Computer Security Symposium 2023
30 October - 2 November 2023

部分開示操作を用いた効率的なカードベースプロトコル

本多 由昂[1,a)]　品川 和雅[1,2]

概要：カードベースプロトコルとは、物理的なカード組を用いて秘密計算を行う暗号プロトコルである。本論文ではカードベースプロトコルのうち、一般に市販されているトランプカードを用いるものを扱う。トランプカードを用いた有限時間コミット型プロトコルについては、2016 年に Mizuki によって提案されたランダム二等分割カット 4 回の 8 枚 AND プロトコルとランダム二等分割カット 1 回の 4 枚 XOR プロトコルが存在する。本論文では、部分開示操作を用いて、ランダムカット 3 回の 4 枚 AND プロトコルとランダムカット 2 回の 4 枚 XOR プロトコルを提案する。部分開示操作とは、Miyahara と Mizuki によって提案された、カードの数字を開示せずにスートのみを開示する操作のことであり、本論文ではそれを一般化したものを使用している。提案プロトコルは、最も実装が容易であると考えられているランダムカットのみを用いており、さらにカード枚数も最小枚数であるという特徴がある。

キーワード：カードベース暗号、トランプカード、部分開示操作、ランダムカット、有限時間コミット型プロトコル

Efficient Card-based Protocols Using Partial-Open Actions

Yoshiaki Honda[1,a)]　Kazumasa Shinagawa[1,2]

Abstract: A card-based protocol is a cryptographic protocol that uses a deck of physical cards for secure computation. This paper deals with card-based protocols that use commercially available playing cards. For finite-runtime committed-format protocols using playing cards, there exist an eight-card AND protocol with four random bisection cuts and a four-card XOR protocol with one random bisection cut proposed by Mizuki in 2016. In this paper, we propose a four-card AND protocol with three random cuts and a four-card XOR protocol with two random cuts using partial-open actions. A partial-open action is a generalized version of the half-open action proposed by Miyahara and Mizuki, which reveals only suits without revealing numbers. The proposed protocols use only random cuts, which are considered the easiest to implement among all shuffles, and also has the property of using the minimum number of cards.

Keywords: Card-based cryptography, Playing cards, Partial-open actions, Random Cuts, Finite-runtime committed-format protocols

1. はじめに

1.1 背景

入力値を秘匿したまま出力のみを得る計算を秘密計算と呼ぶ。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行う暗号プロトコルである。カードベース暗号で主に用いられるカードは、表面が $\boxed{\clubsuit}$ と $\boxed{\heartsuit}$ であり、裏面がすべて $\boxed{?}$ である二色カードと呼ばれるものである。2 枚の二色カード $\boxed{\clubsuit}\boxed{\heartsuit}$ を用いて、1 ビットの情報は

$$\boxed{\clubsuit}\boxed{\heartsuit} = 0, \quad \boxed{\heartsuit}\boxed{\clubsuit} = 1$$

と表現される。1 ビットの情報を保持する裏向きに伏せられた 2 枚のカード組をコミットメントと呼ぶ。

カードベースプロトコルの実行結果の出力方法には、出力値のコミットメントを出力するものと、出力結果自体を

[1] 茨城大学
Ibaraki University
[2] 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology
[a)] 20t4068h@vc.ibaraki.ac.jp

図 1 カード (左) とカバー (右)

図 2 スートの開示

公開するものがある。前者をコミット型プロトコル、後者を非コミット型プロトコルと呼ぶ。コミット型プロトコルは、出力結果を別のプロトコルの入力として使うことができるため、プロトコル同士の結合が可能である。一方、非コミット型プロトコルはプロトコル同士の結合が一般にはできないため、コミット型プロトコルの方が望ましい。

カードベースプロトコルの中には、市販のトランプカードを用いるものがある。トランプカードは、13 種類の数字と 4 種類のスート (♣, ♠, ♡, ♢) の組み合わせから成る 52 枚のカードとジョーカーのカードから構成される。トランプカードは容易に手に入れることができるため、二色カードのプロトコルよりもトランプカードのプロトコルの方が実利用に適していると考えられている。

Miyahara と Mizuki [3] はトランプカードに対してスートだけを開示する操作（部分開示操作）を提案した。部分開示操作の実装方法の一つとしては、カバー（穴の空いた紙）を用いるものがある。例えば、ハートのエースに対して部分開示操作を行う場合、図 1 のようにカバー（図 1 ではジョーカーのカードに穴を空けたもの）を用意し、図 2 のように被せることで、スートのみを開示できる。

トランプカードのプロトコルでは、すべてのカードは互いに異なるため、2 色カードのプロトコルと比べてカードの情報の秘匿が難しい。そのため、既存のトランプカードのプロトコルでは、2 色カードのものと比べて、カード枚数とシャッフル回数が多い傾向がある。しかし、Miyahara と Mizuki [3] の部分開示操作によって、トランプカードを用いて二色カードのプロトコルを実装することが可能となった。そのため、部分開示操作を用いる設定においては、2 色カードのプロトコルと比べて少なくとも同等以上の効率性を有するトランプカードのプロトコルを構成できる。

1.2 本論文の貢献

Miyahara と Mizuki [3] の部分開示は、トランプカードの左上または右下に位置するスートのみを開示する操作である。本論文では、部分開示操作を開示位置について一般化した操作（これも部分開示操作と呼ぶ）を提案し、部分開示を用いたコミット型 AND プロトコルとコミット型 XOR プロトコルを提案する（表 1）。提案 AND プロトコルは、カード枚数が 4 枚であり、シャッフルはランダムカット 3 回を用いる有限時間プロトコルである。カード枚数については、入力コミットメントの他に追加カードを用いないため、最小枚数である。シャッフル回数については、既存のコミット型 AND プロトコルの中で最も少ない。提案 XOR プロトコルは、カード枚数が 4 枚であり、シャッフルはランダムカット 2 回を用いる有限時間プロトコルである。カード枚数については、追加カードを用いないため、最小枚数である。シャッフル回数については、ランダムカットのみを用いる既存のコミット型 XOR プロトコルの中で最も少ない。特筆すべき点として、ランダムカットのみを用いる設定では、既存のコミット型 AND/XOR プロトコルは Las Vegas プロトコル（シャッフル回数が有限回とは限らないが、期待値は有限回であるようなプロトコル）しか存在しなかったため、提案プロトコルはこの設定において初めて有限時間プロトコルを達成している。なお、2 色カードを用いる設定については、Koch–Walzer–Härtel [2] は有限時間のコミット型 4 枚 AND プロトコルが構成不可能であることを示しており、本成果は 2 色カードの設定では達成不可能なプロトコルが、トランプカードと部分開示を用いると達成可能になることを示している。

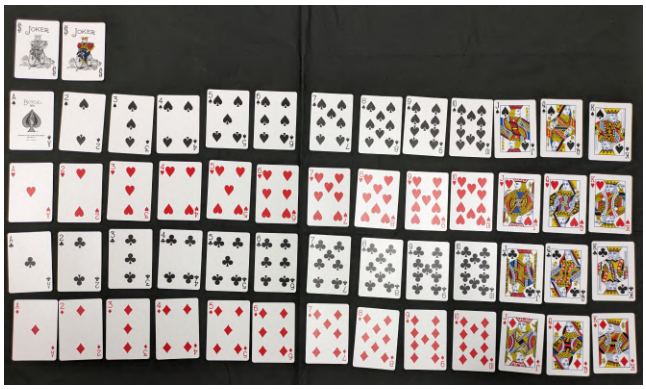


図 3 バイスクルカード

2. 準備

本節では、基本的な用語の定義を行い、既存の AND プロトコルと XOR プロトコルの紹介をする。

2.1 カード

本論文で使用するトランプカードを紹介する。本論文では U.S プレイング・カード社のバイスクルを使用する。バイスクルの表面を図 3 に、裏面を図 4 に示す。 カードの裏面は全て同じ柄であり、区別は出来ないものとする。本論文では、一つのプロトコル中では同一スートの A から 10 のカードを用いることにし、それらのカードの表面を $\boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}\boxed{7}\boxed{8}\boxed{9}\boxed{10}$ と表し、裏面を $\boxed{?}$ と表す。

なお、本論文では U.S プレイング・カード社のバイスクルを使用するが、同社の代表的なトランプカードにはバイスクルの他にビーやタリホーが挙げられる。これらのカー

表 1 既存プロトコルと提案プロトコルの比較

	カード枚数	有限時間	合計シャッフル回数	シャッフルの種類
○ コミット型 AND プロトコル				
Niemi–Renvall [5]	5		9.5(exp.)	ランダムカット
Mizuki [4]	8	✓	4	ランダム二等分割カット
Koch ら [1]	4		6(exp.)	ランダムカット
提案 AND	4	✓	3	ランダムカット
○ コミット型 XOR プロトコル				
Niemi–Renvall [5]	4		7(exp.)	ランダムカット
Mizuki [4]	4	✓	1	ランダム二等分割カット
提案 XOR	4	✓	2	ランダムカット
○ コミット型 COPY プロトコル				
Niemi–Renvall [5]	6		5.5(exp.)	ランダムカット
Mizuki [4]	6	✓	1	ランダム二等分割カット
○ 非コミット型 AND プロトコル				
Miyahara–Mizuki [3]	4	✓	1	ランダムカット

図 4 バイスクルカードの裏面

ドのデザインの違いは、カードの裏面とジョーカーとスペードの $\boxed{1}$ のデザインのみであるため、本論文で紹介するカードベースプロトコルはどのカードを使用しても同様のプロトコルを構成することができる。

2.2 コミットメント

コミットメントとは、1 ビットの情報を保持する裏向きにした 2 枚のカード組のことである。コミットメントを構成する 2 枚のカード $\boxed{i}\boxed{j}$ について、$1 \le i < j \le 10$ のとき、保持するビットを以下の通りであるとする。

$$\boxed{i}\boxed{j} = 0,\ \boxed{j}\boxed{i} = 1$$

このとき、ビット $x \in \{0,1\}$ のコミットメントを以下のように表す。

$$\underbrace{\boxed{?}\boxed{?}}_{[x]^{\{i,j\}}}$$

2.3 ランダムカット

ランダムカットとは、カード列に対してランダムに巡回的な並び替えを行うシャッフル操作のことである。

例えば、$\boxed{1}\boxed{2}\boxed{3}\boxed{4}$ を裏向きに伏せたカード列に対してランダムカットを適用すると、以下の 4 種類のカード列（を裏向きに伏せたもの）のいずれかが得られる。

$$\boxed{1}\boxed{2}\boxed{3}\boxed{4},\ \boxed{2}\boxed{3}\boxed{4}\boxed{1},\ \boxed{3}\boxed{4}\boxed{1}\boxed{2},\ \boxed{4}\boxed{1}\boxed{2}\boxed{3}$$

このとき、それぞれのカード列に遷移する確率は全て等しく、上の例の場合それぞれ 1/4 の確率で遷移する。ランダムカットの適用を以下のように表記する。

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle$$

2.4 Koch らの AND プロトコル

Koch–Schrempp–Kirsten [1] は 4 枚のトランプカードを用いる Las Vegas の AND プロトコルを提案した。用いるシャッフルはランダムカットのみであり、シャッフル回数の期待値は 6 回である。このプロトコルのアイデアは表 2 の通りである。プロトコルの手順を以下に示す。ただし、Koch らの AND プロトコルはシャッフル回数を少なくするために、非常に複雑な手順で構成されている。そのため、ここで紹介する手順は Koch らのプロトコルを単純化したものである。よって、本来のプロトコルのシャッフル回数の期待値が 6 回であるのに対して、以下に示すプロトコルのシャッフル回数の期待値は 11 回である。

(1) 以下のように並べる。

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{1,2\}}}\ \underbrace{\boxed{?}\boxed{?}}_{[b]^{\{3,4\}}}$$

(2) ランダムカットを適用する。

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle$$

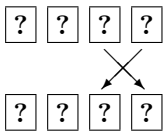
(3) ランダムカットを利用して $\boxed{1}$ を特定し、$\boxed{1}$ が先頭になるように巡回的に並び替える。

$$\boxed{?}\boxed{?}\boxed{?}\boxed{?} \rightarrow \boxed{1}\boxed{?}\boxed{?}\boxed{?}$$

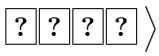
(4) 右側二枚を入れ替える。

表 2 Koch らの AND プロトコルのアイデア

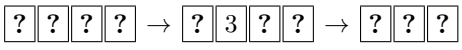
	入力	1 を先頭	右 2 枚の交換	3 を除去	4 を先頭
(0,0)	1234	1234	1243	124	412
(0,1)	1243	1243	1234	124	412
(1,0)	2134	1342	1324	124	412
(1,1)	2143	1432	1423	142	421



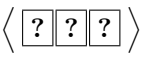
(5) ランダムカットを適用する。



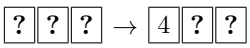
(6) ランダムカットを利用して 3 を特定して除去する。



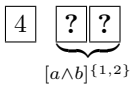
(7) ランダムカットを適用する。



(8) ランダムカットを利用して 4 を特定して、4 が先頭になるように巡回的に並び替えて右二枚を出力する。



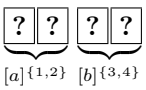
(9) 右二枚を出力する。



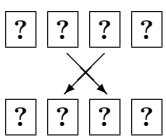
2.5 Niemi-Renvall の XOR プロトコル

Niemi-Renvall [5] は 4 枚のトランプカードを用いる Las Vegas の XOR プロトコルを提案した。用いるシャッフルはランダムカットのみであり、シャッフル回数の期待値は 7 回である。プロトコルのアイデアは表 3 の通りである。プロトコルの手順は以下の通りである。

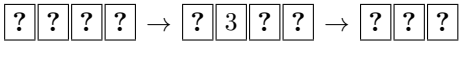
(1) 以下のように並べる。



(2) 中央二枚を入れ替える。



(3) ランダムカットを利用して 3 を特定して除去する。

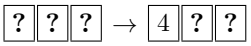


(4) ランダムカットを利用して 4 を特定して、4 が先頭

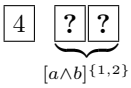
表 3 Niemi-Renvall の XOR プロトコルのアイデア

	入力	中央 2 枚の交換	3 を除去	1 を先頭
(0,0)	1234	1324	124	124
(0,1)	1243	1423	142	142
(1,0)	2134	2314	214	142
(1,1)	2143	2413	241	124

になるように巡回的に並び替えて右二枚を出力する。



(5) 右二枚を出力する。



3. 部分開示操作

3.1 部分開示操作

部分開示操作とは、カードの表面をすべて開示するのではなく、カードの表面の一部のみを開示する操作である。部分開示操作を初めてカードベース暗号に正式に導入したのは Miyahara と Mizuki [3] であり、彼らはトランプカードに対して（数字は秘匿したまま）スートだけを開示する操作（以降、**半開示操作**と呼ぶ）を用いた。本稿では Miyahara と Mizuki の半開示操作を一般化し、カードの任意の部分についての部分開示操作を考える。

一般的なトランプカードの 1 から 10 の表面は、左上と右下に小さくスートと数字が書いてあり、それらよりも内側に数字に対応する数だけスートが並べてある。スートの並び方には決まりがあり、数字が違っていても同じ位置にスートがある組み合わせがある。例えば、カードの中央を見ると 1 3 5 9 のカードはスートがあるが、その他の 2 4 6 7 8 10 には何も無い。つまり、カードの中央を部分開示すると、そのカードが 1 3 5 9 ならスートが見えるが、それ以外なら何も見えない。ただし、スペードの 1 は、他のスートとデザインが大きく違うため、他のカードと同様に使用することは難しい。

3.2 実装方法

部分開示操作の手順は次の通りである。まず、開示したい位置に穴の空いた紙（カバー）を用意する。（例えば、図 5 のように穴を開けたカードをカバーとして用いることができる。）次に部分開示操作を行うカードの下に、カバーを挿入する (図 6)。そして、部分開示操作を行うカードとカバーを合わせ、2 枚まとめて持ち上げる (図 7)。最後に、持ち上げた 2 枚をまとめたまま裏返す (図 8)。図 8 の場合、穴から赤い色が確認できるため、その位置にスートがあることが分かる。

3.3 開示位置と開示結果の関係

部分開示操作における開示位置と開示結果の関係につい

図 5 穴の空いた紙（カバー）

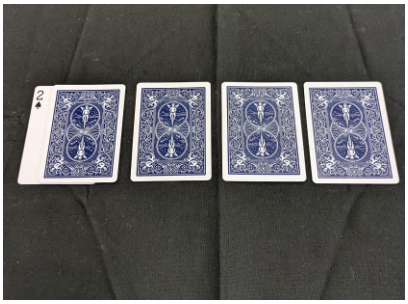


図 6 カバーを下から挿入

図 7 カバーとカードの持ち上げ

図 8 カバーとカードの裏返し

表 4 各カードの開示位置と開示結果の関係

	1	2	3	4	5	6	7	8	9	10
ウ				○	○	○	○	○	○	○
エ									○	○
オ						○	○	○		
カ		○	○							
キ										○
ク							○	○		
ケ	○		○		○				○	
コ								○		

て説明する。トランプカード上のスートおよび数字の位置を図 9 に示す。ただし、図 9 はそれぞれ異なる部分開示結果をもたらす開示位置のみ表示しており、これらと同等の部分開示結果をもたらす開示位置は省略している。

図 9 の各位置の説明をする。長方形 (ア) はトランプカードの数字が描かれている位置である。長方形 (イ) はトランプカードのスートが描かれている位置である。Miyahara と Mizuki [3] の半開示操作は (イ) を開示するものである。楕円 (ウ) から (コ) は 1 から 10 のいずれかのスートが描かれている位置である。楕円 (ウ) から (コ) の位置について、1 から 10 にそれぞれスートが描かれているかどうかは、表 4 の通りである。表 4 において、○はその位置にスートが描かれていることを意味し、空白はスートが描かれていないことを意味する。例えば、楕円 (オ) の位置（左側の中央の位置）にスートが描かれているカードは 6 7 8 であり、それ以外のカードにはスートは描かれていない。

4. 提案プロトコル

4.1 特定プロトコル

特定プロトコルとは特定のカードの位置のみを明らかにするプロトコルである。今回使用する特定プロトコルは特定プロトコル A、特定プロトコル B、特定プロトコル C の三つである。以下、それぞれのプロトコルを説明する。

特定プロトコル A は 2 4 5 6 から構成される裏向きに伏せられたカード列の中から 2 の位置を特定するプロトコルである。プロトコルの手順は以下の通りである。

(1) カード列の一番左のカードについて注目する。
(2) そのカードに対して図 9 の (カ) の部分を開けたカバーを被せて部分開示操作を適用する。
(3) 図 10 のように穴からスートが確認できればそのカードが 2 であり、特定は完了する。何も見えなければ、そのカードを裏向きにして元の位置に戻し、右隣のカードに注目して手順 (2) に戻る。

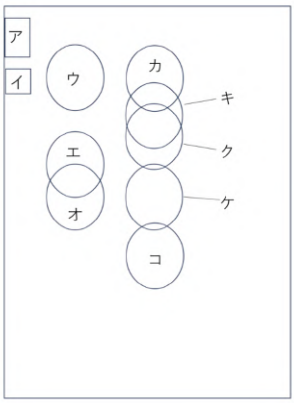


図 9 スートと数字の位置

表 4 から、図 9 の (カ) の部分開示操作を行ったときにスートが確認できるカードは 2 と 3 であり、特に 2 4 5 6 の中では 2 のみである。したがって、上記のプロトコルは 2 を特定し、その他の情報は一切漏らさない。

特定プロトコル B は 2 4 5 6 から構成される裏向きに伏せられたカード列の中から 5 の位置を特定するプロトコルである。具体的な手順は特定プロトコル A とほぼ同様であり、変更点は開示位置を図 9 の (ケ) にするだけである。表 4 から、図 9 の (ケ) の部分開示操作を行ったときにスートが確認できるカードは 1 3 5 9 であり、特に 2 4 5 6 の中では 5 のみである。したがって、このプロトコルは 5 を特定し、その他の情報は一切漏らさない。

特定プロトコル C は 2 4 6 から構成される裏向きに伏せられたカード列の中から 6 の位置を特定するプロトコルである。具体的な手順は特定プロトコル A とほぼ同様であり、変更点は開示位置を図 9 の (オ) にするだけである。表 4 から、図 9 の (オ) の部分開示操作を行ったときにスートが確認できるカードは 6 7 8 であり、特に 2 4 6 の中では 6 のみである。したがって、このプロトコルは 6 を特定し、その他の情報は一切漏らさない。

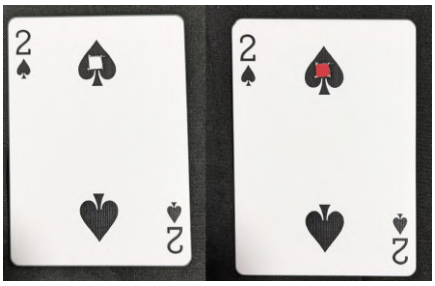


図 10 特定プロトコル A

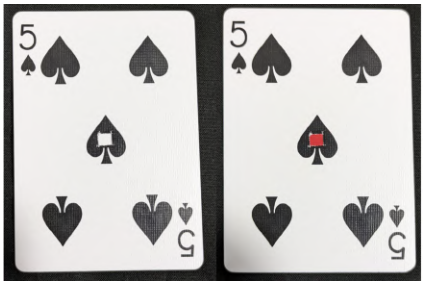


図 11 特定プロトコル B

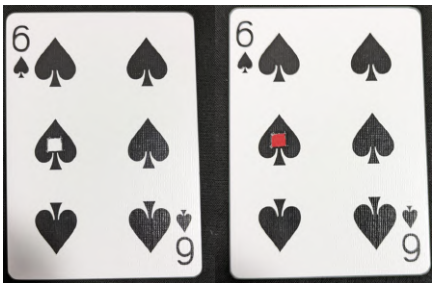


図 12 特定プロトコル C

表 5 提案 AND プロトコルのアイデア

	入力	2 を先頭	右 2 枚の交換	5 を除去	6 を先頭
(0,0)	2456	2456	2465	246	624
(0,1)	2465	2465	2456	246	624
(1,0)	4256	2564	2546	246	624
(1,1)	4265	2654	2645	264	642

4.2 4 枚有限コミット型 AND

本節では、カード 4 枚とランダムカット 3 回を用いる有限時間コミット型 AND プロトコルを提案する。このプロトコルは、Koch らの AND プロトコルを単純化したプロトコル（2.4 節）と、部分開示操作による特定プロトコル（4.1 節）を組み合わせることによって構成されている。提案プロトコルのアイデアを表 5 に示す。プロトコルの手順は以下の通りである。

(1) カード列を以下のように並べる。

$$\underbrace{[?][?]}_{[a]^{\{2,4\}}}\ \underbrace{[?][?]}_{[b]^{\{5,6\}}}$$

(2) ランダムカットを適用する。

$$\langle [?][?][?][?] \rangle$$

(3) 特定プロトコル A により $[2]$ を特定し、$[2]$ が先頭になるように巡回的に並び替える。

$$[?][?][?][?] \to [?][?][2][?] \to [2][?][?][?]$$

(4) 右側二枚を入れ替える。

$$\begin{array}{cccc} [?] & [?] & [?] & [?] \\ & & \searrow\!\!\times\!\!\swarrow & \\ [?] & [?] & [?] & [?] \end{array}$$

(5) ランダムカットを適用する。

$$\langle [?][?][?][?] \rangle$$

(6) 特定プロトコル B により $[5]$ を特定し、$[5]$ を除去する。

$$[?][?][?][?] \to [?][5][?][?] \to [?][?][?]$$

(7) ランダムカットを適用する。

$$\langle [?][?][?] \rangle$$

(8) 特定プロトコル C により $[6]$ を特定し、$[6]$ が先頭になるように巡回的に並び替える。

$$[?][?][?] \to [?][?][6] \to [6][?][?]$$

(9) 右二枚を出力する。

$$[6]\ \underbrace{[?][?]}_{[a\wedge b]^{\{2,4\}}}$$

正当性 提案プロトコルの手順は表 5 のアイディアの通りであることに注意する。すなわち、初期カード列に対して、まず $[2]$ が先頭になるようにし、右側の二枚のカードを入れ替え、$[5]$ を除去し、$[6]$ が先頭になるようにしている。表 5 のように、最終的なカード列は、入力が $(1,1)$ のときに限り $[6][4][2]$ と並び、それ以外のときは $[6][2][4]$ と並ぶため、出力コミットメントは $[a \wedge b]^{\{2,4\}}$ と一致する。よって、正当性が成り立つ。

安全性 提案プロトコルにおいてカードの情報が開示されるのは、ステップ (3)(6)(8) における特定プロトコルの部分開示のみである。ステップ (3) の特定プロトコル A については、$[2]$ のみスートが見えて、それ以外のカードについてはスートが見えないため、この際に開示される情報は $[2]$ のカードの位置のみである。同様に、ステップ (6) と (8) の特定プロトコルについても、開示される情報は $[5]$ の位置と $[6]$ の位置のみである。これらのカードの位置情報は、直前のランダムカットによって一様ランダムに選ばれるため、入力情報 (a,b) とは独立である。よって、安全性が成り立つ。

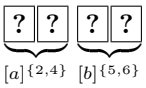
4.3 4 枚有限コミット型 XOR

本節では、カード 4 枚とランダムカット 2 回を用いる有限時間コミット型 XOR プロトコルを提案する。このプロトコルは、Niemi–Renvall の XOR プロトコル（2.5 節）と、部分開示操作による特定プロトコル（4.1 節）を組み合わせることによって構成されている。提案プロトコルのアイデアを表 6 に示す。プロトコルの手順は以下の通りである。

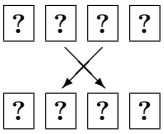
(1) カード列を以下のように並べる。

表 6 提案 XOR プロトコルのアイデア

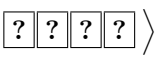
	入力	中央 2 枚の交換	5 を除去	2 を先頭
(0,0)	2456	2546	246	246
(0,1)	2465	2645	264	264
(1,0)	4256	4526	426	264
(1,1)	4265	4625	462	246



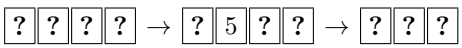
(2) 中央二枚を入れ替える。



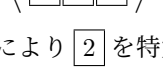
(3) ランダムカットを適用する。



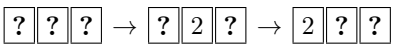
(4) 特定プロトコル B により $\boxed{5}$ を特定し、$\boxed{5}$ を除去する。



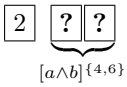
(5) ランダムカットを適用する。



(6) 特定プロトコル A により $\boxed{2}$ を特定し、$\boxed{2}$ が先頭になるように巡回的に並び替える。



(7) 右二枚を出力する。



正当性 提案プロトコルの手順は表 6 のアイディアの通りであることに注意する。すなわち、初期カード列に対して、まず中央の二枚のカードを入れ替え、$\boxed{5}$ を除去し、$\boxed{2}$ が先頭になるようにしている。表 6 のように、最終的なカード列は、入力が $(0,0)$ と $(1,1)$ ときに限り $\boxed{2}\boxed{4}\boxed{6}$ と並び、それ以外のときは $\boxed{2}\boxed{6}\boxed{4}$ と並ぶため、出力コミットメントは $[a \wedge b]^{\{4,6\}}$ と一致することが分かる。よって、正当性が成り立つ。

安全性 提案プロトコルにおいてカードの情報が開示されるのは、ステップ (4)(6) における特定プロトコルの部分開示のみである。ステップ (4) の特定プロトコル B については、$\boxed{5}$ のみスートが見えて、それ以外のカードについてはスートが見えないため、この際に開示される情報は $\boxed{5}$ の位置のみである。同様に、ステップ (6) の特定プロトコルについても、この際に開示される情報は $\boxed{2}$ の位置のみである。これらのカードの位置情報は、直前のランダムカットによって一様ランダムに選ばれるため、入力情報 (a,b) とは独立である。よって、安全性が成り立つ。

5. おわりに

本論文では、Miyahara–Mizuki の部分開示操作を一般化した操作を提案した。そして、一般化した部分開示操作を利用して、従来は Las Vegas プロトコルであったランダムカットに基づく AND プロトコルと XOR プロトコルについて、初めての有限時間プロトコルを構成した。具体的には、ランダムカット 3 回の 4 枚コミット型 AND プロトコルとランダムカット 2 回の 4 枚コミット型 XOR プロトコルを構成した。提案手法を用いることにより、カードを特定する必要のある Las Vegas プロトコルの多くは有限時間プロトコルに変換できる可能性がある。今後の課題として、提案手法の応用先を開拓することが挙げられる。また、部分開示操作を用いたさらなるプロトコルの構成や、部分開示操作の他の活用方法の開拓も課題としたい。

参考文献

[1] A. Koch, M. Schrempp, and M. Kirsten. Card-based cryptography meets formal verification. In S. D. Galbraith and S. Moriai, editors, *Advances in Cryptology–ASIACRYPT 2019*, volume 11921 of *LNCS*, pages 488–517, Cham, 2019. Springer.

[2] A. Koch, S. Walzer, and K. Härtel. Card-based cryptographic protocols using a minimal number of cards. In T. Iwata and J. H. Cheon, editors, *Advances in Cryptology—ASIACRYPT 2015*, volume 9452 of *LNCS*, pages 783–807, Berlin, Heidelberg, 2015. Springer.

[3] D. Miyahara and T. Mizuki. Secure computations through checking suits of playing cards. In *Frontiers in Algorithmics*, Lecture Notes in Computer Science, Cham, 2022. Springer. to appear.

[4] T. Mizuki. Efficient and secure multiparty computations using a standard deck of playing cards. In S. Foresti and G. Persiano, editors, *Cryptology and Network Security*, volume 10052 of *LNCS*, pages 484–499, Cham, 2016. Springer.

[5] V. Niemi and A. Renvall. Solitaire zero-knowledge. *Fundam. Inf.*, 38(1,2):181–188, 1999.