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
2024/5/22(水)　15:45 - 16:25

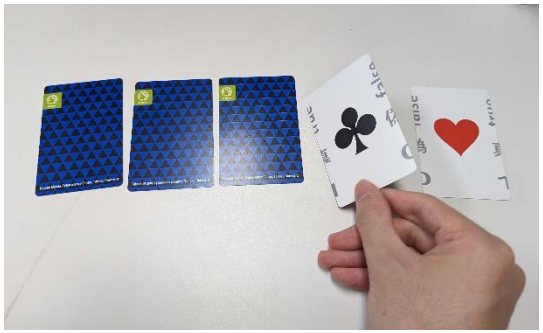
# 3Dプリンタのカードベース暗号への応用

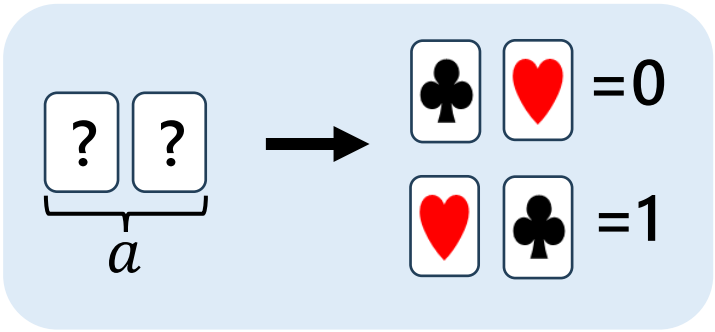
伊藤優樹（東北大）

# 目次

# カードベース暗号とその実装

- カードベース暗号
  - **物理的なカード組**を用いて秘密計算等の暗号機能を実現
- コミットメント
  - 秘密計算の入力ビットを表現するカード列

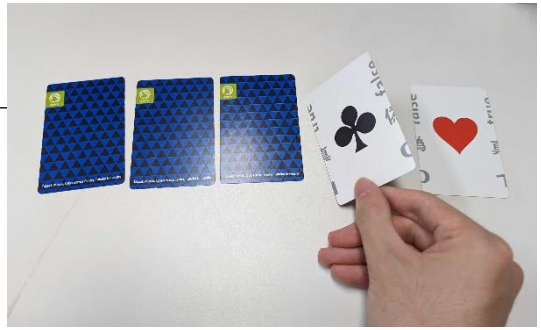




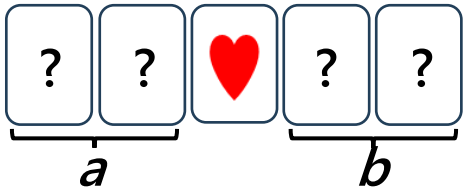

- **Five-Card Trick [DB90]**
  - 歴史上最初のカードベース暗号プロトコル
  - **2入力のANDの秘密計算を5枚のカードで実現**

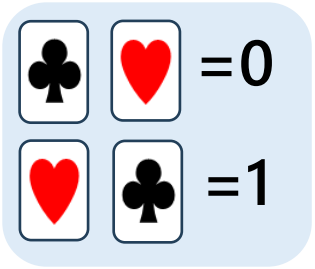
[DB90] Den Boer, B.: More Efficient Match-Making and Satisfiability The Five Card Trick, Advances in Cryptology— EUROCRYPT '89 (Quisquater, J.-J. and Vandewalle, J., eds.), LNCS, Vol. 434, Berlin, Heidelberg, Springer, pp. 208– 217(1990).

# Five-Card Trick

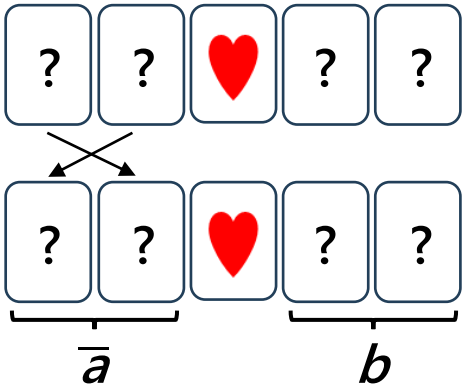


- 初期状態

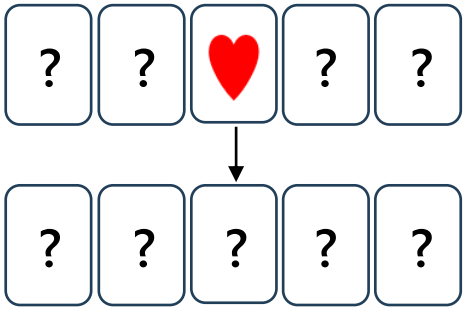


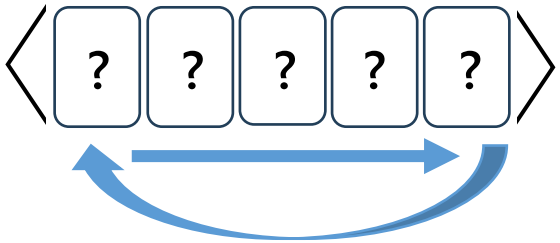

(1)左2枚のカードを入れ替え




(2)中央の♥を裏返す

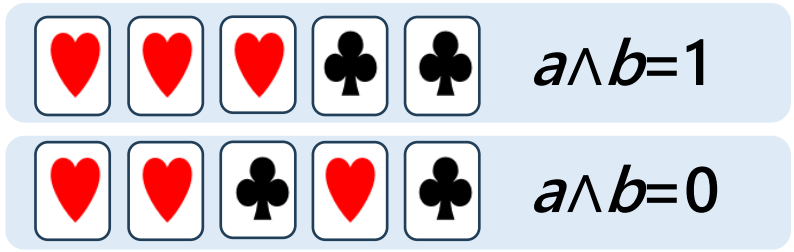



(3)ランダムカットを適用



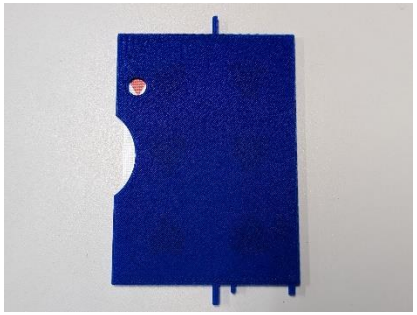

(4)カードをめくり$a \wedge b$を得る

例



# 3Dプリンタで作成した制作物

- 3Dプリンタを用いてカードベース暗号プロトコルの実装に有用な**ケース**や**装置**の設計・作成



  - 部分開示用ケース
    - 部分開示の実装を**容易かつ確実**にし，効率的なプロトコルを構成

  - **Five-Card Trick用オープン装置(部分開示)**
    - トランプカードでの**Five-Card Trick**実行時，最終ステップで**5**枚をめくる際に利用可能

  - **Five-Card trick用オープン装置(2色カード)**
    - **2**色カード組での**Five-Card Trick**実行時，最終ステップで**5**枚をめくる際に利用可能

# 特殊なシャッフル用ケース

- 特殊なシャッフル用ケース
  - 複雑なシャッフル実装のためのケース
  - 既存の5枚コピープロトコルを**安全に**実行

- 特殊ケースの追加機能・装置
  - ケース上部にカードを収容する機構
  - カードを取り出すのための補助装置

- 対称関数の秘密計算への応用

| | カード束作成回数(回) | カード枚数(枚) |
|---|---|---|
| Ruangwises, Ito[RI21] | $n^2/2 + 3n/2 - 2$ | 2n+2 |
| 提案手法 | 2n-2 | 2n+1 |

  - 本成果は国際会議 UCNC2024 (6/17-21@韓国)で発表予定

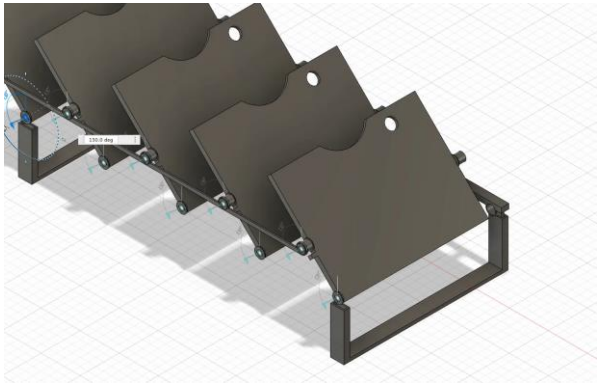
[RI21] Ruangwises, S. and Itoh, T.: Securely computing the nvariable equality function with 2n cards, Theor. Comput. Sci., Vol. 887, pp. 99–110 (2021).

# 目次

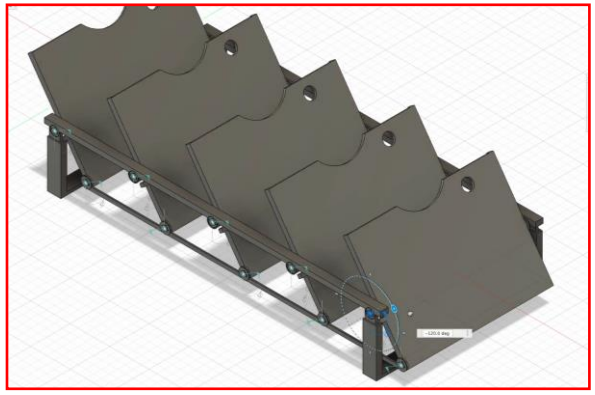
1. はじめに
2. Five-Card Trick用オープン装置
3. 特殊ケースの作成とコピープロトコル
4. 特殊ケースによるソート機能
5. 特殊ケースによる対称関数の秘密計算
6. まとめ

# オープン装置の設計と作成

- 作成における要件
  - 一度の操作で**5枚同時にオープン**する機構
    - 実行の楽しさ，視覚的な魅力の創出
  - すべてのパーツが家庭用**3D**プリンタで作成可能
    - **部品の調達が不要**
    - **誰でも容易に**作成可能
- オープン装置の構造の設計
  - **視覚的な魅力**についての検討
    - **3D CAD**のアセンブリ機能を用いて**シミュレーション**で動作を確認



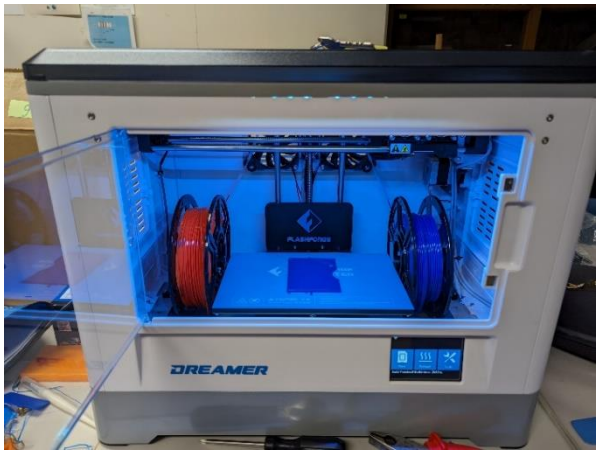
回転軸がケース端



回転軸がケース中央

# オープン装置の設計と作成

- カードホルダーの設計
  - ホルダーとカードの間に余分な隙間が無いよう**正確な寸法**
  - 操作中に**カードが外れず**, かつ**脱着がスムーズ**な構造
    - 脱落防止のツメ
    - カード挿入部の角度調整
- **3D**プリンタでの作成
  - **家庭用3Dプリンタ**(熱溶解積層：**FFF**方式) を用いて作成
  - **PLA**フィラメントを使用



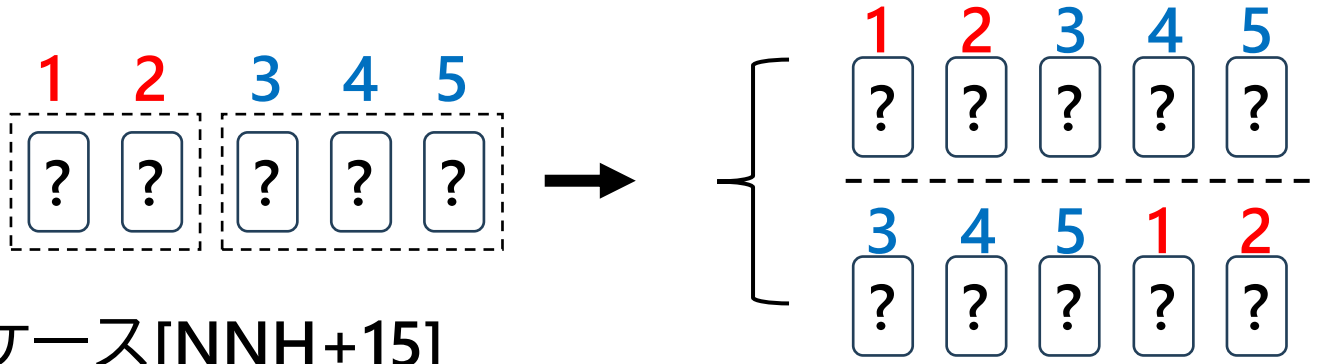

3Dプリンタでの作成の様子

3Dプリンタで出力後組み立てたオープン装置

# 目次

# 複雑なシャッフルと特殊ケース

- 複雑なシャッフルの例　(shuf, {id,(1 4 2 5 3)})
  - **左2枚と残り3枚**を束とし, 1/2の確率で入れ替えるシャッフル
  - **人間の手のみでの実装**は, 束の枚数の違いから**困難**



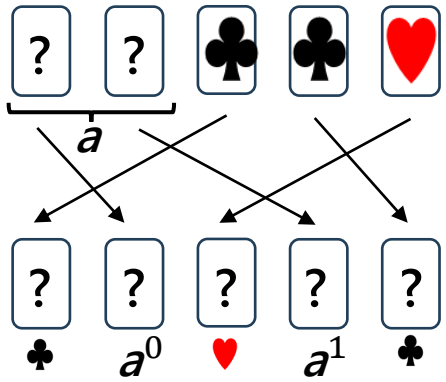

- 特殊ケース[NNH+15]
  - (shuf, {id,(1 4 2 5 3)})の実装方法として言及されたカードケース
  - ケースを重ね, 中のカード束を1つに結合

[NNH+15] Nishimura, A., Nishida, T., Hayashi, Y., Mizuki, T. and Sone, H.: Five-Card Secure Computations Using Unequal Division Shuffle, Theory and Practice of Natural Computing (Dediu, A.-H., Magdalena, L. and Martín-Vide, C., eds.), LNCS, Vol. 9477, Cham, Springer, pp. 109–120(2015).

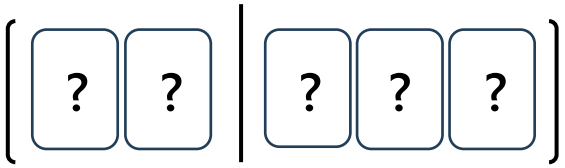
# コピープロトコル[NNH+15]

## (shuf, {id,(1 4 2 5 3)})を用いたコミットメントのコピー

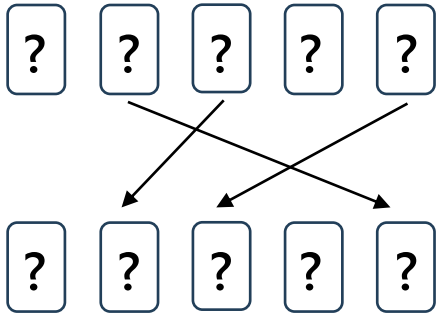
(1)カードを裏返し, 入れ替え




(2) (shuf, {id,(1 4 2 5 3)})を適用

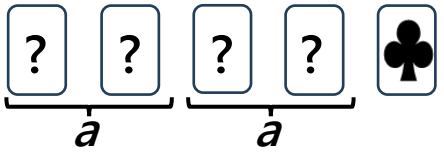



(3) カードを入れ替え

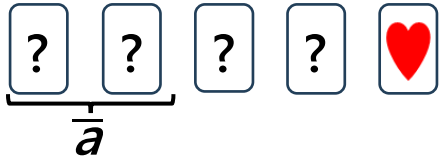



(4) 5枚目のカードをめくる

(a) ♣ の場合, 1,2と3,4枚目が$a$となる



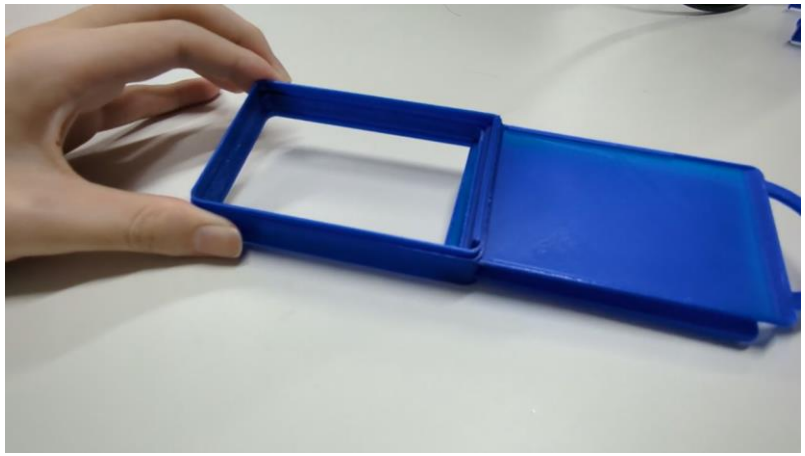

(b) ♥ の場合, 1,2枚目を入れ替え, (1)に戻る




[NNH+15] Nishimura, A., Nishida, T., Hayashi, Y., Mizuki, T. and Sone, H.: Five-Card Secure Computations Using Unequal Division Shuffle, Theory and Practice of Natural Computing (Dediu, A.-H., Magdalena, L. and Martín-Vide, C., eds.), LNCS, Vol. 9477, Cham, Springer, pp. 109–120(2015).

# 特殊ケースの作成

- 特殊ケースの作成とプロトコルの実装
  - 3Dプリンタを用いて特殊ケースを作成
  - コミットメントのコピープロトコル[NNH+15]を実際に実行し，複雑なシャッフルにおけるケースの有用性を検証

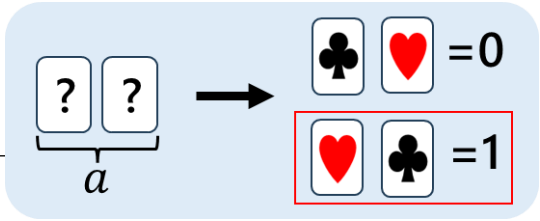


作成したケース
蓋と底がスライド可能

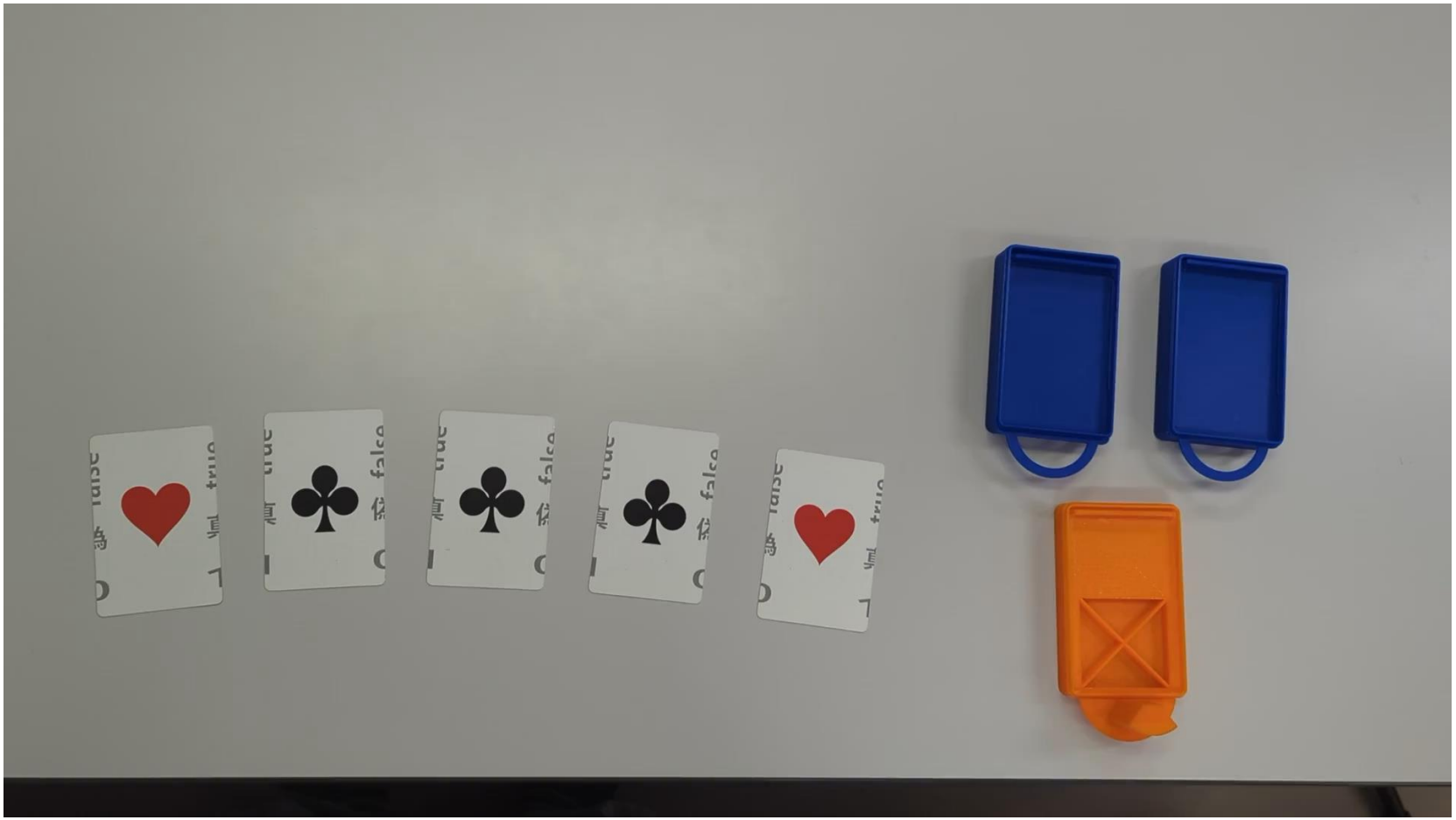
蓋と底のスライドによる、
ケース内のカード束の結合

[NNH+15] Nishimura, A., Nishida, T., Hayashi, Y., Mizuki, T. and Sone, H.: Five-Card Secure Computations Using Unequal Division Shuffle, Theory and Practice of Natural Computing (Dediu, A.-H., Magdalena, L. and Martín-Vide, C., eds.), LNCS, Vol. 9477, Cham, Springer, pp. 109–120(2015).

# 特殊ケースと用いた実装の様子




- 入力を1としたコピープロトコル
  - 5枚目がクローバーの場合

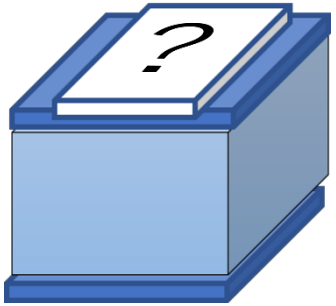


# 目次

1. はじめに
2. Five-Card Trick用オープン装置
3. 特殊ケースの作成とコピープロトコル
4. 特殊ケースによるソート機能
5. 特殊ケースによる対称関数の秘密計算
6. まとめ

# 特殊ケース利用における発展手法

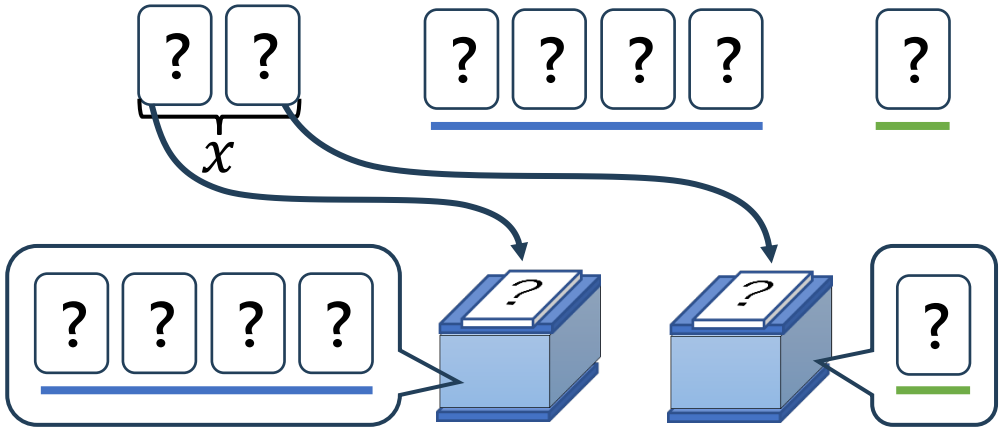
- ケース上部にカードを固定する手法[SCIS2022]
  - 輪ゴム等で固定する方法が示されている

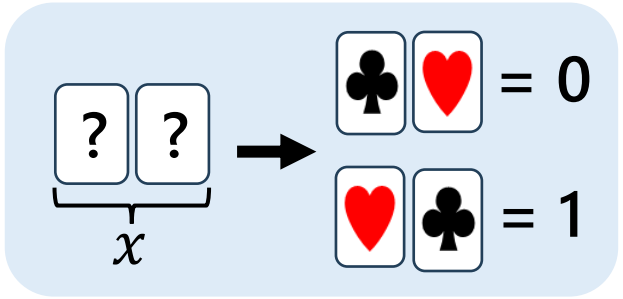



- 3Dプリンタで作成した特殊ケース
  - 上面に固定する機構を付与
  - シャッフル操作においても安定してカードを固定

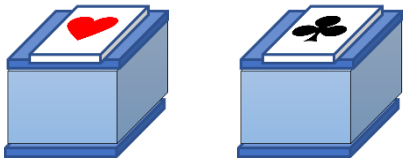
[SCIS2022] 四方隼人, 豊田航大, 宮原大輝, 水木敬明: 最小のカード枚数による対称関数の秘密計算について, 2022 年暗号と情報セキュリティシンポジウム,1F4-3 (2022).

# [SCIS2022]の一般化: サイズの異なる束のソート



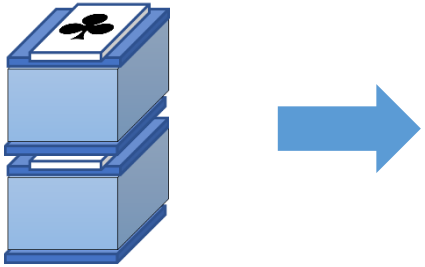




かきまぜて，上部のカードをめくる



xの値を秘密にしたまま
サイズの異なる束をソート

♥のハコを下にして結合



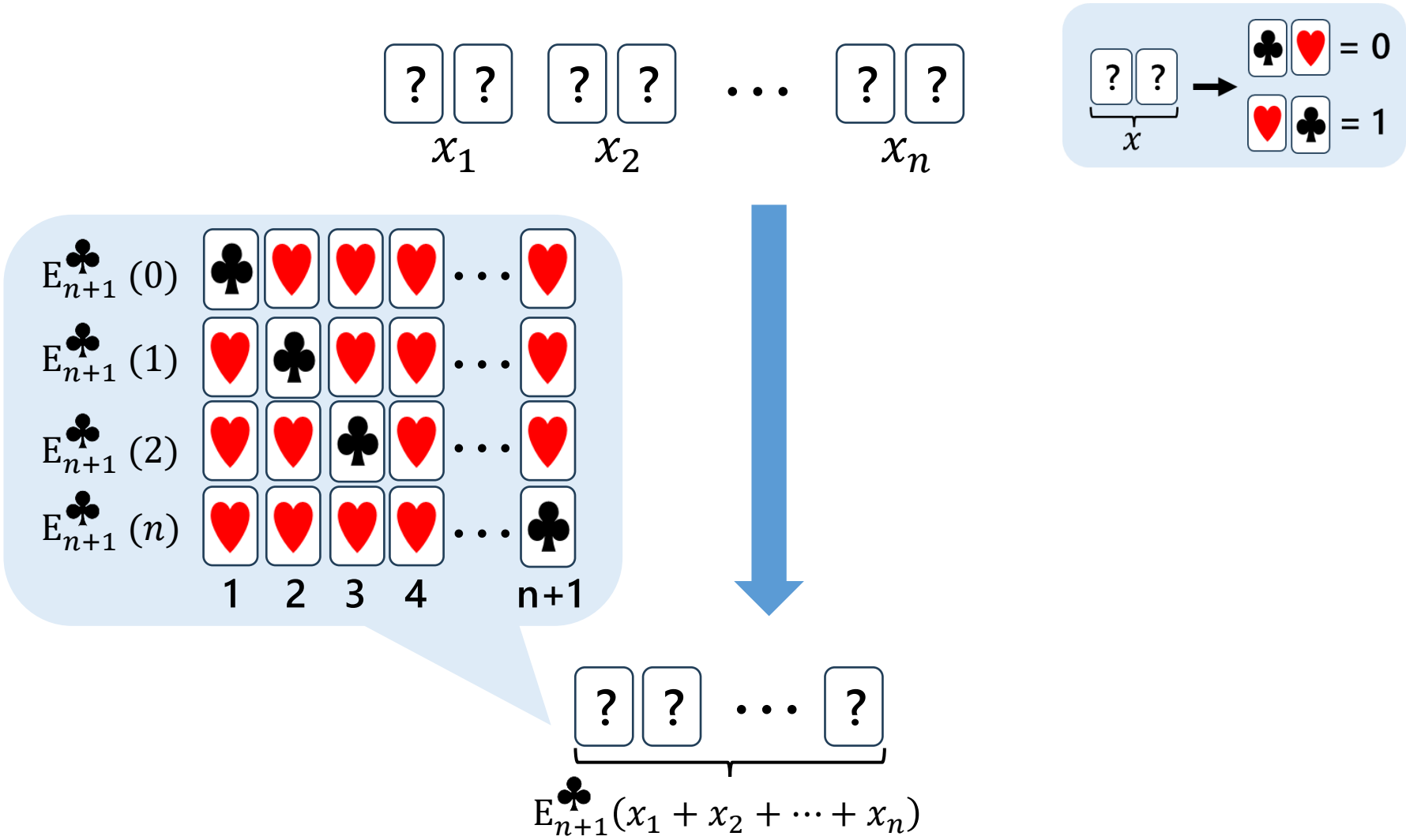
$x = 0$

$x = 1$

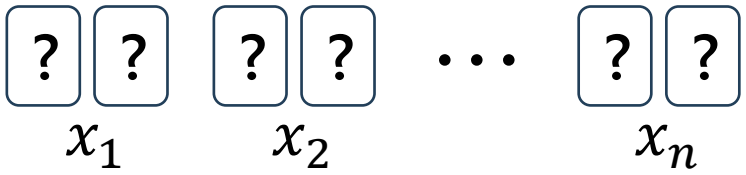
[SCIS2022] 四方隼人, 豊田航大, 宮原大輝, 水木敬明: 最小のカード枚数による対称関数の秘密計算について, 2022 年暗号 と情報セキュリティシンポジウム,1F4-3 (2022).

# 目次

# 対称関数の秘密計算(コミットメントの加算)

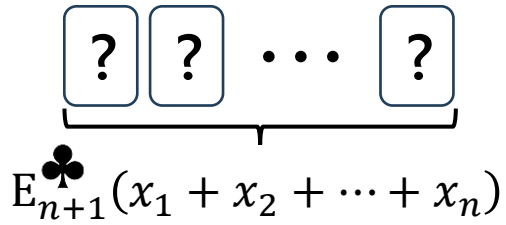


# 対称関数の秘密計算




<u>既存プロトコル[RI21]</u>
- シャッフル
  - パイルシフティングシャッフル
- 束の作成回数
  - $n^2/2 + 3n/2 - 2$ 回

<u>提案プロトコル</u>
- シャッフル
  - 特殊ケースを使用
- 束の作成回数
  - $2n - 2$ 回

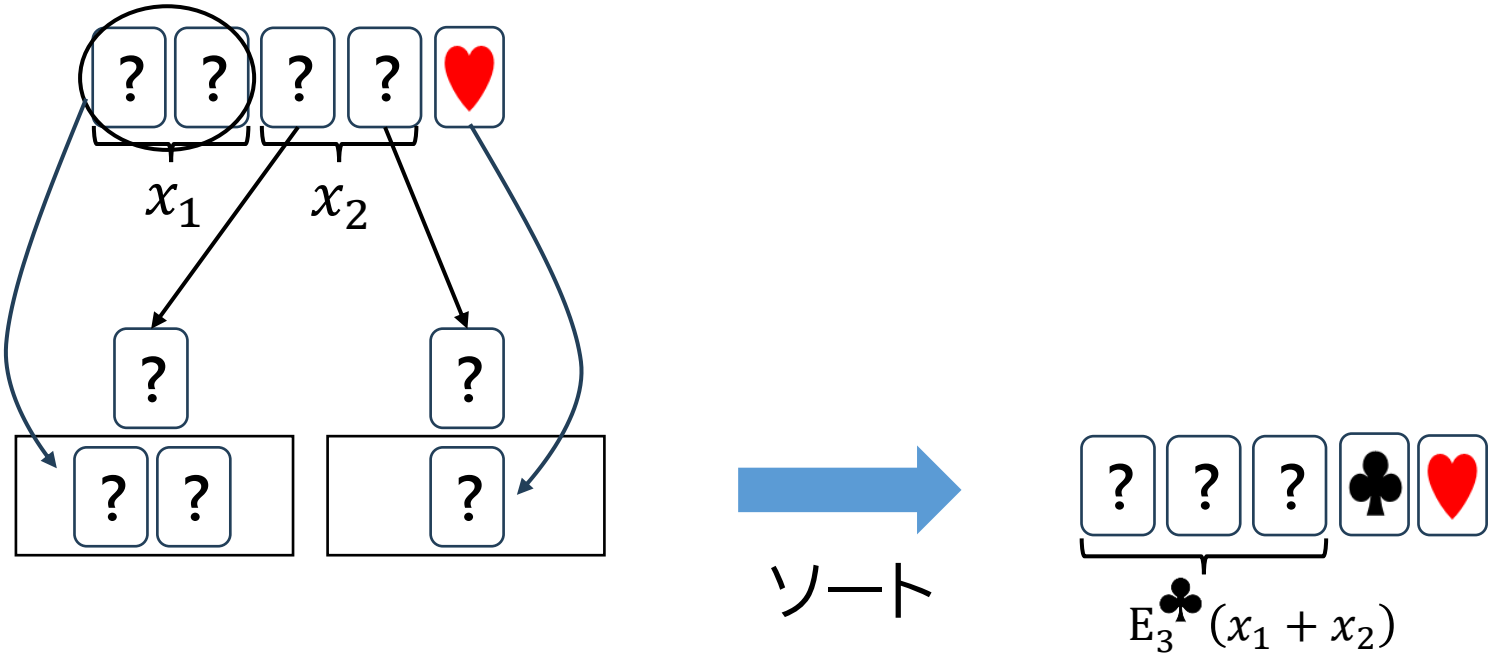



[RI21] Ruangwises, S. and Itoh, T.: Securely computing the nvariable equality function with 2n cards, Theor. Comput. Sci., Vol. 887, pp. 99–110 (2021).

# 対称関数の秘密計算

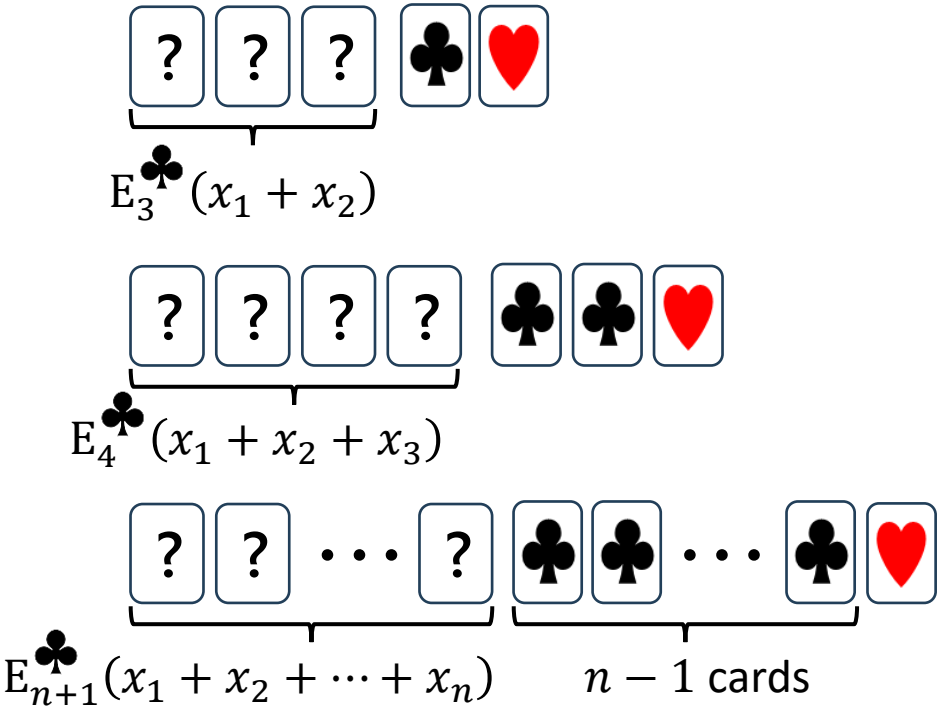
- 特殊ケースを用いたコミットメントの加算
  - 2n+1枚のカードと2つの特殊ケースを使用

(1) $x_1$と$x_2$のコミットメントを加算し，$\mathrm{E}_3^{\clubsuit}(x_1 + x_2)$を得る



# 対称関数の秘密計算

## (2)同様の作業を繰り返し，$x_n$まで加算する

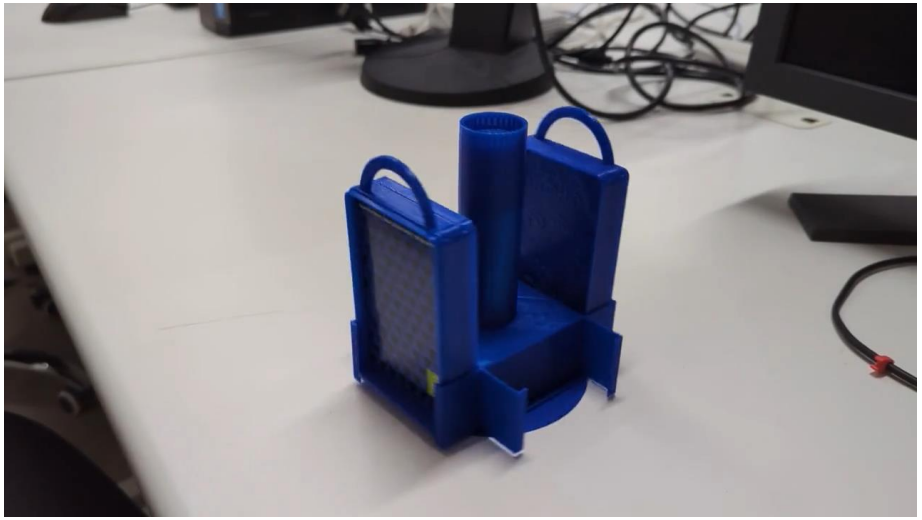



- カード束作成回数の削減
  - Ruangwisesら：$\mathrm{n}^2/2 + 3\mathrm{n}/2 - 2$ 回
  - 提案手法　　：2n-2 回
- カード枚数の削減
  - Ruangwisesら：2n+2 枚
  - 提案手法　　：2n+1 枚

[RI21] Ruangwises, S. and Itoh, T.: Securely computing the nvariable equality function with 2n cards, Theor. Comput. Sci., Vol. 887, pp. 99–110 (2021).

# 特殊ケース操作のための補助装置

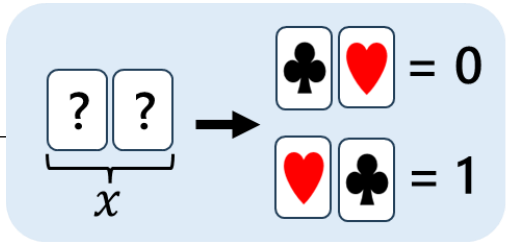
- 補助装置の作成
  - ケースシャッフル器
    - 手のみでは実装が難しいケースのシャッフル操作をサポート
    - 装置が高速で回転することでシャッフル操作を実現
  - カード束の結合と取り出しの補助装置
    - カード取り出しの際, ケースを逆さまにせず安全に排出
    - 束の結合と取り出しの操作を確実化

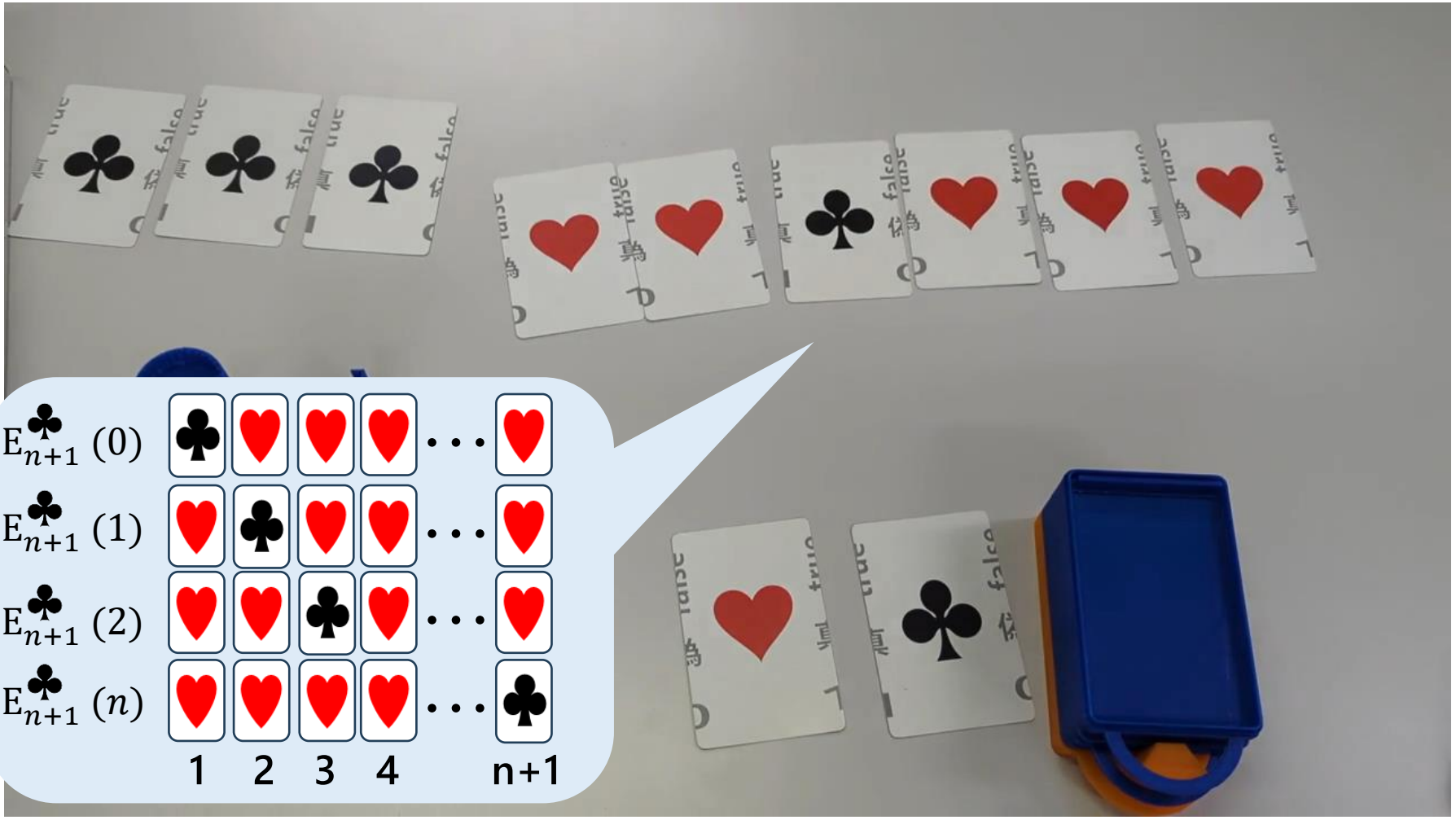


ケースシャッフル器

カード束の取り出し補助装置

# 5入力加算関数の実装


? ?
x
= 0
= 1


$E^{\clubsuit}_{n+1}$ (0)
$E^{\clubsuit}_{n+1}$ (1)
$E^{\clubsuit}_{n+1}$ (2)
$E^{\clubsuit}_{n+1}$ (n)
1 2 3 4 n+1

# 目次

# 5. まとめ

- 本研究での貢献
  - カードベース暗号プロトコルの実装に役立つケース・装置を**3D**プリンタを用いて作成
    - 部分開示ケース
    - **Five-Card Trick**用オープン装置
    - 特殊なシャッフル用ケース
      - ケース操作のための補助装置
  - 特殊ケースによる対称関数の秘密計算の実装
    - カード束作成回数, カード枚数の削減

- おわりに
  - 秘密計算・高機能暗号の社会への普及のために *
    - 暗号機能の意味・意義が幅広いステークホルダーに理解される必要

→ カードベース暗号とその実装が一助となることを期待

* 花岡悟一郎,岩本 貢,渡邉洋平,水木敬明,安部芳紀, 品川和雅,新井美音,矢内直人: 高機能暗号の社会展開 を促進する物理・視覚暗号,電子情報通信学会論文誌 A, Vol. J106-A, No. 8, pp. 214–228 (2023).