Journal of Information Processing Vol.33 276–283 (Apr. 2025)

[DOI: 10.2197/ipsjjip.33.276]

Recommended Paper

Card Protocols that Allow You to Switch Cards to Mahjong Tiles

Yuji Suga[1,a)]

Received: July 10, 2024, Accepted: January 10, 2025

Abstract: Card-based cryptographic protocols are useful for performing secure computations using physical cards instead of digital systems and are well-suited for educational purposes, especially for those new to studying multi-party computation (MPC). In this paper, we investigate using cards (such as business cards or mahjong tiles) with the same design on the back, but the front sides can face different directions. These cards are defined as those whose backs are indistinguishable and whose fronts can be differentiated based on the top and bottom. Mahjong tiles, painted the same color on the back, cannot be differentiated from the back even when swapped. Thus, tiles whose fronts show different designs when swapped can be used as top and bottom cards. Here, we examine the practical feasibility of implementing such protocols, focusing on whether the shuffle is practical. We present a realistic method to determine if protocols using up-down cards can be implemented by replacing cards with mahjong tiles. Additionally, we introduce the construction of a new protocol specifically for shuffling mahjong tiles. This study aims to provide a practical approach to utilizing up-down cards in secure and efficient card protocols, demonstrating their versatility and applicability in real-world scenarios.

Keywords: card-based protocols, non-committed protocols, random cut, m-deck partitioning method, association schemes

1. The Problem We Originally Wanted to Solve

Mahjong is a table game played by four (or three) players, each aiming to score as many points as possible. The initial state consists of 13 tiles, and in each phase, the player repeatedly takes one tile and discards one tile until finally reaching a state of 14 tiles, called a "ron" or "self-draw," where the player scores points from the other players. The 14-tile sequences have various roles, each with different scores depending on the difficulty and elegance of the game. There are 34 different suits of mahjong tiles: nine myriad suit tiles, nine circle suit tiles, nine bamboo suit tiles, and seven honor tiles, each with four tiles. The motivation of this paper is to investigate whether it is possible to implement a normal card protocol using these mahjong tiles or to construct a protocol unique to mahjong tiles.

Mahjong is known as an unproductive game, where a game can take up to an hour, and the winning player gets the honors. There are also potential problems, such as the difficulty of gathering players, as four players are tied up for a long time. When there is a shortage of players, many of those who are recruited are beginners, newcomers, young players, junior players, and other less experienced players. This situation creates issues such as not being able to refuse invitations from superiors and not being able to leave the game midway. Under these circumstances, the decision to start another game (and whether to start another one-hour game) is often left to the higher-ranked player, and many junior and subordinate players may have experienced that they cannot refuse face-to-face.

In this paper, we consider a situation where players are asked to choose whether or not to continue one more game by voting. We propose a protocol that outputs only whether the players' opinions are in agreement, while keeping the input of who wants to continue the game (i.e., YES or NO) secret. If the input is made with mahjong tiles and the output can be obtained by the positional relationship of the tiles, while keeping all information about the input secret, the above problem can be solved. This is because the information about the input is kept secret and the input (e.g., the will to go home) can be made easily. The following is an example of the use of a mahjong game.

In fact, it is known that in three-player mahjong (a game system where the number of players is limited to three and the mahjong tiles used are restricted), the three-party equality function can be realized as Six-Card Trick [3] in the normal card protocol. This method appears to be implementable by using two different suits of mahjong tiles, the white dragon ("white") and the red dragon ("auspicious"). However, Six-Card Trick uses random cuts, which is one of the simplest shuffling methods for cards. Mahjong tiles are physically quite thick, making it very difficult to shuffle six tiles vertically on top of each other like cards. The first contribution of this paper is the study of how to implement this random cut on mahjong tiles.

[1] Internet Initiative Japan Inc., Chiyoda, Tokyo 102–0071, Japan
[a)] suga@iij.ad.jp

The preliminary version of this paper was published at Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOMO2023), July 2023, and the program chair recommended the paper for publication in the Journal of Information Processing (JIP).

On the other hand, in standard four-player mahjong, eight tiles of two different suits are used, and only random cuts are applied for the four-party equality function. It has already been shown that a four-party protocol does not exist for this function, this negative result implying that it cannot constitute a feasible protocol [3]. However, since four-player mahjong is the mainstream, the final research task is to implement this four-player equality function using mahjong tiles.

The next and subsequent chapters are structured as follows. Throughout this paper, we deal with non-committed card protocols among card-based protocols. The output is committed, meaning that the result obtained when the protocol stops is based on the encoding rules of the input. It has the advantage that subprotocols can be concatenated to form a new card protocol. On the other hand, when card protocols are non-committed, the results are obtained by disclosing the cards that were used when the protocol was stopped.

Section 2 describes the implementation of the shuffling method most commonly used in non-committed card protocols, called random cut, on mahjong tiles. Next, Section 3 deals with top-bottom shuffling, which transposes the top and bottom tiles when tiles with the property of being top-bottom tiles are used. We report the results of a study on the application of the card deck partitioning method to mahjong tiles, in which the surfaces of two tiles are joined and fastened with rubber bands, etc., and three types of shuffling are easily performed by throwing several decks (two-tile bundles).

While the previous chapters have applied existing shuffling methods to ordinary cards, Section 4 deals with the Tornado shuffle, a shuffling method unique to mahjong tiles. This paper proposes a new shuffling protocol based on the assumption that the mahjong tiles are physically attached to each other and the deck is tossed as in the card deck partitioning method. We propose a new protocol for the case where the tiles are physically attached and the deck is thrown as in the card deck partitioning method. We show that this method is simpler than the card deck partitioning method, and more specifically, that it is possible to realize a mahjong tile input version of the card protocol that allows a single value of the 4-step Likert scale to be input. Finally, future research directions and open problems are introduced.

2. Application to Random-cut based Protocols

2.1 Original Five-Card Trick with 2-color Cards

The Five-Card trick [2], known as a two-user non-committed card protocol, uses two types of cards: heart $\boxed{\heartsuit}$ and club $\boxed{\clubsuit}$ with reverse side indistinguishability. It is a method of obtaining AND outputs (specifically, operations that reveal hidden cards) while keeping the input values secret by performing random cuts to identify some initial cases immediately after card input. In card-based cryptographic protocols, an encoding rule is a predefined method used to associate specific card orientations or positions with binary values or other symbols. This rule allows each card to represent a unique piece of information, enabling secure computations to be performed without revealing the card's true value until necessary. In general committed card-based protocols, the output follows a format based on the encoding rules of the input, a one-bit input by the user follows the following general encoding rules: $\boxed{\clubsuit}\boxed{\heartsuit} = 0$, $\boxed{\heartsuit}\boxed{\clubsuit} = 1$.

Table 1 Initial input state of the Five-Card trick.

(a, b)	sequence
(0,0)	♡ ♣ ♡ ♣ ♡
(0,1)	♡ ♣ ♡ ♡ ♣
(1,0)	♣ ♡ ♡ ♣ ♡
(1,1)	♣ ♡ ♡ ♡ ♣

When the two inputs are a and b, where $a, b \in \{0, 1\}$ and $\overline{a}$ means the negation of a:

$\boxed{?}\boxed{?}\ (=\overline{a})\ \boxed{\heartsuit}\quad \boxed{?}\boxed{?}\ (=b).$

The five cards are arranged in a row with the center card facing down, and then cut randomly using circular substitution. The circular substitution selects one of the following five operations with equal probability: the identity operation (id), or the 4 operations c_5, c_5^2, c_5^3, c_5^4 (where the circular substitution is c_5) that permute the cards in the bundle. Here $\boxed{?}$ denotes the reverse-side-up position.

Before the random cut, the center card $\boxed{\heartsuit}$ should be turned over to the reverse-side-up position, and all five cards should be shuffled face-down. The initial state of the five cards is shown in **Table 1**. Since the cards are shuffled using cyclic substitution, $a \wedge b = 1$ only when three $\boxed{\heartsuit}$ cards appear in a row out of five cards. In addition, all three cases where $a \wedge b = 0$ are considered identical, so the input values of a and b cannot be determined from the output alone, this feature is a crucial aspect of the protocol.

2.2 Our Entity Model and the Partial Disclosure Technique

We present a method in which only the players get results by using "blind tiles" (a method of identifying the reverse side of a tile by touching it without disclosing the reverse side), which is one of the features of mahjong tiles. Before that, the entity model of the protocol participants is organized.

Submitters Entities that are so-called protocol participants and that perform input by cards.

Observers Entities that do not make inputs, but can check that the protocol is working correctly by observing the protocol on the sidelines.

Gainers Entities that obtain results at the time of final disclosure; Submitters are separated from Submitters and Observers because there are cases where it is not always necessary to know the results. On the other hand, in normal protocols, results can be obtained for both Submitters and Observers.

In this model, the processing is divided into three phases as follows: (1) Submitters enter a deck in a flat space by placing cards according to a defined procedure. (2) One of the Submitters or Gainers manipulates the cards according to the procedure. The Observers can check whether the procedure is correct or not, as the card manipulation is done in a flat space. (3) Finally, the Gainers disclose the cards to the surface to obtain the result of the protocol.

In the disclosure phase (3), the Gainers disclose the cards to

Table 2 Initial states on the Six-Card trick protocol.

(a,b,c)	sequence
(0,0,0)	♣ ♡ ♣ ♡ ♣ ♡
(0,0,1)	♣ ♡ ♣ ♡ ♡ ♣
(0,1,0)	♣ ♡ ♡ ♣ ♣ ♡
(0,1,1)	♣ ♡ ♡ ♣ ♡ ♣
(1,0,0)	♡ ♣ ♣ ♡ ♣ ♡
(1,0,1)	♡ ♣ ♣ ♡ ♡ ♣
(1,1,0)	♡ ♣ ♡ ♣ ♣ ♡
(1,1,1)	♡ ♣ ♡ ♣ ♡ ♣

Table 3 all possibilities after **STEP-2**.

(a,b,c)	sequence
(0,0,0)	♣ ♡ ♣ ♡ ♣ ♡
(0,0,1)	♣ ♣ ♣ ♡ ♡ ♡
(0,1,0)	♣ ♡ ♡ ♡ ♣ ♣
(0,1,1)	♣ ♣ ♡ ♡ ♡ ♣
(1,0,0)	♡ ♡ ♣ ♣ ♣ ♡
(1,0,1)	♡ ♣ ♣ ♣ ♡ ♡
(1,1,0)	♡ ♡ ♡ ♣ ♣ ♣
(1,1,1)	♡ ♣ ♡ ♣ ♡ ♣

the surface to obtain the results, but if the user is lazy, this task can be tedious. Therefore, this paper focuses on whether it is possible to obtain results with as few cards as possible, i.e., with less disclosure work.

In phase (2) above, the cards are sorted in bunches, and operations such as random shuffling and random bisection cuts are performed. Afterwards, card disclosure is performed to check the front-back relationship of the replaced cards, but it is simpler to perform a 'spread', which is an operation in which a bunch of cards is turned out and spread neatly horizontally as a magician handles. However, it is undesirable to do this, as it appears to the Observers as if something has been manipulated.

2.3 Six-Card Trick

Next, we deal with the Six-Card Trick [3] presented by Shinagawa et al. at ICISC 2018. The Six-Card Trick is a 6-card 3-party non-committed card protocol with a 3-input equality function of the three inputs. An equivalence function is a function that determines whether all of the inputs are the same or not, and in the case of three inputs $a, b, c \in \{0, 1\}$, returns True only if $a = b = c = 0$ or $a = b = c = 1$, and outputs False otherwise.

The Six-Card Trick consists of the following steps.

STEP-1 For the 3-user input a, b, c, let the card input be the following.

$\boxed{?}\boxed{?}\ (=a)\ \boxed{?}\boxed{?}\ (=b)\ \boxed{?}\boxed{?}\ (=c)$

STEP-2 Apply the following permutation to the 6 cards.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 3 & 6 & 5 & 2 \end{pmatrix}$$

STEP-3 Random cut permutation is performed for the 6 cards.

STEP-4 If 6 cards are turned over and three $\boxed{\heartsuit}$ are in a sequence, the output is 0, otherwise it is 1. That is, if $a = b = c$, the output is 1.

Table 2 shows the pattern of input initial conditions in **STEP-1**.

Table 3 shows all patterns for the states after **STEP-2** and It can be seen that only when $a = b = c = 0$ or $a = b = c = 1$ are three consecutive $\boxed{\heartsuit}$ not lined up.

The random cut process shows that both the case $(a, b, c) = (0, 0, 0)$ and the case $= (1, 1, 1)$ have the same arrangement. This indicates that when observing this protocol from Observers, even if the result is True, only the result of the equivalence function can be observed, and no information about each user's input is leaked.

Note that the information shared by Submitters and Observers is different.

2.4 Applying Partial Disclosure Techniques to The Six-Card Trick

Partial disclosure techniques are used, for example, in the Six-Card Trick, where only some of the cards are disclosed so that it is not necessary to turn the whole card face down, as shown below: Only cards 1, 3, and 5 from the left of the six cards are turned over; if all three cards are of the same suit, the output is 1 (i.e., $a = b = c$), otherwise 0.

A major effect of partial disclosure is to prevent the results from being known to the Observers. The non-committed card protocols introduced earlier disclose all the cards used when obtaining the final result. Observers can therefore not only check that the protocol is working correctly but also know the final result. This feature is considered to be disadvantageous in some cases for Submitters, depending on the application. Therefore, it is clear that it is more reasonable for Gainers to check not all cards, but a smaller number of cards, so that the state of the cards is not visible to Observers.

Furthermore, although we have so far discussed only cards, a convenient alternative for handling the face of a backed card without the Observers knowing about it is the mahjong tile. In the actual game of Mahjong, mahjong tiles placed in a flat space are hidden, and it is necessary to obtain the mahjong tiles so that only you can see them, preventing other players from seeing their surfaces. Mahjong tiles are also considered more suitable than cards, given the above requirements, as a skilled player can identify the tile without looking at the surface by simply grasping it.

Table 4 lists the differences in the amount of information an entity can obtain between the existing and proposed methods from the above perspective.

2.5 Concrete Implementation on Random-cut Mahjong Tiles

Consider the use of a circular lid with a diameter of 9.0 cm as shown in **Fig. 1** (a). This is the lid of a container for storing foodstuffs such as seaweed and bolos sweets, which are readily available in Japan from ordinary supermarkets.

As with general card protocols, the mahjong tiles entered on the back must be randomly shifted. As with card input, the six mahjong tiles arranged horizontally are rearranged in a circle. The choice of the size of the lid is important, as the six mahjong

Table 4 Differences in the amount of information available to each entity.

Schemes	Submitters	Observers	Submitters & Gainers
Five-Card Trick	Only own input a	$a \wedge b$	$a \wedge b$
Six-Card Trick	Only own input a	Whether $a = b = c$	Whether $a = b = c$ If $a = b = c$ then fixed 0 or 1
partial disclosure Five-Card Trick	Only own input a	None	$a \wedge b$
partial disclosure Six-Card Trick	Only own input a	None	Whether $a = b = c$ If $a = b = c$ then fixed 0 or 1

(a) (b) (c)

Fig. 1 Concrete implementation on random-cut mahjong tiles.

tiles must be arranged in a circle right at the "edge" of the lid, with evenly spaced tiles with a small gap between them. At this time, any empty spaces in the central area are filled with dummy mahjong tiles. In experiments, it was found that by placing two dummy mahjong tiles, the order of the mahjong tiles could be rotated without being changed. Note that in the Six-Card Trick, it is not a problem if the mahjong tiles are flipped upside down.

As shown in Fig. 1 (b), in our proposed card protocol, mahjong tiles arranged in a row are arranged in a circle and covered with a lid, and then the lid is rotated as shown in Fig. 1 (c) to achieve the same effect as a random cut. Here, rather than just rotating the lid, you need to be aware of the weight of the mahjong tiles in your hands and make sure the mahjong tiles inside the lid rotate. Specifically, move the lid in parallel in a circle.

Although there were only four experimental subjects, it is considered to be an effective implementation method, as no errors, such as the mahjong tiles moving back and forth, occurred during the 20 random cuts performed on subjects of different genders and age groups.

3. Application to Protocols based on the Card Deck Partitioning Method

Next, consider the use of cards (e.g., business cards or mahjong tiles) with exactly the same picture on both the front and reverse sides. The advantages and disadvantages of making use of the top-bottom relationship of the picture patterns are discussed in the document [1]. In this case, the differences in the vertical placement of the cards can be used to map each card to a different suit (as used in common card protocols). In other words, we can equate $\boxed{\downarrow}$ with $\boxed{\clubsuit}$ and $\boxed{\uparrow}$ with $\boxed{\heartsuit}$. One advantage of this is that it is possible to construct a protocol using the same set of cards, without having to write notes on the cards expressing the suits. In this paper, cards with indistinguishable backs and faces that can be represented by $\boxed{\uparrow}$ and $\boxed{\downarrow}$ will be referred to as up-down cards. Mahjong tiles satisfy this requirement because they are painted in the same color.

Top and bottom cards are characterized by the fact that by shuffling the top and bottom of the card, $\boxed{\uparrow}$ and $\boxed{\downarrow}$ are interchanged. Top-bottom shuffling is the random application of such transpositions to a bunch of cards that are physically stacked on top of each other, and refers to a process that outputs either the initial state or one of two states: all cards are transposed top and bottom.

Also in this section, we do not consider the continuity of protocols, but deal with non-committed card protocols, in which a protocol is completed only once. One of the characteristics of these protocols is that they are less restrictive than commitment-type protocols in that there is no need to prepare the input to the next protocol according to encoding rules, and therefore many protocols have a relatively simple structure.

3.1 Introduction of the Up-Down Shuffle and Three-Card Trick

The Five-Card trick [2], known as a two-user non-committed card protocol, uses two types of cards: heart $\boxed{\heartsuit}$ and club $\boxed{\clubsuit}$. It is a method of obtaining AND outputs (specifically, operations that reveal hidden cards) while keeping the input values secret by performing random cuts to identify some initial cases immediately after card input.

Here, we consider a two-party AND operation protocol similar to the Five-Card trick. In general card protocols, two cards of each of two different suits are distributed, and two cards represent one bit. Therefore, the minimum number of cards distributed is four. On the other hand, if cards with exactly the same picture on the front and back are used, one card can be used to represent one bit, as it can be input in an up-and-down relationship, i.e., in two different directions $\boxed{\downarrow}$ and $\boxed{\uparrow}$. Therefore, the minimum number of cards that can be distributed is two, and if the AND protocol can be constructed when one card is distributed, it can be said that the number of cards is an optimal method.

For example, if the encoding rule $\boxed{\downarrow} = 0$, $\boxed{\uparrow} = 1$ is to be applied, the following layout is initially obtained by inputting the following as in a Five-Card trick: the extra card in the middle is

Table 5 Initial states of the Three-Card trick.

(a,b)	sequence
(0,0)	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$
(0,1)	$\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$
(1,0)	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$
(1,1)	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$

Table 6 Initial states after up-down shuffle on the Three-Card trick.

(a,b)	sequence
(0,0)	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$
(0,1)	$\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$
(1,0)	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$
(1,1)	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$

$\boxed{\uparrow}$, and each user inputs one $\boxed{\downarrow}$ or $\boxed{\uparrow}$ reverse side from each side. Let us call this the Three-Card trick [9].

As in the Five-Card Trick, a three-card random-cut process is used to disturb the input, but during output, it is found that only when $a \wedge b = 1$, there are three $\boxed{\uparrow}$ cards in a row, including the extra card. On the other hand, in the Five-Card Trick, the three cases where $a \wedge b = 0$ could all be regarded as identical. However, as shown in **Table 5**, the number of $\boxed{\uparrow}$ cards is different, so they cannot be regarded as identical, and thus the inputs a and b cannot be concealed in this way.

Here, we consider the application of the up-down shuffle. One possible method is to use an extra card in the random-cut bundle to conceal the surface of the first of the three cards, and then remove the extra card after switching the top and bottom positions by tossing or other means. Additionally, there is a shuffling method that rotates regular polygonal cards vertically, which is not a normal card shape, and can be considered a similar implementation to the up-down shuffle [4], [5]. There are various implementations of the up-down shuffle, but in any case, the up-down shuffle means that $\boxed{\downarrow}$ and $\boxed{\uparrow}$ are interchanged in multiple card bundles, and in the Three Card Trick, the initial input state changes as follows.

When comparing the states in Table 5 and **Table 6**, after the random cut and the up-down shuffle, the number of $\boxed{\uparrow}$ cards will be 0, 1, 2, or 3. When $a \wedge b = 1$, the number of $\boxed{\uparrow}$ cards is either 0 or 3. Furthermore, when $a \wedge b = 0$, the number of $\boxed{\uparrow}$ cards is 1 or 2, and the output can be obtained while keeping the inputs a and b concealed. In other words, the six possible combinations ($\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$) are all regarded as identical, ensuring the security (input concealment) of this protocol. Additionally, it is evident that the Three Card Trick achieves an optimal AND operation protocol in terms of the number of input cards.

The three-card groups that can be regarded as identical can be classified into the following two types:

Type	Equivalent Card Sets
1	$\boxed{\downarrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\downarrow}$ $\boxed{\downarrow}\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$, $\boxed{\uparrow}\boxed{\uparrow}\boxed{\downarrow}$
3	$\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$

Table 7 States of Two-Card Bundles After Up-Down Shuffle.

	Equivalent Card Sets
τ_0	$\boxed{\uparrow}\boxed{\uparrow}$, $\boxed{\downarrow}\boxed{\downarrow}$
τ_1	$\boxed{\uparrow}\boxed{\downarrow}$, $\boxed{\downarrow}\boxed{\uparrow}$

For example, it is evident that $\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$, categorized as Type 3, is regarded as equivalent to $\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$ due to the up-down shuffle.

3.2 XOR Operation Protocol Using Up-Down Cards

We consider a two-party XOR operation protocol as a starting point. Following the encoding rule where $\boxed{\downarrow}$= 0 and $\boxed{\uparrow}$= 1, when one user holds and inputs one card, the possible patterns are as follows.

(a,b)	sequence
(0,0)	$\boxed{\downarrow}\boxed{\downarrow}$
(0,1)	$\boxed{\downarrow}\boxed{\uparrow}$
(1,0)	$\boxed{\uparrow}\boxed{\downarrow}$
(1,1)	$\boxed{\uparrow}\boxed{\uparrow}$

When the cards are revealed, this can be represented as a 2×2 matrix as follows.

$a\backslash b$	0	1
0	τ_0	τ_1
1	τ_1	τ_0

Here, **Table 7** shows the classification of the variations that two-card bundles can have after an up-down shuffle.

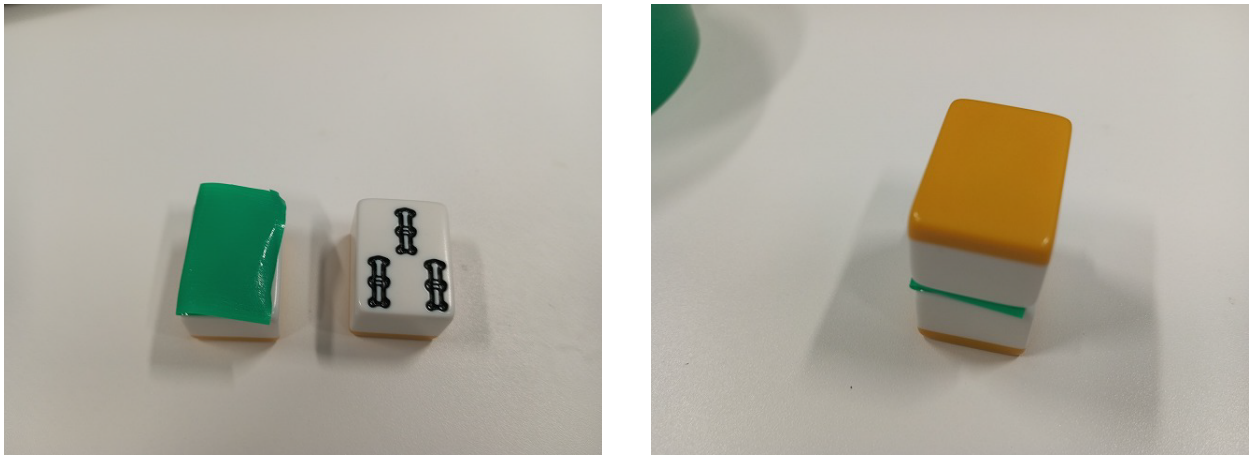
After an up-down shuffle, it is possible to detect only whether the two-card bundle is oriented in the same direction (τ_0) or in different directions (τ_1). This ensures that the user input is concealed and demonstrates the realization of an XOR operation protocol using Up-Down cards.

3.3 A Card-based Protocol Realizing a Four-point Likert Scale

ACNS 2023 Poster [12] proposed a new card-based protocol that involves four cards distributed between two parties, and is based on the assumption that all four values are accepted. The protocol asks both parties to indicate how close their opinions are on a four-point scale (0 = not at all disagree, 1 = somewhat disagree, 2 = somewhat agree, and 3 = strongly agree), which is commonly used in surveys. The protocol consists of three patterns: complete agreement, approximate agreement (cases with inputs $\{0,1\}$ or $\{2,3\}$), and disagreement. The results are only known to the parties, and the inputs are kept secret from the third party.

By introducing the technique of the up-down shuffle, we can move away from the traditional card protocol method of representing one bit with two cards. Instead, we can input 2 bits, i.e., four options, and replace this with input on a 4-step Likert scale. This allows the construction of a protocol where the extent to which two parties have similar opinions can be output as a result of the protocol, without the third party knowing the inputs.

The protocol uses four cards distributed to the two users, mak-



(a) (b)

Fig. 2 Specific implementation of the card deck partitioning method using mahjong tiles.

Table 8 Relations of inputs from 4-step Likert scale.

$a\backslash b$	0	1	2	3
strongly disagree(0)	[0]	[1]	[2]	[2]
somewhat disagree(1)	[1]	[0]	[2]	[2]
somewhat agree(2)	[2]	[2]	[0]	[1]
strongly agree(3)	[2]	[2]	[1]	[0]

ing it an optimal method as it does not require extra cards. Additionally, it is composed solely of random cuts and up-down shuffles, ensuring it is a highly practical protocol.

Furthermore, the case of this proposal has the algebraic structure as one of the association schemes [6] with 4 points: $H(2, 2)$ [16].

3.3.1 *m*-card Deck Partitioning Method

We explain the 2-card deck partitioning method in a card-based protocol realizing a four-point Likert scale [12]. If the inputs from User A are the 1st and 2nd cards, and the inputs from User B are the 3rd and 4th cards, after splitting into two bundles of the 1st and 3rd cards and the 2nd and 4th cards, each bundle is subjected to an up-down shuffle. In other words, for the card inputs $c_{i,1}, c_{i,2}$ from users $u_i (i = 1, 2)$, the two decks (card bundles) can be represented as $D_1 = \{c_{1,1}, c_{2,1}\}$ and $D_2 = \{c_{1,2}, c_{2,2}\}$.

This operation is similar to a random section cut, but it is important to note that the shuffle target is not the card bundle itself but each bundle is subjected to an up-down shuffle. When considering the decks after the up-down shuffle, they can be classified into two types, τ_0 or τ_1, as shown in Table 7. In other words, it only determines whether they are oriented in the same direction. Since an up-down shuffle is also performed, it is not possible to determine the original order of the decks. It can only determine whether the two users placed the cards in the same direction or not.

As a result, if both card bundles result in τ_0, considering the 1st and 3rd cards and the 2nd and 4th cards from **Table 8**, it can be seen that it is either Type-1 or Type-4. This is because Type-1 is $\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}$ or $\boxed{\downarrow}\boxed{\uparrow}\boxed{\downarrow}\boxed{\uparrow}$, and therefore a deck of $\tau_0 \times 2$ is obtained. Similarly, Type-4 is $\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}\boxed{\uparrow}$ or $\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}\boxed{\downarrow}$, and a deck of $\tau_0 \times 2$ is obtained. These two types cannot be distinguished after applying the 2-card deck partitioning method. Similarly, if the two decks are split into τ_0 and τ_1, it can only be Type-2. If both card bundles are τ_1, it is only Type-3.

Based on this example, we name the card processing method that naturally extends to m decks as the "m-card deck partitioning method" in the card processing method proposed in the ACNS 2023 Poster [12]. If the number of players is 3, the "3-card deck partitioning method" is applied, and similarly, if there are m players, it can be extended to the m-card deck partitioning method.

3.4 Specific Implementation of the Card Deck Partitioning Method Using Mahjong Tiles

Select the mahjong tiles that correspond to the up-down cards. One example is the "3 bamboo tile" as shown in **Fig. 2** (a). On the other hand, the honor tile "White Dragon" does not correspond to the up-down cards. When Player A inputs the tiles, they mask the surface with double-sided tape instead of input on the reverse side like in the card protocol. Player B then inputs their tiles in such a way that they cannot be seen, resulting in the state shown in Fig. 2 (b).

By achieving this state, it can be thrown in the same manner as the card deck partitioning method, yielding the same effect. When revealing the tiles, this can be done by carefully removing the masking tape.

4. Proposal of a New Protocol Utilizing Tornado Shuffle

In the previous chapter, we demonstrated that the card deck partitioning method can be implemented using mahjong tiles. In this chapter, we will discuss the Tornado shuffle [11], which is suitable for mahjong tiles. The Tornado shuffle is a method of point-symmetric shuffling applied to mahjong tiles lined up horizontally, without changing their physical positions. In contrast, the implementation method for regular cards has not been thoroughly examined. We propose a new protocol that assumes throwing the deck while keeping the mahjong tiles physically attached, similar to the card deck partitioning method.

In the original Tornado shuffle, three cards are shuffled, but it can be easily extended to any number of cards by removing the three-card constraint.

Each player inputs as follows. Here, the result of the card deck

(a) (b) (c)

Fig. 3 Mahjong tiles for Tornado shuffle.

partitioning method is re-expressed from two cards to one card: only one of the two tiles is revealed. If the revealed tile is $\boxed{\uparrow}$, the position of the second unrevealed tile remains unchanged. If the revealed tile is $\boxed{\downarrow}$, the up and down positions of the unrevealed tile are swapped. Note that the positions of the resulting two cards are not interchanged; that is, the results after throwing each deck are displayed. In practice, it is assumed that the two decks are thrown simultaneously.

$a\backslash b$	$\boxed{\uparrow\uparrow}$	$\boxed{\downarrow\downarrow}$	$\boxed{\downarrow\uparrow}$	$\boxed{\uparrow\downarrow}$
$\boxed{\uparrow\downarrow}$	$\boxed{\uparrow\downarrow}$	$\boxed{\downarrow\uparrow}$	$\boxed{\downarrow\downarrow}$	$\boxed{\uparrow\uparrow}$
$\boxed{\downarrow\uparrow}$	$\boxed{\downarrow\uparrow}$	$\boxed{\uparrow\downarrow}$	$\boxed{\uparrow\uparrow}$	$\boxed{\downarrow\downarrow}$
$\boxed{\downarrow\downarrow}$	$\boxed{\downarrow\downarrow}$	$\boxed{\uparrow\uparrow}$	$\boxed{\uparrow\downarrow}$	$\boxed{\downarrow\uparrow}$
$\boxed{\uparrow\uparrow}$	$\boxed{\uparrow\uparrow}$	$\boxed{\downarrow\downarrow}$	$\boxed{\downarrow\uparrow}$	$\boxed{\uparrow\downarrow}$

The two tiles obtained in this manner are combined face-to-face as shown in Fig. 2 (b) and the 2-card deck partitioning method is applied. By ultimately revealing the two tiles, the states $\boxed{\downarrow\downarrow}$ and $\boxed{\uparrow\uparrow}$ are regarded as identical, and it can be seen that they are finally classified into the following categories.

$a\backslash b$	$\boxed{\uparrow\uparrow}$	$\boxed{\downarrow\downarrow}$	$\boxed{\downarrow\uparrow}$	$\boxed{\uparrow\downarrow}$
$\boxed{\uparrow\downarrow}$	0	2	1	1
$\boxed{\downarrow\uparrow}$	2	0	1	1
$\boxed{\downarrow\downarrow}$	1	1	0	2
$\boxed{\uparrow\uparrow}$	1	1	2	0

Next, we will show how to implement it using the Tornado shuffle. **Figure 3** (a) and Fig. 3 (b) show four mahjong tiles lined up horizontally and stuck together with tape. Since the size is as shown in Fig. 3 (c), initial experiments have shown that a Tornado shuffle can be performed in this state on a desk with sufficient no frictional resistance. However, what we want to achieve is doing the Tornado shuffle of two mahjong tiles. We were unable to rotate the tiles successfully when there were only two tiles, so we presented the following idea. Just like the card deck partitioning method, we divide the tiles into two piles of two mahjong tiles. In this state, we use tape to create two decks. Furthermore, by covering the lid with the lid mentioned above and moving the lid circularly in parallel in the same manner as the random cut, it can be seen that it is possible to achieve the Tornado shuffle.

We can also see that after the Tornado shuffle, there are only three states: $\boxed{\uparrow\downarrow}$, $\boxed{\downarrow\uparrow}$, and $\boxed{\downarrow\downarrow}$. $\boxed{\uparrow\downarrow}$ is noted as 0, the identical $\boxed{\downarrow\downarrow}$ and $\boxed{\uparrow\uparrow}$ are noted as 1, and $\boxed{\downarrow\uparrow}$ is noted as 2. This matrix corresponds exactly to the Hamming association scheme $H(2,2)$, meaning that we have presented an alternative implementation using the Tornado shuffle unique to mahjong tiles as proposed in the ACNS 2023 Poster. This method is simpler than the card deck partitioning method and specifically demonstrates that a card protocol capable of inputting a 4-step Likert scale can be implemented with mahjong tiles.

For realizing the practical implementation, the "lid and masking tape" method discussed in the previous chapter can be used. By securing the reverse sides of the four input mahjong tiles with masking tape and placing them inside a lid, the Tornado shuffle can be implemented by rotating the lid in the same manner as in the random cut implementation.

5. Future Work and Open Problems

This paper has addressed the differences in implementation between cards and mahjong tiles, demonstrating that existing card protocols can be sufficiently implemented with mahjong tiles. The card-based protocol realizing a four-point Likert scale using the Tornado shuffle, as presented last, is closely related to the Hamming scheme $H(2,2)$. It is known that in card protocols, it is possible to implement 2^n-step Likert scale input card-based protocols related to $H(2,n)$ for $n \geq 3$ [16]. Whether this can be achieved with the Tornado shuffle remains an open problem.

References

[1] Mizuki, T. and Shizuya, H.: Practical Card-Based Cryptography, *FUN 2014*, pp.313–324 (2014).

[2] den Boer, B.: More Efficient Match-Making and Satisfiability: The Five Card Trick, *EUROCRYPT'89*, pp.208–217 (1989).

[3] Shinagawa, K. and Mizuki, T.: The Six-Card Trick: Secure Computation of Three-Input Equality, *ICISC 2018* (2018).

[4] Shinagawa, K., Mizuki, T., Schuldt, J., Nuida, K., Kanayama, N., Nishide, T., Hanaoka, G. and Okamoto, E.: Secure multi-party computation using polarizing cards, 10th International Workshop on Security, *IWSEC 2015*, pp.281–297 (2015).

[5] Shinagawa, K., Mizuki, T., Schuldt, J., Nuida, K., Kanayama, N., Nishide, T., Hanaoka, G. and Okamoto, E.: Multi-party Computation with Small Shuffle Complexity Using Regular Polygon Cards, *ProvSec 2015*, pp.127–146 (2015).

[6] Bannai, E. and Ito, T.: *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings, Menlo Park, CA (1984).

[7] Brouwer, A.E. and Koolen, J.: The Distance-Regular Graphs of Valency Four, *Journal of Algebraic Combinatorics*, Vol.10, No.1, pp.5–24 (1999).

[8] van Dam, E.R. and Jazaeri, M.: Distance-regular Cayley graphs

with small valency, Ars Mathematica Contemporanea, Vol.17, No.1, pp.203–222 (2019).
[9] Marcedone, A., Wen, Z. and Shi, E.: Secure Dating with Four or Fewer Cards, IACR Eprint 2015/1031, available from ⟨https://eprint.iacr.org/2015/1031⟩.
[10] Ishikawa, R., Chida, E. and Mizuki, T.: Efficient card-based protocols for generating a hidden random permutation without fixed points, Unconventional Computation and Natural Computation, Calude, C.S. and Dinneen, M.J. (Eds.), *Lect. Notes Comput. Sci.*, Springer International Publishing, Vol.9252, pp.215–226 (2015).
[11] Shinagawa, K., Nuida, K., Nishide, T., Hanaoka, G. and Okamoto, E.: Committed AND protocol using three cards with more handy shuffle, *ISITA 2016*, pp.700–702 (2016).
[12] Suga, Y.: POSTER: A card-based protocol that lets you know how close two parties are in their opinions (agree/disagree) by using a four-point Likert scale, *ACNS Workshops 2023*, pp.716–721 (2023).
[13] Suga, Y.: A classification proof for commutative three-element semigroups with local AND structure and its application to card-based protocols, *IEEE International Conference on Consumer Electronics, 2022 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW*, pp.171–172 (2022).
[14] Suga, Y.: How to implement non-committed card protocols to realize AND operations satisfying the three-valued logics, *2022 10th International Symposium on Computing and Networking Workshops* (*CANDARW*) (2022).
[15] Suga, Y.: A classification for commutative three-element semigroups with local XOR structure and its implementability of card-based protocols, *IEEE International Conference on Consumer Electronics, 2023 IEEE International Conference on Consumer Electronics - Taiwan, ICCE-TW*, pp.543–544 (2023).
[16] Suga, Y.: Constructions of 2-party card-based protocols over a 6-point Likert scale and its relation to association schemes and distance regular graphs (in Japanese), *2023 Symposium on Cryptography and Information Security* (*SCIS2023*), 4F2-3 (2023).

Editor's Recommendation

This paper examines the feasibility of card protocols using mahjong tiles instead of regular cards. It also proposes specific implementation methods for several existing card protocols when using mahjong tiles. Furthermore, it provides a demonstration that allows users who are not familiar with cryptography to easily understand secret computation, making it a good subject that feels familiar to them. The paper gives insights to readers in this research field and thus is selected as a recommended paper.

(Program chair of DICOMO2023 Masashi Saito)

Yuji Suga received his B.Sc. degree in mathematics from Kyushu University in March 1995, and his M.Sc. degree in mathematics from the Graduate School of Mathematics, Kyushu University, in March 1997. He received his Ph.D. degree in engineering from the Graduate School of Systems and Information Engineering, University of Tsukuba in March 2016. After working at the Kyushu Institute of Systems Information Technology and an electrical equipment manufacturer, he joined his current position in July 2008. He has been engaged in research and development on cryptographic technology applications, key management, blockchain governance, and security protocols. He is a member of the CRYPTREC Cryptographic Technology Promotion Committee and the Cryptographic Key Management Guidance WG. He is also a co-initial contributor to the Blockchain Governance Initiative Network (BGIN), an expert member of ISO/TC 307 and ISO/TC 68, and a member of the Cryptoassets Governance Task Force (CGTF). He has also been involved in the organization of international conferences, serving as a general co-chair of ACM AsiaCCS 2022 and IWSEC 2021/2022. Additionally, he is a member of IPSJ and an advisor for the CSEC Special Interest Group of IPSJ. He received the IPSJ Yamashita Memorial Research Award in 2004 and the SCIS Innovation Paper Award from the ISEC group of IEICE in January 2023.