Vol.2019-AL-173 No.2
2019/5/10

# のりのり, 変形版へやわけのゼロ知識証明に対する物理プロトコル

迫田 賢宜[1,a)]　小野 廣隆[1,b)]

**概要**：ゼロ知識証明とは, 証明者が「ある命題が真であることを知っている」と伝えるのに, それ以外の知識を漏らすことなく, 検証者に証明できるようなやりとりの手法である. これは情報セキュリティに大きく関わる手法であるが, カードなどの物理的な道具を用いることによっても実装可能であることが知られている. これらのプロトコルは, 人の手によって道具を用いて実行されるため, 高校生といった非専門家にもプロトコルの安全性や実行の過程などを理解しやすいという利点をもつ.

2009 年に数独に対する物理的ゼロ知識証明プロトコルが考案されて以降, さまざまなペンシルパズルに対する物理プロトコルが考案されている. 本研究では NP 完全問題として知られる, のりのりと変形版へやわけの 2 つのペンシルパズルに対する物理プロトコルを考案する.

**キーワード**：ゼロ知識証明，物理プロトコル，ペンシルパズル

# Physical Protocols for Zero-knowledge Proofs of Norinori and Heyawake Variant

Genki Sakoda[1,a)]　Hirotaka Ono[1,b)]

***Abstract:*** Zero-knowledge proof, which is a method of cryptography, is known to be implemented by some physical items. Since physical protocols were designed for zero-knowledge proofs of Sudoku in 2009, a variety of pencil puzzles' protocols are proposed. These physical protocols have advantage for non-experts to understand their security easily.
In this paper, we give physical protocols for zero-knowledge proofs of two pencil puzzles, Norinori and Heyawake variant.

***Keywords:*** zero-knowledge proof, physical protocol, pencil puzzle

## 1. はじめに

暗号理論の中に, ゼロ知識証明といわれるものがある. これは高い計算能力をもつ証明者（Prover）と多項式時間の計算能力しかもたない検証者（Verifier）によっておこなわれる対話型証明の一種である. ある命題が真であることを知っている証明者 P は, それ以外の情報を漏らすことなく検証者 V にそのことを納得させなければならない. さらに, 証明者 P が命題が真であることを知らない場合, 検証者 V は高い確率でそのことを見抜くことができる必要がある. 以降, 証明者 P, 検証者 V をそれぞれ P, V と呼ぶ.

ゼロ知識証明は公開鍵暗号やデジタル署名など, 実生活にさまざまな応用をもつ. しかし, これらのプロトコルはコンピュータ上で処理されるため, 非専門家にはその仕組みや安全性などが理解しにくいという側面がある.

2009 年には, トランプのようなカードを用いた, 数独に対する物理的ゼロ知識証明が考案された. これらのプロトコルは物理的なアイテムを用いて人の手によりプロトコルがおこなわれるため, 非専門家にもゼロ知識証明がどのよ

[1] 名古屋大学大学院情報学研究科
Graduate school of Informatics, Nagoya University
[a)] sakoda.genki@i.mbox.nagoya-u.ac.jp
[b)] ono@i.nagoya-u.ac.jp

うなものであるのかがわかりやすい, という教育上の利点をもっている.

この数独に対する物理プロトコルが考案されて以降, 時間ドロボー [6] といったパズルや美術館, カックロ, ケンケン [1] など, さまざまなペンシルパズルに対する物理プロトコルが考案されている. また,「非専門家にもわかりやすくゼロ知識証明の概念を伝える」ため, 問題サイズに対して用いられるアイテムの数や手順がより少ないプロトコルも考案されている [3][8].

そこで本論文では, NP 完全問題として知られる「のりのり」と「変形版へやわけ」という 2 つのペンシルパズルに対して, 物理プロトコルを提案する.

## 2. ペンシルパズルの物理的ゼロ知識証明

ゼロ知識証明は, 次の 3 つの性質を満たす.

(完全性) P が「ある命題が真である」と知っていれば, V は必ず P を受理する

(健全性) P が「ある命題が真である」と知らなければ, V は十分高い確率で P を拒否する

(ゼロ知識性) V はプロトコルにおいてどのように振る舞っても「ある命題が真である」以外の情報を得ることができない

本論文で考えるのは, 以下のようなシチュエーションである. まず与えられたパズルの解盤面を, 高い計算能力をもつ P は知っているが, 多項式時間の計算能力しか持たない V は自力で求めることが難しい. そして P は自分が解盤面を知っていることを V に伝えたいが, 解盤面を V に明らかにすると V がパズルを解く楽しみがなくなってしまうので, それはおこなわない. 同様に解盤面に関する情報は一切漏らさない. これらの条件のもとで, P が正しい解盤面を知っていると V に納得させる手法を, ペンシルパズルのゼロ知識証明とよぶ.

## 3. 数独に対する物理プロトコル

ここでは, 先行研究で考案された数独に対する物理的ゼロ知識証明プロトコルを紹介する [3]. まず, 数独とは次のルールに従い, 各セルに数字を埋めるペンシルパズルである. これは NP 完全であることが示されている [2].

**問題 (数独)** n × n のグリッドが m × m のサブグリッドに分割されており（$n = m^2$）, いくつかのセルに数字が書かれている. このとき, 各行, 列, サブグリッドに 1 から $n$ までの数字がちょうど一回ずつ現れるよう, セルを埋めることができるか.

この問題に対しては次のプロトコルが考案されている. なお, ここで使用されるアイテムは表が 1 から $n$, 裏が同一のカードを $3n$ セット, つまり $3n^2$ 枚のカードである.

**数独に対する物理的ゼロ知識証明プロトコル**

- P は各セルに, 解盤面と一致するカードを 3 枚ずつ裏返して置く. あらかじめ数字が書かれていたセルにはその値と一致するカードを表にして置く
- V は各行, 列, サブグリッドごとに 3 枚のうちからランダムにカードを 1 枚選ぶ
- P は選ばれたカードを各行, 列, サブグリッドごとにまとめ, パケットを作る. パケットごとにカードをシャッフルし, V に返す
- V は返されたパケットの中身を確認し, すべてのパケットにおいて 1 から $n$ の数字がちょうど一回ずつ現れていれば受理. そうでなければ拒否

このプロトコルにおいて, 解盤面に関する情報は一切漏れていない. このプロトコルは 2009 年に考案されたものであるが, その後 Sasaki らによって改良されたプロトコルが登場し, 必要なカードの枚数が $3n^2$ から $2n^2 + n$ に削減されている [8].

## 4. のりのり, 変形版へやわけに対する物理プロトコルとその解析

### 4.1 id づけによるカード列の復元

本小節では考案プロトコルに用いる, カード列の復元のための操作の説明を与える. id づけとは, 裏のままのカード列に対し, 同枚数の数字が描かれたカードを使用することでカード列の表を確認することなく初期順列を復元するプロトコルである. id づけには, 橋本らによって考案されたパイルスクランブルシャッフルを利用する [4].

以下が, id づけの具体的な手順である.

(1) id づけを施したいカード列 $v$ を置き, その下に 1 から $n$ の数字カードを順に並べる

| ? | ? | ? | … | ? |
|---|---|---|---|---|
| 1 | 2 | 3 | … | $n$ |

(2) 下段の数字カード列を裏にし, 上下を組にしたままガード列をランダムシャッフルする

| ? | ? | ? | … | ? |
|---|---|---|---|---|
| ? | ? | ? | … | ? |

(3) プロトコルの必要に応じて, 上段のカード列を表にして確認する.
このとき, 上段のカード列の初期順列に関する情報は全く漏れていない

(4) 確認後, 上段のカード列を裏にして再びランダムシャッフルする

(5) 下段のカードを表にして, 上下の組を保ったまま 1 から昇順に並べ替える

| ? | ? | ? | … | ? |
|---|---|---|---|---|
| 1 | 2 | 3 | … | $n$ |

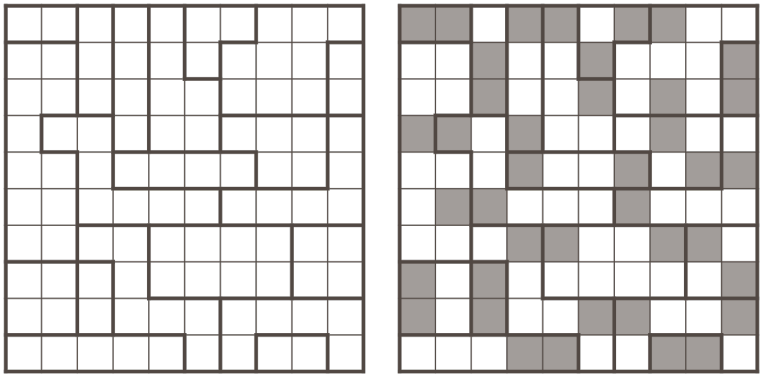

**図 1** のりのりの初期盤面 (左) と解盤面 (右)

以上の操作を行うことで, カード列の初期順列に関する情報を明らかにすることなく, そこに含まれるカード列の内容を知ることができる. さらにカード列の初期順列を復元することも可能である.

### 4.2 のりのりに対する物理的ゼロ知識証明

まず, のりのりの問題を紹介したあと, それに対する物理的ゼロ知識証明を提案する.

**問題 (のりのり)** m × n のグリッドが適当に分割されている. このとき, 次の条件をすべて満たすようにセルを黒く塗ることができるか.

- 各分割されたエリア（以降, 部屋と呼ぶ）にはちょうど 2 つの黒マスが入る
- 黒マスはちょうど 1 つの黒マスと隣接する

この 2 つがペンシルパズルのりのりの条件であるが, その初期盤面と解盤面を図 1 に示す.

これに対するプロトコルに用いるのは表が黒または白で, 裏が同一のカードである.

**のりのりに対する物理的ゼロ知識証明プロトコル**

- P は盤面の各セルに一致する黒または白のカードを 6 枚ずつ裏返して置く. さらに盤面の上下左右の外部にも白カードを 1 枚ずつ置く
- V は (a)(b) の検証のどちらかをランダムにおこなう

(a) P は各セルをパケットにし, 袋に入れる. V は袋からランダムにパケットを取り出し, 表にする. すべてのパケットでカードの色がそろっていれば受理

(b) V は以下の検証をおこなう

- ∗ V はランダムに部屋を指定し, P は各セルからカードを 1 枚ずつ取ってきて, カード組をシャッフルする. カードを表にして, 黒カードの数がちょうど 2 枚であれば受理. これをすべての部屋に対しておこなう
- ∗ V はランダムにセルを 1 つ指定する. P は指定されたセルに置かれたカードを最低面, それに隣接する 4 枚のカードをその上に重ね, パケットを作る. これをすべてのセルに対しておこなう. V は m × n 個のパケットからランダムに 1 つ取り出し, 最低面を確認. 最低面が白であればそのパケットを破棄, 黒であれば展開し, パケット内にちょうど 2 枚の黒カードがあれば受理. これをすべてのパケットに対しておこなう

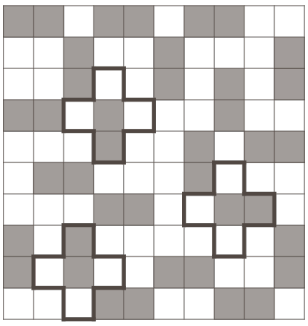

**図 2** のりのり 第 2 条件の検証

図 2 にあるように, (b) の 2 つめの検証をおこなった場合, 最低面が黒であれば必ずそのパケットには黒カードがちょうど 2 枚含まれる.

解盤面を知らない（悪意のある）P は, V によってランダムでおこなわれる 2 つの検証 (a)(b) のどちらも満たすようなカード配置はできない. よってこのプロトコルを $l$ 回繰り返すことによって, この P が拒否される確率は $1 - \left(\frac{1}{2}\right)^l$ である.

### 4.3 変形版へやわけに対する物理的ゼロ知識証明

本小節では変形版へやわけに対する物理的ゼロ知識証明を提案する. 以下が変形版へやわけの問題である.

**問題 (変形版へやわけ)** m × n のグリッドが長方形に分割されていて, いくつかの長方形の内側に数字が埋められている. このとき, 次の条件をすべて満たすようにセルを黒く塗ることができるか.

- 黒マスは隣接しない
- 数字はその長方形内に塗られる黒マスの数
- 白マスは縦, 横方向に 3 つ以上連続して部屋をまたがない

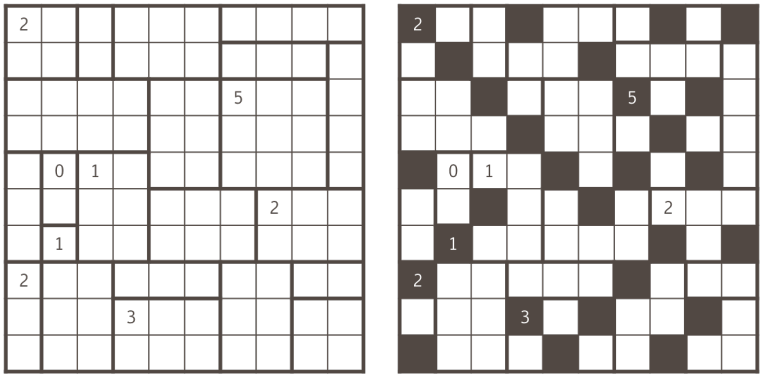

**図 3** 原型へやわけの初期盤面 (左) と解盤面 (右)

へやわけ問題の原形では上に加えて,

- 黒マスで盤面を分断しない

という条件が含まれる. このへやわけ問題の原形は NP 完全, さらに変形版へやわけも NP 完全であることが知られている [5].

この問題に対する提案プロトコルを以下に記す. 用いるアイテムは 2 種類のカードであり, 表の柄が異なる. 1 つは黒または白の色カード, もう 1 つは 1 から $n$ の数字（$n$ は盤面内の長方形の最大サイズ）が書かれた数字カードである. どちらも裏にすると区別のつかない同一の柄であるとする.

**変形版へやわけに対する物理的ゼロ知識証明プロトコル**

- P は盤面の各セルに一致する黒または白のカードを裏返して置く
- V は順に P の置いたカードが, このパズルの条件を満たしているか確認する.
  以降このプロトコルにおける各検証では, 前述の id づけによるカード列の復元をおこない, 盤面を復元するものとする
  - V はランダムに盤面から隣接する 2 つのセルを選び, P はカードを取ってくる. P は選ばれたカードを確認し, （黒, 白）であれば白を, （白, 白）であれば黒のカードを追加し, シャッフルして V に渡す. V は渡されたカード組が（黒, 白, 白）であれば受理. これをすべての隣接するセルに対しておこなう.
  - 各部屋に対する黒マスの数は, のりのりと同様の手法で確認する
  - V はランダムに 1 部屋を縦断または横断するセルと, それに同方向に隣接するセルを 1 つずつ選ぶ. P は選ばれた範囲のカードを取ってくる. P はカードを確認し, そこに含まれる黒のカードの数が「含まれうる黒カードの最大数（つまり範囲のサイズを L とすると, $\lceil \frac{L}{2} \rceil$）」に達していなければ, 黒カードをその枚数になるまで追加する. そして追加した黒カードとの合計が $\lfloor \frac{L-1}{2} \rfloor$ になるように白カードも追加する. シャッフルして返却されたカード組に, 黒いカードが「そこに含まれうる黒カードの最大数」含まれれば V は受理. これをすべての 3 長方形の境界を含む範囲に対しておこなう.

プロトコルの最後の検証は, 指定した範囲がすべて白マスであった場合のみ, 拒否される仕組みになっている. もし, 指定した範囲がすべて白マスであった場合, プロトコルにしたがってカードを追加しても「そこに含まれうる黒マスの最大数」には達しないことがわかる. 図 4 を例にして示すと, ここでは 2 境界をまたぐ連続した 5 つのセルが選択されている. このとき黒カードは 1 枚置かれているので 2 枚の黒カードを追加する. もし黒カードが 2 枚置かれていれば追加するのは黒カード 1 枚と白カード 1 枚である. 選択された範囲がすべて白カードであれば, 2 枚の黒カードを追加してもこの範囲に含まれうる最大枚数である 3 枚には達しない.

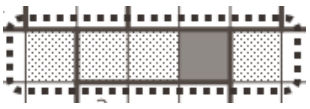

**図 4** 変形版へやわけ 第 3 条件の検証

## 5. おわりに

本論文では, NP 完全問題である 2 つのペンシルパズル, のりのりと変形版へやわけに対する物理的ゼロ知識証明プロトコルを考案した. 今後の課題としては, 変形版へやわけに対するプロトコルの健全性誤りの解析や, どちらのプロトコルに対しても必要なアイテム数や手順の削減が挙げられる.

### 参考文献

[1] Bultel X., Dreier J., Dumas J., Lafourcade P.: Physical Zero-knowledge Proofs for Akari Takuzu, Kakkuro and Kenken - Fun with Algorithms, LIPIcs, vol. 49, pp 8:1–8:20 (2016).
[2] Colbourn, c.: The complexity of copleting partial latin squares, Discrete Applied Mathematics, vol. 8, pp. 25–30

(1984).
[3] Gradwohl, R., Naor, M., Pinkas, B., Rothblum, G.: Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles, Theory of Computing Systems. 44(2), pp. 245–268 (2009).
[4] Hashimoto, Y., Shinagawa, K., Nuida, K., Inamura, M., Hanaoka, G.: Secure grouping protocol using a deck of cards, ICITS 2017. LNCS, vol. 10681, pp. 135–152. Springer (2017).
[5] Holzer M., Ruepp O.: The Troubles of Interior Design - A Complexity Analysis of the Game Heyawake - 4th International Conference on Fun with Algorithms, Lecture Notes in Computer Science, vol.4475, pp.198–212 (2007).
[6] Ueda, K., Nishimura, H.: Physical Zero-Knowledge Proof Systems for Instant Insanity, Publications of the Research Institute for Mathematical Sciences, vol.1849, pp. 120–126 (2013).
[7] Nishida, T., Hayashi, Y., Mizuki, T., Sone, H.: Securely computing three-input functions with eight cards, IEICE Transa. Fundamentals, vol.E98-A, no.6, pp.1145–1152 (2015).
[8] Sasaki, T., Mizuki, T., Sone, H.: Card-Based Zero-Knowledge Proof for Sudoku, LIPIcs-Leibniz International Proceedings in Informatics, vol. 100, pp. 29:1–29:10 (2018).