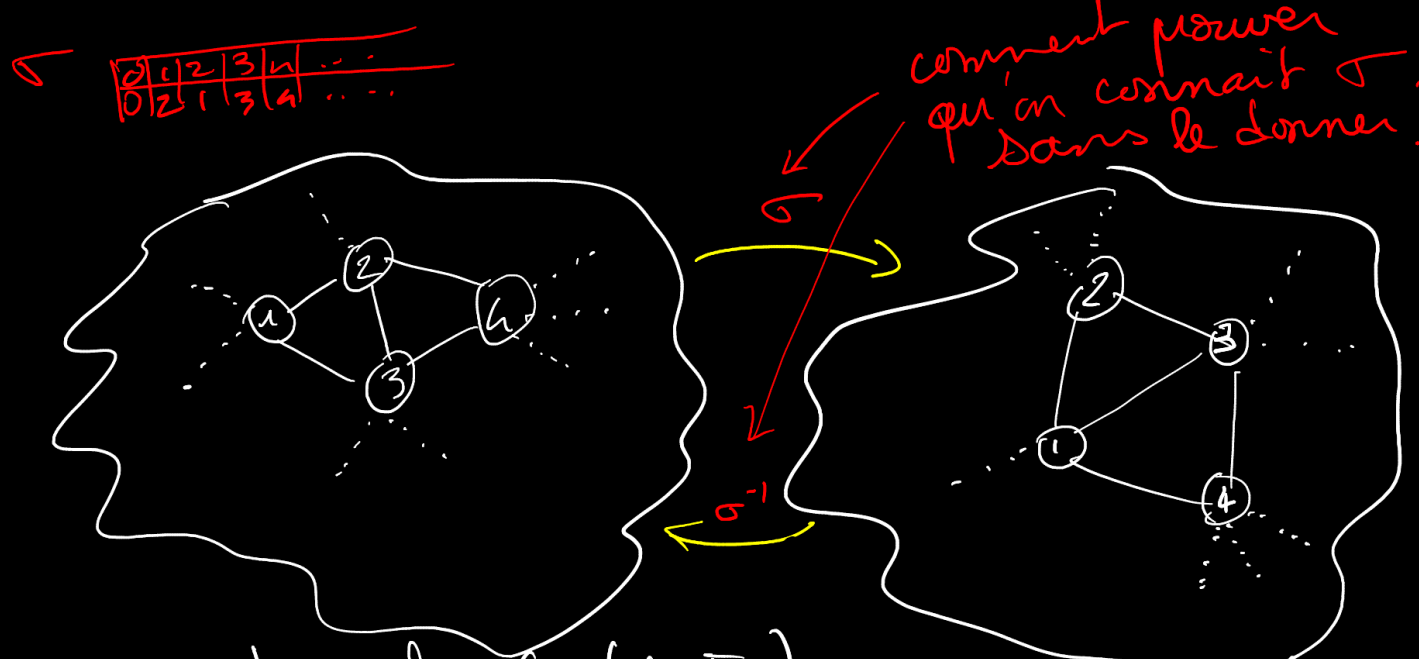
Zero Knowledge Proof
une utilisation de l'isomorphisme de graphes en cryptographie



grand graphe $G_1 = (V_1, E_1)$

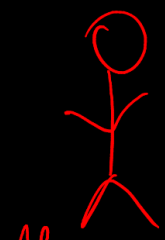
$V_2 = \{\sigma(v) \mid v \in V_1\}$

$E_2 = \{(\sigma(x), \sigma(y)) \mid (x,y) \in E_1\}$

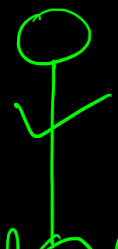
$V_1 = \{\sigma^{-1}(v) \mid v \in V_2\}$

$E_1 = \{(\sigma^{-1}(x), \sigma^{-1}(y)) \mid (x,y) \in E_2\}$

grand graphe $G_2 = (V_2, E_2)$



Alice connaît σ



Bob doit être convaincu que Alice connaît σ.

ne connaît pas σ et ne doit pas le connaître

1. A tire une permutation π aléatoire et un nombre $i \in \{1,2,3\}$ aléatoire puis envoie $G_3 = \pi(G_i)$ à B.

2. Bob tire au hasard un nombre $j \in \{1,2,3\}$ et l'envoie à A.

3. - si $i = j$ (1 chance sur deux) alors A envoie π^{-1} à B
   - si $i=1$ et $j=2$ (1 chance sur 6) A envoie $\pi^{-1} \circ \sigma$ à B
   - si $i=2$ et $j=1$ (1 chance sur 6) A envoie $\pi^{-1} \circ \sigma^{-1}$ à B

indique comment passer de G_3 à G_j

4. Bob vérifie que la permutation reçue transforme G_3 en G_j.

Cette procédure a $\approx \frac{1}{2}$ chance d'échouer si Alice ne connaît pas σ. En la répétant n fois, on peut s'assurer que Alice connaît σ avec proba $\frac{1}{2^n}$.