L-020

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
On the Power of Shuffle Randomness in Card-based Zero-Knowledge Proofs

櫻井　幸一*
Kouichi SAKURAI

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トランプを用いる物理プロトコルとして実現した。Sasaki ら[2]は、Gradwohl らの手法における健全性誤差をゼロにする、数独に対するカード型ゼロ知識証明を与えた。

本研究では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[3,4]を取り上げ、シャッフル乱数の役割と、知識の証明という観点からの解析と評価を行う。

特に、本研究では、pile-shuffleをオラクルとしてモデル化するものである。

2. ランダム・シャッフル

カード型 ZKP では、pile-shuffle が駆使される。ここではランダムにシャッフルする実行者自身も、その乱数が未知という条件である。すでにこの実現性と改良も研究は続いている。

計算量理論での ZKP における既存の乱数モデルは、二種に大別される（i）対話型証明において、乱数を証明者か検証者自身で生成し、生成者しか知らない秘密乱数型か、双方が既知の公開乱数型、(ii)あるいは、証明者と検証者が事前に乱数列を共有し、これを使って、証明者が生成した証明列を、検証者が検証する非対話型証明である。

しかし、ランダムにシャッフルする実行者自身も、その乱数が未知というカード型 ZKP の仮定は、計算論的には、極めて強い条件とみて、本研究では、オラクルとして扱うことにする。Fiat-Shamir 法の安全性証明で導入されたランダムオラクル(RO)モデル[5]に例えて比較するならば、RO のようにオラクルが乱数そのものを提供するのではなく、ランダムシャッフルでは、質問者が与えたカード（群）に対し、オラクルが生成した秘密乱数によるシャッフル/カード暗号化結果をオラクルから質問者が提供を受けるとも解釈できる。

3. 健全性エラーゼロ

特に宮良らの方式を含め、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。ここでは、検証者は乱数を利用しない確定性である。このため、実際には、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いことに注意する。

そこで我々は、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する。ここでは、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、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。

今回、我々が参考にするのは、対話型ゼロ知識証明系(ZKIP)の計算複雑性に関する、初期の次の結果である[6]

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[7, 15]の元になっている。

さて、検証性エラーがゼロであるカード型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。本研究では上記の既存定理との関係と違いを明らかにすることが目的の１つである。

4. 知識の対話型証明[8]

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[12]。

5. カード型暗号の安全性/再考

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、

* 九州大学, Kyushu University

Copyright © 2025 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.

同型写像自体を抽出できることも本研究が指摘する。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。これにより、カード型暗号でも、確率暗号[9]のように、semantic security が要求されることを示唆する。

6. おわりに

本研究のきっかけは、吉塚のコンプ研での発表[10]での質疑「提案のカードZKPは、非対話ではないのではないか？」がきっかけである。続く今村のグラフ非同型問題に対するカード型ZKP[11,12]において、宮原らの同型問題へのカード型 ZKP の再考を行った。

本研究は、宮原自身[13] が論じている未解決問題(4/4)に対する一つの試みであると自己評価する。また、IMI2025 での宮原の最新発表[14]も参考にした。

謝辞

九州大学マス・フォア・インダストリ研究所で、一般研究-短期共同研究をお世話いただいております関係者に感謝します。本研究の遂行は、公開されている IMI 研究集会/発表資料のおかげであります。

また、コンプ研で質問いただきました、幹事や参加者へも謝辞：本研究の発端は、下名らのコンプ研での発表への平原氏(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？” に対する考察から始まりました。

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] 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)
[4] 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)
[5] 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)
[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] 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)
[8] Bellare, M., Goldreich, O. "On Defining Proofs of Knowledge.". CRYPTO' 92. LNCS, vol 740. (1992)
[9] Goldwasser, S. and Micali, S. "Probabilistic encryption & how to play mental poker keeping secret all partial information", ACM Symposium on Theory of Computing (1982).
[10] 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 COMP2024-11
[11] 今村太紀 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 卒業論文（九州大学・電気情報 工学）2025. 3 月
[12] 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)
[13] 宮原 "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[https://joint.imi.kyushu-u.ac.jp] (2023.)
[14] 宮原 "未解決問題の解決状況" 九州大学 IMI 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″（2025. 5 月）
[15] 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 1990

Copyright © 2025 by
The Institute of Electronics, Information and Communication Engineers and
Information Processing Society of Japan All rights reserved.