ISSN 2186-5647



2-4

# 複数種のスリーブを利用した数独に対するシャッフル１回の物理的ゼロ知識証明

日大生産工(院)　○菅野 力　　日大生産工　栃窪 孝也

## 1. まえがき

数独に対する物理的ゼロ知識証明は、数独の解を知る証明者が解についての情報を一切明かすことなく、「解が存在し、証明者が解を知っていること」をトランプなどの身近にあるもので検証者に納得させるものである。物理的ゼロ知識証明は、コンピュータなどの電子端末を一切用いずに、トランプなどの物理的なカード組を用いて、カードのシャッフルなどの人間の手によって行うことのできる操作を活用して実行されるため、プロトコルが正しく実行されているかを実際に目で確認することができ、ゼロ知識証明の概念を知らない非専門家にも理解しやすく、暗号分野への興味関心を持つ人を増やすという教育的価値がある。近年、数コロ[1]やナンバーリンク[2]のような、様々なパズルに対しての物理的ゼロ知識証明が多く研究され、提案されている。

数独に対する物理的ゼロ知識証明においては、2007年にGradwholらによって初めて提案された[3]。そこから幾度も改善が重ねられ、近年では、シャッフル操作1回のみで実行することができるゼロ知識証明が提案されている[4]。しかし、この提案では、連続して行うシャッフルを1回のシャッフルとして許容しているため、個々のシャッフルの回数で見てみると、複数回行われている。

そこで本研究では、複数種のスリーブを利用し、連続的なシャッフルを利用しない、シャッフル1回のゼロ知識証明を提案する。

## 2. 準備

### 2.1 数独

数独は、代表的なペンシルパズルの1つである。標準的な数独は、9×9の盤面を九つの3×3ブロックで区切られており、初期配置として1から9の数字があらかじめ一部のマスにおかれている状態が問題として与えられる(図1左)。解答者は、数字が配置されていないマスに対して、各行、各列、各ブロックに1から9の数字が一つずつ現れるように数字を配置していくことを目指していく(図1右)。

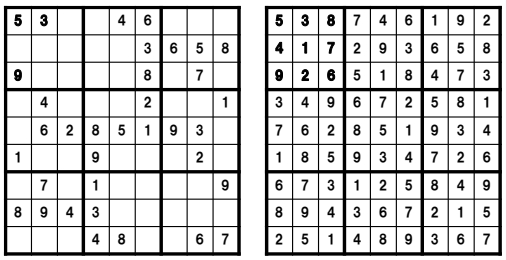


図１　9×9 数独の初期状態(左)と解(右)

### 2.2 ゼロ知識証明

ゼロ知識証明は、証明者Pと検証者Vとの間に行われる対話証明の一種であり、証明者Pが検証者Vに対して、「$x$の解$w$が存在し、Pが解$w$について知っていること」を、解に関する情報をVに一切明かすことなく証明することである。一般的にゼロ知識証明は、Pが$w$を知っていれば、Vは常に納得する完全性、Pが$w$について知らなければ、Vは否定する健全性、そして、Pの持つ命題が真であるならば、Vはその命題が真であること以外の情報を得ることができないゼロ知識性の三つの特性を満たしている必要がある。

## 3. 証明に用いる道具

証明に用いる道具として、カード、スリーブ、丸形のシールを使用していく。

**カード:** 数独の解を表現するために使用する。カードは黄色、赤色の1～9の数字カード各9枚ずつを9セット(計162枚)必要とする。カードの裏面は黄色、赤色のカード関係なく全て同一の絵柄である(図2)。

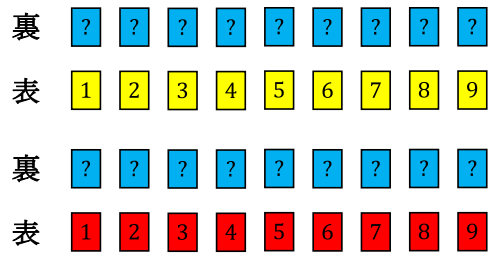


図２　使用するカード

**スリーブ:** 次節で紹介するシャッフルに使用

---

Physical Zero-Knowledge Proof with a Single Shuffle for Sudoku Using Multiple Types of Sleeves

Chikara SUGANO and Kouya TOCHIKUBO

するために使用する。スリーブは片面のみ不透明なものを使用し、黄色、赤色、青色のものを各27枚(計81枚)必要とする。

**丸形のシール:** スリーブに貼り、スリーブを区別させるために使用する。丸形のシールについても、スリーブと同じく、黄色、赤色、青色のものを各27枚(計81枚)必要とする。

## 4. 証明で行う操作

### 4.1 パイルスクランブルシャッフル

Ishikawaらによって提案されたシャッフルの手法である[5]。このシャッフルは、同じカード枚数からなる$k$個のカード束の列に対するシャッフル操作であり、一様なランダムな置換$\pi \in S_k$に従って並べ替えを行う。ここで$S_k$はk次対称群を表す。例として、カード束の列$(p_1, p_2, \cdots, p_k)$にパイルスクランブルシャッフルを適用すると、出力として$(p_{\pi^{-1}(1)}, p_{\pi^{-1}(2)}, \cdots, p_{\pi^{-1}(k)})$が得られる。これは、$k$個のスリーブを用いることにより、物理的に容易に実現できる。

### 4.2 秘匿置換

秘匿置換は、相手にどのカードを配置するのかを知られないようにカードを置換する操作である。今回の提案プロトコルやOnoらのプロトコルでは、同じカード枚数からなる$k$個のカード束の列に対して行い、カード束の中から一つを選び、数独の解の通りに各行、各列に対して秘匿置換を行い配置する[4]。

## 5. プロトコルの手順

9×9マスの数独のゼロ知識証明は各行、各列、各ブロックに1から9のカードがあることを示していく。本章では、本研究が提案する9×9マスの数独に対するプロトコルの手順について、以下に示す。なお今回、数独の初期状態、解については図1のものを用いる。

(i) 準備

(1) PとVは各マスに対し、上段三行には黄色、中段三行には赤、下段三行には青といったようにスリーブを配置する。

(2) PとVは各マスに配置されているスリーブに対し、左三列には黄色、真ん中三列には赤、右三列には青のシールをスリーブの不透明な面に貼り付ける。この操作により、スリーブの種類は9種類となる(図3)。

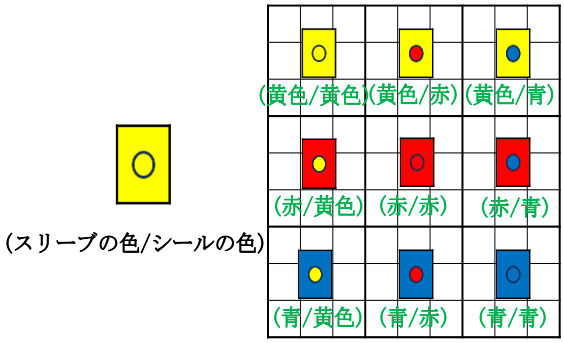


図 3 スリーブの配置

(3) PとVは1から9の番号が付いた黄色と赤のカード1枚ずつでカード束を9個作成する。

(4) Pはカード束をランダムに一束選択し、黄色のカードは1行目(図4黄色枠)、赤のカードは1列目(図4赤枠)となるように、秘匿置換操作によって数独の解の通りに裏向きに配置する。この時、黄色のカードは左、赤のカードは右に置く。この操作を$i$行、$i$列目$(1 \leq i \leq 9)$に対して行う。

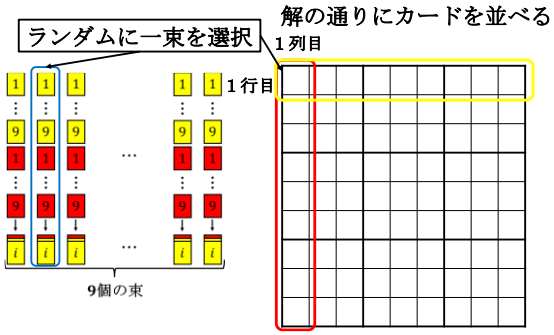


図 4 カード束に対する秘匿置換操作の例

(5) 各マスの裏向きの2枚のカードを右のカード(赤のカード)が上にくるように重ね、一つの束にする。図5は重ねた後の状態である。

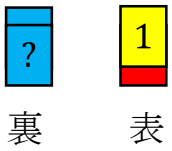


図 5 カード束の作成

(ii) 検証

(1) Vは既に解が分かっているマスにあるカード束を表向きにし、2枚のカードの数字とそのマスの解が等しいことを確認する。解と数字が異なる場合、また、表向きにしたときに、黄色のカードが上に配置されていない場合、証明は棄却される(図6)。

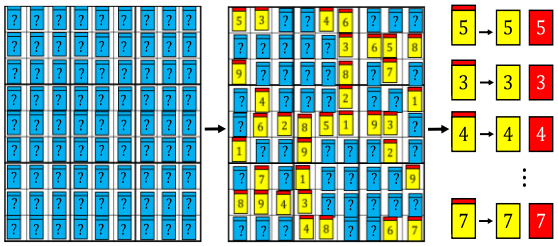

図 6　初期状態のマスの確認

(2)　各マスの束を、準備フェーズの(2)で作成した9種類のスリーブ各9枚に図3に従って挿入する。

(3)　81枚のスリーブに対するパイルスクランブルシャッフルを行う。

(4)　Vはスリーブからカードを取り出し、カードを表向きにして、81個の束に対して以下のことを確認する。

A)　同じ種類のスリーブから取り出されたカードを確認し、1〜9のカードがそれぞれあることを確認する(図7)(ブロック検証)。

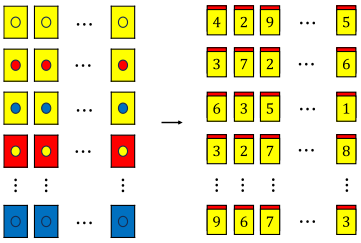

図 7　ブロック検証

B)　同じ束にある2枚のカードが全て同じ数字であることを確認する(図8)。どれか一つでも数字が異なっている場合、また黄色のカードがカード束の上に配置されていない場合は証明が棄却される(行・列検証)。

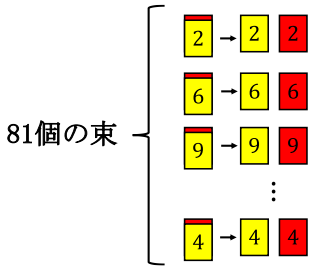


図 8　行・列検証

この二つのどちらかでも確認できない場合があれば、証明が棄却される。以上が本研究の提案プロトコルであり、棄却されなかった場合には証明が受理される。

## 6.　提案プロトコルの正当性

本章では、提案プロトコルが完全性、健全性、ゼロ知識性を満たしていることを確認する。

**完全性:**

Pが解を知っているとする。そのとき、証明者Pが回答に従ってカードを配置すると、各行、各列には1から9までの数字カードがそれぞれ1枚ずつ入っている。また、スリーブにカードを挿入した際、各ブロックは図3の通りになり、1から9の数字カードがはいっていることになる。そして各マスには同じ数字を持つカードが2枚含まれている。色についても黄色、赤の2色のカードが含まれており、黄色が上、赤が下に含まれている。パイルスクランブルシャッフルを実行しても、この状態が変化することはない。よって、プロトコルは途中で棄却されることなく終了する。したがって完全性を満たす。

**健全性:**

検証者Vが証明を受理したとする。そのとき、各カード束には同じ数字のカードが2枚入っている。また、黄色のカードが上に、赤色のカードが下に含まれており、取り出されたスリーブは、元々図3のとおりとなっている。これにより、黄色のカードが各行、赤色のカードが各列、そしてスリーブはブロックを表している。カードを配置時、入力が制限されているため、各行、各列は1から9までのカード一枚ずつで構成されている。また、検証時、同じ種類のスリーブから1から9までのカード束が一個ずつあることにより、ブロックについても行、列同様に1から9のカードが構成されていることになる。よってPが解に従って配置していることになる。すなわち、Pが解に従って配置していない場合は、証明は拒否される。したがって健全性を満たす。

**ゼロ知識性:**

カードがめくられるのは、検証フェーズの(1)と(4)である。(1)については既に分かっている解のマスの開示であり、(4)については、確認をする前にパイルスクランブルシャッフルを適用するため入力に関する情報は一切漏れることはない。したがってゼロ知識性を満たす。

## 7.　プロトコルの比較

本章では、各プロトコルについての比較を行う。各プロトコルの比較については、表1に示している。

本研究の提案プロトコルはOnoらのプロトコル[4]を改善したものであり、複数種のスリーブを活用することにより、連続するシャッフルを適用することなく、シャッフル1回のみでプロトコルを実行することができる。スリーブについては9

表１　9×9 マスの数独における各プロトコルの比較

| プロトコル | カード枚数 | シャッフル回数 | カードの色の数 | 秘匿置換回数 | スリーブの色の数 | スリーブ枚数 | シール枚数 |
|---|---|---|---|---|---|---|---|
| Onoら[4] Protcol 1 | 162枚 | 1（連続PSS許容） | 1 | 18 | 1 | 81枚 | 0枚 |
| Onoら[4] Protcol 2 | 162枚 | 1（連続PSS許容） | 2 | 9 | 1 | 81枚 | 0枚 |
| Onoら[4] Protcol 3 | 162枚 | 1（連続PSS許容） | 6 | 3 | 1 | 81枚 | 0枚 |
| 佐々木–品川[6] プロトコル1 | 243枚 | 1 | 1 | 27 | 1 | 81枚 | 0枚 |
| 佐々木–品川[6] プロトコル2 | 243枚 | 1 | 3 | 9 | 1 | 81枚 | 0枚 |
| 佐々木–品川[6] プロトコル3 | 243枚 | 1 | 9 | 3 | 1 | 81枚 | 0枚 |
| 提案プロトコル | 162枚 | 1 | 2 | 9 | 9 | 81枚 | 81枚 |

種類別々のものを用意しても実行は可能ではあるが、3色の丸形シールを使うことにより、スリーブを3種類だけで、9種類のスリーブを表現することができる。また、今回提案プロトコルでは、カードの種類を黄色と赤の2種のカードを使用しているが、Onoらのプロトコルのように、使用するカードの種類を変えてプロトコルを実行することが可能であり、これによりカード枚数、シャッフル回数、秘匿置換回数はOnoらのプロトコルと変わることはない。佐々木らのプロトコル[6]についてもシャッフル1回のみでプロトコルを実行できるため提案プロトコルと比較してみると、ブロック検証分のカード枚数を削減している。

## 8. まとめ

本研究では、9種類のスリーブを利用して、連続的なシャッフルを適用しないシャッフル1回のプロトコルについて提案した。なお、この提案プロトコルは$n \times n$マスの数独についても実行することができ、必要なカード枚数は$2n^2$枚、スリーブ枚数、およびシール枚数は$n^2$枚、秘匿置換回数は$n$回で実行することができ、シャッフルについては変わらず1回でプロトコルを実行することができる。

しかし、シール分の道具を増やしており、スリーブの種類も増やしている。そして、シールを貼る操作も手順に含まれている。また、秘匿置換に関しても、各行、各列に対して行っており、数回実行しないと検証が行うことができないため、あまり効率がいいプロトコルであるとは言えない。今後の課題としては、シールを用いずに今回のプロトコルを実行する方法、また秘匿置換回数を削減できるような方法などの効率性、またカード枚数が$n^2$枚で実行することができるプロトコルについて検討することが挙げられる。

参考文献


1) S. Sasaki and K. Shinagawa, “Physical zero-knowledge proof for sukoro,” In New Generation Computing, (2024), pp.391-398.

2) R. Ruangwises and T. Itoh., “Physical zero-knowledge proof for numberlink,” In 10th International Conference on Fun with Algorithm, FUN2021, Vol.157 of LIPIcs, (2021), pp.21:1-22:11.

3) R. Gladwohl, M. Naor, B. Pinkas, and G.N. Rothblum., “Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles,” In Fin with Algorithms, 4th International Conference, FUN 2007, (2007) pp.166-182.

4) T. Ono, S. Ruangwises, Y. Abe, K. Hatsugai, and M. Iwamoto, “Single-shuffle physical zero-knowledge proof for sudoku using interactive inputs,” 信学技報, vol.124, no. 21, ISEC2024-3, (2024) pp. 13–19.

5) R. Ishikawa, E. Chida, and T. Mizuki. “Efficient cardbased protocols for generating a hidden random permutation without fixed points,” In Unconventional Computation and Natural Computation - 14th International Conference, UCNC 2015, Vol. 9252 of Lecture Notes in Computer Science, (2015) pp. 215–226.

6) 佐々木 駿, 品川 和雅, “対話入力を用いたパイルスクランブルシャッフル１回の数独に対する物理的ゼロ知識証明,” コンピュータセキュリティシンポジウム（CSS2024), 4H4-1, (2024) pp.1-8.