### Physical Zero-Knowledge Proofs for Five Cells

Suthee Ruangwises The University of Electro-Communications, Tokyo, Japan

LATINCRYPT 2023 - Quito, Ecuador October 6, 2023

### Introduction



#### **Five Cells**

- A pencil puzzle consisting of an  $n \times n$  grid
- Some cells with a number
- Objective: Partition the grid into pentominoes.
  - A number indicates how many edges of that cell are borders of pentominoes (including outer boundary of the grid).

3				
1	2			3
3			2	1
2				2
		1		3

3				
1	2			3
3			2	1
2				2
		1		3



### Five Cells

- Developed by a Japanese company Nikoli
  - Famous for developing many pencil puzzles, e.g. Sudoku, Akari, Numberlink
- Deciding solvability of a given puzzle is NP-complete (Iwamoto and Ide, 2022).

# Zero-Knowledge Proof

- Patricia creates a Five Cells Puzzle and challenges her friend Victor to solve it.
- He can't solve it and doubts whether it really has a solution.
- Patricia needs to convince him that her puzzle has a solution without revealing it.
- She needs a zero-knowledge proof (ZKP).

# Zero-Knowledge Proof

- Interactive proof between a prover *P* and a verifier *V*
- Completeness: If *P* knows the solution, then *P* can convince *V*.
- Soundness: If *P* doesn't know the solution, then *P* can't convince *V*.
- Zero-knowledge: *V* learns nothing about *P*'s solution.

## Physical Card-based Protocols

- Does not require computer
- Uses only small, portable objects
- Easy for observers to verify the correctness and security, even for nonexperts in cryptography
- Suitable for teaching purpose

## Card-based ZKP for Pencils Puzzles

- Sudoku
- Kakuro
- Makaro
- Akari
- Takuzu
- Juosan



- Numberlink
- etc.



## **Our Contribution**

- Develop a card-based ZKP for Five Cells.
  - Has perfect completeness and soundness.

### Preliminaries















### **Pile-Shifting Shuffle**



## **Chosen Cut Protocol**

- Allows *P* to select a desired card from a sequence without revealing which one.
- Developed by Koch and Walzer (2020)



### **Chosen Cut Protocol**





## Idea of the Protocol

- Key Observation: There are only 0(1) different types of pentomino.
  - Namely, there are 63 of them.
- We create 63 templates, one for each pentomino.
- Then, we "print" the templates onto the grid.



#### CreatingTemplates





#### CreatingTemplates





- Create 63 templates and let V verify that they are correct.
- Use the chosen cut protocol to select a desired template, and a desired 5×5 area from the grid.



- Place each card from the template on top of a corresponding card from the grid.
- Shuffle the two cards and reveal one  $\boxed{\emptyset}$  to *V*. (At least one card must be a  $\boxed{\emptyset}$ .)



- Reconstruct a template that was used and replenish the pile of templates with it.
- Let V verify that all 63 templates are correct again. (V doesn't know which template has just been used.)
- Do this for all pentominoes until the grid is fully filled.



- Finally, reveal all cards on the cells with a number (in the original puzzle).
- Let *V* verify that the numbers on the cards match the numbers on the cells.

### **FutureWork**



## FutureWork

- Apply the idea of the printing protocol to construct ZKPs for other decomposition puzzles.
  - E.g. Meadows, Trinudo, Fillmat

#### **Questions and Comments**