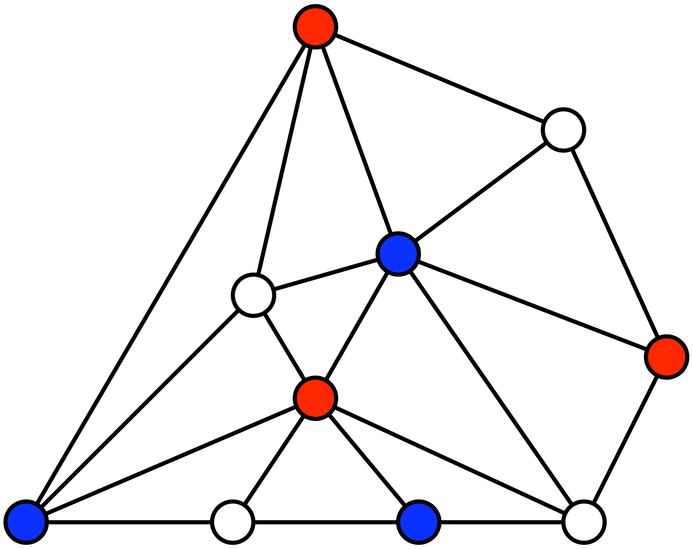
Zero-Knowledge Proofs



Alice knows how to 3-color a graph.

- no two adjacent nodes have the same color
- NP-complete problem
- can impress your friends
- useful for identification

Zero-Knowledge Proofs

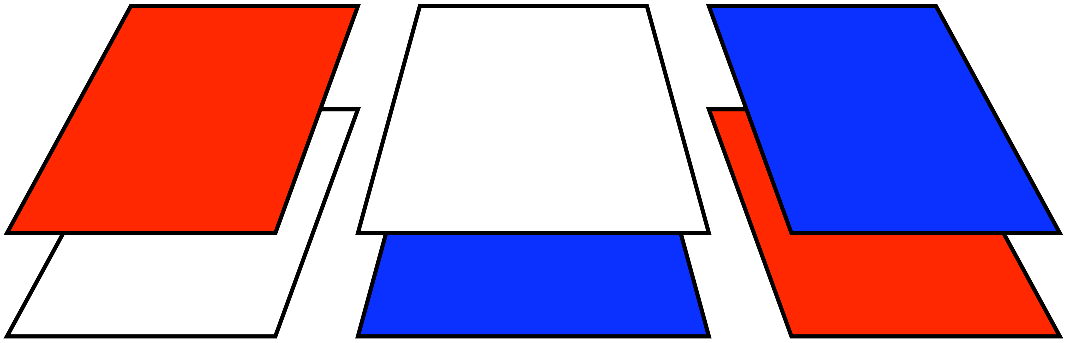
How can Alice convince Bob that she can 3-color the graph without

- letting him steal her work?
- letting him impersonate her?

Zero-Knowledge Proofs

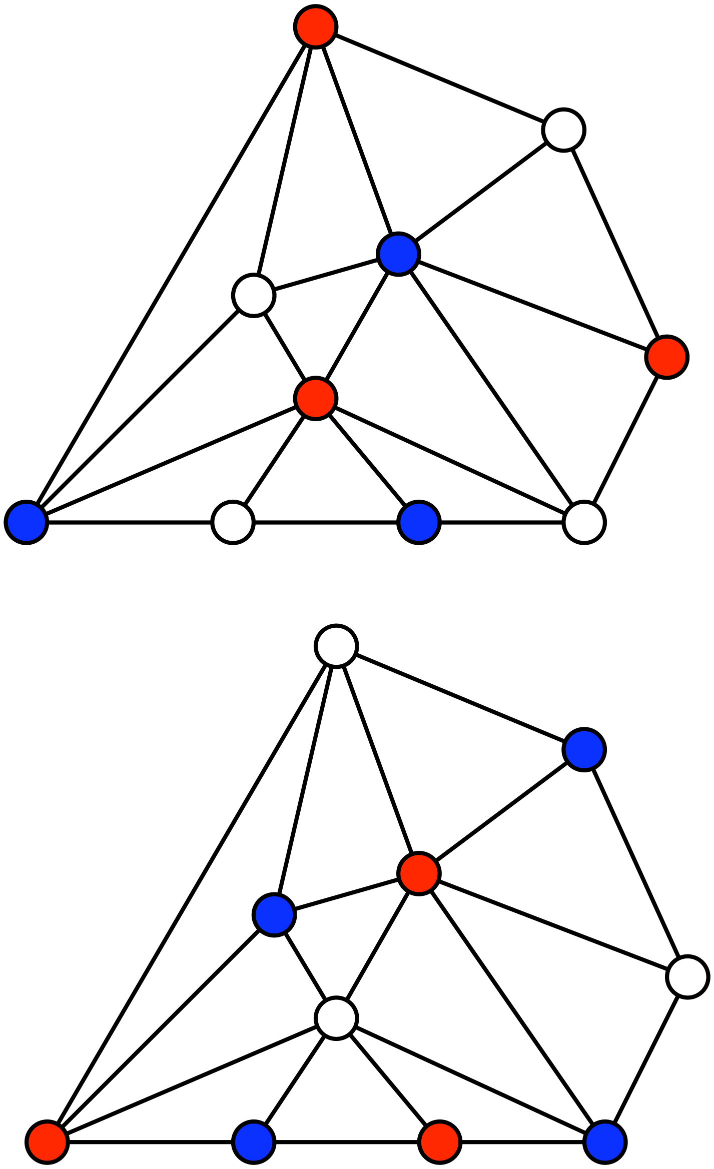
- Bob is convinced Alice can do it
- Bob has no idea how to do it himself.

Zero-Knowledge Proofs



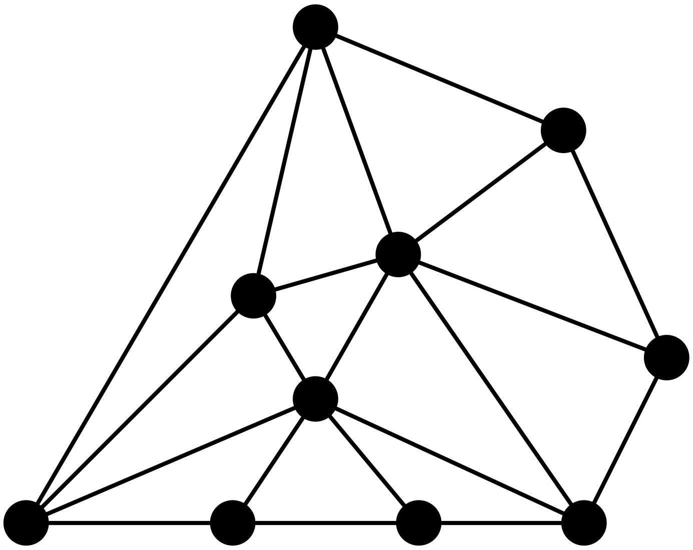
Alice randomly permutes the colors.

Zero-Knowledge Proofs



Alice permutes the vertex colors.

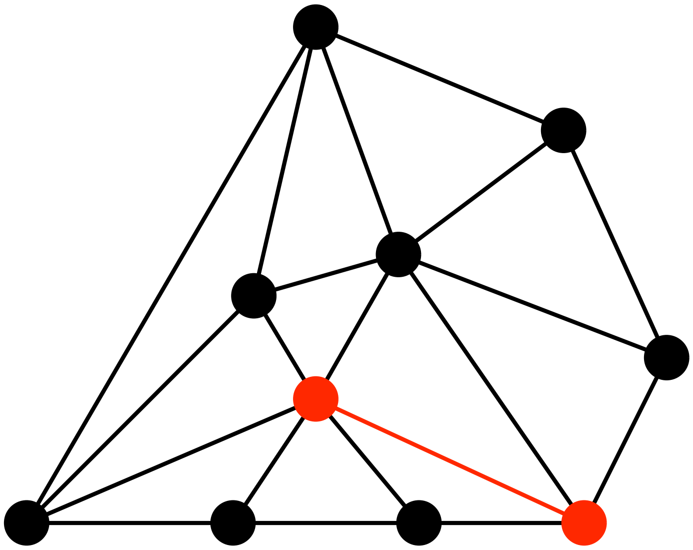
Zero-Knowledge Proofs



Alice

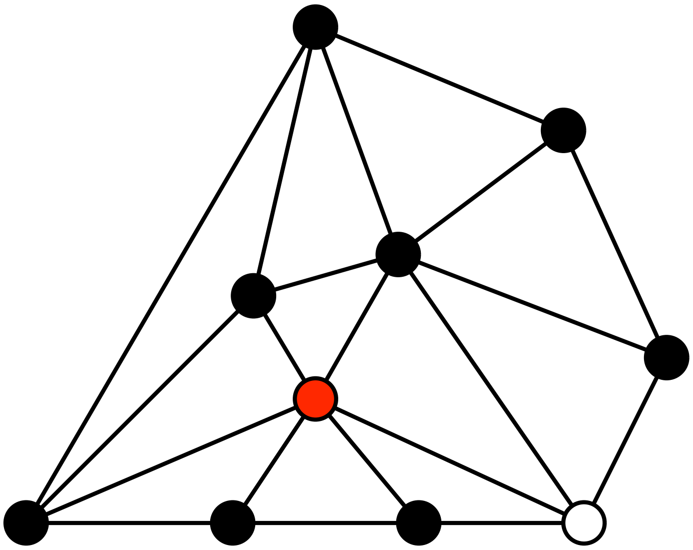
- encrypts vertex colors
- one key per vertex
- and sends graph to Bob

Zero-Knowledge Proofs



Bob picks edge at random.

Zero-Knowledge Proofs



Alice reveals colors of those two keys.

Zero-Knowledge Proofs

Repeat as needed:

- Alice permutes graph coloring
- Alice encrypts each graph node with distinct key
- Alice sends permuted encrypted colors to Bob
- Bob picks an edge
- Alice sends keys for two edges
- Bob checks that colors are distinct

Zero-Knowledge Proofs

If Alice is lying

- probability $\frac{1}{E}$ she will be caught

If Alice is telling the truth

- she will never be caught

After k repetitions, probability she fools Bob is $(1 - \frac{1}{E})^k$.

Zero-Knowledge Proofs

What does Bob see?

- randomly-generated keys
- randomly-generated colors

Because Bob could have generated those keys and colors himself, he learns nothing about the graph coloring.

Claim: Every problem in NP has a zero-knowledge proof.