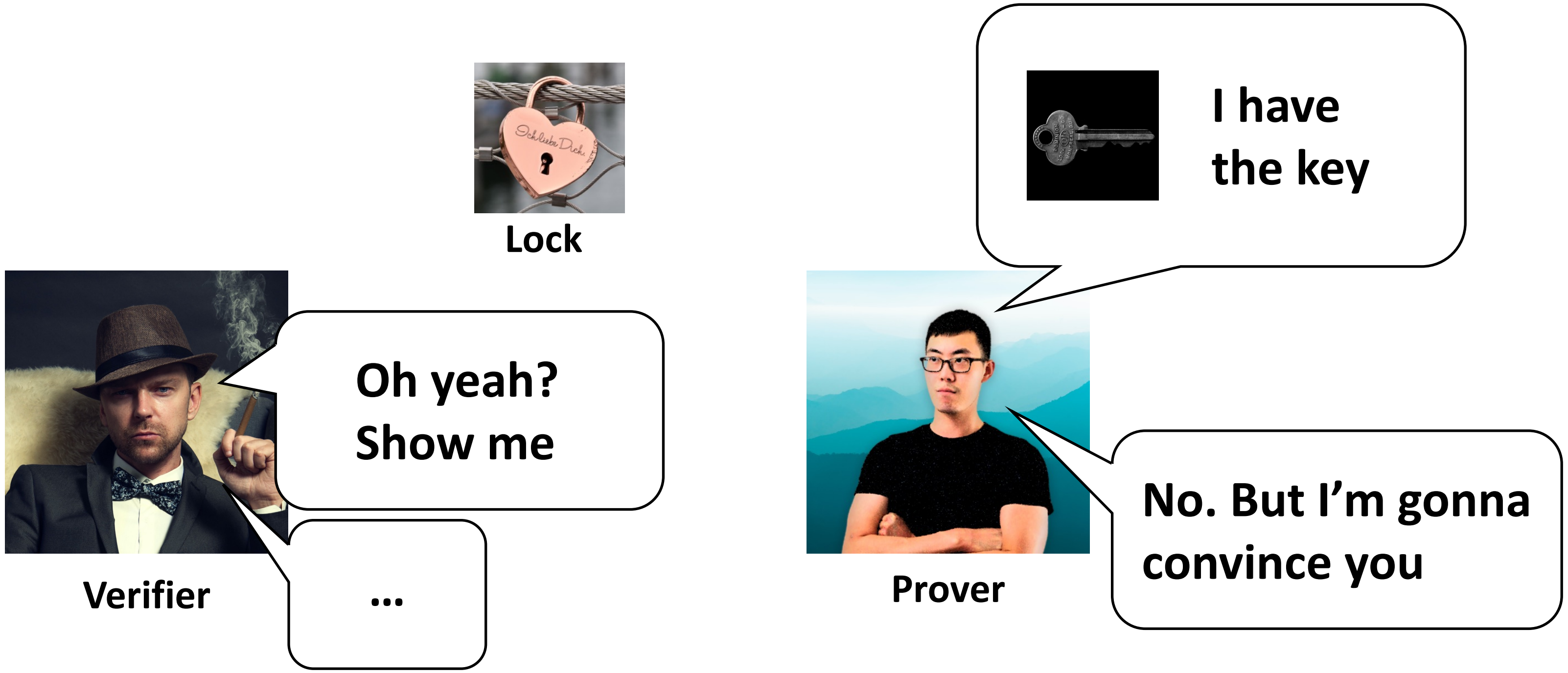
Objective of ZKP

Prove to someone (*the verifier*) that I (*the prover*) have a piece of information that satisfies a criteria without showing them the information.

~~Wikipedia: Prove to someone (*the verifier*) that a given statement is true without revealing any additional information apart from the fact that the statement is indeed true.~~

Example Objective



Lock

I have the key

Oh yeah? Show me

No. But I’m gonna convince you

…

Verifier

Prover

Motivation

Inglourious Basterds, directed by Quentin Tarantino (United States: The Weinstein Company, 2009).

Special Attention to:

1. The setup
2. Interactions

Methodology

How did Maj. Helltrom figure out what's on the card?

1. He asked questions

2. Challenge questions that probe the nature, characteristics or function of the unobservable truth

3. Trail of challenge questions are arbitrarily designed

4. Counterparties in the game that reply with answers

5. The responding counterparty can see the truth

6. Requires a game setup and rules of questioning

7. Probabilistic confidence

Characteristics of ZK

1. Will require *a setup* and rules of interaction.

2. Needs to throw *challenges* to probe the truth (not observable to verifier).

3. The challenge questions probe the feature, capacity, function, unique characteristics of the unobservable truth.

4. Verification succeeds when verifier is sufficiently convinced with a response prover gives. *Acceptance condition*.

5. Will always have an element of uncertainty. *100% certain conclusion is not possible*.