2ZD-09

両面不透明スリーブを用いた数独のゼロ知識証明 *

田中　滉大 †　水木　敬明 ‡
† 東北大学工学部電気情報物理工学科　‡ 東北大学サイバーサイエンスセンター

1　はじめに

1.1　数独

数独（*Sudoku*）は，代表的なペンシルパズルの 1 つである．標準的な数独の問題は 9 つの 3×3 ブロックに区切られた 9×9 の盤面を用い，一部のセルにはあらかじめ 1 から 9 の数字のいずれかが置かれている．プレイヤーは残りの空のセルに各行，各列，各 3×3 ブロックに 1 から 9 の数字がちょうど 1 つずつ現れるように数字を置いていくことを目的とする．

1.2　数独のゼロ知識証明

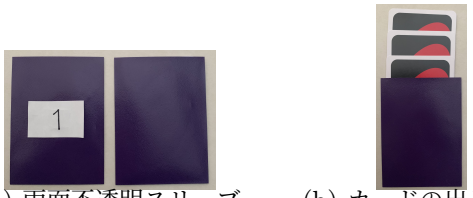
本稿では，数独に対する**ゼロ知識証明**を扱う [1–5]．すなわち，ある数独の問題とその解を知る証明者 P，解を知らない検証者 V がいる状況を仮定し，証明者 P が検証者 V に対して，「与えられた数独の問題の解が存在し，証明者 P がその解を知っていること」を解についての情報を一切明かさずに納得させることを実現する．ゼロ知識証明は一般に，**完全性**，**健全性**，**ゼロ知識性**の 3 つの性質を有することを要請する．

また，本稿で扱うゼロ知識証明は，物理的なカード組を用い，人間の手でプロトコルを実行する**物理的なゼロ知識証明**である．これは，プロトコルが正しく実行されていることの確認が容易であり，ゼロ知識証明の概念を知らない非専門家も理解しやすく，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などの利点を有する．

1.3　既存プロトコルと本稿の貢献

2007 年に Gradwhol ら [1] は数独に対する初の物理的なゼロ知識証明プロトコルを構築し，以後 Sasaki ら [3] により健全性エラーのないプロトコルが，Ruangwises [4] によりトランプカードを用いたプロトコルが，また著者らにより UNO を 2 セットを用いたプロトコルが提案された [5]．

本稿では UNO を 2 セットと両面不透明スリーブを用いた新しいプロトコルを提案する．既存プロトコルとの比較を表 1 に示す．提案プロトコルは，カード枚数とシャッフル回数が少なく，プロトコルの途中で証明者の知識が不要であり，健全性エラーを持たない．具体的には，UNO カード 90 枚，番号付きスリーブ 27 枚を用い，シャッフル回数 11 回でゼロ知識証明を実現する．なお，著者らは SCIS 2023 にて（両面不透明ではない）番号付きスリーブ 81 枚を用いたプロトコルも提案している [6]．



(a) 両面不透明スリーブ　(b) カードの出し入れ

図 1: 両面不透明スリーブの使用

2　両面不透明スリーブ

提案プロトコルでは両面が不透明なスリーブを用いる．また図 1（a）のように両面不透明スリーブの片面に番号をつける．以後，両面不透明スリーブを単にスリーブと呼ぶことにする．（番号を付ける面を工夫することで，片面不透明なスリーブでも代用可能と考えられるが，詳細は省略する．）

3　提案プロトコル

本節では，9×9 数独に対するゼロ知識証明を実現するプロトコルを構築する．プロトコルは証明者 P によるカードの配置を入力とし，色検証，行検証，ブロック検証・色変更，列検証の順に行う．1 から 27 の番号をつけた 27 枚のスリーブと UNO の黄色，赤，青の 1 から 9 のカード 3 セットを用意し，以下の手順により，検証者 V に各行，各列，各 3×3 ブロックに 1 から 9 の数字がちょうど 1 回ずつ現れることを納得させる．各検証では，解のカードを取り出してスリーブに入れ，シャッフルを行い，カードの表面を確認，再びシャッフルを行い，スリーブの番号を参照しカードを元の位置に戻すという流れで行う．以下では，紙面の都合上概略のみ記述する．

3.1　証明者によるカードの配置

まず，証明者 P と検証者 V はすでに数字が書かれているセルに対応する数字のカードを裏向きに置く．ただし，上 3 ブロックには黄色のカード，中 3 ブロックには赤のカード，下 3 ブロックには青のカードを置く．その後，解を知っている P は解に従って，残りの空いているセルにもカードを上述と同じ配色で（V に見られないように）裏向きに置く．

---

* 数独 (Sudoku) は，Nikoli Co., Ltd. の商標あるいは登録商標である．

Zero-Knowledge Proof for Sudoku Using Double-Sided Opaque Sleeves
Kodai TANAKA†, Takaaki MIZUKI‡,
†Department of Electrical, Information and Physics Engineering, Faculty of Engineering, Tohoku University
‡Cyberscience Center, Tohoku University

表 1: 提案プロトコルと既存プロトコルとの比較

プロトコル	カード枚数	シャッフル回数	スリープ枚数（シャッフル実装時）	実装可能なカード種	証明者の知識
Sasaki ら（A）[3]	90	45	9	トランプ 9 セット UNO 5 セット	不要
Sasaki ら（B）[3]	171	36	9	トランプ 18 セット UNO 9 セット	不要
Sasaki ら（C）[3]	243	28	81	トランプ 27 セット UNO 14 セット	要
Ruangwises (Method A) [4]	120	108	9	トランプ 3 セット	要
Ruangwises（Method B）[4]	108	322	6	トランプ 2 セット	要
田中ら [5]	117	16	27	UNO 2 セット	不要
提案プロトコル	90	11	27	UNO 2 セット	不要

3.2 色検証

ここでは，横 3 ブロックが同色であることを検証する．1 から 27 の番号の付いた 27 枚のスリーブそれぞれに，図 1（b）のように 3 枚ずつカードを入れる．各 3 枚は，上 3 ブロック，中 3 ブロック，下 3 ブロックから（相対的な順番を維持して）1 枚ずつ取り出し，入れるものとする．次に，27 枚のスリーブをシャッフルし，各スリーブの 1 番上のカードをチェックすることで上 3 ブロックが黄色のカード 1 から 9 が 3 枚で構成されていることを確認する．チェックしたカードはスリーブ内の 1 番下に移動する．再度シャッフルを行い，同様に中 3 ブロックが赤のカード 1 から 9 が 3 枚で，下 3 ブロックが青のカード 1 から 9 が 3 枚で構成されていることを確認する．最後にまたシャッフルを行い，スリーブの番号を確認しソートすることで，元の配置に戻す．

3.3 行検証

ここでは，各行が 1 から 9 番の数字で構成されていることを検証する．まず，$1, 4, 7$ 行目のカード 27 枚が黄色，赤，青の 1 から 9 で構成されていることを確認する．ここから色検証の結果と合わせると，$1, 4, 7$ 行目が 1 から 9 番の数字で構成されていることがわかる．同様に $2, 5, 8$ 行目も検証する．また，ここまでの検証と色検証の結果から残りの $3, 6, 9$ 行目も自動的にそれぞれ 1 から 9 番の数字で構成されていることになる．

3.4 ブロック検証・色変更

ここでは，各 3×3 ブロックが 1 から 9 番の数字で構成されていることを検証する．同時に，黄色の 1 から 9 のカードを追加し，列の検証を行えるよう，左 3 ブロックが黄色，中央 3 ブロックが赤，右 3 ブロックが青のカードとなるよう色を変更，すなわち縦 3 ブロックが同色となるよう変更する．

3.5 列検証

ここでは，各列が 1 から 9 番の数字で構成されていることを検証する．行検証のように $1, 2, 4, 5, 7, 8$ 列目が 1 から 9 番の数字で構成されていることを検証する．また，ここまでの検証と色検証，色変更の結果から残りの $3, 6, 9$ 列目も自動的にそれぞれ 1 から 9 番の数字で構成されていることになる．

4 おわりに

本稿では，数独に対する新たな物理的ゼロ知識証明プロトコルを提案した．提案プロトコルでは，9×9 の数独に対して，UNO と両面不透明スリーブを用い，カード枚数とシャッフル回数の少ない，効率的なゼロ知識証明プロトコルを実現した．具体的には，90 枚のカードと，11 回のシャッフル回数で実行できる．今後の課題として，数独や他のペンシルパズル等を対象とした，より少ないシャッフル回数とカード枚数で実現可能な新たなプロトコルの構築に取り組む．

参考文献

[1] Gradwohl, R., Naor, M., Pinkas, B. and Rothblum, G. N.: Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles, *Fun with Algorithms* (Crescenzi, P., Prencipe, G. and Pucci, G., eds.), LNCS, Vol. 4475, Berlin, Heidelberg, Springer, pp. 166–182 (2007).

[2] Gradwohl, R., Naor, M., Pinkas, B. and Rothblum, G. N.: Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles, *Theory of Computing Systems*, Vol. 44, No. 2, pp. 245–268 (2009).

[3] Sasaki, T., Miyahara, D., Mizuki, T. and Sone, H.: Efficient card-based zero-knowledge proof for Sudoku, *Theor. Comput. Sci.*, Vol. 839, pp. 135–142 (2020).

[4] Ruangwises, S.: Two Standard Decks of Playing Cards are Sufficient for a ZKP for Sudoku, *New Gener. Comput.*, Vol. 40, pp. 49–65 (2022).

[5] 田中滉大，水木敬明：UNO を用いた数独に対するゼロ知識証明について，研究報告アルゴリズム（AL），Vol. 2022-AL-189（5），pp. 1–8 (2022).

[6] 田中滉大，水木敬明：番号付きスリーブを活用した数独のゼロ知識証明，2023 年暗号と情報セキュリティシンポジウム（SCIS 2023），No. 3D2-3, pp. 1–8 (2023).