産学連携と数理・暗号分野連携による
カードベース暗号の深化と新境地 II

未解決問題の解決状況

電気通信大学　宮原大輝

研究集会の目的(Webサイト記載)

しかし、1つ目の軸として掲げていた**未解決問題**リストについては、その一部が2024年の後半から2025年初頭にかけて**解決**されてきている。すでに解決されている問題に新規参入者が挑戦することは機会損失であり、未解決問題リストのアップデートは緊喫の課題である。そこで最新の研究動向を把握して共有するべく短期共同研究を継続開催する判断に至った。本開催により、国内の潜在的な研究者に**最新**の研究資料および未解決問題のリストを提供することで、新規参入者の増大に寄与し、学術論文数の増大および研究領域の拡大が期待できる。

講演タイトル	発表者	解決(進展)個数
ANDプロトコルにまつわる未解決問題	水木　敬明	2
カードベースZKPプロトコル	宮原　大輝	4
カードベース暗号に登場する さまざまなカード組と符号化	品川　和雅	2
カードベース暗号に現れる数学	縫田　光司	1

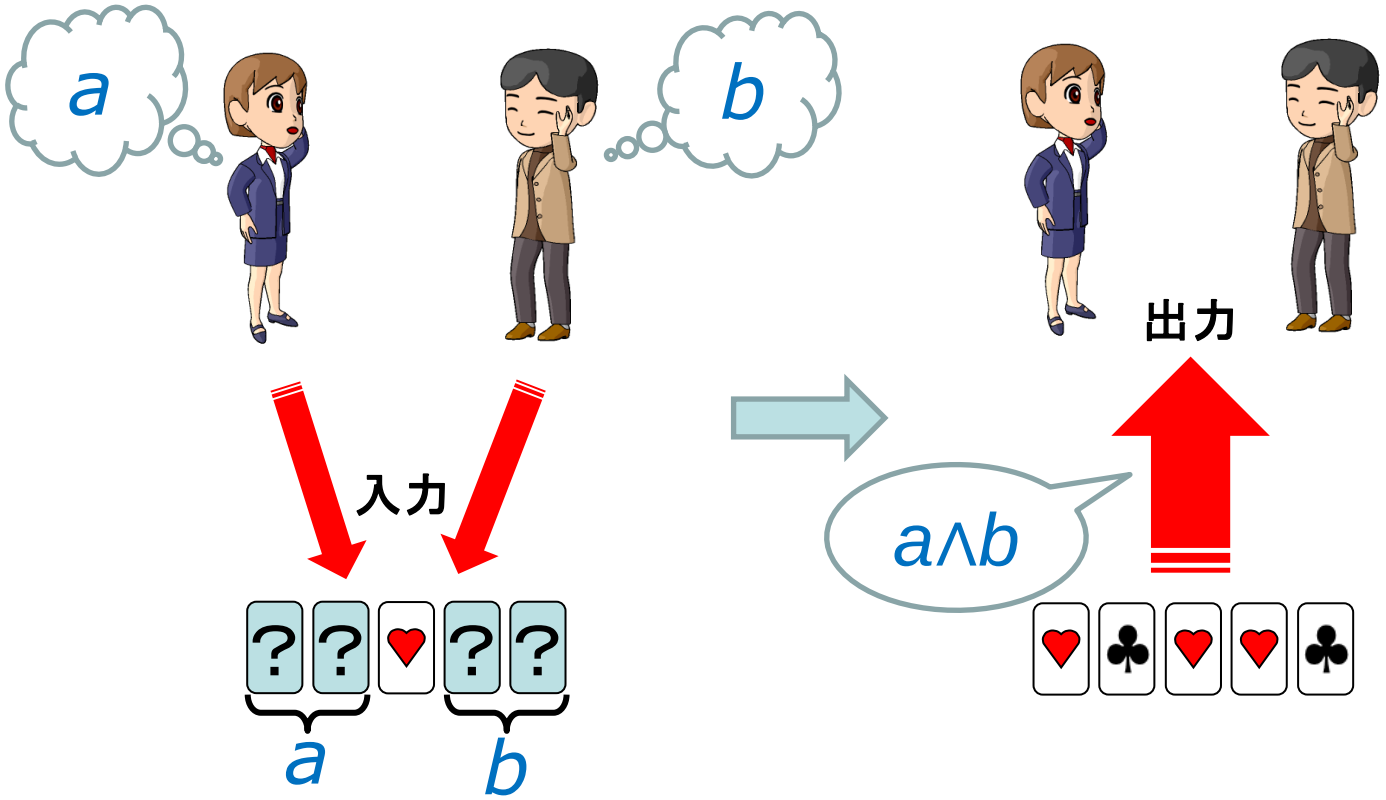
*プライベートモデルでは市販のトランプカードを用いるプロトコルの構成が2023年以降よく研究されている

解決・進展状況の外観（23年度の講演も参照されたい）

講演タイトル	問題概要	スライド#	文献
ANDプロトコルにまつわる未解決問題	4枚非コミット型ANDシャッフル1回での不可能性	p. 17	池田–品川、CSS 2024
	4枚コミット型XORのランダムカットのみでの不可能性	p. 54	Fujita–Ikeda–Shinagawa–Yoneyama、APKC 2025
カードベースZKPプロトコ（(株)ニコリが扱うパズルを対象）	数独	p. 18	TSSM、SOSA 2025 ORA+、APKC 2025
	ドッスンフワリ	p. 19	Iwamoto–Ohara、IEICE Trans. 2025
	シャカシャカ	p. 20	初貝–渡邉–岩本、SCIS 2025
	ストストーン	p. 21	大江–木谷–宇野、第202回AL研究会
カードベース暗号に登場するさまざまなカード組と符号化	n枚n入力ANDの不可能性	p. 8	飯野–李–崎山–宮原、SCIS 2025
カードベース暗号に現れる数学	領域連結性に対する非対話型ZKPの効率化	p. 26	Nuida、ePrint 2025/924

Five-Card Trickの紹介

- 1989年に提案された最初のカードベース暗号：Five-Card Trick[Boer89]
- 赤と黒の2色からなる5枚のカードを用いて、論理積（AND）を秘密計算



ルール

1. 次のようにビットを符号化する

♣ ♥ = 0, ♥ ♣ = 1

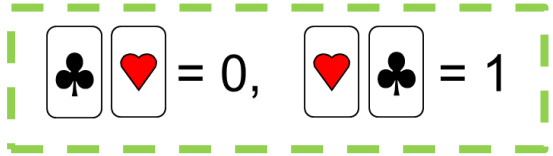
2. $x \in \{0,1\}$ のコミットメントという

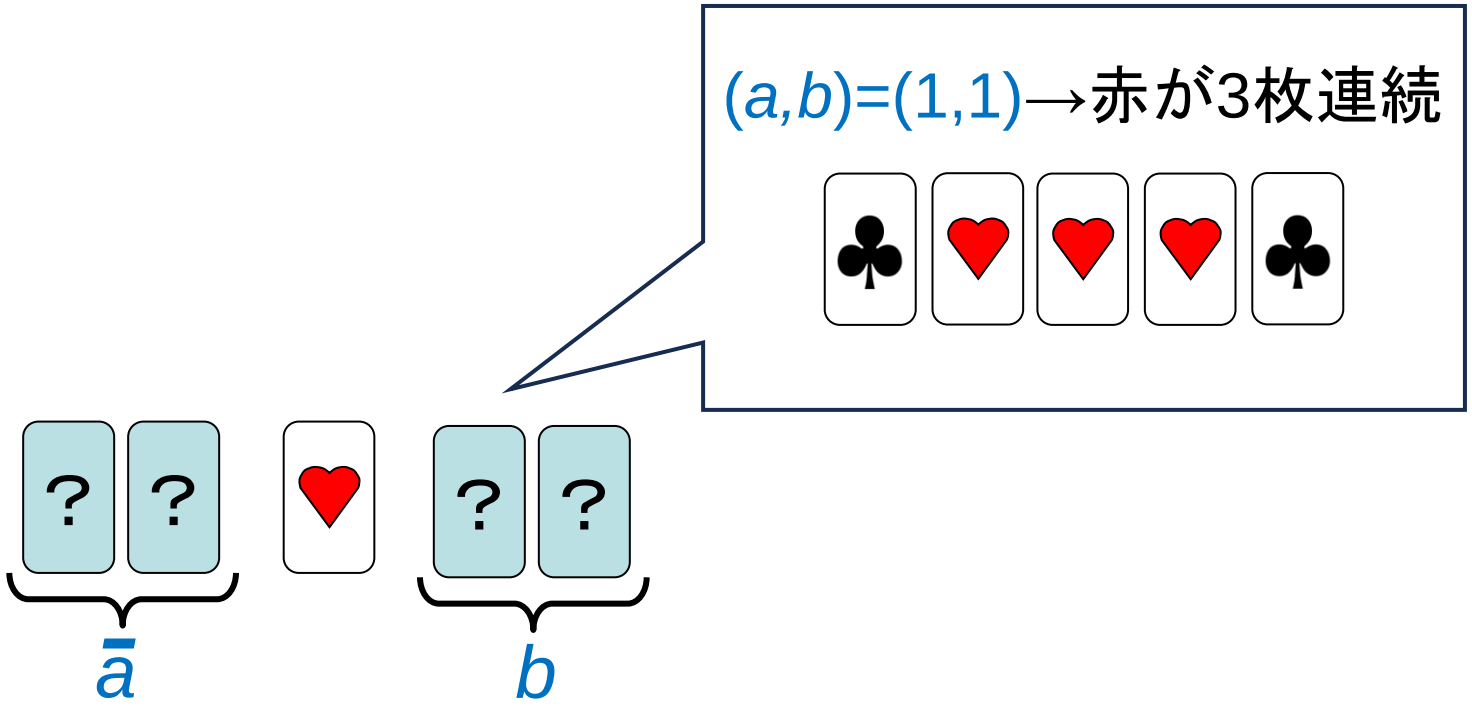
? ?

X

Five-Card Trickの手順

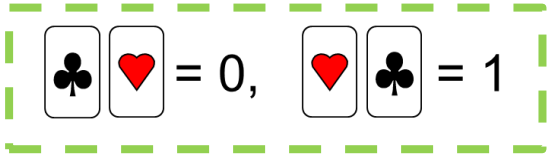
1. aのコミットメントの左右を入れ替え、$\bar{a}$のコミットメントにする

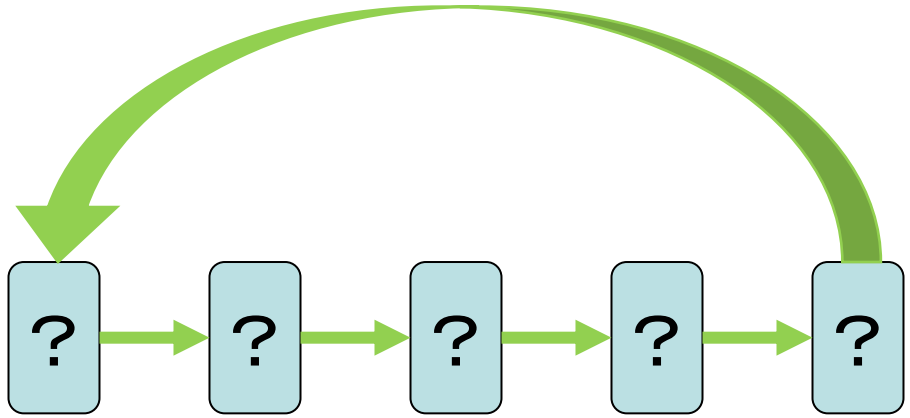




Five-Card Trickの手順

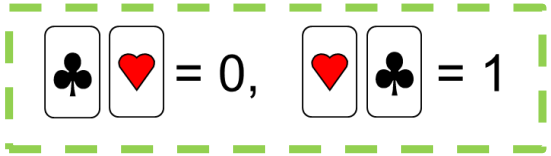
1. aのコミットメントの左右を入れ替え、$\bar{a}$のコミットメントにする
2. 5枚を巡回的にランダムにシフトさせる（**ランダムカット**）

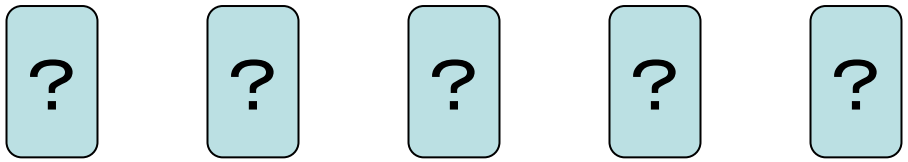




Five-Card Trickの手順

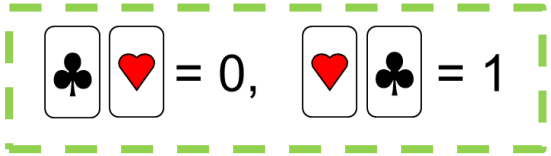
1. aのコミットメントの左右を入れ替え、$\overline{a}$のコミットメントにする
2. 5枚を巡回的にランダムにシフトさせる（**ランダムカット**）
3. 全てのカードをめくり、値だけを得る



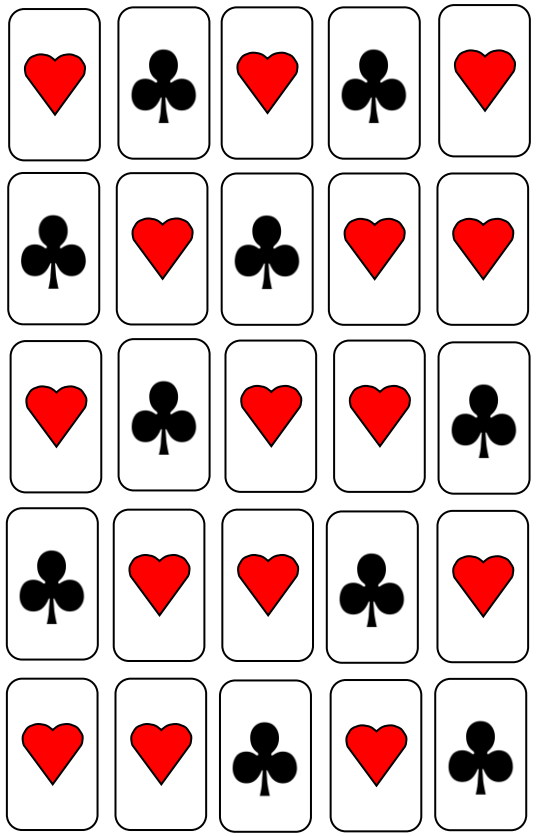


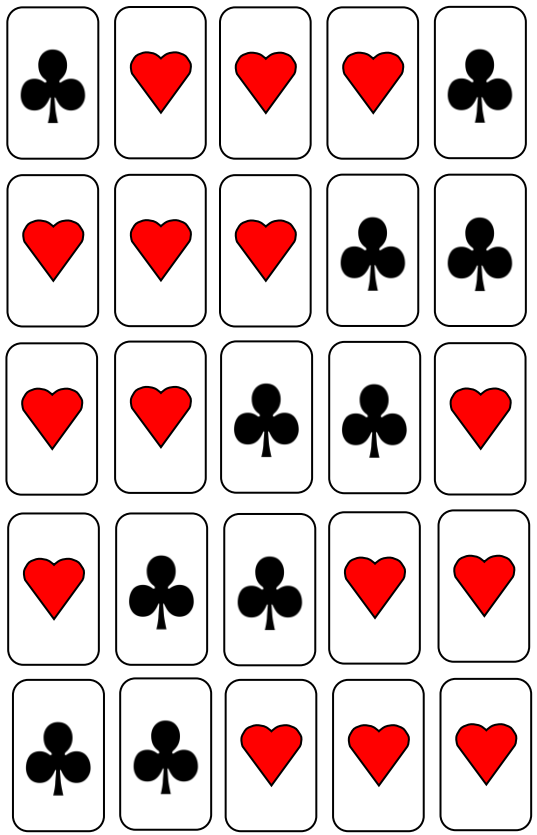
Five-Card Trickの手順

1. aのコミットメントの左右を入れ替え、$\overline{a}$のコミットメントにする
2. 5枚を巡回的にランダムにシフトさせる（**ランダムカット**）
3. 全てのカードをめくり、値だけを得る



$a \wedge b = 0$

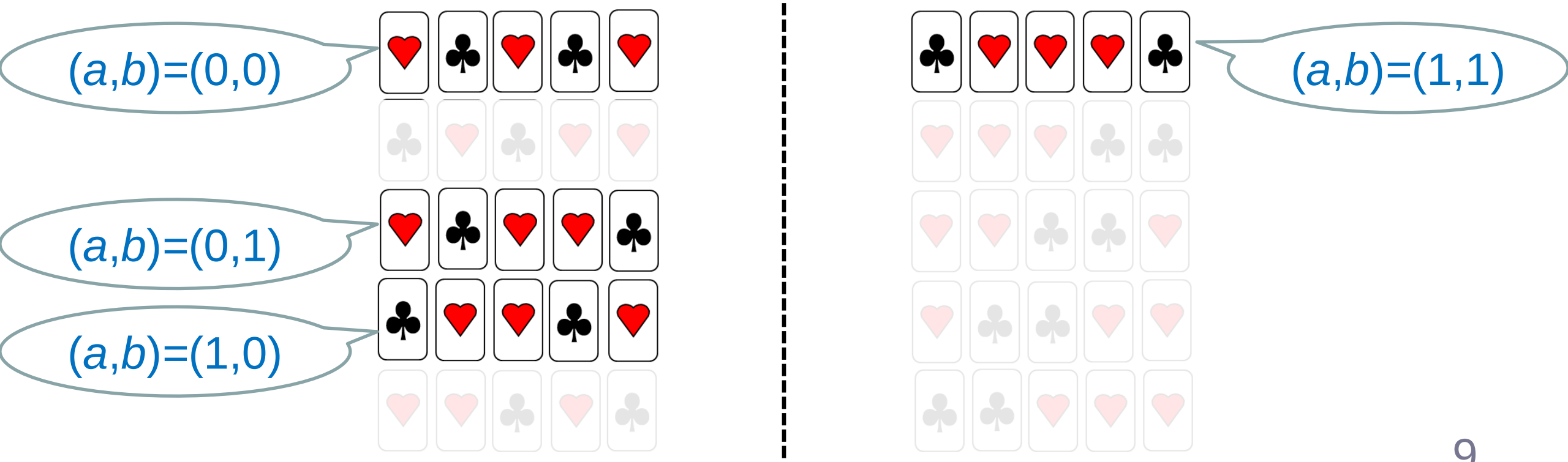




$a \wedge b = 1$

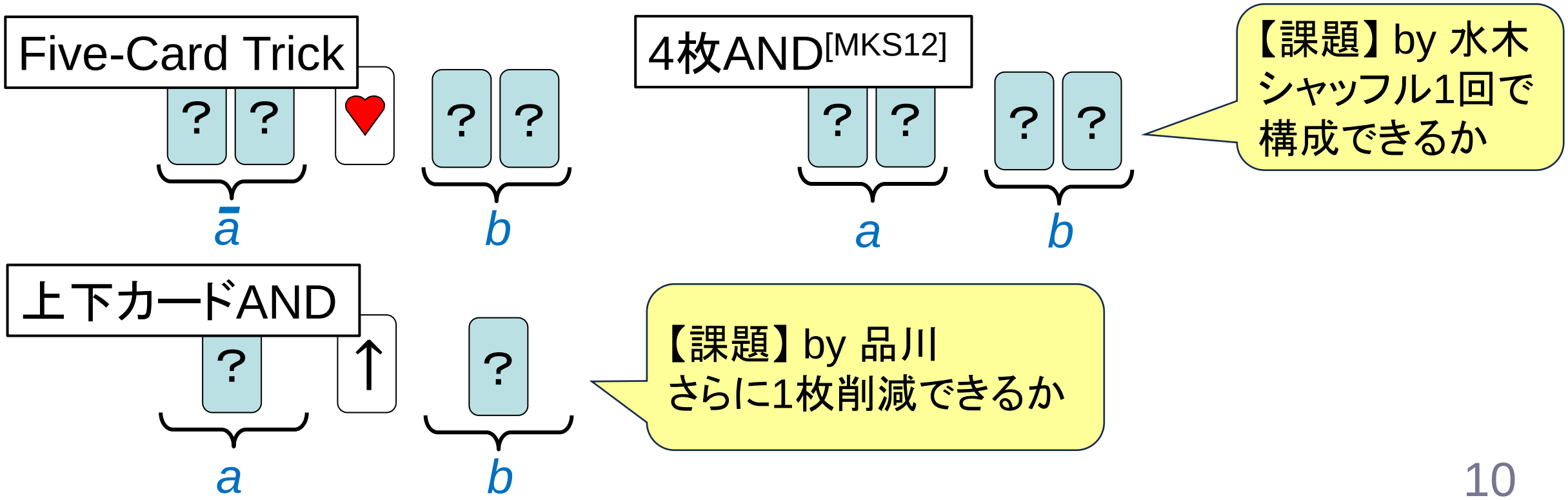
Five-Card Trickの正当性と安全性

- aのコミットメントを入れ替えることにより:
  - $(a,b)=(1,1)$ のときだけ赤が3枚連続で並ぶ
  - $(a,b)=(0,0), (0,1), (1,0)$ のときのカード列は、巡回的に同じ並びである
- ランダムカットにより、$a \wedge b$ の値だけが得られる ← 正当かつ安全



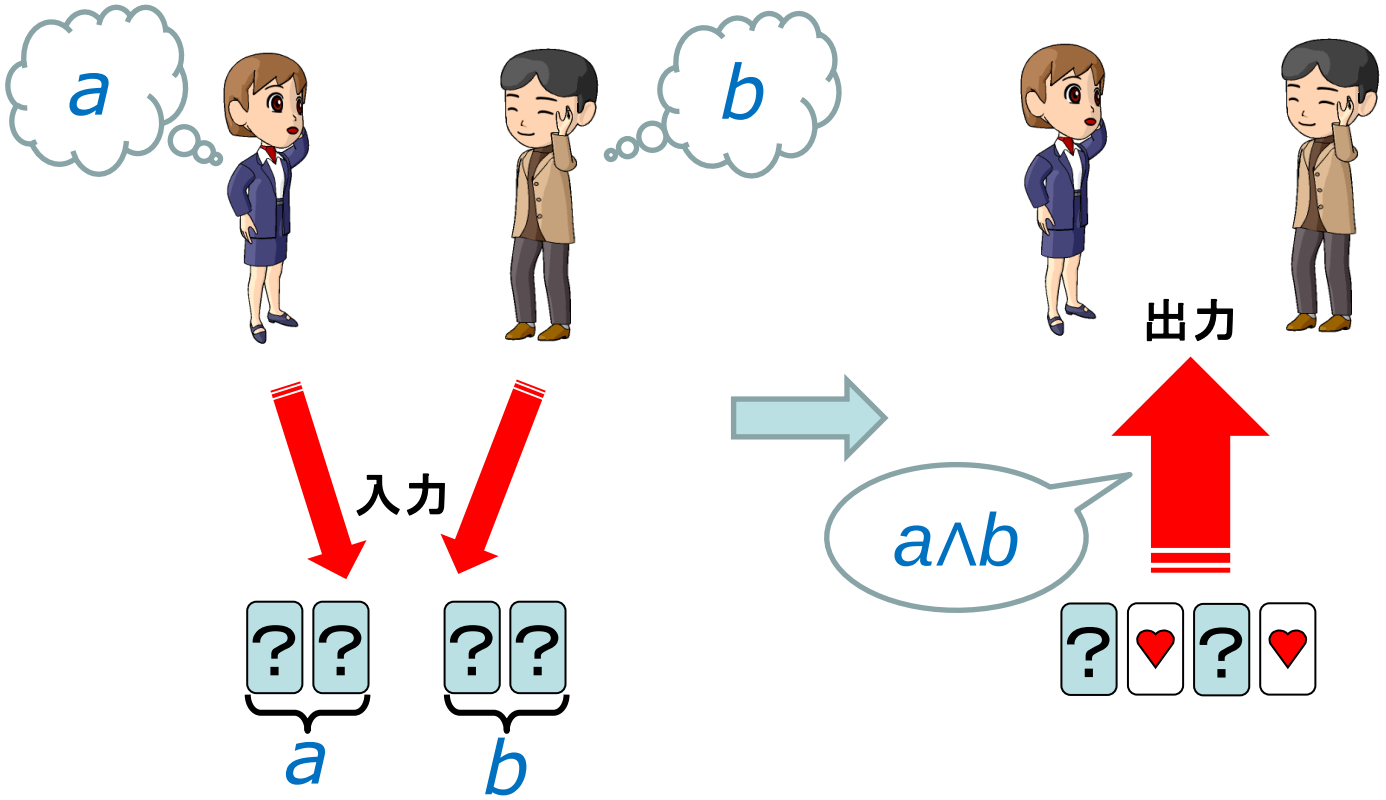
カードベース暗号の研究の方向性

- Five-Card Trickの提案後、主に2つの方向で研究がなされた
  1. カード組を用いて実現できる機能の探索（e.g., 任意の関数の計算・ZKP）
  2. 1で提案されたプロトコル（Five-Card Trick含む）の改良
- 2番目と、近年解決された課題が関連するため、主に2番を紹介する



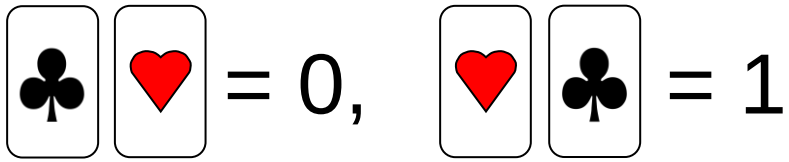
Five-Card Trick can be done with four cards

- 2012年（約20年後！）に4枚ANDプロトコルが提案された[MKS12]
- ランダムカット（RC）と**ランダム二等分割カット**（RBC）を用いる

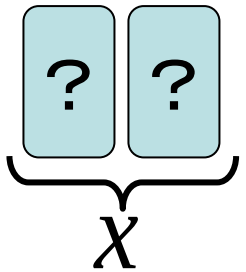


ルール

1. 次のようにビットを符号化する

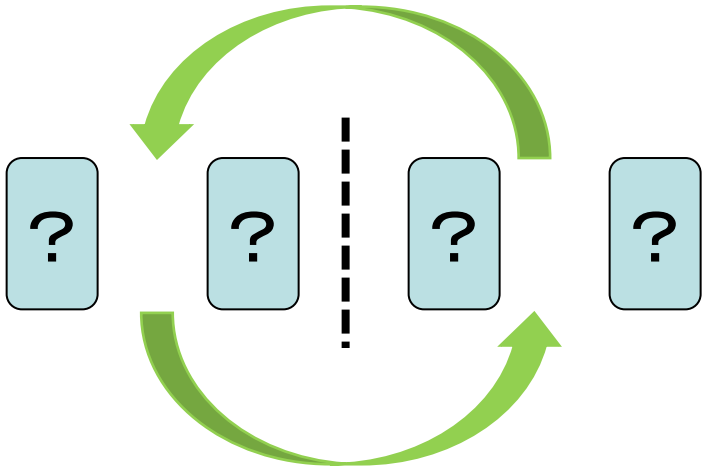


2. $x \in \{0,1\}$ の**コミットメント**という



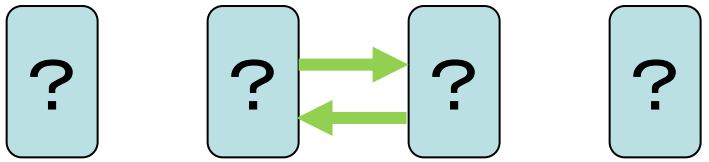
4枚ANDの手順

1. カード列を2分割して、左半分と右半分をランダムに入れ替える（RBC）



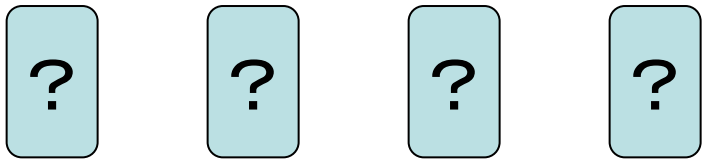
4枚ANDの手順

1. カード列を2分割して、左半分と右半分をランダムに入れ替える（RBC）
2. 真ん中2枚をランダムカットする（i.e., 単に2枚をシャッフルする）



4枚ANDの手順

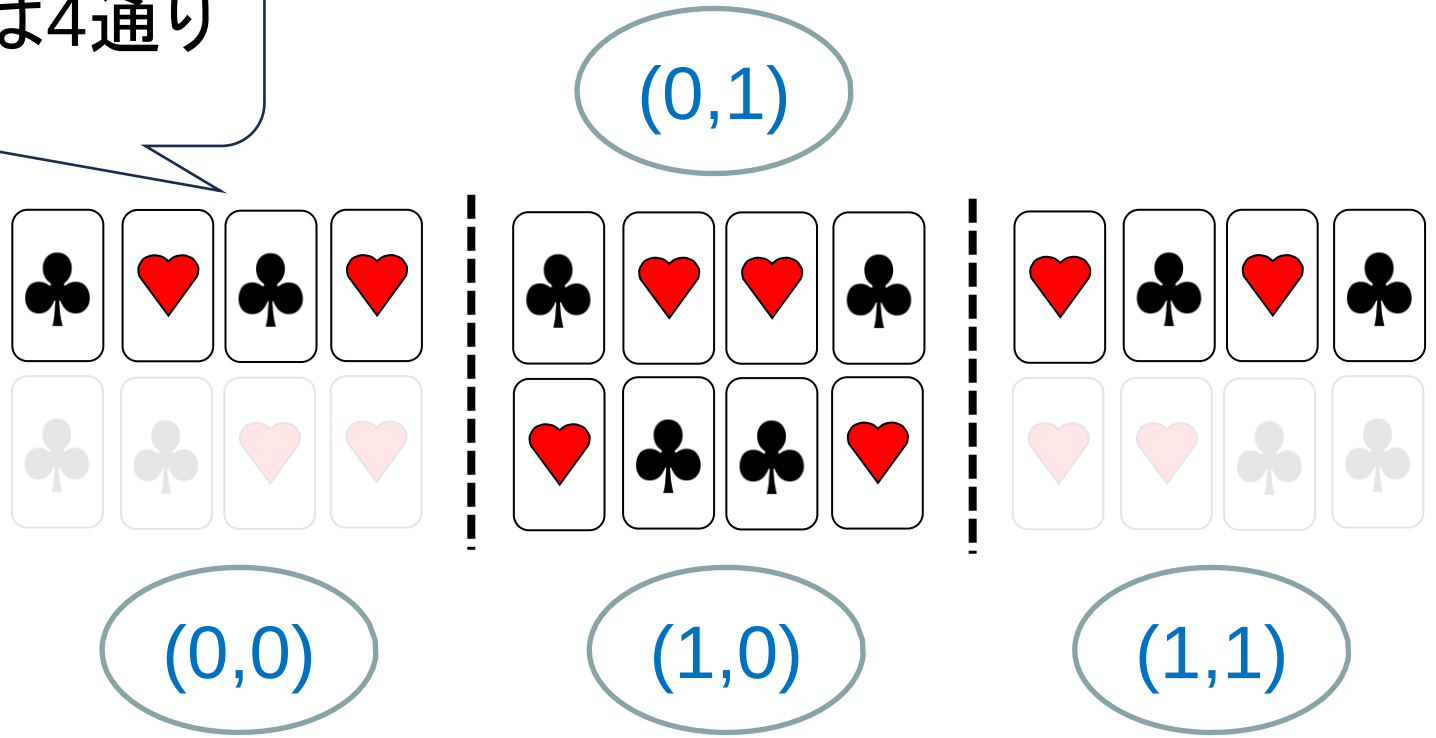
1. カード列を2分割して、左半分と右半分をランダムに入れ替える（RBC）
2. 真ん中2枚をランダムカットする（i.e., 単に2枚をシャッフルする）
3. カード列の2枚目をめくり、出た色に応じて1,4枚目をめくり、$a \wedge b$ を得る



4枚AND[MKS12]の正当性と安全性

- カード列の可能性を列挙すると、正当かつ安全なことが分かる
- 正当性・安全性の直感的な理解は興味深い

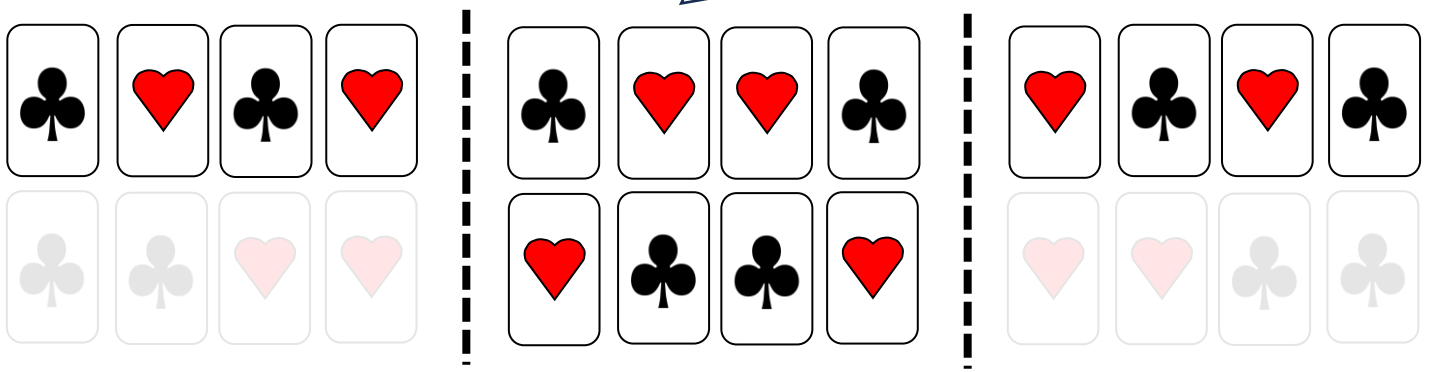
シャッフル前は4通り



4枚AND[MKS12]の正当性と安全性

- カード列の可能性を列挙すると、正当かつ安全なことが分かる
- 正当性・安全性の直感的な理解は興味深い

RBCにより、(0,1)と(1,0)の場合が混ざる（全体は4通りのまま）

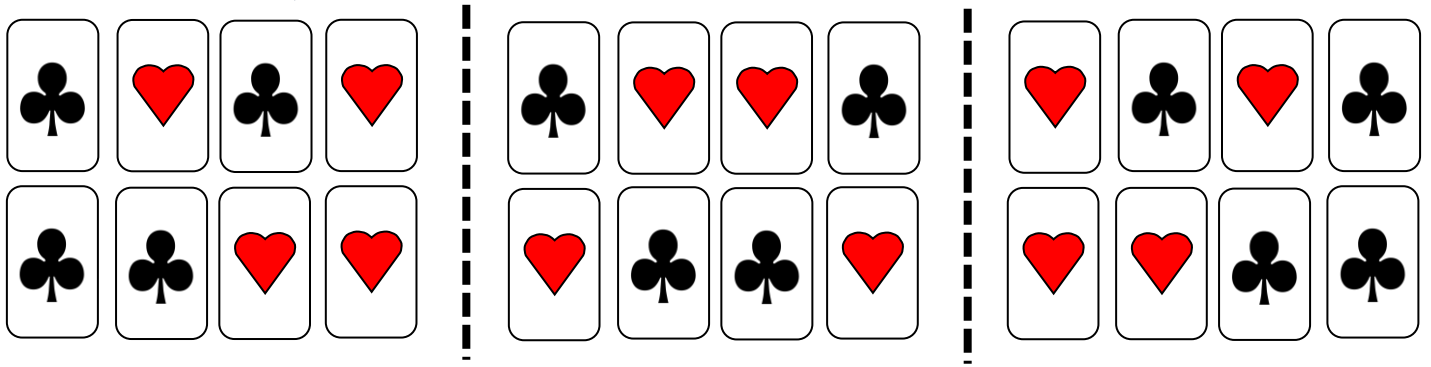


(0,0)　(0,1), (1,0)　(1,1)

4枚AND[MKS12]の正当性と安全性

- カード列の可能性を列挙すると、正当かつ安全なことが分かる
- 正当性・安全性の直感的な理解は興味深い

真ん中2枚のRCにより、全体として6通り

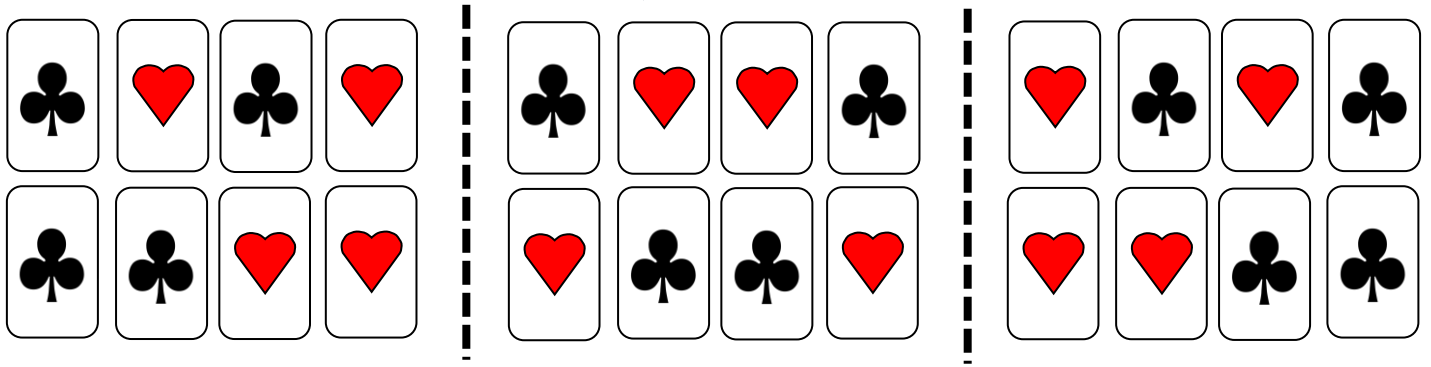


(0,0)　(0,1), (1,0)　(1,1)

4枚AND[MKS12]の正当性と安全性

- カード列の可能性を列挙すると、正当かつ安全なことが分かる
- 正当性・安全性の直感的な理解は興味深い

適切にカードをめくると、$a \wedge b$ の値だけを得られる

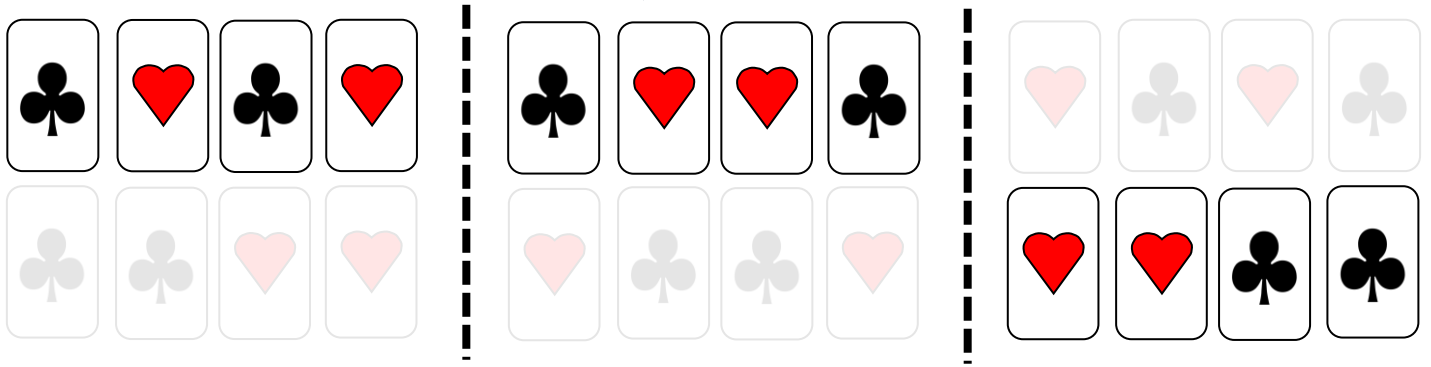


(0,0)　(0,1), (1,0)　(1,1)

4枚AND[MKS12]の正当性と安全性

- カード列の可能性を列挙すると、正当かつ安全なことが分かる
- 正当性・安全性の直感的な理解は興味深い

2枚目が赤（黒）の場合、1（4）枚目の色が$a \wedge b$ の値を表す



(0,0)

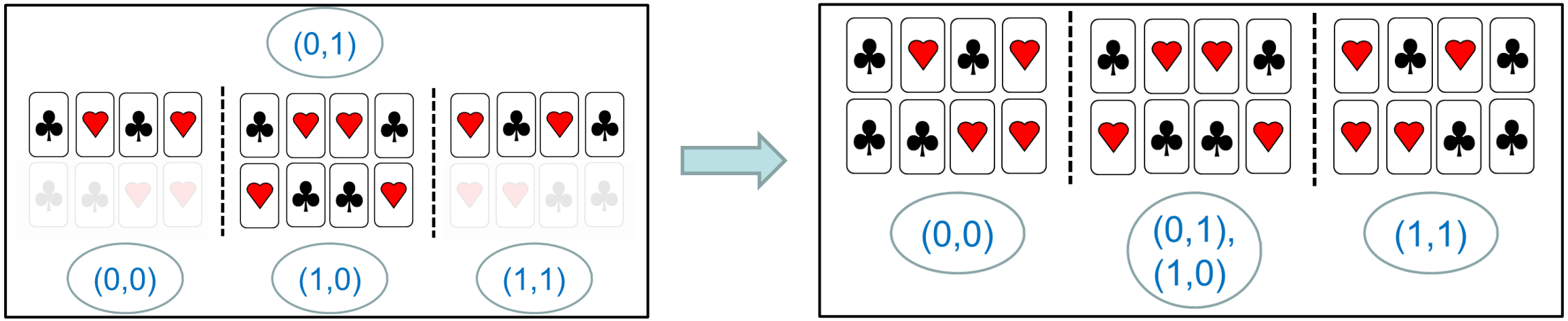
(0,1),
(1,0)

(1,1)

シャッフル回数の削減も注目されている

- 4枚ANDはRC1回とRBC1回で構成できることが分かった[MKS12]
- カード枚数は最適だが、ステップ数は削減できるかもしれない
  - ➢理論的興味として最短のステップ数を目指したい
  - ➢ステップ数（特にシャッフル回数）は実行時間の観点からも重要

RCやRBC1回のみ



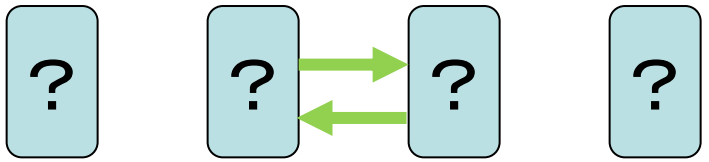
厳密に証明するためには

- カードベース暗号の計算モデルがある[MS14]
  - シャッフル：置換集合 $\Pi \subseteq S_4$ と、Π 上の確率分布 $\mathcal{F}$ によって定式化
  - すなわち、$\pi \in \Pi$ が $\mathcal{F}$ に従って選ばれ、カード列に適用される
- 例：2,3枚目をランダムに入れ替えるシャッフルを次のように書く

$$\left(\mathrm{shuf}, \{\mathrm{id}, (2\ 3)\}, \mathrm{id} \to \frac{1}{2}, (2\ 3) \to \frac{1}{2}\right)$$

一様分布の場合は省略

ただし id は巡回置換、$(2\ 3)$ は巡回置換



証明における有用な道具

- カード列の「状態」と状態遷移の定式化が便利[KWH15]
  - 状態：4枚から成るカード列が全て含まれる集合

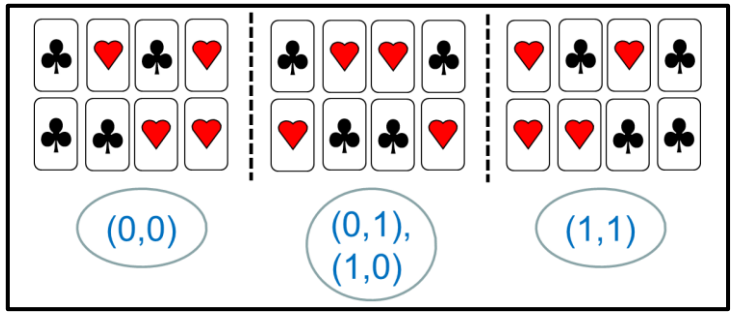
$$S := \{\clubsuit\clubsuit\heartsuit\heartsuit, \clubsuit\heartsuit\clubsuit\heartsuit, \clubsuit\heartsuit\heartsuit\clubsuit, \heartsuit\clubsuit\clubsuit\heartsuit, \heartsuit\clubsuit\heartsuit\clubsuit, \heartsuit\heartsuit\clubsuit\clubsuit\}$$

から（確率を表す）非負係数の一次斉次多項式

$$P := \left\{ \sum_{i,j\in\{0,1\}} p_{ij} \cdot X_{ij} \;\middle|\; p_{ij} \in [0,1] \right\}$$

X_{ij}は、入力が(i,j)となる確率を表す変数

への写像と定式化される



$=$

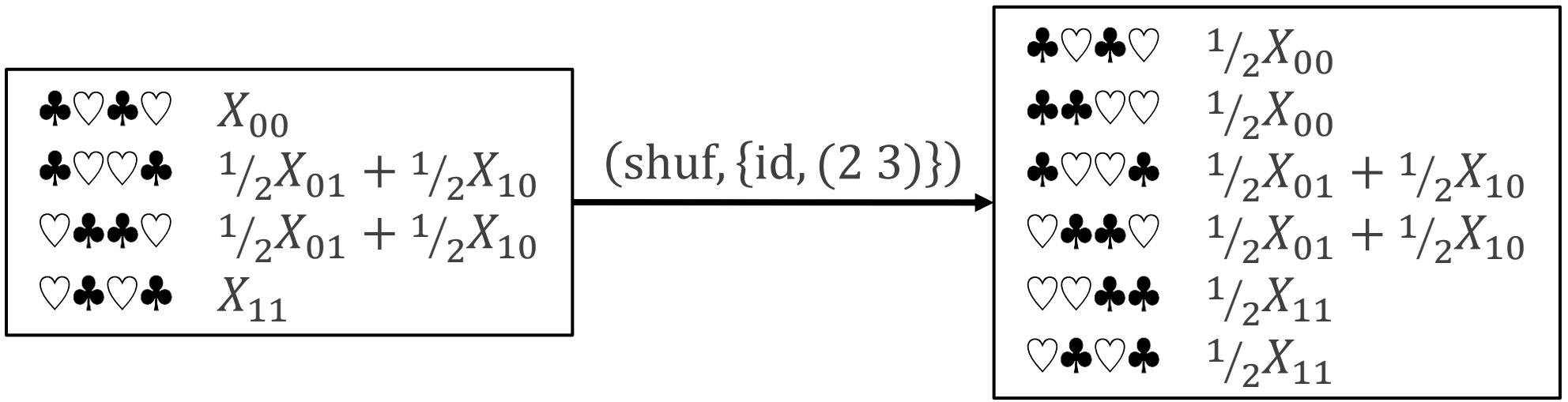
$\clubsuit\heartsuit\clubsuit\heartsuit$	$1/2 X_{00}$
$\clubsuit\clubsuit\heartsuit\heartsuit$	$1/2 X_{00}$
$\clubsuit\heartsuit\heartsuit\clubsuit$	$1/2 X_{01} + 1/2 X_{10}$
$\heartsuit\clubsuit\clubsuit\heartsuit$	$1/2 X_{01} + 1/2 X_{10}$
$\heartsuit\heartsuit\clubsuit\clubsuit$	$1/2 X_{11}$
$\heartsuit\clubsuit\heartsuit\clubsuit$	$1/2 X_{11}$

証明における有用な道具

- カード列の状態と「状態遷移」の定式化が便利[KWH15]
  - 状態 $\mu: S \to P$ から $\mu': S \to P$ に $(\mathrm{shuf}, \Pi, \mathcal{F})$ によって遷移すると、$s \in S$ に対して

$$\mu'(s) = \sum_{\pi \in \Pi} \mathcal{F}(\pi) \cdot \mu\left(\pi^{-1}(s)\right)$$

のように μ' を記述できる

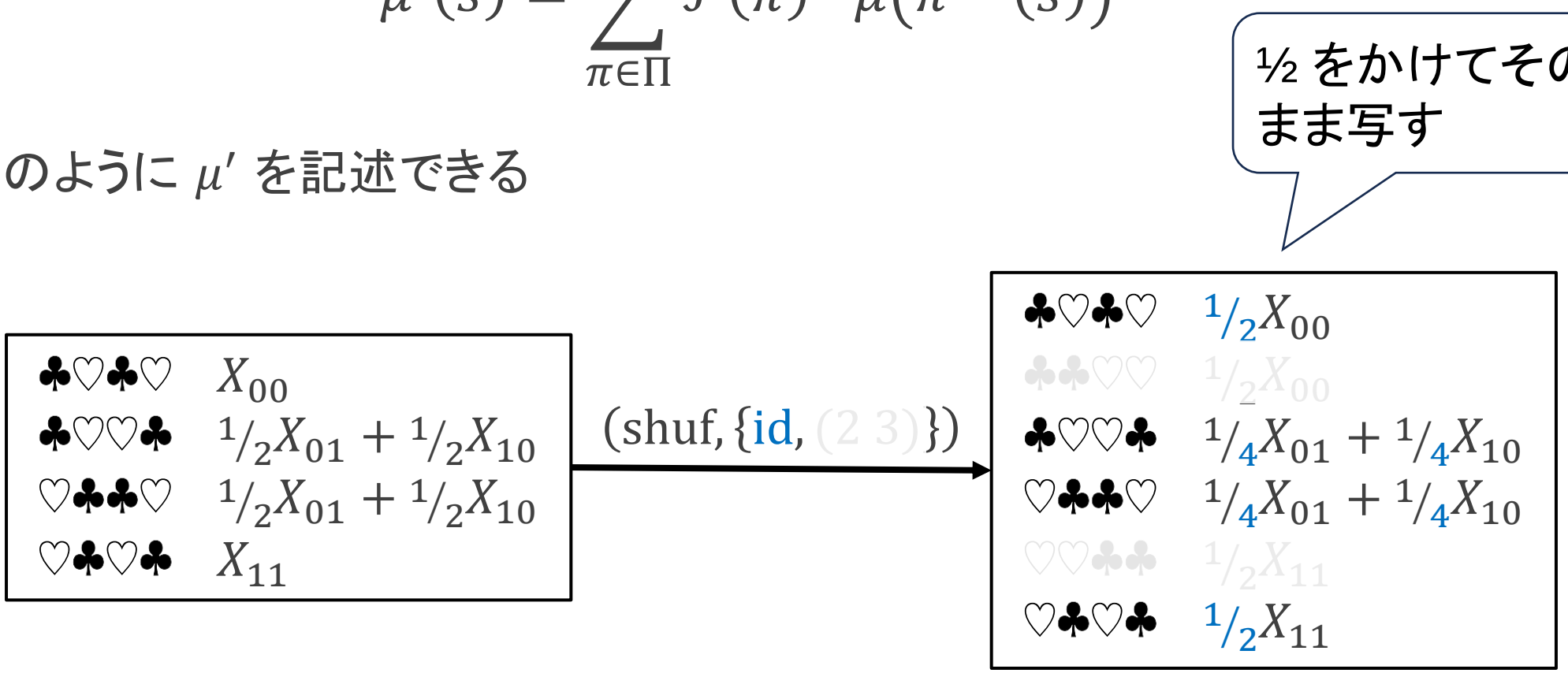


証明における有用な道具

- カード列の状態と「状態遷移」の定式化が便利[KWH15]
  - 状態 $\mu: S \to P$ から $\mu': S \to P$ に $(\mathrm{shuf}, \Pi, \mathcal{F})$ によって遷移すると、$s \in S$ に対して

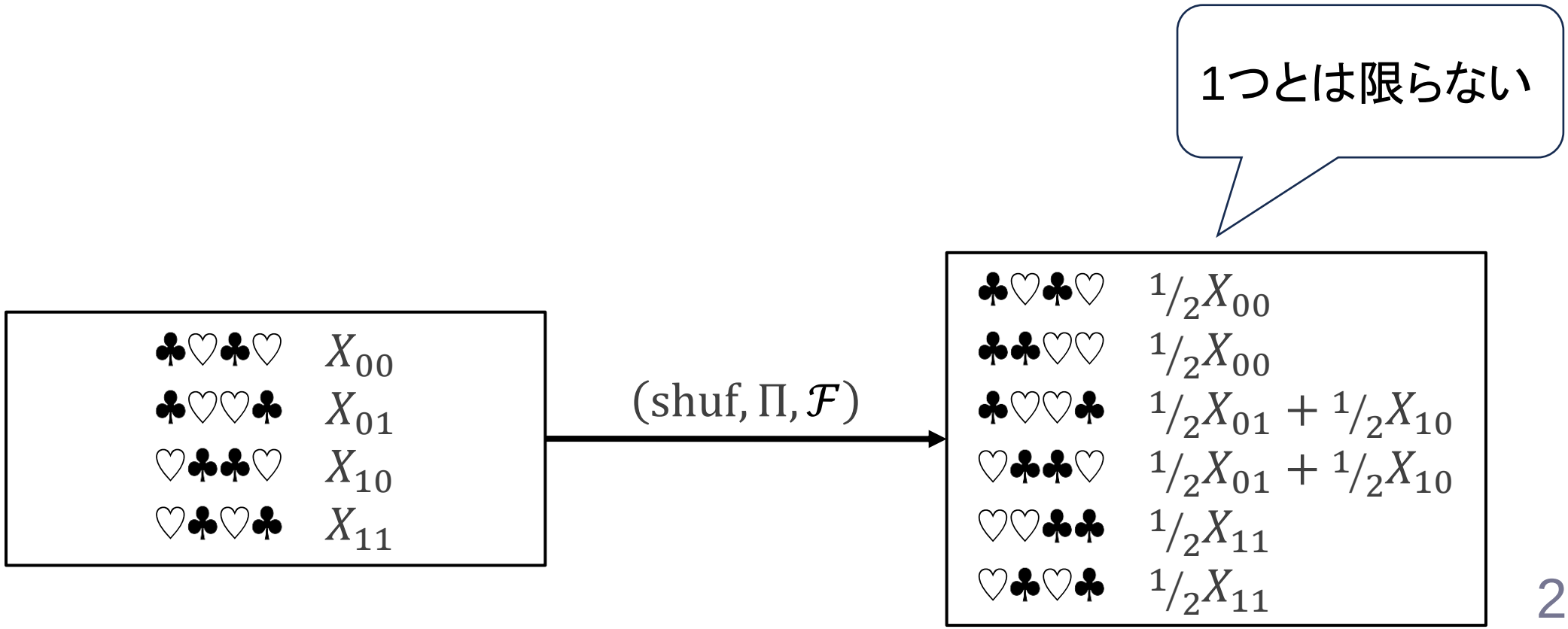
$$\mu'(s) = \sum_{\pi \in \Pi} \mathcal{F}(\pi) \cdot \mu\left(\pi^{-1}(s)\right)$$

のように μ' を記述できる



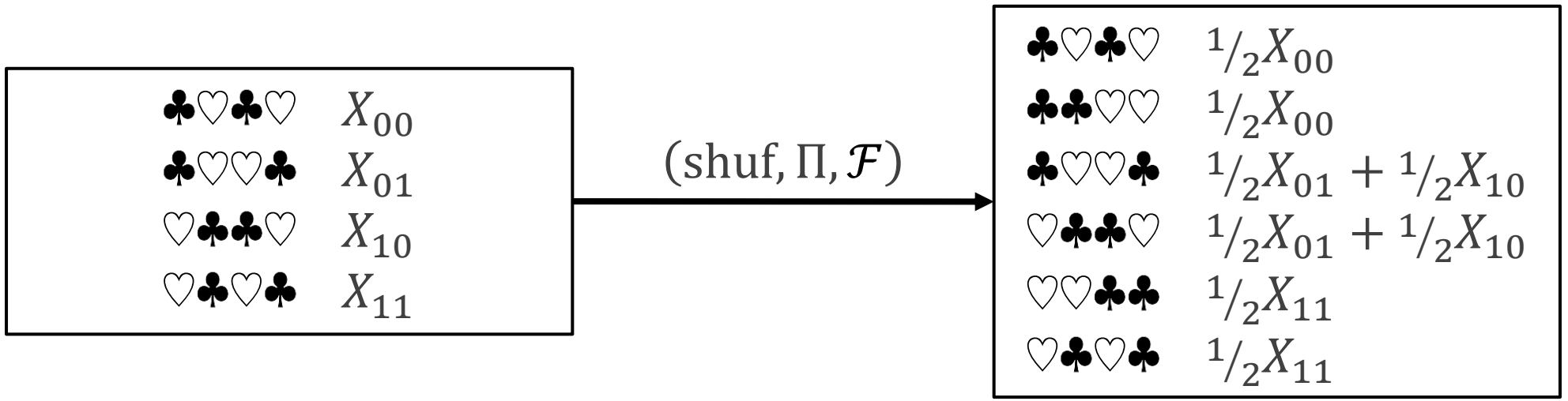
証明の定式化と進展

- 初期状態から、1回のシャッフル $(\mathrm{shuf}, \Pi, \mathcal{F})$ で到達できるか
  - $\Pi = \{\mathrm{id}, (1\ 2\ 4\ 3)\}$ であれば可能、ただし実装が難しい
  - $\Pi^2 = \Pi$、すなわち集合が閉じている場合は実装が易しい[KWH15]



4枚（非コミット型）ANDはシャッフル1回では不可能

- 池田–品川、CSS 2024で**解決**
  - 閉じている Π を全て列挙（30個！）し、一様分布の場合を全通り試した
  - 30個で十分な理由・類似の遷移を省略など、証明を効率化する工夫がある
  - 安全かつ正当にカードをめくられる状態の定式化も必要
- さらに強い結果：閉じている場合は任意の確率分布でも1回では不可能
  - 正当性から $\Pi = 2 \to \mathcal{F}\colon \mathrm{id} \to p, \pi \to 1 - p$ として証明
- 【課題】任意のサイズの閉じている Π を機械的に記述できるか？



[再掲] カードベース暗号の研究の方向性

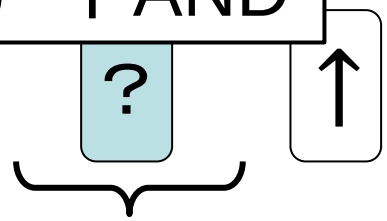
- Five-Card Trickの提案後、主に2つの方向で研究がなされた
  1. カード組を用いて実現できる機能の探索（e.g., 任意の関数の計算・ZKP）
  2. 1で提案されたプロトコル（Five-Card Trick含む）の改良
- 2番目と、近年解決された課題が関連するため、主に2番を紹介する

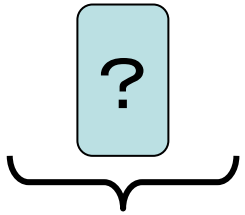
Five-Card Trick

4枚AND[MKS12]

【課題】by 水木
シャッフル1回で
構成できるか

上下カードAND

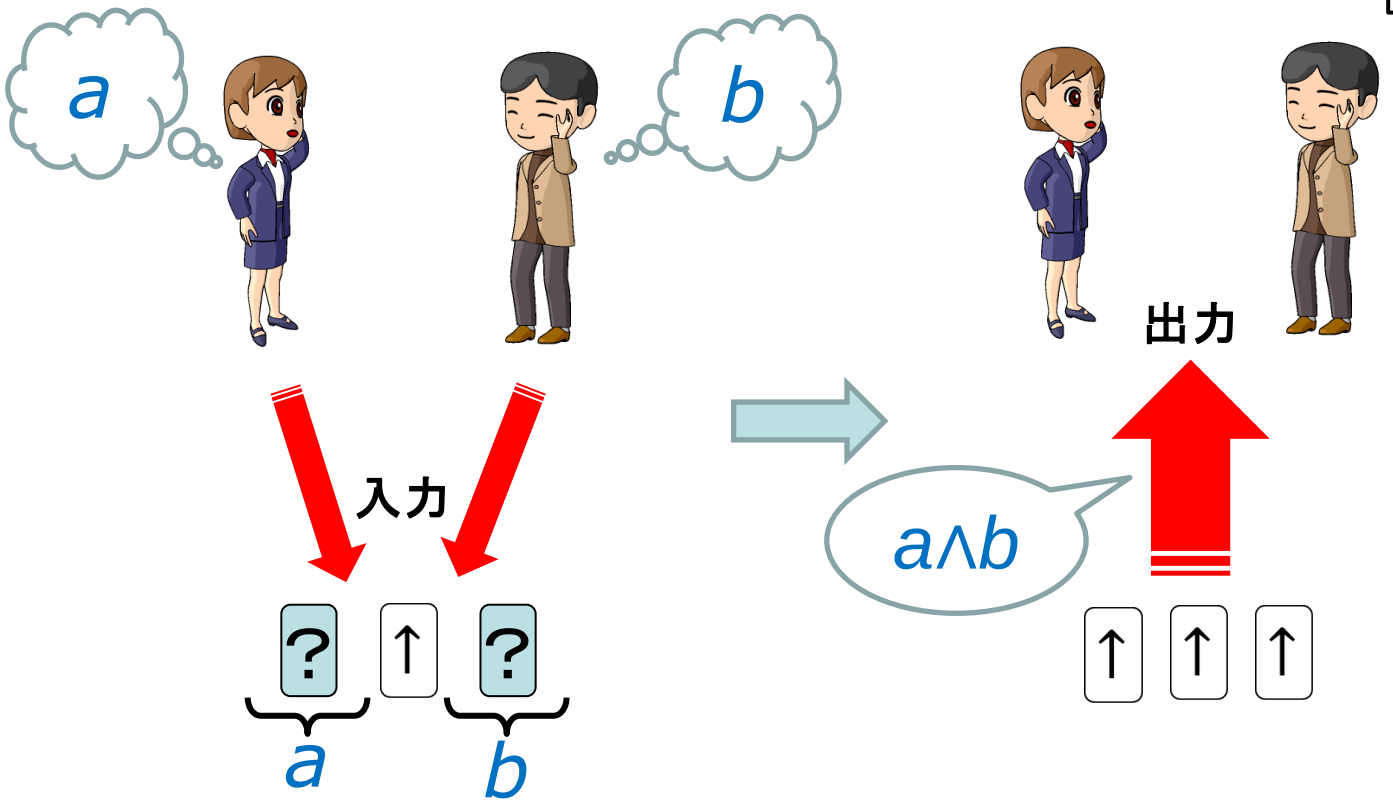




【課題】by 品川
さらに1枚削減できるか

Five-Card Trick can be done with three cards

- 符号化ルールを思い出すと、赤と黒の順番で1ビットを表していた
- 矢印が書かれた上下カードを用いて、1ビットを1枚の上下方向で表す

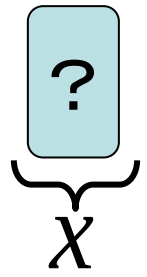


ルール

1. 次のようにビットを符号化する

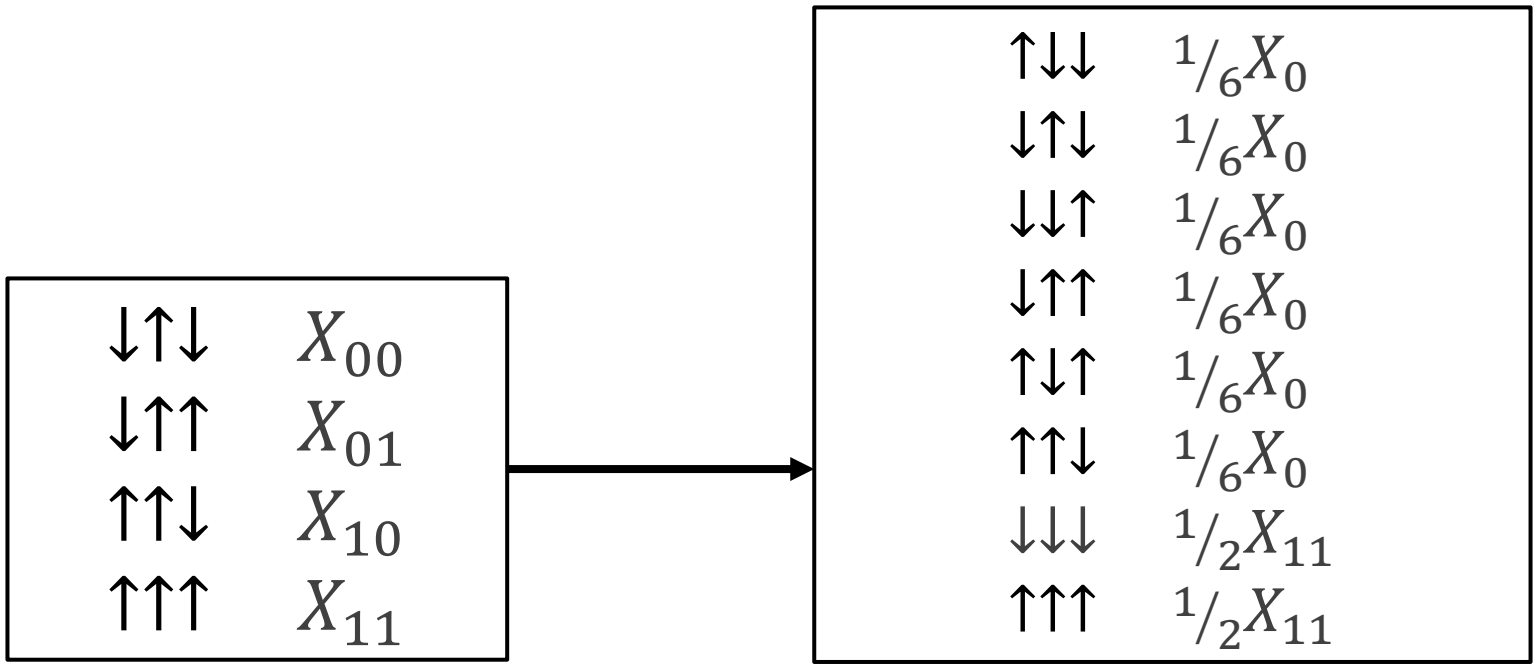
↓ = 0, ↑ = 1

2. $x \in \{0,1\}$ のコミットメントという



3枚ANDの手順と正当性・安全性

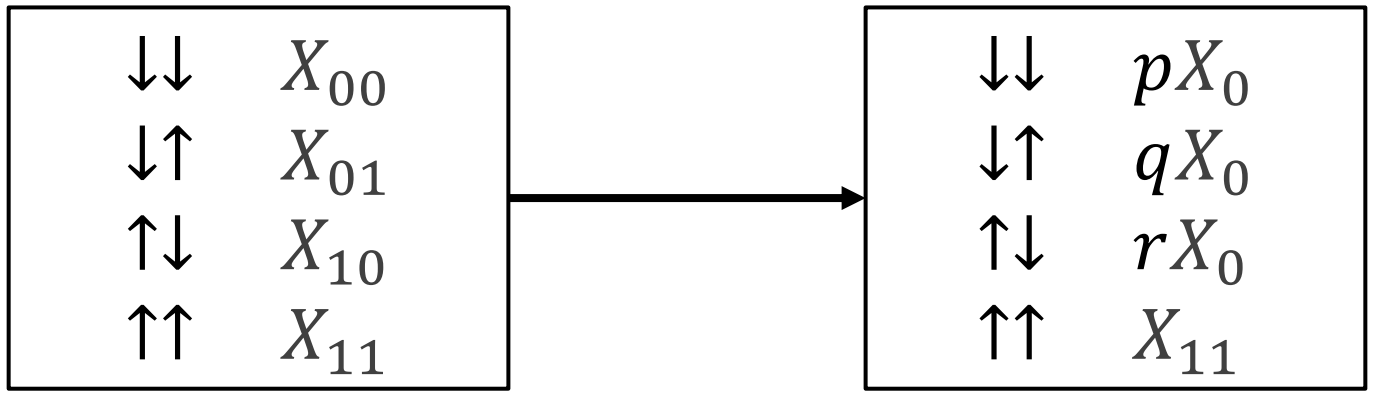
1. カード列3枚をランダムに入れ替える（i.e., 単にシャッフルする）
2. カード列3枚を同時に、ランダムに回転させる
   - ➢定式化するために、置換を拡張させる必要あり[SN25]
3. カード列3枚を全てめくり、$a \wedge b$ の値だけを得る



ただし$X_0 := X_{00} + X_{01} + X_{10}$ は、出力が0となる変数の和

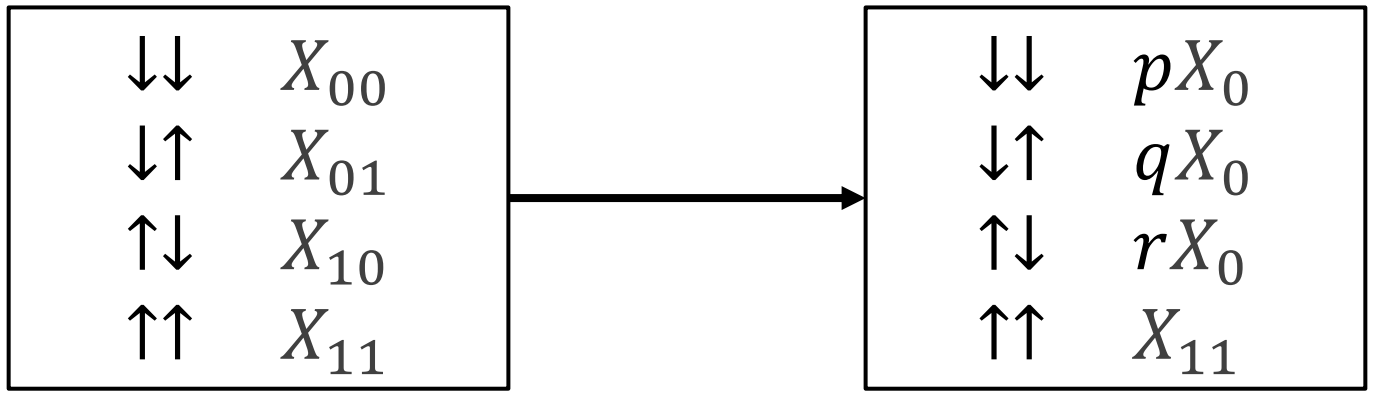
問題とその定式化

- 3枚ANDは可能だが、2枚ANDは取り組まれていなかった
- すなわち、初期状態から次の状態に遷移できるか
  - ただし $p, q, r > 0$ かつ $p + q + r = 1$
  - 全てめくると、$a \wedge b$ の値だけが得られる



n枚ANDプロトコルは構成できない

- 飯野–李–崎山–宮原、SCIS 2025で解決
  - ➢任意のステップを踏んでも、非コミット型であっても、構成できない
- 観察：初期状態に、4通り全てのカード列が含まれている
  - ➢X_{11} のカード列が2通りになる $\Longrightarrow$ X_{00}, X_{01}, X_{10} のカード列と必ず混ざる
  - ➢シャッフルによって X_{00}, X_{01}, X_{10} だけが混ざるしかない
  - ➢しかし、X_{00} と X_{11} のカード列は上下対称 $\Longrightarrow$ X_{00}が混ざるとX_{11}もどれかに混ざる
- 上の議論はn入力でも同様なので、n枚の不可能性を導ける



[再掲] 解決・進展状況の外観

講演タイトル	問題概要	スライド#	文献
ANDプロトコルにまつわる未解決問題	4枚非コミット型ANDシャッフル1回での不可能性	p. 17	池田–品川、CSS 2024
	4枚コミット型XORのランダムカットのみでの不可能性	p. 54	Fujita–Ikeda–Shinagawa–Yoneyama、APKC 2025
カードベースZKPプロトコ（（株）ニコリが扱うパズルを対象）	数独		SOSA 2025
			APKC 2025
	ドッスンフワリ	p. 19	Iwamoto–Ohara、IEICE Trans. 2025
	シャカシャカ	p. 20	–岩本、SCIS 2025
	ストストーン	p. 21	–宇野、第202回AL研究会
カードベース暗号に登場するさまざまなカード組と符号化	n枚n入力ANDの不可能性	p. 8	飯野–李–崎山–宮原、SCIS 2025
カードベース暗号に現れる数学	領域連結性に対する非対話型ZKPの効率化	p. 26	Nuida、ePrint 2025/924

今紹介した

次の発表内容 by 池田さん

今紹介した

[再掲] 解決・進展状況の外観

講演タイトル	問題概要	スライド#	文献
ANDプロトコルにまつわる未解決問題	4枚非コミット型ANDシャッフル1回での不可能性	p. 17	池田–品川、CSS 2024
	4枚コミット型XORのランダムカットのみでの不可能性	p. 18	eyama、2025
カードベースZKPプロトコ（(株)ニコリが扱うパズルを対象）	数独	p. 18	TSSM、SOSA 2025 ORA+、APKC 2025
	ドッスンフワリ	p. 19	Iwamoto–Ohara、IEICE Trans. 2025
	シャカシャカ	p. 20	初貝–渡邉–岩本、SCIS 2025
	ストストーン	p. 21	大江–木谷–宇野、第202回AL研究会
カードベース暗号に登場するさまざまなカード組と符号化	n枚n入力ANDの不可能性		原、SCIS 2025
カードベース暗号に現れる数学	領域連結性に対する非対話型ZKPの効率化	p. 26	Nuida、ePrint 2025/924

今日の発表内容 by 品川先生

リストで整理

論文参照

(株)ニコリが扱うパズルに対するZKPの最新状況

- ZKPプロトコルが構成されていない数字パズルは24個

下線はZKPに関する発表がされていないパズル、赤字は最近取り組まれたパズル、青字は最近追加されたパズル（宮原調べ）

因子の部屋、ウソワン、お家へ帰ろう、カックロ、キンコンカン、クロット、黒どこ(黒マスはどこだ)、碁石ひろい、さしがね、さとがえり、サムライン、四角に切れ、シャカシャカ、シンカミノ、縦横さん、推理パズル、数コロ、数独、ストストーン、スラローム、スリザーリンク、ダブルチョコ、チェンブロ、チョコバナナ、月か太陽、ドッスンフワリ、ドッチループ、流れるループ、ナンスケ、ナンバーリンク、ぬりかべ、ぬりみさき、ぬりめいず、のりのり、波及効果、橋をかけろ、バッグ、美術館、ひとりにしてくれ、フィルオミノ、ふくめん算、へびいちご、へやわけ、ヘルゴルフ、ペンシルズ、マカロ、ましゅ、マックロ、ミッドループ、虫くい算、やじさんかずさん、ヤジリン、よせなべ、LITS

- 図形を扱うパズルに対するZKPが構成されている

まとめ

- 23年度IMI研究集会で提示された未解決問題の解決状況を共有した
- 新規参入者にとって有益な研究資料となれば幸いです

Boer89 Bert Den Boer. More efficient match-making and satisfiability the five card trick. In Jean-Jacques Quisquater and Joos Vandewalle, editors, Advances in Cryptology – EUROCRYPT' 89, volume 434 of LNCS, pages 208–217, Heidelberg, 1990. Springer.

MKS12 Takaaki Mizuki, Michihito Kumamoto, and Hideaki Sone. The five-card trick can be done with four cards. In Xiaoyun Wang and Kazue Sako, editors, Advances in Cryptology—ASIACRYPT 2012, volume 7658 of LNCS, pages 598–606, Berlin, Heidelberg, 2012. Springer.

MS14 Takaaki Mizuki and Hiroki Shizuya. A formalization of card-based cryptographic protocols via abstract machine. Int. J. Inf. Secur., 13(1):15–23, 2014.

KWH15 Alexander Koch, Stefan Walzer, and Kevin Härtel. Card-based cryptographic protocols using a minimal number of cards. In Tetsu Iwata and Jung Hee Cheon, editors, Advances in Cryptology—ASIACRYPT 2015, volume 9452 of LNCS, pages 783–807,Berlin, Heidelberg, 2015. Springer.

SN25 Kazumasa Shinagawa and Koji Nuida. Card-based protocols imply PSM protocols.In Olaf Beyersdorff, Micha l Pilipczuk, Elaine Pimentel, and Nguyễn Kim Thắng, editors, Theoretical Aspects of Computer Science, volume 327 of LIPIcs, pages 72:1–72:18,Dagstuhl, 2025. Schloss Dagstuhl.