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

Proposal of a New Secure Method for Partial Disclosure of Card Information in the Hand

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

（2022年8月22日受理）

By using at most twice as many physical cards as the original total number of cards used in the game, the proposed method allows any player to be the prover and accurately prove partial information to all other players without revealing a single card in his or her hand. While playing a normal game with half the set, N cards in total, the game can be suspended, if necessary, to perform a secret calculation about the hand using at most the remaining N cards of the set, and resume the game immediately after that.

Key words: Secure multiparty computation, Card game, Physical zero-knowledge proof

1. はじめに

多くのカードゲームにおいて、各プレイヤーは自分のみが内容を確認できるカードの集合、すなわち手札を手に持ち遊ぶことが多い。当然、各プレイヤーの持つ手札の表面内容は非公開であるが、ゲームのルールによってはその一部分を公開する必要がでてくる。一般的な 52 枚のトランプカードで考えたとき、たとえば手札にスペードの 3 があり、何かしらの理由によりこの手札の数字を公開したいとする。シンプルな手法としては単純にこのカードの表面を公開すれば十分に目的を達成できる。しかしゲームのルールによっては、数字自体は教えてもいいがスート（スペード、ハートなどのマーク）を教えてはいけない場合もあるだろう。既存のゲームにおいてそのような状況の場合はたいてい口頭で「このカードの数は 3 です」と示すのみでよい。ここで不正なプレイヤーがいるとすると、そのプレイヤーは手札に持っていないカードの数を示すようなうそをついてその後のゲーム展開を有利に進めようとするかもしれない。プレイヤーによってはカード表面の数字を見間違いし、そのために結果的に間違った宣言をすることもありうる。ゲームが終わった後にそのゲーム内で実施されたすべての途中経過を検証することでそのような行為を発見できる可能性が高いが、手札が非公開のカードゲームにおいてはゲーム最中の記録はつけづらい。そこで本稿では、すでに私達が考案した「手札に特定のカード群を含まない」ことを正しく証明できる物理的な手法 [5]を改良し、「手札の任意のカードについて特定の部分的情報」のみを、物理的カードを用いた秘密計算 [1) 2)]を行うことで公開できる手法を提案する。以前の手法 [5]との違いとして、今回紹介する手法はプロトコルそのものとしては本質的な違いがない。以前の手法では手札すべてを対象とする証明を行うことにより証明自体は可能であるが証明後すべての手札の部分情報、すなわち「特定のカードでない」ことが等しく公開されてしまうことが一つの欠点でもあった。今回はこれを防ぎ、手札の一部のみを対象としてそれのみの証明を行うことによって、手札のうち手札の部分的情報の公開を行いたいカード群と一切情報を知られたくないカード群に分けて最小限に証明が可能となる点が大きな改良点と言える。

今回提案する手法は、以前に考案した手法 [3)4)5)]と同じくゲームで使用する本来の全カード数の高々2 倍の枚数の物理的なカードを用いることで、任意のプレイヤーが証明者となり、そのプレイヤーの任意の手札 1 枚の表面を公開することなく部分的情報をその他すべてのプレイヤーに対して正確に示すことができる。この手法は比較的簡単な手順からなっており、カードゲームを行うことのできるようなすべての人が実行可能である。

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条件を書き示す。この節の内容はカードゲーム

を数学的に記述するための準備となり、どのようなカードに関する研究であっても毎回事前に基礎として固めておく必要がある。そのため、この節の内容は以前に公表した原稿[5]をほぼ引用して記述する。

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動くことはしない。

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。デッキはカードの多重集合として数学的に表すことができる。多重集合とは、通常の集合と異なり同じ値の元が複数存在することが許される集合である。例えば、$\{a,a,b\}$のように同じ元 a が複数存在することが許され、その元の数も重要なパラメータになる。$\{a,a,b\}$がデッキを表現しているとすると、このデッキはカード a がちょうど 2 枚、カード b がちょうど 1 枚含まれる 3 枚の集合になる。また、本来の多重集合においては要素の並ぶ順も区別されるが、話を簡単化するため今回はその区別をしない。すなわち、$\{a,a,b\}$, $\{b,a,a\}$はともに同じデッキとみなす。

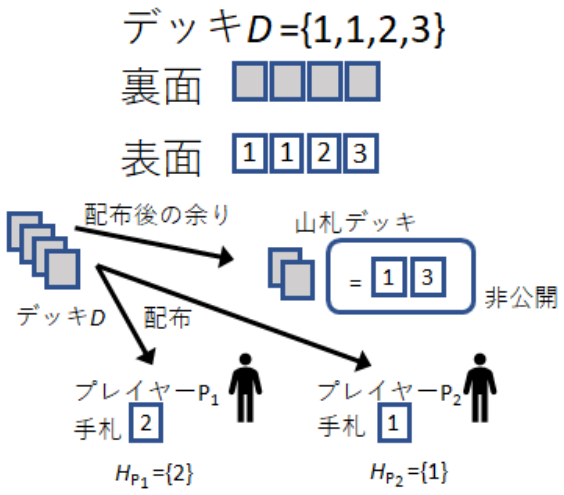

Fig. 1　デッキからランダムに選択されたカードが各プレイヤーに配布され手札 1 枚を構成した例

H_p を、プレイヤーp の保持する手札の多重集合とする。D を、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。D は一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。

Fig. 1 は、デッキ D={1,1,2,3} とし、2 人のプレイヤーがランダムにカードを 1 枚配布されて手札がちょうど 1 枚の状態である。デッキ D から各プレイヤーの手札以外に残った枚数は 4 - 2 で 2 枚であり、その枚数を 2 人のプレイヤーはともに知っているが、それが構成されるカードの表面自体は知らない。この状態から次に山札デッキからカードを 1 枚引くと、1 のカードか 3 のカードのうちどちらかがランダムに引かれるとみなせる。本来は山札デッキが構成された時点で、デッキから引かれるカード順序は固定であるが、今回のモデルでは構成されるカードの中からランダムに引かれることとみなす。カードゲームにおいては必要に応じて山札の上からカードを 1 枚ずつ引くこととなるが、山札デッキの中から好きなカードをランダムに 1 枚ずつ引くようなモデルとみなしても問題ないからである。

3. 手札に関する部分情報のみを公開できる提案手法

この節では、本稿のメインとなる手札 1 枚に関する部分的情報を公開できる手法について説明する。この手法はカードゲームの最中に手軽に実施できるが、準備としてカードゲームで使用する全カード数 N の高々2 倍である 2 N 枚の物理的なカードを用いることが必要となる。具体的には、そのゲームで遊ぶためのカードセット、すなわちデッキ D と同じものが合計 2 セット必要になる。そのうち半分のセット、合計 N 枚を用いて通常のゲームを行いつつも、必要に応じてゲームを一時中断し、高々残り N枚のカードセットを用いて手札に関する秘密計算を行い、その直後にゲームを再開できる。今回提案する手法の方針を大雑把に説明すると以下のようになる。まず、ゲームに使用する N 枚の全カードデッキ D と、まったく同じ構成である N 枚のデッキ D’ の 2 セットを準備する。D を使用してゲームを進めていき、途中で手札の部分的情報を知らせたい状況になったプレイヤーは、該当の手札を完全公開せずに別の場所に伏せて置き、次にデッキ D’ から、示したい部分的情報を含むすべてのカードを抜き去るように公開作成して、そこから元の伏せた手札と同じカードを秘密に取り出して新たな手札とする。最後の手順として、伏せた元の手札を、その一部

のセットに加えてシャッフルし集合内のすべての表面を公開する、というシンプルな手法である。

今回提案する手法は、一般的な定義を行うよりも先に例を用いて示したほうがわかりやすい。そこで、トランプカードを用いて、プレイヤーp の手札にスペードの 2 がある状況においてこれに対して「このカードの数は 2 である」ことのみを示したい場合を扱う。

プレイヤーp は手札を混ぜずに、証明用デッキ D'から示したいことを含んでいるカードをすべて抜き出す。今回は数が 2 であることを示したいので、D' からスペードの 2、ハートの 2、ダイヤの 2、クラブの 2 の合計 4 枚のカードを公開しながら抜き出し、4 枚を裏面にしてシャッフルする。次に p は自分の手札から、表面を隠したスペードの 2 を、テーブル面などの別スペースに区別して表面が見えないように伏せて置いておく。続いて p はシャッフル後の 4 枚の中から、もとの手札と同じスペードの 2 を抜き出して、表面を隠しながらもとの手札に加える。最後に抜き出した後の 3 枚と、伏せたもとの手札とを混ぜてシャッフルして表面を公開する。すると当然 4 枚のカードはスペードの 2、ハートの 2、ダイヤの 2、クラブの 2 の合計 4 枚であり、このことから p の手札のカード 1 枚の数は 2 であることが公開されたことになる。

次に、提案手法の一般的な記述をおこなう。

提案手法

プレイヤーp の手札 H_p に含まれる特定のカード c_1 の部分的な情報を公開する物理的な手法

以下の操作を全プレイヤーに公開しながら実施する。

前準備・任意のプレイヤーはゲームに使用する全カードをちょうど含む、ゲームで使用しているものと物理的に異なるデッキ D' を用意する。示したい部分的情報を含んでいるような D' に含まれるすべてのカードのうち、現在各プレイヤーの手札に存在する可能性があるカードのみからなる集合を D'_{Target} とする。当然 $D'_{\mathrm{Target}} \subseteq D'$ である。

操作 1・証明者 p を含む任意のプレイヤーは、D' から $D_{\mathrm{proof}} = D'_{\mathrm{Target}}$ を証明用デッキとして（表面を公開しながら）物理的に作る。その後、D_{proof} のすべてのカードを裏面にして、任意の方法によりすべてのプレイヤーがカードの表面と位置との対応関係を特定できなくなるまで十分にシャッフルする。

操作 2・証明者 p は、H_p から部分情報を公開したいカード c_1 を選び、決して表面を他のプレイヤーに見せないように注意しながら c_1 の上部を裏面にして他のカードと混ざらないようにテーブル上に区分けして置いておく。これを T_p とする。

操作 3・証明者 p は、D_{proof} をすべて手に取り、D_{proof} に含まれるカードの表面を秘密に確認しながら c_1 のみを選び、これを抜き取って自分の手札 H_p に加える。D_{proof} の作成手順の性質により、D_{proof} の中には c_1 が間違いなく含まれているので、少なくとも 1 枚の c_1 は必ず見つかる。手札に新たに加えるカードの表面を見せることはしないが、新たに手札に加える操作自体は公開状態で行う。その後残った D_{proof} のすべてのカードを他のプレイヤーには表面を公開しないよう注意して裏向きにしておく。

操作 4・証明者 p を含む任意のプレイヤーは、区分けしておいた T_p のカード表面を見ずに、操作 3 で c_1 が抜き去られた後の D_{proof} に裏面のまま加えて、任意の方法で裏向きのまま十分にシャッフルし、すべてのカードがもともと D_{proof} に存在していたものか、T_p から加わったものかどちらなのかわからないようにする。

操作 5・証明者 p を含む任意のプレイヤーは、D_{proof} のすべてのカードの表面を公開し、これが前準備で抜き出しておいた D'_{Target} とカード順序の変更を許して等しければ、証明者のもとの手札 H_p に含まれる 1 枚のカード c_1 の部分情報を公開したことになる。等しくなければ、証明者は何らかの不正を行ったことになる。

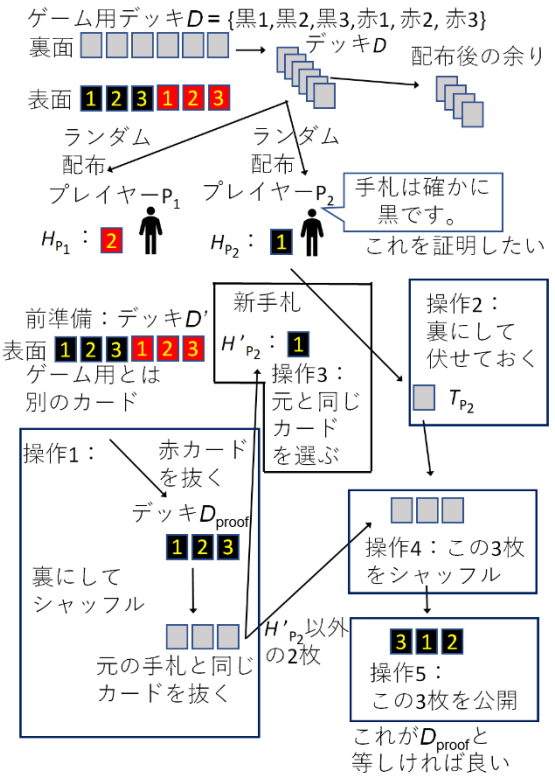

Fig. 2 手札当てゲームに対する提案手法の適用

ここで Fig.2 を用いて、ある手札当てゲームの最中に提案手法を適用する具体例を紹介する。本来であれば手札を複数枚持つ場合を説明すべきかもしれないが、話を簡単にするため各プレイヤーが手札を 1 枚だけ持つゲームを考える.

考えるゲームでは全 6 枚のカードデッキ D={黒 1, 黒 2, 黒 3, 赤 1, 赤 2, 赤 3}を初期デッキとする。2 人のプレイヤーP_1、P_2はシャッフルされた初期山札デッキ D からそれぞれ 1 枚ランダムに引きそれを手札とする。手番のプレイヤーは、予想した相手の手札のカードの色と数を両方宣言し両方とも当てることができたら勝ち、当てられなかった場合、相手は色、数字のどちらが異なるか、もしくはどちらも異なっているかを正直に宣言する、というシンプルなゲームとする。ここで、ランダムに引いた結果 H_{P1} ={赤 2}, H_{P2} ={黒 1}であったとする。P_1 が最初の手番として、「あなたの手札は黒 3 ですか」と P_2 に聞いたとする。ここで P_2 はゲームのルール上「黒ですが 3 ではありません」と宣言する必要がある。このうち、確かに手札の色が黒であることを今回提案するプロトコルを用いて証明するとしよう。前準備としてプレイヤーP_1、P_2のどちらかは、ゲームを行うために準備した D とは異なるがまったく同一の初期カードを要素とする D'={黒 1, 黒 2, 黒 3, 赤 1, 赤 2, 赤 3}を用意する。操作 1 により、D' から表面を公開しながら赤 1, 赤 2, 赤 3 の 3 枚のカードを抜き、残り 3 枚のデッキを D_{proof} = D'_{Target} ={黒 1, 黒 2, 黒 3}とする。裏面の状態にして 3 枚のカードを好きな方法でシャッフルする。操作 2 として、P_2 は持っている 1 枚の手札（黒 1 のカード）を他のカードと混ざらないように伏せて置いておき T_{P2}={黒 1}とする。操作 3 として、P_2 は D_{proof} の 3 枚のカードから自分のもとの手札と同じ表面のカード（黒 1 のカード）を秘密に抜き取り新たな手札とする。このとき D_{proof} ={黒 2, 黒 3}となるがこの内容を P_2 以外の人が知ることはない。操作 4 として、P_1、P_2 のどちらかは D_{proof} に T_{P2} を裏向きのまま混ぜて、その後好きな方法で十分にシャッフルする。最後に操作 5 として P_1、P_2 のどちらかは D_{proof} の表面を公開する。これがもともとの D_{proof} と同じ{黒 1, 黒 2, 黒 3}となっているので、プレイヤーP_2 の手札は黒のカードであることが明白であるが、その数まではわからないことを証明できた。そして、操作 3 で手札を不正に変更もしていないことも明らかである。

次に、「黒ですが 3 ではありません」の宣言のうち、手札が 3 ではないことを証明したいとする。今回は手札枚数がちょうど 1 枚のため、本提案プロトコルでも証明可能であるが以前の原稿で提案した、手札に特定のカードを含まないことを示すことが可能なプロトコル[5] をそのまま用いる形としても証明できる。すなわち、上記のプロトコルのうち証明用デッキ D_{proof} を 3 以外のすべてのカードからなるように構成すればよく、D_{proof} ={赤 1, 赤 2, 黒 1, 黒 2}とすることで簡単に実現できる。また、2 人のプレイヤーが両方とも集合の概念を理解できている仮定であれば、証明用デッキ D_{proof} を D_{proof} ={黒 1, 黒 2}とすることで「黒かつ 3 でない」ことを一度に証明できるが、そうではない場合は一つずつ丁寧に作業して示したほうがよい。

本プロトコルは手札 1 枚の部分情報のみを示すことができることを示したが、複数枚の手札の部分情報を示す形にも簡単に拡張できる。さらに複数のプレイヤー間での手札に関する部分的な証明にもつなげることが可能と考えている。複数のプレイヤーが手札の部分情報を示す必要があるとき、各自の部分的な手札を使い、さらに D_{proof} を証明したい内容に合わせて適切に選択することにより実現可能であると予想している。複数プレイヤー対象版を示す場合 D_{proof} の内容が複雑化する可能性が高いため、次回以降に改めて紹介したい。

4. おわりに

本稿では、カードゲームの途中であっても、プレイヤーの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プロトコルを新たに提案した。提案手法を用いることにより、あるプレイヤーが自分の手札のカードの部分情報を、その情報以外をまったく知らせずに安全かつ確実に公開できる。カードを用いた秘密計算については情報セキュリティ分野においてさらなる活用が見込まれており、先に公開した原稿[3)4)5)]の内容を含めて今回の提案手法もその 1 つとなりうると考えている。また、適切な情報を含んだ適切枚数のゲーム用カードを用いて遊ぶカードゲームは集合の概念を学べるツールとして活用できると考えられる。今後も、さまざまなカードゲームに対応しゲーム中であっても、今回提案した手法により証明できないような事柄を実用的な時間で証明できる方式を考案していきたい。

参 考 文 献

1) Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone, "Practical Card-Based Implementations of Yao's Millionaire Protocol," Theoretical Computer

Science, Elsevier, vol.803, pp.207--221, 2020.

2) 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.
3) 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.
4) 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.
5) 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.