# 再考：カード型ゼロ知識証明の健全性 -- 対話と乱数と知識 --

櫻井 幸一 [1,*]

**概要**：Gradwohl ら[TCS2009]が提案した数独パズルのゼロ知識証明を実現するカード型物理プロトコルは、健全性ゼロの達成と知識の証明に言及している。カード型ゼロ知識証明において、健全性誤差をゼロにすることは重要な研究課題であり、宮原ら[ProvSec2021]はこれを非対話型モデルとして定式化している。対して、櫻井[FIT2025]は、古典的なゼロ知識証明における計算論的限界（NP 完全問題で健全性ゼロの実現は困難[Goldreich-Oren(JoC1994)]）と、カード型でそれが実現できている点との違いに着目し、宮原らの方式をシャッフルオラクルとプレイヤーによる二者間ゲームとしてモデル化した。本研究では、これらの先行研究を踏まえ、カード型ゼロ知識証明における健全性、特に検証誤差と知識の証明に関して、乱数と通信の役割に焦点を当て、一連の提案方式の安全性を再考する。

**キーワード**：カードベース暗号、ゼロ知識証明、健全性、知識の証明, シャッフルオラクル

# Revisiting the Soundness of Card-Based Zero-Knowledge Proofs: Interaction, Randomness, and Proof of Knowledge

Kouichi SAKURAI [1,*]

***Abstract***: The card-based physical protocol for zero-knowledge proofs of Sudoku puzzles proposed by Gradwohl et al. [TCS2009] discusses the achievement of zero soundness error and the notion of proof of knowledge. In card-based zero-knowledge proofs, achieving zero soundness error is a significant research challenge, and Miyahara et al. [ProvSec2021] formalized this as a non-interactive model. In contrast, Sakurai [FIT2025] focused on the computational limitations of classical zero-knowledge proofs—specifically, the difficulty of achieving zero soundness error for NP-complete problems [Goldreich-Oren, JoC1994]—and the fact that such zero soundness is achievable in card-based protocols. Sakurai modeled Miyahara et al.'s scheme as a two-player game involving a shuffle oracle and a player. Building on these previous studies, this research reconsiders the security of a series of proposed schemes in card-based zero-knowledge proofs, with a particular focus on soundness—especially verification error—and proof of knowledge, emphasizing the roles of randomness and communication.

***Keywords***: Card-based Cryptography, zero-knowledge proofs, Soundness, Proof of knowledge, shuffle oracle

## 1. はじめに

Gradwohl ら[1]は、数独パズルに対するゼロ知識証明を、テーブルゲールで利用するカード型の物理プロトコルとして実現した。そこでは、健全性ゼロを実現する方式も提案している。また、Gradwohl らは、提案方式群の知識の証明（Proof of Knowledge）にも言及している。カード型ゼロ知識証明の健全性誤差は、重要な評価指標として、これをゼロにする研究[2]も盛んである。

宮原ら[3]では、健全性誤差ゼロのカード型ゼロ知識証明を、非対話型として定式化している。その一方で、櫻井[4]は、古典的な対話型ゼロ知識証明では、NP 完全問題は、健全性ゼロにはできないという計算論的限界[6]に対し、カード型 ZKP では、NP 完全問題が健全性誤差ゼロで実現できている結果との違いに注目した。そこでは、宮原らのグラフ同型問題に対するカード型 ZKP[6]を、shuffle オラクルとプレイヤー（P）による二者間ゲームとしてモデル化し、プレイヤーの役割を「検証者に対して証明を行う」のではなく、「与えられた入力の特性を、shuffle オラクルを用いて安全かつ秘密裏にプレヤー自身が検証する」ものとして位置づけた。

本研究では、カード型ゼロ知識証明の健全性、特に検証誤差と知識の証明に関して、乱数と通信の役割に焦点を当て、一連の提案方式の安全性を再考するものである。

## 2. カード型 ZKP

### 2.1 Gradwohl-Naor-Pinkas-Rothblum[1]

Gradwohl ら[1]は, NP 完全問題である数独パズルに対して、複数のゼロ知識証明を提案している、前半２つは、暗号論的コミットメントを用いるもの、後半４つは物理的道具、トランプやスクラッチカードなどの道具を使って実施するゼロ知識証明プロトコルである。

後述では、トランプ vs スクラッチカードも議論する。Gradwohl では、トランプは、スクラッチカードの代価品と

1 九州大学
Kyushu University
* sakurai@inf.kyushu-u.ac.jp

しての扱いである。しかし。その後のカード型暗号での、トランプ活用の多様性で、スクラッチの代価以上の役割を演じるが、これが１つの課題（転用性）を生むことを本稿では指摘する。反面、佐々木ら[5]は、トランプの再利用性という利便性を強調している。

本稿の主題の１つである、完全な健全性（エラーゼロ）を、Gradwohl ら[1]は、スクラッチカードを用いて実現している(Protocol-5[G])

### 2.2 佐々木ら[5]

数独の物理的ゼロ知識証明について：

- Gradwohl らによる既存のプロトコル「GNPR Protocol 3」は、数字の書かれたカードを使用し、簡易かつ実装可能だが、健全性エラーが正の確率で発生しる。
- 「GNPR Protocol 5」はスクラッチカードとハサミを用いることで健全性エラーをゼロにするものの、消耗品を使用する欠点がある。
- 佐々木ら[5] が提案したプロトコルでは、カードベース暗号を応用し、消耗品を使わずにカード枚数を減らしつつ、健全性エラーをゼロにしている。主要なアイデアは Ishikawa らによって提案された Pile-Scramble Shuffle [23] を駆使した「コピー計算」で、不正を防ぐ仕組みである。

総じて、新プロトコルは効率的かつ再利用可能な方法を目指している。また、再利用可能なトランプで、健全性誤差ゼロを実現した先駆的研究であり、続くカード型 ZKP の多くも健全性誤差をプトコル評価基準の１つとして採用し、これをゼロにする提案が主流になって、現在に至る。

**注：**NP（完全）問題は、検証者が自分で答えの正当性を誤差なしで確認できるため、カードを駆使すれば、健全性誤差なしの ZKP が構成できると期待できる。これに対して、今村ら[19]が提案したグラフ非同型問題に対するカード型 ZKP は、(NP 問題かどう不明なため)対話型と検証者の乱数が必須なため、健全性誤差をゼロにすることは難しいと予想される。

### 2.3 宮原ら[3]

グラフ同型問題に対するカード型 ZKP は、羽田ら[7]が NP 完全である三彩色問題と並べて、提案された。どちらも健全性誤差ゼロを実現している。特に、グラフ同型問題に対するプロトコルでは、与えられたグラフのサイズに関係なく 3 回のシャッフルのみしか必要としない。

さらに、宮原ら[3]は、提案プロトコルをより厳密に扱うため、健全性誤差のないカードベース ZKP プロトコルを、非対話型としてモデル化した形式的な枠組みも提示した。

宮原らの観察は次のとおり[3]

> 「提案した 2 つのプロトコルは非対話型であり、証明者ペギー（Peggy）が証拠（Peggy のみが知る秘密情報）に従って"隠された"カード列を裏向きに配置することで始まる。このプロトコルは、その後誰でも公的に実行可能であり、例えば、ペギーが全てのアクションを行い、その行動を検証者ヴィクター（Victor）が監視するだけで十分である。なお、数独などのパズルに対する既存の多くの ZKP プロトコルも同様に非対話型である」。

宮原らのグラフ同型問題に対するカード型ゼロ知識証明

宮原らは、提案手法がゼロ知識 ZKP であると主張している。実際には、証明者にすら、２つのグラフが同型であること以外は、知ることができない。さらに、証明の結果、検証できるのは、最初に裏返したカード列に、同型置換 $\pi$ が記述さてれている、という事実だけである。しかし、これは証明者自身が本当に秘密 $\pi$ を知っていることまでは導かないことに注意する。

現実問題としては、同型置換に対応するカード列を、テーブルの上で、証明者が公に準備するという設定も考えられる。カード型 ZKP で、証明者と検証者に何が（共通入力として）与えて、プロコトルを開始しているか、注意がいる。

## 3. 健全性誤差ゼロ

### 3.1 物理的・カード型

数独[1,2]やグラフ同型問題[3,7]を含め、一部のカード型ゼロ知識証明では、健全性エラーなしを実現している。

元祖の GNPR09[1]では、証明者のカード不正を防ぐため、三連のスクラッチカードを導入し、健全性エラーゼロを実現している。

また、検証者が乱数を使った質問や挙動を行う場合も、健全性エラーが派生することに注意する（証明者が、検証者の乱数を事前に推測する成功確率に相当する）。

### 3.2 暗号計算論的対話型 ZKP

古典的なゼロ知識対話型証明では、健全性エラーはむしろ自然な特性であることを Goldreich-Oren[5]は、古くに明らかにしている。

> 定理 A：検証者が決定的な（乱数を利用しない）ゼロ知識対話型証明可能な問題は、クラス RP(Randomized Polynomial time)に限る。

クラス RP であるが、暗号でよく利用される乱数を用いる素数判定はその事例である。

さらには、対話通信の効果に関しては：

定理 B : one-step（１回の一方向通信）ゼロ知識対話型証明可能な問題のクラスは BPP (Bounded error Probabilistic Polynomial time )である。

RP も BPP も、多項式能力の検証者が、乱数を使って、自分で計算/検証できる問題であることに注意する。後者の定理 B が、Blum らの非対話型 ZKP の予備手続きである CRS（共通乱数列)モデル[20,21]導入の根拠にもなっている。

**注**：Ilang[22]は、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」を定義した新しい証明枠組みを与えて、Goldreich-Oren[5]の制限をこえる証明技法与えてり。非対話型かつ検証誤ゼロのカード型 ZKP でも手本にすべきであろうか.

### 3.3 ランダムシャッフルモデル

さて、検証性エラーがゼロである(多くの)カード型 ZKP において、検証者は乱数なしの確定型である。それでも、複数の NP 完全問題が、このカード型 ZKP を持つという。櫻井[4]は上記の既存定理との関係と違いを論じた。
検証者が乱数を利用しない確定性証明系では、証明者が単独で一連のプロトコル処理を実行でき、一方向であり、特定の検証者を必ずしも必要としなこと(un-designated)に注意する。宮原ら[3]はこれをカード型の非対話モデルとして定式化し、その上で、カード型 ZKP の厳密な特性の証明を試みている。

これに対して、 櫻井[4]は、非対話型カード型 ZKP を、shuffle オラクル(SO)と証明者を演ずる player(P)での２者間ゲームとしてモデルを定式化した。そこでの player の役割は、検証者に証明を行うというよりも、与えられた入力の特性を、shuffle オラクルを使って、安全/秘密裏に検証する、というものである。さらに、それまで、明示的には議論されていない知識の証明にも言及している。

### 3.4 再考：グラフ同型問題に対するカード型 ZKP

羽田ら[7]のグラフ同型問題に対するカード型 ZKP は、一見すると、証明者と検証者という対話型モデルにみえる。しかし、実際には、検証者は乱数なしの決定性であることに注意する。このため、証明者が単独で全ての手順を公開テーブル上で行い、検証者は、それを側から見て、最終的には、受理・非受理を判定すればよい。証明者のランダムな行為は必須であるが、pile-shuffle 時に利用する。ただし、pile-shuffle に使う乱数"r"は、その実行者ですら、未知という制限下にある。このため、記憶用の、補助カードを導入し、目的のカードと同時/並行して shuffle する。また、宮原法での、pile-shuffle は、裏返しカードは基本である。補助カードは<id>を記号化したカードの場合は、pile-shuffle の結果は、<id> にランダム置換"r"を施した結果となる。宮原の方法では、同型置換πに対応するカード/裏返しと、口頭置換<id>に対応するカード/裏返しを対にした pile-shuffle を施し、r と rπに対応するカード対/裏返しをえる。この２つのカード列対を同時に表にすれば、秘密のπが露呈するが、宮原法では、rπのみを表にして、次の操作に進む。最終的には、異なる乱数、r=r1,r2,r3 を使った pile-shuffle を３回試行し、同型性の判定が完了する。
宮原らは、提案手法がゼロ知識であると主張している。実際には、証明者にすら、２つのグラフが同型であること以外は、知ることができない：証明の結果、検証できるのは、最初に裏返したカード列に、同型置換πが記述されている、という事実であり、これは証明者自身が本当に秘密πを知っていることまでは導かないことに注意する。
注意：pile-shuffle ではその実行者ですら、乱数がわからない、という仮定である。

## 4. 知識の証明(Proof of Knowledge)

宮原らのグラフ同型問題に対するカード型 ZKP は、証明者がグラフ同型そのもの知っていることを検証者に示す知識の証明ではない。検証者が乱数を使わないため、対話型証明における知識抽出機の構成は（不可能性も含めて）自明ではない。

実際、同型を記述し、符号化したカード群は裏返しで提供される(もちろん、同型置換を知っている証明者は、自分でこの置換をカード群に符号化し、自ら裏返すこともできる)。宮原らの方式を実行すれば、誰もが、この裏返しカード群に正しい同型写像が記述されているか、否かを、そのカード群自体を表にすることなく、100%確定的に検証できる。さらに、この同型を記述し、符号化したカード群(裏返し)を、受け取った者は誰でも、自分でその正当性を、宮原らの手順を再現することで検証できる。

上記の観察は、多様な NP 完全問題に対して設定されている多くのカード型 ZKP に当てはまる。逆に、一部のカード型 ZKP においては、検証者の乱数は必須であり、対話型証明となっており、上記の観察が適用できない事例もある[19]。

**再考 GBPR**:GNPR らの提案でも、対話を用いる方式も提案されている。
GNPR では、 Protocol-1/2/3 は知識型であり、Protocol-4 も知識と主張され、さらに Prococol-5(perfect soundness)も知識型である、と主張はしている。また、Prococol-6：V は{ *rows/columns/ subgrids*}を（ランダムに）選ぶ、では構成的に知識型抽出器を与えている「知識抽出（knowledge extraction)」は、証明者とやり取りし、単にページをめくって解答を確認する抽出器によって示さ

れる」。

## 5. カード型暗号の安全性/再考

### 5.1 意味論的(semantic)安全性[14]

同型を記述し、符号化したカード群/裏返しは、不正に表にしない限りは、同型を知ることはない、という前提の下での、秘密安全な ZKP である。この前提をすこし緩めた shuffle オラクル(SO)を利用することで、プレーヤーは、同型写像自体を抽出できることが、先行研究[4]で指摘されている。これは、カードによる置換の符号化が確定的であることに、宮原らの手順を適用するものである。

具体的には、次のとおり：

対象とする同型グラフカードの検証手順を、オラクルとする。手元には、同型（であると思われる）を記述し、符号化したカード群は裏返しで, Charie(C, Checker/検証者)に提供されている状況を考える。カードには、n 個の頂点の置換に対応する数字が、n 枚のカードに記載されて、裏返しの状態にある。チャーリーC は、最初の裏返しカードに記載の数字を、カードを表にすることなく、検証手順オラクルを使って、たかだか n 回の操作で、確定させることができる。この n 回の操作は、しらみ潰しである。"１"のカードを裏返し、提供されたカード列の最初と交換する。

このカード列に対して、同型グラフカードの検証手順を実行する。受理されれば正解、不受理は不正解。この操作は、毎回たかだか n 回を、n 枚のカード列全てに実行するので $n^2$ の操作で完了するし、並列化も可能である

同型置換のしらみ潰し探索は n!であることに注意する。これは、一枚のカードが、同型置換の情報一部のみを秘匿しており、かつ独立であることに起因する。通常の暗号化では派生しないが､平文が 0 か１かしない､確定暗号では、暗号文も２種のみなので、平文が推定できることと似ている。これにより､カード型暗号でも､確率暗号[14]のように、semantic security が要求されることを示唆する。

**研究課題**

**A) カード型暗号でも、確率的暗号（の類似）は実現できるのであろうか？**

**B) 逆に、カード型暗号に基づく既存の提案手法で、上記のような、プロトコル乱用攻撃で、秘密（の一部）の導出が可能か否か、を検証する必要もあるか？**

### 5.2 検証可能暗号化との関係

検証可能な暗号化[11,12,13] とは、メッセージが暗号化された形で与えられている間に、メッセージ m のある性質を証明できる暗号化方式である。暗号化方式が安全である場合、暗号化 E(m)は m に関する情報を漏らさないはずである。しかし、暗号化されたデータを処理する前に、暗号化されたコンテンツの何らかの性質をチェックする必要がある場合には、この性質は適さないかもしれない。検証可能な暗号化では、検証者が暗号化されたコンテンツのある特性をチェックすることができる。

宮原らの GI に対するカード型 ZKP は、この検証可能暗号に似ているとも言える。同型置換を記載した（n 枚）カード群、これを裏返すことでの暗号化。このカード群を表にすることなく、与えられた２つのグラフに対応する同型置換であることを、カードを表にすることなく、証明する/検証する。実際の手順では、カードは表にするのであるが、表にしたカードからは、秘密の置換自体は、証明者ですらわからない特性をもつ。

## 6. 再現(再利用)性 ZK の問題：

Gradwohl らの手法の一つに、（３連）スクラッチカードを、ハサミで切る分ける方式が提案されている。これが、複雑かつ実用的ではない、ということで、トランプカードを用いた方式が提案された。 前者は、ハサミで切ってしまうので再利用 NG vs. 後者はトランプで再現性/再利用できる可能性もある。 本来、スクラッチ自体が、消耗品で再利用 NG とされている。

ZKP の再利用に関しては、対話型 ZKP では、転用性（divertible）[15]が知られている。さらには、malleable[16]がある。

古典的な非対話型 ZKP では、共通乱数モデル下では、その証明は、乱数を共通した者の間では、転送共有できる。non-malleable な NIZK は、全く自明でなく、Sahai[17]が解決を見出し、最近も研究[18]が続いている。

カード型 ZKP でも、対話型は、古典的な結果を参照できると期待する。Gradwohl らの手法の一つに、（３連）スクラッチカードを、ハサミで切る分ける方式は、初期状態が維持されないという意味では､転用不可(non-divertible)と解釈できる.しかし､トランプ利用の非対話型､特に検証誤差ゼロのものは、注意がいる。

## 7. おわりに

以上の議論を踏まえ、本研究はカード型ゼロ知識証明における健全性誤差ゼロの達成可能性とその意味づけを、乱数生成および通信/対話の役割に着目して再検討した。従来の対話型 ZKP とは異なり、カード型 ZKP では、プレイヤー自身が安全かつ秘密裏に入力の特性を検証するという新たな視点/条件が導入されており、これが健全性誤差ゼロの実現に寄与している可能性がある。本研究では、こうしたプロ

トコルの構造的特徴と、知識の証明としての性質を精査することで、カード型 ZKP の安全性と応用可能性に関する理解を深めることを目的として、独断の未解決予想と研究課題を列挙した。

**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[24]・2024[25]・2025[26]）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、本研究のきっかけは、下名らのコンプ研での発表[27]への平原氏(NII)からの質疑「提案のカード ZKP は、非対話ではないのではないか？」の考察から始まりました。研究会をお世話されております幹事団の皆さまとご議論いただきました参加者の方に深く感謝します。

## 参考文献

[1] Gradwohl, R., Naor, M., Pinkas, B., Rothblum, G.N. . Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles. Fun with Algorithms. FUN 2007. LNCS, vol 4475.(2007)
[2]Sasaki, T., Mizuki, T., & Sone, H. Card-based zero-knowledge proof for Sudoku. 9th International Conference on Fun with Algorithms, FUN 2018 (Leibniz International Proceedings in Informatics, LIPIcs; Vol. 100) (2018)
[3]Miyahara, D., Haneda, H., Mizuki, T. (2021). Card-Based Zero-Knowledge Proof Protocols for Graph Problems and Their Computational Model. In: Huang, Q., Yu, Y. (eds) Provable and Practical Security. ProvSec 2021. Lecture Notes in Computer Science, vol 13059 ( 2021)
[4]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.
[5]佐々木達也、水木敬明、曽根秀昭、 数独の物理的ゼロ知識証明の効率化 , SCIS2018 3B1-2
[6]Goldreich, O., Oren, Y. "Definitions and properties of zero-knowledge proof systems". J. Cryptology 7, 1–32 (1994),also in FOCS'87. (1987)
[7]羽田 大倫,宮原 大輝,水木 敬明, 曽根 秀昭 "２つのグラフ問題に対する物理的ゼロ知識証明" SCIS2021/2F2-4 (2021）
[8]Bellare M. Rogaway P. "Random oracles are practical: A paradigm for designing efficient protocols" Proc. 1st ACM Conference on Computer and Communications Security, pp.62-73 (1993)
[9]Blum, M., Feldman, P. Micali, S. "Non-interactive zero-knowledge and its applications", STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing, pp. 103 - 112 (1988)
[10]Bellare, M., Goldreich, O. "On Defining Proofs of Knowledge.". CRYPTO' 92. LNCS, vol 740. (1992)
[11] Kazue Sako (2011). Verifiable Encryption. In: van Tilborg, H.C.A., Jajodia, S. (eds) Encyclopedia of Cryptography and Security. Springer, Boston, MA.
[12]Camenisch J, Damgård I (2000) Verifiable encryption, group encryption, and their applications to separable group signatures and signature sharing schemes. In: Okamoto T (ed) Proceedings of AłSIACRYPT 2000, Lecture notes in computer science, vol 1976, Springer,
[13]Camenisch J, Shoup V (2003) Practical verifiable encryption and decryption of discrete logarithms. In: Boneh D (ed) Proceedings of CRYPTO 2003, Lecture notes in computer science, vol 2729,
[14]Goldwasser, S. and Micali, S. "Probabilistic encryption & how to play mental poker keeping secret all partial information", ACM Symposium on Theory of Computing (1982).
[15]Yvo Desmedt, Claude Goutier, Samy Bengio, "Special Uses and Abuses of the Fiat-Shamir Passport Protocol," CRYPTO 1987
[16]Danny Dolev, Cynthia Dwork, Moni Naor, " Non-malleable cryptography," STOC '91:
[17]Amit. Sahai, "Non-malleable non-interactive zero knowledge and adaptive chosen-ciphertext security," *FOCS* 1999,
[18]Vincenzo Botta, Michele Ciampi, Emmanuela Orsini, Luisa Siniscalchi, Ivan Visconti, "Black-Box (and Fast) Non-malleable Zero Knowledge, CRYPTO 2024
[19]今村-櫻井 "グラフ非同型問題に対するカードを用いたゼロ知識証明プロトコル 〜 グラフ同型問題に対するカード型証明の再考 〜" Ieice/COMP2025-05-08 (2025.5 月)
[20]Manuel Blum, Paul Feldman, Silvio Micali, "Non-Interactive Zero-Knowledge and Its Applications," STOC 1988
[21]Feige, U., Lapidot, D., Shamir, A.: Multiple non-interactive zero knowledge proofs under general assumptions. SIAM J. Comput. 29(1), 1–28 (1999), Earlier version entitled Multiple Non-Interactive Zero Knowledge Proofs Based on a Single Random String appeared at FOCS 1999
[22]Rahul 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)
[23]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.
[24]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/]
[25] 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/ ]
[26] 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/
[27]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).
[28]Manuel Blum, "How to Prove a Theorem So No One Else Can Claim It," Presented at the International Congress of Mathematicians, Berkeley, California, USA. (1886)

## 付録

### 付録 A.1 コミットメントの物理的実現[Blum]

Gradwohl らは、デジタルのコミットメントによる対話型 ZKP を紹介し、続けて、このデジタルのコミットメントの物理的な実現プロトコルを紹介している。
しかし、古典論文を見直すと、すでに Blum(1986)でも、鍵のかかる金庫のような（物理的）箱を導入している。そ

の上で、暗号論的一方向性関数でも、この箱（の特性）がデジタル化できることを論じている。

「プロトコルでは、証明者が鍵付きの箱を利用でき、その鍵を持っているのは証明者だけであると仮定する。ただし、情報を箱に鍵で閉じ込める代わりに、暗号化することも可能ある。一方向関数はこの目的を果たし、デジタルの鍵付き箱のような役割を果たす。この一方向関数を使用することで、鍵付きの箱や鍵といったハードウェアを使わず、すべてのやり取りを紙の上で行うことが可能になる。」

ちなみに、GMW (Goldreich, Micali, Wigderson, FOCS'86) では、NP 完全である 3 色問題を扱っているが、Blum は、ハミルトニアン閉路問題に対して、直接に ZKP を構成している。さらに、ハミルトニアン閉路問題を扱った ZKP の方が、3 色問題よりも、効率良い利点に言及している。//