Crypto: More Crypto Tools

Slides credit: Dan Boneh, Doug Tygar, David Wagner

Overview

- This lecture
  - Secret sharing
  - Secure multi-party computation
  - Zero-knowledge proof

Secret Sharing

- Suppose we want to share a secret
  - Share among *n* users
  - Any *q* users can recover the secret
  - Any less than *q* users cannot
- Example
  - Corporate bank account
    - Require three out of six corporate officers to access

Shamir Secret Sharing

- Key idea
  - Make a random polynomial curve $f(x)$ of degree $q-1$:
  - Secret is $f(0)$
  - Distribute n points
  - q points determine the curve
  - $q-1$ or less points do not determine the curve
  - All calculations are mod p, where p is a prime

Shamir Secret Sharing

$f(x)=a_{q-1}x^{q-1}+\ldots+a_1x+a_0$ (mod p), where $a_{q-1},\ldots, a_1, a_0$ are picked uniformly at random from Z_p^*

$Z_p^* = \{1,2,\ldots,p-1\}$, where p is a prime.

Share $S_i=(r_i, f(r_i))$, where r_i is sampled uniformly at random from Z_p^*, $i=1,2,\ldots,n$,

Given q points, we can solve for $a_{q-1},\ldots, a_1, a_0$

Secret is $f(0) = a_0$

Finding the Secret

This reduces to solving linear equations

Example with q=3 and n=5 :

$f(1) = a_2+a_1+a_0 \pmod{p}$
$f(2) = 4a_2+2a_1+a_0 \pmod{p}$
$f(3) = 9a_2+3a_1+a_0 \pmod{p}$
$f(4) = 16a_2+4a_1+a_0 \pmod{p}$
$f(5) = 25a_2+5a_1+a_0 \pmod{p}$

Lagrange Interpolation

Given (x_i, y_i), *where* $y_i=f(x_i)$ and $i=1,2,..,q$

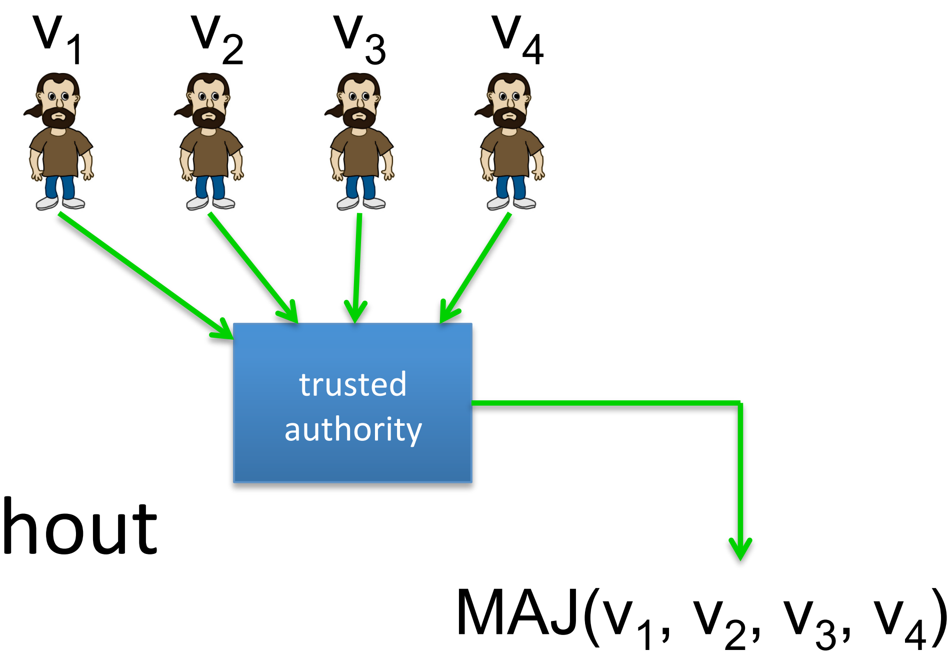
$$L_i(x) = \frac{\prod_{j\neq i}(x - x_j)}{\prod_{j\neq i}(x_i - x_j)}$$

$$a_0=f(0)=\sum_{i=1}^{q} y_i L_i(0)$$

Secure Multi-Party Computation

Protocols

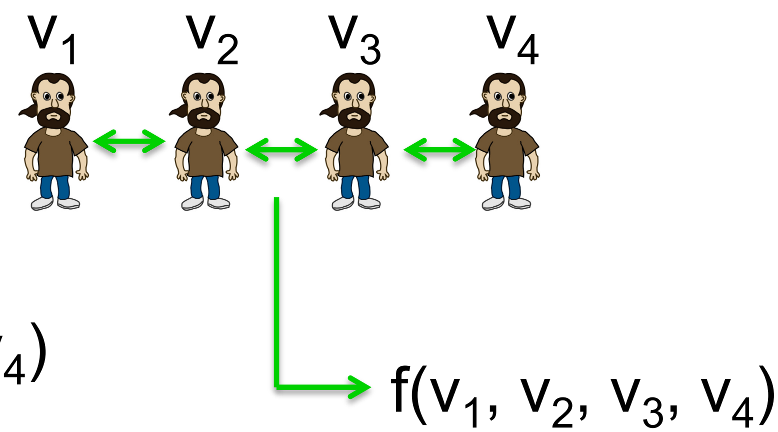
Elections



Can we do the same without a trusted party?

Protocols

Elections



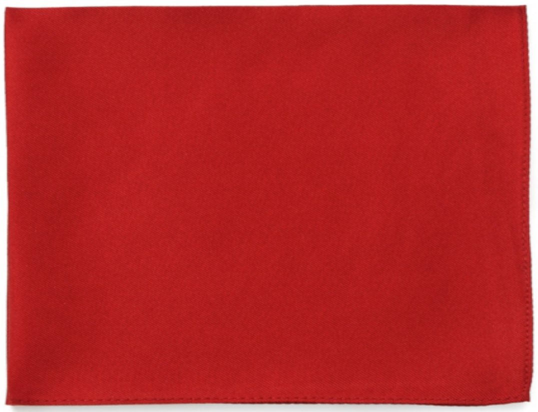
Goal: compute $f(v_1, v_2, v_3, v_4)$

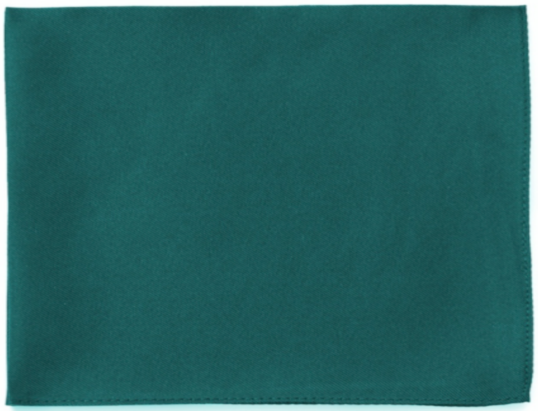
“Thm:” anything that can be done with a trusted authority
can also be done without

Secure multi-party computation

Zero-knowledge Proof

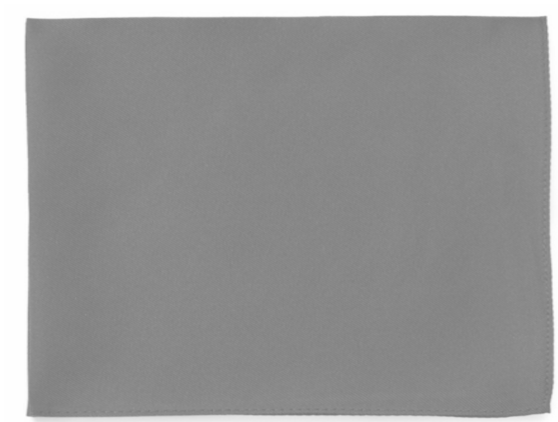
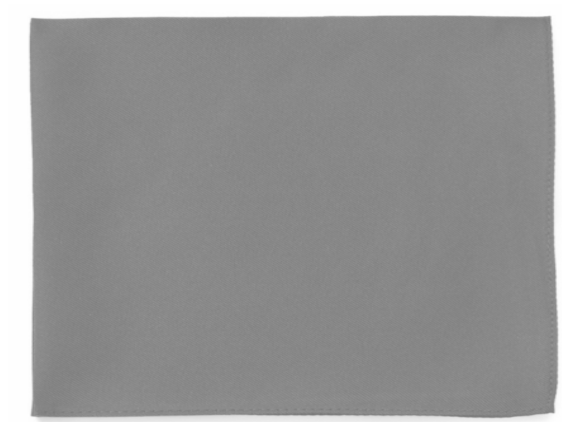
Interactive proofs





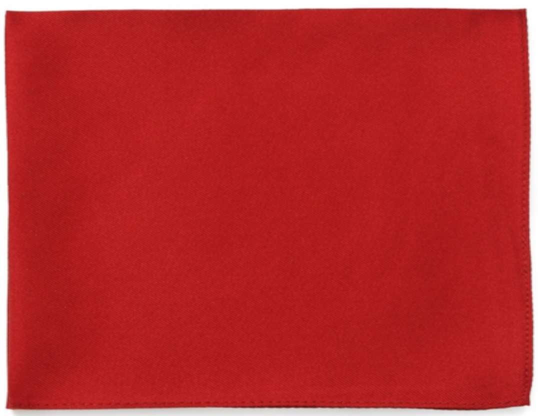
Here are two cloths.

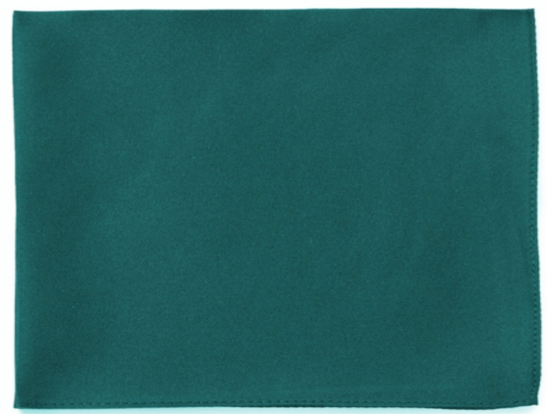
Interactive proofs

Imagine that I am red-green color-blind…

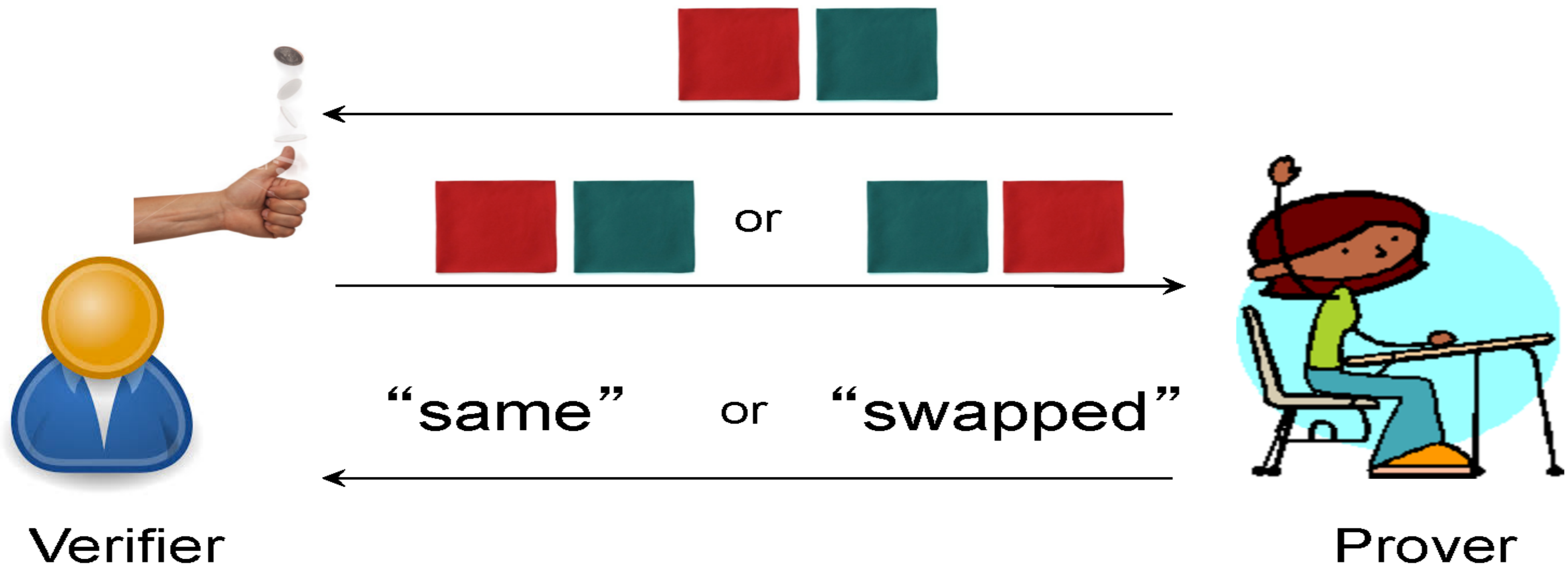
Interactive proofs





How could you prove to me that you can distinguish the red cloth from the green cloth, if I am red-green color-blind?

An interactive proof



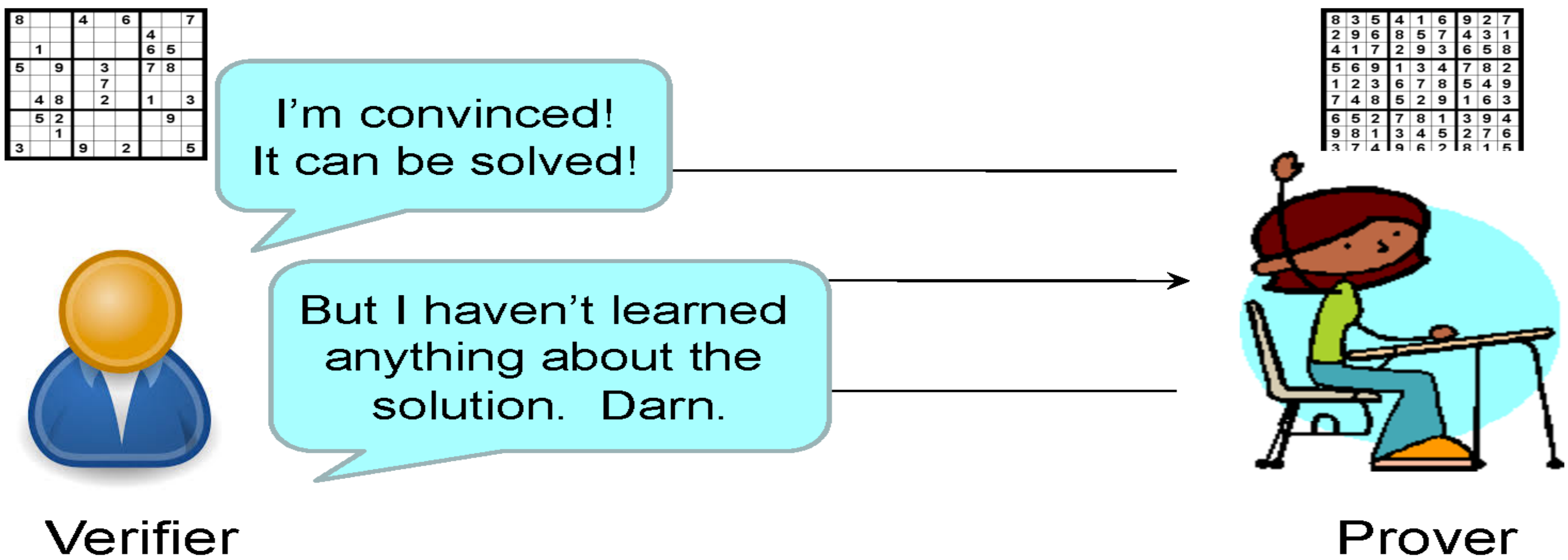
Sudoku

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

Sudoku

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

Goal: Prove the puzzle is solvable



You prepare your proof

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

1 → e
2 → h
3 → c
4 → f
5 → i
6 → d
7 → b
8 → a
9 → g

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

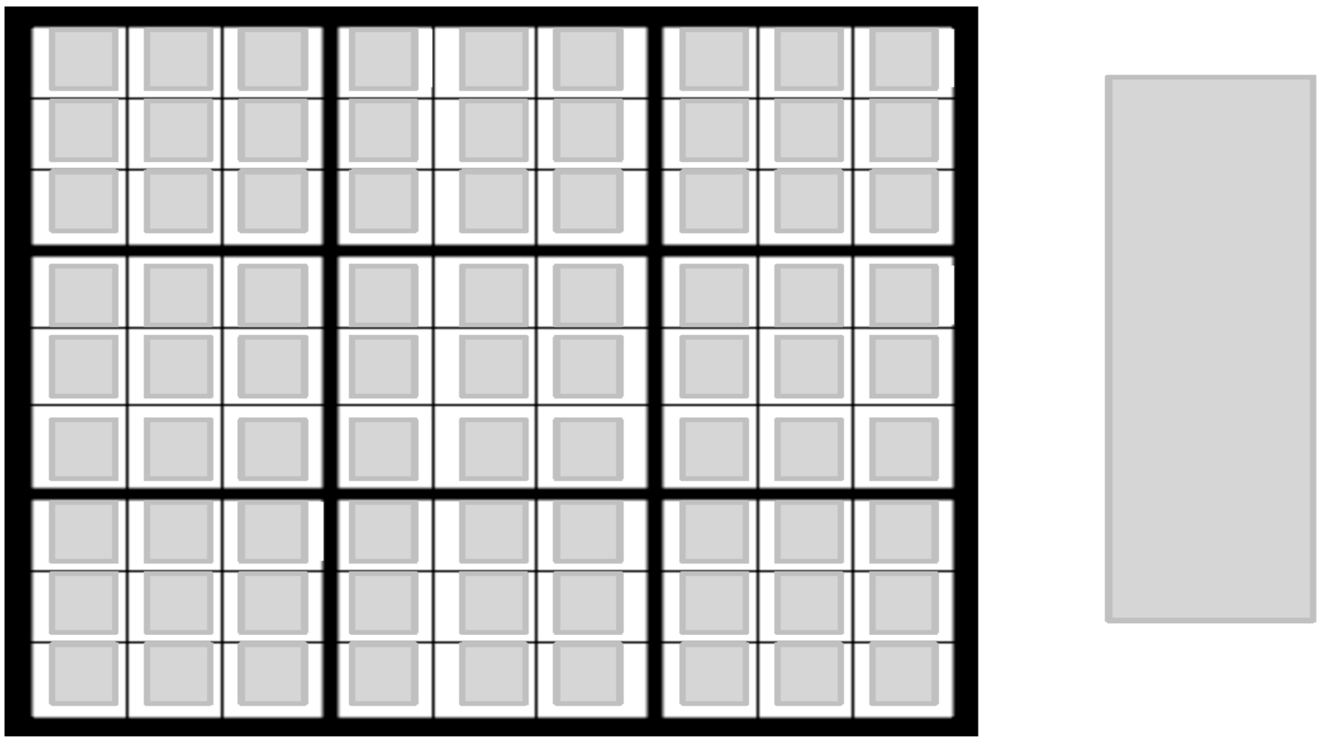
You prepare your proof

a	c	i	f	e	d	g	h	b
h	g	d	a	i	b	f	c	e
f	e	b	h	g	c	d	i	a
i	d	g	e	c	f	b	a	h
e	h	c	d	b	a	i	f	g
b	f	a	i	h	g	e	d	c
d	i	h	b	a	e	c	g	f
g	a	e	c	f	i	h	b	d
c	b	f	g	d	h	a	e	i

1 → e
2 → h
3 → c
4 → f
5 → i
6 → d
7 → b
8 → a
9 → g

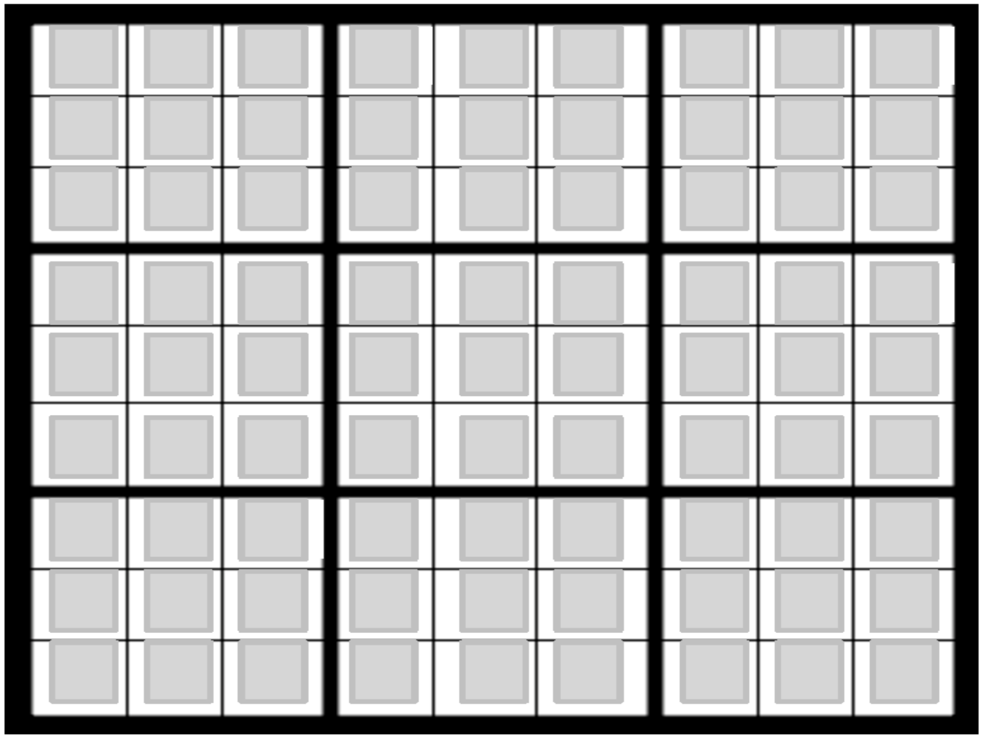
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

You prepare your proof



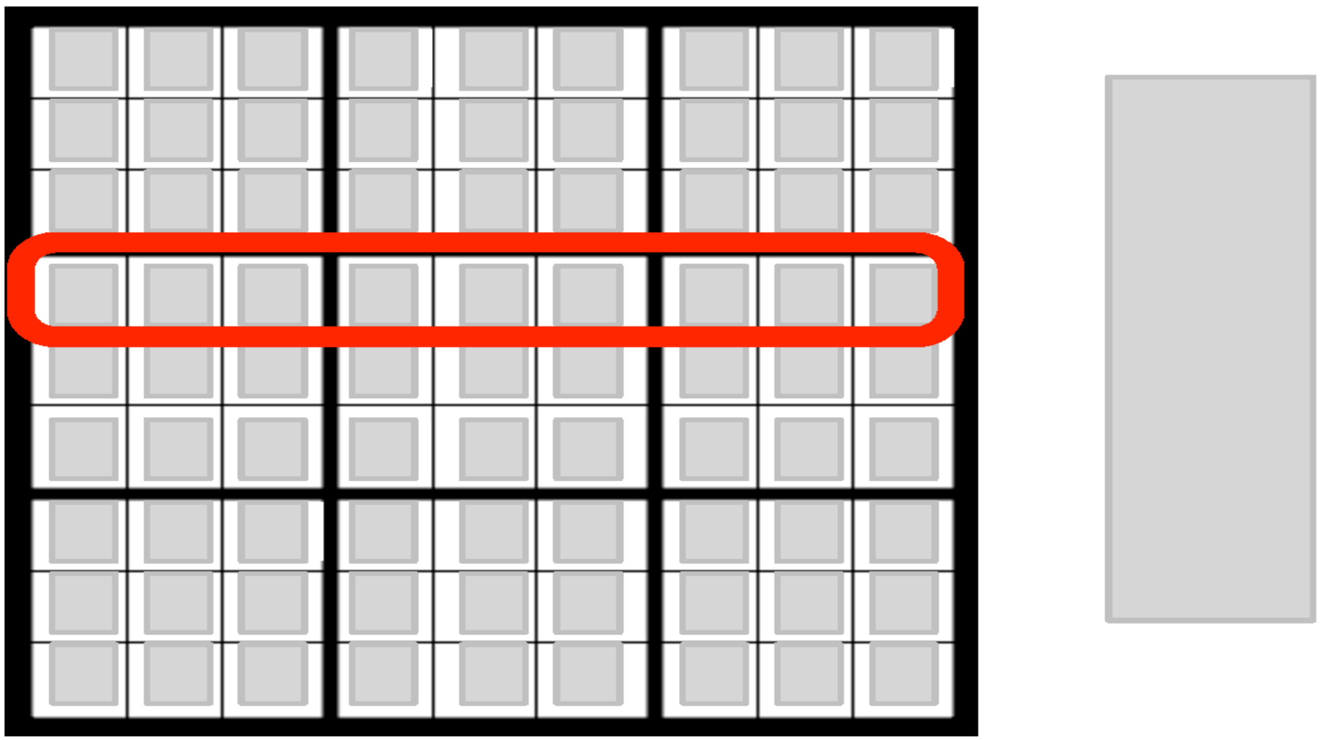
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest



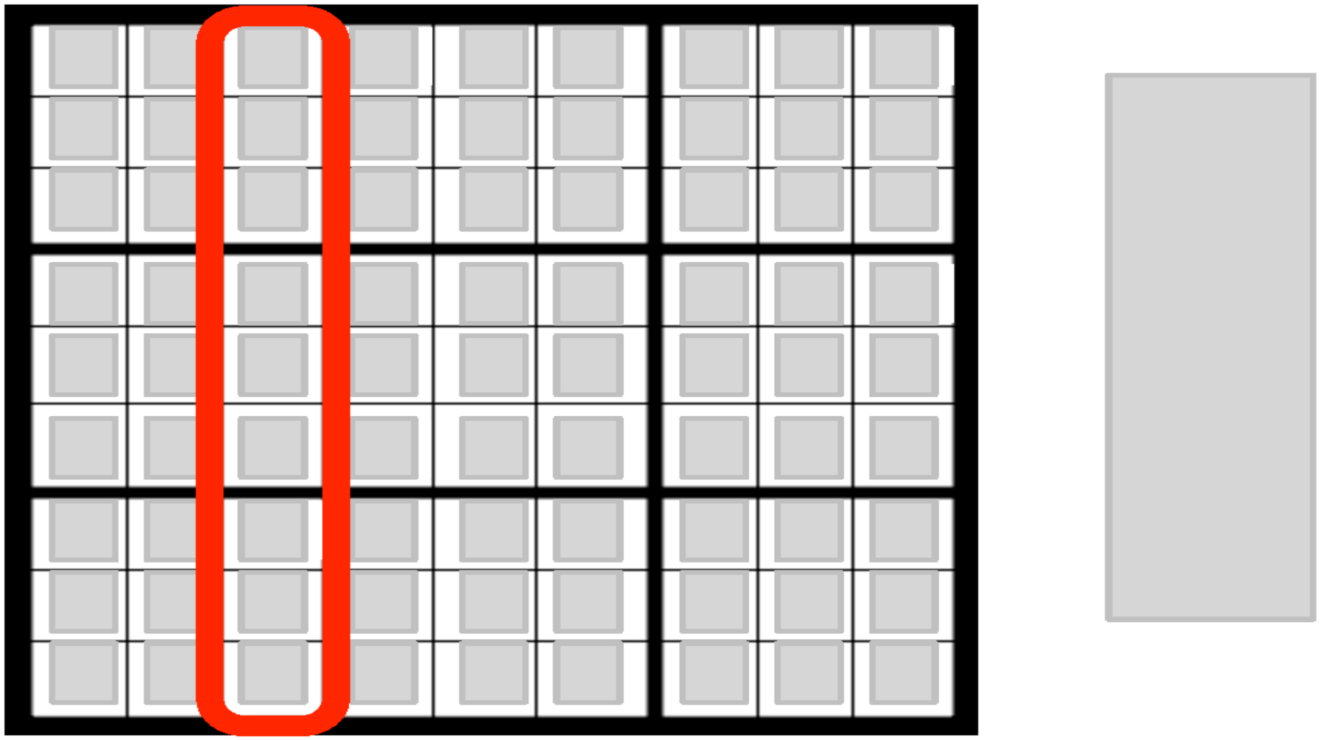
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest (option 1)



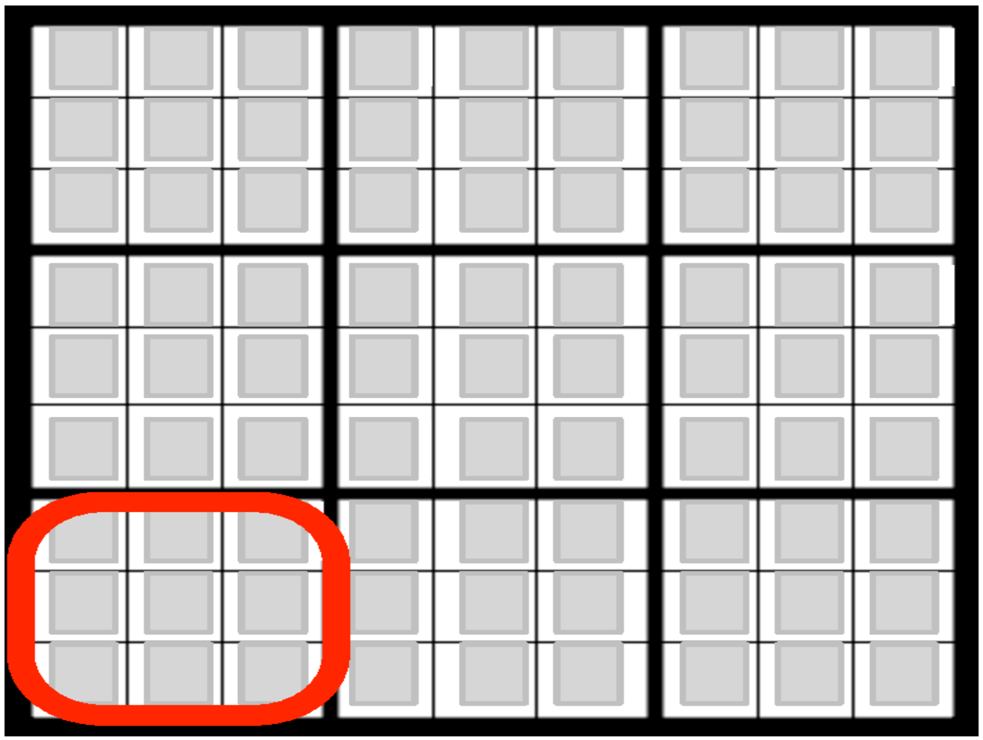
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

My turn: I keep you honest (option 2)



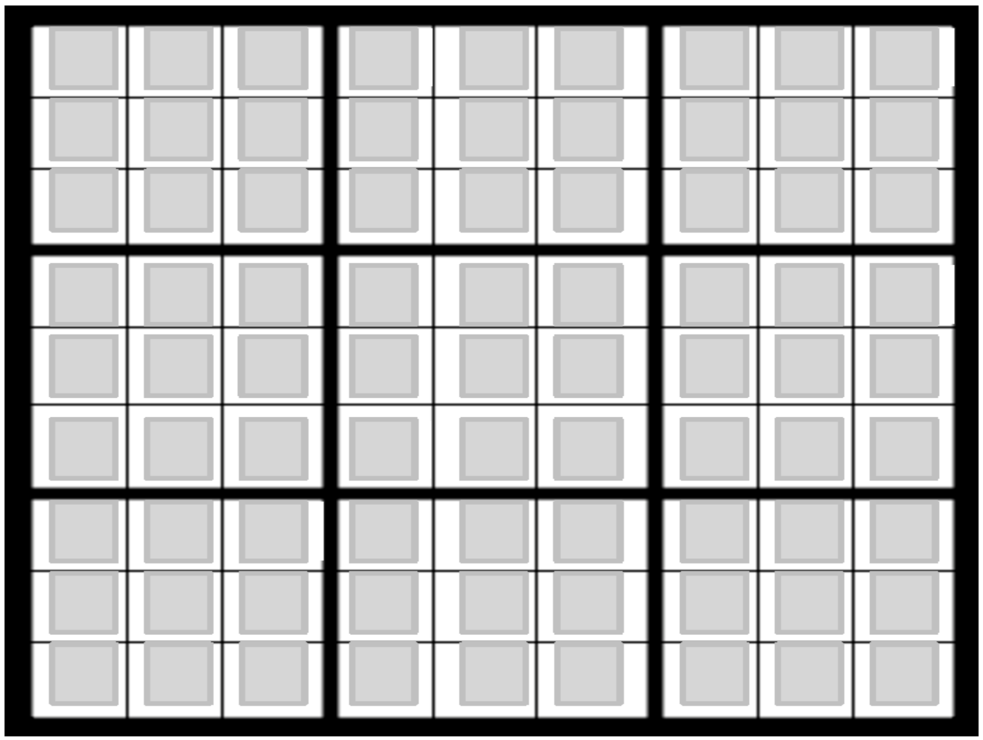
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

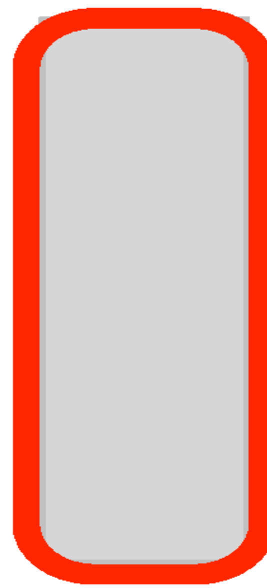
My turn: I keep you honest (option 3)



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

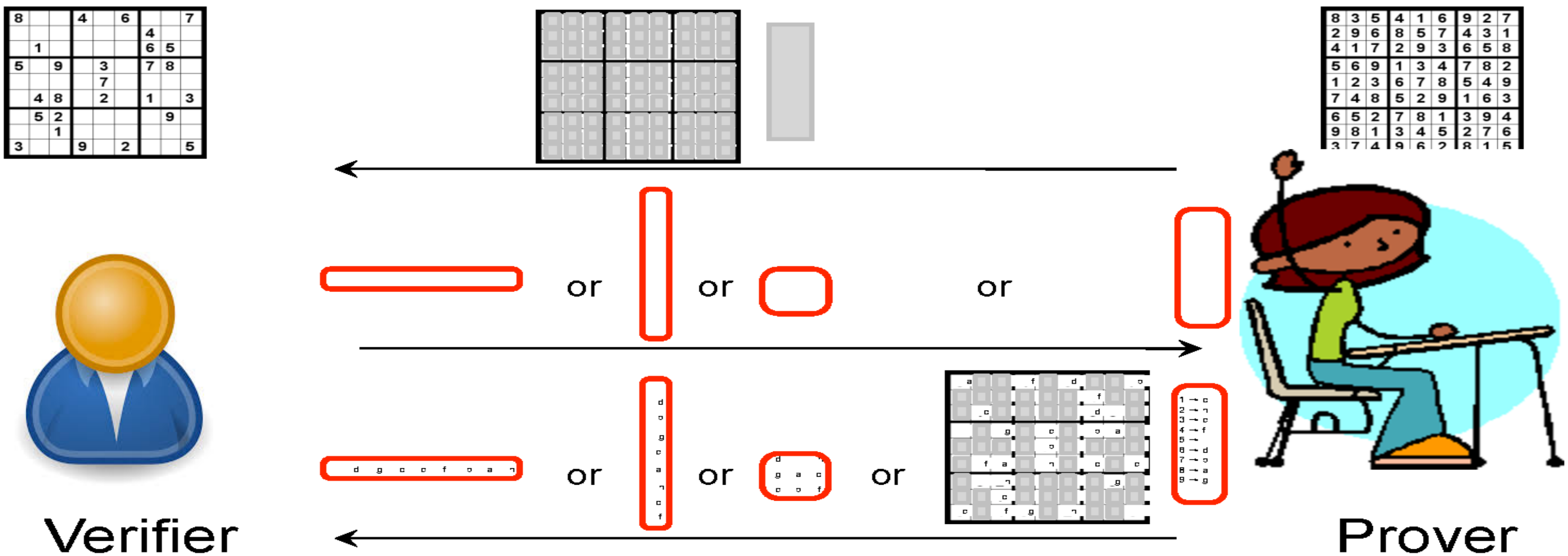
My turn: I keep you honest (option 4)





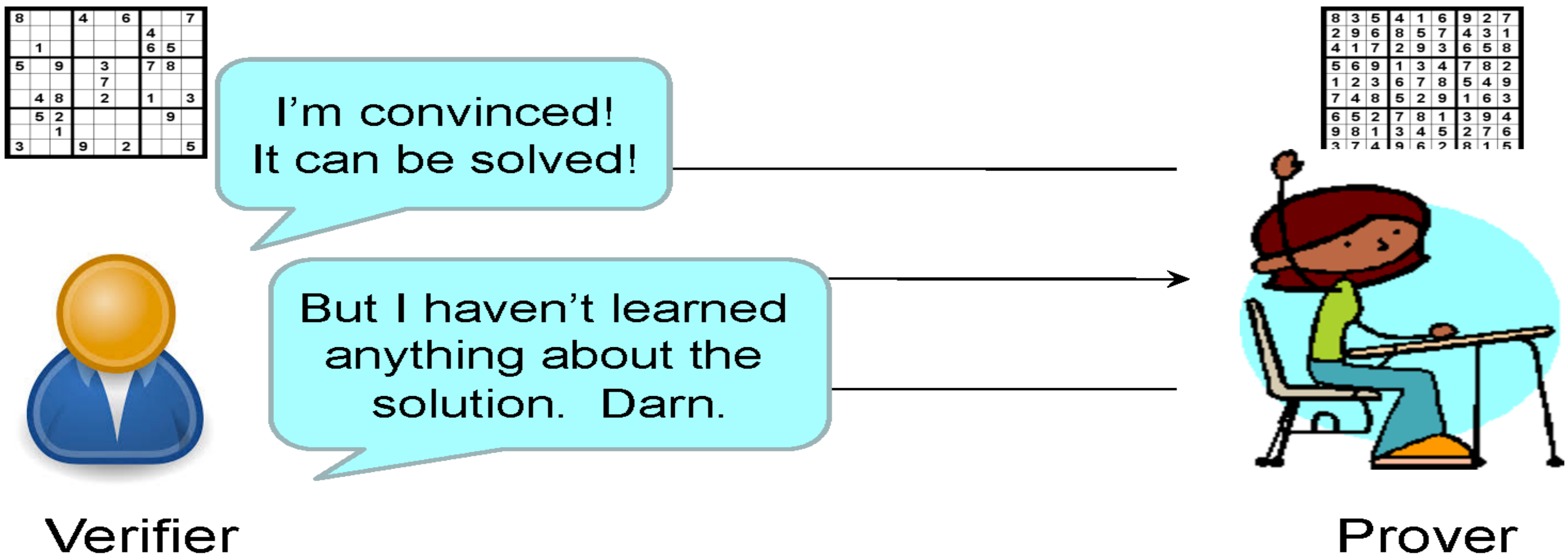
8			4		6			7
						4		
	1					6	5	
5		9		3		7	8	
				7				
	4	8		2		1		3
	5	2					9	
		1						
3			9		2			5

Zero-knowledge proof: puzzle is solvable



Repeat 1000 times

Goal: Prove the puzzle is solvable



Summary

Alice can prove to Dave that the Sudoku puzzle has a solution.
Dave gains zero knowledge about the solution.

Sudoku isn't special:

Theorem. If I can prove it, I can prove it to you without revealing the proof.

Summary

Theorem. If I can prove it, I can prove it to you without revealing the proof.

Zero-Knowledge Proof for Discrete Logs

- Suppose a prover has an identity *x*, which is a number satisfying $B=A^x$ (mod *p*). (*A,B,p*) is publicly available. The prover wants to prove he/she has *x* but does not want to reveal *x* to the verifier.
  – Prover chooses a random number $0\leq r < p-1$ and sends the verifier $h=A^r$ (mod *p*)
  – Verifier sends back a random bit *b*
  – Prover sends $s=(r+bx)$ (mod (*p*-1)) to verifier
  – Verifier computes A^s (mod *p*) which should equal hB^b (mod *p*)