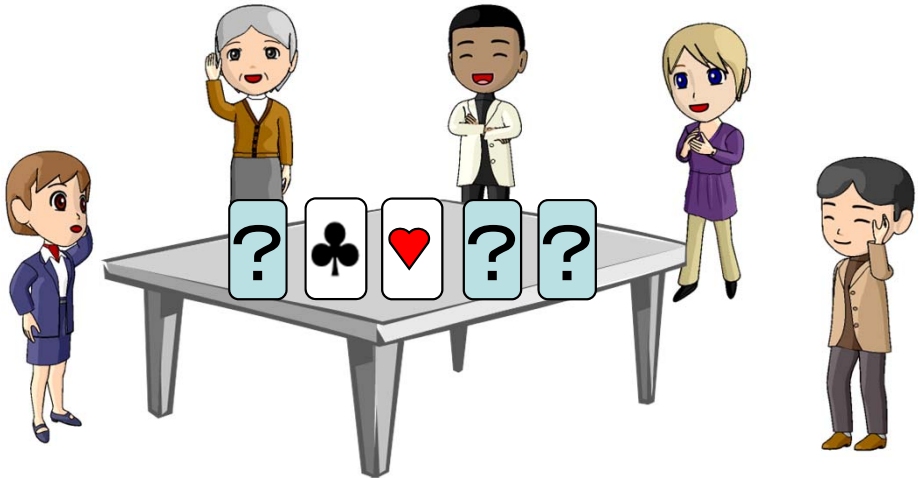
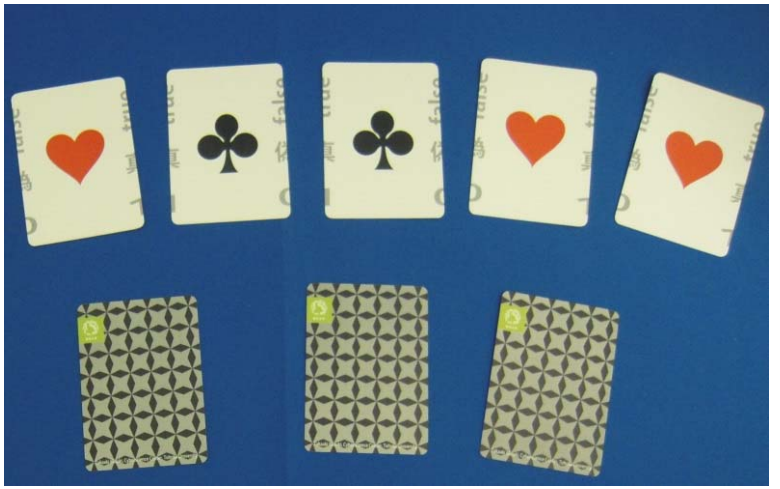




Practical Card-Based Cryptography

Takaaki Mizuki and Hiroki Shizuya

Tohoku University

FUN 2014 (16:55-17:20, Jul. 1, 2014, Lipari Island)

Contents

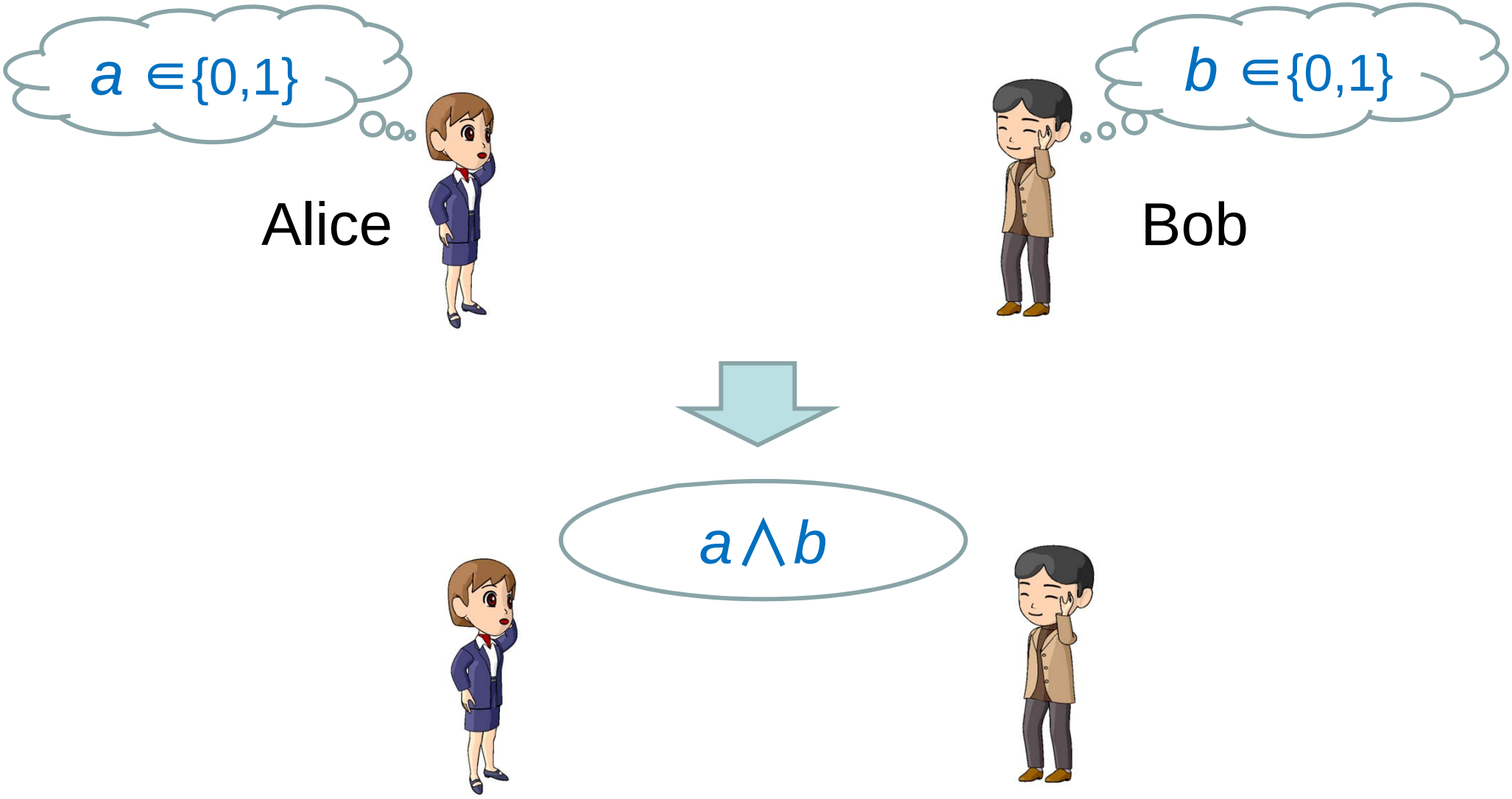
1. Introduction
2. Existing Committed-Format AND/XOR Protocols
3. Attack Exploiting Input Format
4. Backs with a Rotationally Symmetric Pattern
5. Backs with Scuff Marks
6. Conclusion

Contents

1. **Introduction**
   - 1.1 Five-Card Trick
   - 1.2 Other Existing Protocols
   - 1.3 Semi-Honest Model
   - 1.4 Our Main Results
2. **Existing mmitted-Format AND/**
3. **Attac**
4. **Back Symr**
5. **Backs with Scuff Marks**
6. **Conclusion**

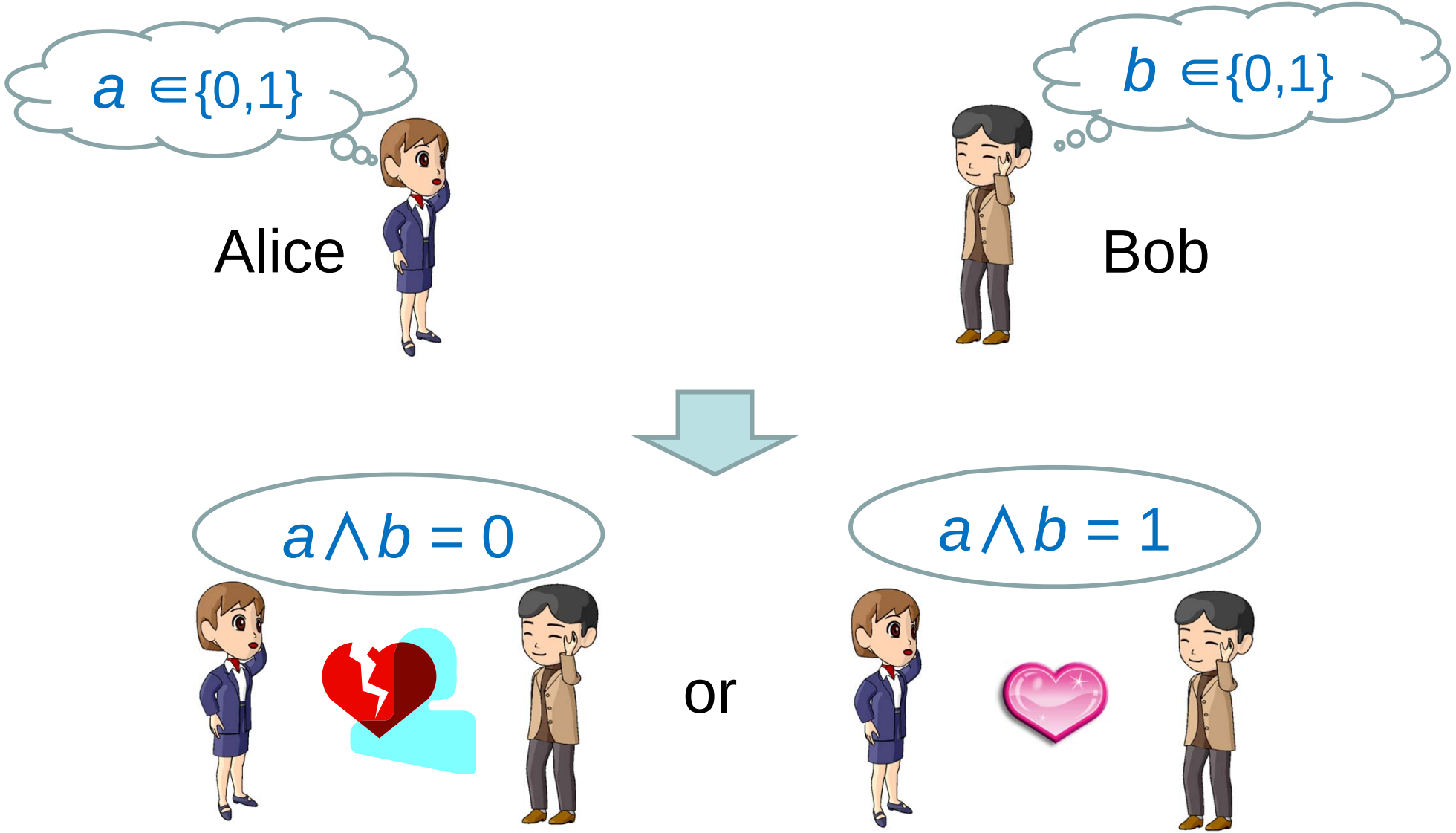
Secure computation

Alice and Bob want to **securely compute AND** without revealing more of their inputs than necessary.

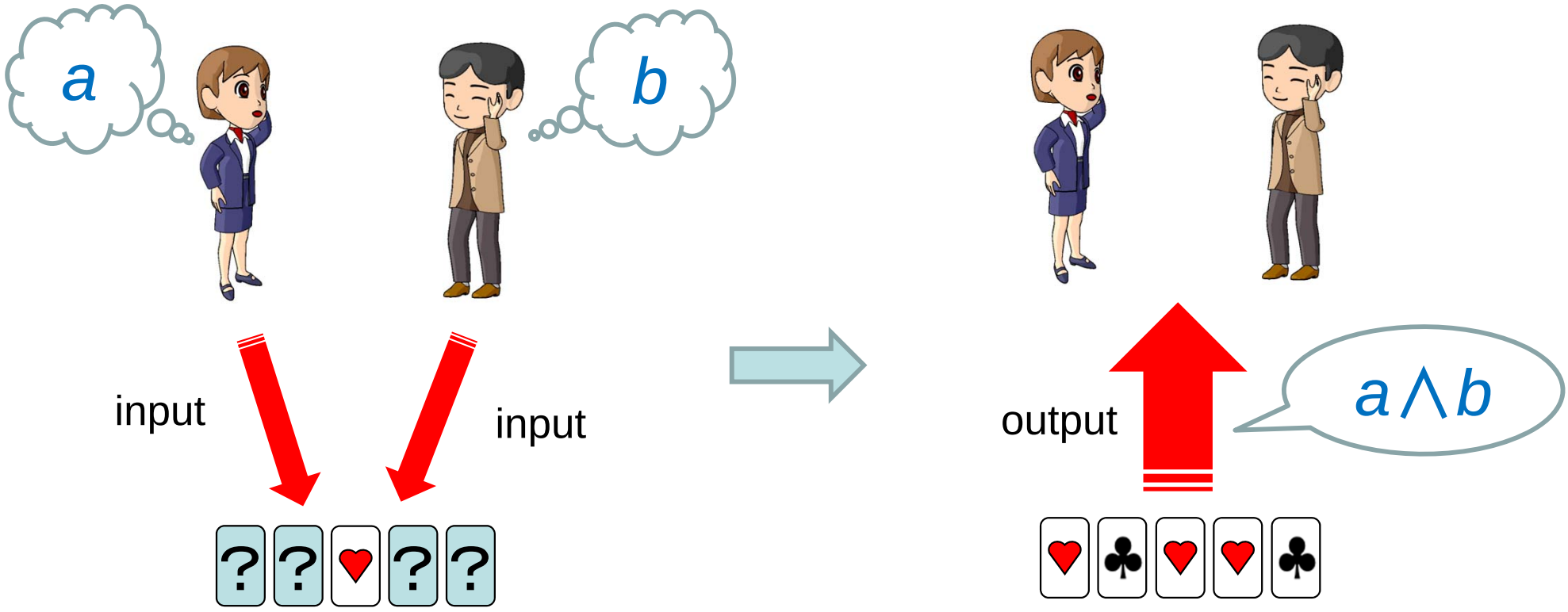


Secure computation; *an application*

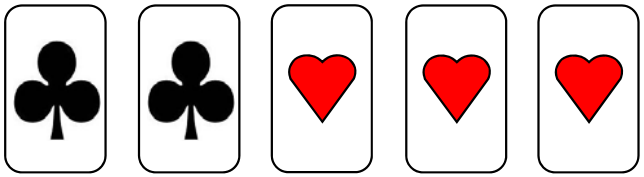
Secure AND can be used to decide whether they go on a date or not **without being embarrassed**.



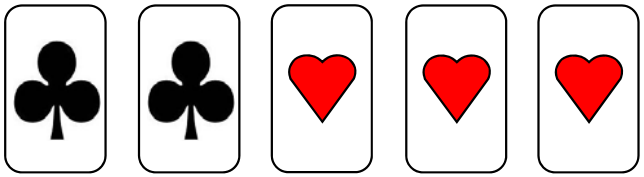
The *Five-Card Trick* [3](den Boer, Eurocrypt '89) achieves such a secure computation of AND using 3 red and 2 black cards.



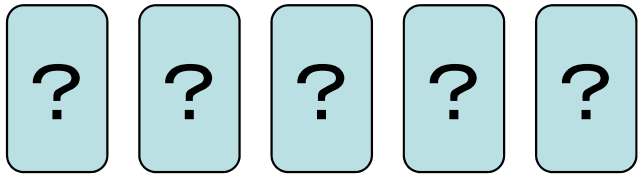
[3] B. den Boer, "More efficient match-making and satisfiability: the five card trick," EUROCRYPT '89, Lecture Notes in Computer Science, vol. 434, pp. 208–217, Springer-Verlag, 1990.



face-up

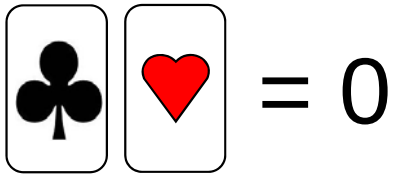


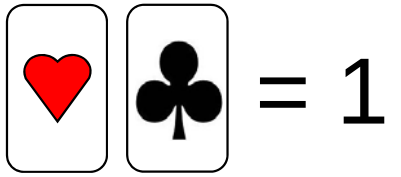
turn over

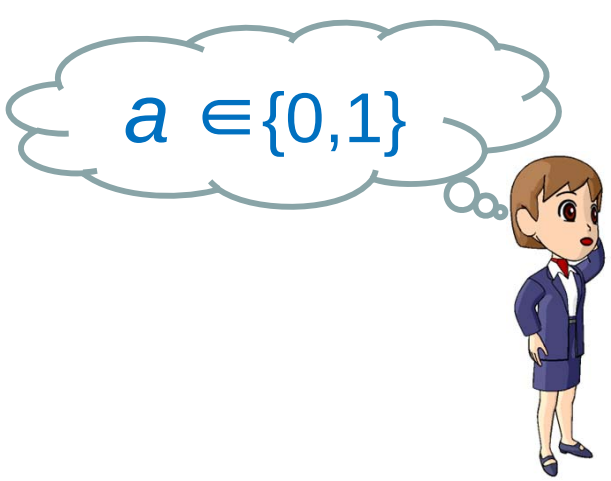


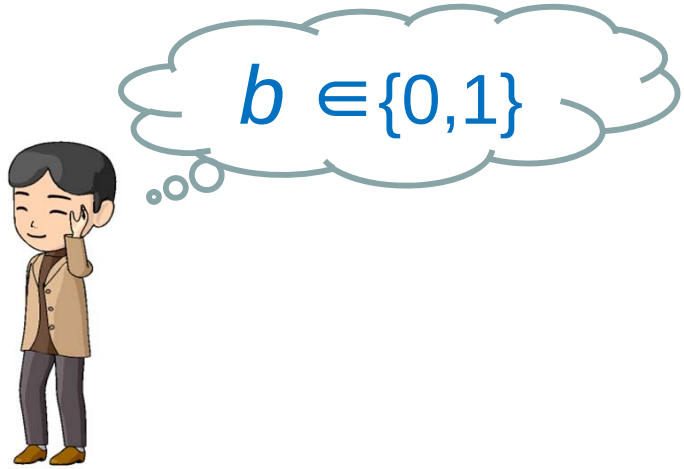
face-down

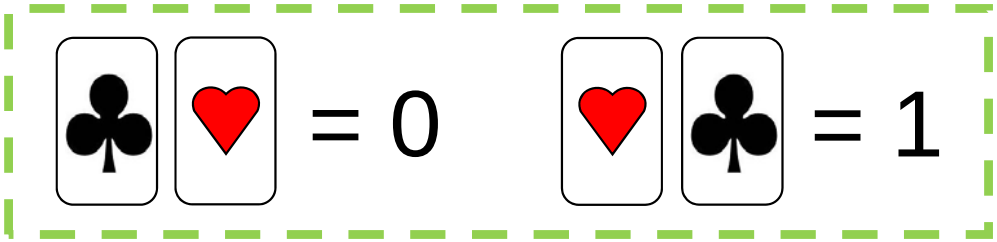
To deal with Boolean values, this encoding is used:

 = 0

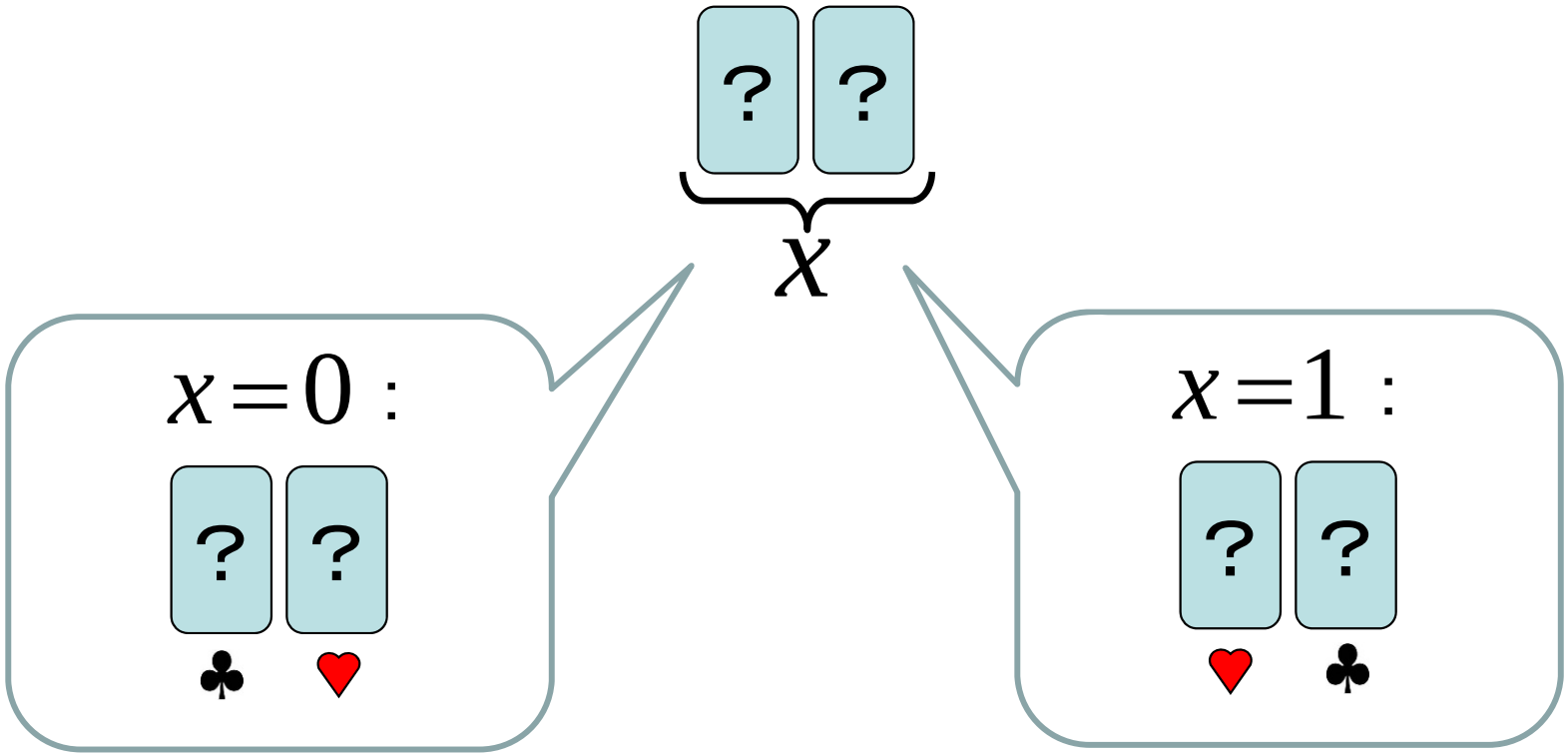
 = 1





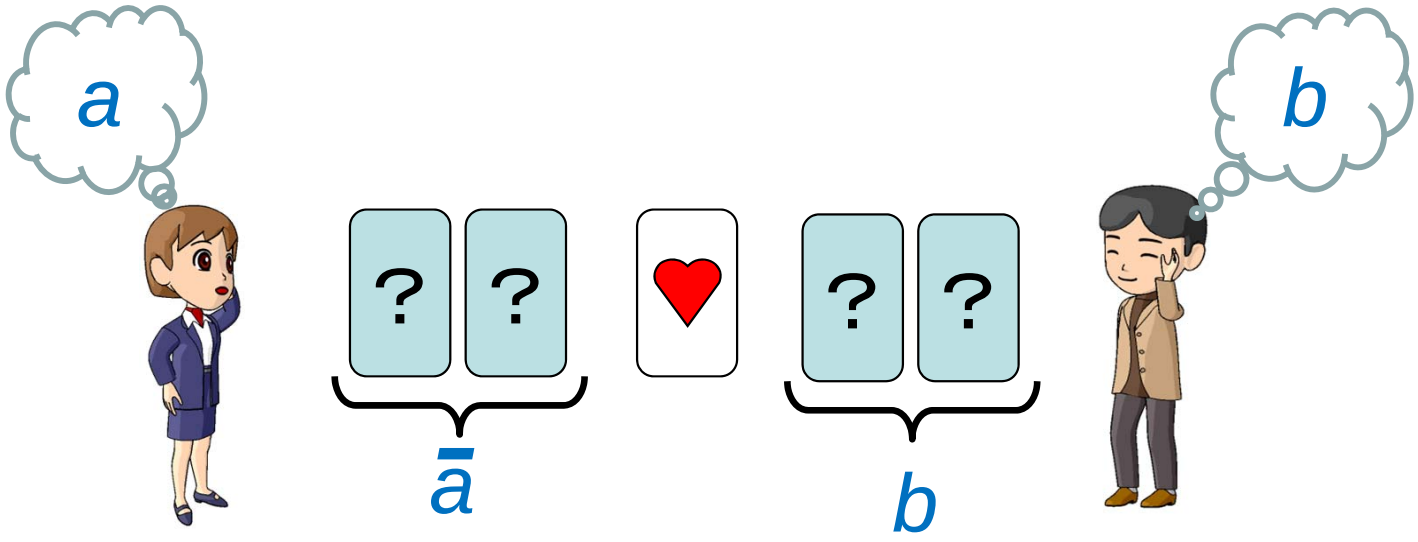


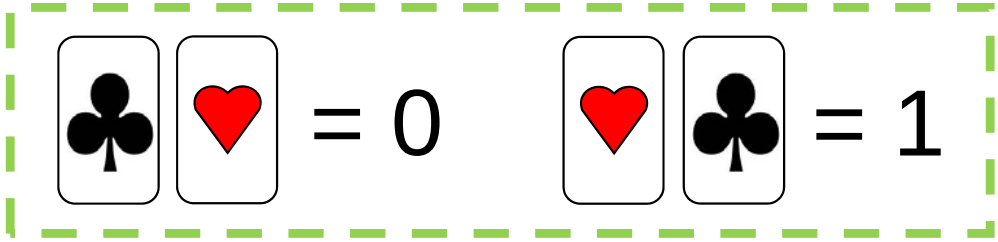
A ***commitment*** to a bit is a pair of face-down cards following the encoding.



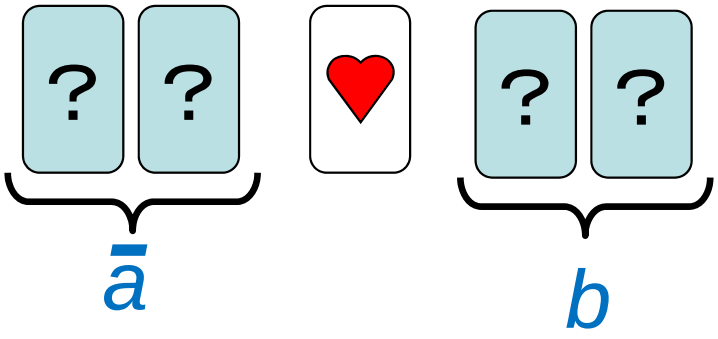
Five-Card Trick; **step 1**

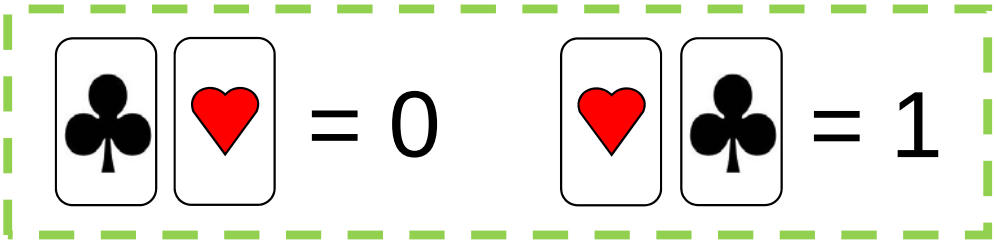
- Alice arranges a commitment to the negation $\bar{a}$ of a.
- Bob arranges a commitment to b.
- They put them forth with a red card.





Five-Card Trick; **step 1**

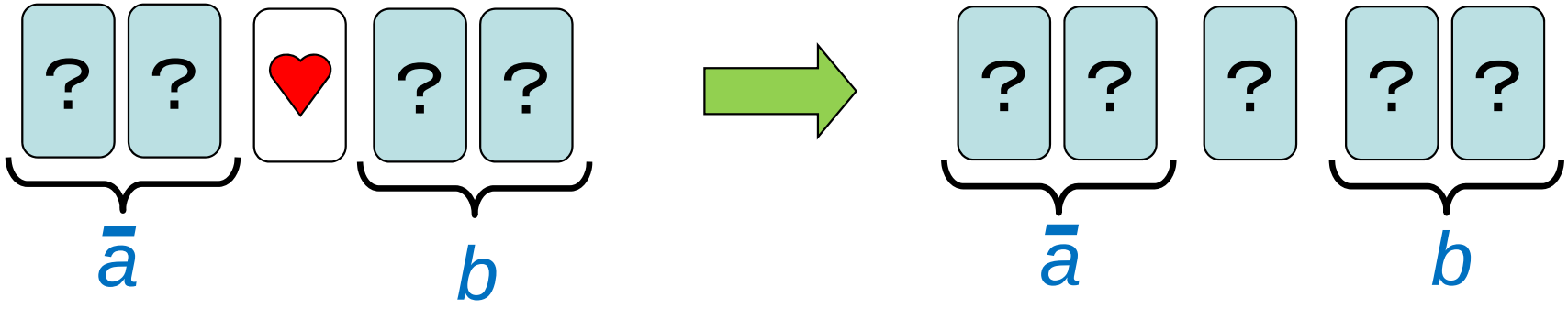




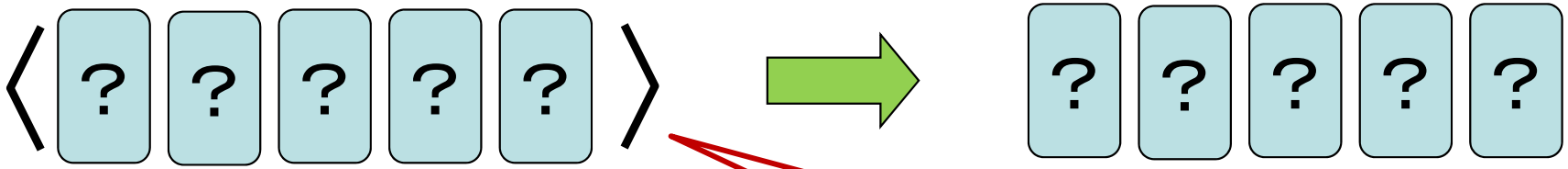
Note that the 3 cards in the middle would be red (namely ♥♥♥) only when $a = b = 1$.

Five-Card Trick; **step 2**

- Turn the centered card face down:



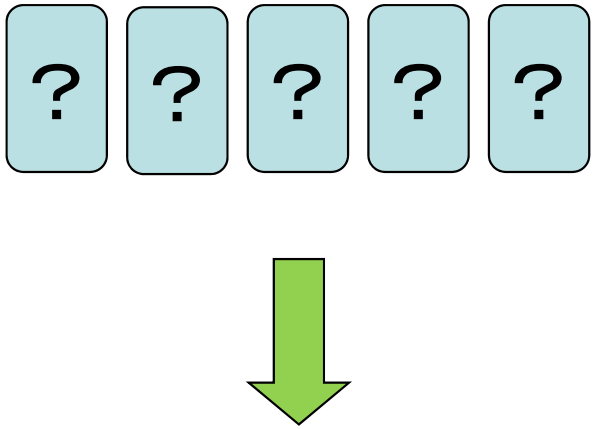
- Apply a ***random*** cut:



random cut
(= cyclic shuffling or random cyclic shift)

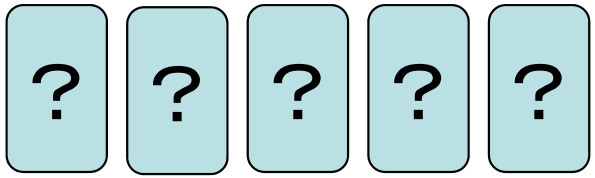
Five-Card Trick; **step 3**

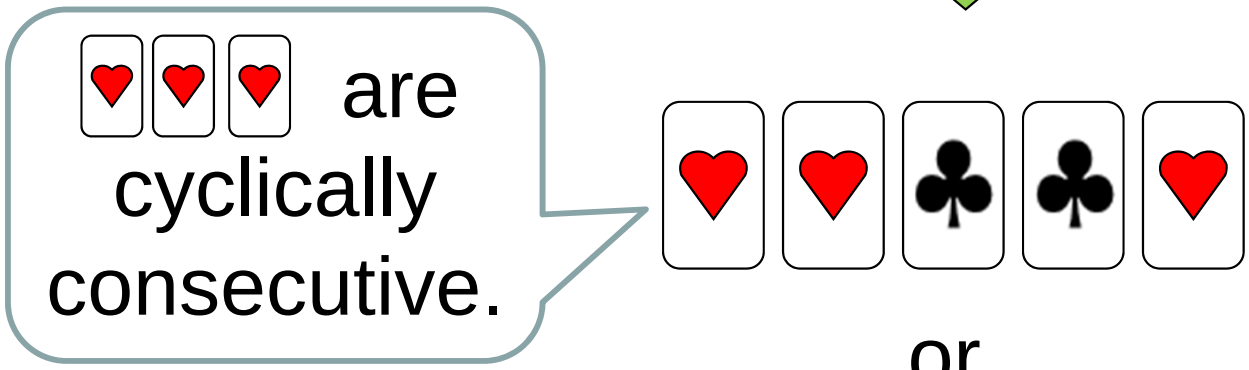
- Reveal all 5 cards:



Five-Card Trick; **step 3**

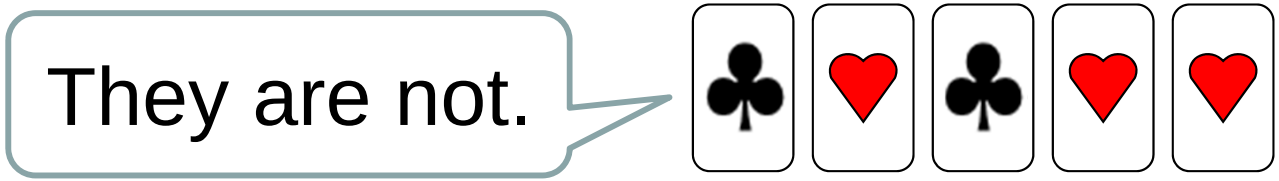
- Reveal all 5 cards:





$a \wedge b = 1$

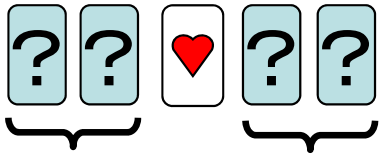
or

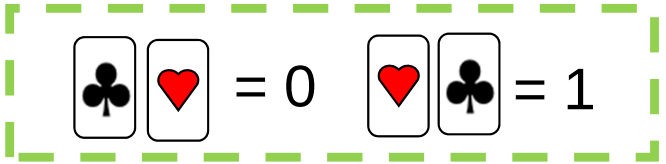


$a \wedge b = 0$

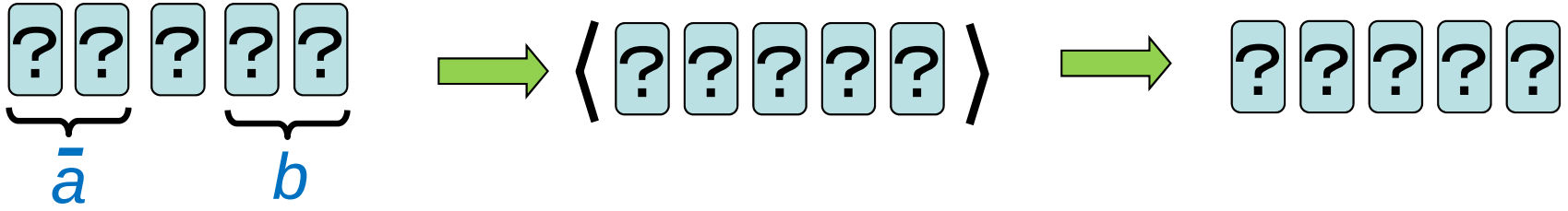
Five-Card Trick; full description

1. Put the 5 cards as follows:

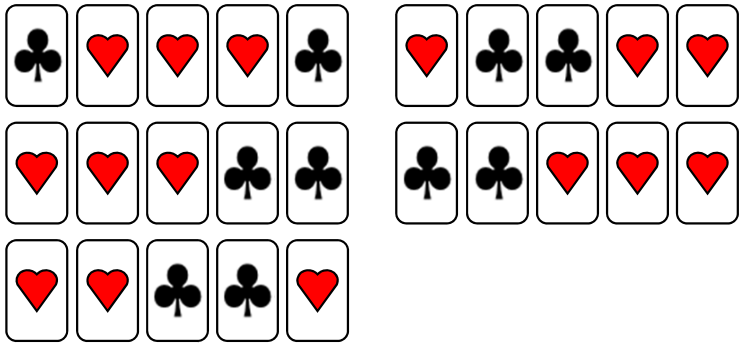




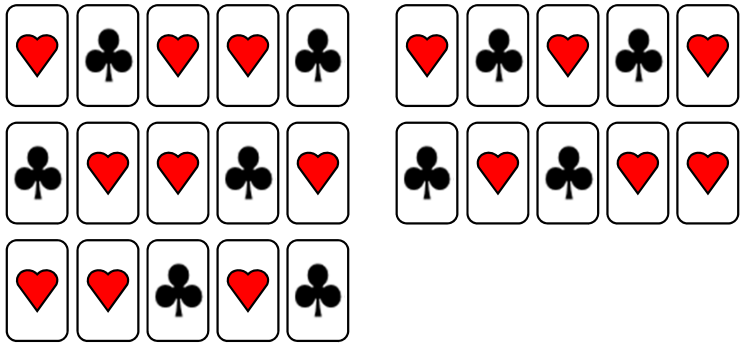
2. Turn the centered card face down, and apply a random cut:



3. Reveal all 5 cards:

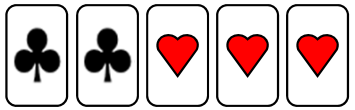
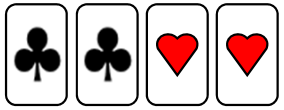


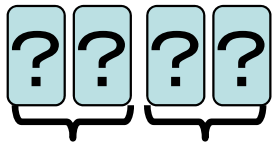
$a \wedge b = 1$

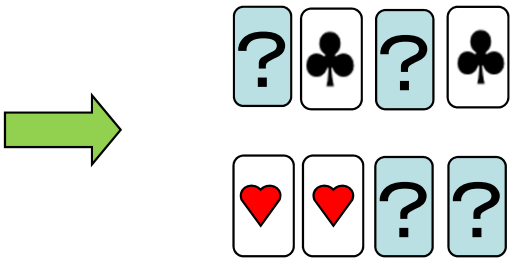


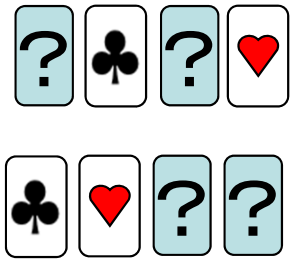
$a \wedge b = 0$

Other Existing Protocols

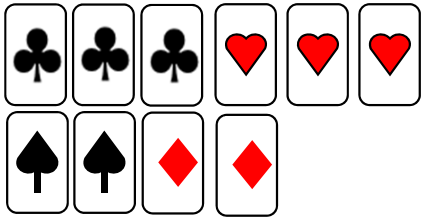
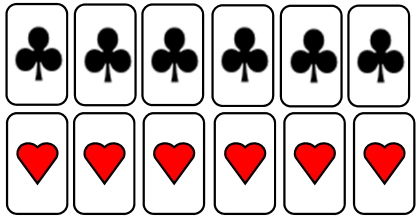
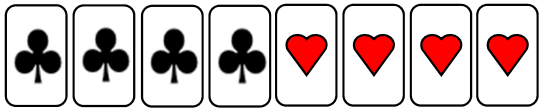
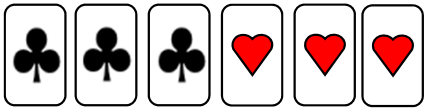
	No. of cards	random cut	bisection cut
den Boer [Eurocrypt '89]	5 	✔	
Mizuki-Kumamoto-Sone [Asiacrypt 2012]	4 	✔	✔







Committed-format AND protocols

	No. of cards & colors	random cut	bisection cut	average No. 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

Secure AND in a committed format

	No. of cards & colors	random cut	bisection cut	average No. of trials
Crepeau-Kilian [CRYPTO '93]	10	✔		6
Niemi-Renvall [TCS, 1998]	12			
Stiglic [TCS, 2001]	8	✔		2
Mizuki-Sone [FAW 2009]	6		✔	1

Will be introduced in Section 2

Secure XOR

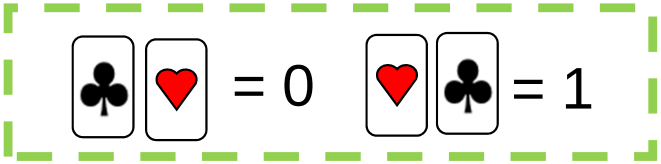
	No. of cards	No. of colors	random cut	bisection cut	average No. of trials
Crepeau-Kilian [CRYPTO '93]	14	4	✔		6
Mizuki, et. al [AJoC, 2006]	10	2	✔		2
Mizuki-Sone [FAW 2009]	4	2		✔	1

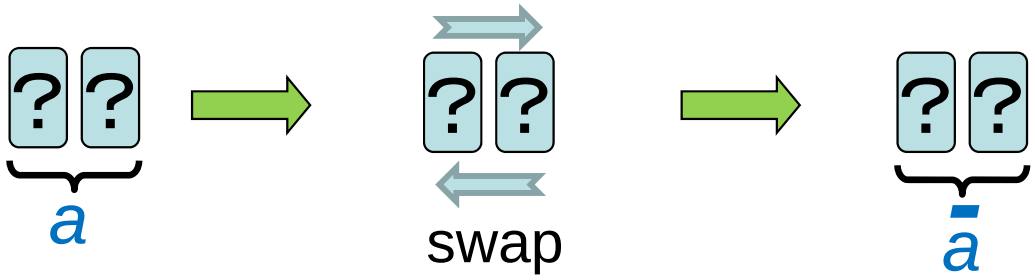
Secure XOR

	No. of cards	No. of colors	random cut	bisection cut	average No. of trials
Crepeau-Kilian [CRYPTO '93]	14	4			
Mizuki, et. al [AJoC, 2006]	10	2	✔		2
Mizuki-Sone [FAW 2009]	4	2		✔	1

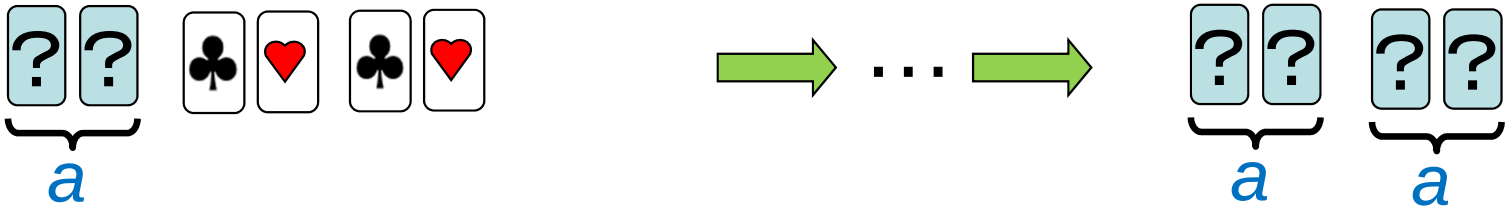
Will be introduced in Section 2

Secure NOT is trivial:





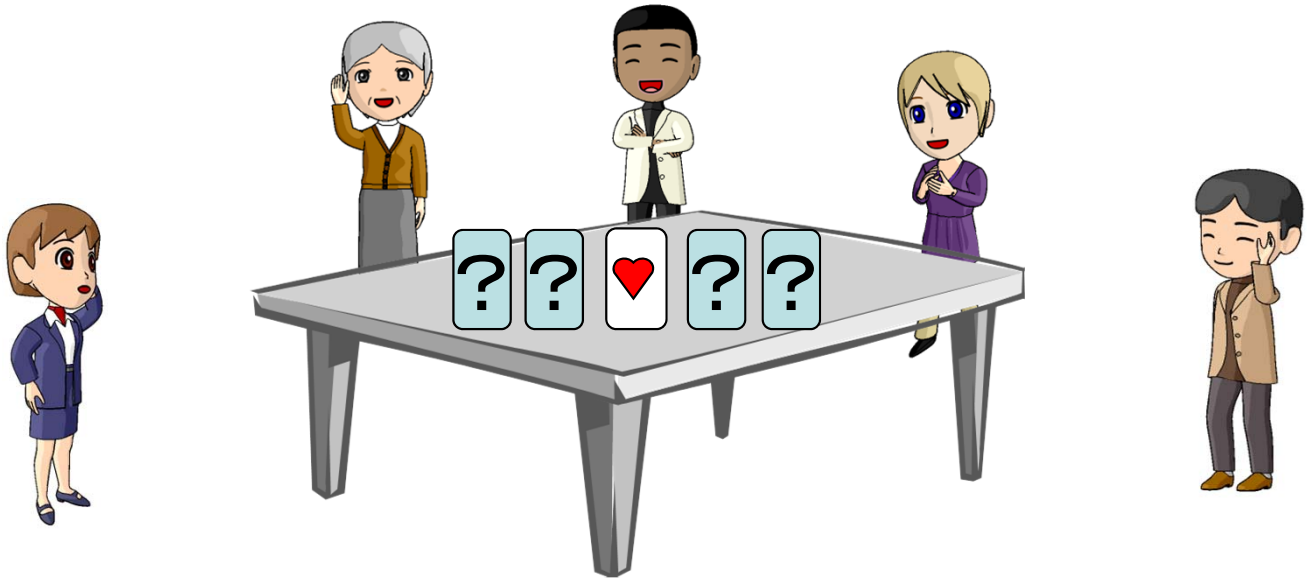
There are protocols for copying a commitment:



Combining these AND/XOR/NOT/copy protocols, we can securely compute ***any*** function.

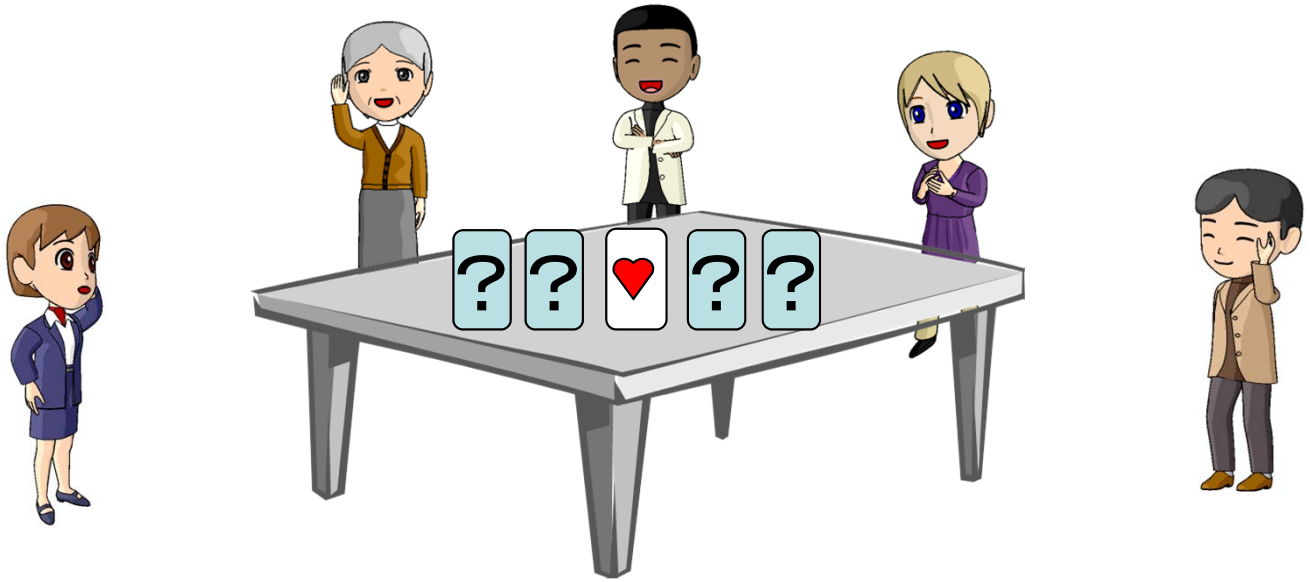
A frequently asked question:

What if a player acts maliciously?



A frequently asked question:

What if a player acts maliciously?

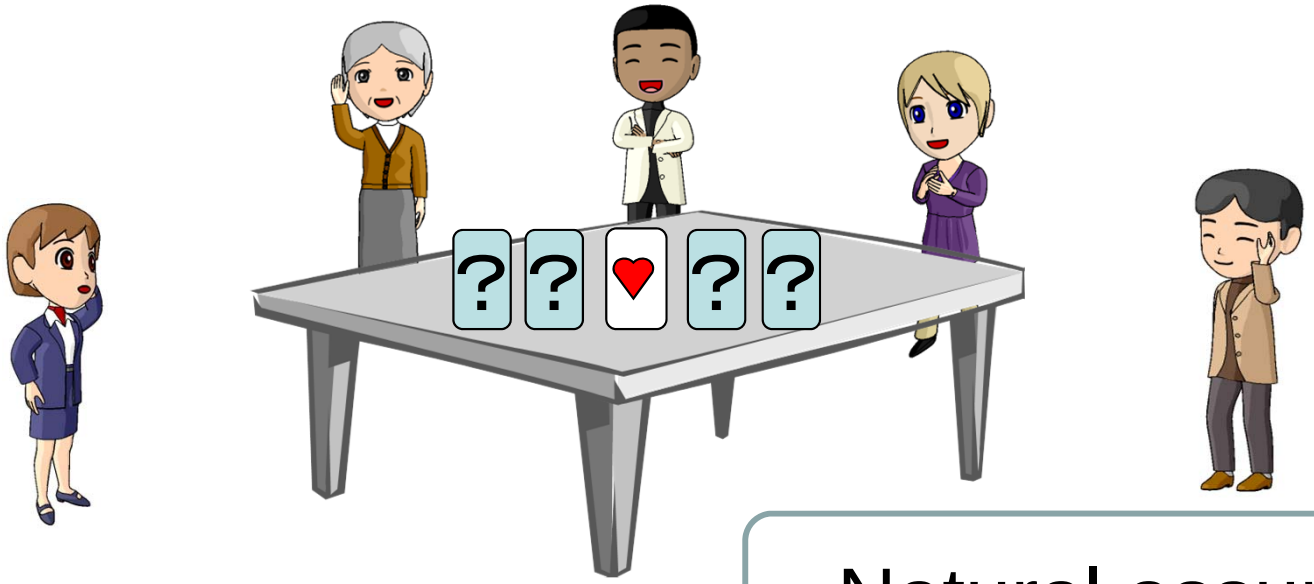


【General answer】

A protocol is executed correctly with all eyes fixed on how the cards are manipulated after all players place commitments on the table (semi-honest model).

A frequently asked question:

What if a player acts maliciously?

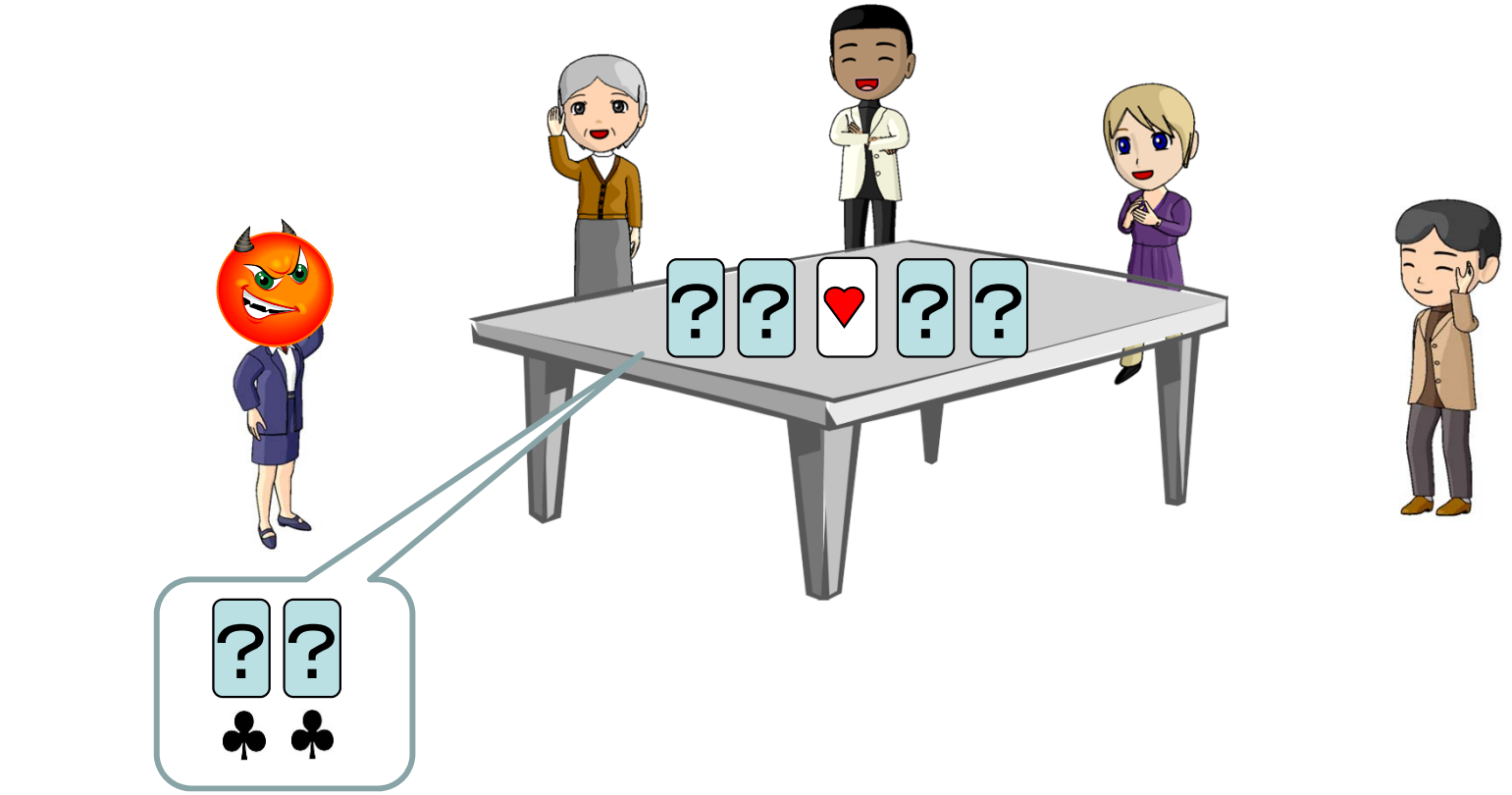


Natural assumption

【General answer】

A protocol is executed correctly with all eyes fixed on how the cards are manipulated after all players place commitments on the table (semi-honest model).

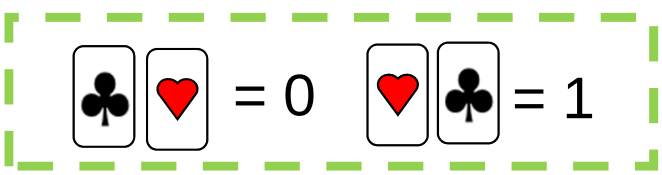
However, when placing a pair of face-down cards as a commitment, a player may be able to act maliciously.

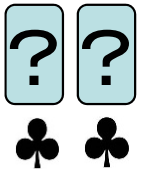


♣ ♥ = 0 ♥ ♣ = 1

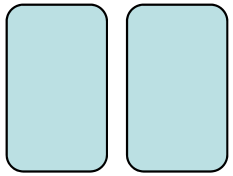
Our main results

- ✓ An attack exploiting input format and its countermeasure



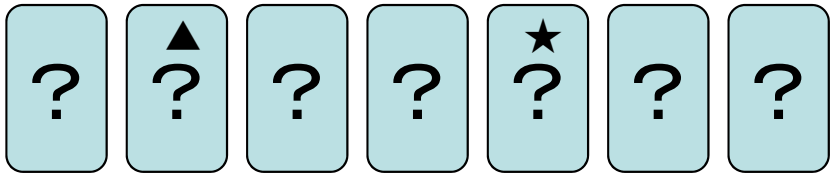


- ✓ Backs with a Rotationally Symmetric Pattern



Pros and Cons

- ✓ Backs with Scuff Marks



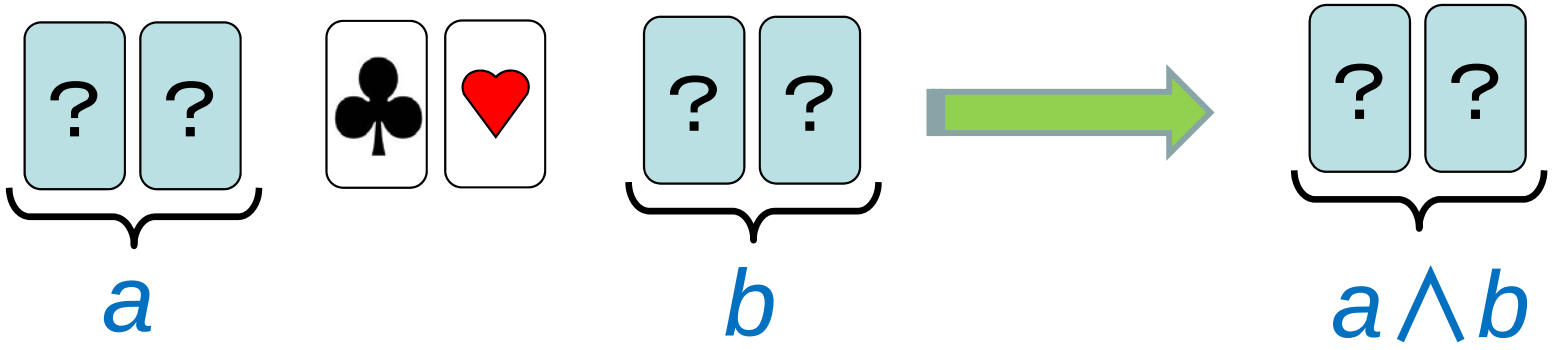
Method to maintain secrecy

Contents

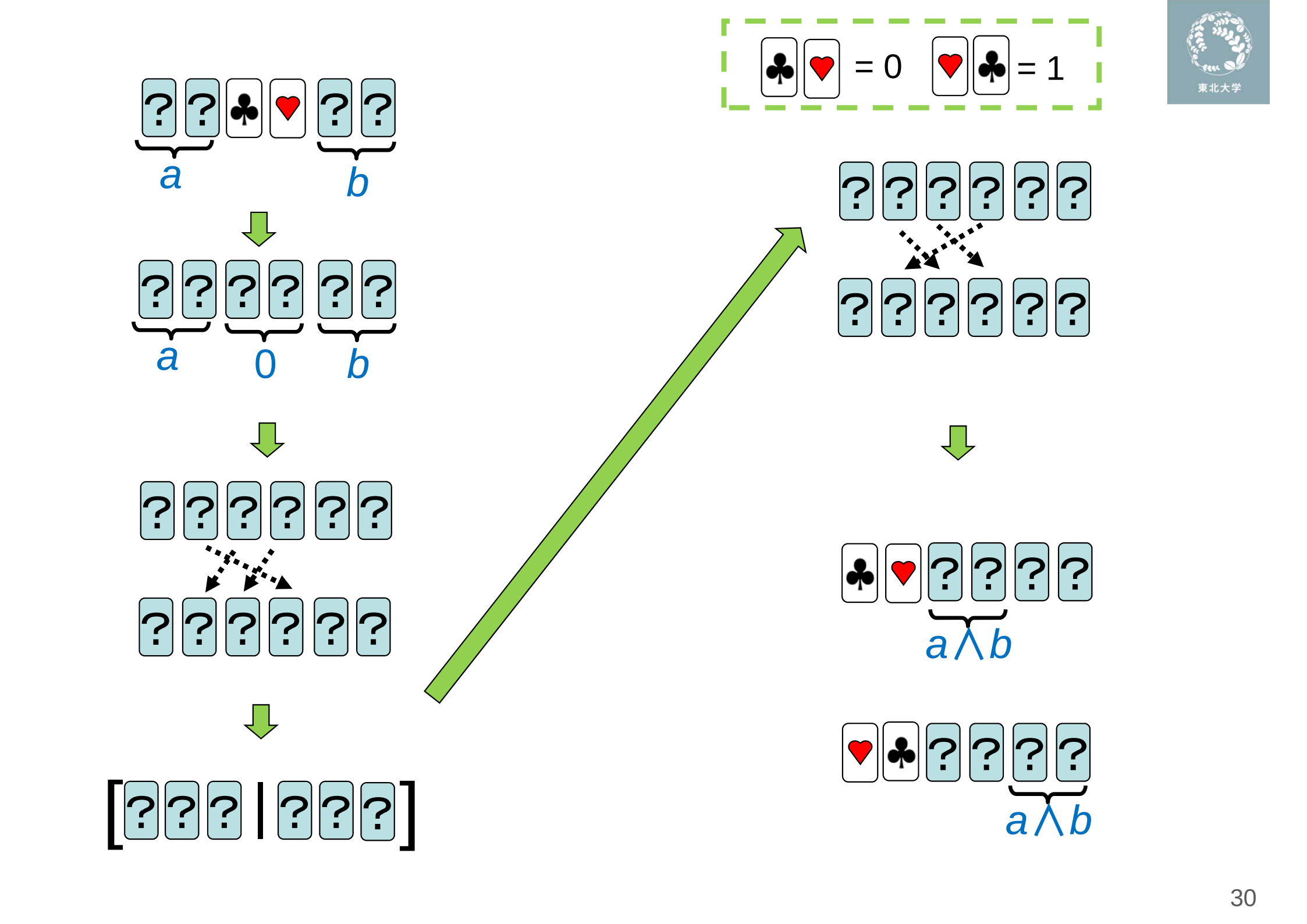
1. Introduction
2. Existing Committed-Format AND/XOR Protocols
3. Attack Exploiting Input Format
4. Backs with a Rotationally Symmetric Pattern
5. Backs with Scuff Marks
6. Conclusion

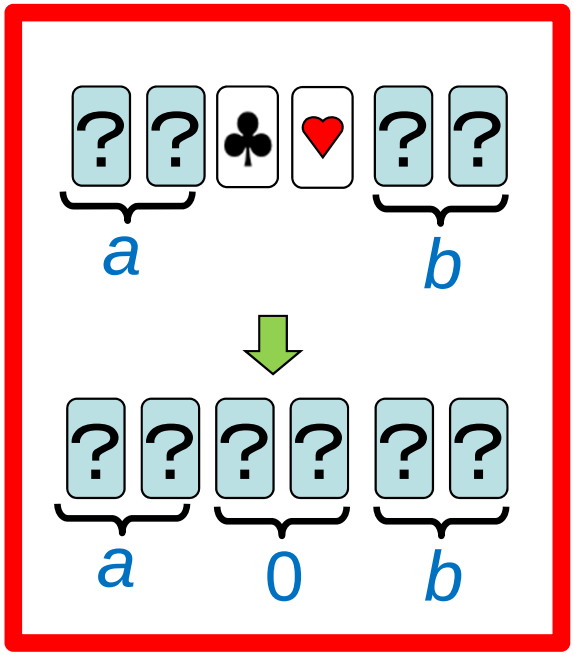
An existing committed-format AND protocol

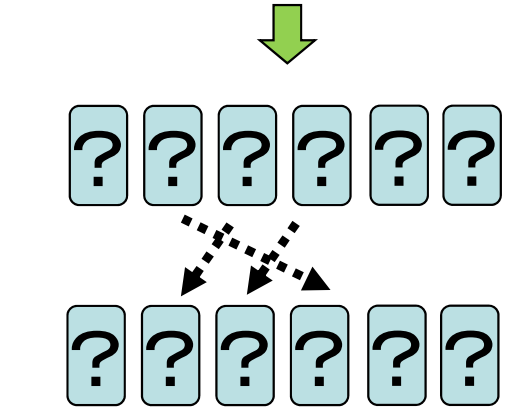
A commitment to $a \wedge b$ can be obtained using 6 cards [5].

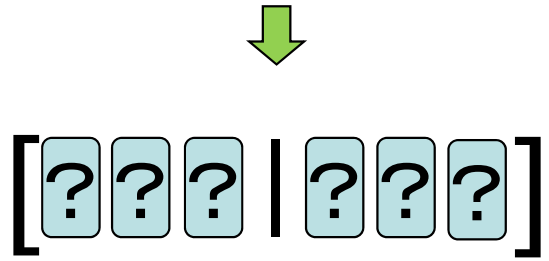


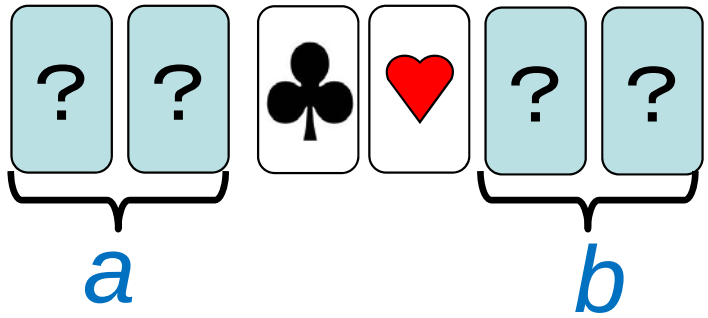
[5] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.


= 0
= 1
a
b
a
0
b
a ∧ b
a ∧ b

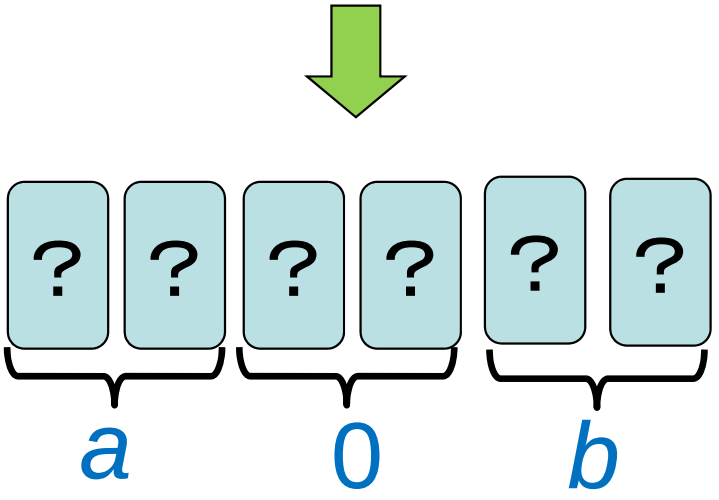




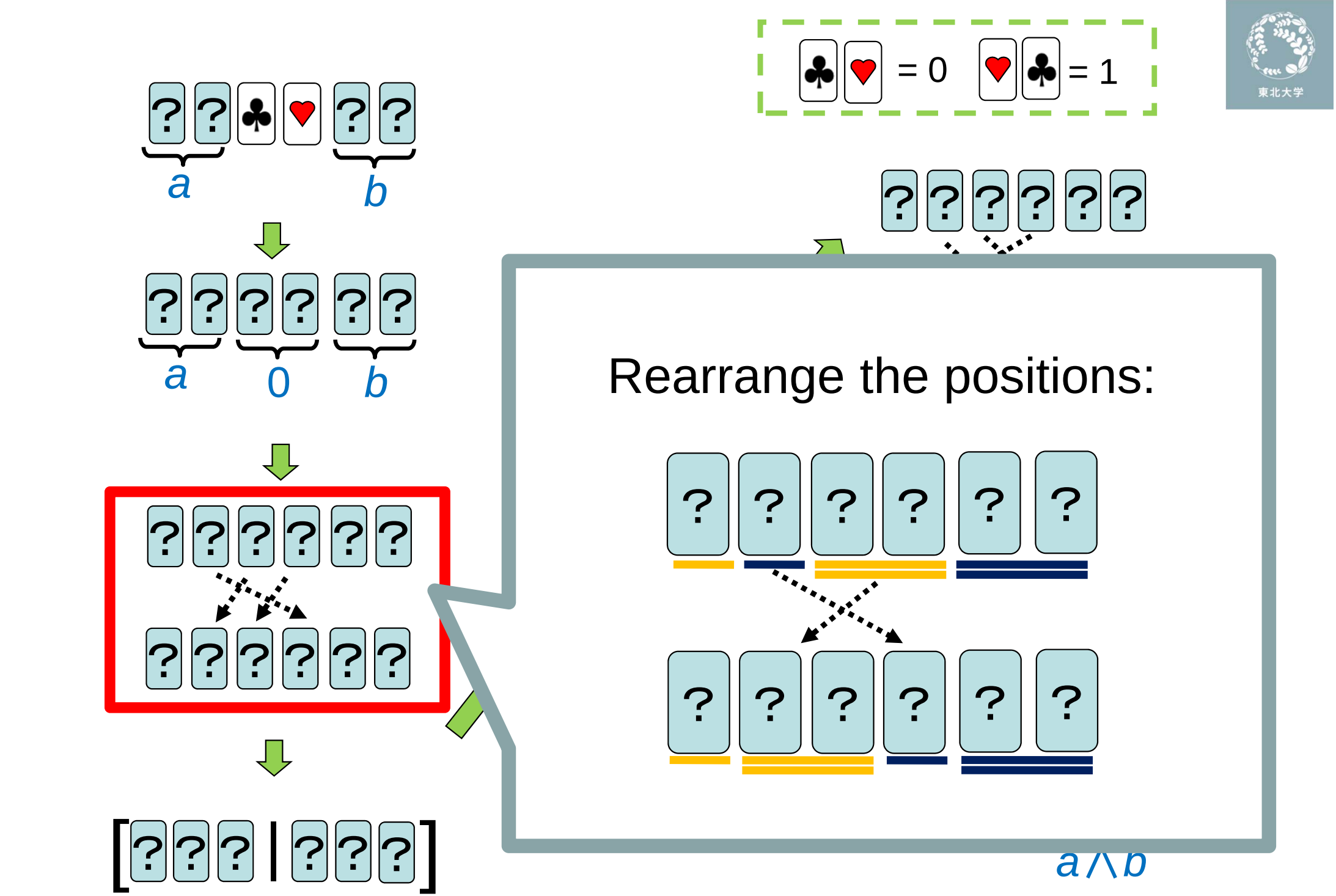


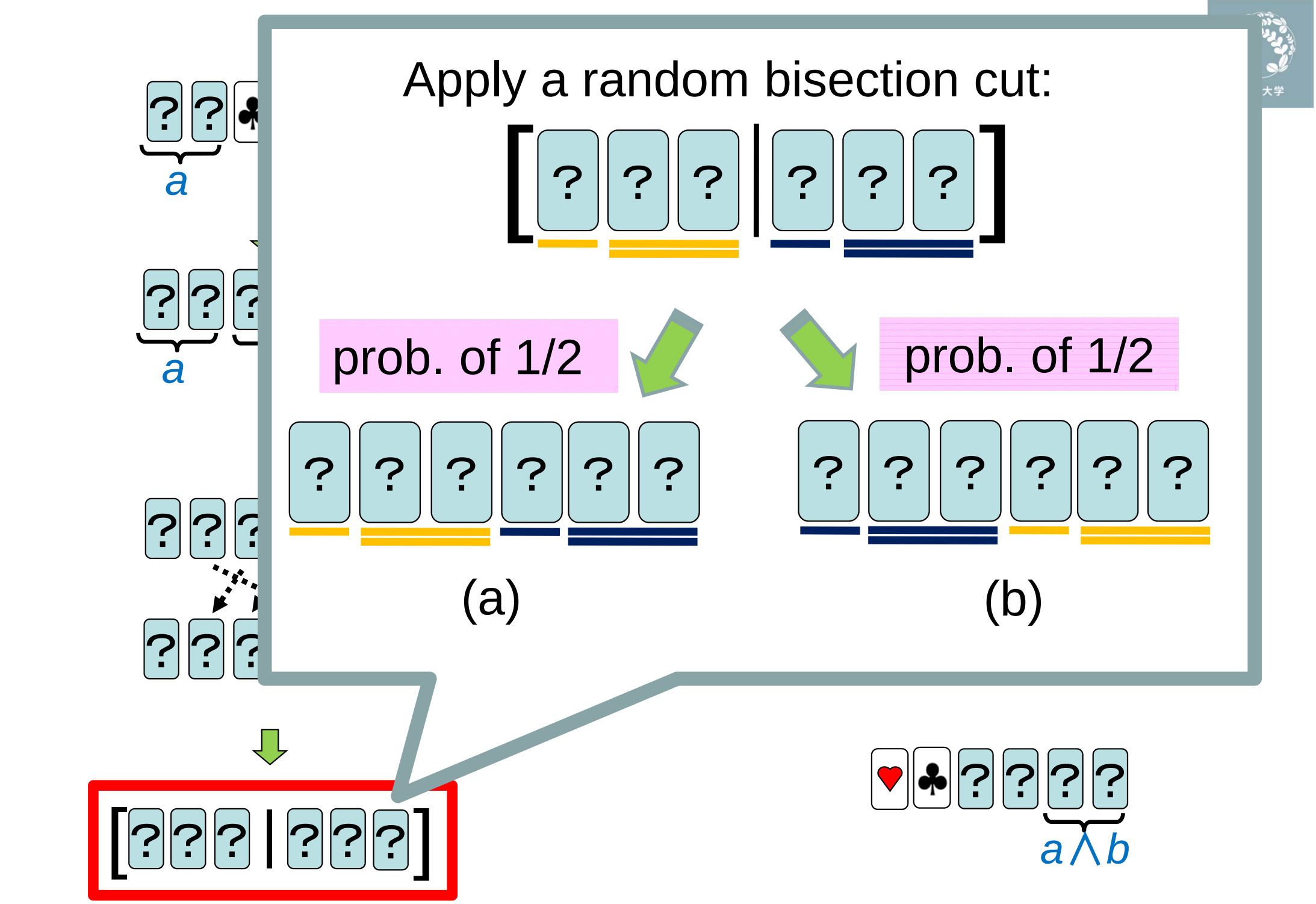


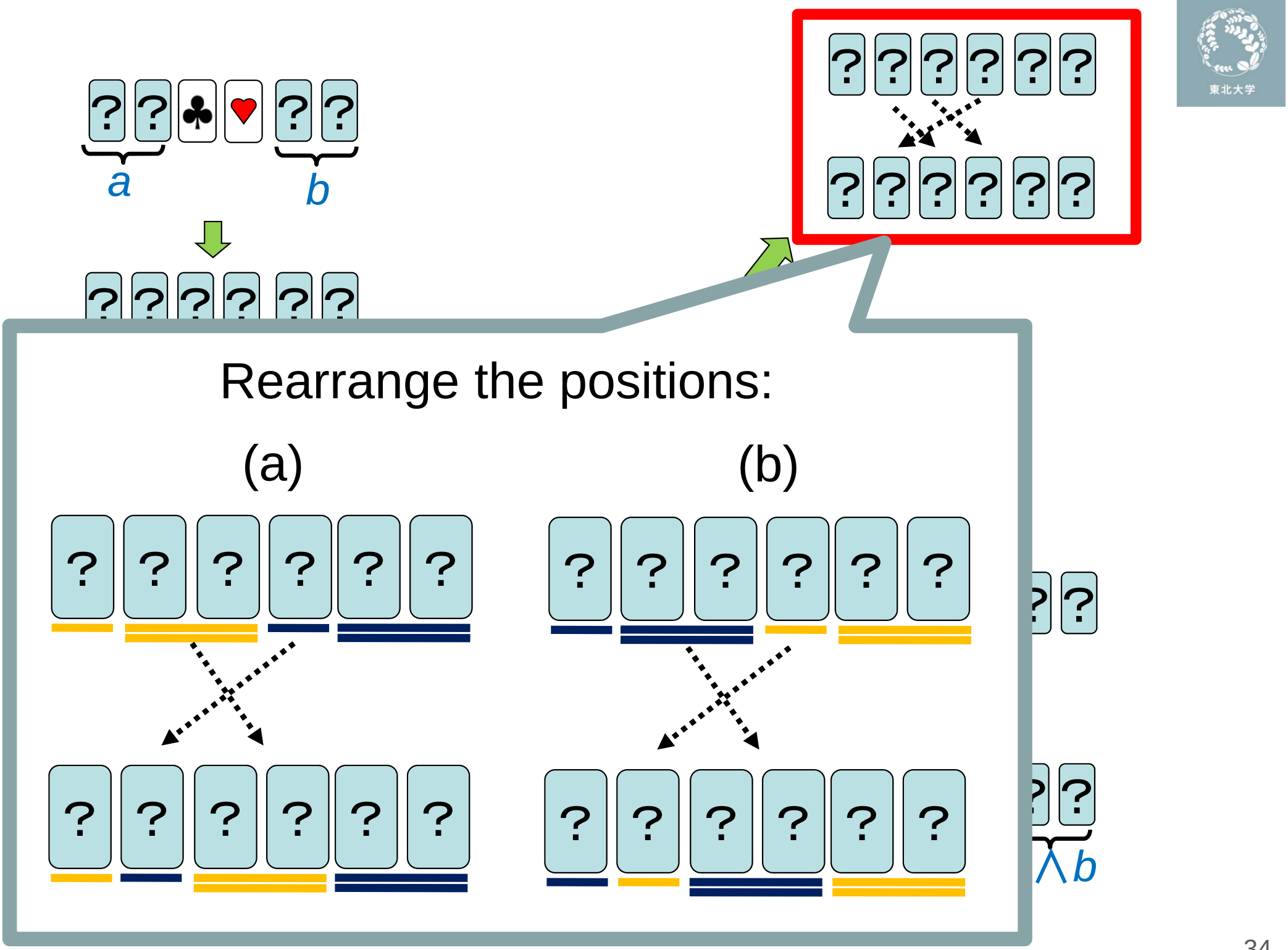
Turn over the two middle cards:

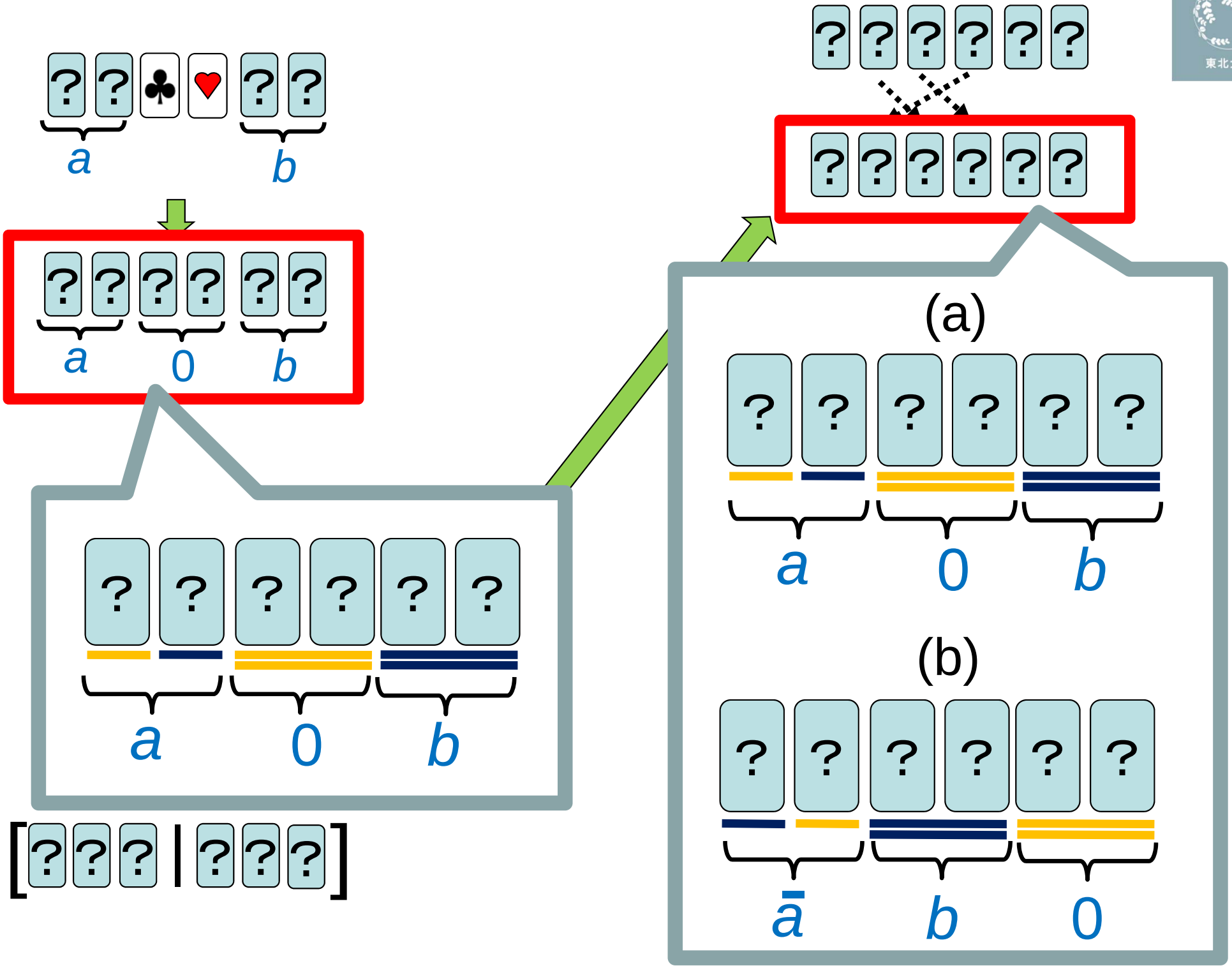


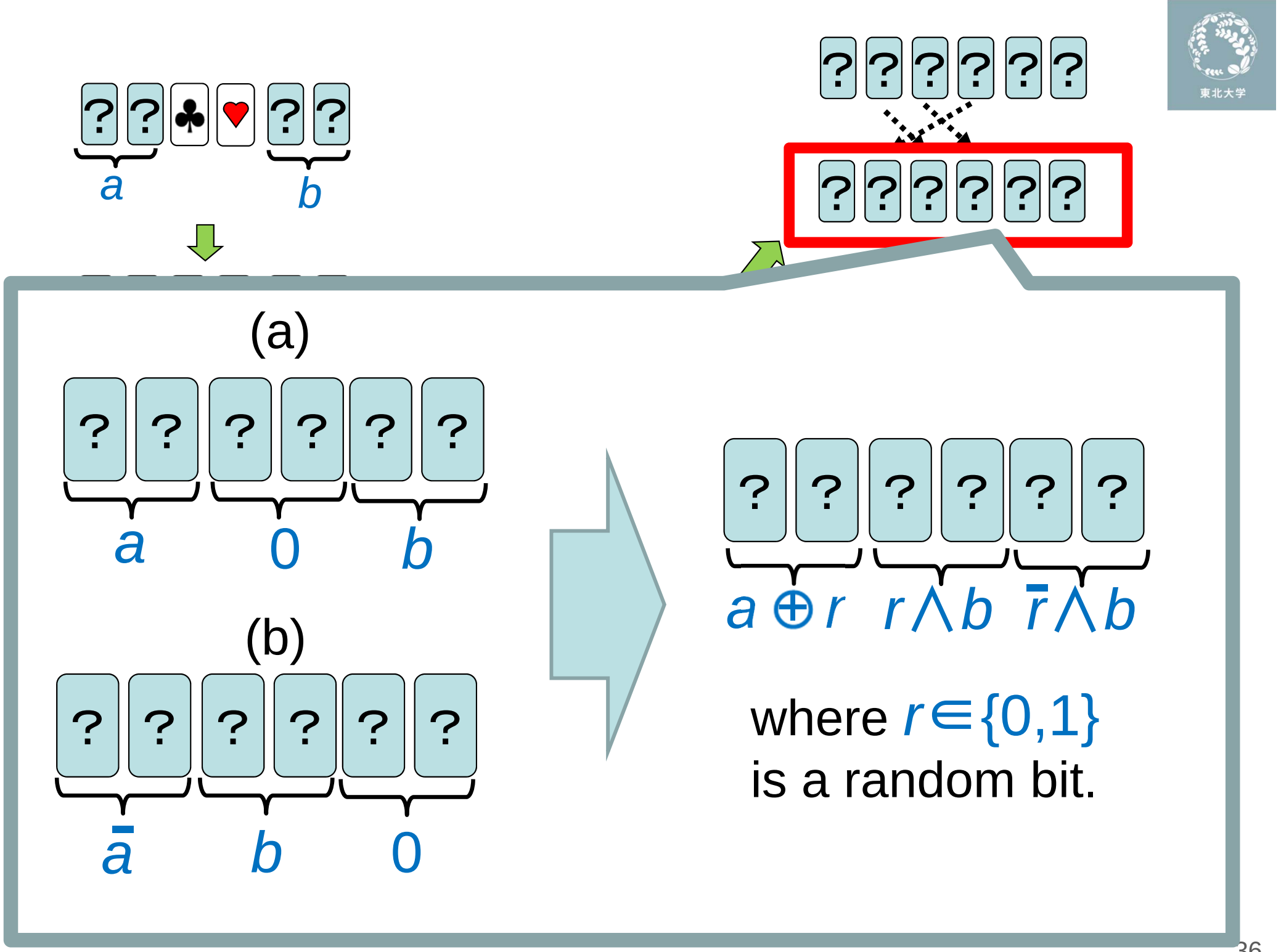
$a \wedge b$

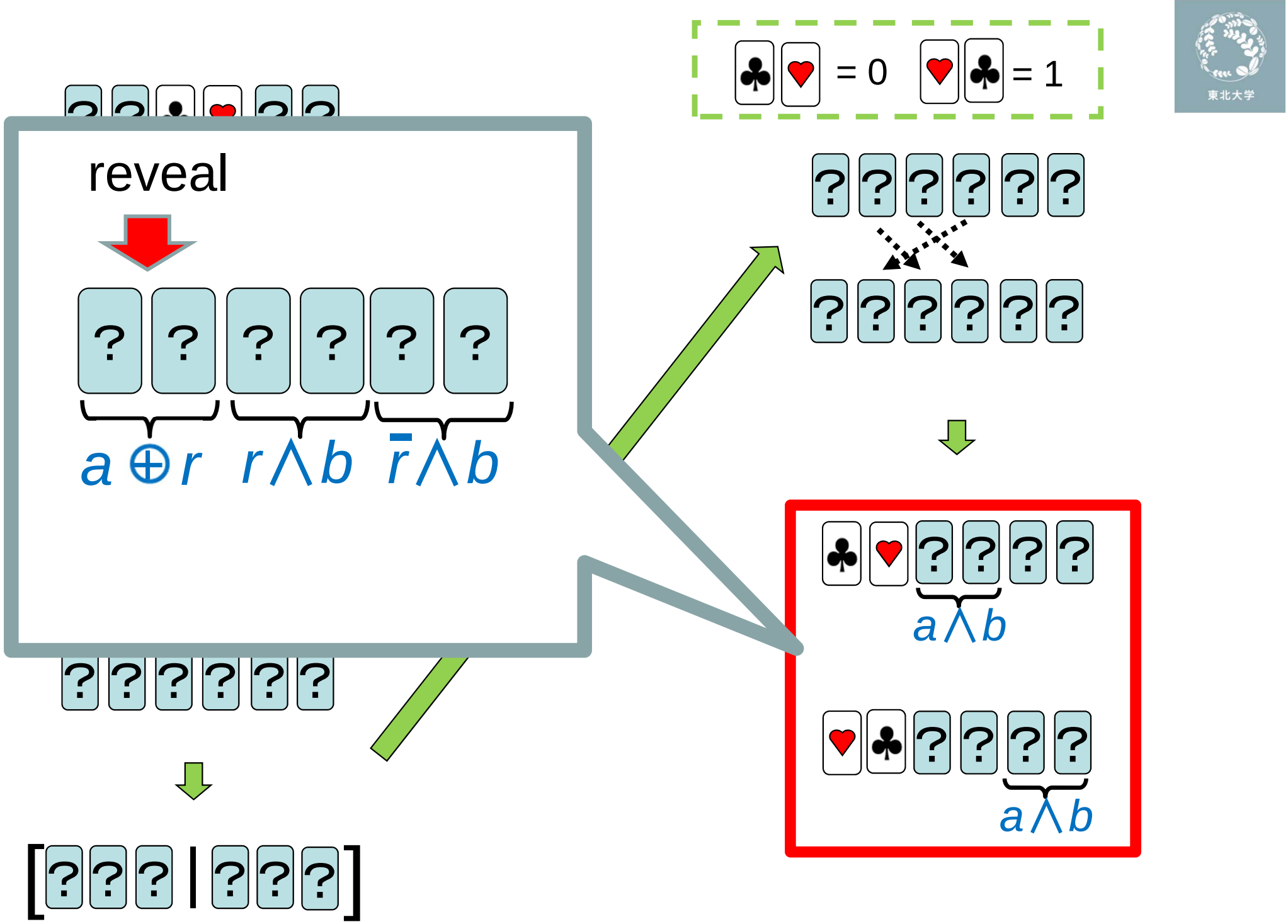

= 0
= 1
a
b
a
0
b
Rearrange the positions:
a ∧ b

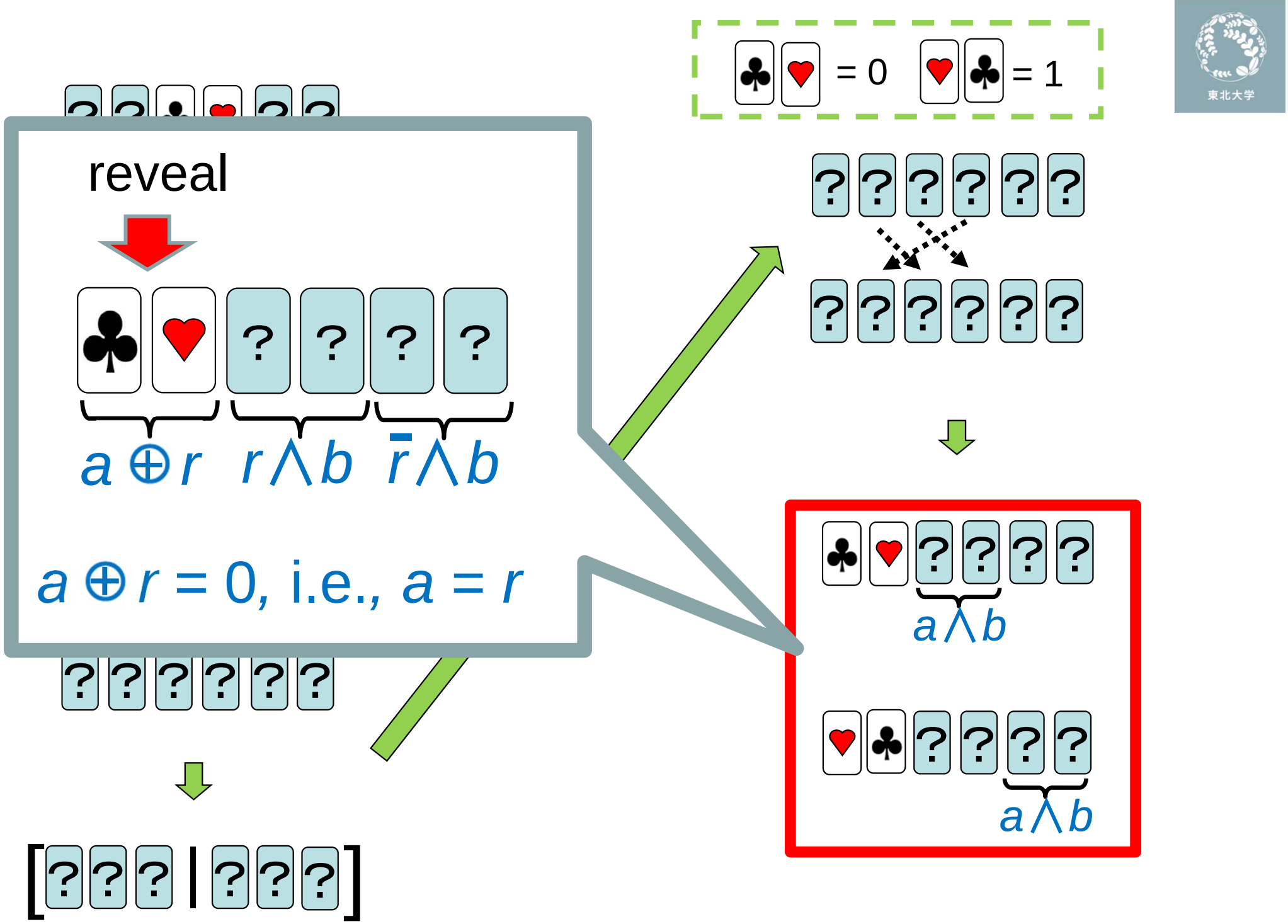

Apply a random bisection cut:
prob. of 1/2
prob. of 1/2
(a)
(b)
a
a
a ∧ b

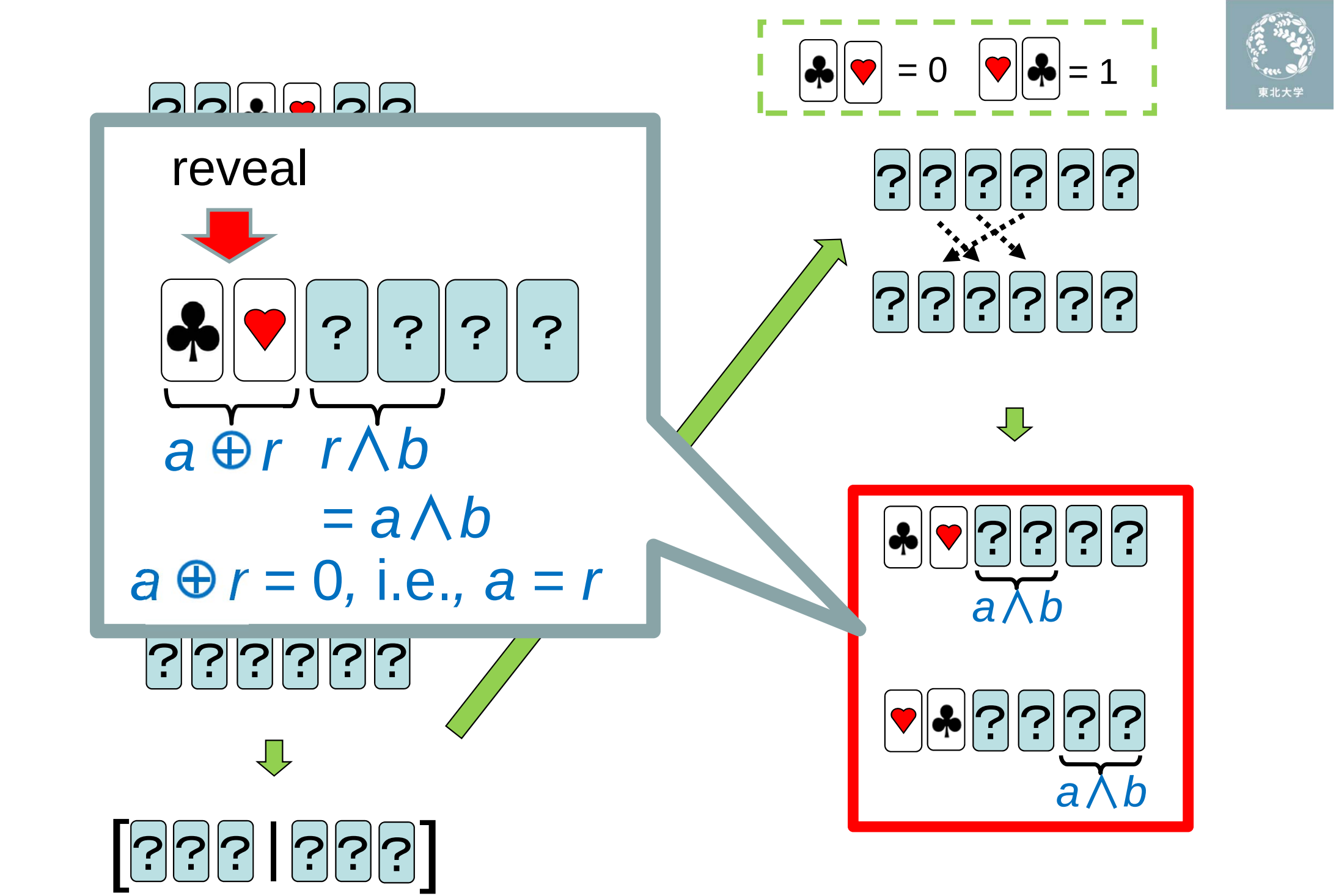

a
b
Rearrange the positions:
(a)
(b)
a
b

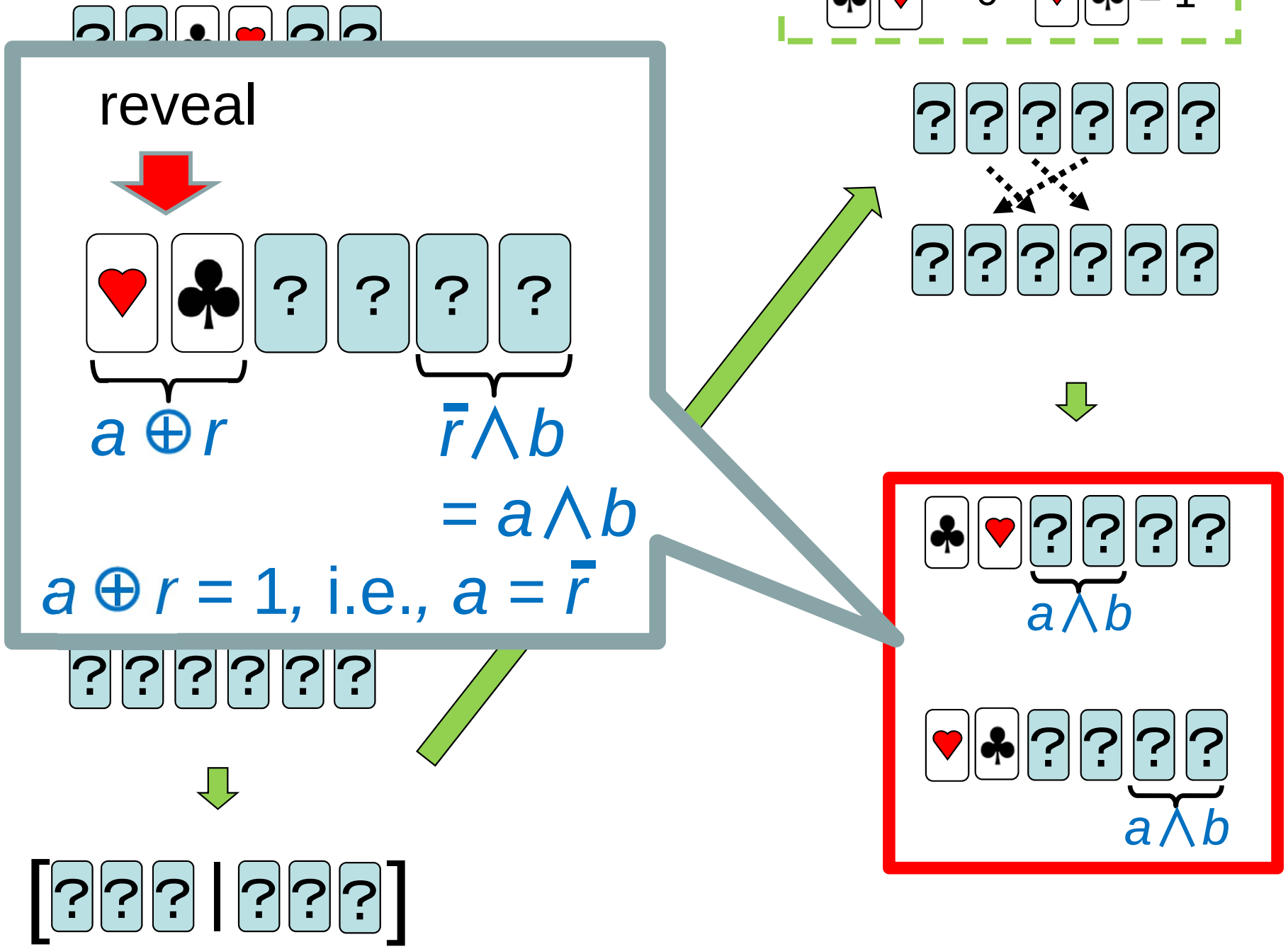

a
b
a
0
b
a
0
b
[|]
(a)
a
0
b
(b)
ā
b
0

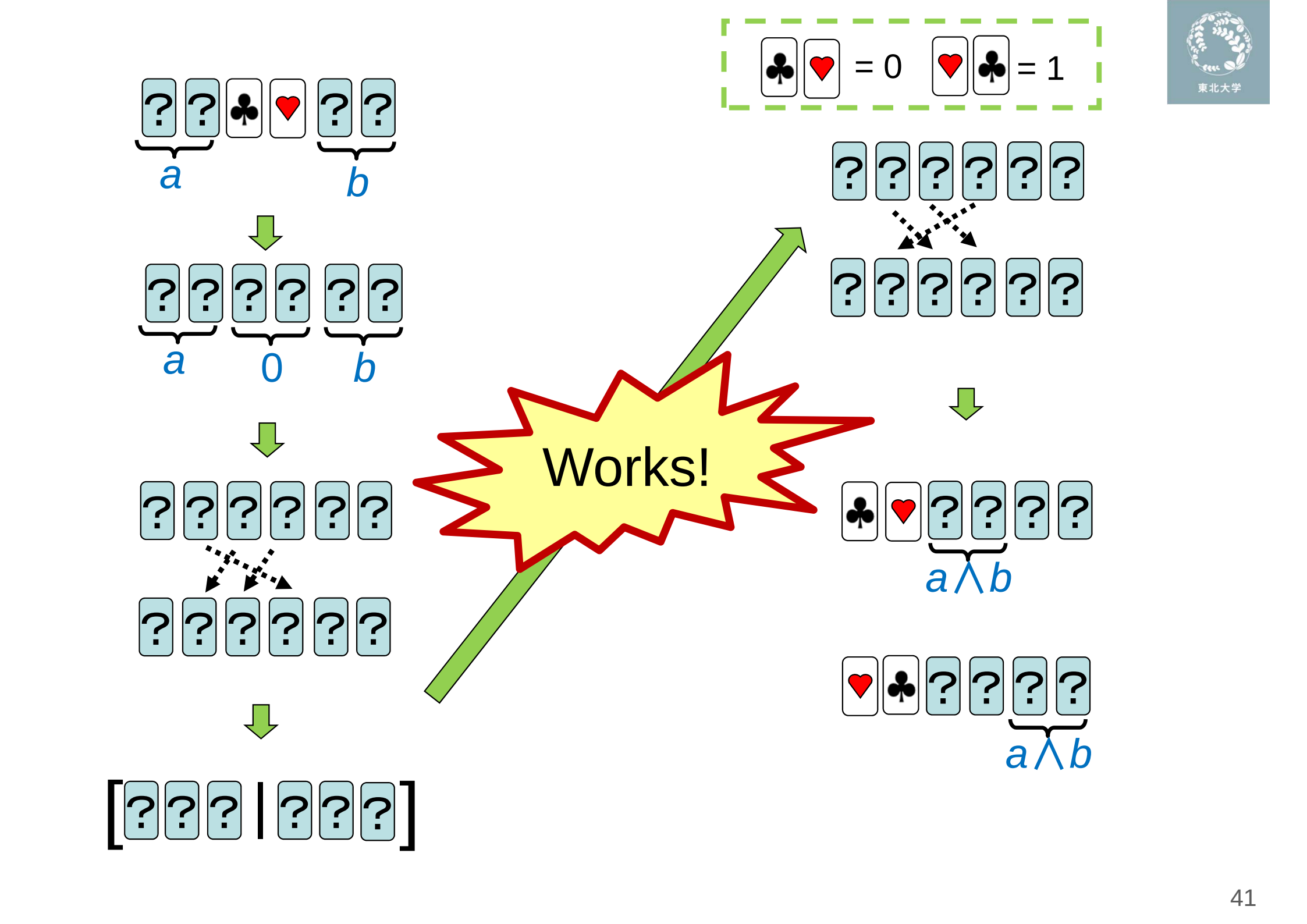

a
b
(a)
a
0
b
(b)
ā
b
0
a ⊕ r
r ∧ b
r̄ ∧ b
where r∈{0,1}
is a random bit.


= 0
= 1
reveal
$a \oplus r$
$r \wedge b$
$\bar{r} \wedge b$
$a \wedge b$
$a \wedge b$


= 0
= 1
reveal
$a \oplus r$
$r \wedge b$
$\bar{r} \wedge b$
$a \oplus r = 0$, i.e., $a = r$
$a \wedge b$
$a \wedge b$

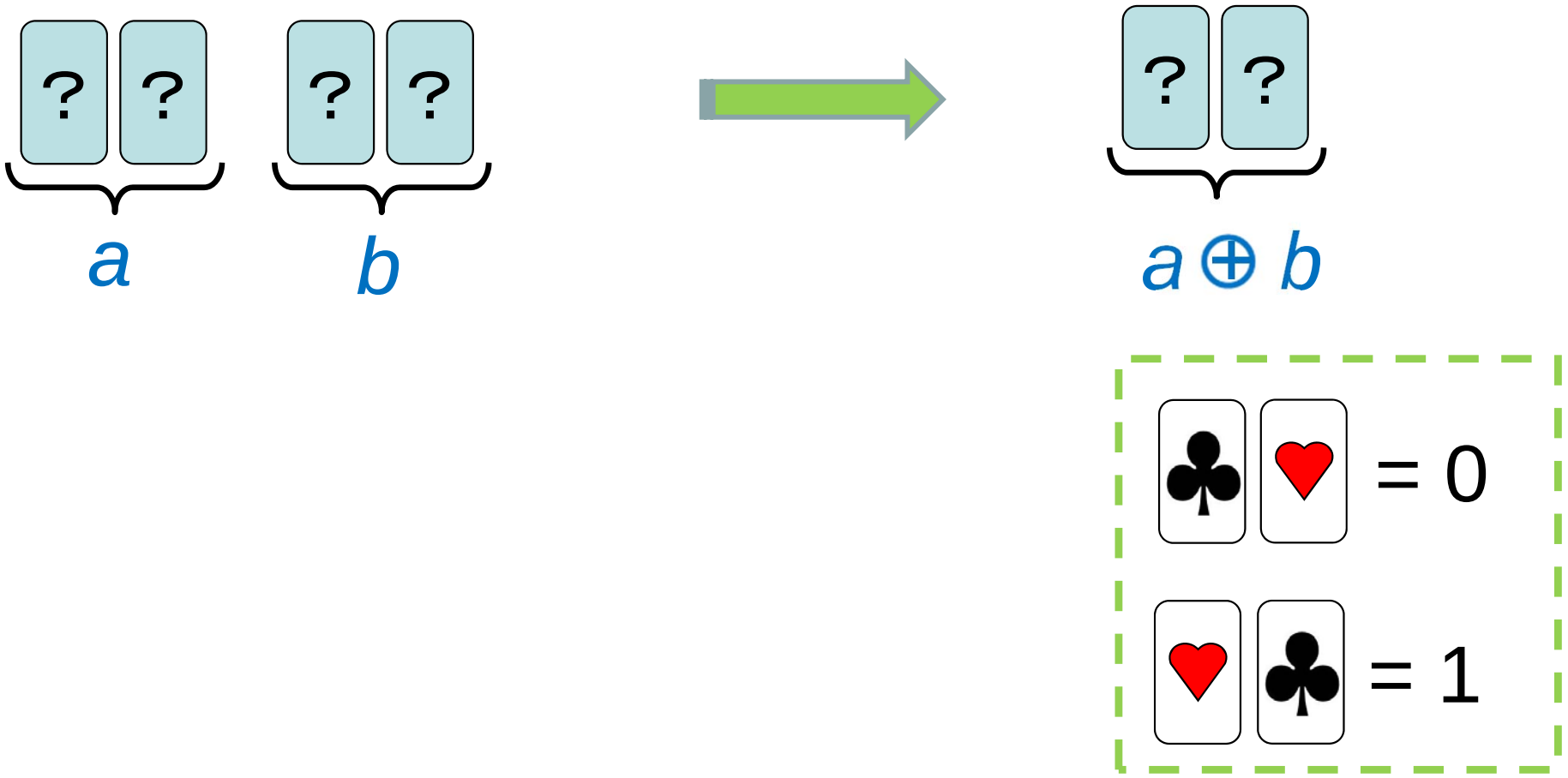

= 0
= 1
reveal
a ⊕ r
r ∧ b
= a ∧ b
a ⊕ r = 0, i.e., a = r
a ∧ b
a ∧ b


= 0
= 1
reveal
$a \oplus r$
$\bar{r} \wedge b$
$= a \wedge b$
$a \oplus r = 1$, i.e., $a = \bar{r}$
$a \wedge b$
$a \wedge b$

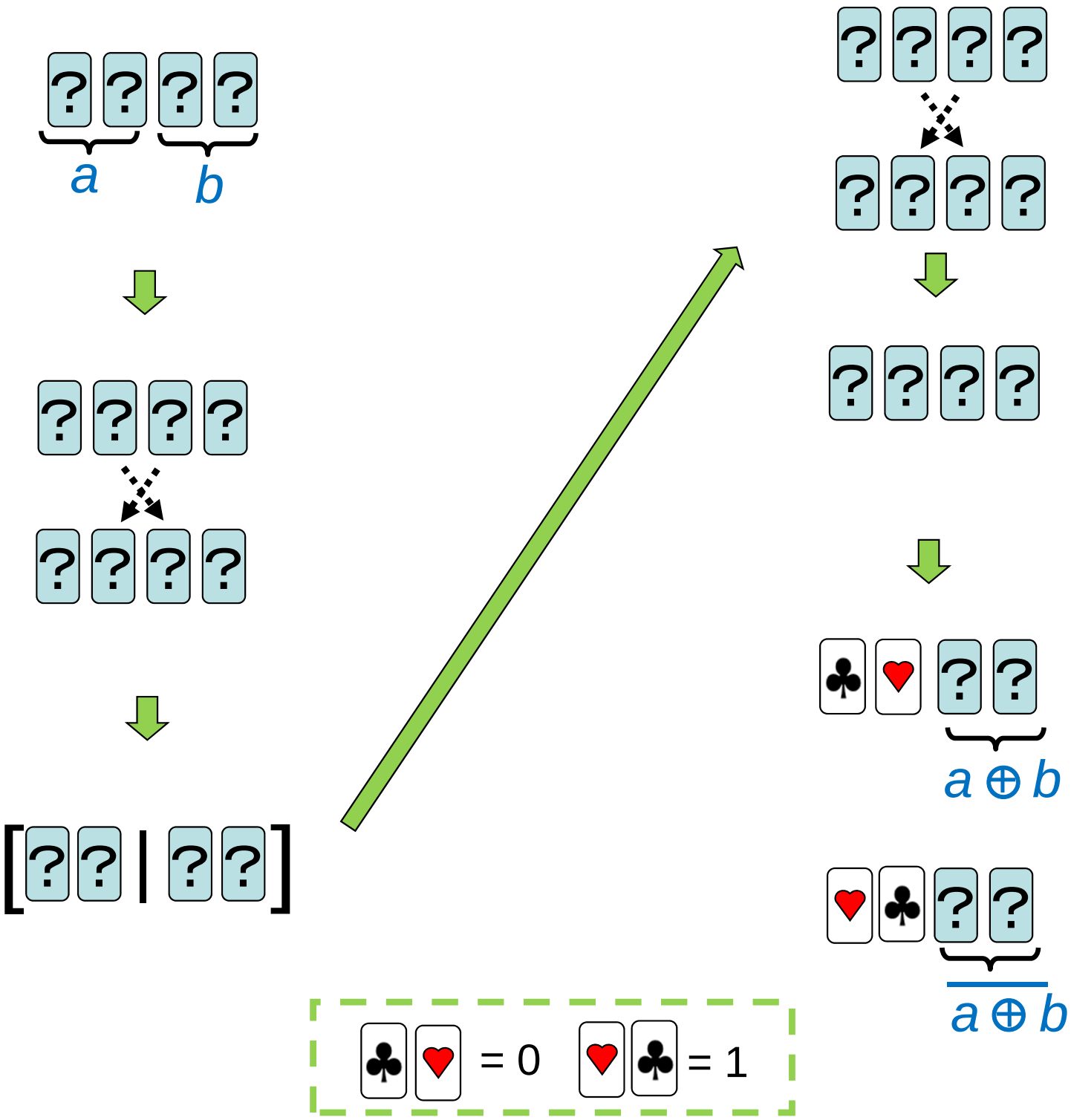

= 0
= 1
a
b
a
0
b
Works!
a ∧ b
a ∧ b

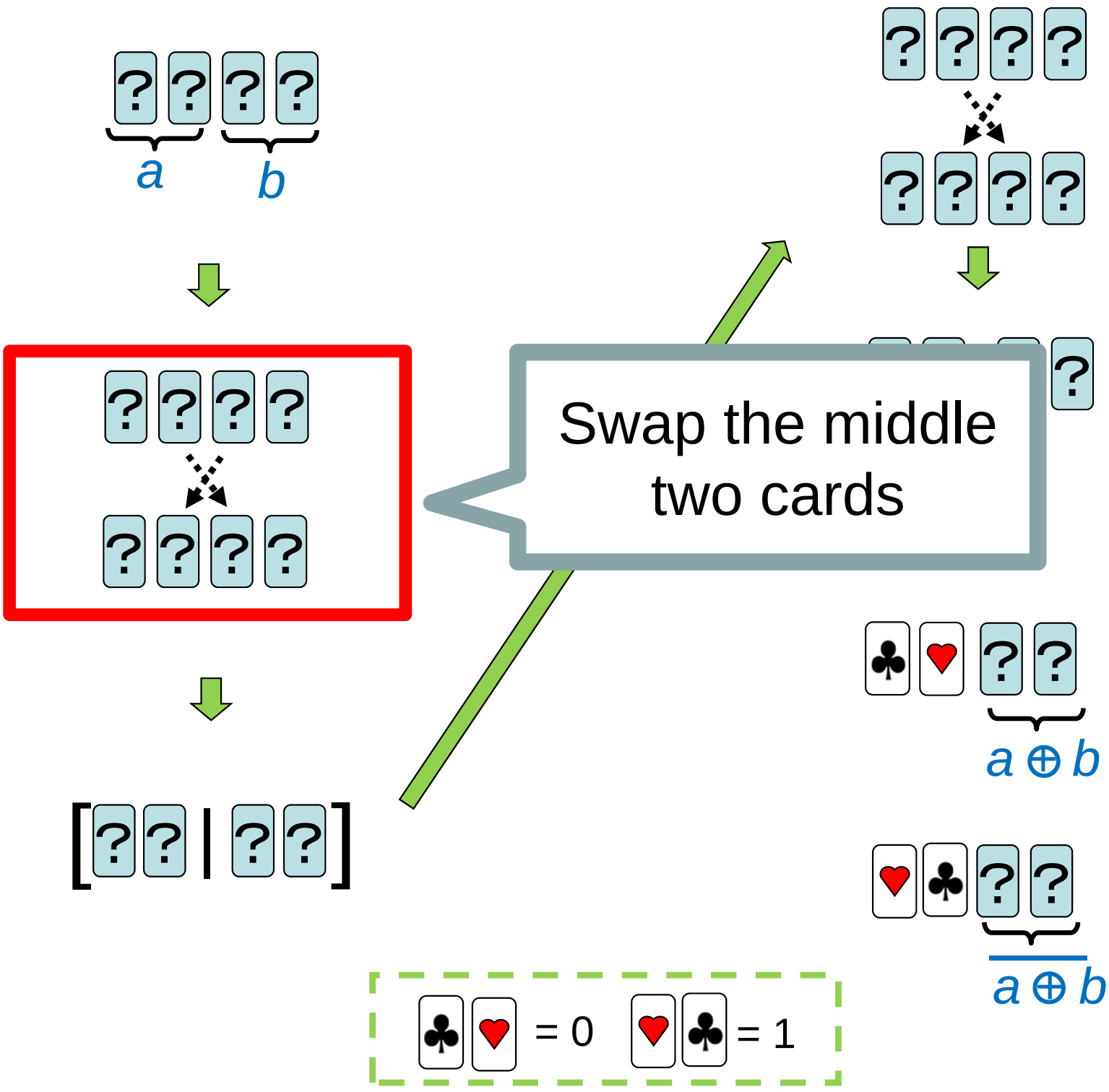
An existing committed-format XOR protocol

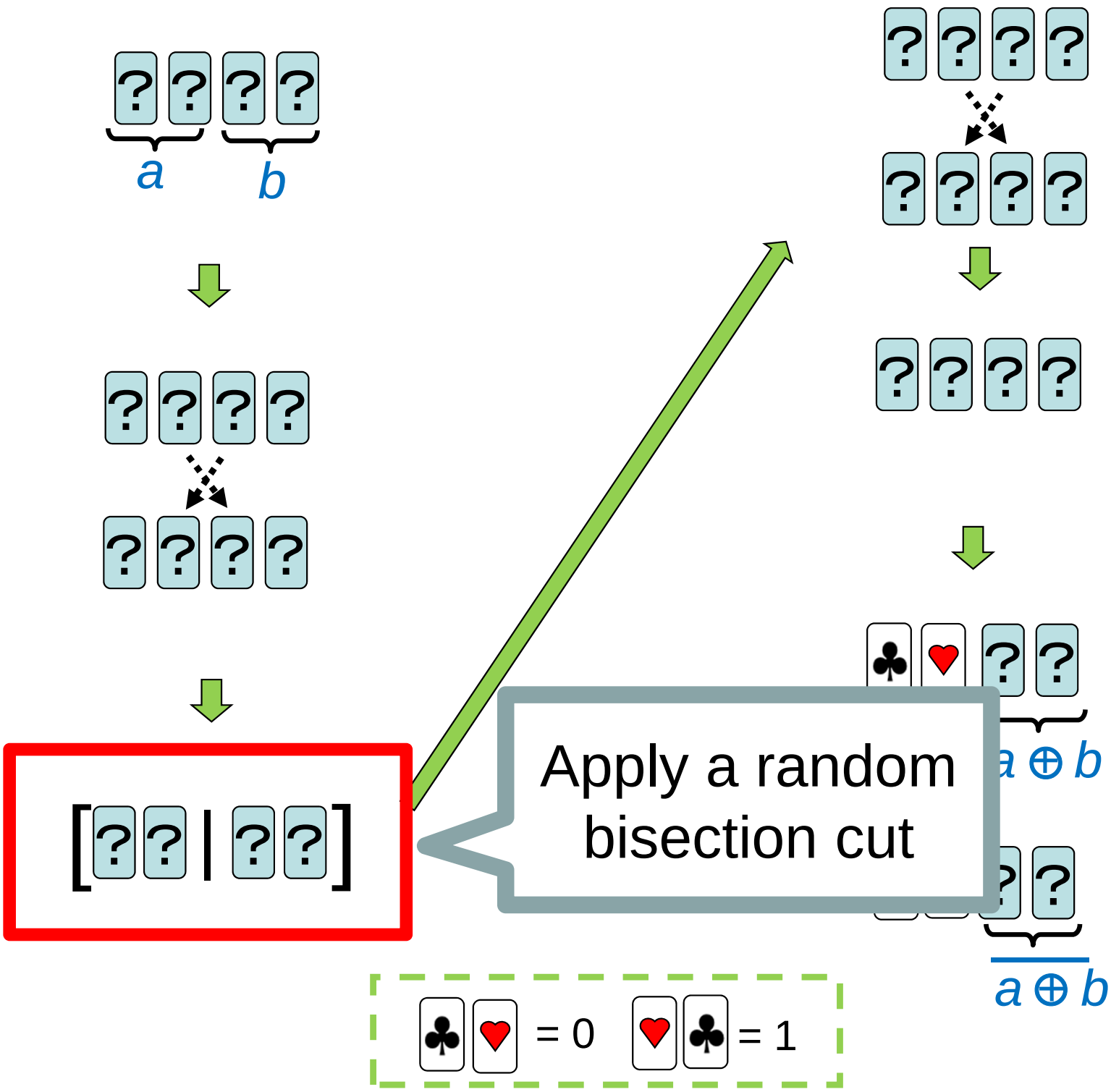
Secure XOR can be done with 4 cards [6].

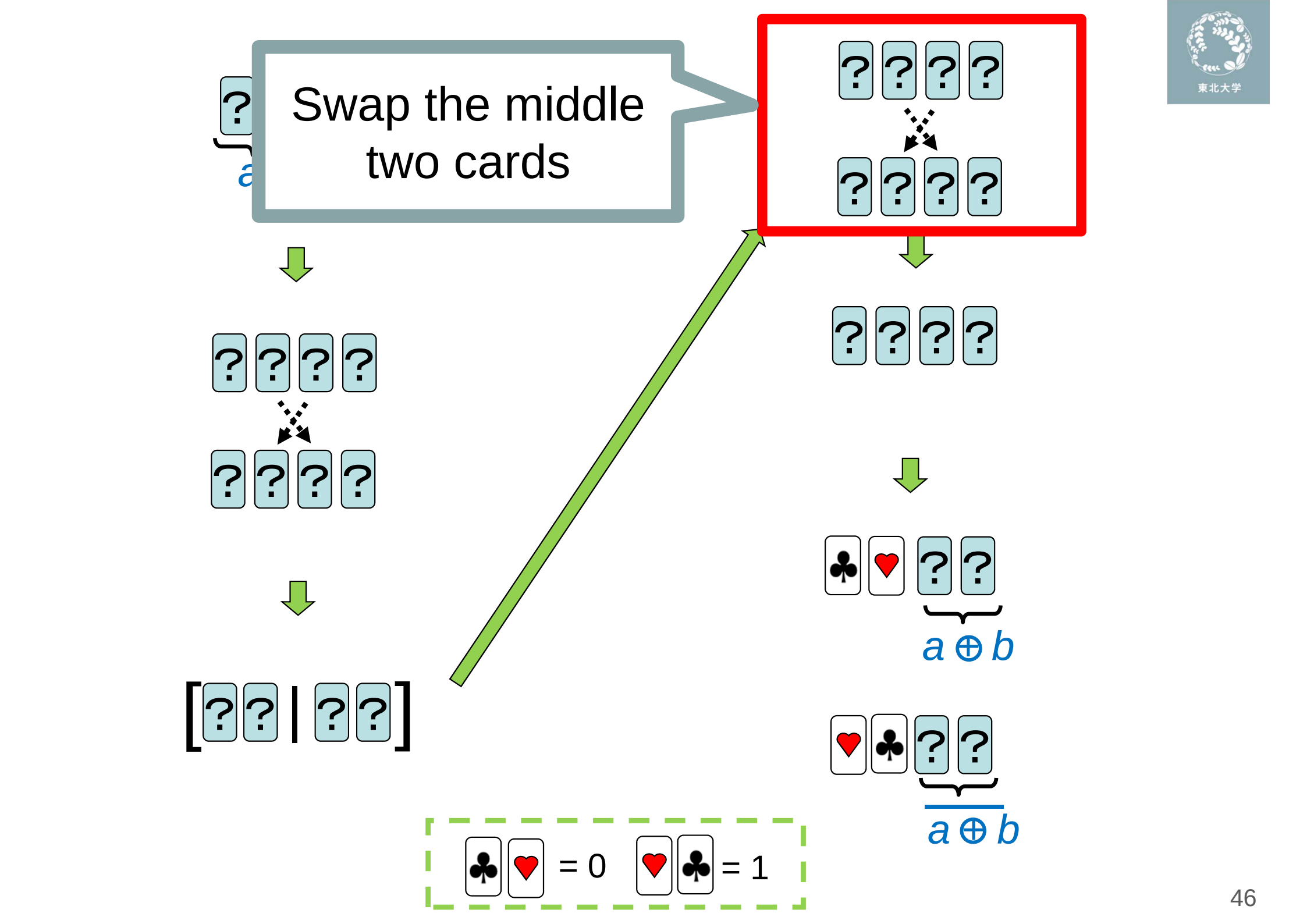


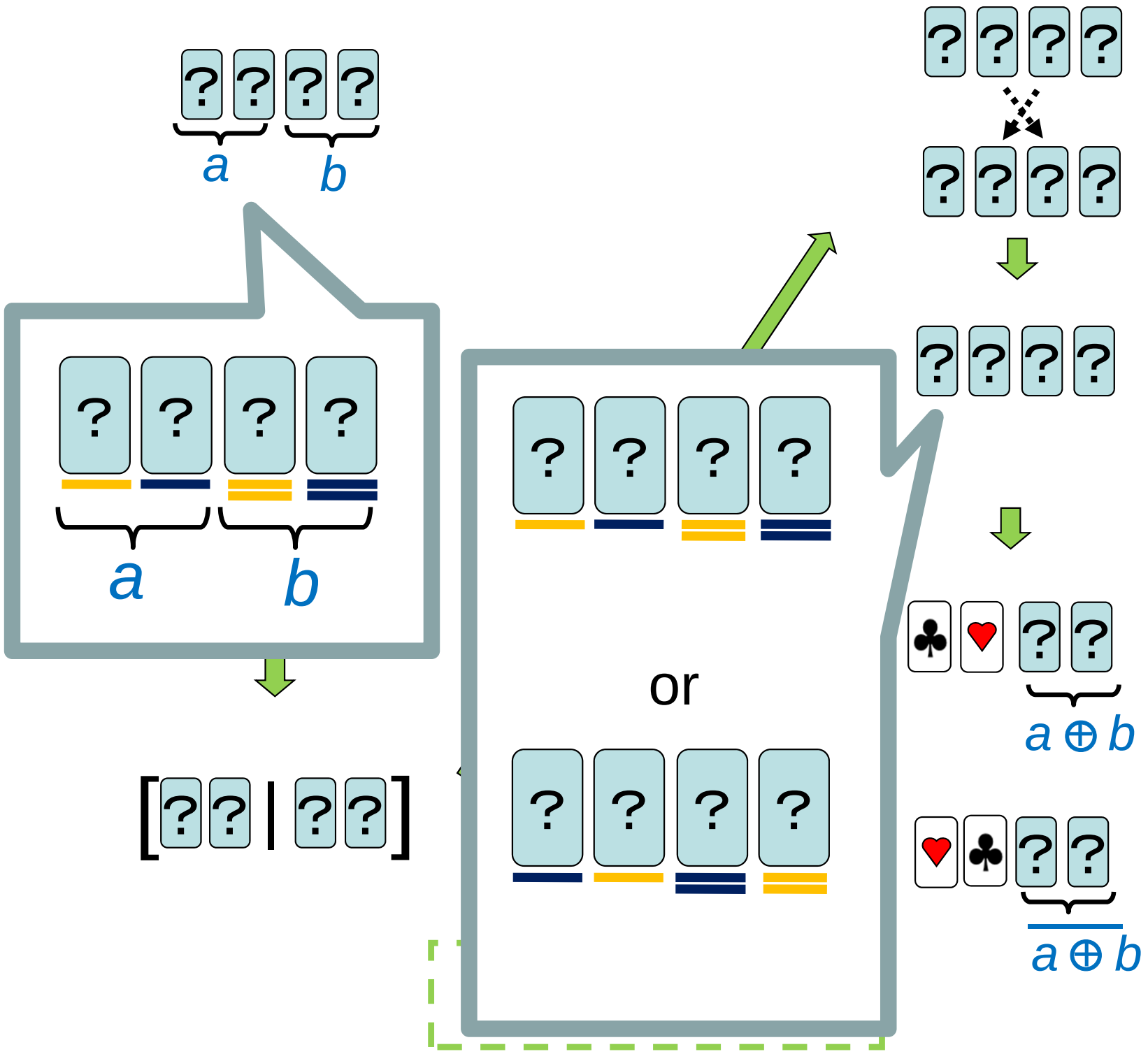
[6] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

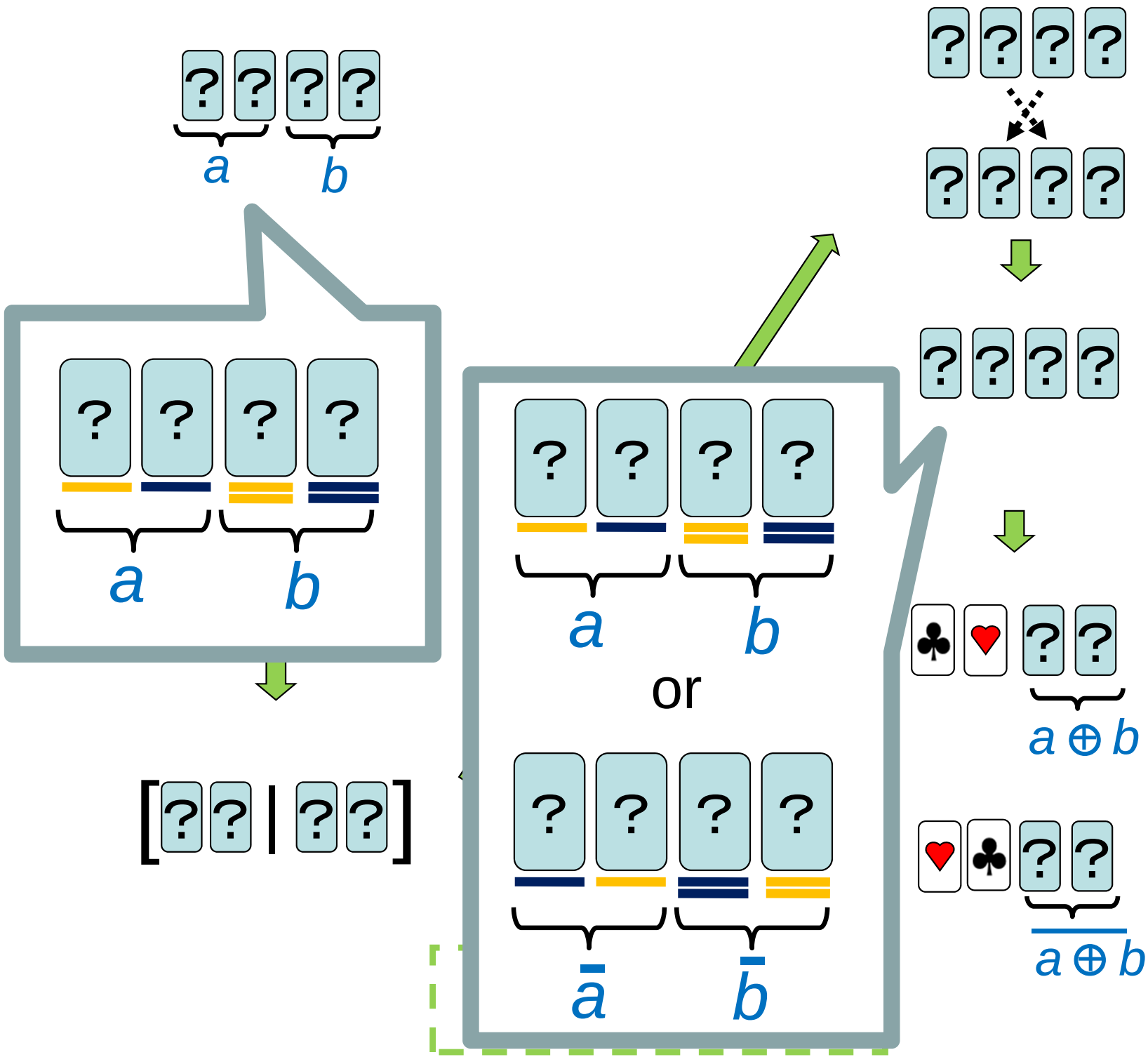

a
b
a ⊕ b
a ⊕ b
= 0
= 1

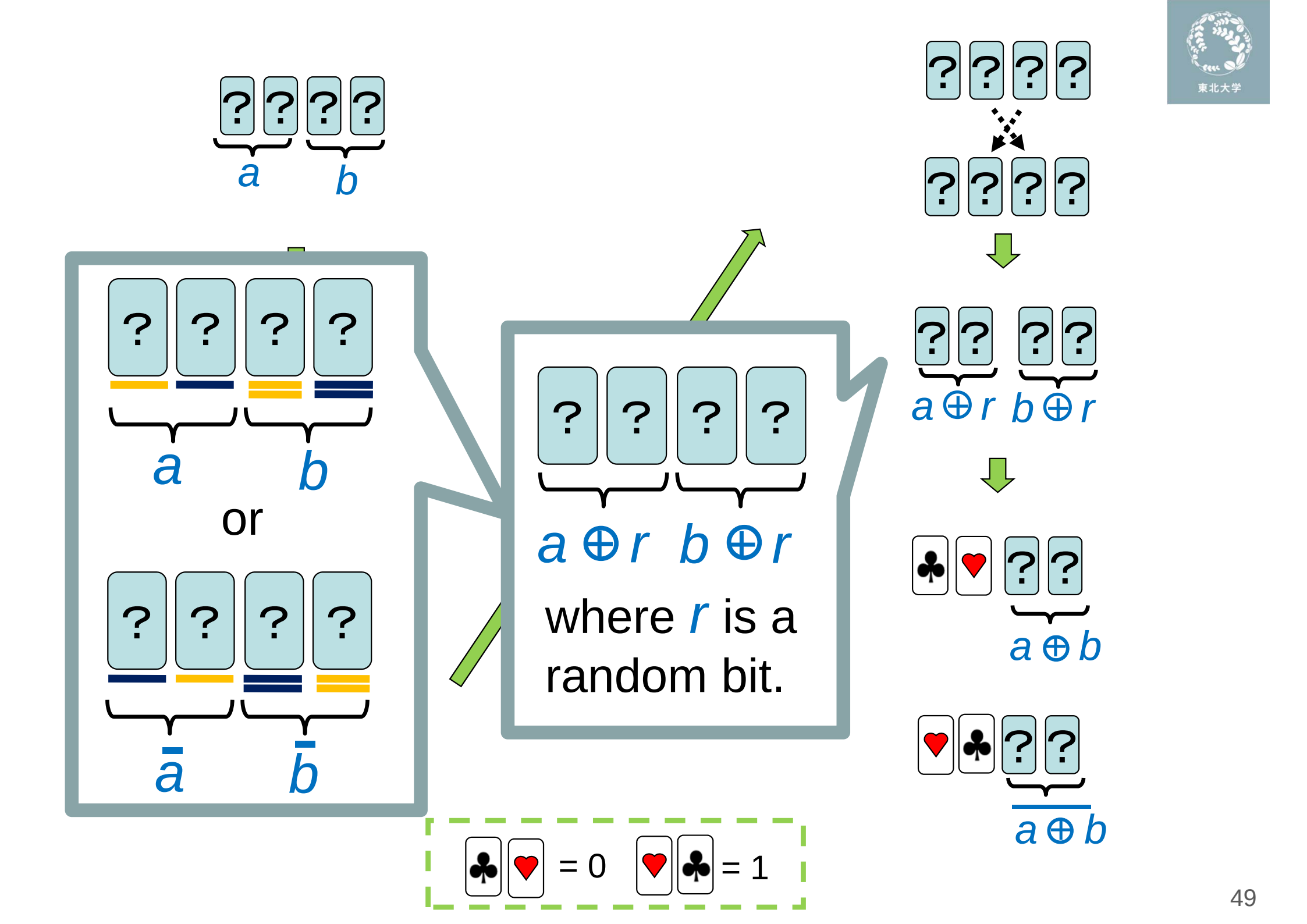

a
b
Swap the middle two cards
a ⊕ b
a ⊕ b
= 0
= 1

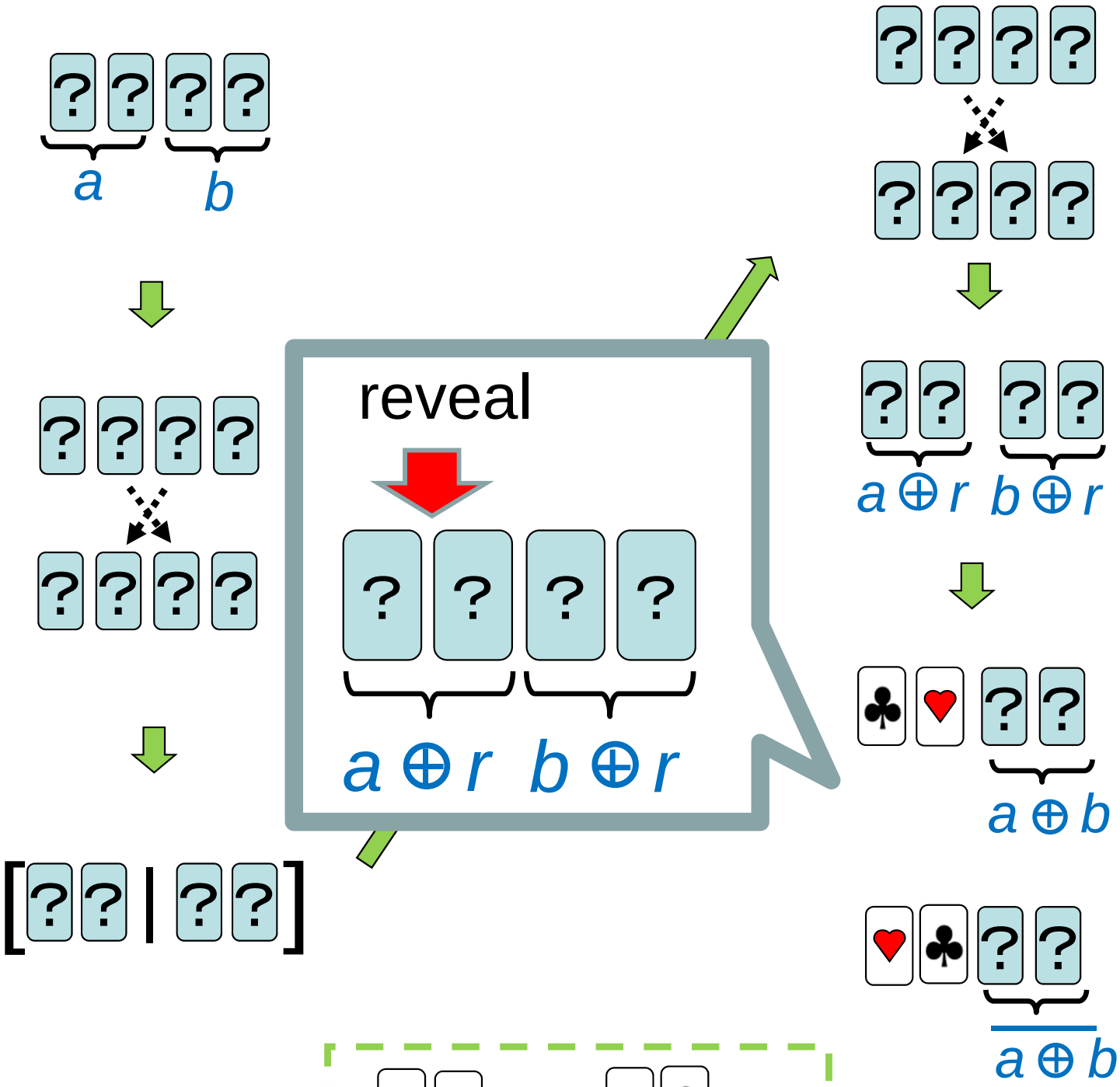

a
b
[|]
Apply a random bisection cut
a ⊕ b
a ⊕ b
= 0
= 1

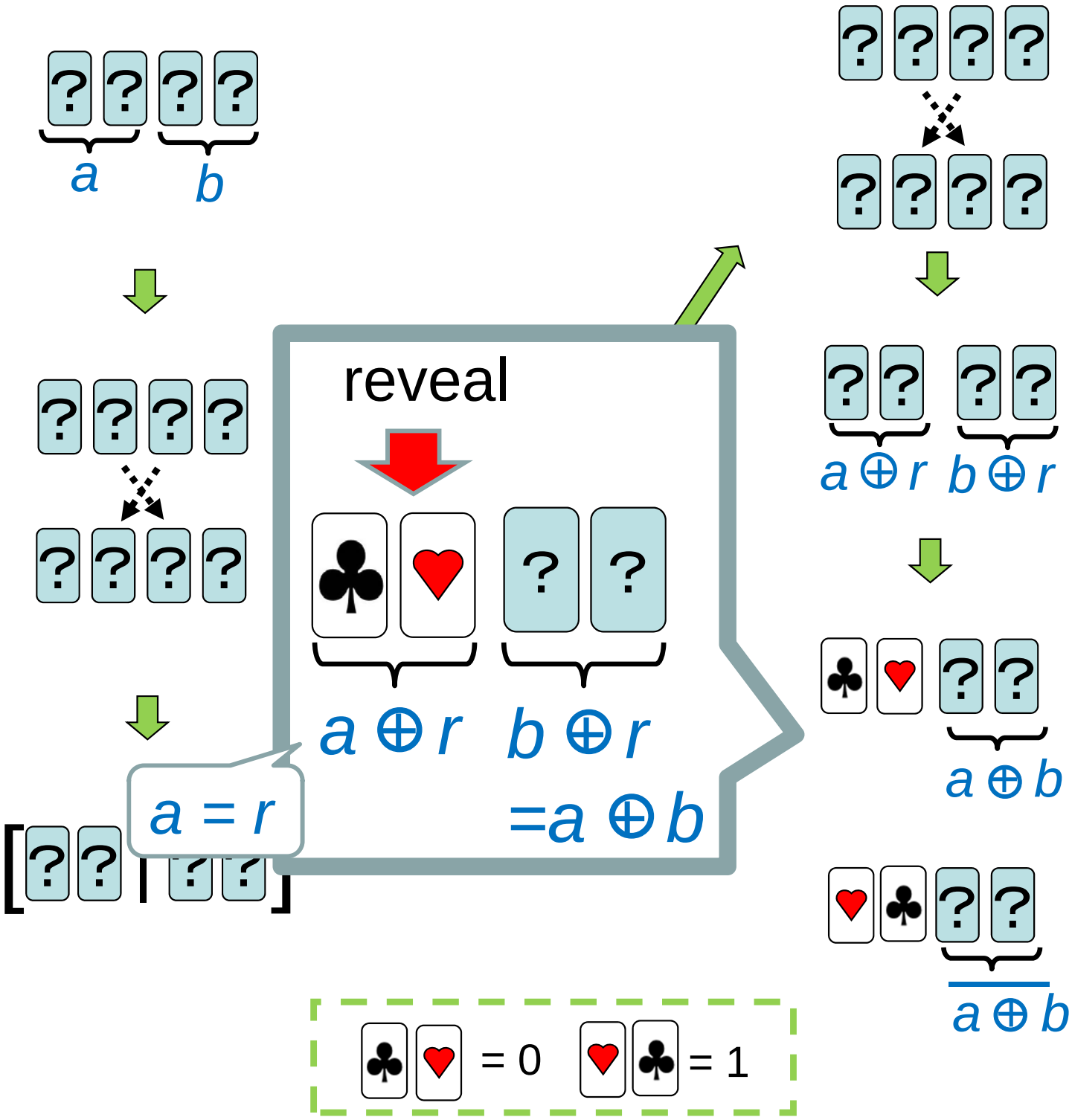

Swap the middle two cards
a
a ⊕ b
a ⊕ b
= 0
= 1

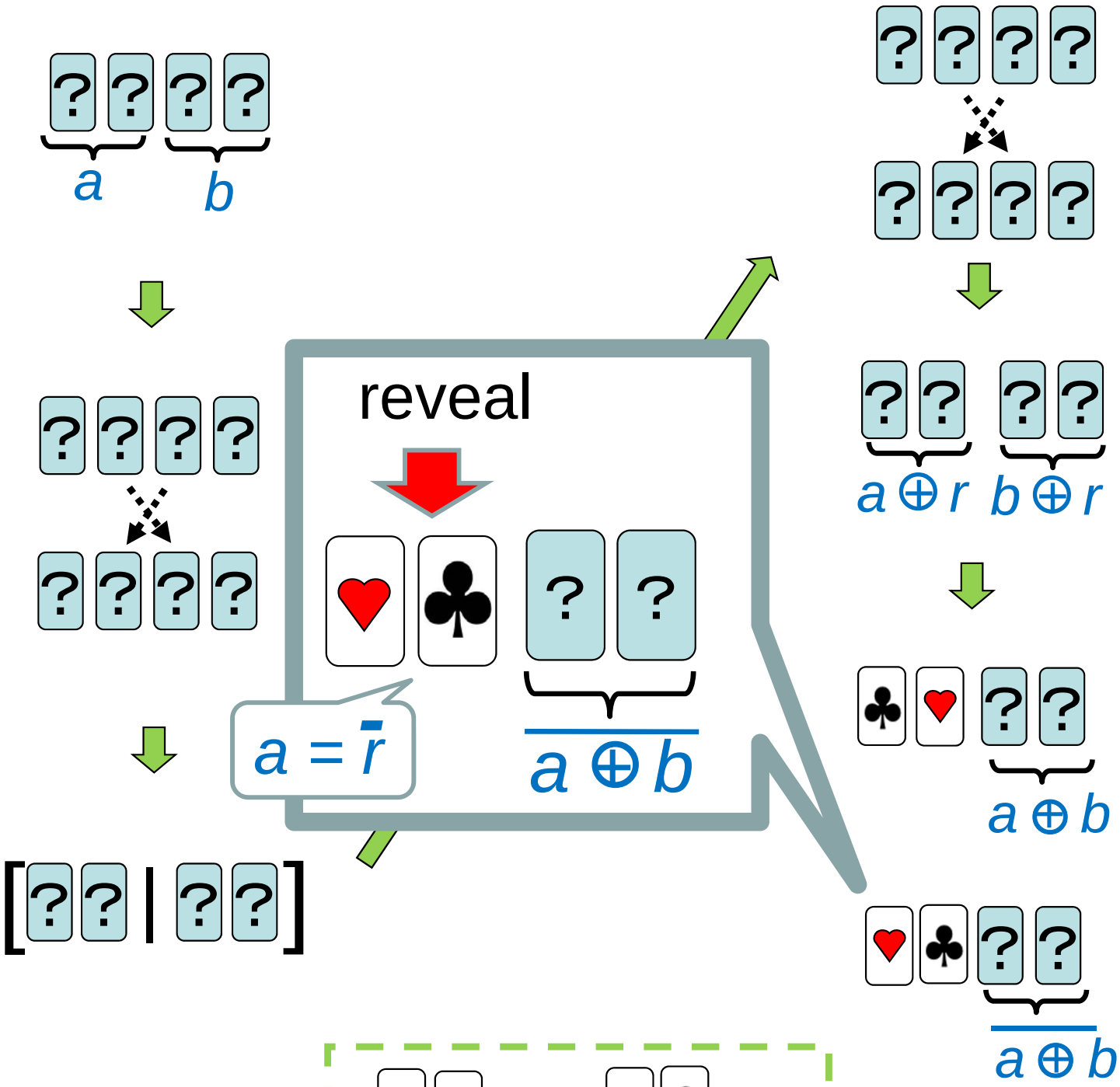

a
b
a
b
or
[|]
a ⊕ b
a ⊕ b

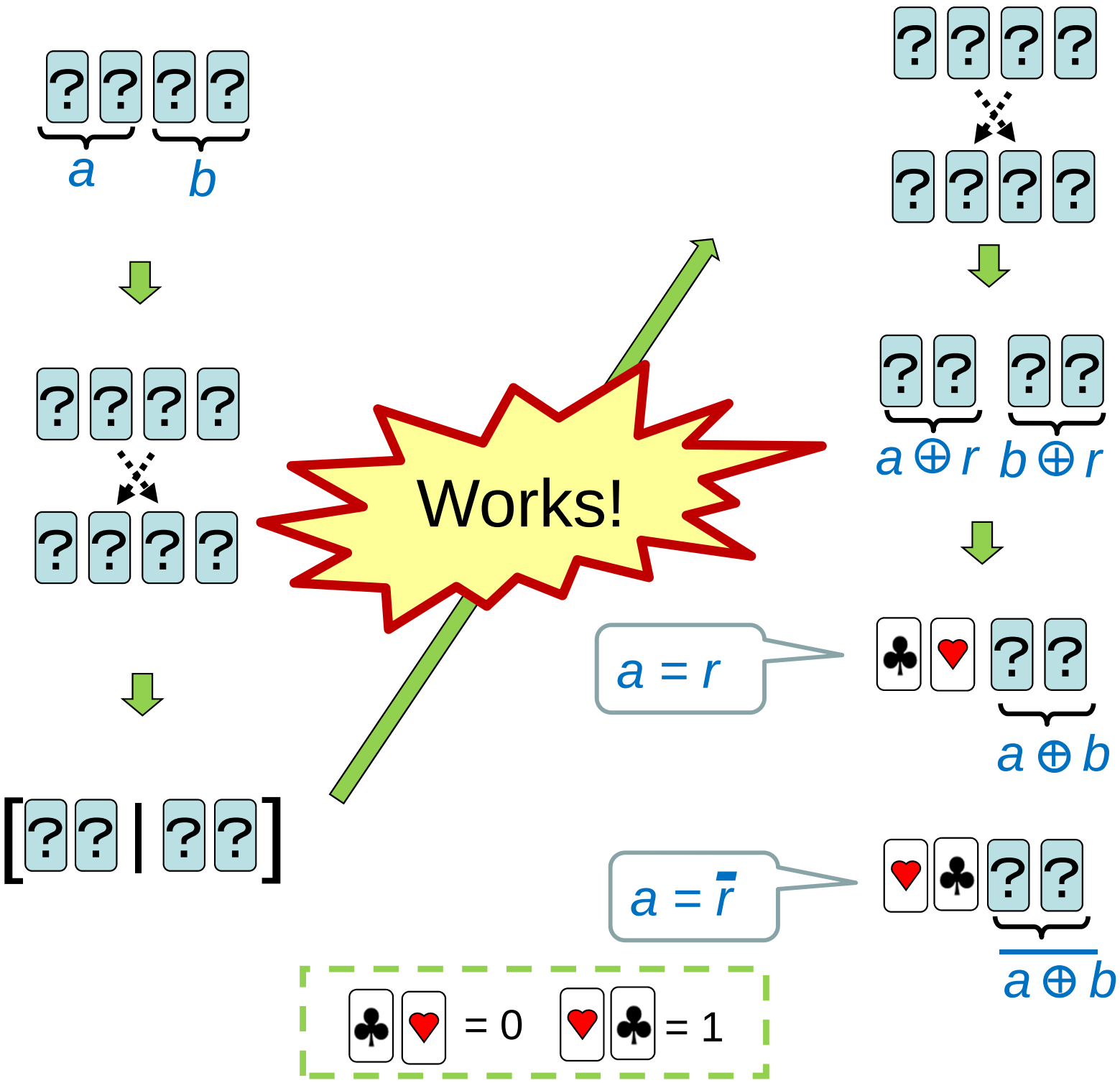

a
b
a
b
a
b
or
ā
b̄
[|]
a ⊕ b
a ⊕ b


? ? ? ?
a b
? ? ? ?
a b
or
? ? ? ?
ā b̄
? ? ? ?
a ⊕ r b ⊕ r
where r is a random bit.
? ? ? ?
? ? ? ?
? ? ? ?
a ⊕ r b ⊕ r
? ? ? ?
a ⊕ b
? ? ? ?
a ⊕ b
= 0
= 1


a
b
reveal
a ⊕ r b ⊕ r
a ⊕ r b ⊕ r
a ⊕ b
a ⊕ b
= 0
= 1


a
b
reveal
a ⊕ r
b ⊕ r
=a ⊕ b
a = r
a ⊕ r
b ⊕ r
a ⊕ b
a ⊕ b
= 0
= 1

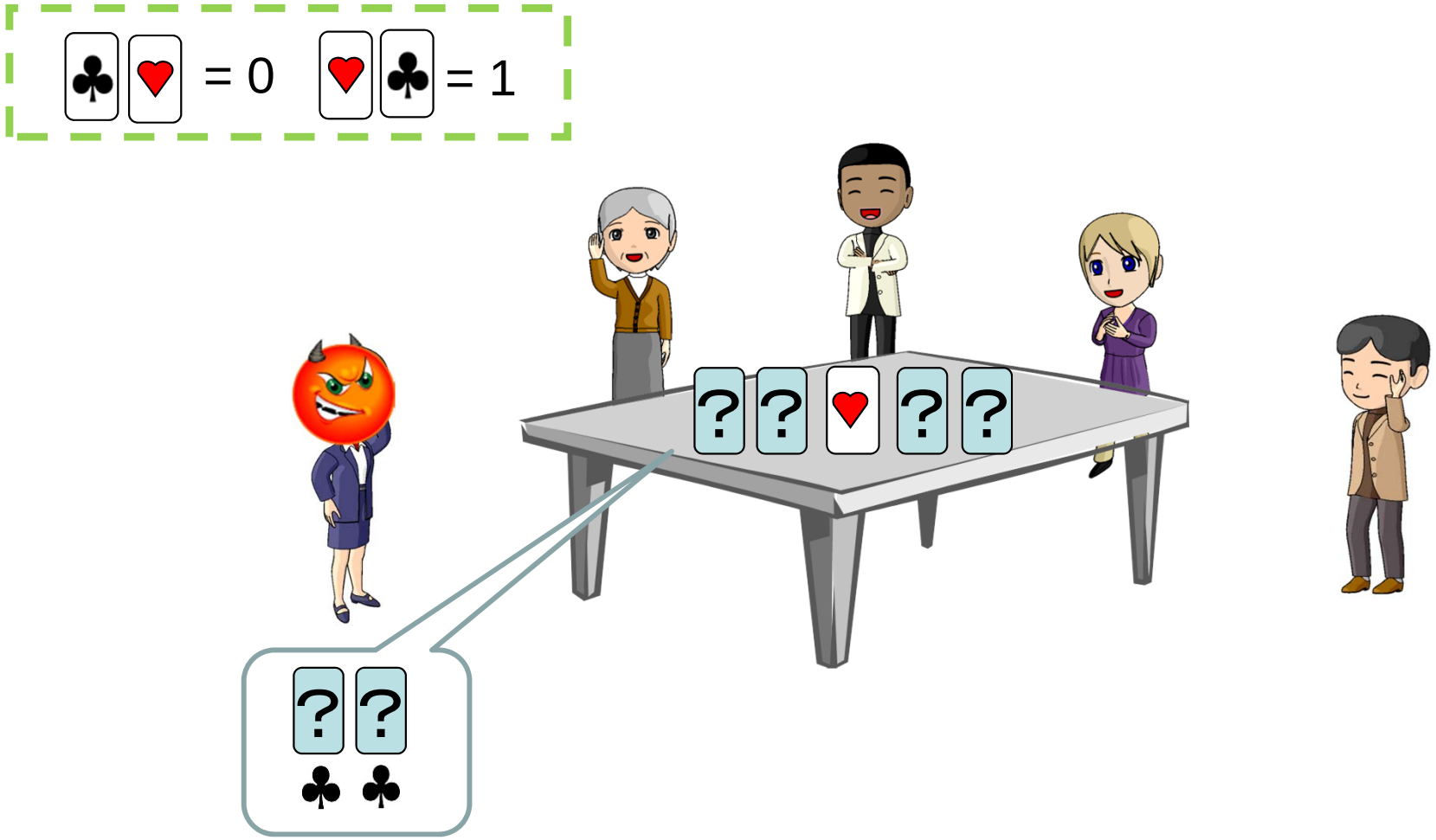

a
b
reveal
a = r̄
a ⊕ b
a ⊕ r
b ⊕ r
a ⊕ b
a ⊕ b
= 0
= 1


a
b
Works!
a ⊕ r
b ⊕ r
a = r
a ⊕ b
a = r̄
a ⊕ b
= 0
= 1

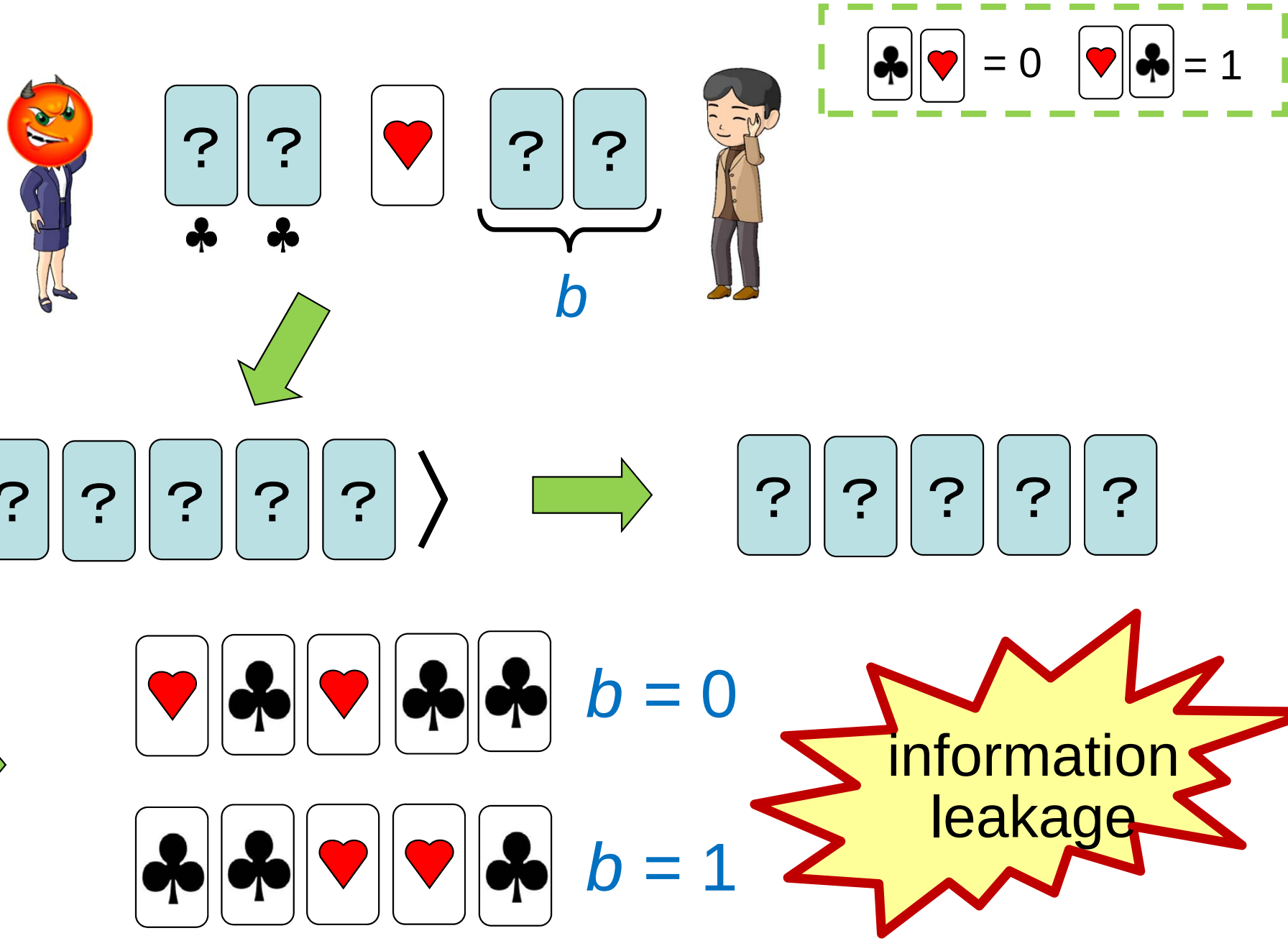
Contents

1. Introduction
2. Existing Committed-Format AND/XOR Protocols
3. Attack Exploiting Input Format
4. Backs with a Rotationally Symmetric Pattern
5. Backs with Scuff Marks
6. Conclusion

“Injection Attack”: not following the encoding rule

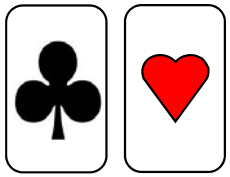


An attack example for the five-card trick



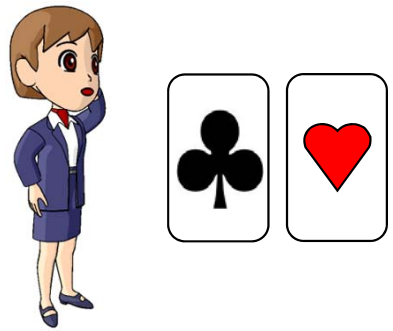
One possible way：

To hand only one pair of a black card and a red one to Alice.

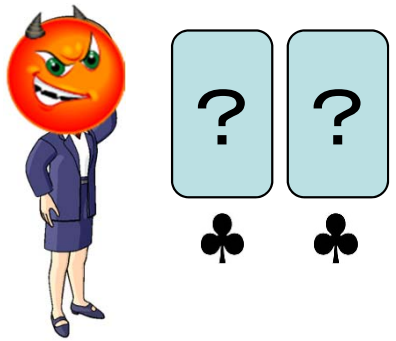


One possible way：

To hand only one pair of a black card and a red one to Alice.



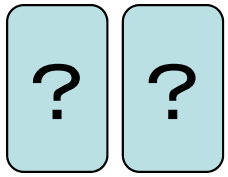
However, it is possible that Alice could conceal her action when she makes her commitment, and hence, the situation where she is able to input an “injection” covertly may reasonably occur.

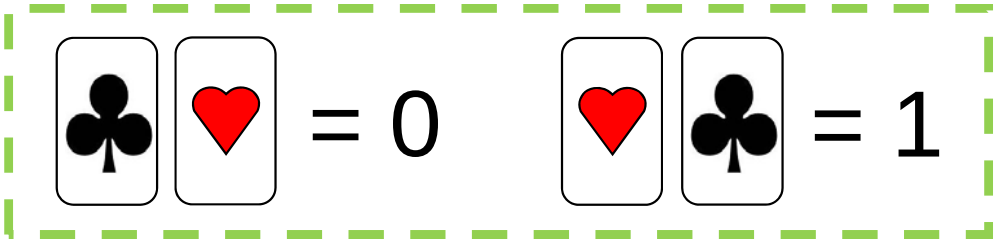


We need a more general solution.

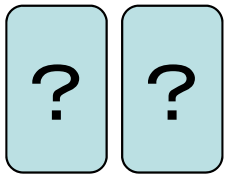
Our countermeasure

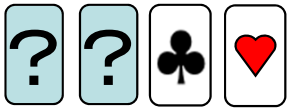
The idea：to check if a pair follows the encoding

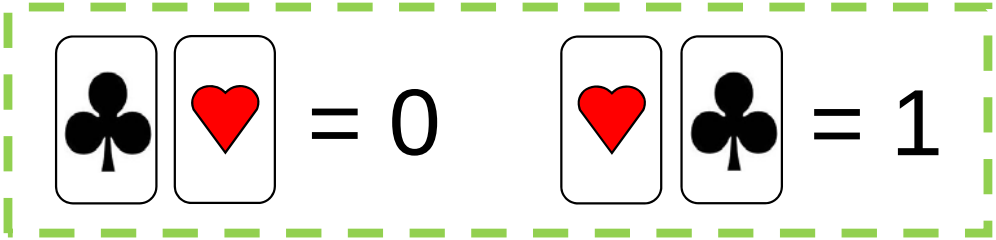




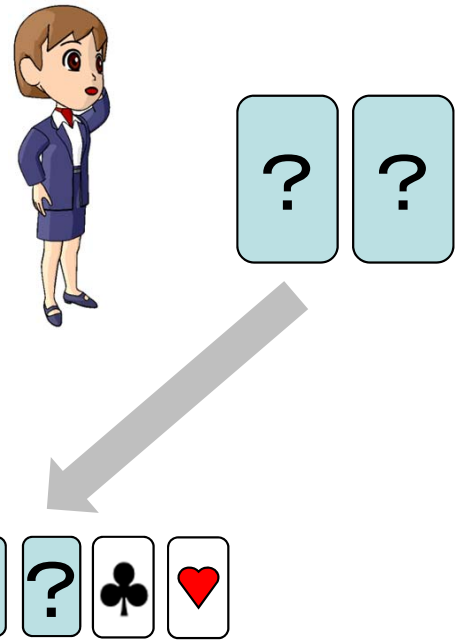
Our countermeasure

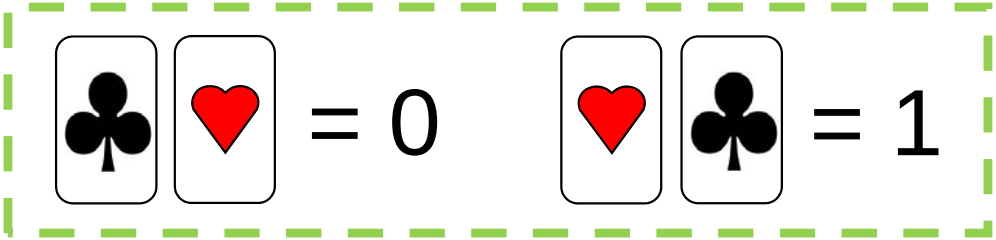






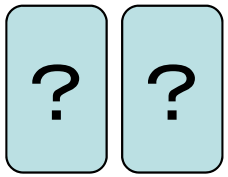
Our countermeasure

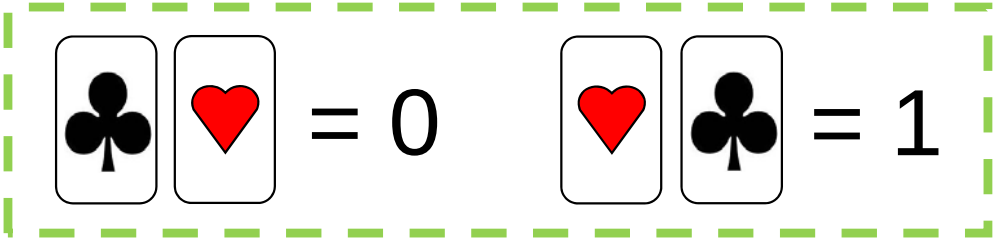


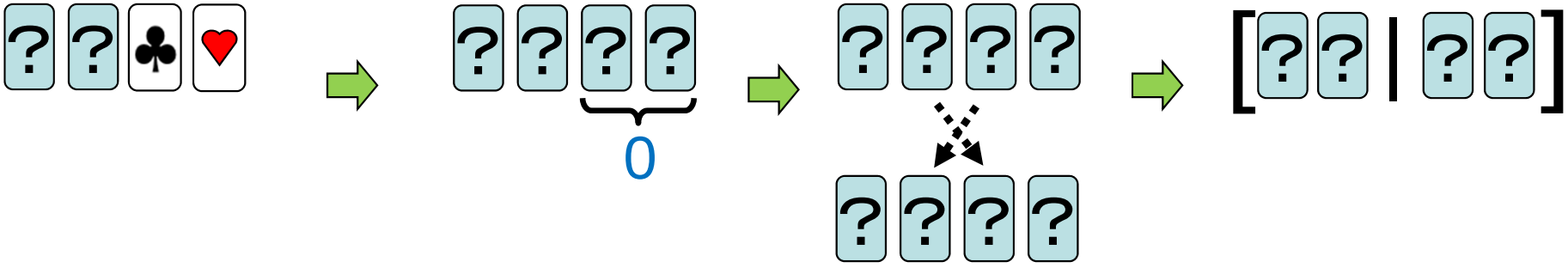


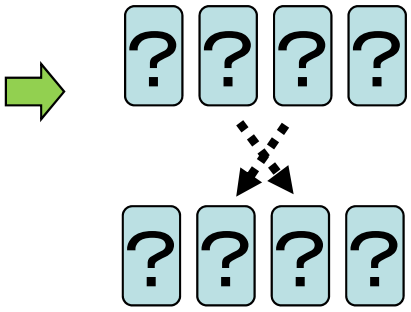
Apply the same procedure as the 4-card XOR protocol mentioned in the previous section.

Our countermeasure

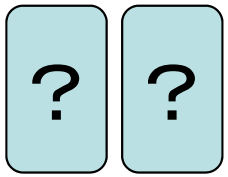


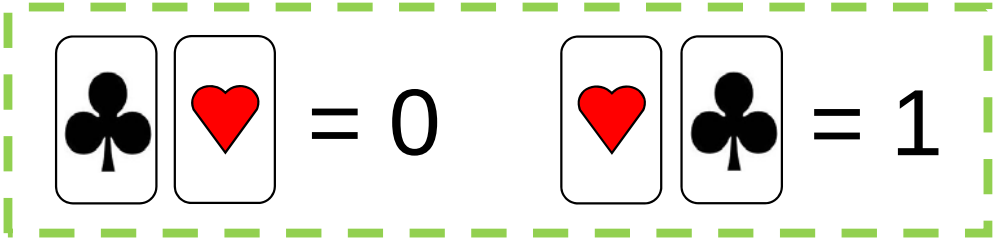


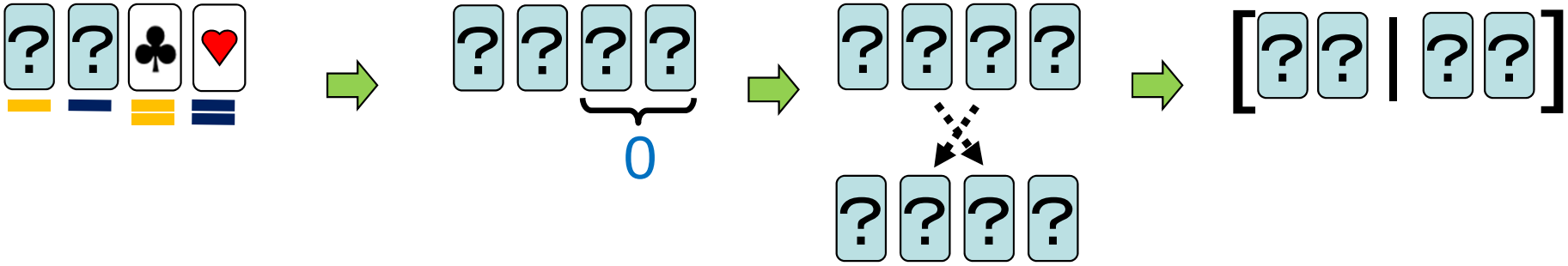


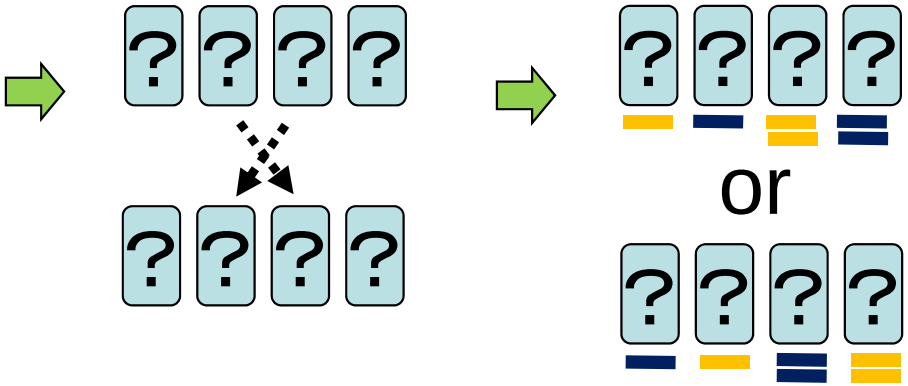


Our countermeasure

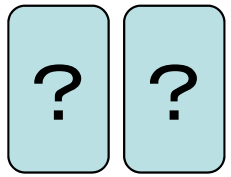


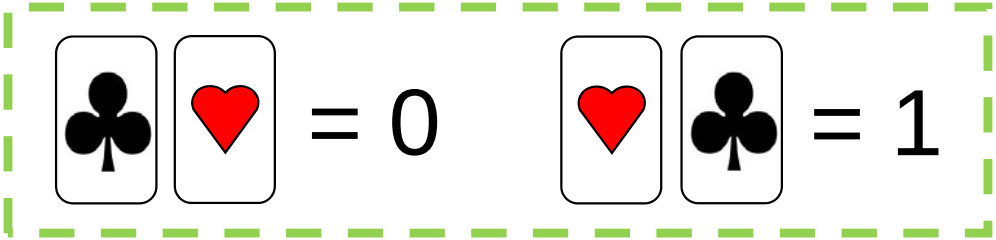


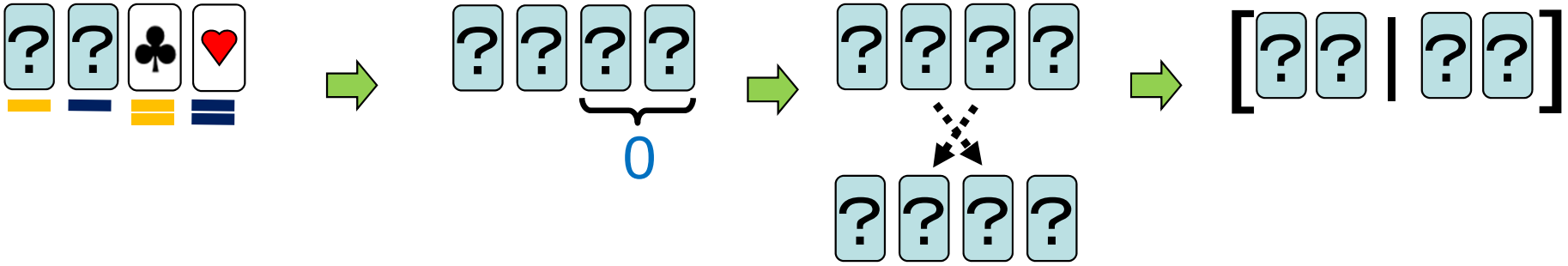


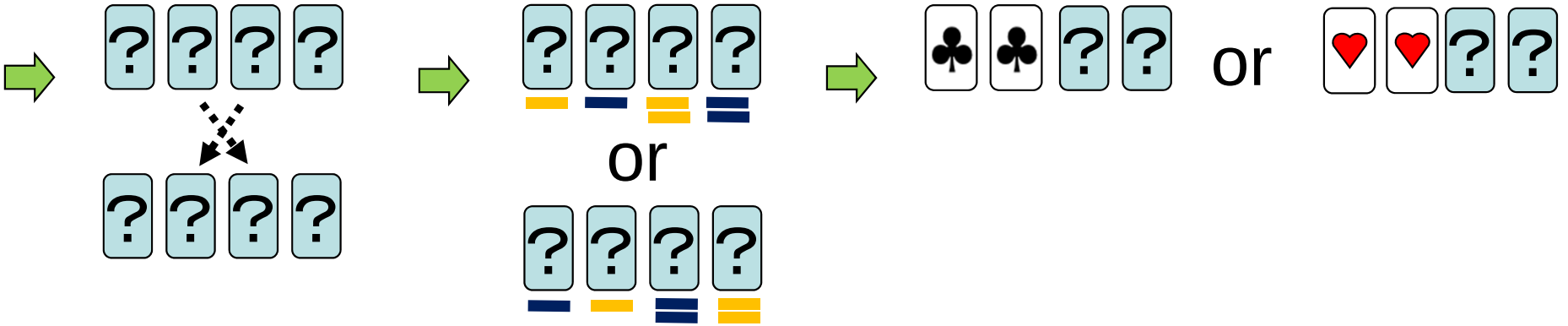


Our countermeasure

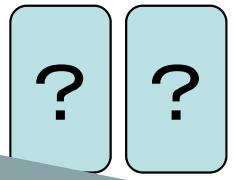


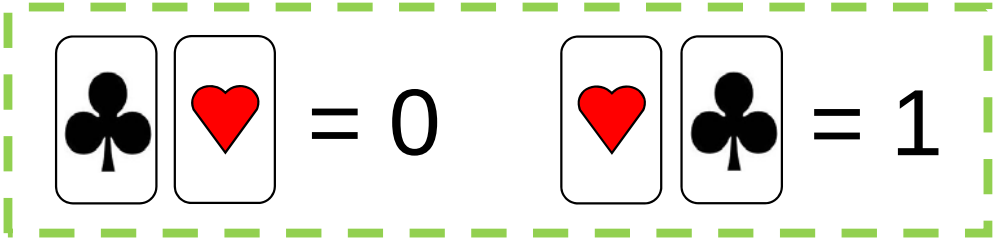




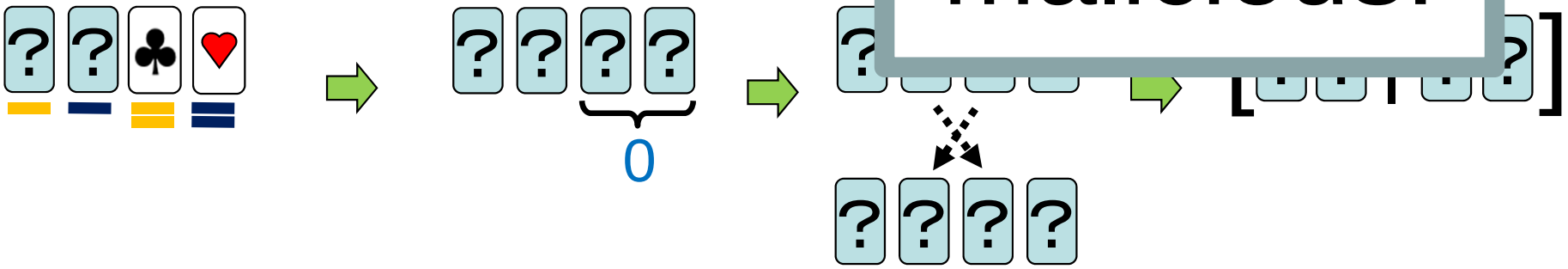


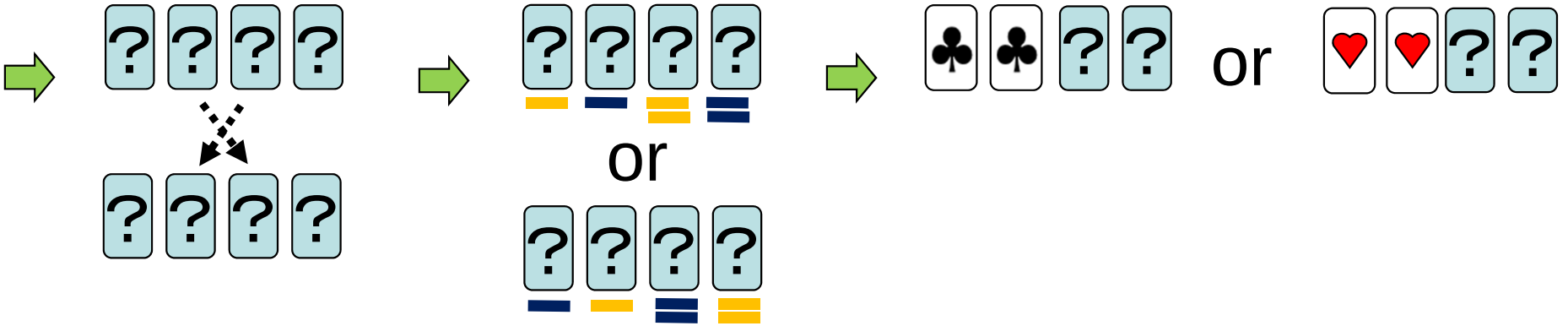
Our countermeasure



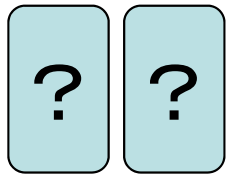


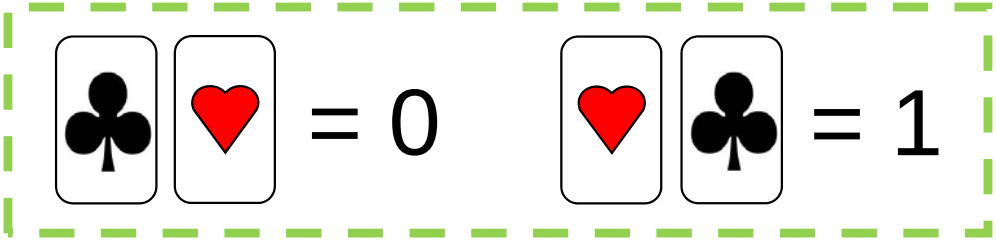
malicious!

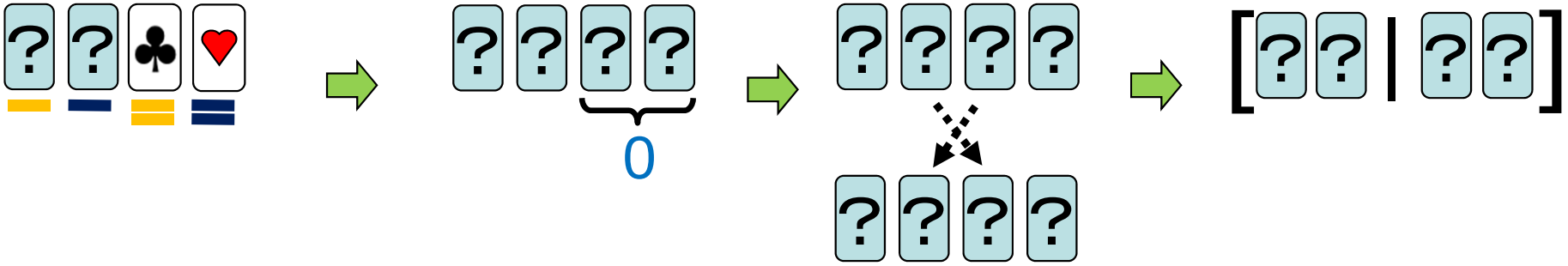


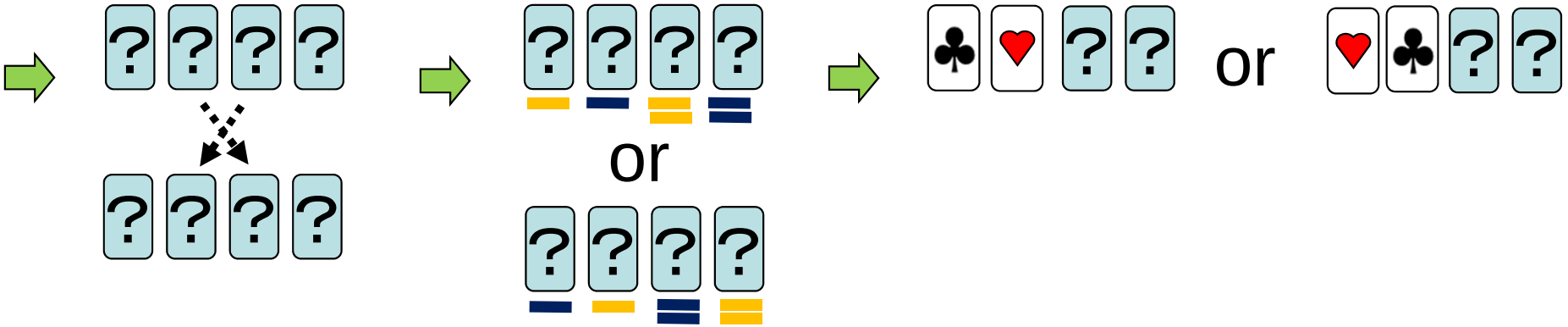


Our countermeasure

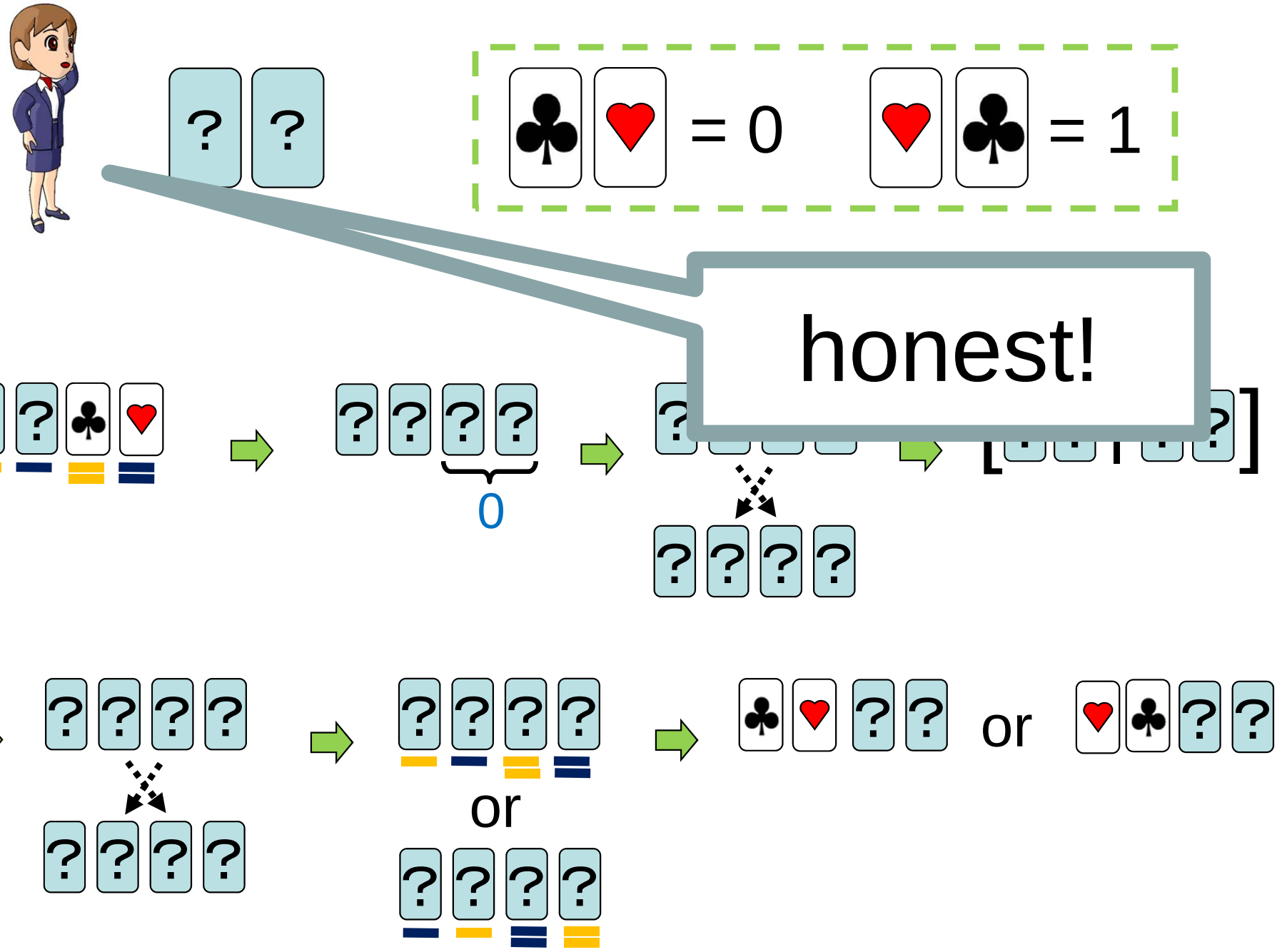




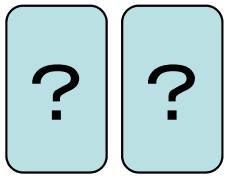


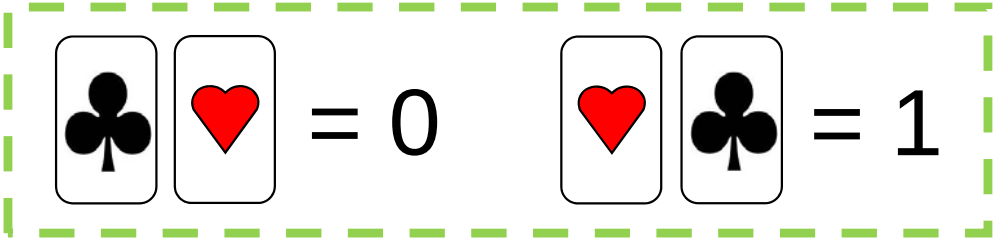


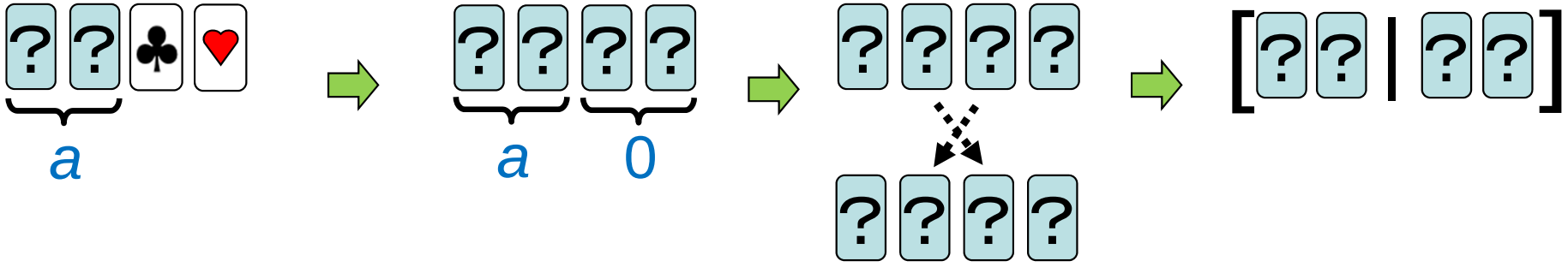
Our countermeasure

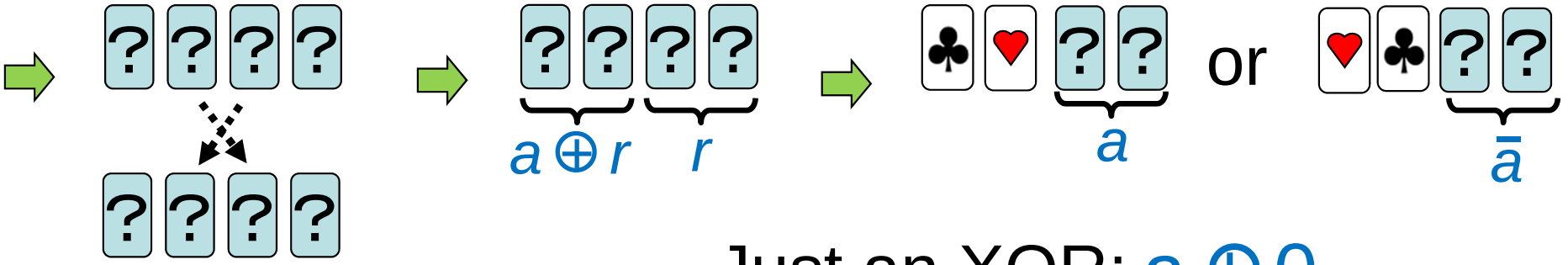


Our countermeasure









Just an XOR: $a \oplus 0$

Our countermeasure

? ?

♣ ♥ = 0 ♥ ♣ = 1

We can keep a commitment to a without leaking its value

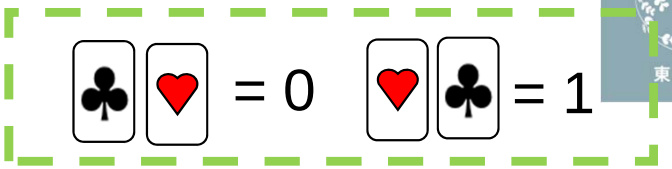
? ? ♣ ♥ → ? ? ? ? → ? ? ? ?

a a 0

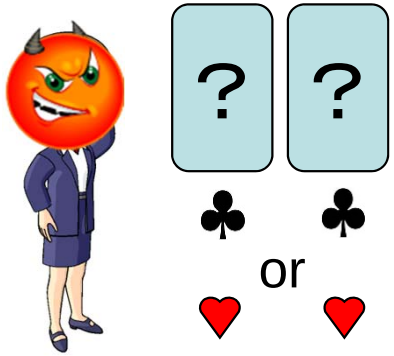
→ ? ? ? ? → ? ? ? ? → ♣ ♥ ? ? or ♥ ♣ ? ?

$a \oplus r$ r a $\bar{a}$

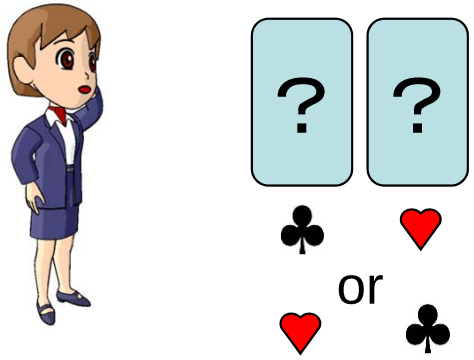
Summary of our countermeasure:



If the input is not in a correct format, we can detect it.



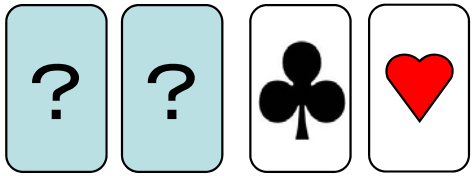
If the input is in a correct format, we can prove it without leaking any information of the secret bit.



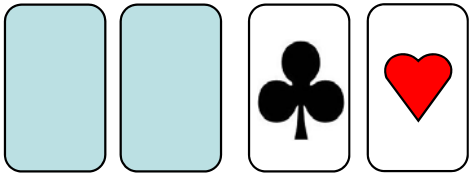
Contents

1. Introduction
2. Existing Committed-Format AND/XOR Protocols
3. Attack Exploiting Input Format
4. Backs with a Rotationally Symmetric Pattern
5. Backs with Scuff Marks
6. Conclusion

Backs with a non-rotationally symmetric pattern

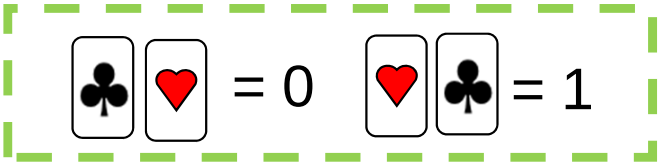


Backs with a rotationally symmetric pattern

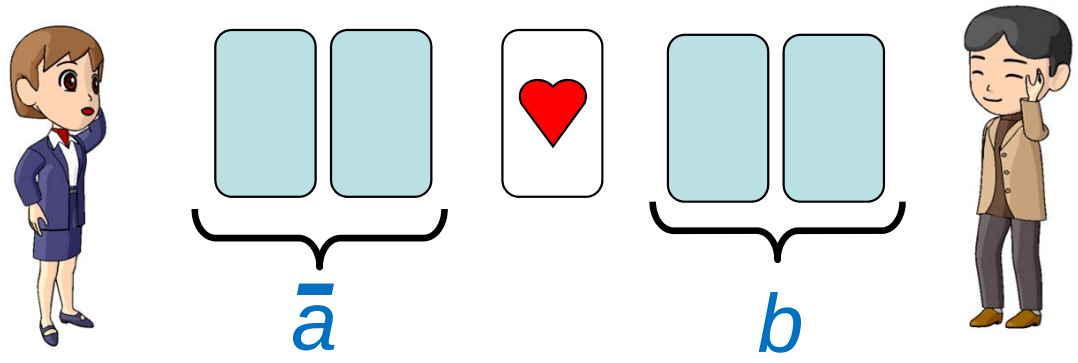


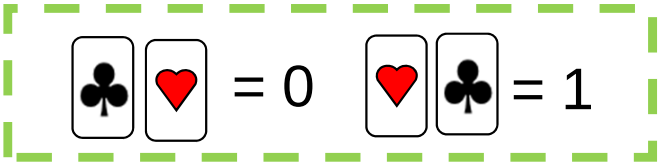
(plain-colored backs)
Pros and Cons

Disadvantages:



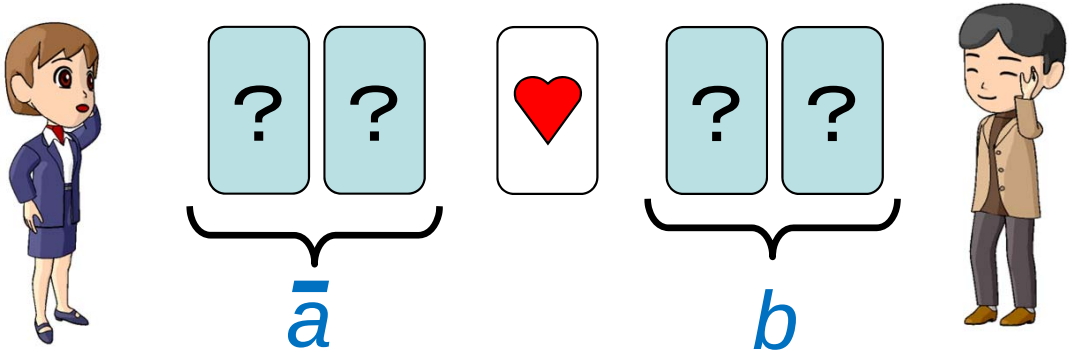
Disadvantages:



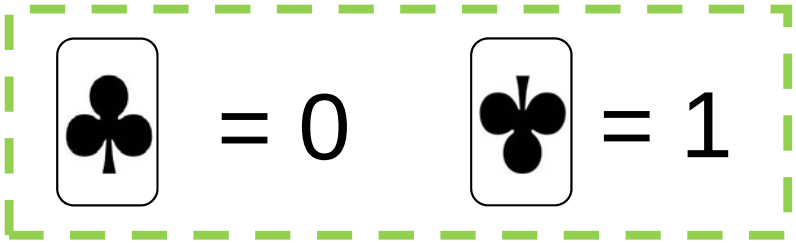


One should note up/down directions of cards.
One can utilize the format-check method given in the previous section.

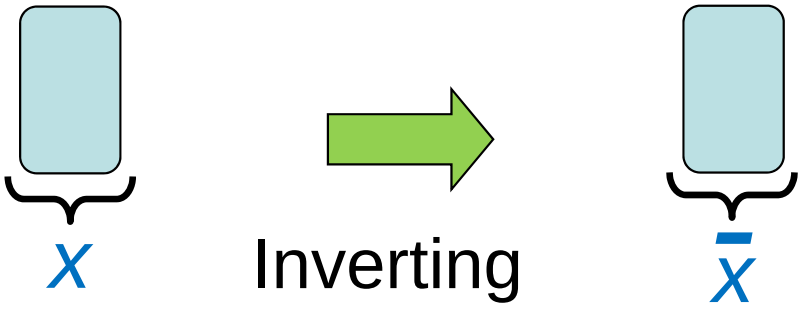
In this sense, non-rotationally symmetric backs would be better.



Advantages:

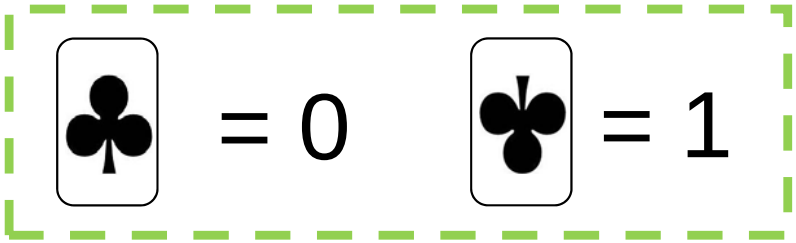


Encoding a bit with only one card

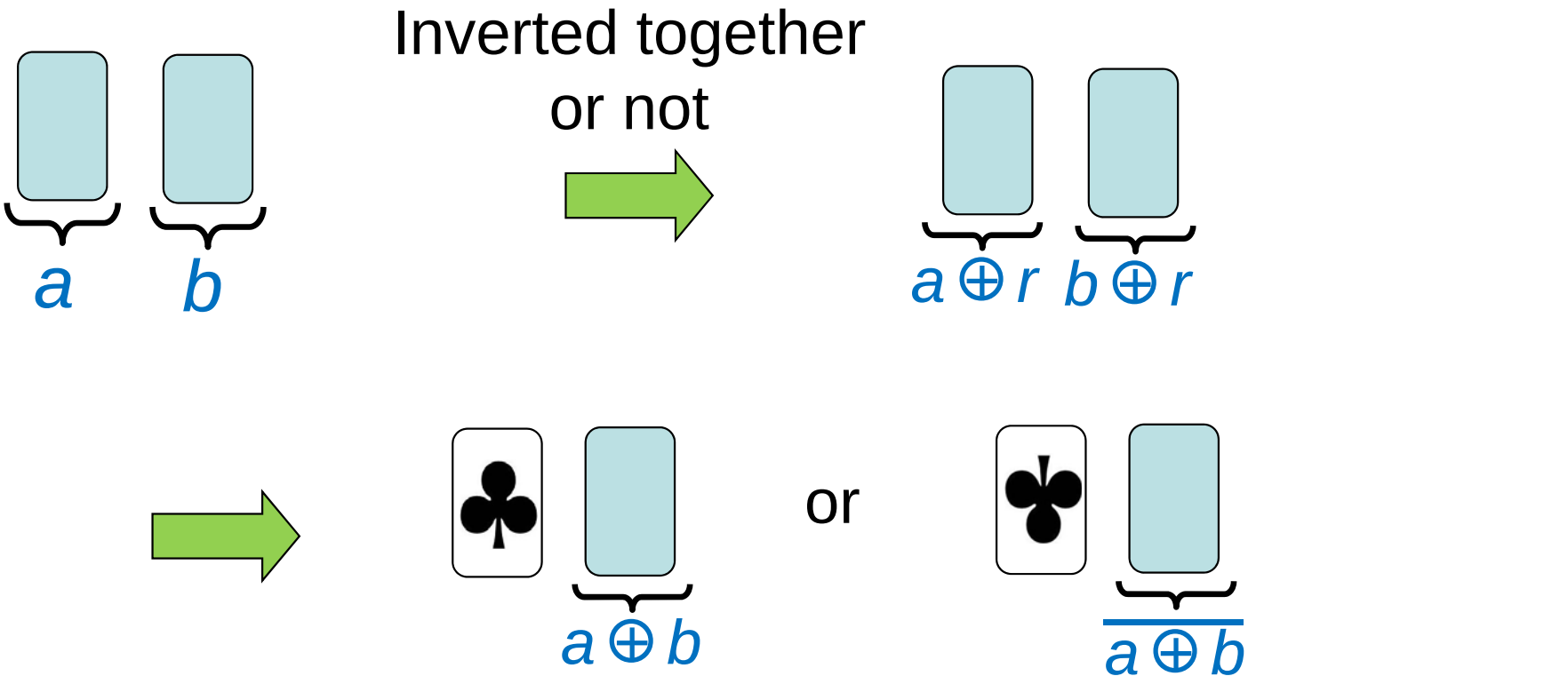


NOT computation

Advantages:

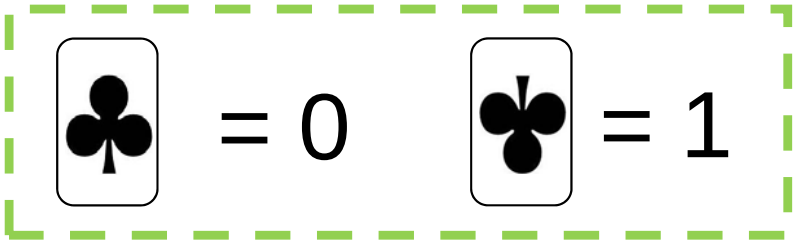


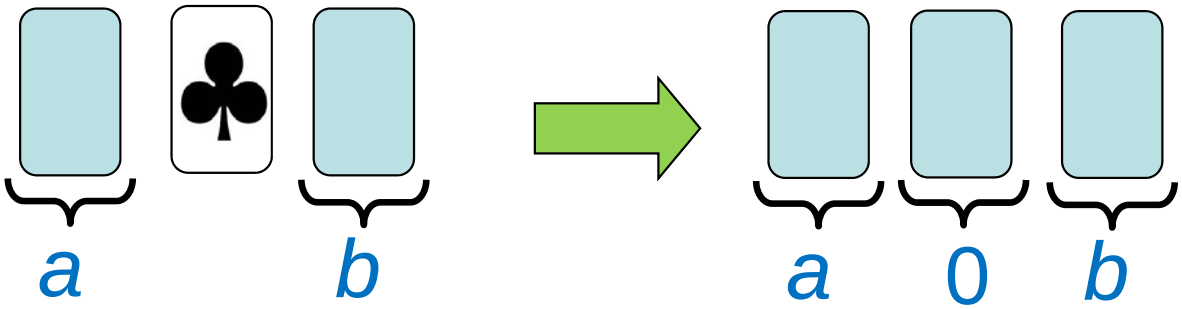
XOR computation



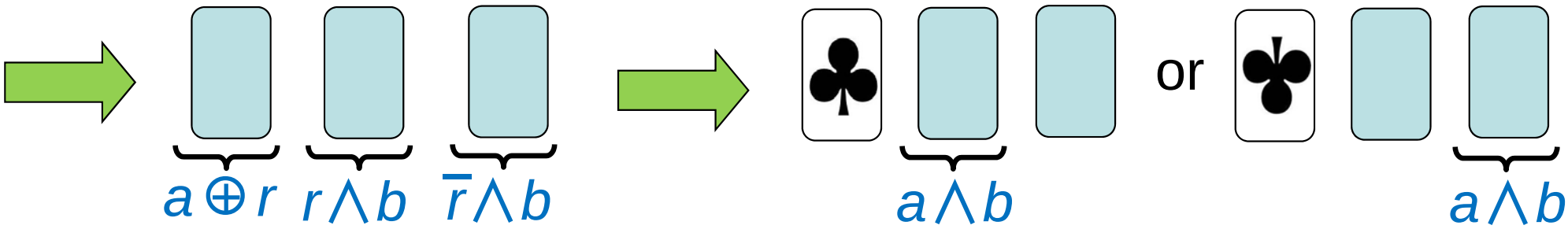
Advantages:

AND computation

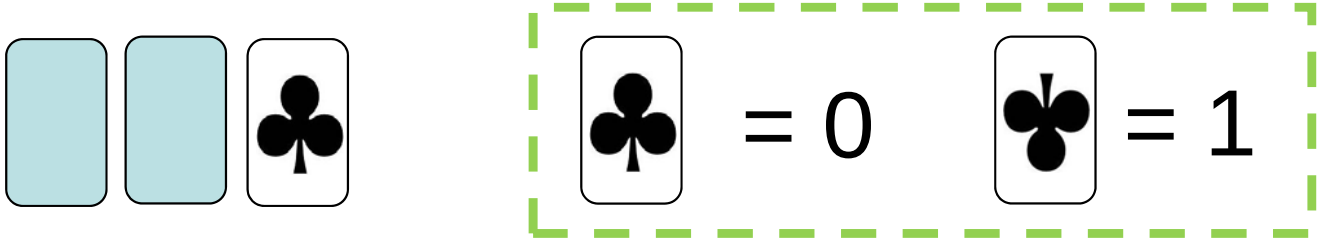




A shuffle where the actions of inverting the first card and swapping the last two cards are synchronized



Advantages；summary



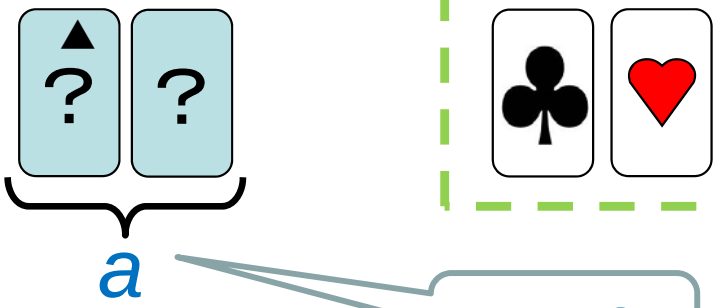
Computations can be done with a single color and half of the number of cards.

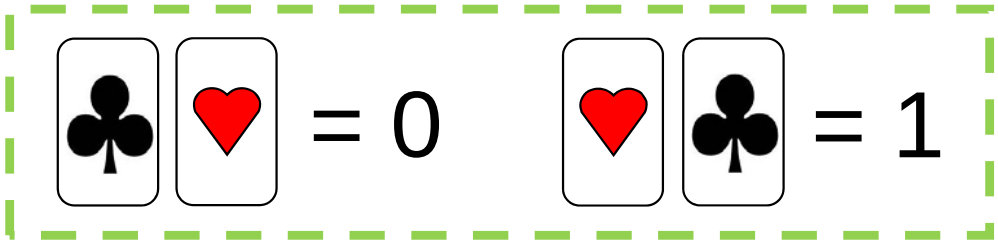
There remains an implementation issue for AND.

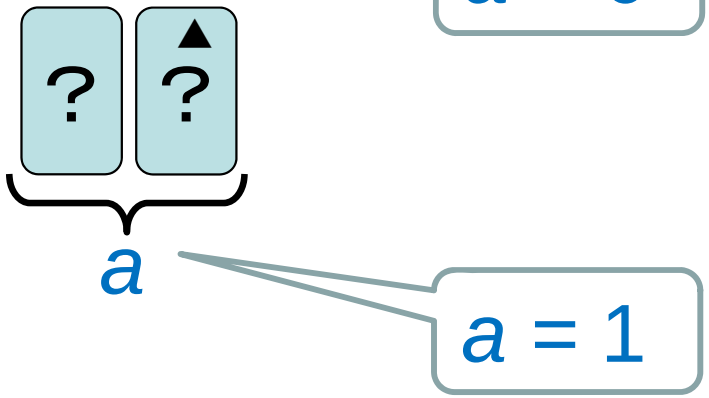
Contents

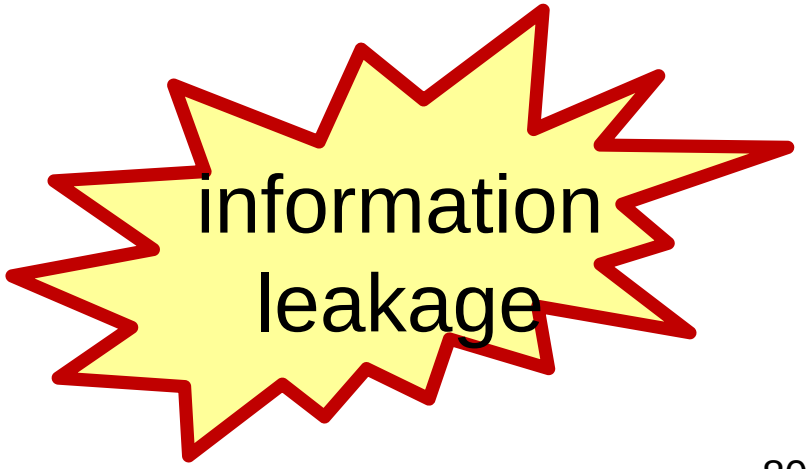
1. Introduction
2. Existing Committed-Format AND/XOR Protocols
3. Attack Exploiting Input Format
4. Backs with a Rotationally Symmetric Pattern
5. Backs with Scuff Marks
6. Conclusion

Backs with Scuff Marks

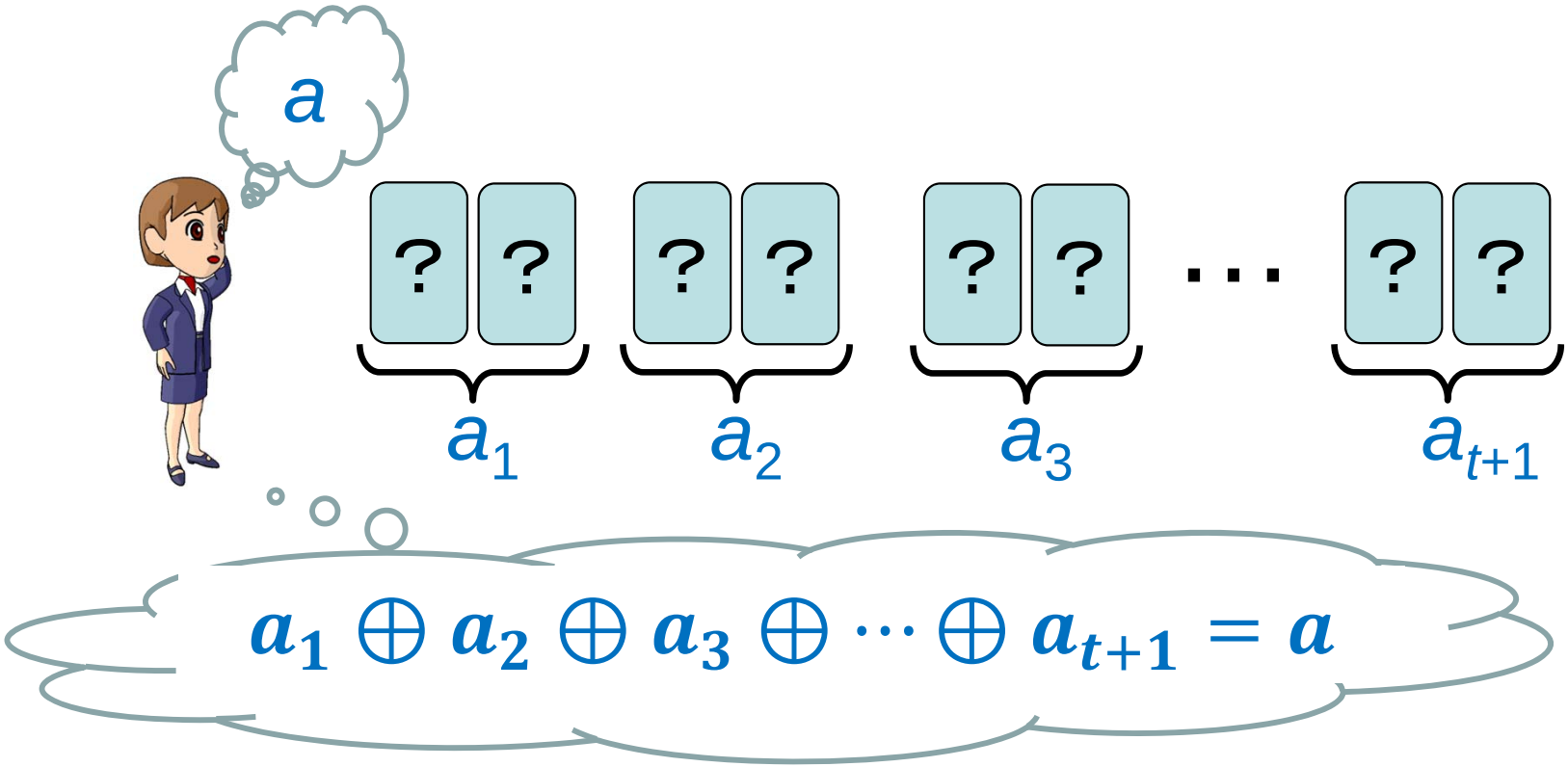




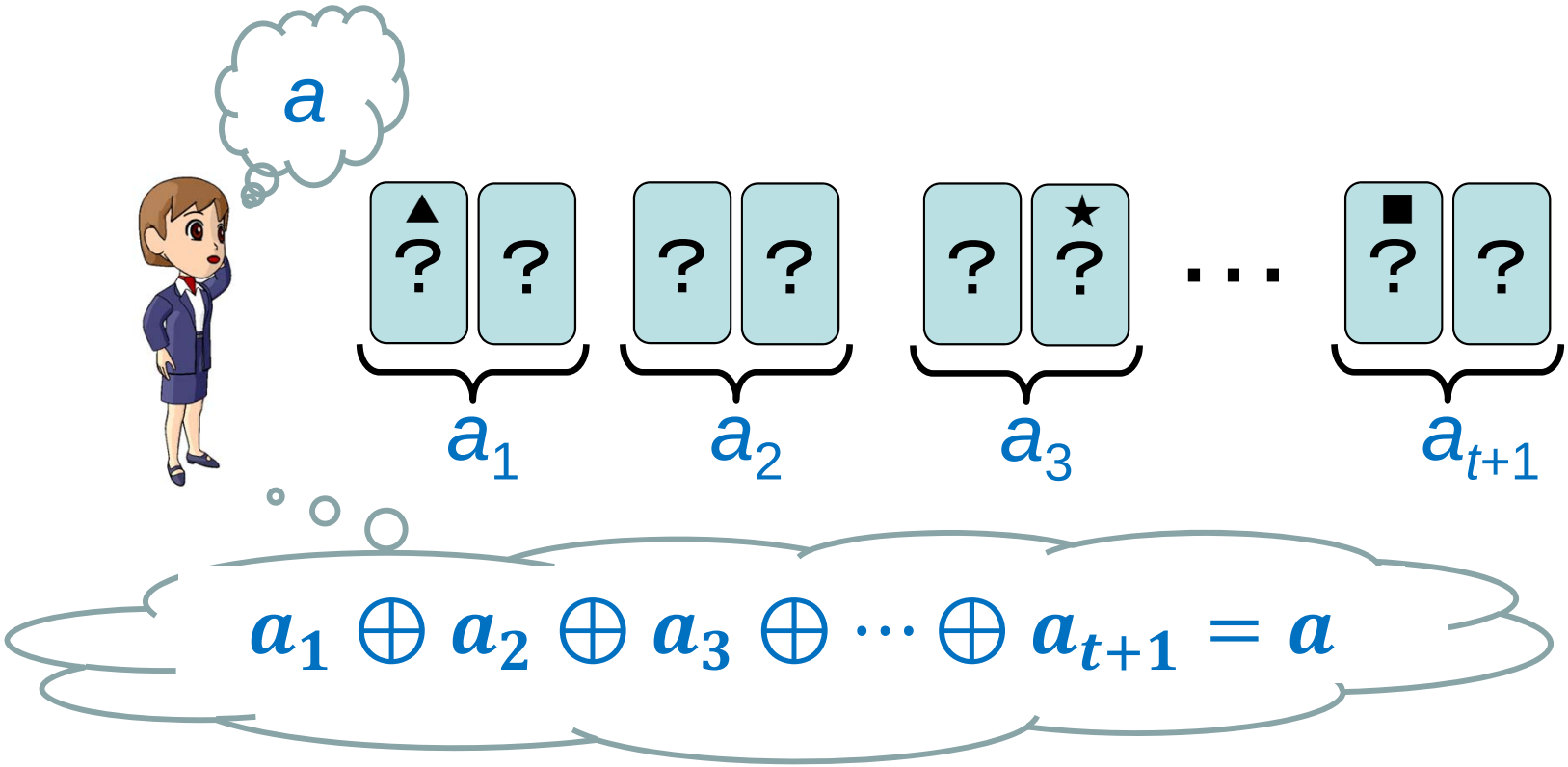




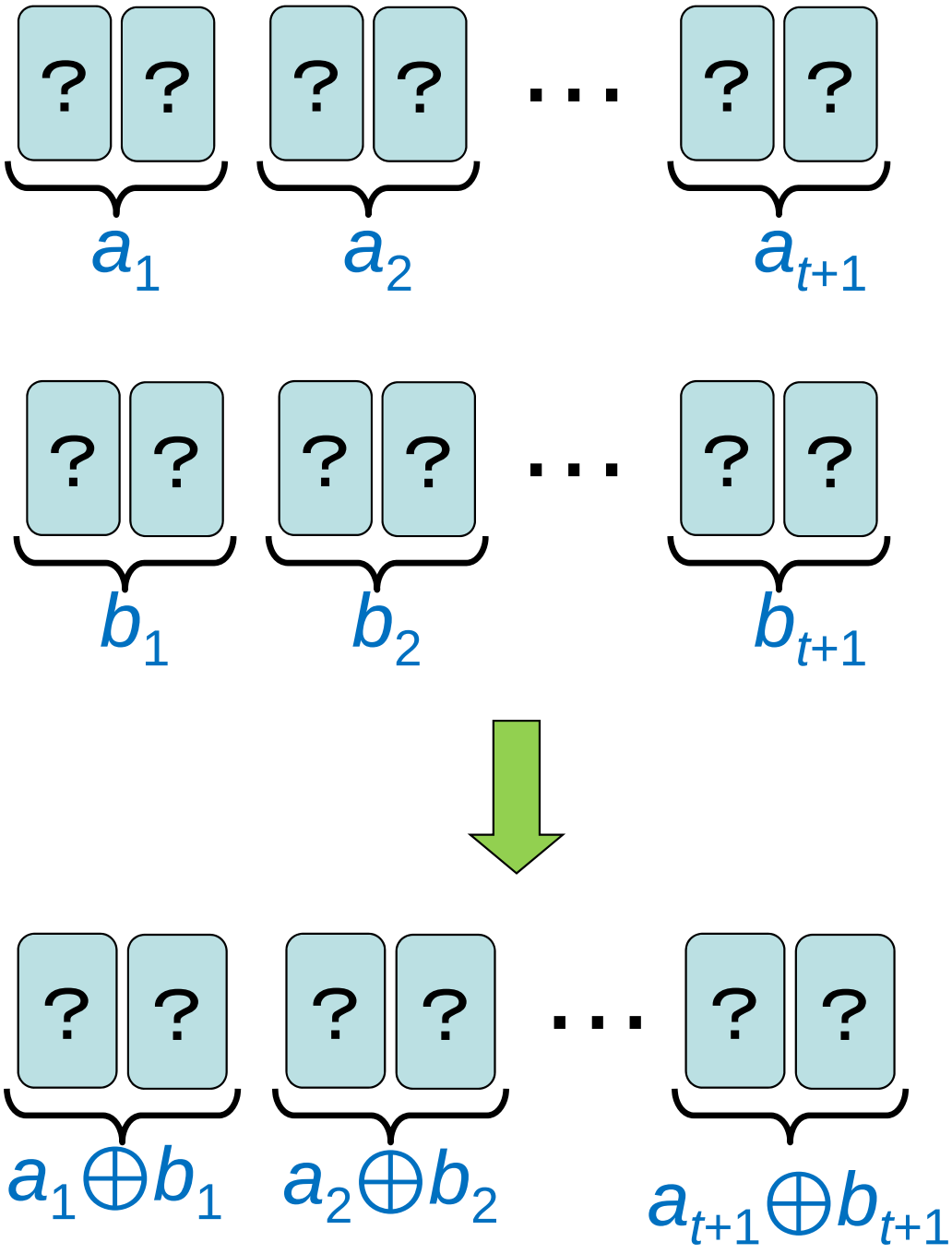
To avoid information leakage, we introduce a new concept, a ***shared commitment***.



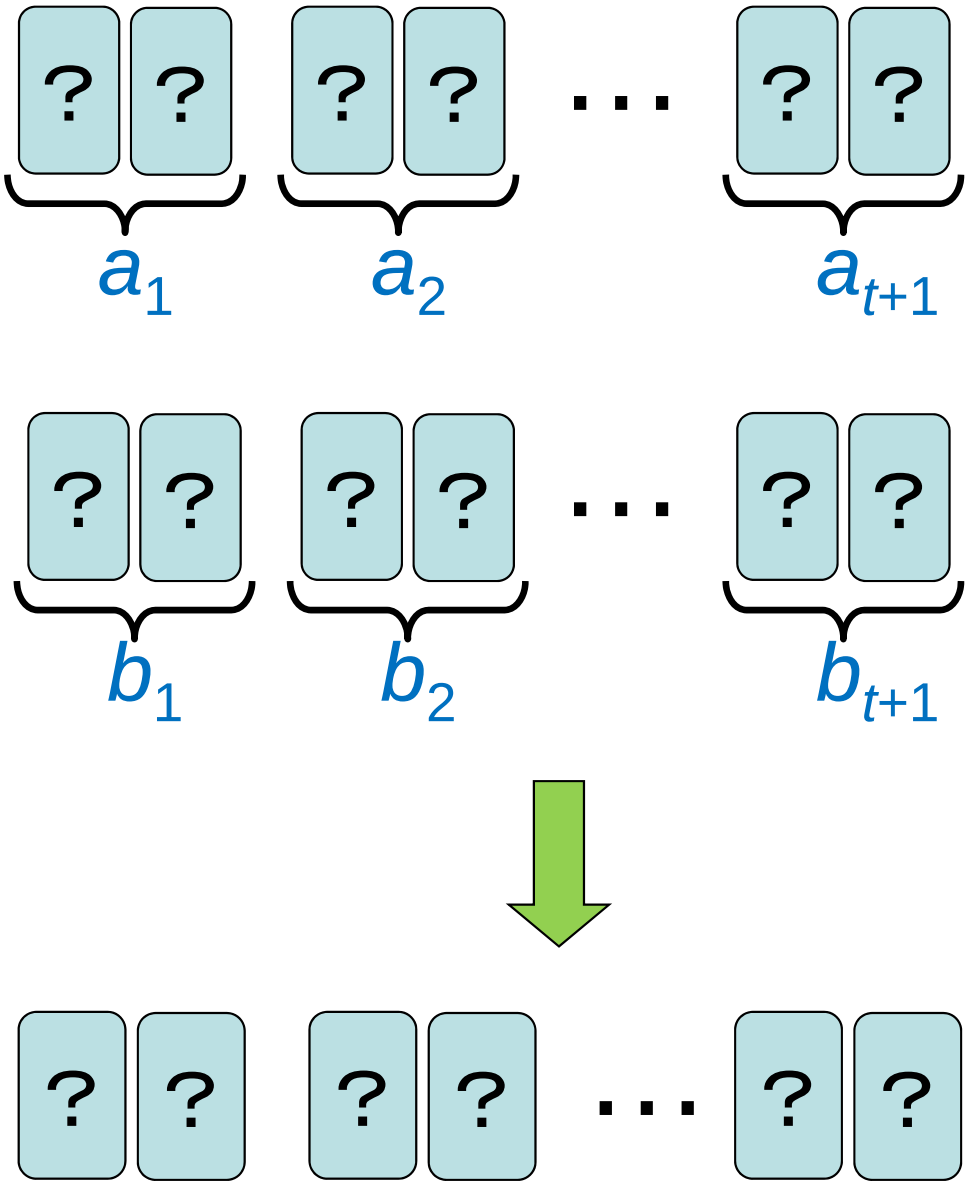
To avoid information leakage, we introduce a new concept, a ***shared commitment***.



Even if at most t cards are flawed, the value of a is kept secret.



Scuff-proof XOR protocol



Scuff-proof AND protocol

shared commitment to $a \wedge b$

The details are omitted

Contents

1. Introduction
2. Existing Committed-Format AND/XOR Protocols
3. Attack Exploiting Input Format
4. Backs with a Rotationally Symmetric Pattern
5. Backs with Scuff Marks
6. Conclusion

Conclusion

- An attack exploiting input format and its countermeasure
- Backs with a Rotationally Symmetric Pattern
- Backs with Scuff Marks

Pros and Cons

Method to keep secrecy

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