Comment expliquer les preuves à divulgation nulle de connaissance à vos enfants ?

Pascal Lafourcade

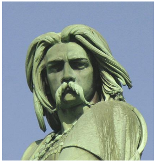
Chaire sur la Confiance Numérique

28 Mai 2014

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something without revealing any information

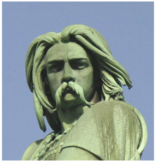


Verifier (V)

Idea of Zero Knowledge Proof

Prover (P)

(P) convinces (V) that it knows something without revealing any information



Verifier (V)

Applications:

- Authentication systems: prove its identity to someone using a password without reavealing anything about the secret.
- Prove that a praticipant behavior is correct according to the protocol (e.g. integrity of ballots in vote).
- Group signature, secure multiparty computation, e-cash ...

Outline

Motivation

Outline

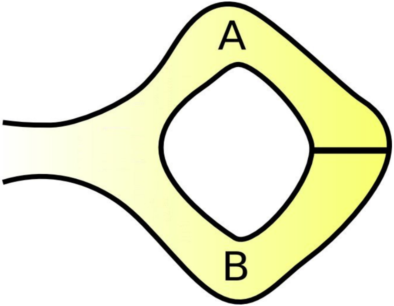
Outline

Outline

Outline

Outline

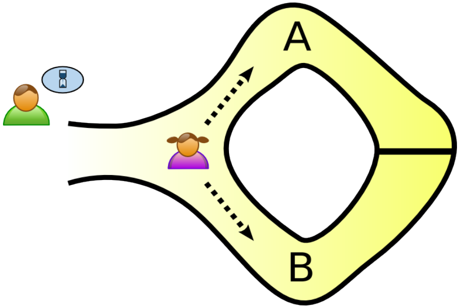
Cave example (0)



Door with a secret code

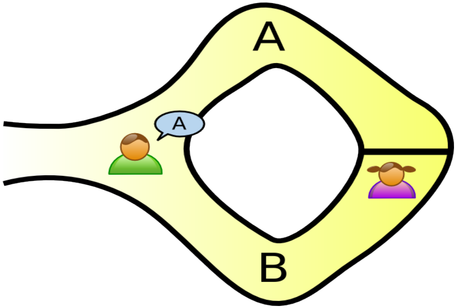
Cave example (I)

V waits outside while P chooses a path



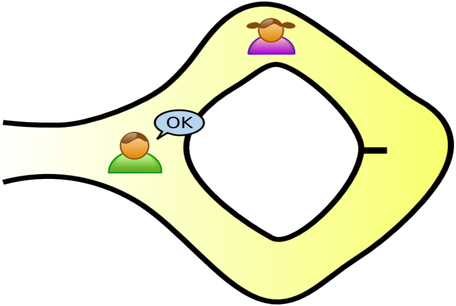
Cave example (II)

V enters and shouts the name of a path



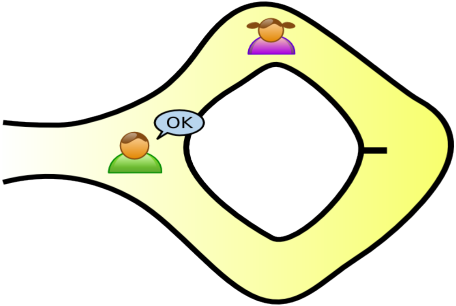
Cave example (III)

P returns along the desired path (using the secret if necessary)



Cave example (III)

P returns along the desired path (using the secret if necessary)

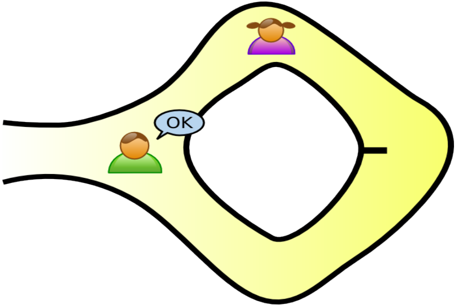


$A =$ "P does not know the secret" is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret" is equivalent to say "P is lucky"

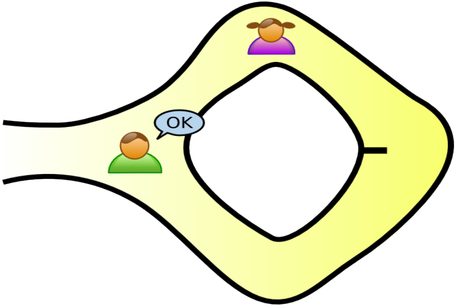
$$Pr[A] = \frac{1}{2}$$

After k tries,

$$Pr[A] = (\frac{1}{2})^k$$

Cave example (III)

P returns along the desired path (using the secret if necessary)



$A =$ "P does not know the secret" is equivalent to say "P is lucky"

$$Pr[A] = \frac{1}{2}$$

After k tries,

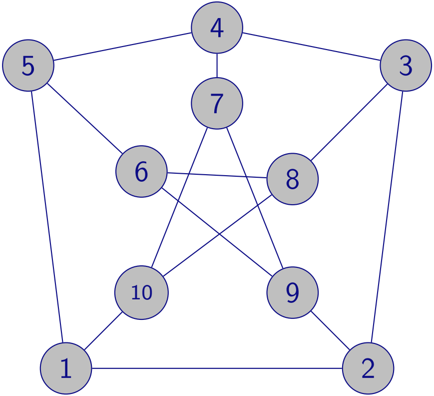
$$Pr[A] = (\frac{1}{2})^k$$

$\overline{A} =$ "P knows the secret", then

$$Pr[\overline{A}] = 1 - Pr[A] = 1 - (\frac{1}{2})^k$$

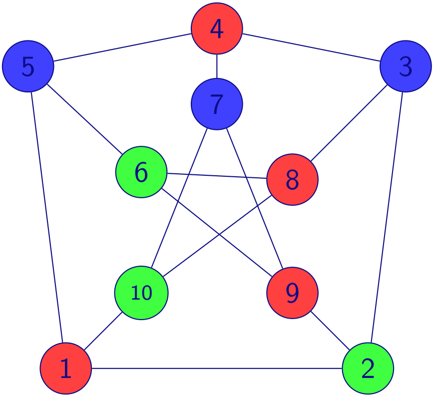
Outline

Graph 3-coloring is NP-complete:



Petersen graph

Graph 3-coloring is NP-complete:

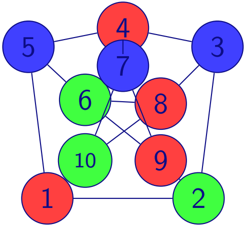


Petersen graph

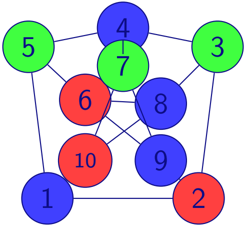
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($

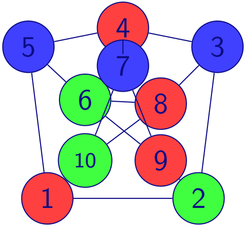


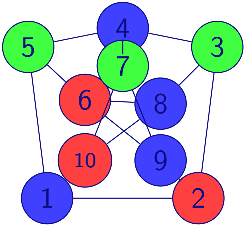
$)=$



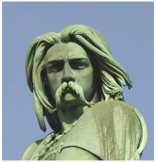
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

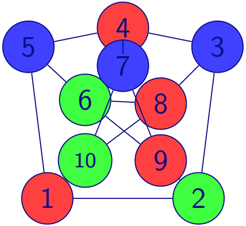
Chooses $\forall u \in V, r_u$



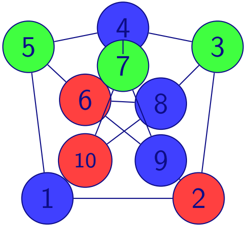
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

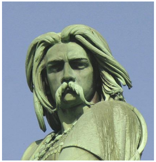
$\pi($



$)=$



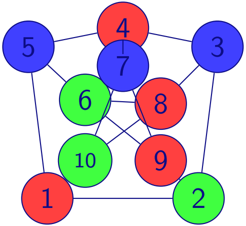
$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$

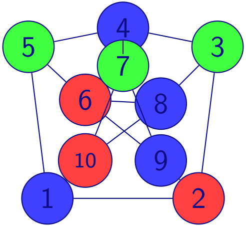


Chooses $\forall u \in V, r_u$

P wants to prove to V his 3-coloring of $G = (E, V)$

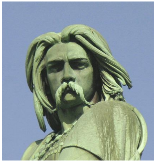
P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

Chooses $\forall u \in V, r_u$

$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$

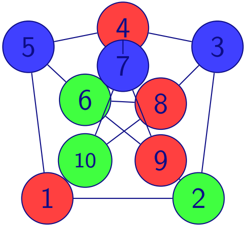


Chooses i and j

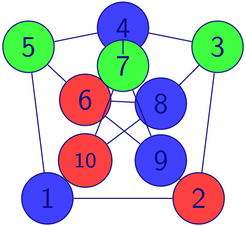
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

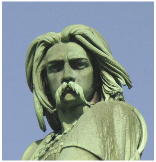
$\pi($



$)=$



$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$

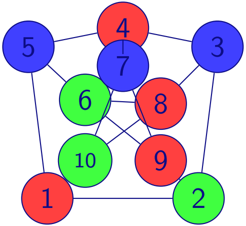


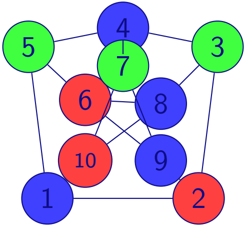
Chooses $\forall u \in V, r_u$

Chooses i and j

P wants to prove to V his 3-coloring of $G = (E, V)$

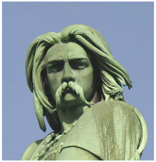
P selects a permutation π of the 3 colors.

$\pi($ 

$)=$ 

Chooses $\forall u \in V, r_u$

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$
$$\longleftarrow u_i, u_j \longleftarrow$$
$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

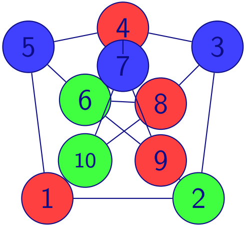


Chooses i and j

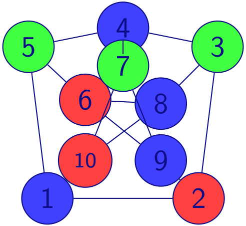
P wants to prove to V his 3-coloring of $G = (E, V)$

P selects a permutation π of the 3 colors.

$\pi($



$)=$



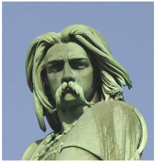
Chooses $\forall u \in V, r_u$

$$\rightarrow \forall u \in V, e_u = H(\pi(c(u))||r_u) \rightarrow$$

$$\longleftarrow u_i, u_j \longleftarrow$$

$$\longrightarrow r_{u_i}, r_{u_j}, \pi(c(u_i)), \pi(c(v_j)) \longrightarrow$$

V accepts, if $e_{u_i} = H(\pi(c(u_i))||r_{u_i})$ and $e_{u_j} = H(\pi(c(u_j))||r_{u_j})$



Chooses i and j

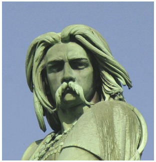
Outline

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

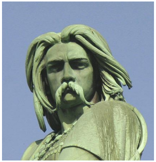


Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$



Chooses a random r

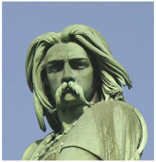
Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

$\longrightarrow t = g^r \longrightarrow$



Chooses a random r

Schnorr Protocol, 1991

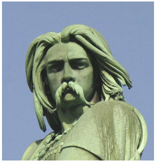
Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$\longrightarrow t = g^r \longrightarrow$



Chooses a random c

Schnorr Protocol, 1991

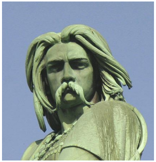
Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

$\longrightarrow t = g^r \longrightarrow$

$\longleftarrow c \longleftarrow$



Chooses a random r

Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

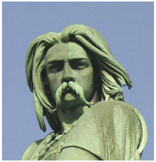
Goal

P wants to prove the knowledge of x, where $y = g^x$

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random r

Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

P wants to prove the knowledge of x, where $y = g^x$

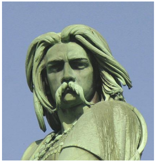
Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$

V accepts, if $t \cdot y^c = g^s$



Chooses a random c

Schnorr Protocol, 1991

Let G_q a cyclic group of order q with a public generator g

Goal

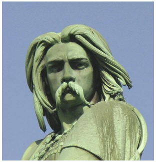
P wants to prove the knowledge of x, where $y = g^x$

Chooses a random r

$$\longrightarrow t = g^r \longrightarrow$$

$$\longleftarrow c \longleftarrow$$

$$\longrightarrow s = r + x \cdot c \longrightarrow$$



Chooses a random c

V accepts, if $t \cdot y^c = g^s$

$$t \cdot y^c = g^r \cdot (g^x)^c = g^{r+x \cdot c} = g^s$$

Outline

Things to bring home

- Existence of Interactive Zero-knowledge Proof
- 3 protocols :
  1. Cave
  2. Graph 3 coloring
  3. Discret Logarithm (Schnorr)

Thank you for your attention.

Questions ?