Access Control and Privacy Policies (9)

Email: christian.urban at kcl.ac.uk
Office: S1.27 (1st floor Strand Building)
Slides: KEATS (also homework is there)

Checking Solutions

How can you check somebody's solution without revealing the solution?

Checking Solutions

How can you check somebody's solution without revealing the solution?

Alice and Bob solve crosswords. Alice knows the answer for 21D (folio) but doesn't want to tell Bob.

You use an English dictionary:

- folio

Checking Solutions

How can you check somebody's solution without revealing the solution?

Alice and Bob solve crosswords. Alice knows the answer for 21D (folio) but doesn't want to tell Bob.

You use an English dictionary:

- folio

  "an individual leaf of paper or parchment, either loose as one of a series or forming part of a bound volume, which is numbered on the recto or front side only."

Checking Solutions

How can you check somebody's solution without revealing the solution?

Alice and Bob solve crosswords. Alice knows the answer for 21D (folio) but doesn't want to tell Bob.

You use an English dictionary:

- folio $\xrightarrow{1}$ individual

  "a single human being as distinct from a group"

Checking Solutions

How can you check somebody's solution without revealing the solution?

Alice and Bob solve crosswords. Alice knows the answer for 21D (folio) but doesn't want to tell Bob.

You use an English dictionary:

- folio $\stackrel{1}{\longrightarrow}$ individual $\stackrel{2}{\longrightarrow}$ human

  "relating to or characteristic of humankind"

Checking Solutions

How can you check somebody's solution without revealing the solution?

Alice and Bob solve crosswords. Alice knows the answer for 21D (folio) but doesn't want to tell Bob.

You use an English dictionary:

- folio $\stackrel{1}{\rightarrow}$ individual $\stackrel{2}{\rightarrow}$ human $\stackrel{3}{\rightarrow}$ or ...

Checking Solutions

How can you check somebody's solution without revealing the solution?

Alice and Bob solve crosswords. Alice knows the answer for 21D (folio) but doesn't want to tell Bob.

You use an English dictionary:

- folio $\stackrel{1}{\rightarrow}$ individual $\stackrel{2}{\rightarrow}$ human $\stackrel{3}{\rightarrow}$ or ...

hash functions...but Bob can only check once he has also the solution

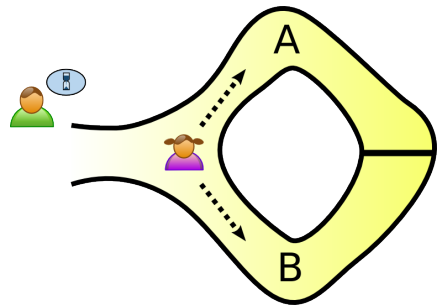
Zero-Knowledge Proofs

Two remarkable properties:

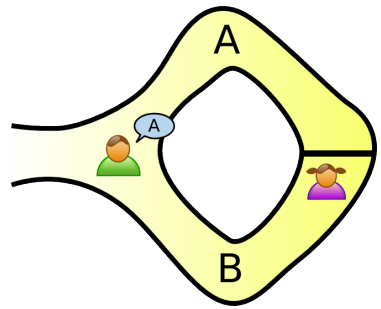
- Alice only reveals the fact that she knows a secret.
- Having been convinced, Bob cannot use the evidence in order to convince Carol.

The Idea

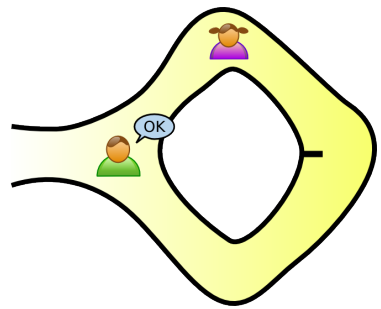
1.



2.

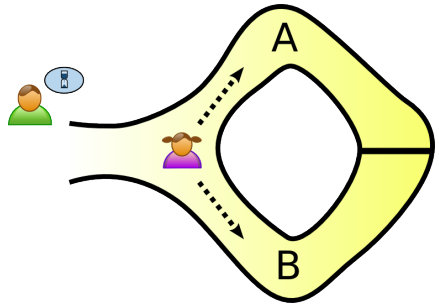


3.

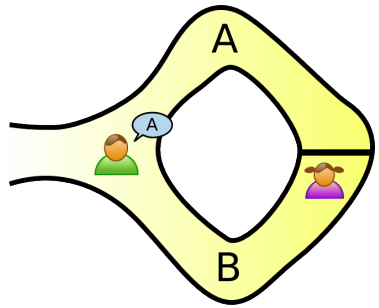


The Idea

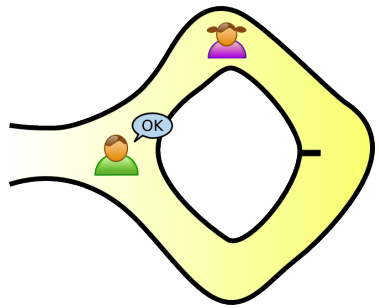
1.



2.



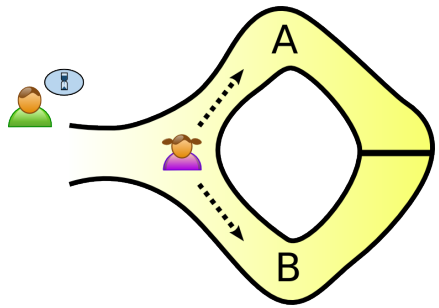
3.



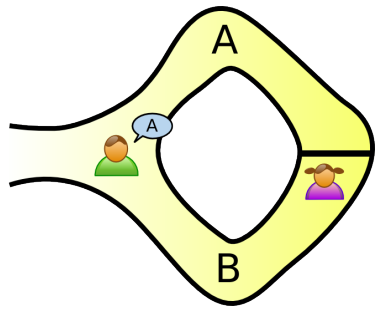
Even if Bob has a hidden camera, a recording will not be convincing to anyone else (Alice and Bob could have made it all up).

The Idea

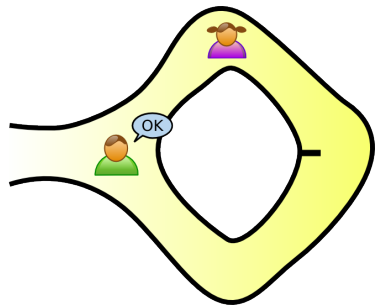
1.



2.

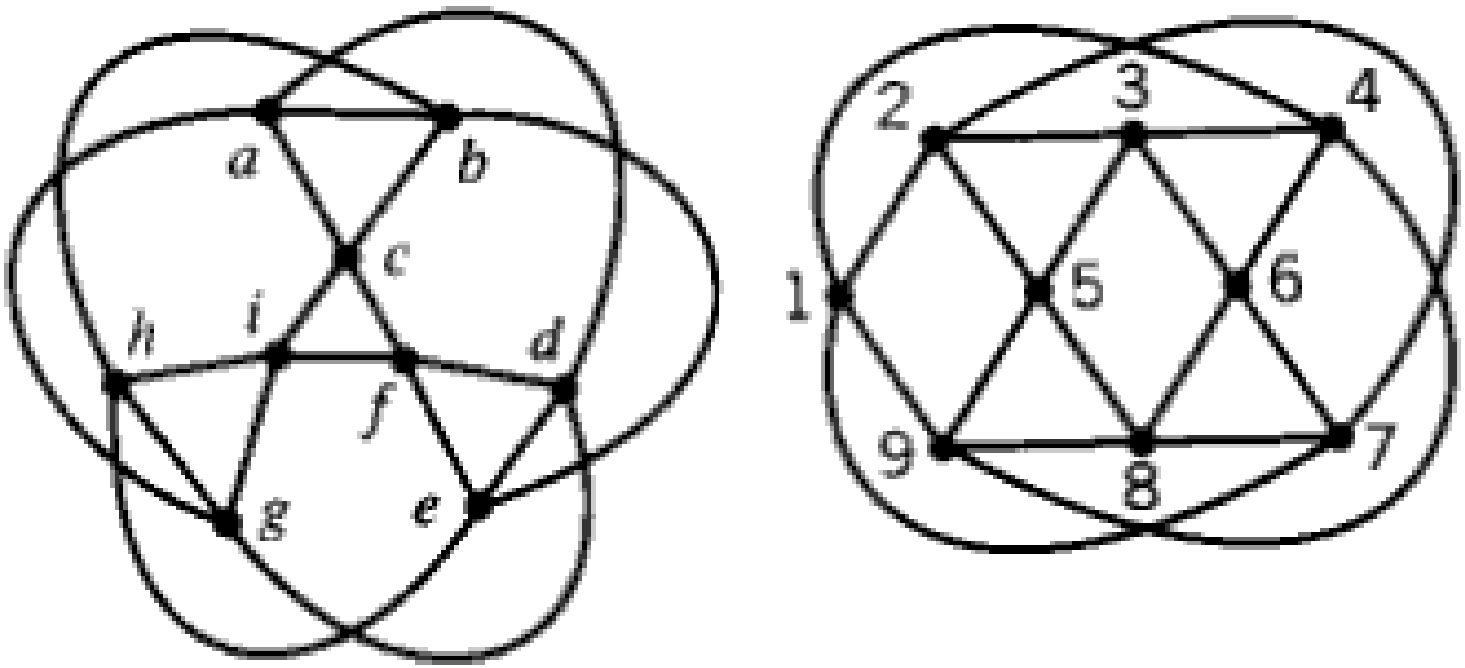


3.



Even worse, an observer present at the experiment would not be convinced.

Graph Isomorphism



Finding an isomorphism between two graphs is an NP complete problem.

Graph Isomorphism Protocol

Alice starts with knowing an isomorphism between graphs G_1 and G_2

1. Alice generates an isomorphic graph H which she sends to Bob
2. Bob asks either for an isomorphism between G_1 and H, or G_2 and H
3. Alice and Bob repeat this procedure n times

Graph Isomorphism Protocol

Alice starts with knowing an isomorphism between graphs G_1 and G_2

1. Alice generates an isomorphic graph H which she sends to Bob
2. Bob asks either for an isomorphism between G_1 and H, or G_2 and H
3. Alice and Bob repeat this procedure n times

these are called commitment algorithms

Non-Interactive ZKPs

This is amazing: Alison can publish some data that contains no data about her secret, but can be used to convince anyone of the secret's existence.

Problems of ZKPs

This is amazing: Alison can publish some data that contains no data about her secret, but can be used to convince anyone of the secret's existence.

Random Number Generators