Secure Computations Through Checking Suits of Playing Cards

Daiki Miyahara[1,2](✉) and Takaaki Mizuki[2,3]

[1] The University of Electro-Communications, Tokyo, Japan
miyahara@uec.ac.jp
[2] National Institute of Advanced Industrial Science and Technology, Tokyo, Japan
[3] Tohoku University, Sendai, Japan

Abstract. Card-based cryptography started with the "five-card trick" designed by Den Boer (EUROCRYPT 1989); it enables Alice and Bob to securely evaluate the AND value of their private bits using a physical deck of five cards. It was then shown that the same task can be done with only four cards, i.e., Mizuki et al. proposed a four-card AND protocol (ASIACRYPT 2012). These two AND protocols are simple and easy even for non-experts, such as high school students, to execute. Their only common drawback is the need to prepare a customized deck consisting of red and black cards such that all cards of the same color must be identical. Fortunately, several existing protocols are based on a standard deck of playing cards (commercially available). Among them, the state-of-the-art AND protocol was constructed by Koch et al. (ASIACRYPT 2019); it uses four playing cards (such as 'A, J, Q, K') to securely evaluate the AND value. The protocol is elaborate, while its possible drawback is the need to repeat a shuffling operation six times (in expectation), which makes it less practical.

This paper aims to provide the first practical protocol working on a standard deck of playing cards. We present an extremely simple AND protocol that terminates after only one shuffle using only four cards; our proposed protocol relies on a new operation, called the "half-open" action, whereby players can check only the suit of a face-down card without revealing the number on it. We believe that this new operation is easy-to-implement, and hence, our four-card AND protocol working on a standard deck is practical. We formalize the half-open action to present a formal description of our proposed protocol. Moreover, we discuss what is theoretically implied by introducing the half-open action and show that it can be applied to efficiently solving Yao's Millionaires' problem with a standard deck of cards.

Keywords: Card-based cryptography · Secure computation · Real-life hands-on cryptography

1 Introduction

Card-based cryptography enables people including non-specialists to easily conduct cryptographic tasks, such as secure multiparty computations and

M. Li and X. Sun (Eds.): IJTCS-FAW 2022, LNCS 13461, pp. 110–128, 2022.
https://doi.org/10.1007/978-3-031-20796-9_9

zero-knowledge proofs, in daily activities using a deck of physical cards. Typically, we use a *two-colored deck* of cards, i.e., a deck consisting of black $\boxed{\clubsuit}$ and red cards $\boxed{\heartsuit}$ whose backs are all identical $\boxed{?}$. In history, the first card-based protocol called the *five-card trick* was presented by Den Boer [2] at EUROCRYPT 1989; it enables Alice and Bob holding private bits $a \in \{0,1\}$ and $b \in \{0,1\}$, respectively, to securely evaluate the AND value $a \wedge b$ using five cards $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, as described below.

1.1 The Five-Card Trick

Assume that, based on a pair of cards of different colors, Alice and Bob agree upon the following encoding rule:

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

If two face-down cards $\boxed{?}\boxed{?}$ represent a bit $x \in \{0,1\}$ according to the above encoding (1), then we call them a *commitment* to x and denote it by

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

The five-card trick [2] proceeds as follows.

1. Alice and Bob privately create commitments to $\overline{a}$ and b, respectively, and between them, place one helping red card $\boxed{\heartsuit}$; then, turn it face down:
$$\underbrace{\boxed{?}\boxed{?}}_{\overline{a}}\,\boxed{\heartsuit}\,\underbrace{\boxed{?}\boxed{?}}_{b} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{\overline{a}}\,\boxed{?}\,\underbrace{\boxed{?}\boxed{?}}_{b}.$$
Note that the three cards in the middle would be $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ if and only if $a = b = 1$.
2. Apply a *random cut*, denoted by $\langle \cdot \rangle$, to the sequence of five cards:
$$\underbrace{\boxed{?}\boxed{?}}_{\overline{a}}\,\boxed{?}\,\underbrace{\boxed{?}\boxed{?}}_{b} \rightarrow \left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$
A random cut is a cyclic shuffling operation such that the resulting sequence is randomly shifted. Note that a secure implementation of a random cut called the Hindu cut has been known [49].
3. Reveal all the five cards; then, we learn the value of $a \wedge b$, which depends on whether or not the three red cards $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ are consecutive (apart from cyclic rotation):
$$\begin{array}{c} \boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit} \\ \boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit} \\ \boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit} \\ \boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit} \\ \boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit} \\ a \wedge b = 0 \end{array} \quad \text{or} \quad \begin{array}{c} \boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit} \\ \boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit} \\ \boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit} \\ \boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit} \\ \boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit} \\ a \wedge b = 1. \end{array}$$
Thus, the five-card trick can elegantly evaluate the AND value securely.

1.2 Protocols with a Standard Deck of Cards

After twenty-three years since the invention of the five-card trick, it was reported at ASIACRYPT 2012 that the same task can be conducted without any helping card [30]. These two AND protocols [2,30] are simple and easy even for non-experts, such as high school students, to understand. Actually, both the protocols are practical and used for introducing the notion of secure computations in university classes [21,39]. On the other hand, their only common drawback is the need to prepare a customized deck consisting of red and black cards ($\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\cdots$) such that all cards of the same color must be indistinguishable.

Fortunately, there are several existing protocols that work on a *standard deck* of playing cards (which is commercially available), such as:

$$\boxed{\mathrm{A}\clubsuit}\boxed{\mathrm{A}\spadesuit}\boxed{\mathrm{A}\heartsuit}\boxed{\mathrm{A}\diamondsuit}\boxed{2\clubsuit}\boxed{2\spadesuit}\boxed{2\heartsuit}\boxed{2\diamondsuit}\cdots\boxed{\mathrm{K}\clubsuit}\boxed{\mathrm{K}\spadesuit}\boxed{\mathrm{K}\heartsuit}\boxed{\mathrm{K}\diamondsuit}.$$

Table 1 enumerates the existing AND protocols working on a standard deck. In these protocols, a standard deck is regarded as a total order on $\{1, 2, \ldots, 52\}$ (because of 13 numbers × 4 suits): that is, a protocol is supposed to work on cards like $\boxed{1}\boxed{2}\boxed{3}\boxed{4}\cdots$ whose backs are all $\boxed{?}$. In this standard deck setting, a Boolean value can be also represented by a pair of cards: a bit $x \in \{0, 1\}$ is encoded with the order of two cards $\boxed{i}$ and $\boxed{j}$, $1 \le i < j \le 52$, according to

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

Therefore, such two face-down cards serve a *commitment* to $x \in \{0, 1\}$, which is denoted by

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

where the set $\{i, j\}$ is called its *base*.

Among the existing AND protocols (shown in Table 1), the state-of-the-art one was presented by Koch et al. at ASIACRYPT 2019 [10]; it is a card-minimal AND protocol, i.e., it uses only four cards (such as $\boxed{1}\boxed{2}\boxed{3}\boxed{4}$). Given two input commitments to $a, b \in \{0, 1\}$, the protocol produces a commitment to $a \wedge b$ after applying a random cut six times in expectation:

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{1,2\}}}\underbrace{\boxed{?}\boxed{?}}_{[b]^{\{3,4\}}} \quad\rightarrow\quad \text{Random cut 6 times (exp.)} \quad\rightarrow\quad \underbrace{\boxed{?}\boxed{?}}_{[a\wedge b]^{B}},$$

where the base B will be one of $\{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 4\}, \{3, 4\}$.

The description of this protocol [10] will be presented in Sect. 2. Although the protocol is elaborate as will be seen, its possible drawback is the need to repeat a random cut six times (in expectation), which makes it less practical.

Table 1. The existing AND protocols with a standard deck

	# of cards	# of shuffles	not Las Vegas?
Niemi and Renvall [37]	5	9.5 (exp.)	
Mizuki [26]	8	4	✓
Koch and Schrempp and Kirsten [10,11]	4	6 (exp.)	

1.3 Contribution

As mentioned above and implied by Table 1, the existing AND protocols working on a standard deck are somewhat impractical due to their numbers of required shuffles and/or cards. Thus, our aim is to provide the first practical AND protocol working on a standard deck of playing cards.

In this study, we present an extremely simple AND protocol that terminates after only *one* random cut using only *four* cards. The key idea behind our construction is to make use of the simple fact that every card in a standard deck has a suit in addition to its number. In other words, we do not regard a standard deck just as a total order, but we directly utilize the suits (♣, ♠, ♥, ♦) to perform an efficient secure AND computation. More precisely, our AND protocol works on a deck of four cards

$$\boxed{3\clubsuit}\boxed{3\heartsuit}\boxed{9\clubsuit}\boxed{9\heartsuit},$$

whose suits (♣ or ♥) will play an important role. Our four-card AND protocol relies on a new operation, called the *half-open* action, whereby players are able to check only the suit of a face-down card without revealing the number on it. Thus, briefly, given two input commitments to $a, b \in \{0,1\}$, our protocol securely evaluates the value of $a \wedge b$ by using one random cut and the half-open action:

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{a\}}}\underbrace{\boxed{?}\boxed{?}}_{[b]^{\{b\}}} \rightarrow \text{Random cut once + Half-open}$$

$$\rightarrow \begin{cases} a \wedge b = 1 & \text{if } \boxed{3\clubsuit}\boxed{\clubsuit},\ \boxed{9\clubsuit}\boxed{\clubsuit},\ \boxed{3\heartsuit}\boxed{\heartsuit}, \text{ or } \boxed{9\heartsuit}\boxed{\heartsuit} \text{ appears,} \\ a \wedge b = 0 & \text{otherwise.} \end{cases}$$

We present the details of our protocol in Sect. 4. As will be seen in Sect. 3, our new operation, the "half-open" action, is easy-to-implement, and hence, we believe that our four-card AND protocol working on a standard deck is practical.

In Sect. 5, we construct, by extending the computational model of card-based protocols, which has been developed in [8,13,31,32,48], a formal computation model that admits the operation mentioned above, i.e., the half-open action. Based on this model, we present a formal description of our proposed protocol in Sect. 6.

Moreover, we discuss what is theoretically implied by introducing the half-open action and show that it can be applied to efficiently solving Yao's Millionaires' problem [50] with a standard deck of cards in Sect. 7. Somewhat surprisingly, our solution requires only one more half-open action compared to the existing solutions [23] that work on a two-colored deck of cards.

2 The Existing Card-Minimal AND Protocol

In this section, we introduce the existing card-minimal AND protocol constructed by Koch et al. [10,11] using four cards $\boxed{1}\boxed{2}\boxed{3}\boxed{4}$.

1. Given input commitments to $a, b \in \{0, 1\}$, apply a random cut:

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{1,2\}}}\ \underbrace{\boxed{?}\boxed{?}}_{[b]^{\{3,4\}}} \rightarrow \left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

2. Turn over the first card; assume that the revealed card is $\boxed{1}$ (the other cases are similar). Then, turn it face down:

$$\boxed{1}\boxed{?}\boxed{?}\boxed{?} \quad\rightarrow\quad \boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

   (a) Swap the third and fourth cards.

$$\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}} \quad\rightarrow\quad \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{4}{\boxed{?}}\overset{3}{\boxed{?}}\ .$$

   (b) Apply a random cut:

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

   (c) Turn over the first card. If $\boxed{3}$ appears, proceed to Step 3; otherwise, go back to (b) after turning over the face-up card.

3. Apply a random cut to the second, third, and fourth cards:

$$\boxed{3}\left\langle \boxed{?}\boxed{?}\boxed{?} \right\rangle \quad\rightarrow\quad \boxed{3}\boxed{?}\boxed{?}\boxed{?}.$$

4. Reveal the second card.
   (a) If either $\boxed{1}$ or $\boxed{4}$ is revealed, then we obtain a commitment to $a \wedge b$:

$$\boxed{3}\boxed{1}\ \underbrace{\boxed{?}\boxed{?}}_{[a\wedge b]^{\{2,4\}}} \qquad \text{or} \qquad \boxed{3}\boxed{4}\ \underbrace{\boxed{?}\boxed{?}}_{[a\wedge b]^{\{1,2\}}}\ .$$

   (b) If $\boxed{2}$ is revealed, we obtain a commitment to $\overline{a \wedge b}$ (which can be easily changed into a commitment to $a \wedge b$ just by swapping the two cards):

$$\boxed{3}\boxed{2}\ \underbrace{\boxed{?}\boxed{?}}_{[\overline{a\wedge b}]^{\{1,4\}}}\ .$$

Note that in Steps 2(b) and (c), the protocol searches for $\boxed{3}$ among the four cards by repeating the application of a random cut; the expected number of shuffles is four (because of the four cards). Therefore, in total, this protocol needs six random cuts (in expectation), and hence, it is a Las Vegas algorithm.

In the next sections, we aim to reduce the number of shuffles required for a secure AND computation.[1]

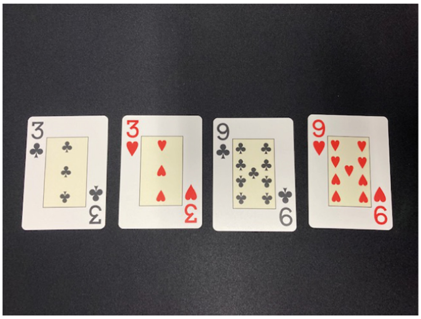


Fig. 1. Typical playing cards

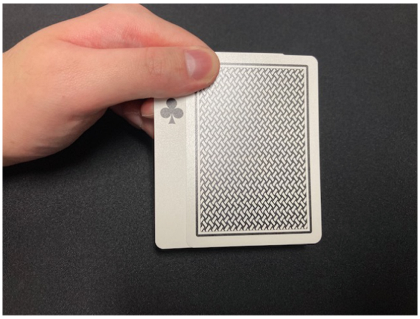


Fig. 2. Half-open with fingers

3 New Action: Half-Open of Playing Cards

In this section, we propose a novel action in card-based cryptography: the *half-open* action reveals only the suit of a given face-down card (of a standard deck) without leaking any information about its number:

$$\boxed{?} \xrightarrow{\text{half-open}} \boxed{\clubsuit} \text{ or } \boxed{\spadesuit} \text{ or } \boxed{\heartsuit} \text{ or } \boxed{\diamondsuit} .$$

We present a couple of implementations of this action.

Because implementing the half-open action depends on a physical design of cards, let us consider typical playing cards as shown in Fig. 1. Here, we mention the general policy of implementing the half-open action, which would be helpful when considering non-typical playing cards. Because the half-open action reveals only a suit, we should find a specific area on the front where a suit is "identically" placed for all cards. The half-open action can be achieved by revealing such an area while hiding the others.

Figure 2 describes a playing card such that nothing but its suit (♣) is visible. One possible way to have such a situation is as follows. Note that a typical

[1] Recently, a zero-knowledge proof protocol for Sudoku has been developed using standard decks of cards [42], and protocols based on private operations have been constructed using a standard deck [19]. In addition, efficient copy and XOR protocols [15], a card-minimal three-input AND protocol [14], and other three-input protocols [5] have been devised.

playing card has a number and suit in the upper left and lower right corners. Given a face-down card (to which apply the half-open), another (face-up) card is inserted below it, the two cards are stacked, and they are turned over. Then, slide out one card while keeping the number hidden with fingers so that only the suit becomes visible.

Because mastering this method requires some effort, we consider an easier method for the half-open action. For this, we made covers that disclose only suits of cards without leaking their numbers, as shown in Fig. 3. Here, we used an A3-size notebook and scissors to make the covers, but any sheet of paper can be used, and it is effortless to make.

Next, we show how to use the covers specifically. We put a cover under a target card (Fig. 4), lift the card and cover together (Fig. 5), and turn them over to check the suit (Fig. 6). We describe this result as $\boxed{\heartsuit}$. Thus, the half-open action can be easily implemented: it is an effortless task to create a cover, insert the cover under the card, and turn them over.

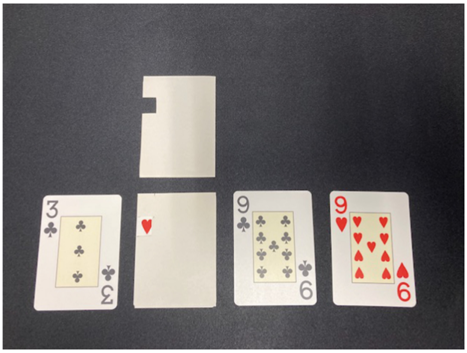


Fig. 3. The use of covers

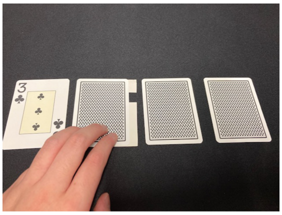


Fig. 4. Put a cover under the card

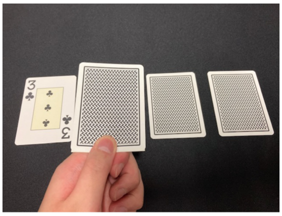


Fig. 5. Lift up the card and cover together

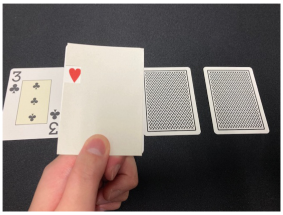


Fig. 6. Turn them over. We describe this as $\boxed{\heartsuit}$.

It should be noted that Marcedone et al. [21, Solution 4] first considered a similar idea of folding up a portion of a customized card such as a square card to obtain partial information. Shinagawa [46] used specialized cards with invisible ink to obtain partial information by illuminating a black light with a cover. Compared to their studies, our study uses a standard deck of commercially available cards, i.e., we do not need to prepare a specialized deck of cards.

4 Our Simple AND Protocol Based on Half-Open Action

In this section, we present our efficient AND protocol working on a standard deck with the help of the half-open action.

In the sequel, we use the following four playing cards:

$$\boxed{3\clubsuit}\boxed{3\heartsuit}\boxed{9\clubsuit}\boxed{9\heartsuit},$$

although any four cards can be chosen as long as two of them have the same suit and the others have another same suit.

Table 2. The principle behind our proposed protocol

(a, b)	Sequence	Right of $\boxed{3\clubsuit}$	Left of $\boxed{9\heartsuit}$	Right of $\boxed{3\heartsuit}$	Left of $\boxed{9\clubsuit}$
(0,0)	$\boxed{3\clubsuit}\boxed{9\heartsuit}\boxed{3\heartsuit}\boxed{9\clubsuit}$	$\boxed{9\heartsuit}$	$\boxed{3\clubsuit}$	$\boxed{9\clubsuit}$	$\boxed{3\heartsuit}$
(0,1)	$\boxed{3\clubsuit}\boxed{9\heartsuit}\boxed{9\clubsuit}\boxed{3\heartsuit}$	$\boxed{9\heartsuit}$	$\boxed{3\clubsuit}$	$\boxed{3\clubsuit}$	$\boxed{9\heartsuit}$
(1,0)	$\boxed{9\heartsuit}\boxed{3\clubsuit}\boxed{3\heartsuit}\boxed{9\clubsuit}$	$\boxed{3\heartsuit}$	$\boxed{9\clubsuit}$	$\boxed{9\clubsuit}$	$\boxed{3\heartsuit}$
(1,1)	$\boxed{9\heartsuit}\boxed{3\clubsuit}\boxed{9\clubsuit}\boxed{3\heartsuit}$	$\boxed{9\clubsuit}$	$\boxed{3\heartsuit}$	$\boxed{9\heartsuit}$	$\boxed{3\clubsuit}$

Alice and Bob hold their private bits $a \in \{0, 1\}$ and $b \in \{0, 1\}$, respectively. Our proposed protocol proceeds as follows.

1. Alice takes $\boxed{3\clubsuit}\boxed{9\heartsuit}$ and places a commitment to a based on the following encoding similar to (2):

$$\boxed{3\clubsuit}\boxed{9\heartsuit} = 0, \quad \boxed{9\heartsuit}\boxed{3\clubsuit} = 1.$$

   Bob takes $\boxed{3\heartsuit}\boxed{9\clubsuit}$ and places a commitment to b in the same way as Alice, i.e., by focusing only on their numbers:

$$\boxed{3\heartsuit}\boxed{9\clubsuit} = 0, \quad \boxed{9\clubsuit}\boxed{3\heartsuit} = 1.$$

   Thus, we have the following two commitments:

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{3\clubsuit,9\heartsuit\}}}\ \underbrace{\boxed{?}\boxed{?}}_{[b]^{\{3\heartsuit,9\clubsuit\}}}\ .$$

Table 2 indicates the actual sequence of cards for each input. Let us focus on $\boxed{3\clubsuit}$: observe that the suit of the card on the right of $\boxed{3\clubsuit}$ has a suit $\clubsuit$ if and only if $a = b = 1$. Therefore, they can obtain only the value of $a \wedge b$ by checking the suit.

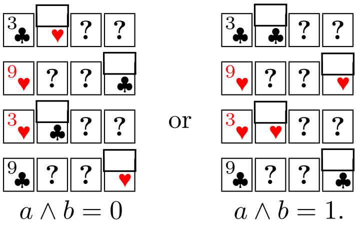
In the same way, the suits of the cards on the right of $\boxed{3\heartsuit}$ and on the left of $\boxed{9\clubsuit}$ and $\boxed{9\heartsuit}$ determine the value of $a \wedge b$. See the third to sixth columns of Table 2. Our protocol uses this relationship to perform a secure computation of the logical AND function.

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

$$\underbrace{\boxed{?}\boxed{?}}_{[a]^{\{3\clubsuit,9\heartsuit\}}}\quad \underbrace{\boxed{?}\boxed{?}}_{[b]^{\{3\heartsuit,9\clubsuit\}}} \quad\rightarrow\quad \left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \quad\rightarrow\quad \boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

Note that the relationship shown in Table 2 remains unchanged (despite the random cut).

3. Reveal the first card. Note that the revealed card should be one of $\boxed{3\clubsuit}$, $\boxed{3\heartsuit}$, $\boxed{9\clubsuit}$, $\boxed{9\heartsuit}$ with the equal probability (i.e., 1/4), and hence, information about the input is never leaked.
4. If the revealed card is either $\boxed{3\clubsuit}$ or $\boxed{3\heartsuit}$, then apply the half-open action to its right card, namely the second card (because a '3' is placed on the right side of a clock or wristwatch). If it is either $\boxed{9\clubsuit}$ or $\boxed{9\heartsuit}$, then apply the half-open action to its left card, namely the fourth card (because a '9' is placed on the left side of a wristwatch). Alice and Bob obtain the value of $a \wedge b$ as follows:



This is our four-card AND protocol, which uses only one random cut and one half-open action. Although we believe that the correctness and security of our protocol are clear from the above description, we present their formal proofs in Sect. 6.2.

It should be noted that if one wants to use the first method shown in Fig. 2 to implement the half-open action in Step 4, the card revealed in Step 3 can be used as a cover (so that no additional card needs).

In the next sections, we formally define the half-open action and formally describe our protocol.

5 Formalizing Half-Open Action

In this section, we formalize a card-based protocol using a standard deck of playing cards such that the *half-open* action is allowed.

In the literature [13,31], a deck was typically represented as a multiset over a symbol set, such as $[\clubsuit, \clubsuit, \heartsuit, \heartsuit, \heartsuit]$ and $\{1, 2, 3, 4\}$. Remember that our protocol proposed in Sect. 4 employs the fact that every card in a standard deck has a suit and its number. Therefore, we call a pair of a number and a suit, such as $(1, \clubsuit)$, $(1, \spadesuit)$, $(2, \heartsuit)$, and $(2, \diamondsuit)$, an *atomic card*. Following this, we denote a *standard deck* $\mathcal{D}$ by a multiset of atomic cards[2]. For an atomic card $c = (i, s)$, we denote its suit symbol by $\mathbf{ss}(c) := s$. For example, $\mathbf{ss}(1, \clubsuit) = \clubsuit$ and $\mathbf{ss}(2, \diamondsuit) = \diamondsuit$.

5.1 Notations

For a deck $\mathcal{D}$, a *face-up* card and a *face-down* card are represented as $\frac{c}{?}$ and $\frac{?}{c}$ for $c \in \mathcal{D}$, respectively. In addition, a face-down card to which the half-open action was applied is represented as $\frac{\mathbf{ss}(c)}{c}$. Given such a face-up, face-down, or "half-open" card, we denote its atomic card by $\mathsf{atom}(\frac{c}{?}) = \mathsf{atom}(\frac{?}{c}) = \mathsf{atom}(\frac{\mathbf{ss}(c)}{c}) = c$, and denote its visible symbol by $\mathsf{top}(\frac{c}{?}) = c$, $\mathsf{top}(\frac{?}{c}) = ?$, and $\mathsf{top}(\frac{\mathbf{ss}(c)}{c}) = \mathbf{ss}(c)$, respectively. We say that a d-tuple $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ consisting of d cards from a standard deck $\mathcal{D}$ is a *sequence* if $[\mathsf{atom}(\alpha_1), \mathsf{atom}(\alpha_2), \ldots, \mathsf{atom}(\alpha_d)] = \mathcal{D}$.

We denote the set of all (possible) sequences from a standard deck $\mathcal{D}$ by

$$\mathsf{Seq}^{\mathcal{D}} := \{\Gamma \mid \Gamma \text{ is a sequence of } \mathcal{D}\}.$$

We extend the use of $\mathsf{top}(\cdot)$ to a sequence: given a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$, we write $\mathsf{top}(\Gamma) = (\mathsf{top}(\alpha_1), \mathsf{top}(\alpha_2), \ldots, \mathsf{top}(\alpha_d))$, and we call it the *visible sequence* of Γ. We also define the *visible sequence set* $\mathsf{Vis}^{\mathcal{D}}$ as

$$\mathsf{Vis}^{\mathcal{D}} := \{\mathsf{top}(\Gamma) \mid \Gamma \in \mathsf{Seq}^{\mathcal{D}}\}.$$

5.2 Protocols

We present a formal description of a protocol. As seen below, starting from an initial sequence, a protocol specifies an action to be applied to a current sequence step by step, depending on its internal state and the visible sequence.

A *protocol* (having a *finite state control* and a *table* on which a single sequence is put) is formally specified with a quadruple $\mathcal{P} = (\mathcal{D}, U, Q, A)$:

- $\mathcal{D}$ is a deck;
- $U \subseteq \mathsf{Seq}^{\mathcal{D}}$ is an *input set*;
- Q is a *state set* having an initial state $q_0 \in Q$ and a final state $q_{\mathrm{f}} \in Q$;
- $A : (Q \backslash \{q_{\mathrm{f}}\}) \times \mathsf{Vis}^{\mathcal{D}} \to Q \times \mathsf{Action}$ is an *action function*, where Action is the set of the following actions:
  - (turn, T) for $T \subseteq \{1, 2, \ldots, |\mathcal{D}|\}$;
  - (perm, π) for $\pi \in S_{|\mathcal{D}|}$, where S_i denotes the symmetric group of degree i;
  - $(\mathsf{shuf}, \Pi, \mathcal{F})$ for $\Pi \subseteq S_{|\mathcal{D}|}$ and a probability distribution $\mathcal{F}$ on Π. If $\mathcal{F}$ is uniform, we omit it and write this action as (shuf, Π);

[2] It should be noted that $\mathcal{D}$ can be any set of cards taken from 52 playing cards.

- (hopen, T) for $T \subseteq \{1, 2, \ldots, |\mathcal{D}|\}$;
- (hclose, T) for $T \subseteq \{1, 2, \ldots, |\mathcal{D}|\}$;

Given a current sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_{|\mathcal{D}|})$, each action in Action transforms the current sequence Γ into the next sequence Γ' as follows.

– (turn, T): $\Gamma' = (\beta_1, \beta_2, \ldots, \beta_{|\mathcal{D}|})$ such that

$$\beta_i = \begin{cases} \mathsf{swap}(\alpha_i) & \text{if } i \in T, \\ \alpha_i & \text{otherwise,} \end{cases}$$

for every i, $1 \leq i \leq |\mathcal{D}|$, where $\mathsf{swap}(\frac{c}{?}) = \frac{?}{c}$ and $\mathsf{swap}(\frac{?}{c}) = \frac{c}{?}$ for an atomic card c;

– (perm, π): $\Gamma' = (\alpha_{\pi^{-1}(1)}, \alpha_{\pi^{-1}(2)}, \ldots, \alpha_{\pi^{-1}(|\mathcal{D}|)})$;

– $(\mathsf{shuf}, \Pi, \mathcal{F})$: Γ' resulting from applying action (perm, π) to Γ, where π is a permutation drawn from Π according to the probability distribution $\mathcal{F}$;

– (hopen, T): $\Gamma' = (\beta_1, \beta_2, \ldots, \beta_{|\mathcal{D}|})$ such that for every i, $1 \leq i \leq |\mathcal{D}|$,

$$\beta_i = \begin{cases} \frac{\mathbf{ss}(c_i)}{c_i} & \text{if } i \in T, \\ \alpha_i & \text{otherwise,} \end{cases}$$

where α_j for every $j \in T$ must be a face-down card $\alpha_j = \frac{?}{c_j}$.

– (hclose, T): $\Gamma' = (\beta_1, \beta_2, \ldots, \beta_{|\mathcal{D}|})$ such that for every i, $1 \leq i \leq |\mathcal{D}|$,

$$\beta_i = \begin{cases} \frac{?}{c_i} & \text{if } i \in T, \\ \alpha_i & \text{otherwise,} \end{cases}$$

where α_j for every $j \in T$ must be a "half-open" card $\alpha_j = \frac{\mathbf{ss}(c_j)}{c_j}$ (to which hopen has been applied).

6 Formal Description of Our Protocol

In this section, we show a formal description of our proposed AND protocol based on the computational model formalized in Sect. 5.

6.1 Pseudocode

The following is a pseudocode of our protocol, where we define $\mathsf{RC}_{1,2,3,4} = \{(1\,2\,3\,4)^i \mid 1 \leq i \leq 4\}$. Its deck is $[(3, \clubsuit), (3, \heartsuit), (9, \clubsuit), (9, \heartsuit)]$.

input set:

$$\left\{\left(\frac{?}{(3,\clubsuit)}, \frac{?}{(9,\heartsuit)}, \frac{?}{(9,\clubsuit)}, \frac{?}{(3,\heartsuit)}\right), \left(\frac{?}{(3,\clubsuit)}, \frac{?}{(9,\heartsuit)}, \frac{?}{(3,\heartsuit)}, \frac{?}{(9,\clubsuit)}\right),\right.$$
$$\left.\left(\frac{?}{(9,\heartsuit)}, \frac{?}{(3,\clubsuit)}, \frac{?}{(9,\clubsuit)}, \frac{?}{(3,\heartsuit)}\right), \left(\frac{?}{(9,\heartsuit)}, \frac{?}{(3,\clubsuit)}, \frac{?}{(3,\heartsuit)}, \frac{?}{(9,\clubsuit)}\right)\right\}$$

```
(shuf, RC$_{1,2,3,4}$)
(turn, $\{1\}$)
if visible seq. $= ((3,♣),?,?,?)$ or $((3,♥),?,?,?)$ then
  (hopen, $\{2\}$)
  if visible seq. $= ((3,♣),♣,?,?)$ or $((3,♥),♥,?,?)$ then $a \wedge b = 1$
  else $a \wedge b = 0$
if visible seq. $= ((9,♣),?,?,?)$ or $((9,♥),?,?,?)$ then
  (hopen, $\{4\}$)
  if visible seq. $= ((9,♣),?,?,♣)$ or $((9,♥),?,?,♥)$ then $a \wedge b = 1$
  else $a \wedge b = 0$
```

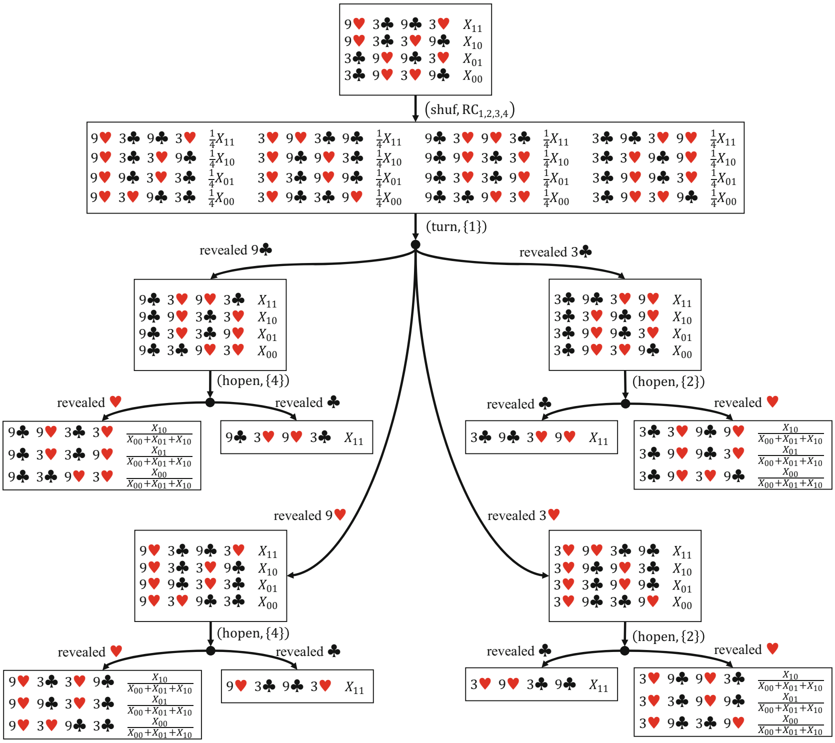

9♥ 3♣ 9♣ 3♥ X_{11}
9♥ 3♣ 3♥ 9♣ X_{10}
3♣ 9♥ 9♣ 3♥ X_{01}
3♣ 9♥ 3♥ 9♣ X_{00}
(shuf, RC$_{1,2,3,4}$)
9♥ 3♣ 9♣ 3♥ $\frac{1}{4}X_{11}$ 3♥ 9♥ 3♣ 9♣ $\frac{1}{4}X_{11}$ 9♣ 3♥ 9♥ 3♣ $\frac{1}{4}X_{11}$ 3♣ 9♣ 3♥ 9♥ $\frac{1}{4}X_{11}$
9♥ 3♣ 3♥ 9♣ $\frac{1}{4}X_{10}$ 3♥ 9♣ 9♥ 3♣ $\frac{1}{4}X_{10}$ 9♣ 9♥ 3♣ 3♥ $\frac{1}{4}X_{10}$ 3♣ 3♥ 9♣ 9♥ $\frac{1}{4}X_{10}$
9♥ 9♣ 3♥ 3♣ $\frac{1}{4}X_{01}$ 3♥ 3♣ 9♥ 9♣ $\frac{1}{4}X_{01}$ 9♣ 3♥ 3♣ 9♥ $\frac{1}{4}X_{01}$ 3♣ 9♥ 9♣ 3♥ $\frac{1}{4}X_{01}$
9♥ 3♥ 9♣ 3♣ $\frac{1}{4}X_{00}$ 3♥ 9♣ 3♣ 9♥ $\frac{1}{4}X_{00}$ 9♣ 3♣ 9♥ 3♥ $\frac{1}{4}X_{00}$ 3♣ 9♥ 3♥ 9♣ $\frac{1}{4}X_{00}$
(turn, {1})
revealed 9♣
revealed 3♣
9♣ 3♥ 9♥ 3♣ X_{11}
9♣ 9♥ 3♣ 3♥ X_{10}
9♣ 3♥ 3♣ 9♥ X_{01}
9♣ 3♣ 9♥ 3♥ X_{00}
3♣ 9♣ 3♥ 9♥ X_{11}
3♣ 3♥ 9♣ 9♥ X_{10}
3♣ 9♥ 9♣ 3♥ X_{01}
3♣ 9♥ 3♥ 9♣ X_{00}
(hopen, {4})
(hopen, {2})
revealed ♥
revealed ♣
revealed ♣
revealed ♥
9♣ 9♥ 3♣ 3♥ $\frac{X_{10}}{X_{00}+X_{01}+X_{10}}$
9♣ 3♥ 3♣ 9♥ $\frac{X_{01}}{X_{00}+X_{01}+X_{10}}$
9♣ 3♣ 9♥ 3♥ $\frac{X_{00}}{X_{00}+X_{01}+X_{10}}$
9♣ 3♥ 9♥ 3♣ X_{11}
3♣ 9♣ 3♥ 9♥ X_{11}
3♣ 3♥ 9♣ 9♥ $\frac{X_{10}}{X_{00}+X_{01}+X_{10}}$
3♣ 9♥ 9♣ 3♥ $\frac{X_{01}}{X_{00}+X_{01}+X_{10}}$
3♣ 9♥ 3♥ 9♣ $\frac{X_{00}}{X_{00}+X_{01}+X_{10}}$
revealed 9♥
revealed 3♥
9♥ 3♣ 9♣ 3♥ X_{11}
9♥ 3♣ 3♥ 9♣ X_{10}
9♥ 9♣ 3♥ 3♣ X_{01}
9♥ 3♥ 9♣ 3♣ X_{00}
3♥ 9♥ 3♣ 9♣ X_{11}
3♥ 9♣ 9♥ 3♣ X_{10}
3♥ 3♣ 9♥ 9♣ X_{01}
3♥ 9♣ 3♣ 9♥ X_{00}
(hopen, {4})
(hopen, {2})
revealed ♥
revealed ♣
revealed ♣
revealed ♥
9♥ 3♣ 3♥ 9♣ $\frac{X_{10}}{X_{00}+X_{01}+X_{10}}$
9♥ 9♣ 3♥ 3♣ $\frac{X_{01}}{X_{00}+X_{01}+X_{10}}$
9♥ 3♥ 9♣ 3♣ $\frac{X_{00}}{X_{00}+X_{01}+X_{10}}$
9♥ 3♣ 9♣ 3♥ X_{11}
3♥ 9♥ 3♣ 9♣ X_{11}
3♥ 9♣ 9♥ 3♣ $\frac{X_{10}}{X_{00}+X_{01}+X_{10}}$
3♥ 3♣ 9♥ 9♣ $\frac{X_{01}}{X_{00}+X_{01}+X_{10}}$
3♥ 9♣ 3♣ 9♥ $\frac{X_{00}}{X_{00}+X_{01}+X_{10}}$

Fig. 7. The KWH-tree for the proposed AND protocol. Here, (hopen, $\{i\}$) indicates that only the suit of the i-th card is to be disclosed.

6.2 Correctness and Security

We depict the *KWH-tree* [9,13,48] of our protocol in Fig. 7, by which we can confirm that the correctness and security of the protocol are satisfied.

The KWH-tree is a tree-like diagram that shows the transitions of possible sequences of cards along with their respective polynomials (or monomials) in a box, where actions to be applied to the sequence are appended to an edge. In the figure, the probability of $(a, b) = (x, y)$ is denoted by X_{xy}. A polynomial annotating a sequence in a box such as $1/4X_{00}$ represents the conditional probability that the current sequence is the one next to the polynomial, given what can be observed so far on the table. Because the sum of all polynomials in each box (except for the bottom-most boxes) is equal to

$$\sum_{x,y\in\{0,1\}} X_{xy},$$

it is guaranteed that no information about the input is leaked.

7 Discussion

In this section, we discuss the relationship between our proposed protocol using the half-open action and an existing protocol working on a two-colored deck of cards, indicating the strongness of the half-open action. We consider the four-card AND protocol [30] as a comparison because the number of required cards is the same. Moreover, we discuss the theoretical aspects of the half-open action and show that it can be applied to efficiently solving Yao's Millionaires' problem [50].

7.1 Comparison

The four-card AND protocol invented by Mizuki et al. [30] computes the logical AND using four cards:

$$\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit} \rightarrow a \wedge b.$$

Their protocol is card-minimal, although the number of required shuffles is two (one random cut and one random bisection cut), and its principle is more difficult to understand than the five-card trick [2].

As mentioned in Sect. 1.2, the efficiency of card-based protocols working on a standard deck [10, 26, 37] was less than those working on a two-colored deck in terms of the number of required shuffles. However, the number of required shuffles in our proposed protocol presented in Sect. 4 is one, and hence, it is more efficient than the existing AND protocol working on a two-colored deck [30] (except for the need of the half-open action), which is the first result of card-based cryptography history. This implies that the half-open action is useful, and we could obtain similar results for other protocols.

7.2 Theoretical Aspects

If we replace the turning-over action with the half-open action, we can regard a playing card with a card having only a suit because only a suit is always revealed on the front of the playing card. For example, face-down $\boxed{\clubsuit}$ and $\boxed{{}^{\text{A}}\clubsuit}$ can be regarded as identical as follows:

$$\boxed{?} \xrightarrow{\text{Turn}} \boxed{\clubsuit} = \boxed{?} \xrightarrow{\text{Half-open}} \boxed{\clubsuit}.$$

That is, we can regard a standard deck as a four-colored deck, and hence, any i-card protocol working on two-colored deck can be implemented using a standard deck for $i \leq 26$. For example, to implement the five-card trick [2] introduced in Sect. 1.1, it suffices to use the half-open action thrice (instead of using the turning-over action). In summary, the half-open action solves the need for a customized deck to implement the existing protocols using red and black cards.

A more striking example is to solve Yao's Millionaire' problem [50]. The problem determines whether $a < b$ or not without revealing any information more than necessary for $a, b \in \{1, 2, \ldots, m\}$ and some natural number $m \geq 2$. Miyahara et al. [23] in 2020 proposed a card-based millionaire protocol working on a standard deck, although its efficiency is less than the one working on a two-colored deck. We show that it can be improved almost as efficiently as working on a two-colored deck in the next subsection.

7.3 Millionaire Protocol Using Half-Open

Our millionaire protocol requires only one more half-open action compared to the existing solution [23] working on a two-colored deck of cards. Our protocol proceeds as follows.

1. Alice holds m club cards and $m-1$ heart cards. She places a sequence of $m+1$ face-down cards in which the cards from the first to a-th are clubs and the remaining cards are hearts:[3]

   $$\begin{array}{cccccccccc} 1 & 2 & & a & a{+}1 & a{+}2 & & m & m{+}1 & \\ \boxed{?} & \boxed{?} & \cdots & \boxed{?} & \boxed{?} & \boxed{?} & \cdots & \boxed{?} & \boxed{?} & . \\ \clubsuit & \clubsuit & & \clubsuit & \heartsuit & \heartsuit & & \heartsuit & \heartsuit & \end{array}$$

   Bob holds m spade cards and one diamond card. He places a sequence of $m+1$ face-down cards below Alice's sequence, in which the b-th card is a diamond and the remaining cards are spades:

   $$\begin{array}{cccccccccc} 1 & 2 & & b{-}1 & b & b{+}1 & & m & m{+}1 & \\ \boxed{?} & \boxed{?} & \cdots & \boxed{?} & \boxed{?} & \boxed{?} & \cdots & \boxed{?} & \boxed{?} & \\ \boxed{?} & \boxed{?} & \cdots & \boxed{?} & \boxed{?} & \boxed{?} & \cdots & \boxed{?} & \boxed{?} & . \\ \spadesuit & \spadesuit & & \spadesuit & \diamondsuit & \spadesuit & & \spadesuit & \spadesuit & \end{array}$$

   Observe that the suit of the card above the Bob's diamond card (i.e., the b-th card in Alice's sequence) determines only whether $a < b$ or not, i.e., the suit is a heart if $a < b$, and the suit is a club if $a \geq b$.

[3] It is sufficient for the suits to satisfy the above arrangement: the orders of the numbers (written on the cards) can be arbitrary.

2. Fix the two cards in each column to make $m+1$ piles, and then apply a random cut to the piles (denoted by $\langle \cdots | \cdots | \cdots \rangle$):

$$\left\langle \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \middle| \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \middle| \cdots \middle| \begin{matrix}\boxed{?}\\ \boxed{?}\end{matrix} \right\rangle \rightarrow \begin{matrix}\boxed{?}\,\boxed{?}\cdots\boxed{?}\\ \boxed{?}\,\boxed{?}\cdots\boxed{?}\end{matrix}.$$

   Note that Alice's and Bob's sequences are randomly shifted, but their offsets are the same.
3. Reveal all the cards in Bob's sequence. Then, one diamond card should appear. Let $r \in \{1, \ldots, m+1\}$ denote the position of the revealed diamond card. Note that information about the value of b does not leak to Alice because r is a uniformly distributed random value.
4. Apply the half-open action to the r-th card in Alice's sequence. If a heart is revealed ♥, then we have $a < b$; otherwise ♣, we have $a \geq b$.
5. If $a \geq b$, we can further determine whether equality holds or not by applying the half-open action to the $(r+1)$-st card in Alice's sequence (i.e., $(b+1)$-st card). If a heart is revealed ♥, then we have $a = b$; otherwise ♣, we have $a > b$.

This is our millionaire protocol working on a standard deck of cards using the half-open action. The numbers of required cards and shuffles are $3m+1$ and one, respectively. Remember that we use the half-open action in Step 4 of our protocol presented in Sect. 7.3. Note that if we just reveal the card in Step 4 instead of using the half-open action, information about the value of b leaks to Alice because she knows where she placed the revealed card in Step 1. We need a more complicated subprotocol if we do not use the half-open action.

The existing millionaire protocol working on a standard deck [23] employs such a complicated subprotocol. This protocol requires $4m$ cards and four shuffles. Therefore, our protocol is more efficient in terms of the numbers of cards and shuffles.

8 Conclusion

In this paper, we proposed a simple two-input AND protocol that requires only one shuffle, which is the trivial lower bound on the number of required shuffles[4]. The key is to consider a new action, called the half-open action, by which players can know only a suit of a face-down card. Surprisingly, this simple action contributes to the significant improvement on the numbers of required shuffles and cards, compared to the existing AND protocols.

Card-based cryptography has evolved steadily [27,28] as new concepts, techniques, and/or applications (such as the random bisection cut [33], permutation manipulation [1,6,7], zero-knowledge proofs for pencil puzzles [4,17,40–45], private operations [20,35,36,38], graph theoretical methods [22,25], information

[4] Single-shuffle protocols have attracted attention recently [16,47].

leakage analysis [29,48], new physical tools [18,24,34], and comparison with Turing complexity [3,12]) were found. We believe that the half-open action will open a new vista in this research field: This paper is a first step toward developing efficient protocols based on the half-open/close actions.

Acknowledgements. We thank the anonymous referees, whose comments have helped us improve the presentation of the paper. We thank Hiroto Koyama, who invented the half-open action, for his cooperation in preparing an earlier Japanese draft version of this paper. This work was supported in part by JSPS KAKENHI Grant Numbers JP21K11881 and JP18H05289.

References

1. Crépeau, C., Kilian, J.: Discreet solitary games. In: Stinson, D.R. (ed.) CRYPTO 1993. LNCS, vol. 773, pp. 319–330. Springer, Heidelberg (1994). https://doi.org/10.1007/3-540-48329-2_27
2. Boer, B.: More efficient match-making and satisfiability *The Five Card Trick*. In: Quisquater, J.-J., Vandewalle, J. (eds.) EUROCRYPT 1989. LNCS, vol. 434, pp. 208–217. Springer, Heidelberg (1990). https://doi.org/10.1007/3-540-46885-4_23
3. Dvořák, P., Koucký, M.: Barrington plays cards: the complexity of card-based protocols. In: Bläser, M., Monmege, B. (eds.) Theoretical Aspects of Computer Science. LIPIcs, vol. 187, pp. 26:1–26:17. Schloss Dagstuhl, Dagstuhl (2021). https://doi.org/10.4230/LIPIcs.STACS.2021.26
4. Gradwohl, R., Naor, M., Pinkas, B., Rothblum, G.N.: Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles. Theor. Comput. Syst. **44**(2), 245–268 (2009). https://doi.org/10.1007/s00224-008-9119-9
5. Haga, R., Hayashi, Y., Miyahara, D., Mizuki, T.: Card-minimal protocols for three-input functions with standard playing cards. In: Batina, L., Daemen, J. (eds.) AFRICACRYPT 2022. LNCS, vol. 13503, pp. 448–468. LNCS, Springer, Cham (2022). https://doi.org/10.1007/978-3-031-17433-9_19
6. Ibaraki, T., Manabe, Y.: A more efficient card-based protocol for generating a random permutation without fixed points. In: Mathematics and Computers in Sciences and in Industry (MCSI), pp. 252–257 (2016). https://doi.org/10.1109/MCSI.2016.054
7. Ishikawa, R., Chida, E., Mizuki, T.: Efficient card-based protocols for generating a hidden random permutation without fixed points. In: Calude, C.S., Dinneen, M.J. (eds.) UCNC 2015. LNCS, vol. 9252, pp. 215–226. Springer, Cham (2015). https://doi.org/10.1007/978-3-319-21819-9_16
8. Kastner, J., et al.: The minimum number of cards in practical card-based protocols. In: Takagi, T., Peyrin, T. (eds.) ASIACRYPT 2017. LNCS, vol. 10626, pp. 126–155. Springer, Cham (2017). https://doi.org/10.1007/978-3-319-70700-6_5
9. Koch, A.: Cryptographic protocols from physical assumptions. Ph.D. thesis, Karlsruhe Institute of Technology (2019). https://doi.org/10.5445/IR/1000097756
10. Koch, A., Schrempp, M., Kirsten, M.: Card-based cryptography meets formal verification. In: Galbraith, S.D., Moriai, S. (eds.) ASIACRYPT 2019. LNCS, vol. 11921, pp. 488–517. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-34578-5_18
11. Koch, A., Schrempp, M., Kirsten, M.: Card-based cryptography meets formal verification. New Gener. Comput. **39**(1), 115–158 (2021). https://doi.org/10.1007/s00354-020-00120-0

12. Koch, A., Walzer, S.: Private function evaluation with cards. New Gener. Comput. **40**, 115–147 (2022). https://doi.org/10.1007/s00354-021-00149-9
13. Koch, A., Walzer, S., Härtel, K.: Card-based cryptographic protocols using a minimal number of cards. In: Iwata, T., Cheon, J.H. (eds.) ASIACRYPT 2015. LNCS, vol. 9452, pp. 783–807. Springer, Heidelberg (2015). https://doi.org/10.1007/978-3-662-48797-6_32
14. Koyama, H., Miyahara, D., Mizuki, T., Sone, H.: A secure three-input AND protocol with a standard deck of minimal cards. In: Santhanam, R., Musatov, D. (eds.) CSR 2021. LNCS, vol. 12730, pp. 242–256. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-79416-3_14
15. Koyama, H., Toyoda, K., Miyahara, D., Mizuki, T.: New card-based copy protocols using only random cuts. In: ASIA Public-Key Cryptography Workshop, pp. 13–22. ACM, New York (2021). https://doi.org/10.1145/3457338.3458297
16. Kuzuma, T., Toyoda, K., Miyahara, D., Mizuki, T.: Card-based single-shuffle protocols for secure multiple-input AND and XOR computations. In: ASIA Public-Key Cryptography, pp. 1–8. ACM, New York (2022, to appear). https://doi.org/10.1145/3494105.3526236
17. Lafourcade, P., Miyahara, D., Mizuki, T., Robert, L., Sasaki, T., Sone, H.: How to construct physical zero-knowledge proofs for puzzles with a "single loop" condition. Theor. Comput. Sci. **888**, 41–55 (2021). https://doi.org/10.1016/j.tcs.2021.07.019
18. Lafourcade, P., Mizuki, T., Nagao, A., Shinagawa, K.: Light cryptography. In: Drevin, L., Theocharidou, M. (eds.) WISE 2019. IFIP AICT, vol. 557, pp. 89–101. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-23451-5_7
19. Manabe, Y., Ono, H.: Card-based cryptographic protocols with a standard deck of cards using private operations. In: Cerone, A., Ölveczky, P.C. (eds.) ICTAC 2021. LNCS, vol. 12819, pp. 256–274. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-85315-0_15
20. Manabe, Y., Ono, H.: Card-based cryptographic protocols with malicious players using private operations. New Gener. Comput. **40**, 67–93 (2022). https://doi.org/10.1007/s00354-021-00148-w
21. Marcedone, A., Wen, Z., Shi, E.: Secure dating with four or fewer cards. Cryptology ePrint Archive, Report 2015/1031 (2015)
22. Miyahara, D., Haneda, H., Mizuki, T.: Card-based zero-knowledge proof protocols for graph problems and their computational model. In: Huang, Q., Yu, Yu. (eds.) ProvSec 2021. LNCS, vol. 13059, pp. 136–152. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-90402-9_8
23. Miyahara, D., Hayashi, Y., Mizuki, T., Sone, H.: Practical card-based implementations of Yao's millionaire protocol. Theor. Comput. Sci. **803**, 207–221 (2020). https://doi.org/10.1016/j.tcs.2019.11.005
24. Miyahara, D., Komano, Y., Mizuki, T., Sone, H.: Cooking cryptographers: Secure multiparty computation based on balls and bags. In: Computer Security Foundations Symposium, pp. 1–16. IEEE, New York (2021). https://doi.org/10.1109/CSF51468.2021.00034
25. Miyamoto, K., Shinagawa, K.: Graph automorphism shuffles from pile-scramble shuffles. New Gener. Comput. **40**, 199–223 (2022). https://doi.org/10.1007/s00354-022-00164-4
26. Mizuki, T.: Efficient and secure multiparty computations using a standard deck of playing cards. In: Foresti, S., Persiano, G. (eds.) CANS 2016. LNCS, vol. 10052, pp. 484–499. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-48965-0_29
27. Mizuki, T.: Preface: special issue on card-based cryptography. New Gener. Comput. **39**(1), 1–2 (2021). https://doi.org/10.1007/s00354-021-00127-1

28. Mizuki, T.: Preface: special issue on card-based cryptography 2. New Gener. Comput. **40**, 47–48 (2022). https://doi.org/10.1007/s00354-022-00170-6
29. Mizuki, T., Komano, Y.: Information leakage due to operative errors in card-based protocols. Inf. Comput., 1–15 (2022). https://doi.org/10.1016/j.ic.2022.104910,in press
30. Mizuki, T., Kumamoto, M., Sone, H.: The five-card trick can be done with four cards. In: Wang, X., Sako, K. (eds.) ASIACRYPT 2012. LNCS, vol. 7658, pp. 598–606. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-34961-4_36
31. Mizuki, T., Shizuya, H.: A formalization of card-based cryptographic protocols via abstract machine. Int. J. Inf. Secur. **13**(1), 15–23 (2013). https://doi.org/10.1007/s10207-013-0219-4
32. Mizuki, T., Shizuya, H.: Computational model of card-based cryptographic protocols and its applications. IEICE Trans. Fundam. **E100.A**(1), 3–11 (2017). https://doi.org/10.1587/transfun.E100.A.3
33. Mizuki, T., Sone, H.: Six-card secure AND and four-card secure XOR. In: Deng, X., Hopcroft, J.E., Xue, J. (eds.) FAW 2009. LNCS, vol. 5598, pp. 358–369. Springer, Heidelberg (2009). https://doi.org/10.1007/978-3-642-02270-8_36
34. Murata, S., Miyahara, D., Mizuki, T., Sone, H.: Public-PEZ cryptography. In: Susilo, W., Deng, R.H., Guo, F., Li, Y., Intan, R. (eds.) ISC 2020. LNCS, vol. 12472, pp. 59–74. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-62974-8_4
35. Nakai, T., Misawa, Y., Tokushige, Y., Iwamoto, M., Ohta, K.: Secure computation for threshold functions with physical cards: power of private permutations. New Gener. Comput. **40**, 95–113 (2022). https://doi.org/10.1007/s00354-022-00153-7
36. Nakai, T., Misawa, Y., Tokushige, Y., Iwamoto, M., Ohta, K.: How to solve Millionaires' problem with two kinds of cards. New Gener. Comput. **39**(1), 73–96 (2021). https://doi.org/10.1007/s00354-020-00118-8
37. Niemi, V., Renvall, A.: Solitaire zero-knowledge. Fundam. Inf. **38**(1,2), 181–188 (1999), https://doi.org/10.3233/FI-1999-381214
38. Ono, H., Manabe, Y.: Card-based cryptographic logical computations using private operations. New Gener. Comput. **39**(1), 19–40 (2020). https://doi.org/10.1007/s00354-020-00113-z
39. Pass, R., Shelat, A.: A course in cryptography (2010). http://www.cs.cornell.edu/~rafael/
40. Robert, L., Miyahara, D., Lafourcade, P., Mizuki, T.: Card-based ZKP for connectivity: applications to Nurikabe, Hitori, and Heyawake. New Gener. Comput. **40**, 149–171 (2022). https://doi.org/10.1007/s00354-022-00155-5
41. Robert, L., Miyahara, D., Lafourcade, P., Libralesso, L., Mizuki, T.: Physical zero-knowledge proof and NP-completeness proof of Suguru puzzle. Inf. Comput. **285**, 1–14 (2022). https://doi.org/10.1016/j.ic.2021.104858
42. Ruangwises, S.: Two standard decks of playing cards are sufficient for a ZKP for Sudoku. New Gener. Comput. **40**, 49–65 (2022). https://doi.org/10.1007/s00354-021-00146-y
43. Ruangwises, S., Itoh, T.: Physical zero-knowledge proof for Numberlink puzzle and k vertex-disjoint paths problem. New Gener. Comput. **39**(1), 3–17 (2020). https://doi.org/10.1007/s00354-020-00114-y
44. Ruangwises, S., Itoh, T.: Physical zero-knowledge proof for Ripple Effect. Theor. Comput. Sci. **895**, 115–123 (2021). https://doi.org/10.1016/j.tcs.2021.09.034
45. Sasaki, T., Miyahara, D., Mizuki, T., Sone, H.: Efficient card-based zero-knowledge proof for Sudoku. Theor. Comput. Sci. **839**, 135–142 (2020). https://doi.org/10.1016/j.tcs.2020.05.036

46. Shinagawa, K.: Card-based cryptography with dihedral symmetry. New Gener. Comput. **39**(1), 41–71 (2021). https://doi.org/10.1007/s00354-020-00117-9
47. Shinagawa, K., Nuida, K.: A single shuffle is enough for secure card-based computation of any Boolean circuit. Discret. Appl. Math. **289**, 248–261 (2021). https://doi.org/10.1016/j.dam.2020.10.013
48. Takashima, K., Miyahara, D., Mizuki, T., Sone, H.: Actively revealing card attack on card-based protocols. Nat. Comput., 1–13 (2021, in press). https://doi.org/10.1007/s11047-020-09838-8
49. Ueda, I., Miyahara, D., Nishimura, A., Hayashi, Y., Mizuki, T., Sone, H.: Secure implementations of a random bisection cut. Int. J. Inf. Secur. **19**(4), 445–452 (2019). https://doi.org/10.1007/s10207-019-00463-w
50. Yao, A.C.: Protocols for secure computations. In: Foundations of Computer Science, pp. 160–164. IEEE Computer Society, Washington, DC (1982). https://doi.org/10.1109/SFCS.1982.88