Preuve *zero-knowledge* pour NP relativistes et réalisables

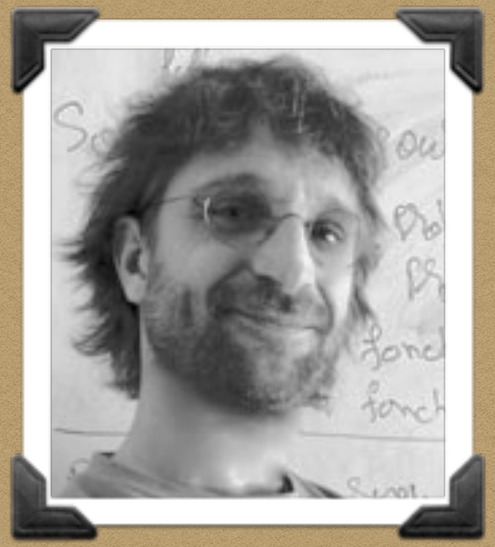
Claude Crépeau

McGill

Preuve *zero-knowledge* pour NP relativistes et réalisables (cohérente malgré l'intrication)

Claude Crépeau

McGill



Claude Crépeau

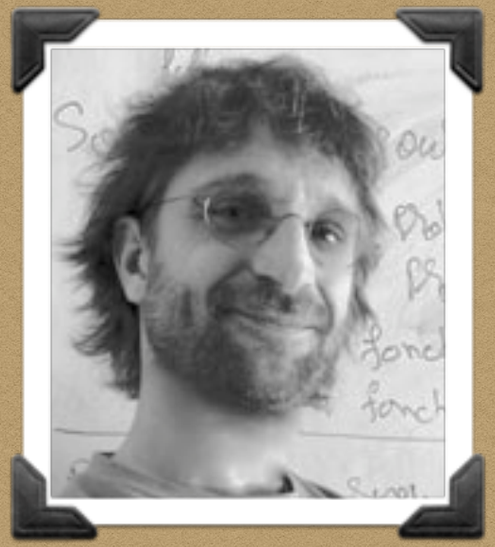
McGill

Arnaud Yoh Massenet-Oshima

Louis Salvail

Lucas Shigeru Stinchcombe

Nan Yang



Claude Crépeau

McGill

Arnaud Yoh Massenet-Oshima
Louis Salvail
Lucas Shigeru Stinchcombe
Nan Yang

PREUVE *ZERO-KNOWLEDGE* POUR NP RELATIVISTES ET RÉALISABLES (COHÉRENTE MALGRÉ L'INTRICATION)

Claude Crépeau

McGill

INTRODUCTION

(P-V-D)

PERSONNAGES

PERSONNAGES

prouveur

PERSONNAGES

prouveur

vérificateur

PERSONNAGES

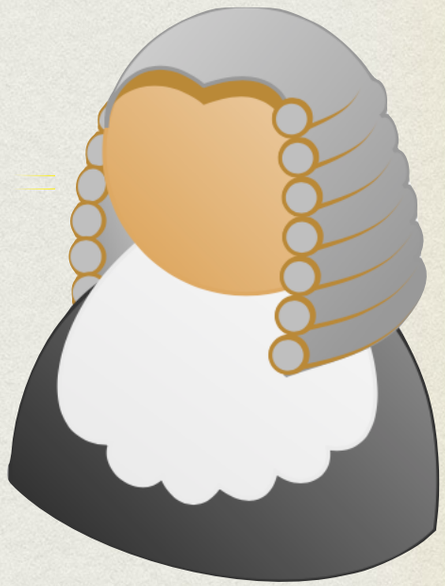
prouveur

vérificateur

PERSONNAGES

prouveur

vérificateur



distingueur

INTRODUCTION

(ZK) IPs


Goldwasser


Micali


Rackoff

1985

W

Goldwasser

Micali

Rackoff

1985

W

a

Goldwasser

Micali

Rackoff

1985

W

a

x

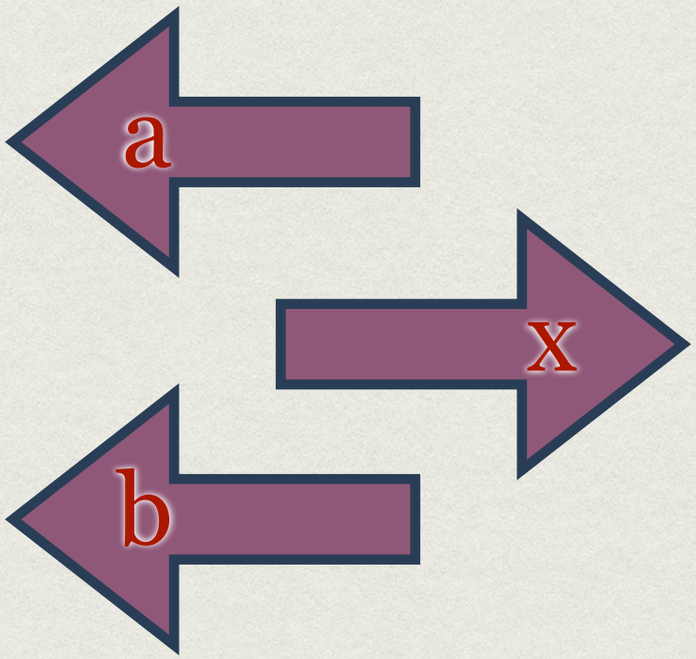
Goldwasser

Micali

Rackoff

1985

W



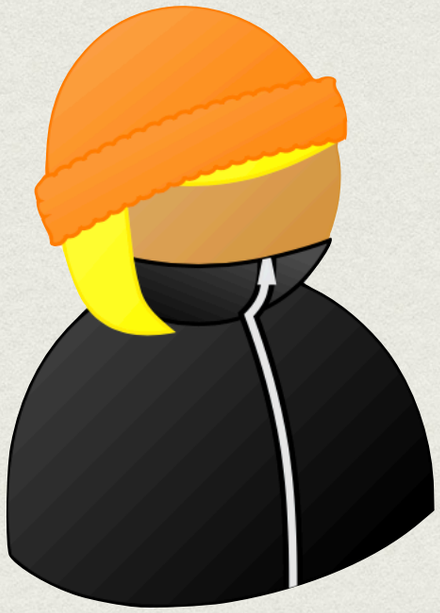

Goldwasser

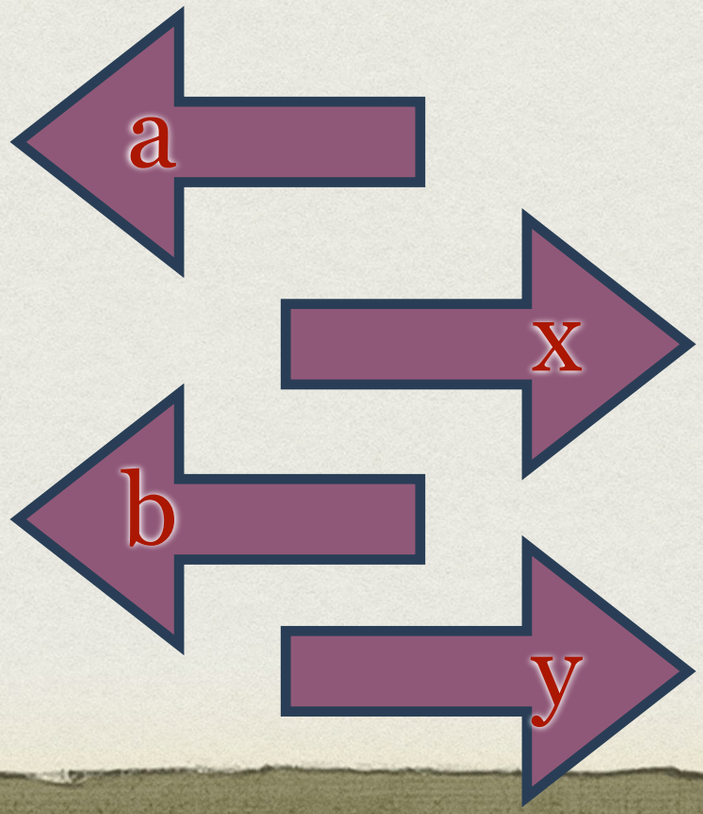

Micali


Rackoff

1985

W






Goldwasser

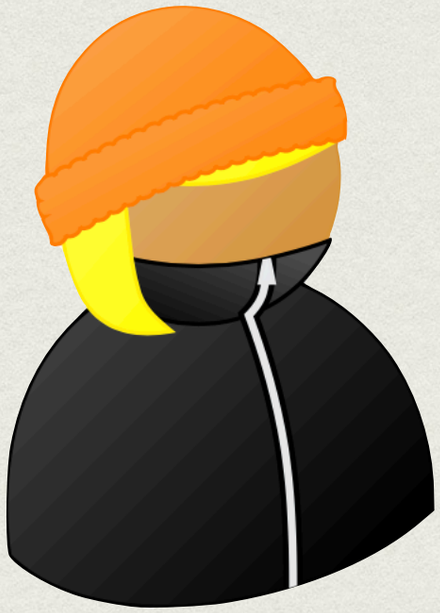

Micali


Rackoff

1985

wEL

w



a

x

b

y


Goldwasser


Micali

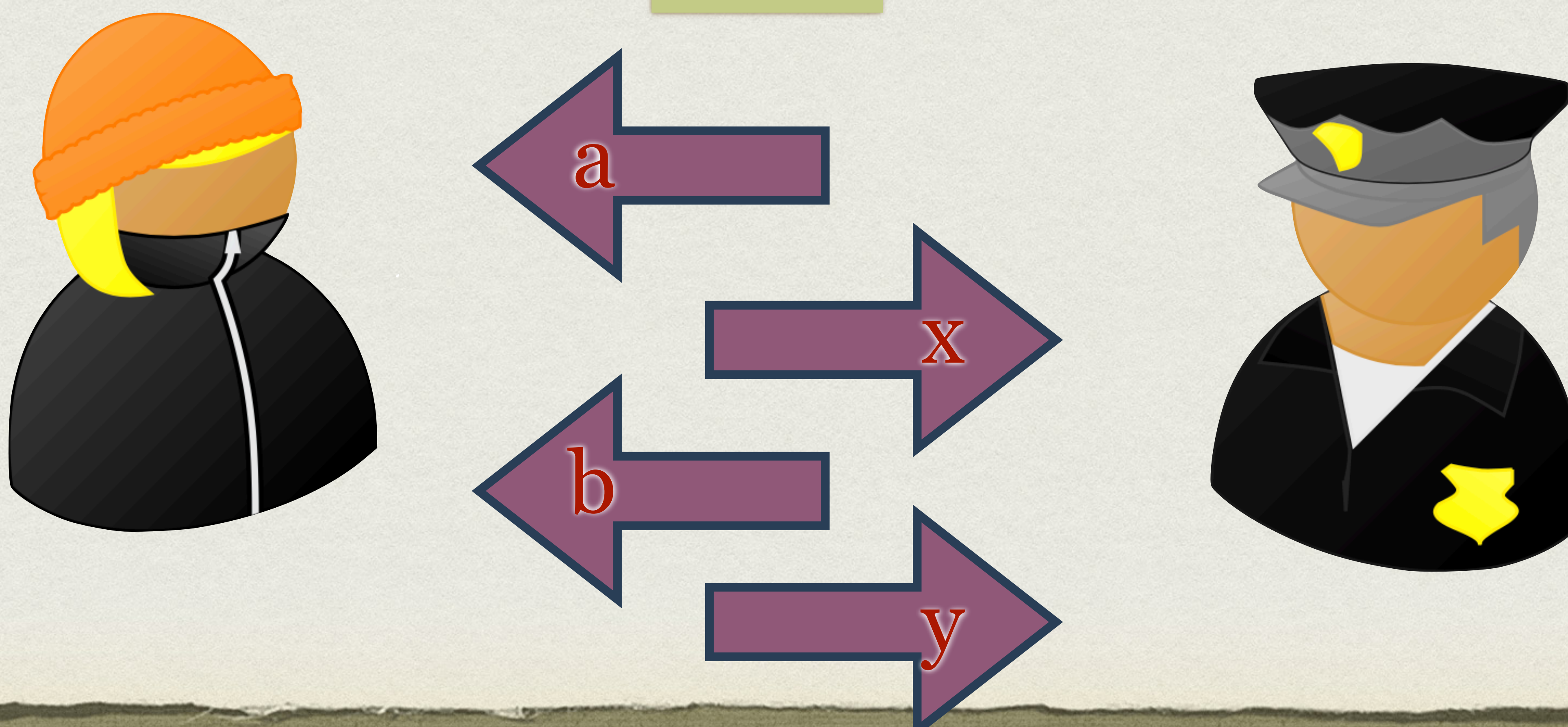

Rackoff

1985

$L \in IP$

$w \in L$

w



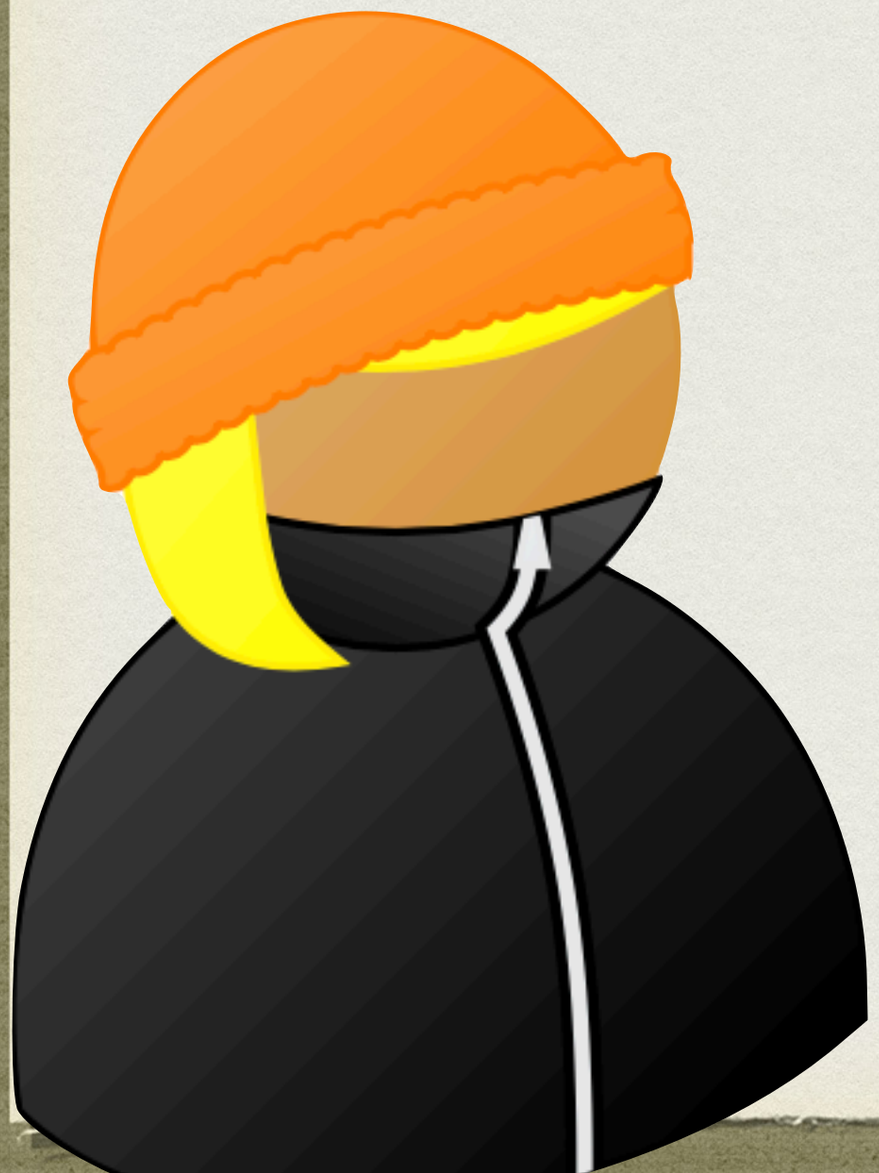
Goldwasser

Micali

Rackoff

1985

LeIP weL



w

a

x

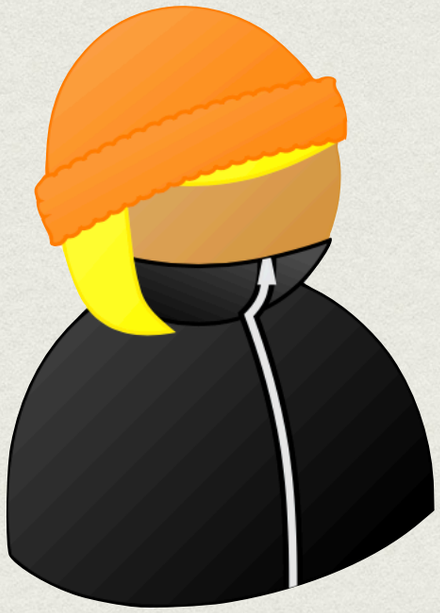
b

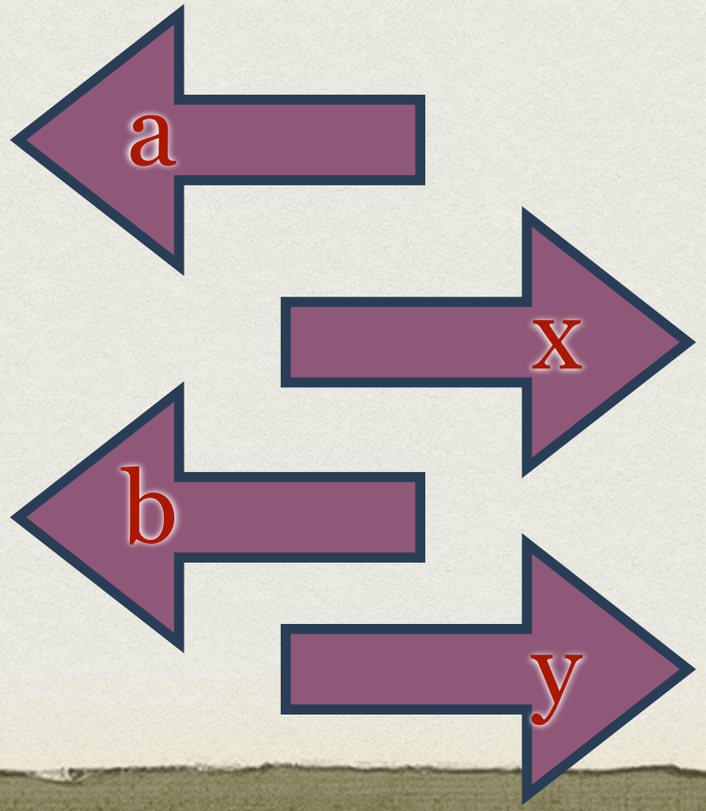
y

Complétude

$\exists$  , $\exists$  , $\forall w \in L$, **Prob**[( : ) accèpte] $\geq 1 - \epsilon$

w



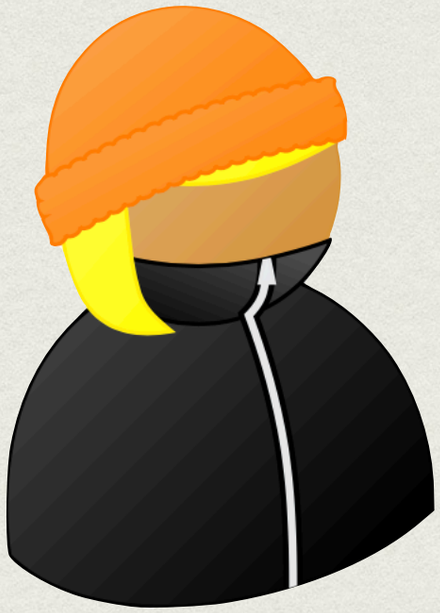


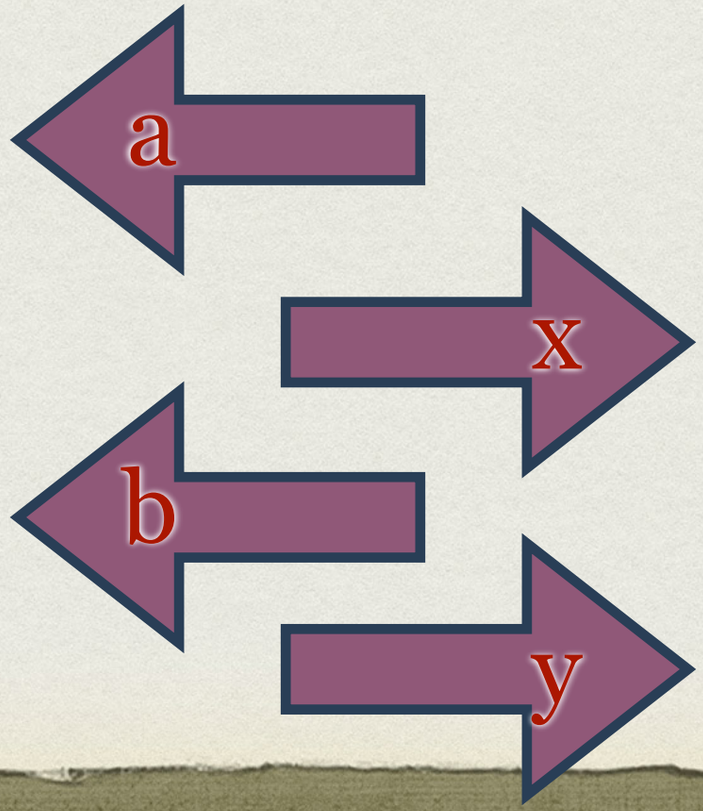
Complétude

$w \in L$

$\exists$  , $\exists$  , $\forall w \in L$, **Prob**[( : ) accèpte] $\geq 1 - \epsilon$

w



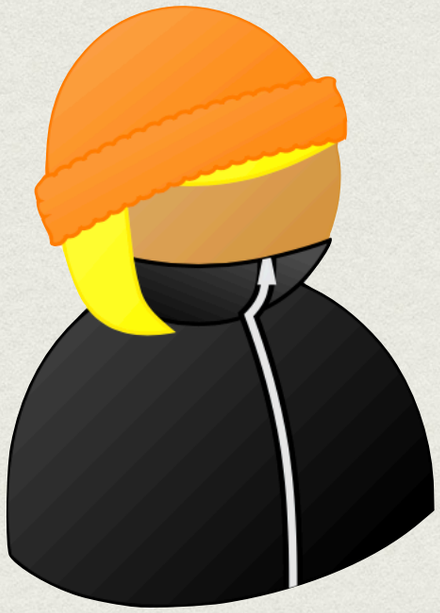


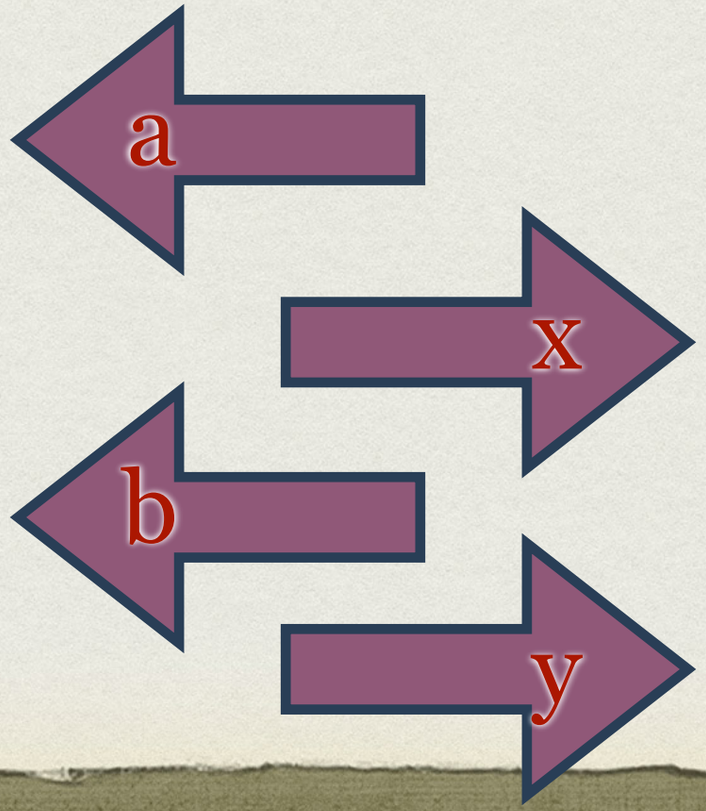
Complétude

$w \in L$

$\exists$  , $\exists$  , $\forall w \in L$, **Prob**[( : ) accèpte] $\geq 1 - \epsilon$

w

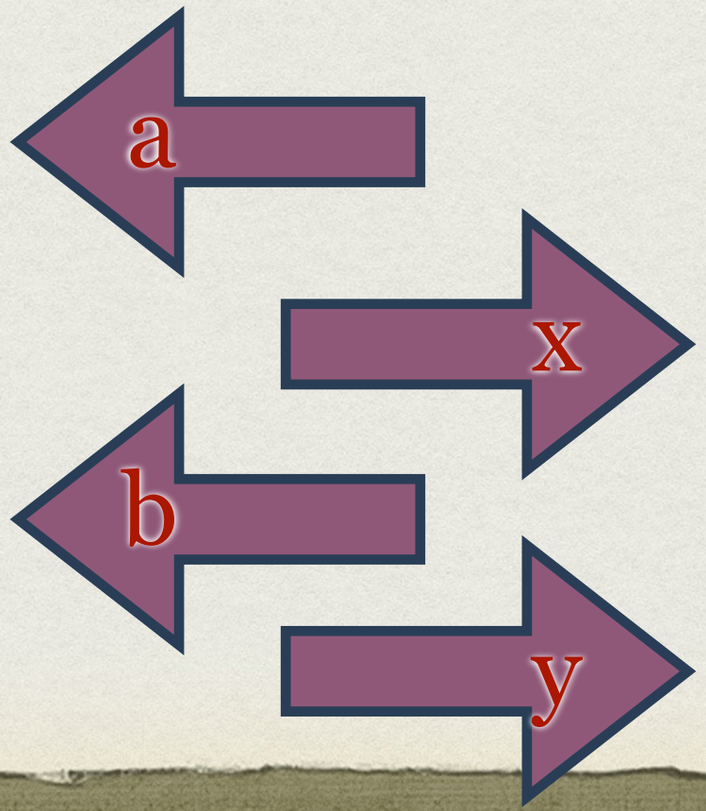




Cohérence

$\exists$  , et $\forall$  , $\forall w \notin L$, **Prob**[( : ) accepte] $\leq \epsilon$

w

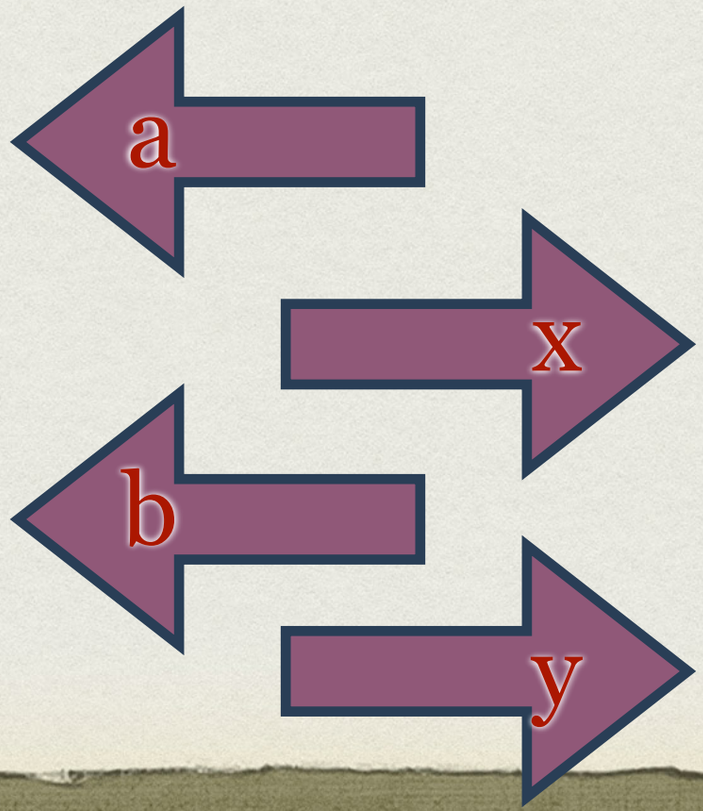


Cohérence

$w \notin L$

$\exists$  , et $\forall$  , $\forall w \notin L$, **Prob**[( : ) accepte] $\leq \epsilon$

w

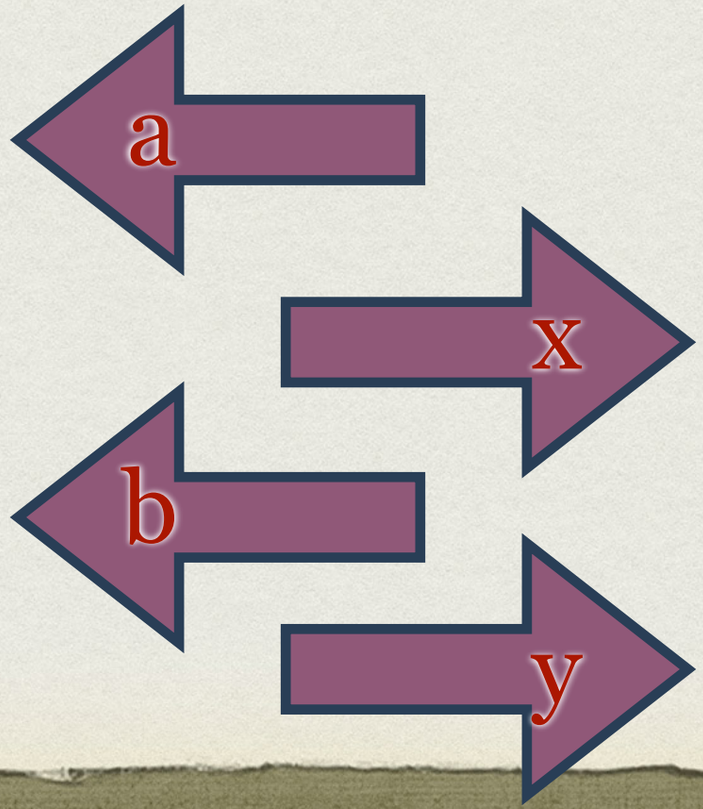


Cohérence

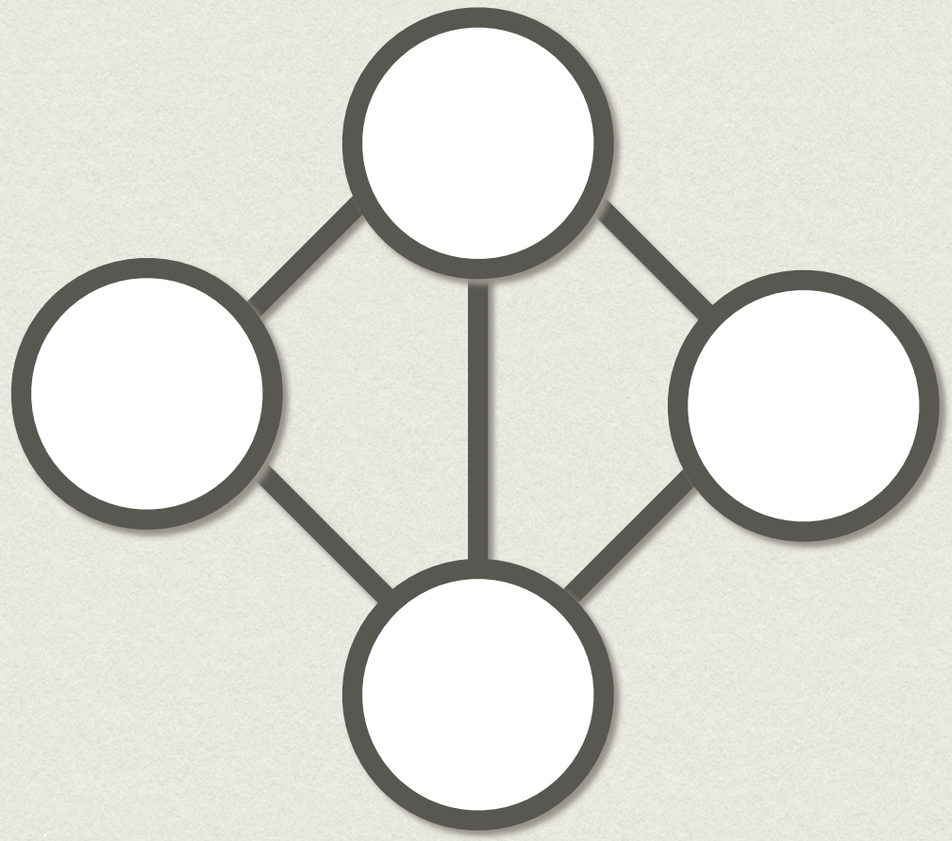
$w \notin L$

$\exists$  , et $\forall$  , $\forall w \notin L$, **Prob**[( : ) accepte] $\leq \epsilon$

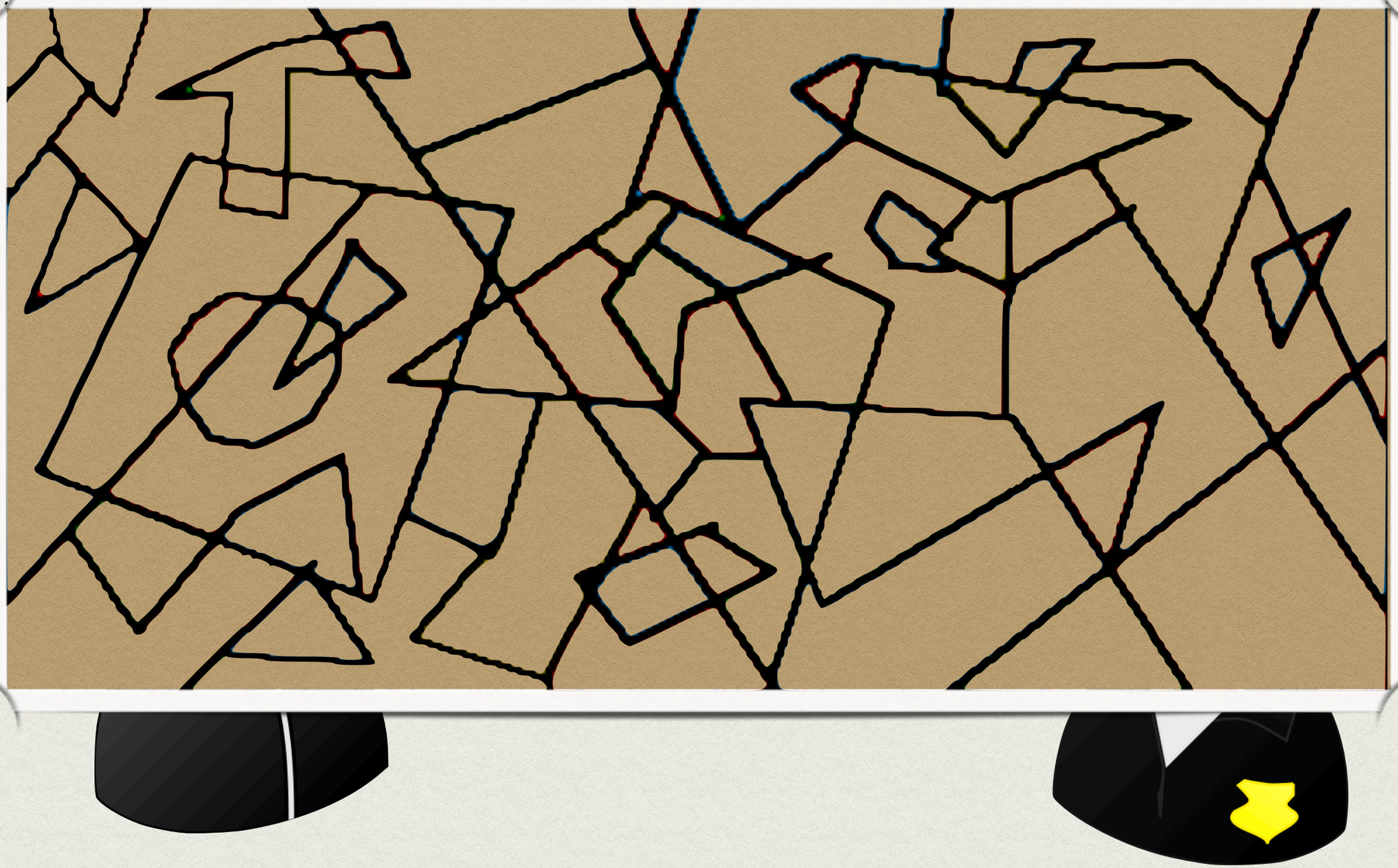
w



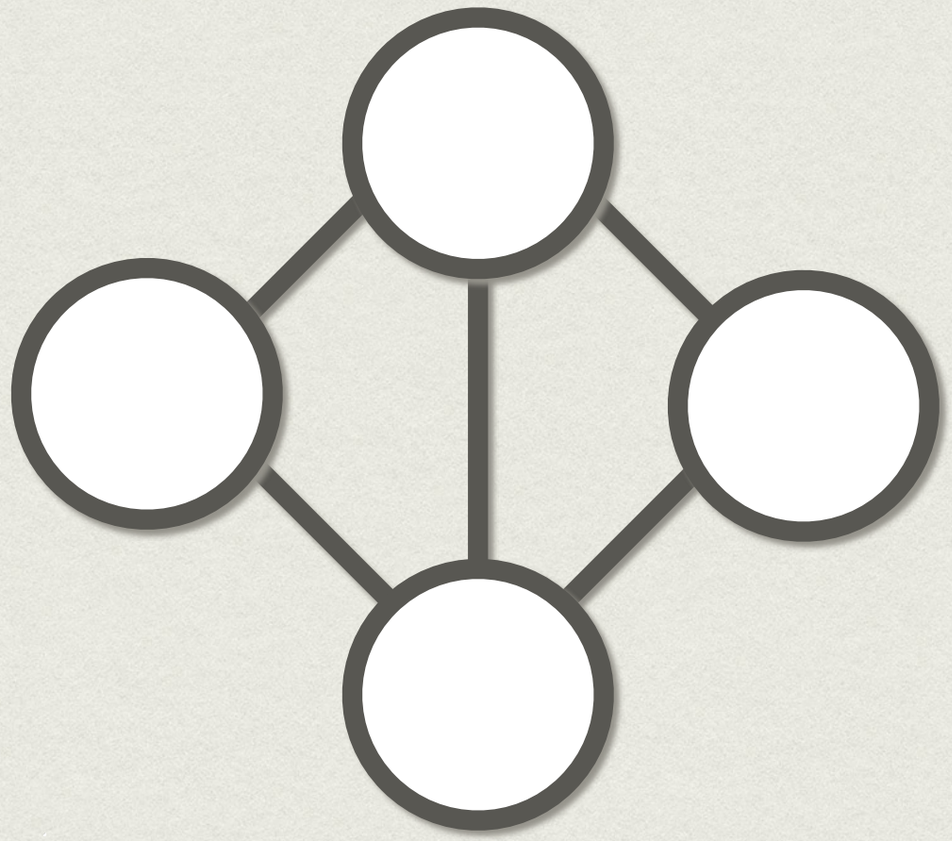
3-COL



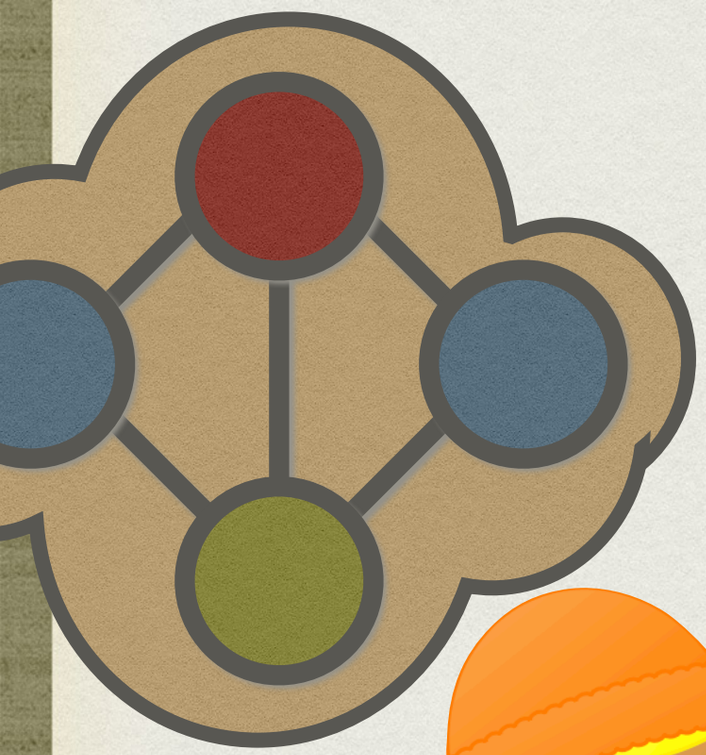
3-COL

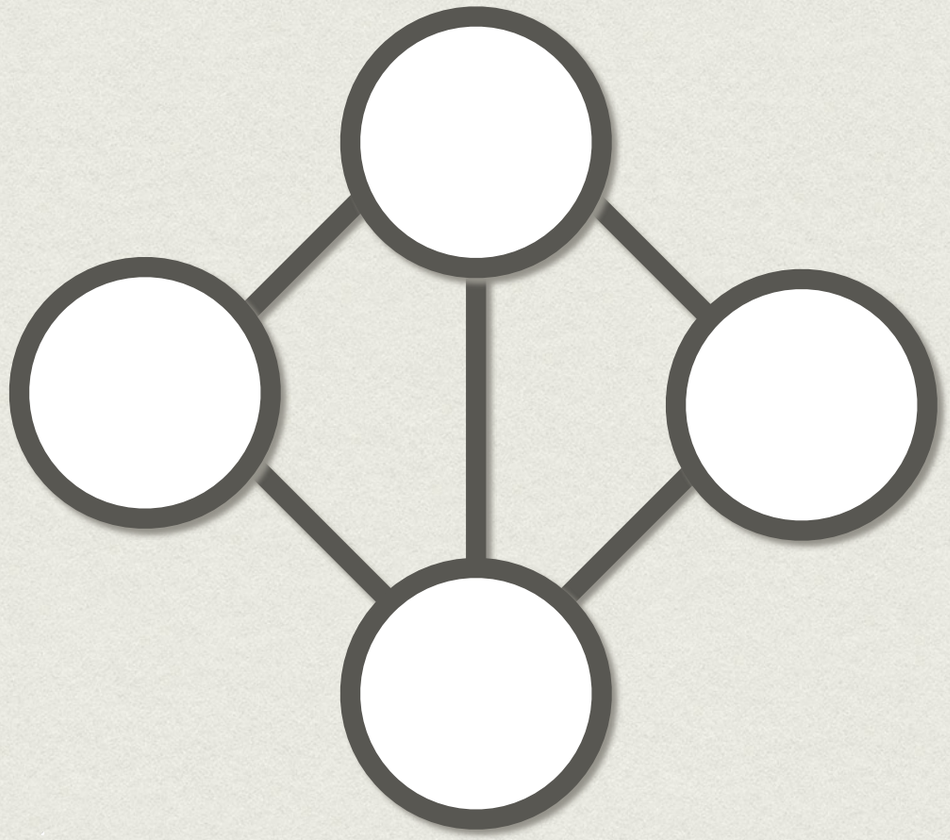


3-COL



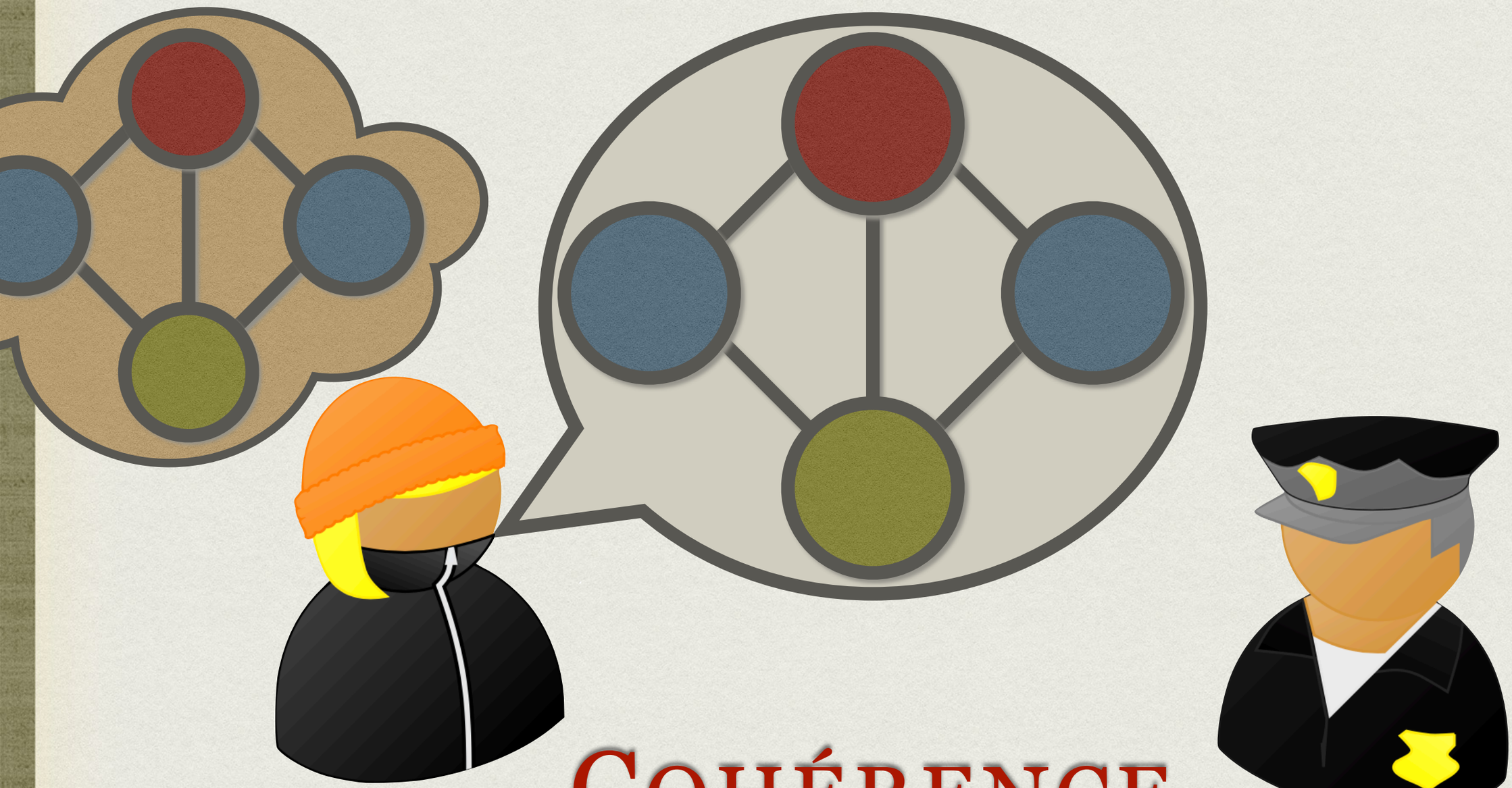
3-COL





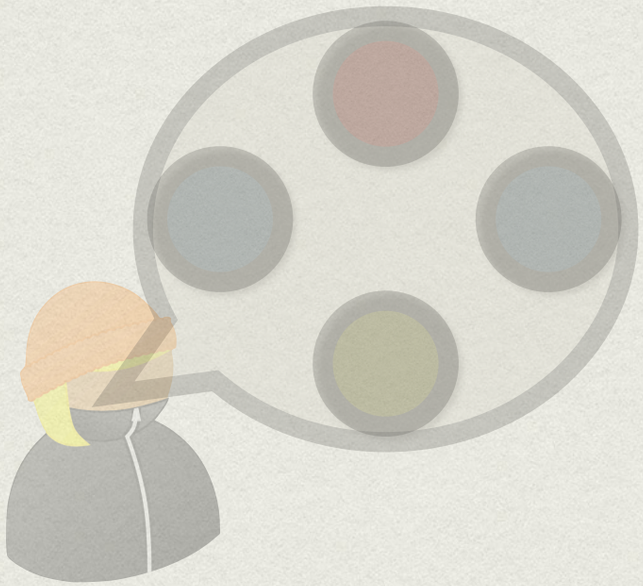
3-COL

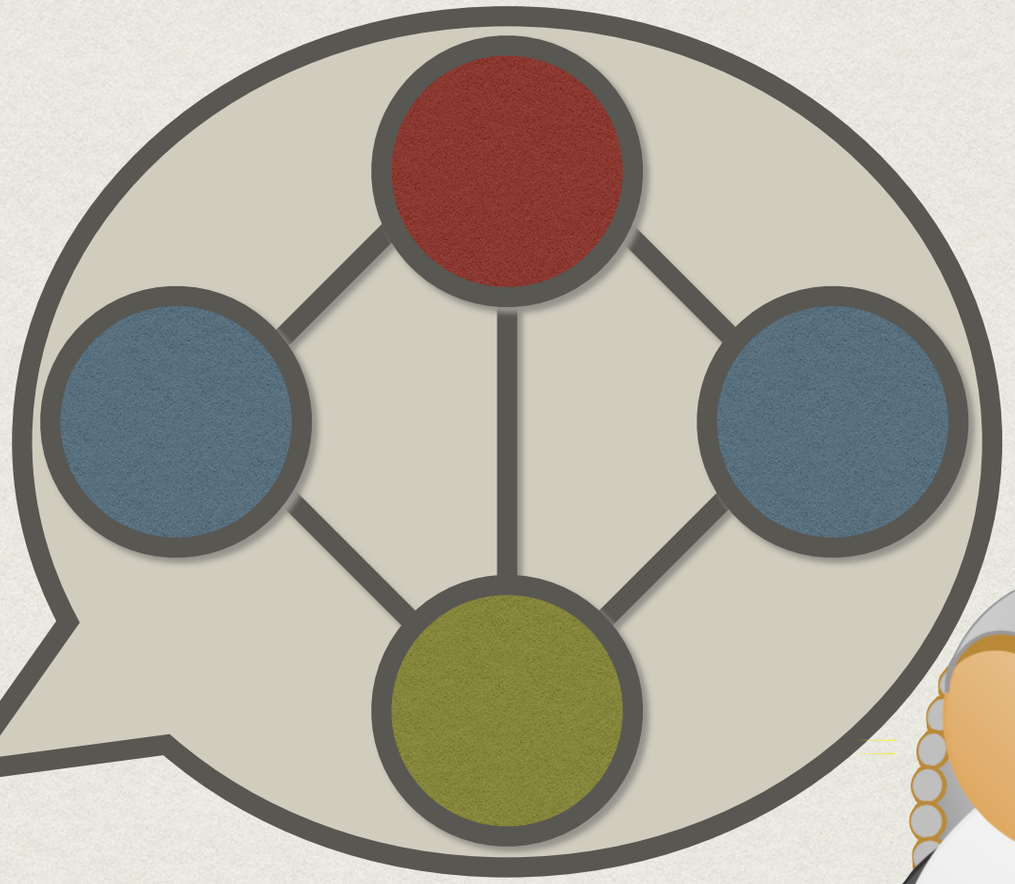
COMPLÉTUDE



COHÉRENCE

3-COL





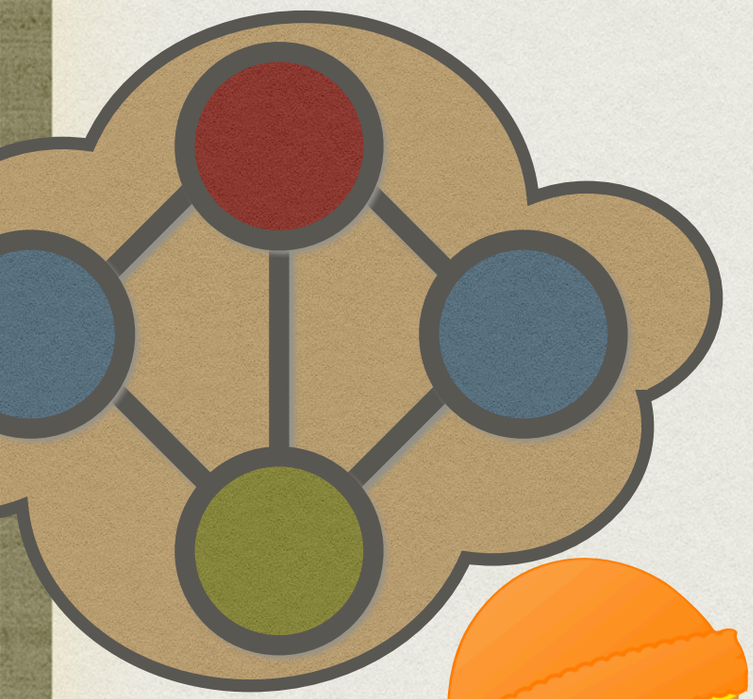
TRANSFÉRABLE

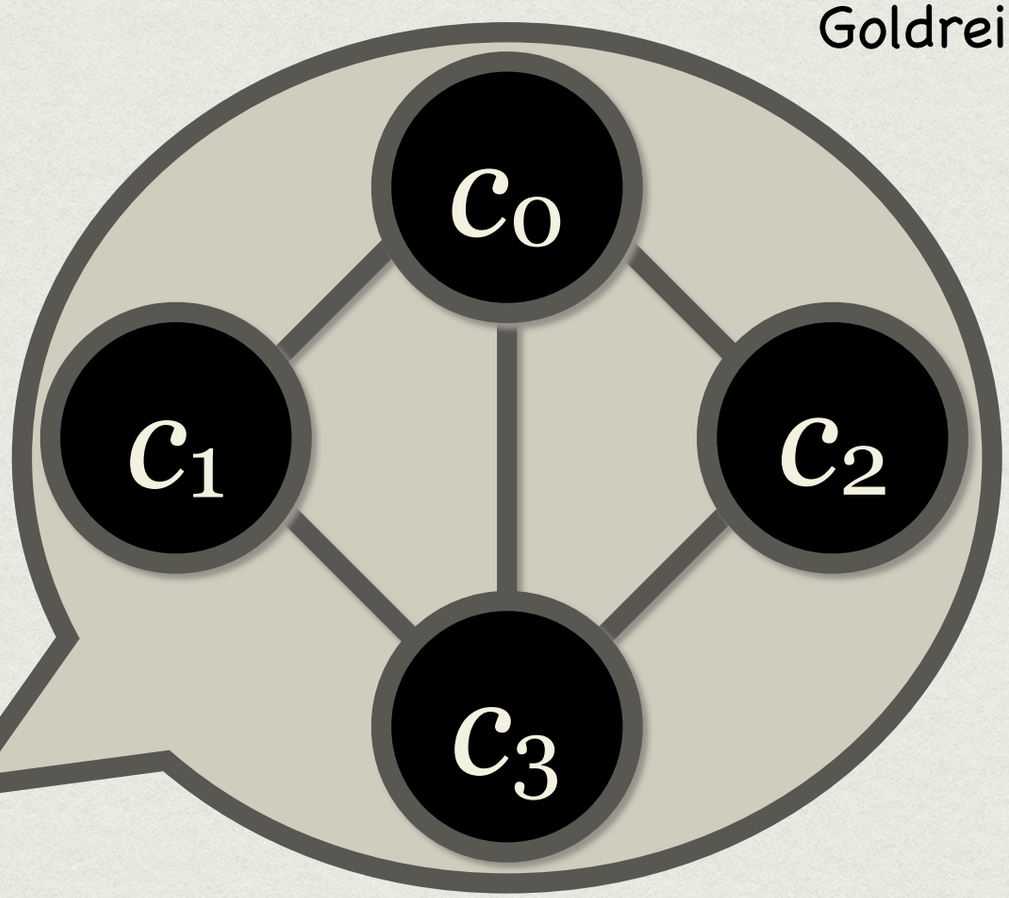
3-COL (86)

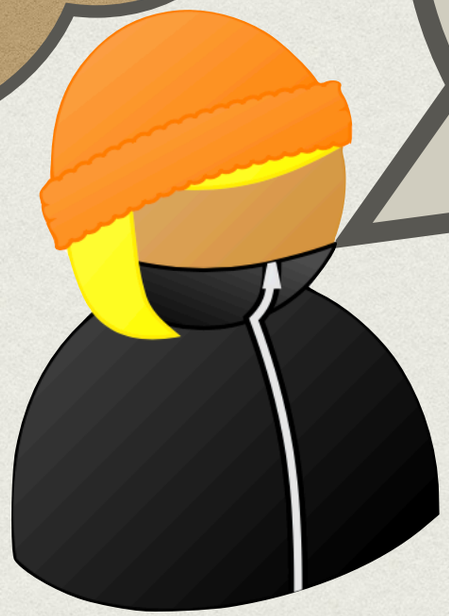

Goldreich


Micali


Wigderson

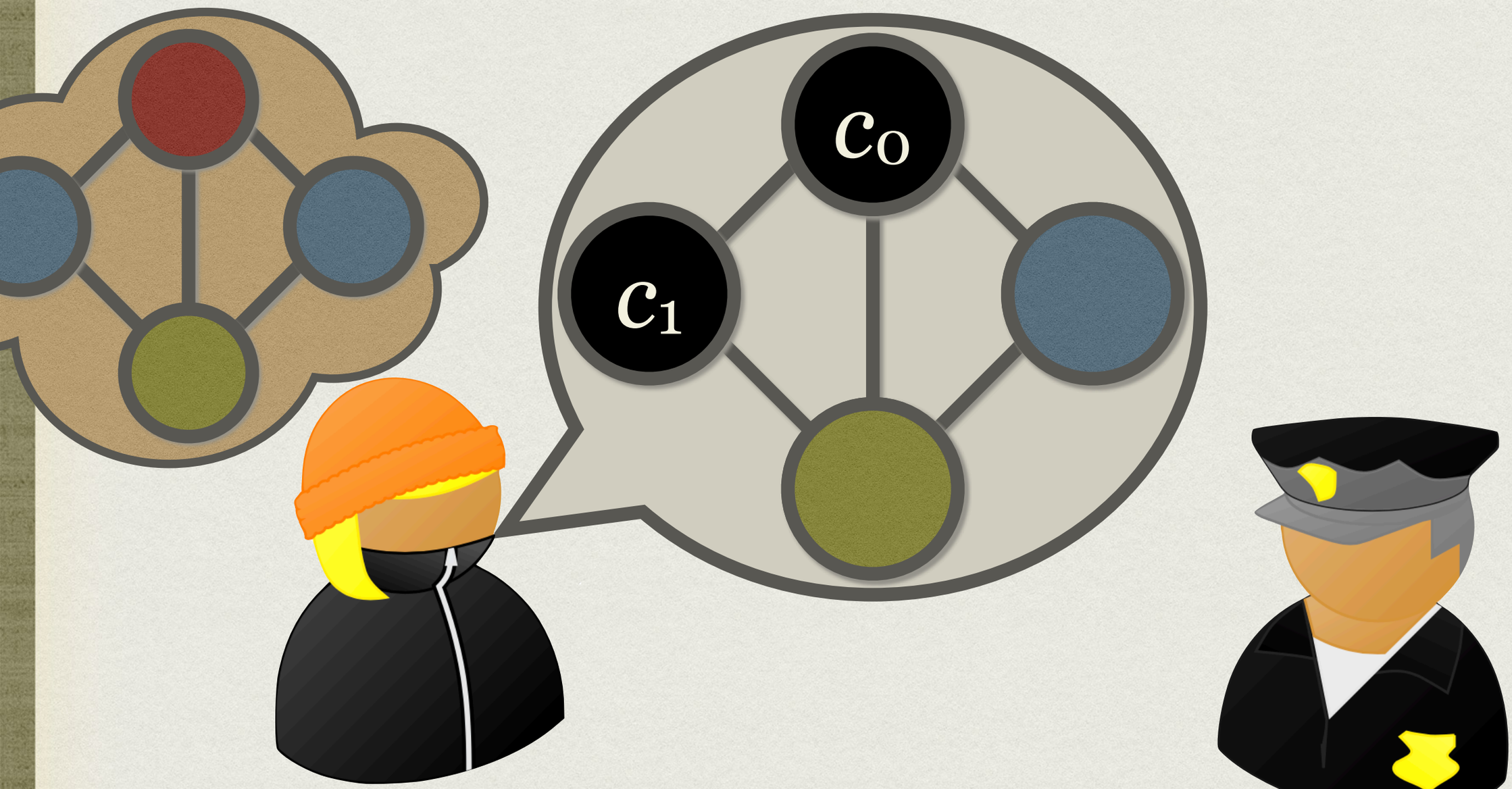




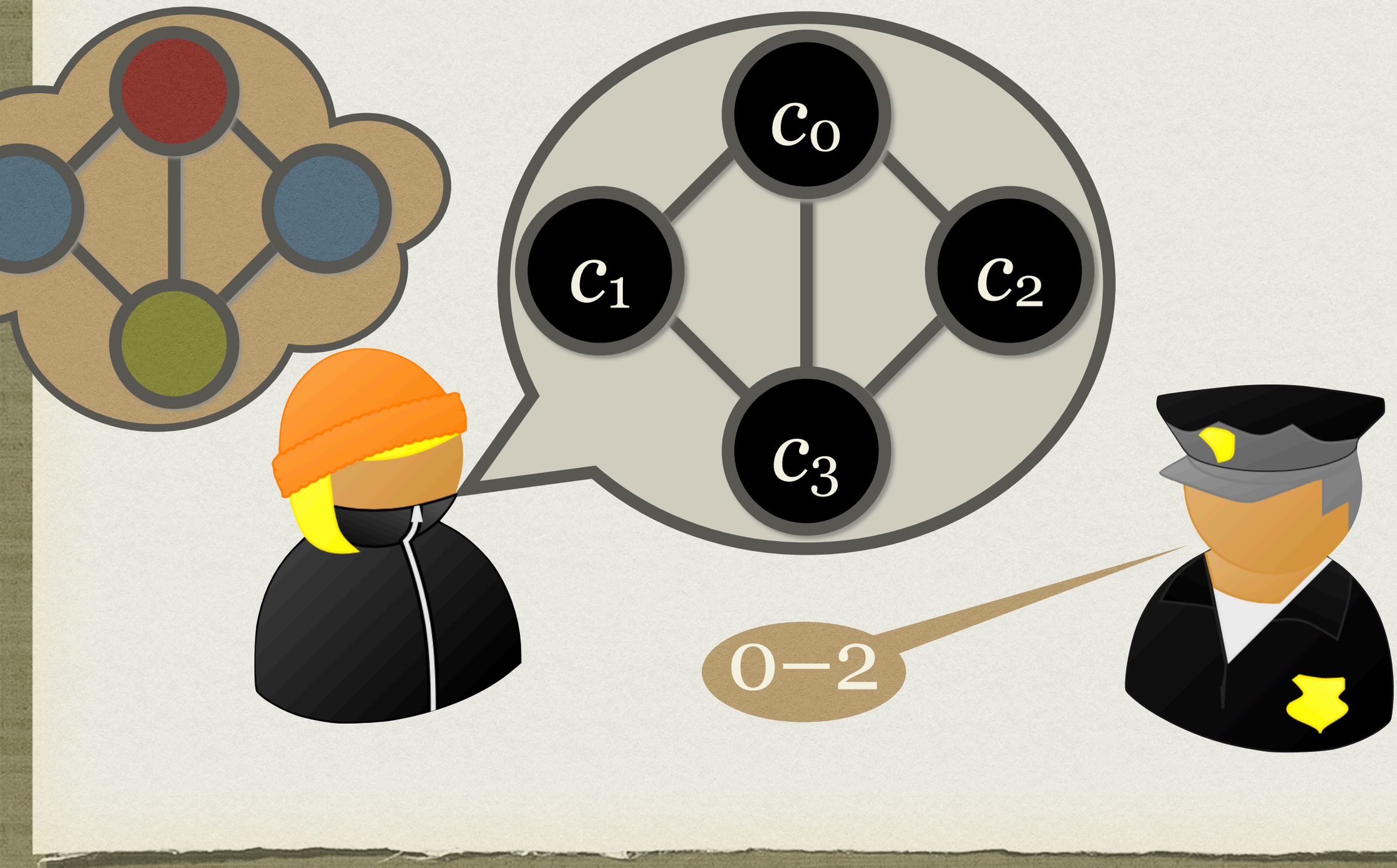


2–3

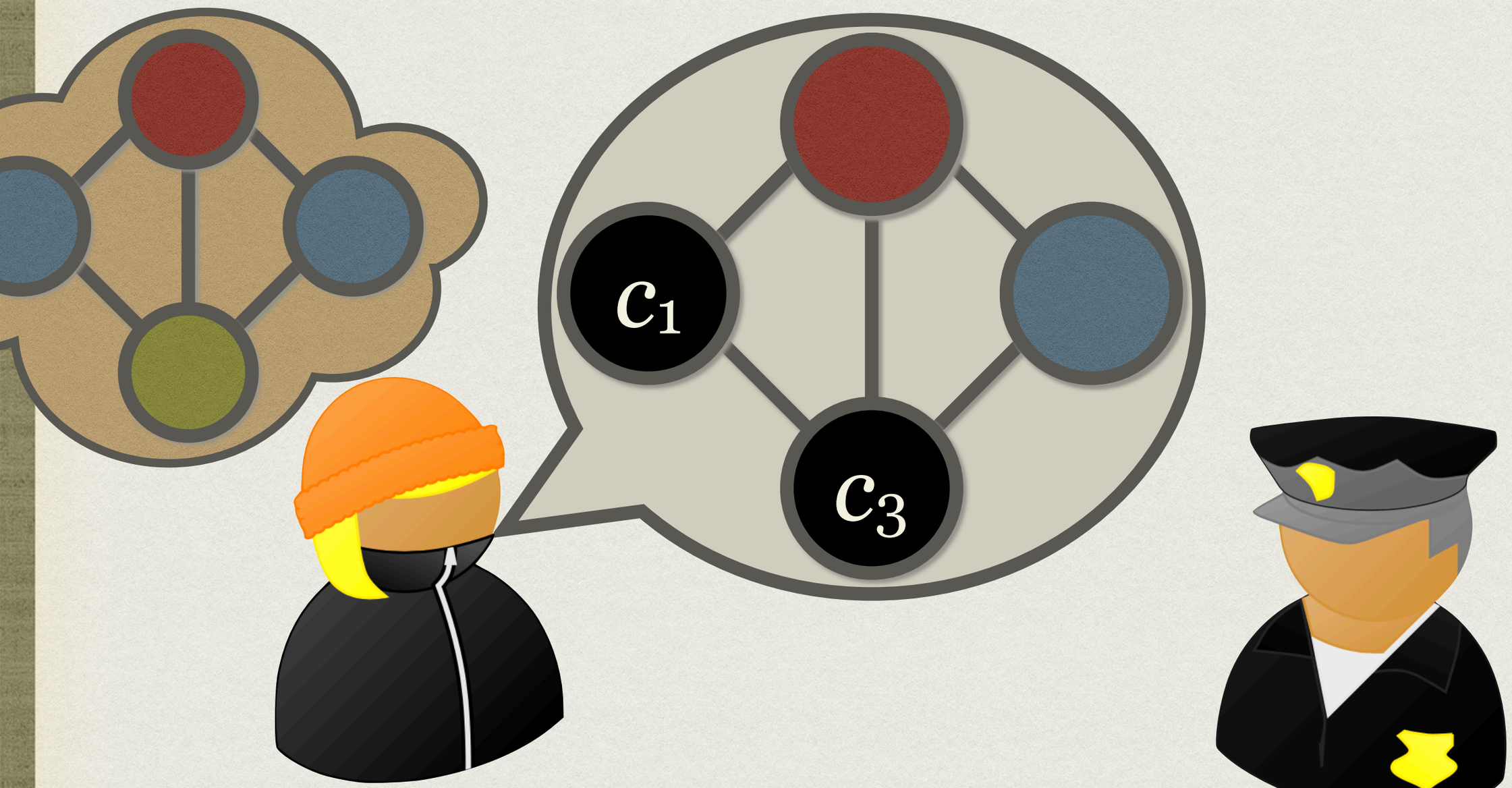
3-COL



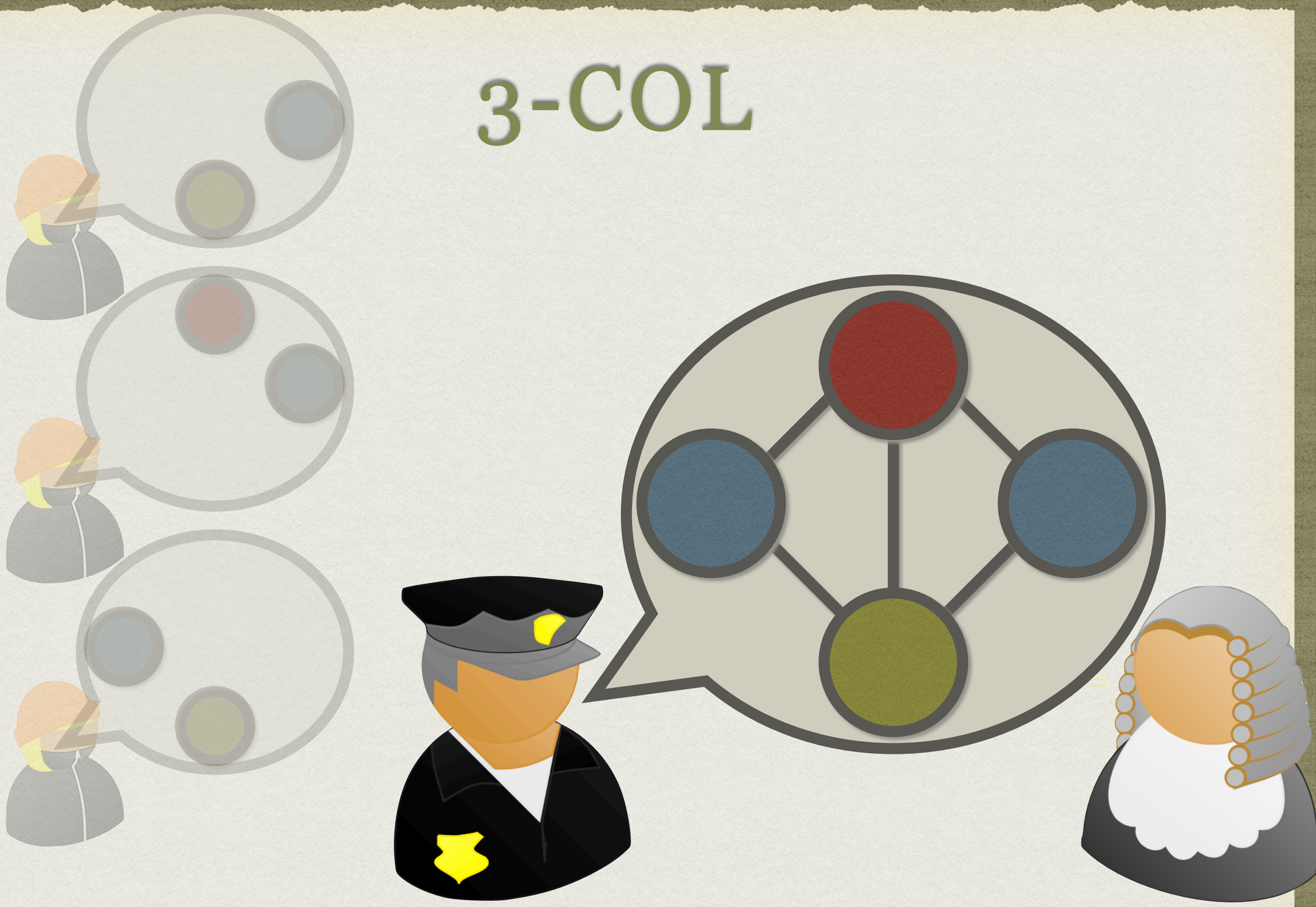
3-COL



3-COL

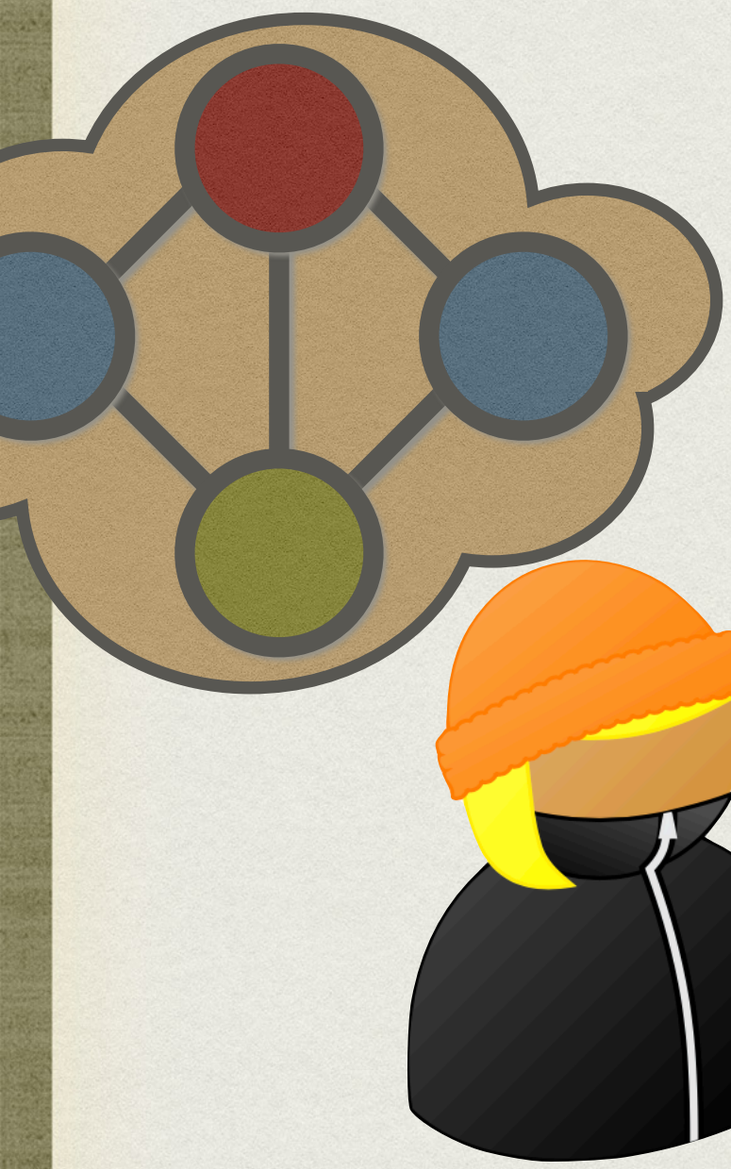


3-COL

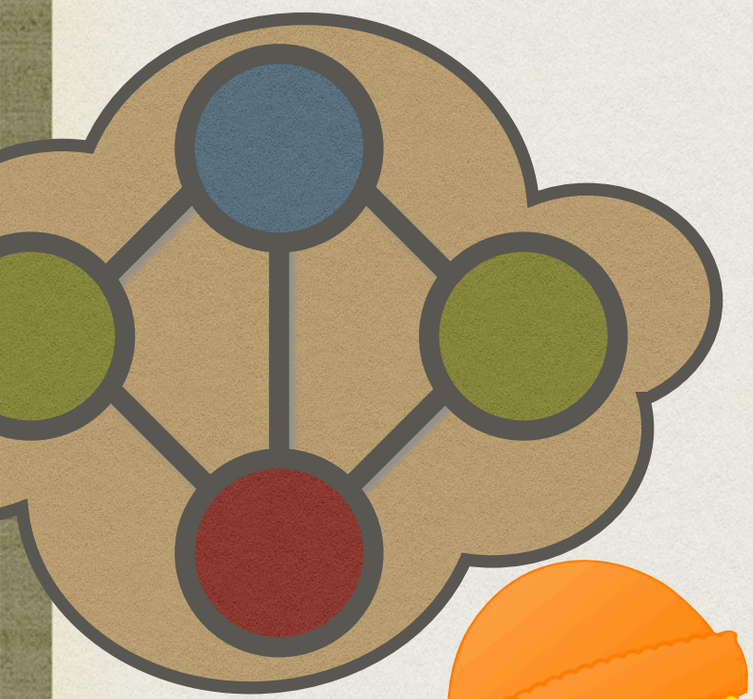


TRANSFÉRABLE

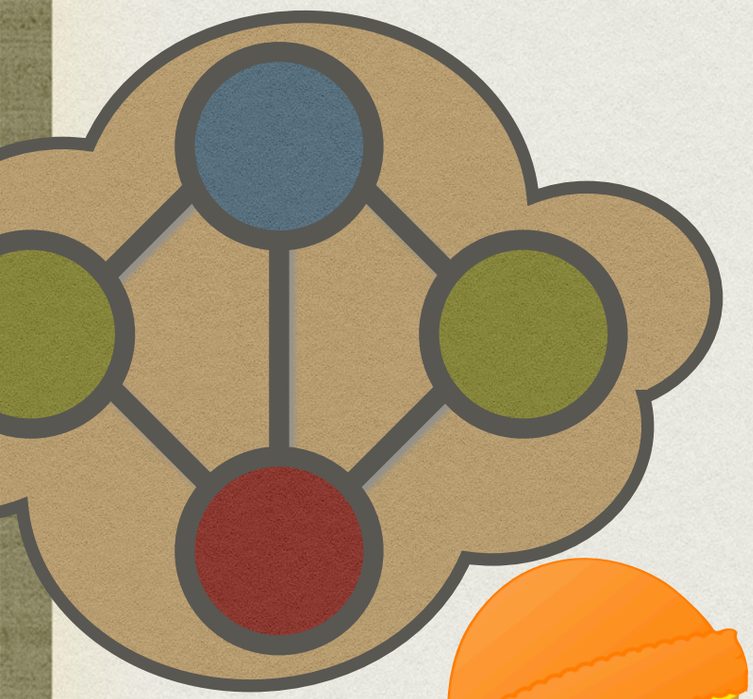
3-COL

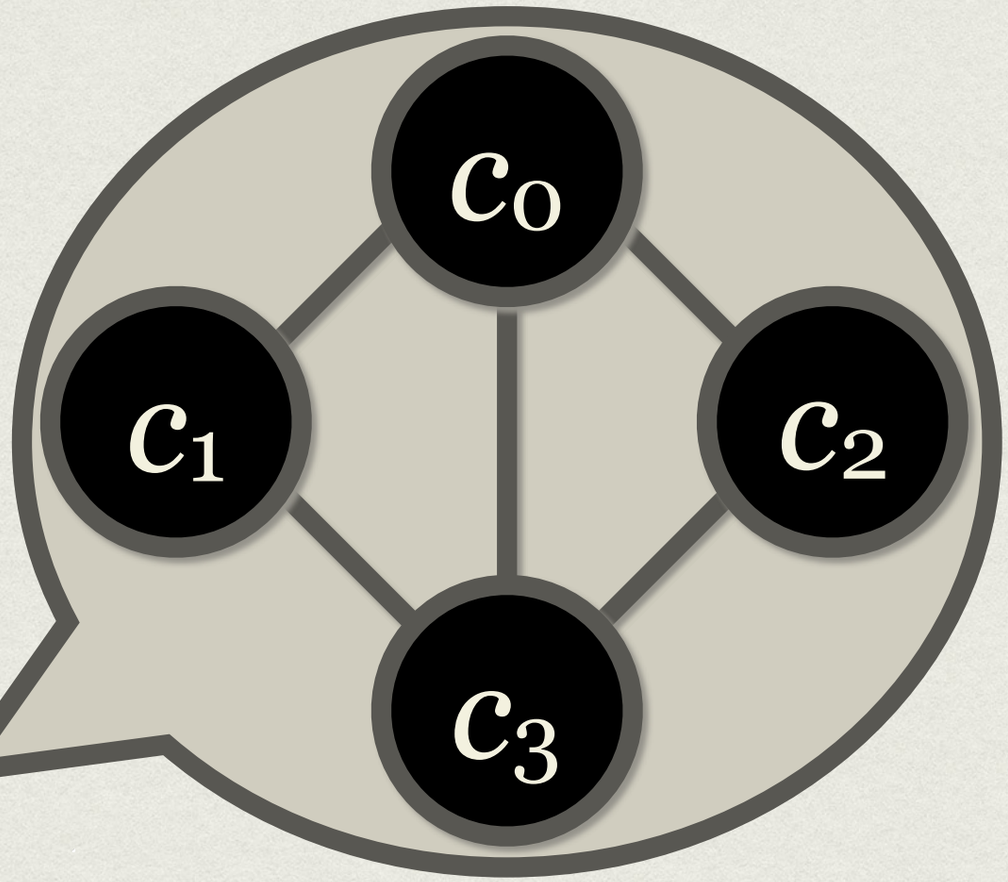


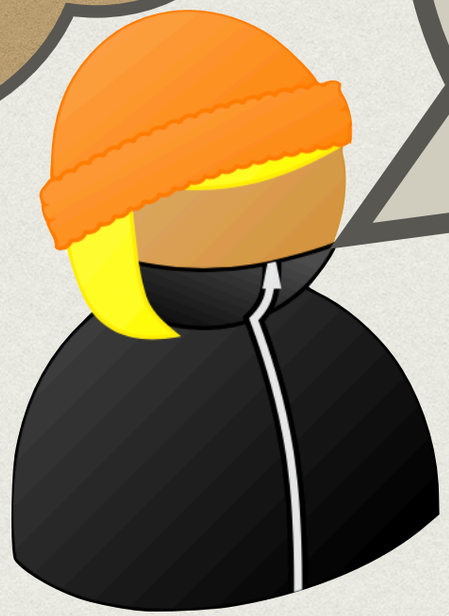
3-COL



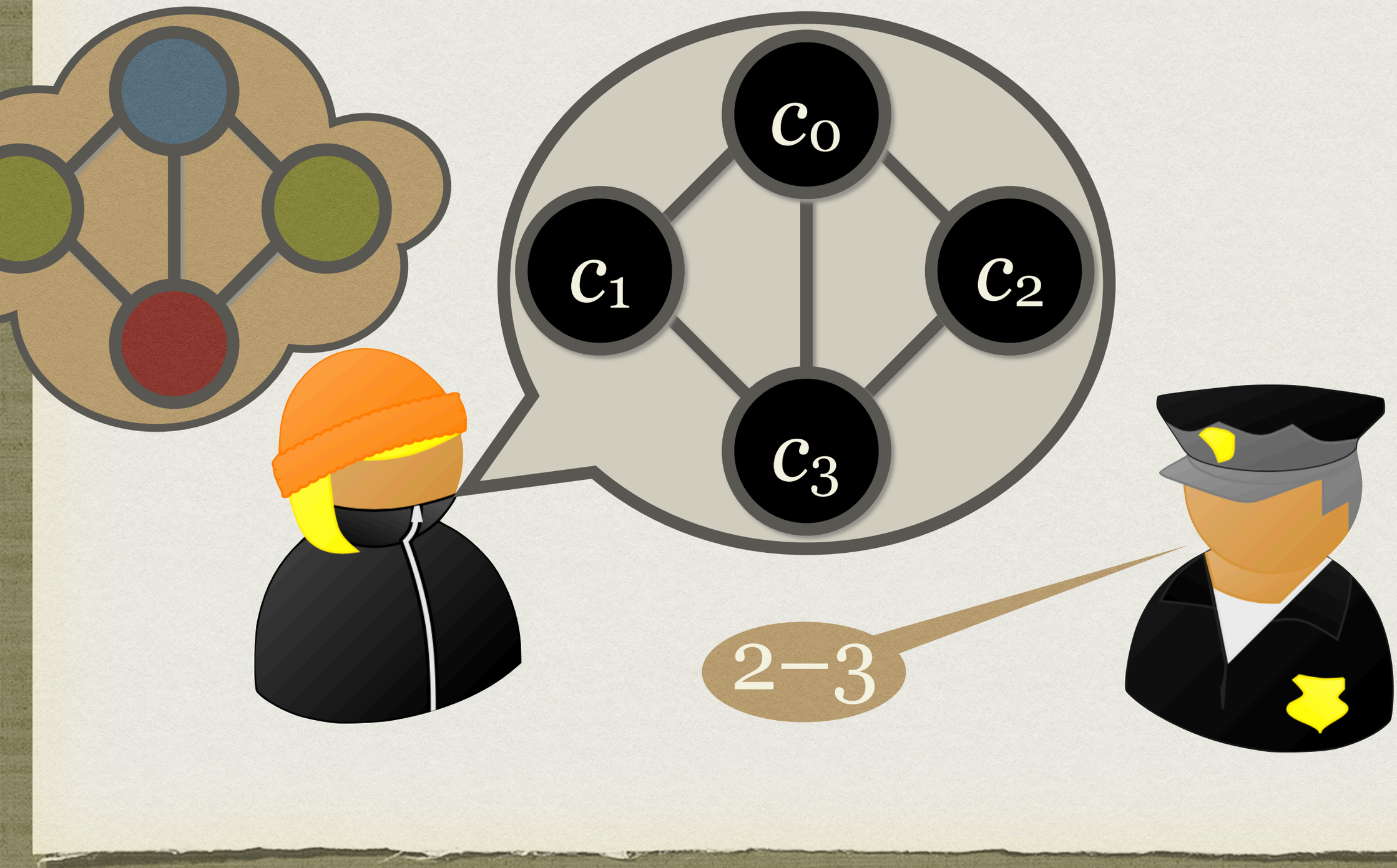
3-COL



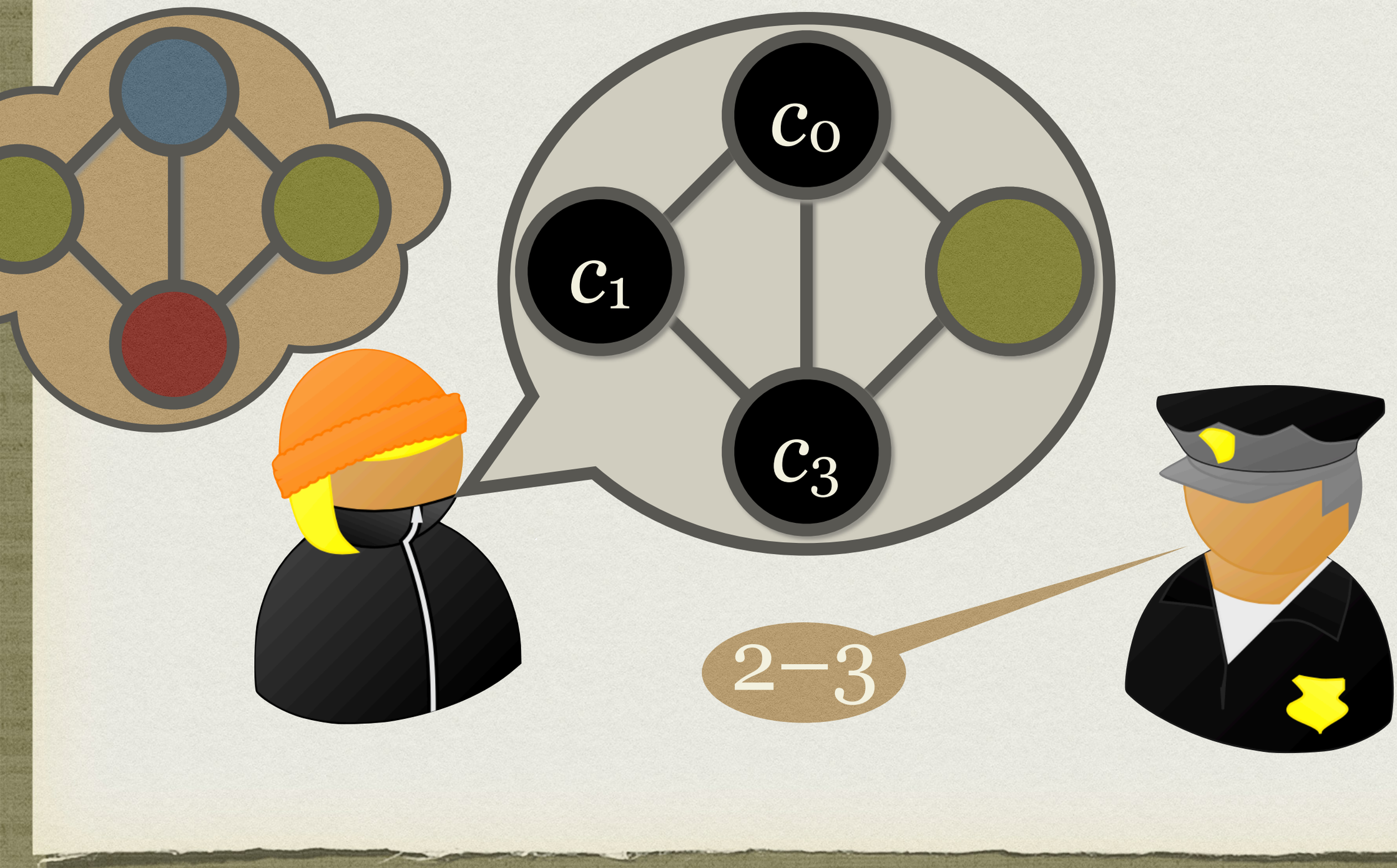




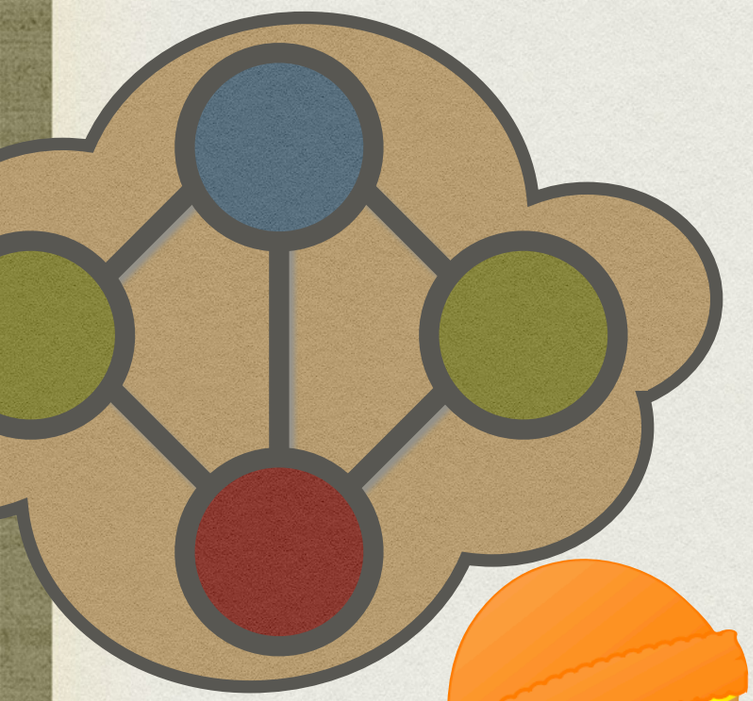
3-COL

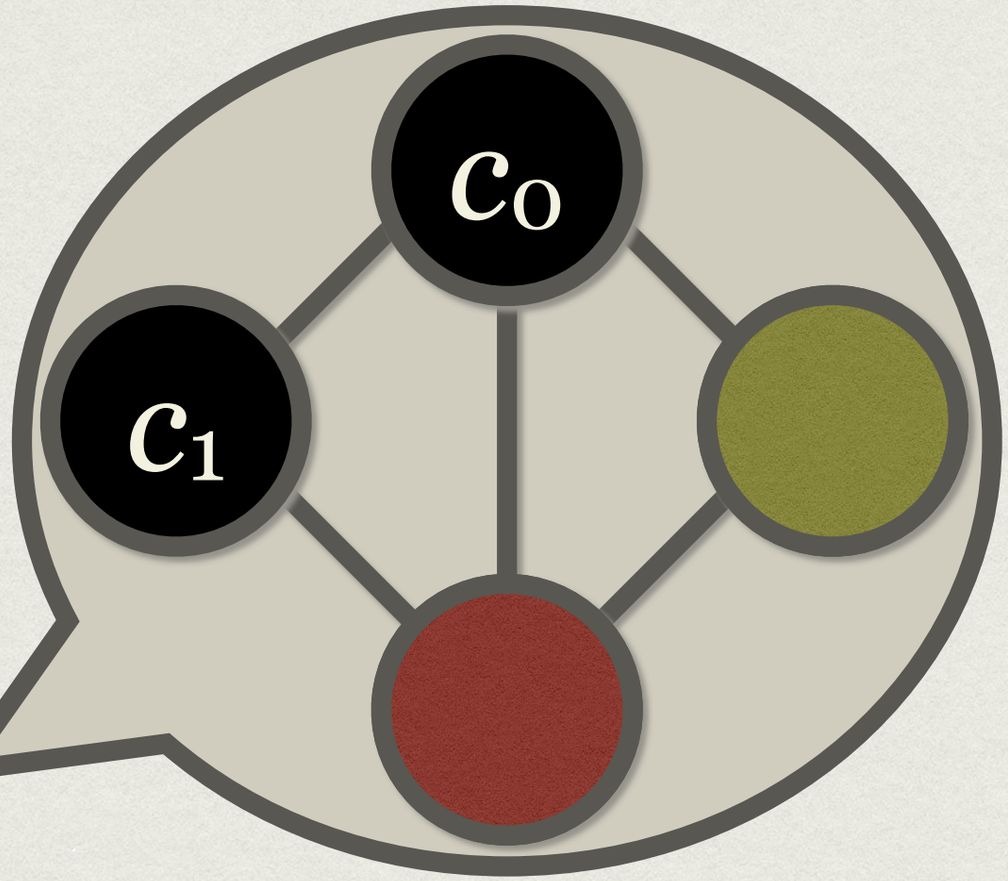


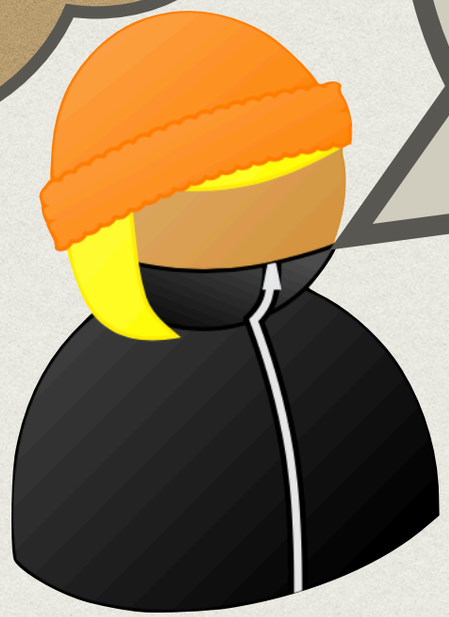
3-COL



3-COL

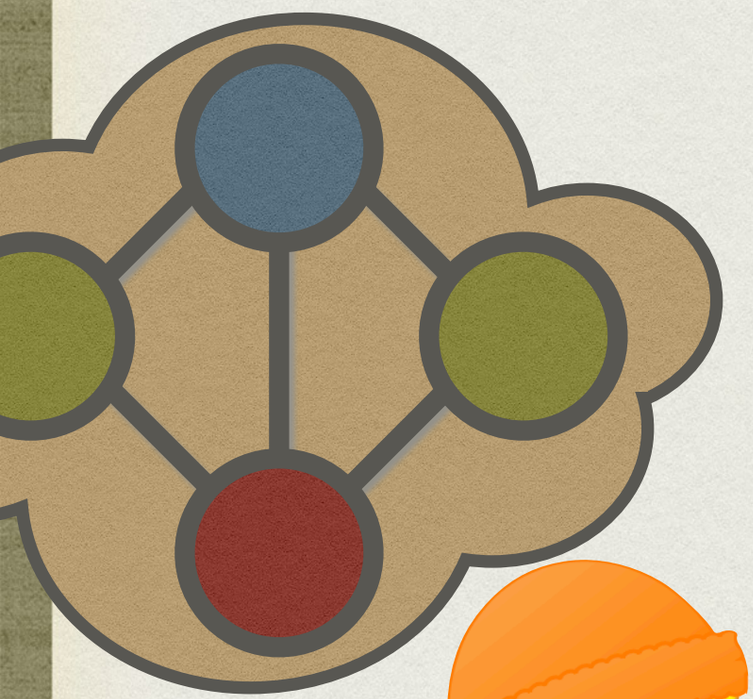




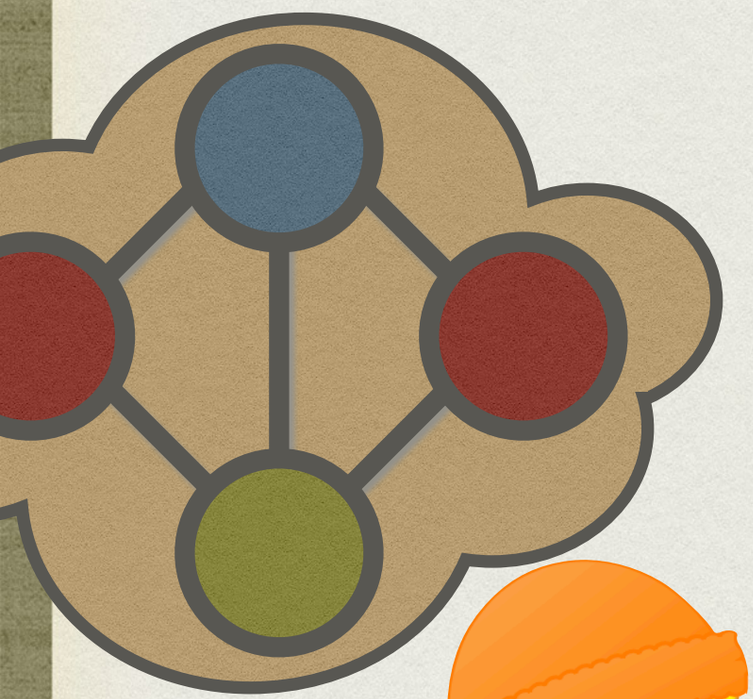


2−3

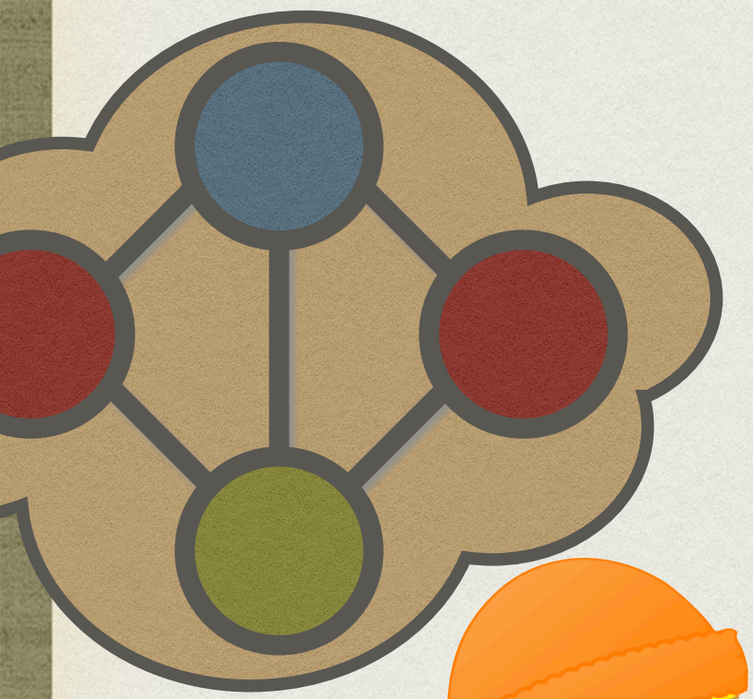
3-COL

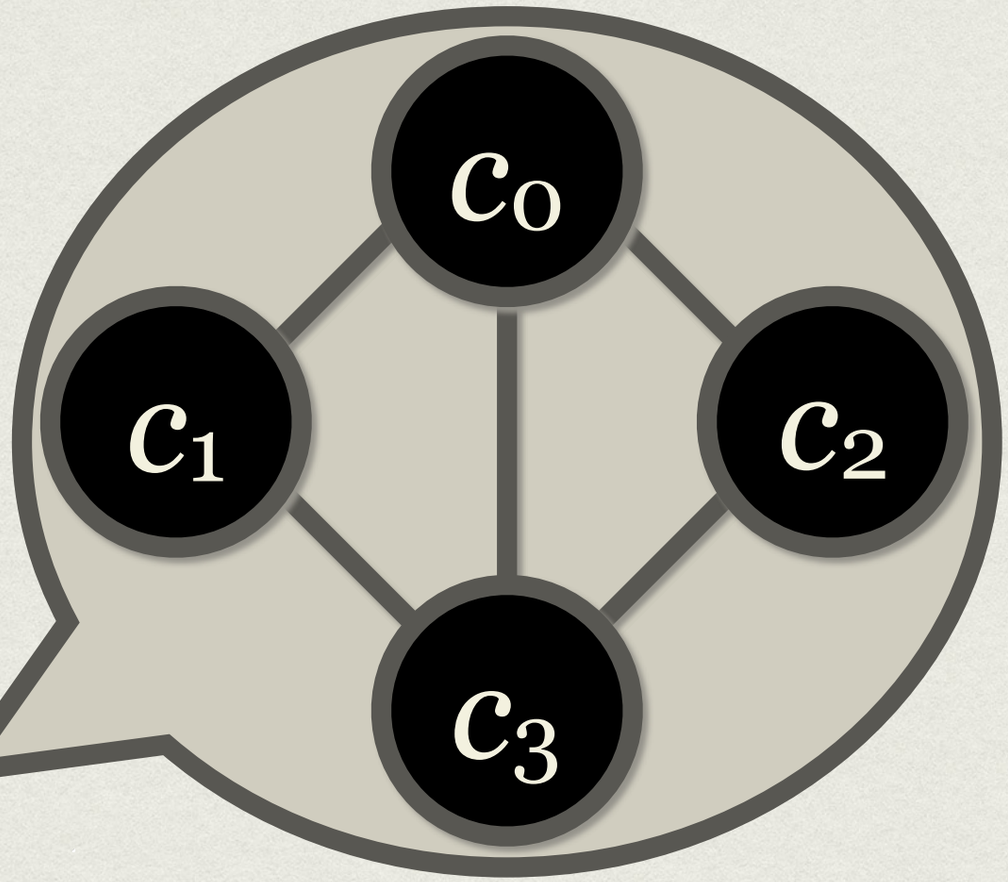


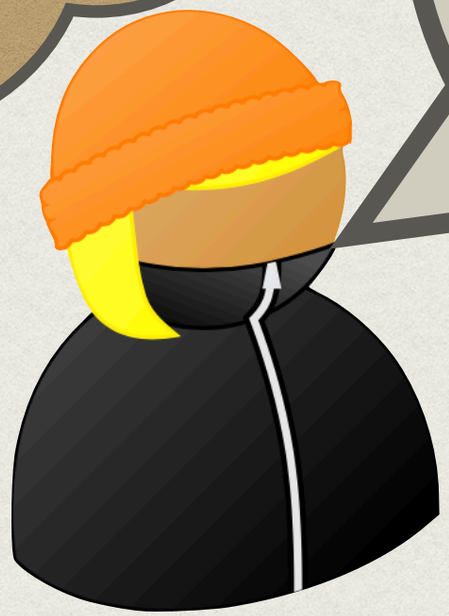
3-COL



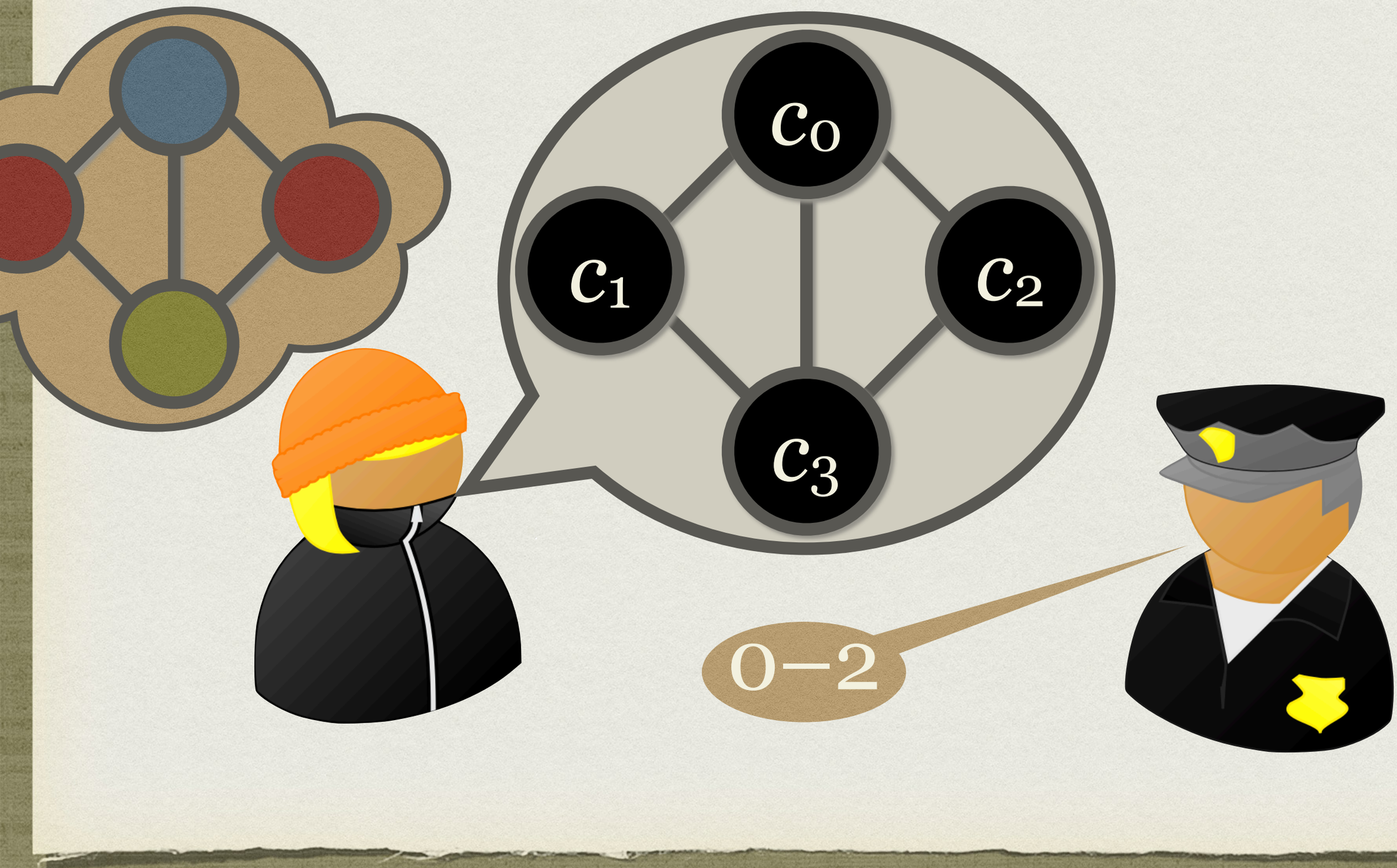
3-COL



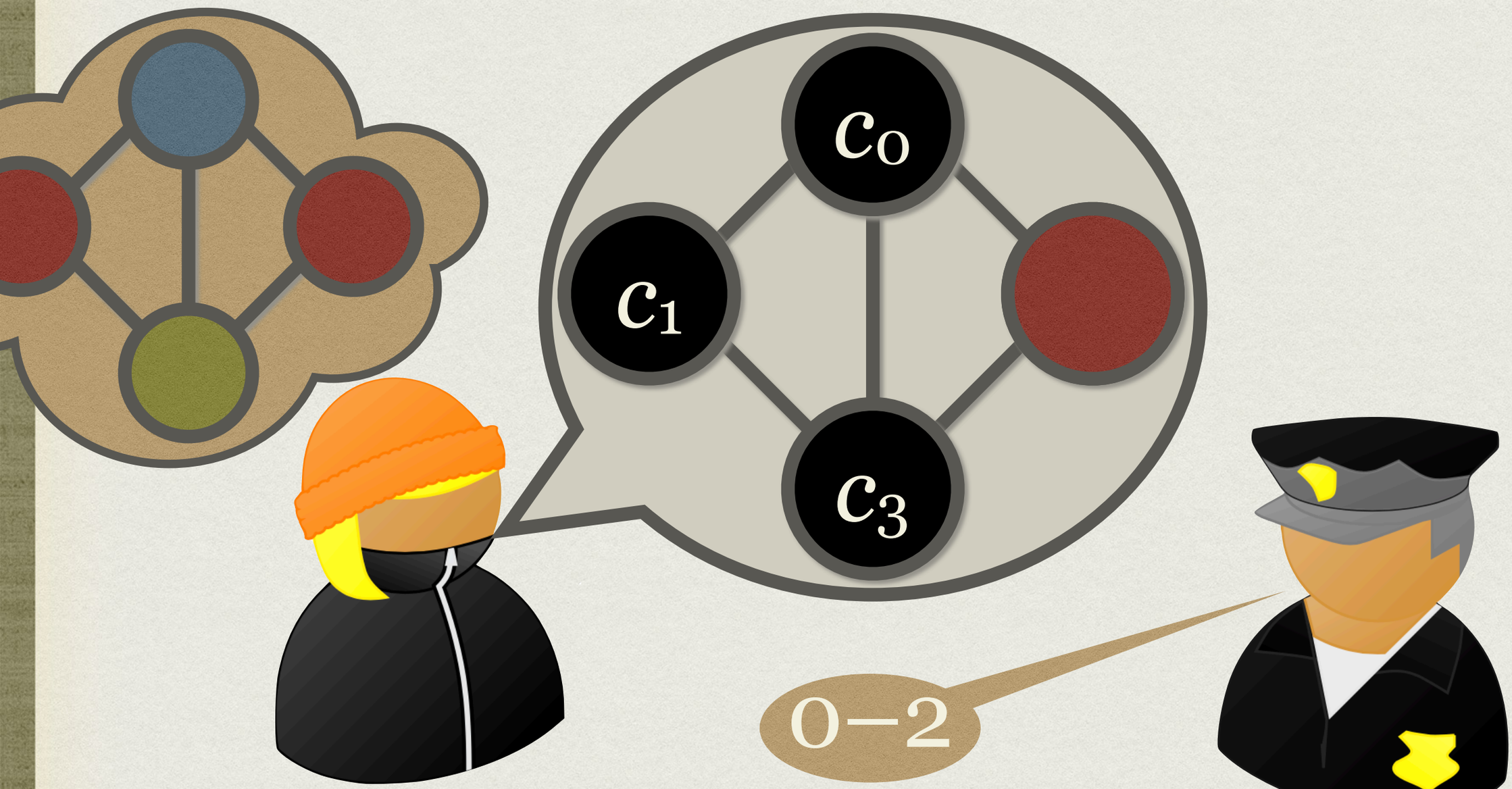




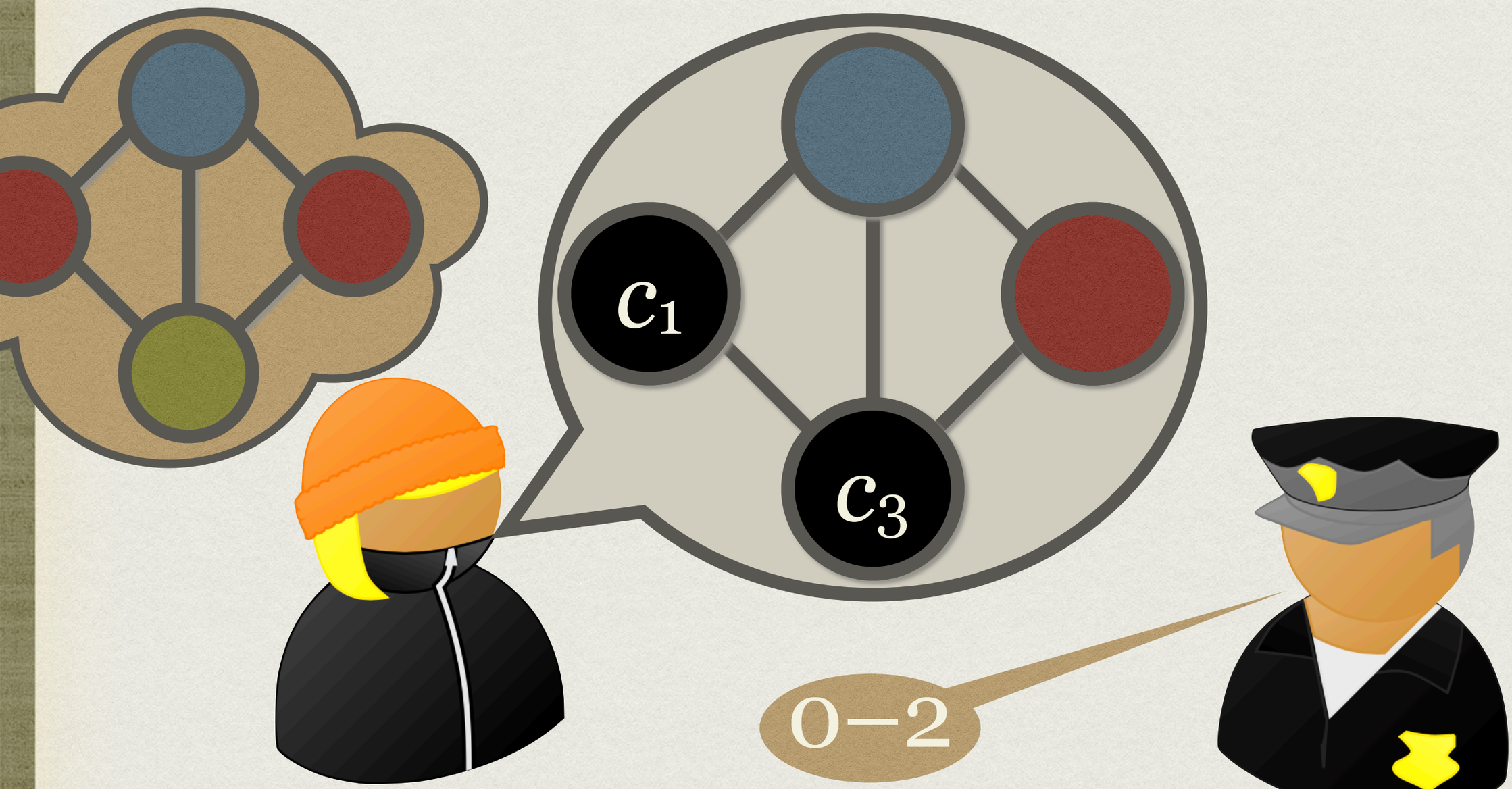
3-COL



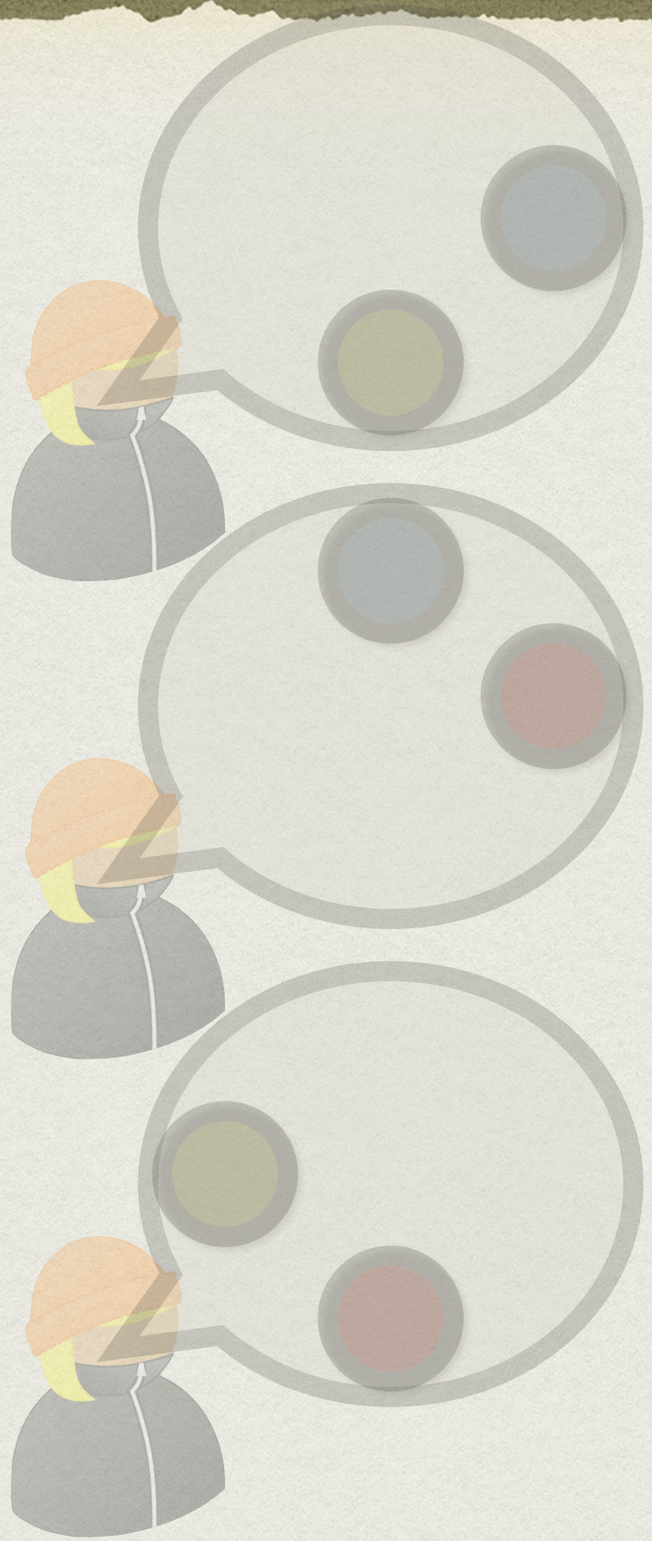
3-COL

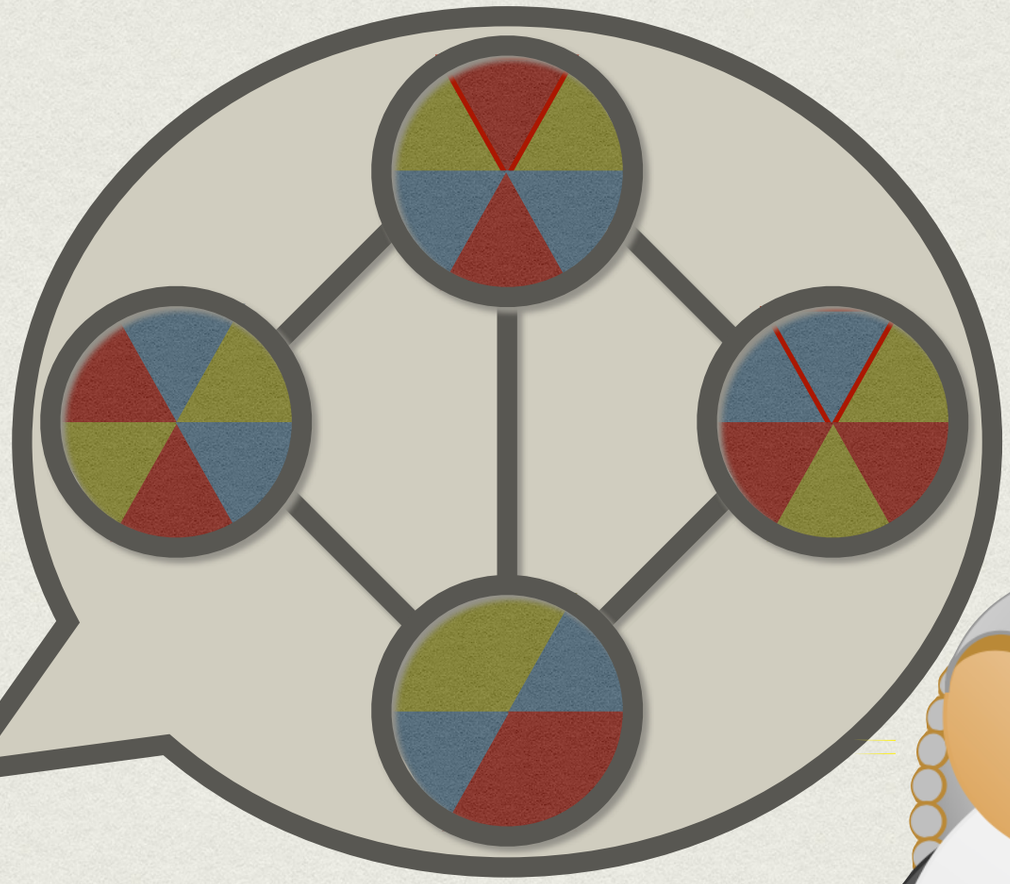


3-COL



3-COL

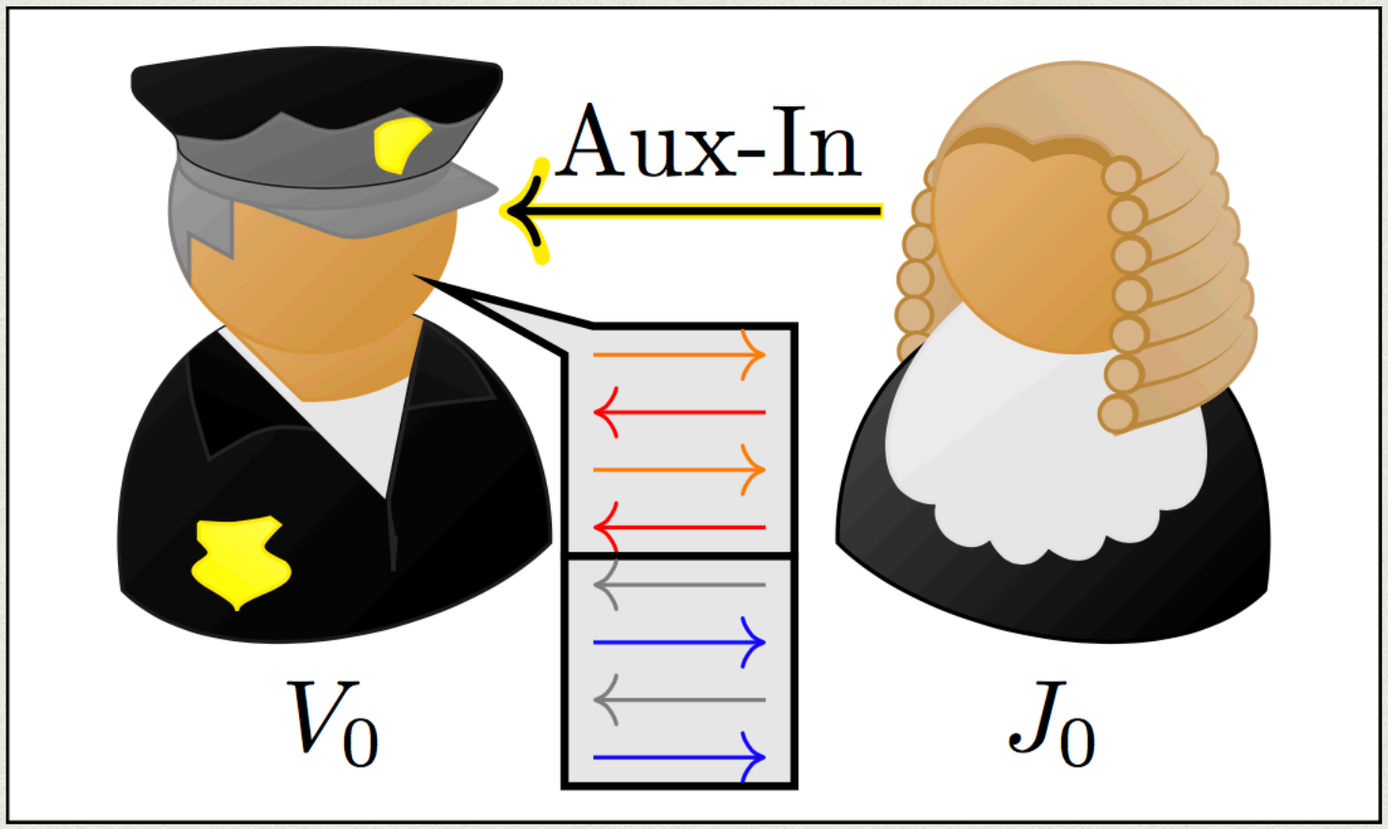




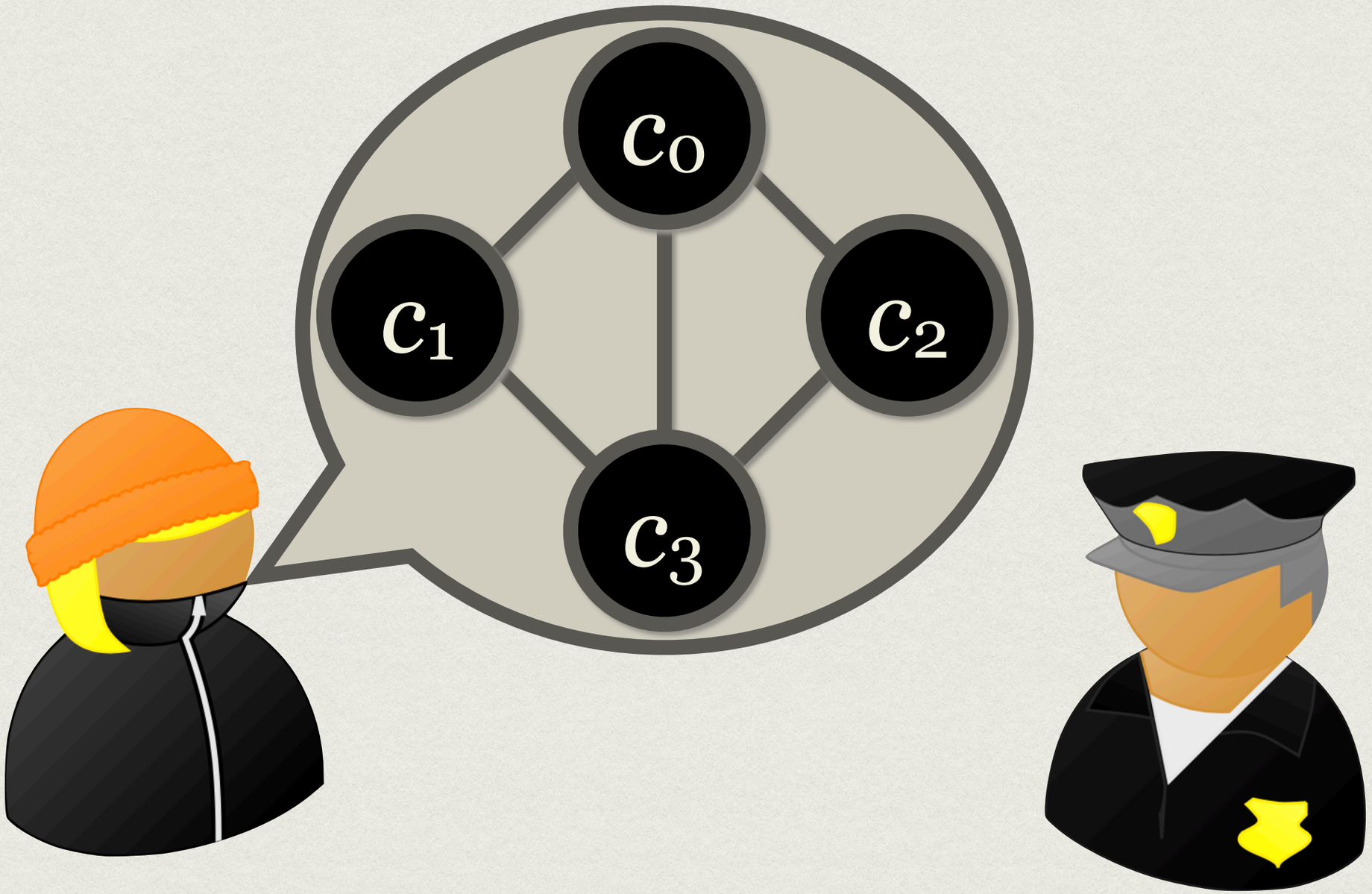
NON TRANSFÉRABLE !

ZERO-KNOWLEDGE

∋ NON TRANSFÉRABLE

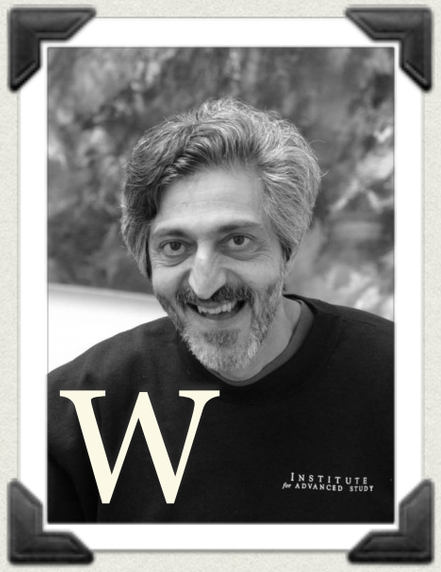


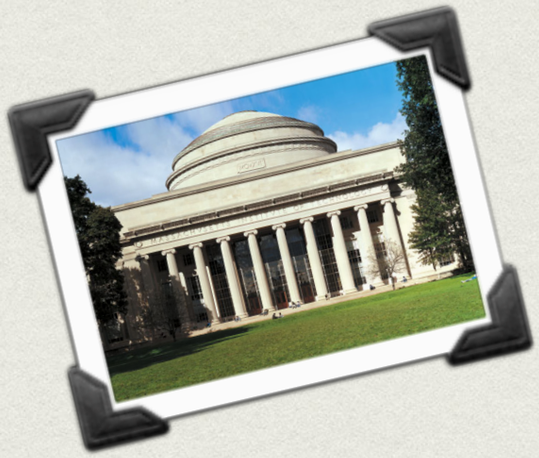
MISE-EN-GAGE ??



INTRODUCTION

(ZK)MIPs





‘88

BGKW88

BGKW88

LEMIP

W

$$$$

$\exists$  , $\exists$  ,  , $\forall w \in L$,

Prob[( :  : ) accepte] $\geq 1 - \epsilon$

a

b

X

Y

W

$$

$$

$\exists$  , $\exists$  ,  , $\forall w \in L$,

Prob[( :  : ) accepte] $\geq 1 - \epsilon$

w∈L

a

b

X

Y

W

$$

$$

$\exists$  , $\exists$  ,  , $\forall w \in L$,

Prob[( :  : ) accepte] $\geq 1 - \epsilon$

accepte $w \in L$

a

b

X

Y

W

$$

$$

$\exists$  ,

et $\forall$  ,  , $\forall w \notin L$,

Prob[( :  : ) accepte] $\leq \epsilon$

a

b

X

Y

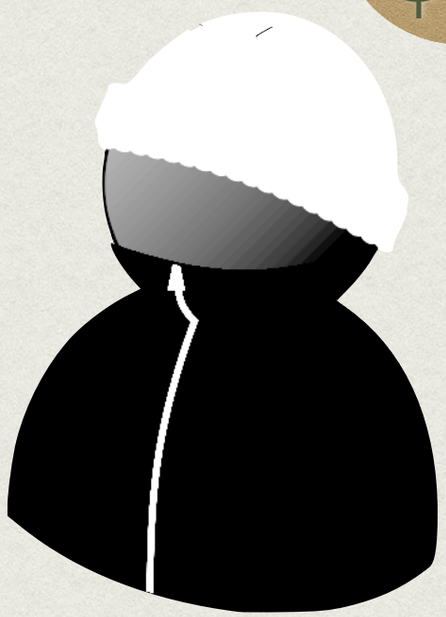
W

$$$$

$$$$

$$$$

$$$$



$\exists$  ,

et $\forall$  ,  , $\forall w \notin L$,

Prob[( :  :  **)** accepte] $\leq \epsilon$

w∉L

a

b

X

Y

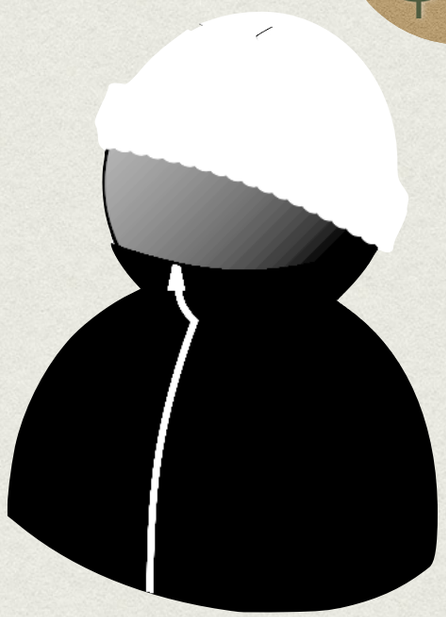
W

$$$$

$$$$

$$$$

$$$$



$\exists$  ,

et $\forall$  ,  , $\forall w \notin L$,

Prob[( :  : ) accepte] $\leq \epsilon$

rejète w$\notin$L

a

b

x

y

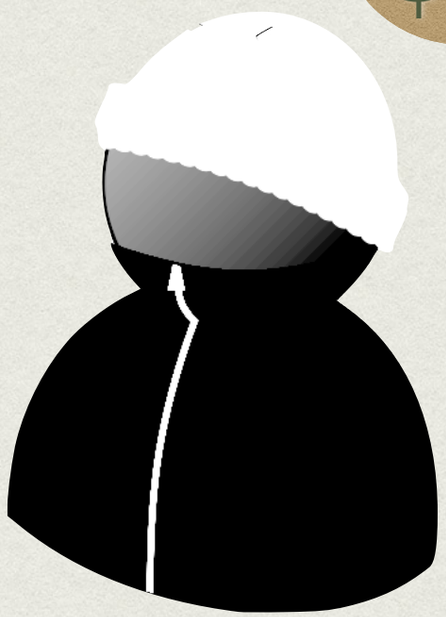
w

$$$$

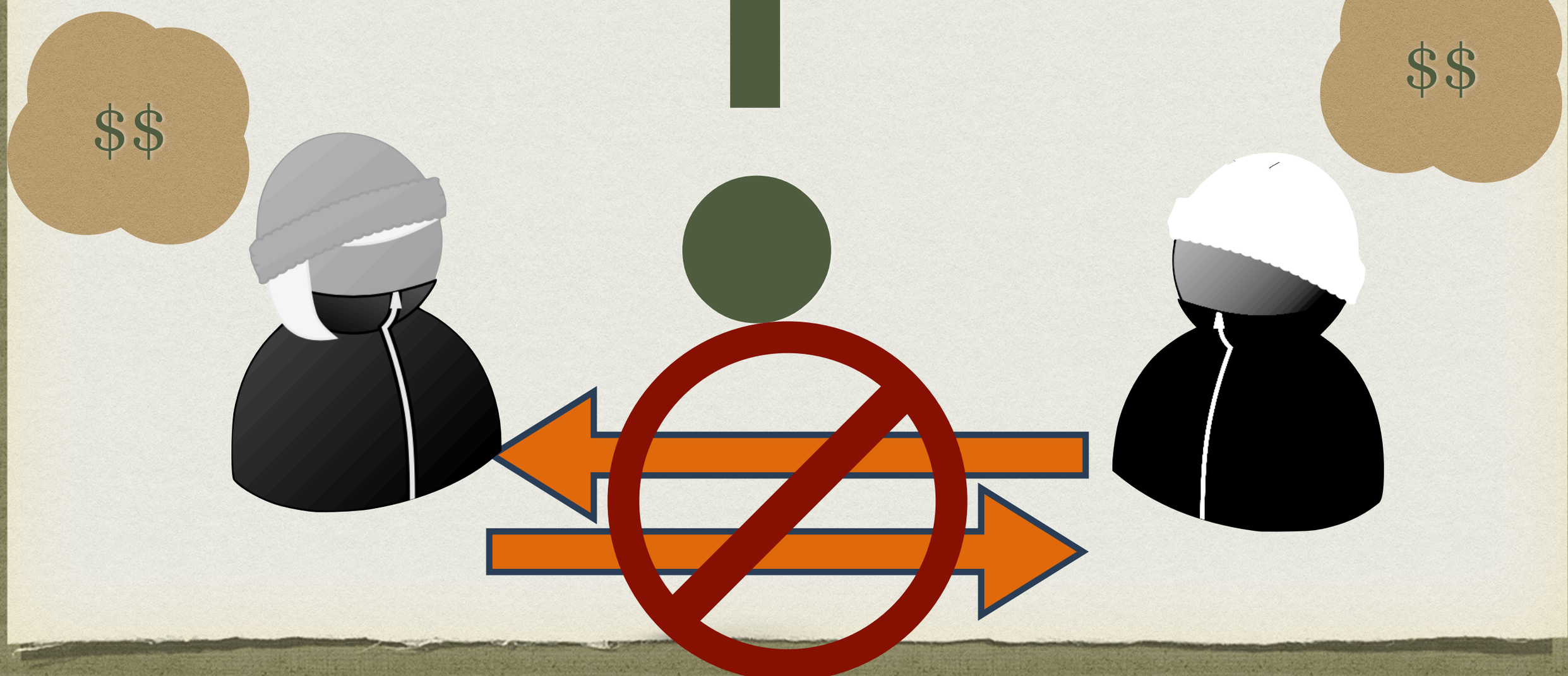
$$$$

$$$$

$$$$



B?KW?8

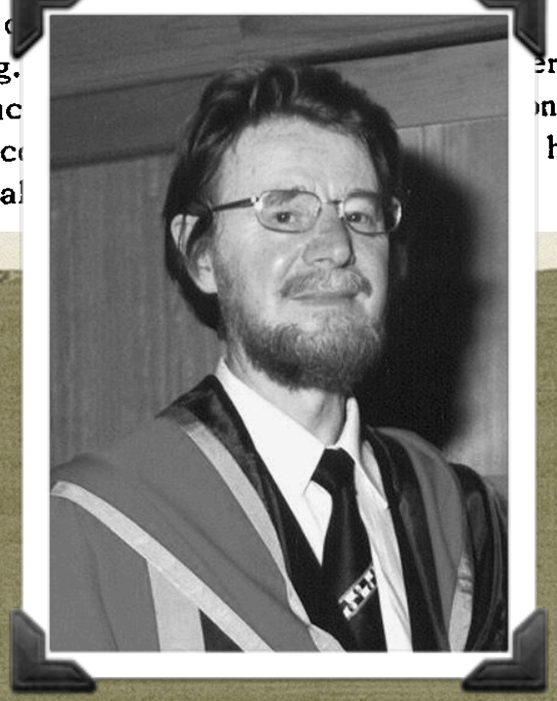


III.5 ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

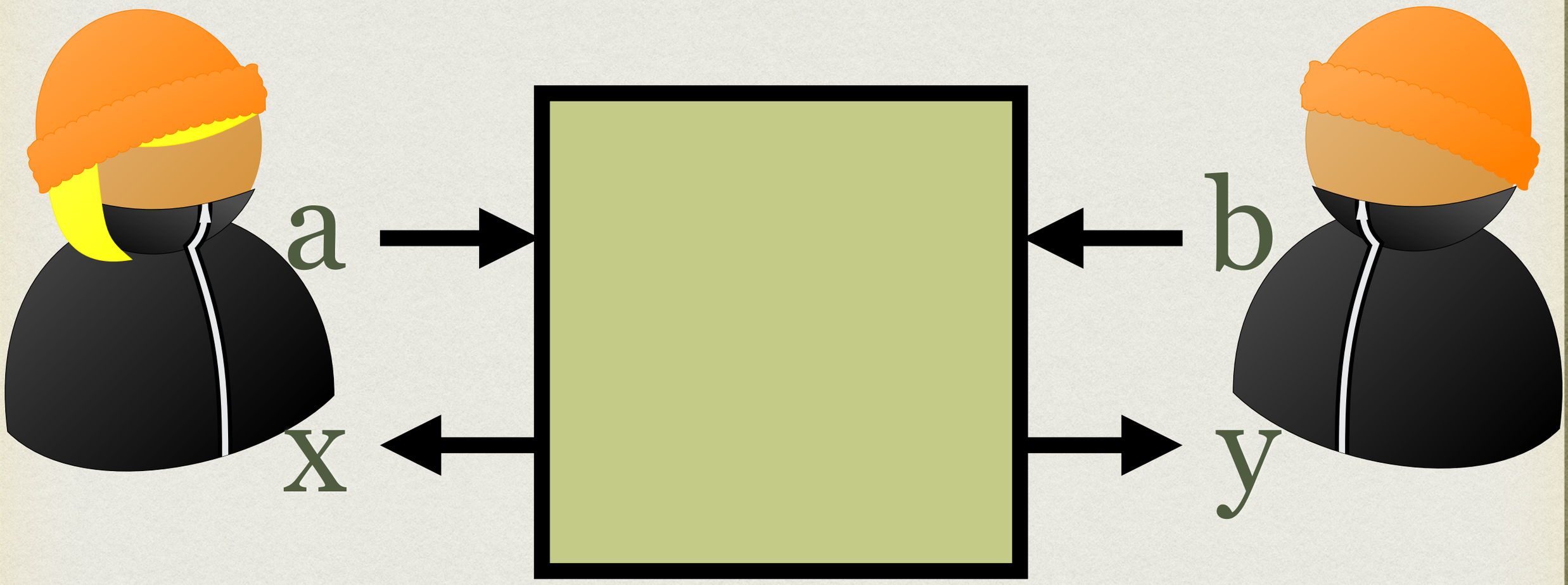
JOHN S. BELL†

1. Introduction

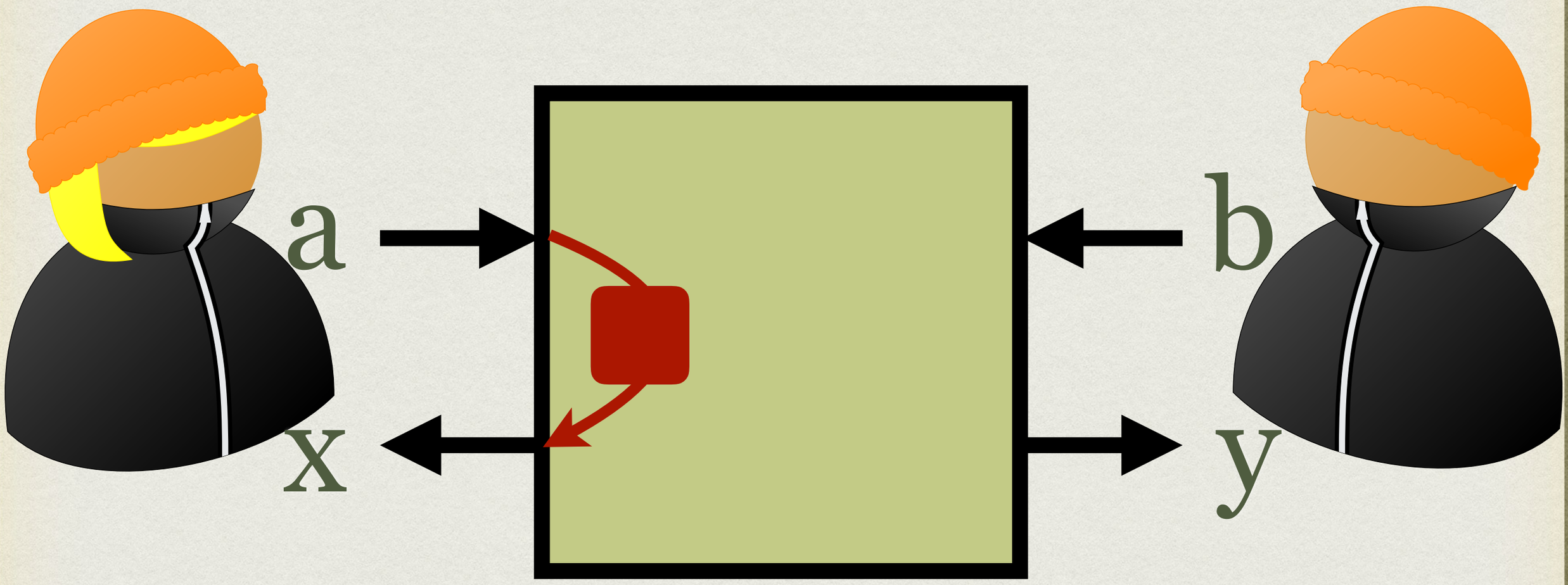
THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated mathematically and shown to be incompatible with the statistical predictions of quantum mechanics. It is the requirement of locality, or more precisely that the result of a measurement on one system be unaffected by operations on a distant system with which it has interacted in the past, that creates the essential difficulty. There have been attempts [3] to s[illegible]hat even without such a [illegible]arability or locality requirement no "hidden variable" interpretation [illegible] These attempts have been examined elsewhere [4] and found wanting. [illegible]erpretation of elementary quantum theory [5] has been explicitly construc[illegible]n has indeed a grossly non-local structure. This is characteristic, ac[illegible] here, of any such theory which reproduces exactly the quantum mechanical



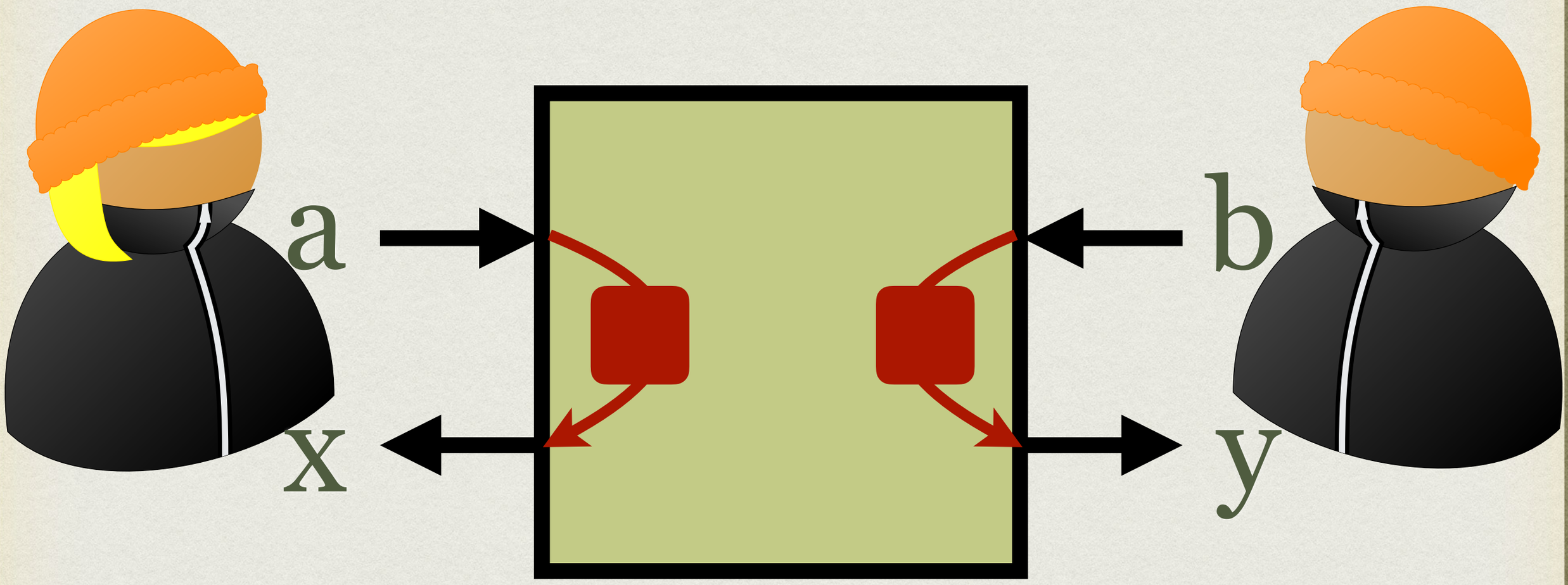
LOCALITÉ



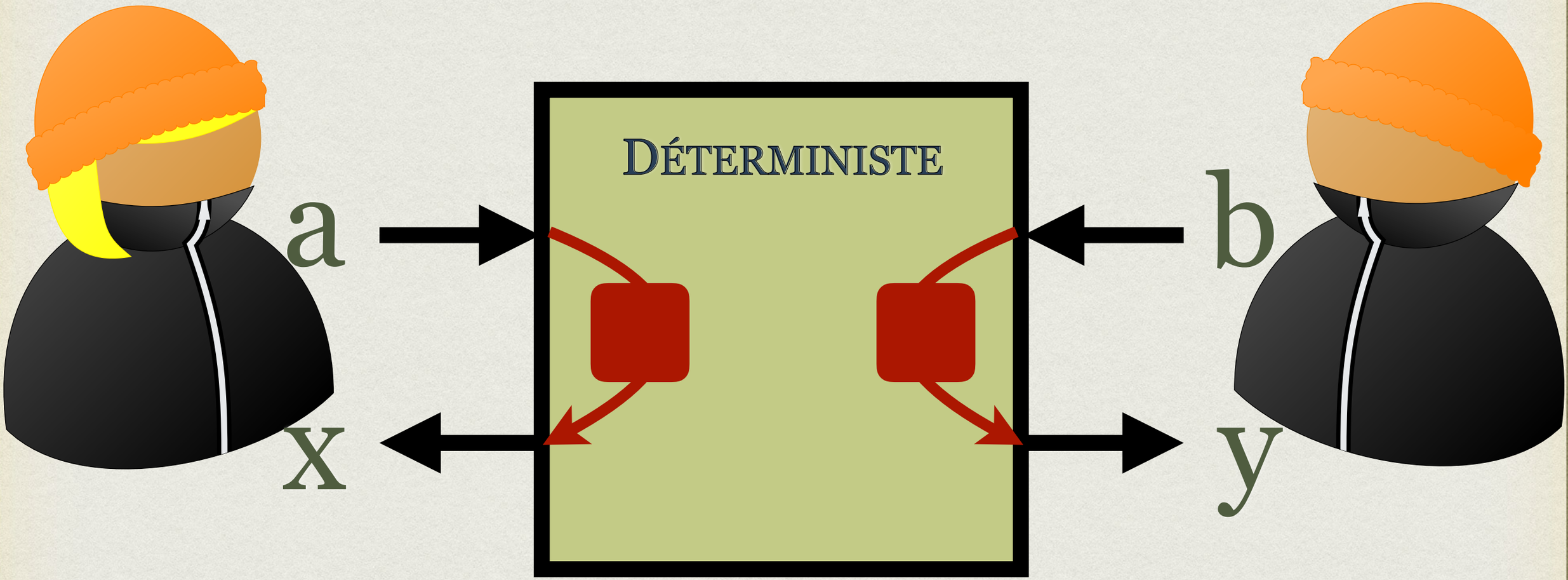
LOCALITÉ



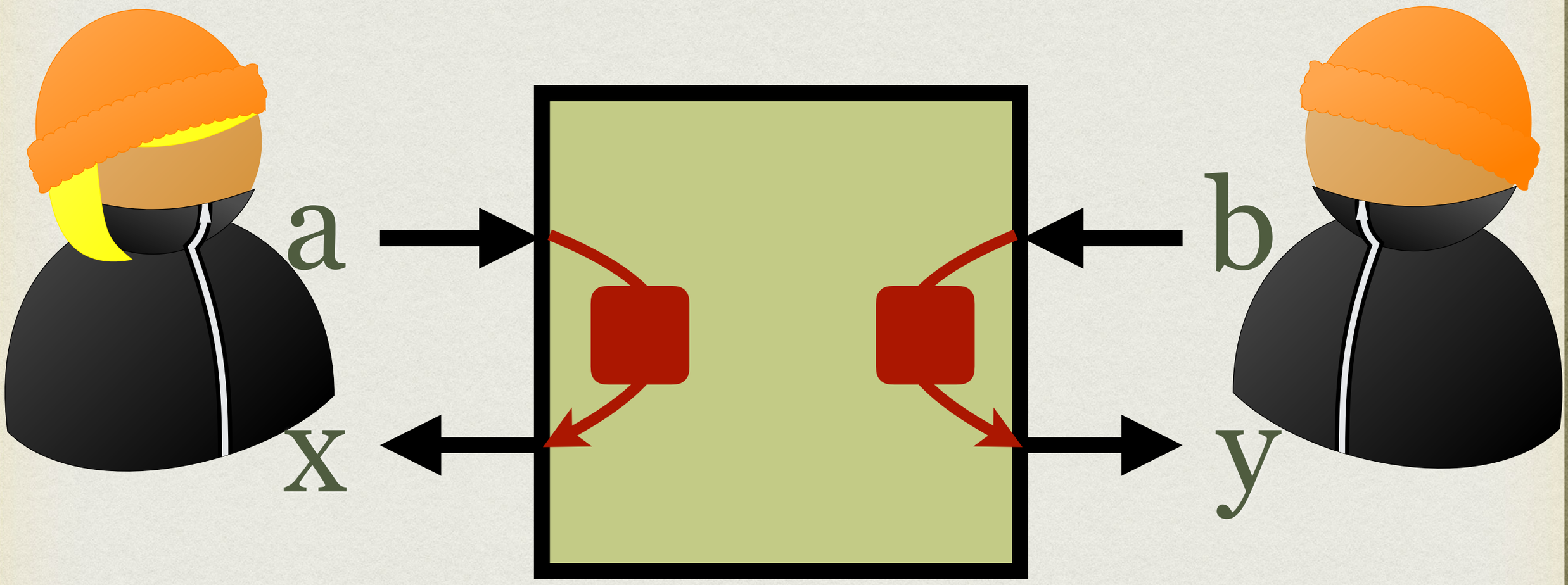
LOCALITÉ



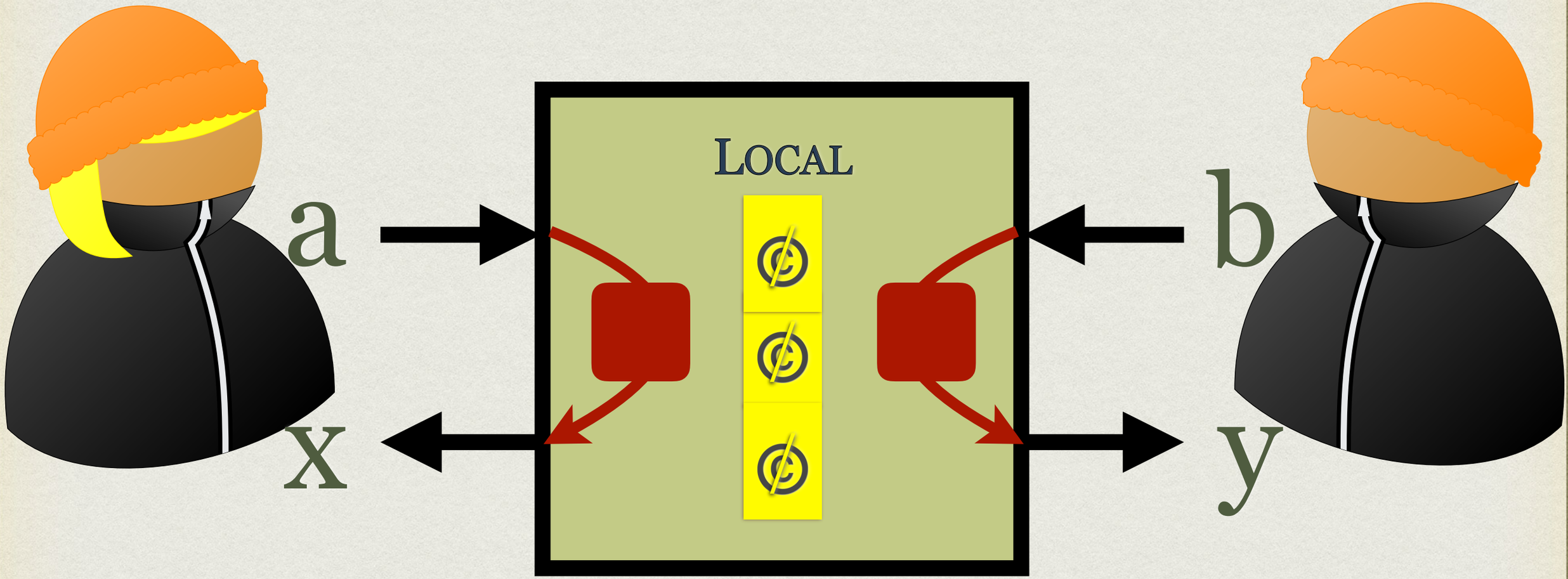
LOCALITÉ



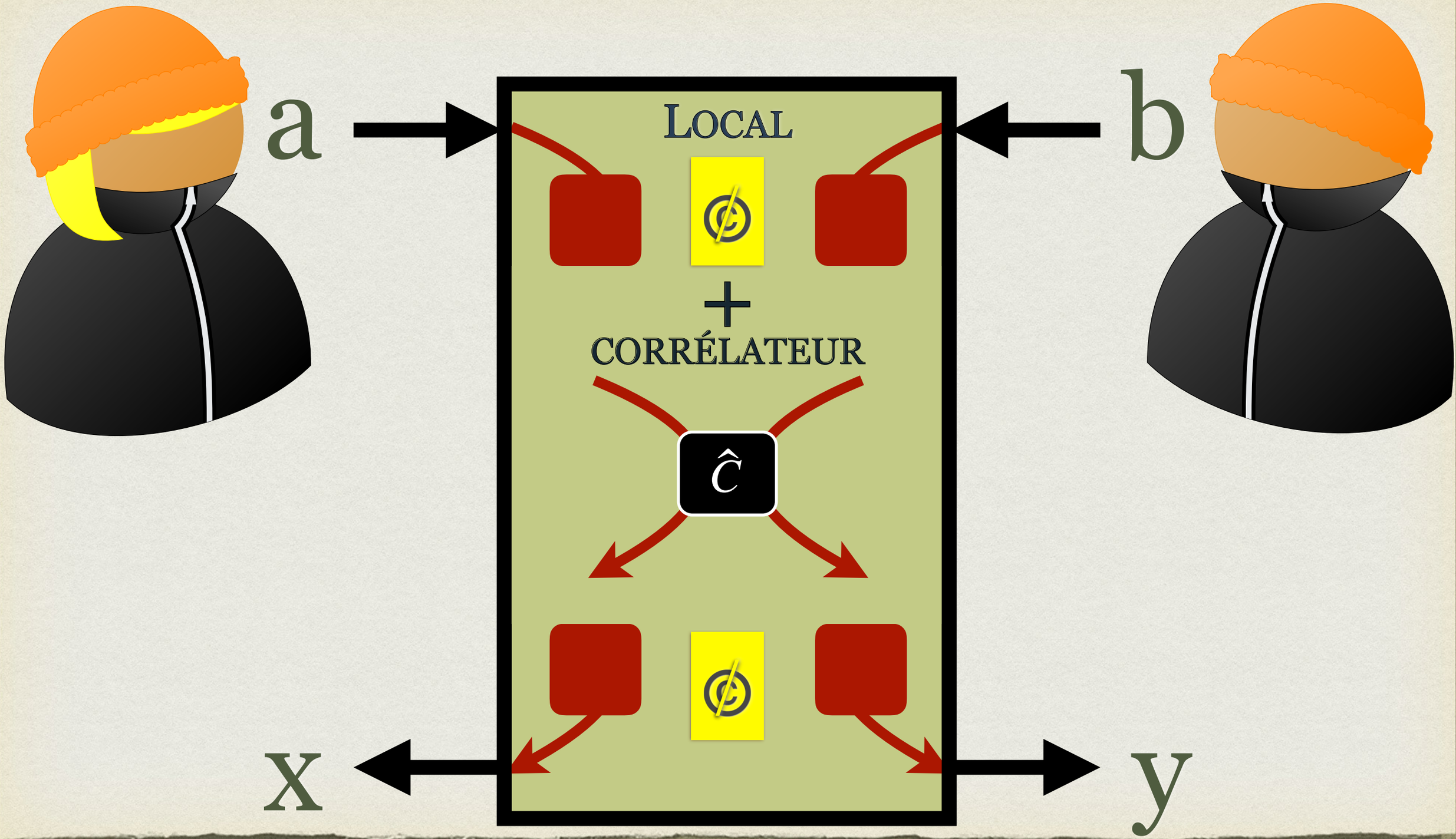
LOCALITÉ



LOCALITÉ

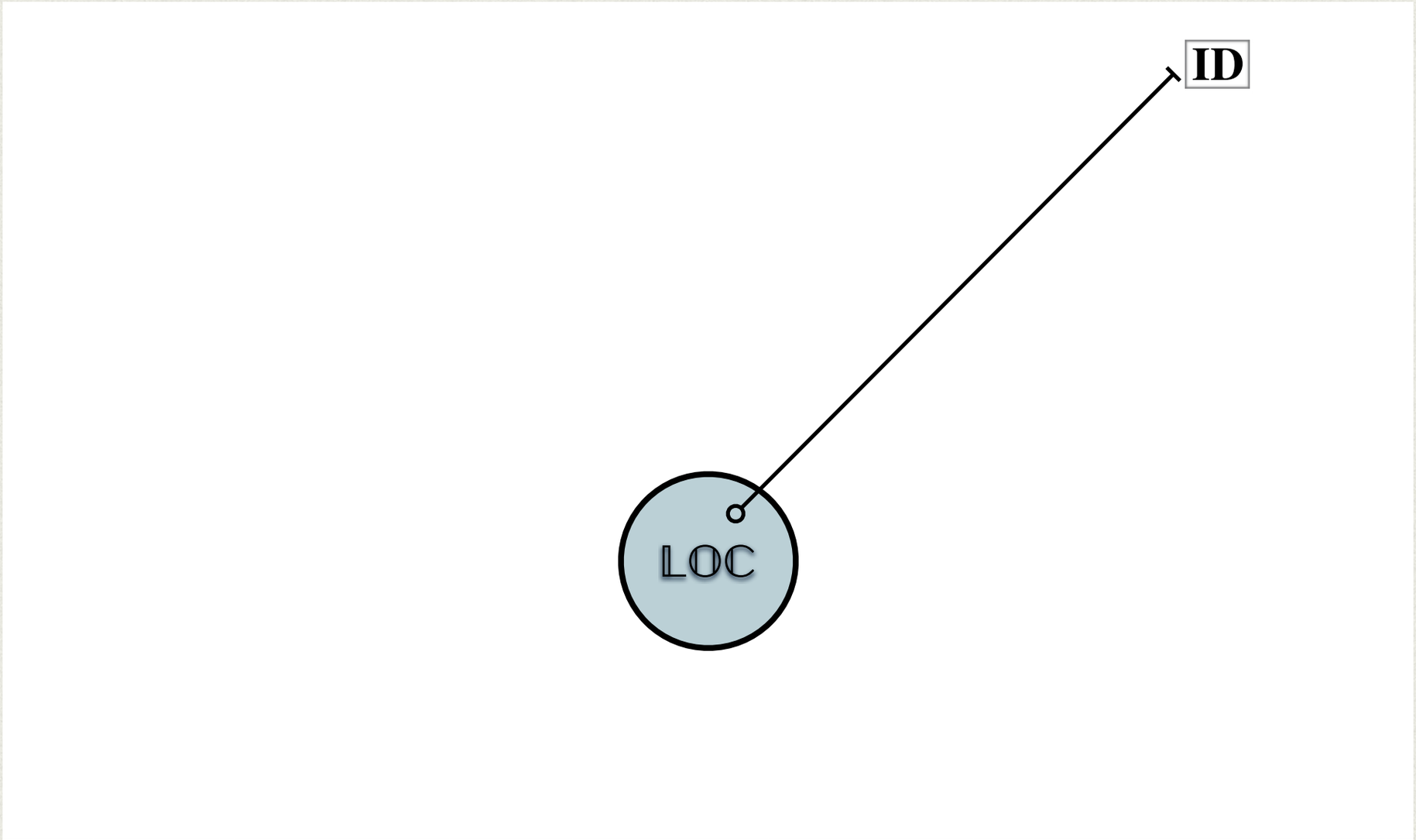


HIERARCHIE DE NON-LOCALITÉ

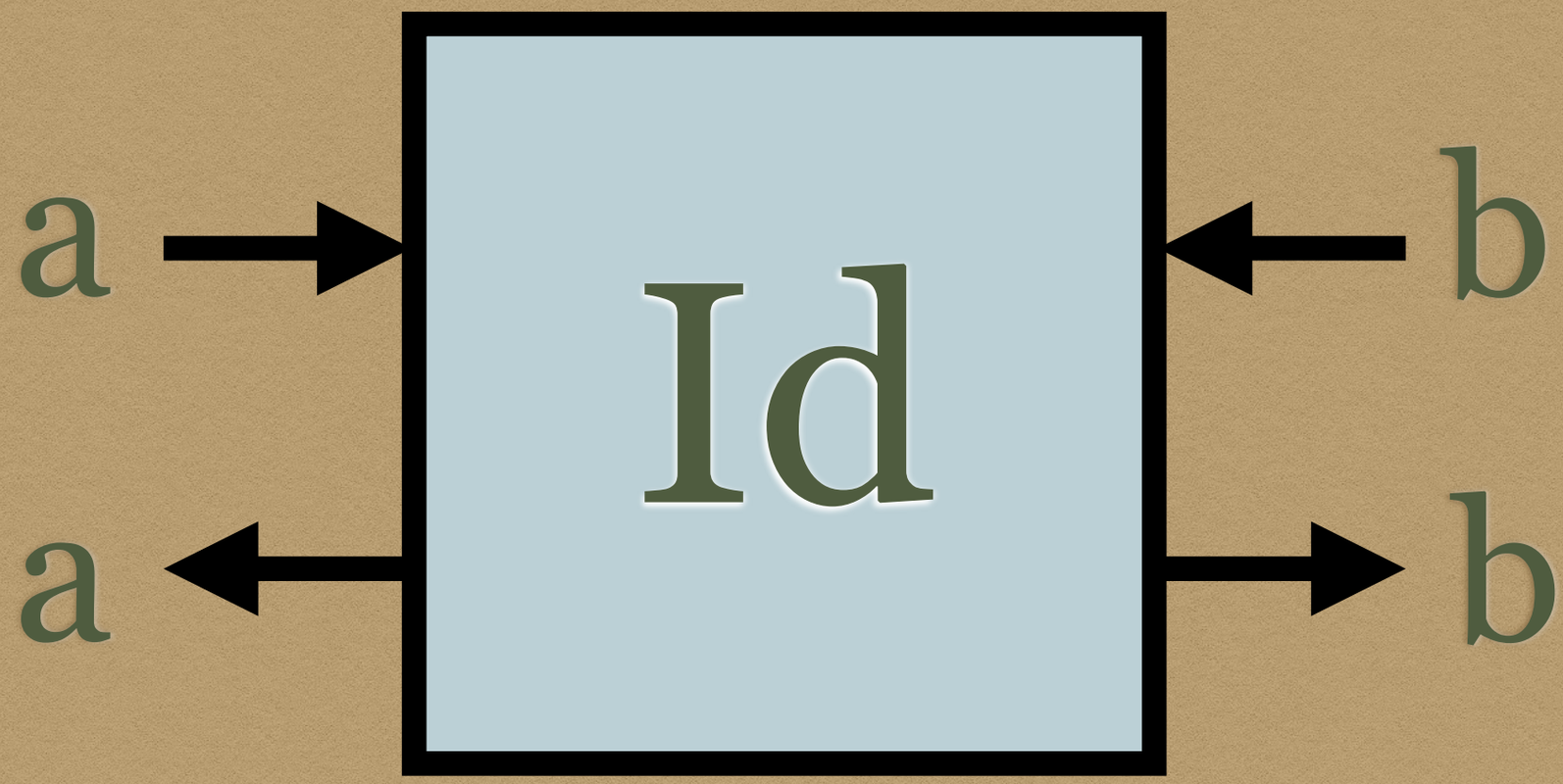


HIERARCHIE DE NON-LOCALITÉ

HIERARCHIE DE NON-LOCALITÉ

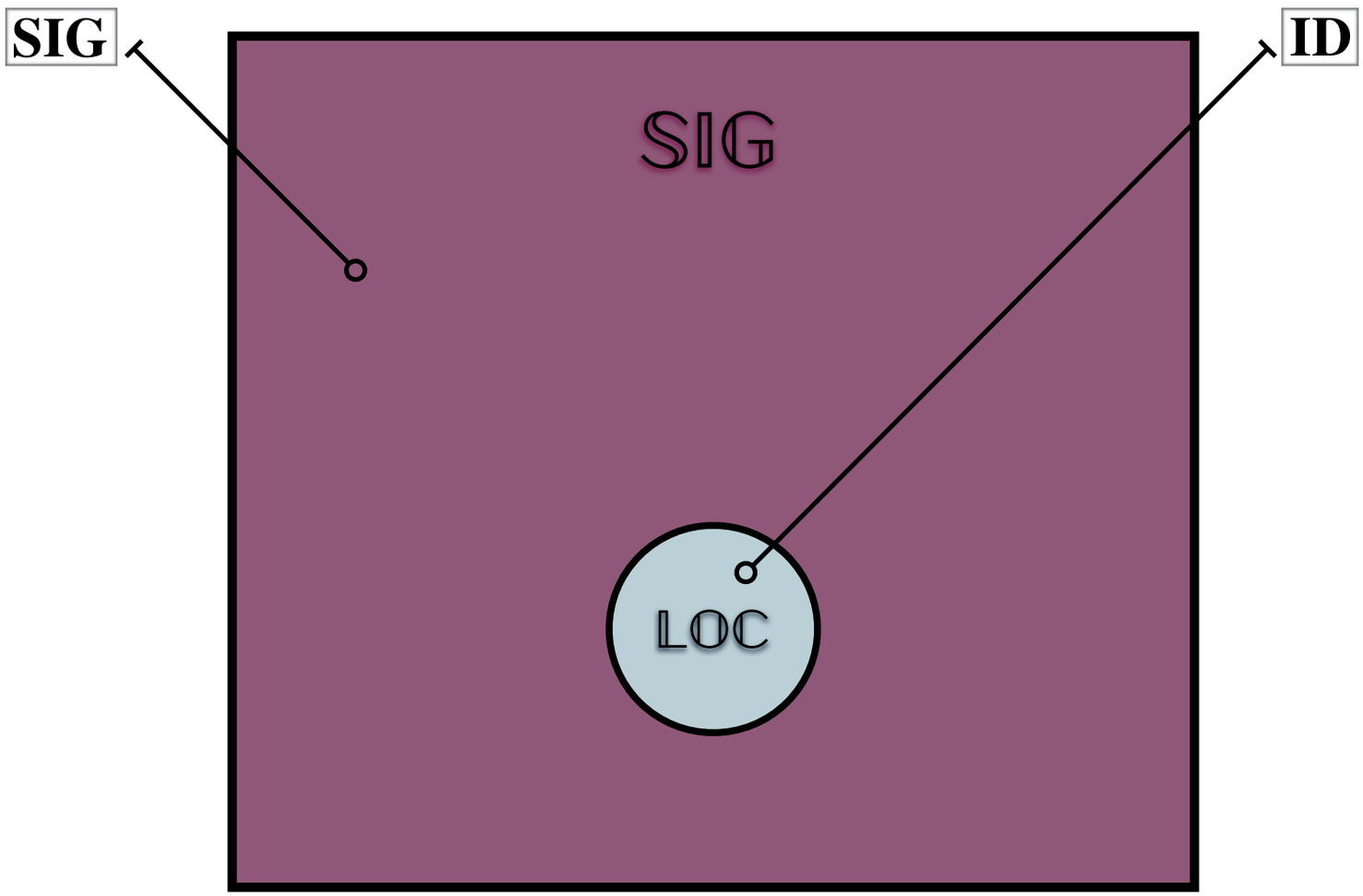


HIERARCHIE DE NON-LOCALITÉ



HIERARCHIE DE NON-LOCALITÉ

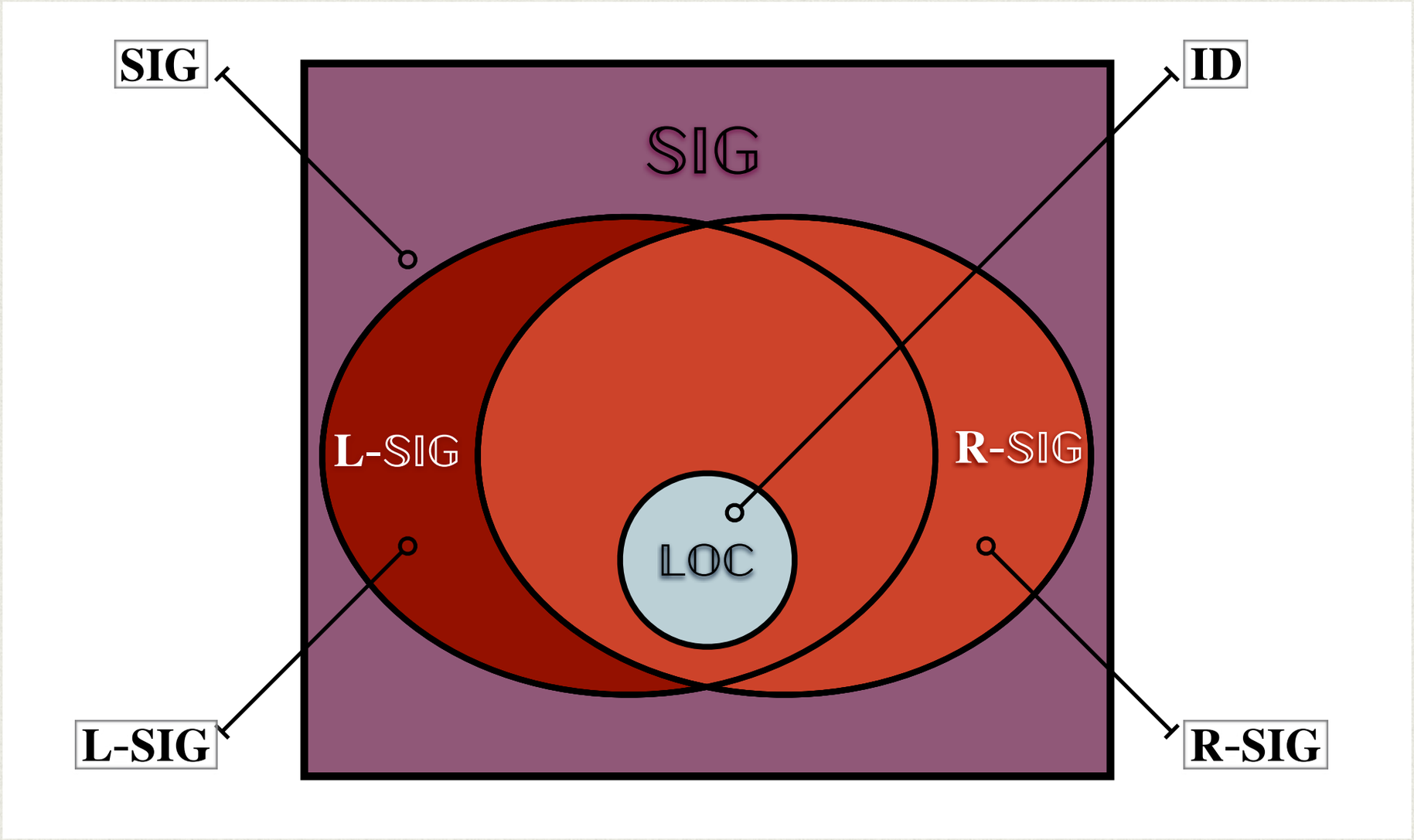
HIERARCHIE DE NON-LOCALITÉ



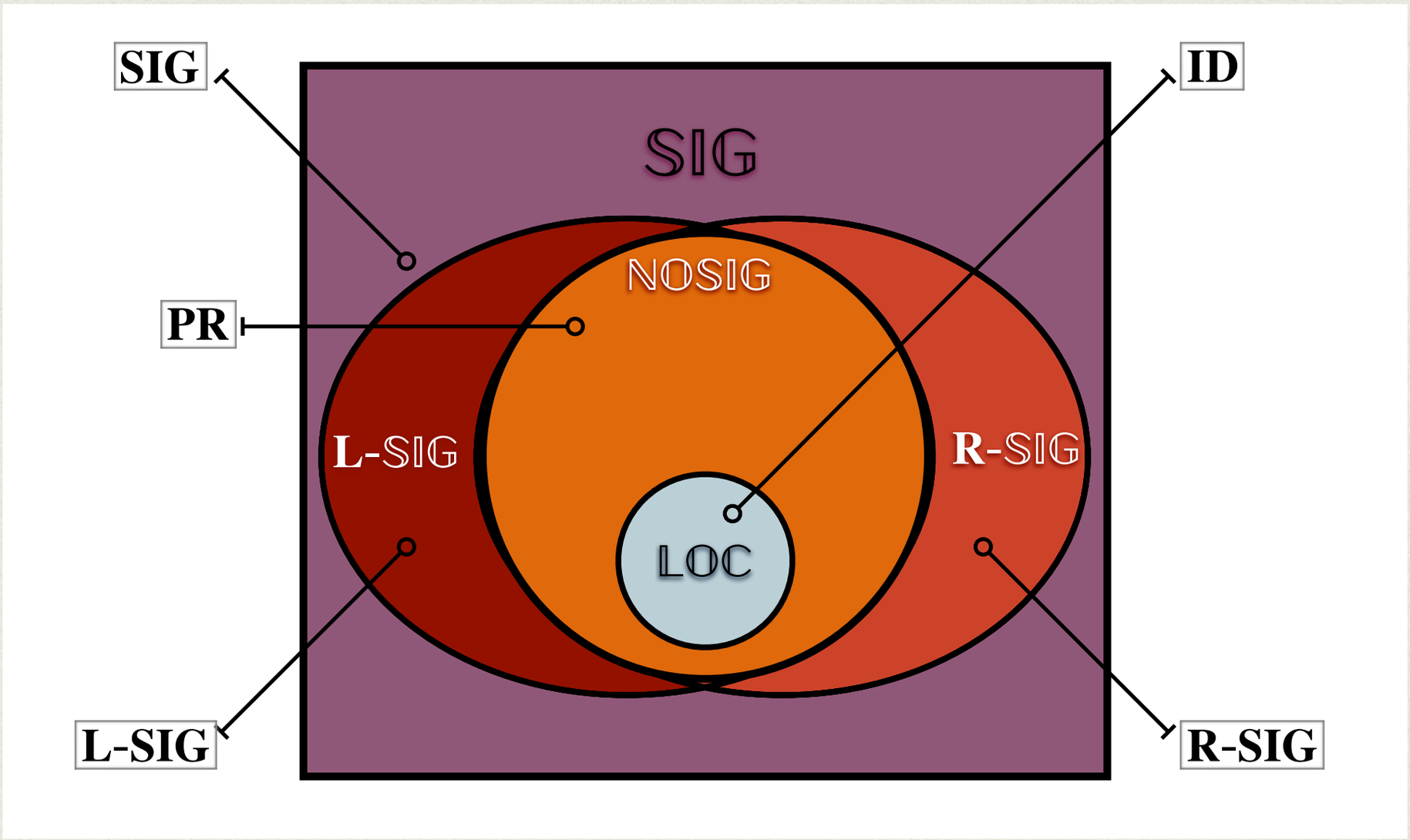
HIERARCHIE DE NON-LOCALITÉ

HIERARCHIE DE NON-LOCALITÉ

HIERARCHIE DE NON-LOCALITÉ



HIERARCHIE DE NON-LOCALITÉ

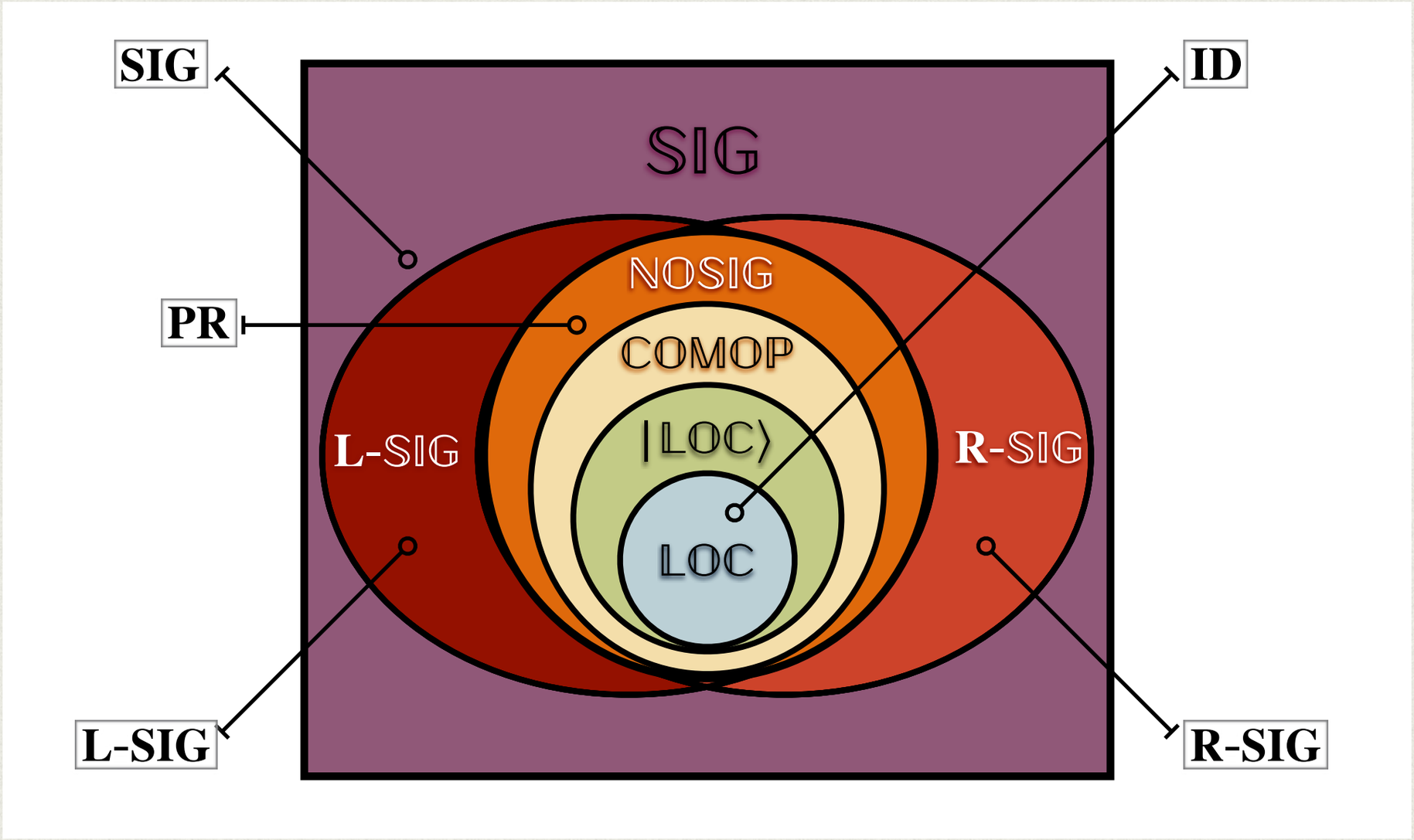


HIERARCHIE DE NON-LOCALITÉ

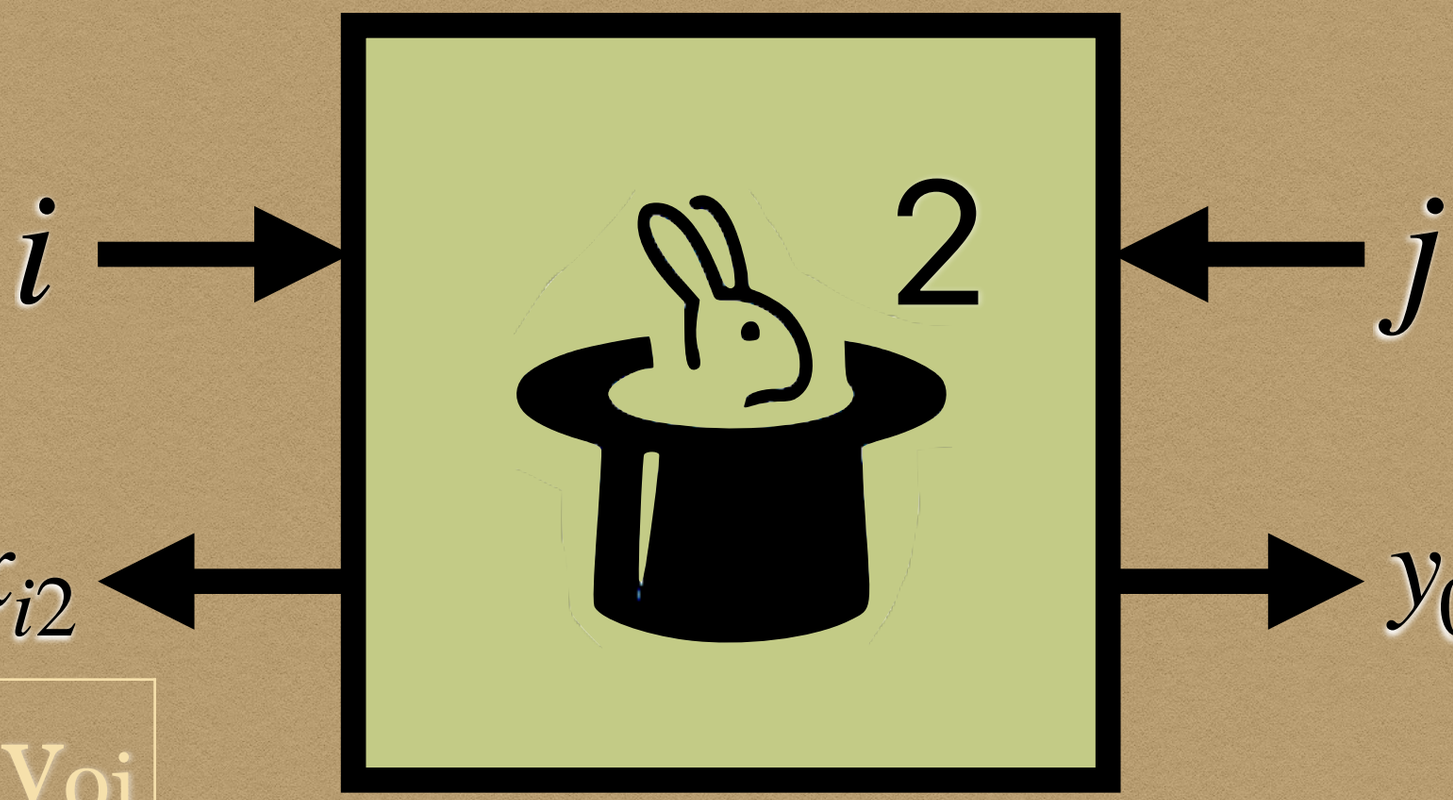
$x \oplus y = a \cdot b$

x est uniforme

HIERARCHIE DE NON-LOCALITÉ



HIERARCHIE DE NON-LOCALITÉ



		y_{0j}
x_{i0}	x_{i1}	$x_{i2} = y_{2j}$
		y_{2j}

➡ paire

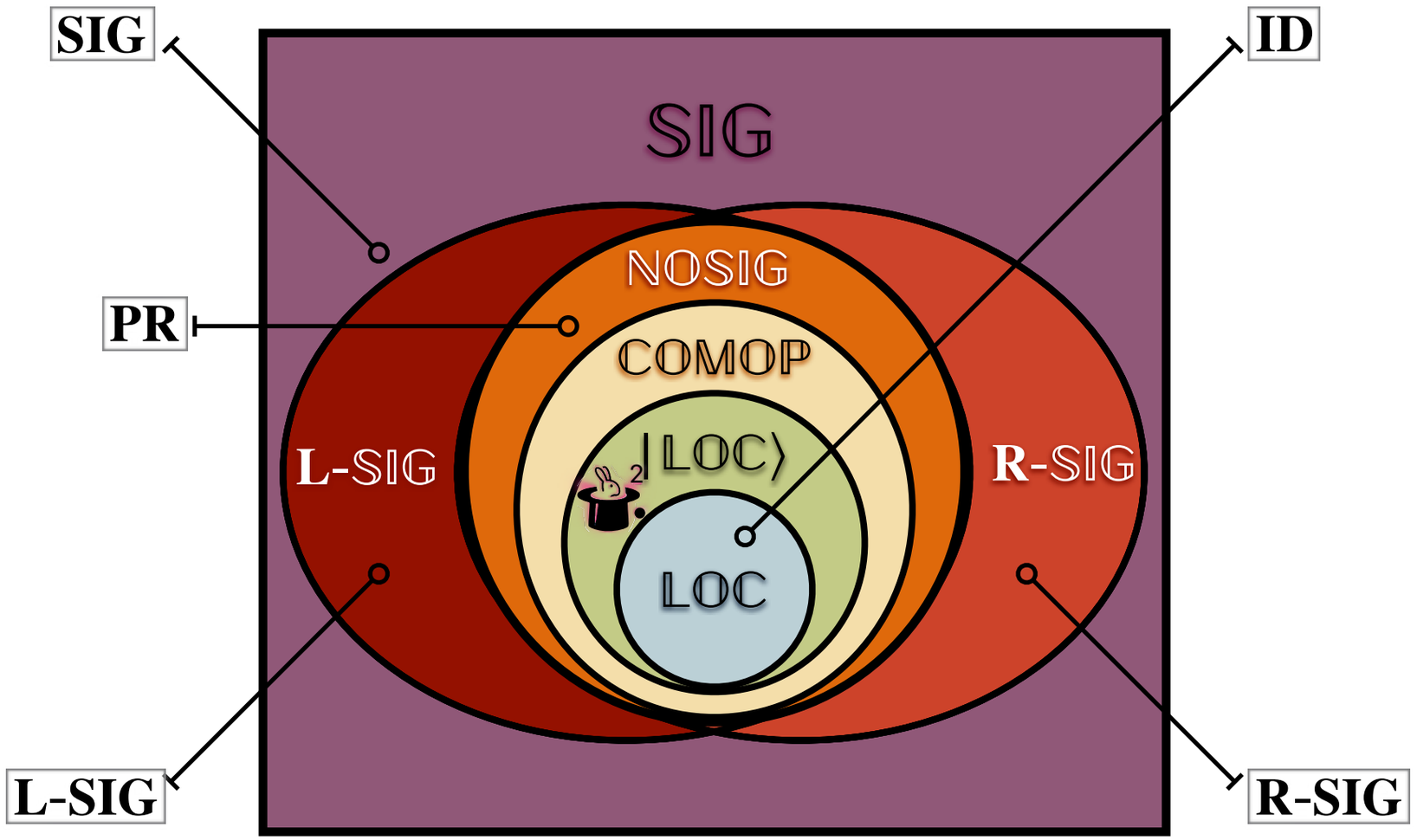
⤷➡ impaire

$$x_{ij} = y_{ij}$$

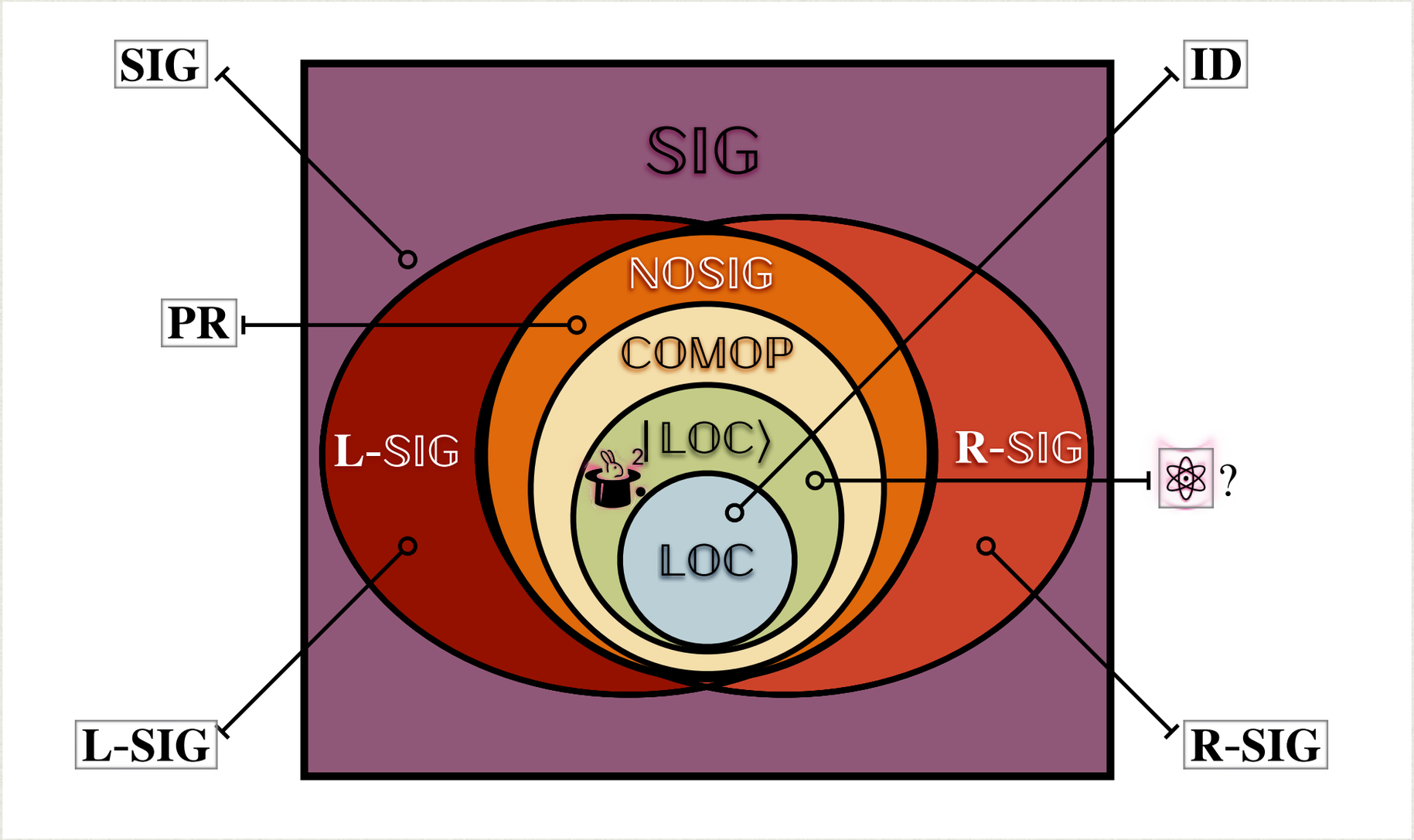
$$x_{i0} \oplus x_{i1} \oplus x_{i2} = 0$$

$$y_{0j} \oplus y_{1j} \oplus y_{2j} = 1$$

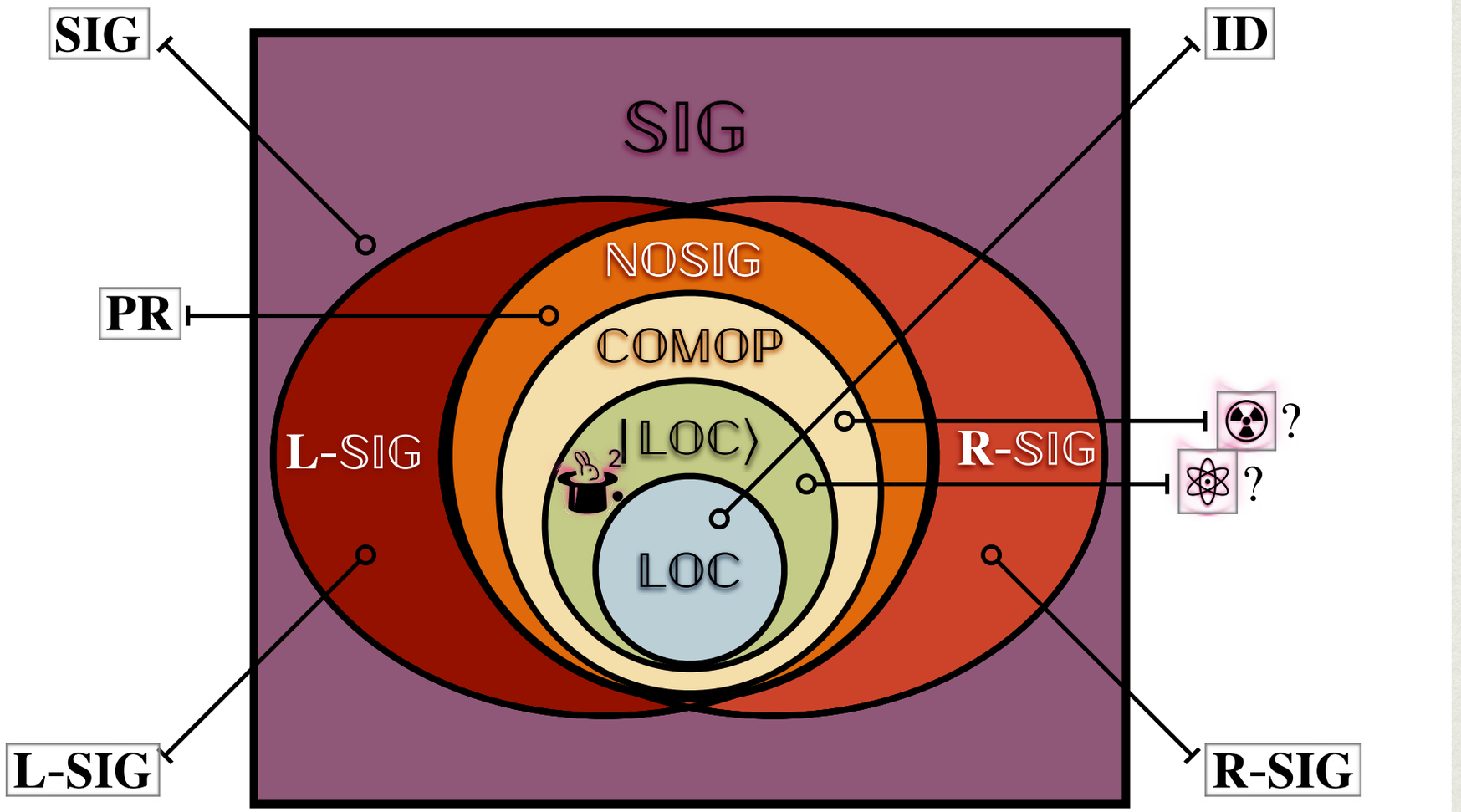
HIERARCHIE DE NON-LOCALITÉ



HIERARCHIE DE NON-LOCALITÉ

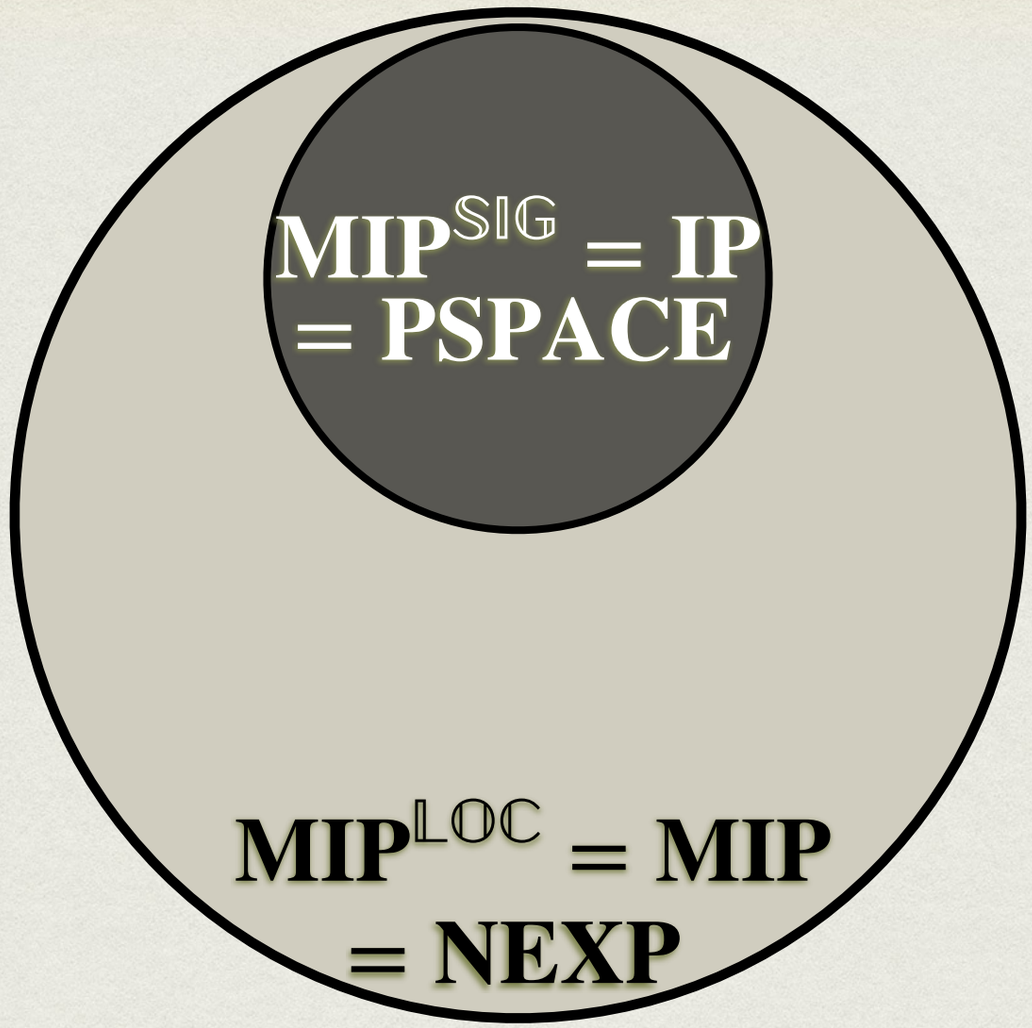


HIERARCHIE DE NON-LOCALITÉ

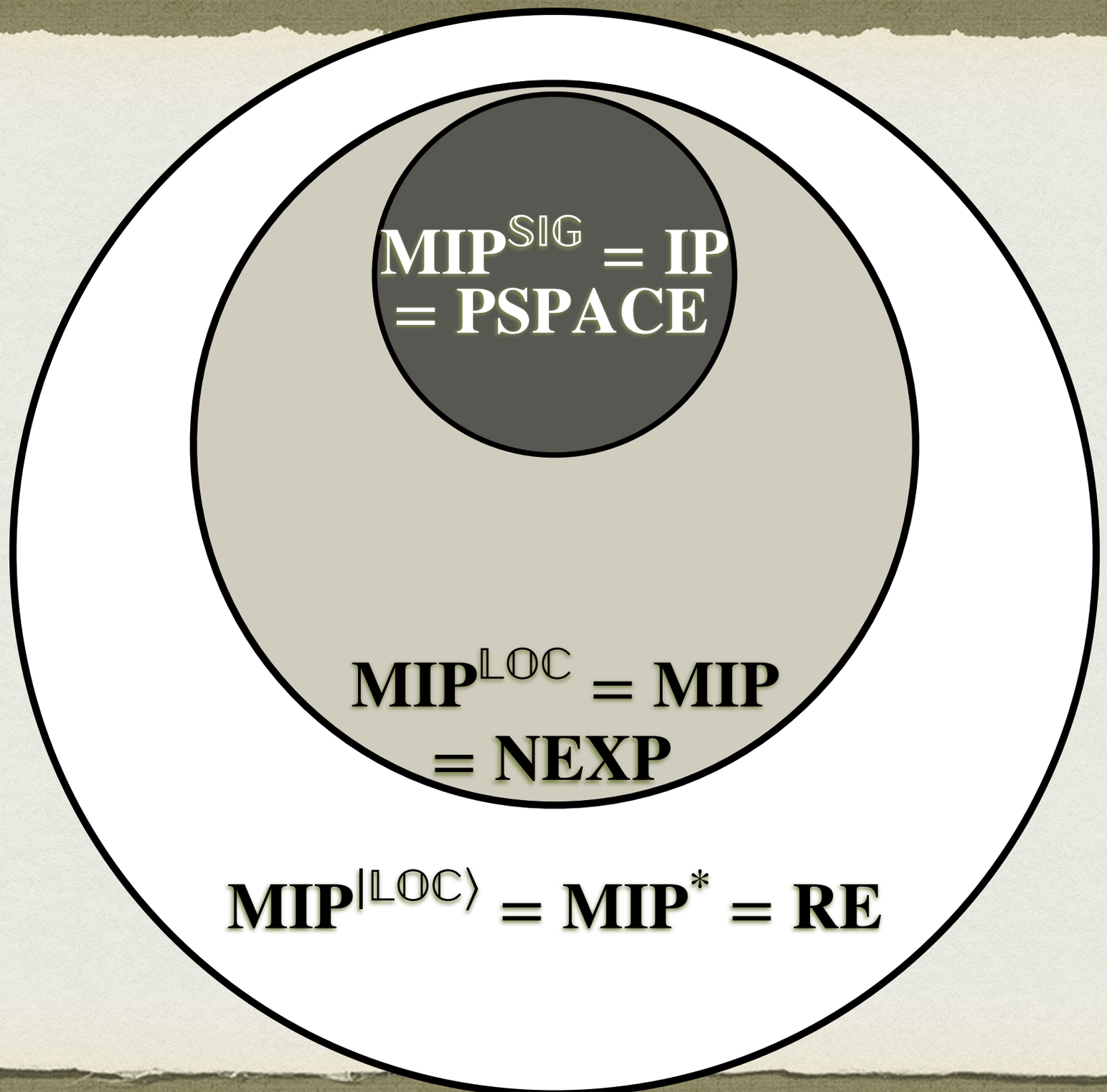


CLASSES DE COMPLEXITÉ

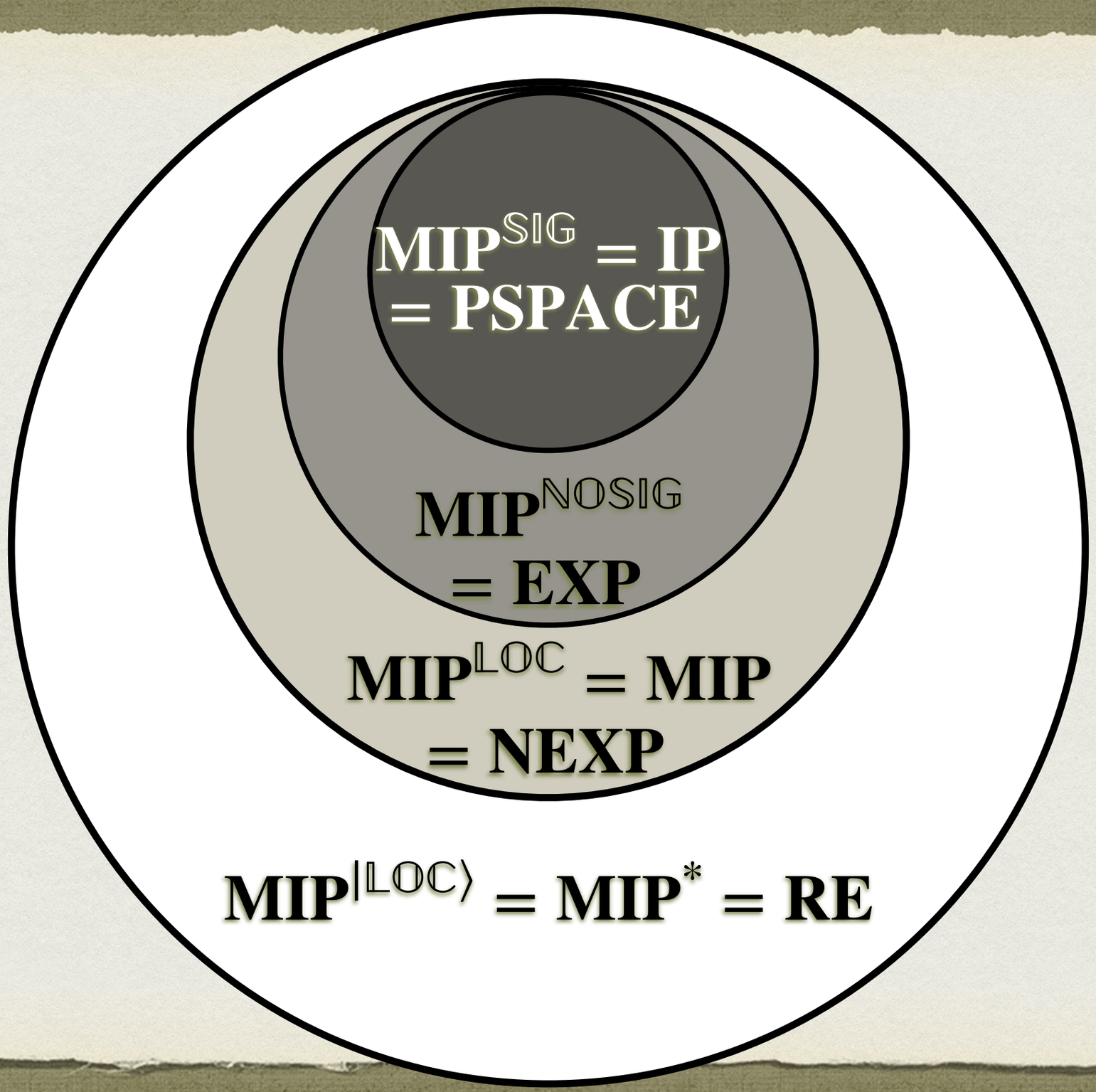
CLASSES DE COMPLEXITÉ



CLASSES DE COMPLEXITÉ



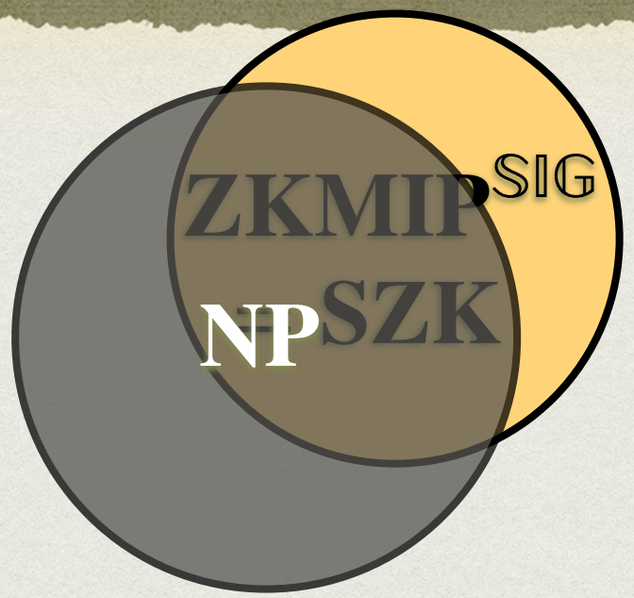
CLASSES DE COMPLEXITÉ



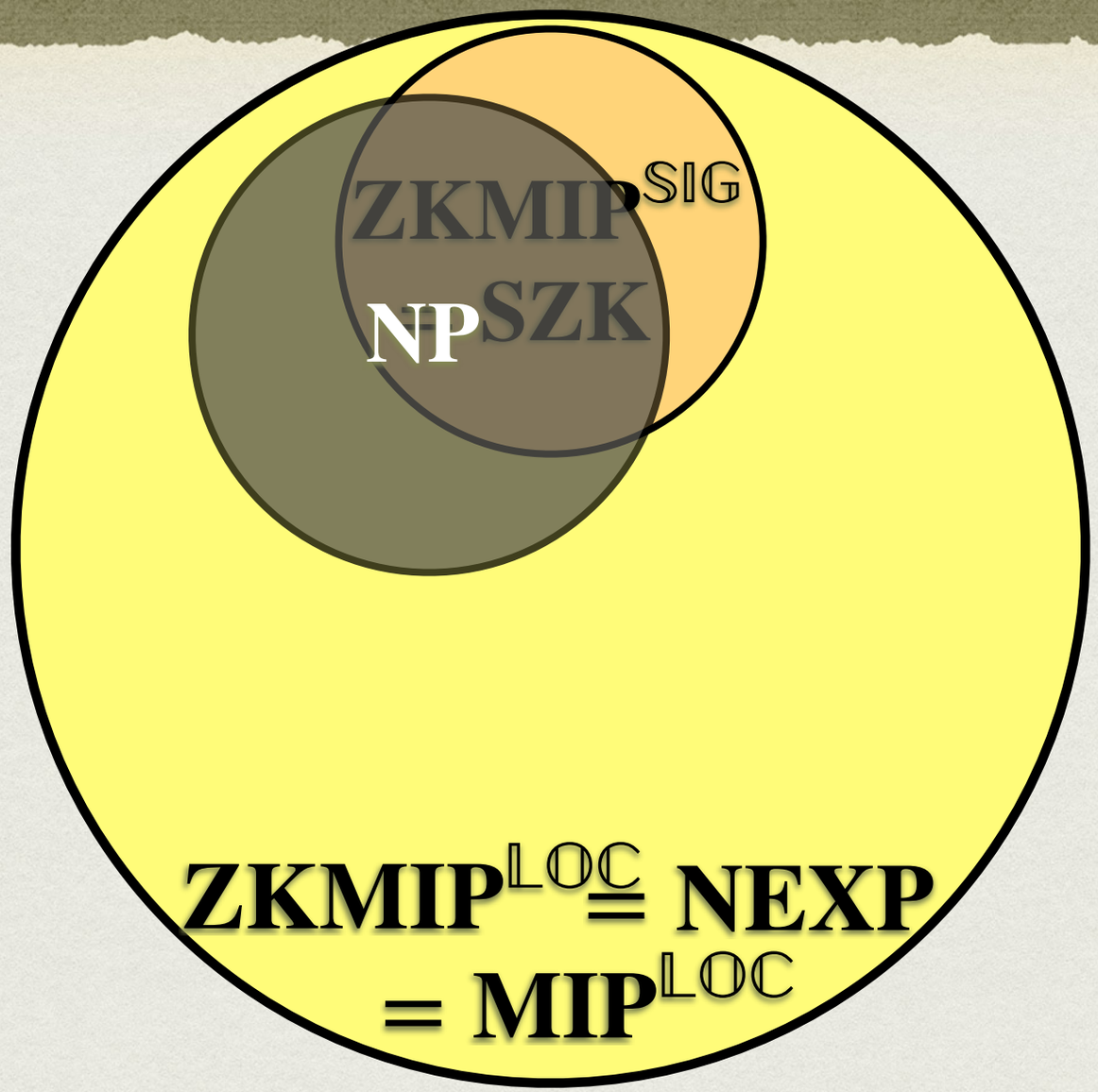
CLASSES DE COMPLEXITÉ ZK

ZKMIP^{SIG} = SZK

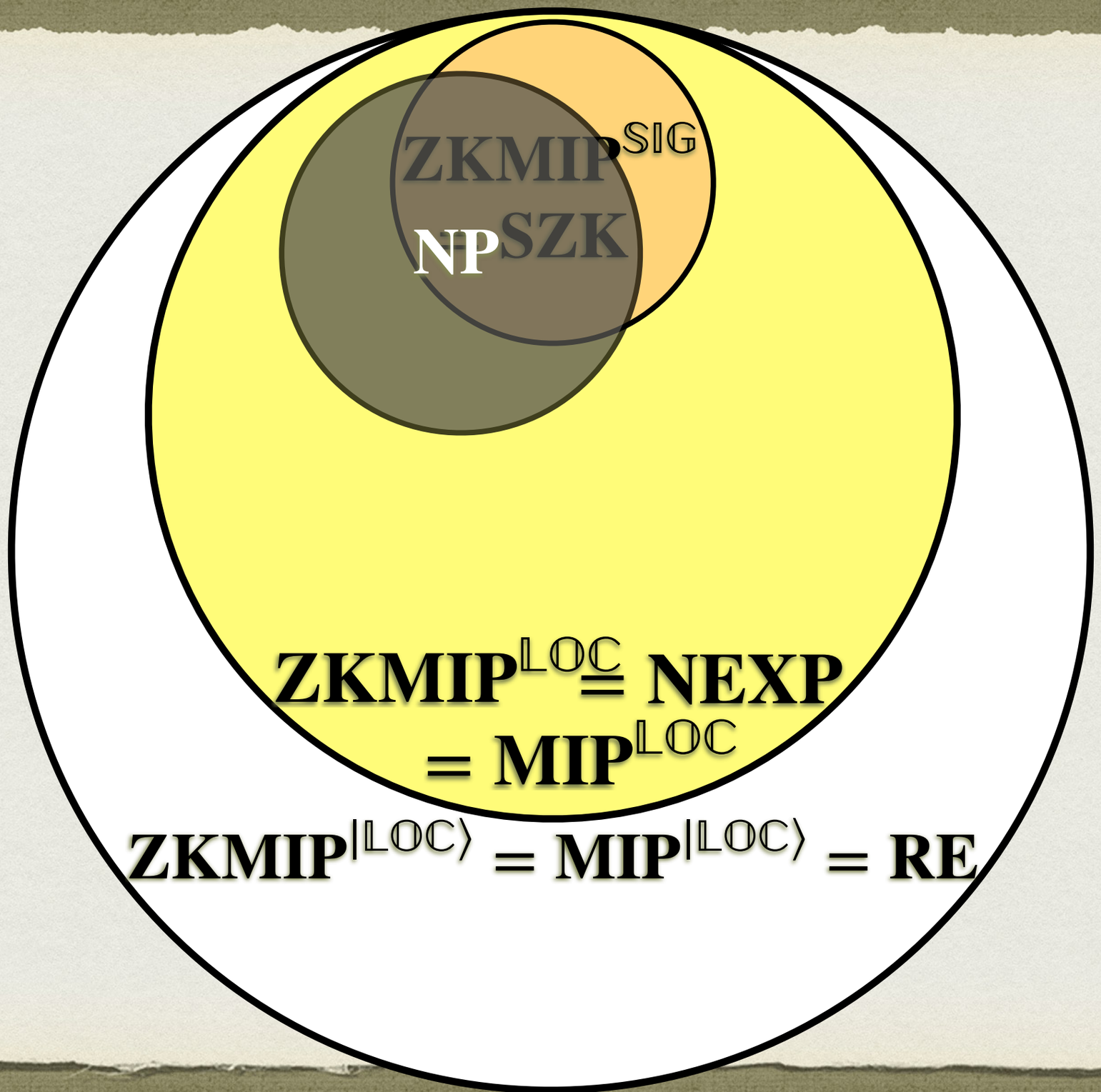
CLASSES DE COMPLEXITÉ ZK



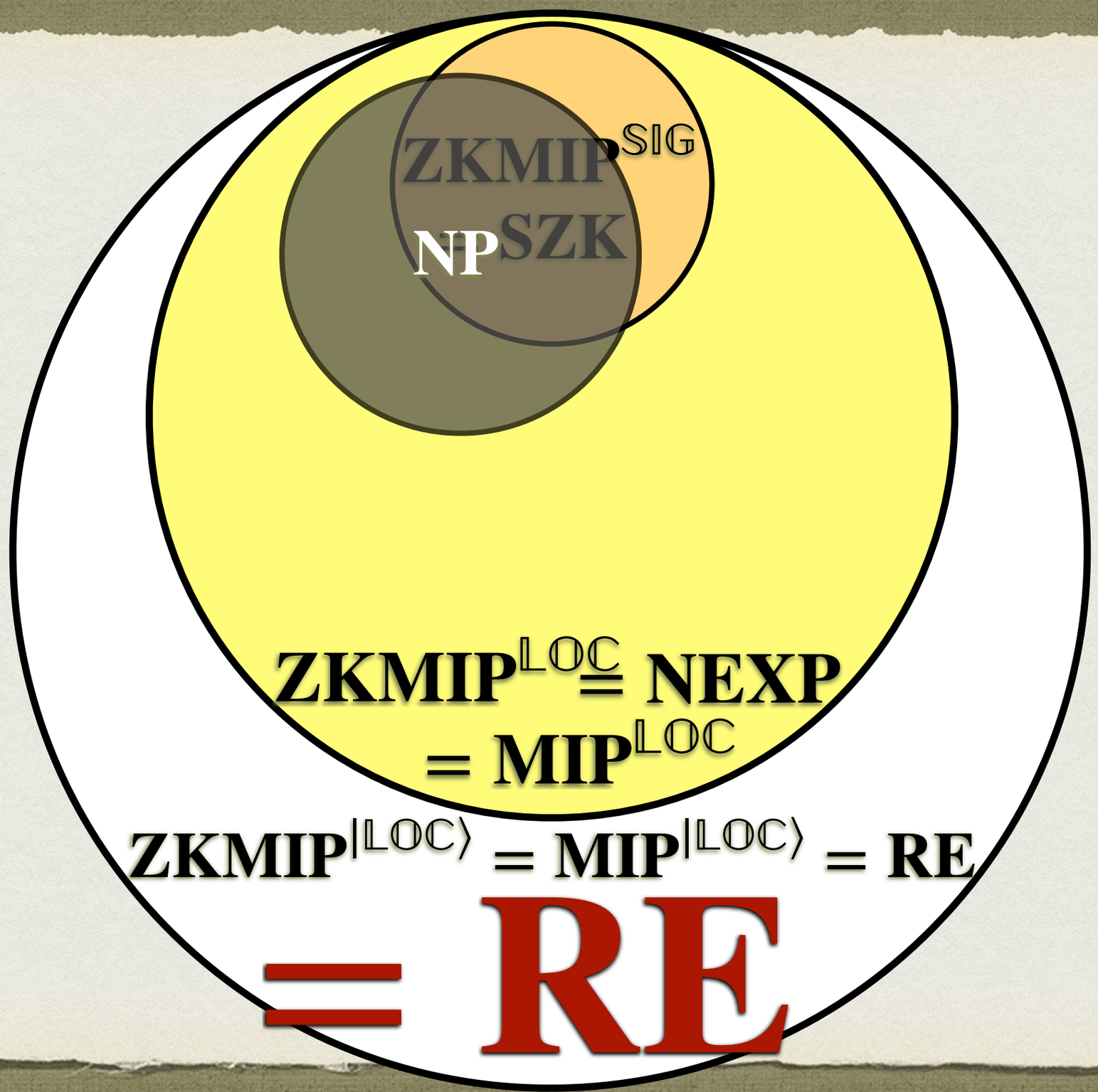
CLASSES DE COMPLEXITÉ ZK



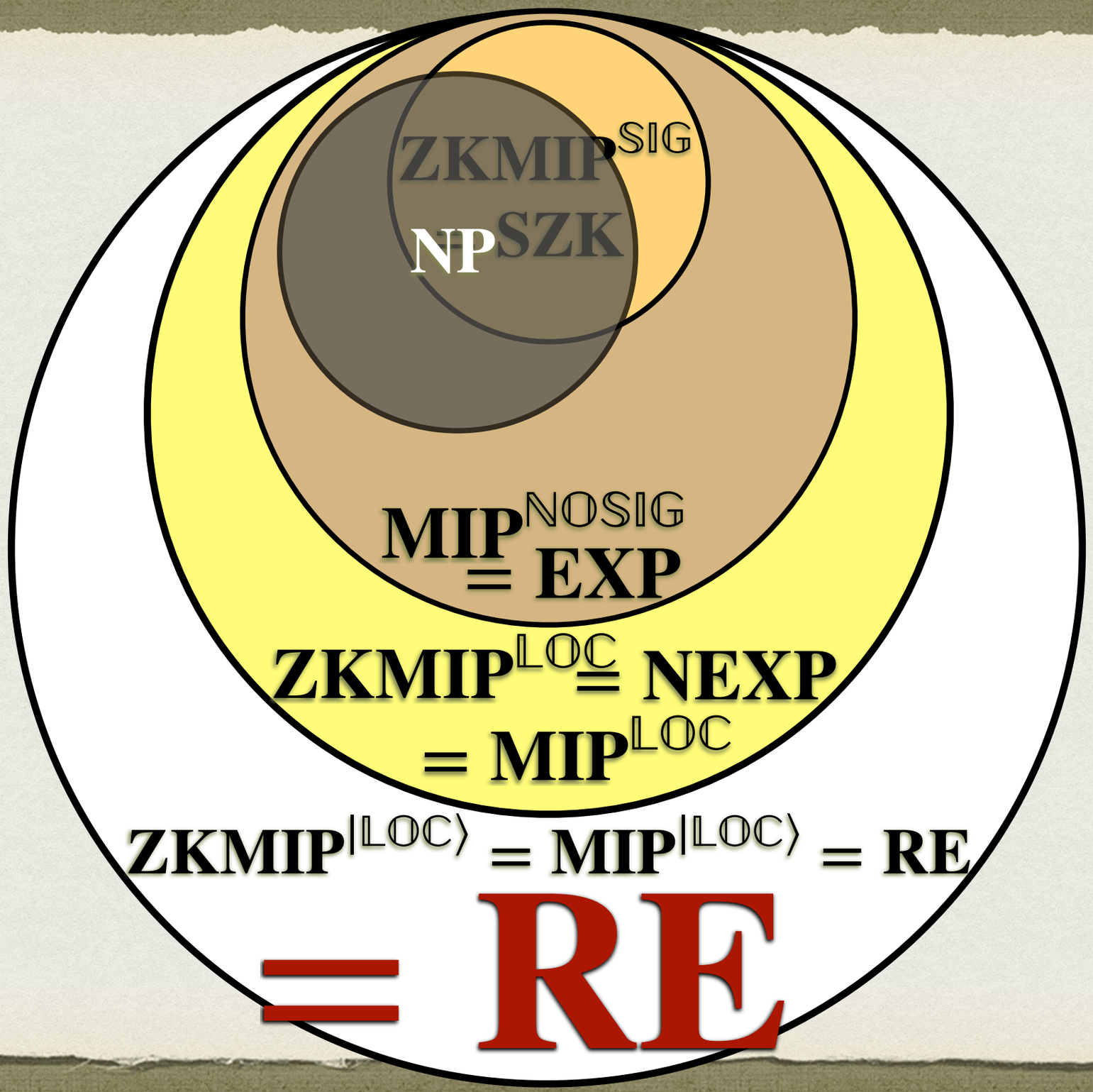
CLASSES DE COMPLEXITÉ ZK



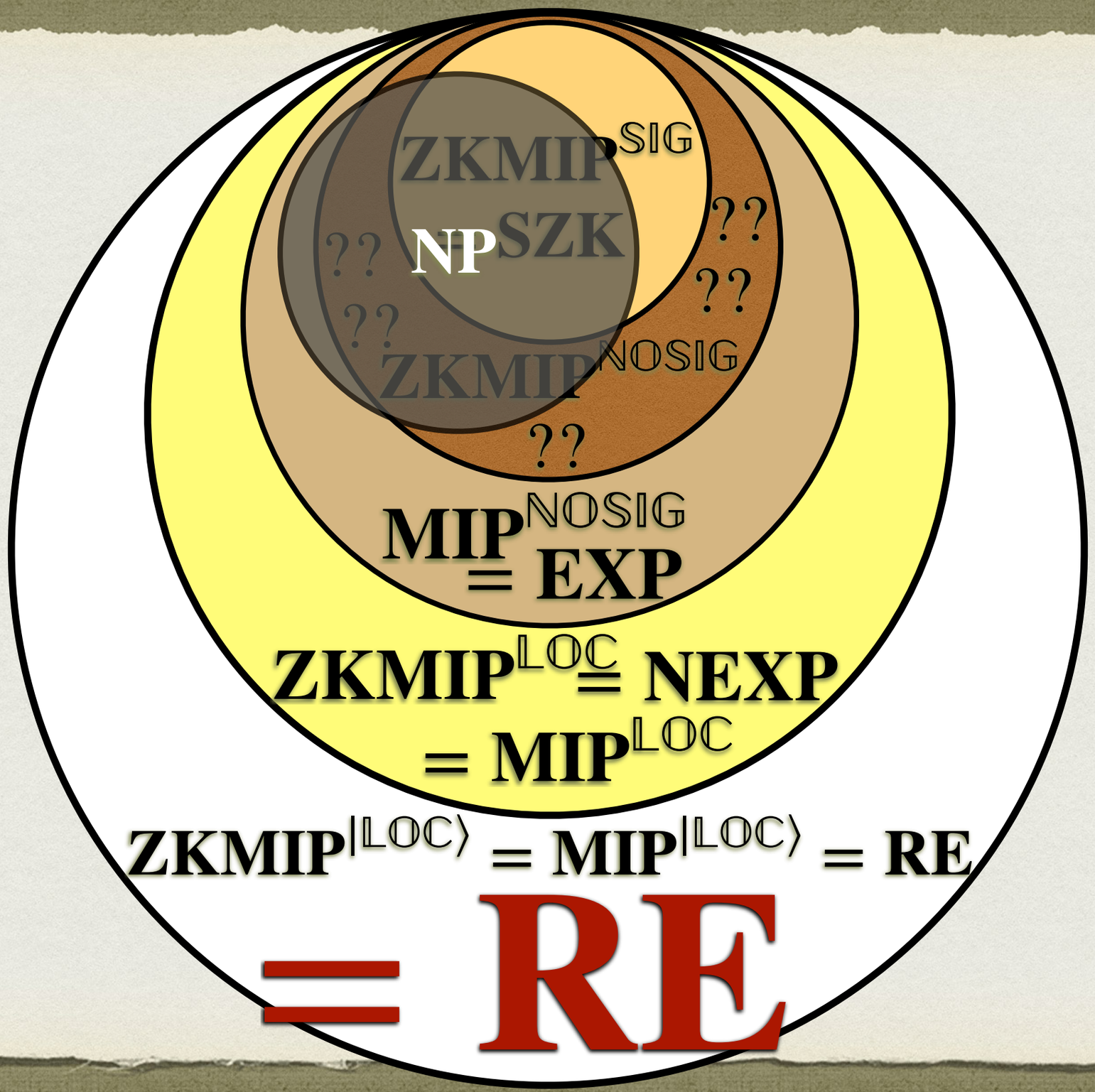
CLASSES DE COMPLEXITÉ ZK



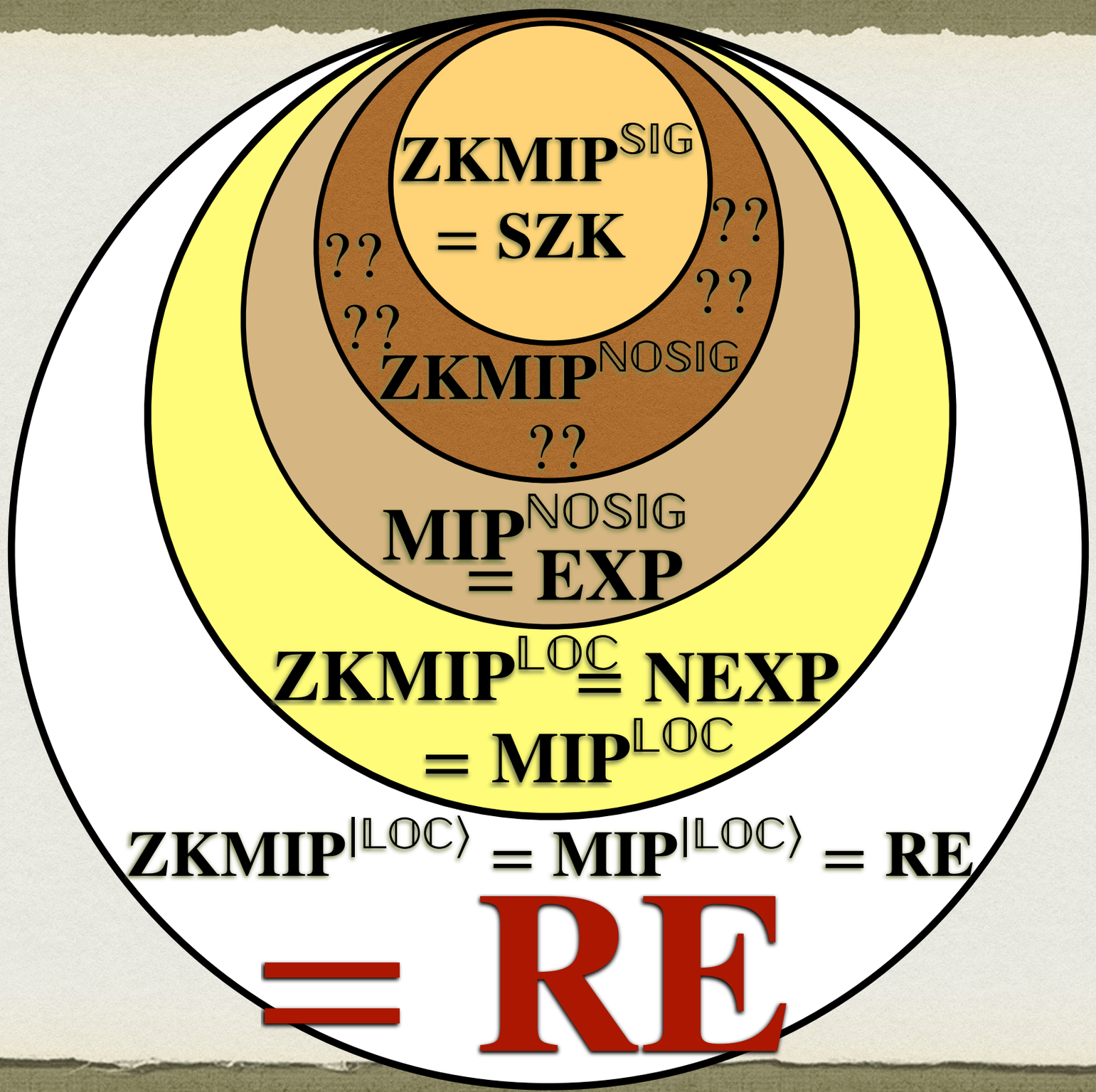
CLASSES DE COMPLEXITÉ ZK

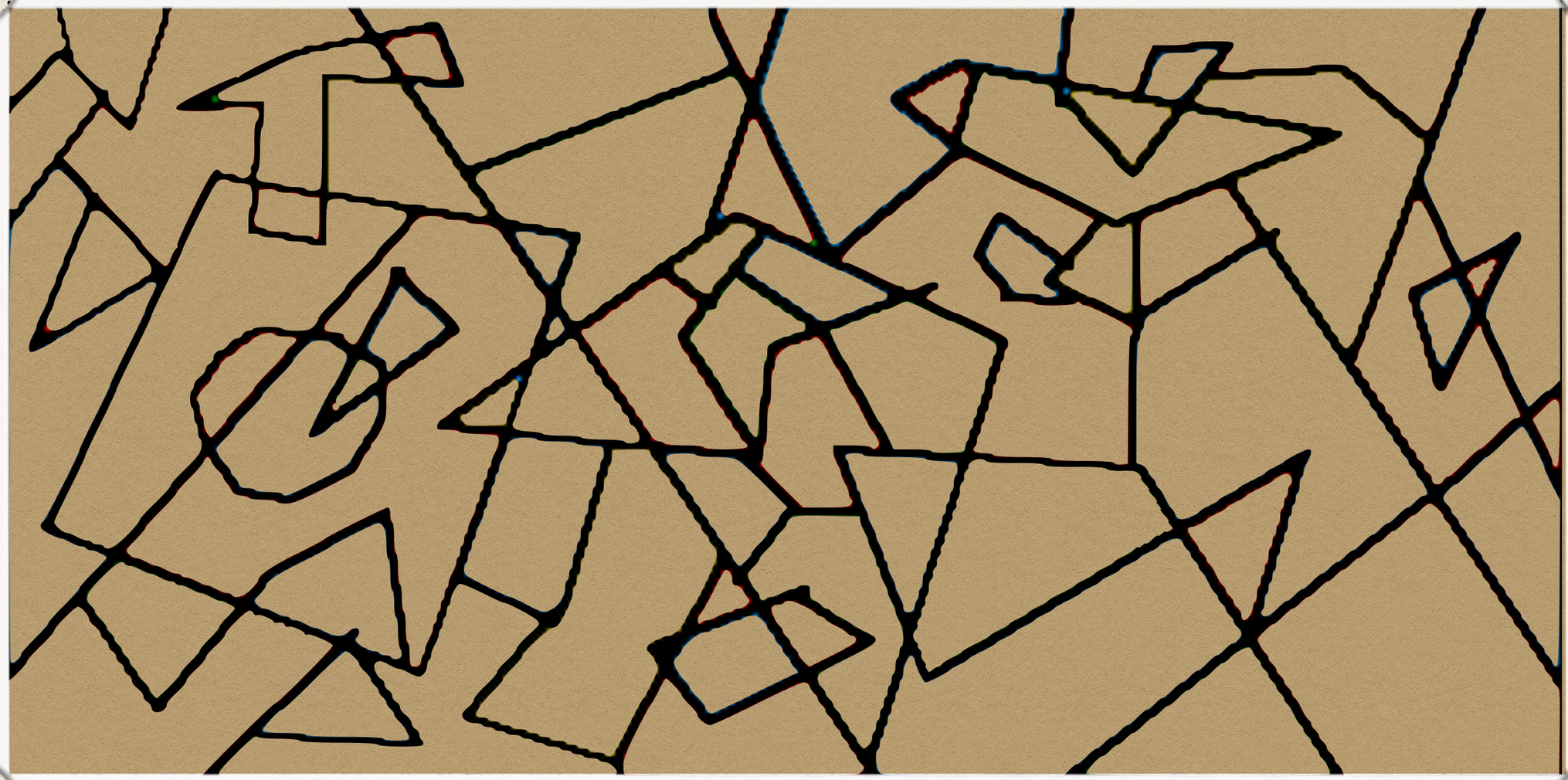


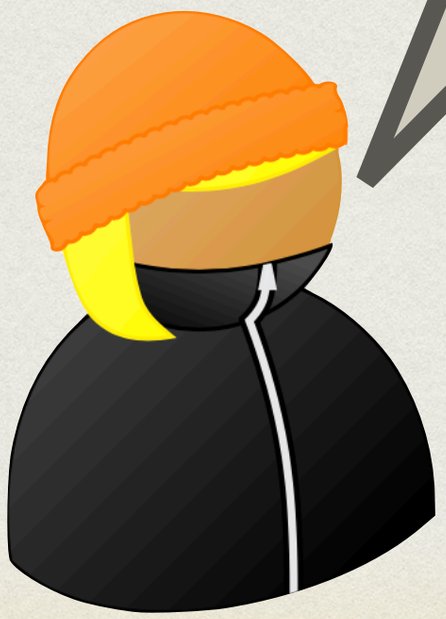
CLASSES DE COMPLEXITÉ ZK

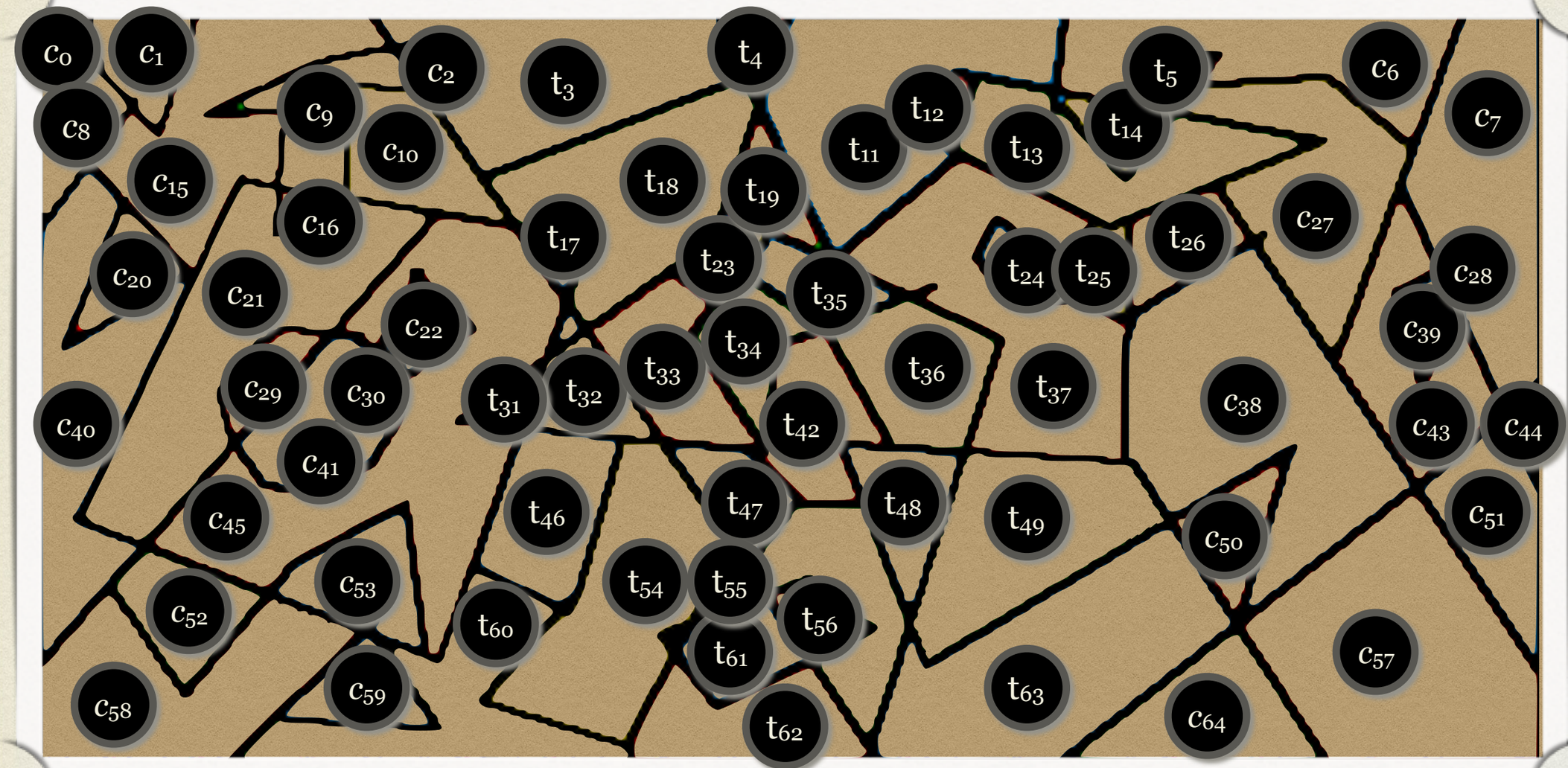


CLASSES DE COMPLEXITÉ ZK

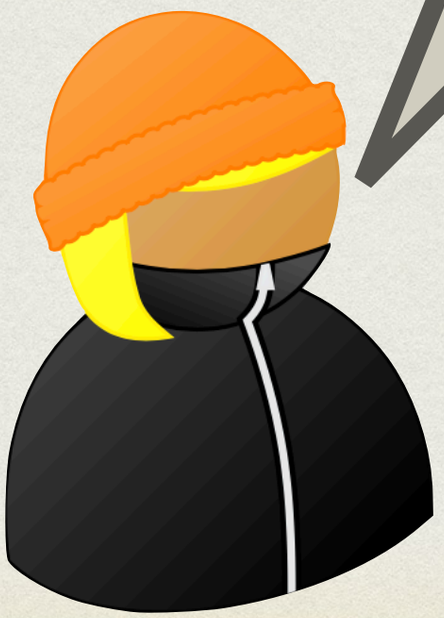







c0
c1
c2
t3
t4
t5
c6
c7
c8
c9
c10
t11
t12
t13
t14
c15
t18
t19
c16
t17
t23
t24
t25
t26
c27
c20
c21
t35
c28
c22
c39
t34
t33
t36
t37
c29
c30
t31
t32
c38
c40
t42
c43
c44
c41
c45
t46
t47
t48
t49
c50
c51
c53
t54
t55
c52
t56
t60
t61
c57
c59
t63
c58
t62
c64

COHÉRENCE INTRIQUÉE ?



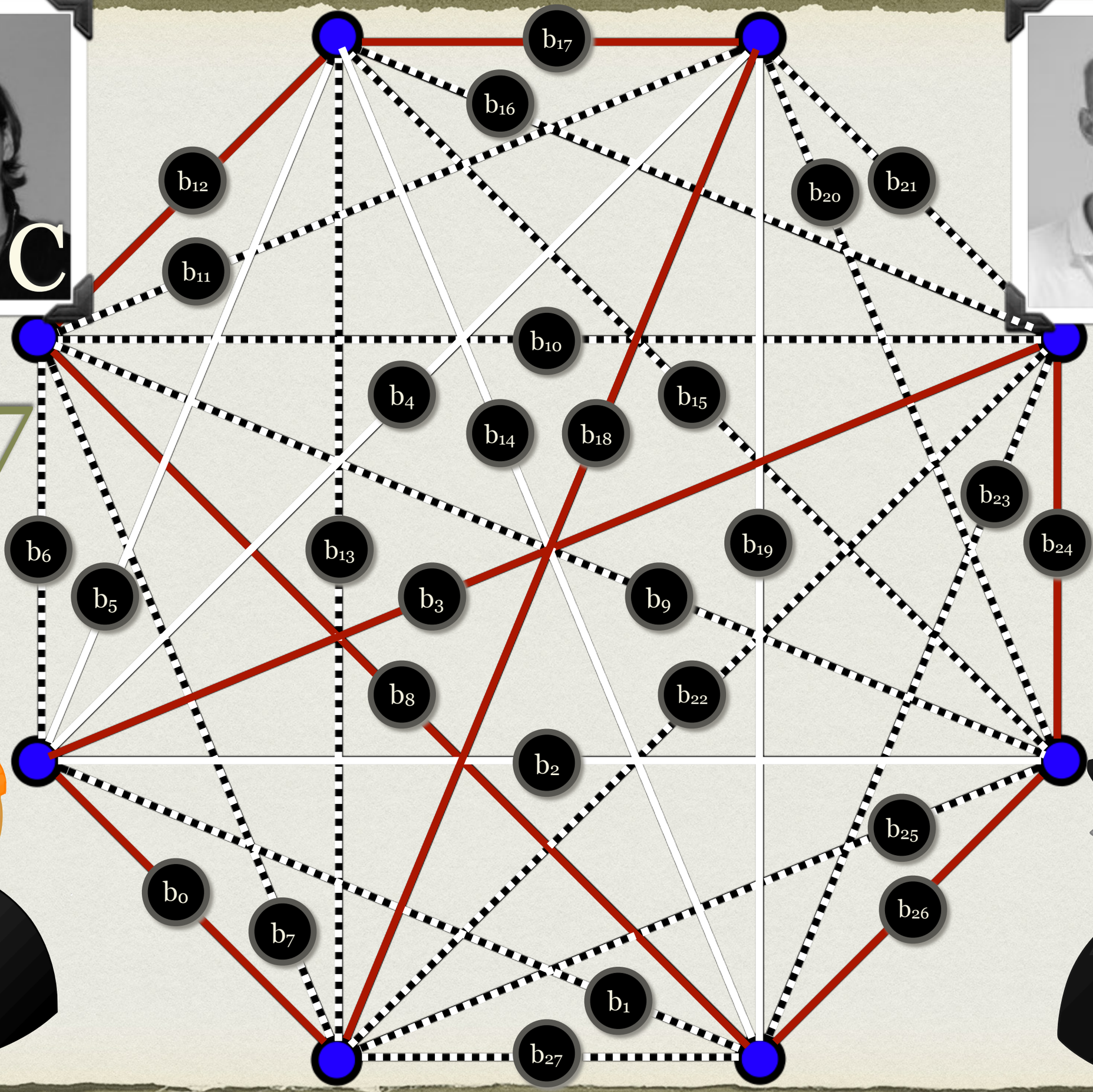
COHÉRENCE INTRIQUÉE ?

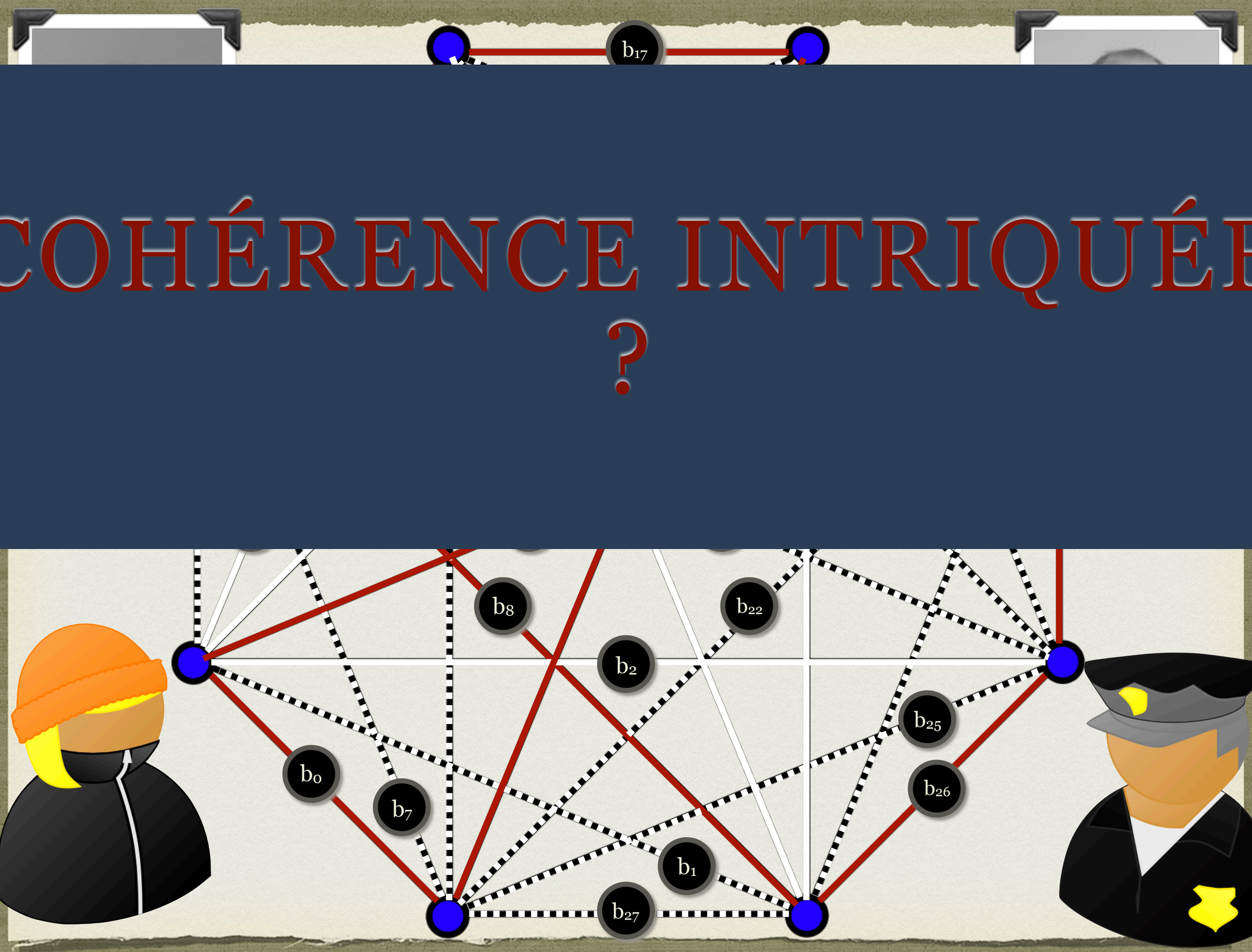
SAIS PAS !


C


L

2017

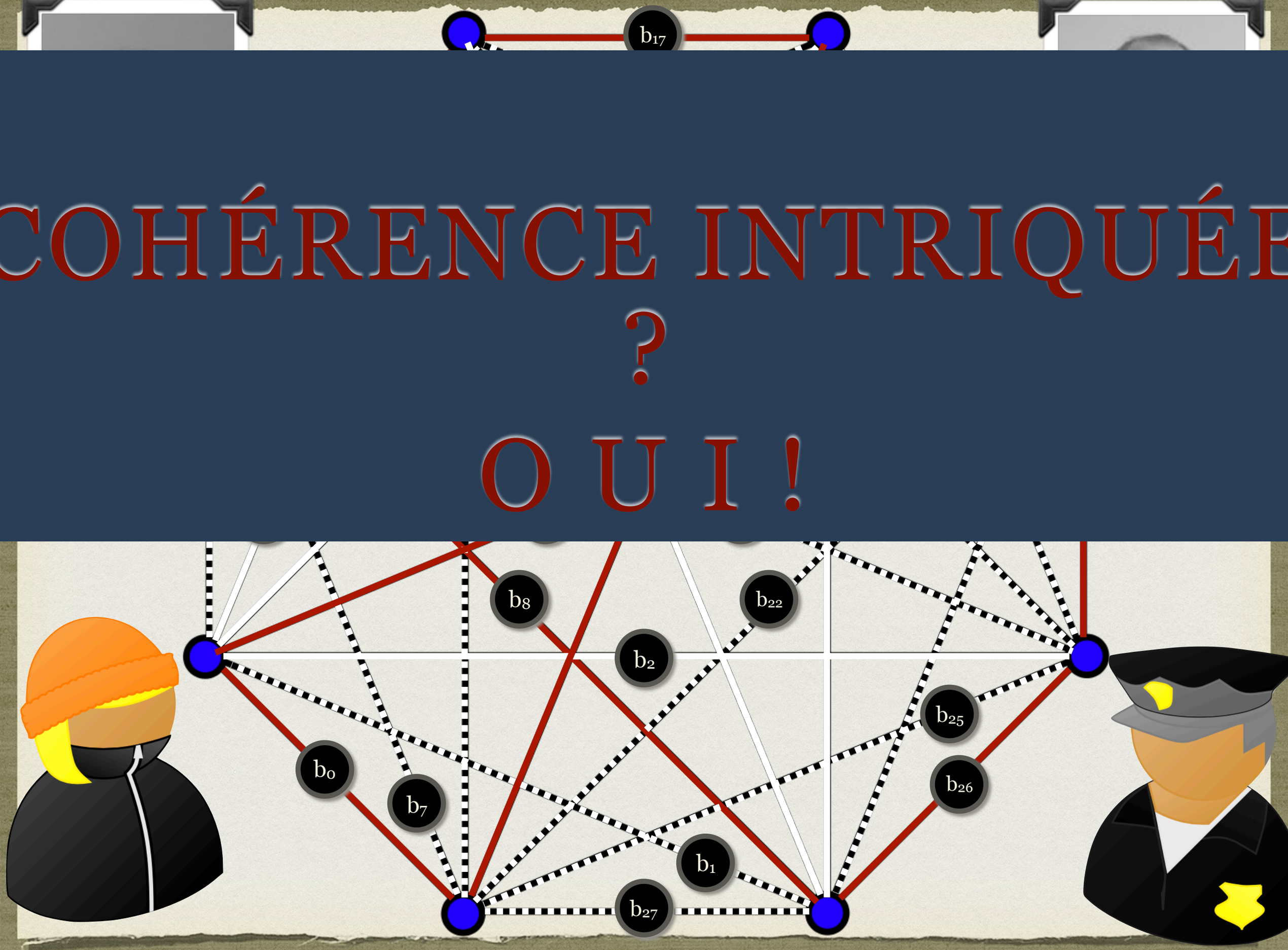

b17
b16
b12
b11
b20
b21
b10
b4
b15
b14
b18
b23
b6
b13
b19
b24
b5
b3
b9
b8
b22
b2
b25
b0
b26
b7
b1
b27

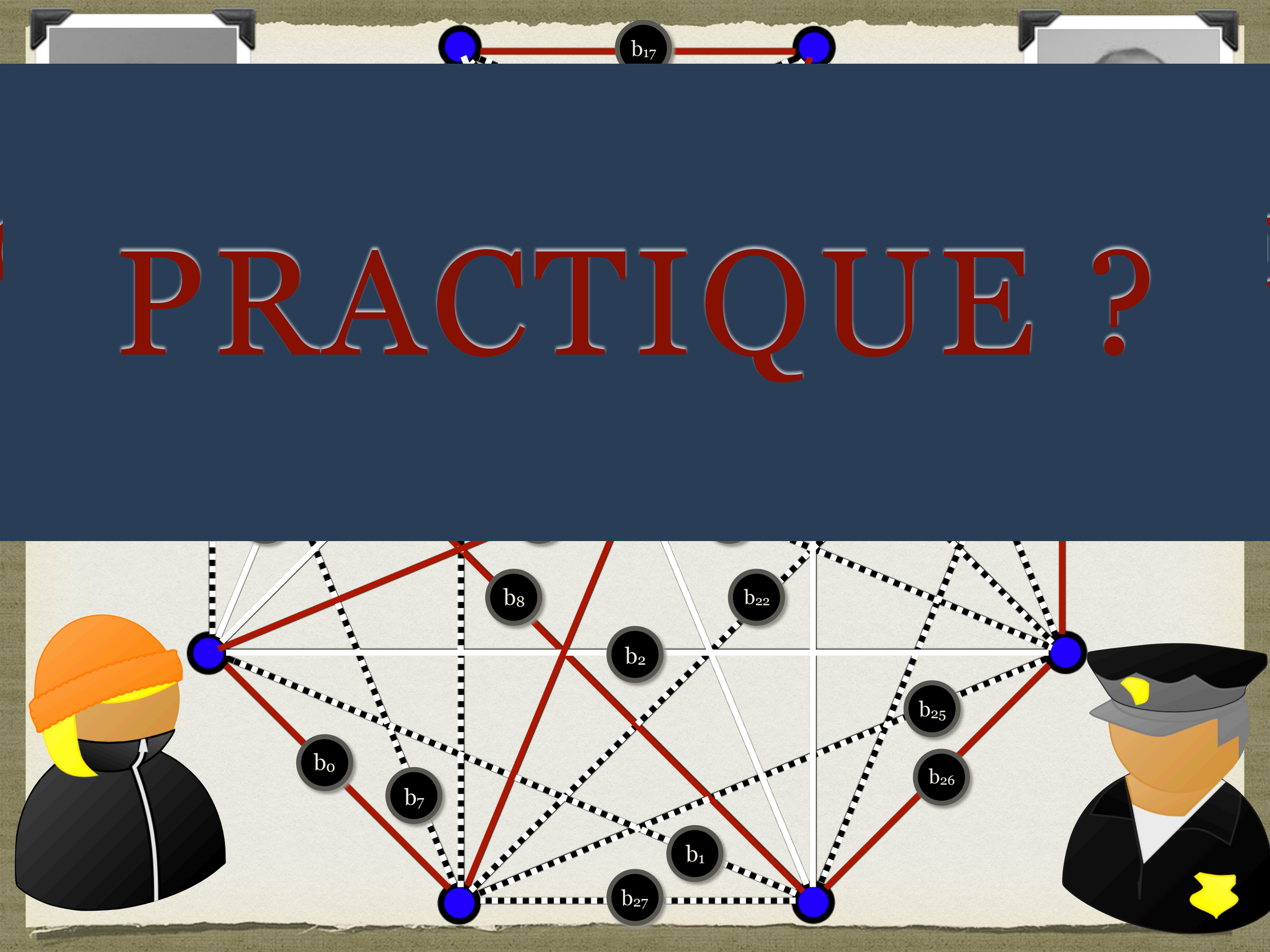


COHÉRENCE INTRIQUÉE ?

COHÉRENCE INTRIQUÉE ?

OUI !

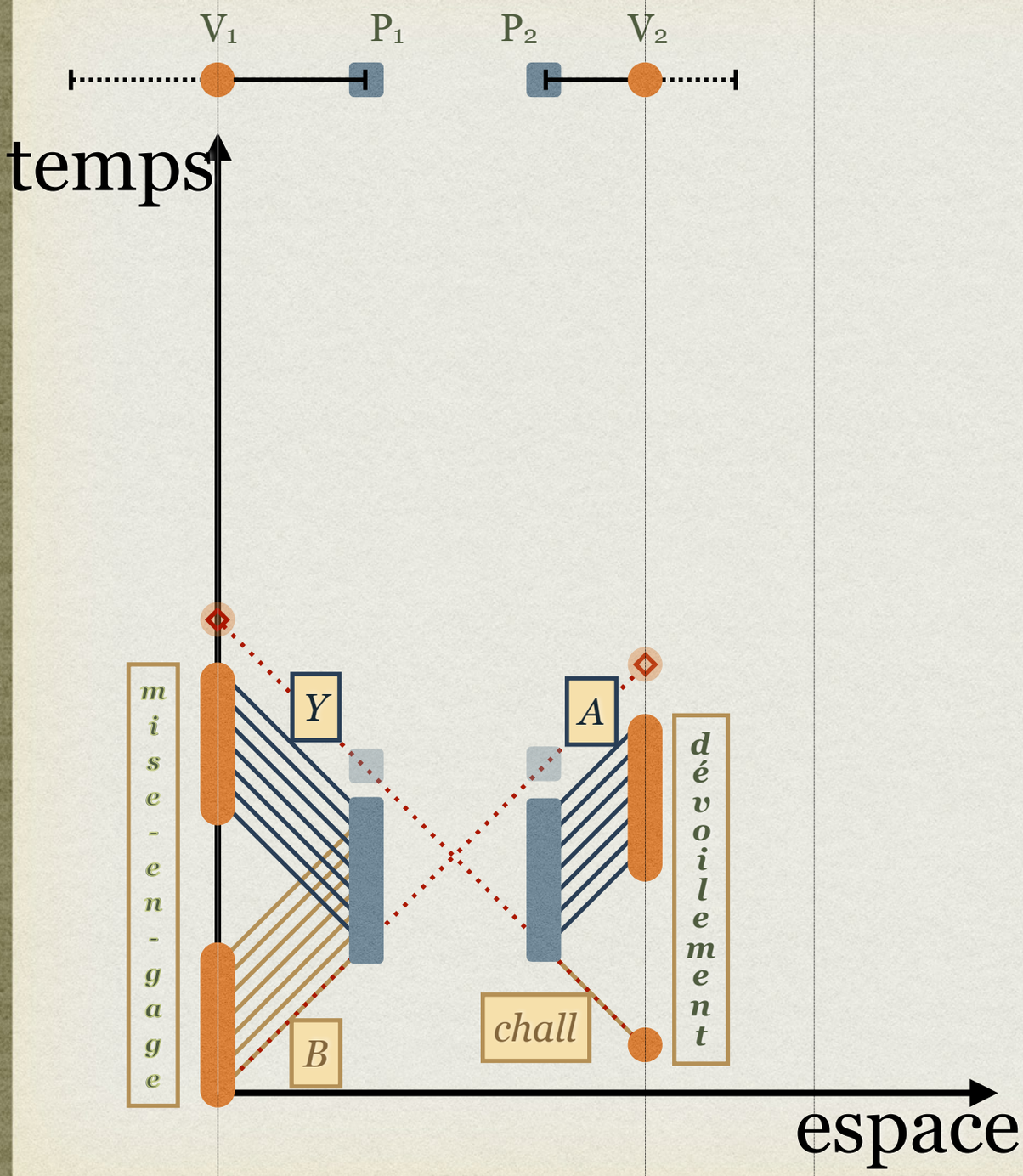


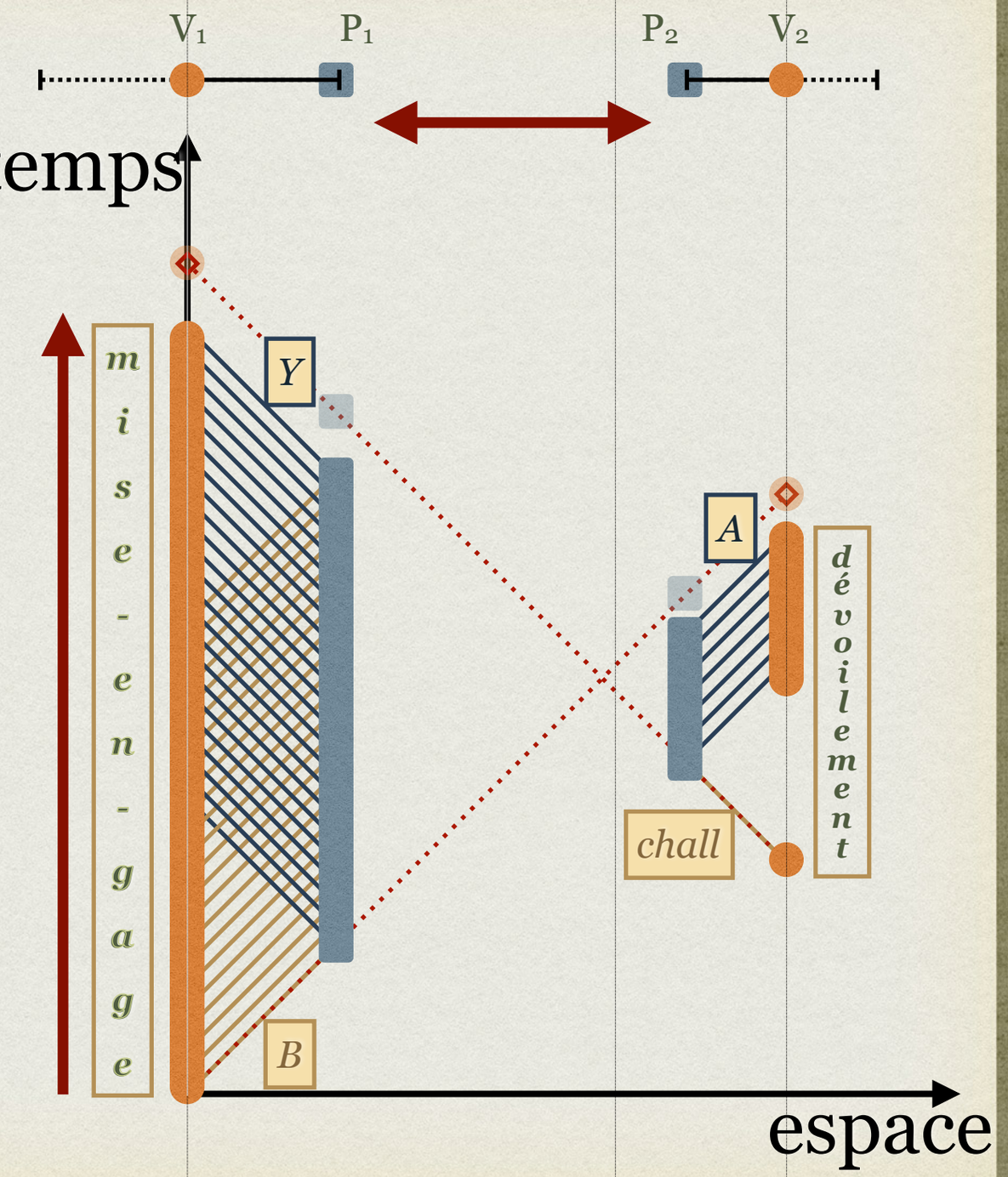

b17
PRACTIQUE ?
b8
b22
b2
b25
b0
b7
b26
b1
b27

PRACTIQUE ?

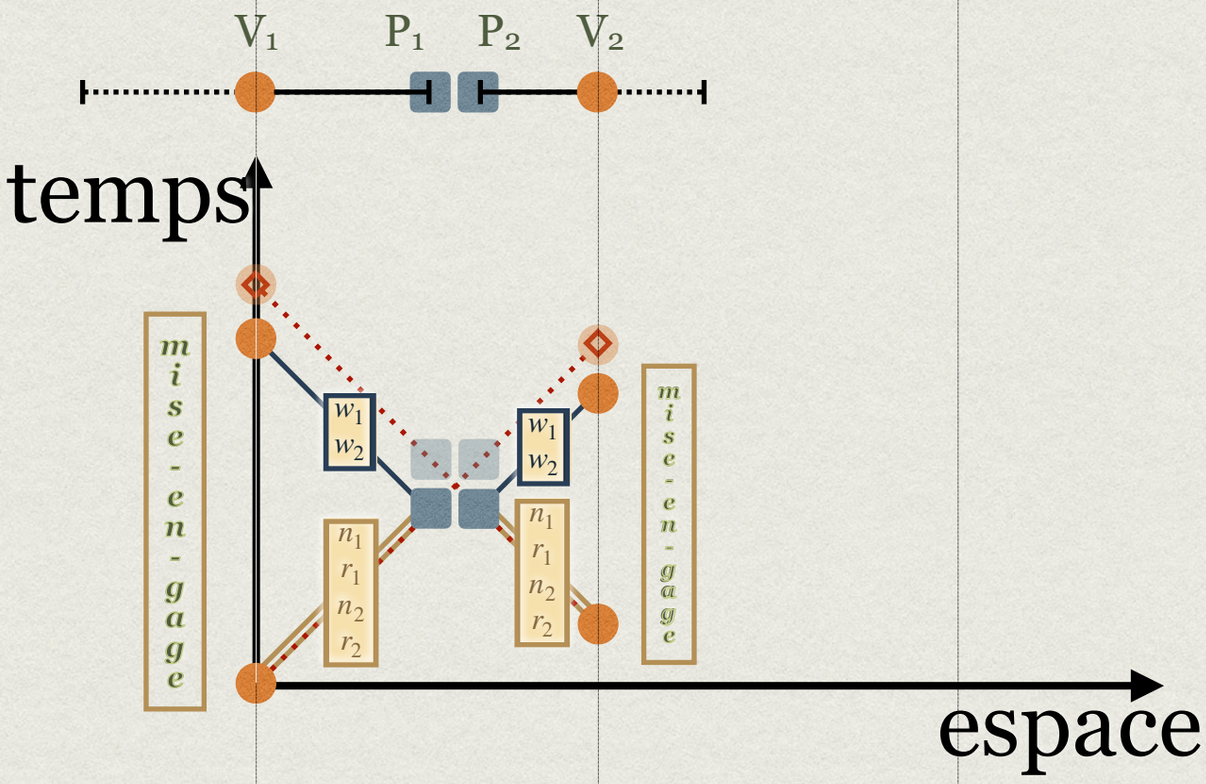
OH QUE NON !

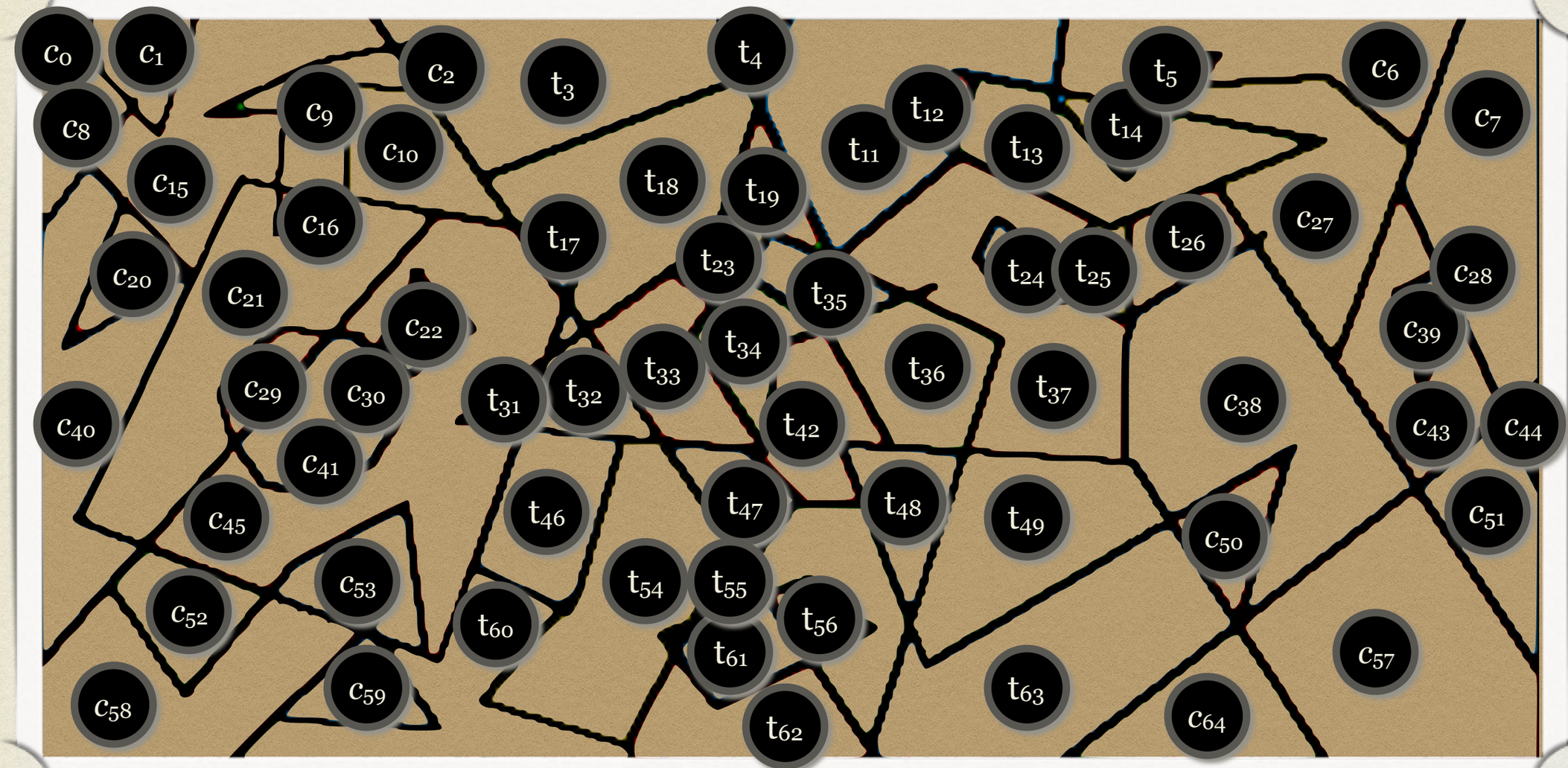
Chailloux-Leverrier





Massenet Salvail Stinchcombe Yang




c0
c1
c2
t3
t4
t5
c6
c7
c8
c9
c10
t11
t12
t13
t14
c15
t18
t19
c16
t17
t23
t24
t25
t26
c27
c20
c21
t35
c28
c22
c39
t34
t33
t36
t37
c29
c30
t31
t32
c38
c40
t42
c43
c44
c41
c45
t46
t47
t48
t49
c50
c51
c53
t54
t55
c52
t56
t60
t61
c57
c59
t63
c58
t62
c64

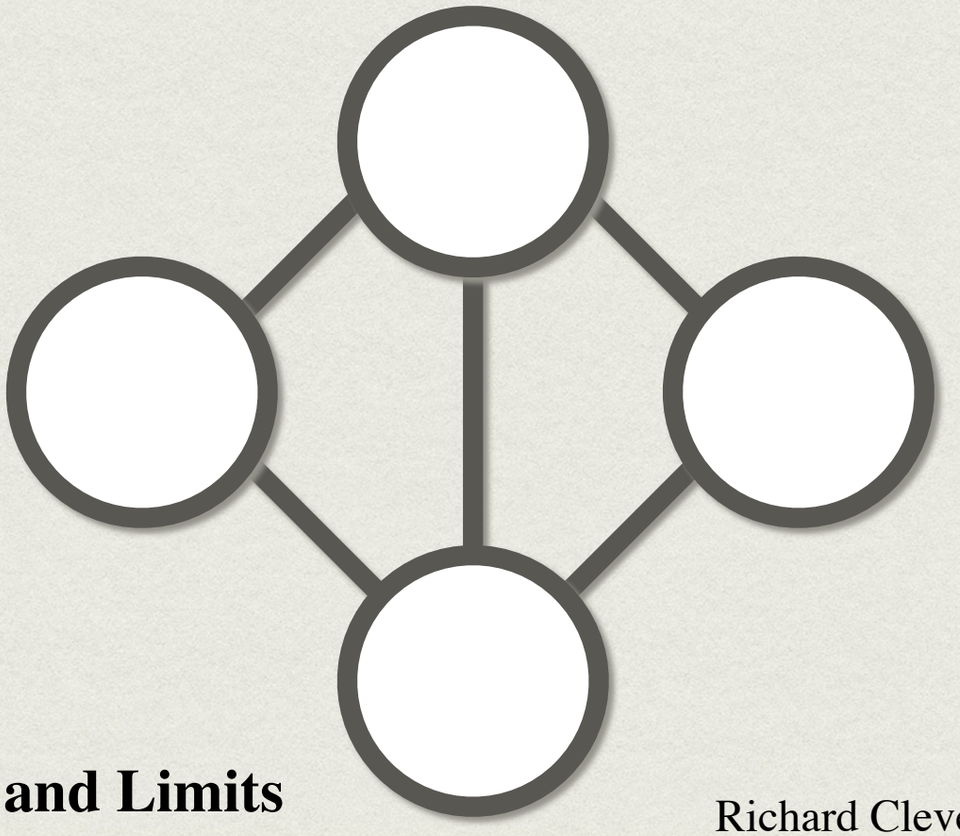
NOTRE APPROCHE

(ZK)MIPs





2004 Complétude



Consequences and Limits of Nonlocal Strategies

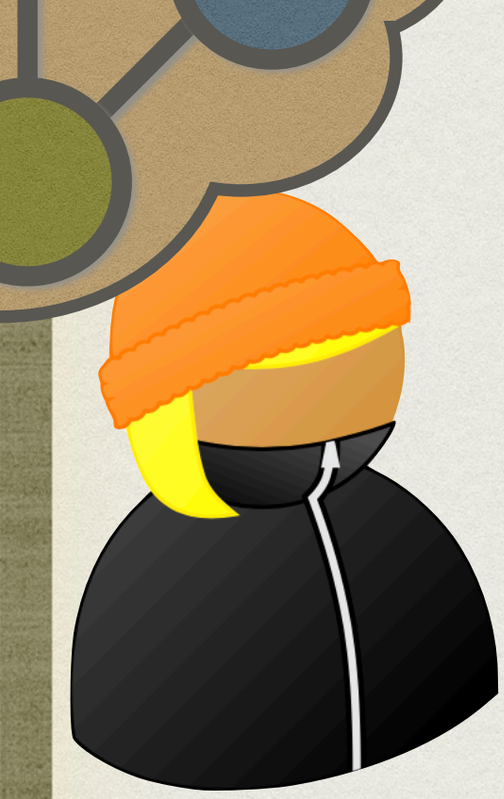
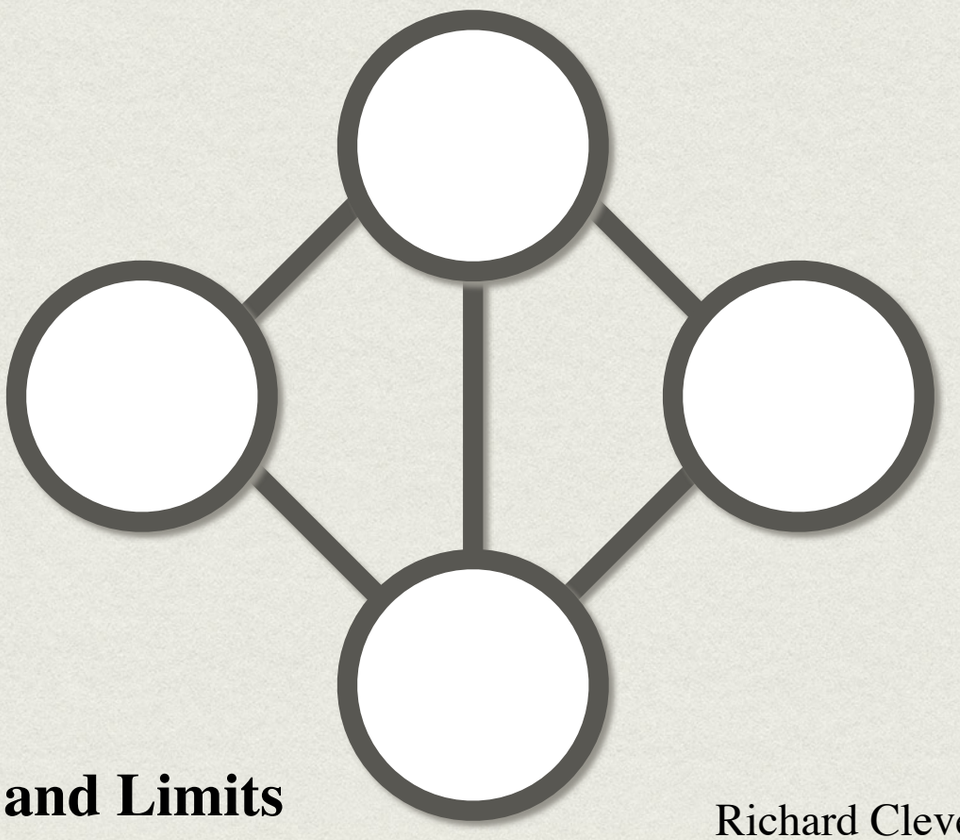
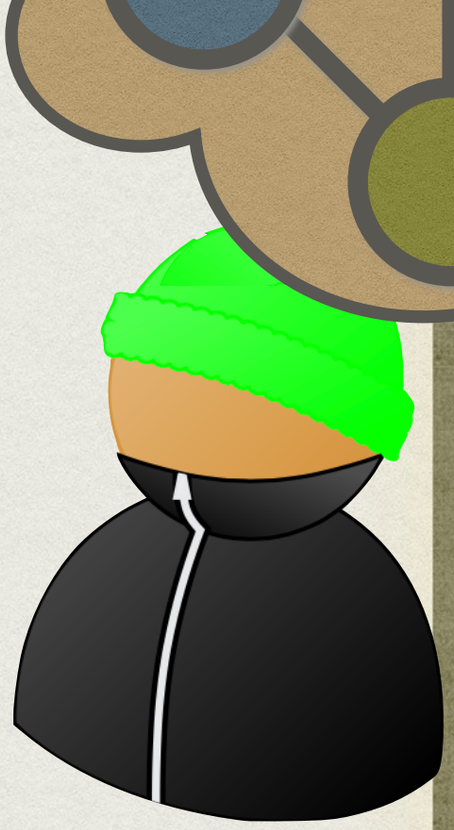
Richard Cleve Peter Høyer
Benjamin Toner John Watrous





2

2004 Complétude

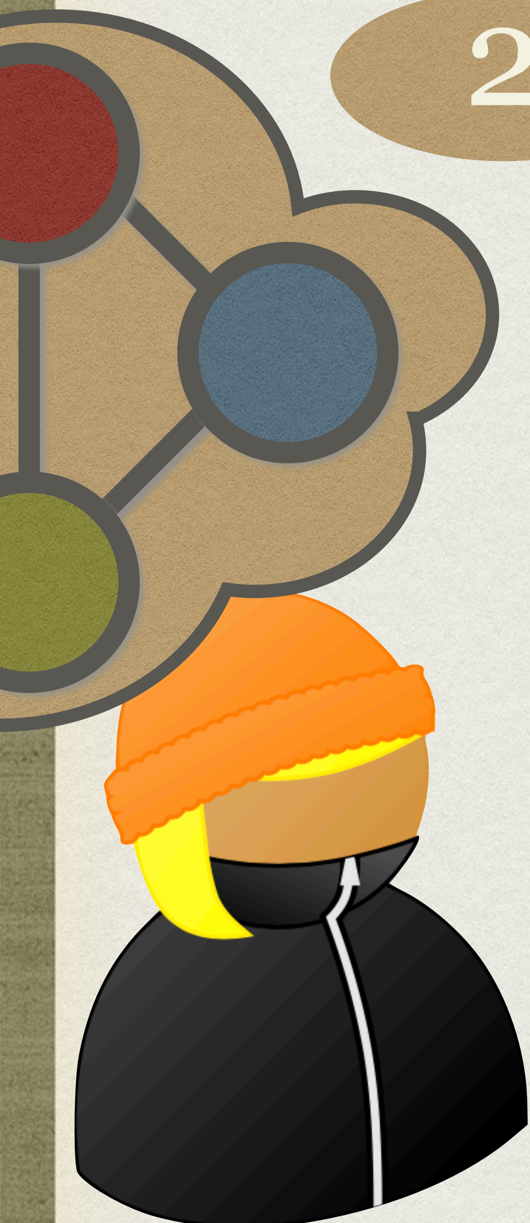




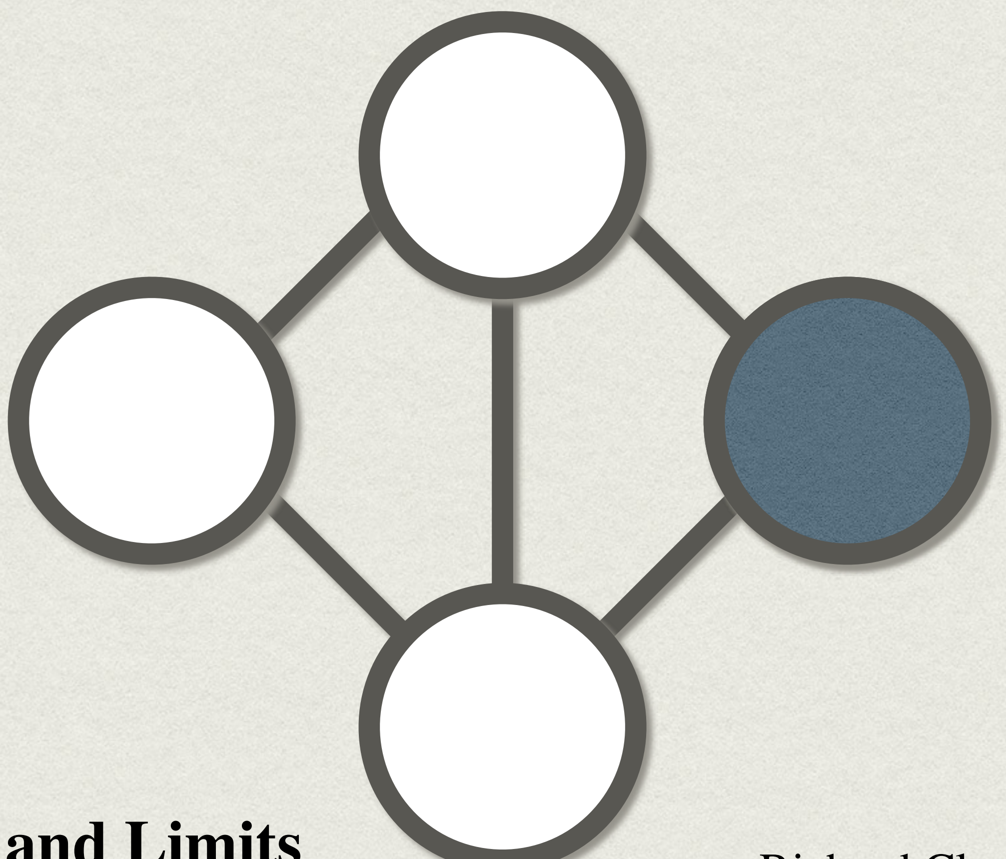
Consequences and Limits of Nonlocal Strategies

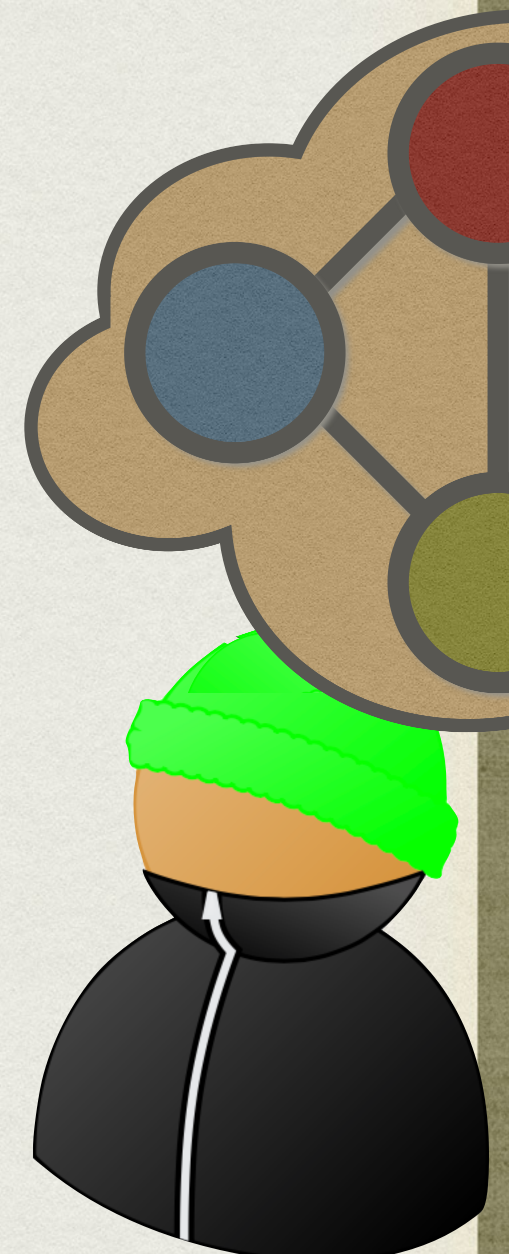
Richard Cleve Peter Høyer
Benjamin Toner John Watrous

2004

COMPLÉTUDE





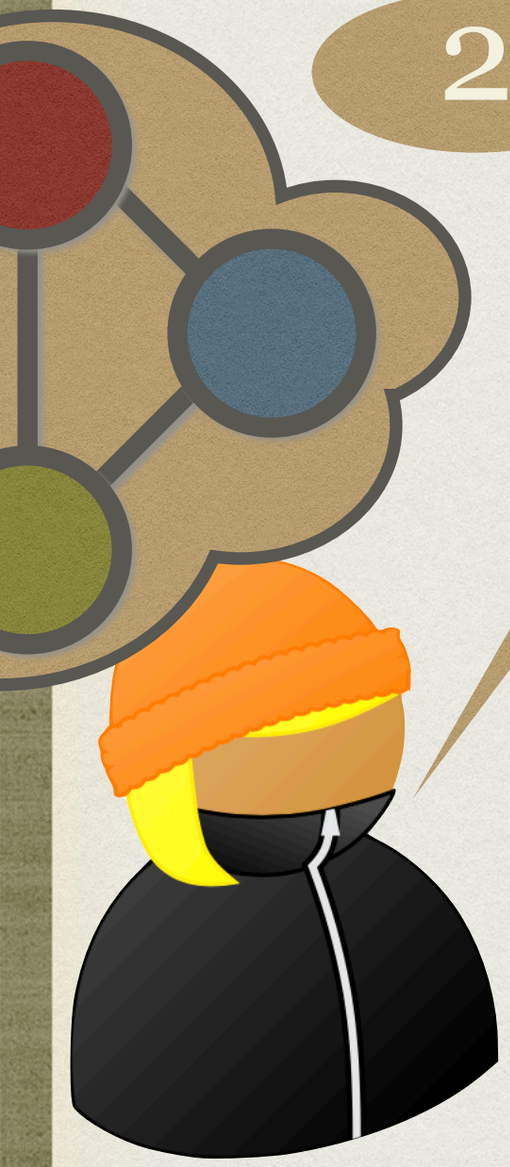


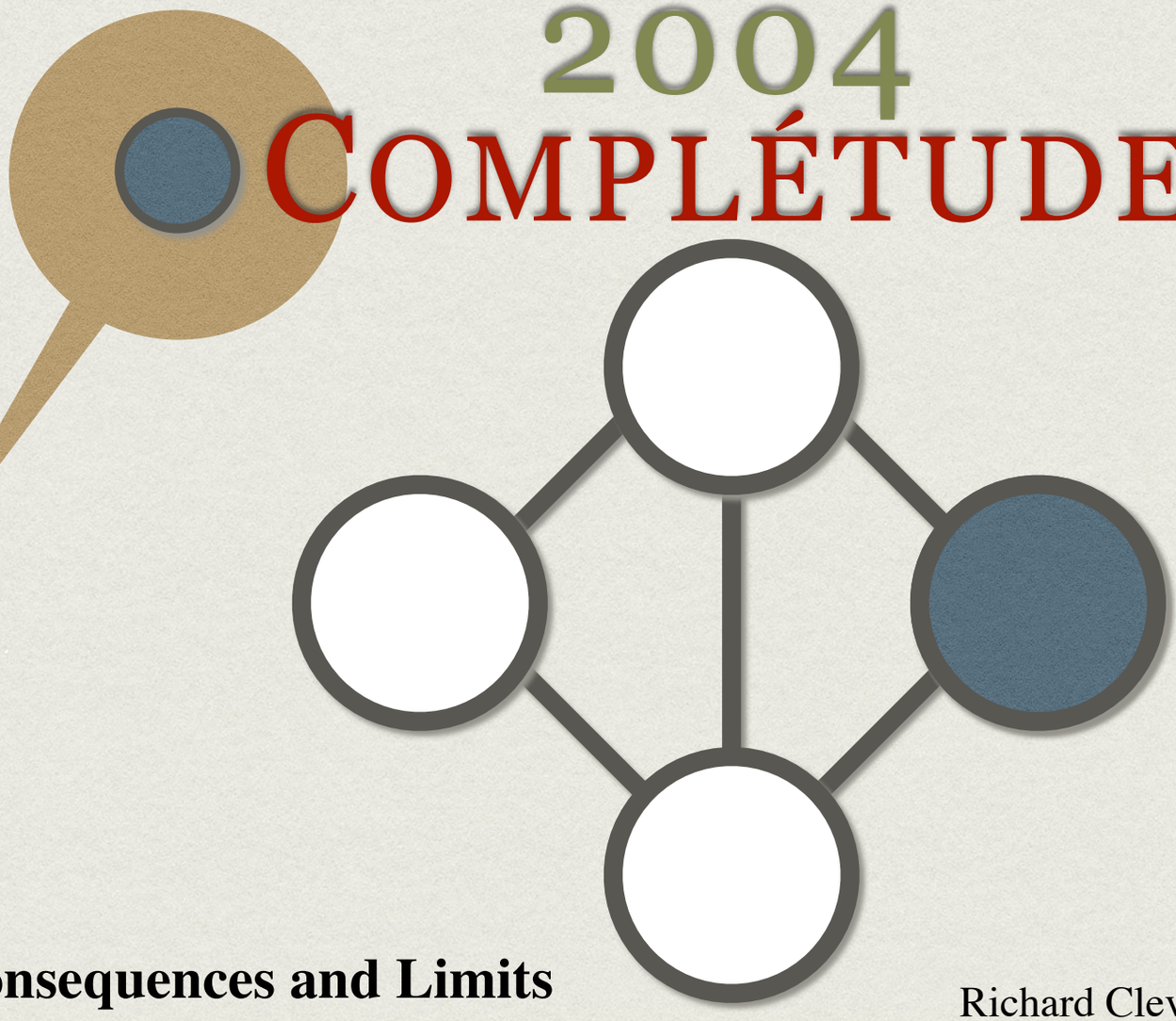
Consequences and Limits of Nonlocal Strategies

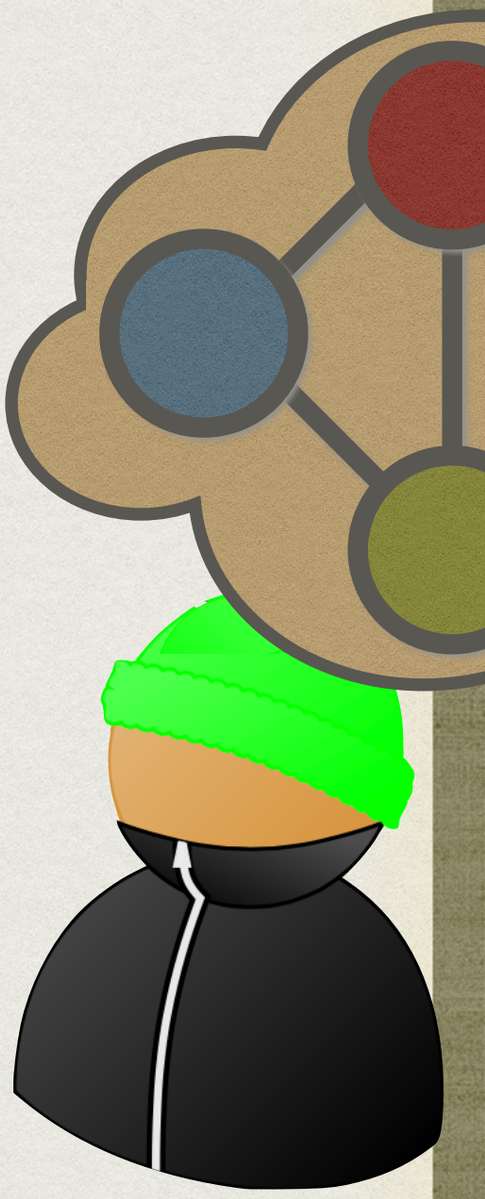
Richard Cleve Peter Høyer
Benjamin Toner John Watrous

2

2004 Complétude







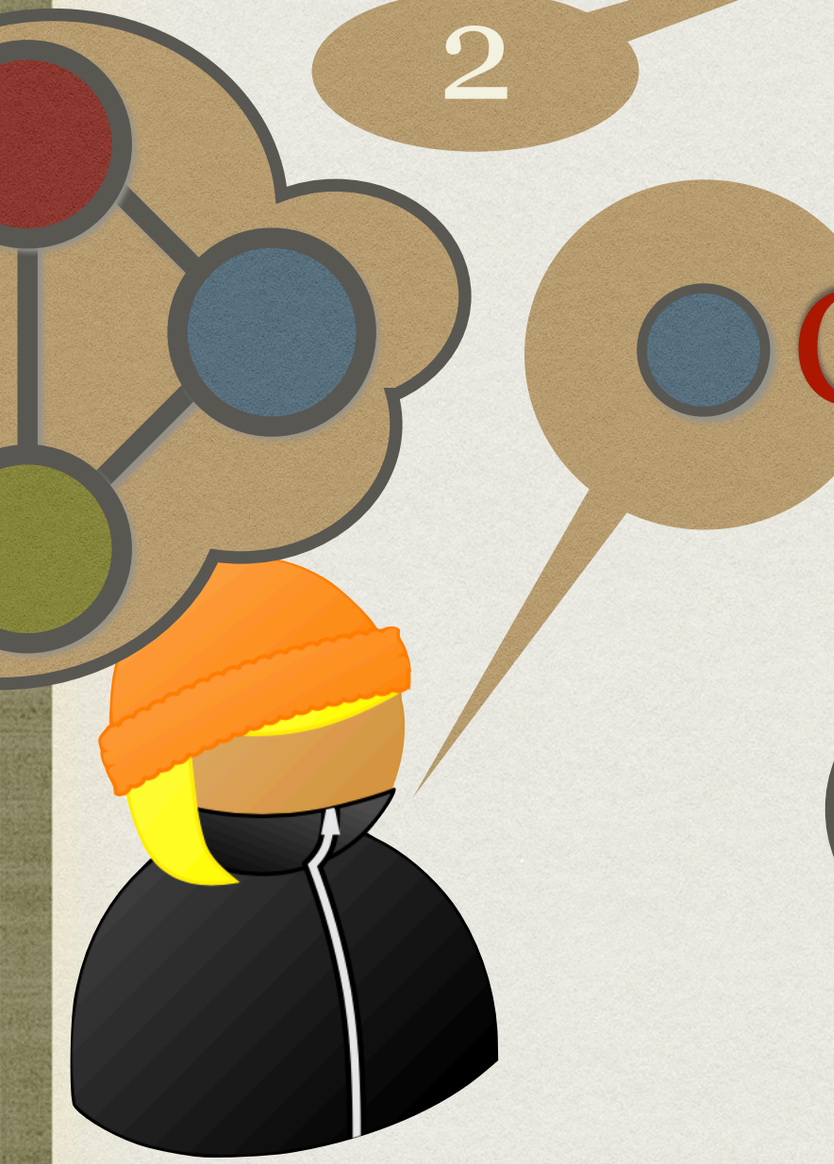
Consequences and Limits of Nonlocal Strategies

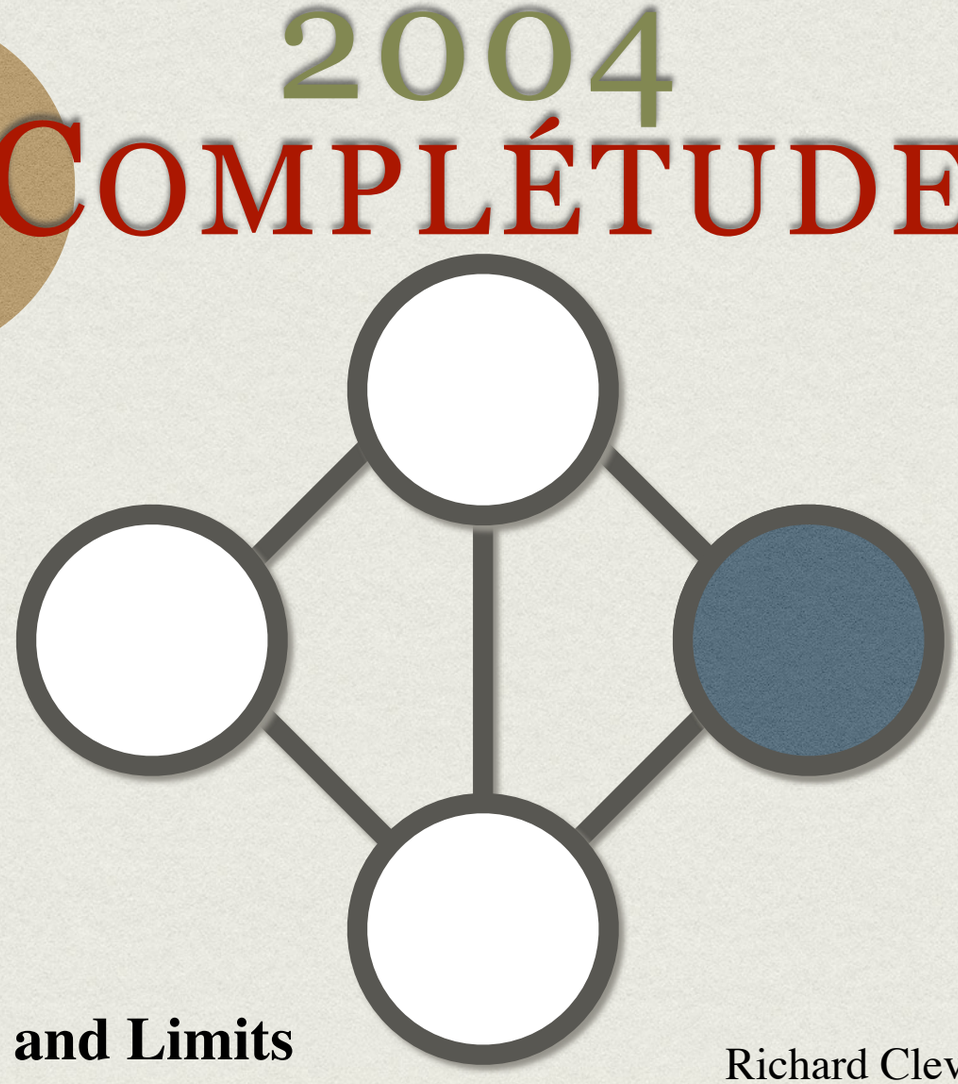
Richard Cleve Peter Høyer
Benjamin Toner John Watrous

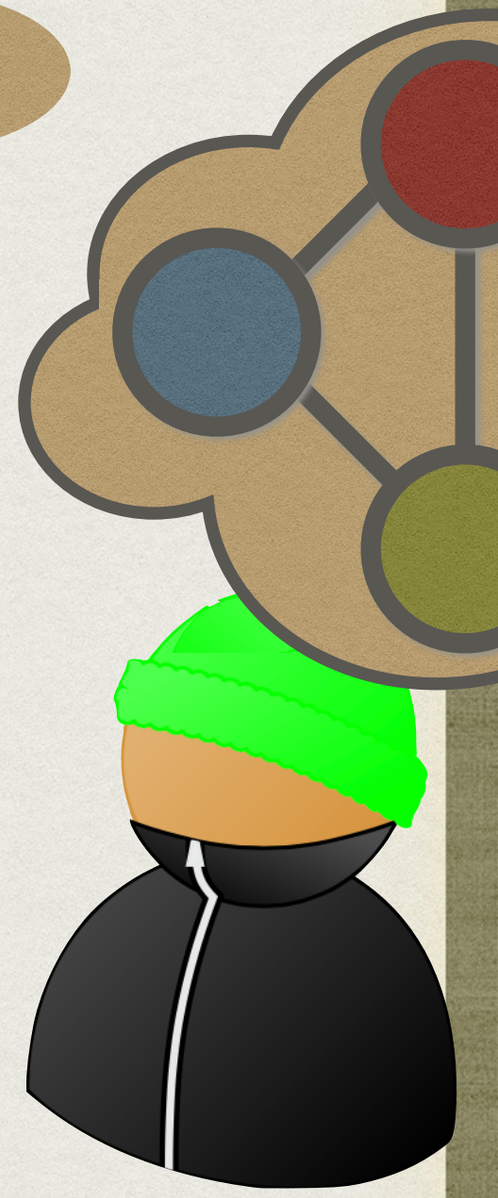
2

3

2004
Complétude







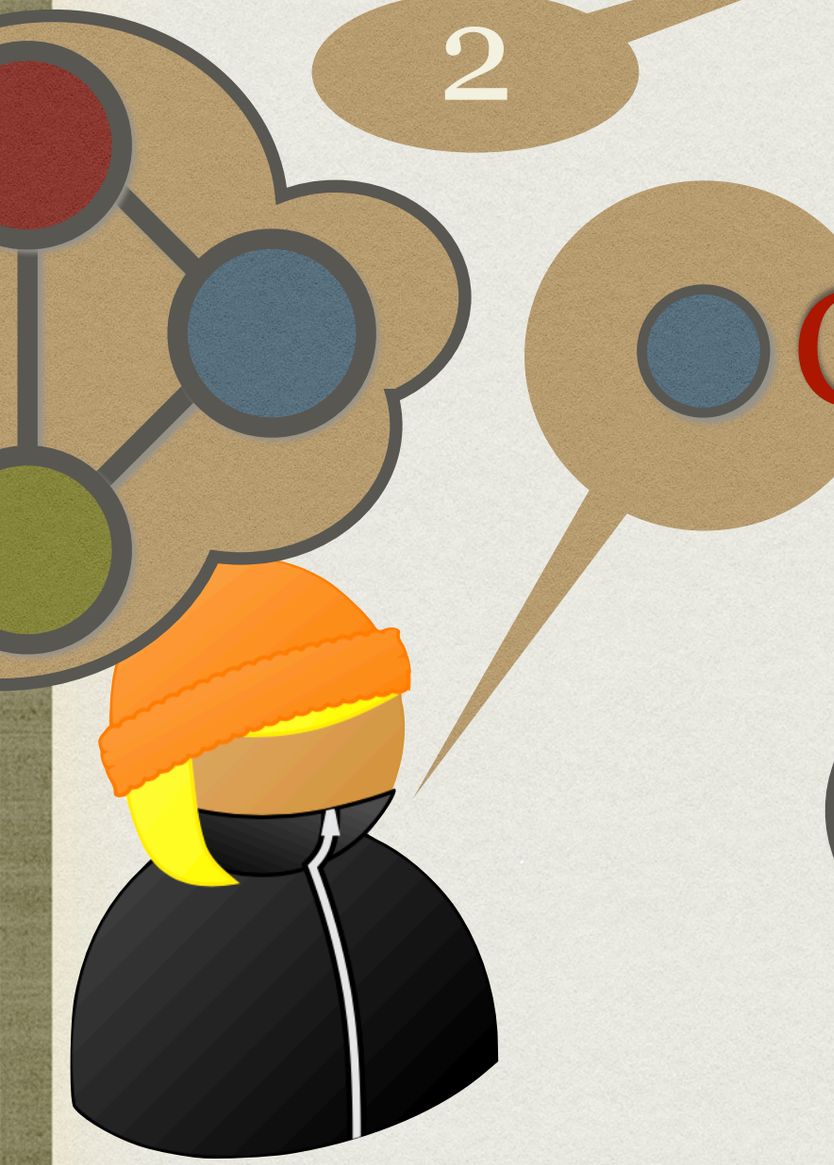
Consequences and Limits of Nonlocal Strategies

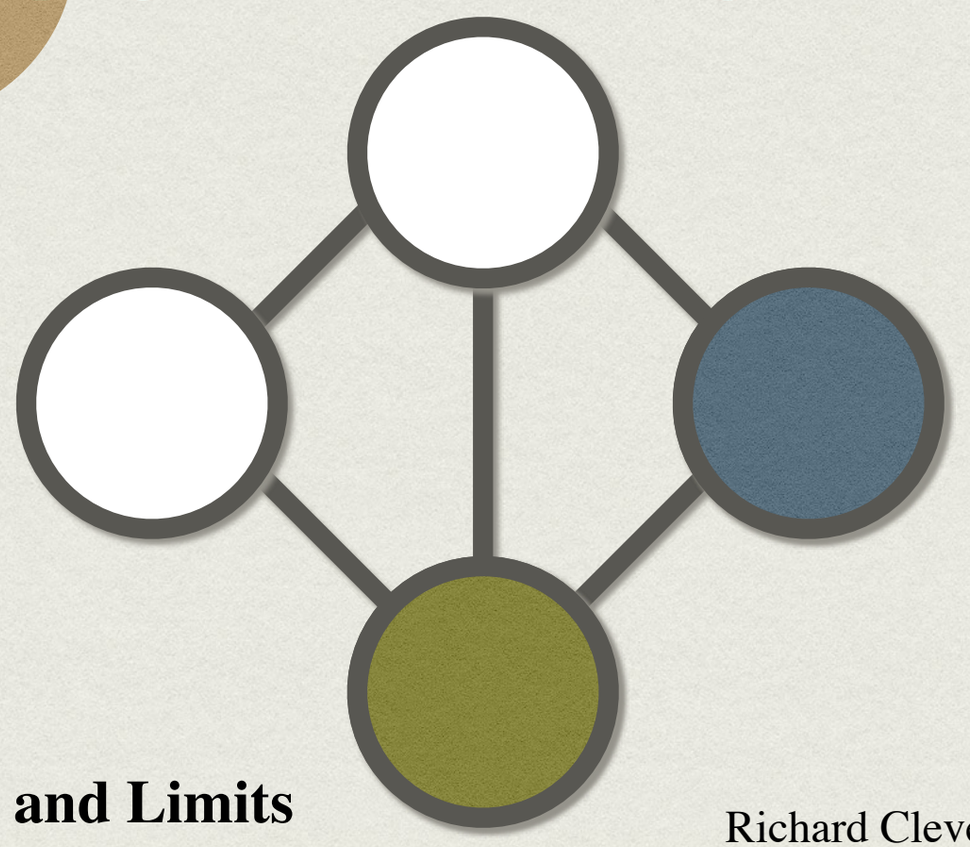
Richard Cleve Peter Høyer
Benjamin Toner John Watrous

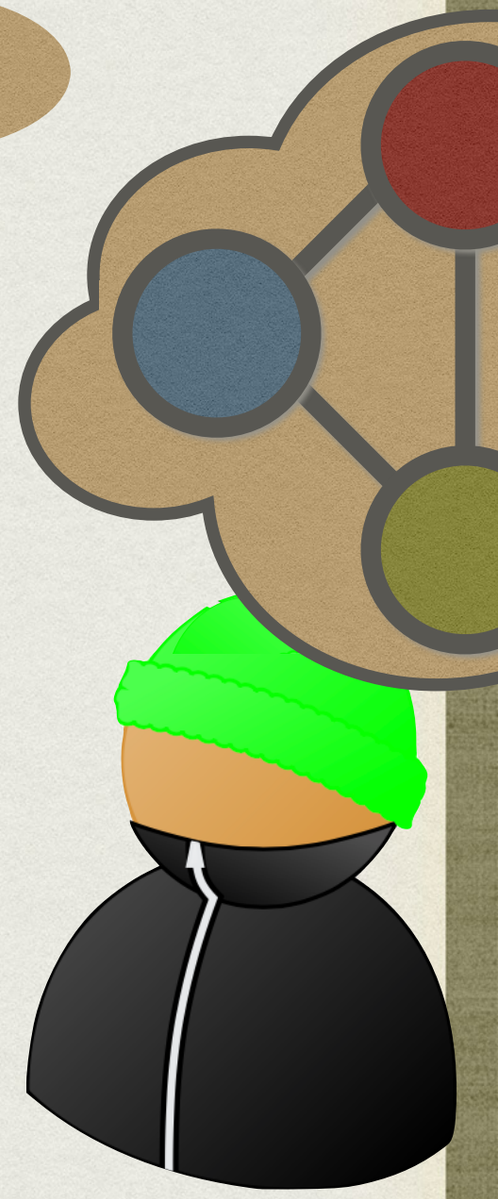
2

3

2004
Complétude







Consequences and Limits of Nonlocal Strategies

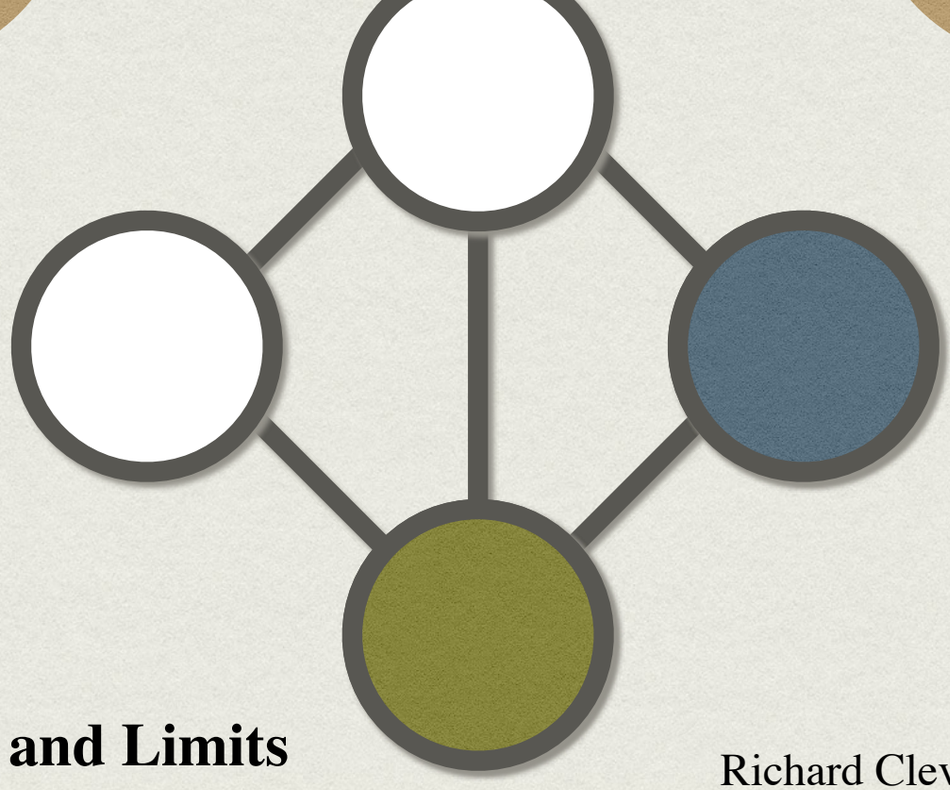
Richard Cleve Peter Høyer
Benjamin Toner John Watrous

2

3

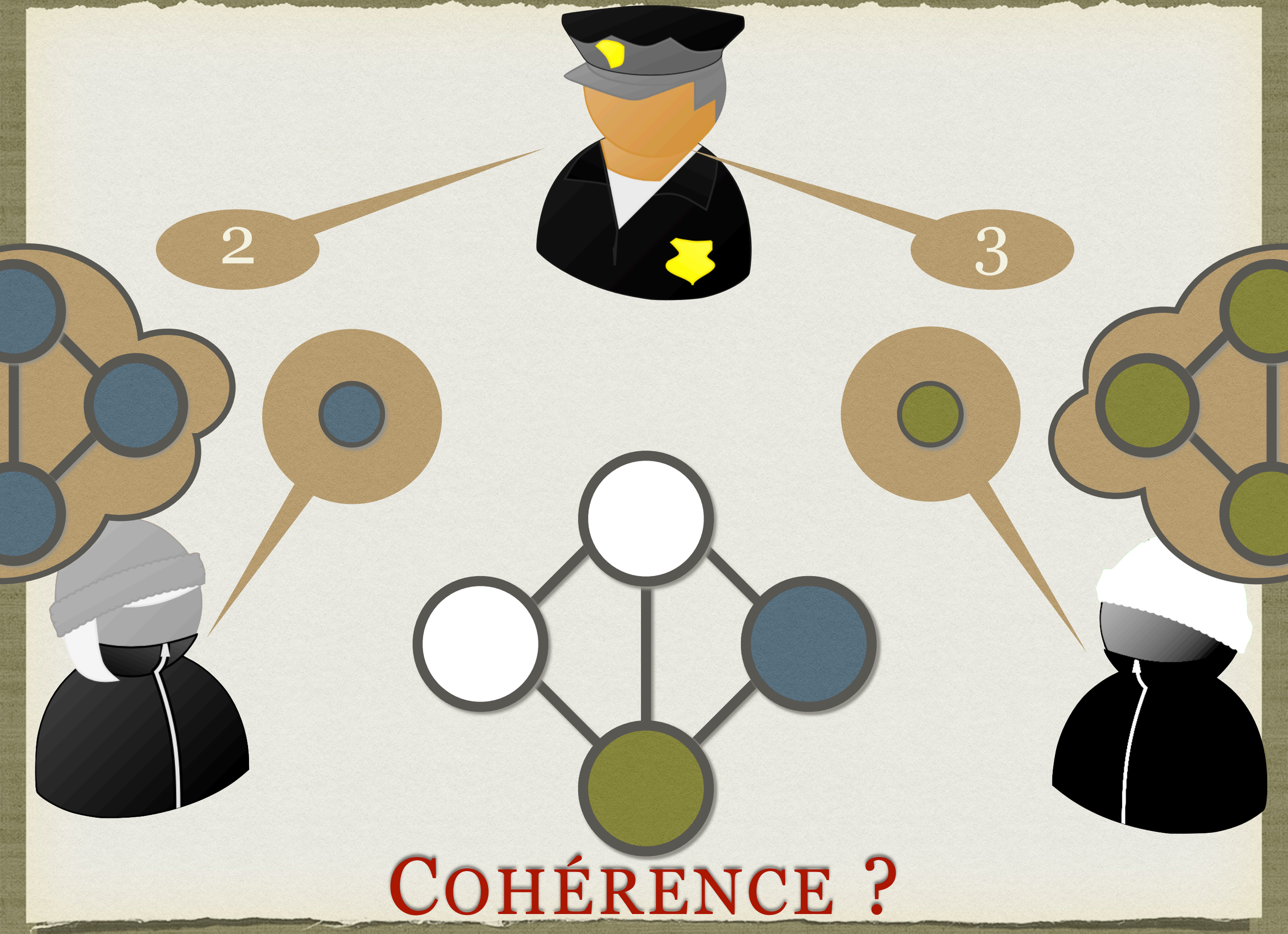
2004

Complétude



Consequences and Limits of Nonlocal Strategies

Richard Cleve Peter Høyer
Benjamin Toner John Watrous

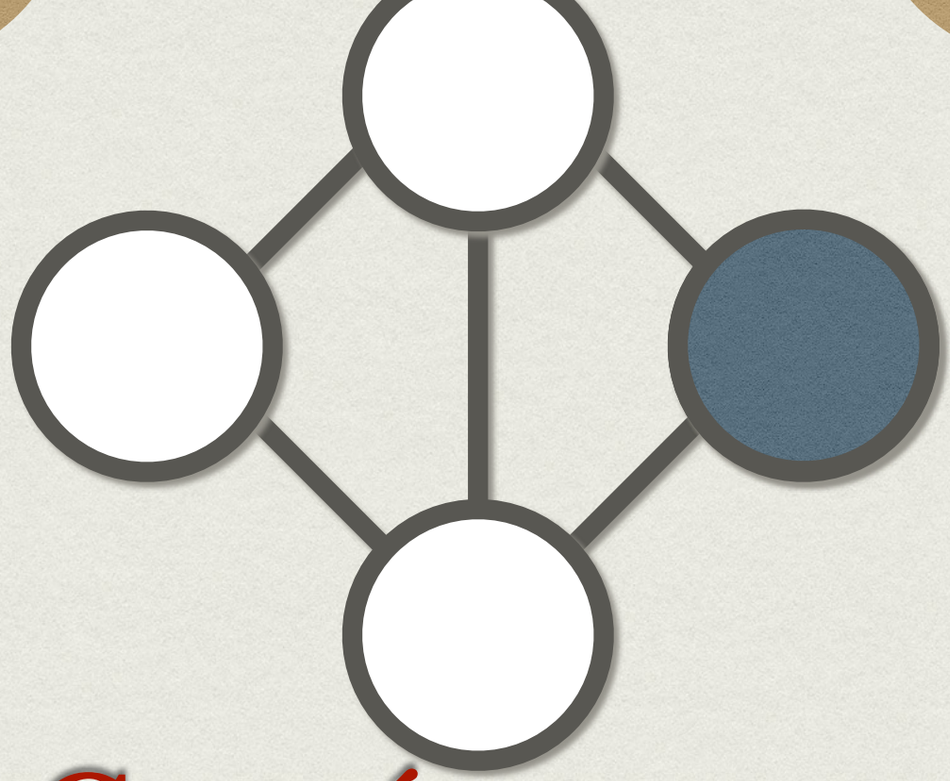


Cohérence ?

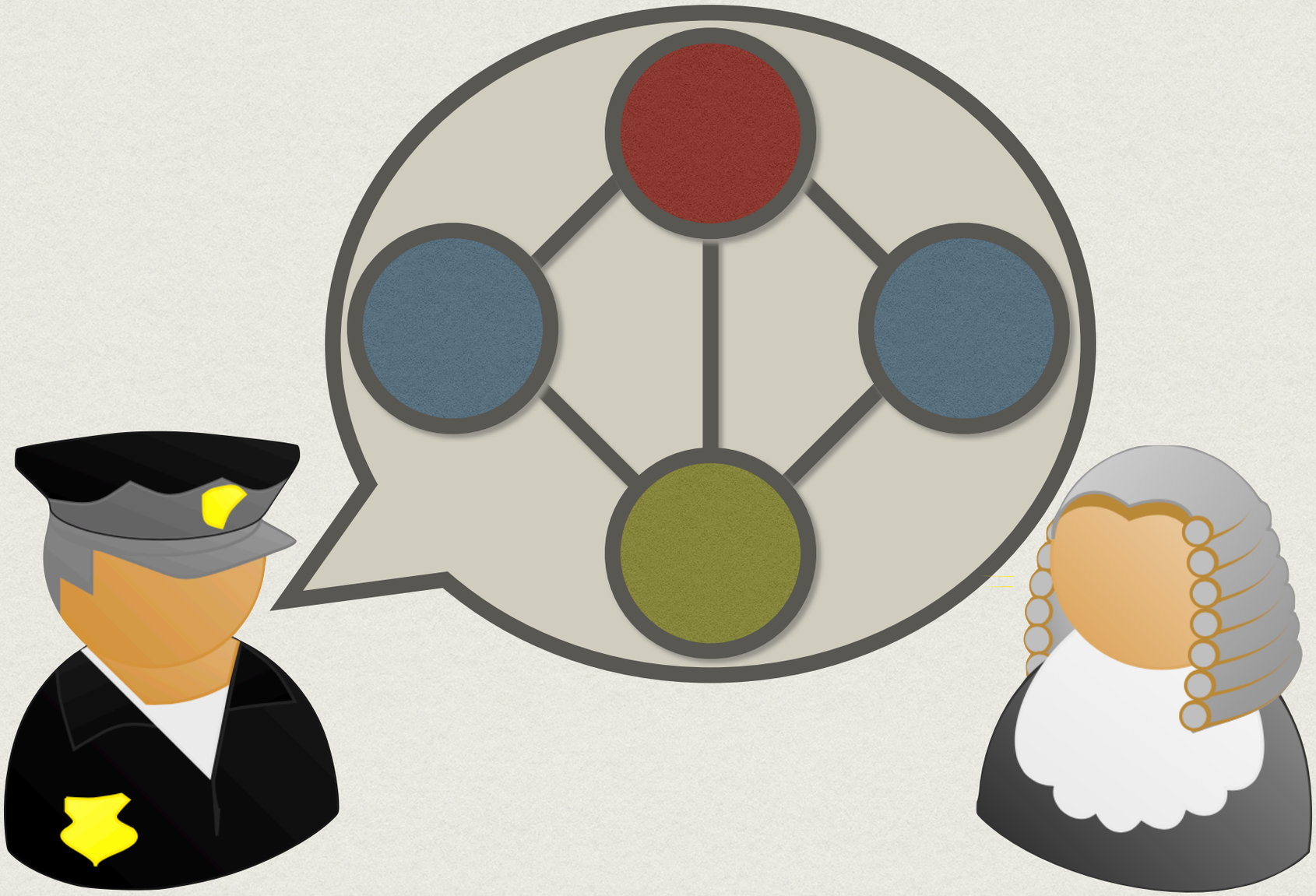
2

2

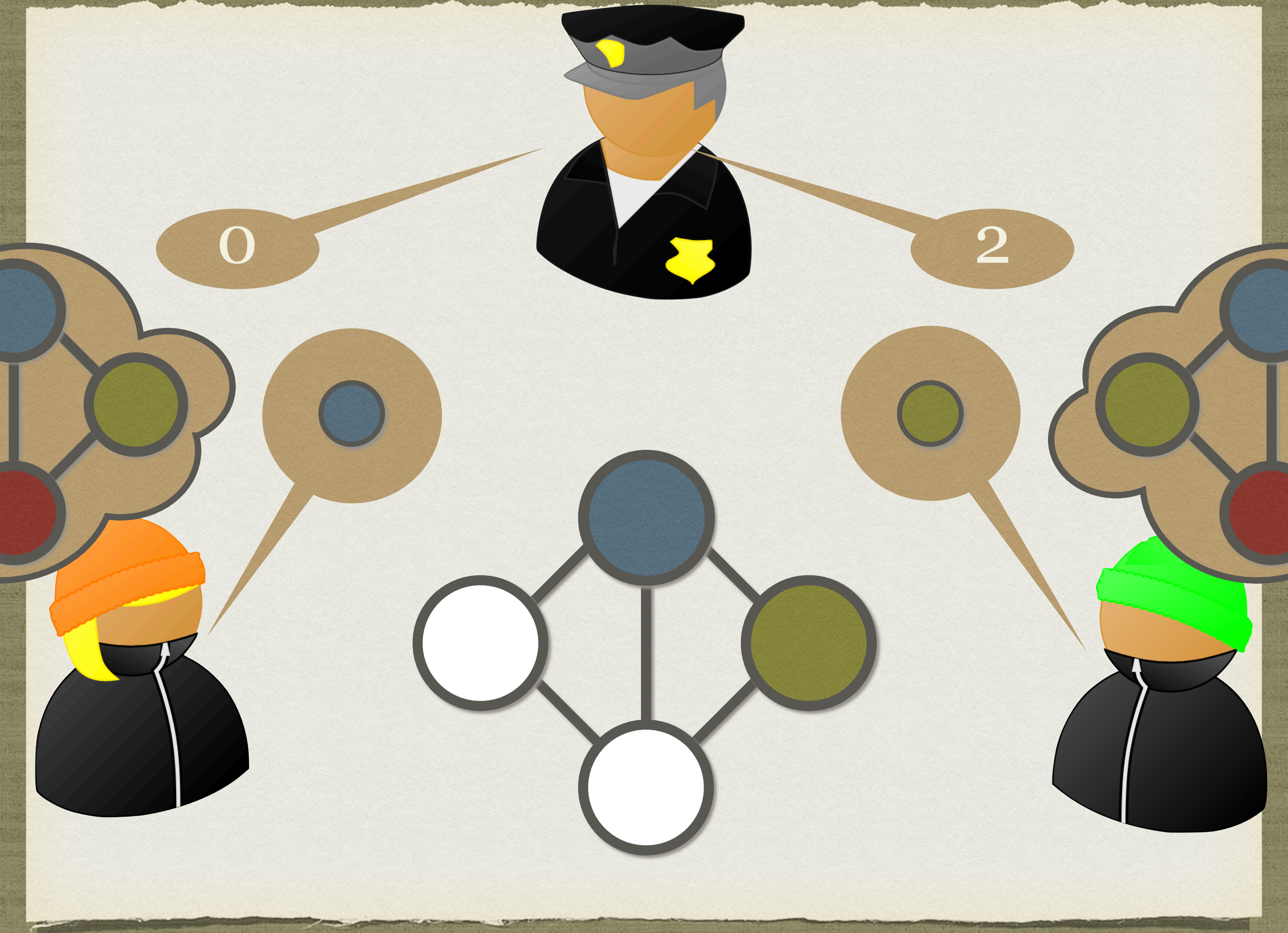
Complétude

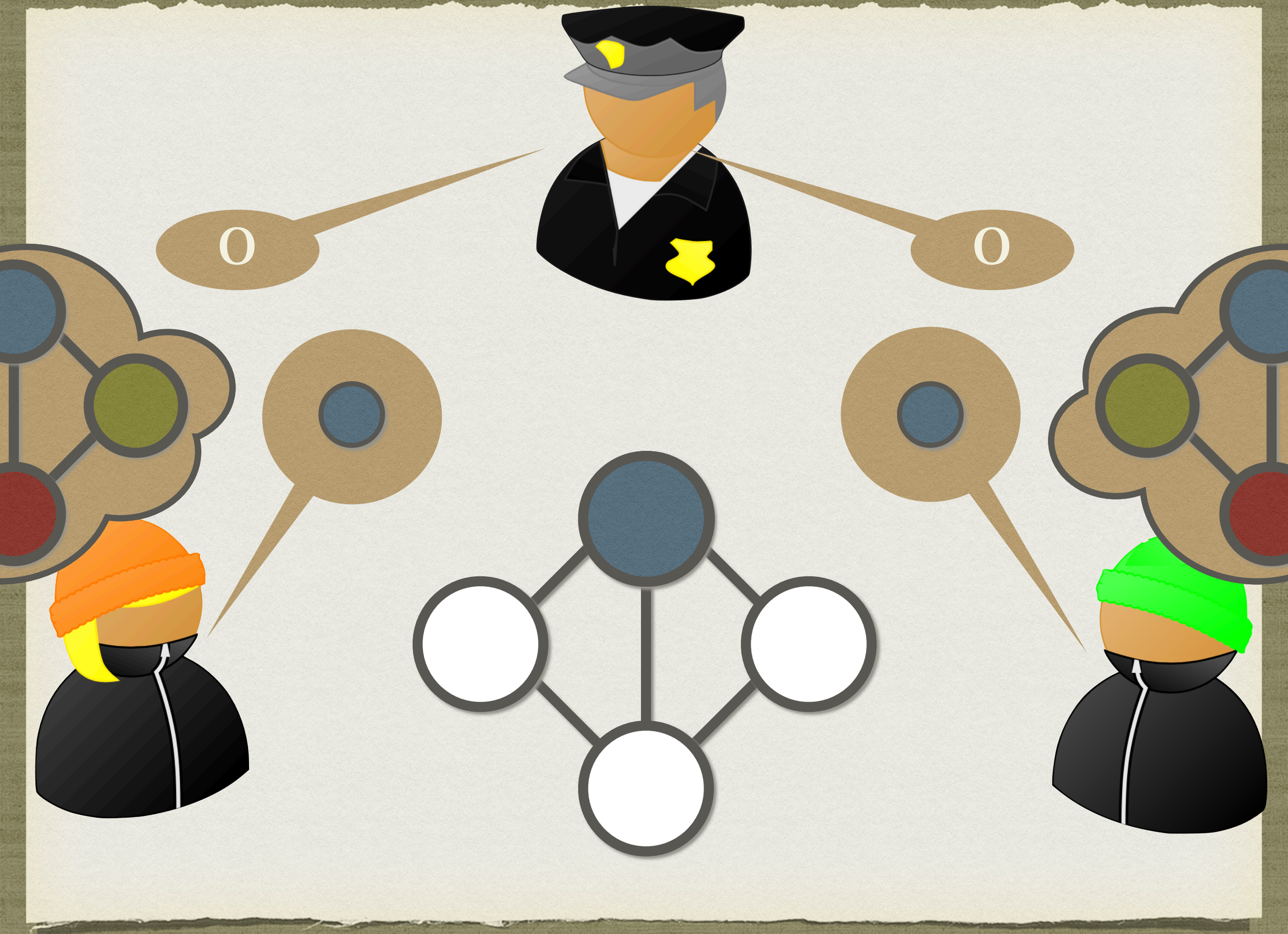


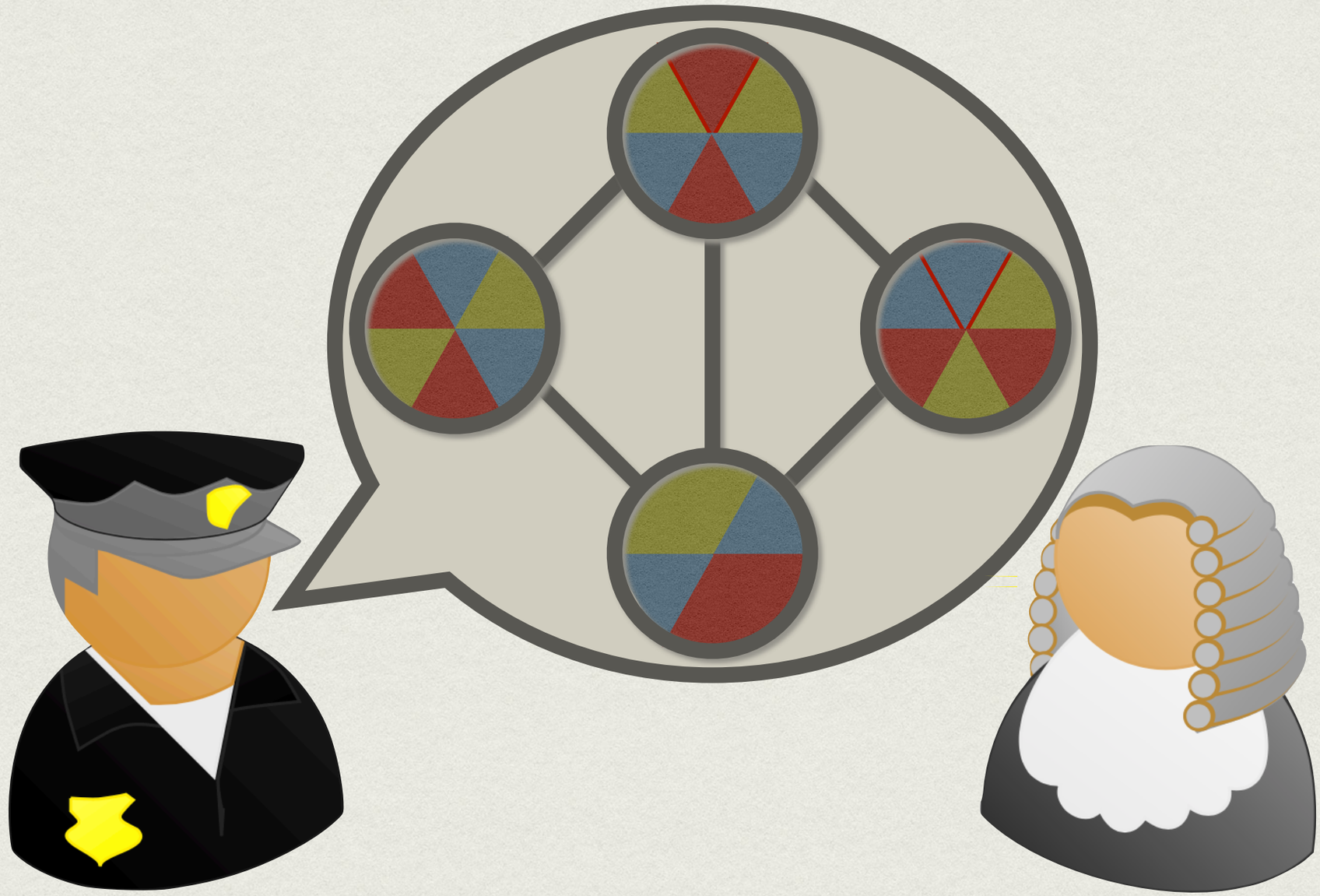
Cohérence



Transférable


0
2

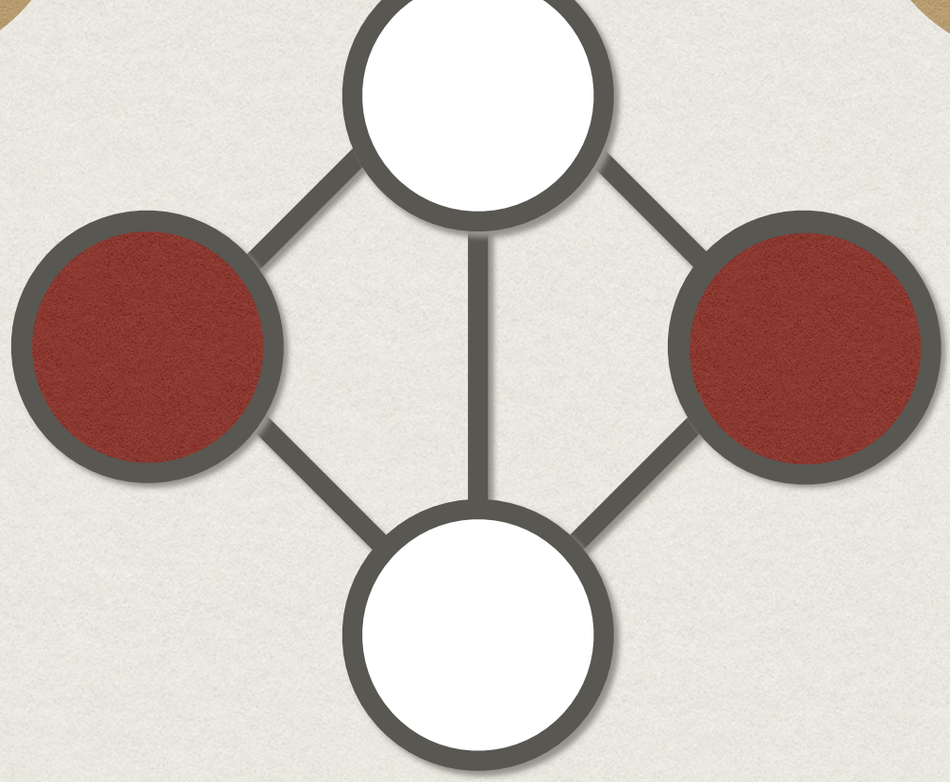

0
0

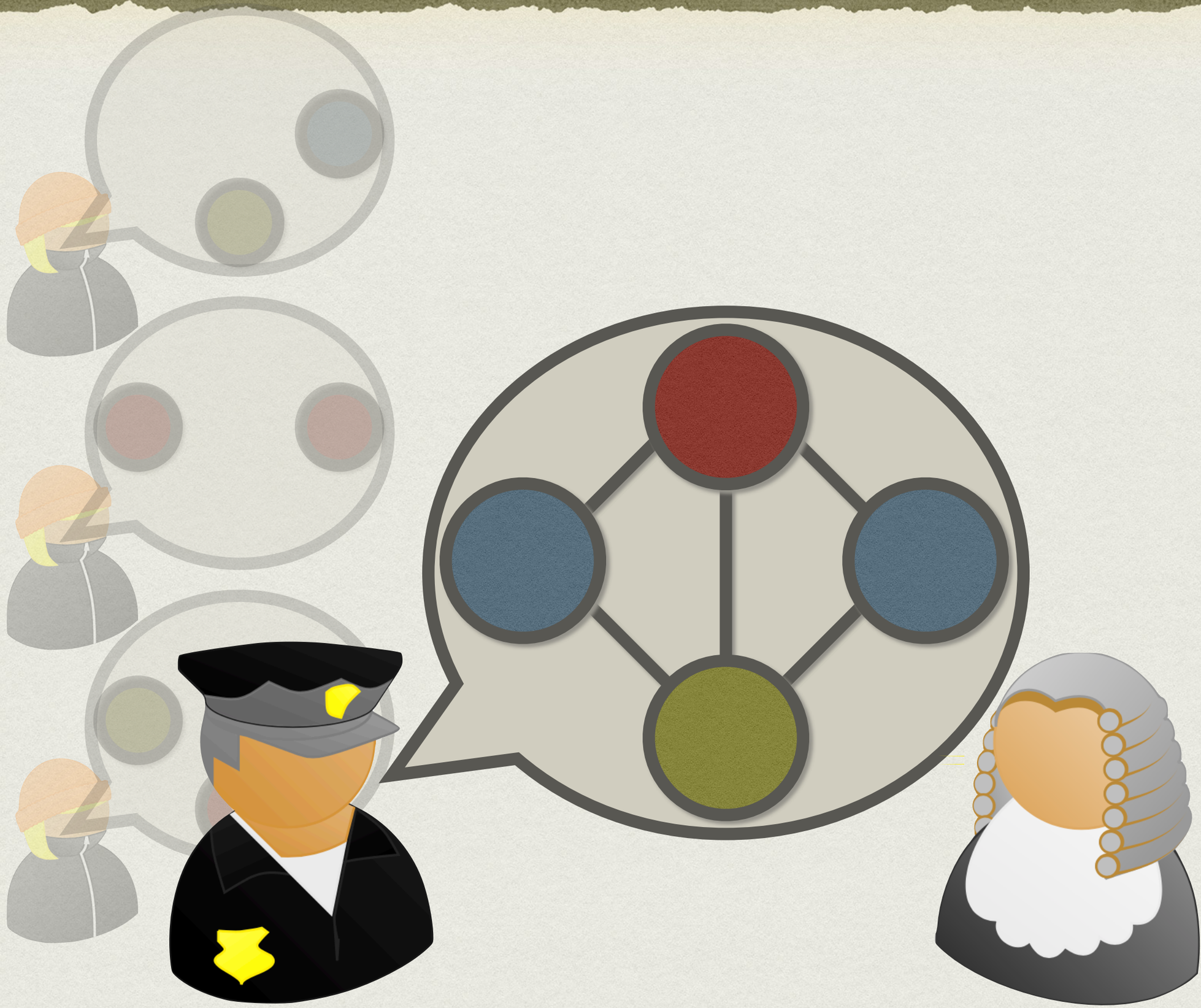


ZK à Vérificateur-honète

1

2

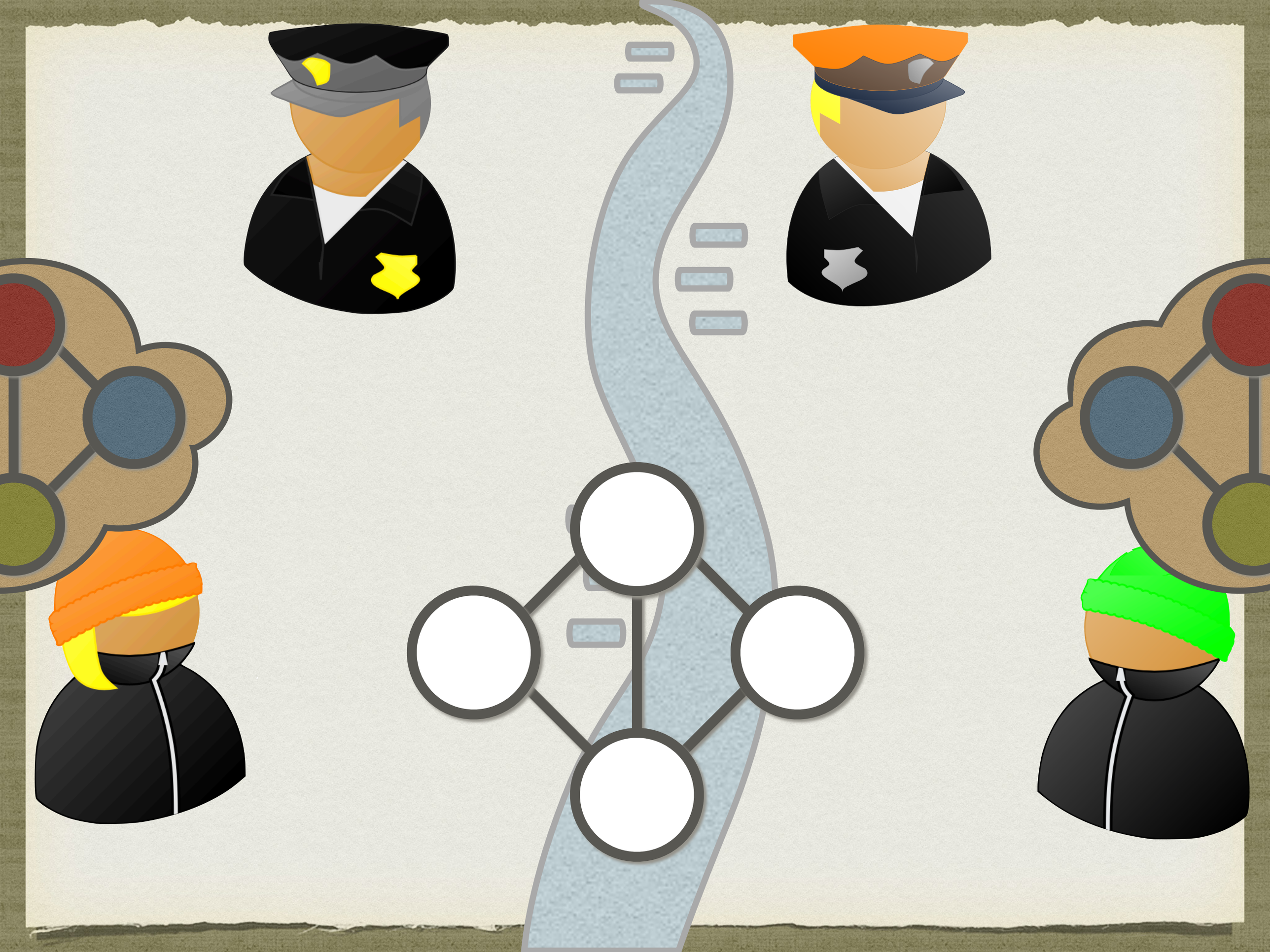




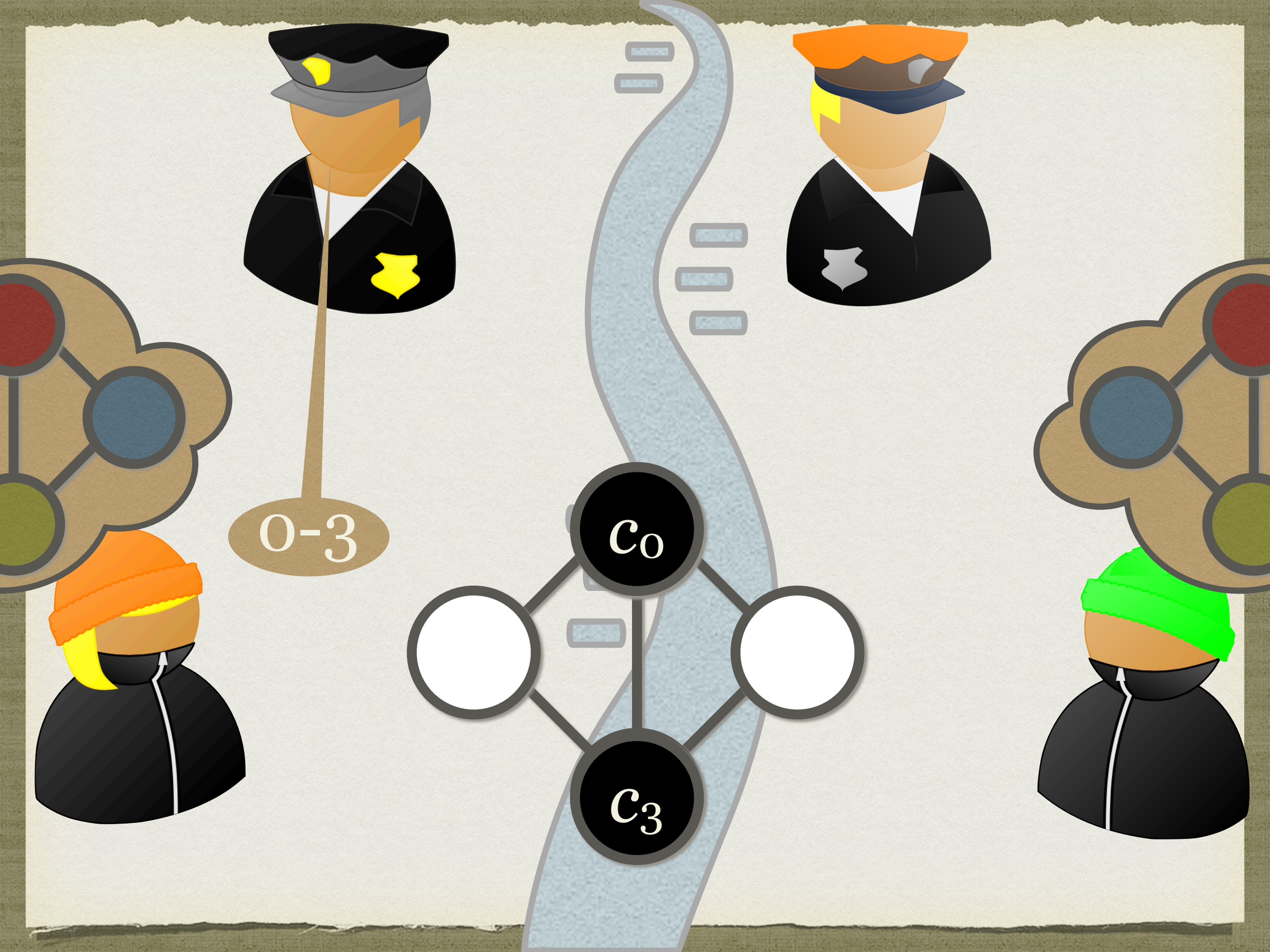
Transférable

IDÉE NOUVELLE

(ZK)MIPs



0-3


0-3
c_0
c_3

c_0

c_3

0-3

c_0

c_3

c_0

c_3

0-3

c_0

c_3

2-3

c_0

c_3

0-3

c_0

c_2'

c_3'

2-3

c_0

c_3

0-3

c_2'

c_3'

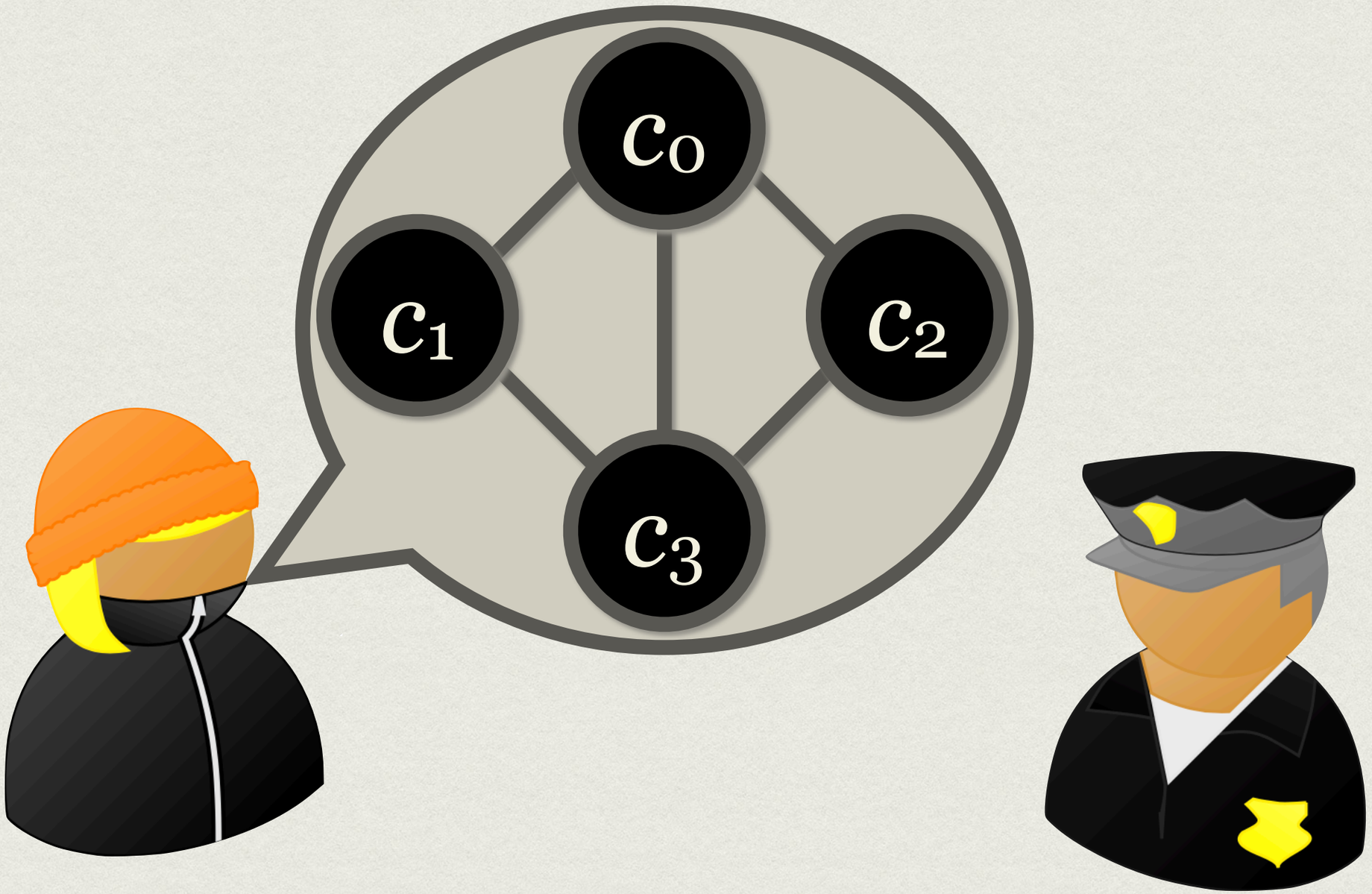
2-3

c_0

c_2'

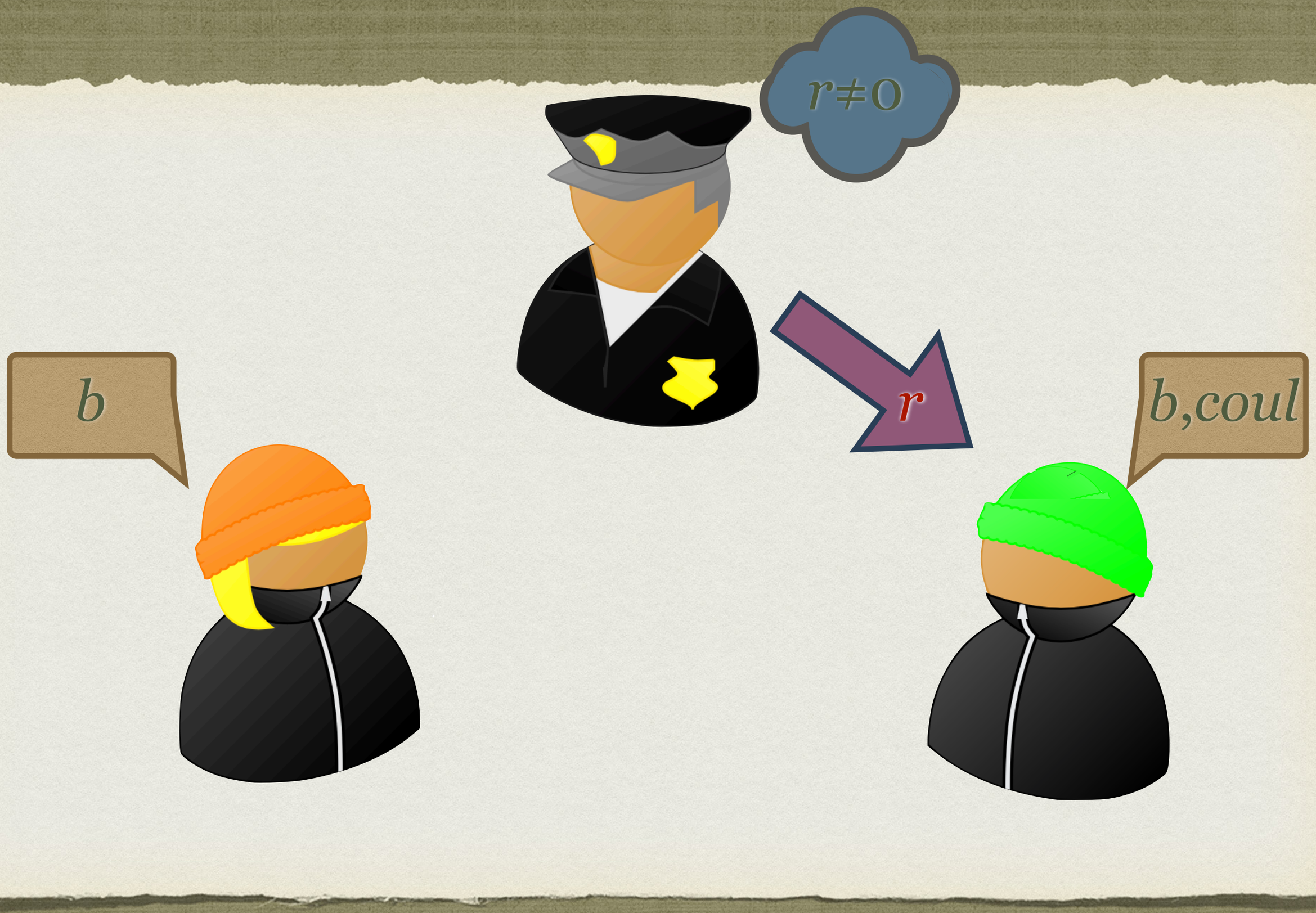
c_3'

MISE-EN-GAGE ??

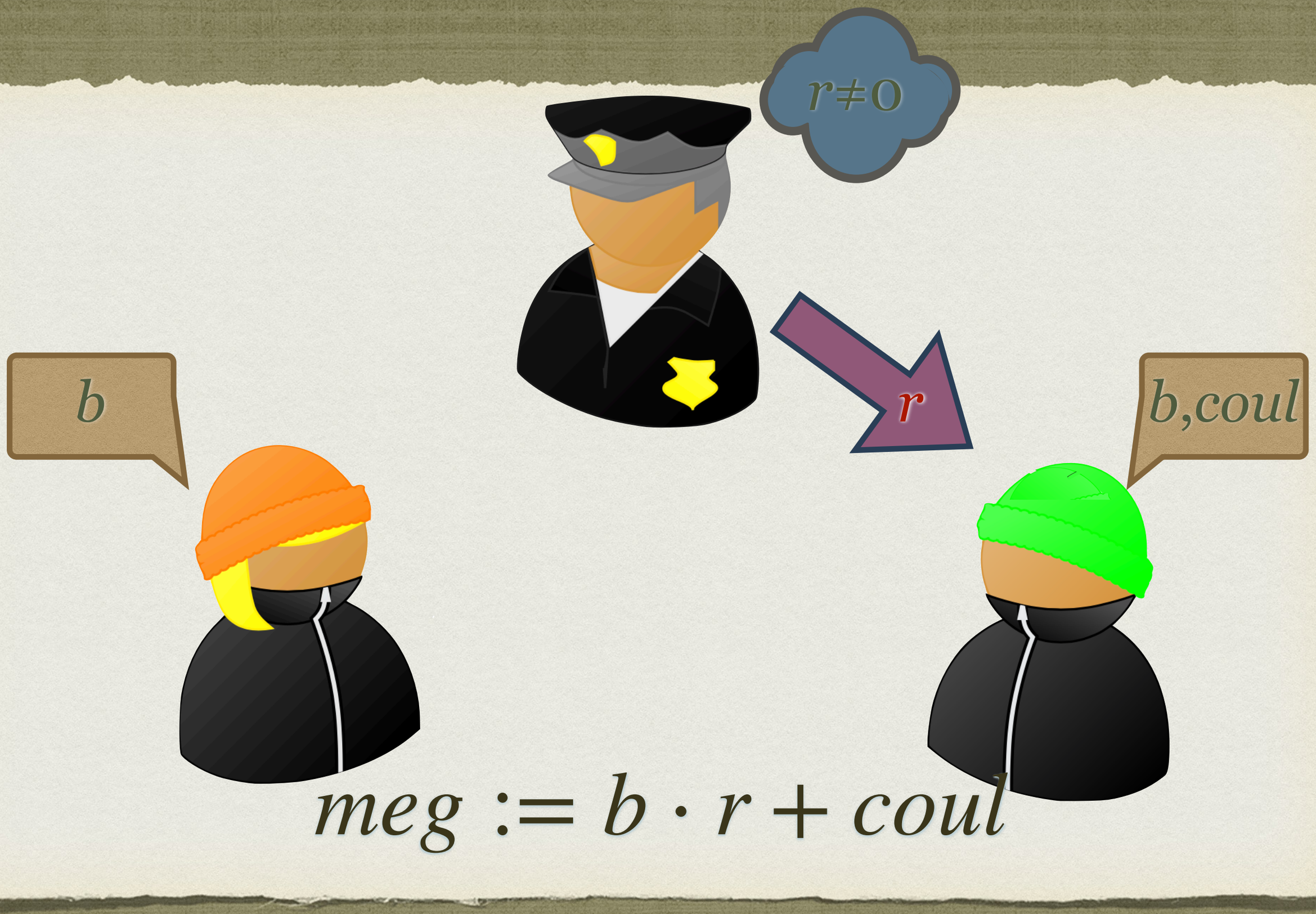


MISE-EN-GAGE

MISE-EN-GAGE

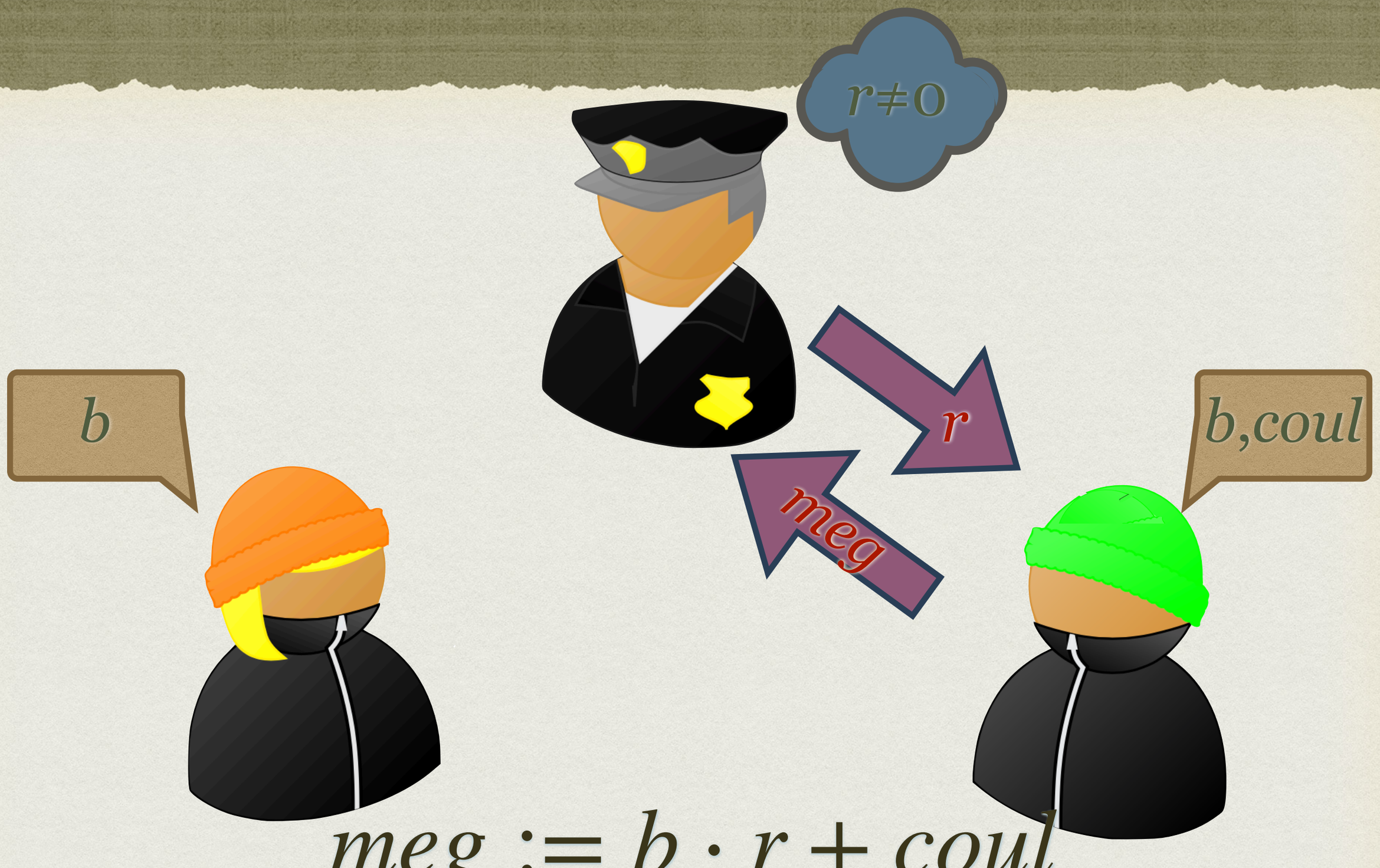


MISE-EN-GAGE



$$meg := b \cdot r + coul$$

MISE-EN-GAGE



$$meg := b \cdot r + coul$$

MISE-EN-GAGE

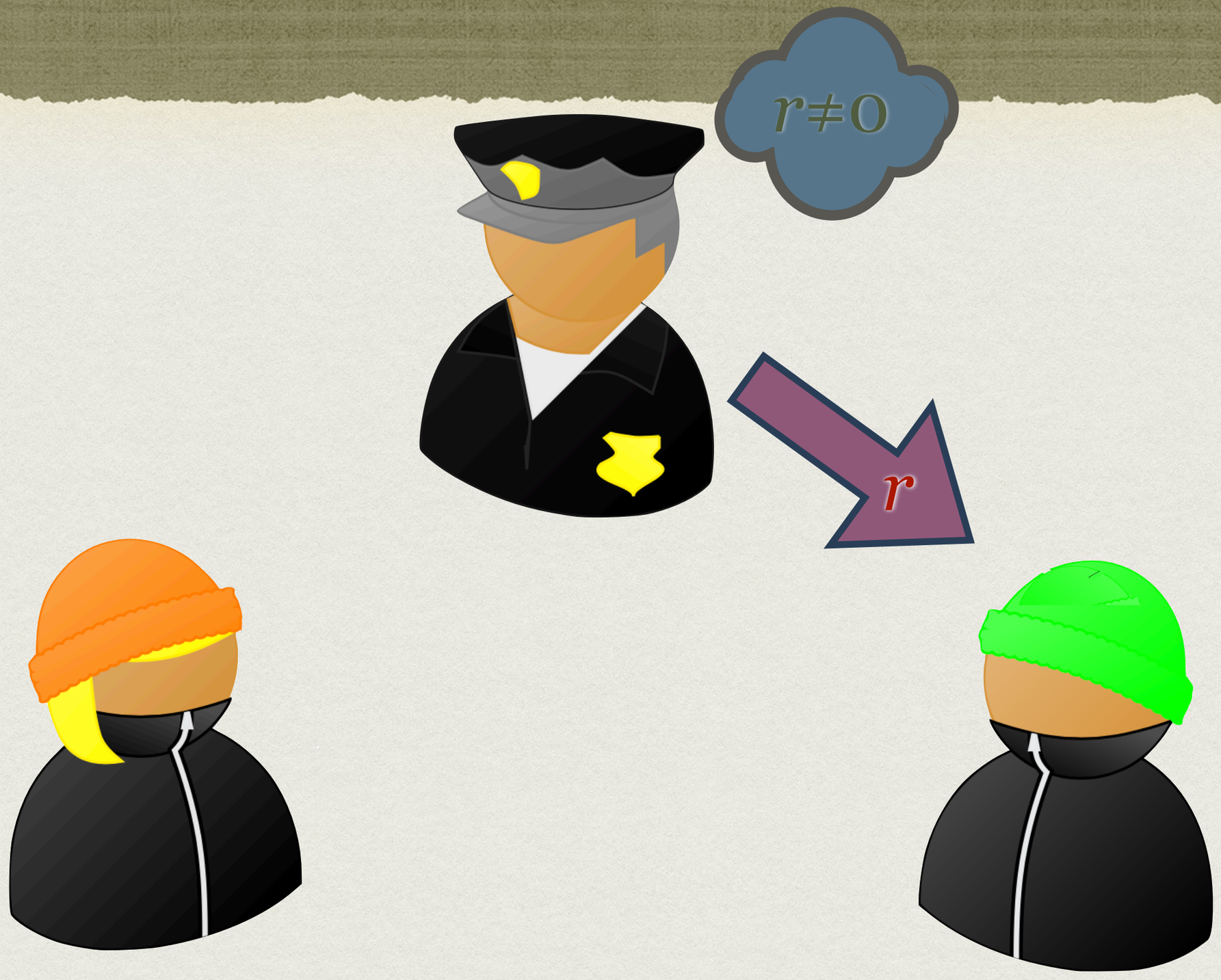
$$meg := b \cdot r + coul$$

MISE-EN-GAGE

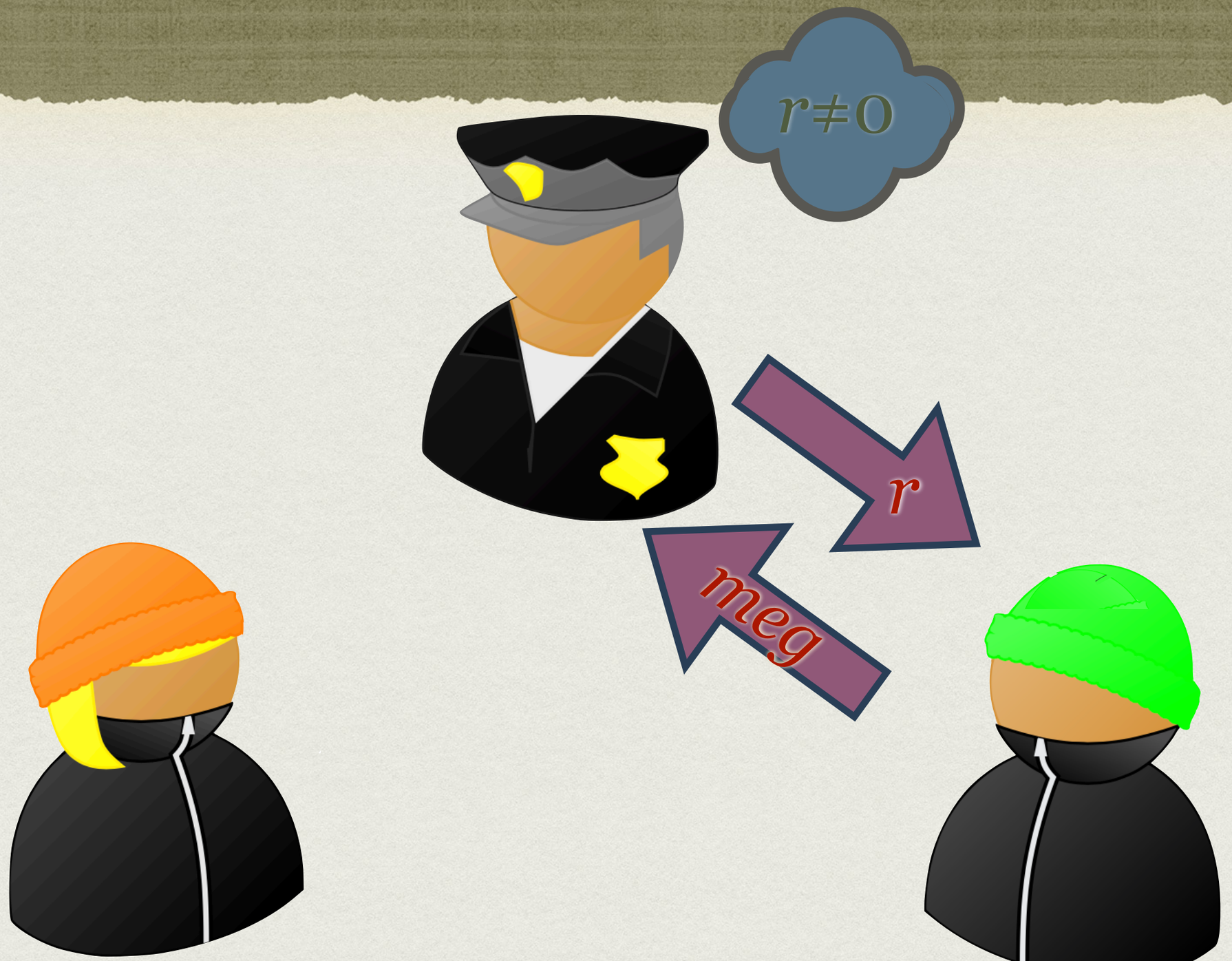
$$meg := b \cdot r + coul$$

MISE-EN-GAGE

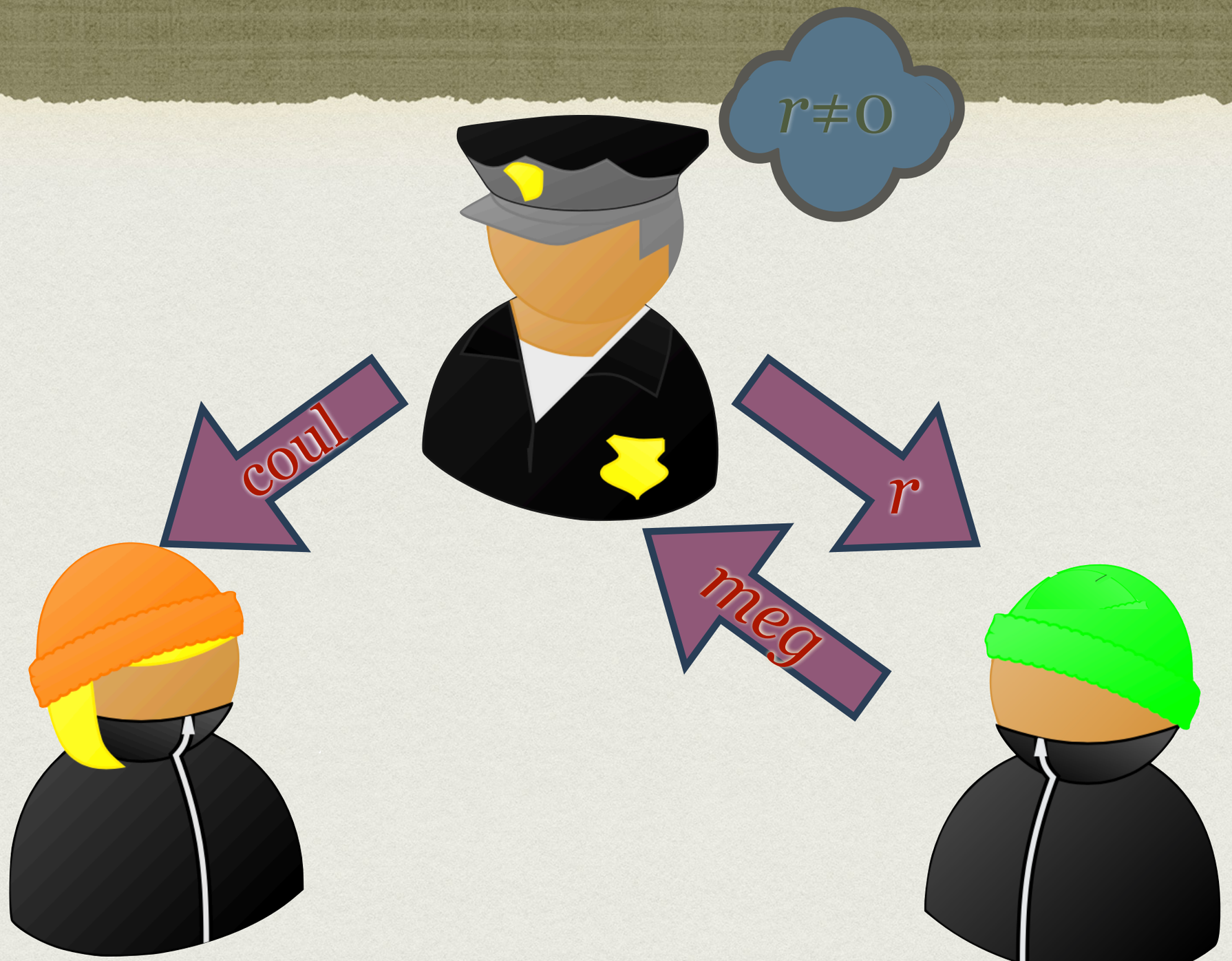
MISE-EN-GAGE



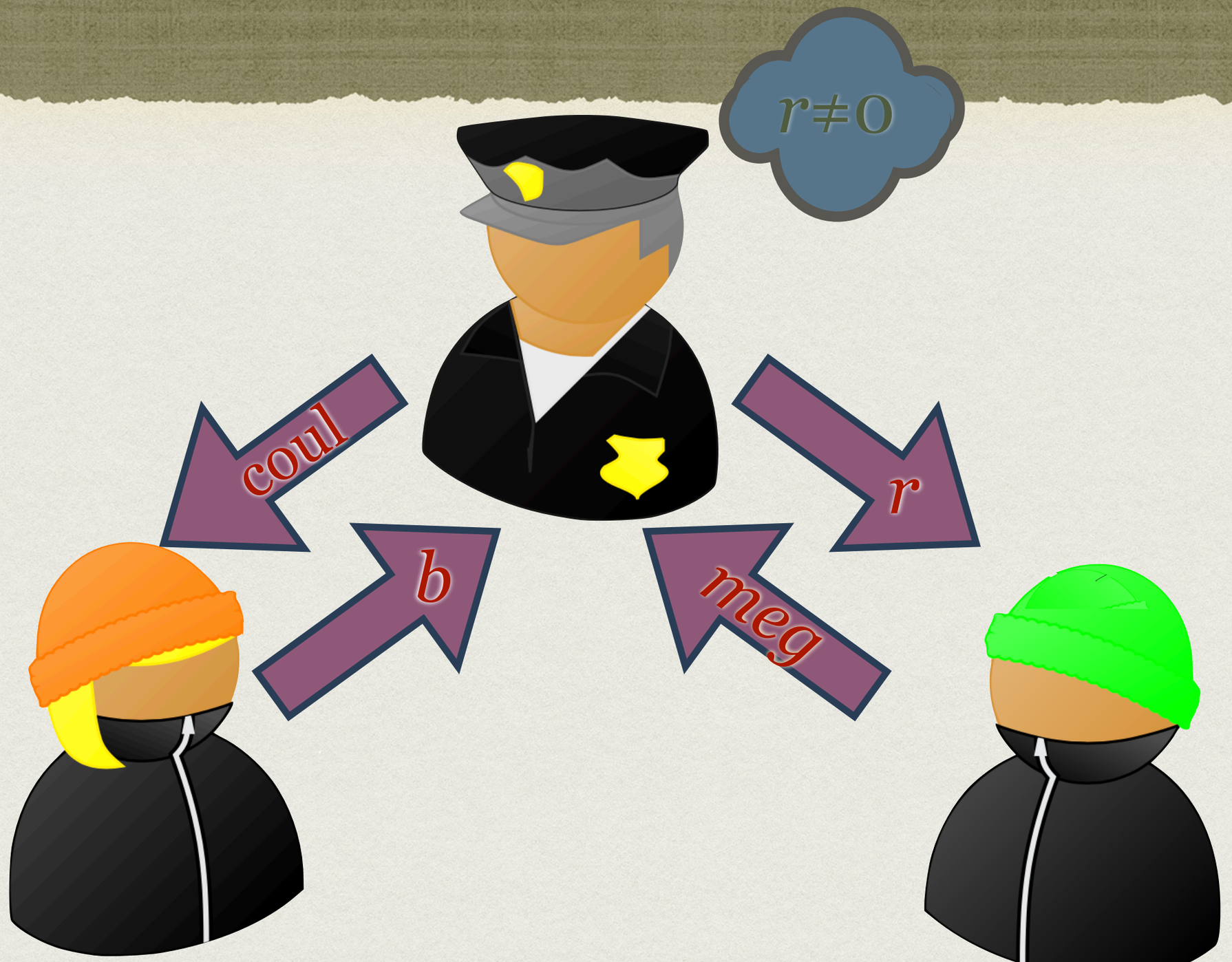
MISE-EN-GAGE



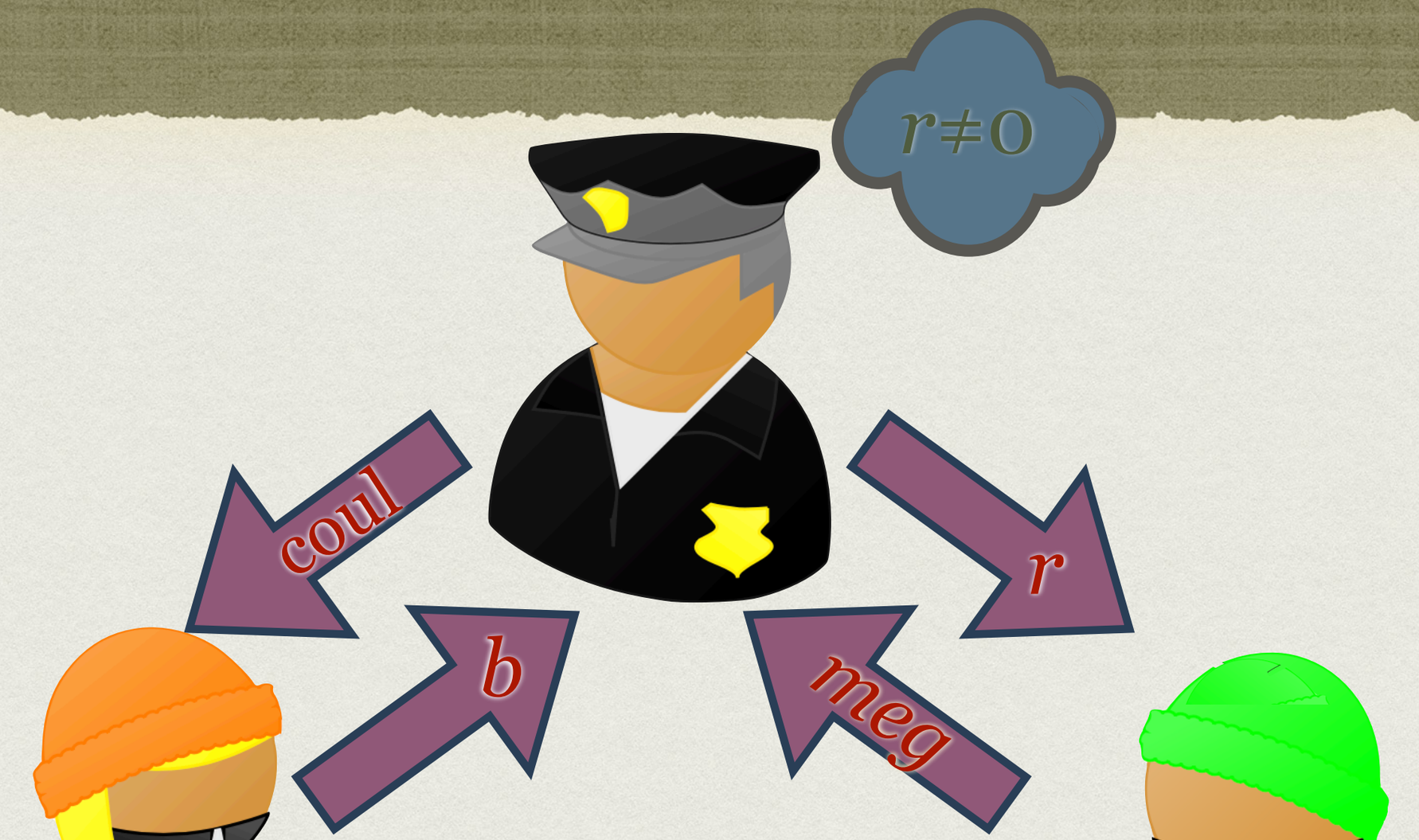
MISE-EN-GAGE



MISE-EN-GAGE



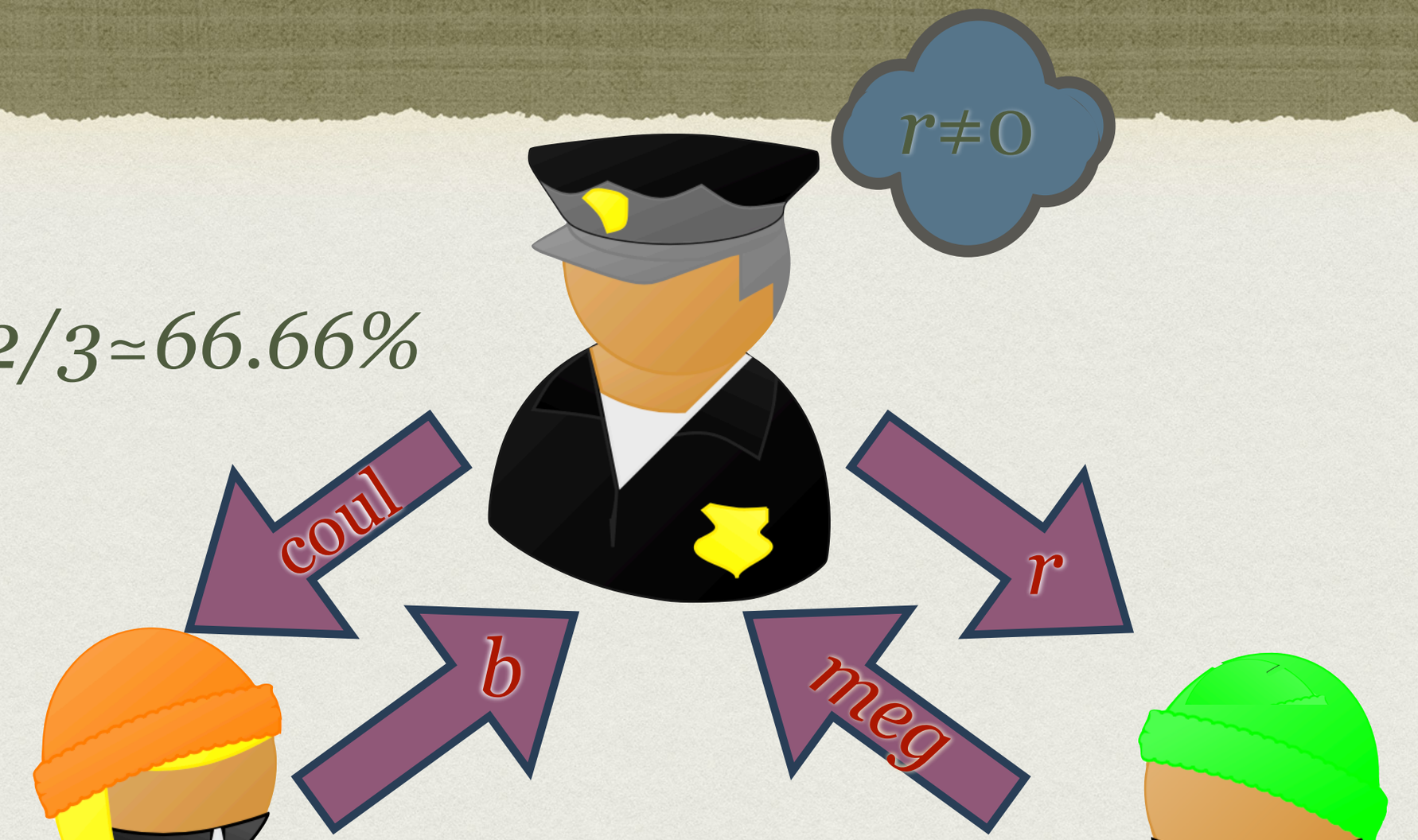
MISE-EN-GAGE



$$b = \frac{meg - coul}{r}$$

MISE-EN-GAGE

LOC=2/3≃66.66%



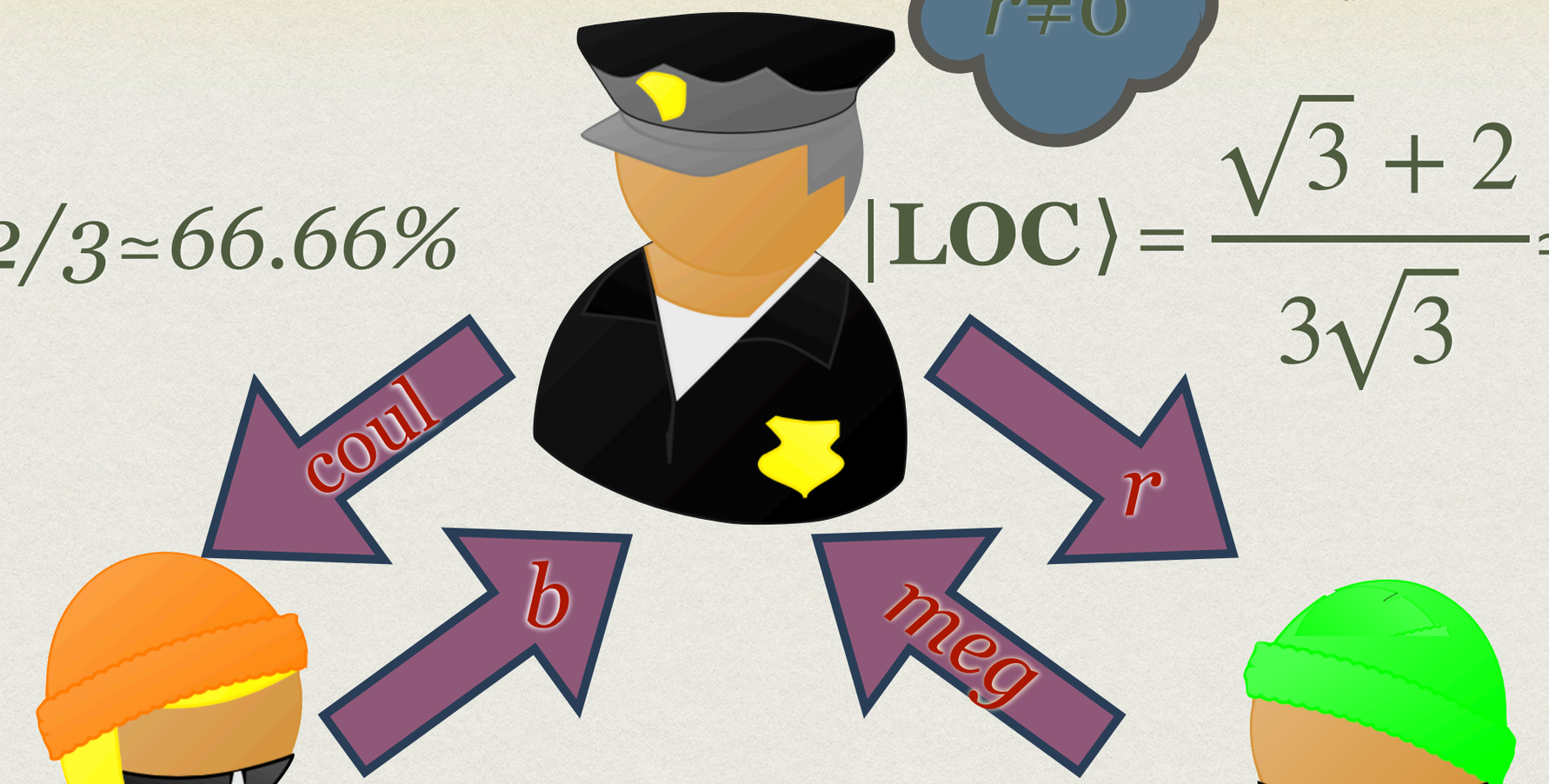
$$b = \frac{meg - coul}{r}$$

MISE-EN-GAGE

$r \neq 0$

LOC$=2/3 \simeq 66.66\%$

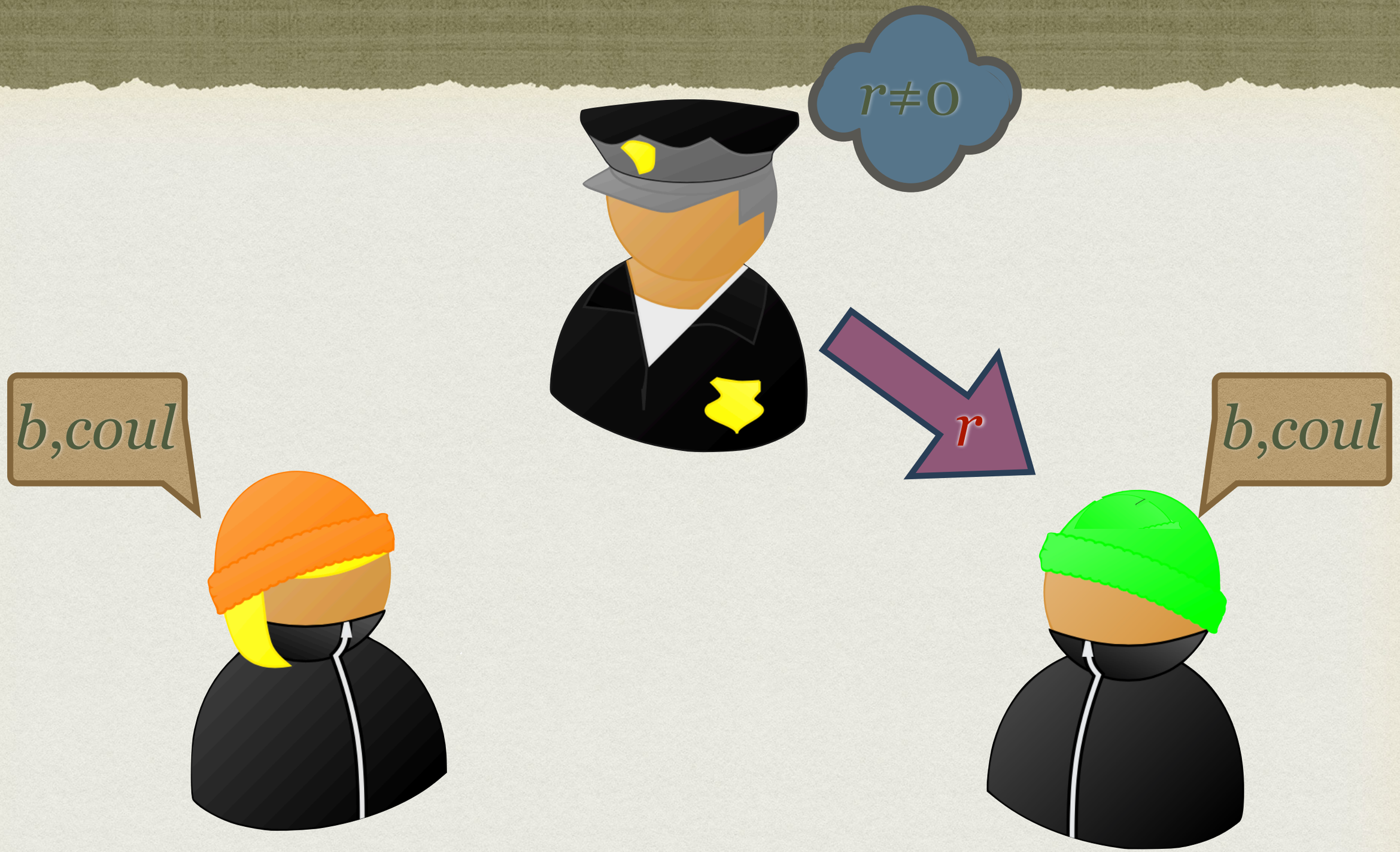
$|\mathbf{LOC}\rangle = \dfrac{\sqrt{3}+2}{3\sqrt{3}} \simeq 71{,}82\%$



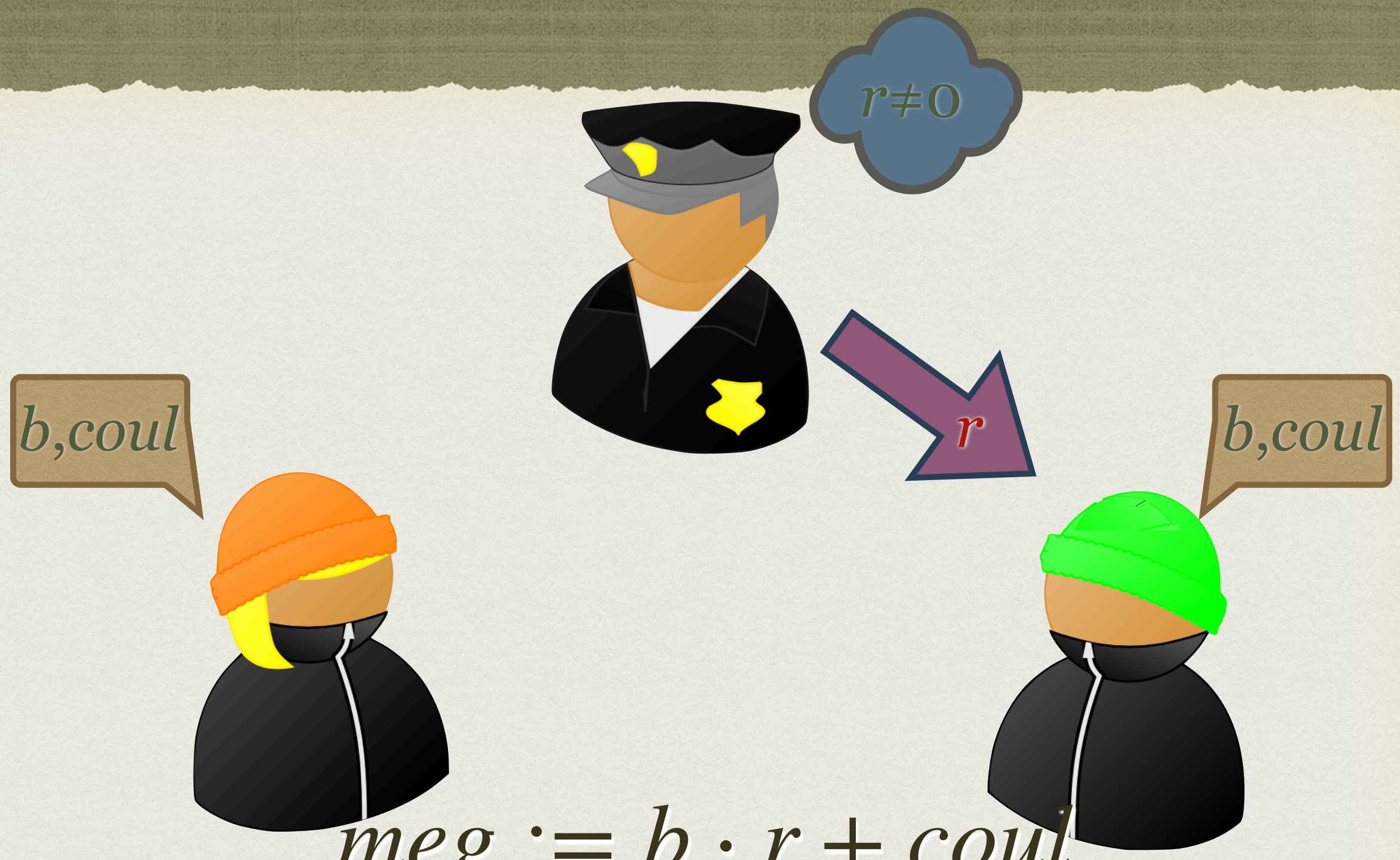
$$b = \frac{meg - coul}{r}$$

MISE-EN-GAGE

MISE-EN-GAGE

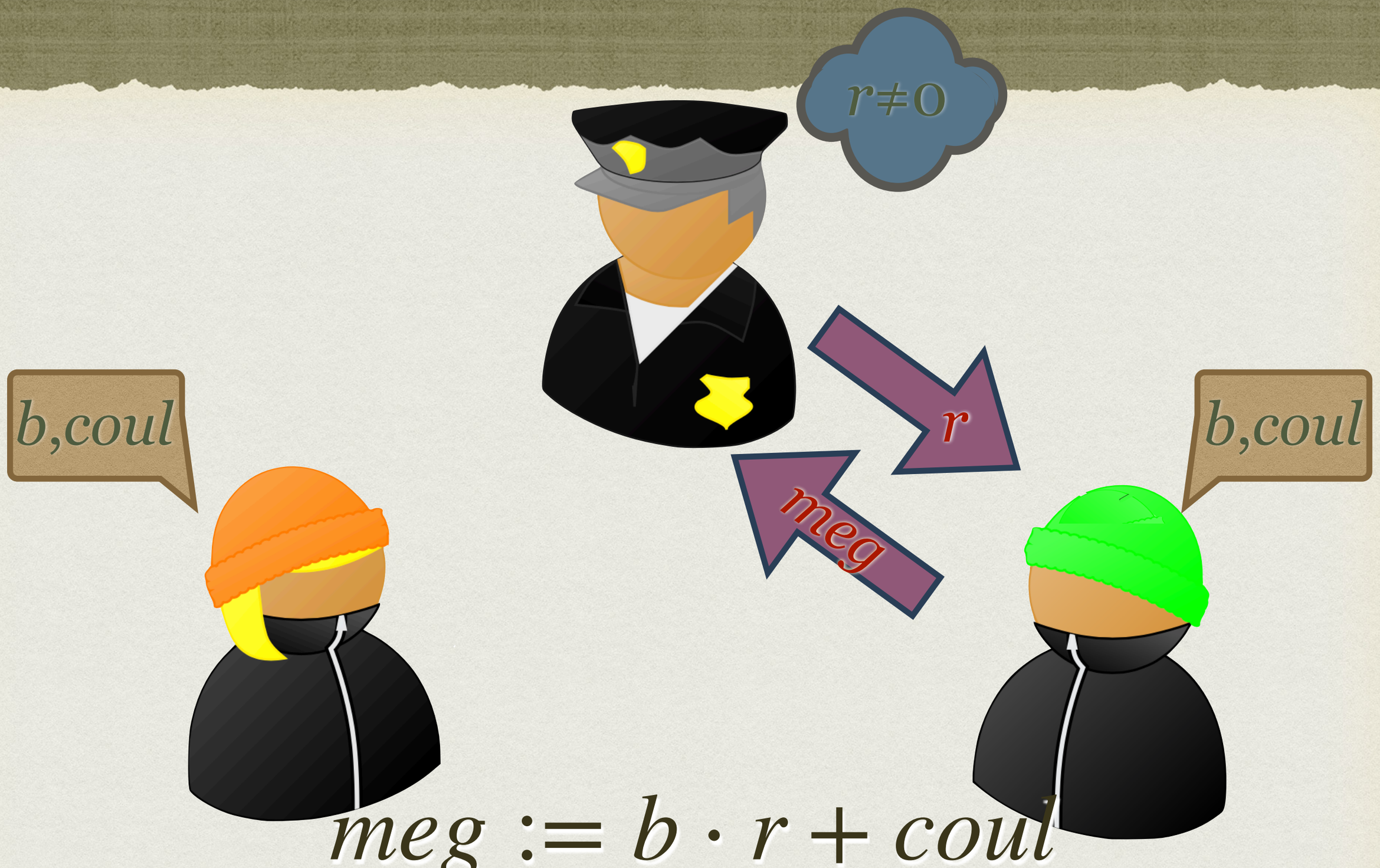


MISE-EN-GAGE



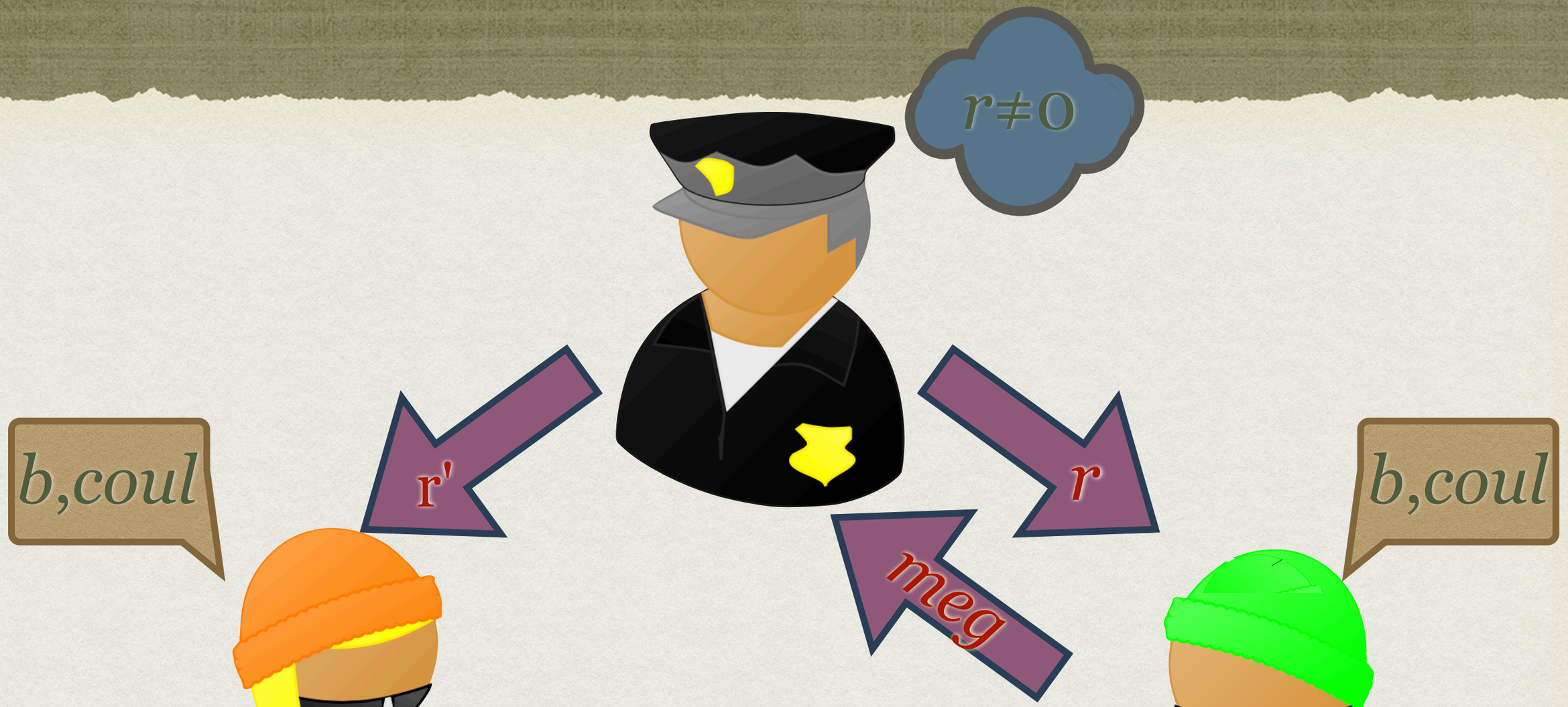
$$meg := b \cdot r + coul$$

MISE-EN-GAGE



$$meg := b \cdot r + coul$$

MISE-EN-GAGE



$$meg := b \cdot r + coul$$

MISE-EN-GAGE

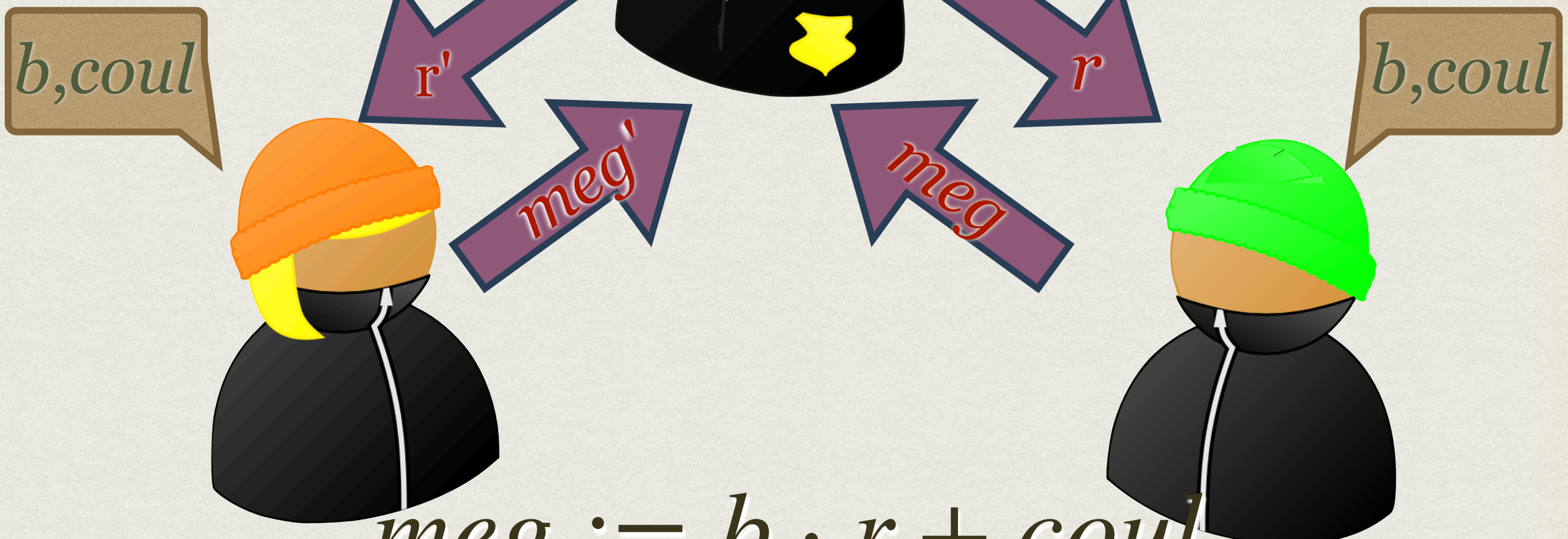
$$meg := b \cdot r + coul$$

MISE-EN-GAGE

$$meg := b \cdot r + coul$$
$$meg' := b \cdot r' + coul$$

MISE-EN-GAGE

$$coul = \frac{meg \cdot r' - meg' \cdot r}{r' - r}$$



$$meg := b \cdot r + coul$$
$$meg' := b \cdot r' + coul$$

MISE-EN-GAGE

PRINCIPE DE DÉVOILEMENT VIA M-E-G

MISE-EN-GAGE

PRINCIPE DE DÉVOILEMENT VIA M-E-G

=

DOUBLE-SPENDING DETECTION MECHANISM

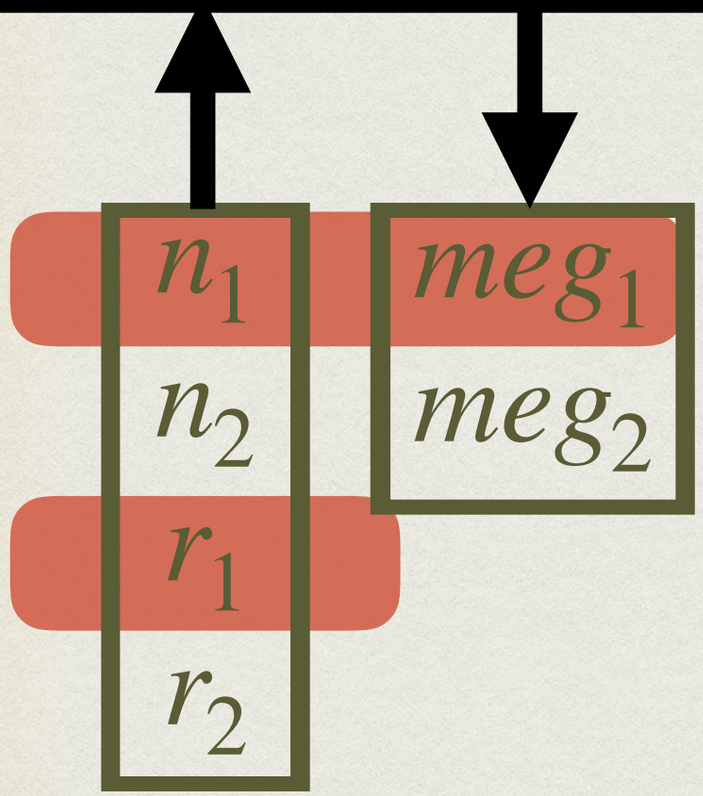
$$meg_i = coul_{n_i} + b_{n_i} r_i$$
$$meg_j = coul_{n_j} + b_{n_j} r_j$$

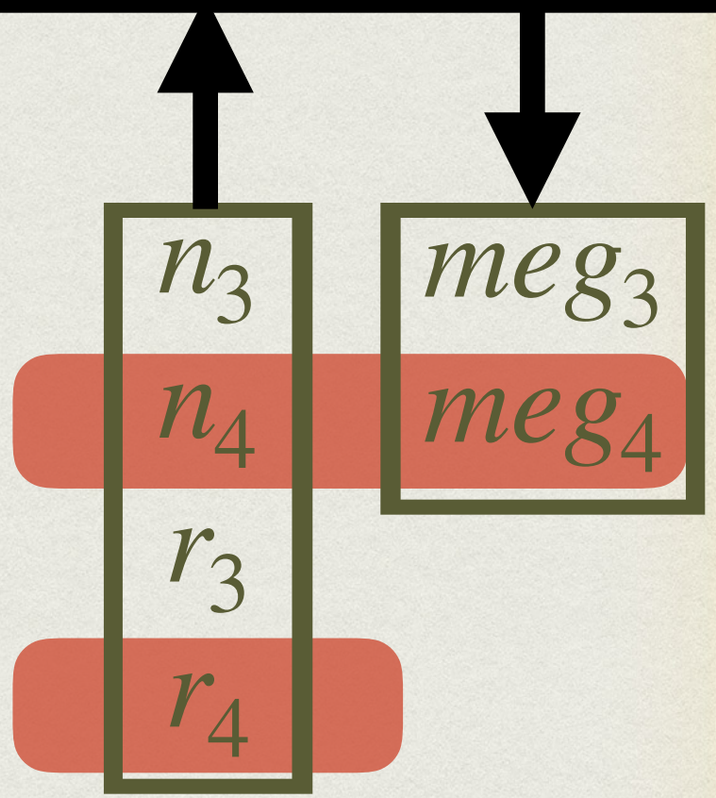
P_1

$(n_1, n_2) \in E$

P_2

$(n_3, n_4) \in E$





$$meg_i = coul_{n_i} + b_{n_i} r_i$$
$$meg_j = coul_{n_j} + b_{n_j} r_j$$

P_1

$(n_1, n_2) \in E$

Demander à deux prouveurs le même noeud avec même r vérifie la consistence.

P_2

$(n_3, n_4) \in E$

n_1	meg_1
n_2	meg_2
r_1	
r_2	

n_3	meg_3
n_4	meg_4
r_3	
r_4	

$$meg_i = coul_{n_i} + b_{n_i} r_i$$
$$meg_j = coul_{n_j} + b_{n_j} r_j$$

P_1

$(n_1, n_2) \in E$

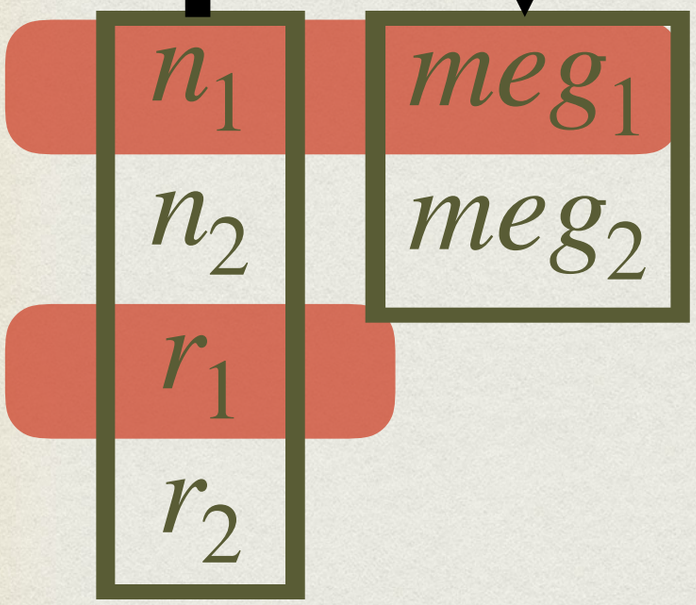
Demander à deux prouveurs le même noeud avec même r vérifie la consistence.

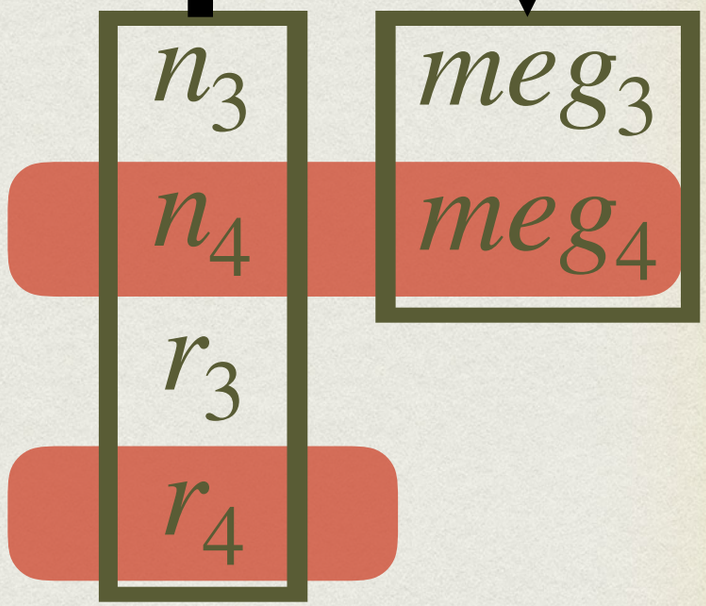
Asking two provers the same node with same r checks their consistency.

$$n_i = n_j \wedge r_i = r_j$$
$$\Longrightarrow meg_i = meg_j$$

P_2

$(n_3, n_4) \in E$





$$meg_i = coul_{n_i} + b_{n_i} r_i$$
$$meg_j = coul_{n_j} + b_{n_j} r_j$$

P_1

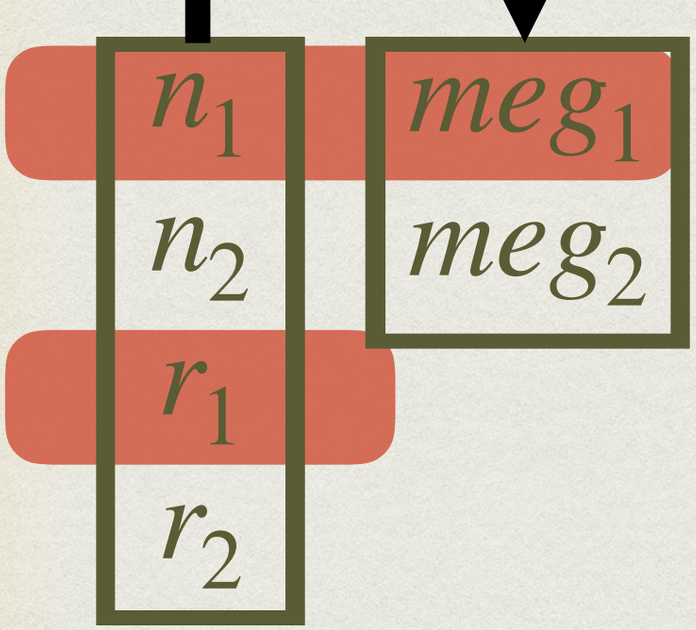
$(n_1, n_2) \in E$

Demander à deux prouveurs le même noeud avec même r vérifie la consistence.

Asking two provers the same node with same r checks their consistency.

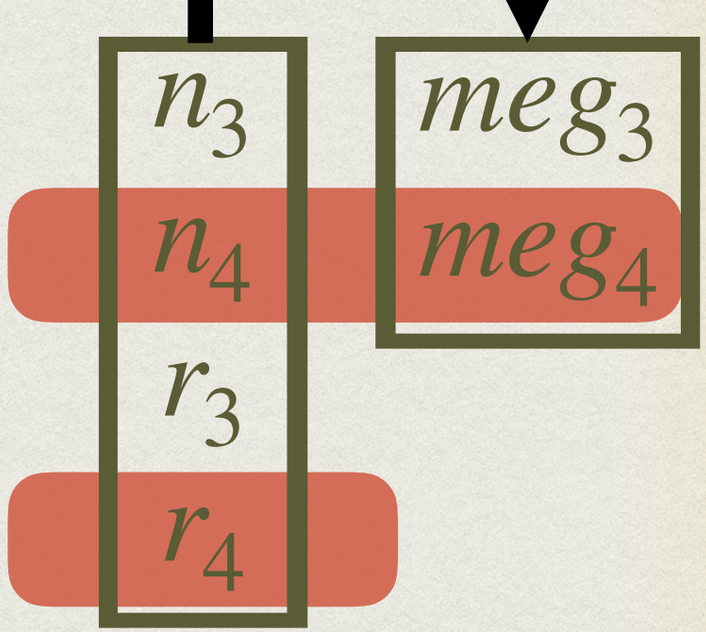
$$n_i = n_j \wedge r_i = r_j$$
$$\Longrightarrow meg_i = meg_j$$

Demander à deux prouveurs le même noeud avec deux r's donne la couleur.



P_2

$(n_3, n_4) \in E$



$$meg_i = coul_{n_i} + b_{n_i} r_i$$
$$meg_j = coul_{n_j} + b_{n_j} r_j$$

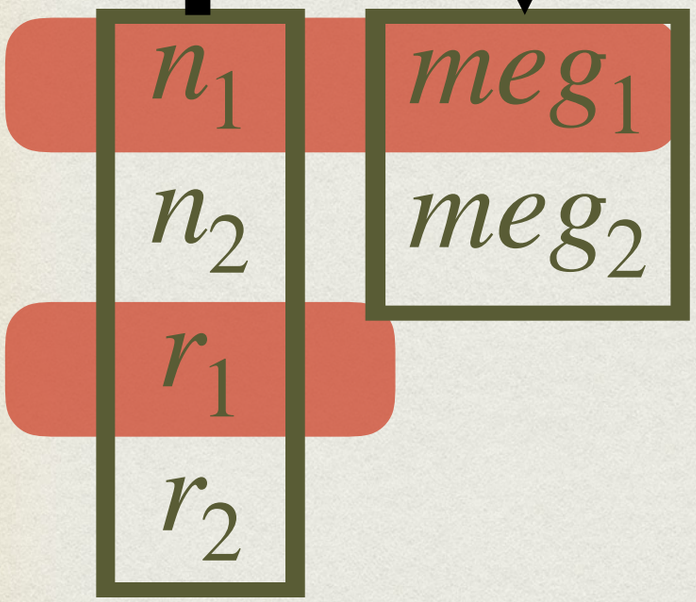
P_1

$(n_1, n_2) \in E$

Demander à deux prouveurs le même noeud avec même r vérifie la consistence.

Asking two provers the same node with same r checks their consistency.

$$n_i = n_j \wedge r_i = r_j \implies meg_i = meg_j$$



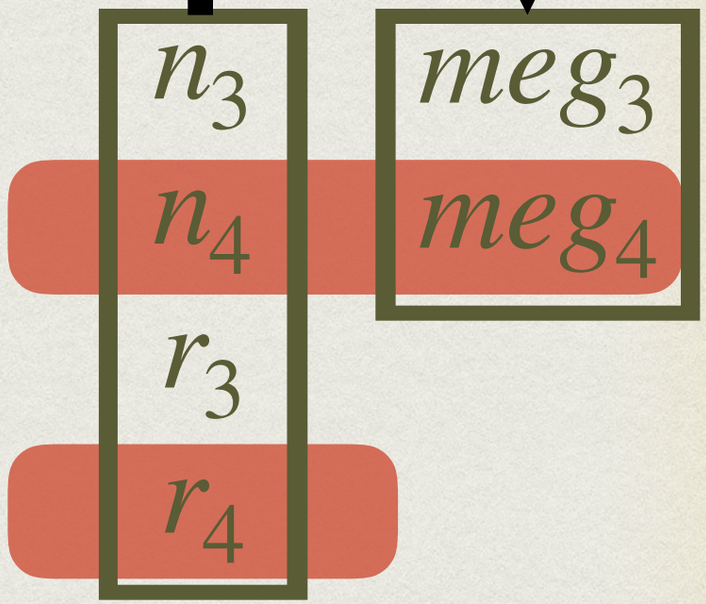
Demander à deux prouveurs le même noeud avec deux r's donne la couleur.

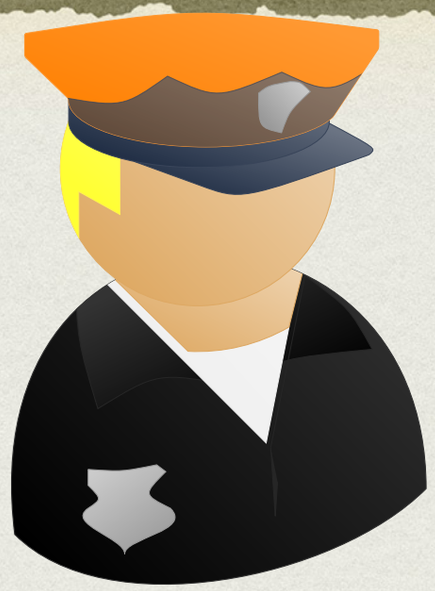
Asking two provers the same node with distinct r's unveils that node colour.

$$n_i = n_j \wedge r_i \neq r_j \implies coul_{n_i} = meg_j + meg_i$$

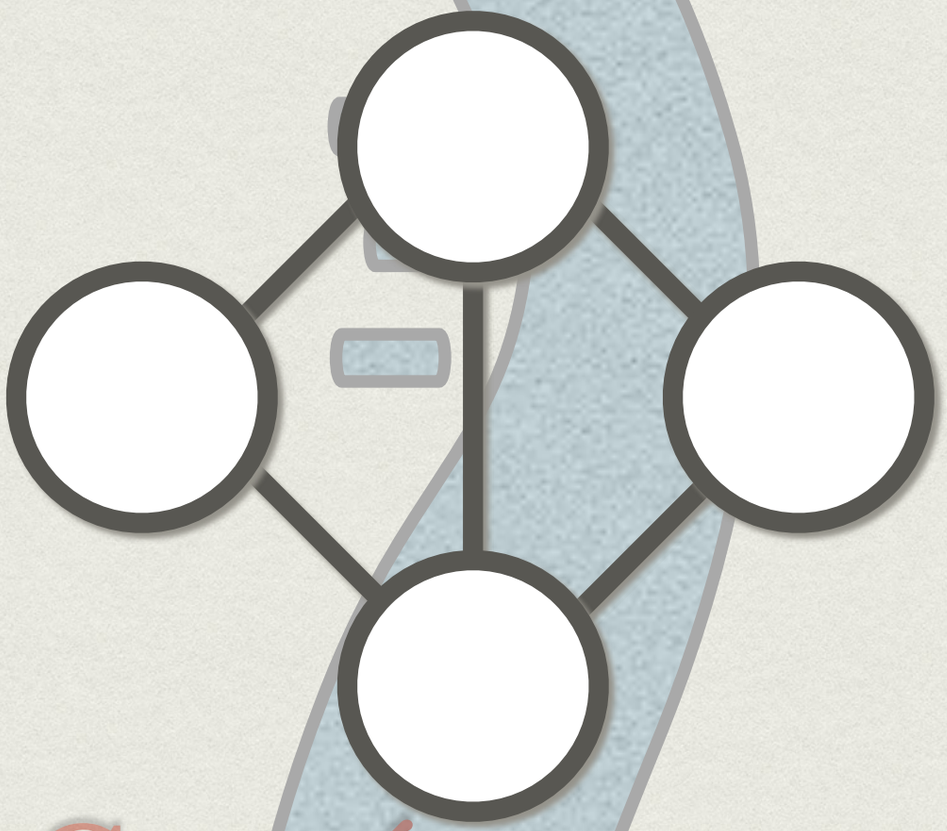
P_2

$(n_3, n_4) \in E$

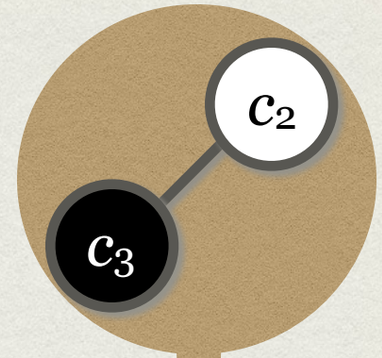


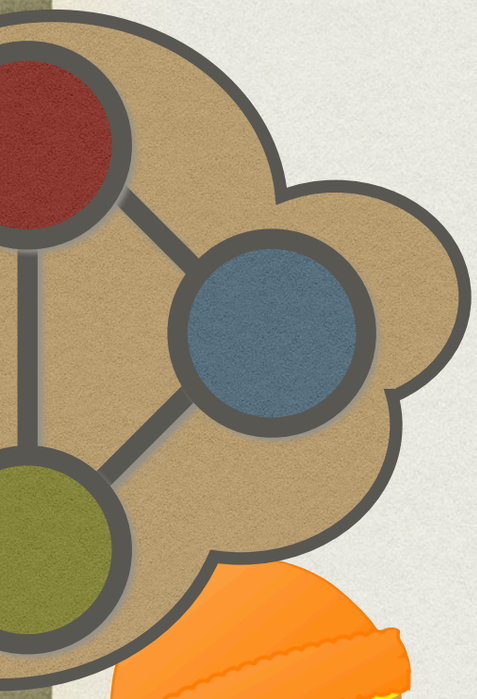


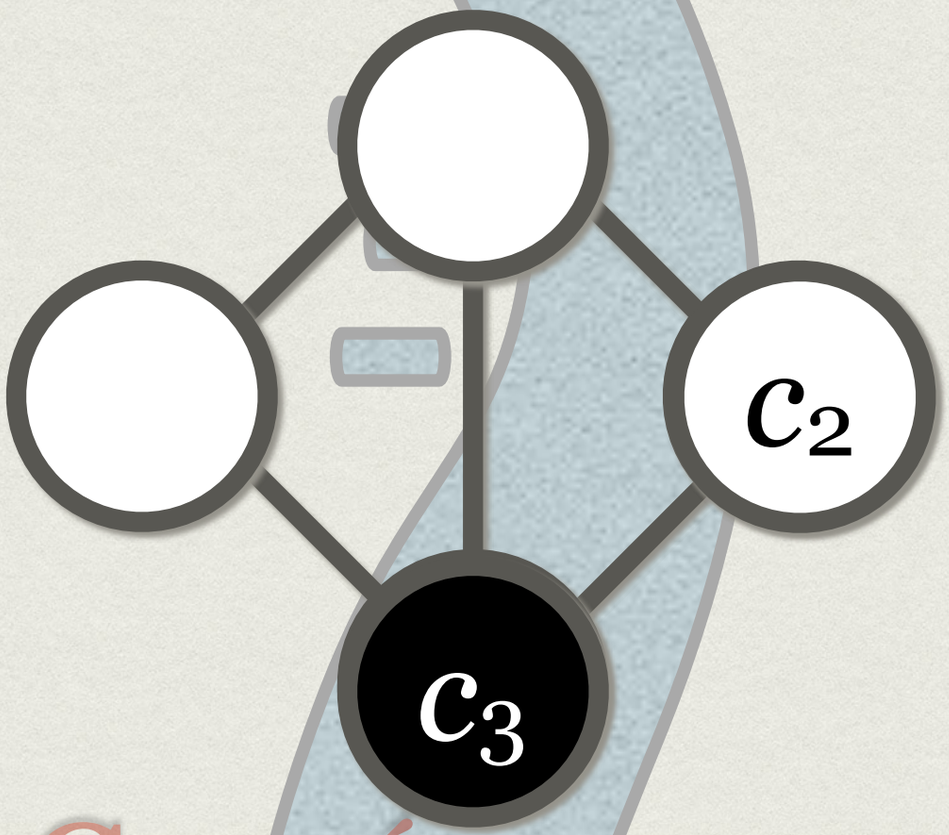
Complétude



Cohérence







Complétude

Cohérence

c_0

c_3

0-3

c_2

c_3

2-3

Complétude

c_0

c_2

c_3

Cohérence

c_0

c_3

0-3

c_2

c_3

2-3

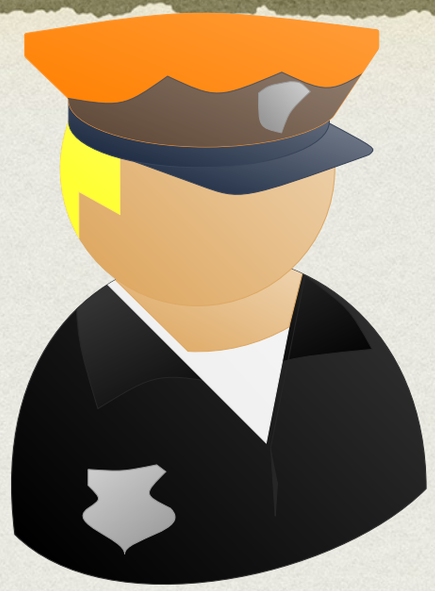
c_0

c_2

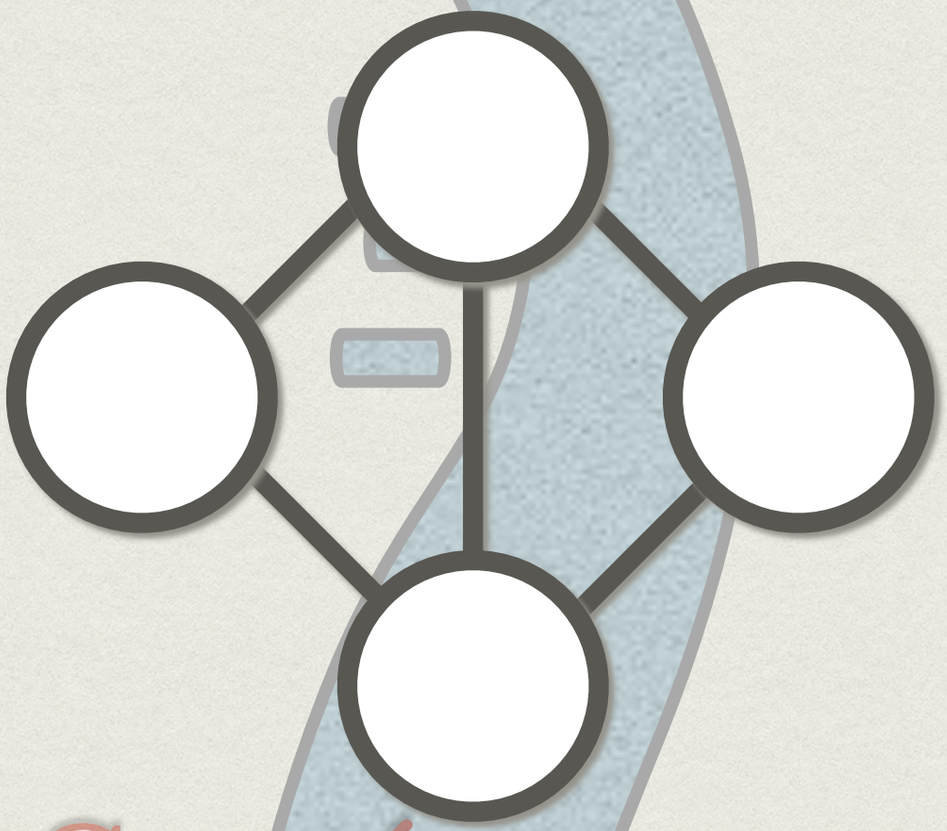
c_3

COMPLÉTUDE

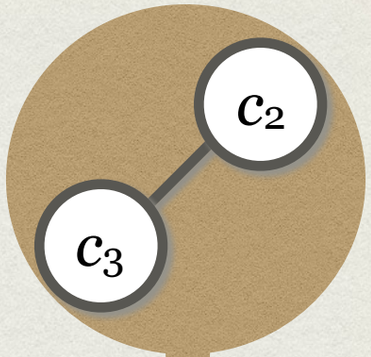
COHÉRENCE

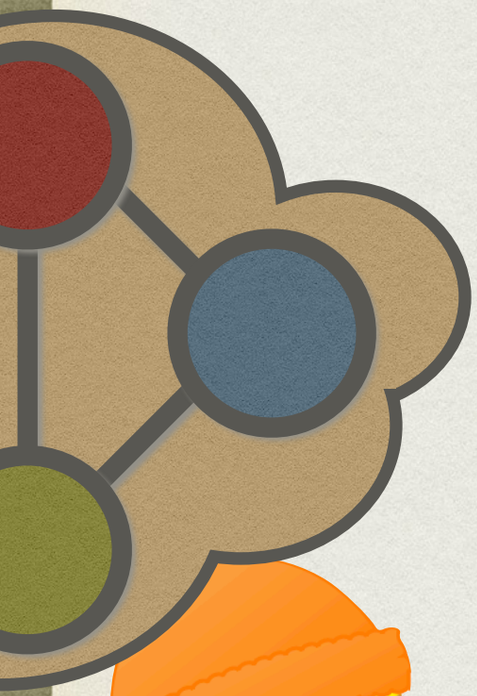


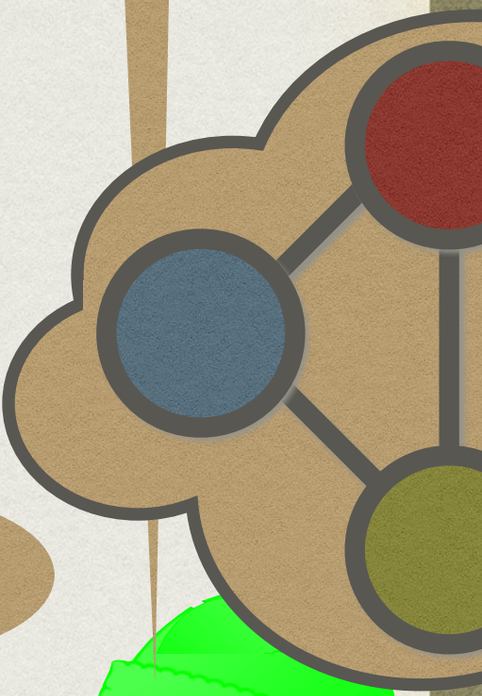
Complétude

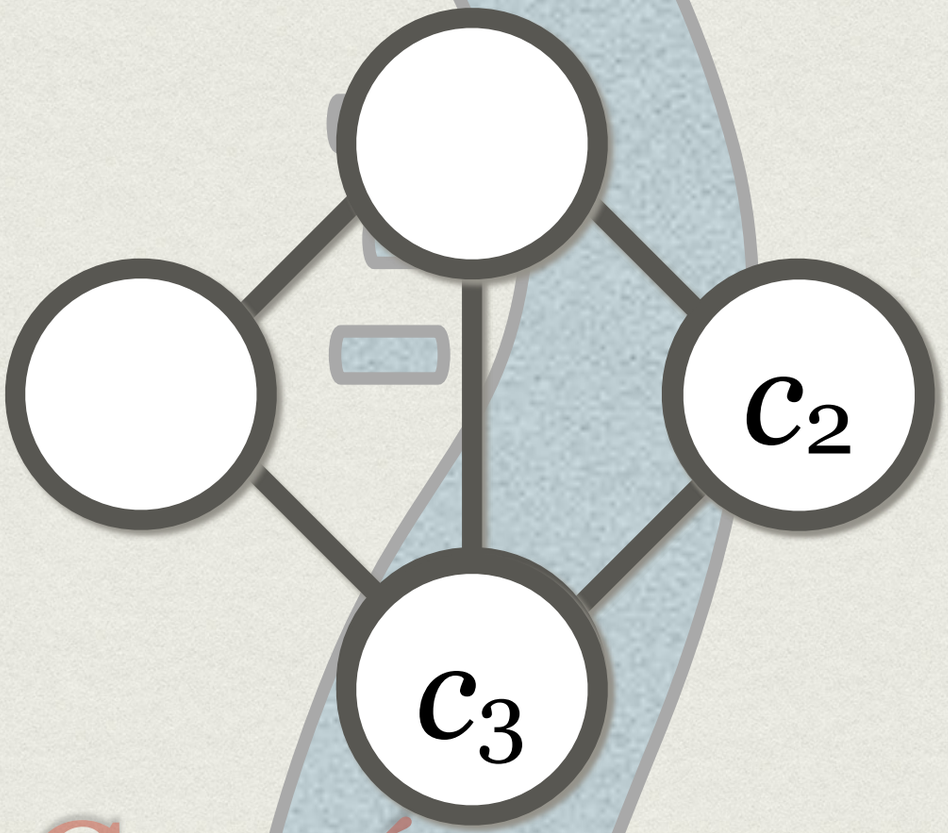


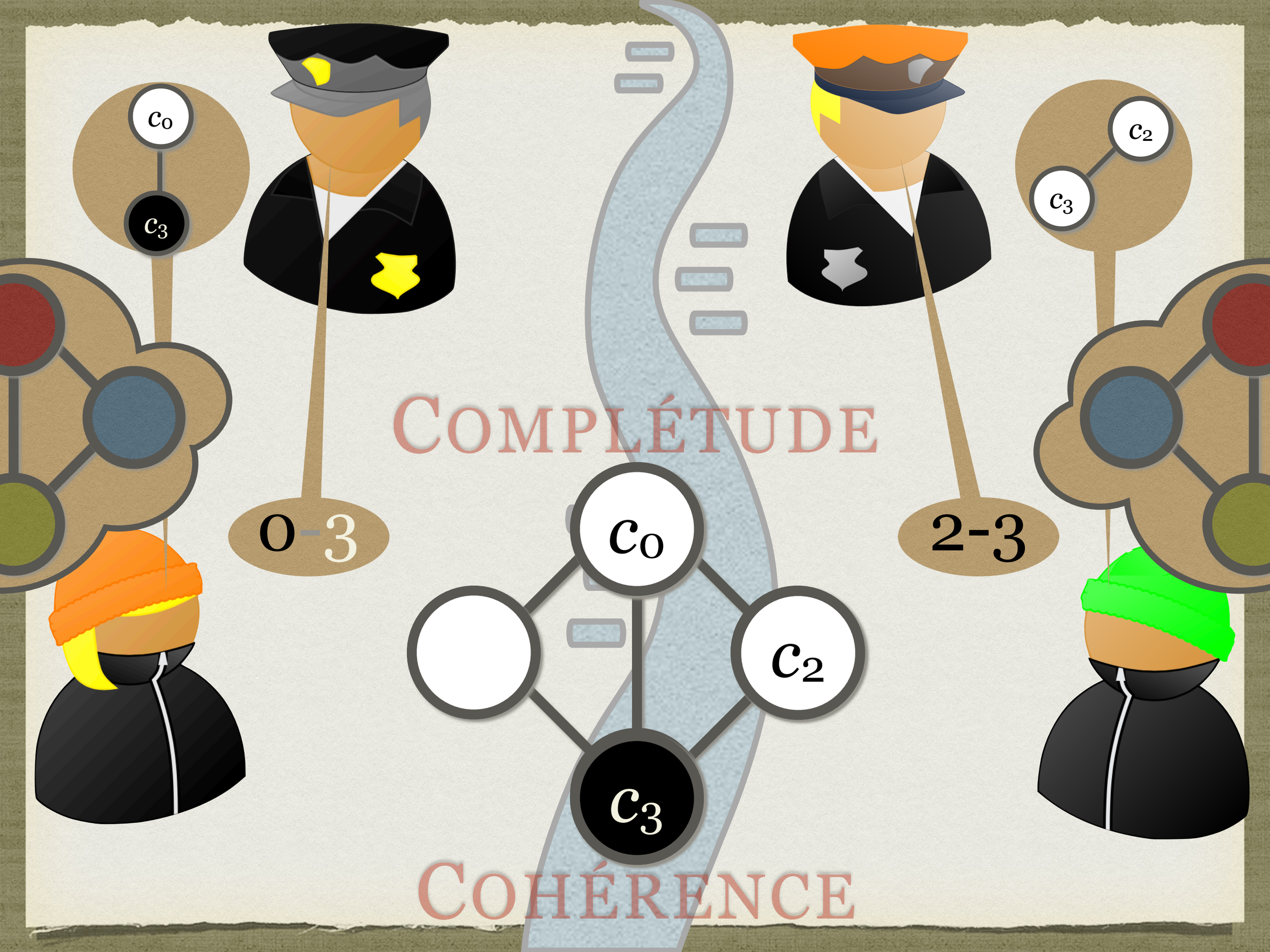
Cohérence

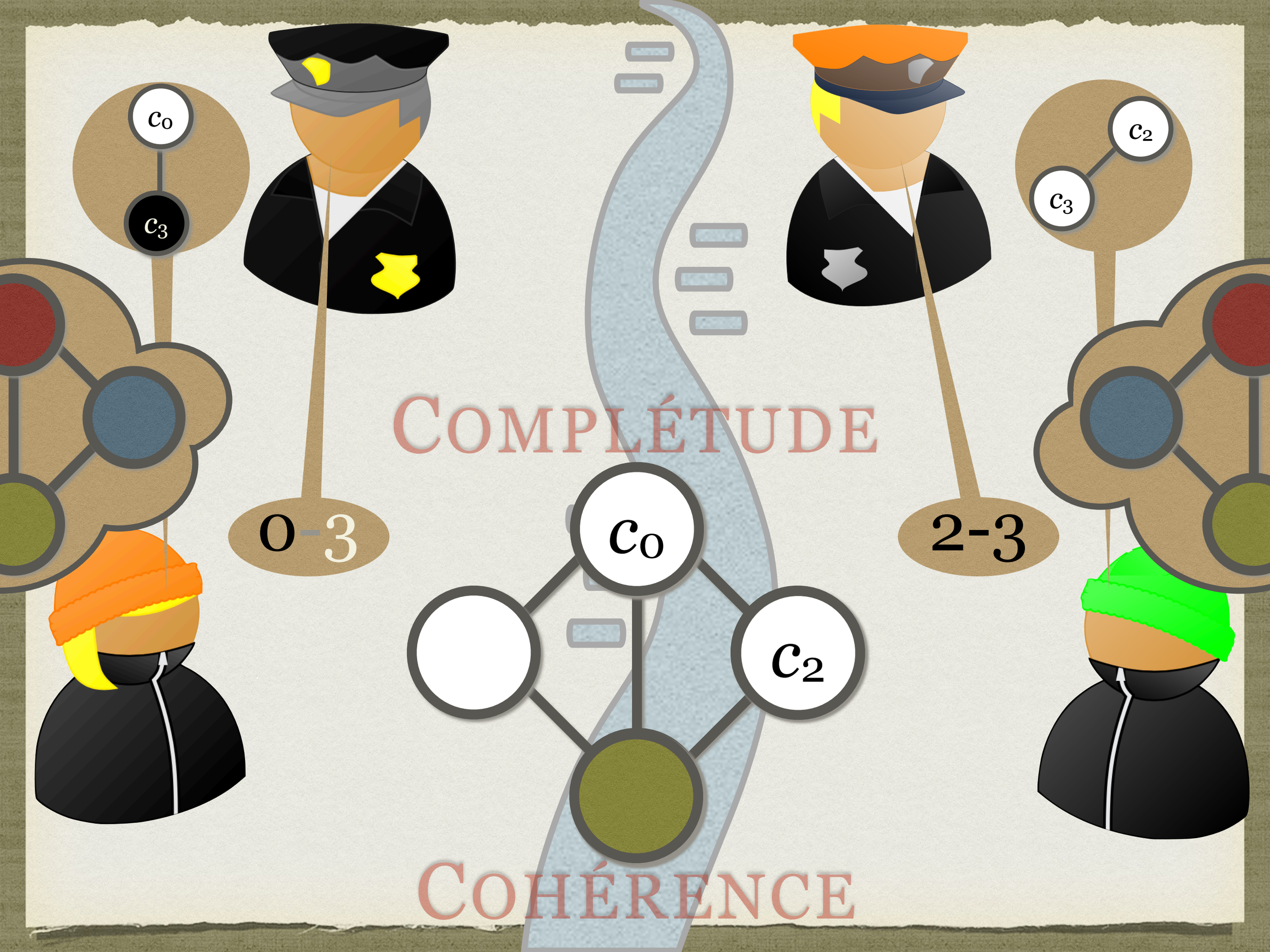


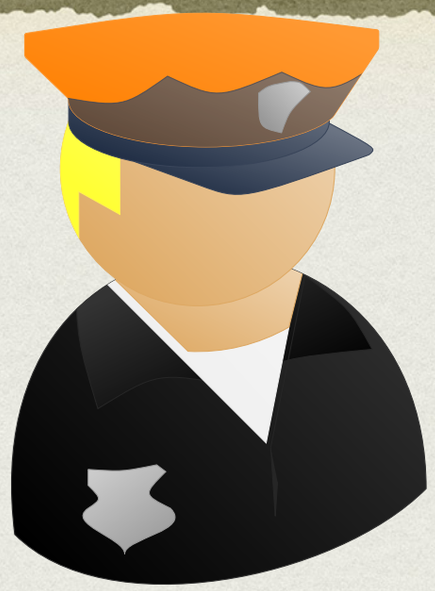




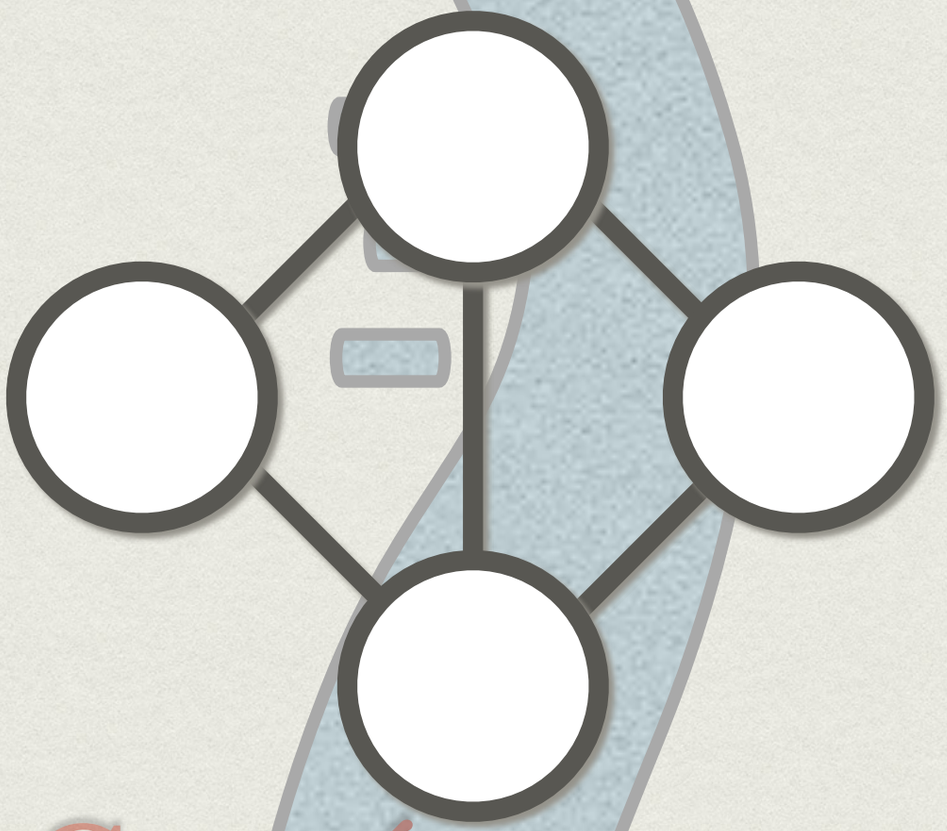



c_0
c_3
0-3
c_0
c_2
c_3
2-3
c_0
c_2
c_3
Complétude
Cohérence

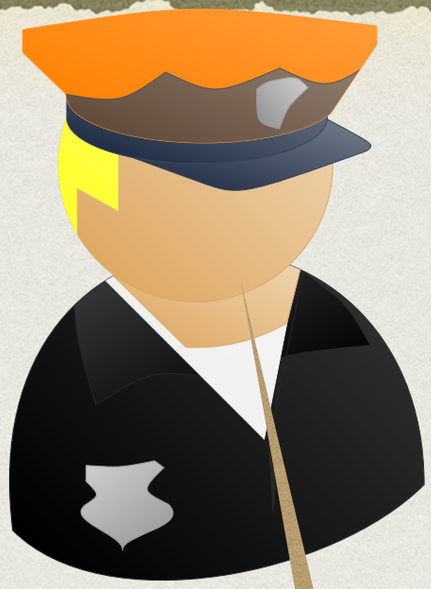

c_0
c_3
0-3
c_0
c_2
c_3
2-3
c_0
c_2
Complétude
Cohérence

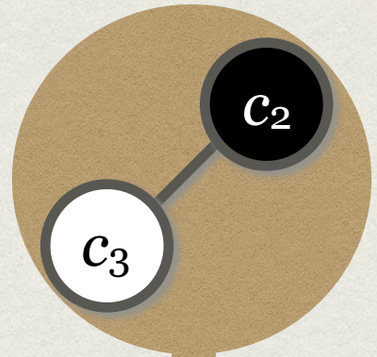


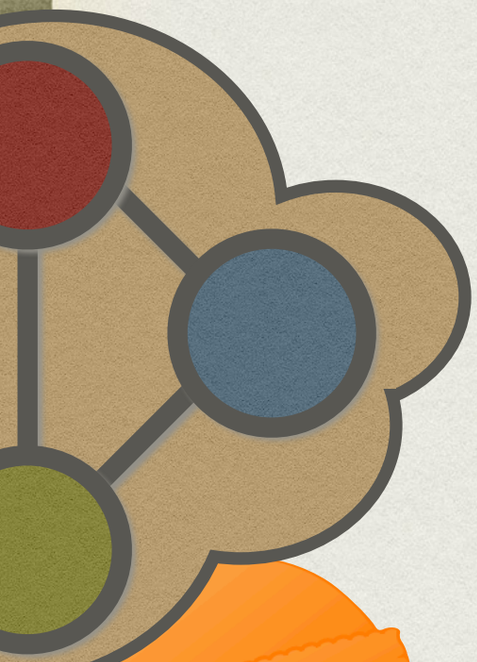
Complétude

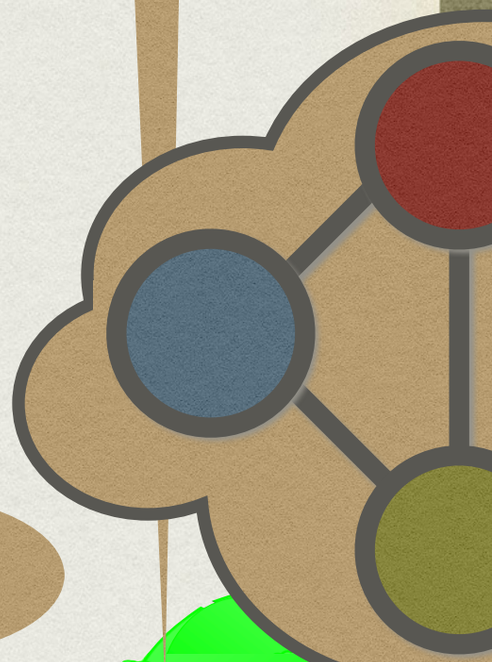


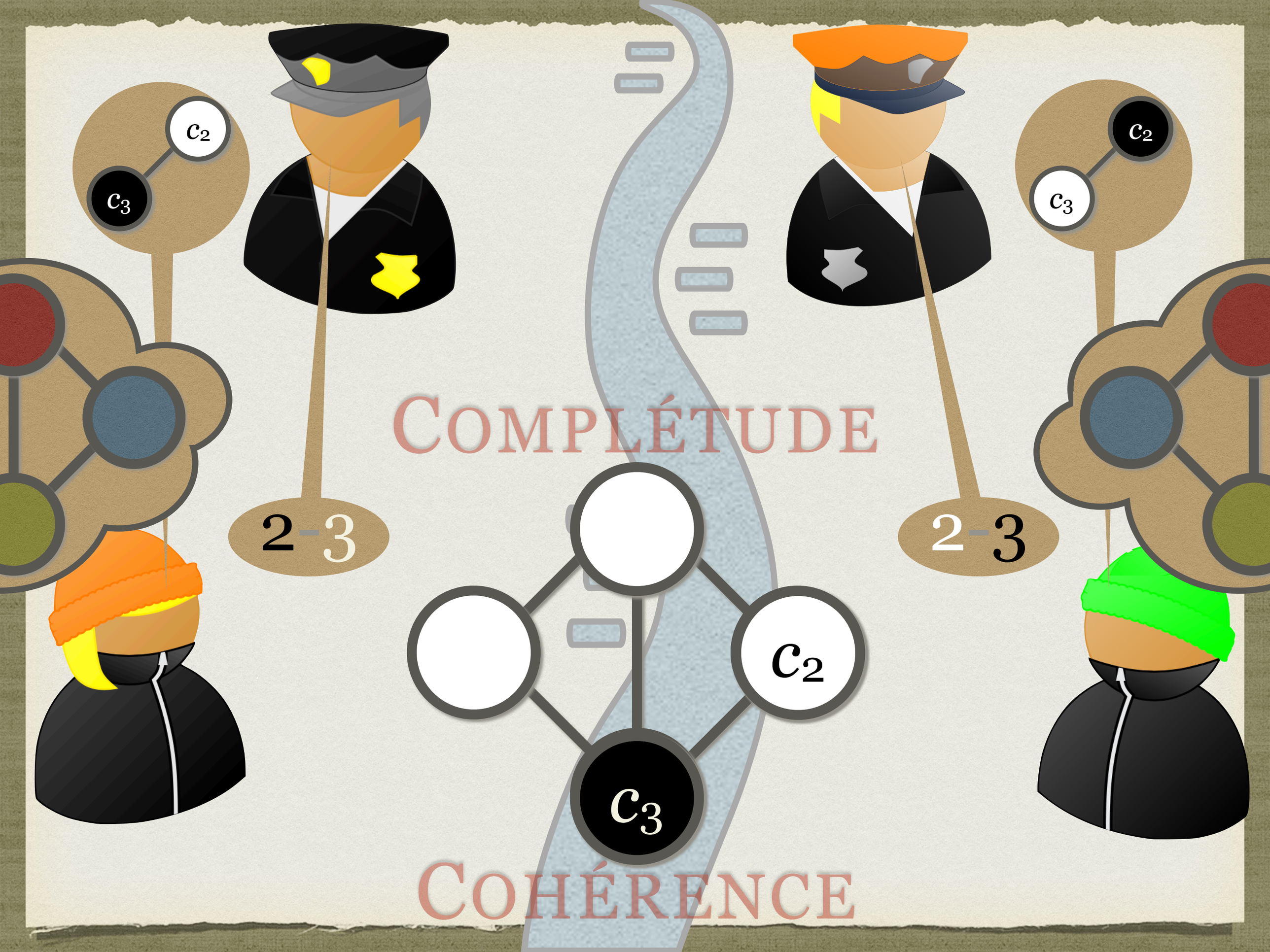
Cohérence

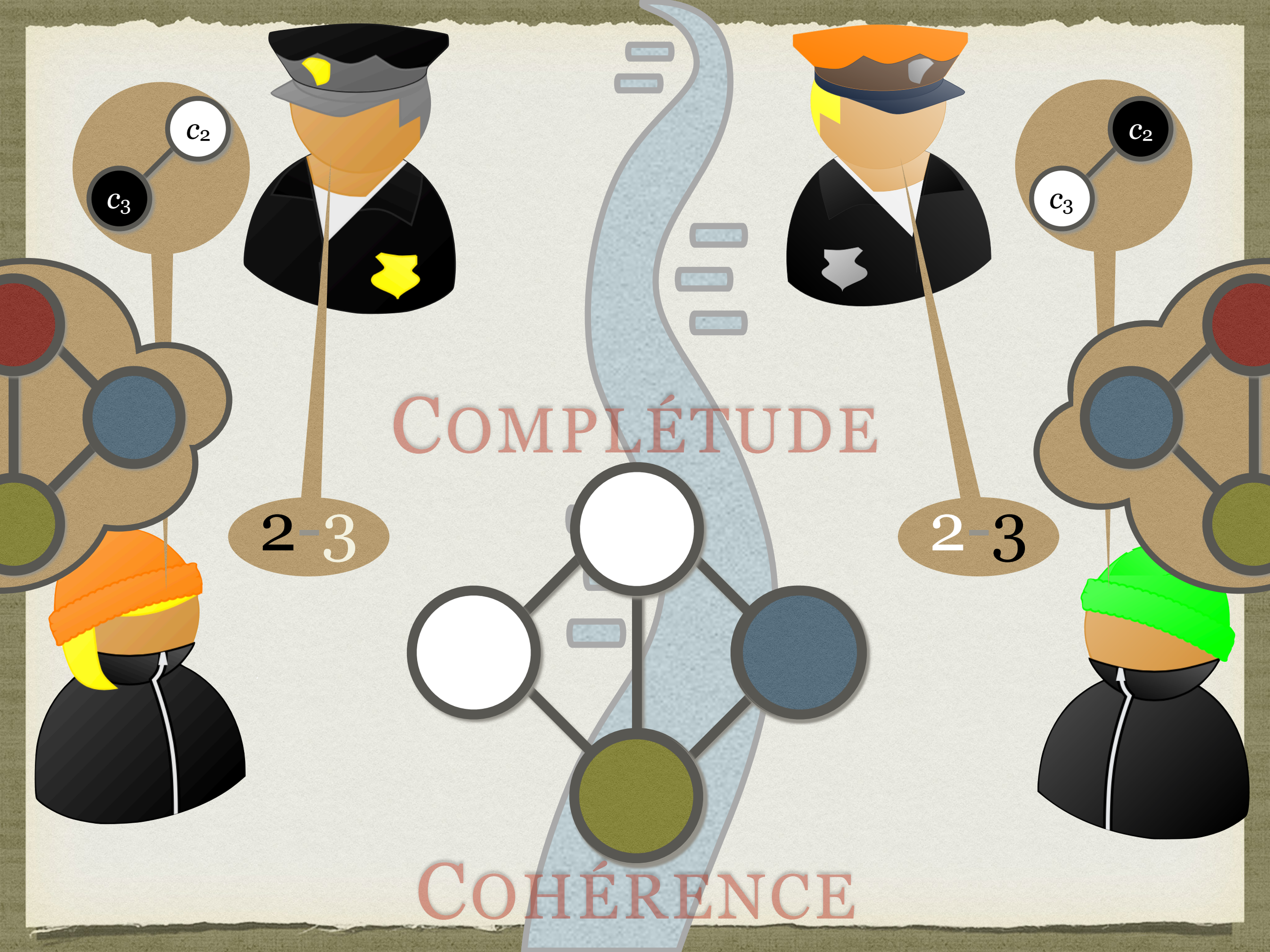









c_2
c_3
2-3
c_2
c_3
2-3
Complétude
c_2
c_3
Cohérence


c_2
c_3
2-3
c_2
c_3
2-3
Complétude
Cohérence

COHÉRENCE MALGRÉ L'INTRICATION

HONNÊTE:

$$MEG^{k}[n_i, r_i, n_j, r_j] = (coul_{n_i} + b_{n_i} r_i \ , \ coul_{n_j} + b_{n_j} r_j)$$

ANALYSE DE CAS

COHÉRENCE MALGRÉ L'INTRICATION

HONNÊTE:

$$MEG^k[n_i, r_i, n_j, r_j] = (coul_{n_i} + b_{n_i} r_i \ , \ coul_{n_j} + b_{n_j} r_j)$$

MALHONNÊTE:

ANALYSE DE CAS

COHÉRENCE MALGRÉ L'INTRICATION

HONNÊTE:

$$MEG^k[n_i, r_i, n_j, r_j] = (coul_{n_i} + b_{n_i} r_i \ , \ coul_{n_j} + b_{n_j} r_j)$$

MALHONNÊTE:

$$MEG^k[n_i, r_i, n_j, r_j] = \text{arbitraire}$$

ANALYSE DE CAS

COHÉRENCE MALGRÉ L'INTRICATION

HONNÊTE:

$$MEG^k[n_i, r_i, n_j, r_j] = (coul_{n_i} + b_{n_i} r_i \ , \ coul_{n_j} + b_{n_j} r_j)$$

MALHONNÊTE:

$$MEG^k[n_i, r_i, n_j, r_j] = \text{arbitraire}$$

$$MEG[n_i, r_i] = \text{bien-défini}$$

ANALYSE DE CAS

COHÉRENCE MALGRÉ L'INTRICATION

HONNÊTE:

$$MEG^k[n_i, r_i, n_j, r_j] = (coul_{n_i} + b_{n_i} r_i \ , \ coul_{n_j} + b_{n_j} r_j)$$

MALHONNÊTE:

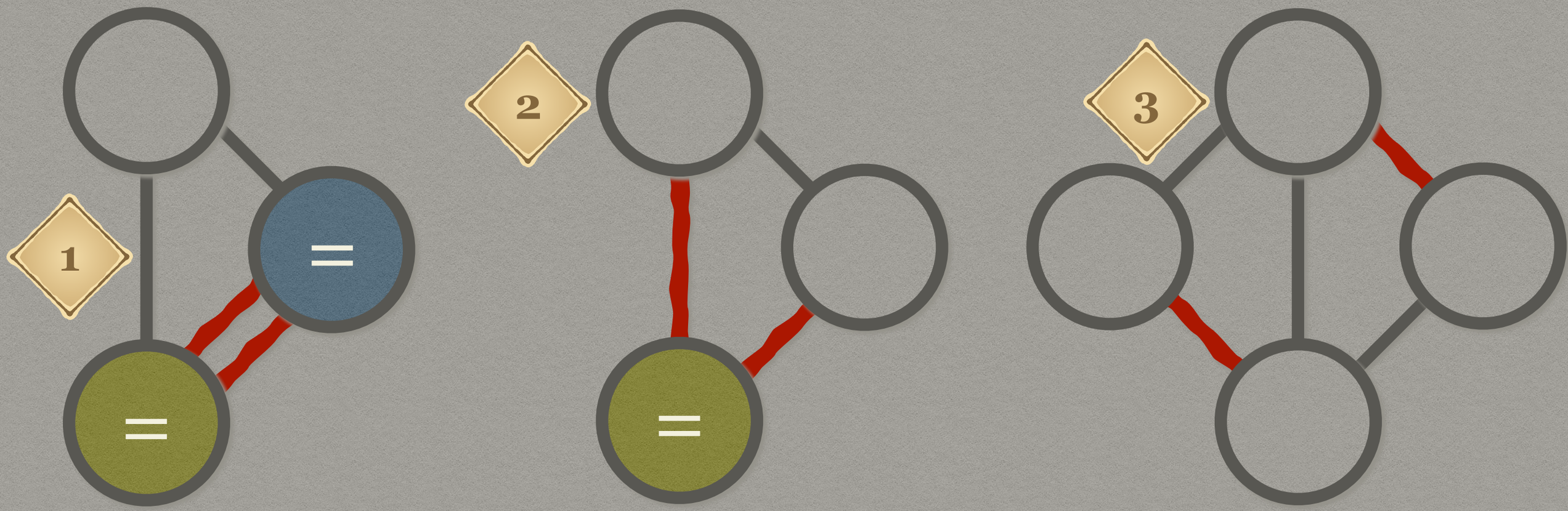
$$MEG^k[n_i, r_i, n_j, r_j] = \text{arbitraire}$$

$$MEG[n_i, r_i] = \text{bien-défini}$$

$$COUL[n_i] = \text{bien-défini}$$

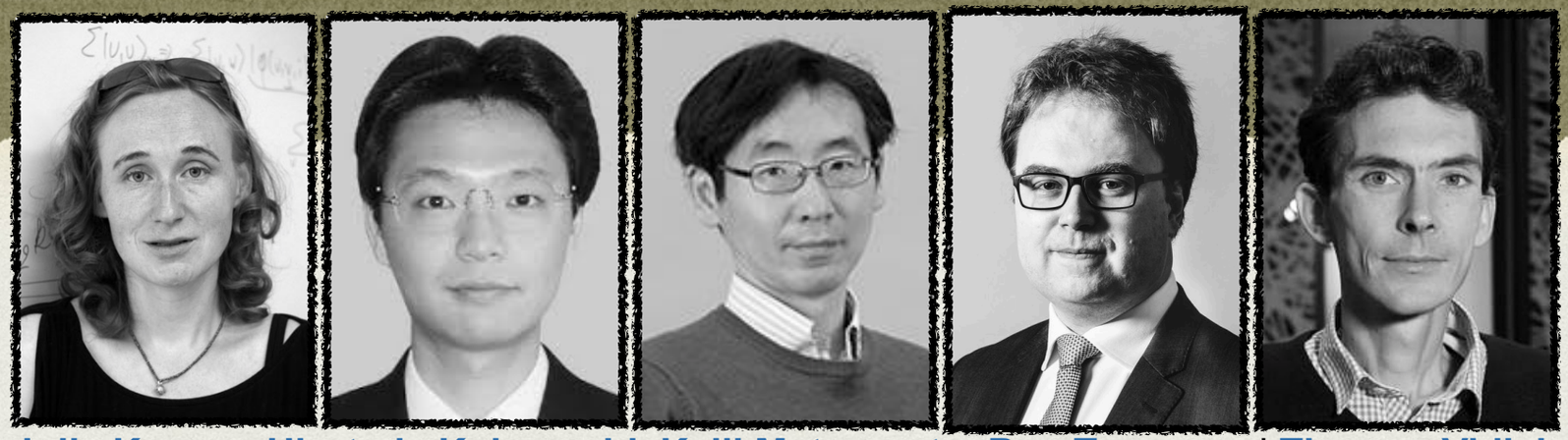
ANALYSE DE CAS

SIMULATION ZK



ANALYSE DE CAS

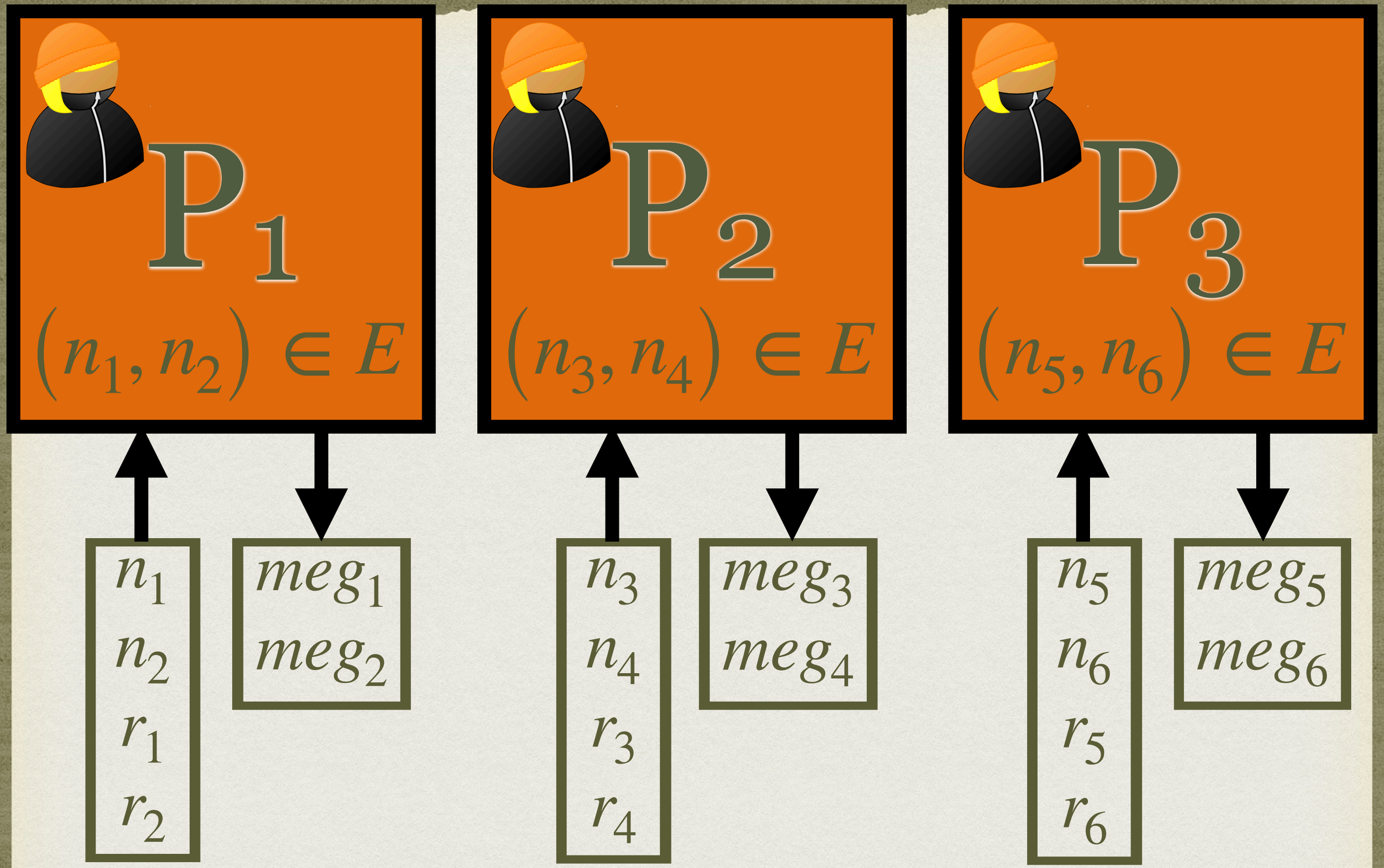
POWERFUL THEOREM



Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick

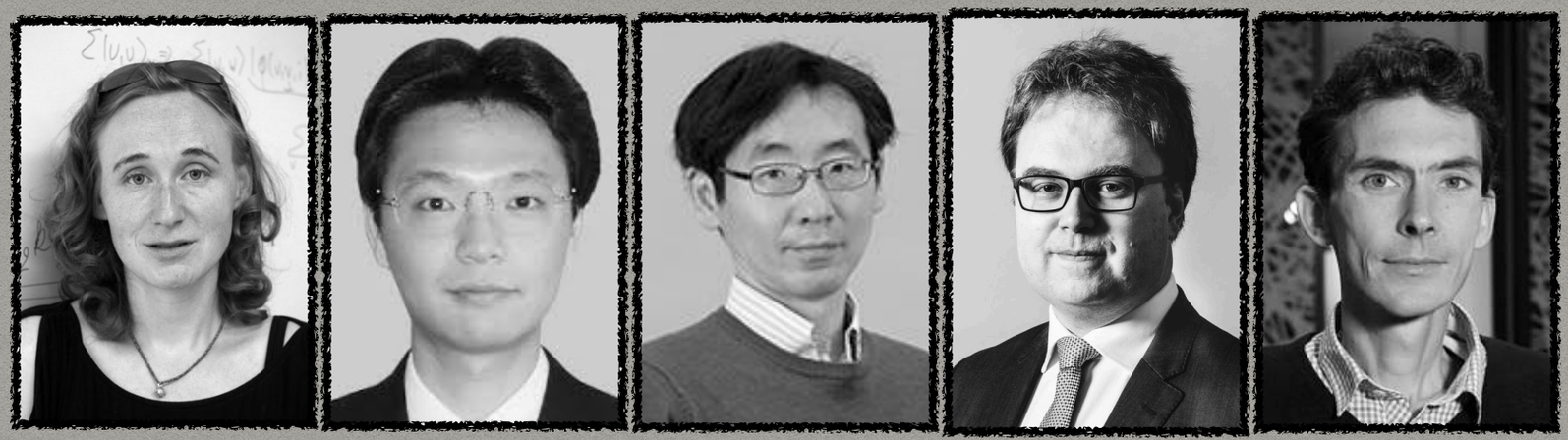
Entangled Games Are Hard to Approximate

- Si PI est cohérente face aux prouveurs *locaux* *alors* PI augmenté grâce à *1* prouveur imitant les premiers est cohérente face aux prouveurs *intriqués*



$$meg_i = b_{n_i} r_i + coul_{n_i}$$

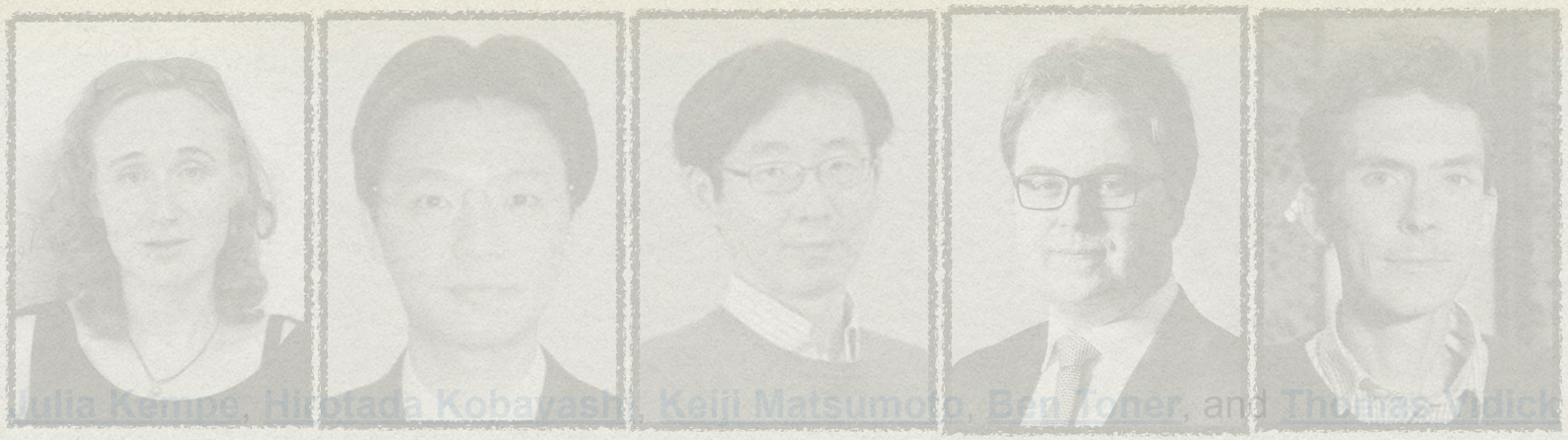
COHÉRENCE MALGRÉ L'INTRICATION



ANALYSE DE CAS

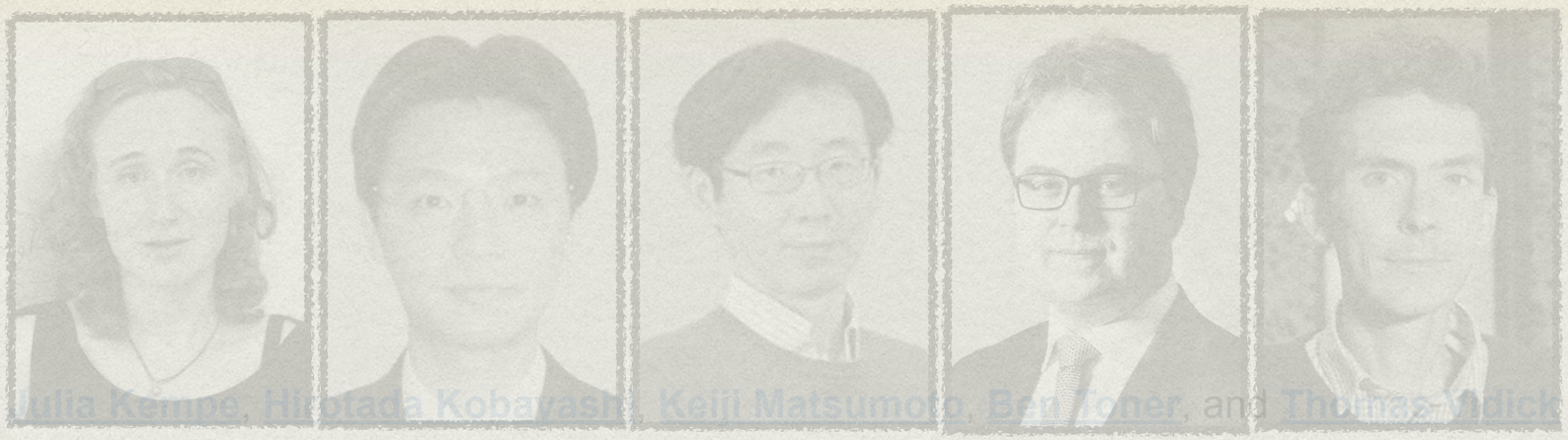
GROUPE TECHNOLOGIES QUANTIQUES
UNIVERSITÉ DE GENÈVE

QUESTIONS OUVERTES: THÉORÈME ANALOGUE?



Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick

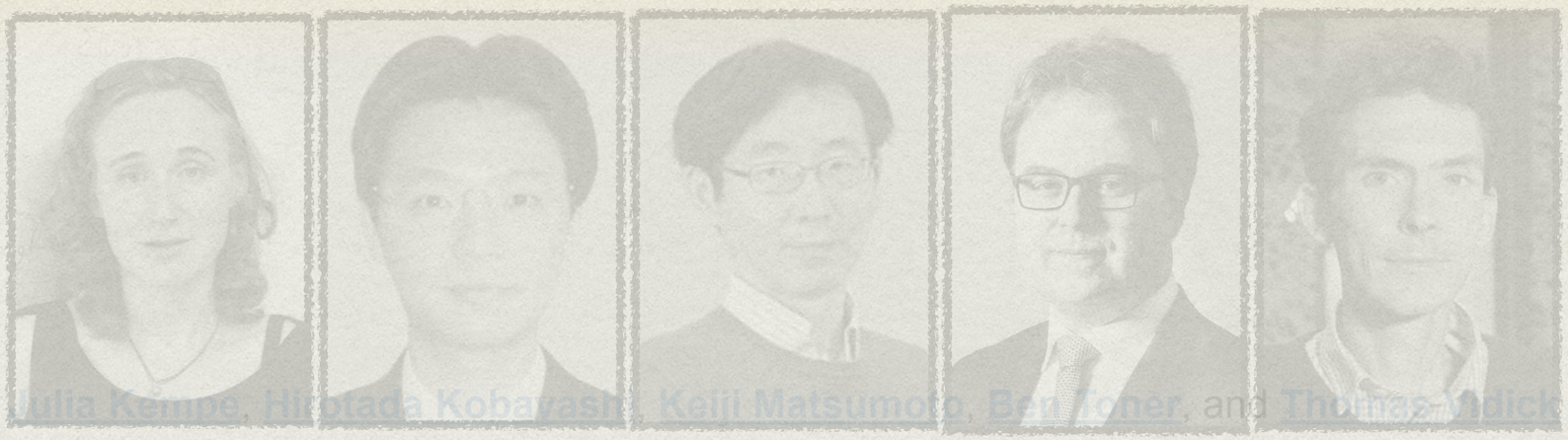
QUESTIONS OUVERTES: THÉORÈME ANALOGUE?



Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick

- Si PI est cohérente contre prouveurs *locaux/intriqués* alors PI augmenté grâce à *N* prouveurs imitant les premiers cohérente face aux prouveurs *Non-Signalants* ?

QUESTIONS OUVERTES: THÉORÈME ANALOGUE?



Julia Kempe, Hirotada Kobayashi, Keiji Matsumoto, Ben Toner, and Thomas Vidick

- Si PI est cohérente contre prouveurs *locaux/intriqués* alors PI augmenté grâce à *N* prouveurs imitant les premiers cohérente face aux prouveurs *Non-Signalants* ?

- Zero-Knowledge ?

Arnaud Yoh Massenet-Oshima
Louis Salvail
Lucas Shigeru Stinchcombe
Nan Yang

PREUVE *ZERO-KNOWLEDGE* POUR NP RELATIVISTES ET RÉALISABLES (COHÉRENTE MALGRÉ L'INTRICATION)

Claude Crépeau

McGill