

Malicious Player Card-based Cryptographic Protocols with a Standard Deck of Cards Using Private Operations

No Author Given



No Institute Given

Abstract. This paper shows new card-based cryptographic protocols to calculate Boolean functions using a standard deck of cards when the players are malicious. Card-based cryptographic protocols use physical cards instead of computers. They can be used when the software on computers is not reliable. We discuss protocols that use a standard deck of cards because it is easy to prepare. Though protocols that use private operations tend to be efficient in the number of cards used in the protocols, malicious actions are possible during private operations. This paper shows three-player protocols to prevent malicious actions by watching another player's actions. We show logical AND, XOR, and copy protocols since any Boolean functions can be realized by a combination of the protocols. The numbers of cards used by the protocol are the minimum.

Keywords: card-based cryptographic protocols · Boolean functions · malicious players · standard deck of cards · multi-party secure computation.

1 Introduction

Card-based cryptographic protocols [15, 37, 39] were proposed in which physical cards are used instead of computers to securely calculate values. They can be used when computers cannot be used or users cannot trust the software on the computer. Also, the protocols are easy to understand, thus the protocols can be used to teach the basics of cryptography [5, 31]. den Boer [3] first showed a five-card protocol to securely calculate the logical AND of two inputs. Since then, many protocols have been proposed to realize primitives to calculate any Boolean functions [8, 13, 19, 23, 40, 50, 60] and specific computations such as a class of Boolean functions [2, 24, 27, 32, 36, 45, 46, 48, 53, 56, 58, 64, 66], millionaires' problem [28, 42, 49], realizing Turing machines [7, 18], voting [34, 43, 47, 65], random permutation [9, 11, 12, 41], grouping [10], ranking [62], lottery [61], proof of knowledge of a puzzle solution [4, 6, 22, 29, 30, 52, 54, 55, 57], and so on. This paper considers calculations of logical AND and logical XOR functions and copy operations since any Boolean function can be realized with a combination of these calculations.

Most of the above works are based on a two-color card model. In the two-color card model, there are two kinds of cards,  and . Cards of the same

marks cannot be distinguished. In addition, the back of both types of cards is $\boxed{?}$. It is impossible to determine the mark in the back of a given card of $\boxed{?}$. Though the model is simple, protocols using the two-color card model cannot be realized as it is using one standard deck of playing cards. Some helping cards are necessary to execute using a standard deck of playing cards. On the other hand, card-based cryptographic protocols using a standard deck of playing cards and their formal security proofs were shown [14, 16, 20, 21, 25, 33, 44, 59]. Protocols to calculate AND, copy, and XOR using private operations using a standard deck of cards were shown [25]. Private operations are executed where the other players cannot see, for example, under the table or in the back. Though private operations are effective in card-based protocols, there is a problem with private operations. Since the private operations are executed where the other players cannot see, a player might execute malicious actions during private operations. For example, a malicious player might see the marks of face-down cards. Another malicious player might swap the cards to change the values. We need to prevent or detect such malicious actions.

A countermeasure to the problems is watching private actions and detect malicious actions. When the protocols are executed by two players, Alice and Bob, Alice must not see Bob's private actions. If Alice sees Bob's private operations, Alice can see all operations, thus Alice sees the relationship between the private inputs and the output. If the output cards are opened to see the final result, Alice can know the private input data from the relationship. Thus, another player other than two players are necessary to watch the private operations. If the watcher sees both Alice and Bob's private operations, the watching player can know all operations and the relationship between the input data and the output data. Thus the watching player knows the private data. If we prepare Alice's watcher and Bob's watcher, four players seems to be necessary.

This paper shows that three players are sufficient to detect malicious actions and keep the protocol secure. In the three-player protocols shown in this paper, Bob watches Alice's private operations, Carol watches Bob's private operations, and Alice watches Carol's private operations.

Few works are done for the case when some players are malicious or make mistakes [1, 17, 26, 35, 38, 63]. They are categorized into two groups. The first one is to use additional cards or special items such as envelopes [17, 26, 63]. The second type introduces the watching player. The watching player for the protocol with a two-color card model is shown [26]. Abe et al. showed a three-player majority voting protocol with a malicious player [1]. Note that the above works are done for the two-color card model. There is no work for a standard deck of cards. As long as the author knows, this is the first work that discusses malicious activities in protocols that use a standard deck of cards and private operations.

In Section 2, basic notations and the private operations introduced in [50] are shown. Section 3 shows logical AND, copy, and logical XOR protocols. Section 4 concludes the paper.

2 Preliminaries

2.1 Basic notations

This section gives the notations and basic definitions of card-based protocols with a standard deck of cards. A deck of playing cards consists of 52 distinct mark cards, which are named 1 to 52. The number of each card (for example, 1 is the ace of the spade, and 52 is the king of the club) is common knowledge among the players. The back of all cards is the same $\boxed{?}$. It is impossible to determine the mark in the back of a given card of $\boxed{?}$.

One-bit data is represented by two cards as follows: $\boxed{i}\boxed{j} = 0$ and $\boxed{j}\boxed{i} = 1$ if $i < j$.

One pair of cards that represents one bit $x \in \{0, 1\}$, whose face is down, is called a commitment of x , and denoted as $commit(x)$. It is written as $\underbrace{\boxed{?}\boxed{?}}_x$.

The base of a commitment is the pair of cards used for the commitment. If card i and j ($i < j$) are used to set $commit(x)$, the commitment is written as $commit(x)^{\{i,j\}}$ and written as $\underbrace{\boxed{?}\boxed{?}}_{x^{\{i,j\}}}$. When the base information is obvious or unnecessary, it is not written.

Note that when these two cards are swapped, $commit(\bar{x})^{\{i,j\}}$ can be obtained. Thus, logical negation can be calculated without private operations.

A set of cards placed in a row is called a sequence of cards. A sequence of cards S whose length is n is denoted as $S = s_1, s_2, \dots, s_n$, where s_i is i -th card of the sequence. $S = \underbrace{\boxed{?}}_{s_1} \underbrace{\boxed{?}}_{s_2} \underbrace{\boxed{?}}_{s_3} \dots \underbrace{\boxed{?}}_{s_n}$. A sequence whose length is even is

called an even sequence. $S_1 || S_2$ is a concatenation of sequence S_1 and S_2 .

All protocols are executed by three players, Alice, Bob, and Carol. The players are malicious, that is, they might not obey the rule of the protocols. In the protocols in this paper, a player watches the private operations executed by another player. If a player misbehaves, the watching player detects the malicious action and says that the player misbehaved. The misbehaved player has a punishment for the misbehavior. The detail of the punishment mechanism is out of the scope of this paper. To avoid punishment, players obey the rule of the protocols. Note that the watching player does not output a false misbehavior detection. For the two-color card model, a three-player misbehavior detection protocol without false alarm detection and a four-player misbehavior detection protocol with the ability of false alarm detection were shown [50]. In order to detect false alarms in a standard deck of cards, four players seem to be necessary. False alarm detection is a further study.

There is no collusion among players, otherwise private input data can be easily revealed.

The inputs of the protocols are given in a committed format, that is, the players do not know the input values. The output of the protocol must be given in a committed format so that the result can be used as input for further calculation.

A protocol is secure when the following two conditions are satisfied: (1) If the output cards are not opened, each player obtains no information about the private input values from the view of the protocol for the player (the sequence of the cards opened to the player). (2) When the output cards are opened, each player obtains no additional information about the private input values other than the information by the output of the protocol. For example, if the output cards of an AND protocol for input x and y are opened and the value is 1, the players can know that $(x, y) = (1, 1)$. If the output value is 0, the players must not know whether the input (x, y) is $(0, 0)$, $(0, 1)$, or $(1, 0)$.

2.2 Private operations

We show three private operations introduced in [50]: private random bisection cuts, private reverse cuts, and private reveals.

Primitive 1 (Private random bisection cut)

A private random bisection cut is the following operation on an even sequence $S_0 = s_1, s_2, \dots, s_{2m}$. A player selects a random bit $b \in \{0, 1\}$ and outputs

$$S_1 = \begin{cases} S_0 & \text{if } b = 0 \\ s_{m+1}, s_{m+2}, \dots, s_{2m}, s_1, s_2, \dots, s_m & \text{if } b = 1 \end{cases}$$

In [50], the operation is executed in a place where the other players cannot see. The player must not disclose the bit b .

Note that if the private random cut is executed when $m = 1$ and $S_0 = \text{commit}(x)^{\{i,j\}}$, given $S_0 = \underbrace{\boxed{?} \boxed{?}}_{x^{\{i,j\}}}$, The player's output $S_1 = \underbrace{\boxed{?} \boxed{?}}_{x \oplus b^{\{i,j\}}}$, which is

$$\underbrace{\boxed{?} \boxed{?}}_{x^{\{i,j\}}} \text{ or } \underbrace{\boxed{?} \boxed{?}}_{\bar{x}^{\{i,j\}}}.$$

Note that a private random bisection cut is the same as the random bisection cut [40], but the operation is not executed in public.

Primitive 2 (Private reverse cut)

A private reverse cut is the following operation on an even sequence $S_2 = s_1, s_2, \dots, s_{2m}$ and a bit $b \in \{0, 1\}$. A player outputs

$$S_3 = \begin{cases} S_2 & \text{if } b = 0 \\ s_{m+1}, s_{m+2}, \dots, s_{2m}, s_1, s_2, \dots, s_m & \text{if } b = 1 \end{cases}$$

In [50], the operation is executed in a place where the other players cannot see. The player must not disclose b .

Note that the bit b is not newly selected by the player. This is the difference between the primitive in Primitive 1, where a random bit must be newly selected by the player.

If a player executes a private random bisection cut to S when the random bit is b and then executes a private reverse cut using b , the result is S .

Note that in some protocols below, selecting left m cards is executed after a private reverse cut. The sequence of these two operations is called a private reverse selection. A private reverse selection is the following procedure on an even sequence $S_2 = s_1, s_2, \dots, s_{2m}$ and a bit $b \in \{0, 1\}$. A player outputs

$$S_3 = \begin{cases} s_1, s_2, \dots, s_m & \text{if } b = 0 \\ s_{m+1}, s_{m+2}, \dots, s_{2m} & \text{if } b = 1 \end{cases}$$

Primitive 3 (*Private reveal*) A player privately opens a given committed bit. The player must not disclose the obtained value.

Using the obtained value, the player privately sets a sequence of cards.

Consider the case when Alice executes a private random bisection cut on $\text{commit}(x)$ and Bob executes a private reveal on the bit. Since the committed bit is randomized by the bit b selected by Alice, the opened bit is $x \oplus b$. Even if Bob privately opens the cards, Bob obtains no information about x if b is randomly selected and not disclosed by Alice. Bob must not disclose the obtained value. If Bob discloses the obtained value to Alice, Alice knows the value of the committed bit.

2.3 Opaque commitment pair

An opaque commitment pair is defined as a useful situation for to design a secure protocol using a standard deck of cards [33]. It is a pair of commitments whose bases are unknown to all players. Let us consider the following two commitments using cards i, j, i' , and j' . The left (right) commitment has value x (y), respectively, but it is unknown that (1) the left (right) commitment is made using i and j (i' and j'), respectively, or (2) the left (right) commitment is made using i' and j' (i and j), respectively. Such a pair of commitments is called an opaque commitment pair and written as $\text{commit}(x)^{\{i,j\},\{i',j'\}} || \text{commit}(y)^{\{i,j\},\{i',j'\}}$.

The protocols in this paper use a little different kind of pair, called semi-opaque commitment pair. A player thinks a pair is an opaque commitment pair but another player knows the bases of the commitments. Let us consider the case when a protocol is executed by Alice and Bob. Bob privately makes the pair of commitments with the knowledge of x and y . For example, Bob randomly selects a bit $b \in \{0, 1\}$ and

$$S = \begin{cases} \text{commit}(x)^{\{i,j\}} || \text{commit}(y)^{\{i',j'\}} & \text{if } b = 0 \\ \text{commit}(x)^{\{i',j'\}} || \text{commit}(y)^{\{i,j\}} & \text{if } b = 1 \end{cases}$$

then $S = \text{commit}(x)^{\{i,j\},\{i',j'\}} || \text{commit}(y)^{\{i,j\},\{i',j'\}}$ for Alice. Such a pair is called semi-opaque commitment pair and written as $\text{commit}(x)^{\{i,j\},\{i',j'\}} |_{\text{Alice}} || \text{commit}(y)^{\{i,j\},\{i',j'\}} |_{\text{Alice}}$, where the name(s) of the players who think the pair as a opaque commitment pair is written. Note that a name is not written does not mean the player knows the bases of the commitments. For example, the above example says nothing about whether Bob knows the bases or not. Note that the name of the player is written with the initial when it is not ambiguous.

2.4 Space and time complexities

The space complexity of card-based protocols is evaluated by the number of cards. Minimizing the number of cards is discussed in many works.

The number of rounds was proposed as a criterion to evaluate the time complexity of card-based protocols using private operations [51]. The first round begins from the initial state. In most protocols, a player initially has all cards, but the definition assumes general cases when each player initially has some number of cards. The first round is (possibly parallel) local executions by each player using the cards initially given to each player. It ends at the instant when no further local execution is possible without receiving cards from another player. The local executions in each round include sending cards to some other players but do not include receiving cards.

The $i(> 1)$ -th round begins with receiving all the cards sent during the $(i-1)$ -th round. Each player executes local executions using the received cards and the cards left to the player at the end of the $(i-1)$ -th round. Each player executes local executions until no further local execution is possible without receiving cards from another player. We can define the number of rounds and average rounds. The number of rounds of a protocol is the maximum number of rounds necessary to output the result among all possible inputs and random values. For randomized (Las Vegas) protocols, the average round is the average number of rounds necessary to output the result.

Let us show an example of a protocol execution, its space complexity, and time complexity with the conventional two-color card model. In the two-color card model, there are two kinds of marks, \spadesuit and \heartsuit . One-bit data is represented by two cards as follows: $\spadesuit\heartsuit = 0$ and $\heartsuit\spadesuit = 1$.

Protocol 1 (*AND protocol in [50]*)

Input: $\text{commit}(x)$ and $\text{commit}(y)$.

Output: $\text{commit}(x \wedge y)$.

1. Alice executes a private random bisection cut on $\text{commit}(x)$. Let the output be $\text{commit}(x')$. Alice sends $\text{commit}(x')$ and $\text{commit}(y)$ to Bob.
2. Bob executes a private reveal on $\text{commit}(x')$. Bob privately sets

$$S_2 = \begin{cases} \text{commit}(y) || \text{commit}(0) & \text{if } x' = 1 \\ \text{commit}(0) || \text{commit}(y) & \text{if } x' = 0 \end{cases}$$

and sends S_2 to Alice.

3. Alice executes a private reverse selection on S_2 using the bit b generated in the private random bisection cut. Let the obtained sequence be S_3 . Alice outputs S_3 .

The AND protocol realizes the following equation.

$$x \wedge y = \begin{cases} y & \text{if } x = 1 \\ 0 & \text{if } x = 0 \end{cases}$$

The correctness of the protocol is shown in [50]. The number of cards is four since the cards of $\text{commit}(x')$ are re-used to set $\text{commit}(0)$.

Let us consider the time complexity of the protocol. The first round ends at the instant when Alice sends $\text{commit}(x')$ and $\text{commit}(y)$ to Bob. The second round begins with receiving the cards by Bob. The second round ends at the instant when Bob sends S_2 to Alice. The third round begins with receiving the cards by Alice. The number of rounds of this protocol is three.

Since each operation is relatively simple, the dominating time to execute protocols with private operations is the time to send cards between players and set up so that the cards are not seen by the other players. Thus the number of rounds is the criterion to evaluate the time complexity of card-based protocols with private operations. If the local execution needs many operations, for example, $O(n)$ operations where n is the size of the problem, we might need another criterion to consider the cost of local executions.

2.5 Problems with a standard deck of cards

The above AND protocol cannot be executed as it is with a standard deck of cards.

The protocol uses the property that all \heartsuit cards (\clubsuit cards) are indistinguishable. Even if the final cards are opened to see the result, it is impossible to know that the opened cards are the cards of $\text{commit}(y)$ or $\text{commit}(0)$. If it is possible to detect the above information, the value of x is known to the players.

Consider the case when the encoding rule $\boxed{i}\boxed{j} = 0, \boxed{j}\boxed{i} = 1$ if $i < j$ is used to the standard deck of playing cards. Suppose that $x = 1$ and $y = 0$. When two inputs are given as $\text{commit}(x)^{\{1,2\}}$ and $\text{commit}(y)^{\{3,4\}}$, $\text{commit}(0)$ and $\text{commit}(y)$ are set as $\text{commit}(0)^{\{1,2\}}$ and $\text{commit}(y)^{\{3,4\}}$, respectively at Step 2. Since $x = 1$, the result is $\text{commit}(y)^{\{3,4\}}$. When the cards are opened to see the result, the cards are 3 and 4. The players can know that y is selected as the output, thus x must be 1. This execution also reveals the information of inputs from the base of the commitments.

When we design a protocol with a standard deck of cards, we must consider the information leakage from the base of the commitment.

2.6 AND protocol by two semi-honest players

If the players are semi-honest, we can execute AND/XOR/copy protocols using a standard deck of cards with the minimum number of cards by two players. We show a base-fixed protocol and AND protocol in [25] since the protocols in this paper execute the protocols with three players. Note that base-fixed protocols that do not use private operations were shown in [14, 33].

Protocol 2 (Base-fixed protocol) [25]

Input: $\text{commit}(x)^{\{1,2\},\{3,4\}|A}| \text{commit}(y)^{\{1,2\},\{3,4\}|A}$.

Output: $\text{commit}(x)^{\{1,2\}}$.

1. Bob executes a private random bisection cut on both pairs using two different random bits $br_1, br_2 \in \{0, 1\}$. The result $S_1 = \text{commit}(x \oplus br_1)^{\{1,2\},\{3,4\}} || \text{commit}(y \oplus br_2)^{\{1,2\},\{3,4\}}$. Bob sends S_1 to Alice.
2. Alice executes a private reveal on S_1 . Alice sees $x \oplus br_1$ and $y \oplus br_2$. Alice makes $S_2 = \text{commit}(x \oplus br_1)^{\{1,2\}}$ and sends it to Bob.
3. Bob executes a private reverse cut using br_1 on S_2 . The result is $\text{commit}(x)^{\{1,2\}}$.

Note that input y is a secret value.

In this protocol, Alice knows the bases of the input commitments in Step 2. The protocol can be used only when this information leakage does not cause a security problem, for example, the bases are randomly set by Bob. The example case is as follows. Initially, Bob knows the relation between the bases and the private input values. If the result is opened and the base becomes public, Bob knows the private input value from the base of the result. Thus, Bob first randomizes the relation between the bases and the values. Since Bob changed the base, Bob still knows the relation between the bases and the values, but Alice cannot know the relation because of the randomization by Bob. Thus, when Alice privately opens the cards, Alice knows no information from the base of the cards. Alice privately opens the cards and fixes the base of the output. When the base is fixed, the base of the output becomes unknown to Bob. Therefore, when the final output is opened, no information about private input value is known to the players from the base.

Next, we show AND protocol by two semi-honest players. Note that the protocol is modified from the one in [25]. Though the order of randomizations is changed, the main idea of the protocol is unchanged.

Protocol 3 (AND protocol by two semi-honest players) [25]

Input: $\text{commit}(x)^{\{1,2\}}$ and $\text{commit}(y)^{\{3,4\}}$.

Output: $\text{commit}(x \wedge y)^{\{1,2\}}$.

1. Alice executes a private random bisection cut on $\text{commit}(x)^{\{1,2\}}$ using random bit a_1 . Alice sends the results, $S_1 = \text{commit}(x \oplus a_1)^{\{1,2\}}$ and $S_2 = \text{commit}(y)^{\{3,4\}}$ to Bob.
2. Bob executes a private reveal on S_1 . Bob sees $x \oplus a_1$. Bob privately sets

$$S_{3,0} = \begin{cases} \text{commit}(0)^{\{1,2\}} || \text{commit}(y)^{\{3,4\}} & \text{if } x \oplus a_1 = 0 \\ \text{commit}(y)^{\{3,4\}} || \text{commit}(0)^{\{1,2\}} & \text{if } x \oplus a_1 = 1 \end{cases}$$

Bob sends $S_{3,0}$ to Alice.

3. Alice executes private random bisection cuts on each of pairs in $S_{3,0}$ using two distinct random bits a_2 and a_3 . Let the result be $S_{3,1}$.

$$S_{3,1} = \begin{cases} \text{commit}(0 \oplus a_2)^{\{1,2\}} || \text{commit}(y \oplus a_3)^{\{3,4\}} & \text{if } x \oplus a_1 = 0 \\ \text{commit}(y \oplus a_2)^{\{3,4\}} || \text{commit}(0 \oplus a_3)^{\{1,2\}} & \text{if } x \oplus a_1 = 1 \end{cases}$$

Alice sends $S_{3,1}$ to Bob.

4. Bob randomly selects bit $b_1 \in \{0, 1\}$. Bob reveals $S_{3,1}$ and exchanges the bases of the two commitments if $b_1 = 1$. Let the result be $S_{3,2}$.

$$S_{3,2} = \begin{cases} \text{commit}(0 \oplus a_2)^{\{1,2\},\{3,4\}|A} || \text{commit}(y \oplus a_3)^{\{1,2\},\{3,4\}|A} & \text{if } x \oplus a_1 = 0 \\ \text{commit}(y \oplus a_2)^{\{1,2\},\{3,4\}|A} || \text{commit}(0 \oplus a_3)^{\{1,2\},\{3,4\}|A} & \text{if } x \oplus a_1 = 1 \end{cases}$$

Bob sends $S_{3,2}$ to Alice.

5. Alice executes private reverse cuts on the two pairs of $S_{3,2}$ using a_2 and a_3 , respectively. Let the result be S_4 .

$$S_4 = \begin{cases} \text{commit}(0)^{\{1,2\},\{3,4\}|A} || \text{commit}(y)^{\{1,2\},\{3,4\}|A} & \text{if } x \oplus a_1 = 0 \\ \text{commit}(y)^{\{1,2\},\{3,4\}|A} || \text{commit}(0)^{\{1,2\},\{3,4\}|A} & \text{if } x \oplus a_1 = 1 \end{cases}$$

Alice then executes a private reverse selection on S_4 using a_1 . Let S_5 be the result and the remaining two cards be S_6 . The result $S_5 = \text{commit}(y)^{\{1,2\},\{3,4\}|A}$ if $(a_1 = 0 \text{ and } x \oplus a_1 = 1)$ or $(a_1 = 1 \text{ and } x \oplus a_1 = 0)$. The condition equals $x = 1$.

$S_5 = \text{commit}(0)^{\{1,2\},\{3,4\}|A}$ if $(a_1 = 0 \text{ and } x \oplus a_1 = 0)$ or $(a_1 = 1 \text{ and } x \oplus a_1 = 1)$. The condition equals $x = 0$. Thus,

$$\begin{aligned} S_5 &= \begin{cases} \text{commit}(y)^{\{1,2\},\{3,4\}|A} & \text{if } x = 1 \\ \text{commit}(0)^{\{1,2\},\{3,4\}|A} & \text{if } x = 0 \end{cases} \\ &= \text{commit}(x \wedge y)^{\{1,2\},\{3,4\}|A} \end{aligned}$$

Alice sends S_5 and S_6 to Bob.

6. Bob and Alice execute Protocol 2 (Base-fixed protocol) to $S_5 || S_6$. Then they obtain $\text{commit}(x \wedge y)^{\{1,2\}}$.

The correctness and security of the protocol are shown in [25].

3 AND, XOR, and copy with three malicious players

This section shows our new protocols for AND, XOR, and copy executed by three malicious players. Any malicious action during private operations is detected by a watching player, thus the malicious actions are prohibited if there is no collusion between players.

Bob watches Alice's operations, Carol watches Bob's operations, and Alice watches Carol's operations. All operations are executed in the following manner. Initially, all players are in the same room. If the next operation is executed by Alice, first, Carol exits the room. Then, Alice executes the private operations in front of Bob. Thus, Bob knows all private values. For example, if Alice executes a private random bisection cut, Bob knows the random bit Alice selected. If Alice executes a private reveal, Bob knows the value of the cards Alice opened. If Alice misbehaves, Bob detects the fact and terminates the protocol execution. If there is no misbehavior, Alice's private operations are correctly finished. Then

Carol comes back to the room and they execute the next step of the protocol. If the next private operation is executed by Bob(Carol), Alice(Bob) exits from the room, Bob(Carol) executes the private operation in front of Carol(Alice), and Alice(Bob) comes back to the room, respectively.

In the following protocol descriptions, we just write “Alice executes a private operation” to mean “Carol exits the room, Alice executes a private operation in front of Bob, and Carol comes back to the room” for simplicity.

Before we show the protocols, we show a subroutine to fix the base of a given commitment.

3.1 Base-fixed protocol with three players

We show a base-fixed protocol with two inputs $\text{commit}(x)$ and $\text{commit}(y)$. The base of $\text{commit}(x)$ is fixed to $\{1, 2\}$. In the following protocol, the second input value y is not used as the output, but the value must be kept secret.

The protocol needs private reveals and the values of cards are seen. Before a player sees a value of $\text{commit}(x)$ and sets cards according to the value, the value must be randomized to hide the value. In the protocol below, Alice sees the value, thus the value must be randomized by the other players. One-player randomization is not enough to hide the private value. Suppose that a player executes a randomization in advance. They obtain $\text{commit}(x \oplus r)$ and then Alice executes a private reveal. Since Bob watches Alice’s execution, Bob knows $x \oplus r$. If the randomization r is executed by Bob, Bob knows r and $x \oplus r$ and Bob knows secret value x . Then consider the case when the randomization is executed by Carol. Alice watches Carol’s private operation and knows r . Since Alice knows $x \oplus r$ and r , Alice knows the secret value x . Therefore, one-player randomization is not enough to hide the private value, and two-player randomizations are necessary. The value must be randomized by Bob and Carol in advance.

Note that the bases of the input commitments are leaked to Alice and Bob during the execution. The protocol can be used only if the information leakage does not cause a security problem, for example, the bases are randomly set by some other player.

Protocol 4 (*Three player base-fixed protocol*)

Input: $\text{commit}(x)^{\{1,2\},\{3,4\}|A} || \text{commit}(y)^{\{1,2\},\{3,4\}|A}$.

Output: $\text{commit}(x)^{\{1,2\}}$.

1. Bob executes a private random bisection cut on each pair using two random bits br_1 and br_2 , respectively. The result $S_1 = \text{commit}(x \oplus br_1)^{\{1,2\},\{3,4\}|A} || \text{commit}(y \oplus br_2)^{\{1,2\},\{3,4\}|A}$.
2. Carol executes a private random bisection cut on each pair using two random bits cr_1 and cr_2 , respectively. The result $S_2 = \text{commit}(x \oplus br_1 \oplus cr_1)^{\{1,2\},\{3,4\}|A} || \text{commit}(y \oplus br_2 \oplus cr_2)^{\{1,2\},\{3,4\}|A}$.
3. Alice executes a private reveal on both pairs of S_2 . Alice makes $S_3 = \text{commit}(x \oplus br_1 \oplus cr_1)^{\{1,2\}}$.

4. Bob executes a private reverse cut using br_1 on S_3 . The result $S_4 = \text{commit}(x \oplus cr_1)^{\{1,2\}}$.
5. Carol executes a private reverse cut using cr_1 on S_4 . The result is $\text{commit}(x)^{\{1,2\}}$.

Theorem 1. *The input values are private in the base-fixed protocol.*

Proof. Alice sees $x \oplus br_1 \oplus cr_1$ and $y \oplus br_2 \oplus cr_2$ in Step 3. Since Alice watches Carol's private operations, Alice sees cr_1 and cr_2 in Step 2. Alice obtains no information about x and y since br_1 and br_2 are unknown to Alice.

Bob knows br_1 and br_2 in Step 1. Since Bob watches Alice's private operations, Bob sees $x \oplus br_1 \oplus cr_1$ and $y \oplus br_2 \oplus cr_2$ in Step 3. Bob obtains no information about x and y since cr_1 and cr_2 are unknown to Bob.

Carol knows cr_1 and cr_2 in Step 2. Since Carol watches Bob's private operations, Carol sees br_1 and br_2 in Step 1. Carol obtains no information about x and y . \square

3.2 AND protocol

In the following AND, copy, and XOR protocols, the bases of the output commitments are fixed to avoid information leakage from the bases when the outputs are opened.

The outline to execute by three players is as follows. The protocol in [25] has two randomizations. The first is the randomization of the bases of the two input values. The second is the randomization of the input values.

Carol executes private reveals in the following protocol. By the same argument written in the description of the base-fixed protocol, the value must be randomized by the other players in advance. Suppose that Alice and Bob use random bits a and b to randomize x , respectively. After Carol's private operation using $x \oplus a \oplus b$, Alice and Bob execute a private reverse cut using a and b , respectively to undo the randomizations. Such randomizations are executed before every private reveals in the protocol.

Next, we need to randomize the bases of the two pairs to hide the relation between the output and inputs. Initially, $\text{commit}(0)$ is made using $\{1, 2\}$ and $\text{commit}(y)$ is made using $\{3, 4\}$. Suppose that the output of AND is $\text{commit}(0)$. It means that $x = 0$. If no base change is executed, the base $\{1, 2\}$ of the output reveal $x = 0$. Thus the randomization of bases is necessary. If the base randomization is executed by one player, the private information is known to one player just like the case of randomization of values. Thus the base randomization must be executed by two players.

The detailed protocol is shown below. Note that for the simplicity of description, we write $S \oplus b$ to mean the pair that the left and the right card are swapped if $b = 1$. If $S = \text{commit}(x)$, $S \oplus b$ means $\text{commit}(x \oplus b)$.

Protocol 5 (*Three player AND protocol*)

Input: $\text{commit}(x)^{\{1,2\}}$ and $\text{commit}(y)^{\{3,4\}}$.

Output: $\text{commit}(x \wedge y)^{\{1,2\}}$.

1. Alice executes a private random bisection cut on $\text{commit}(x)^{\{1,2\}}$ using random bit a_1 . The result is $S_1 = \text{commit}(x \oplus a_1)^{\{1,2\}}$.
2. Bob executes a private random bisection cut on S_1 using random bit b_1 . The result is $S_2 = \text{commit}(x \oplus a_1 \oplus b_1)^{\{1,2\}}$.
3. Carol executes a private reveal on S_2 . Carol sees $x \oplus a_1 \oplus b_1$. According to the value, Carol sets $S_3||S_4$ as

$$S_3||S_4 = \begin{cases} \text{commit}(0)^{\{1,2\}}||\text{commit}(y)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \\ \text{commit}(y)^{\{3,4\}}||\text{commit}(0)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \end{cases}$$

The cards of S_2 are reused to set $\text{commit}(0)$.

4. Alice executes a private random bisection cut on S_3 and S_4 using random bit a_2 and a_3 , respectively. The result is $S_3 \oplus a_2||S_4 \oplus a_3$.
5. Bob executes a private random bisection cut on $S_3 \oplus a_2$ and $S_4 \oplus a_3$ using random bit b_2 and b_3 , respectively. The result is $S_3 \oplus a_2 \oplus b_2||S_4 \oplus a_3 \oplus b_3$.
6. Carol randomly selects bit $c_1 \in \{0,1\}$. Carol executes private reveals on the two pairs and exchanges the bases of two pairs if $c_1 = 1$. Then, Carol executes private random bisection cuts on the two pairs using random bits $c_2, c_3 \in \{0,1\}$. Let the result be $S_5||S_6 =$

$$\begin{cases} \text{commit}(0 \oplus a_2 \oplus b_2 \oplus c_2)^{\{1,2\}}||\text{commit}(y \oplus a_3 \oplus b_3 \oplus c_3)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \text{ and } c_1 = 0 \\ \text{commit}(0 \oplus a_2 \oplus b_2 \oplus c_2)^{\{3,4\}}||\text{commit}(y \oplus a_3 \oplus b_3 \oplus c_3)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \text{ and } c_1 = 1 \\ \text{commit}(y \oplus a_2 \oplus b_2 \oplus c_2)^{\{3,4\}}||\text{commit}(0 \oplus a_3 \oplus b_3 \oplus c_3)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \text{ and } c_1 = 0 \\ \text{commit}(y \oplus a_2 \oplus b_2 \oplus c_2)^{\{1,2\}}||\text{commit}(0 \oplus a_3 \oplus b_3 \oplus c_3)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \text{ and } c_1 = 1 \end{cases}$$

7. Bob executes private reveals on $S_5||S_6$. Bob randomly selects bit $b_4 \in \{0,1\}$. Bob exchanges the bases of the two commitments if $b_4 = 1$. Then Bob executes private reverse cuts on the pairs using b_2 and b_3 , respectively. The result is

$$\begin{cases} \text{commit}(0 \oplus a_2 \oplus c_2)^{\{1,2\}}||\text{commit}(y \oplus a_3 \oplus c_3)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \text{ and } c_1 \oplus b_4 = 0 \\ \text{commit}(0 \oplus a_2 \oplus c_2)^{\{3,4\}}||\text{commit}(y \oplus a_3 \oplus c_3)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y \oplus a_2 \oplus c_2)^{\{1,2\}}||\text{commit}(0 \oplus a_3 \oplus c_3)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y \oplus a_2 \oplus c_2)^{\{3,4\}}||\text{commit}(0 \oplus a_3 \oplus c_3)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \text{ and } c_1 \oplus b_4 = 0 \end{cases}$$

8. Carol executes private reverse cuts on the pairs using c_2 and c_3 , respectively.
9. Alice executes a private reverse cut on each of the pairs using a_2 and a_3 , respectively.

Let $S_7 || S_8$ be the result after the two private reverse cuts. $S_7 || S_8 =$

$$\begin{cases} \text{commit}(0)^{\{1,2\}} || \text{commit}(y)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \text{ and } c_1 \oplus b_4 = 0 \\ \text{commit}(0)^{\{3,4\}} || \text{commit}(y)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 0 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y)^{\{1,2\}} || \text{commit}(0)^{\{3,4\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y)^{\{3,4\}} || \text{commit}(0)^{\{1,2\}} & \text{if } x \oplus a_1 \oplus b_1 = 1 \text{ and } c_1 \oplus b_4 = 0 \end{cases}$$

Alice then executes a private reverse cut using a_1 . The result is

$$\begin{cases} \text{commit}(0)^{\{1,2\}} || \text{commit}(y)^{\{3,4\}} & \text{if } x \oplus b_1 = 0 \text{ and } c_1 \oplus b_4 = 0 \\ \text{commit}(0)^{\{3,4\}} || \text{commit}(y)^{\{1,2\}} & \text{if } x \oplus b_1 = 0 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y)^{\{1,2\}} || \text{commit}(0)^{\{3,4\}} & \text{if } x \oplus b_1 = 1 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y)^{\{3,4\}} || \text{commit}(0)^{\{1,2\}} & \text{if } x \oplus b_1 = 1 \text{ and } c_1 \oplus b_4 = 0 \end{cases}$$

10. Bob executes a private reverse selection using b_1 . Let T_0 be the result and T_1 be the pair that is not selected.

$$T_0 = \begin{cases} \text{commit}(0)^{\{1,2\}} & \text{if } x = 0 \text{ and } c_1 \oplus b_4 = 0 \\ \text{commit}(0)^{\{3,4\}} & \text{if } x = 0 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y)^{\{1,2\}} & \text{if } x = 1 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(y)^{\{3,4\}} & \text{if } x = 1 \text{ and } c_1 \oplus b_4 = 0 \end{cases}$$

The value of T_0 is $\text{commit}(x \wedge y)$ and its base is randomly set by $c_1 \oplus b_4$. Since Alice does not know b_4 , $T_0 = \text{commit}(x \wedge y)^{\{1,2\},\{3,4\}}|^A$. Similarly,

$$T_1 = \begin{cases} \text{commit}(y)^{\{3,4\}} & \text{if } x = 0 \text{ and } c_1 \oplus b_4 = 0 \\ \text{commit}(y)^{\{1,2\}} & \text{if } x = 0 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(0)^{\{3,4\}} & \text{if } x = 1 \text{ and } c_1 \oplus b_4 = 1 \\ \text{commit}(0)^{\{1,2\}} & \text{if } x = 1 \text{ and } c_1 \oplus b_4 = 0 \end{cases}$$

The value of T_1 is $\text{commit}(\bar{x} \wedge y)$ and its base is randomly set by $c_1 \oplus b_4$. $T_1 = \text{commit}(\bar{x} \wedge y)^{\{1,2\},\{3,4\}}|^A$.

Next, execute the base-fixed protocol on these pairs. Then the players obtain $\text{commit}(x \wedge y)^{\{1,2\}}$.

The protocol is 14 rounds since the first step of the base-fixed protocol is executed by Bob. The number of cards is four. Since four cards are necessary to input x and y , the number of cards is the minimum. The correctness of the output value is shown in the protocol, thus we show the security.

Theorem 2. *The AND protocol is secure.*

Proof. First, we show the security for Bob. Since Bob watches Alice, Bob knows the values in Steps 1, 2, 4, 5, 7, 9, 10 and Steps 1, 3, and 4 of the base-fixed protocol. Bob thus sees a_i , b_i , br_i , $x \wedge y \oplus br_1 \oplus cr_1$, $\bar{x} \wedge y \oplus br_2 \oplus cr_2$, and $((0 \oplus a_2 \oplus b_2 \oplus c_2 \text{ and } y \oplus a_3 \oplus b_3 \oplus c_3 \text{ if } x \oplus a_1 \oplus b_1 = 0) \text{ or } (y \oplus a_2 \oplus b_2 \oplus c_2 \text{ and } y \oplus a_3 \oplus b_3 \oplus c_3 \text{ if } x \oplus a_1 \oplus b_1 = 1))$. Bob can obtain no information about

the secret input and output values since the values of cards are randomized by c_2, c_3, cr_1 , or cr_2 that are unknown to Bob.

From the bases of the cards, Bob obtains no information since the bases of two randomized values, $0 \oplus a_2 \oplus b_2 \oplus c_2$ and $y \oplus a_3 \oplus b_3 \oplus c_3$ (or $y \oplus a_2 \oplus b_2 \oplus c_2$ and $0 \oplus a_3 \oplus b_3 \oplus c_3$) are randomized by unknown value c_1 . The bases of two randomized values, $x \wedge y \oplus br_1 \oplus cr_1$ and $\bar{x} \wedge y \oplus br_2 \oplus cr_2$ are randomized by $c_1 \oplus b_4$ but c_1 is unknown to Bob.

Next, we show the security for Carol. Since Carol watches Bob, Carol knows the values in Steps 2, 3, 5, 6, 7, 8, 10 and Steps 1, 2, 4, and 5 of the base-fixed protocol. Carol thus sees $b_i, c_i, br_i, cr_i, x \oplus a_1 \oplus b_1, 0 \oplus a_2 \oplus b_2, y \oplus a_3 \oplus b_3$, and $((0 \oplus a_2 \oplus b_2 \oplus c_2 \text{ and } y \oplus a_3 \oplus b_3 \oplus c_3 \text{ if } x \oplus a_1 \oplus b_1 = 0) \text{ or } (y \oplus a_2 \oplus b_2 \oplus c_2 \text{ and } y \oplus a_3 \oplus b_3 \oplus c_3 \text{ if } x \oplus a_1 \oplus b_1 = 1))$. From the cards, Carol obtains no information about the secret input values since the values are randomized by unknown values a_1, a_2 , or a_3 .

About the bases of the cards, Carol knows whether she set $commit(0)^{\{1,2\}} || commit(y)^{\{3,4\}}$ or $commit(0)^{\{3,4\}} || commit(y)^{\{1,2\}}$ in Step 3 and both two base randomizations by Carol and Bob, thus she knows whether $S_7 || S_8$ is $commit(0) || commit(y)$ or $commit(y) || commit(0)$ and each commitment is made by $\{1, 2\}$ or $\{3, 4\}$. However, Carol cannot see the private reverse cut by Alice in Step 9, Carol cannot know which pair is selected as the final result thus no information is known to Carol. Since Alice sets the base to $\{1, 2\}$, Carol cannot know information about the secret input values from the base of the final result.

Last, we show the security for Alice. Alice knows the values in Steps 1, 3, 4, 6, 8, 9, and Steps 2, 3, and 5 of the base-fixed protocol. Alice thus sees $a_i, c_i, cr_i, x \oplus a_1 \oplus b_1, x \wedge y \oplus br_1 \oplus cr_1$, and $\bar{x} \wedge y \oplus br_2 \oplus cr_2$, and $((0 \oplus a_2 \oplus b_2 \oplus c_2 \text{ and } y \oplus a_3 \oplus b_3 \oplus c_3 \text{ if } x \oplus a_1 \oplus b_1 = 0) \text{ or } (y \oplus a_2 \oplus b_2 \oplus c_2 \text{ and } y \oplus a_3 \oplus b_3 \oplus c_3 \text{ if } x \oplus a_1 \oplus b_1 = 1))$. From the revealed cards, Alice obtains no information about the secret input and output values since each value is randomized by unknown value b_1, b_2, b_3, br_1 , or br_2 .

Alice knows whether $S_3 || S_4$ is $commit(0)^{\{1,2\}} || commit(y)^{\{3,4\}}$ or $commit(y)^{\{3,4\}} || commit(0)^{\{1,2\}}$. Alice also knows the bases of each pair of $S_5 || S_6$. Though Alice knows the bases of $S_5 || S_6$, Bob's base change using b_4 is unknown to Alice. Thus, the bases of T_0 and T_1 are random for Alice because of b_4 . When Alice sees $x \wedge y \oplus br_1 \oplus cr_1$ and $\bar{x} \wedge y \oplus br_2 \oplus cr_2$ in Step 3 of the base-fixed protocol, the bases are randomized by $c_1 \oplus b_4$. Thus, Alice obtains no information from the bases of the commitments. \square

3.3 Copy protocol

Next, we show a new copy protocol by three players.

Protocol 6 (*Three player copy protocol*)

Input: $commit(x)^{\{1,2\}}$ and two new cards 3 and 4.

Output: $commit(x)^{\{1,2\}}$ and $commit(x)^{\{3,4\}}$

1. Alice executes a private random bisection cut on $commit(x)^{\{1,2\}}$ using random bit a . The result is $commit(x \oplus a)^{\{1,2\}}$.

2. Bob executes a private random bisection cut on $\text{commit}(x \oplus a)^{\{1,2\}}$ using random bit b . The result is $\text{commit}(x \oplus a \oplus b)^{\{1,2\}}$.
3. Carol executes a private reveal on $\text{commit}(x \oplus a \oplus b)^{\{1,2\}}$ and sees $x \oplus a \oplus b$. Carol privately makes $\text{commit}(x \oplus a \oplus b)^{\{3,4\}}$.
4. Alice executes a private reverse cut on each of the pairs using a . The result is $\text{commit}(x \oplus b)^{\{1,2\}}$ and $\text{commit}(x \oplus b)^{\{3,4\}}$.
5. Bob executes a private reverse cut on each of the pairs using b . The result is $\text{commit}(x)^{\{1,2\}}$ and $\text{commit}(x)^{\{3,4\}}$.

The protocol is five rounds.

Theorem 3. *The copy protocol is secure.*

Proof. Alice sees a and $x \oplus a \oplus b$. Bob sees a and b . Carol sees b and $x \oplus a \oplus b$. Thus no player knows the secret value x . \square

3.4 XOR protocol

Since AND and copy protocols are shown and NOT is obvious, any Boolean function can be realized by the combination of these protocols. XOR protocol is shown because the realization of XOR is simple.

Protocol 7 (*Three player XOR protocol*)

Input: $\text{commit}(x)^{\{1,2\}}$ and $\text{commit}(y)^{\{3,4\}}$.

Output: $\text{commit}(x \oplus y)^{\{1,2\}}$.

1. Alice executes a private random bisection cut on $\text{commit}(x)^{\{1,2\}}$ and $\text{commit}(y)^{\{3,4\}}$ using the same random bit $a \in \{0, 1\}$. The result is $\text{commit}(x \oplus a)^{\{1,2\}}$ and $\text{commit}(y \oplus a)^{\{3,4\}}$.
2. Bob executes a private random bisection cut on $\text{commit}(x \oplus a)^{\{1,2\}}$ and $\text{commit}(y \oplus a)^{\{3,4\}}$ using the same random bit $b \in \{0, 1\}$. The result is $\text{commit}(x \oplus a \oplus b)^{\{1,2\}}$ and $\text{commit}(y \oplus a \oplus b)^{\{3,4\}}$.
3. Carol executes a private reveal on $\text{commit}(y \oplus a \oplus b)^{\{3,4\}}$. Carol sees $y \oplus a \oplus b$. Carol executes a private reverse cut on $\text{commit}(x \oplus a \oplus b)^{\{1,2\}}$ using $y \oplus a \oplus b$. The result is $\text{commit}((x \oplus a \oplus b) \oplus (y \oplus a \oplus b))^{\{1,2\}} = \text{commit}(x \oplus y)^{\{1,2\}}$.

The protocol is three rounds. The protocol uses four cards. Since any protocol needs four cards to input x and y , the number of cards is the minimum.

Theorem 4. *The XOR protocol is secure.*

Proof. Alice sees a and $y \oplus a \oplus b$. Bob sees a and b . Carol sees b and $y \oplus a \oplus b$. Thus no player knows the secret value y . \square

4 Conclusion

This paper showed AND, XOR, and copy protocols with private operations that use a standard deck of cards when the players are malicious. The protocols are executed by three players and each player watches another player to prevent malicious private operations. The numbers of cards used by the protocols are the minimum. One of the remaining problems is obtaining protocols with two players with the help of additional tools such as envelopes. Another remaining problem is a false alarm detection protocol.

References

1. Abe, Y., Iwamoto, M., Ohta, K.: How to detect malicious behaviors in a card-based majority voting protocol with three inputs. In: 2020 International Symposium on Information Theory and Its Applications (ISITA). pp. 377–381. IEEE (2020)
2. Abe, Y., Hayashi, Y.i., Mizuki, T., Sone, H.: Five-card and computations in committed format using only uniform cyclic shuffles. *New Generation Computing* **39**, 97–114 (2021)
3. den Boer, B.: More efficient match-making and satisfiability the five card trick. In: Proc. of EUROCRYPT ’89, LNCS Vol. 434. pp. 208–217 (1990)
4. Bultel, X., Dreier, J., Dumas, J.G., Lafourcade, P., Miyahara, D., Mizuki, T., Nagao, A., Sasaki, T., Shinagawa, K., Sone, H.: Physical zero-knowledge proof for makaro. In: Proc. of 20th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2018), LNCS Vol.11201. pp. 111–125 (2018)
5. Cheung, E., Hawthorne, C., Lee, P.: Cs 758 project: Secure computation with playing cards (2013), http://cdchawthorne.com/writings/secure_playing_cards.pdf
6. Dumas, J.G., Lafourcade, P., Miyahara, D., Mizuki, T., Sasaki, T., Sone, H.: Interactive physical zero-knowledge proof for norinori. In: Proc. of 25th International Computing and Combinatorics Conference(COCOON 2019), LNCS Vol. 11653. pp. 166–177. Springer (2019)
7. Dvořák, P., Koucký, M.: Barrington plays cards: The complexity of card-based protocols. arXiv preprint arXiv:2010.08445 (2020)
8. Francis, D., Aljunid, S.R., Nishida, T., Hayashi, Y., Mizuki, T., Sone, H.: Necessary and sufficient numbers of cards for securely computing two-bit output functions. In: Proc. of Second International Conference on Cryptology and Malicious Security(Mycrypt 2016), LNCS Vol. 10311. pp. 193–211 (2017)
9. Hashimoto, Y., Nuida, K., Shinagawa, K., Inamura, M., Hanaoka, G.: Toward finite-runtime card-based protocol for generating hidden random permutation without fixed points. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **101-A**(9), 1503–1511 (2018)
10. Hashimoto, Y., Shinagawa, K., Nuida, K., Inamura, M., Hanaoka, G.: Secure grouping protocol using a deck of cards. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **101**(9), 1512–1524 (2018)
11. Ibaraki, T., Manabe, Y.: A more efficient card-based protocol for generating a random permutation without fixed points. In: Proc. of 3rd Int. Conf. on Mathematics and Computers in Sciences and in Industry (MCSI 2016). pp. 252–257 (2016)
12. Ishikawa, R., Chida, E., Mizuki, T.: Efficient card-based protocols for generating a hidden random permutation without fixed points. In: Proc. of 14th International Conference on Unconventional Computation and Natural Computation(UCNC 2015), LNCS Vol. 9252. pp. 215–226 (2015)

13. Kastner, J., Koch, A., Walzer, S., Miyahara, D., Hayashi, Y., Mizuki, T., Sone, H.: The minimum number of cards in practical card-based protocols. In: Proc. of Asiacrypt 2017, Part III, LNCS Vol. 10626. pp. 126–155 (2017)
14. Koch, A.: Cryptographic protocols from physical assumptions. Ph.D. thesis, Karlsruhe Institute of Technology, Germany (2019)
15. Koch, A.: The landscape of optimal card-based protocols. *Mathematical Cryptology* **1**(2), 115–131 (2021)
16. Koch, A., Schrempp, M., Kirsten, M.: Card-based cryptography meets formal verification. *New Generation Computing* **39**(1), 115–158 (2021)
17. Koch, A., Walzer, S.: Foundations for actively secure card-based cryptography. In: Proc. of 10th International Conference on Fun with Algorithms (FUN 2020). Schloss Dagstuhl-Leibniz-Zentrum für Informatik (2020)
18. Koch, A., Walzer, S.: Private function evaluation with cards. *New Generation Computing* **40**(1), 115–147 (2022)
19. Koch, A., Walzer, S., Härtel, K.: Card-based cryptographic protocols using a minimal number of cards. In: Proc. of Asiacrypt 2015, LNCS Vol. 9452. pp. 783–807 (2015)
20. Koyama, H., Miyahara, D., Mizuki, T., Sone, H.: A secure three-input and protocol with a standard deck of minimal cards. In: Santhanam, R., Musatov, D. (eds.) Proc. of 16th International Computer Science Symposium in Russia (CSR 2021), LNCS Vol. 12730. pp. 242–256. Springer International Publishing, Cham (2021)
21. Koyama, H., Toyoda, K., Miyahara, D., Mizuki, T.: New card-based copy protocols using only random cuts. In: Proceedings of the 8th ACM on ASIA Public-Key Cryptography Workshop. pp. 13–22. APKC ‘21, Association for Computing Machinery, New York, NY, USA (2021)
22. Lafourcade, P., Miyahara, D., Mizuki, T., Robert, L., Sasaki, T., Sone, H.: How to construct physical zero-knowledge proofs for puzzles with a “single loop” condition. *Theoretical Computer Science* **888**, 41–55 (2021)
23. Manabe, Y.: Survey: Card-based cryptographic protocols to calculate primitives of boolean functions. *International Journal of Computer & Software Engineering* **27**(1), 178 (2022)
24. Manabe, Y., Ono, H.: Card-based cryptographic protocols for three-input functions using private operations. In: Proc. of 32nd International Workshop on Combinatorial Algorithms (IWOCA 2021), LNCS Vol. 12757. pp. 469–484. Springer (2021)
25. Manabe, Y., Ono, H.: Card-based cryptographic protocols with a standard deck of cards using private operations. In: Proc. of 18th International Colloquium on Theoretical Aspects of Computing (ICTAC 2021), LNCS Vol. 12819. Springer (2021)
26. Manabe, Y., Ono, H.: Card-based cryptographic protocols with malicious players using private operations. *New Generation Computing* **40**(1), 67–93 (2022)
27. Marcedone, A., Wen, Z., Shi, E.: Secure dating with four or fewer cards. *IACR Cryptology ePrint Archive*, Report 2015/1031 (2015)
28. Miyahara, D., Hayashi, Y.i., Mizuki, T., Sone, H.: Practical card-based implementations of yao’s millionaire protocol. *Theoretical Computer Science* **803**, 207–221 (2020)
29. Miyahara, D., Robert, L., Lafourcade, P., Takeshige, S., Mizuki, T., Shinagawa, K., Nagao, A., Sone, H.: Card-based zkp protocols for takuzu and juosan. In: Proc. of 10th International Conference on Fun with Algorithms (FUN 2020). Schloss Dagstuhl-Leibniz-Zentrum für Informatik (2020)
30. Miyahara, D., Sasaki, T., Mizuki, T., Sone, H.: Card-based physical zero-knowledge proof for kakuro. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **102**(9), 1072–1078 (2019)

31. Mizuki, T.: Applications of card-based cryptography to education. In: IEICE Technical Report ISEC2016-53. pp. 13–17 (2016), (In Japanese)
32. Mizuki, T.: Card-based protocols for securely computing the conjunction of multiple variables. *Theoretical Computer Science* **622**, 34–44 (2016)
33. Mizuki, T.: Efficient and secure multiparty computations using a standard deck of playing cards. In: Proc. of 15th International Conference on Cryptology and Network Security(CANS 2016), LNCS Vol.10052. pp. 484–499. Springer (2016)
34. Mizuki, T., Asiedu, I.K., Sone, H.: Voting with a logarithmic number of cards. In: Proc. of 12th International Conference on Unconventional Computing and Natural Computation (UCNC 2013), LNCS Vol. 7956. pp. 162–173 (2013)
35. Mizuki, T., Komano, Y.: Information leakage due to operative errors in card-based protocols. *Information and Computation* **285**, 104910 (2022)
36. Mizuki, T., Kumamoto, M., Sone, H.: The five-card trick can be done with four cards. In: Proc. of Asiacrypt 2012, LNCS Vol.7658. pp. 598–606 (2012)
37. Mizuki, T., Shizuya, H.: A formalization of card-based cryptographic protocols via abstract machine. *International Journal of Information Security* **13**(1), 15–23 (2014)
38. Mizuki, T., Shizuya, H.: Practical card-based cryptography. In: Proc. of 7th International Conference on Fun with Algorithms(FUN2014), LNCS Vol. 8496. pp. 313–324 (2014)
39. Mizuki, T., Shizuya, H.: Computational model of card-based cryptographic protocols and its applications. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **100**(1), 3–11 (2017)
40. Mizuki, T., Sone, H.: Six-card secure and and four-card secure xor. In: Proc. of 3rd International Workshop on Frontiers in Algorithms(FAW 2009), LNCS Vol. 5598. pp. 358–369 (2009)
41. Murata, S., Miyahara, D., Mizuki, T., Sone, H.: Efficient generation of a card-based uniformly distributed random derangement. In: Proc. of 15th International Workshop on Algorithms and Computation (WALCOM 2021), LNCS Vol. 12635. pp. 78–89. Springer International Publishing, Cham (2021)
42. Nakai, T., Misawa, Y., Tokushige, Y., Iwamoto, M., Ohta, K.: How to solve millionaires’ problem with two kinds of cards. *New Generation Computing* **39**(1), 73–96 (2021)
43. Nakai, T., Shirouchi, S., Iwamoto, M., Ohta, K.: Four cards are sufficient for a card-based three-input voting protocol utilizing private permutations. In: Proc. of 10th International Conference on Information Theoretic Security (ICITS 2017), LNCS Vol. 10681. pp. 153–165 (2017)
44. Niemi, V., Renvall, A.: Solitaire zero-knowledge. *Fundamenta Informaticae* **38**(1, 2), 181–188 (1999)
45. Nishida, T., Hayashi, Y., Mizuki, T., Sone, H.: Card-based protocols for any boolean function. In: Proc. of 15th International Conference on Theory and Applications of Models of Computation(TAMC 2015), LNCS Vol. 9076. pp. 110–121 (2015)
46. Nishida, T., Hayashi, Y., Mizuki, T., Sone, H.: Securely computing three-input functions with eight cards. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **98**(6), 1145–1152 (2015)
47. Nishida, T., Mizuki, T., Sone, H.: Securely computing the three-input majority function with eight cards. In: Proc. of 2nd International Conference on Theory and Practice of Natural Computing(TPNC 2013), LNCS Vol. 8273. pp. 193–204 (2013)

48. Nishimura, A., Nishida, T., Hayashi, Y., Mizuki, T., Sone, H.: Card-based protocols using unequal division shuffles. *Soft Computing* **22**(2), 361–371 (2018)
49. Ono, H., Manabe, Y.: Efficient card-based cryptographic protocols for the millionaires’ problem using private input operations. In: *Proc. of 13th Asia Joint Conference on Information Security(AsiaJCIS 2018)*. pp. 23–28 (2018)
50. Ono, H., Manabe, Y.: Card-based cryptographic logical computations using private operations. *New Generation Computing* **39**(1), 19–40 (2021)
51. Ono, H., Manabe, Y.: Minimum round card-based cryptographic protocols using private operations. *Cryptography* **5**(3) (2021)
52. Robert, L., Miyahara, D., Lafourcade, P., Mizuki, T.: Card-based zkp for connectivity: Applications to nurikabe, hitori, and heyawake. *New Generation Computing* **40**(1), 149–171 (2022)
53. Ruangwises, S., Itoh, T.: And protocols using only uniform shuffles. In: *Proc. of 14th International Computer Science Symposium in Russia(CSR 2019)*, LNCS Vol. 11532. pp. 349–358 (2019)
54. Ruangwises, S., Itoh, T.: Physical zero-knowledge proof for numberlink puzzle and k vertex-disjoint paths problem. *New Generation Computing* **39**(1), 3–17 (2021)
55. Ruangwises, S., Itoh, T.: Physical zero-knowledge proof for ripple effect. *Theoretical Computer Science* **895**, 115–123 (2021)
56. Ruangwises, S., Itoh, T.: Securely computing the n-variable equality function with 2n cards. *Theoretical Computer Science* **887**, 99–110 (2021)
57. Sasaki, T., Miyahara, D., Mizuki, T., Sone, H.: Efficient card-based zero-knowledge proof for sudoku. *Theoretical Computer Science* **839**, 135–142 (2020)
58. Shinagawa, K., Mizuki, T.: The six-card trick:secure computation of three-input equality. In: *Proc. of 21st International Conference on Information Security and Cryptology (ICISC 2018)*, LNCS Vol. 11396. pp. 123–131 (2018)
59. Shinagawa, K., Mizuki, T.: Secure computation of any boolean function based on any deck of cards. In: *Proc. of 13th International Workshop on Frontiers in Algorithmics (FAW 2019)*, LNCS Vol. 11458. pp. 63–75. Springer (2019)
60. Shinagawa, K., Nuida, K.: A single shuffle is enough for secure card-based computation of any boolean circuit. *Discrete Applied Mathematics* **289**, 248–261 (2021)
61. Shinoda, Y., Miyahara, D., Shinagawa, K., Mizuki, T., Sone, H.: Card-based covert lottery. In: *Proc. of 13th International Conference on Information Technology and Communications Security(SecITC 2020)*, LNCS Vol. 12596. pp. 257–270. Springer (2020)
62. Takashima, K., Abe, Y., Sasaki, T., Miyahara, D., Shinagawa, K., Mizuki, T., Sone, H.: Card-based protocols for secure ranking computations. *Theoretical Computer Science* **845**, 122–135 (2020)
63. Takashima, K., Miyahara, D., Mizuki, T., Sone, H.: Actively revealing card attack on card-based protocols. *Natural Computing* **21**(4), 615–628 (2022)
64. Toyoda, K., Miyahara, D., Mizuki, T., Sone, H.: Six-card finite-runtime xor protocol with only random cut. In: *Proc. of the 7th ACM Workshop on ASIA Public-Key Cryptography*. pp. 2–8 (2020)
65. Watanabe, Y., Kuroki, Y., Suzuki, S., Koga, Y., Iwamoto, M., Ohta, K.: Card-based majority voting protocols with three inputs using three cards. In: *Proc. of 2018 International Symposium on Information Theory and Its Applications (ISITA)*. pp. 218–222. IEEE (2018)
66. Yasunaga, K.: Practical card-based protocol for three-input majority. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* **E103.A**(11), 1296–1298 (2020)