

The Minimum Number of Cards in Practical Card-based protocols (Asiacrypt'17より)

宮原大輝
東北大学大学院情報科学研究科

Thursday, December 7 2017



= 0



= 1

	R - track	I - track
	Cryptographic Protocols (Khoa Nguyen)	Foundations (Tatsuaki Okamoto)
9:00-9:25	Two-Round PAKE from Approximate SPH and Instantiations from Lattices; <i>Jiang Zhang, Yu Yu</i>	Succinct Spooky Free Compilers Are Not Black Box Sound; <i>Zvika Brakerski, Yael Tauman Kalai, Renen Perlman</i>
9:25-9:50	Tightly-Secure Signatures from Five-Move Identification Protocols; <i>Eike Kiltz, Julian Loss, Jiaxin Pan</i>	Non-Interactive Multiparty Computation without Correlated Randomness; <i>Shai Halevi, Yuval Ishai, Abhishek Jain, Ilam Komargodski, Amit Sahai, Eylon Yogev</i>
9:50-10:15	On the Untapped Potential of Encoding Predicates by Arithmetic Circuits and Their Applications; <i>Shuichi Katsumata</i>	Optimal-Rate Non-committing Encryption; <i>Ran Canetti, Oxana Poburinnaya, Mariana Raykova</i>
10:15-10:40	The Minimum Number of Cards in Practical Card-based Protocols; <i>Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone</i>	Preventing CLT Attacks on Obfuscation with Linear Overhead; <i>Rex Fernando, Peter M. R. Rasmussen, Amit Sahai</i>
10:40-11:10	Coffee Break	

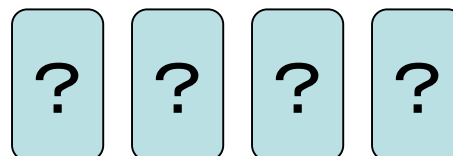
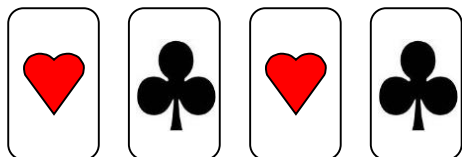
あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

赤や黒のカードを何枚か用いると

秘密計算

を実現できる。

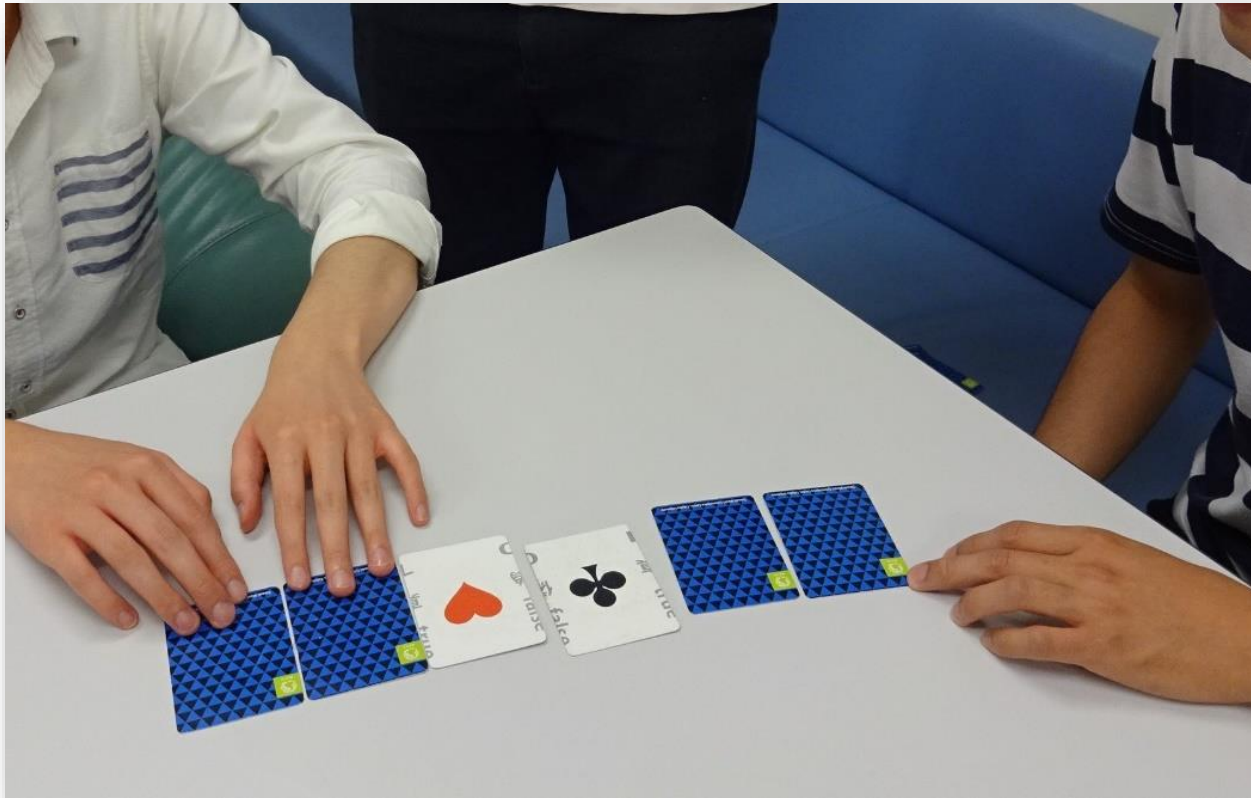


カードベース暗号





あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

誰でも簡単に秘密計算を実行できる



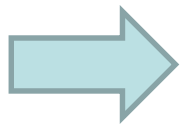
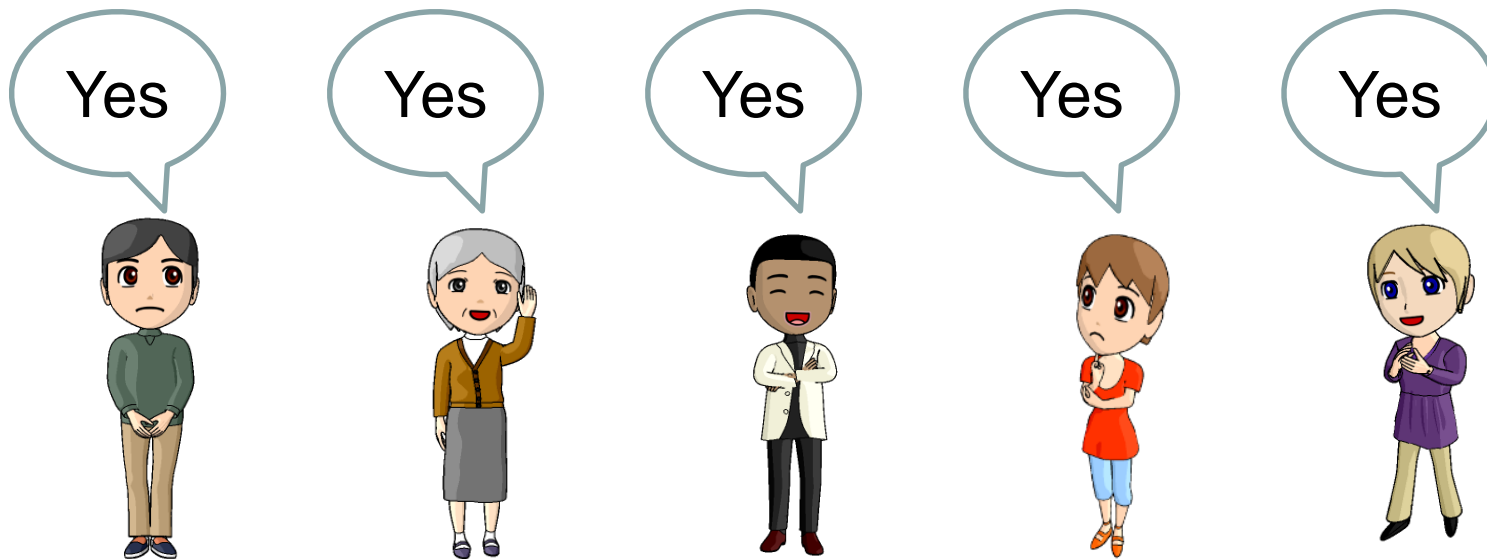
シャッフルする、めくる、並び替える

  = 0   = 1

カラオケ(懇親会)に行きたい？ 行きたくない？

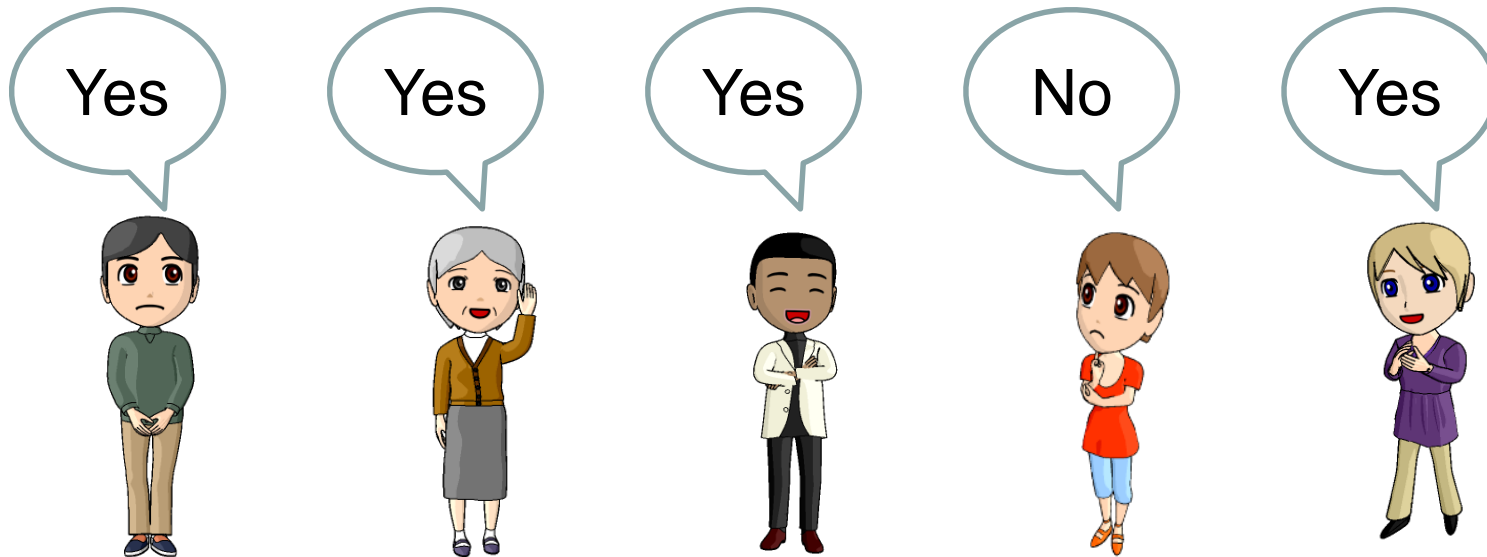


カラオケに行きたい？行きたくない？



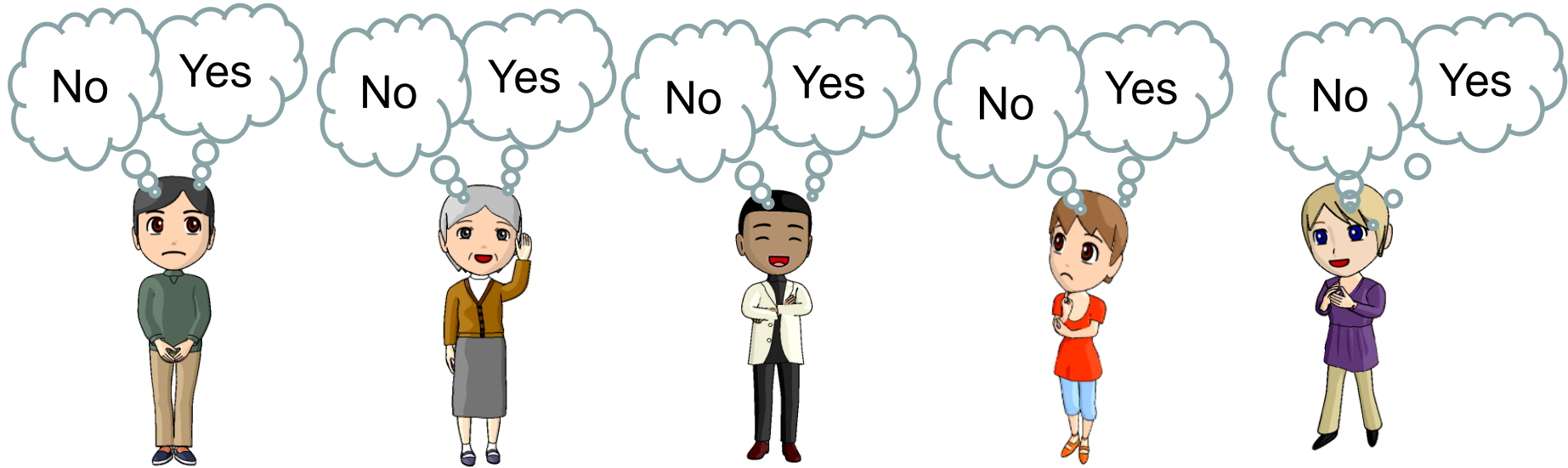
全員Yesだったら，行きましょう！

カラオケに行きたい？ 行きたくない？



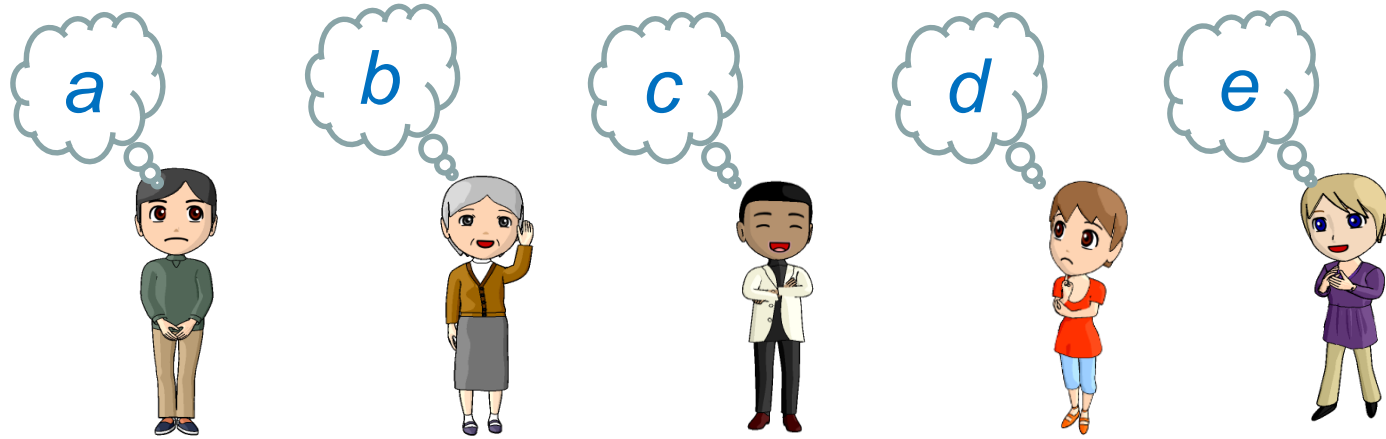
➡ 一人でもNoだったら、今回はやめておこう
(でもなんだか気まずいですね...)

カラオケに行きたい？ 行きたくない？



個々のYES/NOは秘密にしたまま、
全員YESか否かだけを知りたい。

各人は1ビット(0か1)を秘密に持っている



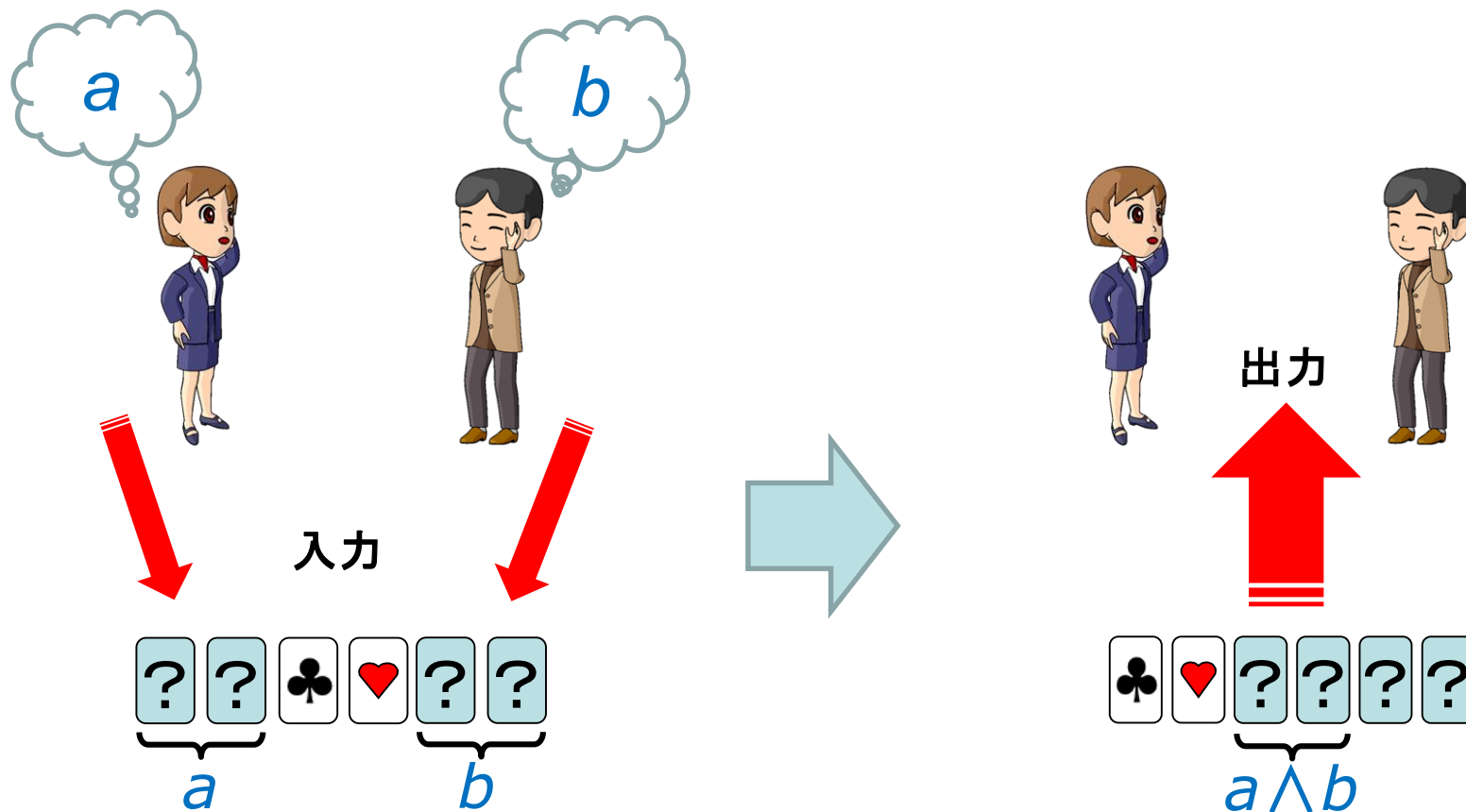
論理積の秘密計算がしたい



あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- 例) 6枚のカードを用いるANDプロトコル^[MS09]

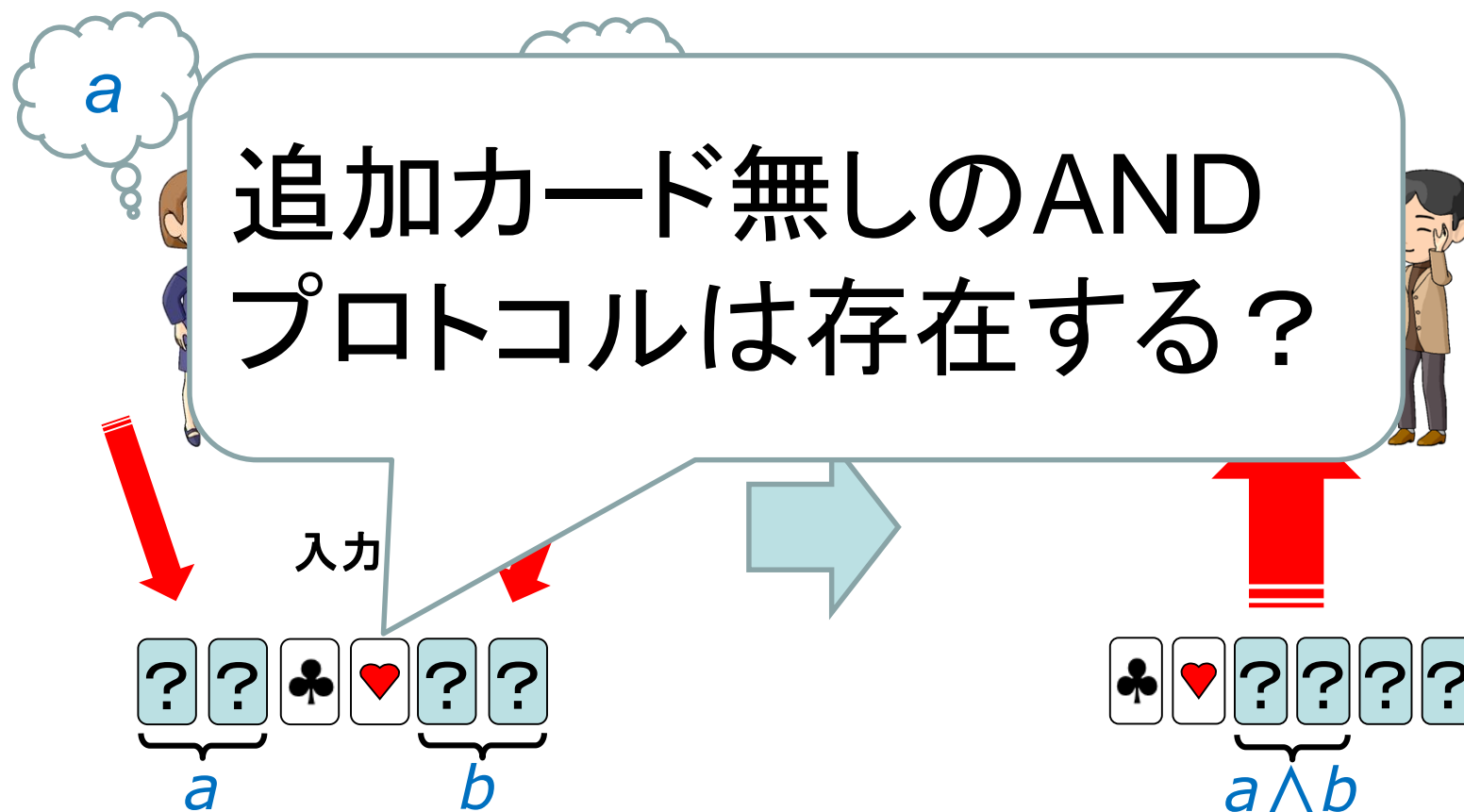


[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- 例) 6枚のカードを用いるANDプロトコル^[MS09]

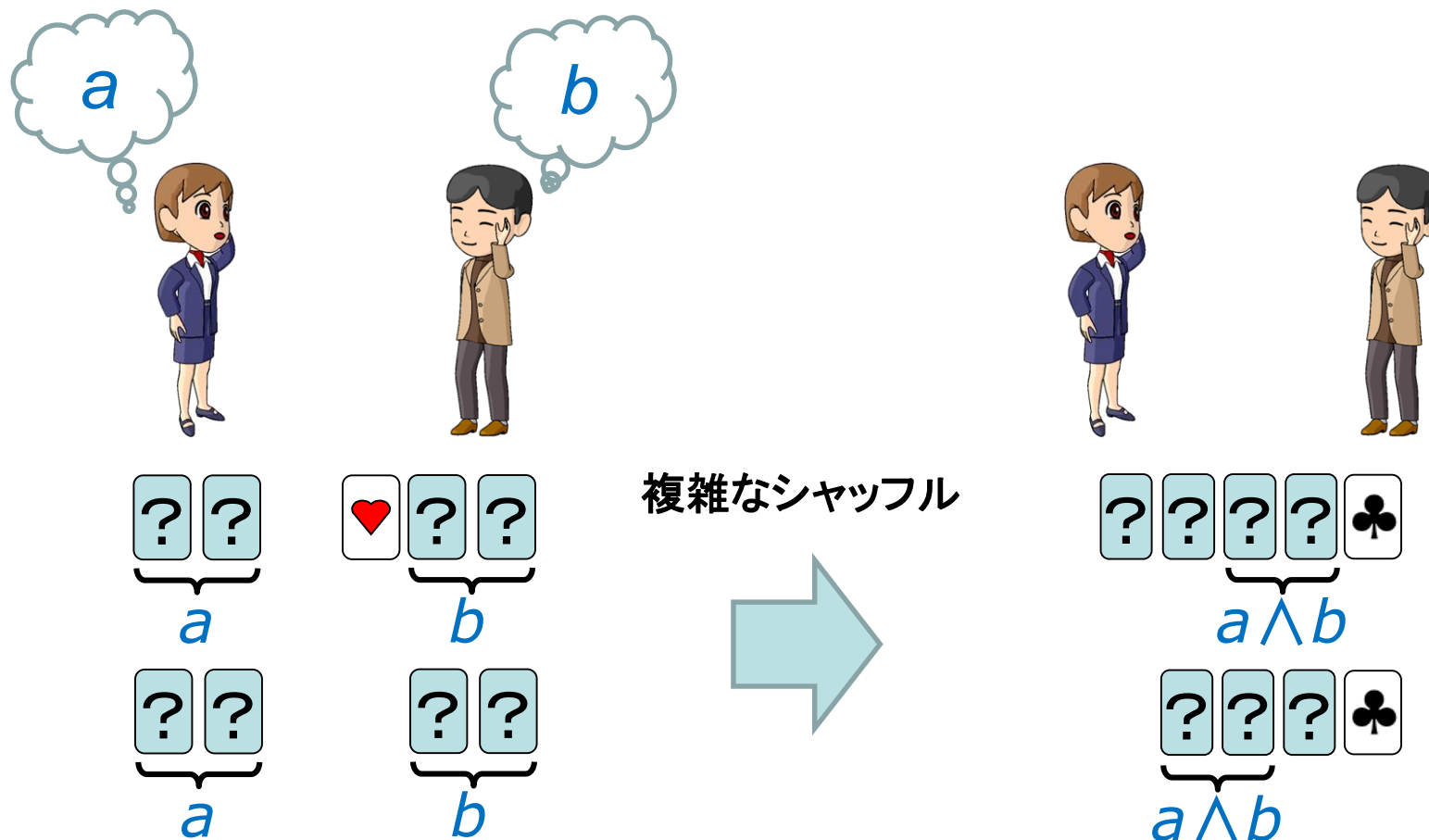


[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- 4, 5枚のカードを用いるAND プロトコル^[KWH15]

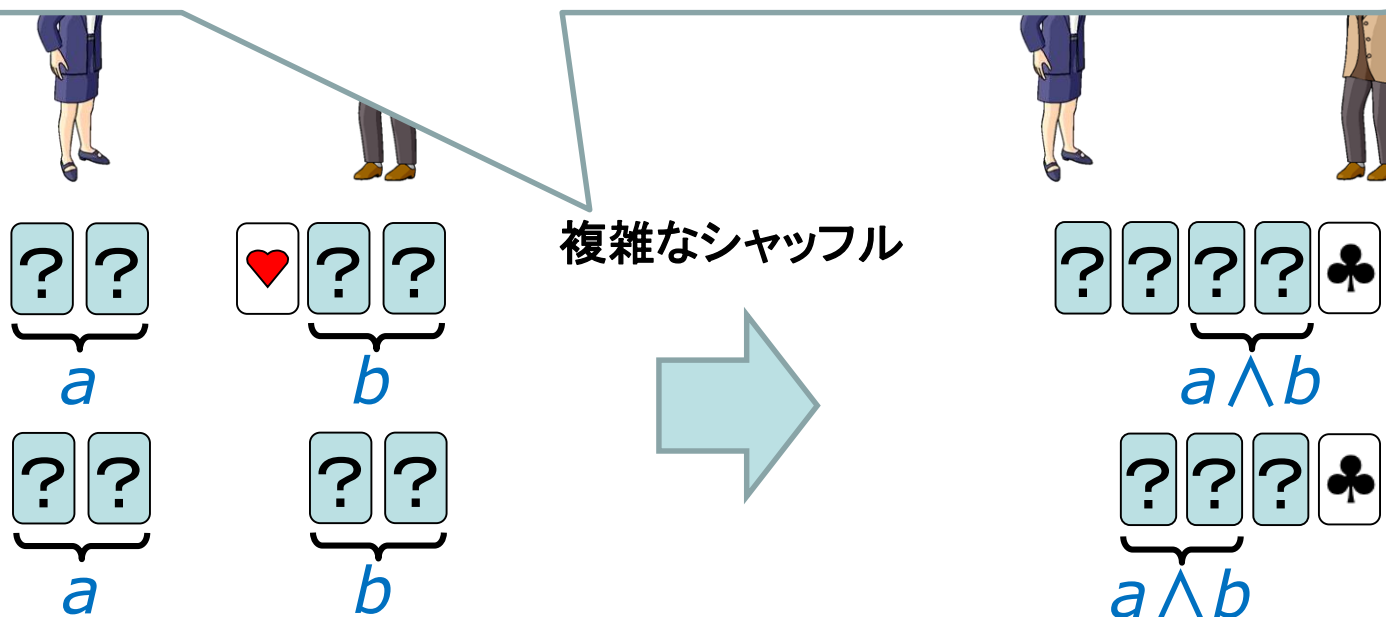


[KWH15] Koch, A., Walzer, S., Härtel, K., "Card-based cryptographic protocols using a minimal number of cards." ASIACRYPT 2015, LNCS, pp. 783–807.

あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- 簡単なシャッフルのみのAND
プロトコルは存在する？

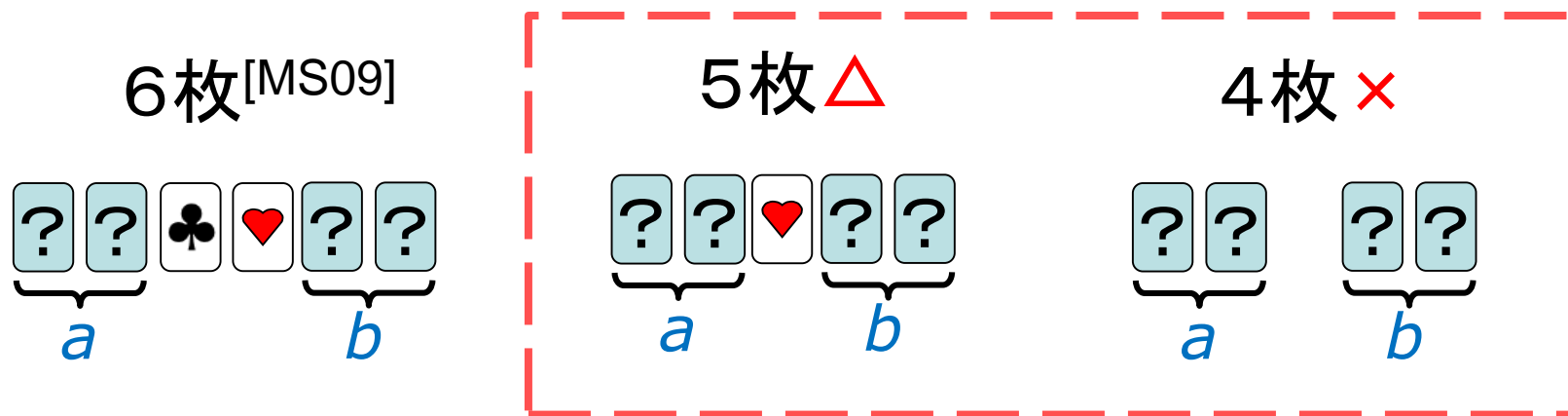


[KWH15] Koch, A., Walzer, S., Härtel, K., “Card-based cryptographic protocols using a minimal number of cards.” ASIACRYPT 2015, LNCS, pp. 783–807.

あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- “実用的な”AND プロトコルを解明
(カード枚数・実行時間・シャッフルの難しさ...)



\triangle : プロトコルは存在する(だろう)が、Las Vegas である

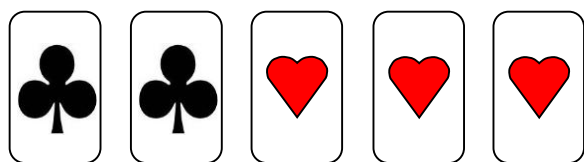
\times : プロトコルは存在しない

目次

$$\begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} = 1$$

1. はじめに
2. ANDプロトコル
3. COPYプロトコル
4. 最新動向
5. むすび

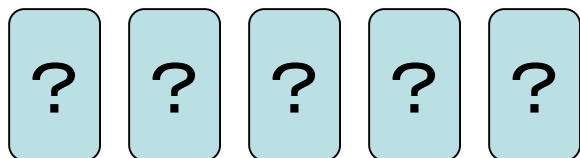
$$\begin{array}{|c|} \hline \spadesuit \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \spadesuit \\ \hline \end{array} = 1$$



表



ひっくり返す



裏

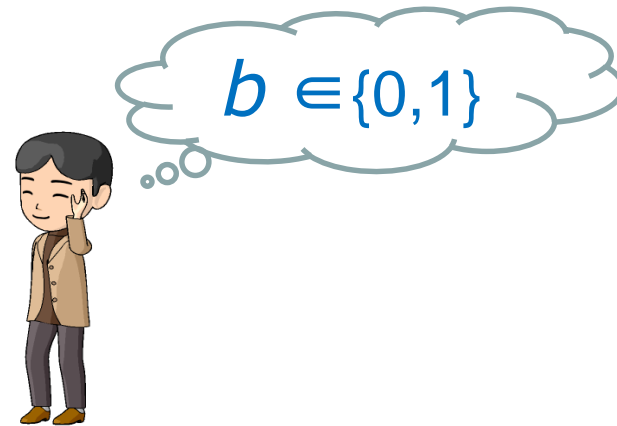
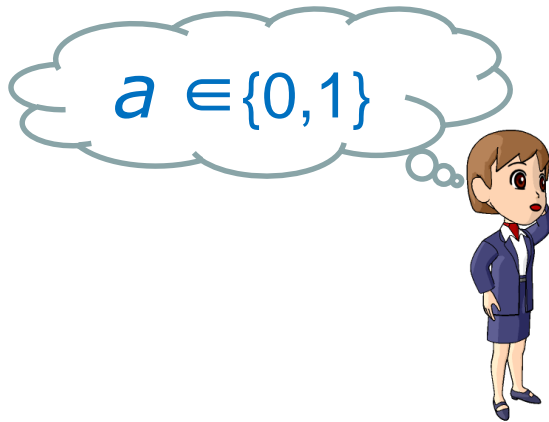


$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

ビットを扱うために、次の符号化を固定する:

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

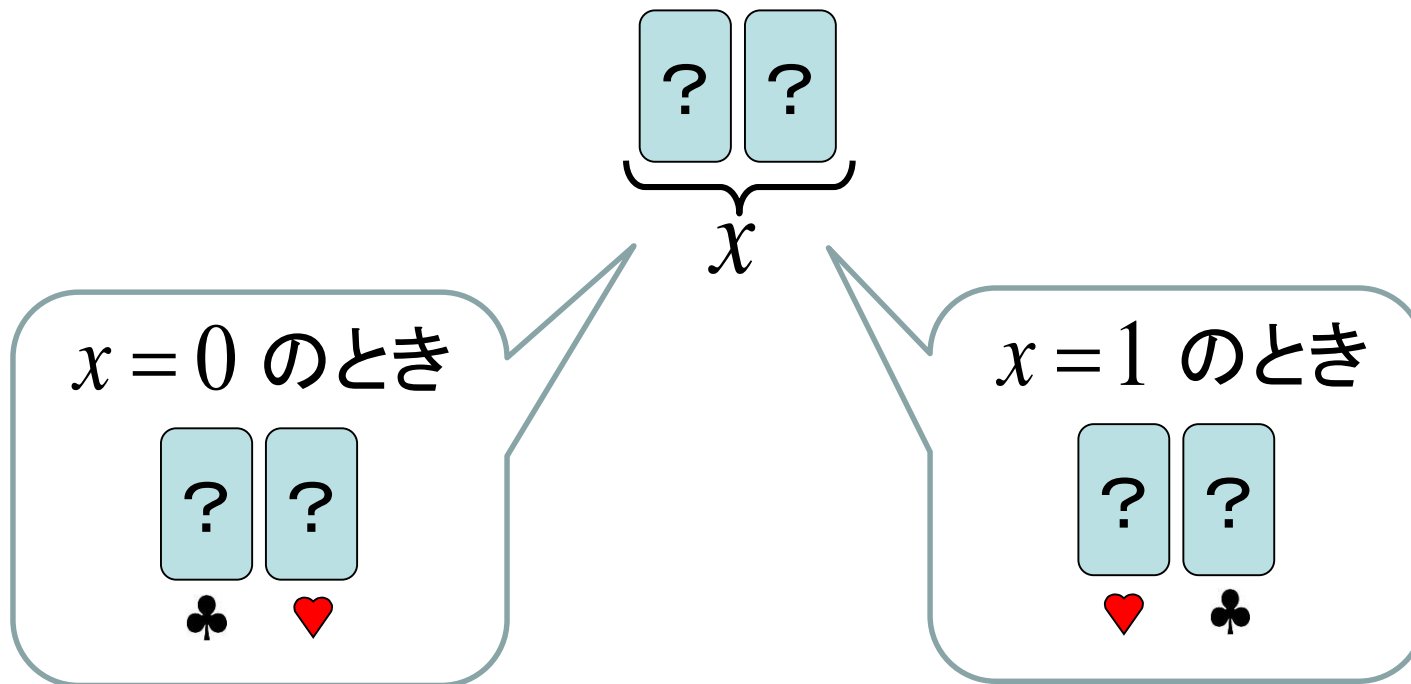
$$\begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$



$$\begin{array}{|c|} \hline \clubsuit \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \clubsuit \\ \hline \end{array} = 1$$

$$\begin{array}{|c|} \hline \clubsuit \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \clubsuit \\ \hline \end{array} = 1$$

符号化に従う裏に置かれたカードを**コミットメント**と呼ぶ:



目次

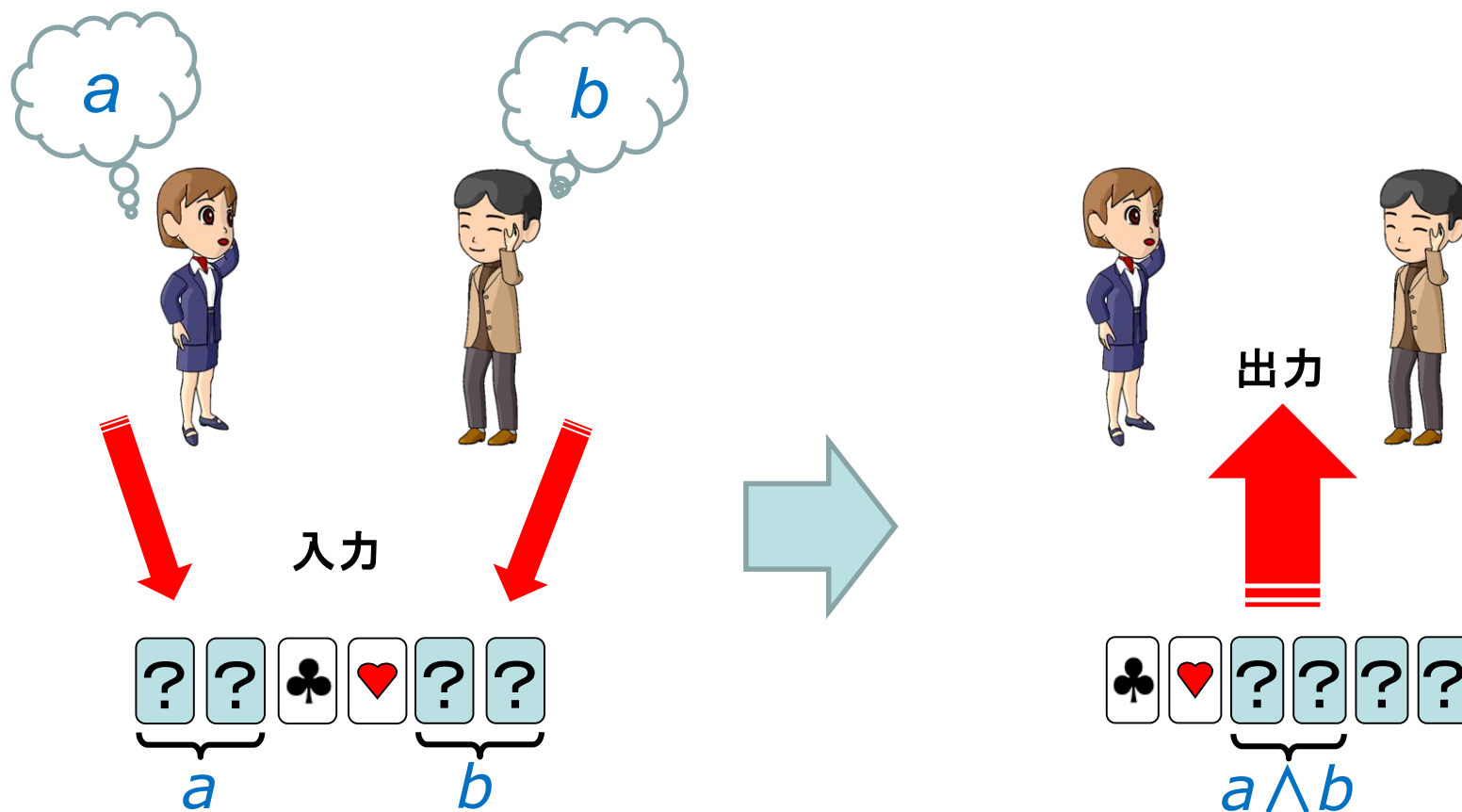
$$\begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} = 1$$

1. はじめに
2. ANDプロトコル
3. COPYプロトコル
4. 最新動向
5. むすび

[再掲] あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- 例) 6-card コミット型ANDプロトコル^[MS09]



[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

ANDの歴史

$$\begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} = 1$$

[CK93]

[NR98]

[Sti01]

第7回公開鍵暗号の安全な構成とその応用ワークショップ

産総研 > RISEC > イベント情報 > 第7回公開鍵暗号の安全な構成とその応用ワークショップ

日時: 2014年3月20日(木) 9:50-18:10

17:20-

カード組を用いた秘匿計算プロトコルについて

[MS09]

18:10

水木 敬明 (東北大学)

[KWH15]

[SMSN+15](偏光板カード)

[SMSN+15](正多角形カード)

[Mizuki16](トランプカード)

[KKWM+17]

2章の構成

  = 0   = 1

シャッフルのクラス

2.3. 複雑なシャッフル
[KWH15]

2.1. ランダムカット

2.2. ランダム二等分割カット

[CK93]
[NR98]
[Sti01]

[MS09]

[KKWM⁺17]

2章の構成

  = 0   = 1

シャッフルのクラス

複雑なシャッフル

[KWH15]

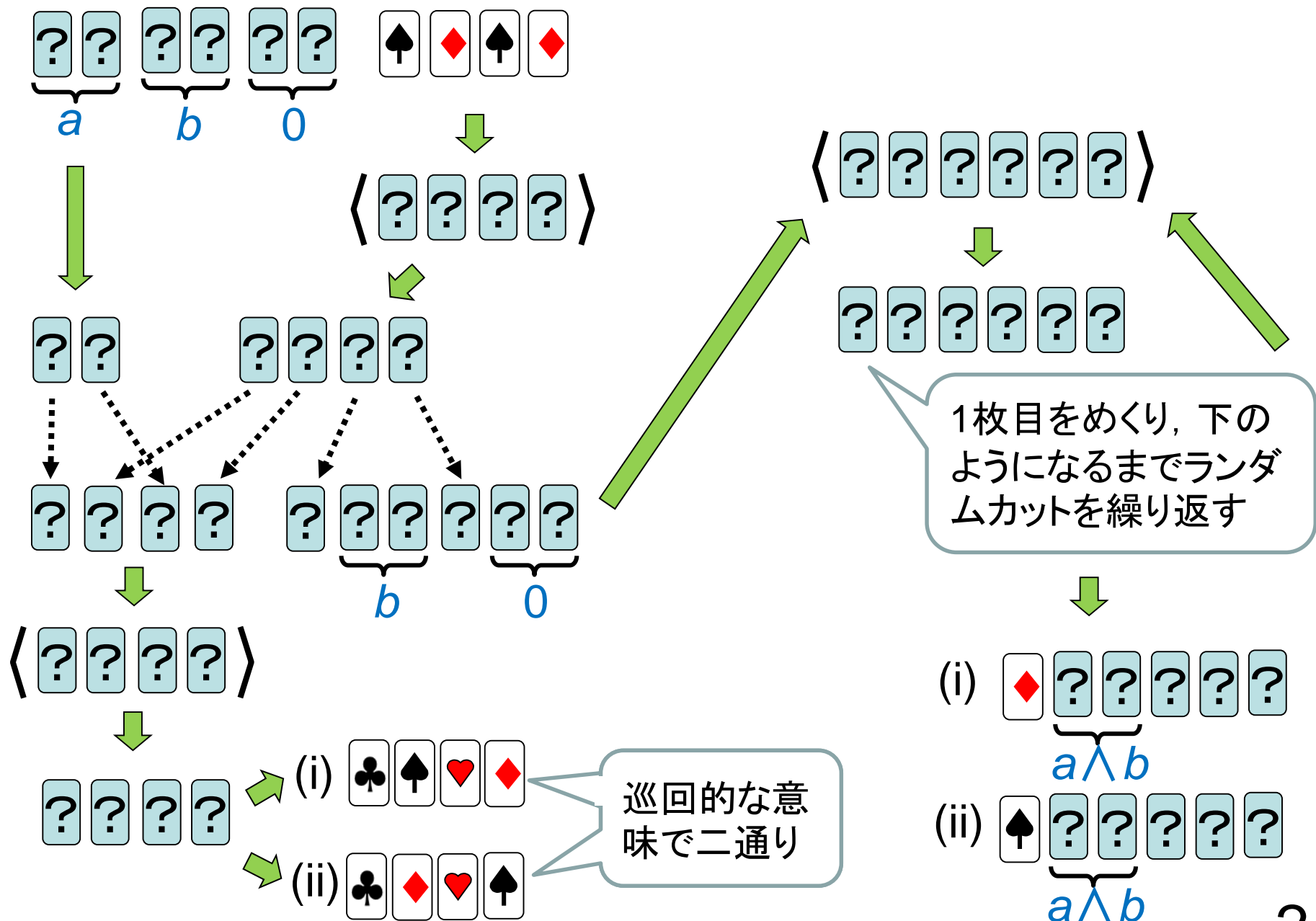
2.4. 簡単なシャッフル [KKWM⁺17]

[CK93]
[NR98]
[Sti01]

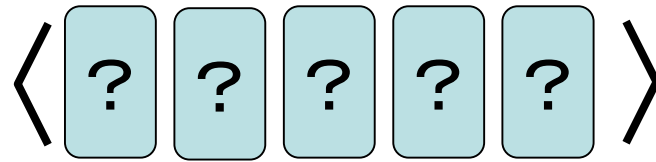
[MS09]

Crepeau-Kilian [CRYPTO '93]

$$\begin{matrix} \spadesuit & \heartsuit \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \end{matrix} = 1$$



ランダムカット







$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$













巡回的にシフトさせることをランダムに繰り返す

まとめると:

  = 0   = 1

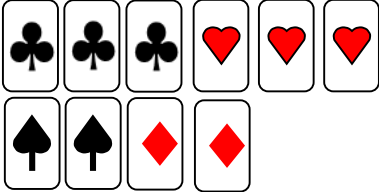
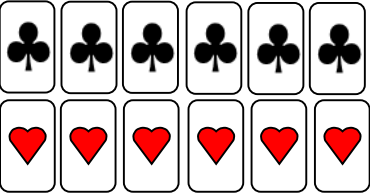
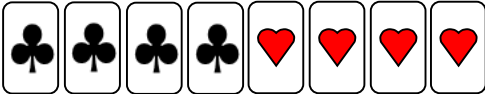
コミット型AND計算

	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10          	6





その後の改良:

$$\begin{matrix} \spadesuit & \heartsuit \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \end{matrix} = 1$$

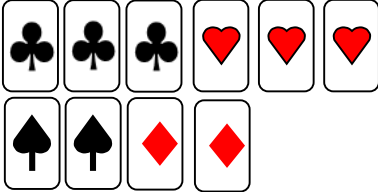
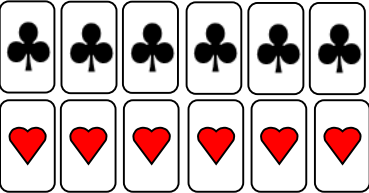

コミット型AND計算

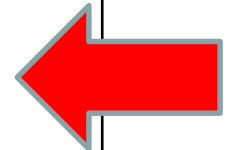
	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 	6
Niemi-Renvall [TCS, 1998]	12 	2.5
Stiglic [TCS, 2001]	8 	2

その後の改良:

  = 0   = 1

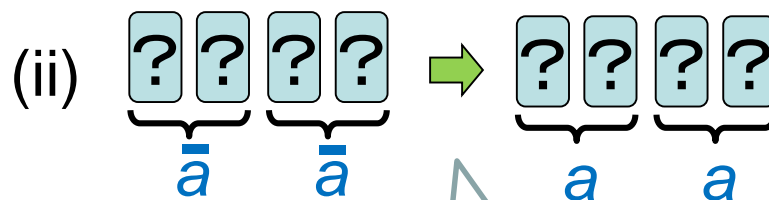
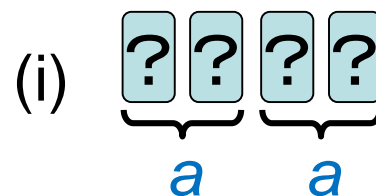
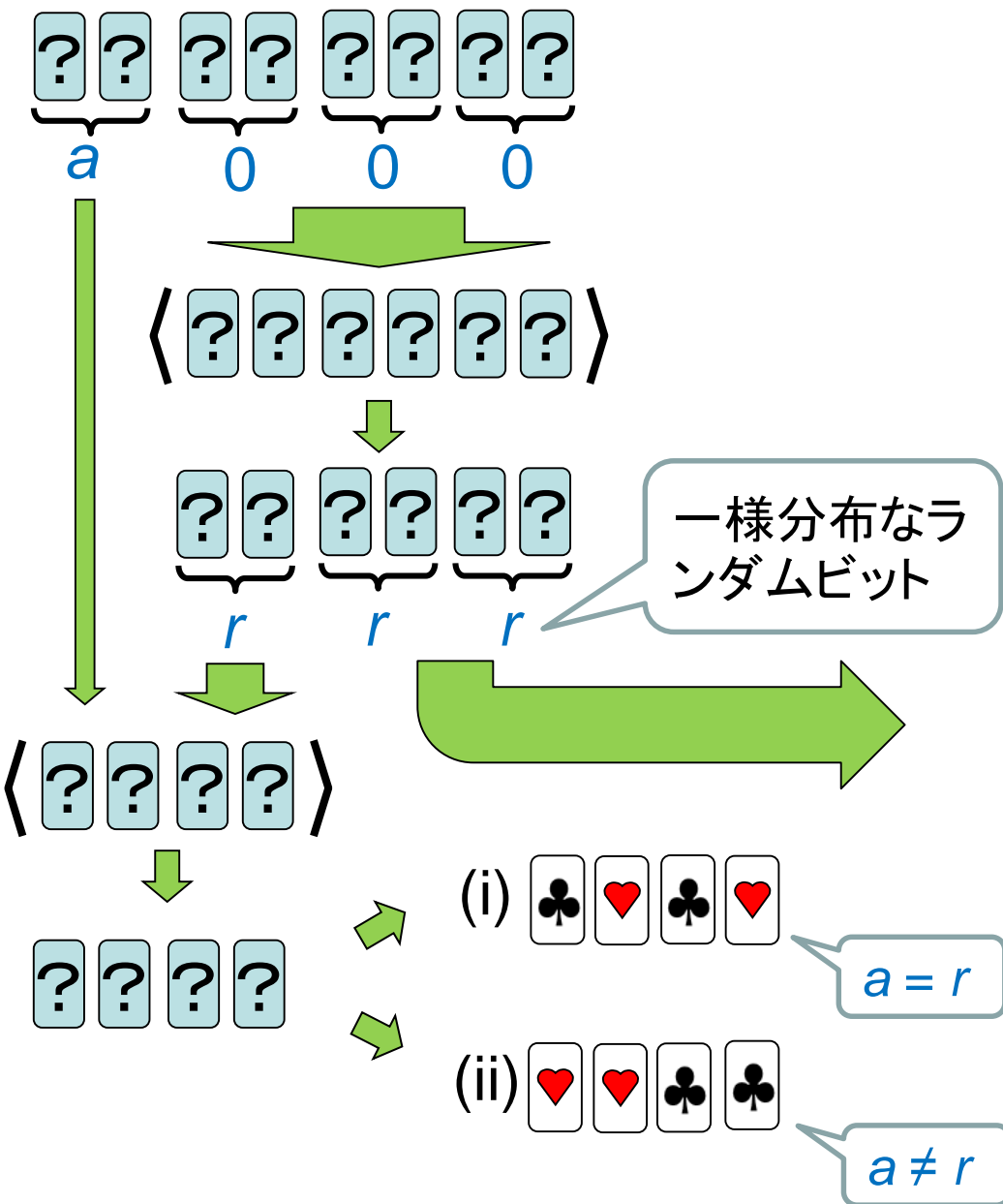
コミット型AND計算

	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 	6
Niemi-Renvall [TCS, 1998]	12 	2.5
Stiglic [TCS, 2001]	8 	2



まず、コピープロトコルを紹介[CK93]

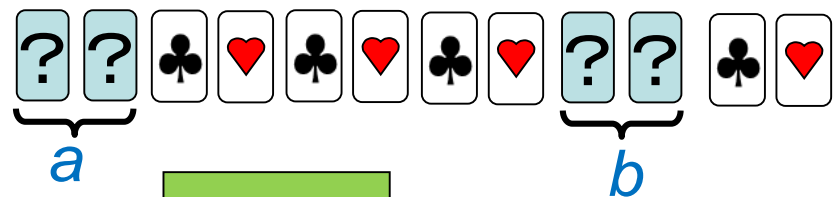
$$\begin{matrix} \spadesuit & \heartsuit \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \end{matrix} = 1$$



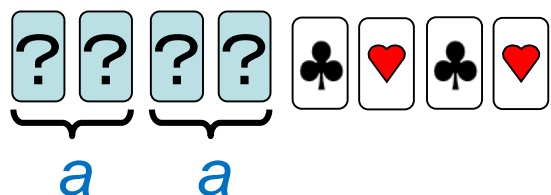
左右を入れ替えることで NOT 計算

Niemi-Renvall [TCS, 1998]

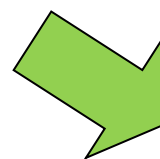
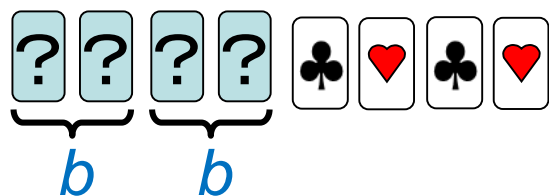
$$\begin{matrix} \spadesuit & \heartsuit \\ \hline \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \\ \hline \end{matrix} = 1$$



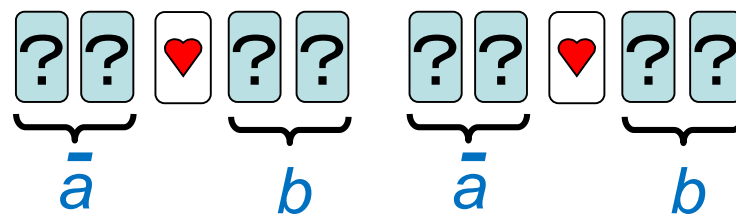
コピー

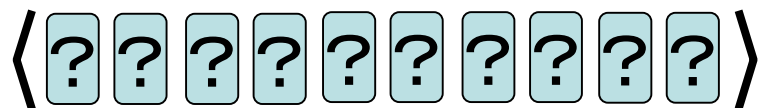
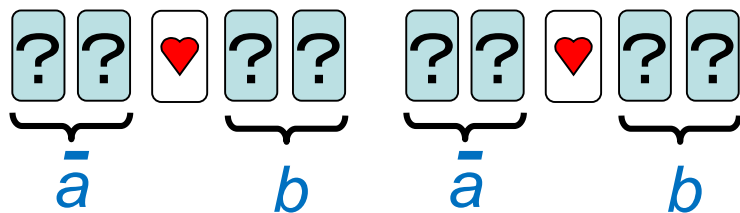


コピー



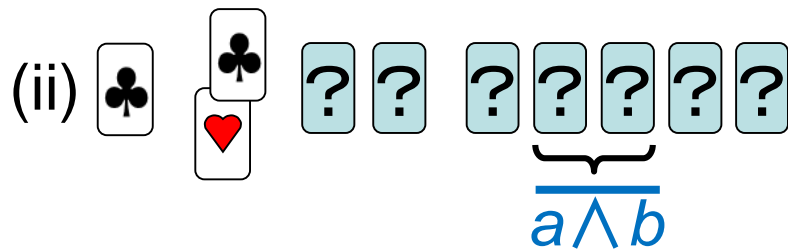
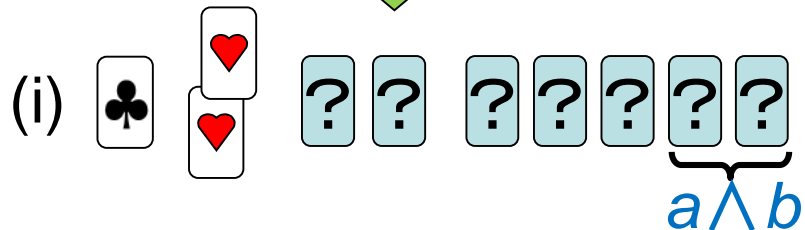
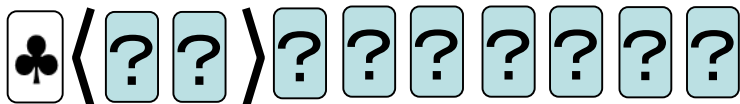
次のように並べる





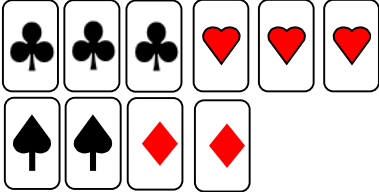
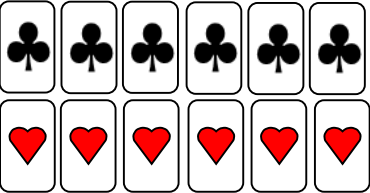
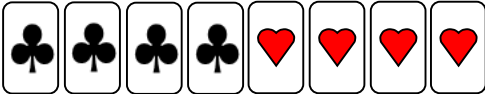
先頭をめくり、黒が出るまで繰り返す

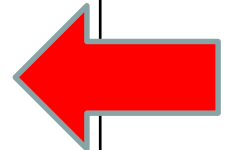
10回に4回の割合で出る



$$\begin{matrix} \spadesuit & \heartsuit \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \end{matrix} = 1$$

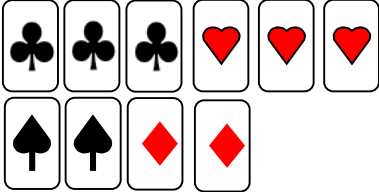
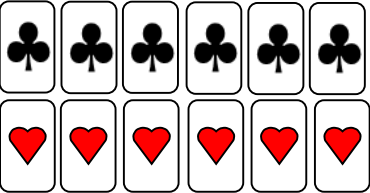
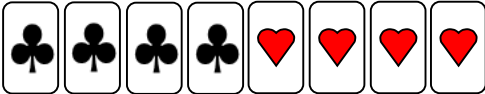
コミット型AND計算

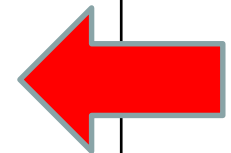
	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 	6
Niemi-Renvall [TCS, 1998]	12 	2.5
Stiglic [TCS, 2001]	8 	2

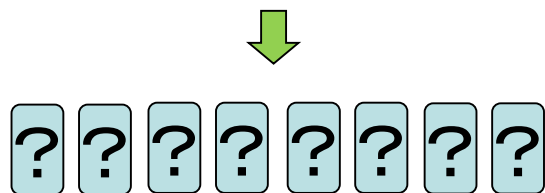
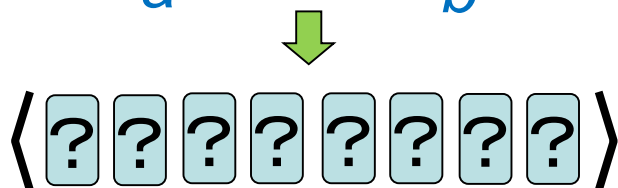
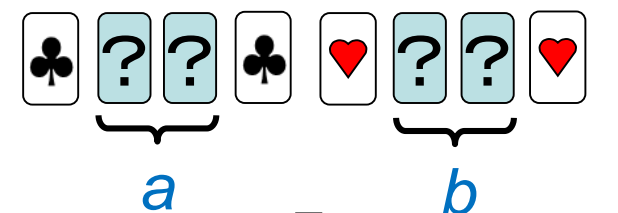


$$\begin{matrix} \spadesuit & \heartsuit \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \end{matrix} = 1$$



コミット型AND計算

	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 	6
Niemi-Renvall [TCS, 1998]	12 	2.5
Stiglic [TCS, 2001]	8 	2

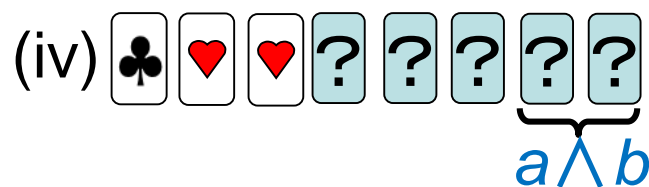
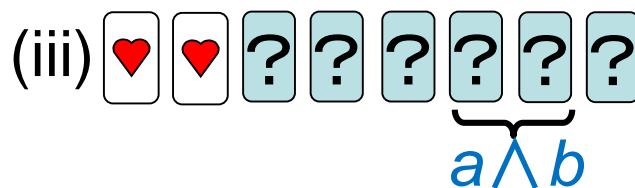
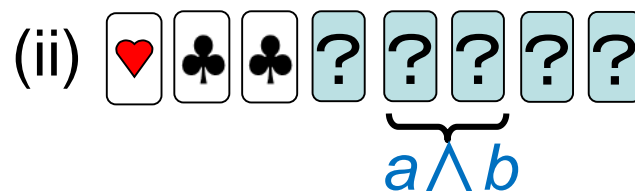
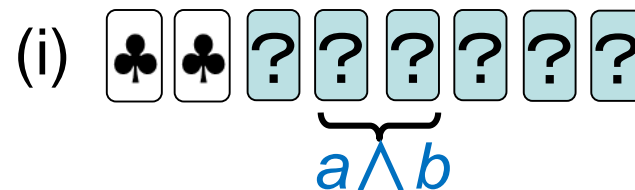








最初の2枚
をめくる


 または 
 の場合,































3枚目をめくる。
次のようになるまで繰り返す。



2001年までのAND計算プロトコル:

  = 0   = 1

コミット型AND計算

	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10          	6
Niemi-Renvall [TCS, 1998]	12            	2.5
Stiglic [TCS, 2001]	8        	2

2章の構成

  = 0   = 1

シャッフルのクラス

2.3. 複雑なシャッフル
[KWH15]

2.1. ランダムカット

2.2. ランダム二等分割カット

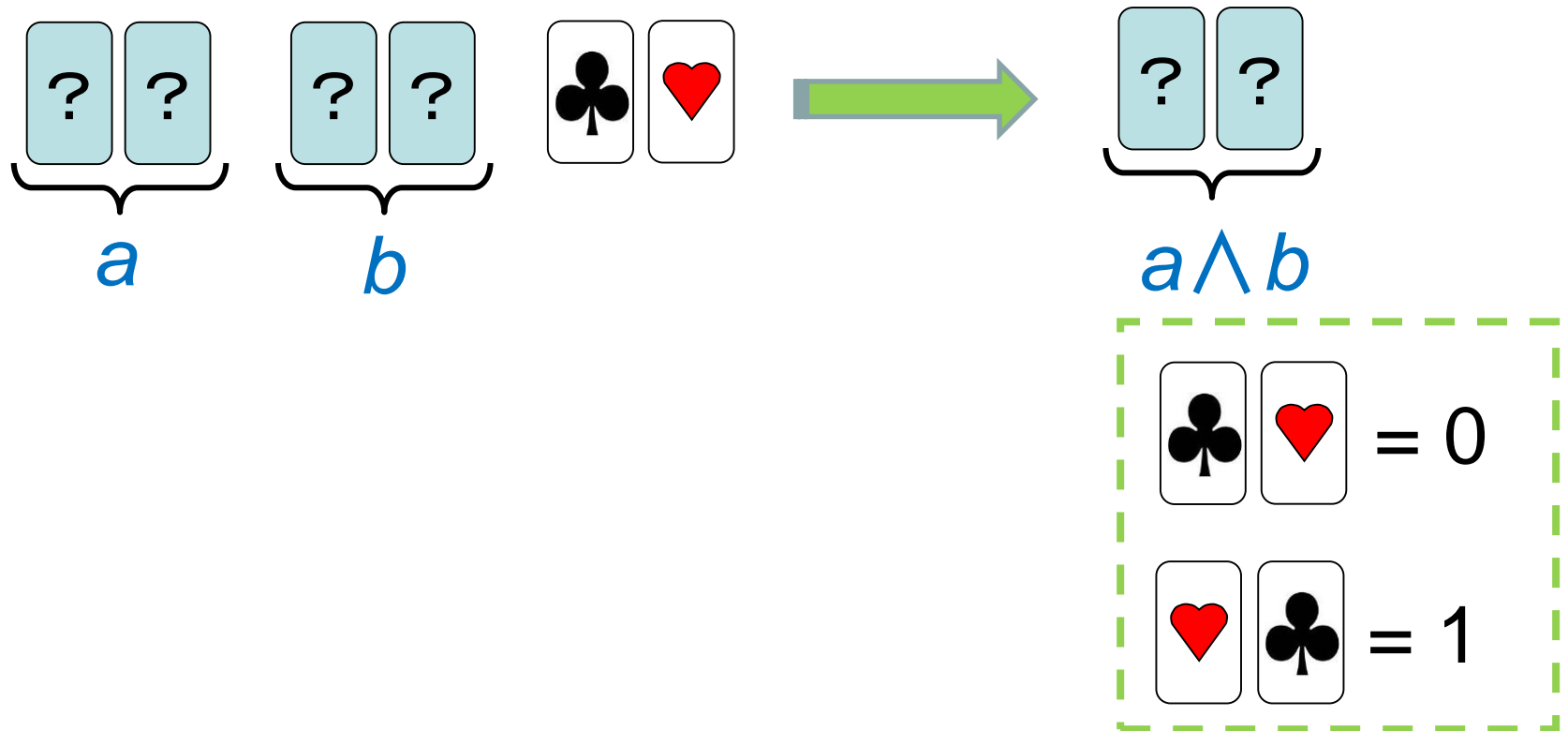
[CK93]
[NR98]
[Sti01]

[MS09]


[KKWM⁺17]

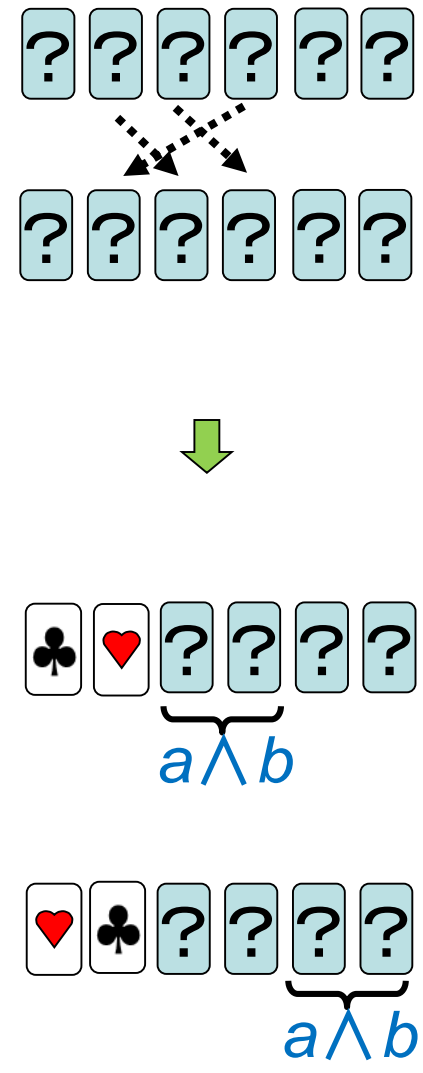
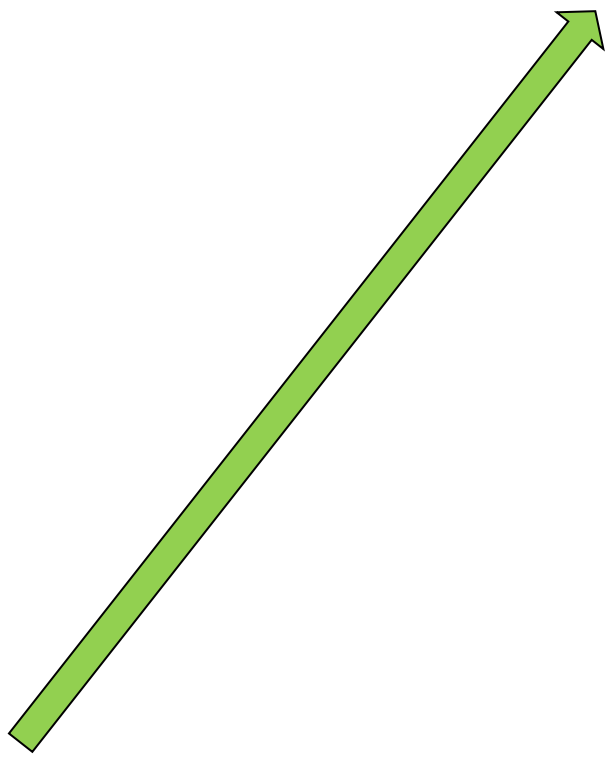
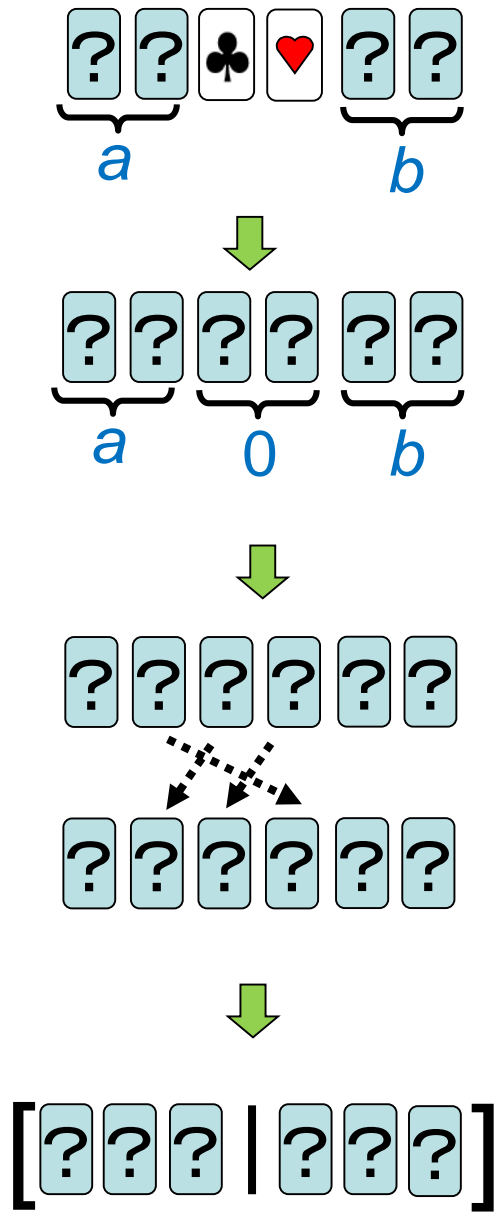
$$\begin{array}{|c|c|} \hline \clubsuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \clubsuit \\ \hline \end{array} = 1$$

6枚のカードで $a \wedge b$ のコミットメントを得る^[MS09]

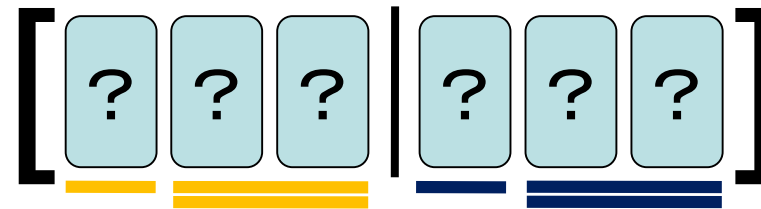


[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

  = 0   = 1



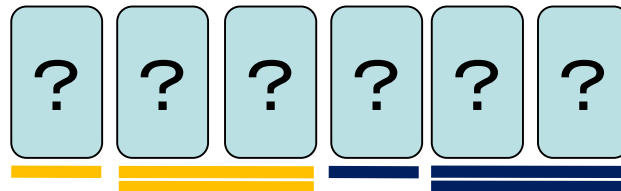
ランダム二等分割カットを適用する:



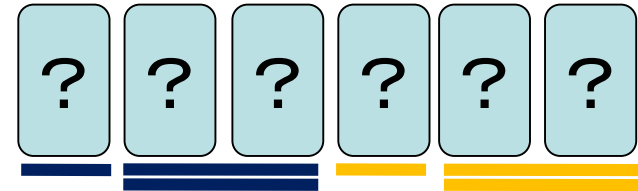
prob. of 1/2



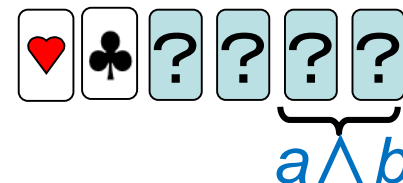
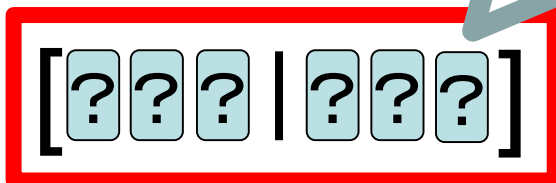
prob. of 1/2




(a)



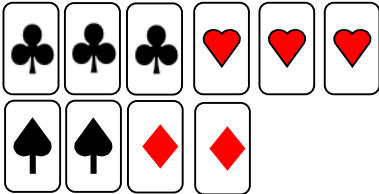
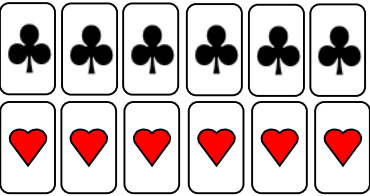

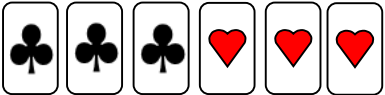
(b)



コミット型ANDプロトコルのまとめ:

  = 0   = 1



	枚数等	ランダム カット	二等分割 カット	平均試行 回数
Crepeau-Kilian [CRYPTO '93]	10 	✓		6
Niemi-Renvall [TCS, 1998]	12 	✓		2.5
Stiglic [TCS, 2001]	8 	✓		2
Mizuki-Sone [FAW 2009]	6 		✓	1

2章の構成

  = 0   = 1

シャッフルのクラス

複雑なシャッフル

[KWH15]

2.4. 簡単なシャッフル [KKWM⁺17]

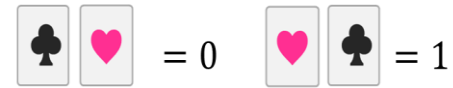
[CK93]

[NR98]

[Sti01]

[MS09]

[KWH15] を紹介する前に...

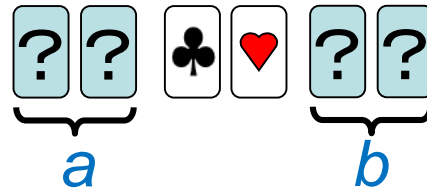


- シャッフル操作を定式化^[MS14]
 - [KWH15] は複雑なシャッフルを必要とするので、その紹介のために必要
 - “簡単”なシャッフルと“複雑”なシャッフルの区分のために必要

[MS14] Takaaki Mizuki and Hiroki Shizuya, “A Formalization of Card-Based Cryptographic Protocols via Abstract Machine,” International Journal of Information Security, Springer-Verlag, vol.13, no.1, pp.15-23, 2014.

カード列

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$



$$\left(\frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit} \right)$$

$$\begin{array}{|c|} \hline \spadesuit \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \spadesuit \\ \hline \end{array} = 1$$

$$\left(\frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit} \right)$$

並び替える



(perm, (2 4 3))

$$\left(\frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit} \right)$$

$$\begin{array}{|c|} \hline \spadesuit \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \spadesuit \\ \hline \end{array} = 1$$

$$\left(\frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit} \right)$$

シャッフル

$$(\text{shuf}, \text{id} \mapsto 1/2, (1\ 4)(2\ 5)(3\ 6) \mapsto 1/2)$$



$$\left(\frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit} \right)$$

$$\left(\frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit} \right)$$

シャッフルは、置換の集合とその上の確率分布

2章の構成

  = 0   = 1

シャッフルのクラス

複雑なシャッフル

4-card KWH

5-card KWH

2.4. 簡単なシャッフル [KKWM+17]

[CK93]

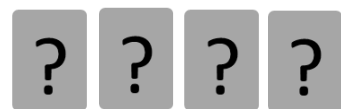
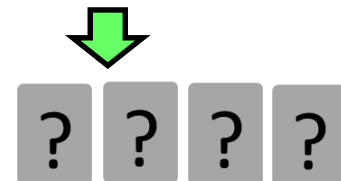
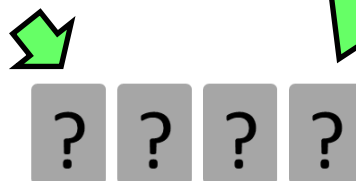
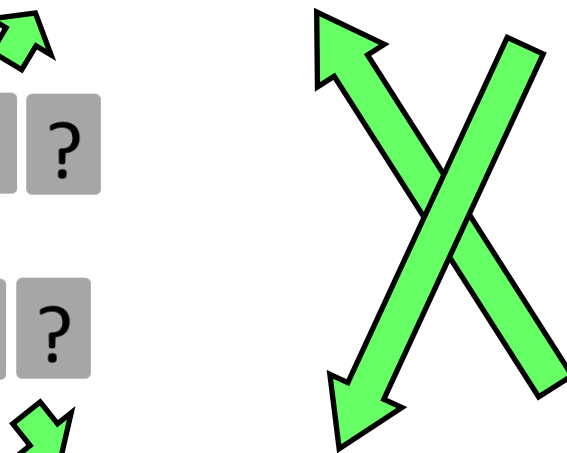
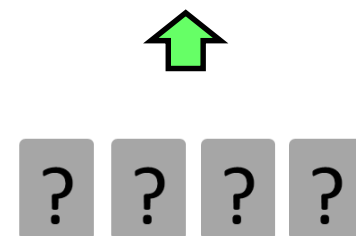
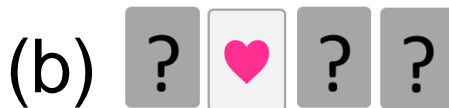
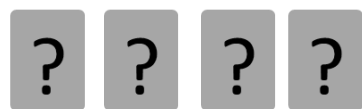
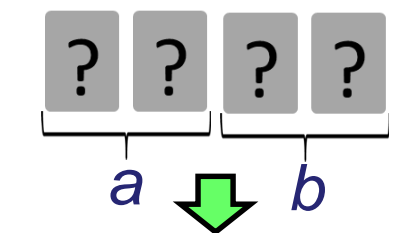
[NR98]

[Sti01]

[MS09]

4-card KWH(詳細略)

♣♥ = 0 ♥♣ = 1



確率1/3
で終了



$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

$$\left(\frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit} \right)$$

KWH プロトコルに必要なシャッフル(1)

(shuf, id \mapsto **1/3**, (1 3)(2 4) \mapsto **2/3**)



$$\left(\frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit} \right)$$

$$\left(\frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\spadesuit} \right)$$

つまり、不均一な(確率分布の)シャッフル

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

$$\left(\frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\spadesuit} \right)$$

KWH プロトコルに必要なシャッフル(2)

(shuf, **id** \mapsto 1/3, (**5 4 3 2 1**) \mapsto 2/3)



$$\left(\frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\spadesuit} \right)$$

$$\left(\frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\spadesuit}, \frac{?}{\spadesuit}, \frac{?}{\heartsuit} \right)$$

つまり、置換集合が群を成していない

$(\text{shuf}, \Pi, \mathcal{F})$ の分類 [KWH15]

- ① \mathcal{F} が均一 (uniform) である
- ② Π が群を成している (closed)

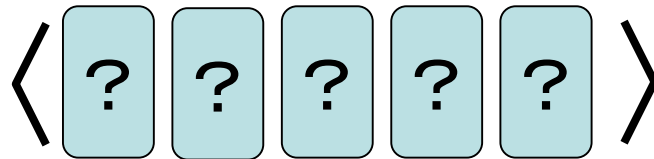
- ランダムカットは① ② を満たす

$$\text{RC}^5 = (\text{shuf}, \{(1\ 2\ 3\ 4\ 5)^i \mid 0 \leq i \leq 4\})$$

- ランダム二等分割カットは① ② を満たす

$$\text{RBC} = (\text{shuf}, \text{id} \mapsto 1/2, (1\ 4)(2\ 5)(3\ 6) \mapsto 1/2)$$

ランダムカット







$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$



uniform-closed だと簡単に手で実装できる(と信じている)

実際に分類を行うと

  = 0   = 1

シャッフルのクラス

複雑なシャッフル

[KWH15]

2.4. 簡単なシャッフル [KKWM⁺17]

[CK93]
[NR98]
[Sti01]

[MS09]

2章の構成

  = 0   = 1

シャッフルのクラス

5-card KWH

uniform

[CK93]
[NR98]
[Sti01]
[MS09]

closed

4-card KWH

お待たせしました...

  = 0   = 1

シャッフルのクラス

5-card KWH

2.4. [KKWM+17]

uniform

closed

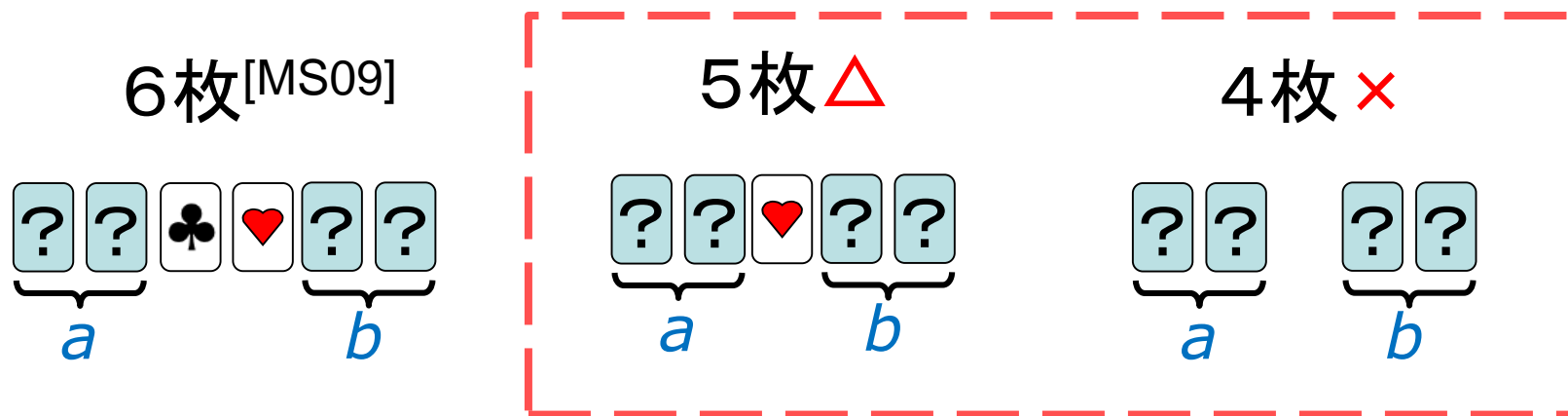
[CK93]
[NR98]
[Sti01]
[MS09]

4-card KWH

[再掲] あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- “実用的な”AND プロトコルを解明
(カード枚数・実行時間・シャッフルの難しさ...)



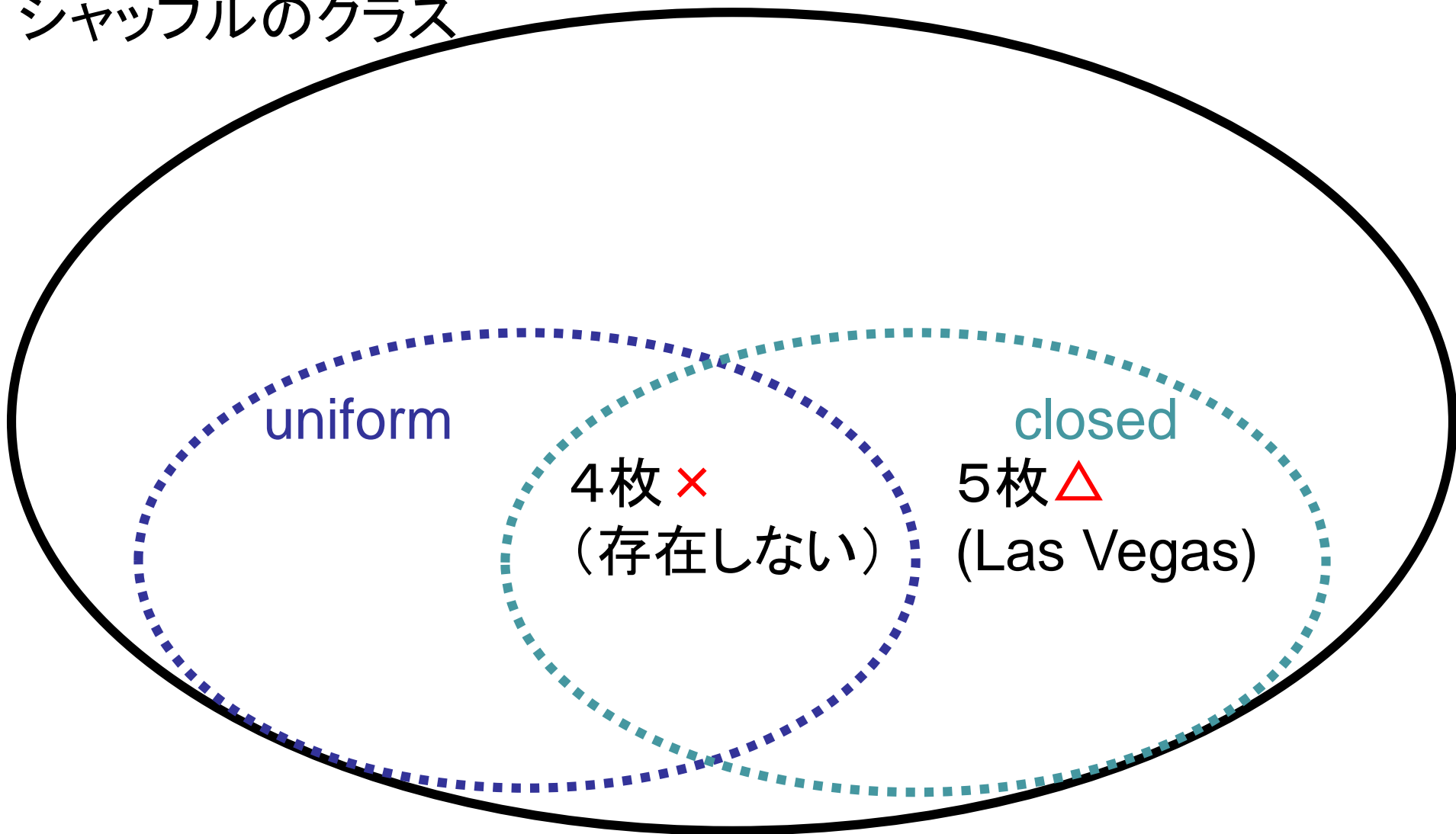
\triangle : プロトコルは存在する(だろう)が、Las Vegas である

\times : プロトコルは存在しない

ANDのために必要な枚数

  = 0   = 1

シャッフルのクラス



※具体的なプロトコルは提案できていないことに注意

ANDのために必要な枚数

  = 0   = 1

シャッフルのクラス

The Minimum
Number of Cards
in Practical Card-
based Protocols

4枚 ×
(存在しない)

6枚 [MS09]

closed
5枚 △
(Las Vegas)

uniform-closedのみを用いたAND

$$\begin{array}{|c|c|} \hline \spadesuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \spadesuit \\ \hline \end{array} = 1$$

枚数	有限	Las Vegas
6	[MS09]	
5		
4	✖ [KWH15]	

uniform-closedでの枚数下界

$$\begin{array}{|c|c|} \hline \spadesuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \spadesuit \\ \hline \end{array} = 1$$

枚数	有限	Las Vegas
6	[MS09]	
5	✖ ※ (ours)	
4	✖ [KWH15]	✖ (ours)

※ closedのみでも不可能

これから詳しく
見ていく

[復習] $(\text{shuf}, \Pi, \mathcal{F})$ の分類 [KWH15]

$$\begin{array}{|c|c|} \hline \spadesuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \spadesuit \\ \hline \end{array} = 1$$

- ① \mathcal{F} が均一 (uniform) である
- ② Π が群を成している (closed)

- ランダムカットは① ② を満たす

$$\text{RC}^5 = (\text{shuf}, \{(1\ 2\ 3\ 4\ 5)^i \mid 0 \leq i \leq 4\})$$

- ランダム二等分割カットは① ② を満たす

$$\text{RBC} = (\text{shuf}, \text{id} \mapsto 1/2, (1\ 4)(2\ 5)(3\ 6) \mapsto 1/2)$$

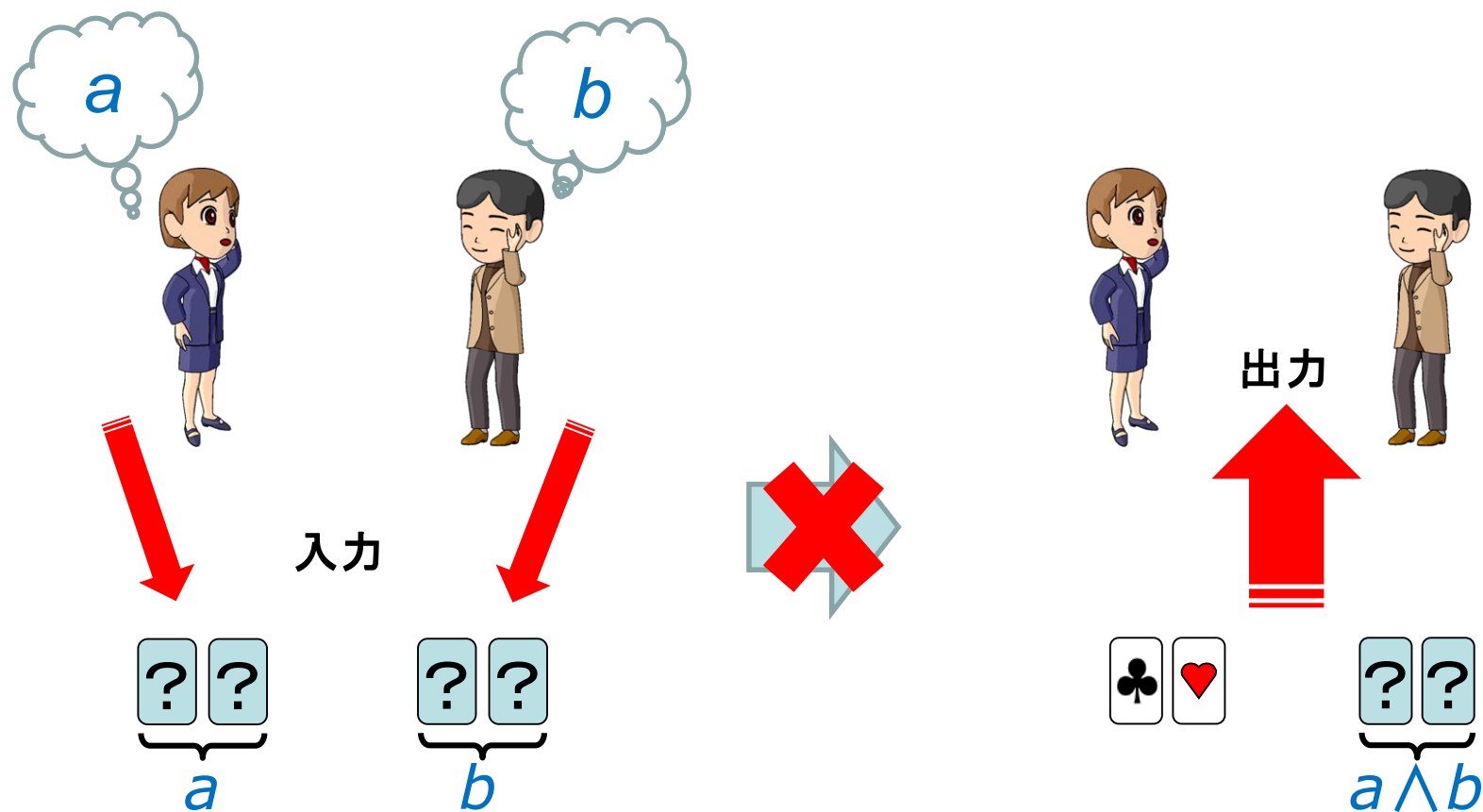
定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない



= 0



= 1



証明の概略(実際のスライド)

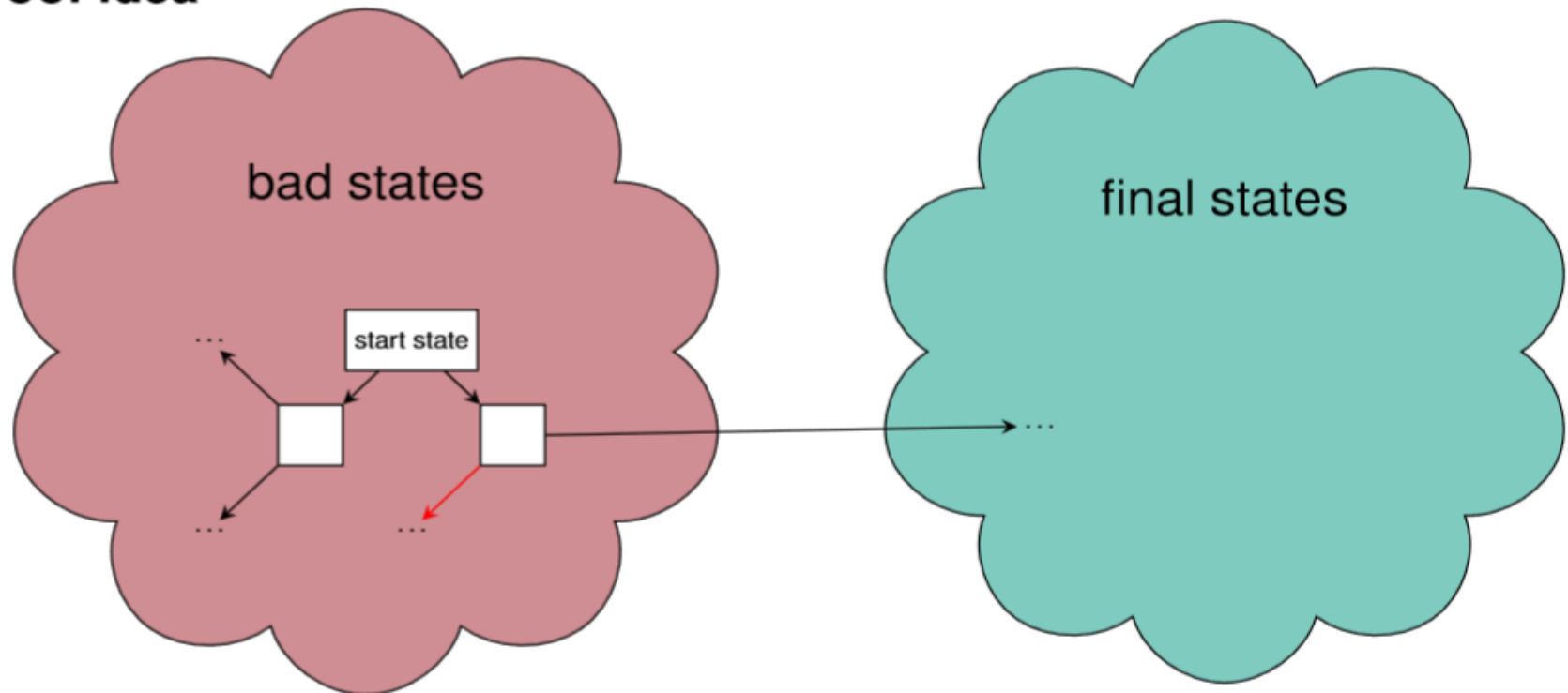
♣♥ = 0 ♥♣ = 1

Impossibility Result

Theorem

There is no secure **finite-runtime closed-shuffle** 5-card AND protocol

Proof Idea



At least one outgoing edge (path) leads to a bad state again.

state: チューリング機械のような状態のこと

証明の概略(実際のスライド)

♣♥ = 0 ♥♣ = 1

Impossibility Re

Theorem

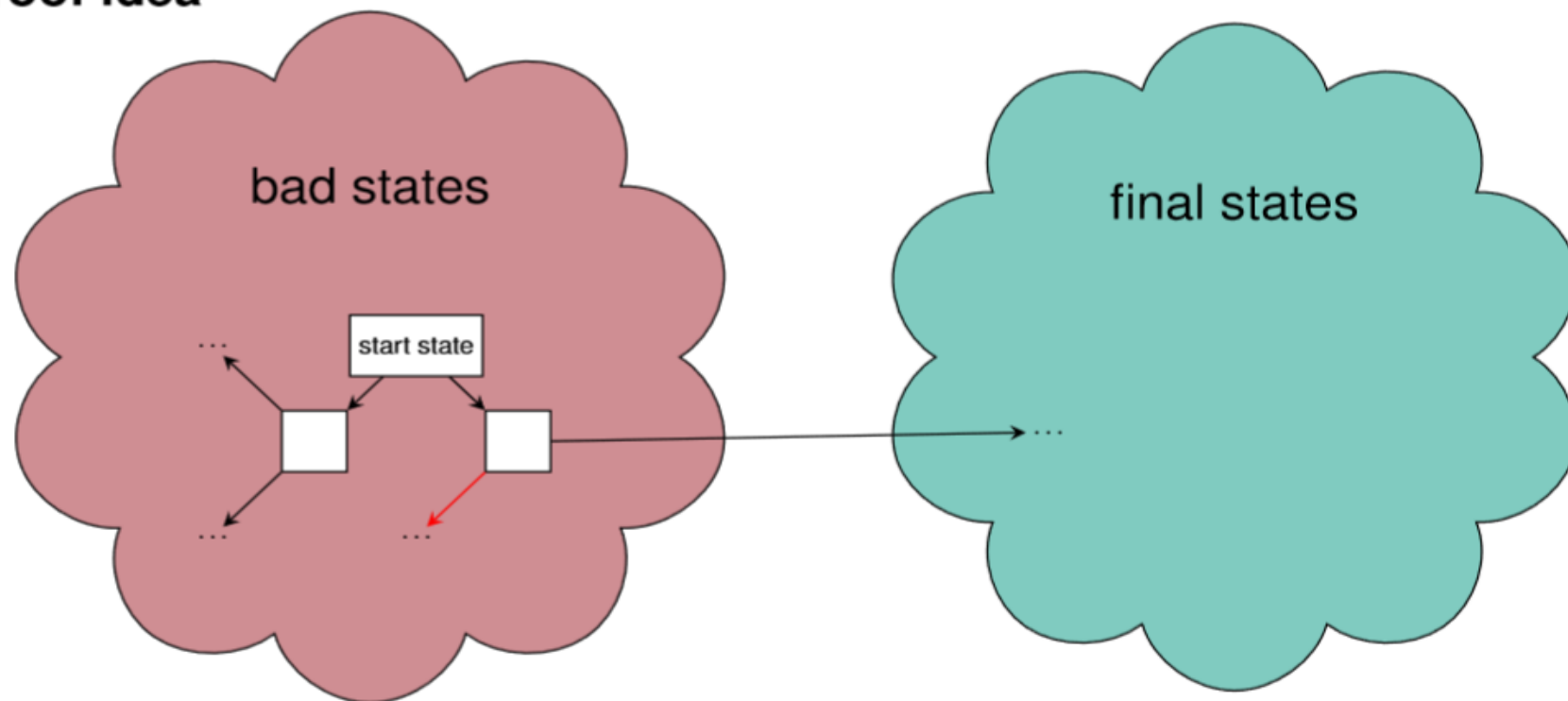
There is no secure f

Proof Idea





(1) stateの定義 [KWH15]

(2) 4枚ANDのbad/final [KWH15]

(3) ucによるstate遷移



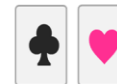
At least one outgoing edge (path) leads to a bad state again.

定理: uniform-closed (uc) シヤッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

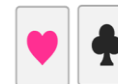
(1) stateの定義

- テーブルに置かれたカード列の絵柄を、入力毎に列挙したもの

定理: uniform-closed (uc) シヤッフルのみを用いた4枚ANDは存在しない



= 0

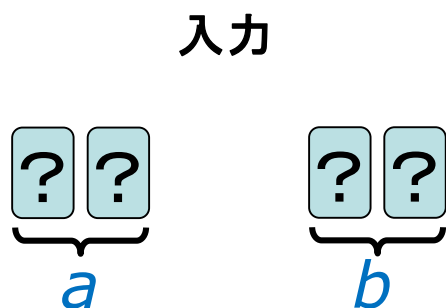


= 1

(1) stateの定義

- テーブルに置かれたカード列の絵柄を、入力毎に列挙したもの
- X_a は、入力が $a \in \{0,1\}^2$ である確率を表す文字

例) 4-card ANDの入力state



♥ ♣ ♥ ♣	X_{11}
♣ ♥ ♥ ♣	X_{01}
♥ ♣ ♣ ♥	X_{10}
♣ ♥ ♣ ♥	X_{00}

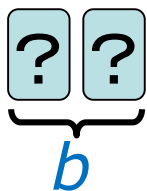
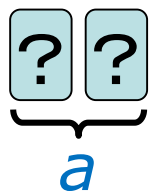
定理: uniform-closed (uc) シヤッフルのみを用いた4枚ANDは存在しない

$$\begin{array}{|c|c|} \hline \spadesuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \spadesuit \\ \hline \end{array} = 1$$





(1) stateの定義(詳しく)

- 絵柄列と多項式の組の集合
- 多項式は、現在置かれているカード列が、その多項式の組の絵柄列である確率

例) 4-card ANDの入力state



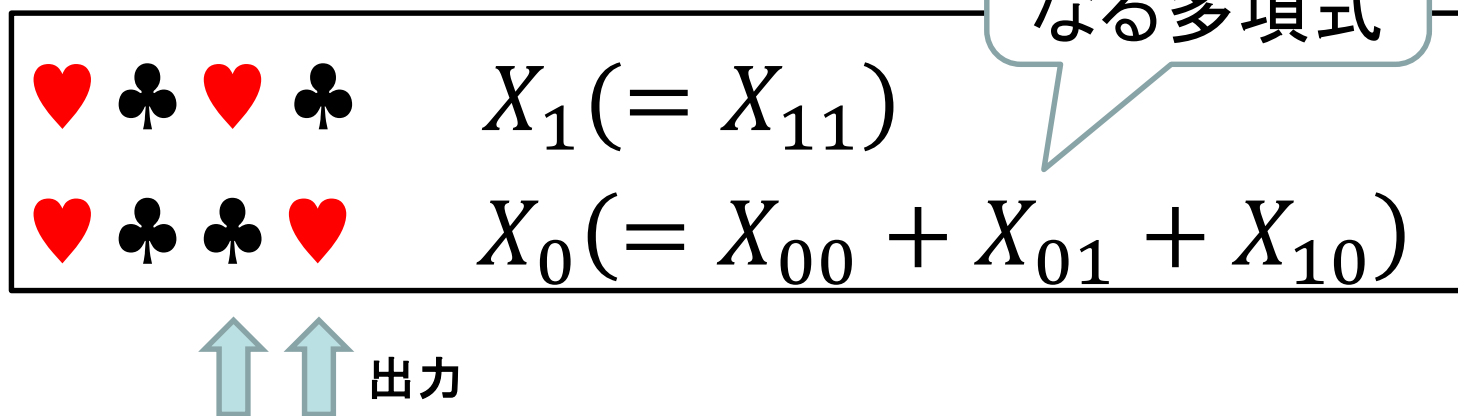
♥ ♣ ♥ ♣	X_{11}
♣ ♥ ♥ ♣	X_{01}
♥ ♣ ♣ ♥	X_{10}
♣ ♥ ♣ ♥	X_{00}





定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(1) stateの定義(詳しく)

- 絵柄列と多項式の組の集合
- 多項式は、現在置かれているカード列が、その多項式の組の絵柄列である確率

例) 4-card ANDのfinal state

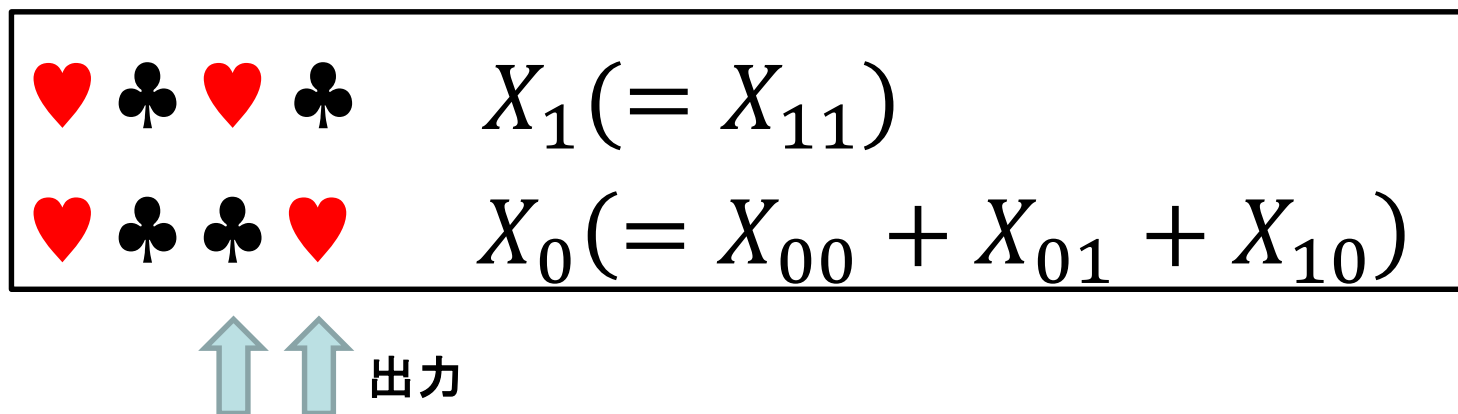


定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(1) i/j stateの定義

- i : 出力が0になる多項式を持つ組の個数
- j : 出力が1になる多項式を持つ組の個数

例) 4-card ANDの1/1 state (必ずfinal)



証明の概略(実際のスライド)

♣♥ = 0 ♥♣ = 1

Impossibility Re

Theorem

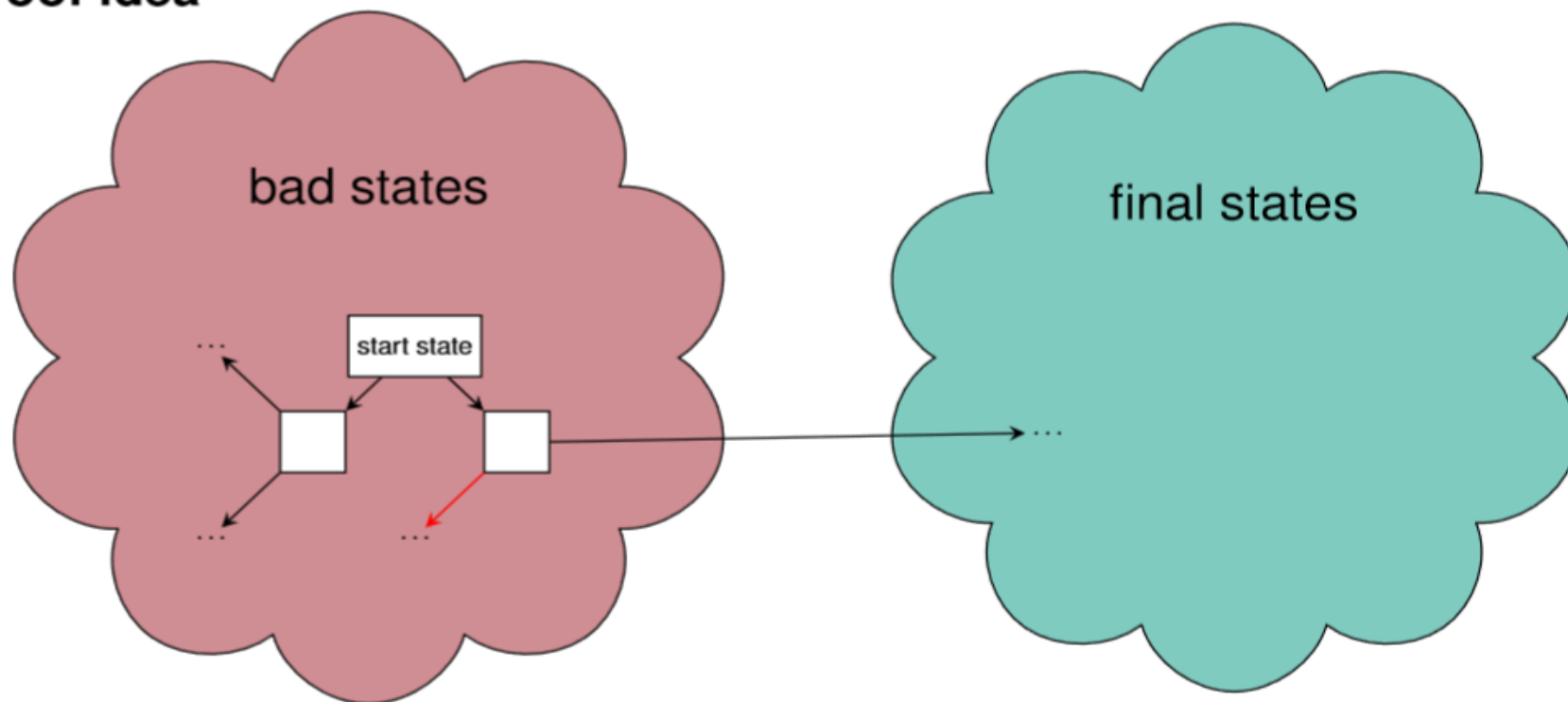
There is no secure f

Proof Idea

(1) stateの定義 [KWH15]

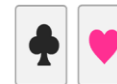
(2) 4枚ANDのbad/final [KWH15]

(3) ucによるstate遷移

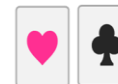


At least one outgoing edge (path) leads to a bad state again.

定理: uniform-closed (uc) シヤッフルのみを用いた4枚ANDは存在しない



= 0



















= 1

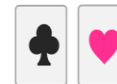
(2) bad/final stateの定義

- **bad state** : コミットメントを出力できない
- **final state** : コミットメントを出力できる

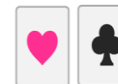
例) 3/1 state (入力state) \Rightarrow bad state

   	X_{11}
   	X_{01}
   	X_{10}
   	X_{00}

定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない



= 0















= 1

(2) bad/final stateの定義

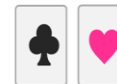
- **bad state** : コミットメントを出力できない
- **final state** : コミットメントを出力できる

例) 2/1 state (絵柄が一致する列無し) \Rightarrow final state

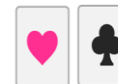
				X_1
				$1/2X_0$
				$1/2X_0$



定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない



= 0



















= 1

(2) bad/final stateの定義

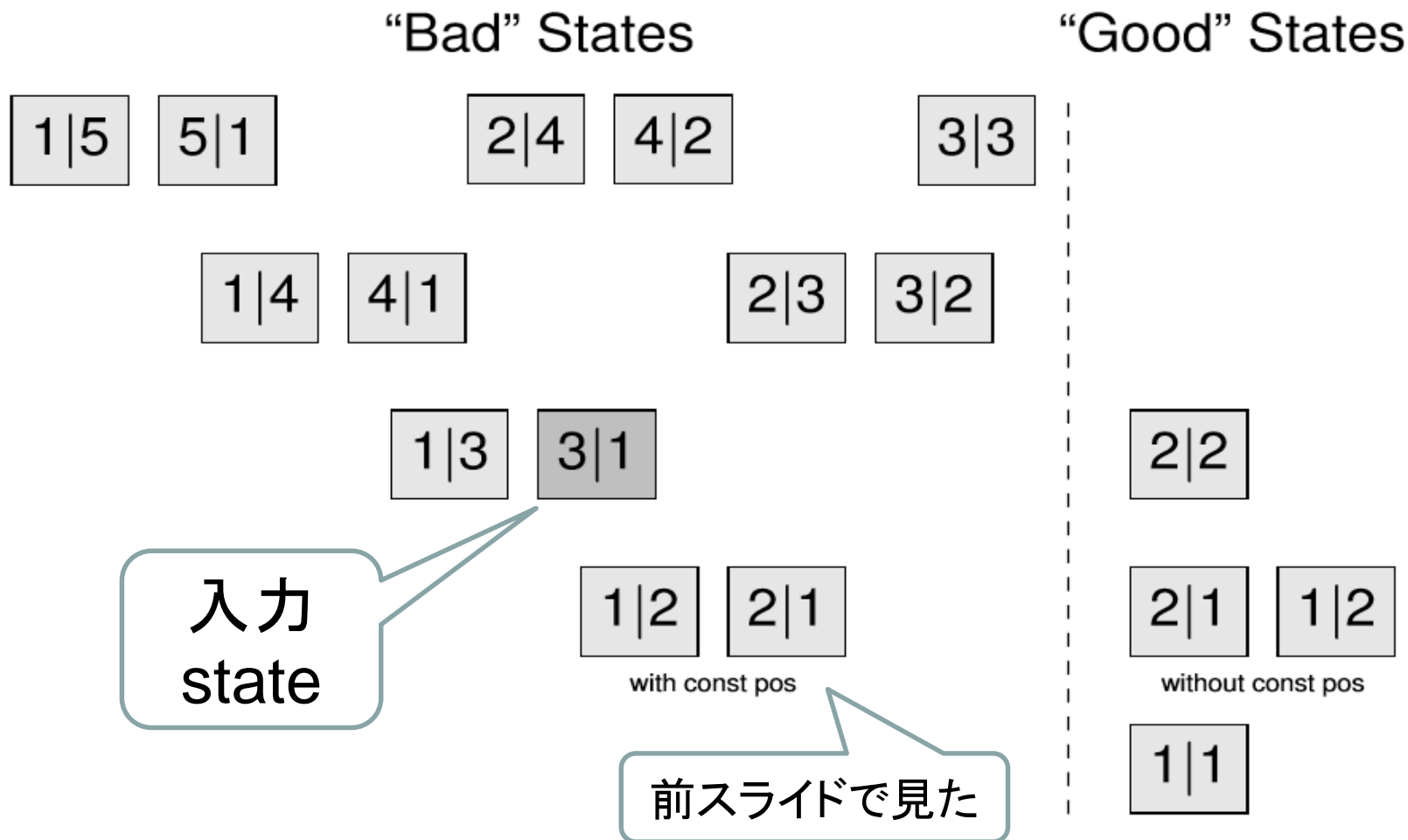
- **bad state** : コミットメントを出力できない
- **final state** : コミットメントを出力できる





例) 2/1 state (絵柄が一致する列有り) \Rightarrow **bad state**

   	X_1
   	$1/2X_0$
   	$1/2X_0$

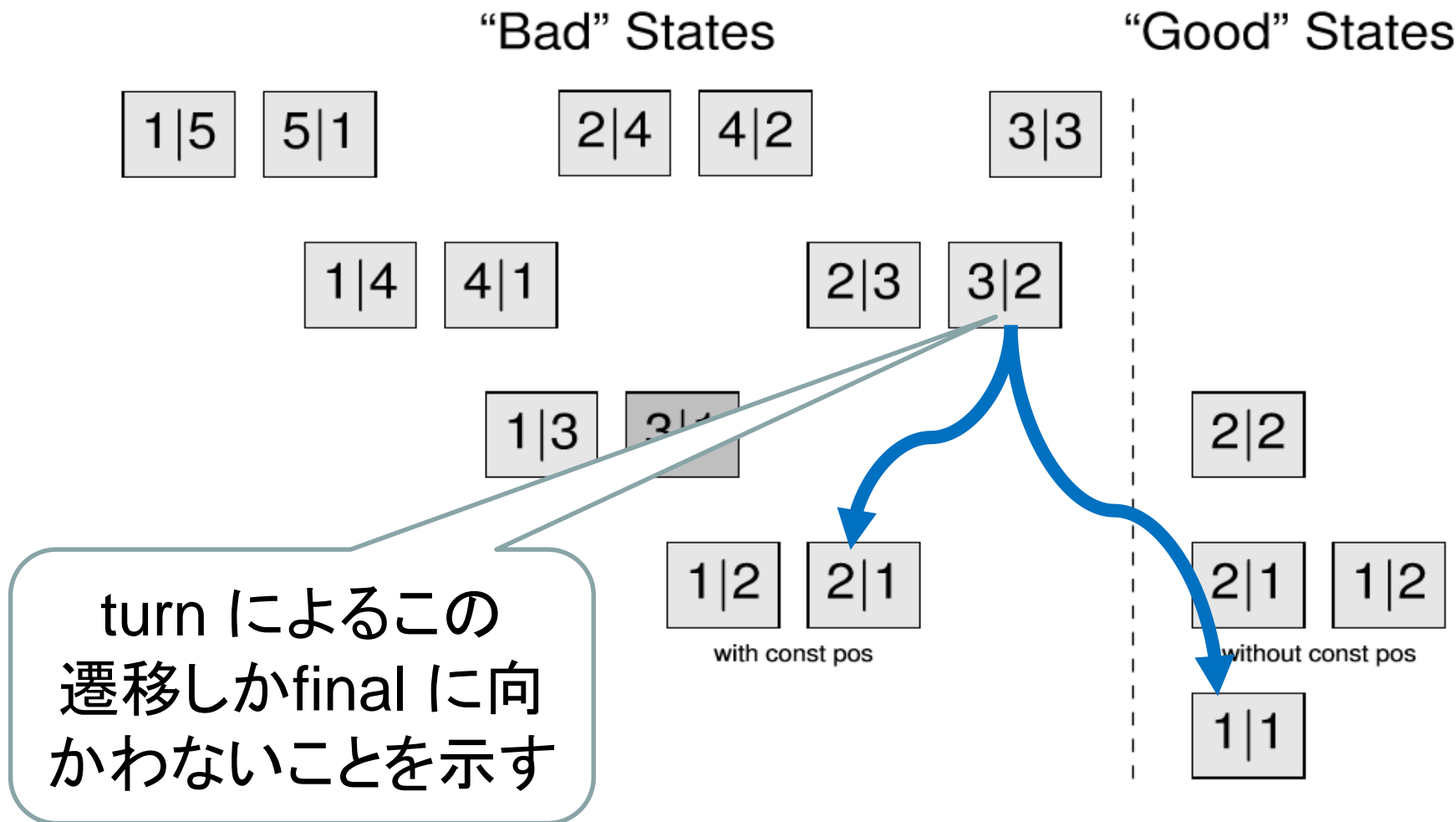
定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(2) 4枚ANDのbad/final stateの区分け



定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(2) 4枚ANDのbad/final stateの区分け























定理: uniform-closed (uc) シヤッフルのみを用いた4枚ANDは存在しない

  = 0   = 1









例) $3/2 \Rightarrow 1/1, 2/1$ の遷移 (final はこれだけ)

4-card KWH の
実際の遷移













   	$1/3X_1$
   	$2/3X_1$
   	$1/2X_0$
   	$1/6X_0$
   	$1/3X_0$





絵柄が一致して
いるのでfinal に
なれないことを思
い出そう

turn 4

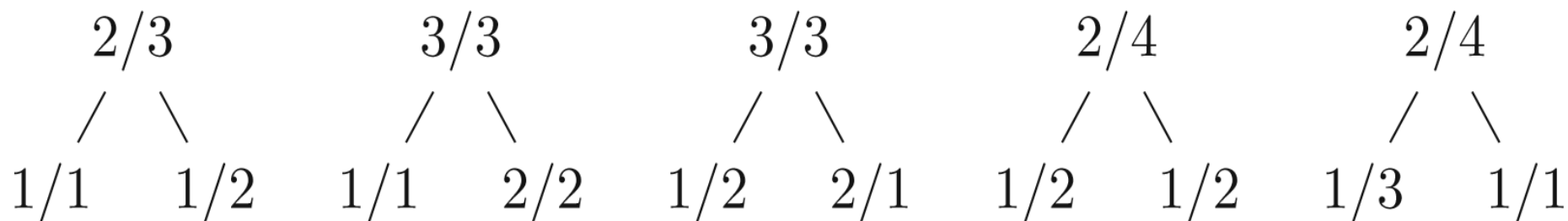
   	X_1
   	X_0

  出力

   	X_1
   	$3/4X_0$
   	$1/4X_0$

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(2) turnによる遷移の考えられる全て



一見、たくさんfinal がありそう

(5/1 state 等にturn を行くと入力が漏れることに注意)

定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない

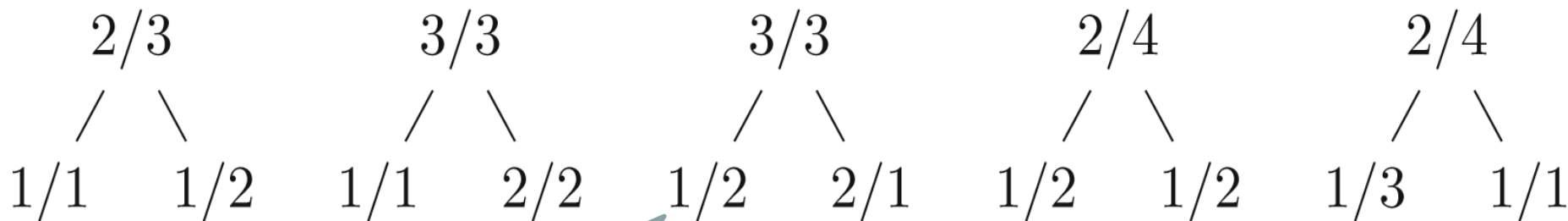


= 0







= 1

(2) turnによる遷移の考えられる全て



turn後は絵柄が一致するのでfinal になれないことは見た

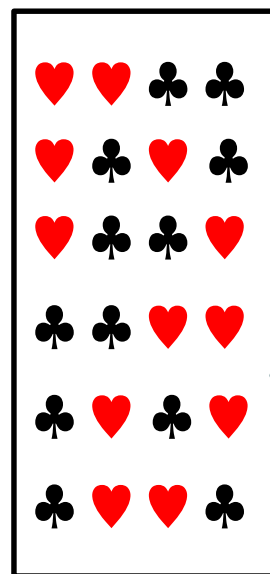
turn 後の $i+j < 4$ であることをこれから示す

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(2) turn 後の $i+j$

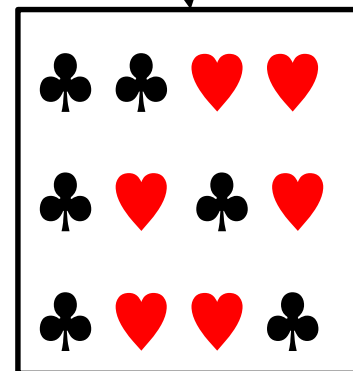
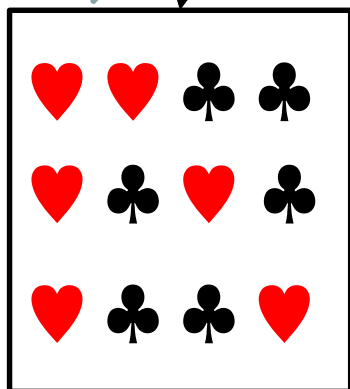
4枚において、共通の絵柄をもつような絵柄列は高々3個





⇒ $i+j < 4$



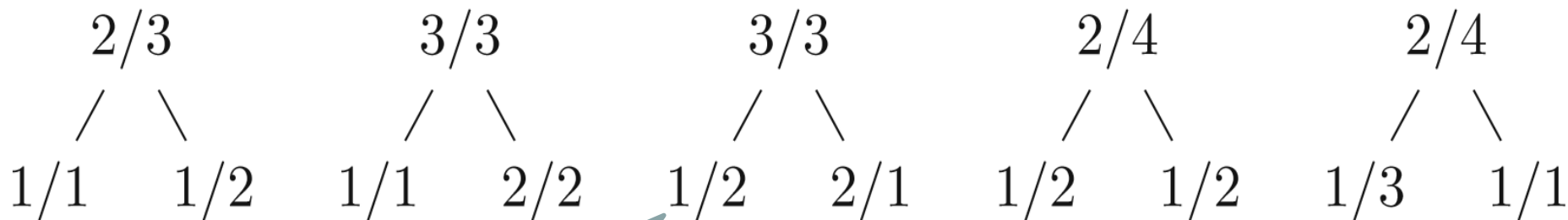
4枚で考えられる全ての絵柄を含んだ state (確率省略)

turn 1







定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(2) turnによるstateの遷移

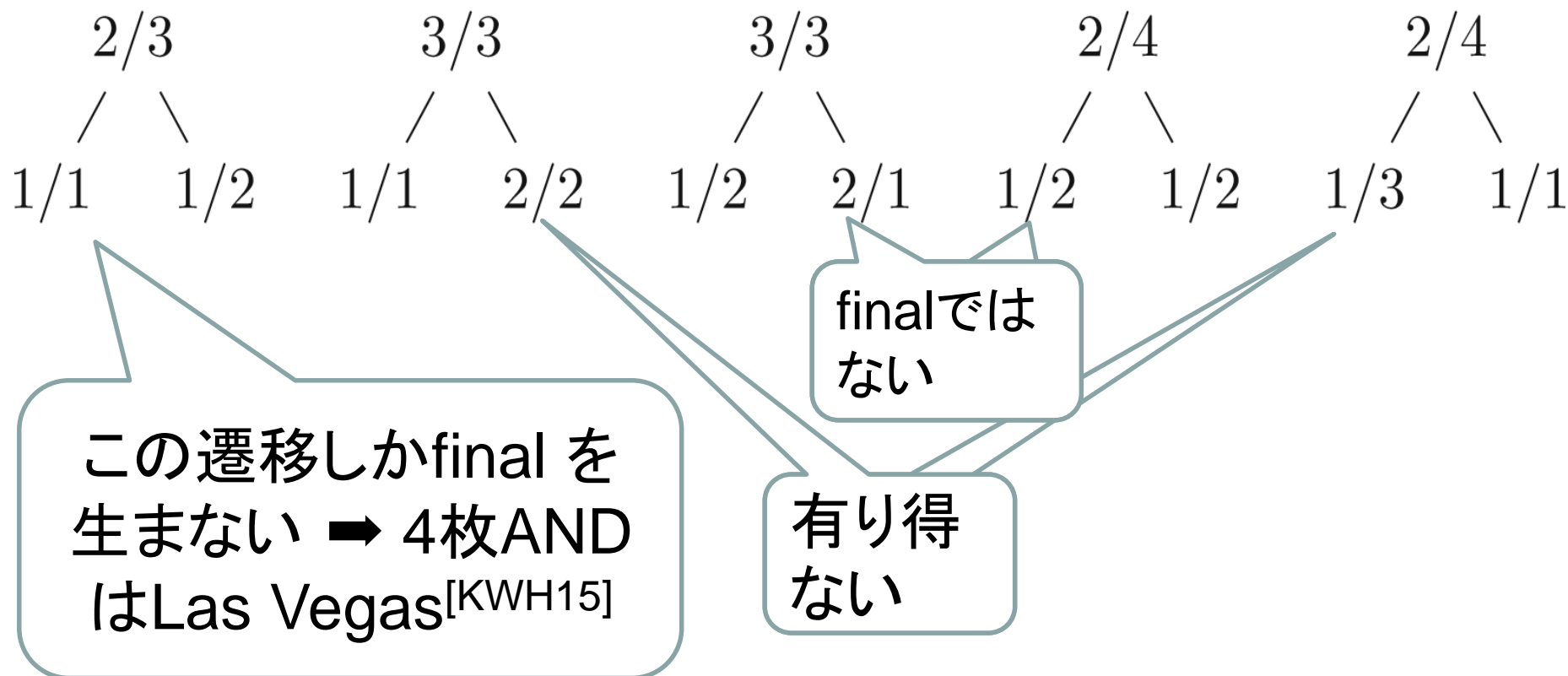


turn後は絵柄が一致するのでfinal になれないことは見た

turn 後の $i+j < 4$ であることを見た

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(2) turnによるstateの遷移



証明の概略(実際のスライド)

♣♥ = 0 ♥♣ = 1

Impossibility Re

Theorem

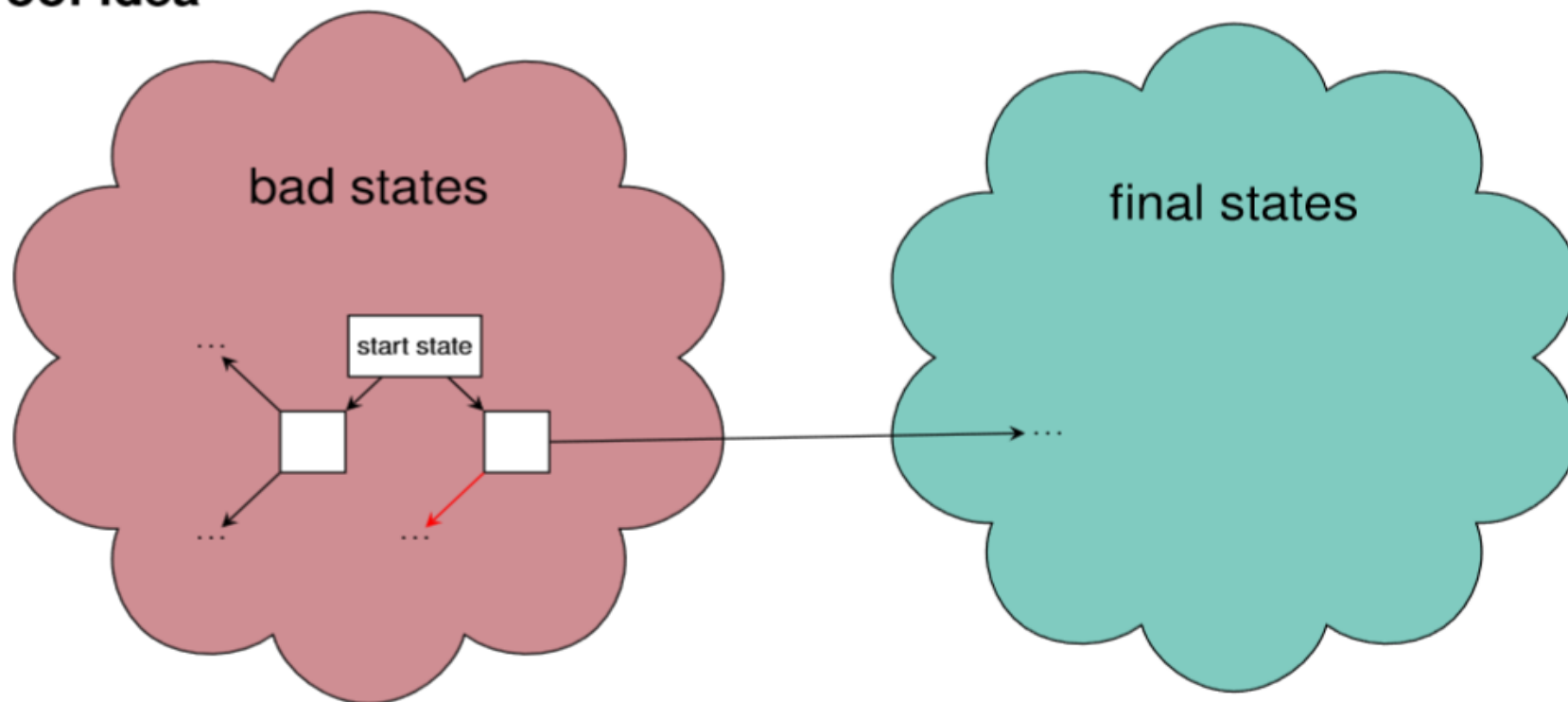
There is no secure f

Proof Idea

(1) stateの定義 [KWH15]

(2) 4枚ANDのbad/final [KWH15]

(3) ucによるstate遷移



At least one outgoing edge (path) leads to a bad state again.

[復習] $(\text{shuf}, \Pi, \mathcal{F})$ の分類 [KWH15]

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- ① \mathcal{F} が均一 (uniform) である
- ② Π が群を成している (closed)

- ランダムカットは① ② を満たす

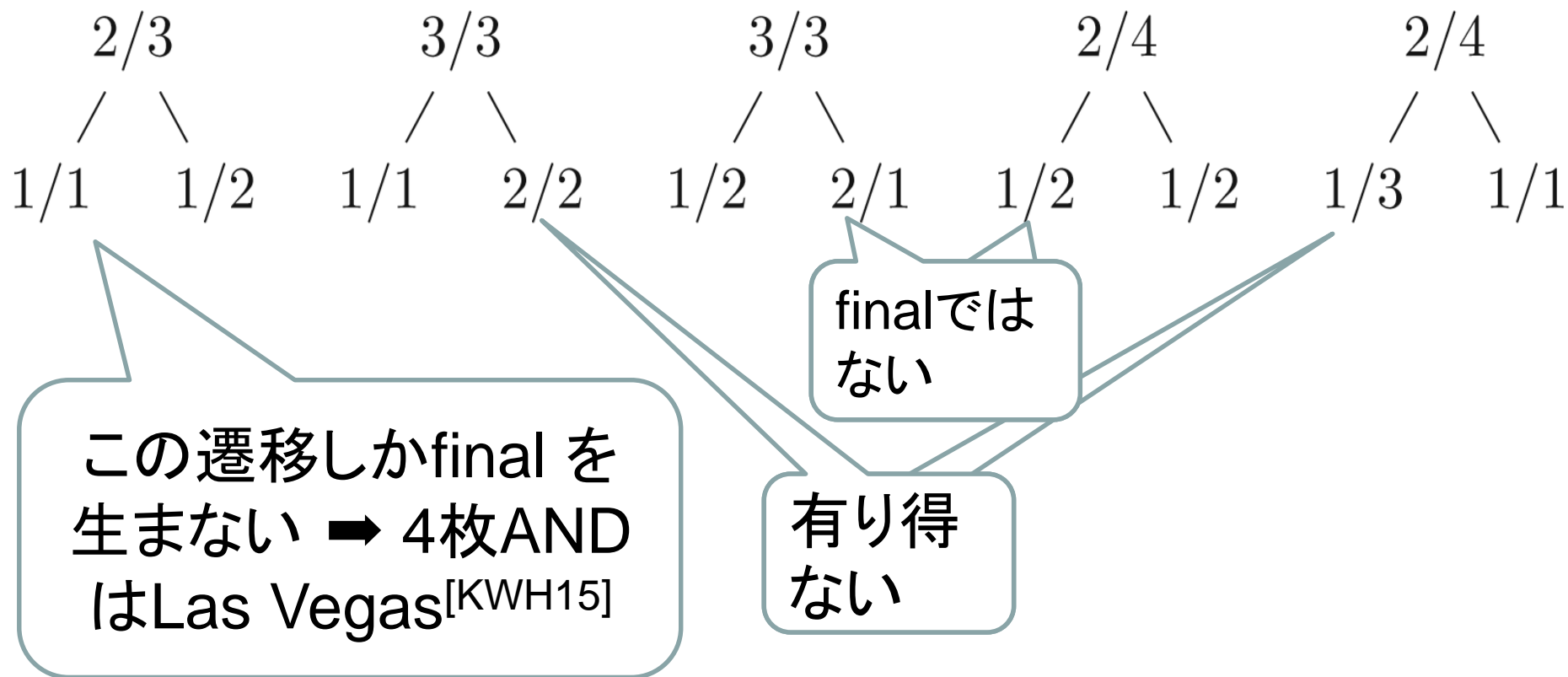
$$\text{RC}^5 = (\text{shuf}, \{(1\ 2\ 3\ 4\ 5)^i \mid 0 \leq i \leq 4\})$$





- ランダム二等分割カットは① ② を満たす

$$\text{RBC} = (\text{shuf}, \text{id} \mapsto 1/2, (1\ 4)(2\ 5)(3\ 6) \mapsto 1/2)$$

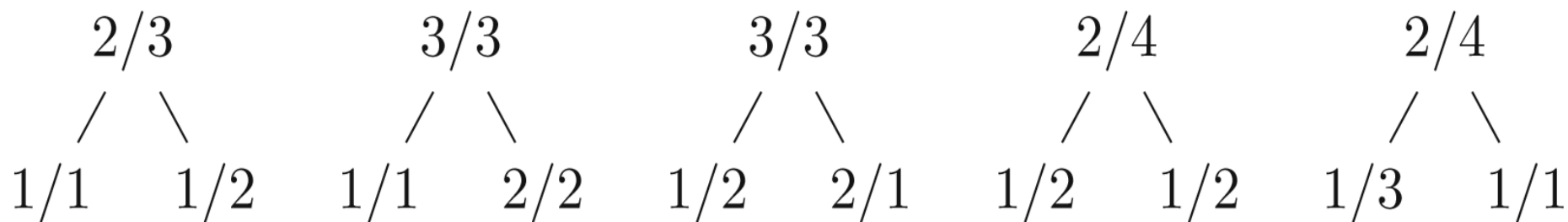
定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない

[復習] (2) turnによるstateの遷移







定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

[復習] (2) turnによるstateの遷移



自然な発想: uc shuffleで2/3 stateに
到達できる? ➡できないことを示す

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(3) 4枚ANDのbad/final stateの区分け

“Bad” States

“Good” States

1|5 5|1

2|4 4|2

3|3

1|4 4|1

2|3 3|2

...

3|1

1|2 2|1

with const pos





2|2

2|1 1|2

without const pos













1|1

uc shuffle では
この遷移があり得
ないことを示す
(他は省略)

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない





















(3) uc shuffleによる $1/2 \rightarrow 2/3$ 遷移の不可能性





1/2 stateは共通する絵柄を必ずもつことに注意しよう

   	X_1
   	X_1
   	X_0

shuf, Π, \mathcal{F}
 Π : closed (群)
 \mathcal{F} : uniform (均一)













一般性を失わずに、
    は2/3に含まれないと仮定

   	X_1
   	X_1
   	X_1
   	X_0
   	X_0





















定理: uniform-closed (uc) シヤッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(3) Π : closed $\Rightarrow \Pi \subset \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$
と限定できる





具体例
で示す

   	X_1
   	X_1
   	X_0













shuf, Π , \mathcal{F}
 Π : closed (群)
 \mathcal{F} : uniform (均一)

   	X_1
   	X_1
   	X_1
   	X_0
   	X_0





















    は含まれ
ないと仮定したこと
に注意

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない





例) $\Pi = \{\text{id}, (1\ 3)\} \Rightarrow \heartsuit \heartsuit \clubsuit \clubsuit$ が含まれるので矛盾





   	X_1
   	X_1
   	X_0

shuf, $\{\text{id}, (1\ 3)\}$

   	X_1
   	X_1
   	X_1
   	X_0
   	X_0













$\heartsuit \heartsuit \clubsuit \clubsuit$ は含まれないと仮定したことに注意





















定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

(3) Π 上で     は不変でなければならない
 $\Rightarrow \Pi \subset \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$





closed が効
いている部分

shuf, Π , \mathcal{F}
 Π : closed (群)
 \mathcal{F} : uniform (均一)

   	X_1
   	X_1
   	X_0

   	X_1
   	X_1
   	X_1
   	X_0
   	X_0

    は含まれ
ないと仮定したこと
に注意

定理: uniform-closed (uc) シャッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

まとめ:

- 4枚ANDは, $2/3 \rightarrow 1/1, 1/2$ の遷移で終了する
- uc シャッフルでは $2/3$ に到達できない

➡ ucのみの4枚ANDは存在し得ない

まとめ: uniform-closedでの枚数下界

$$\begin{array}{|c|c|} \hline \spadesuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \spadesuit \\ \hline \end{array} = 1$$

枚数	有限	Las Vegas
6	[MS09]	
5	✖ ※ (ours)	
4	✖ [KWH15]	✖ (ours)

※ closedのみでも不可能

いま見た

未解決問題

$$\begin{array}{|c|c|} \hline \spadesuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \spadesuit \\ \hline \end{array} = 1$$

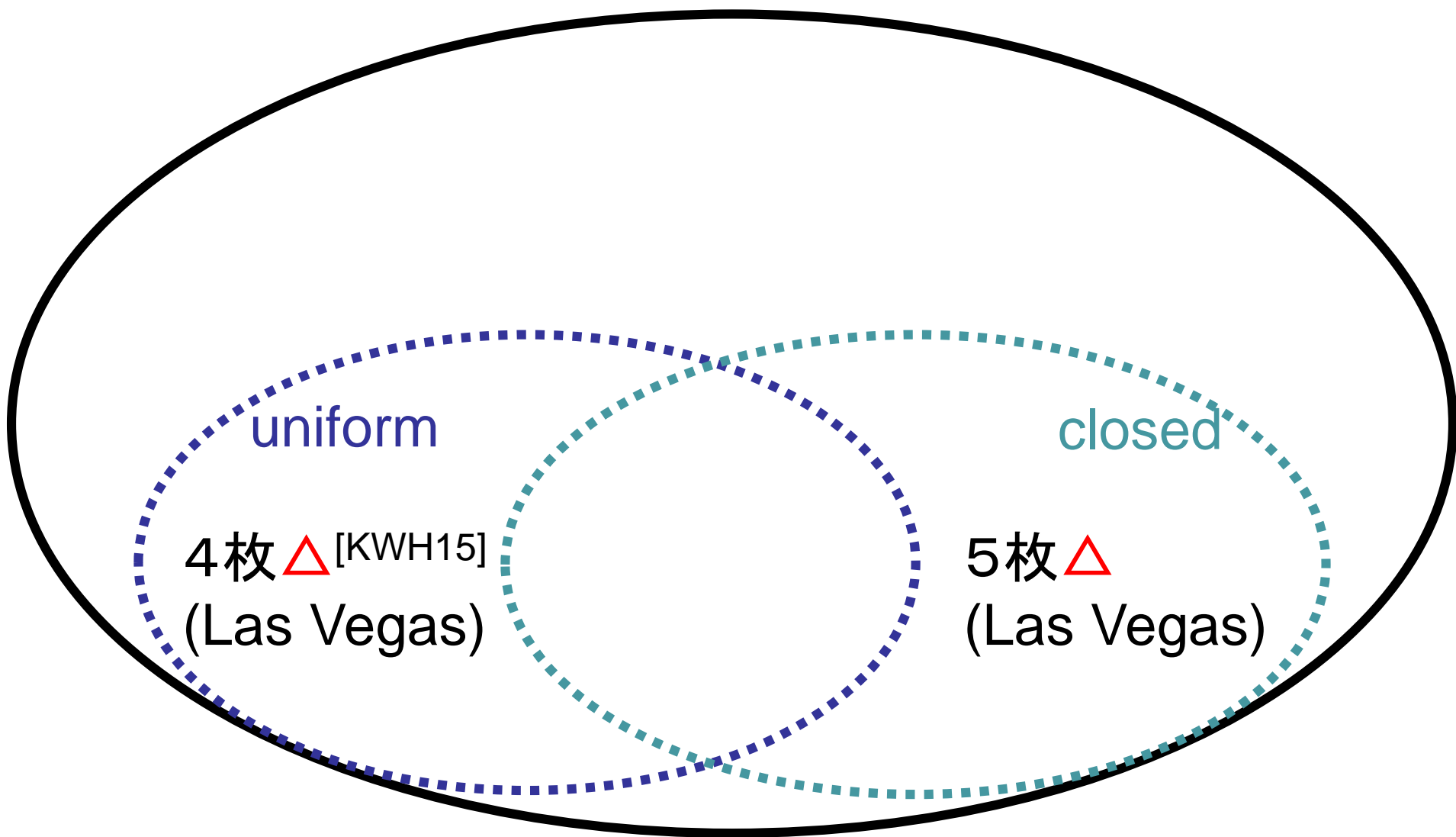
枚数	有限	Las Vegas
6	[MS09]	
5	✖ ※ (ours)	
4	✖ [KWH15]	✧ (ours)

※ closedのみでも不可能

具体的なプロトコルを発見できるか？

未解決問題

  = 0   = 1



下界に合うプロトコルは発見していない

目次

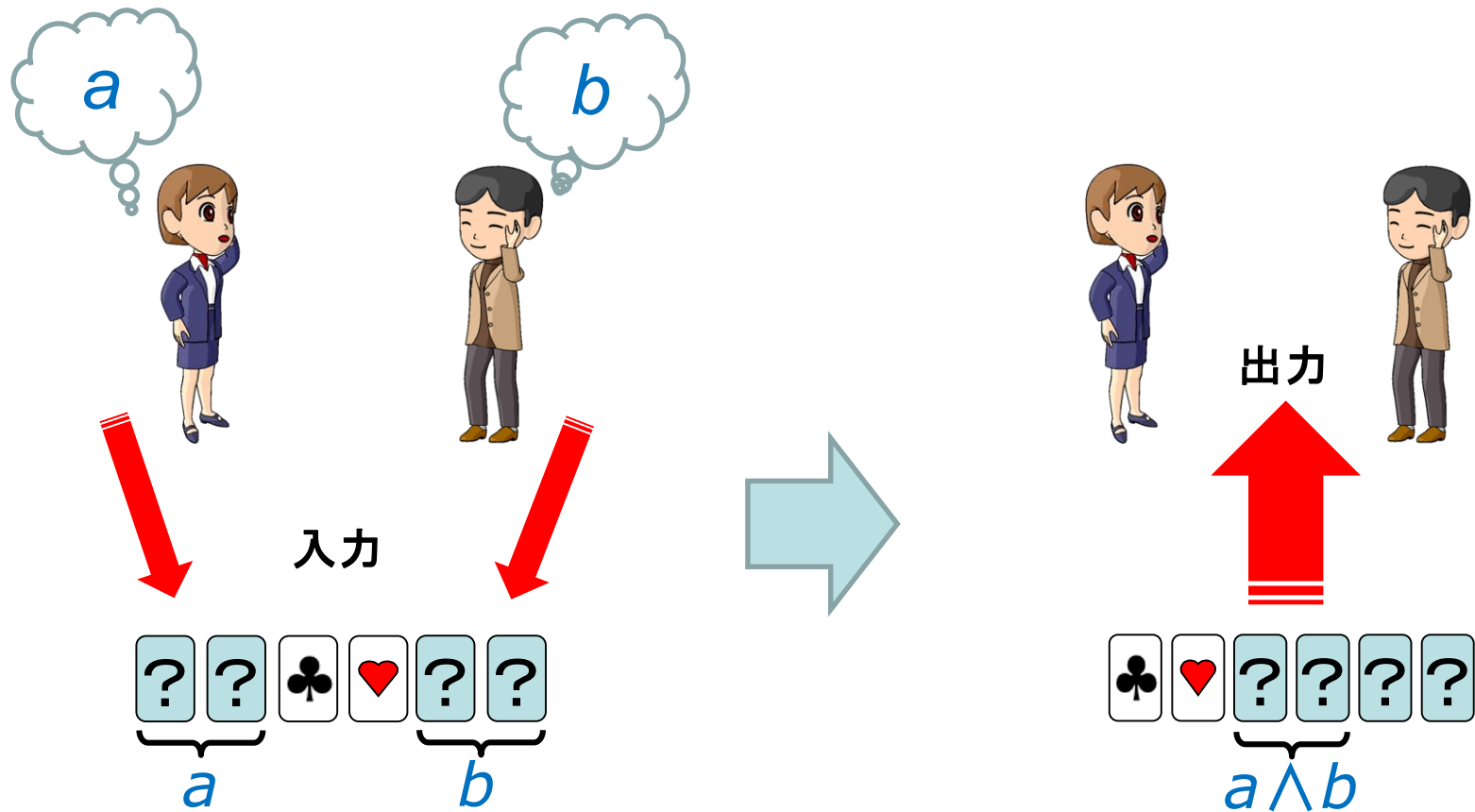
$$\begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} = 1$$

1. はじめに
2. ANDプロトコル
3. COPYプロトコル
4. 最新動向
5. むすび

[再掲] あらまし

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

- 例) 6-card コミット型ANDプロトコル^[MS09]



[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

任意の関数計算

$$\begin{array}{|c|c|} \hline \clubsuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \clubsuit \\ \hline \end{array} = 1$$

- ANDとNOTができるので、任意の論理関数をカードで秘密計算可能である...

- 例) 三変数多数決関数

$$\text{maj}(a, b, c) = (a \wedge b) \vee (b \wedge c) \vee (c \wedge a)$$

AND計算後は入力コミットメントが消滅

➡ コミットメントのコピーが必要

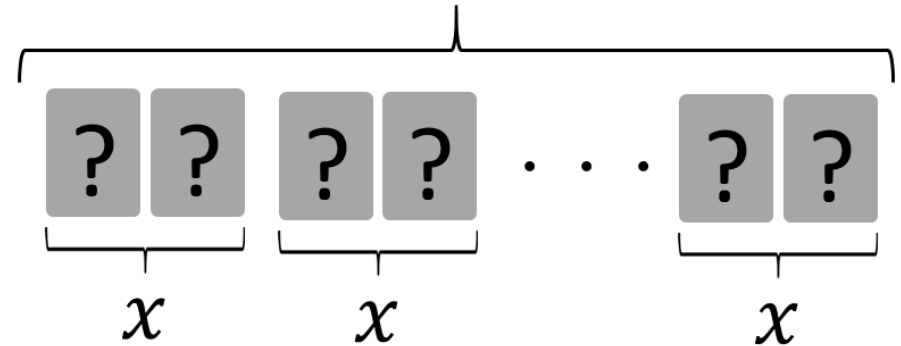
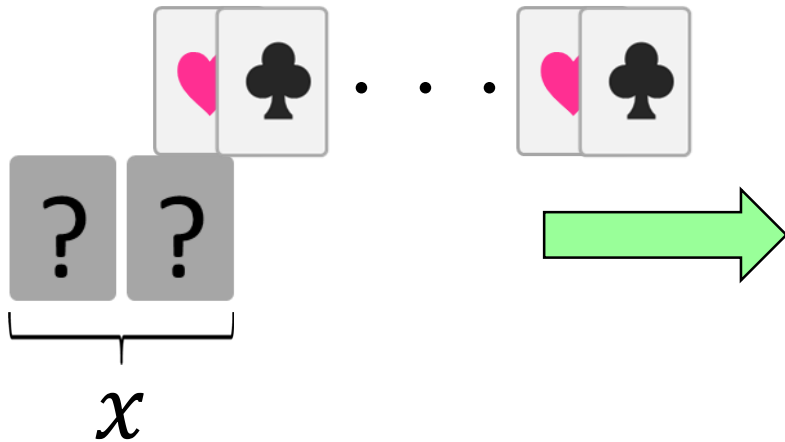
COPY protocols

$$\begin{array}{|c|c|} \hline \clubsuit & \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|c|} \hline \heartsuit & \clubsuit \\ \hline \end{array} = 1$$

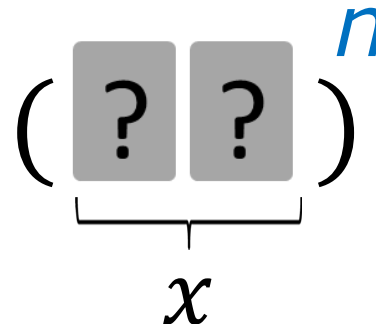
- ✓ Making $n (\geq 2)$ copied commitments from an input commitment.

At least $2n$ cards are necessary.

n commitments



- ✓ We sometimes write



The state-of-the-art COPY protocols

	# cards	Runtime
Mizuki-Sone [FAW09]	$2n+2$	Finite
Nishimura et al. [Soft Com.17]	$2n+1$	Las Vegas

Contribution

- ✓ We show lower bounds on the numbers of cards:
 - ✓ $2n+1$ cards are required for any COPY protocol;
 - ✓ $2n+2$ cards are necessary for finite-runtime.

These are optimal in terms of the number of required cards

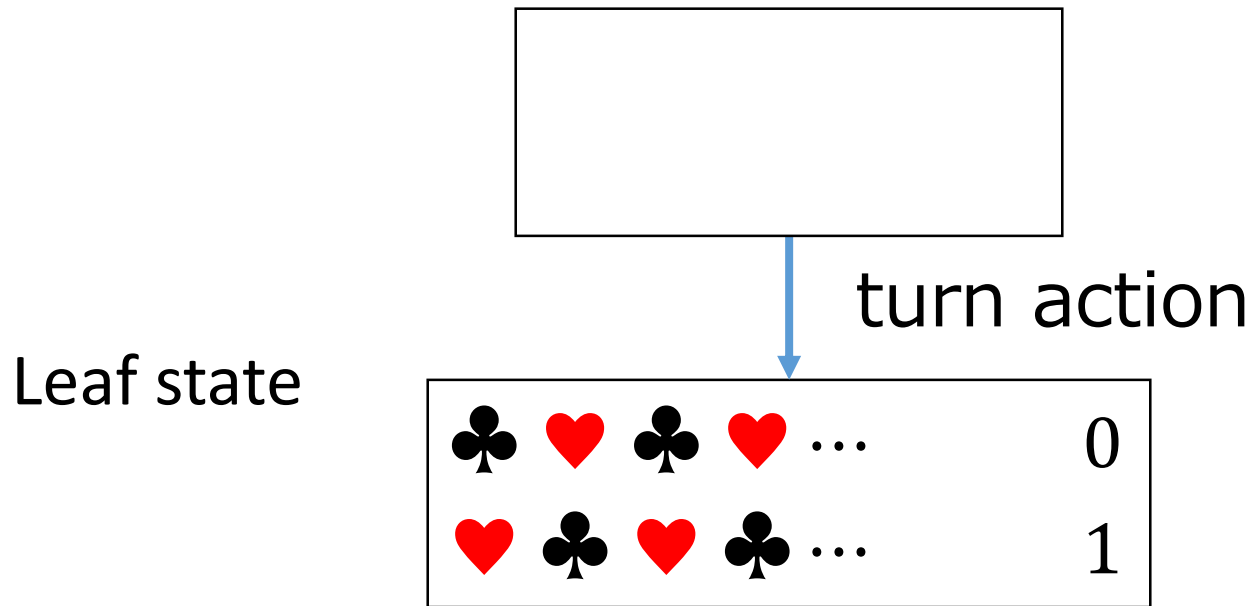
	# cards	Runtime
Mizuki-Sone ^[FAW09]	$2n+2$	Finite
Nishimura et al. ^[Soft Com.17]	$2n+1$	Las Vegas

Impossibility with $2n$ cards

$$\begin{matrix} \spadesuit & \heartsuit \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \end{matrix} = 1$$

✓ The proof outline:

✓ Assume the existence of COPY protocols with $2n$ cards,



Impossibility with $2n$ cards = 0 = 1









✓ The proof outline:

✓ Assume the existence of COPY protocols with $2n$ cards,

Both the turned cards must be the same color, a contradiction.

Leaf state

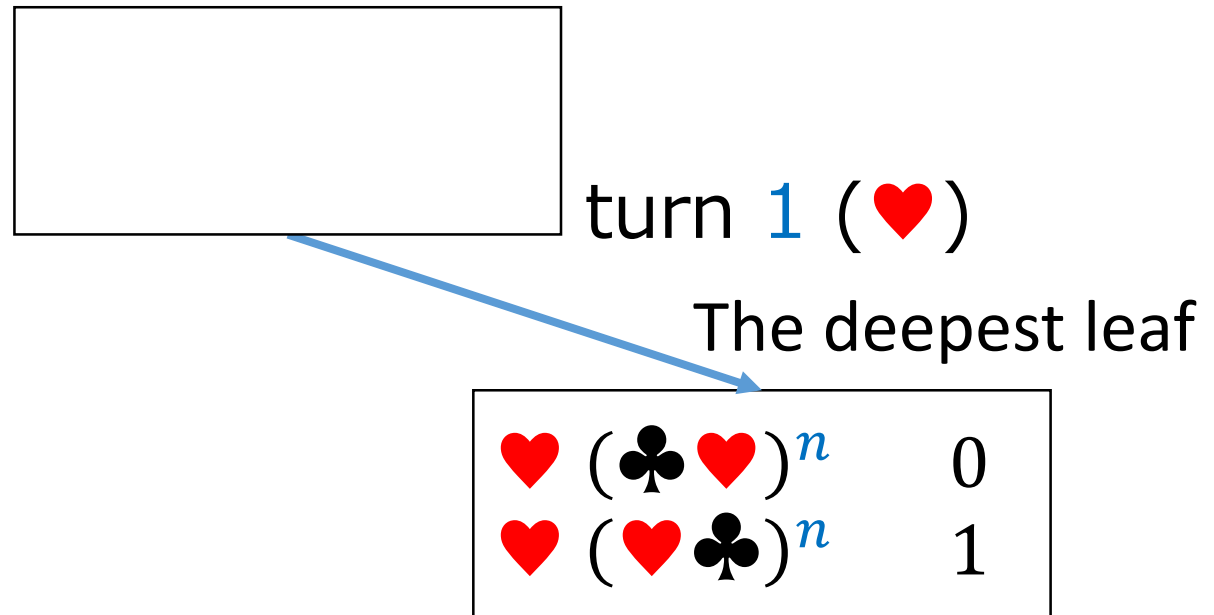
turn action

				...	0
				...	1

Impossibility with $2n+1$ cards for finite

✓The proof outline:

- ✓Assume the existence of finite COPY with $\clubsuit^n, \heartsuit^{n+1}$.
- ✓There must be the deepest leaf.

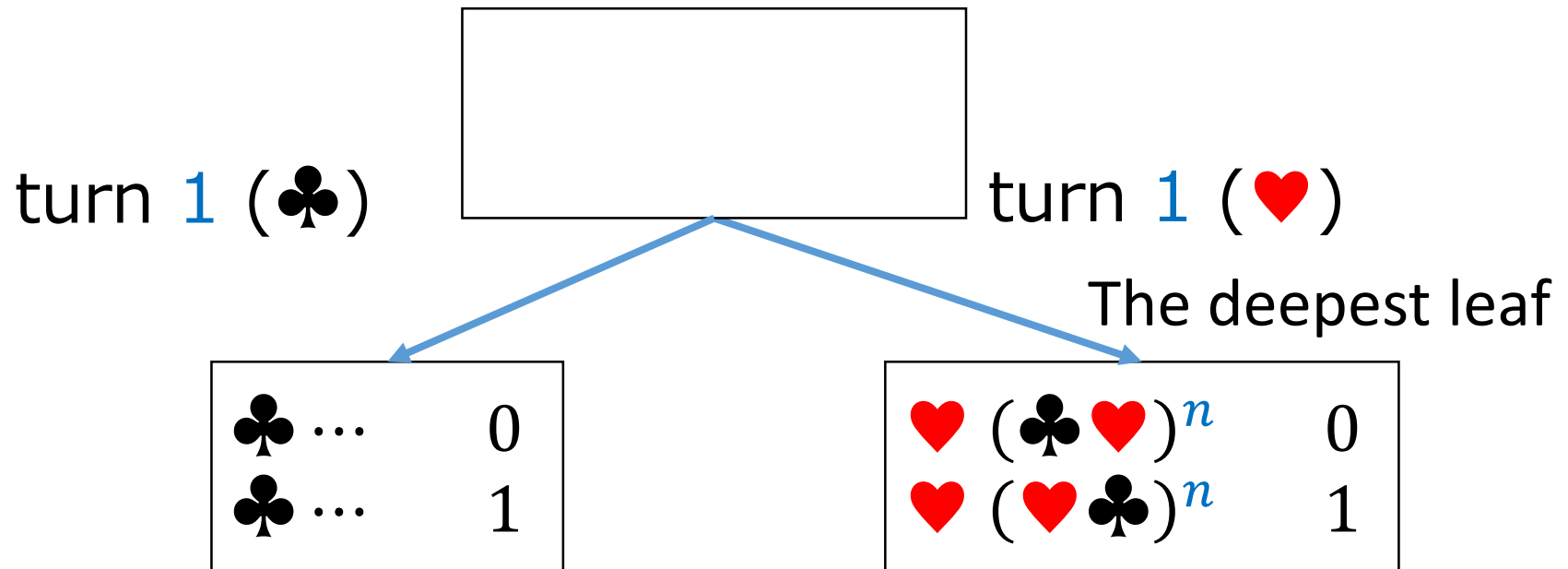


Impossibility with $2n+1$ cards for finite

✓The proof outline:

✓Assume the existence of finite COPY with $\clubsuit^n, \heartsuit^{n+1}$.

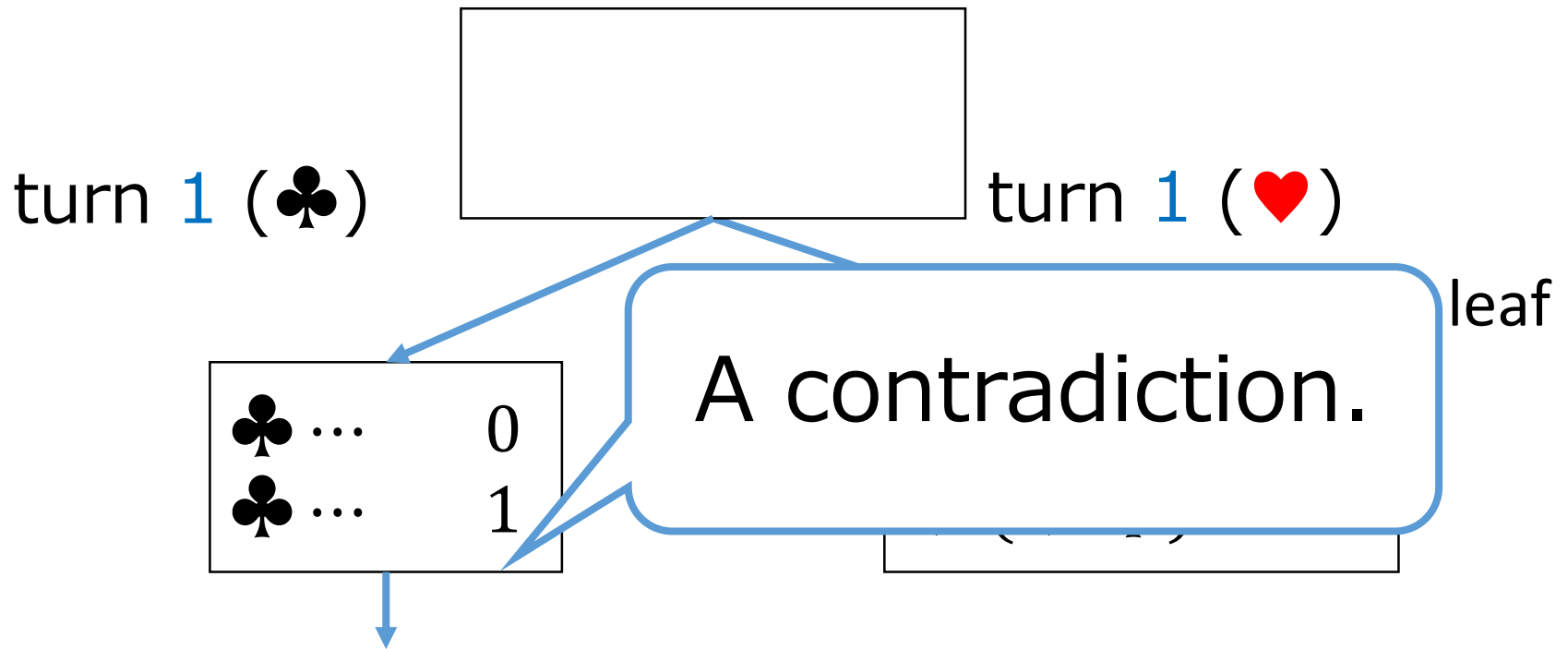
✓There must be the deepest leaf.



Impossibility with $2n+1$ cards for finite

✓The proof outline:

- ✓Assume the existence of finite COPY with $\clubsuit^n, \heartsuit^{n+1}$.
- ✓There must be the deepest leaf.



✓Because we cannot construct n commitments with \clubsuit^{n-1} and \heartsuit^{n+1} , there should be a deeper leaf.

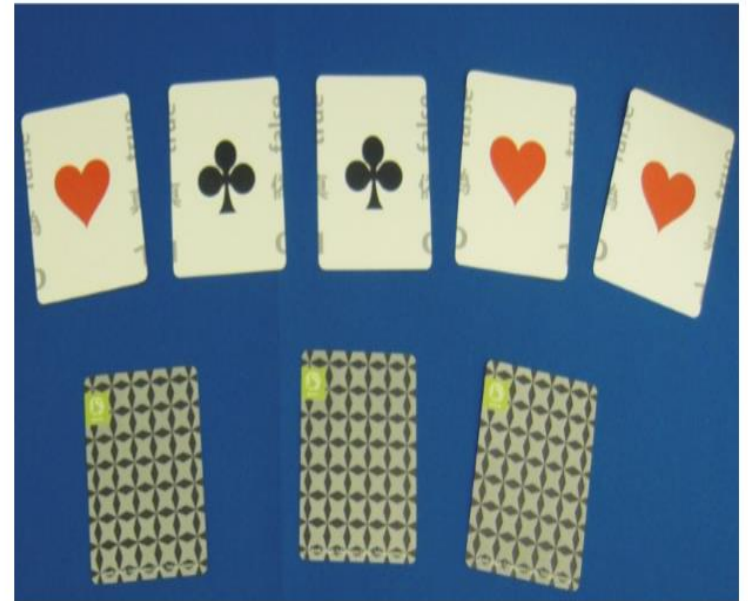
Summary (COPY protocols)

✓ We showed:

- ✓ $2n+1$ cards are required for any COPY protocol;
- ✓ $2n+2$ cards are necessary for finite-runtime.

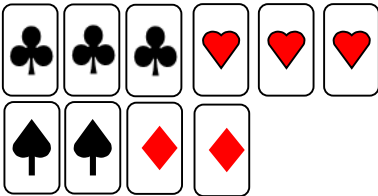
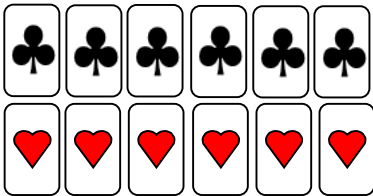

Thank you for your attention!

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



コミット型AND計算

$$\begin{matrix} \spadesuit & \heartsuit \\ \hline \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \\ \hline \end{matrix} = 1$$

	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 	6
Niemi-Renvall [TCS, 1998]	12 	2.5
Stiglic [TCS, 2001]	8 	2

もっと改良できないだろうか？

AND計算の本質を考えると...

基本原理

♣

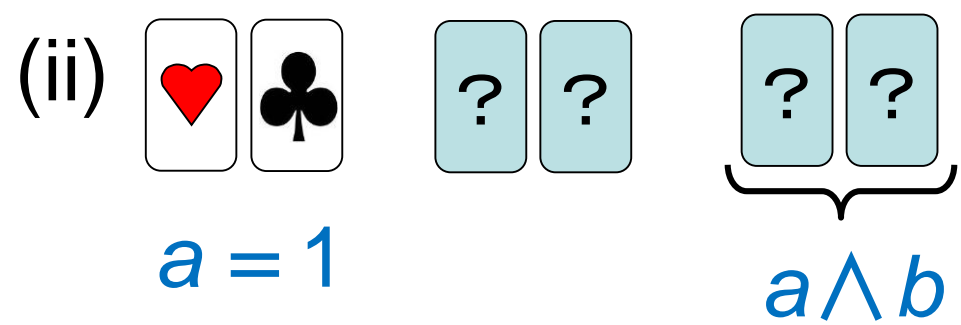
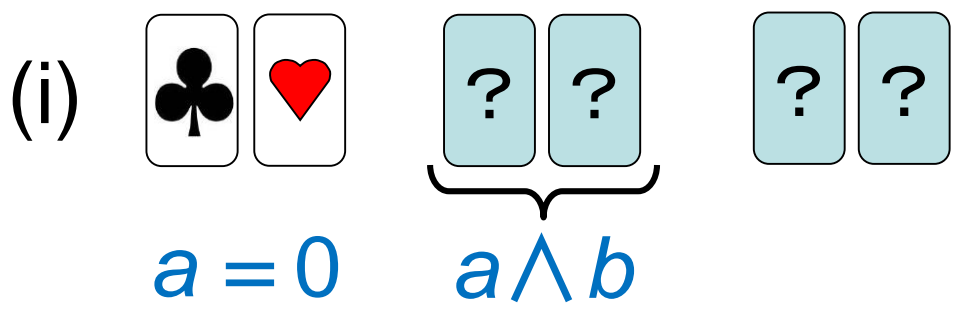
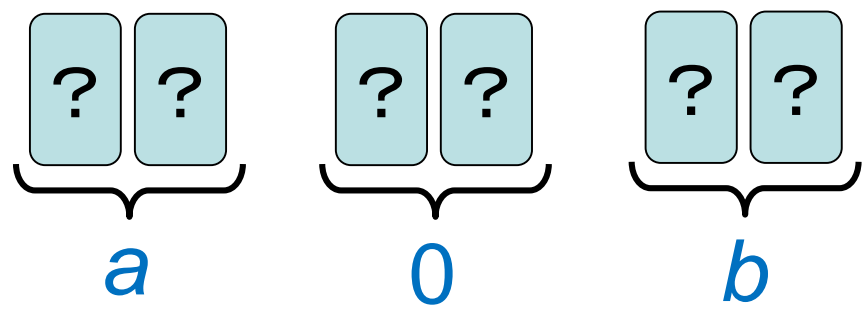
♥

= 0

♥





♣

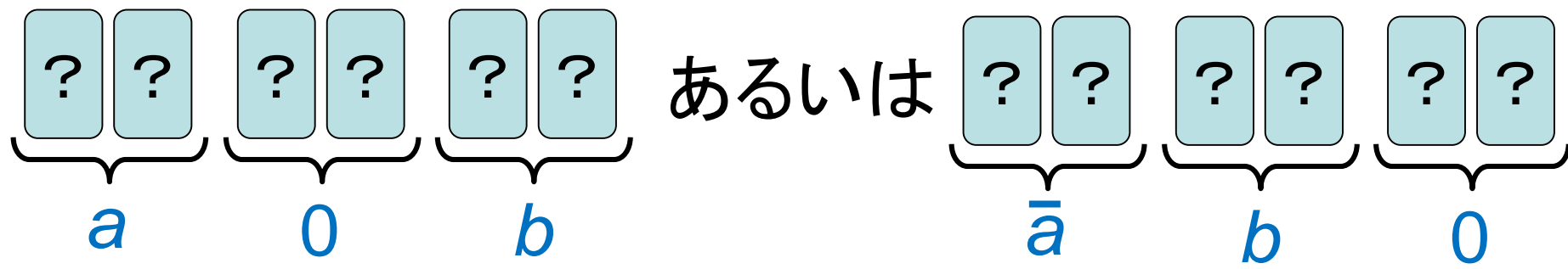
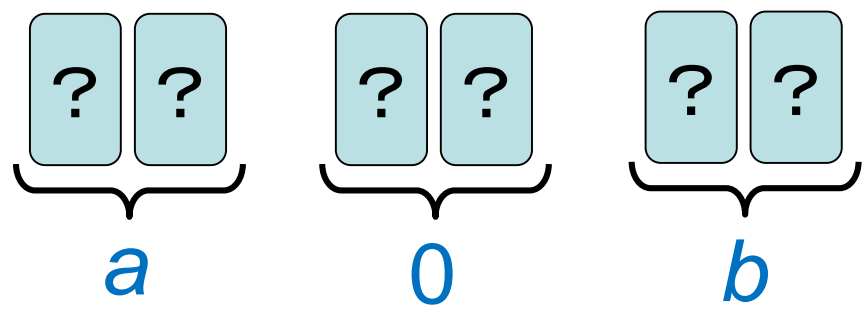
= 1



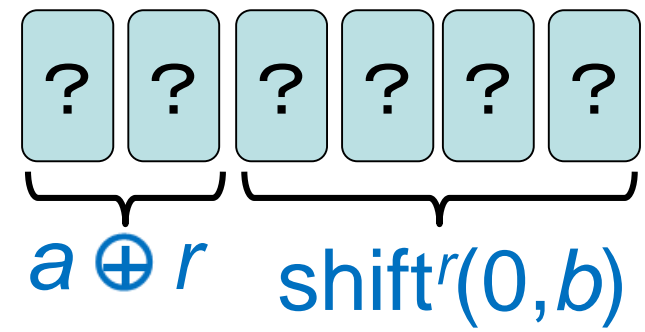
このままだと a の値が漏れるので、ランダム化する

基本原理(2)





  = 0   = 1

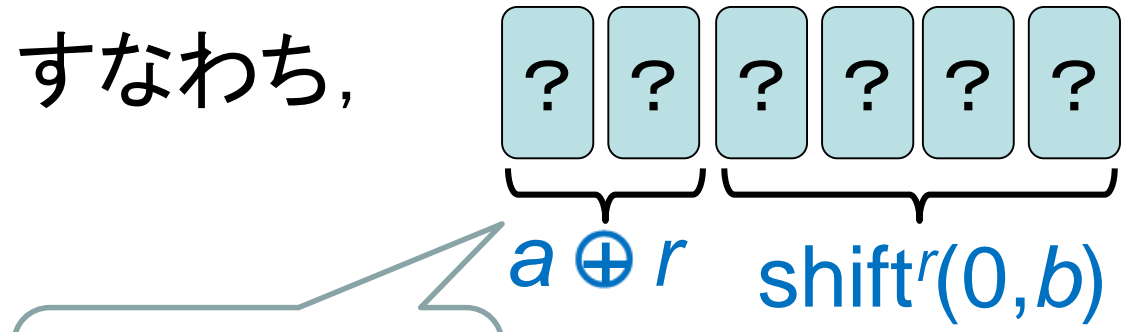
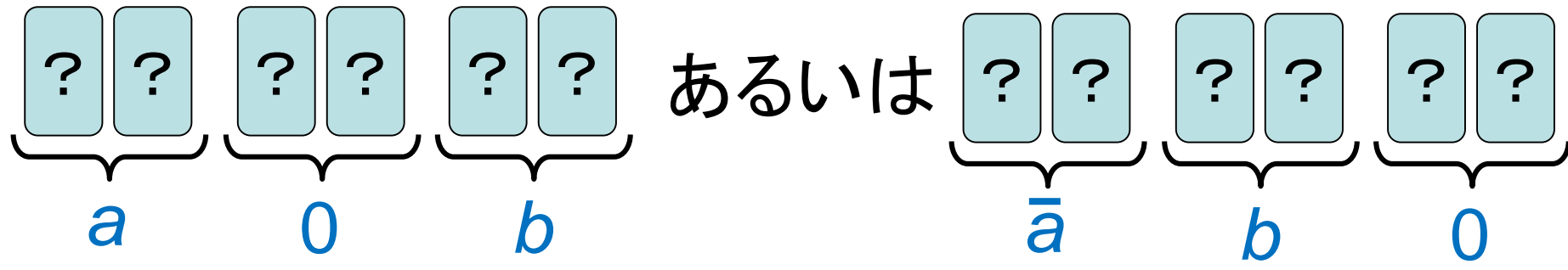


すなわち,

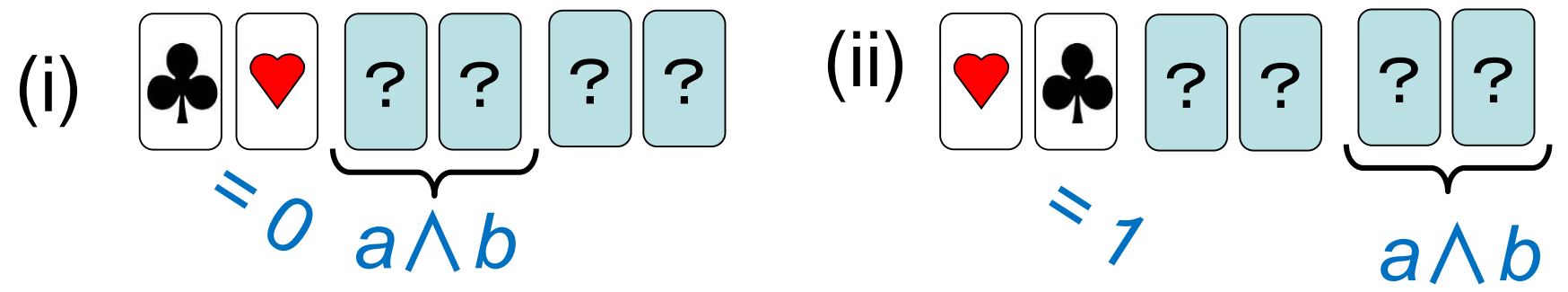


基本原理(3)

  = 0   = 1



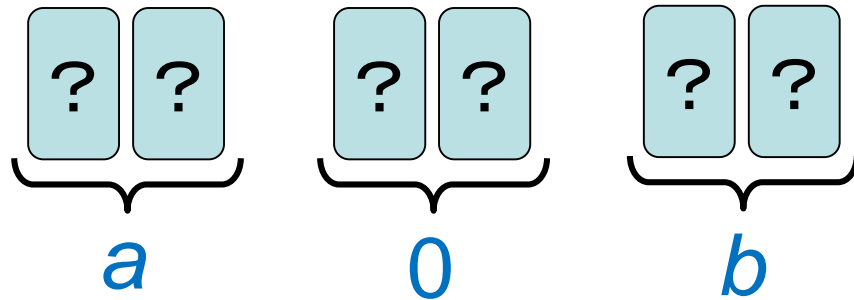
先頭の2枚をめぐっても大丈夫



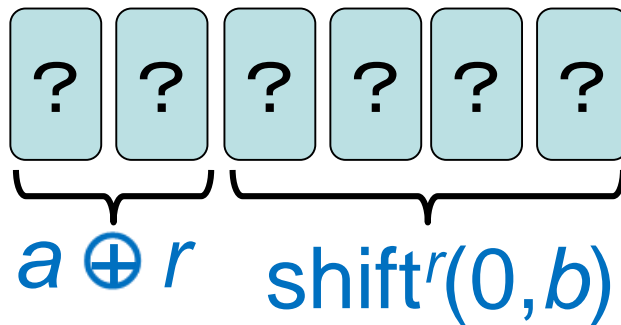
基本原理(4)

$$\begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \spadesuit \\ \hline \end{array} = 1$$

結局,



から



を作り出せばよいな。

→ ランダム二等分割カットという新しい
シャッフルを思い付く