Card-Based ZKP Protocols for Takuzu and Juosan

Daiki Miyahara
Graduate School of Information Sciences,
Tohoku University, Sendai, Japan
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
daiki.miyahara.q4@dc.tohoku.ac.jp

Léo Robert
University Clermont Auvergne, LIMOS,
CNRS UMR (6158), Aubière, France
leo.robert@uca.fr

Pascal Lafourcade
University Clermont Auvergne, LIMOS,
CNRS UMR (6158), Aubière, France
pascal.lafourcade@uca.fr

So Takeshige
School of Engineering, Tohoku University,
Sendai, Japan
so.takeshige.q1@dc.tohoku.ac.jp

Takaaki Mizuki
Cyberscience Center, Tohoku University,
Sendai, Japan
tm-paper+zerotate@g-mail.tohoku-university.jp

Kazumasa Shinagawa
Graduate School of Informatics and Engineering, The University of Electro-Communications,
Tokyo, Japan
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan
shinagawakazumasa@uec.ac.jp

Atsuki Nagao
Department of Information Science,
Ochanomizu University, Tokyo, Japan
a-nagao@is.ocha.ac.jp

Hideaki Sone
Cyberscience Center, Tohoku University,
Sendai, Japan

Abstract

Takuzu and Juosan are logical Nikoli games in the spirit of Sudoku. In Takuzu, a grid must be filled with 0's and 1's under specific constraints. In Juosan, the grid must be filled with vertical and horizontal dashes with specific constraints. We give physical algorithms using cards to realize zero-knowledge proofs for those games. The goal is to allow a player to show that he/she has the solution without revealing it. Previous work on Takuzu showed a protocol with multiple instances needed. We propose two improvements: only one instance needed and a soundness proof. We also propose a similar proof for Juosan game.

2012 ACM Subject Classification Security and privacy → Information-theoretic techniques

Keywords and phrases Zero-knowledge proof, Card-based cryptography, Takuzu, Juosan

Digital Object Identifier 10.4230/LIPIcs.FUN.2021.20

Funding *Daiki Miyahara*: This work was supported by JSPS KAKENHI Grant Number JP19J21153.
Léo Robert: This work was partially supported by the French project ANR-18-CE39-0019 (MobiS5).
Pascal Lafourcade: This work was partially supported by the project ANR-18-CE39-0019 (MobiS5).
Takaaki Mizuki: This work was supported by JSPS KAKENHI Grant Number JP17K00001.
Kazumasa Shinagawa: This work was supported by JSPS KAKENHI Grant Number JP17J01169.

Acknowledgements We thank the anonymous referees, whose comments have helped us to improve the presentation of the paper. In particular, Protocol 1 for Takuzu presented in Section 3.2.1 is based on the fruitful comments given by one referee.

1 Introduction

James Bond and Q decide to spend most of their holidays on the Spiaggia Praia beach (located at Isola di Favignana, Sicily, Italy). Before swimming in the sea, they like to play with logical games. James Bond is a specialist of *Takuzu*. Takuzu is a puzzle invented by Frank Coussement and Peter De Schepper in 2009[1]. It was also called *Binero*, *Bineiro*, *Binary Puzzle*, *Brain Snacks* or *Zernero*. Figure 1 contains a simple Takuzu grid and its solution. Q is an expert of *Juosan*, which was published by Nikoli[2]. Figure 2 contains a Juosan grid and its solution.

Each one proposes his favorite game to the other as a challenge. Both are competitive, and each challenge ends to be so hard that the other cannot solve it. James Bond immediately supposes that something is wrong and asks Q a proof that the grid has a solution. Of course, Q thinks the same way about Bond's challenge. Since they are both suspicious, they want to prove that there is a solution without giving any information about the solution.

In cryptography, the process, which allows a party to prove that it has a data without leaking any information on this data, is called Zero-Knowledge Proof (ZKP).

More formally, a ZKP is a protocol which enables a prover P to convince that it has a solution s of a problem to a verifier V. This proof cannot leak any information on s. The protocol must observe three properties.

- **Completeness:** If P knows s then it can convince V.
- **Soundness:** If P does not know s, it can convince V with only a negligible probability.
- **Zero-Knowledge:** V learns nothing about s. This can be formalized by showing that the outputs of a simulator and outputs of the real protocol follow the same probability distribution.

The concept of interactive ZKP was introduced by Goldwasser et al. [12]. Then it was shown that for any NP complete problem there exists an interactive ZKP protocol [11]. There is also an extension showing that every provable statement can be proved in zero-knowledge [2].

There exist protocols where the prover and the verifier do not need to interact. Such protocols are called non-interactive ZKP [4]. For a complete background on ZKP's, see [18].

Usually ZKP protocols are executed by computers, yet, our aim is to design a solution for Bond and Q's dilemma using physical objects such as cards, since on the Spiaggia Praia beach they do not want to use their computers. We first recall the rules of these two games before presenting our contributions.

Takuzu's Rules

The goal of Takuzu is to fill a rectangular grid of even size with 0's and 1's. An initial Takuzu grid already contains a few filled cases. A grid is solved when it is full (*i.e.*, no empty cases) and respects the following constraints.

1. **Equality Rule:** Each row/column contains exactly the same number of 1's and 0's.
2. **Uniqueness Rule:** Each row (column) is unique among all rows (columns).
3. **Adjacent Rule:** In each row and each column there can be no more than two same numbers adjacent to each other; for example 110010 is possible, but 110001 is impossible.

The problem of solving a Takuzu grid was proven to be NP complete in [3, 34].

Juosan's Rules

A Juosan grid is divided into territories by bold lines, where a territory is possibly associated with a number. The goal is to fill in all cells with a vertical (|) or horizontal (−) dash such

[1] `https://en.wikipedia.org/wiki/Takuzu`
[2] `http://www.nikoli.co.jp/en/puzzles/juosan.html`

							0
	0	0			1		
	0				1		0
		1					
0	0		1			1	
				1			
1	1				0		1
	1						1

0	1	1	0	1	0	1	0
1	0	0	1	0	1	0	1
1	0	0	1	0	1	1	0
0	1	1	0	1	0	0	1
0	0	1	1	0	1	1	0
1	0	0	1	1	0	1	0
1	1	0	0	1	0	0	1
0	1	1	0	0	1	0	1

Figure 1 Example of a 8×8 Takuzu challenge, and its solution. We can verify that each row and column is unique, contains the same number of 0's and 1's, and there are never three consecutive 1's or 0's.

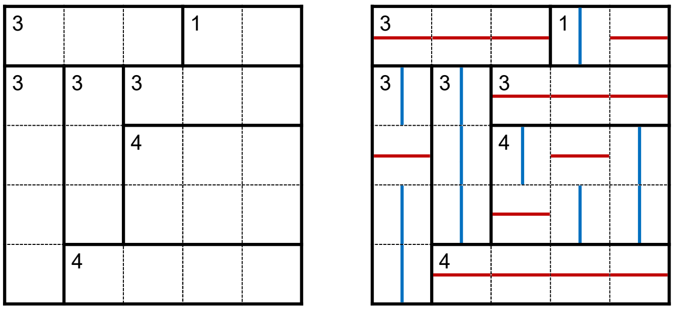


Figure 2 Example of a Juosan challenge, and its solution from Nikoli website.

that the following three constraints are satisfied.

1. **Room Rule:** The number in every territory equals the number of either vertical or horizontal dashes in it (in some cases, there may be equal numbers of both). Territories with no number may have any number of vertical dashes and horizontal dashes.
2. **Adjacent (horizontal) Rule:** Horizontal dashes can extend more than three cells horizontally but no more than two cells vertically.
3. **Adjacent (vertical) Rule:** Vertical dashes can extend more than three cells vertically but no more than two cells horizontally.

In 2018, the problem of solving a Juosan grid was proven to be NP complete in [16].

Contributions

We have the two main following contributions.

1. We propose better ZKP protocols for Takuzu which improve upon the approach given in [5]. The latter used several instances of the protocol while ours use only one instance. We also improve the soundness of the proof in the sense that if the prover does not have a solution, he convinces the verifier with null probability.
2. We also propose an adapted version of this technique to Juosan. Again, only one instance of the protocol is run for proving to V that if P does not know the solution, then P convinces V with probability 0. We also propose an optimized version of the Adjacent Verification which aims to show validity of four consecutive commitments.

Related Work

There are works on implementing cryptographic protocols using physical objects, as in [23] for example, or in [9] where a physical secure auction protocol was proposed. Other implementations have been studied using cards in [8], polarizing plates [32], polygon cards [31], a standard deck of playing cards [20], using a PEZ dispenser [1], using a dial lock [21], using a 15 puzzle [22], or using a tamper-evident seals [25, 26, 27].

In FUN'18, the authors of [29] revisited the ZKP for Sudoku proposed by Gradwohl et al. in FUN'07 [13]. This is a clear progress in the construction of ZKP since the technique proposed in this paper uses specific protocols to perform zero-knowledge proof for Sudoku. Indeed, those protocols use a normal deck of playing cards and have no soundness error with a reasonable number of playing cards. The original technique for Sudoku was extended for Hanje [7]. ZKP's for several other puzzles have been studied such as Akari [5], Takuzu [5], Kakuro [5, 19], KenKen [5], Makaro [6], Norinori [10], and Slitherlink [17].

There is a ZKP proof for Takuzu puzzle [5] (recall in Section 2), but we propose an enhanced version using only one instance of the protocol to convince the verifier. The previous proof is decomposed into several cases to avoid leak of information toward the solution. This implies the need of rerunning the protocol several times for completely convincing V that P has the solution. The construction of the protocol leads to have a negligible probability that the prover P does not know the solution. Our proof is designed in such a way that only one instance is run leading to a complete soundness of the proof (i.e., if P does not have the solution, the probability of convincing V is null). We show that this technique can be adapted to Juosan game which has not been studied before. The detailed security proof for our ZKP protocols for Takuzu is given in Section 3.4 and for Juosan in Section 4.4.

Outline: In Section 2, we present an existing ZKP protocol for Takuzu. In Section 3, we improve the ZKP protocol for Takuzu. In Section 4, we present our ZKP protocol for Juosan. In the last section we conclude.

2 The Existing ZKP Protocol for Takuzu

We give a ZKP proof using physical objects. The goal is to show that the prover P (aka James Bond) can prove to the verifier V (aka Q) that he knows a solution of a given Takuzu grid. The material used for the proof include two printed grids on a sheet of paper, a piece of paper, an envelope and two kinds of cards: cards with a 0 or a 1 printed on them.

There are two phases in this protocol, the Setup which generates the permutations used for the second phase called the verification.

Let G be the $n \times n$ initial Takuzu grid and S the matrix relative to the solution known by P (including the initial cells).

Setup. The prover P chooses uniformly at random two permutations: π_R for the rows, and π_C for the columns. He writes the two permutations on a paper and place the latter into an envelope E. Then he computes $S' = \pi_R(\pi_C(S))$. Finally, P places cards face down on the second grid according to S'. We denote the configuration of these cards by the matrix $\tilde{S'}$

Verification. The verifier V picks c randomly among $\{0, 1, 2, 3\}$.

If $c = 0$: This case corresponds to P proving that the solution is the one of the initial grid. V computes $G' = \pi_R(\pi_C(G))$ with the permutations found in the envelope E. Then V determines the cells of G' corresponding to the initial cells of G. Finally, V checks if the revealed cards are the same as the one revealed in the second grid (that are placed according to $\tilde{S'}$).

If $c = 1$: This case corresponds to P proving that adjacent rule holds.
V permutes (face down) the cards of $\tilde{S}'$ to obtain $\tilde{S} = \pi_c^{-1}(\pi_R^{-1}(\tilde{S}'))$ using the permutations in E. Then, V picks d randomly among $\{0, 1\}$ and e randomly among $\{1, 2, 3\}$.
If $d = 0$: For each row, V sets $x = \lfloor \frac{n-e}{3} \rfloor$ decks of three cards $\{(e + 3 \cdot i + 1, e + 3 \cdot i + 2, e + 3 \cdot i + 3)\}_{\{0 \leq i < x\}}$ where the triplet (i, j, k) denotes a deck containing the i^{th}, the j^{th} and the k^{th} cards of the row.
If $d = 1$: For each column, V sets $x = \lfloor \frac{n-e}{3} \rfloor$ decks of three cards $\{(e + 3 \cdot i + 1, e + 3 \cdot i + 2, e + 3 \cdot i + 3)\}_{\{0 \leq i < x\}}$ where the triplet (i, j, k) denotes a deck containing the i^{th}, the j^{th} and the k^{th} cards of the column.
Then, V gives the triplets to P. For each deck, P removes one of the two identical cards. Then P reveals the cards to V, who accepts only if he sees two different cards.

If $c = 2$: This case corresponds to P proving that uniqueness rule holds.
For this, V picks randomly one row or one column. V reveals all the cards of his chosen row (or column). For each of the $n - 1$ other rows (or columns) the verifier picks the cards where a 0 appears in the revealed rows (or column). At this step, V does not reveal those cards. Each one of these $n - 1$ sets of cards is shuffled by the shuffle functionality and given back to the prover. P reveals one card per set that is a 1. Thus each one of the other $n - 1$ rows (or columns) are different from the revealed row, since the initial row (or column) has a 0 where the other column (or row) has a 1. If there are several 1's in a deck, the prover randomly chooses which one to reveal.

If $c = 3$: This case corresponds to P proving that the equality rule holds.
The verifier V picks d randomly among $\{0, 1\}$.
If $d = 0$, for each row, V takes all the cards in the row and keep them face down. Then V gathers the cards in order to shuffle those n decks. We assume that the verifier has access to a *shuffle functionality* which is essentially an indistinguishable shuffle of face down cards. Note that this action could be done by a trusted third party (M for instance) but not by P or V (since they could cheat and modify the cards).
Finally, V checks that each deck contains exactly the same number of 1's and 0's.
If $d = 1$, the same process is done except that V picks columns instead of rows.

To have the best security guarantees, the verifier should choose his challenges c, d, etc. such that each combination of challenges at the end has the same probability. This protocol is repeated k times where k is a chosen security parameter. Note that the ZKP is again polynomial in the size of the grid.

3 Our improved ZKP Protocols for Takuzu

In this section, we propose two ZKP protocols for Takuzu; our protocols are simple and have no soundness error. Remember that the goal is to show the prover P (aka James Bond) can prove to the verifier V (aka Q) that P knows a solution of a given Takuzu grid.

Our protocols use black cards $\boxed{\clubsuit}$, red cards $\boxed{\heartsuit}$, and number cards $\boxed{1}\boxed{2} \cdots \boxed{6}$ whose backs $\boxed{?}$ are all identical. In the sequel, we use the following encoding rule:

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

That is, black-to-red represents 0 and red-to-black represents 1. We call two face-down cards that correspond to a bit $x \in \{0, 1\}$ according to the above encoding rule (1) a *commitment to* x, and we write it as $\underbrace{\boxed{?}\boxed{?}}_{x}$. Roughly, our improved ZKP protocols for Takuzu proceed as follows.

Table 1 The exact values of $|\mathsf{tkz}(n)|$ when n is up to ten.

n	$\|\mathsf{tkz}(n)\|$
4	6
6	14
8	34
10	84

Setup phase: The prover P places a commitment to each cell according to the solution.

Verification phases: The verifier V verifies that the placement of the commitments satisfies all the constraints.

To present the complete description of our protocols in Section 3.2, we show some preliminaries in Section 3.1. In Section 3.3, we show that there is a trade-off between our two protocols and compare them.

3.1 Preliminaries

In this subsection, we introduce some notations and two subprotocols, which will be used to present our constructions in Section 3.2.

3.1.1 Possible Sequences

For an even number n, we denote by $\mathsf{tkz}(n)$ the set of all binary sequences satisfying the Uniqueness and Equality rules of Takuzu, that is, $\mathsf{tkz}(n) := \{w \in \{0,1\}^n \mid w$ contains exactly $n/2$ 0's and no three consecutive digits$\}$. For example, $\mathsf{tkz}(4) = \{0011, 1100, 0101, 1010, 0110, 1001\}$. The size of $\mathsf{tkz}(n)$ can be computed as Table 1. The size $|\mathsf{tkz}(n)|$ is known in the On-line Encyclopedia of Integer Sequences (OIES) as "the number of paths from $(0,0)$ to (n,n) avoiding 3 or more consecutive east steps and 3 or more consecutive north steps.[3]" We can also show that $\mathsf{tkz}(n) = O((\frac{3+\sqrt{5}}{2})^n n^{-\frac{1}{2}})$.

3.1.2 Basic Shuffles

Pile-scramble shuffle [15]. This is the following shuffling operation: Given a sequence of m piles, each of which consists of the same number of face-down cards, denoted by $\underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_1}\ \underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_2} \cdots \underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_m}$, applying a *pile-scramble shuffle* (denoted by $[\cdot|\ldots|\cdot]$) results in

$$\left[\underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_1}\middle|\underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_2}\middle|\cdots\middle|\underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_m}\right] \rightarrow \underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_{r^{-1}(1)}}\ \underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_{r^{-1}(2)}} \cdots \underbrace{\boxed{?}\!\|\!\|}_{\boldsymbol{p}_{r^{-1}(m)}},$$

where $r \in S_m$ is a uniformly distributed random permutation and S_m denotes the symmetric group of degree m. To implement a pile-scramble shuffle, we use physical cases that can store a pile of cards, such as boxes and envelopes; a player (or players) randomly shuffle them until nobody traces the order of the piles.

[3] https://oeis.org/A177790

Pile-shifting shuffle. A *pile-shifting shuffle* (or a pile-shifting scramble [28]) is to *cyclically* shuffle piles of cards. That is, given m piles, applying a pile-shifting shuffle (denoted by $\langle \cdot | \ldots | \cdot \rangle$) results in $\left\langle \underbrace{\boxed{?}}_{\boldsymbol{p}_1} \middle| \underbrace{\boxed{?}}_{\boldsymbol{p}_2} \middle| \cdots \middle| \underbrace{\boxed{?}}_{\boldsymbol{p}_m} \right\rangle \to \underbrace{\boxed{?}}_{\boldsymbol{p}_{s+1}} \underbrace{\boxed{?}}_{\boldsymbol{p}_{s+2}} \cdots \underbrace{\boxed{?}}_{\boldsymbol{p}_{s+m}}$, where s is uniformly and randomly chosen from $\mathbb{Z}/m\mathbb{Z}$. To implement a pile-shifting shuffle, we use similar materials as a pile-scramble shuffle; a player (or players) cyclically shuffle them by hand until nobody traces the offset.

3.1.3 Mizuki–Sone AND (OR) Protocol

Given two commitments to $a, b \in \{0, 1\}$ (along with additional two cards $\boxed{\clubsuit}\boxed{\heartsuit}$), the Mizuki–Sone AND protocol [24] outputs a commitment to $a \wedge b$: $\underbrace{\boxed{?}\boxed{?}}_{a} \underbrace{\boxed{?}\boxed{?}}_{b} \boxed{\clubsuit}\boxed{\heartsuit} \to \cdots \to \underbrace{\boxed{?}\boxed{?}}_{a\wedge b}$.

Note that the output commitment can be used for another protocol. The protocol proceeds as follows.

1. Rearrange the sequence as follows: $\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}} \to \overset{1}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{2}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}}$.
2. Apply a *random bisection cut*: $[\,\boxed{?}\boxed{?}\boxed{?} \| \boxed{?}\boxed{?}\boxed{?}\,] \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$. A random bisection cut is a special case of a pile-scramble shuffle; it bisects a sequence of cards and then shuffles the two halves.
3. Reveal the first and fourth cards in the sequence. Then, the output commitment can be obtained as follows: $\boxed{\clubsuit}\boxed{?}\boxed{?}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}$ or $\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{a\wedge b}\boxed{\clubsuit}\boxed{?}\boxed{?}$.

Note that by De Morgan's laws we can have the Mizuki–Sone OR protocol that produces a commitment to $a \vee b$ given two commitments to a and b.

3.1.4 Mizuki–Sone XOR protocol

Given two commitments to $a, b \in \{0, 1\}$, the Mizuki–Sone XOR protocol [24] outputs a commitment to $a \oplus b$: $\underbrace{\boxed{?}\boxed{?}}_{a} \underbrace{\boxed{?}\boxed{?}}_{b} \to \cdots \to \underbrace{\boxed{?}\boxed{?}}_{a\oplus b}$. The protocol proceeds as follows.

1. Rearrange the sequence as follows: $\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}} \to \overset{1}{\boxed{?}}\overset{3}{\boxed{?}}\overset{2}{\boxed{?}}\overset{4}{\boxed{?}}$.
2. Apply a random bisection cut to the sequence: $[\,\boxed{?}\boxed{?} \| \boxed{?}\boxed{?}\,] \to \boxed{?}\boxed{?}\boxed{?}\boxed{?}$.
3. Rearrange the sequence as follows: $\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}} \to \overset{1}{\boxed{?}}\overset{3}{\boxed{?}}\overset{2}{\boxed{?}}\overset{4}{\boxed{?}}$.
4. Reveal the first and second cards in the sequence. Then, the output commitment can be obtained as follows: $\boxed{\clubsuit}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{a\oplus b}$ or $\boxed{\heartsuit}\boxed{\clubsuit}\underbrace{\boxed{?}\boxed{?}}_{\overline{a\oplus b}}$.

3.1.5 Six-Card Trick

Given three commitments to $a, b, c \in \{0, 1\}$, the *six-card trick* [30][4] outputs 1 if $a = b = c$ and 0 otherwise: $\underbrace{\boxed{?}\boxed{?}}_{a} \underbrace{\boxed{?}\boxed{?}}_{b} \underbrace{\boxed{?}\boxed{?}}_{c} \to \cdots \to \begin{cases} 1 & \text{if } a = b = c, \\ 0 & \text{otherwise.} \end{cases}$

That is, we can know only whether the values of given three commitments are the same or not by using the six-card trick. We use it in our construction to verify the Adjacent rule.

[4] The protocol had been invented independently by Heather, Schneider, and Teague [14].

The protocol proceeds as follows.

1. Rearrange the sequences as follows: $\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}} \rightarrow \overset{1}{\boxed{?}}\overset{6}{\boxed{?}}\overset{3}{\boxed{?}}\overset{2}{\boxed{?}}\overset{5}{\boxed{?}}\overset{4}{\boxed{?}}$.
2. Apply a *random cut* (which is denoted by $\langle \cdots \rangle$) to the sequence: $\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$. A random cut is a special case of a pile-shifting shuffle; it cyclically shuffles a sequence of cards. Note that a random cut can be implemented easily with human hands [33].
3. Reveal the sequence.
   a. If the resulting sequence is $\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}$ (apart from cyclic shifts), the output is 1, i.e., $a = b = c$ holds.
   b. If the resulting sequence is $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ (apart from cyclic shifts), the output is 0, i.e., $a = b = c$ does not hold.

3.1.6 Input-Preserving Function Evaluation Technique

As seen in Section 3.1.5, we can know whether the equality of three input commitments holds although the input commitments are destroyed after executing the six-card trick. The *input-preserving function evaluation technique* enables us to obtain input commitments again after some function evaluation (such as the equality) by using some number cards.

Let us first explain the *input-preserving six-card trick* as follows.

1. Place a number card below each card, and then turn them over:

$$\underbrace{\boxed{?}\boxed{?}}_{a}\;\underbrace{\boxed{?}\boxed{?}}_{b}\;\underbrace{\boxed{?}\boxed{?}}_{c} \rightarrow \begin{array}{c}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}\end{array} \rightarrow \begin{array}{c}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{array}.$$

2. Rearrange the sequences as follow: $\begin{array}{c}\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}}\overset{6}{\boxed{?}}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{array} \rightarrow \begin{array}{c}\overset{1}{\boxed{?}}\overset{6}{\boxed{?}}\overset{3}{\boxed{?}}\overset{2}{\boxed{?}}\overset{5}{\boxed{?}}\overset{4}{\boxed{?}}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{array}$.
3. Apply a pile-shifting shuffle to the sequences:

$$\left\langle \begin{array}{c|c|c|c|c|c}\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}\\ \boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}\end{array} \right\rangle \rightarrow \begin{array}{c}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{array}.$$

4. Reveal the cards of all sequences except for the number cards; then, we obtain the output as shown in Step 3 in Section 3.1.5.
5. Turn over the face-up cards and apply a pile-scramble shuffle to the sequences:

$$\left[\begin{array}{c|c|c|c|c|c}\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}\\ \boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}&\boxed{?}\end{array} \right] \rightarrow \begin{array}{c}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{array}.$$

6. Reveal the number cards and rearrange the sequence of piles so that the revealed number cards become in ascending order; then, we have restored input commitments to a, b, and c. The following is an example case:

$$\begin{array}{c}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\end{array} \rightarrow \begin{array}{c}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}\\ \boxed{3}\boxed{1}\boxed{5}\boxed{4}\boxed{6}\boxed{2}\end{array} \rightarrow \begin{array}{c}\underbrace{\boxed{?}\boxed{?}}_{a}\underbrace{\boxed{?}\boxed{?}}_{b}\underbrace{\boxed{?}\boxed{?}}_{c}\\ \boxed{1}\boxed{2}\boxed{3}\boxed{4}\boxed{5}\boxed{6}\end{array}.$$

More formally, assume that we have a protocol to evaluate some function with m input piles of cards. Then, the input-preserving function evaluation technique enables us to obtain m input piles again after some function evaluation by using m number cards:

$$\begin{array}{ccc}\boxed{?}\!\!\Vert & \boxed{?}\!\!\Vert & \cdots & \boxed{?}\!\!\Vert\\ \boxed{1} & \boxed{2} & \cdots & \boxed{m}\end{array} \rightarrow \cdots \rightarrow \text{ some function evaluation } \rightarrow \cdots \rightarrow \boxed{?}\!\!\Vert\,\boxed{?}\!\!\Vert \cdots \boxed{?}\!\!\Vert.$$

This proceeds as follows.

1. Attach a corresponding number card to each of m input piles:

$$\begin{array}{cccc} \boxed{?} & \boxed{?} & \cdots & \boxed{?} \\ \boxed{1} & \boxed{2} & \cdots & \boxed{m} \end{array} \rightarrow \cdots \rightarrow \begin{array}{cccc} \boxed{?} & \boxed{?} & \cdots & \boxed{?} \\ \boxed{?} & \boxed{?} & \cdots & \boxed{?} \end{array}.$$

Together with the added number cards, execute a designated protocol to evaluate some function.

2. Apply a pile-scramble shuffle to the sequence of piles:

$$\left[\begin{array}{c|c|c|c} \boxed{?} & \boxed{?} & & \boxed{?} \\ \boxed{?} & \boxed{?} & \cdots & \boxed{?} \end{array}\right] \rightarrow \begin{array}{cccc} \boxed{?} & \boxed{?} & \cdots & \boxed{?} \\ \boxed{?} & \boxed{?} & \cdots & \boxed{?} \end{array}.$$

3. Reveal only the number cards. Then, rearrange the sequence of piles so that the revealed number cards become in ascending order to obtain m input piles.

3.2 Our Constructions

We are now ready to present the full description of our ZKP protocols for Takuzu, namely Protocols 1 and 2.

3.2.1 Protocol 1: Verifying Each Constraint Separately

Given a Takuzu puzzle instance of $n \times n$ grid, *Protocol 1* verifies that all the constraints, namely the Equality, Uniqueness, and Adjacent rules, are satisfied separately.

Setup phase. Remember the encoding rule (1). The prover P places a commitment on each cell according to the solution (which is kind of a (0,1)-matrix).

Adjacent Verification phase. In this phase, V verifies that the Adjacent rule is satisfied. For this, V repeats the following for every three consecutive commitments in rows and columns.

1. Attach the corresponding number card to each of the six cards:

$$\boxed{?}\boxed{?}\,\boxed{?}\boxed{?}\,\boxed{?}\boxed{?} \rightarrow \begin{array}{c} \boxed{?}\boxed{?}\,\boxed{?}\boxed{?}\,\boxed{?}\boxed{?} \\ \boxed{1}\boxed{2}\,\boxed{3}\boxed{4}\,\boxed{5}\boxed{6} \end{array} \rightarrow \begin{array}{c} \boxed{?}\boxed{?}\,\boxed{?}\boxed{?}\,\boxed{?}\boxed{?} \\ \boxed{?}\boxed{?}\,\boxed{?}\boxed{?}\,\boxed{?}\boxed{?} \end{array}.$$

2. Perform the input-preserving six-card trick shown in Section 3.1.6 to prove that the three commitments are not all 0s and 1s. If the six-card trick outputs 1, V rejects it.

Uniqueness Verification phase. In this phase, V verifies that the Uniqueness rule is satisfied. V repeats the following for every pair of rows (and columns), each of which consists of n commitments. Considering such a pair, let $a_1, a_2, \ldots, a_n \in \{0,1\}$ denote the values of commitments placed on the first row (in the pair) and $b_1, b_2, \ldots, b_n \in \{0,1\}$ denote those of commitments on the second row.

1. V attaches the corresponding number card to each of the $4n$ cards.
2. V applies the "input-preserving" Mizuki–Sone XOR protocol obtained by Sections 3.1.4 and 3.1.6 to the commitments to a_i and b_i to produce a commitment to $a_i \oplus b_i$ for every i, $1 \le i \le n$. Note that V will return the $4n$ cards to their original positions after the next step.

3. V uses the "input-preserving" Mizuki–Sone OR protocol obtained by Sections 3.1.3 and 3.1.6[5] exactly $n-1$ times to reveal the value of $\bigvee_{j=1}^{n}(a_j \oplus b_j)$. If it is 0, it means $a_i = b_i$ for every i, and hence, V rejects it.

Equality Verification phase. In this phase, V verifies that the Equality rule is satisfied.

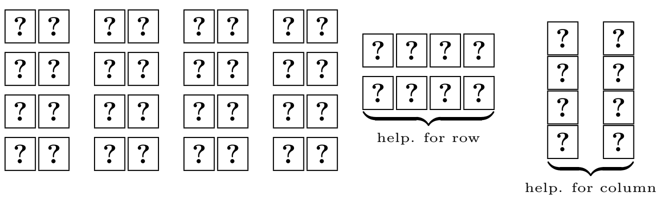
1. For every row, V repeats the following.
   a. V attaches the corresponding number card to each of the $2n$ cards.
   b. V applies a pile scramble shuffle.
   c. V reveals the resulting n commitments. If the number of commitments to 0 is not equal to that of commitments to 1, V rejects it.
   d. Similar to the input-preserving function evaluation technique shown in Section 3.1.6, V returns the n commitments to their original positions.
2. For every column, V follows the same steps except for Steps (a) and (d). Since the n commitments will not be used after this phase, V does not need to return them to their original positions.

This protocol uses n^2 black cards, the same number of red cards, and $4n$ number cards (recall that we have an $n \times n$ Takuzu grid). The numbers of required shuffles are $4n(n-2)$ in the Adjacent Verification phase, $2n^2(n-1)$ in the Uniqueness Verification phase, and $3n$ in the Equality Verification phase.

3.2.2 Protocol 2: Verifying All the Constraints Simultaneously

Protocol 2 verifies that all the constraints are satisfied simultaneously using helping cards that will be placed in the Setup phase. When displaying a figure, we are given a 4×4 Takuzu grid as an example.

Setup phase. The prover P places a commitment to each cell according to the solution. In addition, to show that all the constraints are satisfied, P arranges face-down sequences corresponding to all the sequences in $\mathsf{tkz}(n)$ except for those in the solution (for both row and column):



,

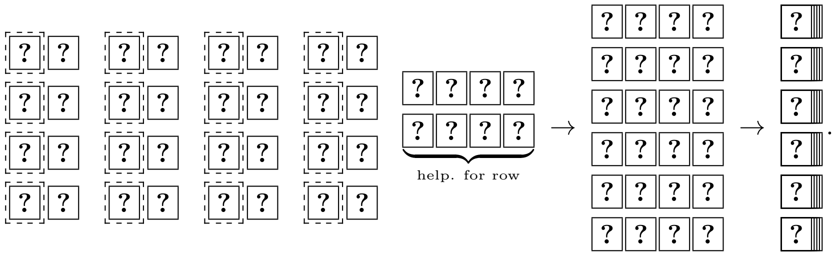
where a black card $\boxed{\clubsuit}$ corresponds to 0 and a red card $\boxed{\heartsuit}$ corresponds to 1 in any helping sequence for the row, and $\boxed{\heartsuit}$ corresponds to 0 and $\boxed{\clubsuit}$ corresponds to 1 in any helping sequence for the column. As shown in Table 1, the number of such helping sequences is two in each direction in this case of 4×4 grid.

---

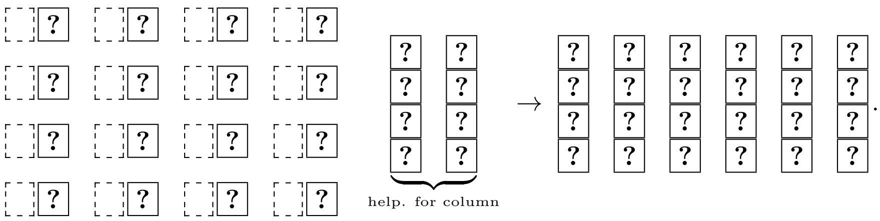
[5] For the two additional cards, we can make use of any two revealed cards appearing in the previous step without opening the number cards.

Verification phase. In this phase, V verifies all the constraints, namely the Equality, Uniqueness, and Adjacent rules by revealing the commitments along with the helping sequences after applying a pile-scramble shuffle. Note that V can also verify that the commitments placed by P in the Setup phase form the valid ones according to the encoding rule (1) (e.g., not $\boxed{\clubsuit}\boxed{\clubsuit}$ or $\boxed{\heartsuit}\boxed{\heartsuit}$).

1. For all the rows, take the left card of each commitment to make n sequences (along with the helping sequences for the rows).



2. Apply a pile-scramble shuffle to the sequence of piles.
3. Reveal the cards of all sequences. If there are either (i) a sequence whose number of black cards is not the same as that of red cards, (ii) two identical sequences, or (iii) a sequence containing more than two consecutive 0s or 1s, then V rejects it.
4. For all the columns, take the right card of each commitment to make n sequences (along with the helping sequences for the columns).



Then, the same is done.

This protocol uses $n \cdot |\mathsf{tkz}(n)|$ black cards and the same number of red cards when we have an $n \times n$ Takuzu grid. See Table 1 again for the value of $|\mathsf{tkz}(n)|$. The number of required shuffles is two.

3.3 Comparison

Let us compare the two protocols for Takuzu presented in the previous subsection. Table 2 summarizes the numbers of required cards and shuffles for the protocols.

Table 2 The numbers of required cards and shuffles for Protocols 1 and 2 when we have an $n \times n$ Takuzu grid such that n is up to eight.

	#Cards			#Shuffles		
	$n=4$	$n=6$	$n=8$	$n=4$	$n=6$	$n=8$
Protocol 1	48	96	160	140	474	1112
Protocol 2	48	168	544	2	2	2

According to this table, there is a trade-off between the numbers of required cards and shuffles, i.e., Protocol 1 presented in Section 3.2.1 needs a less number of cards but needs a more number of shuffles than Protocol 2 presented in Section 3.2.2. Both protocols are reasonable, and hence, P and V may choose their favorite one. Let us stress that pencil puzzles are usually played on a board of small size, say $n = 8$, and also that players enjoying a puzzle normally do not use computers to solve it.

3.4 Security Proofs for Takuzu

We prove the security of our construction. We consider a *shuffle functionality* which is an indistinguishable shuffle of face down cards. The first part is dedicated to give proofs of protocol 1 while the second part is dedicated to prove the security for protocol 2.

3.4.1 Security Proofs of Protocol 1

Takuzu Completeness

We show that if P knows a solution of a given Takuzu grid then he is able to convince V.

Proof. Suppose that P knows a solution S of the initial grid G and runs the input phase described in subsection 3.2.1. Then we show that P is able to perform the proof for the three phases: (AV) adjacent verification phase, (UV) uniqueness and verification phase, and equality verification phase (EV).

Since S is a solution of G, S is a valid grid respecting all the constraints. If S respects the adjacent rule so the six-card trick outputs 0 in all cases. Indeed, if the number are all equals then the rearranging step (step 1 of the six-card trick) has the same output than the input. For example, consider the sequence 101 which is rearrange as:

$$\begin{array}{cccccc} 1&2&3&4&5&6\\ \boxed{\heartsuit}&\boxed{\clubsuit}&\boxed{\clubsuit}&\boxed{\heartsuit}&\boxed{\heartsuit}&\boxed{\clubsuit} \end{array} \rightarrow \begin{array}{cccccc} 1&6&3&2&5&4\\ \boxed{\heartsuit}&\boxed{\clubsuit}&\boxed{\clubsuit}&\boxed{\clubsuit}&\boxed{\heartsuit}&\boxed{\heartsuit} \end{array}.$$

The random cut will keep the pattern, up to a cyclic shift. The same result holds for other possible sequences (there are 6 of them).

We conclude that S succeeds the AV challenge.

We show that S passes the UV challenge. The verification is done toward each possible pair of row (and column) of the grid. Consider two rows where a_i denote the values of commitments on the first row and b_i the values for the second row. Since S is a solution those two rows are different, meaning that there exists at least a value j for which $a_j \neq b_j$. This implies that $a_j = b_j \oplus 1$ (recall that $\forall i = 1 \dots n$ we have $a_i, b_i \in \{0, 1\}$) meaning that $a_j \oplus b_j = 1$. Thus the disjunction of all the possible $a_i \oplus b_i$ will output 1 (since at least on of its term is equal to 1). Repeating this process for each possible pair of rows and columns leads to always output 1 in step 3 of the UV.

Lastly, we show that S succeeds the EV challenge. Since it is a solution there is the same number of 0 and 1 in each row and column. When shuffling the cards, only the their order is modified but not their value thus the equality property still holds.

We conclude that P convinces V for AV, UV and EV phases. ◀

Takuzu Soundness

We show that if P does not provide a solution of a given Takuzu grid then he is not able to convince V with probability 1.

Proof. Suppose that P does not know the solution, we want to show that V will detect it during, at least, one verification phase.

First, notice that if P places a commitment that respects all the Takuzu rules then it is a solution. Thus if at least one rule is not respected then it is not a solution. Hence, we consider three possible cases corresponding to each rule that is not respected:

- If the adjacent rule is not respected, then there exists three consecutive commitments that have the same value (either 0 or 1). Without loss of generality, let consider that those values are all 0's. Thus the the rearrange step is:

$$\begin{array}{cccccc}1&2&3&4&5&6\\ \boxed{\clubsuit}&\boxed{\heartsuit}&\boxed{\clubsuit}&\boxed{\heartsuit}&\boxed{\clubsuit}&\boxed{\heartsuit}\end{array} \rightarrow \begin{array}{cccccc}1&6&3&2&5&4\\ \boxed{\clubsuit}&\boxed{\heartsuit}&\boxed{\clubsuit}&\boxed{\heartsuit}&\boxed{\clubsuit}&\boxed{\heartsuit}\end{array} .$$

  Thus a random cut will keep this alternating pattern. (Note that the same result holds with all 1 but black cards are replaced by red cards and vice-versa.) Hence, the six-card trick outputs 1 so V rejects P's commitments.
- If the uniqueness rule is not respected, then at least two rows or two columns are identical. Thus, for all $i = 1 \dots n$, we have $a_i = b_i \implies a_j \oplus b_j = 0$. This implies that the disjunction of all those terms is equal to 0 so V rejects it.
- If the equality rule is not respected, then there exists a row or column where the number of 0 is not equal to the number of 1. W.l.o.g., consider a row with $\frac{n}{2}+1$ 0-commitment and $\frac{n}{2} - 1$ 1-commitment. When applying a pile scramble shuffle the 0-commitment remains 0-commitment, and 1-commitment still remains 1-commitment so V will notice that there is $\frac{n}{2} + 1$ 0-commitment and $\frac{n}{2} - 1$ 1-commitment. Finally, V won't be convinced. ◀

Zero-knowledge

We show that during the verification process, V learns nothing about P's solution.

Proof. The idea of the proof is described in [13]. Proving zero-knowledge implies to describe an efficient simulator which is an algorithm that simulates any interaction between a cheating verifier and a real prover. The simulator has no access to the correct solution but it has an advantage over the prover: when the cards are shuffled, the simulator can swap the decks with different ones. We thus show how to construct a simulator for each challenge:

Adjacent Verification challenge: The simulator chooses randomly S such that three consecutive cells never contain the same number. Note that the uniqueness and equality rule may not hold. Then it simulates the interaction between the prover and the verifier. For each three vertically (or horizontally) consecutive commitments, the six-card trick outputs 0 (there are exactly two identical number).

Uniqueness Verification challenge: When the verifier checks for pair of rows or columns, the simulator picks cards to form distinct rows or columns (for example, during the Mizuki-Sone XOR shuffle phase).

Equality Verification challenge: During the pile scramble shuffle, the simulator places $\frac{n}{2}$ 0-commitment and $\frac{n}{2}$ 1-commitment in a random order. ◀

We conclude that our protocol for Takuzu is complete, soundness and zero-knowledge.

3.4.2 Security Proofs of Protocol 2

Completeness

We show that if P knows a solution of a given Takuzu grid then he is able to convince V.

Proof. Suppose that P knows a solution S of the initial grid G and runs the input phase described in subsection 3.2.2. Then we show that P is able to perform the proof for the verification phase.

Since S is a solution of G, S is a valid grid respecting all the constraints. Indeed S respects the adjacent rule so each three consecutive commitments cannot be all the same. Thus the left cards of each commitment cannot be the same (recall our encoding 1). The other rules can be verified using the same process since each left card (or right) fully determine the value of a commitment. Indeed, if the left card is $\boxed{\clubsuit}$ the the commitment corresponds to the value 0 and if the left card is $\boxed{\heartsuit}$ then it corresponds to a 1-commitment. We conclude, that if P's commitment corresponds to the solution of G then all the constraints can be verified by V when revealing the commitments. ◀

Soundness

We show that if P does not provide a solution of a given Takuzu grid then he is not able to convince V with probability 1.

Proof. Suppose that P does not know the solution, we want to show that V will detect it during the verification phase.

First, notice that if P places a commitment that respects all the Takuzu rules then it is a solution. Thus if at least one rule is not respected then it is not a solution. Hence, we consider three possible cases corresponding to each rule that is not respected:

- If the adjacent rule is not respected, then there exists three consecutive commitments that have the same value (either 0 or 1). Since the order of the cards is kept (only the pile are shuffled), V can detect when three consecutive cards are identical.
- If the uniqueness rule is not respected, then at least two rows or two columns are identical. Again, V will detect it since all the left (right) cards are revealed and that left (right) cards fully determine a commitment value.
- If the equality rule is not respected, then there exists a row or column where the number of 0 is not equal to the number of 1. As seen in the previous case, V won't be convinced since the number of 0 does not correspond to the number 1. ◀

Zero-knowledge

We show that during the verification process, V learns nothing about P's solution.

Proof. The idea is the same as for protocol 1. We show how to construct a simulator for the challenge. During the pile-scramble phase, the simulator replaces each pile with a sequence of $\mathsf{tkz}(n)$. Thus the set of those sequence verifies the rules. ◀

We conclude that our protocol for Takuzu is complete, soundness and zero-knowledge.

4 Our ZKP Protocol for Juosan

In this section, applying the ideas shown in Section 3, we construct a ZKP protocol for Juosan, which allows the prover P (aka Q) to convince the verifier V (aka James Bond) that he really knows a solution.

4.1 Subprotocol: Five-Card Trick

We introduce the *five-card trick* [8] in this subsection, which is used in our construction to verify Rules 2 and 3.

Given two commitments to $a, b \in \{0,1\}$ (along with a red card $\boxed{\heartsuit}$), the five-card trick [8] outputs $a \wedge b$: $\underbrace{\boxed{?}\boxed{?}}_{a}\ \underbrace{\boxed{?}\boxed{?}}_{b}\ \boxed{\heartsuit} \rightarrow \cdots \rightarrow a \wedge b$. The protocol proceeds as follows.

1. Rearrange the sequence as follows: $\overset{1}{\boxed{?}}\overset{2}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}\overset{5}{\boxed{?}} \rightarrow \overset{2}{\boxed{?}}\overset{1}{\boxed{?}}\overset{5}{\boxed{?}}\overset{3}{\boxed{?}}\overset{4}{\boxed{?}}$.
2. Apply a random cut to the sequence: $\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$.
3. Reveal the sequence. If the resulting sequence is:
   a. $\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}$ (apart from cyclic shifts), the output is $a \wedge b = 1$.
   b. $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}$ (apart from cyclic shifts), the output is $a \wedge b = 0$.

4.2 Our Construction

We are now ready to present the full description of our ZKP protocol for Juosan. Let us consider that we are given a 5×5 Juosan grid as an example.

Our construction consists of three phases, the Setup phase, Adjacent Verification phase, and Room Verification phase.

Setup phase. Regarding a vertical dash (|) as 0 and a horizontal dash (—) as 1, the prover P places a commitment to each cell according to the solution:

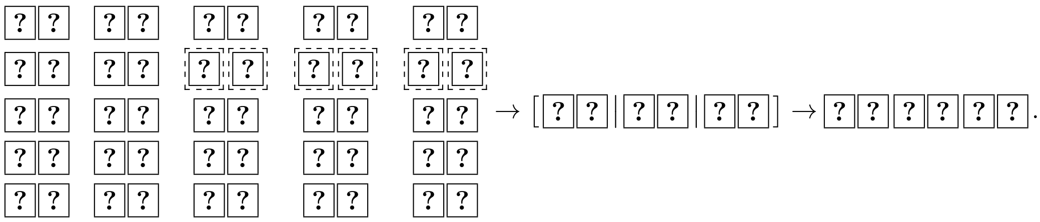
$$\begin{array}{ccccc}
\boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} \\
\boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} \\
\boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} \\
\boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} \\
\boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?} & \boxed{?}\boxed{?}
\end{array}.$$

Adjacent Verification phase. In this phase, V repeats applications of the Mizuki–Sone AND protocol [24] and five-card trick [8] enhanced by the input-preserving function evaluation technique to verify that the Adjacent condition is satisfied. Note that V can also verify that the commitments placed by P in the Setup phase form the valid ones according to the encoding rule (1).

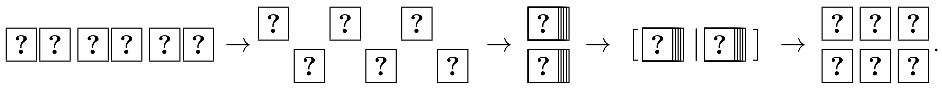
1. Let us verify that there are no three consecutive horizontal dashes in any column. The fact that three horizontal dashes are not consecutive to the vertical means that there is at least one vertical dash among them. Therefore, it suffices to confirm the AND value of of the corresponding three commitments is false because a vertical dash is encoded as 0 and a horizontal dash as 1.
   Let $a, b, c \in \{0,1\}$ be the values of commitments on three consecutive cells in a column. First, for commitments to a and b, perform the Mizuki–Sone AND protocol described in Section 3.1.3. Then, a commitment to $a \wedge b$ is obtained.
2. Perform the five-card trick described in Section 4.1 for the commitments to $a \wedge b$ and c. If the five-card trick outputs 1, V rejects it.
3. Restore commitments to a, b, and c by the input-preserving function evaluation technique described in Section 3.1.6.
4. The same is done for rows. In this case, let the encoding be reversed.

Room Verification phase. In this phase, V verifies the Room rule by revealing the commitments after applying pile-scramble shuffles.

1. Apply a pile-scramble shuffle to all commitments in a territory with a number:



2. Take all the left cards and all the right cards of these commitments to make two piles. Then, apply a pile-scramble shuffle to the two piles:



3. Reveal all the cards of the piles. If the number of black cards or red cards is not the same as the number written on the territory, V rejects it. For example, in the case of a 3-cell territory with a number "3," each of the following two types of card groups should appear with a probability of 1/2: $\begin{matrix}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\\ \boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}\end{matrix}$, $\begin{matrix}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\clubsuit}\\ \boxed{\heartsuit}\boxed{\heartsuit}\boxed{\heartsuit}\end{matrix}$, where the order of cards in the card set does not matter.
4. The same is done for all other numbered territories.

The numbers of required shuffles are $3(m(n-2)+n(m-2))$ in the Adjacent Verification phase and k in the Room Verification phase when we have an $m \times n$ Juosan grid and k territories. This protocol uses $mn+1$ black cards, the same number of red cards, and eight number cards.

4.3 Optimized Adjacent Verification for Juosan

In the original Adjacent Verification phase of our protocol for Juosan presented in Section 4.2, the AND value $a \wedge b \wedge c$ for $a, b, c \in \{0,1\}$ is securely computed to show the validity of three consecutive commitments. We present an optimization technique to show the validity of four consecutive commitments as follows.

1. Let $a, b, c, d \in \{0,1\}$ be commitments of four consecutive cells in a column. First, for commitments to b and c, perform the Mizuki–Sone AND protocol described in Section 3.1.3. Then, a commitment to $b \wedge c$ is obtained.
2. Let $x_1 = b \wedge c$, $x_2 = a$, and $c_3 = d$. By slightly modifying the Mizuki–Sone AND protocol, the following protocol is obtained:

$$\underbrace{\boxed{?}\boxed{?}}_{x_1}\ \underbrace{\boxed{?}\boxed{?}}_{x_2}\ \boxed{\clubsuit}\boxed{\heartsuit}\ \underbrace{\boxed{?}\boxed{?}}_{x_3}\ \boxed{\clubsuit}\boxed{\heartsuit} \to \cdots \to \underbrace{\boxed{?}\boxed{?}}_{x_1\wedge x_2}\ \underbrace{\boxed{?}\boxed{?}}_{x_1\wedge x_3}.$$

Note that this uses one random bisection cut only. Then, two commitments of $x_1 \wedge x_2 = a \wedge b \wedge c$ and $x_1 \wedge x_3 = b \wedge c \wedge d$ are obtained.
3. Open the commitments of $a \wedge b \wedge c$ and $b \wedge c \wedge d$. If they are not $(0,0)$, V rejects it.
4. Obtain the commitments to a, b, c, and d by the input-preserving function evaluation technique described in Section 3.1.6.

4.4 Security Proofs for Juosan

We prove the security of our construction. We consider a *shuffle functionality* which is an indistinguishable shuffle of face down cards.

Juosan Completeness

We show that if P knows a solution of a given Takuzu grid then it is able to convince V.

Proof. Suppose that P knows a solution S of the initial grid G and runs the setup phase described in Section 4. Then we show that P is able to perform the proof for the two phases: adjacent verification phase (AV) and room verification phase (RV).

Since S is a solution of the grid G, we show that S is a valid grid respecting all the constraints.

We first consider the adjacent verification. Let us take an example, the other cases (here 8 possible cases) are done the same way. We consider the case of horizontal dashes in a column for verifying the adjacent (horizontal) rule. We need to show that the AND value of these commitments is not equal to 1. Note that if we inverse the encoding rule ($\boxed{\heartsuit}\boxed{\clubsuit} = 0$ and $\boxed{\clubsuit}\boxed{\heartsuit} = 1$) we can verify that no three consecutive vertical dashes are placed in a given row.

We consider the 101-commitment: $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}$.

First we take the first four cards and apply the Mizuki-Sone AND protocol:

$$\overset{1}{\boxed{\heartsuit}}\overset{2}{\boxed{\clubsuit}}\overset{3}{\boxed{\clubsuit}}\overset{4}{\boxed{\heartsuit}}\overset{5}{\boxed{\heartsuit}}\overset{6}{\boxed{\clubsuit}} \rightarrow \overset{1}{\boxed{\heartsuit}}\overset{3}{\boxed{\clubsuit}}\overset{4}{\boxed{\heartsuit}}\overset{2}{\boxed{\clubsuit}}\overset{5}{\boxed{\heartsuit}}\overset{6}{\boxed{\clubsuit}}.$$

Then the random cut will output two possible combinations:

$$\overset{1}{\boxed{\heartsuit}}\overset{3}{\boxed{\clubsuit}}\overset{4}{\boxed{\heartsuit}}\overset{2}{\boxed{\clubsuit}}\overset{5}{\boxed{\heartsuit}}\overset{6}{\boxed{\clubsuit}} \text{ or } \overset{2}{\boxed{\clubsuit}}\overset{5}{\boxed{\heartsuit}}\overset{6}{\boxed{\clubsuit}}\overset{1}{\boxed{\heartsuit}}\overset{3}{\boxed{\clubsuit}}\overset{4}{\boxed{\heartsuit}}.$$

Both cases has output $\boxed{\clubsuit}\boxed{\heartsuit}$ which is simply 0.

Note that if we replace the second commitment by 1 (which is encoded as $\boxed{\heartsuit}\boxed{\clubsuit}$) then after the random cut we have the two possible outputs: $\overset{1}{\boxed{\heartsuit}}\overset{3}{\boxed{\heartsuit}}\overset{4}{\boxed{\clubsuit}}\overset{2}{\boxed{\clubsuit}}\overset{5}{\boxed{\heartsuit}}\overset{6}{\boxed{\clubsuit}}$ or $\overset{2}{\boxed{\clubsuit}}\overset{5}{\boxed{\heartsuit}}\overset{6}{\boxed{\clubsuit}}\overset{1}{\boxed{\heartsuit}}\overset{3}{\boxed{\heartsuit}}\overset{4}{\boxed{\clubsuit}}$.

The output is $\boxed{\heartsuit}\boxed{\clubsuit}$ which is simply 1 (and this corresponds with the expected value).

Next, we compute the five-card trick for input $\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}$.

The rearrange step outputs $\boxed{\heartsuit}\boxed{\clubsuit}\boxed{\heartsuit}\boxed{\heartsuit}\boxed{\clubsuit}$ which is the same pattern of alternating figure meaning that $a \wedge b = 0$. Note that a random cut will not modify the shape of the pattern.

The same process is applied to all other commitments so we can conclude that S respects the adjacent verification for horizontal and vertical dashes. Hence S succeeds the AV challenge.

Note that we can verify the adjacent rule by looking at three consecutives cells and the next three consecutives cells (that is cells a, b, c and then cells b, c, d) or directly apply the optimized adjacent verification in Section 4.3.

S also succeeds the room verification. Indeed, we make two piles corresponding to left cards of each commitment and right cards of each commitment. Thus each vertical dash (encoded as $\boxed{\clubsuit}\boxed{\heartsuit}$) adds a card $\boxed{\clubsuit}$ in a pile and a card $\boxed{\heartsuit}$ in the other pile. Hence, a pile represents the number of vertical dashes while the other represents the number of horizontal dashes (but those two piles are indistinguishable). It remains to count the number of cards that forms the majority to deduce if the room rule is achieved. Finally S is a correct solution for RV challenge.

We conclude that P convinces V for AV phase and for RV phase. ◀

Juosan Soundness

We show that if P does not provide a solution of a given Juosan grid then it is not able to convince V.

Proof. Suppose that P is able to convince V meaning that P can provide S which succeeds AV challenge and RV challenge. We want to show that P knows a solution to Juosan grid G.

During the input phase, P places a commitment.

Since P is able to perform the proof of AV challenge and RV challenge we have: initial cells are the same as in S, horizontal bars are not arranged three times in a column, vertical bars are not arranged three times in a row, and a room has correct numbers of vertical or horizontal bars corresponding to its number.

We deduce that S is a solution of G (since each rule is respected). Hence if P does not provide a solution of G then it fails the proof for at least one challenge. Since those two phases are perform during the proof, P receives two challenges (AV and RV) out of two possibilities.

Hence, if P gives a wrong grid then at least one of those two challenges will fail.

Thus P cannot convince V with a wrong proposition. ◀

Juosan Zero-knowledge

We show that during the verification process, V learns nothing about P's solution.

Proof. We follow the same process as for the zero-knowledge of Takuzu protocol. We thus show how to construct a simulator for each challenge:

Adjacent Verification challenge: The simulator chooses randomly S. Before the final output of the five-card trick, the simulator always chooses a deck for which red and black cards are alternated. Thus the output is always 0 meaning that the Adjacent Verification challenge succeed. Since S was chosen randomly then simulated proofs and real proofs are indistinguishable.

Room Verification challenge: When the verifier checks for vertical direction, the simulator looks at the room number to form the corresponding number with red cards (or black ones) for each piles. This step is done the same way for all rooms. Since each row (or column) are different from one to another, the simulated proofs and real proofs are indistinguishable. ◀

We conclude that our protocol for Juosan is complete, soundness and zero-knowledge.

5 Conclusion

In this paper we improved the existing interactive zero-knowledge proof for Takuzu. Our protocols use a reasonable number of cards and shuffles, implying that they are easy to implement by humans. Our protocols are designed in such a way that the proof is completely sound meaning that a prover P convinces the verifier V with probability 1 if P has a solution. We also proposed an adapted version of this protocol for the Juosan puzzle which had never been proposed before. An interesting puzzle, called *Suguru*, can also be studied with this technique.

References

1 József Balogh, János A. Csirik, Yuval Ishai, and Eyal Kushilevitz. Private computation using a PEZ dispenser. *Theor. Comput. Sci.*, 306(1-3):69–84, 2003.

2 Michael Ben-Or, Oded Goldreich, Shafi Goldwasser, Johan Håstad, Joe Kilian, Silvio Micali, and Phillip Rogaway. Everything provable is provable in zero-knowledge. In *Advances in Cryptology - CRYPTO '88, 8th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1988, Proceedings*, volume 403 of *Lecture Notes in Computer Science*, pages 37–56. Springer, 1988. `doi:10.1007/0-387-34799-2_4`.

3 Marzio De Biasi. Binary puzzle is NP-complete, July 2012. URL: `http://www.nearly42.org/vdisk/cstheory/binaryp.pdf`.

4 Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, page 103–112, New York, NY, USA, 1988. Association for Computing Machinery. `doi:10.1145/62212.62222`.

5 Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, and Pascal Lafourcade. Physical zero-knowledge proofs for Akari, Takuzu, Kakuro and KenKen. In Erik D. Demaine and Fabrizio Grandoni, editors, *8th International Conference on Fun with Algorithms, FUN 2016, June 8-10, 2016, La Maddalena, Italy*, volume 49 of *LIPIcs*, pages 8:1–8:20. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2016. `doi:10.4230/LIPIcs.FUN.2016.8`.

6 Xavier Bultel, Jannik Dreier, Jean-Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Atsuki Nagao, Tatsuya Sasaki, Kazumasa Shinagawa, and Hideaki Sone. Physical zero-knowledge proof for Makaro. In *SSS 2018 - 20th International Symposium on Stabilization, Safety, and Security of Distributed Systems*, volume 11201 of *Lecture Notes in Computer Science*, pages 111–125, Tokyo, Japan, November 2018. Springer. `doi:10.1007/978-3-030-03232-6_8`.

7 Yu-Feng Chien and Wing-Kai Hon. Cryptographic and physical zero-knowledge proof: From Sudoku to Nonogram. In Paolo Boldi and Luisa Gargano, editors, *Fun with Algorithms 2010*, volume 6099 of *LNCS*, pages 102–112. Springer, 2010.

8 Bert den Boer. More efficient match-making and satisfiability the five card trick. In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89*, pages 208–217, Berlin, Heidelberg, 1990. Springer Berlin Heidelberg.

9 Jannik Dreier, Hugo Jonker, and Pascal Lafourcade. Secure auctions without cryptography. In *Fun with Algorithms, 7th International Conference, FUN'14*, pages 158–170, 2014. `doi:10.1007/978-3-319-07890-8_14`.

10 Jean Guillaume Dumas, Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone. Interactive physical zero-knowledge proof for Norinori. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11653 LNCS:166–177, 2019. `doi:10.1007/978-3-030-26176-4_14`.

11 Oded Goldreich and Ariel Kahan. How to construct constant-round zero-knowledge proof systems for NP. *Journal of Cryptology*, 9(3):167–189, 1996. `doi:10.1007/s001459900010`.

12 Shafi Goldwasser, Silvio Micali, and Charles Rackoff. Knowledge complexity of interactive proof-systems. *Conference Proceedings of the Annual ACM Symposium on Theory of Computing*, pages 291–304, 1985. `doi:10.1145/3335741.3335750`.

13 Ronen Gradwohl, Moni Naor, Benny Pinkas, and Guy N. Rothblum. Cryptographic and physical zero-knowledge proof systems for solutions of Sudoku puzzles. In *Proceedings of the 4th International Conference on Fun with Algorithms*, FUN'07, pages 166–182, Berlin, Heidelberg, 2007. Springer-Verlag.

14 James Heather, Steve A. Schneider, and Vanessa Teague. Cryptographic protocols with everyday objects. *Formal Aspects of Computing*, 26:37–62, 2013.

15 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, *UCNC 2015*, volume 9252 of *LNCS*, pages 215–226. Springer, 2015.

16 Chuzo Iwamoto and Tatsuaki Ibusuki. Kurotto and Juosan are NP-complete. In *The 21st Japan Conference on Discrete and Computational Geometry, Graphs, and Games (JCDCG3 2018)*, pages 46–48, Ateneo de Manila University, Philippines, September 2018.

17 Pascal Lafourcade, Daiki Miyahara, Takaaki Mizuki, Tatsuya Sasaki, and Hideaki Sone. A physical ZKP for Slitherlink: How to perform physical topology-preserving computation. In Swee-Huay Heng and Javier Lopez, editors, *Information Security Practice and Experience*, pages 135–151, Cham, 2019. Springer International Publishing.

18 Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. *Handbook of Applied Cryptography.* CRC Press, Inc., Boca Raton, FL, USA, 1st edition, 1996.

19 Daiki Miyahara, Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone. Card-based physical zero-knowledge proof for Kakuro. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E102.A(9):1072–1078, 2019. doi:10.1587/transfun.E102.A.1072.

20 Takaaki Mizuki. Efficient and secure multiparty computations using a standard deck of playing cards. In *Cryptology and Network Security*, pages 484–499, November 2016. doi:10.1007/978-3-319-48965-0_29.

21 Takaaki Mizuki, Yoshinori Kugimoto, and Hideaki Sone. Secure multiparty computations using a dial lock. In Jin-yi Cai, S. Barry Cooper, and Hong Zhu, editors, *Theory and Applications of Models of Computation, 4th International Conference, TAMC 2007, Shanghai, China*, volume 4484 of *LNCS*, pages 499–510. Springer, May 2007. doi:10.1007/978-3-540-72504-6_45.

22 Takaaki Mizuki, Yoshinori Kugimoto, and Hideaki Sone. Secure multiparty computations using the 15 puzzle. In Andreas W. M. Dress, Yinfeng Xu, and Binhai Zhu, editors, *Combinatorial Optimization and Applications, First International Conference, COCOA 2007, Xi'an, China*, volume 4616 of *LNCS*, pages 255–266. Springer, August 2007. doi:10.1007/978-3-540-73556-4_28.

23 Takaaki Mizuki and Hiroki Shizuya. Practical card-based cryptography. In *Fun with Algorithms, 7th International Conference, FUN'14*, pages 313–324, 2014. doi:10.1007/978-3-319-07890-8_27.

24 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, Third International Workshop, FAW 2009, Hefei, China, June 20-23, 2009. Proceedings*, volume 5598 of *LNCS*, pages 358–369. Springer, 2009.

25 Tal Moran and Moni Naor. Basing cryptographic protocols on tamper-evident seals. In Luís Caires, Giuseppe F. Italiano, Luís Monteiro, Catuscia Palamidessi, and Moti Yung, editors, *ICALP 2005*, volume 3580 of *LNCS*, pages 285–297. Springer, 2005.

26 Tal Moran and Moni Naor. Polling with physical envelopes: A rigorous analysis of a human-centric protocol. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006*, volume 4004 of *LNCS*, pages 88–108. Springer, 2006. doi:10.1007/11761679_7.

27 Tal Moran and Moni Naor. Split-ballot voting: everlasting privacy with distributed trust. *ACM Trans. Inf. Syst. Secur.*, 13:246–255, 2010. doi:10.1145/1315245.1315277.

28 Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Pile-shifting scramble for card-based protocols. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 101(9):1494–1502, 2018.

29 Tatsuya Sasaki, Takaaki Mizuki, and Hideaki Sone. Card-based zero-knowledge proof for Sudoku. In Hiro Ito, Stefano Leonardi, Linda Pagli, and Giuseppe Prencipe, editors, *9th International Conference on Fun with Algorithms, FUN 2018, June 13-15, 2018, La Maddalena, Italy*, volume 100 of *LIPIcs*, pages 29:1–29:10. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2018. doi:10.4230/LIPIcs.FUN.2018.29.

30 Kazumasa Shinagawa and Takaaki Mizuki. The six-card trick: Secure computation of three-input equality. In Kwangsu Lee, editor, *Information Security and Cryptology – ICISC 2018*, volume 11396 of *LNCS*, pages 123–131, Cham, 2019. Springer.

31 Kazumasa Shinagawa, Takaaki Mizuki, Jacob C. N. Schuldt, Koji Nuida, Naoki Kanayama, Takashi Nishide, Goichiro Hanaoka, and Eiji Okamoto. Multi-party computation with small shuffle complexity using regular polygon cards. In Man Ho Au and Atsuko Miyaji, editors, *Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, Proceedings*, volume 9451 of *LNCS*, pages 127–146. Springer, 2015. `doi:10.1007/978-3-319-26059-4_7`.

32 Kazumasa Shinagawa and Koji Nuida. A single shuffle is enough for secure card-based computation of any circuit. *IACR Cryptology ePrint Archive*, pages 1–19, 2019.

33 Itaru Ueda, Daiki Miyahara, Akihiro Nishimura, Yu-ichi Hayashi, Takaaki Mizuki, and Hideaki Sone. Secure implementations of a random bisection cut. *International Journal of Information Security*, 19:445–452, August 2019. `doi:10.1007/s10207-019-00463-w`.

34 Putranto Hadi Utomo and Ruud Pellikaan. Binary puzzles as an erasure decoding problem. In *Proceedings of the 36th WIC Symposium on Information Theory in the Benelux*, pages 129–134, 2015. URL: `www.win.tue.nl/~ruudp/paper/72.pdf`.