

Zero-Knowledge Proofs

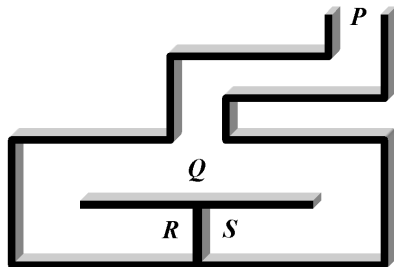
Showing you *can* do something, without showing how

Alex Dehnert

6.UAT

Fall 2011

Problem: Ali Baba's Cave

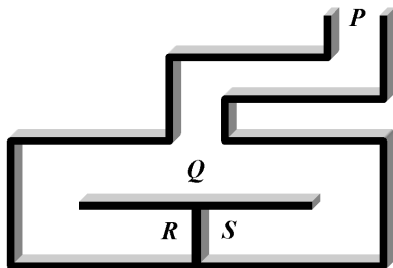


- Imagine that you (Peggy) are exploring a cave with a friend
- You know a secret password to get through the door between R and S
- You want to prove to your friend Victor that you know the password, without him finding out the password.

Image: RSA Laboratories

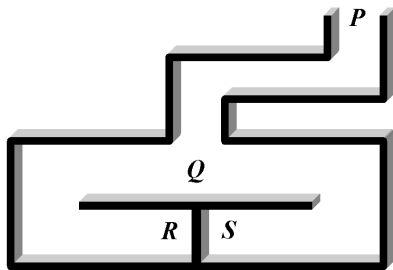
Solution

- Victor stands outside at P
- Peggy vanishes into the cave and stands at R or S
- Victor comes back in, stands at Q , and calls out which side Peggy should return by
- Peggy returns as requested



What if Peggy cheats?

- Victor stands outside at P
- Peggy picks R or S to hide at
- Victor comes back in, stands at Q , and calls out which side Peggy should return by
- If Peggy picked the correct side, she tricks Victor; otherwise, she has to admit she lied
- If Victor does this enough times, Peggy will guess wrong (one trial, 50% she succeeds; two trials, 25%; etc.)



Zero-Knowledge Proofs

Goal: Peggy (prover) wants to convince Victor (verifier) of something

Convincing If true, an honest prover can always convince an honest verifier

No cheating If false, a dishonest prover can only rarely convince an honest verifier

Zero knowledge If true, a cheating verifier cannot learn anything more than that it is true.

General Structure

Peggy: Prepare

Peggy: Commit

Victor: Challenge

Peggy: Respond

General Structure

Victor stands outside

Peggy: Prepare

Peggy vanishes into the cave

Peggy: Commit

Victor: Challenge

Peggy: Respond

General Structure

Peggy: Prepare

Victor stands outside

Peggy vanishes into the cave

Peggy: Commit

Victor comes back in, ...

Victor: Challenge

Peggy: Respond

General Structure

Peggy: Prepare

Victor stands outside

Peggy vanishes into the cave

Peggy: Commit

Victor comes back in, ...

Victor: Challenge

... and calls out which side
Peggy should return by

Peggy: Respond

General Structure

Peggy: Prepare	Victor stands outside
Peggy: Commit	Peggy vanishes into the cave
Victor: Challenge	Victor comes back in, ...
Peggy: Respond	... and calls out which side Peggy should return by
	Peggy returns as requested

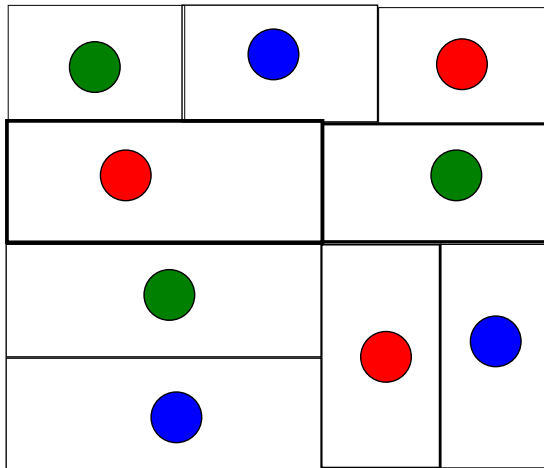
Map 3-coloring

Given a map, prove that it can be colored using only three colors (and that you know a coloring).



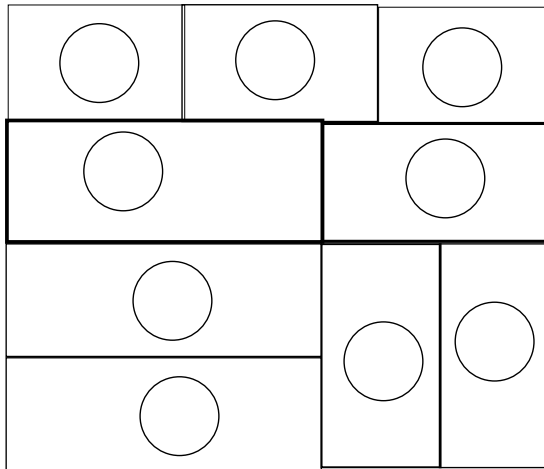
Map coloring ZKP

Prepare

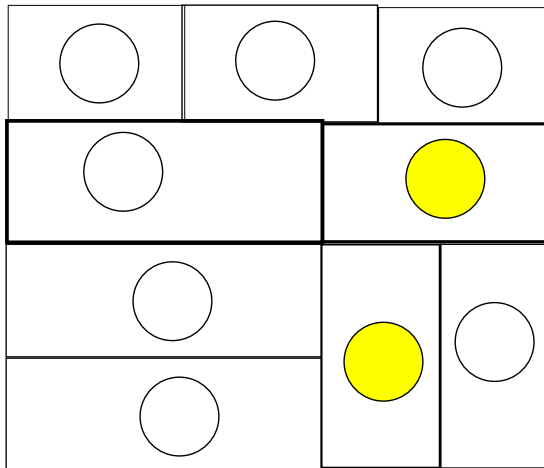


Map coloring ZKP

Commit

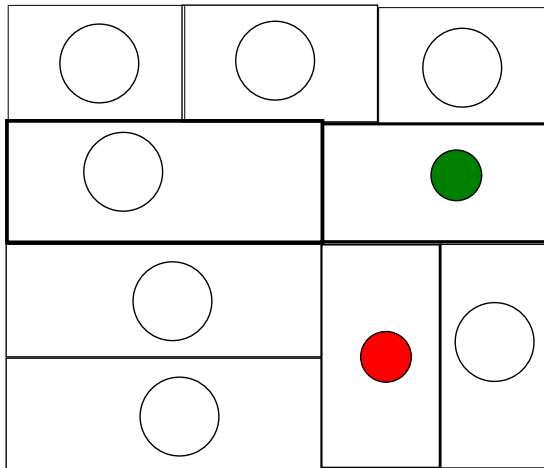


Challenge



Map coloring ZKP

Respond



Possible application: Proof of identity

- Numerous cases where you want to prove who you are
- Example: authorize a credit card transaction
- Don't want stores to be able to charge you for more stuff later
- Use zero-knowledge proof to prove who you are, instead of a credit card number you keep secret