

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

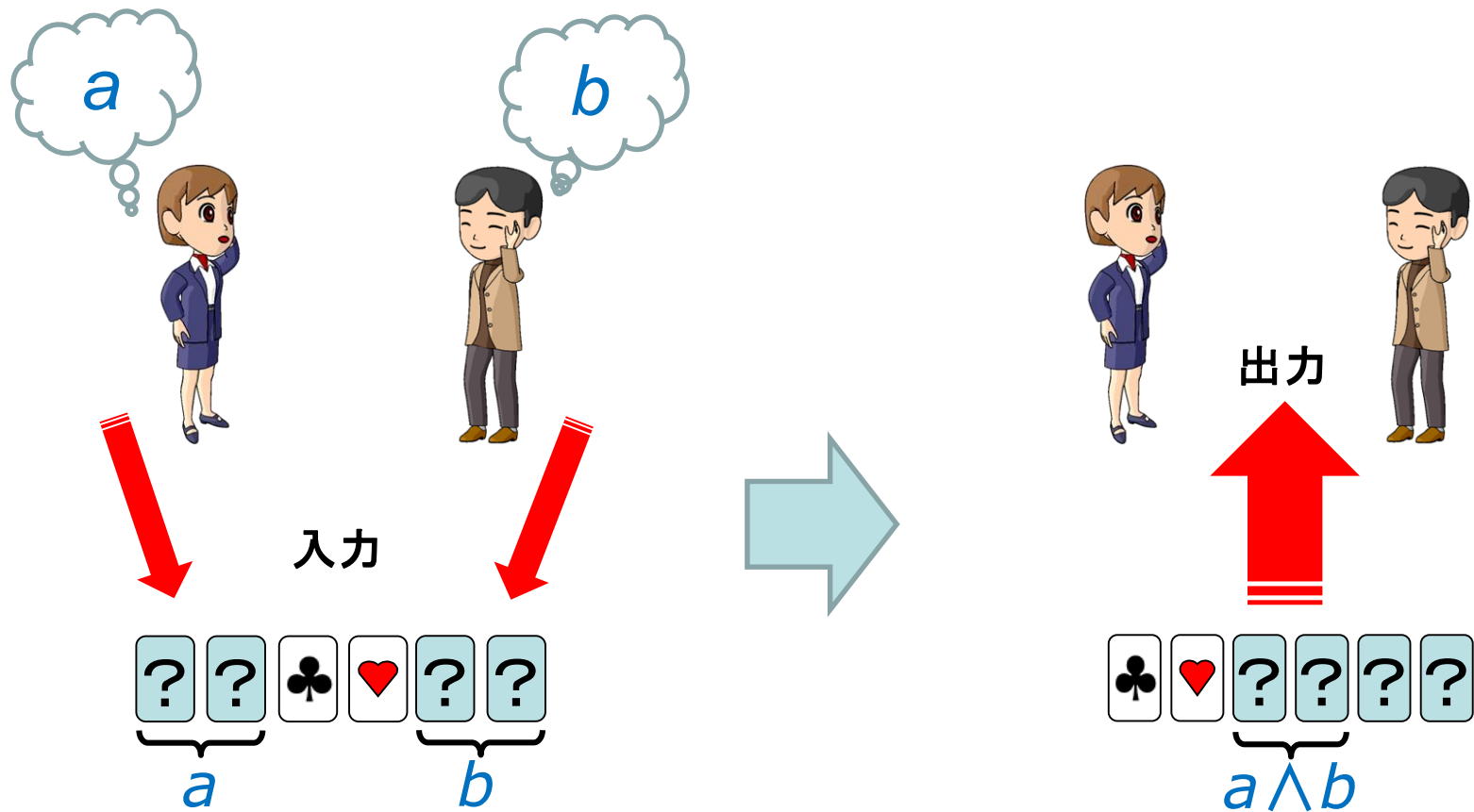
	R - track	I - track
	Cryptographic Protocols (Khoa Nguyen)	Foundations (Tatsuaki Okamoto)
9:00-9:25	Two-Round PAKE from Approximate SPH and Instantiations from Lattices; <i>Jiang Zhang, Yu Yu</i>	Succinct Spooky Free Compilers Are Not Black Box Sound; <i>Zvika Brakerski, Yael Tauman Kalai, Renen Perlman</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 Kobayashi, Paburinnayak, 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

 = 0  = 1

- 例) 6枚のカードを用いるANDプロトコル^[MS09]

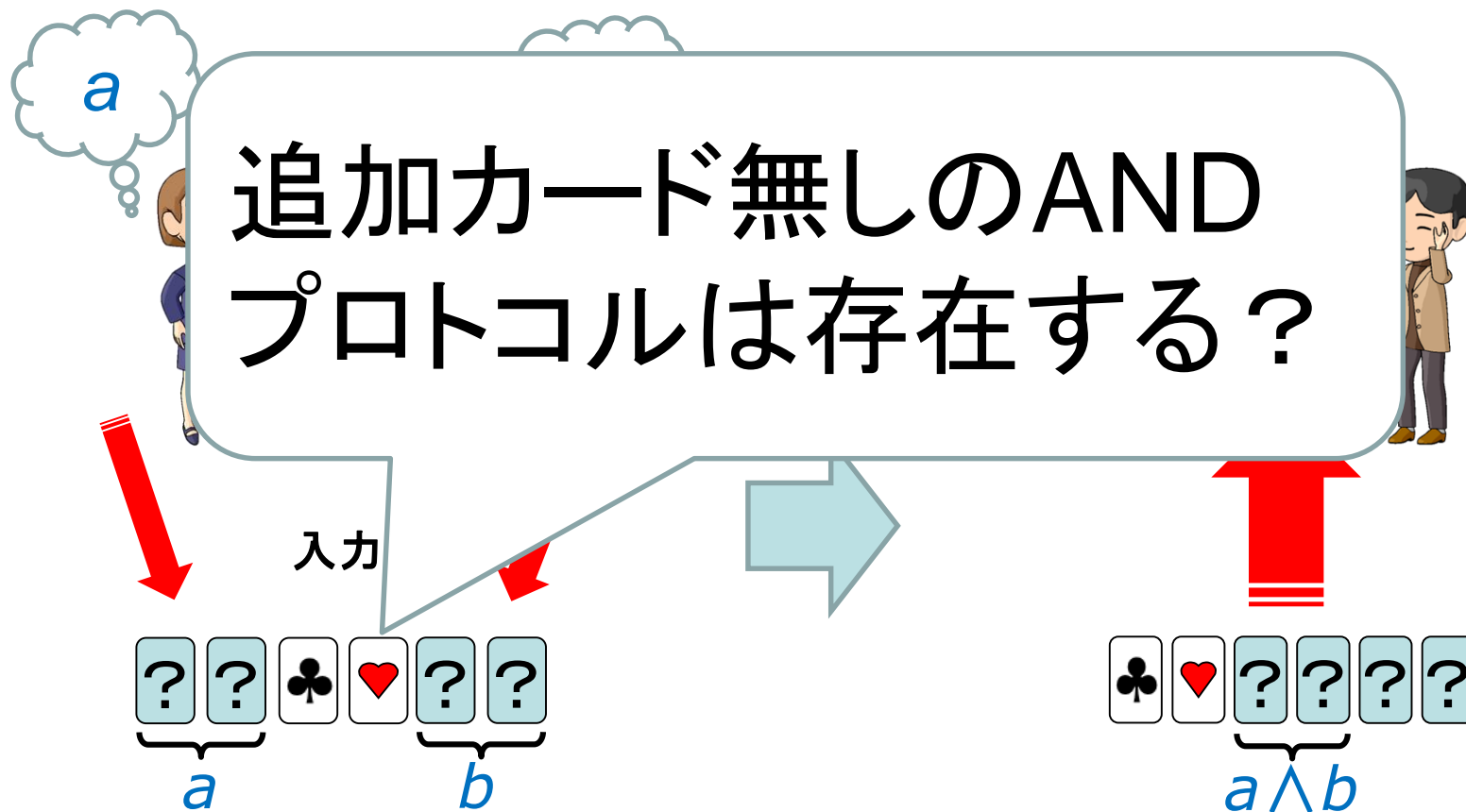


[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

あらまし



- 例) 6枚のカードを用いるANDプロトコル^[MS09]

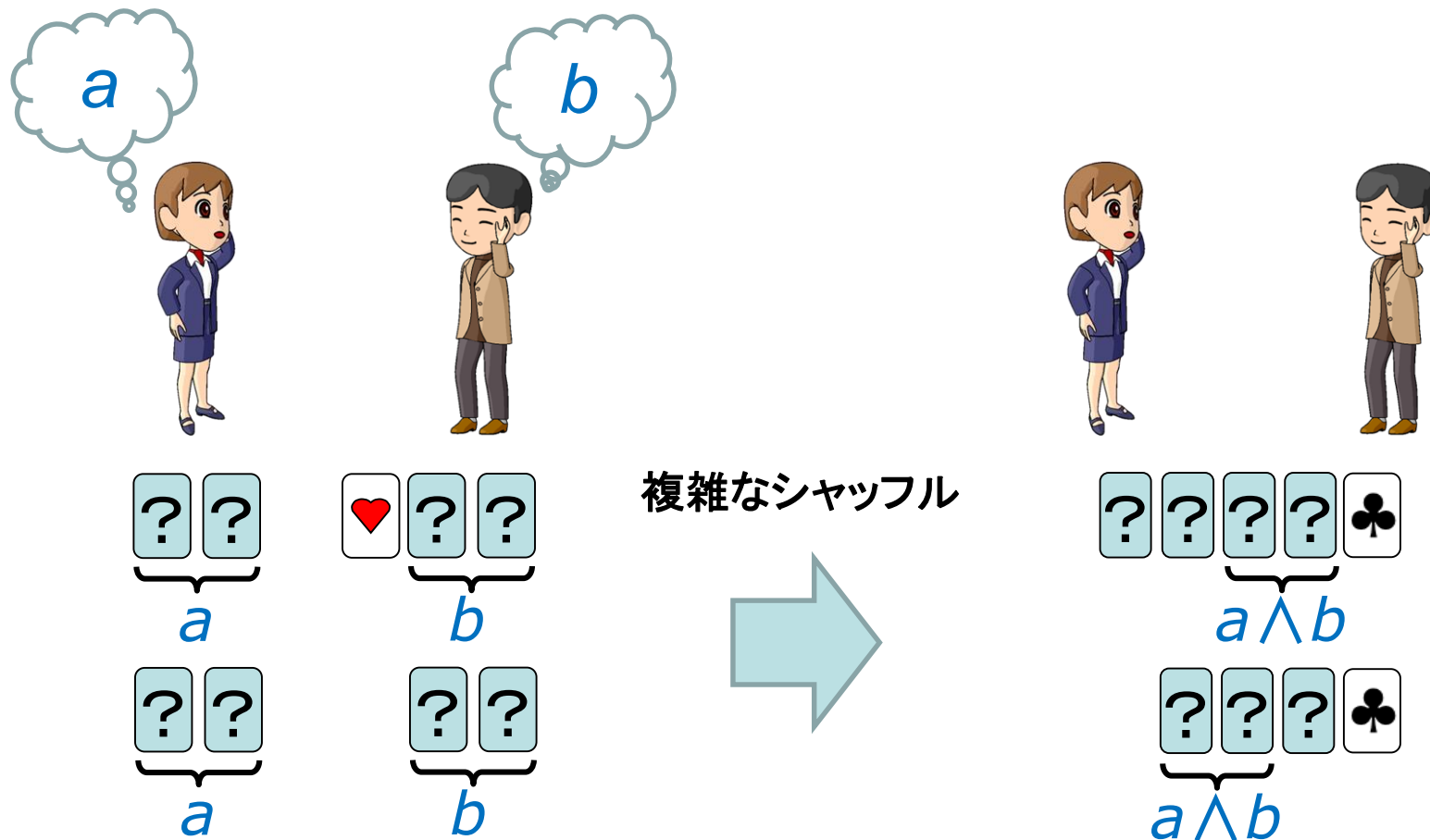


[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009, LNCS 5598, pp. 358–369, 2009.

あらまし

 = 0  = 1

- 4, 5枚のカードを用いるAND プロトコル^[KWH15]

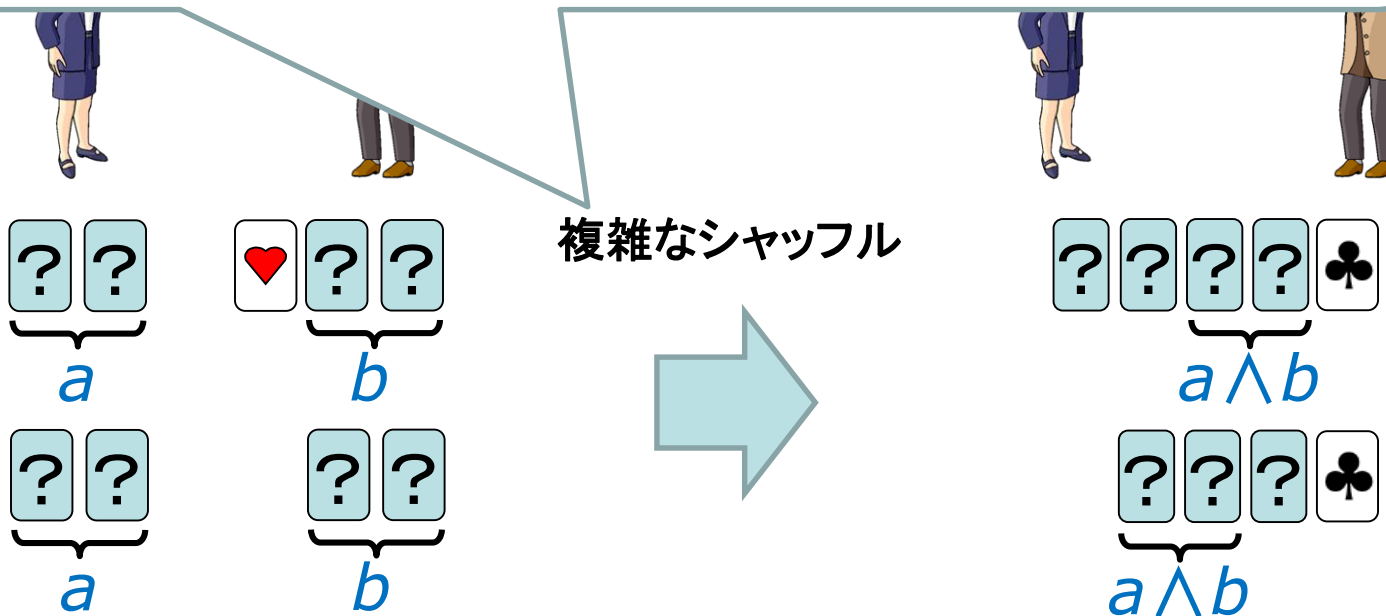


[KWH15] Koch, A., Walzer, S., Härtel, K., "Card-based cryptographic protocols using a minimal number of cards." ASIACRYPT 2015, LNCS, pp. 783–807.

あらまし

 = 0  = 1

簡単なシャッフルのみのAND
プロトコルは存在する？

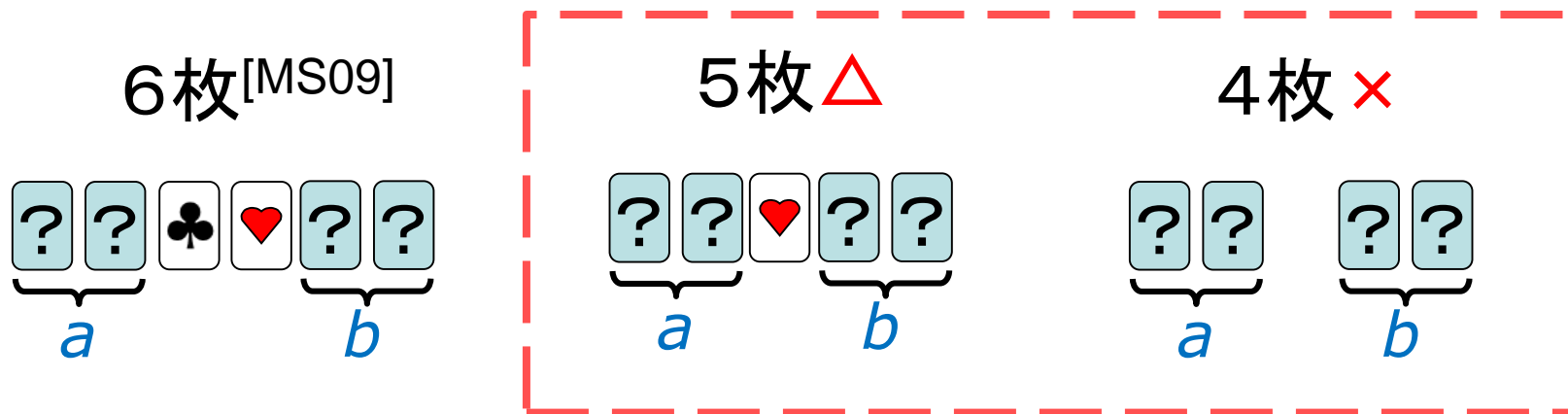


[KWH15] Koch, A., Walzer, S., Härtel, K., "Card-based cryptographic protocols using a minimal number of cards." ASIACRYPT 2015, LNCS, pp. 783–807.

あらまし



- “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...)



Δ : 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

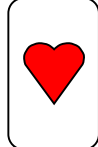
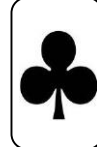
$$\begin{matrix} \spadesuit & \heartsuit \\ \hline \end{matrix} = 0 \quad \begin{matrix} \heartsuit & \spadesuit \\ \hline \end{matrix} = 1$$

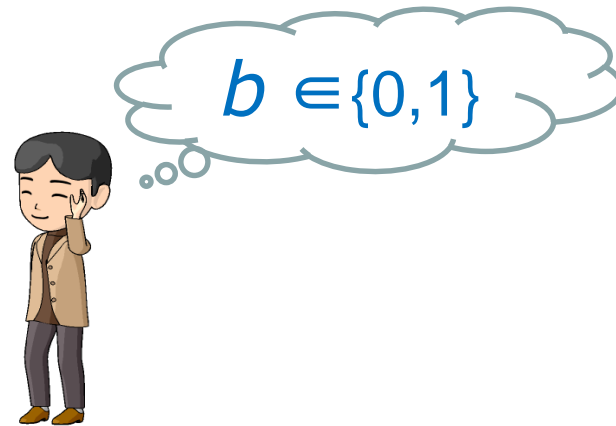
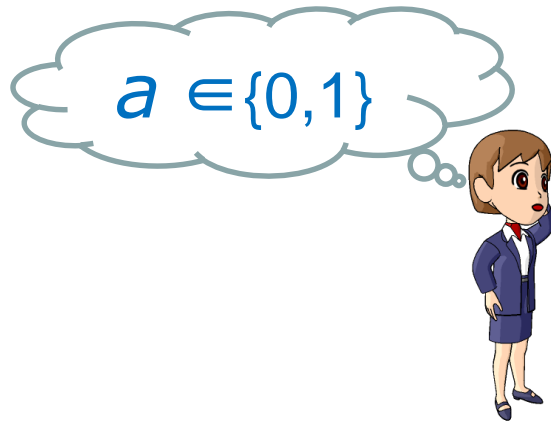
1. はじめに
2. ANDプロトコル
3. COPYプロトコル
4. 最新動向
5. むすび

  = 0   = 1

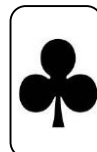
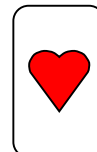
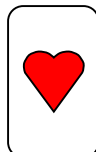
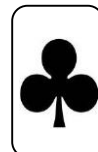
ビットを扱うために、次の符号化を固定する:

  = 0

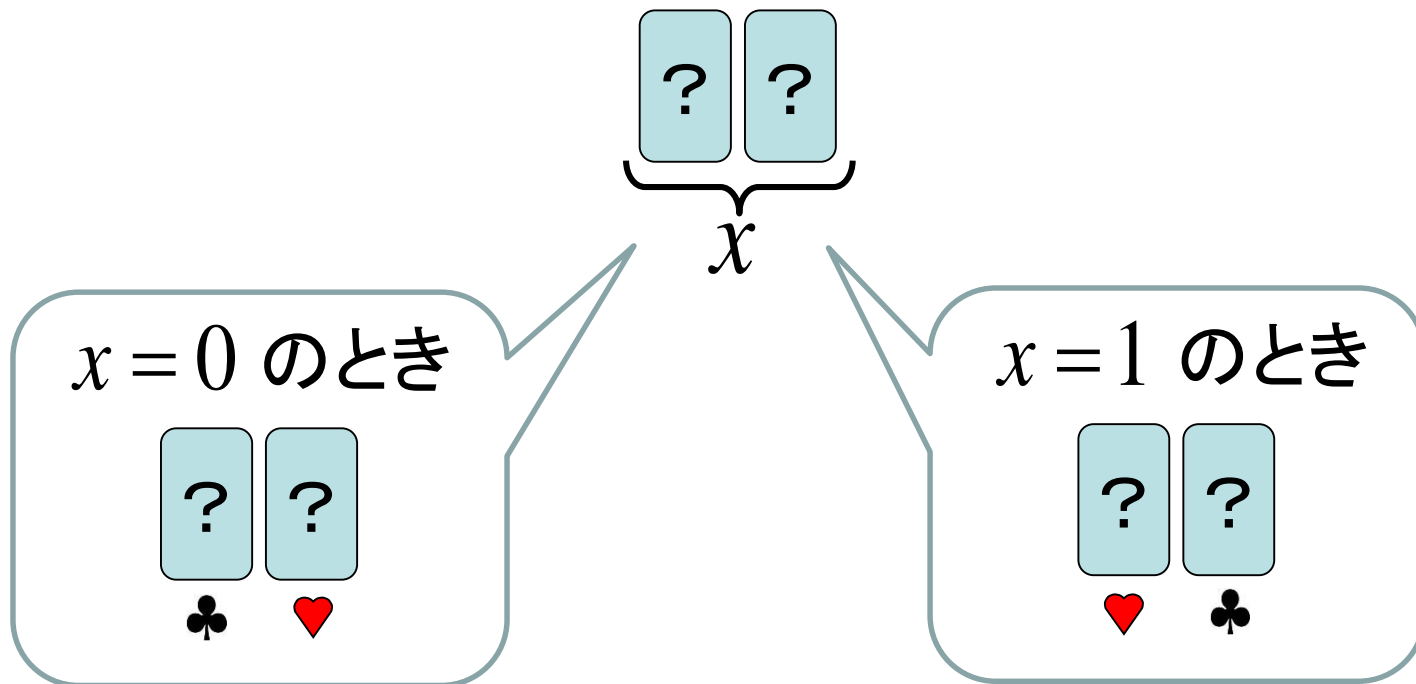
  = 1



  = 0   = 1

  = 0   = 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:

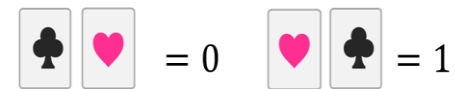


目次

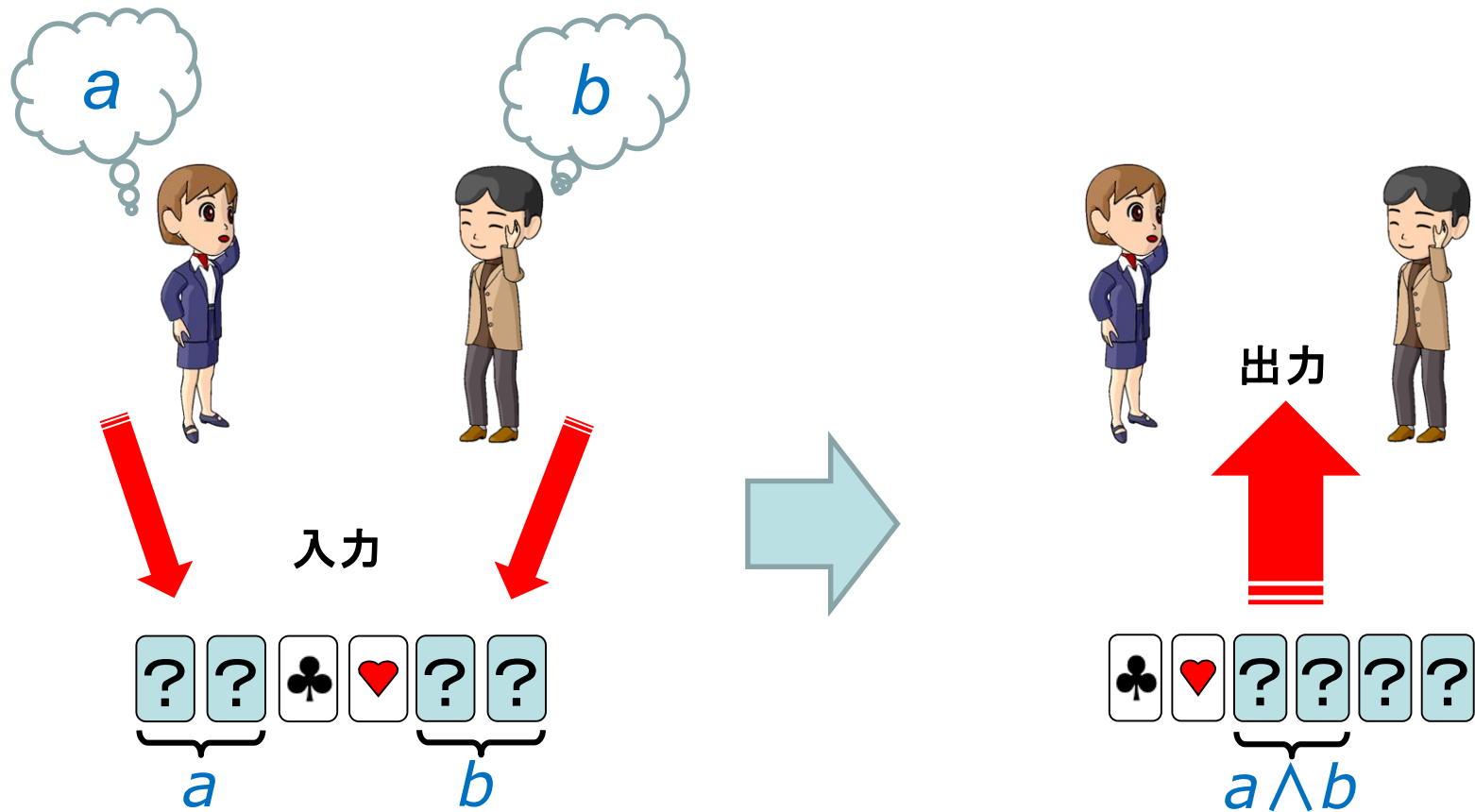
$$\begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} = 0 \quad \begin{array}{|c|} \hline \heartsuit \\ \hline \end{array} \begin{array}{|c|} \hline \clubsuit \\ \hline \end{array} = 1$$

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



- 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



[CK93]

[NR98]

[Sti01]

[MS09]

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

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]

2001年までのAND計算プロトコル:



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



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]

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

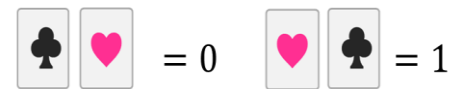
[KWH15]

2.4. 簡単なシャッフル [KKWM+17]

[CK93]
[NR98]
[Sti01]

[MS09]

[KWH15] を紹介する前に...

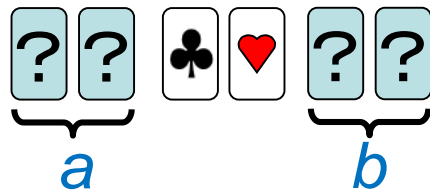


- シャッフル操作を定式化^[MS14]
 - [KWH15] は複雑なシャッフルを必要とするので、その紹介のために必要
 - “簡単”なシャッフルと“複雑”なシャッフルの区分のために必要

[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

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



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

$$\left(\begin{array}{c} ? \\ \hline \clubsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \clubsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \clubsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array} \right)$$

並び替える



(perm, (2 4 3))

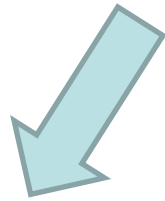
$$\left(\begin{array}{c} ? \\ \hline \clubsuit \end{array}, \begin{array}{c} ? \\ \hline \clubsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \clubsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array} \right)$$

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

$$\left(\begin{array}{cccccc} ? & ? & ? & ? & ? & ? \\ \hline \spadesuit & \spadesuit & \heartsuit & \heartsuit & \spadesuit & \heartsuit \end{array} \right)$$

シャッフル

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



$$\left(\begin{array}{cccccc} ? & ? & ? & ? & ? & ? \\ \hline \spadesuit & \spadesuit & \heartsuit & \heartsuit & \spadesuit & \heartsuit \end{array} \right)$$

$$\left(\begin{array}{cccccc} ? & ? & ? & ? & ? & ? \\ \hline \heartsuit & \spadesuit & \heartsuit & \spadesuit & \spadesuit & \heartsuit \end{array} \right)$$

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

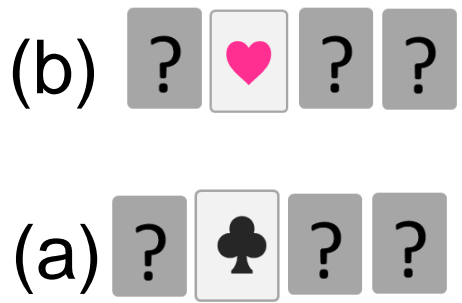
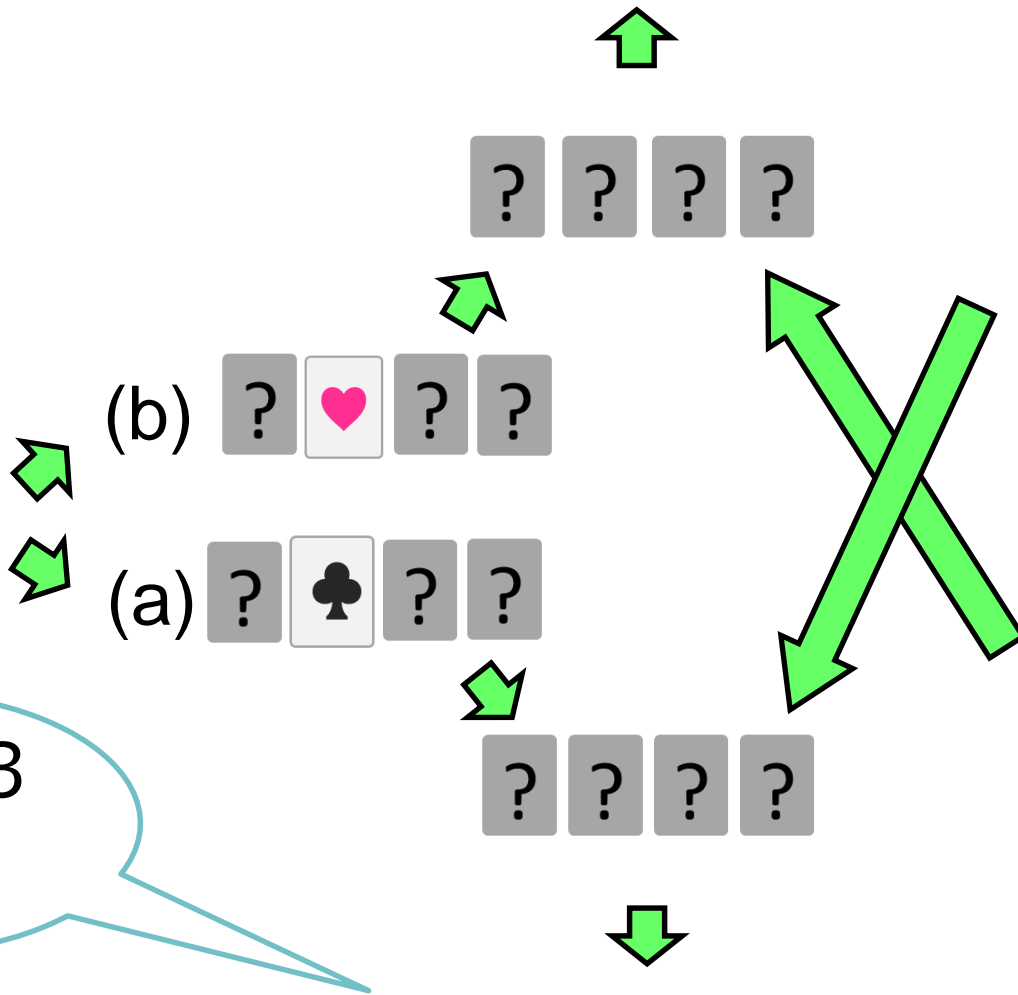
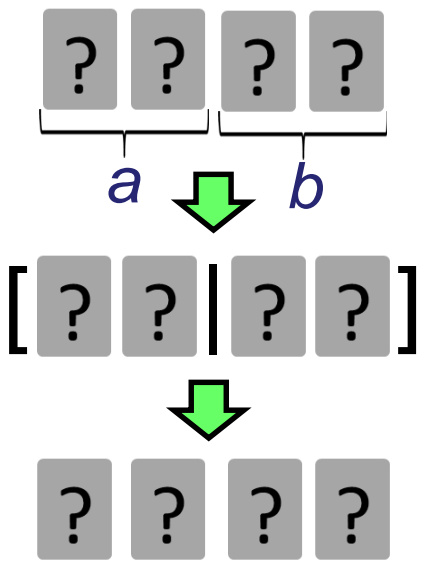
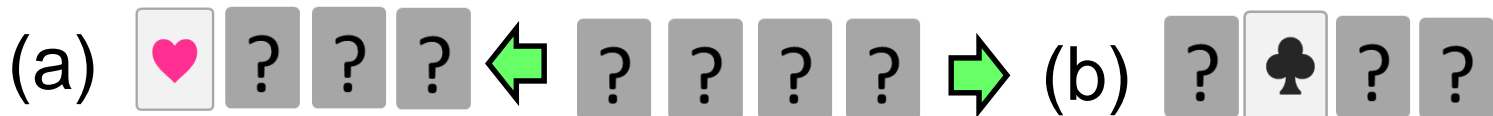
2.4. 簡単なシャッフル [KKWM+17]

[CK93]
[NR98]
[Sti01]

[MS09]

4-card KWH (詳細略)

= 0 = 1



確率 1/3
で終了



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

$$\left(\begin{array}{c} ? \\ \hline \spadesuit \end{array}, \begin{array}{c} ? \\ \hline \spadesuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array} \right)$$

KWH プロトコルに必要なシャッフル(1)

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



$$\left(\begin{array}{c} ? \\ \hline \spadesuit \end{array}, \begin{array}{c} ? \\ \hline \spadesuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array} \right)$$

$$\left(\begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \heartsuit \end{array}, \begin{array}{c} ? \\ \hline \spadesuit \end{array}, \begin{array}{c} ? \\ \hline \spadesuit \end{array} \right)$$

つまり、不均一な(確率分布の)シャッフル

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

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

KWH プロトコルに必要なシャッフル(2)

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



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

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

つまり、置換集合が群を成していない

(shuf, Π , \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 $\langle \text{?} \text{?} \text{?} \text{?} \text{?} \rangle$

$\spadesuit \heartsuit = 0$ $\heartsuit \spadesuit = 1$



uniform-closed だと簡単に手で実装できる(と信じている)
30

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]

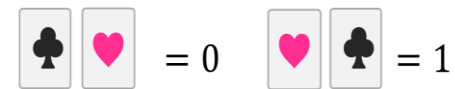
uniform

closed

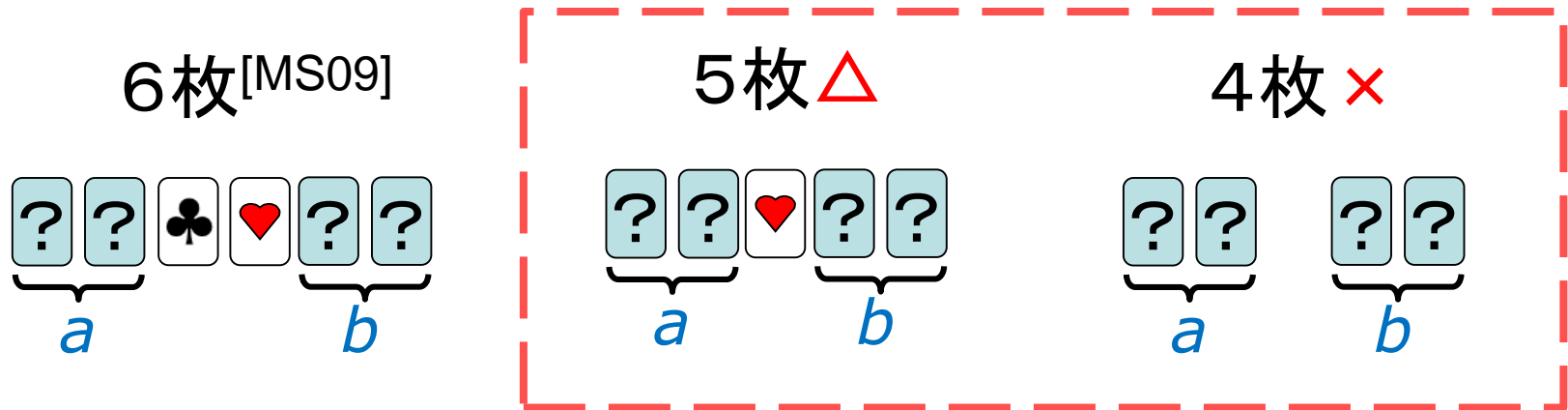
[CK93]
[NR98]
[Sti01]
[MS09]

4-card KWH

[再掲] あらまし



- “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...)



Δ : 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

uniform

4枚 ×
(存在しない)

closed

5枚 △
(Las Vegas)

※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



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

$$\spadesuit \heartsuit = 0 \quad \heartsuit \spadesuit = 1$$

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

uniform-closedのみを用いたAND

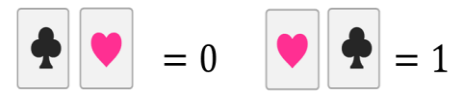
$$\spadesuit \heartsuit = 0 \quad \heartsuit \spadesuit = 1$$

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]



① \mathcal{F} が均一 (uniform) である

② Π が群を成している (closed)

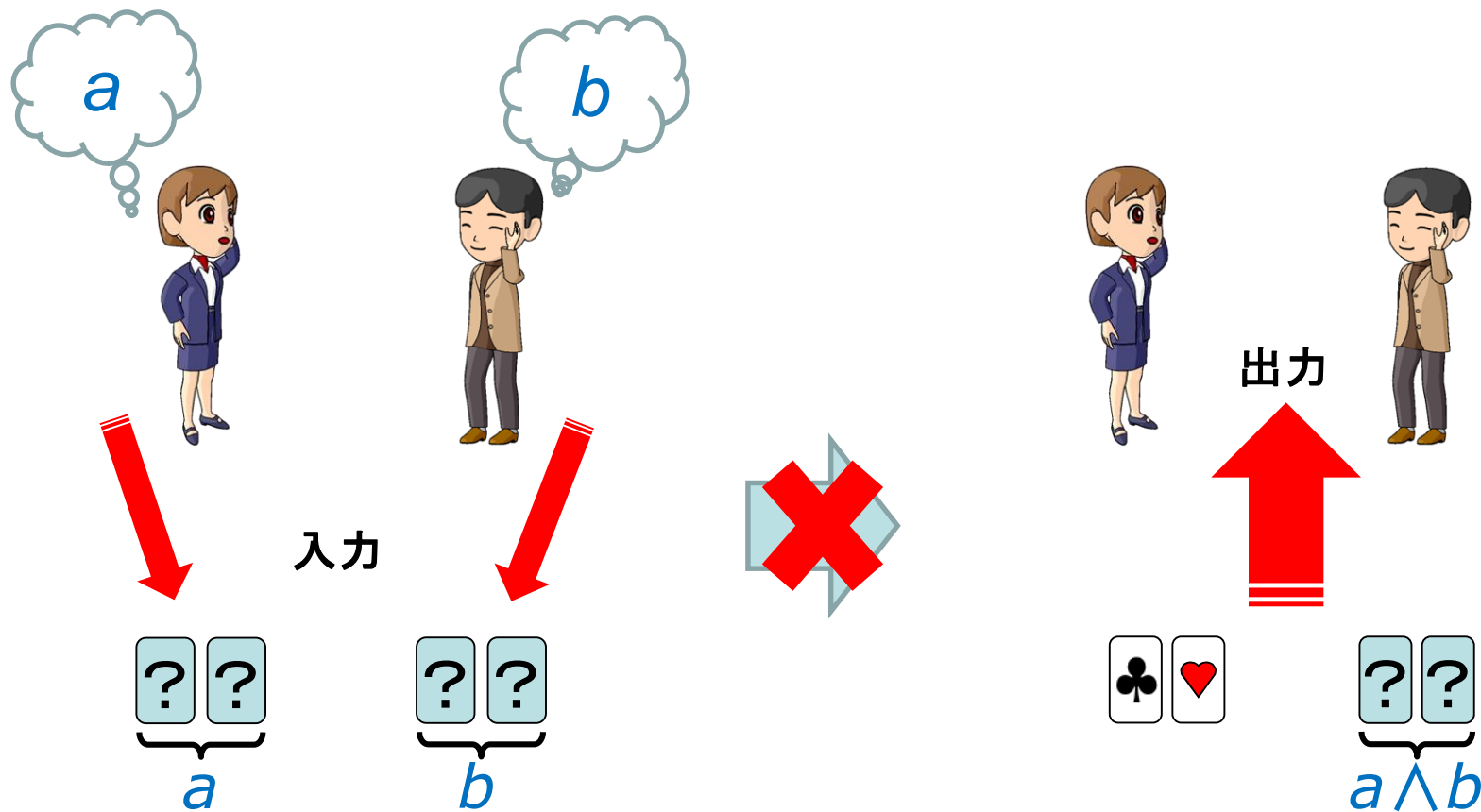
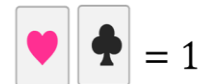
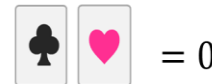
• ランダムカットは① ② を満たす





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

• 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

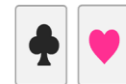


定理: uniform-closed (uc) シヤッフル   = 0   = 1
のみを用いた4枚ANDは存在しない

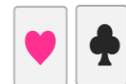
(1) stateの定義

- 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

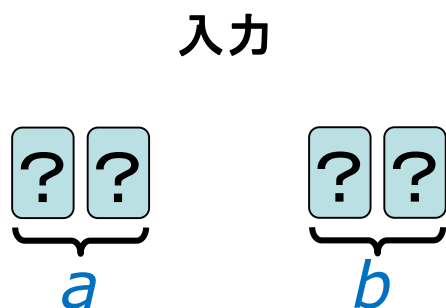


= 1

(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}

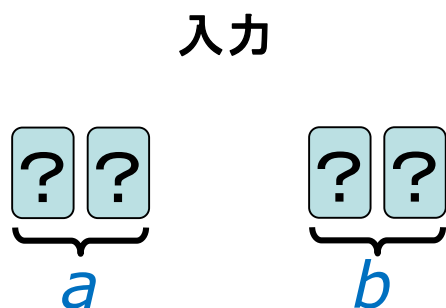
定理: uniform-closed (uc) シヤッフルのみを用いた4枚ANDは存在しない



(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}

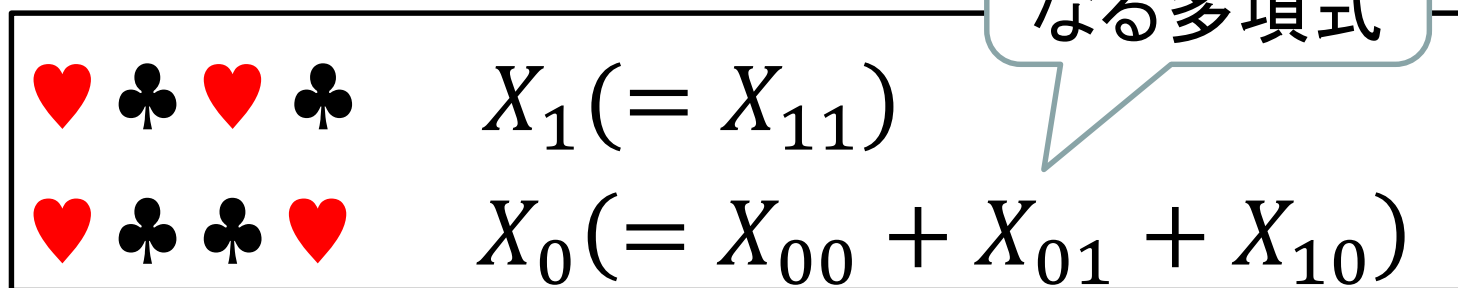
定理: uniform-closed (uc) シヤッフルのみを用いた4枚ANDは存在しない



(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

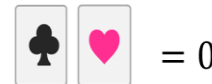
例) 4-card ANDのfinal state



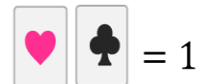
出力が0になる多項式



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) 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)

   	$X_1 (= X_{11})$
   	$X_0 (= X_{00} + X_{01} + X_{10})$



出力

















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



(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) シヤツフル
のみを用いた4枚ANDは存在しない



(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

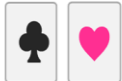
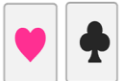


(2) bad/final stateの定義

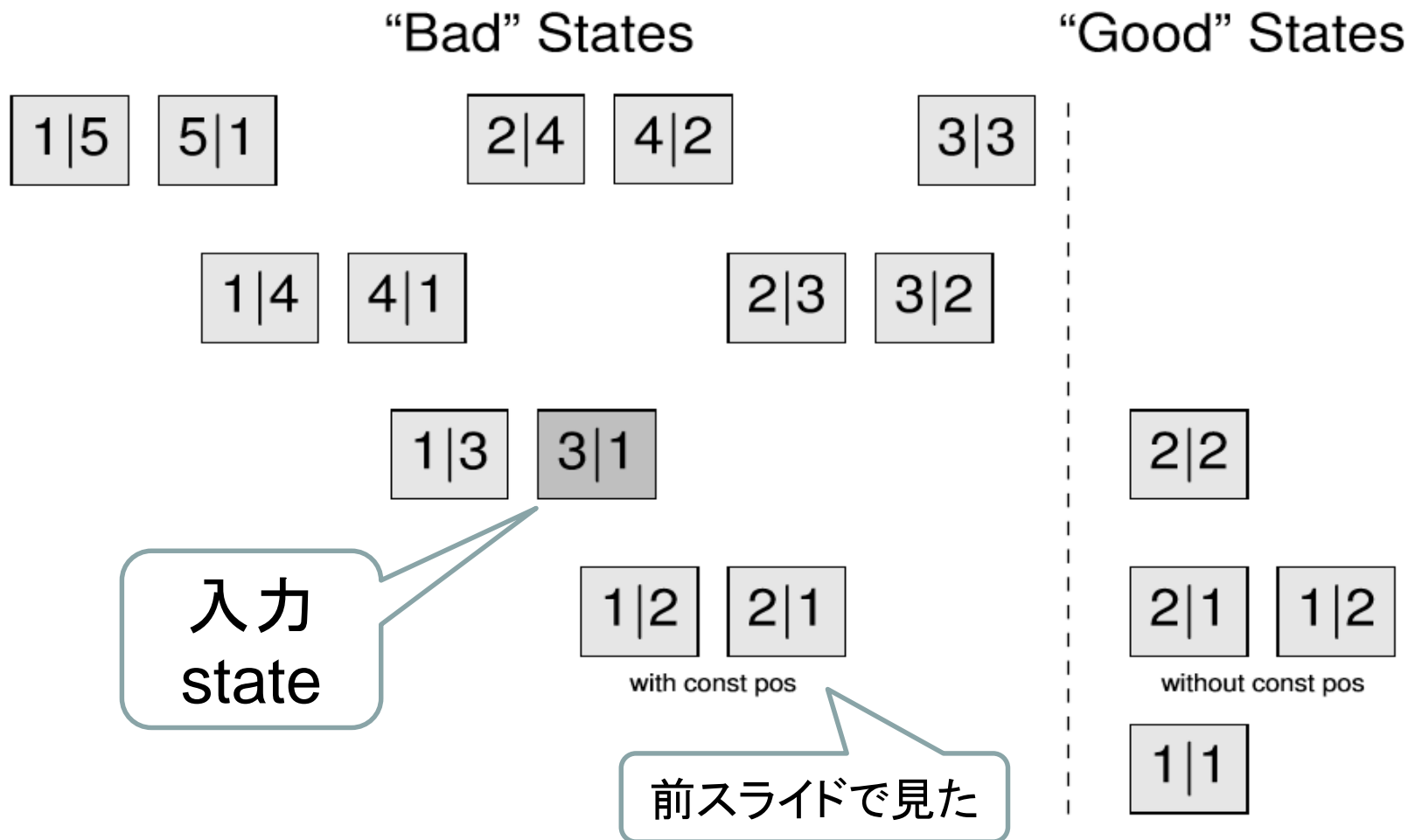
- **bad state** : コミットメントを出力できない
- **final state** : コミットメントを出力できる

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) シヤツフル  = 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 [KWH15]より



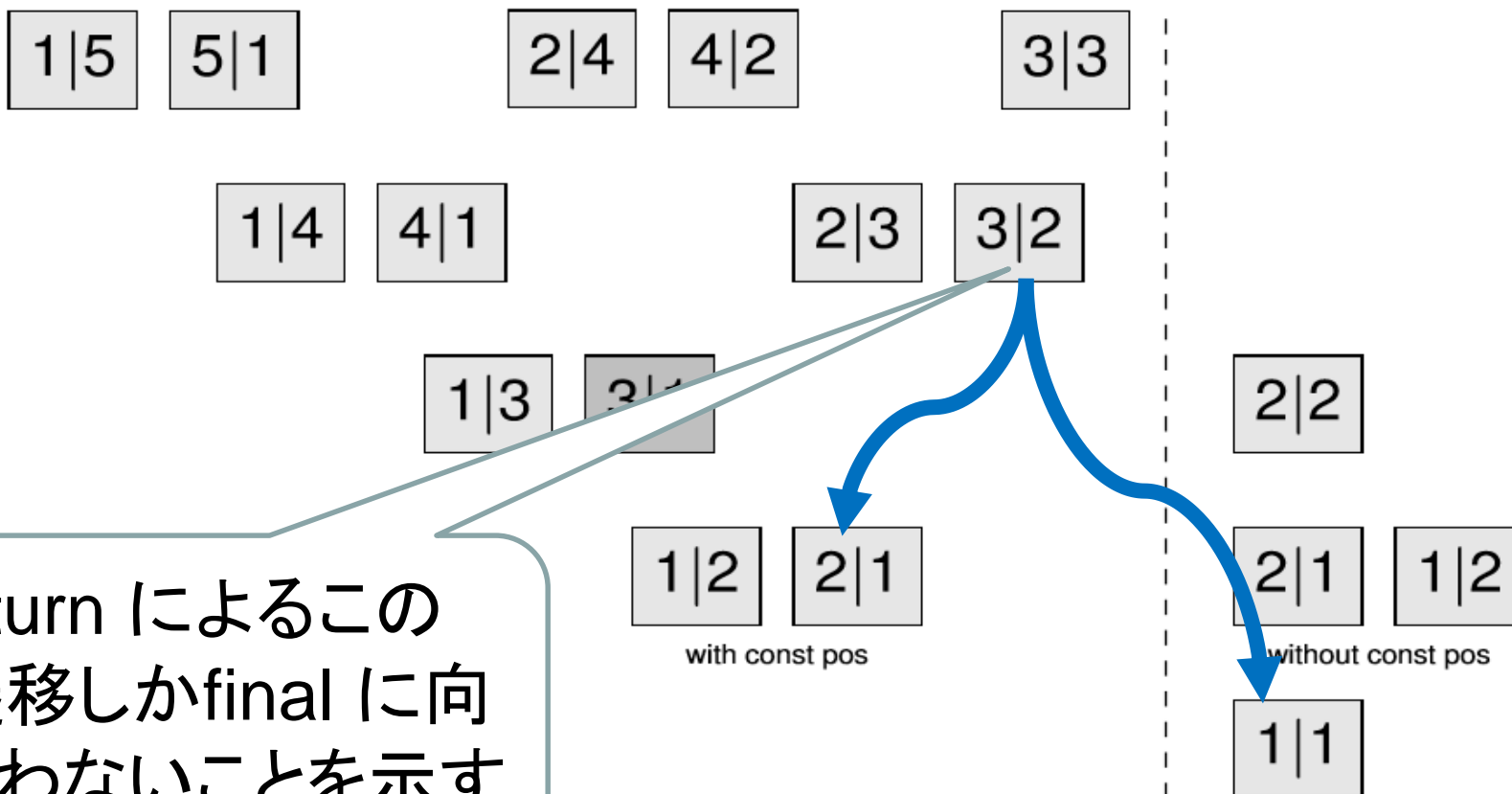
定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない

  = 0   = 1

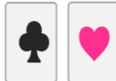
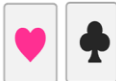
(2) 4枚ANDのbad/final stateの区分け

“Bad” States

“Good” States








turn によるこの遷移しかfinalに向かわないことを示す

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



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




	1/3 X_1
	2/3 X_1
	1/2 X_0
	1/6 X_0
	1/3 X_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

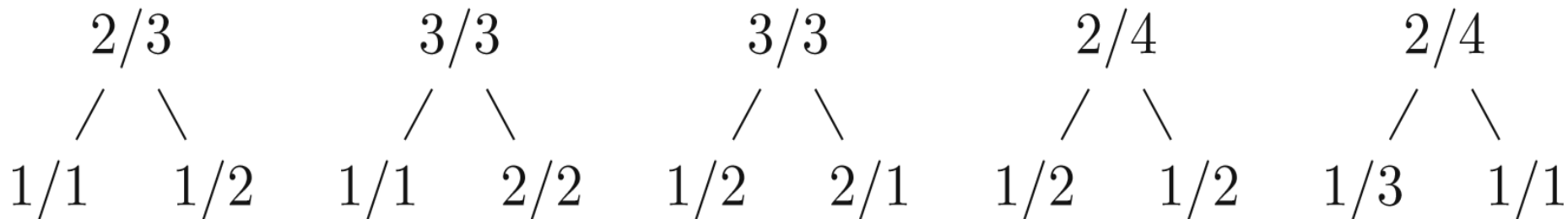
	X_1
	X_0

  出力

	X_1
	3/4 X_0
	1/4 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

(2) turnによる遷移の考えられる全て [KWH15]より



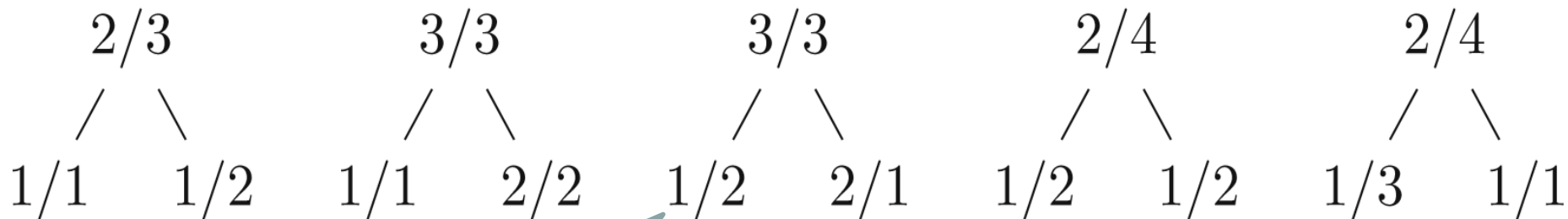
一見、たくさんfinal がありそう

(5/1 state 等にturn を行うと入力が漏れることに注意)

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



(2) turnによる遷移の考えられる全て



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

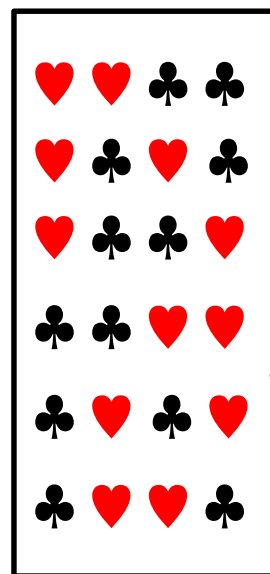
定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない



(2) turn 後の $i+j$

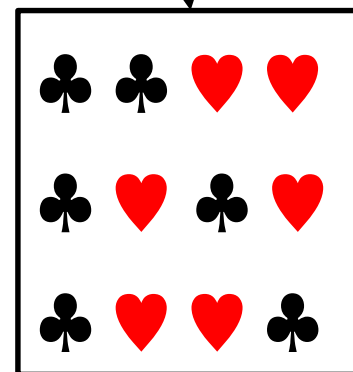
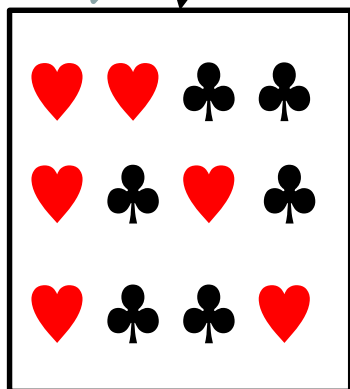
4枚において、共通の絵柄をもつような絵柄列は高々3個

⇒ $i+j < 4$



4枚で考えられる全ての絵柄を含んだ state (確率省略)

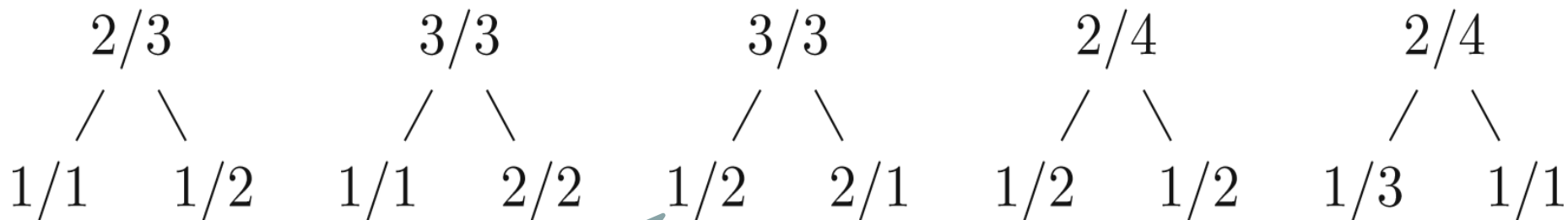
turn 1



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



(2) turnによるstateの遷移



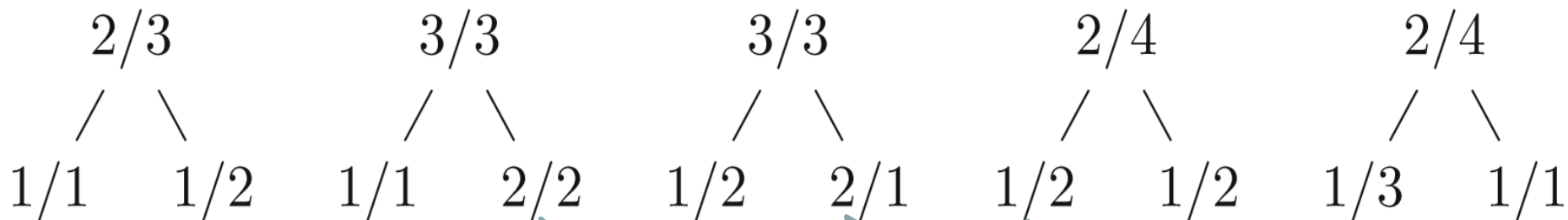
turn後は絵柄が一致するのでfinal になれないことは見た

turn 後の $i+j < 4$ であることを見た

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

  = 0   = 1

(2) turnによるstateの遷移

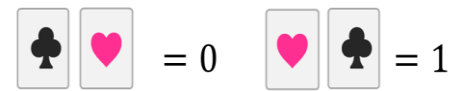


この遷移しかfinalを生まない \Rightarrow 4枚ANDはLas Vegas^[KWH15]

finalではない

有り得ない

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

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

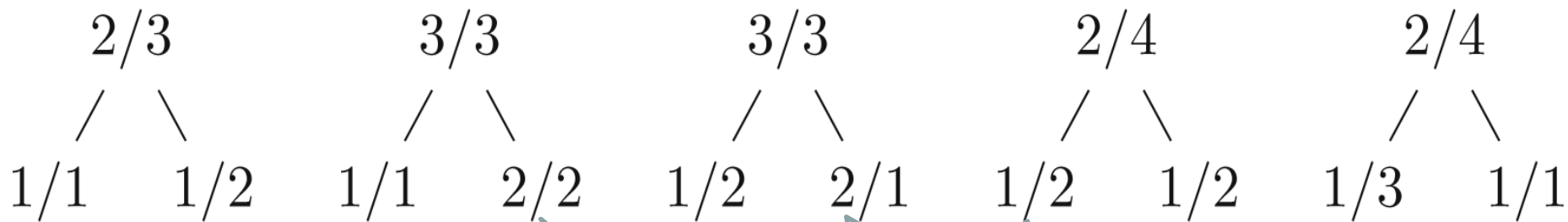
• ランダム二等分割カットは① ② を満たす

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

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

[復習] (2) turnによるstateの遷移



finalではない

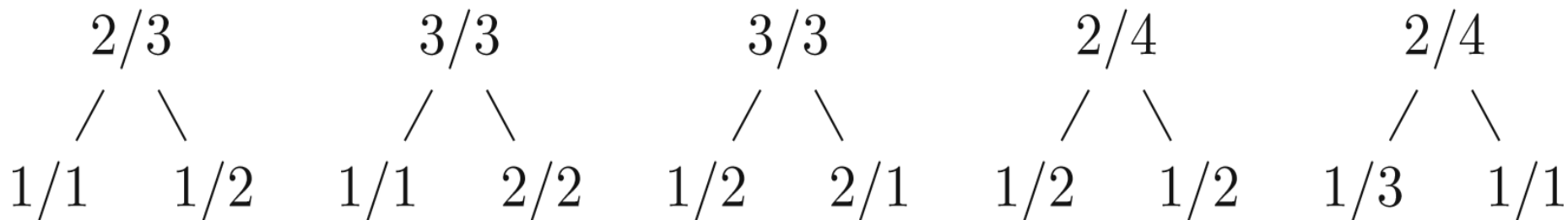
有り得ない

この遷移しかfinalを生まない \Rightarrow 4枚ANDはLas Vegas^[KWH15]

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



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

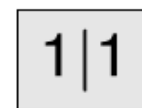
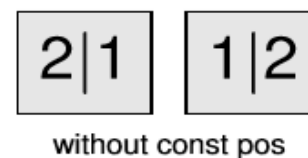
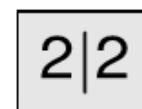
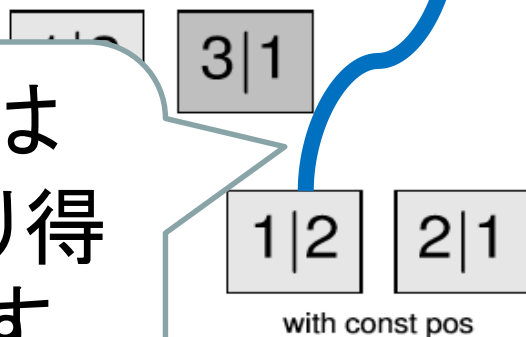
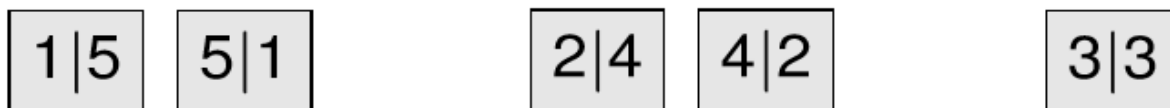
定理: uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない

♣♥ = 0 ♥♣ = 1

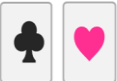
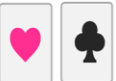
(3) 4枚ANDのbad/final stateの区分け

“Bad” States

“Good” States

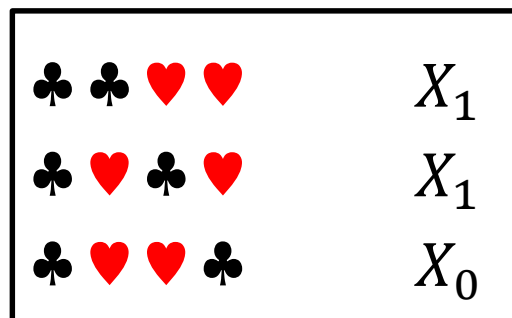


uc shuffle では
この遷移があり得
ないことを示す
(他は省略)

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

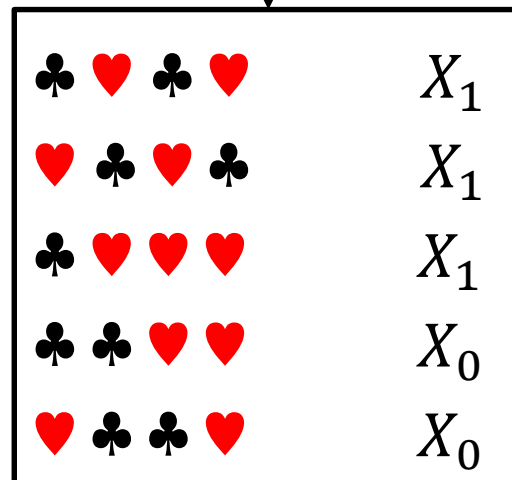
(3) uc shuffleによる1/2→2/3遷移の不可能性

1/2 stateは共通する絵柄を必ずもつことに注意しよう

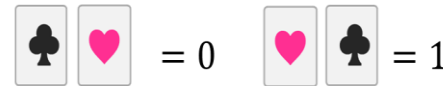


shuf, Π , \mathcal{F}
 Π : closed (群)
 \mathcal{F} : uniform (均一)

一般性を失わずに、
 は2/3に含まれないと仮定



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



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

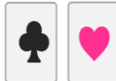
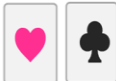
具体例
で示す

♣ ♣ ♥ ♥	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) シヤッフル  = 0  = 1
のみを用いた4枚ANDは存在しない

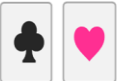
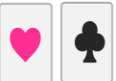
例) $\Pi = \{\text{id}, (1\ 3)\} \Rightarrow \heartsuit \heartsuit \clubsuit \clubsuit$ が含まれるので矛盾

	X_1
	X_1
	X_0

shuf, {id, (1 3)}

	X_1
	X_1
	X_1
	X_0
	X_0

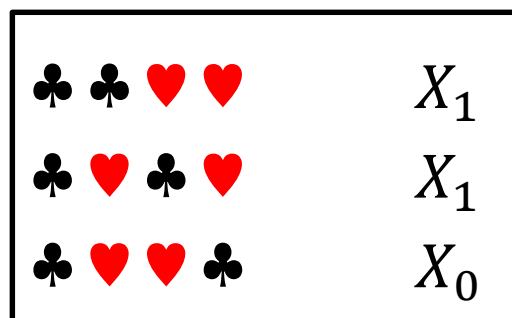
は含まれないと仮定したことに注意

定理: uniform-closed (uc) シヤッフル  = 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

$\Rightarrow \Pi \subset \{\text{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$

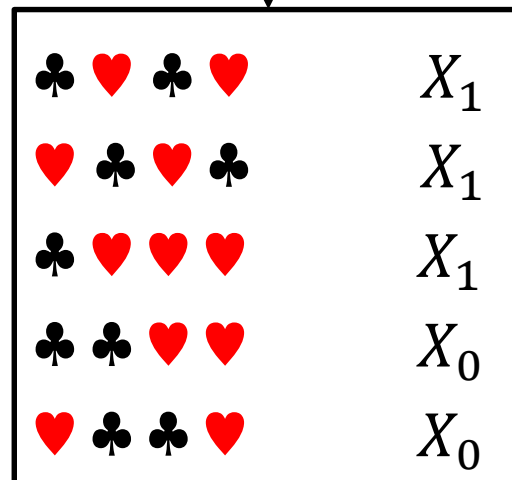
closed が効いている部分







shuf, Π , \mathcal{F}

Π : closed (群)

\mathcal{F} : uniform (均一)



 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

$$\spadesuit \heartsuit = 0 \quad \heartsuit \spadesuit = 1$$

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

$$\spadesuit \heartsuit = 0 \quad \heartsuit \spadesuit = 1$$

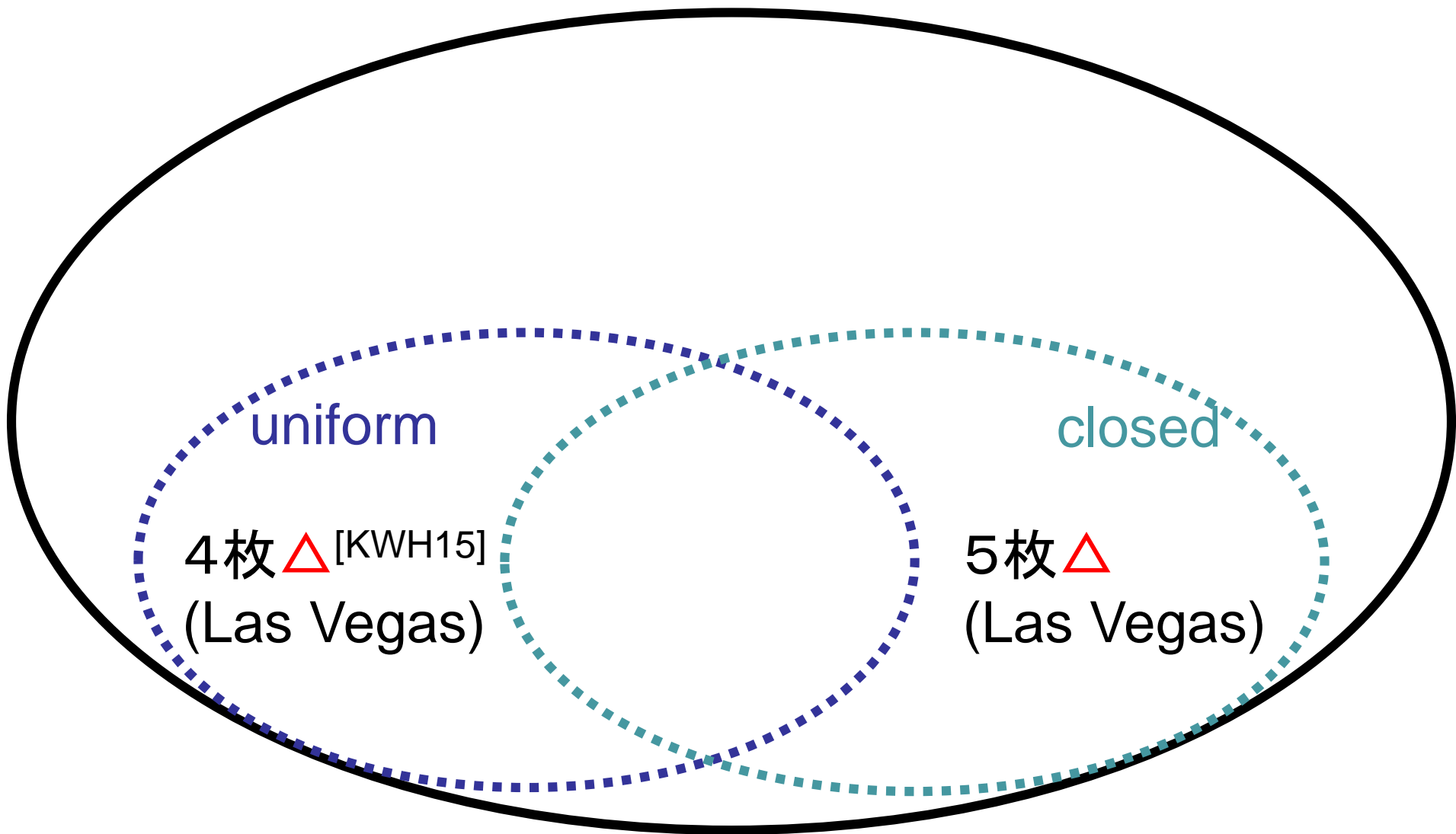
枚数	有限	Las Vegas
6	[MS09]	
5	✖※ (ours)	
4	✖ [KWH15]	♦ (ours)

※ 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