Five-Card AND Protocol in Committed Format Using Only Practical Shuffles

Yuta Abe
Graduate School of Information Sciences
Tohoku University
Sendai, Japan
yuta.abe.r6[at]dc.tohoku.ac.jp

Yu-ichi Hayashi
Graduate School of Information Sciences
Nara Institute of Science and Technology
Nara, Japan

Takaaki Mizuki
Cyberscience Center, Tohoku University
Sendai, Japan
tm-paper+card5coa[at]g-mail.tohoku-university.jp

Hideaki Sone
Cyberscience Center, Tohoku University
Sendai, Japan

ABSTRACT

In card-based cryptography, designing AND protocols in committed format is a major topic of research. The state-of-the-art AND protocol proposed by Koch, Walzer, and Härtel in ASIACRYPT 2015 uses only four cards, which is the minimum permissible number. Their protocol's minimality relies on somewhat complicated shuffles having non-uniform probabilities of possible outcomes. Restricting the allowed shuffles to "practical" ones, namely uniform closed shuffles, to our knowledge, six cards are sufficient: The six-card AND protocol proposed by Mizuki and Sone in 2009 utilizes the random bisection cut, which is a uniform and cyclic (and hence, closed) shuffle. Thus, a question has arisen: Can we improve upon this six-card protocol using only practical shuffles? In other words, whether there exists a five-card AND protocol in committed format using only uniform closed shuffles has been one of the most important open questions in this field. In this paper, we answer the question affirmatively by designing a five-card committed-format AND protocol using only practical shuffles. The shuffles that our protocol uses are random cut and random bisection cut, both of which are uniform cyclic shuffles and can be easily implemented by humans.

KEYWORDS

Card-Based Cryptography, Secure Multi-Party Computation, Deck of Cards

ACM Reference Format:
Yuta Abe, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2018. Five-Card AND Protocol in Committed Format Using Only Practical Shuffles. In *APKC'18: 5th ACM ASIA Public-Key Cryptography Workshop, June 4, 2018, Incheon, Republic of Korea.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3197507.3197510

1 INTRODUCTION

Card-based cryptography started from the "five-card trick" presented by den Boer in 1989 [2]. This card-based protocol performs a secure AND computation using two black cards $\boxed{\clubsuit}\boxed{\clubsuit}$ and three red cards $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, where their backs $\boxed{?}$ are all identical. This paper begins by introducing the five-card trick.

1.1 The Five-Card Trick

In card-based cryptography, to manipulate Boolean values, the following encoding is used:

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

That is, the left card being black represents 0, and the left card being red represents 1. According to this encoding rule (1), Alice can put her private input bit $a \in \{0, 1\}$ on a table using two cards $\boxed{\clubsuit}\boxed{\heartsuit}$, keeping its value hidden:

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

Such a pair of face-down cards is called a *commitment* to a bit $a \in \{0, 1\}$. Similarly, Bob can put a commitment to his private input bit $b \in \{0, 1\}$ on the table, keeping its value secret from Alice (and others). Given the commitments to $a \in \{0, 1\}$ and $b \in \{0, 1\}$, along with an additional card $\boxed{\heartsuit}$, the five-card trick [2] proceeds as follows.

(1) Put the additional red card between the two input commitments, apply a *NOT computation* to a, in the left commitment by swapping the positions of its two cards, so that we have a commitment to the negation $\bar{a}$, and turn over the middle red card:

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

Note that the three cards in the middle will be $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$, i.e., three red cards will be consecutive only when $a = b = 1$, namely $a \wedge b = 1$.

(2) Apply a *random cut* (denoted by $\langle\cdot\rangle$) to the sequence of five cards:

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

A random cut, meaning a cyclic shuffling operation, uniformly randomly shifts the positions of the sequence without changing the order[1]. Mathematically, one permutation

is uniformly randomly chosen from

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

and the chosen permutation is applied to the sequence of five cards, where id is the identity permutation and $(i_1\, i_2\, \ldots\, i_\ell)$ represents a cyclic permutation.

(3) Reveal the five cards. If the three red cards $\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ are consecutive (apart from cyclic rotation), then $a \wedge b = 1$. Otherwise, $a \wedge b = 0$.

This is the five-card trick, which is simple and elegant. Although the five-card trick is extremely useful as mentioned, it has one drawback: The five-card trick cannot deal with a logical conjunction of three or more variables, where players $P_1, P_2, \ldots, P_n$ with $n \geq 3$ want to conduct a secure multiparty AND computation. To overcome such a limitation, researchers have designed "committed-format AND protocols," which are able to perform secure AND computation of three or more inputs.

1.2 The Six-Card AND Protocol in Committed Format

A committed-format AND protocol should produce a commitment to $a \wedge b$

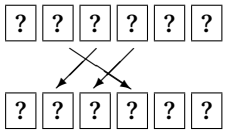
$$\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}$$

from input commitments to a and b. In contrast to the the five-card trick, the output is obtained as a commitment to $a \wedge b$, keeping its value secret; hence, the output commitment can be used as the input for another computation. There are many existing committed-format AND protocols in the literature (as shown in Table 1). Among those, we now introduce the Mizuki–Sone protocol [9], which is considered to be the simplest for humans to execute. This protocol uses two additional cards $\boxed{\clubsuit}\boxed{\heartsuit}$, and proceeds as follows.

(1) Put the two additional cards between two input commitments, and turn them over:

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

(2) Rearrange the order of the sequence as:



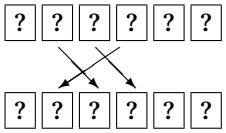
(3) Apply a *random bisection cut* denoted by $[\,\cdot\,|\,\cdot\,]$, that is, bisect the sequence of six cards and shuffle the two halves:

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

Mathematically, the permutation id or $(1\,4)(2\,5)(3\,6)$ is chosen with a probability of $1/2$, and the chosen permutation is applied to the sequence of six cards[2].

[1]Humans can easily implement a random cut so that nobody will know which one (among the five possibilities, in this case) is the current sequence (e.g. [2, 4, 12, 14]).
[2]It is well-known that a random bisection cut can also be easily and securely implemented by humans [14].

(4) Rearrange the order of the sequence as:



(5) Reveal the two left-most cards; then, a commitment to $a \wedge b$ is obtained, depending on the order of the two face-up cards $\boxed{\clubsuit}$ and $\boxed{\heartsuit}$:

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

This is the six-card AND protocol in committed format [9]. Given n input commitments to $x_1, x_2, \ldots, x_n$, and executing such a committed-format AND protocol $n-1$ times, a secure AND computation of n variables can be carried out, i.e., we can obtain a commitment to $x_1 \wedge x_2 \wedge \cdots \wedge x_n$.

Card-based protocols are far more practical than might be imagined. Hundreds of non-specialists, such as high school students, have actually executed AND protocols to facilitate their daily lives, say, to determine whether or not they are all keen to go out for dinner that night. It should be noted that these high school students understand why the protocol they execute works correctly and securely, in addition to what MPC (secure multiparty computation) is.

1.3 Known Results and Our Contribution

As seen above, the committed-format AND protocol is a useful and indispensable primitive, and designing such AND protocols is a major topic in the research field of card-based cryptography. As enumerated chronologically in Table 1, there are many committed-format AND protocols. The Mizuki–Sone protocol proposed in 2009 [9] (and described in Section 1.2) is the fourth committed-format AND protocol in the literature; it uses six cards, which are fewer than the previous three protocols [1, 12, 13] require; furthermore, as shown in the fourth column of Table 1, the Mizuki–Sone protocol is the first committed-format AND protocol that terminates in a finite number of shuffles (actually, it terminates after only one shuffle, namely a random bisection cut, as seen in Section 1.2).

After the invention of the Mizuki–Sone six-card AND protocol in 2009, it had been a challenging open question to determine whether one could construct a committed-format AND protocol with five cards or less. In 2015, Koch, Walzer, and Härtel [5] succeeded in solving the question appropriately, i.e., they presented a four-card AND protocol in committed format, which is the fifth protocol shown in Table 1. Their four-card protocol is optimal in terms of the number of required cards because we need four cards for arranging two input commitments, as long as we follow the encoding (1). As shown in the fourth column of Table 1, their four-card AND protocol does not terminate with a fixed number of shuffles, meaning that it is a Las Vegas algorithm. In addition, they constructed a five-card AND protocol that terminates with a finite number of shuffles; see the sixth protocol shown in Table 1. Furthermore, they proved that there is no four-card committed-format AND protocol with a finite number of shuffles. Therefore,

Table 1: Committed-format AND protocols

	card		shuffle			
	# of colors	# of cards	finite	uniform	cyclic	closed
Crépeau–Kilian, 1993 [1]	4	10	no	yes	yes	yes
Niemi–Renvall, 1998 [12]	2	12	no	yes	yes	yes
Stiglic, 2001 [13]	2	8	no	yes	yes	yes
Mizuki–Sone, 2009 [9] (§1.2)	2	6	yes	yes	yes	yes
Koch–Walzer–Härtel, 2015 [5]	2	4	no	no	yes	yes
Koch–Walzer–Härtel, 2015 [5]	2	5	yes	no	no	no
Ours (§2)	2	5	no	yes	yes	yes

when we restrict our attention to finite runtime protocols, the five-card AND protocol in committed format is optimal in terms of the number of cards.

Now, let us revisit Table 1; it contains columns regarding shuffles being uniform, cyclic, and/or closed. Note that the first four protocols (from 1993 to 2009) all have the answer "yes." We formally define the uniformness, cyclicness, and closedness of shuffles. Following the formal computation model of card-based protocols [7], a shuffle action is specified by a set Π of permutations and a probability distribution $\mathcal{F}$ on Π:

$$(\mathsf{shuf}, \Pi, \mathcal{F});$$

if $\mathcal{F}$ is uniform, we say that the shuffle is *uniform*; if Π is a cyclic subgroup (of the symmetric group), we say that it is *cyclic*; if Π is a subgroup, we say that it is *closed*. For example, the random bisection cut that the Mizuki–Sone protocol uses can be formally written as

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

Thus, a random bisection cut is surely a uniform and cyclic (and hence, closed) shuffle. The first three protocols [1, 12, 13] in Table 1 utilize only random cuts, which are also uniform and cyclic.

On the other hand, the two Koch–Walzer–Härtel protocols [5] use a non-uniform and/or non-closed shuffle, such as

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

and

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

Therefore, it is relatively difficult for humans to implement the existing four-card and five-card protocols in practice.

Thus, a natural question has arisen:

> Can we construct a committed-format AND protocol with five cards or less using only uniform closed shuffles?

This is one of the most important open problems in card-based cryptography.

In this paper, we will answer this question affirmatively, i.e., we will design a five-card AND protocol in committed format using only uniform closed shuffles. See the bottom-most row in Table 1. The shuffles that our protocol uses are random cuts and random bisection cuts, both of which can be easily implemented by humans, as mentioned above, and hence, we believe that humans can easily use our protocol.

2 OUR PROTOCOL

In this section, we construct a five-card committed-format AND protocol using only "practical" shuffles, namely uniform cyclic shuffles.

2.1 Idea

Here, we explain the idea behind our protocol.

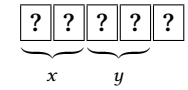
Recall Steps 1 and 2 of the five-card trick:

Let the middle card be revealed, and assume that it is ♣:

Then, there are four possibilities:

(i)	♡♡♣♡♣	$a \wedge b = 0$;
(ii)	♣♡♣♡♡	$a \wedge b = 0$;
(iii)	♡♡♣♣♡	$a \wedge b = 1$;
(iv)	♡♣♣♡♡	$a \wedge b = 1$.

After turning over the middle card, denote the sequence of cards by

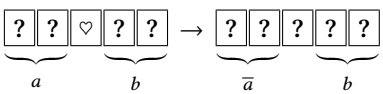


for the sake of convenience (for example, the two left-most cards are not a commitment to a bit for the cases of (i) and (iii)). Note that in cases (ii) and (iv), the first two pairs of cards can be regarded as commitments to bits x and y, and it holds that $x \oplus y = a \wedge b$. Therefore, by applying the four-card XOR protocol [9] to the first four cards, one can obtain a commitment to $x \oplus y = a \wedge b$ in these two cases. Even in cases (i) and (iii), we can continue the computation without leaking any information. The details will be seen in the next subsection.

2.2 Full Description

Here, we give the full description of our protocol.

(1) Execute Step 1 of the five-card trick:



(2) Execute Step 2 of the five-card trick:

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

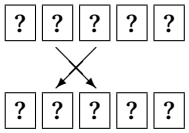
(3) Reveal the middle card, namely the third card. If the face-up card is $\boxed{\heartsuit}$, then turn it over and return to Step 2. If it is $\boxed{\clubsuit}$, then go to the next step. (The probability that $\boxed{\clubsuit}$ appears is $2/5$.)

(4) Turn over the card $\boxed{\clubsuit}$:

$$\boxed{?}\boxed{?}\boxed{\clubsuit}\boxed{?}\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}.$$

(5) Apply the procedure of the four-card XOR protocol [9] to the four left-most cards, as follows.

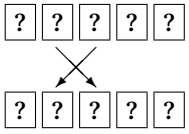
(a) Rearrange the order as:



(b) Apply a random bisection cut to the four left-most cards:

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

(c) Rearrange the order as:



(6) Reveal the two left-most cards.

(a) If $\boxed{\clubsuit}\boxed{\heartsuit}$ or $\boxed{\heartsuit}\boxed{\clubsuit}$ appears, then we have a commitment to $a \wedge b$:

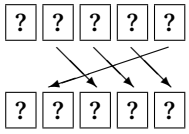
$$\clubsuit\ \heartsuit\ \underbrace{?\ ?}_{a\wedge b}\ ?\quad \text{or} \quad \heartsuit\ \clubsuit\ \underbrace{?\ ?}_{\overline{a\wedge b}}\ ?.$$

In the latter case, a NOT computation (which is to swap two cards) brings a commitment to $a \wedge b$.

(b) If $\boxed{\heartsuit}\boxed{\heartsuit}$ appears, then turn them over

$$\boxed{\heartsuit}\boxed{\heartsuit}\boxed{?}\boxed{?}\boxed{?} \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?},$$

rearrange the order as:



and return to Step 2. (The probability that $\boxed{\heartsuit}\boxed{\heartsuit}$ appears is $1/2$.)

This is our committed-format AND protocol. Since this protocol has loops, it does not terminate within a fixed number of shuffles, that is, it is a Las Vegas algorithm. The expected number of shuffles is seven, as follows. Let N_{RC} and N_{RBC} be the expected numbers of random cuts and random bisection cuts, respectively, then

$$N_{\mathrm{RC}} = 1 + \frac{3}{5}N_{\mathrm{RC}} + \frac{2}{5}\cdot\frac{1}{2}N_{\mathrm{RC}}$$

and

$$N_{\mathrm{RBC}} = \frac{3}{5}N_{\mathrm{RBC}} + \frac{2}{5}(1 + \frac{1}{2}N_{\mathrm{RBC}});$$

hence, we have $N_{\mathrm{RC}} = 5$ and $N_{\mathrm{RBC}} = 2$.

2.3 Pseudocode

The following is a pseudocode for our protocol, where we define

$$\mathrm{RC}_5 \stackrel{\mathrm{def}}{=} \{\mathrm{id}, (1\,2\,3\,4\,5), (1\,2\,3\,4\,5)^2, (1\,2\,3\,4\,5)^3, (1\,2\,3\,4\,5)^4\},$$

and we write simply (shuf, Π) instead of $(\mathrm{shuf}, \Pi, \mathcal{F})$ if $\mathcal{F}$ is uniform.

---

input set:

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

(perm, (1 2))
(turn, {3})
1 (shuf, RC_5)
(turn, {3})
if visible seq. = $(?, ?, \heartsuit, ?, ?)$ **then**
  (turn, {3})
  goto 1
(turn, {3})
(perm, (2 3))
(shuf, {id, (1 3)(2 4)})
(perm, (2 3))
(turn, {1, 2})
if visible seq. = $(\heartsuit, \heartsuit, ?, ?, ?)$ **then**
  (turn, {1, 2})
  (perm, (2 3 4 5))
  goto 1
if visible seq. = $(\clubsuit, \heartsuit, ?, ?, ?)$ **then**
  (result, 3, 4)
if visible seq. = $(\heartsuit, \clubsuit, ?, ?, ?)$ **then**
  (result, 4, 3)

In the next section, we confirm that our protocol definitively produces a commitment to $a \wedge b$ without leaking any information about a and b.

3 CORRECTNESS AND SECURITY

In this section, we verify the correctness and security of the protocol proposed in the previous section.

To this end, we make use of the *KWH-tree*, which is an excellent tool developed by Koch, Walzer, and Härtel [5]. That is, if one can write the KWH-tree satisfying some properties for a protocol, then it automatically implies that the protocol is correct and secure; see [5, 8] for the details.

We describe the KWH-tree for our five-card AND protocol in Figure 1. The first box in Figure 1 corresponds to an initial sequence, consisting of two input commitments and an additional red card; X_{00}, X_{01}, X_{10}, and X_{11} represent the probabilities of $(a, b) = (0, 0)$, $(a, b) = (0, 1)$, $(a, b) = (1, 0)$, and $(a, b) = (1, 1)$, respectively. In the second box (and below), we write X_0 instead of $X_{00} + X_{01} + X_{10}$ and write X_1 instead of X_{11}. A polynomial, such as $\frac{1}{5}X_0$

and $\frac{1}{3}X_1$, represents the conditional probability that the current sequence is the one next to the polynomial, given the view seen on the table. Looking at the two boxes at the bottom, one can see that a commitment to $a \wedge b$ is definitively obtained. Furthermore, in each box, the sum of all polynomials is equal to $X_0 + X_1$, implying that no information about a and b leaks.

Thus, the KWH-tree in Figure 1 guarantees that our protocol is correct and secure.

4 CONCLUSION

In this paper, we constructed a five-card AND protocol in committed format using random cuts and random bisection cuts that are practical enough for humans to implement, solving an important open problem [4, 5]. Therefore, we have the following theorem.

Theorem 1. *There exists a 5-card expected-finite-runtime AND protocol in committed format with only uniform cyclic shuffles.*

Because the previous "practical" AND protocol [9] uses six cards, as mentioned in Section 1.2, our protocol reduced the number of required cards from six to five, and one might think that the contribution of this paper is only incremental; however, we believe that this is not the case. One reason for this is that a "practical" committed-format AND protocol with five cards or less has been solicited for eight years since the six-card AND protocol [9] appeared in 2009. Another reason is that our five-card AND protocol using only uniform cyclic shuffles is the *best possible* because, very recently, the following lower bounds have been found.

Theorem 2 ([3]). *There is no five-card finite-runtime AND protocol in committed format with only closed shuffles.*

Theorem 3 ([3]). *There is no four-card expected-finite-runtime AND protocol in committed format with only uniform closed shuffles.*

Theorem 3 implies that we need at least five cards to have a practical protocol; moreover, even though we have five cards, Theorem 2 tells us that we cannot have a finite-runtime protocol. Thus, to consider five-card expected-finite-runtime protocols is the only possible option. Consequently, Theorems 1, 2, and 3 together imply that, in this sense, our proposed protocol is optimal.

All the protocols mentioned thus far in this paper can be executed publicly: Every operation by players is supposed to be done with all eyes fixed on how the cards are manipulated. In contrast, there is another model where players are allowed to use "private" operations: It is known that such a somewhat strong assumption brings protocols with fewer cards, e.g. [6, 10, 11].

ACKNOWLEDGMENTS

We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. This work was supported by JSPS KAKENHI Grant Number JP17K00001.

REFERENCES

[1] Claude Crépeau and Joe Kilian. 1994. Discreet Solitary Games. In *Advances in Cryptology — CRYPTO '93*, Douglas R. Stinson (Ed.). Lecture Notes in Computer Science, Vol. 773. Springer Berlin Heidelberg, 319–330. https://doi.org/10.1007/3-540-48329-2_27

[2] Bert den Boer. 1990. More Efficient Match-Making and Satisfiability: the Five Card Trick. In *Advances in Cryptology — EUROCRYPT '89*, Jean-Jacques Quisquater and Joos Vandewalle (Eds.). Lecture Notes in Computer Science, Vol. 434. Springer Berlin Heidelberg, 208–217. https://doi.org/10.1007/3-540-46885-4_23

[3] Julia Kastner, Alexander Koch, Stefan Walzer, Daiki Miyahara, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2017. The Minimum Number of Cards in Practical Card-based Protocols. In *Advances in Cryptology — ASIACRYPT 2017*, Tsuyoshi Takagi and Thomas Peyrin (Eds.). Lecture Notes in Computer Science, Vol. 10626. Springer, Cham, 126–155. https://doi.org/10.1007/978-3-319-70700-6_5

[4] Alexander Koch and Stefan Walzer. 2017. Foundations for Actively Secure Card-based Cryptography. Cryptology ePrint Archive, Report 2017/422. (2017).

[5] Alexander Koch, Stefan Walzer, and Kevin Härtel. 2015. Card-Based Cryptographic Protocols Using a Minimal Number of Cards. In *Advances in Cryptology - ASIACRYPT 2015*, Tetsu Iwata and Jung Hee Cheon (Eds.). Lecture Notes in Computer Science, Vol. 9452. Springer Berlin Heidelberg, 783–807. https://doi.org/10.1007/978-3-662-48797-6_32

[6] Antonio Marcedone, Zikai Wen, and Elaine Shi. 2015. Secure Dating with Four or Fewer Cards. Cryptology ePrint Archive, Report 2015/1031. (2015).

[7] Takaaki Mizuki and Hiroki Shizuya. 2014. A formalization of card-based cryptographic protocols via abstract machine. In *International Journal of Information Security*. Vol. 13. Springer Berlin Heidelberg, 15–23. https://doi.org/10.1007/s10207-013-0219-4

[8] Takaaki Mizuki and Hiroki Shizuya. 2017. Computational Model of Card-Based Cryptographic Protocols and Its Applications. In *IEICE TRANSACTIONS on Fundamentals of Electronics, Communicat ions and Computer Sciences*. Vol. E100-A. The Institute of Electronics, Information and Communication Engineers, 3–11.

[9] Takaaki Mizuki and Hideaki Sone. 2009. Six-Card Secure AND and Four-Card Secure XOR. In *Frontiers in Algorithmics*, Xiaotie Deng, John Edward Hopcroft, and Jinyun Xue (Eds.). Lecture Notes in Computer Science, Vol. 5598. Springer Berlin Heidelberg, 358–369. https://doi.org/10.1007/978-3-642-02270-8_36

[10] Takeshi Nakai, Satoshi Shirouchi, Mitsugu Iwamoto, and Kazuo Ohta. 2017. Four Cards Are Sufficient for a Card-Based Three-Input Voting Protocol Utilizing Private Permutations. In *International Conference on Information Theoretic Security, ICITS 2017*, Junji Shikata (Ed.). Lecture Notes in Computer Science, Vol. 10681. Springer, Cham, 153–165. https://doi.org/10.1007/978-3-319-72089-0_9

[11] Takeshi Nakai, Yuuki Tokushige, Yuto Misawa, Mitsugu Iwamoto, and Kazuo Ohta. 2016. Efficient Card-Based Cryptographic Protocols for Millionaires' Problem Utilizing Private Permutations. In *Cryptology and Network Security, CANS 2016*, Sara Foresti and Giuseppe Persiano (Eds.). Lecture Notes in Computer Science, Vol. 10052. Springer, Cham, 500–517. https://doi.org/10.1007/978-3-319-48965-0_30

[12] Valtteri Niemi and Ari Renvall. 1998. Secure multiparty computations without computers. In *Theoretical Computer Science*. Vol. 191. 173–183. https://doi.org/10.1016/S0304-3975(97)00107-2

[13] Anton Stiglic. 2001. Computations with a deck of cards. In *Theoretical Computer Science*. Vol. 259. 671–678. https://doi.org/10.1016/S0304-3975(00)00409-6

[14] Itaru Ueda, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. 2016. How to Implement a Random Bisection Cut. In *Theory and Practice of Natural Computing*, Carlos Martín-Vide, Takaaki Mizuki, and Miguel A. Vega-Rodríguez (Eds.). Vol. 10071. Springer International Publishing, Cham, 58–69. https://doi.org/10.1007/978-3-319-49001-4_5

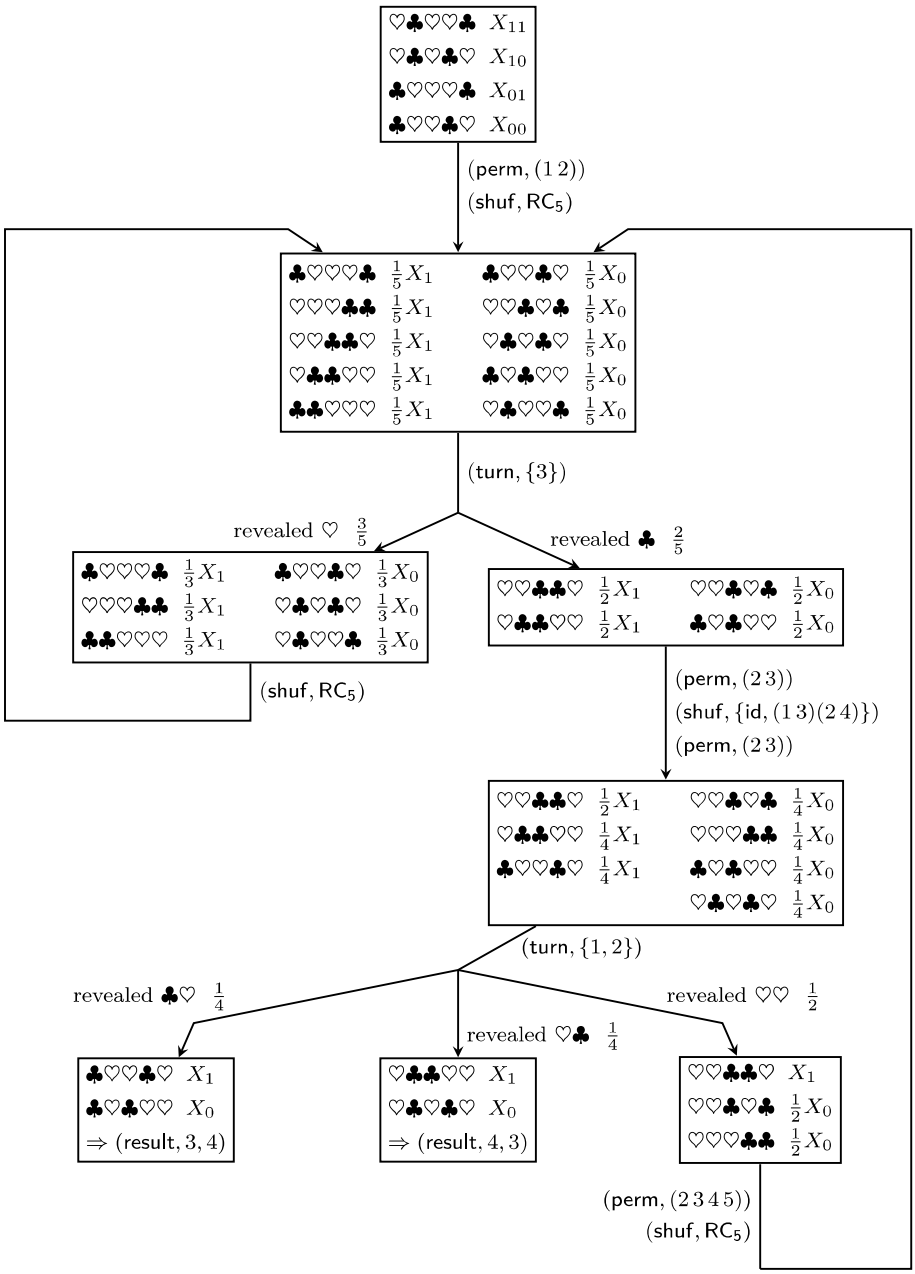


Figure 1: The KWH-tree for our protocol