Card-Based Protocols for Securely Computing the Conjunction of Multiple Variables*

Takaaki Mizuki

Tohoku University
tm-paper+cardconjweb[atmark]g-mail.tohoku-university.jp

Abstract

Consider a deck of real cards with faces that are either black or red and backs that are all identical. Then, using two cards of different colors, we can commit a secret bit to a pair of face-down cards so that its order (i.e., black to red, or red to black) represents the value of the bit. Given such two commitments (consisting of four face-down cards in total) together with one additional black card, the "five-card trick" invented in 1989 by den Boer securely computes the conjunction of the two secret bits. In 2012, it was shown that such a two-variable secure AND computation can be done with no additional card. In this paper, we generalize this result to an arbitrary number of variables: we show that, given any number of commitments, their conjunction can be securely computed with no additional card.

1 Introduction

Consider a deck of real physical cards with faces that are either black ($\boxed{\clubsuit}$) or red ($\boxed{\heartsuit}$) and backs ($\boxed{?}$) that are all identical. Then, using a black card and a red one, we can commit a bit $x \in \{0, 1\}$ to a pair of face-down cards $\boxed{?}\boxed{?}$ in accordance with the following encoding:

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

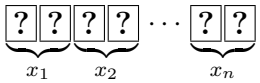
Such a pair of face-down cards is called a *commitment* to the bit x, and is expressed as

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

It has been known since 1989 [1] that a deck of cards of this kind enables us to perform secure computation and, indeed, several card-based cryptographic protocols have been reported in

*This is an accepted manuscript for publication in Theoretical Computer Science. Copyright © 2016. This manuscript version is made available under the CC-BY-NC-ND 4.0 license http://creativecommons.org/licenses/by-nc-nd/4.0/. The formal publication is available via DOI: 10.1016/j.tcs.2016.01.039. The Received Date and the Revised Date are August 29, 2014 and October 19, 2015, respectively. It should be noted that Koch et al. presented a Las Vegas four-card committed AND protocol at Asiacrypt 2015, by which n-variable secure conjunction can also be conducted with no additional card.

the literature (e.g. [2, 4, 5, 7, 9, 10]). Briefly summarizing our main result in this paper, we propose a new, efficient protocol that securely computes the conjunction $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ for given commitments



to n bits $x_1, x_2, \ldots, x_n \in \{0, 1\}$.

This paper begins with a review of the history of card-based protocols.

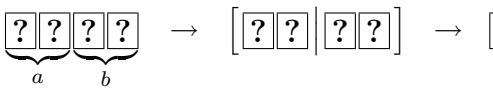
1.1 The History

The first card-based protocol, the "five-card trick," invented in 1989 by den Boer [1] securely computes the conjunction (that is, the AND function) of two secret bits. Specifically, given commitments to bits $a, b \in \{0, 1\}$ together with one additional black card

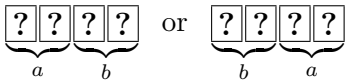
the five-card trick allows us to learn only the value of $a \wedge b$ (without revealing more of the values a and b themselves than necessary). Thus, it uses five cards in total.

In 2012, it was shown that such a two-variable secure AND computation can be done with no additional card [5]: given commitments to $a, b \in \{0, 1\}$, we execute the following "four-card AND protocol" publicly to learn only the value of $a \wedge b$. (The main aim of this paper is to generalize this 2-variable solution to an arbitrary number of variables.)

1. Apply a *random bisection cut*, which means to bisect the sequence of four cards and switch the two halves randomly:

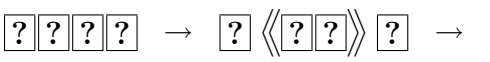
   

   it means that the resulting deck is either

   where each case occurs with probability of exactly 1/2.

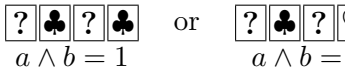
2. Shuffle the two cards in the middle:

   (That is, the middle two cards are switched with probability of exactly 1/2.)

3. Reveal the second card from the left.

   (a) If it is ♣, then we reveal the fourth card, and have either

(b) If it is $\boxed{\heartsuit}$, then we reveal the first card, and have either

$$\underset{a \wedge b = 0}{\boxed{\clubsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}} \quad \text{or} \quad \underset{a \wedge b = 1}{\boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}}.$$

As assumed in this four-card AND protocol, card-based protocols are usually executed publicly with all eyes fixed on the procedure. We are allowed to shuffle some portion of the cards, rearrange their order, and turn over some of them. A formal treatment and a rigorous mathematical model for card-based protocols appear in [3]; we are able to describe all the protocols (including the protocols constructed later in this paper) within the model. Furthermore, there is a known procedure [6] for proving that a given pair of face-down cards is surely a commitment to some bit, i.e., it consists of two cards of different colors, without revealing its bit value (like zero-knowledge proof). In addition, typically, information-theoretically secure protocols are solicited; the four-card AND protocol above computes $a \wedge b$ information-theoretically securely, that is, no information other than the value of $a \wedge b$ leaks.

As explained above, the five-card trick [1] and the four-card AND protocol [5] securely compute the conjunction of two variables; they produce their output (the value of $a \wedge b$) publicly, i.e., the output is in a "non-committed format." In contrast, there are protocols that produce the output in a "committed format," i.e., the output is obtained as a commitment such as

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

following the encoding rule (1) [2, 4, 7, 10].

Note that secure NOT computation is trivial: just swapping the two cards constituting a commitment to a bit x results in a commitment to the negation $\bar{x}$:

$$\underbrace{\boxed{?}\boxed{?}}_{x} \rightarrow \overset{\rightleftharpoons}{\boxed{?}\boxed{?}} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{\bar{x}}.$$

1.2 Our Results

Recall our goal. Given n commitments

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

we want to securely compute the conjunction $x_1 \wedge x_2 \wedge \cdots \wedge x_n$. To this end, we design three protocols, the main specifications of which are as follows.

	# of cards	committed?
Straightforward Protocol (§2)	$2n+2$	yes
One-additional-card Protocol (§3)	$2n+1$	no
No-additional-card Protocol (§4)	$2n$	no

The first protocol (Straightforward Protocol) is a straightforward implementation of n-variable secure conjunction based on the known results. In other words, as implied in the previous subsection, such a secure computation can be done by applying the existing "committed" protocols: for example, repeating Mizuki-Sone AND protocol [4] $n-1$ times with two additional cards brings a commitment to $x_1 \wedge x_2 \wedge \cdots \wedge x_n$. In Section 2, we introduce such a straightforward implementation together with the description of the known protocol. Thus, secure conjunction of n variables can be done with two additional cards: that is, $2n+2$ cards in total.

The second protocol (One-additional-card Protocol) needs one card fewer than the Straightforward Protocol but it does not produce its output as a commitment. In Section 3, we show that n-variable secure conjunction can be conducted with only one additional card: $2n+1$ cards in total. As will be seen later, the tailor-made protocol that we design is simple and easy to understand.

In Section 4, we present a more elaborate protocol (No-additional-card Protocol) which does not need any additional card. That is, we can securely compute the conjunction $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ using only the given n commitments: the protocol uses exactly $2n$ cards in total.

This paper concludes in Section 5 with some discussion and open problems.

2 Applying a Known Protocol

In this section, we introduce a known "committed" AND protocol, Mizuki-Sone AND protocol [4]. Applying the known protocol, secure n-variable conjunction can be straightforwardly done with two additional cards, as described below.

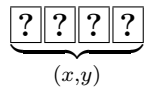
We first introduce some notation [9]. Define two operations for a pair of bits (x, y):

$$\begin{aligned} \mathsf{get}^0(x,y) &= x; \\ \mathsf{get}^1(x,y) &= y; \\ \mathsf{shift}^0(x,y) &= (x,y); \\ \mathsf{shift}^1(x,y) &= (y,x). \end{aligned}$$

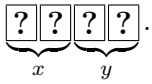
Thus, $\mathsf{get}^0(x, y)$ returns the first bit, $\mathsf{get}^1(x, y)$ returns the second bit, $\mathsf{shift}^0(x, y)$ returns the two bits without change, and $\mathsf{shift}^1(x, y)$ swaps the two bits. Note that, using these operations, the AND function can be written as

$$a \wedge b = \mathsf{get}^{b \oplus r}(\mathsf{shift}^r(0, a)) \tag{2}$$

for any bit $r \in \{0, 1\}$. Hereafter, for two bits x and y, the expression



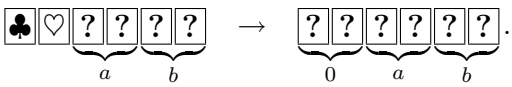
means



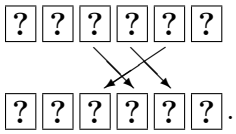
.

Then, Mizuki-Sone AND protocol [4] can be described as follows.

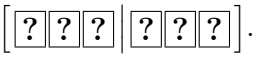
1. Arrange two commitments along with two additional cards:



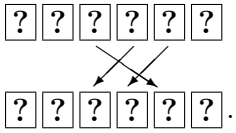
2. Rearrange the sequence of six cards:



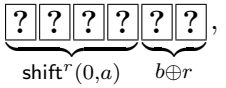
3. Apply a random bisection cut:



4. Rearrange the sequence of six cards again:

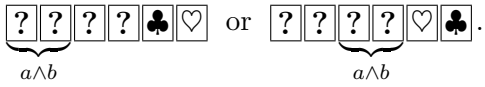


   Then, we have



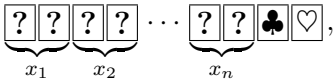
   where r is a (uniformly distributed) random bit because of the random bisection cut.

5. Remember Eq. (2), that is, if $b \oplus r = 0$, then $a \wedge b = \mathsf{get}^0(\mathsf{shift}^r(0, a))$; otherwise, $a \wedge b = \mathsf{get}^1(\mathsf{shift}^r(0, a))$. Reveal the fifth and sixth cards. Then, a commitment to $a \wedge b$ is obtained as follows:



Note that revealing the commitment to $b \oplus r$ in step 5 does not leak any information about b because r is random. In addition, the two revealed cards can be reused for another computation.

Applying Mizuki-Sone AND protocol above, the conjunction $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ of n variables can be securely computed. That is, given n commitments and two additional cards



we can straightforwardly obtain a commitment to $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ by repeating the known protocol $n - 1$ times.

3 Secure Conjunction with One Additional Card

In this section, we present a simple protocol for securely computing the n-variable conjunction with one additional card, where its output is not in a (normal) committed format.

We first define a "single-card commitment" in Section 3.1, and then present a building block in Section 3.2. Using the building block, we construct a new protocol for computing the conjunction in Section 3.3.

3.1 Single-Card Commitments

Consider an encoding rule for a single card

$$\boxed{\clubsuit} = 0, \quad \boxed{\heartsuit} = 1. \tag{3}$$

For a bit $x \in \{0, 1\}$, a face-down card $\boxed{?}$ holding the value of x in accordance with the encoding rule (3) is called a *single-card commitment* to x, and is expressed as

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

Note that a (normal) commitment

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

can therefore be written as single-card commitments to x and its negation

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

Furthermore, it seems to be difficult to have a secure NOT computation for a single-card commitment.

Hereafter, for a pair $(x, y) \in \{0, 1\}^2$, the expression

$$\underbrace{\boxed{?}\boxed{?}}_{(x,y)}$$

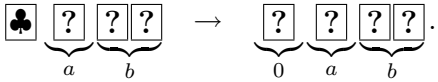
means

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

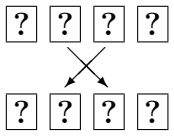
3.2 A Building Block

Here, as a building block, we design a "single-card-committed" AND protocol. That is, given a single-card commitment to a bit a and a commitment to a bit b, one additional black card is sufficient to produce securely a single-card commitment to $a \wedge b$. The idea is closely related to Mizuki-Sone AND protocol [4] (described in Section 2).

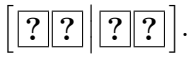
1. Arrange a single-card commitment followed by a commitment, along with an additional black card:



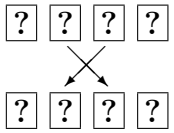
2. Rearrange the sequence of four cards:



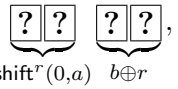
3. Apply a random bisection cut:



4. Rearrange the sequence of four cards again:

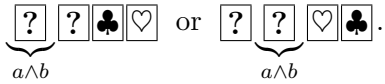


   Then, we have



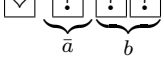
   where r is a random bit because of the random bisection cut.

5. Reveal the third and fourth cards. Then, a single-card commitment to $a \wedge b$ is obtained as follows:



Since r is random, revealing the commitment to $b \oplus r$ in step 5 does not leak any information about a and b.

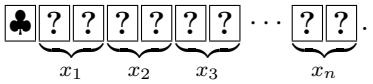
Note that we can also easily obtain a NAND protocol just by starting from



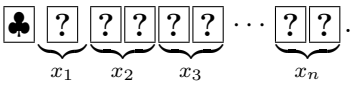
3.3 A Protocol for More Than Two Variables

Using the single-card-committed AND protocol above, we can easily construct a secure n-variable conjunction protocol which uses $2n + 1$ cards, as follows.

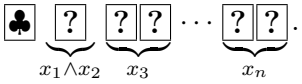
1. Arrange n commitments along with one additional black card:



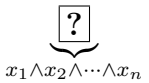
2. Split the commitment to x_1 into two single-card commitments (and discard the single-card commitment to $\overline{x}_1$):



3. Apply the single-card-committed AND protocol to the first four cards (from the left), then we obtain a single-card commitment to $x_1 \wedge x_2$ and two revealed cards (and discard the red card and the remaining face-down card):



4. Repeat this until we obtain a single-card commitment



to $x_1 \wedge x_2 \wedge \cdots \wedge x_n$.

Note that all discarded (face-down) cards must not be revealed; however, once the commitment to $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ is revealed, we may reveal the discarded cards after shuffling. Furthermore, one might think that it could be executed with $2n$ cards (instead of $2n+1$ cards) if we started from step 2; however, that is not the case because we need two cards of different colors to create a single-card commitment to x_1.

4 Secure Conjunction with No Additional Card

In the previous section, we described a secure n-variable conjunction protocol which needs one additional card. In this section, we improve the result further so that the same cryptographic task can be done without any additional card.

We first define a "color-based commitment" in Section 4.1, and present a building block in Section 4.2. Then, we construct efficient protocols for $n = 3$, $n = 4$, and $n \geq 5$ in Sections 4.3, 4.4, and 4.5, respectively.

4.1 Color-Based Commitments

Here, for later use, we introduce "color-based commitments" as follows.

For a bit $x \in \{0, 1\}$, a pair of face-down cards $\boxed{?}\boxed{?}$ holding the value of x in accordance with the encoding rule

$$\boxed{\clubsuit}\boxed{\heartsuit} \text{ or } \boxed{\heartsuit}\boxed{\clubsuit} = 0, \quad \boxed{\clubsuit}\boxed{\clubsuit} = 1 \tag{4}$$

is called a *black-based commitment* to x, and is expressed as

Similarly, a pair of face-down cards for which a bit x satisfies the encoding

$$\boxed{\clubsuit}\boxed{\heartsuit} \text{ or } \boxed{\heartsuit}\boxed{\clubsuit} = 0, \quad \boxed{\heartsuit}\boxed{\heartsuit} = 1 \tag{5}$$

is called a *red-based commitment* to x, and is expressed as

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

Note that

$$\underbrace{\boxed{?}\boxed{?}}_{[0]^{\clubsuit}} \text{ and } \underbrace{\boxed{?}\boxed{?}}_{[0]^{\heartsuit}}$$

do not determine the orders of the two colors ($\boxed{\clubsuit}\boxed{\heartsuit}$ or $\boxed{\heartsuit}\boxed{\clubsuit}$) uniquely.

4.2 A Building Block

Recall the four-card AND protocol [5] described in Section 1.1. Given commitments

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

the outputs are

$$\text{(a)} \ \underset{a\wedge b=1}{\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\clubsuit}} \ \text{or} \ \underset{a\wedge b=0}{\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{\heartsuit}}; \qquad \text{(b)} \ \underset{a\wedge b=0}{\boxed{\clubsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}} \ \text{or} \ \underset{a\wedge b=1}{\boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}}.$$

Notice that the output (namely, the two revealed cards) follows the encoding rules (4) and (5) defined in the previous subsection. That is, if the two revealed cards have different colors, then $a \wedge b = 0$; otherwise, $a \wedge b = 1$. Note that the two face-down cards also follow the encoding rules. For example, for case (b), the two face-down cards constitute a black-based commitment to $a \wedge b$: we can write

$$\boxed{\clubsuit}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{[a\wedge b]^{\clubsuit}} \ \text{or} \ \boxed{\heartsuit}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{[a\wedge b]^{\clubsuit}}$$

(although the value of the black-based commitment is no longer hidden).

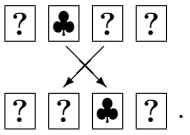
The observation above along with a slight modification of the four-card AND protocol [5] provides the following "color-based-committed" AND protocol.

1. Apply a random bisection cut, and shuffle the two cards in the middle:

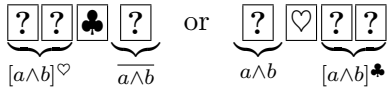
$$\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b} \ \rightarrow \ \left[\boxed{?}\boxed{?}\,\middle|\,\boxed{?}\boxed{?}\right] \ \rightarrow \ \boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

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

2. Reveal the second card. Only if it is $\boxed{\clubsuit}$, rearrange the sequence:



Then, we have

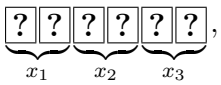


Note that after execution of the protocol, no information about a and b has leaked. Of course, opening the single-card commitment to $\overline{a \wedge b}$ or $a \wedge b$ (being in step 2) enables us to learn only the value of $a \wedge b$. Alternatively, we can learn the value of $a \wedge b$ by revealing the color-based commitment, but we must shuffle the two cards before revealing them to avoid leaking information about a and b.

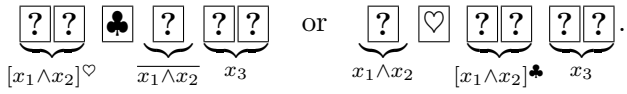
4.3 A Protocol for Three Variables

In this subsection, applying the building block given in the previous subsection, we present a protocol for the case of $n = 3$.

1. Starting from three commitments

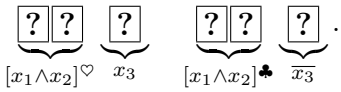


apply the color-based-committed AND protocol (presented in Section 4.2) to the first four cards, then we have either



2. Turn over the face-up card, then, in either case, we have

3. Split the commitment to x_3, and place the single-card commitments as follows:



Note that, only when $x_1 \wedge x_2 \wedge x_3 = 1$, the sequence of six cards will be $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\ \boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}$.

4. Apply shuffles and a random bisection cut:

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

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

5. Reveal the three cards on the left side. If they are $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}$ or $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, then $x_1 \wedge x_2 \wedge x_3 = 1$; otherwise, $x_1 \wedge x_2 \wedge x_3 = 0$.

Note that when $x_1 \wedge x_2 \wedge x_3 = 0$, one of $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}$, $\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ and their permutations appears; in each case, we cannot determine whether (i) $x_1 \wedge x_2 = 0$ and $x_3 = 0$, (ii) $x_1 \wedge x_2 = 1$ and $x_3 = 0$, or (iii) $x_1 \wedge x_2 = 0$ and $x_3 = 1$. A formal proof of the secrecy is below.

Proof. Without loss of generality, we assume that the three cards revealed in step 5 are $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}$, $\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}$ or $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}$ (i.e., two $\boxed{\clubsuit}$s appear), and denote this event by $\mathcal{E}$. Then, we have $x_1 \wedge x_2 \wedge x_3 = 0$, of course, and there are three events $\mathcal{E}^{(\mathrm{i})}$, $\mathcal{E}^{(\mathrm{ii})}$ and $\mathcal{E}^{(\mathrm{iii})}$ which partition $\mathcal{E}$: (i) $x_1 \wedge x_2 = 0$ and $x_3 = 0$, (ii) $x_1 \wedge x_2 = 1$ and $x_3 = 0$, or (iii) $x_1 \wedge x_2 = 0$ and $x_3 = 1$; in case (i) the three revealed cards have come from the left half

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

of the sequence in step 3, while in cases (ii) and (iii) they have come from the right half

$$\underbrace{\boxed{?}\boxed{?}}_{[x_1 \wedge x_2]^{\clubsuit}}\ \underbrace{\boxed{?}}_{\overline{x_3}}.$$

Therefore,

$$\begin{aligned}
\Pr[\mathcal{E}^{(\mathrm{i})}] &= \Pr[x_1 \wedge x_2 = 0,\ x_3 = 0] \cdot 1/2, \\
\Pr[\mathcal{E}^{(\mathrm{ii})}] &= \Pr[x_1 \wedge x_2 = 1,\ x_3 = 0] \cdot 1/2, \\
\Pr[\mathcal{E}^{(\mathrm{iii})}] &= \Pr[x_1 \wedge x_2 = 0,\ x_3 = 1] \cdot 1/2.
\end{aligned}$$

Since $\Pr[\mathcal{E}^{(\mathrm{i})}] + \Pr[\mathcal{E}^{(\mathrm{ii})}] + \Pr[\mathcal{E}^{(\mathrm{iii})}] = \Pr[x_1 \wedge x_2 \wedge x_3 = 0] \cdot 1/2$, we have

$$\begin{aligned}
\Pr[x_1 \wedge x_2 = 0,\ x_3 = 0 \mid \mathcal{E}] &= \frac{\Pr[x_1 \wedge x_2 = 0,\ x_3 = 0,\ \mathcal{E}]}{\Pr[\mathcal{E}]} \\
&= \frac{\Pr[\mathcal{E}^{(\mathrm{i})}]}{\Pr[\mathcal{E}^{(\mathrm{i})}] + \Pr[\mathcal{E}^{(\mathrm{ii})}] + \Pr[\mathcal{E}^{(\mathrm{iii})}]} \\
&= \frac{\Pr[x_1 \wedge x_2 = 0,\ x_3 = 0]}{\Pr[x_1 \wedge x_2 \wedge x_3 = 0]} \\
&= \Pr[x_1 \wedge x_2 = 0,\ x_3 = 0 \mid x_1 \wedge x_2 \wedge x_3 = 0].
\end{aligned}$$

Similarly, we have

$$\Pr[x_1 \wedge x_2 = 1,\ x_3 = 0 \mid \mathcal{E}] = \Pr[x_1 \wedge x_2 = 1,\ x_3 = 0 \mid x_1 \wedge x_2 \wedge x_3 = 0]$$

and

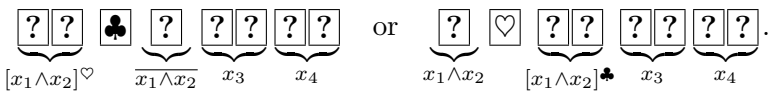
$$\Pr[x_1 \wedge x_2 = 0,\ x_3 = 1 \mid \mathcal{E}] = \Pr[x_1 \wedge x_2 = 0,\ x_3 = 1 \mid x_1 \wedge x_2 \wedge x_3 = 0].$$

Thus, no information about x_1, x_2 and x_3 other than the fact that $x_1 \wedge x_2 \wedge x_3 = 0$ has leaked. □

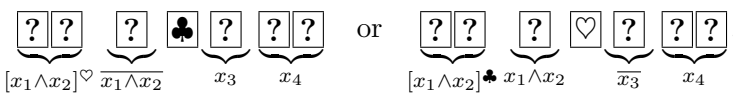
4.4 A Protocol for Four Variables

In this subsection, we present a protocol for the case of $n = 4$.

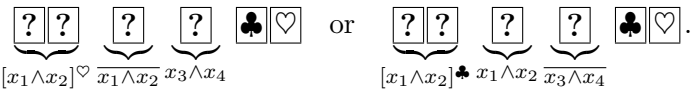
1. After applying the color-based-committed AND protocol (in Section 4.2) to commitments to x_1 and x_2, we have either



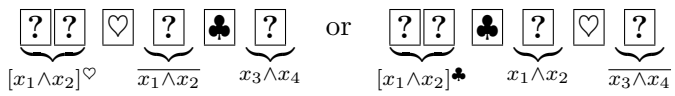
2. Split the commitment to x_3 and rearrange as follows:



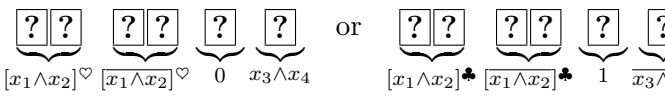
3. Apply the single-card-committed AND/NAND protocol (in Section 3.2) to the rightmost four cards, then we have



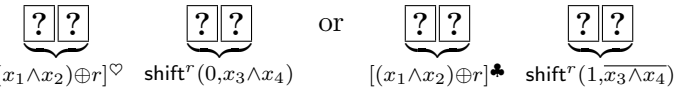
4. Rearrange as follows:



5. Turn over the face-up cards:



6. By some rearrangement and a random bisection cut, we can have



   for a random bit r.

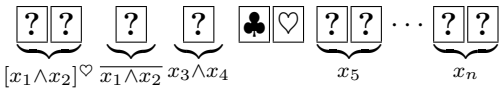
7. Reveal the two cards on the left side after shuffling them, to obtain a single-card commitment to $x_1 \wedge x_2 \wedge x_3 \wedge x_4$ or $\overline{x_1 \wedge x_2 \wedge x_3 \wedge x_4}$.

This protocol is secure because it uses only (perfectly) secure protocols as its subprotocols and revealing the color-based commitment to $(x_1 \wedge x_2) \oplus r$ does not leak any information about x_1 and x_2.

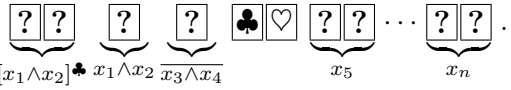
4.5 A Protocol for More Than Four Variables

Finally, we show how to deal with the case of $n \geq 5$ by applying the protocols mentioned thus far.

1. Given n commitments, execute steps 1–3 of the four-variable protocol given in Section 4.4; then, we have either (i)

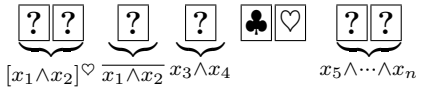


   or (ii)

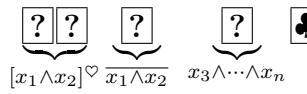


   In the following, we address only case (i) because case (ii) is similar.

2. Using the two face-up cards of different colors, repeatedly execute Mizuki-Sone AND protocol [4] (described in Section 2) so that we have



3. Apply the single-card-committed AND protocol (Section 3.2) so that we have



4. Finally execute steps 4–7 of the four-variable protocol (Section 4.4).

This protocol is also secure because it uses only secure protocols as its sub-protocols.

5 Conclusion

Given two commitments, the five-card trick invented in 1989 [1] securely computes their conjunction in a manner requiring one additional card. In 2012, it was proved that the same task can be done without any additional card [5]. In this paper, we have generalized this result to an arbitrary number of variables. Specifically, we have shown that, given any number of commitments, their conjunction can be securely computed with no additional card.

To execute the protocols described in this paper, we require multiple cards of the same color, say ♣♣♡♡, and hence we have to create a custom-made cards[1] as shown in Figure 1. Therefore, reducing even one additional card required for secure computation is worthwhile.

[1]It should be noted that Niemi and Renvall constructed elegant card-based protocols suited for a standard off-the-shelf deck of playing cards [8]; their 2-variable AND protocol is based on another encoding, uses five cards numbered from 1 to 5, and is a Las Vegas algorithm taking 9.5 trials on the average.

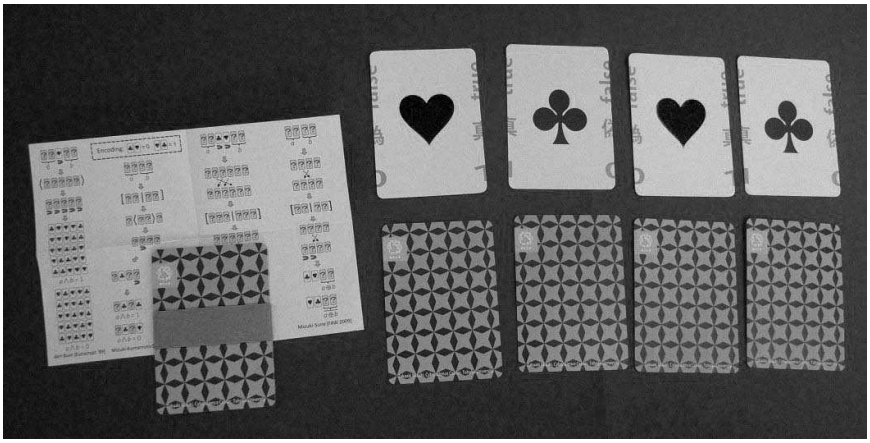


Figure 1: Custom-made cards suited for card-based protocols.

An intriguing problem for future work is to characterize the class of functions which a protocol can securely compute without any additional card. This paper implies that the conjunction function of any number of variables is in this class. As another example, it is easily verified that any two-variable function can be securely computed with no additional card. More exact characterizations should be obtained.

Acknowledgments

We thank the anonymous referees whose comments helped us to improve the presentation of the paper. This work was supported by JSPS KAKENHI Grant Number 26330001.

References

[1] B. den Boer, "More efficient match-making and satisfiability: the five card trick," Proc. EUROCRYPT '89, Lecture Notes in Computer Science, vol. 434, pp. 208–217, Springer-Verlag, 1990.

[2] C. Crépeau and J. Kilian, "Discreet solitary games," Proc. CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 319–330, Springer-Verlag, 1994.

[3] T. Mizuki and H. Shizuya, "A formalization of card-based cryptographic protocols via abstract machine," International Journal of Information Security, vol. 13, no. 1, pp. 15–23, 2014.

[4] T. Mizuki and H. Sone, "Six-card secure AND and four-card secure XOR," Proc. Frontiers in Algorithmics (FAW 2009), Lecture Notes in Computer Science, vol. 5598, pp. 358–369, Springer-Verlag, 2009.

[5] T. Mizuki, M. Kumamoto, and H. Sone, "The five-card trick can be done with four cards," Proc. ASIACRYPT 2012, Lecture Notes in Computer Science, Springer-Verlag, vol. 7658, pp. 598–606, 2012.

[6] T. Mizuki and H. Shizuya, "Practical card-based cryptography," Proc. Fun with Algorithms (FUN 2014), Lecture Notes in Computer Science, vol. 8496, pp. 318–329, Springer-Verlag, 2014.

[7] V. Niemi and A. Renvall, "Secure multiparty computations without computers," Theoretical Computer Science, vol. 191, pp. 173–183, 1998.

[8] V. Niemi and A. Renvall, "Solitaire zero-knowledge," Fundamenta Informaticae, vol. 38, pp. 181–188, 1999.

[9] T. Nishida, T. Mizuki, and H. Sone, "Securely computing the three-input majority function with eight cards," Proc. Theory and Practice of Natural Computing (TPNC 2013), Lecture Notes in Computer Science, Springer-Verlag, vol. 8273, pp. 193-204, 2013.

[10] A. Stiglic, "Computations with a deck of cards," Theoretical Computer Science, vol. 259, pp. 671–678, 2001.