sikoba RESEARCH

ZKLux#1

Luxembourg's First Zero Knowledge Days

Conference on Thursday 27th June 2019

ZKP (zero-knowledge proofs) is a method to prove the knowledge of some fact, without revealing that fact. It is already used in several blockchains and is expected to have a major impact on applications that involve transactions, identity systems, and proprietary information in general. ZKLux#1 is the perfect occasion to find out about this exciting and important new technology.

Venue: House of Startups / LHoFT, "Big Bang" space, 9 Rue du Laboratoire, 1911 Luxembourg

the LHoFT FANTOM Grant Thornton

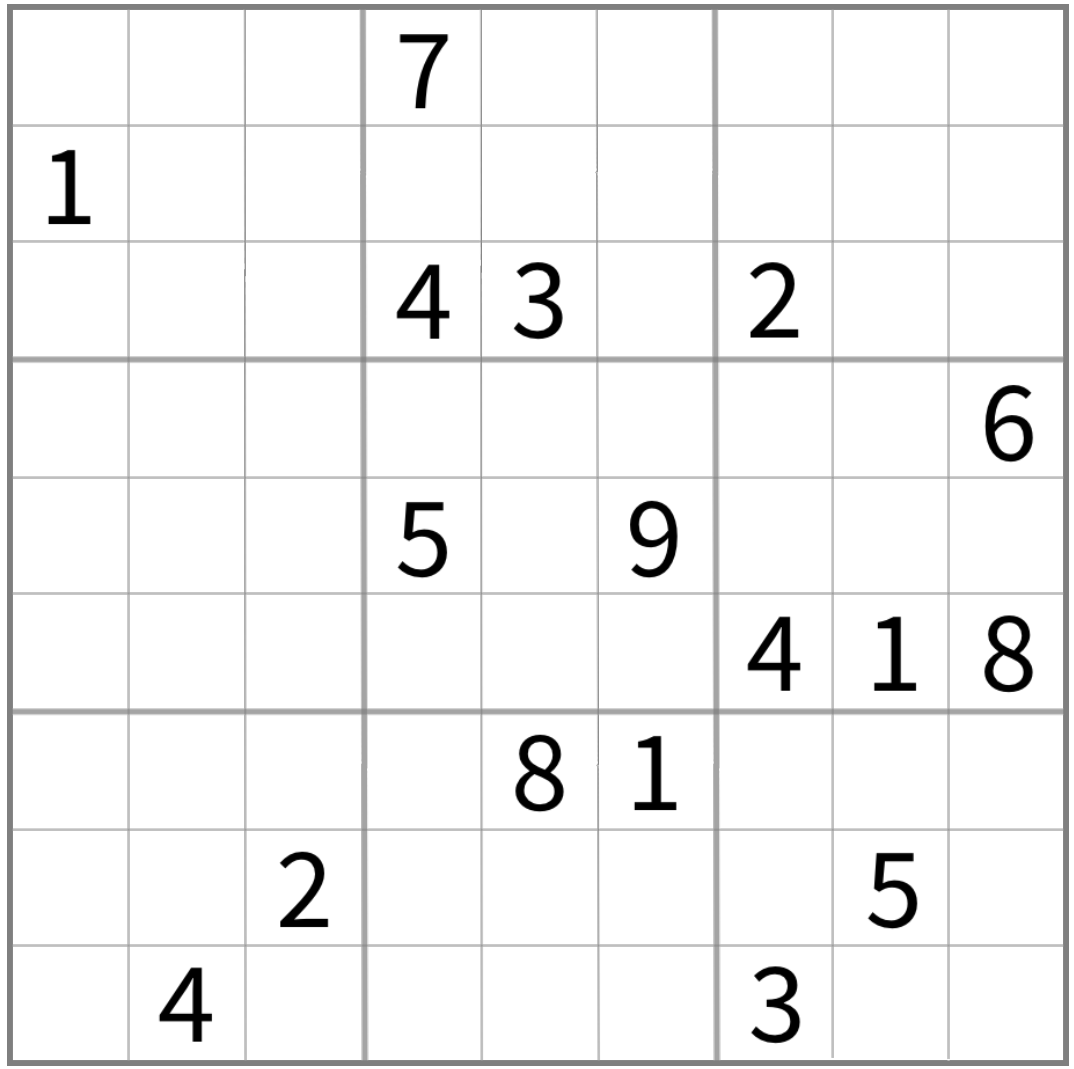
An Introduction to Zero-knowledge proofs

Alex Kampa, Sikoba Research

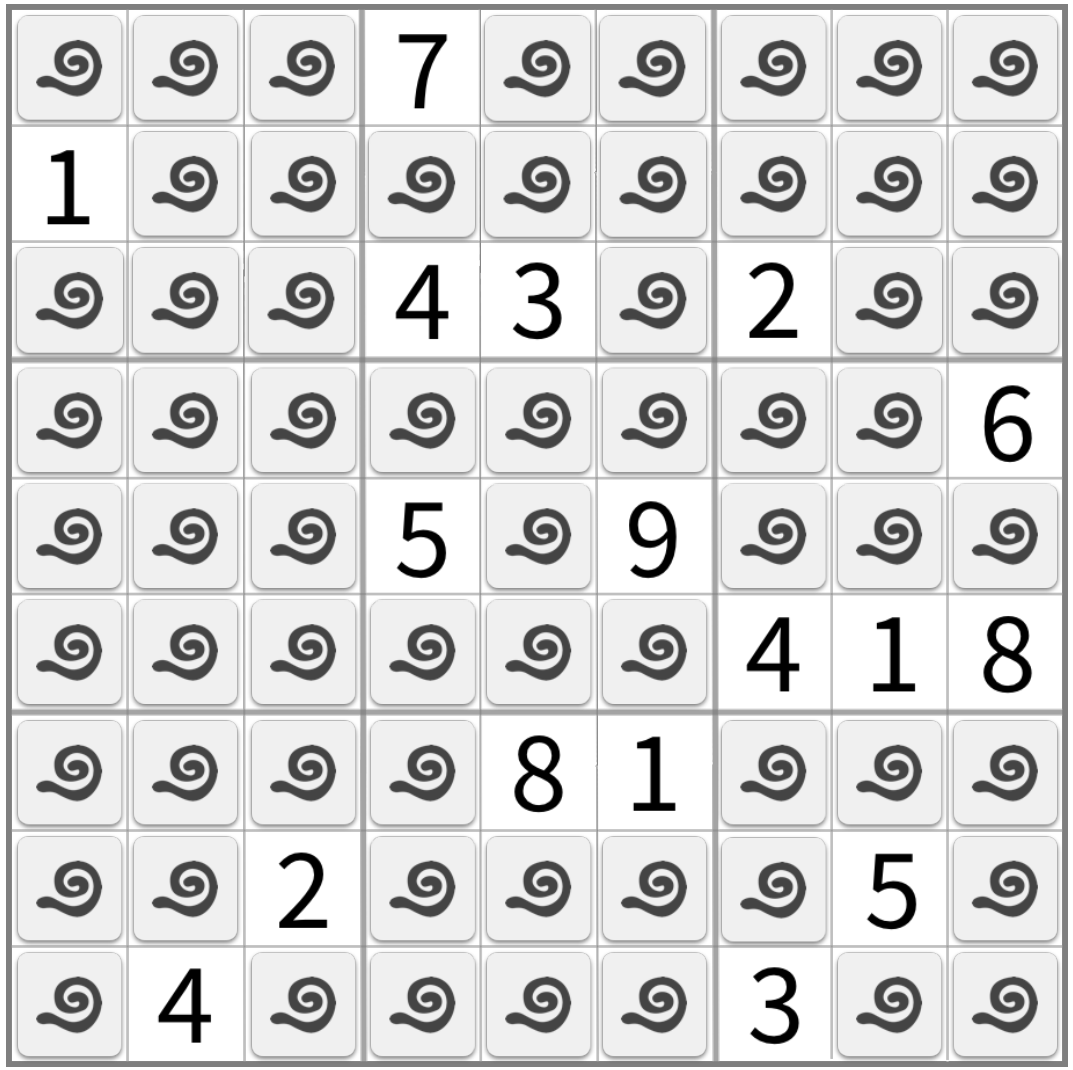
Example of zero-knowledge proof:

Sudoku

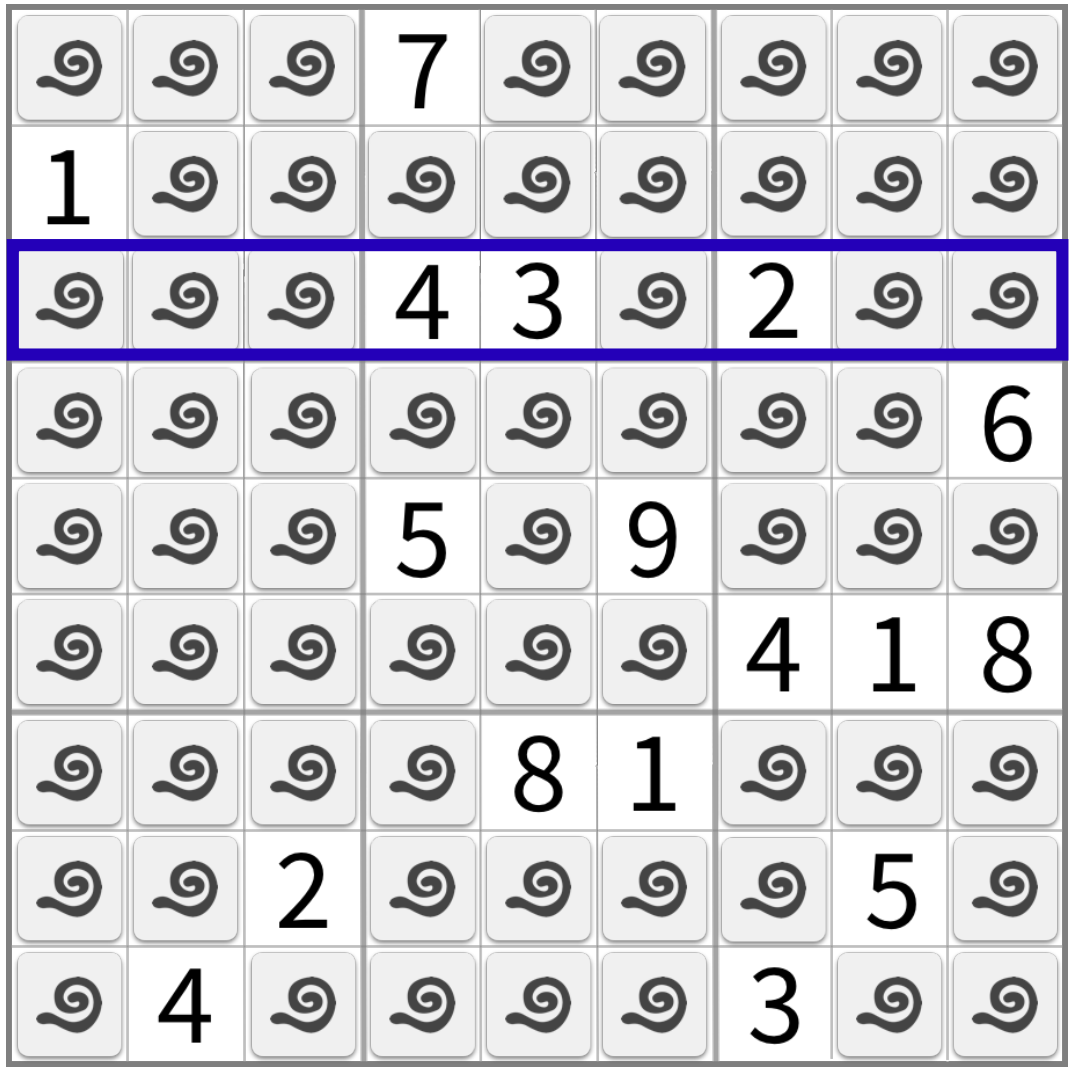
sikoba RESEARCH



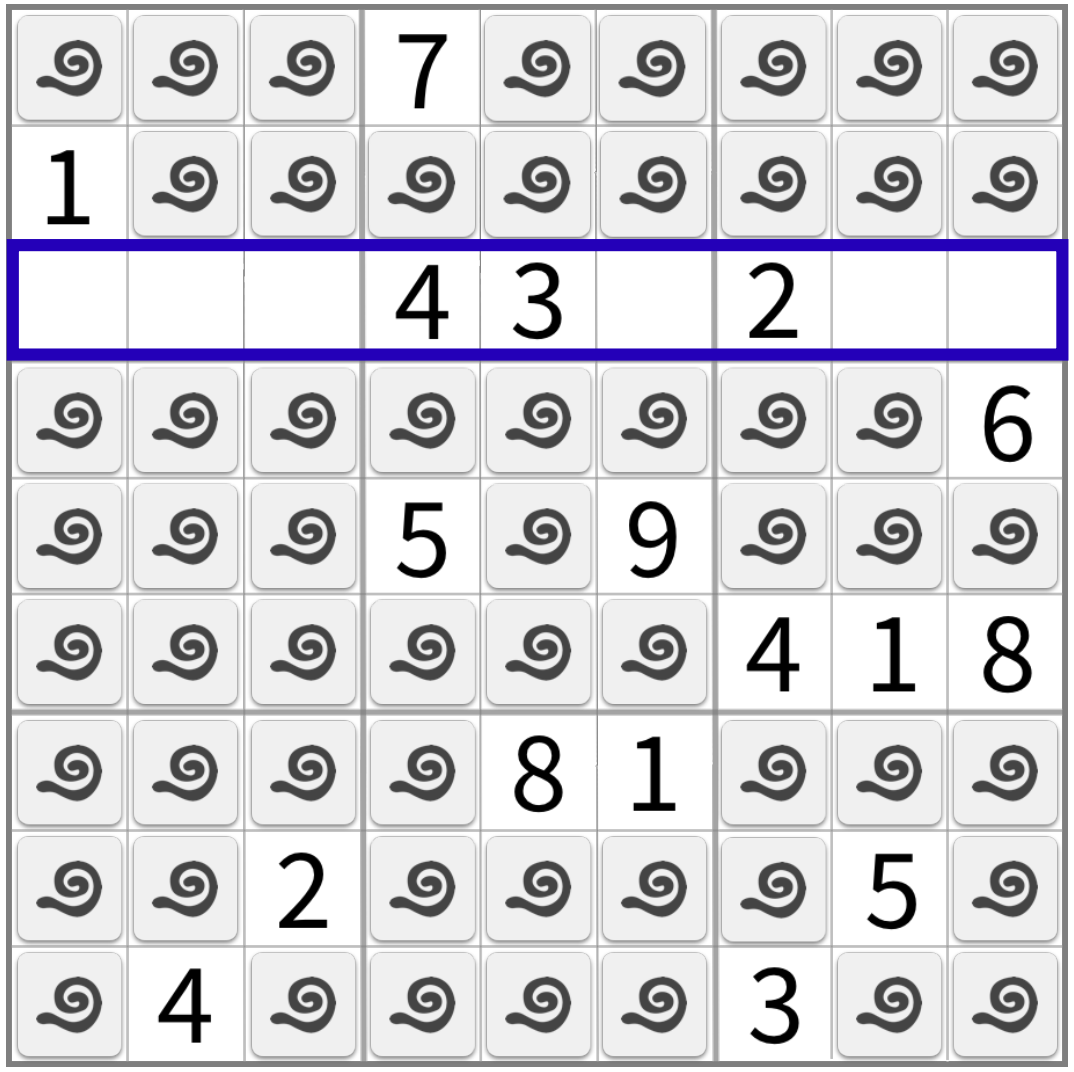
sikoba
RESEARCH



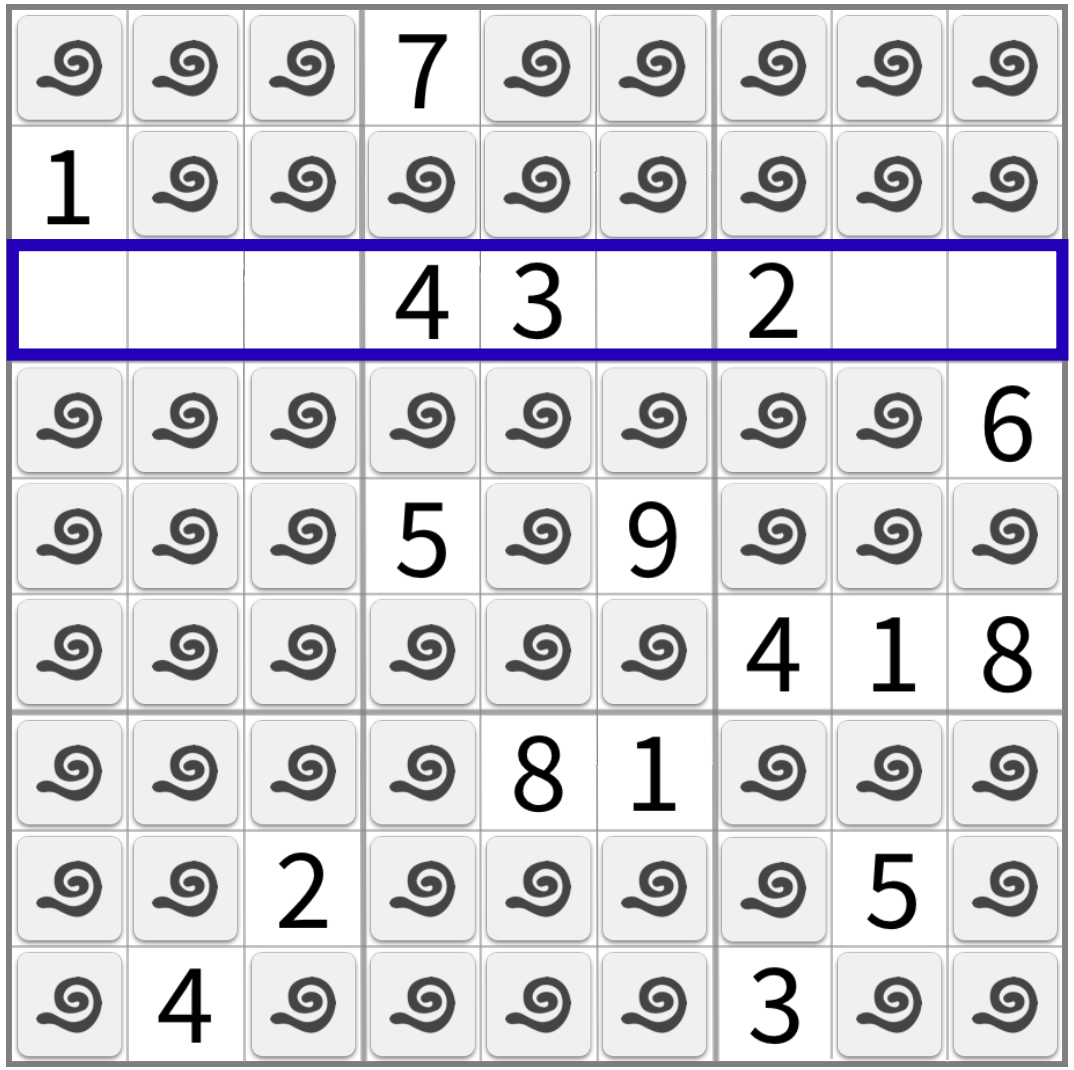
sikoba
RESEARCH



sikoba RESEARCH

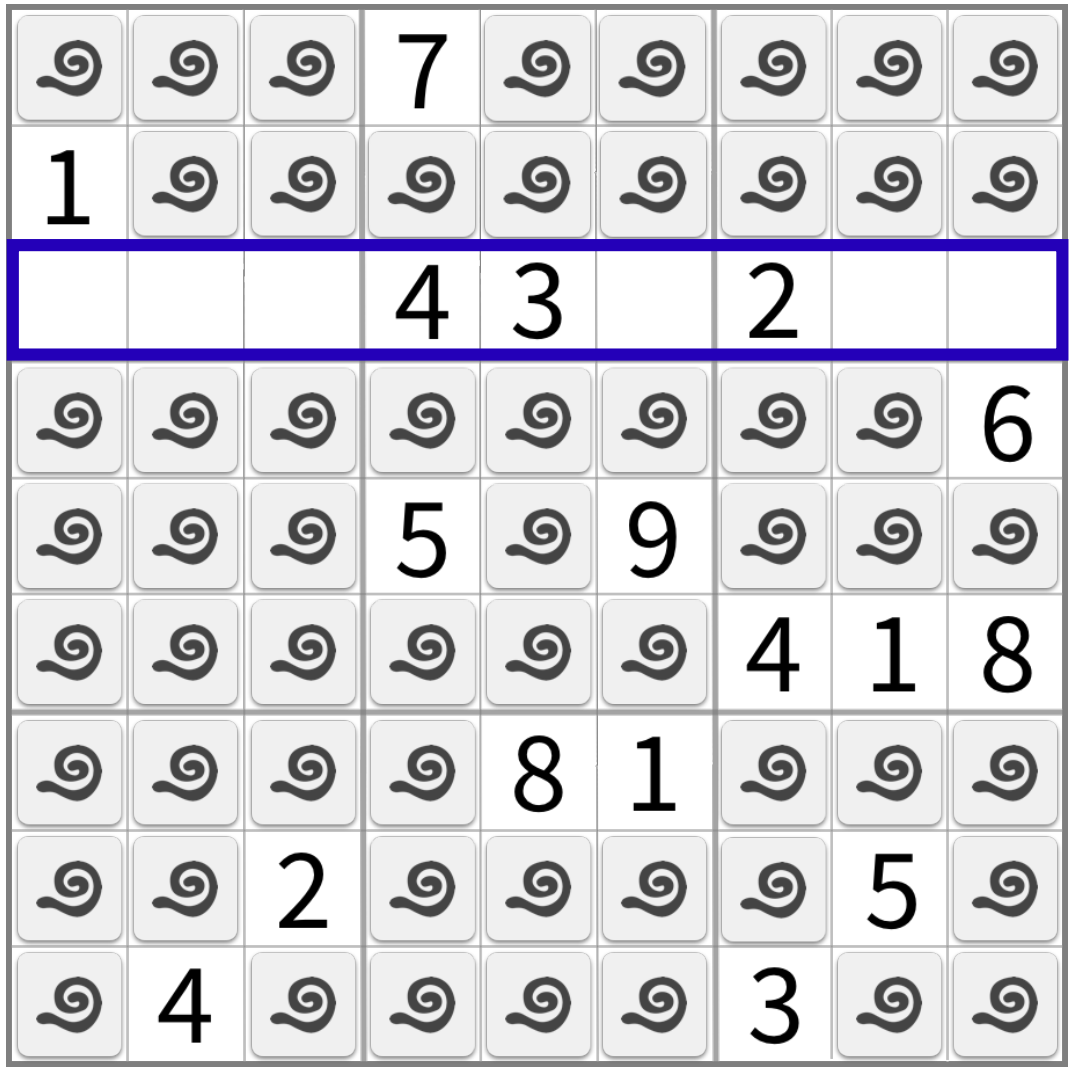


sikoba RESEARCH

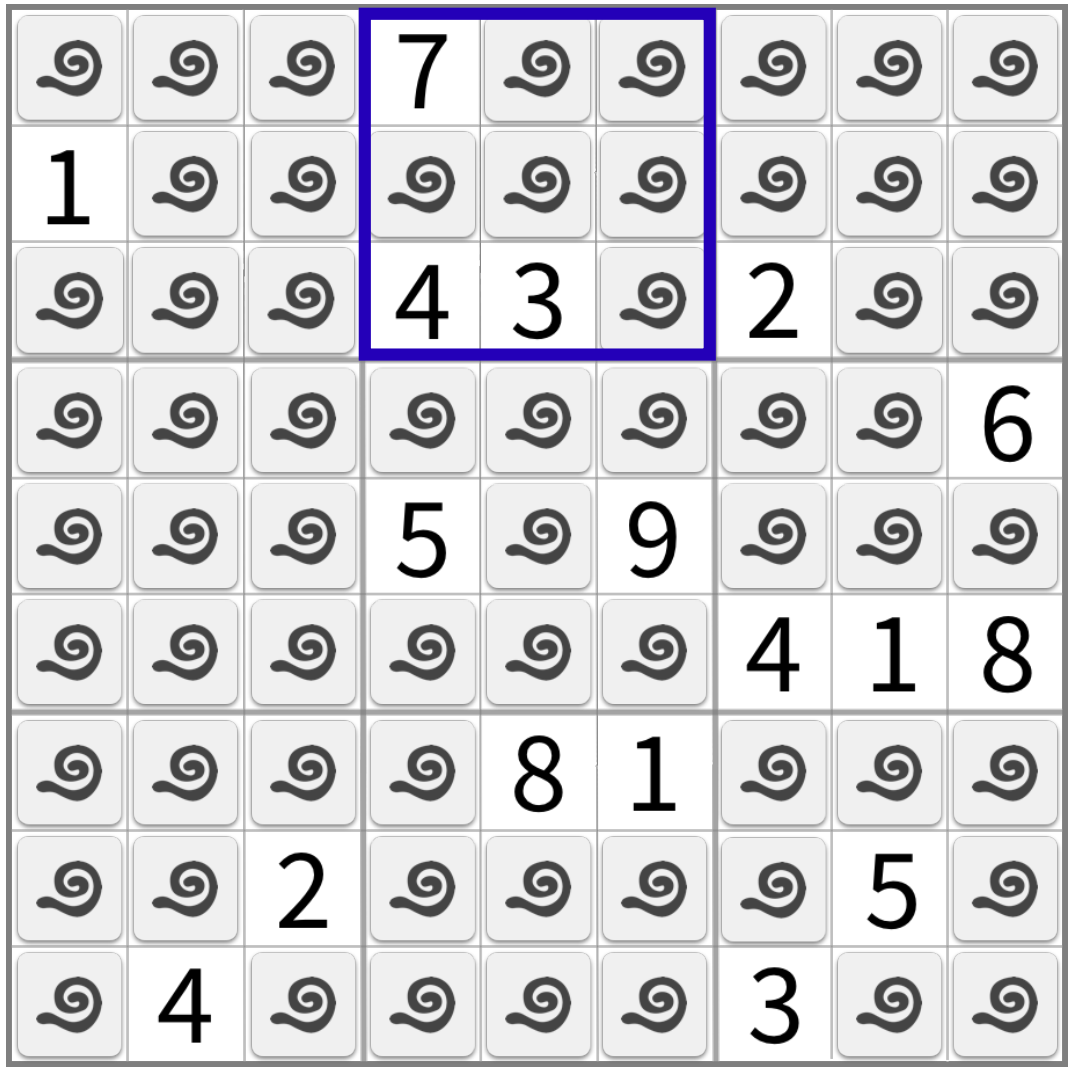


1 5 6 7 8 9

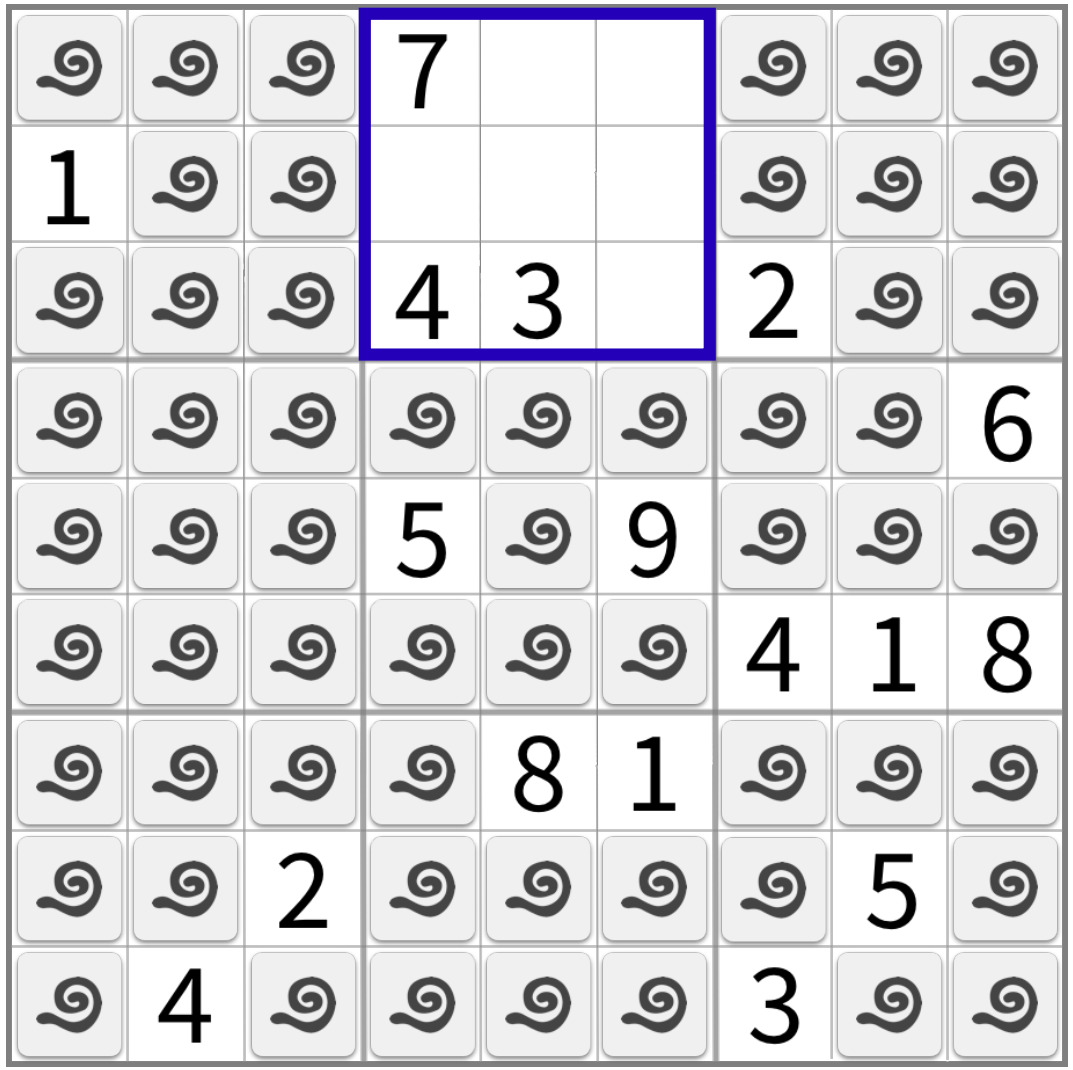
sikoba RESEARCH



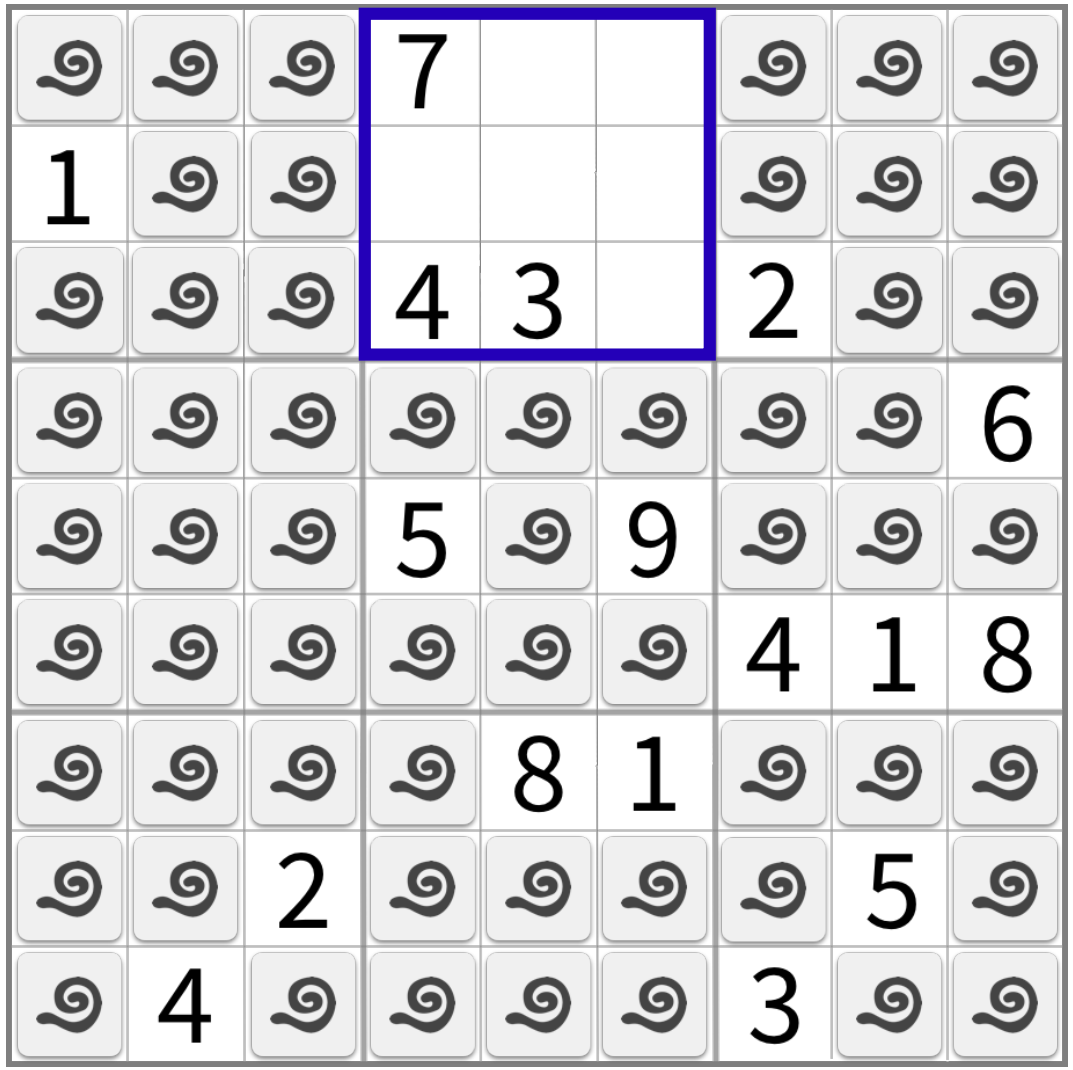
sikoba
RESEARCH



sikoba
RESEARCH



sikoba RESEARCH

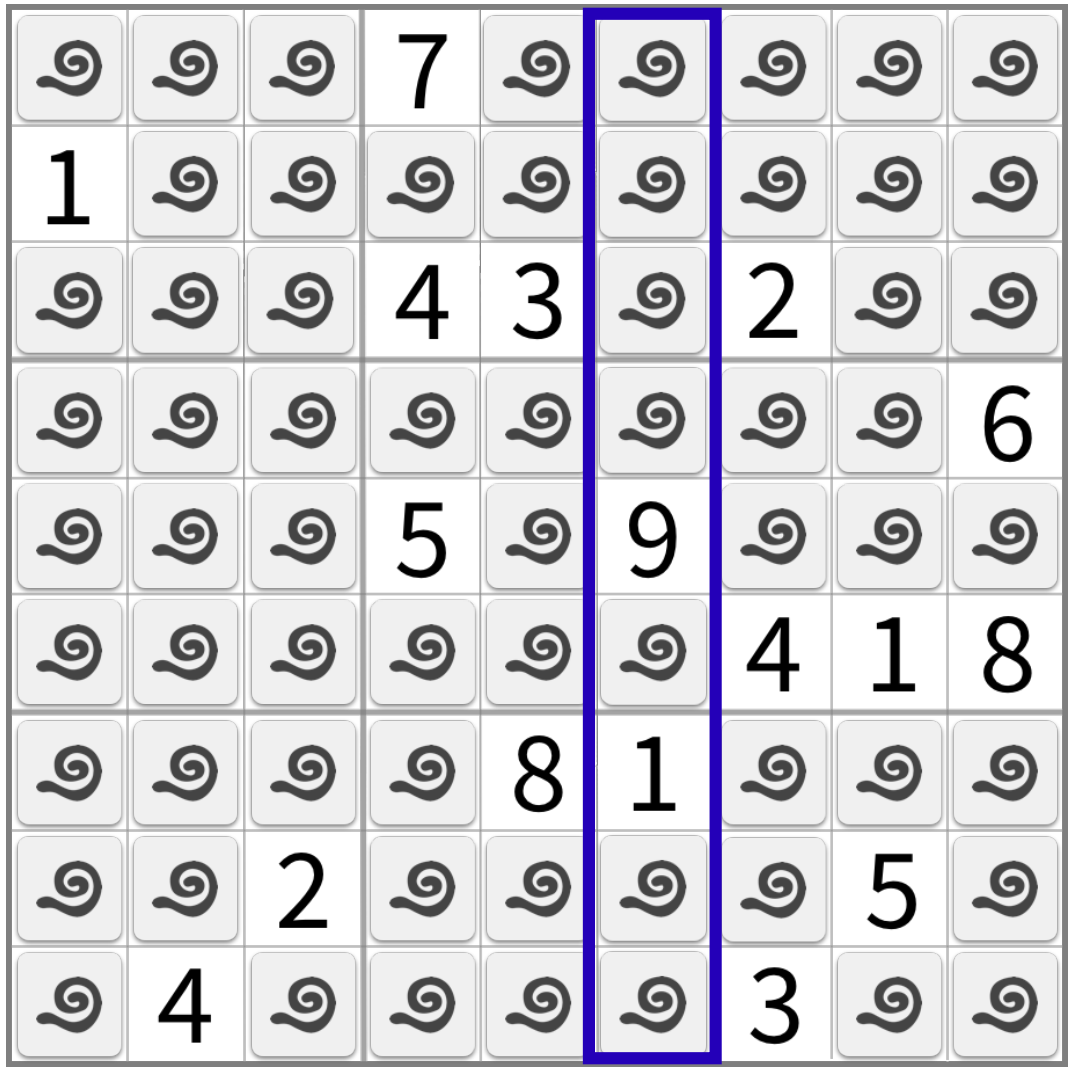


1 2 5 6 8 9

sikoba
RESEARCH

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

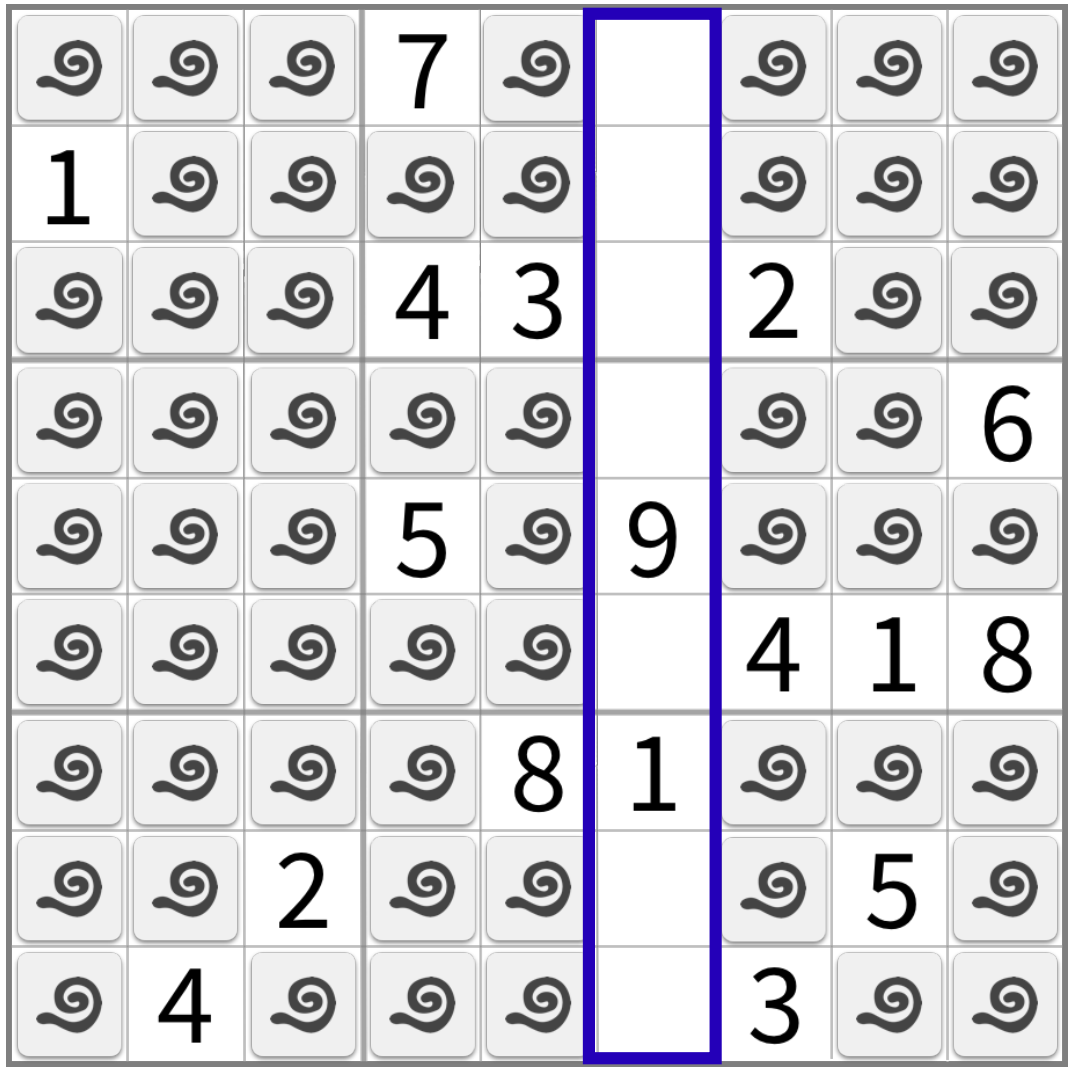
sikoba
RESEARCH



sikoba RESEARCH

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

sikoba RESEARCH



2 3 4 5 6 7 8

sikoba RESEARCH

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

Example of zero-knowledge proof:

The psychic

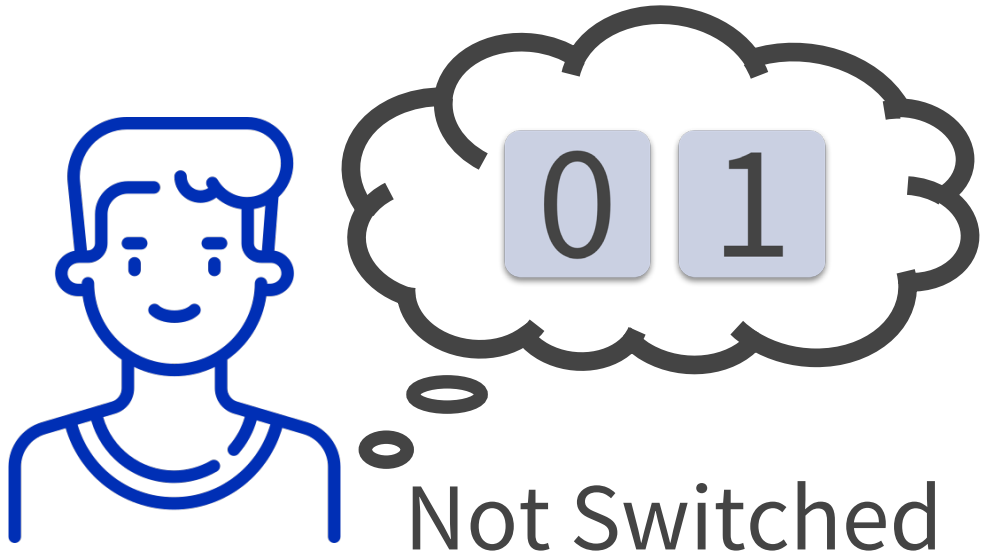
sikoba RESEARCH

0

1

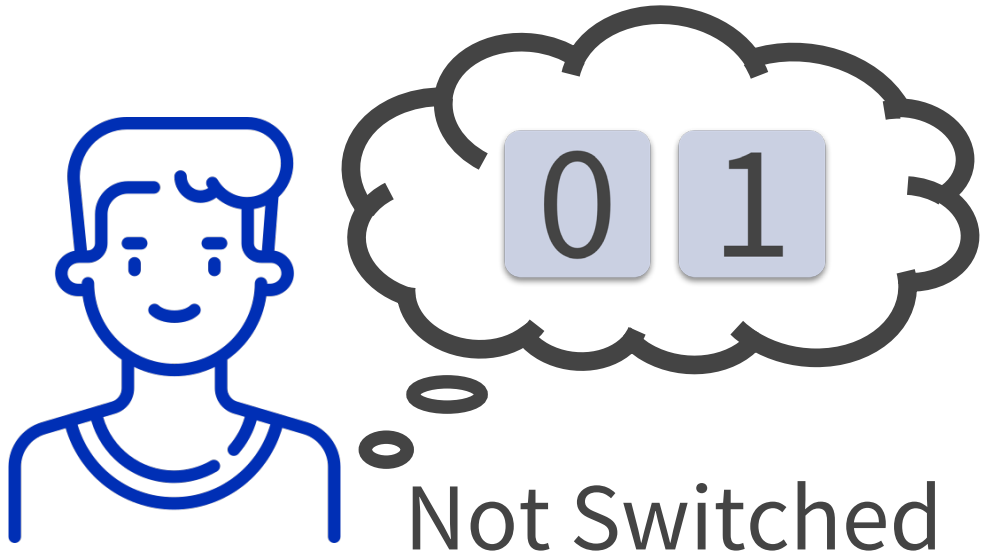
sikoba
RESEARCH

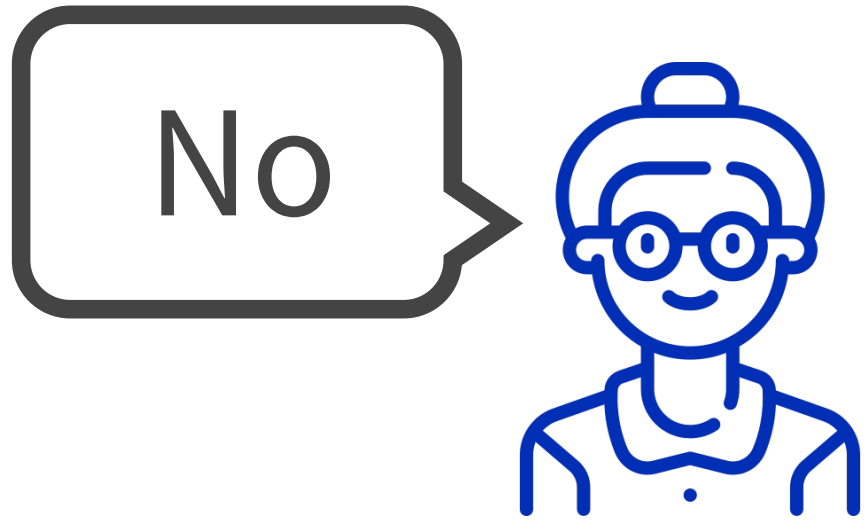
sikoba RESEARCH



Not Switched

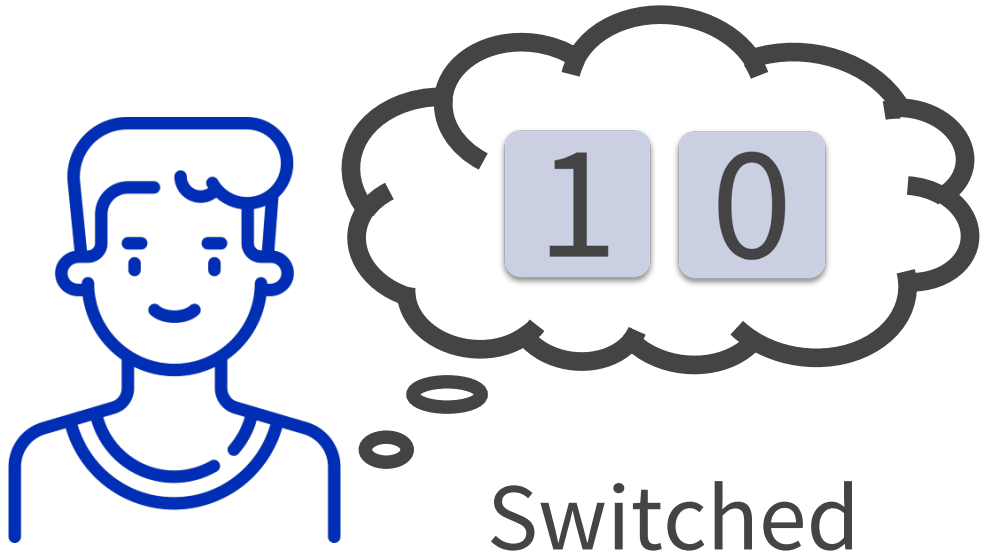
sikoba RESEARCH





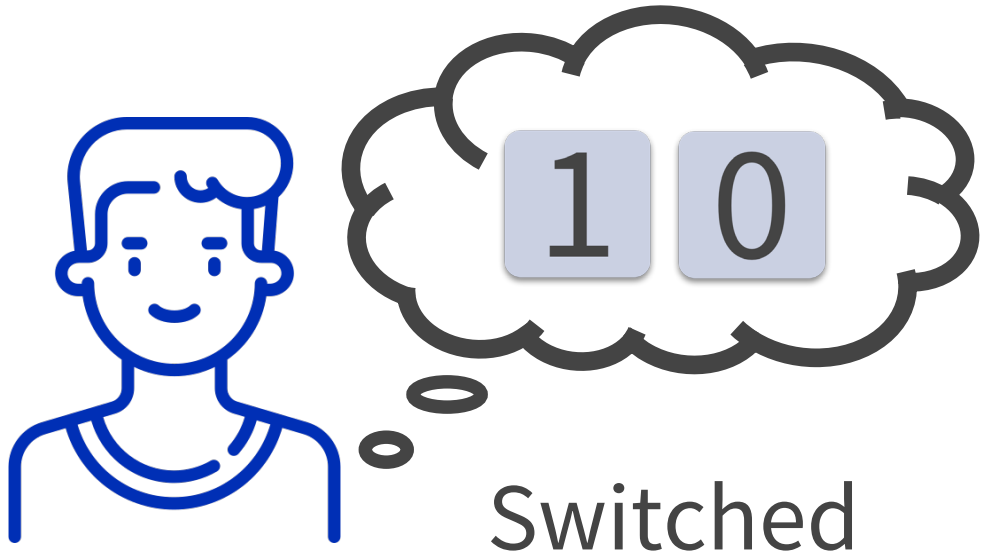
sikoba
RESEARCH

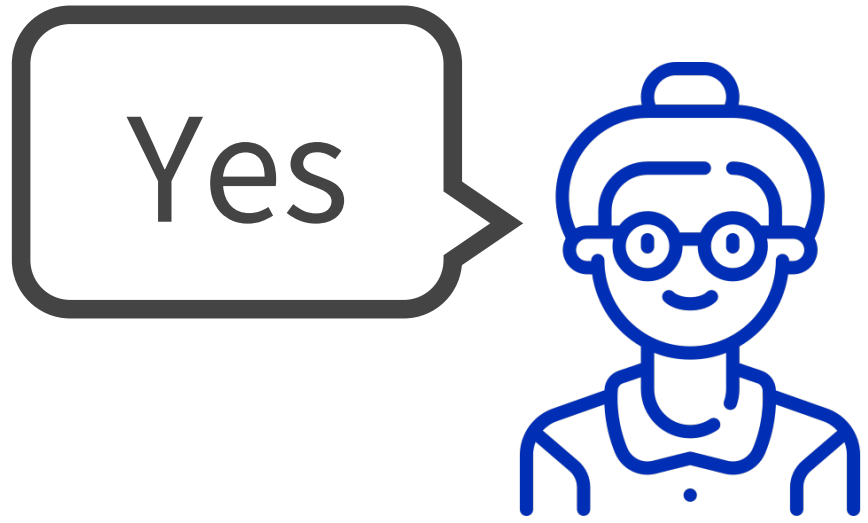
sikoba RESEARCH



Switched

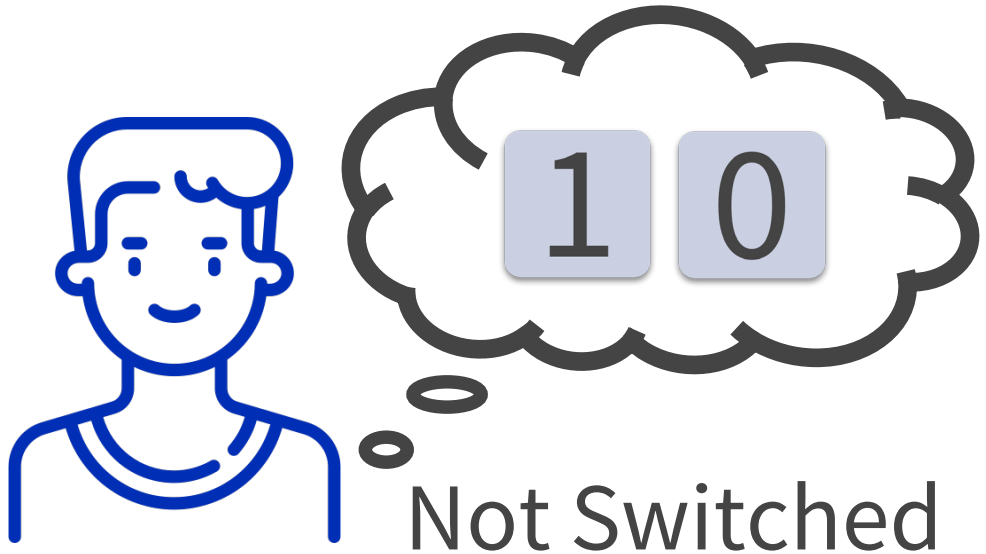
sikoba RESEARCH





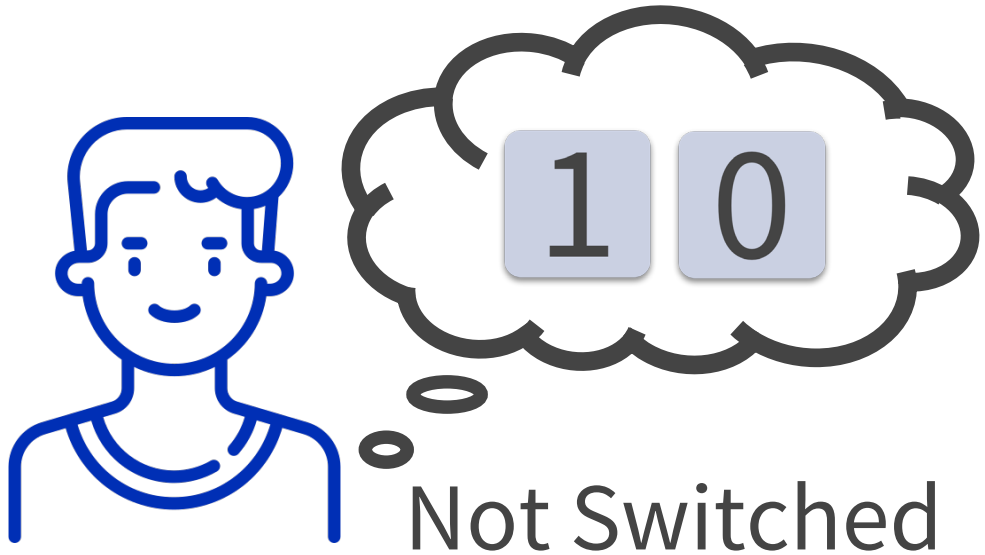
sikoba
RESEARCH

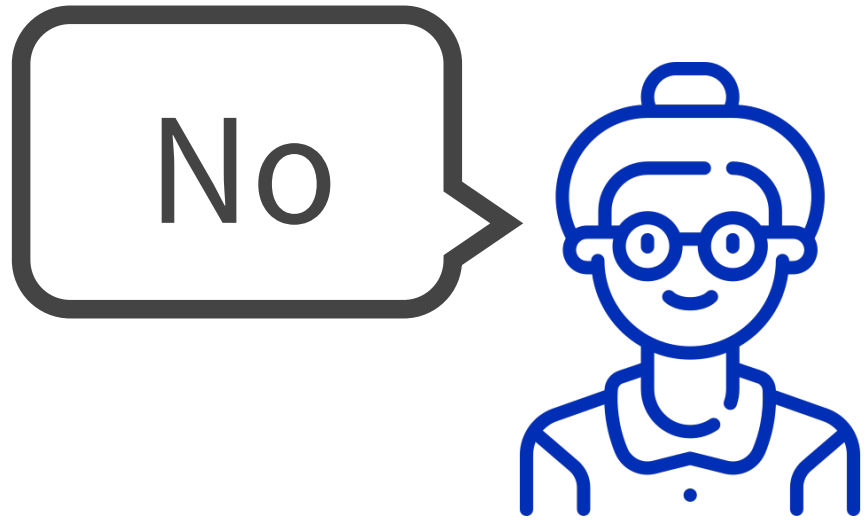
sikoba RESEARCH



Not Switched

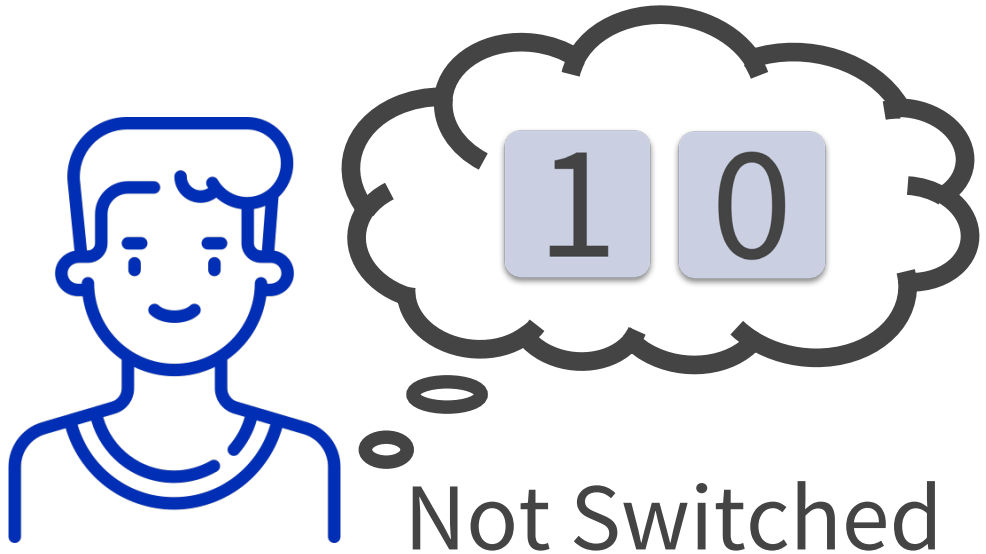
sikoba RESEARCH





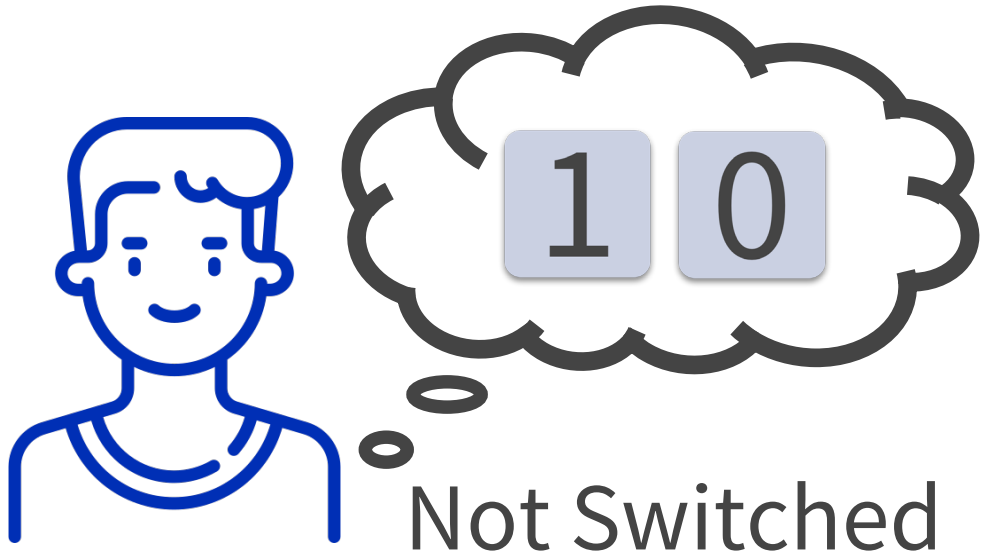
sikoba
RESEARCH

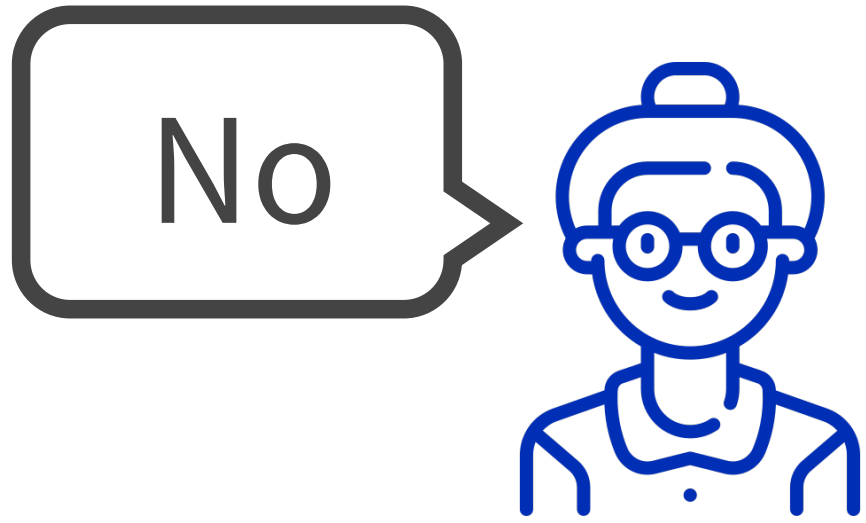
sikoba RESEARCH



Not Switched

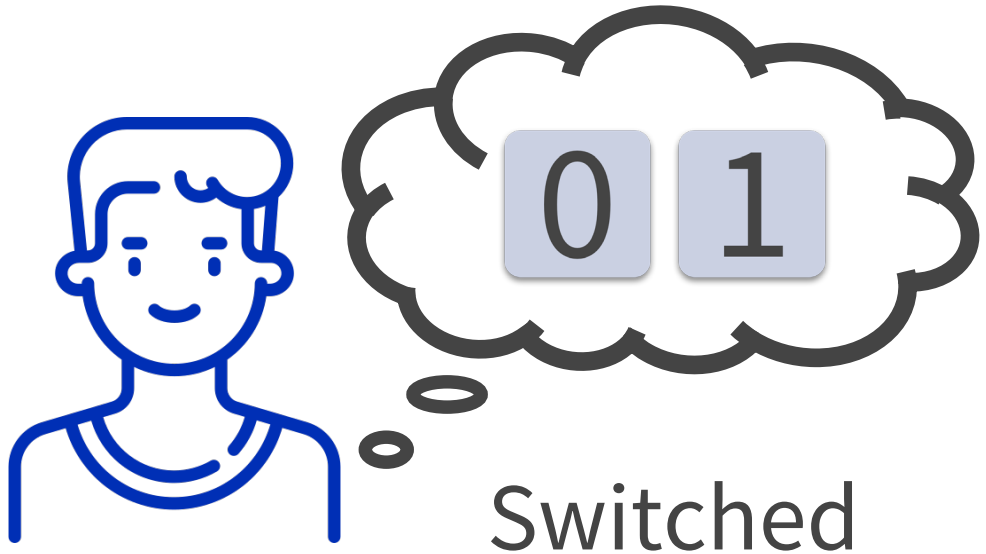
sikoba RESEARCH





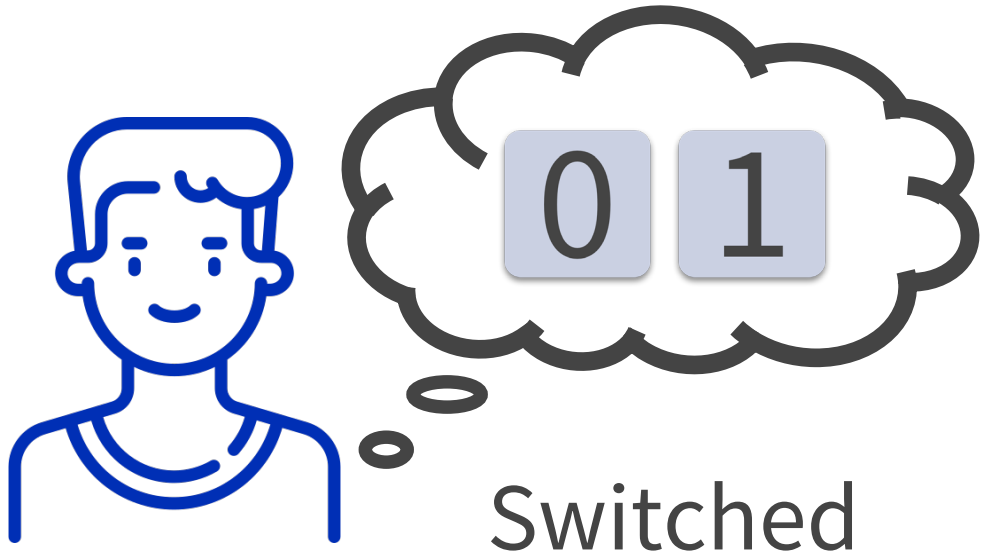
sikoba
RESEARCH

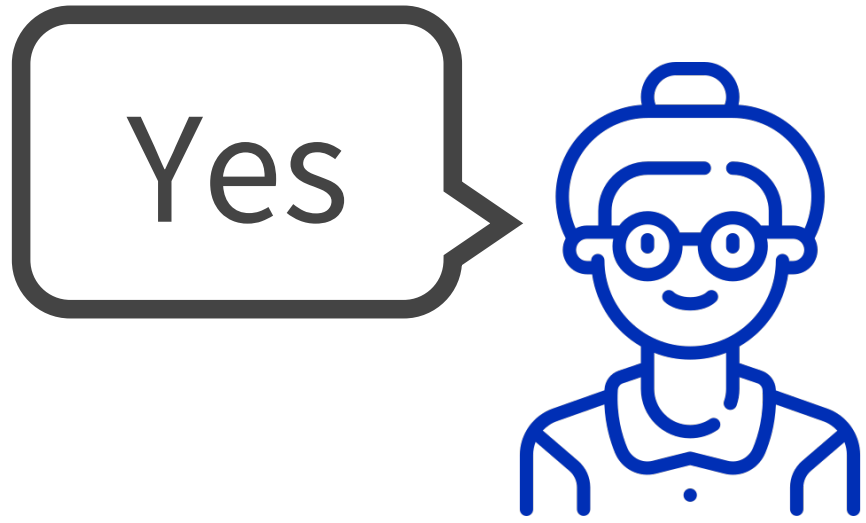
sikoba RESEARCH



Switched

sikoba RESEARCH





Differences

Type of proof:

- Sudoku: the proof can be made certain
- The Psychic: probabilistic proof

Information leakage to oberver:

- Sudoku: the observer is sure that the prover knows
- The Psychic: the observer cannot be certain

Avoiding information leakage

- Requires a probabilistic approach

- Typical approach:

    Commitment, then Challenge / Response

One-way functions (cryptographic hash functions)

sikoba RESEARCH

- Maps data of arbitrary size to pseudo-random data of fixed size, called hash value, or simply **hash**
- Given some data, it is easy to verify that this data maps to a hash.
- Given a hash value, it is practically impossible to find data that maps to that hash ("non-invertible").
- Even a small change to the data will produce a completely different hash value

Example of one-way function(SHA3-256)

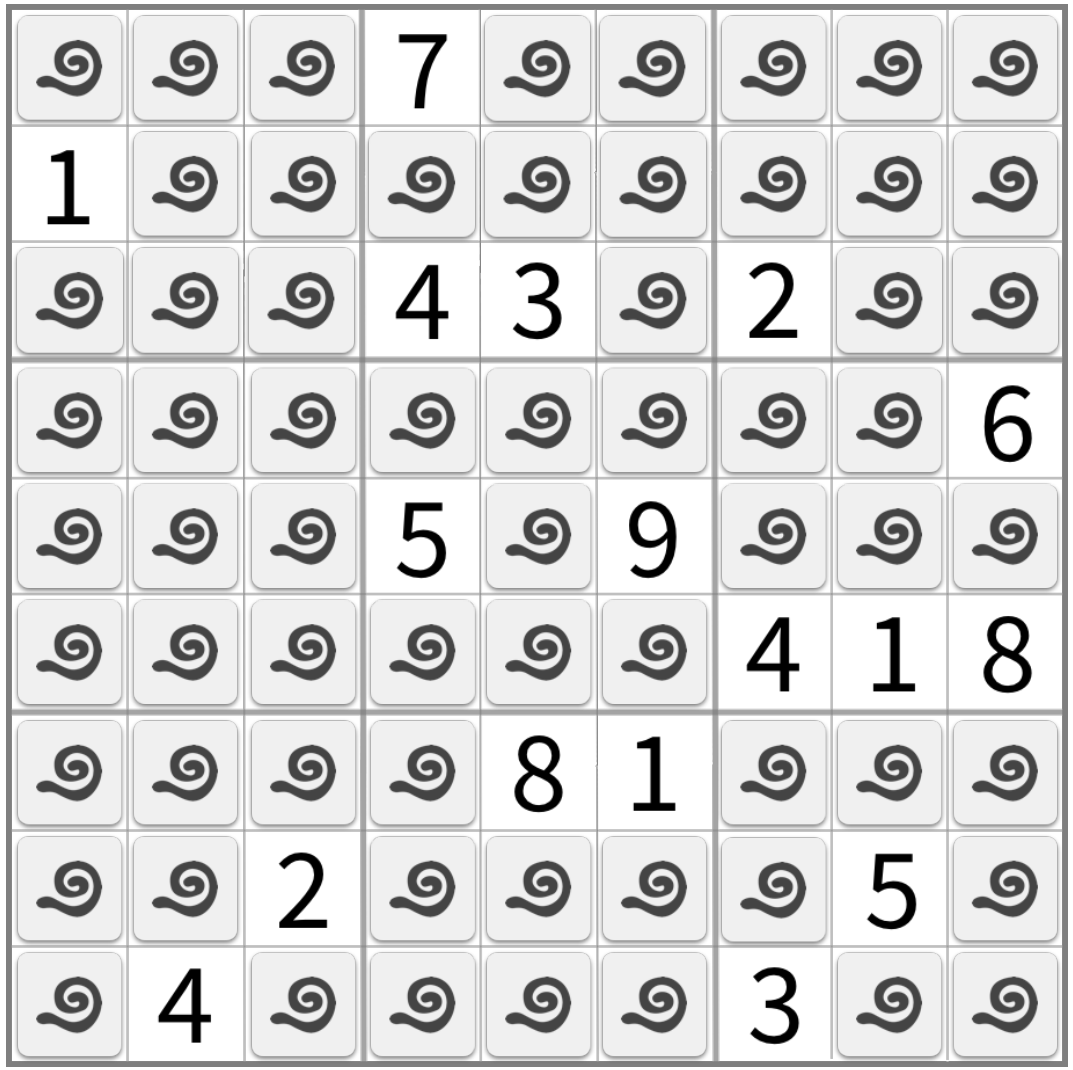
"in the beginning there was light"

```
0xf6f9f09756e41faeee4b6d2baf82d59ac9be3d7f6455f5c1c5
ff0e6dc9b8e750
```

"In the beginning there was light"

```
0xdc2b73c346a88e3bf8de68cc66fe444f6f4663cd8c6b5cab38
d378b71af20df2
```

sikoba RESEARCH



Prover generates a “Commitment” linked to the entire solution.

Repeat :

- Verifier sends a “Challenge” (typically a random number)
- Prover returns “Response” proof
- Verifier checks if proof is consistent with the commitment

… until likelihood of cheating is as small as desired

An observer obtains no information!

Vocabulary

- **Completeness**: the method works with probability 1
- **Soundness**: prover dishonest, verifier honest (prover cannot cheat)
- **Zero Knowledge**: prover honest, verifier dishonest (verifier cannot extract any information)

Thank you!