Zero-knowledge proof demo

Lionel, Soteris, Shannon, and Perry

Source: Wikipedia http://en.wikipedia.org/wiki/Zero_knowledge_proof

Zero-knowledge proof

- method by which a prover can prove to a verifier that a given statement is true, without any additional information beyond the fact that the statement is true

Zero-knowledge proof

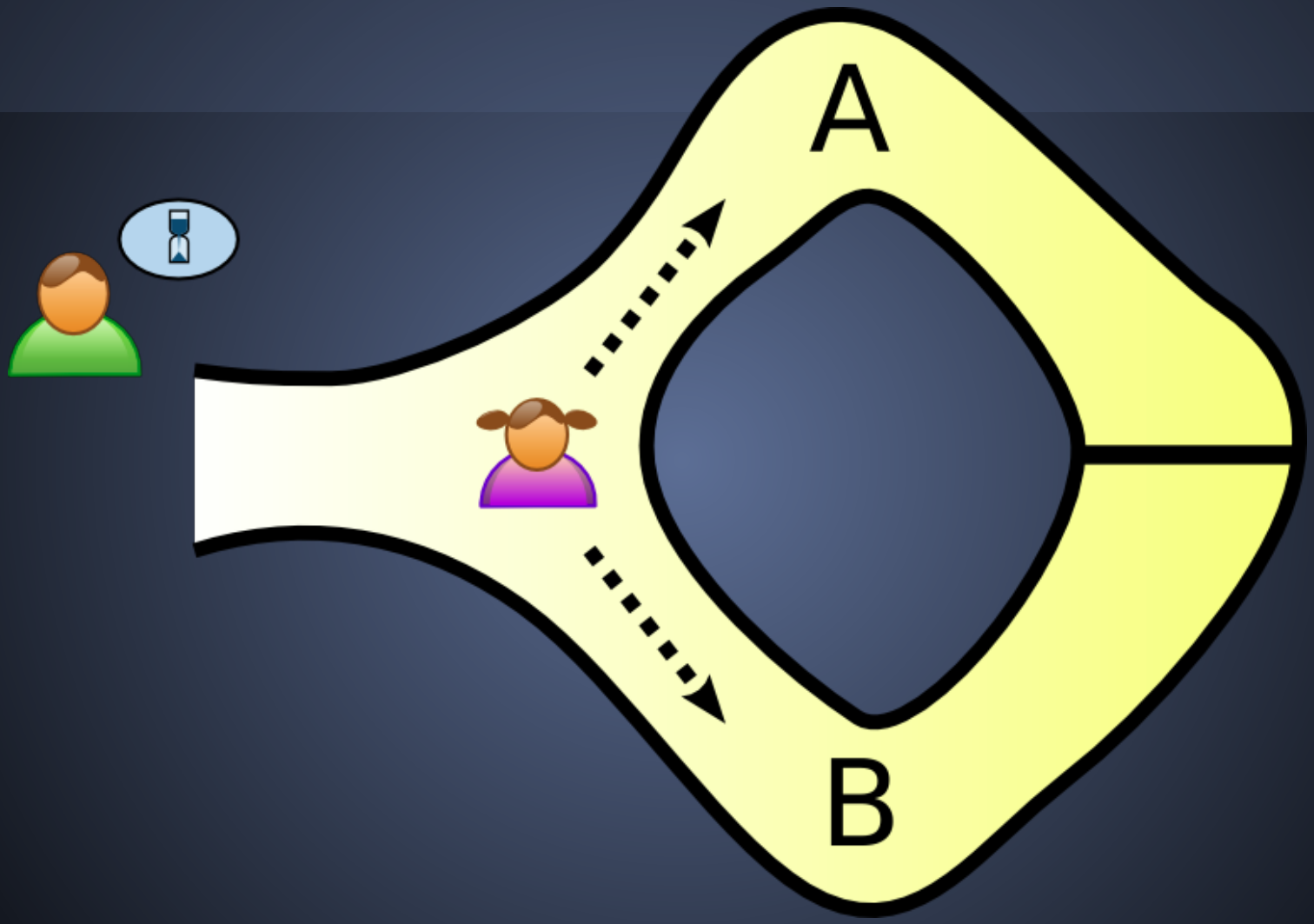
- For cases where the ability to prove the statement requires some secret information on the part of the prover, the definition implies that the verifier will not be able to prove the statement to anyone else

Demo

2 volunteers: named Peggy and Victor

Demo

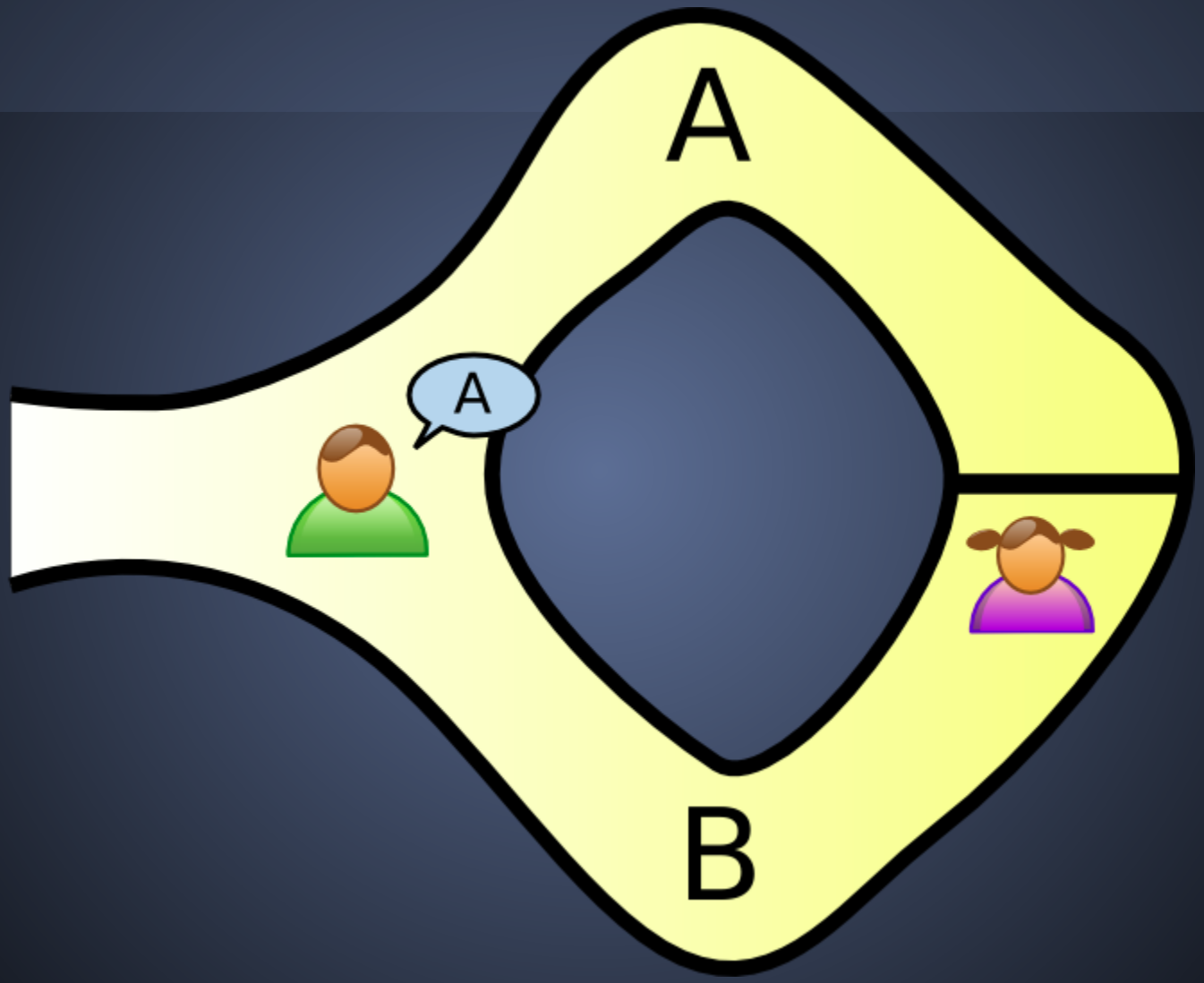
- Peggy has knowledge of the secret word of a magic door in a cave and Victor wants proof of this.
- Peggy wants to prove this in a way such that it cannot be proved to others.


A
B

Demo

- First, Victor waits outside while Peggy enters the cave. Peggy takes a path (either A or B) and Victor has no knowledge of which path she took.

- Victor then enters the cave and shouts either "A" or "B", chosen at random. This is the path that Peggy should return from.


A
A
B

Demo

- Provided that Peggy knows the magic word, she can reliably open the door and return from the desired path.

- If she cannot, then she will have only a 50% chance of guessing correctly.

- If Peggy can do this repeatedly, then Victor can conclude that it is very probable that Peggy knows the magic word.

Demo

- However, even if Victor is wearing a hidden camera that records the whole transaction, the only thing the camera will record is Victor shouting "A!" and Peggy appearing at A; Victor shouting "B!" and Peggy appearing at B.
- A recording of this type would be trivial for any two people to fake.

Definition

A zero-knowledge proof must satisfy three properties:

Completeness: if the statement is true, the honest verifier (that is, one following the protocol properly) will be convinced of this fact by an honest prover.

Soundness: if the statement is false, no cheating prover can convince the honest verifier that it is true, except with some small probability.

Zero-knowledge: if the statement is true, no cheating verifier learns anything other than this fact.