Suken BINGO: An Application of Card-based Cryptography to Psychological Board Games*

Ren Igari[1], Yuichi Komano[1], and Takaaki Mizuki[2]

[1] Chiba Institute of Technology, 2–17–1, Tsudanuma, Narashino, Japan
[2] Cyberscience Center, Tohoku University, 6–3 Aramaki-Aza-Aoba, Aoba-ku, Sendai, Japan

Abstract. BINGO is a classic game where players compete to complete a line on a 5×5 grid card. Since it typically requires a specialized bingo machine, spontaneous BINGO play is challenging. To overcome this, we introduce Suken BINGO, a new board game that allows players to declare integers verbally, similar to the Japanese hand game Suken, eliminating the need for a bingo machine. Furthermore, we propose Secret Suken BINGO by combining Suken BINGO with card-based cryptography. In this secure variant, players conceal the integers on their BINGO cards throughout the game, which enhances the enjoyment of psychological maneuvering and strategic depth. We then detail the implementation and discuss the security and efficiency of the proposed protocol.

Keywords: BINGO, Suken, card-based cryptography

1 Introduction

BINGO is a classic game played by two or more players using BINGO cards and a dedicated bingo machine. A standard BINGO card features a 5×5 grid, excluding the center square, which is often pre-marked as 'open.' The 24 unique integers written on the card are randomly chosen from the range 1 to 75, typically following the established column rules: 1–15 for the leftmost column, 16–30 for the second, and so on.

During the game, the bingo machine draws integers from 1 to 75 in a random order. Players mark the drawn numbers on their cards if applicable, and the first player to complete a line (row, column, or diagonal) declares 'BINGO' and wins. However, this traditional game has a significant practical limitation: the mandatory requirement of a specialized bingo machine makes spontaneous or impromptu play difficult.

* This paper appears in Proceedings of SecITC 2025. This version of the contribution has been accepted for publication, after peer review but is not the Version of Record and does not reflect post-acceptance improvements, or any corrections. The Version of Record is available online at: http://dx.doi.org/10.1007/978-3-032-17443-7_6. Use of this Accepted Version is subject to the publisher's Accepted Manuscript terms of use: https://www.springernature.com/gp/open-research/policies/accepted-manuscript-terms.

To find a solution that enables spontaneous play easily, we drew inspiration from *Suken*, a traditional Japanese hand game. In Suken, two players simultaneously extend random numbers of fingers in their right hands and declare an integer from 0 to 10 verbally. Each player (or a designated judge) then counts the extended fingers of the two players. The player who correctly guesses the sum is the winner. This mechanism demonstrates that a random drawing can be replaced by players' verbal declarations, leading to a game that is highly spontaneous and requires no equipment such as the bingo machine.

This paper introduces two kinds of new psychological games: *Suken BINGO* by combining BINGO with Suken, and *Secret Suken BINGO* by combining Suken BINGO with card-based cryptography.

1.1 Our Contribution

The contributions of this paper are as follows.

- We first propose *Suken BINGO* (Section 3.2), a novel board game designed to address the spontaneity issue of traditional BINGO. By integrating the concept of players' declarations from Suken into BINGO's integer drawing, Suken BINGO eliminates the need for a dedicated bingo machine and can be played anywhere with just BINGO cards.
- Furthermore, we propose *Secret Suken BINGO*, a secure and strategic variant that integrates Suken BINGO with card-based cryptography. In this new variant, the integers on players' BINGO cards are kept secret throughout the game using cryptographic commitments. This concealment transforms the game from a matter of pure luck into a deep strategic challenge, significantly enhancing the enjoyment of psychological maneuvering.
- We also propose another variant of Secret Suken BINGO, *Secret binary Suken BINGO*, to improve the efficiency. We then discuss the security and efficiency of the proposed methods.

The remainder of this paper is organized as follows. Section 1.2 provides an overview of existing research on games applying card-based cryptography. Section 2 introduces the preliminary notations from card-based cryptography required for our proposed games. Section 3 details the rules of Suken BINGO and Secret Suken BINGO. Section 4 then analyzes the security, efficiency, and player experience. Finally, Section 5 concludes this paper.

1.2 Related Works

This section reviews the related works that exemplify the application of card-based cryptography to board games.

Examples in card games include a protocol for creating virtual players in UNO [11], a secret group assignment protocol applicable to Werewolf [1], and a virtual player protocol for the game of Old Maid [13]. In addition, a new game, Gakmoro [7], was created by making use of card-based cryptography.

Furthermore, card-based cryptography has also been applied to games other than card games, such as a protocol that can uniformly and randomly generate problems for the 15-puzzle and Rubik's Cube [12], a protocol that determines the first and second players in shogi or chess based on player preferences [15], a method for enhancing the Hit and Blow game [3], and a method for obtaining new variants of Tagiron [5].

2 Preliminaries

This section provides preparatory explanations of the cards and card operations utilized in this paper, as well as the concept of Secret Suken BINGO.

2.1 Physical Cards

In this paper, two types of physical cards are used:

Integer Cards: Each card has an integer from 1 to n written on its face, such as $\boxed{1}\boxed{2}\boxed{3}\cdots\boxed{n}$. The reverse side of every card has the same pattern $\boxed{?}$.

Colored Cards: Each card has a ♣ or ♡ symbol on its face, and the back of every card has the same pattern $\boxed{?}$.

We use the notation

$$\underset{i}{\boxed{?}}$$

to denote a face-down integer card whose face is $\boxed{i}$ for an integer i, $1 \leq i \leq n$.

2.2 Commitments

This section describes integer representations using cards: integer commitments, multi-digit integer commitments, and binary integer commitments [6].

Integer Commitment: An integer $i \in \{0, 1, 2, \cdots, k-1\}$ is represented using $k-1$ $\boxed{\clubsuit}$ cards and one $\boxed{\heartsuit}$ card. Table 1 summarizes the integer commitments to integers from 0 to 9. The face-down card sequence is called an *integer commitment*. The integer commitment is denoted by $\boxed{?}\boxed{?}\cdots\boxed{?}$ or $\boxed{?\|}$, and is written as $E_k(i)$.

Multi-Digit Integer Commitment: A *multi-digit integer commitment* is a representation of an integer k as an n-digit decimal number ($n > \log_{10} k$), where each digit is encoded using an integer commitment above:

$$\overset{n\text{-th digit}}{\boxed{?\|}} \cdots \overset{\text{2nd digit}}{\boxed{?\|}} \overset{\text{1st digit}}{\boxed{?\|}}.$$

By using multi-digit integer commitments, an integer k can be represented using $10n$ cards, resulting in a card complexity of $O(\log_{10} k)$.

Table 1. Correspondence between Integers and Integer Commitments

integer	integer commitment
0	♡♣♣♣♣♣♣♣♣♣
1	♣♡♣♣♣♣♣♣♣♣
2	♣♣♡♣♣♣♣♣♣♣
3	♣♣♣♡♣♣♣♣♣♣
4	♣♣♣♣♡♣♣♣♣♣
5	♣♣♣♣♣♡♣♣♣♣
6	♣♣♣♣♣♣♡♣♣♣
7	♣♣♣♣♣♣♣♡♣♣
8	♣♣♣♣♣♣♣♣♡♣
9	♣♣♣♣♣♣♣♣♣♡

In Secret Suken BINGO, bundles of cards (*i.e.*, multi-digit integer commitments) are used to conceal (i) integers from 0 to 74 placed on the BINGO card grid and (ii) the sum of the numbers declared by the players, which is in the range of 0 to 79.

In Secret Suken BINGO, the maximum integer is 79, requiring $n = 2$ decimal digits. Since the integer commitment to the first digit (0 to 7) requires eight cards, a total of 18 cards is sufficient to represent an integer from 0 to 79.

Binary Integer Commitment: We call the encoding scheme that represents bit 0 as a sequence of cards with $\boxed{\clubsuit}\boxed{\heartsuit}$ flipped and bit 1 as a sequence with $\boxed{\heartsuit}\boxed{\clubsuit}$ flipped *a binary commitment*. Furthermore, we define *a binary integer commitment* as the method that represents an integer k as an n-bit binary number ($n > \log_2 k$) using the binary commitments as

$$\overset{n\text{-th bit}}{\boxed{?}\boxed{?}} \cdots \overset{\text{2nd bit}}{\boxed{?}\boxed{?}} \overset{\text{1st bit}}{\boxed{?}\boxed{?}}.$$

Later, we propose a variant of Secret Suken BINGO, named Secret Binary Suken BINGO, that reduces the number of cards by utilizing the binary integer commitments.

2.3 Basic Operations

Next, we explain the card operations which are used in Secret Suken BINGO.

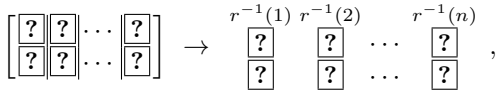
Pile-Scramble Shuffle: A *pile-scramble shuffle* [4] is an operation that shuffles several piles of cards of the same size (e.g., by securing them with rubber bands).

As an example, suppose that we have two lines of n face-down cards as follows:

$$\begin{array}{c} \overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\cdots\overset{n}{\boxed{?}} \\ \boxed{?}\boxed{?}\cdots\boxed{?} \end{array},$$

where the numbers above the cards represent indices for convenience.

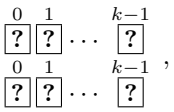
Considering each card and its underlying card as a pile, we apply a pile-scramble shuffle to the n piles, then the transition is as follows:



where $r \in S_n$ is a uniformly distributed random permutation generated by the pile-scramble shuffle, and S_n denotes the symmetric group of degree n.

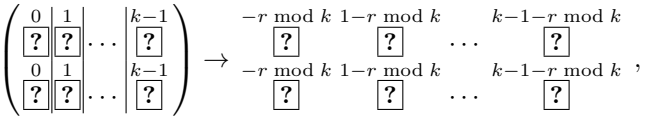
Pile-Shifting Shuffle: A *Pile-shifting shuffle* [9,14] is an operation that cyclically shifts piles of the same size uniformly at random.

As an example, consider two commitments consisting of k cards each, arranged face-down as follows:



where the numbers on the cards are used as convenient indices indicating their positions.

Considering the top and bottom cards as a single pile and applying a pile-shifting shuffle, then the transition is as follows:



where r is a uniformly random integer generated by the pile-shifting shuffle.

Addition of Commitments: Each of Secret Suken BINGO and Secret Binary Suken BINGO requires an addition protocol for multi-digit integer commitments and binary integer commitments, respectively. The idea to construct such addition protocols is similar to an addition of integers: for each digit or bit, we compute a sum of integer commitments or binary commitments with a carry. Due to the space limit, we omit the detail here and give a protocol in Appendices A.1 and A.2.

Equality Check of Commitments: Each of Secret Suken BINGO and Secret Binary Suken BINGO requires an equality check protocol for multi-digit integer commitments and binary integer commitments, respectively. The idea to construct such equality check protocols is similar to an equality check of integer commitments. Due to the space limit, we omit the detail here and give a protocol in Appendix B.

3 Suken BINGO and Variants

In this section, we first explain our idea to construct Suken BINGO and Secret Suken BINGO. Then, we propose Suken BINGO, Secret Suken BINGO, and Secret Binary Suken BINGO.

3.1 Our Idea

Conventional BINGO cards typically feature integers from 1 to 75. In contrast, Suken BINGO and its variants described in this section utilize cards with integers ranging from 0 to 74, excluding one number[3]. In this configuration, the integers on the BINGO cards are constrained to the ranges 0-14, 15-29, 30-44, 45-59, and 60-74 for the leftmost column and subsequent columns, respectively. Furthermore, we define $\mathcal{D}$ as a set of numbers declared by a player (called a saboteur, later); in this paper, we assume that $\mathcal{D} = \{0, 1, 2, 3, 4\}$.

Suken BINGO: Suken BINGO involves two distinct players: a progressor (P_i) and a saboteur (P_j). The progressor is a player who is trying to mark an integer on his own BINGO card by declaring an integer $d_i \in \{0, 1, \cdots, 74\}$. The saboteur is a player who obstructs the progressor from marking an integer on the progressor's BINGO card. For simplicity, this paper assumes only one saboteur, though we can assume two or more saboteurs. The saboteur declares an integer d_j from $\mathcal{D}$.

Subsequently, each player marks the square on their card that contains the sum $d_i + d_j (\mathrm{mod}\ 75)$. This process is repeated by alternating the roles of the progressor and the saboteur. As in traditional BINGO, players compete to be the first to complete a line (row, column, or diagonal) on their card.

Secret Suken BINGO: Secret Suken BINGO is constructed by placing multi-digit integer commitments corresponding to integers from 0 to 74 in each square of the Suken BINGO card. In this variant, the progressor and the saboteur declare integers by placing the corresponding multi-digit integer commitments on the table. The progressor or saboteur runs an addition protocol to sum up the commitments and, with an equality check protocol, checks whether the sum is equal to each of the commitments placed in their BINGO card.

Since the declared integers are concealed throughout the game using these commitments, Secret Suken BINGO significantly enhances the psychological maneuvering compared to Suken BINGO by preventing players from knowing the integers on their opponents' cards.

Secret Binary Suken BINGO: This variant utilizes BINGO cards where each square contains a binary integer commitment. For efficiency, the maximum integer value assigned to a square is set to $2^n - 1$ for some integer n. The candidate

[3] We can use standard BINGO cards numbered 1 to 75 by defining the value to be marked as the sum of the players' declared integers modulo 75, plus one.

maximum values are $15 = 2^4 - 1, 31 = 2^5 - 1$, and $127 = 2^7 - 1$. However, 15 and 31 are considered too small, which could lead to a premature game end and diminish enjoyment. Conversely, a maximum value of 127 is deemed too large, making BINGO difficult to achieve. Therefore, we assume a maximum card value of 63 (*i.e.*, $n = 6$). A key difference is that while conventional BINGO and Secret Suken BINGO utilize a 5×5 grid card, Secret Binary Suken BINGO requires a smaller grid card.

When integers from 0 to 63 are placed on a 5×5 grid card, the probability of a square being marked, assuming random placement and declaration, is $\frac{25}{64}$. This probability is higher than that of conventional BINGO or Secret Suken BINGO ($\approx \frac{1}{3}$), potentially diminishing the player's enjoyment. This is because, in Secret Suken BINGO and Secret Binary Suken BINGO, the progressor declares integers to target holes on their own card, whereas the saboteur declares small integers to prevent this. Consequently, the declarations are not random for the progressor, unlike standard BINGO. Conversely, saboteurs may unintentionally mark squares on their own card. Thus, to maintain players' enjoyments, the size of BINGO card is reduced to a 4×4 grid.

Specifically, Secret Binary Suken BINGO utilizes a 4×4 matrix of binary integer commitments ranging from 0 to 63. Hereinafter, we call this matrix a 4×4 *grid card* or *BINGO card* simply. Under the assumption of random placement and declaration, the probability of a hole appearing is $\frac{1}{4}$. Although this probability is lower than that of conventional BINGO or Secret Suken BINGO, it is deemed acceptable as it preserves the satisfaction of marking a square.

In Secret Binary Suken BINGO, the progressor and the saboteur compute the remainder of the sum of their declared integers modulo 64. This remainder is computed efficiently through the bitwise addition of the two binary integer commitments by ignoring the carry to the 7th bit.

3.2 Suken BINGO

This section proposes Suken BINGO. As explained in Section 3.1, players use standard BINGO cards in Suken BINGO. The procedure is as follows.

1. Distribute one 5×5 grid card to each of players P_1 and P_2.
2. Assign initial roles. Assume that the progressor is P_1 and the saboteur is P_2.
3. Repeat the following steps until either player declares 'BINGO'.
   (a) The progressor and saboteur simultaneously declare integers $d_1 \in \{0, 1, \cdots, 74\}$ and $d_2 \in \mathcal{D}$.
   (b) Calculate $d = d_1 + d_2 \bmod 75$ and mark a square that match d on their BINGO cards.
   (c) If the mark is fourth one in a line (row, column, or diagonal), declare 'Reach.'
   (d) Else if the mark is fifth one in a line (row, column, or diagonal), declare 'BINGO'. If only one player declares 'BINGO,' she wins. If both players declare 'BINGO' simultaneously, the game ends in a draw.
   (e) Otherwise, switch the roles and go to the next iteration.

3.3 Secret Suken BINGO

Secret Suken BINGO is a variant of Suken BINGO that enhances the enjoyment of psychological maneuvering and strategic depth.

In Secret Suken BINGO, players arrange multi-digit integer commitments from 0 to 74 in each square of the Suken BINGO card. During the game, the progressor and saboteur place multi-digit integer commitments, instead of declaring integers as in Suken BINGO. Then, the progressor and saboteur add them by using the addition protocol and check whether their BINGO cards contain the same commitment as the sum by using the equality check protocol.

Note that, allowing players to freely arrange multi-digit integer commitments on their BINGO cards would degrade the enjoyment of the game. Suppose that a player arranges four multi-digit commitments corresponding to integers 10 through 14 in the first column. If the player (as a progressor) places a commitment corresponding to 10, the progressor can mark a square on own BINGO card, regardless of which commitment to integers 0 through 4 the saboteur places. Therefore, Secret Suken BINGO requires a step to randomly arrange multi-digit integer commitments on BINGO cards.

The procedure of Secret Suken BINGO is as follows.

1. Let players P_1 and P_2 each create their own 5×5 grid cards (BINGO cards) as follows. In this step, each player creates their own BINGO card where integers (represented by multi-digit integer commitments) of squares on the card are known only by the card holder (that is, each player has no information about the integers of squares on the opponent's card).
   (a) Player P_1 arranges seventy-five multi-digit integer commitments corresponding to the integers from 0 to 74 in a single line. Apply a pile-scramble shuffle. Place the leftmost twenty-five multi-digit integer commitments in a 5×5 matrix. At this point, P_1 privately looks at the commitments to check the integers on P_1's BINGO card grid without showing them to P_2. Arrange eighteen times fifty cards of the remaining fifty multi-digit integer commitments in a line. Then, apply a pile-scramble shuffle to the card sequence and turn them over to be face-up. These free cards are used in the next step.
   (b) Player P_2 adds fifty $\boxed{\heartsuit}$ cards and sixteen times twenty-five $\boxed{\clubsuit}$ cards to the free cards obtained in Step 1(a). Then, P_2 prepares P_2's BINGO card in the same manner as Step 1(a).
   (c) Player P_i places a face-up $\boxed{\clubsuit}$ next to each multi-digit integer commitment arranged on the 5×5 grid card which indicates that the square is not marked.
2. Let P_1 be the progressor and P_2 be the saboteur.
3. Repeat the following steps until either player declares 'BINGO.'
   (a) The progressor and saboteur select an integer d_1 from $0 \sim 74$ and an integer d_2 from $0 \sim 4$, respectively. Place the corresponding multi-digit integer commitments on the table.

(b) Apply the addition protocol in Appendix A.1 to obtain a multi-digit integer commitment corresponding to $d = d_1 + d_2 \in \{0, 1, 2, \cdots, 79\}$. Then, using the protocol described in Appendix C, compute a multi-digit integer commitment to d mod 75.

(c) Each of P_1 and P_2 applies the equality check protocol to check whether a multi-digit integer commitment in a square with an indicator $\boxed{\clubsuit}$ is equal to the multi-digit integer commitment to d mod 75 as follows:

i. P_i $(i = 1, 2)$ checks the equality of the multi-digit integer commitments using the equality check protocol described in Appendix B. Note that, due to the properties of the protocol, the original two multi-digit integer commitments are recovered after the equality check and are used in the subsequent steps.

ii. If the two multi-digit integer commitments are identical, replace $\boxed{\clubsuit}$ in that square with $\boxed{\heartsuit}$ which indicates that the square is marked. Otherwise, place the recovered multi-digit integer commitment back to the square next to the indicator $\boxed{\clubsuit}$. Then, return to the previous step and check the equality of a multi-digit integer commitment on the next square with the multi-digit integer commitment to d mod 75.

(d) If the equality check in Step 3(c)(i) leads a new line (row, column, or diagonal) where four indicators out of five squares are $\boxed{\heartsuit}$, the card holder declares 'Reach.'

(e) If the equality check in Step 3(c)(i) leads a new line (row, column, or diagonal) where every indicator in the five square is $\boxed{\heartsuit}$, the card holder declares 'BINGO.' If only one player declares 'BINGO,' that player wins. If both players declare 'BINGO' simultaneously, end the game in a draw.

(f) Otherwise, switch the roles and go to the next iteration.

3.4 Secret Binary Suken BINGO

In this section, we propose a variant of Secret Suken BINGO, named a *Secret Binary Suken BINGO*, that reduces the number of colored cards from Secret Suken BINGO. As explained in Section 3.1, this is achieved by arranging binary integer commitments on the players' BINGO cards instead of multi-digit integer commitments.

The procedure of Secret Binary Suken BINGO is as follows.

1. Let players P_1 and P_2 each create their own BINGO cards, so that each player knows the integers corresponding to the squares on own BINGO card and cannot know the integers corresponding to the squares on the opponent's BINGO card, as follows.

(a) Player P_1 arranges sixty-four binary integer commitments corresponding to the integers from 0 to 63 in a single line. Apply a pile-scramble shuffle. Place the leftmost sixteen binary integer commitments in a 4×4 matrix. At this point, P_1 privately looks at the commitments to check the integers on $P_1's$ BINGO card grid without showing them to P_2. Arrange

twelve times forty-eight cards of the remaining forty-eight binary integer commitments in a line. Then, apply a pile-scramble shuffle to the card sequence and turn them over to be face-up. These free cards are used in the next step.

(b) Player P_2 adds six times sixteen $\boxed{\clubsuit}$ and six times sixteen $\boxed{\heartsuit}$ cards to the free cards obtained in Step 1(a). Then, P_2 prepares P_2's BINGO card in the same manner as Step 1(a).

(c) Player P_i places a face-up $\boxed{\clubsuit}$ next to each binary integer commitment arranged on the 4×4 grid card which indicates that the square is not marked.

2. Let P_1 be the progressor and P_2 be the saboteur.
3. Repeat the following steps until either player declares 'BINGO.'
   (a) The progressor and saboteur select an integer d_1 from $0 \sim 63$ and an integer d_2 from $0 \sim 4$, respectively. Place the corresponding binary integer commitments on the table.
   (b) Apply the addition protocol in Appendix A.2 with ignoring carry to the 7th bit, which brings a binary integer commitment corresponding to $d = (d_1 + d_2 \bmod 64) \in \{0, 1, 2, \cdots, 63\}$.
   (c) Each of P_1 and P_2 applies the equality check protocol to check whether a binary integer commitment in its own square with an indicator $\boxed{\clubsuit}$ is equal to the binary integer commitment as follows:
      i. P_i $(i = 1, 2)$ checks the equality of the binary integer commitments using the equality check protocol described in Appendix B. Note that, due to the properties of the protocol, the original two binary integer commitments are recovered after the equality check and are used in the subsequent steps.
      ii. If the two binary integer commitments are identical, replace $\boxed{\clubsuit}$ in that square with $\boxed{\heartsuit}$ which indicates that the square is marked. Otherwise, place the recovered binary integer commitment back to the square next to the indicator $\boxed{\clubsuit}$. Then, return to the previous step and check the equality of a binary integer commitment on the next square with the binary integer commitment.
   (d) If the equality check in Step 3(c)(i) leads a new line (row, column, or diagonal) where three indicators out of four squares are $\boxed{\heartsuit}$, the card holder declares 'Reach.'
   (e) If the equality check in Step 3(c)(i) leads a new line (row, column, or diagonal) where every indicator in the four square is $\boxed{\heartsuit}$, the card holder declares 'BINGO.' If only one player declares 'BINGO,' that player wins. If both players declare 'BINGO' simultaneously, end the game in a draw.
   (f) Otherwise, switch the roles and go to the next iteration.

4 Discussion

Let us discuss the security and efficiency of Secret Suken BINGO and Secret Binary Suken BINGO. The discussion on the security and efficiency of Secret

Suken BINGO is similar to that on Secret Binary Suken BINGO. Therefore, in this section, we only discuss the security and efficiency of Secret Binary Suken BINGO and compare it with Secret Suken BINGO.

4.1 Security

This section discusses the security of Secret Binary Suken BINGO for integrity and confidentiality. The integrity means that, if players follow the rule of game, the winner of the game is correctly determined. On the other hand, the confidentiality means that information on the squares other than those with holes during game execution[4] does not leak.

Integrity: In Secret Binary Suken BINGO, the card arrangement in Step 1(a) ensures that each square contains a binary integer commitment corresponding to a distinct integer (that is, it is impossible to place identical binary integer commitments in multiple squares). With BINGO cards arranged in this manner, card-based cryptographic protocols, such as addition and equality check protocols, force players to execute the game correctly. Furthermore, by making status of each square visible, the winner of a game can be correctly determined.

Confidentiality: In Secret Binary Suken BINGO, the addition of declared integers and the equality check are executed using card-based cryptographic protocols. The security of these protocols guarantees the confidentiality of the integers for the unmarked squares of the BINGO card.

4.2 Efficiency

We then discuss the efficiency of Secret Binary Suken BINGO.

The number of cards required in Secret Binary Suken BINGO is $12 \times 64 + 12 \times 16$ cards[5] in Step 1. Therefore, when the number of players is two, 960 cards are required.

The number of shuffles required in Secret Binary Suken BINGO is $2\times$ (number of players) in Step 1, 36 in Step 3(b), and $13\times$ (number of squares to check) $\times$ (number of players) in Step 3(c)(i). Step 3 is repeated until the game ends, and since the number of squares to check is at most 16, the total number of shuffles is at most $4 + 452\times$ (number of iterations).

4.3 Comparison with Secret Suken BINGO

Table 2 compares Secret Binary Suken BINGO and Secret Suken BINGO.

[4] In Secret Binary Suken BINGO, if a square of a saboteur's BINGO card is marked, the progressor can know that the integer corresponding to that square is close to the integer declared by the progressor (*i.e.*, within the range of the declared number plus 4).

[5] For the equality check of the two binary integer commitments in Step 3, the colored cards discarded in Step 1(a) can be reused instead of number cards.

Table 2. Comparison of Secret Suken BINGO and Secret Binary Suken BINGO

game	grid	integers	commitments	cards	shuffles
Secret Suken BINGO	5×5	0-74	multi-digit integer	1800	$4 + 264\ell$
Secret Binary Suken BINGO	4×4	0-63	binary integer	960	$4 + 452\ell'$

In Table 2, "grid" indicates the size of the BINGO card, "integers" indicates the range of integers placed on the BINGO card, and "commitments" indicates the representation of integers on the BINGO card. In the last two columns, "cards" indicates the number of cards required in each game executed by two players, and "shuffles" indicates the number of shuffles performed during the game. Here, ℓ and ℓ' represent the number of iterations in the integer declaration in Secret Suken BINGO and Secret Binary Suken BINGO, respectively.

Although comparison is difficult due to the differences in BINGO card size and integer ranges, Secret Binary Suken BINGO can reduce both the number of cards and shuffles compared to Secret Suken BINGO.

5 Conclusion

In this paper, we proposed Suken BINGO and its variants, Secret Suken BINGO and Secret Binary Suken BINGO. Among them, Secret Suken BINGO and Secret Binary Suken BINGO are based on card-based cryptography which enhance the enjoyment of psychological maneuvering and strategic depth. We presented the procedures of these games and discussed their security and efficiency. Constructing efficient protocols such as equality check in batch is one of our future works.

Acknowledgements

We thank the anonymous reviewers, whose comments have helped us improve the presentation of the paper. We also thank Yuji Suga for his fruitful comments on an earlier version of our paper. This work was supported by Grant-in-Aid for Scientific Research (JP23H00479, JP24K14951, and JP24K02938).

References

1. Yuji Hashimoto, Kazumasa Shinagawa, Koji Nuida, Masaki Inamura, and Goichiro Hanaoka. Secure grouping protocol using a deck of cards. *IEICE Trans. Fundam.*, E101.A(9):1512–1524, 2018. URL: https://doi.org/10.1587/transfun.E101.A.1512.
2. Ren Igari, Shun Odaka, Yuichi Komano, and Takaaki Mizuki. Digitized integer commitment and addition protocol for card-based cryptography. *Symposium on Cryptography and Information Security (SCIS) 2025, 3D2-3*, 2025. (in Japanese).

3. Shota Ikeda and Kazumasa Shinagawa. How to play Mastermind without game master. In *Theory and Applications of Models of Computation*, LNCS, Cham, 2025, to appear. Springer.
4. Rie Ishikawa, Eikoh Chida, and Takaaki Mizuki. Efficient card-based protocols for generating a hidden random permutation without fixed points. In Cristian S. Calude and Michael J. Dinneen, editors, *Unconventional Computation and Natural Computation*, volume 9252 of *LNCS*, pages 215–226, Cham, 2015. Springer. URL: https://doi.org/10.1007/978-3-319-21819-9_16.
5. Koichi Koizumi and Takaaki Mizuki. An application of secure computation to tagiron. In *Advances in Computer Games*, LNCS, Cham, to appear. Springer.
6. Takaaki Mizuki, Isaac Kobina Asiedu, and Hideaki Sone. Voting with a logarithmic number of cards. In Giancarlo Mauri, Alberto Dennunzio, Luca Manzoni, and Antonio E. Porreca, editors, *Unconventional Computation and Natural Computation*, volume 7956 of *LNCS*, pages 162–173, Berlin, Heidelberg, 2013. Springer. URL: https://doi.org/10.1007/978-3-642-39074-6_16.
7. Takaaki Mizuki, Tomoki Kuzuma, Tomoya Hirano, Ririn Oshima, and Momofuku Yasuda. Gakmoro: An application of physical secure computation to card game. In *Unconventional Computation and Natural Computation*, LNCS, Cham, 2025, to appear. Springer.
8. Takaaki Mizuki and Hideaki Sone. Six-card secure AND and four-card secure XOR. In Xiaotie Deng, John E. Hopcroft, and Jinyun Xue, editors, *Frontiers in Algorithmics*, volume 5598 of *LNCS*, pages 358–369, Berlin, Heidelberg, 2009. Springer. URL: https://doi.org/10.1007/978-3-642-02270-8_36.
9. Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Pile-shifting scramble for card-based protocols. *IEICE Trans. Fundam.*, 101(9):1494–1502, 2018. URL: https://doi.org/10.1587/transfun.E101.A.1494.
10. Suthee Ruangwises, Tomoki Ono, Yoshiki Abe, Kyosuke Hatsugai, and Mitsugu Iwamoto. Card-based overwriting protocol for equality function and applications. In Da-Jung Cho and Jongmin Kim, editors, *Unconventional Computation and Natural Computation*, volume 14776 of *LNCS*, pages 18–27, Cham, 2024. Springer. URL: https://doi.org/10.1007/978-3-031-63742-1_2.
11. Suthee Ruangwises and Kazumasa Shinagawa. Simulating virtual players for UNO without computers. In *Unconventional Computation and Natural Computation*, LNCS, Cham, 2025, to appear. Springer.
12. Kazumasa Shinagawa, Kazuki Kanai, Kengo Miyamoto, and Koji Nuida. How to covertly and uniformly scramble the 15 puzzle and rubik's cube. In Andrei Z. Broder and Tami Tamir, editors, *Fun with Algorithms*, volume 291 of *LIPIcs*, pages 30:1–30:15, Dagstuhl, Germany, 2024. Schloss Dagstuhl. URL: https://doi.org/10.4230/LIPIcs.FUN.2024.30.
13. Kazumasa Shinagawa, Daiki Miyahara, and Takaaki Mizuki. How to play old maid with virtual players. In Bo Li, Minming Li, and Xiaoming Sun, editors, *Frontiers of Algorithmics*, volume 14752 of *LNCS*, pages 53–65, Singapore, 2025. Springer. URL: https://doi.org/10.1007/978-981-97-7752-5_4.
14. Kazumasa Shinagawa, Takaaki Mizuki, Jacob Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. Card-based protocols using regular polygon cards. *IEICE Trans. Fundam.*, E100.A(9):1900–1909, 2017. URL: https://doi.org/10.1587/transfun.E100.A.1900.
15. Yuto Shinoda, Daiki Miyahara, Kazumasa Shinagawa, Takaaki Mizuki, and Hideaki Sone. Card-based covert lottery. In Diana Maimut, Andrei-George Oprina, and Damien Sauveron, editors, *Innovative Security Solutions for Information*

Technology and Communications, volume 12596 of *LNCS*, pages 257–270, Cham, 2021. Springer. URL: https://doi.org/10.1007/978-3-030-69255-1_17.

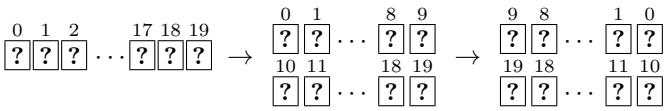
A Details of Addition Protocols

In this section, let us give details of addition protocols for multi-digit integer commitments and binary integer commitments.

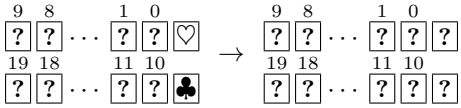
A.1 Addition Protocol for Multi-Digit Integer Commitments

Recently, Igari et al. [2] proposed an addition protocol for multi-digit integer commitments. From two multi-digit integer commitments $\{E_{10}(d_j^{(x)})\}$ and $\{E_{10}(d_j^{(y)})\}$, their protocol computes a multi-digit integer commitment to the sum, $\{E_{10}(d_j^{(x+y)})\}$, as follows.

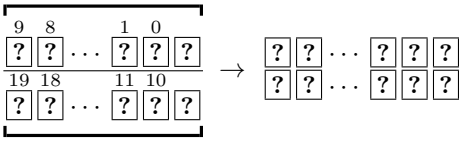
1. Repeat the following steps for $j = 0, 1, 2, \cdots, s-1$, where we assume s-digit integer commitments as input.
   (a) Put ten $\clubsuit$ cards to the right of each of $(j+1)$-th piles $E_{10}(d_j^{(x)})$ and $E_{10}(d_j^{(y)})$. The resulting piles are $E_{20}(d_j^{(x)})$ and $E_{20}(d_j^{(y)})$. When $j > 0$, put eighteen $\clubsuit$ cards right to the sequence of cards $E_2(c_{j-1})$, obtained in the $(j-1)$-th iteration as a commitment to a carry $c_{j-1} \in \{0, 1\}$, to generate $E_{20}(c_{j-1})$.
   (b) Compute the sum of commitments[6] $E_{20}(d_j^{(x)})$, $E_{20}(d_j^{(y)})$, and $E_{20}(c_{j-1})$, obtained in Step 1(a). Then, place the leftmost and rightmost ten cards of the result in the first and second rows, respectively. After that, rearrange cards in each row in the reverse order:



   (c) Place $\heartsuit$ and $\clubsuit$ to the right of the two rows as a new column. Then, turn over these face-up cards:

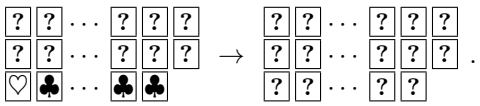


   (d) Apply a pile-scramble shuffle:

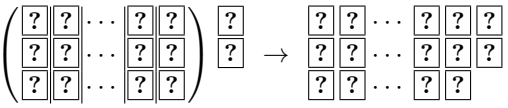


[6] For $j = 0$, the addition of $E_{20}(c_{j-1})$ is skipped.

(e) Put $E_{10}(0)$ as the third row and turn it over:

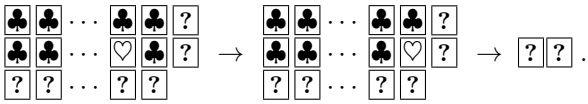


(f) Apply a pile-shifting shuffle to the left ten columns:



(g) Turn over the leftmost ten cards in the first and second rows. Note that one of the face-up cards is ♡ and the others are ♣'s. Then, shift the left ten columns cyclically so that ♡ is in the 10-th column. As a result, the face-down cards in the third row become a $(j+1)$-th digit of commitment to $x+y$. Therefore, output the commitment in the third row as the $(j+1)$-th pile of the result.

Moreover, among the first and second rows, rearrange the rightmost card of the row including face-up ♡ and the rightmost card of the other row into a two-card sequence from left to right. Then, forward the sequence as a carry, $E_2(c_j)$, to the addition of $(j+1)$-th digit. In the following example, the rightmost card in the second row and the rightmost card in the first row are the first and second cards from the left of $E_2(c_j)$, respectively:



The face-up cards can be reused in the following steps.

2. Put eight ♣'s to the right of $E_2(c_{s-1})$, which is obtained as the $(s-1)$-th carry. Then, output it as the $(s+1)$-th digit of the commitment to $x+y$.

We can compare integers encoded in the multi-digit integer commitment as follows. Assume that we want to determine whether $x \geq y$ for two multi-digit integer commitments to x and y. Each of commitments consists of s piles of ten colored cards, $E_{10}(d_i)$ where $i \in \{0, 1, \cdots, s-1\}$ and d_i is a digit of x or y. To compare x and y, we first rearrange the order of each $E_{10}(d_i^{(y)})$ in the reverse order. Note that the resulting piles represent a (commitment to) 9's complement of y. Then, we add it to a multi-digit integer commitment to one (with s piles of ten colored cards) to obtain a (commitment to) 10's complement of y. After that, we add it to a multi-digit integer commitment to x and check whether the topmost pile (final carry) is $E_{10}(0)$ or $E_{10}(1)$. If it is $E_{10}(1)$, then $x \geq y$ holds; otherwise, $x < y$ holds.

A.2 Addition Protocol for Binary Integer Commitments

Mizuki et al. [6] proposed a half-adder to efficiently compute the sum of two binary commitments and a full adder using this half-adder to compute the sum of two binary integer commitments with a carry.

Remember that $\boxed{\clubsuit}\boxed{\heartsuit}$ and $\boxed{\heartsuit}\boxed{\clubsuit}$ represent 0 and 1, respectively. The half-adder which takes bit commitments of two bits a, b as input is constructed as follows.

1. Copy the bit commitment of b using the copy protocol [8]. This requires two each of $\boxed{\clubsuit}$ and $\boxed{\heartsuit}$ cards and one shuffle.
2. Arrange the four bit commitments corresponding to a, b, b, and 0 sequentially in a single row.
3. Rearrange the cards so that the second card moves to the fifth position, the third to the second, the fourth to the sixth, the fifth to the third, and the sixth to the fourth.
4. Divide the eight cards into two groups of left and right four cards and apply a pile-shifting shuffle by regarding each of the left and right four cards as a pile.
5. Rearrange the cards so that the second card moves to the third position, the third to the fifth, the fourth to the sixth, the fifth to the second, and the sixth to the fourth.
6. Turn over the two leftmost cards.
7. If the face-up cards are $\boxed{\clubsuit}\boxed{\heartsuit}$, return the third and fourth cards as $a \oplus b$ (sum), and the seventh and eighth cards as $a \wedge b$ (carry). If the face-up cards are $\boxed{\heartsuit}\boxed{\clubsuit}$, swap the order of the third and fourth cards and return $a \oplus b$ (sum), and the fifth and sixth cards as $a \wedge b$ (carry).

The above half-adder requires four additional cards and two shuffle operations.

A full adder that takes a bit commitment of a carry c from lower bits and bit commitments to two bits a, b as inputs is constructed as follows. Here, $s' = (a \oplus b) \oplus c$ is the sum of its bits including the carry c from the lower bits, and $c' = (a \wedge b) \vee ((a \oplus b) \wedge c)$ represents a carry to the upper bits.

1. Using the aforementioned half-adder, compute the bit commitments to $a \wedge b$ and $a \oplus b$. Apply a shuffle to the remaining two face-down cards and turn them over. These cards are used as free cards later.
2. Input the bit commitments to $a \oplus b$ and c into the aforementioned half-adder, and obtain the bit commitments of $(a \oplus b) \wedge c$ and $s' = (a \oplus b) \oplus c$.
3. Using the OR protocol [8] (which is obtained by inverting the inputs and outputs of the AND protocol), compute the bitwise OR of the bit commitments to $a \wedge b$ and $(a \oplus b) \wedge c$, which is the bit commitment to c'.

The above full adder requires four additional cards and six shuffling operations.

B Detail of Equality Check Protocol

This section describes details of the equality check protocols for two sets of multi-digit integer commitments or binary integer commitments[7].

In Secret Suken BINGO or Secret Binary Suken BINGO, for each square in the grid card, we determine whether a multi-digit integer commitment or a binary integer commitment to an integer on the square matches a multi-digit integer commitment or a binary integer commitment to the sum d, respectively.

If they do not match, we then check the equality between a multi-digit integer commitment or a binary integer commitment in the next square and a multi-digit integer commitment or a binary integer commitment to the sum d, respectively. That is, we require an equality check protocol which restores its input.

Let us first give an equality check protocol for two multi-digit integer commitments.

1. Arrange eighteen integer cards $\boxed{1}, \boxed{2}, \boxed{3}, \ldots$ from left to right and turn them over.
2. Arrange two sets of eighteen cards for two multi-digit integer commitments in two rows (rows 2 and 3) below the face-down integer cards.
3. Apply a pile-scramble shuffle to the cards in these three rows, by regarding each column of three cards as a pile.
4. Turn over the cards in the third row.
5. Place eighteen cards of the same color as the third row in the fourth row.
6. Place eighteen cards of a different color from the fourth row in the fifth row.
7. Turn over cards in rows 3 to 5.
8. Apply a pile-scramble shuffle to the cards in the five rows, by regarding each column of five cards as a pile.
9. Turn over the cards in the second row and specify two columns where $\boxed{\heartsuit}$ appears in the second row.
10. Create two bit commitments by arranging two cards in the fourth and fifth rows from left to right in the specified columns. One of the commitments is $\boxed{\heartsuit}\boxed{\clubsuit}$ or $\boxed{\clubsuit}\boxed{\heartsuit}$ if tens digits are identical or not, and the other is $\boxed{\heartsuit}\boxed{\clubsuit}$ or $\boxed{\clubsuit}\boxed{\heartsuit}$ if ones digits are identical or not.
11. Apply a bitwise AND protocol [8] to the two bit commitments and turn them over. If two multi-digit integer commitments to be compared are identical, they are $\boxed{\heartsuit}\boxed{\clubsuit}$; otherwise, they are $\boxed{\clubsuit}\boxed{\heartsuit}$.
12. Apply a pile-scramble shuffle to the cards in the upper three rows.
13. Turn over the cards in the first row.
14. Rearrange the piles of the cards, by regarding three cards in each column of upper three rows as a pile, so that the integer cards in the first row are in ascending order. Then, two multi-digit integer commitments are restored in the second and third rows.
15. Rearrange the cards of the fourth and fifth rows in a line and apply a pile-scramble shuffle. Then, turn them over, which become free cards.

[7] While Ruangwises et al.'s overwriting protocol [10] can achieve this, we present a more direct and simple protocol here.

Let us then give an equality check protocol for two binary integer commitments to integers x and y.

1. Arrange twenty-four integer cards $\boxed{1}, \boxed{2}, \boxed{3}, \ldots$ from left to right and turn them over.
2. Arrange two sets of twelve cards for two binary integer commitments to integers from 0 to 63 into a line in the second row below the face-down integer cards.
3. Apply a pile-scramble shuffle to the cards in these two rows, by regarding each column of two cards as a pile.
4. Turn over the cards in the second row.
5. Place twenty-four cards of the same color as the second row in the third row.
6. Apply a pile-scramble shuffle to the cards in the three rows, by regarding each column of three cards as a pile.
7. Turn over the cards in the first row.
8. Rearrange the piles of the cards, by regarding three cards in each column as a pile, so that the integer cards in the first row are in ascending order. Then, two binary integer commitments are restored in the second row.
9. By using the four-card XOR protocol [8], compute six bit commitments to XOR values of the first two cards (a bit commitment for the first bit of x) and the thirteen to fourteen cards (a bit commitment for the first bit of y), the third to forth cards (a bit commitment for the second bit of x) and the fifteen to sixteen cards (a bit commitment for the second bit of y), and so on.
10. Rearrange two cards of each of six commitments to XOR values in the reverse order.
11. By using the AND protocol [8] five times, compute the AND of the above six rearranged commitments. If two binary integer commitments to be compared are identical, they are $\boxed{\heartsuit}\boxed{\clubsuit}$; otherwise, they are $\boxed{\clubsuit}\boxed{\heartsuit}$.

Instead of the integer cards in the above protocols, we can use a sequence of colored cards corresponding to integers, such as integer commitments, multi-digit integer commitments, or binary integer commitments.

C Secure Reduction Protocol with Modulo 75

In Secret Suken BINGO proposed in Section 3.3, we need to compute a multi-digit integer commitment to $d \bmod 75$ where d is in $\{0, 1, 2, \cdots, 79\}$. Note that the multi-digit integer commitment consists of the tens digit integer $d_1 \in \{0, 1, 2, \cdots, 7\}$ which is represented by $E_8(d_1)$ using eight colored cards, and the ones digit integer $d_0 \in \{0, 1, 2, \cdots, 9\}$ which is represented by $E_{10}(d_0)$ using ten colored cards. Our reduction protocol with modulo 75 is performed as follows:

1. Arrange integer cards from 1 to 14 in order from left to right.
2. Add six $\boxed{\clubsuit}$ cards to the right of the integer commitment $E_8(d_1)$ to form $E_{14}(d_1)$, then place it below the integer cards arranged in Step 1 from left to right.

3. Divide the integer commitment $E_{10}(d_0)$ into two halves of five cards each (upper and lower). Add two $\boxed{\clubsuit}$ cards to the right of each half. Then, place the lower five cards (with two $\boxed{\clubsuit}$ cards added to their right) as the third row of cards, each below the integer cards 1 through 7. Similarly, place the upper five cards (with two $\boxed{\clubsuit}$ cards added to their right) as the third row cards under the integer cards 8 through 14.
4. As the fourth row cards, place $\boxed{\clubsuit}$ under the integer card 1 and $\boxed{\heartsuit}$ under the integer card 8. These cards will later indicate whether the tens digit is seven or not.
5. As the fifth row of cards, place $\boxed{\clubsuit}$ under the integer card 1 and $\boxed{\heartsuit}$ under the integer card 8. These cards will later indicate whether the ones digit is more than four or not. At this point, the cards are arranged as shown below. Then, turn over all cards to be face-down.

$\boxed{1}\boxed{2}\cdots\boxed{7}\boxed{8}\boxed{9}\cdots\boxed{14}$: Integer cards
$\boxed{?}\boxed{?}\cdots\boxed{?}\boxed{?}\boxed{?}\cdots\boxed{?}$: The tens digit and dummy cards
$\boxed{?}\boxed{?}\cdots\boxed{?}\boxed{?}\boxed{?}\cdots\boxed{?}$: The ones digit and dummy cards
$\boxed{\clubsuit}\quad\quad\boxed{\heartsuit}$: Colored cards
$\boxed{\clubsuit}\quad\quad\boxed{\heartsuit}$: Colored cards

Note that, when d is 75 or greater (*i.e.*, when the right half of each card sequence in second and third rows contains $\boxed{\heartsuit}$), $d \bmod 75$ is obtained by swapping the positions of the left and right seven cards in the second and third rows.

6. For rows 1 through 3, apply a pile-scramble shuffle to each of the left seven cards and the right seven cards.
7. For rows 1 through 5, by regarding each of the left twenty-three cards (left seven cards in the upper three rows and two cards in the forth and fifth rows) and right twenty-three cards as piles, apply a pile-scramble shuffle.
8. Turn over the cards in the third row to be face-up. Rearrange the left and right piles so that a pile containing $\boxed{\heartsuit}$ in the third row moves to the right.
9. Keep the two cards in the fifth row. They are $\boxed{\clubsuit}\boxed{\heartsuit}$ if the ones digit is five or greater, and $\boxed{\heartsuit}\boxed{\clubsuit}$ if it is less than five.
10. Turn over the cards in the third row to be face-down. Apply a pile-scramble shuffle to the columns in the rows through 1 to 4 as in Step 7.
11. Turn over the cards in the second row to be face-up. Rearrange the left and right piles so that a pile containing $\boxed{\heartsuit}$ in the second row moves to the right.
12. Keep the two cards in the fourth row. They are $\boxed{\clubsuit}\boxed{\heartsuit}$ if the tens digit is seven, and $\boxed{\heartsuit}\boxed{\clubsuit}$ if it is less than seven.
13. Turn over the cards in the second row to be face-down. Apply a pile-scramble shuffle to the whole fourteen columns in the rows through 1 to 3.
14. Turn over the cards in the first row to be face-up. Rearrange the columns so the integer cards in the first row are in ascending order from left to right. Then, remove the integer cards from the first row.
15. Divide each of the remaining two rows into two halves of seven cards each.

16. Apply the AND protocol [8] to the two sets of two cards kept in Steps 9 and 12 to obtain $\boxed{?}\boxed{?}$. Note that here, 0 is encoded as $\boxed{\heartsuit}\boxed{\clubsuit}$ and 1 as $\boxed{\clubsuit}\boxed{\heartsuit}$. The resulting cards are $\boxed{\clubsuit}\boxed{\heartsuit}$ if the tens digit is seven and the ones digit is five or greater (that is, $d \geq 75$), and $\boxed{\heartsuit}\boxed{\clubsuit}$ otherwise.
17. Place each of the two cards obtained in Step 16 onto the left and right halves of seven cards obtained in Step 15.
18. Divide the three rows of card sequences obtained in Step 17 (the first row contains the two cards from the AND operation, the second row contains a sequence of fourteen cards including the card corresponding to the tens place, and the third row contains a sequence of fourteen cards including the card corresponding to the ones place) into halves. Apply the pile-scramble shuffle to each half as a pile.
19. Turn over the cards in the first row to be face-up. Then, rearrange the cards from the first to the third row so that $\boxed{\heartsuit}$ among the two cards in the first row moves to the left. Remove the two colored cards from the first row.
20. From the remaining two rows, remove the dummy cards placed in Steps 2 and 3. Consequently, output two sequences of cards in the first and second rows as an integer commitment for the tens place and an integer commitment for the ones place of $d \bmod 75$), respectively.