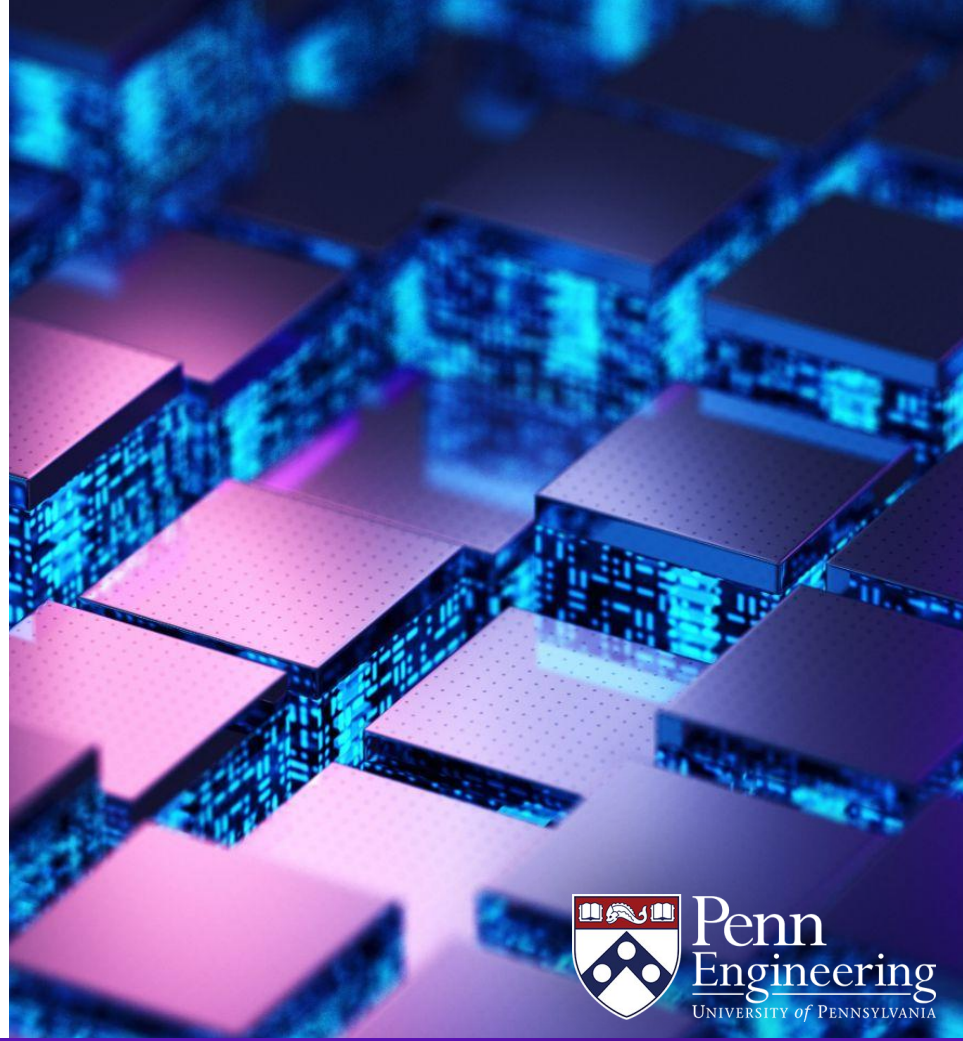
EAS 5830: BLOCKCHAINS

Zero-Knowledge Sudoku

Professor Brett Hemenway Falk



Sudoku

- Every cell has a number 1-9
- Every row has distinct entries
- Every column has distinct entries
- Each 3x3 subgrid has distinct entries

				7			8	
		1						
2					7			
		3						
							4	

Sudoku is NP complete

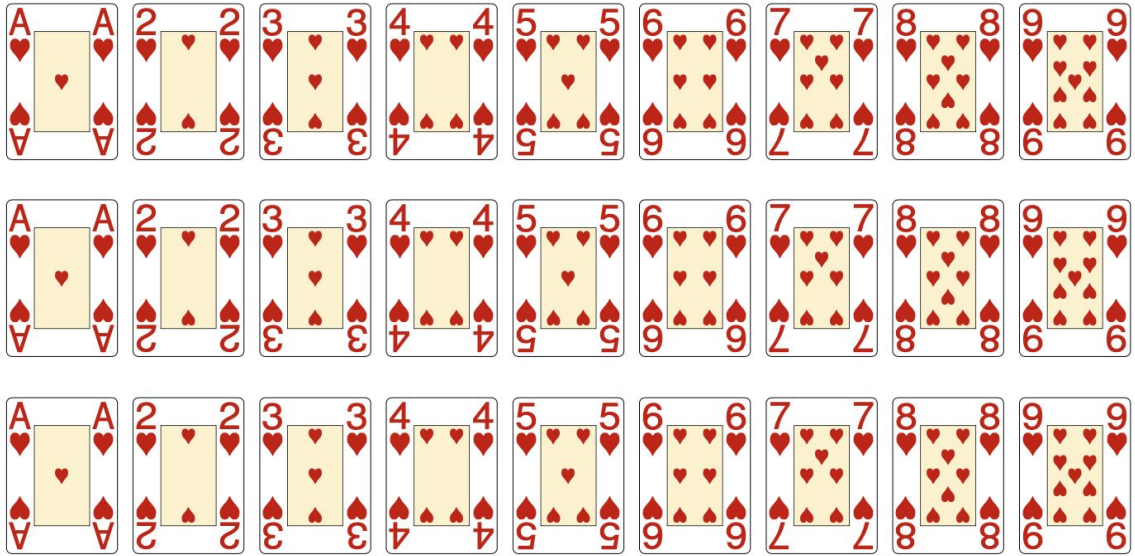
(Generalized) Sudoku is NP complete

Zero-Knowledge Sudoku

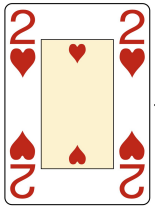
Prove you know a solution to a sudoku board without revealing any information about the solution

Prover

- Prover gets 9 decks of playing cards
  - Extract all the numerical hearts (suit doesn't matter)



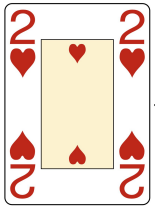
Sudoku prover



- Prover knows a solution
- For each square:
  - Choose a card with that value
  - Place card face down on the square
    - Don’t reveal card to verifier

	2			7			8	
		1						
2					7			
		3						
							4	

Sudoku prover

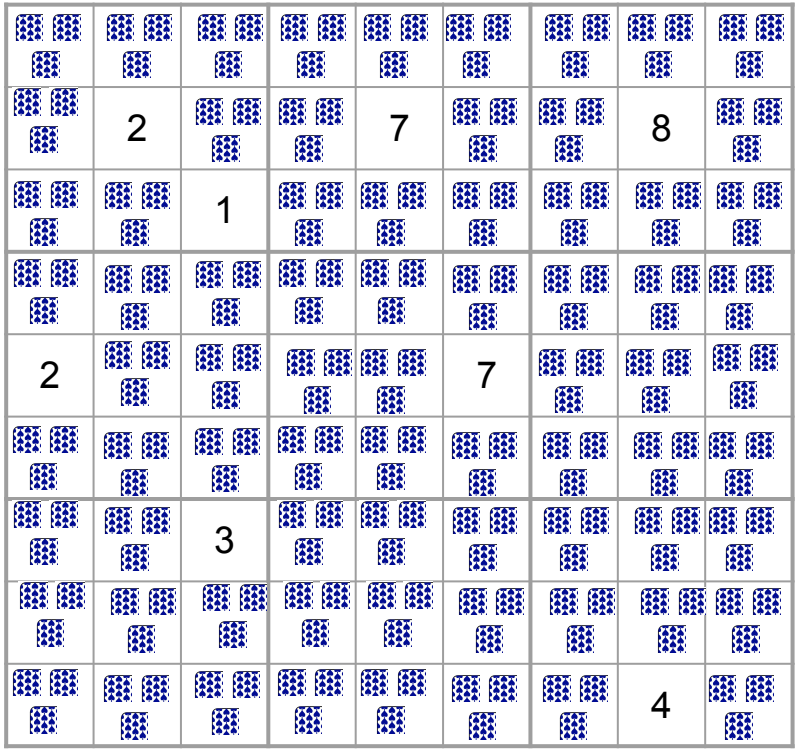


- Prover knows a solution
- For each square:
  - Choose a card with that value
  - Place card face down on the square
    - Don’t reveal card to verifier
  - Verifier cuts off three corners of the card (three copies of the number 2) and leaves them in the cell

	2			7			8	
		1						
2					7			
		3						
							4	

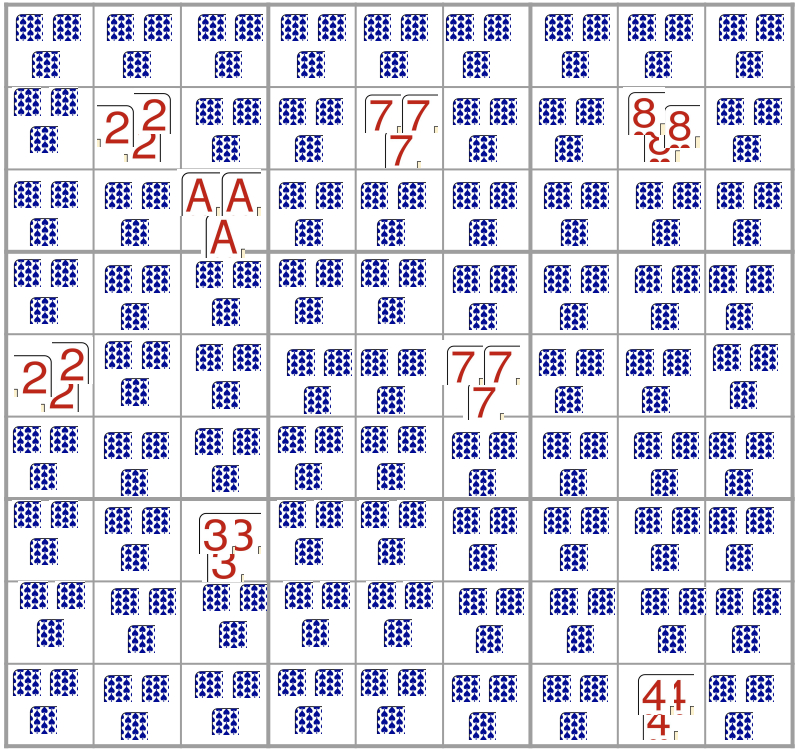
Sudoku prover

- Prover knows a solution
- For each square:
  - Choose a card with that value
  - Place card face down on the square
    - Don’t reveal card to verifier
  - Verifier cuts off three corners of the card (three copies of the number 2) and leaves them in the cell



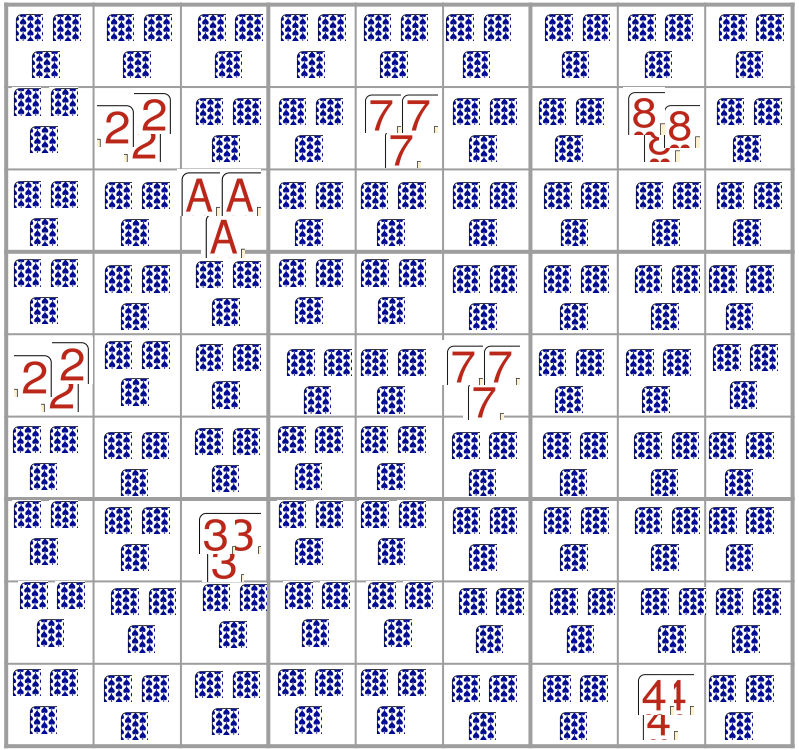
Sudoku prover

- Prover knows a solution
- For each square:
  - Choose a card with that value
  - Place card face down on the square
    - Don’t reveal card to verifier
  - Verifier cuts off three corners of the card (three copies of the number 2) and leaves them in the cell
  - Same procedure for pre-filled squares
    - These are done face-up



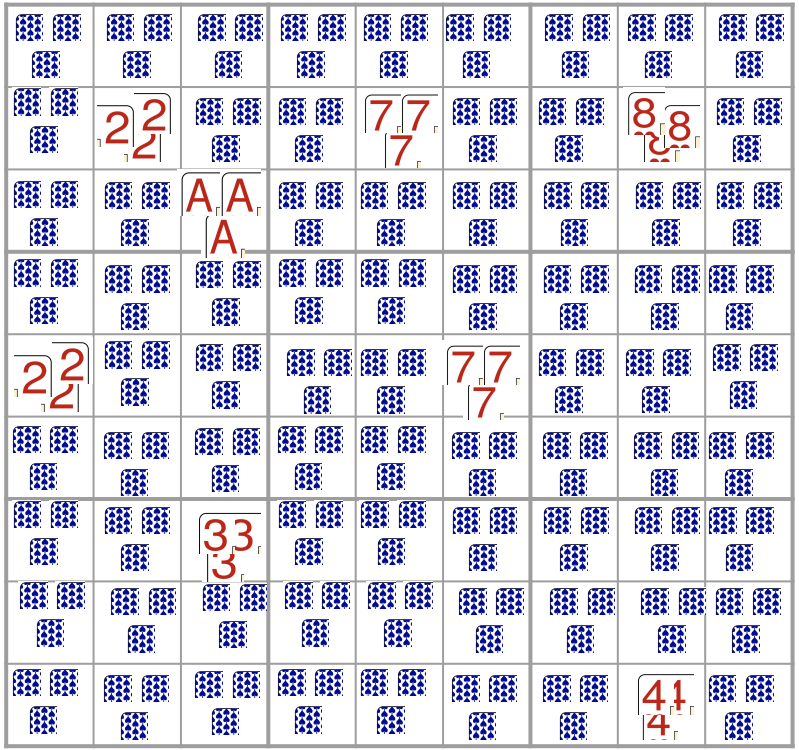
Sudoku prover

- At the end of this procedure:
  - Three card scraps in each square
  - Verifier knows all three have the same value
    - (They came from same card)
  - Three scraps in pre-filled entries are seen by verifier, and match pre-filled values



Sudoku prover

- For each **row**
  - Take one scrap of paper from each cell, and put it in an envelope for that row
- For each **column**
  - Take one scrap of paper from each cell, and put it in an envelope for that column
- For each **3x3 block**
  - Take one scrap of paper from each cell, and put it in an envelope for that block



Sudoku prover

- Prover has 27 envelopes
  - 9 for rows
  - 9 for columns
  - 9 for 3x3 blocks
- Prover shakes envelopes and gives them to the verifier
- If solution is valid, every envelope contains exactly the numbers 1-9

				7			8	
		1						
2					7			
		3						
							4	

Sudoku verifier

- Verifier checks every envelope contains exactly the numbers 1-9

Cryptographic tools

- Prover “commits” to the number in each cell
  - Face down is commitment
- Prover “shuffles” the commitments
  - Places them in an envelope

Cryptographic tools

- Prover “commits” to the number in each cell
  - Face down is commitment
- Prover “shuffles” the commitments
  - Places them in an envelope
- Many “proofs of shuffle” exist