Vol.2022-GI-47 No.1
2022/3/18

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

小泉康一 [1]　　大槻正伸 [1]

概要：2 人のプレイヤーがそれぞれ手札を 1 枚ずつ同時に出しそれらの強さを比較して勝負するカードゲームにおいて，その勝敗判定は公開した手札同士をお互いに見て判断することが一般的であろう．ここで，手札のカードを公開せずに勝敗のみを知ることができると，手の読み合いの必要度が変化し，それ以外の部分は同じルールでのゲームであったとしても，より面白いゲームになる可能性がある．勝敗のみを知るための単純な案としては公平な第三者に勝敗を判定する審判役となってもらうことが考えられるが，カードベース暗号のテクニックを用いると公平な審判が不在でもカードを公開することなく勝敗のみを正しく知ることができることがわかった．そのような新しいプロトコルを考案したので本稿にて提案する．プロトコル実行の前準備としてゲームで使用するカードと同一のセットを 1 から 2 セットと，勝敗表を作成するための特殊カードを必要とする．

キーワード：Secure multiparty computation, Physical zero-knowledge proof, Millionaire protocol

1. はじめに

小さい子どもが考えるカードゲームとしてシンプルなものに，「お互いが 1 から n までのカードを手札として持ち，同時に手札を出して大小を比較し大きいほうが勝ちとし，より勝利数の多いほうが全体での勝ち」というものがある．本稿ではこのようなゲームを n 枚ゲームと呼ぶことにすると，これはトランプカードを用いると簡単に実現できるし，紙に数字を書いても遊べるので，余計なものを学校に持っていけない小学生時代，休み時間に楽しめる遊びの一つとして重宝した人もいるかもしれない．このままのルールではゲームとして面白さに欠けるが，よくあるアレンジルールとしては「1 のカードは最弱だが n にのみ勝てる」というものがある．さらに，1 のカードのみでなく他の数のカードにも特殊な役割をもたせる方向性もある．n = 8 とし，すべての数カードに特殊な役割をもたせることによって面白さを増したゲームとしてカナイセイジさんの 500 円ゲームズ作品「R」(2011)[4], その一般流通版「R-Rivals」[5] または「BraveRats」[6] がある．この手のゲームにおいては，相手のすでに使用したカードを場に公開しておくか覚えておくことにより相手の可能な手を把握した上で次の自分の手を決める選択をしていくことになるが，相手の手札の全容を知りつつも自分の手を選ぶことができるこれらのゲームはこの点においてゲームの楽しさが増す，と考えることもできるし，展開が予想できて途中からは作業となる，と考えることもできてしまうため，良いこともあれば悪いこともあるかもしれない．毎回のゲームで最初に使わない手札を何枚か選び，あらかじめ横においておくことにより相手手札にランダム性をもたせることも可能だが，ここで，お互いの出した手札を公開することなく勝敗のみを正しく知ることができると，たとえば十分大きい数の n 枚ゲームにおいて「自分は 3 を出して負けたということは，相手はこのとき 4 以上のカードを出した」ことしか知ることができず，より相手の手札にランダム性をもたせることが可能になり，ゲームによっては面白さを増すことができる可能性がある．本稿では，カード自体に特殊な役割をもたせる方向性でなく，カードを公開しないことによる面白さ，を重視したい．ここで，カードベース暗号と呼ばれているテクニックを用いると物理的カードを用いて秘密計算を行うことができることが知られている[2]．例えばゲームにおいてはナンバープレースのような紙と鉛筆を用いて遊ぶ様々なペンシルパズルゲームを中心に，その解を知っていることの証明に，カードなどの物体を用いて行う物理的ゼロ知識証明として活用できることが知られている[2]. また，お互いに正直であるという前提はあるが 2 人のプレイヤーの財産を比較しどちらが大きいかを物理的カードを用いて計算することのできる，カードによる金持ち比べプロトコル手法が知られている[1]．本稿では, そのようなカードベース暗号の手法を元に考案した，相手の手札を知ることなく 1 枚対 1 枚の手札勝負の勝敗を知ることができ，さらに不正のできない秘密計算プロトコルを新しく提案する．

提案手法は，既存のカードによる金持ち比べプロトコル[1]を参考に，正しい手札を出さないと正しいプロトコルを実行できないように作成できた．ただし，前準備としてゲームでお互いのプレイヤーが手にする可能性のあるカードをそれぞれ準備する必要がある．n 枚ゲームにおいてはゲ

1 福島工業高等専門学校　電気電子システム工学科, 9708034 福島県いわき市平上荒川字長尾 30

ームで使用するお互いの持つ $n + n$ 枚のほかに，プロトコル用に同一のカード計 $2n$ 枚を必要とする．また，カードを用いて勝敗表を作成するためにそのような特殊カードをそれぞれ $n*n$ 枚必要とする．したがってプロトコルに必要カード枚数は $O(n^2)$となる．

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．また，カードデッキの記述法について示す．

本稿で考えるゲーム用カードは，裏面が共通の絵柄もしくは無地で，カードの大きさや形は完全に一致している．表面はそのカードナンバーとしての数や記号が記されており，まったく傷がつかず，表面を見る行動，またはそのカード以外に存在するすべてカードの表面を知ること以外にその表面情報を確実には知ることができない．カードの束のことをデッキと表現する．各プレイヤーの持つ手札は，常に全員が裏面を確認することができるが，持ち主のみが表面を常に確認できる．各プレイヤーが持つ手札の合計枚数は公開情報とし，意図的に非公開とすることや，うそをつくことはない．例えば，非公開でカードを入れ替えるようないかさまは行わない．

任意のカードの移動について，すべてのプレイヤーはそのすべての移動経路を把握，記憶しているとする．しかし，他のいくつか複数のカードと同時に，表面非公開でシャッフル操作が行われた場合，すべてのプレイヤーはその移動経路をそれ以降，他の要因がない限りは得ることができない．このときシャッフルされたカード束のいずれかのカードが対象カードであったことのみを知ることができる．本稿で行われるシャッフル操作は常に理想的であると考え，シャッフル操作後のカード束に含まれる特定のカードの表面の位置は，どのプレイヤーも均等な確率のみでしか推定できない．

H_p を，プレイヤーp の保持する手札の集合とする．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 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．当然，任意のプレイヤーp に対して $H_p \subseteq D$ が成立する．

3. 手札に関する秘密計算を行う提案手法

3.1 提案手法

この節では，トランプカードゲーム「戦争」のように，2 人のプレイヤーが 1 枚の手札同士を比べて勝敗を競うとき，相手カード情報を知ることなく勝敗のみを知ることができる手法を提案する．

最初に，既存の金持ち比べカードプロトコル[1] を変更し，正直なプレイヤー同士であればシンプルにお互いの勝敗のみを知ることができる変更案を述べる．本稿では話を簡単化するため，$n=5$ とした 5 枚ゲーム，ただし 1 は 5 に勝てる特殊ルールを採用したゲームを固定して考える．2 人のプレイヤーAlice, bob はお互いに裏面共通で絵柄が〇，△，×のような 3 種の対戦表用特殊カードと，絵柄が□（ブランク）と↑の自分の手の位置表現用特殊カードを十分に持つ．ただし，Alice の持つカードと Bob の持つカードはそれぞれの手から離れたとしても，もともとどちらが持っていたものかを区別できるようにする．例えばそれぞれ 1 枚ずつの 2 枚ペアをつくる場合は常に Alice を上にする，などのルールを設けるか，カードの裏面デザインが異なると最も良い．本稿ではお互いの持つ特殊カードは裏面が異なるものとしておく．表 1 は，それぞれのプレイヤーが出す手に対応した勝敗表と，どの手を出すかの位置，ポジションを表す表になっている．〇となるセルの手をお互いに選んだ場合，縦列に対応するプレイヤーが勝利となる．×の場合は負けとなり，△の場合はお互いに引き分けとなる．Bob の選ぶ手が横の行に対応する下側の表については，Alice の勝敗表，ポジション表と対称的にわざと左右逆に配置させている．

表 1　5 枚ゲームの勝敗表と出す手表現用の表の並び

		Bobの手札				
		1	2	3	4	5
Alice の手札	1	△	〇	〇	〇	×
	2	×	△	〇	〇	〇
	3	×	×	△	〇	〇
	4	×	×	×	△	〇
	5	〇	×	×	×	△

Alice の手札	1	↑	□	□	□	□
	2	□	↑	□	□	□
	3	□	□	↑	□	□
	4	□	□	□	↑	□
	5	□	□	□	□	↑

Bob の手札	1	↑	□	□	□	□
	2	□	↑	□	□	□
	3	□	□	↑	□	□
	4	□	□	□	↑	□
	5	□	□	□	□	↑

		Aliceの手札				
		1	2	3	4	5
Bob の手札	1	△	〇	〇	〇	×
	2	×	△	〇	〇	〇
	3	×	×	△	〇	〇
	4	×	×	×	△	〇
	5	〇	×	×	×	△

まず Alice は 1 を出したいなら，表 1 の 4 つの表のうち上側の 2 つの表を見て，対戦表用特殊カード表に従って 1 枚目△，2 枚目〇，3 枚目〇，4 枚目〇，5 枚目〇の順に伏せて並べておく．さらに位置表現用特殊カードとして 1 枚目↑，2 枚目□（ブランク），3 枚目□，4 枚目□，5 枚目□の順に伏せて続けて 10 枚を並べておく．Alice が他の手を出したい場合は表を見て同様に 10 枚伏せて並べる．Bob が 2 を出したい場合は 4 つの表の下側の 2 つの表を見て，まず位置表現用特殊カードとして 1 枚目□，2 枚目↑，3 枚目

□，4 枚目□，5 枚目□の順に伏せて，さらに対戦表用特殊カード表に従って 1 枚目×，2 枚目△，3 枚目○，4 枚目○，5 枚目○と続けて順に伏せて 10 枚を並べておく．Alice の伏せた 10 枚と各カードの位置が上下で合うようにする．先に Bob からカードを並べても問題はない．Bob が 2 ではない他の手を出したい場合も同様に表に従って並べる．同じ上下の 10 箇所にある Alice と Bob の 2 枚ペアのカード組 10 組のペアを半分に左右 5 組ずつ分け，5 組ごとにペア関係を維持しつつ位置がわからなくなるまでシャッフルする．このように組内のカードの位置を変えずに組単位でのシャッフルを行う手法のことをパイルスクランブルシャッフルと呼ぶ[3]． その後，組ごとに伏せた状態で 2 枚ごと並べて，左の 5 組の中から Bob のカードのみをすべて公開する．そして右の 5 組の中から Alice のカードのみをすべて公開する．さらに左の 5 組における Bob の↑のカードのペアである Alice のカードと，右の 5 組における Alice の↑のカードのペアである Bob のカードをそれぞれ公開して，これが○ならば↑を出したプレイヤーの勝ち，△ならば引き分け，×ならば負けである．つまり，Alice と Bob はあらかじめ自分の手に対応する相手の可能なすべての手に対する（相手視点の）勝敗表を，カードを用いて表しておき，相手はそれに対して自分の手を↑カードで示したことになる．プロトコルを以下に示す．これは，2 次元配列の横行と縦列が Alice, Bob の手を表している勝敗表を考えると，お互いに選んだ手の行と列の交差するセルを見れば勝敗がわかるわけだが，お互いにどの行，列を選んだかわからないようにすればお互いの手を知らなくても勝敗のみ知ることができるであろう，という方針で考案した．

提案手法（基本版）

前準備・Alice と Bob は自分の番で出すことのできる可能なすべての手の種類を把握しておき，その種類数を m とする．各プレイヤーは，自分の可能な手 m 種それぞれに対して，相手プレイヤーの m 種すべての可能な手に対応する勝敗表と，自分の出す手の位置，ポジションに対応する表を間違いなく作成し保持しておく．一般性を失うことなく，相手が勝つ対戦組み合わせの場合は○，引き分けの場合は△，負ける場合は×を記載する．各プレイヤーは対戦表用特殊カードとして裏面共通の表面○，表面△，表面×のカードをそれぞれルールに合わせて十分に持つ．最大で各 m 枚，したがって最大で合計 $3m$ 枚持つ．さらに自分の手の位置表現用特殊カードとして裏面共通の↑1 枚と□（ブランク）$m-1$ 枚の合計 m 枚を持つ． Alice と Bob の持つ特殊カードの各裏面は，各プレイヤーが手に持っていなかったとしても常に区別がつくようにする．例えば Alice のカードと Bob のカードの裏面の色が異なるようにする．

操作 1・お互いのプレイヤーは，勝敗表と手の表を見て自分の出す手に対応するように特殊カードを裏向きに，配置位置を明確にして順に並べる．

操作 2・お互いの同じ位置に配置された 2 枚ペアカードを組として，左右半分のグループを作った上で各カード組のペア関係を維持したまま，カードの位置が誰にもわからなくなるまで十分に任意の方法でパイルスクランブルシャッフルを行う．

操作 3・左の m 組のペアのうち，すべての組の Bob のカードの表面を公開する．1 つのみ↑のカードであるはずなので，そのペアである Alice のカードもさらに公開する．これが○ならば Bob の勝ち，△なら引き分け，×ならば Bob の負けである．残りの $m-1$ 枚の Alice のカードは公開せずに Alice の手に戻す．

操作 4・右の m 組のペアのうち，すべての組の Alice のカードの表面を公開する．1 つのみ↑のカードであるはずなので，そのペアである Bob のカードもさらに公開する．これが○ならば Alice の勝ち，△なら引き分け，×ならば Alice の負けである．残りの $m-1$ 枚の Alice のカードは公開せずに Bob の手に戻す．

操作 5・操作 3 と 4 で確認した勝敗に矛盾がないことを確認し，その勝負の勝敗として確定させる．

この提案手法（基本版）は、出すことのできる可能な手がゲーム中変化しない場合と，お互いに正直者であるという前提であれば安全に実行できる．もっと言えば，本手法はお互いのプレイヤーを対等にするために対称的な操作手順としているのだが，お互いに正直でミスを起こさない限りは左側 m 組ペアまたは右側 m 組ペアのみの実行でも十分である．

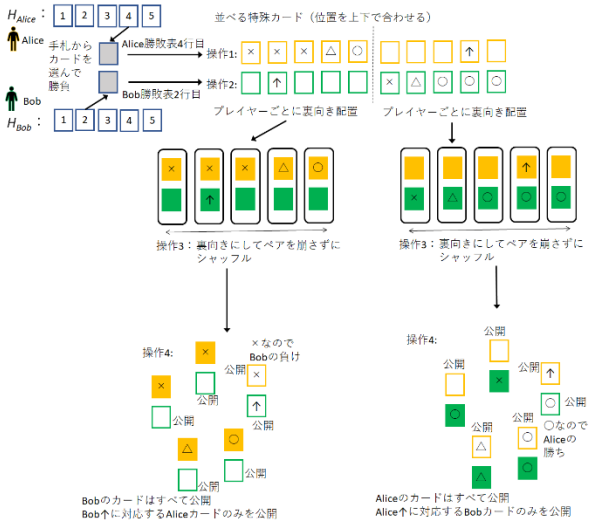

図 1 提案手法（基本版）プロトコル

お互いに正直なプレイヤーであることを仮定し，5 枚ゲームに対する適用例を図 1 に示す．Alice と Bob はあらかじめ表 1 の勝敗表を作成しておく．ゲーム用の合計 10 枚のカード以外に×，△，○の証明用特殊カードをお互いに

十分に持つ．この 5 枚ゲームにおいては，お互いに最大で〇3 枚，×3 枚，△1 枚と，□（ブランク）4 枚，↑1 枚の合計 12 枚で十分である．Alice が 4 を出す場合は手札の 4 のカードは伏せて場に置き，表 1 の 4 行目を見て，Bob が 1 から 3 なら Bob の負けであるから 1 から 3 枚目は×，4 枚目は△，Bob が 5 なら Bob の勝ちだから 5 枚目は〇となっている Alice 勝敗表の 4 行目に基づき特殊カードの並びを×××△〇，□□□↑□の 10 枚にすればよい．Bob が 2 を出す場合は同様に Bob 勝敗表の 2 行目に基づき□↑□□□，×△〇〇〇の 10 枚を，Alice の並べている 10 枚との位置を上下で合わせて並べればよい．その後は位置が合っている上下の特殊カードはペアの関係を崩さずに，左側 5 ペア，右側 5 ペアを別にしてパイルスクランブルシャッフルを行い，左側 5 ペアのついては Bob のカード 5 枚を無条件ですべて公開し，右側 5 ペアについては Alice のカード 5 枚を無条件で公開する．その後，各↑に対応する相手のカード 1 枚をさらに公開してその内容を見て勝敗を判断できる．この例では左側では Bob の↑に対応する Alice のカードは×となっており，これは Bob が負けたことを意味する．また右側では Alice の↑に対応する Bob のカードは〇となっており，これは Alice が勝ったことを意味する．カードゲームとしての勝敗を考えてみても Alice の 4 に対して Bob が 2 であれば確かに Bob の負けなので，この特殊カードによる勝敗判定は正しく機能している．プロトコルにより 1 枚同士の勝敗が決したあとは出したお互いの手札を伏せて捨てる．この方式を用いて勝敗を知る場合，勝ったとしても負けたとしてもこの方式自体からは相手の出したカードを知ることはできない．もちろん，自分が 5 を出したのに負けたのであれば相手は 1 であったことが確実にわかるように，ゲームのルールにより相手の手がわかるようなことは当然ありうる．

ここで問題となるのは，少なくともどちらかのプレイヤーが正直でない場合に不正な処理を実行される可能性がある．例えばジョーカーのようなオールマイティカードがあるゲームの場合，そのような無敵のカードを手札に 1 枚以上持つ可能性があればこれを毎回出すことを示すことにより必ず負けない判定を得ることができてしまう．5 枚ゲームでは初期手札固定のため不正行為，例えば 5 を 2 回使うなどの不正が行われた場合であってもあとから発見しやすいが，初期手札がランダムなゲームにおいては手札を不正に重複して使用されても必ずしも発見できるとは限らない．そこで，このような不正を防ぐことのできる手法を新たに提案する．まずは提案手法の一般的な手順を記載する．その後に図を用いて簡単な場面を用いて手法の説明を行う．この手法は，勝敗表の選択を見せないことにより各プレイヤーが出す手を隠す方針に加えて，以下の方針を追加した．各プレイヤーが出す手札を見せずに勝敗をチェックしたいとき，表の選ぶべき横行と縦列の選択を見せないようにすることで実現するわけだが，ここで出す手に対応しない行，列を選べてしまうと不正が起こってしまう．そこで，実際に勝敗比べに用いる手札 1 枚を鍵として使用し，適切なカードを提示しなければ対応する行，列を選択できなくすれば良い，という方針で考案した．

提案手法（完全版）

2 人のプレイヤーAlice, Bob がお互いの手札 1 枚を出して勝負するカードゲームにおいて，お互いに相手の手札を知ることなく勝敗のみ知ることができる手法

以下の操作について，操作自体を全プレイヤーに公開しながら実施する

前準備・あらかじめ，ゲームに使用するデッキ D に含まれるカードのうち，それぞれのプレイヤーがゲームの上で手札として使用する可能性のあるカードをすべて含む，ゲームで使用するものとは異なるカードで構成された 2 つの証明用デッキ D'_{Alice}, D'_{Bob} をそれぞれ用意し，Alice と Bob はゲームで用いる H_{Alice}, H_{Bob} とは常に区別できるようにしてそれぞれが持つ．D'_{Alice}, D'_{Bob} は対応する各プレイヤーのみが管理し，他のプレイヤーは触れない．2 人はすべてのお互いの m 種の手に対応する $m \times m$ サイズの勝敗表と，自分の出す手の位置，ポジションに対応する表を作成しておく．2 人は D'_{Alice}, D'_{Bob} から，自分が次に出すことのできるすべての可能な手となるカードを取り出し，同じ絵柄，数字のカードが複数枚あればそのうち 1 枚のみでいいのでその種類ごと自分側の勝敗表に対応する各行左方に区別して表面を公開して置いておく．次に 2 人はそれぞれの表に従って m 行分横に，対応する特殊カードの適切な配置を勝敗表通りに公開しながら行う．ここで，勝敗表の 1 セルの大きさを証明用特殊カードの大きさより少し大きめにしておくとそのセルにそのままカードを並べれば良いのでやりやすい．2 人は証明用デッキから並べた 1 列 +自分の手に対応する m 行×特殊カードを並べた $2 \times m$ 列のカードを並べ終わった後に，すべてのカードを裏向きにして，行ごとに左右の位置関係を維持したまままとめて束にしておく．さらに m 種のカード束をお互いに持っていることになるのでそれらの束ごとに，束内の順番を崩すことなく束の位置がお互いにわからなくなるまでシャッフルする．どのように実現するかの例としては物理的に，束ごとに輪ゴムでとめる，または大きめの封筒やカードスリーブに入れることで対応できる．当然使用する封筒やカードスリーブは大きさ等が均一のもので，それをもとに中身が区別できるようなものであってはならない．すべてのカード束は対応する各プレイヤーのみが管理する．

操作 1・お互いのプレイヤー2 人はゲームのルールに則り H_{Alice}, H_{Bob} から出すカードを選ぶ．それぞれ c_{Alice}, c_{Bob} とする．これらをいったん場に伏せて置く．

Vol.2022-GI-47 No.1
2022/3/18

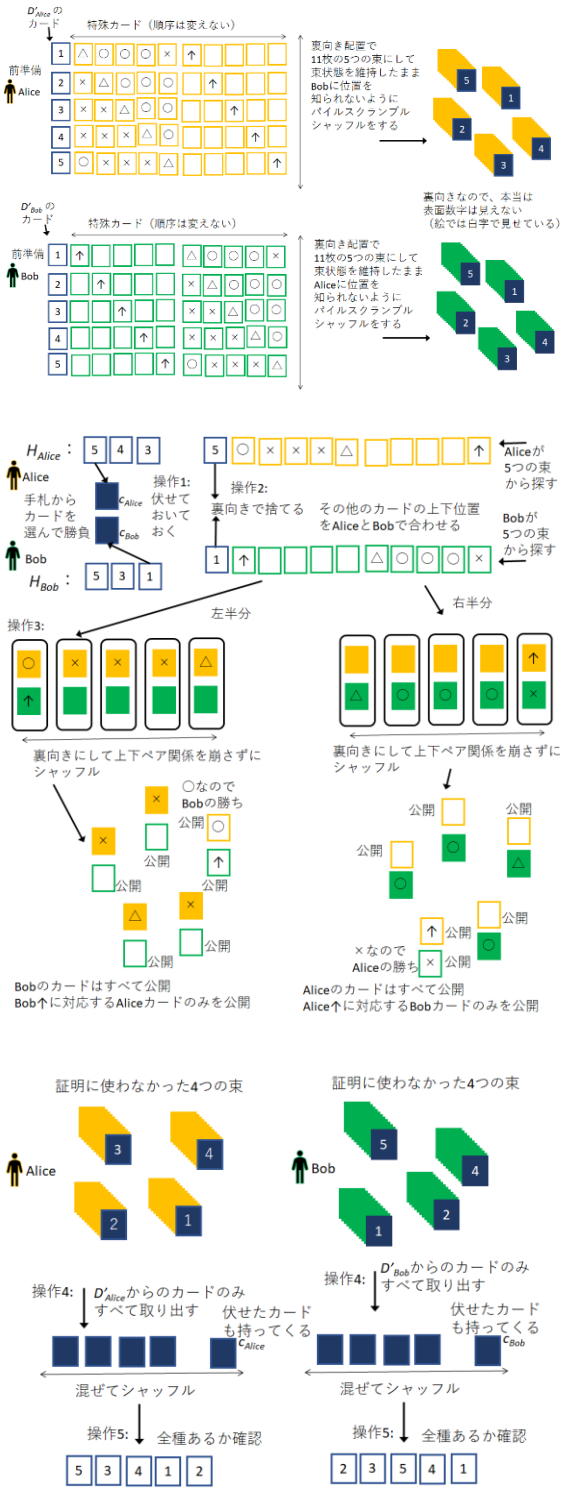

図 2　5 枚ゲームでの提案手法（完全版）の例

操作 2・お互いのプレイヤー2 人は，c_{Alice}, c_{Bob} と同じカードが含まれるような，前準備で作成しておいた m 種のカード束を自分だけ見て，その束を相手に知られないように探し，まずそこからそれぞれ c_{Alice}, c_{Bob} と同じカードを，表面を公開せずに捨てる．同じ束の残りは，c_{Alice}, c_{Bob} に対応した特殊カード配置になっているので，配置を変えることなく裏面のまま並べる．

操作 3・並べた特殊カードを用いて提案手法（基本版）の操作 2 から操作 5 までを順に実行していきカードの勝敗判定を行う．

操作 4・お互いのプレイヤー2 人は，使用しなかったすべての $m-1$ 個の特殊カードの束から，前準備で縦に並べて配置した D'_{Alice} , D'_{Bob} から移動させたカードのみを束ごとに 1 枚ずつ非公開のまま取り出し，さらに操作 1 で手札から伏せたカード c_{Alice}, c_{Bob} を裏向きのまま混ぜて，合計 n 枚のカードの位置がわからなくなるまでシャッフルする．

操作 5・お互いのプレイヤー2 人はシャッフルしたカードを全部表にして，これが前準備で記憶しておいた m 種類と合致するか確認する．合っていなければ，そのプレイヤーは出した手札と異なるカードで勝負するような不正を行ったことになる．

この手法は，手札を同時に出して勝敗を決める対戦型カードゲームであり，勝敗表を作成できるものであればどのようなゲームに対しても対応できる．じゃんけんのようなカードを用いないゲームであってもそれをカードゲームに帰着できれば対応可能となる．

ここで図 2 を用いて例を示す．先に示した 5 枚ゲームの途中場面を考える．$H_{\mathrm{Alice}} = \{5, 4, 3\}$, $H_{\mathrm{Bob}} = \{5,3,1\}$ とする．Alice と Bob の 2 人のプレイヤーは勝敗表用特殊カードとして裏面共通の 25 枚，内訳は○を 10 枚，×を 10 枚，△を 5 枚持つ．さらに位置表示用特殊カードとして裏面共通の 25 枚，内訳は↑を 5 枚，□（ブランク）を 20 枚持つ．前準備として，2 人はあらかじめ，D'_{Alice} , D'_{Bob} から 1 から 5 のカードを公開して表 1 のような勝敗表の各行の横に対応するように公開して並べておき，さらに図 2 上部のように，表 1 をカードの並びで再現するかのごとくに，各行の各セルと同じ絵柄になるように勝敗表用特殊カード，位置表示用特殊カードを公開しながら，すなわちお互いに配置に間違いのないように確認しながら並べる．その後 5 + 25 + 25 = 55 枚をすべてその位置で裏向きにしてから横の位置関係を変えることなく列ごとに 5 種のカード束とする．その後カード順が変更されないように気をつけて各束の確定位置がわからなくなるまで十分にパイルスクランブルシャッフルを行う．ここまでが前準備となる．操作 1 として，Alice が仮に手札 5 を出すとすると，手札から 5 のカードを選び場に伏せ，同様に Bob が 1 を出すとすると，手札 1 を場に伏せる．続いて操作 2 として各プレイヤー2 人はシャッフル後の 5 組の束のうちそれぞれ 5 のカード，1 のカードが含まれる束を探し，それら 5 のカード，1 のカード（各プレイヤーが伏せたカードと表面が同じカード）を裏向きにして捨てる．捨てたあとの残った 10 枚の特殊カードは順序を入れ替えずにお互いに適切な位置を合わせて裏向きで並べる．操作 3 として，適切に並べた左 5 ペア 10 枚と右 5 ペア 10 枚の特殊カードを用いて提案手法（基本版）を行うと Alice の↑に対して Bob×，Bob↑に対して Alice○

となるので Bob の勝ちとなる．確かに Alice が 5 を出し，Bob が 1 を出したので勝敗表通りに結果が出ている上にお互いのカードを見ることなく正しく勝敗を知ることができた．ただし，特殊な勝利条件を満たしているためお互いにそのルールから相手の出した手札を見ることなく知ること自体はできてしまっている．その後，手札が適正に選ばれていたかを確認するために操作 4 として，各プレイヤーが作成した残り 4 組の 1+10 枚のセットから D'_{Alice}，D'_{Bob} からのカード 1 枚を計 4 枚ずつ取り出し，操作 5 として，最初に伏せたカード 1 枚と混ぜて十分にシャッフルしてから公開する．お互いに相手の 5 枚全てを見て 1 から 5 の全種が揃っていれば，不正がなかったことを証明できる．

4. 実際のゲームに対する適用

実際のゲームに対する適用例を示す．例えば最も単純な 2 者対戦ゲームとしては「じゃんけん」がある．じゃんけんは簡単にカードゲーム化でき，対戦表サイズも可能な手数が 3 のため 3×3=9 と少ない．提案手法により，相手の手を見ずに対戦結果のみを正しく知ることが可能である．

別の 2 者対戦ゲームとして「軍人将棋」がある．軍隊で使用される武装等の名称が駒の表面に書かれており，将棋と異なり，自駒が相手駒のマスに入ったとしても即座に相手駒を取ることができず，第三者が自駒，相手駒を見てからさらに勝敗表を見て，勝った駒が盤上に残る．したがって，相手駒の情報を知ることなく勝敗から駒の配置を推測して戦う駒取りゲームである．ゲーム中はすべての相手駒の情報が隠匿されているため対戦ゲームとして遊ぶためには審判である第三者が必須となる．提案手法（完全版）を用いれば操作が煩雑ではあるが審判を必要とせずに遊ぶことができる．軍人将棋の駒はほぼ同じ大きさの裏面共通の駒であるので，駒そのものをカードとみなして提案手法を実行可能である．つまり，全く同じ駒のセットをもう一つ用意することで，それを用いて証明用デッキ D'_{Alice}，D'_{Bob} を構成できる．ただし，お互いに可能な手が 16 種あるため，それらを用いた通常の対戦表サイズが 16×16=256 セルとなり，本提案方式に対応した 4 つの表サイズが単純にその 4 倍であるため，特殊カードもそれぞれ約 500 枚必要となってしまい明らかに煩雑な操作が必要となってしまう．お互いに正直なプレイヤーであるならば，煩雑な提案手法（完全版）でなくても提案手法（基本版）のみでも十分に対戦ゲームとして遊ぶことは可能であり，これであれば必要カード枚数はそれぞれ約 30 枚程度のカード枚数で済むため実用的な時間で遊ぶことができる．この場合証明用デッキとして駒セットをもう 1 つ準備する必要がなくなる．

本稿で示す提案手法（完全版）は，デメリットとしてゲームに使用するカードと全く同一の物理的なカードセットを証明者の人数分必要とする．トランプカードで実行できるゲームであれば同じ絵柄のカードセットを複数デッキ入手することで実現でき，流通量から考えてもそれは容易であるが，現在入手困難なゲームだとセットを複数用意するのは難しいかもしれない．

提案手法はいずれもすべての人間が同じ種類のカードを特定できないことを安全性の根拠としているため，それを擬似的に満たすためにはカードの傷，印刷のかすれなどにより同種のカードの区別がつかないようにすることも必要である．これはカード保護スリーブなどの透明な保護フィルムの中にカードを入れて使用し，スリーブ自体の傷が目立つようになるごとに保護スリーブを交換することにより，理想に近い形で実現できると考えている．

他のカードゲーム，ボードゲームにおいても提案手法が適用できる場面はいくつか考えられる．

5. おわりに

本稿では，カードゲームの途中であっても，プレイヤーの手札に関する秘密計算を比較的短時間，簡単な手法により実現できる手法について紹介した．

既存のカードを用いた金持ち財産比べプロトコル[1]を変更することにより，カードゲームなどで 2 者が持つ情報同士の勝敗をつけたい場合にそれが実現できることを示した．提案手法（基本版）を用いることにより，前準備に手間がかかるが，相手カードの内容を知ることなく手札 1 枚同士の強さ比べを実行できる．そして提案手法（完全版）を適用することにより，不正に手札を使用された場合，それを確実に検知できることを示した．

今後も，今回の手法により示すことのできないような手札に関する秘密計算手法について，さまざまなカードゲームに対応しゲーム中であっても実用的な時間で示すことに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] 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.
[4] “カナイ製作所,” http://kanaifactory.web.fc2.com/products/r/r.html, 参照 2022-01-31.
[5] “GameLife,” https://shop.game-life.jp/blog/2015/04/09/105907, 参照 2022-01-31.
[6] “BGG,” https://boardgamegeek.com/boardgame/112373/braverats, 参照 2022-01-31.