カードベース暗号の30年間

品川 和雅
茨城大学

2024年6月22日(土)
可換代数と組合せ論セミナー＠東邦大学

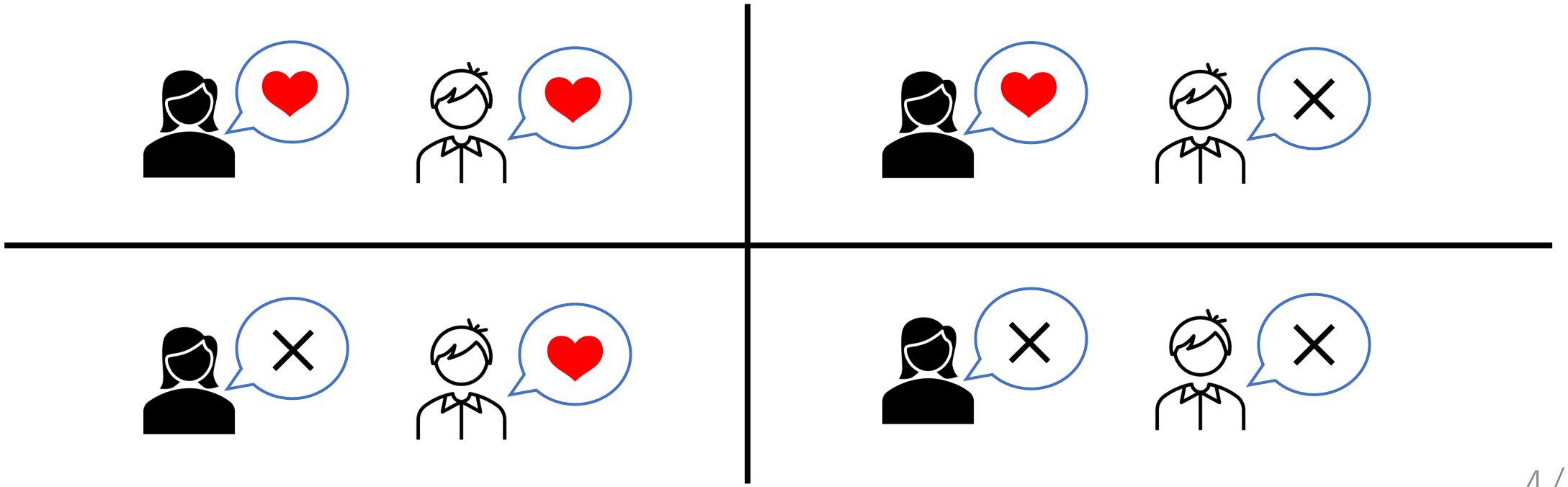
目次

第１部
イントロダクション

気まずくならない告白

- アリスとボブは友達以上恋人未満の関係

- 友情をなるべく壊さずに「両思いかどうか」を確かめるには？



論理積の秘密計算

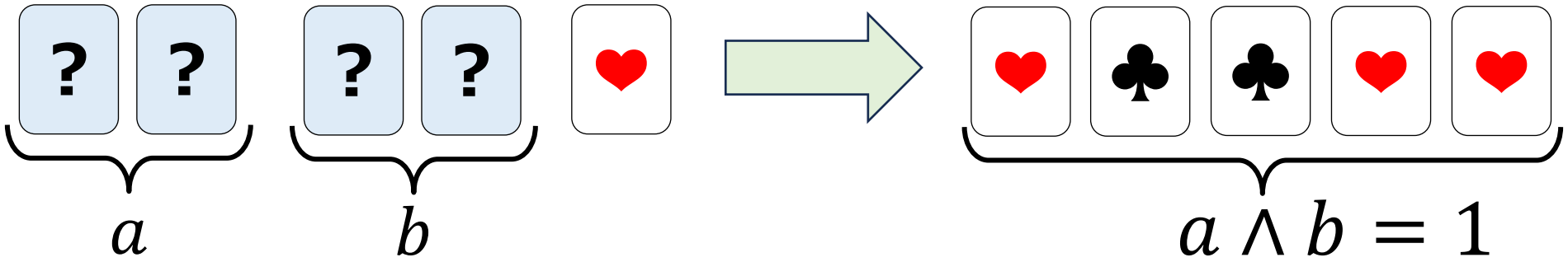
- 秘密計算とは、入力を隠したまま、出力のみを計算する技術
- 今の場合は**論理積の秘密計算**ができればよい
- 好き＝1、興味なし＝0とすると

$a \wedge b = 1 \longleftrightarrow$ 「両思い」

$a \wedge b = 0 \longleftrightarrow$ 「片思い」または「お互い興味なし」

Five-Card Trick [Boer, Eurocrypt 1989]

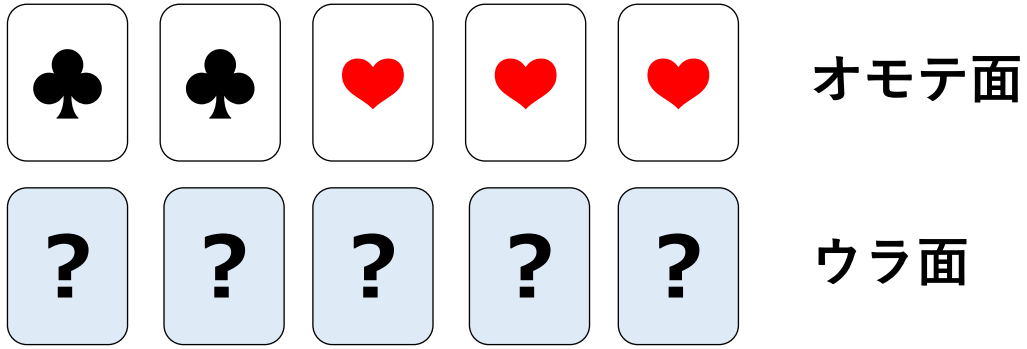
- 論理積$a \wedge b$を計算するプロトコル



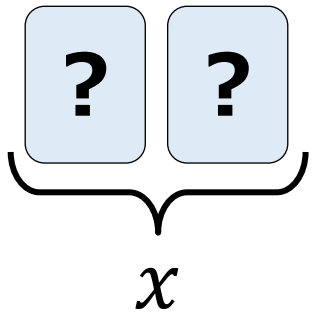
- 最初に提案されたカードベースプロトコル
  - (非物理的)暗号プロトコルの構成要素のアイディアに用いられた

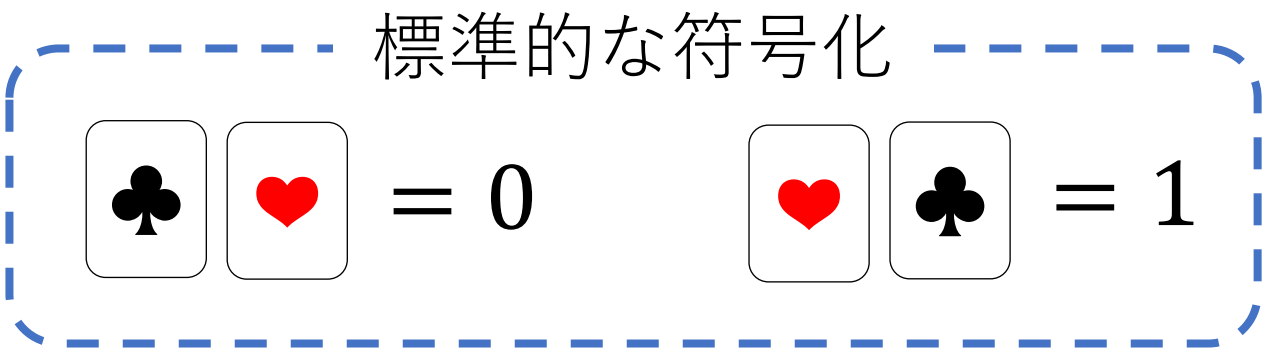
B. den Boer, More Efficient Match-Making and Satisfiability The Five Card Trick, EUROCRYPT 1989.

カードと符号化

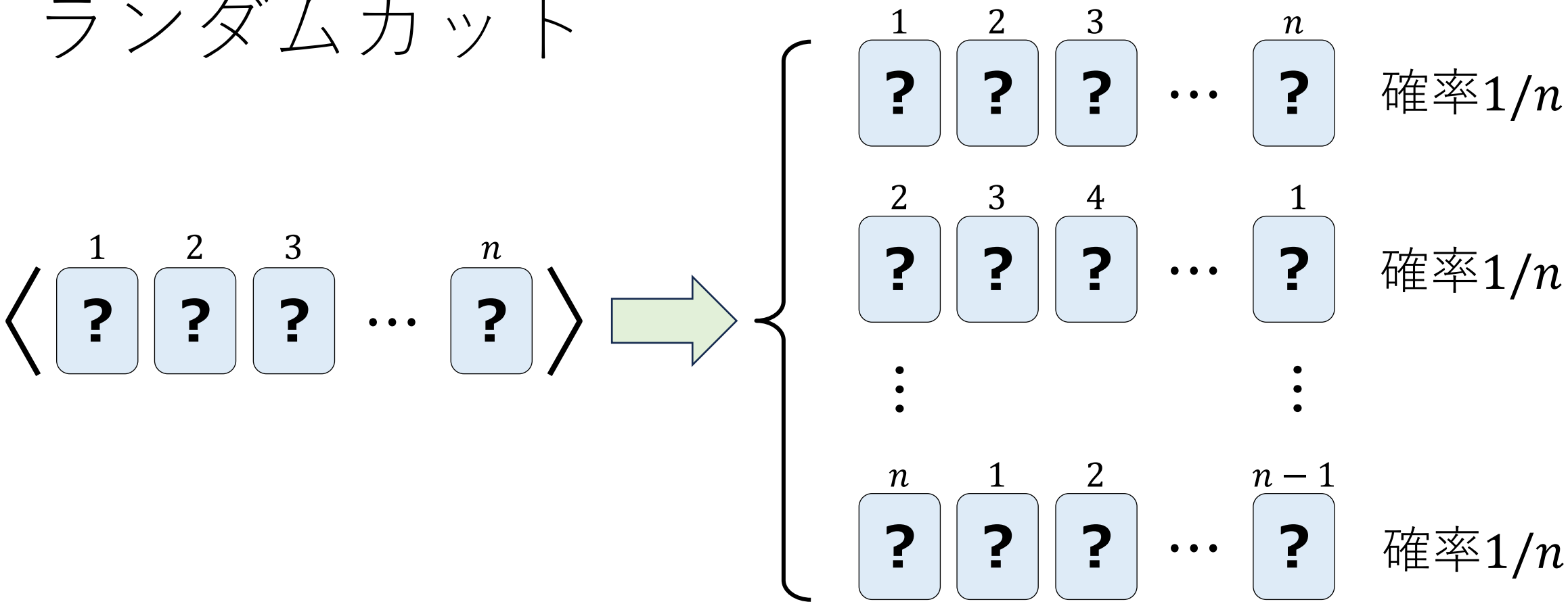


- 符号化に従う裏向きのカードを**コミットメント**と呼ぶ





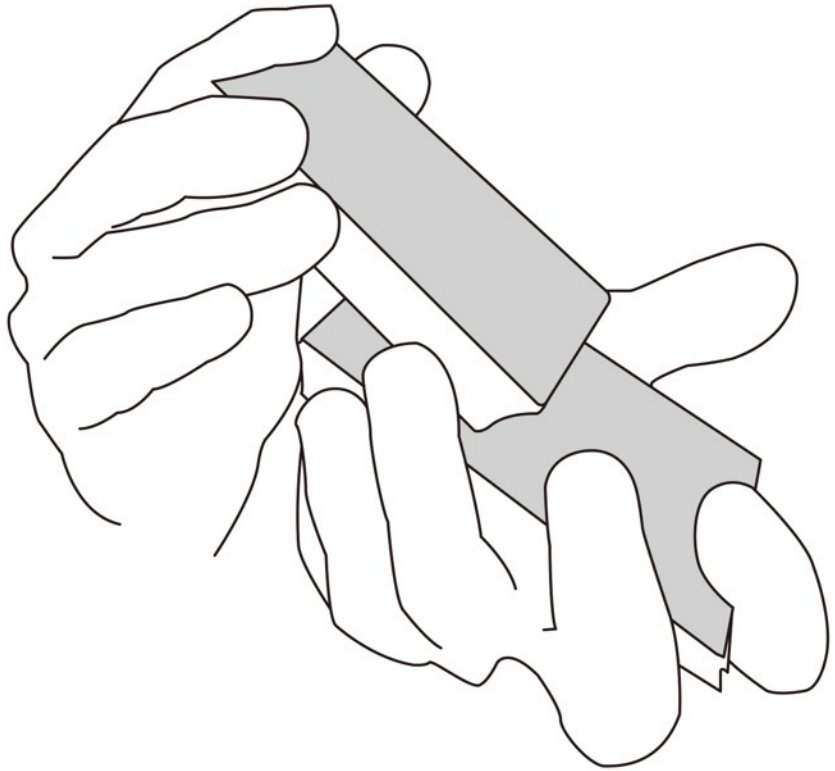
ランダムカット



- n通りの巡回シフトが等確率で生じる
- どの状態が選ばれたかは**誰にも**(操作者でさえも)一切推測できない

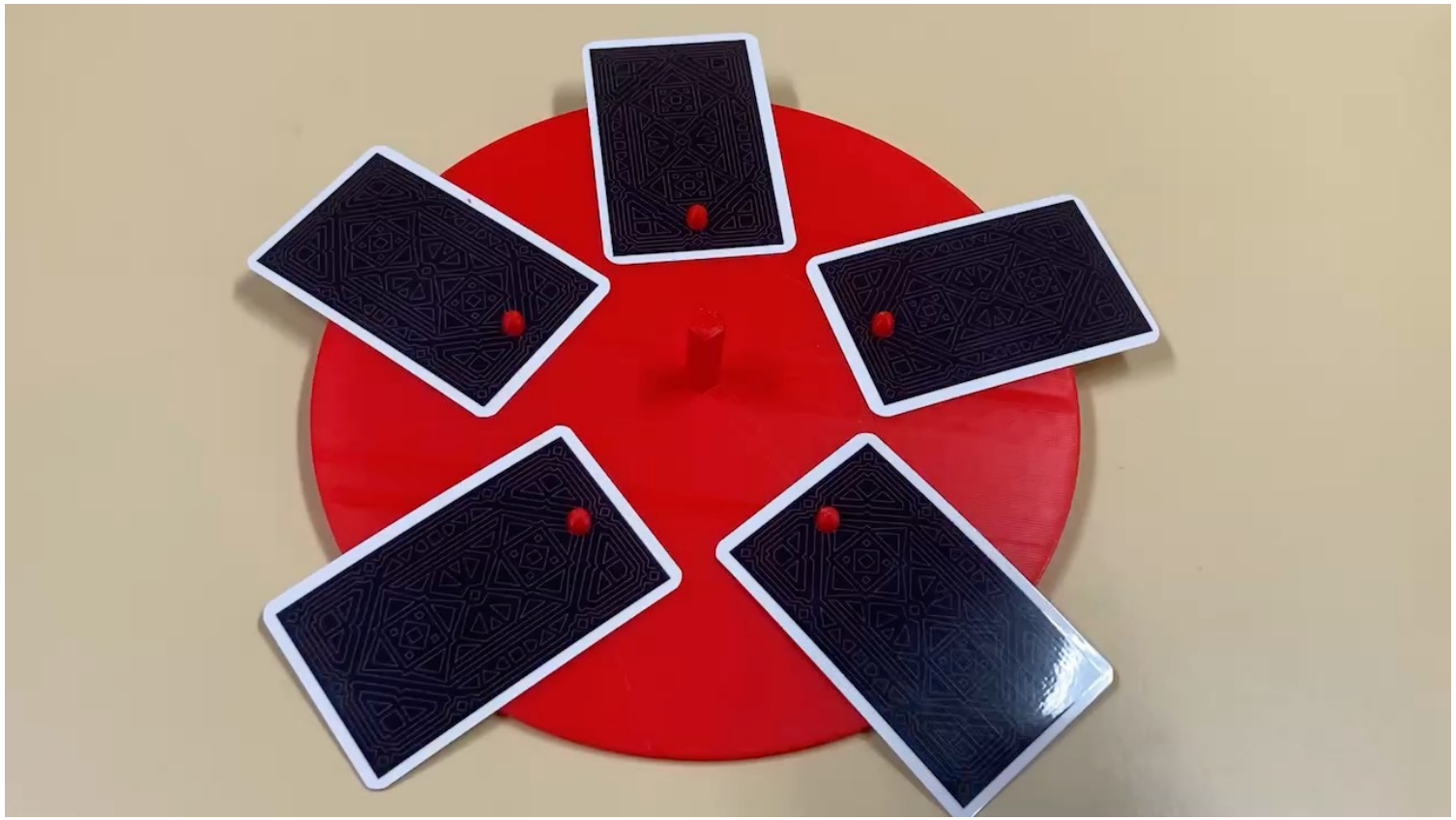
ランダムカットの実装方法①

- 「適当に２分割して入れ替える」という操作を繰り返す

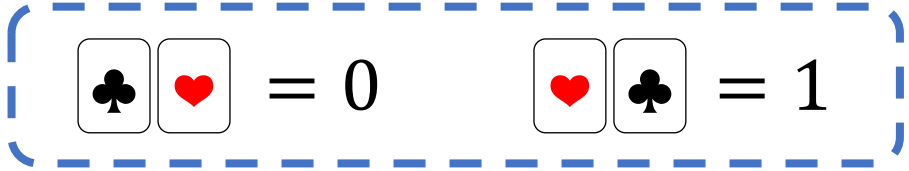


ランダムカットの実装方法②

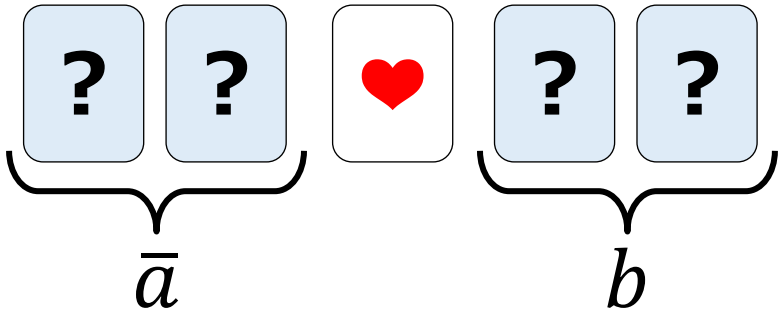
- コマにカードを載せて回す

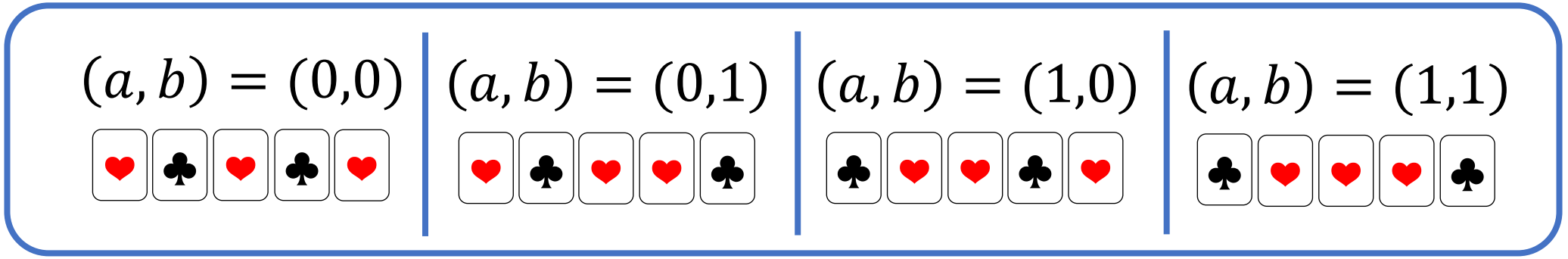


Five-Card Trick (1/3)



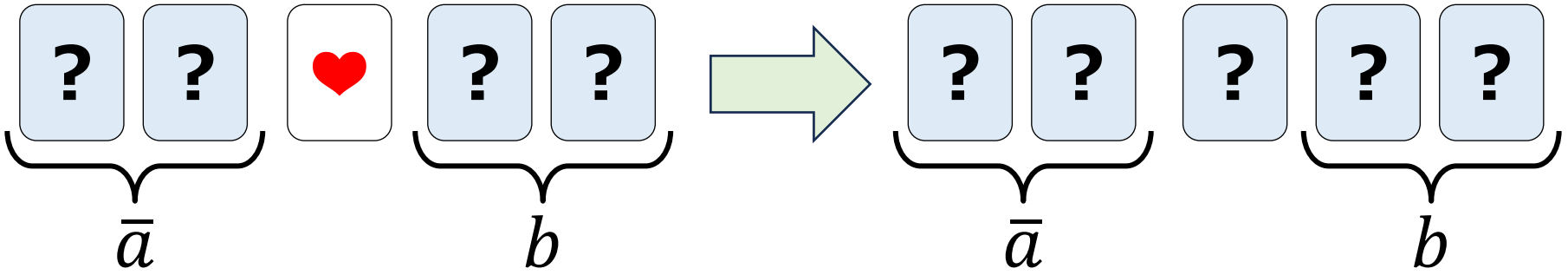
1. アリスとボブはaとbのコミットメントをそれぞれ作り、
   以下のように並べる



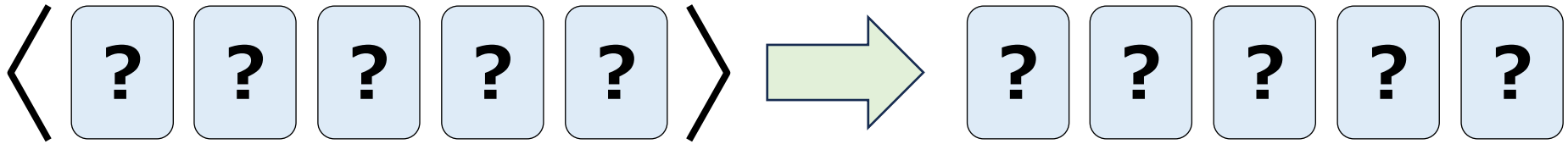


Five-Card Trick (2/3)

2. 中央のカードを裏にする



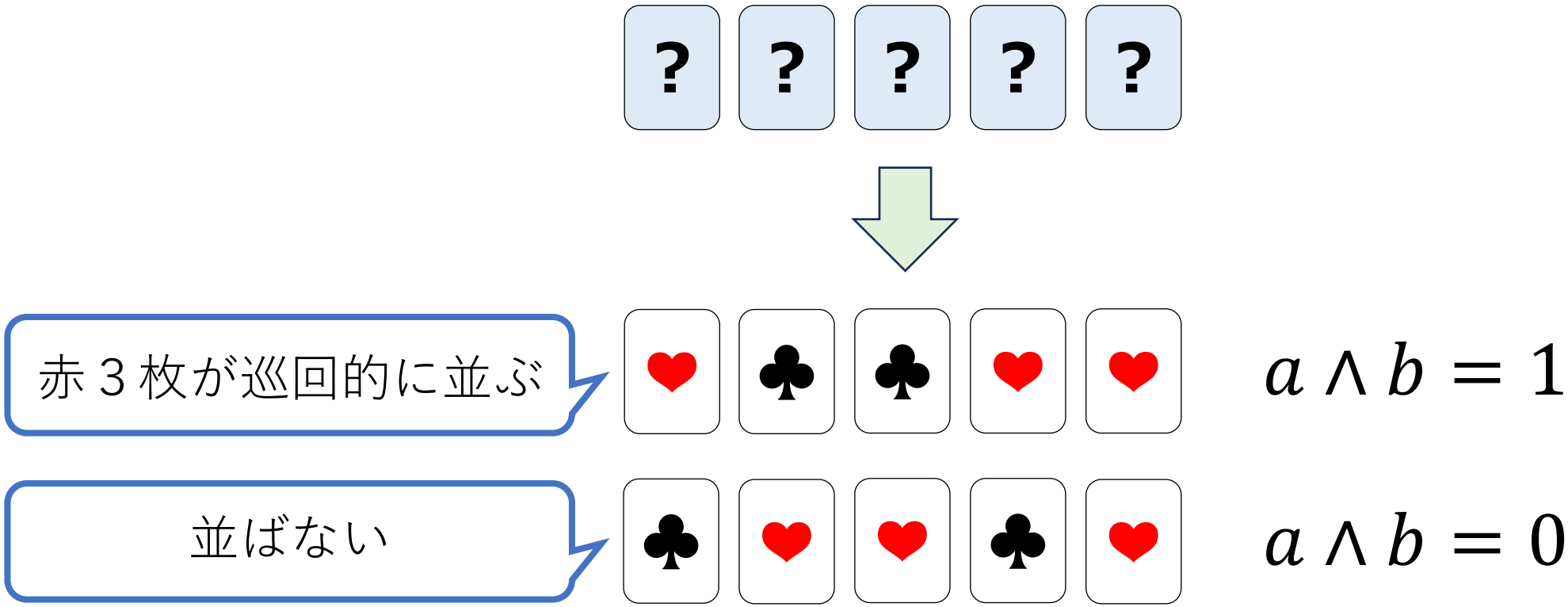
3. ランダムカットを適用する



ランダムカット ＝ 巡回的なシャッフル

Five-Card Trick (3/3)

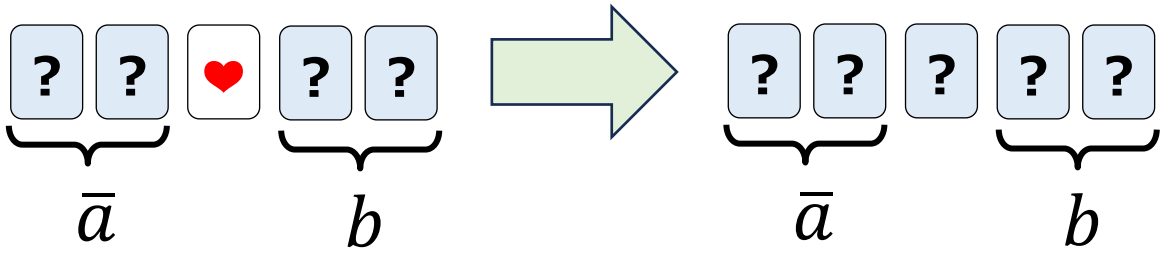
4. すべてのカードをめくる



Five-Card Trickのまとめ

♣♥ $= 0$　　♥♣ $= 1$

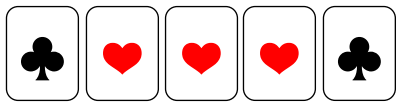
1. カードを並べ、中央を裏にする



2. ランダムカット

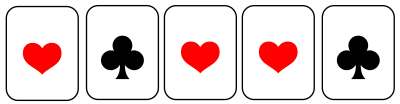
3. すべてのカードをめくる

赤３枚が並ぶ



$a \wedge b = 1$

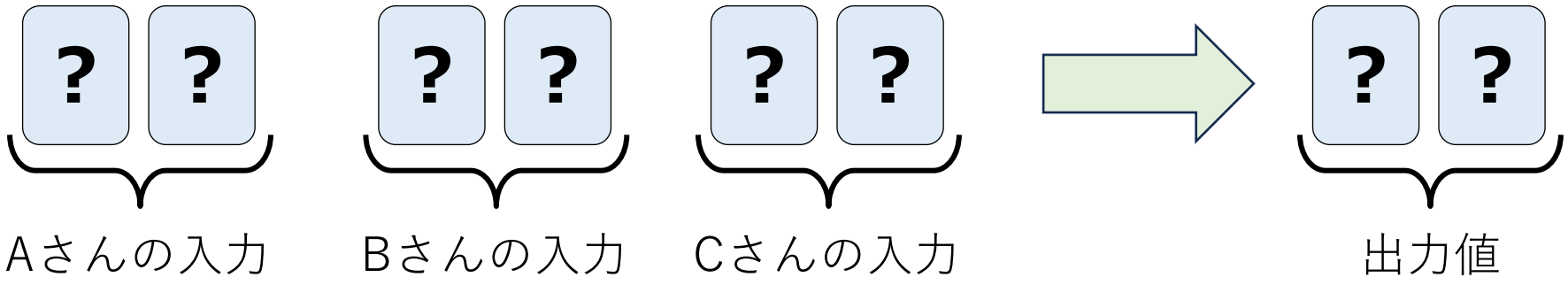
並ばない



$a \wedge b = 0$

カードベース暗号

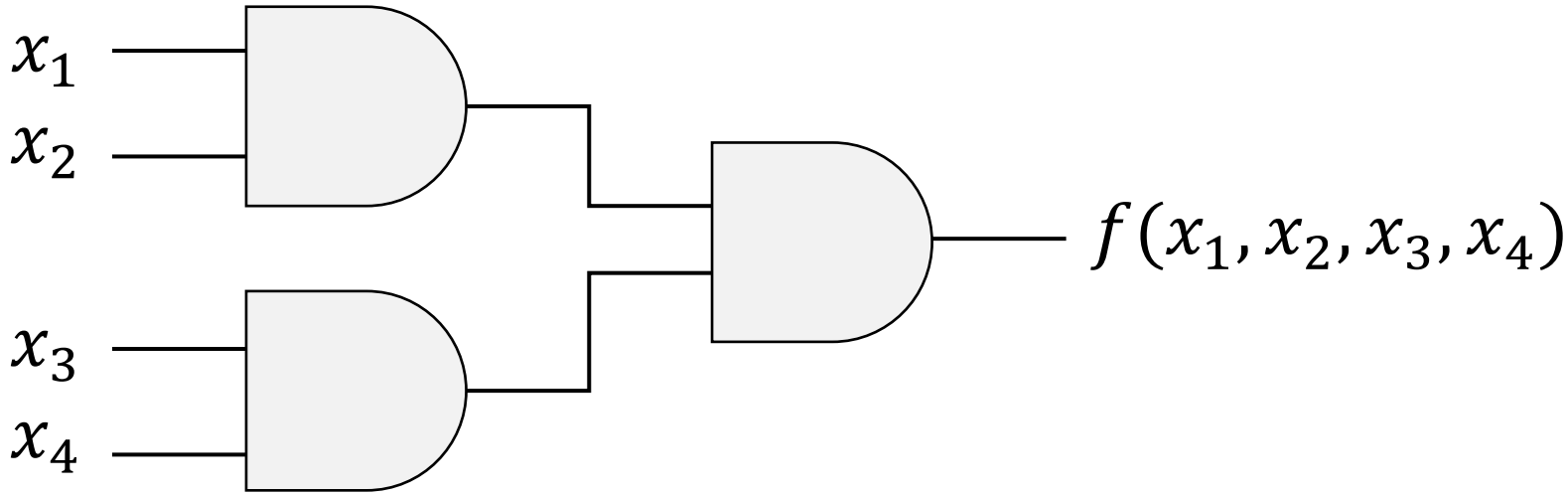
- カードを用いて暗号技術（主に秘密計算）を実現する技術



- カードベース暗号の特徴
  - 情報理論的安全性（計算困難問題などに依存しない／量子計算機の登場とも無関係）
  - 実際に机の上でプロトコルを実行できる
  - 物理的・視覚的なため、仕組みを理解しやすい

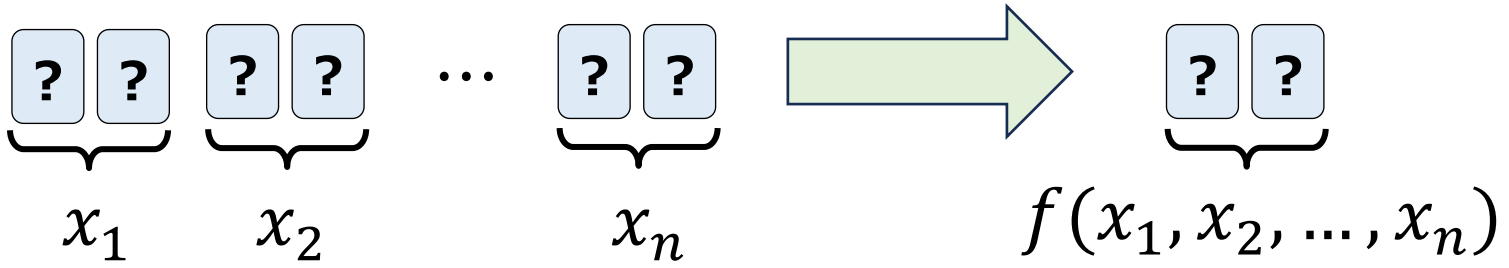
任意関数$f: \{0,1\}^n \to \{0,1\}$の計算

- アプローチ：回路計算（基本ゲートの組合せによる計算）

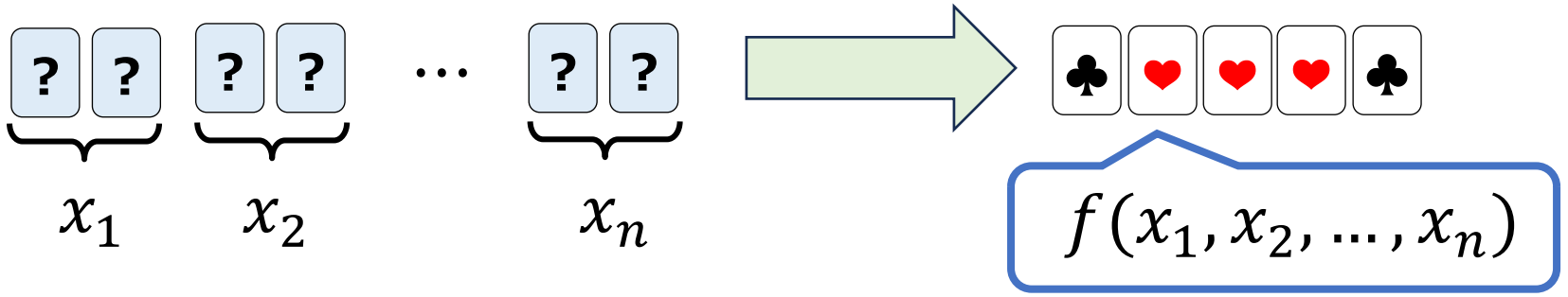


コミット型プロトコル

- **コミット型プロトコル**：コミットメントを出力するプロトコル

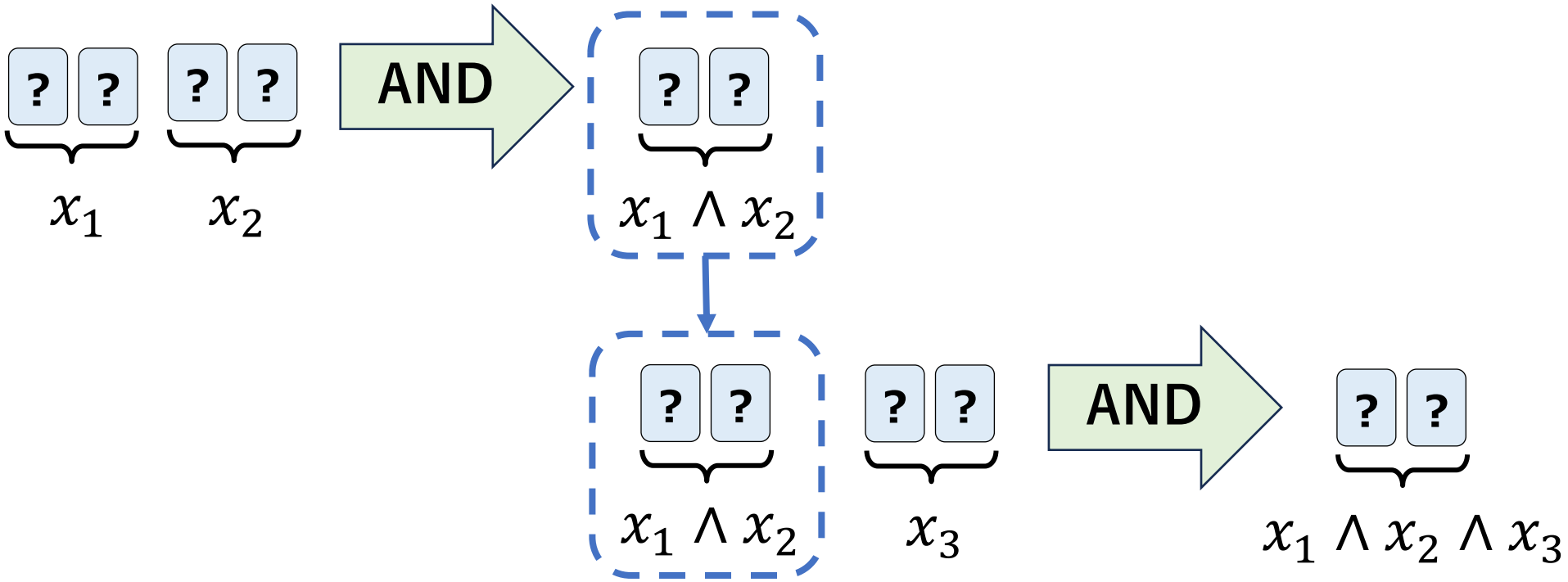


- **非コミット型プロトコル**：出力値そのものを公開するプロトコル



コミット型プロトコルの性質

- コミット型プロトコルは結合可能



- **AND/COPYプロトコルの組合せで任意関数を計算できる**

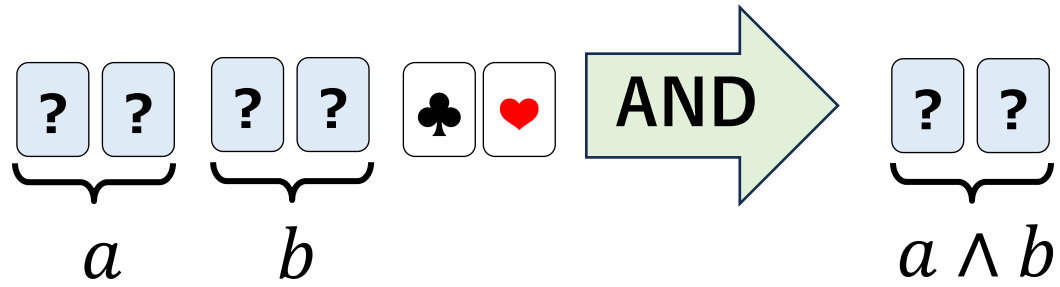
ANDとCOPYで任意関数を計算可能

- 例えば右の真理値表で表される関数は
  $$f = (\overline{x_1} \wedge \overline{x_2} \wedge x_3) \vee (\overline{x_1} \wedge x_2 \wedge x_3)$$
  と表すことができる

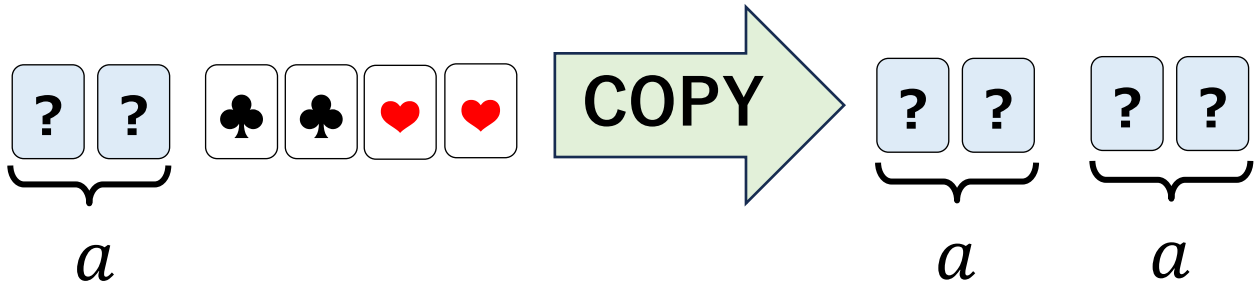
x_1	x_2	x_3	$f(x_1, x_2, x_3)$
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

- ORはAND/NOTで記述可能（De Morganの法則）
- よって、NOT/AND/COPYで記述可能
  - この関数の場合、各ビットを2個ずつCOPYしている
- NOTは自明だから、コミット型AND・COPYプロトコルがあればOK

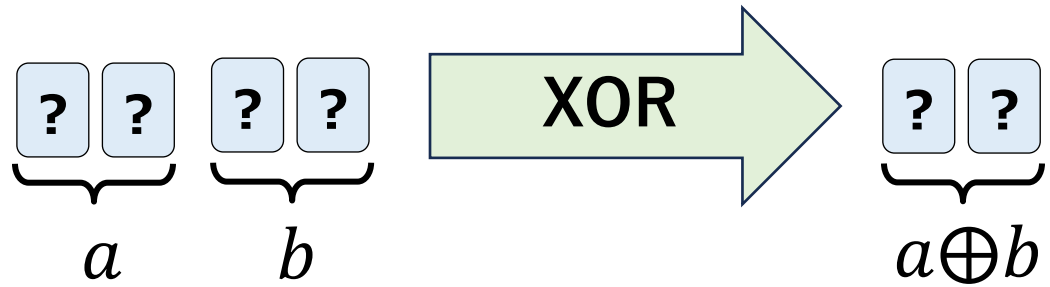
AND/COPY/XORプロトコル[Mizuki-Sone, FAW 2009]



6枚・ **ランダム二等分割カット**1回



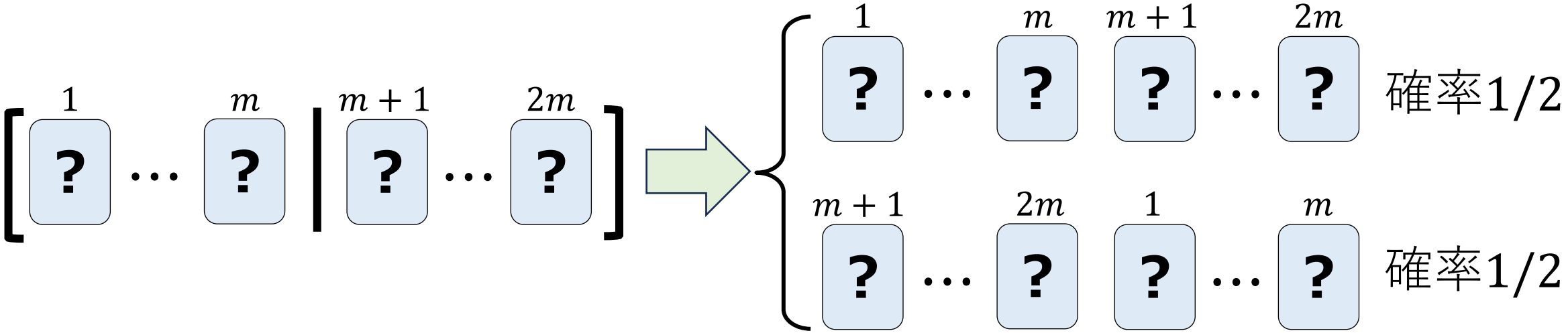
6枚・ **ランダム二等分割カット**1回



4枚・ **ランダム二等分割カット**1回

T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009.

ランダム二等分割カット [Mizuki-Sone, FAW 2009]

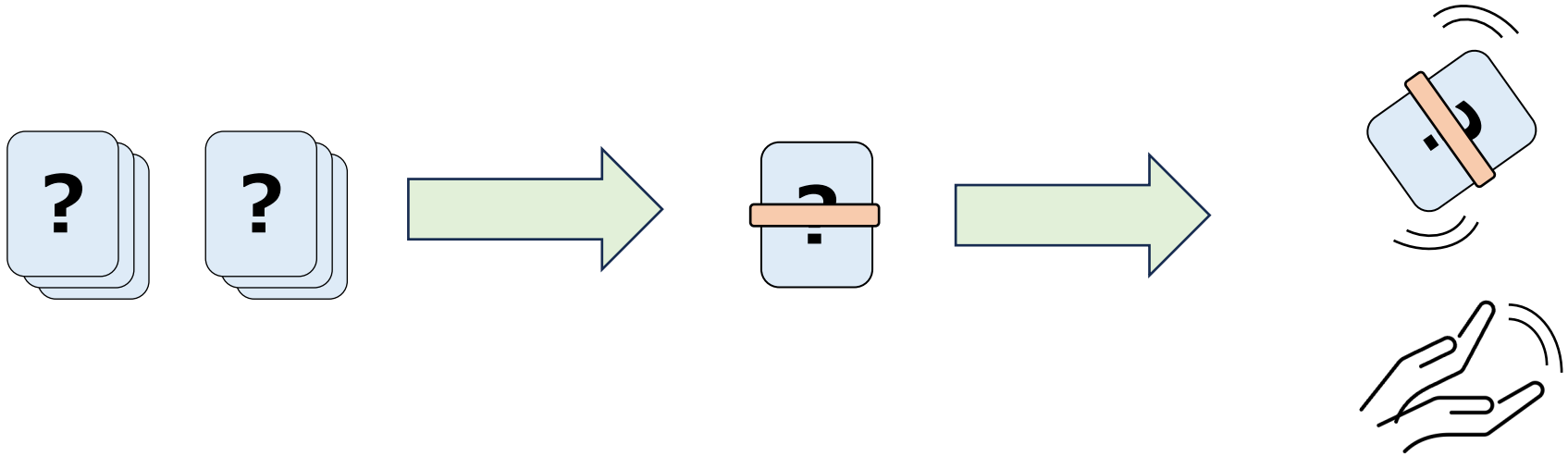


- 同じ枚数の2個の束の入れ替えのシャッフル
- どちらが選ばれたかは誰にも一切推測できない

T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009.

ランダム二等分割カットの実装① [Ueda et al., TPNC 2016]

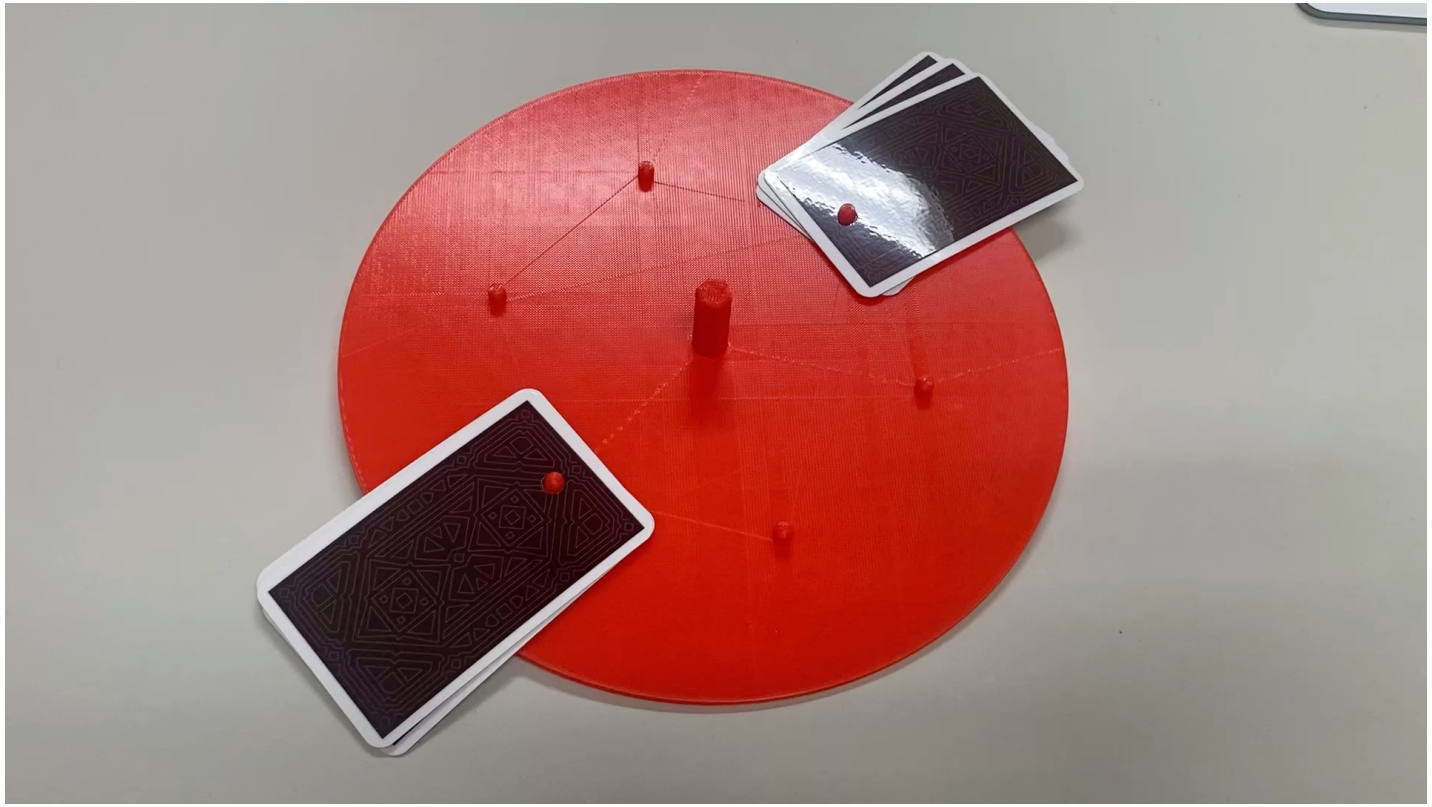
- Spinning throw
  - 2個の束を、オモテ同士を貼り合わせる向きで、ゴムバンドで固定する
  - それを空中に放り投げる



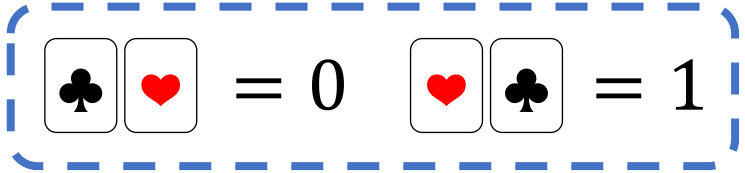
I. Ueda, A. Nishimura, Y. Hayashi, T. Mizuki, and H. Sone, How to Implement a Random Bisection Cut, TPNC 2016.

ランダム二等分割カットの実装方法②

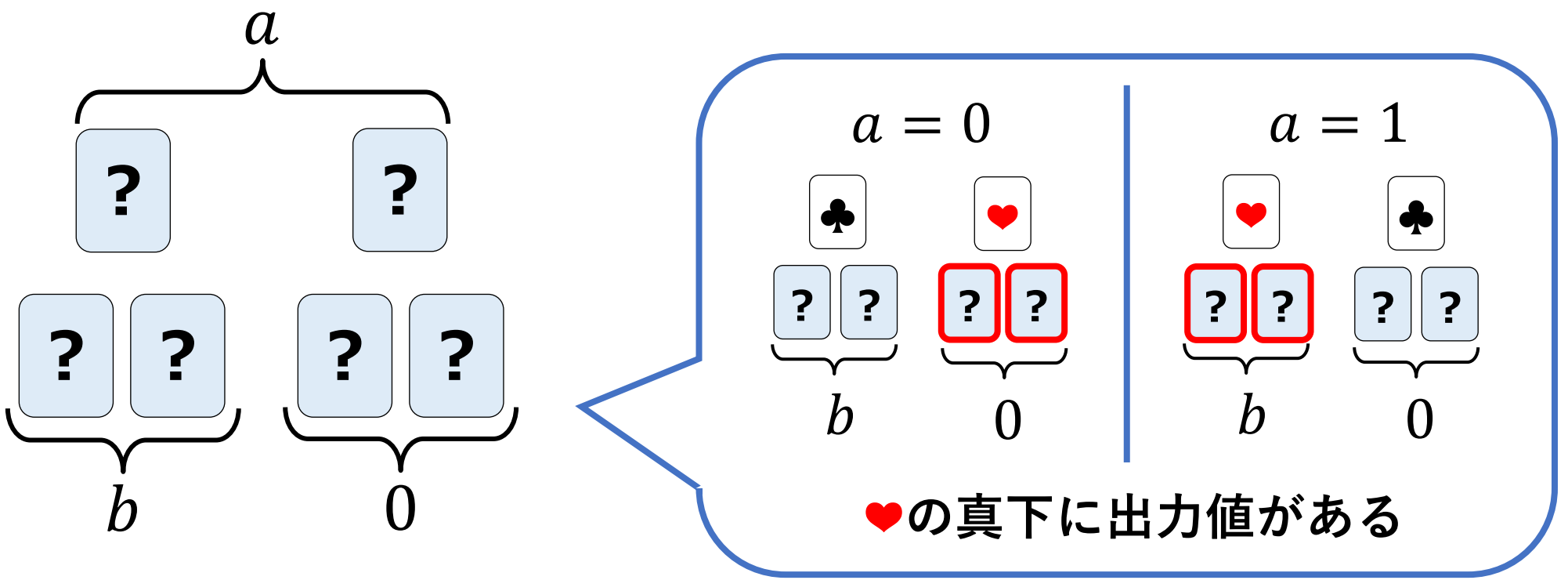
- コマにカード束を載せて回す



[MS09]のANDプロトコル (1/3)



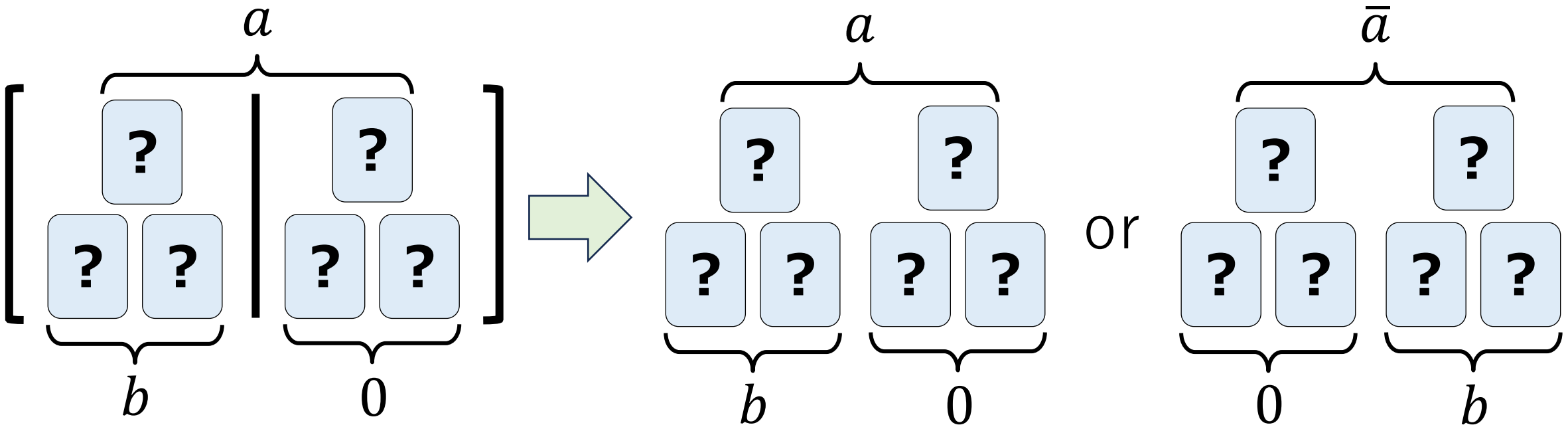
1. 入力コミットメントa, bと追加カード2枚を以下のように並べる



[MS09]のANDプロトコル (2/3)

♣♥ = 0　♥♣ = 1

2. ランダム二等分割カットを施す

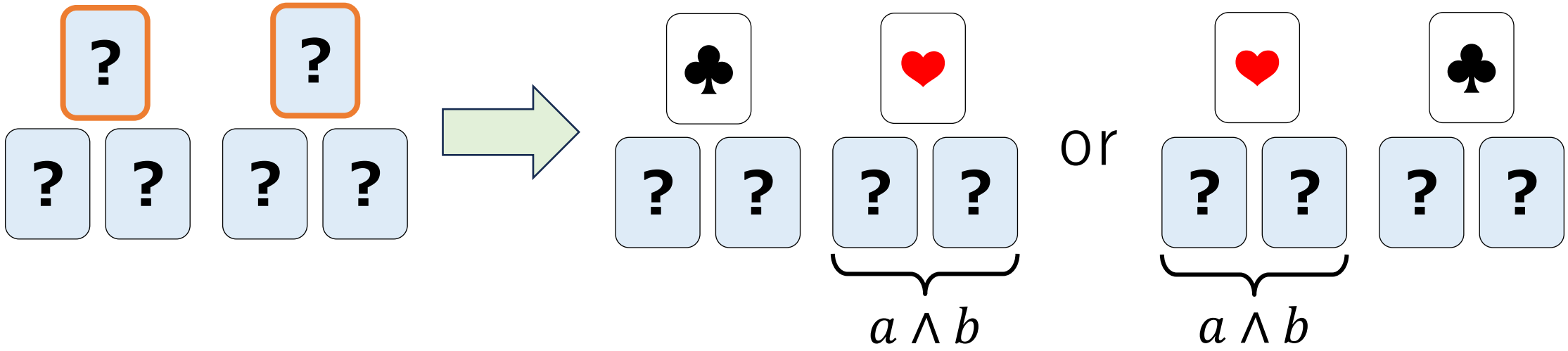


「♥の真下に出力値がある」という関係性は不変

[MS09]のANDプロトコル (3/3)

♣♥ = 0　♥♣ = 1

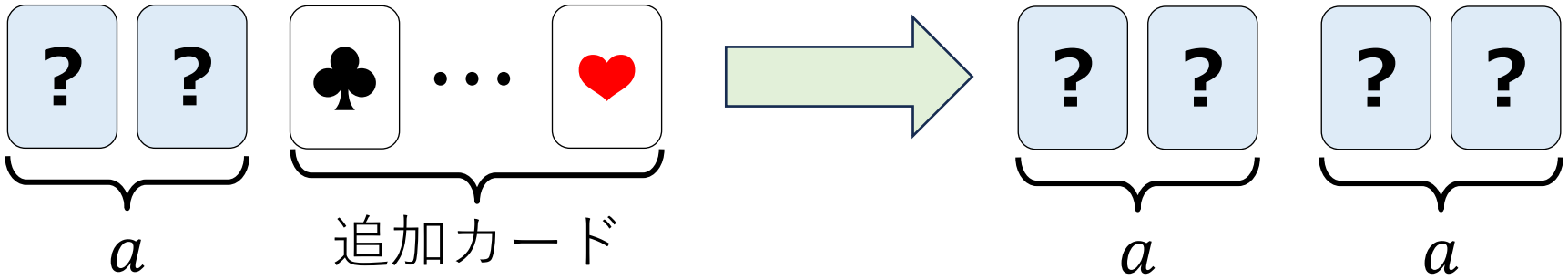
3. 上の2枚をめくり、出力値を以下のように得る



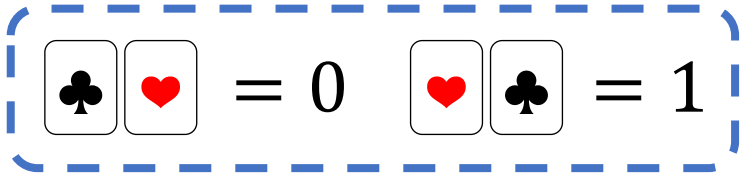
- 正当性：「♥の真下に出力値があること」より明らか
- 安全性：入力情報aとオープン情報は(RBCの効果により)独立

COPYプロトコル

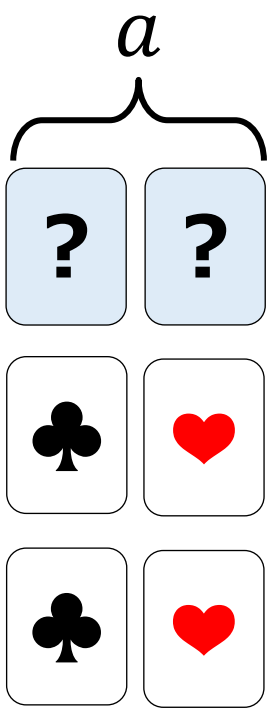
- コミットメントを2個以上に複製するプロトコル



[MS09]のCOPYプロトコル (1/3)



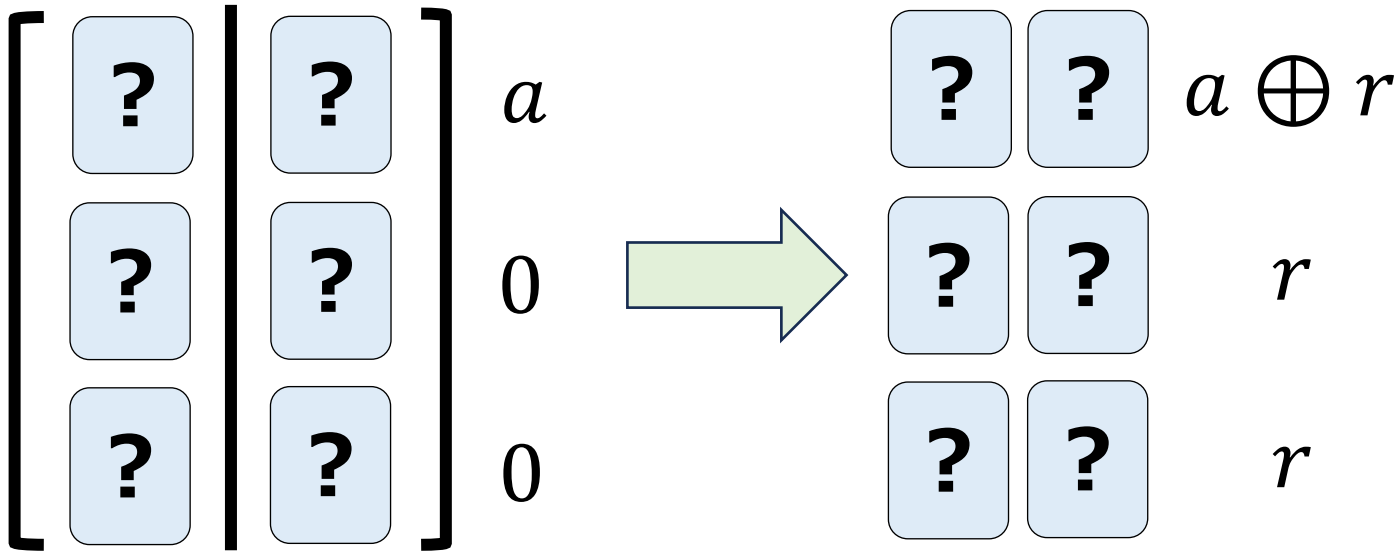
1. 入力コミットメントaと追加カード4枚を以下のように並べる



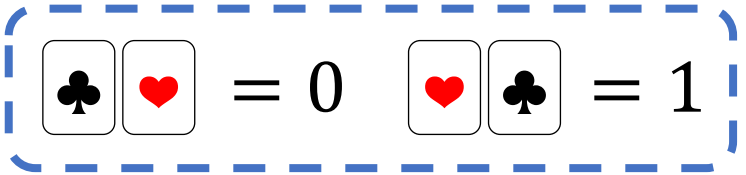
[MS09]のCOPYプロトコル (2/3)

♣♥ = 0　♥♣ = 1

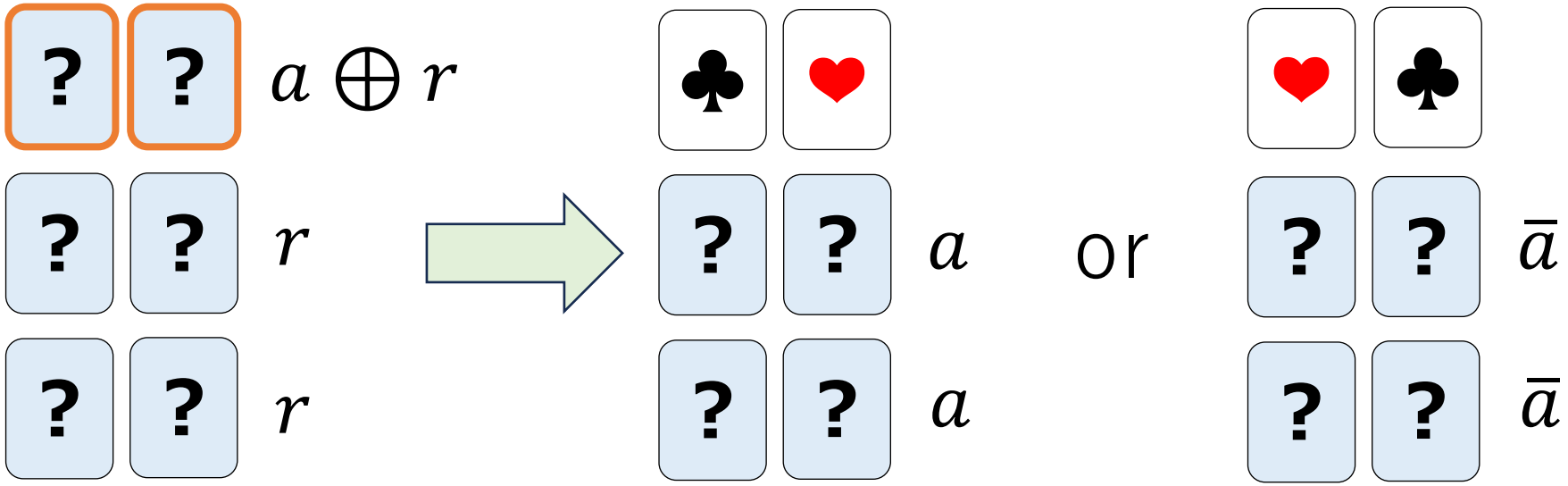
2. すべて裏にし、ランダム二等分割カットを施す



[MS09]のCOPYプロトコル (3/3)

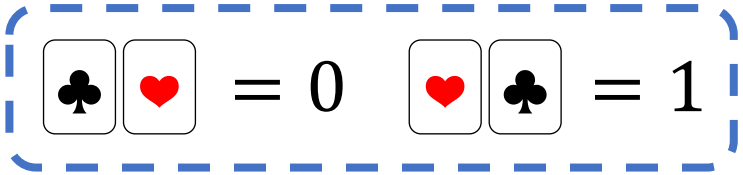


3. 上の2枚をめくり、出力値を以下のように得る

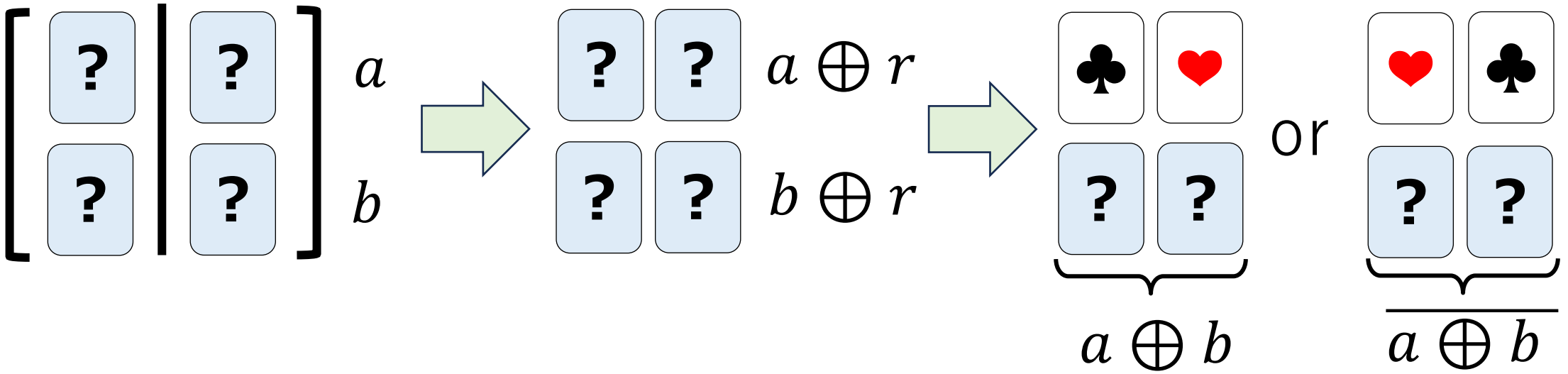


- 正当性：$a \oplus r = 0$なら$a = r$、$a \oplus r = 1$なら$a \neq r$より成り立つ
- 安全性：入力情報aとオープン情報は(RBCの効果により)独立

[MS09]のXORプロトコル

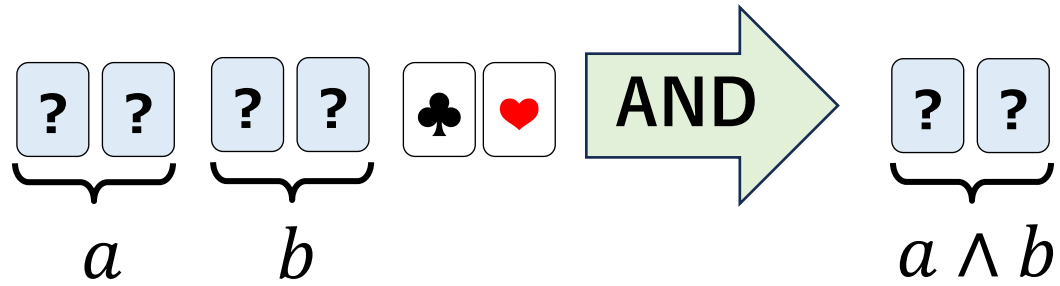


- COPYプロトコルと同様の手順で実現できる

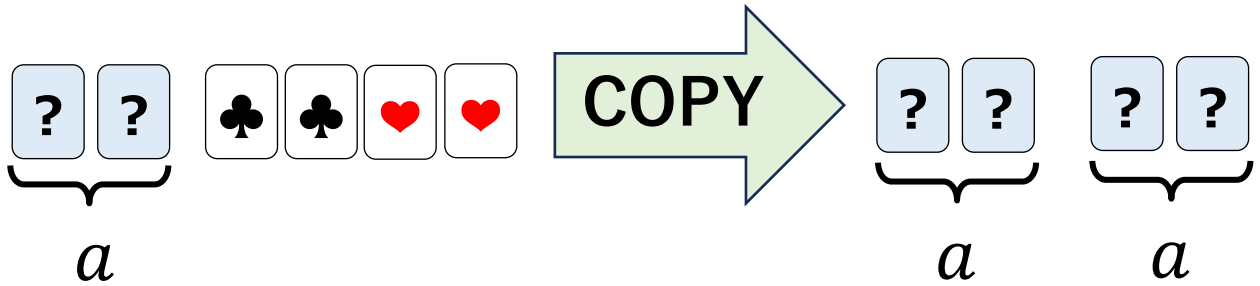


- COPYとXORを同時に（1回のRBCで）実行することも可能
  - 例：$(a, b, 0, 0) \rightarrow (a \oplus b, a, a)$

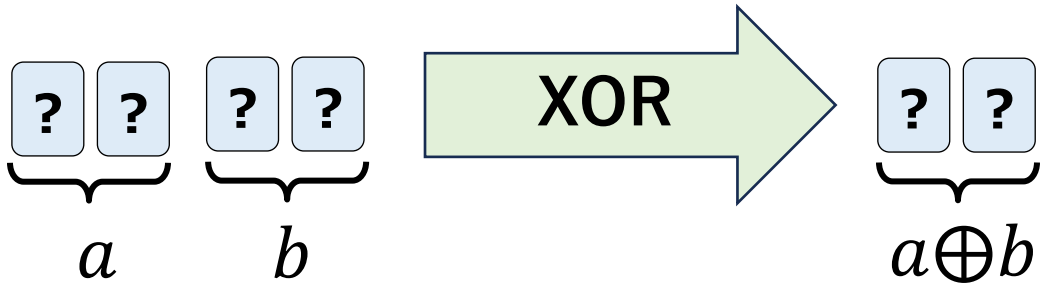
Mizuki-Soneのプロトコル (再掲)



6枚・ **ランダム二等分割カット**1回



6枚・ **ランダム二等分割カット**1回



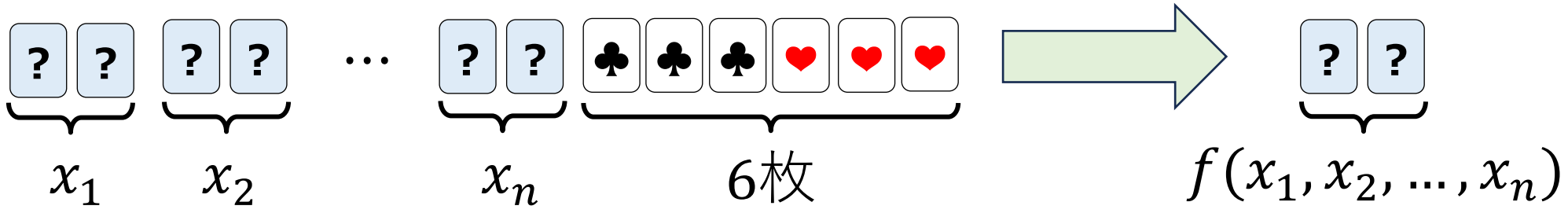
4枚・ **ランダム二等分割カット**1回

計算の効率性の解明

- 理論計算機科学では「計算可能な関数クラス」の特定がまず重要
- 次に考えるべきは「計算の効率性の解明」
  - 計算機の場合：計算時間やメモリ使用量など
- カードベース暗号でまず考えたいのは**カード枚数**
- 任意関数を計算するのに何枚のカードが必要だろうか？

任意関数のプロトコル[Nishida et al., TAMC 2015]

- $2n+6$枚のプロトコル



- 入力に$2n$枚必要だから、最小カード枚数xは$2n \leq x \leq 2n+6$
  - ただし$n=2$のときは有限時間では$x = 2n+1 = 5$であることが解明済

- **未解決問題：$2n+5$枚以下で任意関数を計算可能か？**

T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, Card-Based Protocols for Any Boolean Function, TAMC 2015.

第１部のまとめ

- Five-Card Trick（非コミット型の5枚ANDプロトコル）

- Mizuki-Soneのプロトコル（➡任意関数を計算可能に）
  - コミット型6枚ANDプロトコル
  - コミット型6枚COPYプロトコル
  - コミット型4枚XORプロトコル

- 任意関数の計算に必要なカード枚数は現在のところ$2n+6$枚
  - **未解決問題：$2n+5$枚以下で計算可能か？**

第２部
コミット型ANDプロトコル

なぜANDプロトコルに注目するのか？

- AND/COPY/XORは最も基本的な関数

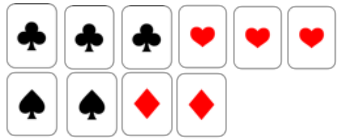
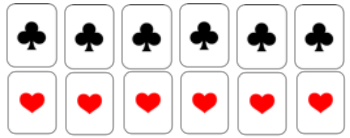
- その中でもANDは構成方法が最も多様
  - XORは加算、ANDは乗算
  - 乗算の方が、加算よりも複雑な計算

- カードベース暗号の歴史を語るのにANDプロトコルは外せない
  - ANDプロトコルの発展に伴い、カードベース暗号の技術が発展してきた

第２部の話

- コミット型ANDの歴史は前半と後半に分かれる
- 前半：2009年のMizuki-Soneまで
- 後半：2015年のKoch-Walzer-Härtelから

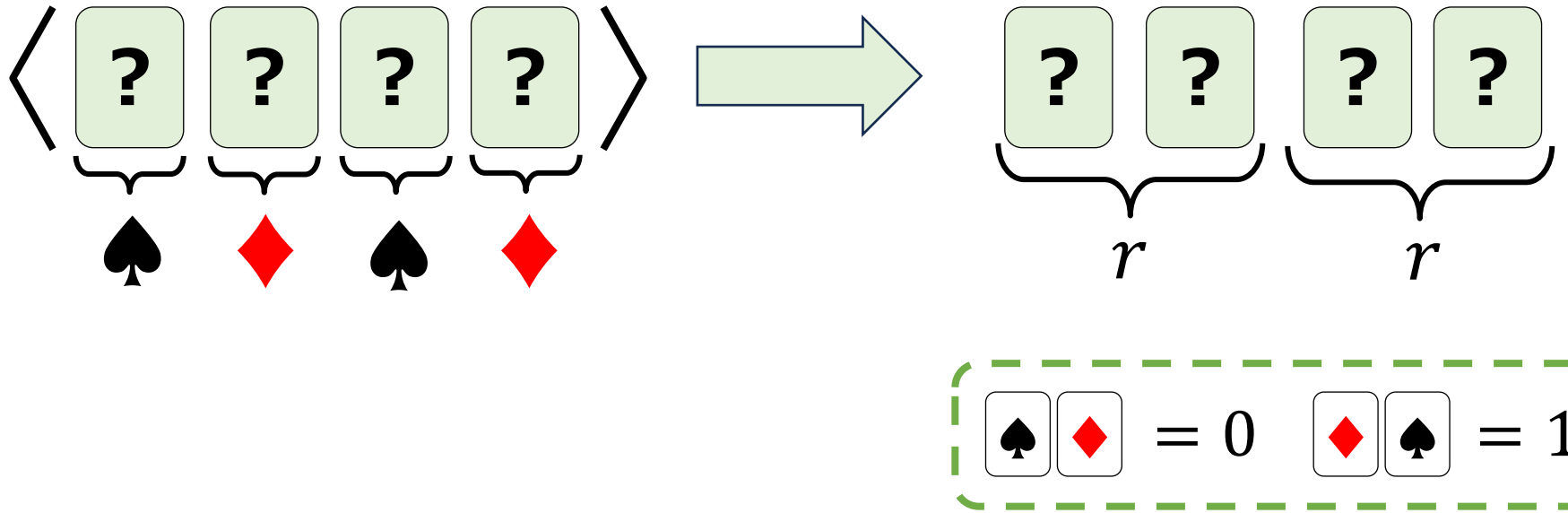
コミット型ANDの歴史 (～2009年)

	カード枚数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)	✓		8 (平均)
Niemi-Renvall [NR98]	12 	✓		7.5 (平均)
Stiglic [Sti01]	8 	✓		2 (平均)
Mizuki-Sone [MS09]	6 		✓	1

[CK94] C. Crépeau and J. Kilian, Discreet Solitary Games, CRYPTO' 93, 1994.
[NR98] V. Niemi and A. Renvall, Secure multiparty computations without computers, Theor. Comput. Sci., 1998.
[Sti01] A. Stiglic, Computations with a Deck of Cards, Theor. Comput. Sci., 2001.
[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009.

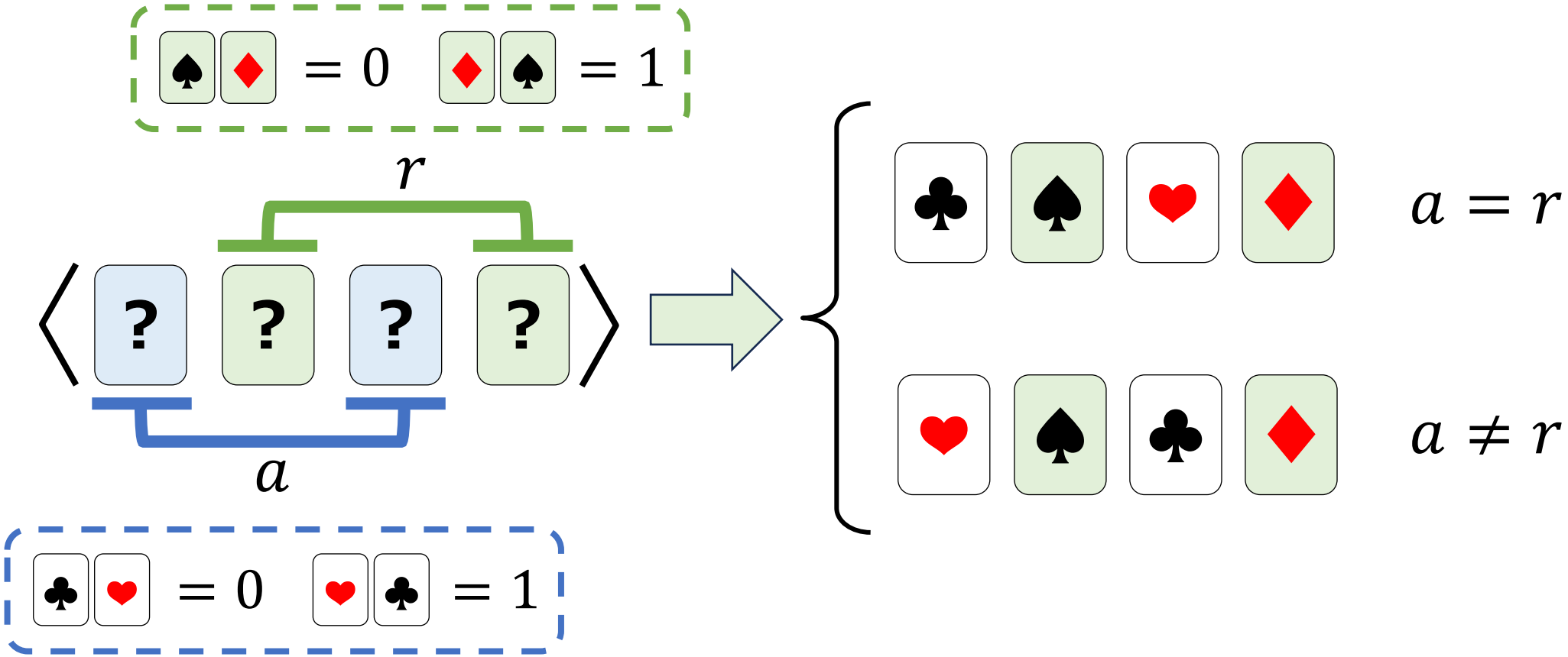
Crépeau-Kilianのアイディア (1/3)

- ♠♦♠♦にランダムカットを施し、ランダムビットrを生成



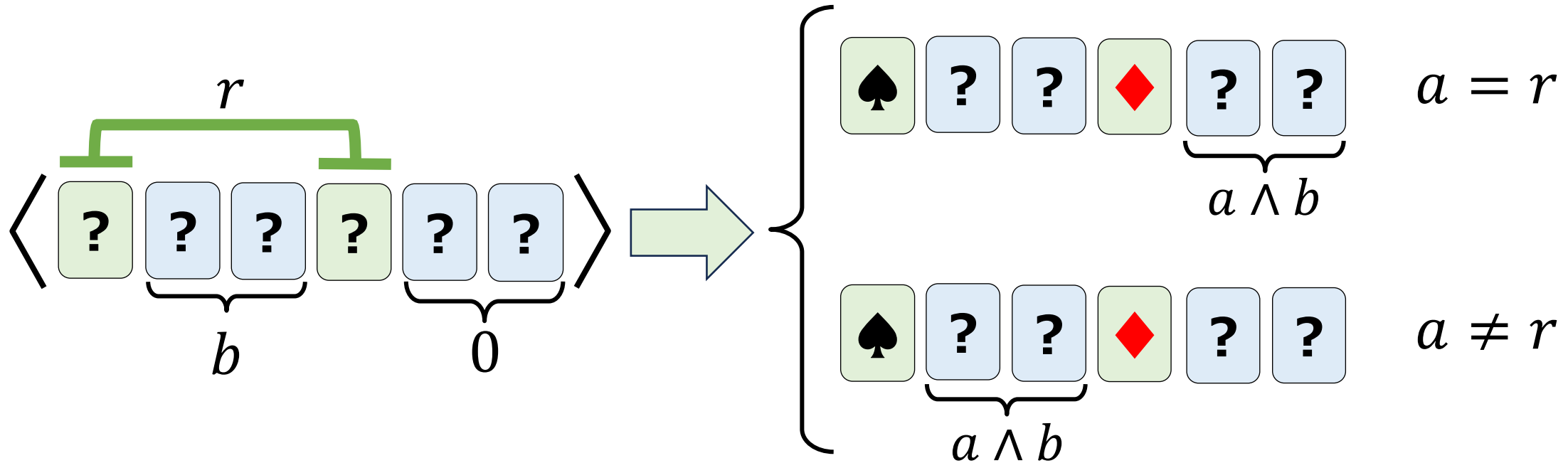
Crépeau-Kilianのアイディア (2/3)

- aとrにランダムカットを施してからめくり、$a = r$かどうか調べる



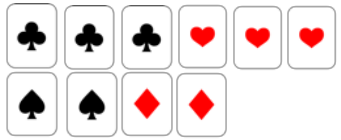
Crépeau-Kilianのアイディア (3/3)

- rと$(b, 0)$にランダムカットを施し、♠♦の位置を特定する
  - めくったカードが♠♦以外ならやり直す（ラスベガスになる原因）



- ポイント：ビットrを介して、aと$(b, 0)$のシャッフルを同期できる

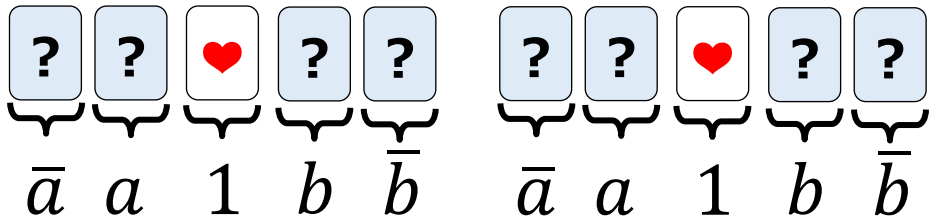
コミット型ANDの歴史 (～2009年)

	カード枚数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)	✓		8 (平均)
Niemi-Renvall [NR98]	12 	✓		7.5 (平均)
Stiglic [Sti01]	8 	✓		2 (平均)
Mizuki-Sone [MS09]	6 		✓	1

[CK94] C. Crépeau and J. Kilian, Discreet Solitary Games, CRYPTO' 93, 1994.
[NR98] V. Niemi and A. Renvall, Secure multiparty computations without computers, Theor. Comput. Sci., 1998.
[Sti01] A. Stiglic, Computations with a Deck of Cards, Theor. Comput. Sci., 2001.
[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009.

Niemi-Renvallのアイディア (1/2)

- Five-Card Trickの列を２個並べる（コピープロトコルを用いる）



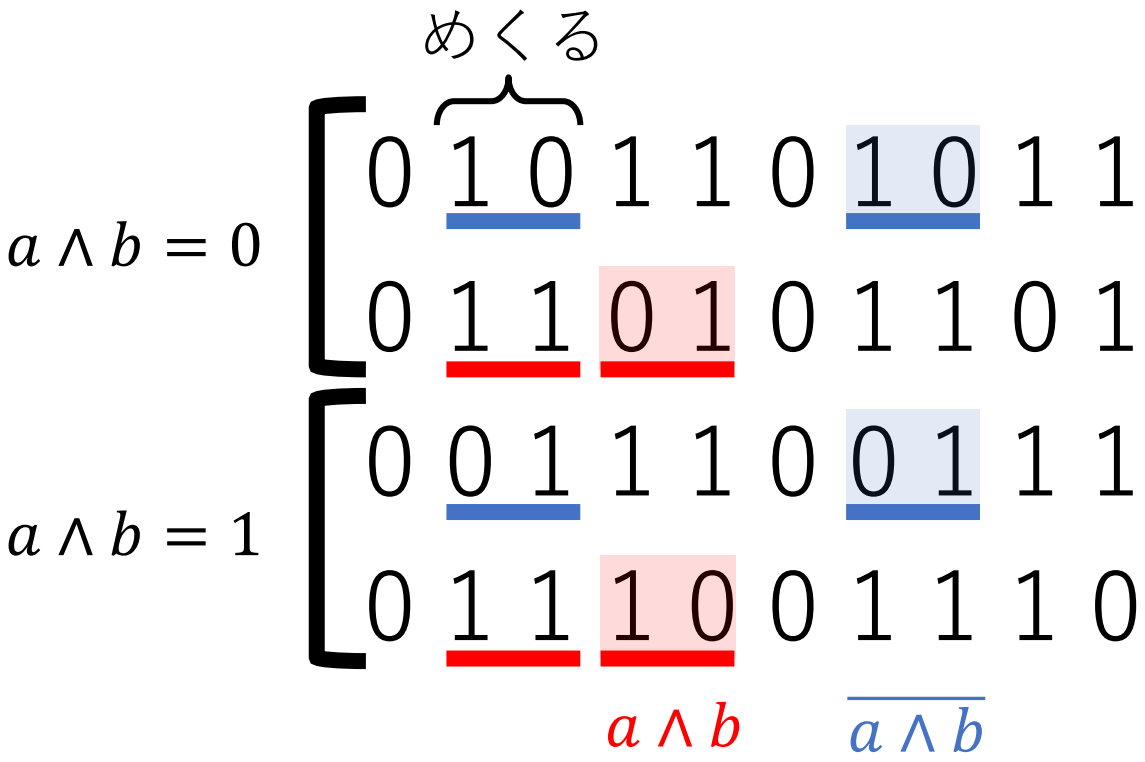
- ♣=0、♥=1の符号化により、真理値表を書いてみる

a	b	$\bar{a}$	a	1	b	$\bar{b}$	$\bar{a}$	a	1	b	$\bar{b}$
0	0	1	0	1	0	1	1	0	1	0	1
0	1	1	0	1	1	0	1	0	1	1	0
1	0	0	1	1	0	1	0	1	1	0	1
1	1	0	1	1	1	0	0	1	1	1	0

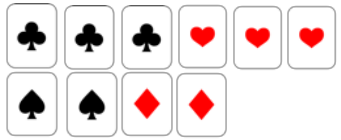
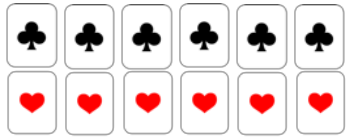
巡回的に等しい

Niemi-Renvallのアイディア (2/2)

- ランダムカットをして、先頭を♣=0に揃える（ラスベガス）
- 2-3枚目をランダムカットしてめくり、青と赤に分岐する



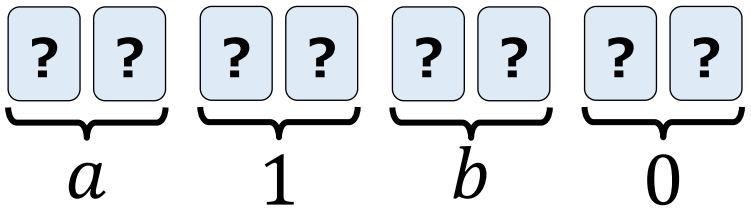
コミット型ANDの歴史 (～2009年)

	カード枚数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)	✓		8 (平均)
Niemi-Renvall [NR98]	12 	✓		7.5 (平均)
Stiglic [Sti01]	8 	✓		2 (平均)
Mizuki-Sone [MS09]	6 		✓	1

[CK94] C. Crépeau and J. Kilian, Discreet Solitary Games, CRYPTO' 93, 1994.
[NR98] V. Niemi and A. Renvall, Secure multiparty computations without computers, Theor. Comput. Sci., 1998.
[Sti01] A. Stiglic, Computations with a Deck of Cards, Theor. Comput. Sci., 2001.
[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009.

Stiglicのアイディア (1/2)

- 以下のようにカード列を並べる



- ♣=0、❤=1の符号化により、真理値表を書いてみる

a	b	a	$\bar{a}$	1	0	b	$\bar{b}$	0	1
0	0	0	1	1	0	0	1	0	1
0	1	0	1	1	0	1	0	0	1
1	0	1	0	1	0	0	1	0	1
1	1	1	0	1	0	1	0	0	1

Stiglicのアイディア (2/2)

- ランダムカットをして、先頭を♣♣=00に揃える（ラスベガス）

$$\begin{matrix} & \\ a\wedge b=0 \\ a\wedge b=1 \\ & \end{matrix}\begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

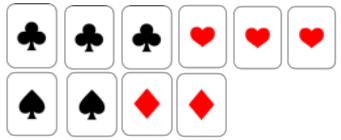
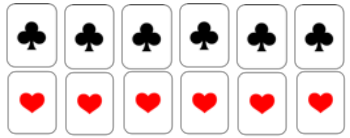
$a\wedge b$

- 先頭を❤❤=11に揃えた場合も計算できる

$$\begin{matrix} & \\ a\wedge b=0 \\ a\wedge b=1 \\ & \end{matrix}\begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$a\wedge b$

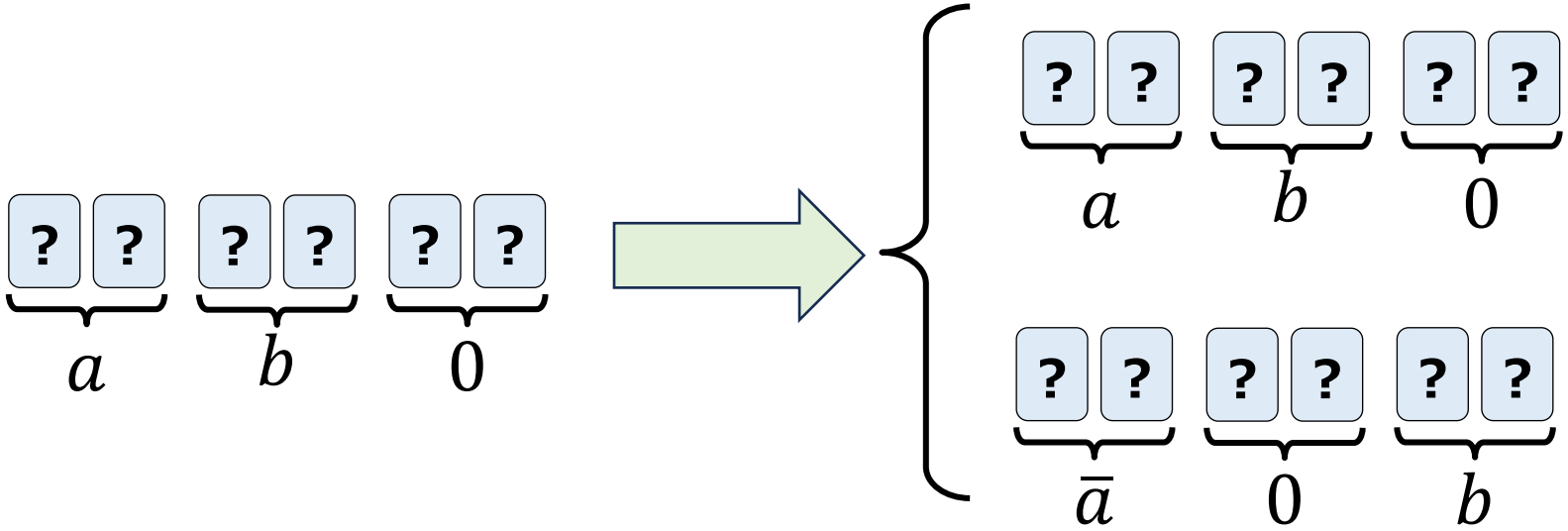
コミット型ANDの歴史 (～2009年)

	カード枚数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)	✓		8 (平均)
Niemi-Renvall [NR98]	12 	✓		7.5 (平均)
Stiglic [Sti01]	8 	✓		2 (平均)
Mizuki-Sone [MS09]	6 		✓	1

[CK94] C. Crépeau and J. Kilian, Discreet Solitary Games, CRYPTO' 93, 1994.
[NR98] V. Niemi and A. Renvall, Secure multiparty computations without computers, Theor. Comput. Sci., 1998.
[Sti01] A. Stiglic, Computations with a Deck of Cards, Theor. Comput. Sci., 2001.
[MS09] T. Mizuki and H. Sone, Six-Card Secure AND and Four-Card Secure XOR, FAW 2009.

Mizuki-Soneのアイディア

- ランダム二等分割カットでaと$(b, 0)$の同期シャッフル



- ランダム二等分割カットでCrépeau-Kilianを実現したともみなせる

この頃 (2009～2014)の重要な進展

- ランダム二等分割カット（RBC）の発見
  - シャッフル操作は以前はランダムカットしか存在しなかった
  - RBCにより種々のプロトコルの効率化が可能となった
    - 例：非コミット型ANDプロトコルを5枚(Five-Card Trick)から4枚に削減

- 計算モデル（**Mizuki-Shizuyaモデル**）の提案[Mizuki-Shizuya, IJIS14]
  - プロトコルは並べ替え/シャッフル/めくる操作を許す
  - 次の操作は現在の**状態**と**可視カード列**から決定する
  - これにより、計算限界の研究（不可能性証明）もできるようになった

T. Mizuki and H. Shizuya, A formalization of card-based cryptographic protocols via abstract machine, Int. J. Inf. Sec. 2014.

この頃 (2009〜2014)の空気感

- ランダム二等分割カットを使って何ができるか
  - 4枚非コミット型ANDプロトコル
  - 多数決関数プロトコル
  - 任意関数プロトコル/対称関数プロトコル

- 予想：Mizuki-Soneの6枚ANDはカード枚数最小
  - 2枚1ビットの符号化では6枚＝3ビット
  - 4枚=2ビットでは感覚的にANDを構成できなさそう
  - 5枚=2.5ビットは使い方が難しそう
    - 「確率的失敗を許す」 5枚ANDプロトコルは構成されていた

Koch-Walzer-Härtelの結果[Koch-Walzer-Härtel, Asiacrypt 2015]

- 不可能性証明
  - 有限時間の4枚ANDプロトコルの不可能性を証明

- プロトコル構成
  - 4枚ラスベガスANDプロトコル
  - 5枚有限時間ANDプロトコル

A. Koch, S. Walzer, and K. Härtel, Card-Based Cryptographic Protocols Using a Minimal Number of Cards, Asiacrypt 2015.

有限時間の4枚ANDの不可能性(1/3)

- オブザベーション
  - 4枚カード列：♡♡♣♣, ♡♣♡♣, ♡♣♣♡, ♣♡♡♣, ♣♡♣♡, ♣♣♡♡
  - プロトコル中の**ステート**は4枚カード列の値をとる確率分布とみなせる

- ステートの例

カード列	確率
♡♡♣♣	0
♡♣♡♣	X_{00}
♡♣♣♡	$0.5X_{01} + 0.5X_{10}$
♣♡♡♣	0
♣♡♣♡	$0.5X_{01} + 0.5X_{10}$
♣♣♡♡	X_{11}

有限時間の4枚ANDの不可能性(2/3)

- ステートの全体集合を二つの集合に分割
  - Bad集合：入力ステートを含む集合
  - Good集合：出力ステート(プロトコル終了時のステート)を含む集合

入力ステート

カード列	確率
♡♡♣♣	0
♡♣♡♣	X_{11}
♡♣♣♡	X_{10}
♣♡♡♣	X_{01}
♣♡♣♡	X_{00}
♣♣♡♡	0

出力ステート

カード列	確率
♡♡♣♣	0
♡♣♡♣	p_1
♡♣♣♡	p_2
♣♡♡♣	q_1
♣♡♣♡	q_2
♣♣♡♡	0

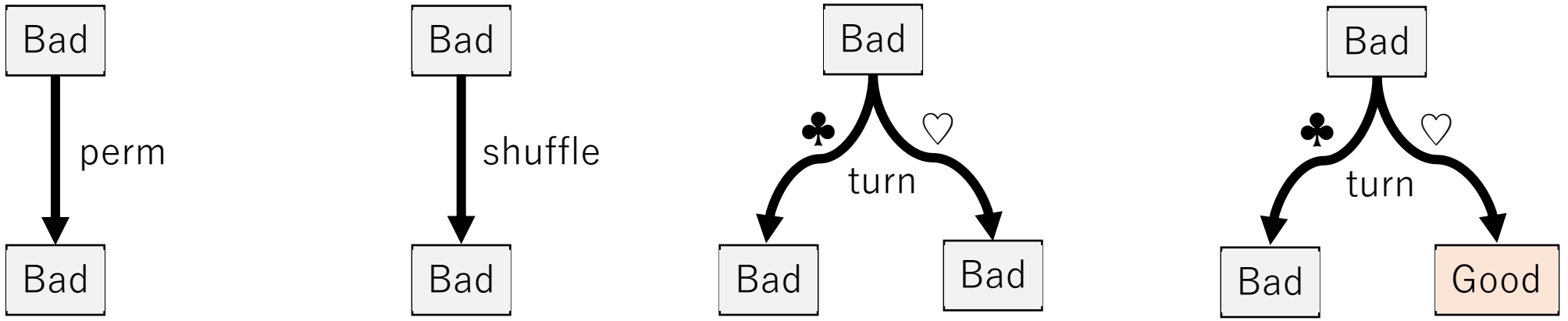
出力列

p_iはX_{11}の多項式

q_iはX_{00}, X_{01}, X_{10}の多項式

有限時間の4枚ANDの不可能性(3/3)

- 補題
  - Badステートに任意の操作を施しても、必ずBadステートが生まれてしまう

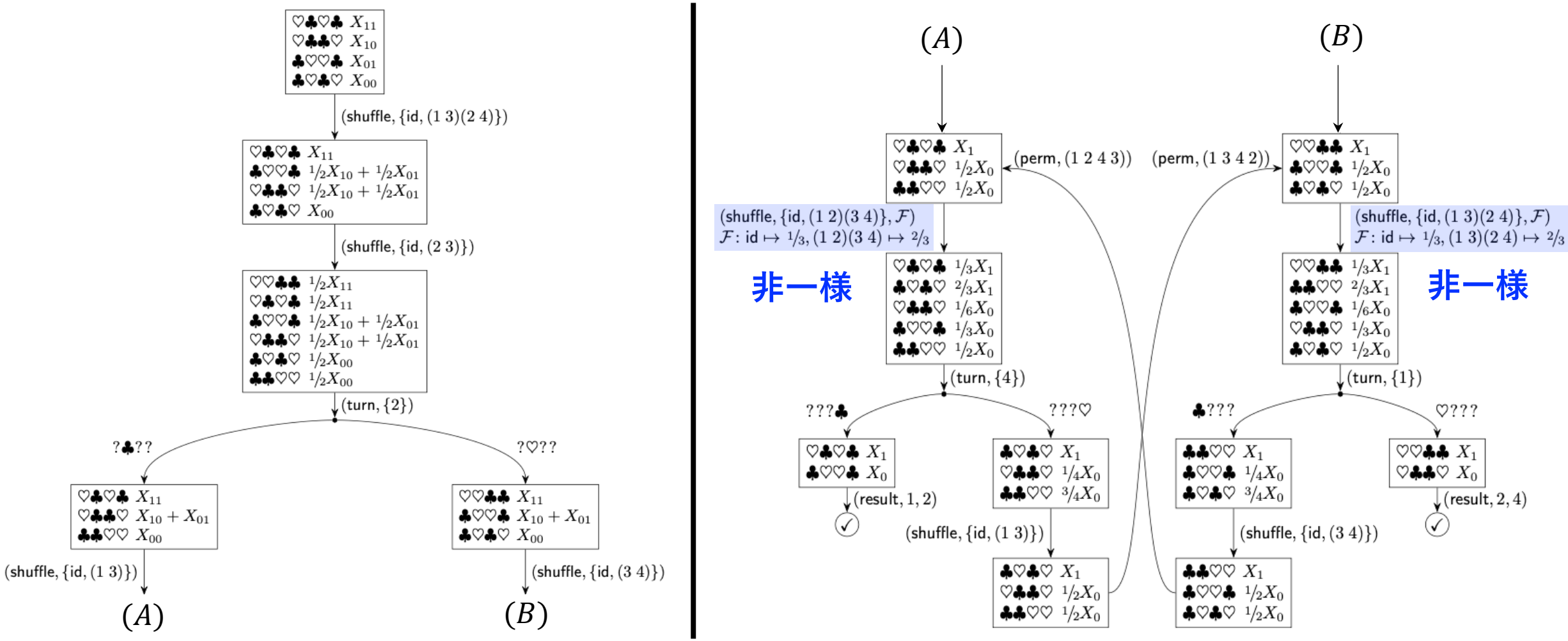


- このことから4枚ANDプロトコルの不可能性が導かれる
  - 「入力ステートから出発し、全部の分岐で出力ステートに到達すること」は不可能

シャッフルの性質

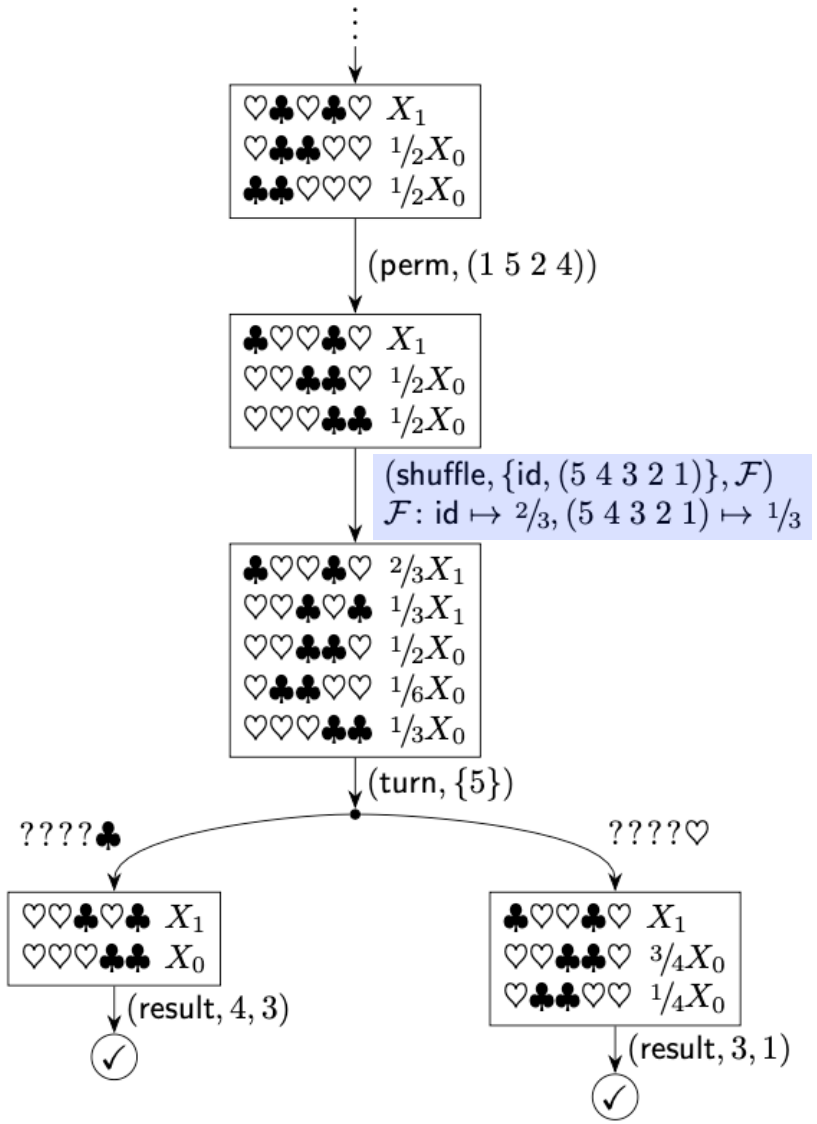
- $(\mathrm{shuffle}, \Pi, \mathcal{F})$：分布$\mathcal{F}$に従って、置換$\pi \in \Pi$を適用
- **一様シャッフル**$(\mathrm{shuffle}, \Pi, \mathcal{F}) \Leftrightarrow \mathcal{F}$が$\Pi$上の一様分布
- **閉シャッフル**$(\mathrm{shuffle}, \Pi, \mathcal{F}) \Leftrightarrow \Pi$が部分群

[KWH15]の4枚ラスベガスANDプロトコル



※[KWH15]のFig.4より

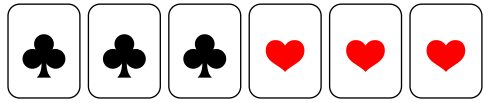
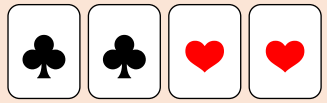
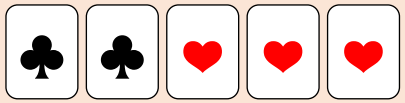
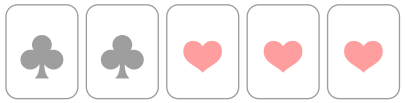
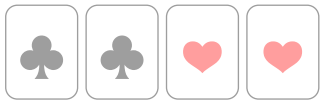
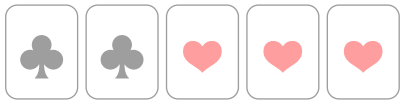
[KWH15]の5枚有限時間ANDプロトコル



非一様かつ非閉

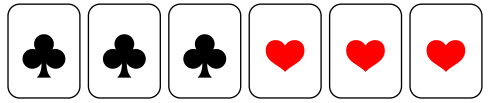
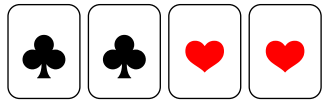
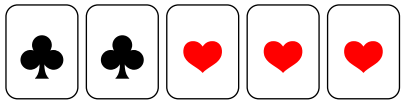
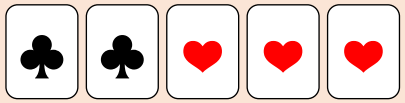
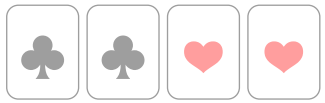
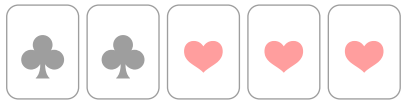
※[KWH15]のFig.5より

コミット型ANDプロトコル (2009年〜)

	カード枚数	有限時間	一様	閉
Mizuki-Sone [MS09]	6 	✓	✓	✓
Koch et al. [KWH15]	4 			✓
Koch et al. [KWH15]	5 	✓		
Abe et al. [AHMS18]	5 		✓	✓
Koch [Koc22] Ruangwises-Itoh [RI19]	4 		✓	
Koch [Koc22] Ruangwises-Itoh [RI19]	5 	✓	✓	

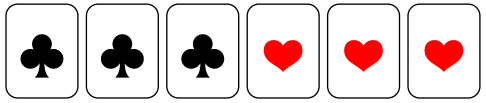
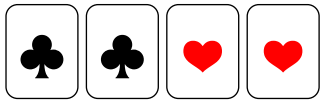
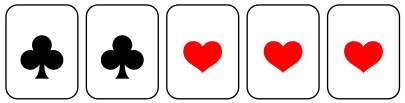
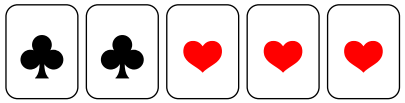
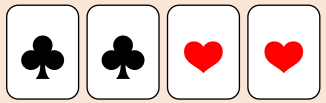
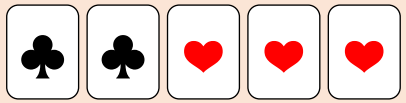
[KWH15] A. Koch, S. Walzer, and K. Härtel, Card-Based Cryptographic Protocols Using a Minimal Number of Cards, Asiacrypt 2015.
[AHMS18] Y. Abe, Y. Hayashi, T. Mizuki, and H. Sone, Five-Card AND Protocol in Committed Format Using Only Practical Shuffles, APKC 2018.
[RI19] S. Ruangwises and T. Itoh, AND Protocols Using only Uniform Shuffles, CSR 2019.
[Koc22] A. Koch, The Landscape of Optimal Card-Based Protocols, Mathematical Cryptology 2022.

コミット型ANDプロトコル (2009年〜)

	カード枚数	有限時間	一様	閉
Mizuki-Sone [MS09]	6 	✓	✓	✓
Koch et al. [KWH15]	4 			✓
Koch et al. [KWH15]	5 	✓		
Abe et al. [AHMS18]	5 		✓	✓
Koch [Koc22] Ruangwises-Itoh [RI19]	4 		✓	
Koch [Koc22] Ruangwises-Itoh [RI19]	5 	✓	✓	

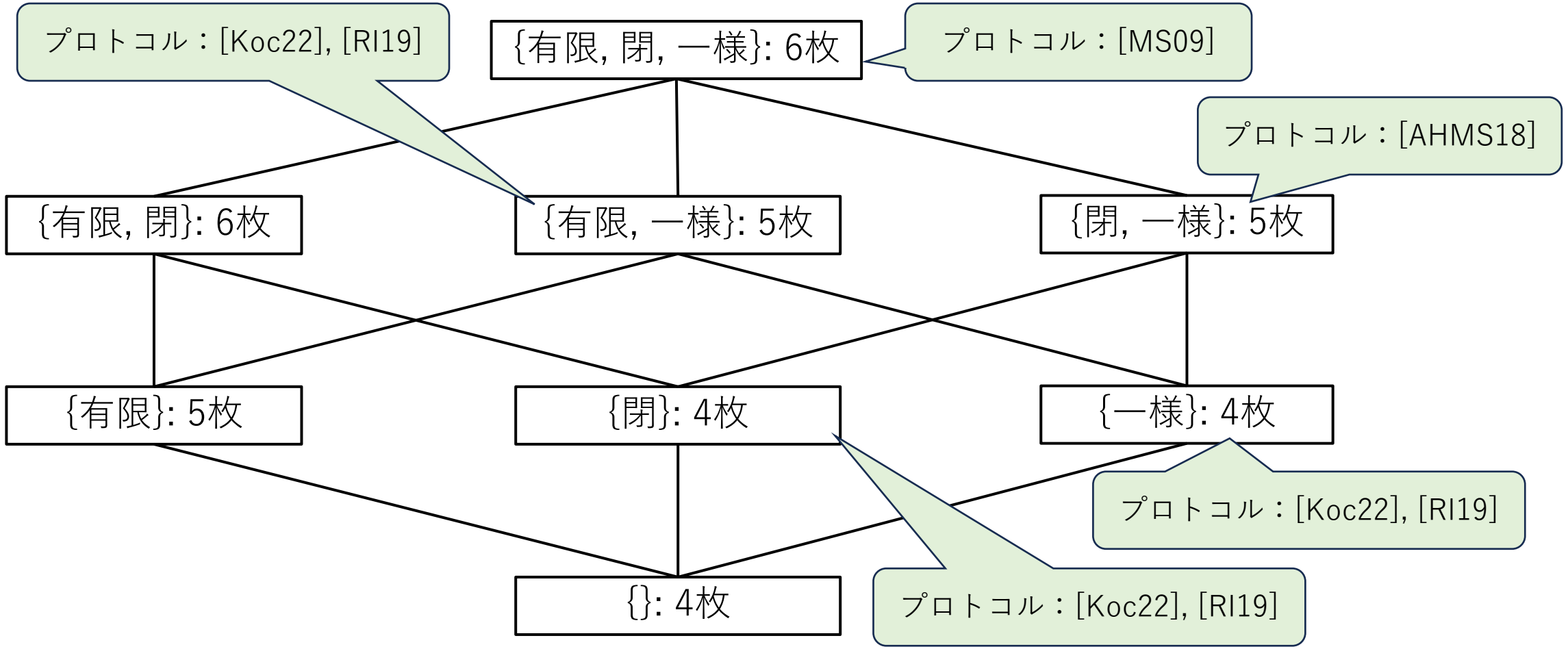
[KWH15] A. Koch, S. Walzer, and K. Härtel, Card-Based Cryptographic Protocols Using a Minimal Number of Cards, Asiacrypt 2015.
[AHMS18] Y. Abe, Y. Hayashi, T. Mizuki, and H. Sone, Five-Card AND Protocol in Committed Format Using Only Practical Shuffles, APKC 2018.
[RI19] S. Ruangwises and T. Itoh, AND Protocols Using only Uniform Shuffles, CSR 2019.
[Koc22] A. Koch, The Landscape of Optimal Card-Based Protocols, Mathematical Cryptology 2022.

コミット型ANDプロトコル (2009年〜)

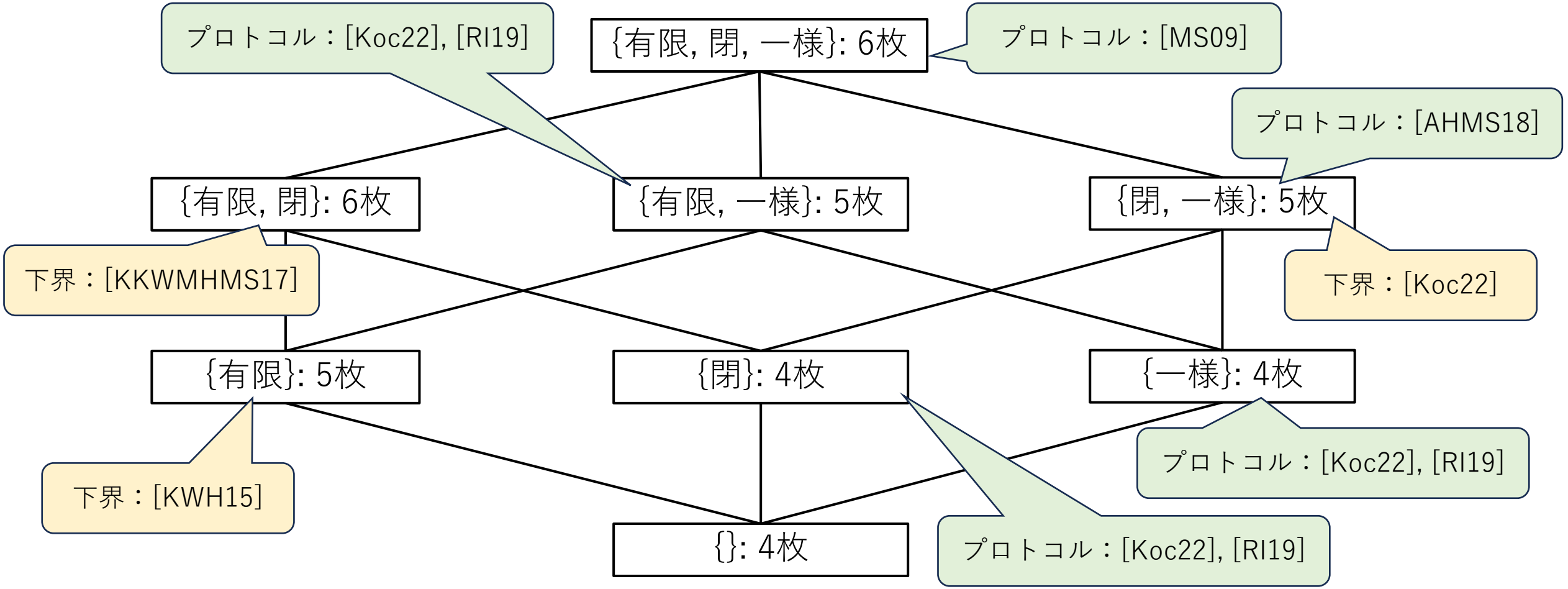
	カード枚数	有限時間	一様	閉
Mizuki-Sone [MS09]	6 	✓	✓	✓
Koch et al. [KWH15]	4 			✓
Koch et al. [KWH15]	5 	✓		
Abe et al. [AHMS18]	5 		✓	✓
Koch [Koc22] Ruangwises-Itoh [RI19]	4 		✓	
Koch [Koc22] Ruangwises-Itoh [RI19]	5 	✓	✓	

[KWH15] A. Koch, S. Walzer, and K. Härtel, Card-Based Cryptographic Protocols Using a Minimal Number of Cards, Asiacrypt 2015.
[AHMS18] Y. Abe, Y. Hayashi, T. Mizuki, and H. Sone, Five-Card AND Protocol in Committed Format Using Only Practical Shuffles, APKC 2018.
[RI19] S. Ruangwises and T. Itoh, AND Protocols Using only Uniform Shuffles, CSR 2019.
[Koc22] A. Koch, The Landscape of Optimal Card-Based Protocols, Mathematical Cryptology 2022.

最適なコミット型ANDプロトコル



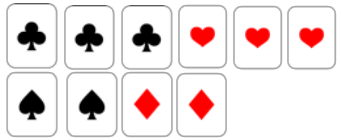
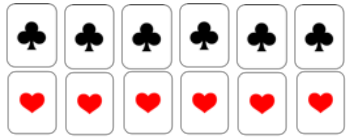
最適なコミット型ANDプロトコル



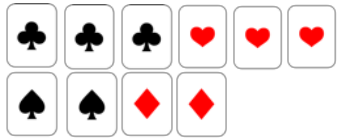
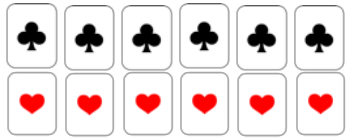
[KKWMHMS17] J. Kastner, A. Koch, S. Walzer, D. Miyahara, Y. Hayashi, T. Mizuki, and H. Sone, The Minimum Number of Cards in Practical Card-Based Protocols, Asiacrypt 2017.

ランダムカットオンリーの世界では？

- 「任意のシャッフルを許す」のはMizuki-Shizuyaモデルの世界観
- ランダムカットのみを用いた有限時間ANDは構成できるか？

	カード枚数	有限時間	ランダムカット	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)		✓	8
Niemi-Renvall [NR98]	12 		✓	7.5
Stiglic [Sti01]	8 		✓	2

ランダムカットオンリーの有限時間AND

	カード枚数	有限時間	RCのみ	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)		✓	8
Niemi-Renvall [NR98]	12 		✓	7.5
Stiglic [Sti01]	8 		✓	2
Abe-Mizuki-Sone [AMS21]	6 	✓	✓	2

[AMS21] Y. Abe, T. Mizuki, H. Sone, Committed-format AND protocol using only random cuts, Natural Computing 2021.

第２部のまとめ

- コミット型ANDプロトコルの改良の歴史を眺めた
  - Crépeau-Kilianの10枚ラスベガスAND
  - Niemi-Renvallの12枚ラスベガスAND
  - Stiglicの8枚ラスベガスAND
  - Mizuki-Soneの6枚有限時間AND
  - Koch-Walzer-Härtelの4枚ラスベガスAND & 5枚有限時間ANDと不可能性証明
  - Abe et al.の5枚ラスベガスAND
  - KochとRuangwises-Itohの4枚ラスベガスAND & 5枚有限時間AND
  - Abe-Mizuki-Soneのランダムカットオンリーの6枚有限時間AND

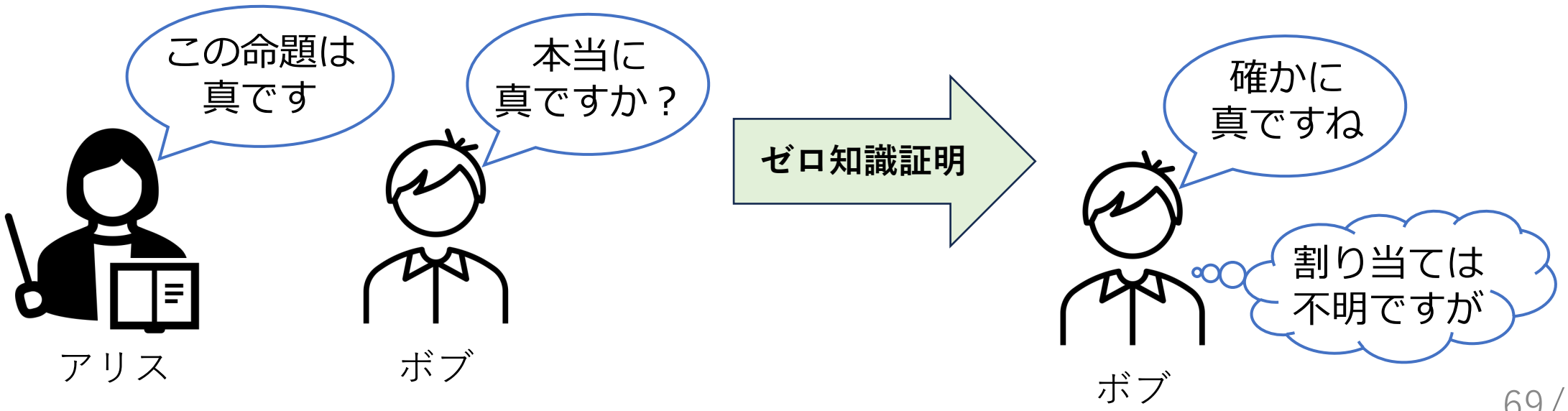
- カード枚数については多くの場合で最適値が解決済
  - **未解決問題：各枚数についてシャッフル回数の最小値は？**
  - **未解決問題：トランプカードを用いた場合は？**

第３部
数独のゼロ知識証明

ゼロ知識証明 (Zero-Knowledge Proof: ZKP)

- ある命題が正しいことを「その命題が正しいこと」以外の情報を漏らさずに納得させることのできる技術

命題： 論理式$\varphi(x_1, \ldots, x_n)$を真にする割り当て$x_i \in \{T, F\}$が存在する



パズルに対するZKP

- アリスはあるパズルの答えを知っている
- ボブは「この問題には答えが存在しないのでは」と疑っている
- どうやって、ボブに「答えが存在すること」を納得させられるか？
- ただし、答え自体を教えて問題を解く楽しみを奪ってはいけない

		3			9		1	
6				4				5
		7	3			6		
		4	2					3
		9		1			8	
	8				5	9		1
			4					
		8		7	6	1		4
							2	

カードベースZKP

- カードを用いたZKP
  - 論理式の秘密計算によるゼロ知識証明[NR99]

- パズルのカードベースZKP
  - Gradwohl, Naor, Pinkas, Rothblumの数独プロトコル[GNPR07]
  - 各種パズルに対するプロトコルが研究されている
    - Robert, Pascal, Miyahara, MizukiのグループとRuangwisesのグループが牽引

- 「実行のしやすさ」の観点から設計される場合が多い
  - 基本的にpracticalなシャッフルのみに限定する

[NR99] V. Niemi and A. Renvall, Solitaire Zero-knowledge, Fundamenta Informaticae 1999.
[GNPR07] R. Gradwohl, M. Naor, B. Pinkas, G. N. Rothblum, Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles, FUN 2007.

数独

- 別名ナンバープレイス（数独はニコリの商標）
- パズル雑誌ニコリの鍜治真起が「数字は独身に限る」と名付けた
- 世界で最も知名度のあるパズルの一つ
- カードZKP分野でも、数独は最も研究が進んでいるパズル

数独のルール

- タテ・ヨコ・ブロックに1～9が揃うように数字を埋めるパズル

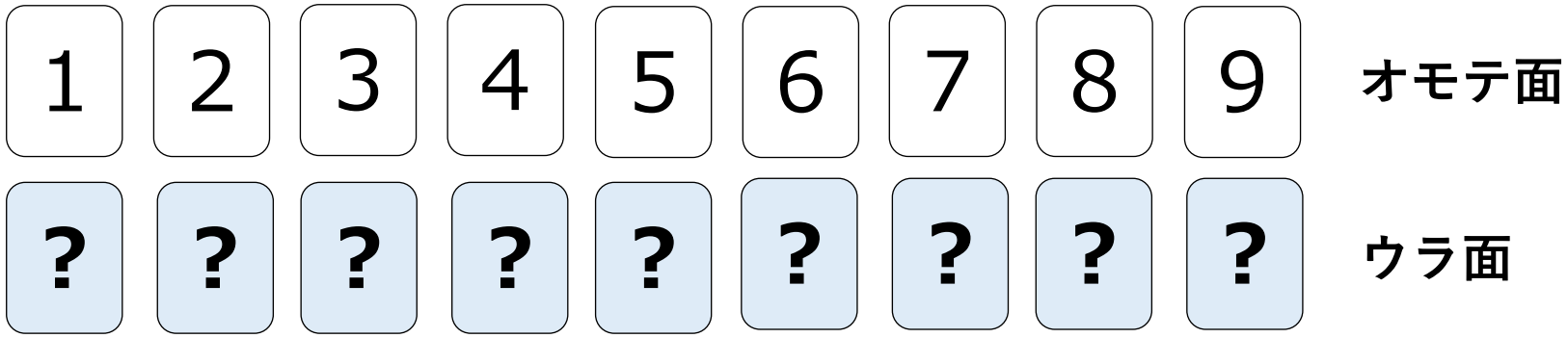
問題

		3			9		1	
6				4				5
		7	3			6		
		4	2					3
		9		1			8	
	8				5	9		1
			4					
		8		7	6	1		4
							2	

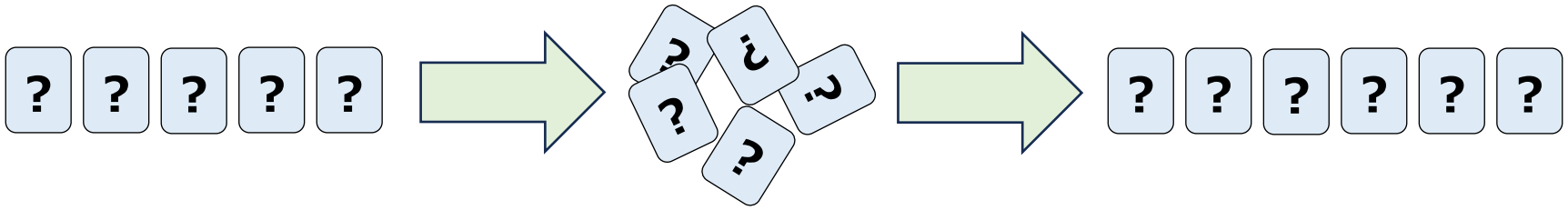
答え

8	2	3	5	6	9	4	1	7
6	9	1	8	4	7	2	3	5
5	4	7	3	2	1	6	9	8
1	5	4	2	9	8	7	6	3
3	6	9	7	1	4	5	8	2
7	8	2	6	3	5	9	4	1
9	1	5	4	8	2	3	7	6
2	3	8	9	7	6	1	5	4
4	7	6	1	5	3	8	2	9

カードとシャッフル

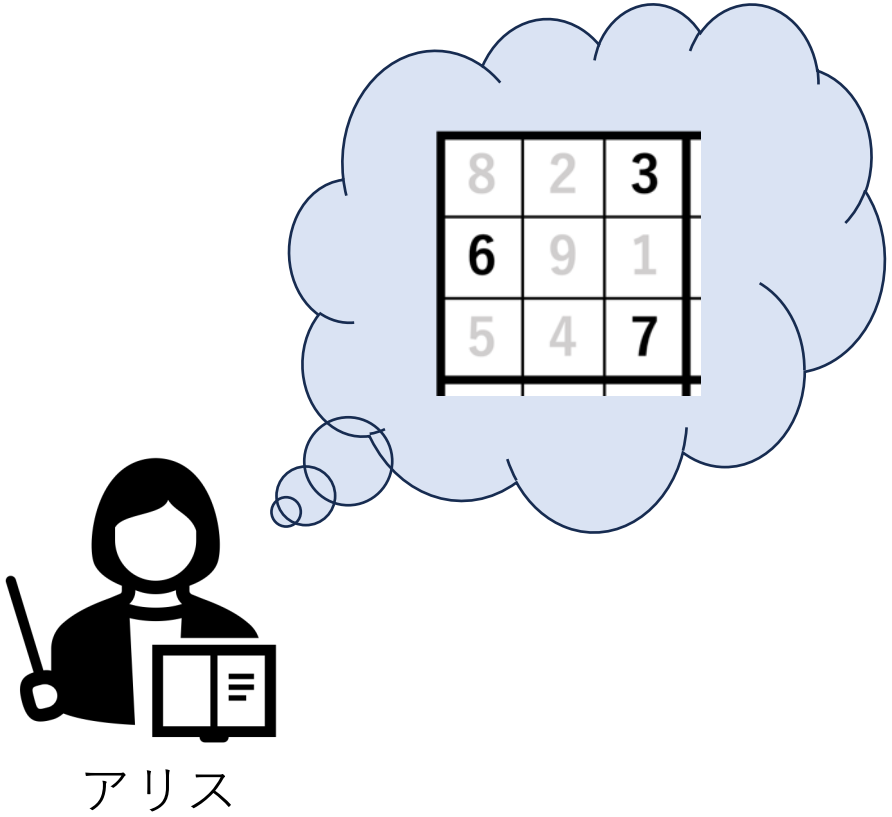


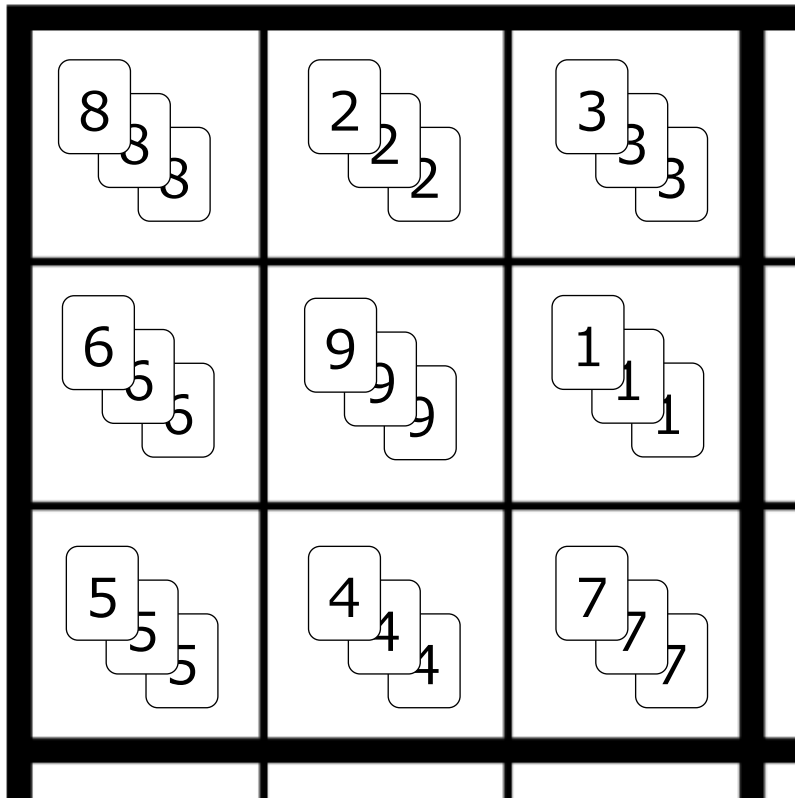
- **完全シャッフル**



GNPRプロトコル[Gradwohl-Naor-Pinkas-Rothblum, FUN 2007]

1. アリスは各マスに対応するカードを3枚ずつ裏向きに置く
   - ただし、最初から数字のあるマスは表向きに置く

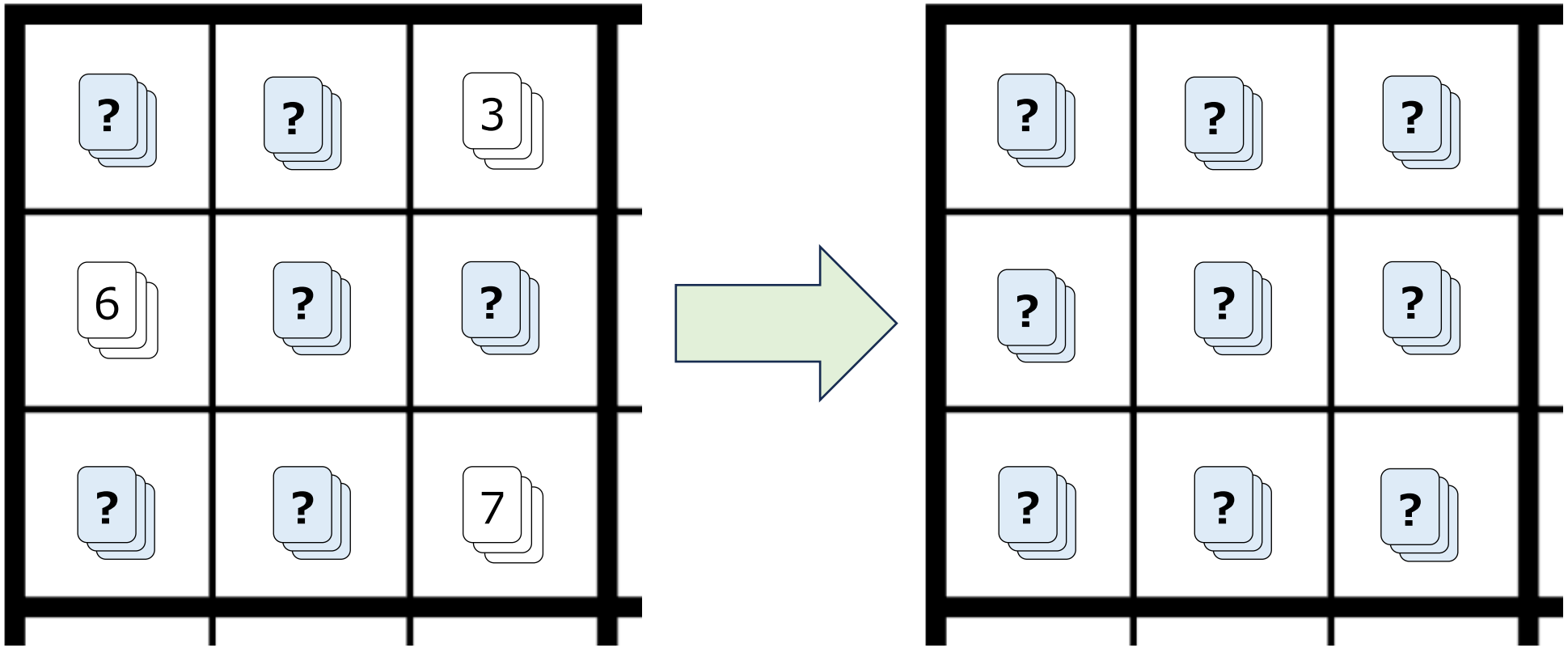




R. Gradwohl, M. Naor, B. Pinkas, and G. N. Rothblum, Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles, FUN 2007.

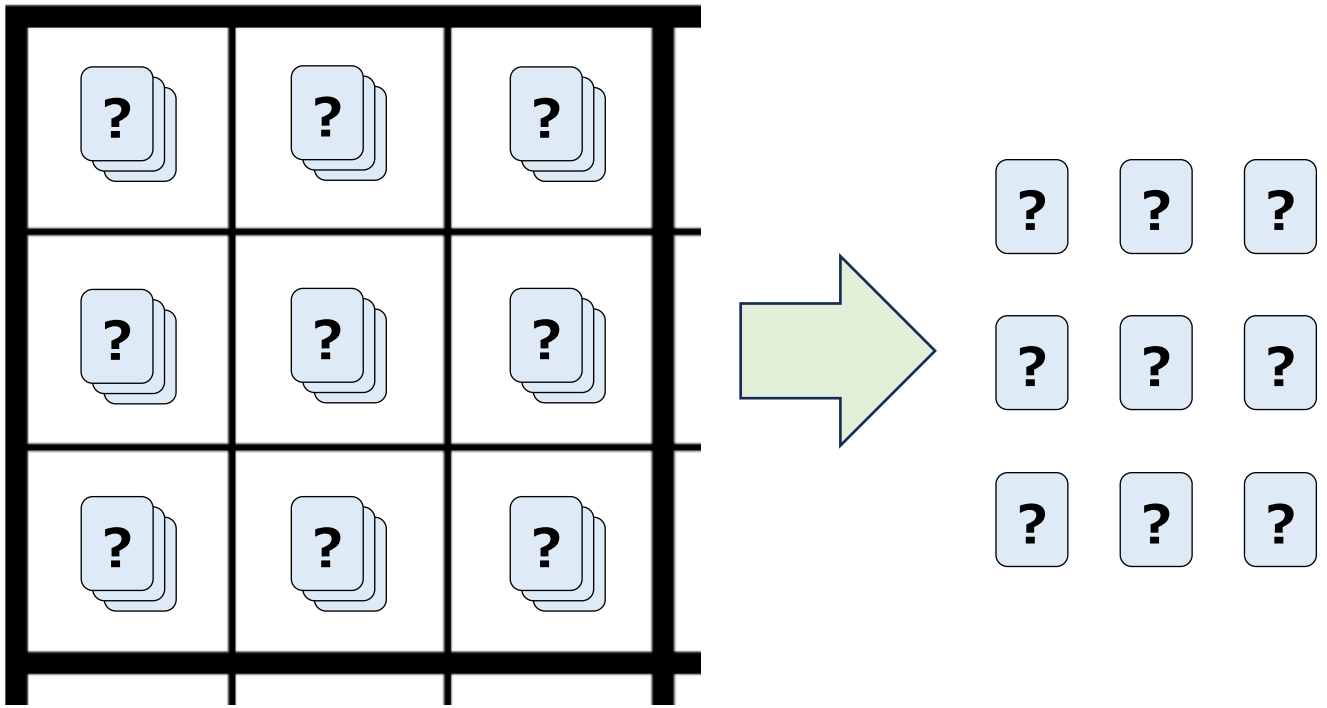
GNPRプロトコル

2. ヒントマスのカードを裏にする



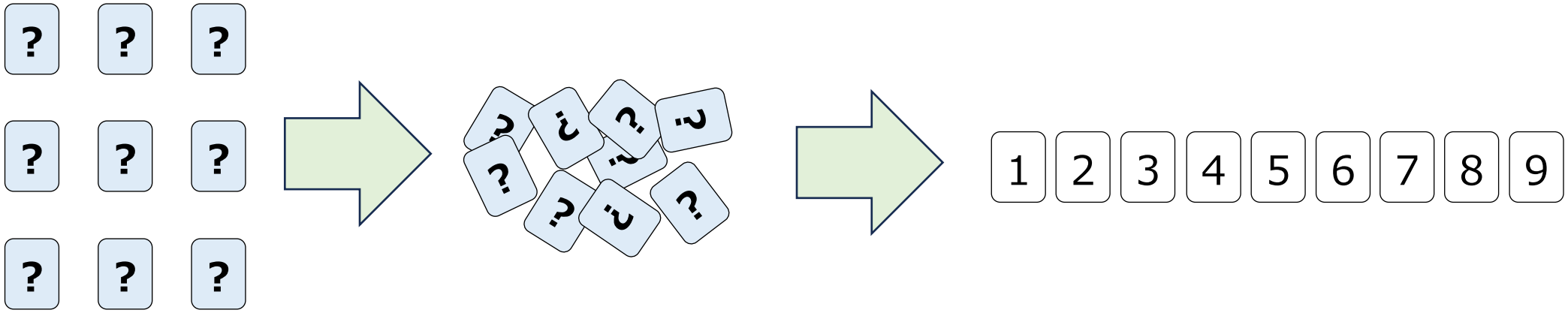
GNPRプロトコル

3. 検証したい行の各マスからカードを1枚ランダムに選び、合計9枚のカードを1つの束とする
   - 各行・各列・各ブロックについて同様に束を作る（合計27個の束を作る）



GNPRプロトコル

4. 各束に完全シャッフルを施し、すべてめくる
   - すべての束について、1～9が揃っていたら、ボブは納得する



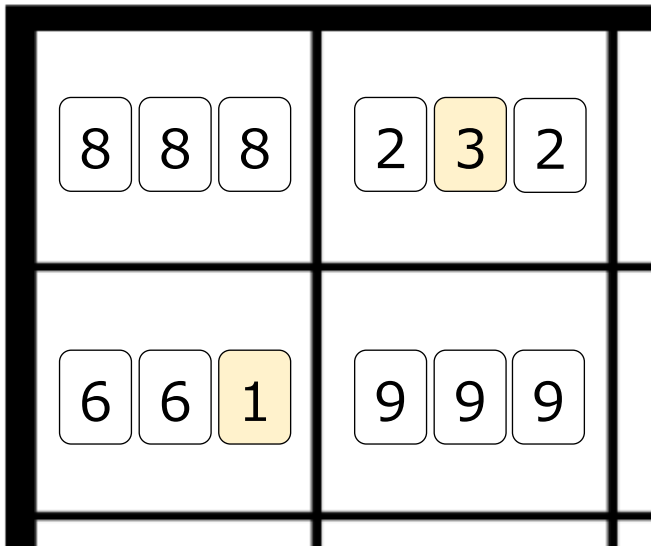
数独のゼロ知識証明プロトコル（※interactiveなプロトコルは除く）

	カード枚数	シャッフル回数	シャッフルの種類
Gradwohl et al. [GNPR07]	$3n^2$	$3n\ell$ (ℓ:繰返し回数)	Complete
Sasaki et al. [SMMS20]	n^2+n	$5n$	PScramble
Sasaki et al. [SMMS20]	$2n^2+n$	$4n$	PScramble
Tanaka-Mizuki [TM23]	$n^2+n(\sqrt{n}+1)$	$7\sqrt{n}-5$	PScramble
佐々木-品川 [SS23]	$4n^2$	3	PScramble
田中-水木 [TM24]	$4n^2$	2	PScramble

[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[TM23] K, Tanaka and T. Mizuki, Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku, FCT 2023.
[SS23] 佐々木, 品川, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム, 2023.
[TM24] 田中, 水木, 2回あるいは1回のシャッフルを用いた数独に対する物理的ゼロ知識証明, 暗号と情報セキュリティシンポジウム, 2024.

GNPRプロトコルの健全性エラー

- 答えが存在しないパズルでもボブが納得する場合がわずかにある
- 悪いアリスの戦略：異なる3枚のカードを配置する



- 健全性エラーを減らすために、繰り返し実行する必要がある
- 健全性エラーをゼロにすることはできないか？

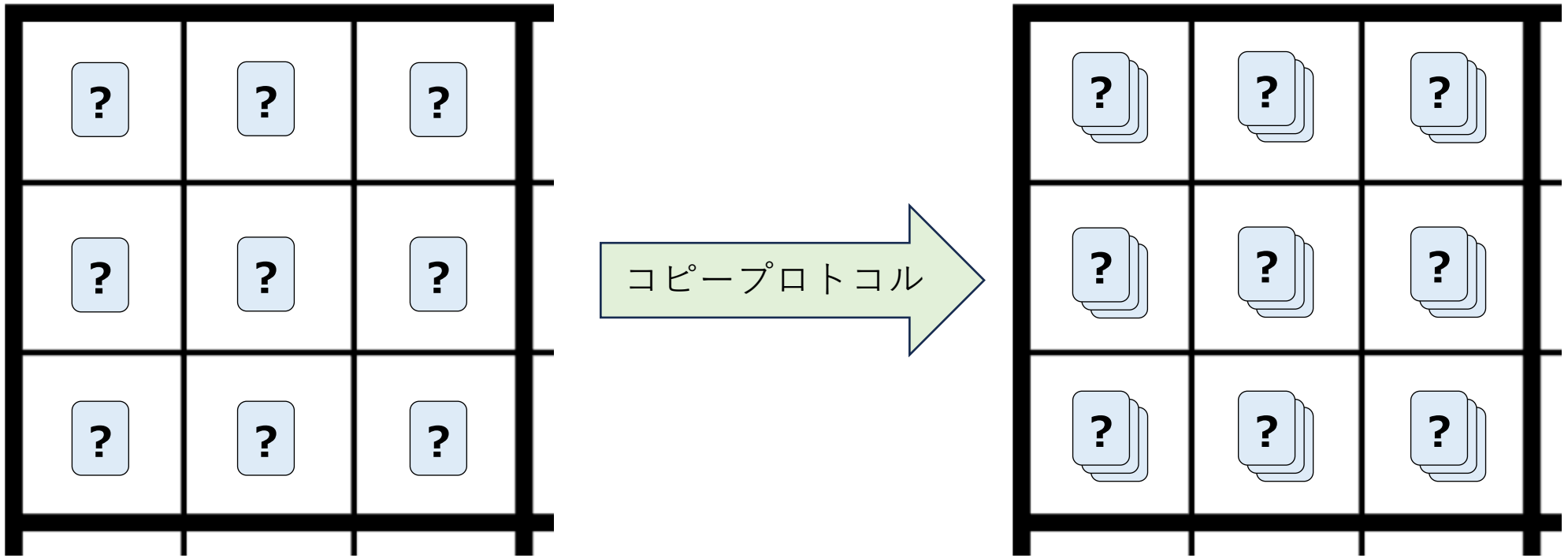
数独のゼロ知識証明プロトコル（※interactiveなプロトコルは除く）

	カード枚数	シャッフル回数	シャッフルの種類
Gradwohl et al. [GNPR07]	$3n^2$	$3n\ell$ (ℓ:繰返し回数)	Complete
Sasaki et al. [SMMS20]	n^2+n	$5n$	PScramble
Sasaki et al. [SMMS20]	$2n^2+n$	$4n$	PScramble
Tanaka-Mizuki [TM23]	$n^2+n(\sqrt{n}+1)$	$7\sqrt{n}-5$	PScramble
佐々木-品川 [SS23]	$4n^2$	3	PScramble
田中-水木 [TM24]	$4n^2$	2	PScramble

[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[TM23] K, Tanaka and T. Mizuki, Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku, FCT 2023.
[SS23] 佐々木, 品川, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム, 2023.
[TM24] 田中, 水木, 2回あるいは1回のシャッフルを用いた数独に対する物理的ゼロ知識証明, 暗号と情報セキュリティシンポジウム, 2024.

Sasaki et al.のアイディア

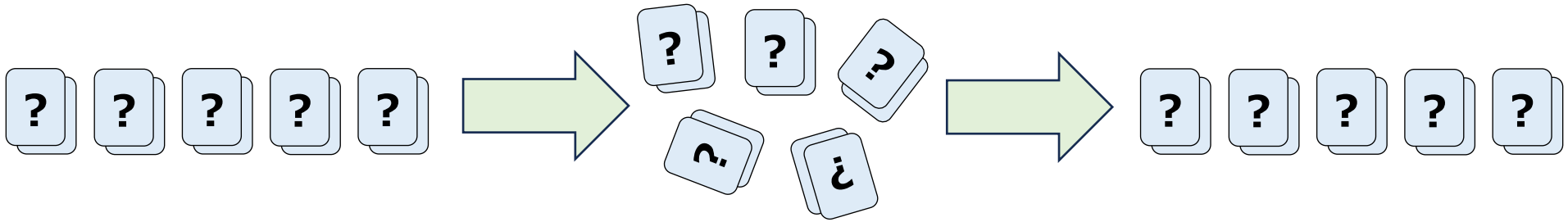
- 1枚ずつカードを置き、それをコピーして増やす



- このアイディアにより健全性エラーをゼロにできる

パイルスクランブルシャッフル[Ishikawa-Chida-Mizuki, UCNC 2015]

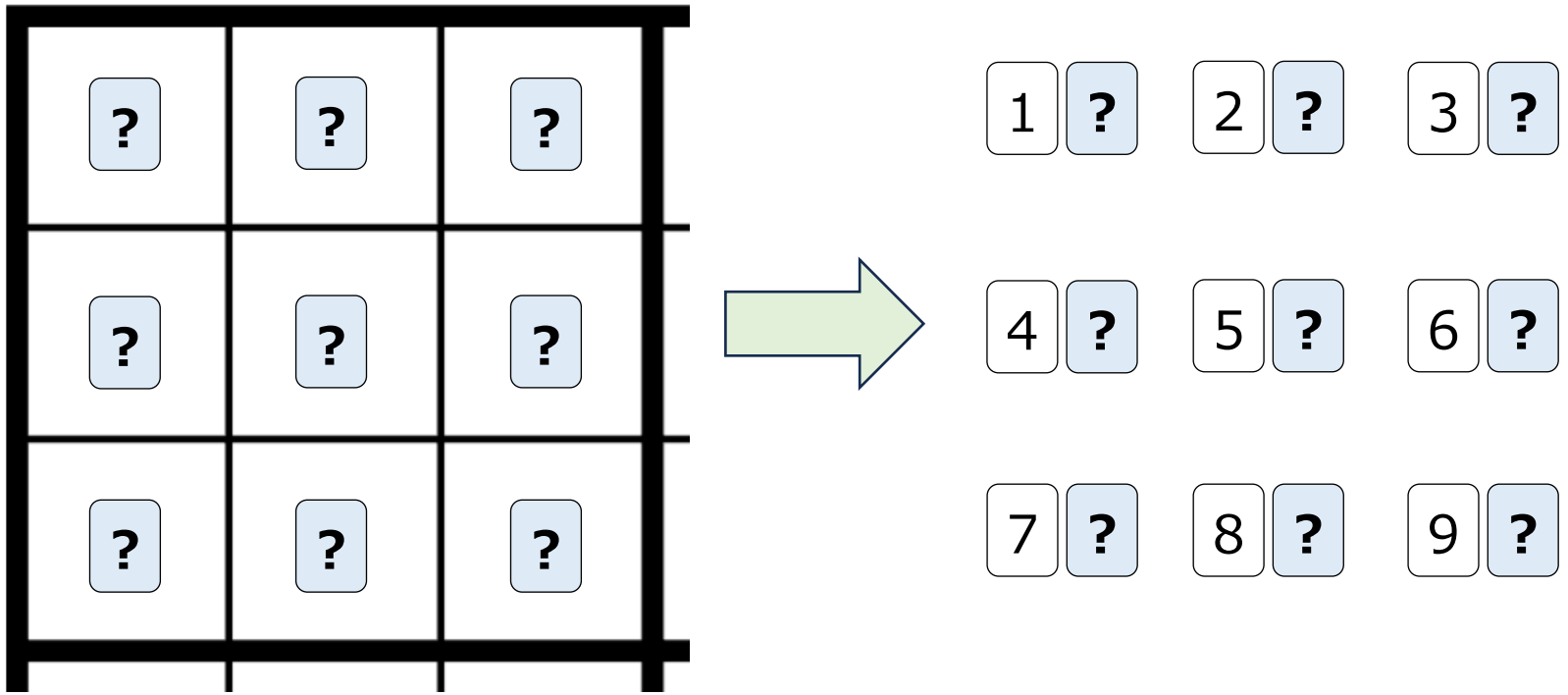
- カード束を一様ランダムに並べ替えるシャッフル
  - 各束のカード枚数は揃っていなければならない



- スリーブやバンドを用いれば簡単に実行できる

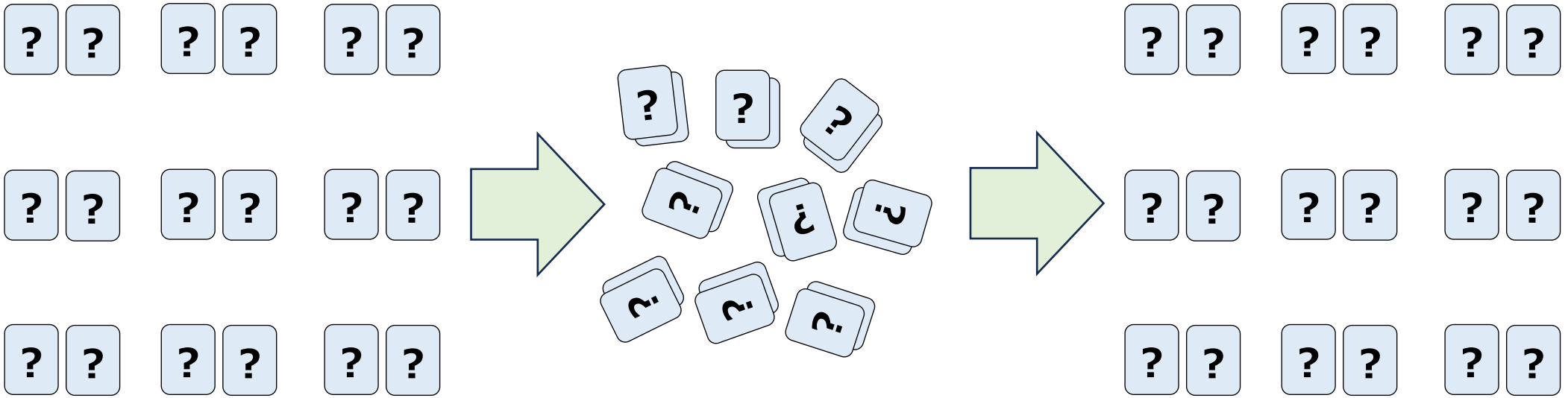
Sasaki et al.のコピープロトコル

1. コピーしたい9枚を取り出し、左隣に数字カードを順番に置く
   - この数字カードは順番を復元するためのもの



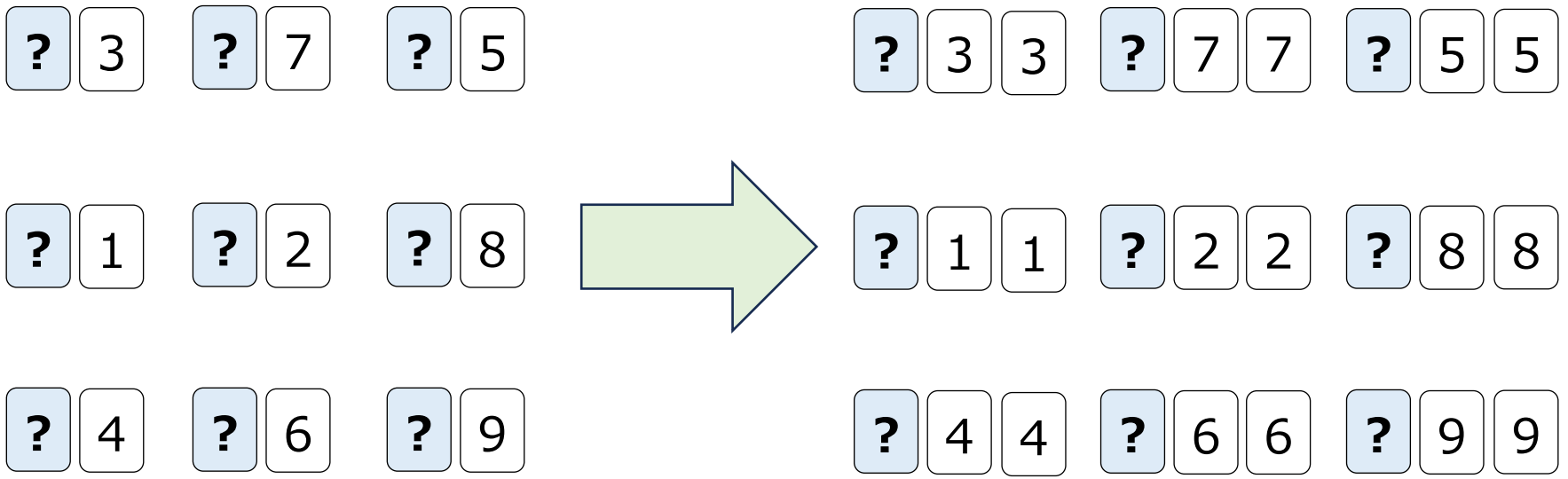
Sasaki et al.のコピープロトコル

2. すべてのカードを裏にし、各2枚を束としてパイルスクランブルシャッフルを実行する



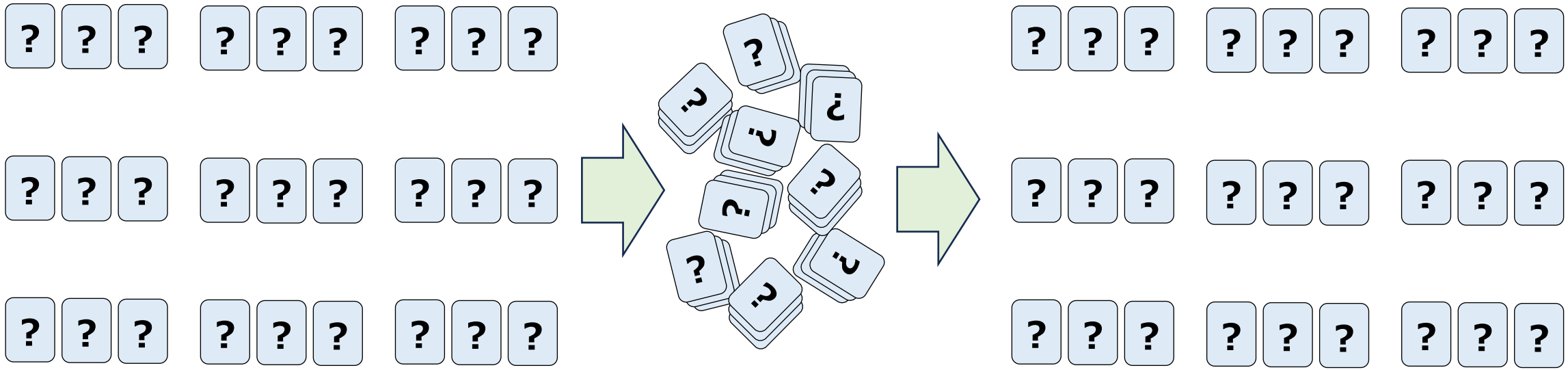
Sasaki et al.のコピープロトコル

3. 各束の右側をめくり、それと同じ数字のカードを右隣に置く



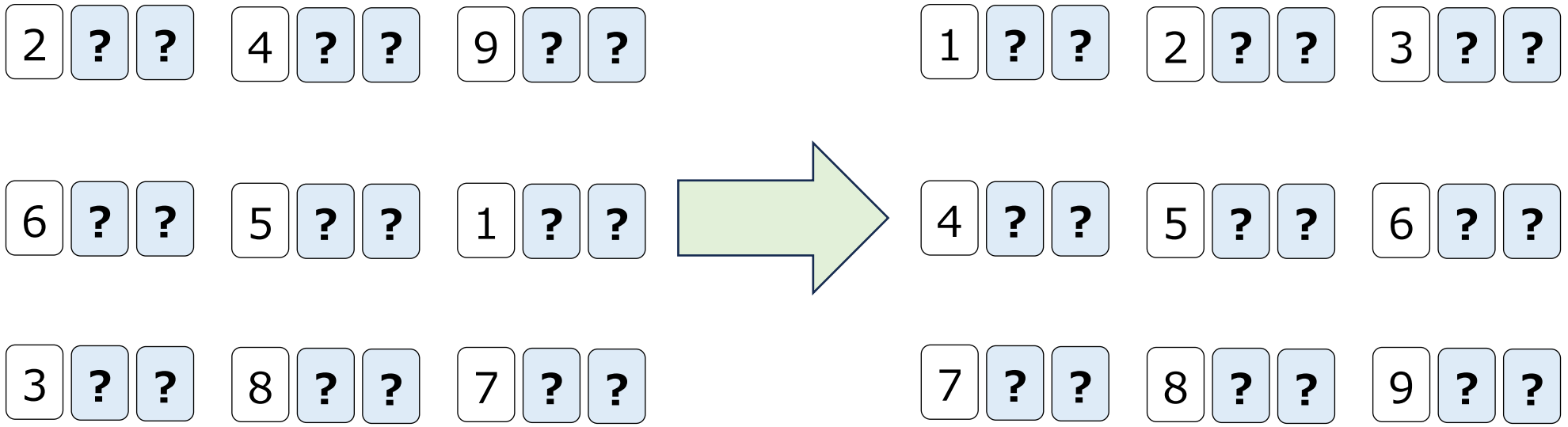
Sasaki et al.のコピープロトコル

4. すべてのカードを裏にし、各3枚を束としてパイルスクランブルシャッフルを実行する



Sasaki et al.のコピープロトコル

5. 各束の左側をめくり、その数字の順番通りに並べる



数独のゼロ知識証明プロトコル（※interactiveなプロトコルは除く）

	カード枚数	シャッフル回数	シャッフルの種類
Gradwohl et al. [GNPR07]	$3n^2$	$3n\ell$ (ℓ:繰返し回数)	Complete
Sasaki et al. [SMMS20]	n^2+n	$5n$	PScramble
Sasaki et al. [SMMS20]	$2n^2+n$	$4n$	PScramble
Tanaka-Mizuki [TM23]	$n^2+n(\sqrt{n}+1)$	$7\sqrt{n}-5$	PScramble
佐々木-品川 [SS23]	$4n^2$	3	PScramble
田中-水木 [TM24]	$4n^2$	2	PScramble

[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[TM23] K, Tanaka and T. Mizuki, Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku, FCT 2023.
[SS23] 佐々木, 品川, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム, 2023.
[TM24] 田中, 水木, 2回あるいは1回のシャッフルを用いた数独に対する物理的ゼロ知識証明, 暗号と情報セキュリティシンポジウム, 2024.

Tanaka-Mizukiのアイディア (1/4)

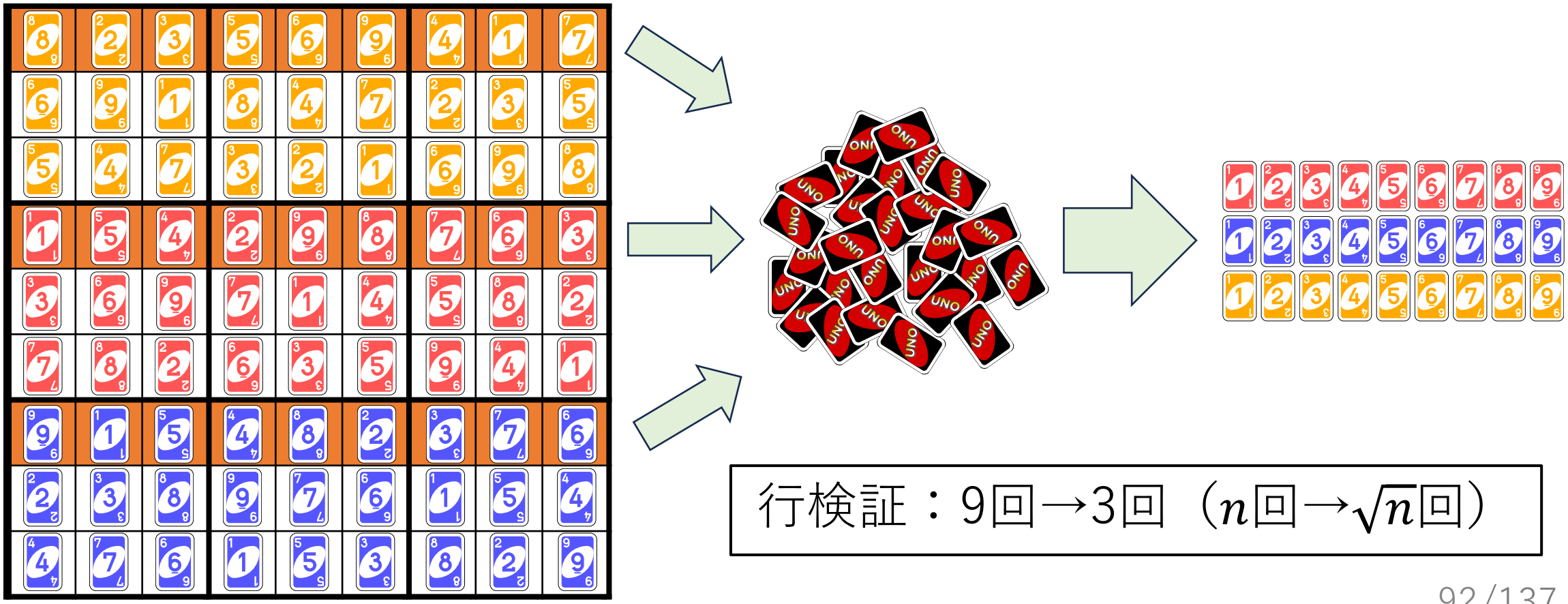
- UNOデッキを用いる

Tanaka-Mizukiのアイディア (2/4)

- アリスは答えに対応するカードを以下のように三色で配置する

Tanaka-Mizukiのアイディア (3/4)

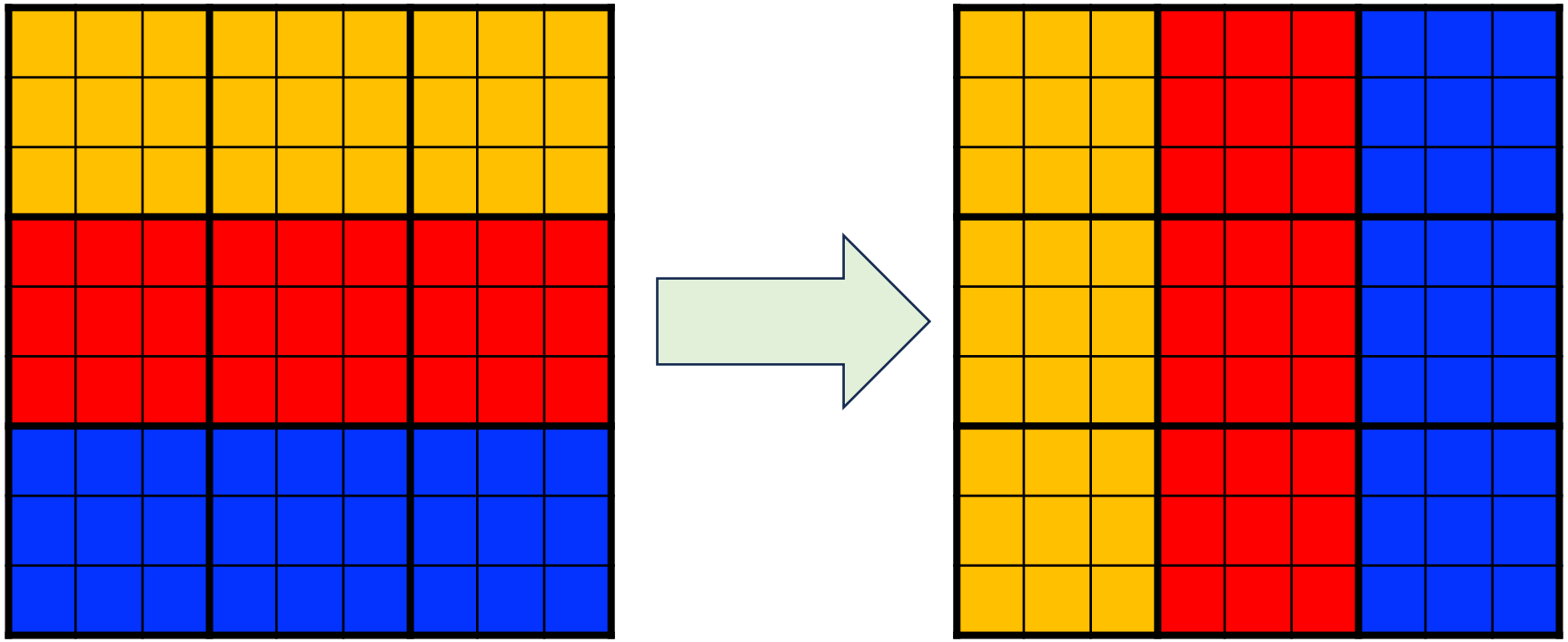
- 1行目と4行目と7行目の検証を同時に行う



行検証：9回→3回（n回→$\sqrt{n}$回）

Tanaka-Mizukiのアイディア (4/4)

- 色変更プロトコル（詳細略）



- このプロトコルの実行時に(自動的に)ブロック検証も行われる

Tanaka-Mizukiのプロトコルの効率性

- 以下の回数のパイルスクランブルシャッフルを用いる

- 初期の配色の検証：$2\sqrt{n}$回
- 行検証プロトコル：$2\sqrt{n}-2$回
- 色変更プロトコル：$2\sqrt{n}-2$回
- 列検証プロトコル：$\sqrt{n}-1$回

- 合計$7\sqrt{n}-5$回

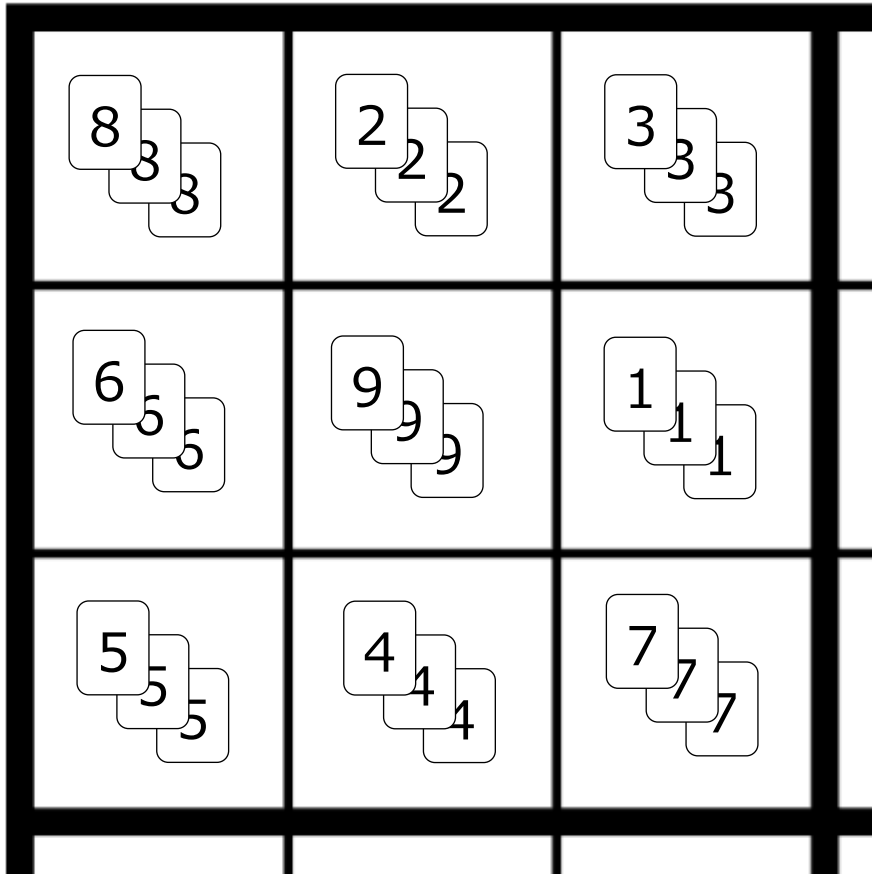
数独のゼロ知識証明プロトコル（※interactiveなプロトコルは除く）

	カード枚数	シャッフル回数	シャッフルの種類
Gradwohl et al. [GNPR07]	$3n^2$	$3n\ell$ (ℓ:繰返し回数)	Complete
Sasaki et al. [SMMS20]	n^2+n	$5n$	PScramble
Sasaki et al. [SMMS20]	$2n^2+n$	$4n$	PScramble
Tanaka-Mizuki [TM23]	$n^2+n(\sqrt{n}+1)$	$7\sqrt{n}-5$	PScramble
佐々木-品川 [SS23]	$4n^2$	3	PScramble
田中-水木 [TM24]	$4n^2$	2	PScramble

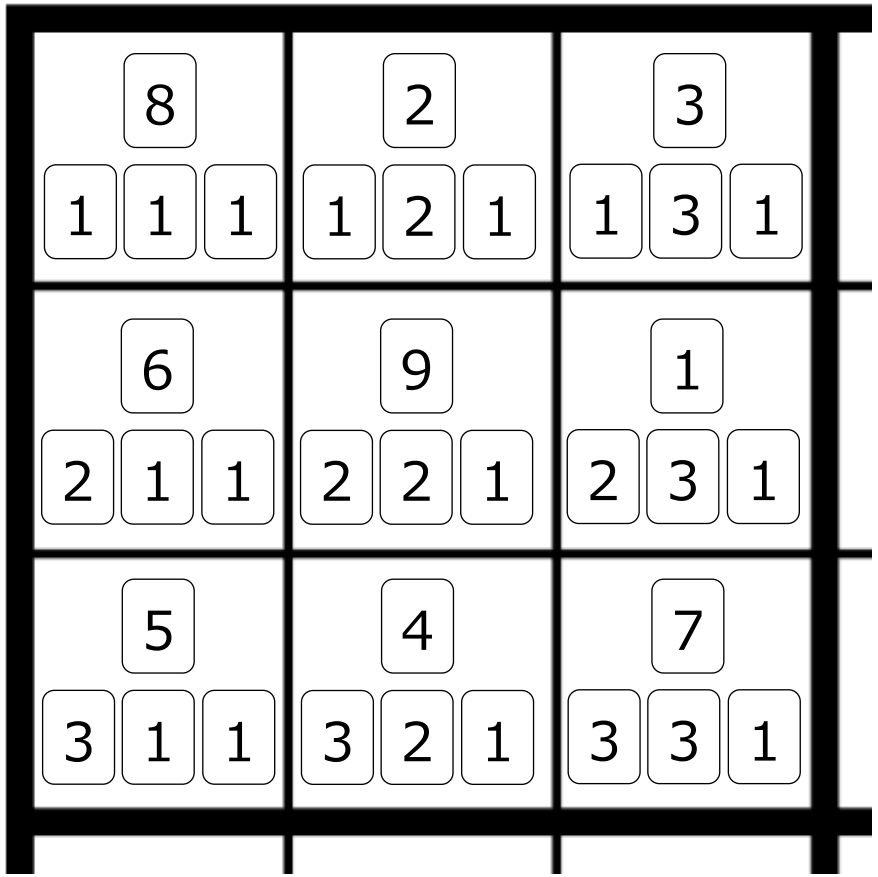
[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[TM23] K, Tanaka and T. Mizuki, Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku, FCT 2023.
[SS23] 佐々木, 品川, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム，2023.
[TM24] 田中, 水木, 2回あるいは1回のシャッフルを用いた数独に対する物理的ゼロ知識証明, 暗号と情報セキュリティシンポジウム, 2024.

佐々木-品川のアイディア

従来：**解答そのもの**を扱う

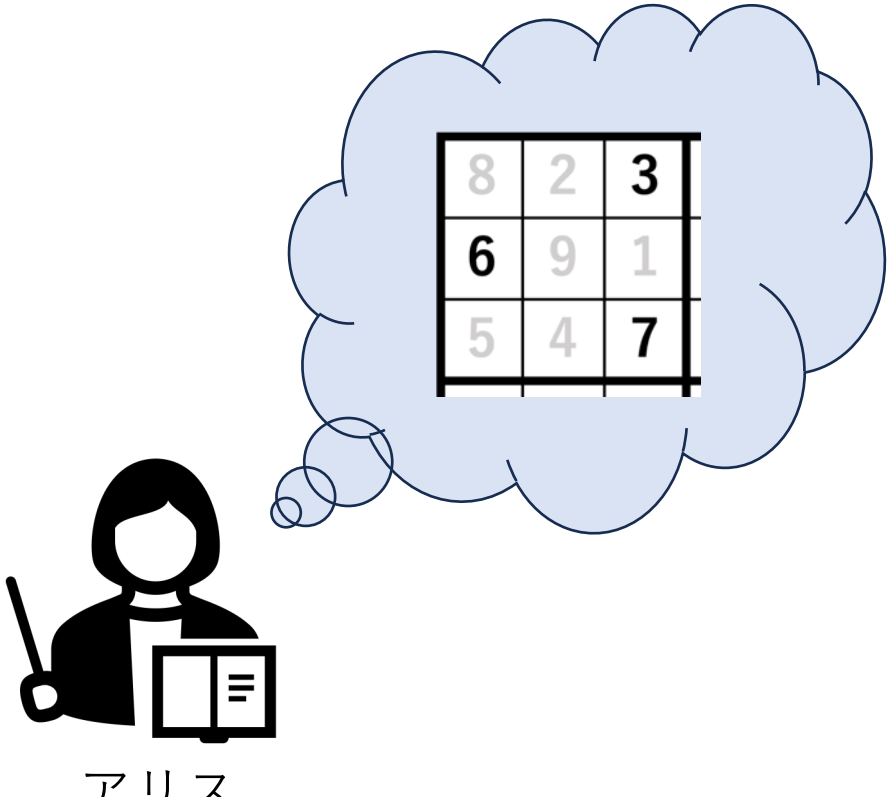


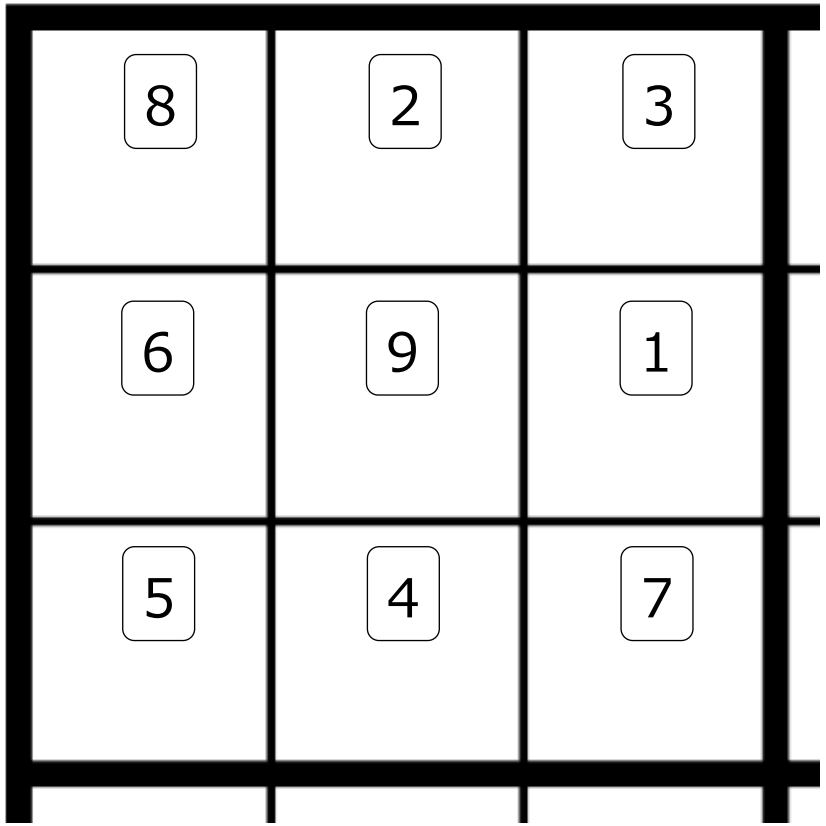
今回：**マスの座標**を扱う



佐々木-品川のプロトコル

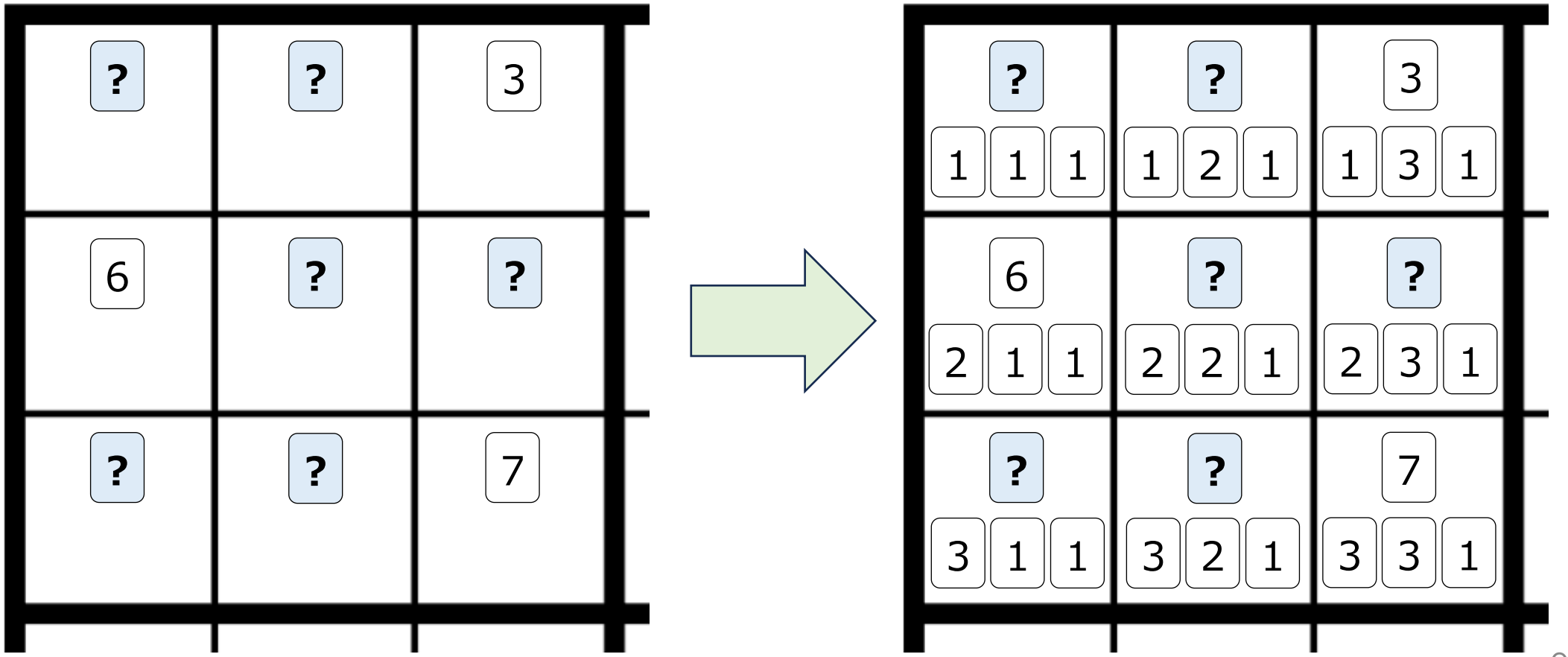
1. アリスは各マスに対応するカードを**1枚ずつ**裏向きに置く
   - ただし、最初から数字のあるマスは表向きに置く





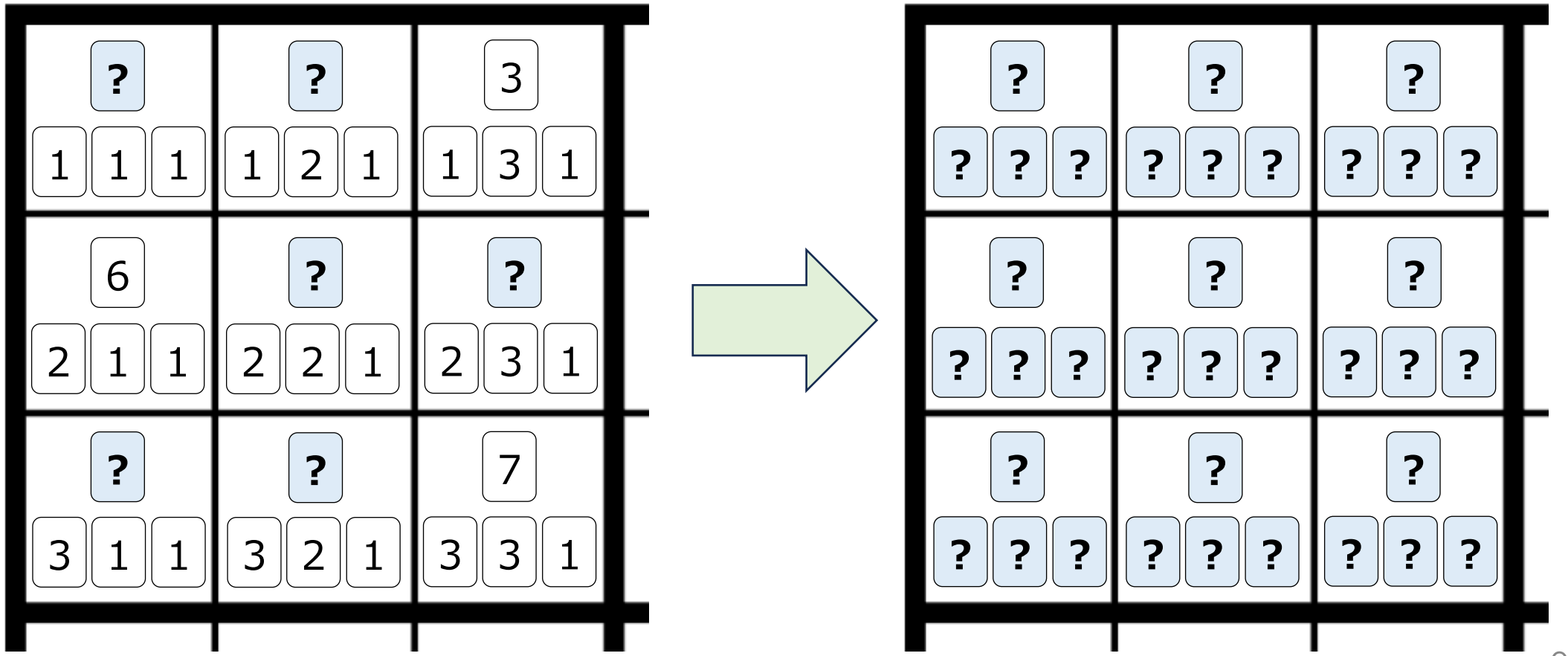
佐々木-品川のプロトコル

2. a行b列cブロックのマスに a b c を置く



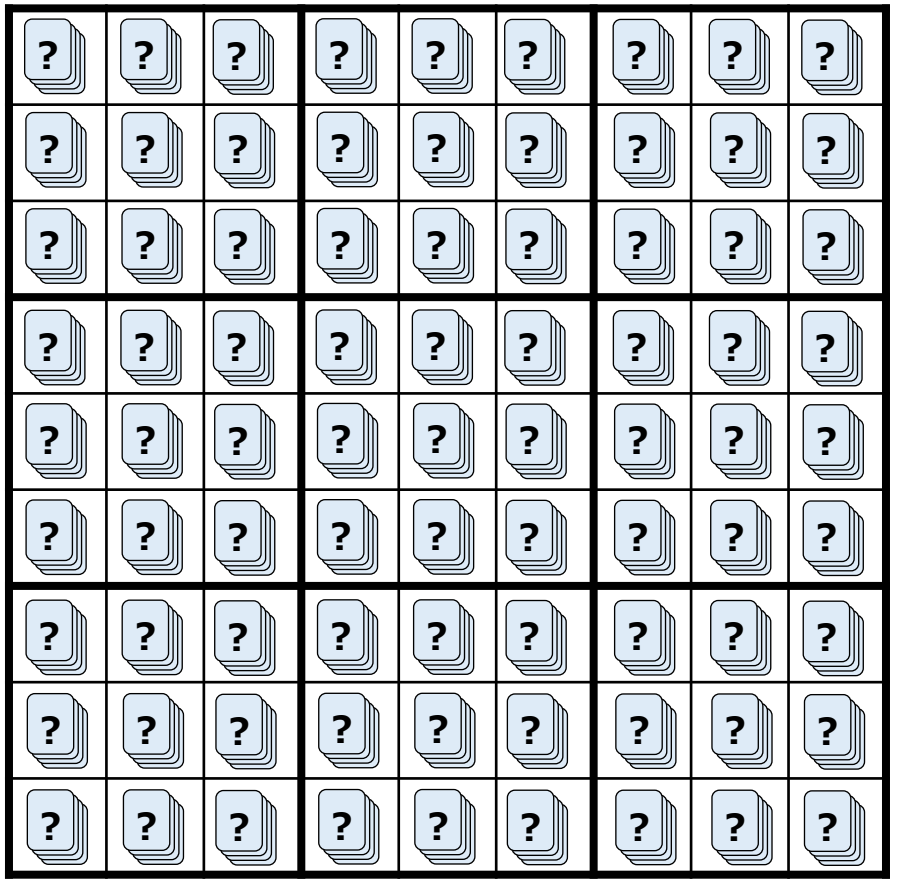
佐々木-品川のプロトコル

3. すべてのカードを裏にする



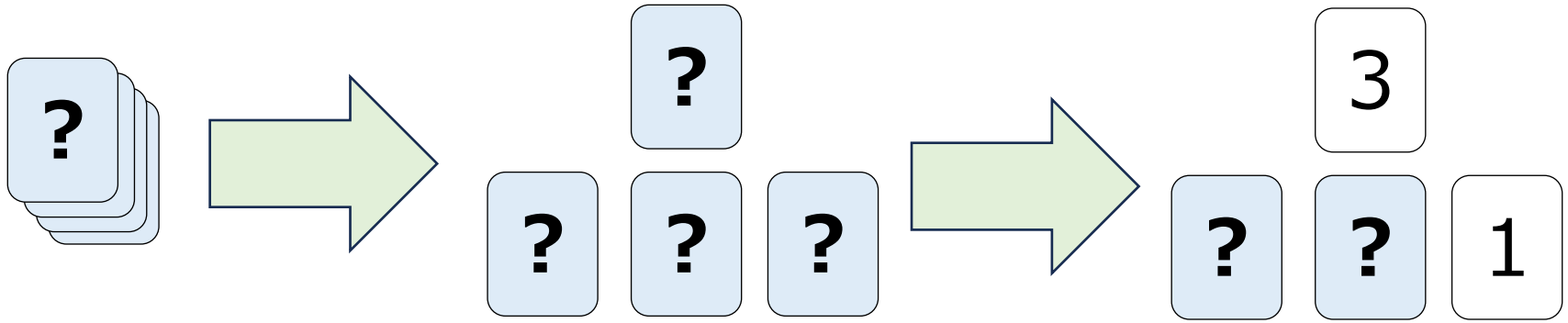
佐々木-品川のプロトコル

4. 81個のカード束にパイルスクランブルシャッフルを施す



佐々木-品川のプロトコル

5. すべての束について、解とブロックを表すカードをめくる
   - 各ブロックについて、1〜9が揃っていることを確認する



6. 同様に行と列の検証を行う
   - 再びパイルスクランブルシャッフルし、解と行を表すカードをめくる

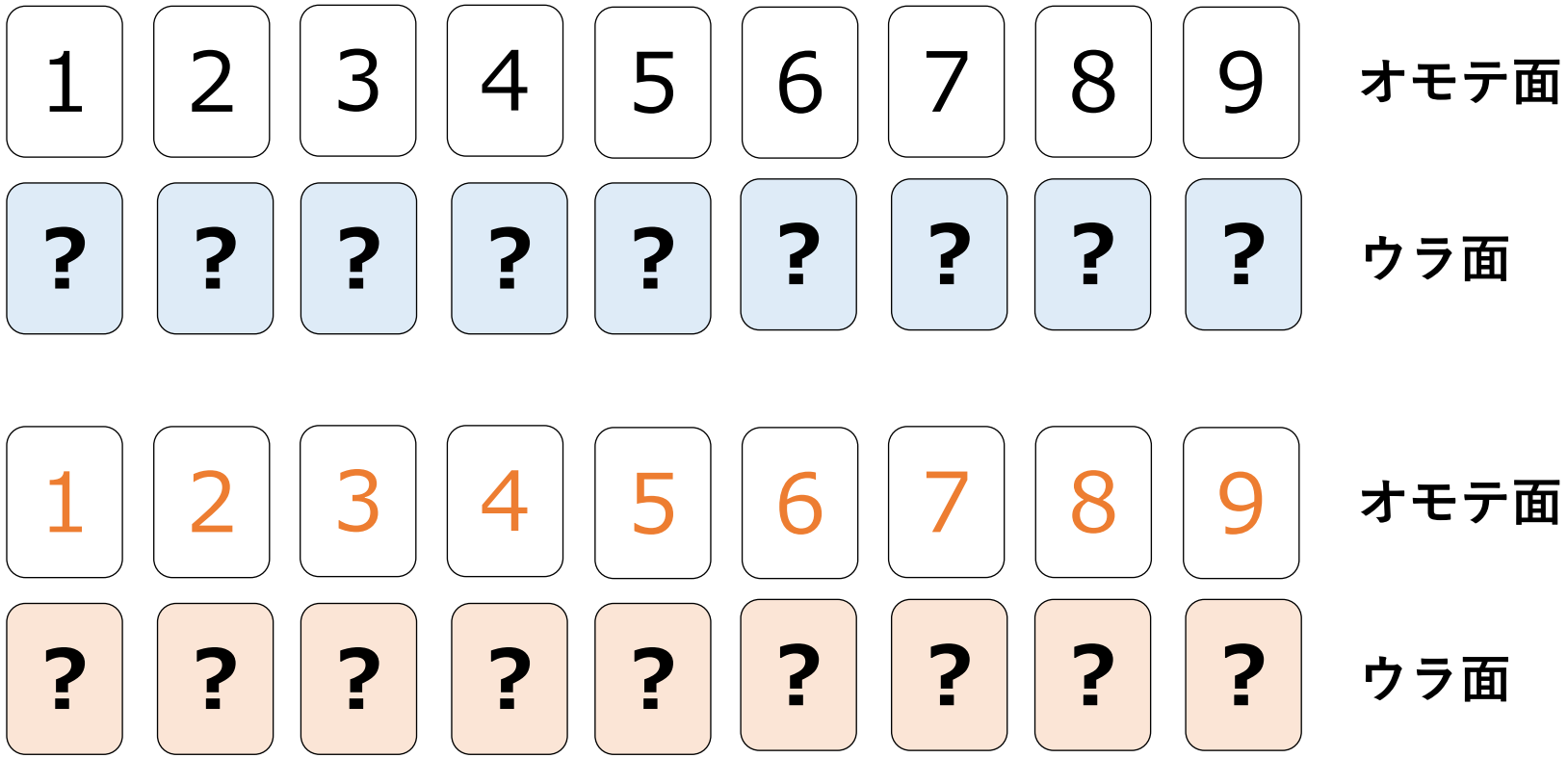
数独のゼロ知識証明プロトコル（※interactiveなプロトコルは除く）

	カード枚数	シャッフル回数	シャッフルの種類
Gradwohl et al. [GNPR07]	$3n^2$	$3n\ell$ (ℓ:繰返し回数)	Complete
Sasaki et al. [SMMS20]	n^2+n	$5n$	PScramble
Sasaki et al. [SMMS20]	$2n^2+n$	$4n$	PScramble
Tanaka-Mizuki [TM23]	$n^2+n(\sqrt{n}+1)$	$7\sqrt{n}-5$	PScramble
佐々木-品川 [SS23]	$4n^2$	3	PScramble
田中-水木 [TM24]	$4n^2$	2	PScramble

[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[TM23] K, Tanaka and T. Mizuki, Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku, FCT 2023.
[SS23] 佐々木, 品川, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム，2023.
[TM24] 田中, 水木, 2回あるいは1回のシャッフルを用いた数独に対する物理的ゼロ知識証明, 暗号と情報セキュリティシンポジウム, 2024.

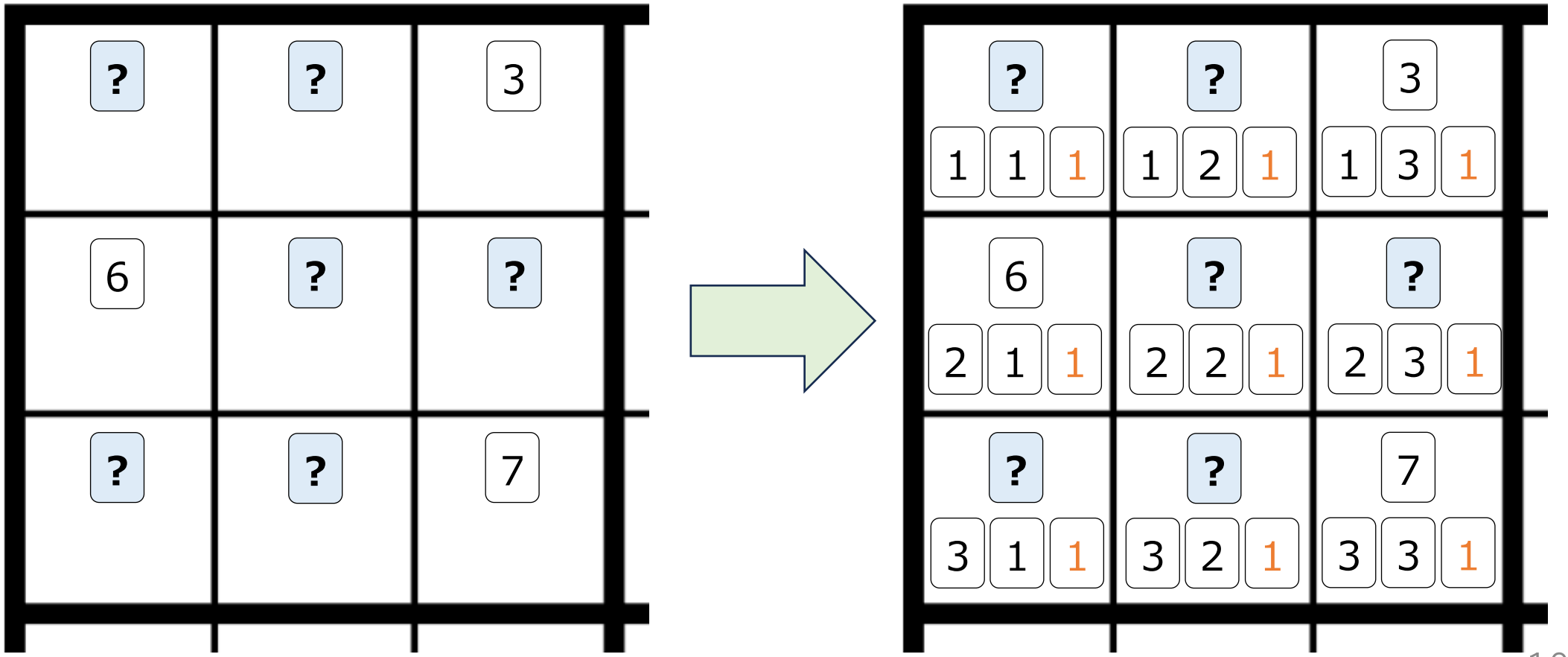
田中-水木のアイディア(1/4)

- 2種類の数字カードを用いる



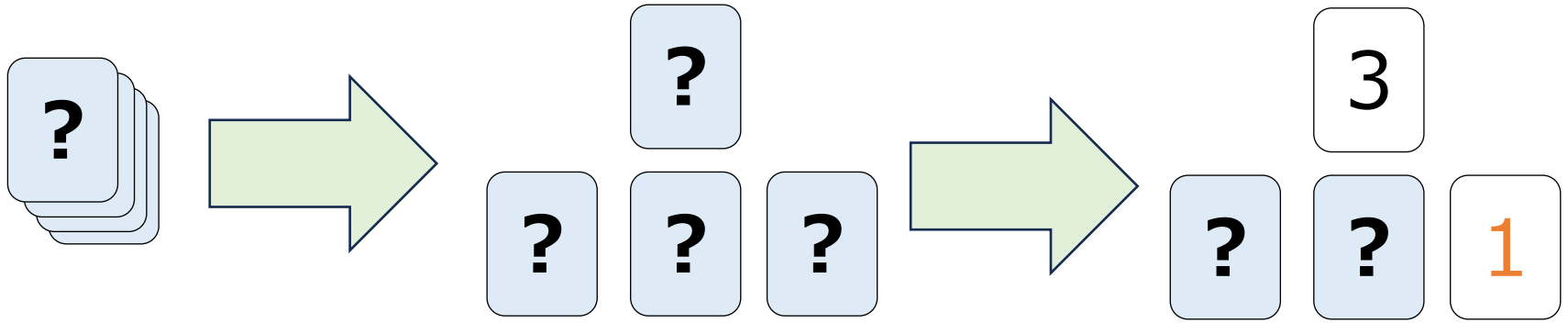
田中-水木のアイディア(2/4)

- ブロック座標のカードだけ赤カードを置く

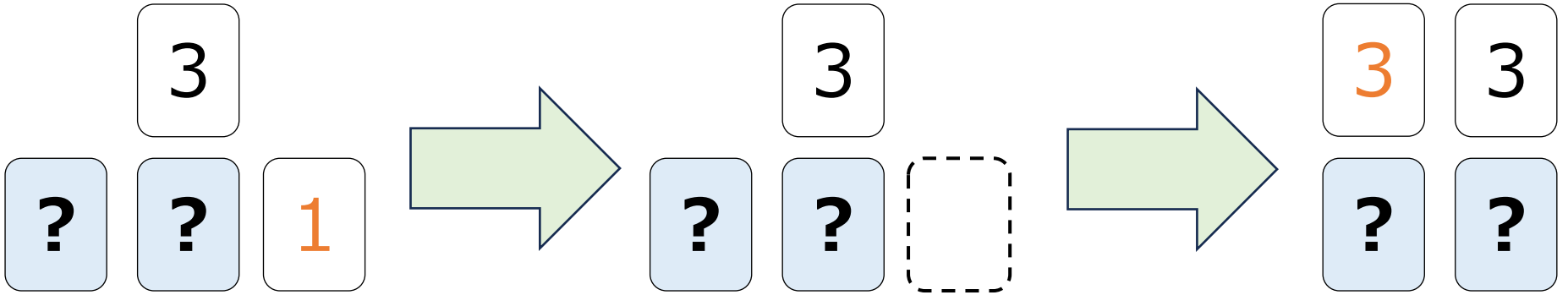


田中-水木のアイディア(3/4)

- 佐々木-品川と同様にブロック検証を行う(1回のPScramble)

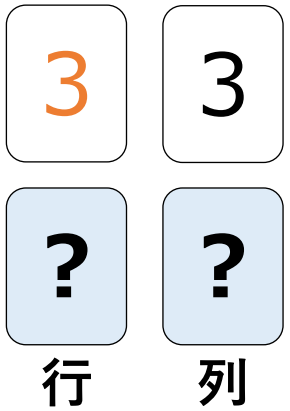


- ブロック検証後、解カードと同じ数字の赤カードを上に置く



田中-水木のアイディア(4/4)

- 行座標の上に赤カードが、列座標の上に黒カードが置かれている



- 縦の2枚を束とし、81×2個の束にパイルスクランブルシャッフル

- 行検証と列検証を1回のパイルスクランブルシャッフルで実行可能

未解決問題

- 数独プロトコルの問題設定
  - 初期カード列は各マスに数字カード1枚ずつ
  - Practicalなシャッフル（対称系または巡回系）のみに限定する
    - 対称系：完全シャッフル/パイルスクランブルシャッフル
    - 巡回系：ランダムカット/ランダム二等分割カット/パイルシフティングシャッフル

- 田中-水木のシャッフル2回が現在までのところ最小

- **シャッフル1回のプロトコルは構成できるか？**

- **シャッフル定数回のままカード枚数を削減できるか？**

さらなる展開：対話的なプロトコル

- 証明者と検証者の間で対話的な操作を用いる設定も研究されている
- **対話的入力**：検証者がカードを確認してから、証明者が配置する

	カード枚数	シャッフル回数	対話的入力	対話的操作
Sasaki et al. [SMMS20]	n^2	$3n+1$	✓	
Ruangwises [Rua21]	$n^2+n(\sqrt{n}+1)+\sqrt{n}$	$4\sqrt{n}$		✓
Ruangwises [Rua21]	$n^2+2n+3\sqrt{n}$	$2n^2(\sqrt{n}-1)+2$		✓
Ono et al. [ORAHI24]	$2n^2$	1	✓	

[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[Rua21] S. Ruangwises, Two Standard Decks of Playing Cards Are Sufficient for a ZKP for Sudoku, COCOON 2021.
[ORAHI24] T. Ono, S. Ruangwises, Y. Abe, K. Hatsugai, and M. Iwamoto, Single-Shuffle Physical Zero-Knowledge Proof for Sudoku Using Interactive Inputs, ISEC研究会, 2024.

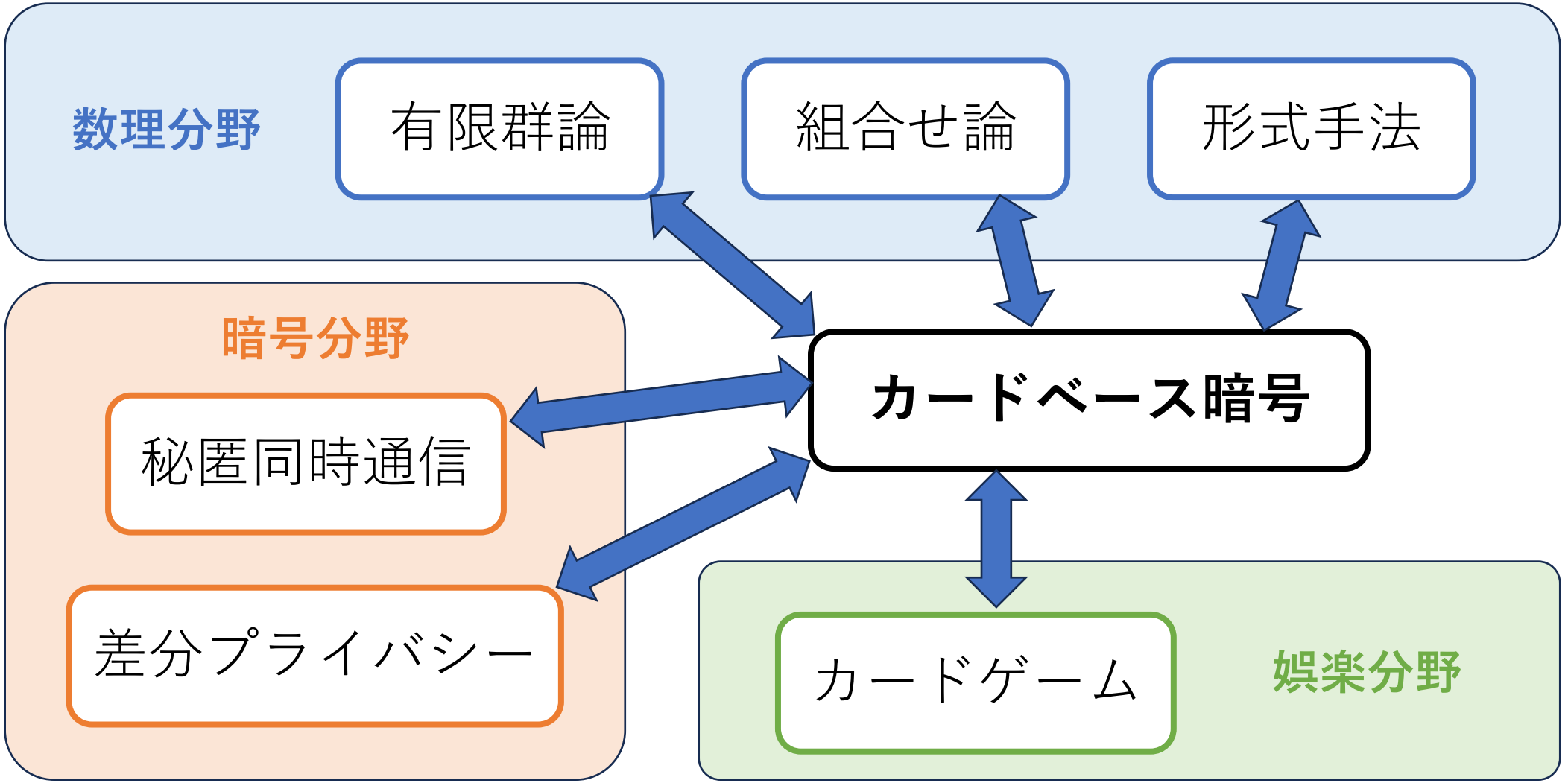
第３部のまとめ

- 数独プロトコルの発展の歴史を眺めた
  - Gradwohl et al.のプロトコル
  - Sasaki et al.の健全性エラーのないプロトコル
  - Tanaka-Mizukiのシャッフル回数の少ないプロトコル
  - 佐々木-品川のシャッフル3回のプロトコル
  - 田中-水木のシャッフル2回のプロトコル
  - 対話的入力/対話的操作を用いたプロトコルたち

- 未解決問題
  - **シャッフル1回のプロトコルは構成できるか？**
  - **シャッフル定数回のままカード枚数を削減できるか？**

第４部
他分野との連携

カードベース暗号と他分野との融合領域



目次

- 数理分野
  - 有限群論
  - 組合せ論
  - 形式手法
- 暗号分野
  - 秘匿同時通信プロトコル
  - 差分プライバシー
- 娯楽分野
  - ババ抜きへの応用
  - ガムロ：新しいカードゲーム

有限群論とシャッフル(1/3)

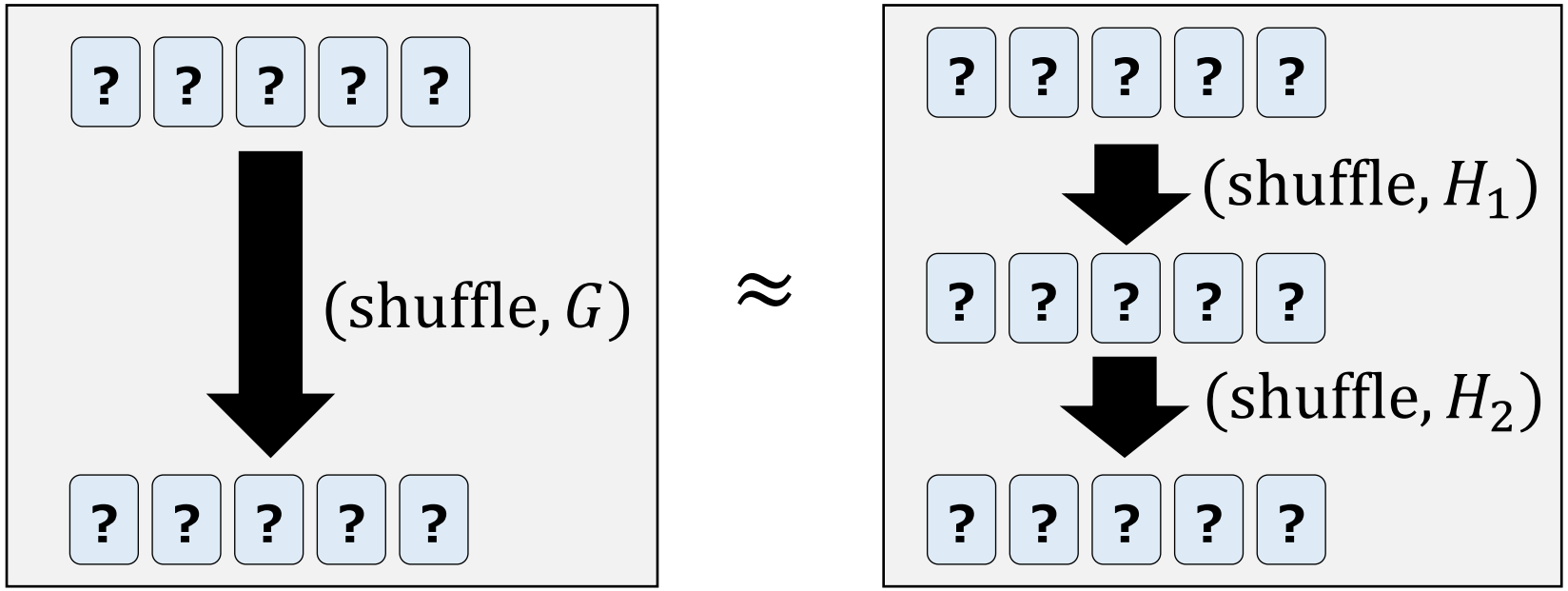
- Gの**部分群**の列$\vec{H} = (H_1, H_2, \ldots, H_k)$が$G$の**一様群分解**であるとは、多重集合$\mathrm{mult}_{\vec{H}} \coloneqq \{h_1 h_2 \cdots h_k \mid h_i \in H_i\}$が以下を満たすこと：
  - $\mathrm{mult}_{\vec{H}}$にGの各元が同じ個数ずつ現れること（重複度一定）

- H_iたちが**巡回群**のとき**一様巡回群分解 (UCF)**という

K. Kanai, K. Miyamoto, K. Nuida, and K. Shinagawa, Uniform cyclic group factorizations of finite groups, Commun. Algebra., 2024.

有限群論とシャッフル(2/3)

- (H_1, H_2)をGのUCFとする
- このとき、$(\mathrm{shuffle}, G)$は$(\mathrm{shuffle}, H_1), (\mathrm{shuffle}, H_2)$に分解できる



- **GがUCFを持つと、$(\mathrm{shuffle}, G)$を簡単な操作列に分解できる**

有限群論とシャッフル(3/3)

- 現状わかっていること[Kanai-Miyamoto-Nuida-Shinagawa, Commun. Algebra. 24]
  - 任意の可解群は一様群分解を持つ
  - もし任意の単純群が一様群分解を持てば、任意の群はUCFを持つ

- **未解決問題：任意の群はUCFを持つか？**

K. Kanai, K. Miyamoto, K. Nuida, and K. Shinagawa, Uniform cyclic group factorizations of finite groups, Commun. Algebra., 2024.

語の組合せ論とカードベース暗号[品川-縫田, SCIS24]

- プロトコル構成を**語の組合せ論**的な問題として捉える
  - 複数個のビット列が巡回的に等しくなるのはいつか？

Five-Card Trickの真理値表

a	b	$\bar{a}$	a	1	b	$\bar{b}$
0	0	1	0	1	0	1
0	1	1	0	1	1	0
1	0	0	1	1	0	1
1	1	0	1	1	1	0

巡回的に等しい

- 定理：ハミング重みの等しい2個のビット列は巡回的に等しくできる

品川 和雅, 縫田 光司, カードベース暗号に現れる語の組合せ論, 暗号と情報セキュリティシンポジウム (SCIS2024), 2024.

代数的組合せ論とカードベース暗号[須賀の一連の研究]

- プロトコルとアソシエーションスキームとの関係に着目
  - アソシエーションスキーム
  - Johnsonスキーム
  - Difference set

- 研究の方向性：カードベースプロトコルで表現可能な代数構造は？

（文献情報の一部）
須賀 祐治, JからHを見つけることによる3×3タイプのマッチングを可能とするカードプロトコルの構成, コンピュータセキュリティシンポジウム, 2023.
須賀 祐治, 2頂点の距離に基づく非コミットメント型カードプロトコルの新しい系列とDifference setを用いた開示フェーズの効率化, 暗号と情報セキュリティシンポジウム, 2024.

形式手法と不可能性証明[Koch-Schrempp-Kirsten, Asiacrypt19]

- SBMC (Software Bounded Model Checking)の利用
- プロトコルの網羅的探索を行う
- 「kステップ以内では計算不可能」などを証明可能
- シャッフル回数の最小化の研究に役立つことが期待されている

A. Koch, M. Schrempp, M. Kirsten, Card-Based Cryptography Meets Formal Verification, Asiacrypt 2019.

目次

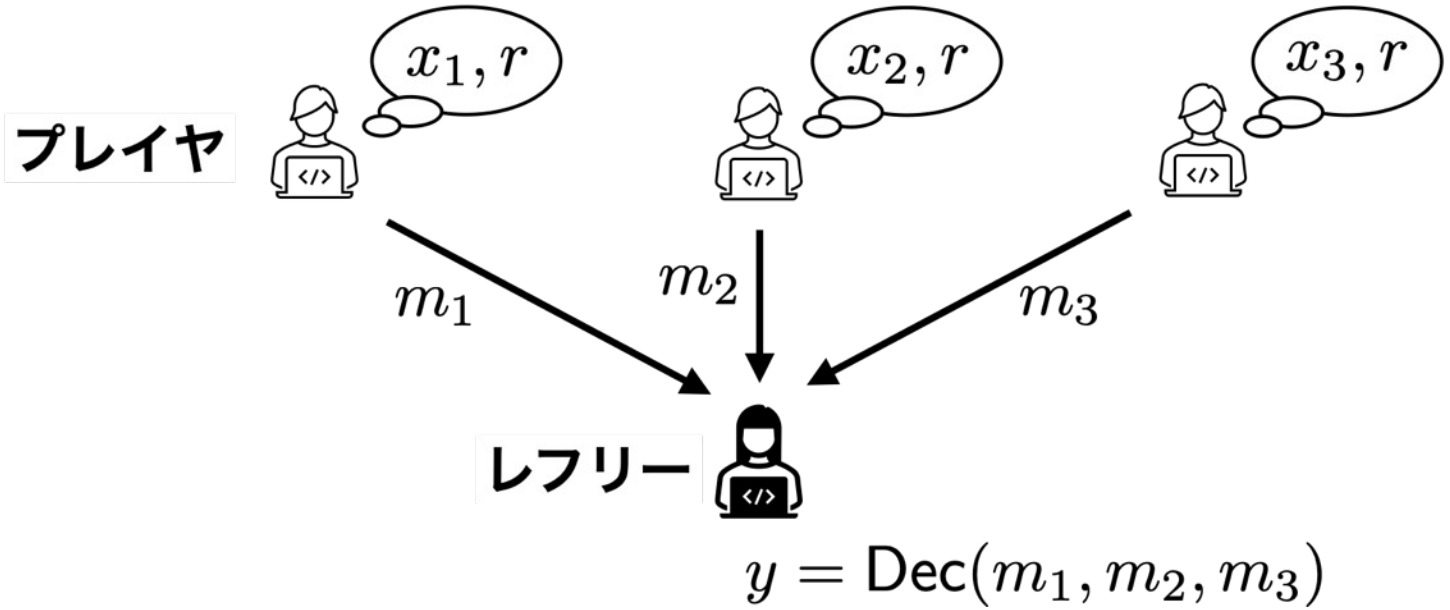
- 数理分野
  - 有限群論
  - 組合せ論
  - 形式手法

- **暗号分野**
  - **秘匿同時通信プロトコル**
  - **差分プライバシー**

- 娯楽分野
  - ババ抜きへの応用
  - ガムロ：新しいカードゲーム

秘匿同時通信プロトコルへの変換[品川-縫田, SCIS23]

- **秘匿同時通信(PSM)プロトコル**（非物理的な暗号プロトコル）



- 有限時間カードプロトコルからPSMプロトコルへの一般変換

品川 和雅, 縫田 光司,有限時間カードベースプロトコルから秘匿同時通信プロトコルへの一般的変換, 暗号と情報セキュリティシンポジウム, 2023.

カード差分プライバシー[Eriguchi-Shinagawa-Murakami, FUN24]

- 秘密計算は出力結果から漏れる情報は「自明な情報」として扱う

- **差分プライバシー**（出力結果から情報を隠す技術）
  - 関数$f(\boldsymbol{x})$を出力する代わりに$y(\boldsymbol{x}) = f(\boldsymbol{x}) + \mathrm{noise}$を出力し、情報を隠す
  - 一般にプライバシーと有用性の間にトレードオフがある

- 差分プライバシーをカードベース暗号で初めて表現

R. Eriguchi, K. Shinagawa, T. Murakami, Card-based Cryptography Meets Differential Privacy, FUN 2024.

目次

- 数理分野
  - 有限群論
  - 組合せ論
  - 形式手法

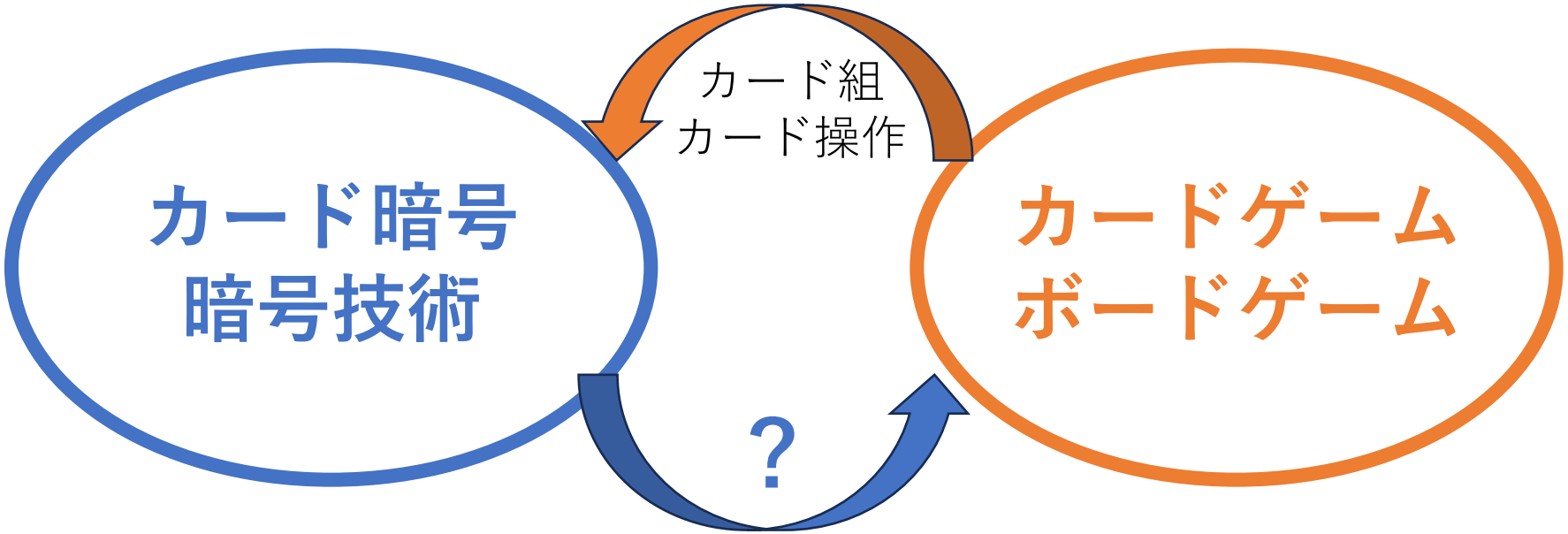
- 暗号分野
  - 秘匿同時通信プロトコル
  - 差分プライバシー

- **娯楽分野**
  - **ババ抜きへの応用**
  - **ガムロ：新しいカードゲーム**

カードゲームへの応用

- カードベース暗号は、まるでカードゲームを遊ぶかのように、暗号プロトコルを実演する技術（と解釈することもできる）

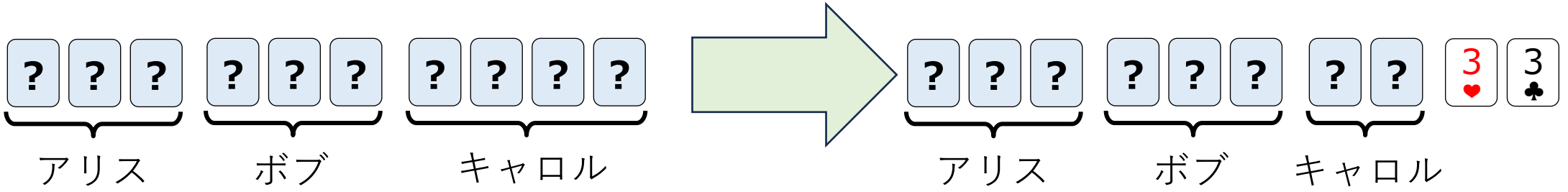
- 逆に、カードベース暗号をカードゲームに応用できないか？



ババ抜きへの応用[Shinagawa-Miyahara-Mizuki, IJTCS-FAW 2024]

- ババ抜きは二人だとゲームが単調になりがち
  - ジョーカーの位置が確定してしまう

- キャロル（三人目のプレイヤ）の手札整理プロトコル



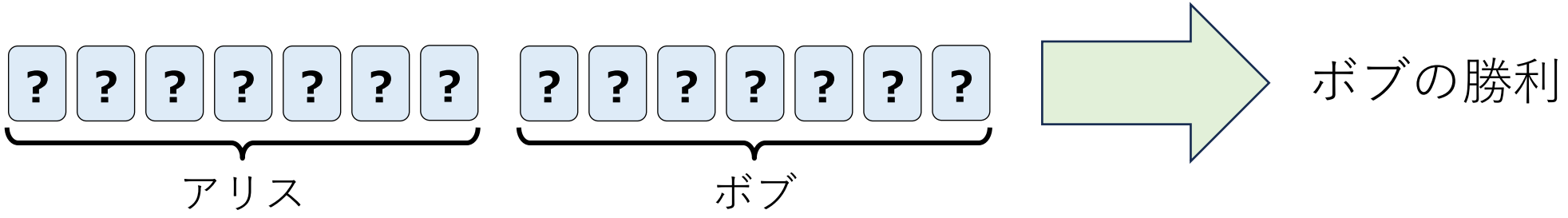
- **Future Work：他のゲームのプレイヤ模倣・ゲームマスター排除**

K. Shinagawa, D. Miyahara, and T. Mizuki, How to Play Old Maid with Virtual Players, IJTCS-FAW 2024.

新しいカードゲームの提案[葛馬ら, CSEC 2024]

- 2人対戦ゲーム『ガムロ』
  - プレイヤーは手札から1〜3枚のカードをディーラーに提出
  - ディーラーは合計値の大きいプレイヤーを勝者として告げる
  - 3ターンのうち2ターンを制した方が勝ち

- 大小比較プロトコルを用いてディーラー無しでプレイ



葛馬知紀, 平野智也, 大島莉凜, 安田百福, 水木敬明, ガムロ：新しいトランプゲームと秘密計算の応用, CSEC研究会, 2024.

第４部のまとめ

- カードベース暗号と諸分野との連携研究を眺めた
  - 数理分野：有限群論/組合せ論/形式手法
  - 暗号分野：PSM/差分プライバシー
  - 娯楽分野：ババ抜き/ガムロ

- 今後の研究の方向性
  - **他にどのような数学分野と関連しているか？**
  - **暗号技術の視覚化のさらなる展開**
  - **ゲームマスターの排除/新しいゲームの創出**

第５部
教育への応用

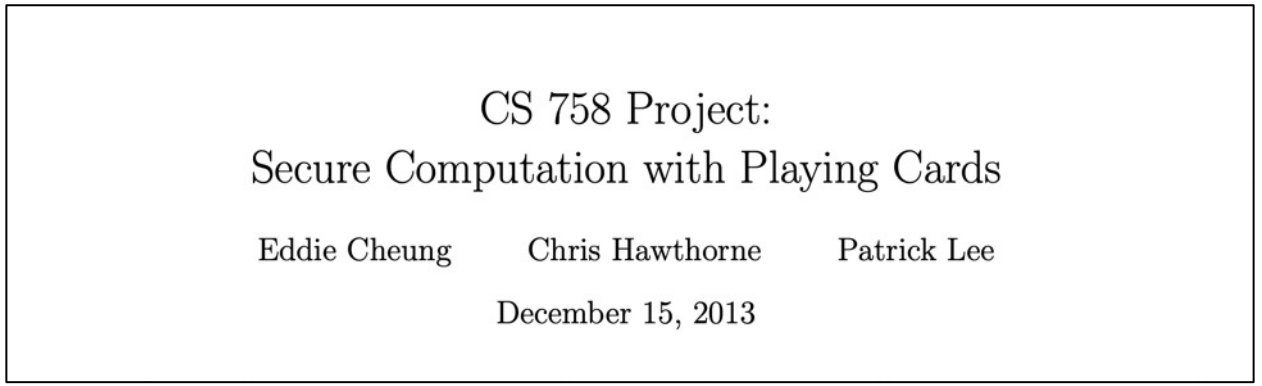
カードベース暗号の教育利用

- カードベース暗号の特徴
  - 実際に自分の手でプロトコルを実行できる
  - 視覚的に仕組みを分かりやすい

- **カードベース暗号をセキュリティ教育に利用できないか？**

実践例①：University of Waterloo, 2013

- CS 758: Cryptography / Network Security (Fall Semester, 2013)
- 講師：Douglas Stinson
- 受講生のCheung, Hawthorne, Leeは変則的なシャッフルを用いた1/2の確率で成功する5枚のコミット型ANDプロトコルを提案



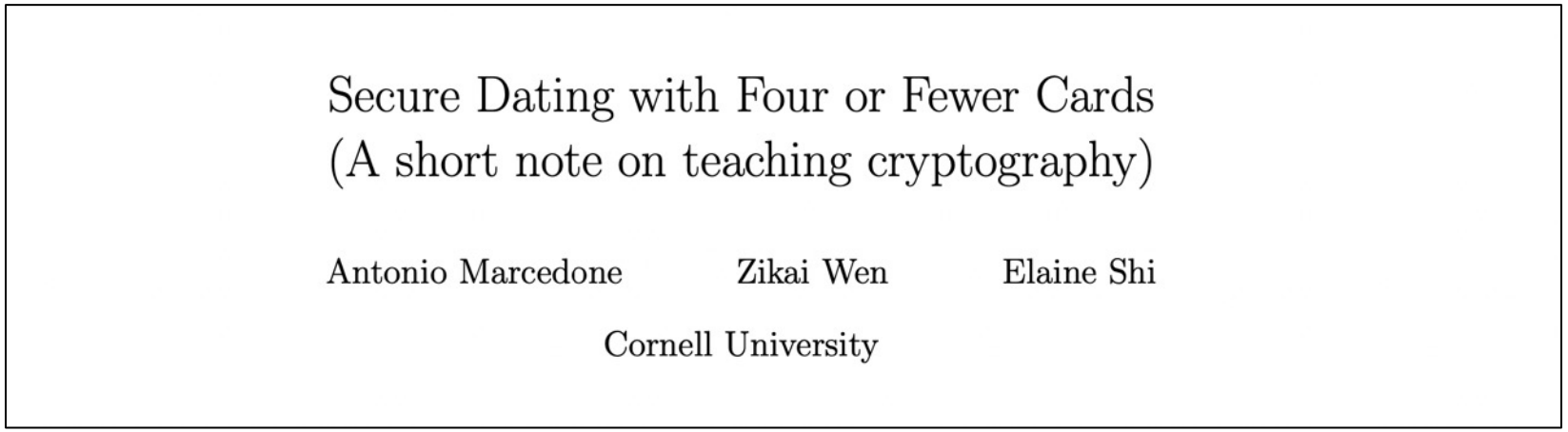
CS 758 Project:
Secure Computation with Playing Cards

Eddie Cheung Chris Hawthorne Patrick Lee

December 15, 2013

実践例②：Cornell University, 2015

- CS 4830: Introduction to Cryptography (Fall Semester, 2015)
- 講師：Elaine Shi
- 受講生が考案した種々のANDプロトコルが報告されている



Secure Dating with Four or Fewer Cards
(A short note on teaching cryptography)

Antonio Marcedone Zikai Wen Elaine Shi

Cornell University

実践例③：東北大学, 2016

- 基礎ゼミ「カード組を用いた暗号プロトコル」（2016年度前期）
- 講師：水木敬明
- Cornell大学のレポートを読み、グループに分かれて内容を議論

社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
TECHNICAL REPORT OF IEICE.

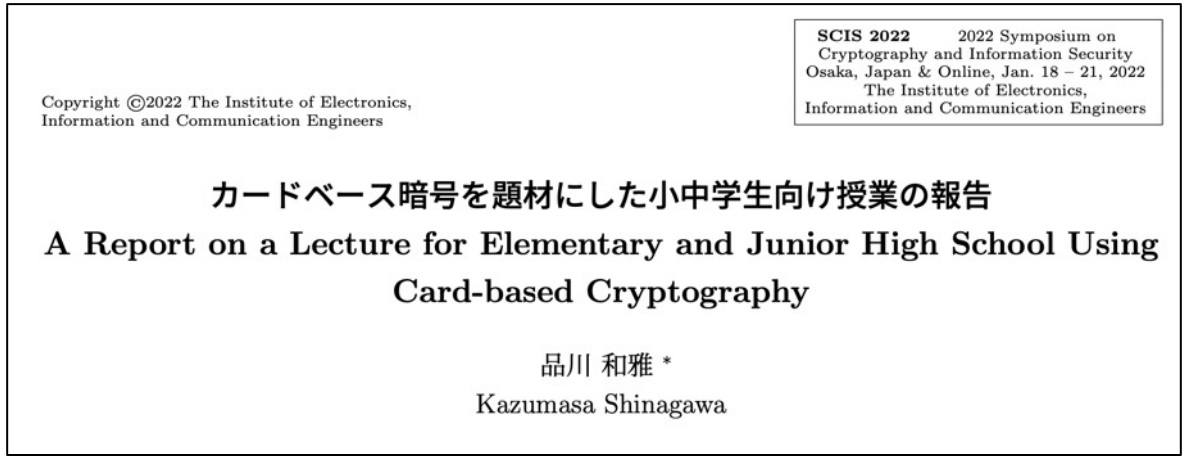
カードベース暗号の教育への応用

水木　敬明†

† 東北大学 サイバーサイエンスセンター
E-mail: †tm-paper+cardkiso@g-mail.tohoku-university.jp

実践例④：小学生・中学生向け授業, 2021

- 日立理科クラブ 茨城大学特別授業『カードで学ぶ秘密計算』
- 身近な問題設定から入り、秘密計算を体験する



SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

カードベース暗号を題材にした小中学生向け授業の報告

A Report on a Lecture for Elementary and Junior High School Using Card-based Cryptography

品川 和雅 *
Kazumasa Shinagawa

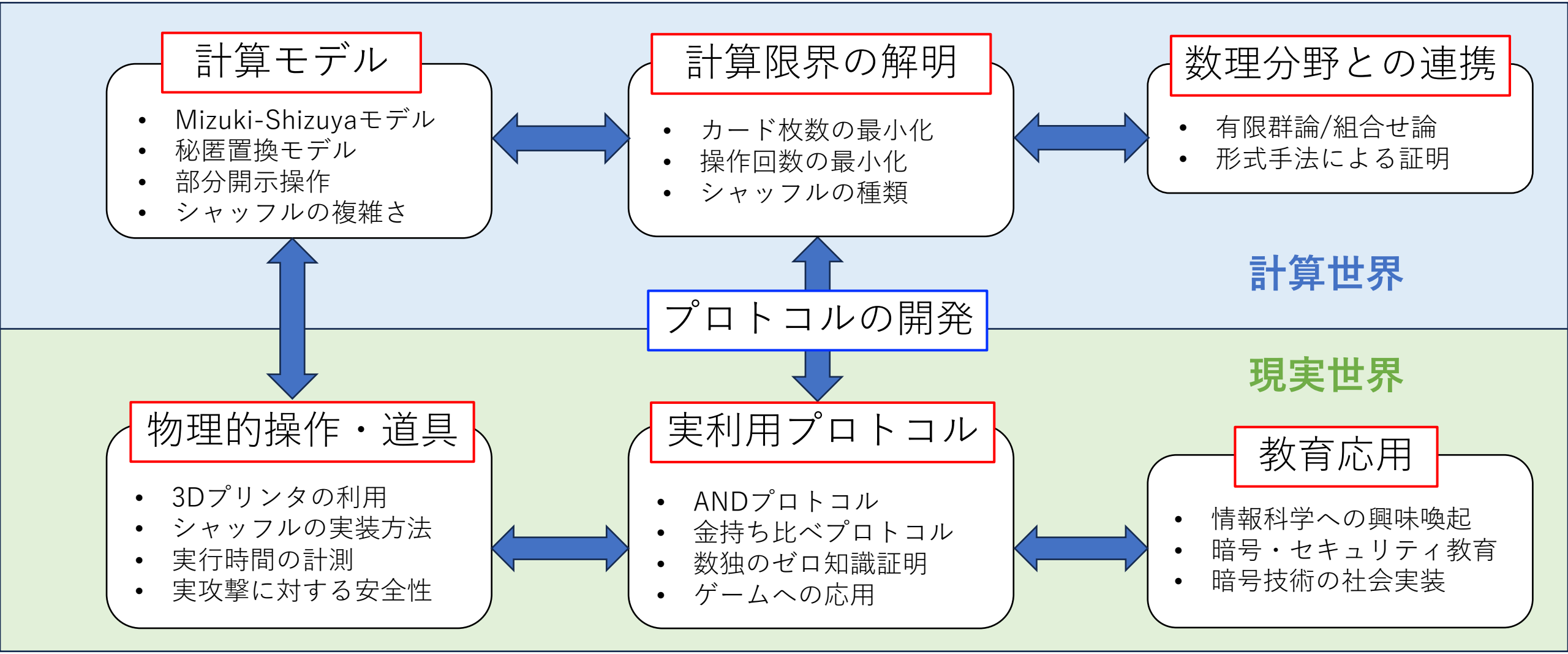
第５部のまとめ

- カードベース暗号の教育利用の事例紹介
  - University of Waterloo
  - Cornell University
  - 東北大学
  - 小中学生向け授業

- 今後の展開
  - **カードベース暗号を用いた教材の作成**
  - **カードベース暗号の教育効果の測定**
  - **暗号技術の普及のための視覚的ツールの開発**

まとめ

カードベース暗号分野の俯瞰図



カードベース暗号分野の今後

- プロトコル構成
  - シャッフルの種類を限定した設定の研究はまだ掘りがいがありそう
  - パイルの束の個数も重要そう（実装上はここがボトルネック）

- 不可能性証明
  - 現状の不可能性の結果は、4枚～6枚の2変数関数がほとんど
  - 不可能性証明のブレイクスルーに期待

- 教育応用・ゲーム応用
  - いくつか試みがあるものの、まだ研究分野として定まっていない印象
  - ゲームへの応用・新しいゲームの考案も興味深い方向性に感じる

本講演のまとめ

- カードベース暗号の歴史と最近の進展について紹介した

- いくつかの重要なトピックを取りこぼしています
  - 秘匿置換 / ガーブルド回路 / 対称関数 / 完全順列 / 金持ち比べ など

- 興味を持ってくださった方には、以下の文献をお勧めします
  - カード組を用いた秘密計算
    - 著者：水木敬明
    - 2016のIEICE Fundamentals Reviewの解説論文
  - 暗号の理論と技術 量子時代のセキュリティ理解のために
    - 編：國廣昇　著：安田雅哉／水木敬明／高安敦／高島克幸／米山一樹／大原一真／江村恵太
    - 出版日：2024年5月22日