SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

パイルスクランブルシャッフルからのグラフ自己同型シャッフルの構成
Graph Automorphism Shuffles from Pile-Scramble Shuffles

宮本 賢伍 * 品川 和雅 †
Kengo Miyamoto Kazumasa Shinagawa

キーワード カードベース暗号，グラフ自己同型，パイルスクランブルシャッフル

あらまし

秘密計算とは，n 人のプレイヤーがそれぞれ入力情報を保持しているとき，他のプレイヤーに入力情報を知られることなく関数値を計算する暗号技術である．**カードベース暗号**とは，物理的カード組を用いて秘密計算を実現する分野である．カードベース暗号プロトコルは，入力情報を表すカード列に物理的操作を施し，出力情報を表すカード列に変換するものである．物理的操作の中でも，安全性を達成するために最も重要な操作が**シャッフル**であり，これはある確率分布に従って置換を選択し，その置換に従ってカード列を並び替える操作である．

カードベース暗号では，これまでに様々なシャッフルが提案されてきた．代表的なシャッフルに **ランダムカット (RC)**，**ランダム二等分割カット (RBC)**，**パイルランダムカット (PRC)**，**パイルスクランブルシャッフル (PSS)** がある．これらのシャッフルは基本的かつ単純なシャッフルであると考えられており，これらのみから実現できるプロトコルは「実用的」であると考えられている．

我々のモチベーションは，基本的なシャッフルを用いて（一見複雑に見える）別のシャッフルを構成することである．加えて，これらの基本的なシャッフルの間にある明示的な関係性を与えることである．例えば，PSS は RC のみを用いて構成することができるが，その逆は非自明である．

本研究の貢献は，PSS のみを用いて**グラフ自己同型シャッフル**と呼ばれるシャッフルを構成したことである．G を任意の有向グラフとし，頂点数を n，辺数を m とする．n 枚のカード列が与えられたとき，G に付随するグラフ自己同型シャッフルとは，G の各頂点にカードを置き，G の自己同型写像 π を一様ランダムに選び，π に従ってカード列を並び替えるシャッフルである．我々は，元々の n 枚のカード列に加えて $n+2m$ 枚のカードを追加し，$k+1$ 回の PSS を用いることで，グラフ自己同型シャッフルを実現する方法を構成した．ただし，k は頂点が取りうる次数の種類の数である．

グラフ自己同型シャッフルは決して特殊なシャッフルではなく，RC/RBC/PRC/PSS はあるグラフに付随するグラフ自己同型シャッフルとして実現される．例えば，RC はサイクルグラフに付随するグラフ自己同型シャッフルである．従って我々の結果の直接の帰結として，PSS から RC を実現できることが分かる．さらに我々は，この構成を効率化し，n 枚の RC を追加カード n 枚と 2 回の PSS から実現できることを示した．この事実と Koch と Walzer [1] の結果を合わせれば，任意の一様閉シャッフルは PSS から構成できることが分かる．

参考文献

[1] Koch and Walzer,“Foundations for Actively Secure Card-Based Cryptography,” FUN 2021.

* 茨城大学, kengo.miyamoto.uz63@vc.ibaraki.ac.jp
† 茨城大学, shinagawakazumasa@gmail.com