ZK with Rubik's Cubes and Non-Abelian Groups

Emmanuel Volte - Valérie Nachef - Jacques Patarin

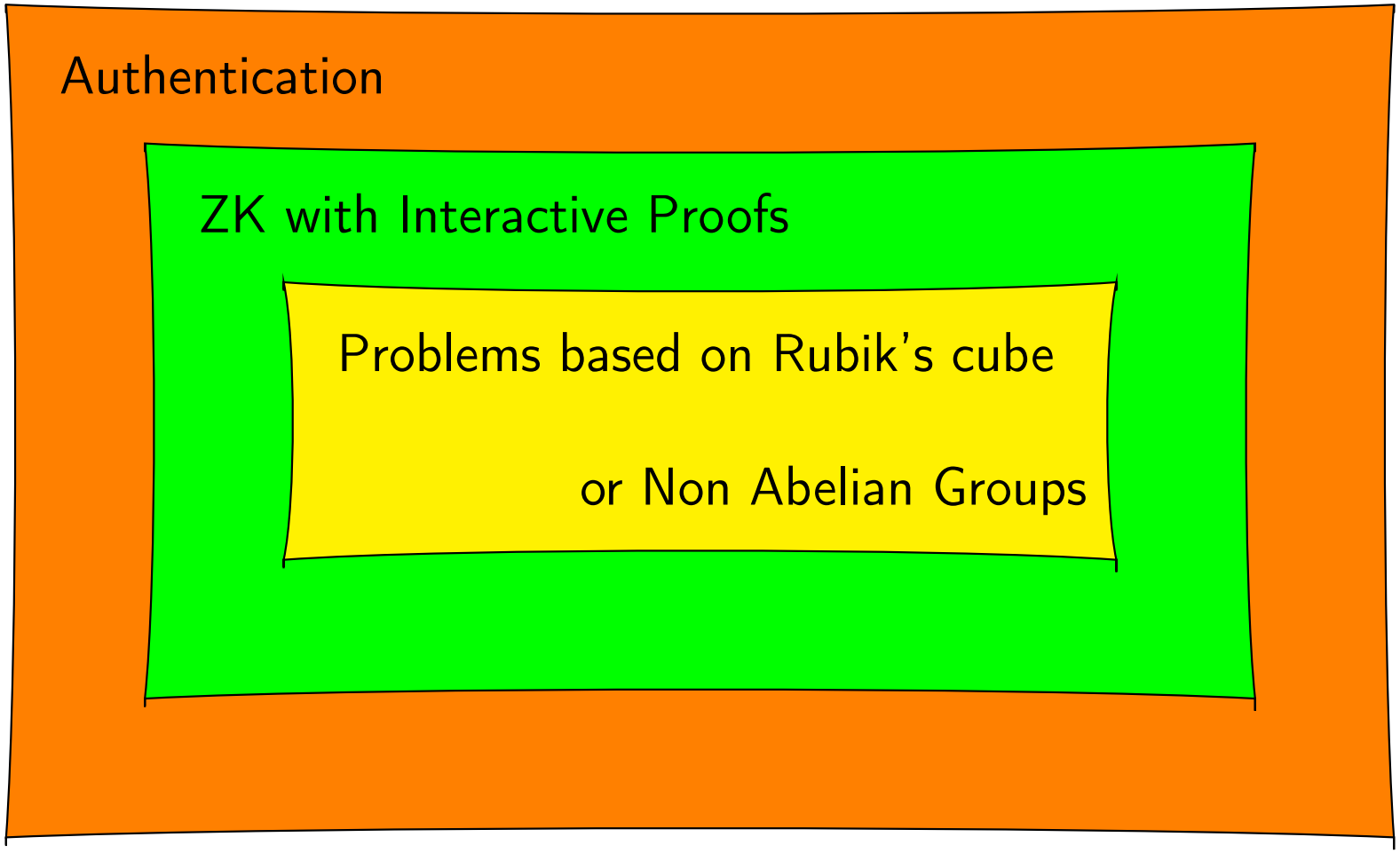
UNIVERSITÉ de Cergy-Pontoise

UNIVERSITÉ de Cergy-Pontoise

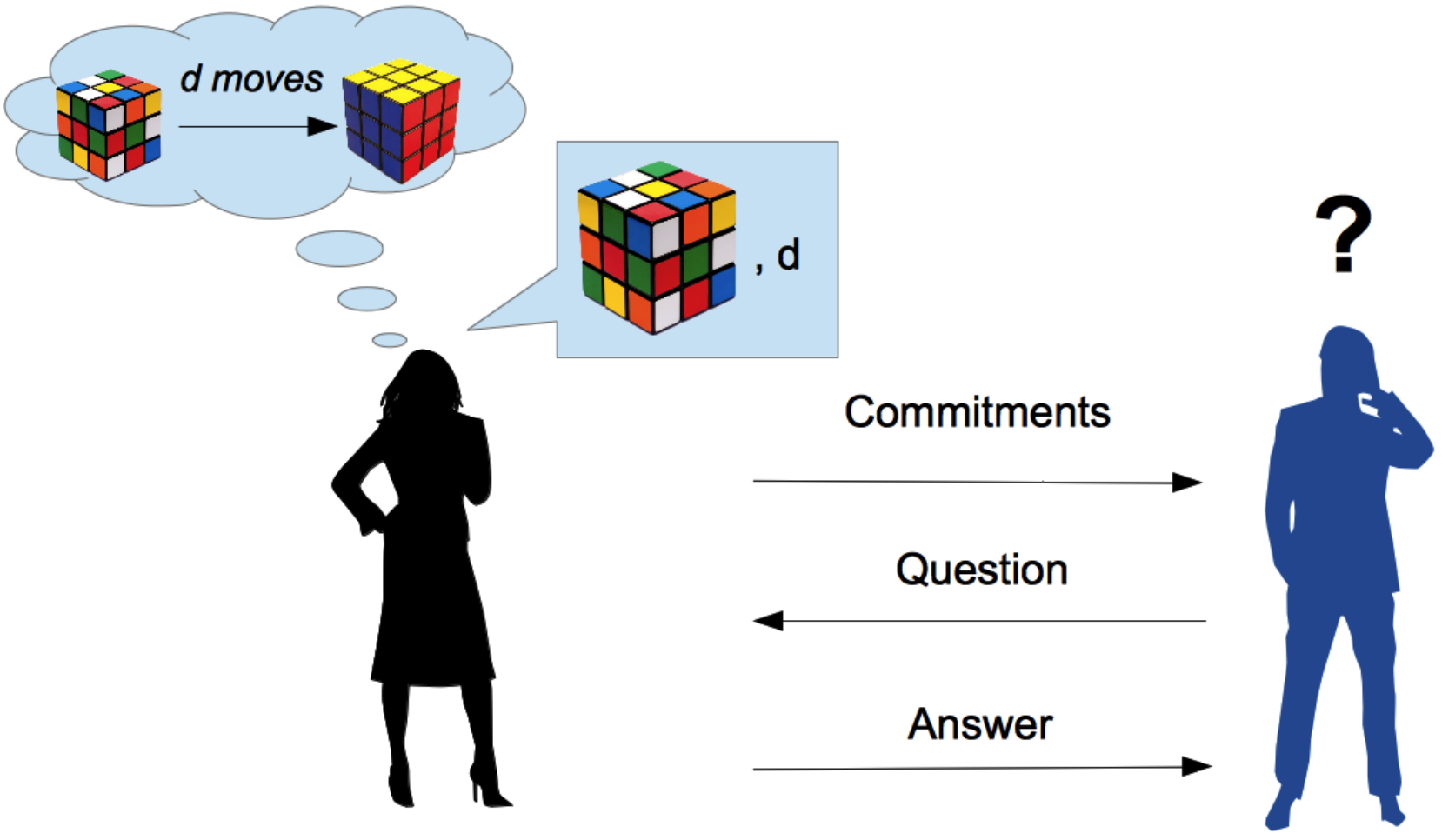
UNIVERSITÉ DE VERSAILLES SAINT-QUENTIN-EN-YVELINES

20 novembre 2013

Overview


Authentication
ZK with Interactive Proofs
Problems based on Rubik's cube
or Non Abelian Groups

ZK with Interactive Proofs



Main motivations

1. Authentication with new kind of problems.
2. Compact size (fit in a pocket).
3. Hardware efficiency.

Outline

S_n, Generators

Symmetric Group : S_X = group of permutation of a finite set X.

If $X = \{1; 2; \ldots; n\}$ then $S_X = S_n$.

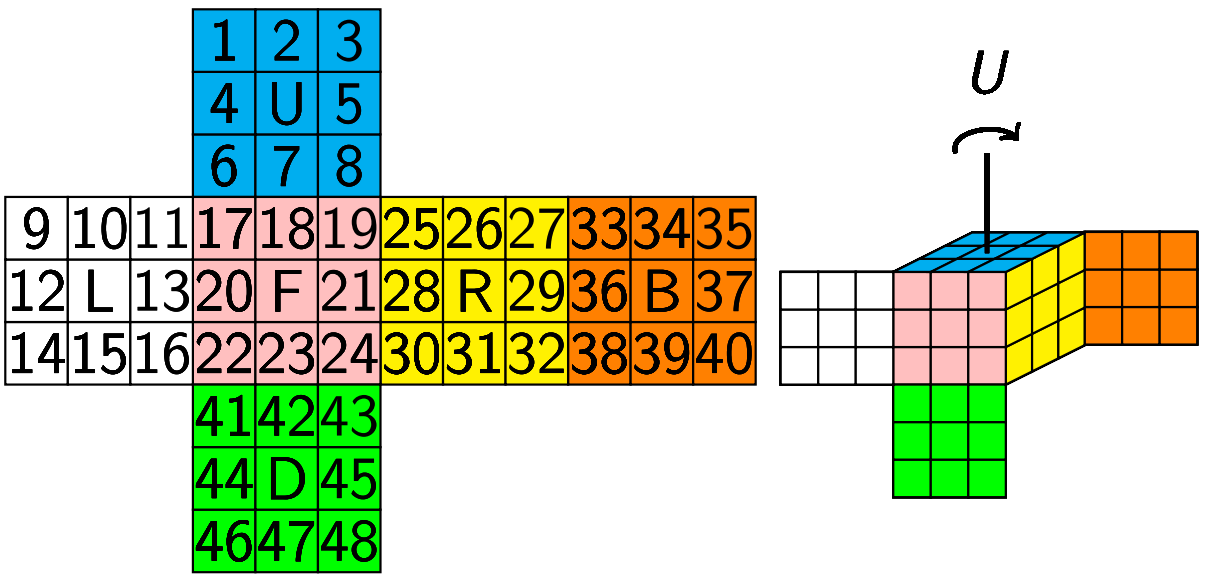
$\forall \sigma, \sigma' \in S_X,\ \sigma\sigma' = \sigma' \circ \sigma$.

$\langle \ldots \rangle$: G group, $(g_1, g_2, \ldots, g_\alpha) \in G^\alpha$

$$\langle g_1, g_2, \ldots, g_\alpha \rangle = \bigcap_{\substack{H \text{ subgroup of } G \\ g_1, g_2, \ldots g_\alpha \in H}} H$$

Set of Generators : $\{g_1, \ldots, g_\alpha\}$ such that $\langle g_1, g_2, \ldots, g_\alpha \rangle = G$

Group of the Rubik's Cube



Generators of the Rubik's Cube's Group

Generators

$F = (17,19,24,22)(18,21,23,20)(6,25,43,16)(7,28,42,13)(8,30,41,11)$
$B = (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27)$
$L = (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35)$
$R = (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24)$
$U = (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19)$
$D = (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40)$

Rubik's cube group

$G_R = \langle F, B, L, R, U, D \rangle \subset S_{48}$.

General Notations for the Problems

- G : Non-Abelian Group
- $\mathcal{F} \subset G$: set of generators.
  $\mathcal{F} = \{f_1; f_2; \ldots; f_\alpha\}$, $\alpha \geq 2$
- $id \in G$: initial position

Two Difficult Problems

Problem 1 : solve the puzzle. (not difficult)

Given $x_0 \in X$, find $d \in \mathbb{N}^*$, and $(i_1, i_2, \ldots, i_d) \in \{1; 2; \ldots; \alpha\}^d$

$$\text{so that} \qquad x_0 f_{i_1} f_{i_2} \ldots f_{i_d} = id$$

Problem 2 : solved the puzzle with a fixed number of moves.

Given $d \in \mathbb{N}^*$, $x_0 \in X$, find $(i_1, i_2, \ldots, i_d) \in \{1; 2; \ldots; \alpha\}^d$

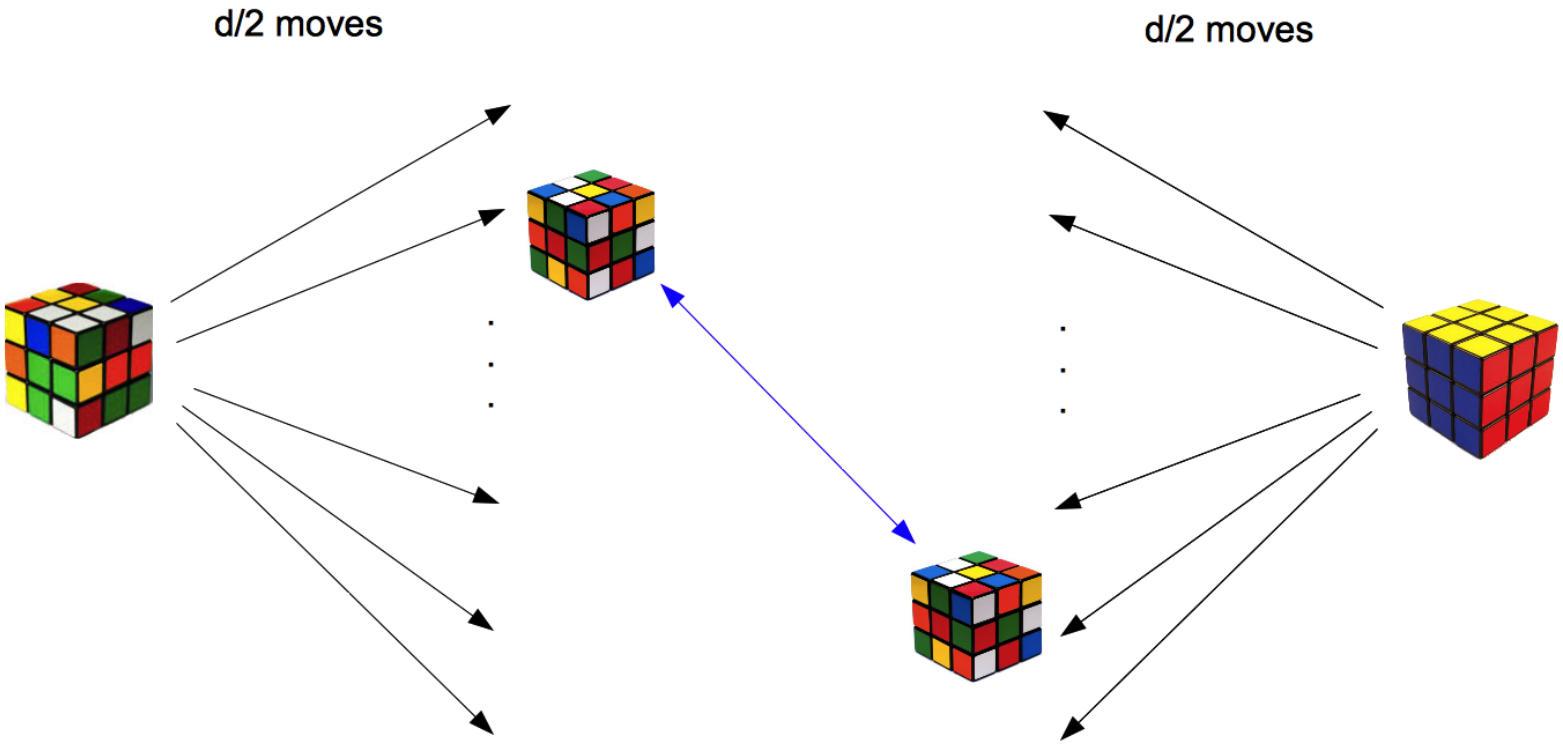
$$\text{so that} \qquad x_0 f_{i_1} f_{i_2} \ldots f_{i_d} = id$$

Problem 3 : go from one position to another with a fixed number of moves.

Given $d \in \mathbb{N}^*$, $(x_0, x_d) \in X^2$, find $(i_1, i_2, \ldots, i_d) \in \{1; 2; \ldots; \alpha\}^d$

$$\text{so that} \qquad x_0 f_{i_1} f_{i_2} \ldots f_{i_d} = x_d$$

Complexity of problem 2



Complexity $= O(d\alpha^{d/2})$

How to choose d

Rubik's $3 \times 3 \times 3$

- God's number : 20 moves to unscramble from any position.
- $|G_R| \approx 2^{61}$.
- $\alpha = 6$ and $d = 24$ since $6^{24} \approx 2^{60} \Rightarrow$ security in about 2^{30} computations.

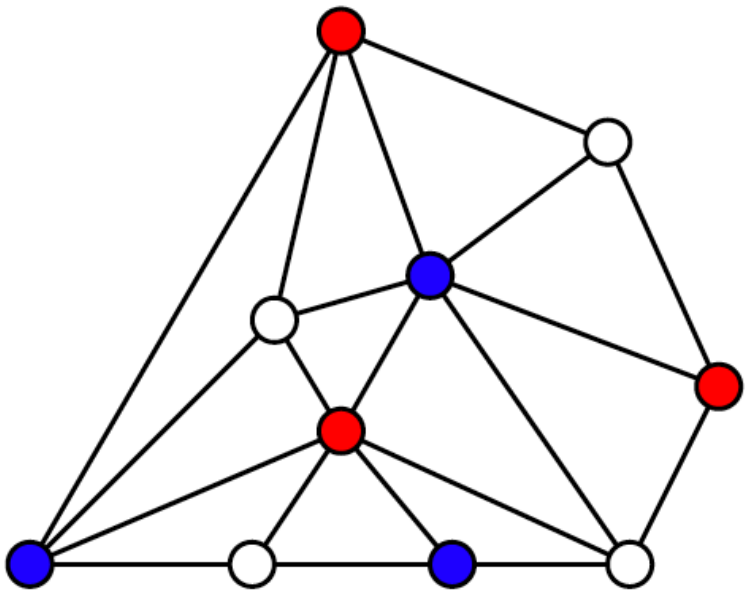
General case

We want $d\alpha^{d/2} \approx 2^{80}$ and $\alpha^d \leq |G|$.

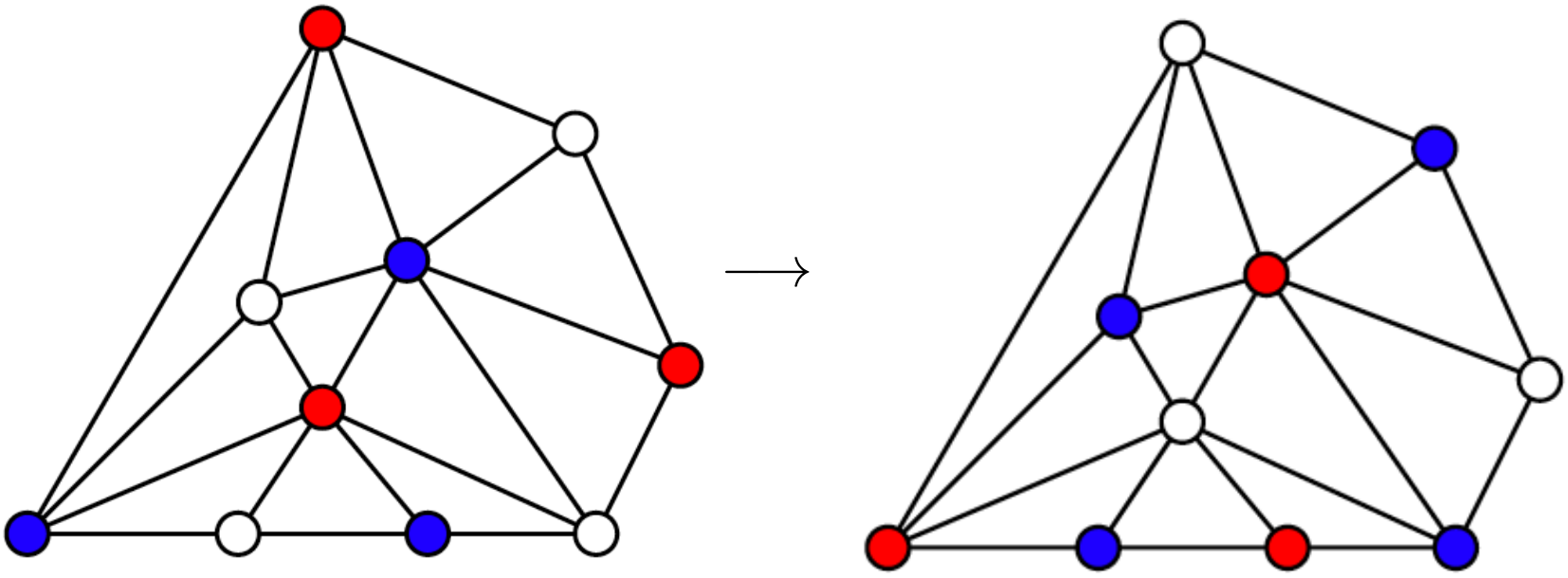
α	2	4	6	8	10	12	14	16	50	100	9240 ($S41$)
d	146	74	58	50	46	42	40	38	28	24	12

Alice's Secret

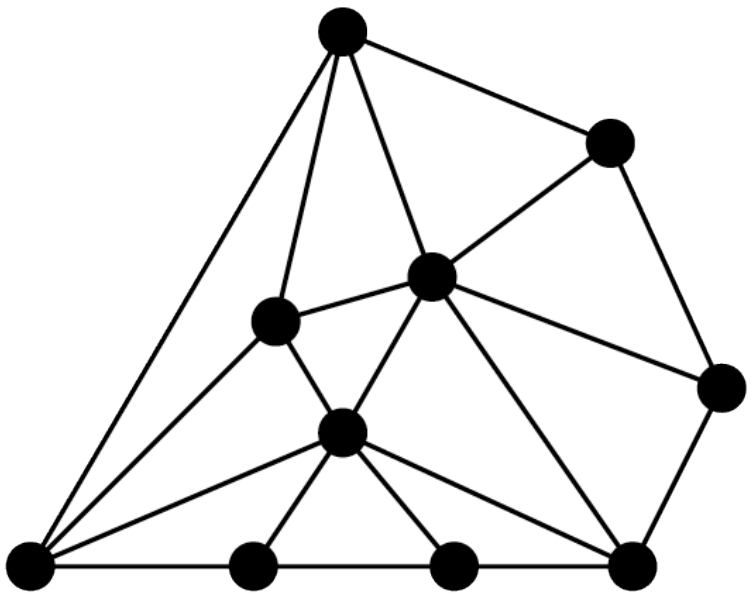
Alice knows how to color a graph with 3 colors.



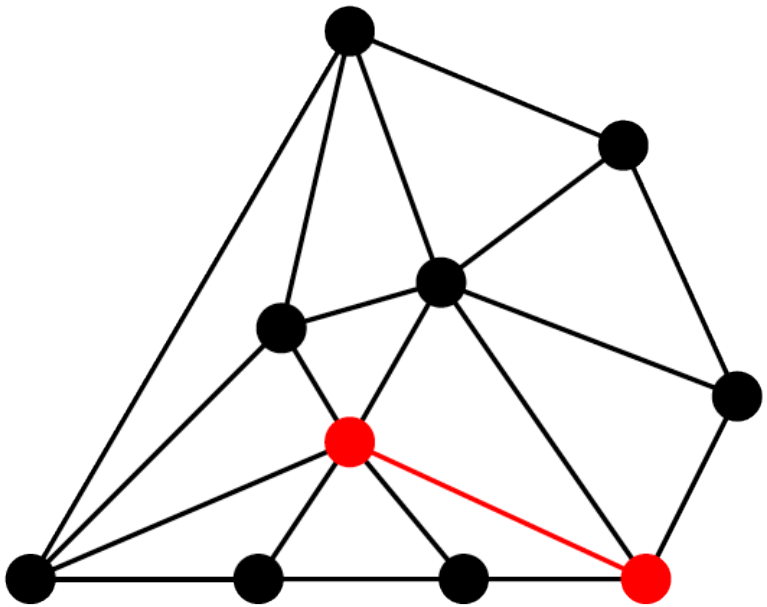
Melting Colors at Random



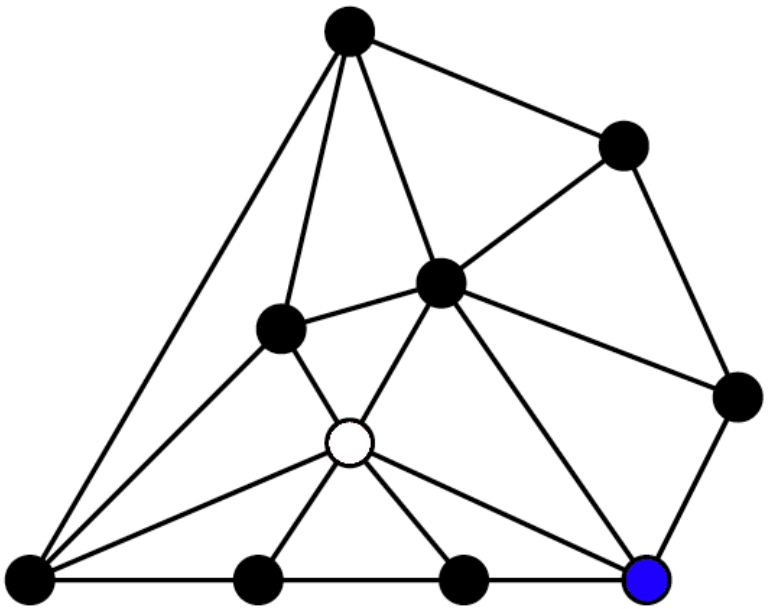
Hiding Colors with Commitments



Bob's question



Alice's answer



ZK Principes

Correctness

A legitimate prover is always accepted.

Statistically Zero Knowledge

There exists an efficient simulating algorithm U such that for every feasible Verifier strategy V, the distributions produced by the simulator and the proof protocol are statistically indistinguishable.

Proof of zero knowledge with error knowledge α

There is a knowledge extractor K and a polynomial Q such that :
$p =$ probability that K finds a valid witness for x using its access to a prover P^*,
$p_x =$ probability that P^* convinces the honest verifier on x,
if $p_x > \alpha$, then $p \geq Q(p_x - \alpha)$.

Conjugation

Definition

Let G be a group.

- $\forall(\sigma, \tau) \in G^2, \quad \sigma^\tau \stackrel{def}{=} \tau^{-1}\sigma\tau$
- $\sigma^G \stackrel{def}{=} \{\sigma^g | g \in G\}$.

Proposition

$\forall(\sigma, \sigma', \tau, \tau') \in G^4, \quad (\sigma^\tau)^{\tau'} = \sigma^{\tau\tau'}, \quad \sigma^\tau\sigma'^\tau = (\sigma\sigma')^\tau$

Repositioning Group

Definition

Let $\mathcal{F} = \{f_1, \ldots, f_\alpha\} \subset G$, where G is a group.
Any subgroup H such that

$$f_1{}^H = \{h^{-1} f_1 h \mid h \in H\} = \mathcal{F}$$

is called a ***repositioning*** *group of $\mathcal{F}$.*

Proposition

If $\mathcal{F}$ has a repositioning group H then for $\tau \in_R H$,

$$\forall (i,j) \in \{1; \ldots; \alpha\}^2, \quad P(f_i{}^\tau = f_j) = \frac{1}{\alpha}.$$

Repositioning Group of the Rubik's Cube

Definition

Let $H = \langle h_1, h_2 \rangle$ *where*

$$\begin{aligned} h_1 &= RL^{-1}(2, 39, 42, 18)(7, 34, 47, 23) \\ h_2 &= UD^{-1}(13, 37, 29, 21)(12, 36, 28, 20) \end{aligned}$$

Proposition

If $f \in_R \mathcal{F}$ *and* $\tau \in_R H$, *then*
f^τ *is a random uniform variable in* $\mathcal{F}$.

$$\begin{array}{ccc} x_0 & \xrightarrow{f} & x_1 \\ {\scriptstyle\tau}\downarrow & & \downarrow{\scriptstyle\tau} \\ x_0\tau & \xrightarrow{f^\tau} & x_1\tau \end{array}$$

Protocol (notations)

Public :

- A group G.
- A set $\mathcal{F} = \{f_1, \ldots, f_\alpha\} \subset G$ of generators of G_R
- A repositioning group $H \subset G$ such that ${f_1}^H = \mathcal{F}$.
- $d \in \mathbb{N}$, $d \geq 3$
- G' subgroup of G generated by $\mathcal{F}$ and H. $G' = \langle \mathcal{F}, H \rangle$.
- K a set of keys, $|K| \geq 2^{80}$.

Secret key : $i_1, i_2, \ldots, i_d \in \{1, 2, \ldots, \alpha\}$.
Public key : $x_0 = (f_{i_1} f_{i_2} \ldots f_{i_d})^{-1}$

Protocol (first phase) :

Prover		**Verifier**
Picks $\tau \in_R H$, $\sigma_0 \in_R G'$, $k_*, k_0, k_1, \ldots, k_d \in_R K$ **Computes** $\forall j \in \{1, \ldots, d\}$, $\sigma_j = (f_{i_j}{}^{\tau})^{-1}\sigma_{j-1}$ $c_0 = Com_{k_*}(\tau)$ $\forall i \in \{0, \ldots d\}$, $s_i = Com_{k_i}(\sigma_i)$	$c_0, s_0, \ldots, s_d \longrightarrow$	

Illustration

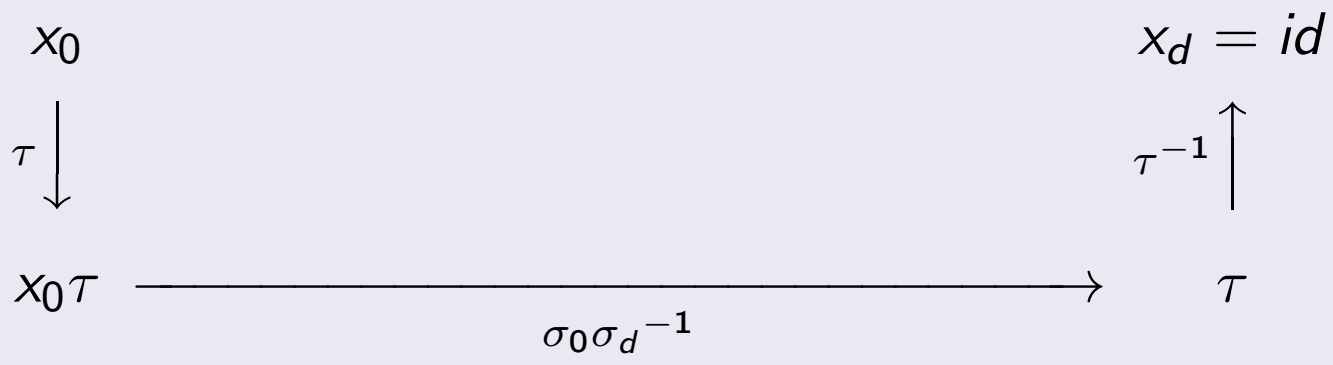
$$\begin{array}{ccccccc}
x_0 & \xrightarrow{f_{i_1}} & x_1 & \xrightarrow{f_{i_2}} & \cdots & x_{d-1} & \xrightarrow{f_{i_d}} & x_d = id \\
\tau \downarrow & & \tau \downarrow & & & \tau \downarrow & & \tau \downarrow \\
x_0\tau & \xrightarrow[\sigma_0{\sigma_1}^{-1}]{{f_{i_1}}^{\tau}} & x_1\tau & \xrightarrow[\sigma_1{\sigma_2}^{-1}]{{f_{i_2}}^{\tau}} & \cdots & x_{d-1}\tau & \xrightarrow[\sigma_{d-1}{\sigma_d}^{-1}]{{f_{i_d}}^{\tau}} & \tau
\end{array}$$

Protocol (second and third phase, $q = 0$) :

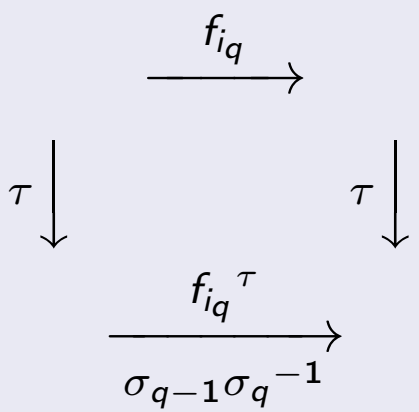
Prover		**Verifier**
	q $\longleftarrow$	**Picks** $q \in_R \{0, \ldots d\}$
Case $q = 0$	$\tau,\ \sigma_0$ $\longrightarrow$	**Computes** $\sigma_d = \tau^{-1} x_0 \tau \sigma_0$ **Checks** $\tau \in H,\ Com_{k_*}(\tau) = c_0,$ $Com_{k_0}(\sigma_0) = s_0,$ $Com_{k_d}(\sigma_d) = s_d$ **If** all tests ok **then accepts else rejects.**
	$k_*,\ k_0,\ k_d$ $\longleftarrow$	

Partial Verifications

$q = 0$



$q \neq 0$ (τ is not revealed)



Protocol (second and third phase, $q \neq 0$) :

Prover		**Verifier**
	q $\longleftarrow$	**Picks** $q \in_R \{0, \ldots d\}$
Case $q \neq 0$	${f_{i_q}}^{\tau}, \sigma_q$ $\longrightarrow$ k_{q-1}, k_q	**Computes** $\sigma_{q-1} = {f_{i_q}}^{\tau} \sigma_q$ **Checks** ${f_{i_q}}^{\tau} \in \mathcal{F}$, $s_{q-1} = Com_{k_{q-1}}(\sigma_{q-1})$ $s_q = Com_{k_q}(\sigma_q)$ **If** all tests ok **then accepts** **else rejects.**

Proof : Correctness and ZK

Correctness

Obvious.

ZK with error knowledge $\frac{d}{d+1}$

$d + 1$ possible questions.
All answers correct $\Rightarrow$ we can extract a solution.
So, a false prover can at most answer correctly to d questions.

Proof : statistically ZK

- We can build a simulator with a distribution close to a legitimate prover's one.
- The simulator can answer to all questions but one (we choose this one).

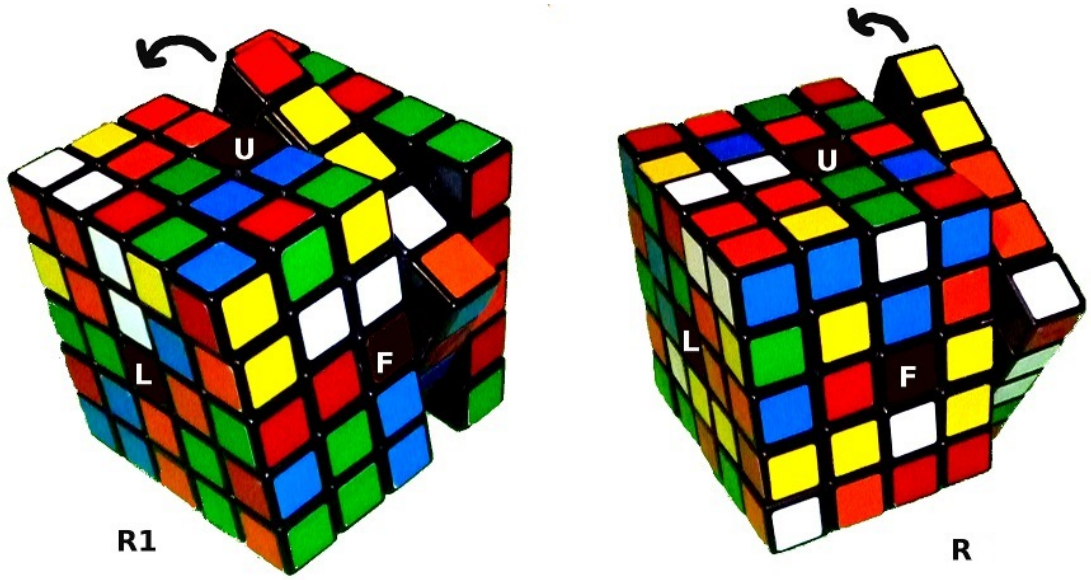
Choice of r (number of rounds)

$$\left(\frac{d}{d+1}\right)^r \approx 2^{-30}$$

α	6 $(3 \times 3 \times 3)$	12 $(5 \times 5 \times 5)$	9240 $(S41)$
d	24 $(*)$	48	12
r	500	988	261

$(*)$ security in 2^{30} computations only.

Non-existence of a repositioning group



$G_R \approx 2^{247}$, $\mathcal{F} = \{U, D, F, B, R, L, U_1, D_1, F_1, B_1, R_1, L_1\}$.

U and U_1 are not conjugate!

One solution

Extension group

- Duplicate the cube.
- Consider $\mathcal{F} = \{(U, U_1), (D, D_1), \ldots, (L_1, L)\}$ and $G_R = \langle \mathcal{F} \rangle \subset G_R \times G_R$. $|G_R| \approx 2^{364}$.
- $H = \langle (h_1, h_1), (h_2, h_2), e \rangle$ where e exchange the cubes.

Any set of generators

What we have

- G group
- $\mathcal{F} = \{f_1, f_2 \ldots, f_n\}$ set of generators : $\langle \mathcal{F} \rangle = G$

Construction of a repositioning group

We work first with G^α. Let $f_i = (f_i, f_{i+1}, \ldots, f_\alpha, f_1, \ldots, f_{i-1})$ and $\mathcal{F} = \{f_1, \ldots, f_\alpha\}$
We define $h \notin G^\alpha$ such that

$$\forall (a_1, \ldots, a_\alpha) \in G^\alpha, \quad (a_1, \ldots, a_\alpha)^h = (a_2, \ldots, a_\alpha, a_1)$$

Let $G = \langle h, f_1, \ldots, f_\alpha \rangle$.
Then $H = \langle h \rangle$ is a repositioning group of $\mathcal{F}$ in G.

Finite factorisation

Problem 4 : solve the puzzle with a maximum number of moves

Given $d \in \mathbb{N}^*$, $x_0 \in X$, find $d' \leq d$ and $(i_1, i_2, \ldots, i_{d'}) \in \{1; 2; \ldots; \alpha\}^{d'}$ so that

$$x_0 f_{i_1} f_{i_2} \ldots f_{i_{d'}} = id$$

Solution

We add $f_0 = id$ in $\mathcal{F}$ and we use precedent construction !

A new puzzle called $S41$

In S_{41} we set :

$$\begin{aligned} h &= (1,14,39,19,31,18,37)(3,36,4,23,20,34,16,25,17,26,35) \\ &\quad (5,13,30,33)(6,7,10)(8,24,15,38,41,27,11,9) \\ &\quad (12,40,32,21,28)(22,29) \text{ and} \\ f_1 &= (1,11,31,6,17,34,25,24,22,12,4,28,3,14,5,27,32,13, \\ &\quad 26,8,23,2,20,41,19,10,40,15,38,16,37,39,35,21,18) \\ &\quad (7,29,36)(9,30). \end{aligned}$$

Then $H = \langle h \rangle$ is a natural repositioning group of $\mathcal{F} = {f_1}^H$.

Obrigado pela sua atenção!