



# Card-based protocols for securely computing the conjunction of multiple variables



Takaaki Mizuki

Cyberscience Center, Tohoku University, Aramaki-Aza-Aoba 6–3, Aoba-ku, Sendai 980-8578, Japan

## ARTICLE INFO

### Article history:

Received 29 August 2014  
 Received in revised form 19 October 2015  
 Accepted 28 January 2016  
 Available online 2 February 2016  
 Communicated by G. Persiano

### Keywords:





Card-based protocols  
 Card games  
 Cryptography without computers  
 Real-life hands-on cryptography  
 Secure multiparty computations

## 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.

© 2016 Elsevier B.V. All rights reserved.

## 1. Introduction

Consider a deck of real physical cards with faces that are either black () or red () and backs () 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  in accordance with the following encoding:

$$\begin{matrix} \blacksquare & \heartsuit \\ \heartsuit & \blacksquare \end{matrix} = 0, \quad \begin{matrix} \heartsuit & \blacksquare \\ \blacksquare & \heartsuit \end{matrix} = 1. \tag{1}$$

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

$$\underbrace{\begin{matrix} \square & \square \\ \square & \square \end{matrix}}_x.$$

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 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  $x_1 \wedge x_2 \wedge \dots \wedge x_n$  for given commitments

$$\underbrace{\begin{matrix} \square & \square \\ \square & \square \end{matrix}}_{x_1} \quad \underbrace{\begin{matrix} \square & \square \\ \square & \square \end{matrix}}_{x_2} \quad \dots \quad \underbrace{\begin{matrix} \square & \square \\ \square & \square \end{matrix}}_{x_n}$$

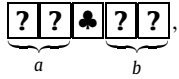
to  $n$  bits  $x_1, x_2, \dots, x_n \in \{0, 1\}$ .

E-mail address: [tm-paper+cardconj@g-mail.tohoku-university.jp](mailto:tm-paper+cardconj@g-mail.tohoku-university.jp).

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

1.1. The history

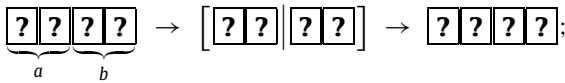
The first card-based protocol, the “five-card trick,” invented in 1989 by den Boer [1] securely computes the conjunction (that is, the AND function) of two secret bits. Specifically, given commitments to bits  $a, b \in \{0, 1\}$  together with one additional black card



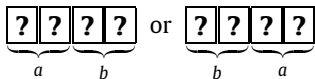
the five-card trick allows us to learn only the value of  $a \wedge b$  (without revealing more of the values  $a$  and  $b$  themselves than necessary). Thus, it uses five cards in total.

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:

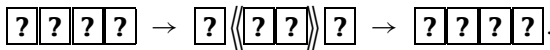


it means that the resulting deck is either



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

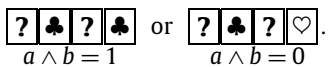
2. Shuffle the two cards in the middle:



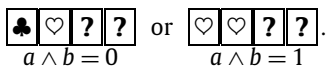
(That is, the middle two cards are switched with probability of exactly 1/2.)

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 , then we reveal the first card, and have either



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



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  $\bar{x}$ :

Download English Version:

<https://daneshyari.com/en/article/6875957>

Download Persian Version:

<https://daneshyari.com/article/6875957>

[Daneshyari.com](https://daneshyari.com)