部分開示操作を用いた多入力 AND プロトコル

本多 由昂[1,a)]　品川 和雅[2,3,b)]

概要：カードベースプロトコルとは、物理的なカード組を用いて秘密計算を行う暗号プロトコルである。部分開示操作は、伏せられたカードのオモテ面の一部のみを明らかにする暗号プロトコル操作である。この操作は、Miyahara と Mizuki が (IJTCS-FAW 2022) でトランプカードのスートのみを開示する操作として導入し、その後、著者ら (IWSEC 2024) によってカードオモテ面の任意の位置を開示する操作へと一般化された。部分開示操作を用いて、Miyahara と Mizuki はランダムカット 1 回の 4 枚 2 入力 AND プロトコルを提案し、著者ら（CANS 2025）はランダムカット 2 回の 6 枚 3 入力 AND プロトコルおよびランダムカット 3 回の 8 枚 4 入力 AND プロトコルを提案した。本論文では、部分開示操作を用いてランダムカット $(n-1)$ 回の $2n$ 枚 n 入力 AND プロトコルを提案する。

キーワード：カードベース暗号、トランプカード、非コミット型、部分開示操作

Multi-Input AND Protocols Using Partial Open Actions

Yoshiaki Honda[1,a)]　Kazumasa Shinagawa[2,3,b)]

Abstract: A card-based protocol is a type of cryptographic protocol that uses a physical set of cards to perform secret computations. A partial-open action is a cryptographic protocol that reveals only part of the face of a face-down card. Miyahara and Mizuki (IJTCS-FAW 2022) introduced this operation as a way to reveal the suit of a playing card. The authors (IWSEC 2024) then generalized it to reveal any position on the face of a card. Miyahara and Mizuki used the partial disclosure operation to propose a four-card, two-input AND protocol with one random cut. The authors (CANS 2025) proposed a six-card, three-input AND protocol with two random cuts and an eight-card, four-input AND protocol with three random cuts. In this paper, we propose an n-input AND protocol with n random cuts using partial disclosure operations.

Keywords: Card-based cryptography, Playing cards, Committed-format, Partial-open actions

1. はじめに

1.1 背景

秘密計算とは、入力値を秘匿したまま計算を実行し、出力値のみを得る暗号技術である。秘密計算は通常コンピュータ上での実装を想定されるが、物理的なカード組を用いて秘密計算を実現する研究も知られており、そのような研究分野をカードベース暗号と呼ぶ。

歴史上最初に提案されたカードベースプロトコルは den Boer [1] による five-card trick であり、これは 2 入力 AND プロトコルである。このプロトコルは、5 枚の 2 色カード組 ♡♡♡♣♣ と、ランダムカットという最も基本的なシャッフルを 1 回のみ用いるプロトコルである。

さて、2 色カード組はカードベース暗号における標準的なカード組である一方、最も一般的に入手可能なカード組はトランプカード組である。トランプカードの絵柄は 52 枚すべて異なるため、もし five-card trick をトランプカード組を用いて実装する場合、3 セットの同じトランプカード組を用意する必要がある。このような背景から、トランプカード組を用いたカードベース暗号プロトコルの研究

[1] 茨城大学 Ibaraki University
[2] 筑波大学 University of Tsukuba
[3] 産業技術総合研究所 National Institute of Advanced Industrial Science and Technology
[a)] 24nm759t@vc.ibaraki.ac.jp
[b)] shinagawa@cs.tsukuba.ac.jp

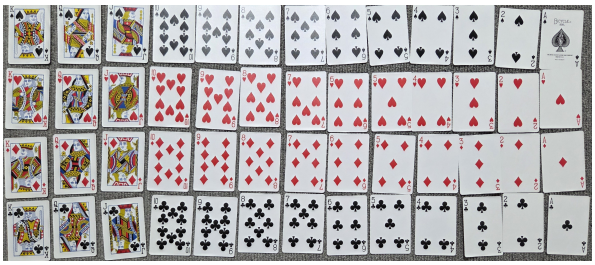

図 1 バイスクルカード

も、2 色カード組と並んで盛んに行われている。

Miyahara と Mizuki [4] は 4 枚のトランプカード組 $\boxed{3^{\heartsuit}}\boxed{3^{\clubsuit}}\boxed{9^{\heartsuit}}\boxed{9^{\clubsuit}}$ を用いて 2 入力 AND プロトコルを構成した。このプロトコルも用いるシャッフルはランダムカット 1 回である。このプロトコルの特筆すべき点は、半開示操作という新しい操作を導入したことである。半開示操作とは、伏せられたトランプカードに対して、そのオモテ面をすべて開示することなく、そのカードのスート（♠♡♢♣）のみを開示する操作である。この操作は、スート以外の部分をカバーしてめくることにより簡単に実装できる。

「カードの一部分だけを開示する」という半開示操作は、従来のカードベース暗号の計算モデルでは定式化されていない操作であるが、物理的な実装が容易であるため、そのような操作を用いた計算モデルにおける研究も興味深いものである。このような操作は、カードの部分的な情報を開示するという意味において、極めて強力な操作に思われる。それでは、このような操作を用いて、より複雑な関数、例えば n 入力 AND 関数 $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ に対するプロトコルを効率的に実装できるだろうか。

著者ら [3] は、半開示操作を一般化した部分開示操作 [2] に基づき、2 回のランダムカットを用いる 3 入力 AND プロトコルと、3 回のランダムカットを用いる 4 入力 AND プロトコルを構成した。部分開示操作とは、伏せられたトランプカードの任意の一部分のみ開示する操作であり、半開示操作の自然な一般化である。Miyahara–Mizuki の 2 入力 AND プロトコルの結果と合わせると、$2 \leq n \leq 4$ の範囲では、$n-1$ 回のランダムカットを用いて n 入力 AND プロトコルを構成できたことになる。それでは、任意の n に対して $n-1$ 回のランダムカットを用いて n 入力 AND プロトコルを構成できるだろうか。

1.2 本論文の貢献

本論文では、$2n$ 枚のトランプカードと $n-1$ 回のランダムカットを用いた n 入力 AND プロトコル（4 章）を構成することにより、上述の未解決問題を解決する。提案プロトコルは $3n-2$ 回の部分開示操作を用いる。

この結果と合わせて、1 回のランダムカットと $n-2$ 回のランダム二等分割カットを用いた n 入力 AND プロトコル（3 章）も提案する。このプロトコルの合計シャッフル回数は同じく $n-1$ 回であり、部分開示操作回数は 4 回である。このプロトコルはランダムカットの他にランダム二等分割カットを用いている代わりに、少ない部分開示操作回数を達成しており、シャッフルの種類と部分開示操作回数の間のトレードオフを与える。なお、既存研究 [5] において 4 回のランダム二等分割カットを用いた 2 入力 AND プロトコルが提案されているが、そのプロトコルを $n-1$ 回実行するとシャッフル回数は $4(n-1)$ 回であり、提案プロトコルよりもシャッフル回数が多いことに注意する。

2. 準備

本節では、基本的な用語と本論文で使用する操作を紹介する。

2.1 カード

本論文で用いるカード組は、U.S. プレイングカード社のバイスクル (図 1) の（ジョーカーを除いた）52 枚のカード組を想定する。これら 52 枚のカードを以下のように表記する。

$$\boxed{A^{\spadesuit}}\boxed{2^{\spadesuit}}\boxed{3^{\spadesuit}}\boxed{4^{\spadesuit}}\boxed{5^{\spadesuit}}\boxed{6^{\spadesuit}}\boxed{7^{\spadesuit}}\boxed{8^{\spadesuit}}\boxed{9^{\spadesuit}}\boxed{10^{\spadesuit}}\boxed{J^{\spadesuit}}\boxed{Q^{\spadesuit}}\boxed{K^{\spadesuit}}$$
$$\boxed{A^{\heartsuit}}\boxed{2^{\heartsuit}}\boxed{3^{\heartsuit}}\boxed{4^{\heartsuit}}\boxed{5^{\heartsuit}}\boxed{6^{\heartsuit}}\boxed{7^{\heartsuit}}\boxed{8^{\heartsuit}}\boxed{9^{\heartsuit}}\boxed{10^{\heartsuit}}\boxed{J^{\heartsuit}}\boxed{Q^{\heartsuit}}\boxed{K^{\heartsuit}}$$
$$\boxed{A^{\clubsuit}}\boxed{2^{\clubsuit}}\boxed{3^{\clubsuit}}\boxed{4^{\clubsuit}}\boxed{5^{\clubsuit}}\boxed{6^{\clubsuit}}\boxed{7^{\clubsuit}}\boxed{8^{\clubsuit}}\boxed{9^{\clubsuit}}\boxed{10^{\clubsuit}}\boxed{J^{\clubsuit}}\boxed{Q^{\clubsuit}}\boxed{K^{\clubsuit}}$$
$$\boxed{A^{\diamondsuit}}\boxed{2^{\diamondsuit}}\boxed{3^{\diamondsuit}}\boxed{4^{\diamondsuit}}\boxed{5^{\diamondsuit}}\boxed{6^{\diamondsuit}}\boxed{7^{\diamondsuit}}\boxed{8^{\diamondsuit}}\boxed{9^{\diamondsuit}}\boxed{10^{\diamondsuit}}\boxed{J^{\diamondsuit}}\boxed{Q^{\diamondsuit}}\boxed{K^{\diamondsuit}}$$

カードの裏面はすべて同じ模様 $\boxed{?}$ であり、これらは区別できないものとする。スートを気にしないときは

$$\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}\boxed{7}\boxed{8}\boxed{9}\boxed{10}\boxed{J}\boxed{Q}\boxed{K}$$

と表記する。

本論文ではトランプデッキとしてバイスクルを用いるが、標準的なデザインであれば他のトランプデッキも使用できる。例えば、U.S. プレイングカード社のタリホーとビーはバイスクルとデザインが似ており、使用することができる。

2.2 コミットメント

コミットメントとはビットの値を保持する裏向きに伏せられた 2 枚のカード組のことである。

トランプカードの既存研究では、52 枚のカードに全順序を入れ、小さい順に $\boxed{1}\boxed{2}\cdots\boxed{52}$ と表していた。このとき、$i<j$ ならば $\boxed{i}\boxed{j}=0$ および $\boxed{j}\boxed{i}=1$ と符号化を定め、ビット値 $x \in \{0,1\}$ を符号化する 2 枚の裏向きカード組 $\boxed{?}\boxed{?}$ を $[x]^{\{i,j\}}$ と表記していた。

本論文では、カードに全順序を与えず[*1]、カードペアごとに符号化を定義する方法を提案する。カードペア $\boxed{i}$ と

[*1] なお、本稿のプロトコルは全順序による符号化で記述することもできる。ペアごとの符号化は、特に部分開示操作を用いるプロトコルの構成において便利である。

表 1　トランプカードを用いたシャッフル $n-1$ 回の非コミット型 n 入力 AND プロトコル

	カード枚数	有限時間	シャッフル回数	部分開示操作回数
○ 非コミット型 AND プロトコル				
2 入力 AND（Miyahara–Mizuki [4]）	4 枚	✓	RC × 1	1 回
3 入力 AND（Honda–Shinagawa [3]）	6 枚	✓	RC × 2	5 回
4 入力 AND（Honda–Shinagawa [3]）	8 枚	✓	RC × 3	9 回
n 入力 AND（3 章）	$2n$ 枚	✓	RC × 1 + RBC × $(n-2)$	4 回
n 入力 AND（4 章）	$2n$ 枚	✓	RC × $(n-1)$	$3n-2$ 回

表中の RC はランダムカット（random cut）を、RBC はランダム二等分割カット（random bisection cut）を表す。

$\boxed{j}$ に対して、$\boxed{i}\,\boxed{j} = 0$ および $\boxed{j}\,\boxed{i} = 1$ と符号化を定め、ビット値 $x \in \{0,1\}$ を符号化する 2 枚の裏向きカード組を以下のように表記する。

$$\underbrace{\boxed{?}\,\boxed{?}}_{[x]^{\langle i,j\rangle}}$$

ここで、順序組 $\langle i,j\rangle$ をこのコミットメントの**ベース**と呼ぶ[*2]。スートが同一であり、さらにスートを気にしないときは $\langle A,2\rangle$ のようにスートを省略して表す。また、数字を気にしないときは $\langle \clubsuit,\clubsuit\rangle$ や $\langle \diamondsuit,\spadesuit\rangle$ のように表す。

2.3　ランダムカット

ランダムカットとは、カード列にランダムな巡回的なシフトを行うシャッフル操作である。例えば、伏せられたカード列 $\boxed{1}\,\boxed{2}\,\boxed{3}\,\boxed{4}$ にランダムカットを適用すると、カード列は以下の 4 つのいずれかになる。

$$\boxed{1}\,\boxed{2}\,\boxed{3}\,\boxed{4},\ \boxed{2}\,\boxed{3}\,\boxed{4}\,\boxed{1},\ \boxed{3}\,\boxed{4}\,\boxed{1}\,\boxed{2},\ \boxed{4}\,\boxed{1}\,\boxed{2}\,\boxed{3}$$

各列への遷移確率はすべて等しく、上の例ではそれぞれ 1/4 である。ランダムカットの適用を次のように表す。

$$\left\langle \boxed{?}\,\boxed{?}\,\boxed{?}\,\boxed{?} \right\rangle$$

2.4　ランダム二等分割カット

ランダム二等分割カットとは、同じ枚数の 2 組のカード束をランダムに入れ替えるシャッフル操作である。例えば、2 個のカード束 $\boxed{1}\,\boxed{2}$ と $\boxed{3}\,\boxed{4}$ にランダム二等分割カットを適用すると、カード列は以下の 2 つのいずれかになる。

$$\boxed{1}\,\boxed{2}\,\boxed{3}\,\boxed{4},\ \boxed{3}\,\boxed{4}\,\boxed{1}\,\boxed{2}$$

各列への遷移確率はすべて等しく、上の例ではそれぞれ 1/2 である。ランダム二等分割カットの適用を次で表す。

$$\left[\, \boxed{?}\,\boxed{?} \,\middle|\, \boxed{?}\,\boxed{?} \,\right]$$

2.5　部分開示操作

部分開示操作とは、カードのオモテ面全体を開示するのではなく、オモテ面の一部だけを開示する操作のことである。この操作は Miyahara と Mizuki [4] によって提案された半開示操作（カードのスート情報のみを公開する部分開示操作）を一般化したものである。図 2 は部分開示操作の開示位置を示している。ただし、これらの開示位置は操作のしやすさの観点から代表的な開示位置であり、これらの他にも有効な開示位置は存在することに注意されたい。表 2 は代表的な 7 つの開示位置の開示結果をまとめたものである。位置（A）はカードの数字と色を公開する位置である。位置（B）はカードのスート情報を公開する位置であり、Miyahara と Mizuki の半開示操作 [4] に相当する。位置（C）、（D）、（E）、（F）、（G）はそれぞれ左上のスート、左下のスート、左中段のスート、中上のスート、中央のスートを公開する位置である。

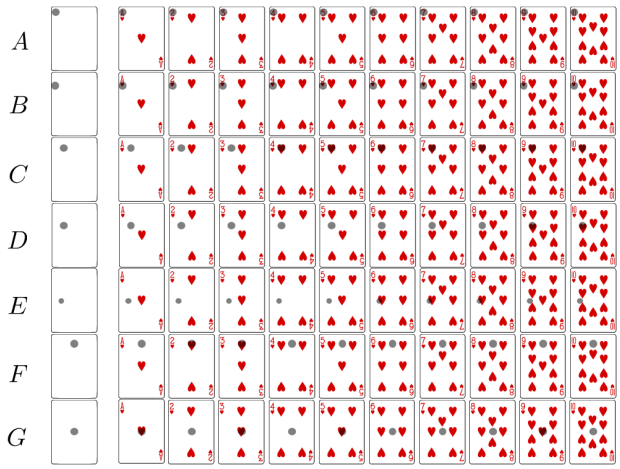

図 2　部分開示操作の開示位置

4 枚の伏せたカードに部分開示を適用し、2 枚目だけ ♡ が出る場合は以下の通りに表記する。

$$\boxed{?}\,\boxed{?}\,\boxed{?}\,\boxed{?} \to (\perp,\heartsuit,\perp,\perp)$$

以下、同様の方法で部分開示操作の適用を表す。位置 (C) ～ (G) について、$\boxed{1}$ から $\boxed{10}$ の各カードがスートを持つかどうかは図 2 の通りである。ただし、$\boxed{\mathrm{J}}\,\boxed{\mathrm{Q}}\,\boxed{\mathrm{K}}$ については本稿では半開示操作（位置 (B) の部分開示操作）しか適用しないため、図 2 に掲載していない。

部分開示操作は異なるスートのカードに対しても有用である。例えば、4 つのスート (ハート、ダイヤ、クラブ、スペード) のカードでは、スートの真ん中にある小さな穴か

[*2] 既存研究の $[x]^{\{i,j\}}$ においても集合 $\{i,j\}$ をベースと呼んでいたが、混乱の恐れがない限り、両者を同一の名前で呼ぶことにする。

表 2　各カードの開示位置と開示結果の関係

Position	1	2	3	4	5	6	7	8	9	10
A	1	2	3	4	5	6	7	8	9	10
B	♡	♡	♡	♡	♡	♡	♡	♡	♡	♡
C				♡	♡	♡	♡	♡	♡	♡
D									♡	♡
E						♡	♡	♡		
F		♡	♡							
G	♡		♡		♡				♡	

図 3　穴の空いたカバー

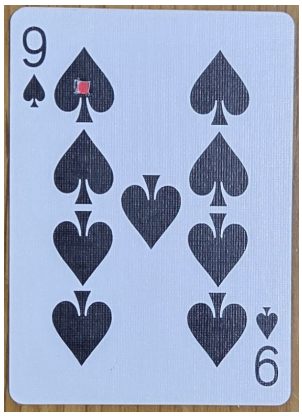

図 4　カバーを被せたカード

ら部分開示を行うことで、赤か黒かの情報を 1 ビットだけ得ることができる。

部分開示操作は、半開示操作と同様に、カバーを用いることで簡単に実装できる。具体的には、開示する位置に穴を開けたカバー (図 3) を用意し、それを部分開示したいカードの下面に挿入し、裏返せばよい (図 4)。

3. ランダム二等分割カットを使用する AND

3.1 プロトコル手順

プロトコルの入力を $x_1, x_2, \ldots, x_n \in \{0,1\}$ とし、x_i のコミットメントのベースを $\langle l_i, r_i \rangle$ とする。すなわち、入力カード列は $[x_i]^{\langle l_i, r_i \rangle}$ の列として与えられ、$x_i = 0$ のとき $\boxed{l_i}\boxed{r_i}$ であり、$x_i = 1$ のとき $\boxed{r_i}\boxed{l_i}$ である。カードに要請する条件は以下の 2 つである。

(i) 部分開示操作により、伏せられたカードが l_1 であるか l_2, r_1, r_2 のいずれかであるかのみ知ることができる。

(ii) 部分開示操作により、伏せられたカードが r_2 であるか $r_1, l_1, l_2, \ldots, l_{n-1}$ のいずれかであるかのみ知ることができる。

プロトコルの手順は以下の通りである。

(1) カードを以下のように並べる。

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1]^{\langle l_1, r_1 \rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_2]^{\langle l_2, r_2 \rangle}}\ \cdots\ \underbrace{\boxed{?}\boxed{?}}_{[x_n]^{\langle l_n, r_n \rangle}}$$

(2) x_1, x_2 に対してランダムカットを適用する。

$$\left\langle\ \underbrace{\boxed{?}\boxed{?}}_{[x_1]^{\langle l_1, r_1 \rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_2]^{\langle l_2, r_2 \rangle}}\ \right\rangle$$

(3) (i) の部分開示操作を用いて l_1 の位置を特定する。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \rightarrow \begin{cases} (\heartsuit, -, -, -) & 1 \text{ 枚目が } l_1 \text{ のとき} \\ (\perp, \heartsuit, -, -) & 2 \text{ 枚目が } l_1 \text{ のとき} \\ (\perp, \perp, \heartsuit, -) & 3 \text{ 枚目が } l_1 \text{ のとき} \\ (\perp, \perp, \perp, -) & 4 \text{ 枚目が } l_1 \text{ のとき} \end{cases}$$

ここで「♡」はそのカードが l_1 であることを、「$\perp$」はそのカードが l_1 以外であることを、「$-$」はそのカードには部分開示操作を適用していないことを表す。先頭の 3 枚とも $\perp$ の場合は 4 枚目が l_1 であることが確定するため、部分開示操作の回数は高々 3 回である。

(4) 前の手順の結果に従って、l_1 が先頭になるように巡回シフトする。例えば、前の手順の結果が $(\perp, \perp, \heartsuit, -)$ であり 3 枚目が l_1 のとき、3 枚目のカードが先頭になるように左に 2 回シフトする。

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}} \rightarrow \overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}$$

このとき先頭 2 枚のカード列を X とおく。X を構成する 2 枚のうち、右側のカードは $x_1 \wedge x_2 = 1$ のときに限り r_2 である。$n = 2$ ならば手順 (6) に進み、$n \geqq 3$ ならば手順 (5) に進む。

(5) $i = 3, 4, \ldots, n$ に対して以下の操作を順に行う。

(a) X と x_i を以下のように並べる。

$$\underbrace{\boxed{?}\boxed{?}}_{[\overline{x_i}]^{\langle l_i, r_i \rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{X}$$

(b) カード列の中央二枚の位置を入れ替える。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

(c) ランダム二等分割カットを適用する。

$$\left[\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\right]$$

(d) 1 枚目と 3 枚目を表向きにする。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \to \boxed{l_i}\boxed{?}\boxed{r_i}\boxed{?} \text{ or } \boxed{r_i}\boxed{?}\boxed{l_i}\boxed{?}$$

(e) l_i とその右隣のカードを改めて X とおく。

$$\underbrace{\boxed{l_i}\boxed{?}}_{X}\boxed{r_i}\boxed{?} \text{ or } \boxed{r_i}\boxed{?}\underbrace{\boxed{l_i}\boxed{?}}_{X}$$

X を構成する 2 枚のうち、右側のカードは $x_1 \wedge \cdots \wedge x_i = 1$ のとき r_2 であり、そうでないときは $r_1, l_1, l_2, \ldots, l_{i-1}$ のいずれかである。

(6) X の右側のカードに (ii) の部分開示操作を適用する。

$$\boxed{?} \to \begin{cases} \heartsuit & r_2 \text{ のとき} \\ \bot & \text{それ以外のとき} \end{cases}$$

r_2 のとき、出力結果は 1 である。r_2 でないとき、出力結果は 0 である。

このプロトコルで用いるカード枚数は $2n$ 枚（最小枚数）であり、シャッフル回数は $n-1$ 回であり、部分開示回数は高々 4 回である。シャッフルの内訳は、$n-2$ 回のランダム二等分割カットと 1 回のランダムカットである。

3.2 条件を満たすカード組

トランプカード 1 デッキの条件下で本プロトコルを実行可能なカード組と開示位置の例は以下の通りである。

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1]^{\langle 4\clubsuit,5\clubsuit\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_2]^{\langle 9\clubsuit,A\clubsuit\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_3]^{\langle 6\clubsuit,6\heartsuit\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_4]^{\langle 7\clubsuit,7\heartsuit\rangle}}$$

$$\underbrace{\boxed{?}\boxed{?}}_{[x_5]^{\langle 8\clubsuit,8\heartsuit\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_6]^{\langle 9\clubsuit,9\heartsuit\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_7]^{\langle 10\clubsuit,10\heartsuit\rangle}}$$

(i) 表 2 の開示位置 (G) に対する部分開示操作では、伏せられたカードが $\boxed{4\clubsuit}$ である場合はスートが見えず、それ以外の $\boxed{5\clubsuit}\boxed{9\clubsuit}\boxed{A\clubsuit}$ の場合はスートが見える。

(ii) 表 2 の開示位置 (C) に対する部分開示操作では、伏せられたカードが $\boxed{A\clubsuit}$ である場合はスートが見えず、それ以外の $\boxed{4\clubsuit}\boxed{5\clubsuit}\boxed{9\clubsuit}\boxed{6\clubsuit}\boxed{7\clubsuit}\boxed{8\clubsuit}\boxed{9\clubsuit}$ の場合はスートが見える。

このカード組は 1 デッキ内で構成できるものであり、複数デッキを使用することで、$n \geqq 8$ についても実装可能である。

4. ランダムカットのみの AND

4.1 プロトコル手順

プロトコルの入力を $x_1, x_2, \ldots, x_n \in \{0,1\}$ とし、x_i のコミットメントのベースを $\langle l_i, r_i \rangle$ とする。カードに要請する条件は以下の 3 つである。

(i) 部分開示操作により、伏せられたカードが l_1 であるかそれ以外の r_1, l_2, r_2 のいずれかであるかのみ知ることができる。

(ii) $2 \leq i \leq n$ とする。部分開示操作により、伏せられたカードが r_i であるか $l_1, l_2, \ldots, l_i, r_1, r_2$ のいずれかであるかのみ知ることができる。

(iii) 部分開示操作により、伏せられたカードが r_2 であるか $r_1, l_1, l_2, \ldots, l_{n-1}$ のいずれかであるかのみ知ることができる。

プロトコルの手順は以下の通りである。

(1) カードを以下のように並べる。

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1]^{\langle l_1,r_1\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{[x_2]^{\langle l_2,r_2\rangle}}\ \cdots\ \underbrace{\boxed{?}\boxed{?}}_{[x_n]^{\langle l_n,r_n\rangle}}$$

(2) x_1, x_2 に対してランダムカットを適用する。

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle$$

(3) (i) の部分開示操作を用いて l_1 の位置を特定する。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \to \begin{cases} (\heartsuit,-,-,-) & 1 \text{ 枚目が } l_1 \text{ のとき} \\ (\bot,\heartsuit,-,-) & 2 \text{ 枚目が } l_1 \text{ のとき} \\ (\bot,\bot,\heartsuit,-) & 3 \text{ 枚目が } l_1 \text{ のとき} \\ (\bot,\bot,\bot,-) & 4 \text{ 枚目が } l_1 \text{ のとき} \end{cases}$$

先頭の 3 枚とも $\bot$ の場合は 4 枚目が l_1 であることが確定するため、部分開示操作の回数は高々 3 回である。

(4) 前の手順の結果に従って、l_1 が先頭になるように巡回シフトする。例えば、前の手順の結果が $(\bot,\bot,\bot,-)$ であり 4 枚目が l_1 のとき、4 枚目のカードが先頭になるように左に 3 回シフトする。

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}} \to \overset{4}{\boxed{?}}\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}$$

このとき先頭 2 枚のカード列を X とおく。X を構成する 2 枚のうち、右側のカードは $x_1 \wedge x_2 = 1$ のときに限り r_2 である。$n = 2$ ならば手順 (6) に進み、$n \geqq 3$ ならば手順 (5) に進む。

(5) $i = 3, 4, \ldots, n$ に対して以下の操作を順に行う。

(a) X と $\overline{x_i}$ を以下のように並べる。

$$\underbrace{\boxed{?}\boxed{?}}_{[\overline{x_i}]^{\langle l_i,r_i\rangle}}\ \underbrace{\boxed{?}\boxed{?}}_{X}$$

(b) カード列の中央二枚の位置を入れ替える。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

(c) ランダムカットを適用する。

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle$$

(d) (ii) の部分開示操作を用いて r_i の位置を特定する。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \to \begin{cases} (\heartsuit,-,-,-) & 1\text{ 枚目が }r_i\text{ のとき} \\ (\perp,\heartsuit,-,-) & 2\text{ 枚目が }r_i\text{ のとき} \\ (\perp,\perp,\heartsuit,-) & 3\text{ 枚目が }r_i\text{ のとき} \\ (\perp,\perp,\perp,-) & 4\text{ 枚目が }r_i\text{ のとき} \end{cases}$$

部分開示操作の回数は高々 3 回である。

(e) 前の手順の結果に従って、r_i が 3 枚目になるように巡回シフトする。このとき l_i は先頭になることに注意する。この操作の後、先頭 2 枚のカード列を改めて X とおく。

(6) X の右側のカードに (iii) の部分開示操作を適用する。

$$\boxed{?} \to \begin{cases} \heartsuit & r_2\text{ のとき} \\ \perp & \text{それ以外のとき} \end{cases}$$

r_2 のとき、出力結果は 1 である。r_2 でないとき、出力結果は 0 である。

このプロトコルで用いるカード枚数は $2n$ 枚、シャッフル回数は $n-1$ 回、部分開示回数は $3n-2$ 回である。

4.2 条件を満たすカード組

トランプカード 1 デッキの条件下で本プロトコルを実行可能なカード組と開示位置の例は以下の通りである。

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1]\langle\clubsuit4,\clubsuit5\rangle}\ \underbrace{\boxed{?}\boxed{?}}_{[x_2]\langle\clubsuit9,\clubsuit A\rangle}\ \underbrace{\boxed{?}\boxed{?}}_{[x_3]\langle\clubsuit6,\heartsuit6\rangle}\ \underbrace{\boxed{?}\boxed{?}}_{[x_4]\langle\clubsuit7,\heartsuit7\rangle}$$

$$\underbrace{\boxed{?}\boxed{?}}_{[x_5]\langle\clubsuit8,\heartsuit8\rangle}\ \underbrace{\boxed{?}\boxed{?}}_{[x_6]\langle\clubsuit9,\heartsuit9\rangle}\ \underbrace{\boxed{?}\boxed{?}}_{[x_7]\langle\clubsuit10,\heartsuit10\rangle}$$

(i) 表 2 の開示位置 (G) に対する部分開示操作では、伏せられたカードが $\boxed{4\clubsuit}$ である場合はスートが見えず、それ以外の $\boxed{5\clubsuit}\boxed{9\clubsuit}\boxed{A\clubsuit}$ の場合はスートが見える。

(ii) 表 2 の開示位置 (B) に対する部分開示操作では、伏せられたカードのスートに対応したスートが見える。

(iii) 表 2 の開示位置 (C) に対する部分開示操作では、伏せられたカードが $\boxed{A\clubsuit}$ である場合はスートが見えず、それ以外の $\boxed{5\clubsuit}\boxed{4\clubsuit}\boxed{9\clubsuit}\boxed{6\clubsuit}\boxed{7\clubsuit}\boxed{8\clubsuit}\boxed{9\clubsuit}$ の場合はスートが見える。

謝辞 本研究は JSPS 科研費 JP23H00479、JP21K17702 と JST CREST JPMJCR22M1 の支援を受けた。

参考文献

[1] B. D. Boer. More efficient match-making and satisfiability the five card trick. In J.-J. Quisquater and J. Vandewalle eds., *EUROCRYPT 1989*, Vol. 434 of *LNCS*, pp. 208–217, Heidelberg, 1990. Springer.

[2] Y. Honda and K. Shinagawa. Efficient card-based protocols with a standard deck of playing cards using partial opening. In K. Minematsu and M. Mimura eds., *Advances in Information and Computer Security*, Vol. 14977 of *LNCS*, pp. 85–100, Singapore, 2024. Springer.

[3] Y. Honda and K. Shinagawa. Efficient three-input and four-input and protocols using playing cards with partial-open actions. In *Cryptology and Network Security*, LNCS, Singapore, 2025. Springer.

[4] D. Miyahara and T. Mizuki. Secure computations through checking suits of playing cards. In M. Li and X. Sun eds., *Frontiers in Algorithmics*, Vol. 13461 of *LNCS*, pp. 110–128, Cham, 2023. Springer.

[5] T. Mizuki. Efficient and secure multiparty computations using a standard deck of playing cards. In S. Foresti and G. Persiano eds., *Cryptology and Network Security*, Vol. 10052 of *LNCS*, pp. 484–499, Cham, 2016. Springer.