Cryptographic and Physical Zero-Knowledge Proof Systems for Solutions of Sudoku Puzzles

Ronen Gradwohl **Moni Naor** **Benny Pinkas** **Guy Rothblum**

http://www.wisdom.weizmann.ac.il/~naor/PAPERS/sudoku_abs.html

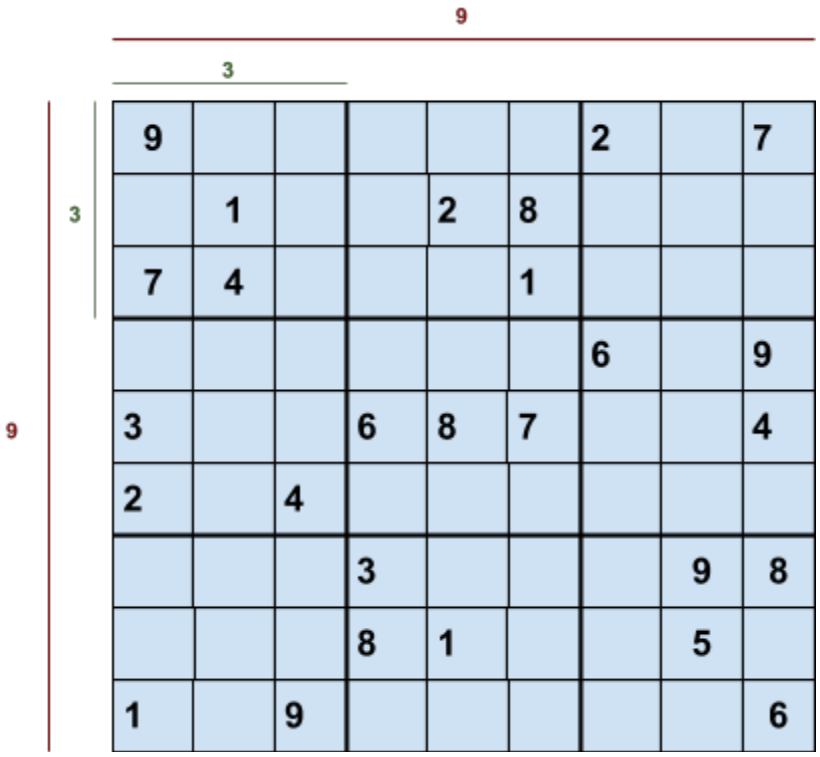
The game

- Defined by the size $n = k^2$ of an $n * n$ grid
- Subgrids of $k * k$
- Some of the cells are filled with values in the range $\{1, ..., n\}$

GOAL: Fill the remaining cells with numbers from the same range so that each number appears exactly once in each **row**, **column** and **subgrid.**

Common Example:

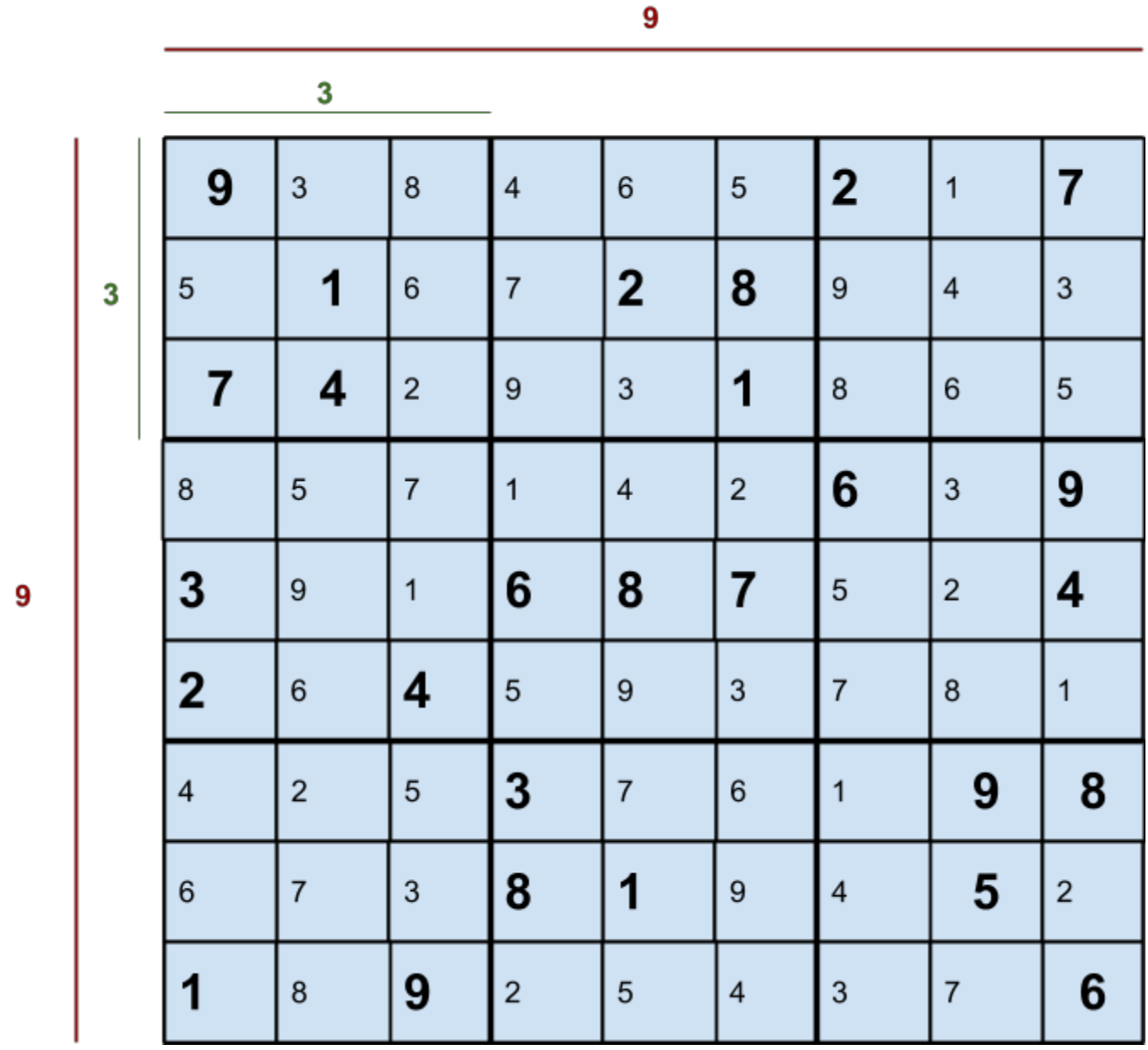
- $n = 3^2$ **,** Grid **9 * 9**
- Subgrids of **3 * 3**



9						2		7
	1			2	8			
7	4				1			
						6		9
3			6	8	7			4
2		4						
			3				9	8
			8	1			5	
1		9						6

Fill the empty entries in the grid in a way that:

- **every row contains digits 1 to 9**
- **every column contains digits 1 to 9**
- **every 3x3 subgrid contains digits 1 to 9**



9	3	8	4	6	5	**2**	1	**7**
5	**1**	6	7	**2**	**8**	9	4	3
7	**4**	2	9	3	**1**	8	6	5
8	5	7	1	4	2	**6**	3	**9**
3	9	1	**6**	**8**	**7**	5	2	**4**
2	6	**4**	5	9	3	7	8	1
4	2	5	**3**	7	6	1	**9**	**8**
6	7	3	**8**	**1**	9	4	**5**	2
1	8	**9**	2	5	4	3	7	**6**

Protocol 6 A physical protocol using scissors

1. The prover takes a sheet of paper on which the puzzle is printed. He then writes down, for every cell with a filled-in value, this filled-in value on back side of the cell (namely, on the back of the page, right behind the printed filed-in value). The result is that filled-in cells, and only them, have their values written on both sides of the page.
2. The prover writes down the solution to the puzzle on the (original) printed puzzle, and keeps this side of the page hidden from the verifier.
3. The verifier checks that the prover wrote the right values on the back of the puzzle.
4. If the previous check is fine, the verifier chooses one option out of rows/columns/subgrids.
5. Suppose that the verifier chooses “rows”. The prover then cuts the puzzle and separates it into n rows. (If the choice is “columns” the prover separates the columns from each other, and similarly for subgrids. In the rest of the protocol description we then replace the word “row” by “column”, or “subgrid”, according to the verifier’s choice above.) The prover then cuts each row to separate it into n cells. He shuffles the cells of each row (separately from the cells of other rows) and then hands them to the verifier.
6. The verifier checks that: (1) each row contains all n values, (2) in each row the cells whose value is written on both sides agree with the filled-in values of that row in the puzzle, and (3) these cells have the same value written on both their sides.

Can the prover cheat?

Perfect soundness with a trusted copy machine:

1. Prepare copies of the solution
2. One copy is cut along the rows
3. One copy is cut along the columns
4. One copy is cut along the subgrids
5. Each strip is cut into cells
6. Prover shuffles or sorts the cells
7. Verifier checks that:
    a. all 1...9 values are there
    b. the filled-in cells have the same values on both sides

The trusted copy machine:

1. **makes copies in a way which ensures the verifier that the copies are identical**
2. **ensures the prover that the verifier does not see the copied solution**

Our example puzzle:

8	3	9	4	6	1	7	5	2
5	4	6	8	7	2	3	1	9
2	1	7	3	5	9	6	4	8
4	2	8	9	3	6	1	7	5
6	9	5	2	1	7	8	3	4
3	7	1	5	8	4	9	2	6
1	6	2	7	9	5	4	8	3
7	8	4	6	2	3	5	9	1
9	5	3	1	4	8	2	6	7