カードベース暗号の最近の進展

品川 和雅
茨城大学

2024年5月30日(木)
IT研/EMM研合同研究会＠千葉大学

目次

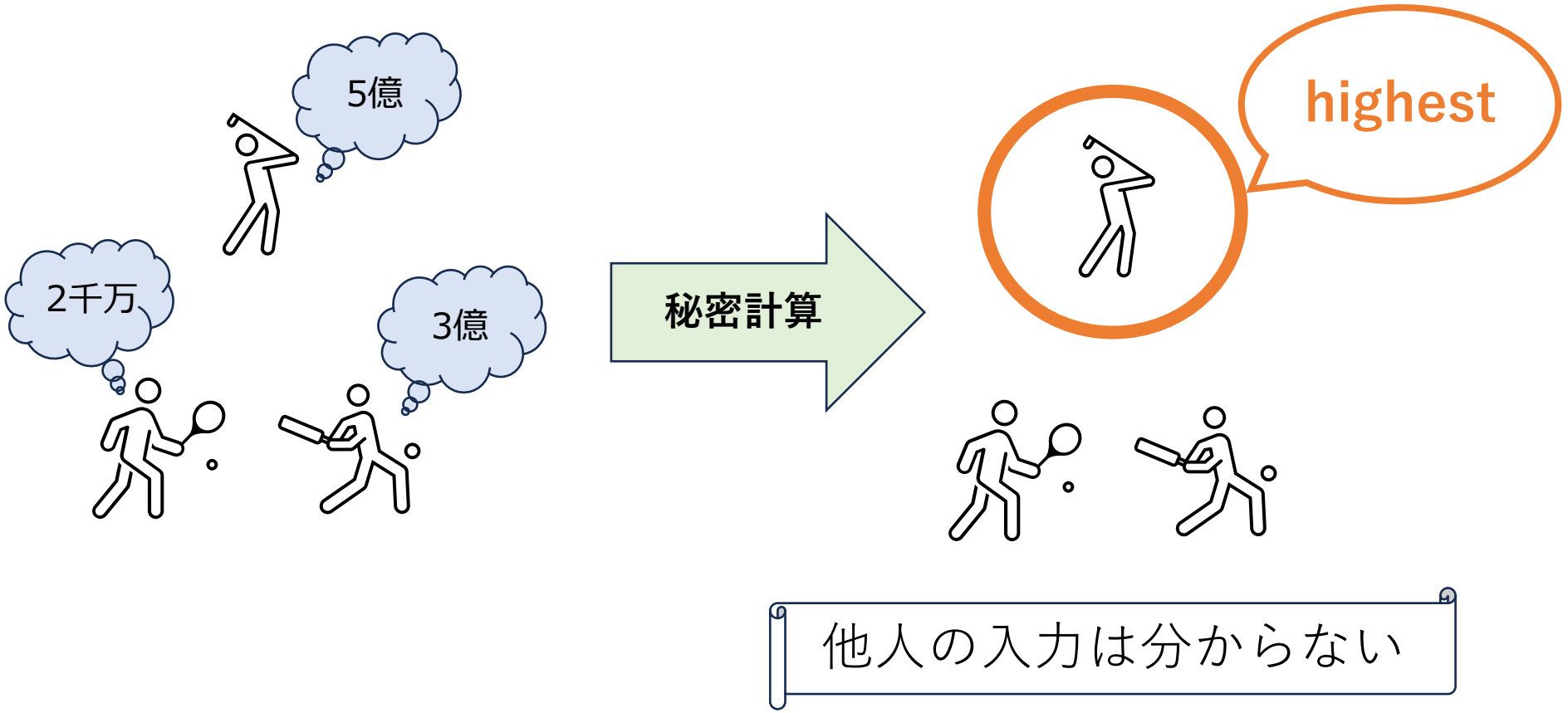
- イントロダクション

- カードベース暗号の重要な研究テーマ：計算限界の解明
  - 任意関数の計算可能性
  - カード枚数の削減
  - シャッフル回数の削減

- カードベース暗号の最近の話題
  - 有限群論とカードベース暗号
  - 数独のゼロ知識証明
  - カードゲームへの応用

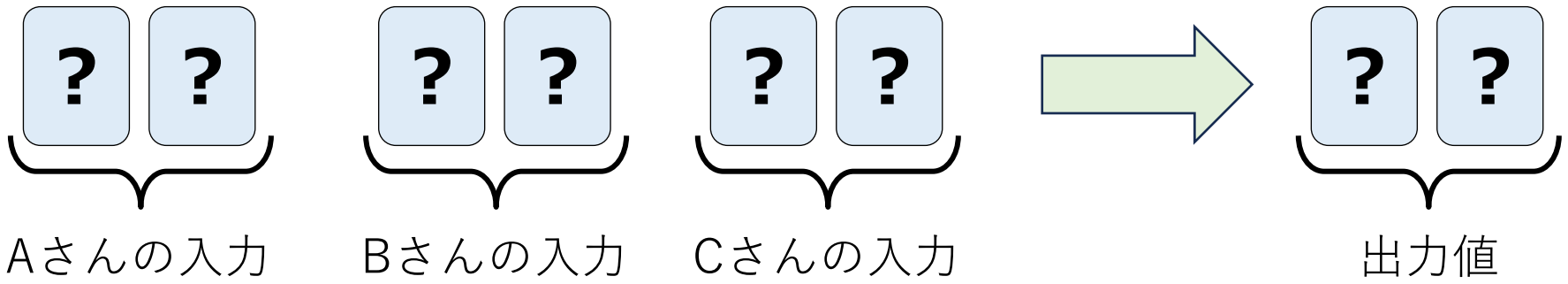
秘密計算

- 互いの入力を隠したまま、所望の出力を得る技術



カードベース暗号

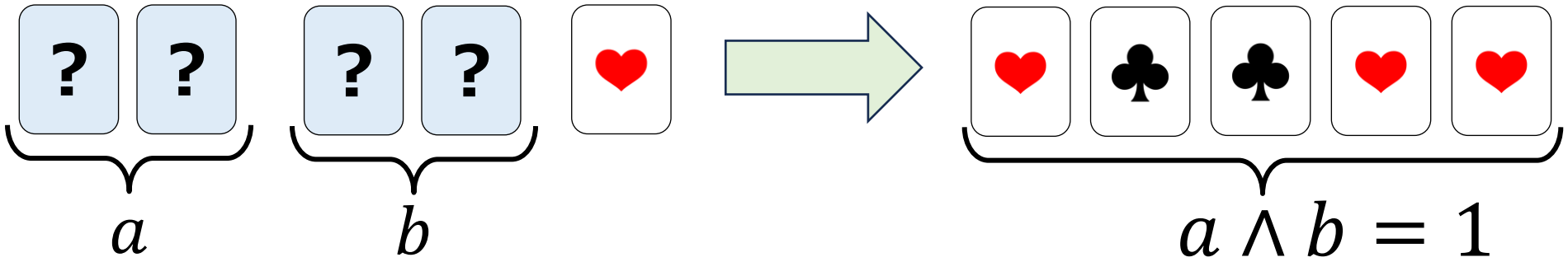
- カードを用いて秘密計算を実現する技術



- カードベース暗号の特徴
  - 手軽に実演でき、仕組みを理解しやすい

プロトコルの例：Five-Card Trick [den Boer, Eurocrypt 1989]

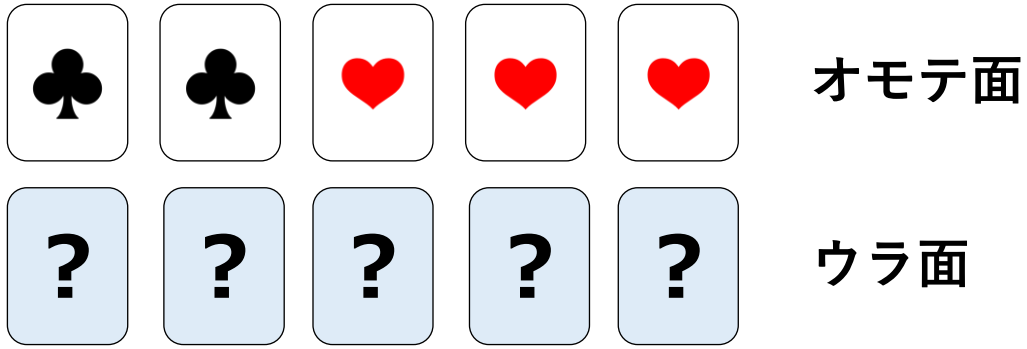
- 論理積$a \wedge b$を計算するプロトコル



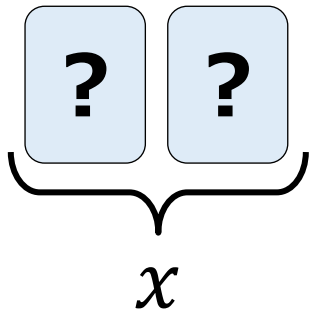
- 利用例：気まずくならない告白
  - 「好き」なら$a = 1$、「興味なし」なら$a = 0$
  - $a \wedge b = 1$なら「両思い」、$a \wedge b = 0$なら「片思い」か「お互い興味なし」

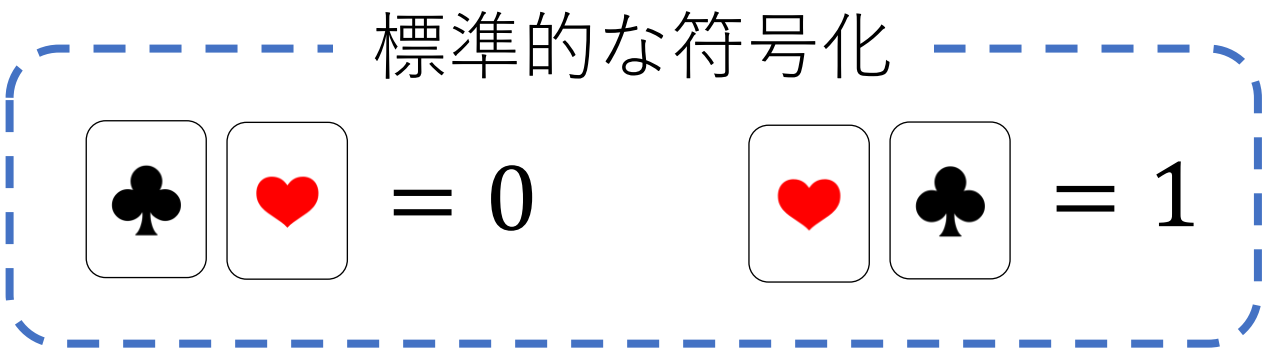
B. den Boer, More Efficient Match-Making and Satisfiability The Five Card Trick, EUROCRYPT 1989.

カードと符号化

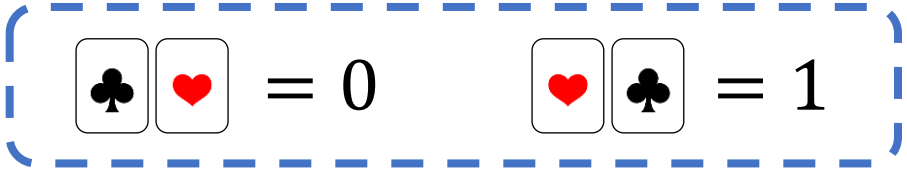


- 符号化に従う裏向きのカードを**コミットメント**と呼ぶ

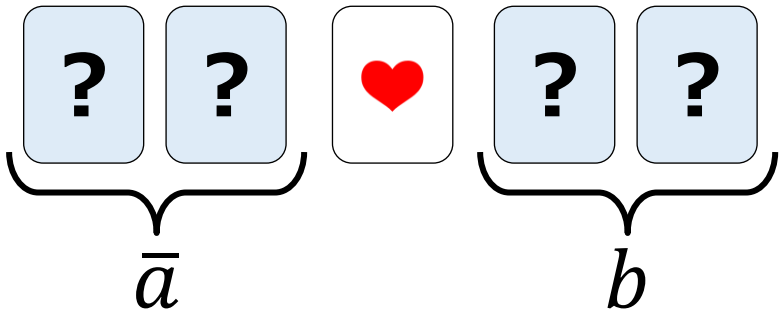




Five-Card Trick (1/3)

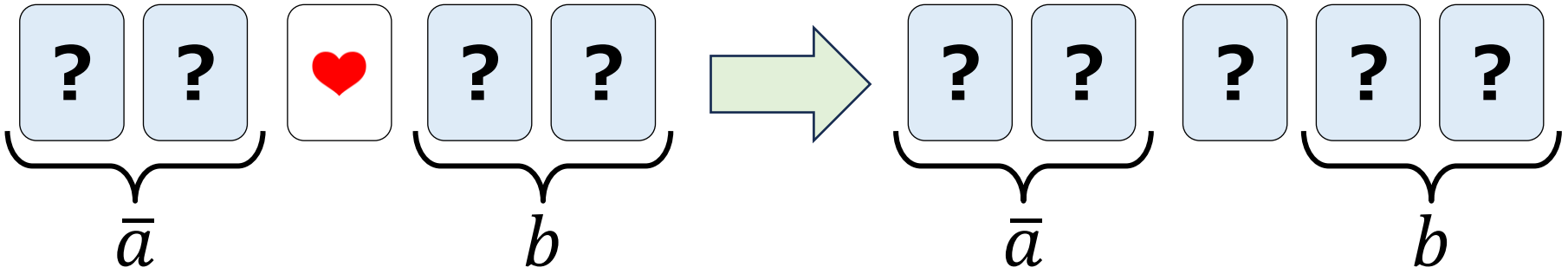


1. アリスはaのコミットメント、ボブはbのコミットメントを作り、以下のように並べる

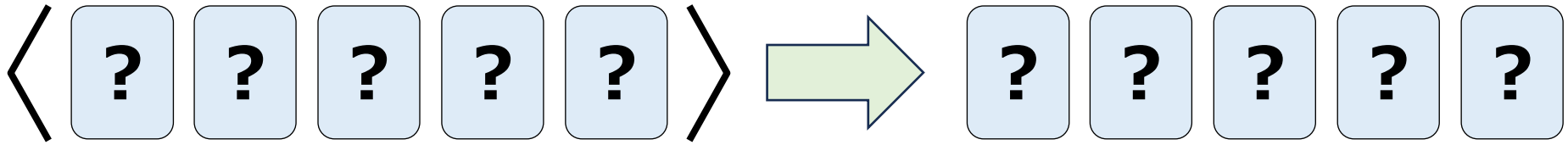


Five-Card Trick (2/3)

2. 中央のカードを裏にする



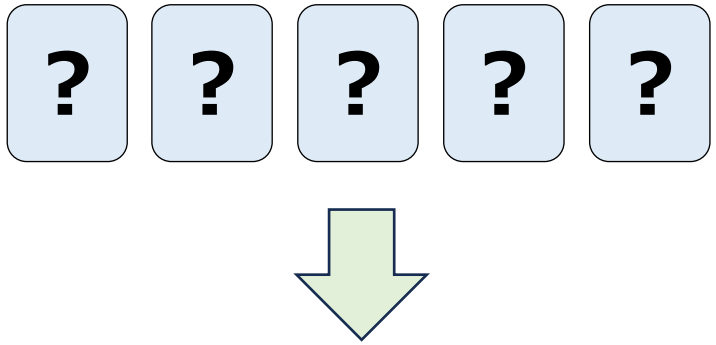
3. ランダムカットを適用する



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



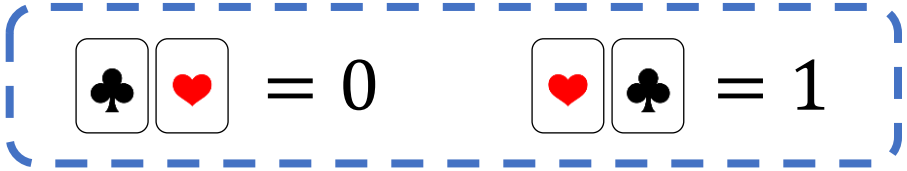
赤３枚が巡回的に並ぶ

$a \wedge b = 1$

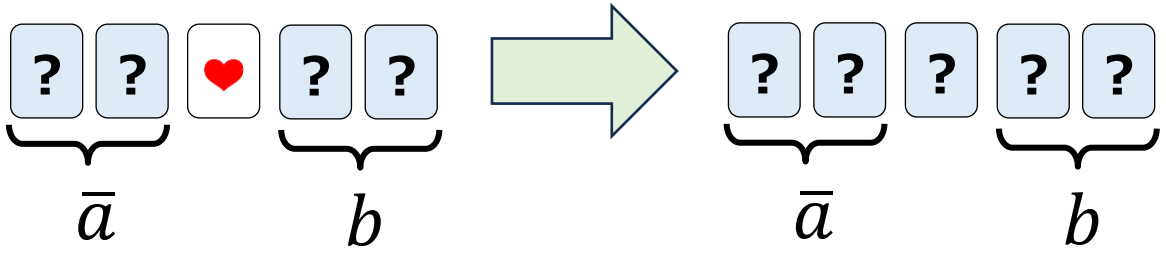
並ばない

$a \wedge b = 0$

Five-Card Trickのまとめ



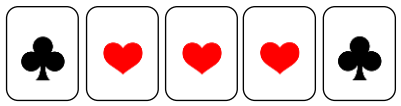
1. カードを並べ、中央を裏にする



2. ランダムカット

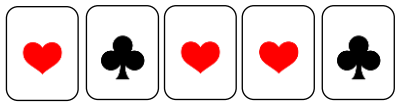
3. すべてのカードをめくる

赤３枚が並ぶ



$a \wedge b = 1$

並ばない



$a \wedge b = 0$

目次

- イントロダクション

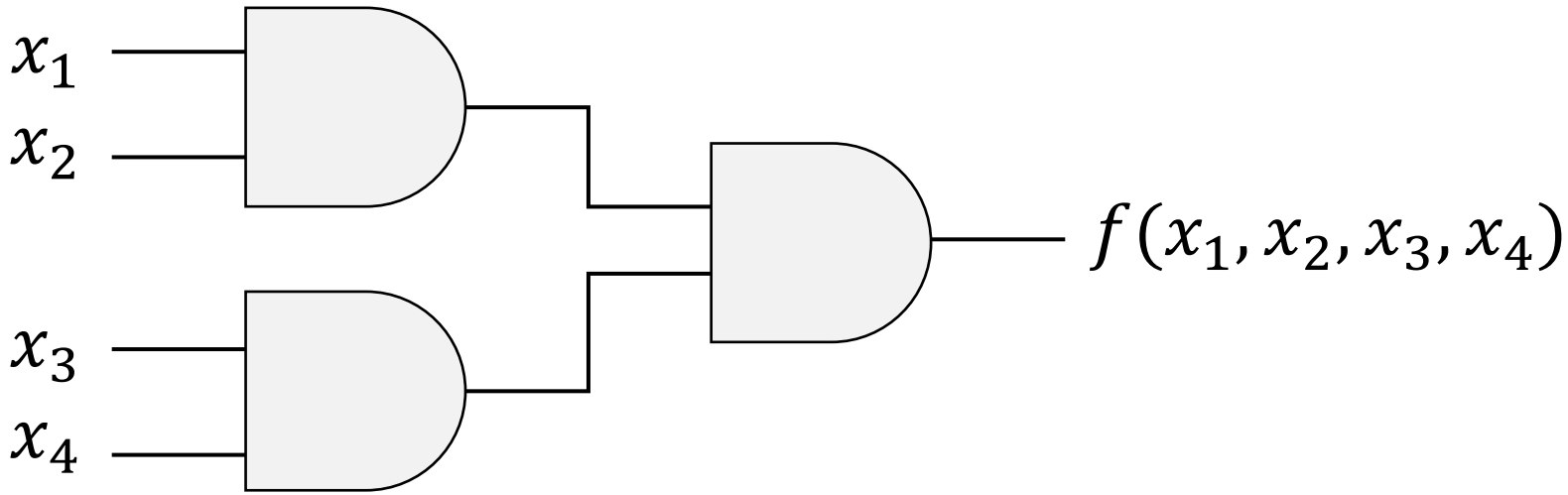
- **カードベース暗号の重要な研究テーマ：計算限界の解明**
  - **任意関数の計算可能性**
  - カード枚数の削減
  - シャッフル回数の削減

- カードベース暗号の最近の話題
  - 有限群論とカードベース暗号
  - 数独のゼロ知識証明
  - カードゲームへの応用

任意の関数は計算できるか？

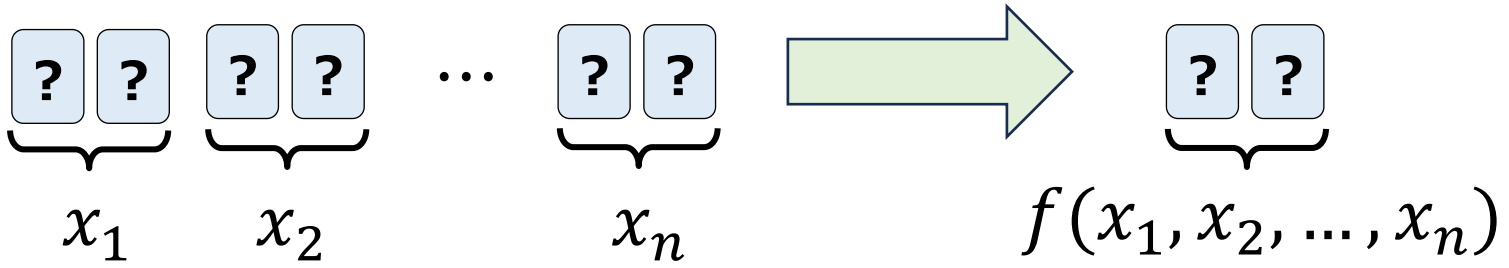
- **YES**：任意関数$f: \{0,1\}^n \rightarrow \{0,1\}$は計算できる

- アプローチ：ゲートごとの計算

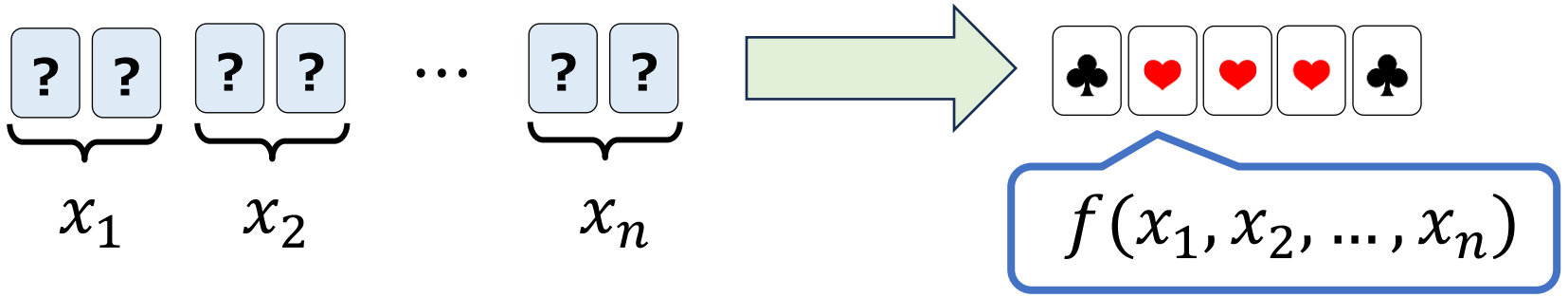


コミット型プロトコル

- **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

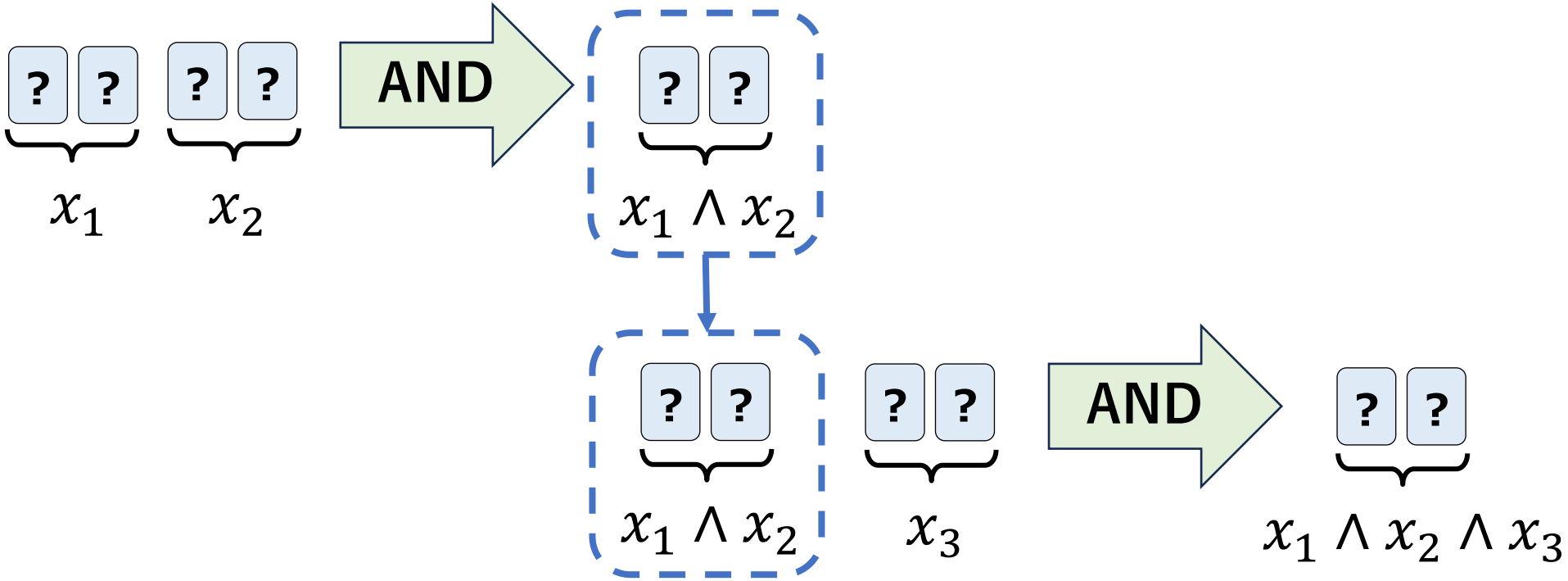


- **非コミット型プロトコル**：出力値そのものを公開するプロトコル



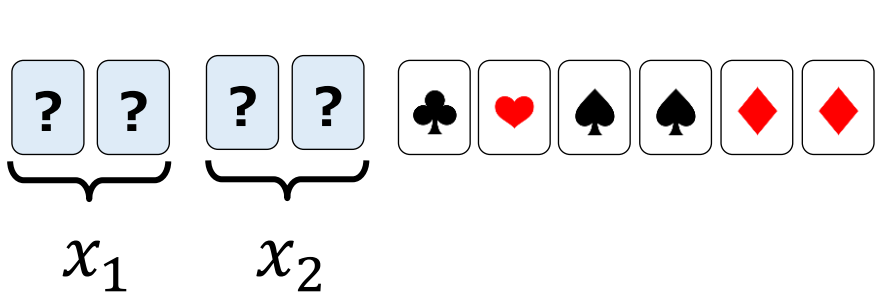
コミット型プロトコルの性質

- コミット型プロトコルは結合可能

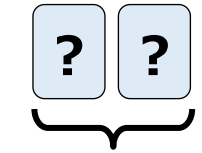


- **コミット型AND/COPYがあれば、任意関数を計算できる**

任意関数の計算可能性①[Crépeau-Kilian, CRYPTO 1993]

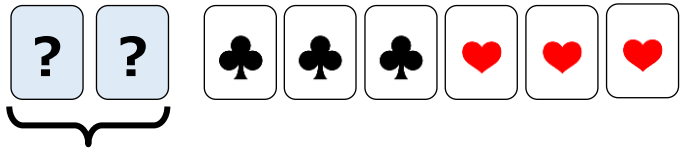


AND

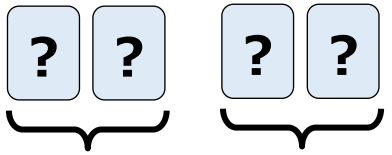


$x_1 \wedge x_2$

10枚・RC 8回 (期待値)



COPY

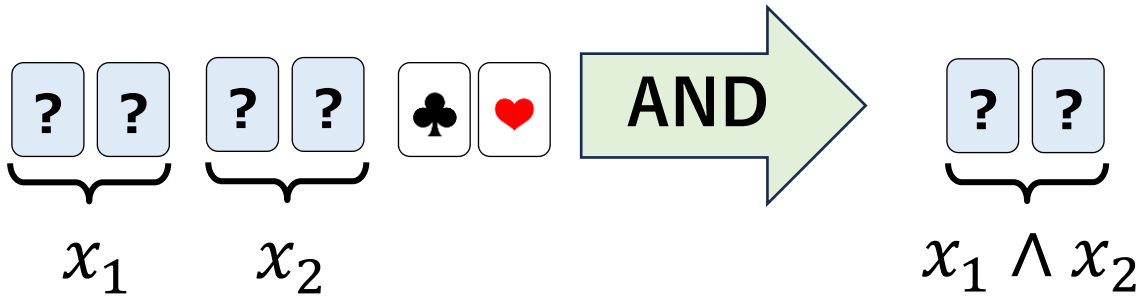


8枚・ RC 2回

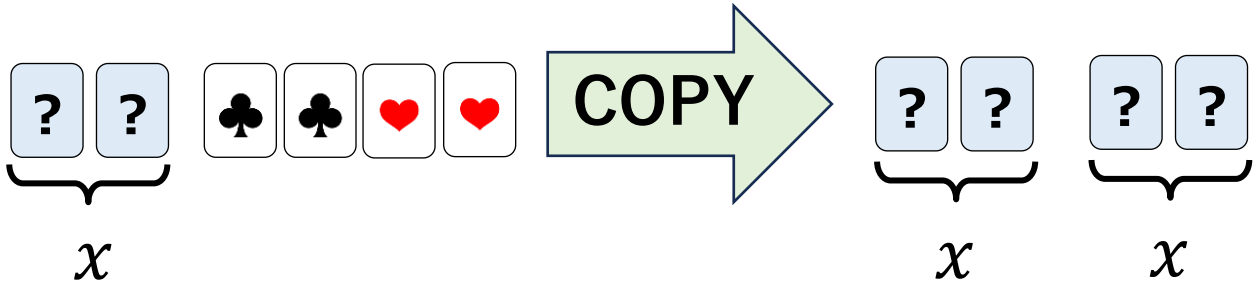
- ラスベガス（ステップ数の期待値有限）の意味で任意関数は計算可能
- 有限時間にできないか？

C. Crépeau and J. Kilian, Discreet Solitary Games, CRYPTO' 93, 1994.

任意関数の計算可能性②[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

- 任意関数の計算可能性が**有限時間の意味でも**解決された

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

目次

- イントロダクション

- **カードベース暗号の重要な研究テーマ：計算限界の解明**
  - 任意関数の計算可能性
  - **カード枚数の削減**
  - シャッフル回数の削減

- カードベース暗号の最近の話題
  - 有限群論とカードベース暗号
  - 数独のゼロ知識証明
  - カードゲームへの応用

カード枚数はどこまで削減できるか？

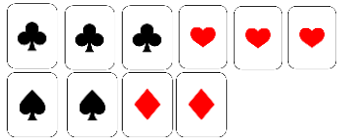
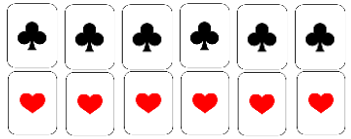
- カード枚数は重要な効率性指標
- 計算モデル：**Mizuki-Shizuyaモデル**[Mizuki-Shizuya, IJISec 2014]

  - 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

- プロトコル構成（上界）と不可能性証明（下界）の両方から迫る

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

コミット型ANDプロトコル (～2009年)

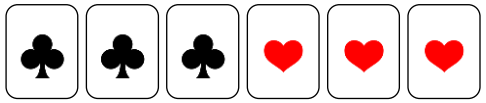
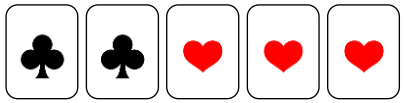
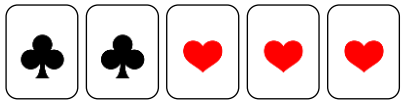
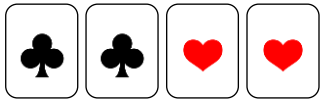
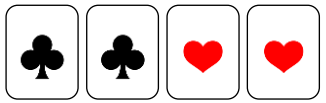
	カード枚数	ランダムカット	二等分割カット	シャッフル回数
Crépeau-Kilian [CK94]	10  (※4色)	✓		8
Niemi-Renvall [NR98]	12 	✓		7.5
Stiglic [Sti01]	8 	✓		2
Mizuki-Sone [MS09]	6 		✓	1

[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.

シャッフルの性質

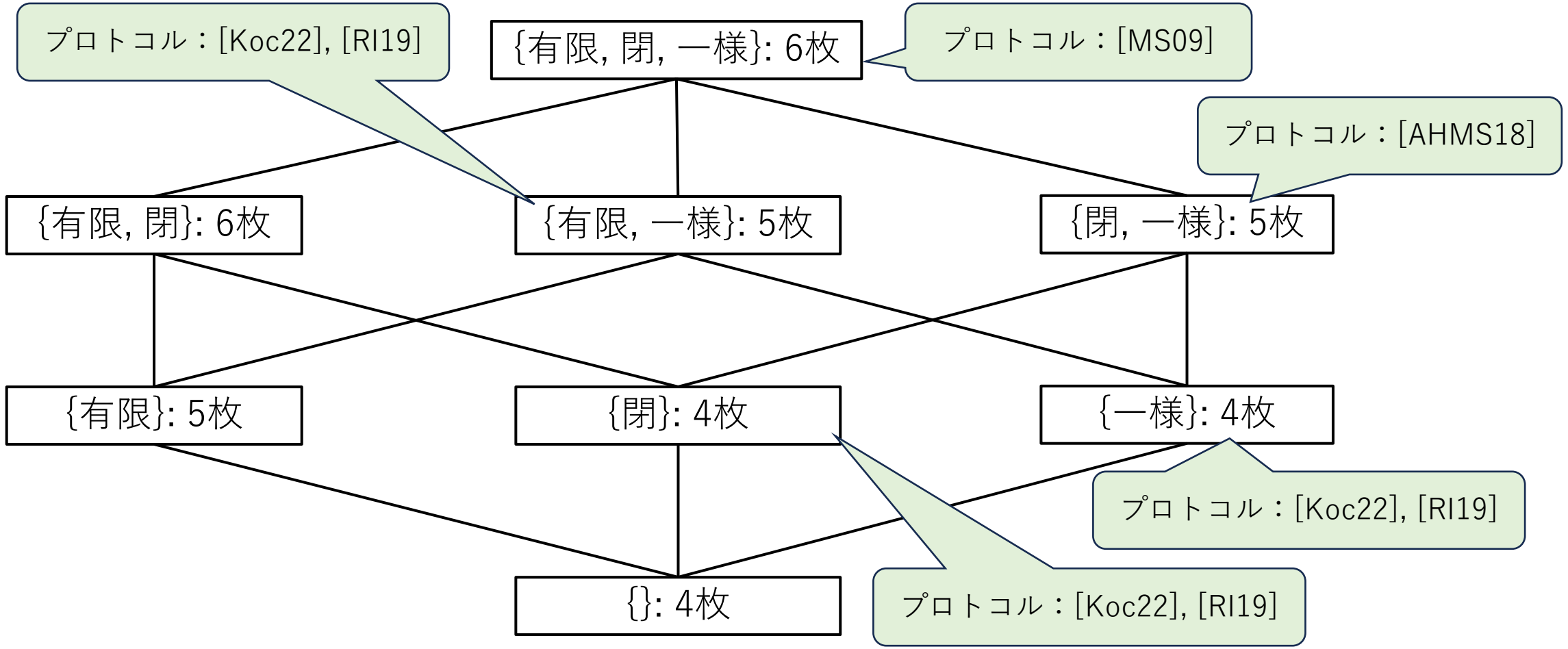
- $(\mathrm{shuffle}, \Pi, \mathcal{F})$：分布$\mathcal{F}$に従って、置換$\pi \in \Pi$を適用
- **一様シャッフル**$(\mathrm{shuffle}, \Pi, \mathcal{F}) \Leftrightarrow \mathcal{F}$が$\Pi$上の一様分布
- **閉シャッフル**$(\mathrm{shuffle}, \Pi, \mathcal{F}) \Leftrightarrow \Pi$が部分群

コミット型ANDプロトコル (2009年〜)

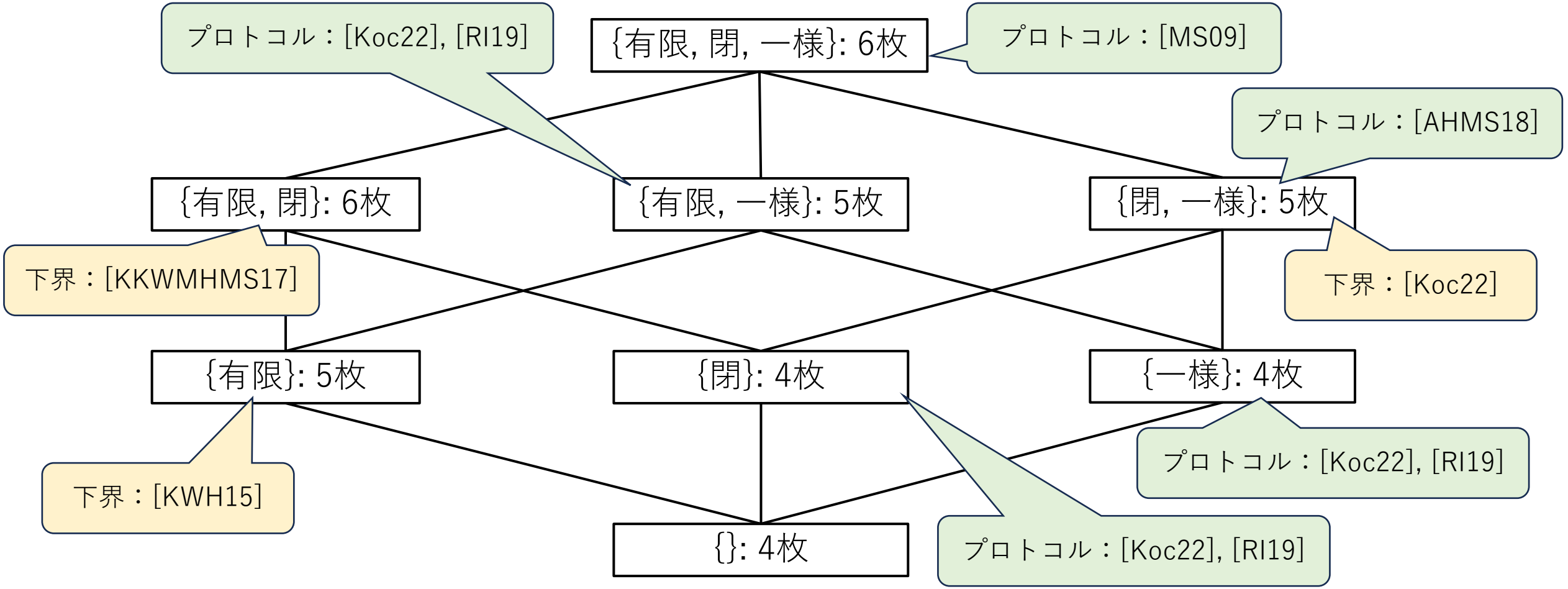
	カード枚数	有限時間	一様	閉
Mizuki-Sone [MS09]	6 	✓	✓	✓
Abe et al. [AHMS18]	5 		✓	✓
Koch [Koc22] Ruangwises-Itoh [RI19]	5 	✓	✓	
Koch et al. [KWH15]	4 			✓
Koch [Koc22] Ruangwises-Itoh [RI19]	4 		✓	

[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



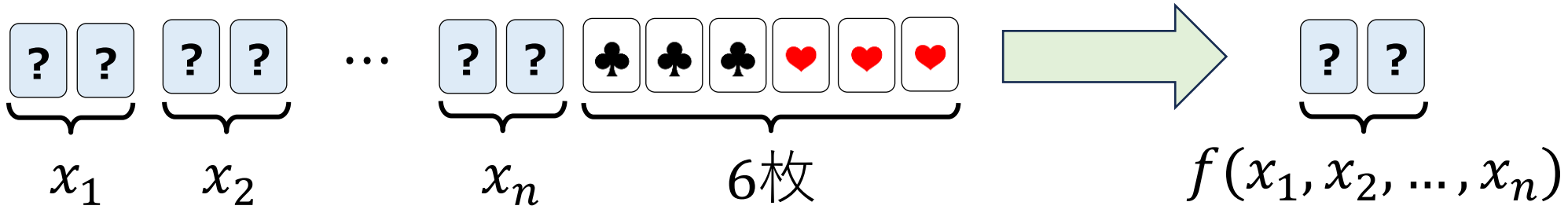
最適なコミット型ANDプロトコル



[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.

任意関数プロトコルのカード枚数

- $2n+6$枚のプロトコル[Nishida et al., TAMC 2015]



- 入力に$2n$枚必要だから、最小カード枚数xは$2n \leq x \leq 2n+6$

- **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.

目次

- イントロダクション

- **カードベース暗号の重要な研究テーマ：計算限界の解明**
  - 任意関数の計算可能性
  - カード枚数の削減
  - **シャッフル回数の削減**

- カードベース暗号の最近の話題
  - 有限群論とカードベース暗号
  - 数独のゼロ知識証明
  - カードゲームへの応用

シャッフル回数はどこまで削減できるか？

- シャッフル回数は時間計算量の支配的パラメータ

- 上界：回路のゲート数
  - AND/XOR/COPYプロトコルはゲートごとにシャッフル1回

- 上界を改善できるか？

シャッフル1回のプロトコル[Shinagawa-Nuida, DAM 2021]

- 1回の一様閉シャッフルで任意の論理回路を計算できる
- ガーブルド回路手法：ゲートのランダマイズを同時に行う

x_1	x_2	g
0	0	0
0	1	0
1	0	0
1	1	1

行の置換

x_1	x_2	g
1	0	0
0	0	0
0	1	0
1	1	1

値のマスク

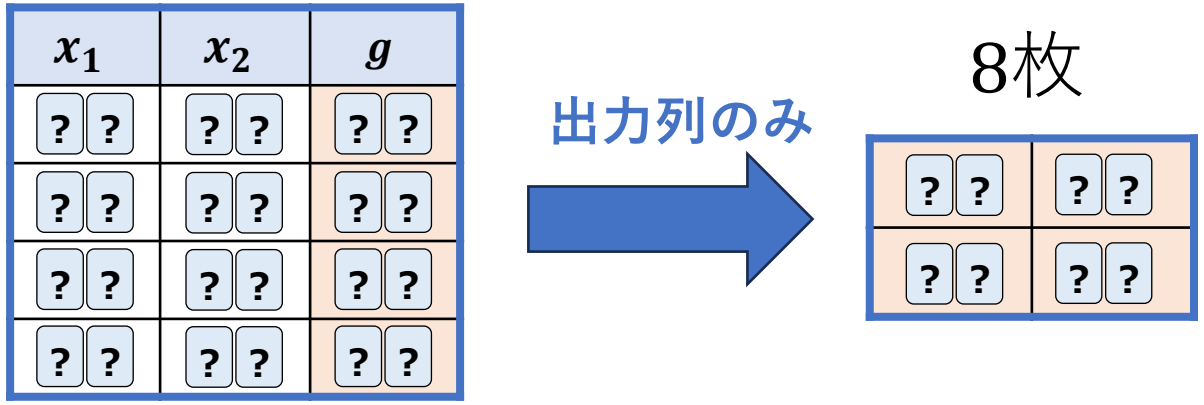
x_1	x_2	g
$1 \oplus r_1$	$0 \oplus r_2$	$0 \oplus r_3$
$0 \oplus r_1$	$0 \oplus r_2$	$0 \oplus r_3$
$0 \oplus r_1$	$1 \oplus r_2$	$0 \oplus r_3$
$1 \oplus r_1$	$1 \oplus r_2$	$1 \oplus r_3$

- 各ゲート24枚のカードを用いる

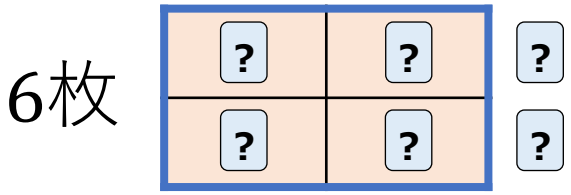
K. Shinagawa and K. Nuida, A Single Shuffle is Enough for Secure Card-Based Computation of Any Boolean Circuit, DAM, 2021.

改良版 [Tozawa-Morita-Mizuki, UCNC 2023], [Ono et al., ICISC 2023]

- 各ゲート8枚への改良[TMM23]



- 各ゲート6枚への改良（一様シャッフルを用いる）[OSNWI23]



[TMM23] K. Tozawa, H. Morita, and T. Mizuki, Single-Shuffle Card-Based Protocol with Eight Cards per Gate, UCNC 2023.
[OSNWI23] T. Ono, K. Shinagawa, T. Nakai, Y. Watanabe, and M. Iwamoto, Single-Shuffle Card-Based Protocols with Six Cards per Gate, ICISC 2023.

目次

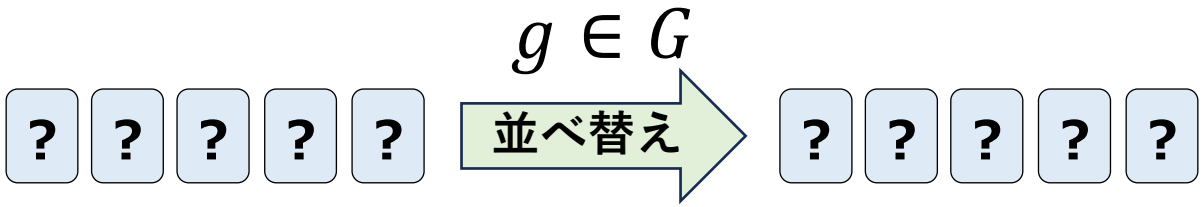
- イントロダクション

- カードベース暗号の重要な研究テーマ：計算限界の解明
  - 任意関数の計算可能性
  - カード枚数の削減
  - シャッフル回数の削減

- **カードベース暗号の最近の話題**
  - **有限群論とカードベース暗号**
  - 数独のゼロ知識証明
  - カードゲームへの応用

有限群論とカードベース暗号

- 群Gをn次対称群S_nの部分群とする
- シャッフル$(\mathrm{shuffle}, G)$：Gの一様ランダム元で並び替える操作



- ランダムカットはGが巡回群$\langle(1,2,3,4,5)\rangle$の場合

- Gが巡回群の場合は「ある置換を繰り返し適用する操作」
- 一方、一般の群の場合、$(\mathrm{shuffle}, G)$の実装が大変な場合もある

一様巡回群分解 (Uniform Cyclic group Factorization)

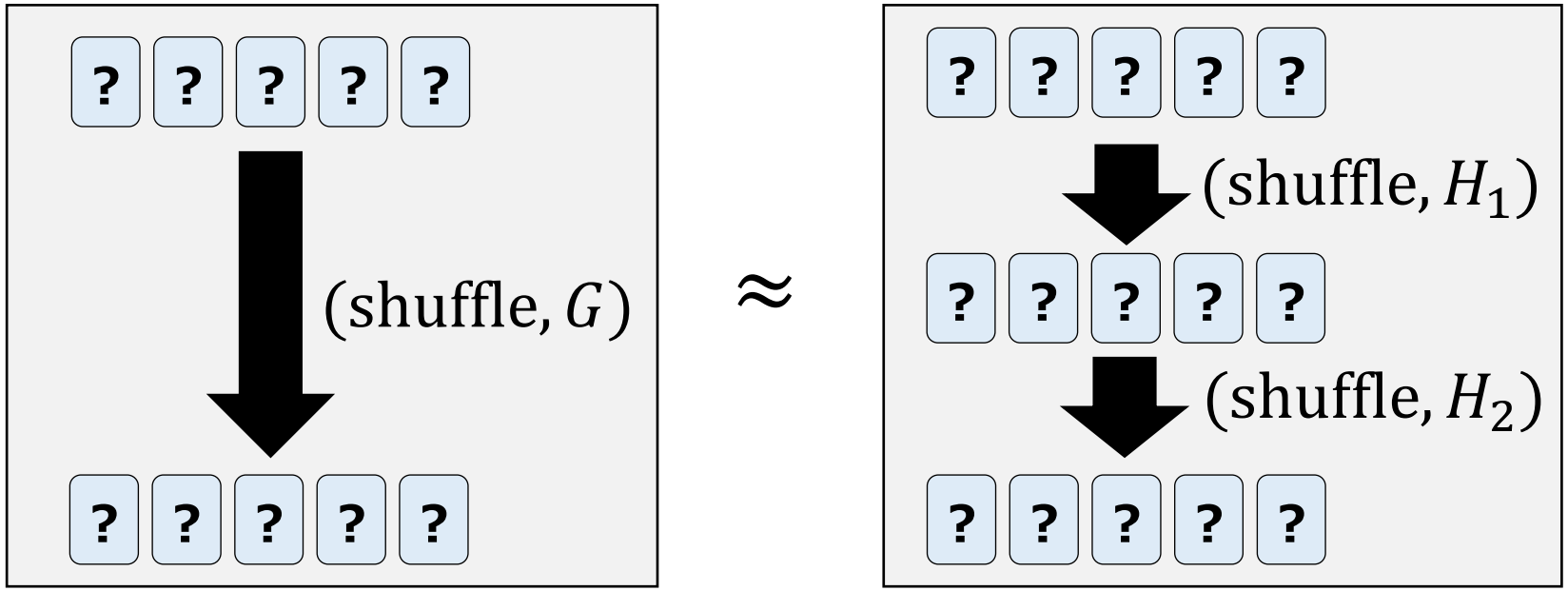
- Gの**部分群**の列$\vec{H} = (H_1, H_2, \ldots, H_k)$が$G$の**一様群分解**であるとは、多重集合$\mathrm{mult}_{\vec{H}} := \{h_1 h_2 \cdots h_k \mid h_i \in H_i\}$が以下を満たすこと：
  - $\mathrm{mult}_{\vec{H}}$にGの各元が同じ個数ずつ現れること（重複度一定）

- 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.

UCFとシャッフル

- (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

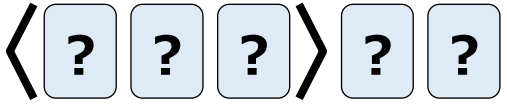


- **GがUCFを持つと、$(\mathrm{shuffle}, G)$を簡単な操作列に分解できる**

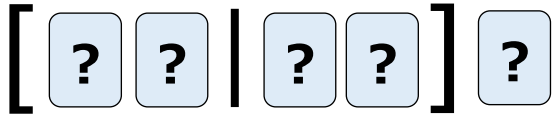
具体例：交代群A_5シャッフル

- $\langle(1\ 2\ 3)\rangle, \langle(1\ 3)(2\ 4)\rangle, \langle(1\ 2)(3\ 4)\rangle, \langle(1\ 2\ 3\ 4\ 5)\rangle$は$A_5$のUCF

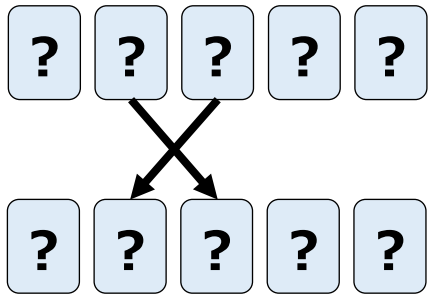
1. ランダムカット



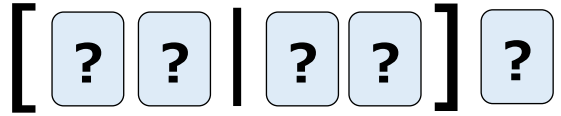
2. ランダム二等分割カット



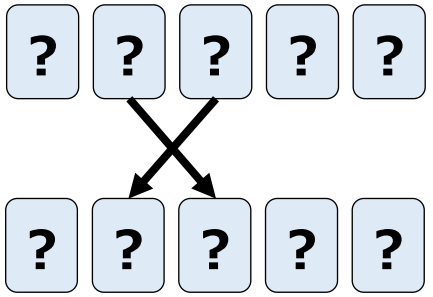
3. 並べ替える



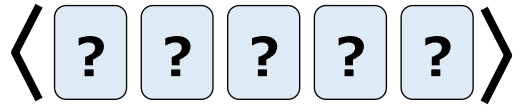
4. ランダム二等分割カット



5. 並べ替える



6. ランダムカット



どのような群がUCFを持つか？

- 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.

目次

- イントロダクション

- カードベース暗号の重要な研究テーマ：計算限界の解明
  - 任意関数の計算可能性
  - カード枚数の削減
  - シャッフル回数の削減

- **カードベース暗号の最近の話題**
  - 有限群論とカードベース暗号
  - **数独のゼロ知識証明**
  - カードゲームへの応用

数独のゼロ知識証明

- アリスはある数独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	

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

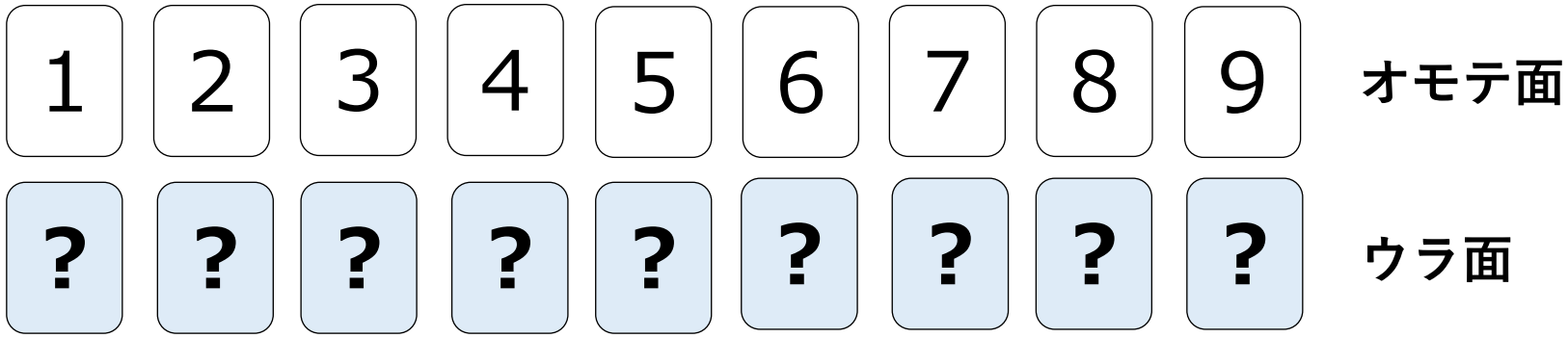
問題

		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	

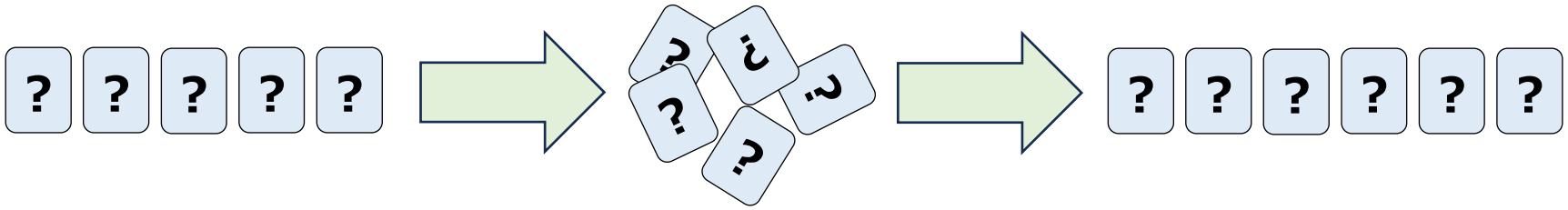
答え

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

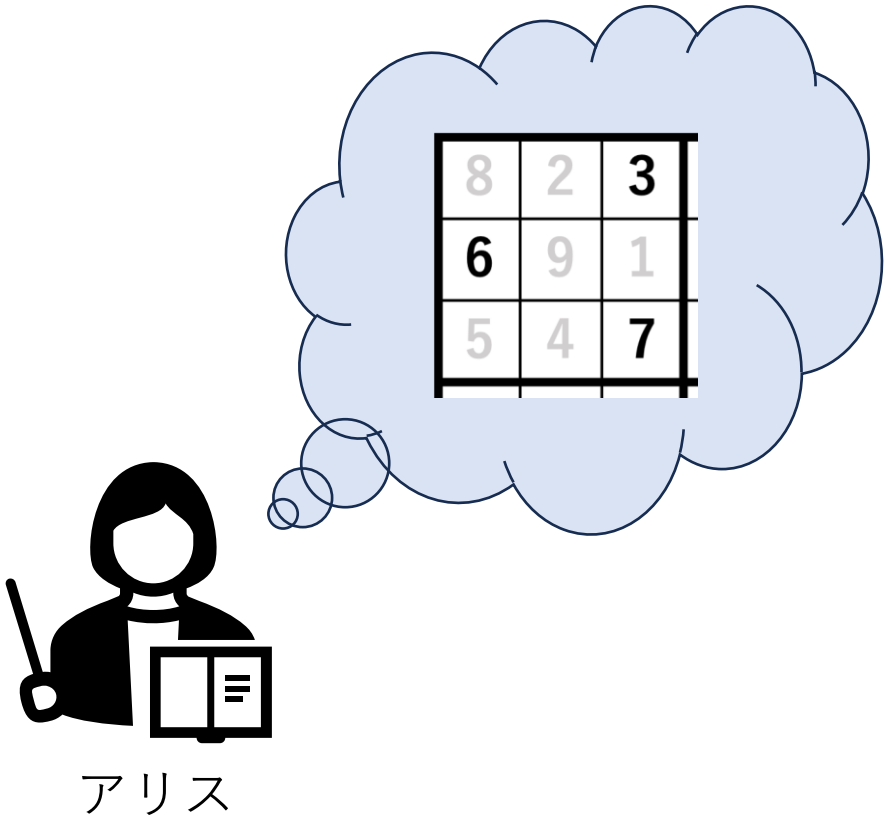


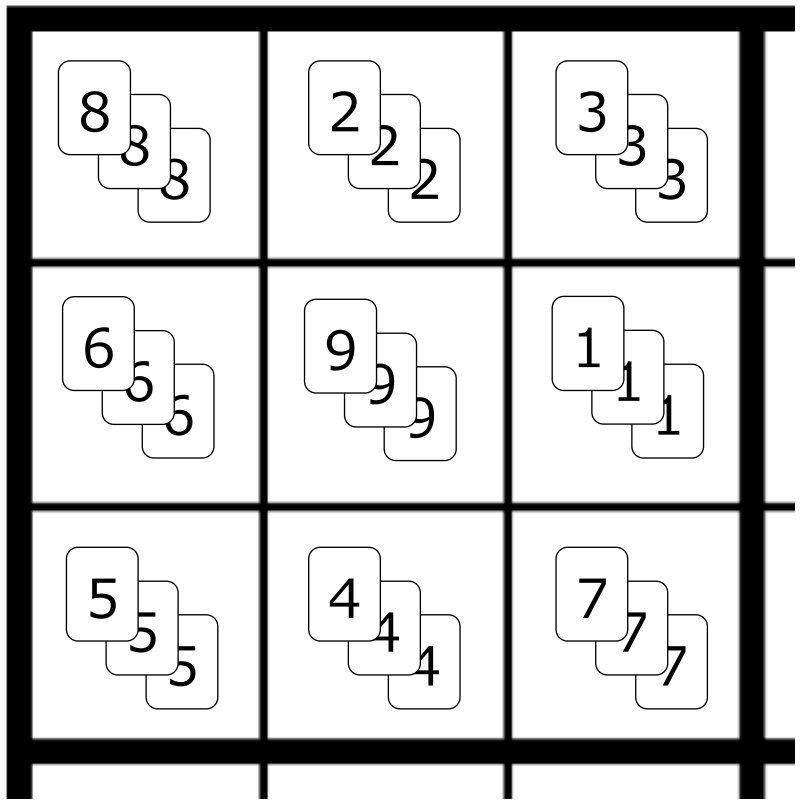
- **完全シャッフル**



GNPRプロトコル[Gradwohl-Naor-Pinkas-Rothblum, FUN 2009]

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

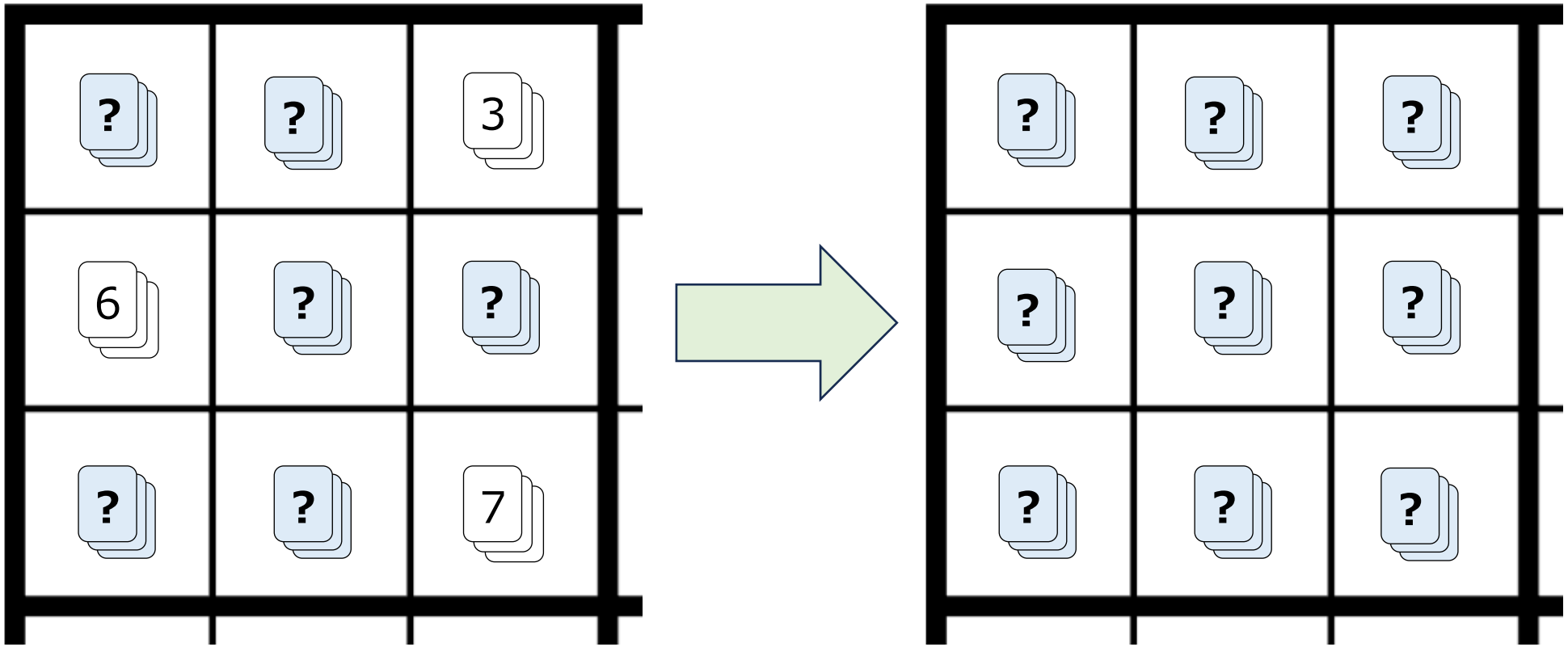




R. Gradwohl, M. Naor, B. Pinkas, and G. N. Rothblum, Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles, FUN 2007.

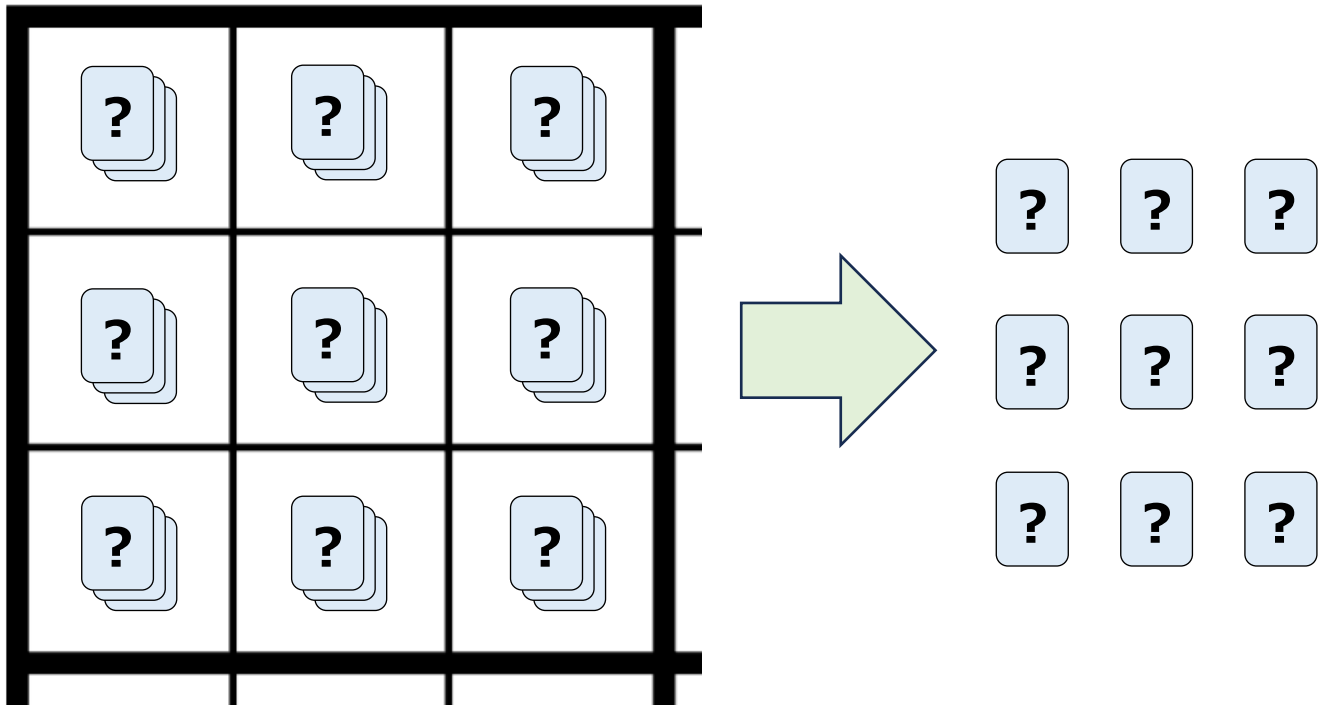
GNPRプロトコル

2. すべてのカードを裏にする



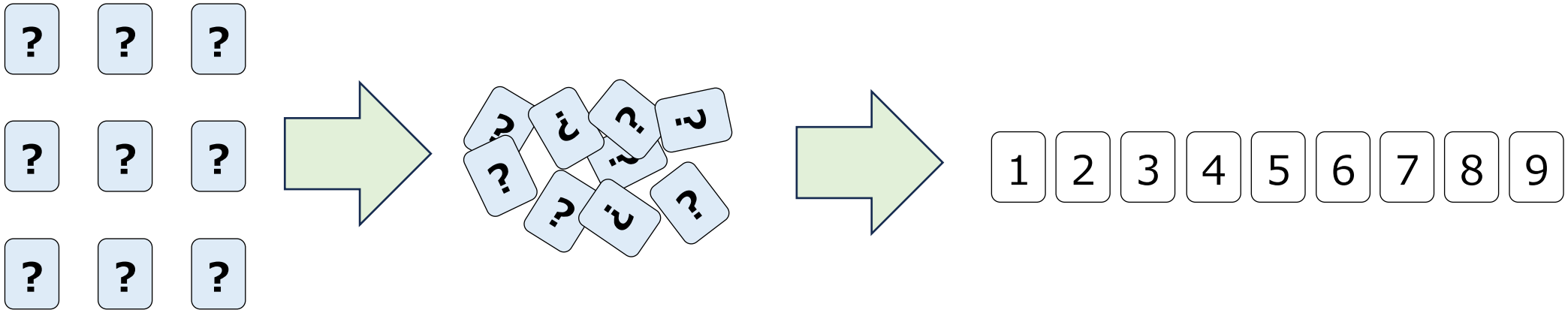
GNPRプロトコル

3. 各行・列・ブロックについて、各マスからカードを1枚ずつ選び、9枚の束を合計27個（9行＋9列＋9ブロック分）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



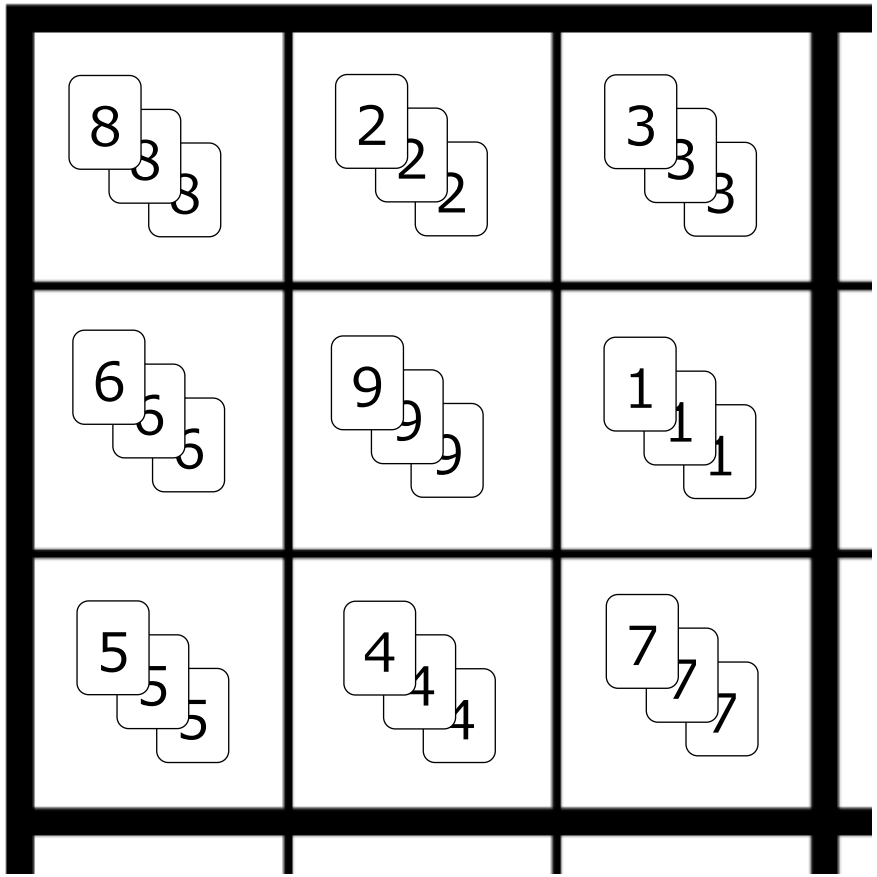
数独のゼロ知識証明プロトコル(※interactiveなプロトコルは除く)

	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

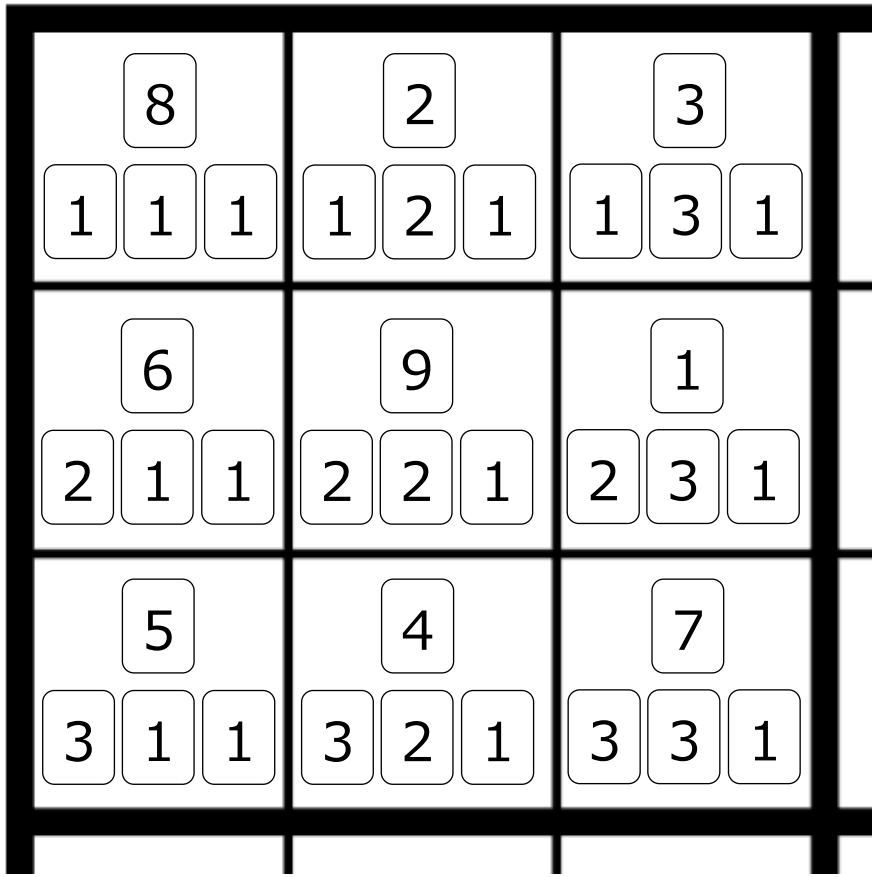
[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, FUN 2018.
[TM23] K, Tanaka and T. Mizuki, Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku, FCT 2023.
[SS23] 佐々木, 品川, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム, 2023.
[TM24] 田中, 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.

従来アイディアと改良アイディア

従来：**解答そのもの**を扱う

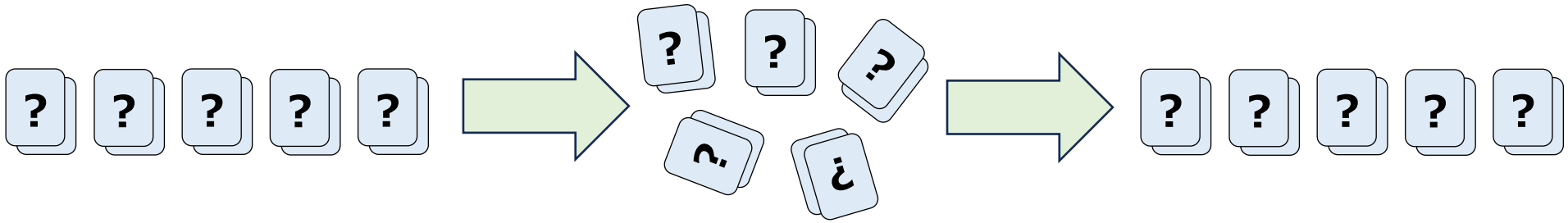


改良：**マスの座標**を扱う



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

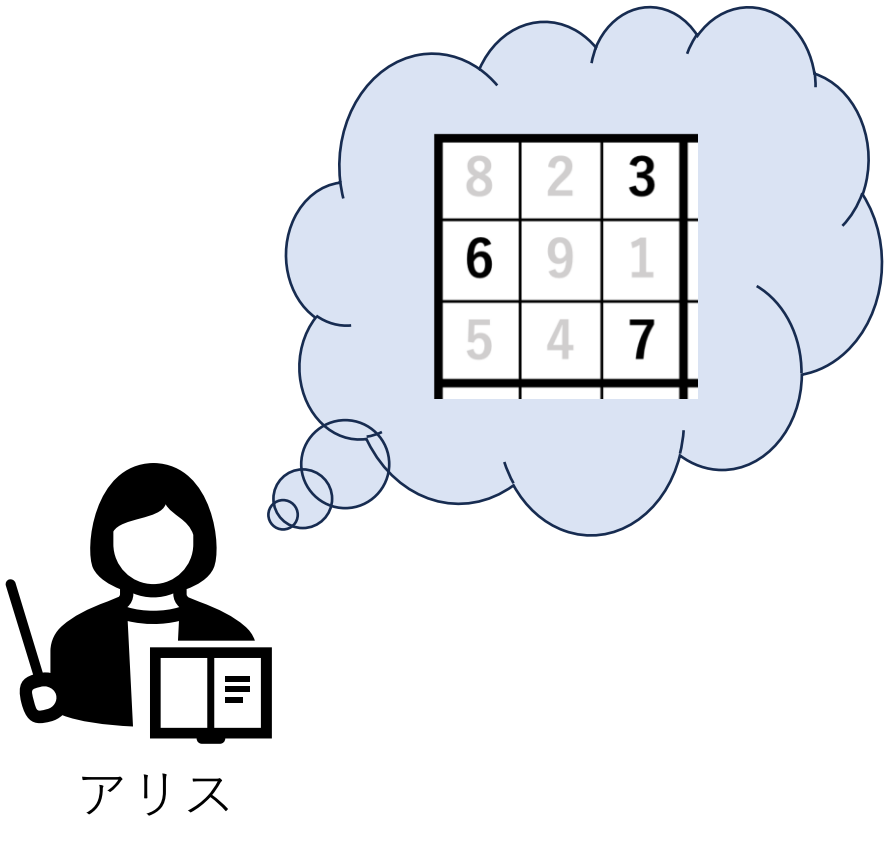
- カード束を一様ランダムに並べ替えるシャッフル

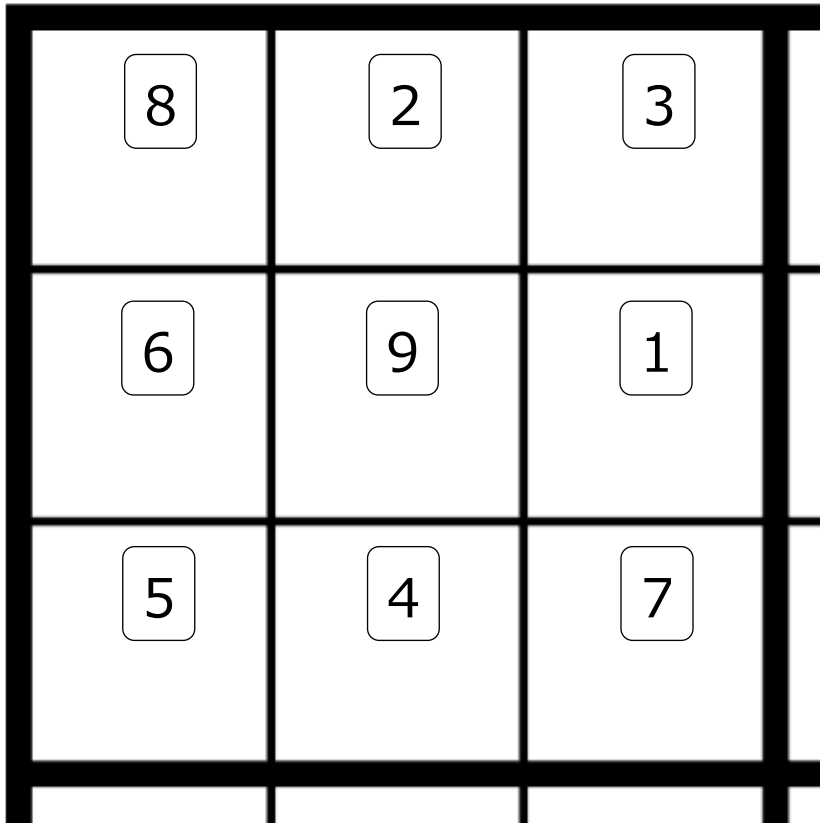


- 以下のシャッフルと共にPracticalな操作と考えられている
  - ランダムカット（巡回）
  - ランダム二等分割カット（巡回）
  - パイルシフティングシャッフル（巡回）
  - 完全シャッフル（S_n）
  - パイルスクランブルシャッフル（S_n）

佐々木-品川のプロトコル[佐々木-品川, CSS2023]

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

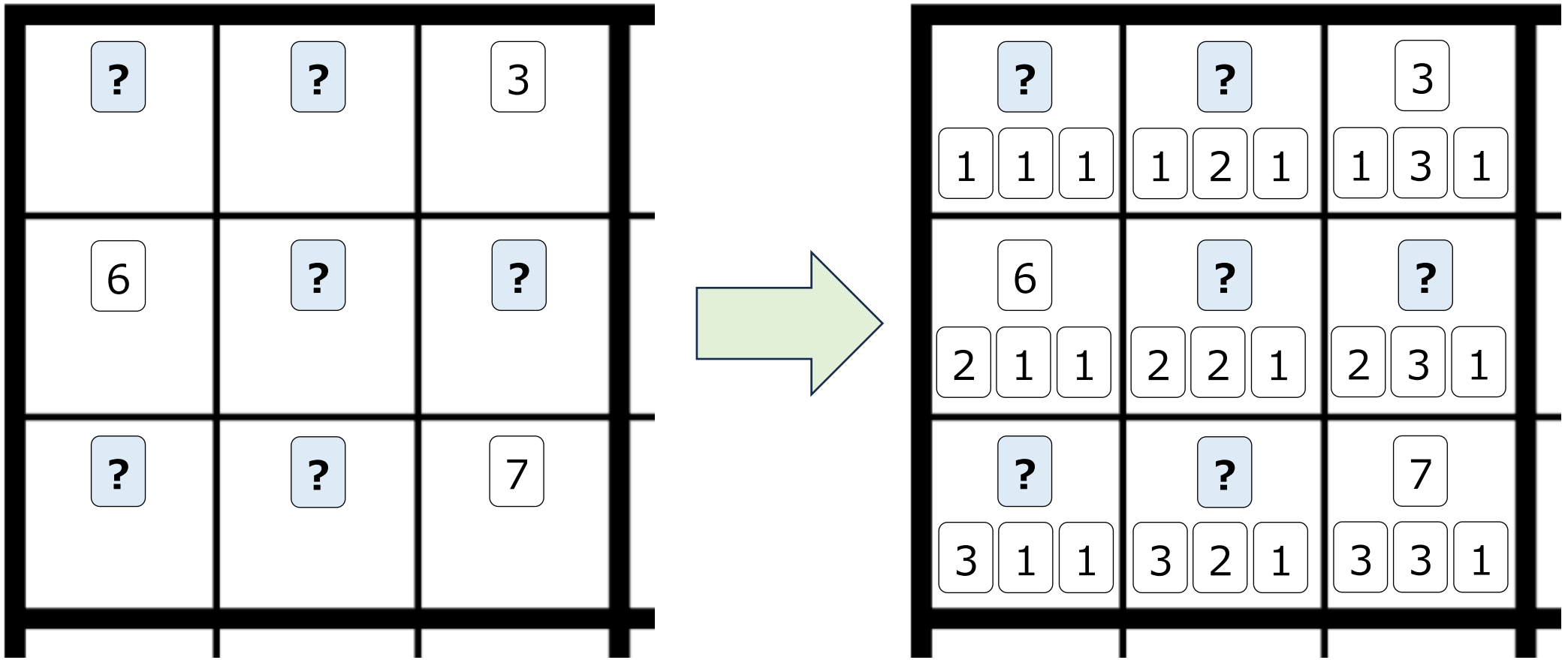




佐々木駿, 品川和雅, 数独に対するシャッフル3回のゼロ知識証明, コンピュータセキュリティシンポジウム (CSS 2023), 2023.

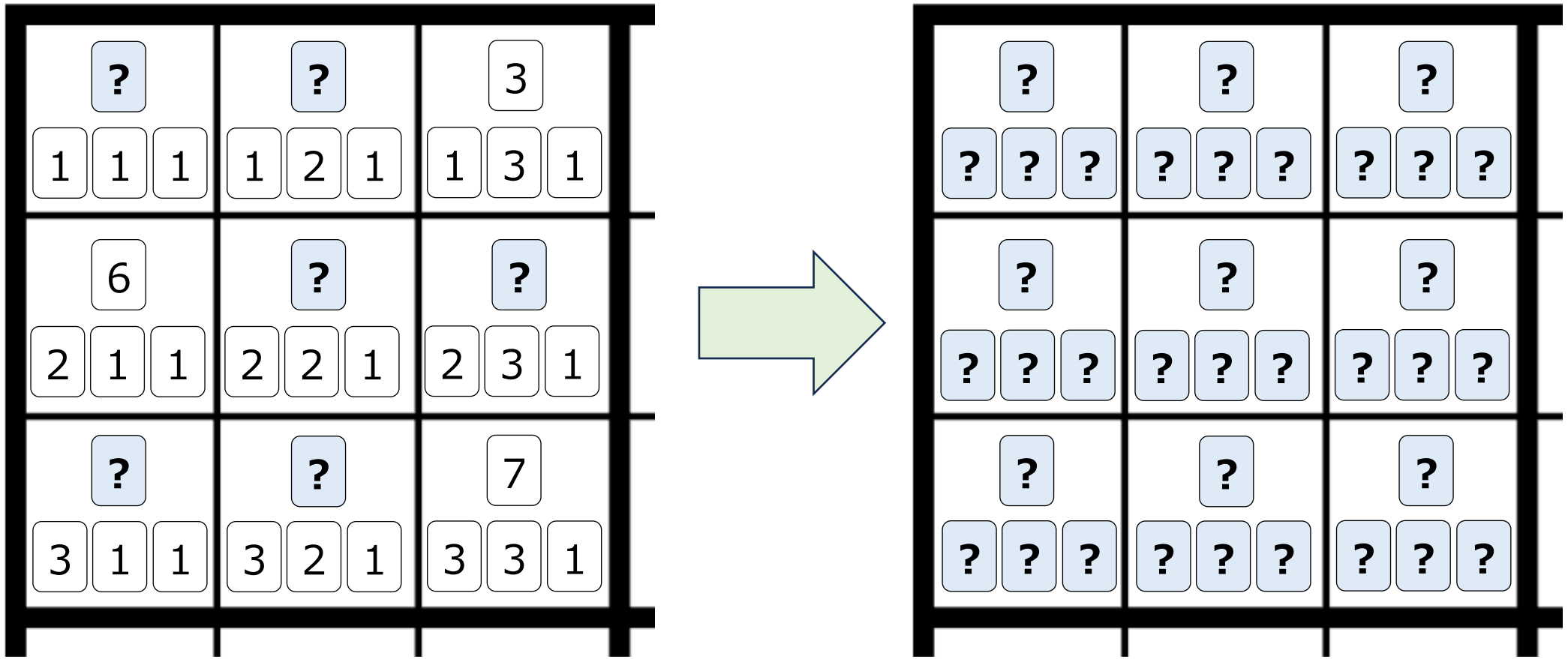
佐々木-品川のプロトコル

2. a行b列cブロックのマスに a b c を置く



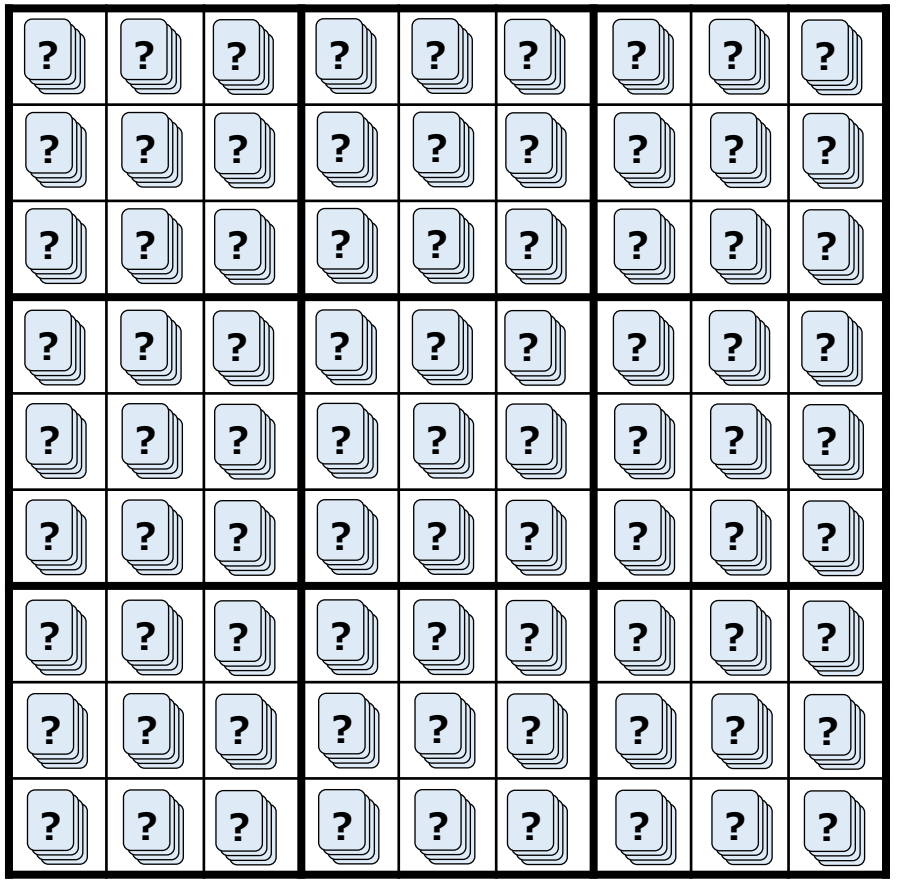
佐々木-品川のプロトコル

3. すべてのカードを裏にする



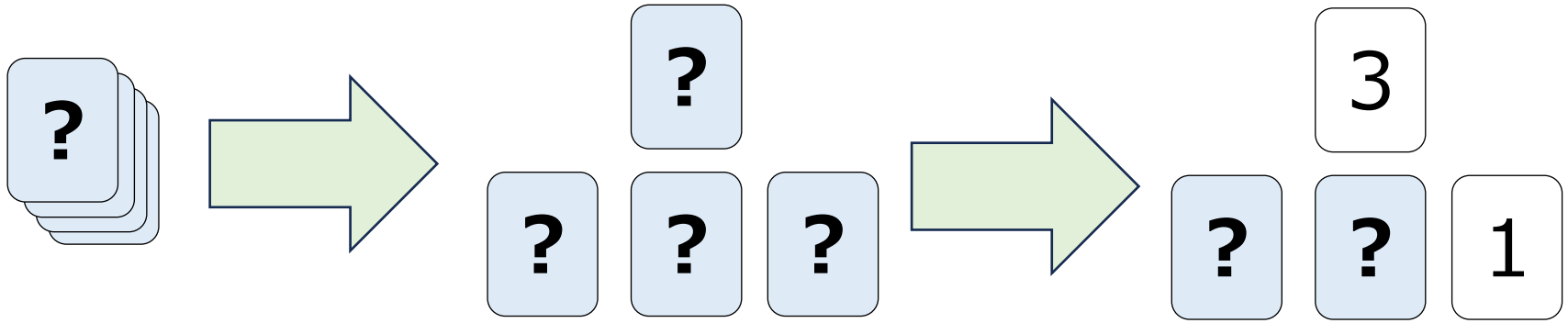
佐々木-品川のプロトコル

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

田中-水木のプロトコル[田中-水木, SCIS2024]

- 佐々木-品川の行検証と列検証を同時に行う方法を提案
- 2回のPScrambleのみで実行できる（シャッフル回数最小）
- **未解決問題：1回のPScrambleの数独プロトコルは可能か？**
- **未解決問題：どのパズルが定数回のPScrambleで検証できるか？**

田中滉大, 水木敬明, 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 (SCIS2024), 2024.

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.

目次

- イントロダクション

- カードベース暗号の重要な研究テーマ：計算限界の解明
  - 任意関数の計算可能性
  - カード枚数の削減
  - シャッフル回数の削減

- **カードベース暗号の最近の話題**
  - 有限群論とカードベース暗号
  - 数独のゼロ知識証明
  - **カードゲームへの応用**

カードゲームへの応用

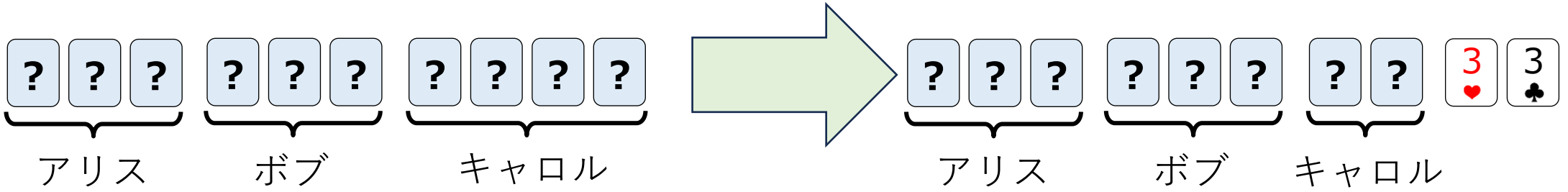
- カードベース暗号は、まるでカードゲームを遊ぶかのように、暗号プロトコルを実演する技術（と解釈することもできる）

- 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



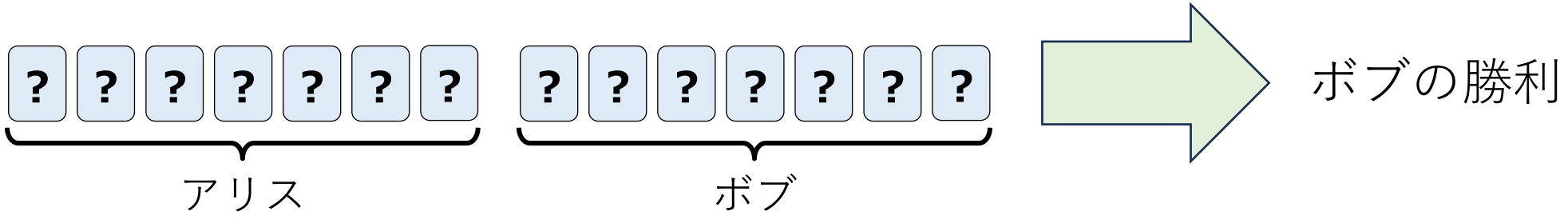
- **Future Work：他のゲームのプレイヤ模倣・ゲームマスター排除**

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.

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
- 最近活発に研究が進んでおり、他分野との融合領域も開拓中
- 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