複数人のプレイヤーが手札情報を部分的に開示できる新手法

New Method That Allows Partial Disclosure of Hand Information by Multiple Players

小泉　康一・大槻　正伸

福島工業高等専門学校電気電子システム工学科

KOIZUMI Koichi and OHTSUKI Masanobu

National Institute of Technology, Fukushima College, Department of Electrical and Electronic System Engineering

（2023年8月8日受理）

There are several players who have one hand with the same one. Suppose that you have to inform all the other players of this fact. If it were possible to inform only "players have the same card" without informing them of the face of the hand in such a situation, it might prevent the game from losing its fun in various games. In this paper, we present a protocol that would solve this problem.

Key words: Secure multiparty computation, Card game, Secret computation

1. はじめに

複数人のプレイヤーがいて、手札を何枚か持つような何らかのカードゲームで遊んでいるとしよう。使用するカードの表面には数字、絵柄などの情報が描かれているとする。同じ表面のカードは複数枚存在するかもしれず、裏面からはまったくカードの区別はできない。このような理想的なカードを用いて何らかのカードゲームがプレイされているとする。

ゲームルール上、何人かのプレイヤーが共通の表面情報を持つ手札を 1 枚持っていることをお互いに知ったとする。全プレイヤー数より小さい k を用いて、k 人のプレイヤー$P_1, P_2, ..., P_k$を考える。ここで、k 人のプレイヤー以外の他のプレイヤー全員に対して、「同じ表面のカードを k 人全員が持っている」事実を伝えなくてはならなくなったとしよう。もちろん、該当プレイヤーが全員その表面を持つ手札のカード 1 枚を公開すれば目的を達成できる。ただし、カードゲームという性質上、手札表面の公開はその後のゲームの展開に支障をきたし、面白さを損なう恐れがある。

1.1 ゲームの例

人狼ゲームを例として説明する。人狼ゲームには様々な派生版が存在するが、基本的なルールとしては、複数人のプレイヤーのうち何人かが同じ陣営となり、各陣営の勝利条件を満たすように行動するゲームである。どのプレイヤーがどの陣営になるのかはランダムに決定されるが、各プレイヤーがどの陣営かどうかは秘密のままゲームが進行する。陣営の決定はカードの配布によることが多い。

ここで、プレイヤーが 8 人、 $P_1, P_2, ..., P_8$ がいたとして、仮に何らかのゲームルールに基づき、P_1, P_3, P_7が同じ陣営であることを知り、かつ 3 人のプレイヤーがそのことを示したいとしよう。このとき、3 人のプレイヤーに渡された陣営カードを公開することで、同じかどうかを示すことは可能である。しかし、これを公開することはどの陣営かをすべてのプレイヤーに知られてしまうことになり、その後のゲーム展開が変化する可能性が考えられる。3 人が同じ陣営であるが、それ以外のことについてはまったくわからない、のような形で他のプレイヤーに対して示すことはできないだろうか。

1.2 既存の手法

前節のような場面においても、手札の表面の情報を部分的に公開する、つまり「該当プレイヤー全員が同じカードを持っている」ことのみを示すことができ、それ以外の情報を隠しておくことができれば、様々なゲームにおいて面白さを失うことを防ぎつつ、いままでにない行動をすることが可能となるだろう。さらに、新しいカードゲームを作りたいとき、ルール構築の幅が広がり、より便利になるかもしれない。

著者の既発表成果として、1 人のプレイヤーのすべての手札を対象として、特定の表面情報を持つカードを含まないことを示すことができる手法 [1] と、1 人のプレイヤーの手札 1 枚を対象として、その数字、色などの部分的な情報のみを公開できる手法 [2] が存在する。これらの基本的な方針は以下の通りである。

・ゲームで使用するものと完全に同じカード構成であるカードデッキを別に用意し、証明に必要なカードすべてを抜き出して検証用部分集合を公開で作成する。

・プレイヤー（証明者）は証明したい手札を、検証用部分集合に含まれる同じカードと交換する。

・検証用部分集合に含まれるカードを十分にかき混ぜて、それぞれの場所をわからなくした後、表面をすべて公開する。これらがもとと同じ構成となっているかどうかを全員で確認する。

既存手法をただちに複数人プレイヤー版へ拡張しようとすると、証明すべき内容がごく簡単なものであれば可能かもしれない。しかし、既存手法では検証用部分集合を 1 つしか作成しないため、1.1 節のような問題に対応できない。他にも、例えば複数人が、トランプカードで同じ数の書かれた手札を持つことを証明したいとしても、単純な拡張は不可能であった。

1.3 本稿の貢献

本稿では 1. 1 節のような問題に取り組み、また前節で取り上げたような問題をも解決でき、複数人で実行したとしても安全に実行できるプロトコルの提案を行う。

提案するのは複数人のプレイヤーk 人の各手札 1 枚、合計 k 枚を対象として、それらの部分的な情報のみを公開できる手法である。既存手法との大きな違いは、検証用部分集合を複数個構築することにより、多様な証明を可能にした点である。さらに、証明者が複数人であることを許す。複数人で実行する場合、証明者の間であっても証明したいこと以外に手札情報を漏らしてはならない。本稿ではそのための安全な実装方法も新たに提案する。なお、各プレイヤーの手札数 1 枚に対応する証明手法として提案するが、手札の任意の枚数に対応できる形に簡単に変更できる。

プロトコルの複雑さを表す指標の 1 つである**シャッフル回数**は 2 であり、効率の良い手法と言える。本稿の手法は既存手法[1)2)]を包含しており、これらの一般化とも言える。そこで、計算モデルを新たに構築し、既存手法はこのモデルの中の特殊ケースであることも示す。提案手法では一部、特殊な操作を行うが、比較的簡単な操作のみで実行できるため、カードゲームを難なく遊ぶことができるような人であれば、簡単に実行可能である。

1.4 関連研究

カードベース暗号は、物理的なカードを用いて複数のプレイヤーが秘密に入力を行い、目的とする関数の出力だけを得る**秘密計算**等を実現する手法であり、AND や XOR などの基本演算を計算する手法が数多く知られている。参考文献としては代表的なものを示す[3) 4)]。それらの組み合わせにより任意の関数を秘密計算できることが知られている[4) 5)]。

したがって、1.1 節の問題についても解決できる手法自体はすでに存在することになる。しかし、組み合わせる演算の多くは 2 入力の基本演算が中心となっており、必ずしも効率よく解くことができるとは限らない。いまのところ多入力関数については、それに特化した効率の良いものは少ない。

著者の既発表の内容[6) 7)]は、2 人のプレイヤーが同時に、手札 1 枚の強さを比べ合うようなタイプのカードゲームにおいて、カードの表面を見せずに勝敗のみを知ることのできる新手法の提案である。手札の表面を見せないで実行できるため、本当は持っていない強いカードを、持っているものとして取り扱う、いわゆる、いかさまができてしまう。これを防ぐ手段として、1.2 節で示した既発表の手法[1) 2)] をサブプロトコルとして適用している。

1.5 本稿の構成

本稿の構成を以下に示す。2 節にて、本稿で取り扱うカードやシャッフルについて説明する。また、本稿で取り扱う問題のモデルを述べる。3 節で提案するプロトコルを与え、その理解の手助けとなるようにわかりやすい具体例を挙げる。最後に 4 節で本稿をまとめる。

2. 準備

この節では、提案手法を説明する前準備として、本稿で使用するカードやプロトコルの計算モデルを述べ、使用するシャッフルであるパイルスクランブルシャッフルを説明する。

カードベース暗号プロトコルは、カードの列に対して、**並べ替え**、**シャッフル**、**めくる**操作を行うことで、目的とする機能を実現する。そのような操作を含め、プロトコルは抽象機械により数学的に定式化されている[8) 9)]。簡単のため本稿では自然言語を用いて説明する。

なお、本稿で取り扱うカードゲームで使用するカードや、プレイヤーに対する詳細な条件は付録に示す。付録の内容は以前の原稿の定義を踏まえている[1) 2)]。

2.1 カード

各カードを区別するために、表面に描かれる情報が c であるようなカード 1 枚を、カード c と記載する。c は必ずしも表面情報の種類 1 つのみに対応するわけではなく、情報が複数種類の場合もある。例えば、「赤の 4」のカードであれば、これを「カード赤 4」のように記載する。

カードの束のことをカードデッキ、または省略してデッキと表現する。デッキはカードの集合として表すことができる。ただし、ゲームによっては、全く同じ表面絵柄で、人間が見てもそれぞれ区別のできないようなカードが複数枚存在することもある。もしもそのようなカード群に共通して表面に描かれている情報を c とし、それが m 枚存在する場合、各カードをデッキに含まれる集合の要素として $c^{(1)}, c^{(2)}, ..., c^{(m)}$ と表現する。 こうすることで、デッキを構成するカード集合としては別要素として見なすが、プレイヤーたちにとってはすべて同じカード c と認識し、それぞれ区別のできないものとして表現できる。 今後簡単のため同じ情報を持つカードの右上(1)(2)などのナンバリング表現は省略することもある。

デッキ D を、1 つのゲームに使用する可能性のあるすべてのカードを含み、それらのみで構成される初期デッキとする。

複数枚のカードを入れることのできるスリーブ(封筒)を自由に用いることができる。

2.2 モデル

この節では、本稿で扱う問題のモデルを示す。n 人のプレイヤーのうち $P_1, P_2, ..., P_k$ $(k<n)$ が証明者となり、残りのプレイヤーが検証者となる。ゲームのデッキを D とし、ゲームデッキと異なる検証用デッキを D' とする。$D \subseteq D'$ を満たす。各証明者が持つ、証明したい対象の手札のみから構成されるカード集合を H_p とする。 証明者が示すことは、検証用デッキ D' の部分集合 $D_1, ..., D_m$ があるとき、H_p が（カードの表面情報が同じという意味で） いずれかの部分集合に含まれることである。 ただし、$1 \leqq i \leqq m$ である各 D_i はすべて独立、すなわち各部分集合中に共通の要素（カード）を持たない。

証明したい具体的な内容により、H_p と $D_1, ..., D_m$ の構成が変化する。例えば、既存の成果 [3]のように証明者となるプレイヤーが 1 人であり、手札に特定のカード c を含まないことを示したいとき、H_p は証明者となるプレイヤーの手札すべてとなる。検証用デッキ D' の部分集合は D_1 ひとつとなり、その D_1 の構成は D からカード c すべてを除いたものとなる。成果 [4]も同様にこのモデル上で動く。したがって、本稿の成果の特殊形が成果 [3][4]となり、本稿ではそれらを含む一般形を与えたことになる。

2.3 シャッフル

本稿で登場するプロトコルで使用される特殊なシャッフルに、パイルスクランブルシャッフル [10] という種類のものがある。

パイルスクランブルシャッフルは、大きさが等しい複数のカード束があるとき、各束を構成するカードの順序を変えずに、束そのものを一様ランダムにかきまぜる。数学的には各束をそれぞれカード 1 枚とみなし、2 節の最初に紹介した操作の一つである「シャッフル」を適用する。すなわち各束の位置を一様ランダムな置換によって入れ替えることを指す。

繰り返しになるが、本稿で示すプロトコルにおいて、パイルスクランブルシャッフルを適用する対象の複数のカード束は、それぞれ構成する枚数、サイズが同じものとする。束のサイズが異なる場合でもシャッフル可能とする一般化版も存在する [11] が、本稿のプロトコルにおいては束のサイズを等しくすることで情報の漏れを防ぐ。

もしも各束のサイズが合わない場合、サイズの小さい束にダミーカードを追加して、サイズを合わせる。ダミーカードとは、裏面がゲームで使用するものと共通で、表面には何も情報のかかれていないカードとする。必ずしも表面がブランクでなくても、ペンなどでカード情報が無効であることを意味する印をつけてもよい。

3. 提案プロトコル

この節では、本稿のメインとなる、「k 人のプレイヤー全員が同じカードを持っている」ことのみを公開できる手法、さらにもっと一般的に「k 人のプレイヤー全員が特定の集合に属するカードを持っている」ことのみを示すことができる手法について説明する。これらの手法はカードゲームの最中にそのゲームを中断して手軽に実施できる。

3.1 k 人のプレイヤーが同じカードを持つことのみを示す手法

まず、1.1 節で示した問題である「k 人のプレイヤー全員が同じカード 1 枚を持っている」ことを証明可能なプロトコルを与える。2.2 節で示したモデルのうち、H_p は同じ情報を持つカード c が k 枚からなる集合となる。H_p は証明者である k 人のプレイヤーにとって既知の内容で

あるので、どの証明者が操作してもよい。したがってここでは、デッキ D' の部分集合 $D_1, ..., D_m$ の作成方法と、どのようにして H_p が部分集合のいずれか 1 つに含まれるかを示すか、を与える。

検証用デッキ $D'=D$ をあらかじめ準備する。検証用デッキも含めて本プロトコルで必要なカード枚数をカウントすると、$2|D|$となる。具体的には、そのゲームで遊ぶためのカードセットを 2 セット準備し、そのうち半分の 1 セットを用いて通常のゲームを行いつつ、必要に応じてゲームを一時中断し、残りの 1 セットのカードセットを用いて手札に関する秘密計算を行う。証明後すぐにゲームを再開できる。

プレイヤー$P_1, P_2, ..., P_k$ がカード c を同時に所持しているとき、そのことのみを他のプレイヤー全員に知らせることのできるプロトコル

前準備

検証用デッキ D' から、k 枚以上存在し、同じ表面情報を持つカードをすべて k 枚ずつ公開して集めて、部分集合をそのような表面の種類数だけ作成する。各部分集合を $D_1, ..., D_m$ とする。$D_1, ..., D_m$ に対してパイルスクランブルシャッフルを適用する。これを実装するには、各束を別々のスリーブに均一の向きで入れ、スリーブのままかき混ぜる。

1. 各プレイヤー$P_1, P_2, ..., P_k$は自分の持つ 1 枚のカード c をテーブルなどに伏せて置いておく。

2. k 人のプレイヤーのうち任意の 1 人はスリーブに入った複数の部分集合から、カード c が含まれるものを探す。そこからカード 1 枚を、表面を公開することなく手札に加える。まだ手札にカードを加えていないプレイヤーに同じ部分集合をわたし、そのプレイヤーも同様の行動を行う。これを続けていき、部分集合が空になったとき、k 人のプレイヤーの手札にそれぞれカード c が 1 枚加わるため、すべてのプレイヤーの手札は（表面情報が同じ、という意味で）プロトコル実行前の状態に戻る。

3. k 人のプレイヤーのうち、任意の 1 人は、テーブルに伏せられた k 枚のカードを公開せずに空になったスリーブに入れて、部分集合を 1 つ作成する。これを部分集合の束に戻して、それらの束にパイルスクランブルシャッフルを適用する。すなわち、各スリーブにどの部分集合が入っているのかわからなくなるまでかき混ぜる。

4. 任意のプレイヤーは部分集合の入ったすべてのスリーブから、中のカードを順に取り出し、前準備と同じ枚数構成になっているかを確認する。

Fig.1 はこの手法の実行例となる。何らかのカードゲーム中の状況で、6 人のプレイヤーがいる。使用するカードの表面にはグレー、ブルー、イエロー、レッド、グリーンの 5 色のいずれかが情報として描かれており、それぞれカードデッキ内に 3 枚以上存在している。

各プレイヤーは手札を 3 枚持っている。このとき、何らかのルールにより、3 人のプレイヤーが同じ色の手札（この例ではグレーのカード）を 1 枚持っていることを共有情報として知ったとして、そのことを示したいとしよう。まず前準備で、検証用デッキ D' を準備してそこから 5 色のカードを 3 枚ずつ取り出し、色ごとにスリーブに入れる。すなわち、5 つの部分集合がそれぞれ入ったスリーブセットを作成する。その後、それらの位置が区別できなくなるまでかき混ぜておく。

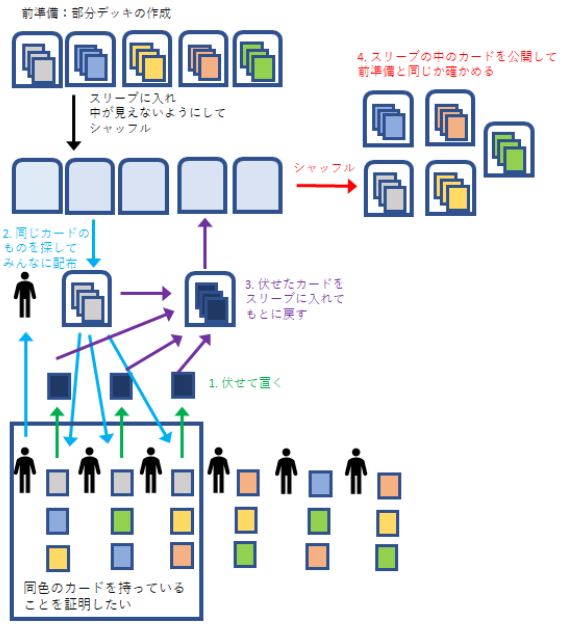

Fig. 1 本節で紹介した提案手法の実行例
Examples of executing the proposed method presented in this section

操作 1 として、3 人のプレイヤーは証明対象のグレーの手札を伏せて置く。表面は公開しない。

操作 2 として、プレイヤーの 1 人は 5 つのスリーブからグレーのカードのものをみつけて、公開せずに自分を含めた 3 人に配布する。3 人は渡されたカードを手札に

加える。

操作 3 として、伏せたカードを集めてそのスリーブに入れる。スリーブは元の位置に戻して、どれを操作したかわからなくなるまでスリーブごとかき混ぜる。

操作 4 として、全プレイヤーにスリーブの中身を公開する。ここで各部分集合が前準備と同じ枚数構成であれば、確かに 3 人のプレイヤーは同じ色のカードを持っていたことがわかる。しかし、その他のプレイヤーは 3 人がどの色を持っていたかを知ることはできない。

3.2　3.1 節のプロトコルの実行例

UNO（以下ウノ）カードゲーム用カードをすべて用いて、ウノではない何らかのゲームを行っていたとする。ウノカードセットには同じ数字と色のカード、もしくは特殊な効果のあるカードが、その数字が 0 でない限り 2 枚以上含まれる。2 人のプレイヤーA, B の手札 1 枚がまったく同じとき、そのことのみを証明したいとしよう。

検証用デッキ D' として、ゲーム用カードセットと構成が同じカードセットを 1 組用意する。D' から、同じ表面情報のカードを 2 枚ずつ取り出し、それらを 2 枚ペアの部分集合とみなす。それぞれ別のスリーブに入れる。なお、1 から 9 までの 4 色の 36 ペア、ドロー2、スキップ、リバースの 4 色 12 ペア、ワイルド、ワイルドドロー 4 の合計 50 ペア存在するので、部分集合は 50 組作成される。各スリーブにどの部分集合が入っているのかわからなくなるまで、スリーブのままかき混ぜておく。

プレイヤーA, B は手札のうち、例えば「赤の 5」を両方が持っていることを証明したいとしよう。それぞれ赤 5 のカードを手札から取り出し、テーブルに伏せる。A, B どちらのプレイヤーから実行しても良いが、今回はまず A が実行することにして、A は 50 個の部分デッキの中から「赤の 5」のカードが含まれるものを見つけて、この中身を公開することなく 1 枚手札に加える。同様に公開することなくもう 1 枚の「赤の 5」を B の手札に加える。

テーブルに伏せたカード 2 枚を空いたスリーブに表面公開せずに均一の向きで入れる。このスリーブをスリーブ束に混ぜて各スリーブにどの部分集合が入っているのかわからなくなるまでかき混ぜる。これを行わないと、混ぜたスリーブの位置を他のプレイヤーに覚えられてしまい、その後の手順におけるスリーブ内カードの公開によりプレイヤーA, B の持つ手札を知られてしまう。その場合は秘密計算にならない。

任意のプレイヤーは、すべてのスリーブの束から、中のカードを 2 枚ずつ取り出し、50 ペアすべてがそろっているか、表面を公開して確認する。前準備で作成したペア 50 組がすべてそろっていることを確認できたとき、プレイヤーA, B の手札には全く同じカードが含まれていることを、全プレイヤーが知ることができる。そして、そのカード自体がどの表面情報を持っていたかを知ることはできない。

3.3 k 人のプレイヤーが表面の部分情報が同じカードを持つことを示すことのできる手法

3.1 節で示した手法は、 表面の情報が同じカードが複数枚存在するゲームであれば簡単に適用できる。しかし、一般的にカードゲームで遊ぶ場面で使用されることの多いのは、トランプカードによるものであると思われる。トランプカードの場合、ジョーカー除く 52 枚のカード全てが異なる表面情報を持つ。本節ではそのようなカードを使用したゲームであっても、すなわち k 人の持つ証明対象の手札の情報が異なるが、部分情報が同じであれば、同様な手法でそれを証明できることを示す。部分情報が同じ、とは、トランプカードを例に挙げると、「数字」「スート」「色」などが同じ場合である。3.1 節で示した方式と同様に、この手法はカードゲームの最中にそのゲームを中断して手軽に実施できる。

2.2 節で示した問題のモデルのうち、3.1 節のプロトコルとは異なり、本節で取り上げる問題では H_p の構成が必ずしも証明者である k 人のプレイヤーにとって既知の内容とはならないことに注意する。したがって、H_p の操作は各証明者が既知であるようなカードのみ操作できる、という制限がかかる。ここでは部分集合の作成方法と、どのようにして情報を漏らさずに H_p が部分集合のいずれか 1 つに含まれるかを示すか、これらを与える。

プレイヤー $P_1, P_2, ..., P_k$ が全員、部分情報 q の記載されたカード $c_1, c_2, ..., c_k$ のいずれか 1 枚を所持しているとき、そのことのみを他のプレイヤー全員に知らせることのできるプロトコル

前準備

検証用デッキ D' を用意する。ここから、表面に部分情報 q と同種の情報が記載されており、かつ k 枚以上存在するような情報の描かれたカードをすべて集めて、部分情報の種類ごとに複数の部分集合を作成する。部分集合を $D_1, ..., D_m$ とする。

各部分集合に対してパイルスクランブルシャッフルを

適用する。このとき、各部分集合のサイズが合わない場合は、ダミーカードを追加してサイズを揃える。ダミーの追加作業自体は公開して行う。以後ダミーカードは追加したままにしておく。

1. 各プレイヤー$P_1, P_2, ..., P_k$は、それぞれ自分の持つ証明対象のカード 1 枚をテーブルなどに伏せて置いておく。
2. k 人のプレイヤーのうち任意の 1 人は、スリーブに入った複数の部分集合から、自分が伏せておいた証明対象のカードと同じ情報を持つカードを含む部分集合を探す。そこから元の手札とまったく同じ情報を持つカード 1 枚を、表面を公開することなく手札に加える。
そのあと、自分の伏せたカードをそのスリーブ内に加える。カードを挿入する箇所はランダムに決めて、公開はしない。
まだ手札にカードを加えていないプレイヤーにこの部分集合をわたし、そのプレイヤーも同様の行動を行う。
これを続けていき、k 人の全プレイヤーの手札に元の手札と同じものが加わり、全プレイヤーの伏せたカードがすべてスリーブに入れられたとき、全プレイヤーの手札は（表面情報が同じ、という意味で）プロトコル実行前の状態に戻る。
3. 任意のプレイヤーは、手順 2.で使用していたスリーブを部分集合の束に戻し、それらの束にパイルスクランブルシャッフルを適用する。すなわち、各スリーブにどの部分集合が入っているのかわからなくなるまで、スリーブのまま任意の方法でかき混ぜる。
4. 任意のプレイヤーは部分集合の入ったすべてのスリーブから、中のカードを順に取り出し、前準備と同じ枚数構成になっているかを確認する。

Fig. 2 はこのプロトコルの実行例となる。 何らかのカードゲーム中の状況で、6 人のプレイヤーがいる。使用するカードの表面にはイエロー、ブルー、レッドの 3 色の色情報と、1 から 6 までの数字の情報が描かれていて、合計 18 枚が全員にランダムに 3 枚ずつ配られていたとする。

このとき何らかのルールにより 3 人のプレイヤーが同じ数字情報を持つ手札（この例では 2 のカード）を持っていることを共有情報として知ったとして、そのことを示したいとしよう。

まず前準備で、検証用デッキ D' を準備して、そこから同じ数字情報を持つカードを 3 枚ずつ取り出し、それぞれ部分集合とみなす。部分集合ごとスリーブに入れ、6 つのスリーブセットを作成し、スリーブのままかき混ぜて位置をわからなくする。

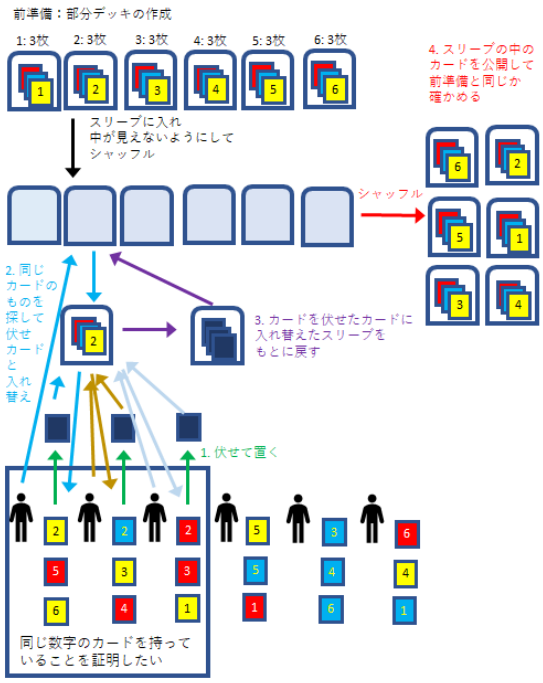

Fig. 2 本節で紹介した提案手法の実行例
Examples of executing the proposed method presented in this section

操作 1 として、3 人のプレイヤーは、証明対象の 2 の数字が書かれた手札を伏せて置く。表面は公開しない。

操作 2 として、プレイヤーの 1 人は、6 つのスリーブから 2 の数字が書かれたカードが含まれているものをみつけて、公開せずに元の自分と手札と同じ色のものを手札に加える。図であれば左のプレイヤーから順に実行したとすると、最初のプレイヤーは黄色の 2 をスリーブから取り出し、これを手札に加える。その後、自分の伏せたカードをスリーブに入れる。次に 2 番目のプレイヤーも同様に、同じスリーブから青の 2 を取り出し手札に加えて、自分で伏せたカードをスリーブに入れる。最後に 3 番目のプレイヤーも同様に同じスリーブから赤の 2 を取り出し手札に加えて、自分で伏せたカードをスリーブに入れる。

操作 3 として、入れ替えられたカードセットの入ったスリーブを、元の束に戻して、6 つの束が区別できなくなるまでかき混ぜる。

操作 4 として、全プレイヤーに全スリーブの中身を公開する。ここで前準備と同じ構成であれば、たしかに 3 人のプレイヤーは同じ数字のカードを持っていたことが

わかる。しかし、その他のプレイヤーは 3 人が持っていた手札についてそれ以外の情報を知ることができない。

3.4　3.3 節のプロトコルの実行例

トランプゲーム用カードを用いて、何らかのゲームを行っていたとする。2 人のプレイヤーA, B が同じ数字の手札を持っていたとき、そのことのみを証明したいとしよう。

検証用カードセットを D' として、ゲーム用カードセットとは異なるカードセットを 1 組用意する。D' から全く同じ数字のカードを 4 枚ずつ取り出し、それらを 4 枚組として 13 組の部分集合を作成して集合ごとに位置をランダムにしてスリーブに入れていく。部分集合の中身がわからないようにスリーブをかき混ぜておく。

プレイヤーA, B は手札に 2 のカードを持っていることを証明したいとする。 具体的には A は「ハートの 2」を、B は「スペードの 2」を持っているとき、各プレイヤーはこれらをそれぞれテーブルに伏せておく。

まず A は 13 組の部分集合の入ったスリーブから 2 のカードが含まれるものを見つけて、この中身を公開することなく、元の手札と同じ「ハートの 2」を手札に加える。そのあと、先に伏せた「ハートの 2」を公開しないように注意してスリーブ内のランダムな位置に入れる。

次に B がこのスリーブを受け取り、同様に、中身を公開することなく、元の手札と同じ「スペードの 2」を手札に加える。そのあと、先に伏せた「スペードの 2」を公開しないように注意してスリーブ内のランダムな位置に入れる。カードの交換を終えたとき、このスリーブを元の束に混ぜて、位置がわからなくなるまで束をかき混ぜておく。

任意のプレイヤーは、13 組のスリーブ束から順にスリーブの中のカードを 4 枚ずつ取り出し、表面を公開して確認する。すべて前準備と同じくそろっていることを確認できたとき、プレイヤーA, B の手札には全く同じ数字のカードが含まれていることのみを全プレイヤーが知ることができる。

3. 3節のプロトコルは、証明者である各プレイヤーの手札が1枚である場合の証明手法として紹介したが、証明したい手札枚数が増えたとしても同様に実行可能である。したがって、手札1枚でなく、手札すべてを対象とする事が可能である。よって、プレイヤー1人のみに対応する既存手法[1]も、3. 3節のプロトコルの特殊型となっている。また、3. 3節のプロトコルのうち、証明者を1人、部分集合を1個に制限した場合が既存手法[2] となるため、これも3. 3節のプロトコルの特殊型である。したがって、本稿で提案するプロトコルは、既存手法をすべて包含し、既存手法のみでは不可能であった証明も可能としている一般的なもの、という位置づけとなる。

4. おわりに

本稿では、カードゲームの途中に、複数人のプレイヤーが共通して持っている手札の部分的な情報を、比較的短時間かつ簡単に公開できる秘密計算手法を、新たに提案した。カードベース暗号のテクニックを用いた秘密計算は、情報セキュリティ分野における教育的ツールとしてさらなる活用が見込まれており、今回の提案手法もその 1 つとなりうると考えられる。今後も、複数人のプレイヤーを対象にして、さまざまなカードゲームに対応した秘密計算手法を考案したい。カードゲーム中であっても、実用的な時間で証明できる方式としたい。

参 考 文 献

1) 小泉康一，大槻正伸，“物理的ゼロ知識証明を用いた新しいカードゲーム不正プレイヤー検出手法の提案，” 福島工業高等専門学校研究紀要第 62 号，pp.15‐18， 2022.
2) 小泉康一，大槻正伸，“手札のカード情報を部分的に開示できる安全な新手法の提案，” 福島工業高等専門学校研究紀要第 63 号，pp.1–5， 2023.
3) T. Mizuki and H. Sone, “Six-card secure AND and four-card secure XOR,” Frontiers in Algorithmics, eds. by X. Deng, J.E. Hopcroft, and J. Xue, vol.5598, pp.358–369, LNCS, Springer, Berlin, Heidelberg, 2009.
4) C. Crépeau and J. Kilian, “Discreet solitary games,” Advances in Cryptology—CRYPTO’93, ed. by D.R. Stinson, vol.773, pp.319–330, LNCS, Springer, Berlin, Heidelberg, 1994.
5) T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, “Card-based protocols for any Boolean function,” Theory and Applications of Models of Computation, eds. by R. Jain, S. Jain, and F.Stephan, vol.9076, pp.110–121, LNCS, Springer, Cham, 2015.
6) 小泉康一，大槻正伸，“手札に関する不正者を検出可能な 新しい秘密計算カードプロトコルの提案，” 暗号と情報セキュリティシンポジウム SCIS2022 2F(1), 2022.
7) 小泉康一，大槻正伸，“対戦カードゲームにおいて強さを公開することなく勝敗のみを知りゲームをより面白くできる可能性のある新しい秘密計算カードプロトコルの提案，” ゲーム情報学（GI）研究会，2022-GI-47(1), pp.1--6, 2022.
8) T. Mizuki and H. Shizuya, “A formalization of card-based cryptographic protocols via abstract machine,” Int. J. Inf. Secur., vol.13, no.1, pp.15–23, 2014.
9) Takaaki Mizuki and Hiroki Shizuya, "Computational Model of Card-Based Cryptographic Protocols and Its

Applications, " IEICE Trans. Fundamentals, vol.E100-A, no.1, pp.3--11, 2017.
10) Rie Ishikawa, Eikoh Chida, and Takaaki Mizuki, "Efficient Card-based Protocols for Generating a Hidden Random Permutation without Fixed Points," Unconventional Computation and Natural Computation (UCNC 2015), Lecture Notes in Computer Science, Springer-Verlag, vol.9252, pp.215-226, 2015.
11) 石崎 悠斗, 品川 和雅, “追加カード 2 枚の多入力 AND 計算におけるシャッフル回数の新しい削減方法,” SCIS2024, 3D1-(1), 2024.

付録　使用するカードの具体的な説明

すべてのプレイヤーはプレイするゲームのルールを完全に理解しており、ルール解釈の間違いによるミスは起こさない。すべてのプレイヤーはゲームのルールを基本的には守り、自分の勝利条件を満たすように最大限努力するように動き、わざと負けるような動作はしない。ただし、自分の勝利のために可能ならばうそをつき、その後のゲーム展開で自分が有利になるように動くことがあるかもしれない。うそをつく以外の、カードの不正な入れ替えなどのいわゆる「いかさま」は行わない。複数のプレイヤーが結託し、結託者たちに都合の良いようにカードを入れ替えるなどの動作もしない。

1 つのゲームに使用されるカードの裏面は共通の絵柄であり、表面にはゲームで使用するための情報に対応する絵柄がプリントされる。表面に記される情報の種類は色、記号、数字などゲームによって異なる。トランプカードであれば、裏面には任意の共通絵柄が描かれ、表面にはカード情報としてスート（記号、マーク）、番号（ランク）の 2 種類が描かれる。「絵柄」という表現は必ずしもデザイン的なものを示すわけではなく、カードが単色で染められて印刷されている場合もそれは絵柄とみなし、該当する色がついているという情報を持つ。

すべてのプレイヤーは印刷のずれ、色むら、傷の有無などからはカードの区別ができない。したがって表面がまったく同じ情報を持つ複数枚のカードを区別することはできない。また、複数枚のカードの表面に描かれる情報が異なっていたとしてもそれらを裏面にしてシャッフルすると、その後表面を見ない限りどの情報を持つカードがどこにあるのかがわからなくなる。すなわち、シャッフル操作は理想的なランダマイザとして働く。

ゲームで使用するカードから構成されるカードデッキを D とする。D は 1 つのゲームが決まると一意に定まり、ゲーム中に変更されることはない。デッキ D の構成内容は公開情報であり、すべてのプレイヤーはその内容を熟知している。

複数枚のカードを入れることのできるスリーブ(封筒)を自由に用いることができる。スリーブは不透明ですべて均一の大きさ、素材でできており、それぞれ区別はできないとする。プレイヤーがカードをスリーブに入れるとき、そのプレイヤーはカードの表面情報を見ずに入れることも、見ながら入れることもできる。スリーブを操作しているプレイヤーはスリーブ内のカードの並び、向きを知ることができ、それ以外のすべてのプレイヤーは何らかのスリーブ操作がなされていること自体を知ることができる。あるプレイヤーが公開しながらスリーブ操作をした場合、すべてのプレイヤーは入れたカードがどのスリーブに入っているか、対応関係を知ることができる。すなわち、カードが入ったスリーブを特定でき、そのスリーブ内のカードの並び､向きを知ることができる。ただし、その後同じ枚数のカードが入った複数のスリーブが存在してそれらをシャッフルしたとき、どのスリーブにどのカードが入っているのか特定ができなくなる。スリーブにカードを複数枚入れた場合、上下、左右の並び、順番はスリーブに入っている限り入れた時点と変わることはない。それらを取り出すときも入れた時点と同じ並び、順番を維持したままである。したがって、スリーブに任意の枚数のカードを公開しながら入れ、その後それらを公開して取り出す場合、すべてのプレイヤーはそれらの順番が変わっていないことを確認することができることに注意する。