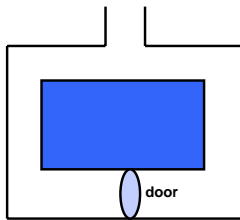


Zero-knowledge protocol

- Idea: (interactive) proof btw prover A & verifier B
- At the end of the proof, B is convinced A knows a secret satisfying a fact F
- But B has no information about that secret

13

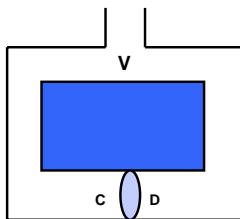
The Zero-knowledge Cave (I)



- Alice wants to prove to Bob that she knows how the magic word to open door
 - Without telling Bob the magic word

14

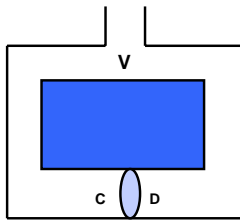
The Zero-knowledge Cave (II)



1. Alice walks to either C or D;
2. Bob stands at V, calling either Left or Right;
3. Alice complies, using her magic word to open door if needed;
4. Alice & Bob repeats steps 1-3 for n times

15

The Zero-knowledge Cave (III)



- What if Alice didn't know the magic word?
- What does Bob learn at the end of the proof?

16

How to prove knowledge of square root

- Finding square root mod $N=pq$ is as hard as factoring
- A knows b s.t. $b^2 \equiv y \pmod{pq}$, & wishes to prove to B that she knows such b .
- $A \rightarrow B$: $s = r^2 \pmod{pq}$ (A picks random r)
- B flips coin
- $B \rightarrow A$: coin flip
- If heads
 - $A \rightarrow B$: $t = r \pmod{pq}$
 - B verifies $t^2 \equiv s \pmod{pq}$
- If tails
 - $A \rightarrow B$: $t = rb \pmod{pq}$
 - A verifies $t^2 \equiv sy \pmod{pq}$
- What if A didn't know the square root?
- What did B learn after the proof?

17
