Physical Zero-Knowledge Proofs for Akari, Takuzu, Kakuro and KenKen

X. Bultel\textsuperscript{1}  J. Dreier\textsuperscript{2}  J-G. Dumas\textsuperscript{3}  P. Lafourcade\textsuperscript{1}

\textsuperscript{1}LIMOS, University Clermont Auvergne, France
\textsuperscript{2}Université de Lorraine, LORIA, Nancy, France
\textsuperscript{3}LJK, Université Grenoble Alpes, Grenoble, France

FUN’16, 9th June 2016, Sardinia
Zero-Knowledge proof of knowledge

**Prover** knows a solution $s$ of $P$

**Verifier** knows the problem $P$

bla bla...  \[\rightarrow\]

bla bla?  \[\leftarrow\]

bla bla!  \[\rightarrow\]

accept or reject $s$ as a solution of $P$
Completeness

**Prover** knows a solution $s$ of $P$

**Verifier** knows the problem $P$

bla bla…

bla bla?

bla bla!

Hum, ok…
I’m convinced!
$s$ is a solution of $P$
Soundness

**Prover** does not know a solution $s$ of $P$

---

**Verifier** knows the problem $P$

---

bla bla...

bla bla?

bla bla!

---

Hum, ...

I detect a problem!

$s$ is not a solution
Zero-Knowledge

**Prover** knows a solution $s$ of $P$

**Verifier** knows the problem $P$

---

bla bla...

<table>
<thead>
<tr>
<th>bla bla?</th>
</tr>
</thead>
</table>

| bla bla! |

---

I do not learn anything about $s$
Origins of ZKP


Related Works

R. Gradwohl, M. Naor, B. Pinkas, and G. N. Rothblum \textit{(FUN’07)}

Physical (using cards) ZKP for Sudoku.

<table>
<thead>
<tr>
<th>Prover</th>
<th>Verifier</th>
</tr>
</thead>
<tbody>
<tr>
<td>\begin{array}{</td>
<td>c</td>
</tr>
</tbody>
</table>

bla bla bla... →
bla bla bla?
bla bla bla!
accept or reject
Contributions

Physical Zero-Knowledge Proofs for 4 NP-complete games:

- **Akari**
- **Takuzu**
- **Kakuro**
- **KenKen**
1 Zero-Knowledge Proofs and Logical Games
   - Zero-Knowledge proofs
   - Related Works

2 Akari
   - Rules for Akari
   - ZKP Protocol

3 Kakuro
   - Rules for Kakuro
   - ZKP Protocol
   - Extension to KenKen

4 Conclusion
**GOAL**: Place lights on the white cells on the grid such that 3 constraints are respected.
A light \( \bigcirc \) illuminates the whole row and column up to a black cell.
Constraints (1/3)

- Two lights cannot illuminate each other

```
   〇 〇 〇 〇
   〇 4 〇 〇
   〇 〇 1 〇
   0 0 〇 〇
   〇

   〇 〇 〇 〇
   〇 4 〇 〇
   〇 〇 1 〇
   0 0 〇 〇
   〇
```
Contraints (2/3)

- All cells are illuminated!
Contraints (3/3)

- Numbers in black cells = adjacent lights
Prover Commitment

Prover commitment:

- use the empty grid, empty cards and ○ cards.
Prover commitment:

- use the empty grid, empty cards and ○ cards.
- put a packet of identical cards on each white cell according to the solution.
Verification (1/3)

Numbers in black cells = adjacent lights
Verification (1/3)

Numbers in black cells = adjacent lights

For each black cell with number $x$:
pick one card in all adjacent white cells and shuffle them.
Verification (1/3)

Numbers in black cells = adjacent lights

For each black cell with number $x$:
- pick one card in all adjacent white cells and shuffle them.

$\lor$ checks that there is exactly $x \circ$ cards.
Verification (2/3)

No two lights see each other $\iff$ At most one $\bullet$ by row/column.
Verification (2/3)

No two lights see each other \iff At most one \( \bigcirc \) by row/column.
For each row/column, take one card per cell and shuffle them.
Verification (2/3)

No two lights see each other ⇔ At most one ○ by row/column. For each row/column, take one card per cell and shuffle them.

- **case 1**, empty cards: $P$ adds a ○ card
**Verification (2/3)**

No two lights see each other $\iff$ At most one $\bigcirc$ by row/column. For each row/column, take one card per cell and shuffle them.

- **case 1**, empty cards: $P$ adds a $\bigcirc$ card $\rightarrow$ exactly 1 $\bigcirc$
Verification (2/3)

No two lights see each other $\iff$ At most one $\bigcirc$ by row/column. For each row/column, take one card per cell and shuffle them.

- **case 1**, empty cards: $P$ adds a $\bigcirc$ card $\rightarrow$ exactly 1 $\bigcirc$
- **case 2**, one $\bigcirc$: $P$ adds an empty card
No two lights see each other \iff \text{At most one } \bigcirc \text{ by row/column.} 
For each row/column, take one card per cell and shuffle them.

- **case 1**, empty cards: P adds a \bigcirc card \rightarrow exactly 1 \bigcirc
- **case 2**, one \bigcirc: P adds an empty card \rightarrow exactly 1 \bigcirc

V checks that there is exactly one \bigcirc card.
**Verification (3/3)**

<p>| | | | | | | | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**All cells are illuminated** ⇔ For each cell, at least one `○` in its row and column.
Verification (3/3)

All cells are illuminated $\iff$ For each cell, at least one $\bigcirc$ in its row and column.

For each cell, take one card per cell in the same row and column and shuffle them.
All cells are illuminated ⇔ For each cell, at least one ○ in its row and column.
For each cell, take one card per cell in the same row and column and shuffle them.

- **case 1**, one ○: $P$ adds a ○ card
Verification (3/3)

All cells are illuminated $\Leftrightarrow$ For each cell, at least one $\bigcirc$ in its row and column.

For each cell, take one card per cell in the same row and column and shuffle them.

- case 1, one $\bigcirc$: $P$ adds a $\bigcirc$ card $\rightarrow$ exactly 2 $\bigcirc$

All cells are illuminated ⇔ For each cell, at least one  in its row and column.
For each cell, take one card per cell in the same row and column and shuffle them.

- case 1, one : P adds a card → exactly 2
- case 2, two : P adds an empty card
Verification (3/3)

All cells are illuminated ⇔ For each cell, at least one ○ in its row and column.
For each cell, take one card per cell in the same row and column and shuffle them.

- **case 1**, one ○: $P$ adds a ○ card ↦ exactly 2 ○
- **case 2**, two ○: $P$ adds an empty card ↦ exactly 2 ○
All cells are illuminated $\iff$ For each cell, at least one $\bigcirc$ in its row and column.
For each cell, take one card per cell in the same row and column and shuffle them.

- case 1, one $\bigcirc$: $P$ adds a $\bigcirc$ card $\rightarrow$ exactly 2 $\bigcirc$
- case 2, two $\bigcirc$: $P$ adds an empty card $\rightarrow$ exactly 2 $\bigcirc$

$V$ checks that there is exactly two $\bigcirc$ cards.
1 Zero-Knowledge Proofs and Logical Games
   • Zero-Knowledge proofs
   • Related Works

2 Akari
   • Rules for Akari
   • ZKP Protocol

3 Kakuro
   • Rules for Kakuro
   • ZKP Protocol
   • Extension to KenKen

4 Conclusion
Kakuro: Cross Sums

- Digits from 1 to 9.
- Triangular cell = sum of digits in the row/column
- A number can appear only once per row/column.
Digit Encoding

Using black and red cards.
To represent a number $x$ put in an envelope:
- $9 - x$ black cards
- $x$ red cards

For 3: 

\[\text{■■■■■■■■■} \rightarrow \text{Envelope}\]
Prover Commitment

- Draw an empty grid

Commitment:
Prover Commitment

- Draw an empty grid
- On each empty cell: put 4 identical envelopes encoding the digit

Commitment:
Prover Commitment

- Draw an empty grid
- **On each empty cell:** put 4 identical envelopes encoding the digit
- **On each triangular cell:** put envelopes encoding all missing digits in the row/column

Commitment:

$\times7$ for 3, 4, 5, 6, 7, 8 and 9
Verification (1/2)

A number appears only once per row/column

- For each row/column, pick an envelope per cell plus the envelopes on the triangular cell.
Verification (1/2)

A number appears only once per row/column

- For each row/column, pick an envelope per cell plus the envelopes on the triangular cell.
- Shuffle and open them.
Verification (1/2)

A number appears only once per row/column

- For each row/column, pick an envelope per cell plus the envelopes on the triangular cell.
- Shuffle and open them.
- Verify that all numbers between 1 and 9 appear exactly once.

1,2,3,4,5,6,7,8,9
Verification (2/2)

The sum per row and per column corresponds to the number in the triangular cell

- Randomly picks one envelope per cell in the row/column.
- Opens (face down) the content of each envelope and shuffle it.
- Check that red cards corresponds to the number given in the triangular cell.

\[
\begin{array}{ccc}
4 & & 3 \\
3 & 1 & 2 \\
4 & & \\
\end{array}
\]

\[
\begin{array}{c}
\text{Red cards} \\
\text{Total sum}
\end{array}
\]

\[
\begin{array}{c}
\text{X.Bultel et al.} \\
ZKP for Akari et al. \\
FUN’16
\end{array}
\]
KenKen

- **Addition**: similar to Kakuro.
- **Multiplication**: addition of the exponent of each prime factors.

\[ 9 \times 6 = (2^03^2) \times (2^13^1) = 2^{0+1}3^{2+1} = 54 \]

- **Subtraction/division**: finding the maximum.
Conclusion

Physical Zero-Knowledge Proofs for:

- Akari
- Takuzu
- Kakuro
- KenKen

More Games!
Conclusion

Physical zero-knowledge mechanisms for several constraints:

- At least/most one occurrence of a symbol in a row/column.
- Equality of the number of 1 and 0 per row/column.
- Result of the addition/subtraction of cells.
- Result of the multiplication/division of cells.
- Number of adjacent symbol.
- All rows/columns are different.
- No \( k \) consecutive identical symbols.
Thank you for your attention.

Questions?
Takuzu Rules: Binary Puzzle

**Goal:** fill the grid with 0’s and 1’s

![Takuzu Grid Example](image)

- Each row/column has exactly the same number of 1’s and 0’s
- Each row/column is unique
- In each row/column there can be no more than 2 identical numbers next to each other: **110010**, but **110001**

![Takuzu Grid Example](image)