月か太陽に対する
物理的ゼロ知識証明

電気通信大学　助教　宮原大輝

※「数独」「カックロ」「スリザーリンク」は株式会社ニコリの商標です
公開用のために、いくつかのパズルを消去しています

国立大学法人 電気通信大学

産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地

目次

去年の研究集会からの更新

- 4つの未解決問題を提示
  - ➢数独などに対するZKPプロトコルの進展を2つ紹介

未解決問題(1/4):数独

18

- Sasakiら[TCS20]、Ruangwises[NGCO22]、田中ら[SCIS23]によって必要な枚数・シャッフル数が改良された

著者	枚数	シャッフル数	必要なデッキ
Gradwohlら	243	27	トランプ27組
Sasakiら	90	45	トランプ9組
Ruangwises	120	322	トランプ2組
田中ら*	90	11	UNO2組

*シャッフルの実装に工夫あり

- 現実的な時間で実行可能になるためには？
- 他のパズルに対するZKPは効率化できるか？

未解決問題(2/4):他のペンシルパズル

19

- ZKPプロトコルが構成されていない(ニコリ社の)数字パズルは約25個

因子の部屋、ウソワン、お家へ帰ろう、カックロ、キンコンカン、クロット、黒どこ(黒マスはどこだ)、碁石ひろい、さしがね、さとがえり、サムライン、四角に切れ、シャカシャカ、縦横さん、推理パズル、数コロ、数独、ストストーン、スラローム、スリザーリンク、ダブルチョコ、チェンブロ、チョコバナナ、月か太陽[次の8月に発表]、ドッスンフワリ、ドッチループ、流れるループ、ナンスケ、ナンバーリンク、ぬりかべ、ぬりみさき、ぬりめいず、のりのり、波及効果、橋をかけろ、バッグ、美術館、ひとりにしてくれ、フィルオミノ、ふくめん算、へびいちご、へやわけ、ヘルゴルフ、ペンシルズ、マカロ、ましゅ、マックロ、ミッドループ、虫くい算、やじさんかずさん、ヤジリン、よせなべ、LITS

下線はZKPに関する発表がされていないパズル(宮原調べ)

* 数字のパズル一覧:https://www.nikoli.co.jp/ja/puzzles/

プロトコルの定式化における未解決課題

未解決問題(3/4):対話型 vs. 非対話型

22

- 効率性(必要なカード枚数・シャッフル回数・シャッフル操作の難易度)に差があるか研究する
- 複雑なパズルに対しては非対話型になりがち
- スリザーリンク[Lafourcadeら、ISPEC19]では、証明者が検証者と対話して盤面に1つのループを作る

- スリザーリンクに対するZKPを非対話型で構成できるか、つまり盤面に1つのループが存在することを非対話で(効率的に)検証できるのか、対話型よりも効率的なのか

未解決問題(4/4):計算機 vs. カードベース

23

- カードベース非対話型ZKPは定式化され[Miyaharaら、ProvSec21]、完全性・健全性・安全性(情報理論的安全性)を満たす
- 計算機ベース方式の安全性証明において用いられるrewindとの関係は十分に研究されていない
- 健全性の証明において悪意のある証明者ができる行動範囲も十分に議論されていない
- 計算機ベースにおける健全性・安全性との関係をどのように解釈していくのか今後の課題である

未解決問題(1/4):数独

- Sasakiら[TCS20]、Ruangwises[NGCO22]、田中ら[SCIS23]によって必要な枚数・シャッフル数が改良された

著者	枚数	シャッフル数	必要なデッキ
Gradwohlら	243	27	トランプ27組
Sasakiら	90	45	トランプ9組
Ruangwises	120	322	トランプ2組
田中ら	117	16	UNO2組

- 現実的な時間で実行可能になるためには？
- 他のパズルに対するZKPは効率化できるか？

未解決問題(1/4):数独における進展

崎山·李·宮原 研究室

- SCISなどの国内研究会において4つの研究が発表

著者	枚数	シャッフル数	必要なデッキ
Gradwohlら	243	27	トランプ27組
Sasakiら	90	45	トランプ9組
Ruangwises	120	322	トランプ2組
Tanakaら	117	16	UNO2組
佐々木ら	243	3	トランプ9組
田中ら	243	2	トランプ9組
小野ら*	162	1	トランプ3組

*入力の準備に工夫あり

- 未解決:入力工夫無しのシャッフル数1回プロトコル

未解決問題(2/4):他のペンシルパズル

崎山·李·宮原 研究室

- ZKPプロトコルが構成されていない(ニコリ社の)数字パズルは約25個

下線はZKPに関する発表がされていないパズル(宮原調べ)

因子の部屋、ウソワン、お家へ帰ろう、カックロ、キンコンカン、クロット、黒どこ(黒マスはどこだ)、碁石ひろい、さしがね、さとがえり、サムライン、四角に切れ、シャカシャカ、縦横さん、推理パズル、数コロ、数独、ストストーン、スラローム、スリザーリンク、ダブルチョコ、チェンブロ、チョコバナナ、月か太陽[HKL+23]、ドッスンフワリ、ドッチループ、流れるループ、ナンスケ、ナンバーリンク、ぬりかべ、ぬりみさき、ぬりめいず、のりのり、波及効果、橋をかけろ、バッグ、美術館、ひとりにしてくれ、フィルオミノ、ふくめん算、へびいちご、へやわけ、ヘルゴルフ、ペンシルズ、マカロ、ましゅ、マックロ、ミッドループ、虫くい算、やじさんかずさん、ヤジリン、よせなべ、LITS

- 近年注目を浴びたパズルへのZKPが構成された

数字のパズル一覧:https://www.nikoli.co.jp/ja/puzzles/

[HLL+23] S. Hand et al., Check Alternating Patterns: A Physical Zero-Knowledge Proof for Moon-or-Sun, IWSEC 2023

目次

物理暗号・カードベース暗号とは

- 日本が発信する特色ある分野
  - ➢最大級の暗号シンポジウムで5つセッションが設けられる
  - ➢AIセキュリティ・耐量子暗号に次ぐ3番目の多さ
- 海外からは、3つの機関から継続的に論文が輩出

最終日に1つ（合同）

2016年1月22日(金)		
	9:00-10:40	11:00-12:40
A会場	4A1 マルチパーティ計算	4A2 UC・カードプロトコル
B会場	4B1 マルウェア対策	4B2 ネットワーク攻撃検知(2)
C会場	4C1 生体認証(2)	4C2 システムセキュリティ
D会場	4D1 楕円曲線暗号(2)	4D2 楕円曲線暗号(3)
E会場	4E1 暗号理論(2)	4E2 暗号理論(3)
F会場	4F1 自動車セキュリティ(4)	4F2 自動車セキュリティ(5)

8年後

終日占拠

2024年1月25日(木)					
	9:00-10:20	10:40-12:00	13:10-14:30	14:50-16:30	16:50-18:10
A会場	3A1 耐量子暗号(3)	3A2 耐量子暗号(4)	3A3 耐量子暗号(5)	3A4 耐量子暗号(6)	3A5 公開鍵暗号
B会場	3B1 ブロックチェーン(2)	3B2 暗号プロトコル(2)	3B3 バイオメトリクス(2)	3B4 ブロックチェーン(3)	3B5 デジタルアイデンティティ・認証(2)
C会場	3C1 ID ベース暗号・属性ベース暗号・関数暗号	3C2 高機能暗号(3)	3C3 共通鍵暗号(3)	3C4 共通鍵暗号(4)	3C5 共通鍵暗号(5)
D会場	3D1 カードベース暗号・物理暗号(1)	3D2 カードベース暗号・物理暗号(2)	3D3 カードベース暗号・物理暗号(3)	3D4 カードベース暗号・物理暗号(4)	3D5 カードベース暗号・物理暗号(5)
E会場	3E1 自動車セキュリティ(3)	3E2 自動車セキュリティ(4)	3E3 IoTセキュリティ(3)	3E4 制御システムセキュリティ(1)	3E5 制御システムセキュリティ(2)
	3F1 AIセキュリティ	3F2 AIセキュリティ(4)	3F3 ネットワークセキュリティ(1)	3F4 ネットワークセキュリティ(2)	3F5 ネットワークセキュリティ(3)

SCIS webサイトより

本研究：パズルの物理ゼロ知識証明

- PはパズルのVに納得させたい

P

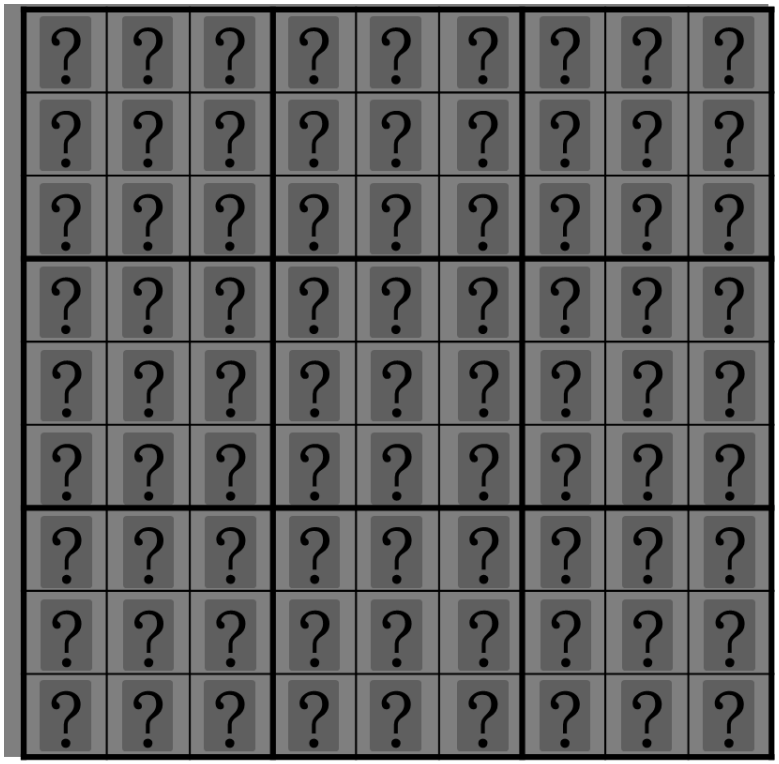
		1			5	6	7	
	2				4	8		
6	7							
3				5				
				4			1	8
					8	2		9
					2	4		
	9	2			7		8	3
	6		1					2

数独パズル

V

数独を機に研究が広まっている

- カード組を用いてゼロ知識証明（ZKP）を実現[SMMS20]
- 日本発信の研究で日本のプレゼンス向上に繋げる



初学者
向け教育

導入の
きっかけ

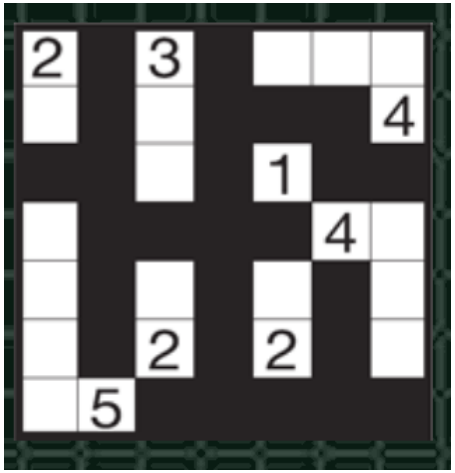
日本発信

[SMMS20] Tatsuya Sasaki, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone, “Efficient Card-Based Zero-Knowledge Proof for Sudoku,” Theoretical Computer Science, Elsevier, vol.839, pp.135–142, 2020

研究目的：数字から図形へ

- 数字に関するパズルは多く取り組まれている
  - 数独[GNPR09,SMMS20]、カックロ[BDDL16,MSMS19]、マカロ[BDD+18]など
  - カードベース暗号に関する研究をそのまま応用できる
- 図形の性質の証明は比較的複雑
  - スリザーリンク：1つの輪であること
  - ぬりかべ：ひとつながりになっていること（分断禁）

ニコリWeb
サイトより



スリザーリンク[LMM+21]

ぬりかべ[RML+22]

貢献:「月か太陽」に対するZKP

崎山・李・宮原 研究室

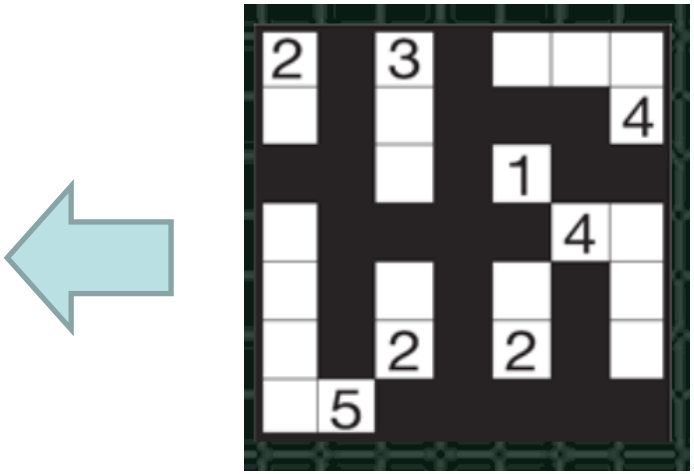
- 「月か太陽」を扱う(NP完全[II22])
- 比較的複雑なルールを検証
  - 1つの輪であること(今日の内容)
  - 部屋ごとに異なる図形を通ること[HLL+23]

ニコリWeb
サイトより

[II22] Chuzo Iwamoto and Tatsuya Ide, Moon-or-Sun, Nagareru, and Nurimeizu are NP-complete, IEICE Trans. Fundamentals, 2022
[HLL+23] S. Hand et al., Check Alternating Patterns: A Physical Zero-Knowledge Proof for Moon-or-Sun, IWSEC 2023

貢献：1つの輪検証の効率化

- 「月か太陽」に対するZKPを構成、効率化
  - ➢既存方式[LMM+21]の非効率な手順を指摘
  - ➢一つながりの検証[RML+22]を応用
- 手順（シャッフル回数）を半分にまで削減



スリザーリンク[LMM+21]　　ぬりかべ[RML+22]

[LMM+21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone, How to Construct Physical Zero-Knowledge Proofs for Puzzles with a “Single Loop” Condition, TCS 2021

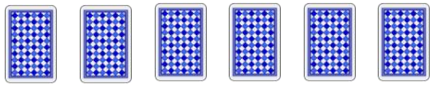
目次

カードと値の符号化

崎山·李·宮原 研究室

- 黒と赤の2色カード組を使用

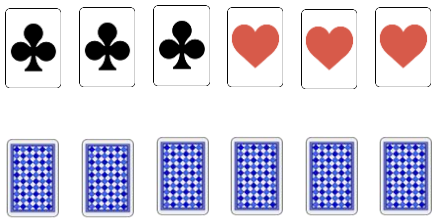
Front

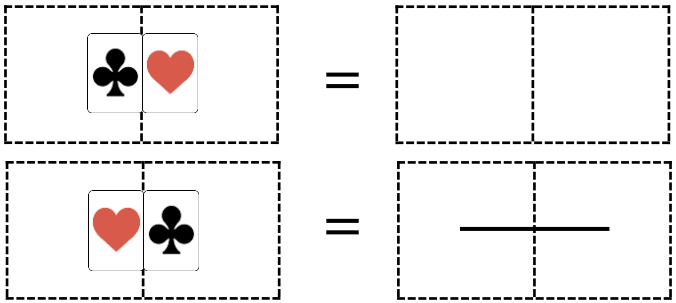


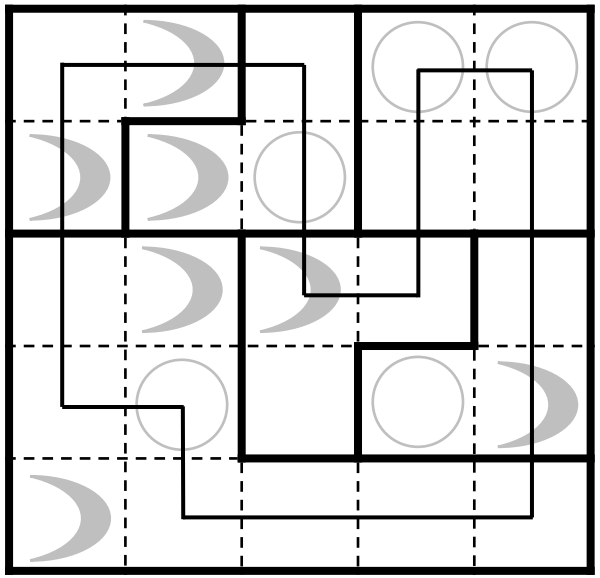
Back

カードと値の符号化

- 黒と赤の2色カード組を使用
- 2つのセルの間の線の存在を、2枚のカードで符号化

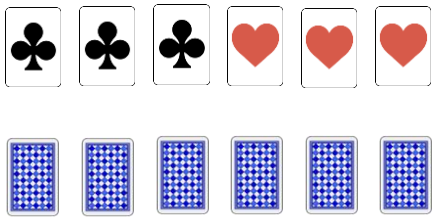


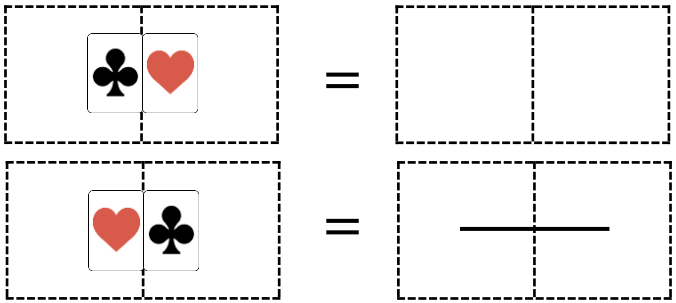


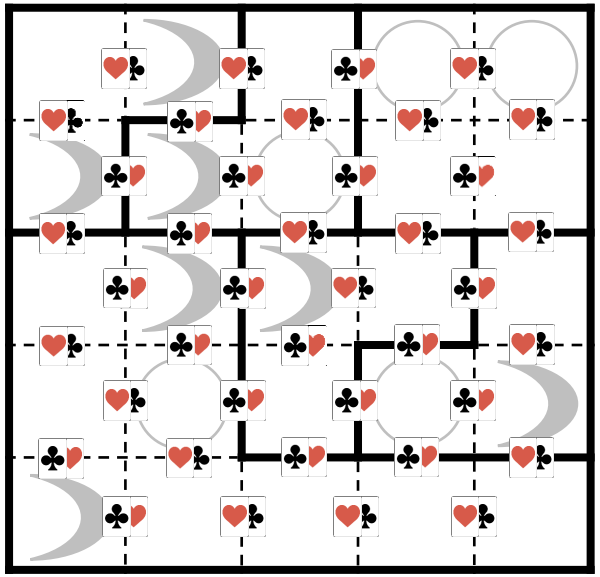


カードと値の符号化

- 黒と赤の2色カード組を使用
- 2つのセルの間の線の存在を、2枚のカードで符号化

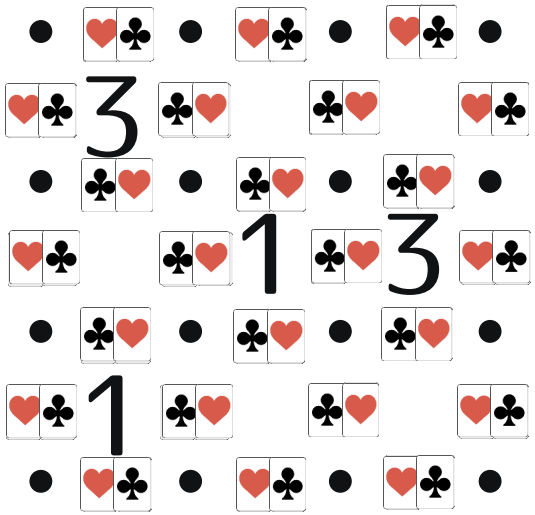






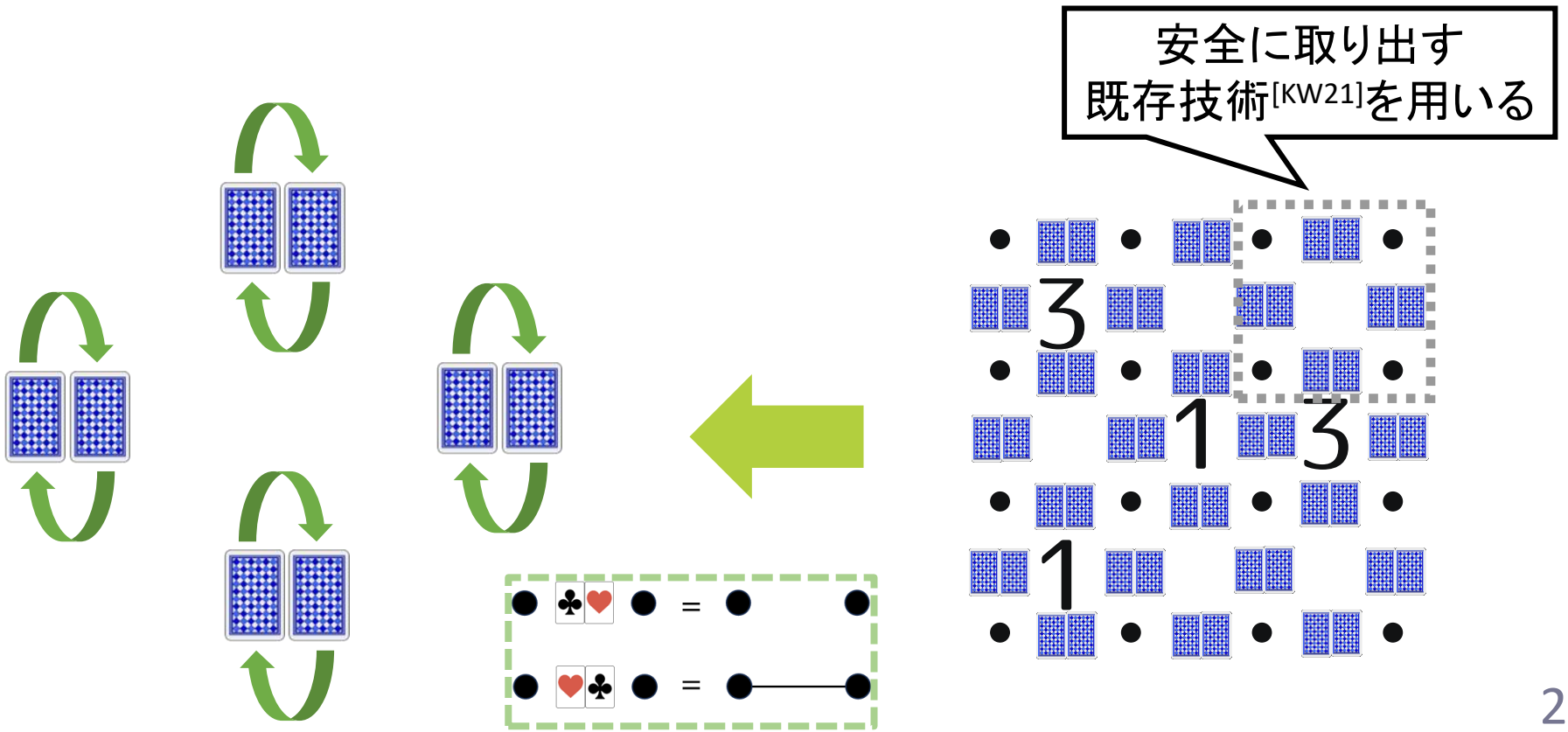
スリザーリンクに対する既存ZKP

- 基本アイデア：Pに解を安全に「作らせる」
- セットアップ：盤面サイズのループを表すカードを置く



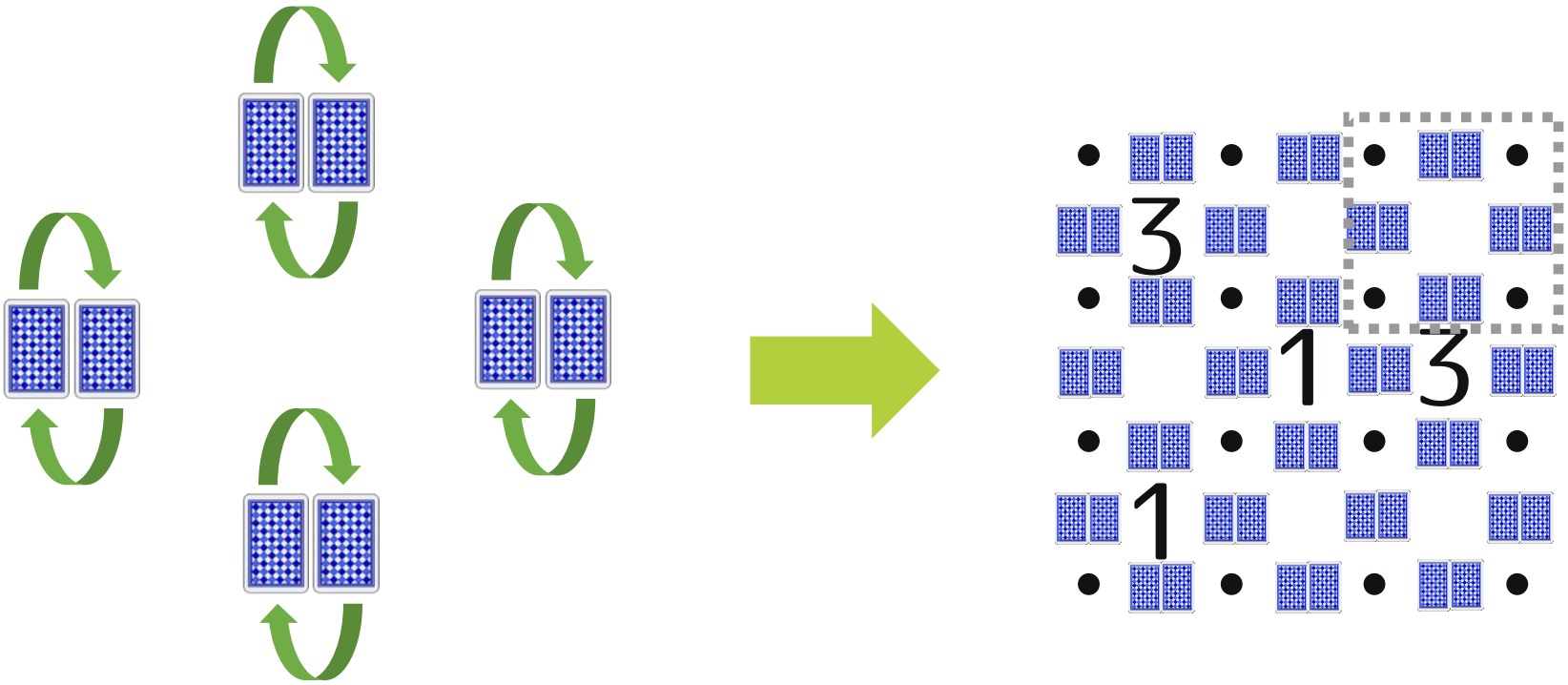
スリザーリンクに対する既存ZKP

- 基本アイデア：Pに解を安全に「作らせる」
- セットアップ：盤面サイズのループを表すカードを置く
- 作成フェーズ：Pにループを安全に「凹ませる」



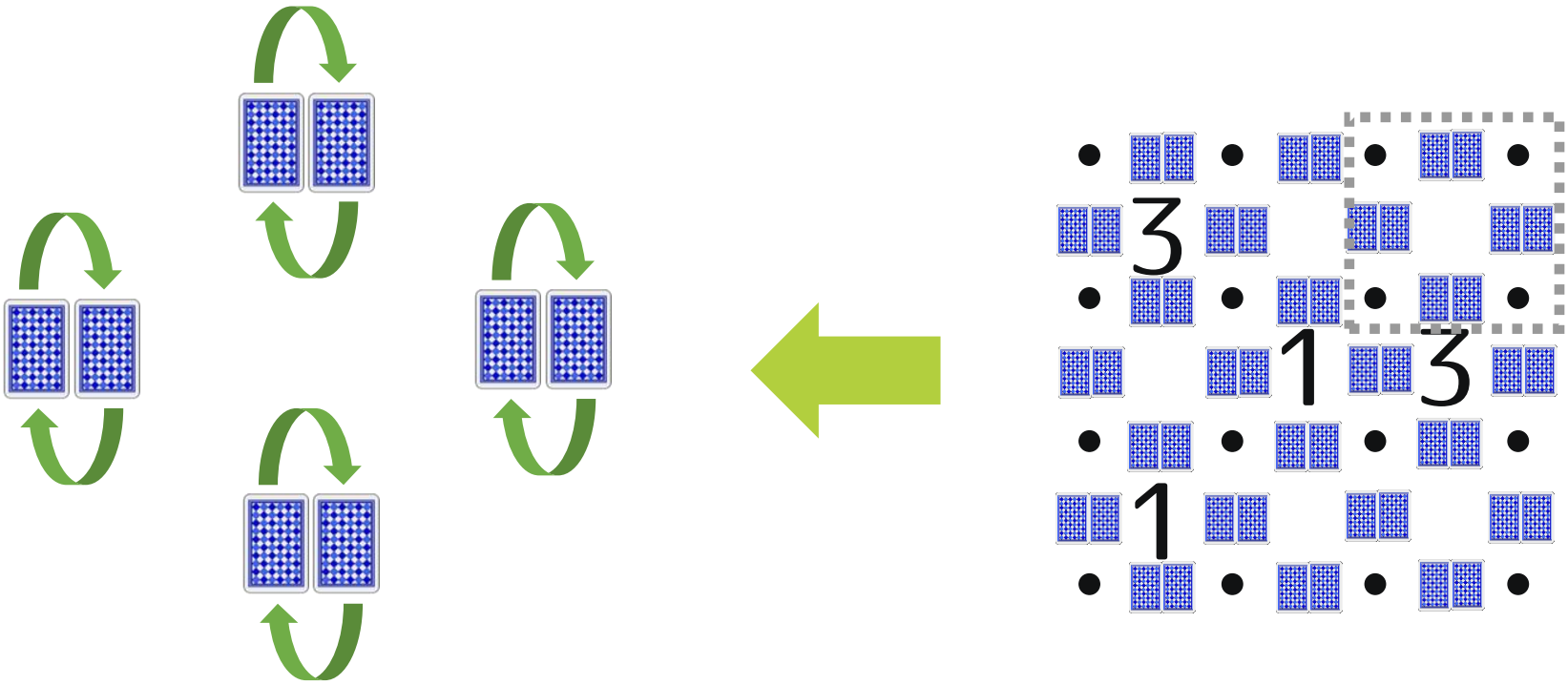
スリザーリンクに対する既存ZKP

- 基本アイデア：Pに解を安全に「作らせる」
- セットアップ：盤面サイズのループを表すカードを置く
- 作成フェーズ：Pにループを安全に「凹ませる」
  - ➢解を知っているPは一連の手順を繰り返せば良い

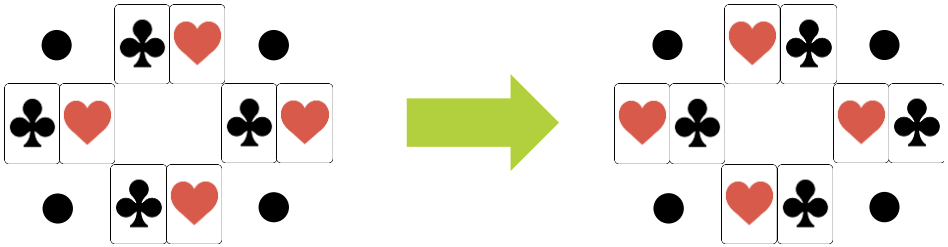


既存ZKPの欠点

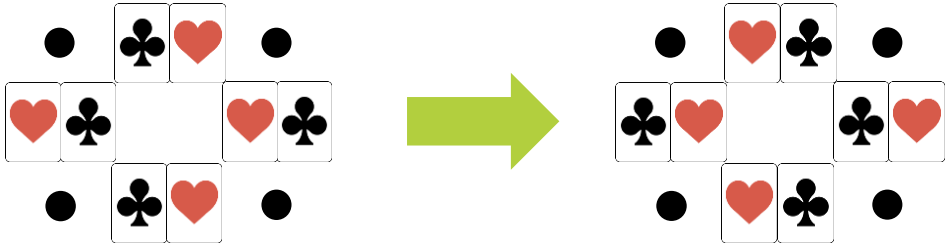
- 凹み前後に追加検証が必要
  - Pが選んだ4点の間に線が存在すること（シャッフル2回）

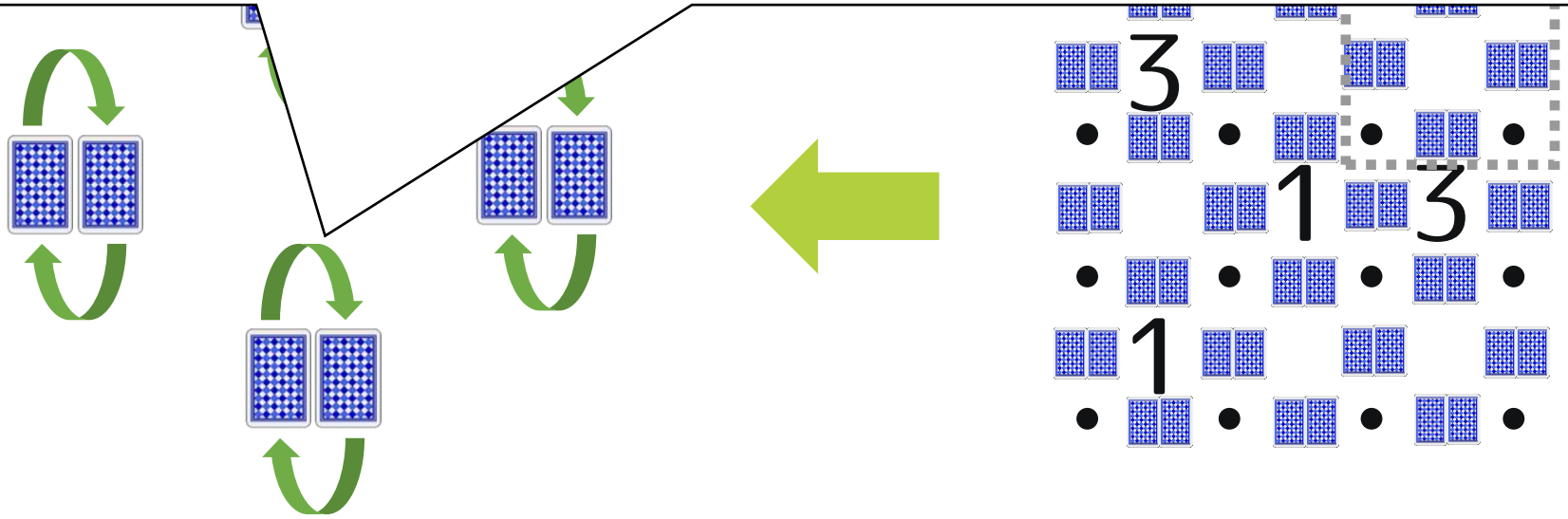


- 新たなループ



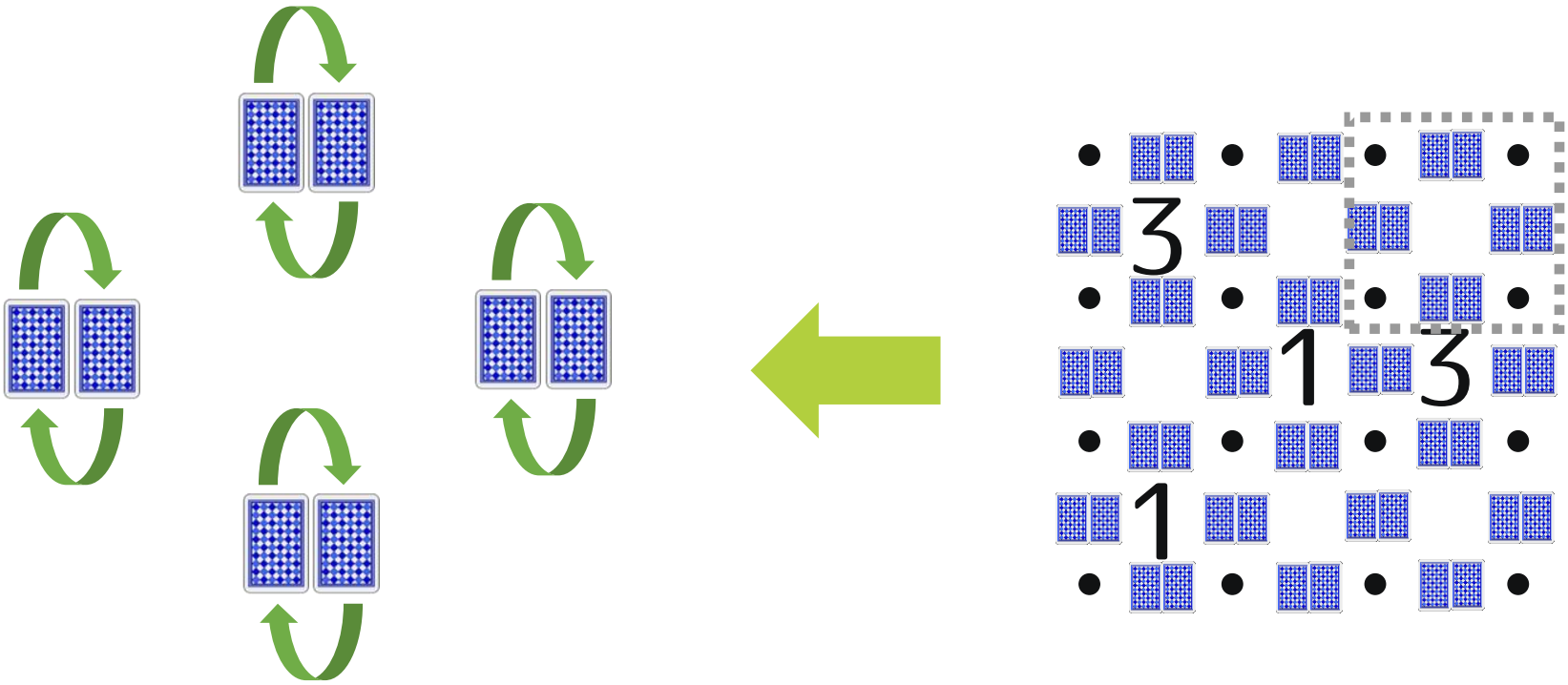
- 線の交錯

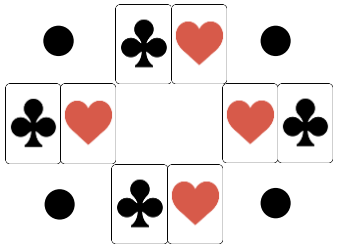


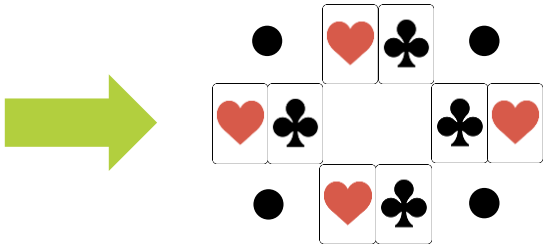


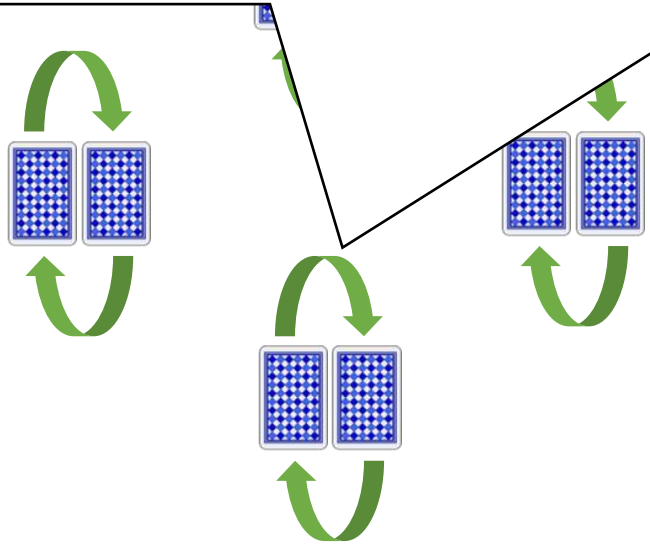
既存ZKPの欠点

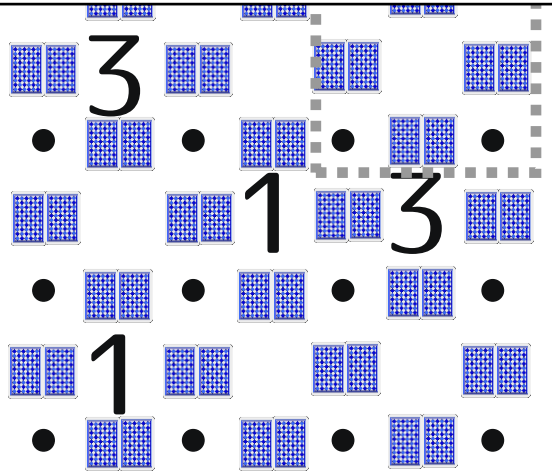
- 凹み前後に追加検証が必要
  - Pが選んだ4点の間に線が存在すること（シャッフル2回）
  - 凹ませた後に線が交差していないこと（シャッフル8回）



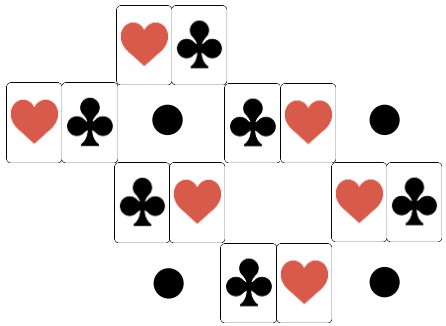


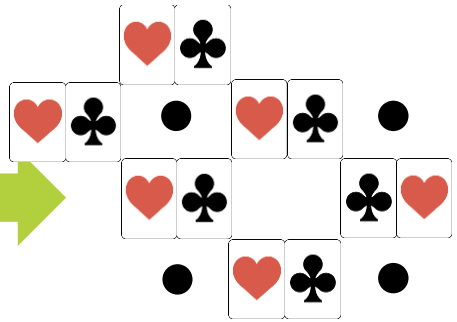


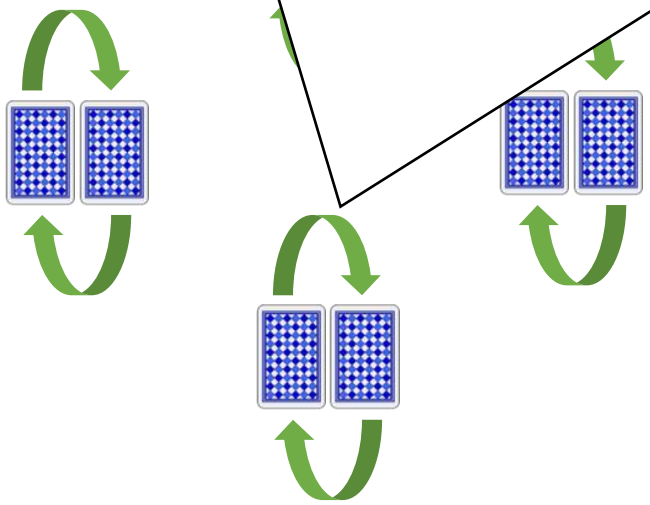


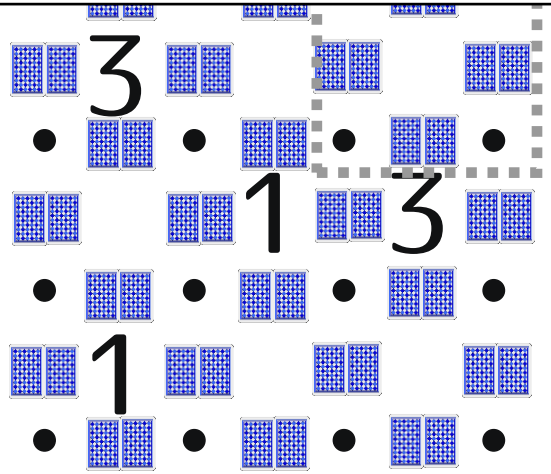

3
1
3
1

凹ませた先で交錯する可能性





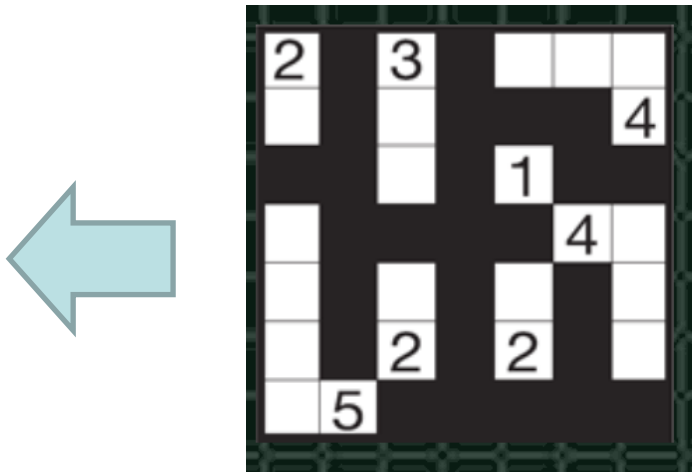




目次

[再掲] 貢献:1つの輪検証の効率化

- 1つの輪を描くパズルに対するZKPを効率化
  - ➢既存方式[LMM+21]の非効率な手順を指摘
  - ➢ひとつながりの検証[RML+21]を応用
- 手順(シャッフル回数)を半分にまで削減

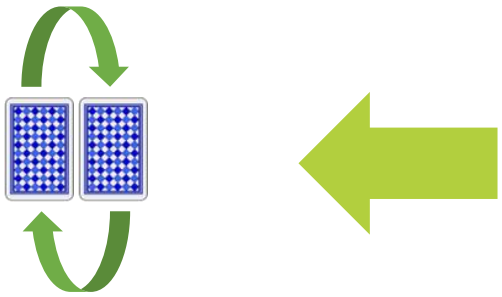


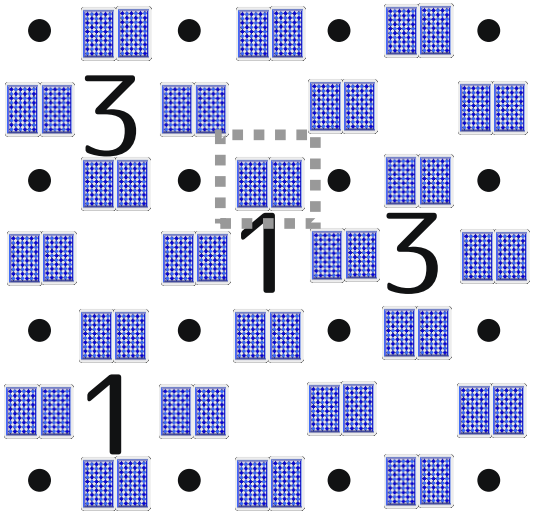
スリザーリンク[LMM+21]　　ぬりかべ[RML+22]

[LMM+21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone, How to Construct Physical Zero-Knowledge Proofs for Puzzles with a “Single Loop” Condition, TCS 2021

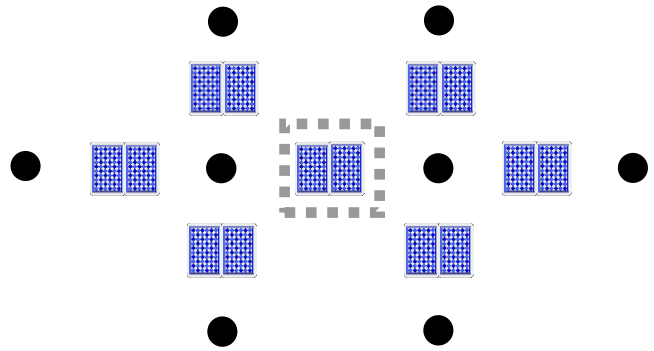
アイデア：線を1つずつ描く

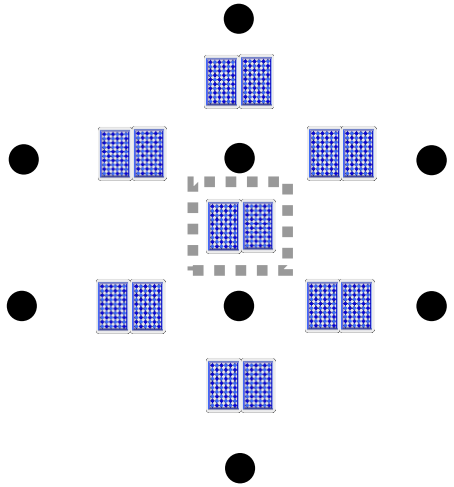
- Pに線を安全に「描かせる」
  - ➢既に描いた線に繋ぐように描く
  - ➢追加検証が比較的楽（シャッフル4回）

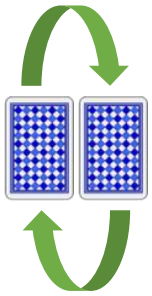


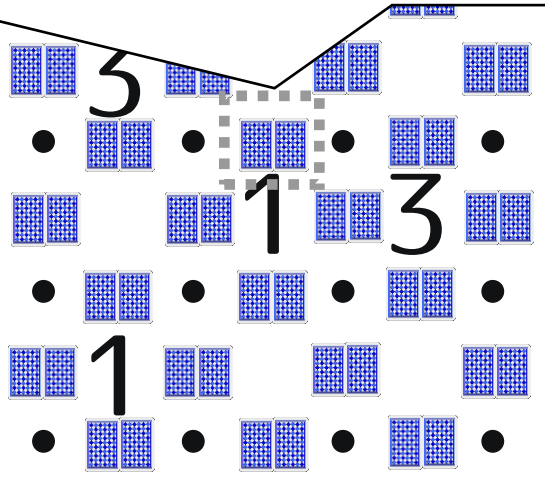


- 描く位置によって検証すべき位置が異なる
- 描く位置は秘密なので工夫が必要



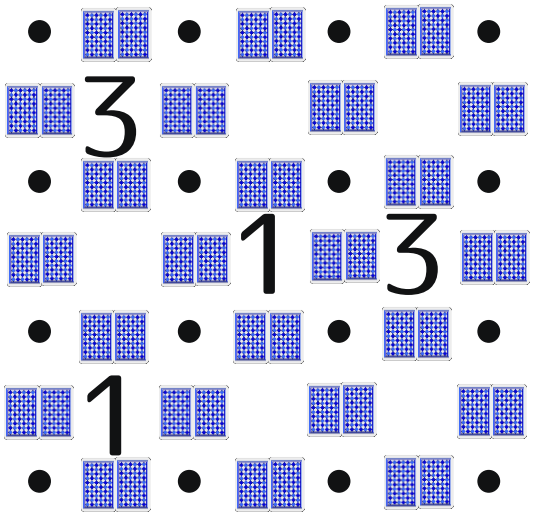






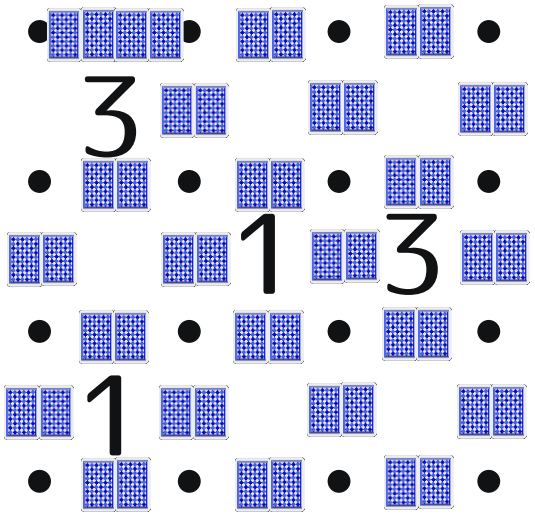
提案プロトコル

1. 各ドットの間に ♣♥ を置き、裏返す
2. Pに線を描かせることを繰り返す



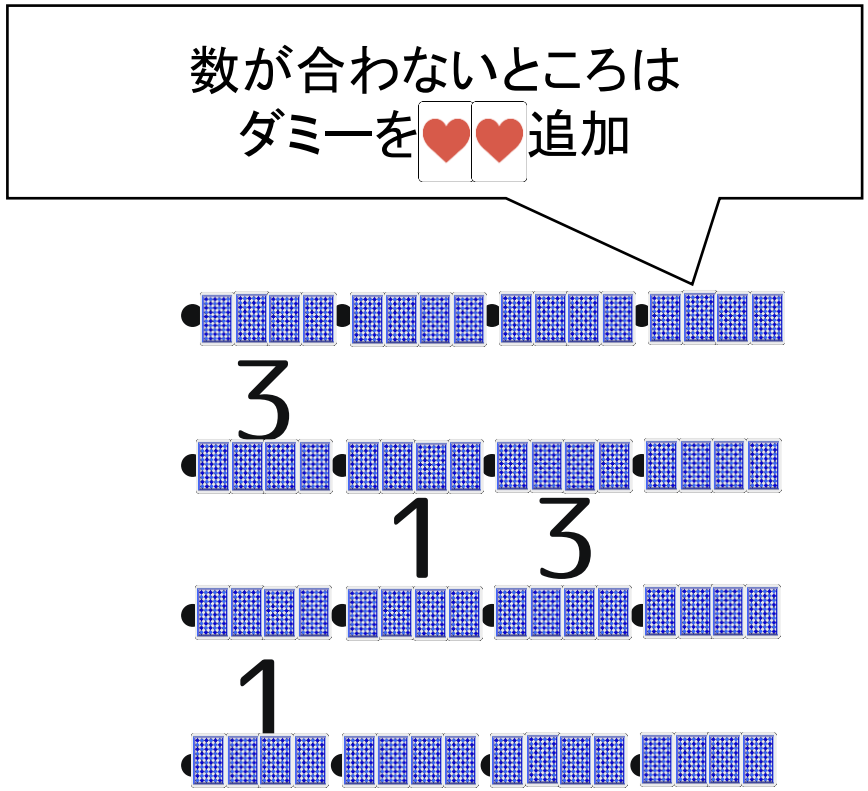
提案プロトコル

1. 各ドットの間に ♣♥ を置き、裏返す
2. *P*に線を描かせることを繰り返す
   a. 各四角の上・左辺上に置かれたカードをまとめる



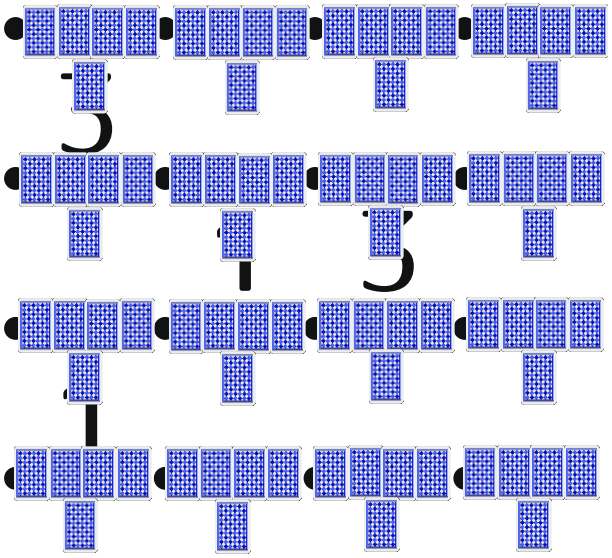
提案プロトコル

1. 各ドットの間に ♣♥ を置き、裏返す
2. Pに線を描かせることを繰り返す
   a. 各四角の上・左辺上に置かれたカードをまとめる



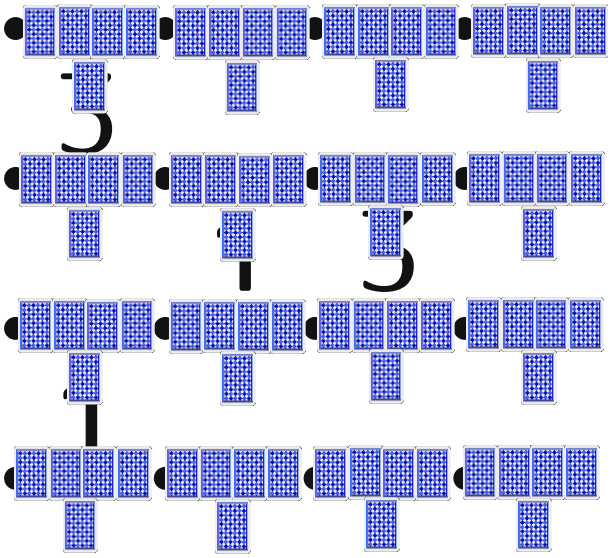
提案プロトコル

1. 各ドットの間に ♣♥ を置き、裏返す
2. *P*に線を描かせることを繰り返す
   a. 各四角の上・左辺上に置かれたカードをまとめる
   b. *P*は描きたいところに ♥ 、それ以外に ♣ を裏にして置く



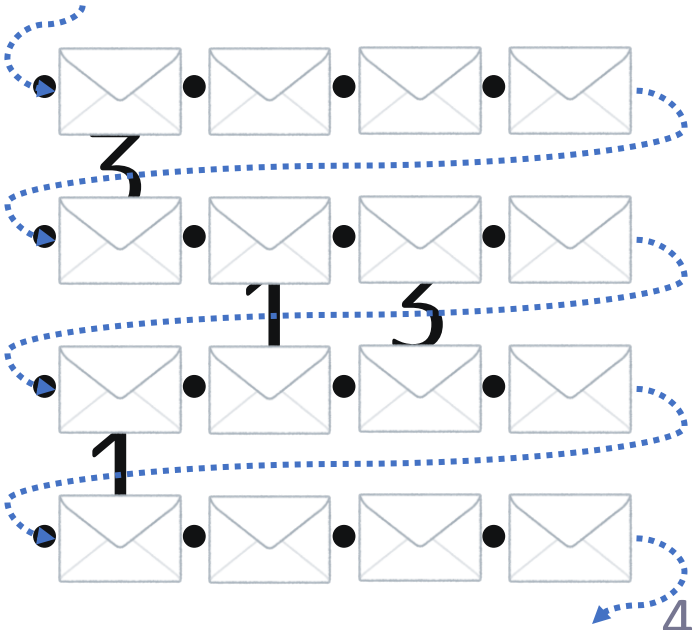
提案プロトコル

1. 各ドットの間に ♣♥ を置き、裏返す
2. *P*に線を描かせることを繰り返す
   a. 各四角の上・左辺上に置かれたカードをまとめる
   b. *P*は描きたいところに ♥ 、それ以外に ♣ を裏にして置く
   c. 5枚から成るカード束を巡回的にシャッフルする



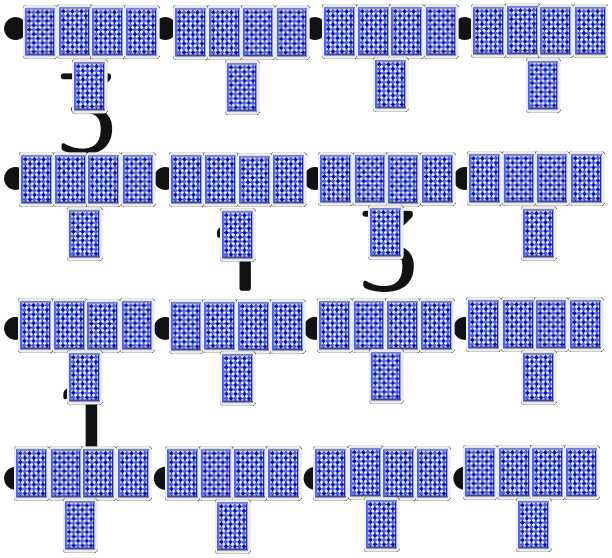
提案プロトコル

1. 各ドットの間に ♣♥ を置き、裏返す
2. *P*に線を描かせることを繰り返す
   a. 各四角の上・左辺上に置かれたカードをまとめる
   b. *P*は描きたいところに ♥ 、それ以外に ♣ を裏にして置く
   c. 5枚から成るカード束を巡回的にシャッフルする



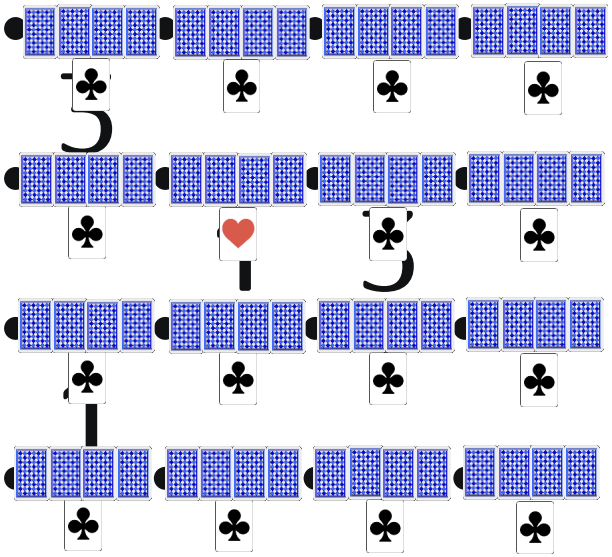
提案プロトコル

2. Pに線を描かせることを繰り返す
   d. Pが置いたカードをめくり、赤が含まれる束を見る



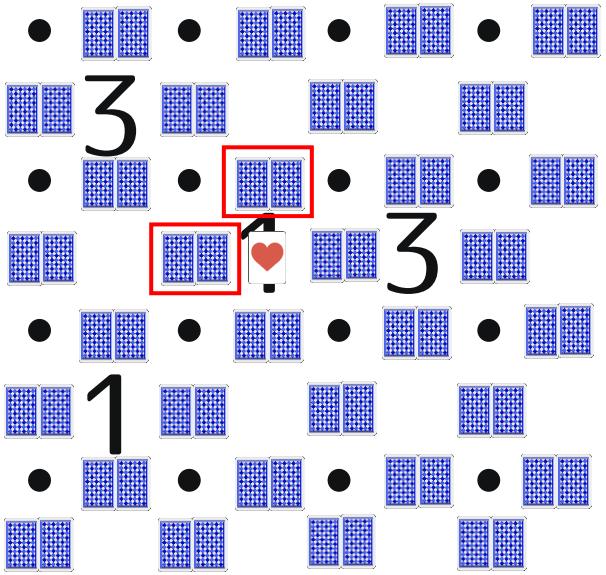
提案プロトコル

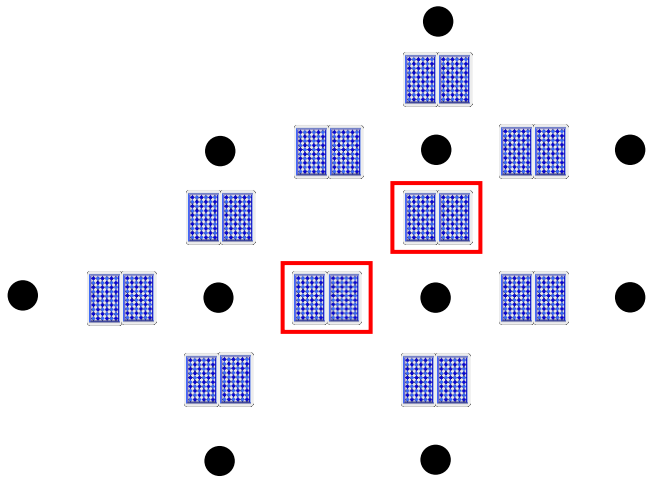
2. Pに線を描かせることを繰り返す
   d. Pが置いたカードをめくり、赤が含まれる束を見る



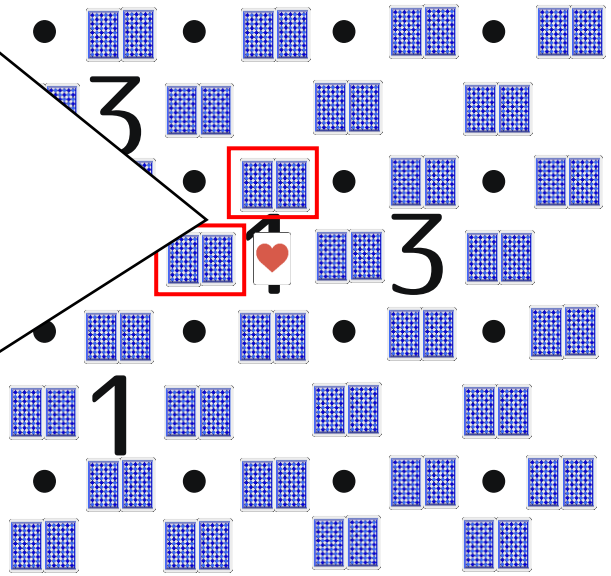
提案プロトコル

2. *P*に線を描かせることを繰り返す
   - *d.* *P*が置いたカードをめくり、赤が含まれる束を見る
   - e. 再度*P*に、どの2つに線を描くのかを選ばせる

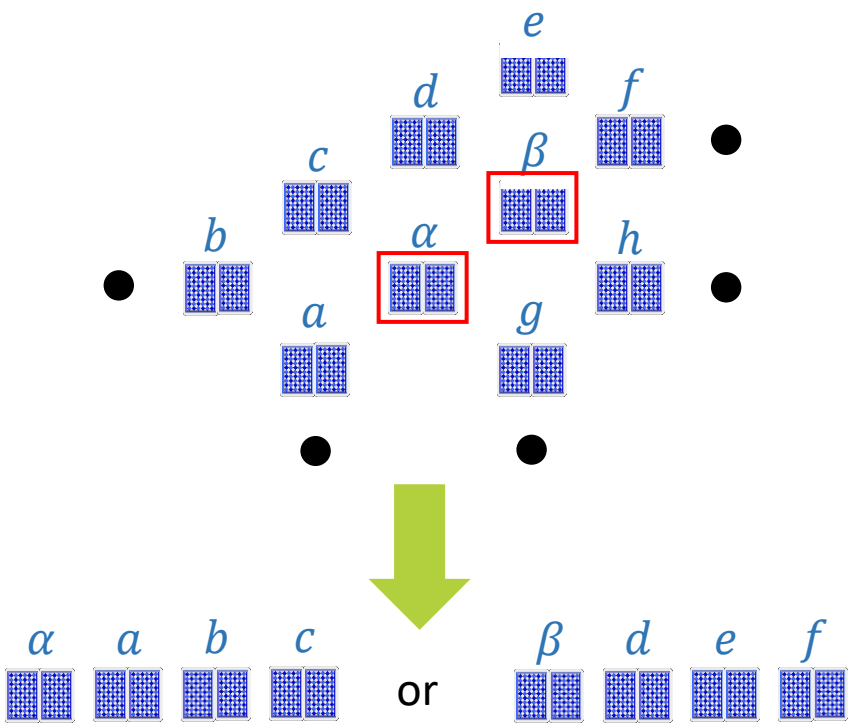




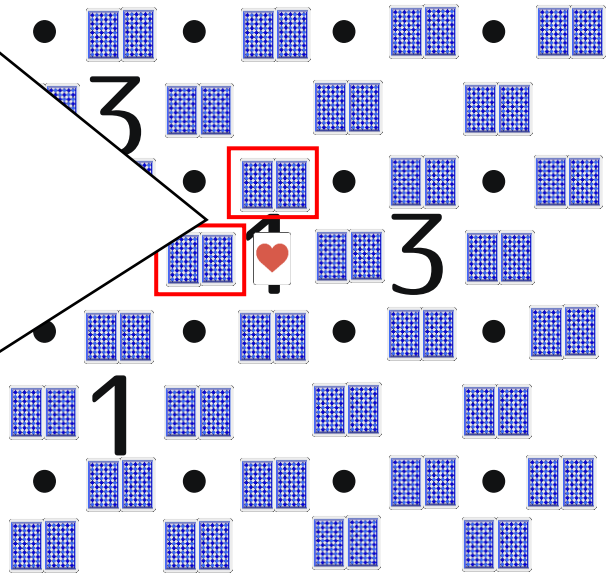
す
含まれる束を見る
かを選ばせる



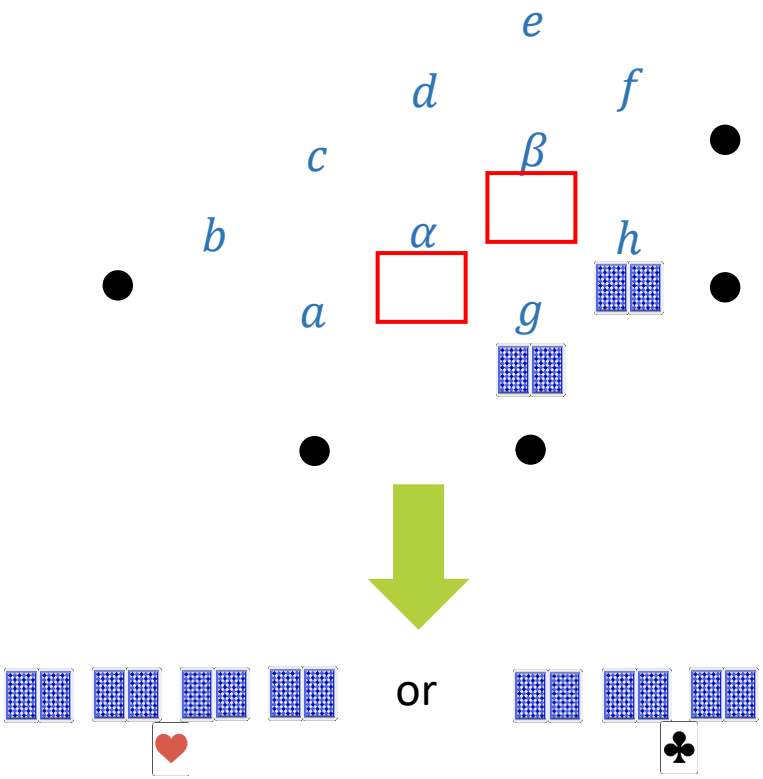
- 検証に必要なカードは上記の通り



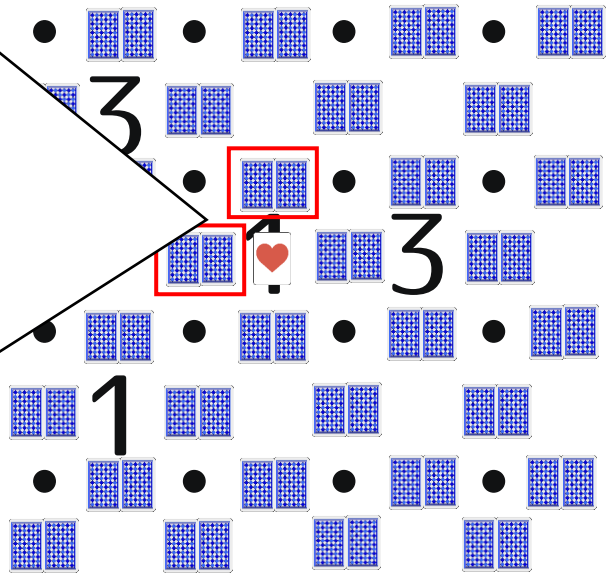
す
含まれる束を見る
かを選ばせる



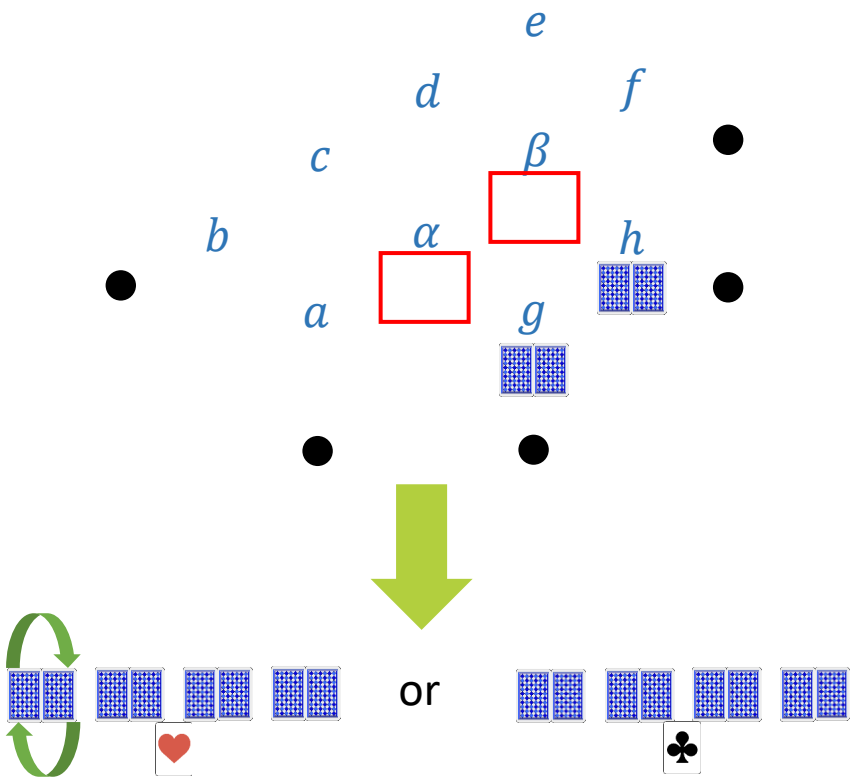
- どちらを描いて検証するかを選ぶ



す
含まれる束を見る
かを選ばせる

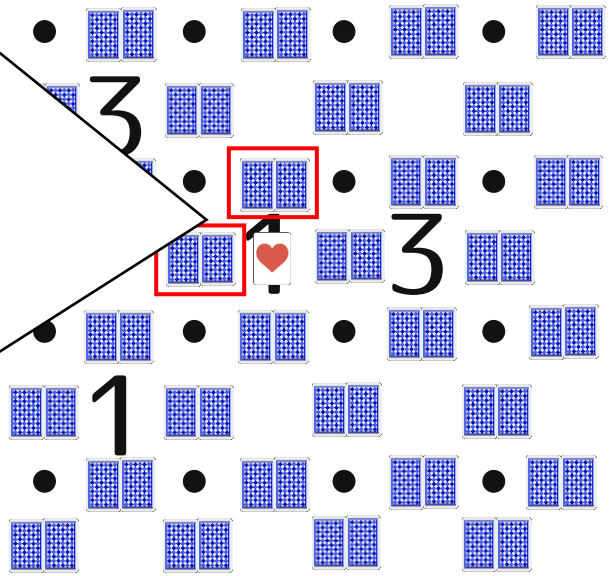


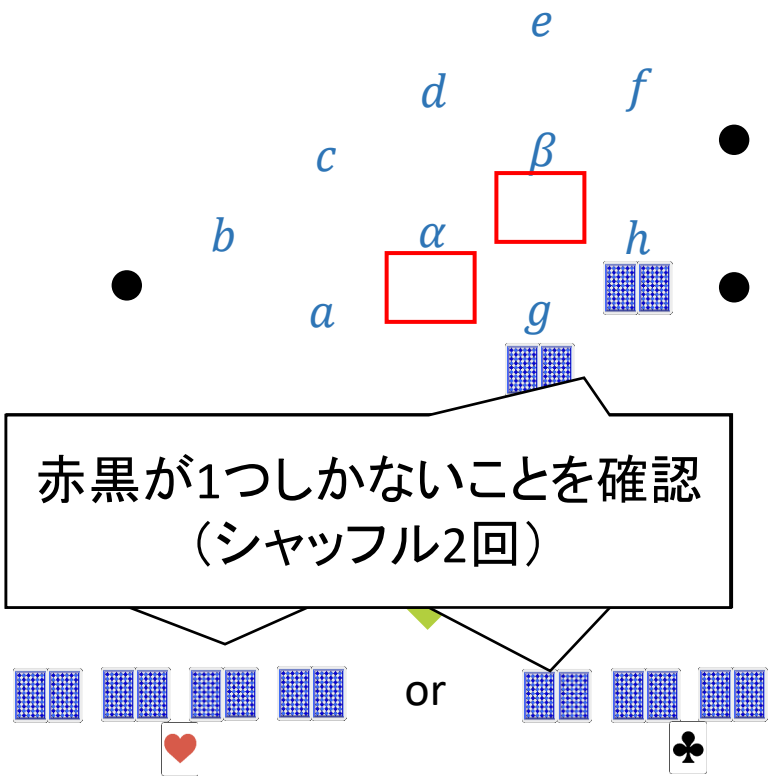
- 左のカード束が安全に選ばれた



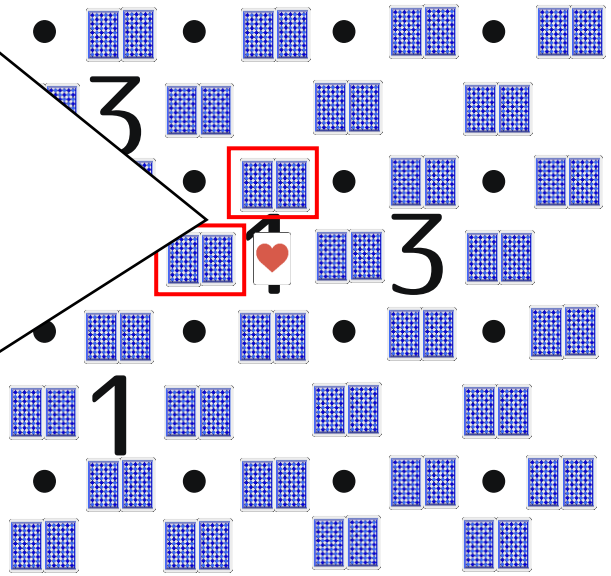
1. 選ばれたコミットメントをスワップ

す
含まれる束を見る
かを選ばせる





す
含まれる束を見る
かを選ばせる



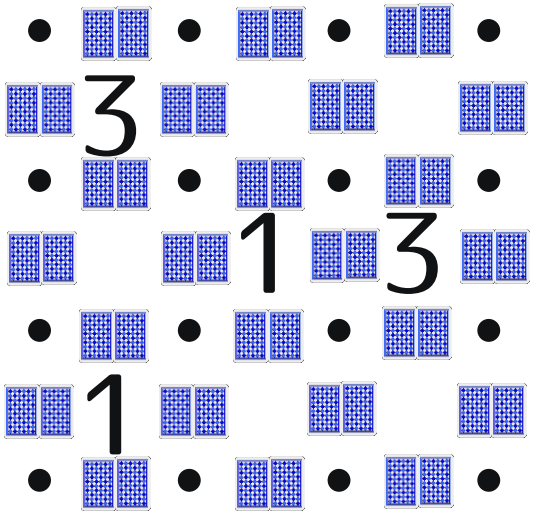
1. 選ばれたコミットメントをスワップ
2. 描いた線が先端になることを確認
   - 最後は結合されることを確認

提案プロトコル

- 以上をループが描かれるまで繰り返す
  - ➢解を知らないPであっても、必ず1つのループが描かれる
  - ➢1つのループが数字ルールも満たす→解を知っている
- シャッフル回数は（各繰り返しの中で）6回
  - ➢既存方式は12回[LMM+21]

P

V



[LMM+21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone, How to Construct Physical Zero-Knowledge Proofs for Puzzles with a “Single Loop” Condition, TCS 2021

目次

議論

- 提案プロトコル中の最大繰り返し数は盤面サイズ
  - ➢既存方式と全く一緒の繰り返し数[LMM+21]
  - ➢つまりシャッフル回数は半分に効率化
- 周長も秘匿する必要あり[LMM+21]
  - ➢あり得る解の最大周長分を繰り返す
  - ➢先端の線を消す（全く同じ操作）ことも行う

最大周長は
点の数と等しい

[LMM+21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone, How to Construct Physical Zero-Knowledge Proofs for Puzzles with a “Single Loop” Condition, TCS 2021

結論

- 1つの輪を描くパズルに対するZKPを効率化
  - ➢既存方式[LMM+21]の非効率な手順を指摘
  - ➢ひとつながりの検証[RML+22]を応用
- 未解決：重力を安全に証明する
  - ➢ストストーンに対するZKPの構築

[LMM+21] Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Léo Robert, Tatsuya Sasaki, and Hideaki Sone, How to Construct Physical Zero-Knowledge Proofs for Puzzles with a “Single Loop” Condition, TCS 2021