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

有限群の一様分解とその一様閉シャッフルへの応用
Uniform Decomposition of Finite Groups and Its Application to Uniform-closed Shuffles

金井 和貴 * 宮本 賢伍 † 品川 和雅 ‡
Kazuki Kanai Kengo Miyamoto Kazumasa Shinagawa

キーワード カードベース暗号，一様閉シャッフル，対称群，シロー部分群

あらまし

カードベース暗号とは，物理的なカード列に対してシャッフル等を施して秘密計算を実現する研究分野である．ここで，シャッフルとはカード列を確率的に並べ替える操作である．

カードベース暗号はシャッフルの開発に伴って発展してきた．初期の研究では**ランダムカット**のみが用いられていたが，**ランダム二等分割カット**が登場したことによって多くのプロトコルは劇的に効率化された．また，**パイルスクランブルシャッフル**の登場によって完全順列生成やゼロ知識証明等のプロトコル構成が容易になった．このように，新しいシャッフルが提案されるたびに，新しいプロトコル構成のアイディアが生まれてきた．

一般のシャッフルは，置換の集合 $\Pi \subset \mathfrak{S}_n$ と Π 上の確率分布 $\mathcal{F}$ によって特徴付けられ，$(\mathsf{shuffle}, \Pi, \mathcal{F})$ と表記される．シャッフル $(\mathsf{shuffle}, \Pi, \mathcal{F})$ は，Π が $\mathfrak{S}_n$ の部分群のとき閉シャッフル，$\mathcal{F}$ が一様分布のとき一様シャッフル，閉シャッフルかつ一様シャッフルのとき一様閉シャッフルと呼ばれる．ランダムカット，ランダム二等分割カット，パイルスクランブルシャッフルはいずれも一様閉シャッフルであり，一様閉シャッフルのクラスは重要である．

それでは有限群 G を与えられたときに，G の一様閉シャッフルを実現することはどれくらい容易だろうか．Koch と Walzer [1] は任意の有限群 G に対してその一様閉シャッフルをランダムカットを用いて実現する方法を提案している．しかしながら，各プレイヤーが G の一様ランダムな元を脳内で生成する必要がある点や，操作回数が G の位数に比例する点から，実用性に関しては改良の余地が残る．

本研究では，一様閉シャッフルの実現を群論的アプローチによって試みる．まず，有限群 G に対して**一様分解**という分解 $G = H_1H_2\cdots H_k$ を定義する．特に $H_1, H_2, \ldots, H_k$ が G のシロー部分群のとき，**シロー分解**という．このとき，G の一様分解 $G = H_1H_2\cdots H_k$ が存在すれば，G の一様閉シャッフルは $H_1, H_2, \ldots, H_k$ の一様閉シャッフルに還元される．よって，一様分解（特にシロー分解）が見つかれば，一様閉シャッフルを簡単なシャッフルに還元できる．

上記の方法に従って，6 枚以下の任意の一様閉シャッフルを実現した．我々の方法は Koch と Walzer の方法よりもランダムカットの回数に関して効率的である．なお，全ての有限群がシロー分解を持つわけではないことに注意する．実際，28 点に作用するユニタリー群 $O_3(3)$ はシロー分解を持たない [2].

参考文献

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

[2] Holt and Rowley,“On products of Sylow subgroups in finite groups,” Arch. Math. 1993.

* 新潟大学, kanai@m.sc.niigata-u.ac.jp
† 茨城大学, kengo.miyamoto.uz63@vc.ibaraki.ac.jp
‡ 茨城大学, shinagawakazumasa@gmail.com