# Five-Card Secure Computations Using Unequal Division Shuffle

Akihiro Nishimura[1], Takuya Nishida[1], Yu–ichi Hayashi[2], Takaaki Mizuki[3], and Hideaki Sone[3]

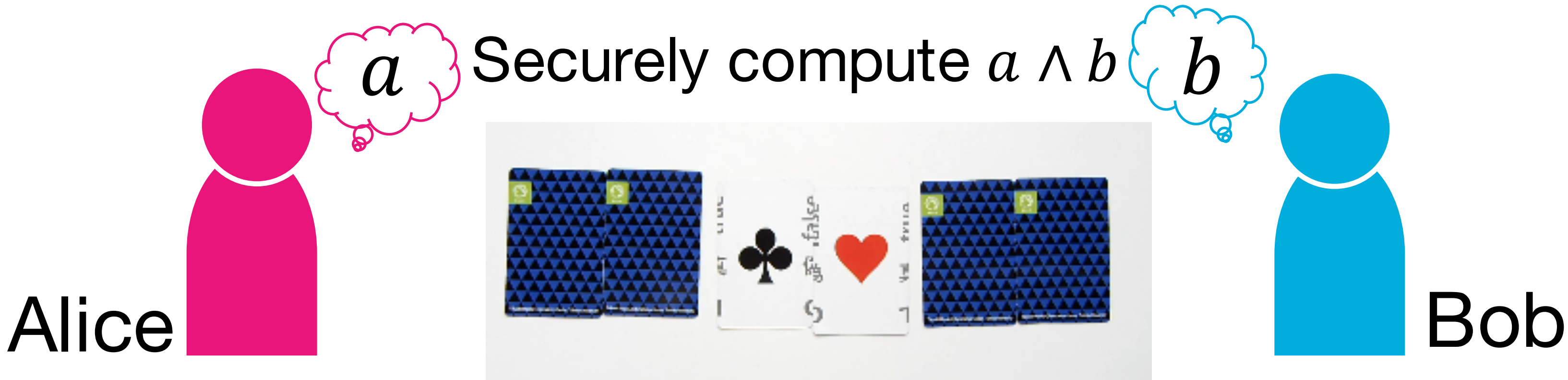
1 Sone-Mizuki Laboratory, Graduate School of Information Sciences, Tohoku University
2 Faculty of Engineering, Tohoku Gakuin University
3 Cyberscience Center, Tohoku University

TPNC2015 December, 16 10:45~11:10

# Index

# 1.1 Introduction

Suppose that Alice and Bob have Boolean values $a \in \{0,1\}$ and $b \in \{0,1\}$, and they want to conduct secure AND computation.




| Protocol | # of cards | Shuffle |
|---|---|---|
| Six-card AND [6] | 6 | Random Bisection Cut |

[6]Mizuki, T., Sone, H. Six-card secure AND and four-card secure XOR. Frontiers in Algorithmics, LNCS, vol. 5598, pp.358-369. Springer Berlin Heidelberg (2009)

# AND Protocols

| Protocol | # of cards | Shuffle | Failure rare |
|---|---|---|---|
| Six-card AND [6] | 6 | Random Bisection Cut | 0% |
| Cheung's AND [2] | 5 | Unequal Division Shuffle | 50% |

[2]Eddie Cheung, Chris Hawthorne, and Patrick Lee, CS 758 project: secure computation with playing cards, http://csclub.uwaterloo.ca/~cdchawth/static/secure_playing cards.pdf, 2013. (last visitedJune 22, 2015)

# AND Protocols

| Protocol | # of cards | Shuffle | Failure rare |
|---|---|---|---|
| Six-card AND [6] | 6 | Random Bisection Cut | 0% |
| Cheung's AND [2] | 5 | Unequal Division Shuffle | 50% |
| Ours | 5 | Unequal Division Shuffle | 0% |

# Copy Protocols

| Protocol | # of cards | Shuffle | Avg. # of trials |
|---|---|---|---|
| Six-card Copy [6] | 6 | Random Bisection Cut | 1 |
| Ours | 5 | Unequal Division Shuffle | 2 |

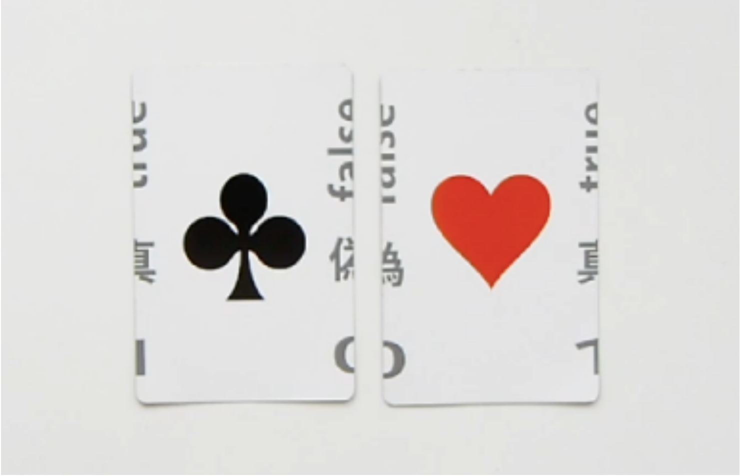
## The Cards' Properties

1. All cards of the same type are indistinguishable from one another.
2. Each card has the same pattern on its back side.

# 1.2 Preliminary Notations

## Encoding Scheme

$$0 = \boxed{\clubsuit}\,\boxed{\heartsuit} \quad 1 = \boxed{\heartsuit}\,\boxed{\clubsuit}$$

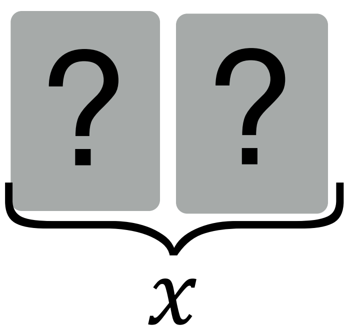


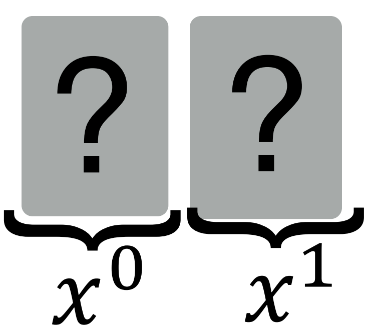
# 1.2 Preliminary Notations

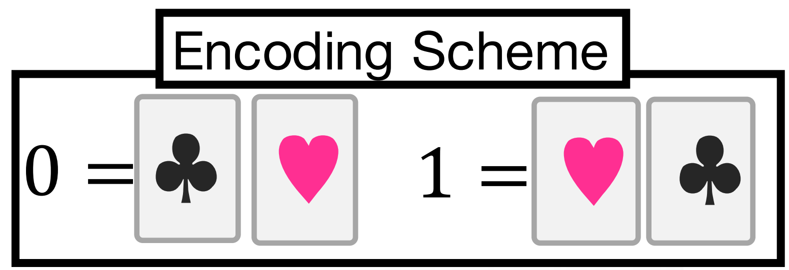
## Commitment

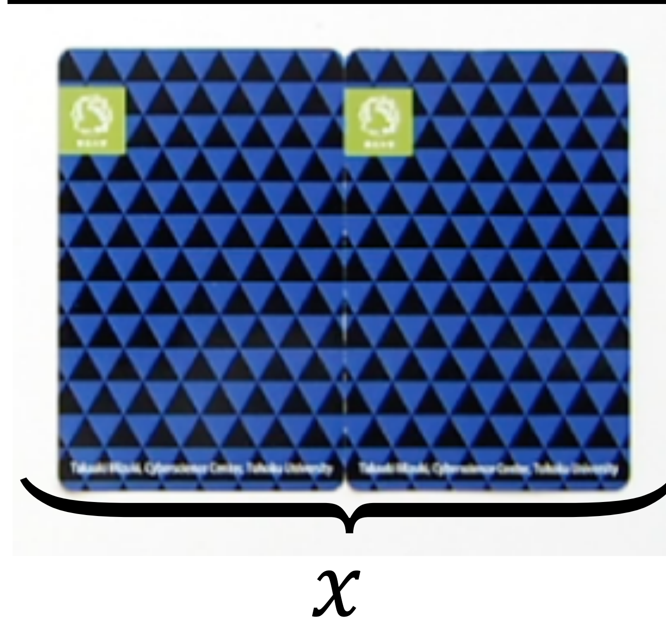
A pair of face-down cards which describes the value of $x \in \{0,1\}$ with the encoding scheme.

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



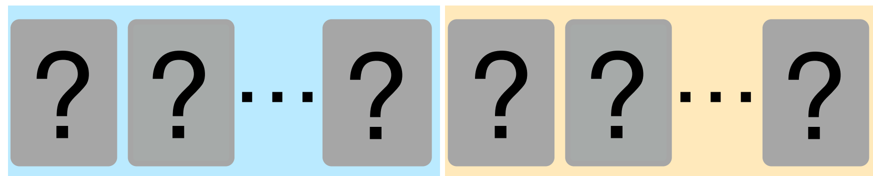



# Index

1. Introduction
2. Card Shuffling Operations and Known Protocol
3. Improved Cheung's AND Protocol
4. Five-Card Copy Protocols
5. Conclusion

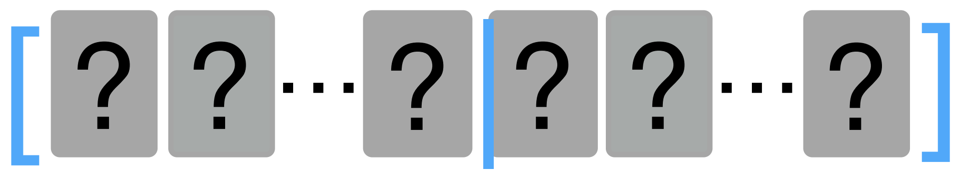
# 2.1 Bisection Cut

Suppose that there is a sequence of $2m$ face-down cards.



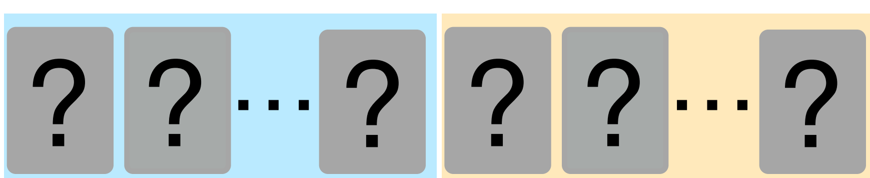
$m$ cards $m$ cards

Bisect the sequence and randomly switch the two portions.

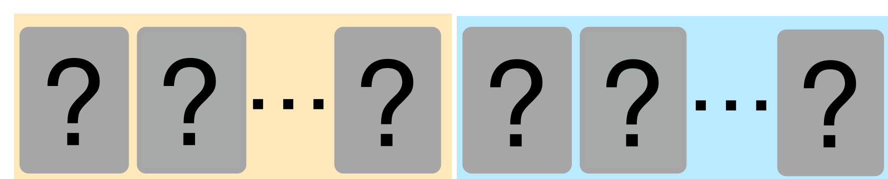


$m$ cards $m$ cards

The result of the operation will be either



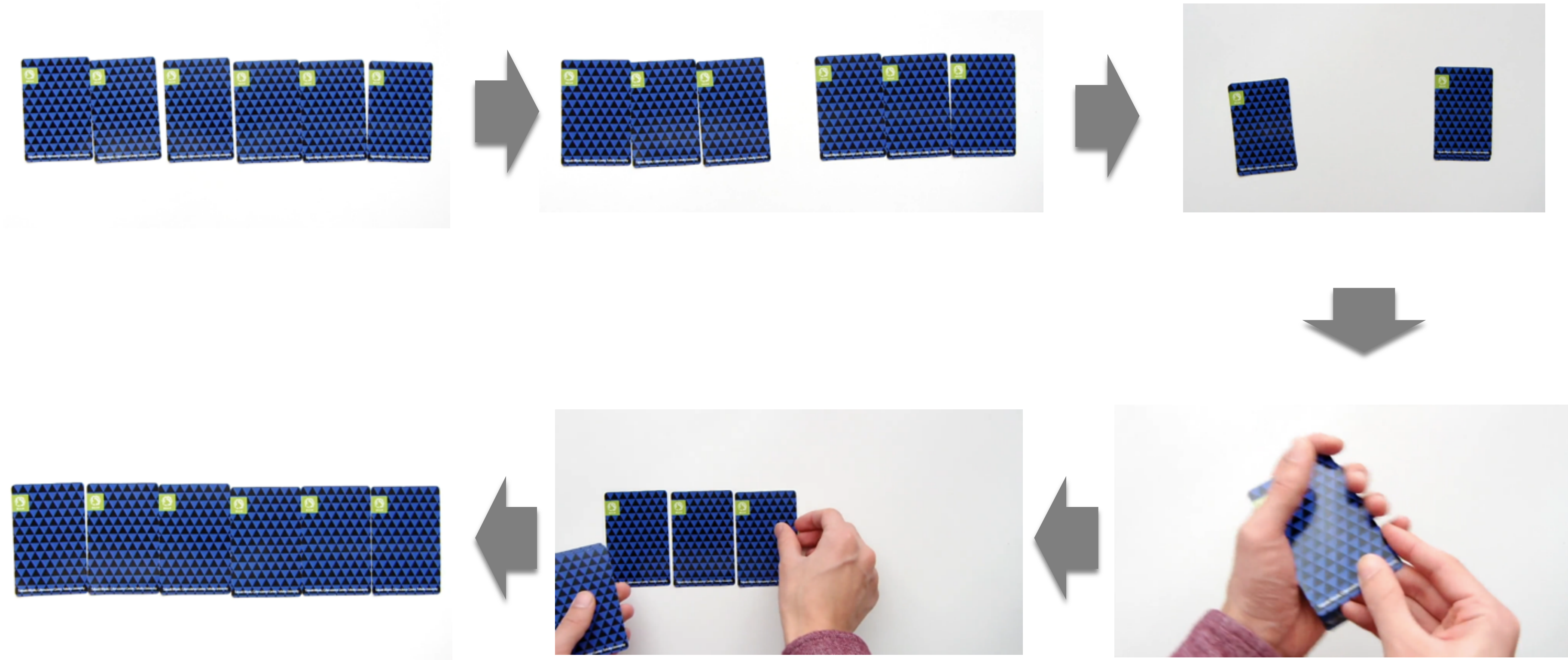
or



where each occurs with a probability of exactly 1/2.

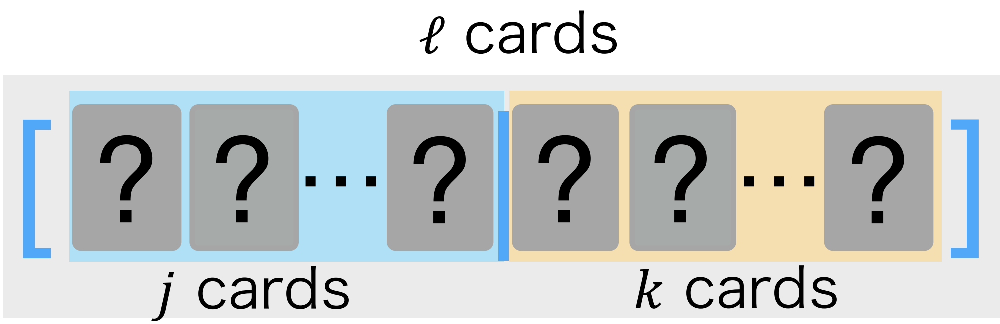
# 2.1 Bisection Cut

Example: 6 cards

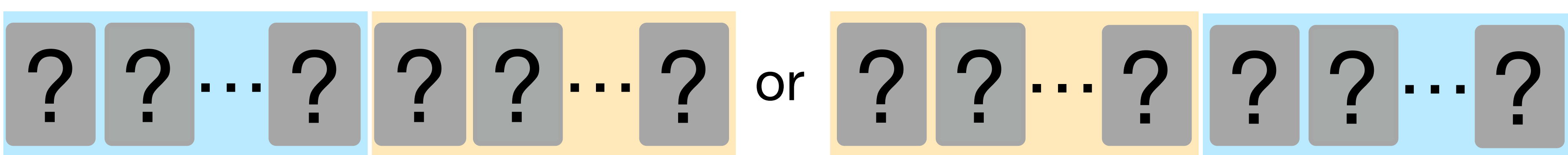


# 2.2 Unequal Division Shuffle

Suppose that there is a sequence of $\ell$ face-down cards.
Divide it into two portions of unequal sizes ($j$ cards and $k$ cards).
Then randomly switch these two portions.
We refer to it as *unequal division shuffle* or *$(j, k)$-division shuffle*.



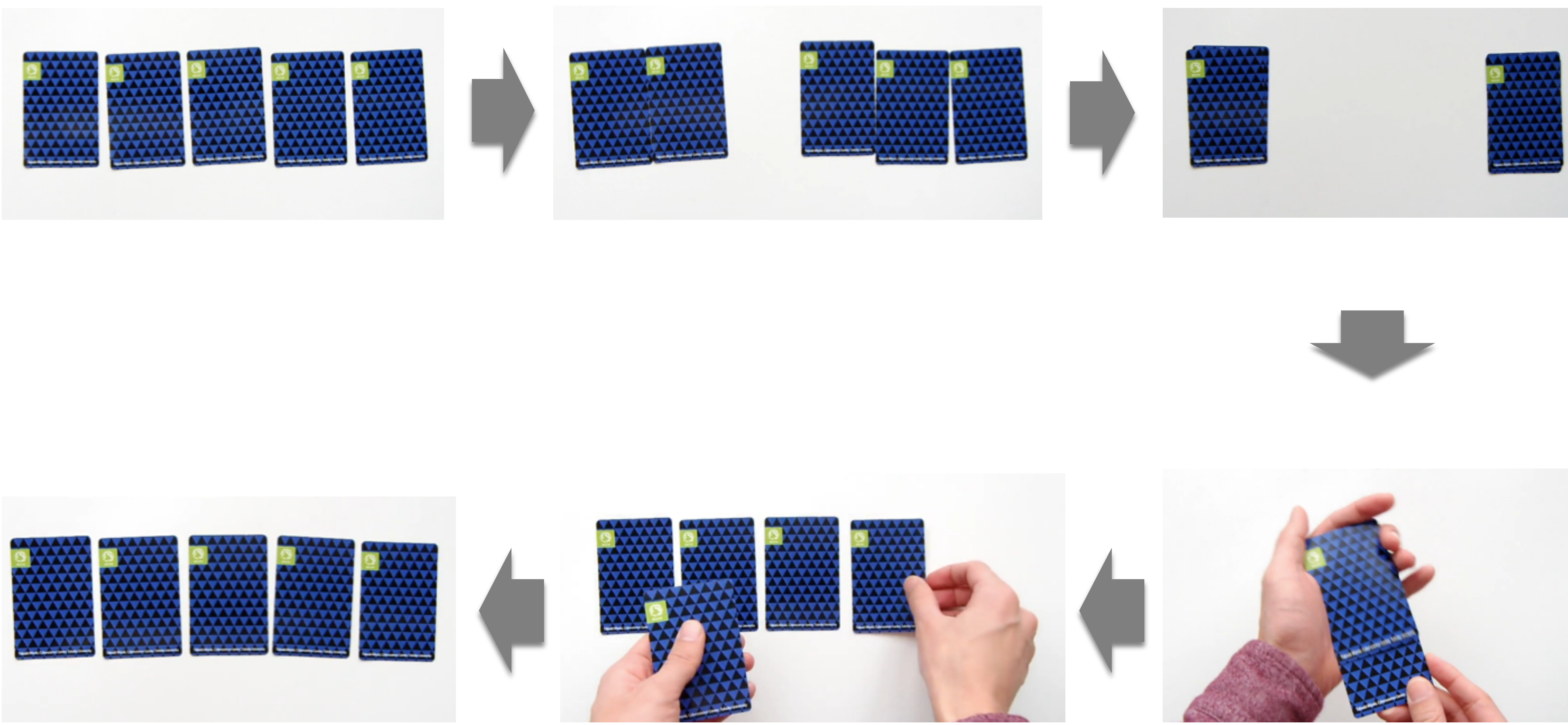

Thus, the result of the operation will be either




where each occurs with a probability of exactly 1/2.

# 2.2 Unequal Division Shuffle

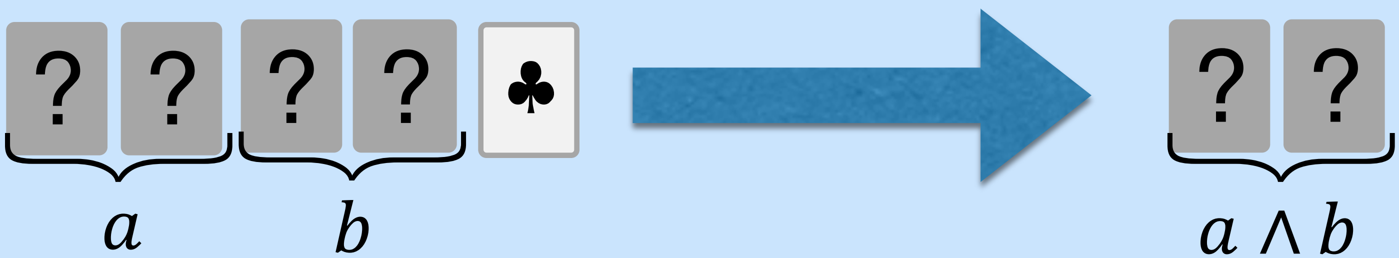
Example: total of 5 cards, (2,3)-division shuffle



# 2.3 Cheung’s AND Protocol

## Cheung’s AND Protocol [2]

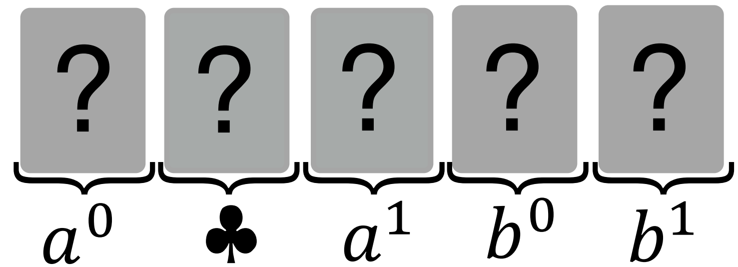
It requires only one additional card.



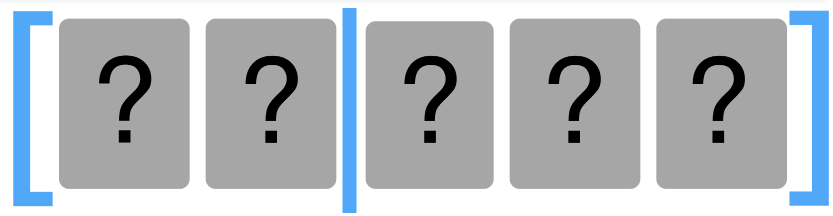

| Protocol | # of cards | Shuffle | Failure rare |
|---|---|---|---|
| Cheung’s AND [2] | 5 | Unequal Division Shuffle | 50% |

# 2.3 Cheung's AND Protocol

1. Arrange the cards of the two input commitments $(a, b)$ and the additional card.

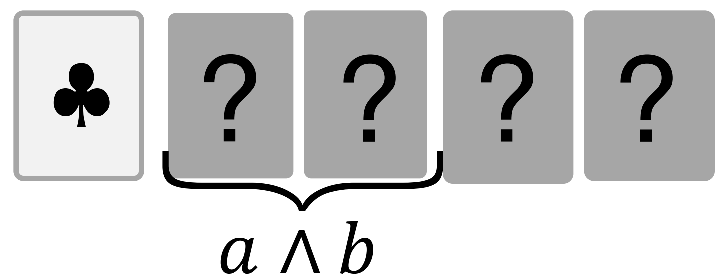



2. Apply $(2,3)$-division shuffle.

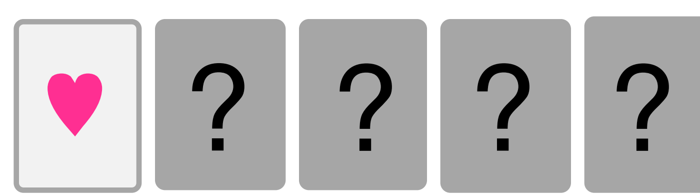



3. Reveal the card at position 1.

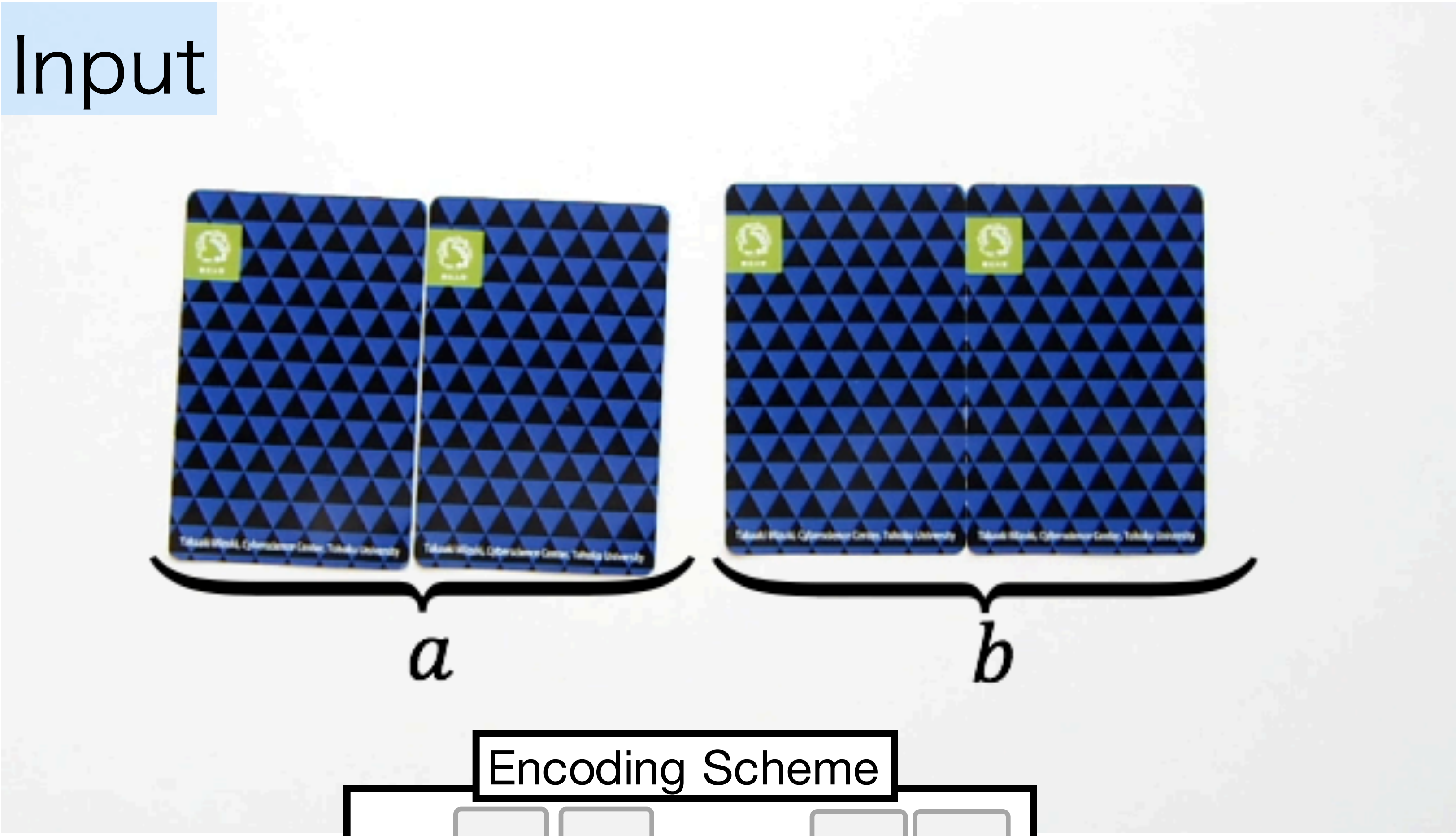
   If ♣ , then the cards at positions 2 and 3 constitute a commitment to $a \wedge b$.




   If ♥ , then Alice and Bob create input commitments again to restart the protocol.



# 2.3 Cheung's AND Protocol




Encoding Scheme

$0 = $ ♣ ♥  $1 = $ ♥ ♣

# 2.3 Cheung's AND Protocol

Step 1: Arrange the five cards.

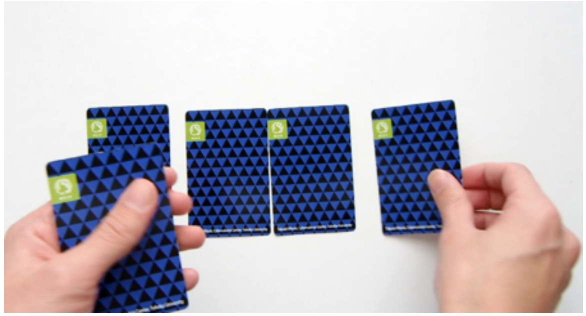
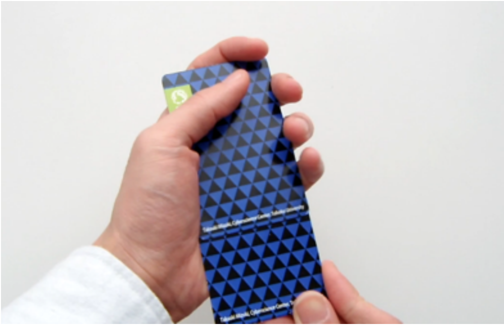
$a^0$ ♣ $a^1$ $b^0$ $b^1$

# 2.3 Cheung’s AND Protocol

## Step 2: Apply $(2,3)$-division shuffle.



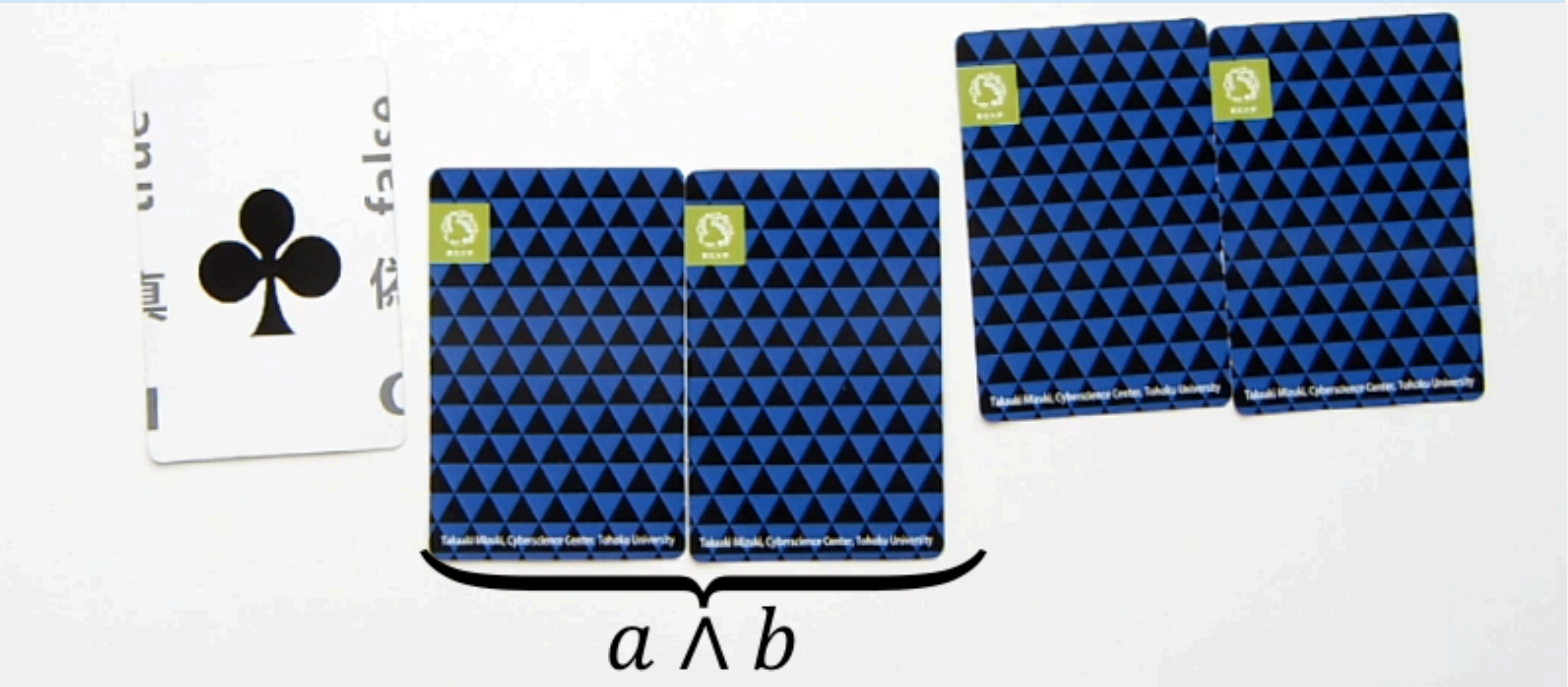


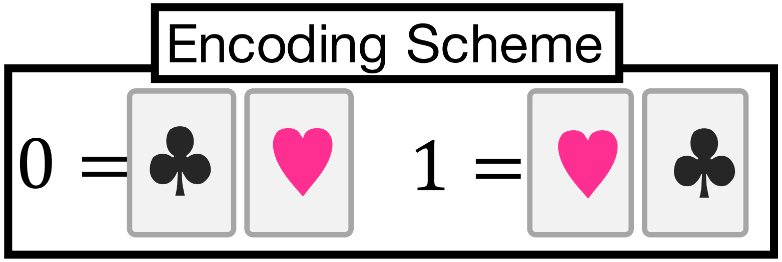



# 2.3 Cheung's AND Protocol

Example: in case of success

## Step 3: Reveal the card at position 1.



# 2.3 Cheung’s AND Protocol

Example: in case of failure

Step 3: Reveal the card at position 1.

Restart the protocol from scratch.

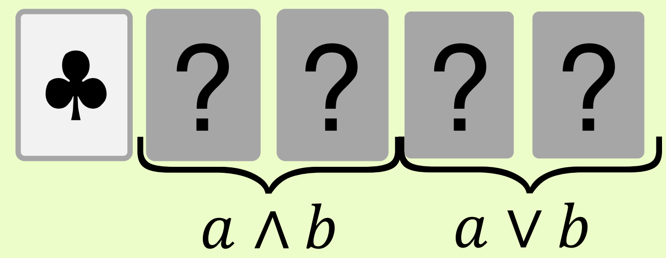
# Cheung's AND protocol

| Protocol | # of cards | Shuffle | Failure rare |
|---|---|---|---|
| Cheung's AND [2] | 5 | Unequal Division Shuffle | 50% |

# Index

# 3.1 Bonus Commitment to OR

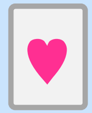
The OR value $a \vee b$ is simultaneously obtained at positions 4 and 5 when we succeed in obtaining a commitment to $a \wedge b$.

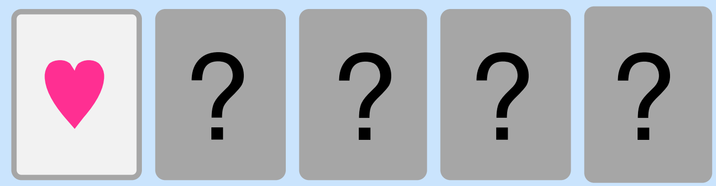


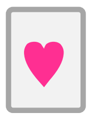

| Input $(a, b)$ | Card sequenses | |
|---|---|---|
| | $a^0$ ♣ \| $a^1$ $b^0$ $b^1$ | $a^1$ $b^0$ $b^1$ \| $a^0$ ♣ |
| $(0, 0)$ | ♣ ♣ ♥ ♣ ♥ | ♥ ♣ ♥ ♣ ♣ |
| $(0, 1)$ | ♣ ♣ ♥ ♥ ♣ | ♥ ♥ ♣ ♣ ♣ |
| $(1, 0)$ | ♥ ♣ ♣ ♣ ♥ | ♣ ♣ ♥ ♥ ♣ |
| $(1, 1)$ | ♥ ♣ ♣ ♥ ♣ | ♣ ♥ ♣ ♥ ♣ |

# 3.2 In Case of Failure

## In case of failure (Cheung’s AND protocol)

If the card at position 1 is  ,
then restart the protocol.




The other  position corresponds to the input $a, b$.

Their protocol does not fail.

We can still evaluate the AND value as a non-committed protocol.

*non-committed protocol: The output is not a commitment.

# 3.2 In Case of Failure

The other ♥ position corresponds to the input $a, b$.

| Input $(a,b)$ | Card sequences | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $a^0$ | ♣ | $a^1$ | $b^0$ | $b^1$ | $a^1$ | $b^0$ | $b^1$ | $a^0$ | ♣ |
| $(0,0)$ | ♣ | ♣ | ♥ | ♣ | ♥ | ♥ | ♣ | ♥ | ♣ | ♣ |
| $(0,1)$ | ♣ | ♣ | ♥ | ♥ | ♣ | ♥ | ♥ | ♣ | ♣ | ♣ |
| $(1,0)$ | ♥ | ♣ | ♣ | ♣ | ♥ | ♣ | ♣ | ♥ | ♥ | ♣ |
| $(1,1)$ | ♥ | ♣ | ♣ | ♥ | ♣ | ♣ | ♥ | ♣ | ♥ | ♣ |

## Computation of AND value

Reveal the card at position 4.

If ♥, then $a \wedge b = 1$. If ♣, then $a \wedge b = 0$.

## 3.2 In Case of Failure

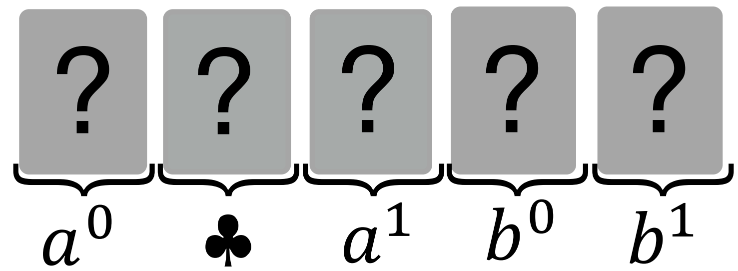
The other ♥ position corresponds to the input $a, b$.

| Input $(a,b)$ | Card sequences | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $a^0$ | ♣ | $a^1$ | $b^0$ | $b^1$ | $a^1$ | $b^0$ | $b^1$ | $a^0$ | ♣ |
| $(0,0)$ | ♣ | ♣ | ♥ | ♣ | ♥ | ♥ | ♣ | ♥ | ♣ | ♣ |
| $(0,1)$ | ♣ | ♣ | ♥ | ♥ | ♣ | ♥ | ♥ | ♣ | ♣ | ♣ |
| $(1,0)$ | ♥ | ♣ | ♣ | ♣ | ♥ | ♣ | ♣ | ♥ | ♥ | ♣ |
| $(1,1)$ | ♥ | ♣ | ♣ | ♥ | ♣ | ♣ | ♥ | ♣ | ♥ | ♣ |

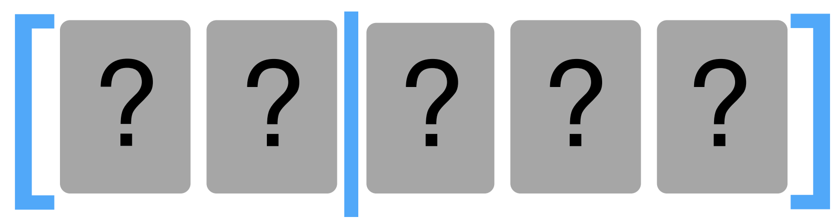
Shuffle all cards at positions corresponding to $f(a,b) = 1$ and reveal them.
If there is ♥, then $f(a,b) = 1$; otherwise $f(a,b) = 0$.

# 3.3 Improved Cheung's AND Protocol

1. Arrange the cards of the two input commitments $(a, b)$ and the additional cards.




2. Apply $(2{,}3)$-division shuffle.



# 3.3 Improved Cheung's AND Protocol

## 3. Reveal the card at position 1.

| | Cheung's AND protocol | Improved protocol |
|---|---|---|
| ♣ | ♣ $\underbrace{?\ ?}_{a \wedge b}$ ? ? | ♣ $\underbrace{?\ ?}_{a \wedge b}$ $\underbrace{?\ ?}_{a \vee b}$ |
| ♥ | Restart the protocol from scratch. | Shuffle all cards at positions corresponding to $f(a,b) = 1$ and reveal them.<br>If there is ♥, then $f(a,b) = 1$; otherwise $f(a,b) = 0$. |

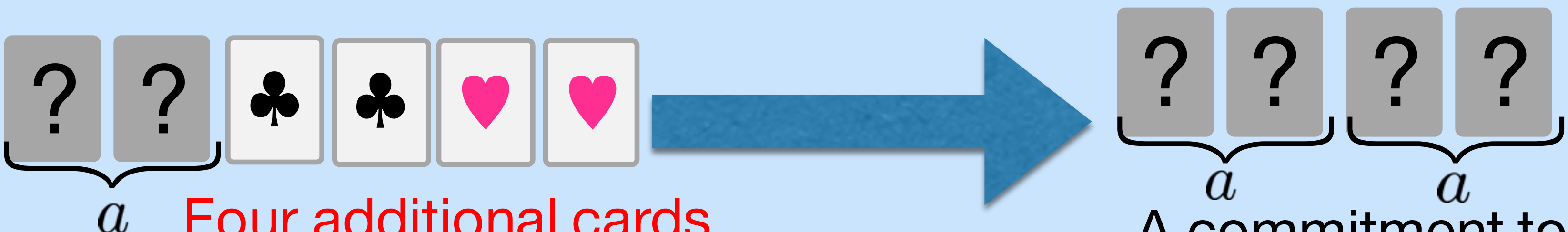
# Index

1. Introduction
2. Card Shuffling Operations and Known Protocol
3. Improved Cheung's AND Protocol
4. Five-Card Copy Protocols
5. Conclusion

# 4 Five-Card Copy Protocols

## Six-Card Copy Protocol[6]

The most efficient protocol currently known.



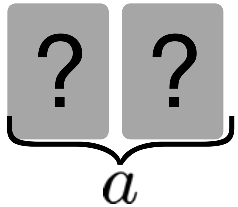

Four additional cards

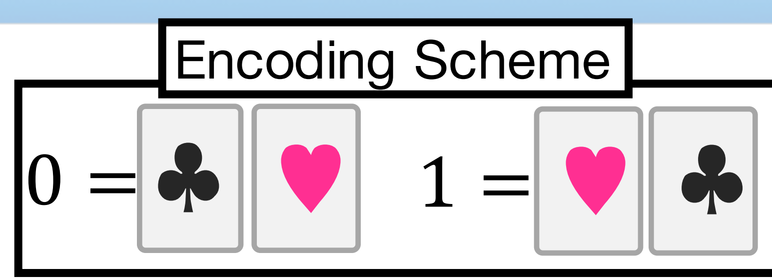
A commitment to $a$ is copied.

We propose five-card copy protocol using unequal division shuffle.

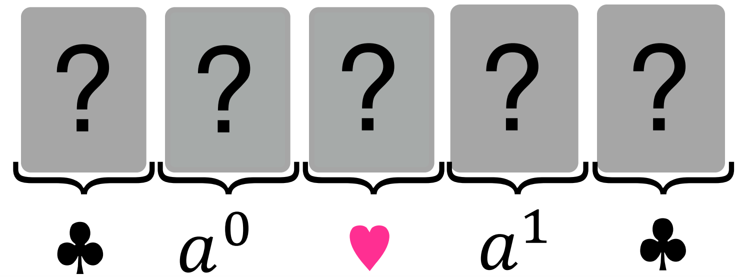
This means three additional cards are sufficient to copy a commitment.

# 4.1 Copy Protocol Using Unequal Division Shuffle

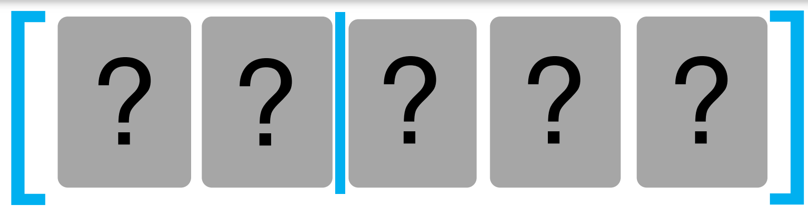
Input: 

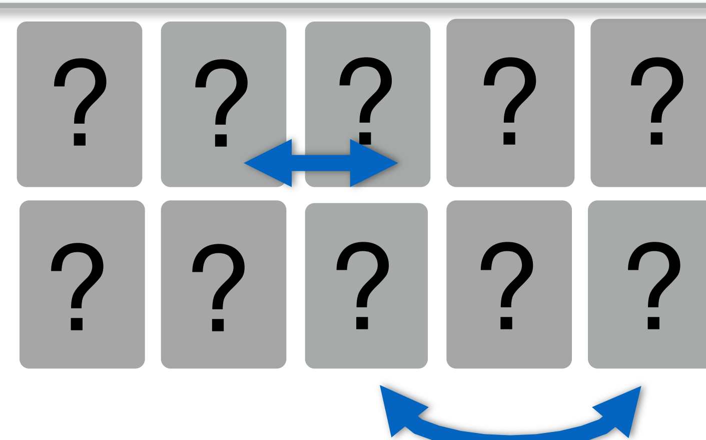

1. Arrange the five cards.




2. Apply $(2,3)$-division shuffle.



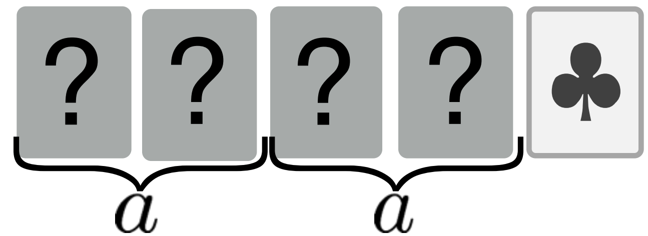

3. Rearrange the sequence of five cards.

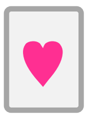


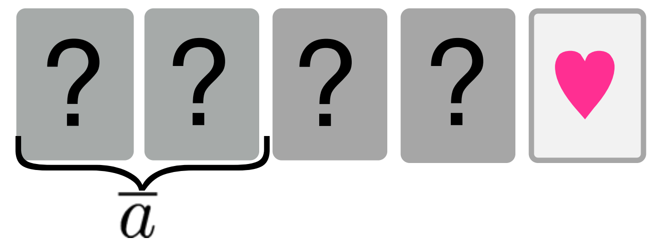
# 4.1 Copy Protocol Using Unequal Division Shuffle

4. Reveal the card at position 5.

If , then we have two commitments to $a$.




If , then we have the commitment to negation of $a$.




Swap the cards at positions 1 and 2 to obtain a commitment to $a$.
After revealing the cards at positions 3 and 4, return to step 1.

# 4.1 Copy Protocol Using Unequal Division Shuffle

The possibility of card sequences after step 3.

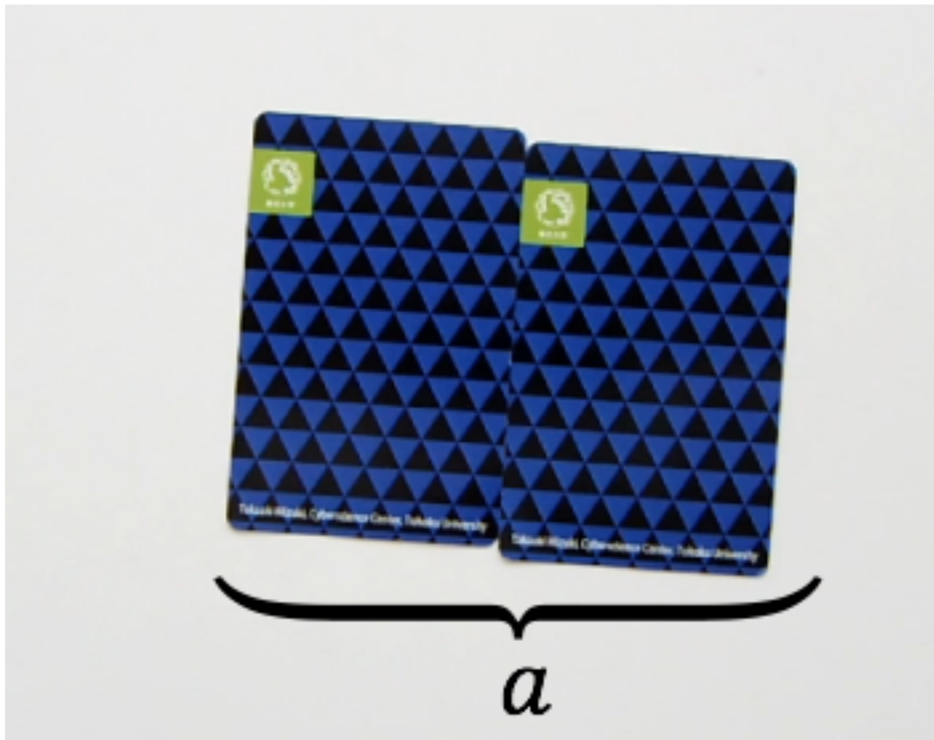
| Input $a$ | Card sequences | |
|---|---|---|
| | ♣ ♥ ♣ $a^1$ $a^0$ | ♥ ♣ $a^0$ ♣ $a^1$ |
| 0 | ♣ ♥ ♣ ♥ ♣ | ♥ ♣ ♣ ♣ ♥ |
| 1 | ♣ ♥ ♣ ♣ ♥ | ♥ ♣ ♥ ♣ ♣ |

Encoding Scheme

$0 =$ ♣ ♥ $1 =$ ♥ ♣

# 4.1 Copy Protocol Using Unequal Division Shuffle

## Input




**Encoding Scheme**

$0 =$ ♣ ♥    $1 =$ ♥ ♣

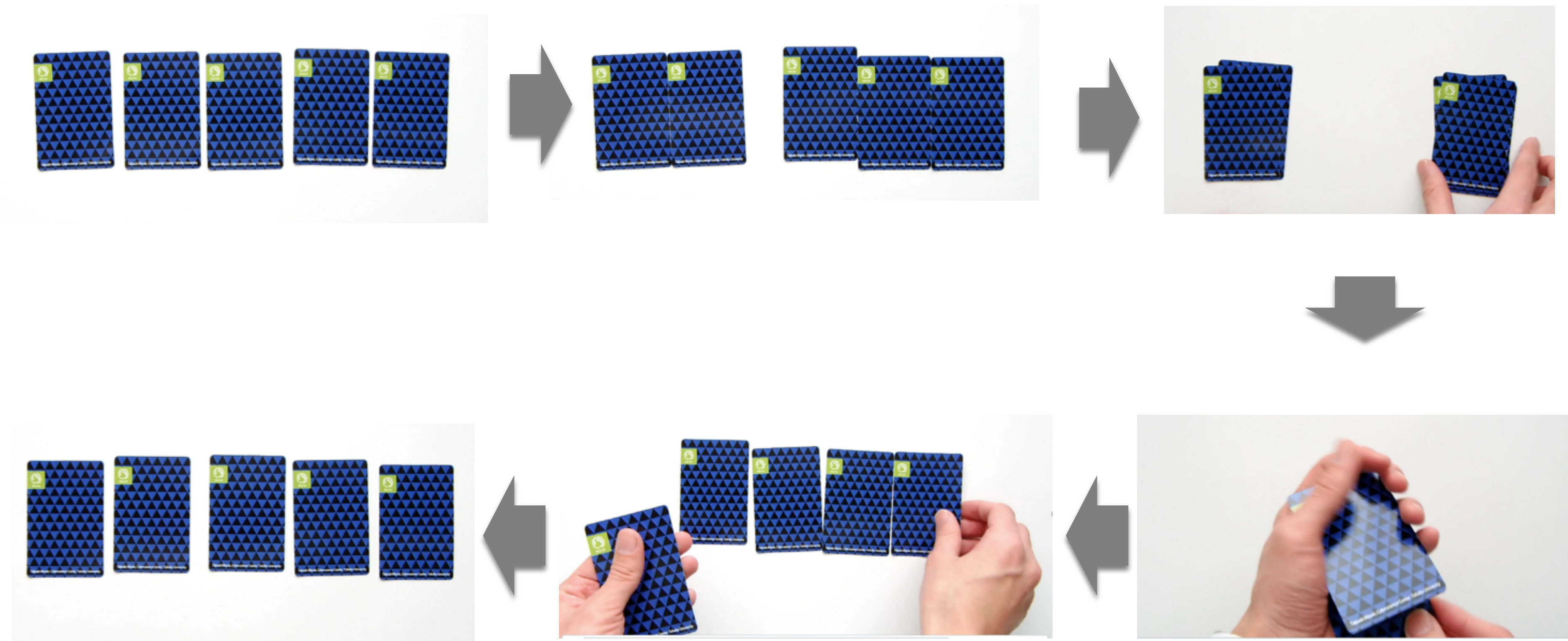
## 4.1 Copy Protocol Using Unequal Division Shuffle

Step 1: Arrange the five cards.

♣ $a^0$ ♥ $a^1$ ♣

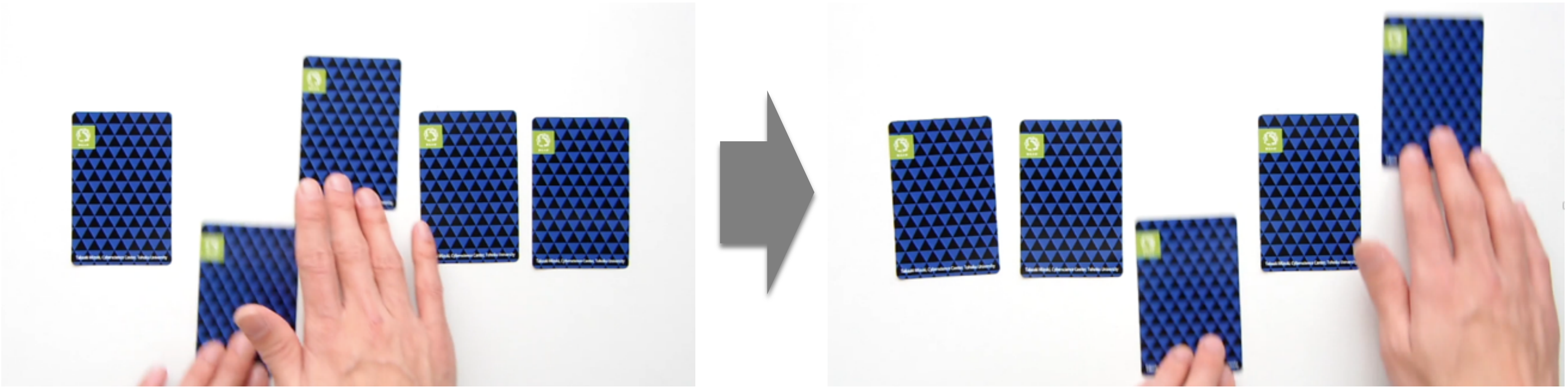
# 4.1 Copy Protocol Using Unequal Division Shuffle

## Step 2: Apply $(2,3)$-division shuffle.



# 4.1 Copy Protocol Using Unequal Division Shuffle

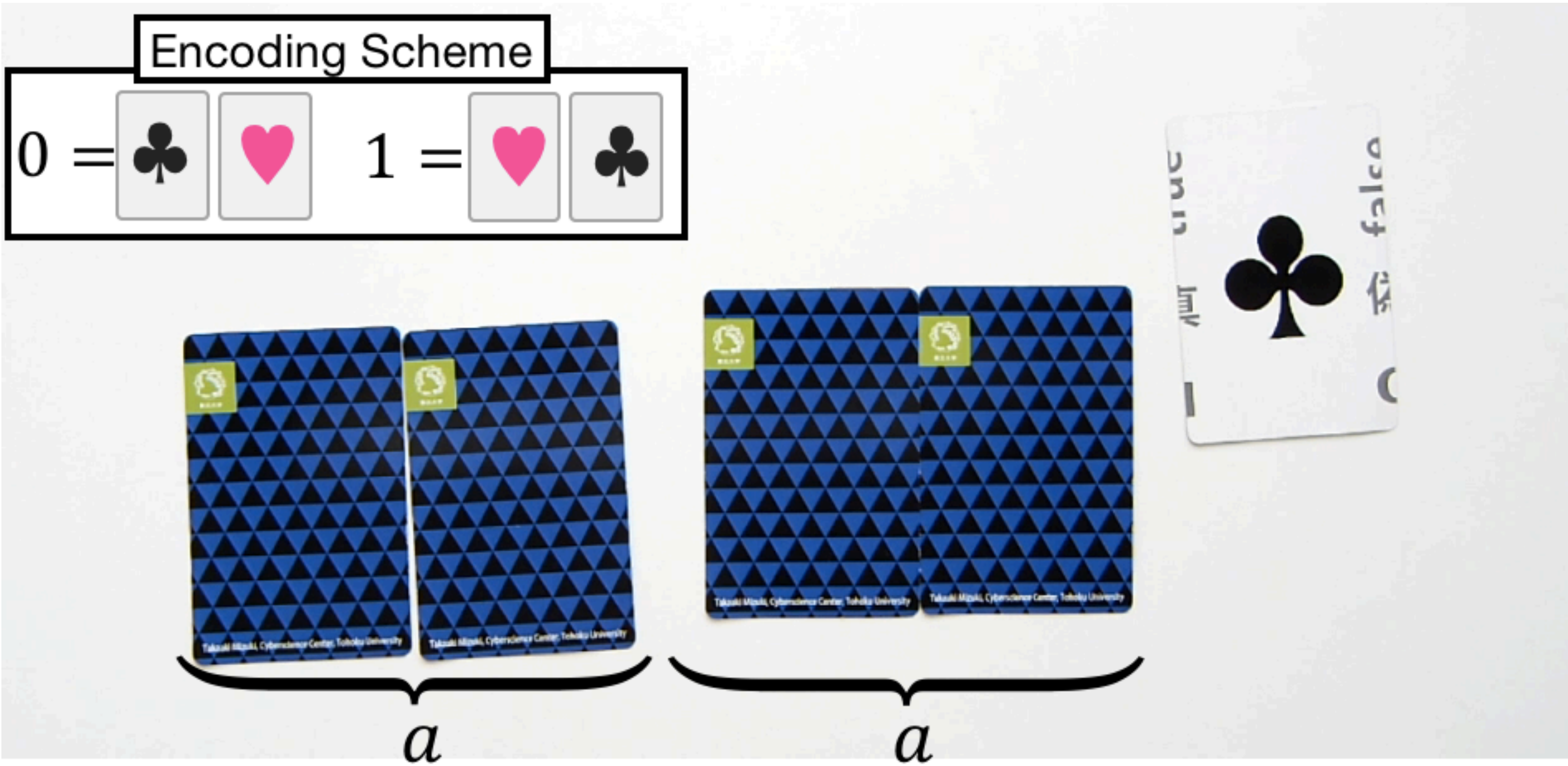
Step 3: Rearrange the cards.



# 4.1 Copy Protocol Using Unequal Division Shuffle

In case that two copies are obtained.

## Step 4: Reveal the card at position 5.



# 4.1 Copy Protocol Using Unequal Division Shuffle

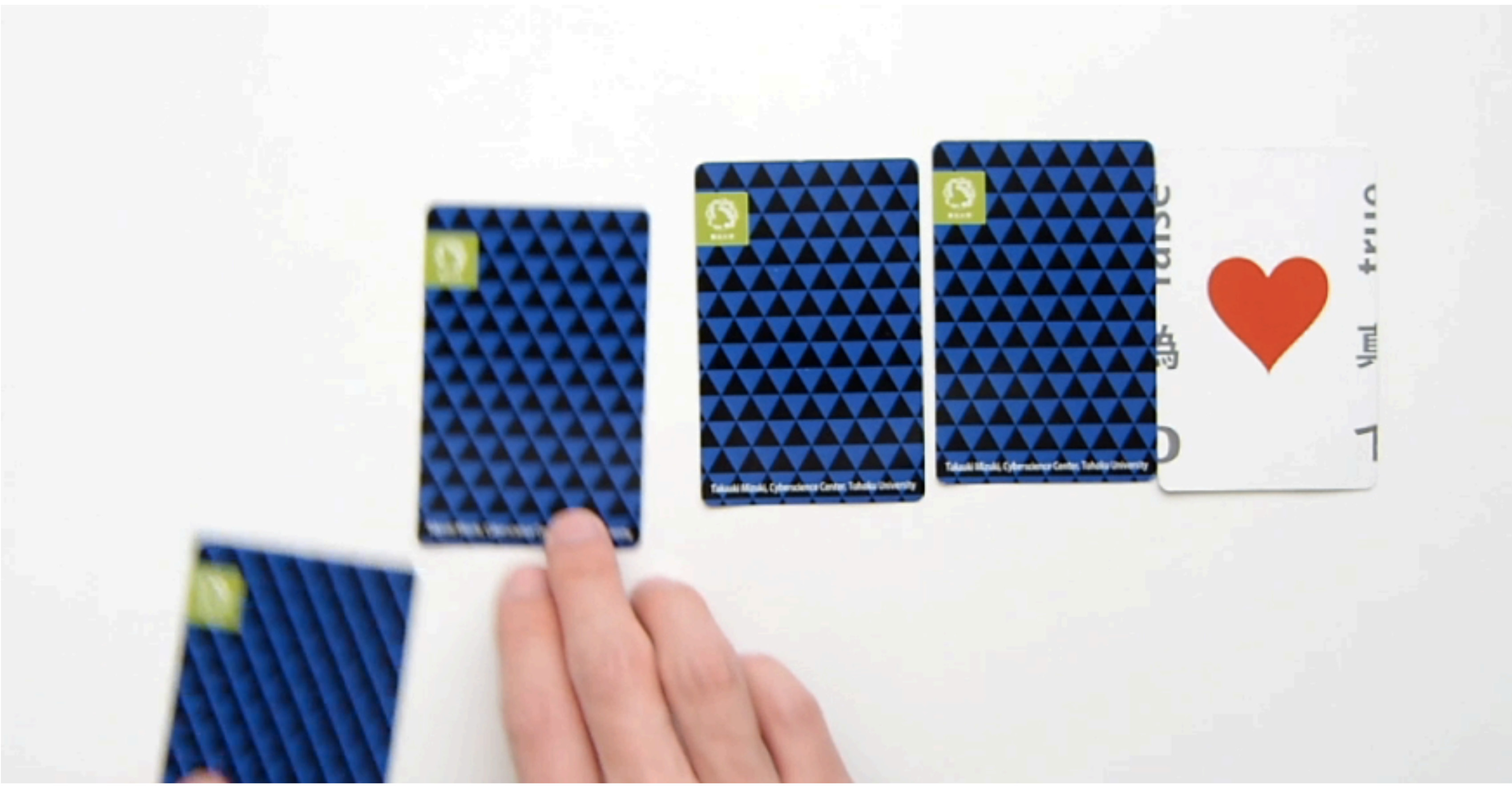
In case of returning to step 1.

## Step 4: Reveal the card at position 5.

# 4.1 Copy Protocol Using Unequal Division Shuffle

In case of returning to step 1.

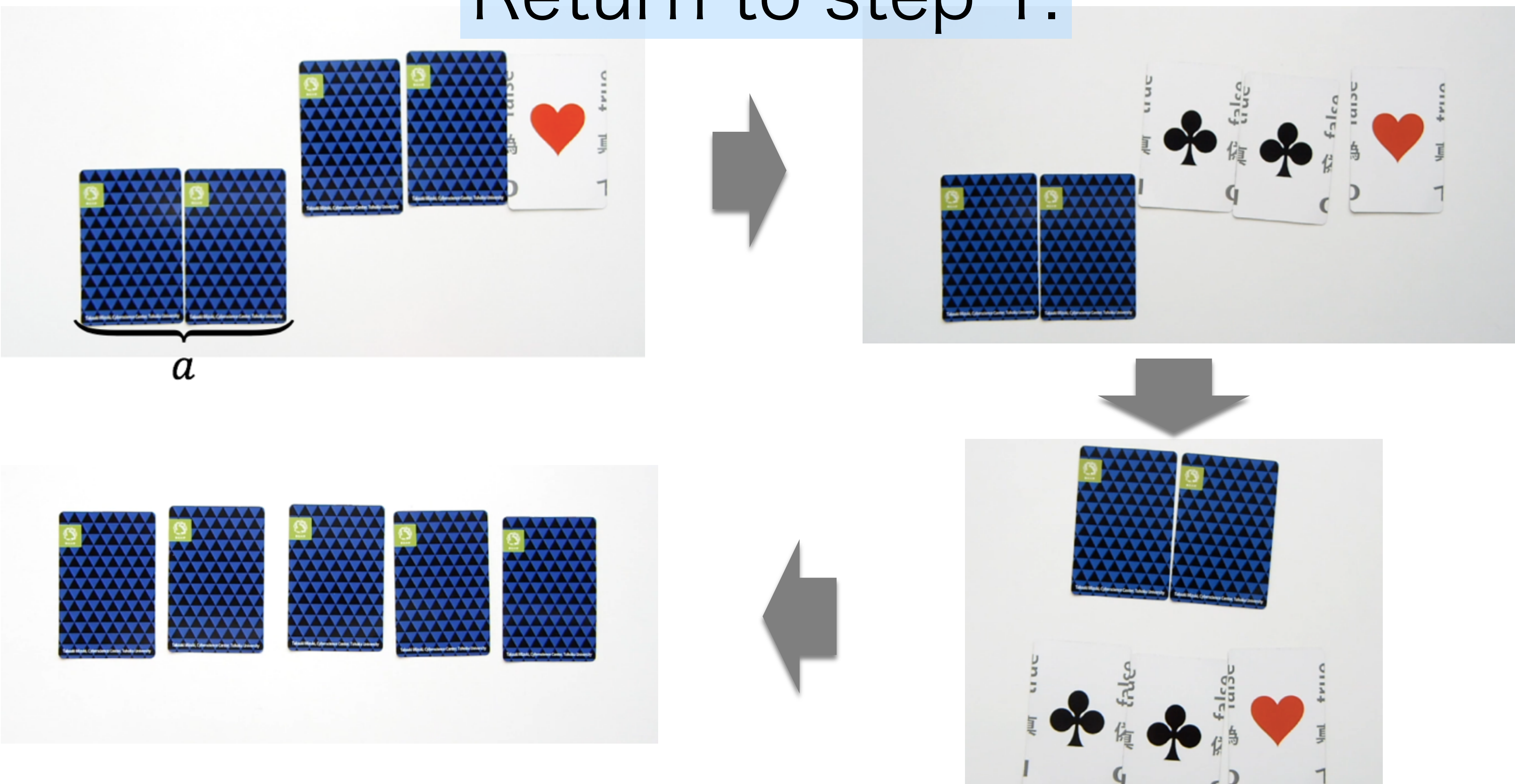
Swap the cards at positions 1 and 2.



# 4.1 Copy Protocol Using Unequal Division Shuffle

In case of returning to step 1.

Return to step 1.



# Copy Protocols

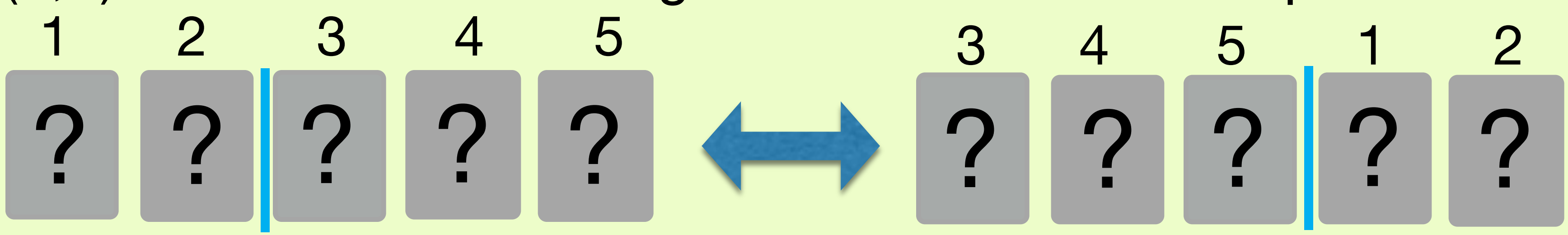
| Protocol | # of cards | Shuffle | Avg. # of trials |
|---|---|---|---|
| Six-card Copy [6] | 6 | Random Bisection Cut | 1 |
| Ours | 5 | Unequal Division Shuffle | 2 |

## 4.2 Copy Protocol Using Double Unequal Division Shuffle

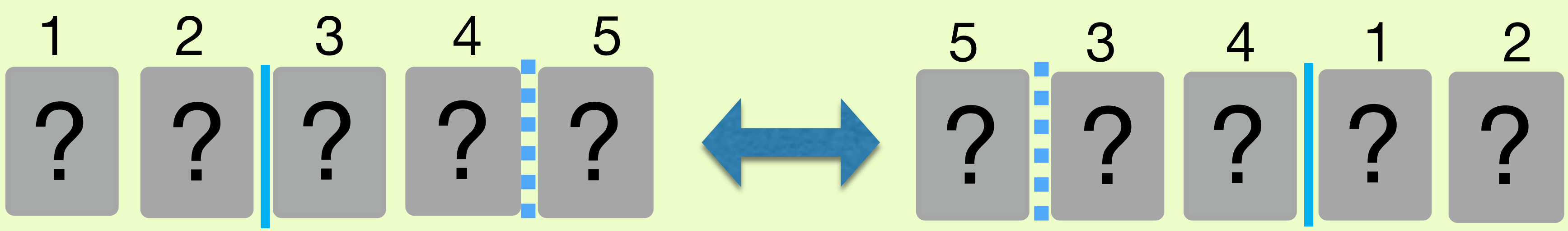
To reduce the number of steps, we consider:

### Double Unequal Division Shuffle

(2,3)-division shuffle changes the order of the two portions.



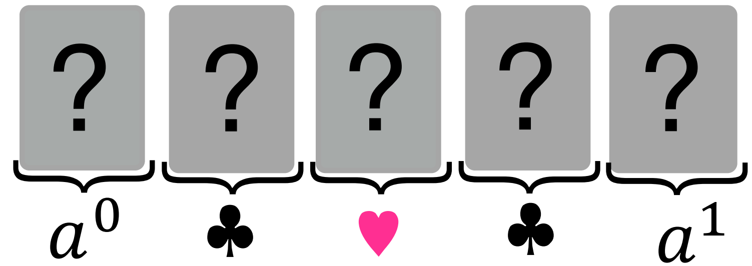

Here, we consider a further division of the three-card portion:



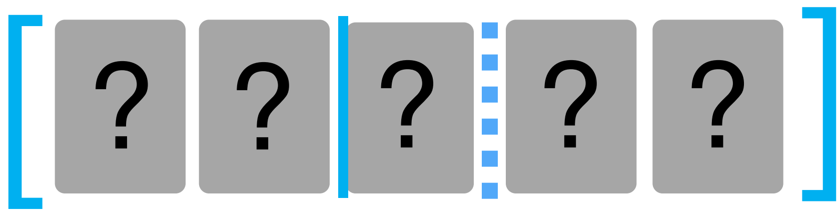

However, we are not sure whether this shuffle can be easily implemented by humans.

# 4.2 Copy Protocol Using Double Unequal Division Shuffle

1. Arrange the five cards.



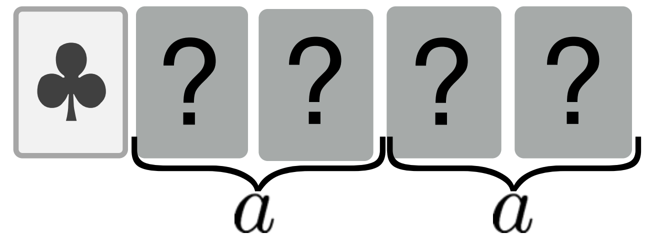

2. Apply double unequal division shuffle.

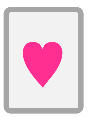


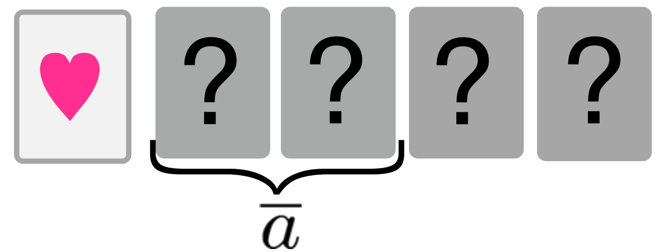
# 4.2 Copy Protocol Using Double Unequal Division Shuffle

3. Reveal the card at position 1.

If , then we have two commitments to $a$.




If , then we have negation of $a$.




Swap the cards at positions 2 and 3 to obtain a commitment to $a$.
After revealing the cards at positions 4 and 5, return to step 1.

# 4.2 Copy Protocol Using Double Unequal Division Shuffle

The possibility of card sequences after step 3.

| Input $a$ | Card Sequences | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $a^0$ | ♣ | ♥ | ♣ | $a^1$ | $a^1$ | ♥ | ♣ | $a^0$ | ♣ |
| 0 | ♣ | ♣ | ♥ | ♣ | ♥ | ♥ | ♥ | ♣ | ♣ | ♣ |
| 1 | ♥ | ♣ | ♥ | ♣ | ♣ | ♣ | ♥ | ♣ | ♥ | ♣ |

**Encoding Scheme**

$0 =$ ♣ ♥  $1 =$ ♥ ♣

# Index

# 5 Conclusion

## AND Protocols

| Protocol | # of cards | Shuffle | Failure rare | Output (Input($a, b$)) |
|---|---|---|---|---|
| Six-card AND [6] | 6 | Random Bisection Cut | 0% | $\underbrace{?\ ?}_{a \land b}$ |
| Cheung's AND [2] | 5 | Unequal Division Shuffle | 50% | $\underbrace{?\ ?}_{a \land b}$ |
| Ours | 5 | Unequal Division Shuffle | 0% | $\underbrace{?\ ?}_{a \land b}$ non-hidden value of $a \land b$ |

# 5 Conclusion

## Copy Protocols

| Protocol | # of cards | Shuffle | Avg. # of trials |
|---|---|---|---|
| Six-card Copy [6] | 6 | Random Bisection Cut | 1 |
| Ours | 5 | Unequal Division Shuffle | 2 |