# Committed-Format AND Protocol Using Only Random Cuts[*]

Yuta Abe Takaaki Mizuki Hideaki Sone

Tohoku University

**Abstract**

In the research area of card-based cryptography, designing committed-format AND protocols that are efficient in terms of the number of required cards is a major topic. Such an AND protocol should receive two pairs of face-down (physical) cards representing two secret input bits, from which it should securely produce a pair of face-down cards representing the AND value of the two bits via a series of actions, such as shuffling and turning over cards, along with some helping cards. The number of required cards typically depends on allowed kinds of shuffling operations. This paper focuses on "RC-protocols" meaning to be able to use only the random cut (RC), which is the easiest shuffling operation to implement. The best committed-format AND RC-protocol currently known was devised by Stiglic in 2001, where eight cards are used (i.e., his protocol needs four helping cards). Since then, it has been an open question to determine whether there exists a committed-format AND RC-protocol using less than eight cards. In this study, we answer to the question: We propose a six-card committed-format AND RC-protocol (using exactly two random cuts). Therefore, we can reduce the number of required cards by two.

## 1 Introduction

Card-based cryptography provides us a practical method for performing secure multiparty computations using a deck of physical cards. A card-based protocol typically uses a two-colored deck of cards, such as $\boxed{\clubsuit}$ and $\boxed{\heartsuit}$, with their backs being $\boxed{?}$. A pair of cards of different colors is used to represent a Boolean value, as follows:

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

According to this encoding rule, a pair of face-down cards representing a bit $x \in \{0, 1\}$ is called a *commitment*, denoted by

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

In the research area of card-based cryptography, designing *committed-format AND protocols* that are efficient in terms of the number of required cards is a major topic. Such an AND protocol should receive two commitments

$$\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}$$

to $a, b \in \{0, 1\}$ as input, from which it should securely produce a commitment

$$\underbrace{\boxed{?}\boxed{?}}_{a \wedge b}$$

to the AND value $a \wedge b$ via a series of actions, such as shuffling and turning over cards, along with some helping cards. As an example of committed-format AND protocols, this paper begins with introducing Stiglic's AND protocol (Stiglic, 2001), which was devised in 2001.

[*] This is a post-peer-review, pre-copyedit version of an article published in Natural Computing. The final authenticated version is available online at: https://doi.org/10.1007/s11047-021-09862-2.

## 1.1 Stiglic's AND protocol

Given commitments to $a$ and $b$ along with four helping cards $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, Stiglic's AND protocol (Stiglic, 2001) proceeds as follows.

1. Place the two input commitments and the four helping cards, and turn over the face-up cards as:

$$\underbrace{\boxed{?}\boxed{?}}_{a}\boxed{\heartsuit}\boxed{\clubsuit}\underbrace{\boxed{?}\boxed{?}}_{b}\boxed{\clubsuit}\boxed{\heartsuit} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{a}\boxed{?}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{b}\boxed{?}\boxed{?}.$$

2. Apply a *random cut*, denoted by $\langle\cdot\rangle$, to the sequence of eight cards:

$$\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

The term random cut means a cyclic shuffle such that the sequence of cards will be shifted randomly with the offset being unknown to everyone. Thus, if we attach numbers to the cards for the sake of convenience:

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}}\overset{7}{\boxed{?}}\overset{8}{\boxed{?}},$$

then a random cut results in one of the following eight sequences (with a probability of 1/8):

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}}\overset{7}{\boxed{?}}\overset{8}{\boxed{?}},$$

$$\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}}\overset{7}{\boxed{?}}\overset{8}{\boxed{?}}\overset{1}{\boxed{?}},$$

$$\vdots$$

$$\overset{8}{\boxed{?}}\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}}\overset{7}{\boxed{?}}\ .$$

The random cut is considered to be one of the easiest shuffling operations to implement; a specific implementation of a random cut is the *Hindu cut* (Ueda et al., 2016).

3. Reveal the first two cards (from the left).

   (a) If the revealed cards are $\boxed{\heartsuit}\boxed{\heartsuit}$, then a commitment to $a \wedge b$ is obtained as follows:

$$\boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}\boxed{?}.$$

   (b) If the revealed cards are $\boxed{\clubsuit}\boxed{\clubsuit}$, then we obtain

$$\boxed{\clubsuit}\boxed{\clubsuit}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}\boxed{?}\boxed{?}\boxed{?}.$$

   (c) If the revealed cards are $\boxed{\clubsuit}\boxed{\heartsuit}$ or $\boxed{\heartsuit}\boxed{\clubsuit}$, turn over the third card.

      i. If the three face-up cards are $\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, we have

$$\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}\ .$$

      ii. If the three face-up cards are $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}$, we have

$$\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}\boxed{?}\boxed{?}.$$

iii. If the three face-up cards are $\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}$ or $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}$, turn them over and return to Step 2.

This is Stiglic's AND protocol, which uses the random cut in Step 2. Because the probability that Step 3–(c)–iii occurs and we go back to Step 2 is 1/2, the expected number of shuffles (namely, random cuts) is two. Thus, Stiglic's AND protocol is not a finite-runtime one but a Las Vegas algorithm.

## 1.2 The History of Committed-Format AND Protocols

As seen above, Stiglic's AND protocol uses a two-color deck of eight cards. Including this protocol, Table 1 enumerates all the existing committed-format AND protocols.

Table 1: Existing Committed-format AND protocols

| | Card | | Shuffle | Finite |
|---|---|---|---|---|
| | #Colors | #Cards | | |
| Crépeau–Kilian, 1993 (Crépeau and Kilian, 1994) | 4 | 10 | random cut | |
| Niemi–Renvall, 1998 (Niemi and Renvall, 1998) | 2 | 12 | random cut | |
| Stiglic, 2001 (Stiglic, 2001) | 2 | 8 | random cut | |
| Mizuki–Sone, 2009 (Mizuki and Sone, 2009) | 2 | 6 | random bisection cut | ✓ |
| Koch–Walzer–Härtel, 2015 (Koch et al., 2015) | 2 | 4 | includes non-uniform shuffle | |
| | 2 | 5 | includes non-uniform non-closed shuffle | ✓ |
| Abe–Mizuki–Sone, 2018 (Abe et al., 2018, 2021) | 2 | 5 | random cut + random bisection cut | |
| Koch, 2018 (Koch, 2018) | 2 | 4 | includes non-closed shuffle | |
| Ruangwises–Itoh, 2018 (Ruangwises and Itoh, 2019) | 2 | 5 | includes non-closed shuffle | ✓ |

As known from Table 1, there are several kinds of shuffles. Remember the random cut applied at Step 2 of Stiglic's AND protocol explained in Section 1.1: This random cut shifts the sequence of eight cards randomly, and hence, using the cyclic permutation $(1\,2\,\cdots\,8)$, the shuffle can be written as:

$$(\mathsf{shuf}, \{\mathsf{id}, (1\,2\,\cdots\,8), (1\,2\,\cdots\,8)^2, \cdots, (1\,2\,\cdots\,8)^7\}),$$

where $\mathsf{id}$ is the identity permutation. Generally, a shuffle can be expressed as

$$(\mathsf{shuf}, \Pi, \mathcal{F})$$

using a set of permutations $\Pi$ and a probability distribution $\mathcal{F}$ on $\Pi$; when the distribution $\mathcal{F}$ is uniform, we omit it in the description. An action $(\mathsf{shuf}, \Pi, \mathcal{F})$ results in rearranging a sequence of cards following a permutation $\pi$ drawn from $\Pi$ according to the distribution $\mathcal{F}$.

We now formally define a random cut for a (sub)sequence of length $n$ starting at the $k$-th position, as follows:

$$(\mathsf{shuf}, \mathsf{RC}_{k,n})$$

where

$$\mathsf{RC}_{k,n} = \{\mathsf{id}, (k\,k+1\,\cdots k+n-1), \cdots, \\ (k\,k+1\,\cdots\,k+n-1)^{n-1}\}.$$

A protocol using such random cuts only as shuffling actions is called an *RC-protocol* in this paper. Stiglic's AND protocol is an RC-protocol, and the first protocol (Crépeau and Kilian, 1994) and the second protocol (Niemi and Renvall, 1998) in Table 1 are also RC-protocols.

Another well-known shuffle is the "random bisection cut," that bisects a sequence of cards and swaps the two halves randomly. For example, a random bisection cut for six cards can be written as

$$(\mathsf{shuf}, \{\mathsf{id}, (1\,4)(2\,5)(3\,6)\}).$$

The fourth protocol (Mizuki and Sone, 2009) and the seventh protocol (Abe et al., 2018, 2021) in Table 1 use the random bisection cut.

The numbers of required cards of protocols typically depend on the allowed kinds of shuffles. For example, if we are allowed to use "non-uniform shuffles," we can construct a four-card protocol (Koch et al., 2015) as the fifth protocol in Table 1 (i.e., we do not need any helping card). A non-uniform shuffle means $(\mathsf{shuf}, \Pi, \mathcal{F})$ such that the distribution $\mathcal{F}$ is not uniform. Similarly, a non-closed shuffle means $(\mathsf{shuf}, \Pi, \mathcal{F})$ such that the set of permutations $\Pi$ is not a group. As imagined, implementing such non-uniform shuffles and/or non-closed shuffles is not easy; for instance, humans require some special cases to implement them. By contrast, as mentioned before, it is easy for humans to implement the random cut.

Thus, in this study, we focus on the use of the easiest shuffle, the random cut, i.e., we deal only with RC-protocols.

### 1.3 Our Contribution

As seen in Section 1.1 and Table 1, Stiglic's AND protocol requires eight cards, and this is the best committed-format AND RC-protocol in terms of the number of cards; see also Table 2. Thus, since 2001, it has been an open question to determine whether there exists a committed-format AND RC-protocol using less than eight cards. In this study, we will answer to the question.

Table 2: Committed-format AND RC-protocols and their numbers of shuffles

| | Card | | #Shuffles | Finite |
|---|---|---|---|---|
| | #Colors | #Cards | | |
| Crépeau–Kilian, 1993 (Crépeau and Kilian, 1994) | 4 | 10 | 8 (expected) | |
| Niemi–Renvall, 1998 (Niemi and Renvall, 1998) | 2 | 12 | 7.5 (expected) | |
| Stiglic, 2001 (Stiglic, 2001) | 2 | 8 | 2 (expected) | |
| Ours (§3) | 2 | 6 | 2 | ✓ |

That is, we propose a six-card committed-format AND RC-protocol. All the existing RC-protocols (as shown in Table 2) are not finite-runtime, that is, they are Las Vegas algorithms. By contrast, our protocol is finite-runtime, using exactly two random cuts, and hence, we believe that it is practical.

Note that, although this paper deals with only AND protocols, there are XOR protocols (e.g., Mizuki et al. (2006); Mizuki and Sone (2009); Toyoda et al. (2020)) and copy protocols (e.g., Mizuki and Sone (2009); Nishimura et al. (2018)), which are often required when evaluating logical circuits (cf. Ono and Manabe (2020)). It should be also noted that more complex tasks, such as Millionaires' problem (e.g., Nakai et al. (2021)) and zero-knowledge proofs (e.g., Ruangwises and Itoh (2020)), can be conducted using a deck of cards.

# 2 Preliminaries

In this section, we provide a basic technique used in our protocol presented later.

A rearrangement action $(\mathsf{perm}, \pi)$ results in permuting a sequence of cards according to the permutation $\pi$.

In Section 1.2, we formally defined a random cut $(\mathsf{shuf}, \mathsf{RC}_{k,n})$. Here, we consider a combination of it with rearrangement actions $\left(\mathsf{perm}, \pi^{-1}\right)$ and $(\mathsf{perm}, \pi)$ for a permutation $\pi$, namely,

$$\left(\mathsf{perm}, \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}^{-1}\right), (\mathsf{shuf}, \mathsf{RC}_{1,n}),$$

$$\left(\mathsf{perm}, \begin{pmatrix}1 & 2 & \cdots & n\\ \pi(1) & \pi(2) & \cdots & \pi(n)\end{pmatrix}\right).$$

For simplicity of description of our protocol, we express these three actions together as one action, as follows.

**Definition 1** *Let $\pi$ be a permutation on $\{1, 2, \cdots, n\}$, and let*

$$\sigma = (\pi(1)\, \pi(2)\, \cdots\, \pi(n)).$$

*Define*

$$\mathsf{RC}_\sigma = \{\sigma^i | 1 \leqq i \leqq n\},$$

*and $\sigma$ is called a* generator*. The action $(\mathsf{shuf}, \mathsf{RC}_\sigma)$ is called a $\sigma$-random cut, sometimes denoted by $\sigma$-$\mathsf{RC}$.*

As mentioned above, the introduction of $(\mathsf{shuf}, \mathsf{RC}_\sigma)$ is just for simplicity. To implement this, we apply three actions $(\mathsf{perm}, \pi^{-1})$, $(\mathsf{shuf}, \mathsf{RC}_{1,n})$, and $(\mathsf{perm}, \pi)$. Alternatively, the following procedure implements $\sigma$-$\mathsf{RC}$ with generator $\sigma = (\pi(1)\, \pi(2)\, \cdots\, \pi(n))$.

1. Given a sequence of cards on the table, take the $\pi(1)$-th, $\pi(2)$-th, …, $\pi(n)$-th cards in this order to make a bundle.
2. The Hindu cut (Ueda et al., 2016) is applied to the resulting card bundle. In other words, the following is quickly performed a sufficient number of random times:
   - Take some from the bottom and put them on top.
3. From the top of the card bundle, return all cards to the $\pi(n)$-th, $\pi(n-1)$-th, …, $\pi(1)$-th positions in this order.

Thus, $\sigma$-$\mathsf{RC}$ is implementable by the Hindu cut along with two rearrangements.

## 3 Proposal of Six-card Protocol

This section presents our proposed protocol using only the random cut, namely a committed-format AND RC-protocol using six cards.

Our AND protocol proceeds, as follows.

1. Place two helping cards to the right of two input commitments and turn them over:
$$\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}\boxed{\heartsuit}\boxed{\clubsuit} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}\boxed{?}\boxed{?}.$$
2. Apply $(\mathsf{shuf}, \mathsf{RC}_{\sigma_1})$ with generator $\sigma_1 = (1\,2\,4\,6\,3\,5)$ (denoted by $\langle\cdot\rangle_{\sigma^1}$) to the sequence of six cards:
$$\left\langle\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\right\rangle_{\sigma_1} \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$
3. Turn over the second card. We denote this action by $(\mathsf{turn}, \{2\})$.
   (a) If $\heartsuit$ appears:
$$\boxed{?}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{?}\boxed{?},$$
   reveal the fifth card. (The probability of this $\heartsuit$ appearing is 1/2.)

        i. If $\clubsuit$ appears:

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

        reveal the first card. (The probability of this $\clubsuit$ appearing is 2/3.)

            A. If $\clubsuit$ appears, turn over all face-up cards:

$$\boxed{\clubsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{\clubsuit}\boxed{?} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

            Apply $(\mathsf{perm}, (1\,2\,5\,6\,3\,4))$. Then, go to the next step (4). (The probability of this $\clubsuit$ appearing is 1/2.)

            B. If $\heartsuit$ appears, turn over all face-up cards:

$$\boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{\clubsuit}\boxed{?} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

            Apply $(\mathsf{perm}, (1\,3\,4)(2\,6))$, and go to the next step (4).

        ii. If $\heartsuit$ appears, turn over all face-up cards:

$$\boxed{?}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{\heartsuit}\boxed{?} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

        Apply $(\mathsf{perm}, (2\,6\,5\,3))$, and go to the next step (4).

    (b) If $\clubsuit$ appears:

$$\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{?}\boxed{?}\boxed{?},$$

    reveal the sixth card. (The probability of this $\clubsuit$ appearing is 1/2.)

        i. If $\heartsuit$ appears:

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

        reveal the fourth card.

            A. If $\heartsuit$ appears, turn over all face-up cards:

$$\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\heartsuit}\boxed{?}\boxed{\heartsuit} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

            Apply $(\mathsf{perm}, (1\,4\,3)(2\,5))$, and go to the next step (4). (The probability of this $\heartsuit$ appearing is 1/2.)

            B. If $\clubsuit$ appears, turn over all face-up cards:

$$\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\heartsuit} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

            Apply $(\mathsf{perm}, (1\,4\,6\,5\,3))$, and go to the next step (4).

        ii. If $\clubsuit$ appears, turn over all face-up cards:

$$\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{?}\boxed{?}\boxed{\clubsuit} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

        Go to the next step (4). (The probability of this $\clubsuit$ appearing is 1/3.)

4. Apply $(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$ with generator $\sigma_2 = (1\,2\,6\,3\,4\,5)$:

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle_{\sigma_2} \;\rightarrow\; \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

5. Reveal the first card.

    (a) If $\heartsuit$ appears:

$$\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?},$$

    reveal the fourth card. (The probability of this $\heartsuit$ appearing is 1/2.)

i. When ♣ appears, the third and second cards constitute a commitment to $a \wedge b$:

$$\boxed{\heartsuit}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\boxed{\clubsuit}\boxed{?}\boxed{?} \rightarrow \underbrace{\overset{3}{\boxed{?}}\overset{2}{\boxed{?}}}_{a\wedge b}.$$

(The probability of this ♣ appearing is 2/3.)

ii. If ♡ appears, the second and fifth cards constitute a commitment to $a \wedge b$:

$$\boxed{\heartsuit}\overset{2}{\boxed{?}}\boxed{?}\boxed{\heartsuit}\overset{5}{\boxed{?}}\boxed{?} \rightarrow \underbrace{\overset{2}{\boxed{?}}\overset{5}{\boxed{?}}}_{a\wedge b}.$$

(b) If ♣ appears:

$$\boxed{\clubsuit}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?},$$

reveal the sixth card.

i. If ♡ appears, the fifth and third cards constitute a commitment to $a \wedge b$:

$$\boxed{\clubsuit}\boxed{?}\overset{3}{\boxed{?}}\boxed{?}\overset{5}{\boxed{?}}\boxed{\heartsuit} \rightarrow \underbrace{\overset{5}{\boxed{?}}\overset{3}{\boxed{?}}}_{a\wedge b}.$$

ii. If ♣ appears, the second and fifth cards constitute a commitment to $a \wedge b$:

$$\boxed{\clubsuit}\overset{2}{\boxed{?}}\boxed{?}\boxed{?}\overset{5}{\boxed{?}}\boxed{\clubsuit} \rightarrow \underbrace{\overset{2}{\boxed{?}}\overset{5}{\boxed{?}}}_{a\wedge b}.$$

This is our six-card committed-format AND protocol that uses only two random cuts. Since the protocol does not include any loop, it terminates with a finite number of shuffles (namely, two random cuts).

## 4 Correctness and Security of Our Protocol

Our protocol can be expressed as a KWH-tree, as shown in Figure 1.

The KWH-tree (Koch et al., 2015) is a diagram representing a protocol with nodes corresponding to "states" and edges corresponding to actions that connect them. Here, $X_{ab}$ represents the probability that the input is $(a, b)$, and we have $X_{11} + X_{10} + X_{01} + X_{00} = 1$. A polynomial annotating a card sequence in a state, such as $\frac{1}{6}(X_{10} + X_{01})$, represents the conditional probability that the current sequence is the one next to the polynomial, given the trace of visible sequences observed so far (where a "visible sequence" means a sequence of symbols on the faces of all lying cards on the table). When a turn action is applied, it divides a state into two states; intuitively, if the conditional probabilities are 'split' with 'equal ratio,' no information leaks. Formally, if the sum of probabilities in a state is equal to $X_{11} + X_{10} + X_{01} + X_{00}$, then the information about input $a, b$ is kept secret. Refer to Koch et al. (2015); Kastner et al. (2017); Mizuki and Shizuya (2017) for more details.

The KWH-tree guarantees that our protocol is correct and secure: The bottom states tell us that the output commitment is correct; the sum of probabilities in every state is equal to $X_{11}+X_{10}+X_{01}+X_{00} = 1$, meaning that the (conditional) distribution on input does not change, and hence, the protocol is secure.

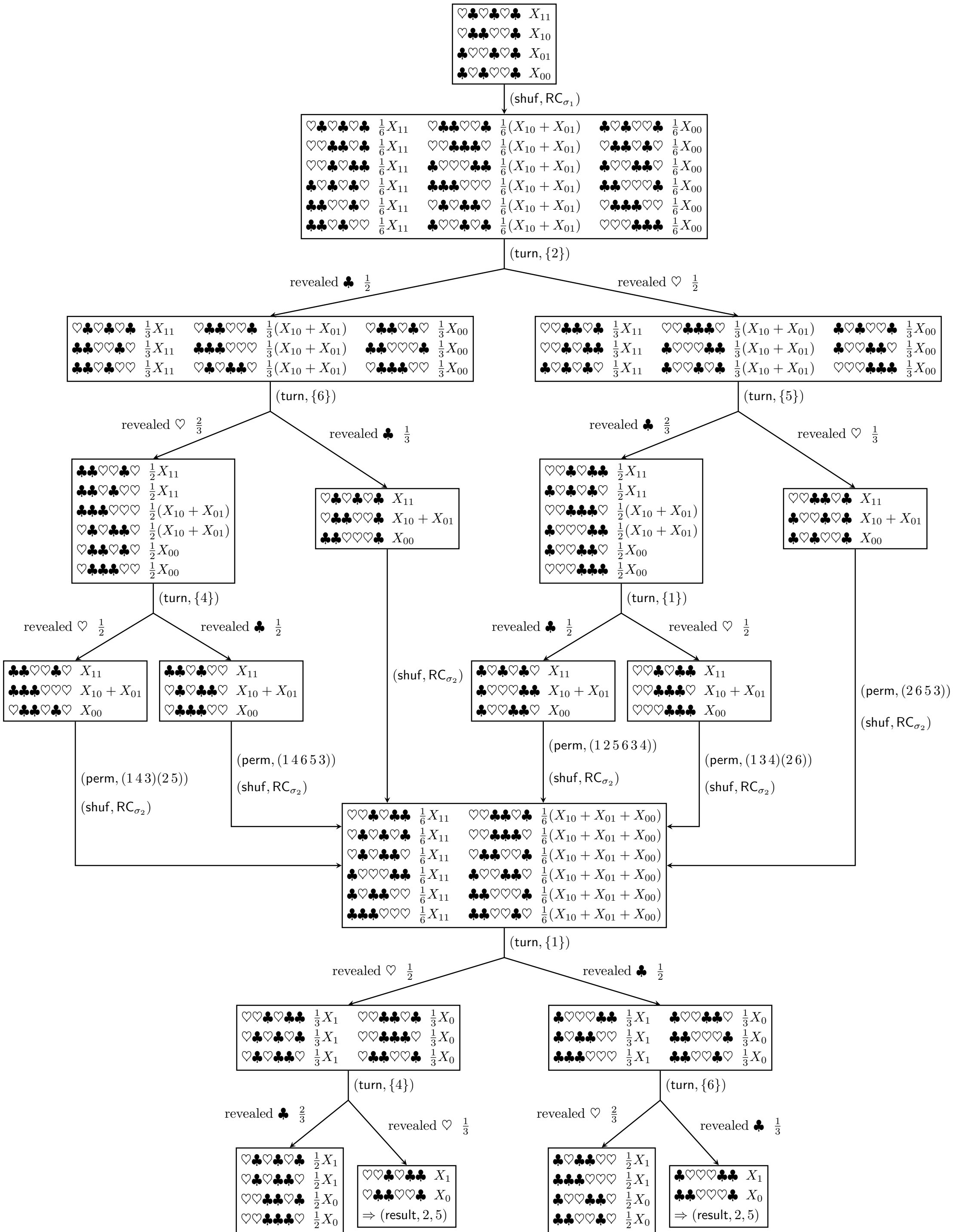
♡♣♡♣♡♣ $X_{11}$
♡♣♣♡♡♣ $X_{10}$
♣♡♡♣♡♣ $X_{01}$
♣♡♣♡♡♣ $X_{00}$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_1})$
♡♣♡♣♡♣ $\frac{1}{6}X_{11}$ ♡♣♣♡♡♣ $\frac{1}{6}(X_{10}+X_{01})$ ♣♡♣♡♡♣ $\frac{1}{6}X_{00}$
♡♡♣♣♡♣ $\frac{1}{6}X_{11}$ ♡♡♣♣♣♡ $\frac{1}{6}(X_{10}+X_{01})$ ♡♣♣♡♣♡ $\frac{1}{6}X_{00}$
♡♡♣♡♣♣ $\frac{1}{6}X_{11}$ ♣♡♡♡♣♣ $\frac{1}{6}(X_{10}+X_{01})$ ♣♡♡♣♣♡ $\frac{1}{6}X_{00}$
♣♡♣♡♣♡ $\frac{1}{6}X_{11}$ ♣♣♣♡♡♡ $\frac{1}{6}(X_{10}+X_{01})$ ♣♣♡♡♡♣ $\frac{1}{6}X_{00}$
♣♣♡♡♣♡ $\frac{1}{6}X_{11}$ ♡♣♡♣♣♡ $\frac{1}{6}(X_{10}+X_{01})$ ♡♣♣♣♡♡ $\frac{1}{6}X_{00}$
♣♣♡♣♡♡ $\frac{1}{6}X_{11}$ ♣♡♡♣♡♣ $\frac{1}{6}(X_{10}+X_{01})$ ♡♡♡♣♣♣ $\frac{1}{6}X_{00}$
$(\mathsf{turn}, \{2\})$
revealed ♣ $\frac{1}{2}$
revealed ♡ $\frac{1}{2}$
♡♣♡♣♡♣ $\frac{1}{3}X_{11}$ ♡♣♣♡♡♣ $\frac{1}{3}(X_{10}+X_{01})$ ♡♣♣♡♣♡ $\frac{1}{3}X_{00}$
♣♣♡♡♣♡ $\frac{1}{3}X_{11}$ ♣♣♣♡♡♡ $\frac{1}{3}(X_{10}+X_{01})$ ♣♣♡♡♡♣ $\frac{1}{3}X_{00}$
♣♣♡♣♡♡ $\frac{1}{3}X_{11}$ ♡♣♡♣♣♡ $\frac{1}{3}(X_{10}+X_{01})$ ♡♣♣♣♡♡ $\frac{1}{3}X_{00}$
♡♡♣♣♡♣ $\frac{1}{3}X_{11}$ ♡♡♣♣♣♡ $\frac{1}{3}(X_{10}+X_{01})$ ♣♡♣♡♡♣ $\frac{1}{3}X_{00}$
♡♡♣♡♣♣ $\frac{1}{3}X_{11}$ ♣♡♡♡♣♣ $\frac{1}{3}(X_{10}+X_{01})$ ♣♡♡♣♣♡ $\frac{1}{3}X_{00}$
♣♡♣♡♣♡ $\frac{1}{3}X_{11}$ ♣♡♡♣♡♣ $\frac{1}{3}(X_{10}+X_{01})$ ♡♡♡♣♣♣ $\frac{1}{3}X_{00}$
$(\mathsf{turn}, \{6\})$
revealed ♡ $\frac{2}{3}$
revealed ♣ $\frac{1}{3}$
$(\mathsf{turn}, \{5\})$
revealed ♣ $\frac{2}{3}$
revealed ♡ $\frac{1}{3}$
♣♣♡♡♣♡ $\frac{1}{2}X_{11}$
♣♣♡♣♡♡ $\frac{1}{2}X_{11}$
♣♣♣♡♡♡ $\frac{1}{2}(X_{10}+X_{01})$
♡♣♡♣♣♡ $\frac{1}{2}(X_{10}+X_{01})$
♡♣♣♡♣♡ $\frac{1}{2}X_{00}$
♡♣♣♣♡♡ $\frac{1}{2}X_{00}$
♡♣♡♣♡♣ $X_{11}$
♡♣♣♡♡♣ $X_{10}+X_{01}$
♣♣♡♡♡♣ $X_{00}$
♡♡♣♡♣♣ $\frac{1}{2}X_{11}$
♣♡♣♡♣♡ $\frac{1}{2}X_{11}$
♡♡♣♣♣♡ $\frac{1}{2}(X_{10}+X_{01})$
♣♡♡♡♣♣ $\frac{1}{2}(X_{10}+X_{01})$
♣♡♡♣♣♡ $\frac{1}{2}X_{00}$
♡♡♡♣♣♣ $\frac{1}{2}X_{00}$
♡♡♣♣♡♣ $X_{11}$
♣♡♡♣♡♣ $X_{10}+X_{01}$
♣♡♣♡♡♣ $X_{00}$
$(\mathsf{turn}, \{4\})$
revealed ♡ $\frac{1}{2}$
revealed ♣ $\frac{1}{2}$
$(\mathsf{turn}, \{1\})$
revealed ♣ $\frac{1}{2}$
revealed ♡ $\frac{1}{2}$
♣♣♡♡♣♡ $X_{11}$
♣♣♣♡♡♡ $X_{10}+X_{01}$
♡♣♣♡♣♡ $X_{00}$
♣♣♡♣♡♡ $X_{11}$
♡♣♡♣♣♡ $X_{10}+X_{01}$
♡♣♣♣♡♡ $X_{00}$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$
♣♡♣♡♣♡ $X_{11}$
♣♡♡♡♣♣ $X_{10}+X_{01}$
♣♡♡♣♣♡ $X_{00}$
♡♡♣♡♣♣ $X_{11}$
♡♡♣♣♣♡ $X_{10}+X_{01}$
♡♡♡♣♣♣ $X_{00}$
$(\mathsf{perm}, (2\,6\,5\,3))$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$
$(\mathsf{perm}, (1\,4\,3)(2\,5))$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$
$(\mathsf{perm}, (1\,4\,6\,5\,3))$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$
$(\mathsf{perm}, (1\,2\,5\,6\,3\,4))$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$
$(\mathsf{perm}, (1\,3\,4)(2\,6))$
$(\mathsf{shuf}, \mathsf{RC}_{\sigma_2})$
♡♡♣♡♣♣ $\frac{1}{6}X_{11}$ ♡♡♣♣♡♣ $\frac{1}{6}(X_{10}+X_{01}+X_{00})$
♡♣♡♣♡♣ $\frac{1}{6}X_{11}$ ♡♡♣♣♣♡ $\frac{1}{6}(X_{10}+X_{01}+X_{00})$
♡♣♡♣♣♡ $\frac{1}{6}X_{11}$ ♡♣♣♡♡♣ $\frac{1}{6}(X_{10}+X_{01}+X_{00})$
♣♡♡♡♣♣ $\frac{1}{6}X_{11}$ ♣♡♡♣♣♡ $\frac{1}{6}(X_{10}+X_{01}+X_{00})$
♣♡♣♣♡♡ $\frac{1}{6}X_{11}$ ♣♣♡♡♡♣ $\frac{1}{6}(X_{10}+X_{01}+X_{00})$
♣♣♣♡♡♡ $\frac{1}{6}X_{11}$ ♣♣♡♡♣♡ $\frac{1}{6}(X_{10}+X_{01}+X_{00})$
$(\mathsf{turn}, \{1\})$
revealed ♡ $\frac{1}{2}$
revealed ♣ $\frac{1}{2}$
♡♡♣♡♣♣ $\frac{1}{3}X_1$ ♡♡♣♣♡♣ $\frac{1}{3}X_0$
♡♣♡♣♡♣ $\frac{1}{3}X_1$ ♡♡♣♣♣♡ $\frac{1}{3}X_0$
♡♣♡♣♣♡ $\frac{1}{3}X_1$ ♡♣♣♡♡♣ $\frac{1}{3}X_0$
♣♡♡♡♣♣ $\frac{1}{3}X_1$ ♣♡♡♣♣♡ $\frac{1}{3}X_0$
♣♡♣♣♡♡ $\frac{1}{3}X_1$ ♣♣♡♡♡♣ $\frac{1}{3}X_0$
♣♣♣♡♡♡ $\frac{1}{3}X_1$ ♣♣♡♡♣♡ $\frac{1}{3}X_0$
$(\mathsf{turn}, \{4\})$
revealed ♣ $\frac{2}{3}$
revealed ♡ $\frac{1}{3}$
$(\mathsf{turn}, \{6\})$
revealed ♡ $\frac{2}{3}$
revealed ♣ $\frac{1}{3}$
♡♣♡♣♡♣ $\frac{1}{2}X_1$
♡♣♡♣♣♡ $\frac{1}{2}X_1$
♡♡♣♣♡♣ $\frac{1}{2}X_0$
♡♡♣♣♣♡ $\frac{1}{2}X_0$
⇒ $(\mathsf{result}, 3, 2)$
♡♡♣♡♣♣ $X_1$
♡♣♣♡♡♣ $X_0$
⇒ $(\mathsf{result}, 2, 5)$
♣♡♣♣♡♡ $\frac{1}{2}X_1$
♣♣♣♡♡♡ $\frac{1}{2}X_1$
♣♡♡♣♣♡ $\frac{1}{2}X_0$
♣♣♡♡♣♡ $\frac{1}{2}X_0$
⇒ $(\mathsf{result}, 5, 3)$
♣♡♡♡♣♣ $X_1$
♣♣♡♡♡♣ $X_0$
⇒ $(\mathsf{result}, 2, 5)$

Figure 1: A KWH-tree for our 6-card committed-format AND RC-protocol

# 5 Conclusion

In this paper, we designed a six-card committed-format AND RC-protocol. Our protocol uses only two random cuts and we believe that it is practical.

Kastner et al. (Kastner et al., 2017) provided an impossibility result, which implies that there exists no four-card committed-format AND RC-protocol. Thus, determining whether there is a five-card committed-format AND RC-protocol is an interesting open problem.

# References

Abe Y, Hayashi Y, Mizuki T, Sone H (2018) Five-card AND protocol in committed format using only practical shuffles. In: Proceedings of the 5th ACM on ASIA Public-Key Cryptography Workshop, ACM, New York, NY, USA, APKC '18, pp 3–8

Abe Y, Hayashi Y, Mizuki T, Sone H (2021) Five-card AND computations in committed format using only uniform cyclic shuffles. New Generation Computing URL `https://doi.org/10.1007/s00354-020-00110-2`

Crépeau C, Kilian J (1994) Discreet solitary games. In: Stinson DR (ed) Advances in Cryptology — CRYPTO' 93, Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, vol 773, pp 319–330

Kastner J, Koch A, Walzer S, Miyahara D, Hayashi Y, Mizuki T, Sone H (2017) The minimum number of cards in practical card-based protocols. In: Takagi T, Peyrin T (eds) Advances in Cryptology – ASIACRYPT 2017, Springer, Cham, Lecture Notes in Computer Science, vol 10626, pp 126–155

Koch A (2018) The landscape of optimal card-based protocols. Cryptology ePrint Archive, Report 2018/951, URL `https://eprint.iacr.org/2018/951`

Koch A, Walzer S, Härtel K (2015) Card-based cryptographic protocols using a minimal number of cards. In: Iwata T, Cheon JH (eds) Advances in Cryptology – ASIACRYPT 2015, Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, vol 9452, pp 783–807

Mizuki T, Shizuya H (2017) Computational model of card-based cryptographic protocols and its applications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences E100.A(1):3–11, DOI 10.1587/transfun.E100.A.3

Mizuki T, Sone H (2009) Six-card secure AND and four-card secure XOR. In: Deng X, Hopcroft JE, Xue J (eds) Frontiers in Algorithmics, Springer, Berlin, Heidelberg, Lecture Notes in Computer Science, vol 5598, pp 358–369

Mizuki T, Uchiike F, Sone H (2006) Securely computing XOR with 10 cards. The Australasian Journal of Combinatorics 36:279–293

Nakai T, Misawa Y, Tokushige Y, Iwamoto M, Ohta K (2021) How to solve millionaires' problem with two kinds of cards. New Generation Computing URL `https://doi.org/10.1007/s00354-020-00118-8`

Niemi V, Renvall A (1998) Secure multiparty computations without computers. Theoretical Computer Science 191(1–2):173–183, DOI 10.1016{\slash}S0304-3975(97)00107-2

Nishimura A, Nishida T, Hayashi Y, Mizuki T, Sone H (2018) Card-based protocols using unequal division shuffles. Soft Computing 22:361–371, DOI 10.1007/s00500-017-2858-2

Ono H, Manabe Y (2020) Card-based cryptographic logical computations using private operations. New Generation Computing

Ruangwises S, Itoh T (2019) AND protocols using only uniform shuffles. In: van Bevern R, Kucherov G (eds) Computer Science – Theory and Applications, Springer, Cham, Lecture Notes in Computer Science, vol 11532, pp 349–358

Ruangwises S, Itoh T (2020) Physical zero-knowledge proof for Numberlink puzzle and k vertex-disjoint paths problem. New Generation Computing URL `https://doi.org/10.1007/s00354-020-00114-y`

Stiglic A (2001) Computations with a deck of cards. Theoretical Computer Science 259(1–2):671–678, DOI 10.1016{\slash}S0304-3975(00)00409-6

Toyoda K, Miyahara D, Mizuki T, Sone H (2020) Six-card finite-runtime XOR protocol with only random cut. In: Proceedings of the 7th ACM on ASIA Public-Key Cryptography Workshop, ACM, New York, NY, USA, APKC'20, pp 1–7

Ueda I, Nishimura A, Hayashi Y, Mizuki T, Sone H (2016) How to implement a random bisection cut. In: Martín-Vide C, Mizuki T, Vega-Rodríguez MA (eds) Theory and Practice of Natural Computing, Springer, Cham, Lecture Notes in Computer Science, vol 10071, pp 58–69