Physical Zero-Knowledge Proofs for Five Cells

E -C ,

,

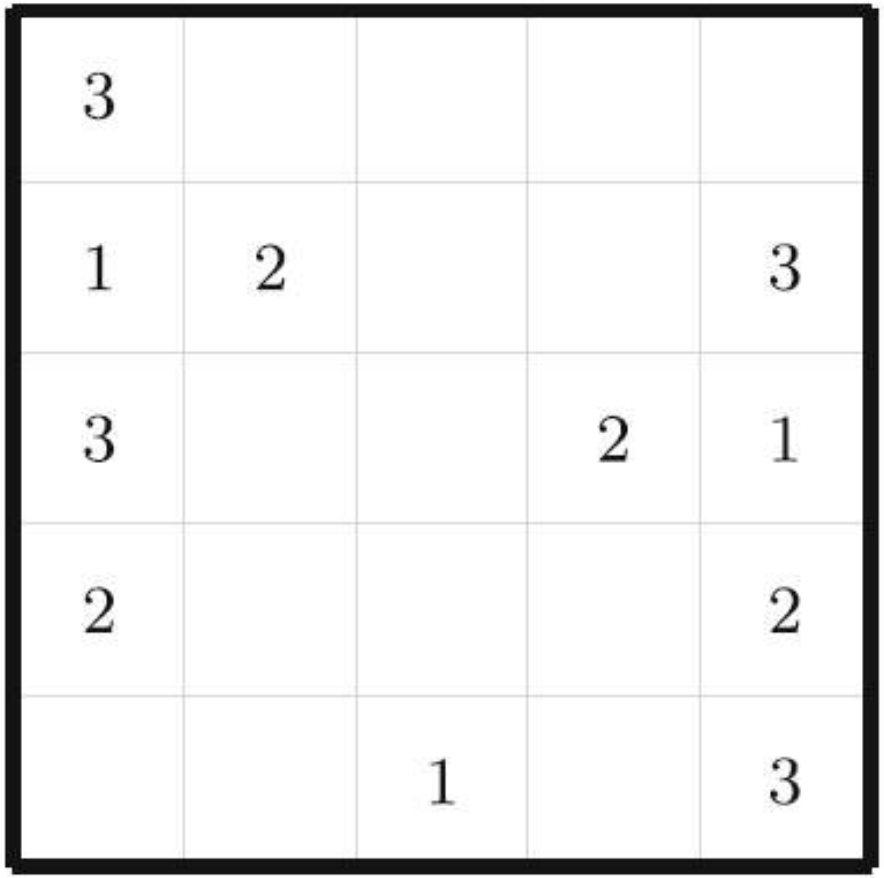
A C 2023 - ,E

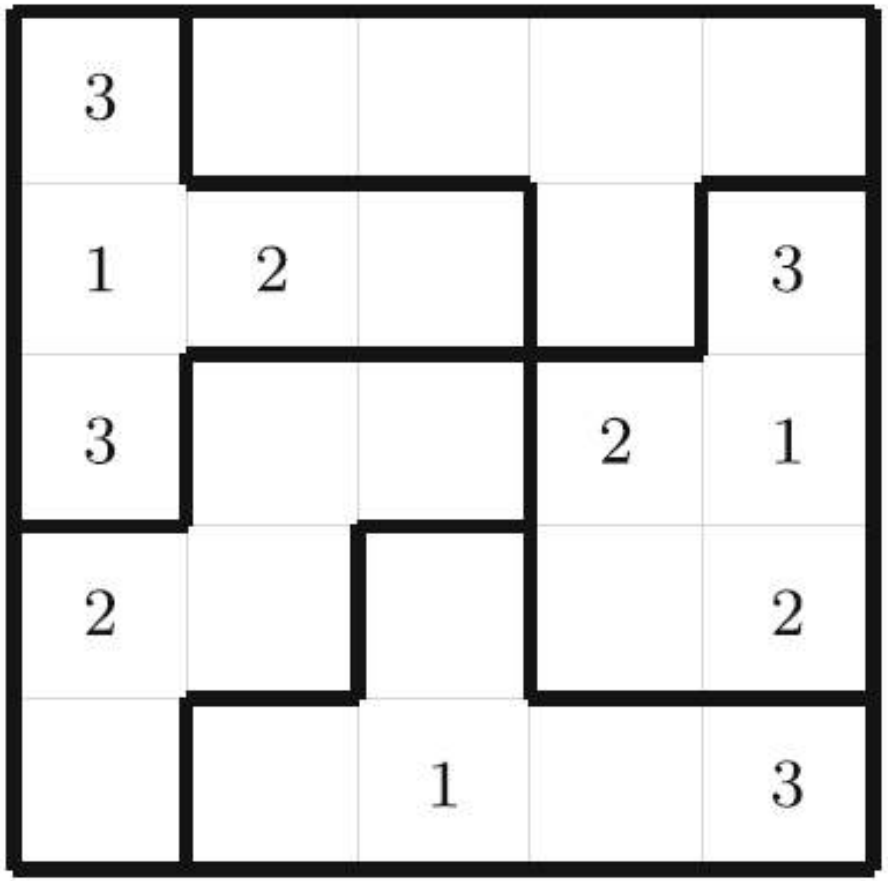
6, 2023

Introduction

Five Cells

- A $n \times n$
-
- :
  - A ( ).


3
1 2 3
3 2 1
2 2
1 3


3
1 2 3
3 2 1
2 2
1 3

Five Cells

- D[illegible]
  - F[illegible], [illegible] A[illegible], [illegible]
- D[illegible] [illegible]-[illegible] (I[illegible] [illegible], 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 (ZK).

Zero-Knowledge Proof

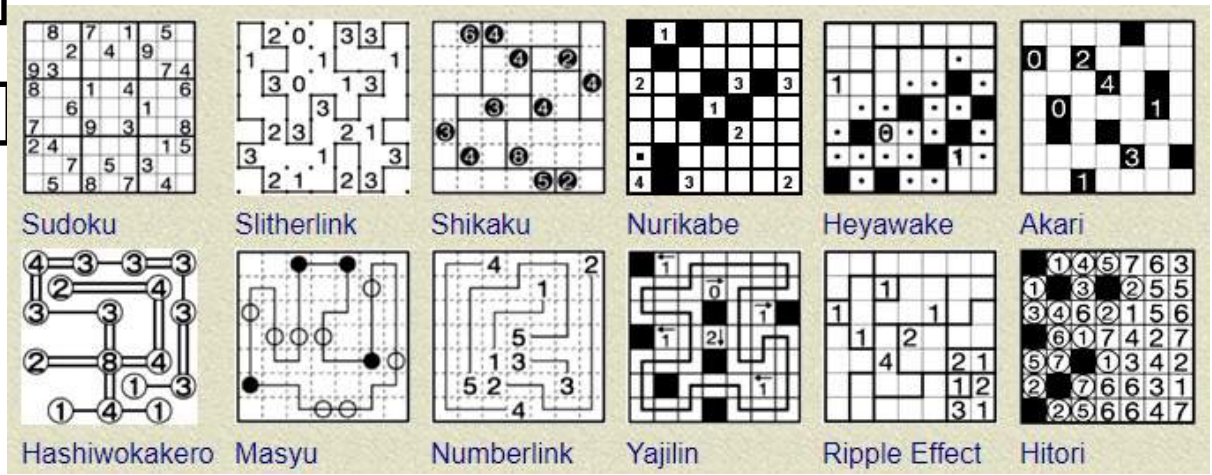
- Interaction between P and V
- Completeness: If P knows the secret, P can convince V.
- Soundness: If P doesn't know the secret, P can't convince V.
- Zero-knowledge: V learns nothing from P.

Physical Card-based Protocols

- D
- ,
- E
  ,
  -
- .

[illegible]

- [illegible]
- [illegible]
- [illegible]
- A [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

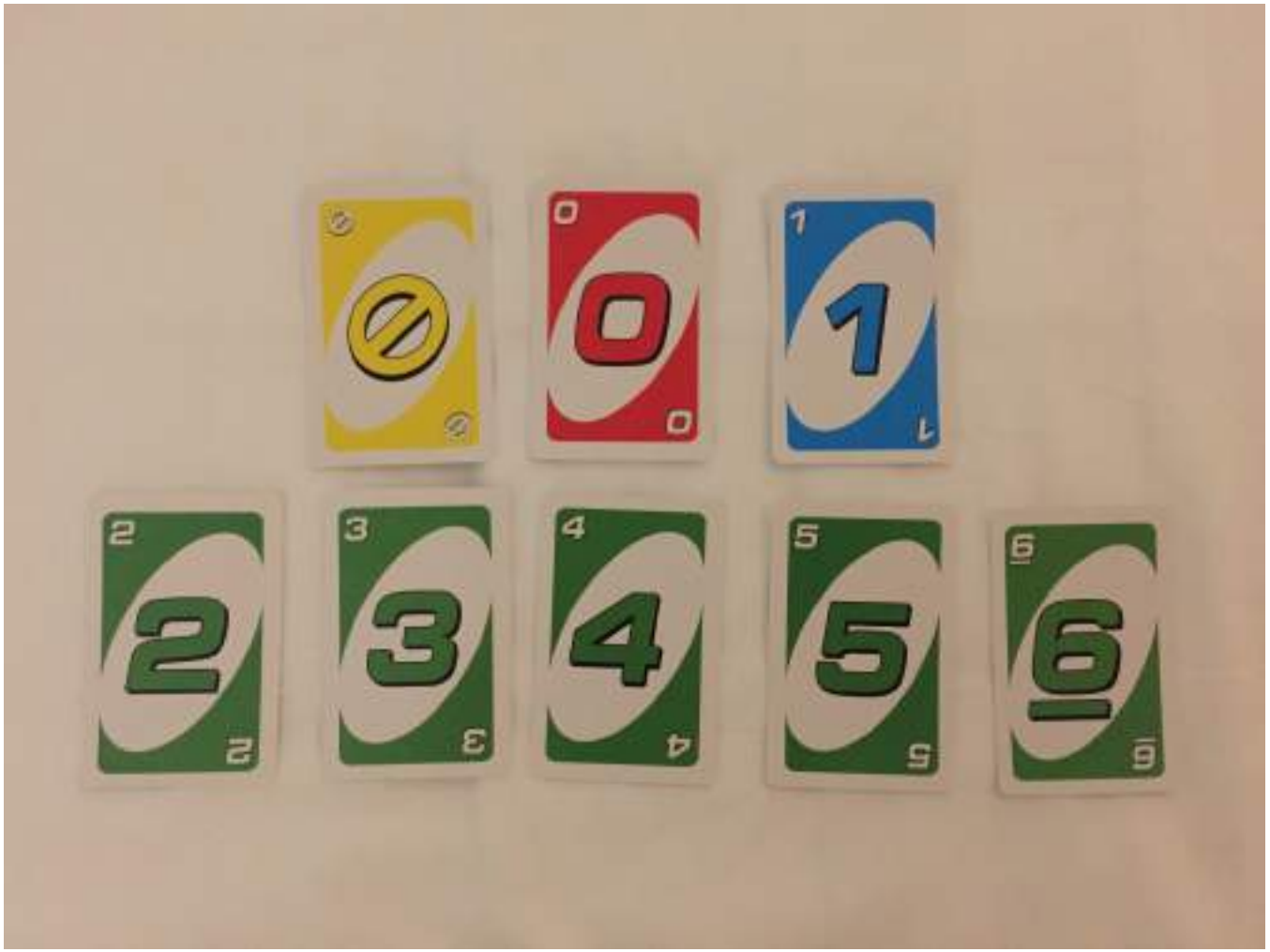

Sudoku
Slitherlink
Shikaku
Nurikabe
Heyawake
Akari
Hashiwokakero
Masyu
Numberlink
Yajilin
Ripple Effect
Hitori

Our Contribution

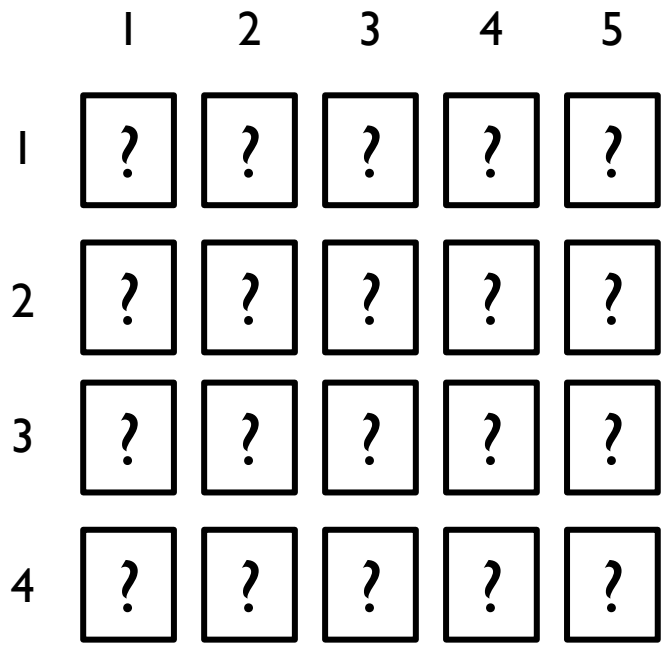
- D[illegible]-[illegible]F[illegible]C[illegible].
  - H[illegible].

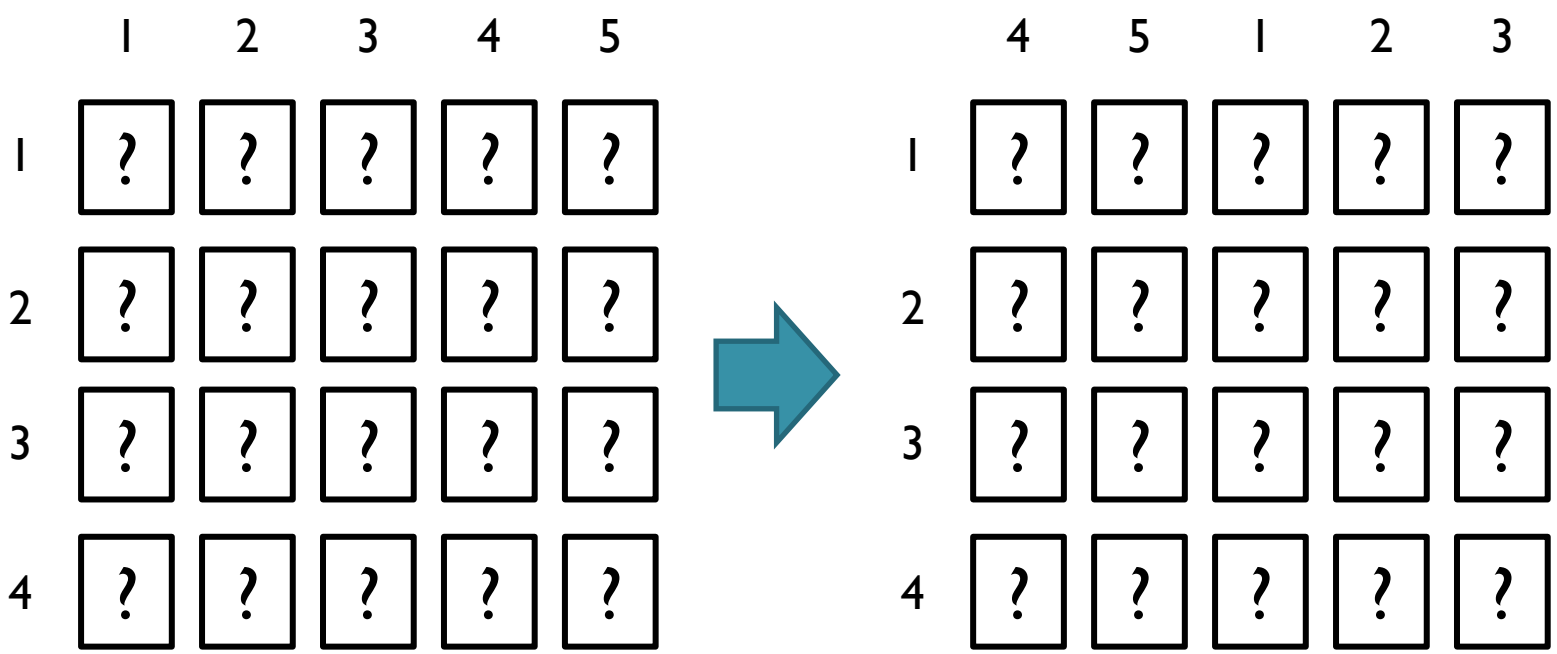
Preliminaries

C□□□□



Matriks




1 2 3 4 5
1 ? ? ? ? ?
2 ? ? ? ? ?
3 ? ? ? ? ?
4 ? ? ? ? ?
4 5 1 2 3
1 ? ? ? ? ?
2 ? ? ? ? ?
3 ? ? ? ? ?
4 ? ? ? ? ?

Chosen Cut Protocol

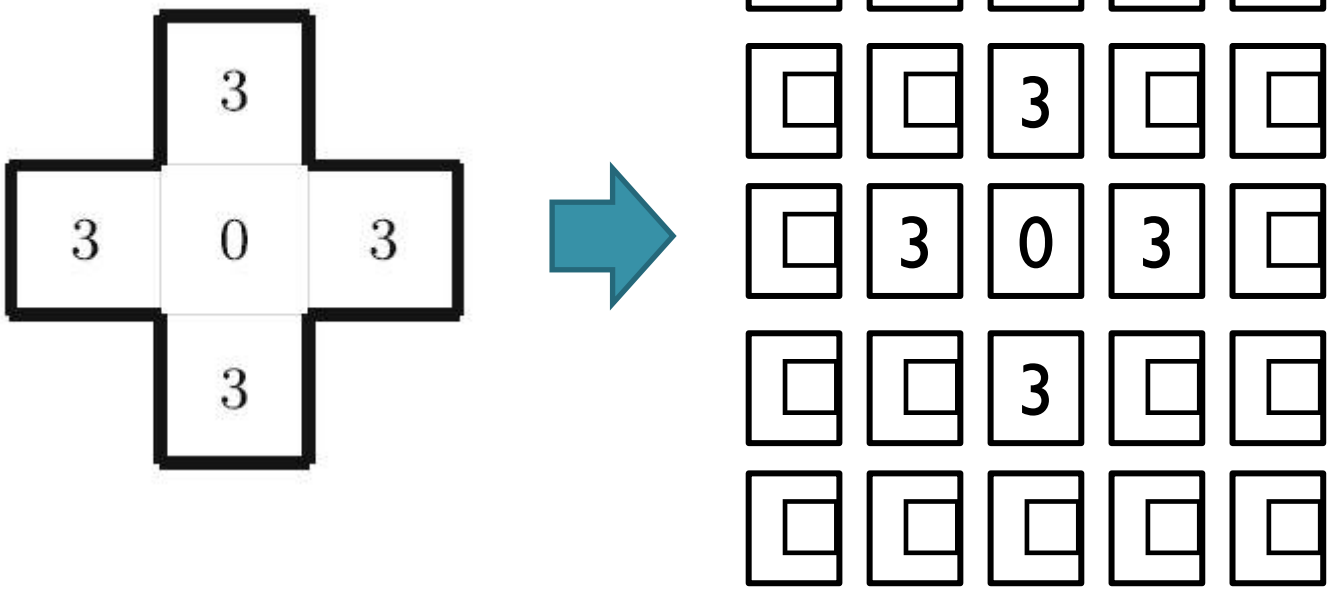
- Allows P to select a desired card from a sequence without revealing which one
- Developed by Koch and Walzer (2020)

Chosen Card Placeholder

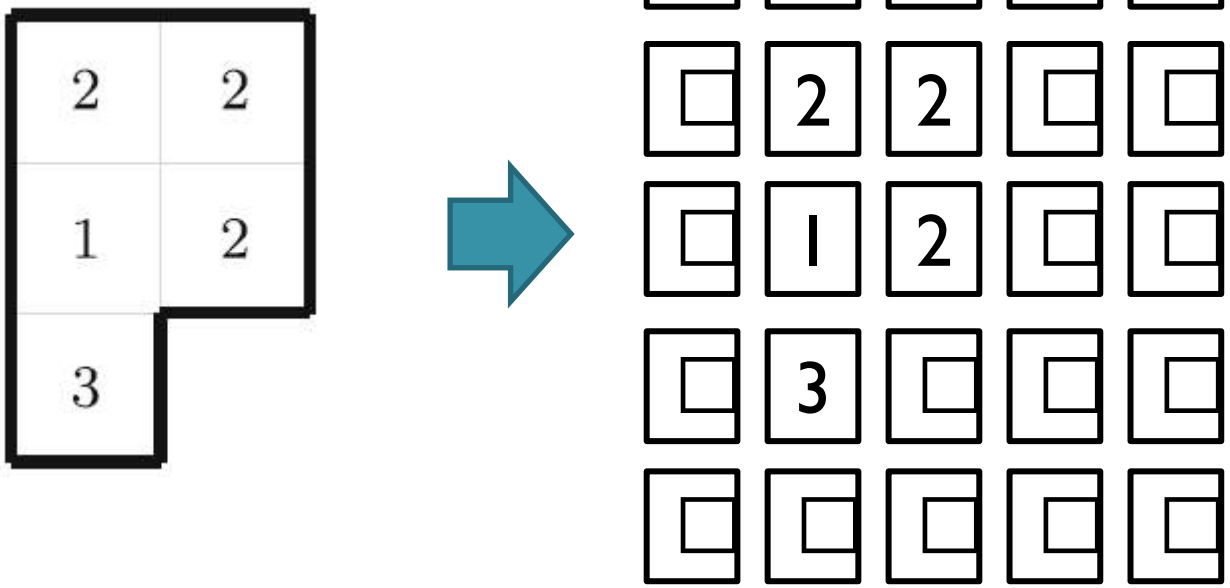
Idea of the Protocol

- Basic Concept: Operations in O(1) time.
  - Example, Bitmap of 63 elements.
- A Bitmap of 63 elements, Bitmap Operations
- Finally, Bitmap Operations

Creating Templates



Creating Templates



Main Protocol

- 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

Main Protocol

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

Main Protocol

- Reconstruct a template that was used and replenish the pile of templates with it
- Let V verify that all 33 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

Main Protocol

- 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

Future Work

- A
  - E.

Questions and Comments