

6 カード 3 入力 equality function (Six-Card Trick) における置換バリエーションの完全分類

須賀 祐治^{1,a)}

概要：本稿は 6 カード 3 入力 equality function (Six-Card Trick) を実現するカードプロトコルを扱う。ICISC2018 において品川らによって提案された Six-Card Trick は前処理である一般置換（巡回置換と対比させるためにあえて呼ぶ）とランダムカット（巡回置換）のみで構成されるシンプルな方式である。本稿では一般置換にあたる部分の完全分類を行い、ユーザビリティの観点で従来よりも優位と考えられる方式を新たに発見したため報告する。

キーワード：Card-based protocols, Six-Card Trick, Three-input equality function

A complete classification of permutations on 6-card 3-input equality function (Six-Card Trick)

YUJI SUGA^{1,a)}

Abstract: This paper deals with a card protocol for 6-card 3-input equality functions (six-card trick). The six-card trick, proposed by Shinagawa et al. at ICISC2018, is a simple method consisting of the pre-processing method of general substitutions (contrast with the cyclic substitutions) and narrowly-defined random cuts (cyclic substitutions). In this paper, we provide the complete classification of the part corresponding to general permutation and the discovery of new methods that are considered to be superior to the conventional method in terms of usability.

1. はじめに

カードベースプロトコル [1] はトランプカードを利用し、お互いの入力を秘匿したまま AND や XOR などの演算を行うマルチパーティ計算である。トランプカードを用いた手法でランダムにカードをシャッフルしたり置換するなどの手順を繰り返して所望の結果を得ることができるため、暗号技術を身近に感じることができる。このような身近なものを用いたレクリエーション暗号としては、カードベースプロトコルを皮切りに、お菓子の PEZ [7], [8] やコイン [9] やボール [10] などの玩具を用いる方式があり、様々な方式に拡張されている。これらの方式は大学のオープンキャン

パスなどで催されることがあり、日頃硬い研究を行っている研究室においては、研究の楽しみを理解してもらう導入として効果が高いと考えられている。同じような方式としてはスキュタレー暗号（棒状に紐を巻き付けることで暗号文を復号する方式）や視覚型復号秘密分散（複数の透明性のある画像を重ね合わせることで隠された画像を復元する方式）などがあり同様に紹介されてきた。

1.1 準備

本稿はカードベースプロトコルのうち非コミット型のプロトコルを扱う。ユーザにより 1 ビット入力是一般的なエンコーディングルール $\clubsuit\heartsuit = 0, \heartsuit\clubsuit = 1$ に従う。出力がコミット型であるとは、定められたエンコーディングルールに基づいた形式でプロトコル停止時に結果を得るのである。最も有名な非コミット型カードプロトコルであ

¹ 株式会社インターネットイニシアティブ
Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan

^{a)} suga@iij.ad.jp

る Five-Card Trick は 2 ユーザ間で AND 演算を行うプロトコルである。2 入力を a, b としたとき

$\boxed{\heartsuit} \boxed{?} \boxed{?} (= a) \boxed{?} \boxed{?} (= b)$ として 5 枚のカードを並べてランダムシャッフル (巡回置換を c_5 としたとき、恒等置換 $id, c_5, c_5^2, c_5^3, c_5^4$ の 5 通りから等確率で選択してカード束に処理する操作) を行う。ここで $\boxed{?}$ は裏面にして入力したことを示している。ランダムシャッフルを行う際には先頭の $\boxed{\heartsuit}$ も $\boxed{?}$ とし、5 枚とも裏面に向けて処理する。出力は 5 枚のカードをすべて開示するで得られる。3 枚の $\boxed{\heartsuit}$ が連続して並んで出力されたとき $a \wedge b = 1$ 、それ以外は $a \wedge b = 0$ となる。以下は初期状態の状態を示している。

(a, b)	sequence
(0,0)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit}$
(0,1)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(1,0)	$\boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit}$
(1,1)	$\boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit}$

Five-Card Trick は、カード入力時 (もしくはすべて裏面にしてから) の置換とランダムシャッフルのみで構成されるシンプルなプロトコルである。

2020 年 10 月に開催されたコンピュータセキュリティシンポジウムでも物理暗号としてセッションが組まれており、様々なレクリエーション暗号が発表されている。特に 6 枚利用 3 入力の 3 入力多数決プロトコル [12] は非常にシンプルでエレガントな方式である。このうち非コミット型プロトコルの操作環境や前提条件を本稿でも同一として取り扱う。

本稿は ICISC2018 で品川らにより発表された Six-Card Trick [2] を扱う。Six-Card Trick は 6 枚 3 入力の非コミット型カードプロトコルであり、3 入力の equality function を出力する。Six-Card Trick は以下のステップにより構成される。

STEP-1 3 ユーザの入力 a, b, c に対してカード入力を

$$\boxed{?} \boxed{?} (= a) \boxed{?} \boxed{?} (= b) \boxed{?} \boxed{?} (= c)$$

とする。

STEP-2 6 枚のカードに

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

の置換を施す。

STEP-3 位数 6 のランダムカットを施す。

STEP-4 裏返して 3 枚の $\boxed{\heartsuit}$ が連続して並んでいる場合出力は 0 であり、それ以外は 1 である。つまり $a = b = c$ の場合は 1 として出力される。

以下は **STEP-1** での入力初期状態のパターンを示している。

(a, b, c)	sequence
(0,0,0)	$\boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(0,0,1)	$\boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit}$
(0,1,0)	$\boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(0,1,1)	$\boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit}$
(1,0,0)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(1,0,1)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit}$
(1,1,0)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(1,1,1)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit}$

以下は **STEP-2** 直後の状態についてすべてのパターンを示しており、 $a = b = c = 0$ または $a = b = c = 1$ のときのみ $\boxed{\heartsuit}$ が 3 枚連続して並んでいないことが分かる。

(a, b, c)	sequence
(0,0,0)	$\boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(0,0,1)	$\boxed{\clubsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\heartsuit}$
(0,1,0)	$\boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit}$
(0,1,1)	$\boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit}$
(1,0,0)	$\boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit}$
(1,0,1)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\heartsuit}$
(1,1,0)	$\boxed{\heartsuit} \boxed{\heartsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\clubsuit} \boxed{\clubsuit}$
(1,1,1)	$\boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit} \boxed{\heartsuit} \boxed{\clubsuit}$

2. 一般置換のバリエーション

STEP-2 での一般置換として

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

を用いているが、全探索により以下の 12 のバリエーションがあることが分かった。ただし巡回置換

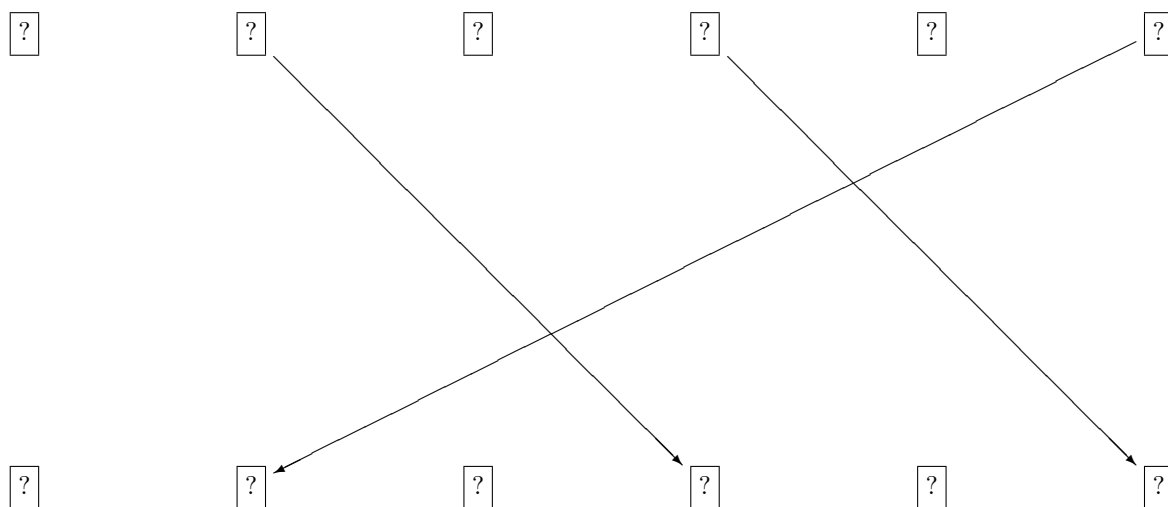
$$c_6 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 6 & 1 \end{pmatrix}$$

とする。

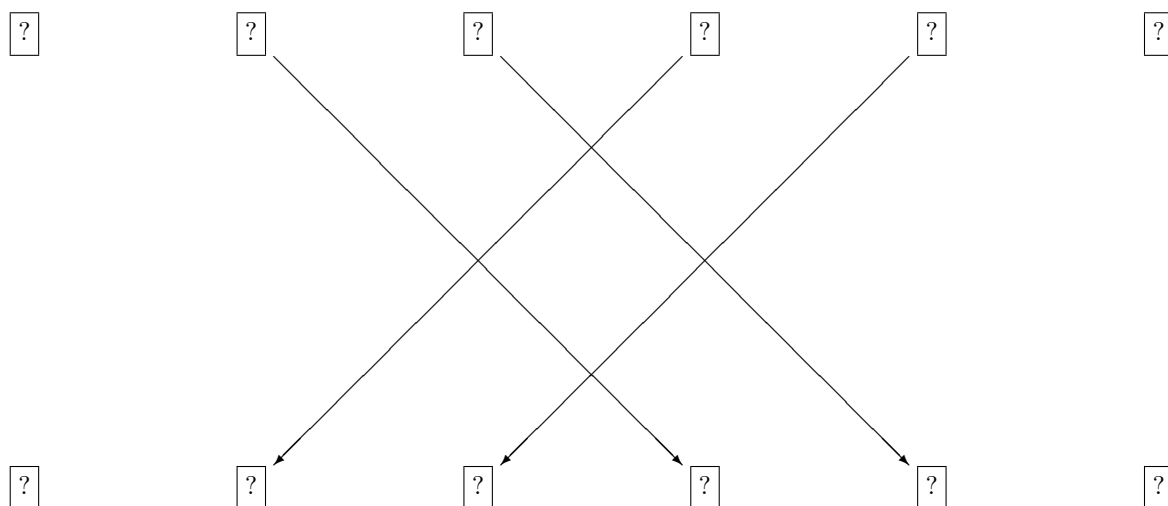
- σ
- $c_6 \circ \sigma$
- $c_6^2 \circ \sigma$
- $c_6^3 \circ \sigma$
- $c_6^4 \circ \sigma$
- $c_6^5 \circ \sigma$
- $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 5 & 2 & 3 & 6 \end{pmatrix}$
- $c_6 \circ \tau$
- $c_6^2 \circ \tau$
- $c_6^3 \circ \tau$
- $c_6^4 \circ \tau$

• $c_6^5 \circ \tau$

オリジナルの σ は以下のカード変換が行われている。



一方で



のようなパターン (τ) があることが分かった。不動点は 3 ではなく 2(両端のカード) であるが、2 枚の隣り合ったカードを 2 指（例えば人差し指と中指）で同時に移動させることにより 2 ターンで移動させることができる。また、両手を用いることで円を描くようにスムーズに入れ替えることができるメリットを持つ。定量的な評価は今後の課題とする。

3. まとめと今後について

ICISC2018において品川らによって提案された Six-Card Trick は前処理である一般置換（巡回置換と対比させるためにあえて呼ぶ）とランダムカット（巡回置換）のみで構成されるシンプルな方式である．本稿では一般置換にあたる部分の完全分類を行い，ユーザビリティの観点で従来よりも優位と考えられる方式を新たに発見した．ユーザ実験を行っていないためユーザビリティの観点で今後調査を行う．

参考文献

- [1] 水木, 電子情報通信学会 基礎・境界ソサイエティ Fundamentals Review, 2016 年 9 巻 3 号 pp.179-187, カード組を用いた秘密計算, https://www.jstage.jst.go.jp/article/essfr/9/3/9_179/_article/-char/ja
- [2] Kazumasa Shinagawa, Takaaki Mizuki, The Six-Card Trick: Secure Computation of Three-Input Equality, ICISC 2018.
- [3] B. denBoer, More efficient match-making and satisfiability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.
- [4] T. Mizuki and H. Sone, Six-card secure AND and four-card secure XOR, International Workshop on Frontiers in Algorithmics, pp.358-369, 2009.
- [5] T. Mizuki, M. Kumamoto and H. Sone, The Five-Card Trick Can Be Done with Four Cards, Asiacrypt2012.
- [6] T. Nishida, Y. Hayashi, T. Mizuki and H. Sone, Card-based protocols for any boolean function, TAMC2015.
- [7] 安部, 山本, 岩本, 太田, 初期文字列が 29 文字の 4 入力多数決 Private PEZ プロトコル, 信学技報, vol.118, no.478, ISEC2018-117, pp.223-228, 2019.
- [8] Y. Abe, M. Iwamoto and K. Ohta, Efficient Private PEZ Protocols for Symmetric Functions, TCC2019.
- [9] 駒野, コインを用いる新たなマルチパーティ計算, DICO2018.
- [10] 駒野, ボールと袋を用いた秘密計算, DICO2019.
- [11] K. Shinagawa, K. Nuida, T. Nishide, G. Hanaoka and E. Okamoto, Size-Hiding Computation for Multiple Parties, ASIACRYPT2016.
- [12] 豊田, 宮原, 水木, 曾根, 6 枚のカードを用いた 3 入力多数決関数の秘密計算, CSS2020, 4D1-4, 2020.