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

Proposal of New Detection Method for Unfair Player of a Card Game Using Physical Zero-Knowledge Proof

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

（2021年6月29日受理）

Physical zero-knowledge proof refers to zero-knowledge proof performed using cards or other physical objects. We propose a new method of Physical zero-knowledge proof. Using our method, it is possible to prove that any player's hand does not contain any particular kinds of card, by using at most twice as many physical cards as the original total number of cards used in a card game. Our method consists of relatively simple steps and is feasible for anyone who can play a card game. With our method, we can play a normal game with N cards, pause the game when needed, use at most the remaining N cards to achieve zero-knowledge proof for anyone's hand, and then we can resume to play the game.

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

1. はじめに

カードゲームはそのルールにおいて歴史的に「各プレイヤーはルールを守り、ルールの判断、解釈を間違わずにゲームを進めることができるような正直者である」ことを前提として作成されているものが多い。ただし、各プレイヤーの持つ手札の内容は非公開であるために、いくつかの不正問題が起こりうる。たとえばほとんどのゲームにおいて、あるカードを手札に持っていないことを示す際にはその事実のみを口頭で示せば良い。ここで、不正なプレイヤーがいるとすると、そのプレイヤーはあるカードを手札に持っているにもかかわらず、持っていないとうそをついてその後のゲーム展開を有利にするかもしれない。プレイヤーによってはカード表面の絵柄、数字等を見間違いし、そのために結果的にうそをつくこともありうる。故意にしろ、そうでないにしろこのような不正が起こったときに低コスト、短時間で発見できる手法があると不正行為の抑止力となるだろう。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不正を発見できる可能性が高いが、そのためにはすべての記録をつける必要がある。手札が非公開のカードゲームにおいてはその記録もつけづらい。また、ゲーム終了時に不正が見つかった場合、そのゲームの結果には信憑性がなくなってしまう。もしも、ゲームの最中にそのような不正行為を逐次発見できれば、ゲームの勝敗結果に及ぼす影響を少なくできるだろう。そこで本稿では、物理的カードを用いたゼロ知識証明を行うことで、このような不正を発見できる手法を提案する。ゼロ知識証明とは、証明者が検証者に対して、ある秘密情報を持っていることを知らせるとき検証者はその事実のみしか知ることができない手法のことである。[1)]　物理的ゼロ知識証明とは、カードやその他物理的な物体を用いて行うゼロ知識証明のことを指し、最近で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を中心に、その解を知っていることの証明に活用できることが知られている。[2)3)]

提案手法は、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、その手札に特定の種類のカードを 1 枚も含まないことをその他すべてのプレイヤーを検証者とみなして証明できる。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。

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、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。デッキは多重集合として表される。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ものとする。すなわち、$\{a,a,b\}$, $\{b,a,a\}$はともに同じデッキとみなす。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。N を、デッキ D のサイズ、すなわちゲームで使用される可能性のあるカードの総枚数とする。n_c を、デッキ D に含まれているカード c の枚数とする。ゲームに参加するプレイヤーの合計数を P とする。ゲーム中、場の中央に置かれ手番プレイヤーがカードを引いて手札に加えるための部分デッキのことを、必要ならば山札デッキ D_{pile} と表現する。D_{pile} はゲーム中に変動していき、日本国内でよく遊ばれているウノのようなゲームでは $D_{\text{pile}} = \varnothing$ （空集合）となった時点で捨て札を再利用してシャッフルし新たなデッキ D_{pile} とすることが多い。D_{pile} の表面の構成内容自体は非公開だが、D_{pile} を構成するカードの枚数は公開情報とする。

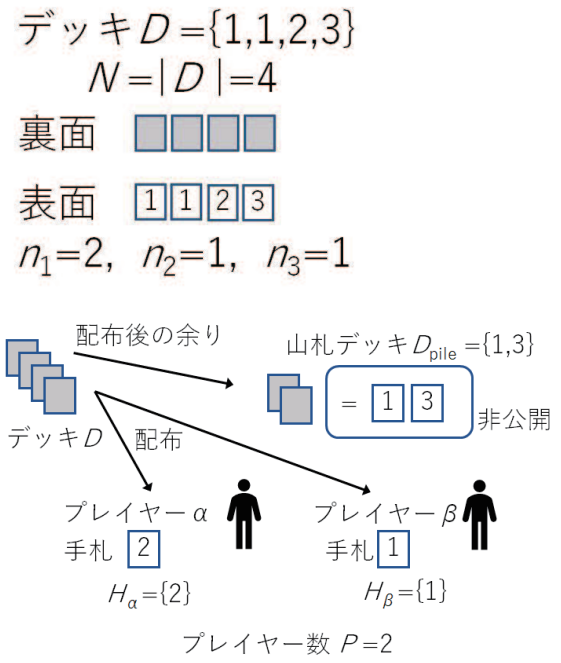

Fig. 1 あるゲームの一場面の例

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。山札デッキ D_{pile} の枚数は 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 D_{pile} 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。

3. 手札に関する物理的なゼロ知識証明を行うための提案手法

ここでは、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で、そのカードのうち半分の 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 枚を用いて手札に関するゼロ知識証明を実

現し、その後にゲームを再開できる手法について説明する。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、ゲームに使用する全カードとまったく構成の同じ N 枚のデッキ D' を、ゲームに使用しないカード束として準備する。手札に関する何らかの証明をしたいプレイヤーは、手札を公開せずに別の場所に伏せて置き、次にゲームに使用しないデッキ D' から一部のカードを抜き去るように公開作成して、そこから元の手札と同じ構成のカードを秘密に取り出して新たな手札とする。最後に伏せておいた元の手札を、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。プログラミングの初心者が学ぶような「変数要素の交換」を彷彿させる手法である。ゲームに使用しないデッキから一部のカードを抜き去った集合を作成する際に、証明したい事柄に応じて適切な選択を行い、何枚かのカードを抜くことで目的を達成できる。

提案手法

プレイヤーp の手札 H_p に特定のカード c_1 が 1 枚も含まれていないことを p が証明する物理的な手法

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。

操作 1・証明者 p を含む任意のプレイヤーは $D_{\text{proof}} = D' - \{c_1\}^{*n_{c\_1}}$ 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。ただし、n_{c_1} は D' に含まれるカード c_1 の総枚数である。したがって、D_{proof} にはカード c_1 が 1 枚も含まれていないことに注意する。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シャッフルする。

操作 2・証明者 p は、H_p の全カード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（手札のカードが複数枚あったときは束状にしてもよい）おいておく。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もとの H_p と同じ構成（すなわち T_p と同じ構成）になるように秘密に選び、それらをすべて抜き取って新たな手札 H'_p とする。その後残った D_{proof} のすべてのカードを裏向きにしておく。

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 のすべてのカードの表面を見ずに、操作 3 で $|H_p|$ ($=|T_p|$) 枚のカード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} からのものか、T_p からのものかどちらか、全プレイヤーに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、これが操作 1 で作成した $D' - \{c_1\}^{*n_{c\_1}}$ 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 にはカード c_1 が 1 枚も含まれていないことが証明される。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。

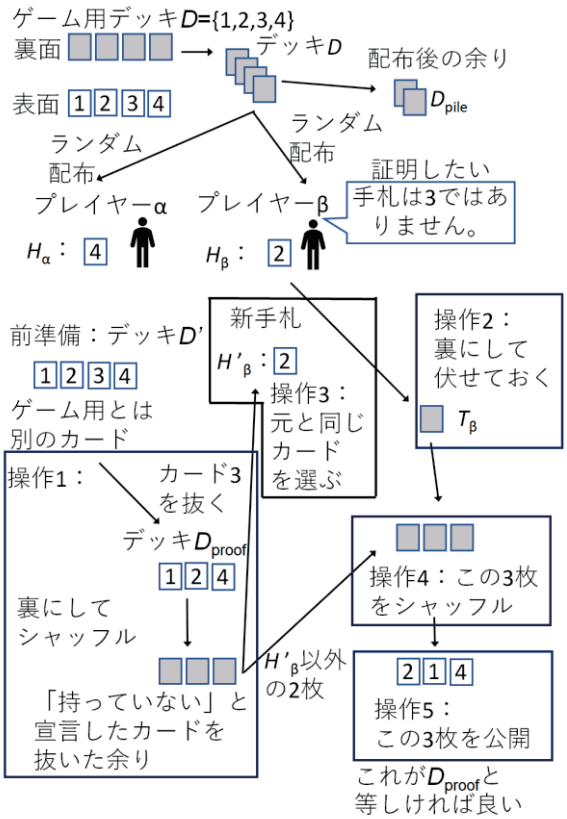

Fig. 2 あるゲームに対する提案手法の適用

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。

考えるゲームでは全 4 枚のカードデッキ D={1,2,3,4} を初期デッキとする。2 人のプレイヤー α、β はシャッフルされた山札デッキ 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数を宣言し当てることができたら勝ち、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_α={4}, H_β={2} であったとする。 α

が最初の手番として、「あなたの手札は 3 ですか」と β に聞いたとする。ここで β は手札が 3 のカードでないことを示さなくてはならない。これを提案手法で実現できることを説明しよう。前準備としてプレイヤー α、β 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'={1,2,3,4}を用意する。操作 1 により、D' から表面を公開しながら 3 のカードを抜き、残り 3 枚のデッキを D_{proof}={1,2,4}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、β は持っている 1 枚の手札（2 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_β={2}とする。操作 3 として、β は D_{proof} の 3 枚のカードから自分のもとの手札と同じカード（2 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} ={1,4}となるがこの内容を β 以外のプレイヤーが知ることはない。操作 4 として、α、β のどちらかは D_{proof} に T_β 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 α、β 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{1,2,4}となっているので、プレイヤー β は手札に 3 のカードを持っていないことを証明できた。そして、操作 3 で手札を変更もしていないことも明らかである。

証明者であるプレイヤー p が不正行為を行った場合、それを必ず見つけることができる。プレイヤー p の行う可能性のある不正は、次に示す 2 種類が考えられる。1 つは、そもそもカード c_1 を 1 枚以上手札に持っていたのに「c_1 を持っていない」とうそをつき、それにかかわらず提案手法により証明を試みようとした場合である。もう 1 つは、「c_1 を持っていない」という宣言自体はうそではなく、手札もそのようになっているが、操作 3 で D_{proof} から新たな H'_p を構成する際に、今後のゲームに都合の良いようなものを選び任意の手札に変更する場合である。

まず、前者の行動を行うと、操作 3 において D_{proof} にはカード c_1 が 1 枚も含まれていないため、元の手札と同じ構成を抜き出すことができない。当然、元の枚数と異なる枚数のカードを手にした場合はその時点で不正となる。したがって、枚数を合わせるために元の手札とは異なるカードをいくつか手に取るしかない。そして、その後に混ぜるカード集合 T_p の中には持っていないと宣言したはずのカード c_1 が含まれている。したがって、操作 5 における D_{proof} の公開時に、c_1 が少なくとも 1 枚含まれるという矛盾が必ず生じるためその不正を確実に発見できる。

次に後者の行動を行うと、やはり操作 3 で D_{proof} から抜き取るカードと操作 4 で D_{proof} に加えるカードが異なるため、操作 5 の公開時に矛盾が生じるためその不正を確実に発見できる。

正直なプレイヤー p が提案手法を用いたとき、特定のカードを持たない、というただちに得られる情報以外に、操作 5 において公開された D_{proof} から他のプレイヤーはプレイヤー p の手札の情報 $H'_p = H_p$ をまったく得ることができない。なぜなら、全プレイヤーが D_{proof} の表面を確認できるのは、操作 1 で D_{proof} を作成した時点と操作 5 で公開したときのみであり、操作 5 時点での D_{proof} を $D_{\mathrm{proof\_5}}$ とし、操作 1 時点での D_{proof} を $D_{\mathrm{proof\_1}}$ としたとき、$D_{\mathrm{proof\_5}} = D_{\mathrm{proof\_1}} - H'_p + H_p$ である。 ここで p が正直であれば当然 $H'_p = H_p$ であるので問題なく $D_{\mathrm{proof\_5}} = D_{\mathrm{proof\_1}}$ となり、直前のシャッフルによりどのカードが $D_{\mathrm{proof\_1}}$ から抜かれて、どのカードが追加されて $D_{\mathrm{proof\_5}}$ になったのかはまったくわからないため、この集合の公開からは既知の情報しか得ることができないためである。

4. おわりに

本稿では、カードゲームの途中であっても、プレイヤーの手札に関する物理的ゼロ知識証明を比較的短時間かつ簡単に実現できる手法について紹介した。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に特定のカードがまったく含まれないことを、その事実以外を知らせずに確実に証明できる。物理的ゼロ知識証明を含む、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活用が見込まれており、本提案手法もその 1 つとなりうると考えている。今後も、今回提案した手法により証明できないような不正が起こりうる場面において、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証明できる方式を考案していきたい。

参 考 文 献

1) 辻井 重男，笠原 正雄 : 情報セキュリティ　暗号・認証・倫理まで，昭晃堂，pp. 92--95, 2003.

2) 水木 敬明 : カード組を用いた秘密計算，電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review 9(3), pp. 179--187, 2016.

3) 水木 敬明 : カードベース暗号の最近の動向，SITA2018 特別セッション(情報セキュリティ)スライド.