Zero-Knowledge Proofs

Akshayaram Srinivasan

Gödel prize 1993: László Babai, Shafi Goldwasser, Silvio Micali, Shlomo Moran, and Charles Rackoff

Zero-Knowledge Proofs

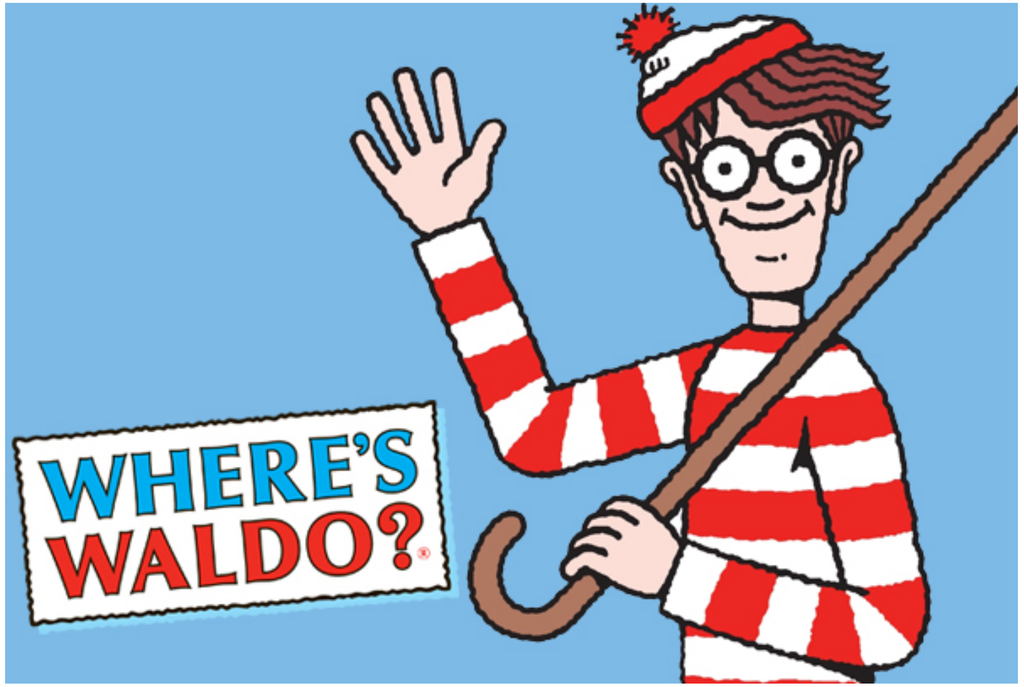
Akshayaram Srinivasan

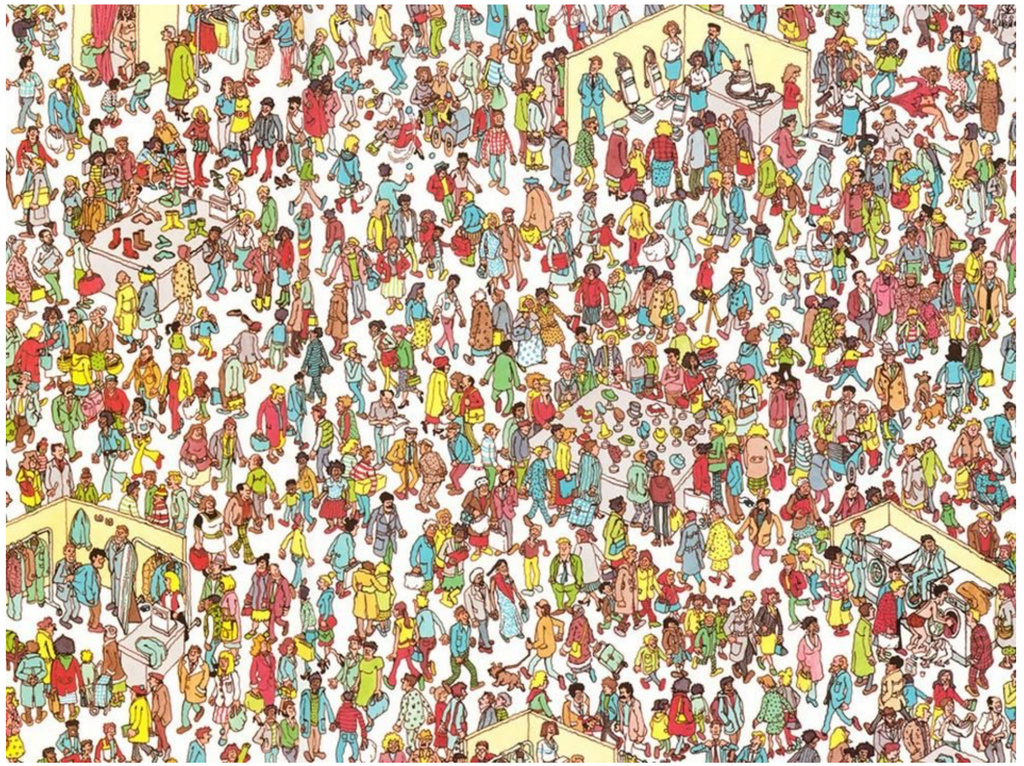
Gödel prize 1993: László Babai, Shafi Goldwasser, Silvio Micali, Shlomo Moran, and Charles Rackoff

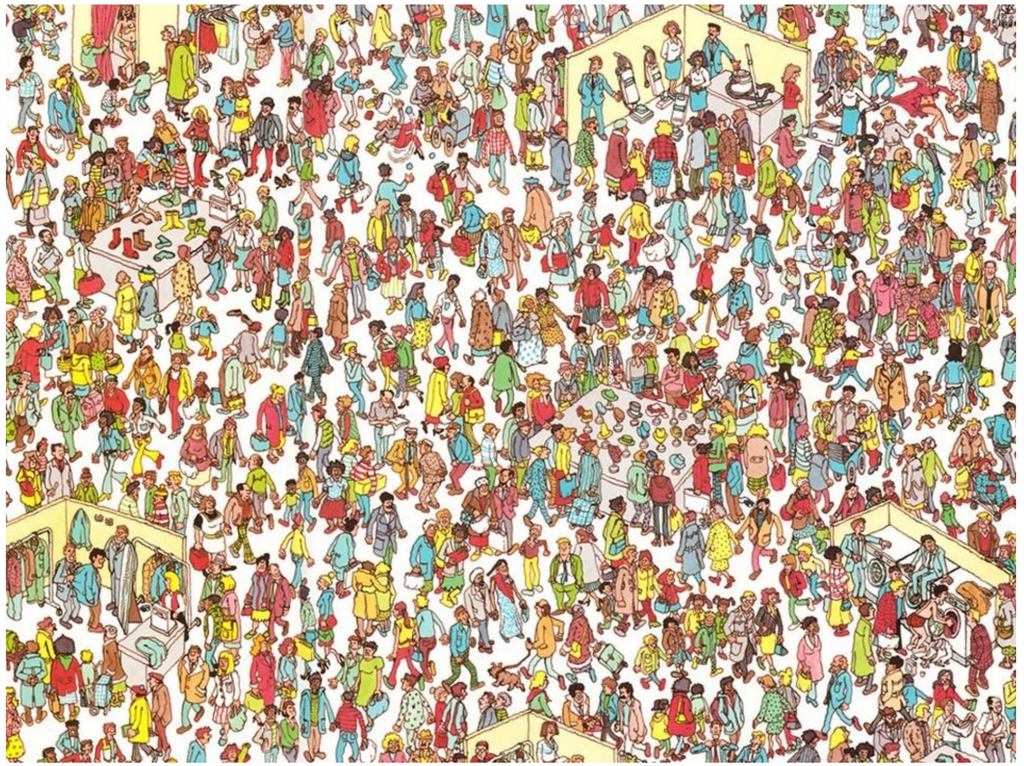
Turing Award 2012: Shafi Goldwasser and Silvio Micali

Zero-Knowledge Proofs

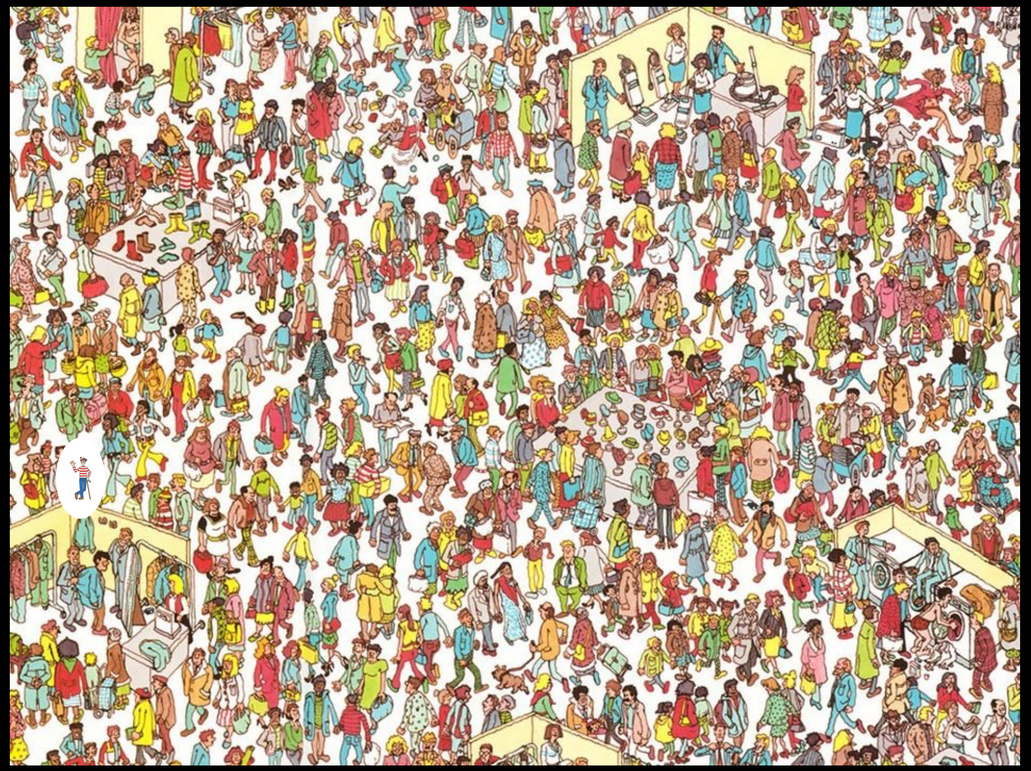
Akshayaram Srinivasan

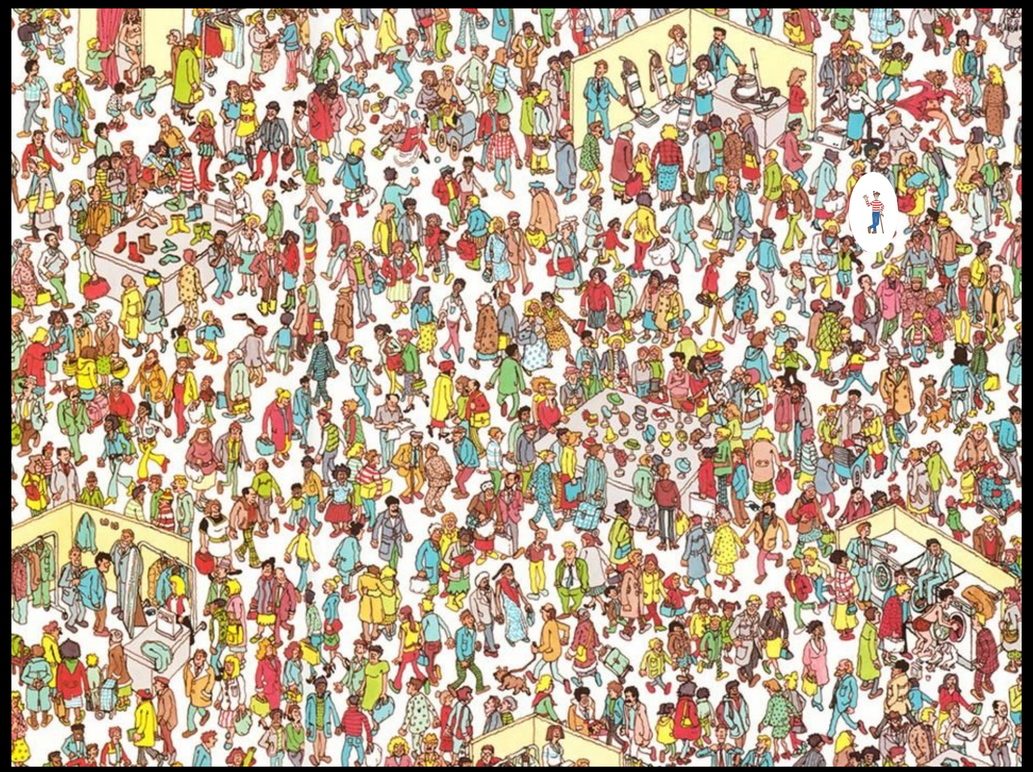

WHERE'S
WALDO?

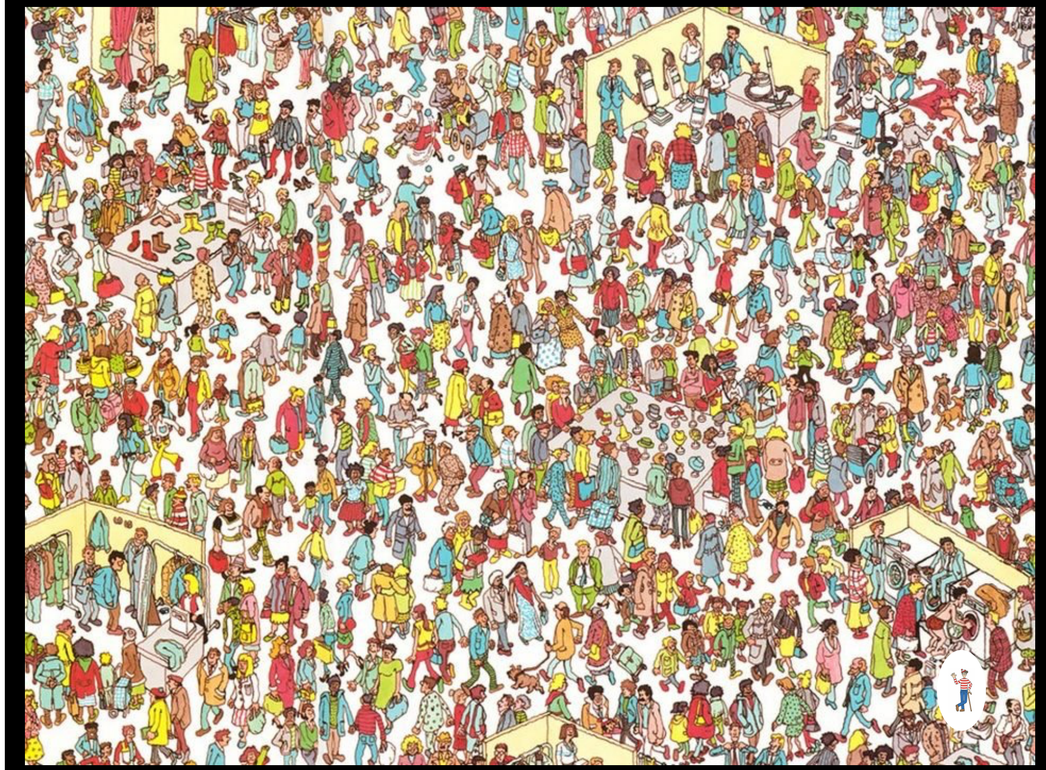




Can I prove where's Waldo without revealing his coordinates?







Example

Example

You were convinced about an Assertion

Example

You were convinced about an Assertion

You didn’t learn any other information apart from the fact that the assertion is true.

Example

You were convinced about an Assertion

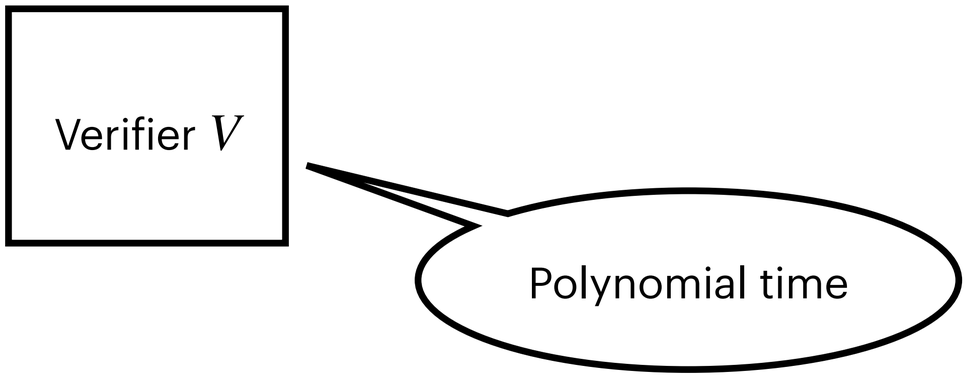
You didn’t learn any other information apart from the fact that the assertion is true.

This is the core idea behind zero-knowledge proofs

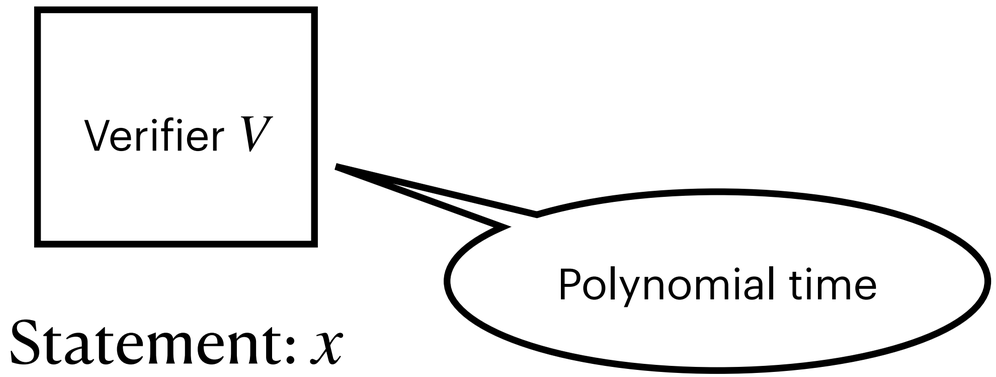
Interactive Proofs

Interactive Proofs

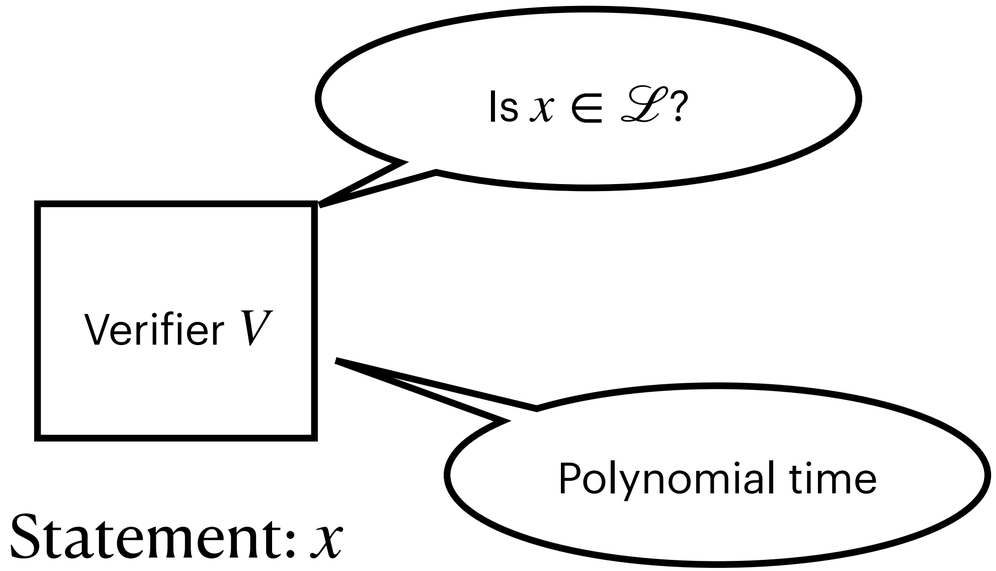
Interactive Proofs



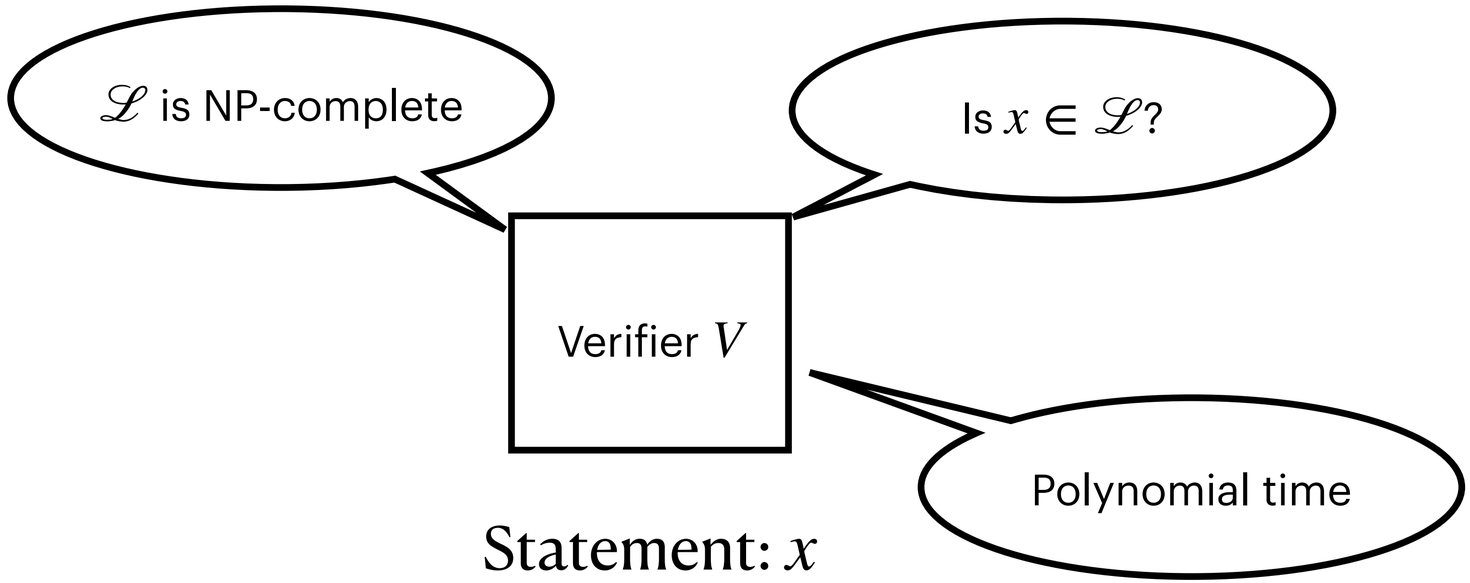
Interactive Proofs



Interactive Proofs



Interactive Proofs



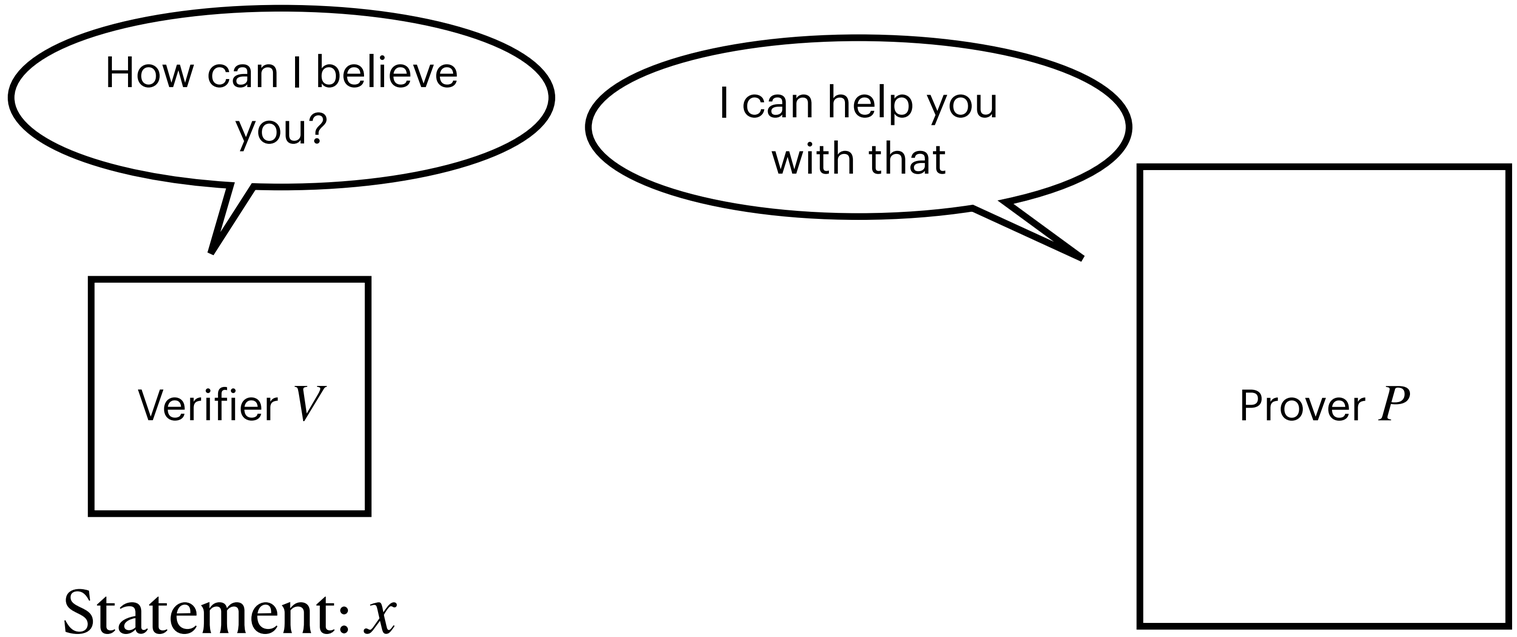
Interactive Proofs

Statement: x

Interactive Proofs

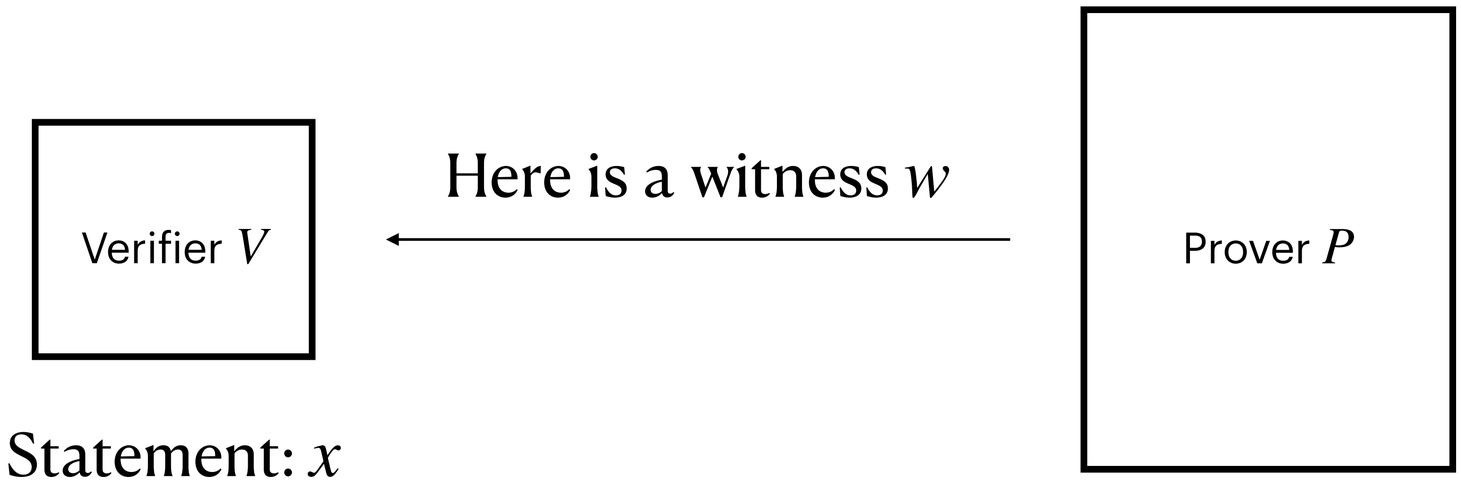
Interactive Proofs

Interactive Proofs

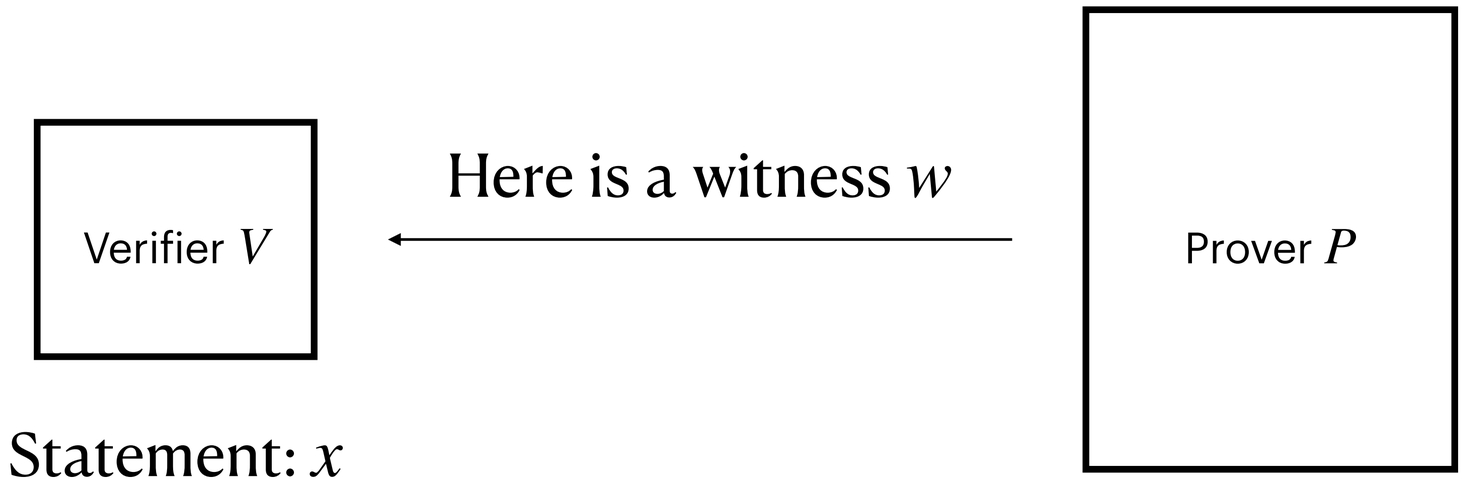


Interactive Proofs

Interactive Proofs

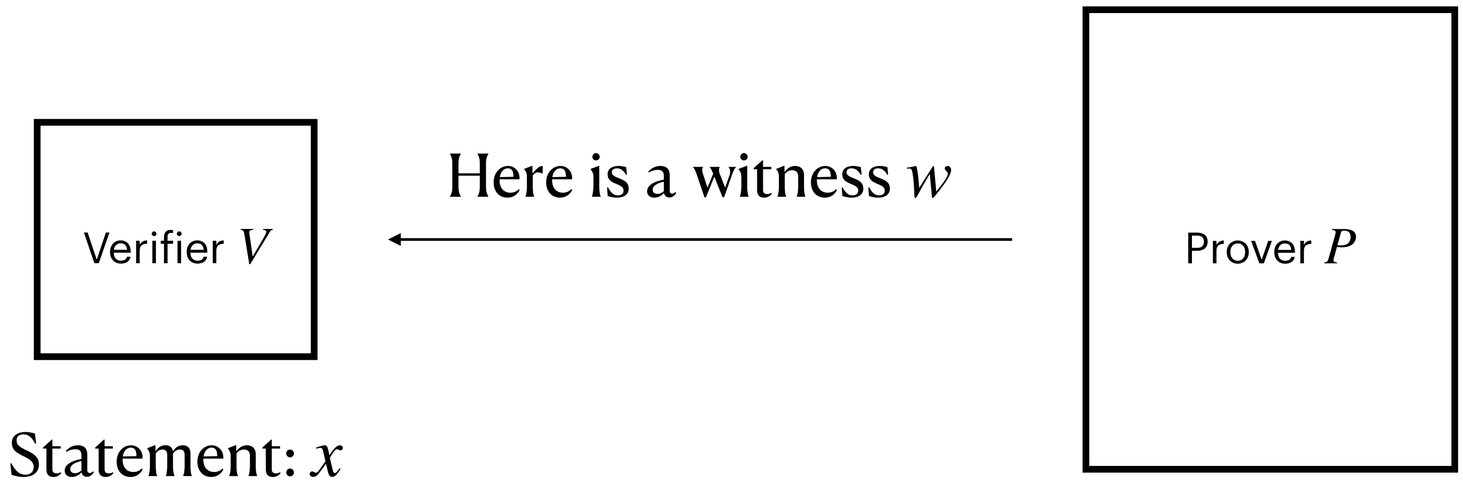


Interactive Proofs



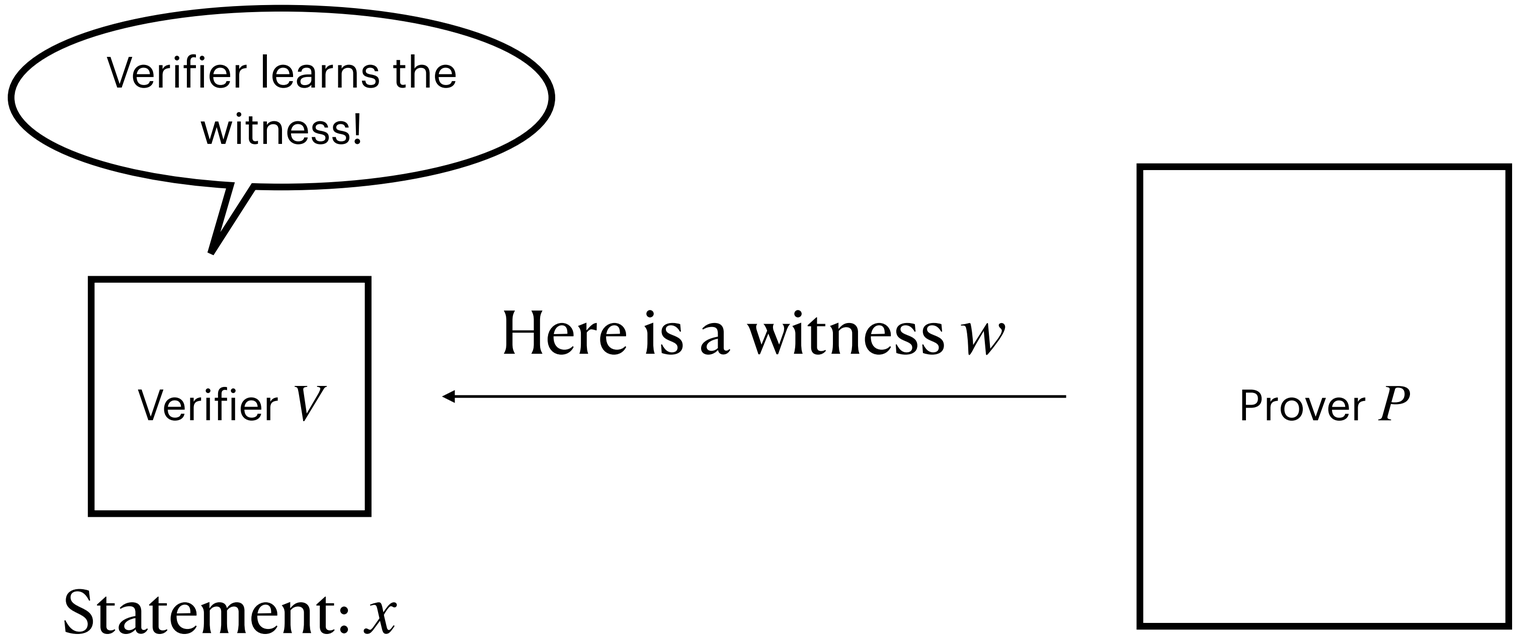
- **Completeness:** If $x \in \mathscr{L}$, then prover can send a witness that makes the verifier accept.

Interactive Proofs



- **Completeness:** If $x \in \mathscr{L}$, then prover can send a witness that makes the verifier accept.
- **Soundness:** If $x \notin \mathscr{L}$, then whatever string prover sends, the verifier rejects.

Interactive Proofs

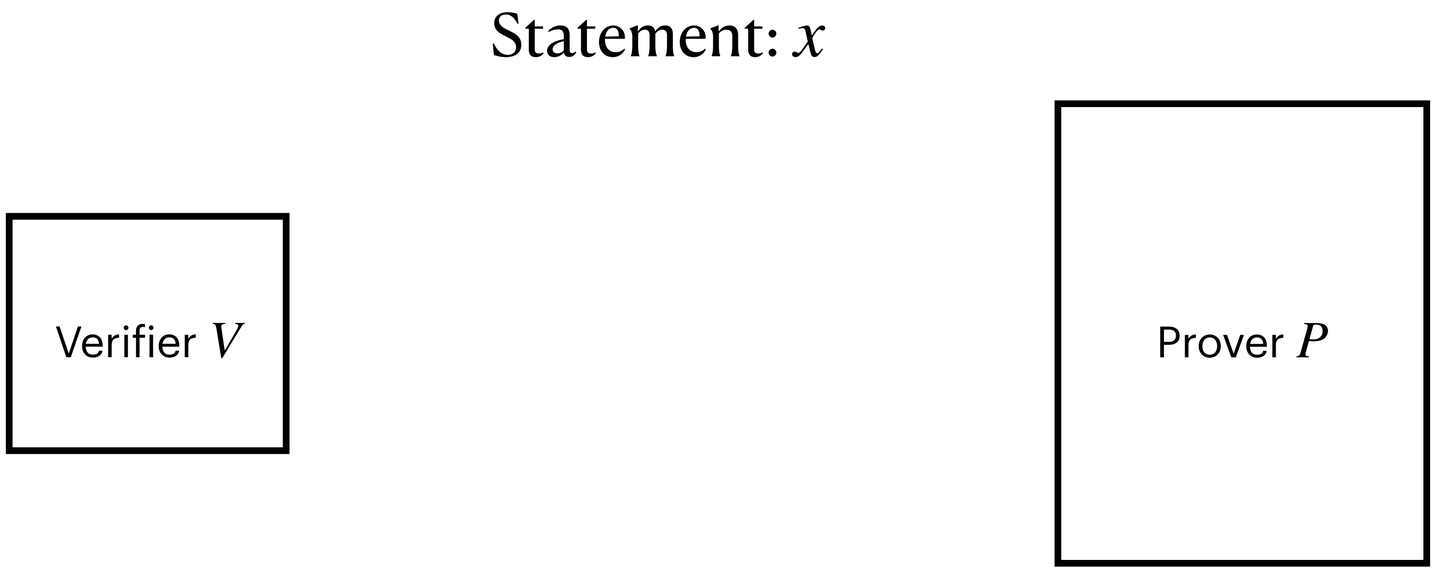


- **Completeness:** If $x \in \mathscr{L}$, then prover can send a witness that makes the verifier accept.
- **Soundness:** If $x \notin \mathscr{L}$, then whatever string prover sends, the verifier rejects.

Can we convince the verifier that $x \in \mathscr{L}$ without leaking any information about the witness?

Zero-Knowledge Proofs

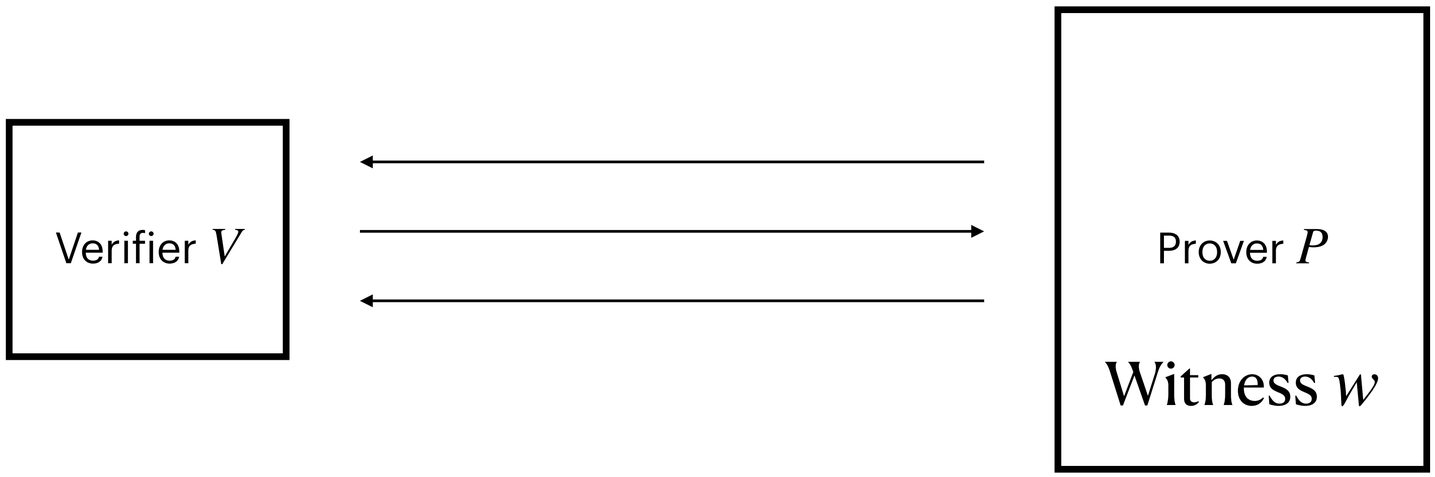
Zero-Knowledge Proofs



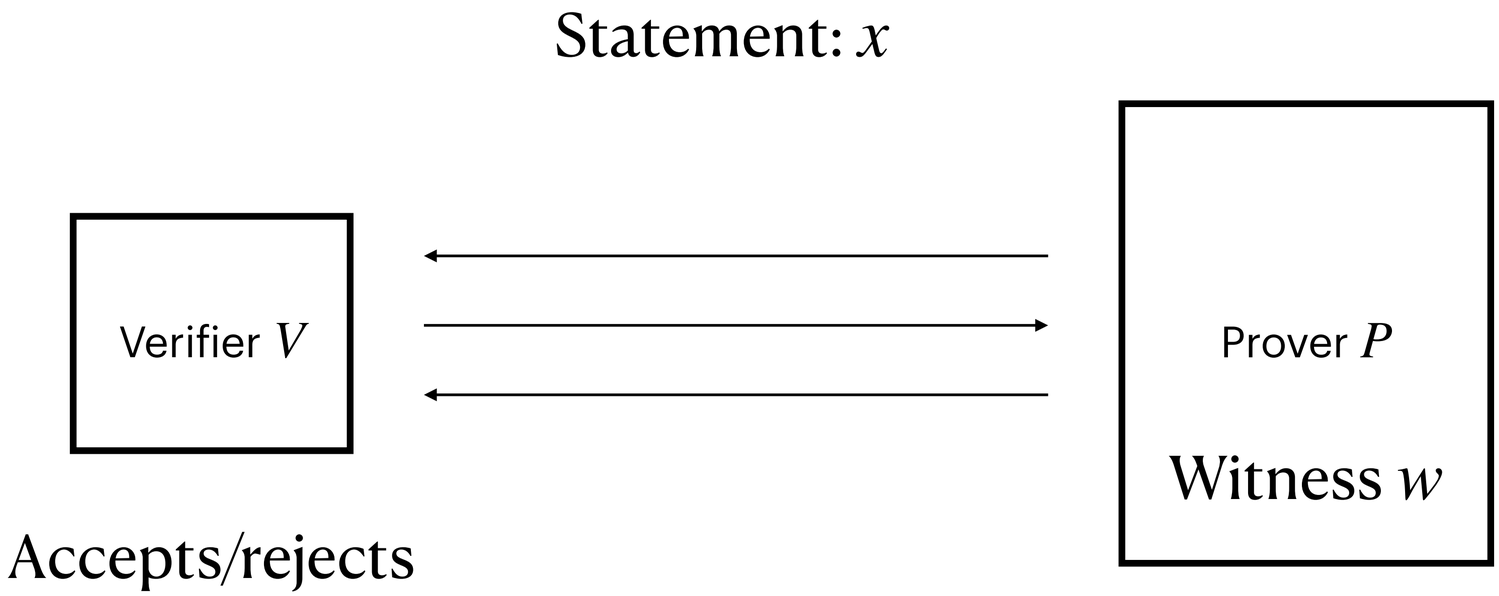
Zero-Knowledge Proofs

Statement: x

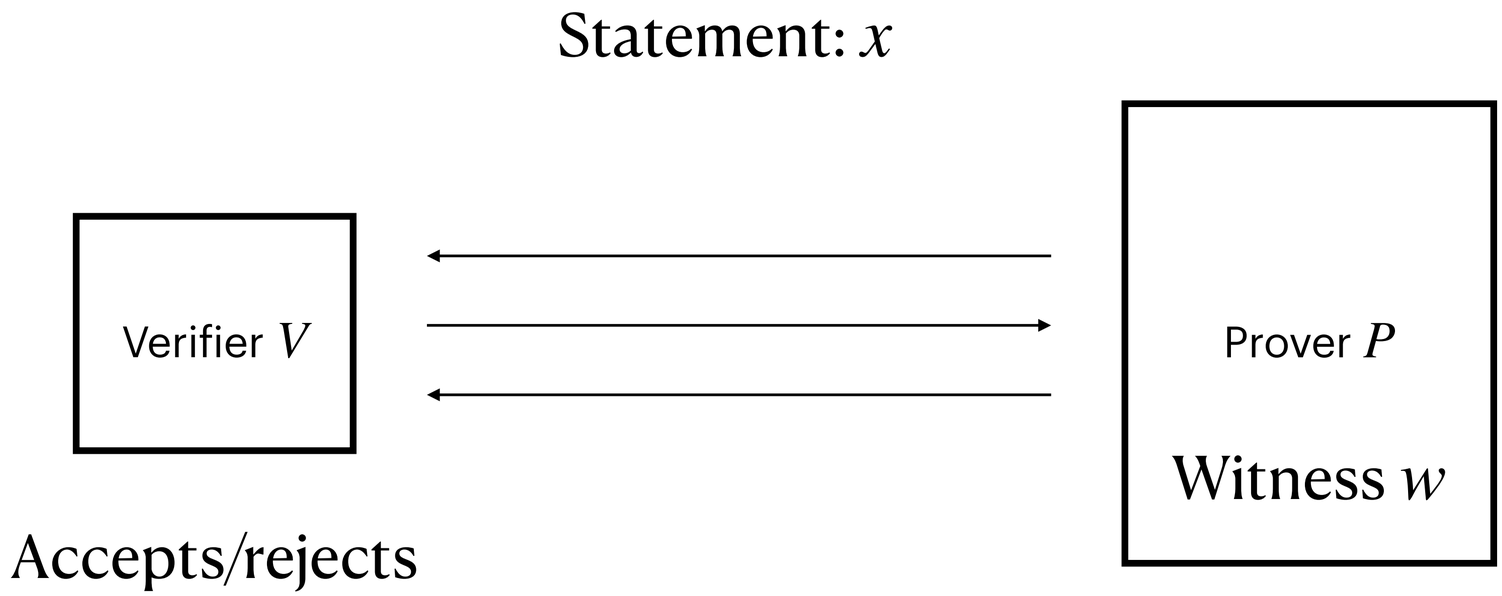
Zero-Knowledge Proofs



Zero-Knowledge Proofs

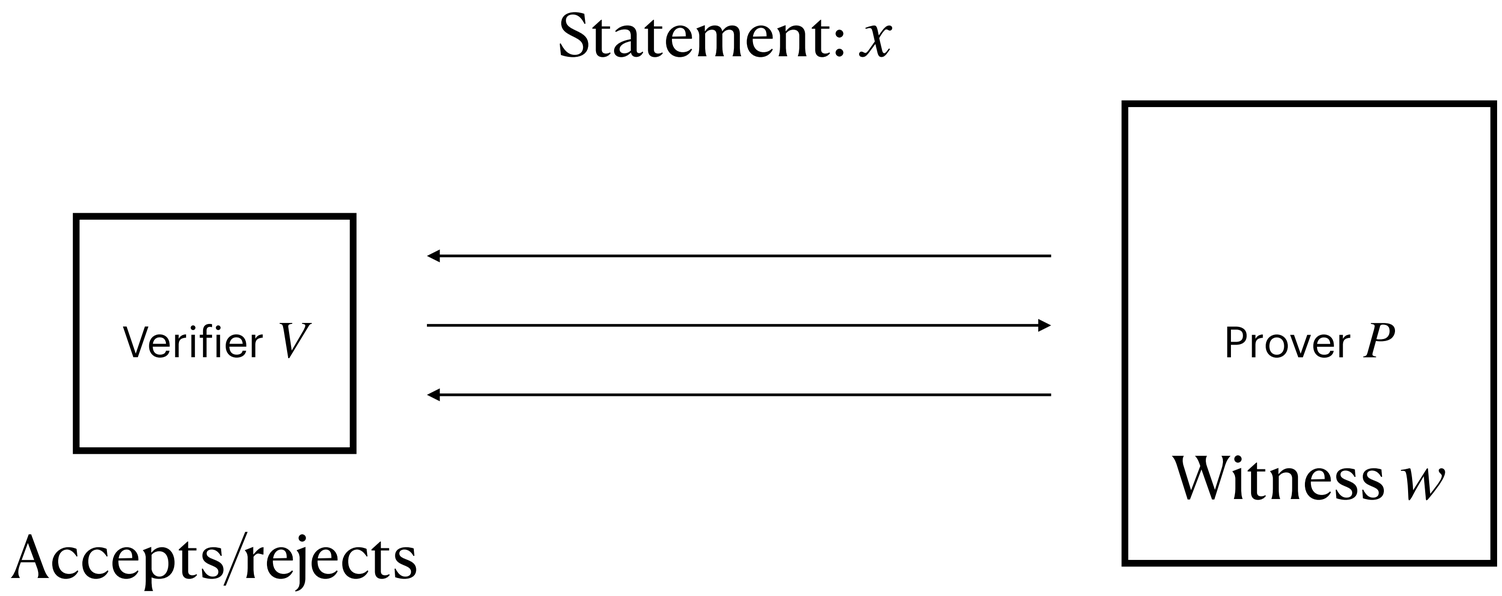


Zero-Knowledge Proofs



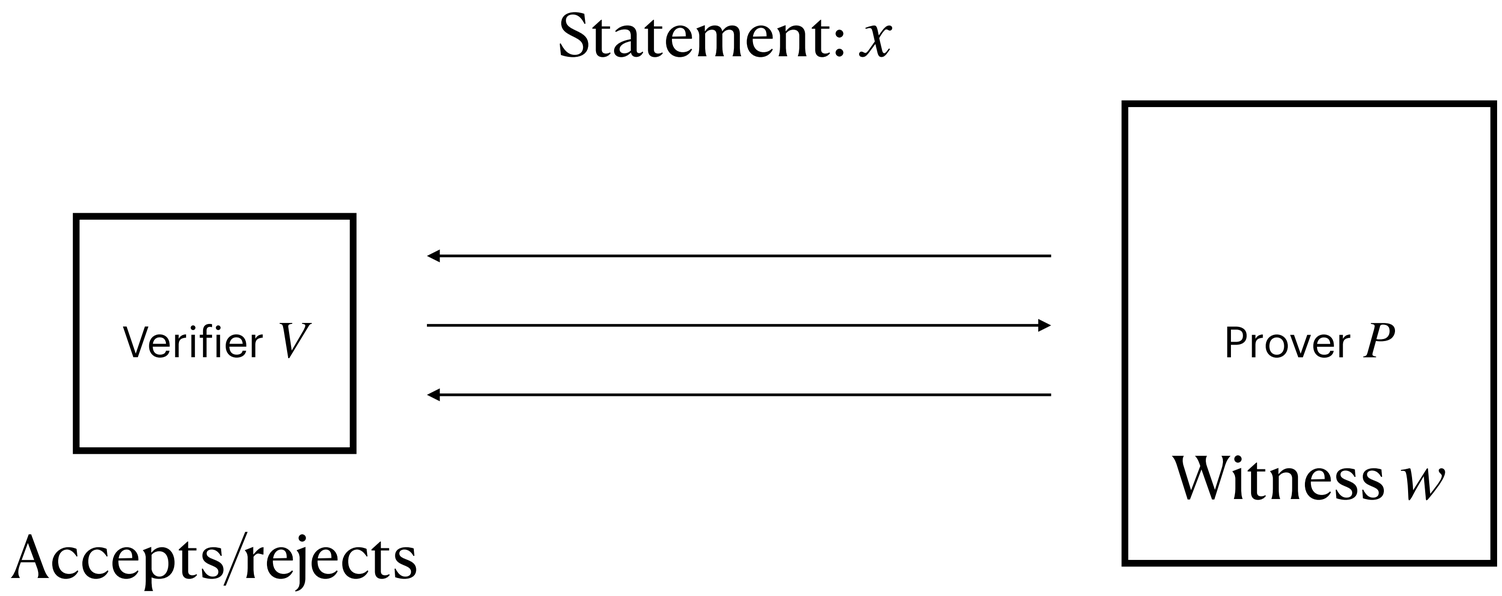
- **Completeness:** If $x \in \mathscr{L}$, then verifier accepts at the end of the interaction.

Zero-Knowledge Proofs



- **Completeness:** If $x \in \mathscr{L}$, then verifier accepts at the end of the interaction.
- **Soundness:** If $x \notin \mathscr{L}$, then verifier accepts with probability at most 1/3.

Zero-Knowledge Proofs



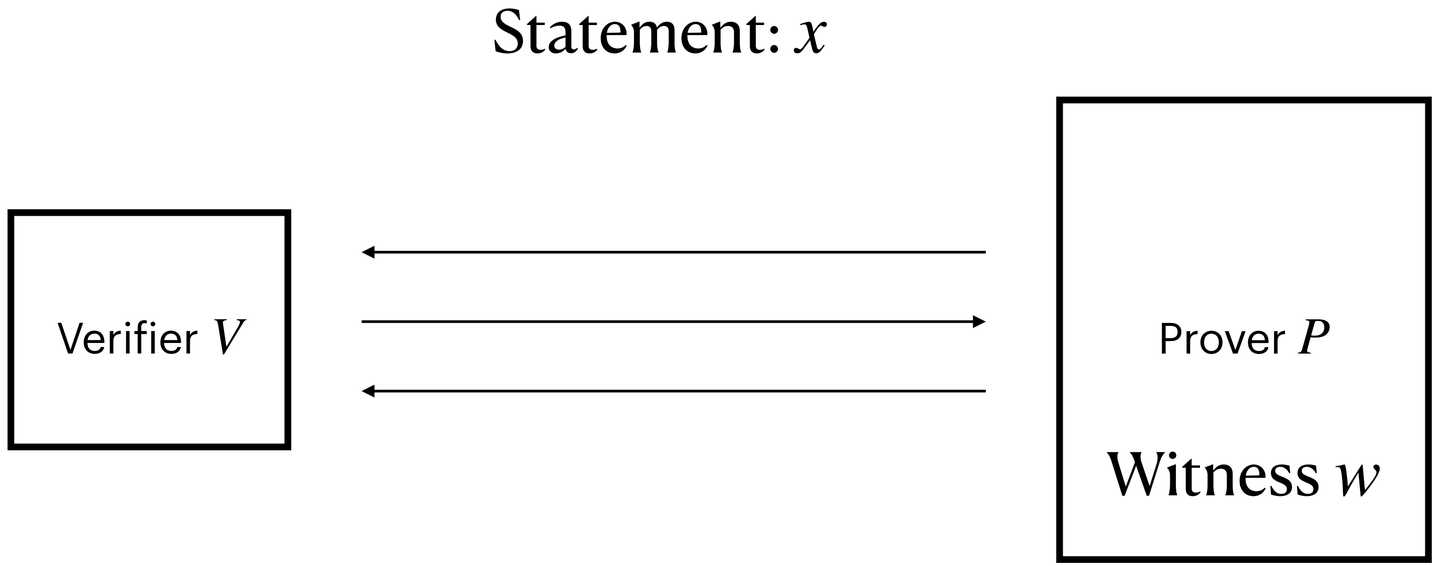
- **Completeness:** If $x \in \mathscr{L}$, then verifier accepts at the end of the interaction.
- **Soundness:** If $x \notin \mathscr{L}$, then verifier accepts with probability at most 1/3.
- **Zero-knowledge:** The verifier should learn no information about the witness.

How to formally define?

An Attempt

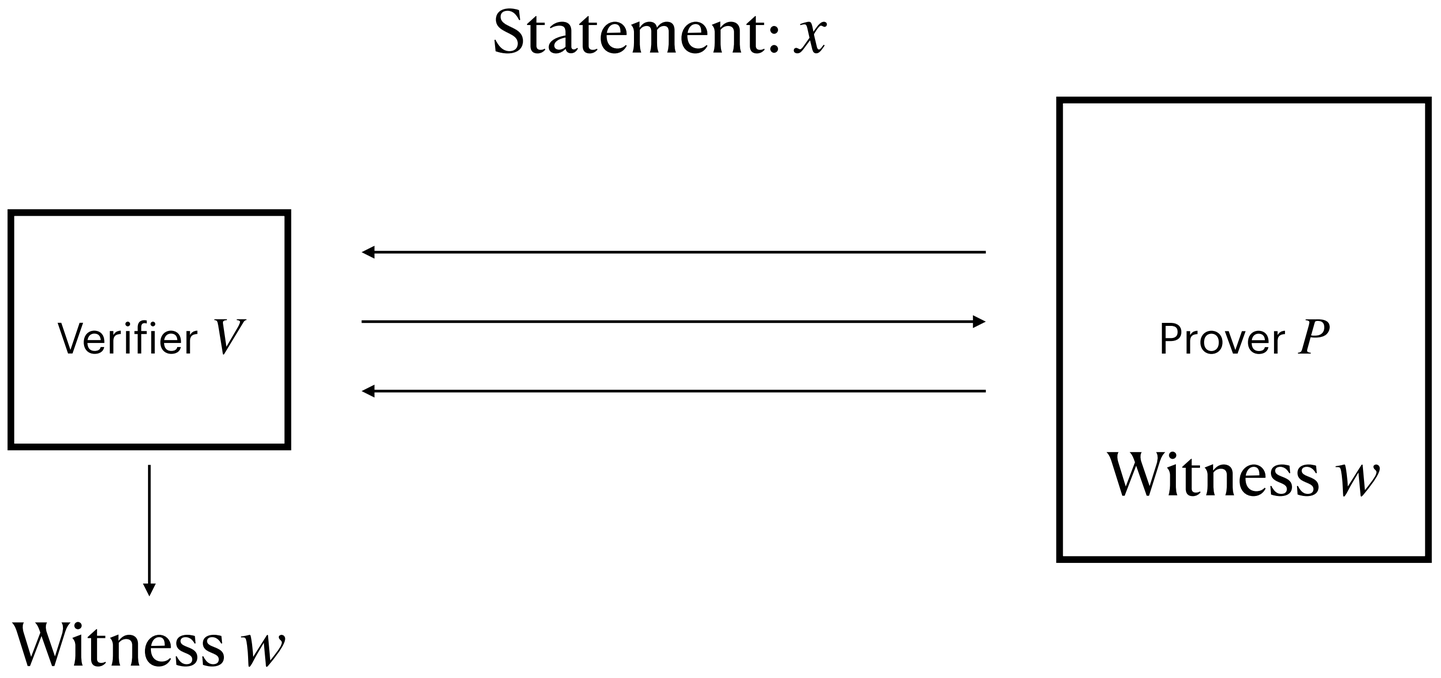
How to formally define?

An Attempt



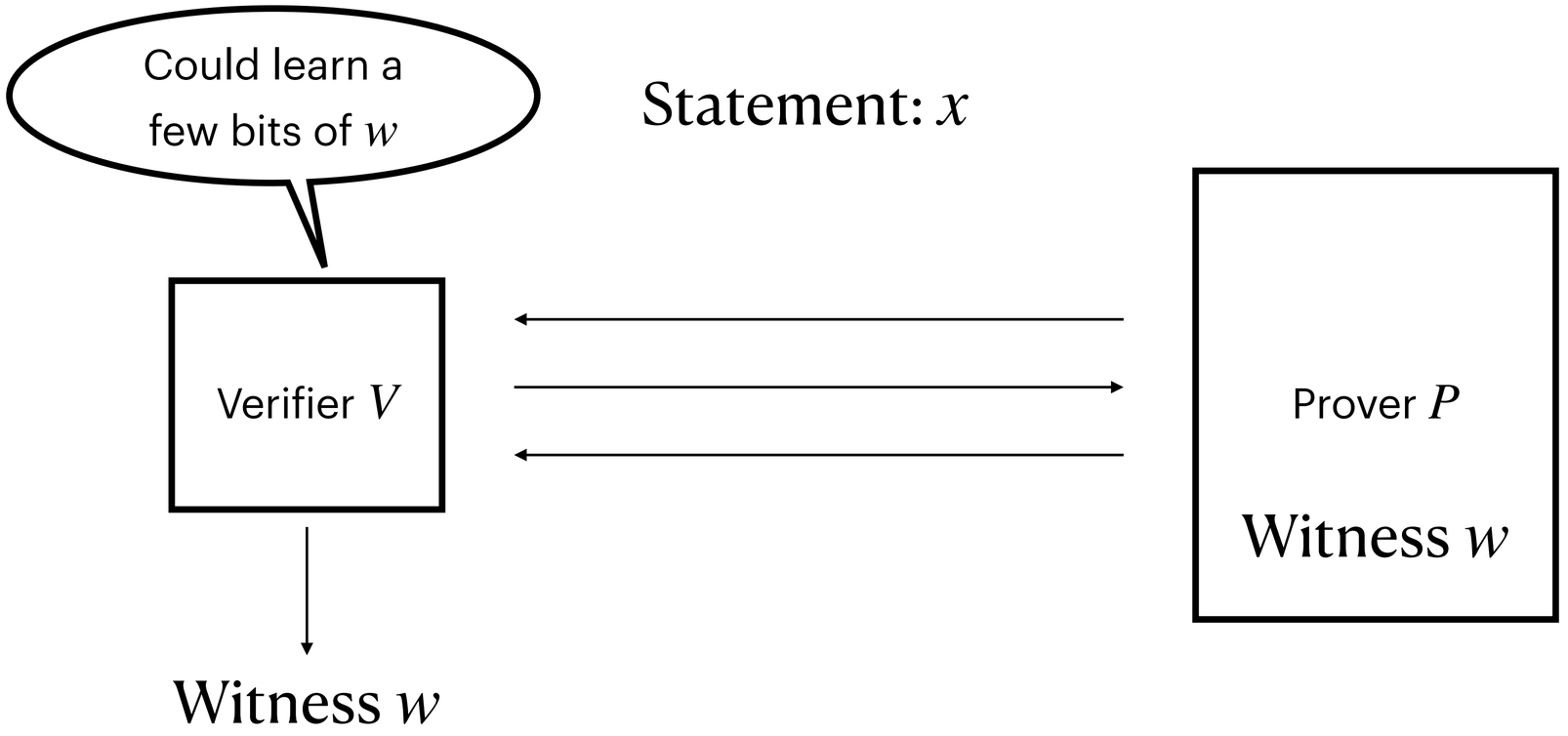
How to formally define?

An Attempt



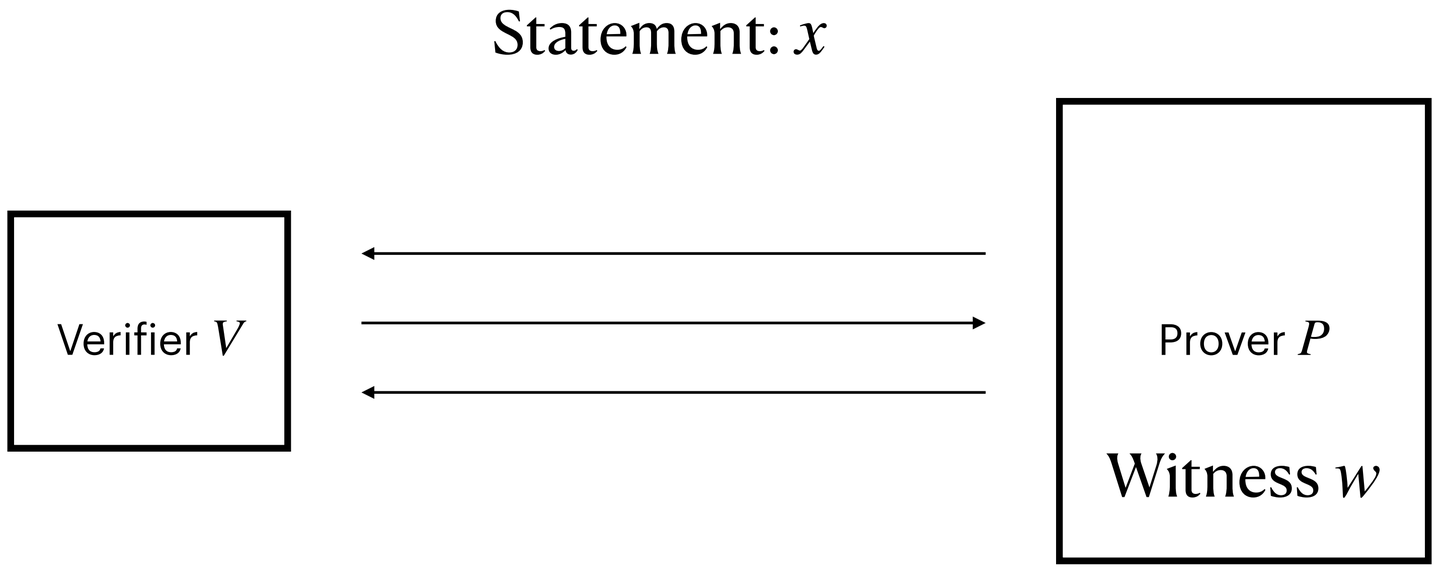
How to formally define?

An Attempt



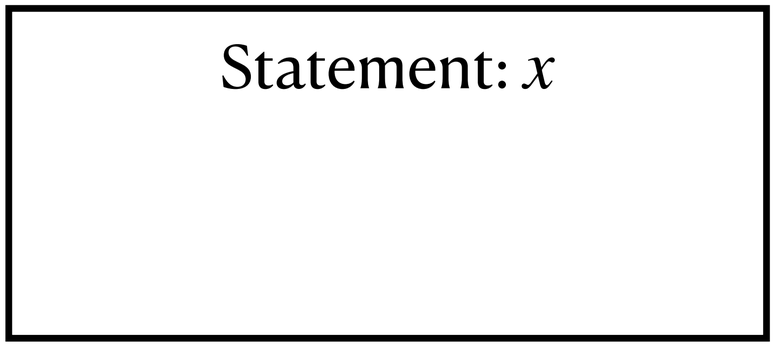
Formal Definition

Formal Definition

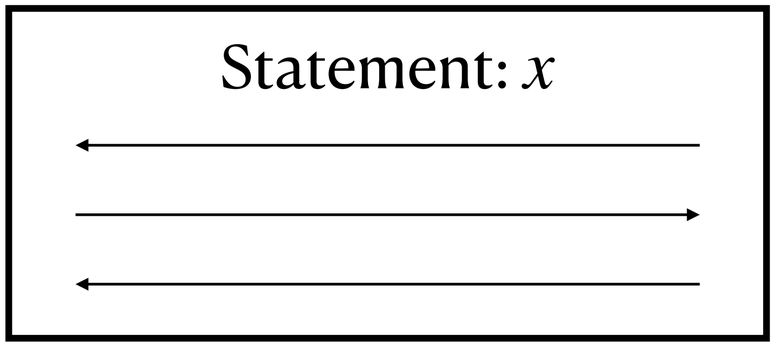


Formal Definition

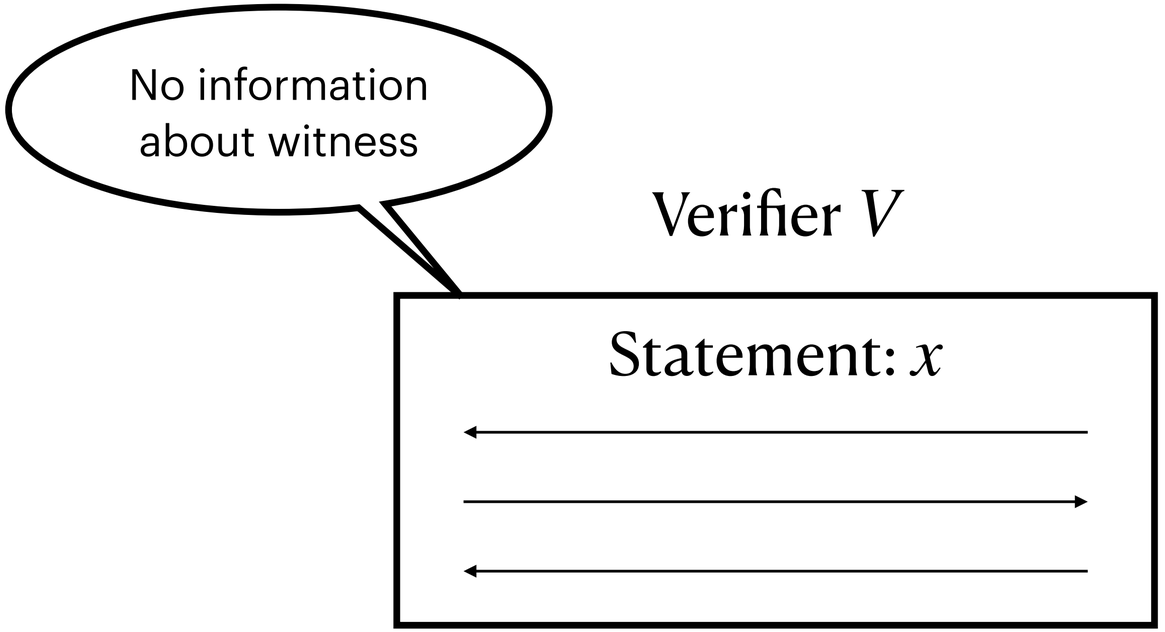
Formal Definition



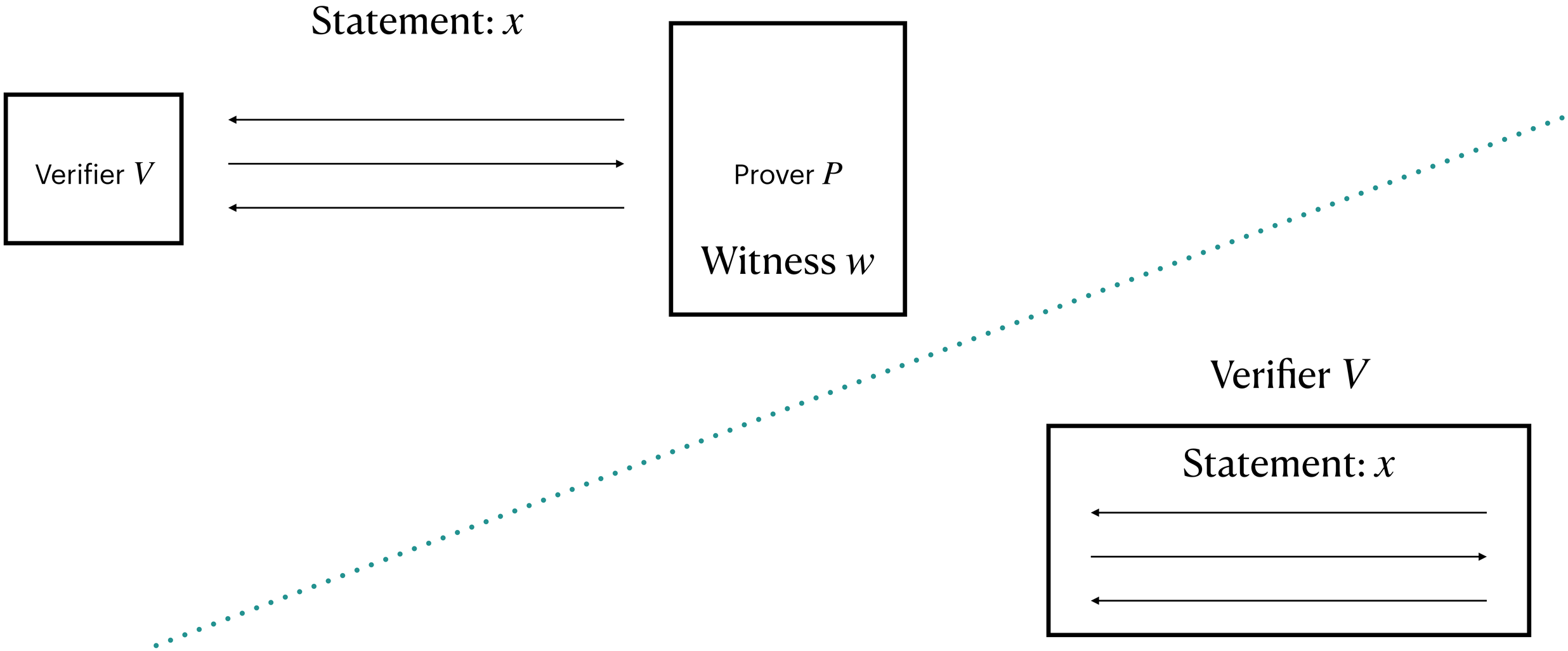
Formal Definition



Formal Definition

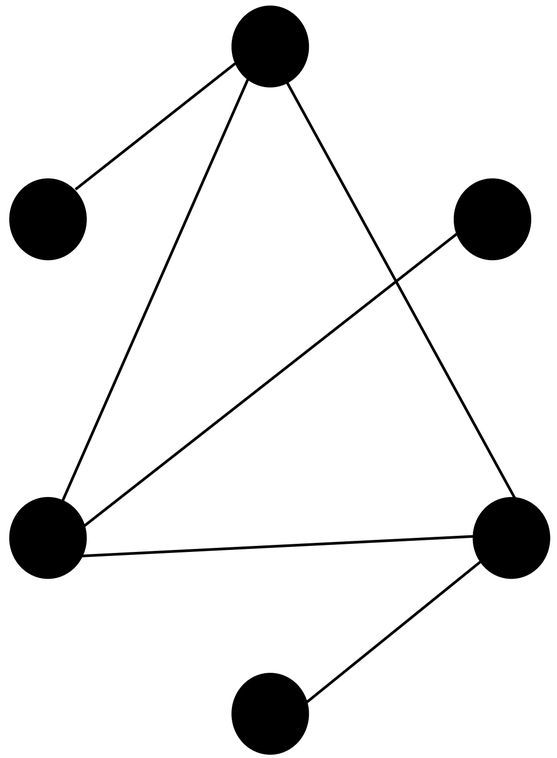


Formal Definition

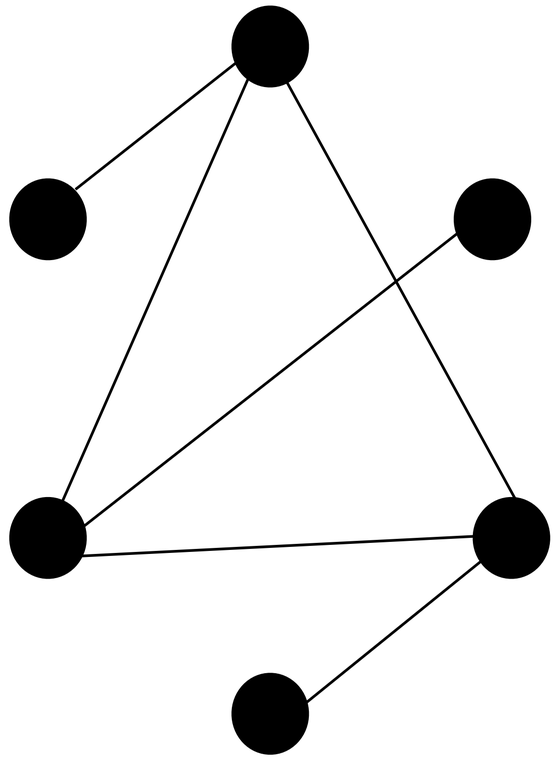


3-Colorability

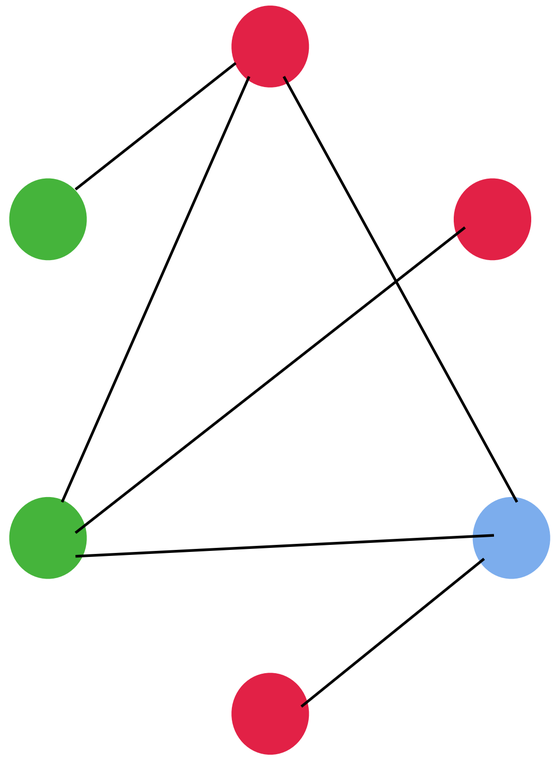
3-Colorability



3-Colorability

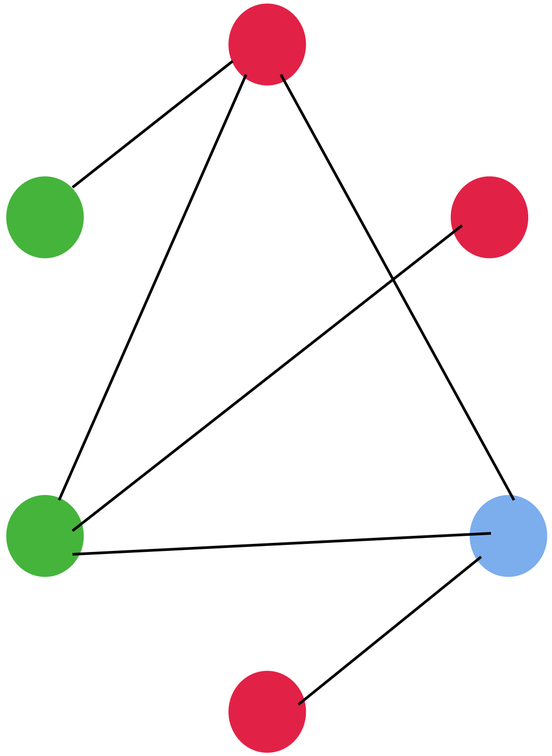


3-Colorability



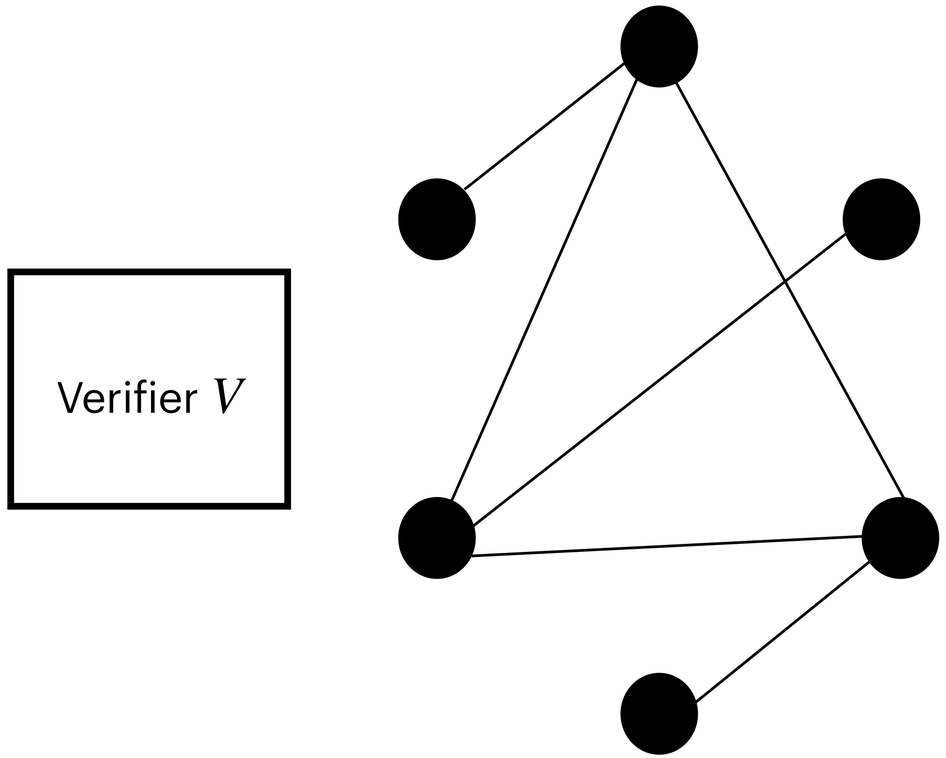
3-Colorability

3-colorability is NP-complete

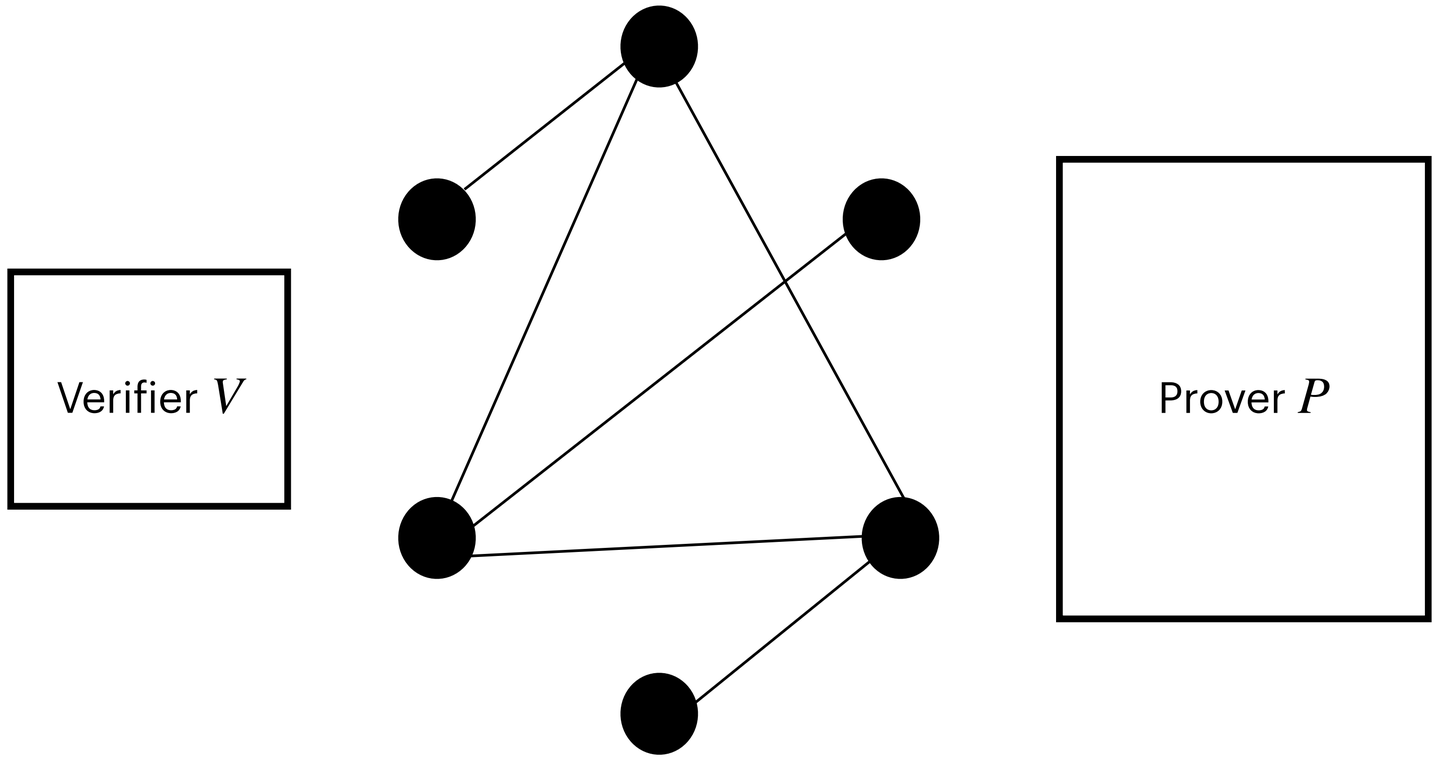


Zero-knowledge proof for NP

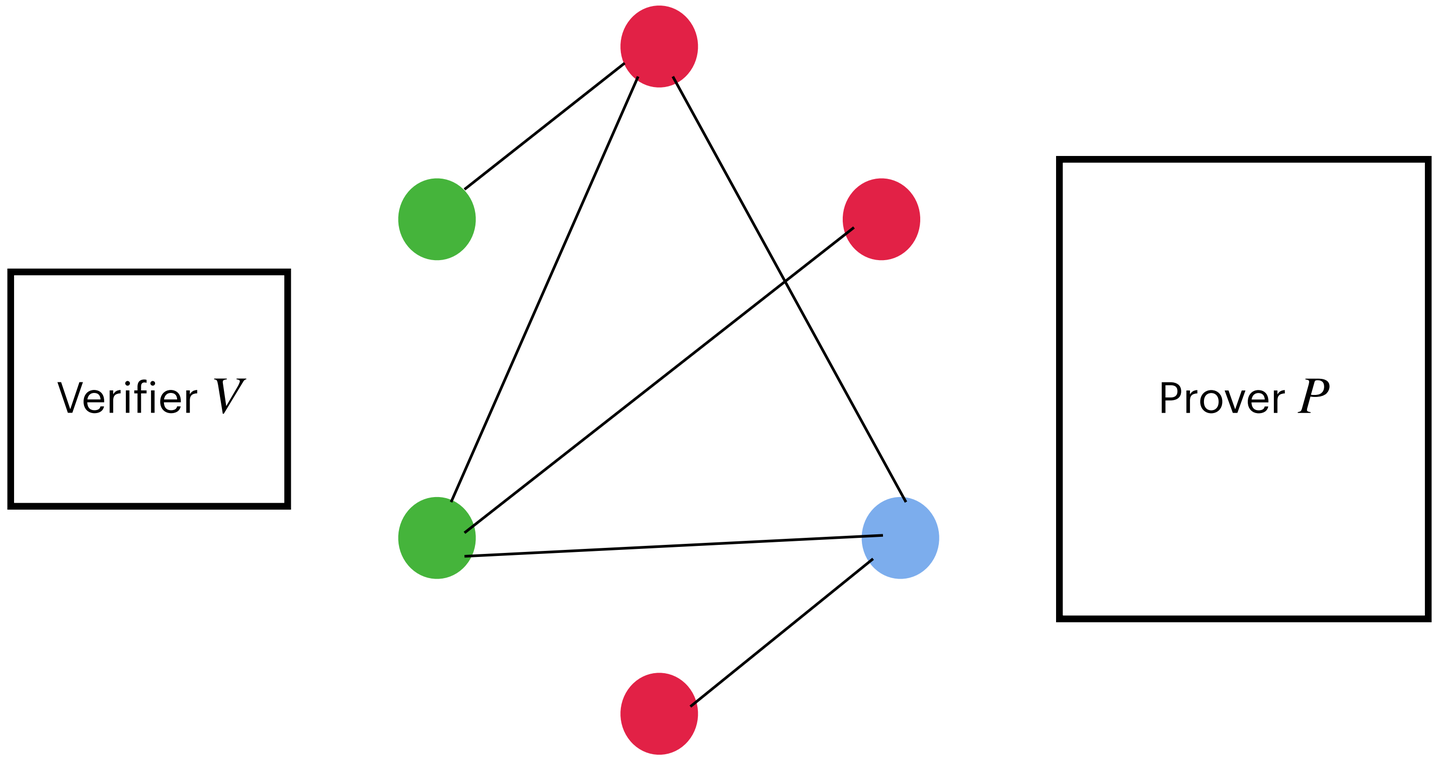
Zero-knowledge proof for NP



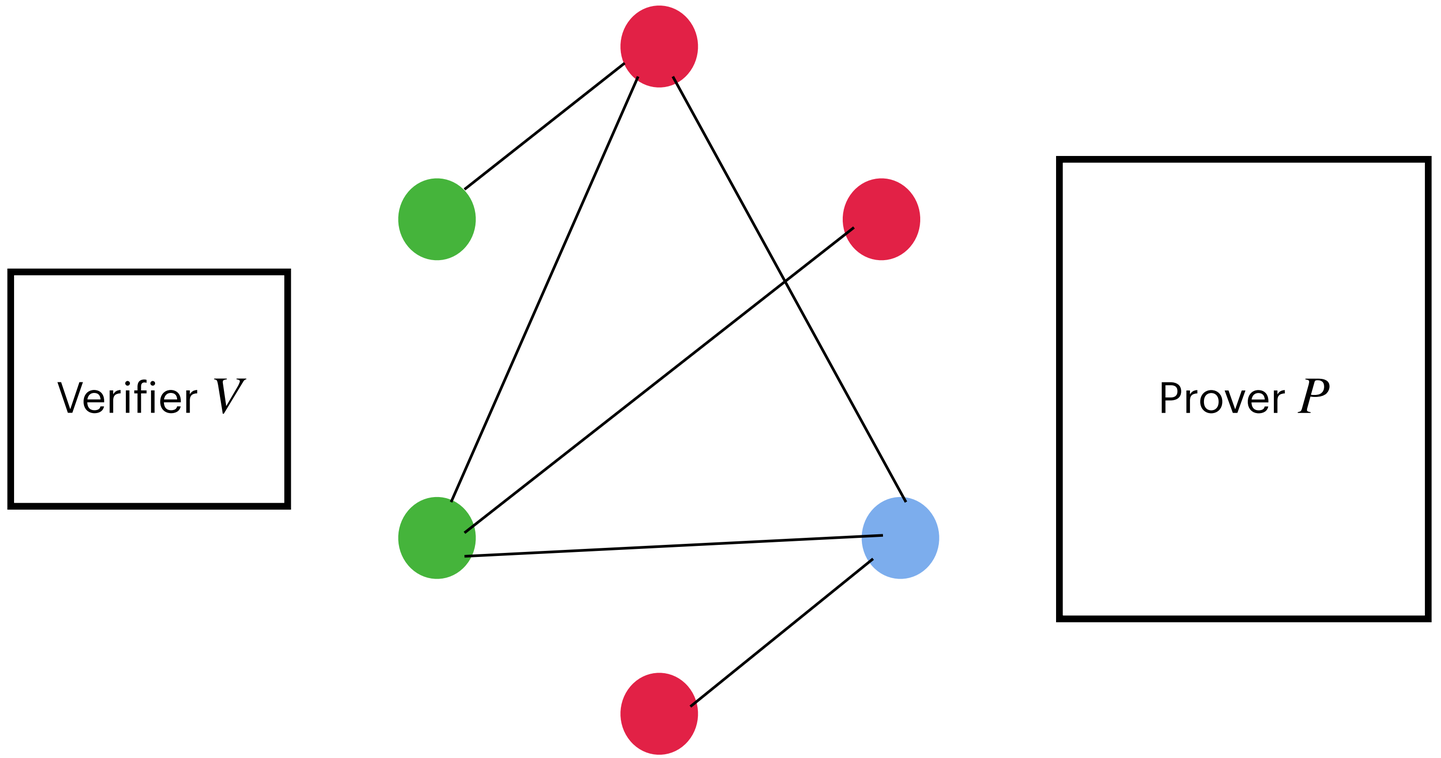
Zero-knowledge proof for NP



Zero-knowledge proof for NP

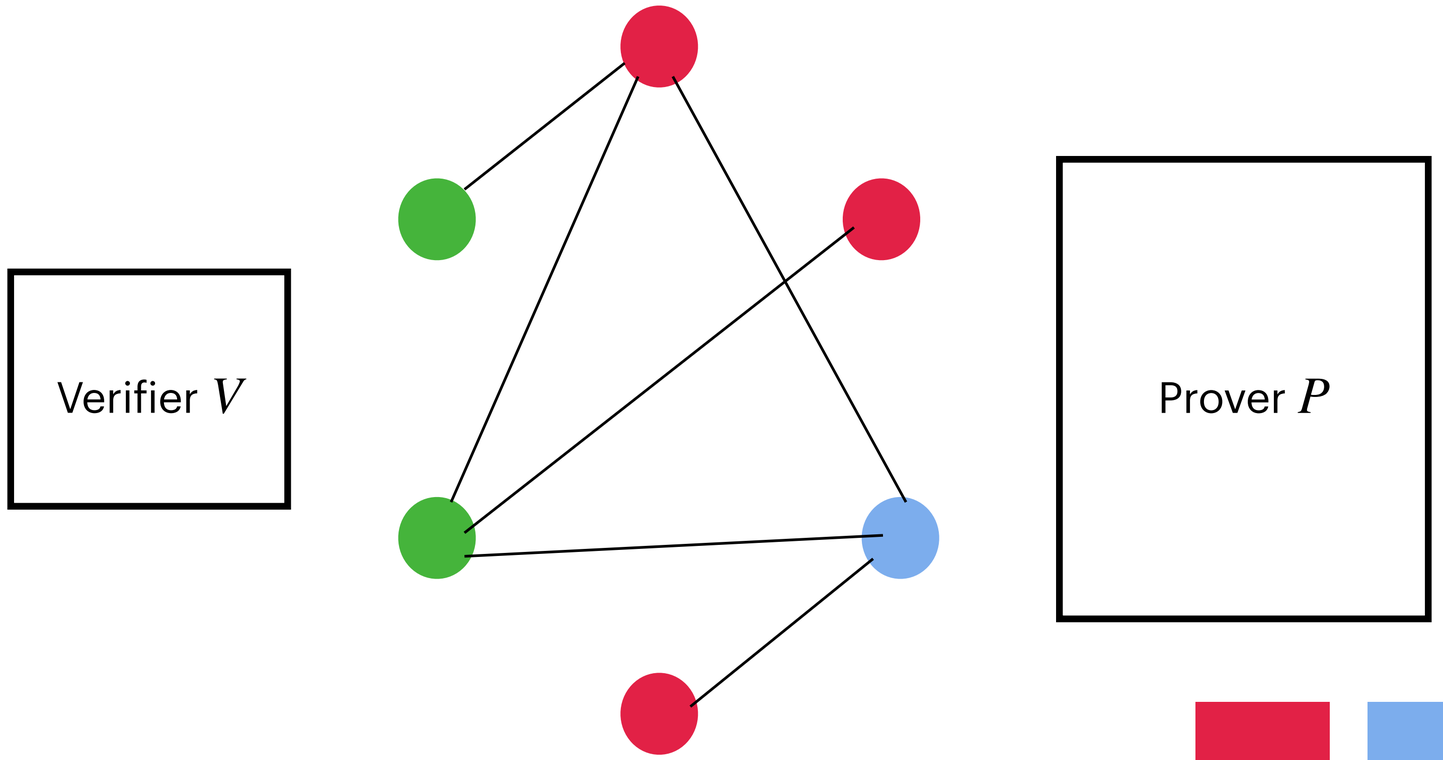


Zero-knowledge proof for NP

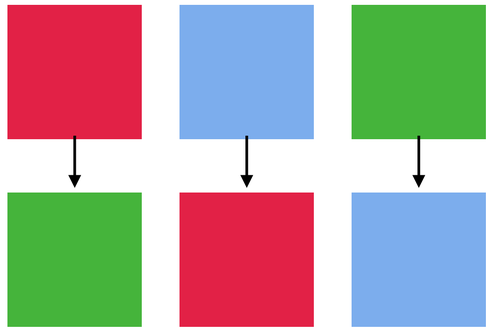


Step-1: Prover chooses a random permutation of the colors.

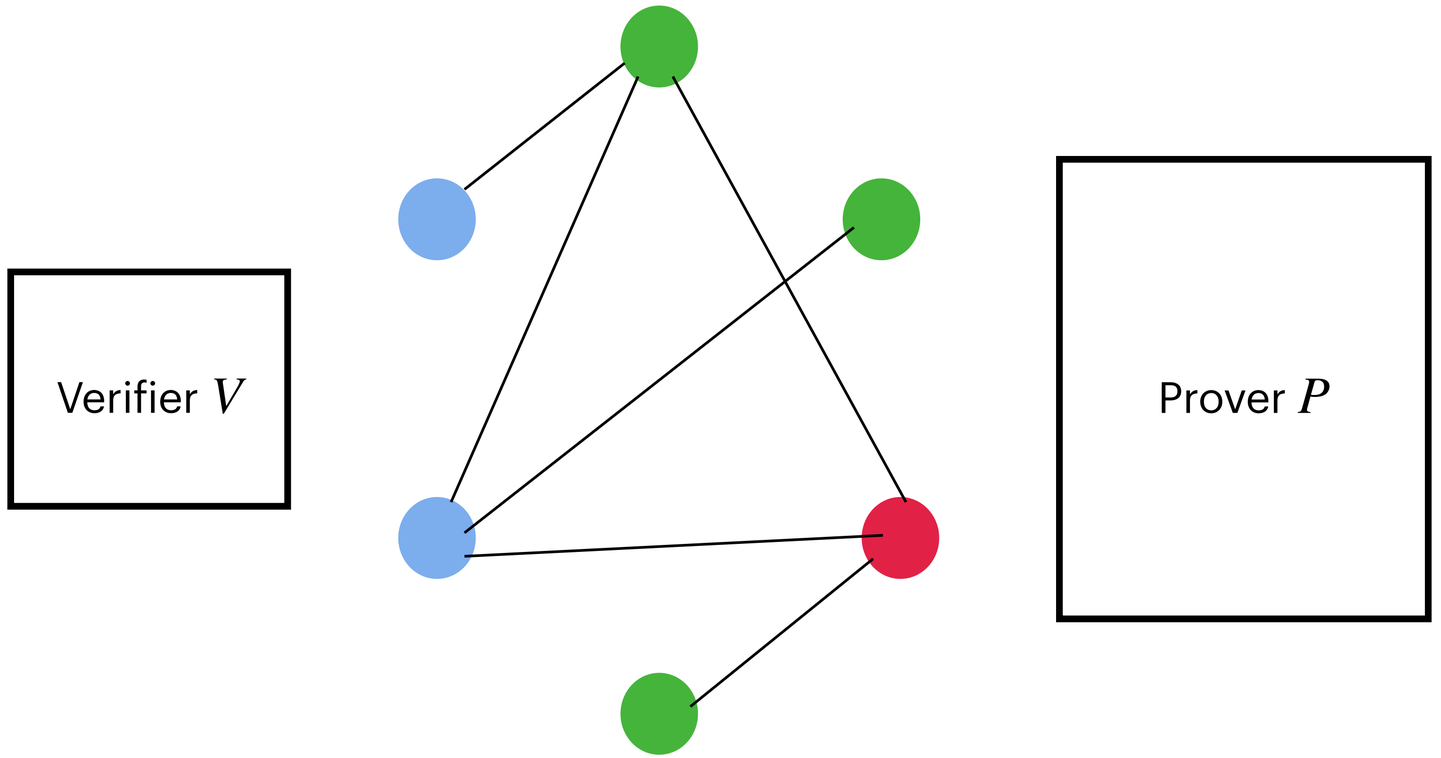
Zero-knowledge proof for NP



Step-1: Prover chooses a random permutation of the colors.

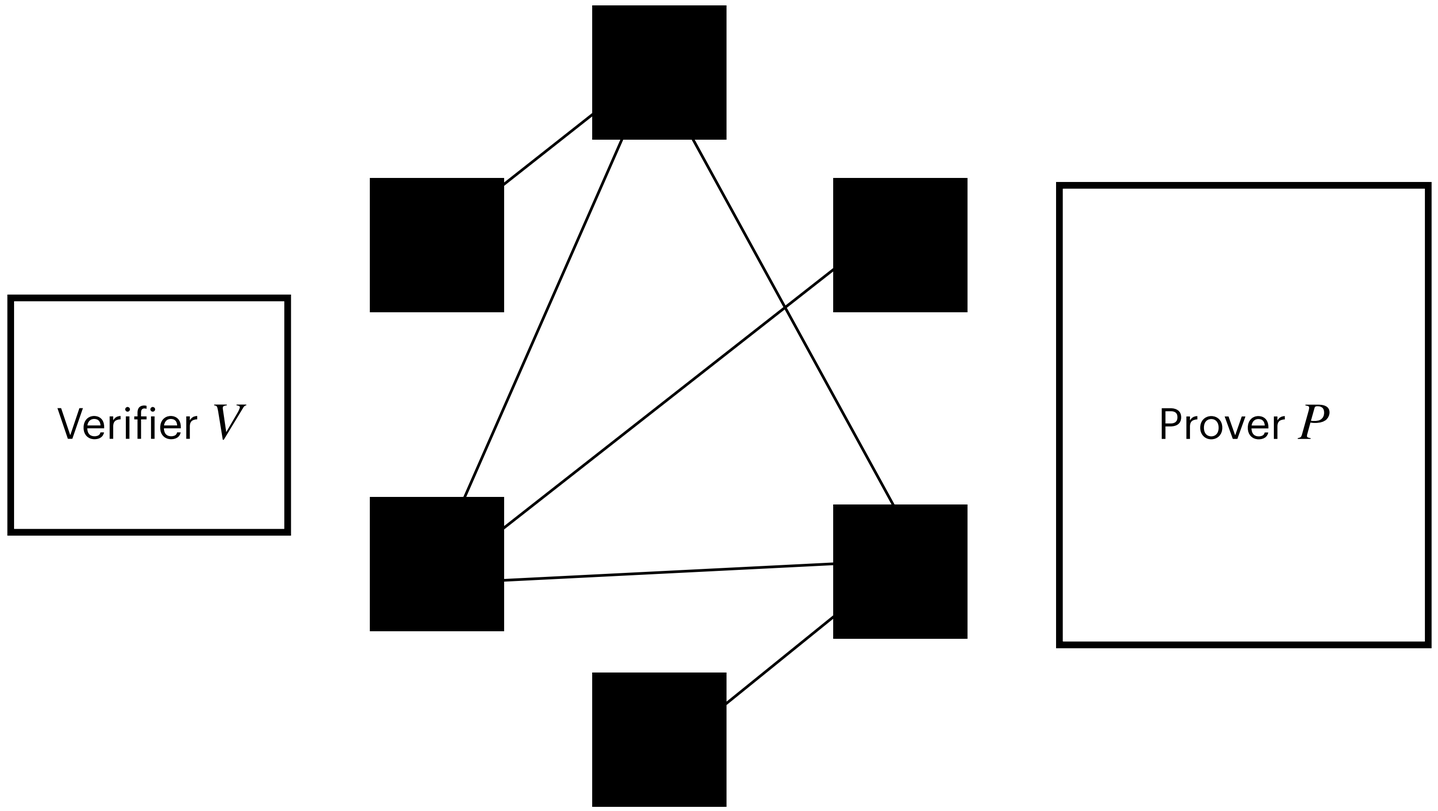


Zero-knowledge proof for NP



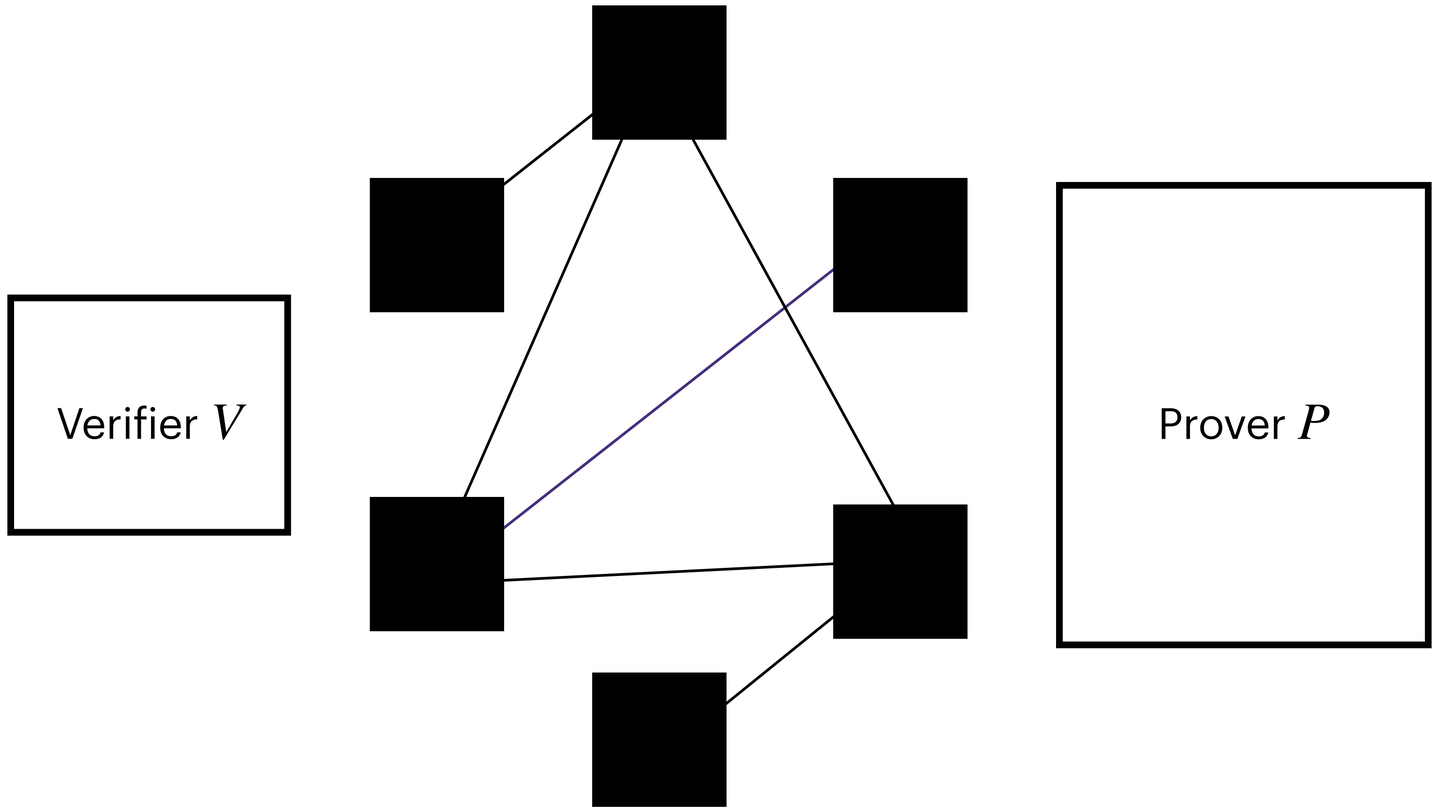
Step-1: Prover chooses a random permutation of the colors.

Zero-knowledge proof for NP



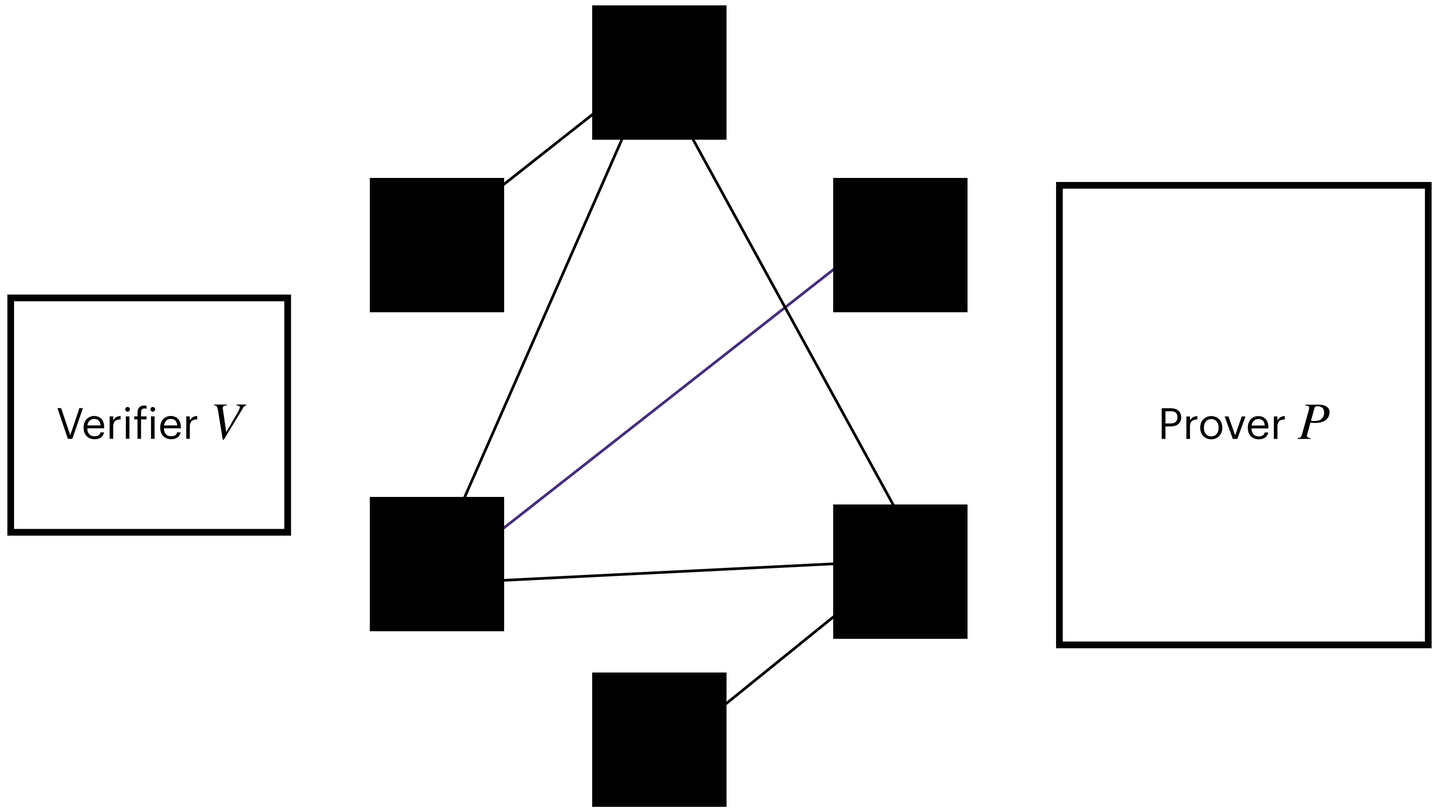
Step-2: Prover places each color behind a black-box

Zero-knowledge proof for NP



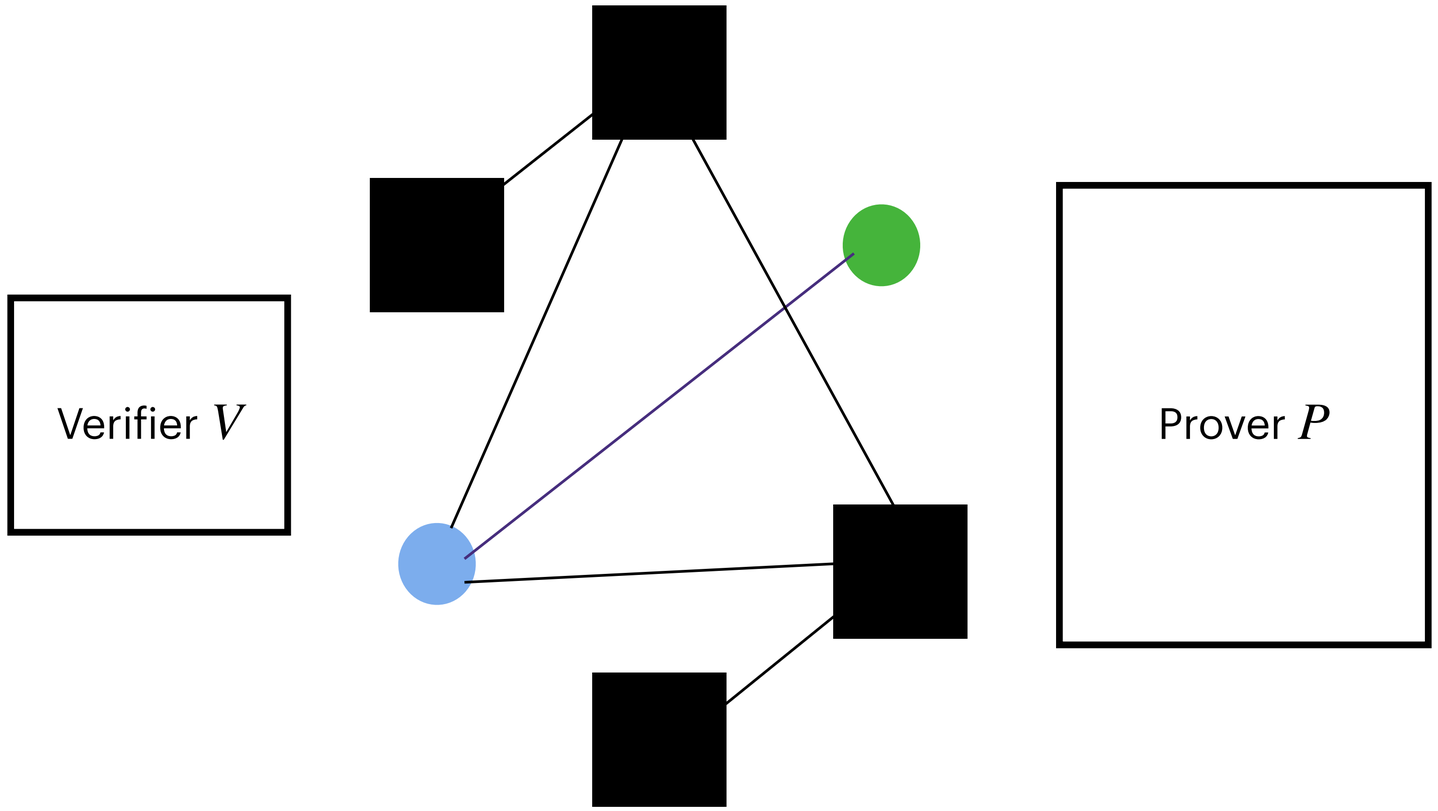
Step-3: Verifier chooses a random edge

Zero-knowledge proof for NP



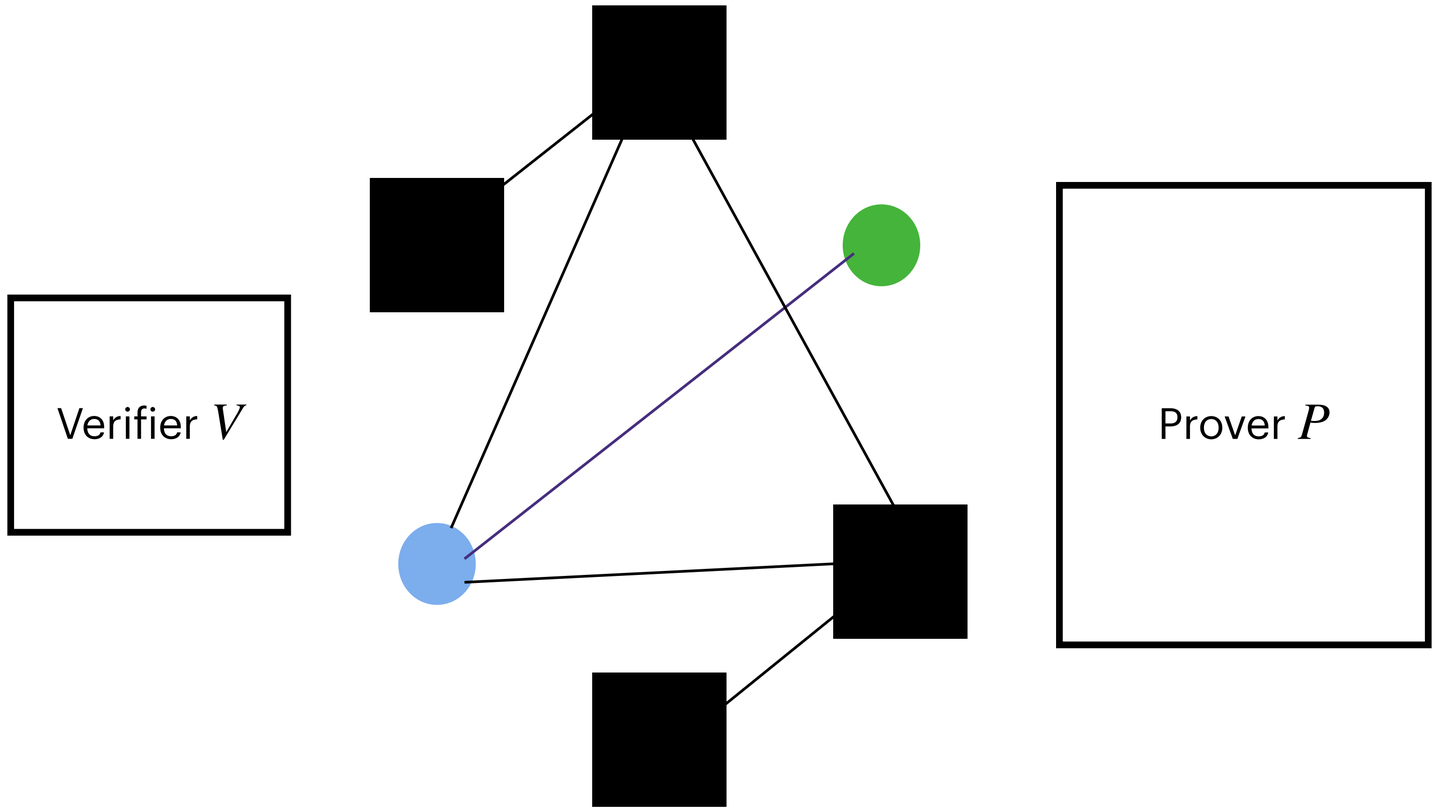
Step-3: Verifier chooses a random edge

Zero-knowledge proof for NP



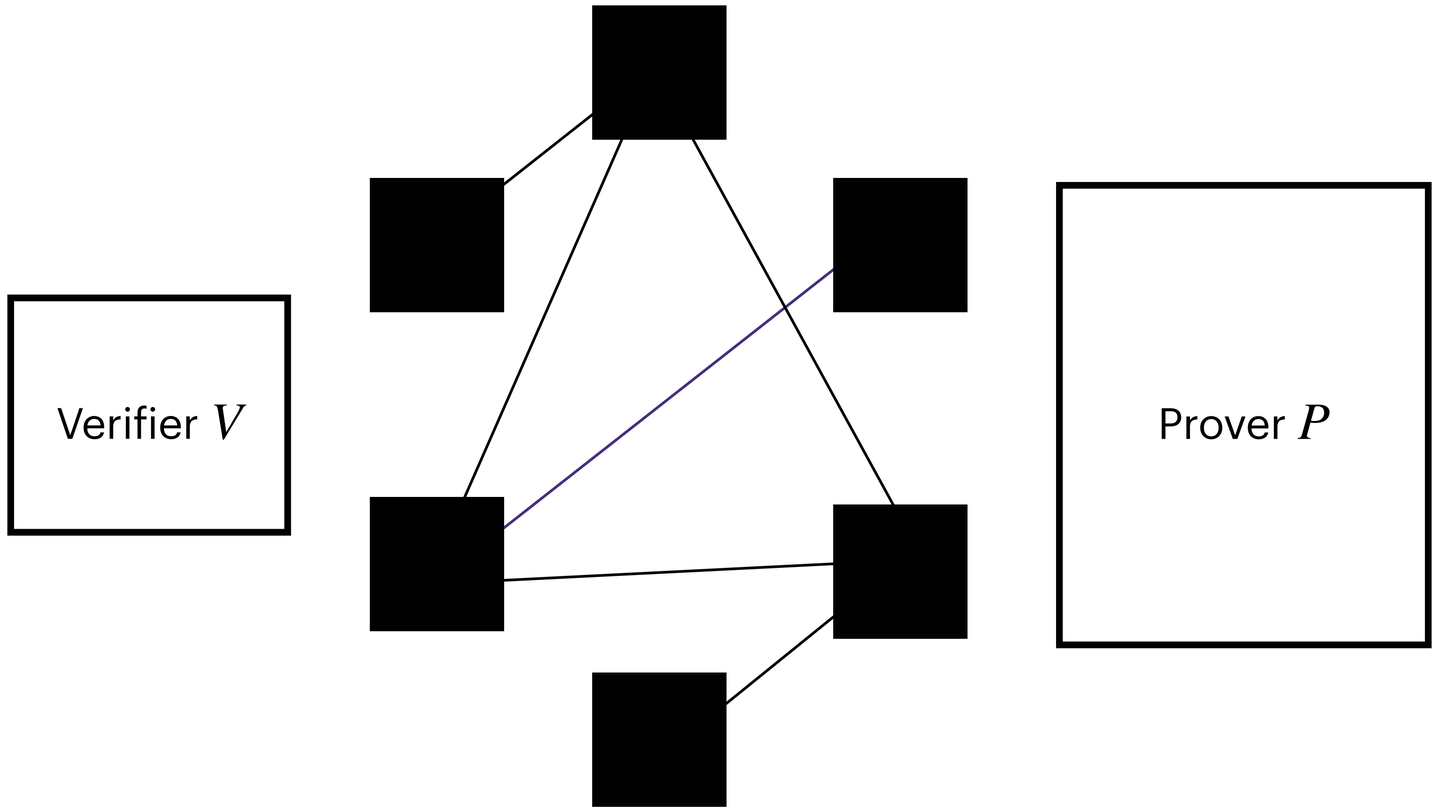
Step-4: Prover opens the colors on the endpoints of this edge.

Zero-knowledge proof for NP



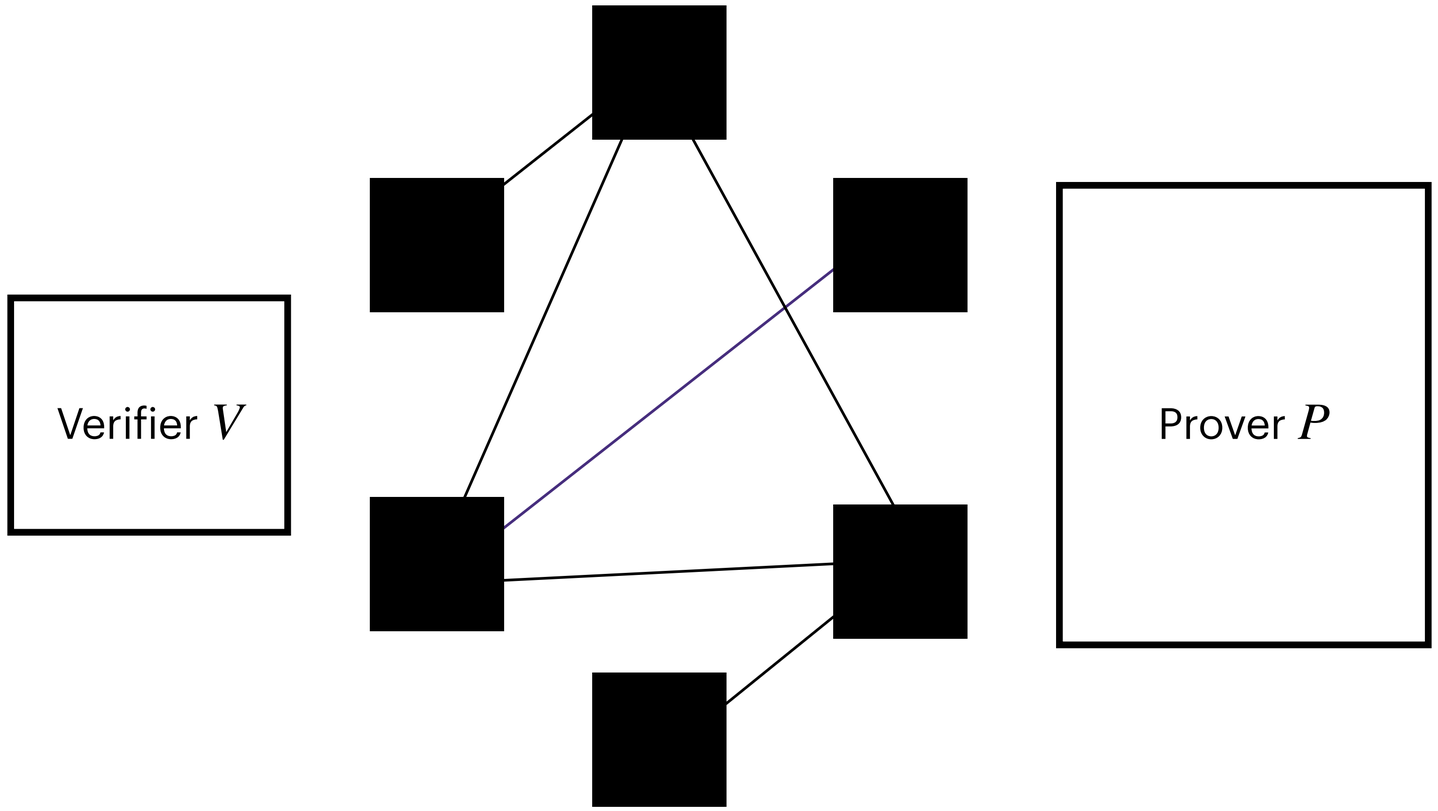
Step-5: Verifier checks if the endpoints are colored differently.

Completeness



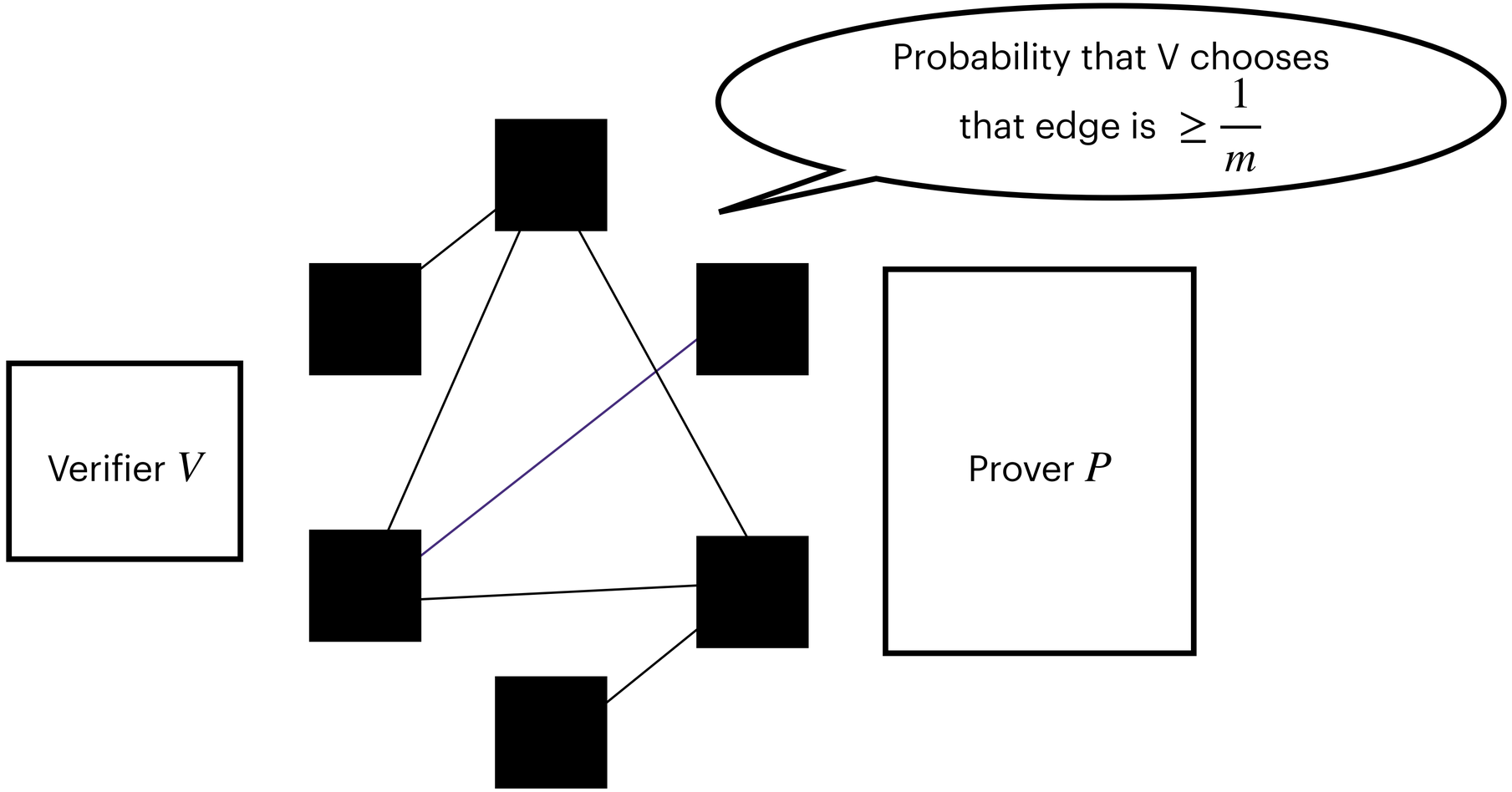
If the graph is 3-colorable, then the verifier always accepts.

Soundness



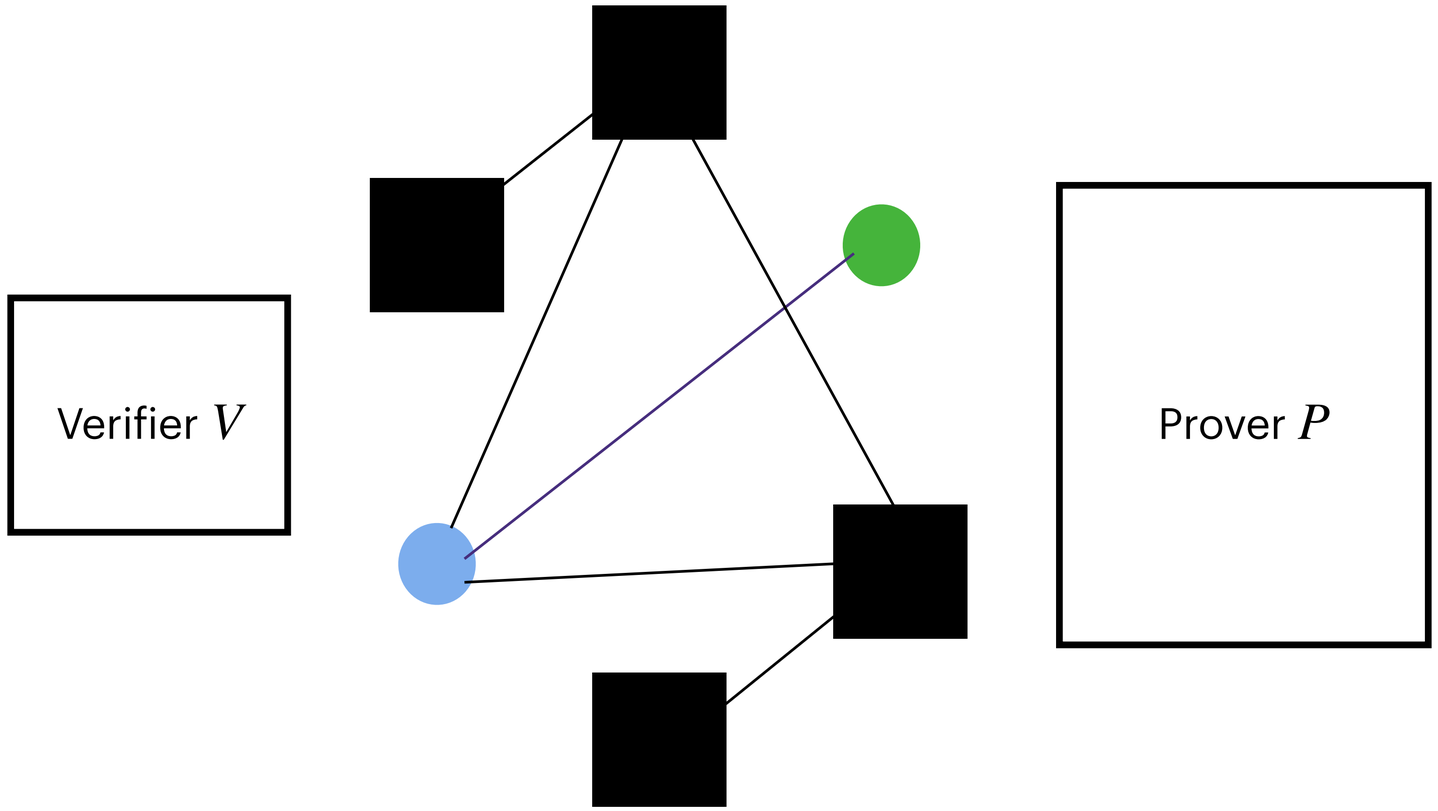
If the graph is not 3-colorable, then there exists at least one edge that has both endpoints colored using the same color.

Soundness



If the graph is not 3-colorable, then there exists at least one edge that has both endpoints colored using the same color.

Zero-Knowledge



Zero-Knowledge