New Card-based Copy Protocols Using Only Random Cuts

Hiroto Koyama
Graduate School of Information Sciences, Tohoku University
Sendai, Japan

Kodai Toyoda
Graduate School of Information Sciences, Tohoku University
Sendai, Japan

Daiki Miyahara
Graduate School of Information Sciences, Tohoku University
National Institute of Advanced Industrial Science and Technology (AIST)
Sendai, Japan

Takaaki Mizuki
Cyberscience Center, Tohoku University
National Institute of Advanced Industrial Science and Technology
Sendai, Japan

ABSTRACT

In card-based cryptography, a commitment to a Boolean value is usually represented by two face-down cards of different colors or numbers, whose order specifies the one-bit value (namely, 0 or 1). One of the most important primitives in card-based cryptography is a "copy protocol," which is supposed to make two identical copies of a given commitment. In the literature, there are several copy protocols, which can be categorized by kinds of shuffles they use; this paper focuses on those using only the so-called random cut, which is the simplest shuffle, and we propose two copy protocols that are more efficient than the existing ones. Specifically, we first work on a standard deck of cards and design a six-card copy protocol using three random cuts (on average). Since the previous protocol needs 5.5 random cuts, our protocol improves upon it. Next, we shift our attention to the case of a two-colored deck of cards, and construct a six-card copy protocol using three random cuts (on average). Because the previous protocol requires eight cards, our protocol uses two cards fewer than the previous one (although it uses one more shuffle). In addition, going back to the standard-deck setting, we provide a four-card XOR protocol using only one random cut for the first time.

CCS CONCEPTS

• **Security and privacy → Cryptography**.

KEYWORDS

Card-based cryptography, Secure computation, Real-life hands-on cryptography, Copy protocols

ACM Reference Format:
Hiroto Koyama, Kodai Toyoda, Daiki Miyahara, and Takaaki Mizuki. 2021. New Card-based Copy Protocols Using Only Random Cuts. In *Proceedings of the 8th ACM ASIA Public-Key Cryptography Workshop (APKC '21), June 7, 2021, Virtual Event, Hong Kong*. ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3457338.3458297

1 INTRODUCTION

Card-based cryptography enables us to perform cryptographic tasks, such as secure multiparty computations, using a deck of physical cards. Typically, a "two-colored deck" of cards or a "standard deck" of cards is used in a card-based protocol. This paper begins with introducing these two types of decks in Sections 1.1 and 1.2.

1.1 Two-Colored Deck of Cards

Many card-based protocols use a *two-colored deck* of cards, which consists of black cards $\boxed{\clubsuit}$ and red cards $\boxed{\heartsuit}$ whose backs are all identical $\boxed{?}$ (refer to [8, 18, 35] for a survey).

Depending on the order of two cards of different colors, a Boolean value is represented as follows:

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

Based on the above encoding rule, a player can commit his or her private bit $x \in \{0, 1\}$ by placing two cards face down, keeping its value hidden:

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

We call such a pair of face-down cards a *commitment* to x.

1.2 Standard Deck of Cards

Some card-based protocols [9, 10, 16, 24] work on a *standard deck* of cards, which consists of 52 cards (except for jokers) and each card has a unique pattern (suit and number) on its face: We regard it as a total order on $\{1, 2, \ldots, 52\}$ and assume a deck consisting of 52 numbered cards:

$$\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots\boxed{51}\boxed{52},$$

where the backs of all cards are identical $\boxed{?}$.

Similar to the encoding rule (1), Niemi and Renvall [24] considered an encoding rule based on which of two cards is smaller: Define

$$\boxed{i}\boxed{j} = 0, \quad \boxed{j}\boxed{i} = 1 \tag{2}$$

for any two cards $\boxed{i}$ and $\boxed{j}$ with $1 \leq i < j \leq 52$. Thus, if the left card is smaller, it represents 0, and if the left card is larger, it represents 1. Throughout this paper, we denote a *commitment* to

$x \in \{0, 1\}$ consisting of two numbered cards $\boxed{i}\,\boxed{j}$ by

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

where we call such a set $\{i, j\}$ the *base* of the commitment. For example,

$$\underbrace{\boxed{?}\,\boxed{?}}_{[x]^{\{3,4\}}}$$

is a commitment of base $\{3, 4\}$; when we turn over these two cards, the order $\boxed{3}\,\boxed{4}$ implies $x = 0$, and $\boxed{4}\,\boxed{3}$ implies $x = 1$.

1.3 The History of Copy Protocols

This paper mainly deals with *copy protocols*; given a commitment to $a \in \{0, 1\}$, a copy protocol is supposed to make two identical copied commitments to the bit a:

$$\underbrace{\boxed{?}\,\boxed{?}}_{a} \to \cdots \to \underbrace{\boxed{?}\,\boxed{?}}_{a}\ \underbrace{\boxed{?}\,\boxed{?}}_{a};$$
$$\underbrace{\boxed{?}\,\boxed{?}}_{[a]^{\{i,j\}}} \to \cdots \to \underbrace{\boxed{?}\,\boxed{?}}_{[a]^{\{i_1,j_1\}}}\ \underbrace{\boxed{?}\,\boxed{?}}_{[a]^{\{i_2,j_2\}}}.$$

A copy protocol plays an important role in securely computing an arbitrary Boolean function (as well as AND/OR/XOR/NOT protocols do), and hence, it is one of the most important primitives studied in card-based cryptography [2, 7, 11, 16, 19, 24–26].

Here, we illustrate the necessity of a copy protocol with a concrete function example. Consider a secure computation of the five-input majority function, whose possible circuit is:

$$\begin{aligned}\mathrm{maj}(a, b, c, d, e) = {} & (a \wedge b \wedge c) \vee (a \wedge b \wedge d) \vee (a \wedge b \wedge e) \\ & \vee (a \wedge c \wedge d) \vee (a \wedge c \wedge e) \vee (a \wedge d \wedge e) \vee (b \wedge c \wedge d) \\ & \vee (b \wedge c \wedge e) \vee (b \wedge d \wedge e) \vee (c \wedge d \wedge e).\end{aligned}$$

Since the bit a appears six times in the above equation, we need six commitments to a in total to compute the function according to the circuit (the same is true for the other bits). Therefore, to begin with, we need to perform a copy protocol to duplicate the commitments. Thus, copy protocols are indispensable.

In the literature, there are several copy protocols as shown in Tables 1 and 2, in which we show their numbers of required cards, those of required shuffles, and types of shuffles they use.

The first copy protocol was proposed by Crèpeau and Kilian [2] working on a two-colored deck of cards. This protocol uses the "random cut (RC)" (denoted by $\langle\cdot\rangle$), which is a cyclic shuffling operation. Although the details will be given in Section 2.2, we take a sequence of six cards to illustrate: after applying a random cut, the resulting sequence becomes one of the six cases with the equal probability (i.e., 1/6) as follows:

$$\left\langle \overset{1\ 2\ 3\ 4\ 5\ 6}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}} \right\rangle \to \left\{ \begin{array}{l} \overset{1\ 2\ 3\ 4\ 5\ 6}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{2\ 3\ 4\ 5\ 6\ 1}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{3\ 4\ 5\ 6\ 1\ 2}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{4\ 5\ 6\ 1\ 2\ 3}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{5\ 6\ 1\ 2\ 3\ 4}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{6\ 1\ 2\ 3\ 4\ 5}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}. \end{array} \right.$$

The Crèpeau–Kilian copy protocol [2] takes a commitment to $a \in \{0, 1\}$ and six additional cards as input, and outputs two commitments to the bit a after applying the random cut twice without leaking any information about the value of the bit a:

$$\underbrace{\boxed{?}\,\boxed{?}}_{a}\ \boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit} \to \cdots \to \underbrace{\boxed{?}\,\boxed{?}}_{a}\ \underbrace{\boxed{?}\,\boxed{?}}_{a}.$$

In 2009, Mizuki and Sone [19] introduced a new shuffling method, called the "random bisection cut (RBC)" (denoted by $[\cdot|\cdot]$), which bisects a sequence of cards and shuffles these two halves at random. Although the details will be given in Section 2.3, taking a sequence of six cards as an example, after applying a random bisection cut, the resulting sequence becomes either of the two cases with the equal probability (i.e., 1/2) as follows:

$$\left[\overset{1\ 2\ 3}{\boxed{?}\boxed{?}\boxed{?}} \middle| \overset{4\ 5\ 6}{\boxed{?}\boxed{?}\boxed{?}} \right] \to \left\{ \begin{array}{l} \overset{1\ 2\ 3\ 4\ 5\ 6}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{4\ 5\ 6\ 1\ 2\ 3}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}. \end{array} \right.$$

Making use of the random bisection cut, the Mizuki-Sone copy protocol [19] uses only six cards (including an input commitment) and only one shuffle:

$$\underbrace{\boxed{?}\,\boxed{?}}_{a}\ \boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit} \to \cdots \to \underbrace{\boxed{?}\,\boxed{?}}_{a}\ \underbrace{\boxed{?}\,\boxed{?}}_{a}.$$

In 2015, Nishimura et al. [25, 26] designed a five-card copy protocol that requires an average of two shuffles. Their protocol uses an unfamiliar shuffling operation, namely the "unequal division shuffle (UDS)," as follows:

$$\left[\overset{1\ 2}{\boxed{?}\boxed{?}} \middle| \overset{3\ 4\ 5}{\boxed{?}\boxed{?}\boxed{?}} \right] \to \left\{ \begin{array}{l} \overset{1\ 2\ 3\ 4\ 5}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}, \\ \overset{3\ 4\ 5\ 1\ 2}{\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}}. \end{array} \right.$$

It is not easy for humans to implement this shuffle (without any special auxiliary tools).

Let us shift our attention to the case of a standard deck of cards; there are two existing copy protocols. In 1999, Niemi and Renvall [24] proposed the first copy protocol using a standard deck of cards, which uses six cards and needs 5.5 random cuts on average:

$$\underbrace{\boxed{?}\,\boxed{?}}_{[a]^{\{1,2\}}}\ \boxed{3}\boxed{4}\boxed{5}\boxed{6} \to \cdots \to \underbrace{\boxed{?}\,\boxed{?}}_{[a]^{\{1,2\}}}\ \underbrace{\boxed{?}\,\boxed{?}}_{[a]^{\{3,4\}}}.$$

In 2016, making use of the random bisection cut, Mizuki [16] proposed a six-card copy protocol that requires only one random bisection cut.

Table 1: Copy protocols on a two-colored deck of cards

	# of cards	# of shuffles	Type of shuffles
Crépeau–Kilian [2]	8	2	RC
Mizuki–Sone [19]	6	1	RBC
Nishimura et al. [25]	5	2 (exp)	UDS
Ours	**6**	**3 (exp)**	**RC**

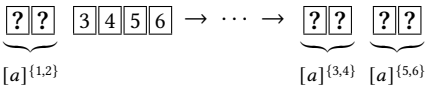
Table 2: Copy protocols on a standard deck of cards

	# of cards	# of shuffles	Type of shuffles
Niemi–Renvall [24]	6	5.5 (exp)	RC
Mizuki [16]	6	1	RBC
Ours	**6**	**3 (exp)**	**RC**

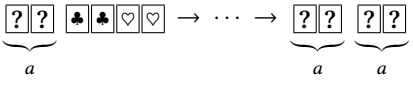
1.4 Contribution

As mentioned above, there are several kinds of shuffles, and they contribute to improving the efficiency of copy protocols (in terms of the numbers of cards and shuffles). Now, let us compare these shuffling operations from the perspective of practicality when implementing them. While a random bisection cut and an unequal division shuffle require auxiliary tools, such as special card cases, to be performed securely [26, 40], a random cut requires no such an auxiliary tool. Therefore, a random cut is superior to the other shuffling operations in terms of practicality. This implies that seeking a more efficient protocol using only random cuts is a meaningful challenge in the research area of card-based cryptography. It should be noted that Koch and Walzer [12] proposed actively secure protocols depending only on random cuts and they implied that finding card-minimal protocols using only random cuts is an interesting open problem.

In this paper, focusing on using only random cuts, we propose two new copy protocols which are more efficient than the existing ones. Specifically, we first work on a standard deck of cards and design a six-card copy protocol using three random cuts on average:



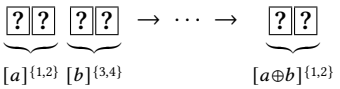
Since the previous protocol, namely the Niemi–Renvall copy protocol [24], uses 5.5 random cuts as mentioned before, our protocol improves on it. See Table 2 again. Next, we shift our attention to the case of a two-colored deck of cards, and construct a six-card copy protocol using three random cuts on average:



Since the Crèpeau–Kilian copy protocol [2] uses eight cards and two random cuts (as mentioned before), our protocol uses two cards fewer than the previous protocol (although it requires one more shuffle). See Table 1 again.

We will prove the correctness and security of our proposed protocols by using the *KWH-tree* (whose idea and notion were invented in [13]), from which we can visually confirm state transitions of the protocols.

In addition to the two new copy protocols, we provide a new XOR protocol working on a standard deck without any additional card, such as:



This is a card-minimal protocol and is the first construction of an XOR protocol using only one random cut.

1.5 Related Work

To the best of our knowledge, no recent literature has studied elementary card-based protocols using only random cuts except for Toyoda et al. in 2020 [39]; they proposed a six-card XOR protocol using only random cuts, improving the existing ones [2, 20]. Apart from secure computations of logical functions, card-based protocols have attractive applications such as solving Yao's millionaires' problem [15, 22, 23, 27, 38], zero-knowledge proof protocols for pencil puzzles [31–34], secure grouping [4] and lottery [37], generating a derangement [5, 6, 21], and efficient secure multi-valued function evaluation using dihedral symmetry [36]. Instead of using shuffles, card-based protocols relying on private operations have been studied [1, 14, 28–30, 42, 43]. Recently, the relationship between card-based protocols and the (conventional) computational complexity was discussed [3].

1.6 Outline

The remainder of this paper is organized as follows. In Section 2, we introduce a formal description of actions and the notions of two kinds of shuffles. In Section 3, we present our copy protocol on a standard deck. In Section 4, we present our copy protocol on a two-colored deck. In Section 5, we present our XOR protocol on a standard deck. We conclude this paper in Section 6.

2 PRELIMINARIES

In this section, we first present a formal treatment of actions appearing in card-based protocols (which has been developed in [7, 17, 18]).

Then, we introduce two important kinds of shuffles, i.e., the random cut and the random bisection cut.

2.1 Actions

Assume that we have a sequence of n face-down cards on a table:

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{n}{\boxed{?}},$$

where we attach the number i, $1 \le i \le n$, to the i-th card (from the left) for convenience sake. Let S_n denote the symmetric group of degree n. We present four actions, as follows.

Permuting. Apply a permutation $\pi \in S_n$ to the sequence of n cards. We denote this action by (perm, π):

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

Turning. Turn over all cards whose positions are in $T \subseteq \{1, \dots, n\}$ to check the numbers or colors of the cards: We denote this action by (turn, T). For instance, if $T = \{t\}$,

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{t}{\boxed{?}}\cdots\overset{n}{\boxed{?}} \xrightarrow{(\mathsf{turn},\{t\})} \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{t}{\boxed{3}}\cdots\overset{n}{\boxed{?}};$$
$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{t}{\boxed{?}}\cdots\overset{n}{\boxed{?}} \xrightarrow{(\mathsf{turn},\{t\})} \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{t}{\boxed{\heartsuit}}\cdots\overset{n}{\boxed{?}}.$$

Shuffle. Apply a permutation $\pi \in \Pi$ chosen uniformly randomly from a permutation set $\Pi \subseteq S_n$. We denote this action by (shuf, Π):

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

Note that nobody can know which permutation in Π was applied. In the next two subsections, we show two specific kinds of shuffles.

Result. Specify positions of output commitments. In a copy protocol, $(\mathsf{result}, (i_1, i_2), (j_1, j_2))$ means that two copied commitments are obtained at the corresponding positions:

$$\overset{1}{\boxed{?}}\cdots\overset{i_1}{\boxed{?}}\cdots\overset{i_2}{\boxed{?}}\cdots\overset{j_1}{\boxed{?}}\cdots\overset{j_2}{\boxed{?}}\cdots\overset{n}{\boxed{?}}$$
$$\xrightarrow{(\mathsf{result},(i_1,i_2),(j_1,j_2))} \underbrace{\overset{i_1}{\boxed{?}}\overset{i_2}{\boxed{?}}}_{a}\ \underbrace{\overset{j_1}{\boxed{?}}\overset{j_2}{\boxed{?}}}_{a}.$$

Note that, technically, the order of i_1, i_2, j_1, j_2 can be arbitrary.

2.2 Random Cut

As seen in the previous subsection, a shuffle is mathematically defined by giving a permutation set Π. In this sense, we can consider *any* shuffles. However, when constructing practical card-based protocols, it is crucial how easy-to-implement the shuffles to be used are.

The simplest and most easy-to-implement shuffle is the *random cut (RC)*, denoted by $\langle\cdot\rangle$, that shifts a sequence of cards cyclically and randomly. If a random cut is applied to a sequence of n cards, then the resulting sequence becomes one of the following n sequences, each of which occurs with a probability of $1/n$:

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

This random cut is formally described as

$$(\mathsf{shuf}, \{\mathsf{id}, \pi, \pi^2, \dots, \pi^{n-1}\})$$

for a cyclic permutation $\pi = (1\,2\,3\,\cdots\,n)$, where $\mathsf{id} \in S_n$ denotes the identity permutation.

In the sequel, we use $\mathsf{RC}_{1,2,\dots,n}$ to represent $\{\mathsf{id}, \pi, \pi^2, \dots, \pi^{n-1}\}$. For example, $(\mathsf{shuf}, \mathsf{RC}_{1,2,3,4,5,6})$ is a random cut to a sequence of six face-down cards:

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

A random cut can be easily performed by human hands; a secure implementation called the Hindu cut is well known [40, 41].

2.3 Random Bisection Cut

The *random bisection cut (RBC)* is another major shuffle action invented in 2009 [19]. This shuffle, denoted by $[\cdot|\cdot]$, bisects a sequence of $2n$ cards and randomly swaps the two halves; the resulting sequence becomes one of the following two sequences:

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

That is, the resulting sequence either remains the same as the original one, or becomes a sequence such that the two halves are swapped with a probability of $1/2$. This random bisection can be expressed as

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

A few secure implementations of a random bisection cut were shown in [40]. One is a method called the spinning throw using a rubber band and a separator. In this method, a separator is put in the middle of a sequence of cards so that the sequence is bisected, and the separator and the two halves are fixed by using a rubber band. Then, they are thrown in a spinning manner so that the two halves are shuffled randomly. Another method employs the vertical asymmetricity of the backs of cards and reduces applying a random bisection cut to applying a random cut.

3 COPY PROTOCOL ON STANDARD DECK

In this section, working on a standard deck of cards, we present a new copy protocol that uses only three random cuts (on average).

In Section 3.1, we provide a basic technique: We show that a random bisection cut (RBC) with opening leading cards can be conducted via a series of random cuts (RCs) if we are working on a standard deck. Applying this basic technique, we construct our copy

protocol in Section 3.2, followed by its pseudocode in Section 3.3. We prove that our protocol is correct and secure in Section 3.4.

3.1 Basic Technique: RBC and Opening Leading Cards via RCs

Assume that we have $2n$ face-down cards (of a standard deck) whose first and $(n+1)$-st cards are $\boxed{i}\boxed{j}$ or $\boxed{j}\boxed{i}$ and that we want to reveal the first card after applying a random bisection cut:

$$\overset{1}{\boxed{?}}\cdots\overset{n}{\boxed{?}}\overset{n+1}{\boxed{?}}\cdots\overset{2n}{\boxed{?}} \to \left[\boxed{?}\cdots\boxed{?}\middle|\boxed{?}\cdots\boxed{?}\right] \to \underbrace{\boxed{?}}_{\text{reveal}}\cdots\boxed{?}\boxed{?}\cdots\boxed{?}. \quad (3)$$

We assume that everyone knows that the $2n$ cards consist of cards numbered 1 through $2n$, and hence, $1 \le i \ne j \le 2n$.

As mentioned in Section 2.3, secure implementations of a random bisection cut are known [40] under certain constraints. For commercially available standard decks of cards, however, the back of every card is often vertically symmetric, i.e., a secure implementation using the vertical asymmetricity of the backs does not work. Moreover, it might happen that no auxiliary tool such as a rubber band is available.

Fortunately, we can consider the following (partial) implementation of a random bisection cut via the random cut.

1. Apply a random cut to the sequence of $2n$ cards:
$$\left\langle\overset{1}{\boxed{?}}\cdots\overset{n}{\boxed{?}}\overset{n+1}{\boxed{?}}\cdots\overset{2n}{\boxed{?}}\right\rangle \to \underbrace{\boxed{?}\cdots\cdots\boxed{?}}_{2n}.$$
2. Turn over the first card. If it is $\boxed{i}$ or $\boxed{j}$, this means that a random bisection cut was applied to the sequence, i.e., we have achieved the goal (3). Otherwise, turn the first card face down, and return to Step 1. Note that this step leaks no information because the revealed card is chosen uniformly from the sequence of $2n$ cards at random.

Note that the expected number of random cuts for finishing the above procedure is n.

More usefully, along with $2n$ cards, if we have a commitment which we want to reveal after shuffling, the goal (3) can be achieved using random cuts as follows.

1. Assume that we have a commitment to $a \in \{0,1\}$ whose base is $\{1,2\}$. Place the commitment and the sequence of $2n$ cards as follows:
$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{1,2\}}}\overset{1}{\boxed{?}}\cdots\overset{n}{\boxed{?}}\overset{n+1}{\boxed{?}}\cdots\overset{2n}{\boxed{?}}.$$
Note that the sequence of $2n$ cards contains neither $\boxed{1}$ nor $\boxed{2}$.
2. Move the right card of the commitment to the middle as follows:
$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{1,2\}}}\overset{1}{\boxed{?}}\cdots\overset{n}{\boxed{?}}\overset{n+1}{\boxed{?}}\cdots\overset{2n}{\boxed{?}} \to \overset{1}{\boxed{?}}\cdots\overset{n}{\boxed{?}}\boxed{?}\overset{n+1}{\boxed{?}}\cdots\overset{2n}{\boxed{?}}.$$
3. Apply a random cut to the sequence of all cards:
$$\left\langle\overset{1}{\boxed{?}}\boxed{?}\cdots\overset{n}{\boxed{?}}\boxed{?}\overset{n+1}{\boxed{?}}\cdots\overset{2n}{\boxed{?}}\right\rangle \to \underbrace{\boxed{?}\cdots\cdots\boxed{?}}_{2n+2\text{ cards}}.$$
4. Turn over the first card; if it is $\boxed{1}$ or $\boxed{2}$, reveal the $(n+2)$-nd card (i.e., the other card constituting the commitment to a) as well. Otherwise, return to Step 3.

Since the probability of returning to Step 3 in Step 4 is $\frac{1}{n+1}$, the expected number of required shuffles is $n+1$.

Using this technique, we can simulate the six-card copy protocol invented by Mizuki [16], which uses a random bisection cut once, so that we obtain a six-card copy protocol using only random cuts, as seen in the next subsection.

3.2 Protocol Description

Now, we are ready to present our copy protocol on a standard deck. Given a commitment to $a \in \{0,1\}$ whose base is $\{1,2\}$ along with four additional cards $\boxed{3}\boxed{4}\boxed{5}\boxed{6}$, our copy protocol outputs two commitments to a whose bases are $\{3,4\}$ and $\{5,6\}$:

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{1,2\}}}\boxed{3}\boxed{4}\boxed{5}\boxed{6} \to \cdots \to \underbrace{\boxed{?}\boxed{?}}_{[a]^{\{3,4\}}}\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{5,6\}}}.$$

The protocol proceeds as follows.

1. Apply the technique shown in Section 3.1 to the commitment to a and the sequence of additional four cards, as follows.
   (a) Rearrange the sequence:
   $$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}} \to \overset{1}{\boxed{?}}\overset{3}{\boxed{?}}\overset{5}{\boxed{?}}\overset{2}{\boxed{?}}\overset{4}{\boxed{?}}\overset{6}{\boxed{?}}.$$
   (b) Apply a random cut to the sequence of all cards:
   $$\left\langle\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\right\rangle \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$
   (c) Turn over the first card; if it is $\boxed{1}$, swap the third and fifth cards. If it is $\boxed{2}$, apply a permutation (2 3 6 5). Otherwise, return to Step 1(b).
2. Then we have
$$\boxed{1}\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{3,4\}}}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{5,6\}}} \text{ or } \boxed{2}\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{3,4\}}}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{5,6\}}}.$$

Thus, our copy protocol uses three random cuts on average. Note that Step 1(c) rearranges the cards so that they are in order; in the pseudocode below, we will omit this rearrangement.

3.3 Pseudocode

In this subsection, we show a pseudocode for our copy protocol described in Section 3.2.

---

input set:

$$\left\{\left(\frac{?}{1},\frac{?}{2},\frac{?}{3},\frac{?}{4},\frac{?}{5},\frac{?}{6}\right),\left(\frac{?}{2},\frac{?}{1},\frac{?}{3},\frac{?}{4},\frac{?}{5},\frac{?}{6}\right)\right\}$$

(perm, (2 4 5 3))
1 (shuf, $\mathsf{RC}_{1,2,3,4,5,6}$)
(turn, {1})

if visible seq. = $(1, ?, ?, ?, ?, ?)$ **then**
  (result, $(2, 5), (3, 6)$)
else if visible seq. = $(2, ?, ?, ?, ?, ?)$ **then**
  (result, $(5, 2), (6, 3)$)
else
  (turn, $\{1\}$)
  go to 1

3.4 Correctness and Security

In this subsection, we verify the correctness and security of the protocol presented in Section 3.2.

A copy protocol is said to be *correct* if, given an input commitment to a, it always produces two commitments to a. We say a protocol is *secure* if it leaks no information for any run of the protocol (in other words, random variables I and V denoting the inputs and the visible sequence trace, respectively, are stochastically independent, where the visible sequence trace means what can be observed on the table). See [13, 17, 18] for the more formal definitions based on abstract machine and information theory.

We describe the *KWH-tree* (which is a nice way of depicting a diagram developed by Koch, Walzer, and Härtel [13]) of our proposed protocol in Figure 2. In this figure, we call each box a *state*. The first state (box) in Figure 2 corresponds to an initial sequence, consisting of an input commitment and four additional cards; X_0 and X_1 represent the probabilities of $a = 0$ and $a = 1$, respectively. A polynomial annotating a card sequence in a state, such as $+1/6X_0$, represents the conditional probability that the current sequence is the one next to the polynomial, given the visible sequence trace observed so far on the table. The two states (boxes) at the bottom imply that two commitments to a are definitively obtained. Furthermore, in each state, the sum of all polynomials is equal to $X_0 + X_1$, implying that no information about a leaks, i.e., the inputs and visible sequence trace are stochastically independent.

Thus, the KWH-tree in Figure 1 guarantees that our proposed protocol is correct and secure. (As stated in [7], the KWH-tree is a witness for the correctness and security.)

4 COPY PROTOCOL ON TWO-COLORED DECK

In this section, we present a new copy protocol that uses only the random cut (three times on average) with a two-colored deck of cards. We show the description of our protocol in Section 4.1 and its pseudocode in Section 4.2. We verify the correctness and security of our protocol in Section 4.3.

4.1 Description

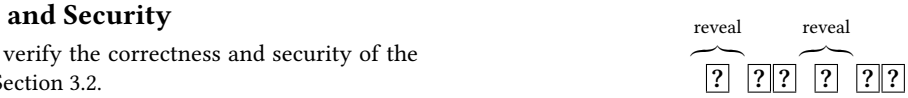
Here, we give the description of our copy protocol working on a two-colored deck.

1. Place a commitment to $a \in \{0, 1\}$ and four additional cards as follows:

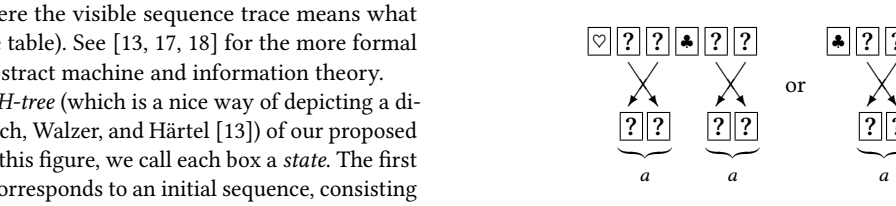
Then, turn over the four face-up cards:

2. Apply a random cut to the sequence of six cards:

3. Reveal the first and the fourth cards:



   (a) If ♡♡ or ♣♣ appears, then turn them face down and go back to Step 2.
   (b) If ♡♣ or ♣♡ appears, then we obtain two commitments to a as follows:



This is our copy protocol. As noticed, this protocol is very simple and takes an average of three random cuts to complete. Since the previous protocol using random cuts, i.e., the Crèpeau–Kilian copy protocol, requires six additional cards, our protocol is more efficient in this regard, although it uses one more shuffle (on average). See the bottom row in Table 1 again.

4.2 Pseudocode

The following is a pseudocode for our copy protocol.

input set:

$$\left\{\left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right), \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right)\right\}$$

1 (shuf, $\mathsf{RC}_{1,2,3,4,5,6}$)
  (turn, $\{1, 4\}$)
  if visible seq. = $(\heartsuit, ?, ?, \heartsuit, ?, ?)$ or $(\clubsuit, ?, ?, \clubsuit, ?, ?)$ **then**
    (turn, $\{1, 4\}$)
    go to 1
  else if visible seq. = $(\heartsuit, ?, ?, \clubsuit, ?, ?)$ or $(\clubsuit, ?, ?, \heartsuit, ?, ?)$ **then**
    (result, $(3, 2), (6, 5)$)

In the next subsection, we confirm that our protocol definitively produces two commitments to a without leaking any information about a.

4.3 Correctness and Security

We can show the correctness and security of this protocol in the same way as we did with a standard deck in Section 3.4. The KWH-tree in Figure 2 guarantees that our proposed protocol is correct and secure.

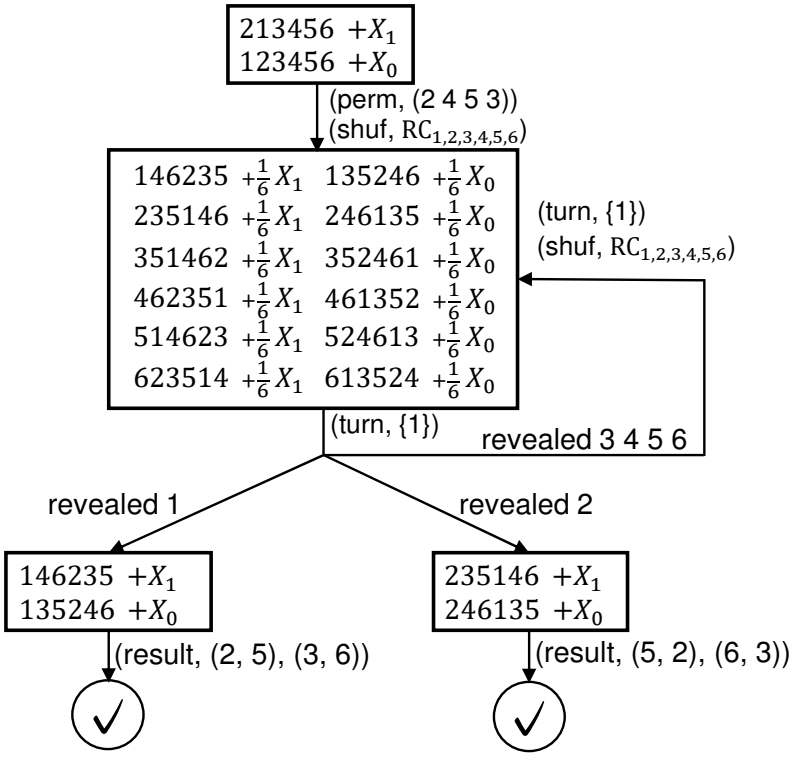


Figure 1: The KWH-tree of our six-card copy protocol on a standard deck

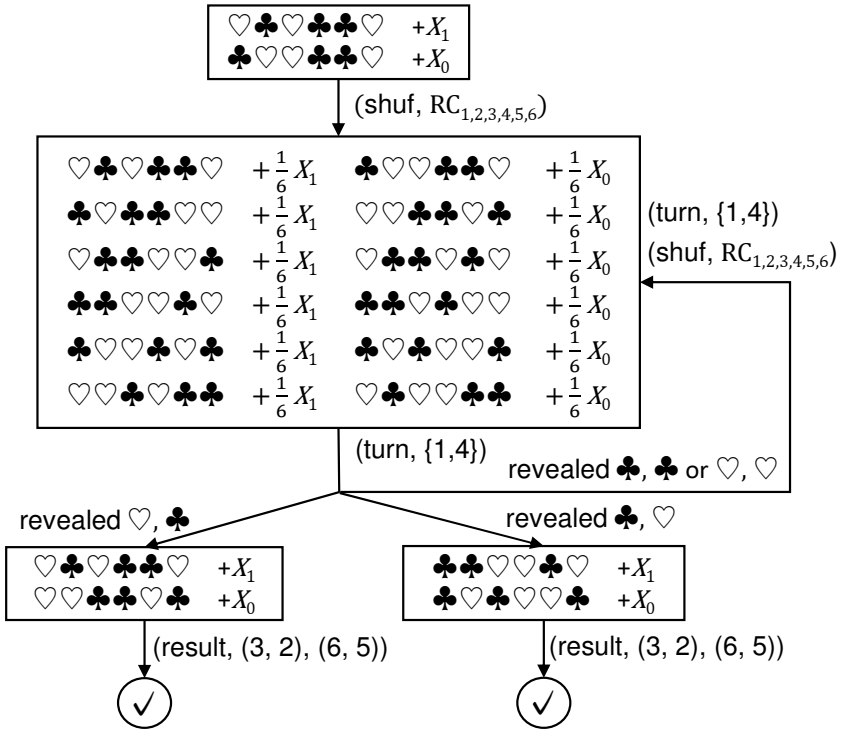


Figure 2: The KWH-tree of our six-card copy protocol on a two-colored deck

5 XOR PROTOCOL USING ONLY RANDOM CUT

In this section, going back to the standard-deck case, we construct a new XOR protocol by applying the idea behind the technique presented in Section 3.1. This makes it possible to perform a secure XOR computation where the number of cards and the number of shuffles are both minimized and the used shuffle is a random cut.

5.1 Protocol Description

Given two commitments to $a, b \in \{0, 1\}$, our protocol proceeds as follows.

1. Place the input commitments:
$$\underbrace{?\,?}_{[a]^{\{1,2\}}}\ \underbrace{?\,?}_{[b]^{\{3,4\}}}\ .$$
2. Rearrange the sequence:
$$\overset{1\ 2\ 3\ 4}{?\,?\,?\,?} \to \overset{1\ 3\ 2\ 4}{?\,?\,?\,?}\ .$$
3. Apply a random cut to the sequence of four cards:
$$\left\langle ?\,?\,?\,? \right\rangle \to ?\,?\,?\,?.$$
4. Turn over the first card. If it is $\boxed{1}$ or $\boxed{4}$, swap the second and third cards. If it is $\boxed{2}$ or $\boxed{3}$, permute the cards according to (2 4 3).
5. Then we have
$$1\,? \ \underbrace{?\,?}_{[a\oplus b]^{\{3,4\}}}\ ,\quad 2\,? \ \underbrace{?\,?}_{[a\oplus b]^{\{3,4\}}}\ ,$$
$$3\,? \ \underbrace{?\,?}_{[a\oplus b]^{\{1,2\}}}\ \text{or}\ \ 4\,? \ \underbrace{?\,?}_{[a\oplus b]^{\{1,2\}}}\ .$$

Thus, our protocol requires only one random cut and does not require any additional card. Since the existing XOR protocol using only random cuts, namely Niemi and Renvall's XOR protocol [24], requires an average of seven shuffles, as shown in Table 3, our protocol is superior to it. Furthermore, under the encoding rule (2), our protocol is optimal in terms of both the number of cards and the number of shuffles, and is no worse than the existing XOR protocol using a random bisection cut proposed by Mizuki [16].

5.2 Pseudocode

The following is a pseudocode for our XOR protocol on a standard deck.

---

input set:

$$\left\{\left(\frac{?}{2},\frac{?}{1},\frac{?}{4},\frac{?}{3}\right),\left(\frac{?}{2},\frac{?}{1},\frac{?}{3},\frac{?}{4}\right),\left(\frac{?}{1},\frac{?}{2},\frac{?}{4},\frac{?}{3}\right),\left(\frac{?}{1},\frac{?}{2},\frac{?}{3},\frac{?}{4}\right)\right\}$$

(perm, (2 3))
(shuf, $\mathsf{RC}_{1,2,3,4}$)
(turn, {1})
if visible seq. = (1, ?, ?, ?) or (4, ?, ?, ?) **then**
  (perm, (2 3))
else if visible seq. = (2, ?, ?, ?) or (3, ?, ?, ?)**then**
  (perm, (2 4 3))
(result, (3, 4))

5.3 Correctness and Security

We can show the correctness and security of this protocol in the same way as we did thus far. The KWH-tree in Figure 3 guarantees that our proposed protocol is correct and secure. Note that, contrary to the previous XOR protocols [16, 24], the base of output commitment is not deterministic, i.e., is either $\{1, 2\}$ or $\{3, 4\}$.

6 CONCLUSION

In card-based cryptography, the random cut is believed to be the most easy-to-implement shuffle, and hence, card-based protocols that rely only on random cuts are much preferable. In this paper, we have constructed three new protocols using only random cuts as shuffle actions.

Specifically, the first protocol is a six-card copy protocol working on a standard deck, and uses three random cuts on average. The second one is also a six-card copy protocol with three random cuts, working on a two-colored deck. The third one is a standard-deck XOR protocol using only one random cut without any additional card. Every protocol is superior to the existing ones in terms of the number of cards or shuffles.

Because our copy protocols produce two copied commitments, an intriguing open problem is to extend our results to constructing copy protocols which generate more than two copied commitments. Note that our protocol presented in Section 3 can be generalized (based on the basic technique shown in Section 3.1) although it would increase the expected number of shuffles. In particular, to make k copied commitments, we use $2k$ additional cards and $k + 1$ shuffles (on average).

ACKNOWLEDGMENTS

We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. This work was supported in part by JSPS KAKENHI Grant Number JP19J21153.

REFERENCES

[1] Yoshiki Abe, Mitsugu Iwamoto, and Kazuo Ohta. 2020. How to Detect Malicious Behaviors in a Card-Based Majority Voting Protocol with Three Inputs. In *2020 International Symposium on Information Theory and Its Applications (ISITA)*. 377–381. https://doi.org/10.34385/proc.65.C01-9

[2] Claude Crépeau and Joe Kilian. 1994. Discreet Solitary Games. In *Advances in Cryptology—CRYPTO' 93 (LNCS, Vol. 773)*, Douglas R. Stinson (Ed.). Springer, Berlin, Heidelberg, 319–330. https://doi.org/10.1007/3-540-48329-2_27

[3] Pavel Dvořák and Michal Koucký. 2021. Barrington Plays Cards: The Complexity of Card-based Protocols. In *Theoretical Aspects of Computer Science (LIPIcs, Vol. 187)*, Markus Bläser and Benjamin Monmege (Eds.). Schloss Dagstuhl, Dagstuhl, 26:1–26:17. https://doi.org/10.4230/LIPIcs.STACS.2021.26

[4] Yuji Hashimoto, Koji Nuida, Kazumasa Shinagawa, Masaki Inamura, and Goichiro Hanaoka. 2018. Toward Finite-Runtime Card-Based Protocol for Generating a Hidden Random Permutation without Fixed Points. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E101.A, 9 (2018), 1503–1511. https://doi.org/10.1587/transfun.E101.A.1503

[5] T. Ibaraki and Y. Manabe. 2016. A More Efficient Card-Based Protocol for Generating a Random Permutation without Fixed Points. In *Mathematics and Computers in Sciences and in Industry (MCSI)*. 252–257. https://doi.org/10.1109/MCSI.2016.054

[6] Rie Ishikawa, Eikoh Chida, and Takaaki Mizuki. 2015. Efficient Card-Based Protocols for Generating a Hidden Random Permutation Without Fixed Points. In *Unconventional Computation and Natural Computation (LNCS, Vol. 9252)*,

Table 3: XOR protocols on a standard deck of cards

	# of cards	# of shuffles	Type of shuffles
Niemi–Renvall [24]	4	7 (exp)	RC
Mizuki [16]	4	1	RBC
Ours	4	1	**RC**

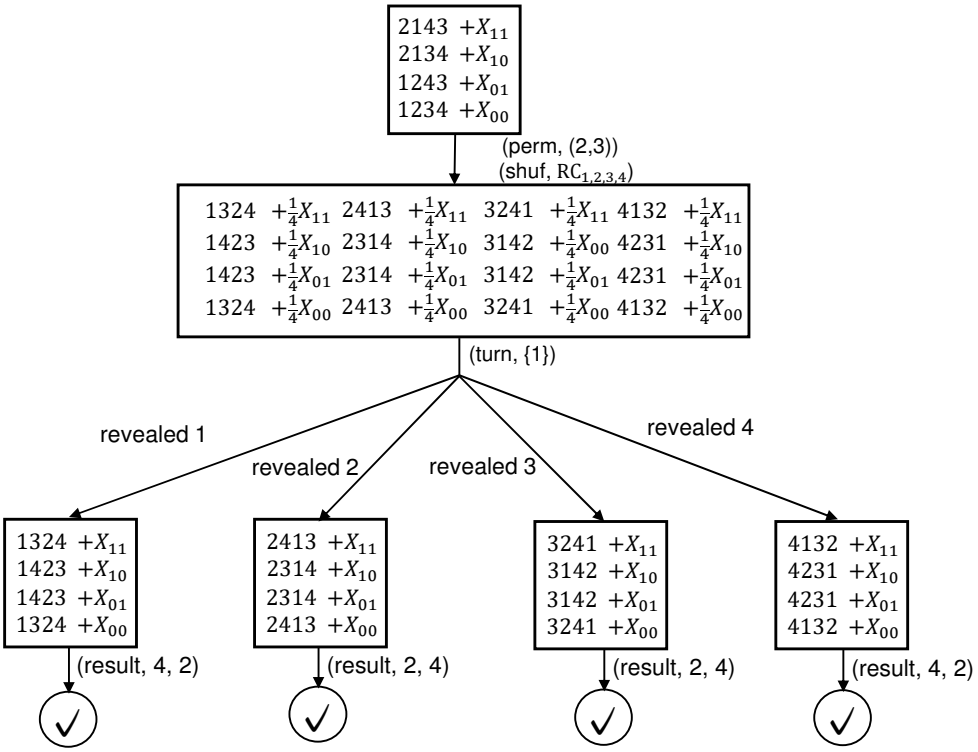


Figure 3: The KWH-tree of our four-card XOR protocol on standard deck

Cristian S. Calude and Michael J. Dinneen (Eds.). Springer, Cham, 215–226. https://doi.org/10.1007/978-3-319-21819-9_16

[7] Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2017. The Minimum Number of Cards in Practical Card-Based Protocols. In *Advances in Cryptology—ASIACRYPT 2017 (LNCS, Vol. 10626)*, Tsuyoshi Takagi and Thomas Peyrin (Eds.). Springer, Cham, 126–155. https://doi.org/10.1007/978-3-319-70700-6_5

[8] Alexander Koch. 2019. *Cryptographic Protocols from Physical Assumptions.* Ph.D. Dissertation. Karlsruhe Institute of Technology. https://doi.org/10.5445/IR/1000097756

[9] Alexander Koch, Michael Schrempp, and Michael Kirsten. 2019. Card-Based Cryptography Meets Formal Verification. In *Advances in Cryptology–ASIACRYPT 2019 (LNCS, Vol. 11921)*, Steven D. Galbraith and Shiho Moriai (Eds.). Springer, Cham, 488–517. https://doi.org/10.1007/978-3-030-34578-5_18

[10] Alexander Koch, Michael Schrempp, and Michael Kirsten. 2021. Card-based cryptography meets formal verification. *New Gener. Comput.* 39, 1 (2021), 115–158. https://doi.org/10.1007/s00354-020-00120-0

[11] Alexander Koch and Stefan Walzer. 2018. Private Function Evaluation with Cards. Cryptology ePrint Archive, Report 2018/1113. https://eprint.iacr.org/2018/1113.

[12] Alexander Koch and Stefan Walzer. 2020. Foundations for Actively Secure Card-Based Cryptography. In *Fun with Algorithms (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 157)*, Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara (Eds.). Schloss Dagstuhl, Dagstuhl, Germany, 17:1–17:23. https://doi.org/10.4230/LIPIcs.FUN.2021.17

[13] Alexander Koch, Stefan Walzer, and Kevin Härtel. 2015. Card-Based Cryptographic Protocols Using a Minimal Number of Cards. In *Advances in Cryptology—ASIACRYPT 2015 (LNCS, Vol. 9452)*, Tetsu Iwata and Jung Hee Cheon (Eds.). Springer, Berlin, Heidelberg, 783–807. https://doi.org/10.1007/978-3-662-48797-6_32

[14] Yoshifumi Manabe and Hibiki Ono. 2021. Secure Card-Based Cryptographic Protocols Using Private Operations Against Malicious Players. In *Innovative Security Solutions for Information Technology and Communications (LNCS, Vol. 12596)*, Diana Maimut, Andrei-George Oprina, and Damien Sauveron (Eds.). Springer, Cham, 55–70. https://doi.org/10.1007/978-3-030-69255-1_5

[15] Daiki Miyahara, Yu ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2020. Practical card-based implementations of Yao's millionaire protocol. *Theor. Comput. Sci.* 803 (2020), 207–221. https://doi.org/10.1016/j.tcs.2019.11.005

[16] Takaaki Mizuki. 2016. Efficient and Secure Multiparty Computations Using a Standard Deck of Playing Cards. In *Cryptology and Network Security (LNCS, Vol. 10052)*, Sara Foresti and Giuseppe Persiano (Eds.). Springer, Cham, 484–499. https://doi.org/10.1007/978-3-319-48965-0_29

[17] Takaaki Mizuki and Hiroki Shizuya. 2014. A formalization of card-based cryptographic protocols via abstract machine. *Int. J. Inf. Secur.* 13, 1 (2014), 15–23. https://doi.org/10.1007/s10207-013-0219-4

[18] Takaaki Mizuki and Hiroki Shizuya. 2017. Computational Model of Card-Based Cryptographic Protocols and Its Applications. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E100.A, 1 (2017), 3–11. https://doi.org/10.1587/transfun.E100.A.3

[19] Takaaki Mizuki and Hideaki Sone. 2009. Six-Card Secure AND and Four-Card Secure XOR. In *Frontiers in Algorithmics (LNCS, Vol. 5598)*, Xiaotie Deng, John E. Hopcroft, and Jinyun Xue (Eds.). Springer, Berlin, Heidelberg, 358–369. https://doi.org/10.1007/978-3-642-02270-8_36

[20] Takaaki Mizuki, Fumishige Uchiike, and Hideaki Sone. 2006. Securely computing XOR with 10 cards. *The Australasian Journal of Combinatorics* 36 (2006), 279–293. https://ajc.maths.uq.edu.au/?page=get_volumes&volume=36

[21] Soma Murata, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. 2021. Efficient Generation of a Card-Based Uniformly Distributed Random Derangement. In *WALCOM: Algorithms and Computation (LNCS, Vol. 12635)*, Ryuhei Uehara, Seok-Hee Hong, and Subhas C. Nandy (Eds.). Springer, Cham, 78–89. https://doi.org/10.1007/978-3-030-68211-8_7

[22] Takeshi Nakai, Yuto Misawa, Yuuki Tokushige, Mitsugu Iwamoto, and Kazuo Ohta. 2021. How to Solve Millionaires' Problem with Two Kinds of Cards. *New Gener. Comput.* 39, 1 (2021), 73–96. https://doi.org/10.1007/s00354-020-00118-8

[23] Takeshi Nakai, Yuuki Tokushige, Yuto Misawa, Mitsugu Iwamoto, and Kazuo Ohta. 2016. Efficient Card-Based Cryptographic Protocols for Millionaires' Problem Utilizing Private Permutations. In *Cryptology and Network Security (LNCS, Vol. 10052)*, Sara Foresti and Giuseppe Persiano (Eds.). Springer, Cham, 500–517. https://doi.org/10.1007/978-3-319-48965-0_30

[24] Valtteri Niemi and Ari Renvall. 1999. Solitaire Zero-knowledge. *Fundam. Inf.* 38, 1,2 (1999), 181–188. https://doi.org/10.3233/FI-1999-381214

[25] Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2015. Five-Card Secure Computations Using Unequal Division Shuffle. In *Theory and Practice of Natural Computing (LNCS, Vol. 9477)*, Adrian-Horia Dediu, Luis Magdalena, and Carlos Martín-Vide (Eds.). Springer, Cham, 109–120. https://doi.org/10.1007/978-3-319-26841-5_9

[26] Akihiro Nishimura, Takuya Nishida, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2018. Card-based protocols using unequal division shuffles. *Soft Comput.* 22 (2018), 361–371. https://doi.org/10.1007/s00500-017-2858-2

[27] H. Ono and Y. Manabe. 2018. Efficient Card-Based Cryptographic Protocols for the Millionaires' Problem Using Private Input Operations. In *Asia Joint Conference on Information Security (AsiaJCIS)*. 23–28. https://doi.org/10.1109/AsiaJCIS.2018.00013

[28] Hibiki Ono and Yoshifumi Manabe. 2019. Card-Based Cryptographic Protocols with the Minimum Number of Cards Using Private Operations. In *Foundations and Practice of Security (LNCS, Vol. 11358)*, Nur Zincir-Heywood, Guillaume Bonfante, Mourad Debbabi, and Joaquin Garcia-Alfaro (Eds.). Springer, Cham, 193–207. https://doi.org/10.1007/978-3-030-18419-3_13

[29] Hibiki Ono and Yoshifumi Manabe. 2019. Card-Based Cryptographic Protocols with the Minimum Number of Rounds Using Private Operations. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology (LNCS, Vol. 11737)*, Cristina Pérez-Solà, Guillermo Navarro-Arribas, Alex Biryukov, and Joaquin Garcia-Alfaro (Eds.). Springer, Cham, 156–173. https://doi.org/10.1007/978-3-030-31500-9_10

[30] Hibiki Ono and Yoshifumi Manabe. 2021. Card-Based Cryptographic Logical Computations Using Private Operations. *New Gener. Comput.* 39, 1 (2021), 19–40. https://doi.org/10.1007/s00354-020-00113-z

[31] Suthee Ruangwises and Toshiya Itoh. 2020. Physical Zero-Knowledge Proof for Numberlink. In *Fun with Algorithms (Leibniz International Proceedings in Informatics (LIPIcs), Vol. 157)*, Martin Farach-Colton, Giuseppe Prencipe, and Ryuhei Uehara (Eds.). Schloss Dagstuhl, Dagstuhl, Germany, 22:1–22:11. https://doi.org/10.4230/LIPIcs.FUN.2021.22

[32] Suthee Ruangwises and Toshiya" Itoh. 2021. Physical Zero-Knowledge Proof for Numberlink Puzzle and k Vertex-Disjoint Paths Problem. *New Gener. Comput.* 39, 1 (2021), 3–17. https://doi.org/10.1007/s00354-020-00114-y

[33] Suthee Ruangwises and Toshiya Itoh. 2021. Physical Zero-Knowledge Proof for Ripple Effect. In *WALCOM: Algorithms and Computation (LNCS, Vol. 11737)*, Seokhee Hong, Subhas Nandy, and Ryuhei Uehara (Eds.). Springer, Cham, 296–307. https://doi.org/10.1007/978-3-030-68211-8_24

[34] Tatsuya Sasaki, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. 2020. Efficient card-based zero-knowledge proof for Sudoku. *Theor. Comput. Sci.* 839 (2020), 135–142. https://doi.org/10.1016/j.tcs.2020.05.036

[35] Kazumasa Shinagawa. 2020. *On the Construction of Easy to Perform Card-Based Protocols*. Ph.D. Dissertation. Tokyo Institute of Technology.

[36] Kazumasa Shinagawa. 2021. Card-based Cryptography with Dihedral Symmetry. *New Gener. Comput.* 39, 1 (2021), 41–71. https://doi.org/10.1007/s00354-020-00117-9

[37] Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone. 2021. Card-Based Covert Lottery. In *Innovative Security Solutions for Information Technology and Communications (LNCS, Vol. 12596)*, Diana Maimut, Andrei-George Oprina, and Damien Sauveron (Eds.). Springer, Cham, 257–270. https://doi.org/10.1007/978-3-030-69255-1_17

[38] Ken Takashima, Yuta Abe, Tatsuya Sasaki, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone. 2020. Card-based protocols for secure ranking computations. *Theor. Comput. Sci.* 845 (2020), 122–135. https://doi.org/10.1016/j.tcs.2020.09.008

[39] Kodai Toyoda, Daiki Miyahara, Takaaki Mizuki, and Hideaki Sone. 2020. Six-Card Finite-Runtime XOR Protocol with Only Random Cut. In *ACM Workshop on ASIA Public-Key Cryptography (APKC '20)*. ACM, New York, 2–8. https://doi.org/10.1145/3384940.3388961

[40] Itaru Ueda, Daiki Miyahara, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2020. Secure implementations of a random bisection cut. *Int. J. Inf. Secur.* 19, 4 (2020), 445–452. https://doi.org/10.1007/s10207-019-00463-w

[41] Itaru Ueda, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2016. How to Implement a Random Bisection Cut. In *Theory and Practice of Natural Computing (LNCS, Vol. 10071)*, Carlos Martín-Vide, Takaaki Mizuki, and Miguel A. Vega-Rodríguez (Eds.). Springer, Cham, 58–69. https://doi.org/10.1007/978-3-319-49001-4_5

[42] Y. Watanabe, Y. Kuroki, S. Suzuki, Y. Koga, M. Iwamoto, and K. Ohta. 2018. Card-Based Majority Voting Protocols with Three Inputs Using Three Cards. In *2018 International Symposium on Information Theory and Its Applications (ISITA)*. 218–222. https://doi.org/10.23919/ISITA.2018.8664324

[43] Kenji Yasunaga. 2020. Practical Card-Based Protocol for Three-Input Majority. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* E103.A, 11 (2020), 1296–1298. https://doi.org/10.1587/transfun.2020EAL2025