IEICE TRANSACTIONS

# on Fundamentals of Electronics, Communications and Computer Sciences

VOL. E100-A NO. 1
JANUARY 2017



A PUBLICATION OF THE ENGINEERING SCIENCES SOCIETY
The Institute of Electronics, Information and Communication Engineers
Kikai-Shinko-Kaikan Bldg., 5-8, Shibakoen 3 chome, Minato-ku, TOKYO, 105-0011 JAPAN

INVITED PAPER *Special Section on Cryptography and Information Security*

# Computational Model of Card-Based Cryptographic Protocols and Its Applications

**Takaaki MIZUKI**[†a)] ***and*** **Hiroki SHIZUYA**[††]**,** ***Members***

**SUMMARY** Card-based protocols enable us to easily perform cryptographic tasks such as secure multiparty computation using a deck of physical cards. Since the first card-based protocol appeared in 1989, many protocols have been designed. A protocol is usually described with a series of somewhat intuitive and verbal descriptions, such as "turn over this card," "shuffle these two cards," "apply a random cut to these five cards," and so on. On the other hand, a formal computational model of card-based protocols via abstract machine was constructed in 2014. By virtue of the formalization, card-based protocols can be treated more rigorously; for example, it enables one to discuss the lower bounds on the number of cards required for secure computations. In this paper, an overview of the computational model with its applications to designing protocols and a survey of the recent progress in card-based protocols are presented.

***key words:*** *card-based protocols, card games, cryptography without computers, real-life hands-on cryptography, secure multiparty computations*

## 1. Introduction

Card-based protocols allow cryptographic tasks, such as secure multiparty computation, to be performed easily using a deck of physical cards. Assume two types of several cards with faces that are either black (♣) or red (♡) and identical backs (?). Using two cards of different colors, one can easily encode a bit value, for example,

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

According to the above encoding (1), a player, Alice, can commit her private bit $a \in \{0, 1\}$ to a pair of face-down cards

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

which we call a *commitment* to bit $a$. Typically, a card-based protocol receives a few commitments as its input and applies a series of actions to produce its output.

Let us start with one of the simplest protocols, the NOT protocol. Given a commitment to a bit $a$ as input, the NOT protocol swaps only the two cards constituting the commitment so that a commitment to the negation $\bar{a}$ as output is obtained:

$$\underbrace{\boxed{?}\boxed{?}}_{a} \rightarrow \overbrace{\boxed{?}\boxed{?}}^{\rightleftharpoons} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{\bar{a}}.$$

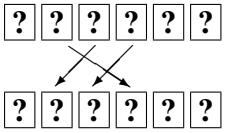
Thus, one can easily negate a commitment while keeping its value secret.

As another example of protocols, we here introduce the Mizuki-Sone AND protocol [1], which receives commitments to Alice's bit $a$ and Bob's bit $b$, and generates a commitment to $a \wedge b$, as follows.

1. Put a black card and a red card between the two commitments, and turn them over:

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

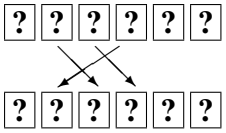
   Note that the two face-down cards in the middle constitute a commitment to 0.
2. Rearrange the sequence of six cards:



3. Apply a *random bisection cut*, which means bisecting the sequence and shuffling the two portions:

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

   Therefore, the resulting sequence of six cards is either the same as the original one or a sequence, the two halves of which have been switched with a probability of 1/2.
4. Rearrange the sequence of six cards:



5. Reveal the first two cards (from the left). Then, a commitment to $a \wedge b$ is obtained as

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

This protocol produces a commitment to $a \wedge b$ without leaking any information about $a$ and $b$. We explain its correctness

Manuscript received June 30, 2016.
Manuscript revised August 26, 2016.

[†]The author is with the Cyberscience Center, Tohoku University, Sendai-shi, 980-8578 Japan.
[††]The author is with the Center for Information Technology in Education, Tohoku University, Sendai-shi, 980-8576 Japan.
a) E-mail: tm-paper+cardieiceinv@g-mail.tohoku-university.jp
DOI: 10.1587/transfun.E100.A.3

**Table 1** Some of the existing card-based protocols.

| | # of colors | # of cards | Avg. # of trials |
|---|---|---|---|
| ◦ *Committed AND protocols* | | | |
| Crépeau-Kilian [3] | 4 | 10 | 6 |
| Niemi-Renvall [4] | 2 | 12 | 2.5 |
| Stiglic [5] | 2 | 8 | 2 |
| Mizuki-Sone [1] (§1, 2, 4) | 2 | 6 | 1 |
| Koch-Walzer-Härtel [6] (§5) | 2 | 5 | 1 |
| Koch-Walzer-Härtel [6] (§5) | 2 | 4 | 1.8 |
| ◦ *Committed XOR protocols* | | | |
| Crépeau-Kilian [3] | 4 | 14 | 6 |
| Mizuki-Uchiike-Sone [7] | 2 | 10 | 2 |
| Mizuki-Sone [1] | 2 | 4 | 1 |
| ◦ *Non-committed AND protocols* | | | |
| den Boer [2] | 2 | 5 | 1 |
| Mizuki-Kumamoto-Sone [8] | 2 | 4 | 1 |

and security in Sect. 4. The protocol, which uses six cards, is hereinafter referred to as the *six-card AND protocol*.

Similarly to the six-card AND protocol [1] described above, a protocol producing a commitment to the value of the AND function is called a *committed* AND protocol. As shown in Table 1, several committed AND protocols as well as committed XOR protocols have been proposed. Furthermore, as seen also in Table 1, *non-committed* AND protocols have been developed. In fact, the first card-based protocol designed by den Boer in 1989 [2] was a non-committed AND protocol; given two commitments as input, the protocol produces its output in a format that differs from encoding (1).

In addition to the NOT protocol and the committed AND/XOR protocols, there are copy protocols [1], [3], [9] that can make identical copied commitments from a given commitment. Thus, as easily imagined, combining these elementary protocols, one can construct a protocol for any function (see, e.g., [10]). Moreover, efficient protocols have been developed for specific functions, such as the adder [11], three-variable functions [12], and the conjunction of multiple variables [13].

As seen in the above descriptions of the protocols, a protocol is usually described with a series of somewhat intuitive illustrations and verbal descriptions, for example, "turn over this card," "shuffle these two cards," "apply a random cut to these five cards," and so on. In contrast, a formal computational model of card-based protocols via abstract machine was constructed by Mizuki and Shizuya [14] in 2014. By virtue of the formalization, it has become possible to treat card-based protocols more rigorously. For example, it enables one to discuss the lower bounds on the number of cards required for secure computations. In fact, Koch, Walzer, and Härtel [6] proved that there does not exist a finite-runtime committed AND protocol using four cards. They also proposed an excellent method, based on the formal computational model, for describing a protocol by which one can easily confirm its correctness and security [6]. In this paper, an overview of the computational model of card-based protocols with its applications to designing protocols and a survey of the recent progress in card-based cryptography are presented.

Historically, card games may stem from the cards invented in the 9th century, but card protocols for cryptographic purposes were not known until Peter Winkler's 1981 article [15]. Fischer, Paterson, and Rackoff [16] extended the idea presented in [15] to implement a secret bit transmission between two players. Following their results, many researchers designed secret bit transmission and secret key exchange schemes using a deck of cards (see, e.g., [17]–[21]); it should be noted that they do not intend that a real deck of cards be used, i.e., dealing cards is rather an abstract notion to capture a priori information distributed to players. In contrast, as mentioned before, card-based protocols are supposed to use a real deck of physical cards, i.e., humans can practically execute a card-based protocol with everyday objects. There are other physically implemented cryptographic protocols, e.g., those presented in [22]–[26].

The remainder of this paper is organized as follows. We review the computational model of card-based protocols formalized by Mizuki and Shizuya [14] in Sect. 2 and mention a framework for committed protocols in Sect. 3. In Sect. 4, we present the "Koch-Walzer-Härtel diagram [6]," which enriches descriptions of protocols. We then introduce the recent AND protocols developed by Koch, Walzer, and Härtel [6] in Sect. 5 and some lower bounds in Sect. 6. In Sect. 7, we mention additional recent progress in card-based cryptography. This paper is concluded in Sect. 8 with possible directions of future work.

## 2. Computational Model

As mentioned above, a formal computational model of card-based protocols was constructed in 2014 [14]. Then, Koch, Walzer, and Härtel [6] made some improvement to the descriptions of the model in 2015. In this section, according to these two papers [6], [14], we overview the computational model by taking the six-card AND protocol [1] shown in Sect. 1 as an example to exhibit the concepts.

### 2.1 Notations

Clearly, the most important object for card-based protocols is a deck of cards, for example, a deck of six cards $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, as used in the six-card AND protocol [1]. To represent a deck, we use a multiset such as

$$\mathcal{D}^{\mathrm{ex}} = [\,\clubsuit, \clubsuit, \clubsuit, \heartsuit, \heartsuit, \heartsuit\,],$$

where "ex" represents "example." Formally, such a non-empty finite multiset $\mathcal{D}$ is called a *deck* if $\mathcal{D} \cap \{?\} = \emptyset$ where "?" is the "back-side" symbol. We call any element $c \in \mathcal{D}$ in a deck $\mathcal{D}$ (such as $\clubsuit$ and $\heartsuit$) an *atomic card*.

When a card is placed on the table, there are two options: it is either face-up (e.g., $\boxed{\clubsuit}$) or face-down ($\boxed{?}$). To capture this property, we use an expression $\frac{\clubsuit}{?}$ or $\frac{?}{\clubsuit}$. Formally, $\frac{c}{?}$ with $c \in \mathcal{D}$ represents a *face-up card* (of a deck $\mathcal{D}$), and $\frac{?}{c}$ represents a *face-down card*. We call a face-up or face-down

card a *lying card*. Given a lying card $\frac{c}{?}$ or $\frac{?}{c}$, we denote its atomic card by $\mathsf{atom}(\frac{c}{?}) = \mathsf{atom}(\frac{?}{c}) = c$; further, we denote what we can see when looking at the lying card on the table by $\mathsf{top}(\frac{c}{?}) = c$ and $\mathsf{top}(\frac{?}{c}) = ?$.

Let us remember the input to the six-card AND protocol [1], namely, a sequence of six cards put on the table:


In order to represent such lying cards, we have to consider four possible sequences because we do not know the values of $a$ and $b$:

$$\Gamma^{00} = \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right),$$

$$\Gamma^{01} = \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}\right),$$

$$\Gamma^{10} = \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right),$$

and

$$\Gamma^{11} = \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}\right).$$

Note that $\Gamma^{00}$ corresponds to $(a, b) = (0, 0)$, $\Gamma^{01}$ corresponds to $(a, b) = (0, 1)$, and so on. Thus, the set $\{\Gamma^{00}, \Gamma^{01}, \Gamma^{10}, \Gamma^{11}\}$ is considered to be the input set to the protocol, as seen again in the next subsection. Formally, we say that a $d$-tuple $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ consisting of $d$ lying cards from a deck $\mathcal{D}$ with $d = |\mathcal{D}|$ is a *sequence* from $\mathcal{D}$ if $[\,\mathsf{atom}(\alpha_1), \mathsf{atom}(\alpha_2), \ldots, \mathsf{atom}(\alpha_d)\,] = \mathcal{D}$. We define

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

for a deck $\mathcal{D}$. That is, $\mathsf{Seq}^{\mathcal{D}}$ is the set of all (possible) sequences from a deck $\mathcal{D}$.

Next, we extend the use of $\mathsf{top}(\cdot)$ to use for 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 $\Gamma$. For instance, for the above sequence $\Gamma^{00}$, the visible sequence is

$$\mathsf{top}(\Gamma^{00}) = (?, ?, \clubsuit, \heartsuit, ?, ?).$$

We also define the *visible sequence set* $\mathsf{Vis}^{\mathcal{D}}$ of $\mathcal{D}$ as

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

## 2.2 Protocols

In this subsection, we formally define 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.

Recall the actions that the six-card AND protocol [1] applies to a sequence: turning over the two middle cards (for which we use the expression "turn"), rearranging the order of the sequence ("perm"), shuffling the halves of the sequence ("shuf"), and specifying the output commitment ("result"). In addition to these four actions, there is one unfamiliar action, random flip ("rflip"). The detailed explanations of these five actions are given in the following.

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* $q_{\mathrm{f}} \in Q$;
- $A : (Q - \{q_{\mathrm{f}}\}) \times \mathsf{Vis}^{\mathcal{D}} \to Q \times \mathsf{Action}$ is an *action function*, where $\mathsf{Action}$ is the set of the following actions:
  - $(\mathsf{turn}, T)$ for $T \subseteq \{1, 2, \ldots, |\mathcal{D}|\}$;
  - $(\mathsf{perm}, \pi)$ for $\pi \in S_{|\mathcal{D}|}$, where $S_i$ denotes the symmetric group of degree $i$ throughout this paper;
  - $(\mathsf{shuf}, \Pi, \mathcal{F})$ for $\Pi \subseteq S_{|\mathcal{D}|}$ and a probability distribution $\mathcal{F}$ on $\Pi$;
  - $(\mathsf{rflip}, \Phi, \mathcal{G})$ for $\Phi \subseteq 2^{\{1,2,\ldots,|\mathcal{D}|\}}$ and a probability distribution $\mathcal{G}$ on $\Phi$;
  - $(\mathsf{result}, p_1, \ldots, p_\ell)$ for $p_1, p_2, \ldots, p_\ell \in \{1, 2, \ldots, |\mathcal{D}|\}$.

The protocol $\mathcal{P} = (\mathcal{D}, U, Q, A)$ proceeds as the Turing machine does: starting from the initial state $q_0$ and the initial sequence $\Gamma_0$ for some input sequence $\Gamma_0 \in U$, its current state $q$ and sequence $\Gamma$ move to the next state $q'$ and sequence $\Gamma'$ according to the output of the action function $A$. (Note that the action function $A$ outputs the next state and action depending on the current state $q$ and visible sequence $\mathsf{top}(\Gamma)$.) Specifically, given a current sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ with $d = |\mathcal{D}|$, each action in $\mathsf{Action}$ transforms the current sequence $\Gamma$ into the next sequence $\Gamma'$:

- $(\mathsf{turn}, T)$: $\Gamma' = (\beta_1, \beta_2, \ldots, \beta_d)$ such that

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

  for every $i$, $1 \le i \le d$, where $\mathsf{swap}(\frac{c}{?}) = \frac{?}{c}$ and $\mathsf{swap}(\frac{?}{c}) = \frac{c}{?}$ for an atomic card $c$;
- $(\mathsf{perm}, \pi)$: $\Gamma' = (\alpha_{\pi^{-1}(1)}, \alpha_{\pi^{-1}(2)}, \ldots, \alpha_{\pi^{-1}(d)})$;
- $(\mathsf{shuf}, \Pi, \mathcal{F})$: $\Gamma'$ resulting from applying action $(\mathsf{perm}, \pi)$ to $\Gamma$, where $\pi$ is a permutation drawn from $\Pi$ according to the probability distribution $\mathcal{F}$;
- $(\mathsf{rflip}, \Phi, \mathcal{G})$: $\Gamma'$ resulting from applying action $(\mathsf{turn}, T)$ to $\Gamma$, where $T$ is a set drawn from $\Phi$ according to the probability distribution $\mathcal{G}$;
- $(\mathsf{result}, p_1, \ldots, p_\ell)$: this action specifies the positions of the output, and appears if and only if the first component of the output of $A$ is the final state $q_{\mathrm{f}}$ (and the protocol terminates).

It should be noted that the rearrangement action is a special case of the shuffle action, i.e., $(\mathsf{perm}, \pi)$ can be expressed

as $(\mathsf{shuf}, \{\pi\}, \mathcal{F})$ with $\Pr_{\mathcal{F}}(\pi) = 1$. Similarly, the turn action is a special case of the random flip action. Thus, we could exclude the rearrangement and turn actions from the model without loss of generality. However, in our opinion, removing these elementary actions would lead to a protocol that is not human-friendly. Furthermore, the random flip action has not been used in any known protocols, and at present it is not even known how to implement it.

If the probability distribution $\mathcal{F}$ of a shuffle action $(\mathsf{shuf}, \Pi, \mathcal{F})$ is uniform, then we omit $\mathcal{F}$ and simply write $(\mathsf{shuf}, \Pi)$. Let us take the random bisection cut

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

used in the six-card AND protocol [1] as an example. The shuffle action is expressed as

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

where $\mathsf{id}$ denotes the identity permutation and $(i_1\, i_2\, \ldots\, i_\ell)$ means a cyclic permutation. Since it is uniformly distributed, we simply write

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

for the random bisection cut above.

As seen above, the formalization of the shuffle action $(\mathsf{shuf}, \Pi, \mathcal{F})$ given in [14] is quite general, that is, $\Pi$ can be any subset of $S_{|\mathcal{D}|}$ and $\mathcal{F}$ can be any distribution. In fact, this yielded strong possibility results: Koch, Walzer, and Härtel [6] conceived a four-card committed AND protocol (and so on) by considering unconventional shuffles, as shown in Sect. 5.

### 2.3 Formal Description of the Six-Card AND Protocol

We are now ready to formally describe the six-card AND protocol [1] based on the computational model explained above.

The deck for the six-card AND protocol is $\mathcal{D}^{\mathrm{ex}}$, shown in Sect. 2.1, and the input set is $\{\Gamma^{00}, \Gamma^{01}, \Gamma^{10}, \Gamma^{11}\}$, shown also in Sect. 2.1. Therefore, the quadruple is

$$\mathcal{P}^{\mathrm{ex}} = (\mathcal{D}^{\mathrm{ex}}, \{\Gamma^{00}, \Gamma^{01}, \Gamma^{10}, \Gamma^{11}\}, \{q_0, q_1, \ldots, q_5, q_{\mathrm{f}}\}, A^{\mathrm{ex}})$$

such that

$$\begin{aligned}
A^{\mathrm{ex}}(q_0, (?, ?, \clubsuit, \heartsuit, ?, ?)) &= (q_1, (\mathsf{turn}, \{3, 4\})) \\
A^{\mathrm{ex}}(q_1, (?, ?, ?, ?, ?, ?)) &= (q_2, (\mathsf{perm}, (2\,4\,3))) \\
A^{\mathrm{ex}}(q_2, (?, ?, ?, ?, ?, ?)) &= (q_3, (\mathsf{shuf}, \{\mathsf{id}, (1\,4)(2\,5)(3\,6)\})) \\
A^{\mathrm{ex}}(q_3, (?, ?, ?, ?, ?, ?)) &= (q_4, (\mathsf{perm}, (2\,3\,4))) \\
A^{\mathrm{ex}}(q_4, (?, ?, ?, ?, ?, ?)) &= (q_5, (\mathsf{turn}, \{1, 2\})) \\
A^{\mathrm{ex}}(q_5, (\clubsuit, \heartsuit, ?, ?, ?, ?)) &= (q_{\mathrm{f}}, (\mathsf{result}, 3, 4)) \\
A^{\mathrm{ex}}(q_5, (\heartsuit, \clubsuit, ?, ?, ?, ?)) &= (q_{\mathrm{f}}, (\mathsf{result}, 5, 6)).
\end{aligned}$$

This $\mathcal{P}^{\mathrm{ex}}$ is the formal description of the six-card AND protocol. The following type of pseudo-code makes it easier to understand it.

---

*Six-card AND protocol*
input set:

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

$(\mathsf{turn}, \{3, 4\})$
$(\mathsf{perm}, (2\,4\,3))$
$(\mathsf{shuf}, \{\mathsf{id}, (1\,4)(2\,5)(3\,6)\})$
$(\mathsf{perm}, (2\,3\,4))$
$(\mathsf{turn}, \{1, 2\})$
**if** visible seq. $= (\clubsuit, \heartsuit, ?, ?, ?, ?)$ **then**
  $(\mathsf{result}, 3, 4)$
**else if** visible seq. $= (\heartsuit, \clubsuit, ?, ?, ?, ?)$ **then**
  $(\mathsf{result}, 5, 6)$

---

## 3. Framework for Committed Protocols

In this section, we introduce the framework for committed protocols, based on the formalization given by Koch, Walzer, and Härtel [6].

First, we mention some terms. Consider an execution where a protocol $\mathcal{P}$ terminates; then, the enumeration $(\Gamma_0, \Gamma_1, ..., \Gamma_t)$ of all sequences from the initial to the final one (where $\Gamma_{i-1}$ is transformed into $\Gamma_i$ by an action for every $i$, $1 \le i \le t$) is called a *sequence-trace* (of $\mathcal{P}$). Similarly, such $(\mathsf{top}(\Gamma_0), \mathsf{top}(\Gamma_1), ..., \mathsf{top}(\Gamma_t))$ is called a *visible sequence-trace*. For example, there are two possible visible sequence-traces of the six-card AND protocol $\mathcal{P}^{\mathrm{ex}}$ (presented in Sect. 2.3):

$$\begin{aligned}
&((?, ?, \clubsuit, \heartsuit, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?), \\
&\quad (?, ?, ?, ?, ?, ?), (\clubsuit, \heartsuit, ?, ?, ?, ?), (\clubsuit, \heartsuit, ?, ?, ?, ?)) \quad (2)
\end{aligned}$$

and

$$\begin{aligned}
&((?, ?, \clubsuit, \heartsuit, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?), \\
&\quad (?, ?, ?, ?, ?, ?), (\heartsuit, \clubsuit, ?, ?, ?, ?), (\heartsuit, \clubsuit, ?, ?, ?, ?)). \quad (3)
\end{aligned}$$

Next, we show a formal definition of a committed protocol. To make the treatment general, let us assume that we have commitments to $n$ bits $x_1, x_2, \ldots, x_n$ and want to produce a commitment to the value of $f(x_1, x_2, \ldots, x_n)$ for a Boolean function $f : \{0, 1\}^n \rightarrow \{0, 1\}$. Without loss of generality, we obey the encoding scheme (1) (and hence a deck $\mathcal{D}$ is supposed to contain sufficient numbers of $\clubsuit$ and $\heartsuit$, as seen in the following Definition 1).

**Definition 1:** Let $f : \{0, 1\}^n \rightarrow \{0, 1\}$ be a Boolean function. We say that $\mathcal{P} = (\mathcal{D}, U, Q, A)$ is a *committed protocol for* $f$ if the following holds:

- the deck $\mathcal{D}$ has at least $n$ atomic cards of $\clubsuit$ and $n$ atomic cards of $\heartsuit$;

- the input set $U$ consists of $2^n$ sequences

  $$\Gamma^{(x_1,x_2,\ldots,x_n)} = (\alpha_1, \alpha_2, \ldots, \alpha_{|\mathcal{D}|})$$

  (where the superscript $(x_1, x_2, \ldots, x_n)$ runs in $\{0,1\}^n$) such that

  $$(\alpha_{2i-1}, \alpha_{2i}) = \begin{cases} \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right) & \text{if } x_i = 0; \\ \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}\right) & \text{if } x_i = 1 \end{cases}$$

  for every $i$, $1 \le i \le n$;
- the protocol terminates with a sequence-trace having a finite average number of sequences;
- for an execution starting with $\Gamma^{(x_1,x_2,\ldots,x_n)}$, it terminates with an action $(\mathsf{result}, p_1, p_2)$ such that

  $$(\beta_{p_1}, \beta_{p_2}) = \begin{cases} \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}\right) & \text{if } f(x_1, x_2, \ldots, x_n) = 0; \\ \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}\right) & \text{if } f(x_1, x_2, \ldots, x_n) = 1, \end{cases}$$

  where $(\beta_1, \beta_2, \ldots, \beta_{|\mathcal{D}|})$ is the final sequence;
- it is secure in the sense of the following Definition 2.

We next consider the security of protocols. Given a protocol $\mathcal{P} = (\mathcal{D}, U, Q, A)$, let $\mathcal{M}$ be a probability distribution on the input set $U$; then, we denote the random variable associating probability to a visible sequence-trace by $V^{(\mathcal{M},\mathcal{P})}$.

**Definition 2:** We say that a protocol $\mathcal{P} = (\mathcal{D}, U, Q, A)$ is *secure* if, for any probability distribution $\mathcal{M}$ on the input set $U$, $M$ and $V^{(\mathcal{M},\mathcal{P})}$ are independent of each other, where $M$ (induced by $\mathcal{M}$) is the random variable associating probability to a sequence of $U$.

We see in the next section that $\mathcal{P}^{\mathrm{ex}}$ is secure, and hence, is a committed protocol for the AND function $(a, b) \mapsto a \wedge b$.

## 4. Koch-Walzer-Härtel Diagram

In 2015, Koch, Walzer, and Härtel [6] proposed an excellent method to describe a protocol using a type of diagram, which we call a *Koch-Walzer-Härtel diagram*. This diagram provides good understanding of the manner in which a protocol works correctly and securely.

Figure 1 displays the Koch-Walzer-Härtel diagram of the six-card AND protocol

$$\mathcal{P}^{\mathrm{ex}} = (\mathcal{D}^{\mathrm{ex}}, \{\Gamma^{00}, \Gamma^{01}, \Gamma^{10}, \Gamma^{11}\}, \{q_0, q_1, \ldots, q_5, q_{\mathrm{f}}\}, A^{\mathrm{ex}})$$

presented in Sect. 2.3. In the diagram, there are six boxes, each of which contains several *atomic sequences* (such as ♣♡♣♡♣♡ and ♣♣♡♡♣♡) together with polynomials (such as $X_{00}$ and $\frac{1}{2}X_{00} + \frac{1}{2}X_{10}$).

Each box is associated to a prefix of the visible sequence-trace. (Recall the two visible sequence-traces (2) and (3) shown in Sect. 3.) For instance, the first (topmost) box in Fig. 1 is associated with the prefix

$$((?, ?, \clubsuit, \heartsuit, ?, ?), (?, ?, ?, ?, ?, ?)),$$

that is, it occurs immediately after turning over the two middle cards. The second box is associated with

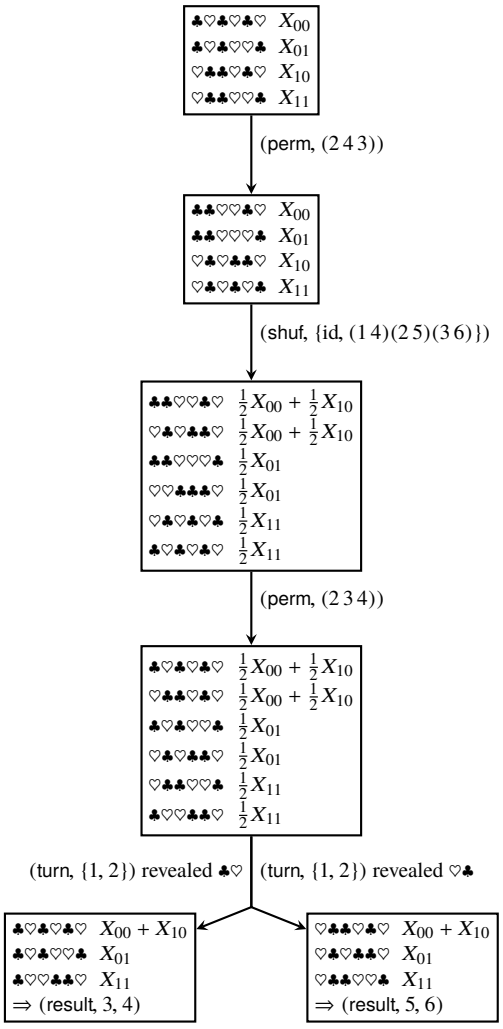



**Fig. 1** Koch-Walzer-Härtel diagram of the six-card AND protocol.

$$((?, ?, \clubsuit, \heartsuit, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?)),$$

that is, it occurs immediately after applying action $(\mathsf{perm}, (2\,4\,3))$. The two bottommost boxes are associated with the visible sequence-traces (2) and (3) themselves.

The variable $X_{00}$ ($X_{01}$, $X_{10}$, $X_{11}$) represents the probability that the input sequence $\Gamma^{00}$ ($\Gamma^{01}$, $\Gamma^{10}$, $\Gamma^{11}$, respectively) occurs.

Each polynomial next to an atomic sequence inside a box represents the conditional probability that the atomic sequence occurs, given the prefix of the visible sequence. Let us take the third box in Fig. 1 as an example. The topmost polynomial $\frac{1}{2}X_{00} + \frac{1}{2}X_{10}$ inside the box represents the probability that the current atomic sequence is ♣♣♡♡♣♡, given the prefix of the visible sequence

$$((?, ?, \clubsuit, \heartsuit, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?), (?, ?, ?, ?, ?, ?)).$$

In fact, considering the two actions $(\mathsf{perm}, (2\,4\,3))$ and $(\mathsf{shuf}, \{\mathrm{id}, (1\,4)(2\,5)(3\,6)\})$, one can confirm that the atomic sequence ♣♣♡♡♣♡ comes from the input sequence $\Gamma^{00}$ or $\Gamma^{10}$

with a probability of 1/2. One can also easily confirm that other polynomials (and those in other boxes) are compatible with the corresponding atomic sequences.

From the observation thus far, one can imagine the manner in which the Koch-Walzer-Härtel diagram of a given protocol can be derived (see [6] for the details).

Just by looking at the Koch-Walzer-Härtel diagram of a protocol, we can easily check that it works correctly. Indeed, the last boxes in the diagram (i.e., Fig. 1) of the six-card AND protocol immediately show that the actions $(\mathsf{result}, 3, 4)$ and $(\mathsf{result}, 5, 6)$ correctly specify the location of a commitment to the AND value.

Furthermore, the security of the six-card AND protocol can be confirmed through the Koch-Walzer-Härtel diagram. When summing up all polynomials in any of the six boxes, we always have $X_{00} + X_{01} + X_{10} + X_{11}$, that is, the coefficient of every variable is 1. This implies that the input sequence and the visible sequence-trace are stochastically independent, and hence, $\mathcal{P}^{\mathrm{ex}}$ is secure. In general, if, for each box of the Koch-Walzer-Härtel diagram of a protocol, the coefficient of every variable is 1 when summing up all polynomials in the box, then the protocol is secure; see [6] for the details.

Thus, we can formally say that $\mathcal{P}^{\mathrm{ex}}$ is a committed protocol for the AND function.

## 5. Koch-Walzer-Härtel AND Protocols

We elaborated on the six-card AND protocol in the previous sections. Recall that it is a committed AND protocol, proposed in 2009, using six cards. Recently, in 2015, Koch, Walzer, and Härtel [6] improved on the result in terms of the number of required cards, i.e., they constructed a four-card committed AND protocol and a five-card committed AND protocol. While the former needs to take an average number of trials, the latter always terminates within a bounded number of actions (i.e., with a sequence-trace of bounded length). See Table 1 again.

Their four-card AND protocol is as follows.

---

*Koch-Walzer-Härtel four-card AND protocol*
input set:

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

$(\mathsf{shuf}, \{\mathsf{id}, (1\,3)(2\,4)\})$
$(\mathsf{shuf}, \{\mathsf{id}, (2\,3)\})$
$(\mathsf{turn}, \{2\})$
**if** visible seq. = $(?, \clubsuit, ?, ?)$ **then**
  $(\mathsf{turn}, \{2\})$
  $(\mathsf{shuf}, \{\mathsf{id}, (1\,3)\})$
**1** $(\mathsf{shuf}, \{\mathsf{id}, (1\,2)(3\,4)\}, \mathsf{id}\mapsto 1/3, (1\,2)(3\,4)\mapsto 2/3)$
  $(\mathsf{turn}, \{4\})$
  **if** visible seq. = $(?, ?, ?, \clubsuit)$ **then**
    $(\mathsf{result}, 1, 2)$
  **else if** visible seq. = $(?, ?, ?, \heartsuit)$ **then**
    $(\mathsf{turn}, \{4\})$
    $(\mathsf{shuf}, \{\mathsf{id}, (1\,3)\})$
    $(\mathsf{perm}, (1\,3\,4\,2))$
    **goto 2**
**else if** visible seq. = $(?, \heartsuit, ?, ?)$ **then**
  $(\mathsf{turn}, \{2\})$
  $(\mathsf{shuf}, \{\mathsf{id}, (3\,4)\})$
**2** $(\mathsf{shuf}, \{\mathsf{id}, (1\,3)(2\,4)\}, \mathsf{id}\mapsto 1/3, (1\,3)(2\,4)\mapsto 2/3)$
  $(\mathsf{turn}, \{1\})$
  **if** visible seq. = $(\heartsuit, ?, ?, ?)$ **then**
    $(\mathsf{result}, 2, 4)$
  **else if** visible seq. = $(\clubsuit, ?, ?, ?)$ **then**
    $(\mathsf{turn}, \{1\})$
    $(\mathsf{shuf}, \{\mathsf{id}, (3\,4)\})$
    $(\mathsf{perm}, (1\,2\,4\,3))$
    **goto 1**

---

It can be seen in the Koch-Walzer-Härtel diagram of the protocol depicted in [6] (although we omit it in this paper) that one can confirm that the protocol above is surely a committed protocol for the AND function. Notice that the protocol has a loop, and the expected number of times the loop is repeated is calculated as $9/5 = 1.8$ (see [6] for the details).

Since we need at least four cards for input commitments to $a$ and $b$, this four-card AND protocol is optimal in terms of the number of required cards.

The protocol uses somewhat unusual shuffle actions:

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

and

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

That is, the probability distributions are non-uniform. When the protocol was designed, finding a feasible implementation of such a non-uniform shuffle action (by humans) was an open problem [6] (although a solution was proposed more recently in 2016 [27]; see Sect. 7.1).

Koch, Walzer, and Härtel [6] also provided a five-card committed AND protocol that always terminates before a bounded number of actions are executed. The protocol uses one additional card $\boxed{\heartsuit}$ in addition to the four cards for the input commitments, as follows.

---

*Koch-Walzer-Härtel five-card AND protocol*
input set:

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

$(\mathsf{turn}, \{5\})$
$(\mathsf{shuf}, \{\mathsf{id}, (1\,3)(2\,4)\})$
$(\mathsf{shuf}, \{\mathsf{id}, (2\,3)\})$
$(\mathsf{turn}, \{2\})$
**if** visible seq. = $(?, \clubsuit, ?, ?, ?)$ **then**

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

---

This protocol also uses non-uniform shuffle actions:

(shuf, {id, (5 4 3 2 1)}, id↦2/3, (5 4 3 2 1)↦1/3)

and

(shuf, {id, (1 3)(2 4)}, id↦1/3, (1 3)(2 4)↦2/3).

Note that, while the latter shuffle, which already appears in the four-card protocol above, is "closed" (because $((1\,3)(2\,4))^2 = \mathsf{id}$), the former shuffle is not. These two unconventional shuffle actions can also be implemented by humans [27]; see Sect. 7.1.

## 6. Lower Bounds

By virtue of the formal computational model presented in Sect. 2, it is now possible to discuss impossibility results or lower bounds on the number of required cards.

The first impossibility result that was shown in [14] is that it is impossible to make two identical copied face-down cards from an unknown face-down card (with perfect secrecy).

Next, Koch, Walzer, and Härtel [6] proved that there is no finite-runtime committed AND protocol using four cards. In their proof, after they supposed a four-card finite-runtime committed AND protocol, they carefully analyzed and characterized possible atomic sequences in a box in the Koch-Walzer-Härtel diagram of such a protocol to derive a contradiction. Therefore, this non-existence result immediately implies that their five-card AND protocol presented in Sect. 5 is the best possible (remember that it uses five cards and is of finite-runtime).

It will be appreciated if other lower bounds are found.

## 7. Recent Progress

In this section, we introduce other recent progress in card-based cryptography.

### 7.1 Implementation of Non-Uniform Shuffle

As seen in Sect. 5, the Koch-Walzer-Härtel AND protocols [6] developed in 2015 utilize non-uniform shuffle actions.

In 2016, Nishimura et al. [27] presented a secure implementation of a non-uniform shuffle. To implement the shuffle, they utilized physical cases that can store piles of cards, such as boxes and envelopes. Therefore, humans are able to perform the non-uniform shuffle using these everyday objects.

### 7.2 Random Permutation without Fixed Points

Card-based protocols can perform not only secure multiparty computation but also other cryptographic tasks. In fact, in 1993, Crépeau and Kilian [3] proposed a card-based protocol that generates a random permutation having no fixed point. Such a random permutation is preferable when $n$ players want to exchange gifts, because they can avoid the undesirable situation where a player must buy a present for himself/herself. Crépeau and Kilian's protocol [3] requires $2n^2$ cards of four colors. The permutation is produced as a sequence of face-down cards and each of $n$ players can receive his/her portion that privately tells him/her for whom he/she is going to buy a present.

Recently in 2015, Ishikawa, Chida, and Mizuki [28] improved on the result, i.e., they designed a new protocol to solve the "no fixed point" problem, showing that $n^2$ cards of two colors are sufficient. They also proposed a protocol using $O(n \log n)$ cards of two colors.

### 7.3 Use of Polarizing Cards and Polygon Cards

Shinagawa et al. [29] considered using a different type of card, i.e., they proposed protocols based on polarizing plates. Roughly speaking, one can encode a bit value by using two polarizing plates, depending on whether light can pass through the superimposed plates or not.

Shinagawa et al. [30] also considered the use of regular polygon cards. This allows efficient protocols to be constructed for secure computations of multi-valued input and output functions, because, roughly speaking, one can encode such an $i$-valued input using a regular $i$-sided polygon card according to its angle when it is put on the table.

## 8. Conclusion

In this paper, we reviewed the computational model of card-based protocols with its applications to designing protocols and recent progress. As considering a non-uniform shuffle has contributed to reducing the number of required cards, the

general computational model interestingly yields not only impossibility results but also broad feasibility results.

To conclude this paper, it is worth noting that many issues remain to be addressed in the future, as follows.

- Past research activities have been devoted mainly to reducing the number of cards used in a protocol. However, also of interest is the number of actions executed in a protocol. It is not yet known whether there is a trade-off between the number of cards and number of actions. The two numbers may correspond to the space complexity and time complexity, respectively. Protocols having fewer actions might be necessary for some applications.
- As mentioned in Sect. 2.2, one can consider any complicated shuffle action based on a mathematical theory. However, humans might not be able to execute such complicated shuffles in practice. A more exact characterization of shuffle actions that humans can easily implement is desirable (cf. [6]).
- The construction of more formal computational models for polarizing cards and regular polygon cards (introduced in Sect. 7.3) is one intriguing direction of future work.
- Card-based cryptography is useful for educational purposes; indeed, it has attracted many computer science students (e.g., [31]). We have confirmed that non-specialists such as high school students can easily perform card-based protocols using a real deck of cards; for example, without experiencing a problem, 21 students in our course were able to execute the six-card AND protocol 20 times to determine whether they were all keen to go for lunch together or not (avoiding an embarrassing situation). Suggestions for other attractive applications would be welcome.
- When executing a card-based protocol in daily life, there might be a "hardware" issue; for example, some cards may have scuff marks on their faces. Since only Mizuki and Shizuya [32] have attempted to resolve this issue, further research would be beneficial.

## Acknowledgments

We thank the editor and the anonymous reviewers, whose comments helped us to improve the presentation of this paper. This work was supported in part by JSPS KAKENHI Grant Numbers 26330001 and 26330150.

### References

[1] T. Mizuki and H. Sone, "Six-card secure AND and four-card secure XOR," Frontiers in Algorithmics, Lecture Notes in Computer Science, vol.5598, pp.358–369, Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[2] B. den Boer, "More efficient match-making and satisfiability the five card trick," Advances in Cryptology, EUROCRYPT'89, Lecture Notes in Computer Science, vol.434, pp.208–217, Springer Berlin Heidelberg, Berlin, Heidelberg, 1990.

[3] C. Crépeau and J. Kilian, "Discreet solitary games," Advances in Cryptology, CRYPTO'93, Lecture Notes in Computer Science, vol.773, pp.319–330, Springer Berlin Heidelberg, 1994.

[4] V. Niemi and A. Renvall, "Secure multiparty computations without computers," Theor. Comput. Sci., vol.191, no.1-2, pp.173–183, 1998.

[5] A. Stiglic, "Computations with a deck of cards," Theor. Comput. Sci., vol.259, no.1-2, pp.671–678, 2001.

[6] A. Koch, S. Walzer, and K. Härtel, "Card-based cryptographic protocols using a minimal number of cards," Advances in Cryptology, ASIACRYPT 2015, Lecture Notes in Computer Science, vol.9452, pp.783–807, Springer Berlin Heidelberg, Berlin, Heidelberg, 2015.

[7] T. Mizuki, F. Uchiike, and H. Sone, "Securely computing XOR with 10 cards," Australasian J. Combinatorics, vol.36, pp.279–293, 2006.

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

[9] A. Nishimura, T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, "Five-card secure computations using unequal division shuffle," Theory and Practice of Natural Computing, Lecture Notes in Computer Science, vol.9477, pp.109–120, Springer International Publishing, Cham, 2015.

[10] T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, "Card-based protocols for any Boolean function," Theory and Applications of Models of Computation, Lecture Notes in Computer Science, vol.9076, pp.110–121, Springer International Publishing, Cham, 2015.

[11] T. Mizuki, I.K. Asiedu, and H. Sone, "Voting with a logarithmic number of cards," Unconventional Computation and Natural Computation, Lecture Notes in Computer Science, vol.7956, pp.162–173, Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[12] T. Nishida, Y. Hayashi, T. Mizuki, and H. Sone, "Securely computing three-input functions with eight cards," IEICE Trans. Fundamentals, vol.E98-A, no.6, pp.1145–1152, 2015.

[13] T. Mizuki, "Card-based protocols for securely computing the conjunction of multiple variables," Theor. Comput. Sci., vol.622, pp.34–44, 2016.

[14] T. Mizuki and H. Shizuya, "A formalization of card-based cryptographic protocols via abstract machine," Int. J. Inf. Secur., vol.13, no.1, pp.15–23, 2014.

[15] P. Winkler, "Cryptologic techniques in bidding and defense: Part i," Bridge Magazine, pp.148–149, 1981.

[16] M.J. Fischer, M.S. Paterson, and C. Rackoff, "Secret bit transmission using a random deal of cards," Distributed Computing and Cryptography, Proc. DIMACS Workshop, pp.173–182, Princeton, New Jersey, USA, 1989.

[17] Z. Duan and C. Yang, "Unconditional secure communication: A Russian cards protocol," J. Comb. Optim., vol.19, no.4, pp.501–530, 2010.

[18] M.J. Fischer and R.N. Wright, "Bounds on secret key exchange using a random deal of cards," J. Cryptol., vol.9, no.2, pp.71–99, 1996.

[19] T. Mizuki, H. Shizuya, and T. Nishizeki, "A complete characterization of a family of key exchange protocols," International Journal of Information Security, vol.1, no.2, pp.131–142, 2002.

[20] T. Mizuki, H. Shizuya, and T. Nishizeki, "Characterization of optimal key set protocols," Discrete Appl. Math., vol.131, no.1, pp.213–236, 2003.

[21] C.M. Swanson and D.R. Stinson, "Combinatorial solutions providing improved security for the generalized Russian cards problem," Des. Codes Cryptogr., vol.72, no.2, pp.345–367, 2014.

[22] J. Balogh, J.A. Csirik, Y. Ishai, and E. Kushilevitz, "Private computation using a PEZ dispenser," Theor. Comput. Sci., vol.306, no.1-3, pp.69–84, 2003.

[23] R. Fagin, M. Naor, and P. Winkler, "Comparing information without leaking it," Commun. ACM, vol.39, no.5, pp.77–85, 1996.

[24] T. Moran and M. Naor, "Polling with physical envelopes: A rigorous analysis of a human-centric protocol," Advances in Cryptology,

EUROCRYPT 2006, Lecture Notes in Computer Science, vol.4004, pp.88–108, Springer Berlin Heidelberg, Berlin, Heidelberg, 2006.
[25] B. Fisch, D. Freund, and M. Naor, "Physical zero-knowledge proofs of physical properties," Advances in Cryptology, CRYPTO 2014, Lecture Notes in Computer Science, vol.8617, pp.313–336, Springer Berlin Heidelberg, Berlin, Heidelberg, 2014.
[26] A. Glaser, B. Barak, and R.J. Goldston, "A zero-knowledge protocol for nuclear warhead verification," Nature, vol.510, no.7506, pp.497–502, 2014.
[27] A. Nishimura, Y. Hayashi, T. Mizuki, and H. Sone, "An implementation of non-uniform shuffle for secure multi-party computation," Proc. 3rd ACM International Workshop on ASIA Public-Key Cryptography, AsiaPKC'16, pp.49–55, 2016.
[28] R. Ishikawa, E. Chida, and T. Mizuki, "Efficient card-based protocols for generating a hidden random permutation without fixed points," Unconventional Computation and Natural Computation, Lecture Notes in Computer Science, vol.9252, pp.215–226, Springer International Publishing, Cham, 2015.
[29] K. Shinagawa, T. Mizuki, J. Schuldt, K. Nuida, N. Kanayama, T. Nishide, G. Hanaoka, and E. Okamoto, "Secure multi-party computation using polarizing cards," Advances in Information and Computer Security, Lecture Notes in Computer Science, vol.9241, pp.281–297, Springer International Publishing, Cham, 2015.
[30] K. Shinagawa, T. Mizuki, J.C.N. Schuldt, K. Nuida, N. Kanayama, T. Nishide, G. Hanaoka, and E. Okamoto, "Multi-party computation with small shuffle complexity using regular polygon cards," Provable Security, Lecture Notes in Computer Science, vol.9451, pp.127–146, Springer International Publishing, Cham, 2015.
[31] A. Marcedone, Z. Wen, and E. Shi, "Secure dating with four or fewer cards," Cryptology ePrint Archive, Report 2015/1031, 2015.
[32] T. Mizuki and H. Shizuya, "Practical card-based cryptography," Fun with Algorithms, Lecture Notes in Computer Science, vol.8496, pp.313–324, Springer International Publishing, Cham, 2014.

**Takaaki Mizuki** received his B.E. degree in information engineering and his M.S. and Ph.D. degrees in information sciences from Tohoku University, Japan, in 1995, 1997, and 2000, respectively. He is currently an associate professor of the Cyberscience Center, Tohoku University. His research interests include cryptology and information security. He is a member of IEICE, IEEE, and IPSJ.

**Hiroki Shizuya** received his B.E, M.E., and Ph.D. degrees from Tohoku University, Japan, in 1981, 1984, and 1987, respectively. He joined Tohoku University in 1987, and has been a Professor since 1995. He is currently with both the Center for Information Technology in Education and the Department of Computer and Mathematical Sciences, Graduate School of Information Sciences. His current interests are in Cryptology and Computational Complexity Theory. He is a member of ACM and IEEE.