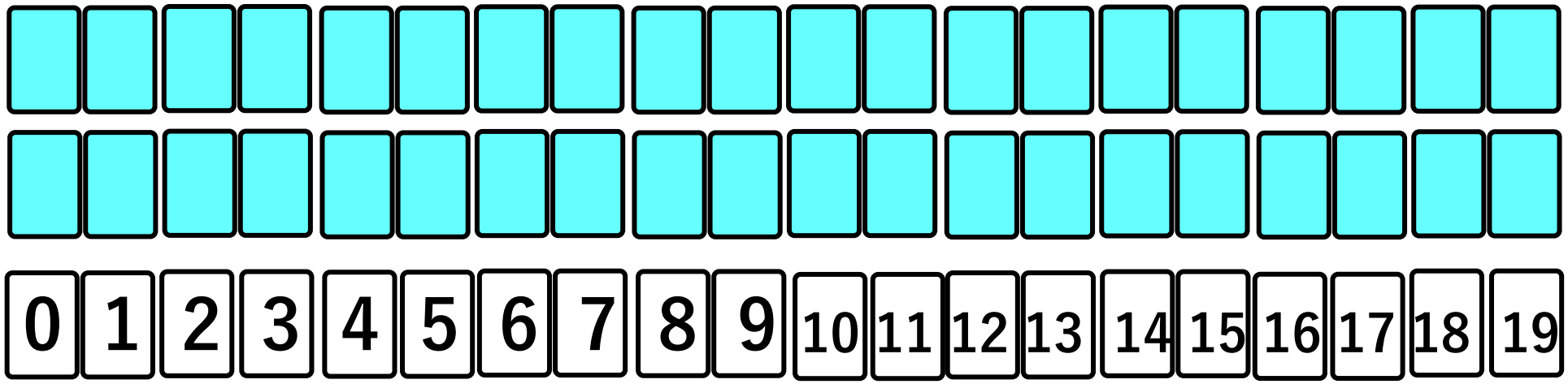
Preprocessing protocol

Open the bottom card of each pile:

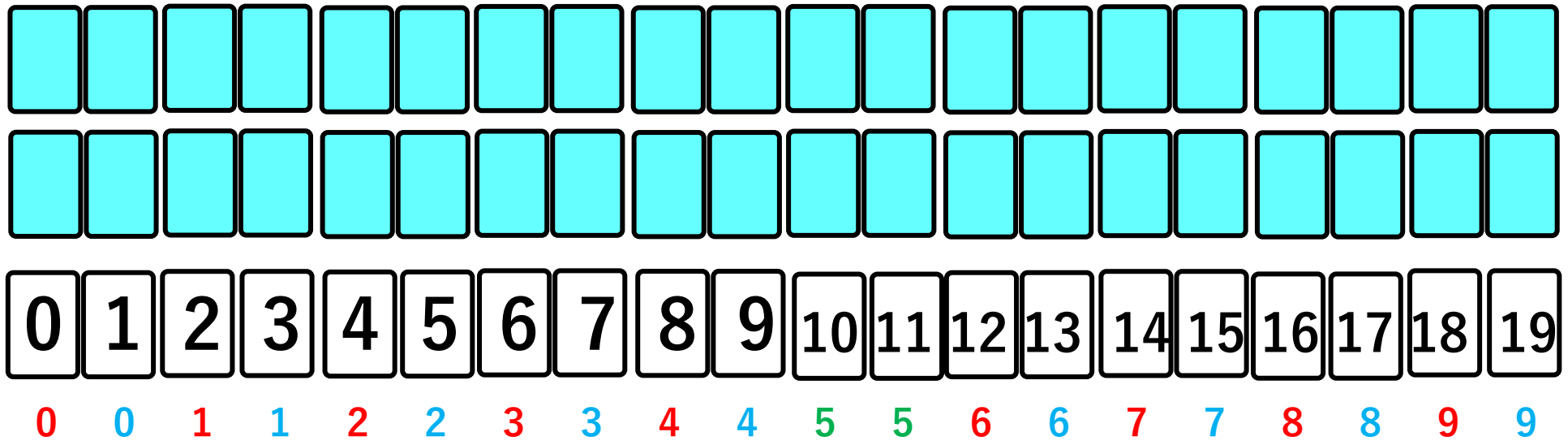


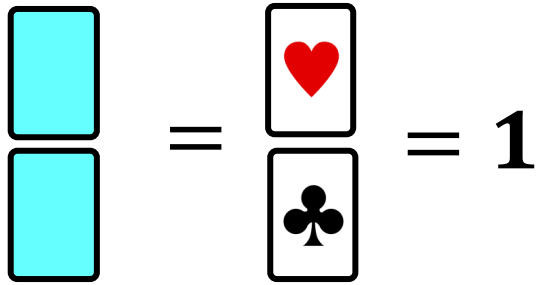
Preprocessing protocol

Sort the piles based on the bottom cards:

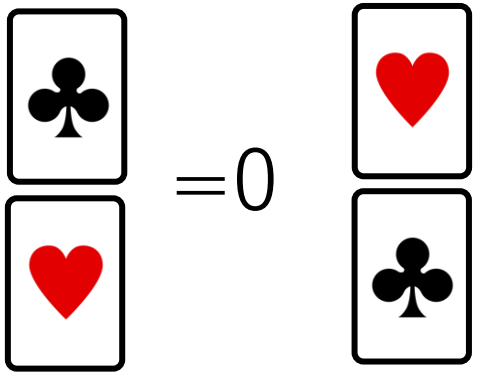


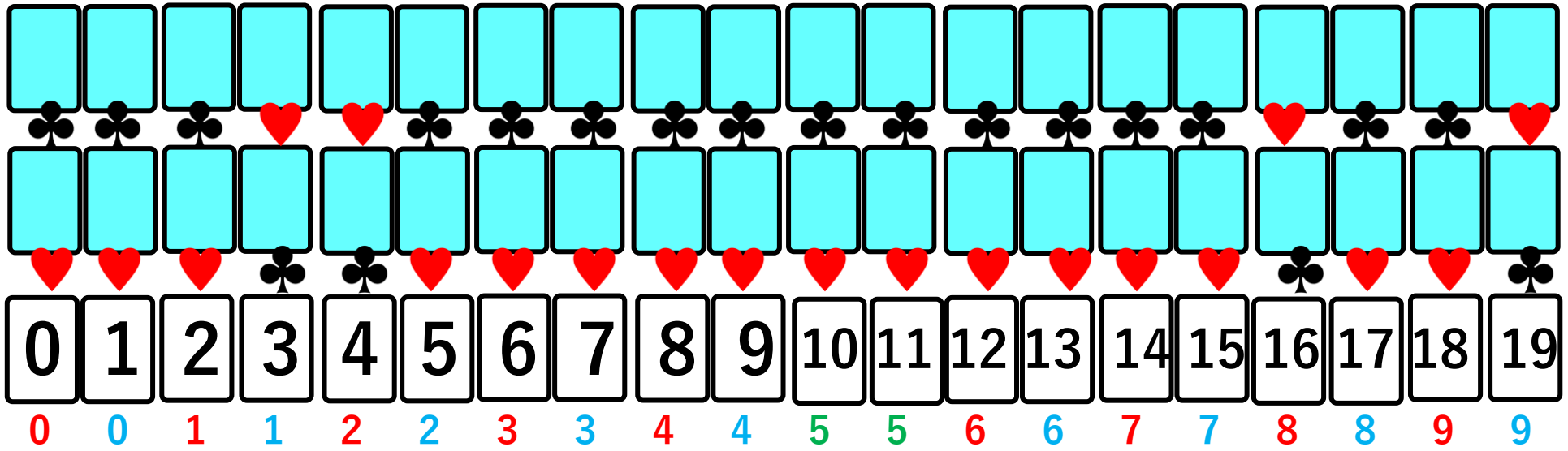
Preprocessing protocol



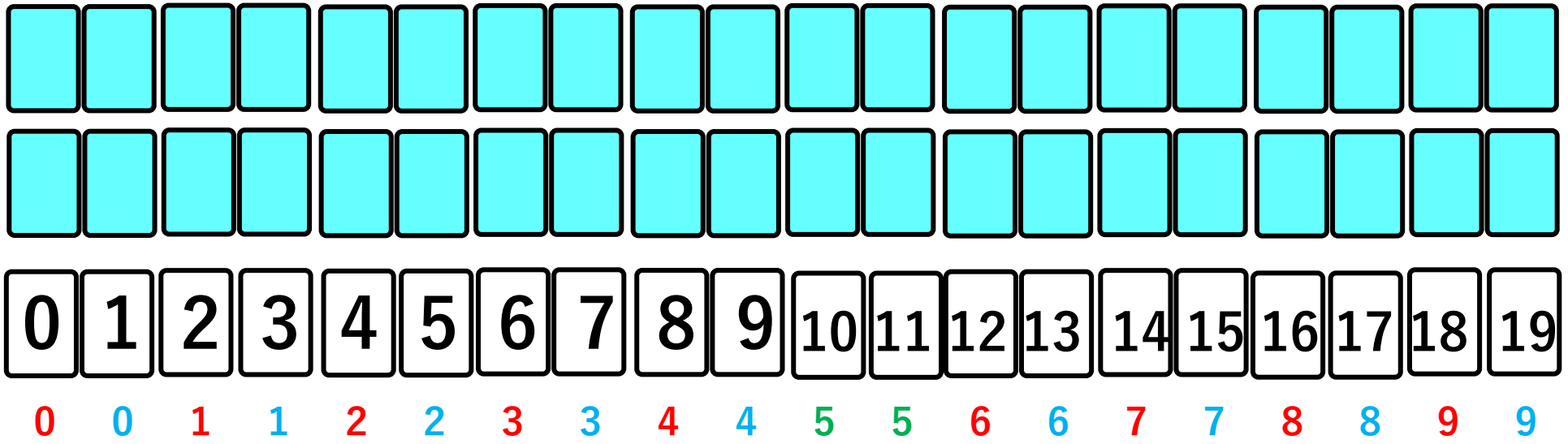
target card $\Leftrightarrow$  $= 1$

For example, if target cards are 2 1 9 8





Preprocessing protocol



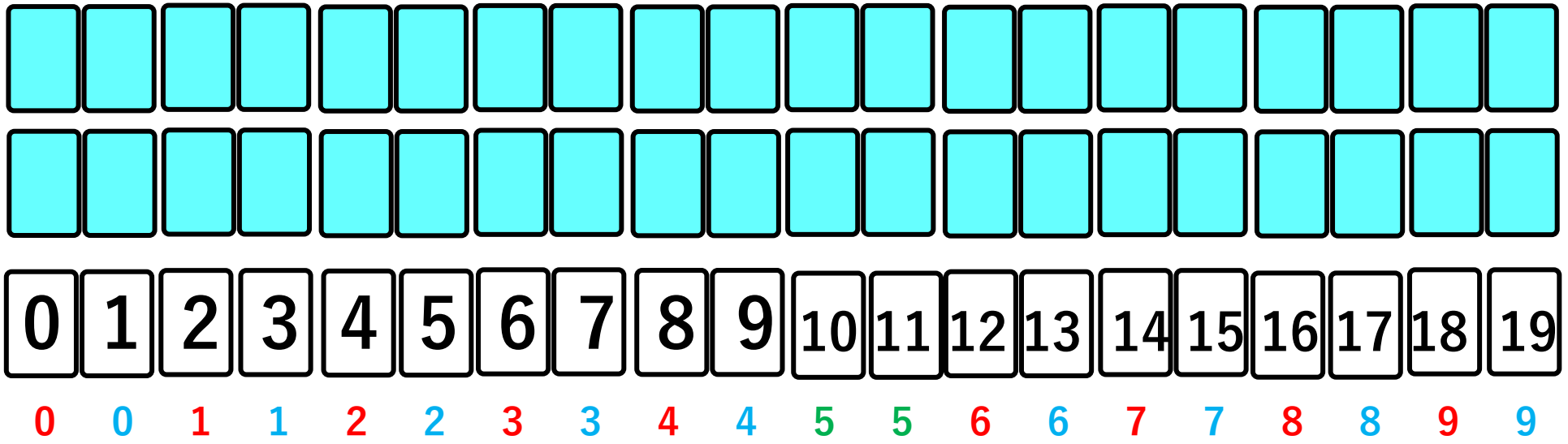
target card $\Leftrightarrow$ $= = \mathbf{1}$

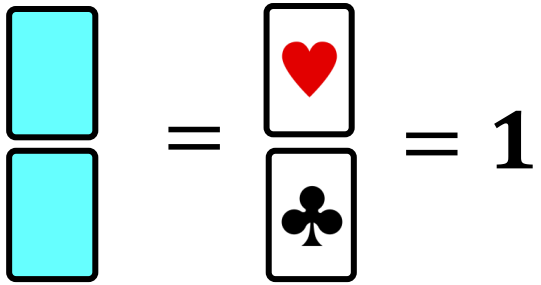
This is the preprocessing protocol.

(Here, we omit the steps for handling two green cards)

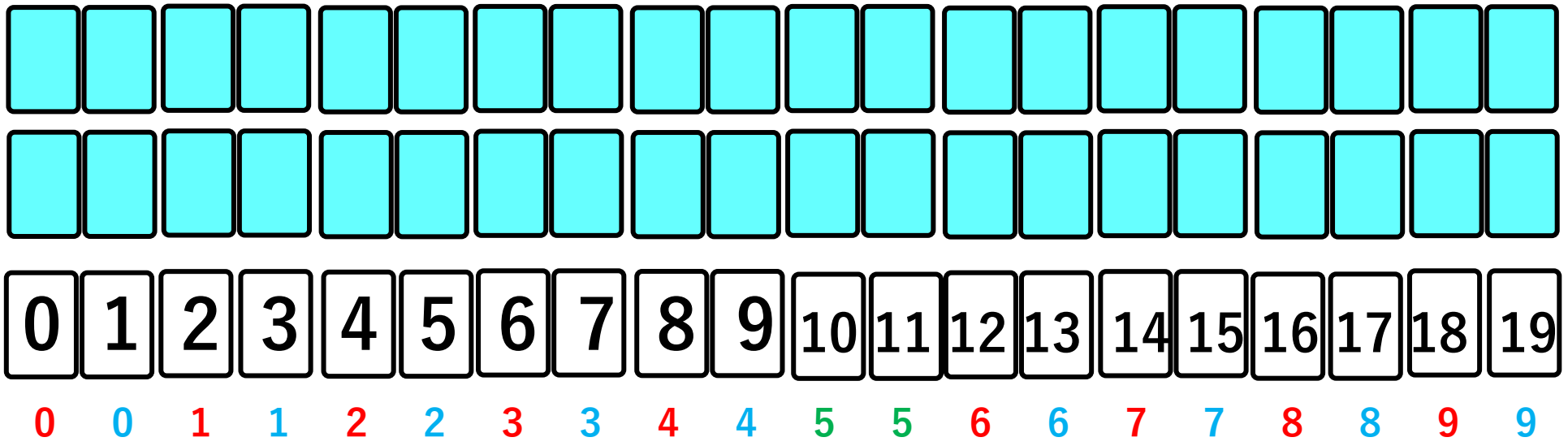
Table of Contents

By the preprocessing protocol, we have:

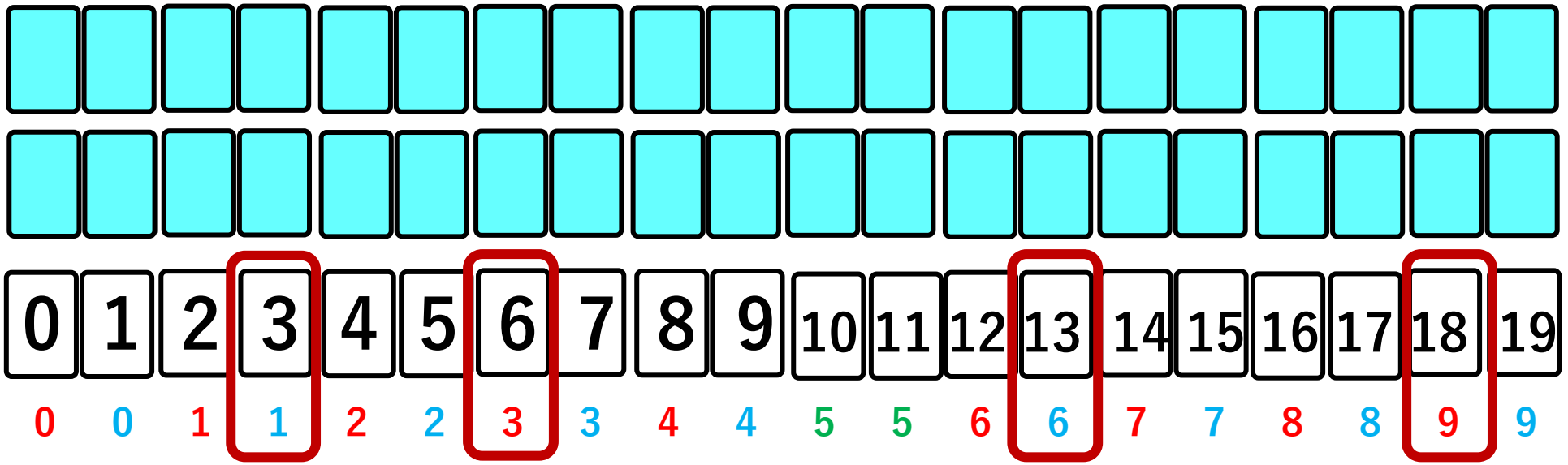


target card $\Leftrightarrow$  $= 1$

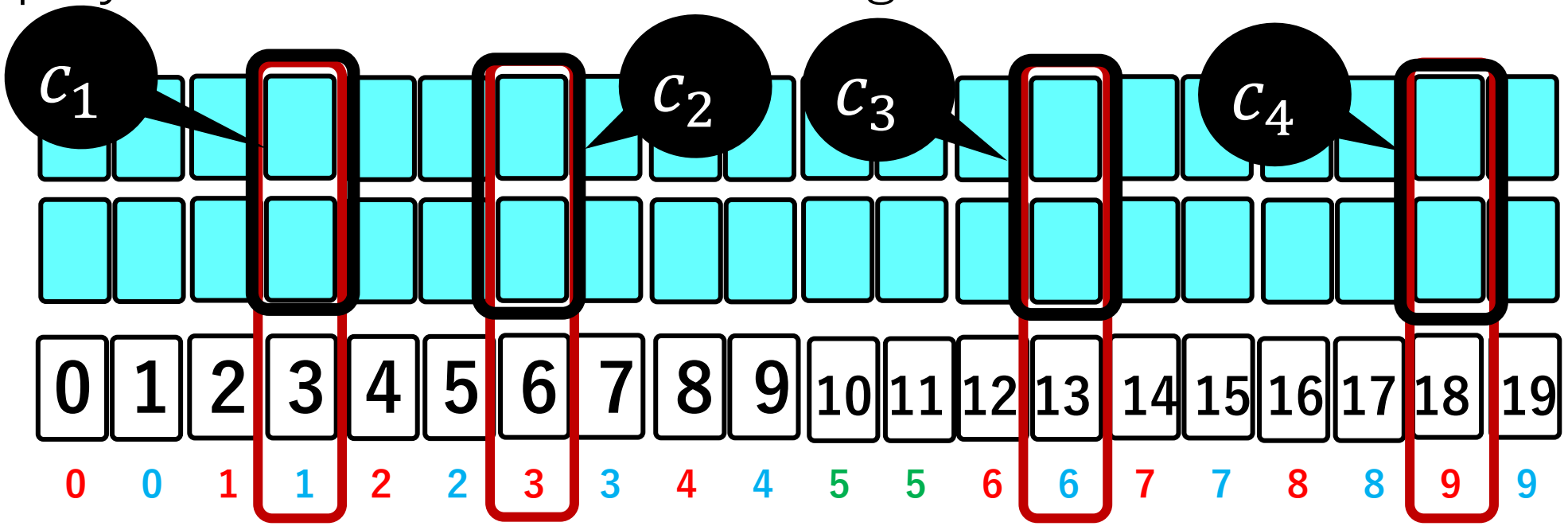
A player wants to make a challenge:

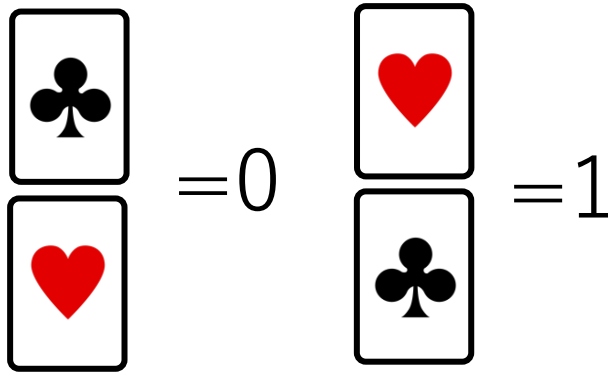


A player wants to make a challenge:

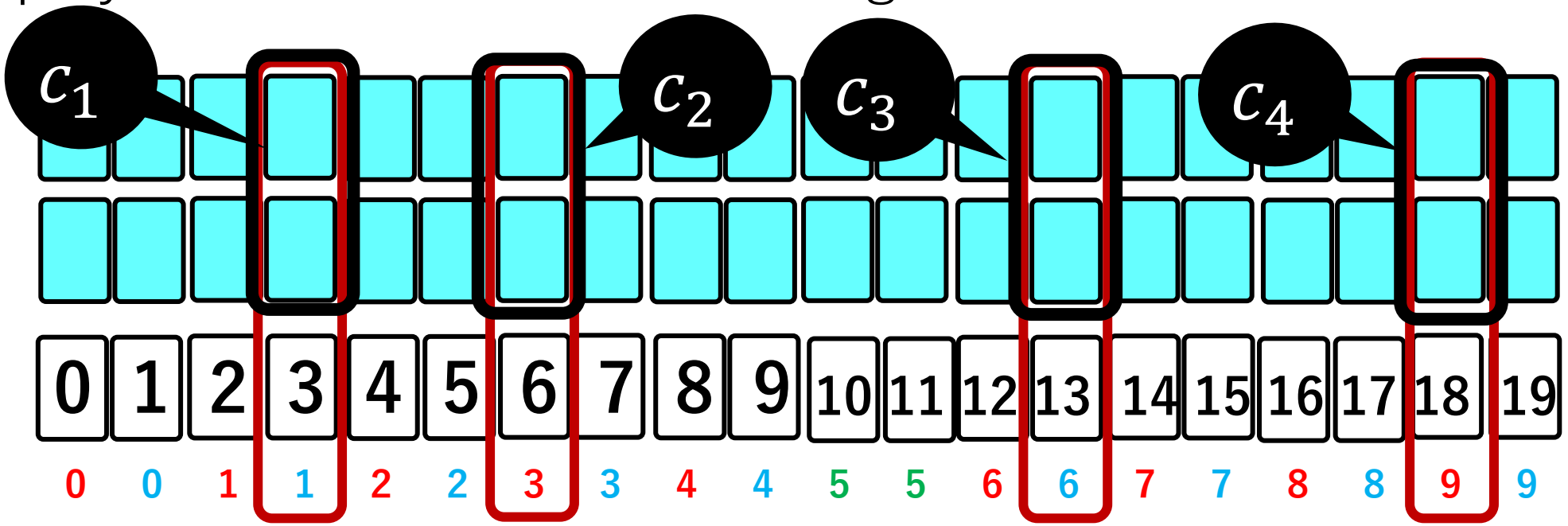


A player wants to make a challenge:



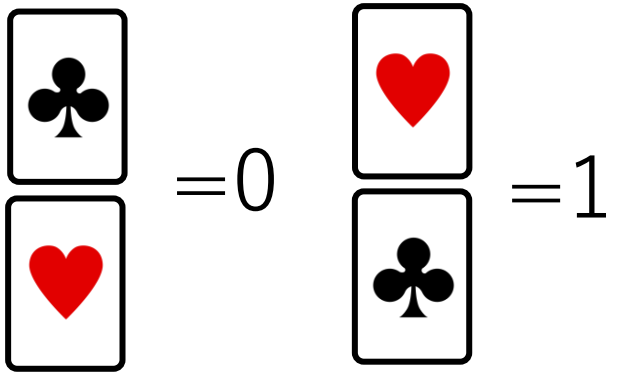


A player wants to make a challenge:

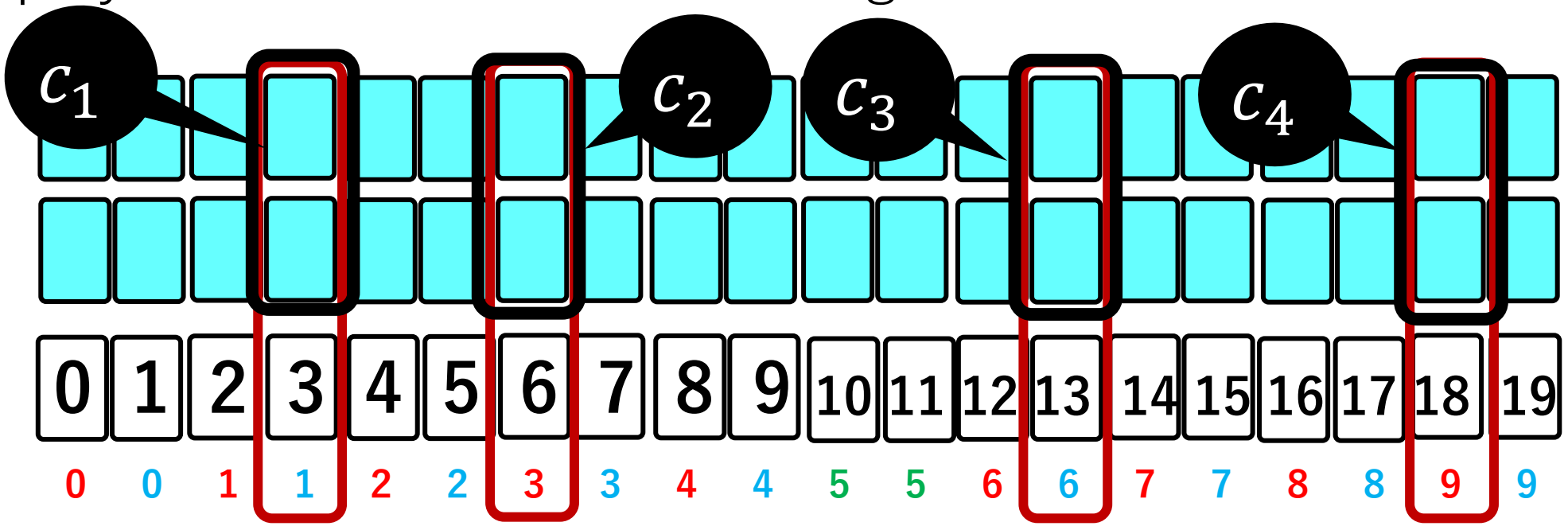


guess is correct

$$c_1 = c_2 = c_3 = c_4 = 1$$



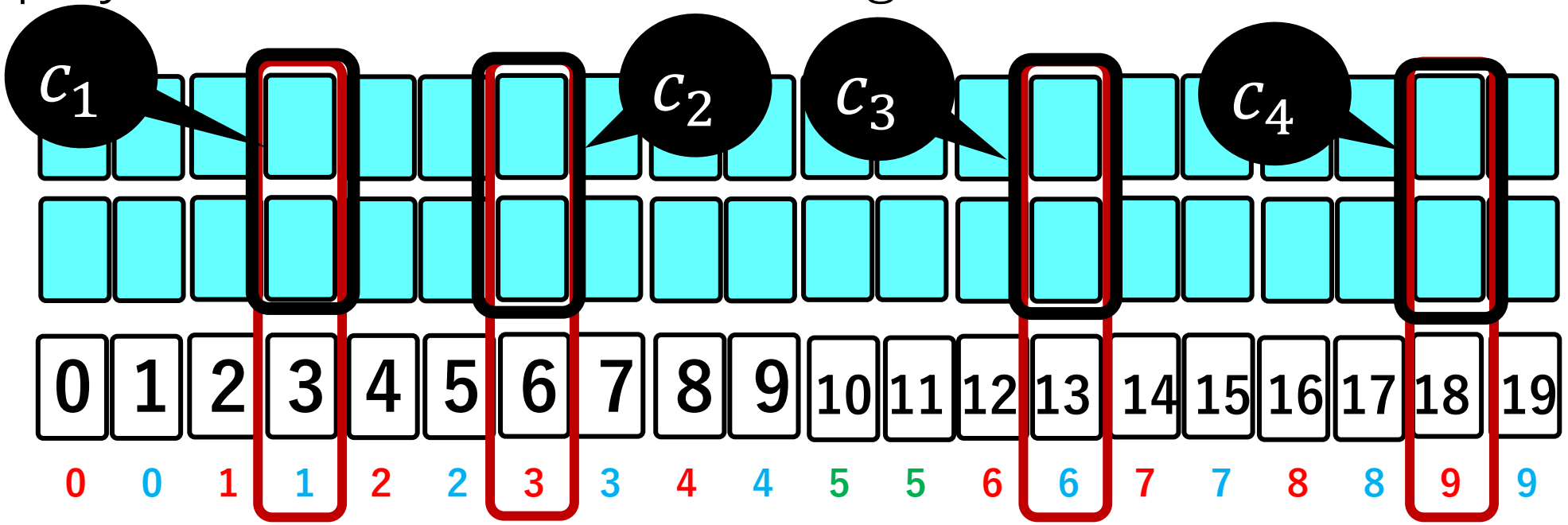
A player wants to make a challenge:



$c_1 \wedge c_2 \wedge c_3 \wedge c_4 = 1$ ⇒ **success**

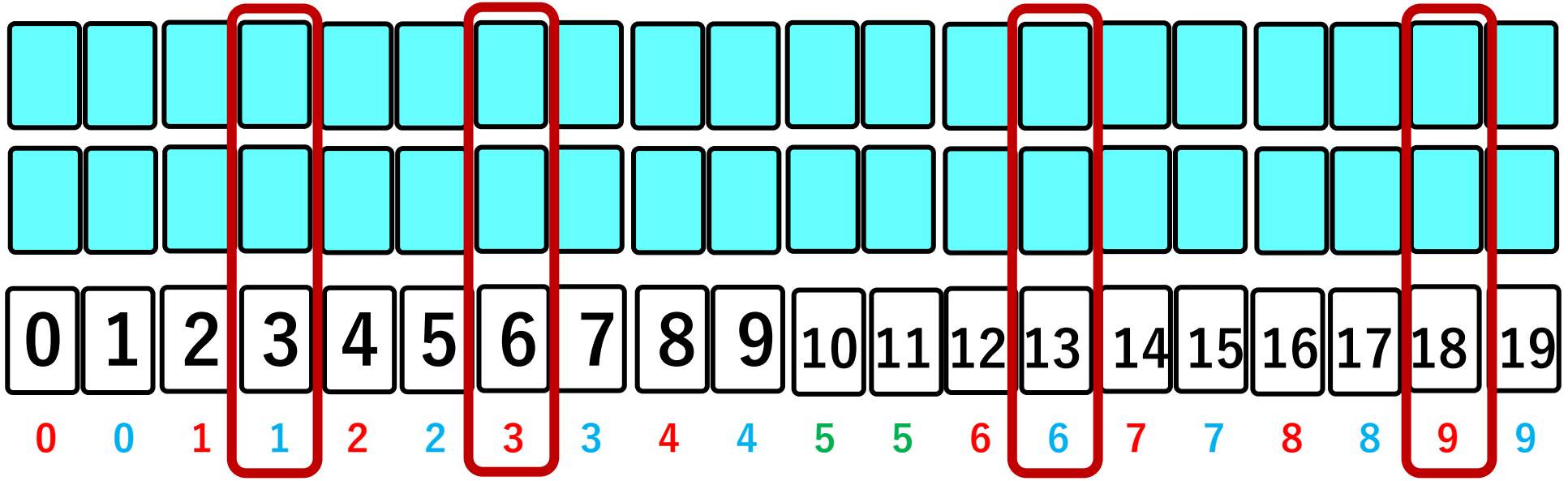
$c_1 \wedge c_2 \wedge c_3 \wedge c_4 = 0$ ⇒ **failure**

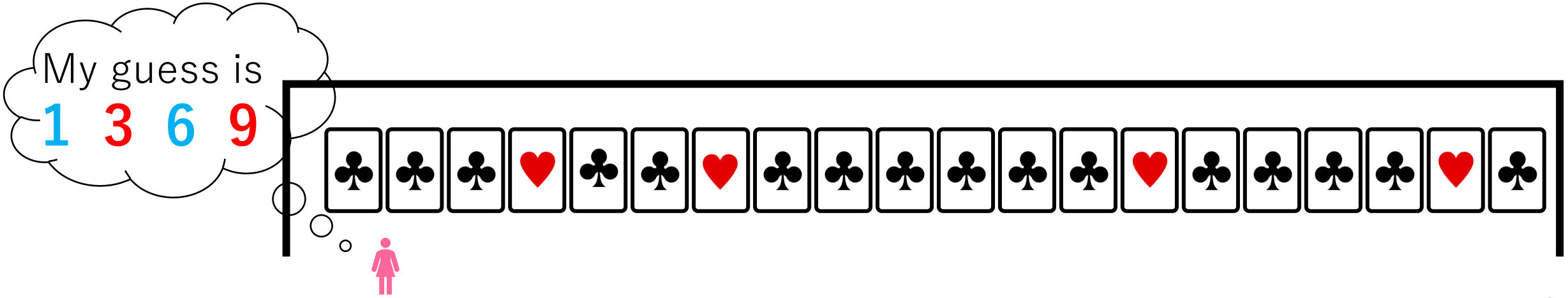
A player wants to make a challenge:



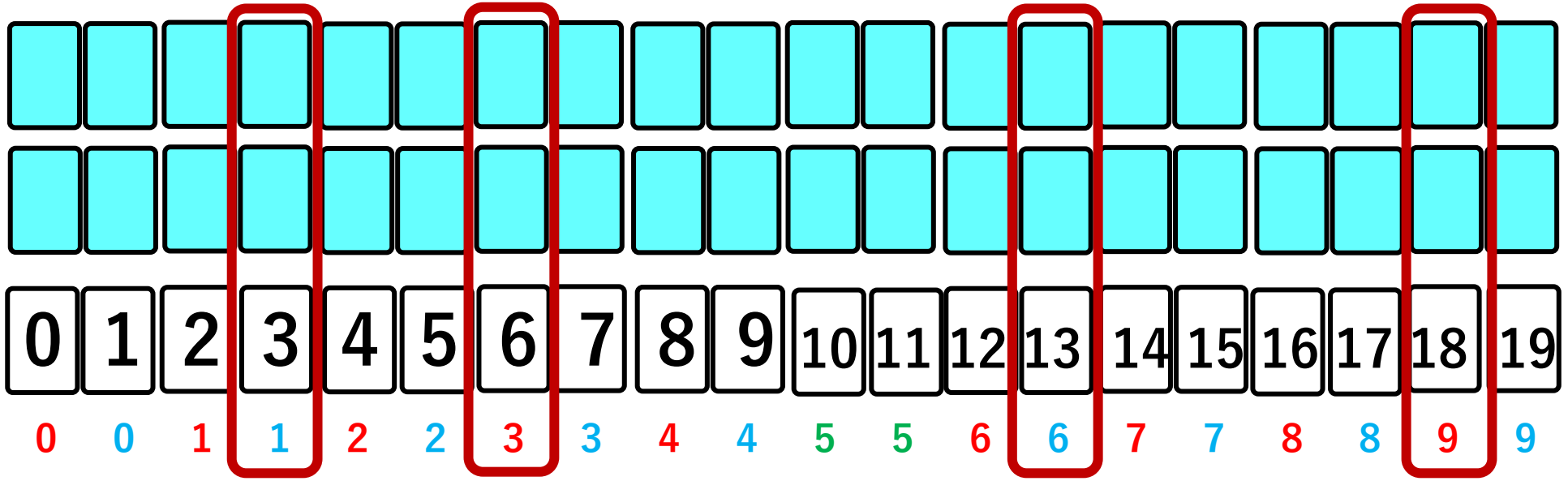
How to secretly select the 4 commitments corresponding to the guess?

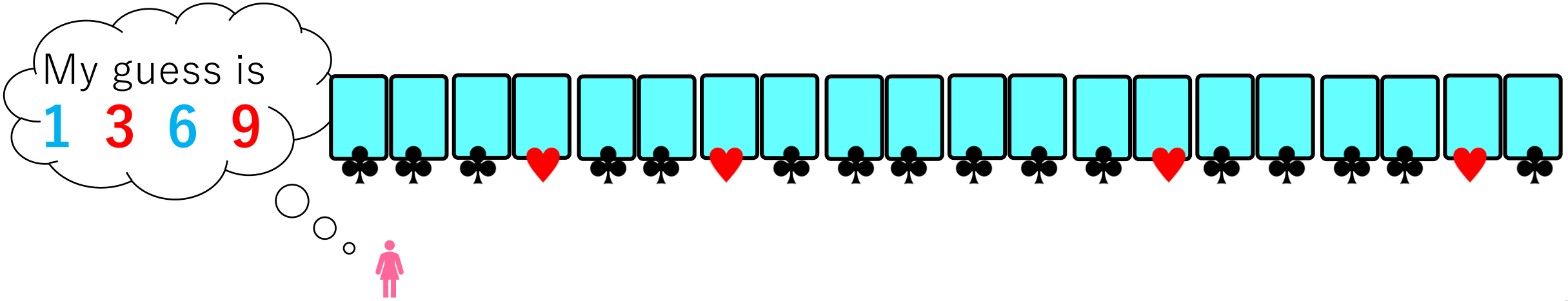
Challenge protocol



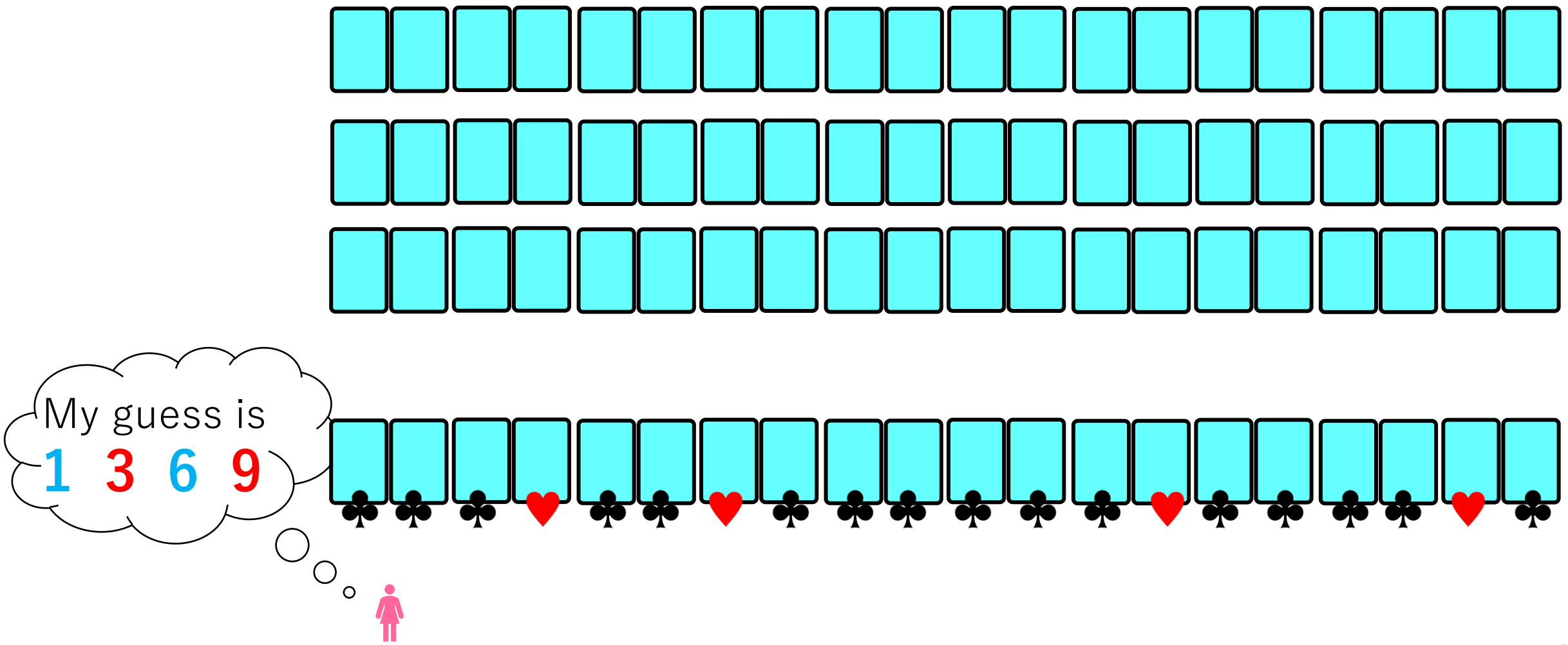


Challenge protocol

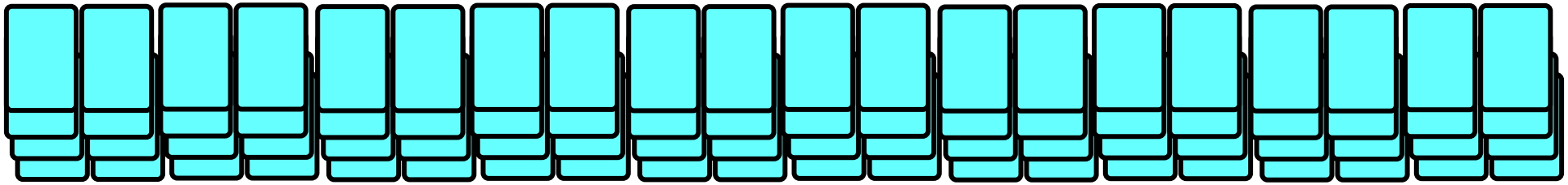




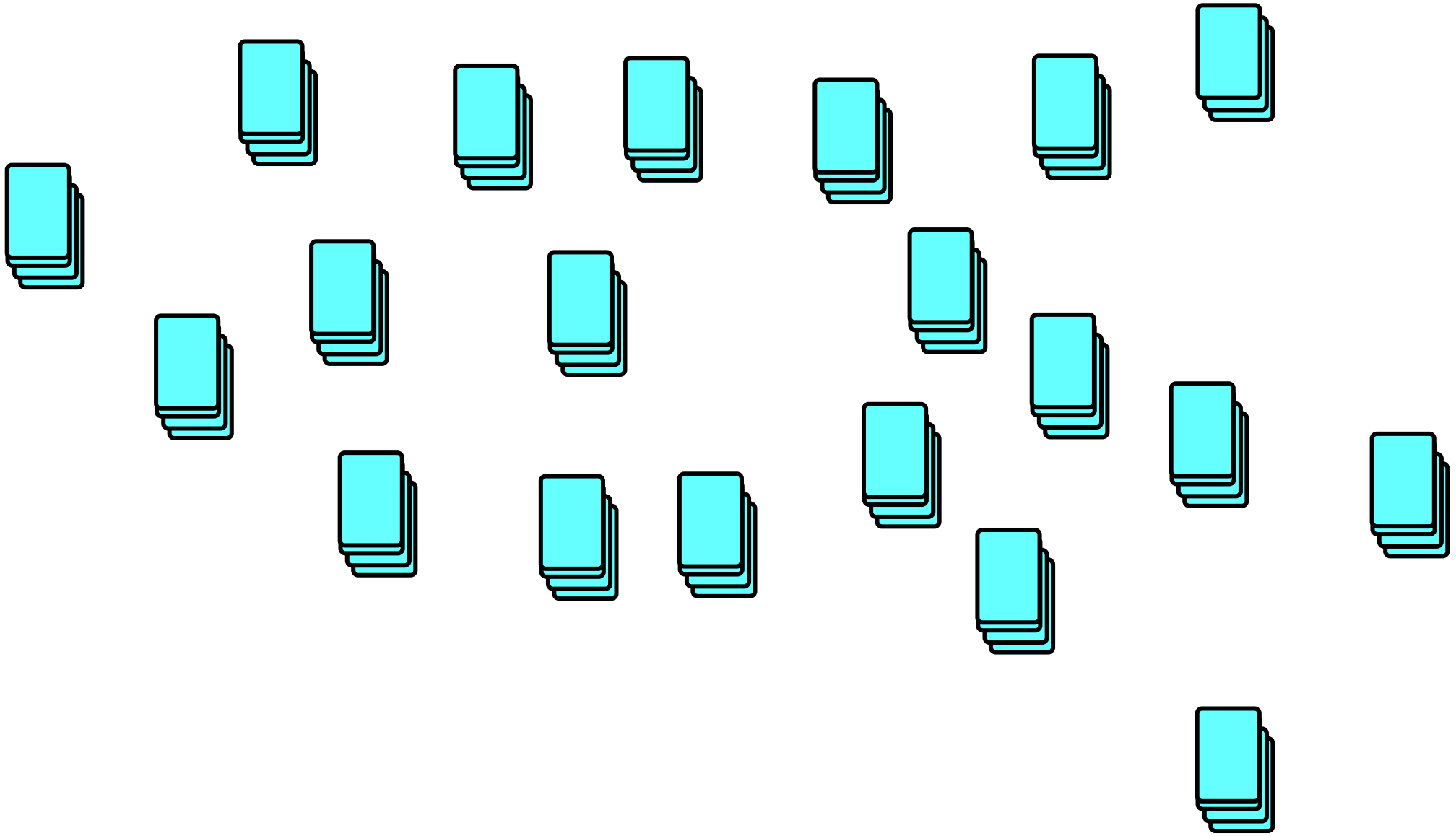
Challenge protocol



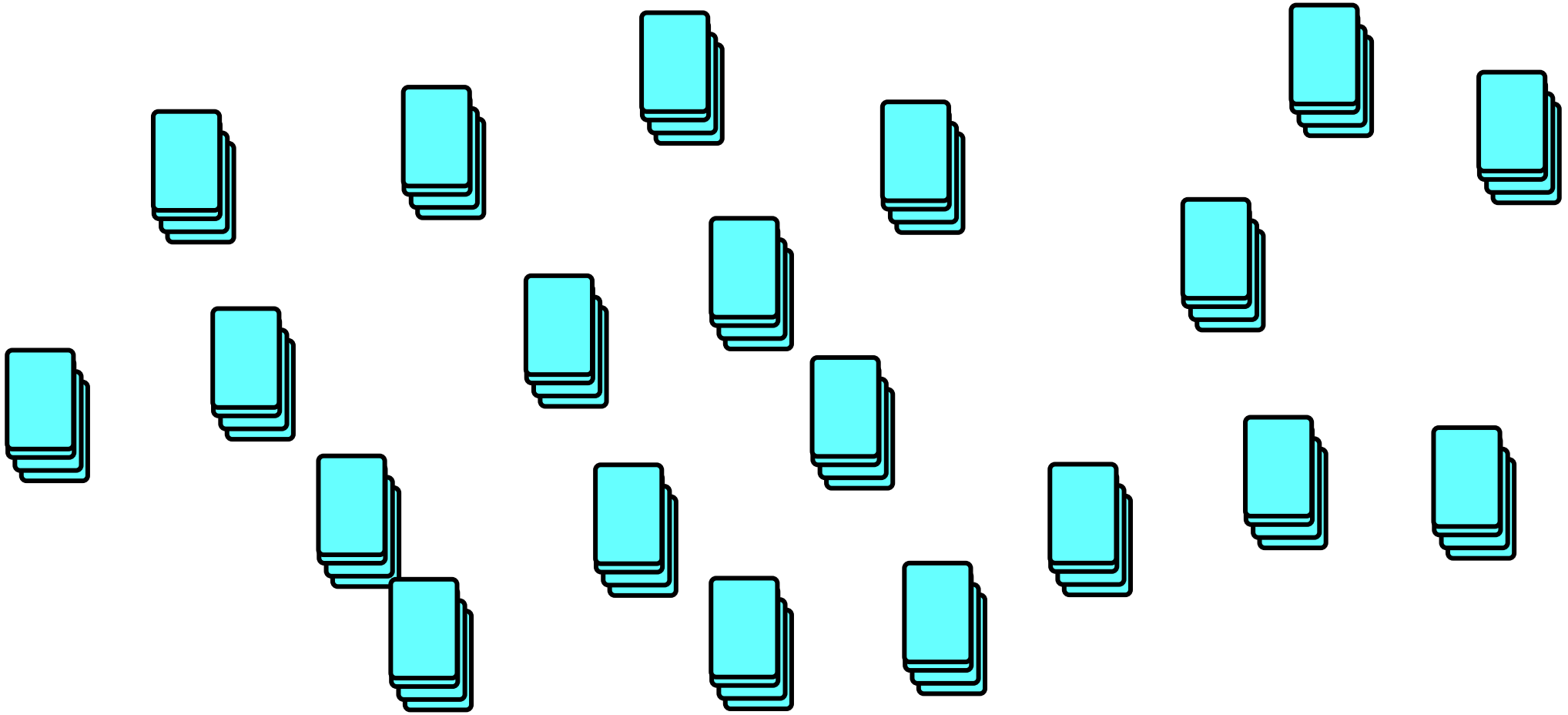
Challenge protocol



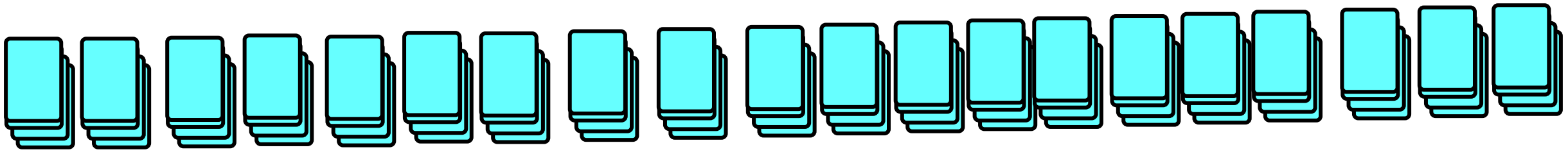
Challenge protocol



Challenge protocol

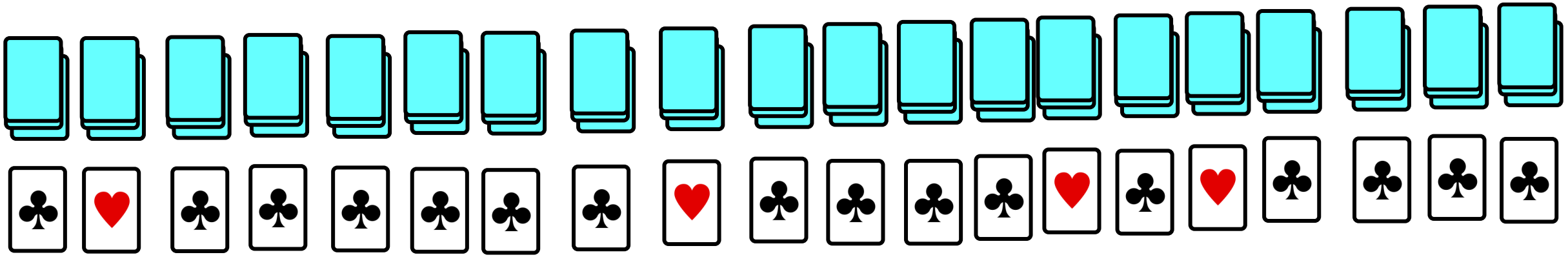


Challenge protocol

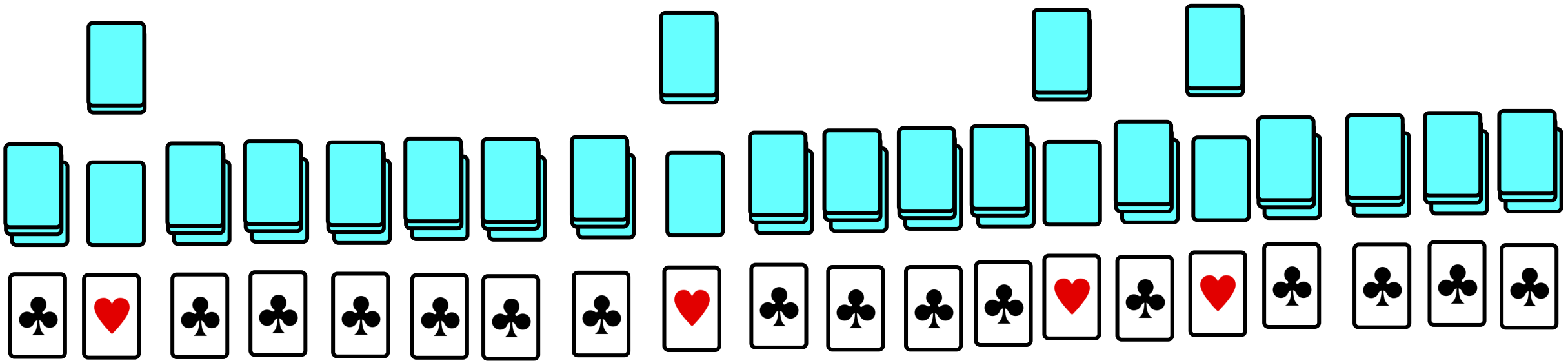


Challenge protocol

Open the bottom cards

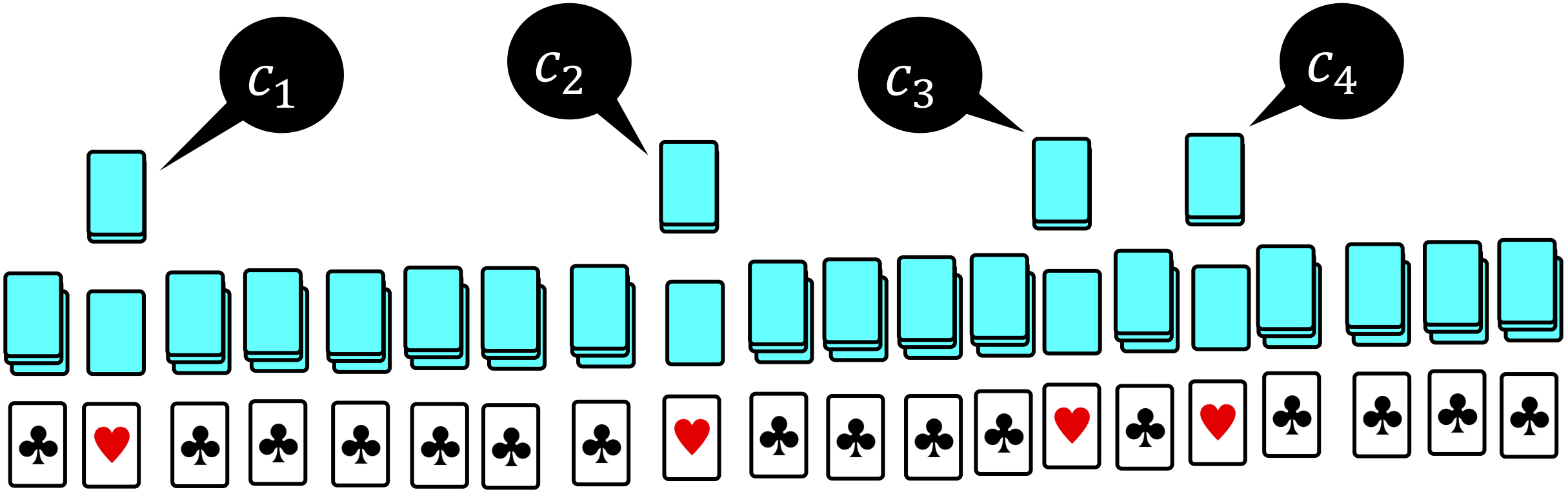


Challenge protocol

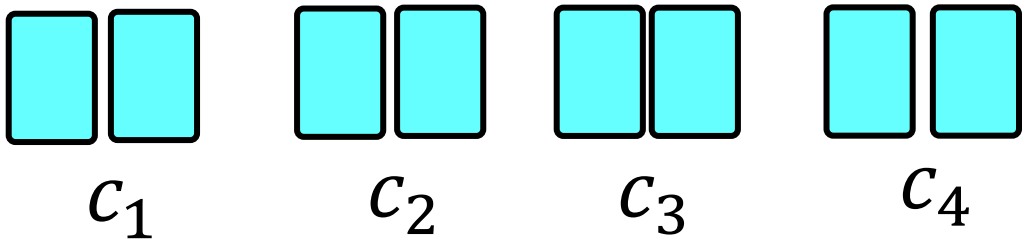


The cards above each ♥ correspond to her guess

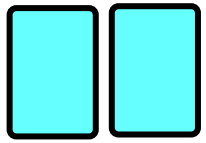
Challenge protocol



Challenge protocol



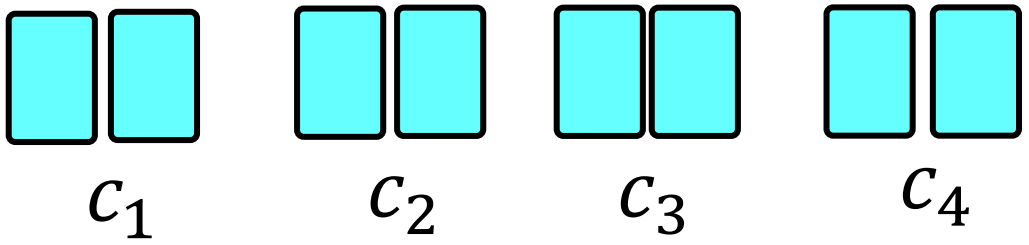
(Variants of) the AND protocol

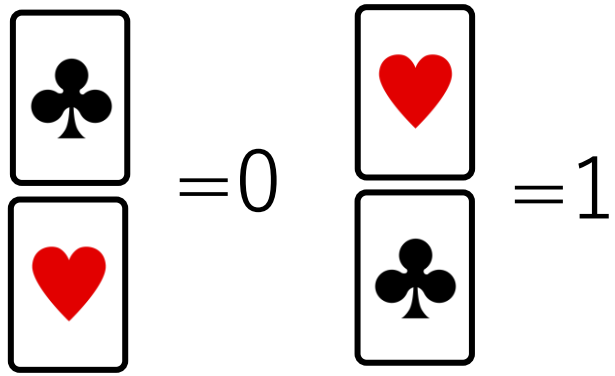


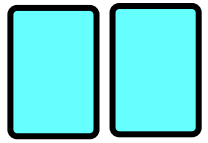
$c_1 \wedge c_2 \wedge c_3 \wedge c_4$

We also make copies here; see Step 4 in Section 3.3.

Challenge protocol

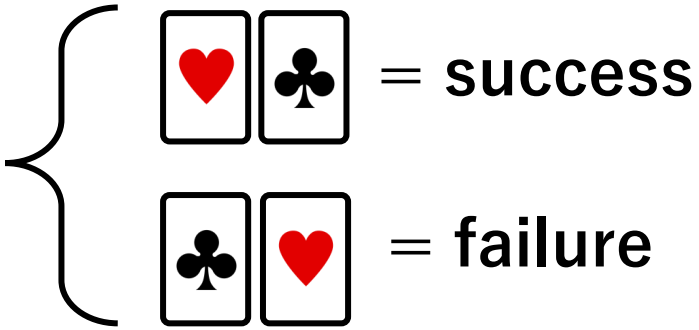






$c_1 \wedge c_2 \wedge c_3 \wedge c_4$

Open



We can only know whether
the challenge succeeds or not

Table of Contents

Conclusion

- We apply card-based cryptography to enhancing the gameplay of Tagiron.
- Useful tool to promote intuitive understanding of secure computations.
- The number of cards used in our method is not small, and further optimization is future work.