再考：ステンドグラスパズルに対するカード型ゼロ知識証明

野田 陸翔[1]　吉塚 創也[2]　櫻井 幸一[3]

概要：ステンドグラスパズルは各ピースを赤または青の 2 色の内いずれかに塗り分けるパズルでありピースの境界には赤・青・黄色の点があり，それぞれの点に隣接するピース群が，指定された色の過半数または同数になるように配置しなければならないという条件付きのパズルである。このパズルは最近 NP 完全性が証明された[WAAC'23]。さらにこのステンドグラスの色の塗り分け問題の解に対する，物理的なカードを用いたゼロ知識証明プロトコルも提案された[Ieice/Comp 技報 2024-11]。本研究では，この既存プロトコルにおいて，証明者が正しい解答を知らずとも，条件を満たすようカード列を操作してプロトコルを通過することができる健全性の問題点を明らかにする． さらに， この問題を解消する改良プロトコルも提案する．

キーワード：ゼロ知識証明，ステンドグラスパズル，カードベース暗号，パズル，健全性

Revisited: Card-Based Zero-Knowledge Proofs for Stained Glass Puzzles

Rikuto Noda[1], Souya Yoshizuka[2], Koichi Sakurai[3]

Abstract: The Stained Glass Puzzle is a type of puzzle where each piece is colored in one of two colors: red or blue. On the boundaries of the pieces, there are red, blue, and yellow dots. Based on these dots, the adjacent group of pieces must be arranged to contain either a majority or an equal number of the specified color. Recently, the NP-completeness of this puzzle has been proven (WAAC'23). Furthermore, a zero-knowledge proof protocol using physical cards has been proposed for the solution to this Stained Glass Problem (IEICE/Comp Tech Report 2024-11). In this research, the existing protocol's soundness issue, wherein the prover can manipulate the card sequence to pass the protocol without knowing the correct answer, is highlighted. Additionally, an improved protocol to address this issue is proposed.

Keywords: Zero-knowledge proof, Stained Glass Puzzle, card-based cryptography, puzzle, soundness

1. はじめに

1.1 ステンドグラスパズルとカード型ゼロ知識証明

ステンドグラスパズル[1]は，各ピースを赤または青の 2 色のいずれかに塗り分けるパズルである．ピースの境界には赤・青・黄色の点が配置されており，それぞれの点に隣接するピース群が，その点で指定された色の過半数または同数になるように配置しなければならないという制約条件を持つ．

ステンドグラスパズルは高石ら [4] によって NP 完全性が証明されている．高石らは任意のステンドグラスパズルの盤面を，NP 完全であることが知られている 3SAT 問題へ変換することが可能であることを示した．

これまでに研究されてきたパズルの多くは、碁盤の目の上の数字列を扱うものが多い(ニコリ社の分類[3]でいうところの″数字のパズル″)．これに対して，ステンドグラスパズルは，盤面にある丸をヒントにして、線で区切られた部分(ピースと呼ぶ)のいくつかを塗り分ける(ニコリ社の分類での″絵のパズル″)．特に，この色を塗り分けられるピースの形状が不定であるという特徴を持つパズルである．このため，既存のパズルに対するゼロ知識証明プロトコルとは様相が異なり，新たなプロトコルの設計が課題であった．これに対して，ステンドグラスパズルに関しても，解の存在を証明する物理的なカードを用いたゼロ知識証明プロトコルが提案された[2].

しかし，本研究では，この既存プロトコル[2]において，証明者が正しい解答を知らずとも，条件を満たすようカード列を操作してプロトコルを通過することができるという健全性の問題を明らかにし，我々はそれに対する解決法も提案する．

1 九州大学工学部電気情報工学科
Department of Electrical Engineering and Computer Science, Faculty of Engineering, Kyushu University
2 九州大学大学院システム情報科学府
Graduate School of Information Science and Electrical Engineering, Kyushu University
3 九州大学大学院システム情報科学研究院
Faculty of Information Science and Electrical Engineering, Kyushu University

1.2 健全性の問題点と改良策

パズル問題に対するゼロ知識証明プロトコル(ZKP)とは，証明者 P が，そのパズルの解を知っていることを，検証者 V に解に関する知識を与えずに証明するものである．多くのパズルに対する ZKP は次の基本構造で構築されている．

I. 証明者 P が検証者 V に明かすことなく解答を作成し，コミットメントする．
II. 作成した解答が,すべての解の条件を満たすかどうかを，作成した解答に関する情報を漏らさずに(V が知ることなく)検証する．
III. 解答がすべての解の条件を満たしているとき，その解答が解である．したがって証明者が作成した解答が解であることから，証明者 P が解を知っていることが示される．

この基本構造では，健全性が(II)の検証に依存することに注意する．

ステンドグラスパズルに対する既存プロトコル[2]では，(I)が行われておらず，毎回作成したカード列に対して(II)を行っている．つまり(I)と(III)が連携しない構造のプロトコルとなっている．このため，実際には，証明者 P が作成した解答が解であると示すことが必要であるが，作成した解答が存在しなくとも，結果的に受理される結果となっている．

本研究で指摘する問題点は，「問題を部分(局所)問題に分割し，すべての部分問題を証明することで全体（大域）を証明する」型のプロトコルにおいて，異なる部分問題で共通して使用されるべき値が一貫していない可能性があることに起因する．ここで，ステンドグラス問題の部分問題とは，1 つの点において「隣接するピースの色の数が，点の色が赤（青）のとき過半数は赤（青）であり，点の色が黄色のとき赤と青の数が同数である」という条件を満たすか否かを判定することである．

我々が提案する改良手法では，異なる部分問題で使用される値の参照元となる共通のカード列 S を用意し，使用の度に参照することで値の一貫性保証を実現する．これにより，既存プロトコル[2]の健全性問題を解決し，ステンドグラスパズルが，カード型ゼロ知識証明を持つことの証明を完結させる．

1.3 カード型 ZKP の健全性証明と知識の証明系

物理的カードを用いた NP 完全問題に対する証明プロトコル群の健全性は，すでに Gradwohl ら[3]が議論している．Gradwohl らは，6 つのプロトコル(前半の 2 つは古典的暗号技術の対話型 ZKP，後半の 4 つは物理的カード型 ZKP)を提案し，それぞれの健全性と知識の証明（Proof of Knowledge）[7,8]に言及している．その中で，5 つ目の方式では,健全性誤差ゼロも実現している．特にカード型 ZKP の評価尺度として、必要なカードの枚数,シャッフル回数に加えて，健全性誤差は重要な評価項目となっており， ゲーム問題に対するカード型 ZKP で、健全性誤差ゼロの実現が 1 つの研究主題の現状にある[10].

Gradwohl らの原論文[3]の議論と証明とが十分な完全性（か否か）に関しては，本論文の最後に記述するが，すでに宮原ら[13]は，健全性誤差ゼロのカード型 ZKP の多くは、実質的に検証者に依存しない非対話型であること考慮したモデルの定式化を与えている． さらには，この非対話型モデルの変形を，シャッフルをオラクルとする(証明ではなく)検証モデルと解釈する研究への展開も始まっている[14].

本論文の最後では、健全性の厳密な証明に向けての今後の課題を論じる。

2. ゼロ知識証明について

ゼロ知識証明は，秘密情報を開示することなく，その情報を知っているということだけを相手に証明する暗号学的手法である[7]．ゼロ知識証明プロトコルが満たすべき基本的な性質として，以下の三つが挙げられる：

完全性：正当な証明者が正しい秘密を知っている場合，検証者は高い確率でその証明を受理する
健全性：不正な証明者が秘密を知らない場合，検証者は高い確率でその証明を棄却する
ゼロ知識性：証明過程において，秘密そのものに関する情報が一切漏洩しない

近年，コンピュータを用いた従来の暗号学的手法とは異なり，トランプカードや封筒などの身近な物理的道具を活用したゼロ知識証明プロトコル[5]が注目を集めている．これらは物理ゼロ知識証明プロトコルと呼ばれ，専用の電子計算機器を必要とせず，計算論を専門としない一般の人々にも理解しやすいという長所が評価されている．

論理パズルの分野において，物理ゼロ知識証明プロトコルは特に有用性を発揮する．数独[5]を筆頭に，様々なパズル[8,9]に対して，解を秘匿しながらその存在を証明するプロトコルが開発されており，教育的な観点からも価値ある研究分野として活性化している．

3. ステンドグラスパズルについて

3.1 ステンドグラスパズルの定義 [1,4]

ステンドグラスパズルは，各ピースを赤または青の 2 色のいずれかに塗り分けるパズルである．ピースの境界線上には予め赤，青，黄色のいずれかの色に塗られた点が存在している．各点に隣接するピース群は，その点の色によって以下の条件を満たさなければならない：

- 点の色が赤の場合：隣接するピースの過半数が赤色でなければならない
- 点の色が青の場合：隣接するピースの過半数が青色でなければならない
- 点の色が黄色の場合：隣接するピースの赤と青の数

が同数でなければならない
すべての点の色は問題設定時に予め決定されている．

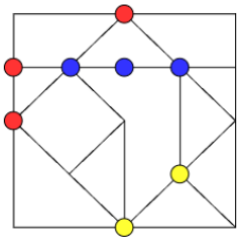

図 1 ステンドグラスパズルの例[2]

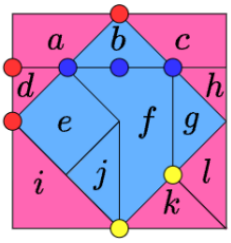

図 2 解答例[2]

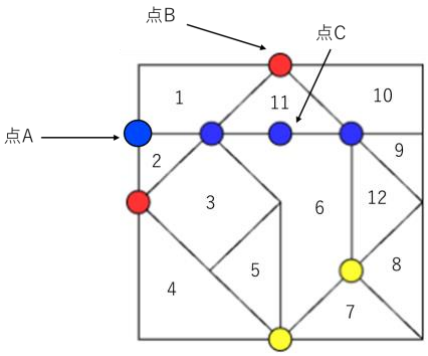

図 3　解が存在しないステンドグラスパズル

次に，解の存在しないステンドグラスパズルについて説明する．解が存在しないとは，どのような色の塗り分けを行っても，少なくとも 1 つの点で制約条件を満たすことができないことである．

図 3 は図 1 のパズルにおいて点 A の色のみを赤から青に変更したパズルである．図 3 のパズルにおいて，点 A と点 C の色は青色であり，点 B の色は赤色である．先述した制約条件により，各点に隣接するピースの過半数は当該点と同じ色でなければならない．点 A が青色であることから，点 A に隣接するピース 1，2 のうち過半数は青色でなければならず，点 C が青色であることから，点 C に隣接するピース 6，11 のうち過半数は青色でなければならない．

しかしながら，点 B は赤色であるため，点 B に隣接するピース 1, 11, 10 のうち過半数は赤色でなければならない．ここで，ピース 1 は点 A と点 B の両方に隣接し，ピース 11 は点 C と点 B の両方に隣接している．点 A の制約を満たすためには，ピース 1，2 のうち少なくとも 2 個が青色である必要があり，点 C の制約を満たすためには，ピース 6，11 のうち少なくとも 2 個が青色である必要がある．

一方，点 B の制約を満たすためには，ピース 1，11，10 のうち少なくとも 2 個が赤色である必要がある．各ピースは赤色または青色のいずれか一方の色のみを持つことができるという制約の下では，すべての点 A，点 B，点 C の制約条件を同時に満たすピースの色の組み合わせは存在しない．

以上の分析により，図 3 のパズルでは点 A，点 B，点 C のうち少なくとも一つの点において，隣接するピースの過半数が当該点と同じ色になるという制約条件を満たすことができない．したがって，図 3 のパズルには解が存在しない．

3.2 ステンドグラスパズルの NP 完全性

ステンドグラスパズルに関する解の存在判定問題は，その NP 完全性が最近， 高石らによって証明された[4]．高石らは NP 完全問題である 3SAT の任意のインスタンスを，ステンドグラスパズルの盤面へ変換することが可能であることを示した．

4. 利用するカードおよびシャッフルの定義

4.1 利用するカードの定義

本プロトコルで利用するカードは次の 2 種類である：

- カード 1：表側が♣または♡の 2 種類のいずれかであり，裏側が?のみの 1 種類であるカード．プロトコル[2]では赤く塗られたピースに♡，青いピースに♣が対応する．
- カード 2：表側に 1, 2, ...のような自然数が表記されており，裏側が?のみの 1 種類であるカード．

4.2 使用するシャッフルの定義[12]

石川ら［12］によって提案されたシャッフルの技法であるパイルシャッフルを，ここでも利用する．

- ✓ **シャッフル**：m 枚のカードが裏向きに配列された状態 $(c_1, c_2, \cdots, c_m)$ において，m 次対称群 S_mから任意に選択された置換 $\sigma \in S_m$を適用し，$(c_{\sigma^{-1}(1)}, c_{\sigma^{-1}(2)}, \cdots, c_{\sigma^{-1}(m)})$ を出力するする操作を「シャッフル」と定義する．
- ✓ **パイルスクランブルシャッフル**：複数のカードからなる束を基本単位としたシャッフルである．この手法では，各束を単一のカードと同等に扱い，束単位でのシャッフルを実行する．具体的には，m 個の束が裏向き状態で配列された $(p_1, p_2, \cdots, p_m)$ に対して，m 次対称群 S_m から任意選択された置換 $\rho \in S_m$ により $(p_{\rho^{-1}(1)}, p_{\rho^{-1}(2)}, \cdots, p_{\rho^{-1}(m)})$ を出力する操作を指す．

5. 既存プロトコル[2]

5.1 既存プロトコルの概要

既存プロトコル[2]では，赤く塗られたピースに♡，青いピースに♣が対応する．プロトコルの概要は次の３つ手順である：

(1) 証明者 P は，ある点において，その点に隣接するピースの色に対応したカードを裏向きに並べ, カード列 Aα を作成する

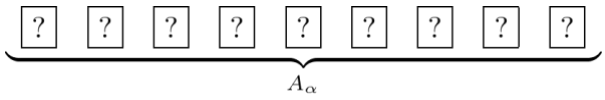

図 4 カード列 A α

(2) 点の色に応じて以下を証明する：

- 点の色が赤（青）の場合：カード列 Aα の過半数のカードが♡（♣）であること
- 点の色が黄色の場合：カード列 Aα の♡と♣のカードが同数であること

(3) すべての点に対して上記の手順を繰り返す

これにより，すべての点が制約条件を満たすことを示し，証明者 P が正しい解答を知っていることを主張するものである．

なお，本論文では，手順（1）の問題点を指摘し，その改善策を論じる．

5.2 （2）の具体的な内容

カード列 Aα のカード枚数を N 枚とする．

(1) 証明者 P は検証者 V に対して 1 から N までの番号が記載された N 枚のカードを提示する．その後，カードをシャッフルし，カード列 Aα の下に裏向きで配置する．この新たなカード列を Bα とする．

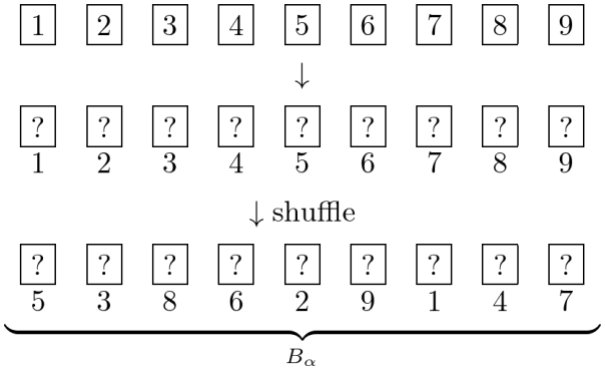

図 5 カード列 B α 作成の例[2]

(2) P は，V から見えない状態で Bα の番号を確認し，点と同色のピースの下に配置されたカードの番号を記憶する．ただし，点が黄色の場合は記憶する必要はない．

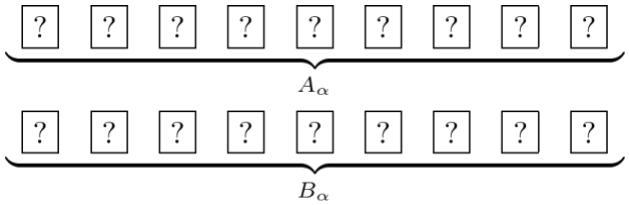

図 6 (2)の例[2]

(3) Bα の下に, 1 から N までの番号が記載されたカードを昇順で裏向きに配置する. この新たなカード列を Cα とする．

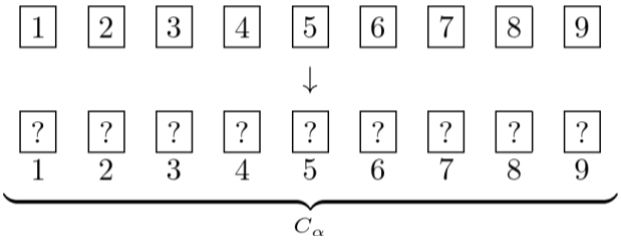

図 7 カード列 C α の作成例[2]

(4) Aα，Bα，Cα の 3 つの列を束にまとめ，パイルスクランブルシャッフルを実行する．

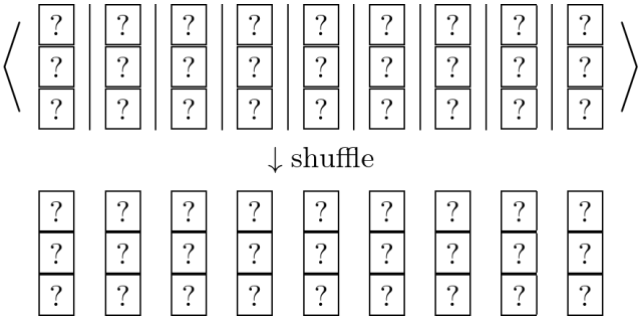

図 8 (4)の例 1，2，3 行目はカード列 A α，B α，C α [2]

(5) Bα を開示し，P は以下の手順を実行する：

- 点が赤色または青色の場合：(2)で記憶した点と同色のピースに対応する番号のカードの上に配置された Aα のカードを[N/2] + 1 枚開示する

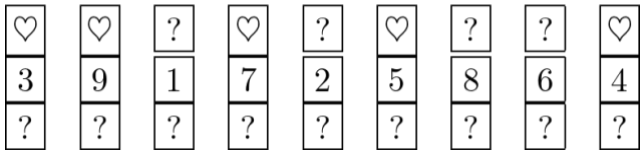

図 9 P は[9/2] + 1 = 5 枚だけカードを捲る[2]

- 点が黄色の場合：Aα のカードをすべて開示する

(6) 検証手順を実行する：

- 点が赤色の場合：捲ったすべてのカードが♡であれば手順を継続し，異なる図柄のカードが 1 枚でも存在すれば棄却する
- 点が青色の場合：捲ったすべてのカードが♣であれば手順を継続し，異なる図柄のカードが 1 枚でも存在

すれば棄却する

- 点が黄色の場合：♡と♣の枚数が同数であれば手順を継続し，そうでなければ棄却する

(7) すべてのカードを裏向きにし，列ごとに束にまとめてパイルスクランブルシャッフルを実行する．その後，Cα のカードをすべて開示し，カードの番号順に束（列ごとにまとめたもの）を昇順に並び替える．これにより，Aα，Bα，Cα が初期状態（(3)の終了した際の状態）に復元される．

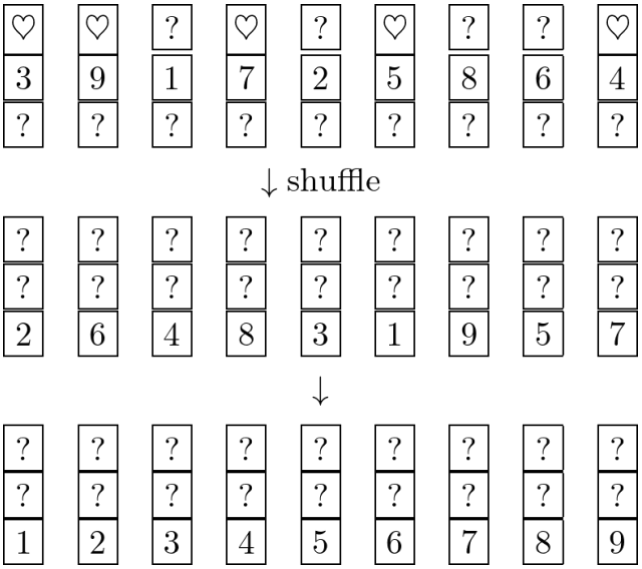

図 10　(7)の例[2]

6. 既存プロトコルの問題点

既存プロトコル[2]では，点ごとの証明を実行する際に，証明者 P が毎回カード列 Aα（隣接するピースの色の集合）を新規に作成する仕様である．このため，異なる点におけるカード列 Aα の作成において，同一のピースに対応するカードが異なっていても，検証者はこの矛盾を検出することができない．すなわち，ピースの色が固定されていることの保証がなされていない，という点が健全性達成の障害となる．

6.1 具体例による問題点の説明

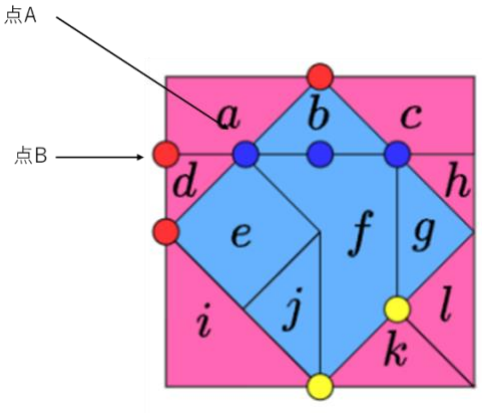

図 11　6.1 の例

図 3 のような点 A と点 B を考える．点 A ではピース a, b, d, e, f のうち過半数が青色であることを，点 B ではピース a, d のうち過半数が赤色であることを証明する必要がある．この場合，ピース a と d が両方の点の証明に登場する．正当な証明では，ピース a と d の色（プロトコル[2]ではカードの表の記号♡, ♣）はカード列 Aα の作成時に一貫している必要がある．

しかし，既存プロトコル[2]では証明者 P が毎回新たにカード列 Aα を作成するため，色（カードの記号）の一貫性が保証されていない．その結果，証明者 P は次のような不正を行うことが可能となる：

1. 点 α が赤（青）の場合：隣接するピース数 N の過半数が♡（♣）である任意の N 枚のカード列を作成
2. 点 α が黄色の場合：♡と♣の数が等しい任意の N 枚のカード列を作成

この操作により，実際の解答とは異なるカード列 Aα を用いても，プロトコルは受理されてしまう．

また，図 3 のように解が存在しないステンドグラスパズル問題でも，上述の操作を行えばプロトコルは受理してしまう．

7. 提案する改良プロトコル

7.1 プロトコルの手順

本研究で提案する改善プロトコルの手順は以下の通りである：

(1) ステンドグラスパズルの各ピースに 1, 2, 3, ..., m（m はピースの総数）と番号を割り当てる．

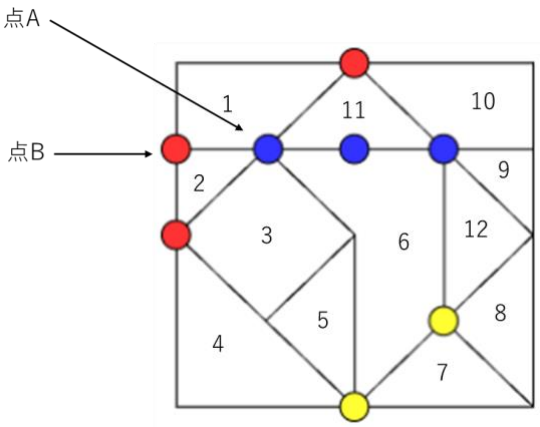

図 12　(1)の例

(2)　ピース番号の昇順に，そのピースの色に対応したカード（赤色のピースに♡，青色のピースに♣，裏面は共通して?）を裏向きに並べ，カード列 S を作成する．カード列 S の左から i 番目のカードは，ピース i の色に対応している．

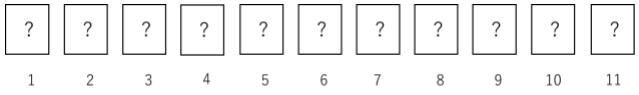

図 13　(2)の例

(3)　ある点 α に隣接するピースの番号を確認し，カード列 S から対応する番号のカードを取り出して昇順に並べ，カード列 Aα を作成する．

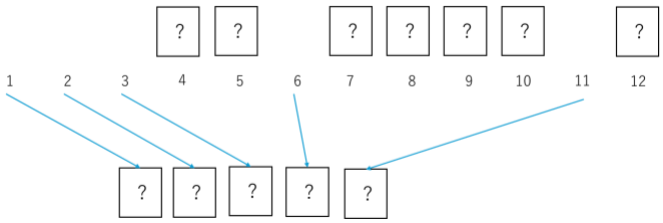

図 14　(3)の例

(4)既存プロトコル[2]の手順(2)～(8)（5.2 の(1)~(7)に対応する）を実行する．

(5)復元されたカード列 Aα のカードを，カード列 S の元の位置に順次戻す．この操作により，カード列 S が復元される．

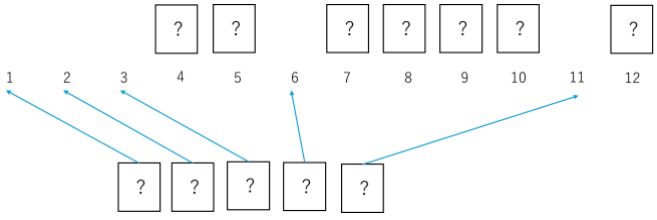

図 15　(5)の例

(6)手順 3～5 をすべての点に対して実行する．すべての点で拒否されなければ，検証者は受理する．

7.2　改善点の説明

我々が提案する改善プロトコルでは，各点での証明の開始時点と終了時点でカード列 S が不変に保たれる．また，ピースの色に対応するカードはカード列 S からピース番号に対応したカードを取り出すことで作成されるため，各点での証明においてピースの色は一貫して固定される．

この改善により，既存プロトコル[2]の健全性問題は解決された．

8.　安全性，健全性及びゼロ知識性の証明

8.1　完全性（Completeness）

証明者 P が正しい解を知っている場合，提案プロトコルにおいて検証者 V が拒否することはない．これは，正しい解に基づいてカード列 S が作成され，各点での制約条件が満たされるためである．

8.2　健全性（Soundness）

(3)の開始時点と(5)の終了時点で，カード列 S の状態は同一である．(4)は，既存プロトコル[2]の手順(2)～(8)（5.2 の(1)～(7)に対応する）を実行する．ここでは点の色に対応した解の条件を隣接するピースが満たしているかの検証が行われる．

ここで，証明者 P が解ではない解答を作成した場合，解の条件を満たさない点が少なくとも一つ存在する（すべての点で条件を満たす場合，解であるため）．したがって提案プロトコルの中でカード列 S から作成されるカード列 Aα のうち，少なくとも一つは点の色に対応した条件を満たさない．つまり点が赤（青）のとき♡（♣）の枚数が過半数でなく，点が黄色のとき♡と♣が同数でないということである．

(4)では点が赤（青）のとき♡（♣）の枚数が過半数でない場合，必ず棄却される．点が黄色のとき♡と♣が同数でない場合も必ず棄却される．したがって，証明者 P が解ではない解答を作成した場合，提案プロトコルの検証において必ず棄却される．

解が存在しないパズルにおいても同様である．

8.3　ゼロ知識性（Zero-Knowledge）

提案プロトコルの実行中において，カードの図柄とピースの対応関係が明かされることはない．したがって，検証者が解答に関して新たに獲得する情報は存在しない．

9.　計算量評価

シャッフル回数	カード枚数	健全性の誤り確率
3n	高々4m	0

表 1　提案プロトコルの各計算量

提案プロトコルは，既存プロトコル[2]の「カード列 Aα の作成」工程を改善したものである．したがって，ピースの数を m，点の数を n とすると，以下の計算量特性を持つ：

- ✓ カード枚数：既存プロトコルにカード列 S 作成のためのピース数 m 枚を追加
- ✓ シャッフル回数：既存プロトコルと同様（改善によるシャッフルの追加なし）
- ✓ 全体の計算量：シャッフル回数 3n 回，カード枚数最大 4m 枚，健全性誤差 0

10. まとめ：健全性の厳密な証明に向けて

我々が指摘する

「『問題を部分(局所)問題に分割し，すべての部分問題を証明することで全体（大域）を証明する』という型の証明プロトコルにおいて，異なる部分問題で共通して参照されるべき値が一貫していない」

という問題点を，他の既存カード型プロトコルに対しても，調査/検証しているが，類似の問題を有する方式は（現時点では）見つかっていない．

しかし，それでも「現在まで提案されている多数のカード型プロトコルの健全性に関して厳密な証明が本当に与えられているか?」という基本的な課題は残る．これに関しては，物理的カード型の証明プロトコル群の健全性を，GNPR[4]にまで遡って，再考する必要がある[14,15].

検証者が自身の乱数に応じて，証明者に質問するカード型証明の多く(例えば研究[16])は，古典的な対話型 ZKP[6]での知識抽出機(knowledge extractor)の構成を適用できる[7]. しかし，今回のステンドグラス問題に対するゼロ知識プロトコルも含めて，検証誤差ゼロの ZKP の多くは，検証者の質問乱数に依存しない (宮原ら[13]の言葉では）非対話型である．このため，NP 問題に対する知識の証明(proof of knowledge)で構成する抽出機の構成は自明ではない． 実際，カードの初期配置状況によっては（解答に対応する{裏返し}カードを所有すれば), 証明者は解そのものを知らずとも,プロトコルを実行し受理され, (古典の意味[7]での)知識の証明とはなりえない[14].

この健全性の厳密な証明の試みの 1 つとしては，形式検証手法[17]を掘り下げることになるか．とすれば，最近の非対話型証明系 SNARKS の健全性に関する Baily らの研究[18]も手本にした追求が今後の課題であろう．あるいは別の試みとして， Ilang の最新研究[19]のように，古典的 ZKP における「シミュレーターの存在を証明する」構成的な議論ではなく,「そのようなシミュレーターの存在が否定できない論理的な状態」を定義し,この Ilang による新しい枠組みと証明技法とをカード型 ZKP でも手本にすべきであろうか.

謝辞: 本研究の遂行にあたり，九州大学マス・フォア・インダストリ(IMI)研究所「一般研究・短期共同研究」にご尽力されております関係者，およびご発表いただいた研究者の方々に深く感謝します．本研究は IMI 研究集会での発表/公開資料（2023[20]・2024[21]・2025[22]）でのカードベース暗号に関する深い議論に大きく支えられての成果であります.
また、本論文の草案を読んでいただき、内容確認や誤植の訂正までご指導いただきました岩本宙造教授（広島大）に深く感謝します。

参考文献:

[1] 株式会社ニコリ，"ステンドグラスの遊び方，ルール，解き方 --- nikoli," [https://www.nikoli.co.jp/ja/puzzles/stained_glass/（参照 2025.08.19）]
[2] 吉塚創也，岩本宙造，櫻井幸一“ステンドグラスパズルに対するカードを用いたゼロ知識証明プロトコル," Ieice COMP 研/信学技法 2024-11 (2024.9 月).
[3] 株式会社ニコリ，"パズルの紹介" [https://www.nikoli.co.jp/ja/puzzles/ (参照 2025.08.19)]
[4] C. Iwamoto and R. Takaishi, “Yajisan-kazusan and stained glass are np-complete,” WAAC2023 2023. also "Computational Complexity of Yajisan-Kazusan and Stained Glass" Ieice Trans. Vol. E108.D Issue 3 2025
[5] R. Gradwohl, M. Naor, B. Pinkas, and G.N. Rothblum, "Cryptographic and physical zero-knowledge proof systems for solutions of sudoku puzzles," Fun with Algorithms, 2007.
[6] S. Goldwasser, S. Micali, and C. Rackoff, “The knowledge complexity of interactive proof-systems,” STOC ’85: Proc. ACM symp. on Theory of computing, 1985.
[7] M. Bellare, and O. Goldreich, "On Defining Proofs of Knowledge," In: CRYPTO 1992. Lecture Notes in Computer Science, vol 740. Springer (1993).
[8] X. Bultel, J. Dreier, J. Dumas, and P. Lafourcade, "Physical Zero-Knowledge Proofs for Akari, Takuzu, Kakuro and KenKen," In 8th International Conference on Fun with Algorithms (FUN 2016). Leibniz International Proceedings in Informatics (LIPIcs), Volume 49, Schloss Dagstuhl – Leibniz-Zentrum für Informatik (2016)
[9] L. Robert, D. Miyahara, P. Lafourcade, and T. Mizuki, “Interactive physical zkp for connectivity: Applications to nurikabe and hitori,” Connecting with Computability," eds. by L. De Mol, A. Weiermann, F. Manea, and D. Fernandez-Duque, 2021. ´
[10]佐 々木駿，品川和雅，“数コロに対する物理的ゼロ知識証明プロトコル”， 暗号と情報セキュリティシンポジウム (SCIS2023) 予稿集，2023.
[11] G. Kendall, A.J. Parkes, and K. Spoerer, “A survey of np-complete puzzles,” ICGA Journal, vol.31, no.1, 2008.
[12] R. Ishikawa, E. Chida, and T. Mizuki, “Efficient card-based protocols for generating a hidden random permutation without fixed points,” Unconventional Computation and Natural Computation, vol.9252, 2015.
[13] D. Miyahara, H. Haneda, and T. Mizuki, "Card-based Zero-knowledge Proof Protocols for Graph Problems and Their Computational Model," ProvSec'21 Springer LNCS Vol.13059
[14] 櫻井幸一 "カード型ゼロ知識証明系のシャッフル乱数の効果に関する考察" FIT 2025 L-020.
[15] 櫻井幸一 "カード型ゼロ知識証明の健全性と知識の再考：

シャッフルオラクルによる枠組み" CSS2025 本シンポジウム予稿
[16] 谷口太一, バグス サントソ, 横田明卓 "部分ラテン方陣完成問題に基づいたカードベース対話証明プロトコル" SCIS2024
[17] 藤田和弘, 米山一樹, 品川和雅, "カードベース暗号の形式検証の再考", 日本応用数理学会 2024 年度年会, 9 月 15 日 [http://fais.jsiam.org/doc/20240915-fujita.pdf]
[18] B. Bailey, and A. Miller "Formalizing Soundness Proofs of Linear PCP SNARKs," USENIX Security Symposium 2024
[19] R. Ilango "Gödel in Cryptography: Effectively Zero-Knowledge Proofs for NP with No Interaction, No Setup, and Perfect Soundness," IACR/ePrint 2025/1296 (also to be in FOCS2025)
[20] 九州大学マス・フォア・インダストリ研究所/一般研究-短期共同研究：産学連携によるカードベース暗号の数理的未解決問題と新課題の整理(研究代表：水木敬明) 2023 年 5 月 29 日--6 月 1 日 [https://joint.imi.kyushu-u.ac.jp/post-9009/]
[21] 九州大学マス・フォア・インダストリ研究所/一般研究-短期共同研究:：産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地(研究代表：須賀祐治 2024 年 5 月 20-23 日 [https://joint.imi.kyushu-u.ac.jp/post-15010/]
[22] 九州大学マス・フォア・インダストリ研究所/一般研究-短期共同研究: 産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地Ⅱ (研究代表：宮原大輝) 2025 年 5 月 27--30 日[https://joint.imi.kyushu-u.ac.jp/post-18086/]