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

To be presented in FUN in Algorithms 2007

Benny Pinkas

Joint work with Ronen Gradwohl, Moni Naor and Guy Rothblum

Sudoku

Can be generalized to an n×n grid, where $n=k^2$.

Here, k=3, n=9.

The question

- How to convince someone that you solved a Sudoku puzzle, without revealing the solution.

- In other words, prove that
  - There is a solution to the puzzle
  - You know the solution
  - But do this without revealing the solution.

- In other words: ZK proofs of knowledge for Sudoku.

Related Work [NNR]

- Where is Waldo?

ZK proofs for Sudoku

- Sudoku is in NP (in fact, it is NP Complete)
  - So why bother designing special proofs?

- Direct ZK proofs for Sudoku are preferable:
  - Efficiency
  - Practicality: Implementable without the aid of computers
  - Understandability (by non-experts!): Ensure that participants have intuitive understanding of the proof.
- Our Results
  - Cryptographic solutions: two machines exchange messages. Security based on computational assumptions.
  - Physical solutions: Implementable by humans without involving computers.

A demo of a Physical ZK protocol for Sudoku

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

Daily SuDoku: Tue 1-May-2007 very hard

Analysis

- Completeness: perfect.

- Soundness: If Prover doesn't know a solution, then it cannot answer at least one of the verifier's 3 choices.
  – Cheating probability ("Soundness error"): 2/3 *(might be too high)*

- Zero-knowledge:
  – Obviously you didn't learn anything from what you saw.
  – This property can be defined and analyzed.
- Knowledge extractor:
  – Can be defined and analyzed (not hard).

We describe several physical protocols

- The protocols use playing cards, or scratch-off cards.

- Possible criteria:
  - Number of cards
  - Number of shuffles
  - Soundness error

	# of cards	shuffles	soundness error
Protocol 1: “one card per cell”	n^2	n	2/3
Protocol 2: “all packets”	$3n^2$	3n	1/9
Protocol 3: “aggregate packets”	$3n^2$	c-1	1/9+8/(9c)
Protocol 4: “triplicate”	n (3n) special cards	3n	0

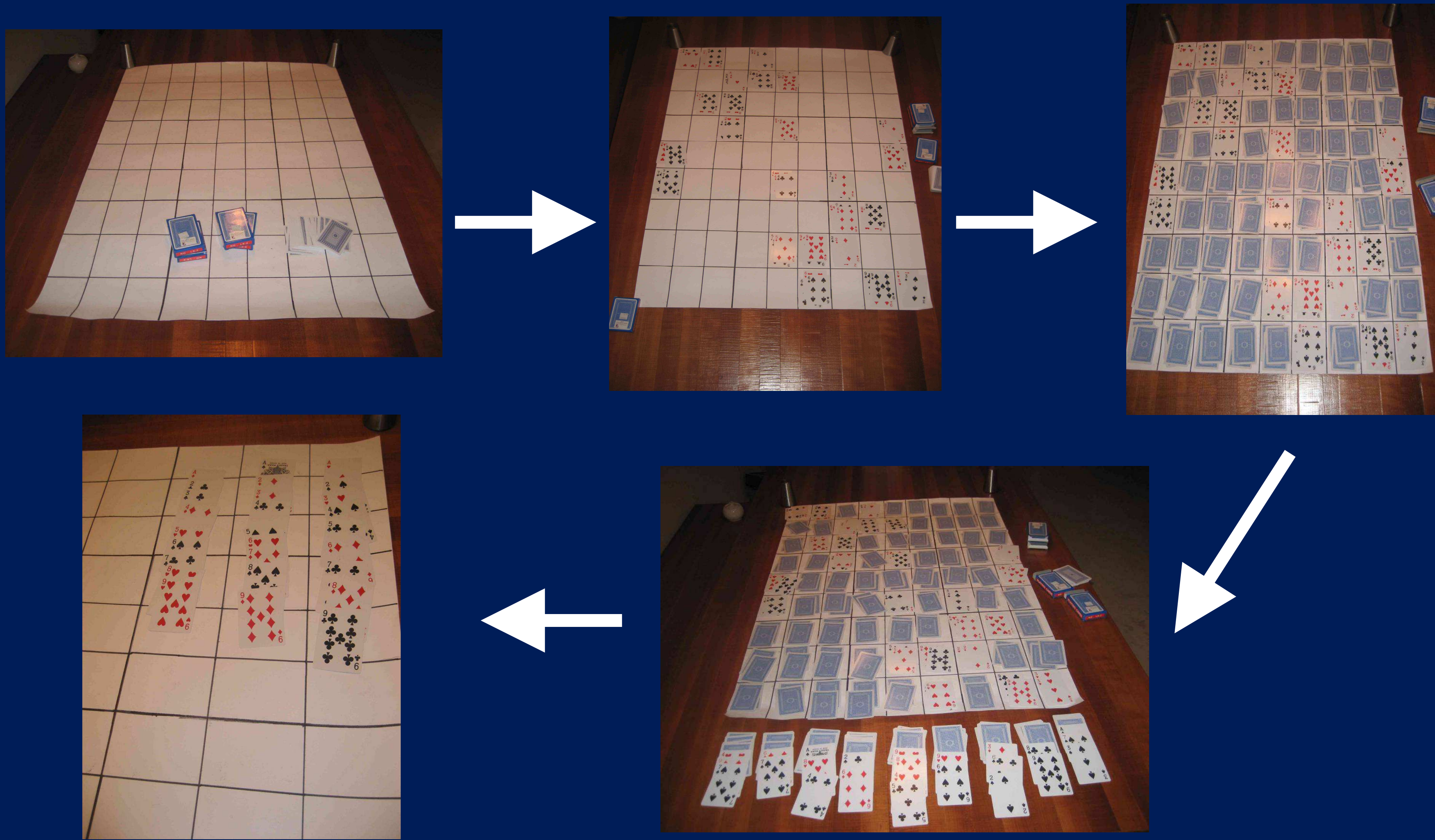
We describe several physical protocols

- The protocols use playing cards, or scratch-off cards.

- Possible criteria:
  - Number of cards
  - Number of shuffles
  - Soundness error

	# of cards	shuffles	soundness error
Protocol 1: “one card per cell”	n^2 **81**	n 9	2/3
Protocol 2: “all packets”	$3n^2$ 243	3n 27	**1/9**
Protocol 3: “aggregate packets”	$3n^2$ 243	**c-1** **3**	1/9+8/(9c)
Protocol 4: “triplicate”	n special cards	3n 27	0

Protocol 2 (using decks of cards)
http://www.wisdom.weizmann.ac.il/~naor/PAPERS/SUDOKU_DEMO



Discussion

- A good way to explain zero-knowledge for kids?

- Open problems:
  - Protocols over the mail?
    - [MN] showed how to implement commitments from scratch-off cards.
    - However, an amplification stage requires many repetitions
    - Not easy for humans

  - Non-interactive proofs (by the puzzle creator) [Berson]

  - Other puzzles?