Zero knowledge proofs

Showing off your knowledge without giving it away

Julián Mestre

School of Information Technologies
The University of Sydney

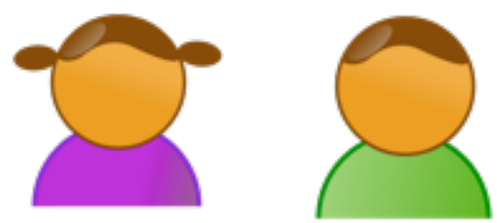
Zero knowledge proofs

The setup

- Two parties: Peggy and Victor
- Peggy claims to know something that Victor doesn't
- Peggy would like to convince Victor that she knows without giving it away

We would like to design a protocol where

- If Peggy is telling the true then she can convince Victor
- If Peggy is lying then there is a good chance that Victor will catch her
- Victor doesn't learn anything about Peggy's secret



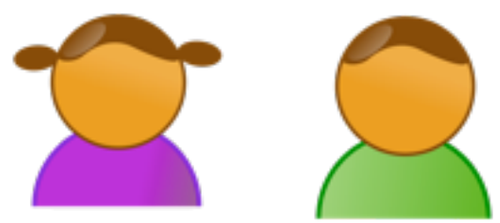
Making things concrete

Suppose Victor and Peggy have been working, separately, on a difficult Sudoku puzzle

After much hard work, Peggy manages to finish the puzzle but Victor is still working on it

Is it possible for Peggy to convince Victor that she knows the solution without giving it away?

Surprisingly, the answer is YES!



Sudoku

A Sudoku puzzle is a 9x9 grid subdivided into nine 3x3 squares. Some cells are empty and some are already filled.

Our job is to fill empty cells so that

- Every column contains the numbers 1, 2, ... , 9
- Every row contains the numbers 1, 2, ... , 9
- Every square contains the numbers 1, 2, ... , 9

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

Interactive protocol

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

Peggy the prover

Victor the verifier

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

question

answer

question

answer

OK, I'm convinced*

* there is a good chance that Peggy actually knows the answer

Interactive protocol

1. Peggy picks a random permutation, and re-writes her solution using this random mapping

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

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

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

Interactive protocol

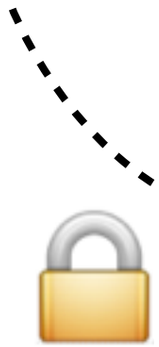
2. Peggy encrypts her permuted solution and sends it to Victor

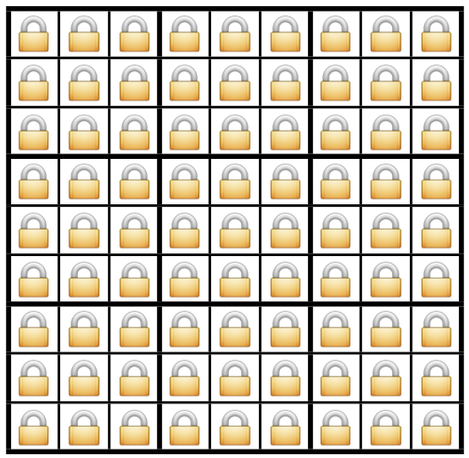
	4	3	5	2	6	9	7	8	1
	6	8	2	5	7	1	4	9	3
7	6	1	3	9	2	4	5	8	6	2
9	5	3	1	4	8	7	2	6	4	7
8	2	4	5	6	7	1	9	3	1	5
5	3	9	8	2	1	6	7	4	2	8
6	4	7	9	5	3	2	8	1	7	4
2	1	8	4	7	6	9	3	5	3	6
1	8	2	6	3	9	5	4	7	5	9
3	7	5	2	1	4	8	6	9		
4	9	6	7	8	5	3	1	2		

Peggy the prover

Victor the verifier

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





Each lock has its own individual key, which Peggy keeps.

Interactive protocol

3. Victor challenges Peggy with a question that she must answer

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

Peggy the prover

Victor the verifier

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

question

answer

What should Victor ask?

Victor's question must have these properties

- *[Completeness]* If Peggy knows the answer, she should be able to answer
- *[Soundness]* If Peggy doesn't know the answer, Victor should be able to catch her with some fixed probability
- *[Zero-knowledge]* Victor should not learn anything from Peggy's answer

These three properties handle the following scenarios:

- Both Peggy and Victor follow the protocol
- Peggy tries to cheat but Victor follows the protocol
- Peggy follows the protocol but Victor tries to cheat

Victor's questions

Victor could challenge Peggy to reveal one subsquare

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

Peggy the prover

Victor the verifier

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

Reveal middle square

Here are the keys

OK, I'm convinced*

Victor's questions

Victor could challenge Peggy to reveal a column

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

Peggy the prover

Victor the verifier

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

Reveal second column

Here are the keys

OK, I'm convinced*

Victor's questions

Victor could challenge Peggy to reveal a row

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

Peggy the prover

Victor the verifier

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

Reveal forth row

Here are the keys

OK, I'm convinced*

Victor's questions

Victor could challenge Peggy to reveal filled-in entries

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

Peggy the prover

Victor the verifier

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

Reveal filled-in entries

Here are the keys

OK, I'm convinced*

Victor's questions

All together Victor can ask one of 28 questions:

- [9 questions] reveal some square
- [9 questions] reveal some column
- [9 questions] reveal some row
- [1 question] reveal filled-in entries

Notice that the answer to a single question doesn't reveal any information, but the answer to two questions does. So which one should he pick?

Easy, pick one at random!

Interactive protocol for Sudoku

1. Peggy picks a random permutation, and re-writes her solution using this random mapping

2. Peggy encrypts her permuted solution and sends it to Victor

3. Victor chooses one of his 29 questions uniformly at random. He challenges Peggy who must answer it

Outcome: Victor either accepts or rejects the proofs

Completeness

If Peggy knows the answer, then she should be able to answer Victor's questions

- [9 questions] reveal some square
- [9 questions] reveal some column
- [9 questions] reveal some row
- [1 question] reveal filled-in entries

Clearly Peggy can answer every single question

Obs. The protocol is complete

Soundness

If Peggy doesn't knows the answer, then Victor should be able to catch her with some fixed probability

- [9 questions] reveal some square
- [9 questions] reveal some column
- [9 questions] reveal some row
- [1 question] reveal filled-in entries

If Peggy doesn't know the solution to the Sudoku puzzle then there is at least one question that she won't be able to answer

Obs. The protocol is sound with error 27/28

Zero-knowledge

Victor should not learn anything from Peggy's answer

- [9 questions] reveal some square
- [9 questions] reveal some column
- [9 questions] reveal some row
- [1 question] reveal filled-in entries

All that Victor learns is information about the random permutation used by Peggy

Obs. The protocol is zero-knowledge

Interactive protocol for Sudoku

1. Peggy picks a random permutation, and re-writes her solution using this random mapping

2. Peggy encrypts her new solution and sends it to Victor

3. Victor chooses one of his 28 questions uniformly at random. He challenges Peggy who must answer it

Thm. The above interactive protocol is complete, sound with error 27/28, and zero-knowledge

Tying up the loose ends

How does Peggy "lock" those Sudoku entries?

Victor can be fooled 27 out of 28 times!

Is Sudoku the only problem with zero-knowledge proofs?

Are there any applications of this?

How about a demo?

Interactive protocol with cards

Filling the table:

- Peggy places 3 cards face up on each filled-in cell
- Peggy places 3 cards face down on each empty cell according to her solution
- Victor checks that all filled-in cell have the right number

Splitting the cards into 3x9=27 packets of 9 cards each:

- For each column, Victor randomly picks one card from each cell
- For each row, Victor randomly pick one card from each cell
- For each subsquare, Victor gathers remaining cards

For each packet, Peggy turns all cards facing up and shuffles

Victor verifies that each packet has the cards 1 through 9

Demo

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

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

Demo

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

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

Demo

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

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

Demo

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

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

Boosting the soundness

Suppose that we have a protocol that is complete, zero-knowledge, and has soundness error p

Repeat the protocol k times. Victor accepts only if Peggy can answer all k challenges successfully.

The new protocol is complete, zero-knowledge, and has soundness error p^k

Suppose we wanted soundness error of 0.01 then

$$k > \log 0.01 / \log p$$