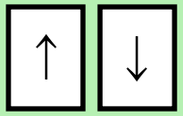
カードベース暗号に登場する さまざまなカード組と符号化

品川 和雅（茨城大学）

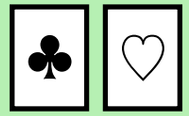
本発表の位置付け

- カードプロトコルでは伝統的に**二色カード** ♣ ♡ が用いられてきた
- 30年以上の歴史の中で**さまざまな種類のカード**が提案されている

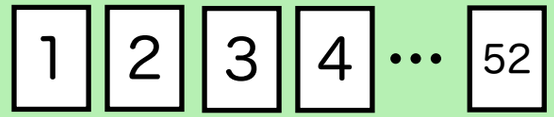
上下カード



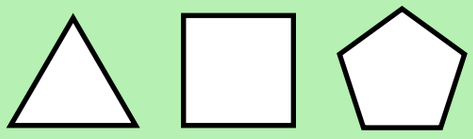
二色カード



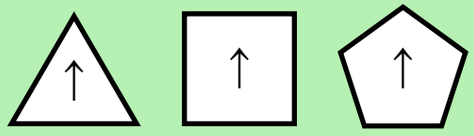
トランプ



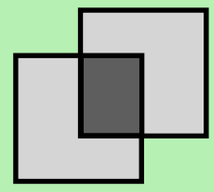
不可視インク



正多角形カード



偏光板カード



- いくつかのカードについて**未解決問題**を紹介する

目次

- **上下カード**
  - Mizuki-Shizuyaの上下カード
  - 未解決問題

- **正多角形の形状をしたカード**
  - Shinagawa et al.の正多角形カード
  - 不可視インクを用いた正多角形カード
  - 未解決問題

- **二色カードの1枚符号化**
  - Niemi-Renvallのコピープロトコル
  - 未解決問題

上下カード

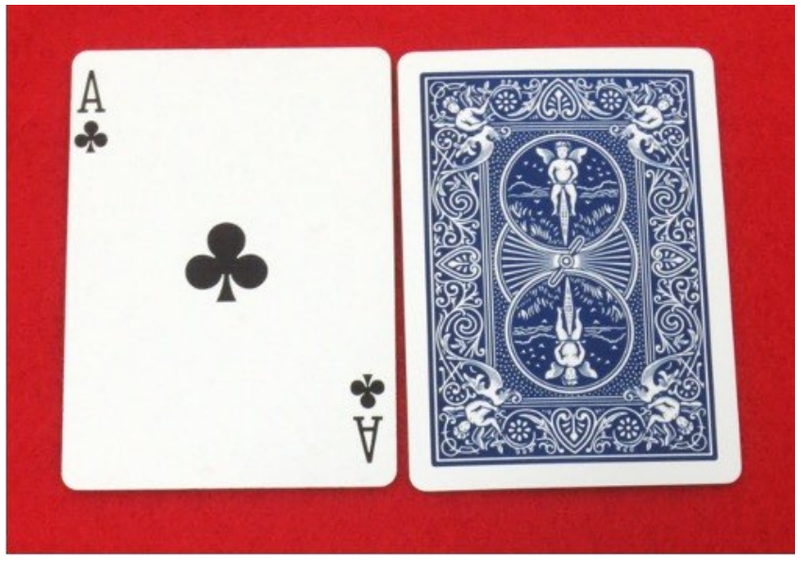
上下カード

- **二色カード** ♣ ♡ と**トランプ** 1 2 … 52 が伝統的に用いられてきた
- 上記以外で歴史上はじめて登場した変種カードが**上下カード**である

上下カード

オモテ： ↑ （上下非対称）

ウラ： （**上下対称**）



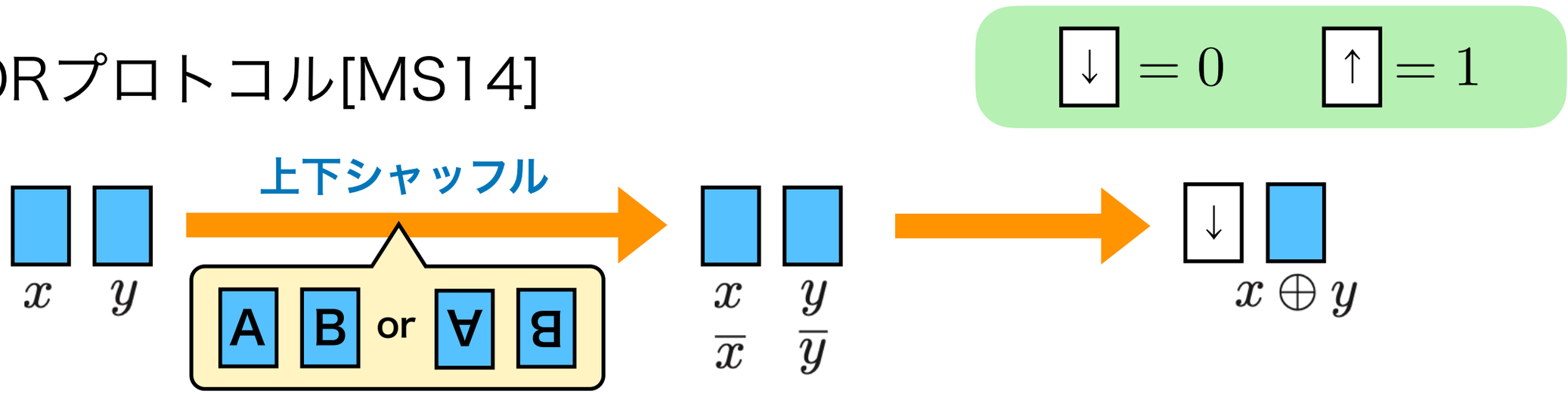
上下カードの例

- Mizuki-Shizuyaによって提案された[MS14]

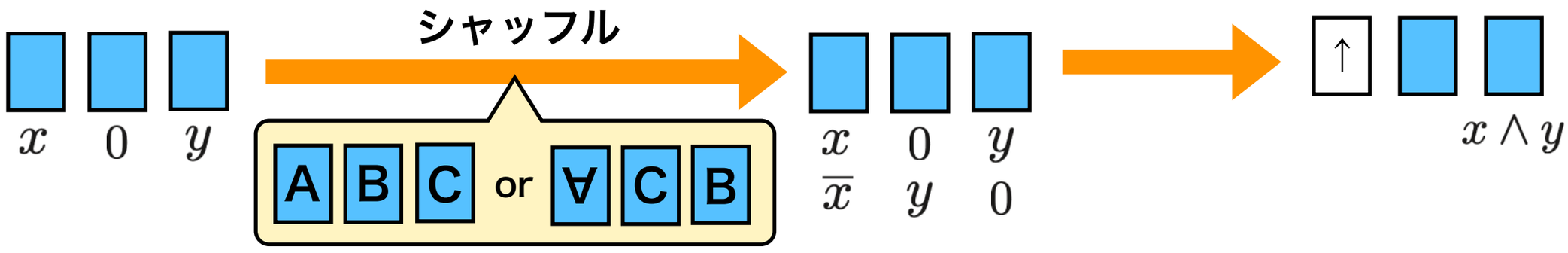
[MS14] Takaaki Mizuki, Hiroki Shizuya. Practical Card-Based Cryptography. FUN 2014.

上下カードのプロトコル

- XORプロトコル[MS14]



- ANDプロトコル[MS14]



  - 他にトルネードシャッフルを用いる構成[SNN+16]もある

- 非コミット型プロトコル[S22a], [S22b]

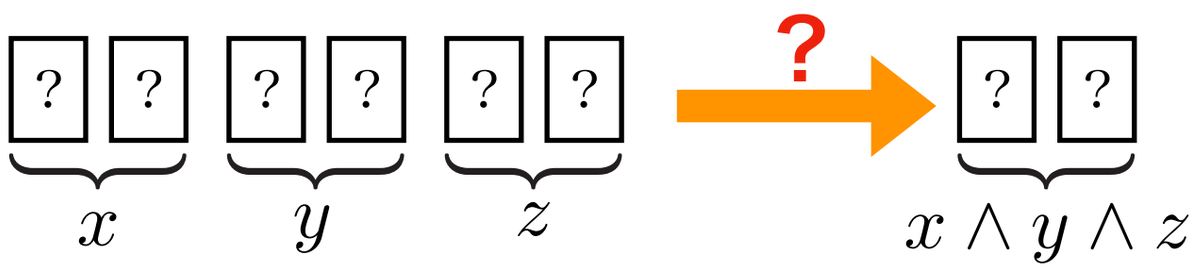
[SNN+16] Kazumasa Shinagawa, Koji Nuida, Takashi Nishide, Goichiro Hanaoka, Eiji Okamoto. Committed AND protocol using three cards with more handy shuffle. ISITA 2016.
[S22a] Yuji Suga. A classification proof for commutative three-element semigroups with local AND structure and its application to card-based protocols. ICCE-TW 2022.
[S22b] Yuji Suga. How to implement non-committed card protocols to realize AND operations satisfying the three-valued logics. CANDARW 2022.

上下カードと二色カードの関係

- 上下カードn枚プロトコル ➡ 二色カード2n枚プロトコル

- **不可能性証明は上下カードの方がしやすい**

- **二色カードの不可能性証明は難しい**
  - 現状：2入力ANDとコピーの不可能性証明 (e.g. [KKW+17])
  - 3入力ANDの有限時間6枚の不可能性は重要な未解決問題
    - 2入力が解決されてから8年以上経つが全く進展していない



- **上下カードの不可能性を手掛かりにできないか**

[KKW+17] Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone. The Minimum Number of Cards in Practical Card-Based Protocols. ASIACRYPT 2017.

未解決問題：AND関数

- 設定：上下カードの有限時間コミット型プロトコル

- n入力ANDは(n+1)枚で計算できる
  - 構成法：3枚ANDプロトコル[MS14]の繰り返し

- **n入力ANDはn枚では計算できないことを示せ**
  - n=2のときは解決済み
    - 二色カードの4枚ANDが不可能であること[KWH15]からただちに従う
  - nが3以上のときは未解決

[MS14] Takaaki Mizuki, Hiroki Shizuya. Practical Card-Based Cryptography. FUN 2014.
[KWH15] Alexander Koch, Stefan Walzer, Kevin Härtel. Card-Based Cryptographic Protocols Using a Minimal Number of Cards. ASIACRYPT 2015.

未解決問題：対称関数と任意関数

- 設定：上下カードの有限時間コミット型プロトコル

- **任意の対称関数に対するプロトコルを構成し、その最適性を示せ**
  - 二色カード：2n+2枚プロトコル[NHMS15]
  - 上下カードでも(n+1)枚のプロトコルが構成できるか？

- **任意関数に対するプロトコルを構成し、その最適性を示せ**
  - 二色カード：2n+6枚プロトコル[NHMS15]
  - 上下カードでも(n+3)枚のプロトコルが構成できるか？

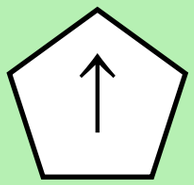
[NHMS15] Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, Hideaki Sone. Card-Based Protocols for Any Boolean Function. TAMC 2015.

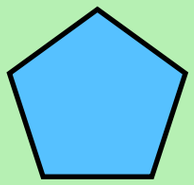
正多角形の形状をしたカード

正多角形カード

- 上下カードは180度回転を許すことにより1枚で1ビットを表した
- **(360/n)度回転を許すことによりn値を扱うこと**は自然な一般化
- **正多角形カード**はこの発想により提案された[SMS+15]

正多角形カード

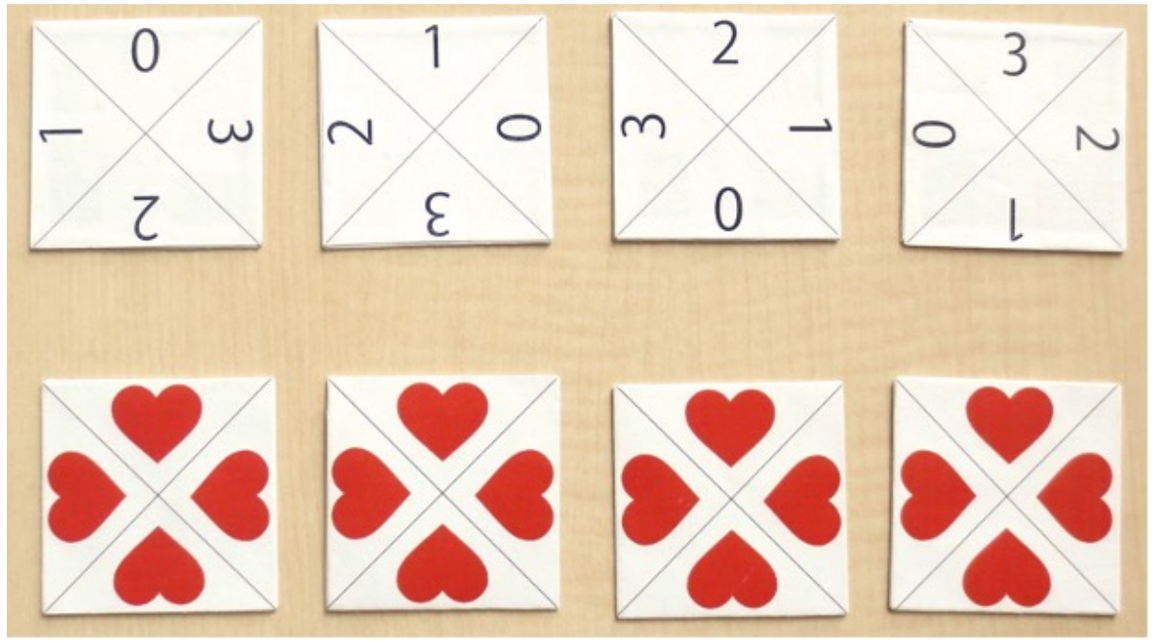
オモテ：  （回転非対称）

ウラ：  **（回転対称）**

[SMS+15] Kazumasa Shinagawa, Takaaki Mizuki, Jacob C. N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, Eiji Okamoto. Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards. ProvSec 2015.

正4角形カードの例

- オモテの絵柄は(360/n)度回転**非**対称なら何でもよい



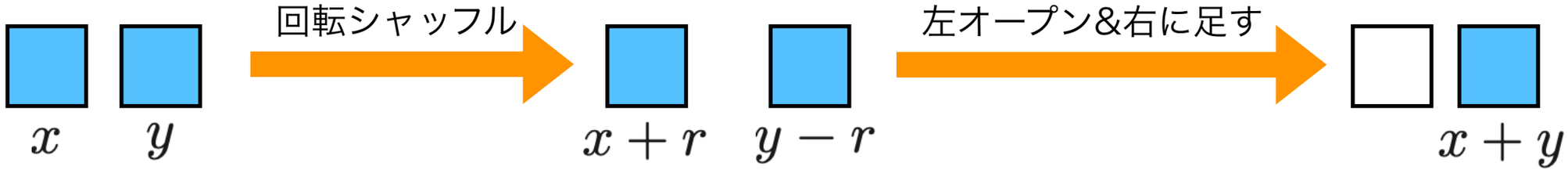
正4角形カードの例

- 上記のカードは自然にZ/4Zの値を保持する

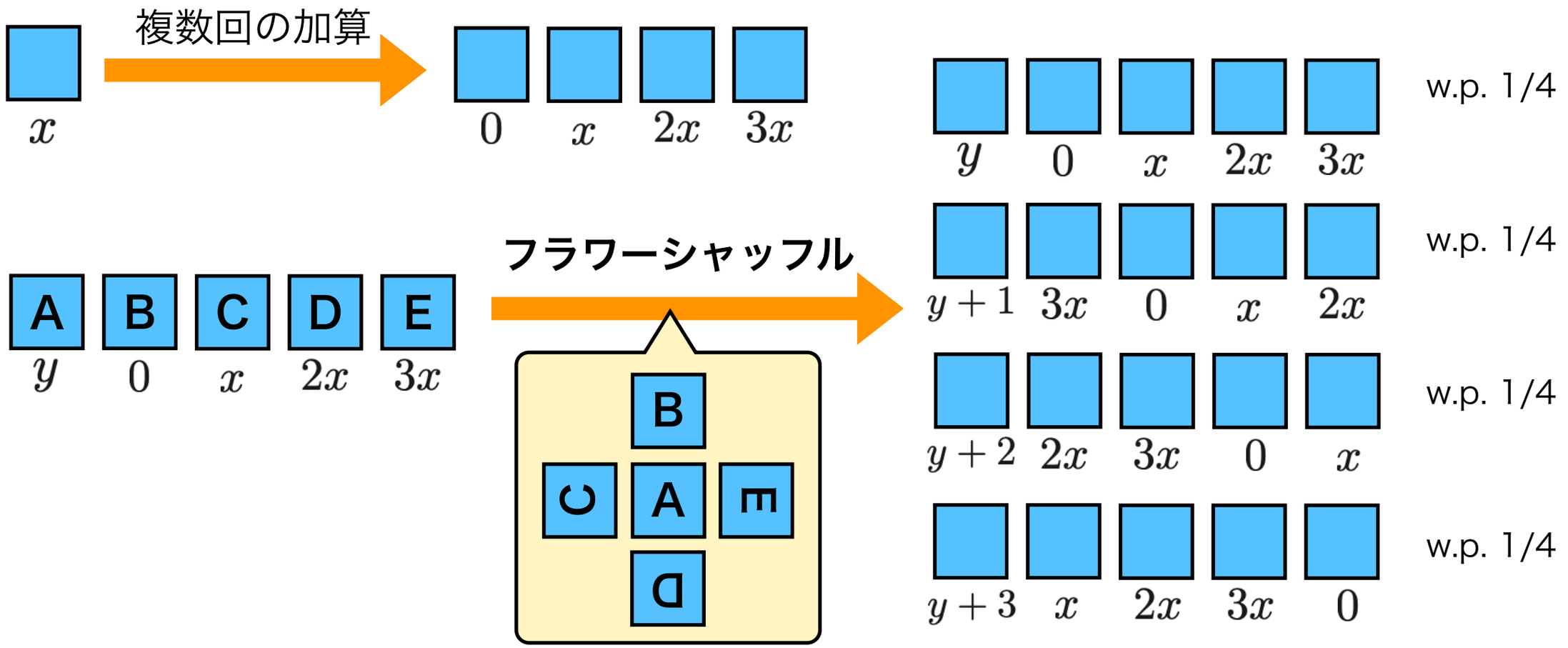
オモテ	0	1	2	3
ウラ				

加算と乗算

- 2枚の加算プロトコル[SMS+15]



- (n+1)枚の乗算プロトコル[S20]



[S20] On the Construction of Easy to Perform Card-Based Protocols. PhD thesis 2020.

未解決問題：乗算プロトコル

- 現状
  - 自明な下界は2枚（入力に2枚必要）
  - 既存プロトコルは(n+1)枚[S20]

- **乗算プロトコルの効率化**
  - n=3のとき、3枚乗算プロトコルは構成できるか？
  - nに条件をつけたとき、効率化は可能か？
    - 条件の例：素数、2のべき乗など

- **乗算プロトコルの下界証明**
  - n=3のとき、3枚乗算プロトコルの不可能性を示せるか？

[S20] On the Construction of Easy to Perform Card-Based Protocols. PhD thesis 2020.

大きな数の加算

- **合計値（平均値）の秘密計算**は日常生活でも使う場面が多くある
  - 例：3人の平均体重を求めたい

- 合計値の計算をする場合は、出来るだけ大きな数を扱えると良い

- しかし、正n角形カードの角数nはあまり増やせない
  - 理論的には、nはいくらでも増やせる
  - 現実的には、nが大きすぎると、操作誤りが起きやすい
  - カードのサイズにもよるが、nは3〜8程度が妥当

- **大きな数の加算をするには？**

n進法の加算プロトコル

- **n進法**を用いる

$$\boxed{1}\ \boxed{3} = 1 \times 4 + 3 = 7$$

$$\boxed{3}\ \boxed{2} = 3 \times 4 + 2 = 14$$

- **繰り上がりの計算**をどう実現するか？

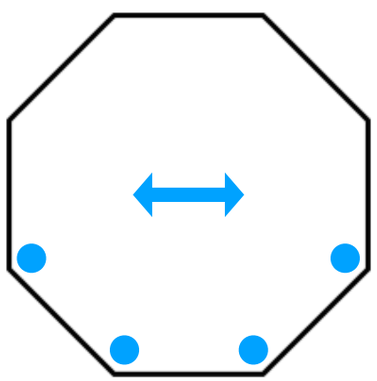
$$\begin{array}{rccc} & \boxed{1} & \boxed{1} & \\ + & \boxed{3} & \boxed{2} & \\ \hline \boxed{1} & \boxed{0} & \boxed{3} & \end{array}$$

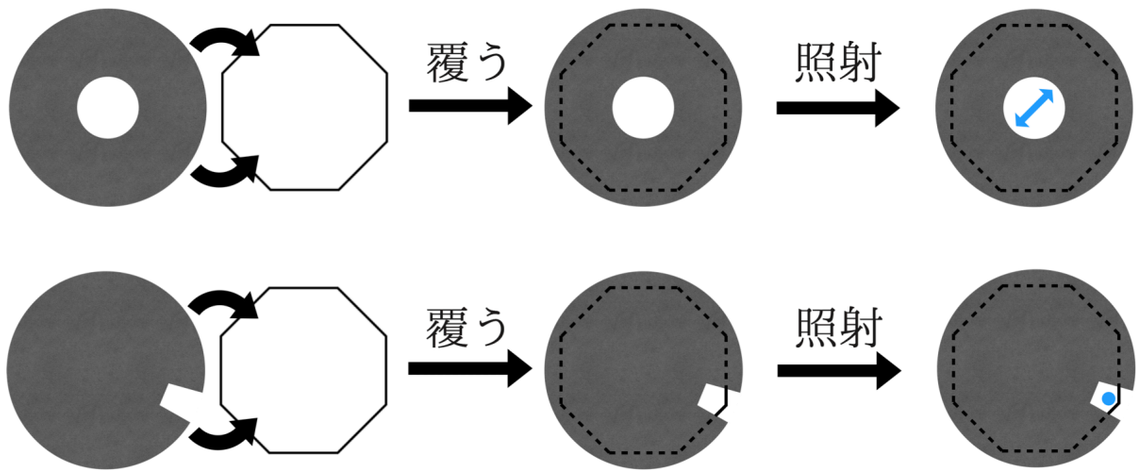
正多角形カードは
このような計算は
向いていない(ように思える)

アイディア：不可視インクの使用

- **不可視インク**
  - ブラックライトを照射すると見える特殊インク

- **不可視インクを用いた正多角形カード**[S19]
  - 別名：層状多角形カード、二面体カード
  - n進法の計算をする場合は**正2n角形**を用いる
  - 中央に矢印を書き込む（整数値を保持するため）
  - いくつかの頂点にドットを書き込む（繰り上がり検知のため）

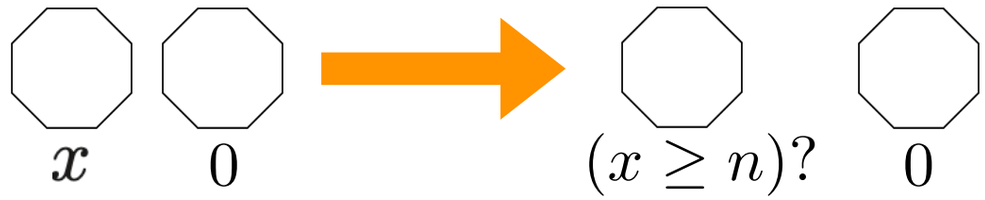




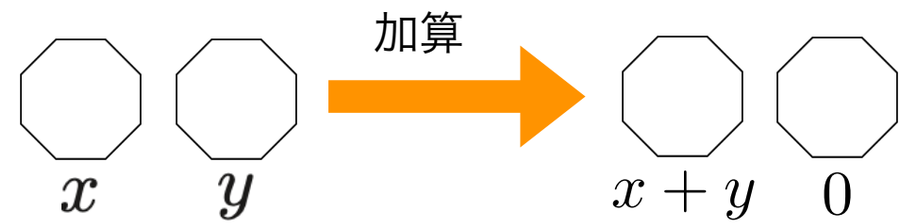
[S19] Kazumasa Shinagawa. Card-Based Cryptography with Invisible Ink. TAMC 2019.

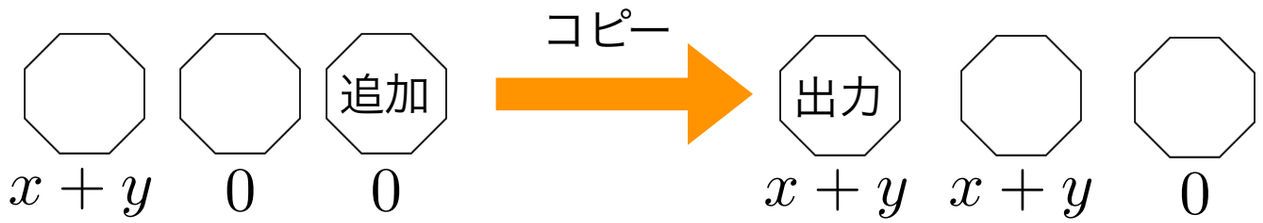
半加算器プロトコル

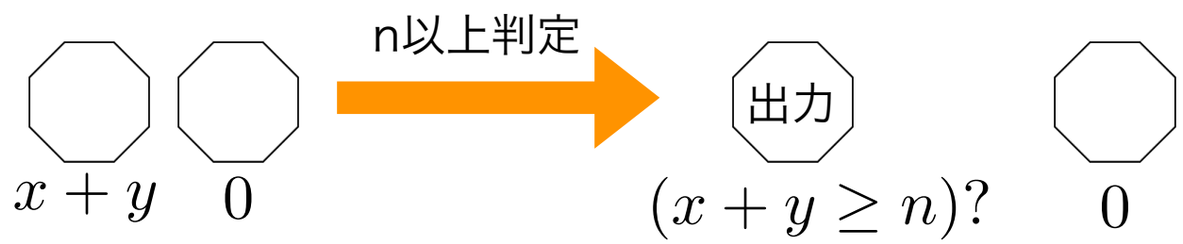
- n以上判定プロトコル



- 半加算器プロトコル（入力x, yは0以上n未満）
  - カード3枚
  - シャッフル6回







- 枚数は少ないが、シャッフル回数が多く、実際の実行は大変

未解決問題：大きな数の加算

- 大きな数
  - 具体的には100〜1000の加算
  - n=301なら3人のテスト(100点満点)の合計点を計算できる

- **大きな数の加算プロトコルの構成**
  - 実用的なプロトコルであることが望ましい
    - シャッフル回数が少なく、かつ、物理的実装が容易であること
    - 手操作で実際に実演できればOK
  - カードの種類は問わない
    - 新しいカードを設計・デザインしてOK

二色カードの1枚符号化

1枚符号化

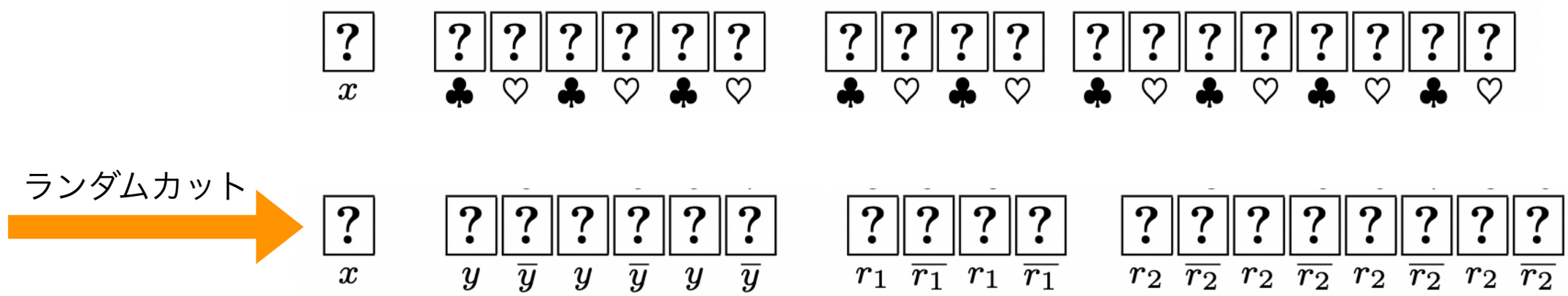
- 1枚符号化
  - 最も素朴な符号化

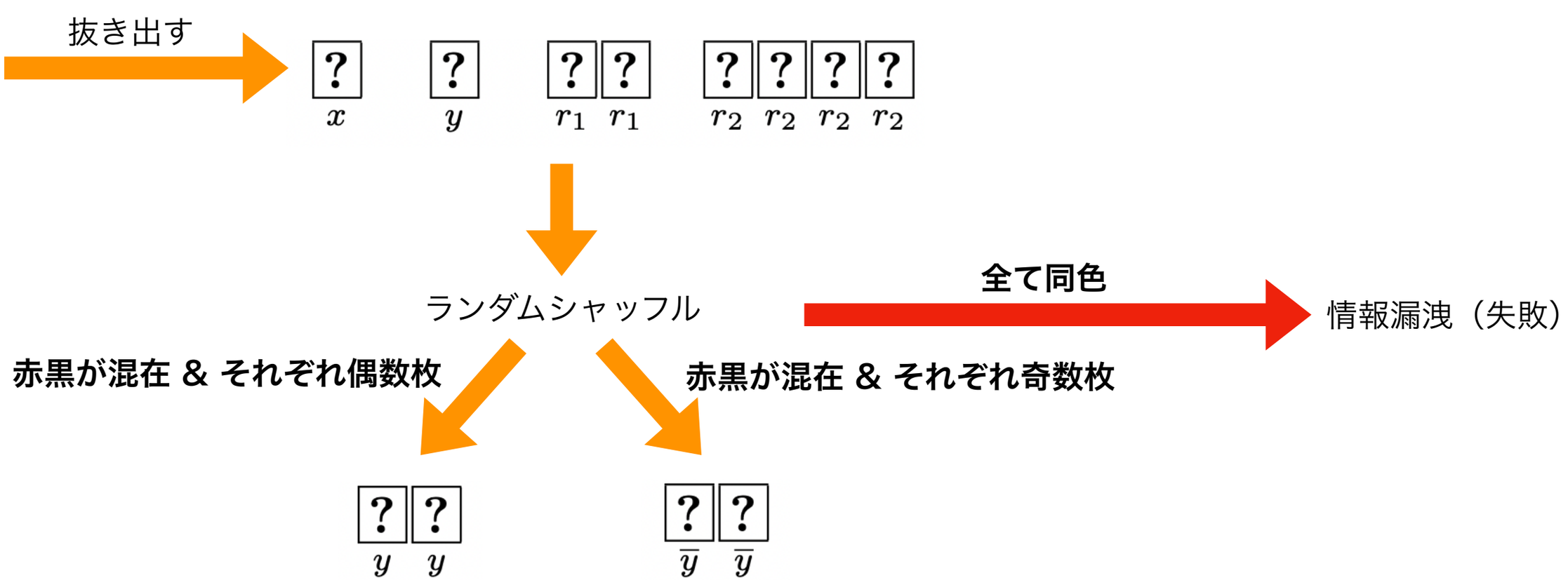
$$\boxed{\clubsuit} = 0 \qquad \boxed{\heartsuit} = 1$$

- さまざまな演算が非自明
  - NOTさえも自明ではない
  - コピーは可能？

Niemi-Renvallのコピープロトコル①

- 確率的な情報漏洩を許すコピープロトコル[NR98]





[NR98] Valtteri Niemi, Ari Renvall. Secure Multiparty Computations Without Computers. Theor. Comput. Sci. 1998.

Niemi-Renvallのコピープロトコル②

- 追加カードを増やせば失敗確率を下げられる
  - k個コピー、失敗確率$1/2^s$ ➡ 追加カード枚数：$(2^{s+1}+2k-2)$枚

- k個のコピーとともに、否定の1枚符号化もk個生成される
  - **1枚符号化から2枚符号化への変換プロトコル**ともみなせる

- 失敗確率は不可避
  - 1枚コピーでは確率的な情報漏洩は必ず生じる[MS14]

[MS14] Takaaki Mizuki, Hiroki Shizuya. A formalization of card-based cryptographic protocols via abstract machine. Int. J. Inf. Sec., 2014.

未解決問題：コピープロトコルの効率化

- Niemi-Renvallのコピープロトコル[NR98]
  - k個コピー、失敗確率$1/2^s$ ➡ 追加カード：$(2^{s+1}+2k-2)$枚

- **カード枚数の削減（または失敗確率の低減）は可能か？**
  - Mizuki-Shizuyaの不可能性より完全なコピーは不可能
  - しかしNiemi-Renvallプロトコルが最適かは分かっていない
    - 現代的な技術（例：ランダム二等分割カット）が用いられていない

[NR98] Valtteri Niemi, Ari Renvall. Secure Multiparty Computations Without Computers. Theor. Comput. Sci. 1998.

未解決問題：他のプロトコルの効率化

- 任意関数の計算は以下の方法で実現可能
  1. 1枚符号化を2枚符号化に変換（Niemi-Renvallコピープロトコル）
  2. 通常の2枚符号化のプロトコルを実行

- **上記の方法（2枚符号化を経由する方法）よりも**
カード枚数/失敗確率について効率的なプロトコルを構成可能か？

まとめ

- 上下カード
  - n枚ANDの不可能性
  - 対称関数と任意関数のプロトコル構成と下界証明
- 正多角形の形状をしたカード
  - 乗算プロトコルの効率化と下界証明
  - 大きな数の加算プロトコルの構成
- 二色カードの1枚符号化
  - コピープロトコルの効率化
  - 他の関数に対するプロトコルの効率化