Computer Security Symposium 2021
26 - 29 October 2021

最小枚数の非コミット型６入力ANDプロトコルのシャッフル回数の改善

五十鈴川 頼宗[1,a)]　宮原 大輝[1,2]　水木 敬明[1,2]

概要：カードベース暗号では通常黒と赤の 2 枚のカードを用いて 1 ビットを表現するため，n 入力 AND 関数を $2n$ 枚で秘密計算するプロトコルは最小枚数の AND プロトコルと呼ばれる．本稿では，最小枚数の非コミット型 n 入力 AND プロトコルを扱い，特に必要なシャッフル回数に注目する．現状知られているシャッフル回数が少ないという意味で最良のプロトコルは，2 入力では 2012 年に Mizuki らが提案した 2 回のシャッフルのプロトコル，3 入力では 2021 年に佐々木らが提案した 2 回のシャッフルのプロトコル，4 入力以上では 2016 年に Mizuki が提案した $n+1$ 回のシャッフルのプロトコルである．本稿では上述の佐々木らの 3 入力プロトコルを応用することで 12 枚のカードを用いた非コミット型 6 入力 AND プロトコルを新たに提案する．このプロトコルは最小枚数であり，シャッフル回数が 6.5 回（期待値）で実行でき，既存プロトコルから 0.5 回の削減に成功している．さらに 7 入力以上にプロトコルを拡張でき，シャッフル回数は $n+0.5$ 回（期待値）であり，既存の $n+1$ 回から削減している．

キーワード：カードベース暗号，秘密計算，カード組，非コミット型，論理積

Improvement on the Number of Shuffles for Card-Minimal Non-Committed Six-Input AND Protocol

Raimu Isuzugawa[1,a)]　Daiki Miyahara[1,2]　Takaaki Mizuki[1,2]

Abstract: Because card-based cryptography usually encodes one bit using a pair of black and red cards, the protocols that perform secure computations of n-input AND functions with $2n$ cards are called card-minimal AND protocols. In this paper, we deal with card-minimal non-committed n-input AND protocols and focus on the number of shuffles. The best n-input AND protocols currently known use two shuffles for $n = 2$, two shuffles for $n = 3$, and $n+1$ shuffles for $n > 3$. In this paper, we propose a new non-committed 6-input AND protocol with 12 cards by applying the existing 3-input protocol. This protocol is card-minimal and can be executed with expectation of 6.5 shuffles, which is 0.5 times less than the existing protocol. Furthermore, the protocol can be extended to 7 or more inputs, and the number of shuffles is $n+0.5$ in expectation, which is a reduction from $n+1$ shuffles the existing protocol requires.

Keywords: Card-based protocols, Secure computation, Deck of cards, Non-committed format, Logical AND function

1. はじめに

トランプのような物理的なカード組を用いて秘密計算を行う手法を**カードベース暗号**という．カードベース暗号では，表面が $\boxed{\clubsuit}$ または $\boxed{\heartsuit}$ の 2 色のどちらかであり，裏面が $\boxed{?}$ で区別のつかない 2 種類のカードを用いる．これら

1 東北大学
Tohoku University
2 産業技術総合研究所
National Institute of Advanced Industrial Science and Technology (AIST)
a) raimu.isuzugawa.q6@dc.tohoku.ac.jp

© 2021 Information Processing Society of Japan

のカードを用いて次のようにブール値を表す．

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

ビット $x \in \{0,1\}$ がこの符号化ルールに従って 2 枚のカードとして裏返しに置かれるとき，この 2 枚のカードを x の**コミットメント**と呼び，次のように表現する．

$$\underbrace{\boxed{?}\boxed{?}}_{x}$$

コミットメントを入力として秘密計算を行う一連の手順をカードベース暗号**プロトコル**という．

1.1 非コミット型 AND プロトコル

カードベース暗号プロトコルは 1989 年に Den Boer によって初めて提案された [1]．このプロトコルは **five-card trick** と呼ばれ，2 つのコミットメント $x_1, x_2 \in \{0,1\}$ と 1 枚の追加カード $\boxed{\heartsuit}$ を入力とし，シャッフルやめくる等の操作を経て 2 入力 AND $x_1 \wedge x_2$ を秘密計算する．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{?}\boxed{?}}_{x_2}\boxed{\heartsuit} \to \cdots \to \begin{cases} x_1 \wedge x_2 = 1 & \text{if } \boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\cdots \\ x_1 \wedge x_2 = 0 & \text{otherwise} \end{cases}$$

このプロトコルのように，出力がコミットメントのフォーマットと異なるプロトコルは**非コミット型**と呼ばれ[*1]，本稿では非コミット型プロトコルを対象とする．

この five-card trick プロトコルは，入力コミットメントの他に 1 枚の追加カードを用いて 2 入力 AND を秘密計算している．それに対し，追加カードを使用せずに AND を計算するプロトコルも存在し，それらは**最小枚数の AND プロトコル**と呼ばれる．上述の符号化ルール（1）から，1 つのコミットメントを作成するのに 2 枚のカードが必要であるため，最小枚数の n 入力 AND プロトコルではちょうど $2n$ 枚のカードを使用する．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{?}\boxed{?}}_{x_2}\cdots\underbrace{\boxed{?}\boxed{?}}_{x_n} \to \cdots \to x_1 \wedge x_2 \wedge \cdots \wedge x_n$$

本稿では，このような最小枚数の非コミット型 n 入力 AND プロトコルを扱う．

1.2 既存研究

カードベース暗号プロトコルではカード枚数の他にも操作時間の観点からシャッフル回数も性能を示す指標としている．本稿では，特に必要なシャッフル回数に注目する．現在知られている最小枚数の非コミット型 AND プロトコルの内，シャッフル回数が少ないという意味で最良の既存研究を表 1 に示す．

表 1 に示した通り，2 入力では 2012 年に Mizuki らが提案したプロトコル [6] が最良である．

表 1 既存の最小枚数の非コミット型 AND プロトコルと提案プロトコル

	入力の数	カード枚数	シャッフル回数
Mizuki ら [6]	2	4	2
佐々木ら [2,11]	3	6	2
Mizuki [4]	$n\,(\geq 4)$	$2n$	$n+1$
本稿	**6**	**12**	**6.5（期待値）**
本稿	$\boldsymbol{n\,(\geq 7)}$	$\boldsymbol{2n}$	$\boldsymbol{n+0.5}$**（期待値）**

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{?}\boxed{?}}_{x_2} \xrightarrow{\text{2 shuffles}} \cdots \to \begin{cases} x_1 \wedge x_2 = 0 & \text{if } \boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\heartsuit} \\ x_1 \wedge x_2 = 0 & \text{if } \boxed{\clubsuit}\boxed{\heartsuit}\boxed{?}\boxed{?} \\ x_1 \wedge x_2 = 1 & \text{if } \boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\clubsuit} \\ x_1 \wedge x_2 = 1 & \text{if } \boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?} \end{cases}$$

このプロトコルは 4 枚のカードを使用し，2 回のランダム二等分割カットと呼ばれるシャッフル操作（2.3 節で説明する）を行うことで 2 入力 AND を秘密計算している．

3 入力では 2021 年に佐々木らが提案したプロトコル [2,11] が最良である．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{?}\boxed{?}}_{x_2}\underbrace{\boxed{?}\boxed{?}}_{x_3} \xrightarrow{\text{2 shuffles}} \cdots$$

$$\to \begin{cases} x_1 \wedge x_2 \wedge x_3 = 1 & \text{if } \boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}\cdots \\ x_1 \wedge x_2 \wedge x_3 = 1 & \text{if } \boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\cdots \\ x_1 \wedge x_2 \wedge x_3 = 0 & \text{otherwise} \end{cases}$$

このプロトコルは 6 枚のカードを使用し，1 回のランダム二等分割カットと 1 回のランダムカット（2.2 節で説明する）の合計 2 回のシャッフル操作で 3 入力 AND を秘密計算している．

4 入力以上で最良のプロトコルは 2016 年に Mizuki によって提案されたプロトコル [4] である．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{?}\boxed{?}}_{x_2}\cdots\underbrace{\boxed{?}\boxed{?}}_{x_n} \xrightarrow{n+1\text{ shuffles}} \cdots$$

$$\to \begin{cases} x_1 \wedge x_2 \wedge \cdots \wedge x_n = 0 & \text{if } \boxed{\clubsuit}\cdots \\ x_1 \wedge x_2 \wedge \cdots \wedge x_n = 1 & \text{if } \boxed{\heartsuit}\cdots \end{cases}$$

このプロトコルは $n\,(\geq 4)$ 個のコミットメントを入力とし（すなわち，$2n$ 枚のカードを用いて），$n+1$ 回のシャッフルで n 入力 AND を秘密計算している．

1.3 本稿の貢献

本稿では既存プロトコルのシャッフル回数の削減に取り組む．具体的には，表 1 の佐々木らの 3 入力 AND プロトコル [2,11] と 2009 年に Mizuki らによって提案された **MS-AND プロトコル** [9] を応用することで，12 枚のカードを用いた非コミット型 6 入力 AND プロトコルを新たに

*1 出力がコミットメントであるプロトコルを**コミット型**プロトコル，そうでないプロトコルを非コミット型プロトコルと呼ぶ．

提案する．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\ \underbrace{\boxed{?}\boxed{?}}_{x_2}\ \cdots\ \underbrace{\boxed{?}\boxed{?}}_{x_6} \xrightarrow{6.5\ \text{shuffles}} \cdots$$

$$\rightarrow \begin{cases} x_1 \wedge \cdots \wedge x_6 = 1 & \text{if } \boxed{\heartsuit}\boxed{\heartsuit}\cdots \text{ or } \boxed{\clubsuit}\boxed{\clubsuit}\cdots \\ x_1 \wedge \cdots \wedge x_6 = 0 & \text{otherwise} \end{cases}$$

このプロトコルは最小枚数であり，ランダムカットとランダム二等分割カット，及び通常のシャッフルのみで実行できる．その合計回数の期待値は 6.5 回であり，既存プロトコルからシャッフル回数について 0.5 回の削減に成功している（表 1 参照）．

さらに 7 入力以上にプロトコルを拡張でき，シャッフル回数は期待値で $n + 0.5$ 回であり，既存の $n + 1$ 回から削減している（表 1 参照）．

1.4 本稿の構成

本稿の構成は次の通りである．1 節では最小枚数の非コミット型 AND プロトコルの既存研究と本稿の貢献について述べた．2 節では提案プロトコルに必要な操作と MS-AND プロトコル [9] について説明する．3 節では新しい用語を定義した後，佐々木らの 3 入力 AND を前半と後半に分けて説明する．そして，4 節で提案プロトコルについて述べて，最後に 5 節で結論を述べる．

2. 準備

本節では，初めにカードベース暗号で使用される操作について説明した後，提案プロトコルで使用するランダムカットとランダム二等分割カットの 2 つのシャッフル操作について説明する．最後に MS-AND プロトコル [9] について説明する．

2.1 カードベース暗号で使用される操作

カードベース暗号では，カード列に対して主に 3 つの操作が行われる [7,8]．以下では，m 枚のカード列を考える．

並び替え　カード列に対してある置換 π を適用する．この操作を (perm, π) と表記する．

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{m}{\boxed{?}} \xrightarrow{(\mathsf{perm},\pi)} \overset{\pi^{-1}(1)}{\boxed{?}}\ \overset{\pi^{-1}(2)}{\boxed{?}}\ \cdots\ \overset{\pi^{-1}(m)}{\boxed{?}}$$

めくる　インデックスの集合 T に関して，全ての $t \in T$ についてカード列の左から t 番目をめくってカードの色を確認する．この操作を (turn, T) と表記する．

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{t\in T}{\boxed{?}}\cdots\overset{m}{\boxed{?}} \xrightarrow{(\mathsf{turn},T)} \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{t\in T}{\boxed{\clubsuit}}\cdots\overset{m}{\boxed{?}}$$

シャッフル　ある置換の集合 Π から一様ランダムに選ばれた置換 $\pi \in \Pi$ をカード列に適用する．この操作を (shuf, Π) と表記する．

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{m}{\boxed{?}} \xrightarrow{(\mathsf{shuf},\Pi)} \overset{\pi^{-1}(1)}{\boxed{?}}\ \overset{\pi^{-1}(2)}{\boxed{?}}\ \cdots\ \overset{\pi^{-1}(m)}{\boxed{?}}$$

ただし，Π に含まれるどの置換が適用されたかは誰も知り得ない．

2.2 ランダムカット

ランダムカットとは，カードベース暗号において最もシンプルかつ実装が容易であるシャッフル操作であり，適用後の並びが誰にも分からなくなるようにカード列を巡回的にランダムにシフトさせるものである．ランダムカットは $\langle\cdot\rangle$ と表記する．m 枚のカード列にランダムカットを適用すると次の m 通りのカード列のいずれか 1 つが得られ，その生起確率はそれぞれ $1/m$ である．

$$\left\langle \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\cdots\overset{m-1}{\boxed{?}}\overset{m}{\boxed{?}} \right\rangle \rightarrow \begin{cases} \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\cdots\overset{m-1}{\boxed{?}}\overset{m}{\boxed{?}}, \\ \overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\cdots\overset{m}{\boxed{?}}\overset{1}{\boxed{?}}, \\ \vdots \\ \overset{m-1}{\boxed{?}}\overset{m}{\boxed{?}}\overset{1}{\boxed{?}}\cdots\overset{m-3}{\boxed{?}}\overset{m-2}{\boxed{?}}, \\ \overset{m}{\boxed{?}}\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{m-2}{\boxed{?}}\overset{m-1}{\boxed{?}} \end{cases}$$

このランダムカットは，巡回置換 $\pi = (1\,2 \cdots m)$ を用いて

$$(\mathsf{shuf}, \{\mathsf{id}, \pi, \pi^2, \ldots, \pi^{m-1}\})$$

と書くことができる．ここで id は恒等置換を表す．本稿では簡単のため，このランダムカットを

$$(\mathsf{shuf}, \mathsf{RC}_{1,2,\ldots,m})$$

と表記することにする．ランダムカットは操作が簡単で，人間が安全に実行できることが実験的に確認されている [10]．

2.3 ランダム二等分割カット

ランダム二等分割カット [9] とは，2009 年に考案されたシャッフル操作であり，$[\cdot|\cdot]$ と表記され，カード列を半分に分けて分割された 2 つのカード列をランダムに入れ替えるものである．例として，$2m$ 枚のカード列にランダム二等分割カットを適用すると次のカード列のいずれかが 1/2 の確率で得られる．

$$\left[\overset{1}{\boxed{?}}\cdots\overset{m}{\boxed{?}}\,\middle|\,\overset{m+1}{\boxed{?}}\cdots\overset{2m}{\boxed{?}}\right] \rightarrow \begin{cases} \overset{1}{\boxed{?}}\cdots\overset{m}{\boxed{?}}\overset{m+1}{\boxed{?}}\cdots\overset{2m}{\boxed{?}}, \\ \overset{m+1}{\boxed{?}}\cdots\overset{2m}{\boxed{?}}\overset{1}{\boxed{?}}\cdots\overset{m}{\boxed{?}} \end{cases}$$

このランダム二等分割カットは次のように表記できる．

$$(\mathsf{shuf}, \{\mathsf{id}, (1\ m{+}1)(2\ m{+}2)\cdots(m\ 2m)\})$$

ランダム二等分割カットは身近な道具を用いて安全に実装できることが知られている [10]．

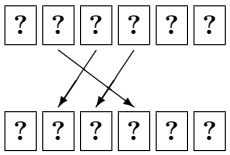
2.4 MS-AND プロトコル

MS-AND プロトコル [9] は，2009 年に提案されたコミット型の 2 入力 AND プロトコルであり，$x_1, x_2 \in \{0, 1\}$ のコミットメントと $\boxed{\clubsuit}\boxed{\heartsuit}$ の 2 枚の追加カードを入力として，1 回のランダム二等分割カットで $x_1 \wedge x_2$ のコミットメントを出力する．その手順は以下の通りである．

(1) 2 つの入力コミットメントと 2 枚の追加カードを次のように置き，中央の 2 枚を裏返す．このとき，中央の 2 枚は 0 のコミットメントとなる．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{\clubsuit}\boxed{\heartsuit}}_{0}\underbrace{\boxed{?}\boxed{?}}_{x_2} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{x_1}\underbrace{\boxed{?}\boxed{?}}_{0}\underbrace{\boxed{?}\boxed{?}}_{x_2}$$

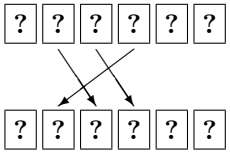
(2) カード列を次のように並び替える．



(3) カード列に対してランダム二等分割カットを適用する．

$$\left[\boxed{?}\boxed{?}\boxed{?} \,\middle|\, \boxed{?}\boxed{?}\boxed{?}\right] \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

(4) カード列を次のように並び替える．



(5) 左から 1 枚目と 2 枚目のカードをめくる．めくられたカード列の並びに応じて次のように $x_1 \wedge x_2$ のコミットメントが得られる．なお，$x_1 \wedge x_2$ のコミットメントでないめくられていない 2 枚のカードは $\overline{x_1} \wedge x_2$ のコミットメントである．

$$\boxed{\clubsuit}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{x_1\wedge x_2}\underbrace{\boxed{?}\boxed{?}}_{\overline{x_1}\wedge x_2} \quad \text{or} \quad \boxed{\heartsuit}\boxed{\clubsuit}\underbrace{\boxed{?}\boxed{?}}_{\overline{x_1}\wedge x_2}\underbrace{\boxed{?}\boxed{?}}_{x_1\wedge x_2}$$

この MS-AND プロトコルによって生成される $x_1 \wedge x_2$ のコミットメントは，他のプロトコルへの入力として使うことができる．また，先頭の表になっている 2 枚のカードは**フリーカード**として自由に使うことができる．さらに，もう一つ得られている $\overline{x_1} \wedge x_2$ のコミットメントは一般にはあまり活用されないが，それらに通常のシャッフルを加えることで，フリーカードとすることができる．

3. 新しい符号化と既存 3 入力 AND プロトコル

1 節で言及した既存の非コミット型 3 入力 AND プロトコル [2,11] は，2021 年に佐々木らによって提案され，追加カードを使用せず $x_1, x_2, x_3 \in \{0, 1\}$ のコミットメントのみを入力として $x_1 \wedge x_2 \wedge x_3$ を秘密計算する．本稿で提案するプロトコルは，この既存プロトコルのアイデアを利用する．そのため，文献 [2,11] に記述されている既存プロトコルに新しい解釈を与え，それに合わせて語句の定義とプロトコルの表記の分割を行う．具体的には，3.1 節で新しい符号化を定義し，既存 AND プロトコルを前半と後半に分けてそれぞれの手順を 3.2 節と 3.3 節で説明する．

3.1 新しい符号化

コミットメントを定義している符号化ルール（1）では，$\boxed{\clubsuit}$, $\boxed{\heartsuit}$ がそれぞれ 1 枚ずつで構成されている．本稿では新たに $\boxed{\clubsuit}\boxed{\clubsuit}$ と $\boxed{\heartsuit}\boxed{\heartsuit}$ の組み合わせも考慮し，次のような新しい符号化ルールを定義する．

$$\boxed{\clubsuit}\boxed{\clubsuit}, \boxed{\clubsuit}\boxed{\heartsuit}, \boxed{\heartsuit}\boxed{\clubsuit} = 0, \quad \boxed{\heartsuit}\boxed{\heartsuit} = 1 \qquad (2)$$

この符号化を $\heartsuit^+$ **ベース**，この符号化ルールで作成されたコミットメントを $\heartsuit^+$ **ベースコミットメント**と呼び，

$$\underbrace{\boxed{?}\boxed{?}}_{[x]^{\heartsuit+}}$$

のように表すことにする[*2]．$\clubsuit^+$ ベースコミットメントは

$$\boxed{\heartsuit}\boxed{\heartsuit}, \boxed{\clubsuit}\boxed{\heartsuit}, \boxed{\heartsuit}\boxed{\clubsuit} = 0, \quad \boxed{\clubsuit}\boxed{\clubsuit} = 1 \qquad (3)$$

として同様に定義する．

既存 3 入力 AND プロトコル [2,11] は，非コミット型で $x_1 \wedge x_2 \wedge x_3$ を秘密計算するものであるが，解釈を変えると $\heartsuit^+$ ベースコミットメント

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1\wedge x_2\wedge x_3]^{\heartsuit+}}$$

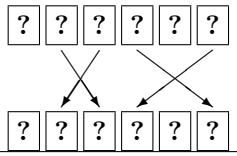
（あるいは $\clubsuit^+$ ベースコミットメント）を出力するものとみなせる．このことを，プロトコルの前半と後半に分けて以降で説明する．

3.2 プロトコルの前半

本小節では，既存 3 入力 AND プロトコルの前半の手順を説明する．具体的な手順は以下の通りである．

(1) 次の (a)–(c) の操作を行うことで $(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,6)\})$ を適用する．

(a) 次のように左から 2 枚目と 3 枚目及び 4 枚目と 6 枚目のカードをそれぞれ入れ替える．

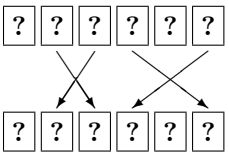


*2 文献 [4] において，$\clubsuit\heartsuit, \heartsuit\clubsuit = 0, \quad \heartsuit\heartsuit = 1$ という符号化の下のコミットメントを $[x]^{\heartsuit}$ と記述しているため，ここでは + の記号を付けて，$\heartsuit^+$ ベースとした．

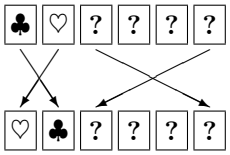
(b) 左側の 4 枚のカードにランダム二等分割カットを適用する．

$$\left[\boxed{?}\boxed{?}\middle|\boxed{?}\boxed{?}\right]\ \boxed{?}\boxed{?} \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

(c) 次のように左から 2 枚目と 3 枚目及び 4 枚目と 6 枚目のカードをそれぞれ入れ替える．



(2) いま，左から 1 枚目と 2 枚目のカードは 1/2 の確率で x_1 か $\overline{x_1}$ のコミットメントになっていることに注意したい．それら 2 枚のカードをめくり，カードの色を確認する．$\boxed{\clubsuit}\boxed{\heartsuit}$ が出た場合，1 枚目と 2 枚目及び 3 枚目と 6 枚目をそれぞれ入れ替える．



以上がプロトコルの前半であり，次のようなカード列になっており，左側 2 枚はフリーカードとなっている．

$$\boxed{\heartsuit}\boxed{\clubsuit}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

また，残りの 4 枚は次のようになっている．

$$\begin{array}{ll}
\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit} & \text{if } (x_1,x_2,x_3)=(0,0,0) \\
\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit} & \text{if } (x_1,x_2,x_3)=(0,0,1) \text{ or } (1,0,1) \\
\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit} & \text{if } (x_1,x_2,x_3)=(0,1,0) \text{ or } (1,1,0) \\
\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit} & \text{if } (x_1,x_2,x_3)=(0,1,1) \\
\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit} & \text{if } (x_1,x_2,x_3)=(1,0,0) \\
\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit} & \text{if } (x_1,x_2,x_3)=(1,1,1)
\end{array} \tag{4}$$

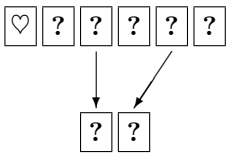
3.3 プロトコルの後半

本小節では，既存 3 入力 AND プロトコルの後半の手順を説明する．

(1) 左側の 2 枚を裏返しにした後，カード列に対しランダムカットを適用する．

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

(2) 左から 1 枚目のカードをめくり，次のように 3 枚目と 5 枚目のカードを取り出す．



この例のように 1 枚目が $\boxed{\heartsuit}$ の場合には，取り出した 2 枚のカードは

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1\wedge x_2\wedge x_3]^{\heartsuit+}}$$

となっており，$x_1 \wedge x_2 \wedge x_3$ の $\heartsuit^+$ ベースコミットメントが得られる．1 枚目が $\boxed{\clubsuit}$ の場合は $\clubsuit^+$ ベースコミットメントになる．

このあと，$\heartsuit^+$ ベース（あるいは $\clubsuit^+$ ベース）のコミットメントをめくることで，既存 3 入力 AND プロトコルでは $x_1 \wedge x_2 \wedge x_3$ を非コミット型で秘密計算している．

4. 提案プロトコル

本節では，12 枚のカードを用いた非コミット型 6 入力 AND プロトコルを新たに提案する．

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\ \underbrace{\boxed{?}\boxed{?}}_{x_2}\ \cdots\ \underbrace{\boxed{?}\boxed{?}}_{x_6} \rightarrow \cdots$$

$$\rightarrow \underbrace{\boxed{?}\boxed{?}}_{[x_1\wedge x_2\wedge\cdots\wedge x_6]^{\heartsuit+}} \quad \text{or} \quad \underbrace{\boxed{?}\boxed{?}}_{[x_1\wedge x_2\wedge\cdots\wedge x_6]^{\clubsuit+}} \rightarrow \text{めくる}$$

このプロトコルのシャッフル回数は期待値で 6.5 である．まず 4.1 節で提案プロトコルのアイデアを述べる．その後提案プロトコルで利用するサブプロトコルとして MS-AND プロトコル 2 回の結果の出力と 2 入力 AND でない 2 つのコミットメントを生成するプロトコル，$\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ の 4 枚のカードから 0 の $\heartsuit^+$ ベースコミットメントを出力するプロトコル，$\heartsuit^+$ ベースコミットメントと通常のコミットメントから AND を計算するプロトコルをそれぞれ 4.2 節，4.3 節，4.4 節で構築する．そして 4.5 節で提案プロトコルの手順を述べ，最後に 4.6 節で提案プロトコルの正当性と安全性を証明する．

4.1 提案プロトコルのアイデア

提案プロトコルの概要を図 1 に示す．

2.4 節で述べた MS-AND プロトコル [9] はコミット型であるため，$\boxed{\clubsuit}\boxed{\heartsuit}$ の 2 枚のフリーカードを用意できれば何度でも繰り返し AND を計算することができる．一方で，既存 3 入力 AND プロトコル [2,11] は 3.2 節のステップ 2 で 2 枚のフリーカードが得られる．これらを MS-AND プロトコルの追加カードとして利用することで，既存 3 入力 AND プロトコルと合わせて 3 入力 AND を 2 つ秘密計算することができる．後は秘密計算した 2 つの 3 入力 AND のコミットメントを MS-AND プロトコルの入力として計算すれば良いが，既存 3 入力 AND プロトコルの出力は通常の符号化ルール（1）で符号化されたコミットメントではないためそのままでは MS-AND プロトコルの入力とすることができない．そこで MS-AND プロトコルを 1 回実行する度に 2 枚のフリーカードができることを利用して 0

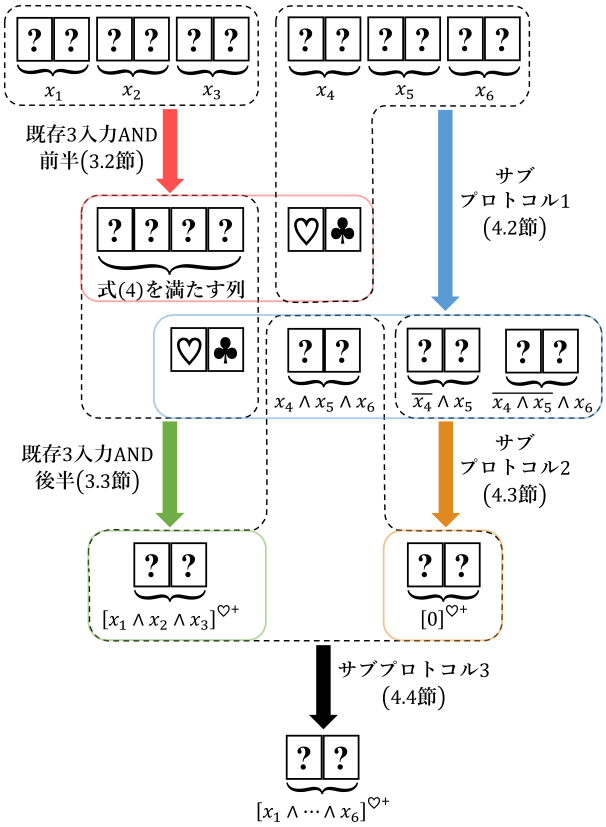


図 1　提案プロトコルの概要

の $\heartsuit^+$ ベースコミットメントを作成することで，MS-AND プロトコルの入力にできるようにする．MS-AND プロトコルから 0 の $\heartsuit^+$ ベースコミットメントを作成する手法は 4.2 節と 4.3 節で，$\heartsuit^+$ ベースコミットメントを MS-AND プロトコルに組み込む手法は 4.4 節で説明する．

4.2　サブプロトコル 1：MS-AND2 回

本小節では，$a, b, c \in \{0, 1\}$ の 3 つのコミットメントと $\boxed{\clubsuit}\boxed{\heartsuit}$ の 2 枚のフリーカードから，MS-AND プロトコルを 2 回実行することで $a \wedge b \wedge c$ のコミットメントを出力するサブプロトコルを説明する．なお，プロトコル終了時には $\overline{a} \wedge b$ と $\overline{a \wedge b} \wedge c$ のコミットメントも得られる．サブプロトコルの手順は次の通りである．

(1) a と b のコミットメントと 2 枚のフリーカードで MS-AND プロトコルを実行する．

$$\clubsuit\ \heartsuit\ \underbrace{?\ ?}_{a\wedge b}\ \underbrace{?\ ?}_{\overline{a}\wedge b}\ \underbrace{?\ ?}_{c} \quad \text{or} \quad \heartsuit\ \clubsuit\ \underbrace{?\ ?}_{\overline{a}\wedge b}\ \underbrace{?\ ?}_{a\wedge b}\ \underbrace{?\ ?}_{c}$$

適用後のカード列は，c のコミットメントの他に 2 枚のフリーカード，$a \wedge b$ のコミットメント，そして $\overline{a} \wedge b$ のコミットメントで構成されている．

(2) $a \wedge b$ と c のコミットメントと 2 枚のフリーカードで MS-AND プロトコルを実行する．

$$\clubsuit\ \heartsuit\ \underbrace{?\ ?}_{a\wedge b\wedge c}\ \underbrace{?\ ?}_{\overline{a\wedge b}\wedge c}\ \underbrace{?\ ?}_{\overline{a}\wedge b} \quad \text{or} \quad \heartsuit\ \clubsuit\ \underbrace{?\ ?}_{\overline{a\wedge b}\wedge c}\ \underbrace{?\ ?}_{a\wedge b\wedge c}\ \underbrace{?\ ?}_{\overline{a}\wedge b}$$

適用後のカード列は，2 枚のフリーカードと $a \wedge b \wedge c$ のコミットメント，そして $\overline{a} \wedge b$ と $\overline{a \wedge b} \wedge c$ のコミットメントで構成されている．ここで符号化ルール（1）より，$\overline{a} \wedge b$ と $\overline{a \wedge b} \wedge c$ のコミットメントはどちらも $\boxed{\clubsuit}$ と $\boxed{\heartsuit}$ の 2 枚によって構成されていることに注意したい．

このサブプロトコルのシャッフル回数は 2 回である．

4.3　サブプロトコル 2：$\heartsuit^+$ ベース 0 コミットメントの出力

$\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ の 4 枚が任意の並びで裏になっている状態で与えられたとき，0 の $\heartsuit^+$ ベースコミットメントを出力するサブプロトコルを構成する．その手順は次の通りである．

(1) 4 枚のカードに対し通常のシャッフルを適用する（S_4 を 4 次の対称群とするとき (shuf, S_4) を適用する）．

(2) 左から 1 枚目のカードをめくる．$\boxed{\clubsuit}$ の場合はステップ 3 へ，$\boxed{\heartsuit}$ の場合はステップ 5 へ進む．

$$\clubsuit\ ?\ ?\ ? \quad \text{or} \quad \heartsuit\ ?\ ?\ ?$$

(3) ステップ 2 でめくっていない残り 3 枚もめくり，$\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}$ の並びになるように並び替えを行う．

$$\clubsuit\ ?\ ?\ ? \rightarrow \heartsuit\ \heartsuit\ \clubsuit\ \clubsuit$$

(4) カードを全て裏返しにした後，右側 3 枚のカードに対しランダムカットを適用する．

$$?\ \langle ?\ ?\ ? \rangle \rightarrow ?\ ?\ ?\ ?$$

(5) 右側の 2 枚のカードを取り出すと，0 の $\heartsuit^+$ ベースコミットメントとなる．

$$?\ ?\ \underbrace{?\ ?}_{[0]^{\heartsuit+}}$$

$\heartsuit^+$ ベースの符号化ルール（2）から，$\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}$ の 3 枚からランダムに 2 枚抽出すれば 0 の $\heartsuit^+$ ベースコミットメントが得られることが分かる．すなわち，4 枚の内めくった 1 枚が $\boxed{\heartsuit}$ の場合はそのまま残り 3 枚から，$\boxed{\clubsuit}$ の場合は改めて $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}$ をシャッフルしたものから 3 枚取り出せば 0 の $\heartsuit^+$ ベースコミットメントが得られる．

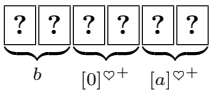
このサブプロトコルでは，ステップ 1 と 4 でシャッフルを 1 回用いているが，ステップ 4 が実行されるのは 1/2 の確率であるため，全体のシャッフル回数は 1.5 回（期待値）である．また，$\clubsuit^+$ ベースの 0 のコミットメントも同様に構成できる．

4.4　サブプロトコル 3：$\heartsuit^+$ ベース AND

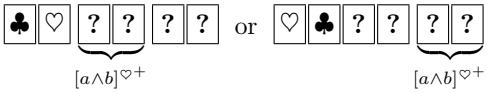
本小節では，a の $\heartsuit^+$ ベースコミットメント，0 の $\heartsuit^+$

ベースコミットメント，及び（通常の）b のコミットメントが与えられたときに，$a \wedge b$ の $\heartsuit^+$ ベースコミットメントを出力するサブプロトコルを構成する．その手順は次の通りである．

(1) コミットメントを次のように並べる．



(2) カード列に対して MS-AND プロトコルと同じ手順を適用する．

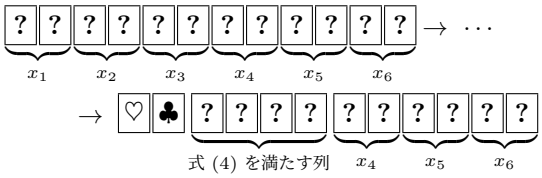


最後のステップで出力となるカードの位置は MS-AND プロトコルと同じだが，得られるコミットメントは $\heartsuit^+$ ベースのものである．このサブプロトコルのシャッフル回数は 1 回である．$\clubsuit^+$ ベースのものも同様に構成できる．

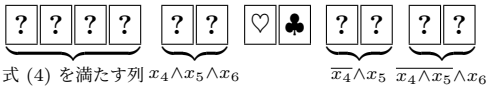
4.5 提案プロトコルの手順

提案プロトコルの手順を説明する．提案プロトコルは入力として $x_1, \ldots, x_6 \in \{0, 1\}$ のコミットメント（計 12 枚のカード）から始まる．

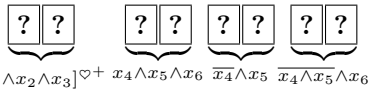
(1) x_1, x_2, x_3 のコミットメントに対し 3.2 節の既存 3 入力 AND プロトコルの前半までを適用する．このとき 2 枚のフリーカード ♡ ♣ が得られる．



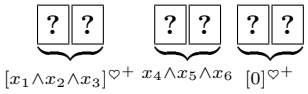
(2) フリーカード ♡ ♣ と x_4, x_5, x_6 のコミットメントに対し 4.2 節のサブプロトコル 1 を適用する．



(3) 左側 4 枚のカードとフリーカード ♡ ♣ に対し，3.3 節の既存 3 入力 AND プロトコルの後半を適用する．このとき $\heartsuit^+$ ベースか $\clubsuit^+$ ベースのどちらかのコミットメントが得られるが，以降では $\heartsuit^+$ であるものとして考える（$\clubsuit^+$ ベースの場合も同様に読み替えられる）．



(4) 右側 4 枚の裏になっているカードに対し 4.3 節のサブプロトコル 2 を適用する．



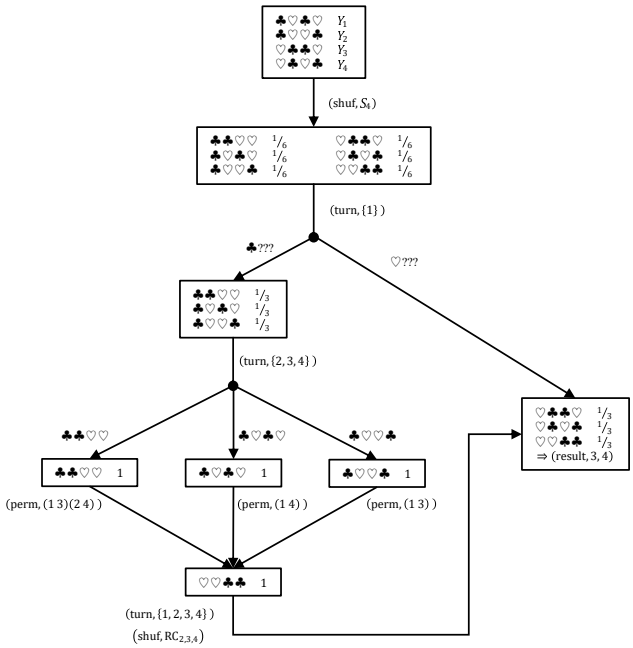
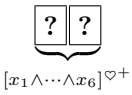


図 2 サブプロトコル 2 の KWH-tree．$Y_1, \cdots, Y_4$ は $Y_1 + \cdots + Y_4 = 1$ なる任意の変数とする．

(5) 4.4 節のサブプロトコル 3 を適用することで，



が得られ，この 2 枚をめくることで $x_1 \wedge \cdots \wedge x_6$ の値だけが公開される．

以上が提案プロトコルの手順である．シャッフル回数は，ステップ 1 が 1 回，ステップ 2 が 2 回，ステップ 3 が 1 回，ステップ 4 が 1/2 の確率で 1 回か 2 回，ステップ 5 が 1 回であり，期待値として合計 6.5 回のシャッフルで終了する[*3]．

4.6 提案プロトコルの正当性と安全性

提案プロトコルの正当性と安全性について述べる．

既存プロトコルとサブプロトコル 1 については，過去の文献 [2, 9, 11] でその安全性や正当性が示されている．

サブプロトコル 2 の正当性と安全性は KWH-tree [3] を用いて証明する．KWH-tree とは，カードの状態を表すノードとそれらを結ぶ操作を表すエッジで構成されている図である．あるプロトコルの KWH-tree において，各ノードの確率分布を確認すること，及び各葉ノードのカード列を確認することで，そのプロトコルの正当性と安全性が自動的に証明される．サブプロトコル 2 の KWH-tree を図 2 に示す．これによりサブプロトコル 2 は正当かつ安全である．

サブプロトコル 3 については，ページ数制限の都合上，

*3 1/2 の確率で 6 回，1/2 の確率で 7 回のシャッフルであり，このプロトコルは有限時間で終了し，いわゆるラスベガスアルゴリズムではないことに注意しよう．

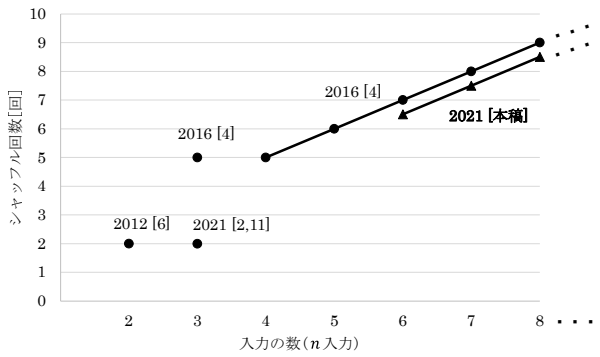
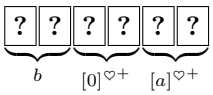


図 3 最小枚数の非コミット型 AND プロトコルのシャッフル回数

その KHW-tree の記載は省略する．ポイントは，入力の



において，0 の $\heartsuit^+$ ベースコミットメントは図 2 の KWH-tree から分かるように，3 通りの可能性が等確率に起こるようになっており，a の $\heartsuit^+$ ベースコミットメントについても同様であることである．

5. おわりに

本稿の主要な成果は，4 節で提案した最小枚数の非コミット型 6 入力 AND プロトコルであり，そのシャッフル回数が 6.5 であることから，既存プロトコル [4] が 7 回のシャッフルを要することを踏まえると，0.5 回の削減に成功している．

提案プロトコルは 7 入力以上へ容易に拡張できる．すなわち，$n\,(\geq 7)$ 入力に対して同様にプロトコルを進め，ステップ 2 におけるサブプロトコル 1 の適用時に，MS-AND プロトコルを 2 回ではなく $n-4$ 回実行するだけでよい．このとき，シャッフル回数の合計は $n+0.5$ 回（期待値）であり[*4]，既存プロトコル [4] よりも 0.5 回少ない．

最小枚数の非コミット型 n 入力 AND プロトコルのシャッフル回数について図 3 のグラフにまとめた（使用できるシャッフルは，ランダムカット，ランダム二等分割カット，及び通常のシャッフルとする）[*5]．

シャッフル回数のより少ないプロトコルの考案は重要な未解決問題であり，積極的なチャレンジを期待したい．

近年カードベース暗号の研究が盛んであり（例 [5,12,13]），上述のチャレンジ問題が分野のさらなる拡大に資することを期待したい．

謝辞 本研究は JSPS 科研費 JP19J21153，JP21K11881 の助成を受けたものです．

[*4] より正確には，1/2 の確率で n 回であり，1/2 の確率で $n+1$ 回である．

[*5] 1.2 節で紹介した既存プロトコルの他に，$n=3$ のときに 5 回のシャッフルのものがあり [4]，それもプロットしている．

参考文献

[1] Den Boer, B.: More Efficient Match-Making and Satisfiability The Five Card Trick, *Advances in Cryptology—EUROCRYPT '89* (Quisquater, J.-J. and Vandewalle, J., eds.), LNCS, Vol. 434, Berlin, Heidelberg, Springer, pp. 208–217 (online), available from ⟨https://doi.org/10.1007/3-540-46885-4_23⟩ (1990).

[2] Isuzugawa, R., Toyoda, K., Sasaki, Y., Miyahara, D. and Mizuki, T.: A Card-Minimal Three-Input AND Protocol Using Two Shuffles, *Computing and Combinatorics*, LNCS, Cham, Springer (2021, to appear).

[3] Koch, A., Walzer, S. and Härtel, K.: Card-Based Cryptographic Protocols Using a Minimal Number of Cards, *Advances in Cryptology—ASIACRYPT 2015* (Iwata, T. and Cheon, J. H., eds.), LNCS, Vol. 9452, Berlin, Heidelberg, Springer, pp. 783–807 (online), available from ⟨https://doi.org/10.1007/978-3-662-48797-6_32⟩ (2015).

[4] Mizuki, T.: Card-based Protocols for Securely Computing the Conjunction of Multiple Variables, *Theor. Comput. Sci.*, Vol. 622, No. C, pp. 34–44 (online), available from ⟨https://doi.org/10.1016/j.tcs.2016.01.039⟩ (2016).

[5] Mizuki, T.: Preface: Special Issue on Card-Based Cryptography, *New Gener. Comput.*, Vol. 39, No. 1, pp. 1–2 (2021).

[6] Mizuki, T., Kumamoto, M. and Sone, H.: The Five-Card Trick Can Be Done with Four Cards, *Advances in Cryptology—ASIACRYPT 2012* (Wang, X. and Sako, K., eds.), LNCS, Vol. 7658, Berlin, Heidelberg, Springer, pp. 598–606 (online), available from ⟨https://doi.org/10.1007/978-3-642-34961-4_36⟩ (2012).

[7] Mizuki, T. and Shizuya, H.: A formalization of card-based cryptographic protocols via abstract machine, *Int. J. Inf. Secur.*, Vol. 13, No. 1, pp. 15–23 (online), available from ⟨https://doi.org/10.1007/s10207-013-0219-4⟩ (2014).

[8] Mizuki, T. and Shizuya, H.: Computational Model of Card-Based Cryptographic Protocols and Its Applications, *IEICE Trans. Fundamentals*, Vol. E100.A, No. 1, pp. 3–11 (online), available from ⟨https://doi.org/10.1587/transfun.E100.A.3⟩ (2017).

[9] Mizuki, T. and Sone, H.: Six-Card Secure AND and Four-Card Secure XOR, *Frontiers in Algorithmics* (Deng, X., Hopcroft, J. E. and Xue, J., eds.), LNCS, Vol. 5598, Berlin, Heidelberg, Springer, pp. 358–369 (online), available from ⟨https://doi.org/10.1007/978-3-642-02270-8_36⟩ (2009).

[10] Ueda, I., Miyahara, D., Nishimura, A., Hayashi, Y., Mizuki, T. and Sone, H.: Secure implementations of a random bisection cut, *Int. J. Inf. Secur.*, Vol. 19, No. 4, pp. 445–452 (online), available from ⟨https://doi.org/10.1007/s10207-019-00463-w⟩ (2020).

[11] 佐々木優，宮原大輝，水木敬明，曽根秀昭：6 枚のカードを用いた非コミット型 3 入力 AND プロトコル，第 92 回 CSEC 研究発表会，6 (2021).

[12] 須賀祐治：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，第 92 回 CSEC 研究発表会，7 (2021).

[13] 中井雄士，徳重佑樹，　岩本貢，太田和夫：秘匿置換を用いたカードベースしきい値関数プロトコル，暗号と情報セキュリティシンポジウム SCIS2021，2F1-3 (2021).