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

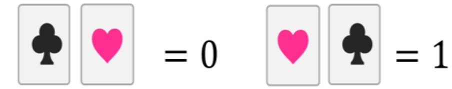
宮原大輝
東北大学大学院情報科学研究科

♣ ♥ = 0 ♥ ♣ = 1

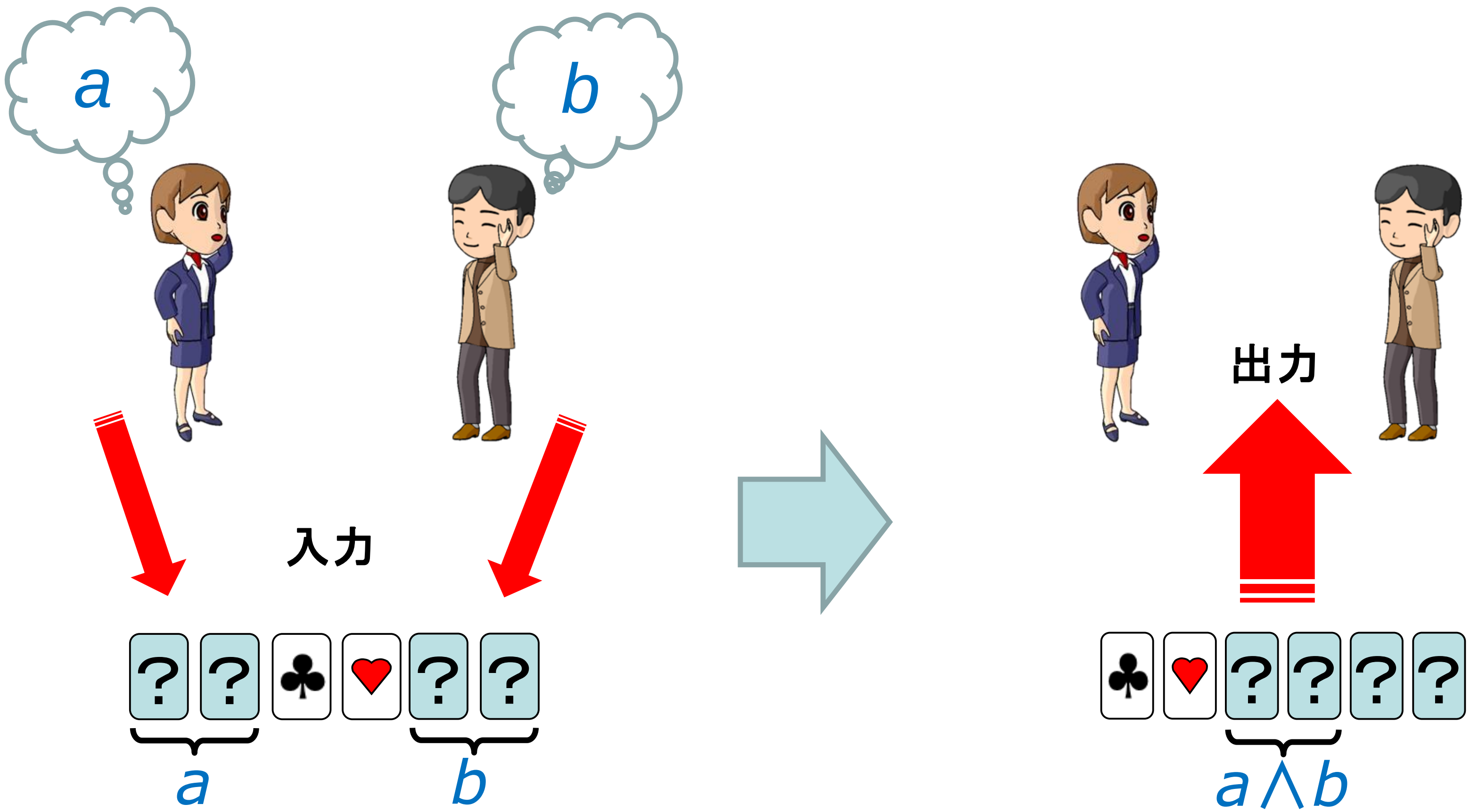
Thursday, December 7 2017		
	R - track	**I - track**
	Cryptographic Protocols (Khoa Nguyen)	**Foundations** (Tatsuaki Okamoto)
9:00-9:25	Two-Round PAKE from Approximate SPH and Instantiations from Lattices; *Jiang Zhang, Yu Yu*	Succinct Spooky Free Compilers Are Not Black Box Sound; *Zvika Brakerski, Yael Tauman Kalai, Renen Perlman*
9:25-9:50	Tightly-Secure Signatures from Five-Move Identification Protocols; *Eike Kiltz, Julian Loss, Jiaxin Pan*	Non-Interactive Multiparty Computation without Correlated Randomness; *Shai Halevi, Yuval Ishai, Abhishek Jain, Ilam Komargodski, Amit Sahai, Eylon Yogev*
9:50-10:15	On the Untapped Potential of Encoding Predicates by Arithmetic Circuits and Their Applications; *Shuichi Katsumata*	Optimal-Rate Non-committing Encryption; *Ran Canetti, Oxana Poburinnaya, Mariana Raykova*
10:15-10:40	The Minimum Number of Cards in Practical Card-based Protocols; *Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone*	Preventing CLT Attacks on Obfuscation with Linear Overhead; *Rex Fernando, Peter M. R. Rasmussen, Amit Sahai*
10:40-11:10	Coffee Break	

ここ

あらまし

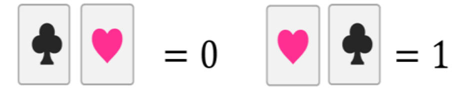


- 例）6枚のカードを用いるANDプロトコル[MS09]



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

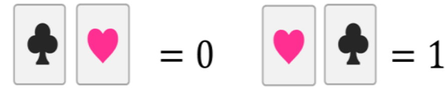
あらまし



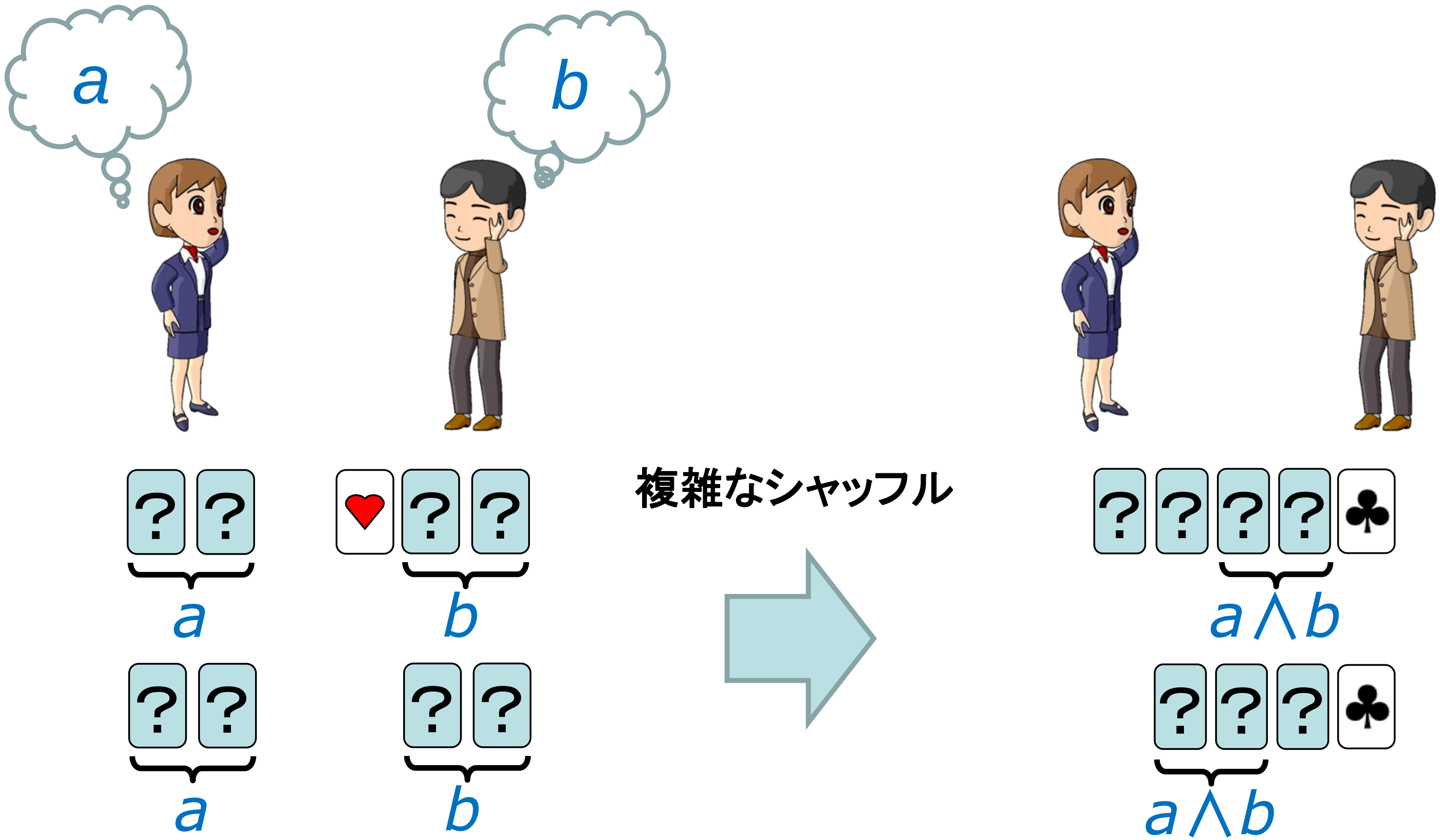
- 例）６枚のカードを用いるANDプロトコル[MS09]

[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



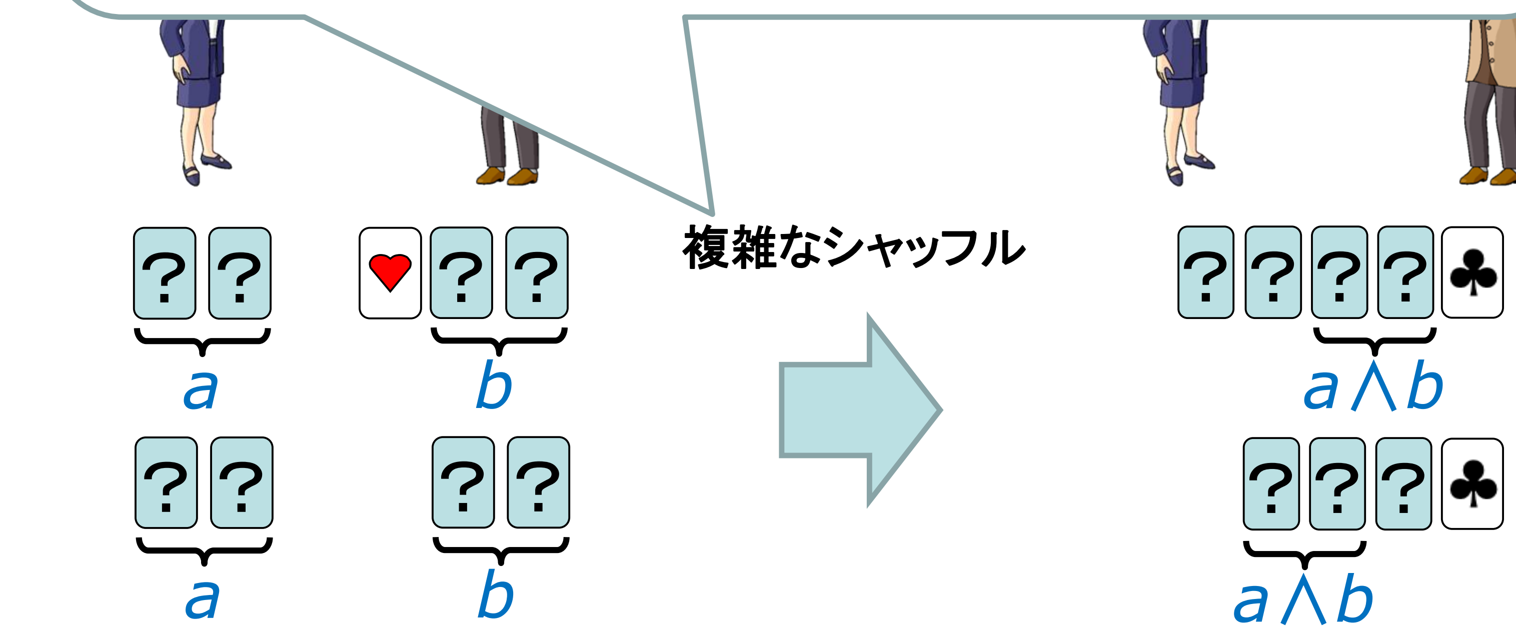
- 4, 5枚のカードを用いるAND プロトコル[KWH15]



[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

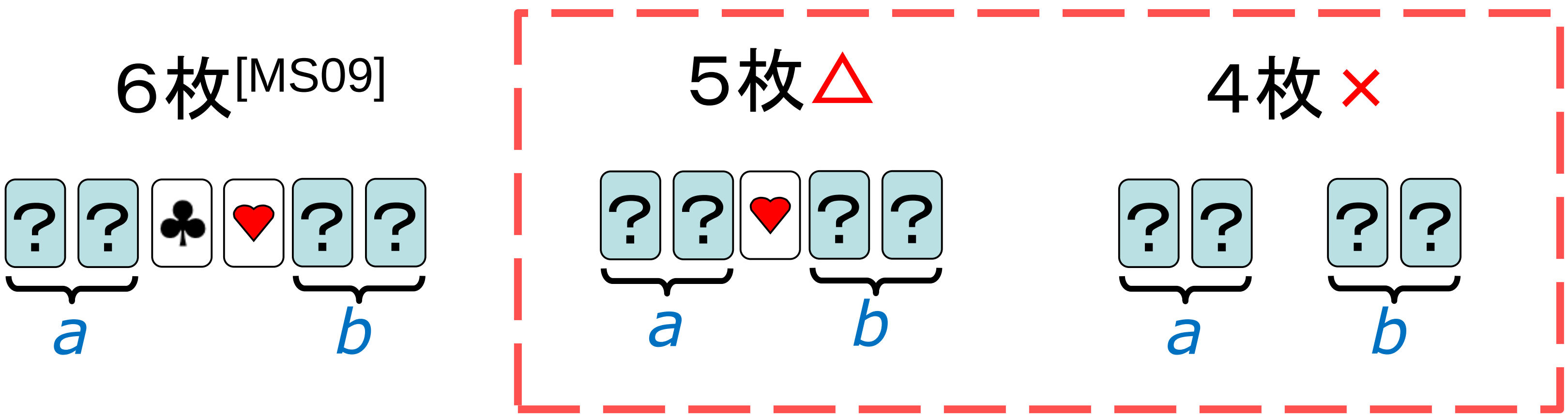
簡単なシャッフルのみのAND
プロトコルは存在する？



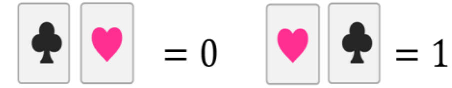
[KWH15] Koch, A., Walzer, S., Härtel, K., ``Card-based cryptographic protocols using a minimal number of cards.'' ASIACRYPT 2015, LNCS, pp. 783–807.

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**…）

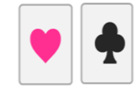


△: プロトコルは存在する（だろう）が、Las Vegas である
×: プロトコルは存在しない

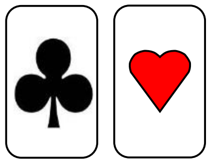
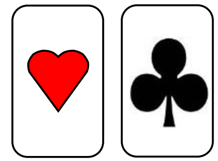


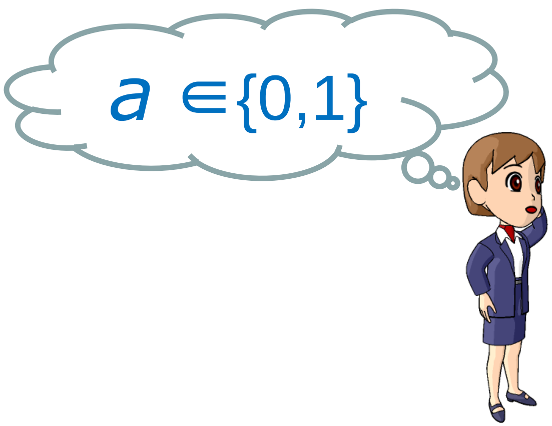
目次

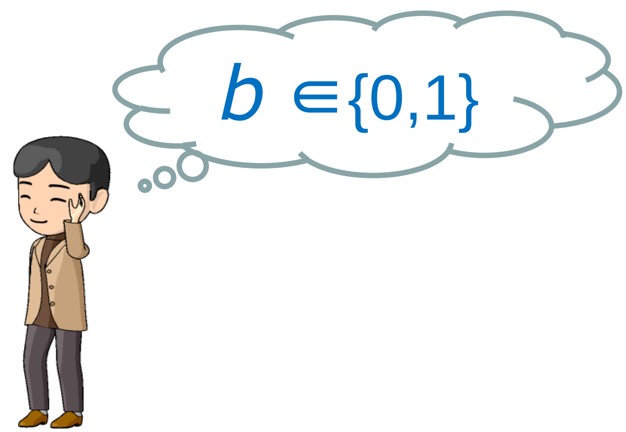
1. はじめに
2. ANDプロトコル
3. COPYプロトコル
4. 最新動向
5. むすび

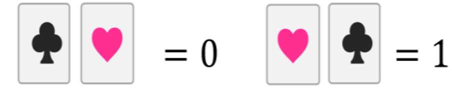
 = 0  = 1

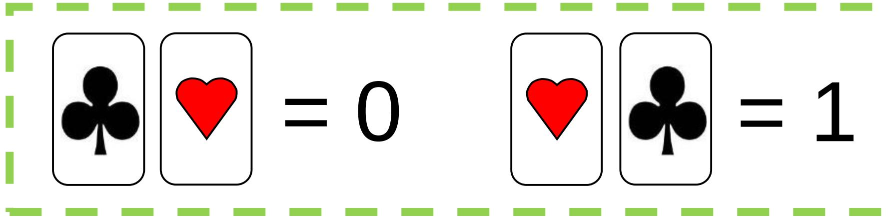
ビットを扱うために，次の符号化を固定する：

 = 0　　 = 1

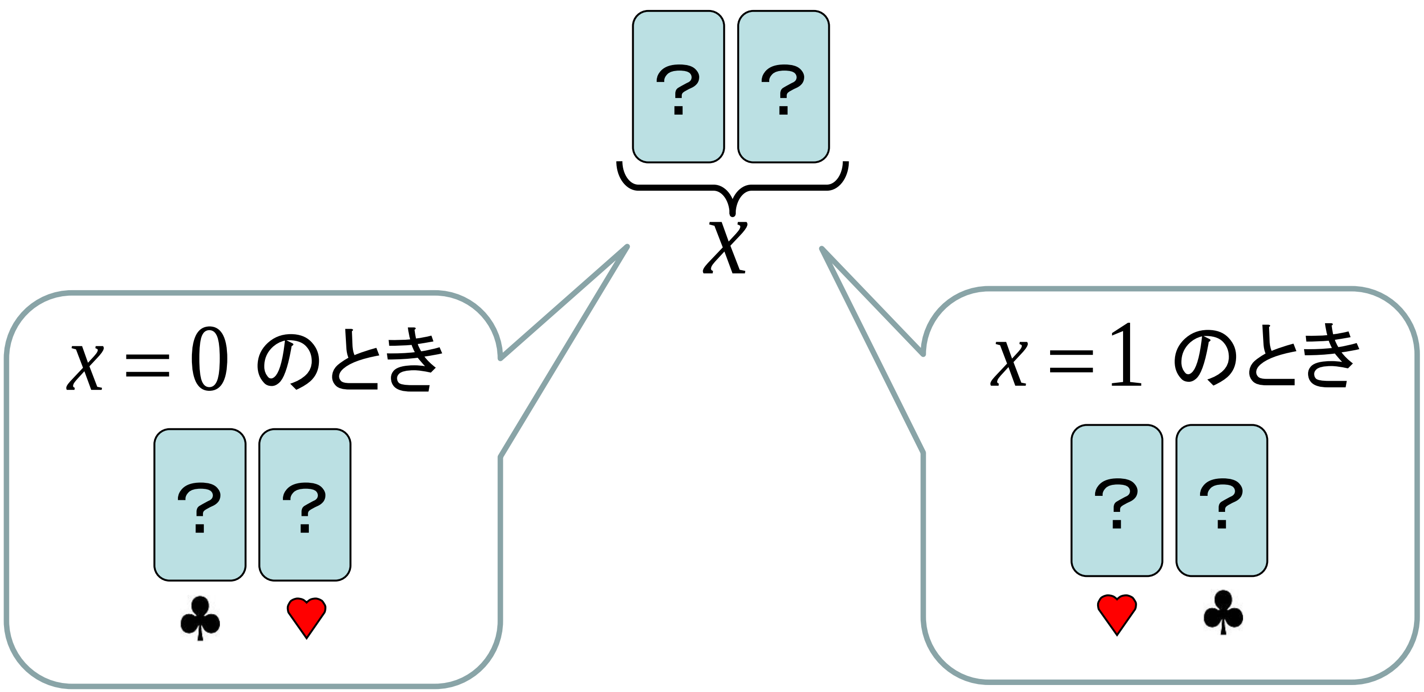


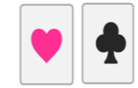






符号化に従う裏に置かれたカードを***コミットメント***と呼ぶ:



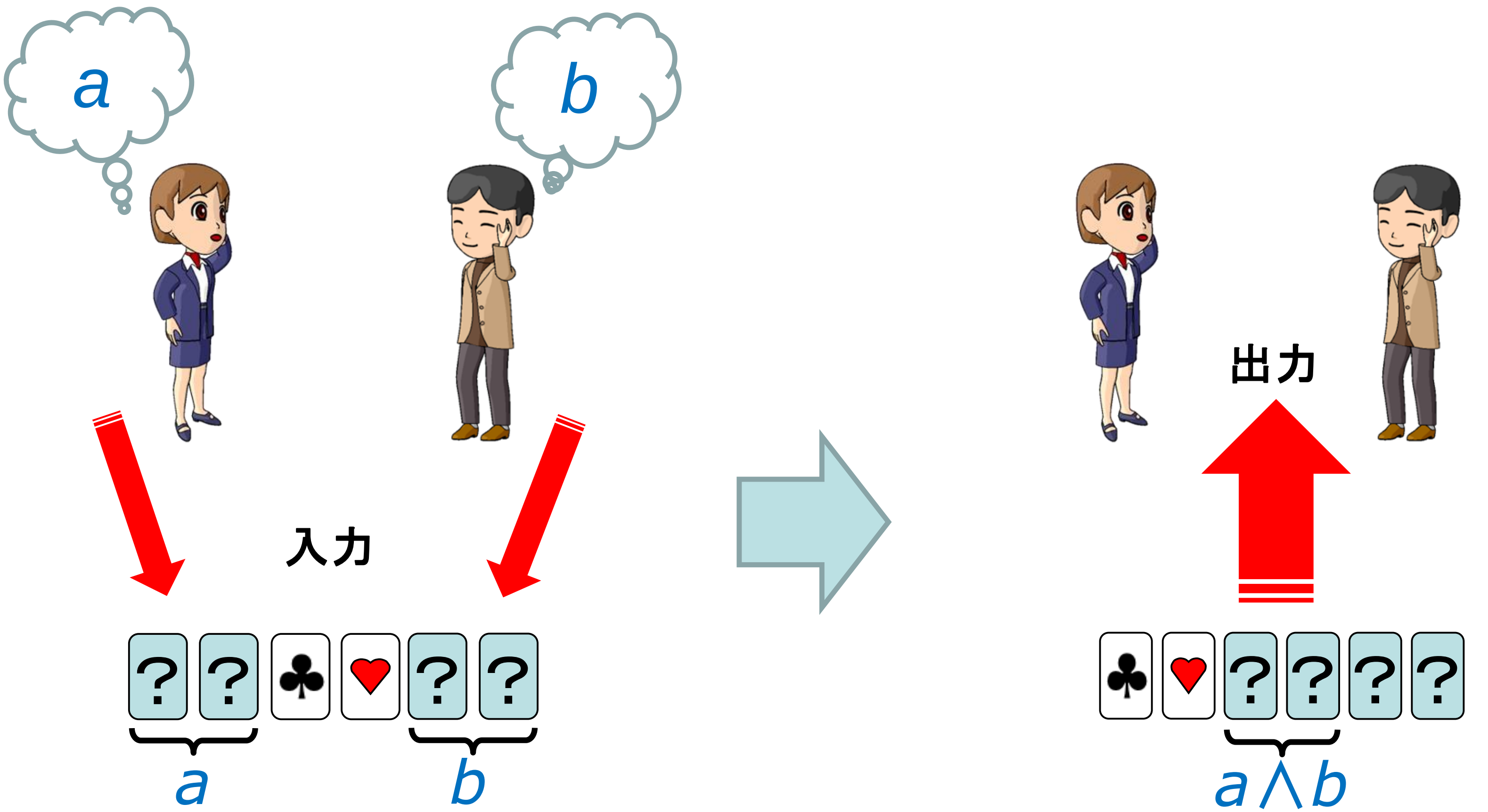
 = 0  = 1

目次

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

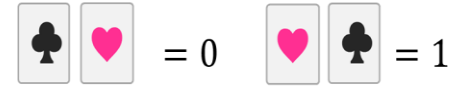
[再掲] あらまし

- 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

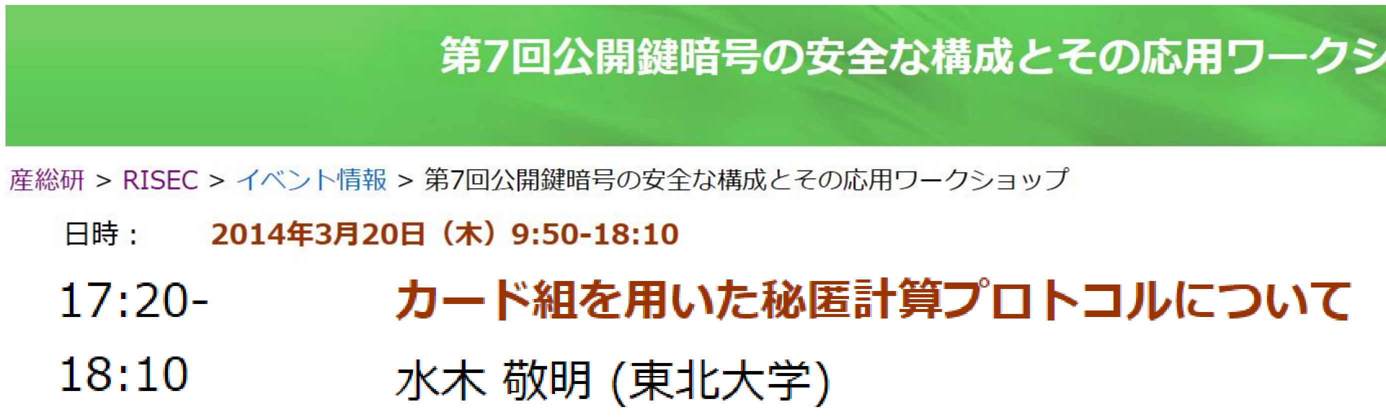


[CK93]

[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

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

17:20-18:10	カード組を用いた秘匿計算プロトコルについて 水木 敬明 (東北大学)

[KWH15]

[SMSN+15]（偏光板カード）

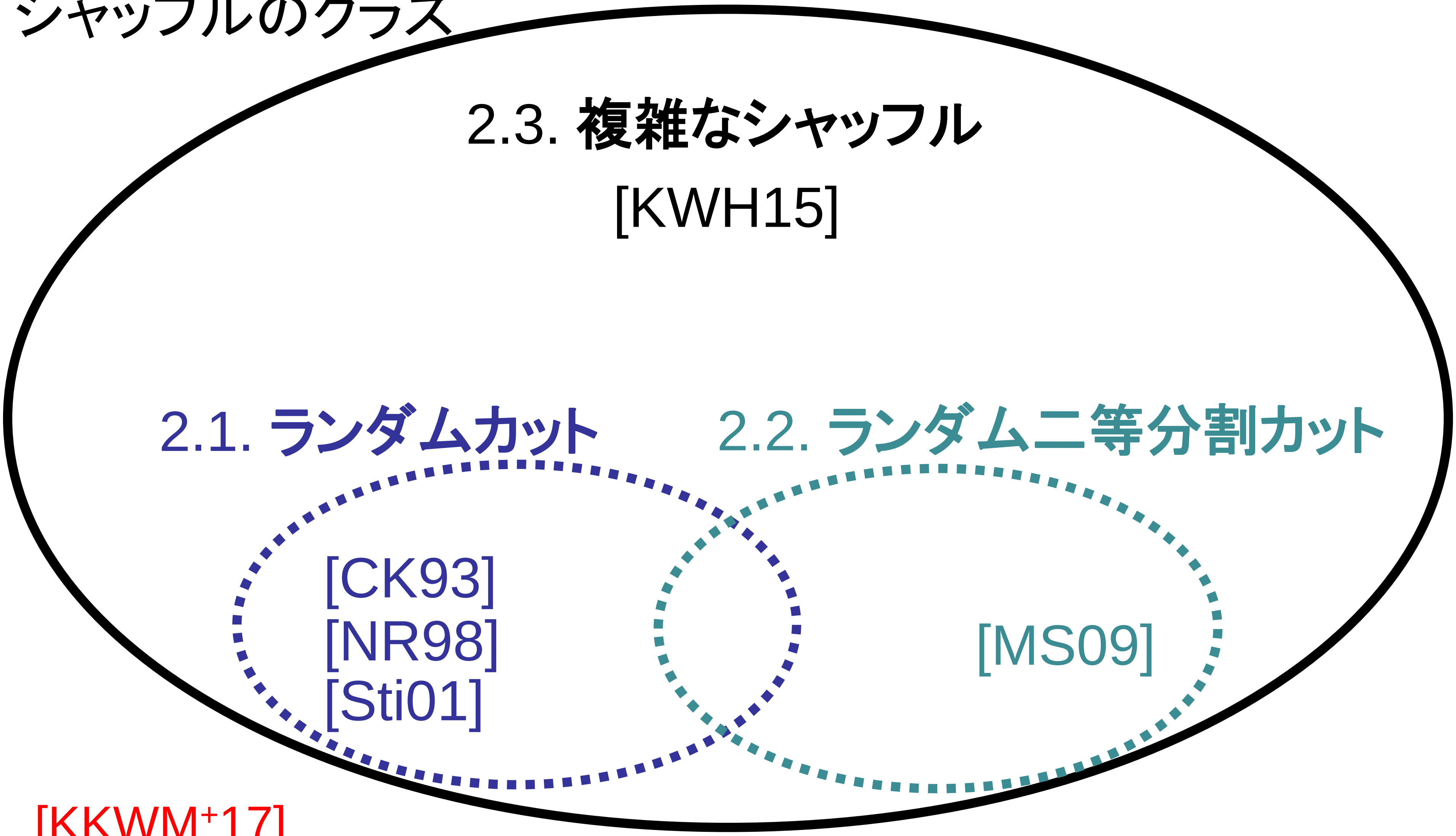
[SMSN+15]（正多角形カード）

[Mizuki16]（トランプカード）

[KKWM+17]

2章の構成

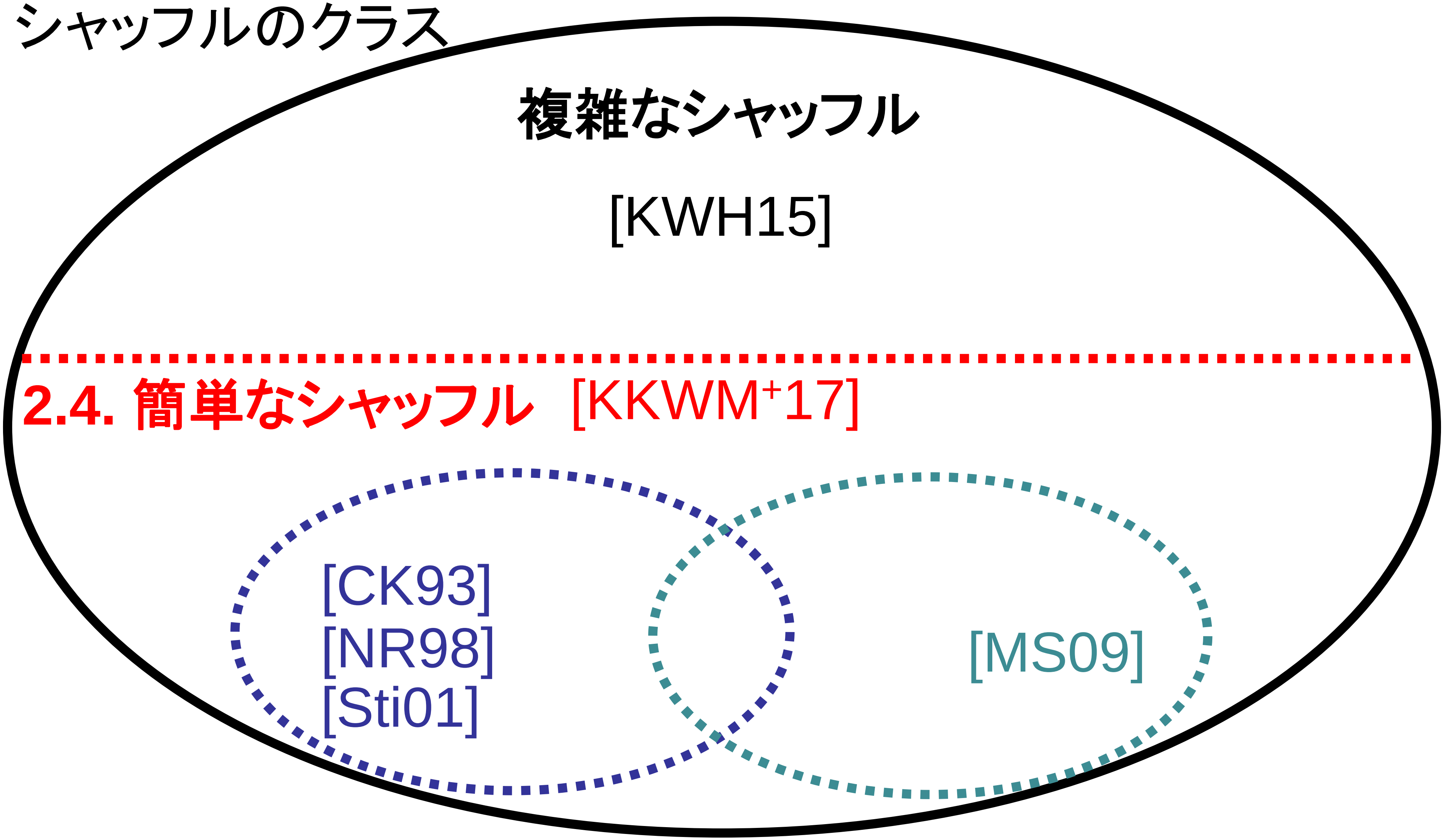
シャッフルのクラス



[KKWM+17]

２章の構成

シャッフルのクラス



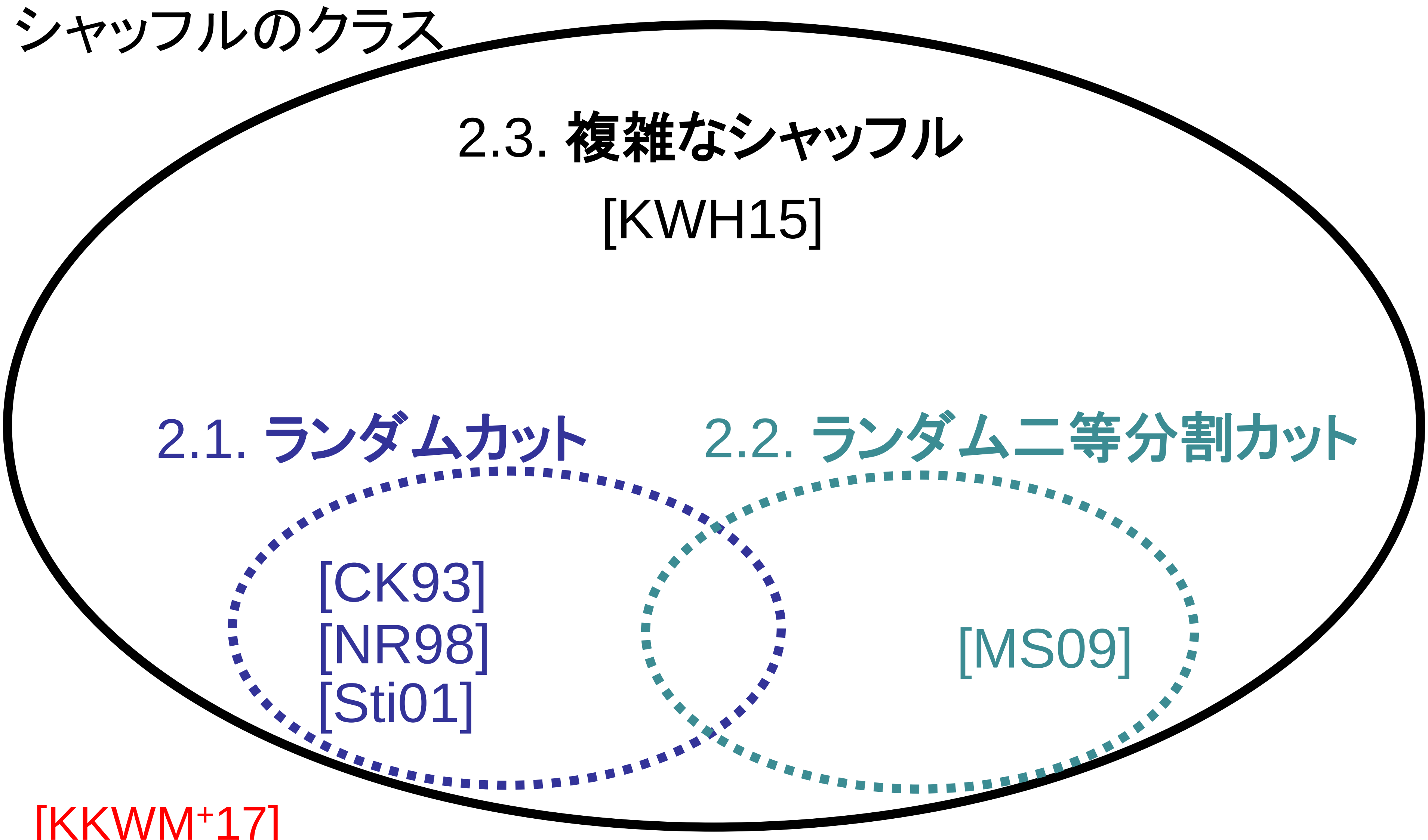
2001年までのAND計算プロトコル：

♣♥ = 0　♥♣ = 1

コミット型AND計算

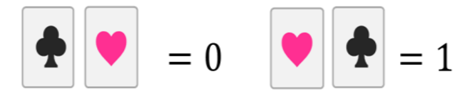
	枚数等	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 ♣♣♣♥♥♥♠♠♦♦	6
Niemi-Renvall [TCS, 1998]	12 ♣♣♣♣♣♣♥♥♥♥♥♥	2.5
Stiglic [TCS, 2001]	8 ♣♣♣♣♥♥♥♥	2

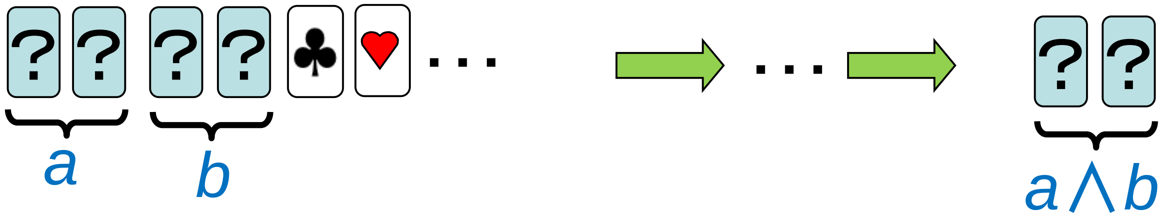
2章の構成



[KKWM+17]

コミット型ANDプロトコルのまとめ：

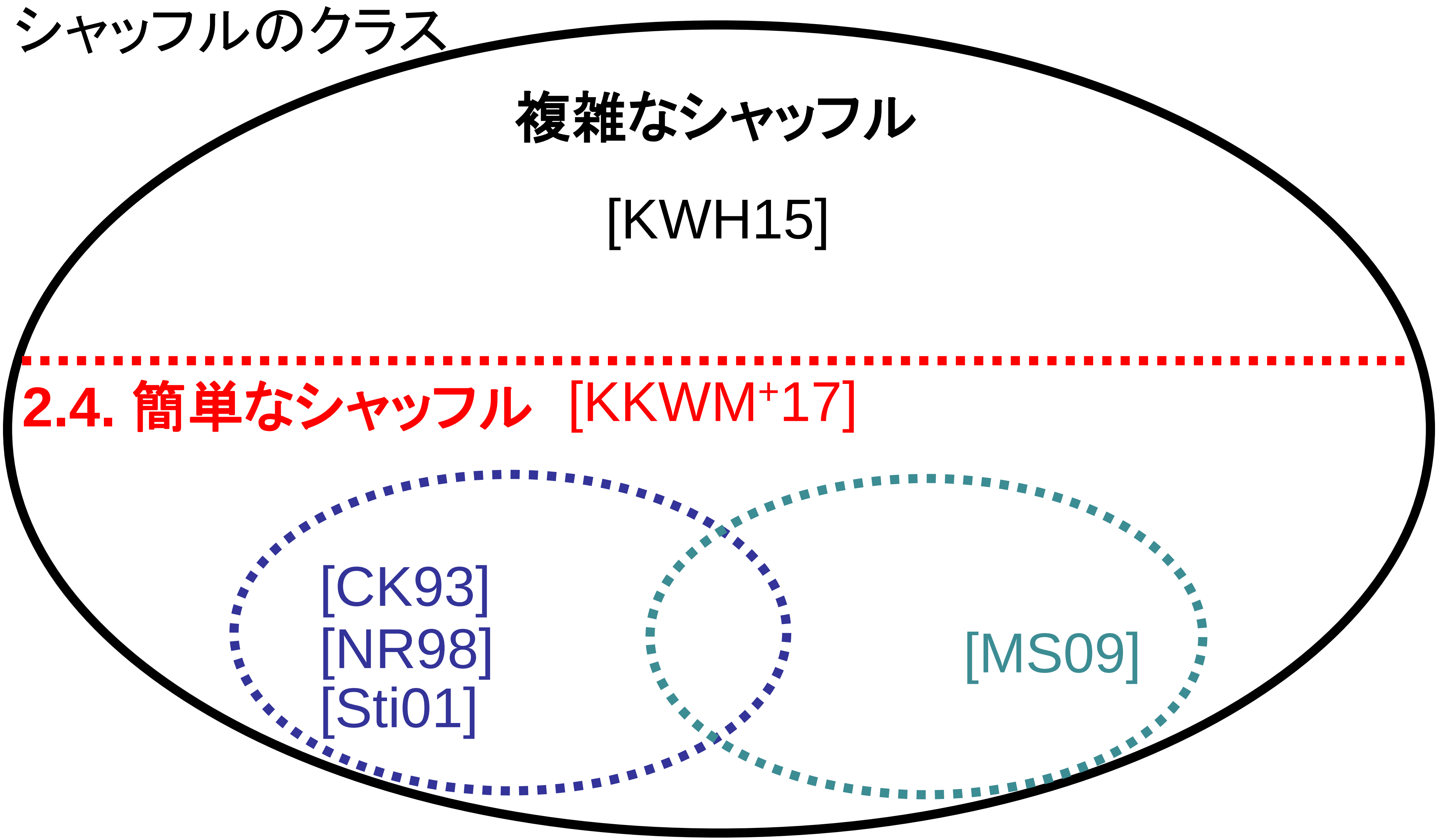




	枚数等	ランダムカット	二等分割カット	平均試行回数
Crepeau-Kilian [CRYPTO '93]	10 ♣♣♣♥♥♥ ♠♠♦♦	✔		6
Niemi-Renvall [TCS, 1998]	12 ♣♣♣♣♣♣ ♥♥♥♥♥♥	✔		2.5
Stiglic [TCS, 2001]	8 ♣♣♣♣♥♥♥♥	✔		2
Mizuki-Sone [FAW 2009]	6 ♣♣♣♥♥♥		✔	1

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]

♣ ♥ = 0 ♥ ♣ = 1

[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.

$\clubsuit\heartsuit = 0$ $\heartsuit\clubsuit = 1$

カード列

$$\underbrace{?\ ?}_{a}\ \clubsuit\ \heartsuit\ \underbrace{?\ ?}_{b}$$

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

$\clubsuit\heartsuit = 0$ $\heartsuit\clubsuit = 1$

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

並び替える (perm, (2 4 3))

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

$\clubsuit\heartsuit = 0 \quad \heartsuit\clubsuit = 1$

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

シャッフル

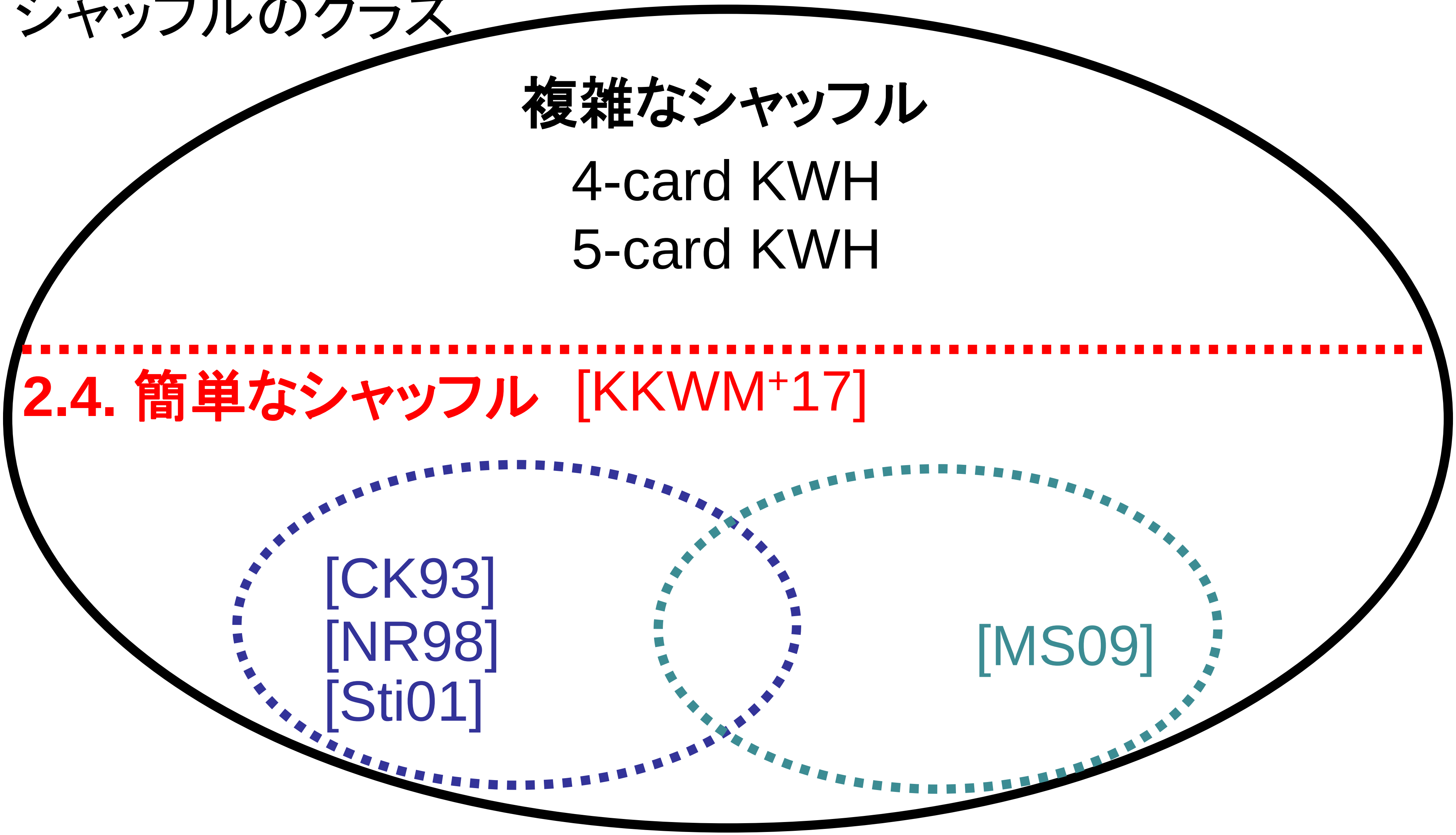
$$(\mathrm{shuf}, \mathrm{id} \mapsto 1/2, (1\ 4)(2\ 5)(3\ 6) \mapsto 1/2\ )$$

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

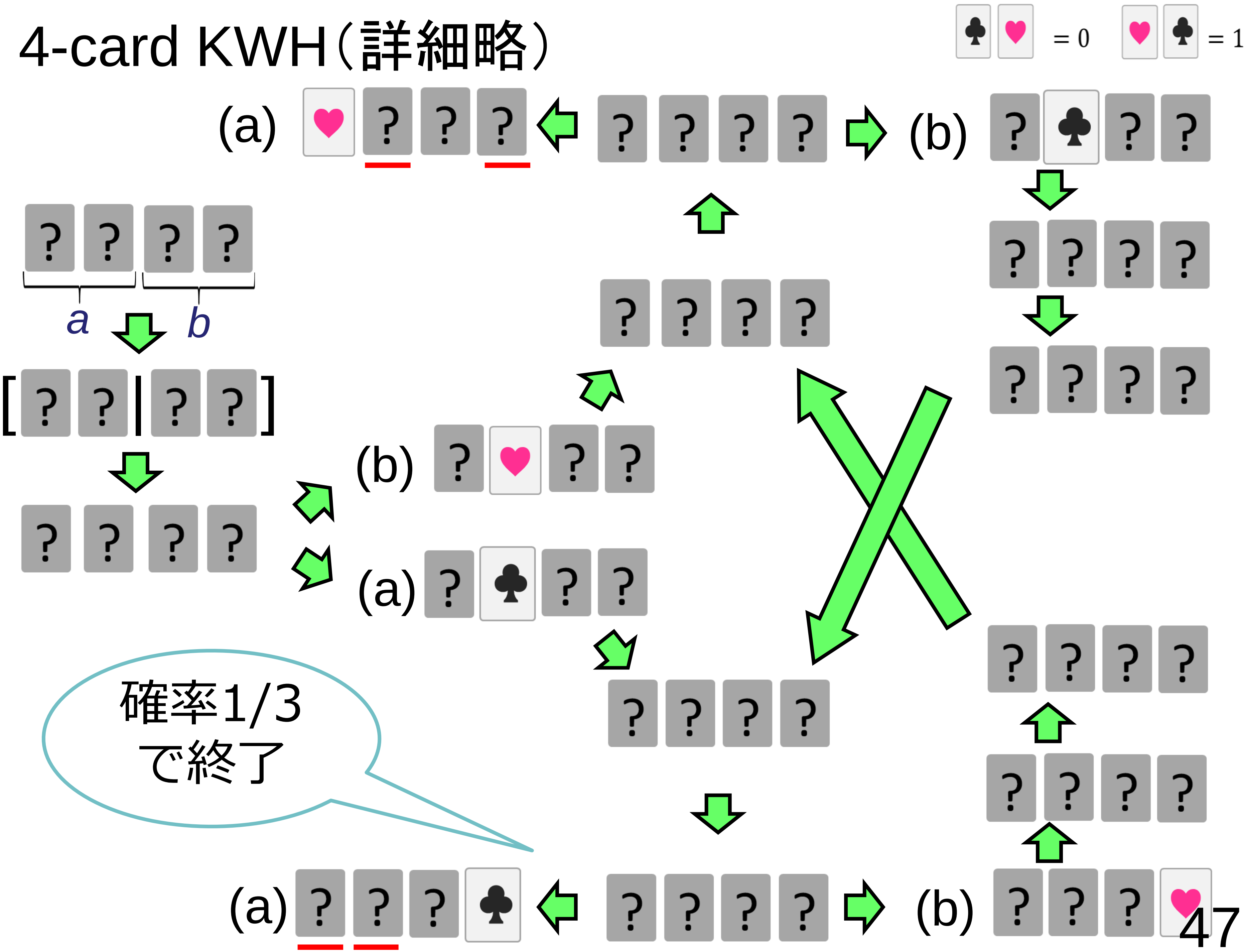
シャッフルは、置換の集合とその上の確率分布

2章の構成

シャッフルのクラス



4-card KWH（詳細略）



$\clubsuit\heartsuit = 0$　$\heartsuit\clubsuit = 1$

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

KWH プロトコルに必要なシャッフル(1)

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

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

つまり、不均一な（確率分布の）シャッフル

$\clubsuit\,\heartsuit = 0$ $\heartsuit\,\clubsuit = 1$

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

KWHプロトコルに必要なシャッフル(2)

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

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

つまり、置換集合が群を成していない

$(\mathrm{shuf}, \Pi, \mathcal{F})$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

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

- ランダム二等分割カットは① ② を満たす

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

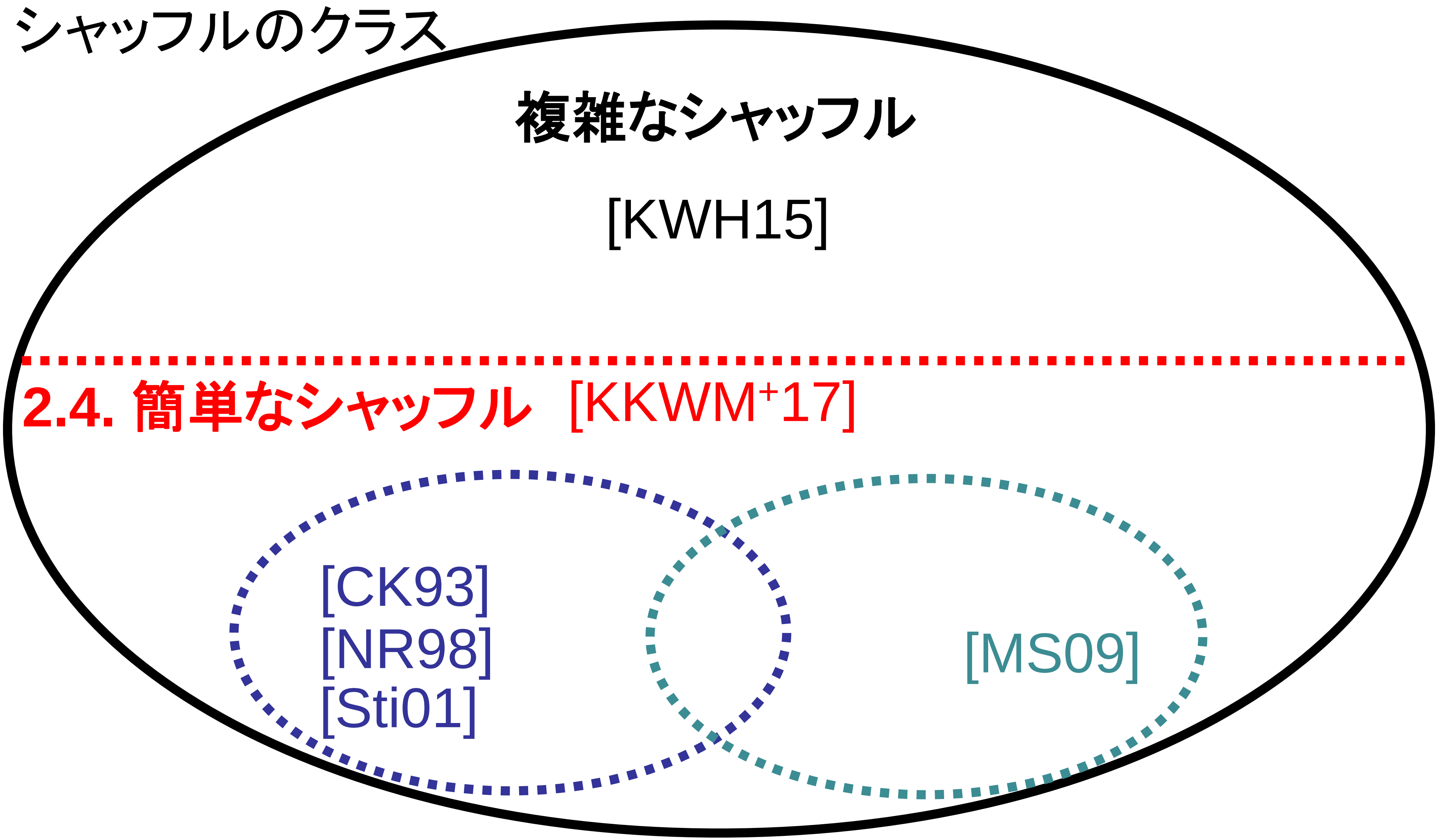
ランダムカット $\langle$? ? ? ? ? $\rangle$

♣ ♥ = 0 ♥ ♣ = 1

uniform-closed だと簡単に手で実装できる（と信じている）

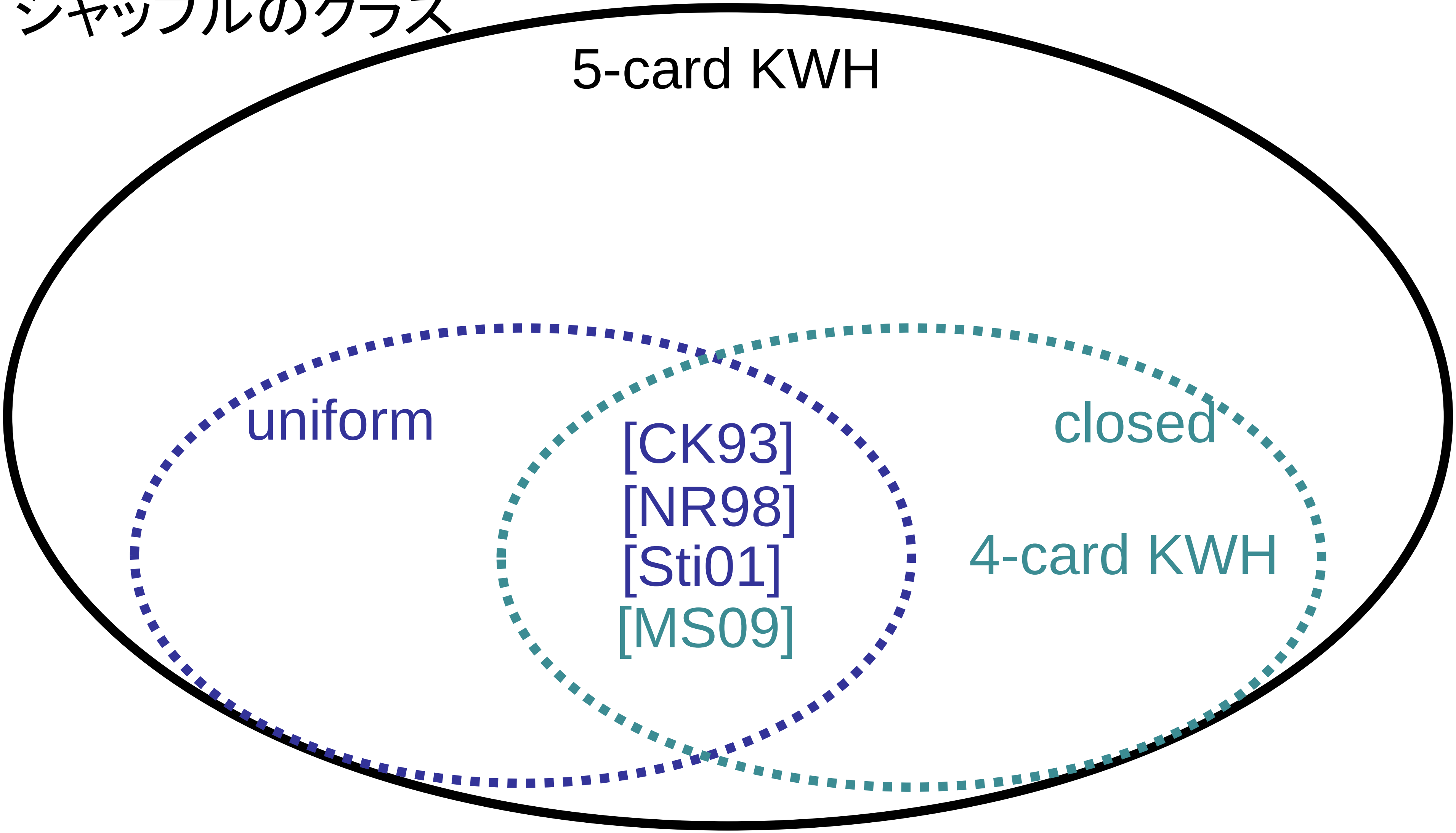
実際に分類を行うと


= 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]

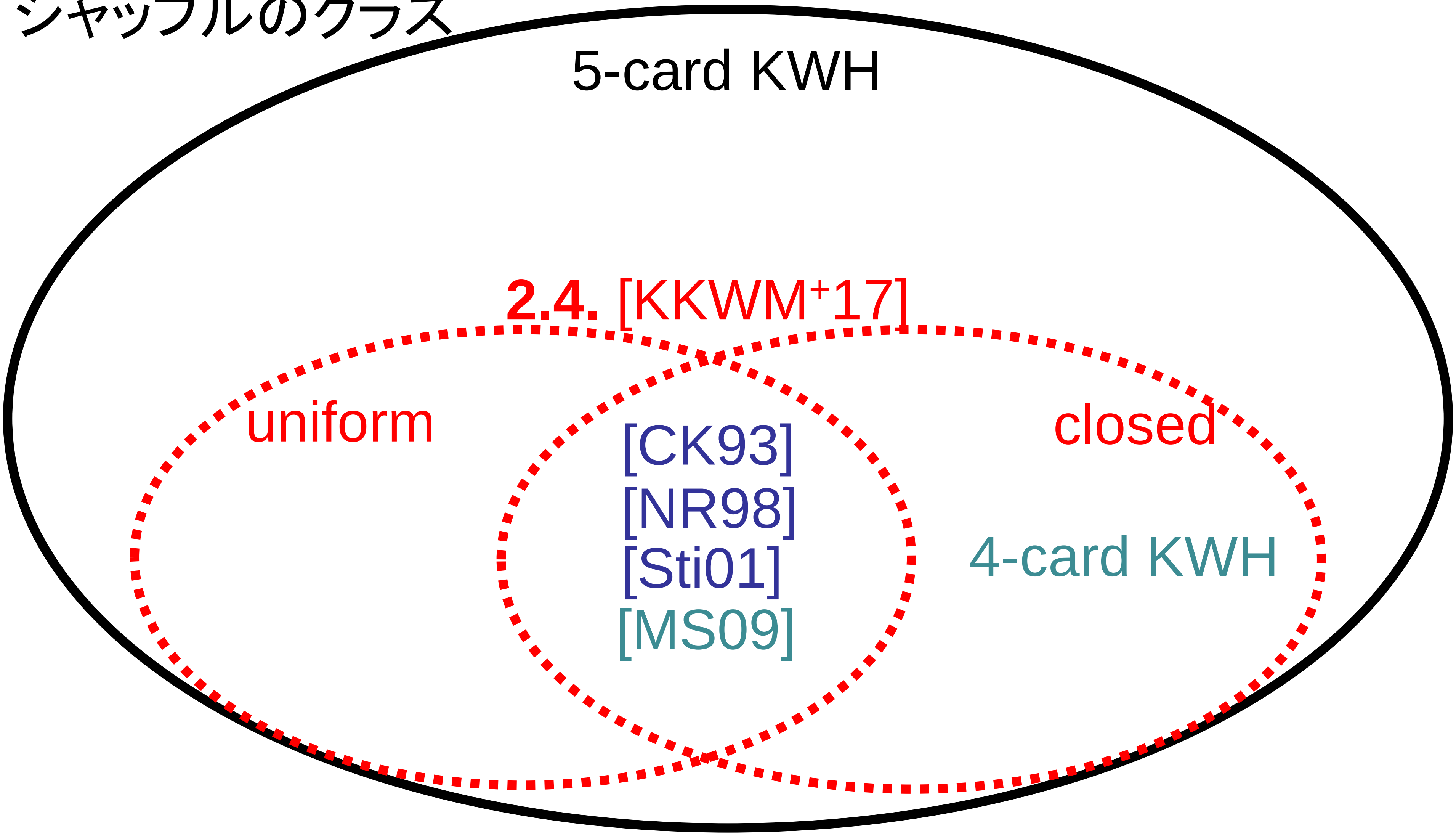
2章の構成

シャッフルのクラス



お待たせしました…

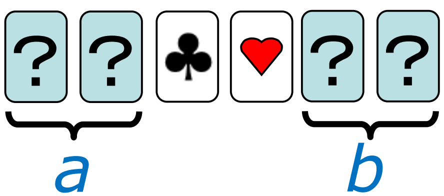
シャッフルのクラス



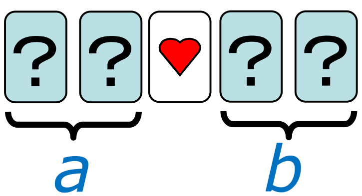
[再掲] あらまし

- “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**…）

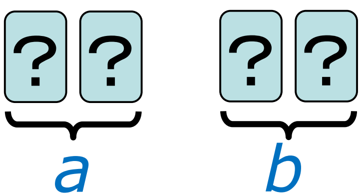
６枚[MS09]



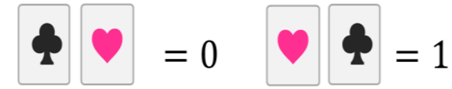
５枚△



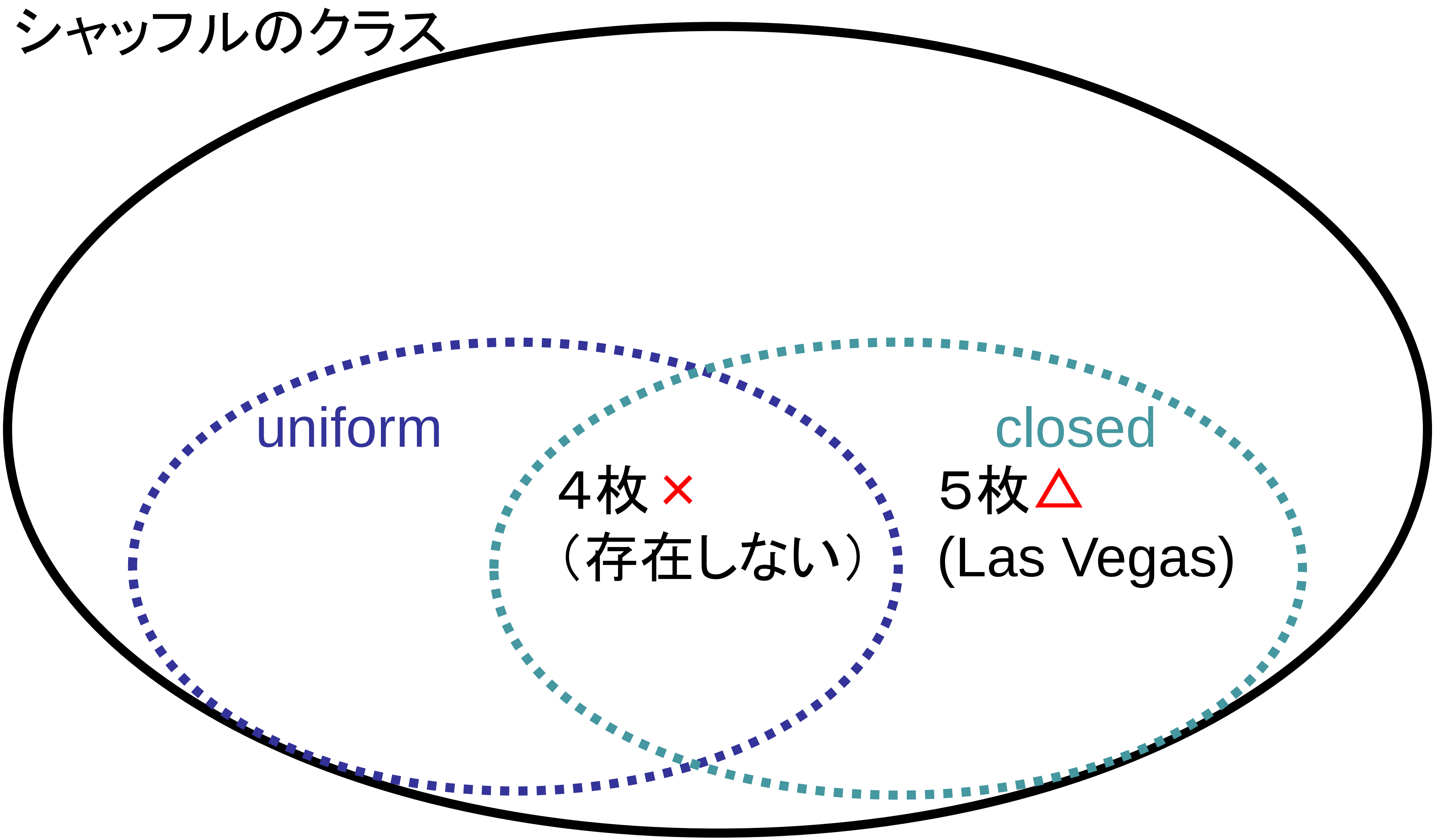
４枚×



△: プロトコルは存在する（だろう）が、Las Vegas である
×: プロトコルは存在しない



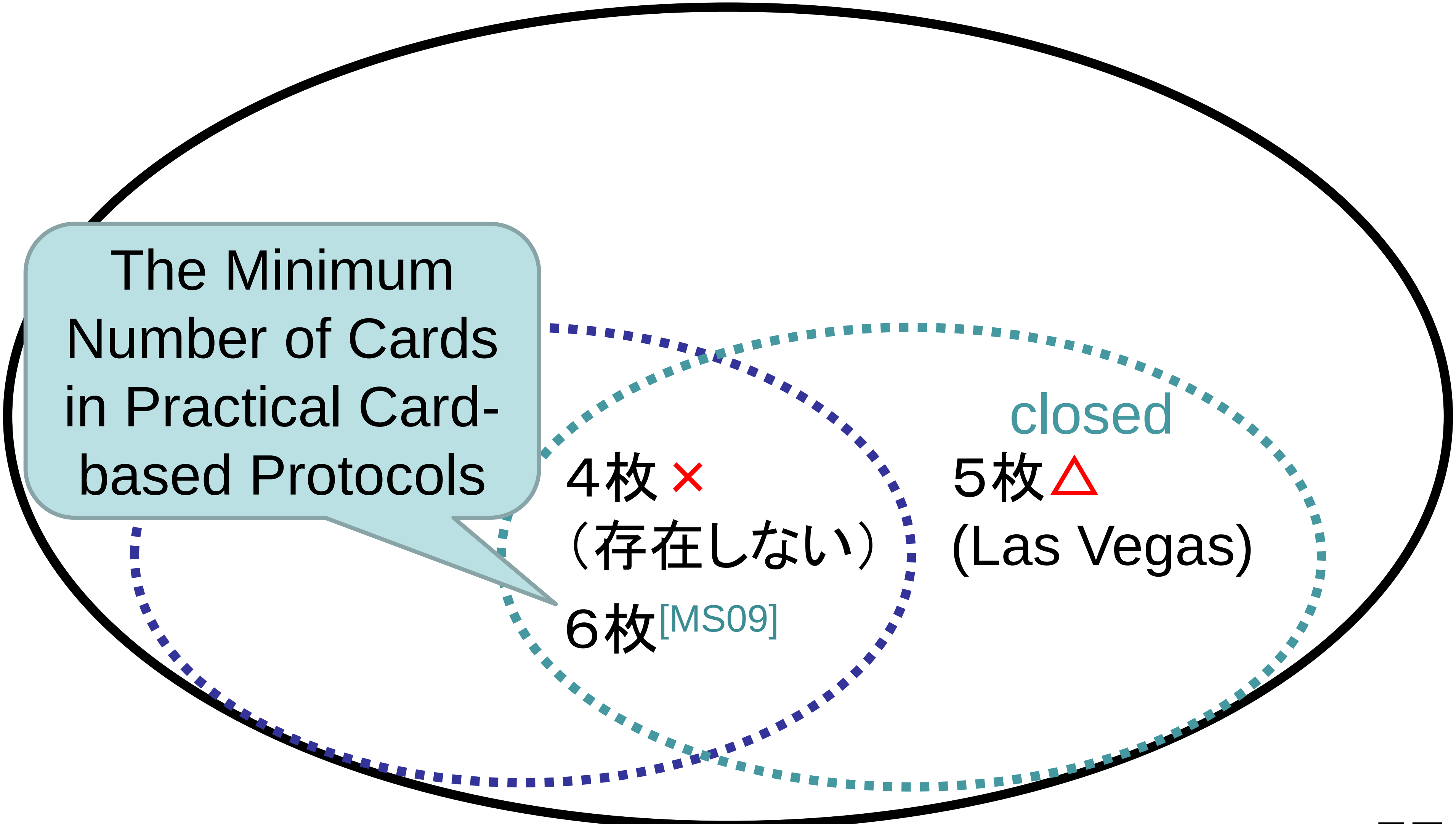
ANDのために必要な枚数



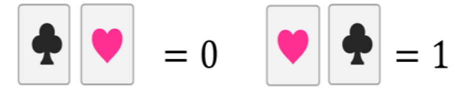
※具体的なプロトコルは提案できていないことに注意

ANDのために必要な枚数

シャッフルのクラス



uniform-closedのみを用いたAND



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

♣♥ = 0　♥♣ = 1

uniform-closedのみを用いたAND

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

♣♥ $= 0$ ♥♣ $= 1$

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

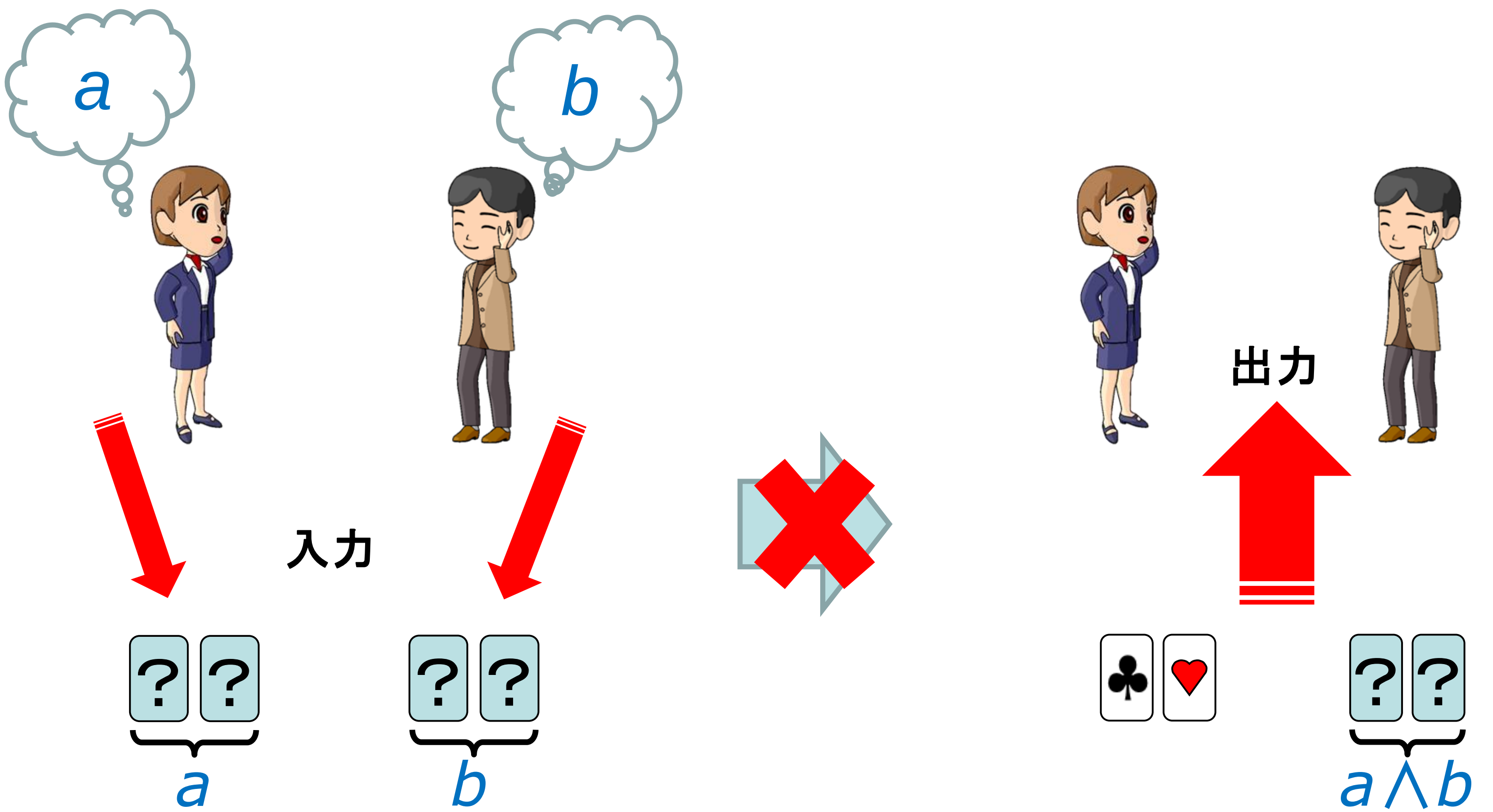
- ランダムカットは① ② を満たす

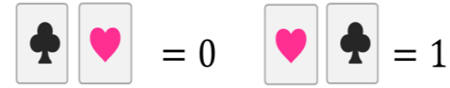
$$\mathrm{RC}^5 = (\mathrm{shuf}, \{(1\ 2\ 3\ 4\ 5)^i \mid 0 \le i \le 4\})$$

- ランダム二等分割カットは① ② を満たす

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

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





証明の概略（実際のスライド）

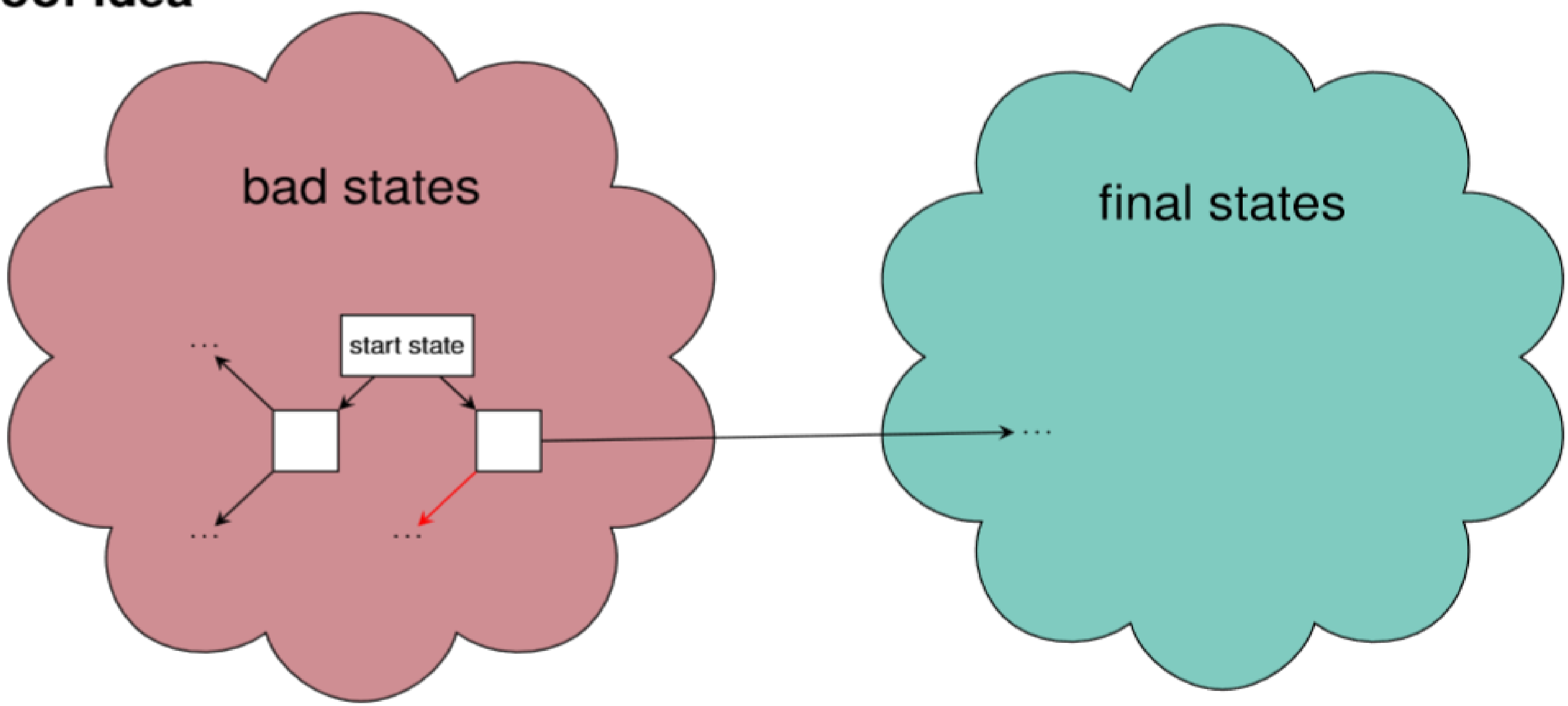
state: チューリング機械のような状態のこと

Impossibility Result

Theorem

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

Proof Idea



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

証明の概略(実際のスライド)

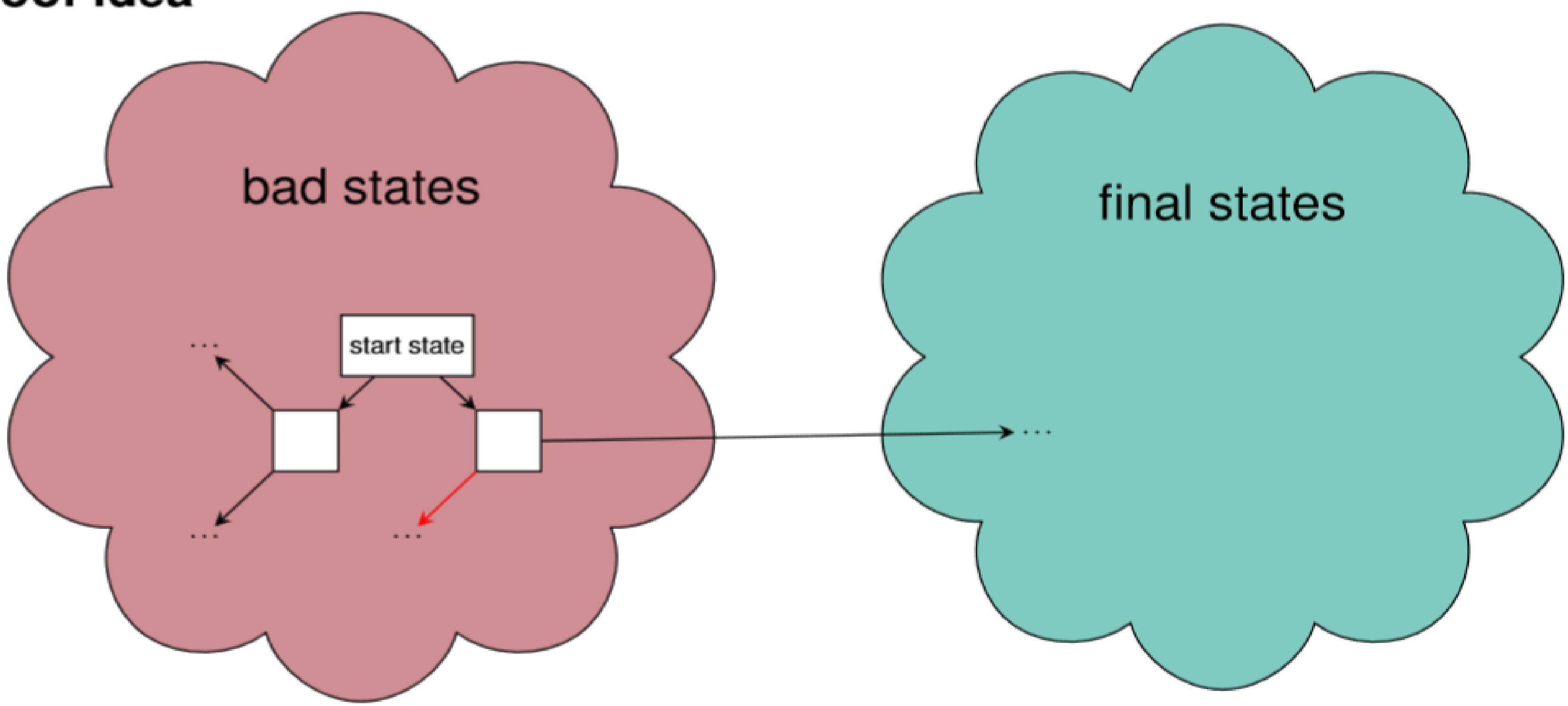
♣♥ = 0 ♥♣ = 1

(1) stateの定義[KWH15]
(2) 4枚ANDのbad/final [KWH15]
(3) ucによるstate遷移

Impossibility Re

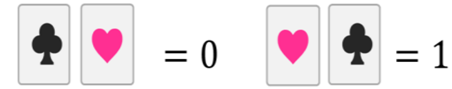
Theorem
There is no secure f

Proof Idea



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

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



(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

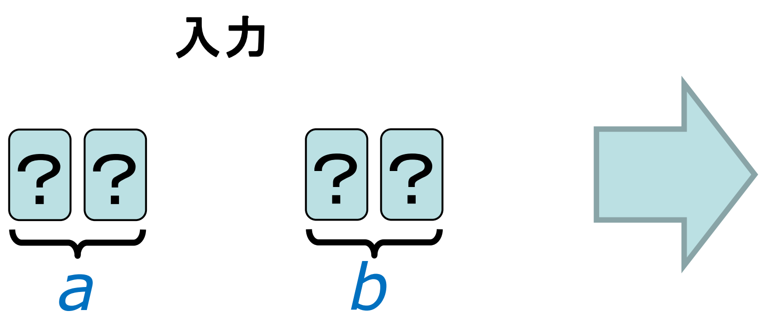
定理：uniform-closed (uc) シャッフルのみを用いた4枚ANDは存在しない

♣♥ = 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



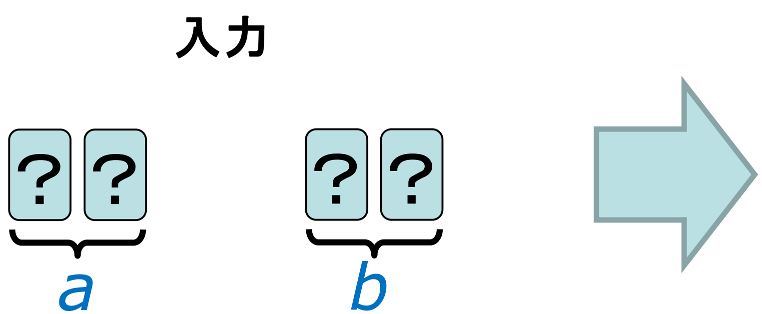
♥	♣	♥	♣	X_{11}
♣	♥	♥	♣	X_{01}
♥	♣	♣	♥	X_{10}
♣	♥	♣	♥	X_{00}

定理：uniform-closed (uc) シャ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) シャ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（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

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

出力

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

♣♥ $= 0$ ♥♣ $= 1$

(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

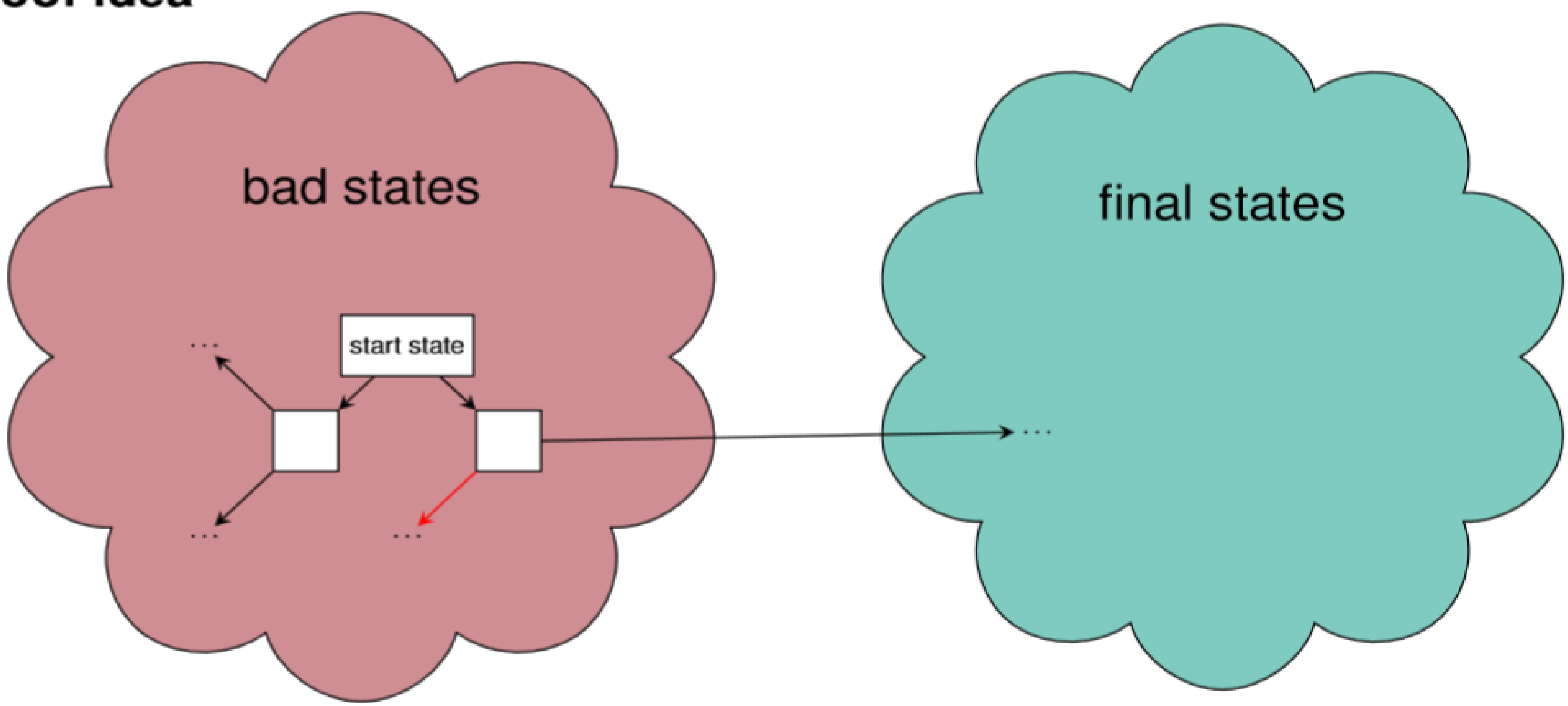
証明の概略（実際のスライド）

(1) stateの定義[KWH15]
(2) 4枚ANDのbad/final [KWH15]
(3) ucによるstate遷移

Impossibility Re

Theorem
There is no secure f

Proof Idea



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

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) 3/1 state（入力state）➡ 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）➡ final state

♥	♣	♥	♣	X_1
♥	♣	♣	♥	$1/2X_0$
♣	♥	♣	♥	$1/2X_0$

出力

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

♣♥ $= 0$ ♥♣ $= 1$

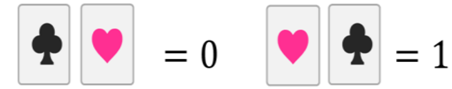
(2) bad/final stateの定義

- **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**

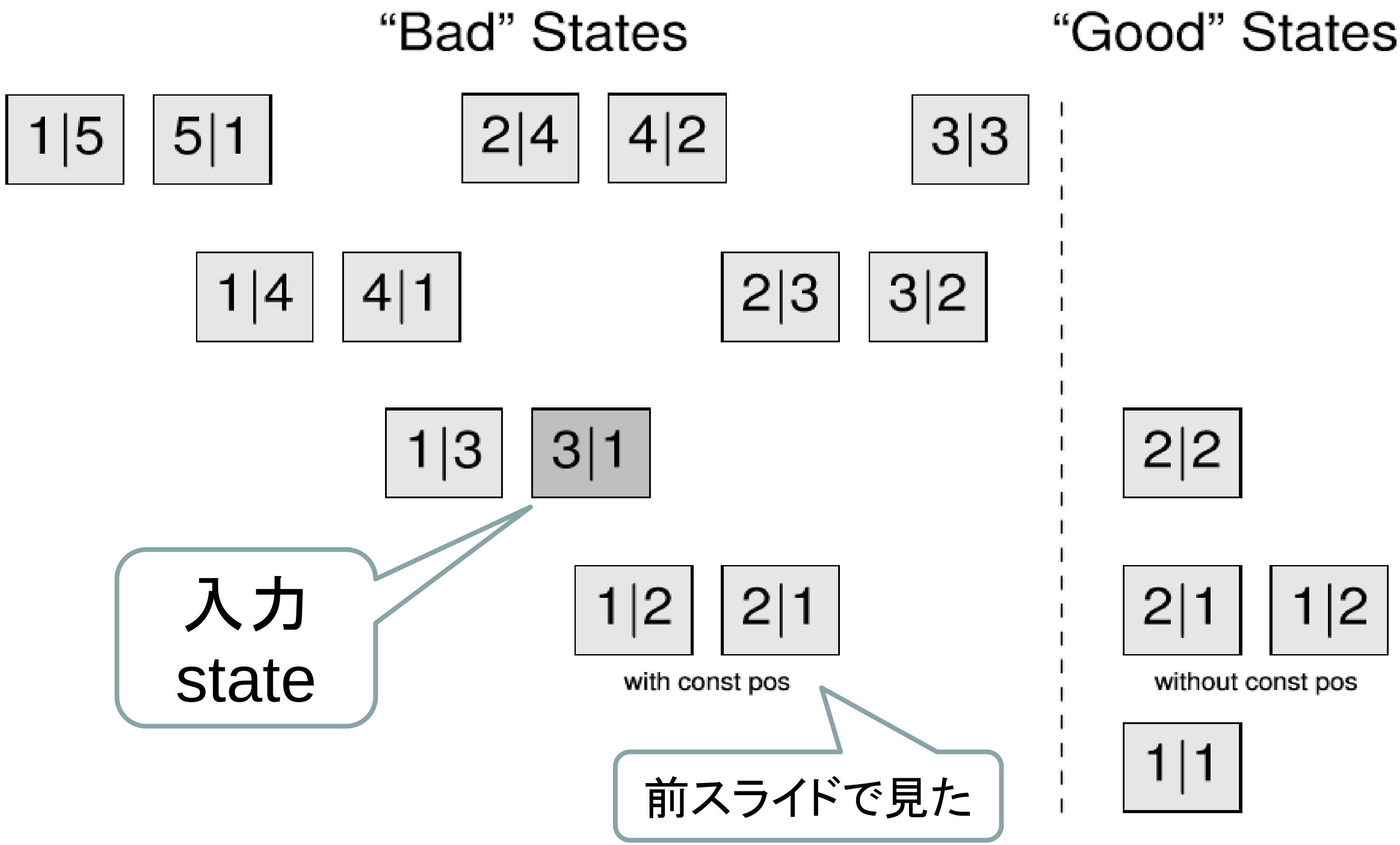
例) 2/1 state（絵柄が一致する列**有り**）➡ **bad** state

♥ ♣ ♥ ♣	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

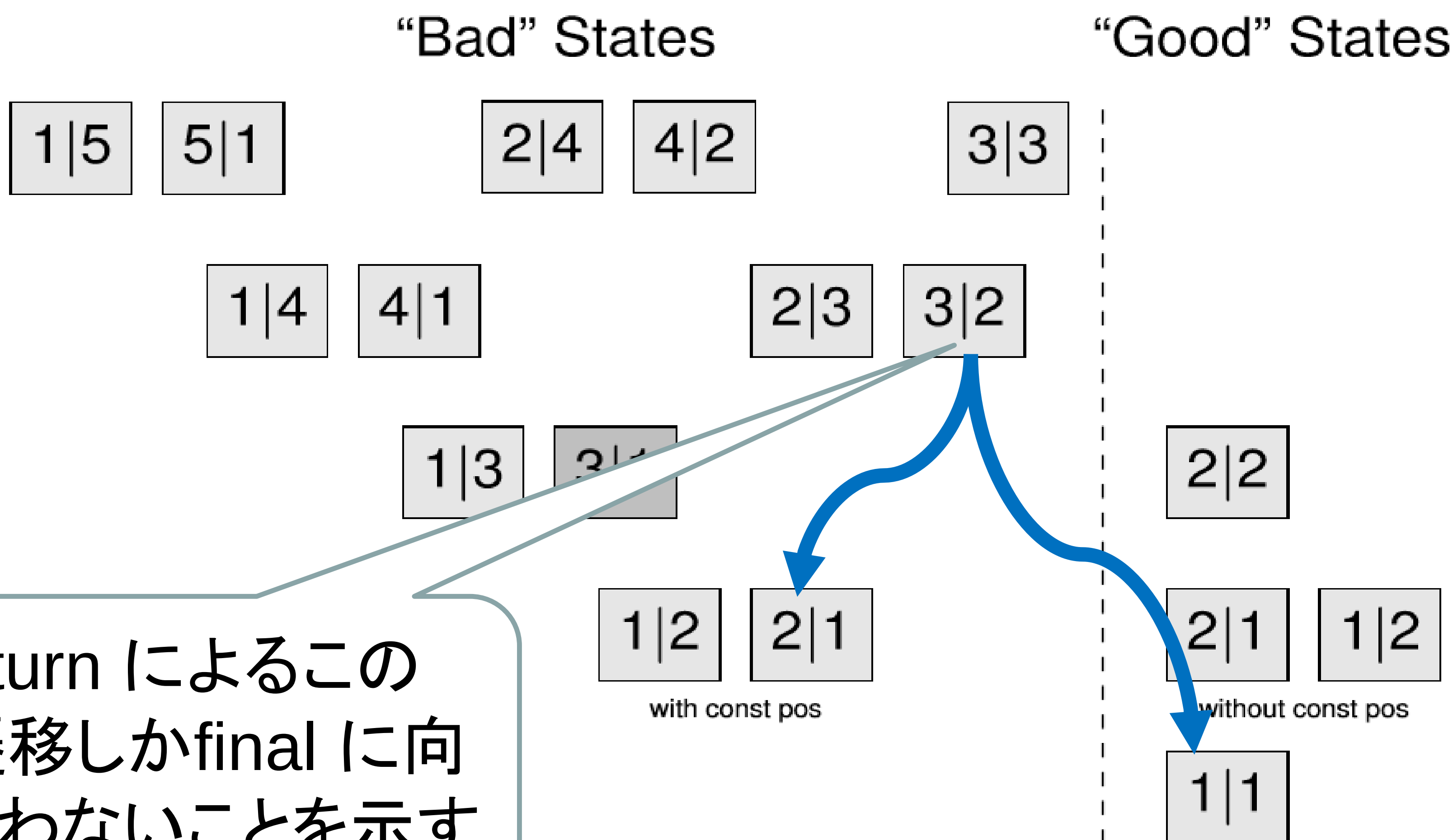


(2) 4枚ANDのbad/final stateの区分け[KWH15]より



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

(2) 4枚ANDのbad/final stateの区分け



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) シャッフルのみを用いた4枚ANDは存在しない

♣♥ = 0　♥♣ = 1

例) 3/2 ➡ 1/1, 2/1 の遷移（final はこれだけ）

4-card KWH の実際の遷移

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

turn 4

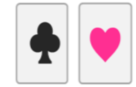
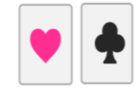
♥♣♥♣	X_1
♣♥♥♣	X_0

出力

♣♥♣♥	X_1
♣♣♥♥	$3/4X_0$
♥♣♣♥	$1/4X_0$

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

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

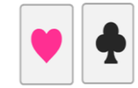
(2) turnによる遷移の考えられる全て[KWH15]より

2/3	3/3	3/3	2/4	2/4
1/1 1/2	1/1 2/2	1/2 2/1	1/2 1/2	1/3 1/1

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

2/3		3/3		3/3		2/4		2/4	
1/1	1/2	1/1	2/2	1/2	2/1	1/2	1/2	1/3	1/1

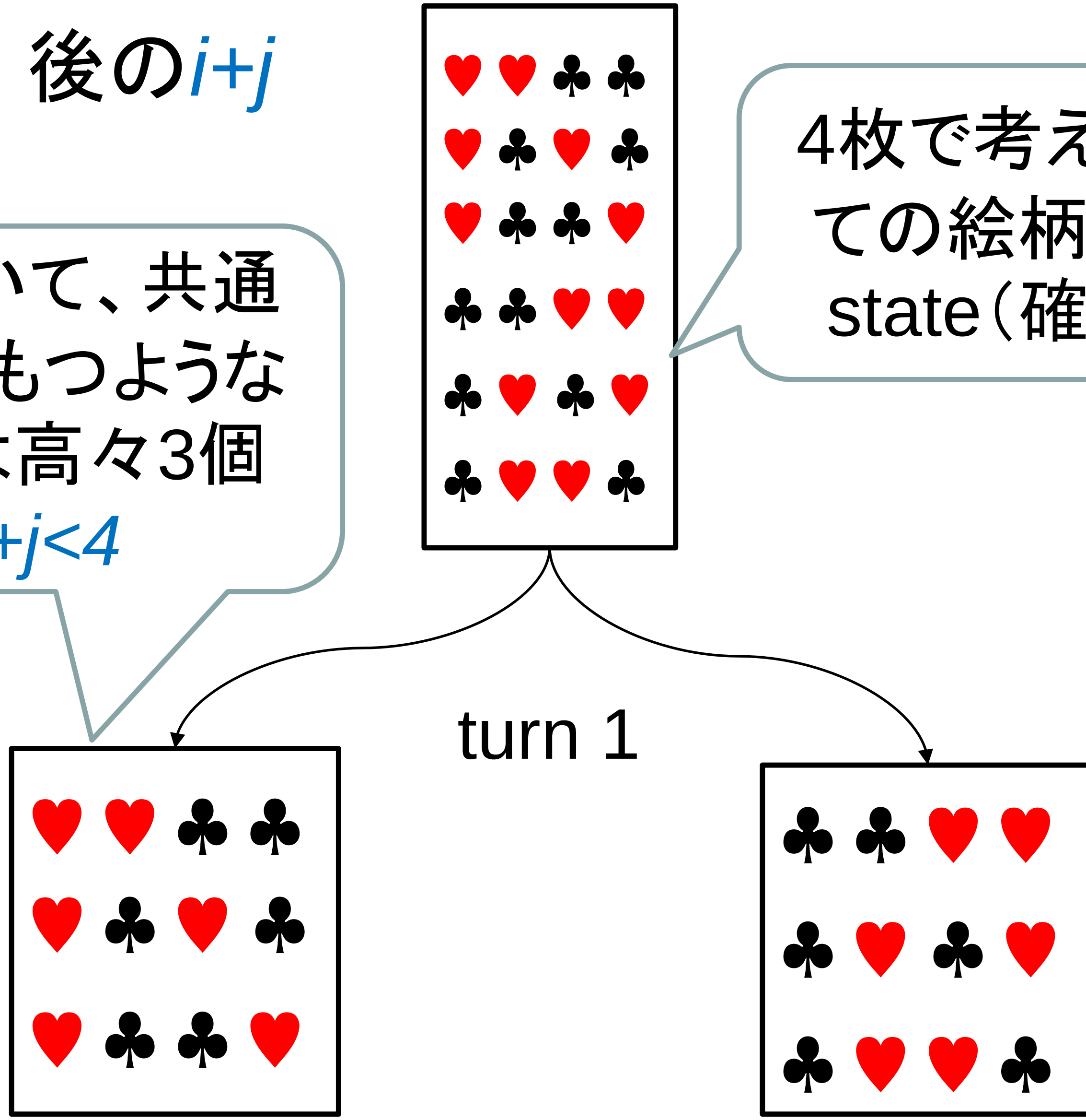
turn後は絵柄が一致するのでfinal になれないことは見た

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

♣♥ = 0　♥♣ = 1

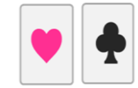
(2) turn 後の*i*+*j*



4枚で考えられる全ての絵柄を含んだstate（確率省略）

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
➡ $i+j<4$

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

$$
\begin{array}{ccccccccccccccc}
 & 2/3 & & & 3/3 & & & 3/3 & & & 2/4 & & & 2/4 & \\
 & / \quad \backslash & & & / \quad \backslash & & & / \quad \backslash & & & / \quad \backslash & & & / \quad \backslash & \\
1/1 & & 1/2 & 1/1 & & 2/2 & 1/2 & & 2/1 & 1/2 & & 1/2 & 1/3 & & 1/1
\end{array}
$$

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

(2) turnによるstateの遷移

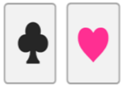
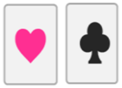
$2/3$	$3/3$	$3/3$	$2/4$	$2/4$
$1/1$ $\quad$ $1/2$	$1/1$ $\quad$ $2/2$	$1/2$ $\quad$ $2/1$	$1/2$ $\quad$ $1/2$	$1/3$ $\quad$ $1/1$

finalではない

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

有り得ない

証明の概略(実際のスライド)

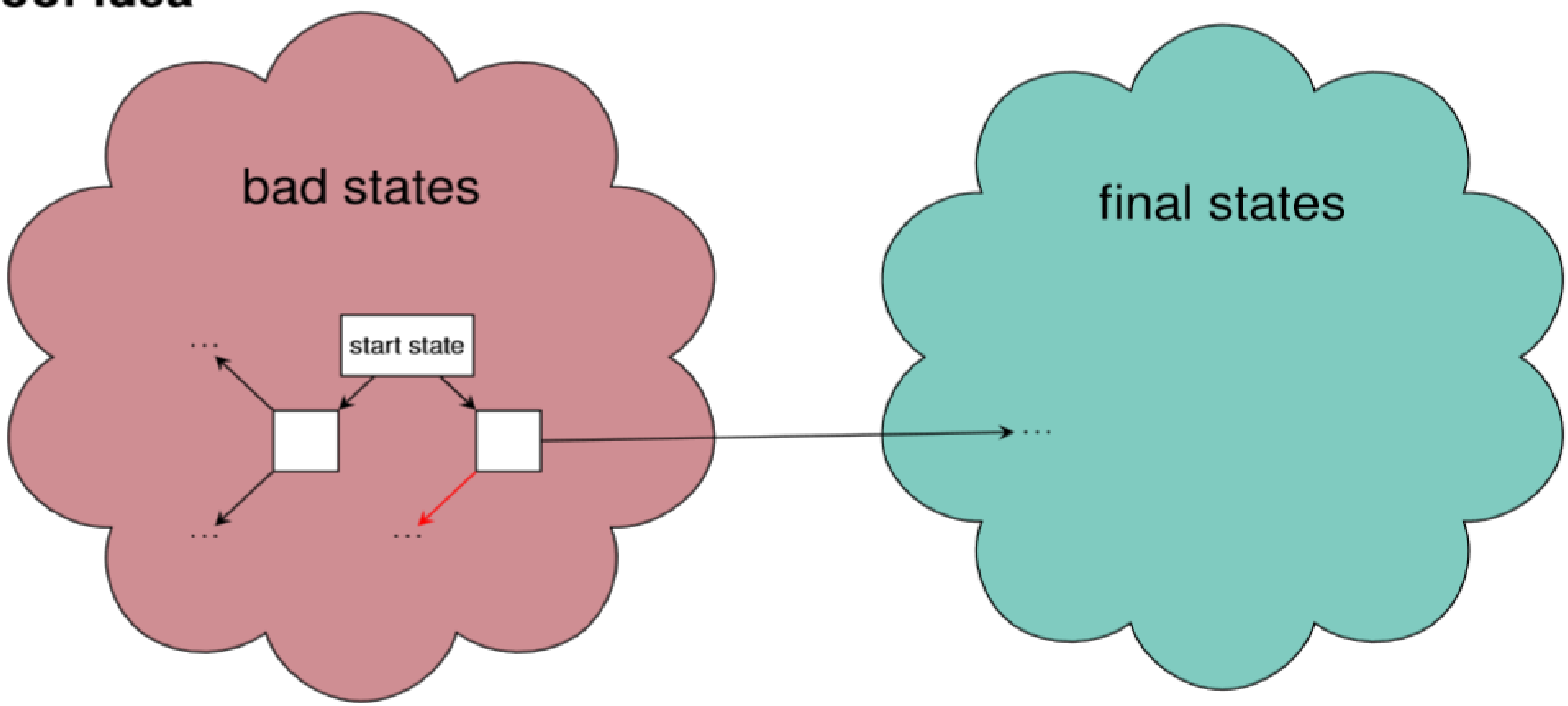
 = 0  = 1

(1) stateの定義[KWH15]
(2) 4枚ANDのbad/final [KWH15]
(3) ucによるstate遷移

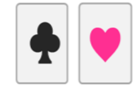
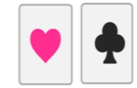
Impossibility Re

Theorem
There is no secure f

Proof Idea



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


$= 0$

$= 1$

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

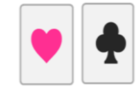
- ランダムカットは① ② を満たす

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

- ランダム二等分割カットは① ② を満たす

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

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

2/3		3/3		3/3		2/4		2/4	
1/1	1/2	1/1	2/2	1/2	2/1	1/2	1/2	1/3	1/1

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

finalではない

有り得ない

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

♣♥ $= 0$　♥♣ $= 1$

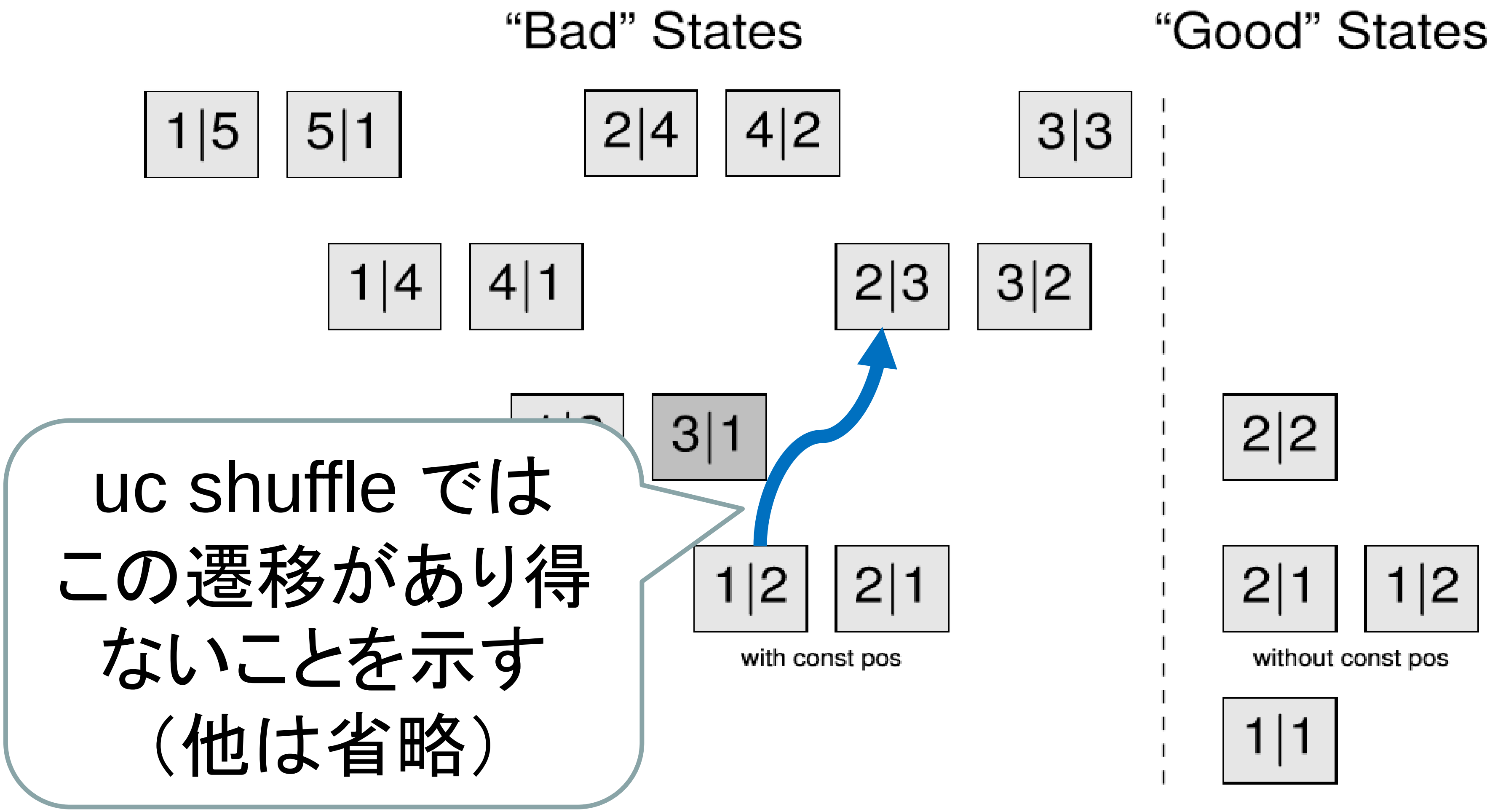
[復習] (2) turnによるstateの遷移

$2/3$		$3/3$		$3/3$		$2/4$		$2/4$	
$1/1$	$1/2$	$1/1$	$2/2$	$1/2$	$2/1$	$1/2$	$1/2$	$1/3$	$1/1$

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

(3) 4枚ANDのbad/final stateの区分け



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) 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

♣♣♥♥	X_1
♣♥♣♥	X_1
♣♥♥♣	X_0

↓

♣♥♣♥	X_1
♥♣♥♣	X_1
♣♥♥♥	X_1
♣♣♥♥	X_0
♥♣♣♥	X_0

一般性を失わずに、♥♥♣♣は2/3に含まれないと仮定

$\mathrm{shuf}, \Pi, \mathcal{F}$

Π: closed（群）

$\mathcal{F}$: uniform（均一）

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) Π: closed ➡ $\Pi \subset \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$
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) シャッフルのみを用いた4枚ANDは存在しない

♣♥ = 0　♥♣ = 1

例) $\Pi = \{\mathrm{id}, (1\ \ 3)\}$ ➡ ♥♥♣♣ が含まれるので矛盾

♣♣♥♥	X_1
♣♥♣♥	X_1
♣♥♥♣	X_0

$\downarrow$ $\mathrm{shuf}, \{\mathrm{id}, (1\ \ 3)\}$

♣♣♥♥	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) シャッフルのみを用いた4枚ANDは存在しない

♣♥ $= 0$　♥♣ $= 1$

(3) Π上で♥♥♣♣は不変でなければならない

➡ $\Pi \subset \{\mathrm{id}, (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}$

closed が効いている部分

♣♣♥♥	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

$\mathrm{shuf}, \Pi, \mathcal{F}$

Π: closed（群）

$\mathcal{F}$: uniform（均一）

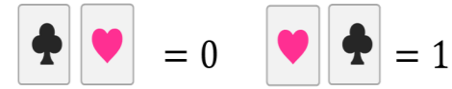
定理：uniform-closed (uc) シャッフルのみを用いた４枚ANDは存在しない　♣♥ $=0$ 　♥♣ $=1$

まとめ：

- ４枚ANDは，2/3→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



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

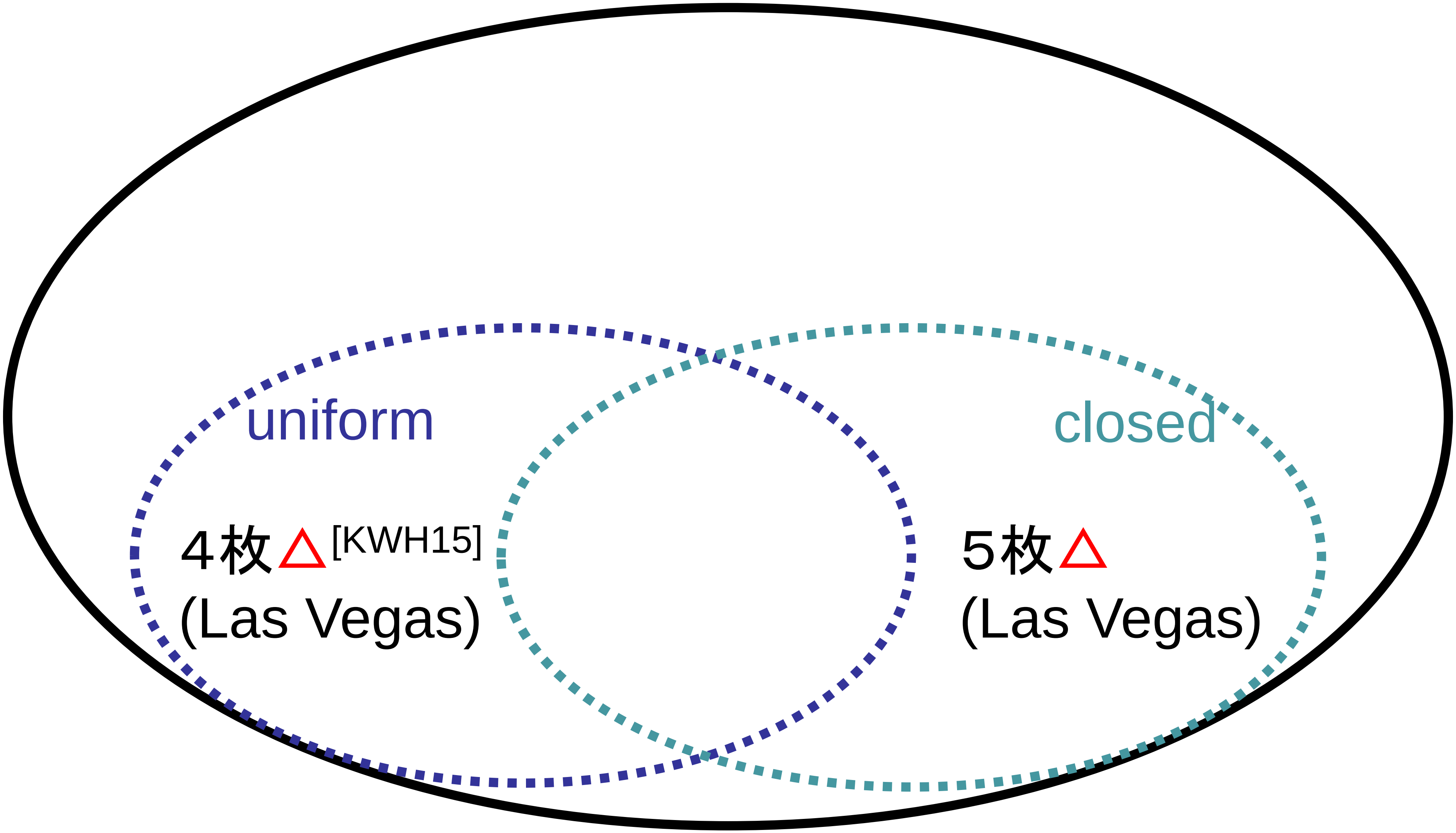
未解決問題

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

※ closedのみでも不可能

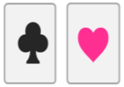
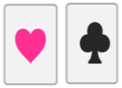
具体的なプロトコルを発見できるか？

未解決問題



下界に合うプロトコルは発見していない

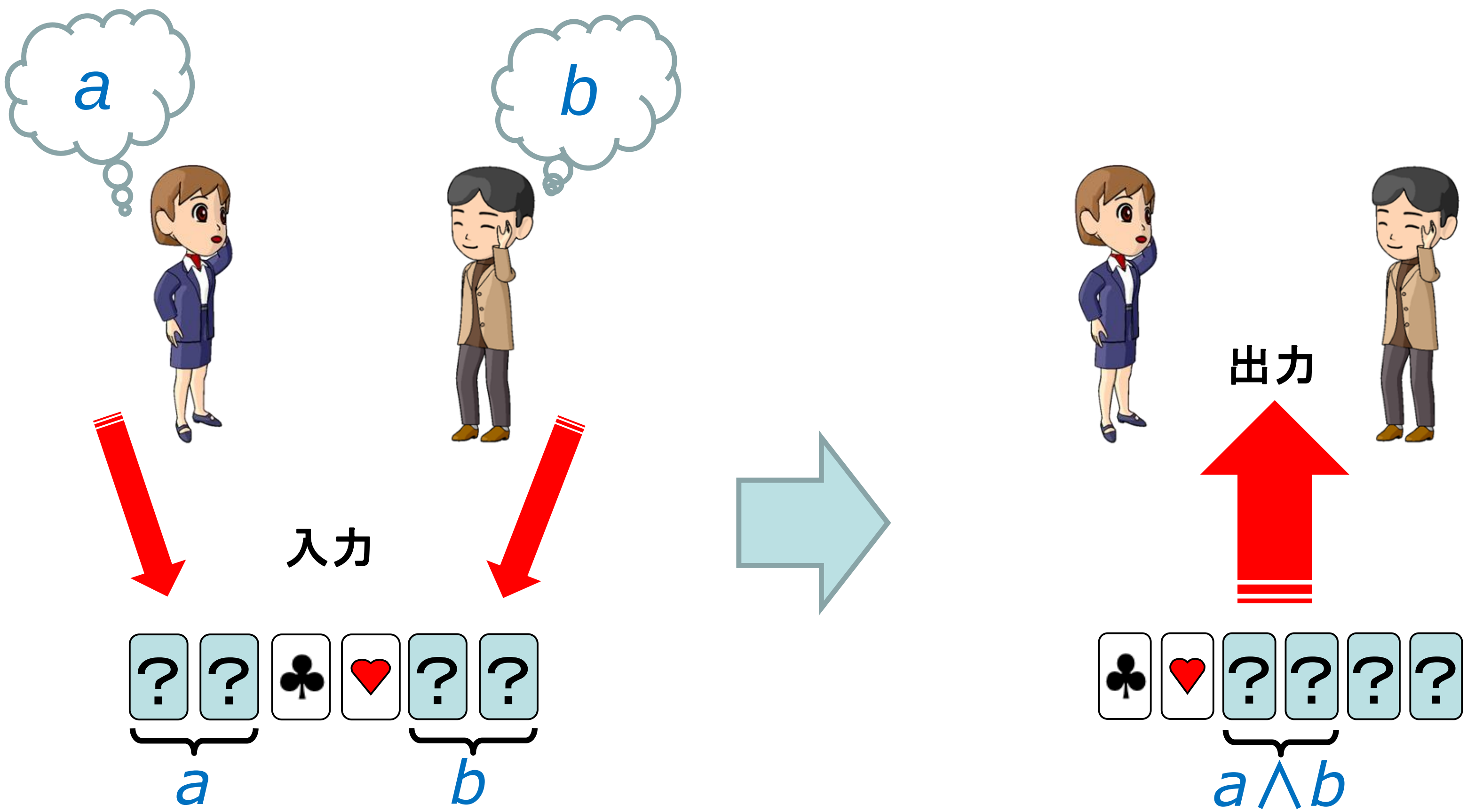
目次

 = 0  = 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

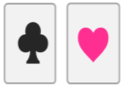
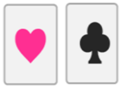
[再掲] あらまし

- 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.

任意の関数計算

 = 0  = 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
  $\mathrm{maj}(a, b, c) = (a \land b) \lor (b \land c) \lor (c \land a)$

  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

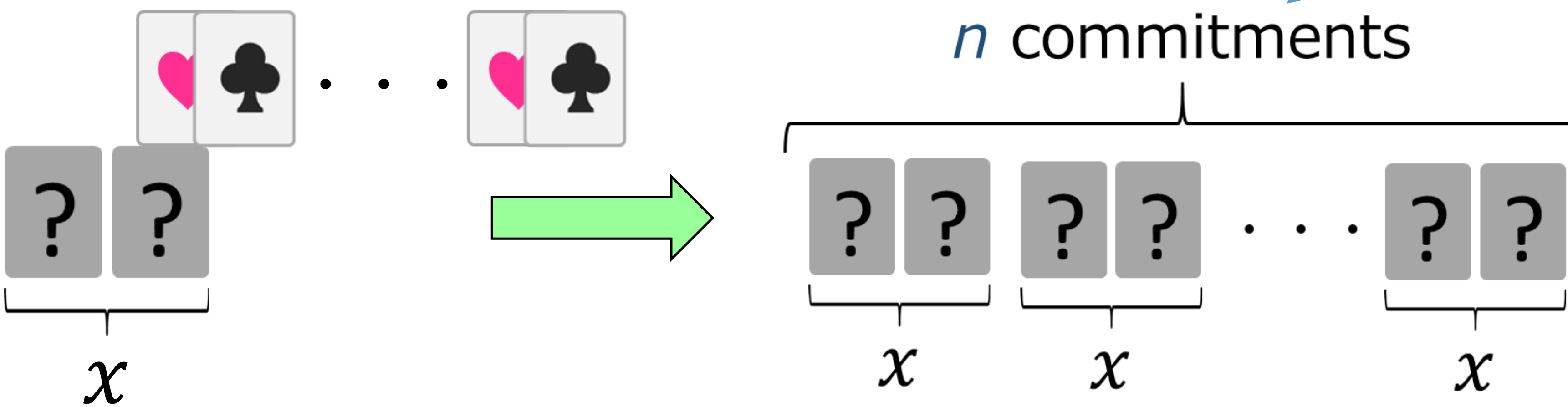
COPY protocols

✓Making n (≥2) copied commitments from an input commitment.

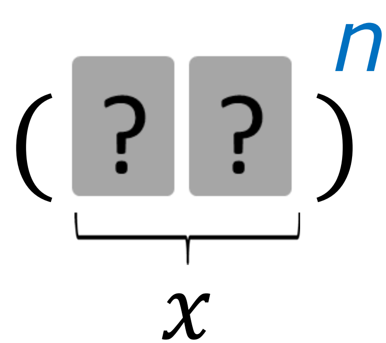
✓We sometimes write

✓Making n (≥ 2) copied commitments from an input commitment.

At least $2n$ cards are necessary.



✓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 <u>any</u> COPY protocol;
- ✓$2n+2$ cards are necessary for <u>finite-runtime</u>.

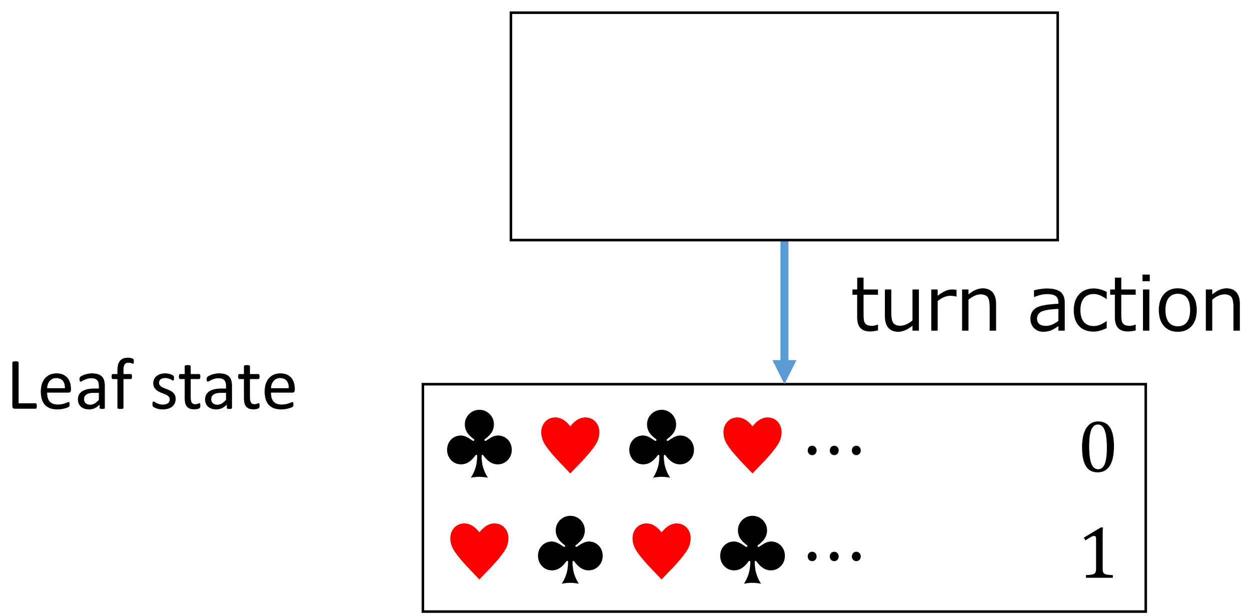
These are <u>optimal</u> in terms of the number of required cards

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

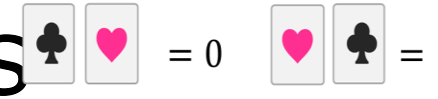
Impossibility with 2*n* cards

♣♥ = 0 ♥♣ = 1

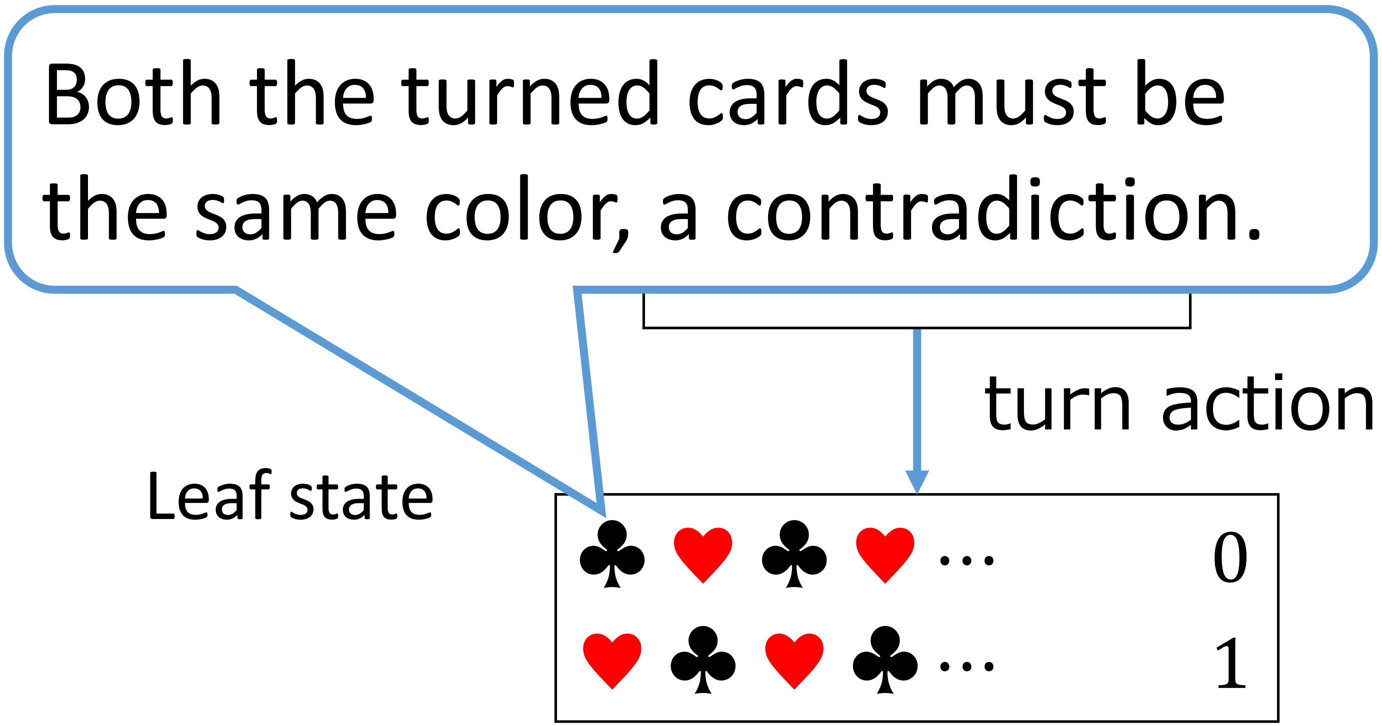
- ✓The proof outline:
  - ✓Assume the <u>existence</u> of COPY protocols with 2*n* cards,



Impossibility with $2n$ cards

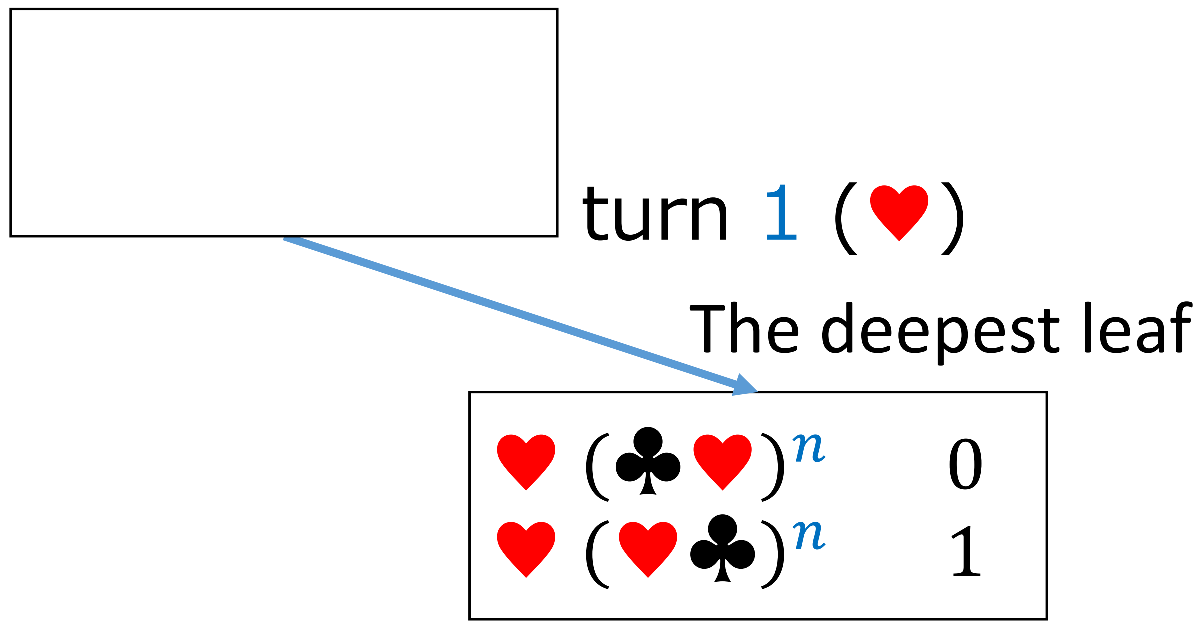


- ✓The proof outline:
  - ✓Assume the <u>existence</u> of COPY protocols with $2n$ cards,



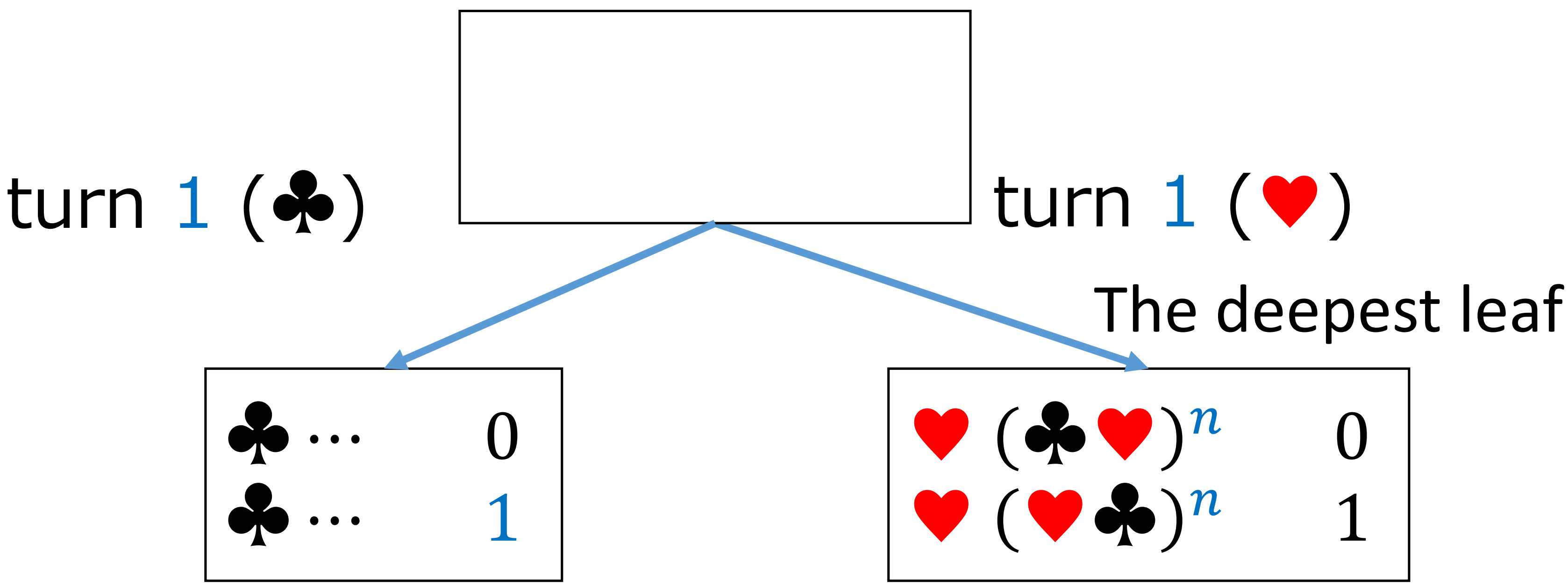
Impossibility with 2n+1 cards for finite

- ✓The proof outline:
  - ✓Assume the existence of finite COPY with ♣^{n}, ♥$^{n+1}$.
  - ✓There must be the <u>deepest</u> leaf.



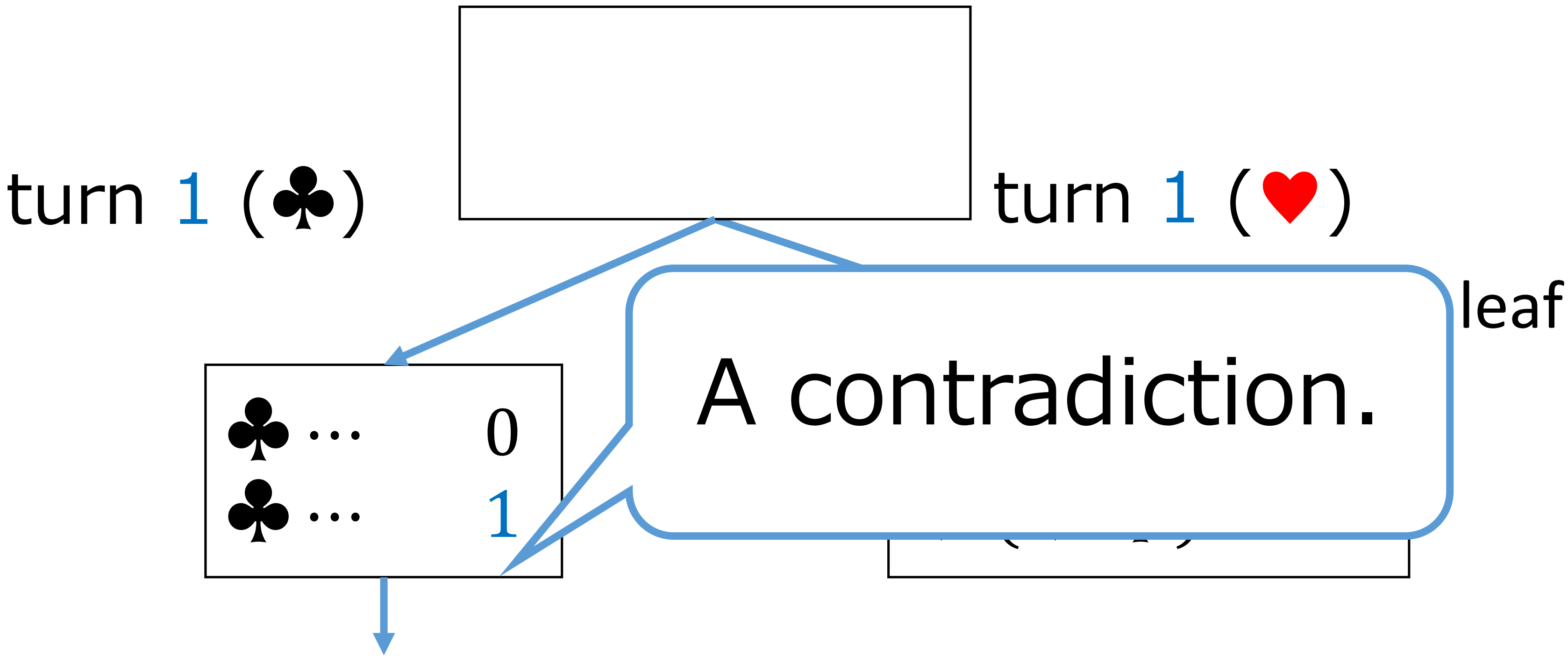
Impossibility with $2n+1$ cards for finite

- ✓The proof outline:
  - ✓Assume the existence of finite COPY with $♣^{n}$, $♥^{n+1}$.
  - ✓There must be the deepest leaf.



Impossibility with 2n+1 cards for finite

- ✓The proof outline:
  - ✓Assume the existence of finite COPY with ♣^{n}, ♥$^{n+1}$.
  - ✓There must be the deepest leaf.



- ✓Because we cannot construct n commitments with ♣$^{n-1}$ and ♥$^{n+1}$, there should be a deeper leaf.

Summary (COPY protocols)

- ✓ We showed:
  - ✓ $2n+1$ cards are required for <u>any</u> COPY protocol;
  - ✓ $2n+2$ cards are necessary for <u>finite-runtime</u>.

Thank you for your attention!

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