CL-003

グラフアクセス構造を表現する非コミットメント型カードプロトコルの上下カードへの適用と不正入力攻撃の考察

Application of non-commitmental card protocols for representing access structures of a given graph to up-and-down cards, and considerations of rogue input attacks

須賀 祐治 *
Yuji SUGA

概要 2 者間非コミットメント型カードプロトコルにおいて，グラフをアクセス構造として取り扱う．与えられたグラフから 1 頂点を選択することを秘密のカード入力とし，入力を秘匿しつつ 2 点間の距離に応じた出力する秘密計算が提案されており，この手法は一致関数の拡張として考えることができる．特に Johnson association schemes を実現する 2 色カードを用いたナイーブなプロトコル実装の拡張と考えることもできる．今回，ランダムカットを用いた単純な新しいカード入力の制限方法を導入する際に，2 色カードではなく，名刺や一部の麻雀牌のような上下カードを適用することを検討する．このとき 2 色カードでは考慮する必要のなかったカード入力不正もしくは誤入力の検知と対策方法について考察を与える．

1 研究の背景と本論文の貢献

カードベースプロトコルはトランプカードのような物理的なアイテムを利用し，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．一般的なカードベース暗号における標準モデルもしくは General セッティングでは，2 種類のスート $\boxed{\clubsuit}\boxed{\heartsuit}$ が用いられる [2]．1 ビット入力は 2 種類 2 枚のカードを用いて以下の一般的なエンコーディングルールに従って入力される：$\boxed{\clubsuit}\boxed{\heartsuit} = 0$, $\boxed{\heartsuit}\boxed{\clubsuit} = 1$．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，ペンシルパズル，コインやボール，麻雀牌 [24] などの玩具やチーズを用いる方式が提案されており様々な方式に拡張されている．初期的プロトコルには AND 演算や XOR 演算 [1] があるが，演算のバリエーションについても高機能化しており，リッカート尺度のうちのひとつの値を秘密の入力として，2 ユーザの意見がどのくらい近いかを知るプロトコルの一連の研究もある．例えば 4 段階のリッカート尺度の構成には上下カード $\boxed{\uparrow}\boxed{\downarrow}$（名刺のように上下を入れ替えて 2 パターンを入力可能で，裏面が上下入れ替えに対して識別不可能性を持つ）の 2 枚を用いて多値入力を表現している．上下カードを用いることで通常モデルにくらべ約半分の枚数で同様のプロトコルを実現できる点に加え，名刺など比較的入手が容易なカードであり，より実現可能で（カード枚数が少ないことから）簡便な操作である点も利点と考えられている．

カードベース暗号において，代数的構造やグラフ構造に着目しアソシエーションスキームの 1 種である Hamming scheme $H(q,n)$ の自然な実装としてマッチング可能なカードプロトコルを考え，カード入力を一部に制限することで これまでの方式よりもカード枚数を削減することのできる試みがある [25]．同じくアソシエーションスキームの 1 種である Johnson scheme の induced sub matrix を考えることで代数的構造を保持しているケースについて，アソシエーションスキームの位数が 10 以下について Johnson schemes $J(4,2), J(5,2)$ および $J(6,3)$ において完全な分類を与えている [26]．この中には位数 9 の Hamming scheme $H(3,2)$ が含まれており，3×3 タイプのマッチングに関する新しいカードプロトコルを構成するなど新しいスキームを見出すことを可能としている．

SCIS2024 では XOR 演算プロトコルを 2 者間の多値入力が可能な一致関数に素直な拡張することを考えている [27]．さらにこの考えを進め，2 ユーザの入力が一致していることを知るだけでなく，入力に応じた距離を出力させるようにグラフでアクセス構造を表現するケースに拡張することを考える．与えられたグラフが完全グラフの場合には，これは一致関数と全く同じ構造となる．本稿では 2 頂点の距離に基づく非コミットメント型カードプロトコルを取り上げる．出力がコミットメント型であるとは，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

* 株式会社インターネットイニシアティブ, 〒 102-0071 東京都千代田区富士見 2-10-2 飯田橋グラン・ブルーム, Internet Initiative Japan Inc., Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo, 102-0071 Japan suga@iij.ad.jp

す．一方で非コミットメント型であるとは，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．本稿では後者である非コミットメント型のプロトコルのみを扱うこととする．

1.1 本稿の貢献

2 者間非コミットメント型カードプロトコルにおいて，グラフをアクセス構造ととして取り扱う．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．最も有名な非コミット型カードプロトコルのひとつである Five-card trick [3] はハートとクラブ 2 種類のスートのカードを用いる 2 ユーザ間での 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 $\boxed{?}\boxed{?}(=\bar{a})\ \boxed{\heartsuit}\ \boxed{?}\boxed{?}(=b)$ として 5 枚のカードを並べてランダムカットを行う．ここで t 個の元に対する巡回置換を c_t としたとき，恒等置換 id と $c_5, \ldots, c_5^{t-2}, c_5^{t-1}$ の t 通りから等確率で選択してカード束に処理する操作のことをランダムカットと呼ぶ．また $\boxed{?}$ は裏面にして入力したことを示しており $\bar{a}$ は a の否定 (negation) であり，通常モデルでのエンコーディングルールでは 1 ビットを表現する 2 枚のカードの左右を入れ替える操作と一致する．

与えられたグラフから 1 頂点を選択することを秘密の入力とし，入力を秘匿しつつ 2 点間の距離のみを出力する秘密計算を考える．このとき Johnson association schemes を実現する 2 色カードを用いたナイーブなプロトコル実装を出発点とする．与えられたグラフ上の距離で出力を表現する非コミットメント型カードプロトコルに関する複数の具体的な事例として SCIS2024 にてカードプロトコルの系列で n-gon グラフ C_n のアクセス構造を持つカードプロトコルが提示されている [27]．実装方法としてはカード入力時にランダムカットを用いた単純な新しい入力方法が導入されており，入力後はデッキ分割法を適用しパイルスクランブルシャッフルとランダムカットを一度に行う効率的な処理を行っている．

本稿は位数が 6 まで，つまり 1 ユーザの配布枚数が 3 から 6 枚までの状況において上限カードを用いて構成される入力パターンの初期状態を分類し，この入力に応じて構成されるアクセス構造がグラフで表現されるかどうかについて検討を行った．ちなみに 2 枚のケースは XOR 演算と考えることができるという観点では XOR 演算の拡張と考えることもできる．実際多値入力の一致関数は XOR 演算プロトコルの拡張であることからもこの事実を捉えることができる．

2 準備

2.1 アソシエーションスキーム

有限集合 X（位数 $n := |X|$）に対して分割 $R_0, R_1, \ldots, R_d$ を考える．このとき次の 4 つの性質を満たすとき $(X, \{R_i\}_{0 \le i \le d})$ をクラス d のアソシエーションスキームと呼ぶ [15].

- (i) $R_0 = \{(x, x) \in X \times X \mid x \in X\}$
- (ii) $R_0, R_1, \ldots, R_d$ は集合 $X \times X$ の分割となる．$R_0 \cup R_1 \cup \cdots \cup R_d = X \times X$ かつ $i \neq j$ ならば $R_i \cap R_j = \emptyset$ である．
- (iii) 各 $i \in \{0, 1, \ldots, d\}$ に対し $R_i^T = Ri'$ を満たす $i' \in \{0, 1, \ldots, d\}$ が存在する．ここで $R_i^T = \{(y, x) \in X \times X \mid (x, y) \in R_i\}$ とする．
- (iv) 任意の $i, j, k \in \{0, 1, \ldots, d\}$ に対し集合 $\{z \in X \mid (x, z) \in R_i, (z, y) \in R_j\}$ の位数 p_{ij}^k は組 $(x, y) \in R_k$ の取り方に依らず i, j, k のみによって定まる．

次に上記定義を行列表現することを考える．隣接行列の成分 $(A_i)_{x,y}$ を 1 if $(x, y) \in R_i$, 0 if $(x, y) \notin R_i$ とする．このとき A_i は成分が 0 か 1 となる位数 n の正方行列となる．アソシエーションスキームの 4 条件は以下のように表現し直すことができる．

- (i) $A_0 = I$
- (ii) $\sum_{i=0}^{d} A_i = J$
- (iii) 任意の i に対して $A_i^T = A_{i'}$ となる i' が存在する
- (iv) $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$

ここで I は n 次の単位行列，J は成分が全て 1 となる n 次正方行列である．

行列による定義の条件 (iii) について，本稿で扱うカードプロトコルでは入力の対称性が求められるため任意の i に対して $A_i^T = A_i$ を満たす，つまり対称な（Symmetric）アソシエーションスキームのみを扱うこととなる点に留意する．

また，アソシエーションスキームの行列表現として関係行列 (relation matrix) を $\sum_{k=0}^{d} kA_k$ と定める．

2.1.1 Hamming schemes

アソシエーションスキームの 1 例としてハミングスキームがある．$X := {F_q}^n$ とし $d(x.y)(x, y \in X)$ をハミング距離とし $R_i := \{(x, y) \mid d(x.y) = i\}$ と分割した場合，アソシエーションスキームの条件を満たす．このアソシエーションスキームを $H(q, n)$ と記載し，ハミングスキーム (Hamming schemes) と呼ぶ．

2.1.2 Johnson schemes

アソシエーションスキームの系列に関してもう 1 例としてジョンソンスキームを紹介する．

v 点集合 $\Omega = 1, 2, \ldots, v$ とし $k < v$ を満たす自然数 k，X を v の k-部分集合全体の集合とする．$x, y \in X$ に対して $d(x, y) := k - |x \cap y|$ とおく．このとき $d()$ は距離の公理を満たす．

$R_i := \{(x, y) \mid d(x, y) = i\}$ として X 上の関係 $R_i (i = 0, 1, \ldots, k)$ を定義する．

このとき $\{X, \{R_i\} | i = 0, 1, \ldots, k)$ はアソシエーションスキームである．これをジョンソンスキーム (Johnson schemes) といい $J(v, k)$ と記載する．

2.2 m-デッキ分割法

2-party のカードプロトコルにおいて，リッカート尺度のうちのひとつの値を秘密の入力として，2 ユーザの意見がどのくらい近いかを知るプロトコルの一連の研究が存在する [17, 18, 19, 20, 21, 22, 24]．各研究において実装方法は異なるが，基本的なシャッフル方式については m-デッキ分割法が利用されている．

ユーザ 1 およびユーザ 2 がカード入力した m 枚ずつカード束のうち i 枚目同士の表面を重ね合わせて入力を秘匿する．それぞれの 2 枚のカードは輪ゴムなどで留められた上で m 個のカード束を一気に空に放り投げる操作を行う方式が m-デッキ分割法である．このとき一度のシャッフルで 1）2 枚のランダムカット，2）上下シャッフル，3）パイルスクランブルシャッフルの 3 つを一度に効率的に行うことができる非常によい性質を持っている点に留意する．

3 上下カードを利用するカードプロトコル

本稿では表面裏面ともに全く同じ絵柄であるカード（例えば名刺や麻雀牌）を用いることを考える（文献 [2] において水木らは絵柄の上下関係を生かしたメリットとデメリットについて考察されている）．このときカードの上下配置の違いを用いて，それぞれ（一般的なカードプロトコルで用いられる）異なるスートと対応づけることができる．つまり $\boxed{\downarrow}$ を $\boxed{\clubsuit}$ と，$\boxed{\uparrow}$ を $\boxed{\heartsuit}$ と同一視することで既存のプロトコルを実現可能である．スートを表現するメモ書きをしないでも，同一カードの束を用いてプロトコルを構成することができる点も一つのメリットである．本稿ではこのような裏面は識別不可能性を持ち，表面は $\boxed{\uparrow}$ と $\boxed{\downarrow}$ で表現可能なカードを Up-Down カードと呼ぶこととする．後述する上下シャッフルを施すことを鑑み，裏面は上下を入れ替えても識別不可能性を持つことが要求される．上記例で挙げた名刺の場合には裏面は白紙であり，かつ裏写りしない（表面が透けない）ことが条件となる．麻雀牌は裏面が同色で塗られているためこの要件を満たす．

またユーザは不正な入力を行わないという semi-honest なモデルについても検討されている．ユーザのカード入力時の不正についてはこれまでにいくつかの研究が行われており [6] [7] [8] [9] [13] [14]，今回扱う同一パターンカードにおいても不正の検知という観点で CSEC96 においてすでに議論がなされている [16]．今回提案するプロトコルにおいてはこのような不正入力が起きないように構成している点でも優位性が確認できる．上下カードの特性について理解するために，まず 2 者間の XOR 演算プロトコルを検討する．$\boxed{\downarrow} = 0$, $\boxed{\uparrow} = 1$ というエンコーディングルールに倣い 1 ユーザが 1 枚のカードを保持して入力する場合は以下のパターンとなる．

(a, b)	sequence
(0,0)	$\boxed{\downarrow}\boxed{\downarrow}$
(0,1)	$\boxed{\downarrow}\boxed{\uparrow}$
(1,0)	$\boxed{\uparrow}\boxed{\downarrow}$
(1,1)	$\boxed{\uparrow}\boxed{\uparrow}$

表 1: Up-Down カードを用いた XOR 演算プロトコル

カードを開示した際にはこれを 2×2 行列で表現すると以下のようになる．

$a \backslash b$	0	1
0	τ_0	τ_1
1	τ_1	τ_0

ここで 2 枚カード束が上下シャッフルによってどのようなバリエーションがあるかについて分類したものが表 2 である．

	同一視されるカード組
τ_0	$\boxed{\uparrow}\boxed{\uparrow}, \boxed{\downarrow}\boxed{\downarrow}$
τ_1	$\boxed{\uparrow}\boxed{\downarrow}, \boxed{\downarrow}\boxed{\uparrow}$

表 2: 2 枚カード束の上下シャッフル後の状態

上下シャッフルによって，2 枚のカード束が同じ方向を向いている τ_0 か異なる方向を向いている τ_1 かについてのみ検出することができる．これはユーザ入力を秘匿することができており Up-Down カードを用いた XOR 演算プロトコルを実現していることが分かる．

3.1 上下カードを利用した Hamming schemes $H(2, n)$ の実装方法

Hamming schemes $H(2, n)$ は 2-party のマッチングを可能とする．例えば $H(2, 3)$ は 3 つの質問（それぞれの答えは 2 通り）に対して，どのくらい相手と意見が合うかどうかをカードプロトコルを用いて知ることができ

る．具体的な $H(2,3)$ の実現方法は以下である．ここで 3 次元のバイナリベクトルつまり 8 通りのベクトルを考えることとする．

$a\backslash b$	000	110	101	011	111	001	010	100
000	0	2	2	2	3	1	1	1
110	2	0	2	2	1	3	1	1
101	2	2	0	2	1	1	3	1
011	2	2	2	0	1	1	1	3
111	3	1	1	1	0	2	2	2
001	1	3	1	1	3	2	2	2
010	1	1	3	1	2	2	0	2
100	1	1	1	3	2	2	2	0

3 次元のバイナリベクトルつまり 8 通りのベクトルを考え，0,1 をそれぞれ $\boxed{\downarrow}$, $\boxed{\uparrow}$ に置き換えることで，3-デッキ分割法を適用した場合にハミング距離に応じたカード出力を得ることができる．バイナリベクトルのハミング距離を関係としたカードプロトコルでの出力は右に示すとおりである．

$a\backslash b$	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$				
$\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	0	2	2	2	3	1	1	1
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$	2	0	2	2	1	3	1	1
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$	2	2	0	2	1	1	3	1
$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$	2	2	2	0	1	1	1	3
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$	3	1	1	1	0	2	2	2
$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$	1	3	1	1	2	0	2	2
$\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$	1	1	3	1	2	2	0	2
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$	1	1	1	3	2	2	2	0

Hamming schemes $H(2,n)$ のカードプロトコルへの応用のユースケースとしてはマッチングプロトコルが実現できる点がある．2 択の質問 n 個のうち，マッチング具合を測るためにどのくらい相手の意見と合致しているか（ハミング距離との捉えることができる）のみを出力とするプロトコルが実現でき，入力を秘匿したままで実行可能である．

4　小さい位数におけるプロトコルの完全分類

本章ではカード枚数 n が 6 以下のケースについてプロトコルの存在性に関して完全に分類を行う．まず，2 色カードを用いた一致関数（グラフ構造としては完全グラフに呼応する）を実現する方法について紹介する．実際には 2 色カードを用いた Johnson schemes についてナイーブな方法を示し，これを起点に上下カードへの適用を考える．

4.1　2 色カードを利用した Johnson schemes $H(v,k)$ の実装方法

各ユーザに v 枚 2 種類のカード，そのうち $\boxed{\heartsuit}$ k 枚，$\boxed{\clubsuit}$ を $(n-k)$ 枚配布する．入力としてカードの左より 1 から v までインデックス付けし，入力したい k-部分集合が位置する箇所のみに $\boxed{\heartsuit}$ を置くことで入力する．

2 ユーザはそれぞれ裏面でカード入力を行ったあと m-デッキ分割法を適用しカードを開示すると，各デッキにおける $\boxed{\heartsuit}$ の出現状態に応じて，2 ユーザの距離（集合としての被り具合）のみが開示される．

k-部分集合 x,y に対して $d(x,y) := k - |x \cap y|$ で定義されていることからデッキごとに開示する際に $\boxed{\heartsuit}\boxed{\heartsuit}$ と両方とも入力された箇所のデッキ数が $|x \cap y|$ であることから距離が出力される．距離が k つまり部分集合として被りがない場合には $\boxed{\heartsuit}\boxed{\heartsuit}$ が現れないし，距離 0 つまり全く入力が同じだったケースは $\boxed{\heartsuit}\boxed{\heartsuit}$ が k 回現れる．そのため $\boxed{\heartsuit}$ を含むデッキが k 回現れた時点でプロトコルとしては終了してよく，最小開示回数は k，最悪値は v である．

ここで入力に関しては秘匿されたままで，出力，つまり相手ユーザとの入力集合の被り具合（距離）のみが開示される点に留意する．Johnson schemes $H(v,k)$ のカードプロトコルへの応用のユースケースとしては複数の選択肢 v 個のうちから k 個を選択することから，選挙での複数人への投票や，複数の意見の中から賛成する項目を選ぶなどのシチュエーションにおいて，どのくらい意見が合致しているかのみを知ることができる機能を有している..

4.2　分類の方針

カードの上下配置の違いを用いて，それぞれ（一般的なカードプロトコルで用いられる）異なるスートと対応づけることを考える．つまり $\boxed{\downarrow}$ を $\boxed{\clubsuit}$ と，$\boxed{\uparrow}$ を $\boxed{\heartsuit}$ と同一視することで既存のプロトコルを実現可能である．

一方で上下カードで同様のプロトコルを実現する際には，カード操作の不正を議論する必要がある．具体的には与えられたカード組に対してまるごと上下を入れ替える操作により入力不正を行うことである．以下はランダムカットのみを行うようユーザに操作を制限しているがカード束の状態では上下関係を入れ替えることは容易であると考えられる．

デッキ分割法における結果開示の改善

既にデッキ分割法での開示フェーズの効率化について議論されている [27]．今回は，複数の分割デッキ（2 枚）のうち，すべてを開示することなく結果を得ることを想定する．その際には上下カードのカード束が上下関係を入れ替えることは容易であることを仮定して，それを防ぐ方法を検討することが求められる．以下このような攻撃を「上下入替攻撃」と呼ぶこととする

ここで分かることは，1 ユーザに渡されるカード枚数が奇数と偶数では大きく異なる点であり，奇数枚においては根本的な解決が難しい．理論的にはすべてのカード束を開示するまで不正を検知できないケースもあり得る．

4.3 各ユーザが 3 枚のカードを入力するケース

各ユーザが 3 枚しか持たない場合には $J(3,1)$ に該当するケース，つまり $\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$ の場合しか存在しない．$\boxed{\uparrow}$ が 2 枚の場合もスートを入れ替えることで同型なプロトコルが構成できるためである．この場合，グラフとしては完全グラフ K_3 に該当するプロトコルであり，これは 3 値入力の一致関数と同一である．ここでの上下入替攻撃を防ぐ方法はなく，すべて開示する必要がある．

4.4 各ユーザが 4 枚のカードを入力するケース

4 枚のケースは以下で網羅されることが容易に導き出される．

初期状態	距離分布	対応グラフ	攻撃耐性
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	$[0,1,1,1]$	K_4	3
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$	$[0,1,2,1]$	C_4	$\surd$

ここで距離分布はグラフ上のノードからの他のノードとの距離の分布を示しており，対応グラフはすべてのノードで，この距離分布に従ってノードが配置されているという対称性を持つことに留意する．また，ここでもスートの入れ替えや左右の配置などを考慮した同型なプロトコルについては同一視している．また $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$ のようなイタレーションが発生しているケースでは一致関数の拡張になっていない，つまり異なるノードの間の距離がゼロになるようなケースは排除している．

ここで攻撃耐性とは $\surd$ は攻撃を完全に防いでいること，また数字を表示しているケースについてはその枚数を開示すれば攻撃を「検知」できる最大枚数を示している．

4.5 各ユーザが 5 枚のカードを入力するケース

初期状態	距離分布	対応グラフ	攻撃攻撃
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	$[0,1,1,1,1]$	K_5	3
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	$[0,1,2,2,1]$	C_5	5
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$	$[0,2,1,1,2]$	C_5	5

C_5 となるケースが 2 種類現れていることが分かる．初期配置が違うにも関わらず，対応するグラフとしては同型となっている事例となる．いずれも攻撃耐性はなく，最大 5 枚を開示しない限り不正を検出できない．

4.6 各ユーザが 6 枚のカードを入力するケース

初期状態	グラフ	攻撃耐性
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	K_6	6
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	$C_6^\sharp$	5
$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	$K_{3,3}$	5
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$	C_6	$\surd$
$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$	$\overline{K_{2,2,2}}$	–

位数 6 で距離分布が $[0,1,2,2,2,1]$ となるグラフは存在しないが，距離に応じて出力が変化するのではなく，グラフ C_6 のノードが隣り合っているかどうかを判定することには利用できる点に留意する．つまりユースケースやシチュエーションによっては，グラフの距離ではなく隣接しているかどうかだけを確認するプロトコルの存在が求めれているかもしれないことを示している．このように隣接しているかだけを見極めるためのユースケースで利用されるグラフを $C_6^\sharp$ のように表現することとする．これは対応グラフが C_6 とはアクセス構造が異なり，C_6 のグラフのノードを秘密入力として，相手の入力したノードと一致・隣接・それ以外，の 3 パターンを出力するカードプロトコルが構成できたことを示すこととする．

攻撃耐性が – の箇所については，入力に依存する．つまり普遍的な不正入力が検出できず，不正入力は 1/3 の確率で不正な出力が得られることが分かった．

5 まとめ

2 者間非コミットメント型カードプロトコルのうち，グラフをアクセス構造として取り扱い，与えられたグラフから 1 頂点を選択することを秘密のカード入力とし，入力を秘匿しつつ 2 点間の距離に応じた出力する秘密計算を扱った．ここで一般的に利用されている 2 色カードではなく上下カードに置き換えることによる上下入替攻撃について指摘し，小さい位数でのプロトコルにおいてどのようなプロトコルにおいては検出可能かどうかについて検討した．

今回，ランダムカットを用いた単純な新しいカード入力の制限方法を導入しており，この制約のもとでは上下カードでも完全に不正を検出できるプロトコルについて見つけることができた．今後は他の入力制約に基づいた場合での検出可能性についても検討する余地がある．

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] T. Mizuki, H.Shizuya, Practical Card-Based Cryptography, FUN2014, pp.313-324, 2014.

[3] B. denBoer, More efficient match-making and satisability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.

[4] J. Heather, S. Schneider, and V. Teague, Cryptographic Protocols with Everyday Objects, Formal Aspects of Computing 26(1), pp.37-62, 2014.

[5] K. Shinagawa, T. Mizuki, The Six-Card Trick: Secure Computation of Three-Input Equality, ICISC 2018.

[6] カードベース暗号プロトコルに対する攻撃に関する考察, 信学技報, vol.113, no.326, ISEC2013-62, pp.21-28, 2013.

[7] 高島, 宮原, 水木, 曽根, 非コミット型カードベースプロトコルと不正開示攻撃の定式化, コンピュータセキュリティシンポジウム 2019(CSS2019), 2F4-3, pp.886-893, 2019.

[8] 安部，山本，岩本，太田，不正検知可能な 3 入力多数決カードプロトコル，3C3-2, SCIS2019.

[9] Y. Abe, M. Iwamoto,K.Ohta, How to Detect Malicious Behaviors in a Card-Based Majority Voting Protocol with Three Inputs, ISITA2020, C01-9, pp.377-381, 2020

[10] H. Ono, Y. Manabe, Card-Based Cryptographic Protocols with the Minimum Number of Rounds Using Private Operations, New Generation Computing, 2020.

[11] H. Ono, Y. Manabe, Card-based cryptographic logical computations using private operations, New Generation Computing, 2021

[12] Y. Manabe, H. Ono, Card-Based Cryptographic Protocols with Malicious Players Using Private Operations, New Generation Computing, 2022

[13] 駒野, 水木, カードベースプロトコルにおける並べ替え誤りに関する考察, 信学技報, vol.117, no.369, ISEC2017-86, pp.95-101, 2017.

[14] 駒野, 水木, コインベースプロトコルの初期配置誤りに関する考察, コンピュータセキュリティシンポジウム 2020(CSS2020), 4D1-5, pp.1283-1288, 2020.

[15] E. Bannai, T. Ito, Algebraic Combinatorics I, Association Schemes, Benjamin/Cummings, Menlo Park, CA, 1984.

[16] 須賀, 3 値入力可能な拡張 Five Card Trick における第 4 の未定義値の扱いについて, 情報処理学会研究報告 Vol.2022-CSEC-96, No.36, 2022.

[17] 須賀, そう思う・思わないの 4 段階リッカート尺度入力で 2 者がどのくらい近い意見か知るカードベースプロトコル, コンピュータセキュリティシンポジウム 2022(CSS2022), 1A3-I-1, 2022.

[18] 須賀, 8 段階リッカート尺度入力カードベースプロトコルの構成とハミングスキーム H(3,2) との関連性について, 情報処理学会研究報告 Vol.2022-CSEC-99, No.25, 2022.

[19] 須賀，6 段階リッカート尺度入力カードベースプロトコルの構成とアソシエーションスキーム・距離正則グラフとの関連性について, 4F2-3, SCIS2023, 2023.

[20] 須賀, 2 種類のカードを用いた 12 段階リッカート尺度入力カードベースプロトコルの構成, 情報処理学会 第 85 回全国大会講演論文集, 4E-01, 2023.

[21] 須賀, 12 段階リッカート尺度入力カードベースプロトコルの構成とアソシエーションスキームとの関係について, 情報処理学会研究報告 Vol.2022-CSEC-100, 2023.

[22] 須賀, カード入力を制限することで段階をダウングレードするリッカート尺度入力カードベースプロトコルの構成, 信学技報, vol.122, no.428, ISEC2022-94, pp.297-304, 2023.

[23] 須賀，奇数位数のリッカート尺度入力カードベースプロトコルの検討, 情報処理学会研究報告 Vol.2023-CSEC-101, 2023.

[24] 須賀, カードプロトコルで麻雀牌に持ち替えると, マルチメディア，分散協調とモバイルシンポジウム 2023(DOCOMO2023), pp.1493-1500, 2023.

[25] 須賀，J から H を見つけることによる 3 × 3 タイプのマッチングを可能とするカードプロトコルの構成，コンピュータセキュリティシンポジウム 2023(CSS2023), 1E3-4, 2023.

[26] 須賀, Johnson Association Schemes とカードプロトコルの関係について, 第 46 回情報理論とその応用シンポジウム (SITA2023), 1-2-1, 2023.

[27] 須賀, 2 頂点の距離に基づく非コミットメント型カードプロトコルの新しい系列と Difference set を用いた開示フェーズの効率化, 3D2-3, SCIS2024, 2024.

[28] 須賀，2 頂点の距離に基づく 1 ユーザ 6 枚のカードプロトコルの分類，2024 年電子情報通信学会総合大会，A-7-24, 2024.