Vol.2021-DPS-186 No.7
Vol.2021-CSEC-92 No.7
2021/3/15

手の内だけで簡単に実行可能な Six Card Trick とカード入力後の置換に関する考察

須賀 祐治[1,a)]

概要：非コミット型カードベース暗号の 1 種である Six Card Trick は 3 入力の equality function（等価関数）を出力する 3 入力 6 カードのプロトコルである．本稿では，SCIS2021 で提案された最終結果の一部開示というアイデアを用いることにより，3 者のカード入力後の置換を排除しても Six Card Trick と同様の出力結果を得られることを示す．この方式は机などの平らな場所にカードを置いてからカードを入れ替える操作を必要としないことから究極的に簡素な方式であり，手の内だけで簡単にプロトコルを実行可能なメリットを持つ．本稿の後半では，CSEC-91 で提示された Six Card Trick にてランダムシャッフルを行うカード置換の事前処理に関する完全分類と既存手法を再考し，カード入力に関する考察を行うことで既存方式との同値関係について論じる．

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

A new proposal for the Six Card Trick that can be easily executed by hands and discussions of permutations after user's card inputs

Yuji Suga[1,a)]

Abstract: The Six Card Trick, a kind of non-committed card-based protocol, is a three-input, six-card protocol that outputs a three-input equality function. In this paper, we show that by using the idea of partial disclosure of the final result proposed in SCIS2021, we can obtain the same output result as the Six Card Trick without the permutation after the three user's card inputs. This proposal is ultimately simple because it does not require replacements on a flat space such as a desk, and it has the advantage that the protocol can be easily executed by one's own hands. In the latter part of this paper, we present a complete classification of the pre-processing of card replacement by random shuffling in the Six Card Trick presented at CSEC-91, recall existing methods and discuss equivalent relations with existing methods by considering user's card inputs.

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[8], [9]，ペンシルパズル [15]，コイン [10] やボール [11] 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

[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

ⓒ 2021 Information Processing Society of Japan

Vol.2021-DPS-186 No.7
Vol.2021-CSEC-92 No.7
2021/3/15

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 非コミット型プロトコル

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 ビット入力は一般的なエンコーディングルール $\boxed{\clubsuit}\boxed{\heartsuit} = 0$, $\boxed{\heartsuit}\boxed{\clubsuit} = 1$ に従う．出力がコミット型であるとは，プロトコル停止時に得られる結果が，入力のエンコーディングルールに基づいた形式であることを指す．一方で非コミット型であるとは，プロトコル停止時に利用されたカードを開示するなどして結果を得る方式である．

1.2 Five-Card Trick

最も有名な非コミット型カードプロトコルである 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 $a, b \in \{0,1\}$ としたとき

$\boxed{\heartsuit}$ $\boxed{?}\boxed{?}(=a)$ $\boxed{?}\boxed{?}(=\bar{b})$ 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 と 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．また $\bar{b}$ は b の否定 (negation) である．

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ことで得られる．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 5 枚のカードの初期状態を示している．

(a,b)	sequence
(0,0)	♡ ♣ ♡ ♡ ♣
(0,1)	♡ ♣ ♡ ♣ ♡
(1,0)	♡ ♡ ♣ ♡ ♣
(1,1)	♡ ♡ ♣ ♣ ♡

Five-Card Trick は，カード入力時の一般置換（このケースでは b を入力の際にカードを倒置して置いているため 5 枚のカード全体として $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$ の置換を行っていると考える）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．

1.3 6 枚利用 3 入力多数決プロトコル

その他の非コミット型カードプロトコルとしては，CSS2020 で発表された 6 枚利用 3 入力多数決プロトコル [17] がある．6 枚カードに対して，恒等置換か $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 4 & 5 & 3 \end{pmatrix}$ を 1/2 ずつの確率で発生させるためにランダム二等分割カット [5] を活用して巧みに構成している．結果開示においては，一部開示の結果によりその後の処理フローが分岐するが，一度表面にしたカードを再度裏面にする処理はなく，有限回で終了する効率的なプロトコルでもある．カード開示時には一般性を失うことなく最も左のカードをめくることができる．第 1 の位置のカードが $\boxed{\heartsuit}$ の場合には残り 5 枚のカード全てを開示し $\boxed{\clubsuit}$ が 3 枚並んで登場するかどうかを確認する．この確認処理はオリジナルの Five-Card Trick と同じように行われる．また第 1 の位置のカードが $\boxed{\clubsuit}$ の場合も，残り 5 枚のカードをすべて開示しそのうち 3 枚の $\boxed{\heartsuit}$ が並んでいるかどうかを確認する．このように，豊田らによる 6 枚利用 3 入力多数決プロトコルは，サブルーチンとして $\boxed{\heartsuit}$ ベースの Five-Card Trick もしくは $\boxed{\clubsuit}$ ベースの Five-Card Trick を内包していると考えることができる．

1.4 Six-Card Trick

本稿は ICISC2018 で品川らにより発表された Six-Card Trick [3] をスターティングポイントとする．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（等価関数）の結果を出力する．等価関数とは入力のすべてが同じであるかどうかを判定する関数であり，3 入力 $a, b, c \in \{0,1\}$ の場合には $a = b = c = 0$ または $a = b = c = 1$ の場合のみ True を返却しそれ以外は False を出力する．Six-Card Trick は以下のステップにより構成される．なお，各ステップのシーケンス図は図 1 のとおりである．

図 1 Six-Card Trick における各ステップの処理概要

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．

ⓒ 2021 Information Processing Society of Japan

Vol.2021-DPS-186 No.7
Vol.2021-CSEC-92 No.7
2021/3/15

STEP-3 位数 6 のランダムカットを施す．

STEP-4 すべてのカードを裏返して 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)	♣♡♣♡♣♡
(0,0,1)	♣♡♣♡♡♣
(0,1,0)	♣♡♡♣♣♡
(0,1,1)	♣♡♡♣♡♣
(1,0,0)	♡♣♣♡♣♡
(1,0,1)	♡♣♣♡♡♣
(1,1,0)	♡♣♡♣♣♡
(1,1,1)	♡♣♡♣♡♣

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)	♣♡♣♡♣♡
(0,0,1)	♣♣♣♡♡♡
(0,1,0)	♣♡♡♡♣♣
(0,1,1)	♣♣♡♡♡♣
(1,0,0)	♡♡♣♣♣♡
(1,0,1)	♡♣♣♣♡♡
(1,1,0)	♡♡♡♣♣♣
(1,1,1)	♡♣♡♣♡♣

またランダムカットの処理により $(a,b,c)=(0,0,0)$ のケースも $=(1,1,1)$ のケースも同じ配置となることが分かる．これは第 3 者からこのプロトコルを観測した際にたとえ結果が True だったとしても，等価関数の結果のみが観測できるだけで，各ユーザの入力に関するいかなる情報も漏れていないことを示している．

2. 一部開示テクニック

Six-Card Trick における **STEP-4** について再考し，カード開示時にすべてのカードではなく一部のみを開示するテクニックが SCIS2021 にて提案されている [18]．本稿はこの一部開示テクニックを用いて，Six-Card Trick をより簡便な方式に変更することができることを示していく．具体的には **STEP-2** の処理を取っ払い，ユーザが一般置換の思い違いを無くす，例えば $\begin{pmatrix}1&2&3&4&5&6\\1&4&3&6&5&2\end{pmatrix}$ を $\begin{pmatrix}1&2&3&4&5&6\\1&6&3&2&5&4\end{pmatrix}$ と間違えてしまうようなミスを防ぐことができユーザビリティを向上させることができる．また，**STEP-2** が無いことから机などの平らな場所にカードを置くなどしてカードを入れ替える操作を必要としないことから究極的に簡素な方式であり，手の内だけで簡単にプロトコルを実行可能なメリットを持つと考えられる．

一部開示テクニックの概要に触れる前に，まずエンティティモデルの概要を説明する．

2.1 エンティティモデルの整理

非コミット型プロトコルにおいて以下のエンティティを考える．

入力者（Submitters） いわゆるプロトコル参加者でありカードによる入力を行うエンティティ．

観測者（Observers） 入力は行わないが，プロトコルを傍観することで当該プロトコルが正しく動作しているか確認することができるエンティティ．

獲得者（Gainers） 最終開示時に結果を得るエンティティ．入力者は必ずしも結果を知る必要がないケースもあるため敢えて入力者や観測者と分別している．一方で，通常のプロトコルにおいて結果は入力者・観測者ともに得ることができる．

図 2 は上記エンティティの関係と役割を示すモデル図である．

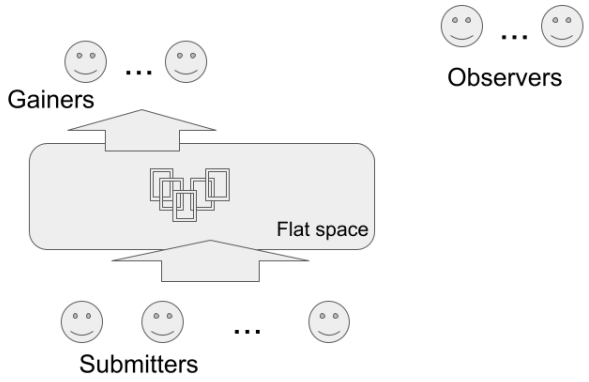


図 2 非コミット型プロトコルにおけるエンティティモデル

本モデルでは，以下のように 3 つのフェーズに分かれて処理が行われる．1）入力者（Submitters）は机などの Flat space に定められた手順でカードを置くことで入力する．2）入力者または獲得者（Gainers）のひとりが手順に基づいてカードを操作する．カード操作は Flat space で行われるため観測者（Observers）はその手順が正しいかどうかを確認することができる．つまり Flat space で行われるすべてのカード操作は観測者により観測可能であることを意味する．3）最後に獲得者（Gainers）はカードを表面に開示し，プロトコルの結果を得る．

ⓒ 2021 Information Processing Society of Japan

方式	入力者	観測者	入力者かつ獲得者
5 Card Trick	自らの入力 a のみ	$a \wedge b$	$a \wedge b$
6 Card Trick	自らの入力 a のみ	$a=b=c$ かどうか	$a=b=c$ かどうか もし $a=b=c$ なら 0,1 かどうかまで確定
一部開示 5 Card Trick	自らの入力 a のみ	なし	$a \wedge b$
一部開示 6 Card Trick	自らの入力 a のみ	なし	$a=b=c$ かどうか もし $a=b=c$ なら 0,1 かどうかまで確定

表 1 各エンティティがアクセスできる情報の違い

ここで３）開示フェーズにおいて獲得者はカードを表面に開示して結果を得るが，カードの一部のみを開示することを考える．例えば Six-Card Trick における **STEP-4** において 6 枚のカードよりも少ないカード枚数でプロトコル結果を得られないかという点に注目する．

上記２）のフェーズにおいてはカードを並べ替えるために，一度カードを束にしてランダムシャッフルやランダム二等分割カットなどの操作が行われる．その後，入れ替えられたカードの前後関係を確認するためにカード開示を行うが，マジシャンが扱うようにカード束を表にして綺麗に横に広げる操作である「スプレッド」を行うことはより簡便にはなる．しかし観測者からは何か細工をされたように見えるため望ましくない．

また一部開示に関する大きな効果としては次のように，観測者に結果を知られないようにすることも考えられる．先に紹介した非コミット型プロトコルは最終的な結果を得る際に，利用していた全てのカードを開示している．そのため観測者はプロトコルが正しく動作しているかどうか確認できるだけでなく，最終結果を知ることもできる．この特徴は利用用途によっては入力者に不都合なユースケースもあると考えられる．そのためカードの状態がどのようになっているか観測者から見えないように，獲得者が確認するためには，全てのカードではなく，より枚数の少ない方がリーズナブルであることは明らかである．

さらに，これまでカードのみを想定して議論してきたが，裏面になったカードの表面をできるだけ観測者に知られずに扱うことに都合のよい代替物として麻雀牌がある．実際麻雀競技において Flat space に置かれた麻雀牌は伏せられており，それを他の競技者から表面が知られないよう自分だけが見えるように麻雀牌を入手する必要がある．また熟練者になると麻雀牌を掴むだけで表面を見ずとも何の牌であるかを知ることができるという意味でも，本稿で扱うような上記の要件を考えるとカードよりも麻雀牌が適していると考えられる [19].

表 1 は上記のような観点のもと既存方式と一部開示方式との各エンティティが得られる情報量の違いを列挙したものである．表 1 記載の 2 つの一部開示方式に関して以下説明を行う．より操作が簡便である Six-Card Trick の拡張を最初に行う．

2.1.1 一部開示 Six-Card Trick

構成方式 1 Six-Card Trick **STEP-4** を以下とする．6 枚のうち左から 1,3,5 枚目のみを裏返す．3 枚とも同じカード種が並んでいる場合 出力は 1 (つまり $a=b=c$) であり，それ以外は 0 である．

注意 2 上記構成方式 6 において 3 枚一斉に開示してよい．つまり逐次開示で途中結果に応じてフローが変化することはない．

観測者と獲得者の視点で以下のような議論ができる．ここで，獲得者しかカード内容がわからないように開示する方法を「秘匿開示」と呼ぶこととする．

注意 3 2 枚まで観測者の分かるように開示しても結果に関する情報を漏らさない．よって観測者に最終結果を秘匿するために，実運用では 1,3 枚目を開示し，5 枚目のみを獲得者が秘匿開示する方式が適している．

観測者に結果を秘匿したい場合には，2 枚の公開開示，1 枚のみ秘匿開示で済むためリーズナブルな方式であることが分かる．

2.1.2 一部開示 Five-Card Trick

観測者に結果を秘匿しない通常のケースから考える．

構成方式 4 Five-Card Trick において 5 枚開示を以下のように置き換える．ただし 5 枚のうち左から i 枚目を T_i とする．1) T_1 のみを裏返す．2) $T_1 =$ ♣ のとき T_3, T_4 を裏返す．$T_1 =$ ♡ のとき T_3 を裏返す．$T_3 =$ ♣ のときは T_5 を $T_3 =$ ♡ のときは T_2 を開示する．

一部開示 Six-Card Trick において秘匿開示の概念を提示したが，観測者に結果を秘匿する方式を検討する場合には以下を考慮する必要がある．

注意 5 5 枚のうち任意の 1 枚を裏返しても結果に関する情報を一切漏らさないが，2 枚裏返した際にともに ♣ であった場合には結果が確定してしまう点を鑑み，観測者は 1 枚のみ開示まで許される．また 2 枚目を得た時点で結果が判定するケースもあることからダミーで 3 枚目も継続して開示する，という操作が必要となる．

ⓒ 2021 Information Processing Society of Japan

Vol.2021-DPS-186 No.7
Vol.2021-CSEC-92 No.7
2021/3/15

3. 一般置換のない Six-Card Trick

一部開示テクニックを適用した新しい方式を以下とする．ランダムシャッフルを行うだけで構成できる，これ以上簡便な方法がない方式である．

構成方式 6　前章で説明した一部開示 Six-Card Trick の構成 の変更に加え Six-Card Trick **STEP-2** をスキップする．

構成 6 でうまく動作する仕組みについて詳しく見ていく．

3.1 状態の 10 進数表現と代表元の導入

6 枚のカードを示すための表現方法として以下を導入する．横一列に並べられた 6 枚のカードを 6 桁 2 進数として見る，つまり [♣] を 1, [♡] を 0 として考える．例えば入力 $(a,b,c)=(0,0,0)$ のときの Six-Card Trick 初期入力状態 [♣][♡][♣][♡][♣][♡] は $(101010)_2$ と考える．2 進数表現のままであると可読性が低いため，このカード状態を 10 進数表現である 42 を用いることとする．

Six-Card Trick **STEP-2** をスキップし **STEP-3** のランダムシャッフルを行った場合，カードがシフトされることにより，この 10 進数表現が変化することとなる．例えば $(a,b,c)=(1,1,0)$ のときシフト無しの状態は [♡][♣][♡][♣][♣][♡] であり 10 進数表現としては 22 である．左シフトすることはこの数字が 2 倍され，キャリーがある，つまり左に追い出されたカードが [♣] であり最右に位置することから 64 以上の 10 進数になった場合には $mod\ 63$ をすればよいこととなる．$(a,b,c)=(1,1,0)$ のとき

$$22 \to 44 \to 25 \to 50 \to 37 \to 11(\to 22)$$

のように左シフトするたびに変化し元に戻ることが分かる．このとき代表元を最も小さい数値を採択することとし，この場合は 11 であり代表元として (11) と表現することとする．

他のすべての (a,b,c) のパターンについて代表元を調べると (13), (21) のバリエーションがあり，それぞれ以下のように遷移する．周期は (11) および (13) については 6, (21) は 2 となる．

$$13 \to 26 \to 52 \to 41 \to 19 \to 38(\to 13)$$

$$21 \to 42(\to 21)$$

Six-Card Trick 初期入力状態 **STEP-1** に対する代表元は以下のとおりである．

(a,b,c)	sequence &	representative
(0,0,0)	♣♡♣♡♣♡	(21)
(0,0,1)	♣♡♣♡♡♣	(13)
(0,1,0)	♣♡♡♣♣♡	(13)
(0,1,1)	♣♡♡♣♡♣	(11)
(1,0,0)	♡♣♣♡♣♡	(13)
(1,0,1)	♡♣♣♡♡♣	(11)
(1,1,0)	♡♣♡♣♣♡	(11)
(1,1,1)	♡♣♡♣♡♣	(21)

ここで，代表元だけを扱えばよいのは **STEP-3** におけるランダムシャッフルが効いてくるため，どのくらいシャッフルされたか観測者はわからないためである．代表元が同じであれば，それらのカード配列は同一視されることを意味する．さらに Six-Card Trick の要件を満たすためには $(a,b,c)=(0,0,0)$ または $(a,b,c)=(1,1,1)$ 以外の状態が同一視される必要があることも分かる．つまり上記の状態では要件を満たさない．そこで **STEP-2** による一般置換を行う必要があった．このカード置換を施した場合の代表元は以下のとおりである．

(a,b,c)	sequence &	representative
(0,0,0)	♣♡♣♡♣♡	(21)
(0,0,1)	♣♣♣♡♡♡	(7)
(0,1,0)	♣♡♡♡♣♣	(7)
(0,1,1)	♣♣♡♡♡♣	(7)
(1,0,0)	♡♡♣♣♣♡	(7)
(1,0,1)	♡♣♣♣♡♡	(7)
(1,1,0)	♡♡♡♣♣♣	(7)
(1,1,1)	♡♣♡♣♡♣	(21)

このように a,b,c のうち一つでも異なる入力があった場合には同じ代表元である (7) しか現れないようにすることが Six-Card Trick の本質である．

次に初期状態のままのときについて考察する．ここで $(a,b,c)=(0,0,0)$ または $(a,b,c)=(1,1,1)$ 以外のケースにおいて代表元は (11) と (13) の 2 パターンにぶれてしまっている．このぶれが原因で入力 (a,b,c) に関する情報が漏れてしまう問題が発生していることが分かる．

ⓒ 2021 Information Processing Society of Japan

そこで構成 6 を見直すと本構成は 1,3,5 枚目に位置するカードのみを開示することが既存方式との違いである．各代表元について実際のカードがどのように開示されるか考察すると，(11) と (13) の 2 パターンともに $\boxed{\clubsuit}$ が 2 枚，$\boxed{\heartsuit}$ が 1 枚のケースか，$\boxed{\clubsuit}$ が 1 枚，$\boxed{\heartsuit}$ が 2 枚のケースであることが分かる．一方で代表元 (21) では同じ種類のカードのみが現れることとなる．さらに各代表元において等確率で出現することも示される．これらの特徴により (11) と (13) が同一視されることから，この提案方式がうまく動作し，かつ入力 (a, b, c) に関する情報が漏らさないという観点で安全なプロトコルであることを示すことができる

4. 一般置換のバリエーション

Six-Card Trick における **STEP-2** での一般置換として

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

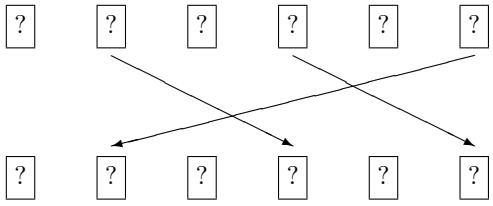
を用いられている．STEP-2 における一般置換の他の可能性を調査するために全探索を行い，以下の 12 のバリエーションがあることが示されている [20]．ただし巡回置換

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

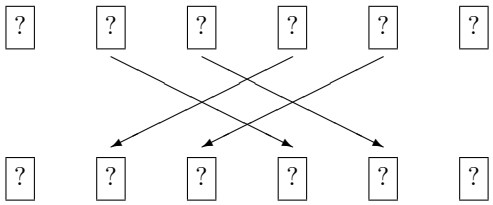
とする．

- 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 Six-Card Trick で用いられる一般置換 σ は以下のカード変換が行われている．



一方で

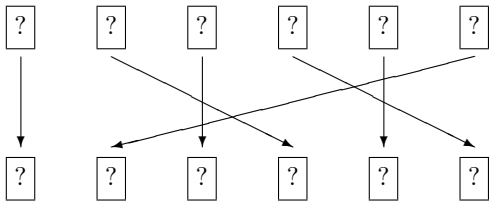


となるパターン (一般置換 τ) があることが分かった．このオリジナルの Six-Card Trick で用いられる一般置換とは異なる変換を用いる場合，**STEP-2** 直後の状態についてすべてのパターンは以下のとおりである．

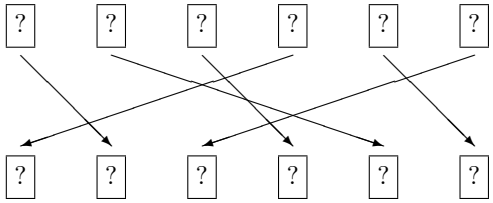
(a, b, c)	sequence
(0,0,0)	♣ ♡ ♣ ♡ ♣ ♡
(0,0,1)	♣ ♡ ♡ ♡ ♣ ♣
(0,1,0)	♣ ♣ ♣ ♡ ♡ ♡
(0,1,1)	♣ ♣ ♡ ♡ ♡ ♣
(1,0,0)	♡ ♡ ♣ ♣ ♣ ♡
(1,0,1)	♡ ♡ ♡ ♣ ♣ ♣
(1,1,0)	♡ ♣ ♣ ♣ ♡ ♡
(1,1,1)	♡ ♣ ♡ ♣ ♡ ♣

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．ユーザビリティの定量的評価は今後の課題とする．

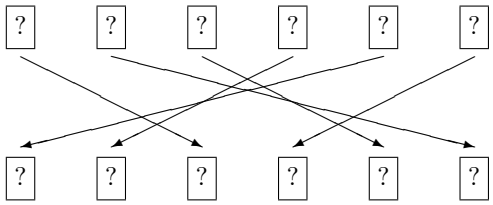
(1) $id \circ \sigma$



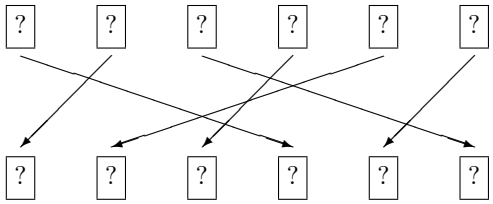
(2) $c_6 \circ \sigma$



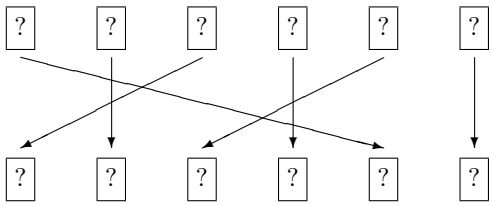
(3) $c_6^2 \circ \sigma$



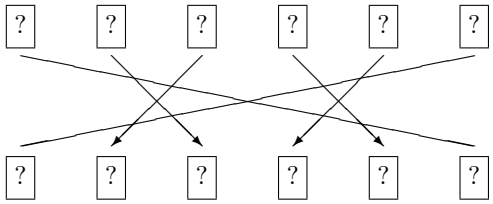
(4) $c_6^3 \circ \sigma$



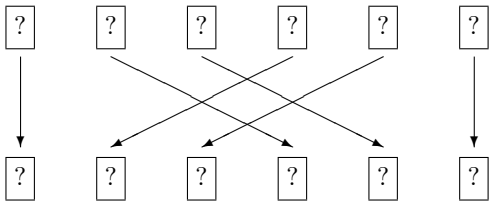
(5) $c_6^4 \circ \sigma$



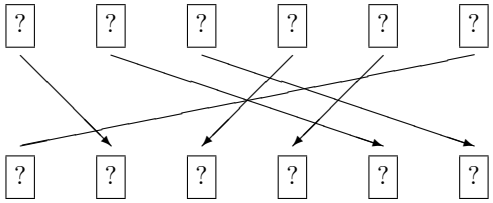
(6) $c_6^5 \circ \sigma$



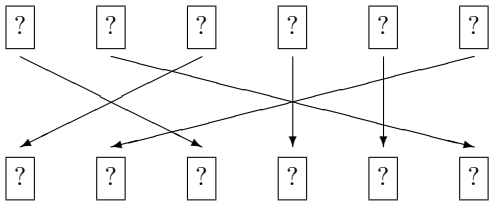
(7) $id \circ \tau$



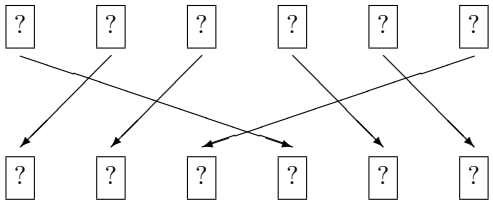
(8) $c_6 \circ \tau$



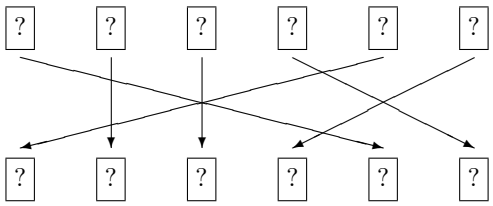
(9) $c_6^2 \circ \tau$



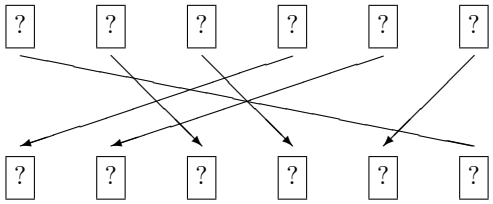
(10) $c_6^3 \circ \tau$



(11) $c_6^4 \circ \tau$



(12) $c_6^5 \circ \tau$



ⓒ 2021 Information Processing Society of Japan

4.1 ユーザビリティの視点での優位性考察

一般置換が覚えやすいかどうか，ミスを誘発しないで済むかどうか，などの観点で優位性を定性的な評価ができる．

置換 (1) σ の単純な亜種としては (4) $c_6^3 \circ \sigma$ が該当し（不動点以外の）3 枚のカード置換の逆置換を用いることで操作可能である．しかしこのケースでは置換が覚えにくくなるためミスを誘発する可能性をはらんでいる．

テーブルなどの平らな場所を用いずに（一人の）手中に収めたままでカードを移動させる場合，オリジナルの置換 (1) σ よりも (7) τ の方が手順が簡単であることが分かる．またテーブルを用いる場合，b の入力時に 2 枚のカードの隙間をスパースにしておく（2 枚分のカードが入る余地を残しておく）ことで (10) $c_6^3 \circ \tau$ の置換では 2 枚のカードのみに触れるだけでよいこともメリットとして見いだせる．

4.2 HST14 との比較

Heather らによる方式 HST14 [2] は 6 枚のカードを円状に配置し，各ユーザは対面に向けてカードを置くことで実現する方法である．円状に並べたカードを一直線に並べると 一般置換 σ と τ と同じ配置となることが分かった．さらに σ と τ の違いは 2 ユーザ b と c を入れ替えることで実現されることにも注意する．

5. 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とランダムカットでのみで構成されるシンプルな方式である．本稿では SCIS2021 で提案された最終結果の一部開示というアイデアを用いることにより，3 者のカード入力後の置換を排除しても Six Card Trick と同様の出力結果を得られることを示された．その際にはカード状態を 10 進数表現し，代表元に集約するという新しい表現方法を導入することで安全性の議論を行っている．

本方式は机などの平らな場所にカードを置いてからカードを入れ替える操作を必要としないことから究極的に簡素な方式であり，手の内だけで簡単にプロトコルを実行可能なメリットを持つと考えられる．今後さらなるユーザビリティ確保のための手法を定量的に評価するとともに，4 人以上の入力への拡張を試みる．

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] J. Heather, S. Schneider, and V. Teague, Cryptographic Protocols with Everyday Objects, Formal Aspects of Computing 26(1), pp.37-62, 2014.
[3] Kazumasa Shinagawa, Takaaki Mizuki, The Six-Card Trick: Secure Computation of Three-Input Equality, ICISC 2018.
[4] B. denBoer, More efficient match-making and satisability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.
[5] T. Mizuki and H. Sone, Six-card secure AND and four-card secure XOR, International Workshop on Frontiers in Algorithmics, pp.358-369, 2009.
[6] T. Mizuki, M. Kumamoto and H. Sone, The Five-Card Trick Can Be Done with Four Cards, Asiacrypt2012.
[7] T. Nishida, Y.Hayashi, T. Mizuki and H. Sone, Card-based protocols for any boolean function, TAMC2015.
[8] 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.
[9] Y. Abe, M. Iwamoto and K. Ohta, Efficient Private PEZ Protocols for Symmetric Functions, TCC2019.
[10] 駒野, コインを用いる新たなマルチパーティ計算, DICOMO2018.
[11] 駒野, ボールと袋を用いた秘密計算, DICOMO2019.
[12] K. Shinagawa, K. Nuida, T. Nishide, G. Hanaoka and E. Okamoto, Size-Hiding Computation for Multiple Parties, ASIACRYPT2016, 2016.
[13] S. Ruangwises, T. Itoh, Securely Computing the n-Variable Equality Function with 2n Cards, TAMC2020, 2020
[14] S. Ruangwises, T. Itoh, Physical Zero-Knowledge Proof for Numberlink Puzzle and k Vertex-Disjoint Paths Problem, New Generation Computing, 2020.
[15] T. Sasaki, D. Miyahara, T. Mizuki, H. Sone, Efficient card-based zero-knowledge proof for Sudoku, Theoretical Computer Science, Volume 839, pp.135-142, November 2020.
[16] H. Ono, Y. Manabe, Card-Based Cryptographic Protocols with the Minimum Number of Rounds Using Private Operations, New Generation Computing, 2020.
[17] 豊田, 宮原, 水木, 曽根, 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.
[18] 須賀, 怠惰なユーザのための非コミット型カードベース暗号, SCIS2021, 2F2-1, 2021.
[19] Y. Suga, Card-based Cryptography Meets Mahjong Tiles, Small-workshop on Communications between Academia and Industry for Security 2021, 2021.
[20] 須賀, 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, 情報処理学会研究報告 Vol.2020-CSEC-91, No.34, 2020.

ⓒ 2021 Information Processing Society of Japan