New Generation Computing (2021) 39:97–114
https://doi.org/10.1007/s00354-020-00110-2

NEW GENERATION COMPUTING

Five-Card AND Computations in Committed Format Using Only Uniform Cyclic Shuffles

Yuta Abe[1] · Yu-ichi Hayashi[2] · Takaaki Mizuki[3] · Hideaki Sone[3]

Received: 26 April 2020 / Accepted: 29 September 2020 / Published online: 18 January 2021

Abstract

In card-based cryptography, designing AND protocols in committed format is a major research topic. The state-of-the-art AND protocol proposed by Koch, Walzer, and Härtel in ASIACRYPT 2015 uses only four cards, which is the minimum permissible number. The minimality of their protocol relies on somewhat complicated shuffles having non-uniform probabilities of possible outcomes. Restricting the allowed shuffles to uniform closed ones entails that, to the best of our knowledge, six cards are sufficient: the six-card AND protocol proposed by Mizuki and Sone in 2009 utilizes the random bisection cut, which is a uniform and cyclic (and hence, closed) shuffle. Thus, a question has arisen: "Can we improve upon this six-card protocol using only uniform closed shuffles?" In other words, the existence or otherwise of a five-card AND protocol in committed format using only uniform closed shuffles has been one of the most important open questions in this field. In this paper, we answer the question affirmatively by designing five-card committed-format AND protocols using only uniform cyclic shuffles. The shuffles that our protocols use are the random cut and random bisection cut, both of which are uniform cyclic shuffles and can be easily implemented by humans.

Keywords Card-based cryptography · Secure multiparty computation · Deck of cards

An earlier version of this study was presented at the 5th ACM ASIA Public-Key Cryptography Workshop, APKC 2018, Korea, June 4, 2018, and appeared in the Proceedings of the 5th ACM ASIA Public-Key Cryptography Workshop, pp. 3–8, 2018 [1].

✉ Takaaki Mizuki
tm-paper+card5coa@g-mail.tohoku-university.jp

1 Graduate School of Information Sciences, Tohoku University, 6-3 Aramaki-Aza-Aoba, Aoba, Sendai, Japan

2 Graduate School of Sciences and Technology, Nara Institute of Science and Technology, 8916-5 Takayama, Ikoma, Nara, Japan

3 Cyberscience Center, Tohoku University, 6-3 Aramaki-Aza-Aoba, Aoba, Sendai, Japan

Introduction

Card-based cryptography started from the "five-card trick" presented by den Boer in 1989 [2]. This card-based protocol performs a secure AND computation using two black cards $\boxed{\clubsuit}\boxed{\clubsuit}$ and three red cards $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, where their backs $\boxed{?}$ are all identical. This paper begins by introducing the five-card trick.

The Five-Card Trick

In card-based cryptography, manipulating Boolean values entails the use of the following encoding:

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

That is, the left card being black represents 0, and the left card being red represents 1. According to this encoding rule (1), Alice can put her private input bit $a \in \{0, 1\}$ on a table using two cards $\boxed{\clubsuit}\boxed{\heartsuit}$, keeping its value hidden:

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

Such a pair of face-down cards is called a *commitment* to a bit $a \in \{0, 1\}$. Similarly, Bob can put a commitment to his private input bit $b \in \{0, 1\}$ on the table, keeping its value secret from Alice (and others). Given the commitments to $a \in \{0, 1\}$ and $b \in \{0, 1\}$, along with a helping card $\boxed{\heartsuit}$, the five-card trick [2] proceeds as follows.

1. Put the helping red card between the two input commitments, apply a *NOT computation* to the left commitment (to a) by swapping the positions of its two cards, so that we have a commitment to the negation $\bar{a}$, and turn over the middle red card:

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

   Note that the three cards in the middle will be $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, i.e., three red cards will be consecutive only when $a = b = 1$, namely, $a \wedge b = 1$.
2. Apply a *random cut* (denoted by $\langle\cdot\rangle$) to the sequence of the five cards:

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

   A random cut, meaning a cyclic shuffling operation, uniformly randomly shifts the positions of the sequence without changing the order[1]. Mathematically, one permutation is uniformly randomly selected from

[1] Humans can easily implement a random cut, such that nobody will know which one (among the five possibilities, in this case) is the current sequence (e.g., [2,6,13,19]).

$$\{\mathsf{id},\ (1\,2\,3\,4\,5),\ (1\,2\,3\,4\,5)^2,\ (1\,2\,3\,4\,5)^3,\ (1\,2\,3\,4\,5)^4\},$$

and the selected permutation is applied to the sequence of the five cards, where id is the identity permutation and $(i_1\, i_2\, \ldots\, i_\ell)$ represents a cyclic permutation. (Nobody knows the selected permutation.)

3. Reveal the five cards. If the three red cards $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ are consecutive (apart from cyclic rotation), then $a \wedge b = 1$. Otherwise, $a \wedge b = 0$.

This is the five-card trick, which is simple and elegant. Although the five-card trick is extremely useful as mentioned, it has one drawback: it cannot deal with a logical conjunction of three or more variables, where players $P_1, P_2, \ldots, P_n$ with $n \geq 3$ want to conduct a secure multiparty AND computation. To overcome such a limitation, researchers have designed "committed-format AND protocols," which are able to perform secure AND computation of three or more inputs.

The Six-Card AND Protocol in Committed Format

A committed-format AND protocol should produce a commitment to $a \wedge b$:

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

from the input commitments to a and b. In contrast to the five-card trick, the output is obtained as a commitment to $a \wedge b$, keeping its value secret; hence, the output commitment can be used as the input for another computation. There are many existing committed-format AND protocols in the literature (as shown in Table 1). Among these, we herein introduce the Mizuki–Sone protocol [10], which is considered to be the simplest for humans to execute. This protocol uses two helping cards $\boxed{\clubsuit}\boxed{\heartsuit}$ and proceeds as follows.

1. Put the two helping cards between two input commitments, and turn them over:

$$\underbrace{\boxed{?}\boxed{?}}_{a}\boxed{\clubsuit}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{b} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{0}\underbrace{\boxed{?}\boxed{?}}_{b}.$$

2. Rearrange the order of the sequence as:

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

3. Apply a *random bisection cut* denoted by $[\,\cdot \mid \cdot\,]$, i.e., bisect the sequence of the six cards and shuffle the two halves:

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

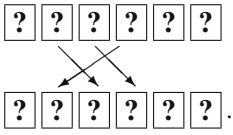
Table 1 Committed-format AND protocols

	Card		Shuffle				
	# of colors	# of cards	Finite	Uniform	Cyclic	Closed	# of shuffles
Crépeau–Kilian, 1993 [3]	4	10	No	Yes	Yes	Yes	8
Niemi–Renvall, 1998 [13]	2	12	No	Yes	Yes	Yes	7.5
Stiglic, 2001 [17]	2	8	No	Yes	Yes	Yes	2
Mizuki–Sone, 2009 [10] (§1.2)	2	6	Yes	Yes	Yes	Yes	1
Koch–Walzer–Härtel, 2015 [7]	2	4	No	No	Yes	Yes	8
	2	5	Yes	No	No	No	14/3
Koch, 2018 [5]	2	4	No	Yes	No	No	8
Ruangwises–Itoh, 2019 [16]	2	5	Yes	Yes	No	No	14/3
Our first protocol (§2)	2	5	No	Yes	Yes	Yes	7
Our second protocol (§3)	2	5	No	Yes	Yes	Yes	4.5

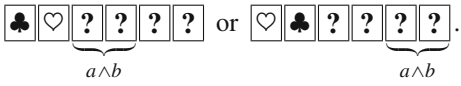
The numbers of shuffles in the last column are expected values (except for the fourth protocol)

Mathematically, the permutation id or $(1\,4)(2\,5)(3\,6)$ is selected with a probability of $1/2$, and the selected permutation is applied to the sequence of the six cards. [2]

4. Rearrange the order of the sequence as:



5. Reveal the two left-most cards; then, a commitment to $a \wedge b$ is obtained, depending on the order of the two face-up cards ♣ and ♡:



This is the six-card AND protocol in committed format [10]. Given n input commitments to $x_1, x_2, \ldots, x_n$, and executing such a committed-format AND protocol $n-1$ times, a secure AND computation of n variables can be conducted, i.e., we can obtain a commitment to $x_1 \wedge x_2 \wedge \cdots \wedge x_n$.

Known Results and Our Contribution

As discussed previously, committed-format AND protocols are a useful and indispensable primitive, and designing such AND protocols is a major research topic in the field of card-based cryptography. As enumerated chronologically in Table 1, there are

[2] It is well known that a random bisection cut can also be easily and securely implemented by humans [18,19].

many committed-format AND protocols. The Mizuki–Sone protocol proposed in 2009 [10] (and described in Section 1.2) is the fourth committed-format AND protocol in literature; it uses six cards, which are fewer than the previous three protocols [3,13,17] require; furthermore, as shown in the fourth column of Table 1, the Mizuki–Sone protocol is the first committed-format AND protocol that terminates in a finite number of shuffles (actually, it terminates after a single shuffle, namely, a random bisection cut, as indicated in Sect. 1.2).

After the invention of the Mizuki–Sone six-card AND protocol in 2009, it had been a challenging open question to determine whether one could construct an AND protocol (in committed format) with five cards or less. In 2015, Koch, Walzer, and Härtel [7] succeeded in answering the question appropriately; i.e., they presented a four-card AND protocol in committed format, which is the fifth protocol, as shown in Table 1. Their four-card protocol is optimal in terms of the number of required cards, because we need four cards for arranging two input commitments, as long as we follow the encoding (1). As shown in the fourth column of Table 1, their four-card AND protocol does not terminate with a fixed number of shuffles, indicating that it is a Las Vegas algorithm. In addition, they constructed a five-card AND protocol that terminates with a finite number of shuffles; see the sixth protocol shown in Table 1. Furthermore, they proved that there is no four-card committed-format AND protocol with a finite number of shuffles. Therefore, when we focus our attention on finite-runtime protocols, the five-card AND protocol in committed format is optimal in terms of the number of cards.

Now, let us revisit Table 1, which contains columns regarding shuffles being uniform, cyclic, and/or closed. Note that the first four protocols (from 1993 to 2009) all have the answer "yes." We formally define the uniformity, cyclicity, and closedness of shuffles. Following the formal computation model of card-based protocols [8], a shuffle action is specified by a set Π of permutations and a probability distribution $\mathcal{F}$ on Π:

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

if $\mathcal{F}$ is uniform, we say that the shuffle is *uniform*; if Π is a cyclic subgroup (of the symmetric group), we say that it is *cyclic*; if Π is a subgroup, we say that it is *closed*. For example, the random bisection cut that the Mizuki–Sone protocol uses can be formally written as:

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

Thus, a random bisection cut is surely a uniform and cyclic (and hence, closed) shuffle. The first three protocols [3,13,17] in Table 1 utilize only random cuts, which are also uniform and cyclic.

On the other hand, the two Koch–Walzer–Härtel protocols [7] use non-uniform and/or non-closed shuffles, such as:

$$(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,4)\},\ \mathsf{id} \mapsto 1/3,\ (1\,2)(3\,4) \mapsto 2/3)$$

and

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

Recently, Koch [5], as well as Ruangwises and Itoh [16], independently modified the Koch–Walzer–Härtel protocols to obtain protocols using only uniform shuffles, although those shuffles are non-closed; see the seventh and eighth protocols, as shown in Table 1. Thus, it is relatively difficult for humans to practically implement the existing four-card and five-card protocols. Note that Koch and Walzer [6] showed that any uniform closed shuffles can be implemented by human hands with the help of a secure implementation of the random cut (such as the Hindu cut [18,19]).

Therefore, a natural question has arisen:

> Can we construct a committed-format AND protocol with five cards or less using only uniform closed shuffles?

This is one of the most important open problems in card-based cryptography.

In this paper, we will answer this question affirmatively, i.e., we will design five-card AND protocols in committed format using only uniform closed shuffles (see the last two rows in Table 1). The shuffles that our protocols use are random cuts and random bisection cuts, both of which can be easily implemented by humans, as mentioned above. Hence, we believe that humans can effortlessly execute our protocols. Specifically, we propose two protocols: in Sect. 2, we present a five-card AND protocol whose expected number of shuffles is seven, while in Sect. 3, we improve upon the protocol, such that the expected number of shuffles can be reduced to 4.5 (although the construction is somewhat complicated).

An earlier version of this study was presented and appeared as a conference paper [1]. This present paper is extended compared to the conference paper: This paper provides another novel five-card AND protocol using a less number of shuffles and verify the correctness and security of the protocol. Section 3 is devoted to these new findings.

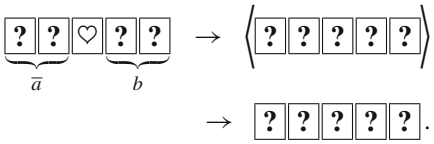
First Five-Card AND Protocol Using Only Uniform Cyclic Shuffles

In this section, we construct a five-card committed-format AND protocol using only uniform cyclic shuffles.

Idea

Here, we explain the idea behind our protocol.

Recall Steps 1 and 2 of the five-card trick:

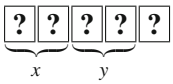


Let the middle card be revealed, and assume that it happens to be ♣ :

Then, there are four possibilities:

(i)	♡♡♣♡♣	$a \wedge b = 0$;
(ii)	♣♡♣♡♡	$a \wedge b = 0$;
(iii)	♡♡♣♣♡	$a \wedge b = 1$;
(iv)	♡♣♣♡♡	$a \wedge b = 1$.

After turning the middle card face down, denote the sequence of cards by

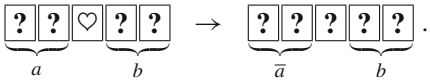


for the sake of convenience [for example, the two left-most cards are not a commitment to a bit for the cases of (i) and (iii)]. Note that in cases (ii) and (iv), the first pair of cards can be regarded as a commitment to x, the second pair can be regarded as a commitment to y, and it holds that $x \oplus y = a \wedge b$. Therefore, by applying the four-card XOR protocol [10] to the first four cards, one can obtain a commitment to $x \oplus y = a \wedge b$ in these two cases. Even in cases (i) and (iii), we can continue the computation without leaking any information. The details will be revealed in the next subsection.

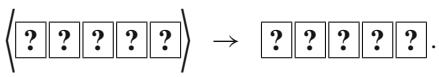
Description

Here, we provide the complete description of our protocol.

1. Execute Step 1 of the five-card trick:



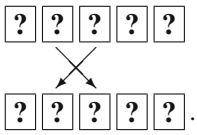
2. Execute Step 2 of the five-card trick:



3. Reveal the middle card, i.e., the third card. If the face-up card is $\boxed{\heartsuit}$, turn it over and return to Step 2. If it is $\boxed{\clubsuit}$, go to the next step. (The probability that $\boxed{\clubsuit}$ appears is 2/5.)
4. Turn over the card $\boxed{\clubsuit}$:

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

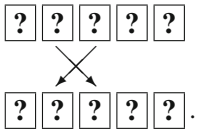
5. Apply the procedure of the four-card XOR protocol [10] to the four left-most cards, as follows.
   (a) Rearrange the order as:



   (b) Apply a random bisection cut to the four left-most cards:

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

   (c) Rearrange the order again as:



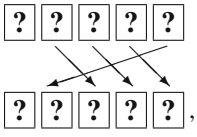
6. Reveal the two left-most cards.
   (a) If $\boxed{\clubsuit}\boxed{\heartsuit}$ or $\boxed{\heartsuit}\boxed{\clubsuit}$ appears, then we have a commitment to $a \wedge b$:

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

   In the latter case, a NOT computation (which involves swapping the positions of two cards) brings a commitment to $a \wedge b$.
   (b) If $\boxed{\heartsuit}\boxed{\heartsuit}$ appears, then turn them over:

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

   rearrange the order as:



and return to Step 2. (The probability that $\boxed{\heartsuit}\boxed{\heartsuit}$ appears is $1/2$.)

This is our committed-format AND protocol. Since this protocol has loops, it does not terminate within a fixed number of shuffles; that is, it is a Las Vegas algorithm. The expected number of shuffles is seven, as follows. Let N_{RC} and N_{RBC} be the expected numbers of random cuts and random bisection cuts, respectively; then,

$$N_{\mathrm{RC}} = 1 + \frac{3}{5}N_{\mathrm{RC}} + \frac{2}{5}\cdot\frac{1}{2}N_{\mathrm{RC}}$$

and

$$N_{\mathrm{RBC}} = \frac{3}{5}N_{\mathrm{RBC}} + \frac{2}{5}(1 + \frac{1}{2}N_{\mathrm{RBC}});$$

hence, we have $N_{\mathrm{RC}} = 5$ and $N_{\mathrm{RBC}} = 2$.

Pseudocode

The following is a pseudocode[3] for our protocol, where we define:

$$\mathsf{RC}_5 \stackrel{\mathrm{def}}{=} \{\mathsf{id},\ (1\,2\,3\,4\,5),\ (1\,2\,3\,4\,5)^2,\ (1\,2\,3\,4\,5)^3,\ (1\,2\,3\,4\,5)^4\},$$

and we simply write (shuf, Π) rather than $(\mathsf{shuf}, \Pi, \mathcal{F})$ if $\mathcal{F}$ is uniform; (perm, π) means to permute the sequence of cards according to π, (turn, T) means to turn over all the cards in T, (result, i, j) means to terminate the protocol with an output commitment consisting of the ith and jth cards, and "visible seq." means what are seen when looking at the sequence of cards on the table.

---

input set:

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

(perm, (1 2))
(turn, {3})
1 (shuf, RC_5)
(turn, {3})
if visible seq. = (?, ?, ♡, ?, ?) **then**
  (turn, {3})
  goto 1
(turn, {3})
(perm, (2 3))

[3] Technically, describing this pseudocode is redundant, but it will allow easy reference.

(shuf, {id, (1 3)(2 4)})
(perm, (2 3))
(turn, {1, 2})
if visible seq. = (♡, ♡, ?, ?, ?) **then**
  (turn, {1, 2})
  (perm, (2 3 4 5))
  goto 1
else if visible seq. = (♣, ♡, ?, ?, ?) **then**
  (result, 3, 4)
else if visible seq. = (♡, ♣, ?, ?, ?) **then**
  (result, 4, 3)

In the next subsection, we confirm that our protocol definitively produces a commitment to $a \wedge b$ without leaking any information about a and b.

Correctness and Security

In this subsection, we verify the correctness and security of the protocol proposed in the previous subsections.

To this end, we make use of the *KWH-tree*, which is an excellent tool developed by Koch, Walzer, and Härtel [7]. That is, if one can write the KWH-tree satisfying some properties for a protocol, then it automatically implies that the protocol is correct and secure; see [7,9] for the details.

We describe the KWH-tree for our five-card AND protocol in Fig. 1. The first box in Fig. 1 corresponds to an initial sequence, consisting of two input commitments and a helping red card; X_{00}, X_{01}, X_{10}, and X_{11} represent the probabilities of $(a, b) = (0, 0), (a, b) = (0, 1), (a, b) = (1, 0)$, and $(a, b) = (1, 1)$, respectively. In the second box (and below), we write X_0 rather than $X_{00} + X_{01} + X_{10}$ and write X_1 instead of X_{11}. A polynomial, such as $\frac{1}{5}X_0$ and $\frac{1}{3}X_1$, represents the conditional probability that the current sequence is the one next to the polynomial, given the view seen on the table. Looking at the two boxes at the bottom, one can see that a commitment to $a \wedge b$ is definitively obtained. Furthermore, in each box, the sum of all polynomials is equal to $X_0 + X_1$, implying that no information about a and b leaks.

Thus, the KWH-tree in Fig. 1 guarantees that our protocol is correct and secure.

Optimality of Our Protocol

As presented above, we constructed a five-card AND protocol in committed format using random cuts and random bisection cuts that are sufficiently practical for humans to implement, solving an important open problem [6,7]. Therefore, we have the following theorem.

Theorem 1 *There exists a 5-card expected-finite-runtime AND protocol in committed format with only uniform cyclic shuffles.*

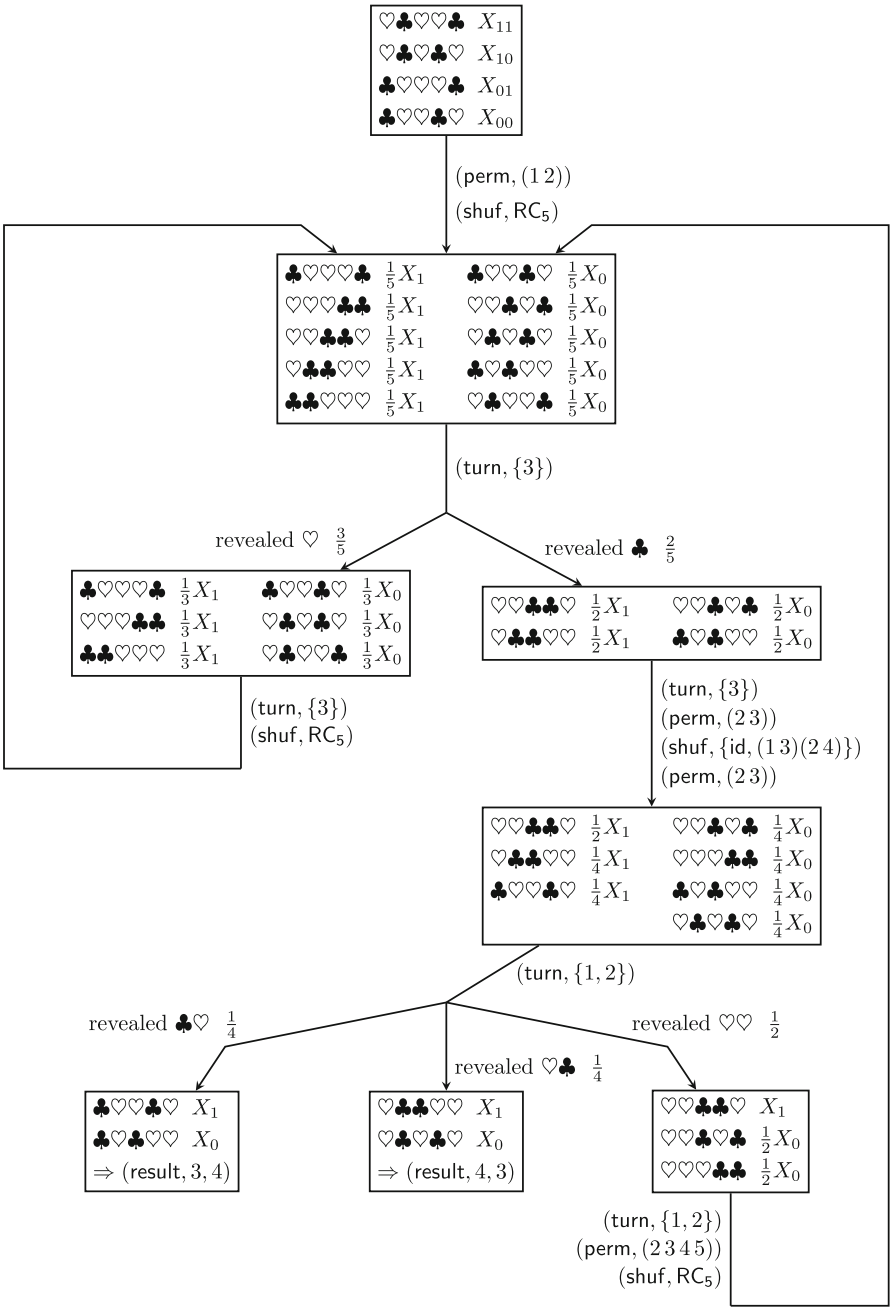


Fig. 1 The KWH-tree for our first five-card AND protocol

Given that the previous "practical" AND protocol [10] uses six cards, as mentioned in Section 1.2, our protocol reduced the number of required cards from six to five, and one might presume that the contribution of this protocol is only incremental. However, we believe that this is not the case. One reason for this is that a "practical" committed-format AND protocol with five cards or less has been solicited for many years since the six-card AND protocol [10] appeared in 2009. Another reason is that our five-card AND protocol using only uniform cyclic shuffles is the *best possible*, because the following lower bounds have been found.

Theorem 2 [4] *There is no five-card finite-runtime AND protocol in committed format with only closed shuffles.*

Theorem 3 [4] *There is no four-card expected-finite-runtime AND protocol in committed format with only uniform closed shuffles.*

Theorem 3 implies that we need at least five cards to have a protocol using only uniform closed shuffles; moreover, even though we have five cards, Theorem 2 dictates that we cannot have a finite-runtime protocol. Thus, considering five-card expected-finite-runtime protocols is the only possible option. Consequently, Theorems 1, 2, and 3 together imply that, in this context, our proposed protocol is optimal.

Another Five-Card Protocol Using a Less Number of Shuffles

Recall that our five-card AND protocol presented in Sect. 2 uses seven shuffles on average. In this section, we show that one can decrease the number of required shuffles to 4.5 by designing a somewhat complicated protocol.

Idea and Description

Remember Step 3 of our first protocol presented in Section 2.2: If the face-up card is $\boxed{\heartsuit}$, go back to the previous step to apply a random cut again; only when the face-up card is $\boxed{\clubsuit}$, move forward. Therefore, if we can move forward even if the face-up card is $\boxed{\heartsuit}$, we have a chance to reduce the number of required shuffles. This is the main idea behind our second protocol.

Figure 2 is the (partial) KWH-tree of our second five-card AND protocol, which uses a less number of shuffles compared to the first protocol (presented in Sect. 2), as follows.

Comparing Fig. 2 with Fig. 1 (that is, contrasting the KWH-tree of the second protocol with that of the first protocol) reveals that they are similar: The first box and the second box named (A) in Fig. 2 are the same as the ones in Fig. 1, and box (B) and all the boxes following box (C) (including (C) itself) are also the same as the ones in Fig. 1. The only difference appears after box (B): while it always goes back to (A) after (B) in the first protocol (namely, Fig. 1), there are three possibilities in the second protocol (namely, Fig. 2) via the "See Fig. 3 box" part. That is, it goes back to (A) with a probability of $1/6$, it terminates with a probability of $1/3 + 1/6$, and it goes

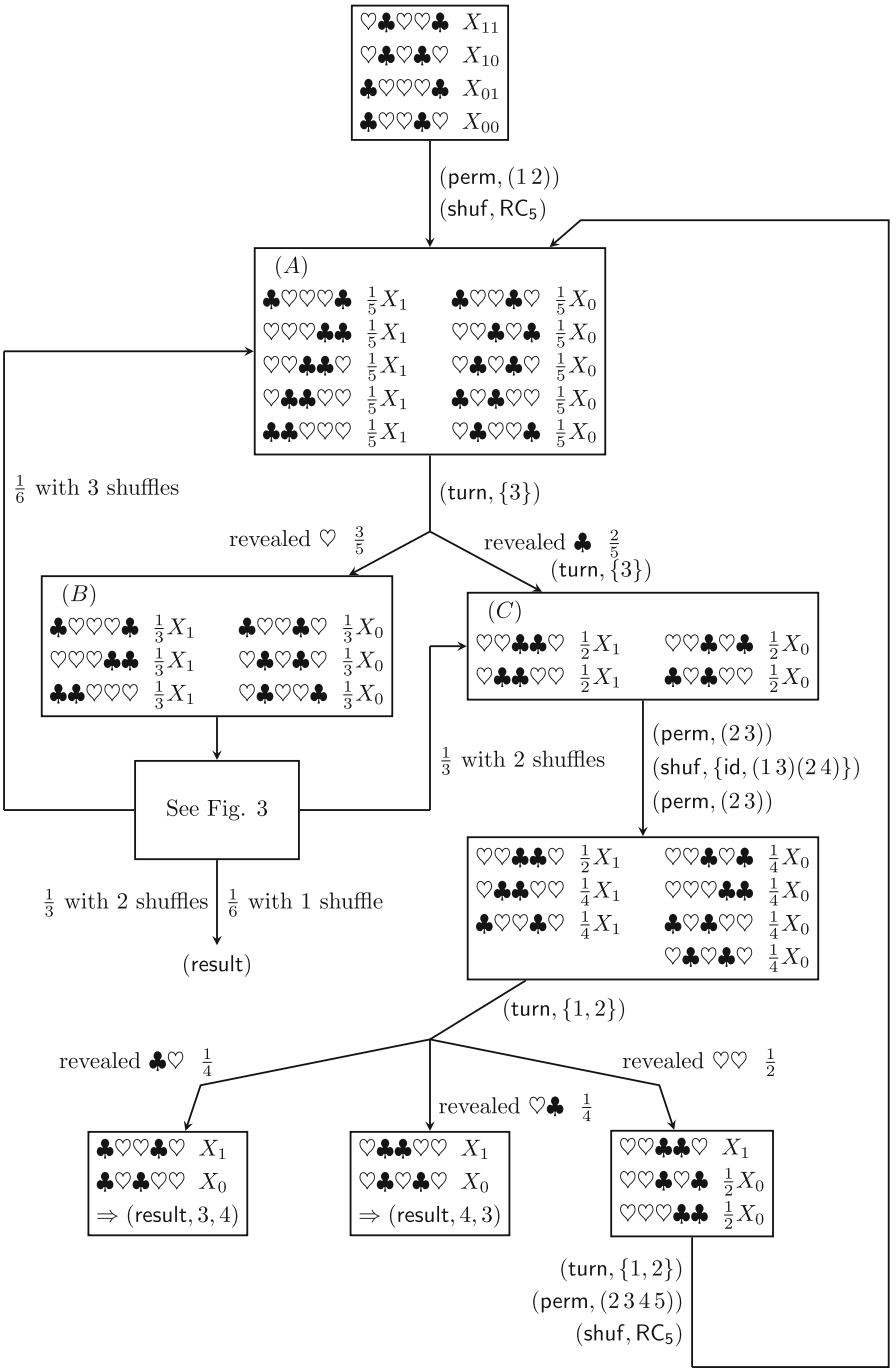


Fig. 2 The KWH-tree for our second five-card AND protocol (Part I)

to (C) with a probability of $1/3$. This contributes to reducing the expected number of trials, as imagined.

Specifically, to count the expected number of shuffles, let N_A be the expected number of shuffles from box (A) to the end of the protocol, and let N_C be the expected number of shuffles from box (C) to the end. Then,

$$N_A = \frac{3}{5}\left(\frac{3+N_A}{6} + \frac{2}{3} + \frac{1}{6} + \frac{2+N_C}{3}\right) + \frac{2}{5}N_C$$

and

$$N_C = 1 + \frac{1+N_A}{2},$$

and hence, we have $N_A = 3.5$. Therefore, the total number of shuffles is $1+N_A = 4.5$ on average.

The details of the "See Fig. 3 box" part are shown in Fig. 3. Thus, Figs. 2 and 3 complete the description of our second five-card AND protocol (whose pseudocode will be presented in the next subsection). Because we can easily confirm that the KWH-tree for our second protocol also satisfies the required properties, it is correct and secure.

Pseudocode

The following is a pseudocode for the second protocol.

---

input set:

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

(perm, (1 2))
(turn, {3})
1 (shuf, RC_5)
(turn, {3})
if visible seq. = (?, ?, ♡, ?, ?) **then**
  (turn, {3})
  (perm, (2 3)(4 5))
  (shuf, {id, (1 3)(2 4)})
  (turn, {1})
  if visible seq. = (♣, ?, ?, ?, ?) **then**
    (turn, {1})
    (perm, (2 3)(4 5))
    (shuf, {id, (1 3)(2 4)})
    (turn, {2, 4})

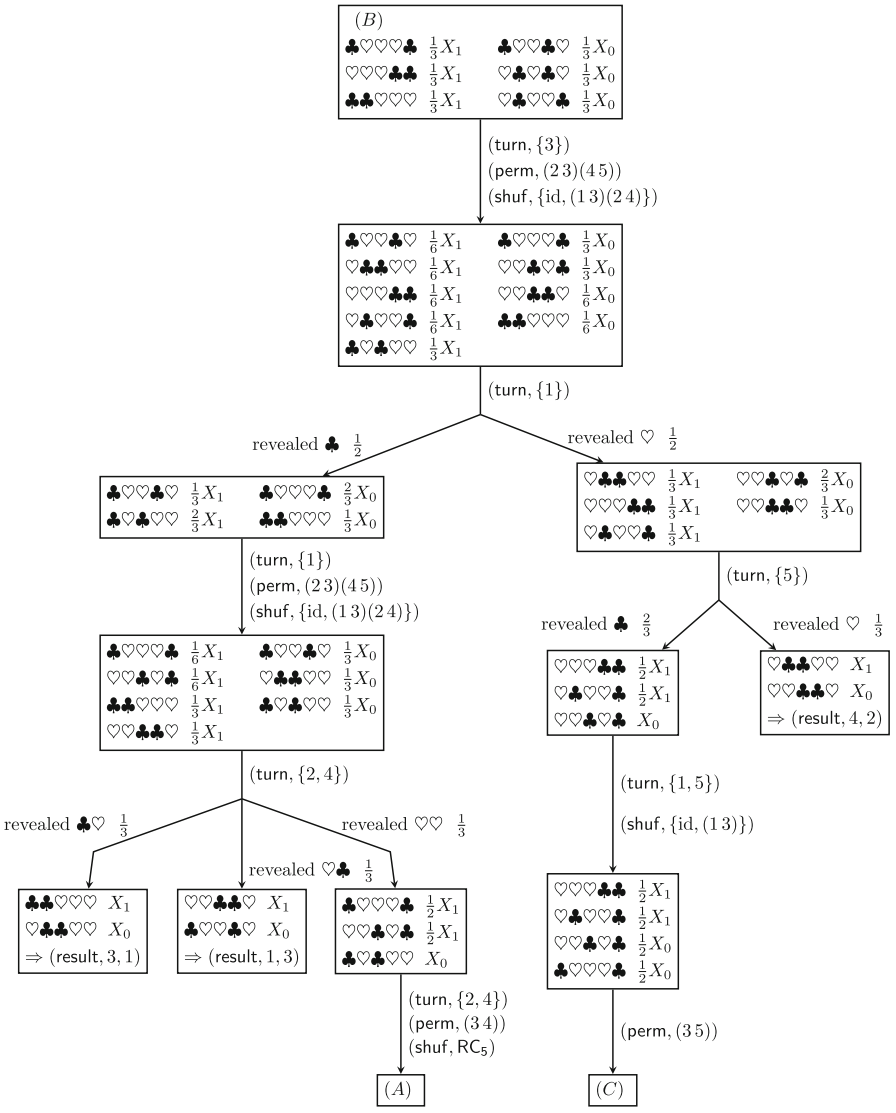


Fig. 3 The KWH-tree for our second five-card AND protocol (Part II)

if visible seq. = (?, ♣, ?, ♡, ?) **then**
  (result, 3, 1)
else if visible seq. = (?, ♡, ?, ♣, ?) **then**
  (result, 1, 3)
else if visible seq. = (?, ♡, ?, ♡, ?) **then**
  (turn, {2, 4})
  (perm, (3 4))
  goto 1

```
    else if visible seq. = (♡, ?, ?, ?, ?) then
      (turn, {5})
      if visible seq. = (♡, ?, ?, ?, ♣) then
        (turn, {1, 5})
        (shuf, {id, (1 3)})
        (perm, (3 5))
        goto 2
      else if visible seq. = (♡, ?, ?, ?, ♡) then
        (result, 4, 2)
  else if visible seq. = (?, ?, ♣, ?, ?) then
    (turn, {3})
2   (perm, (2 3))
    (shuf, {id, (1 3)(2 4)})
    (perm, (2 3))
    (turn, {1, 2})
    if visible seq. = (♡, ♡, ?, ?, ?) then
      (turn, {1, 2})
      (perm, (2 3 4 5))
      goto 1
    else if visible seq. = (♣, ♡, ?, ?, ?) then
      (result, 3, 4)
    else if visible seq. = (♡, ♣, ?, ?, ?) then
      (result, 4, 3)
```

Conclusion

In this paper, we first constructed a five-card AND protocol in committed format using only random cuts and random bisection cuts. This nicely has closed the open problem, and our protocol is optimal, as shown in Theorems 1, 2, and 3.

In addition, whereas our five-card AND protocol in Sect. 2 uses seven shuffles on average, we were successful in reducing the expected number of shuffles from 7 to 4.5 with the same number of cards (five) and the same allowed shuffles (uniform cyclic shuffles) by changing part of the protocol.

It is an intriguing open problem to determine whether we can reduce the expected number of shuffles to less than 4.5 with the same conditions.

All the protocols mentioned thus far in this paper can be executed publicly: every operation by players is supposed to be conducted with all eyes fixed on how the cards are manipulated. In contrast, there is another model wherein players are allowed to use "private" operations: it is known that such a somewhat strong assumption results in protocols with fewer cards, e.g., [11,12,14,15,20].

Acknowledgements We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. This work was supported by JSPS KAKENHI Grant number JP17K00001.

References

1. Abe, Y., Hayashi, Y., Mizuki, T., Sone, H.: Five-card AND protocol in committed format using only practical shuffles. In: Proceedings of the 5th ACM ASIA Public-Key Cryptography Workshop, APKC '18, pp. 3–8. ACM, New York, NY, USA (2018). https://doi.org/10.1145/3197507.3197510
2. den Boer, B.: More efficient match-making and satisfiability: the five card trick. In: Quisquater, J.J., Vandewalle, J. (eds.) Advances in Cryptology–EUROCRYPT '89, Lecture Notes in Computer Science, vol. 434, pp. 208–217. Springer, Berlin (1990). https://doi.org/10.1007/3-540-46885-4_23
3. Crépeau, C., Kilian, J.: Discreet solitary games. In: Stinson, D.R. (ed.) Advances in Cryptology–CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 319–330. Springer, Berlin (1994). https://doi.org/10.1007/3-540-48329-2_27
4. Kastner, J., Koch, A., Walzer, S., Miyahara, D., Hayashi, Y., Mizuki, T., Sone, H.: The minimum number of cards in practical card-based protocols. In: Takagi, T., Peyrin, T. (eds.) Advances in Cryptology–ASIACRYPT 2017, Lecture Notes in Computer Science, vol. 10626, pp. 126–155. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70700-6_5
5. Koch, A.: The landscape of optimal card-based protocols. Cryptology ePrint Archive, Report 2018/951 (2018). https://eprint.iacr.org/2018/951
6. Koch, A., Walzer, S.: Foundations for actively secure card-based cryptography. In: Farach-Colton, M., Prencipe, G., Uehara R (eds.) 10th International Conference on Fun with Algorithms (FUN 2021), vol. 157, pp. 17:1, 17:23, Schloss Dagstuhl–Leibniz-Zentrum für Informatik, Germany (2020). https://doi.org/10.4230/LIPIcs.FUN.2021.17
7. Koch, A., Walzer, S., Härtel, K.: Card-based cryptographic protocols using a minimal number of cards. In: Iwata, T., Cheon, J.H. (eds.) Advances in Cryptology–ASIACRYPT 2015, Lecture Notes in Computer Science, vol. 9452, pp. 783–807. Springer, Berlin (2015). https://doi.org/10.1007/978-3-662-48797-6_32
8. Mizuki, T., Shizuya, H.: A formalization of card-based cryptographic protocols via abstract machine. Int. J. Inf. Secur. **13**, 15–23 (2014). https://doi.org/10.1007/s10207-013-0219-4
9. Mizuki, T., Shizuya, H.: Computational model of card-based cryptographic protocols and its applications. In: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E100-A, pp. 3–11. The Institute of Electronics, Information and Communication Engineers (2017)
10. Mizuki, T., Sone, H.: Six-card secure AND and four-card secure XOR. In: Deng, X., Hopcroft, J.E., Xue, J. (eds.) Frontiers in Algorithmics, Lecture Notes in Computer Science, vol. 5598, pp. 358–369. Springer, Berlin (2009). https://doi.org/10.1007/978-3-642-02270-8_36
11. Nakai, T., Shirouchi, S., Iwamoto, M., Ohta, K.: Four cards are sufficient for a card-based three-input voting protocol utilizing private permutations. In: Shikata, J. (ed.) International Conference on Information Theoretic Security, ICITS 2017, Lecture Notes in Computer Science, vol. 10681, pp. 153–165. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-72089-0_9
12. Nakai, T., Tokushige, Y., Misawa, Y., Iwamoto, M., Ohta, K.: Efficient card-based cryptographic protocols for millionaires' problem utilizing private permutations. In: Foresti, S., Persiano, G. (eds.) Cryptology and Network Security, CANS 2016, Lecture Notes in Computer Science, vol. 10052, pp. 500–517. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-48965-0_30
13. Niemi, V., Renvall, A.: Secure multiparty computations without computers. Theor. Comput. Sci. **191**, 173–183 (1998). https://doi.org/10.1016/S0304-3975(97)00107-2

14. Ono, H., Manabe, Y.: Card-based cryptographic protocols with the minimum number of cards using private operations. In: Zincir-Heywood, N., Bonfante, G., Debbabi, M., Garcia-Alfaro, J. (eds.) Foundations and Practice of Security, Lecture Notes in Computer Science, vol. 11358, pp. 193–207. Springer, Cham (2019)
15. Ono, H., Manabe, Y.: Card-based cryptographic protocols with the minimum number of rounds using private operations. In: Pérez-Solà, C., Navarro-Arribas, G., Biryukov, A., Garcia-Alfaro, J. (eds.) Data Privacy Management, Cryptocurrencies and Blockchain Technology. Lecture Notes in Computer Science, vol. 11737, pp. 156–173. Springer, Cham (2019)
16. Ruangwises, S., Itoh, T.: AND Protocols Using only Uniform Shuffles. Computer Science—Theory and Applications. Lecture Notes in Computer Science, vol. 11532, pp. 349–358. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-19955-5_30
17. Stiglic, A.: Computations with a deck of cards. Theor. Comput. Sci. **259**, 671–678 (2001). https://doi.org/10.1016/S0304-3975(00)00409-6
18. Ueda, I., Miyahara, D., Nishimura, A., Hayashi, Y., Mizuki, T., Sone, H.: Secure implementations of a random bisection cut. Int. J. Inf. Sec. **19**(4), 445–452 (2020). https://doi.org/10.1007/s10207-019-00463-w
19. Ueda, I., Nishimura, A., Hayashi, Y., Mizuki, T., Sone, H.: How to implement a random bisection cut. In: Martín-Vide, C., Mizuki, T., Vega-Rodríguez, M.A. (eds.) Theory and Practice of Natural Computing, Lecture Notes in Computer Science, vol. 10071, pp. 58–69. Springer International Publishing, Cham (2016). https://doi.org/10.1007/978-3-319-49001-4_5
20. Watanabe, Y., Kuroki, Y., Suzuki, S., Koga, Y., Iwamoto, M., Ohta, K.: Card-based majority voting protocols with three inputs using three cards. In: 2018 International Symposium on Information Theory and Its Applications (ISITA), pp. 218–222 (2018). https://doi.org/10.23919/ISITA.2018.8664324