A Formalization of Card-Based Cryptographic Protocols via Abstract Machine[*]

Takaaki Mizuki Hiroki Shizuya

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

Abstract

Consider a face-down card lying on the table such that we do not know whether its suit color is black or red. Then, how do we make identical copies of the card while keeping its color secret? A partial solution has been devised: using a number of additional black and red cards, Niemi and Renvall proposed an excellent protocol which can copy a face-down card while allowing only a small probability of revealing its color. In contrast, this paper shows the non-existence of a perfect solution, namely, the impossibility of copying a face-down card with perfect secrecy. To prove such an impossibility result, we construct a rigorous mathematical model of card-based cryptographic protocols; giving this general computational model is the main result of this paper.

1 Introduction

Consider a face-down card $\boxed{?}$ lying on the table such that we do not know whether its suit color is black ($\boxed{\clubsuit}$) or red ($\boxed{\heartsuit}$). Then, how do we make identical copies of the card, say two copies $\boxed{?}\boxed{?}$ (having the same color as the original card), while keeping its color secret?

A partial solution has been presented in the literature: using a number of additional black and red cards $\boxed{\clubsuit}\boxed{\clubsuit}\cdots\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\cdots\boxed{\heartsuit}$ (whose backs $\boxed{?}$ are identical), Niemi and Renvall [11] proposed an excellent protocol which can copy a face-down card $\boxed{?}$ while allowing only a small probability of revealing its color; as seen later, in their protocol, a large number of cards reduces the probability of failure (namely, leaking the color information).

Because of nonzero probability of leaking information about the color of the face-down card to be copied, Niemi-Renvall's copy protocol provides a *partial* solution to the above problem. In contrast, to the best of our knowledge, the question "what about *perfect* solutions?" has not yet been answered. In this paper, we deal with this problem, and show the non-existence of a perfect solution. That is, we prove the impossibility of copying a face-down card with perfect secrecy. To prove such an impossibility result, we construct a rigorous mathematical model of card-based cryptographic protocols; giving a general computational model via abstract machine is the main result of this paper.

This paper begins with an example of executing Niemi-Renvall's copy protocol.

[*] This paper appears in International Journal of Information Security. The final publication is available at link.springer.com (DOI: 10.1007/s10207-013-0219-4).

1.1 Making two copies with success probability 7/8

Given a face-down card $\boxed{?}$, Niemi-Renvall's copy protocol [11] allows us to securely make its k copies with success probability $1-1/2^{s+1}$ using $(k+1)+(2^{s+1}-2)$ pairs of additional black and red cards (where the integer $s \geq 0$ is a security parameter; see [11] for details). Here, take the simple case of $k = s = 2$ as an example. Then, the protocol uses $(2+1)+(2^{2+1}-2) = 9$ pairs of $\boxed{\clubsuit}\boxed{\heartsuit}$, and thus we have a sequence of cards

$$\underset{x}{\boxed{?}}\quad \boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\quad \boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\quad \boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit} \tag{1}$$

on the table, where the leftmost card is the given face-down card (to be copied) whose secret color is denoted by $x \in \{\clubsuit, \heartsuit\}$ attached below it. Starting from the sequence (1), the protocol proceeds as follows.

First, turn over all face-up cards so that they are facing down:

$$\underset{x}{\boxed{?}}\quad \underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\quad \underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\quad \underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}\underset{\clubsuit}{\boxed{?}}\underset{\heartsuit}{\boxed{?}}$$

(where a symbol indicating the color is provided below each card for convenience), and apply three *random cuts*, each of which is denoted by $\langle\cdot\rangle$:

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

A random cut means that, as in the case of usual card games, a random number of cards on the left are moved on the right side of the sequence without changing their order (of course, the random number must be unknown). Therefore, we now have

$$\overset{1}{\underset{x}{\boxed{?}}}\quad \overset{2}{\underset{y}{\boxed{?}}}\overset{3}{\underset{\overline{y}}{\boxed{?}}}\overset{4}{\underset{y}{\boxed{?}}}\overset{5}{\underset{\overline{y}}{\boxed{?}}}\overset{6}{\underset{y}{\boxed{?}}}\overset{7}{\underset{\overline{y}}{\boxed{?}}}\quad \overset{8}{\underset{r_1}{\boxed{?}}}\overset{9}{\underset{\overline{r_1}}{\boxed{?}}}\overset{10}{\underset{r_1}{\boxed{?}}}\overset{11}{\underset{\overline{r_1}}{\boxed{?}}}\quad \overset{12}{\underset{r_2}{\boxed{?}}}\overset{13}{\underset{\overline{r_2}}{\boxed{?}}}\overset{14}{\underset{r_2}{\boxed{?}}}\overset{15}{\underset{\overline{r_2}}{\boxed{?}}}\overset{16}{\underset{r_2}{\boxed{?}}}\overset{17}{\underset{\overline{r_2}}{\boxed{?}}}\overset{18}{\underset{r_2}{\boxed{?}}}\overset{19}{\underset{\overline{r_2}}{\boxed{?}}} \tag{2}$$

for three random colors $y, r_1, r_2 \in \{\clubsuit, \heartsuit\}$, where $\overline{y}$ denotes the color opposite to that of y, i.e., $\{\overline{y}\} = \{\clubsuit, \heartsuit\} - \{y\}$ ($\overline{r_1}$ and $\overline{r_2}$ are defined similarly). Next, consider the 1st, 2nd, 8th, 10th, 12th, 14th, 16th and 18th cards (from the left):

$$\overset{1}{\underset{x}{\boxed{?}}}\quad \overset{2}{\underset{y}{\boxed{?}}}\quad \overset{8}{\underset{r_1}{\boxed{?}}}\overset{10}{\underset{r_1}{\boxed{?}}}\quad \overset{12}{\underset{r_2}{\boxed{?}}}\overset{14}{\underset{r_2}{\boxed{?}}}\overset{16}{\underset{r_2}{\boxed{?}}}\overset{18}{\underset{r_2}{\boxed{?}}}.$$

Note that if $x = y$, i.e., both colors of the first and second cards are the same, then the number of black cards (as well as the number of red cards) among these eight cards must be even; if $x \neq y$, i.e., $x = \overline{y}$, then it must be odd. Finally, after shuffling all eight cards (namely, after applying a random permutation), reveal all of them. If an even number of black cards appear, then the fourth and sixth cards

$$\overset{4}{\underset{y}{\boxed{?}}}\overset{6}{\underset{y}{\boxed{?}}}$$

in the sequence (2) are two copies having the color x (because $x = y$), as desired. If an odd number of black cards appear, then the fifth and seventh cards

$$\overset{5}{\underset{\overline{y}}{\boxed{?}}}\overset{7}{\underset{\overline{y}}{\boxed{?}}}$$

are the desired two copies.

When all eight revealed cards have the same color, i.e., $x = y = r_1 = r_2$, one can deduce the color x unambiguously, of course, and hence the secure copy fails; this event occurs with probability $1/2^3$. When $x = y = r_1 = r_2$ does not hold, one obtains no information about the color x from looking at the colors of the eight shuffled cards. (See [11] for a formal proof.) Thus, Niemi-Renvall's copy protocol for $k = s = 2$ nicely makes two copies with success probability 7/8.

1.2 Our results and related work

As mentioned in the previous subsection, if a small probability of leaking information about the color of a given face-down card is acceptable, then one can construct a protocol for copying the card; this may be sufficient for some practical purposes.

In contrast, this paper deals with perfect secrecy. Intuitively, it seems impossible to design a perfectly secure copy protocol. However, relying on intuition sometimes leads to errors. Therefore, to prove such an impossibility result, we construct a rigorous mathematical model of card-based protocols. Based on such a general computational model, we show the impossibility of copying a face-down card with perfect secrecy.

Our computational model (constructed later in Section 2) is rather general, and hence we believe that it can be used for proving the impossibility, finding lower bounds, or showing the optimality of certain protocols. For example, several card-based cryptographic protocols for secure computation are listed in Table 1, and it might be possible to show that a protocol is optimal under some criteria, such as the number of required cards, by using our computational model; more specifically, for instance, the six-card "committed format" secure AND protocol given in [8] could be proven to be best possible or not. In this context, constructing a formal computational model itself is worthwhile work.

	# of colors	# of cards	Avg. # of trials
○ *Secure AND in a non-committed format*			
den Boer [2]	2	5	1
Mizuki-Kumamoto-Sone [7]	2	4	1
○ *Secure AND in a committed format*			
Crépeau-Kilian [3]	4	10	6
Niemi-Renvall [11]	2	12	2.5
Stiglic [13]	2	8	2
Mizuki-Sone [8]	2	6	1
○ *Secure XOR in a committed format*			
Crépeau-Kilian [3]	4	14	6
Mizuki-Uchiike-Sone [9]	2	10	2
Mizuki-Sone [8]	2	4	1
○ *Secure Half Adder in a committed format*			
Mizuki-Asiedu-Sone [6]	2	8	1
○ *Secure Full Adder in a committed format*			
Mizuki-Asiedu-Sone [6]	2	10	1

Table 1: Known card-based protocols for secure computation.

The research area of card-based protocols along with other physically implemented cryptographic protocols (e.g. [1, 4, 10]) can aid professional cryptographers to intuitively explain to nonspecialists the nature of their constructed cryptographic protocols or what cryptography is in general. Some card-based protocols are implemented and used in online games [12].

The remainder of this paper is organized as follows. In Section 2, we give a general computational model of card-based protocols. In Section 3, based on our constructed model, we present a framework for copy protocols. In Section 4, we prove the impossibility of copying a face-down card with perfect secrecy. This paper is concluded in Section 5 with possible directions of future work.

2 Computational Model of Card-Based Protocols

In this section, we formally define a computational model which captures what can possibly be done in playing cards. Specifically, we define a deck, cards and sequences (on a table) in Section 2.1, consider operations (which can be applied to sequences) in Section 2.2, and give a formal definition of a protocol in Section 2.3.

As seen below, we introduce many terms and notations. However, we believe that such a long definition would be unavoidable when constructing a computation model that precisely captures a new concept (not formalized before).

2.1 A deck, cards and sequences

We refer to a non-empty finite multiset $\mathcal{D}$ with $\mathcal{D} \cap \{?\} = \emptyset$ as a *deck*, where '?' is the "back-side" symbol (as easily imagined). Any element $c \in \mathcal{D}$ in a deck $\mathcal{D}$ is called an *atomic card*. For instance, as seen in Section 1.1, Niemi-Renvall's copy protocol for $k = s = 2$ implicitly assumes a deck

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

consisting of 10 $\clubsuit$s and 10 $\heartsuit$s (where we use square brackets to represent a multiset), because in addition to the nine pairs of $\boxed{\clubsuit}\boxed{\heartsuit}$, another pair is necessary for producing an unknown face-down card

$$\underset{x}{\boxed{?}}$$

to be copied (recall the sequence (1)).

Next, we consider a card lying on the table. For a deck $\mathcal{D}$, an expression $\frac{c}{?}$ with $c \in \mathcal{D}$ is called a *face-up card* (of $\mathcal{D}$), and $\frac{?}{c}$ with $c \in \mathcal{D}$ is called a *face-down card* (of $\mathcal{D}$). For instance, in accordance with the expressions appearing before, a face-up card $\frac{\clubsuit}{?}$ means $\boxed{\clubsuit}$, and a face-down card $\frac{?}{\heartsuit}$ means

$$\underset{\heartsuit}{\boxed{?}}.$$

Hereafter, any face-up or face-down card α of $\mathcal{D}$ (i.e., $\alpha = \frac{c}{?}$ or $\alpha = \frac{?}{c}$ with $c \in \mathcal{D}$) is called a *lying card* (of $\mathcal{D}$). Given a lying card α of $\mathcal{D}$, we denote its atomic card by $\mathsf{atom}(\alpha)$, that is, we define $\mathsf{atom}(\alpha) \overset{\mathrm{def}}{=} c$ for a lying card $\alpha = \frac{c}{?}$ or $\alpha = \frac{?}{c}$. For instance, $\mathsf{atom}(\frac{\clubsuit}{?}) = \clubsuit$, and $\mathsf{atom}(\frac{?}{\heartsuit}) = \heartsuit$.

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 $d = |\mathcal{D}|$ (namely, d is the number of atomic cards in $\mathcal{D}$) is a *sequence* from $\mathcal{D}$ if

$[\,\mathsf{atom}(\alpha_1), \mathsf{atom}(\alpha_2), \ldots, \mathsf{atom}(\alpha_d)\,] = \mathcal{D}$. For instance, the initial "sequence" (1) seen in Section 1.1 can be expressed as a sequence from the above deck $\mathcal{D}^{\mathrm{ex}}$:

$$\Gamma^{\mathrm{ex1}} = \Big(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}\Big)$$

or

$$\Gamma^{\mathrm{ex2}} = \Big(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}, \frac{\clubsuit}{?}, \frac{\heartsuit}{?}\Big).$$

Note that the first two face-down cards (in both Γ^{ex1} and Γ^{ex2}) are intended to be utilized for producing an unknown face-down card

$$\underset{x}{\boxed{?}}$$

(to be copied); if we regard the second face-down card as the unknown one, then the sequence Γ^{ex1} corresponds to $x = \clubsuit$, and Γ^{ex2} corresponds to $x = \heartsuit$. Thus, in Niemi-Renvall's copy protocol, given Γ^{ex1} or Γ^{ex2}, it suffices to copy the second face-down card while ignoring the first one. (Throughout this paper, the sequences Γ^{ex1} and Γ^{ex2} together with the deck $\mathcal{D}^{\mathrm{ex}}$ and so on are used as a fixed example to illustrate our terminology and computational model.)

To employ later, we denote by $\mathsf{Seq}^{\mathcal{D}}$ the set of all (possible) sequences from a deck $\mathcal{D}$: we define

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

for a deck $\mathcal{D}$.

2.2 Operations

Given a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d) \in \mathsf{Seq}^{\mathcal{D}}$ from a deck $\mathcal{D}$ (on the table), we have three natural operations and one new operation, as described below.

2.2.1 Turning over

Define $\mathsf{swap}(\frac{c}{?}) \stackrel{\mathrm{def}}{=} \frac{?}{c}$ and $\mathsf{swap}(\frac{?}{c}) \stackrel{\mathrm{def}}{=} \frac{c}{?}$ for an atomic card c. To express the operation of turning over lying cards, we introduce an operation $\mathsf{turn}_T(\cdot)$ with a *turn set* $T \subseteq \{1, 2, \ldots, d\}$ for a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$:

$$\mathsf{turn}_T((\alpha_1, \alpha_2, \ldots, \alpha_d)) \stackrel{\mathrm{def}}{=} (\beta_1, \beta_2, \ldots, \beta_d)$$

such that

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

for every i, $1 \le i \le d$. Thus, every card whose position is in the turn set T is turned over by $\mathsf{turn}_T(\cdot)$.

For example, for the sequence Γ^{ex1} above,

$$\begin{aligned} &\mathsf{turn}_{\{3,4,\ldots,20\}}(\Gamma^{\mathrm{ex1}}) \\ &= \Big(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \frac{?}{\heartsuit}\Big). \end{aligned}$$

2.2.2 Rearrangement

One may sometimes want to change the order of a sequence. To this end, we introduce an operation $\mathsf{perm}_\pi(\cdot)$ based on a permutation $\pi \in S_d$ for a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$:

$$\mathsf{perm}_\pi((\alpha_1, \alpha_2, \ldots, \alpha_d)) \stackrel{\text{def}}{=} (\alpha_{\pi^{-1}(1)}, \alpha_{\pi^{-1}(2)}, \ldots, \alpha_{\pi^{-1}(d)})$$

where S_d denotes the symmetric group of degree d (throughout this paper).

2.2.3 Shuffling

Remember that Niemi-Renvall's copy protocol utilizes a random cut, which is a type of shuffle operation. All existing protocols listed in Table 1 also utilize some form of shuffle operation. Unquestionably, shuffling must be the most important operation for card-based cryptographic protocols. Here, we consider as general a treatment of shuffling as possible. Whereas the operations $\mathsf{turn}_T(\cdot)$ and $\mathsf{perm}_\pi(\cdot)$ are deterministic as seen above, the shuffle operation is randomized.

For a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$, we define an operation $\mathsf{shuf}_{\Pi,\mathcal{F}}(\cdot)$ with a *shuffle pair* $(\Pi, \mathcal{F})$ where $\Pi \subseteq S_d$ is called a *permutation-set* and $\mathcal{F}$ is a probability distribution on Π:

$$\mathsf{shuf}_{\Pi,\mathcal{F}}((\alpha_1, \alpha_2, \ldots, \alpha_d)) \stackrel{\text{def}}{=} \mathsf{perm}_\pi((\alpha_1, \alpha_2, \ldots, \alpha_d))$$

such that π is a permutation drawn from Π according to the probability distribution $\mathcal{F}$. Thus, $\mathsf{shuf}_{\Pi,\mathcal{F}}(\Gamma)$ probabilistically chooses a permutation π from the permutation-set Π according to the distribution $\mathcal{F}$, and applies it to the sequence Γ.

For example, let $\Pi^{\text{ex1}} = \{\pi_1, \pi_2, \ldots, \pi_6\}$ with

$$\begin{aligned}
\pi_1 &= (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20)\\
\pi_2 &= (1, 2, 8, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20)\\
&\ \vdots\\
\pi_6 &= (1, 2, 4, 5, 6, 7, 8, 3, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20),
\end{aligned}$$

and let $\mathcal{F}^{\text{ex1}}$ be such that

$$\Pr_{\mathcal{F}^{\text{ex1}}}(\pi_i) = 1/6$$

for every i, $1 \le i \le 6$. Then, $\mathsf{shuf}_{\Pi^{\text{ex1}},\mathcal{F}^{\text{ex1}}}(\Gamma)$ means a random cut to the stack consisting of the 3rd, 4th, 5th, 6th, 7th and 8th cards in the sequence $\Gamma = \mathsf{turn}_{\{3,4,\ldots,20\}}(\Gamma^{\text{ex1}})$ (as applied in Niemi-Renvall's copy protocol).

To use later, we present a notation for the set of all (possible) shuffle pairs under a deck $\mathcal{D}$ with $d = |\mathcal{D}|$:

$$\mathsf{SP}^d \stackrel{\text{def}}{=} \{(\Pi, \mathcal{F}) \mid \mathcal{F} \text{ is a probability distribution on } \Pi \in 2^{S_d}\}.$$

It should be noted that the rearrangement operation $\mathsf{perm}_\pi(\cdot)$ above can be expressed exactly as $\mathsf{shuf}_{\{\pi\},\mathcal{F}}(\cdot)$ such that $\Pr_{\mathcal{F}}(\pi) = 1$. Therefore, if preferable, one could exclude the operation $\mathsf{perm}_\pi(\cdot)$ from the model without loss of generality. Furthermore, note that any number of consecutive shuffle operations can be combined into a single shuffle operation; for example, let $(\Pi^{\text{ex2}}, \mathcal{F}^{\text{ex2}})$ be a shuffle pair corresponding to a random cut to the stack consisting of the 9th, 10th, 11th and 12th cards (as also applied in Niemi-Renvall's copy protocol), then $\mathsf{shuf}_{\Pi^{\mathrm{ex2}},\mathcal{F}^{\mathrm{ex2}}}(\mathsf{shuf}_{\Pi^{\mathrm{ex1}},\mathcal{F}^{\mathrm{ex1}}}(\cdot))$ can be expressed as $\mathsf{shuf}_{\Pi',\mathcal{F}'}(\cdot)$ such that

$$\Pi' = \{\sigma^2 \circ \sigma^1 \mid \sigma^1 \in \Pi^{\mathrm{ex1}},\ \sigma^2 \in \Pi^{\mathrm{ex2}}\}$$

and $\Pr_{\mathcal{F}'}(\pi) = 1/24$ for every $\pi \in \Pi'$. (On the other hand, removing rearrangement operations or combining shuffle operations might lead to a protocol that is not player-friendly.)

2.2.4 Random flip

As seen above, we obtained the shuffle operation $\mathsf{shuf}_{\Pi,\mathcal{F}}(\cdot)$ by adding randomization to the rearrangement operation $\mathsf{perm}_\pi(\cdot)$. Analogically, one may add randomization to the turn over operation $\mathsf{turn}_T(\cdot)$. For example, given a sequence, one might want to reveal a face-down card at a random position in the sequence.

For a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$, we define an operation $\mathsf{rflip}_{\Phi,\mathcal{G}}(\cdot)$ with a *flip-pair* $(\Phi, \mathcal{G})$ where $\mathcal{G}$ is a probability distribution on $\Phi \subseteq 2^{\{1,2,\ldots,d\}}$:

$$\mathsf{rflip}_{\Phi,\mathcal{G}}((\alpha_1, \alpha_2, \ldots, \alpha_d)) \overset{\mathrm{def}}{=} \mathsf{turn}_T((\alpha_1, \alpha_2, \ldots, \alpha_d))$$

such that T is a turn set drawn from Φ according to the probability distribution $\mathcal{G}$. We also define

$$\mathsf{FP}^d \overset{\mathrm{def}}{=} \{(\Phi, \mathcal{G}) \mid \mathcal{G} \text{ is a probability distribution on } \Phi \subseteq 2^{\{1,2,\ldots,d\}}\}.$$

A random flip operation has not been used in the construction of any of the existing protocols, and at present, its usefulness and potential power (and even the difficulty of its implementation) are unclear. However, we positively include this operation in our model because we desire as general a model as possible.

2.3 A protocol

In this subsection, we provide a formal definition of a "protocol." Roughly speaking, a protocol, which has a finite state control and a table, specifies an operation to be applied to a current sequence step by step, depending on its internal state and the view of looking down the sequence on the table. Our formalization of protocols is partially based on the ideas behind the Turing machine [14] with a random tape and Fischer-Wright's communication model [5].

2.3.1 Notations

Let $\mathcal{D}$ be a deck.

First of all, we have to consider the "input" to a protocol. For example, as seen before, Niemi-Renvall's copy protocol for $k = s = 2$ starts from the sequence Γ^{ex1} or Γ^{ex2} (illustrated in Section 2.1), and hence we can consider the set $\{\Gamma^{\mathrm{ex1}}, \Gamma^{\mathrm{ex2}}\}$ as an input. Thus, the *input set* U to a protocol is a set of sequences from $\mathcal{D}$, i.e., $U \subseteq \mathsf{Seq}^{\mathcal{D}}$.

Next, consider what one can look at on the table during the execution of a protocol. That is, the action of a protocol can depend on the view on the table. Therefore, we define the *visible sequence* $\mathsf{vis}(\Gamma)$ of a sequence $\Gamma = (\alpha_1, \alpha_2, \ldots, \alpha_d)$ as:

$$\mathsf{vis}((\alpha_1, \alpha_2, \ldots, \alpha_d)) \overset{\mathrm{def}}{=} (\mathsf{top}(\alpha_1), \mathsf{top}(\alpha_2), \ldots, \mathsf{top}(\alpha_d))$$

where $\mathsf{top}(\frac{c}{?}) \overset{\text{def}}{=} c$ and $\mathsf{top}(\frac{?}{c}) \overset{\text{def}}{=} ?$ for an atomic card c. For instance, for the above sequence Γ^{ex1},

$$\mathsf{vis}(\Gamma^{\mathrm{ex1}}) = (?, ?, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit, \clubsuit, \heartsuit).$$

Furthermore, we define the *visible sequence set* $\mathsf{Vis}^{\mathcal{D}}$ of $\mathcal{D}$ as:

$$\mathsf{Vis}^{\mathcal{D}} \overset{\text{def}}{=} \{\mathsf{vis}(\Gamma) \mid \Gamma \in \mathsf{Seq}^{\mathcal{D}}\};$$

recall that $\mathsf{Seq}^{\mathcal{D}}$ is the set of all sequences from $\mathcal{D}$.

The action of a protocol also depends on its state. The *state set* Q is a finite set of *states* having an *initial* state $q_0 \in Q$ and a *final* state $q_{\mathrm{f}} \in Q$.

Given a state $q \in Q - \{q_{\mathrm{f}}\}$ and a visible sequence $v \in \mathsf{Vis}^{\mathcal{D}}$, a protocol has to specify an operation, $\mathsf{turn}_T(\cdot)$, $\mathsf{perm}_\pi(\cdot)$, $\mathsf{shuf}_{\Pi,\mathcal{F}}(\cdot)$ or $\mathsf{rflip}_{\Phi,\mathcal{G}}(\cdot)$, to be performed at that step. This can be captured by a partial function, called an *action function*,

$$A : (Q - \{q_{\mathrm{f}}\}) \times \mathsf{Vis}^{\mathcal{D}} \to Q \times (2^{\{1,2,\dots,d\}} \cup S_d \cup \mathsf{SP}^d \cup \mathsf{FP}^d)$$

where $d = |\mathcal{D}|$. Recall that S_d is the symmetric group of degree d, and that SP^d and FP^d are the set of all shuffle pairs and the set of all flip-pairs, respectively; therefore, note that $2^{\{1,2,\dots,d\}}$, S_d, SP^d and FP^d are pairwise disjoint. The action function determines both the next state and the operation to be performed. That is, $A(q, v) = (q', T)$ with $q' \in Q$ and $T \in 2^{\{1,2,\dots,d\}}$ means that the state in the finite state control becomes q' and the sequence on the table becomes $\mathsf{turn}_T(\Gamma)$ where Γ is the current sequence and hence $v = \mathsf{vis}(\Gamma)$. Similarly, $A(q, v) = (q', \pi)$ with $\pi \in S_d$ means that the sequence turns into $\mathsf{perm}_\pi(\Gamma)$ from Γ, $A(q, v) = (q', (\Pi, \mathcal{F}))$ with $(\Pi, \mathcal{F}) \in \mathsf{SP}^d$ means that the sequence probabilistically becomes $\mathsf{shuf}_{\Pi,\mathcal{F}}(\Gamma)$, and $A(q, v) = (q', (\Phi, \mathcal{G}))$ with $(\Phi, \mathcal{G}) \in \mathsf{FP}^d$ means that the sequence probabilistically becomes $\mathsf{rflip}_{\Phi,\mathcal{G}}(\Gamma)$.

2.3.2 How to move

We are now ready to formally define a protocol. A *protocol* (having a *finite state control* and a *table* on which a single sequence is placed) is a quadruple $\mathcal{P} = (\mathcal{D}, U, Q, A)$ where

- $\mathcal{D}$ 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 $q_{\mathrm{f}} \in Q$;
- $A : (Q - \{q_{\mathrm{f}}\}) \times \mathsf{Vis}^{\mathcal{D}} \to Q \times (2^{\{1,2,\dots,|\mathcal{D}|\}} \cup S_{|\mathcal{D}|} \cup \mathsf{SP}^{|\mathcal{D}|} \cup \mathsf{FP}^{|\mathcal{D}|})$ is an action function.

A protocol $\mathcal{P} = (\mathcal{D}, U, Q, A)$ proceeds as expected: starting from the initial *instantaneous description* (q_0, Γ_0) for some input $\Gamma_0 \in U$, its instantaneous description, namely a pair of its current state and sequence on the table moves to another one according to the output of the action function A. When the state becomes the final state q_{f}, the protocol terminates. Note that when A outputs a shuffle pair $(\Pi, \mathcal{F})$ or a flip-pair $(\Phi, \mathcal{G})$, the move is randomized (unless $\Pr_{\mathcal{F}}(\pi) = 1$ for some $\pi \in \Pi$ or $\Pr_{\mathcal{G}}(T) = 1$ for some $T \in \Phi$). If the action function $A(q, \Gamma)$ for some instantaneous description (q, Γ) is undefined during the execution of the protocol, then the execution aborts. For an execution where the protocol $\mathcal{P}$ terminates, the enumeration $(\Gamma_0, \Gamma_1, \dots, \Gamma_t)$ of all sequences appearing on the table is called a *sequence-trace* (of $\mathcal{P}$), and such Γ_t is called a *final sequence*; similarly, such

$(\mathsf{vis}(\Gamma_0), \mathsf{vis}(\Gamma_1), ..., \mathsf{vis}(\Gamma_t))$ and $\mathsf{vis}(\Gamma_t)$ are called a *visible sequence-trace* and a *final visible sequence*, respectively.

Consider Niemi-Renvall's copy protocol for $k = s = 2$ (seen in Section 1.1) as an example to be specified by using our model: it can be formally described by a quadruple $(\mathcal{D}^{\rm ex}, \{\Gamma^{\rm ex1}, \Gamma^{\rm ex2}\}, \{q_0, q_1, q_2, q_3, q_4, q_5, q_{\rm f}\}, A^{\rm ex})$ such that

$$\begin{aligned}
A^{\rm ex}(q_0, \mathsf{vis}(\Gamma^{\rm ex1})) &= (q_1, \{3, 4, \ldots, 20\}) \\
A^{\rm ex}(q_1, (?, ?, \ldots, ?)) &= (q_2, (\Pi^{\rm ex1}, \mathcal{F}^{\rm ex1})) \\
A^{\rm ex}(q_2, (?, ?, \ldots, ?)) &= (q_3, (\Pi^{\rm ex2}, \mathcal{F}^{\rm ex2})) \\
A^{\rm ex}(q_3, (?, ?, \ldots, ?)) &= (q_4, (\Pi^{\rm ex3}, \mathcal{F}^{\rm ex3})) \\
A^{\rm ex}(q_4, (?, ?, \ldots, ?)) &= (q_5, (\Pi^{\rm ex4}, \mathcal{F}^{\rm ex4})) \\
A^{\rm ex}(q_5, (?, ?, \ldots, ?)) &= (q_{\rm f}, \{2, 3, 9, 11, 13, 15, 17, 19\})
\end{aligned}$$

where the shuffle pair $(\Pi^{\rm ex3}, \mathcal{F}^{\rm ex3})$ (which represents a random cut) can be defined similarly to $(\Pi^{\rm ex1}, \mathcal{F}^{\rm ex1})$ and $(\Pi^{\rm ex2}, \mathcal{F}^{\rm ex2})$,

$$\Pi^{\rm ex4} = \{\pi \in S_{20} \mid {}^{\forall} i \in \{1, 4, 5, 6, 7, 8, 10, 12, 14, 16, 18, 20\}\ \pi(i) = i\}$$

and $\Pr_{\mathcal{F}^{\rm ex4}}(\pi) = 1/8!$ for every $\pi \in \Pi^{\rm ex4}$. Note that $\mathsf{vis}(\Gamma^{\rm ex1}) = \mathsf{vis}(\Gamma^{\rm ex2})$, and that $(\Pi^{\rm ex4}, \mathcal{F}^{\rm ex4})$ represents a shuffle of the eight cards.

3 Framework for Copy Protocol

In the previous section, we have constructed a formal computational model of the card-based protocols. In this section, based on it, we deal with a framework for copying a face-down card, by using Niemi-Renvall's copy protocol

$$\mathcal{P}^{\rm NR} = (\mathcal{D}^{\rm ex}, \{\Gamma^{\rm ex1}, \Gamma^{\rm ex2}\}, \{q_0, q_1, q_2, q_3, q_4, q_5, q_{\rm f}\}, A^{\rm ex})$$

(specified above in Section 2.3) as an example. Note that the size of every sequence-trace $(\Gamma_0, \Gamma_1, ..., \Gamma_6)$ of $\mathcal{P}^{\rm NR}$ is equal to 7.

Before proceeding further, we define an "execution-trace" as follows. Remember that during an execution of a protocol $\mathcal{P}$, its current sequence Γ is changing from Γ into either (i) $\mathsf{turn}_T(\Gamma)$ for a turn set T or (ii) $\mathsf{perm}_\pi(\Gamma)$ for a permutation π; we call such T or π a *transformer*. Enumerating such transformers $\tau_i \in 2^{\{1,2,\ldots,d\}} \cup S_d$ together with the sequence-trace $(\Gamma_0, \Gamma_1, ..., \Gamma_t)$, we have the *execution-trace*

$$\big((\Gamma_0, \Gamma_1, ..., \Gamma_t), (\tau_1, \tau_2, ..., \tau_t)\big)$$

of the protocol $\mathcal{P}$.

3.1 Being a copy protocol

Consider the characteristics allowing the protocol $\mathcal{P}^{\rm NR}$ to make identical copies of a face-down card:

- it has a suitable input set;
- it always terminates with a sequence-trace of a finite size;

- every visible sequence-trace (more specifically, the number of $\clubsuit$s in the final visible sequence) determines the positions at which correct copies certainly reside;
- it does not touch the first lying card.

Carrying this observation further, we obtain the following definition without loss of generality.

Definition 1. *We say that a protocol $\mathcal{P} = (\mathcal{D}, \{\Gamma^{\clubsuit}, \Gamma^{\heartsuit}\}, Q, A)$* achieves making two copies *if*

- *the two sequences in the input set are*

$$\Gamma^{\clubsuit} = \left(\frac{?}{\heartsuit}, \frac{?}{\clubsuit}, \alpha_3, \alpha_4, \ldots, \alpha_{|\mathcal{D}|}\right)$$

  and

$$\Gamma^{\heartsuit} = \left(\frac{?}{\clubsuit}, \frac{?}{\heartsuit}, \alpha_3, \alpha_4, \ldots, \alpha_{|\mathcal{D}|}\right)$$

  for face-up cards $\alpha_3, \alpha_4, \ldots, \alpha_{|\mathcal{D}|}$;

- *it terminates with an execution-trace having a finite average number of sequences;*
- *there exist two functions*

$$f_1 : (\mathsf{Vis}^{\mathcal{D}})^* \to \{2, 3, \ldots, |\mathcal{D}|\}$$

  and

$$f_2 : (\mathsf{Vis}^{\mathcal{D}})^* \to \{2, 3, \ldots, |\mathcal{D}|\}$$

  such that, for every sequence-trace

$$(\Gamma_0, \Gamma_1, ..., (\beta_1, \beta_2, \ldots, \beta_{|\mathcal{D}|}))$$

  of $\mathcal{P}$ and its visible sequence-trace

$$\nu = (\mathsf{vis}(\Gamma_0), \mathsf{vis}(\Gamma_1), ..., \mathsf{vis}((\beta_1, \beta_2, \ldots, \beta_{|\mathcal{D}|}))),$$

  $f_1(\nu) \neq f_2(\nu)$ and

$$\beta_{f_1(\nu)} = \beta_{f_2(\nu)} = \begin{cases} \frac{?}{\clubsuit} & \text{if } \Gamma_0 = \Gamma^{\clubsuit} \\ \frac{?}{\heartsuit} & \text{if } \Gamma_0 = \Gamma^{\heartsuit}, \end{cases}$$

  where

$$(\mathsf{Vis}^{\mathcal{D}})^* = \bigcup_{i \geq 1} (\mathsf{Vis}^{\mathcal{D}})^i.$$

- *the action function A does nothing against the first lying card, i.e., each transformer in every execution-trace of $\mathcal{P}$ is either a turn set T with $1 \notin T$ or a permutation π with $\pi(1) = 1$.*

Note that, as implied by the second item in Definition 1, we admit a copy protocol to be a *Las Vegas algorithm*. (Actually, as seen in the last column of Table 1, some existing protocols are Las Vegas algorithms.)

The protocol $\mathcal{P}^{\mathrm{NR}}$ satisfies all of the conditions in Definition 1, of course: in regard to the third condition, it suffices to set

$$f_1(\nu) = 5,\ f_2(\nu) = 7$$

for any visible sequence-trace ν whose final visible sequence has an even number of $\clubsuit$s, and

$$f_1(\nu) = 6,\ f_2(\nu) = 8$$

for any ν whose final visible sequence has an odd number of $\clubsuit$s.

3.2 Security

We next consider the security. To make an information-theoretical argument, we need to define two random variables (as below); to this end, it is necessary to take a probability distribution on the input set U into account.

Given a protocol $\mathcal{P} = (\mathcal{D}, U, Q, A)$, a probability distribution $\mathcal{M}$ on U is called an *input distribution* for $\mathcal{P}$. A protocol $\mathcal{P}$ together with an input distribution $\mathcal{M}$ for it specifies the entire world; we call such a pair $(\mathcal{M}, \mathcal{P})$ a *system* (following the terminology in Fischer-Wright's communication model [5]).

Let $\mathcal{P} = (\mathcal{D}, \{\Gamma^{\clubsuit}, \Gamma^{\heartsuit}\}, Q, A)$ be a protocol achieving making two copies, and let $\mathcal{M}$ be an input distribution for $\mathcal{P}$. Then, the system $(\mathcal{M}, \mathcal{P})$ induces a probability distribution on the input set $\{\Gamma^{\clubsuit}, \Gamma^{\heartsuit}\}$, of course. Therefore, we can characterize the secret color of the unknown faced-down card (to be copied) by a random variable $X^{(\mathcal{M},\mathcal{P})}$ (whose superscript is omitted if it is clear from context); $X = \clubsuit$ means that the secret color is $\clubsuit$, and $X = \heartsuit$ means that it is $\heartsuit$. Similarly, we use a random variable $V^{(\mathcal{M},\mathcal{P})}$ (whose superscript is also omitted if it is clear from context) to express the visible sequence-trace; $V = (v_0, v_1, \ldots, v_t)$ means that we have seen each visible sequence v_i, $0 \leq i \leq t$, on the table in this order. Note that the randomization comes from not only the input distribution $\mathcal{M}$ but also the randomized operations $\mathsf{shuf}_{\Pi,\mathcal{F}}(\cdot)$ and $\mathsf{rflip}_{\Phi,\mathcal{G}}(\cdot)$ output by the action function A.

The two random variables X and V are sufficient for evaluating the security. Take the protocol $\mathcal{P}^{\mathrm{NR}}$ as an example. (Remember that $\mathcal{P}^{\mathrm{NR}}$ fails to securely copy with probability 1/8 as mentioned in Section 1.1.) Using random variables X and V along with the (Shannon) entropy $H(\cdot)$ and the conditional entropy $H(\cdot|\cdot)$, we can information-theoretically write that

- $H(X|V = \nu) = H(X)$ and $\Pr[V = \nu] = 7/8$ for any visible sequence-trace $\nu = (v_0, v_1, \ldots, v_6)$ such that the final visible sequence v_6 contains at least one $\clubsuit$ and at least one $\heartsuit$;

- $H(X|V = \nu) = 0$ and $\Pr[V = \nu] = 1/8$ for any $\nu = (v_0, v_1, \ldots, v_6)$ such that v_6 contains only cards of a single color.

4 Impossibility of Perfectly Secure Copy

In this section, we prove that there does not exist a protocol that achieves making two copies with perfect secrecy.

We first formally define perfectly secure copy protocols.

Definition 2. *We say that a protocol $\mathcal{P}$* achieves making two copies with perfect secrecy *if it achieves making two copies, and moreover,*

$$H(X^{(\mathcal{M},\mathcal{P})}|V^{(\mathcal{M},\mathcal{P})}) = H(X^{(\mathcal{M},\mathcal{P})})$$

holds for any system $(\mathcal{M},\mathcal{P})$.

We next prove that such a protocol does not exist. Roughly speaking, the idea behind our proof is based on a simple fact: when the unknown card (to be copied) is possibly turned over, its entropy must decrease.

Take a system $(\mathcal{M},\mathcal{P}^{\mathrm{NR}})$ of the protocol $\mathcal{P}^{\mathrm{NR}}$ with $\Pr[X=\clubsuit]>0$ and $\Pr[X=\heartsuit]>0$ as an example. Consider when the eight cards are revealed in the final step, i.e., when the operation

$$\mathsf{turn}_{\{2,3,9,11,13,15,17,19\}}(\Gamma_5)$$

is applied, where $(\Gamma_0,\Gamma_1,...,\Gamma_5,\Gamma_6)$ will be the sequence-trace. For convenience, we virtually split the turn over operation into $\mathsf{turn}_{\{2\}}(\Gamma_5)$ and

$$\mathsf{turn}_{\{3,9,11,13,15,17,19\}}(\Gamma_{5.5}),$$

that is, we focus on the case when the second (face-down) card has just been turned over. Assume that the revealed (face-up) card is $\frac{\clubsuit}{?}$. Then, the probability that the second card revealed now has come from the unknown card (to be copied) is exactly 1/8, and hence

$$\begin{aligned}\Pr[X=\clubsuit\,|\,\mathcal{E}] &= \frac{(1/8)\cdot\Pr[X=\clubsuit]+(7/8)\cdot\Pr[X=\clubsuit]\cdot(1/2)}{(1/8)\cdot\Pr[X=\clubsuit]+(7/8)\cdot(1/2)}\\ &= \frac{9\Pr[X=\clubsuit]}{2\Pr[X=\clubsuit]+7} \;>\; \Pr[X=\clubsuit]\end{aligned}$$

where $\mathcal{E}$ is such an event. Therefore, the entropy must decrease (as formally shown below in Lemma 1). Note that $\mathcal{E}$ is an "intermediate" event; subsequently, the remaining seven cards are turned over, i.e., $\mathsf{turn}_{\{3,9,11,13,15,17,19\}}(\Gamma_{5.5})$ is applied, and the protocol terminates with a visible sequence-trace ν such that $H(X|V=\nu)=H(X)$ or $H(X|V=\nu)=0$ (as described in the previous section), and hence we have $H(X^{(\mathcal{M},\mathcal{P}^{\mathrm{NR}})}|V^{(\mathcal{M},\mathcal{P}^{\mathrm{NR}})}) < H(X^{(\mathcal{M},\mathcal{P}^{\mathrm{NR}})})$.

For a random variable Z, we denote by $Z^{-1}(z)$ the (maximal) event resulting in $Z=z$. We say that an event $\mathcal{E}$ *respects* a random variable Z if either $Z^{-1}(z)\subseteq\mathcal{E}$ or $Z^{-1}(z)\cap\mathcal{E}=\emptyset$ for any z [5]. We have the following lemma.

Lemma 1. *Let Y,Z be random variables, and let $\mathcal{E}$ be an event respecting Z. If $\Pr[Y=y\,|\,\mathcal{E}]\neq\Pr[Y=y]$ for some y, then $H(Y|Z)<H(Y)$.*

Proof. Assume that $\Pr[Y=y\,|\,\mathcal{E}]\neq\Pr[Y=y]$ for some y, and suppose for a contradiction that $H(Y|Z)=H(Y)$. Then, Y and Z are independent, and hence $\Pr[Y=y,Z=z]=\Pr[Y=y]\Pr[Z=z]$ for any z. Since $\mathcal{E}$ respects Z, there exists η such that $\{Z^{-1}(z)\mid z\in\eta\}$ partitions $\mathcal{E}$. Thus,

$$\Pr[Y=y\,|\,\mathcal{E}]=\frac{\Pr[Y=y,\mathcal{E}]}{\Pr[\mathcal{E}]}=\frac{\sum_{z\in\eta}\Pr[Y=y,Z=z]}{\sum_{z\in\eta}\Pr[Z=z]}=\Pr[Y=y],$$

which contradicts $\Pr[Y=y\,|\,\mathcal{E}]\neq\Pr[Y=y]$. □

We are now ready to prove our theorem.

Theorem 1. *There exists no protocol that achieves making two copies with perfect secrecy.*

Proof. Let $(\mathcal{M}, \mathcal{P})$ be a system of a protocol $\mathcal{P} = (\mathcal{D}, \{\Gamma^{\clubsuit}, \Gamma^{\heartsuit}\}, Q, A)$ achieving making two copies, such that $\Pr[X = \clubsuit] > 0$ and $\Pr[X = \heartsuit] > 0$. Choose (and fix) an arbitrary execution-trace of $\mathcal{P}$ whose sequence-trace $(\Gamma_0, \Gamma_1, ..., \Gamma_t)$ satisfies $\Gamma_0 = \Gamma^{\clubsuit}$. For every sequence Γ_i, we denote by pos^i the position of the unknown card (which is the second lying card $\frac{?}{\clubsuit}$ in the initial sequence $\Gamma_0 = \Gamma^{\clubsuit}$). That is, we set $\mathsf{pos}^0 = 2$, and for every i, $1 \le i \le t$, recursively define $\mathsf{pos}^i = \pi(\mathsf{pos}^{i-1})$ if the i-th transformer is a permutation π; and $\mathsf{pos}^i = \mathsf{pos}^{i-1}$ otherwise.

Suppose that every i-th transformer which is a turn set T satisfies $\mathsf{pos}^{i-1} \notin T$, i.e., the unknown card has never been turned over. Then, if we started the protocol $\mathcal{P}$ from the other sequence $\Gamma^{\heartsuit}$ (contained in the input set) instead of $\Gamma^{\clubsuit}$, we would necessarily have a case where the resulting sequence-trace would be $(\Gamma^{\heartsuit}, \Gamma_1, ..., \Gamma_t)$. Since their visible sequence-traces are the same, namely

$$(\mathsf{vis}(\Gamma^{\clubsuit}), \mathsf{vis}(\Gamma_1), \ldots, \mathsf{vis}(\Gamma_t)) = (\mathsf{vis}(\Gamma^{\heartsuit}), \mathsf{vis}(\Gamma_1), \ldots, \mathsf{vis}(\Gamma_t)),$$

we could not determine where desired identical copies are, a contradiction. Hence, there must exist an i-th transformer which is a turn set T such that $\mathsf{pos}^{i-1} \in T$.

Focus on the case where such a transformer, namely a turn set T, first appears, and assume that such T appears as the ℓ-th transformer. Hence, $\mathsf{turn}_T(\Gamma_{\ell-1}) = \Gamma_\ell$. Without loss of generality, one may assume that T is a singleton set, i.e., $T = \{k\}$ for some k. Then, the k-th lying card in $\Gamma_{\ell-1}$ is $\frac{?}{\clubsuit}$, and that in Γ_ℓ is $\frac{\clubsuit}{?}$. We now consider an event, denoted by $\mathcal{E}$, in which the first $(\ell+1)$ visible sequences are the same as $\mathsf{vis}(\Gamma^{\clubsuit}), \mathsf{vis}(\Gamma_1), \ldots, \mathsf{vis}(\Gamma_\ell)$. Note that the event $\mathcal{E}$ respects the random variable V (expressing visible sequence-traces). Also, denote by $\mathcal{E}^-$ the event that the first ℓ visible sequences are $\mathsf{vis}(\Gamma^{\clubsuit}), \mathsf{vis}(\Gamma_1), \ldots, \mathsf{vis}(\Gamma_{\ell-1})$. Within the event $\mathcal{E}^-$, we consider two events $\mathsf{Pos} \subseteq \mathcal{E}^-$ and $\mathcal{O}^{\clubsuit} \subseteq (\mathcal{E}^- - \mathsf{Pos})$: Pos represents that "the k-th lying card in the ℓ-th sequence (counting from 1) is the unknown card," and $\mathcal{O}^{\clubsuit}$ represents that "it comes from other cards and is $\frac{?}{\clubsuit}$." Then, we have

$$\begin{aligned}\Pr[X = \clubsuit \,|\, \mathcal{E}] &= \frac{\Pr[\mathsf{Pos}]\Pr[X = \clubsuit] + (1 - \Pr[\mathsf{Pos}])\Pr[X = \clubsuit]\Pr[\mathcal{O}^{\clubsuit}]}{\Pr[\mathsf{Pos}]\Pr[X = \clubsuit] + (1 - \Pr[\mathsf{Pos}])\Pr[\mathcal{O}^{\clubsuit}]} \\ &> \Pr[X = \clubsuit].\end{aligned}$$

Note that the inequality holds even when $\Pr[\mathcal{O}^{\clubsuit}] = 0$. Hence, by Lemma 1 we have $H(X|V) < H(X)$. □

5 Conclusion

In this paper, we constructed a rigorous mathematical model of card-based cryptographic protocols. Based on this general computational model, we showed that it is impossible to make identical copies of a face-down card with perfect secrecy.

Since our constructed computational model is rather general, we believe that it can be used to find another impossibility result, or to show the optimality of a certain protocol. For example, as listed in Table 1, six cards are sufficient for securely computing AND in a committed format [8], and it is open to answer the question whether there exists a "committed format" AND protocol that requires fewer than six cards. We hope that our computational model can provide unambiguous answers to such questions in the future.

The model is also expected to enable us to discuss the "time complexity" and "shuffle complexity" of protocols more precisely.

As seen, the cards considered in our model (as well as in previous works [2, 3, 6, 7, 8, 9, 11, 13]) have no "polarity," that is, we never put them upside down like $\boxed{\clubsuit}\boxed{\rotatebox{180}{$\heartsuit$}}\boxed{\heartsuit}\boxed{\rotatebox{180}{$\clubsuit$}}$. Introducing polarity or rotation of a card might be one intriguing direction of future works.

Acknowledgments

This work was supported by JSPS KAKENHI Grant Number 23700007.

References

[1] J. Balogh, J. A. Csirik, Y. Ishai, and E. Kushilevitz, "Private computation using a PEZ dispenser," Theoretical Computer Science, vol. 306, pp. 69–84, 2003.

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

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

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

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

[6] T. Mizuki, I. K. Asiedu, and H. Sone, "Voting with a logarithmic number of cards," Proc. UCNC 2013, Lecture Notes in Computer Science, Springer-Verlag, vol. 7956, pp. 162–173, 2013.

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

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

[9] T. Mizuki, F. Uchiike, and H. Sone, "Securely computing XOR with 10 cards," Australasian Journal of Combinatorics, vol. 36, pp.279-293, 2006.

[10] T. Moran and M. Naor, "Polling with physical envelopes: a rigorous analysis of a human-centric protocol," Proc. EUROCRYPT 2006, Lecture Notes in Computer Science, vol. 4004, pp. 88–108, Springer-Verlag, 2006.

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

[12] H. Stamer, “Efficient electronic gambling: an extended implementation of the toolbox for mental card games,” Proc. Western European Workshop on Research in Cryptology (WEWoRC 2005), Lecture Notes in Informatics, vol. P-74, pp. 1–12, 2005.

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

[14] A. M. Turing, “On computable numbers with an application to the Entscheidungsproblem,” Proc. London Math. Soc., vol. 42, pp. 230–265, 1936.