IMI 共同利用ワークショップ
産学連携によるカードベース暗号の数理的未解決問題と新課題の整理

秘匿置換を用いたカードベース暗号

2023年5月31日

豊橋技術科学大学　中井雄士

カードベース暗号とは

■カードベース暗号とは
- トランプの様な物理的なカードを用いて行う暗号プロトコル

■使用するカード
- 表面に ♣ と ♥ が描かれた2種類のカード
  - ➢同じ絵柄のカードは区別ができない
  - ➢すべてのカードの裏面は同じ絵柄で，区別ができない

通常の暗号プロトコルにおける暗号化に対応

カードベース暗号研究の流れ：2つの操作モデル

ランダムカット

den Boer, EUROCRYPT'89

Crepeau-Kilian, CRYPTO'93

ランダム二等分割カット

Mizuki-Sone, FAW'09

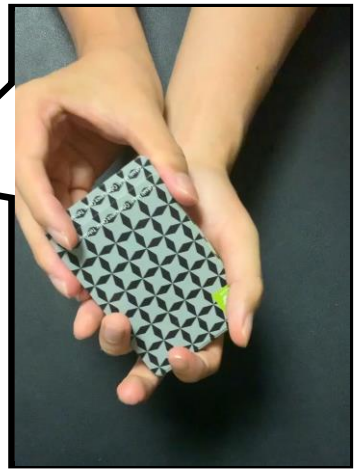
パイルスクランブルシャッフル

Ishikawa et al., UCNC'15

非一様シャッフル

Koch et al., ASIACRYPT'15

シャッフルに基づく
カードベース暗号



本発表のテーマ

カードベース暗号への
秘匿操作の導入

Nakai et al., CANS'16

⋮

本発表の流れ

■背景: シャッフルに基づくカードベース暗号

■秘匿置換に基づくカードベース暗号

■秘匿置換に基づくカードベースプロトコルの紹介
- 金持ち比べプロトコル
- 3入力多数決プロトコル

本発表の流れ

■背景: シャッフルに基づくカードベース暗号

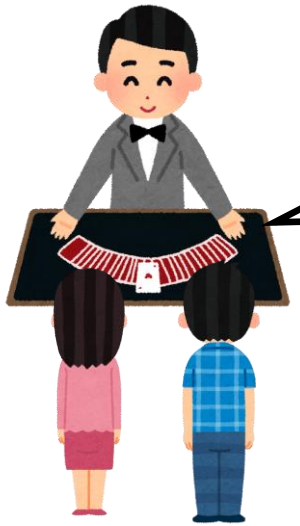
■秘匿置換に基づくカードベース暗号

■秘匿置換に基づくカードベースプロトコルの紹介
- 金持ち比べプロトコル
- 3入力多数決プロトコル

シャッフルに基づくカードベース暗号の操作モデル

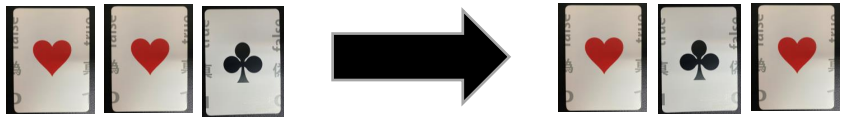
■ **パブリックモデル**

- テーブル上などですべての操作を公開して行う
  - ➢ イメージ：カードマジック

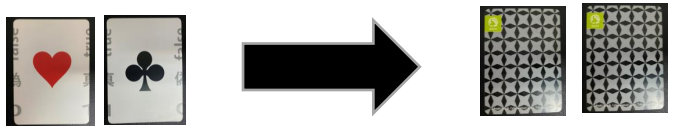


■ 操作

- 置換



- 反転



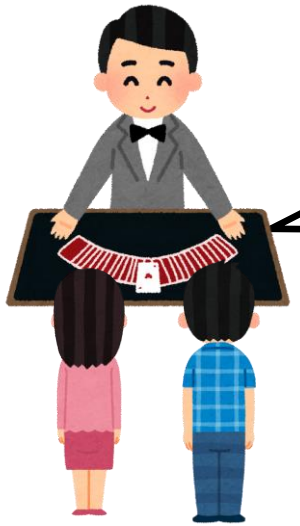
- シャッフル

パブリックモデルで秘匿性を実現するKey Technique

シャッフルとは

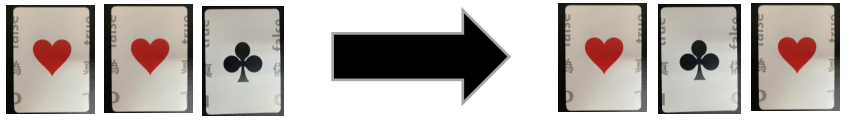
■シャッフル

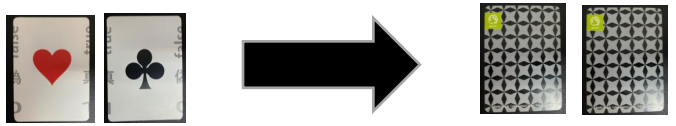
- 公開の場で行われるランダムな置換操作
  - ➢操作を実行したプレイヤ含め，結果の並びはすべてのプレイヤーが特定できない



■ 操作

- 置換





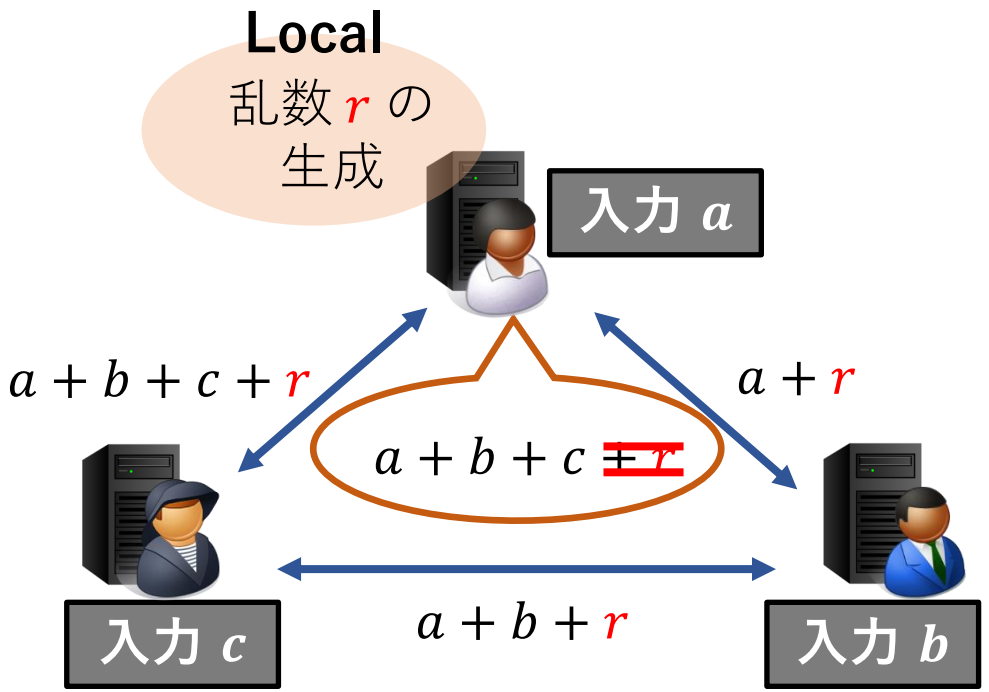
カードの性質に基づく
特殊なランダマイズ操作

- シャッフル

通常の暗号プロトコルとのギャップ

■ パブリックモデルのカードベース暗号
- すべての操作が公開
- 通信がない

■ 通常の(計算機ベースの)暗号プロトコル
- 各パーティがローカルで,
  プライベートな処理を行う



Private Randomness

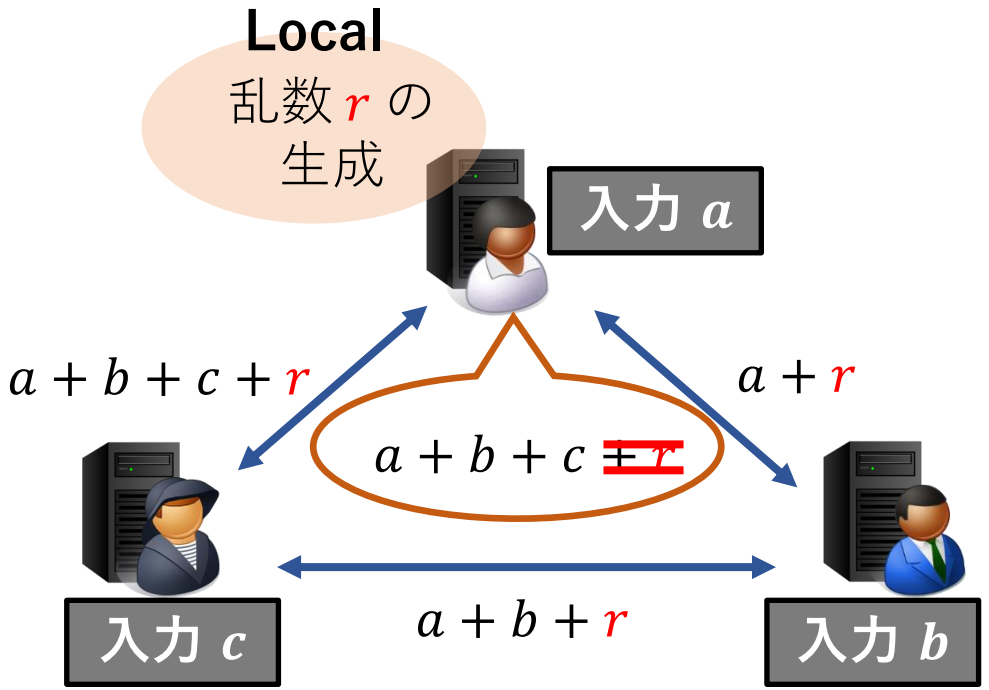
通常の暗号プロトコルとのギャップ

■ パブリックモデルのカードベース暗号
- すべての操作が公開
- 通信がない

■ 通常の(計算機ベースの)暗号プロトコル
- 各パーティがローカルで,
  プライベートな処理を行う

公開の場で
乱数生成

モデルが大きく
異なる



Private randomnessは
カードベース暗号でも
利用可能か？

Private Randomness

本発表の流れ

■背景: シャッフルに基づくカードベース暗号

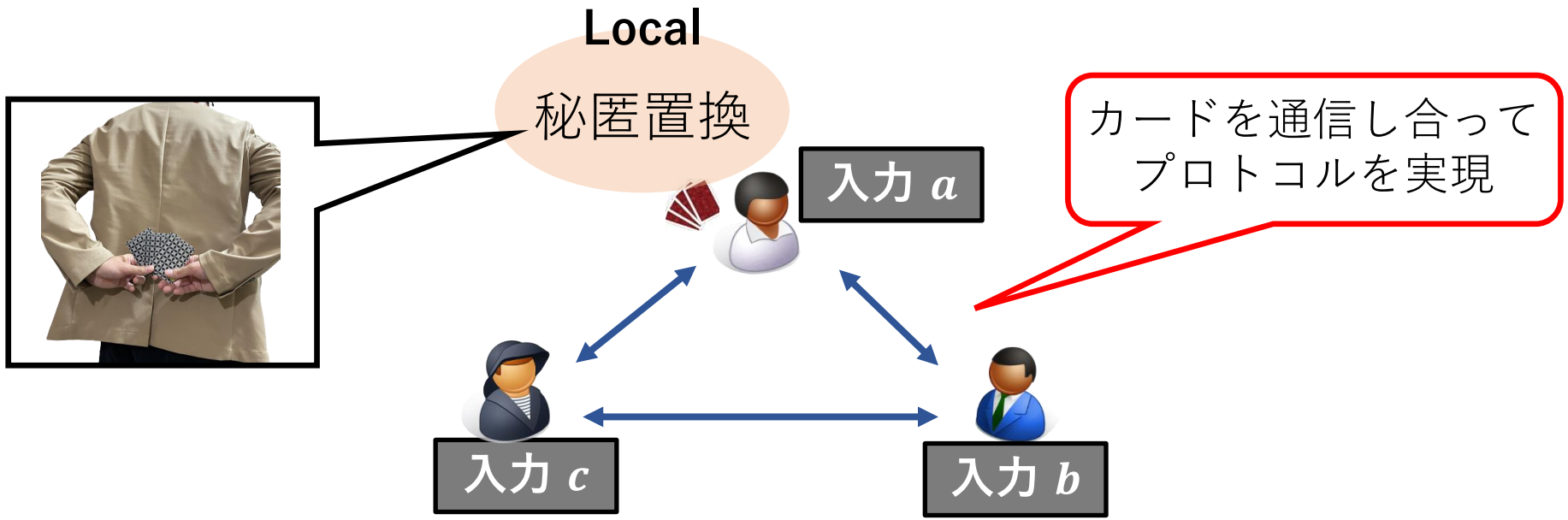
■秘匿置換に基づくカードベース暗号

■秘匿置換に基づくカードベースプロトコルの紹介
- 金持ち比べプロトコル
- 3入力多数決プロトコル

カードベース暗号へのPrivate Randomnessの導入

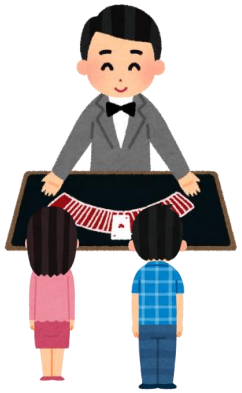
■ **プライベートモデル**

- 背に隠すなどしたプライベートな操作を許す
  - 秘匿置換　：プライベートに行う並べ替え操作
  - 通信　　：カードを手渡す操作
- イメージ：ババ抜き



パブリックモデルとプライベートモデル

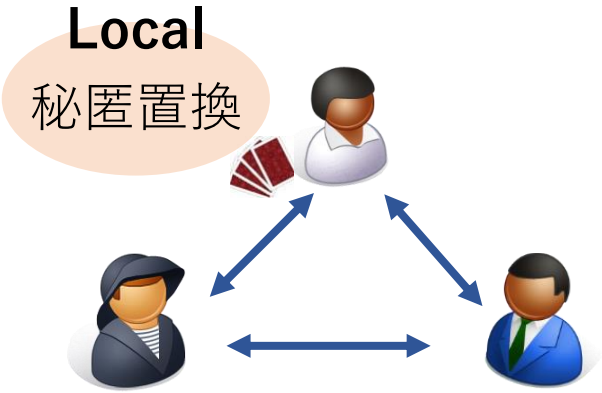
■ パブリックモデル
- すべての操作を公開する



不正なふるまいは
必ず検知できる
(不正対策が不要)

- 用いる操作
  - ✓公開置換
  - ✓公開反転（カードを裏返す操作）
  - ✓シャッフル

■ プライベートモデル
- プライベートな操作を許す



秘匿置換中の不正を
防ぐため
Semi-honestモデルの
前提が必要

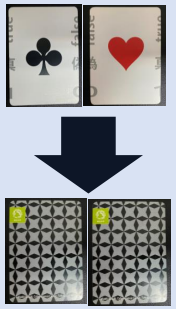
- 用いる操作
  - ✓公開置換
  - ✓公開反転
  - ✓秘匿置換
  - ✓通信（カードを手渡す操作）

操作モデルの比較

パブリックモデル

すべての
操作が公開

暗号化

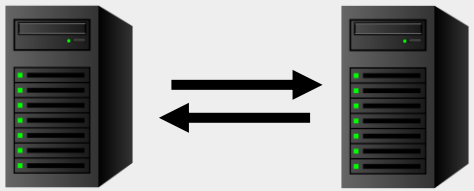


乱数生成
(public)

カードならではの
操作モデル

ギャップが
大きい

計算機ベース



暗号化

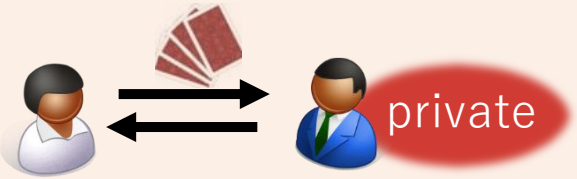
m

$\mathrm{Enc}(m, r)$

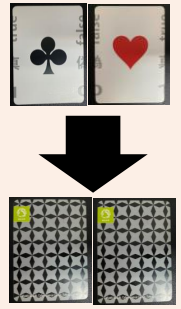
乱数生成
(private)
↓
r

ギャップが
小さい

プライベートモデル



暗号化

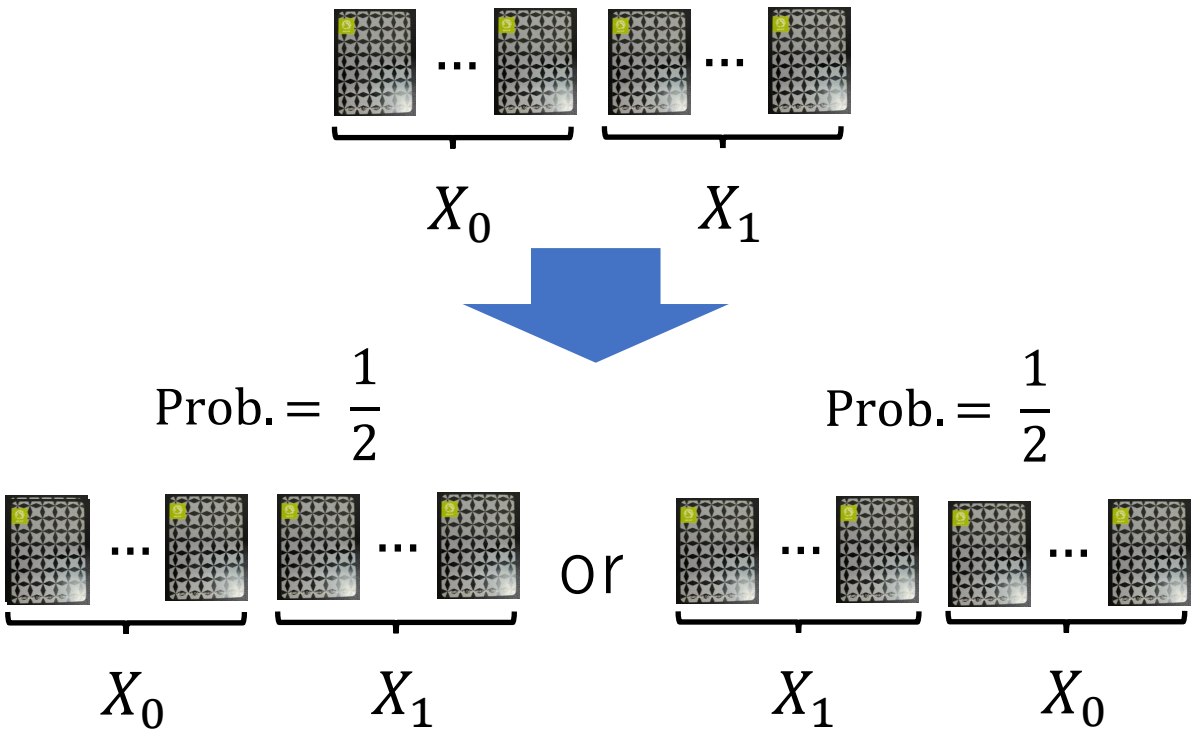


乱数生成
(private)

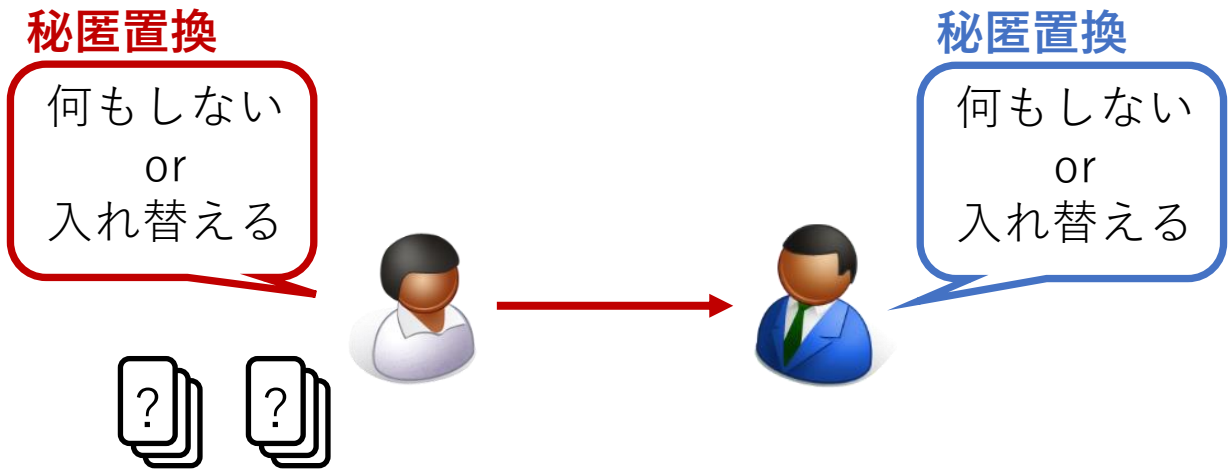
より計算機ベースに
近い操作モデル

プライベートモデルにおけるシャッフルの実現

■ シャッフル
- 例）ランダム二等分割カット



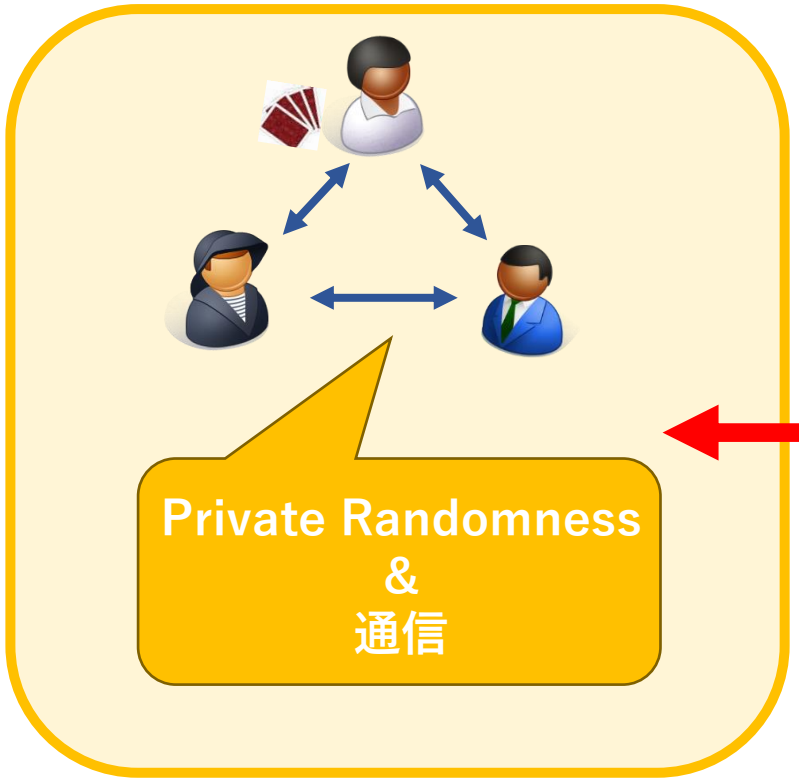
■ 秘匿置換
- 例）秘匿置換に基づく
  ランダム二等分割カットの実現



プライベートモデル下では
シャッフルを2つの秘匿置換と1回の通信からなる
操作であると解釈できる

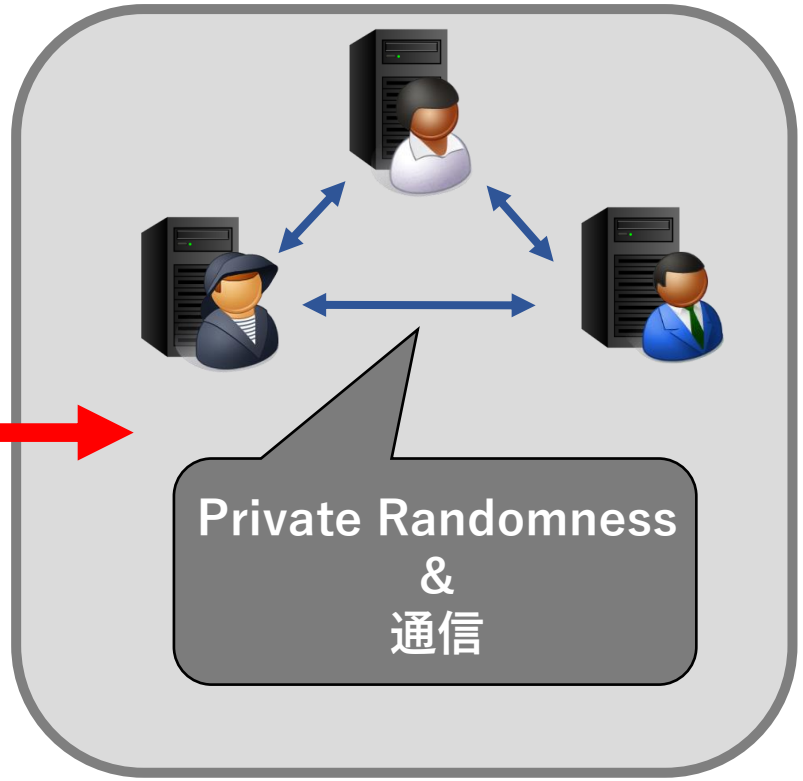
秘匿置換導入のメリット①:モデルのギャップ解消

プライベートモデルの
カードベース暗号



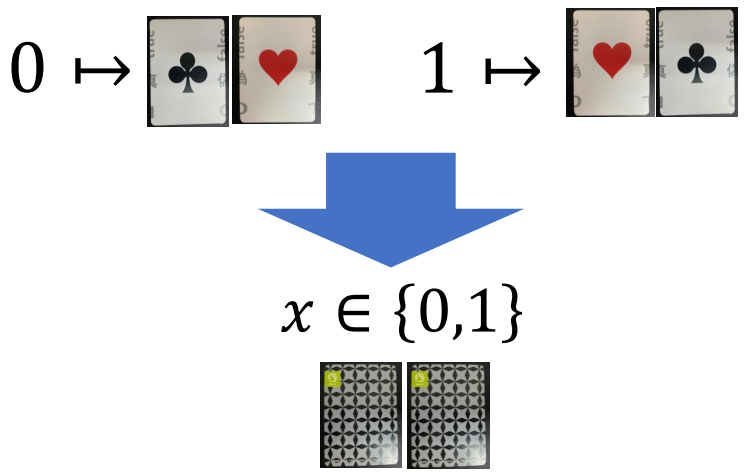
プロトコル構築の
技術を互いに活用
しやすくなる

通常の
暗号プロトコル



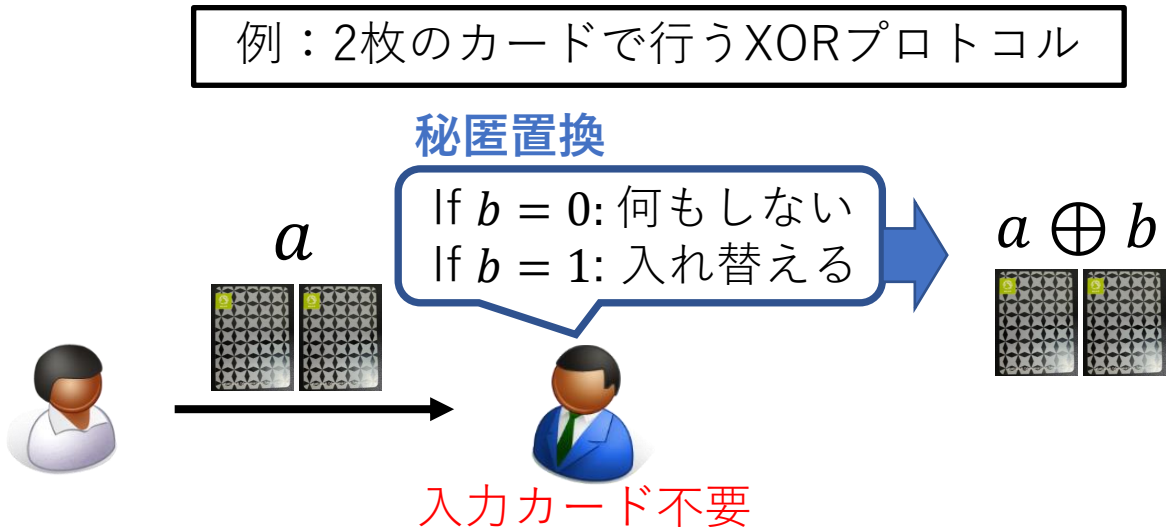
秘匿置換導入のメリット②: 入力カード枚数の削減

■ パブリックモデル
- すべての操作が公開
  - 入力には裏面のカードによるエンコーディングが必要



n-bit入力プロトコルには
少なくとも $2n$ 枚のカード必要

■ プライベートモデル
- プライベートな操作を許す
  - 入力に秘匿置換を用いることが可能



従来の下限値 $2n$ を下回る
カード枚数でプロトコルを実現可能に

プライベートモデルにおける主要な研究成果

国際会議での発表

■ 論理演算プロトコル (AND, XORなど)
- Ono-Manabe, Card-Based Cryptographic Protocols with the Minimum Number of Cards Using Private Operations, FPS2018.
- Ono-Manabe, Card-Based Cryptographic Protocols with the Minimum Number of Rounds Using Private Operations, DPM2019.

■ 金持ち比べプロトコル (2者間の大小比較)
- Nakai et al., Efficient Card-Based Cryptographic Protocols for Millionaires' Problem Utilizing Private Permutations, CANS2016.
- Ono-Manabe, Efficient Card-Based Cryptographic Protocols for the Millionaires' Problem Using Private Input Operations, AsiaJCIS2018.

■ 多数決プロトコル(Majority voting)
- Nakai et al., Four cards are sufficient for a card-based three-input voting protocol utilizing private permutations, ICITS2017.
- Watanabe et al., Card-based majority voting protocols with three inputs using three cards, ISITA2018.

■ 秘匿積集合プロトコル (Private set intersection)
- Doi et al., Card-based Cryptographic Protocols for Private Set Intersection, ISITA2022.

■ Malicious Security (秘匿置換中の不正対策)
- Manabe-Ono, Secure Card-Based Cryptographic Protocols Using Private Operations Against Malicious Players, SecITC2020.
- Abe-Iwamoto-Ohta, How to detect malicious behaviors in a card-based majority voting protocol with three inputs, ISITA2020.

プライベートモデルにおける主要な研究成果

国際会議での発表

■ 論理演算プロトコル (AND, XORなど)

メリット①に対応

- Ono-Manabe, Card-Based Cryptographic Protocols with [illegible]PS2018.
- Ono-Manabe, Card-Based Cryptographic Protocols with [illegible]DPM2019.

計算機ベースプロトコルのアイデアを基に
実現されたカードベースプロトコルを提案

■ 金持ち比べプロトコル (2者間の大小比較)

- Nakai et al., Efficient Card-Based Cryptographic Protocols for Millionaires' Problem Utilizing Private Permutations, CANS2016.
- Ono-Manabe, Efficient Card-Based Cryptographic Protocols for the Millionaires' Problem Using Private Input Operations, AsiaJCIS2018.

■ 多数決プロトコル(Majority voting)

- Nakai et al., Four cards are sufficient for a card-based three-input voting protocol utilizing private permutations, ICITS2017.
- Watanabe et al., Card-based majority voting protocols with three inputs using three cards, ISITA2018.

3入力多数決プロトコルを4枚のカードで実現
（パブリックモデルでは少なくとも６枚必要）

■ 秘匿積集合プロトコル (Private set intersection)

- Doi et al., Card-based Cryptographic Protocols for Private Set Inter[illegible]

■ Malicious Security (秘匿置換中の不正対策)

メリット②に対応

- Manabe-Ono, Secure Card-Based Cryptographic Protocols Using Private Operations Against Malicious Players, SecITC2020.
- Abe-Iwamoto-Ohta, How to detect malicious behaviors in a card-based majority voting protocol with three inputs, ISITA2020.

秘匿置換の導入で得られるメリットの例として2つのプロトコルを紹介

本発表の流れ

■背景: シャッフルに基づくカードベース暗号

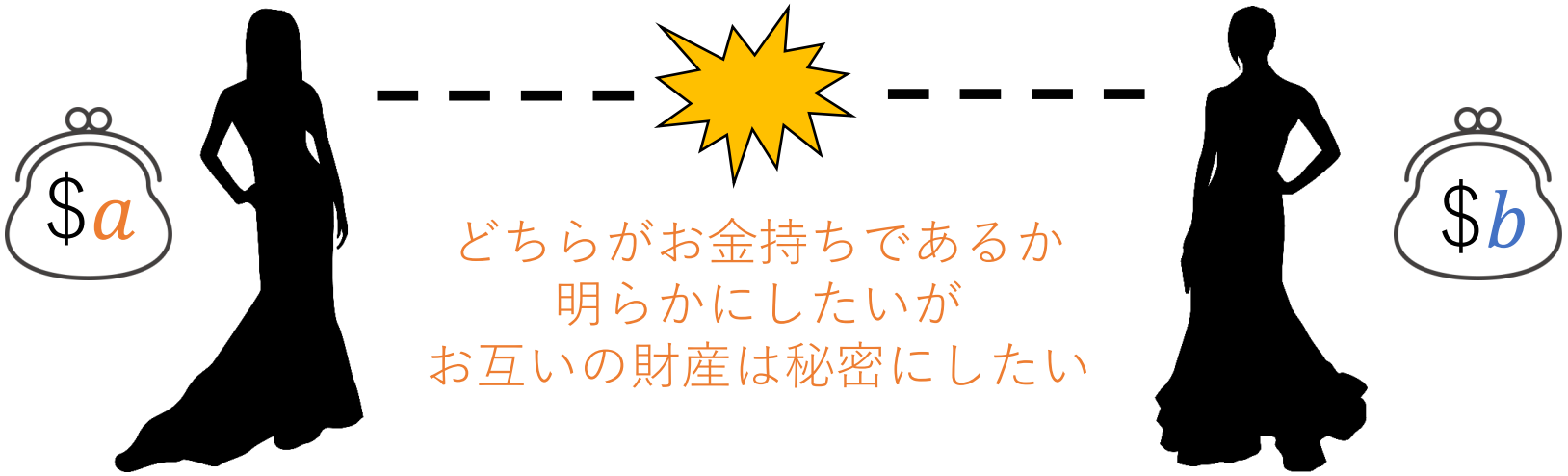
■秘匿置換に基づくカードベース暗号

■秘匿置換に基づくカードベースプロトコルの紹介
- 金持ち比べプロトコル
- 3入力多数決プロトコル

メリット①：モデルのギャップ解消の例

カードを用いた
金持ち比べプロトコル

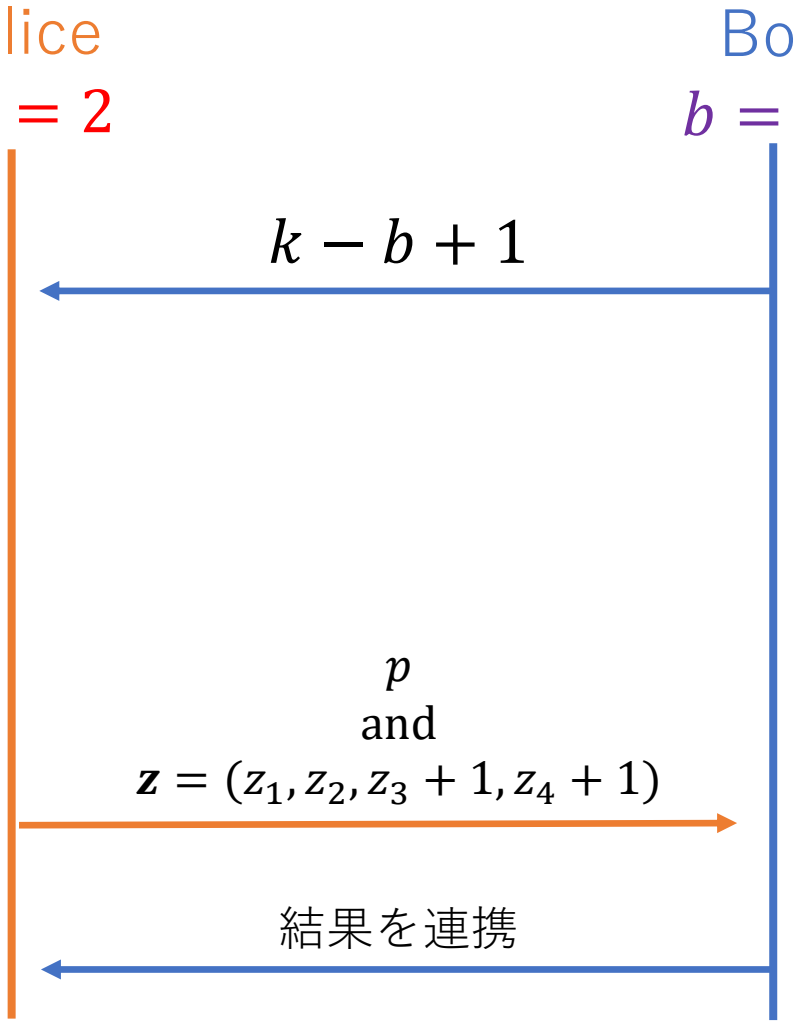
金持ち比べプロトコルとは



2値の大小比較プロトコル で解決

Yaoの金持ち比べプロトコル（Original）

$0 \leq a, b \leq 4$



$x \leftarrow [2^N - 1]$

$k \coloneqq \mathrm{Enc}_A(x)$

For $u = 1$ to m

$y_u \coloneqq \mathrm{Dec}_A(k - b + u)$

$p \leftarrow [2^{\frac{N}{2}} - 1]$ -(★)

For $u = 1$ to m

$z_u \coloneqq y_u \bmod p$

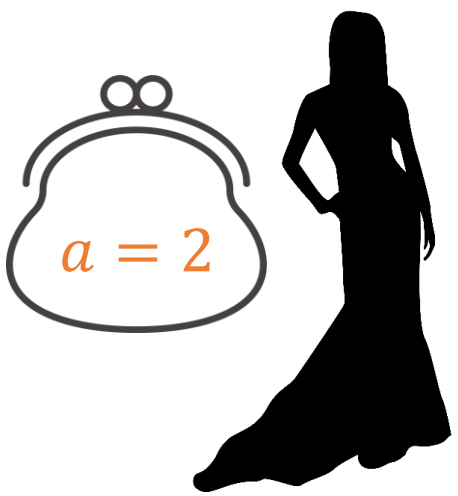
if $\exists i, j, |z_i - z_j| \leq 1$, then 次の手順へ
o/w (★)からリスタート

ベクトル $\boldsymbol{z}$ の b 番目の値 z_b を確認
if $z_b \equiv x \bmod p$, then $a > b$
o/w $a \leq b$

Yao, A.: Protocols for secure computations, IEEE Symposium on FOCS, IEEE, 1982.

Yaoの金持ち比べプロトコルの概要 (1/2)

$0 \leq a, b \leq 4$



4つの暗号文

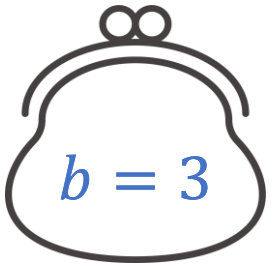
④ +1

③ +1

暗号文を破壊

② ← $a = 2$ 番目

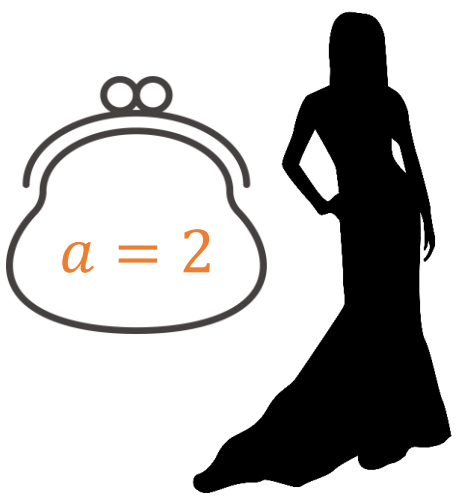
①



Yaoの金持ち比べプロトコルの概要 (2/2)

$0 \leq a, b \leq 4$

■ b番目を復号
- 正しく復号できる: $a \geq b$
- 正しく復号できない: $a < b$



送信

4つの暗号文

④

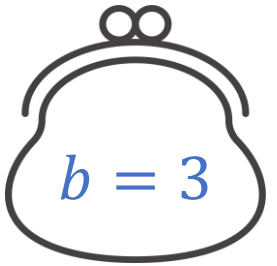
③

正しく
復号できない

②

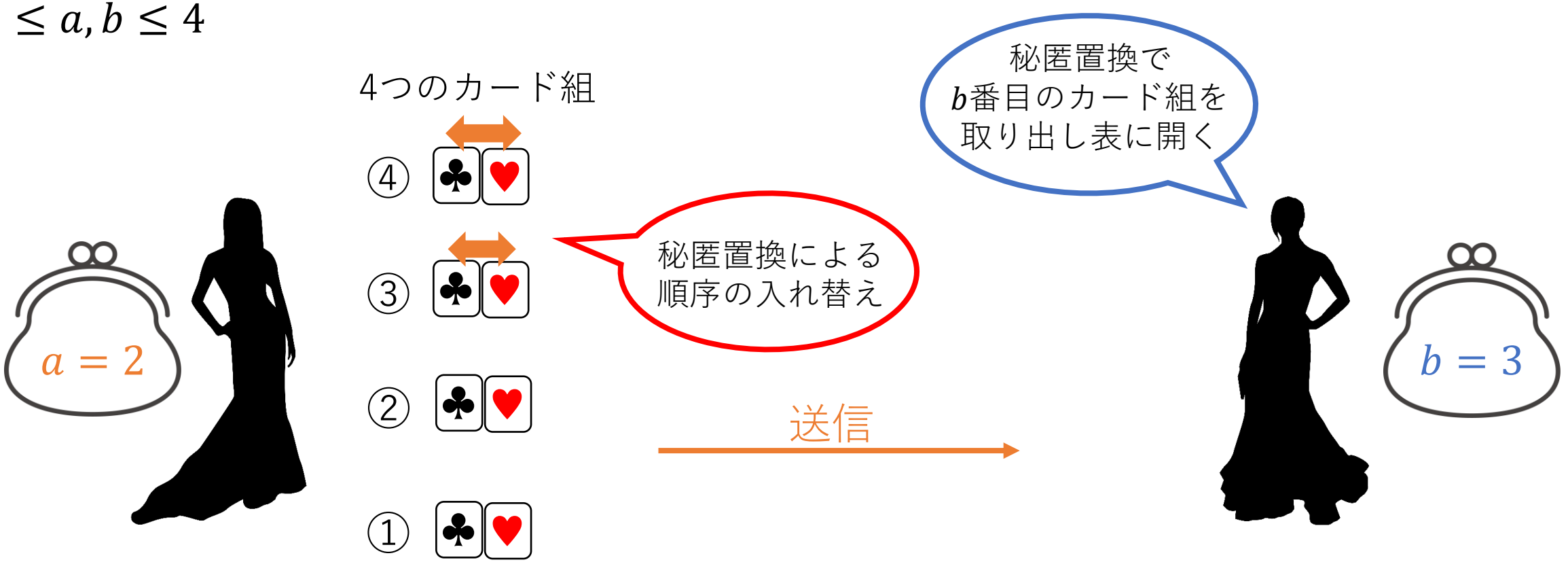
①

正しく
復号できる



カードを用いた金持ち比べプロトコル(Yaoベース)

$0 \leq a, b \leq 4$



Yaoの方式と同様の仕組みで，金持ち比べプロトコルを実現

メリット②：入力カード枚数の削減の例

4枚のカードを用いた
3入力多数決プロトコル

秘匿置換を用いた3入力多数決プロトコル

- 入力値: Alice(a), Bob(b), Carol(c) where $a, b, c \in \{0,1\}$
- 出力値:

$$\mathrm{maj}_3(a,b,c) = \begin{cases} 0 & \text{if } a+b+c \leq 1 \\ 1 & \text{if } a+b+c \geq 2 \end{cases}$$

- プロトコルのアイデア
  - 3入力多数決とAND/ORの関係

If $c = 0$: $a + b + c \geq 2 \Leftrightarrow a + b \geq 2 \Leftrightarrow a \wedge b = 1$

If $c = 1$: $a + b + c \geq 2 \Leftrightarrow a + b \geq 1 \Leftrightarrow a \vee b = 1$

- 多数決プロトコルの戦略
  1. AliceとBobで$a \wedge b$及び$a \vee b$を算出しCarolへ渡す
  2. Carolが入力値に従いどちらかを出力とする

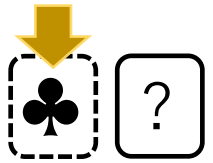
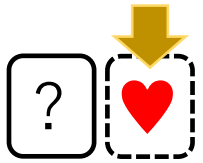
4-card AND/OR Hybrid プロトコル

0. Alice: ♣♥, Bob: ♣♥

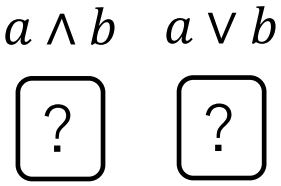
1. Aliceフェーズ
   - If $a = 0$: 裏面の ♣ をBobへ送信
   - If $a = 1$: 裏面の ♥ をBobへ送信

2. Bobフェーズ
   - If $b = 0$: 裏面の ♣ を左に配置
   - If $b = 1$: 裏面の ♥ を右に配置

秘匿置換

$0 \Rightarrow$  $1 \Rightarrow$ 

3. Outputフェーズ
   - $(a \wedge b, a \vee b)$ を表すカード組を得る



■ 3入力多数決プロトコル
- 3人目のCarolが自身の入力値に従い秘匿置換でどちらか一方を出力

a	b	結果の並び
0	0	♣ ♣
0	1	♣ ♥
1	0	♣ ♥
1	1	♥ ♥

♣ $= 0$

♥ $= 1$

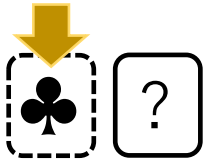
4-card 3入力多数決プロトコル

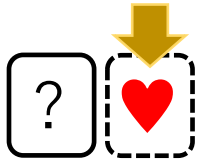
0. Alice: ♣♥, Bob: ♣♥, Carol, 入力カード不要

1. Aliceフェーズ
   - If $a = 0$: 裏面の ♣ をBobへ送信
   - If $a = 1$: 裏面の ♥ をBobへ送信

秘匿置換

2. Bobフェーズ
   - If $b = 0$: 裏面の ♣ を左に配置し，Carolへ送信
   - If $b = 1$: 裏面の ♥ を右に配置し，Carolへ送信

$0 \Rightarrow$ 

$1 \Rightarrow$ 

秘匿置換

3. Carolフェーズ
   - If $c = 0$: 左のカード$(a \wedge b)$を出力
   - If $c = 1$: 右のカード$(a \vee b)$を出力

a	b	結果の並び
0	0	♣ ♣
0	1	♣ ♥
1	0	♣ ♥
1	1	♥ ♥

♣ $= 0$

♥ $= 1$

まとめ

■本発表のまとめ

- パブリックモデル（シャッフルに基づくカードベース暗号）
  - ➢全ての操作を公開で行うことを前提とした操作モデル
  - ➢シャッフルで乱数生成を行うことで秘匿性を達成

- プライベートモデル（秘匿置換に基づくカードベース暗号）
  - ➢シャッフルの代わりに秘匿置換と通信でプロトコルを構成
    - ➢通常の暗号プロトコルがベースとするprivate randomnessを活用
  - ➢秘匿置換導入の利点
    - ① モデル間のギャップを解消したことで通常の暗号プロトコルのアイデアを活用することがより容易に（例として，金持ち比べを紹介）
    - ② 秘匿置換による入力値表現で，パブリックモデルにおけるカード枚数下限値を下回る枚数でプロトコルを構成可能（例として，3入力多数決を紹介）

今後の研究課題

■研究課題の例

① 計算機ベースからカードベースへ変換可能なプロトコルの発見
- 金持ち比べの例のように本質的なアイデアを捉えた方式を構成できれば，元の計算機ベース方式の理解促進のための教材としても活用できることが期待

② その他の秘匿操作の導入による効果の検証
- カードゲームの中で用いられる秘匿操作は秘匿置換だけではない
- 秘匿置換以外の秘匿操作の導入がプロトコル効率化に有効に働くかについての研究
  - ➢例）自分だけがカードの表面を見るチラ見操作(Private Reveal)

③ 秘匿操作を用いたカードベースZKPの構成
- 今回は秘密計算に焦点を当てているが，秘匿操作はZKPの構成にも有効に働くかもしれない