異種カードを用いるカードベース暗号のメリット

須賀 祐治[1,a)]

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，各ユーザが異なる「異種カード」を用いることで既存方式であるデッキ分割法を用いずに，通常のランダムカットを用いた実装方法を提案する．背面や形状の異なる異種カードは，デッキ分割法のように各ユーザからの入力を重ね合わせたときに，区切りを示すデリミタカードを基準とすることで，2 色カード 4 枚 XOR 演算プロトコル [3] などの既存プロトコルにおいて RBC（ランダム二等分割カット）を RC（ランダムカット）で置換できる．これにより，RBC の実装が難しい媒体（例：麻雀牌）でも適用可能なプロトコルの幅が広がる．
さらに，デッキ分割法では各種フォールトが発生する可能性があったたが，1 回のランダムカットと片方のカード入力をすべてオープンすることにより効率的に実装可能な方式についても提案する．新規応用事例として，v 点集合 V の k 個部分集合全体（Johnson association schemes と関連）から X をユーザ A の入力とし，ユーザ B が $x \in V$ を選ぶとき，$x \in X$ を満たすかどうかのメンバーシップ判定カードプロトコルを構成することができる．

キーワード：カードベースプロトコル，非コミット型プロトコル, m-デッキ分割法, アソシエーションスキーム，メンバーシップ判定

Upon using different types of decks in the Card-based Cryptography

Yuji Suga[1,a)]

Abstract: We propose an implementation of two-party *non-commitment* card protocols that dispenses with the conventional deck partitioning method and instead uses only the *random cut* (RC), by letting the two players employ *heterogeneous cards* (*delimiter cards*). When the players' inputs are superposed as in the deck partitioning method, cards distinguishable by back design or physical form serve as fixed delimiters; with these delimiters, existing protocols such as the two-color four-card XOR [3] can replace the *random bisection cut* (RBC) with RC. This broadens applicability to physical media where RBC is difficult to implement (e.g., Mahjong tiles).
We further present an efficient realization that mitigates failure modes inherent to the deck partitioning method: it uses a single RC and fully opens one party's input. As a new application, we construct a card protocol for *membership* testing: given a v-element set V and the family of all k-subsets (related to Johnson association schemes), user A inputs X and user B chooses $x \in V$; the protocol decides whether $x \in X$.

Keywords: Card-based protocols, Non-committed protocols, m-deck partitioning method, Association schemes, Membership judgment

1. 本稿で扱うカードプロトコル

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カード入力とし，入力を秘匿しつつグラフ上の 2 点間の関係を出力する秘密計算を考え

[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．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であると捉え，これを素直に拡張することを検討している [27]．2 ユーザの入力が一致していることを知るだけでなく，入力に応じて複数のパターンを出力させることができ，かつ有向グラフでアクセス構造を表現するケースへの拡張を検討している．その一例としては（アクセス構造を表現する）与えられたグラフに 2 頂点の連結性に基づいて出力を変更する方式である．連結性だけを考慮しているため，1) 2 者が同じ頂点を入力（入力が一致），2) 2 頂点が連結している, 3) 2 頂点は連結していない，の 3 パターンのみで構成されており，比較的単純な構造とも言える．

入力のために各ユーザに与えられたカード束（デッキ）に対して，ランダムカットのみを実行することで所望の入力値を表現する方式を採択することで，入力のバリエーションから与えられたグラフは正則グラフとなり association schemes の構造を持つケースも存在するなどグラフとしても代数的に制約を受けた構造が得られることが分かっている．

実際，2 種類のスート $\boxed{\heartsuit}\boxed{\clubsuit}$だけで構成される入力パターンについて，「ランダムカットのみを実行することで所望の入力値を表現する方式」の初期状態を，小さいカード枚数（これはグラフの頂点数であり，入力のバリエーションの数と一致する）において分類を行った結果のひとつは以下となる．これは出力パターンとして 3 パターンのみを列挙している．

初期状態	距離分布	対応グラフ
♡♡♣♣♣	$[0,1,2,2,1]$	C_5
♡♡♣♣♣♣	$[0,1,2,2,2,1]$	C_6
♡♣♡♣♣♣	$[0,2,1,2,1,2]$	$K_{3,3}$
♡♡♣♡♣♣	$[0,2,2,1,2,2]$	$\overline{K_{2,2,2}}$
♡♡♣♣♣♣♣	$[0,1,2,2,2,2,1]$	C_7
♡♡♣♣♣♣♣♣	$[0,1,2,2,2,2,2,1]$	C_8
♡♣♡♣♣♣♣♣	$[0,2,1,2,2,2,1,2]$	$\overline{K_{2,2}+K_{2,2}}$
♡♡♣♡♣♣♣♣	$[0,2,2,2,3,2,2,2]$	$\overline{K_{2,2,2,2}}$
♡♣♡♣♡♣♣♣	$[0,3,1,3,1,3,1,3]$	$\overline{K_{4,4}}$

2. 準備

標準的なカードプロトコルの導入のための基礎的な概念をと，トランプカードを含む異種カードを利用した方式の前に 2 色カードを用いた既存の結果を中心にこれまでの結果を示す．

2.1 カードへの操作の整理

以下，本稿で用いるカードプロトコルにおける操作を一覧する．ただしデッキ分割法は後ほど詳しく扱う．

- **RC (Random Cut)**：長さ n の列に対し，巡回シフト群
  $mathrmid, rho, rho^2, dots, rho^{n-1}$（
  $rho = (1\ 2$
  $cdots\ n)$）から一様に 1 つを適用
- **RBC (Random Bisection Cut)**：偶数長 $2m$ の列に対し，
  $mathrmid, (1\ m{+}1)(2\ m{+}2)cdots(m\ 2m)$ から一様に 1 つを適用（前半/後半の入替）
- **PSS$_k$ (Pile–Scramble Shuffle)**：長さ n の列に対し，固定した $k \geq 2$ について**ラウンドロビン分配** → **山の連結** を行う操作．乱択として $\pi \in S_k$（山の連結順）と $\delta \in \{0,\dots,k{-}1\}$（配り始めのずらし）を一様に選ぶ．$t \in \{1,\dots,n\}$ に対し

  $$r(t)((t-1+\delta) \bmod k)+1, \qquad s(t)\left\lfloor \tfrac{t-1+\delta}{k} \right\rfloor + 1,$$

  また各山の大きさを $n_r\left\lceil \frac{n-r+1}{k} \right\rceil$（$r = 1,\dots,k$）とし，連結時の先頭までのオフセット $o_\pi(r)\sum_{r':\,\pi(r')<\pi(r)} n_{r'}$ を定める．このとき置換 $\sigma_{\pi,\delta} \in S_n$ を

  $$\sigma_{\pi,\delta}(t) \;=\; o_\pi\big(r(t)\big) \;+\; s(t)$$

  と定義し，PSS$_k$ は $\{\sigma_{\pi,\delta} : \pi \in S_k,\, \delta \in \{0,\dots,k-1\}\}$ から一様に 1 つを適用する操作とする（各山内の相対順は保持される）．
- **perm**：事前規定の固定置換（公開結果に基づく分岐を含む）
- **turn** S：位置集合 S を公開（表向き）し，必要に応じて伏せ戻す

2.2 非コミットメント型プロトコル

本稿はカードベースプロトコルのうち非コミットメント型のプロトコルを扱う．一般的なカードベース暗号では 1 ビット入力を 2 種類 2 枚のカードが用いられる．例えば，ユーザによる 1 ビット入力は以下の一般的なエンコーディングルールに従う：$\boxed{\clubsuit}\boxed{\heartsuit}= 0$, $\boxed{\heartsuit}\boxed{\clubsuit}= 1$.

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．

2.3 Six Card Trick

上記のように 2 色カード（$\boxed{\clubsuit}\boxed{\heartsuit}$）を用いた非コミットメント型プロトコルの例としては Five Card Trick [2] や Six Card Trick [4] [5] などがあるが，本稿では 6 カード 3 値入力 equality function（一致関数）を実現するカードプロトコルを説明する．Six-Card Trick は前処理である一般

置換とランダムカット（巡回置換）のみで構成されるシンプルな方式である．

一致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．

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．

ランダムカットとは 2 以上の整数 n に対する巡回置換を c_n としたとき，恒等置換 $id, c_n, c_n^2, \ldots c_n^{n-1}$ の n 通りから等確率で選択してカード束に処理する操作である．比較的操作が簡便なことからカードプロトコルにおいては多用されている．

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，

2.4 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 [16], [19], [20], [21], [22], [23], [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．

2.5 完全グラフ K_n のアクセス構造を持つカードプロトコルの具体的実装

具体的な実装に関しては $m-$ デッキ分割法で容易に実現可能であり，位数の小さいプロトコルとしては以下にように分類がなされている [29].

初期状態	距離分布	グラフ
♡♣♣♣	[0,1,1,1]	K_4
♡♣♣♣♣	[0,1,1,1,1]	K_5
♡♣♣♣♣♣	[0,1,1,1,1,1]	K_6
♡♣♣♣♣♣♣	[0,1,1,1,1,1,1]	K_7
♡♡♣♡♣♣♣	[0,2,2,2,2,2,2]	K_7
♡♣♣♣♣♣♣♣	[0,1,1,1,1,1,1,1]	K_8

ここで，異なる構成方法から完全グラフの構造が得られる例があることが分かる．

例えば，初期状態が $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}$のケースでは diffrence set の存在性から完全グラフ K_7 と同じ構造になることが指摘されている [27].

2.6 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の具体的実装

C_n のアクセス構造を持つカードプロトコル [27][28] は以下のように与えられる．

構成方式 1 (C_n のアクセス構造を持つカードプロトコル) 2 者間のカードプロトコルにおいて各ユーザに n 枚 2 種類のカード，そのうち$\boxed{\heartsuit}$ $\lfloor n/2 \rfloor$ 枚，$\boxed{\clubsuit}$を $n - \lfloor n/2 \rfloor$ 枚配布する．ここで $\lfloor n \rfloor$ は n を超えない最大の整数であることを示す

このとき左から $\boxed{\heartsuit}\ldots\boxed{\heartsuit}\boxed{\clubsuit}\ldots\boxed{\clubsuit}$として配布を行う．入力としてカードの左より 1 から n までインデックス付けし，入力は以下の n 通りとする．$\{1,2\},\{2,3\},\ldots,\{n-1,n\},\{1,n\}$

入力を行うユーザは自らランダムカットを行ったあと表面の n 枚を見ながら所望の入力になるまでカードをシフトする．i を入力する場合にはインデックス i と $i+1$ に $\boxed{\heartsuit}$が位置するように入力する．

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．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．具体的には $\boxed{\heartsuit}\boxed{\heartsuit}$となるデッキの個数を r とすると距離は $2-r$ が出力されることを意味する．∎

3. 異色カード導入を用いた m-デッキ分割法の効率化

m-デッキ分割法は十分軽いシャッフル方式であるが，今回異種カードを用いることで通常のランダムカットのみで実装できる方式について提案する．

3.1 起点：通常のトランプカード 1 セットで実現

まず C_n のアクセス構造を持つカードプロトコルが通常のトランプカード 1 セットで実現できる方式を起点として議論する．

構成方式 2 通常のトランプカード 1 セットを考える．4 スートあるうち例えば $\boxed{\heartsuit}$ と $\boxed{\clubsuit}$ の 2 種類の 1 から連番で n 枚のカードを使用することとする．ユーザ A は $\boxed{\heartsuit}_1$ から $\boxed{\heartsuit}_n$ の n 枚を持ち，ユーザ B は $\boxed{\clubsuit}_1$ から $\boxed{\clubsuit}_n$ の n 枚を持つ．このときカード束として連番で $1\ldots n$ の順番で整理された n 枚のカードが配布されるとする．

アクセス構造として 有向グラフとして n-gon グラフ（n 頂点サイクルグラフ） $C_n^{\rightarrow}$ が与えられ，各頂点には $1\ldots n$ の順番でインデックス付けされており，隣り合う頂点同士は $i \to i+1 \mod n$ という有向辺を持つこととする．各ユーザは，これまでの方式と同様に，ランダムカットだけの操作で所望の入力を行うものとし，グラフ頂点 i を入力したい場合にはカードを入力した際に最も上にあるカードが i となるようにランダムカットを行う．

次にユーザ A とユーザ B の入力カードを 1 枚ずつ交互に重ね合わせ，$2n$ 枚のカード束を作る．これをユーザのどちらかがランダムカットを行う．先頭のカードをめくりこれが $\boxed{\heartsuit}$ であればユーザ A の入力であることがわかり，次のカード $\boxed{\clubsuit}$ もめくる．もし先頭カードが $\boxed{\clubsuit}$ の場合には，最下位のカードは $\boxed{\heartsuit}$であり，このカードを 2 枚目としてめくる．

このようにして得られたカードの数字の差，例えば$\boxed{\heartsuit}_s$ と $\boxed{\clubsuit}_t$ が開示カードであれば $t-s \mod n$ がちょうど有向グラフ上での距離となっており，これを出力としてプロトコルを終了する．もちろん$\boxed{\heartsuit}_s$ と $\boxed{\clubsuit}_t$ と同じ数字のカードが得られた場合には，距離は 0 であり 2 ユーザの入力が一致したことを示している．

このプロトコルの大きなメリットは，1 回のランダムカットと 2 枚のカード開示のみで実行可能な簡便性を持つことである．また，残りのカードを仮に第 3 者などにより公開されたとしても，2 者間の距離 $t-s \mod n$ 以外の情報が漏れることはなく安全なカードプロトコルであることも既存方式に比べ有利な点である．

3.2 基本アイデア：異種カードの利用

前節の有向グラフに対する事例をもとに，2 種類の異種カードを利用した実現方法を考える．ユーザ A 用のカードか，ユーザ B 用カードかが背面からでも分かることを前提とする．例えば色が違うなどが考えられるが，トランプと UNO などの異色カードを利用することもできる．

これらの異種カードはトランプカードや UNO など $1,\ldots,n$ とそれぞれ n 枚のカードがナンバリングされているものとする．もちろんナンバリングのためのエンコーディングルールが決定していれば，必ずしも数字で記載されたカードを利用する必要はなく，各カードに番号がバインドしていればよい．

以下，異種カードに関する事項を列挙する．

- **定義**：背面模様や形状が明確に区別できるカード（*Delimiter*）を混在させる．
- **役割**：**位置合わせ**（セグメント境界のマーキング）に限定して利用し，**有意情報は載せない**.
- **効果の直観的解釈**：**局所** RC を繰り返す構成により，従来 RBC による「前半/後半入替」の効果を，**巡回**

シフトの組合せで代替可能にする（n=2 では RC ≡ RBC）.

3.3 効率化 A

既存の効率化手法を効率化 A 方式 [33] と呼ぶこととする，以下が効率化 A 方式のプロトコルである.

構成方式 3 (有向グラフ $C_n^{\rightarrow}$ のアクセス構造を持つ方式)

[STEP 1] 初期状態に設定されたカード束（n 枚）の配布を行い．それぞれのユーザはランダムカットを行って所望の入力を行う.

[STEP 2] ユーザ A の入力をユーザ B の入力を交互に 1 枚ずつ重ねていく.

$\Psi_A := (a_1, a_2, \ldots, a_n)$, $\Psi_B := (b_1, b_2, \ldots, b_n)$

$\Psi := (a_1, b_1, a_2, b_2 \ldots, a_n, b_n)$

[STEP 3] 2 つの入力から生成された新しいカード列 Ψ をランダムカットし，最上位カードがユーザ B であればさらに 1 回シフトしてユーザ A カードが最上位になるように配置する．最上位から 2 枚のカードを $\{a_s, b_t\}$ とする．$\{a_s, b_t\}$ を開示する.

[STEP 4] 2 者間の距離 $t - s \mod n$ を出力として確定する．距離 0 の場合は 2 者の入力が一致したことを示す.

本プロトコルにおいて，ランダムカットを行い先頭に移動された 2 枚のカードはデッキ分割法におけるひとつのデッキを開示していることを意味する．この開示により，出力として有向グラフの 2 点間の距離が算出できるが，入力情報に関する一切は漏れていない，つまり $1/n$ の確率で等しく分散されることに留意する.

3.3.1 構成方式 3 の例

2 色（例えば赤と黒）の裏面を持つトランプカードを利用することを考える．この例では $n = 7$，つまり各ユーザが 7 枚ずつ入力に利用した場合，$\boxed{\heartsuit}_5 (s = 5)$ $\boxed{\clubsuit}_3$ (t=3) が開示カードであるため $t - s \mod n = 3 - 5 \mod 7 = 5$ がちょうど有向グラフ上での距離となっており，これを出力としてプロトコルを終了する.

構成方式 3 は有向グラフ上での距離を算出するプロトコルであった．実利用時には様々なアプリケーションが考えられるが，例えば $n = 12$ とした場合には，誕生年の「干支」の違いや，色相環配色から好きな色を選択してマッチングを行うなどの実例が考えられる．このとき，1 歳差や 1 色違いにも関わらず（有向グラフ上での）距離 11 と算出されてしまうため 2 者間の関係がお互いに知られてしまうリスクがある．そのため無向グラフではなく有向グラフ上での距離が知りたいケースが発生する．このようなケースでは構成方式 3 ではなく，構成方式 1 を利用すればよく，それぞれのアクセス構造に適したアプリケーションに応じて構成方式を選択すればよい点に注意する.

4. 新しいアプリケーションと提案方式

4.1 効率化 B

効率化 A 方式ではトランプカードなど数字が記載されており，1 ユーザに配布されたカードデッキで同じカードを含まないことを前提に効率化されていた．そこで，ここでは 2 色カードの利用に立ち返り，効率化を検討する．具体的には，2 種類のスート $\boxed{\heartsuit}\boxed{\clubsuit}$ だけで構成される入力パターンについて，「RC のみを実行することで所望の入力値を表現する方式」を取り上げる（第 1 章で具体的事例を提示済）.

ここでは初期状態から RC のみ用いて所望のカード状態に移動させることから n パターンの入力が考えられる．また RC を行うことから，処理後のカード列からは入力を推測することはできない（$1/n$ の確率で一様に分配される）．この性質を用いることにより，構成方式 3 と同様に STEP2 でユーザ同士の入力を重ね合わせたあと全体を RC することで，片方，例えばユーザ A の RC 後の状態は開示可能である．このときユーザ A の状態に呼応したユーザ B のカードの一部を開示することで 2 ユーザの入力を秘匿したまま入力の関係だけを開示することができる.

この方針により，以下の新しいプロトコルと構成できる.

構成方式 4 (メンバーシップ判定) ユーザ A は $\boxed{\heartsuit}$ k 枚，$\boxed{\clubsuit}$ $v-k$ 枚のカードを，ユーザ B は $\boxed{\heartsuit}$ 1 枚，$\boxed{\clubsuit}$ $v-1$ 枚のカードを配布されているとする.

v 点集合 V の k 個部分集合全体から X をユーザ A の入力とし，ユーザ B が $x \in V$ を選ぶとき，$x \in X$ を満たすかどうかのメンバーシップ判定カードプロトコルを構成することができる.

[STEP 1] 初期状態に設定されたカード束（v 枚）の配布を行い．それぞれのユーザは所望の入力を行う．ここで RC に制限されていない点に注意する．バリエーションとしてはユーザ A は ${}_nC_k$ 通り，ユーザ B は v 通りの入力がある.

[STEP 2] ユーザ A の入力をユーザ B の入力を交互に 1 枚ずつ重ねていく.

$\Psi_A := (a_1, a_2, \ldots, a_v)$, $\Psi_B := (b_1, b_2, \ldots, b_v)$

$\Psi := (a_1, b_1, a_2, b_2 \ldots, a_v, b_v)$

[STEP 3] 2 つの入力から生成された新しいカード列 Ψ をランダムカットし，最上位カードがユーザ B であればさらに 1 回シフトしてユーザ A カードが最上位になるように配置する.

[STEP 4] ユーザ B のカードを全開示する．ユーザ B の $\boxed{\heartsuit}$ に呼応するユーザ A のカードを開示する．もしこのカードが $\boxed{\heartsuit}$ であれば $x \in X$ である（メンバーに属する）ことを意味する．もし当該カードが $\boxed{\clubsuit}$ であれば $x \notin X$ であることを意味する.

5. 従来技術との関係

5.1 RBC を RC に置き換える方式

区切りを示すデリミタカードとして既存方式にそのまま適用することで RBC（ランダム二等分割カット）を RC（ランダムカット）で置換できる事例を紹介する．これにより，RBC の実装が難しい媒体（例：麻雀牌）でも適用可能なプロトコルの幅が広がる．

2 色カード 4 枚 XOR 演算プロトコル [3] は，入力 a, b の各コミットのみで，RBC と固定 perm および turn で構成できるシンプルなプロトコルである．

- (1) 初期：$[a][b]$ を 4 枚列で配置．
- (2) perm で列を A_1, B_1, A_2, B_2 形へ．
- (3) RBC：前半 2 枚/後半 2 枚の入替（乱択ビット r を注入することを意味する）．
- (4) ペアを取り直しと turn を組合せ，片側の公開で r を打ち消し，他方を $a \oplus b$ のコミットとして残す．

有限回で XOR を達成することは明らかであり，RBC の使用により，補助カード不要・カード数も最小で構成できる．

このとき，たとえば $[a]$ をデリミタカードとし，裏面だけで認識できるようにすることを考える．手順 (3)' として上記プロトコルでの手順 (2) の状態で 4 枚を RC を施す．このときデリミタカードを認識することで 0 回もしくは 1 回だけシフト処理を行う．このとき，$[a][b]$ か $[b][a]$ の状態のどちらかであるようにすることができ，これは元プロトコルの手順 (3) の最終状態と変わらないこととなる．このようにして BRC ではなく RC だけで XOR 演算を行うことができる．

なお，デリミタカードを導入せずとも XOR 演算においては RC だけで実行可能な方式が提案されている点に留意されたい．

5.2 デリミタカードと酷似したカード導入事例

Ueda らは dummy cards と呼ばれる概念を導入し，これをデリミタカードとして，本稿と同じく RBC を RC のみで実装できることを示している．実例として Mizuki-Sone 6 枚 AND 演算プロトコルへ適用しているが，デリミタカード入力を「値入力」としては活用せず，あくまでダミーカードとして挿入することを想定している [6].

Miyahara らは，裏面の異なるもう一つのカードデッキを準備 [7]，Koch らは位置合わせのためだけに利用しているだけではあるが”the helping deck”とやはりカードデッキを準備するアイデア [9] を提示している．

さらに Ueda らは RBC する際に入力カードの頭のカードを上下入れ替えすればよいことを指摘し，同じ裏面のカードをデリミタカードの役割として持たせ，Mizuki-Sone 6 枚 AND 演算プロトコルへ適用している [8].

6. 本論文の貢献と今後の課題

区切りを示すデリミタカードとして異なる裏面を持つように異種カードを導入することにより，メンバーシップ判定カードプロトコルを構成した．このとき，旧来のデッキ分割法でも実装可能であるが，より効率的な具体的には RC のみを用いた方式を提案した．今後，メンバーシップ判定以外のアプリケーションの創出や，非コミットメント型のプロトコルへの適用などを検討する．

謝辞 本研究は九州大学マス・フォア・インダストリ研究所 共同利用・共同研究拠点の支援を受けた．（2025 年度短期共同研究「産学連携と数理・暗号分野連携によるカードベース暗号の深化と新境地 II」（2025a036））

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] B. den Boer, More efficient match-making and satisfiability: the five card trick, EUROCRYPT'89, pp.208-217, 1989.

[3] T. Mizuki and H. Sone, Six-card secure AND and four-card secure XOR, International Workshop on Frontiers in Algorithmics, pp.358-369, 2009.

[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] I. Ueda, A. Nishimura, Y. Hayashi, T. Mizuki and H. Sone, How to implement a random bisection cut, The 5th International Conference on Theory and Practice of Natural Computing (TPNC2016), pp.58-69, 2016.

[7] Miyahara et al., Practical Card-Based Implementations of Yao's Millionaire Protocol, Theoretical Computer Science 803, 2020.

[8] Ueda et.al, Secure Implementations of a Random Bisection Cut, International Journal of Information Security 19(4), 2020.

[9] Koch, Walzer, Foundations for Actively Secure Card-Based Cryptography, FUN2021.

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

[11] A.E. Brouwer J. Koolen, The Distance-Regular Graphs of Valency Four, Journal of Algebraic Combinatorics 10(1):5-24, 1999.

[12] E. R. van Dam, M. Jazaeri. Distance-regular Cayley graphs with small valency, Ars Mathematica Contemporanea 17(1), pp.203-222, 2019.

[13] A. Marcedone, Z. Wen, E. Shi, Secure Dating with Four or Fewer Cards, IACR eprint 2015/1031, https://eprint.iacr.org/2015/1031

[14] Anastasiia Doi, Tomoki Ono, Yoshiki Abe, Takeshi Nakai, Kazumasa Shinagawa, Yohei Watanabe, Koji Nuida, Mitsugu Iwamoto, Card-Based Protocols for Private Set Intersection and Union. New Gener. Comput.

42, pp.359–380, 2024.
[15] 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.
[16] 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.
[17] Y. Suga, A classification proof for commutative three-element semigroups with local AND structure and its application to card-based protocols, IEEE International Conference on Consumer Electronics, 2022 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW, pp.171-172, 2022.
[18] Y. Suga, How to implement non-committed card protocols to realize AND operations satisfying the three-valued logics, 2022 Tenth International Symposium on Computing and Networking Workshops (CANDARW), 2022.
[19] 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.
[20] 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.
[21] 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.
[22] 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.
[23] 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.
[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，与えられたグラフでアクセス構造を表現する 2 種スートカードプロトコルにおける 1 ユーザの配布枚数が 8 枚までの完全分類, 情報処理学会研究報告 Vol.2023-CSEC-104, 2024.
[29] 須賀，3 パターン出力のグラフアクセス構造を表現する 2 種スートカードプロトコル, 情報処理学会研究報告 Vol.2024-CSEC-106, 2024.
[30] 須賀, 正則グラフから導出される 2 者間非コミットメントカードプロトコルの分類における巡回同型性の導入, 第 47 回情報理論とその応用シンポジウム (SITA2024), 1-2-3, 2024.
[31] 須賀, ババ抜きランダムカットを用いたデッキ分割法の効率的実装, 4D2-5, SCIS2025, 2025.
[32] 須賀, カード入力を制限する 2 者間非コミットメントカードプロトコルにおける巡回同型導入とその周辺, 信学技報, vol.124, no.397, ISEC2024-127, pp.254-260, 2025.
[33] 須賀, 有向グラフにおける距離を出力する 2 者間カードプロトコル, マルチメディア，分散協調とモバイルシンポジウム 2025(DOCOMO2025), pp.1427-1432, 2025.