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

一様で閉じたシャッフルの効率的な実装
How to Efficiently Implement Uniform Closed Shuffles

岩成 慶太 * 中井 雄士 * 渡邉 洋平 * † 栃窪 孝也 ‡
Keita Iwanari Takeshi Nakai Yohei Watanabe Kouya Tochikubo
岩本 貢 *
Mitsugu Iwamoto

キーワード 秘密計算，カードベース暗号，シャッフル，秘匿置換

あらまし

カードベース暗号とは物理的なカード組を用いて秘密計算を実現する暗号技術である．秘密計算を実現するための乱数は，テーブル上などの公開の場でシャッフル操作を行うことで生成される．代表的なシャッフル操作にランダムカットがある．ランダムカットはカード組で山札を作り，上から何枚か取って下に重ねる動作をランダムな回数繰り返し行うシャッフルである．取ったカードの枚数が正確に把握できないことから，ランダムカットで安全に乱数が生成できるという仮定がしばしば用いられる．カードをシャッフルするアクションは置換集合とその確率分布により定義され，その中でも置換集合が対称群の部分群かつ確率分布が一様なものを「一様で閉じたシャッフル（Uniform Closed Shuffle）」という [1]．シャッフルの実装可能性も重要な点であり，任意の一様で閉じたシャッフルはランダムカットのみから実装できることが知られている [2]．具体的には，一様で閉じたシャッフルをサイクル分解し，各サイクルを同じ回数シフトすることで実現する．このとき，各サイクルに対して同じ回数巡回シフトをするために追加カードを用いる．また，各サイクルに異なる回数の巡回シフトを適用するような攻撃も考えられるが，追加カードにより不正検知も可能である．

本稿では，ランダムカットによる一様で閉じたシャッフルの実装におけるカード枚数の効率化を行う．具体的には，既存手法 [2] を改良し，すでに巡回シフトが終了したカード組を再利用することで追加カード枚数を削減する手法を提案する．また，シャッフルの代わりに秘匿置換を許した操作モデルにおける，一様で閉じたシャッフルの実装手法を提案する．提案手法は [2] の方式をベースとし，カードに加え番号付きの封筒を用いることで確率的な不正検知が可能である．

* 電気通信大学, 〒 182-8585 東京都調布市調布ヶ丘 1-5-1, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu, Tokyo, 182-8585, Japan.
† 産業技術総合研究所, 〒 135-0064 東京都江東区青海 2-4-7, National Institute of Advanced Industrial Science and Technology (AIST), 2-4-7 Aomi, Koto-Ku, Tokyo, 135-0064, Japan.
‡ 日本大学, 〒 275-8575 千葉県習志野市泉町 1-2-1, Nihon University, 1-2-1 Izumi-cho, Narashino-shi, Chiba, 275-8575, Japan.

参考文献

[1] Takaaki Mizuki, Hiroki Shizuya, “A Formalization of Card-based Cryptographic Protocols via Abstract Machine,” International Journal of Information Security volume 13, pp. 15–23, 2014

[2] Alexander Koch and Stefan Walzer, “Foundations for Actively Secure Card-Based Cryptography,” 10th International Conference on Fun with Algorithms (FUN 2021), vol.157, pp. 17:1-17:23, 2020