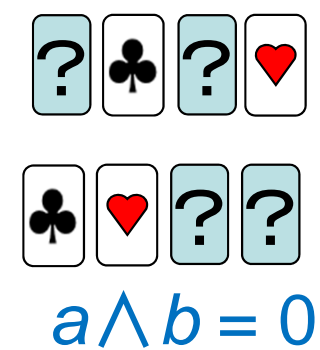
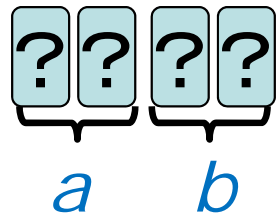


The Five-Card Trick Can Be Done with Four Cards



Takaaki Mizuki, Michihito Kumamoto, Hideaki Sone
 Tohoku University

Abstract

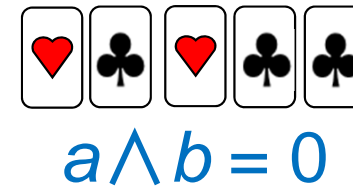
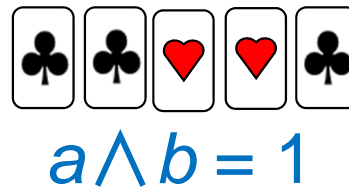
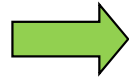
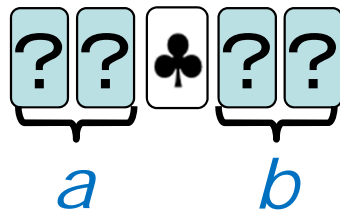


東北大学

Abstract

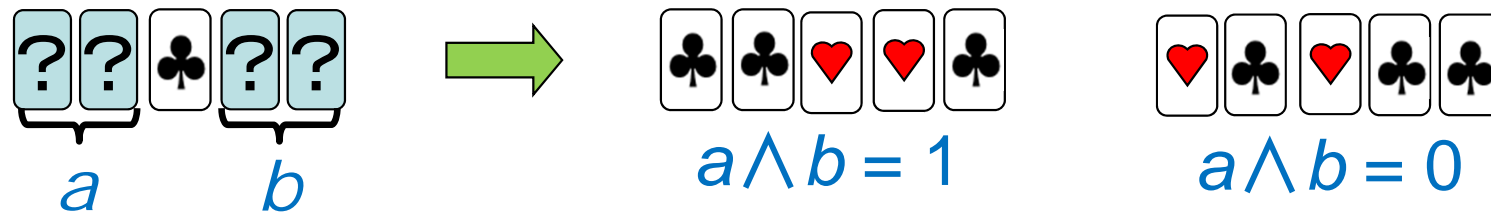


- ✓ The ***five-card trick***, by Bert den Boer [Eurocrypt 89], securely computes AND using **5** cards.

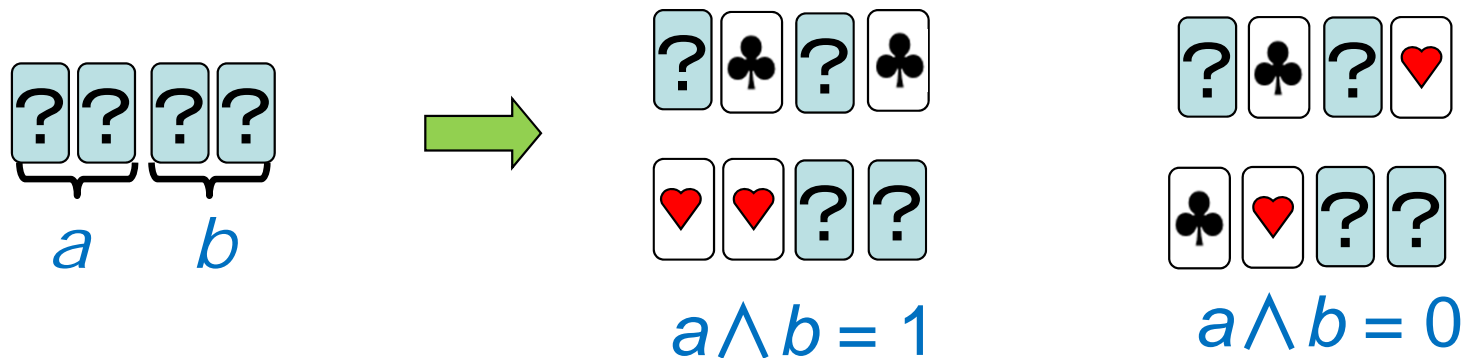


Abstract

- ✓ The ***five-card trick***, by den Boer [Eurocrypt 89], securely computes AND using **5** cards.



- ✓ ***This paper*** gives a protocol which securely computes AND using **4** cards.



Contents



- 1. Introduction**
- 2. Description of Our Protocol**
- 3. Correctness of Our Protocol**
- 4. Conclusions**

Contents



1. Introduction

2. Description of Our Protocol

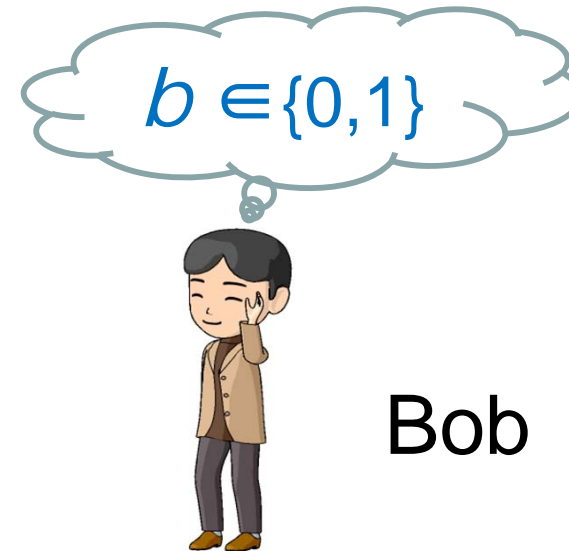
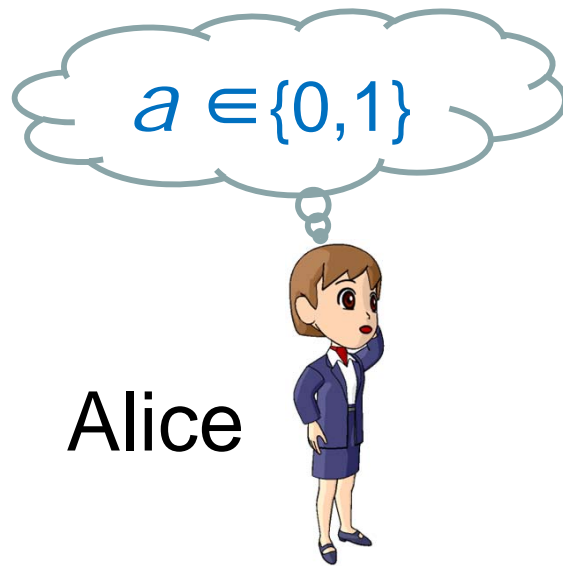
3. Conclusion

1.1 The five-card trick

1.2 Our result and related work

4. Conclusions

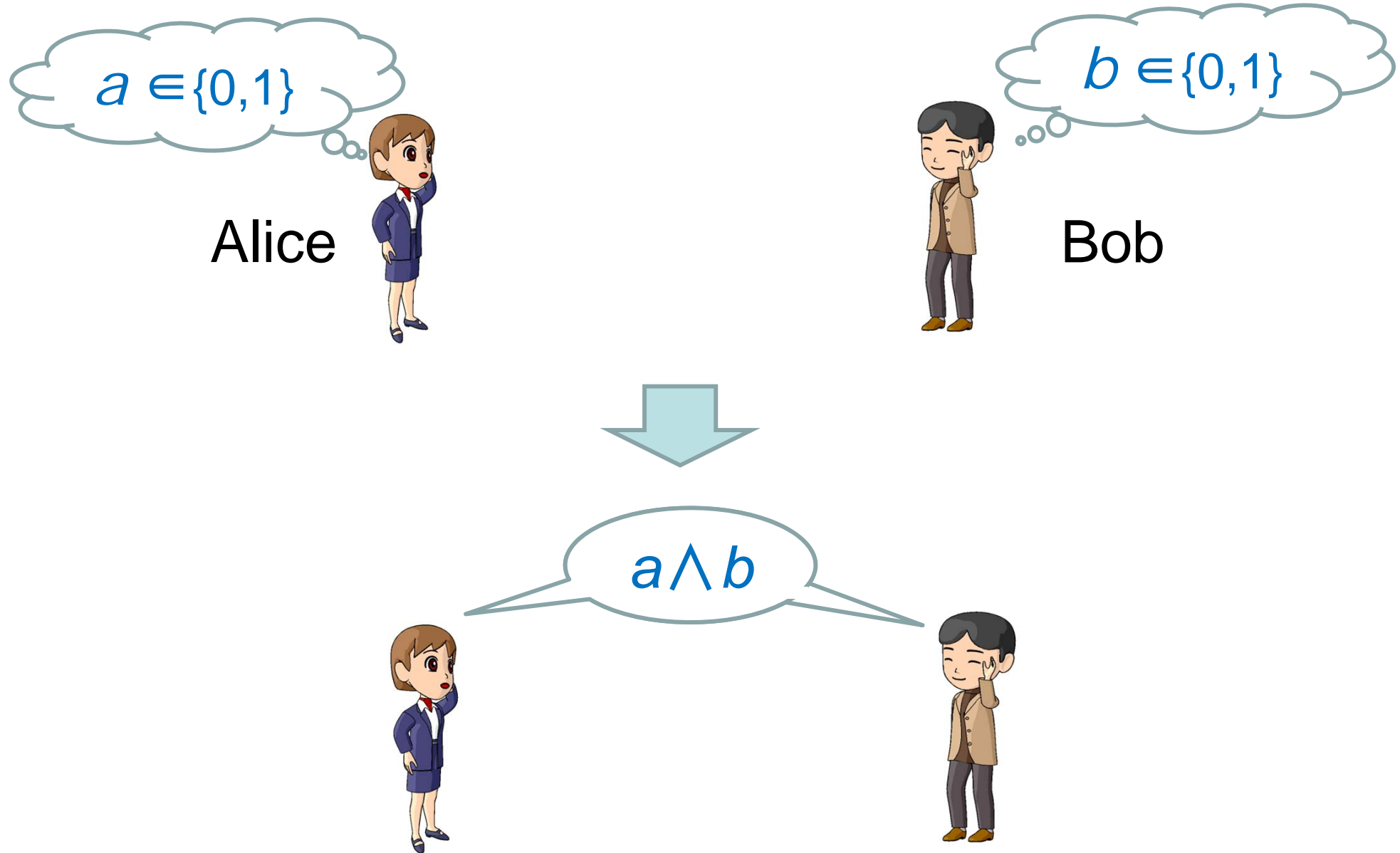
Scenario



two semi-honest players

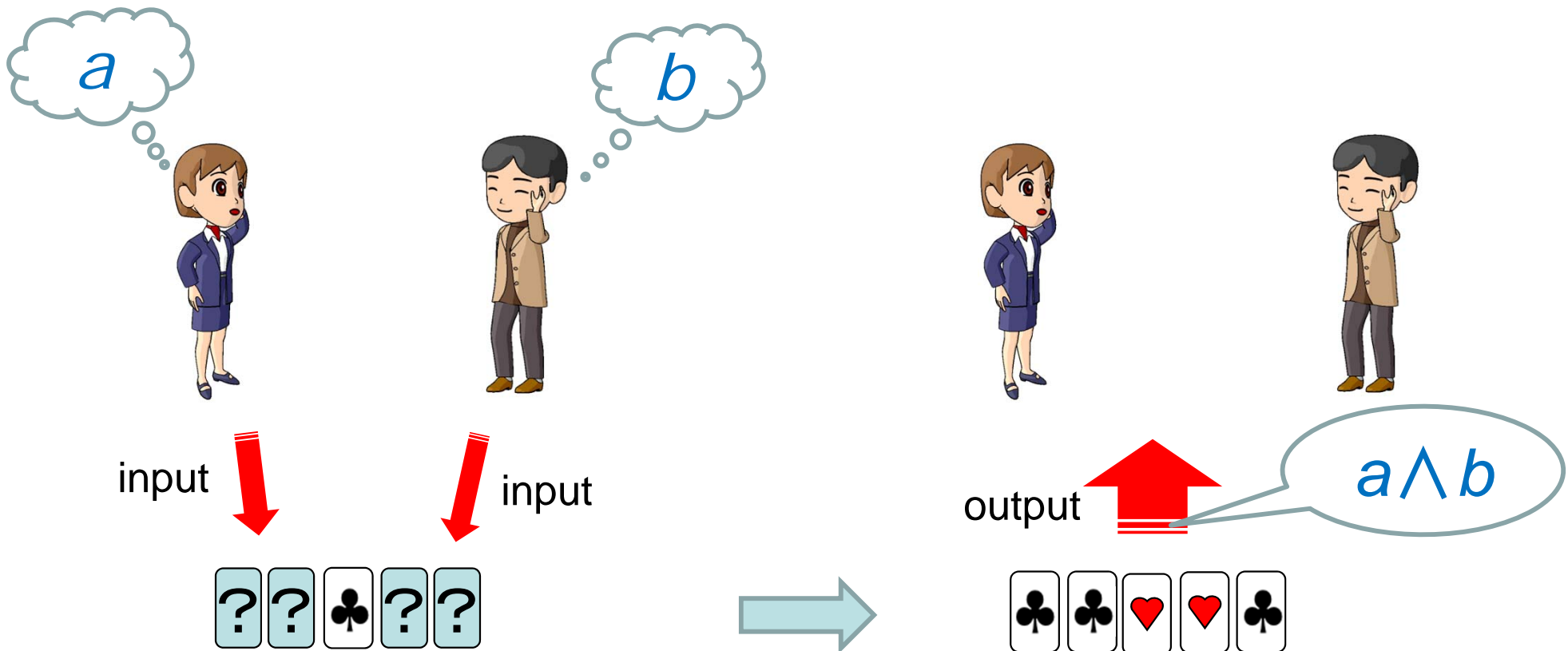
Scenario

Alice and Bob want to securely compute AND.

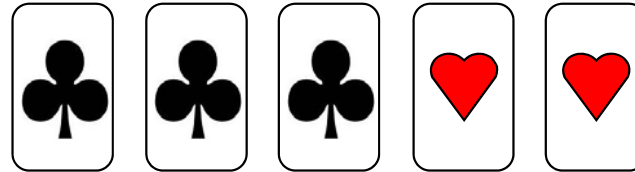


Scenario

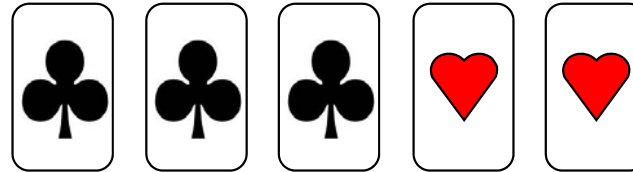
The five-card trick achieves such a secure computation of AND.



Scenario



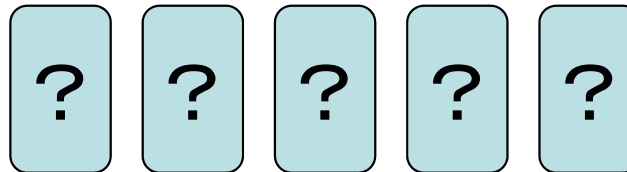
Scenario



face-up



turn over



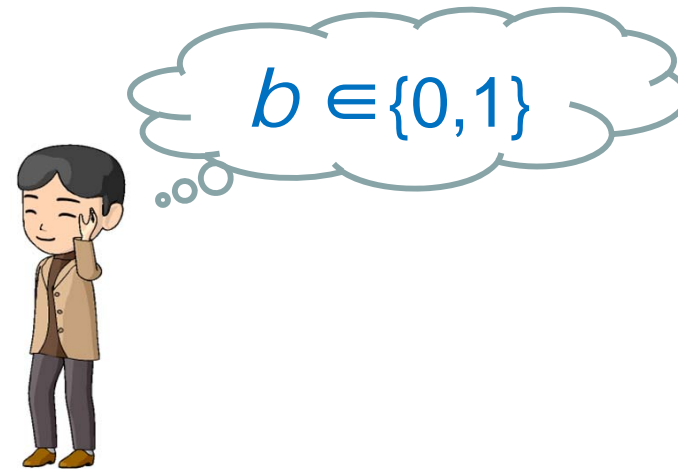
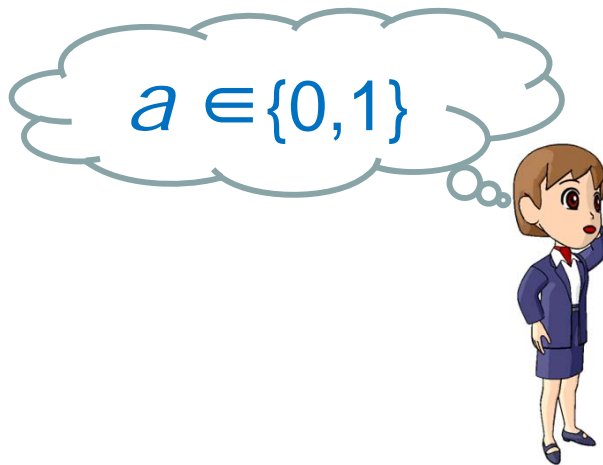
face-down

Scenario

To deal with Boolean values, this encoding is used:

$$\begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0$$

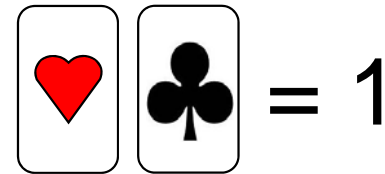
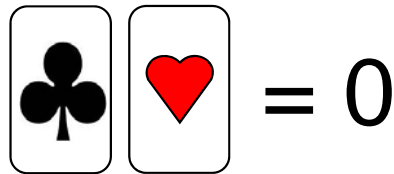
$$\begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} = 1$$



Scenario

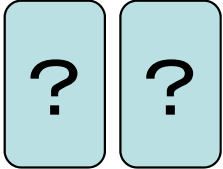


To deal with Boolean values, this encoding is used:



commitment

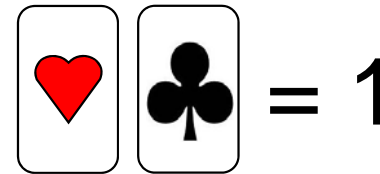
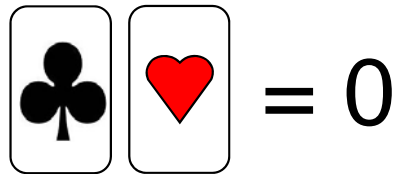
A **commitment** to a bit $x \in \{0,1\}$ is

a pair  of two face-down cards holding the value of x .

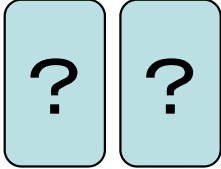
Scenario

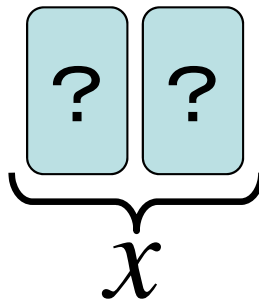


To deal with Boolean values, the encoding is used:



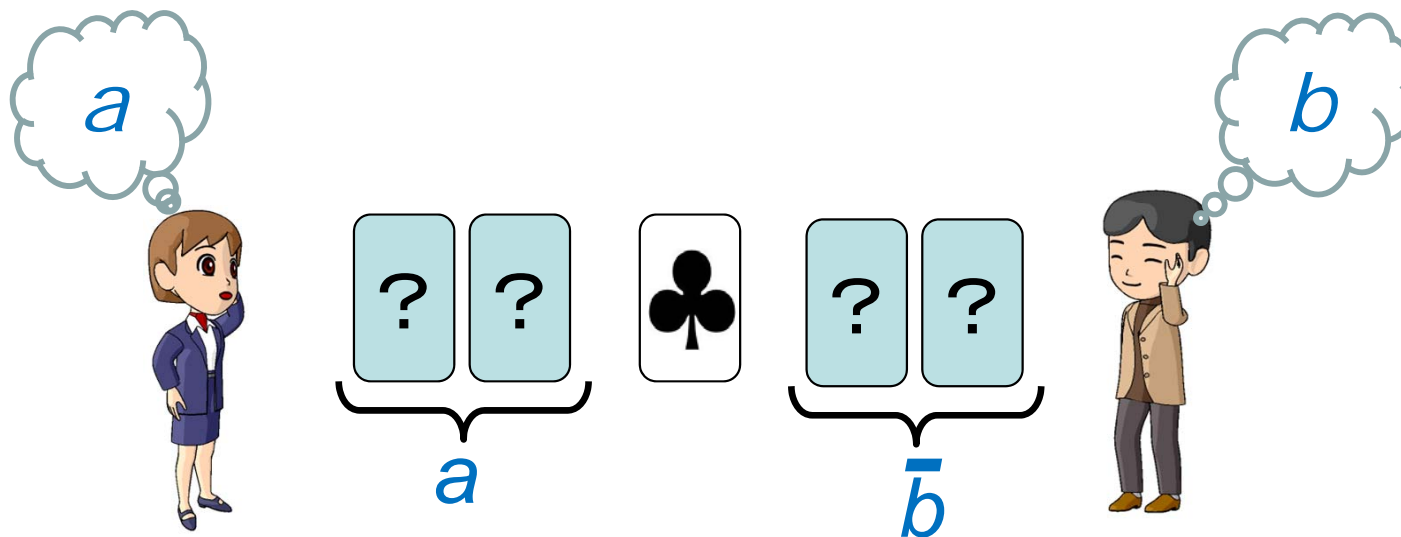
commitment



A **commitment** to a bit $x \in \{0,1\}$ is
a pair  of two face-down cards
holding the value of x .


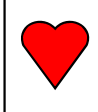


Five-card trick; **step 1**

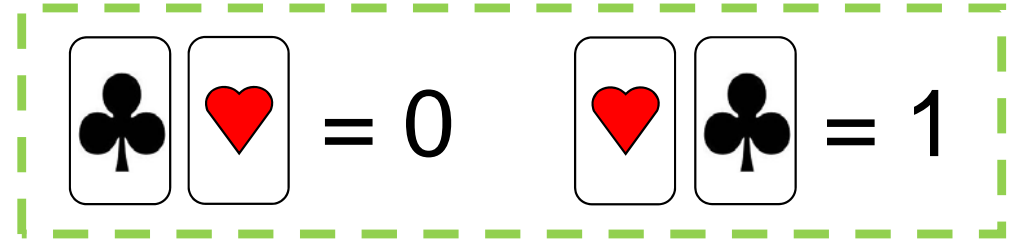
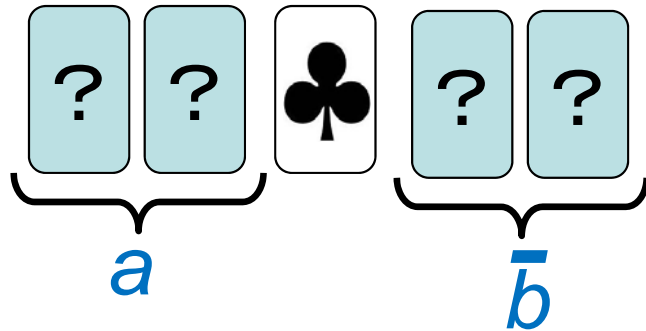
- Alice privately makes a commitment to her bit a .
- Bob makes a commitment to the negation \bar{b} of b .
- They put them forth with the remaining black card.






 = 0

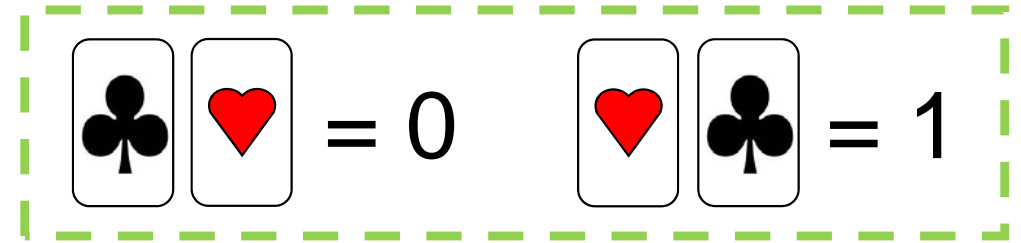
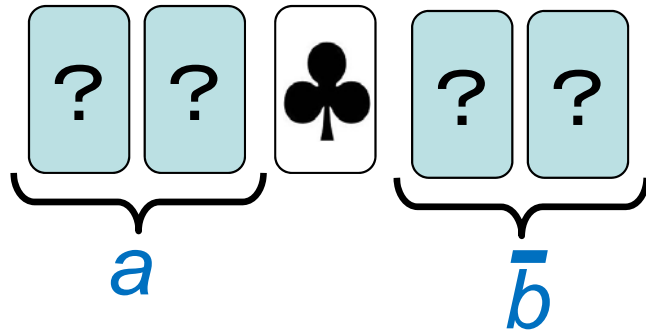
 = 1




Five-card trick; **step 1**

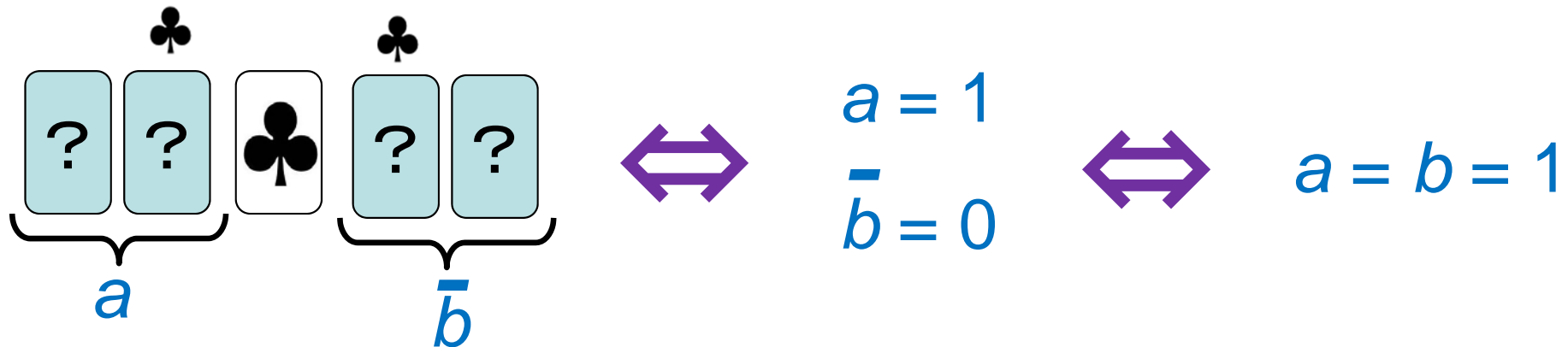


Note that the 3 cards in the middle would be black (namely   ) only when $a = b = 1$.

Five-card trick; **step 1**

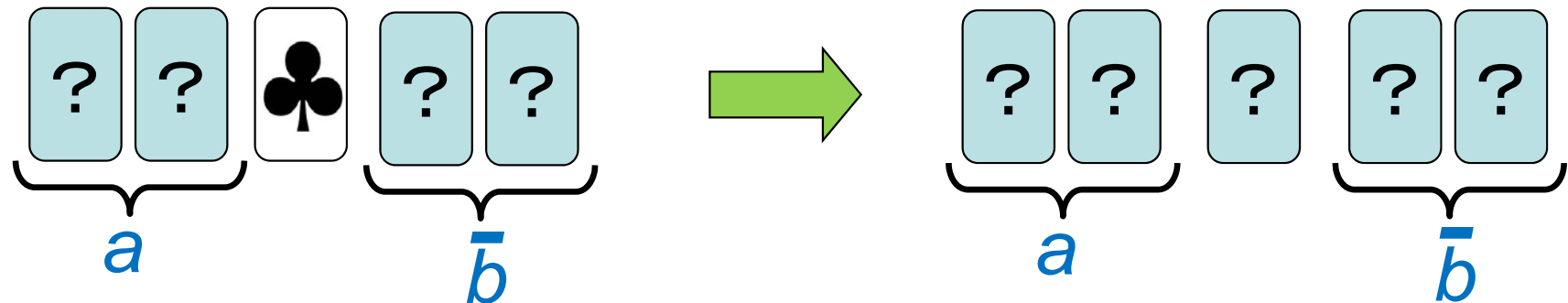


Note that the 3 cards in the middle would be black (namely   ) only when $a = b = 1$.

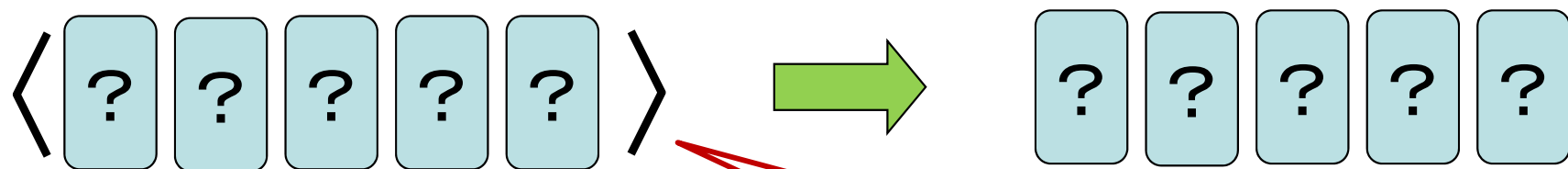


Five-card trick; **step 2**

- Turn the centered card face down:



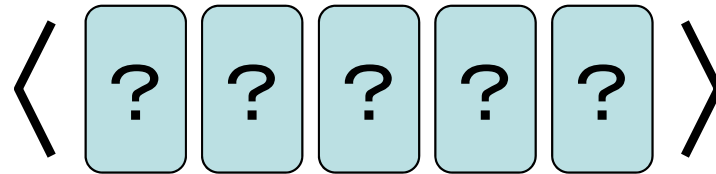
- Apply a **random** cut:



random cut
(= cyclic shuffling or random cyclic shift)

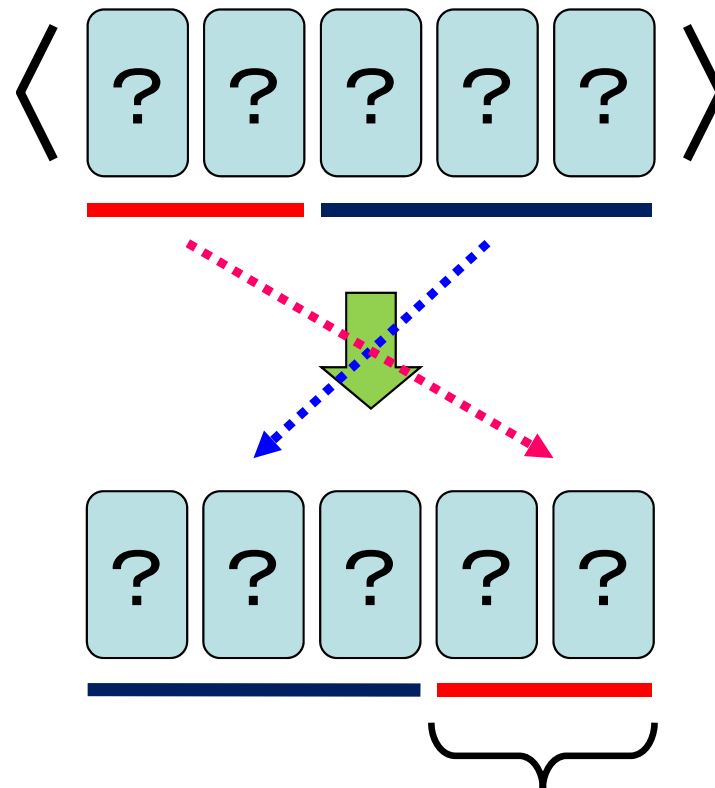
What is a *random cut*?

A *random* number of leftmost cards are moved to the right without changing their order.



What is a *random cut*?

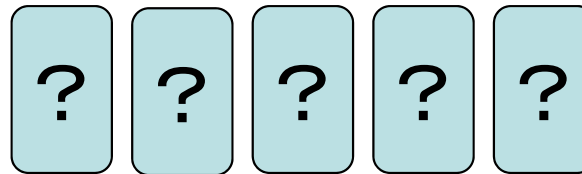
A *random* number of leftmost cards are moved to the right without changing their order.



a random number,
which *nobody* knows

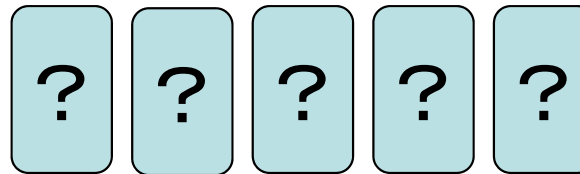
Five-card trick; **step 3**

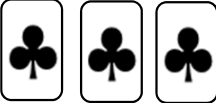
- Reveal all 5 cards:

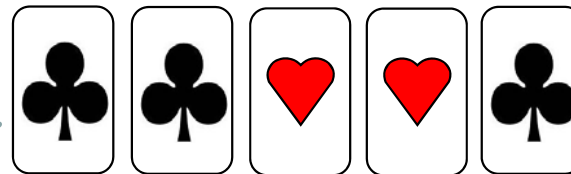


Five-card trick; **step 3**

- Reveal all 5 cards:



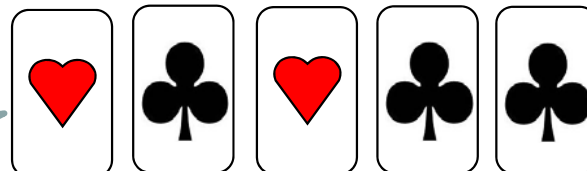
 are
cyclically
consecutive.



$$a \wedge b = 1$$

or

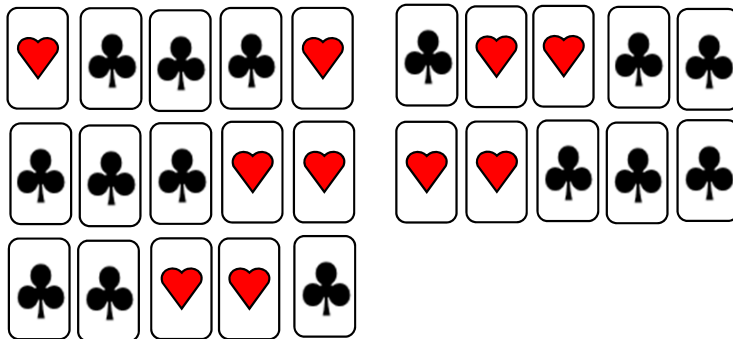
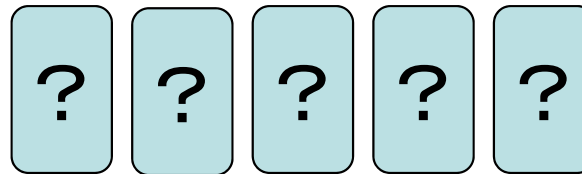
They are not.



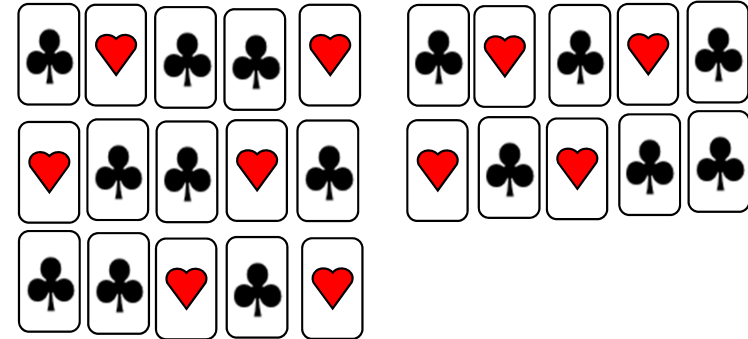
$$a \wedge b = 0$$

Five-card trick; **step 3**

- Reveal all 5 cards:



$$a \wedge b = 1$$

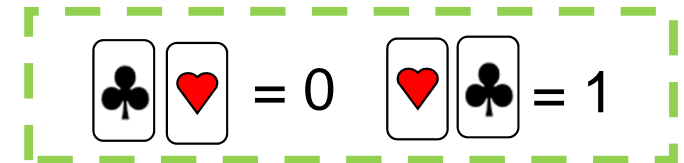
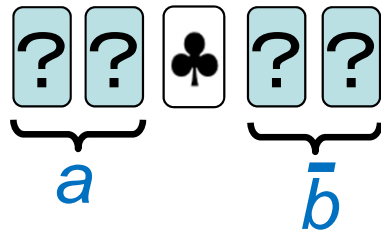


$$a \wedge b = 0$$

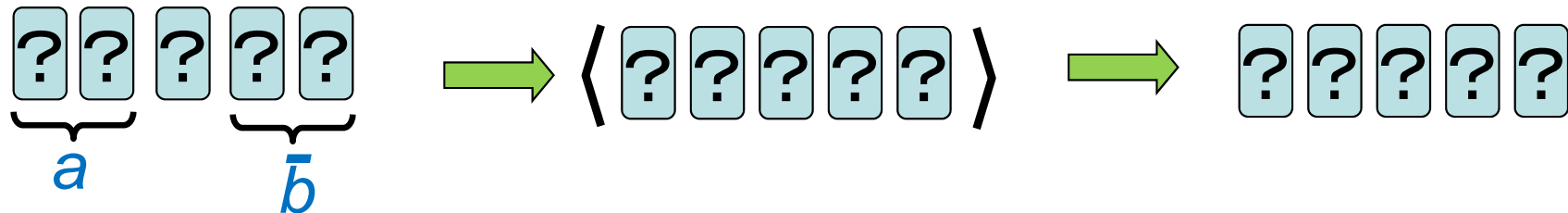
Five-card trick; **full description**



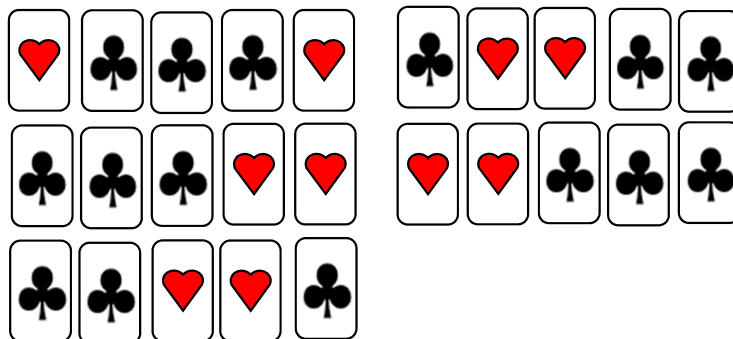
1. Put the 5 cards as follows:



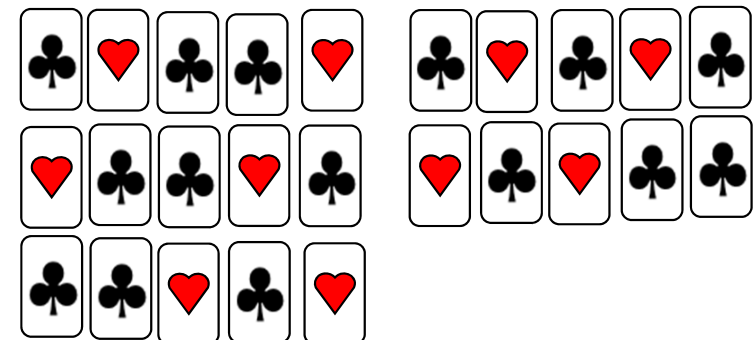
2. Turn the centered card face down, and apply a random cut:



3. Reveal all 5 cards:



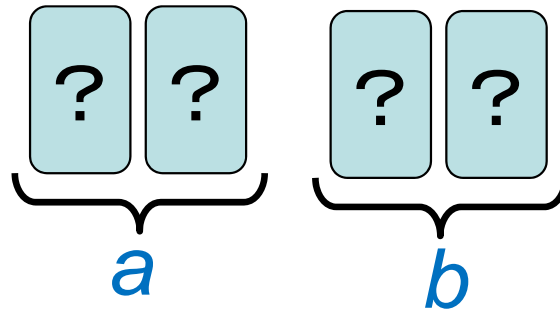
$$a \wedge b = 1$$

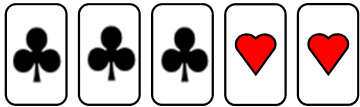
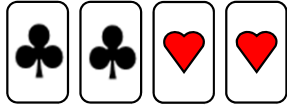


$$a \wedge b = 0$$

Our result

We reduce the number of required cards: our protocol needs no cards other than the 4 cards for commitments.



	# of required cards
den Boer [Eurocrypt '89]	5 
Ours [This paper]	4 

Contents



1. Introduction

2. Description of Our Protocol

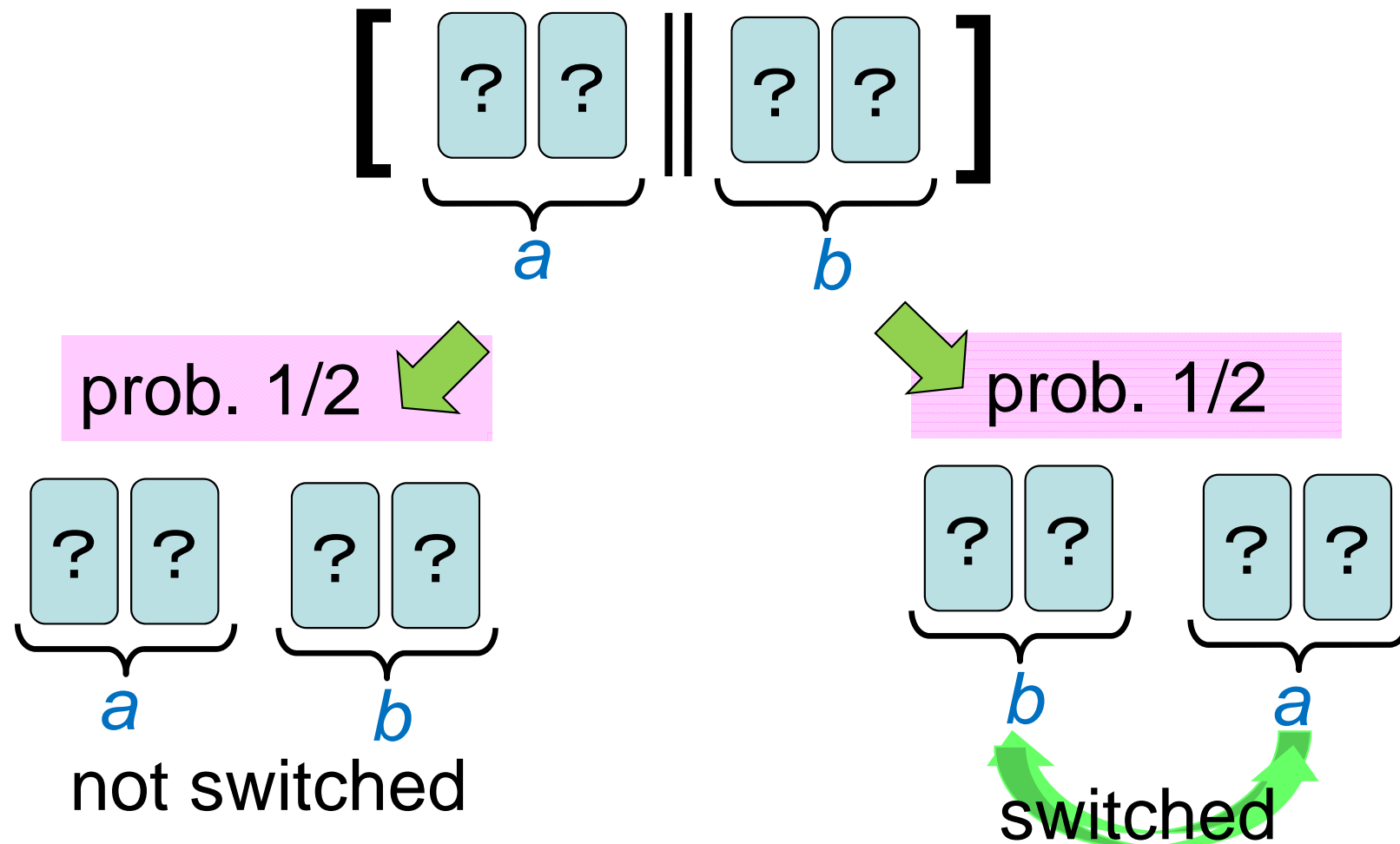
3. Correctness of Our Protocol

4. Complexity

- 2.1 Random bisection cuts
- 2.2 The protocol

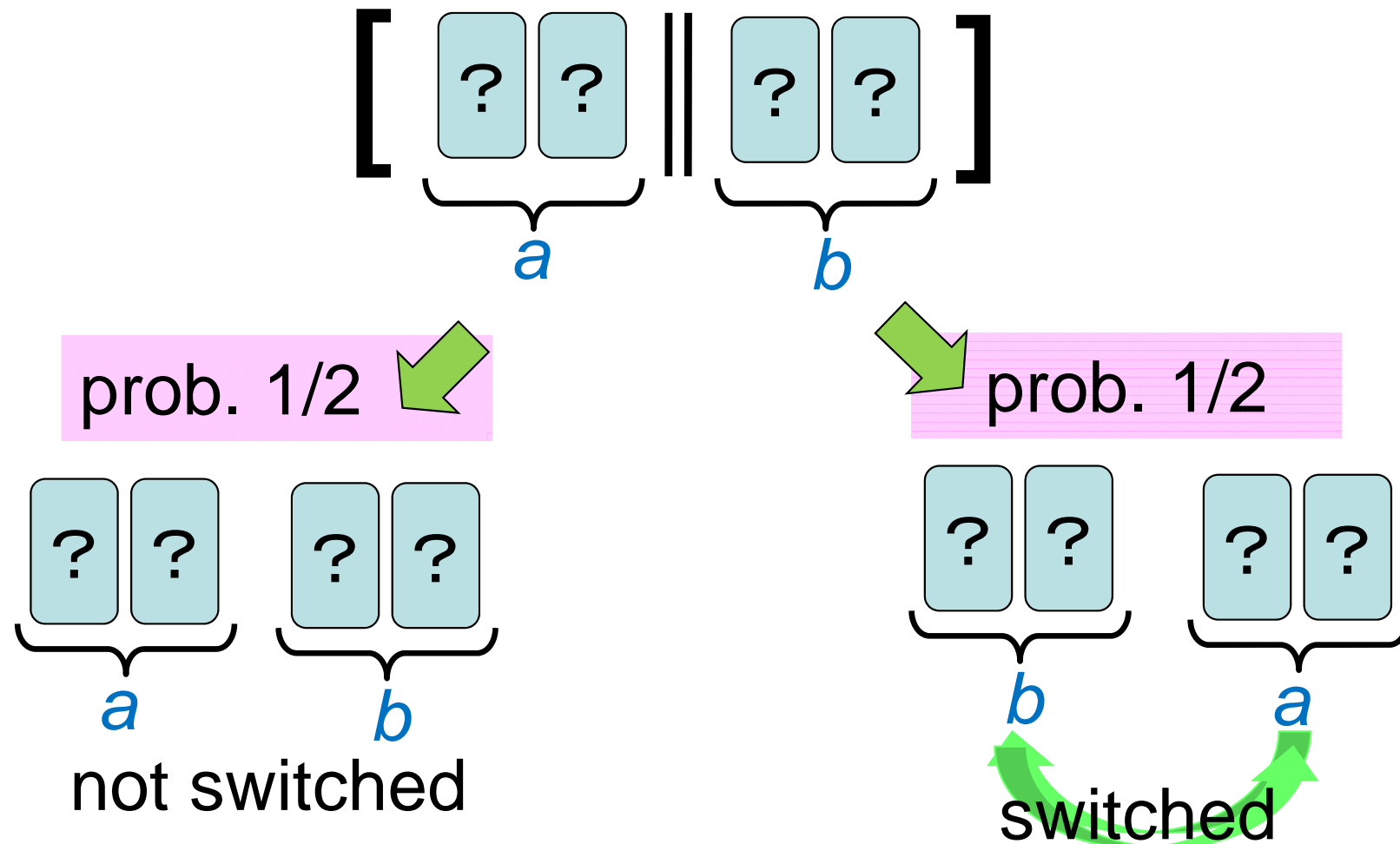
A *random bisection cut*

Bisect a given deck of cards, and then randomly switch the resulting two portions:



A *random bisection cut*

Bisect a given deck of cards, and then randomly switch the resulting two portions:



easy-to-implement card shuffling operation

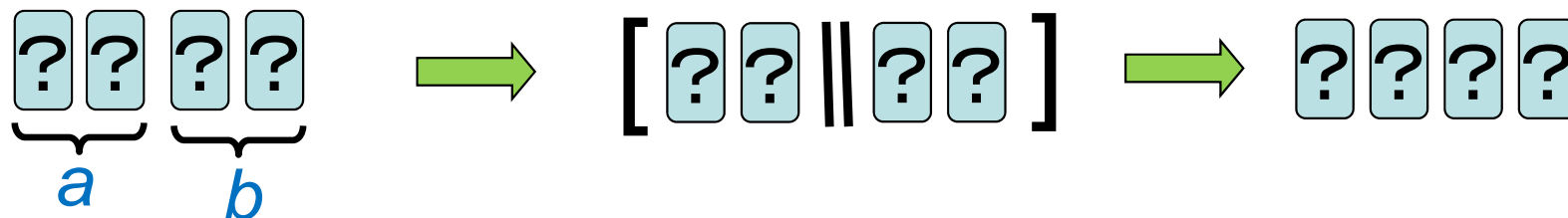
Our 4-card secure AND protocol



Our 4-card secure AND protocol

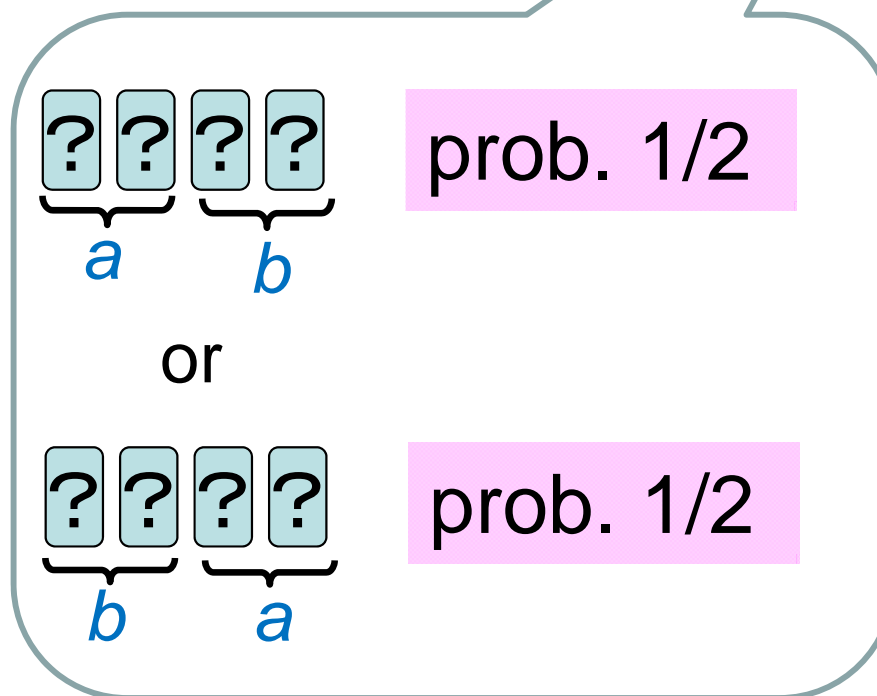
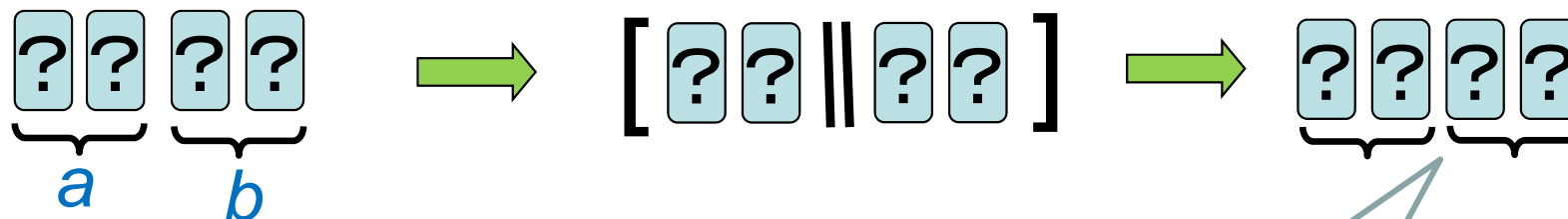


1. Apply a random bisection cut:



Our 4-card secure AND protocol

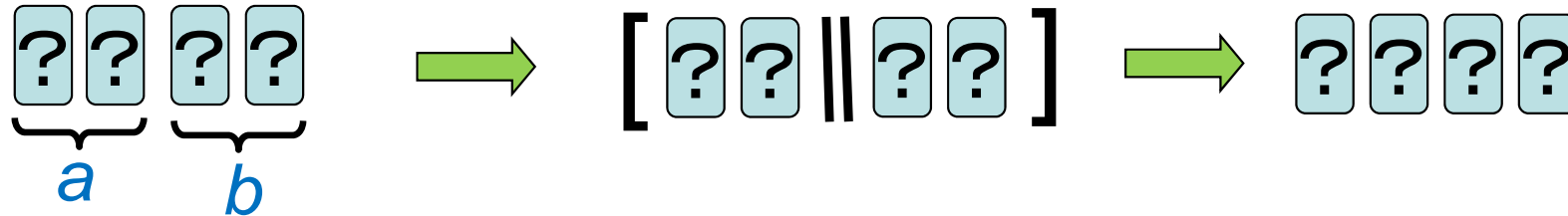
1. Apply a random bisection cut:



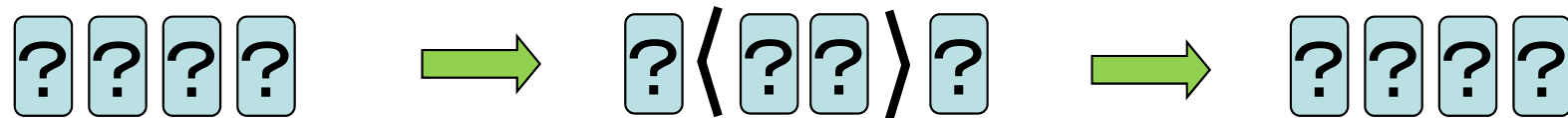
Our 4-card secure AND protocol



1. Apply a random bisection cut:

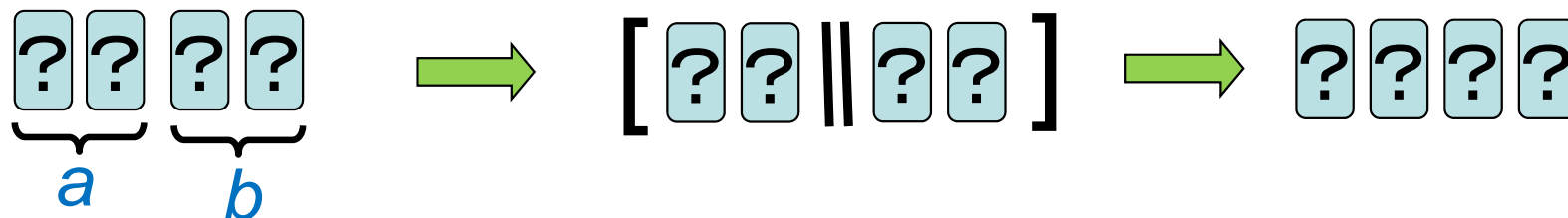


2. Apply a random cut to the two cards in the middle:

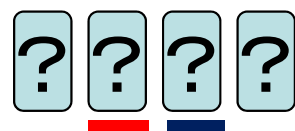
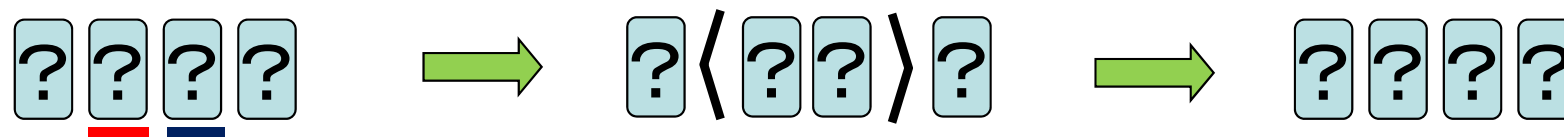


Our 4-card secure AND protocol

1. Apply a random bisection cut:

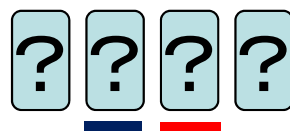


2. Apply a random cut to the two cards in the middle:



prob. $1/2$

or

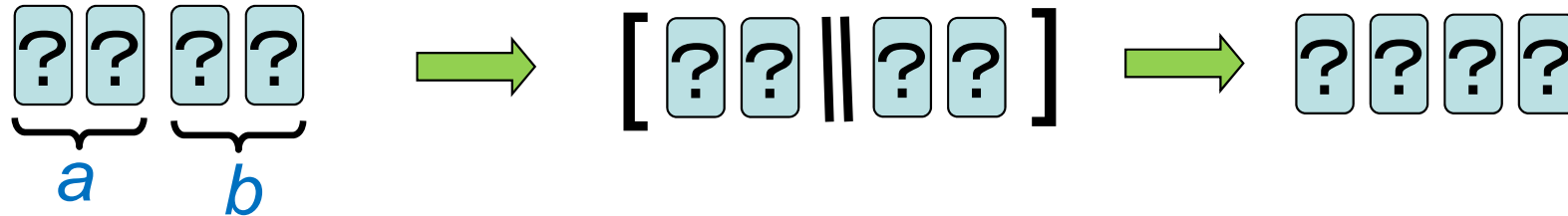


prob. $1/2$

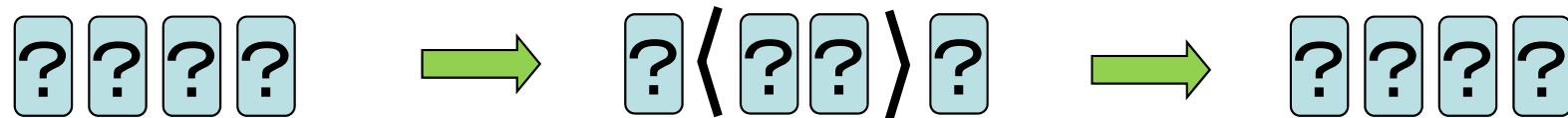
Our 4-card secure AND protocol



1. Apply a random bisection cut:



2. Apply a random cut to the two cards in the middle:

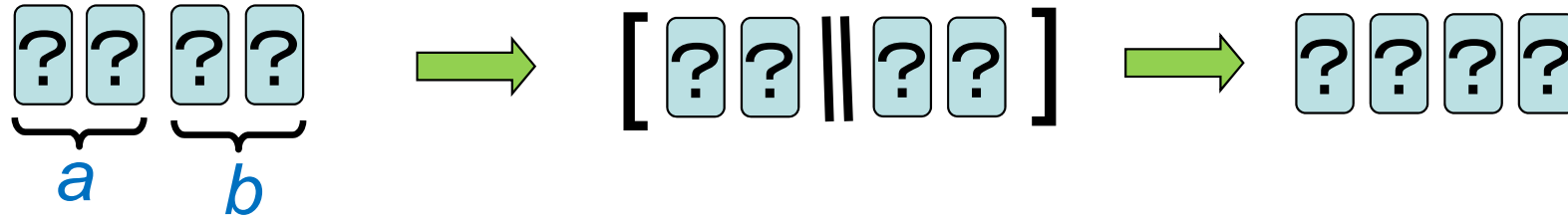


3. Reveal the 2nd card.

Our 4-card secure AND protocol



1. Apply a random bisection cut:



2. Apply a random cut to the two cards in the middle:

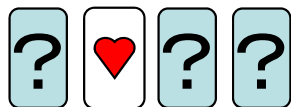


3. Reveal the 2nd card; there are two cases.

(a)



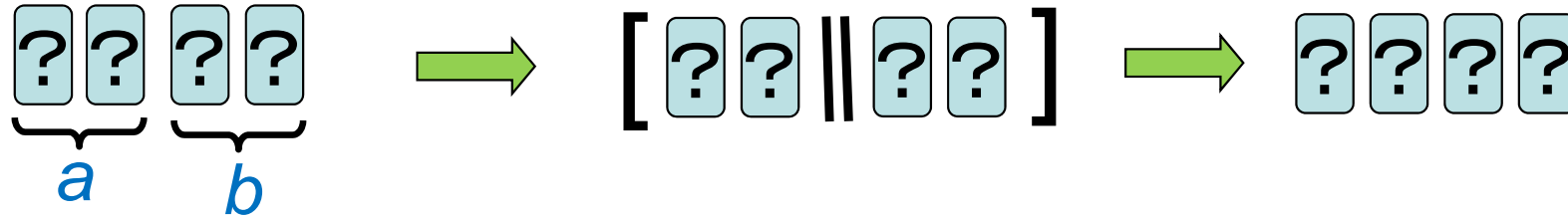
(b)



Our 4-card secure AND protocol



1. Apply a random bisection cut:

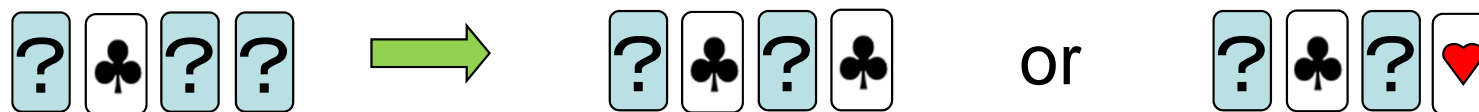


2. Apply a random cut to the two cards in the middle:



3. Reveal the 2nd card; there are two cases.

(a) Reveal the 4th card:

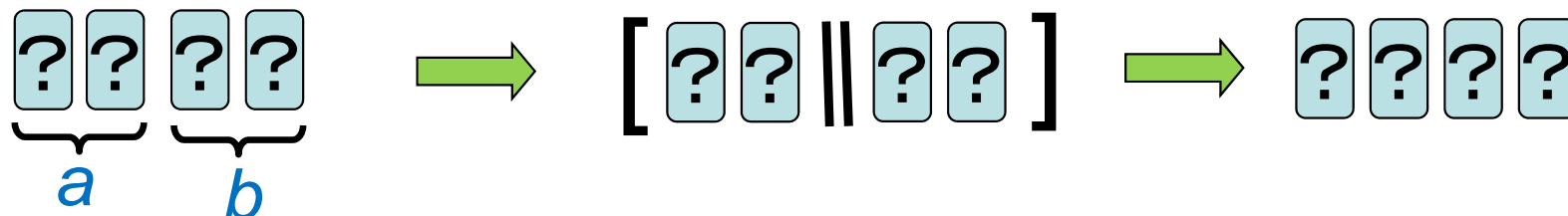


(b)

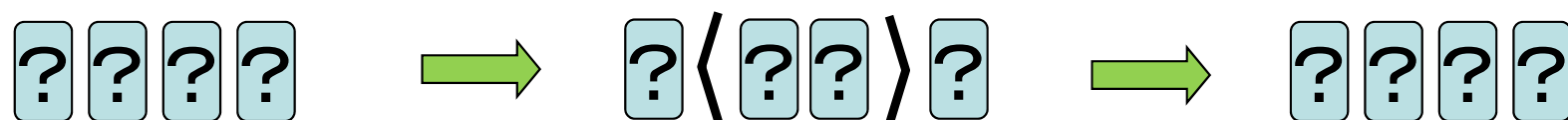


Our 4-card secure AND protocol

1. Apply a random bisection cut:



2. Apply a random cut to the two cards in the middle:



3. Reveal the 2nd card; there are two cases.

(a) Reveal the 4th card:

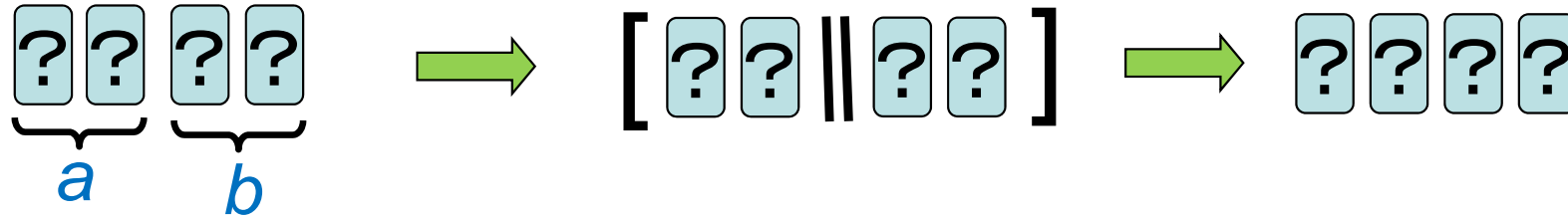


(b) Reveal the 1st card:

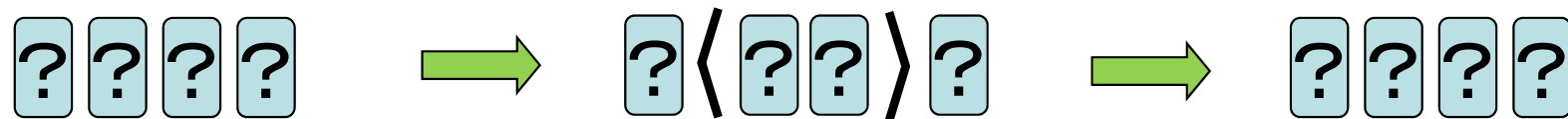


Our 4-card secure AND protocol

1. Apply a random bisection cut:

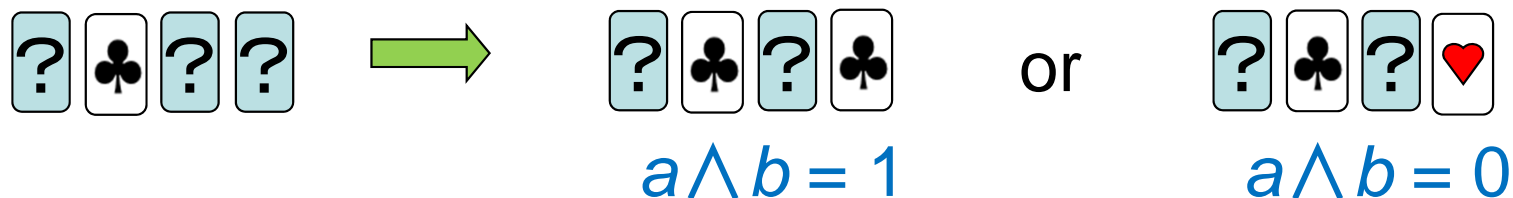


2. Apply a random cut to the two cards in the middle:

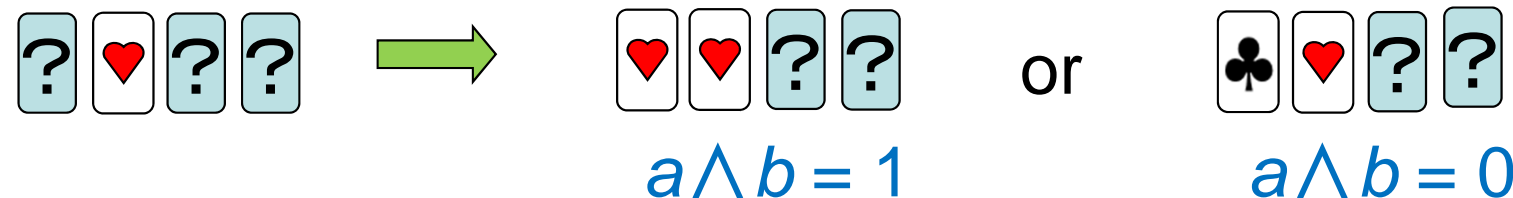


3. Reveal the 2nd card; there are two cases.

(a) Reveal the 4th card:

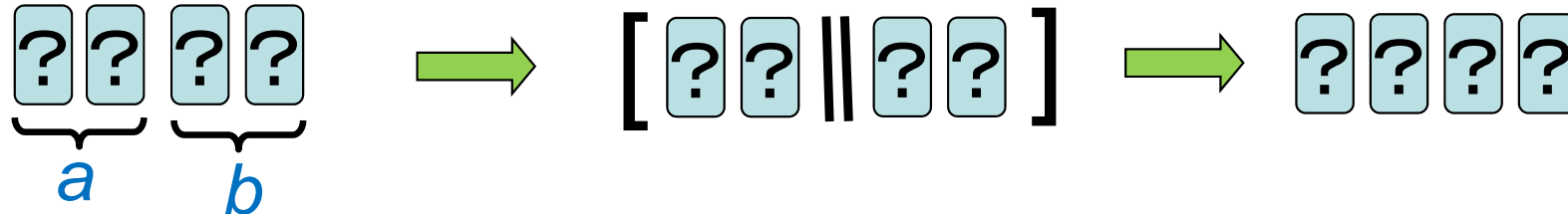


(b) Reveal the 1st card:



Our 4-card secure AND protocol

1. Apply a random bisection cut:

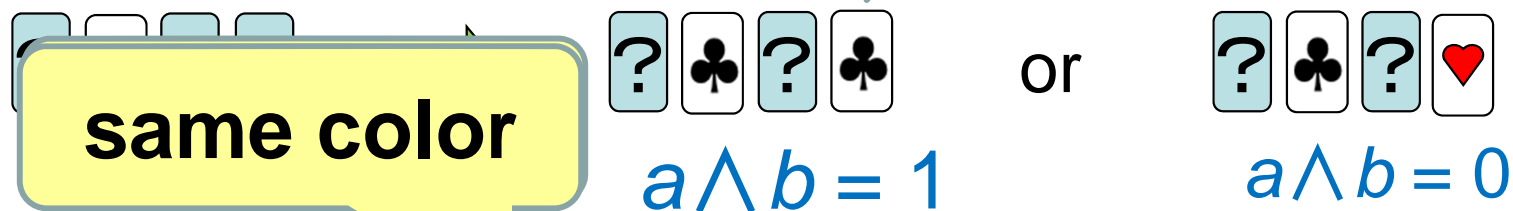


2. Apply a random cut to the two cards in the middle:

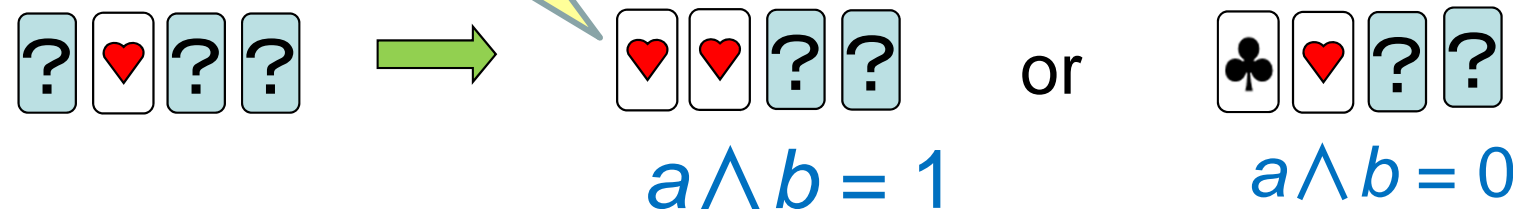


3. Reveal the 2nd card; **same color** es.

(a) Reveal the 4th card:

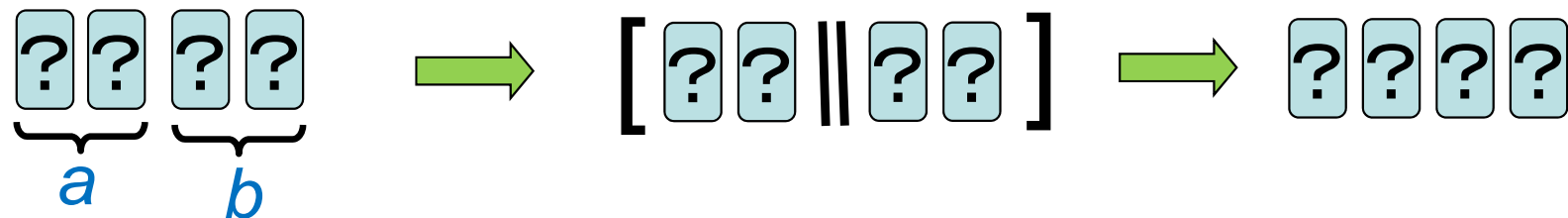


(b) Reveal the 1st card:

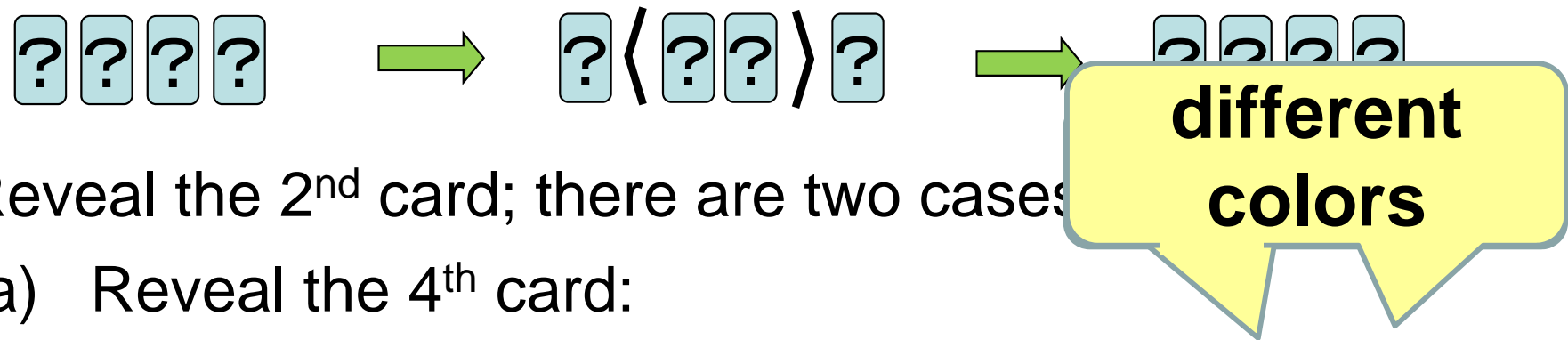


Our 4-card secure AND protocol

1. Apply a random bisection cut:



2. Apply a random cut to the two cards in the middle:

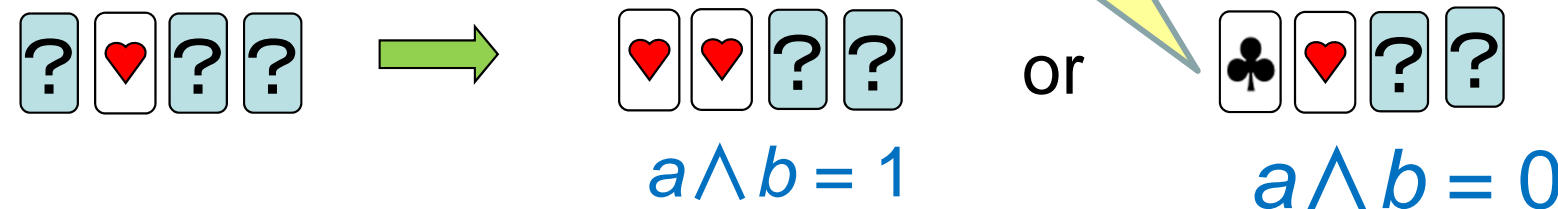


3. Reveal the 2nd card; there are two cases

(a) Reveal the 4th card:



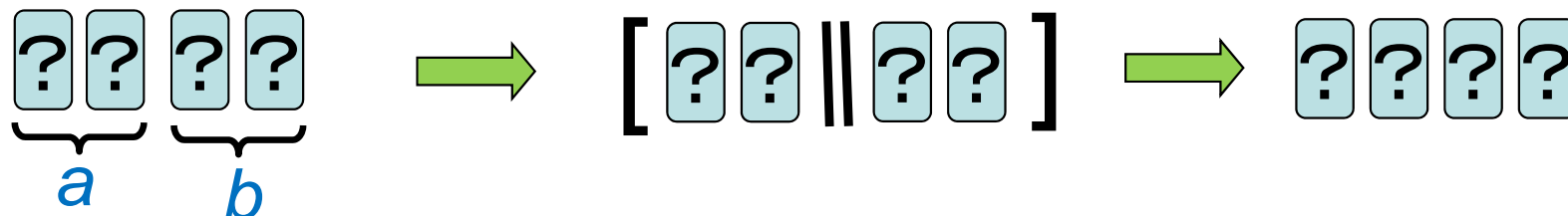
(b) Reveal the 1st card:



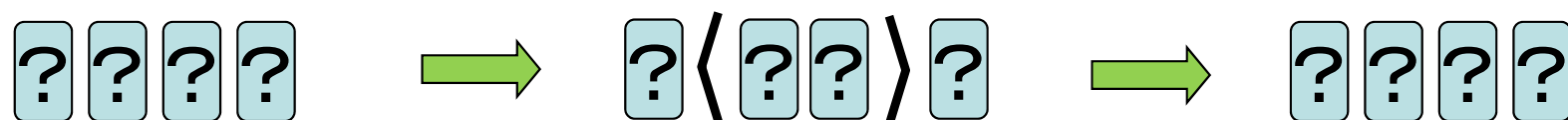
Our 4-card secure AND protocol



1. Apply a random bisection cut:

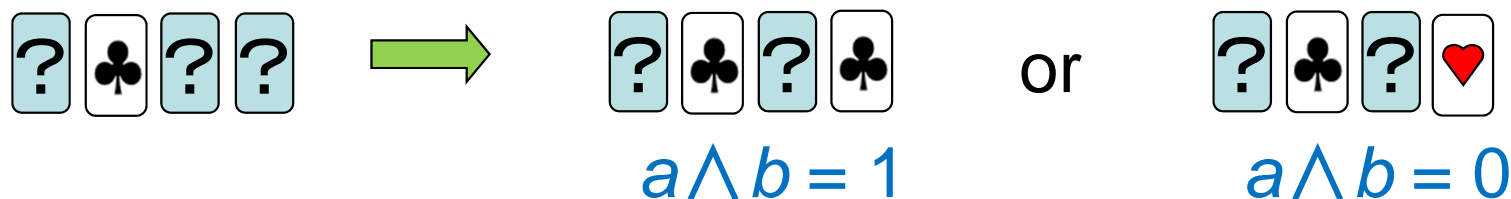


2. Apply a random cut to the two cards in the middle:

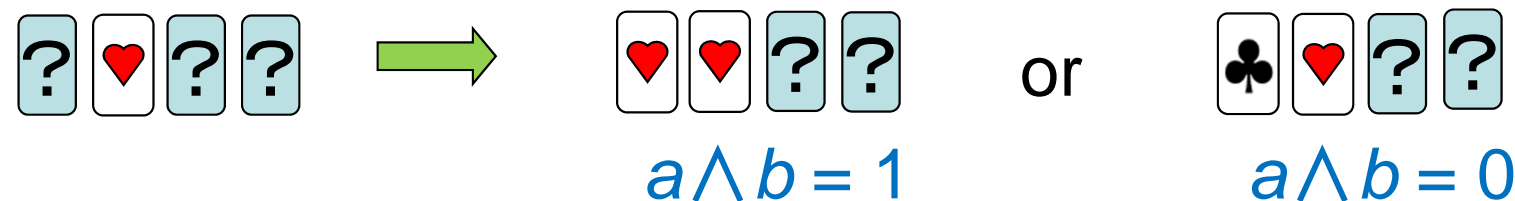


3. Reveal the 2nd card; there are two cases.

(a) Reveal the 4th card:



(b) Reveal the 1st card:



Contents

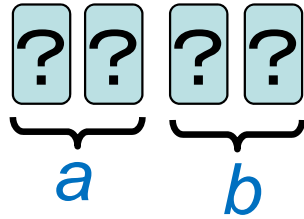


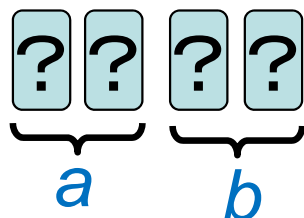
1. Introduction

2. Description of Our Protocol

3. Correctness of Our Protocol

















4. Conclusions









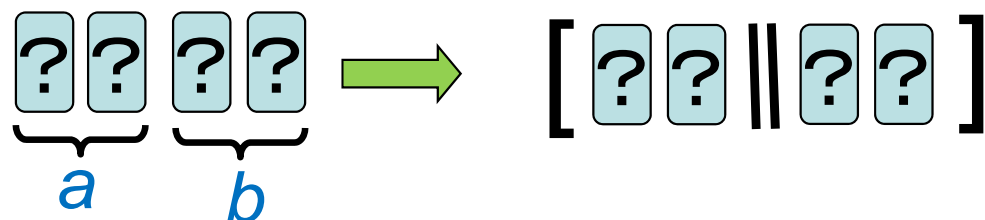
(a,b)

initial

$(0,0)$	   
$(0,1)$	   
$(1,0)$	   
$(1,1)$	   

















  = 0   = 1

step 1



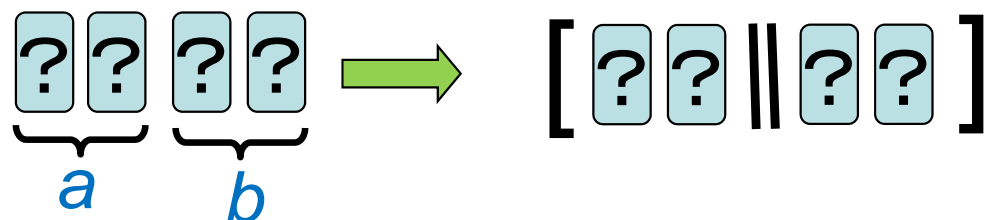
(a,b)

initial

















$(0,0)$	   
$(0,1)$	   
$(1,0)$	   
$(1,1)$	   

$\left[\begin{array}{cc} \text{club} & \text{heart} \\ \text{heart} & \text{club} \end{array} \right]$

$\text{club heart} = 0 \quad \text{heart club} = 1$

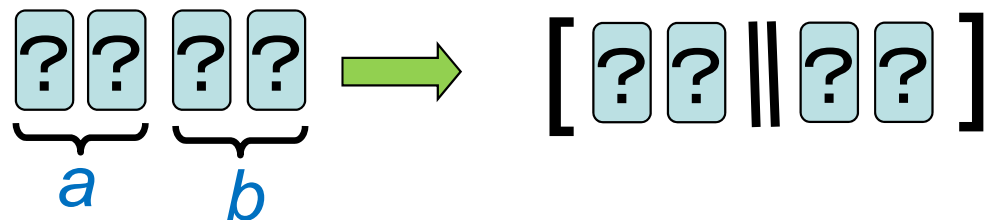


(a,b) initial

$(0,0)$	   
$(0,1)$	   
$(1,0)$	   
$(1,1)$	   

after step 1

$$\left[\begin{array}{cc} \text{club} & \text{heart} \\ \hline \text{heart} & \text{club} \end{array} \right] = 0 \quad \text{heart} \text{ club} = 1$$



(a,b) initial

$(0,0)$	♣♥♣♥
$(0,1)$	♣♥♥♣
$(1,0)$	♥♣♣♥
$(1,1)$	♥♣♥♣

after step 1

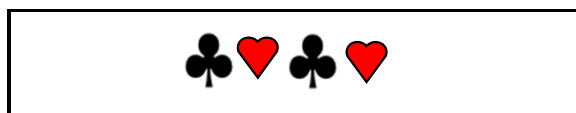
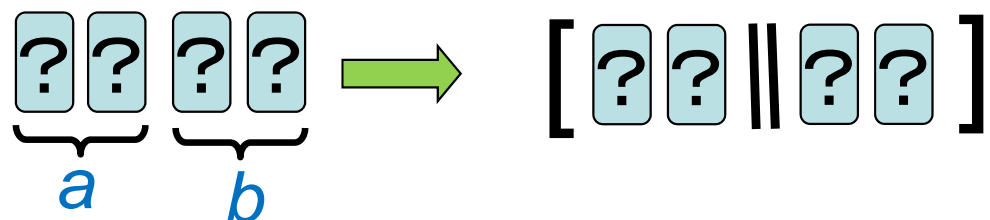


















Diagram illustrating the mapping of card pairs to binary values:

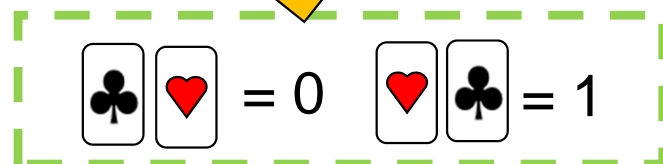
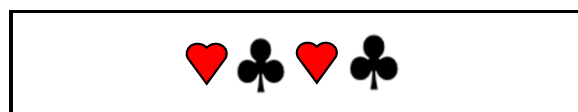
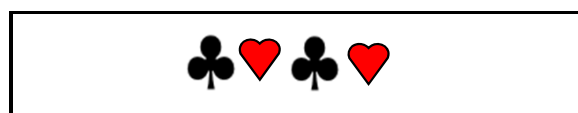
$\text{♣♥} = 0$ $\text{♥♣} = 1$

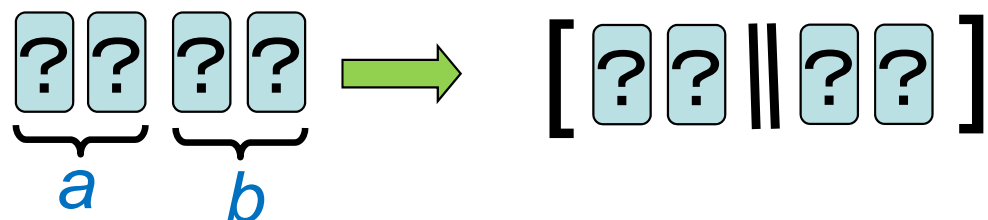


(a,b) initial

















$(0,0)$	   
$(0,1)$	   
$(1,0)$	   
$(1,1)$	   

after step 1





















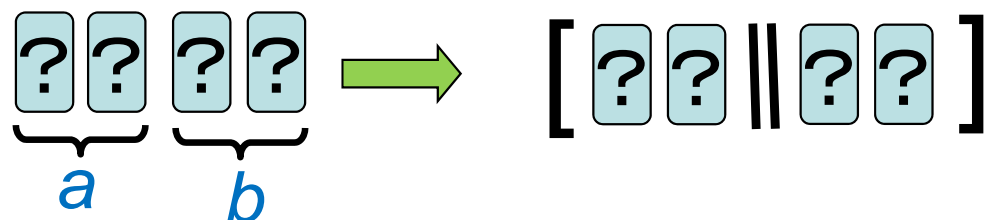
(a,b) initial

$(0,0)$	   
$(0,1)$	   
$(1,0)$	   
$(1,1)$	   

















after step 1

   
    or    
   

















$\begin{bmatrix} \text{Club} \text{ Heart} = 0 & \text{Heart} \text{ Club} = 1 \end{bmatrix}$







(a,b) initial

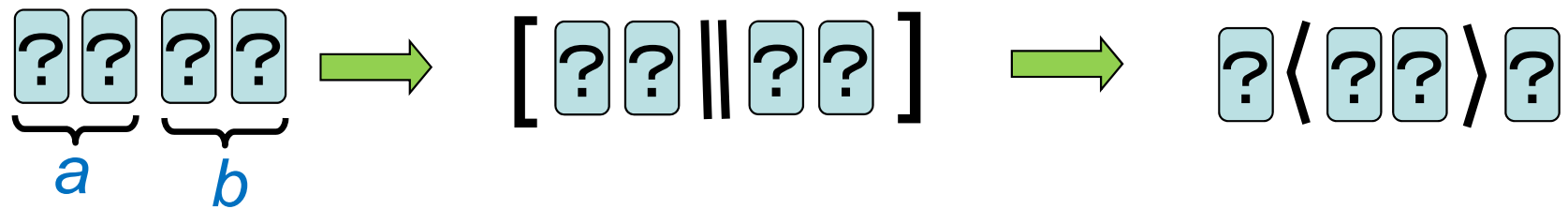
$(0,0)$	   
$(0,1)$	   
$(1,0)$	   
$(1,1)$	   

after step 1

   
    or    
same as $(0,1)$
   

  = 0   = 1

step 2



































(a,b)





initial

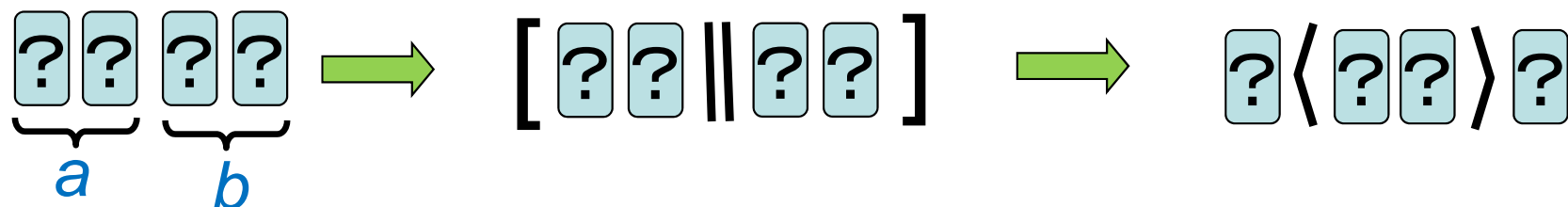
after step 1

$(0,0)$
$(0,1)$
$(1,0)$
$(1,1)$

   
    or    
same as $(0,1)$
   

  = 0   = 1



(a,b)

initial

$(0,0)$	♣♥♣♥
$(0,1)$	♣♥♥♣
$(1,0)$	♥♣♣♥
$(1,1)$	♥♣♥♣

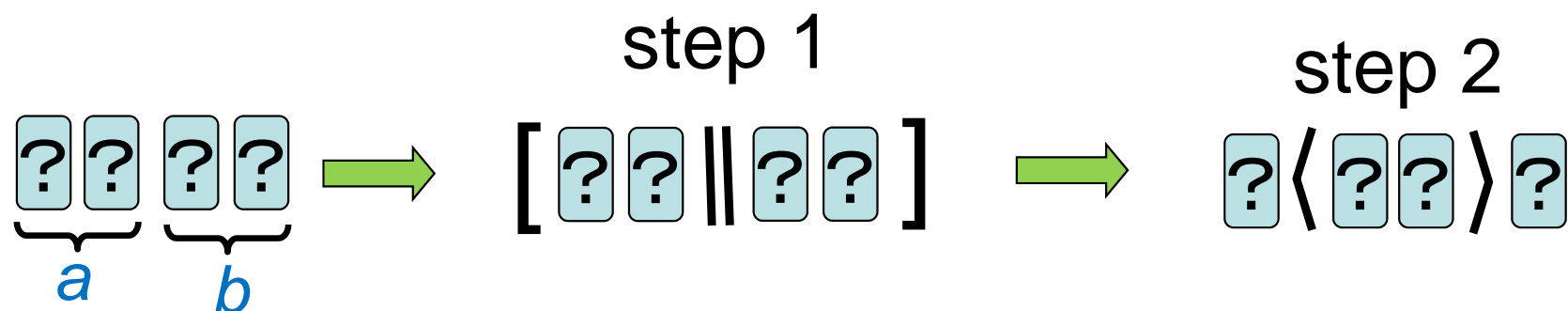
after step 1

♣♥♣♥
♣♥♥♣ or ♥♣♣♥
same as $(0,1)$
♥♣♥♣

after step 2

♣♣♥♥ or ♣♥♣♥
♥♣♣♥ or ♣♥♥♣
same as $(0,1)$
♥♣♥♣ or ♥♥♣♣

♣♥ = 0 ♥♣ = 1

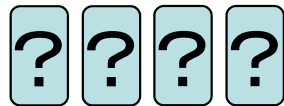


(a,b)

before step 3

$(0,0)$	♣♣♥♥ or ♣♥♣♥
$(0,1)$	♥♣♣♥ or ♣♥♥♣
$(1,0)$	♥♣♣♥ or ♣♥♥♣
$(1,1)$	♥♣♥♣ or ♥♥♣♣

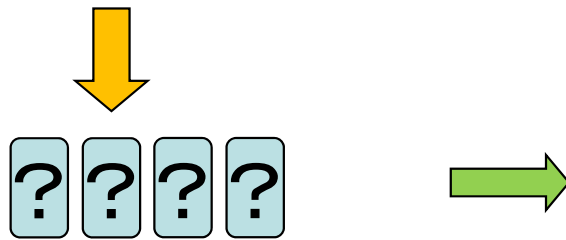
Step 3 reveals the 2nd card.



(a,b)

$(0,0)$	♣♣♥♥ or ♣♥♣♥
$(0,1)$	♥♣♣♥ or ♣♥♥♣
$(1,0)$	♥♣♣♥ or ♣♥♥♣
$(1,1)$	♥♣♥♣ or ♥♥♣♣

Step 3 reveals the 2nd card.



(a) ? ♣ ? ?

(b) ? ♥ ? ?

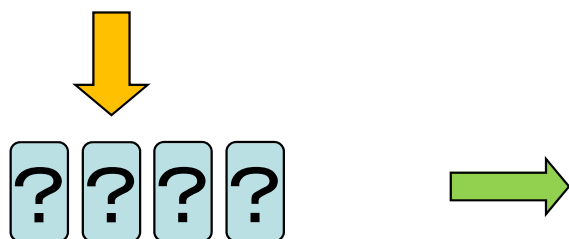
(a, b)

$(0, 0)$	♣♣♥♥ or ♣♥♣♥
$(0, 1)$	♥♣♣♥ or ♣♥♥♣
$(1, 0)$	♥♣♣♥ or ♣♥♥♣
$(1, 1)$	♥♣♥♣ or ♥♥♣♣

(a)

(b)

Step 3 reveals the 2nd card.

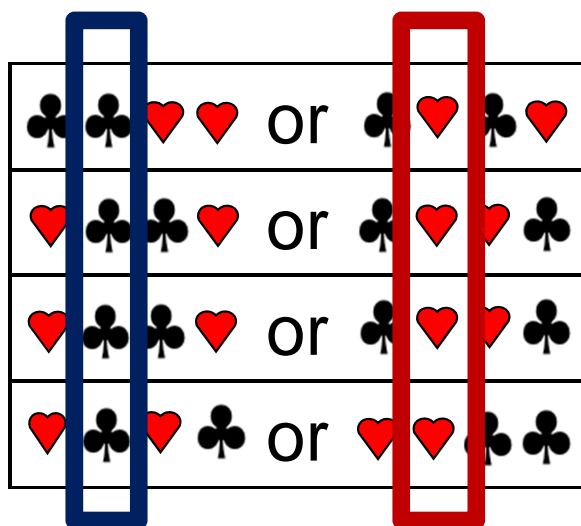


(a) ? ♣ ? ?

(b) ? ♥ ? ?

(a,b)

$(0,0)$
$(0,1)$
$(1,0)$
$(1,1)$

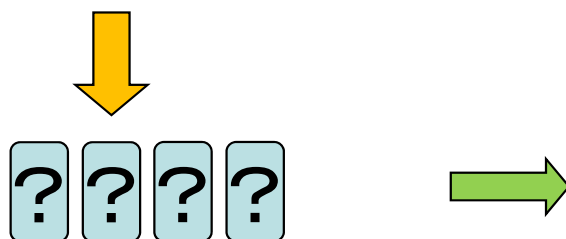


(a)

(b)

The color and (a,b) are independent.

Step 3 reveals the 2nd card.

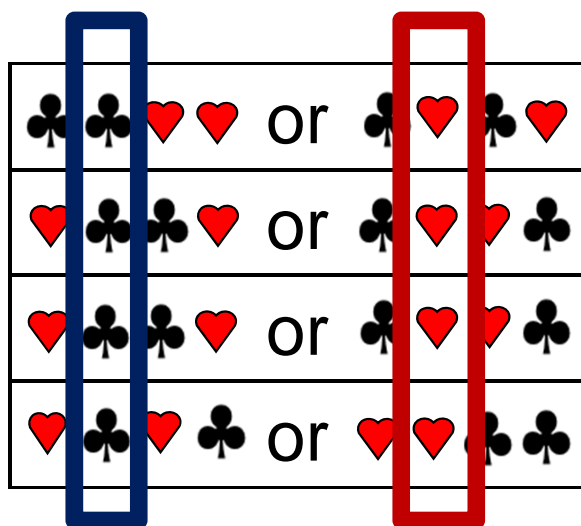


(a) ? ♣ ? ?

(b) ? ♥ ? ?

(a,b)

$(0,0)$
$(0,1)$
$(1,0)$
$(1,1)$



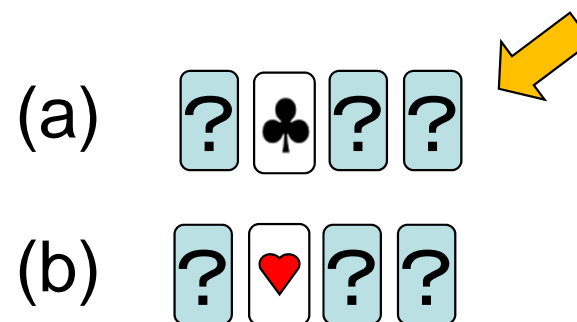
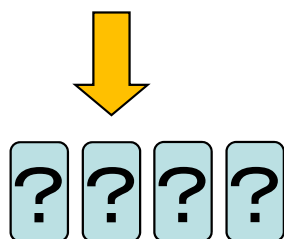
(a)

(b)

The color and (a,b) are independent.

No secret information leaks.

Step 3 reveals the 2nd card.



(a,b)

$(0,0)$	♣ ♣ ♥ ♥ or ♣ ♥ ♣ ♥
$(0,1)$	♥ ♣ ♣ ♥ or ♣ ♥ ♥ ♣
$(1,0)$	♥ ♣ ♣ ♥ or ♣ ♥ ♥ ♣
$(1,1)$	♥ ♣ ♥ ♣ or ♥ ♥ ♣ ♣

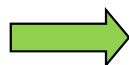
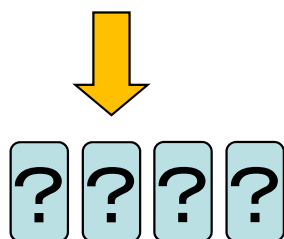
(a)

(b)

The color and (a,b) are independent.

No secret information leaks.

Step 3 reveals the 2nd card.



(0,0)
(0,1)
(1,0)
(1,1)

♣♣♥♥ or ♣♥♣♥
♥♣♣♥ or ♣♥♥♣
♥♣♣♥ or ♣♥♥♣
♥♣♥♣ or ♥♥♣♣

(a)

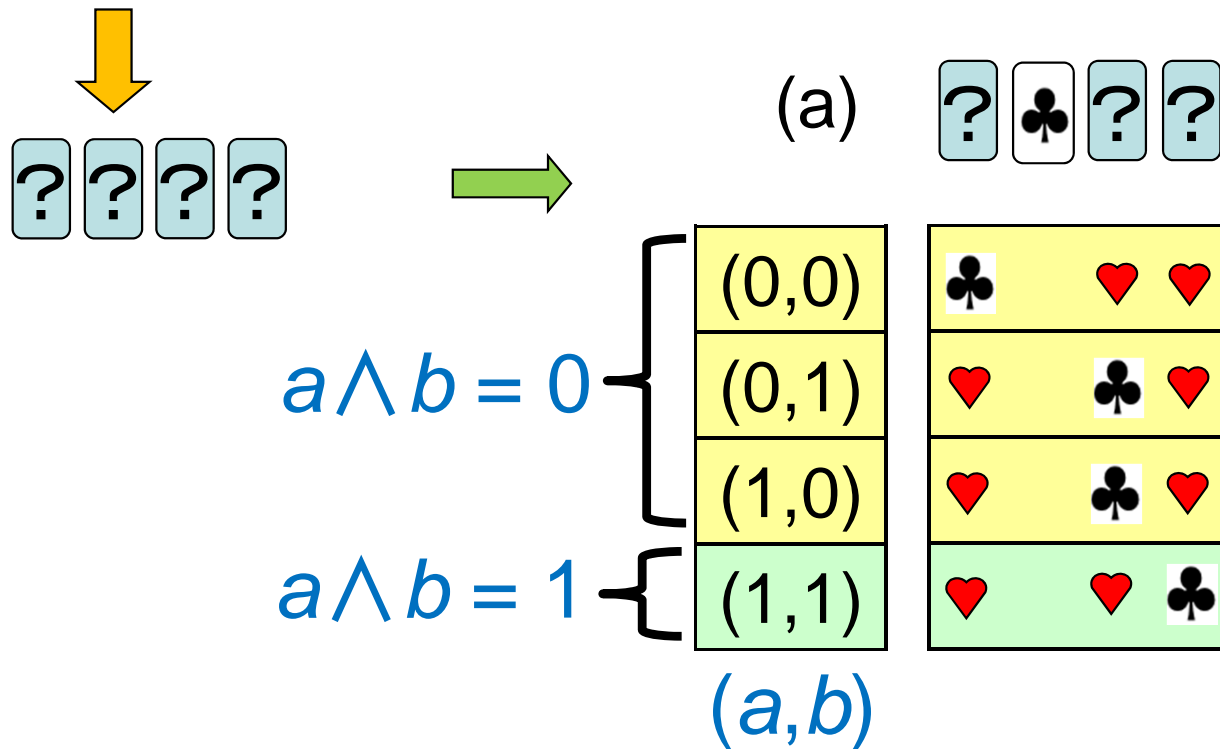
(b)

(0,0)
(0,1)
(1,0)
(1,1)

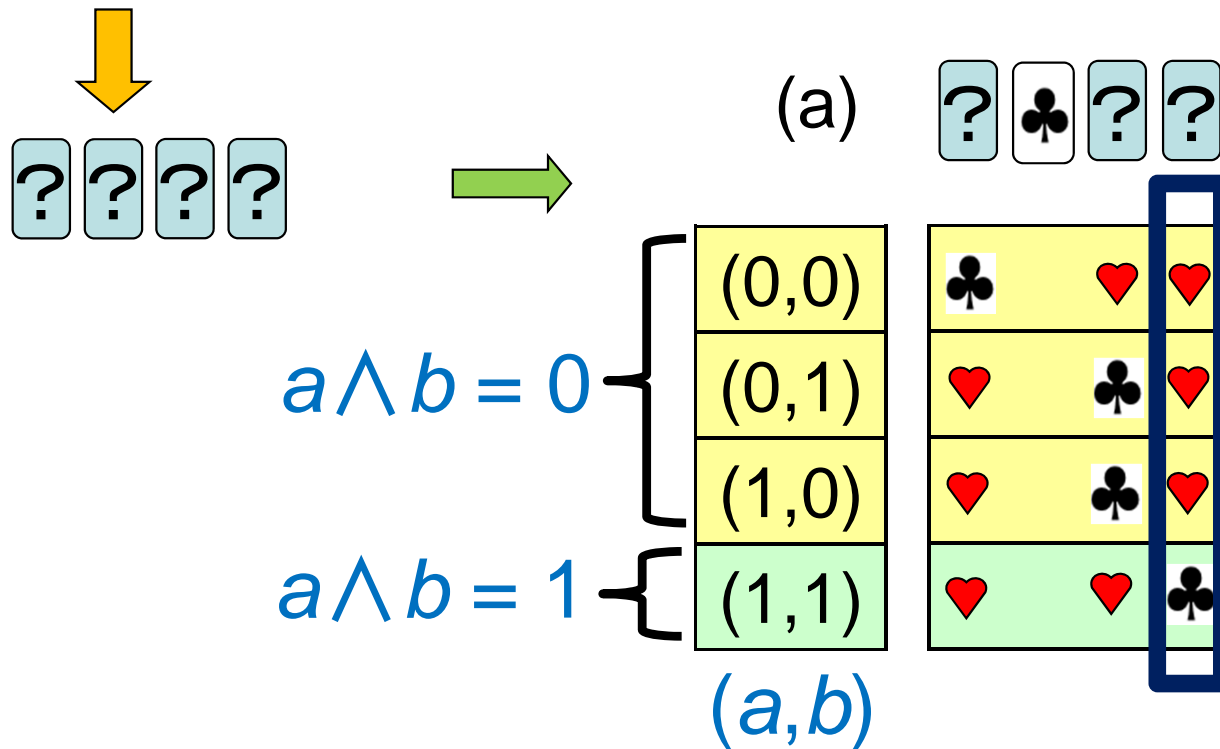
(a,b)

♣♥♥
♥♣♥
♥♣♥
♥♥♣

Step 3 reveals the 2nd card.

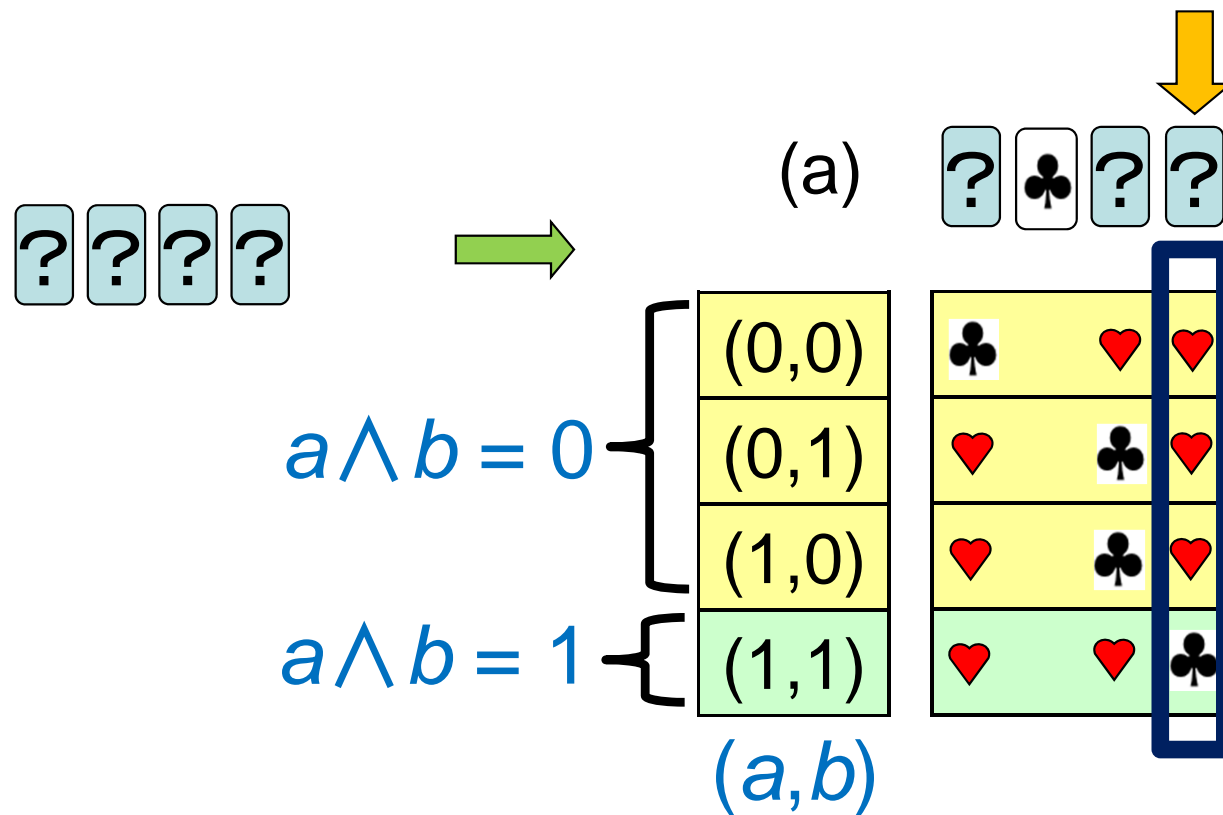


Step 3 reveals the 2nd card.



It suffices to look at the color of the fourth card.

Step 3(a) reveals the 4th card.



(a) Reveal the 4th card:

(a,b)

$(0,0)$
$(0,1)$
$(1,0)$
$(1,1)$

♣		♥	♥
♥		♣	♥
♥		♣	♥
♥	♥		♣



$$a \wedge b = 1$$

or

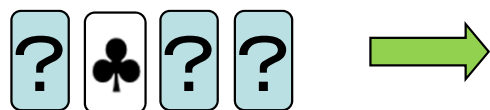


$$a \wedge b = 0$$

(a) Reveal the 4th card:

(a,b)

(0,0)	♣	♥	♥
(0,1)	♥	♣	♥
(1,0)	♥	♣	♥
(1,1)	♥	♥	♣



or



(b) Reveal the 1st card:

(0,0)	♣	♣	♥
(0,1)	♣	♥	♣
(1,0)	♣	♥	♣
(1,1)	♥	♣	♣



or

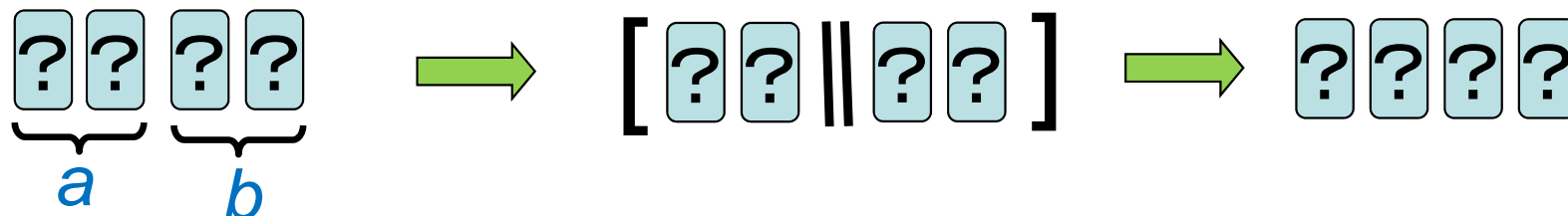


Our 4-card secure AND protocol

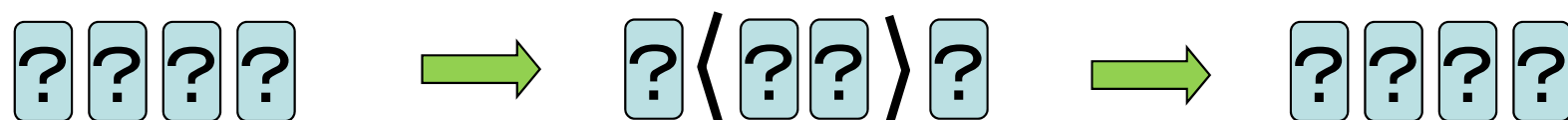


works!

1. Apply a random bisection cut:

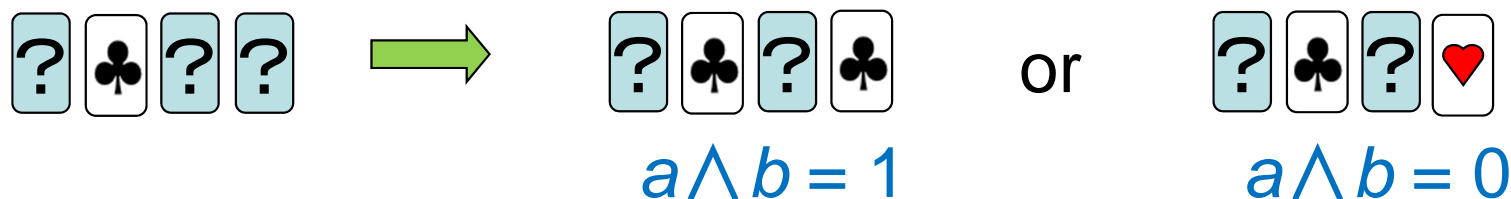


2. Apply a random cut to the two cards in the middle:

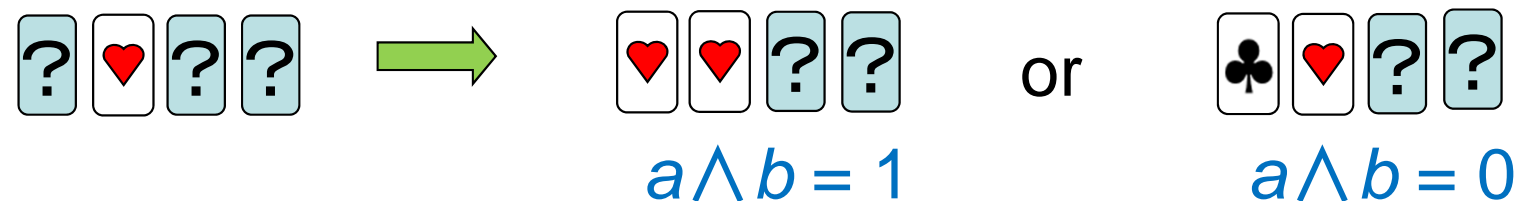


3. Reveal the 2nd card; there are two cases.

(a) Reveal the 4th card:



(b) Reveal the 1st card:



Contents



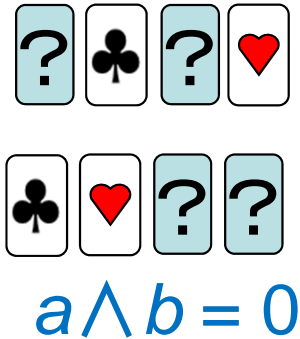
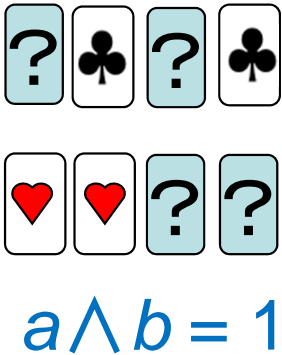
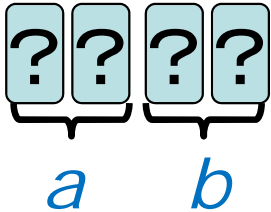
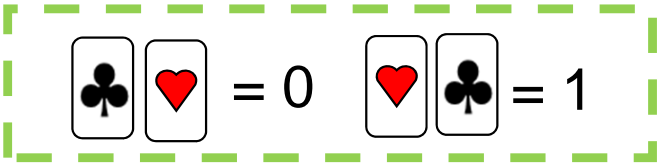
1. Introduction

2. Description of Our Protocol

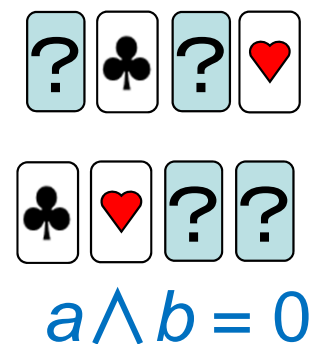
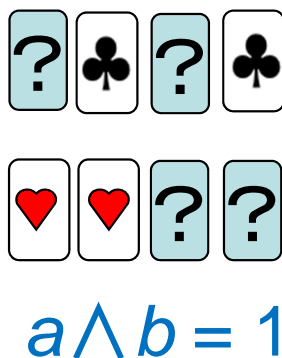
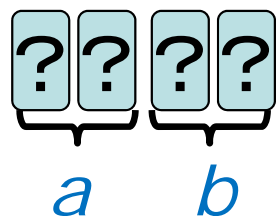
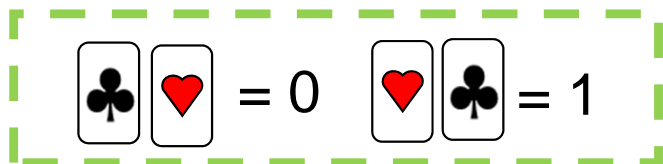
3. Correctness of Our Protocol

4. Conclusions

We gave a 4-card secure AND protocol.

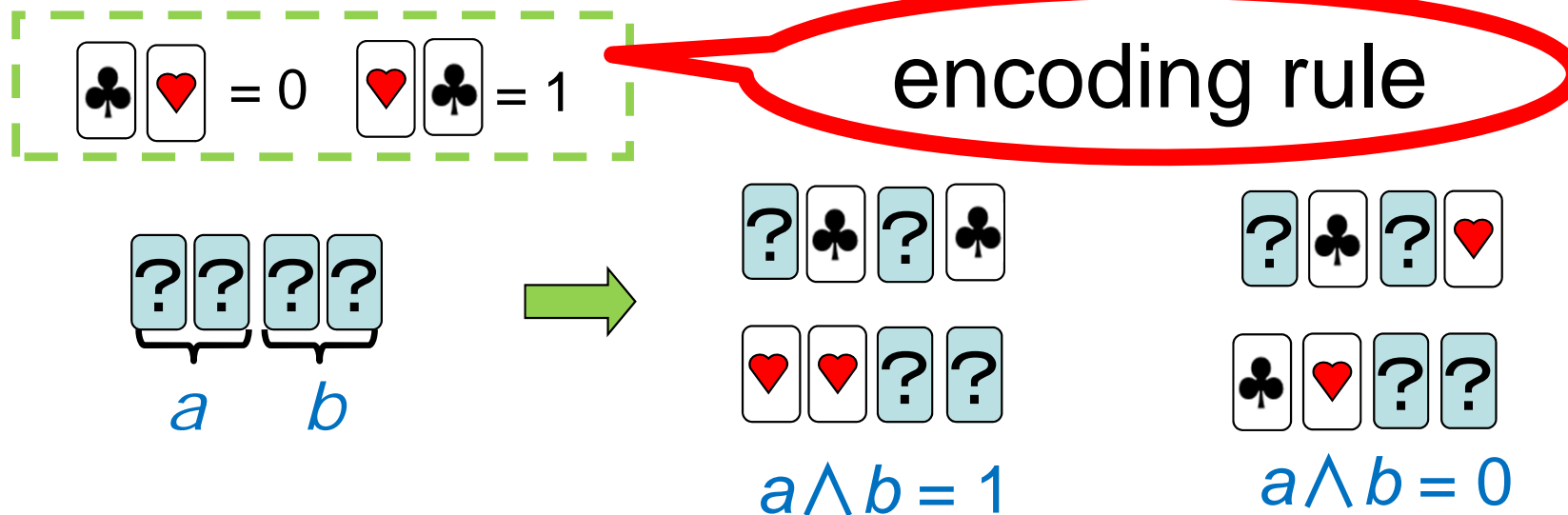


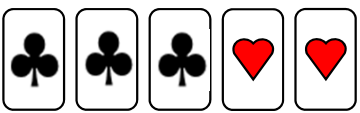
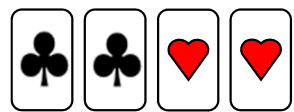
We gave a 4-card secure AND protocol.



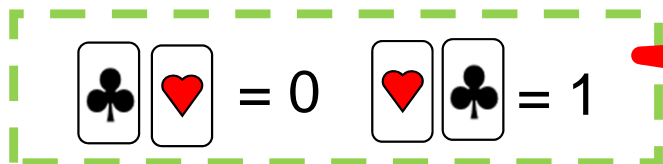
	# of cards	random cut	bisection
den Boer [Eurocrypt '89]	5 	✓	
Ours [This paper]	4 	✓	✓

We gave a 4-card secure AND protocol.

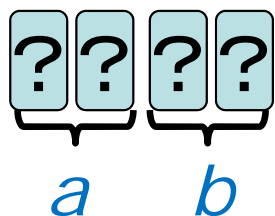


	# of cards	random cut	bisection
den Boer [Eurocrypt '89]	5 	✓	
Ours [This paper]	4 	✓	✓

We gave a 4-card secure AND protocol.



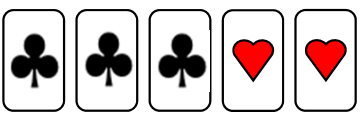
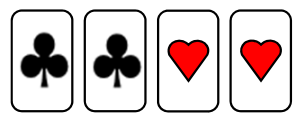
encoding rule



$a \wedge b = 1$

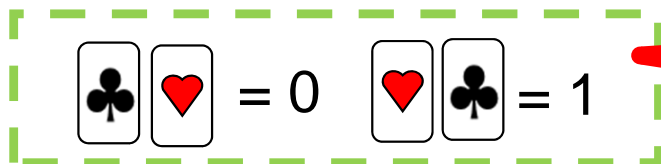


$a \wedge b = 0$

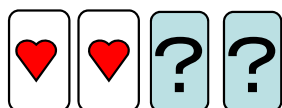
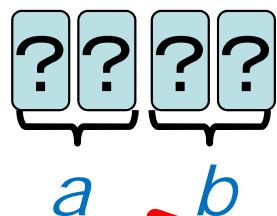
	# of cards	random cut	bisection
den Boer [Eurocrypt '89]	5 	✓	
Ours [This paper]	4 	✓	✓

optimal

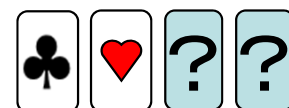
We gave a 4-card secure AND protocol.



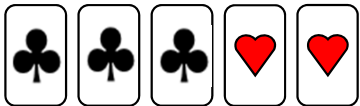
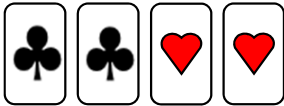
encoding rule



$a \wedge b = 1$

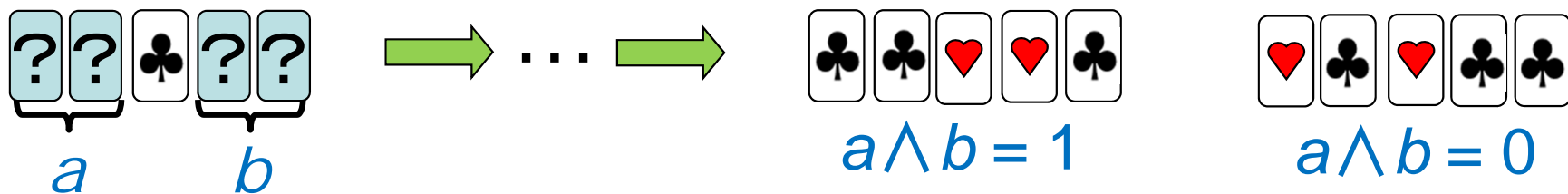


$a \wedge b = 0$

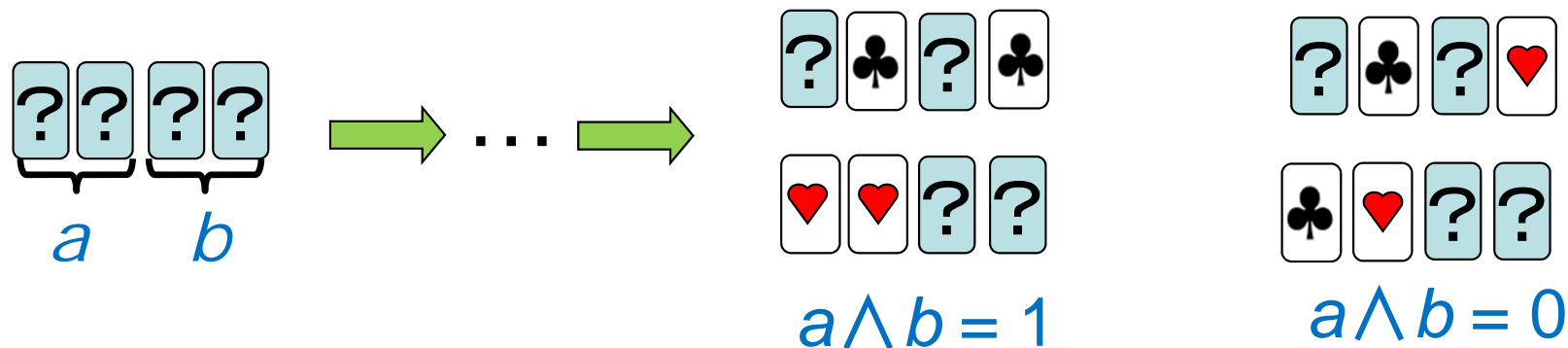
	two input commitments		bisection
den Boer [Eurocrypt '89]	5 	✓	
Ours [This paper]	4 	✓	✓

optimal

The five-card trick

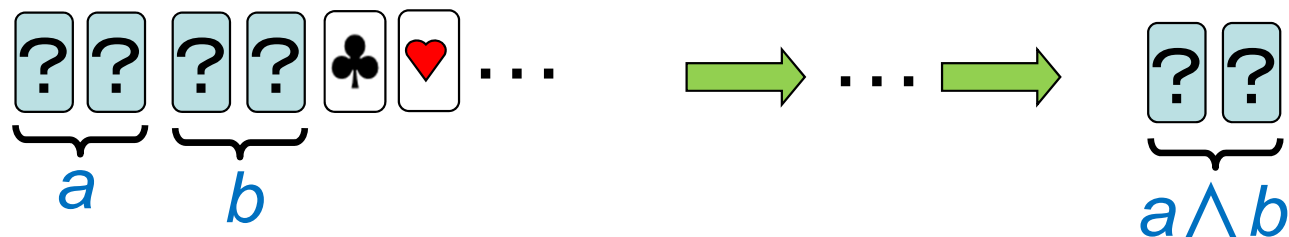


and our protocol

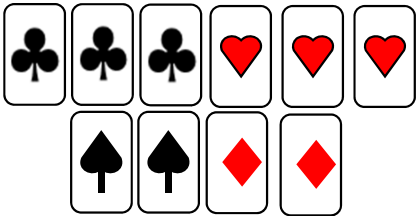
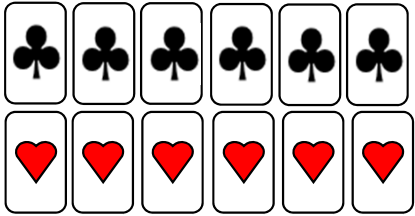
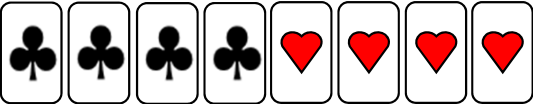
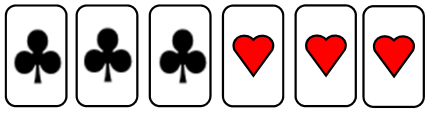


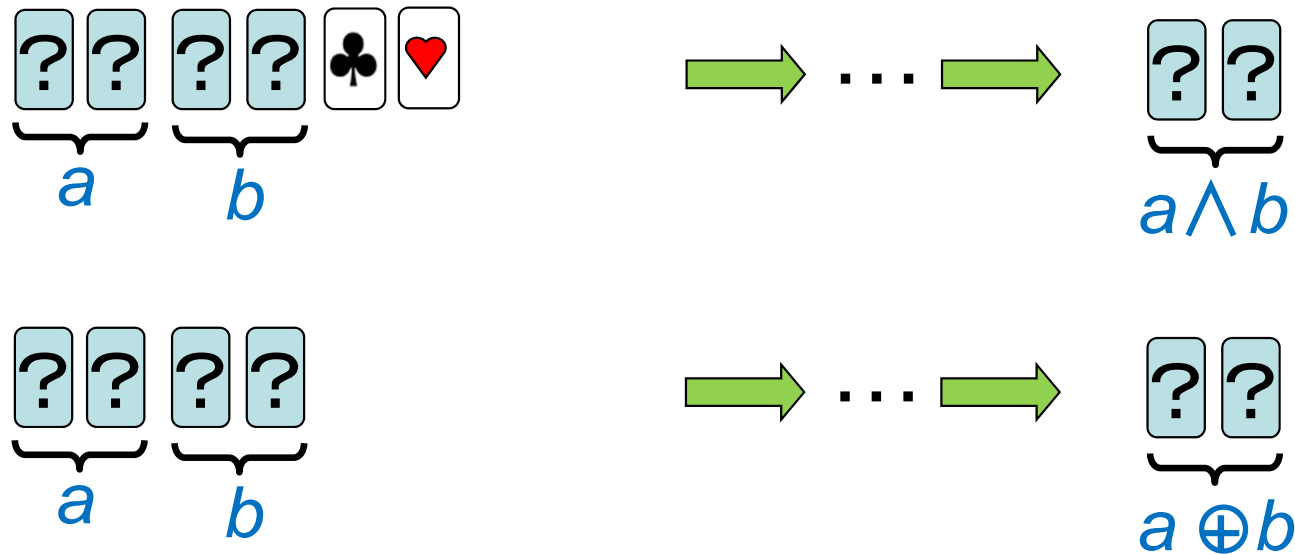
do not produce their output in a **committed format**.

There are some committed format protocols.



Committed-format secure AND protocols

	required cards	random cut	bisection cut	avg. # of trials
Crepeau-Kilian [CRYPTO '93]	10 	✓		6
Niemi-Renvall [TCS, 1998]	12 	✓		2.5
Stiglic [TCS, 2001]	8 	✓		2
Mizuki-Sone [FAW 2009]	6 		✓	1



Also, some known protocols securely compute XOR and NOT in a committed format.

Therefore, ***any*** (n -variable m -valued) ***function*** can be securely computed using a deck of cards.

I hope card-based protocols would help you with

- intuitive explanation of crypto. to non-specialists
- education in classroom.

That's all.

Thank you for your attention.



A (real) deck of cards available to the first several people; please contact the speaker.

