数独に対する物理的ゼロ知識証明

安部芳紀

電気通信大学（現：セコム株式会社　IS研究所）

IMI研究集会@九州大学

目次

- 物理的ゼロ知識証明の背景
- 数独に対するゼロ知識証明の分類
  - Gradwholらの手法
  - 佐々木･品川の手法
- プロトコルの更なる効率化
  - 入力方法の再考
  - Onoらの手法
- 新しい証明手法のアイデア

数独とは

問題

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

解答

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

「数独(SUDOKU)」はニコリの登録商標です。

数独とは

問題

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

解答

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

数独とは

問題

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

解答

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

数独とは

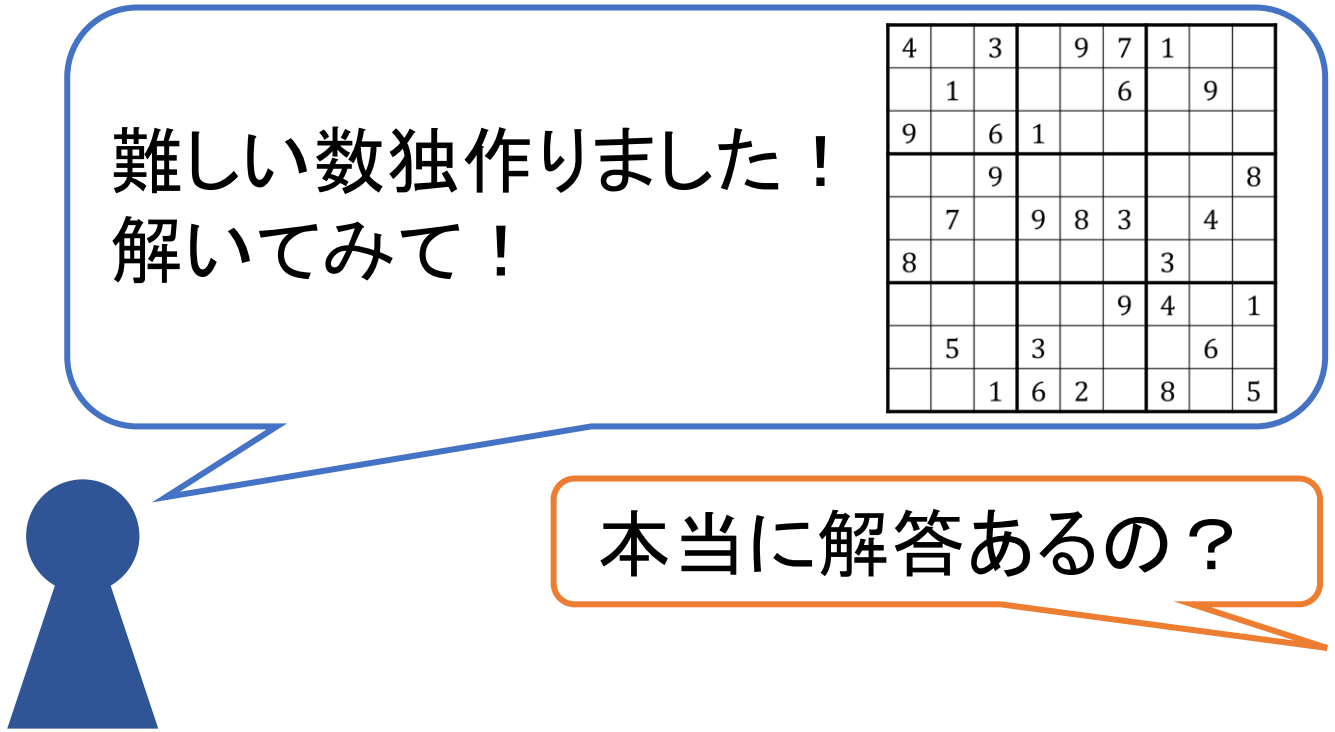
問題

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

解答

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

ゼロ知識証明（Zero-Knowledge Proof, ZKP）

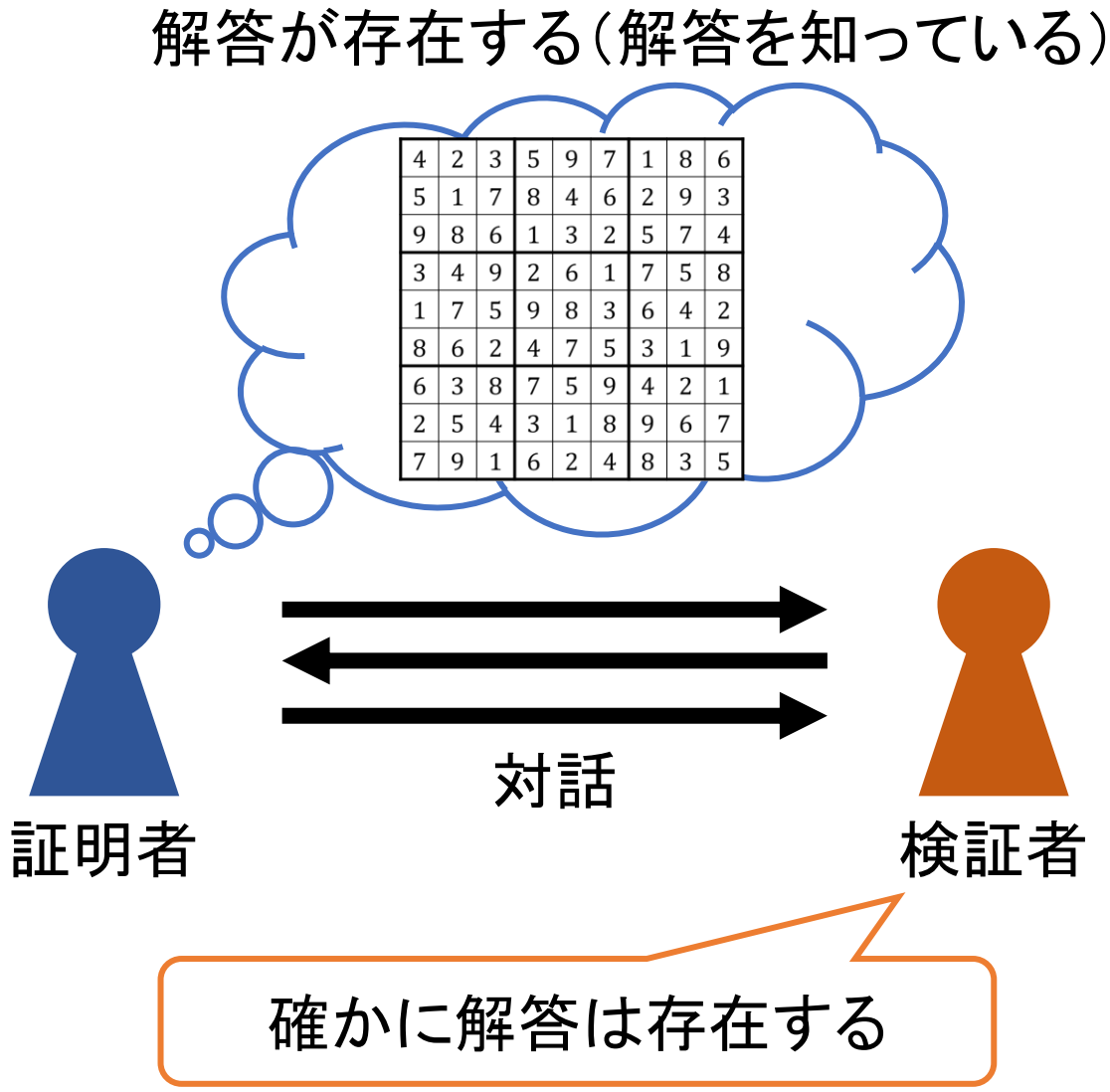


4		3		9	7	1		
	1				6		9	
9		6	1					
		9						8
	7		9	8	3		4	
8						3		
					9	4		1
	5		3				6	
		1	6	2		8		5

ゼロ知識証明：両者を両立する2者間プロトコル

ゼロ知識証明の要件①：完全性

- ➢完全性
  - ◆解答が存在
    ⇒ 検証者は必ず納得する
- ➢健全性
  - ◆解答が存在しない
    ⇒ 検証者は高確率で納得しない
- ➢ゼロ知識性
  - ◆検証者は解答に関する情報を（存在の有無に関する情報以外）何も得られない



ゼロ知識証明の要件②：健全性

➢完全性

◆解答が存在

⇒ 検証者は必ず納得する

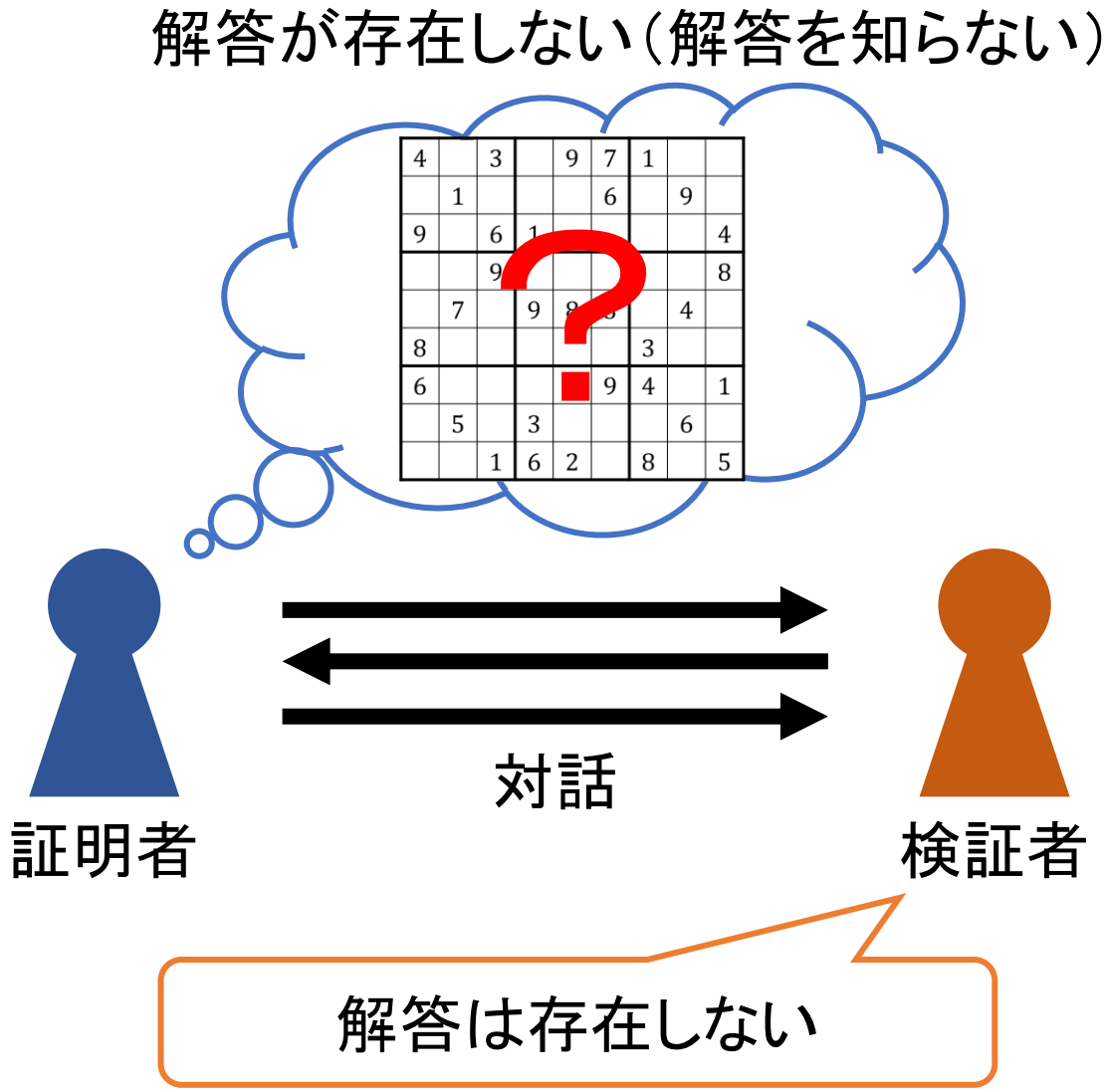
➢健全性

◆解答が存在しない

⇒ 検証者は高確率で納得しない

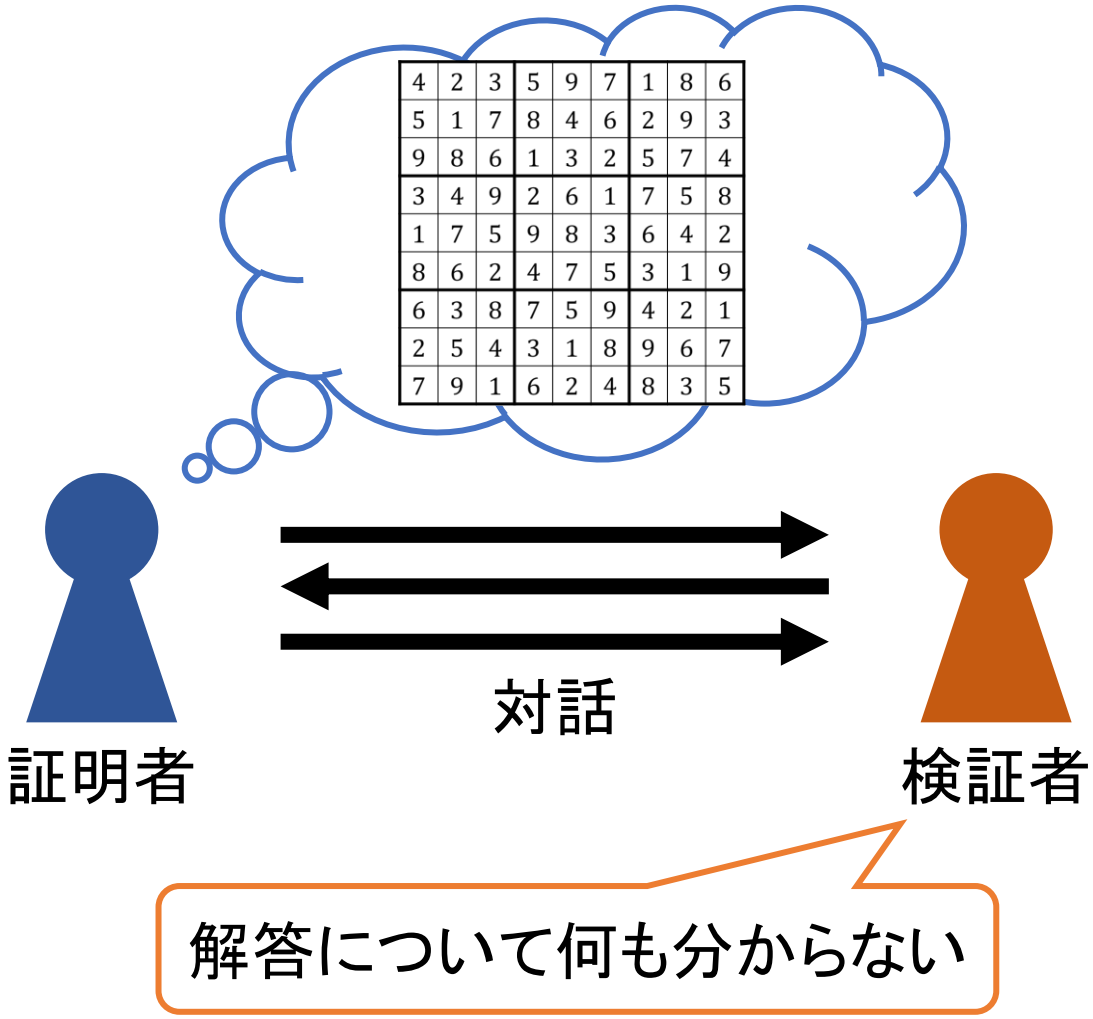
➢ゼロ知識性

◆検証者は解答に関する情報を（存在の有無に関する情報以外）何も得られない



ゼロ知識証明の要件③：ゼロ知識性

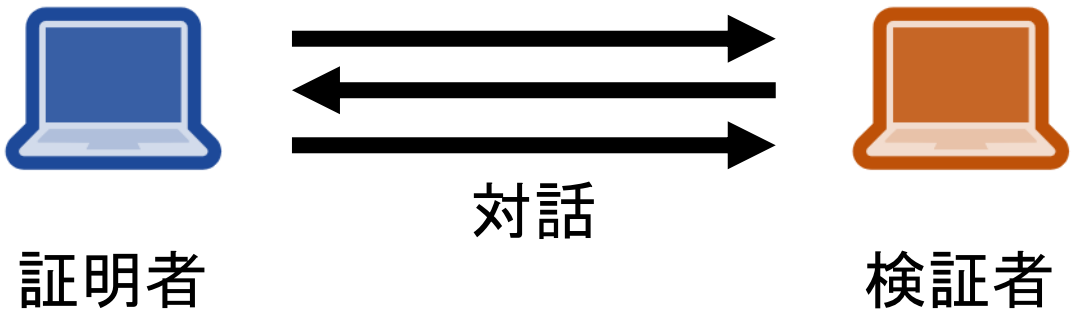
- 完全性
  - ◆解答が存在
    ⇒ 検証者は必ず納得する
- 健全性
  - ◆解答が存在しない
    ⇒ 検証者は高確率で納得しない
- ゼロ知識性
  - ◆検証者は解答に関する情報を（存在の有無に関する情報以外）何も得られない



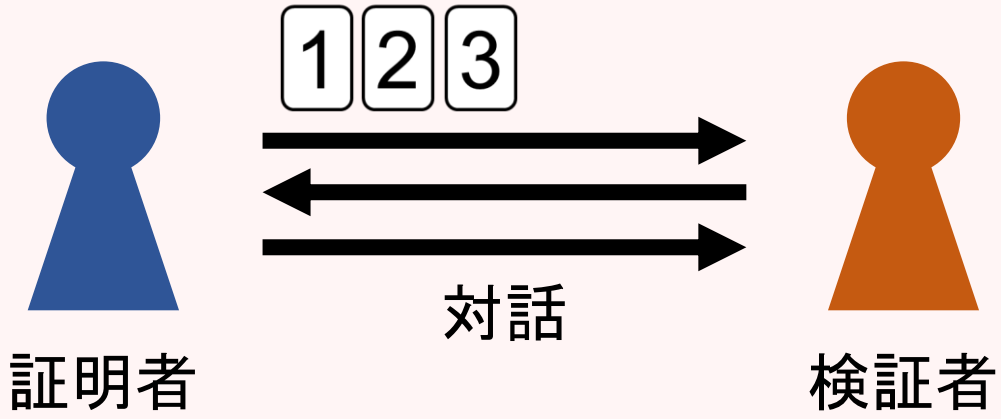
物理的ゼロ知識証明

与えられた命題が真であることを

- 通常のゼロ知識証明
  ⇒ 計算機を用いて示す



- 物理的ゼロ知識証明
  ⇒ 物理的な道具を用いて示す
  ◆ カードや封筒など

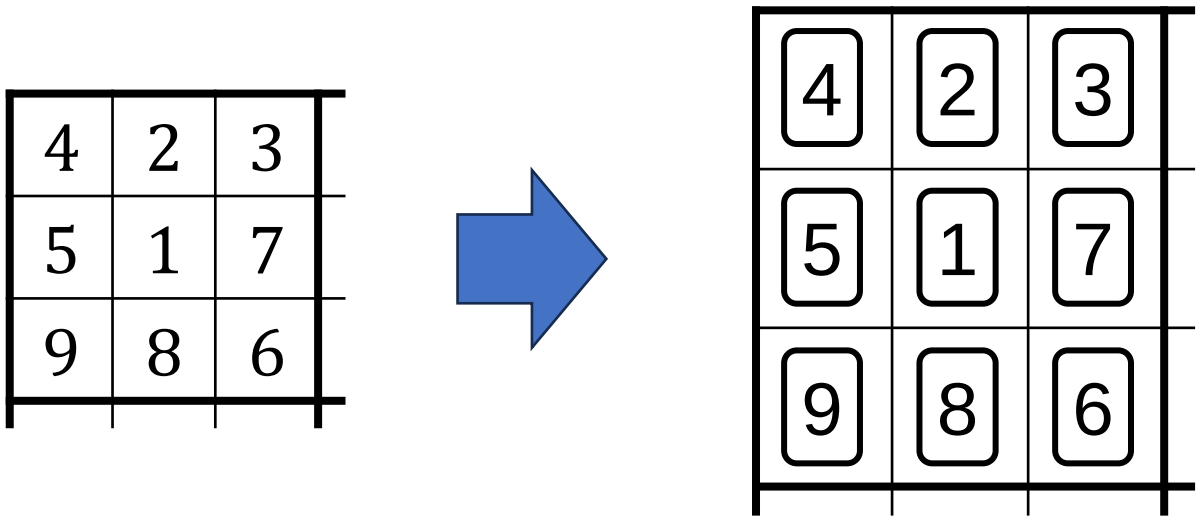


目次

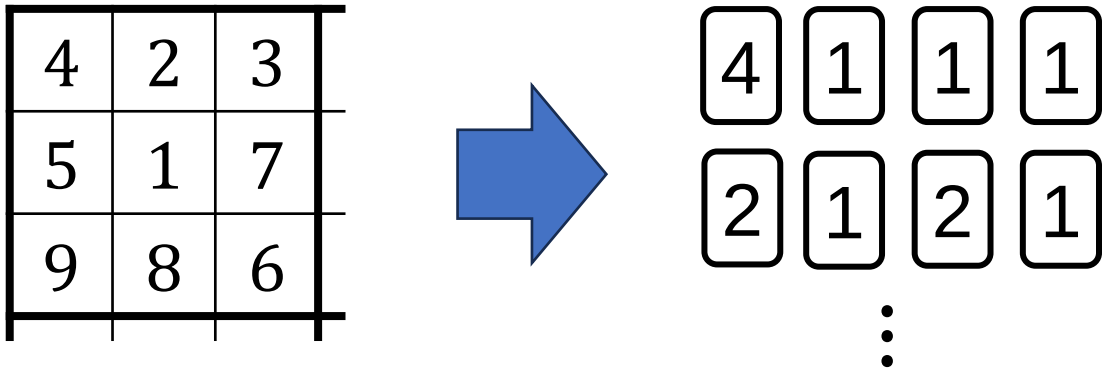
- 物理的ゼロ知識証明の背景
- 数独に対するゼロ知識証明の分類
  - Gradwholらの手法
  - 佐々木･品川の手法
- プロトコルの更なる効率化
  - 入力方法の再考
  - Onoらの手法
- 新しい証明手法のアイデア

数独に対する物理的ZKPの分類

- 解答そのものを数字カードで表現 [GNPR09, SMMS20, Rua22, TM23a,TM23b, HAWI23, ORA+24]



- 解答の数字が入る座標を数字カードで表現 [SS23, TM24]



数字の4：1行1列目1ブロックにある

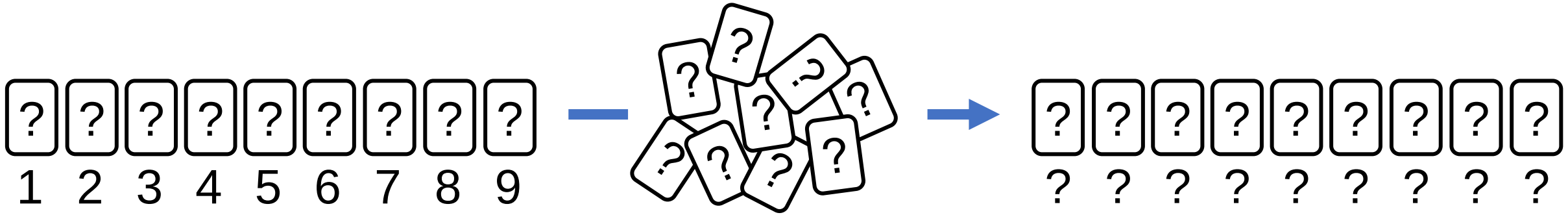
数字の2：1行2列目1ブロックにある

Gradwohl et al. の手法 [GNPR09 Protocol 3]

解答そのものを数字カードで表現

準備

- カード：[1]~[9] の数字カードを各27枚ずつ，計243枚
  - ◆同じ数字のカードは区別不可能
  - ◆全てのカードの裏面は [?] で区別不可能
- 操作：シャッフル
  - ◆カード列をランダマイズ

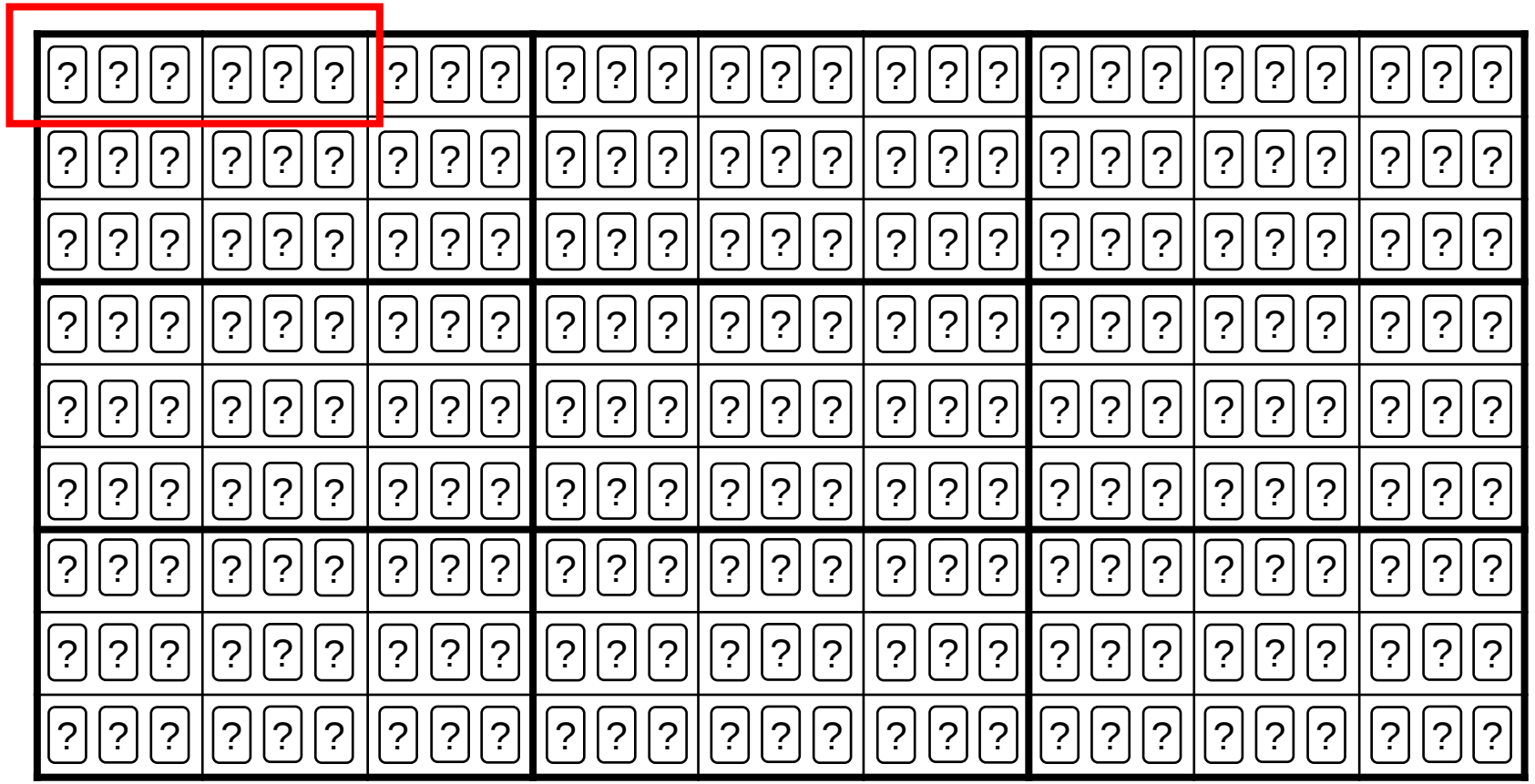


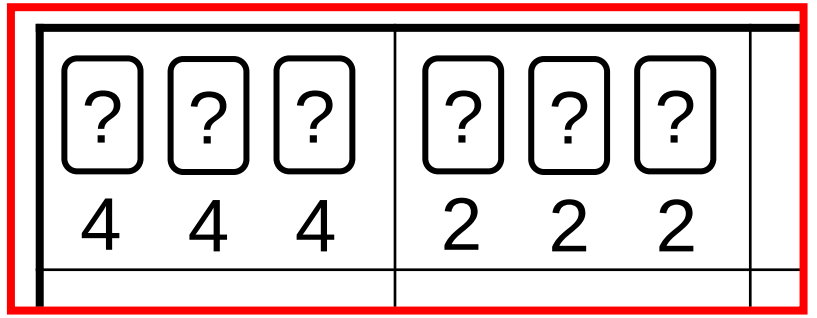
シャッフル

✓ 出力結果は誰にも分からない
◆ 操作した人にも

手順1/4：解答の配置

- 証明者は，各マスに対応する数字のカードを3枚ずつ裏向きで配置
  - 初めから数字が書かれているマスは一度表向きにしてから裏返す

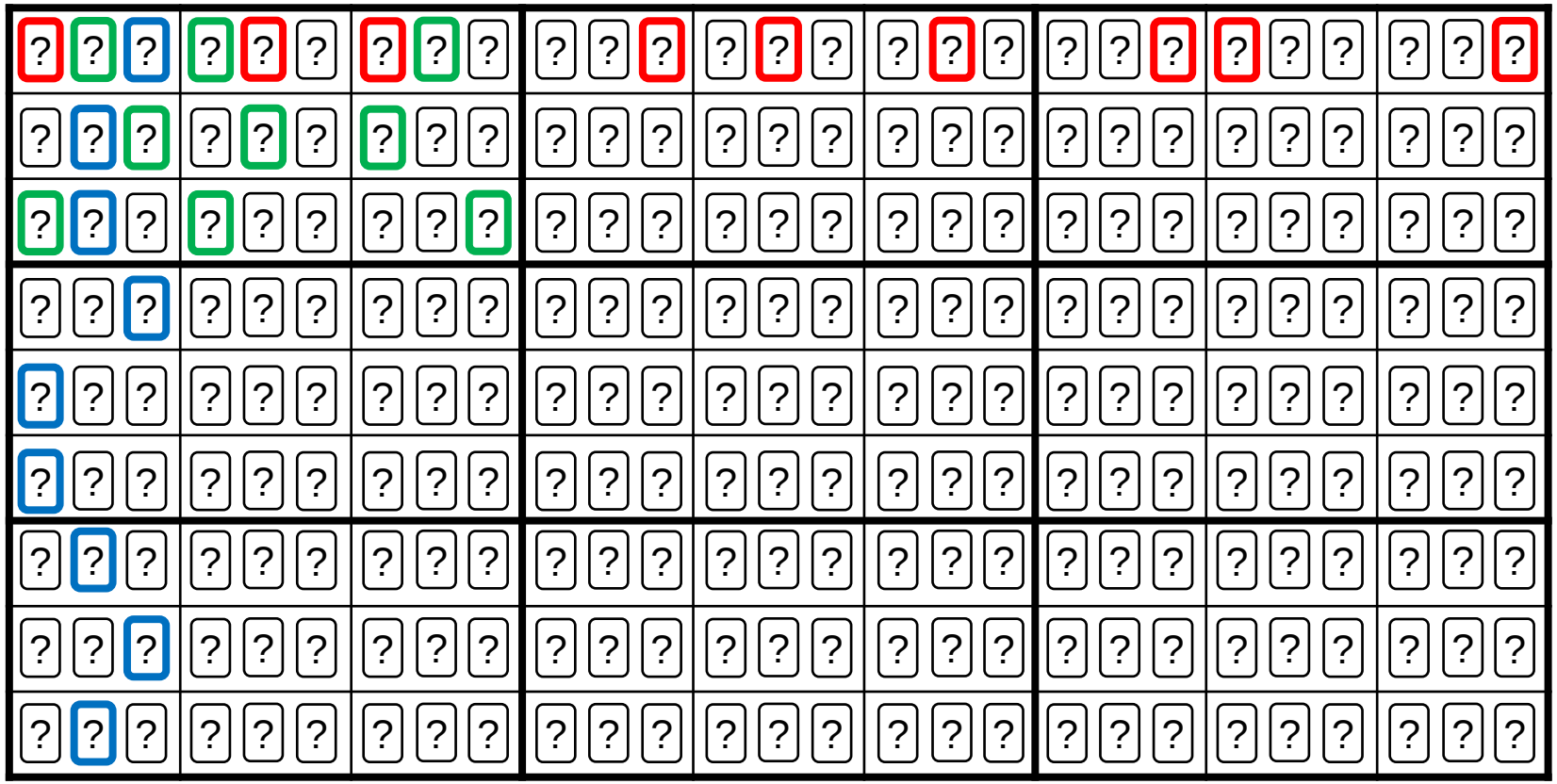




手順2/4：カード束作成

ランダムに

➢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
カード束を作る（計27束）



行のカード束 ×9

列のカード束 ×9

ブロックのカード束 ×9

手順3/4：シャッフル

➢各カード束をそれぞれシャッフル

行のカード束  ×9

列のカード束  ×9

ブロックのカード束  ×9

計27回シャッフル

手順4/4：解答条件の検証

a. 各カード束について，カードをめくり 1 ~ 9 が揃っているか確認

b. 全カード束で揃っていれば証明を受理，1つでも揃っていなければ拒否

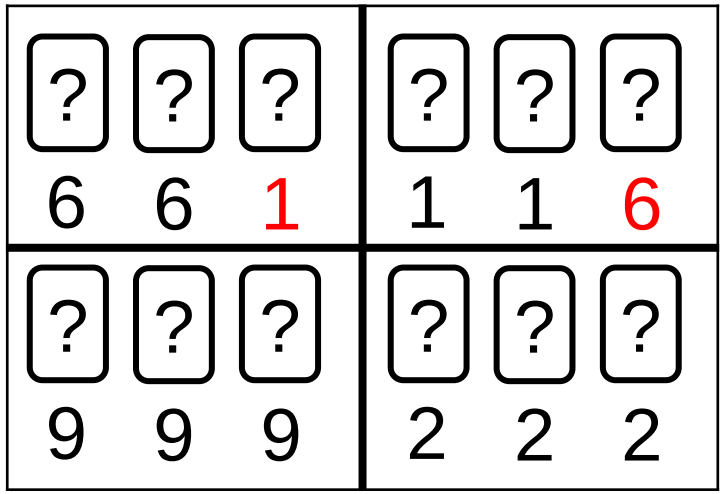
ZKPの条件の確認

➢完全性

◆解答を知っている証明者：解答条件を満たすようカードを配置可能
⇒ 手順4の解答条件の検証で拒否されることが無く，常に受理される

➢健全性

◆同じマスに違う数字のカードを置くという不正が可能
✓カード束作成時，辻褄が合う確率は高々 1/3×1/3
✓健全性誤り（不正な解答を受理する）確率は高々 1/9



➢ゼロ知識性

◆カードが配置された後，カードは常に裏面のまま
◆最後の手順4でカードをめくる際，各カード束には 1 ~ 9 が1枚ずつ含まれる
✓シャッフルによりその並び順は一様ランダム

✓解答を知らなくても分かる ⇒ 解答に関する情報は何も得られない

後続研究：健全性誤りが無いプロトコル

- [GNPR09]の健全性誤りの原因：同じマスに違う数字のカードを置ける
- 健全性誤りへの対策
  - ◆禁止：違う数字のカードを置けなくする
    - ✓各マス1枚配置後，コピープロトコルで各マス3枚ずつに複製
  - ◆回避：複数枚のカードを1つのマスに置かない
    - ✓行の検証 → カード配置の復元 → 列の検証 → カード配置の復元 → ブロックの検証

使用カード	禁止	回避
数字カード（1~nの数字）	[SMMS20 Protocol B]	[SMMS20 Protocol A]
UNO（1~nの数字× 4色）	–	[TM23a, TM23b]
二値カード（2色）	[HAWI23]	–
トランプ（1~54の数字）	–	[Rua22 Method A, B]

「UNO」はマテルの登録商標です。

効率の比較

SS：シャッフル
PSS：パイルスクランブルシャッフル

プロトコル	使用道具	操作	証明者の知識
[GNPR09 Protocol 3]	数字カード：$3n^2$ 枚	SS：$3n$ 回（合成⇒ 1回）	不要
[SMMS20 Protocol A]	数字カード：n^2+n 枚	PSS：$5n$ 回	不要
[SMMS20 Protocol B]	数字カード：$2n^2+n$ 枚	PSS：$2n$ 回 SS：$2n$ 回（合成⇒ 1回）	不要
[SMMS20 Protocol C]	数字カード：$3n^2$ 枚	PSS：1 回 SS：$3n$ 回（合成⇒ 1回）	必要
[Rua22 Method A]	トランプ：$n^2+n\sqrt{n}+n+\sqrt{n}$ 枚	PSS：$4n\sqrt{n}$ 回	必要
[Rua22 Method B]	トランプ：$n^2+2n+3\sqrt{n}$ 枚	PSS：$2n^2(\sqrt{n}-1)+2$ 回	必要
[TM23b]	UNO：$n^2+n\sqrt{n}+n$ 枚	PSS：$6\sqrt{n}-4$ 回 SS：$\sqrt{n}-1$ 回	不要
[TM23a]	UNO：n^2 枚 番号付きスリーブ：n^2 枚	(P)SS：7 回	不要

健全性誤り有

後述

効率の比較

SS：シャッフル
PSS：パイルスクランブルシャッフル

プロトコル	使用道具		操作	証明者の知識
[GNPR09 Protocol 3]	数字カード：	$3n^2$ 枚	SS： $3n$ 回（合成⇒ 1回）	不要
[SMMS20 Protocol A]	数字カード：	n^2+n 枚	PSS： $5n$ 回	不要
[SMMS20			PSS： $3n$ 回	不要
[SMMS20				必要
[Rua22 M				必要
[Rua22 M				必要
[TM23b]	UNO：	$n^2+n\sqrt{n}+n$ 枚	PSS： $6\sqrt{n}-4$ 回 SS： $\sqrt{n}-1$ 回	不要
[TM23a]	UNO： 番号付きスリーブ：	n^2 枚 n^2 枚	(P)SS： 7 回	不要

シャッフル回数：実行時間に影響

シャッフル回数をさらに減らせるか？

健全性誤り有

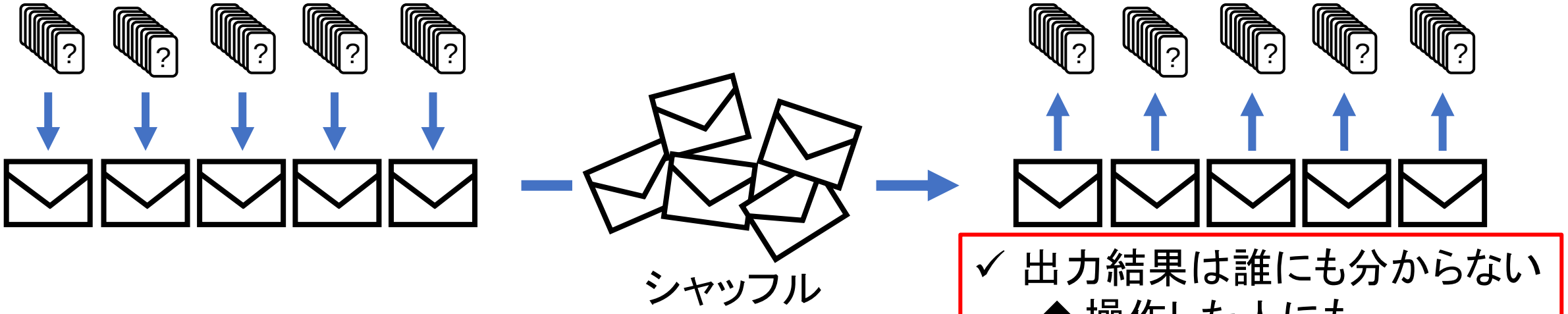
後述

佐々木･品川の手法 [SS23 プロトコル1]

解答の数字が入る座標を数字カードで表現

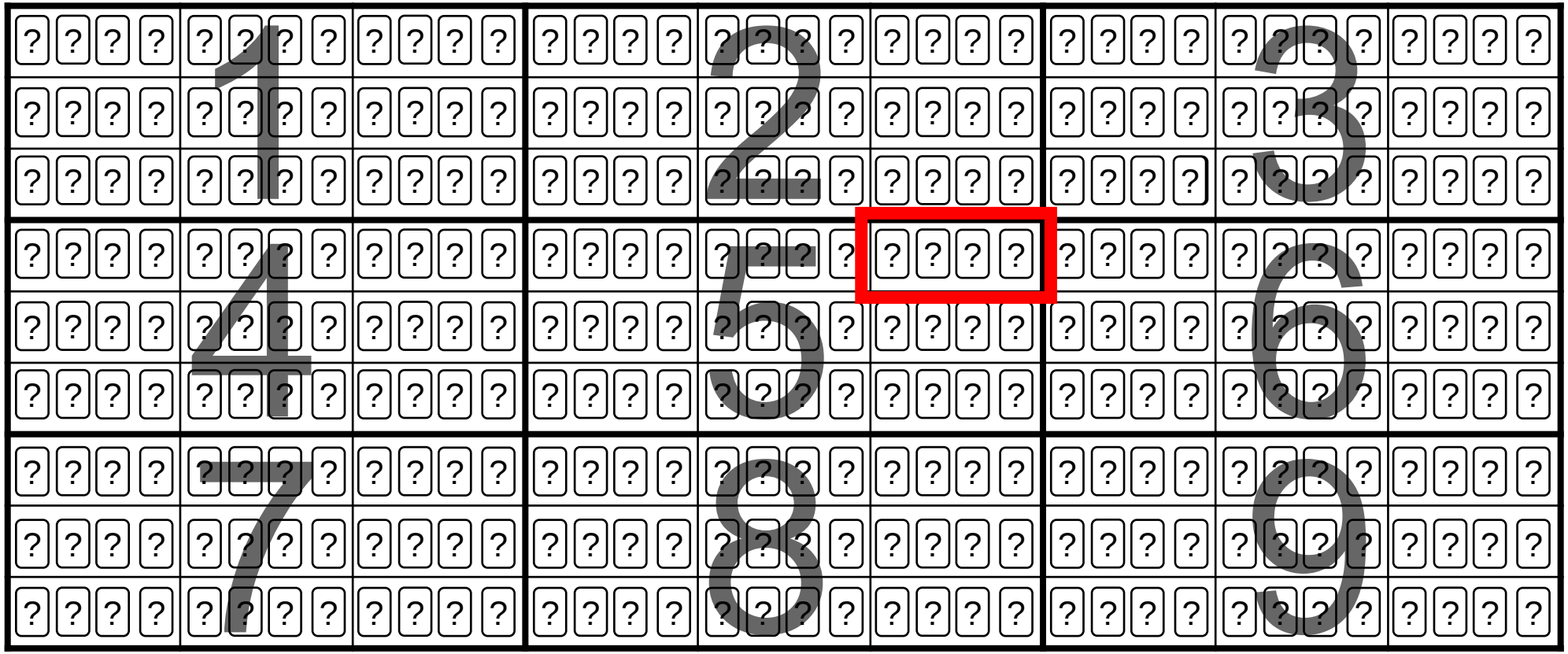
準備

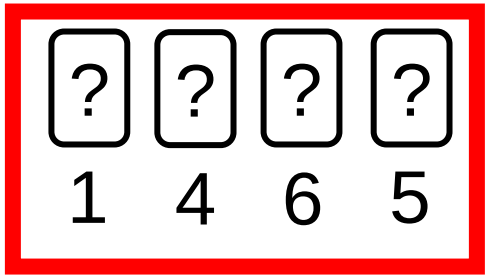
- カード：1 ~ 9 の数字カードを各36枚ずつ，計324枚
  - ◆同じ数字のカードは区別不可能
  - ◆全てのカードの裏面は ? で区別不可能
- 操作：パイルスクランブルシャッフル（Pile-Scramble Shuffle, PSS）
  - ◆カード束の列をランダマイズ
    - ✓カード束を封筒やスリーブに入れてシャッフル



手順1/4：カードの配置

1. 証明者は，各マスに対応する数字カードを1枚裏向きで配置
   ◆初めから数字が書かれているマスは一度表向きにしてから裏返す
2. 各マスのカードの右に，行・列・ブロックのindexを示すカードを配置



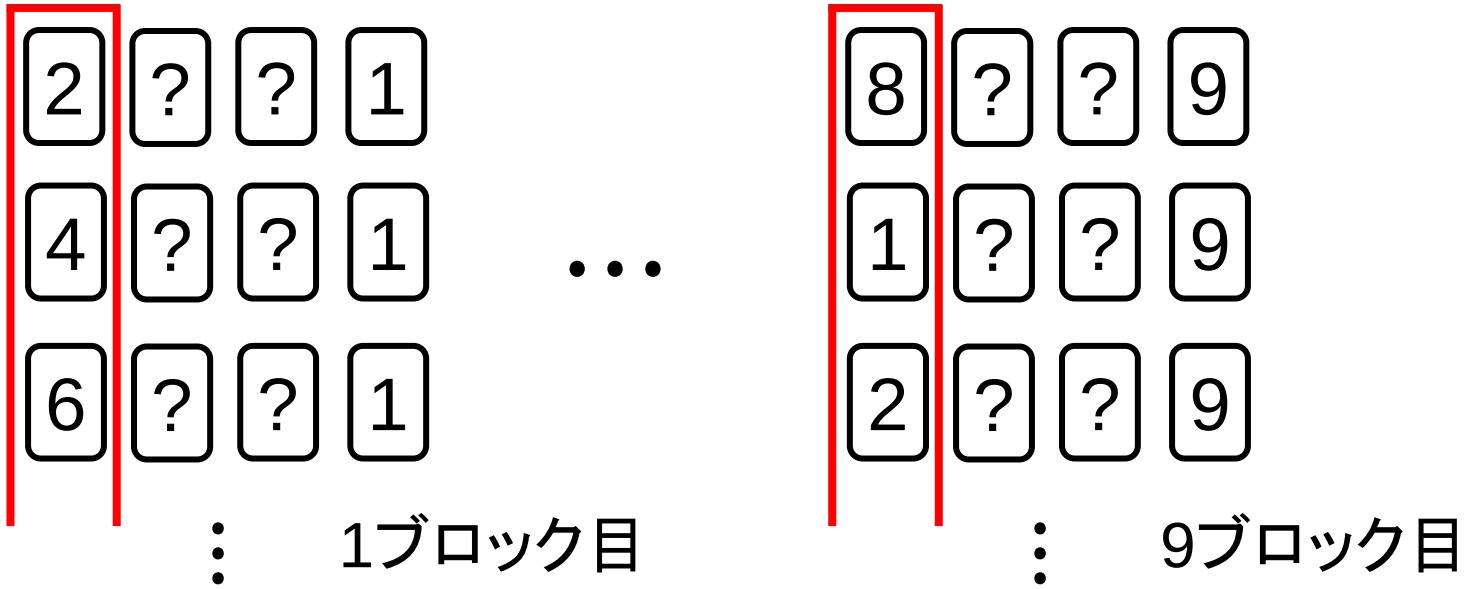


数字の1が
- 4行目
- 6列目
- 5ブロック目

にある

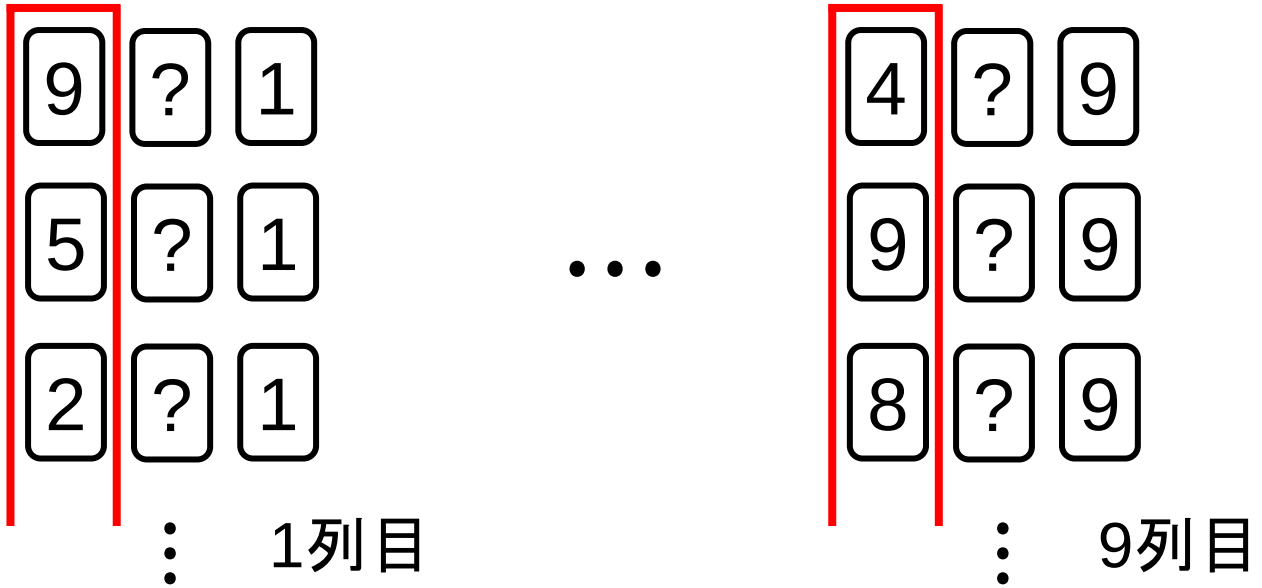
手順2/4：ブロックの検証

1. 各マスの4枚のカードを1束として，81個のカード束でPSSを実行
2. 右端のカードをめくり，同じブロックに属するカード束を集める
3. 左端のカードをめくり，同じブロック内に 1 ~ 9 が揃っているか確認
   ✓揃っていない束があれば証明を拒否 & プロトコル終了
4. 右端のカードを取り除く & 左端のカードを再度裏返す



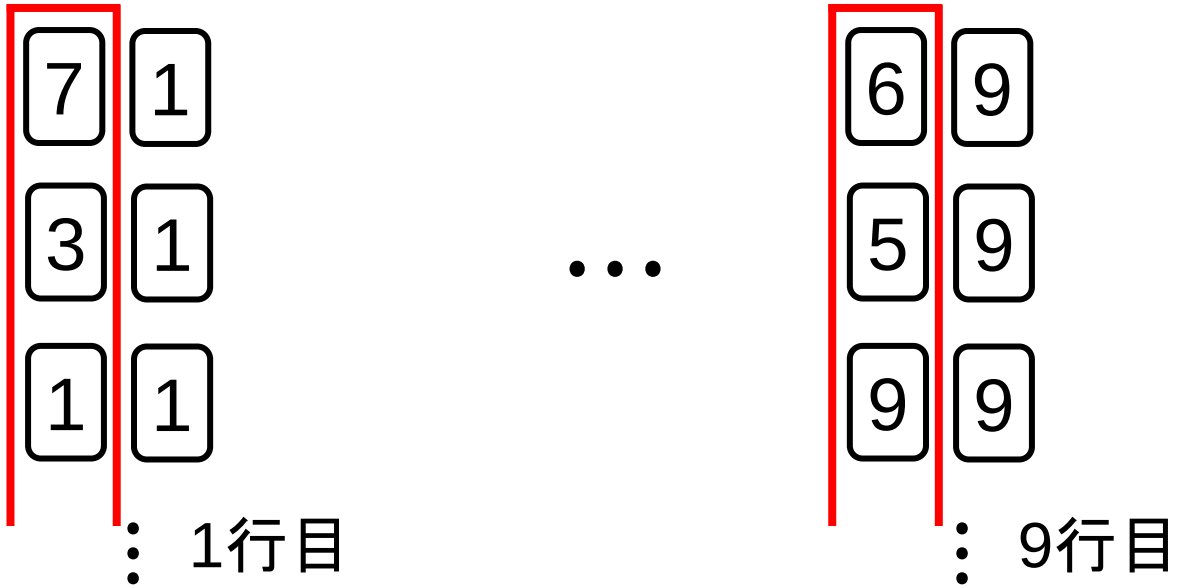
手順3/4：列の検証

1. 各マスの3枚のカードを1束として，81個のカード束でPSSを実行
2. 右端のカードをめくり，同じ列に属するカード束を集める
3. 左端のカードをめくり，同じ列内に 1 ~ 9 が揃っているか確認
   ✓揃っていない束があれば証明を拒否 & プロトコル終了
4. 右端のカードを取り除く & 左端のカードを再度裏返す



手順4/4：行の検証

1. 各マスの2枚のカードを1束として，81個のカード束でPSSを実行
2. 右端のカードをめくり，同じ行に属するカード束を集める
3. 左端のカードをめくり，同じ行内に 1 ~ 9 が揃っているか確認
   ✓揃っていない束があれば証明を拒否，全ての束で揃っていれば証明を受理



ZKPの条件の確認

- 完全性
  - ◆解答を知っている証明者：解答条件を満たすようカードを配置可能 ⇒ 常に受理
- 健全性
  - ◆「証明者が解答を知らない ⇒ 検証者は証明を拒否する」
    対偶
    ⟺「検証者が証明を受理する ⇒ 証明者は解答を知っている」
    - ✓検証者が証明を受理
      ⇒ 各行・列・ブロックに 1 ~ 9 が揃っている
      ⇒ そのようなカード配置を置ける証明者は解答を知っているに等しい
- ゼロ知識性
  - ◆各行・列・ブロックの検証でめくられる左端のカードは 1 ~ 9 が1枚ずつ
    - ✓シャッフルにより，その順番は一様ランダム
    - ✓解答を知らなくても分かる ⇒ 解答に関する情報は何も得られない

後続研究：シャッフル回数の削減

- [SS23]のシャッフル回数：3回（ブロック・列・行の各検証時）
- シャッフルをこれ以上減らせるか？
  - [TM24]：シャッフル（PSS）を2回に
    - ✓ブロックの検証 & 列と行の同時検証

プロトコル	使用道具	操作	証明者の知識
[TM23a]	UNO：n^2 枚 番号付きスリーブ：n^2 個	(P)SS：7 回	不要
[SS23 プロトコル 1]	数字カード：$4n^2$ 枚	PSS：3 回	不要
[SS23 プロトコル 2]	数字カード：$3n^2$ 枚 番号付きスリーブ：n^2 個	(P)SS：3 回	不要
[SS23 プロトコル 3]	数字カード：n^2 枚 番号付きスリーブ：$3n^2$ 個	(P)SS：3 回	不要
[TM24 プロトコルA]	UNO：n^2枚× 4色＝ $4n^2$ 枚	PSS：2 回	不要

目次

- 物理的ゼロ知識証明の背景
- 数独に対するゼロ知識証明の分類
  - Gradwholらの手法
  - 佐々木･品川の手法
- プロトコルの更なる効率化
  - 入力方法の再考
  - Onoらの手法
- 新しい証明手法のアイデア

シャッフル1回のプロトコルを目指して

「証明者の知識が必要」とは

プロトコル	使用道具	操作	証明者の知識
[SMMS20 Protocol A]	数字カード: n^2+n 枚	PSS: $5n$ 回	不要
[SMMS20 Protocol B]	数字カード: $2n^2+n$ 枚	PSS: $2n$ 回 SS: $2n$ 回（合成⇒ 1回）	不要
[SMMS20 Protocol C]	数字カード: $3n^2+n$ 枚	PSS: 1 回 SS: $3n$ 回（合成⇒ 1回）	必要
[Rua22 Method A]	トランプ: $n^2+n\sqrt{n}+n+\sqrt{n}$ 枚	PSS: $4n\sqrt{n}$ 回	必要
[Rua22 Method B]	トランプ: $n^2+2n+3\sqrt{n}$ 枚	PSS: $2n^2(\sqrt{n}-1)+2$ 回	必要

プロトコルの実行中に証明者が，検証者が知らない知識を用いて操作を行う

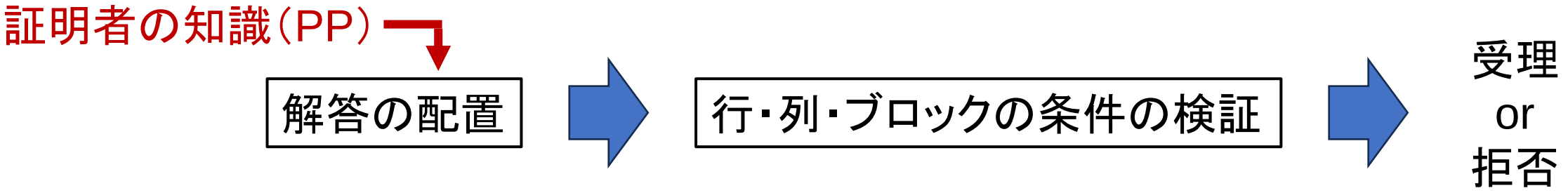
- 検証者に知識（情報）が漏れないよう秘密裏に操作する
  - ↳ 秘匿置換（Private Permutation, PP）

証明者の知識の利用方法

➢[SMMS20 Protocol C]

◆同じ数字カードが3枚重なっていることを確認した後，
その3枚をまとめた状態のまま解答に従いカードを配置

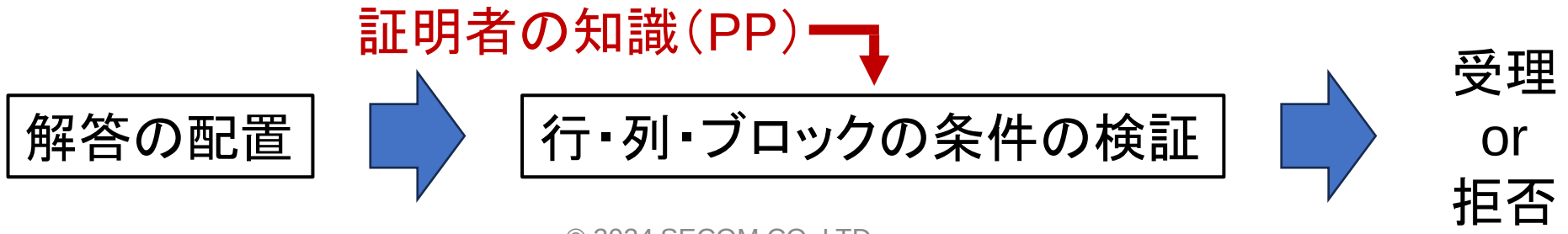
対話的に配置



➢[Rua22 Method A, B]

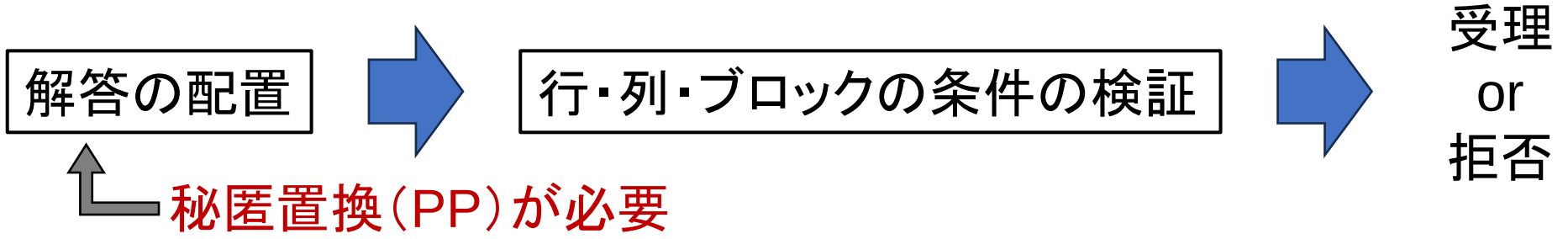
◆各行・列に，数字iのカード$(1 \leq i \leq n)$が1個だけ含まれていることを確認

✓秘匿置換でカード列を並べ替え → 数字iのカードの位置を指定



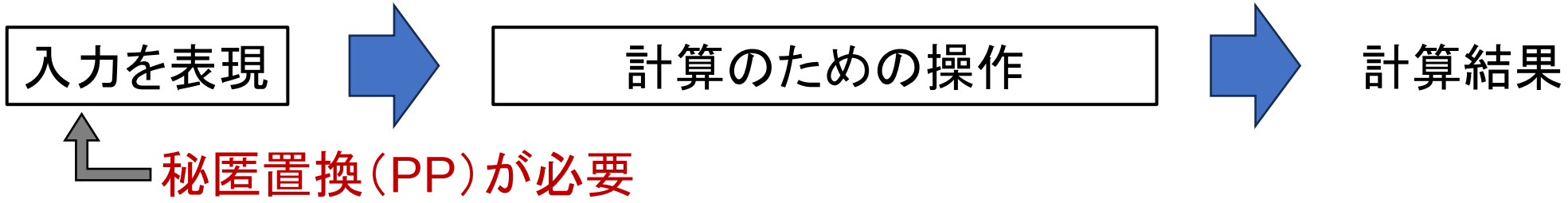
入力における秘匿置換の必要性

➢ゼロ知識証明



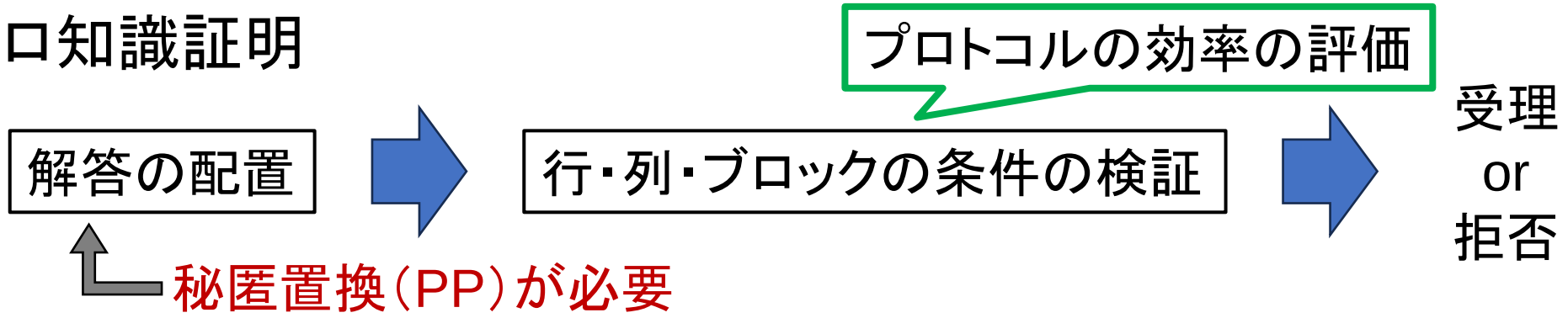
[SMMS20　Protocol C] と他のプロトコルの違い：入力が対話的か否か

cf. カードベース暗号（秘密計算）



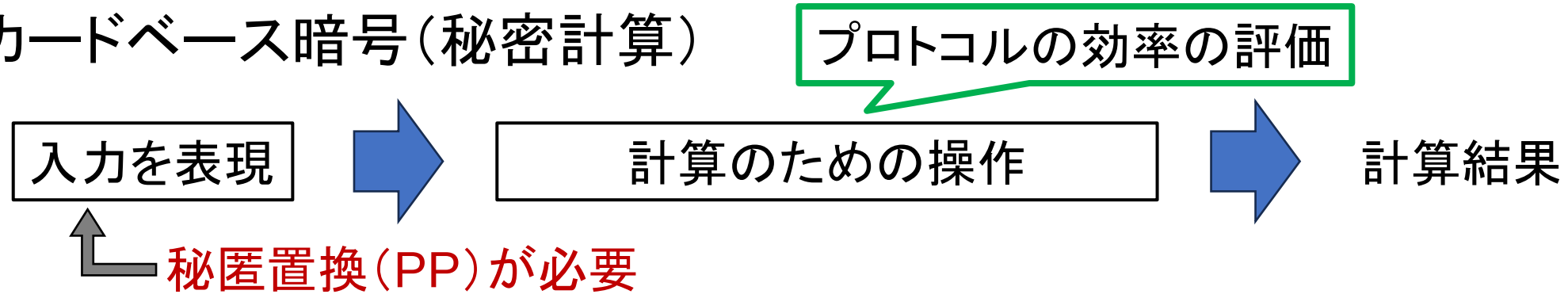
プロトコルの効率の考慮範囲

➢ゼロ知識証明



対話的な入力(解答の配置)を許す代わりに,
シャッフル回数削減を目指す

cf. カードベース暗号(秘密計算)



Ono et al. の手法 [ORA+24 Protocol 1]

対話的な入力の利用

アイデア

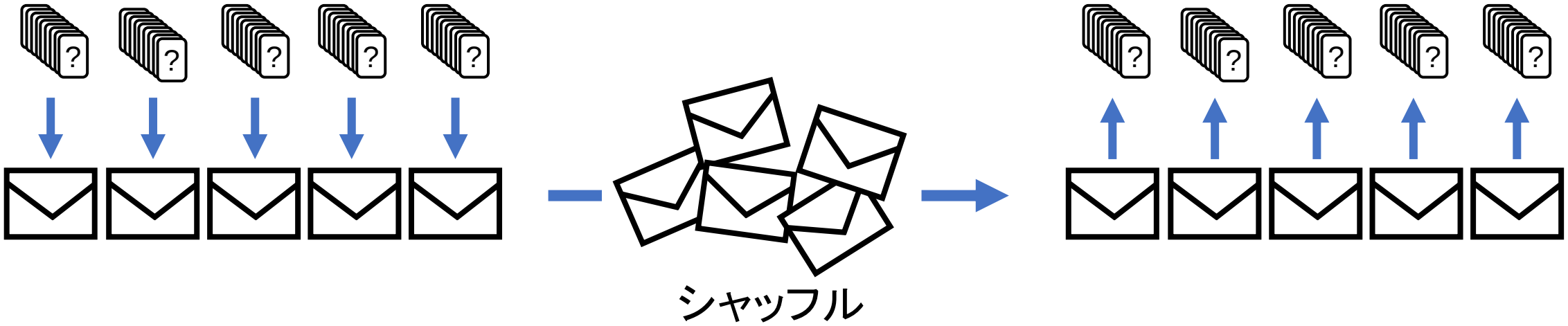
➢対話的な入力において，行と列の検証を済ませる

解答を重ねる手法での検証項目と検証のタイミング

検証項目	[SMMS20 Protocol C]	[ORA+24 Protocol 1]
同じ数字のカードが重なっていること	入力時	プロトコル内
各行で1~9が揃っていること	プロトコル内	入力時
各列で1~9が揃っていること	プロトコル内	入力時
各ブロックで1~9が揃っていること	プロトコル内	プロトコル内

準備

- カード：1 ~ 9 の数字カードを各18枚ずつ，計162枚
  - ◆同じ数字のカードは区別不可能
  - ◆全てのカードの裏面は ? で区別不可能
- 操作：パイルスクランブルシャッフル（PSS）



手順1/4：解答の配置（行）

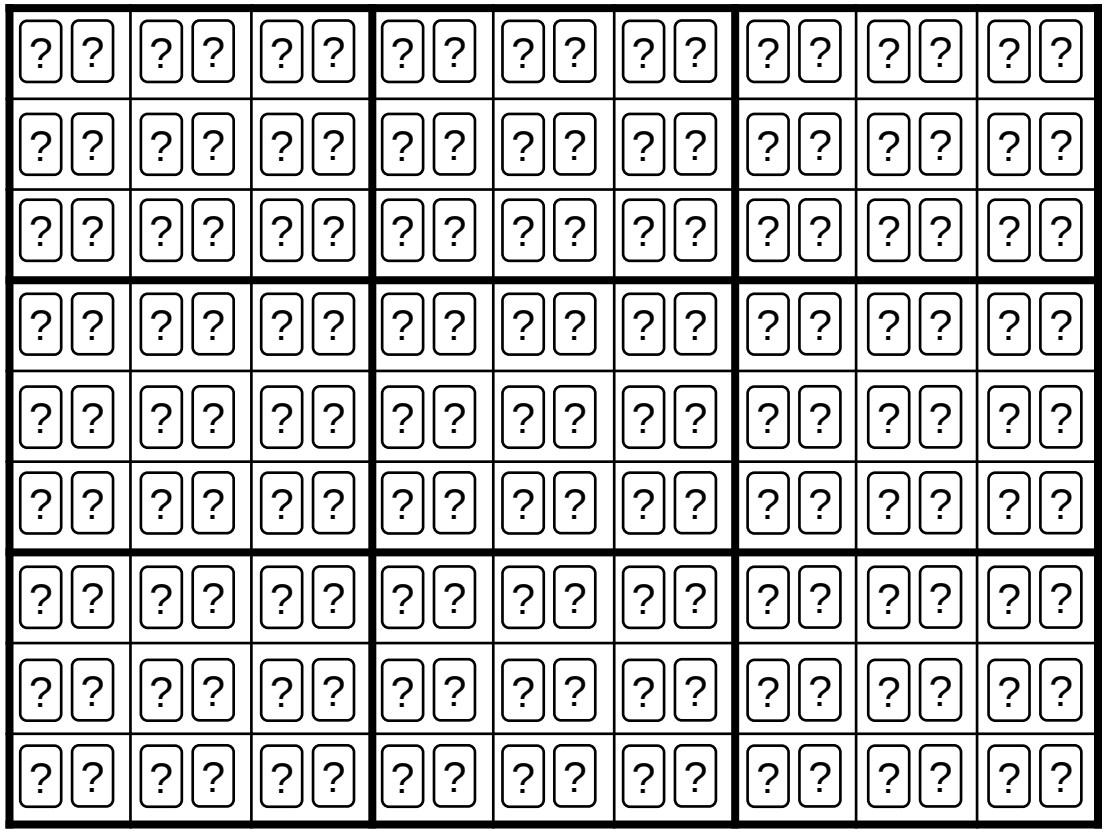
- 各行について以下を繰り返す
  1. 1 ~ 9 の数字が揃ったカード束を検証者の前で用意
  2. 各マスの左側に，対応する数字のカードを秘密裏に裏向きで配置する

?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?
?	?	?	?	?	?	?	?	?

秘匿置換は$n = 9$回

手順2/4：解答の配置（列）

- 各列について以下を繰り返す
  1. 1 ~ 9 の数字が揃ったカード束を検証者の前で用意
  2. 各マスの右側に，対応する数字のカードを秘密裏に裏向きで配置する

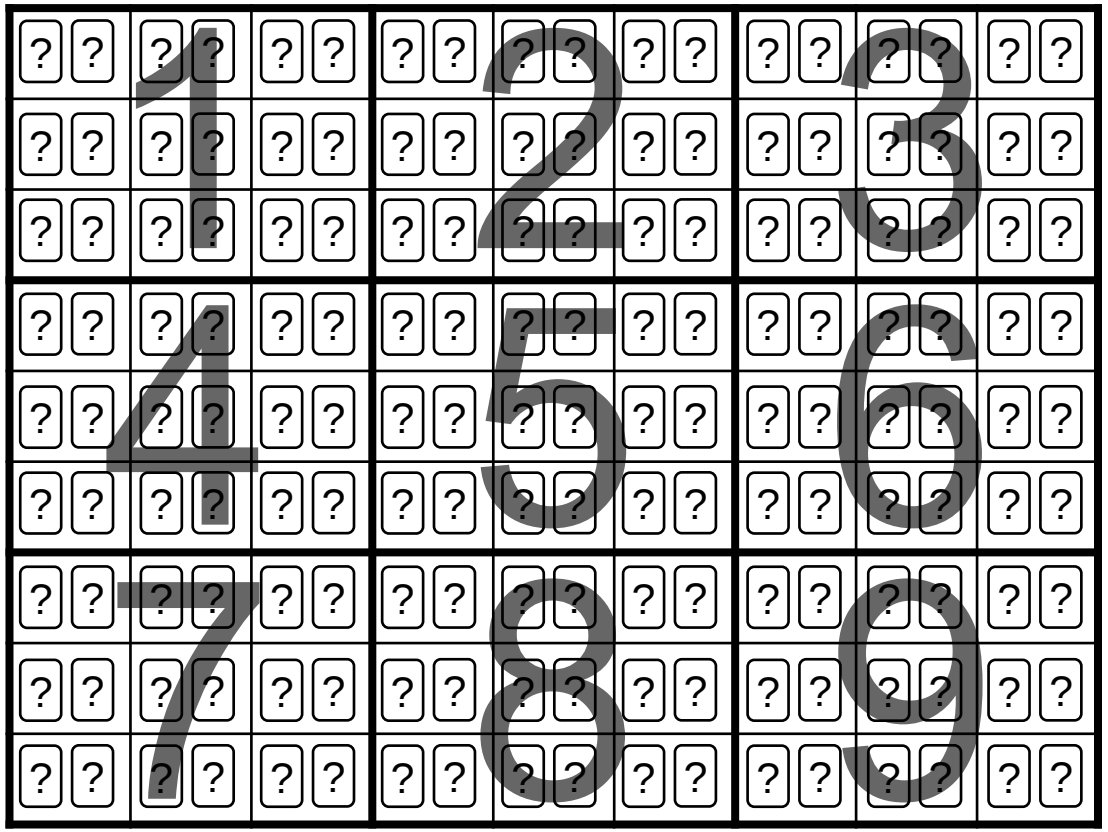


秘匿置換は$n = 9$回

手順1と合わせて
$2n = 18$回

手順3/4：シャッフル

- ブロック毎に，各マスの2枚のカードを1束としてPSS
  - 9回のPSS ⇒ 連続するシャッフルなので合成が可能
    - ✓合成後のシャッフル回数：1



手順4/4：ブロックの検証と一貫性の検証

1. 全てのカードをめくる
2. ブロックの検証：ブロック毎に[1]~[9]が揃っているか確認
   ✓揃っていないブロックがあれば証明を拒否
3. 一貫性の検証：各マスの2枚について，同じ数字のカードか確認
   ✓数字が異なるマスがあれば証明を拒否，全てのマスで数字が同じなら受理

ZKPの条件の確認

- 完全性
  - 解答を知っている証明者：解答条件を満たすようカードを配置可能 ⇒ 常に受理
- 健全性
  - 「証明者が解答を知らない ⇒ 検証者は証明を拒否する」
    対偶
    ⟺「検証者が証明を受理する ⇒ 証明者は解答を知っている」
    - ✓検証者が証明を受理
      ⇒ 各行・列・ブロックに 1 ~ 9 が揃っている
      ⇒ そのようなカード配置を置ける証明者は解答を知っているに等しい
- ゼロ知識性
  - ブロックの検証でめくられるカードは 1 ~ 9 が1束ずつ
    - ✓シャッフルにより，その順番は一様ランダム ⇒ 解答に関する情報は何も得られない

効率の比較

SS：シャッフル
PSS：パイルスクランブルシャッフル
PP：秘匿置換

プロトコル	使用道具	シャッフル回数	PP回数
[GNPR09 Protocol 3]	数字カード：$3n^2$ 枚	SS：$3n$ 回（合成⇒ 1回）	1 回
[SMMS20 Protocol C]	数字カード：$3n^2$ 枚	PSS：1 回 SS：$3n$ 回（合成⇒ 1回）	n^2 回
[TM23a]	UNO：n^2 枚 番号付きスリーブ：n^2 個	(P)SS：7 回	1 回
[SS23 プロトコル 3]	数字カード：n^2 枚 番号付きスリーブ：$3n^2$ 個	(P)SS：3 回	1 回
[TM24 プロトコルA]	UNO：n^2枚× 4色= $4n^2$ 枚	PSS：2 回	1 回
[ORA+24 プロトコル1]	数字カード：$2n^2$ 枚	PSS：n 回（合成⇒ 1回）	$2n$ 回
[ORA+24 プロトコル2]	UNO：n^2 枚× 2色= $2n^2$ 枚	PSS：n 回（合成⇒ 1回）	n 回
[ORA+24 プロトコル3]	UNO：$n\sqrt{n}$枚× $2\sqrt{n}$色= $2n^2$ 枚	PSS：n 回（合成⇒ 1回）	$\sqrt{n}$ 回

健全性誤り有

目次

- ➢物理的ゼロ知識証明の背景
- ➢数独に対するゼロ知識証明の分類
  - ◆Gradwholらの手法
  - ◆佐々木･品川の手法
- ➢プロトコルの更なる効率化
  - ◆入力方法の再考
  - ◆Onoらの手法
- ➢新しい証明手法のアイデア

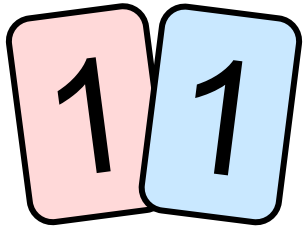
新たな物理的ZKPのアイデア

目標：カード＆シャッフルからの脱却

➢既存手法

◆使用する道具：カード

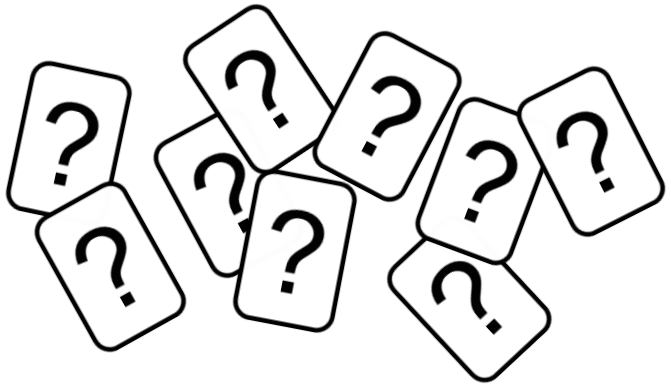
数字カード



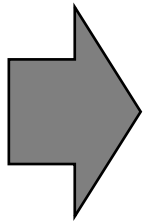
UNO

トランプ

◆手順：シャッフル ＆ 数字の確認

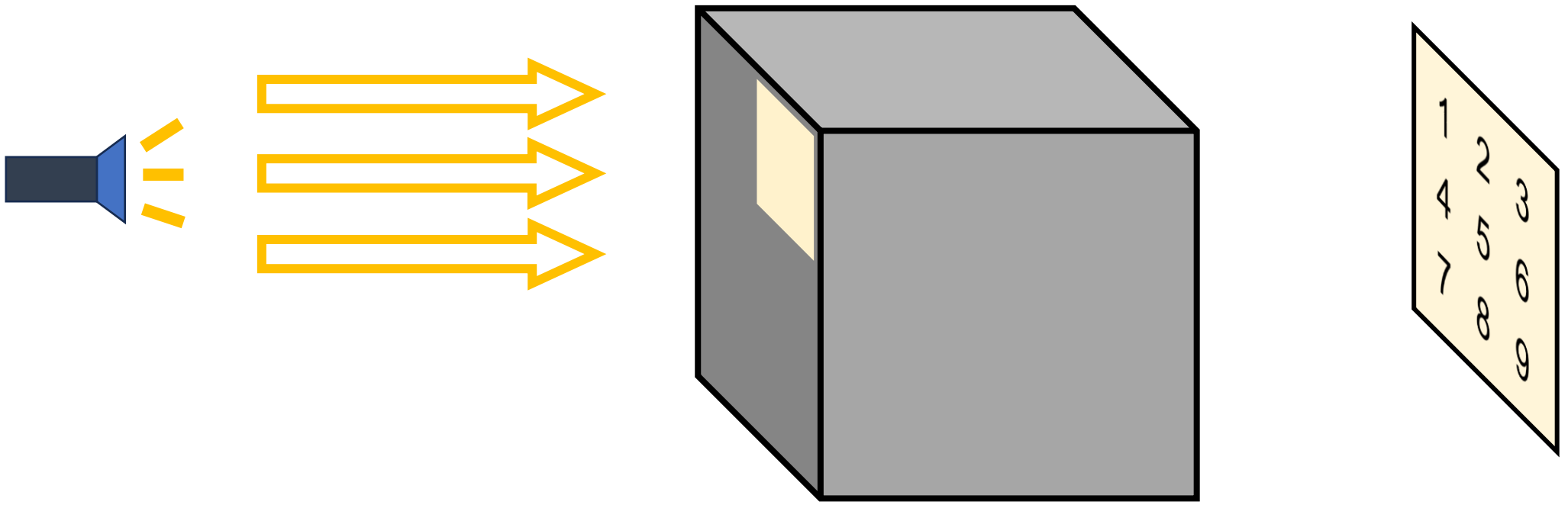


シャッフル



1~9が揃っているか確認

アイデア①：光ZKP

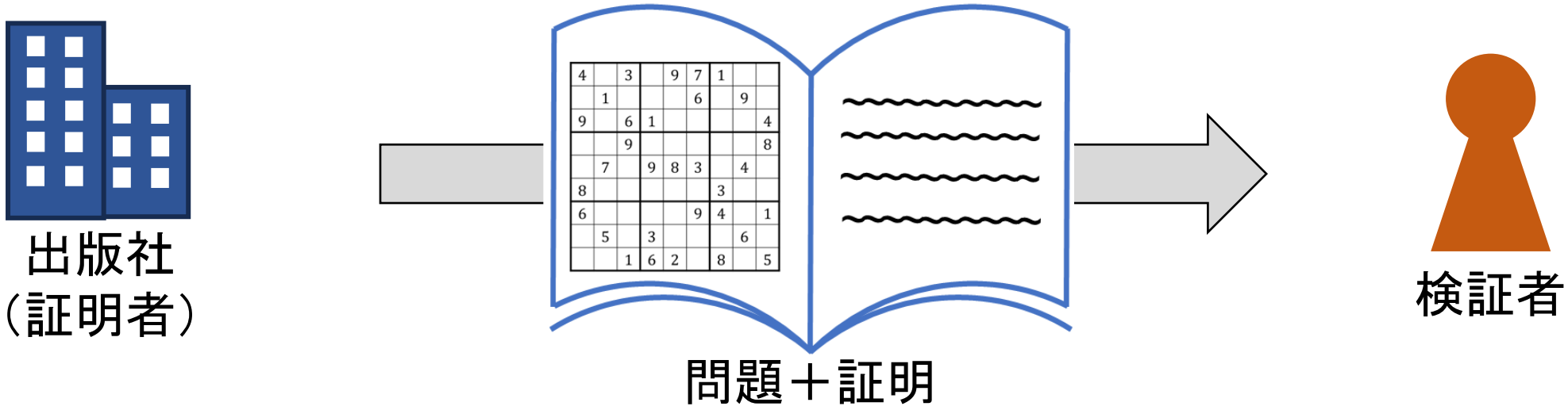


1~9が揃っている

⇒
- ✓ 1~9の数字が表れる
- ✓ 真っ白になる（↔対応する色が残る）
- etc.

- x軸方向：行の検証
- y軸方向：列の検証
- z軸方向：ブロックの検証

アイデア②：物理的NIZK



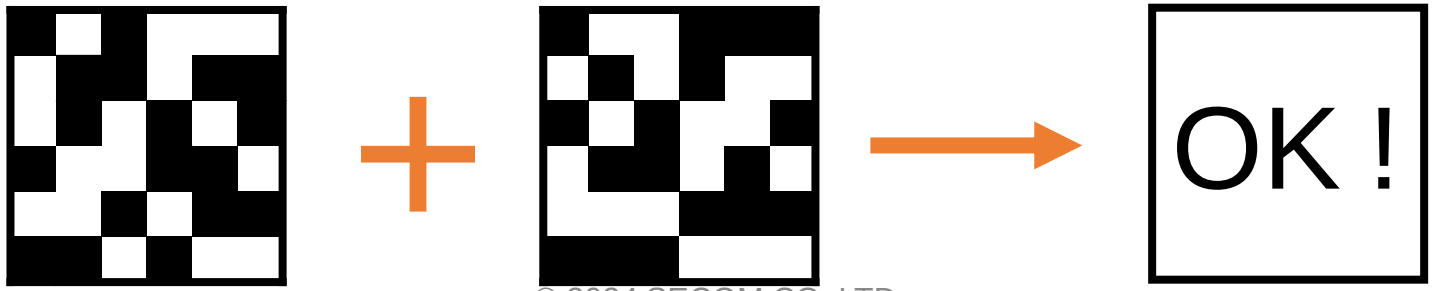
方針

完全性・健全性・ゼロ知識性を簡略化する代わりに非対話化・検証の軽量化

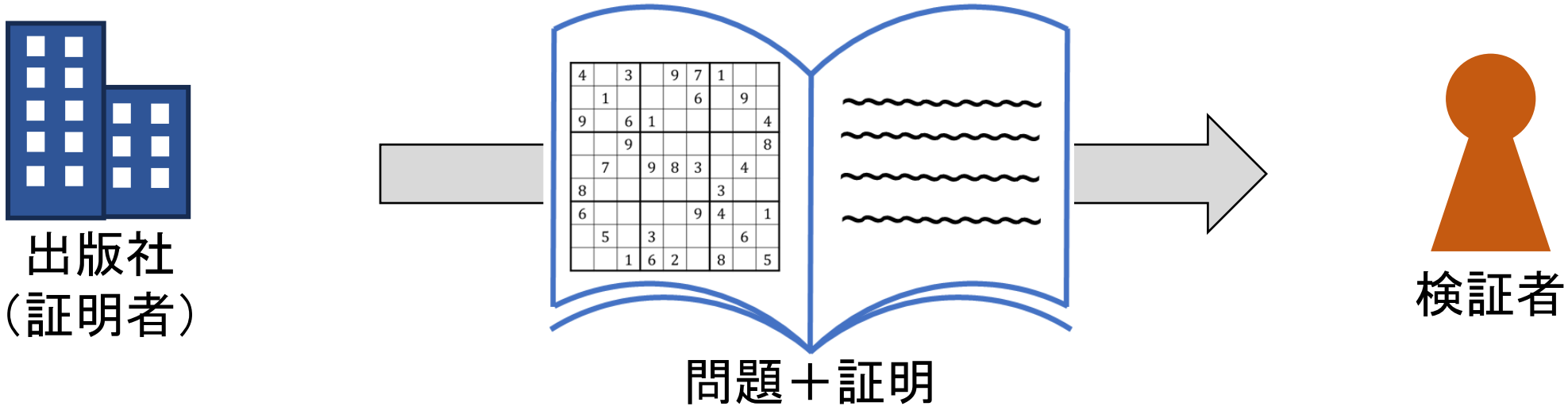
- 仮定：検証者の計算能力は極めて低い

  検証者は数独を簡単には解けない

  - ◆ 例：視覚型秘密分散のシェアを重ねる程度



アイデア②：物理的NIZK



方針

完全性・健全性・ゼロ知識性を簡略化する代わりに非対話化・検証の軽量化

- 仮定：検証者の計算能力は極めて低い

検証者は数独を簡単には解けない

  - ◆ 弱ゼロ知識性
    - ✓ 証明から情報を取り出すより，問題を解くほうが簡単なら良い
  - ◆ パズルを楽しみたい読者 ≒ honestな検証者
    - ✓ 完全にhonest ⇒ 既存のカードZKPでも良い

まとめ

- 数独に対する物理的ZKP
  - ◆解答そのものを数字カードで表現
    - ✓健全性誤り防ぐ手法
      - ●コピープロトコルで解答を複製
      - ●検証毎に解答を復元する
      - ●後でチェックする
  - ◆解答の数字が入る座標を数字カードで表現

- カード & シャッフルを使わない物理的ZKPのアイデア
  - ◆光ZKP
  - ◆物理的NIZK

参考文献

[GNPR09] R. Gradwohl, M. Naor, B. Pinkas, G. N. Rothblum, “Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles,” Theor. Comput. Syst., 2009.

[SMMS20] T. Sasaki, D. Miyahara, T. Mizuki, and H. Sone, “Efficient card-based zero-knowledge proof for Sudoku,” Theor. Comput. Sci., 2020.

[Rua22] S. Ruangwises, “Two Standard Decks of Playing Cards are Sufficient for a ZKP for Sudok,” New Gener.Comput. 2022.

[TM23a] 田中 滉大，水木 敬明，“番号付きスリーブを活用した数独のゼロ知識証明”，SCIS2023.

[TM23b] K. Tanaka, T. Mizuki, “Two UNO Decks Efficiently Perform Zero-Knowledge Proof for Sudoku,” FCT2023.

[HAWI23] 初貝 恭祐，安部 芳紀，渡邉 洋平，岩本 貢，“モジュラーデザインによる物理的ゼロ知識証明”，CSS2023.

[SS23] 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”，CSS2023.

[TM24] 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”，SCIS2024.

[ORA+24] T. Ono, S. Ruangwises, Y. Abe, K. Hatsugai, M. Iwamoto, “Single-Shuffle Physical Zero-Knowledge Proof for Sudoku Using Interactive Inputs”，2024年5月ISEC研究会.