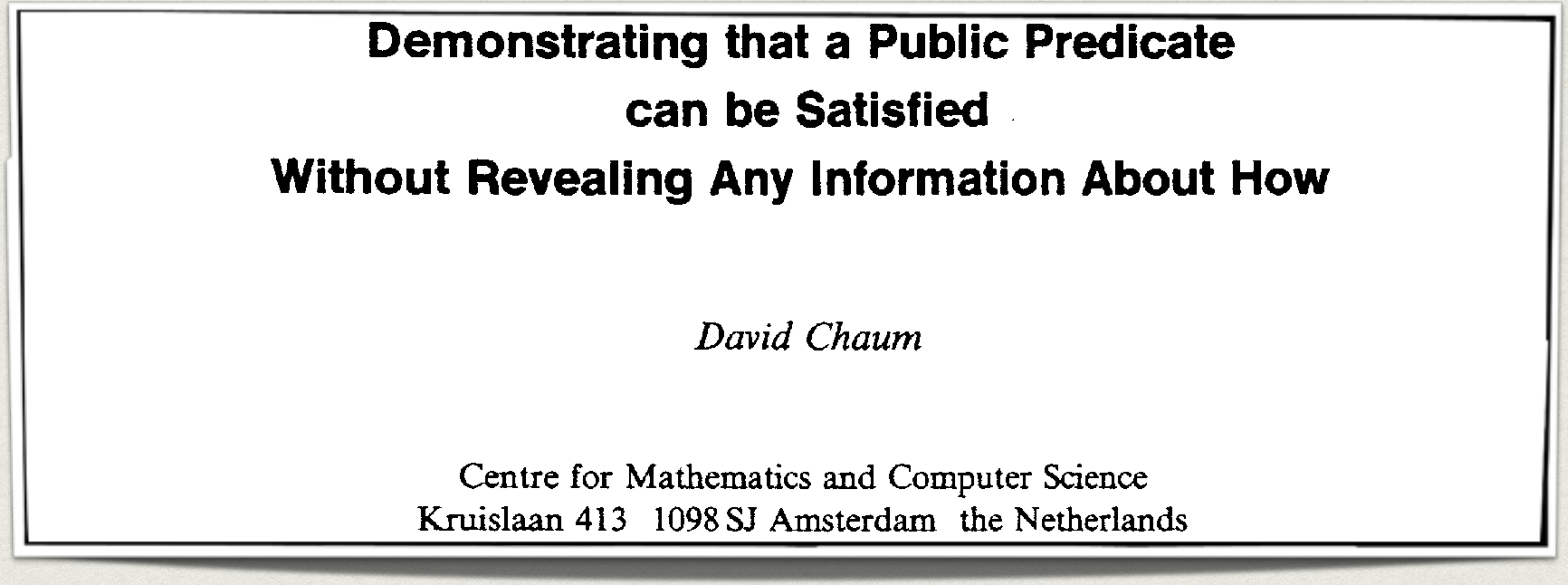
Demonstrating that a Public *Graph* can be *3-Coloured* Without Revealing Any *Knowledge* About How

Claude Crépeau

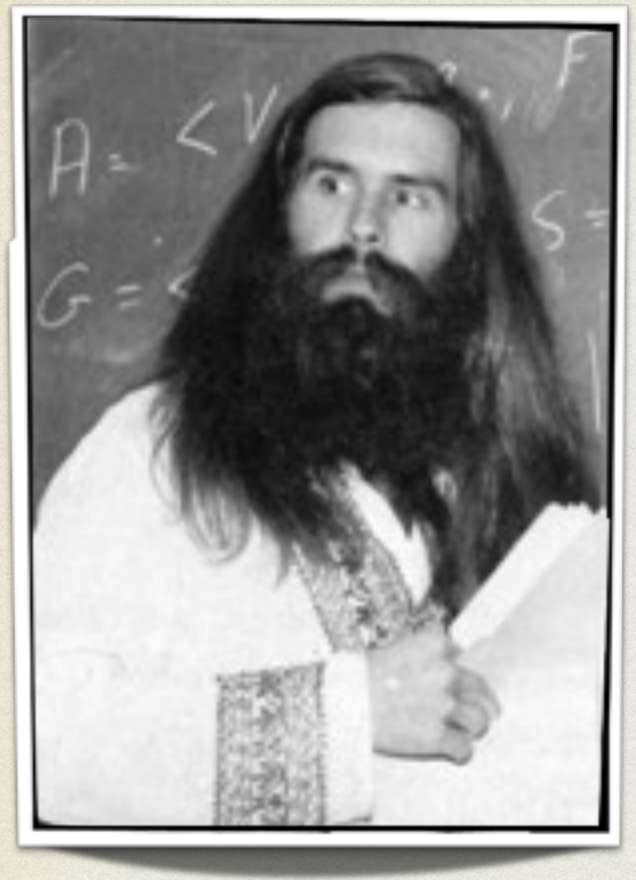
McGill

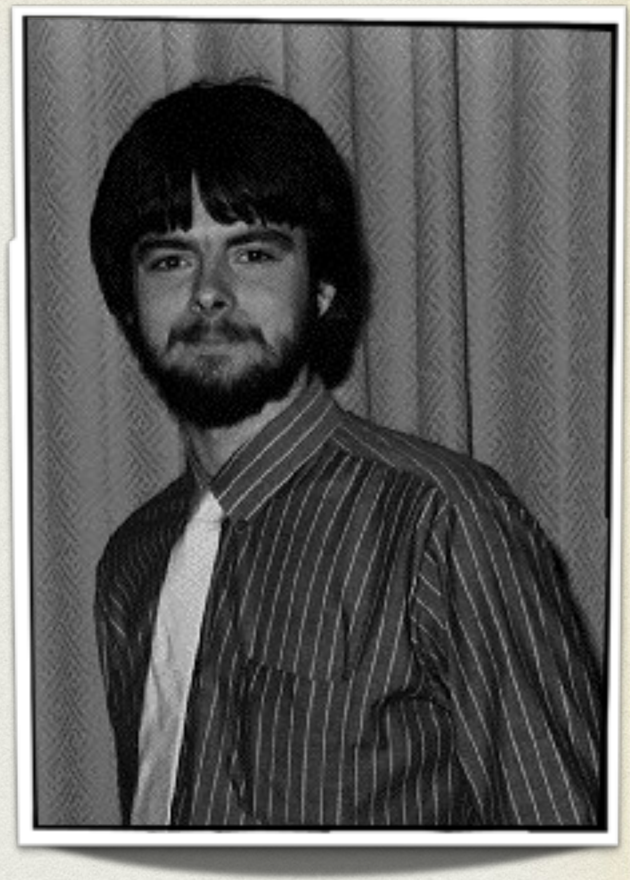


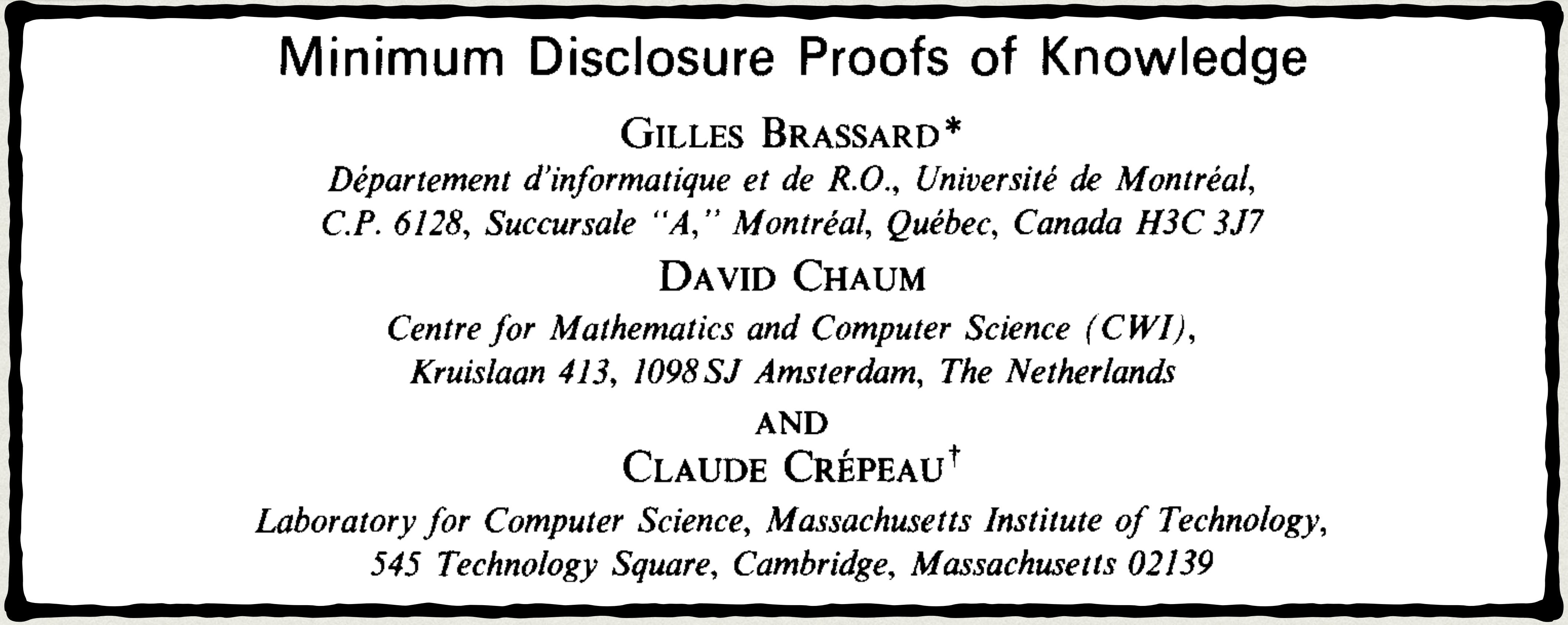
Demonstrating that a Public Predicate can be Satisfied Without Revealing Any Information About How

David Chaum

Centre for Mathematics and Computer Science
Kruislaan 413 1098 SJ Amsterdam the Netherlands







Minimum Disclosure Proofs of Knowledge

GILLES BRASSARD*
Département d'informatique et de R.O., Université de Montréal,
C.P. 6128, Succursale "A," Montréal, Québec, Canada H3C 3J7

DAVID CHAUM
Centre for Mathematics and Computer Science (CWI),
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

AND
CLAUDE CRÉPEAU†
Laboratory for Computer Science, Massachusetts Institute of Technology,
545 Technology Square, Cambridge, Massachusetts 02139

Proving that a Public ***Graph***

can be ***3-Coloured***

Without Revealing Any ***Knowledge*** About How

Claude Crépeau

McGill

Proving

Graph 3-Colouring

Knowledge

(Interactive-)Proving

Shafi Goldwasser

Silvio Micali

Charles Rackoff

(Interactive-)Proving

Shafi Goldwasser

Silvio Micali

Charles Rackoff

Interactive Proofs [GMR-85/89]

(Interactive-)Proving

Shafi Goldwasser

Silvio Micali

Charles Rackoff

Interactive Proofs [GMR-85/89] of membership or knowledge

(Interactive-)Proving

Shafi Goldwasser

Silvio Micali

Charles Rackoff

Interactive Proofs [GMR-85/89] of membership or knowledge

Interactive Arguments [BCC-86/88]

(Interactive-)Proving

Shafi Goldwasser

Silvio Micali

Charles Rackoff

Interactive Proofs [GMR-85/89] of membership or knowledge

Interactive Arguments [BCC-86/88]

  SNARGs (Succinct Non-interactive ARGuments)
  SNARKs (SNARGs of Knowledge) [Di Crescenzo-Lipmaa-08]

(Interactive-)Proving

Shafi Goldwasser

Silvio Micali

Charles Rackoff

Interactive Proofs [GMR-85/89] of membership or knowledge

Interactive Arguments [BCC-86/88]

- **SNARGs (Succinct Non-interactive ARGuments)**
- **SNARKs (SNARGs of Knowledge) [Di Crescenzo-Lipmaa-08]**

CS proofs (Computationally Sound Proofs) [Micali-00]

Graph 3-Colouring

Oded Goldreich

Micali

Avi Wigderson

Graph 3-Colouring

Oded Goldreich

Micali

Avi Wigderson

3-COL [GMW-86/91]

Graph 3-Colouring

Oded Goldreich

Micali

Avi Wigderson

3-COL [GMW-86/91]

SAT [BCC-86/88]

Graph 3-Colouring

Oded Goldreich Micali Avi Wigderson

3-COL [GMW-86/91]

SAT [BCC-86/88]

Hamiltonian circuit [Blum-86]

Manuel Blum

(Zero-)Knowledge

Goldwasser

Micali

Rackoff

(Zero-)Knowledge

Goldwasser

Micali

Rackoff

Zero-Knowledge [GMR-85/89]

(Zero-)Knowledge

Goldwasser

Micali

Rackoff

Zero-Knowledge [GMR-85/89]

Minimum Disclosure [BCC-86/88]

(Zero-)Knowledge

Goldwasser

Micali

Rackoff

Zero-Knowledge [GMR-85/89]

Minimum Disclosure [BCC-86/88]

Witness Hiding
Witness Indistinguishability [FS-90]

Feige

Shamir

INTRODUCTION

(P-V-D)

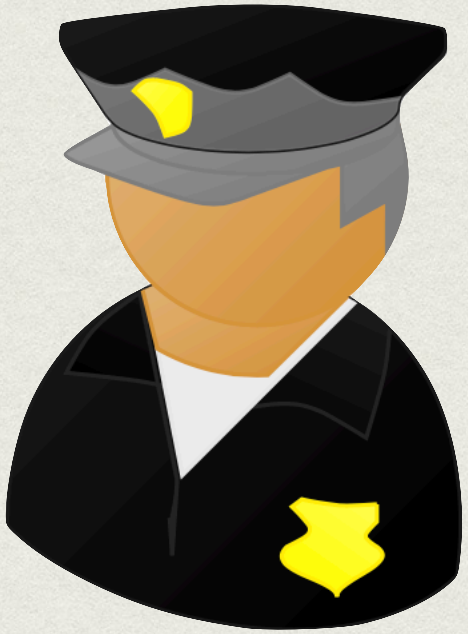
CHARACTERS

CHARACTERS

prover

CHARACTERS

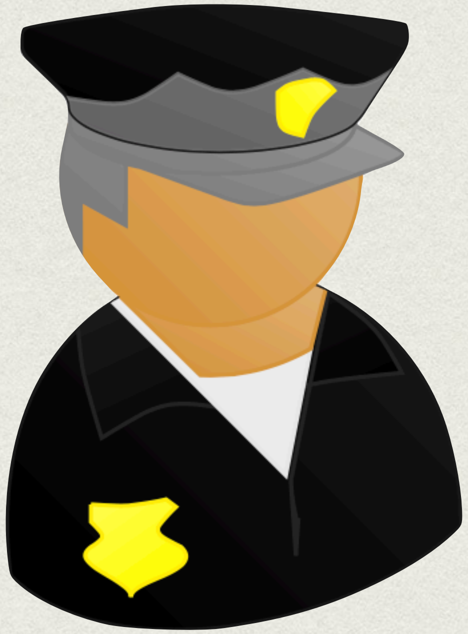
prover



verifier

CHARACTERS

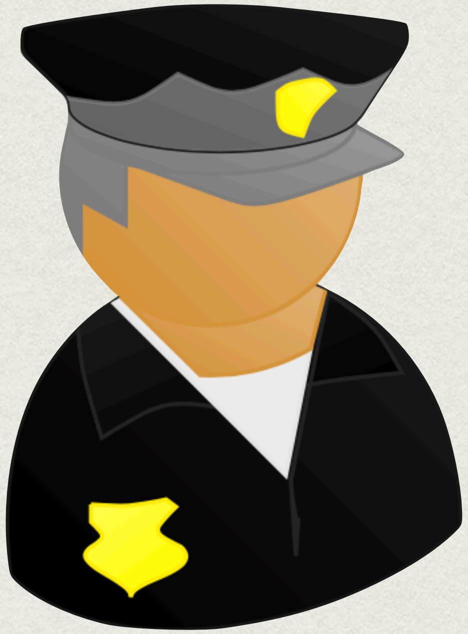
prover



verifier

CHARACTERS

prover



verifier

distinguisher

INTRODUCTION

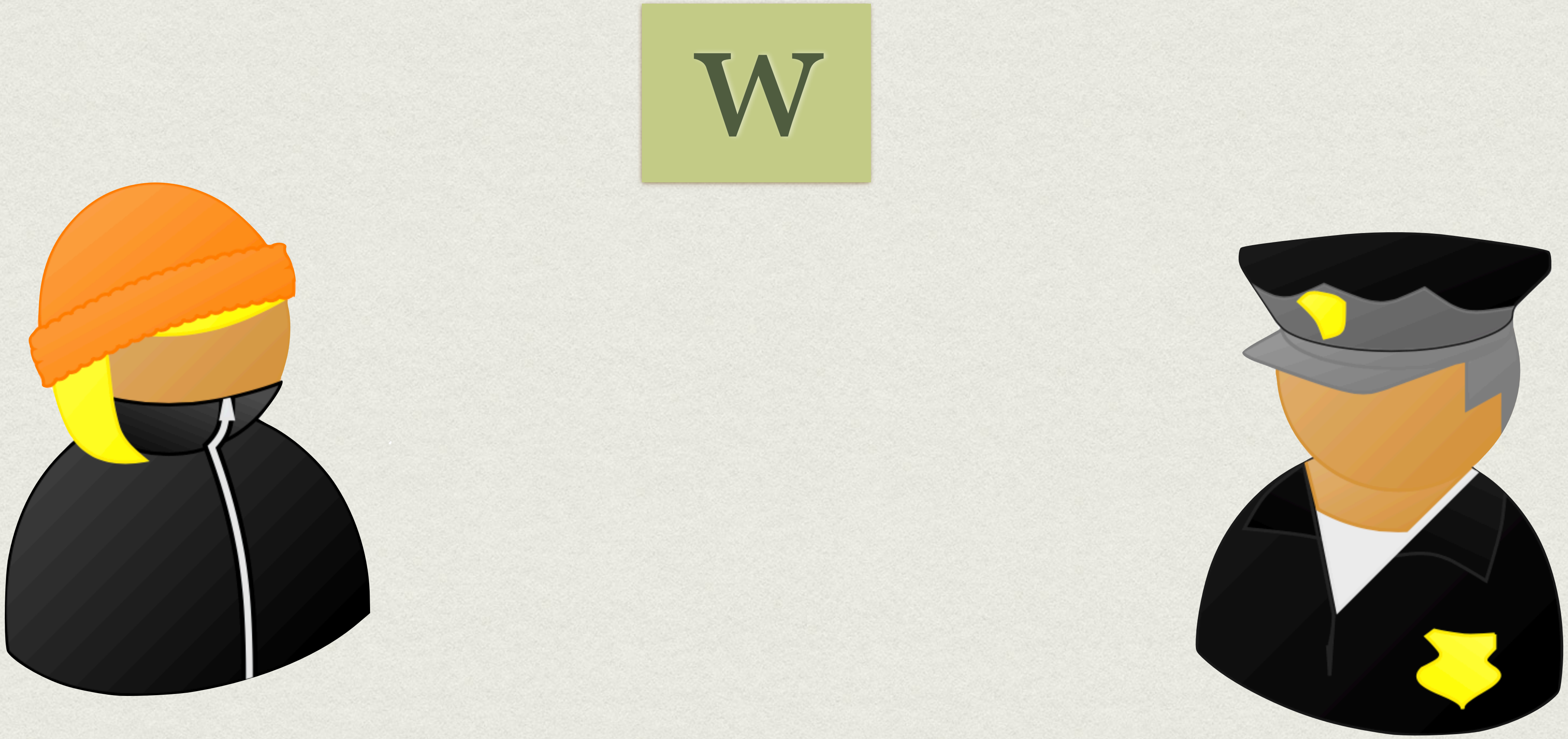
(ZK) IPs


Goldwasser


Micali


Rackoff

1985

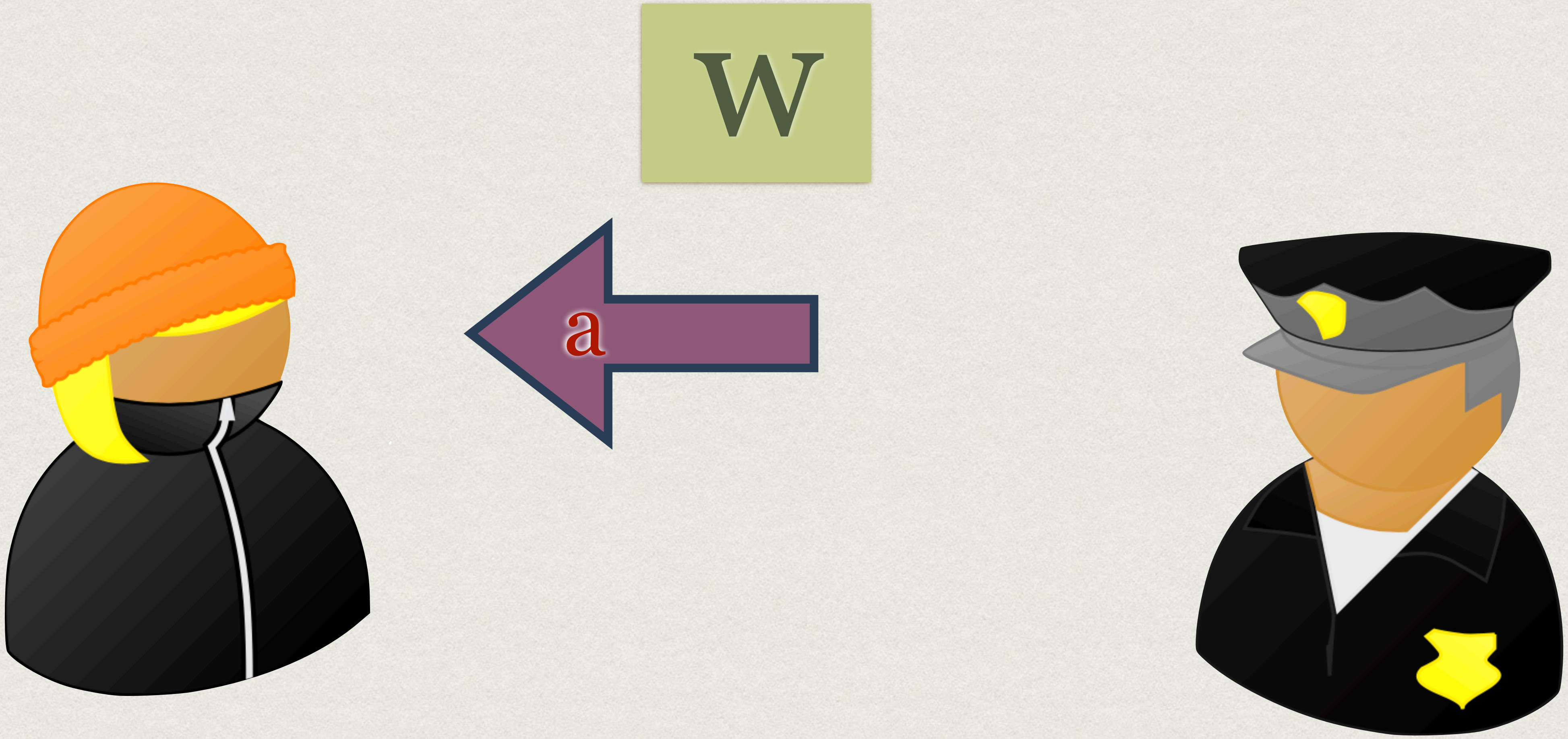

W


Goldwasser


Micali


Rackoff

1985

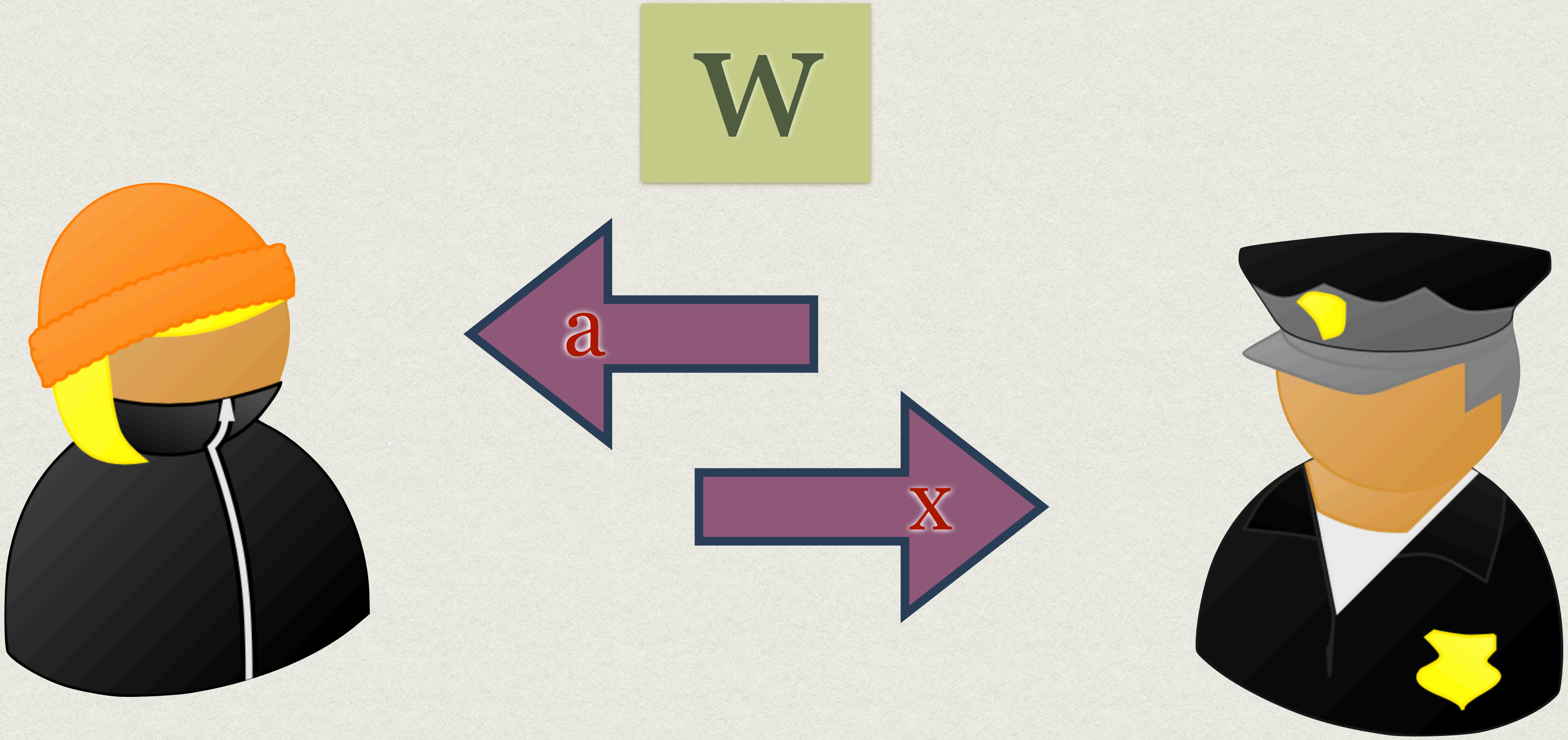


Goldwasser

Micali

Rackoff

1985

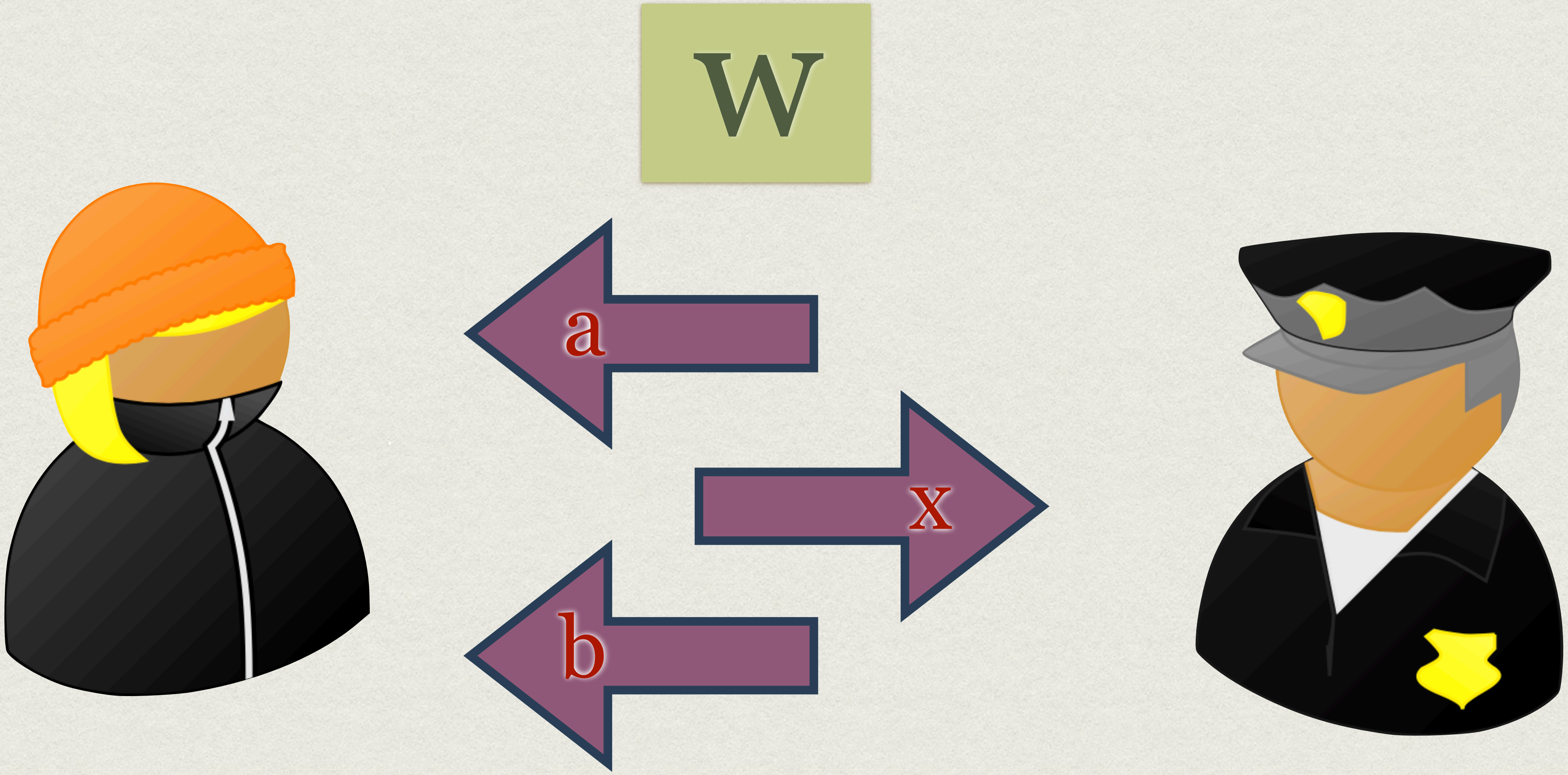


Goldwasser

Micali

Rackoff

1985

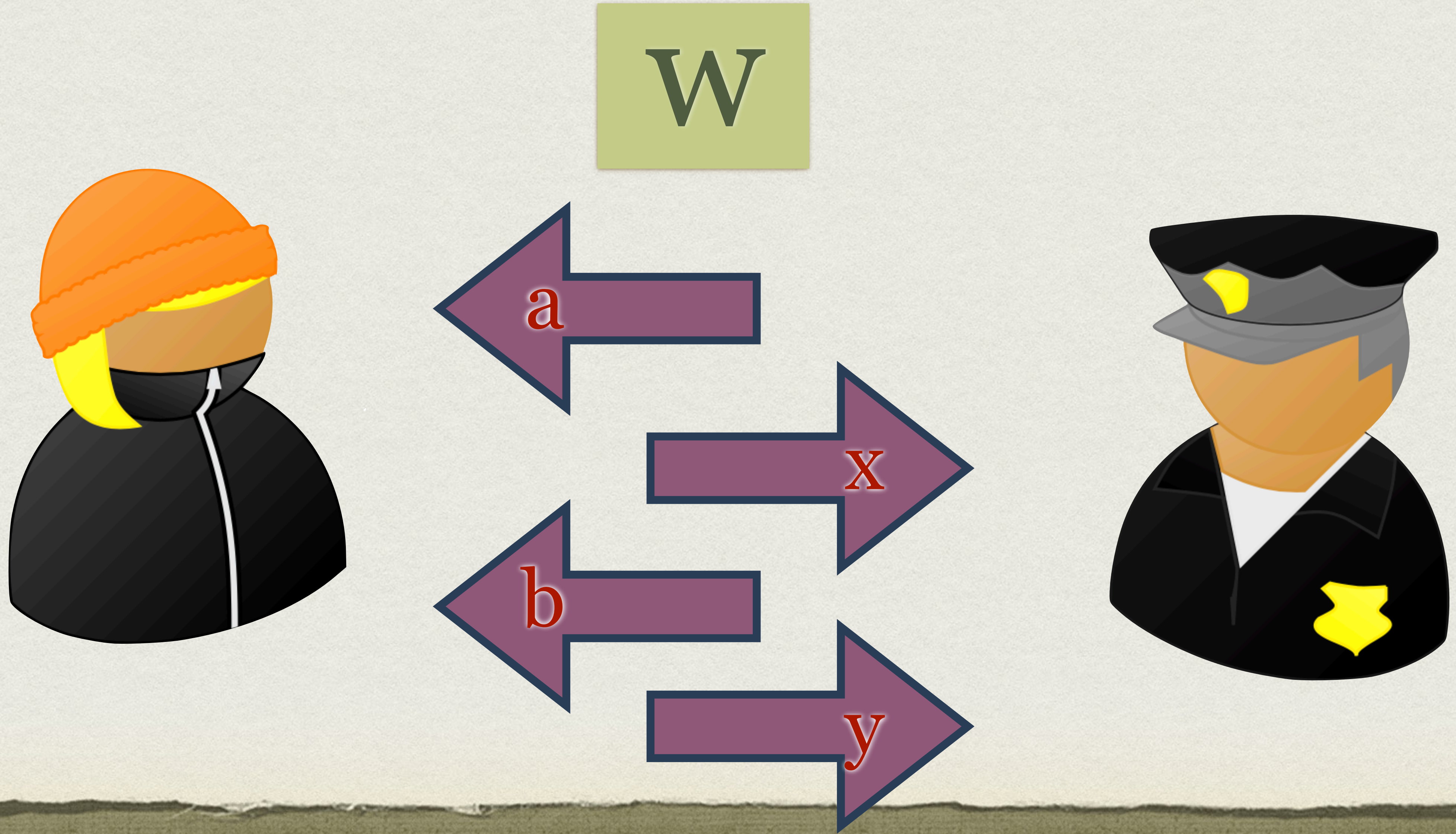


Goldwasser

Micali

Rackoff

1985




Goldwasser

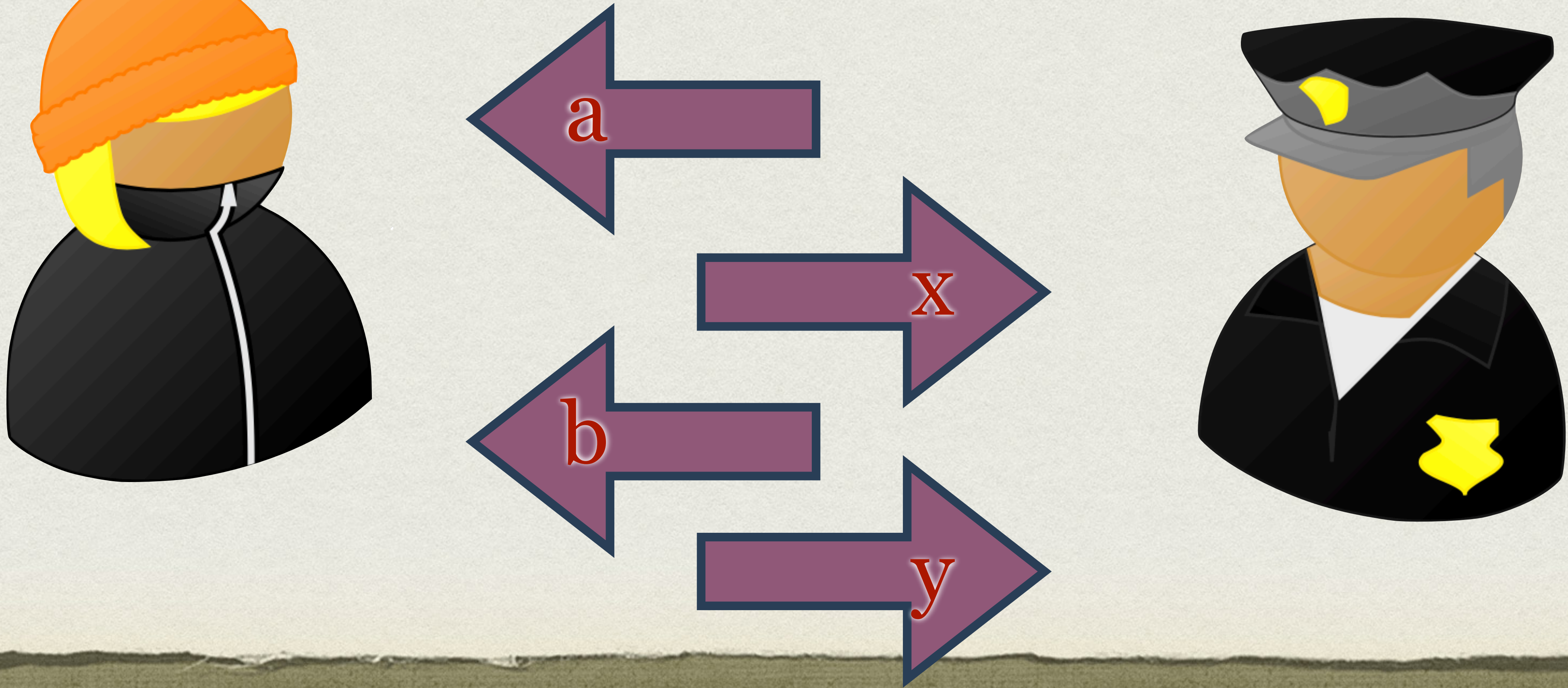

Micali


Rackoff

1985

$w \in L$

w




Goldwasser


Micali

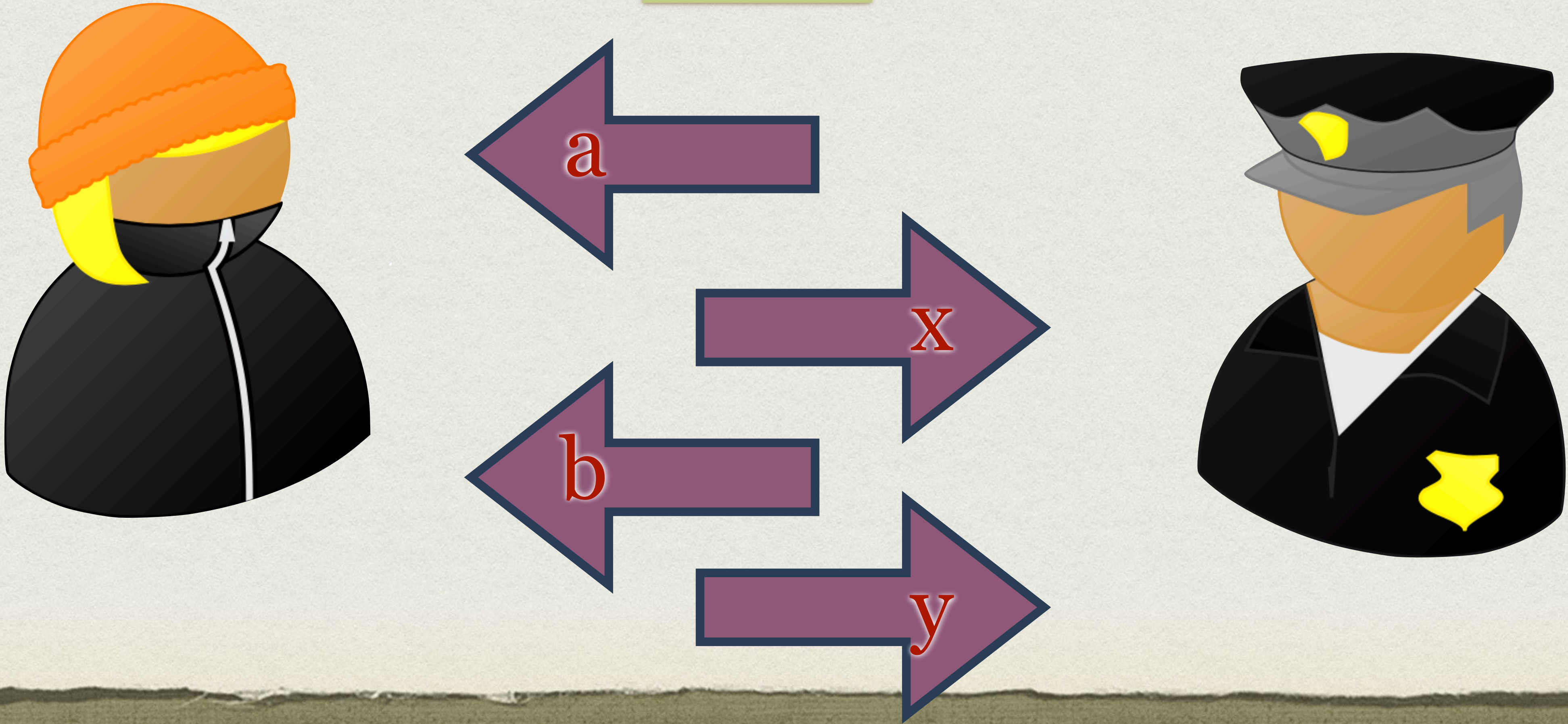

Rackoff

1985

$L \in IP$

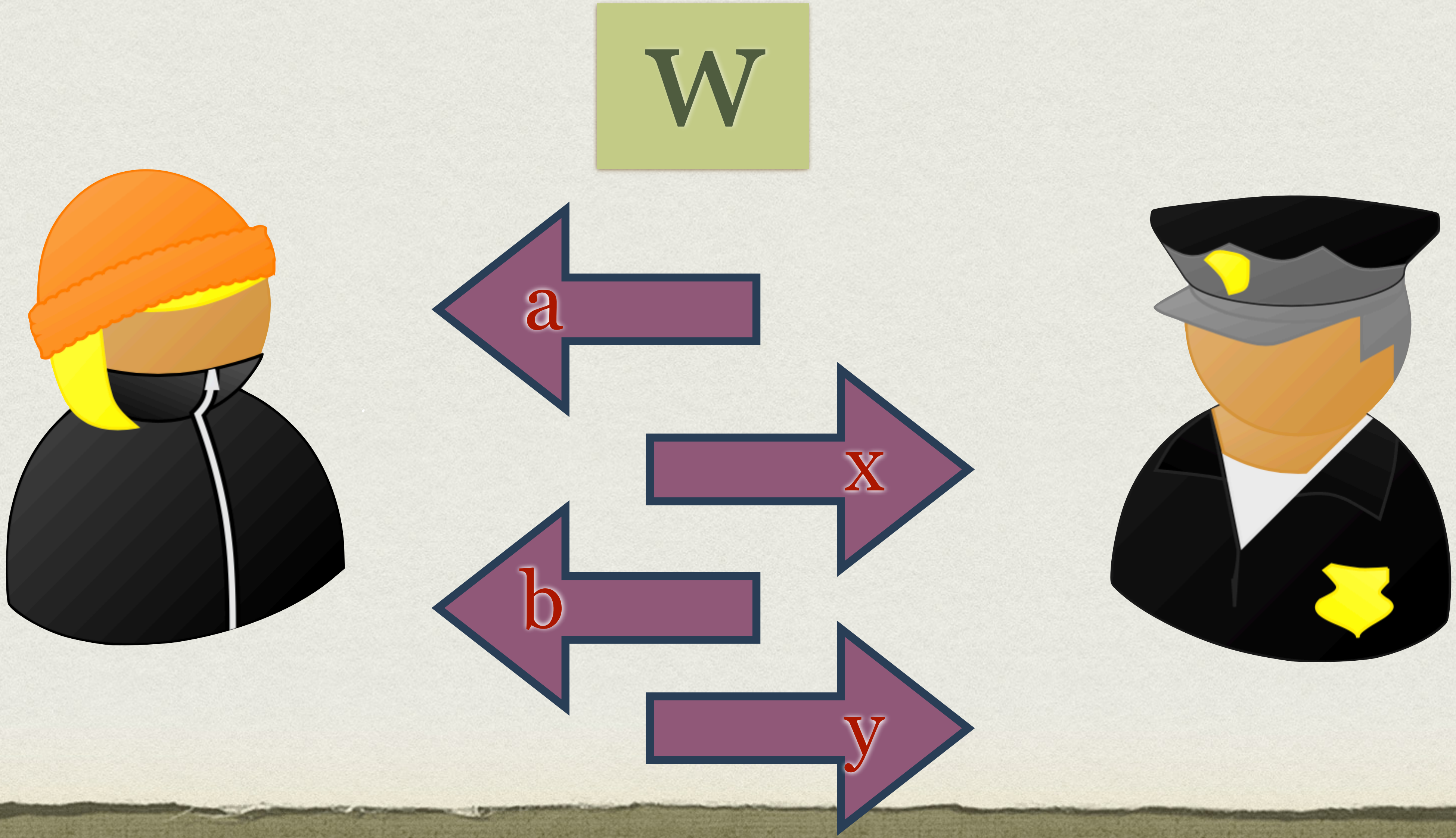
$w \in L$

w



COMPLETENESS

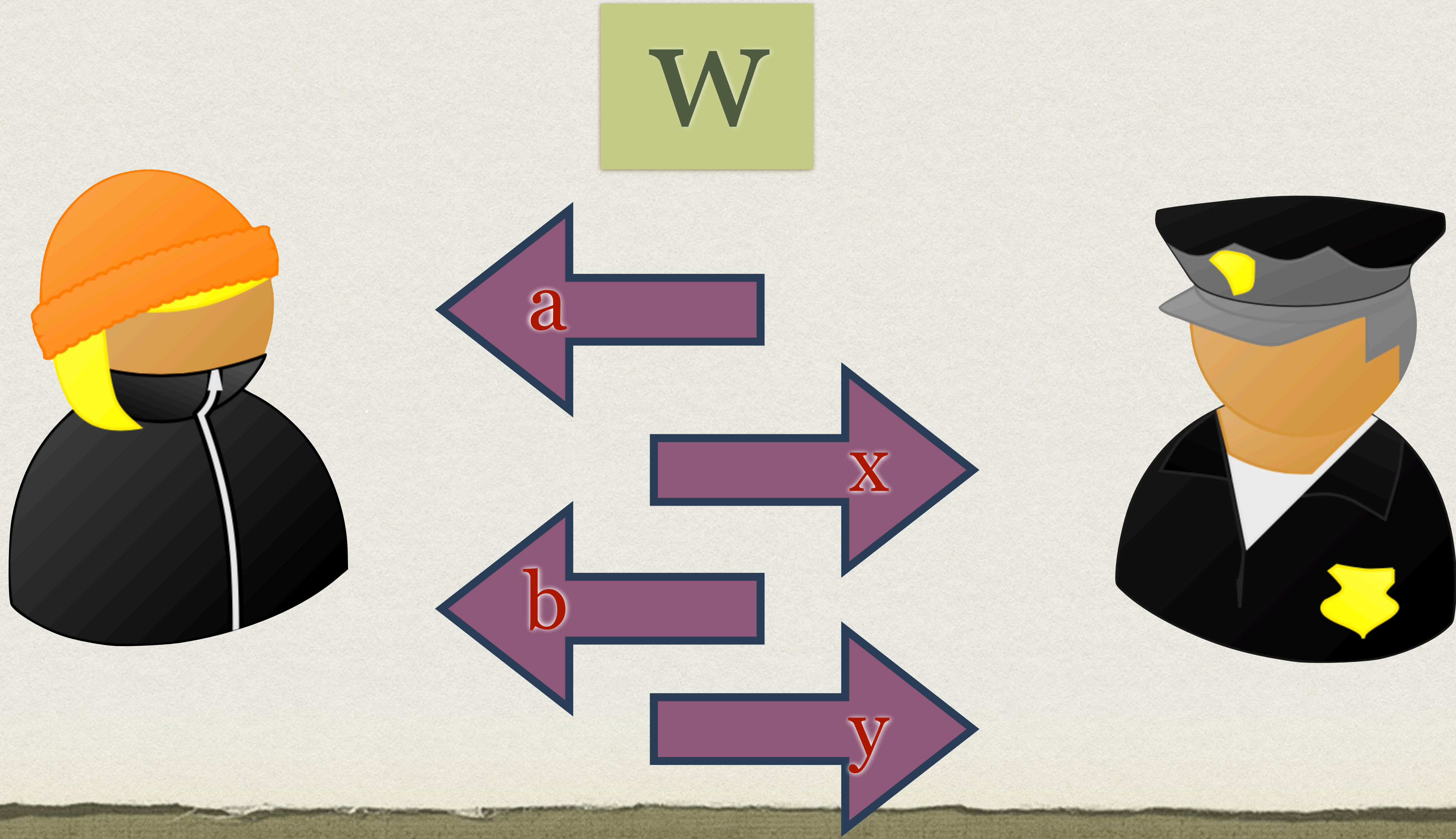
$\exists$ 👮, $\exists$ 🧑, $\forall w \in L$, **Prob**[(🧑:👮) accepts] $\geq 1 - \epsilon$



Completeness

w∈L

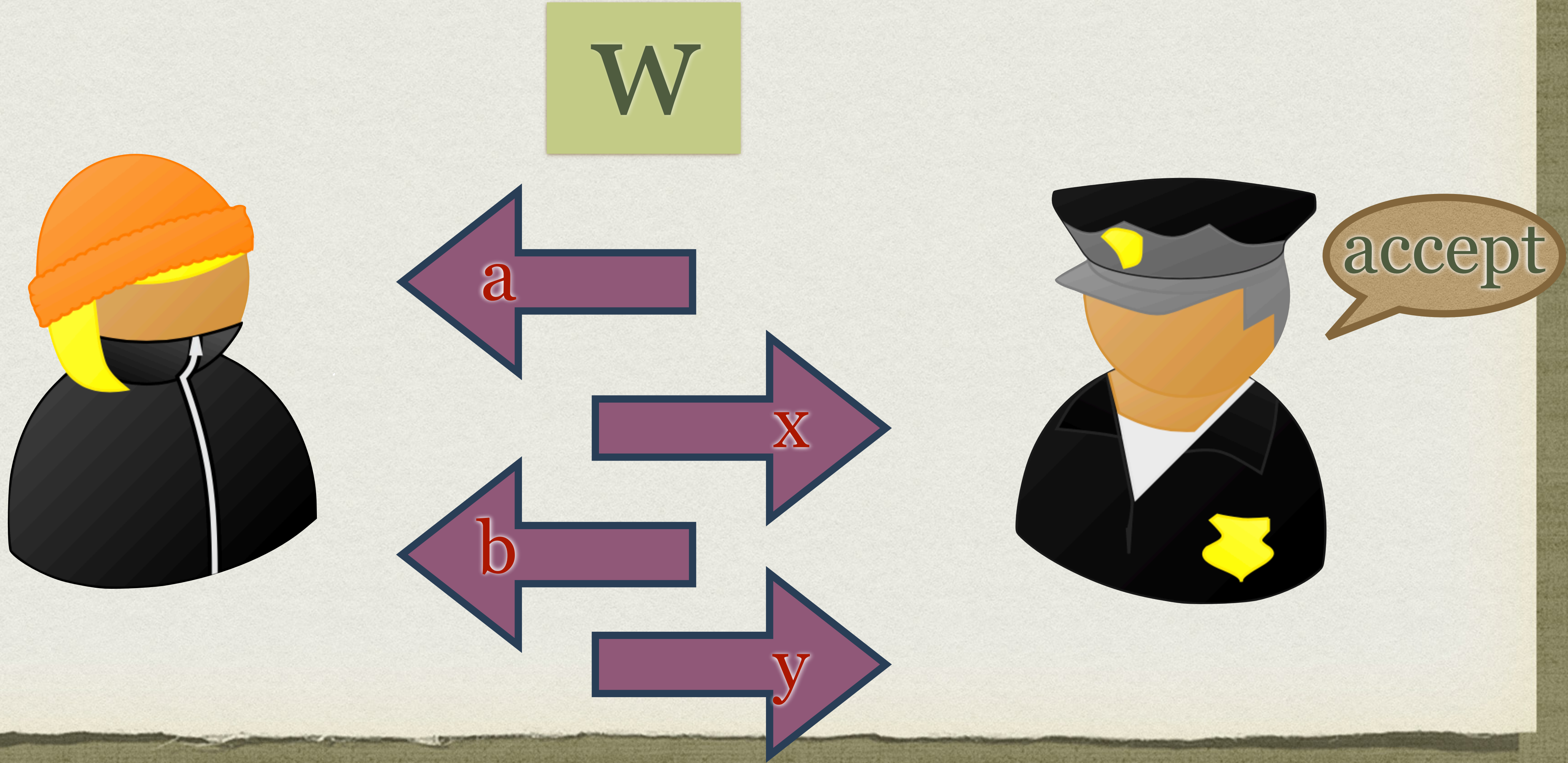
$\exists$ 👮, $\exists$ 🦹, $\forall w \in L$, **Prob**[(🦹:👮) accepts] $\geq 1 - \epsilon$



COMPLETENESS

w∈L

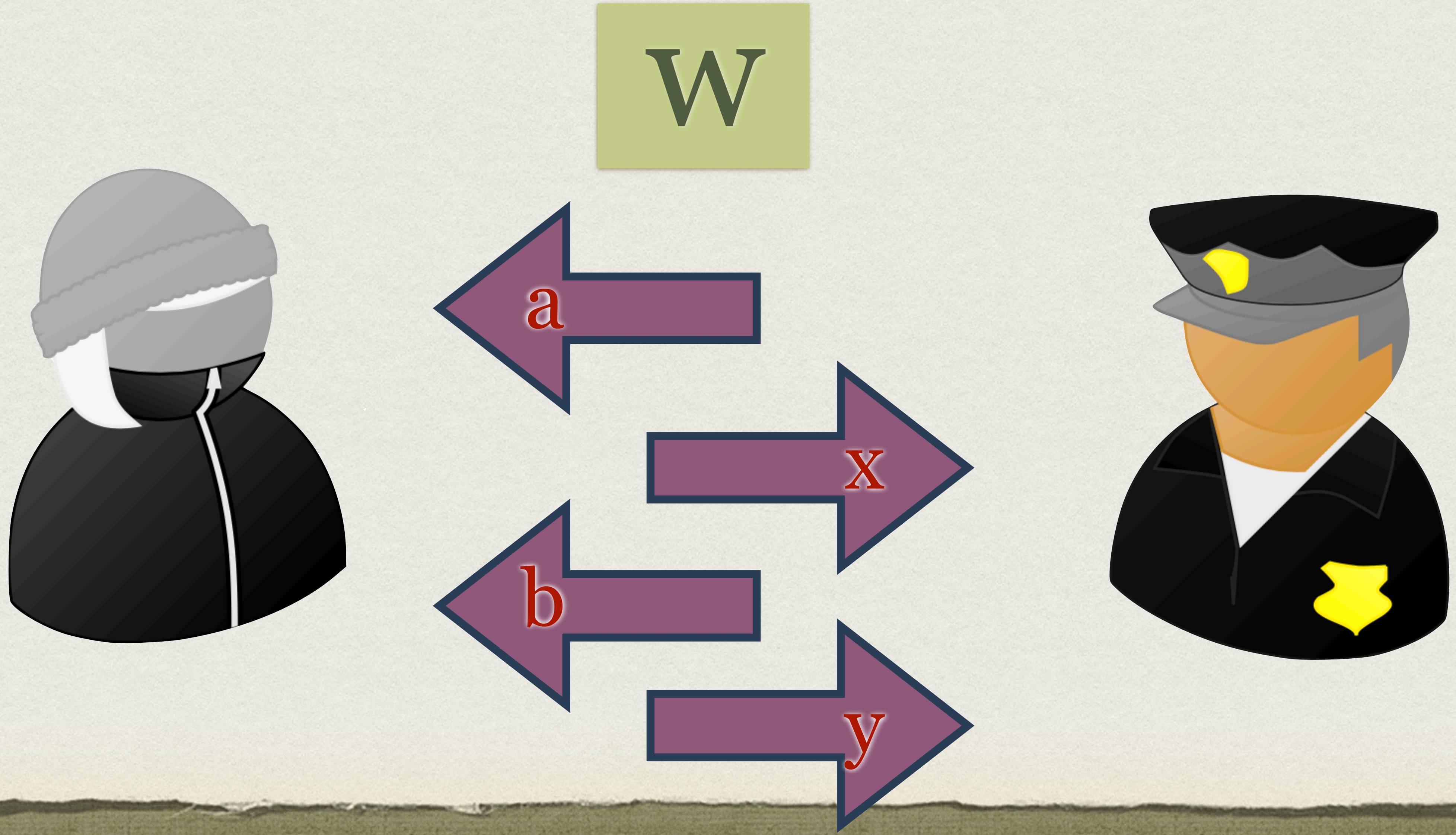
$\exists$ 👮, $\exists$ 👤, $\forall w \in L$, **Prob**[(👤:👮) accepts] $\geq 1 - \epsilon$



SOUNDNESS

$\exists$,

and $\forall$, $\forall w \notin L$, **Prob**[(:) accepts] $\leq \epsilon$



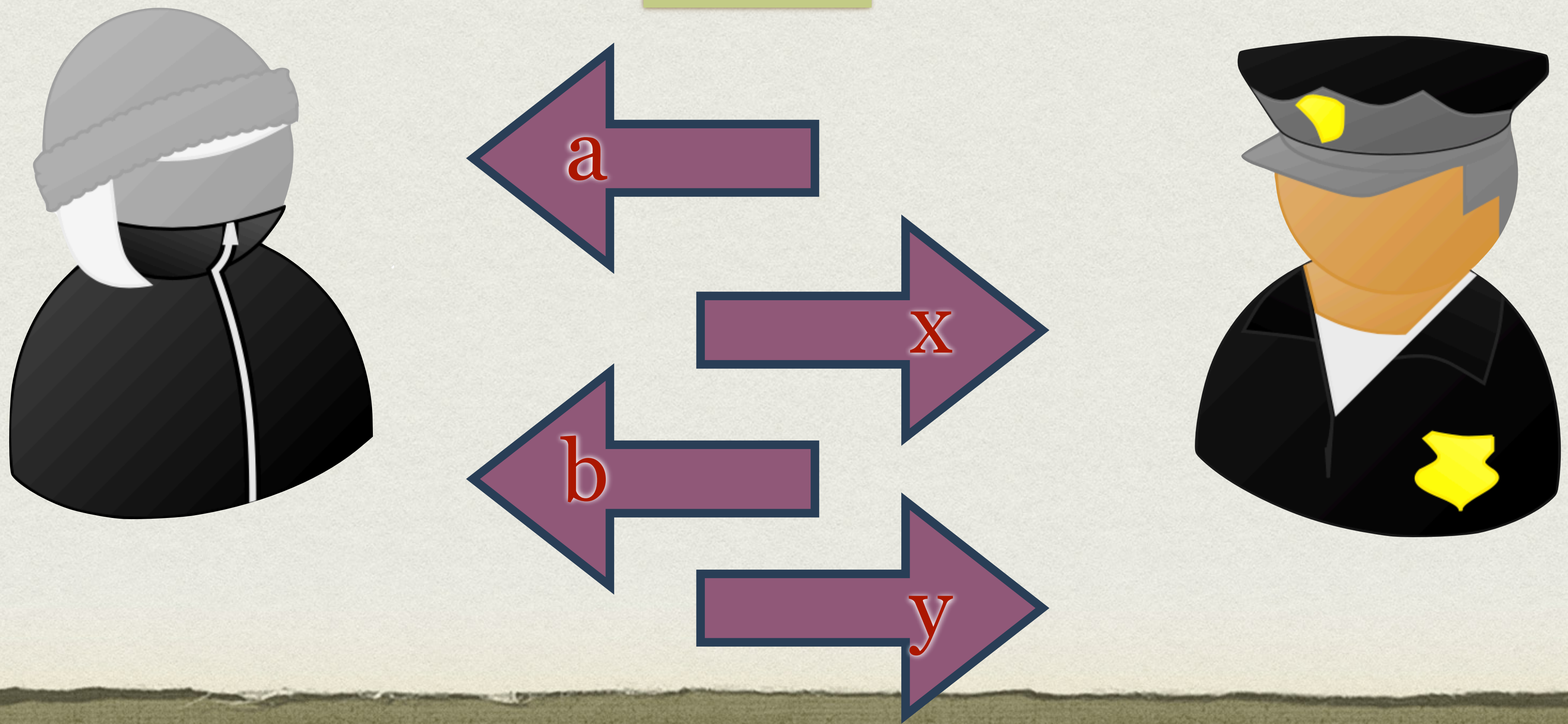
SOUNDNESS

w∉L

∃ 👮,

and ∀ 👤, $\forall w \notin L$, **Prob**[(👤:👮) accepts] $\leq \epsilon$

W

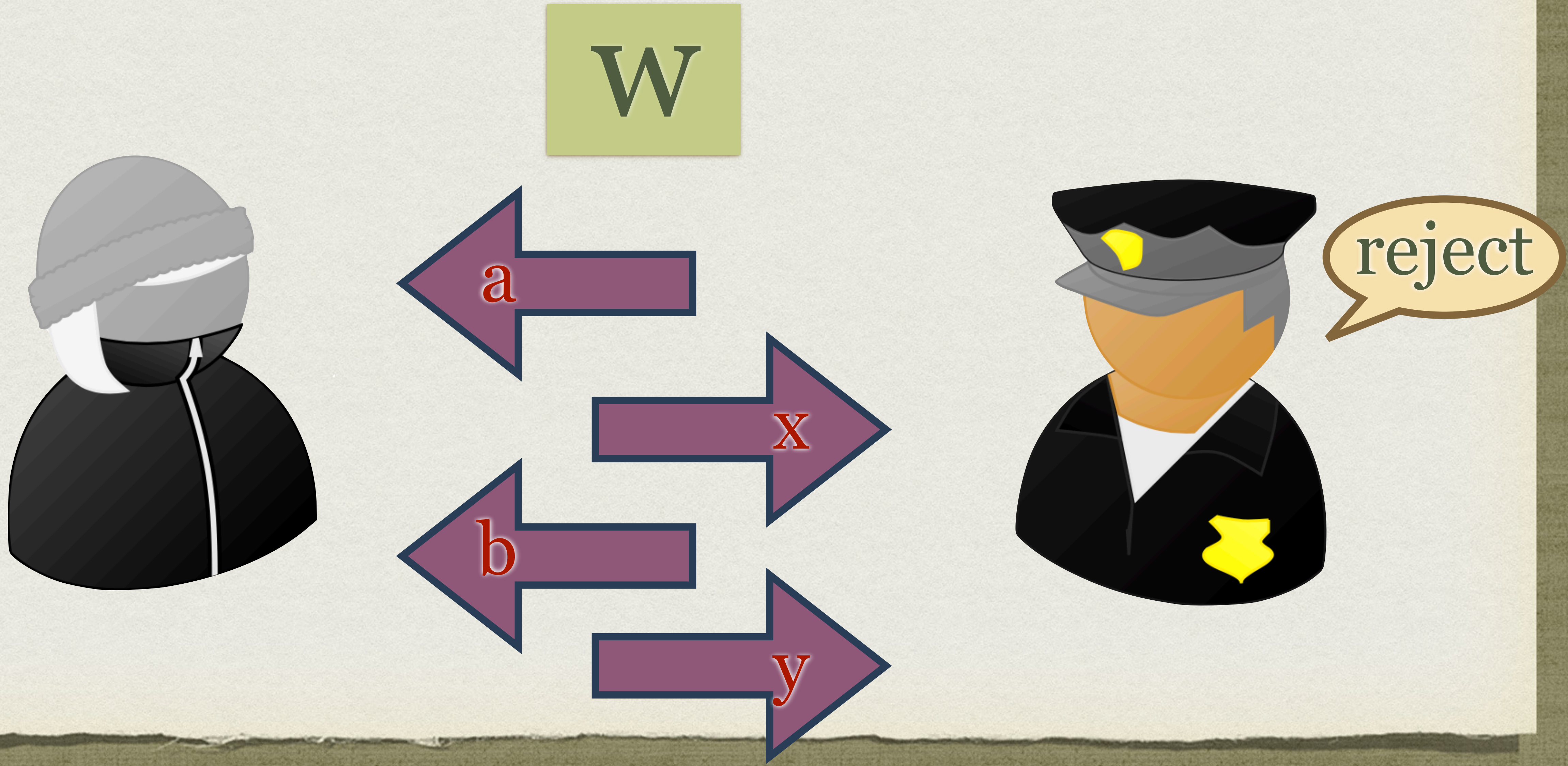


SOUNDNESS

$w \notin L$

∃ , ∃

and ∀ , $\forall w \notin L$, **Prob**[(:) accepts] $\leq \epsilon$



Goldwasser

Micali

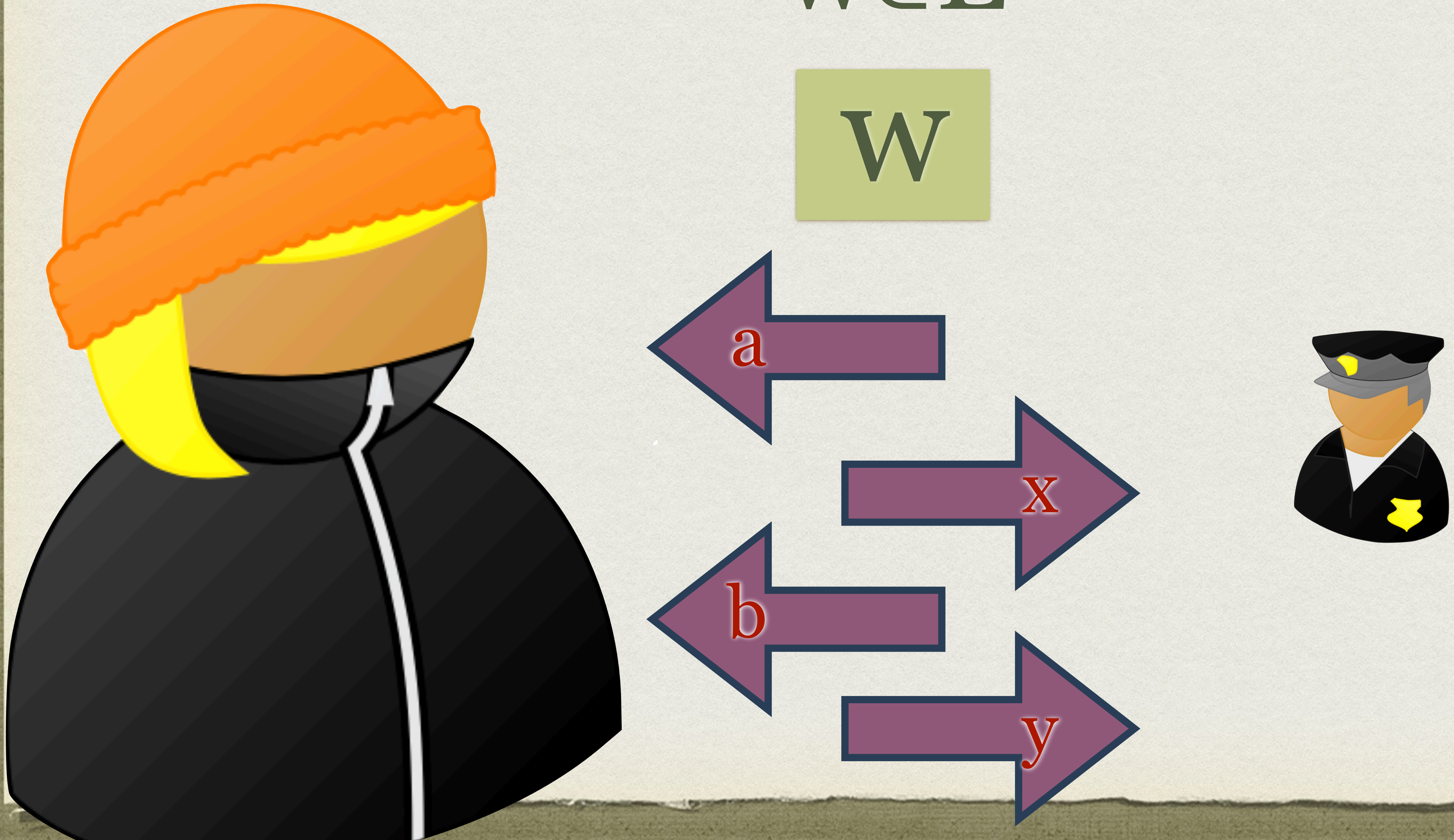
Rackoff

1985

$L \in IP$

$w \in L$

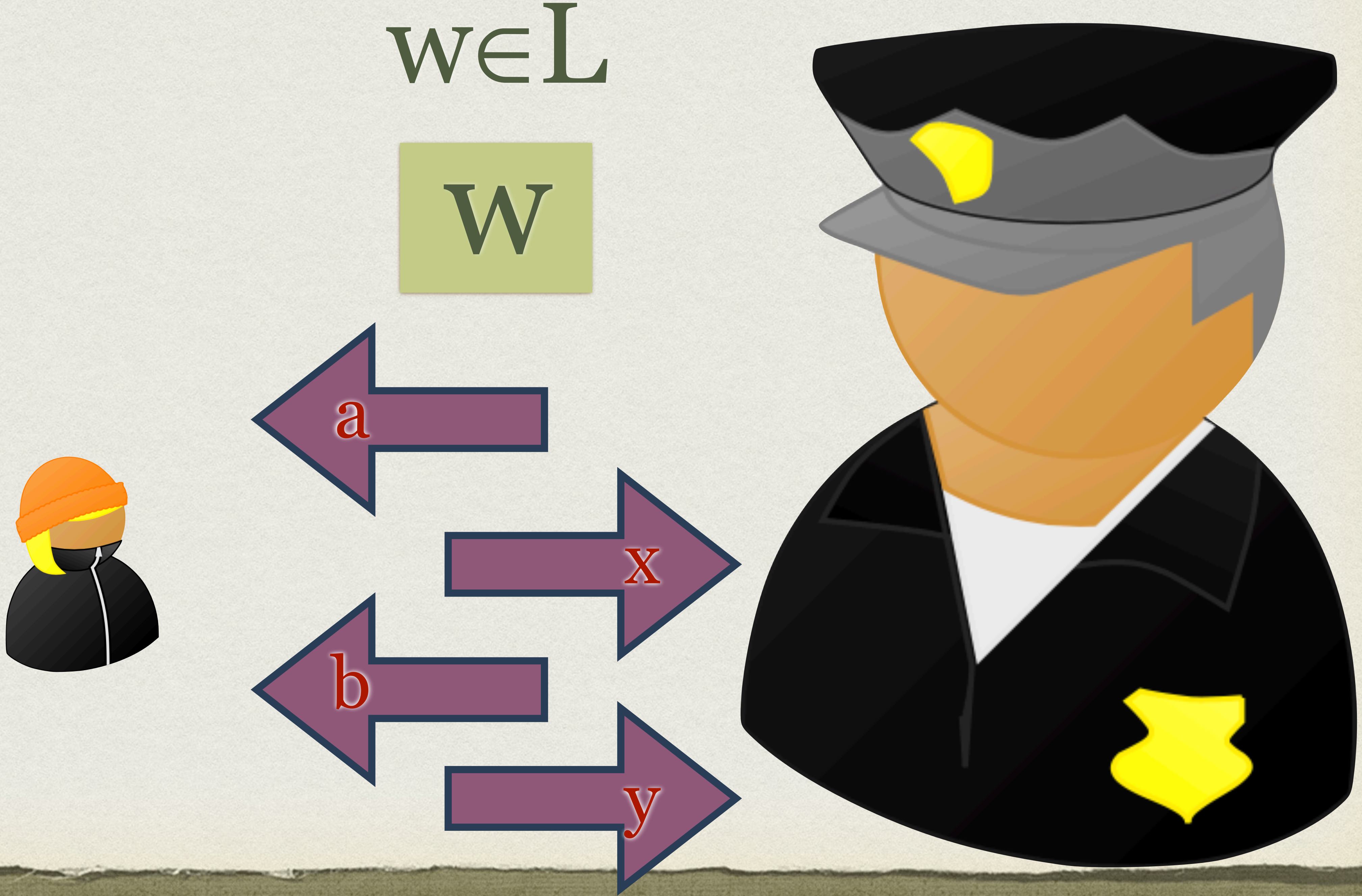
w



1986

$L \in IP$

$w \in L$

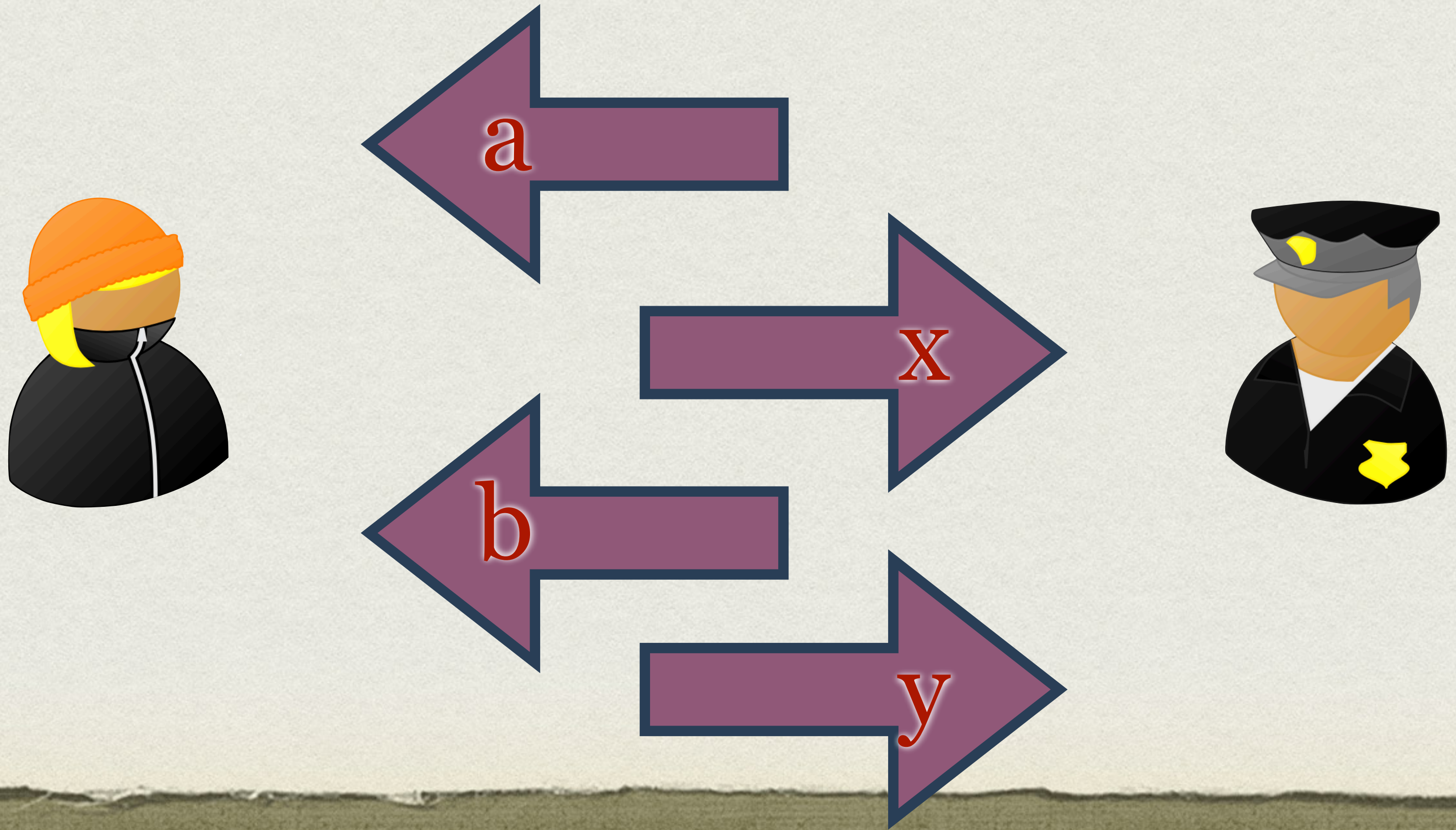


1986

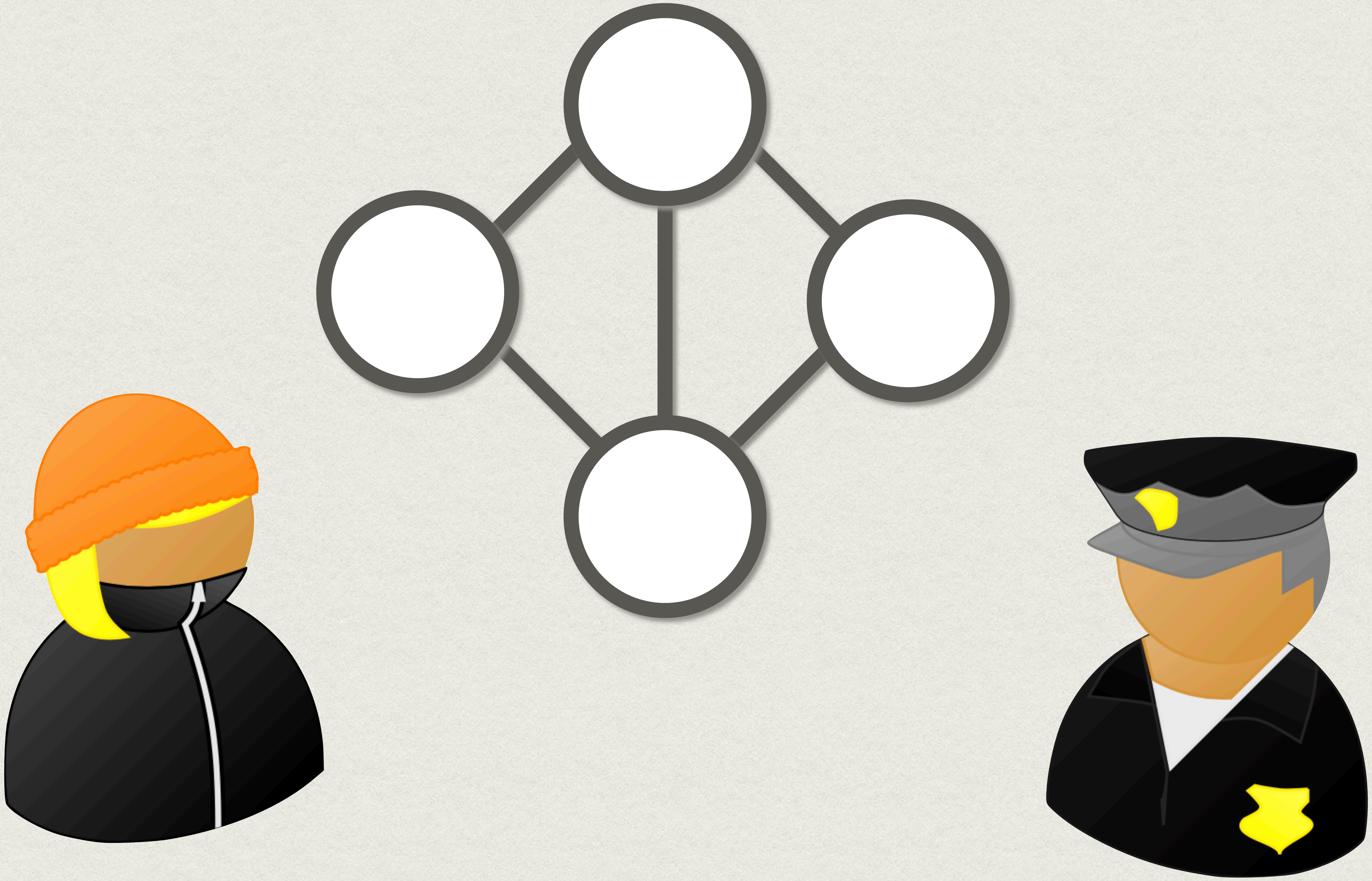
$L \in IP$

$w \in L$

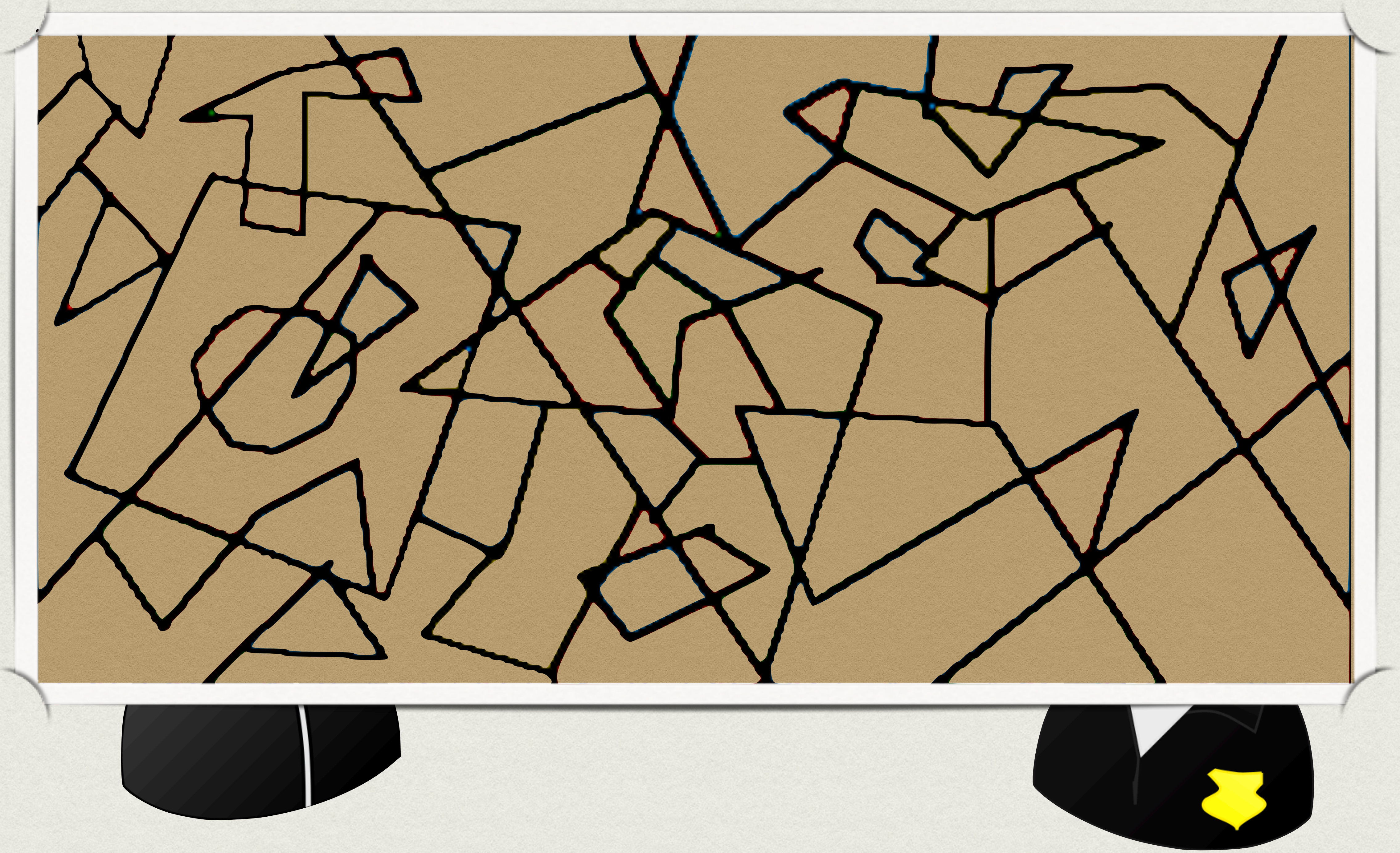
$\boxed{w}$



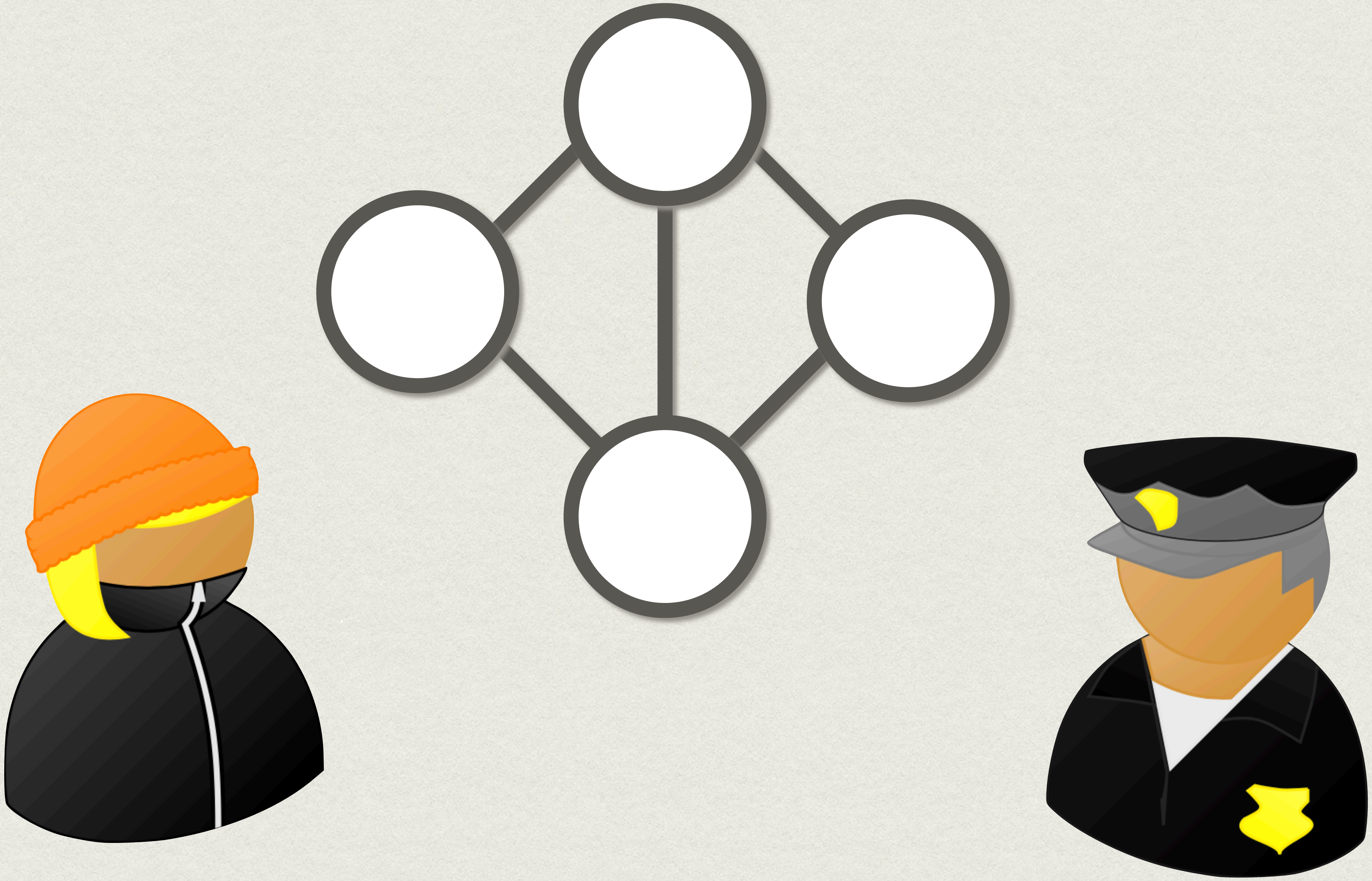
3-COL



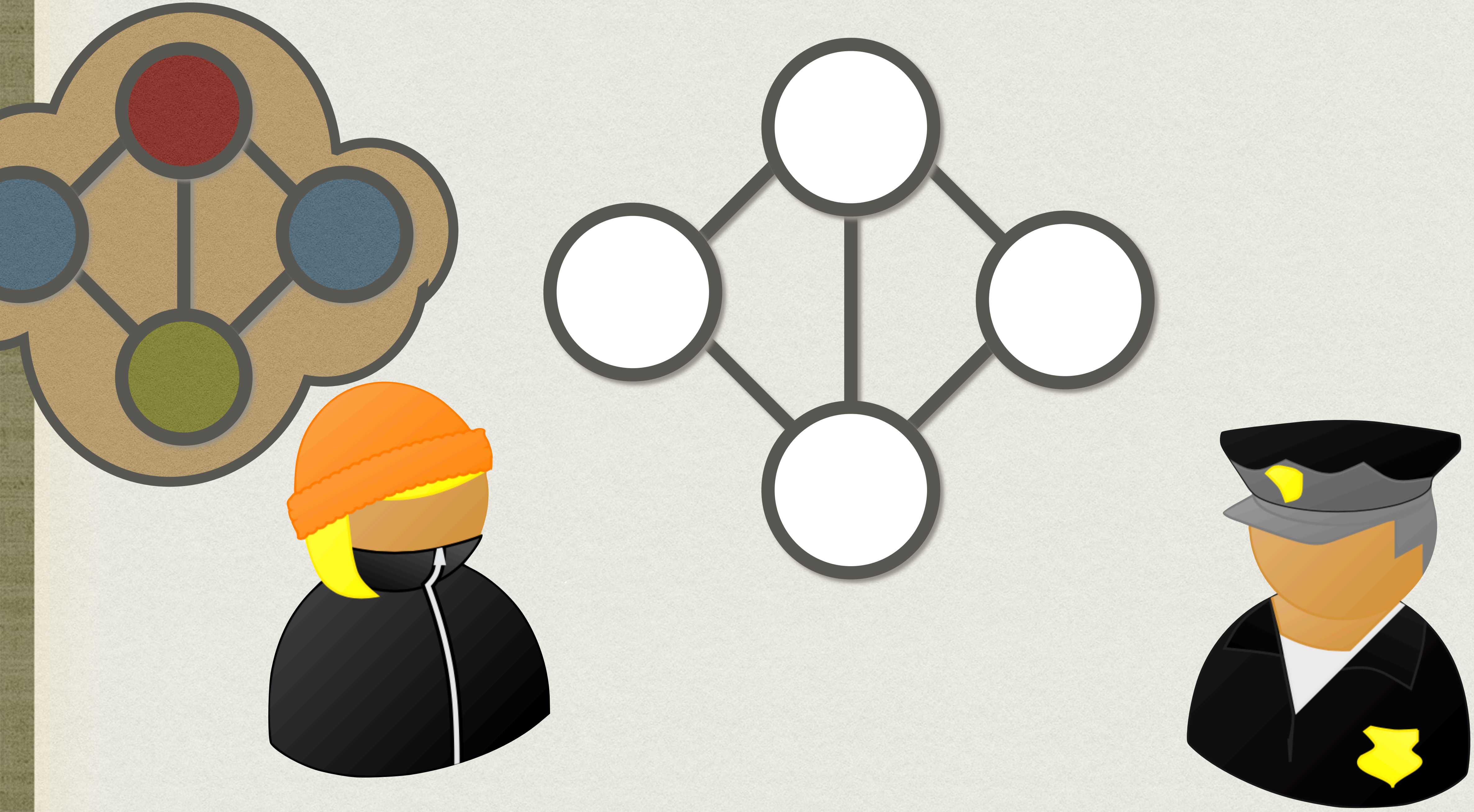
3-COL



3-COL

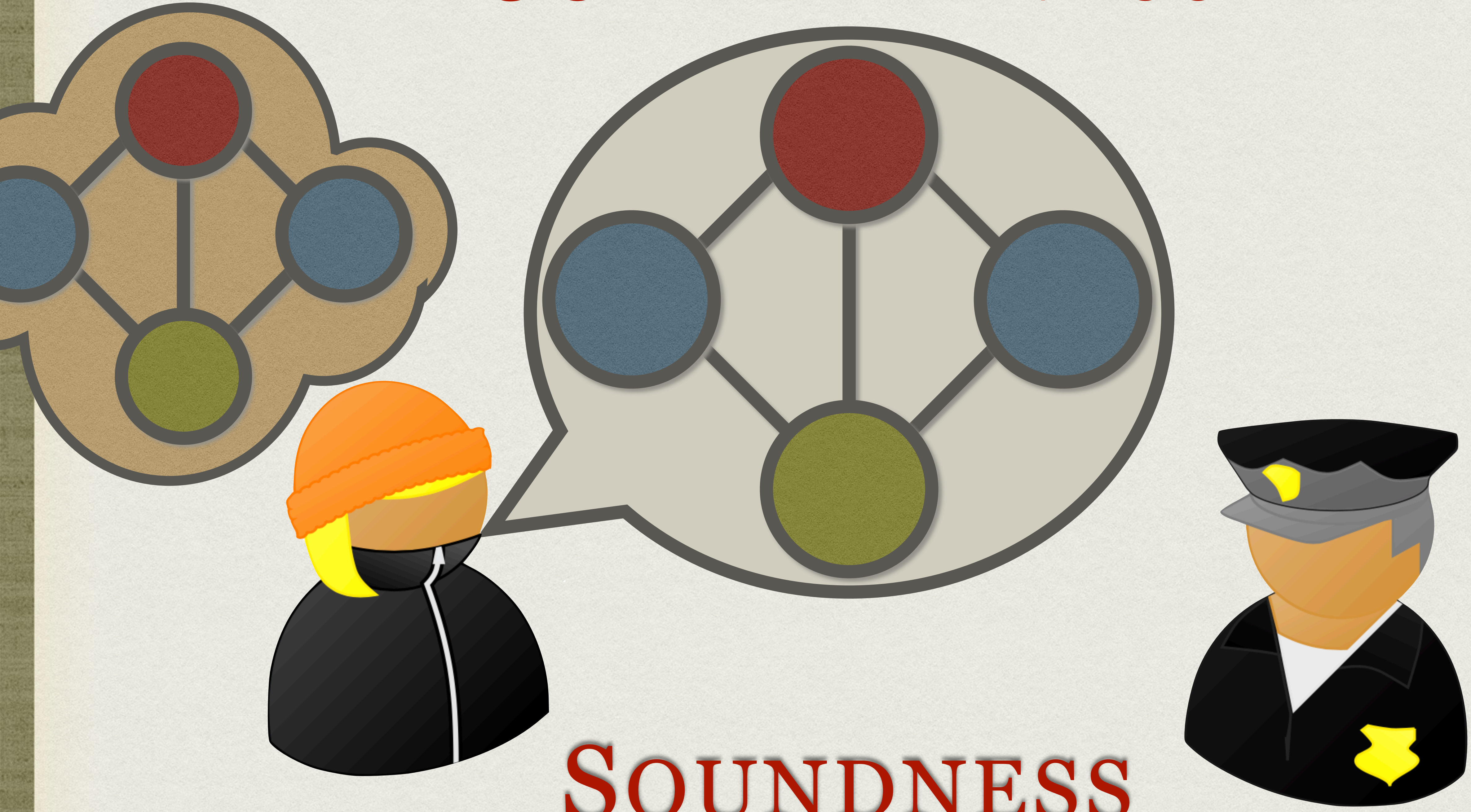


3-COL



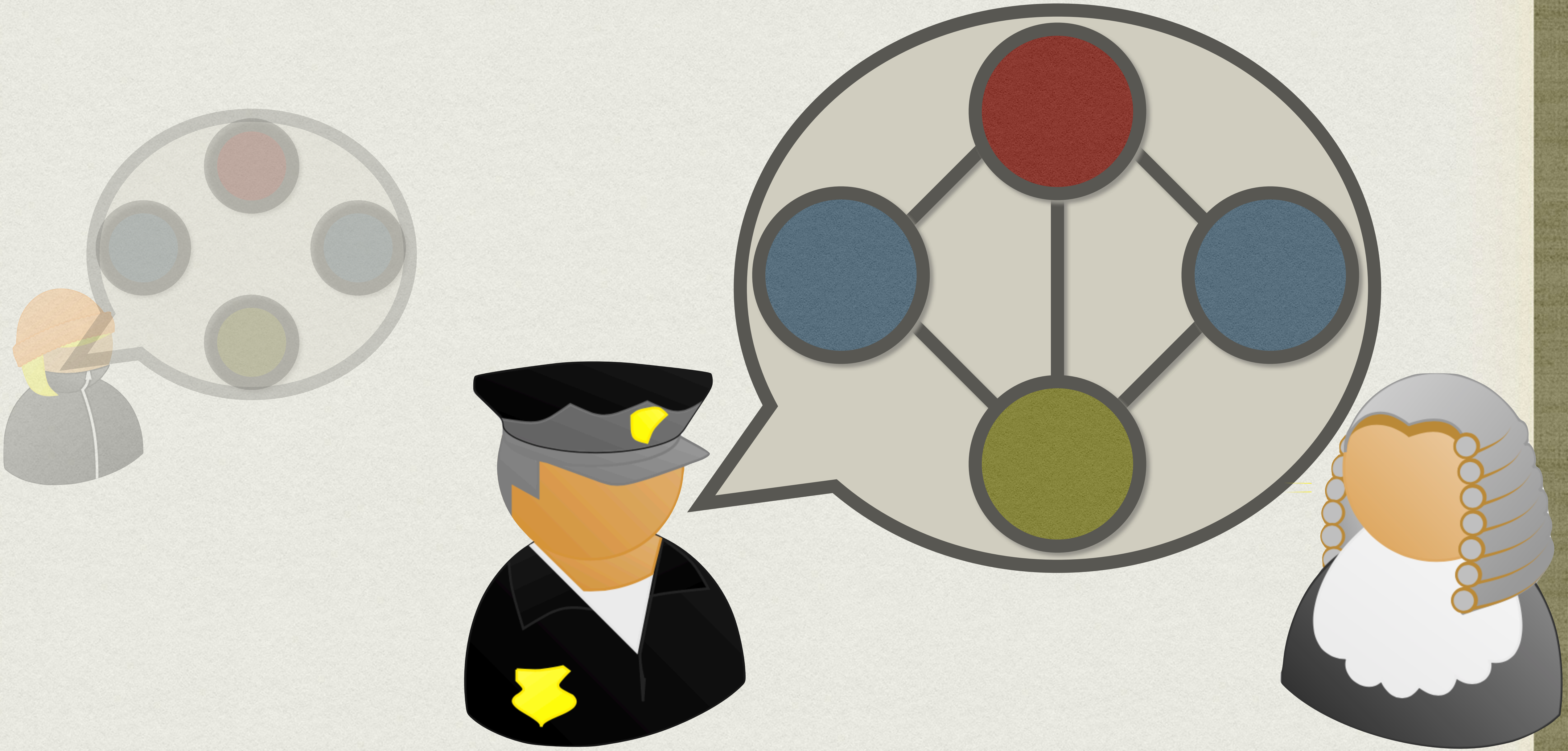
3-COL

COMPLETENESS



SOUNDNESS

3-COL



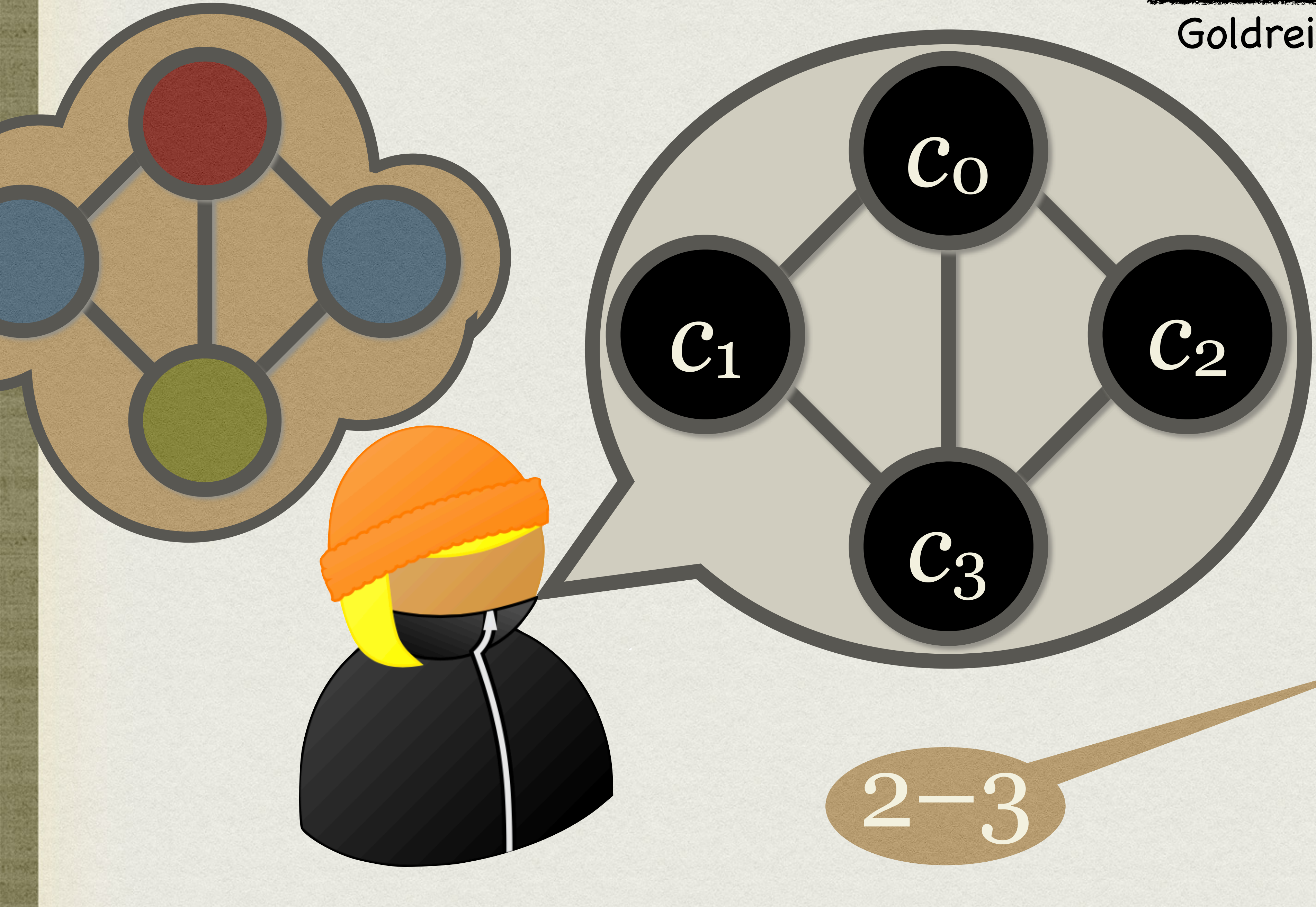
TRANSFERABLE

3-COL (86)

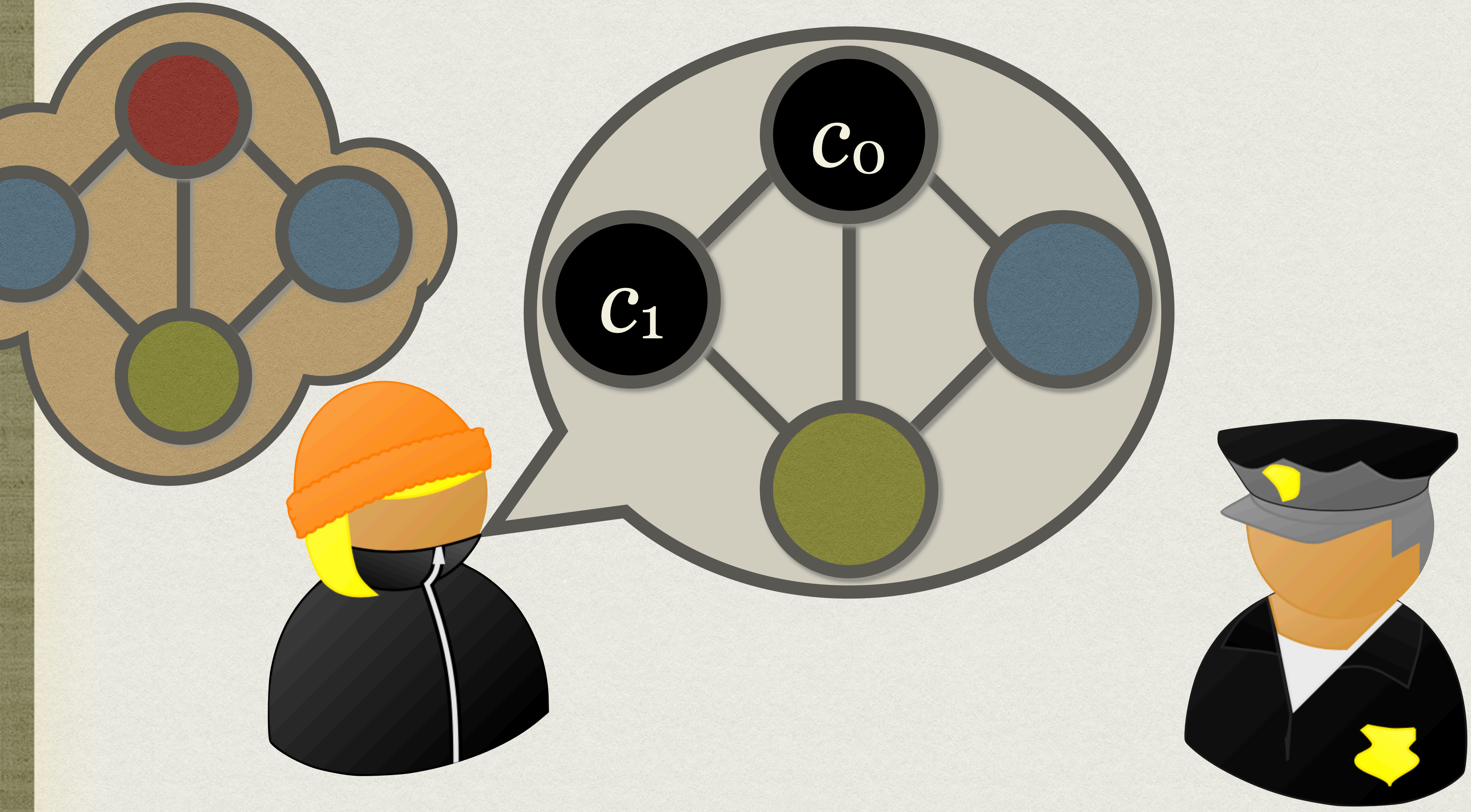
Goldreich

Micali

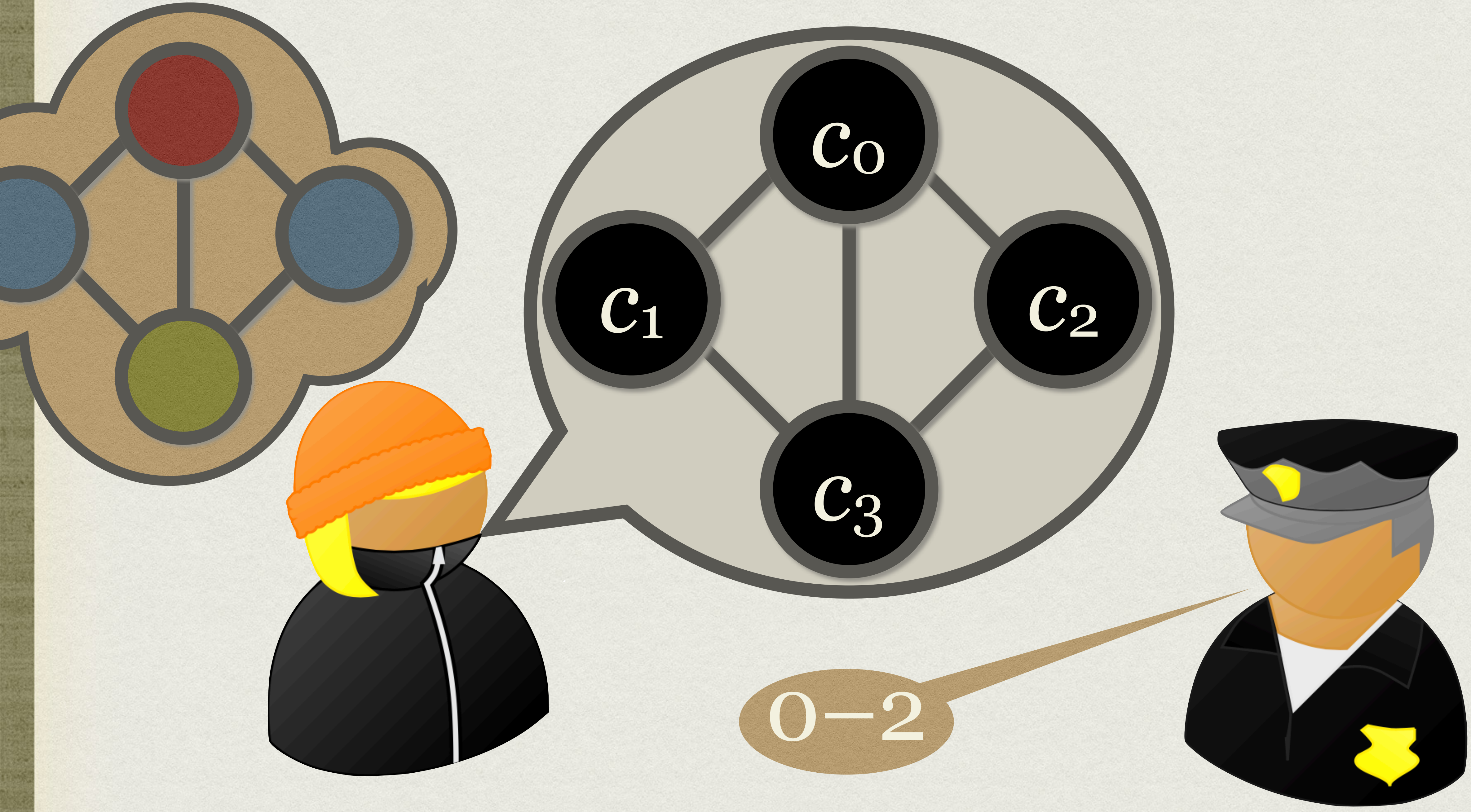
Wigderson



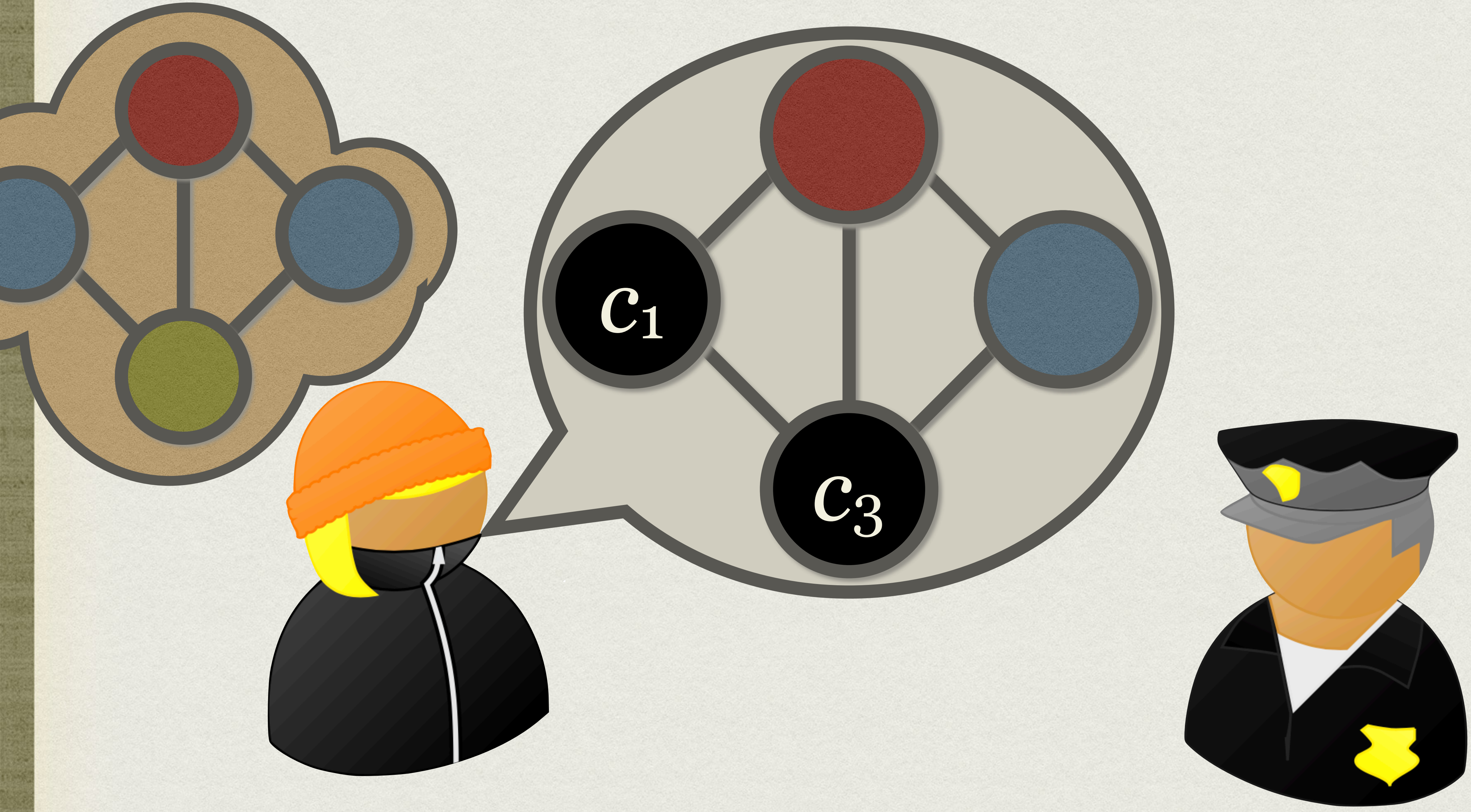
3-COL



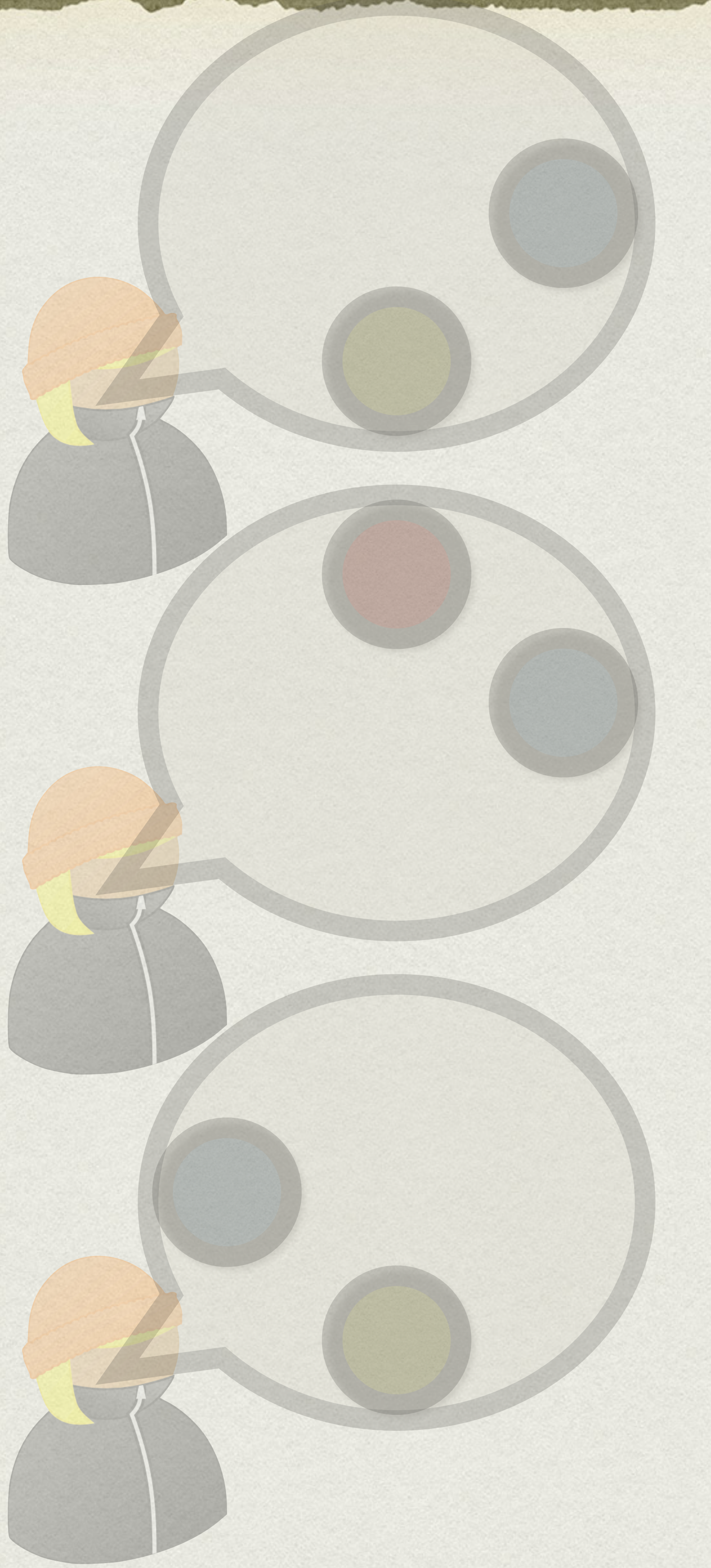
3-COL

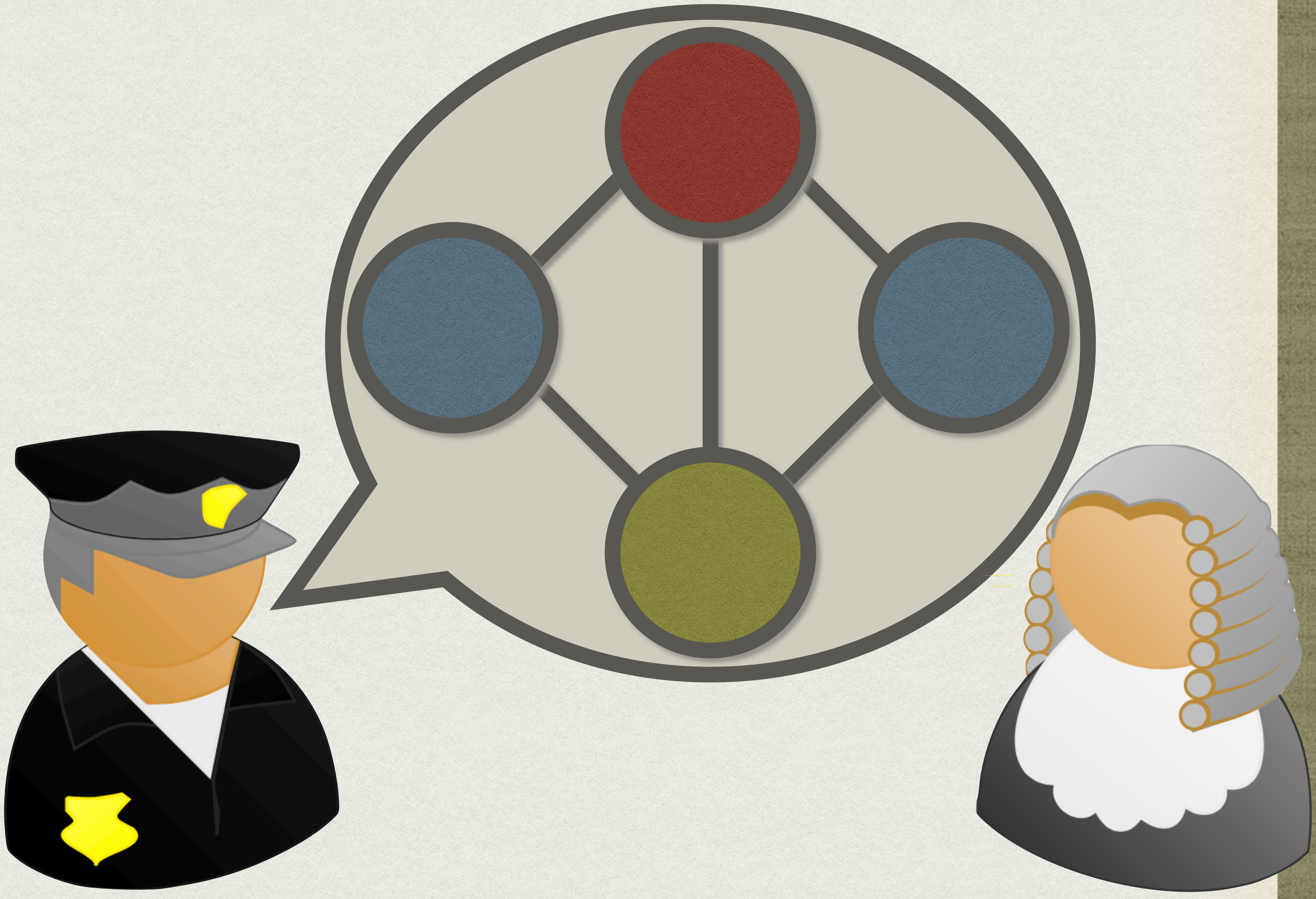


3-COL



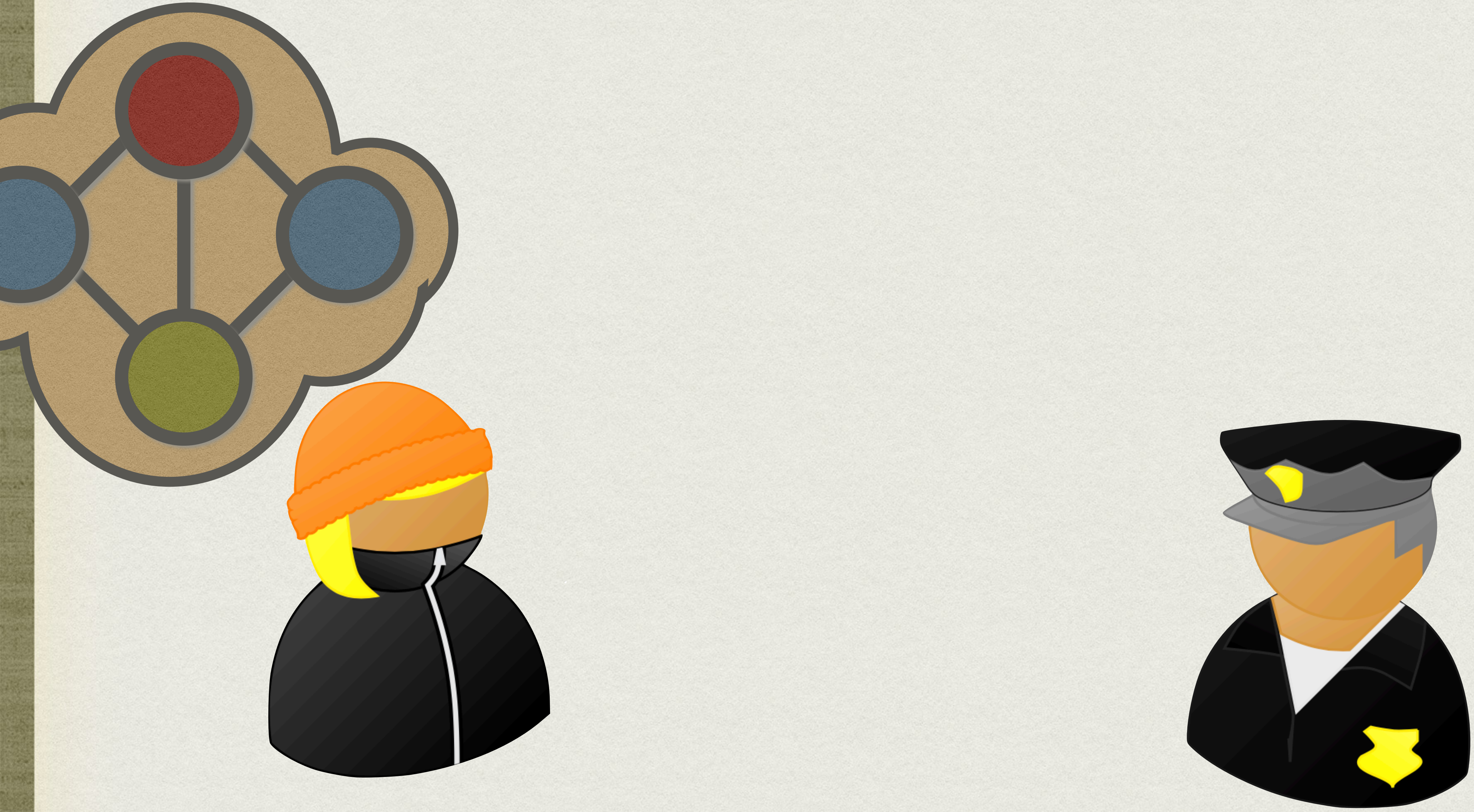
3-COL





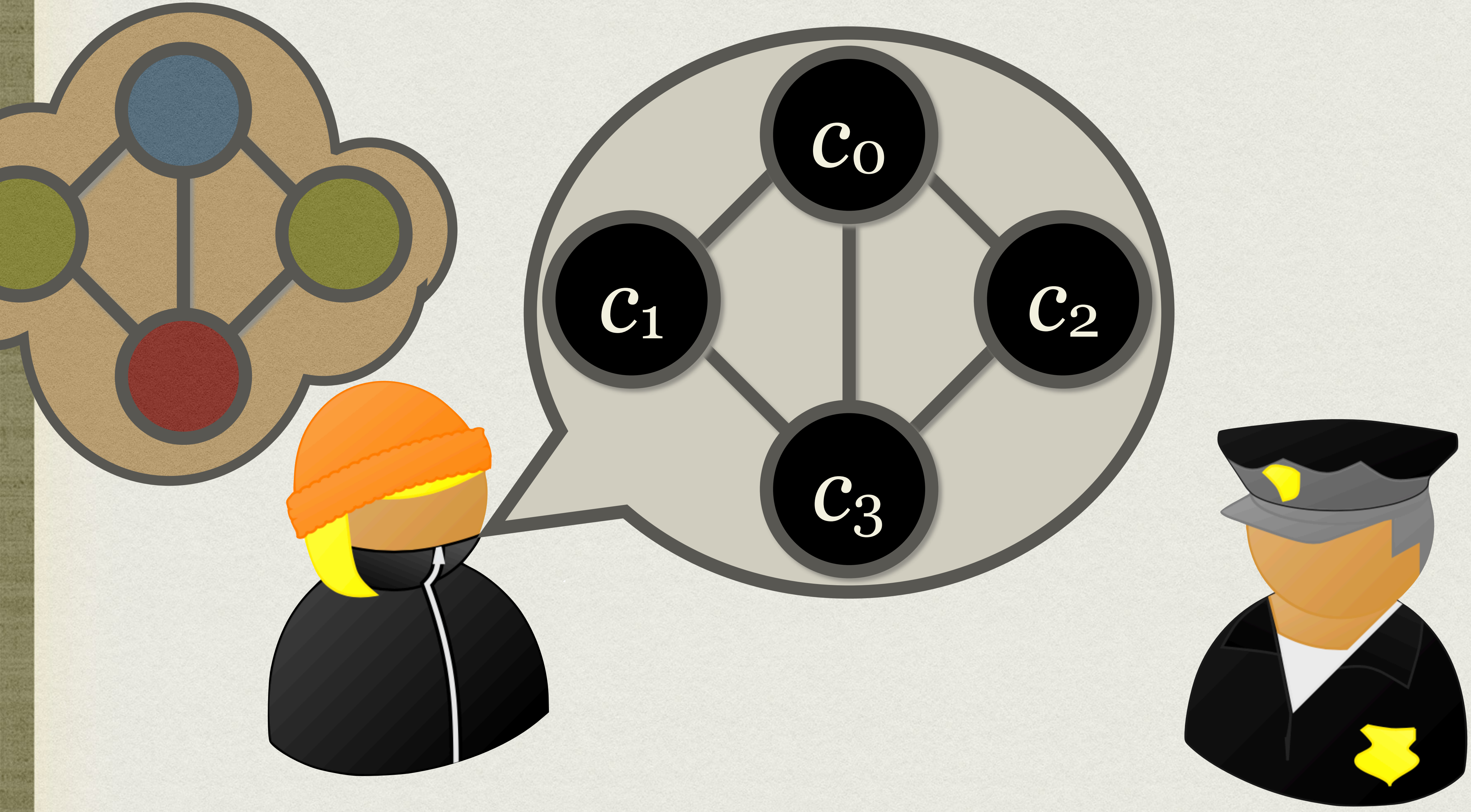
TRANSFERABLE

3-COL

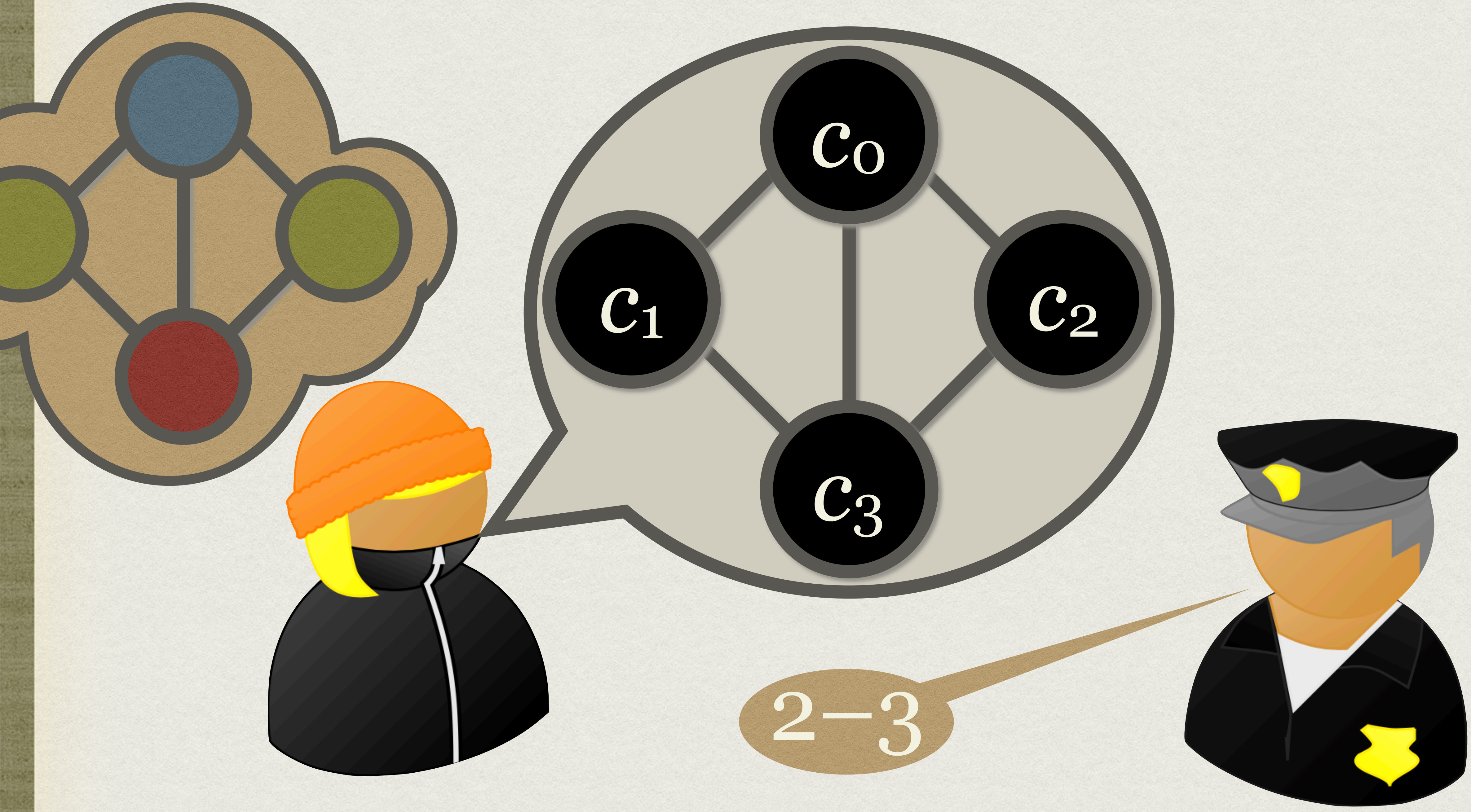


3-COL

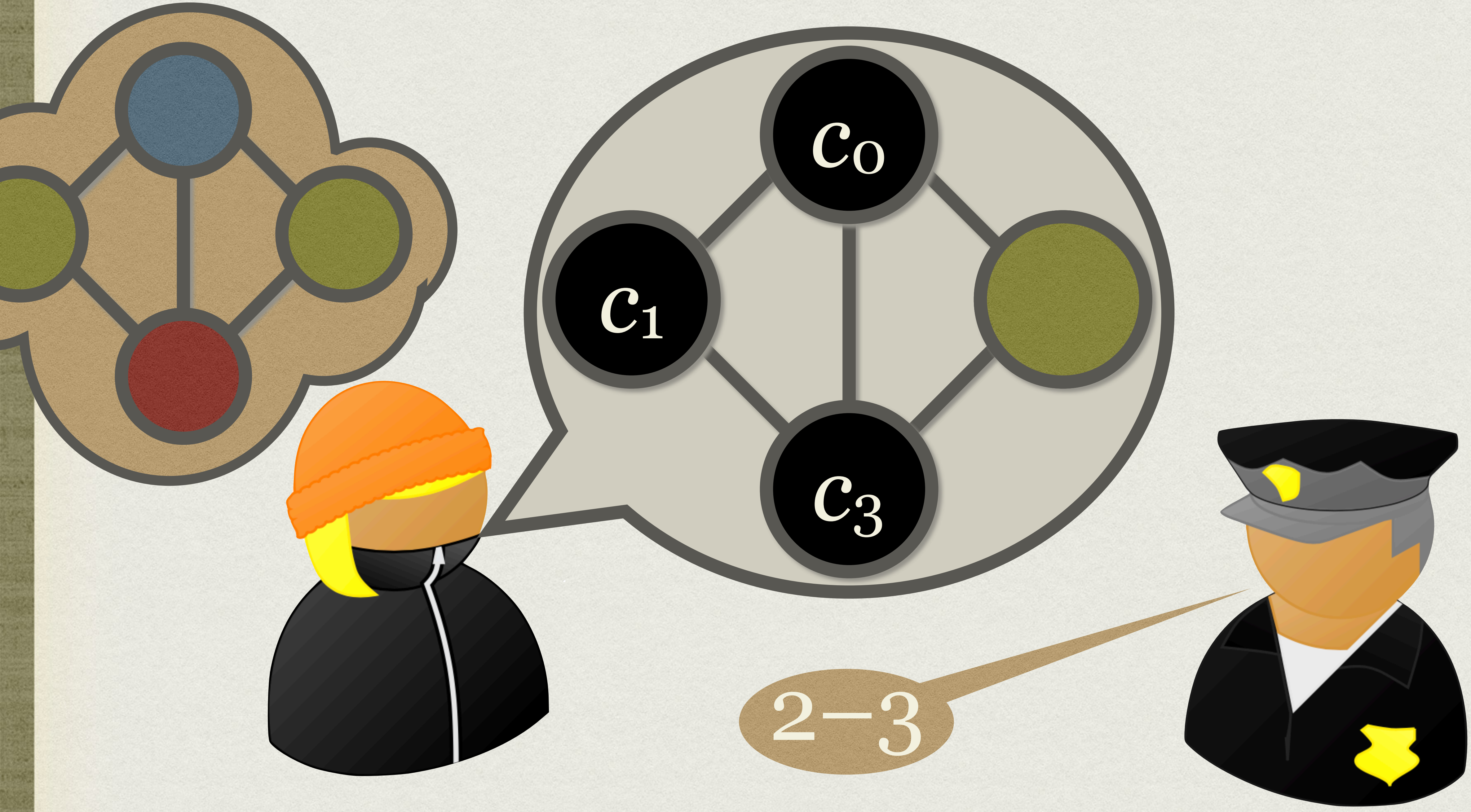
3-COL



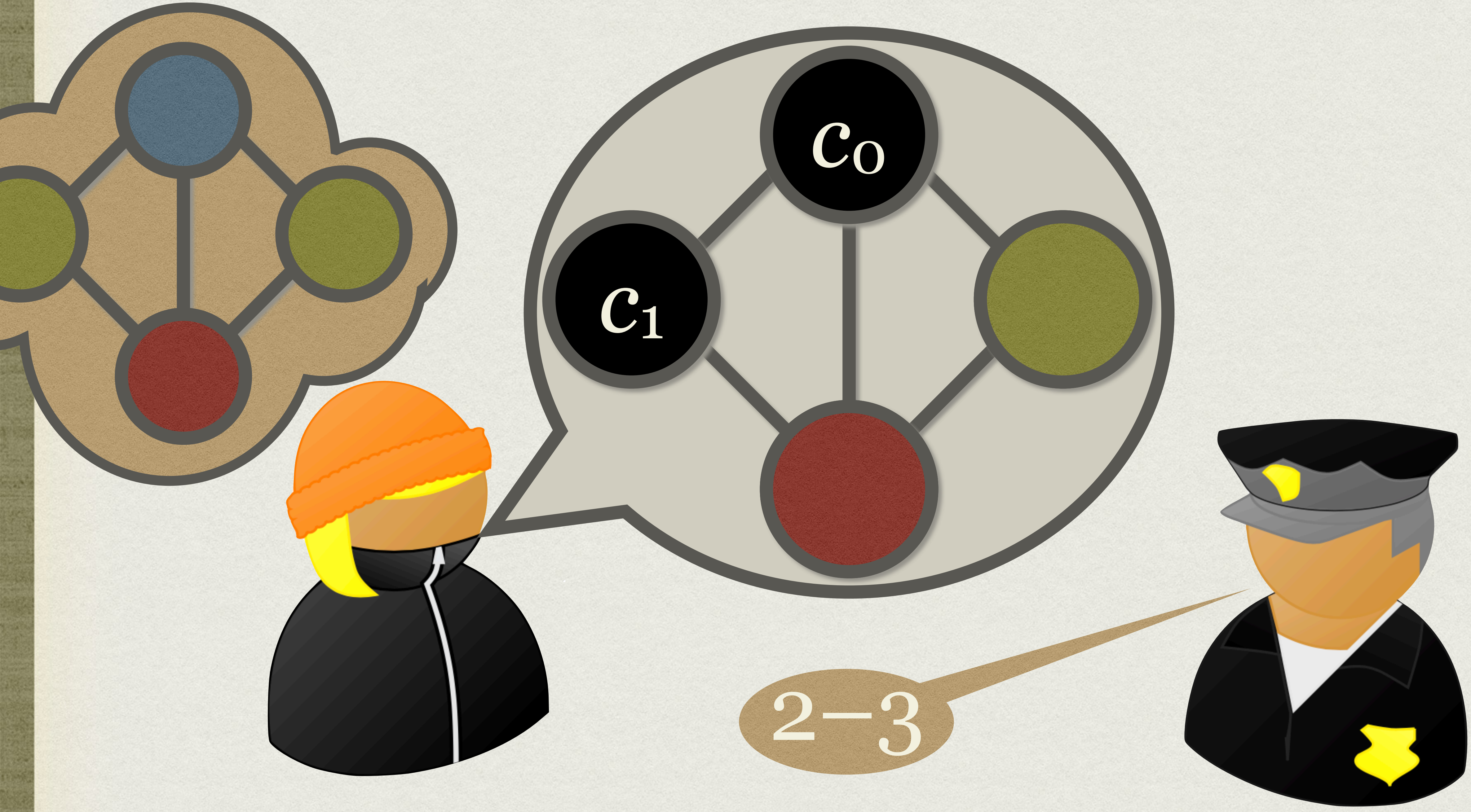
3-COL



3-COL

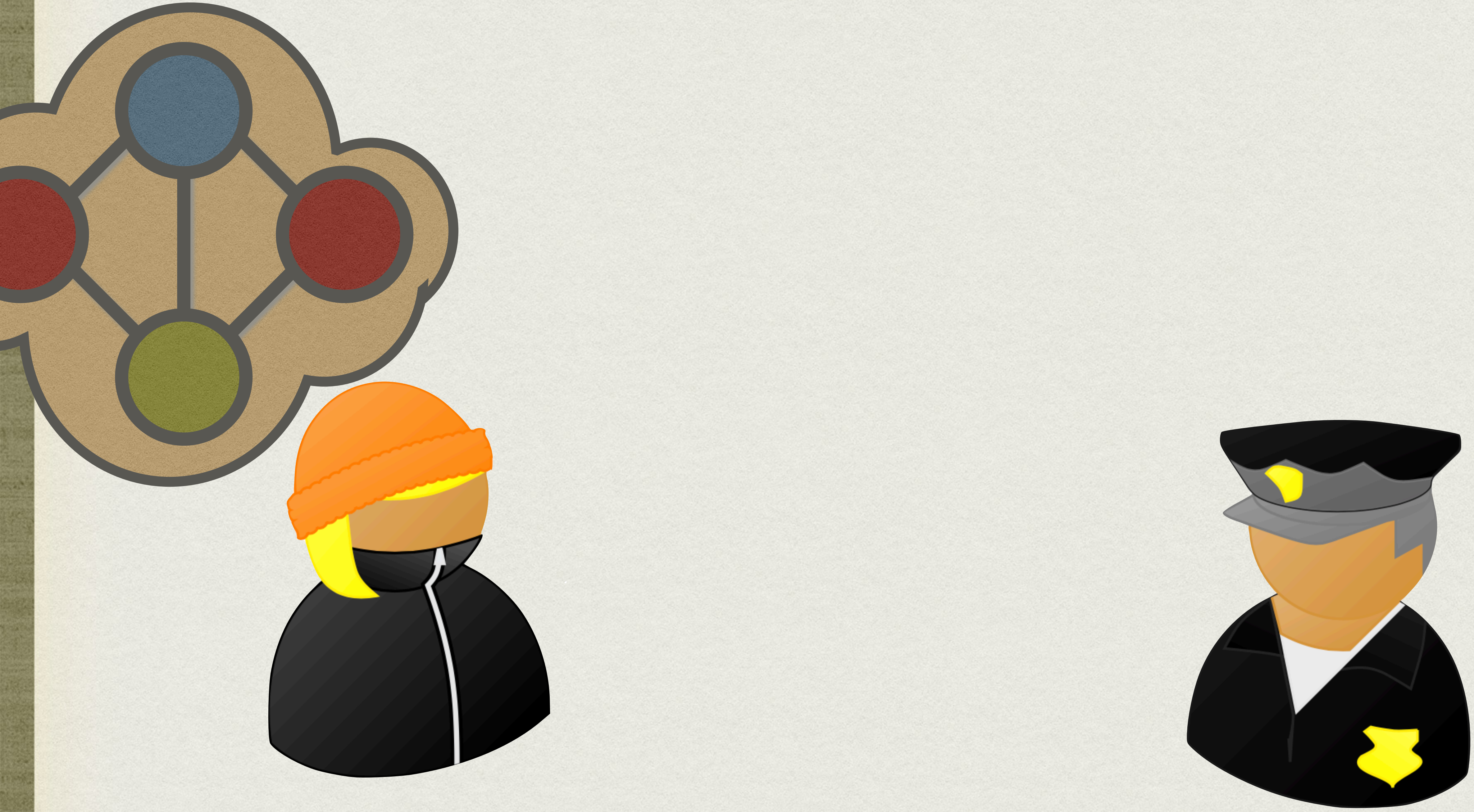


3-COL

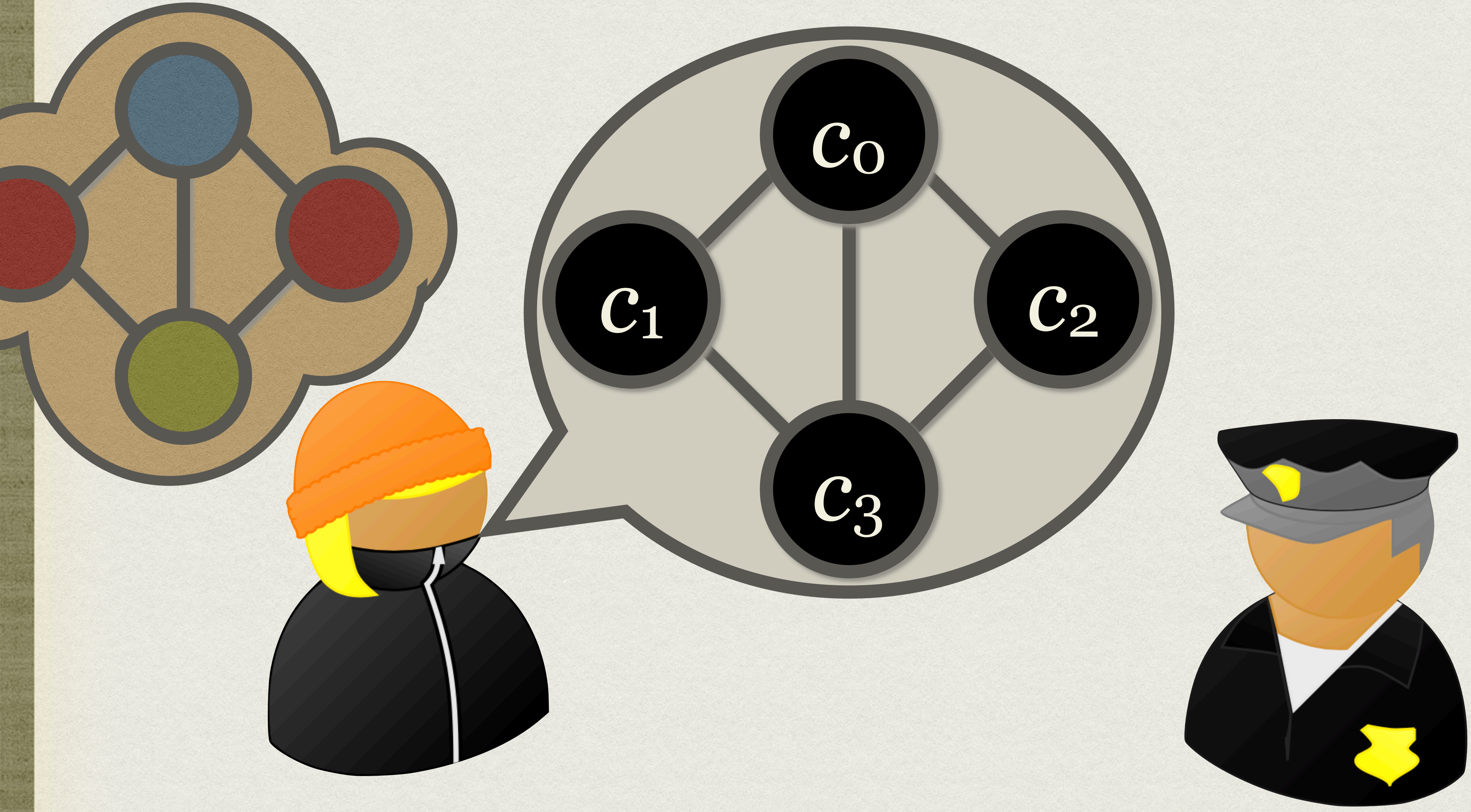


3-COL

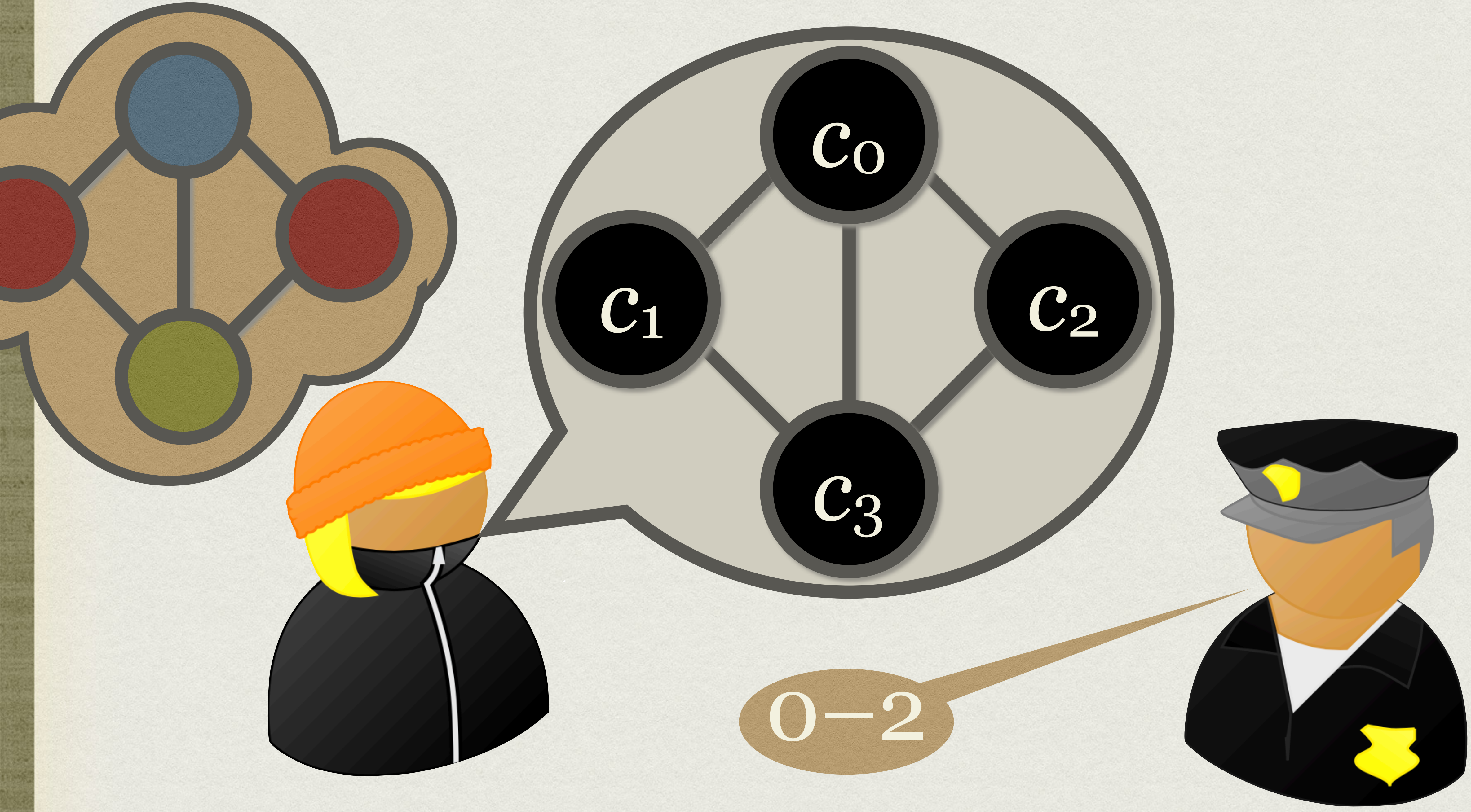
3-COL



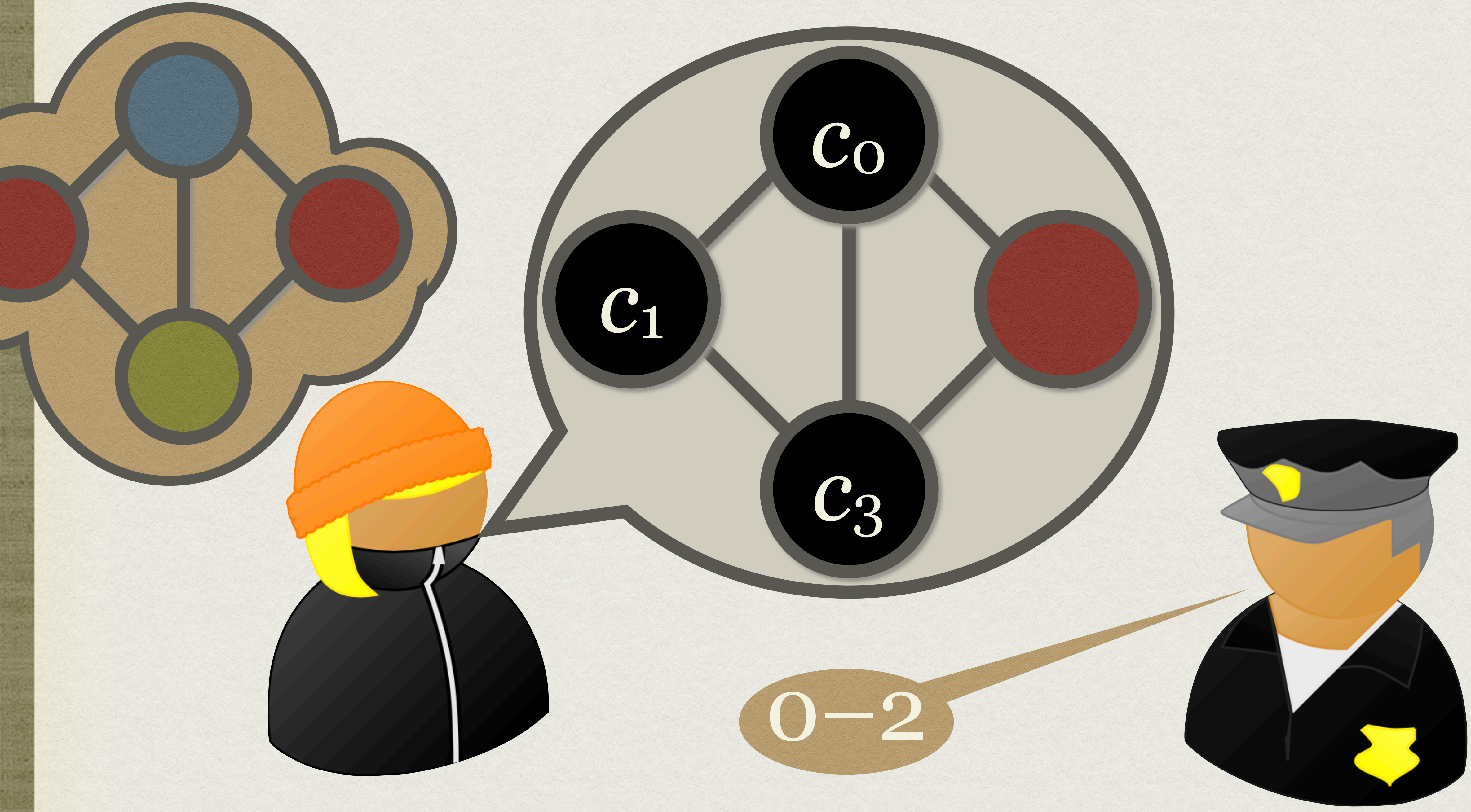
3-COL



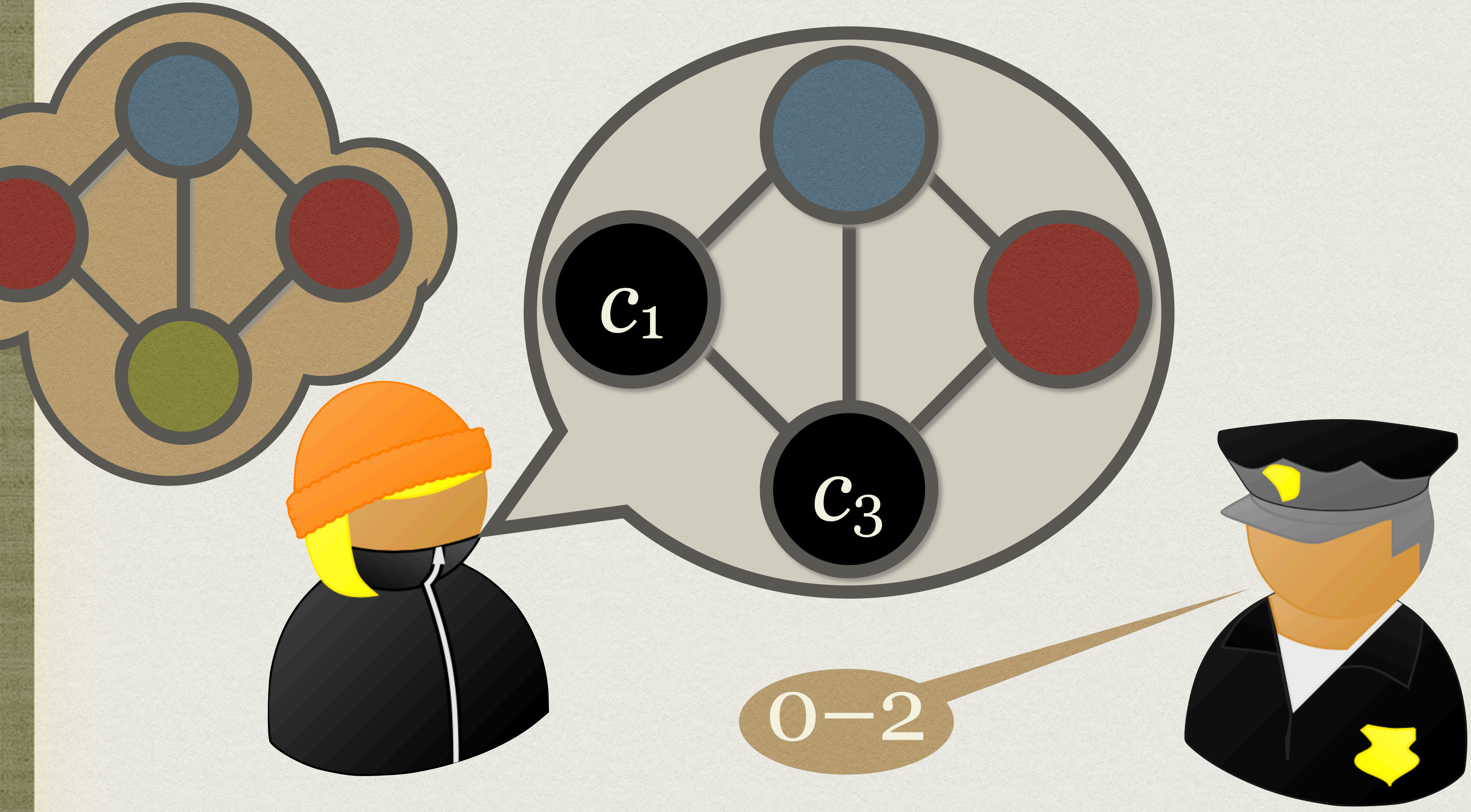
3-COL



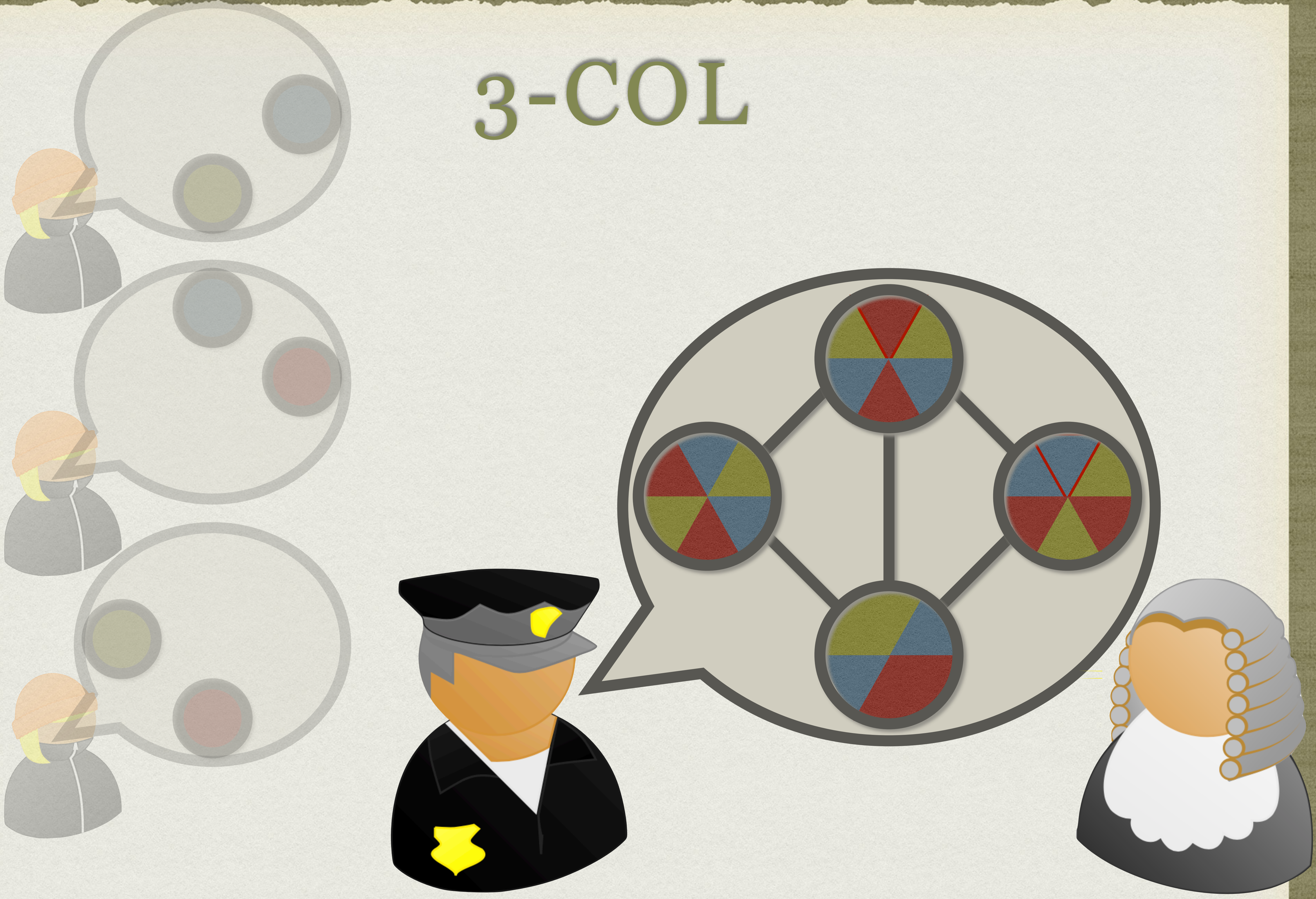
3-COL



3-COL



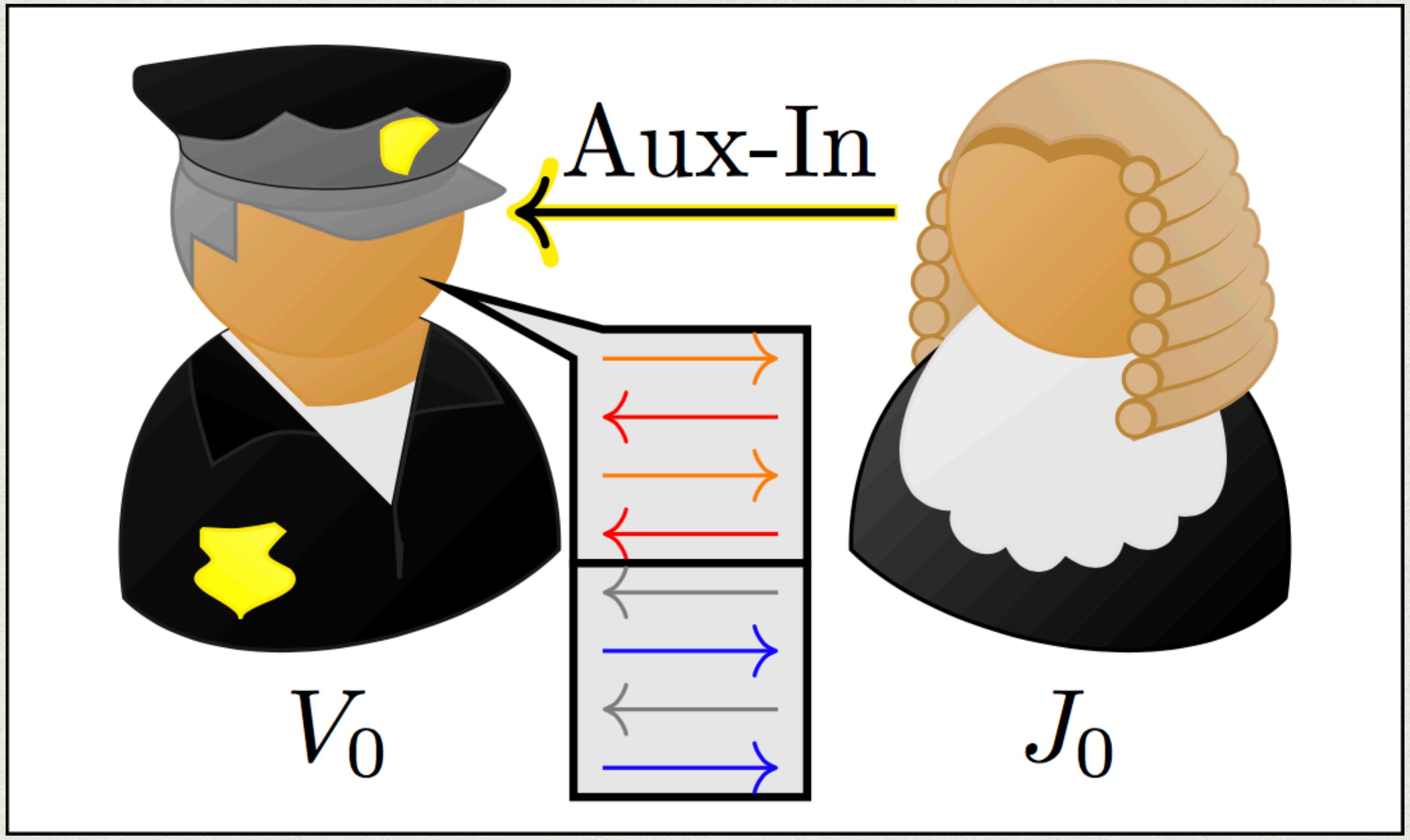
3-COL



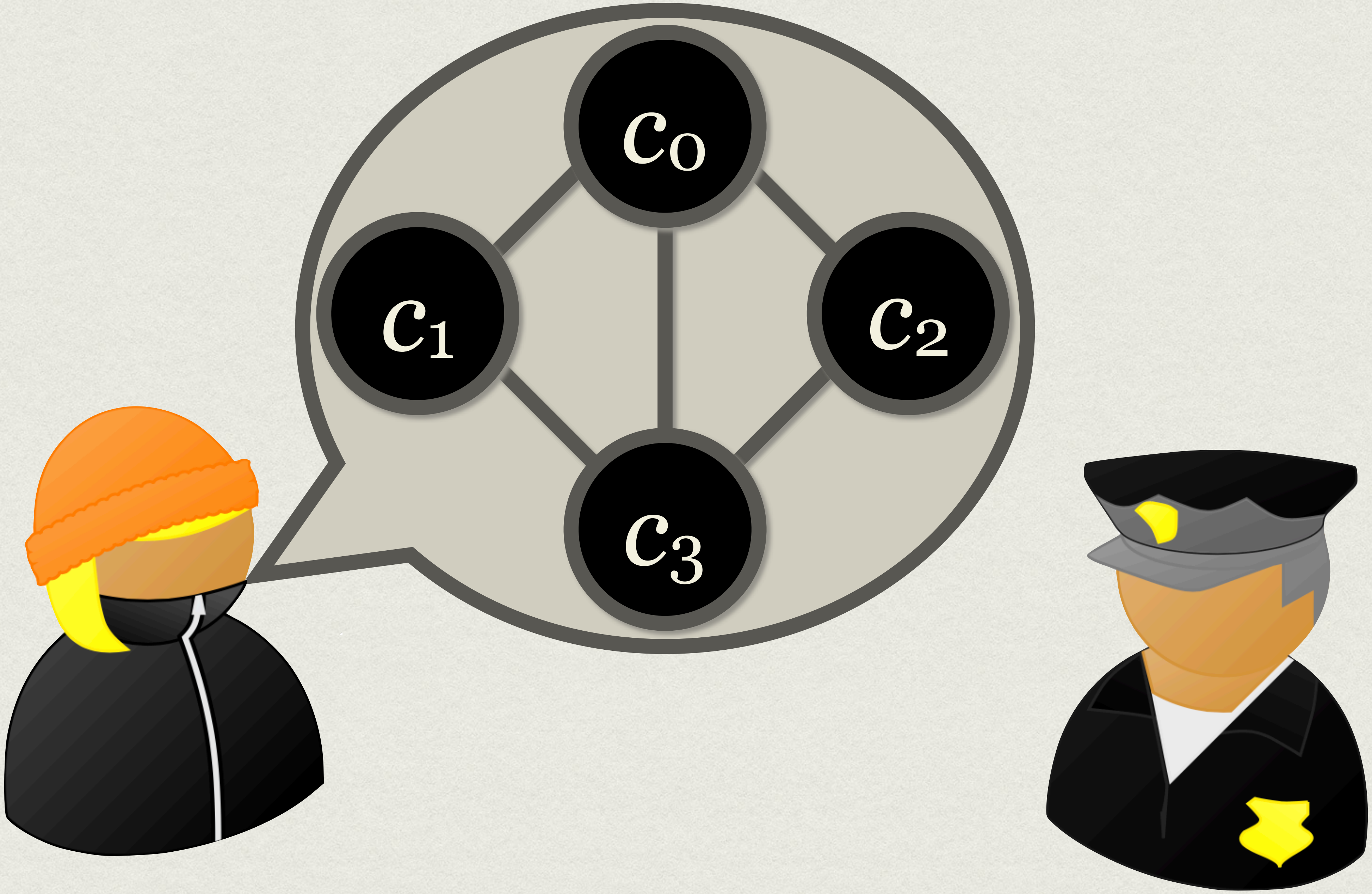
NOT TRANSFERABLE !

ZERO-KNOWLEDGE

∋ NOT TRANSFERABLE

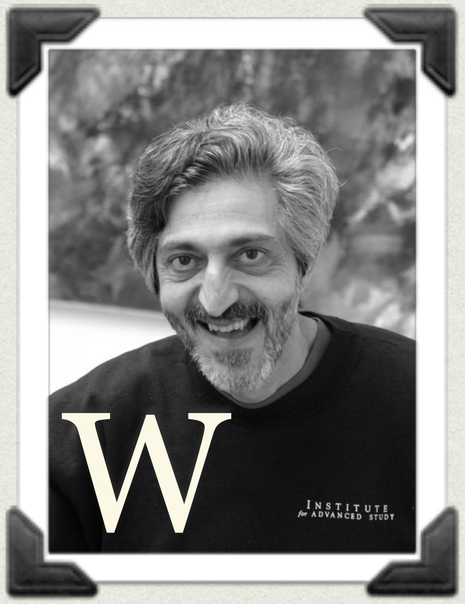


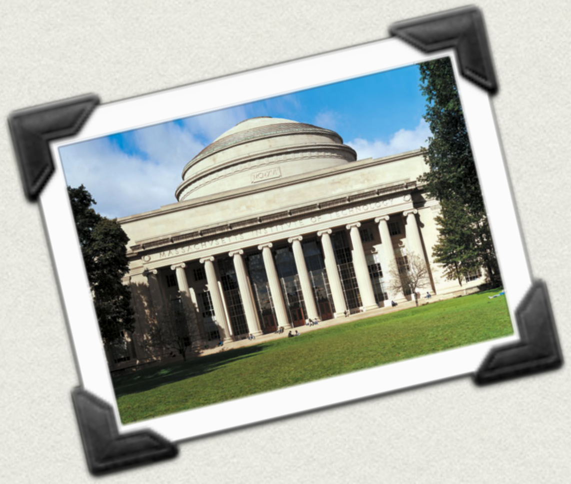
COMMITMENTS ??



INTRODUCTION

(ZK)MIPs



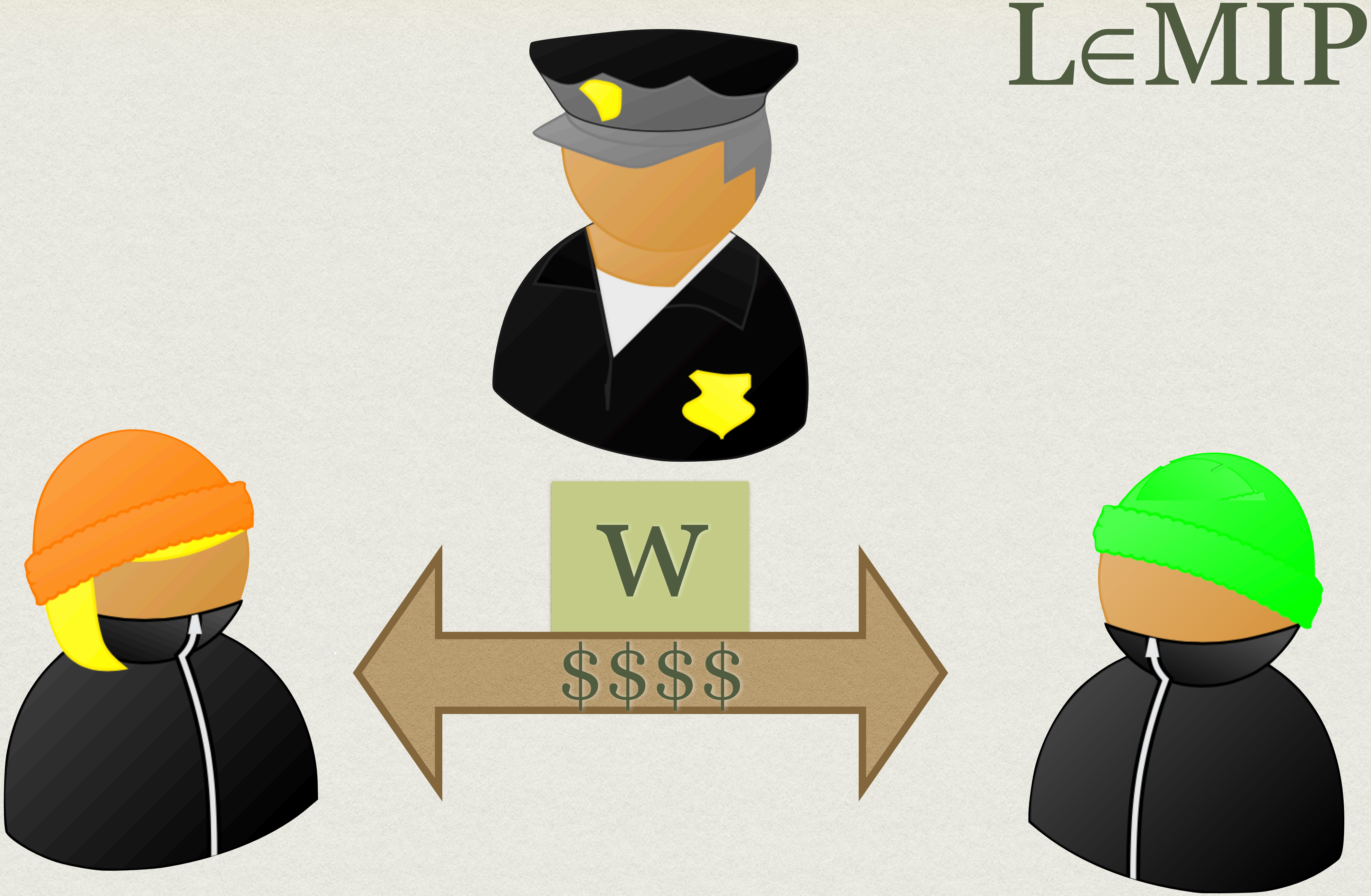


‘88

BGKW88

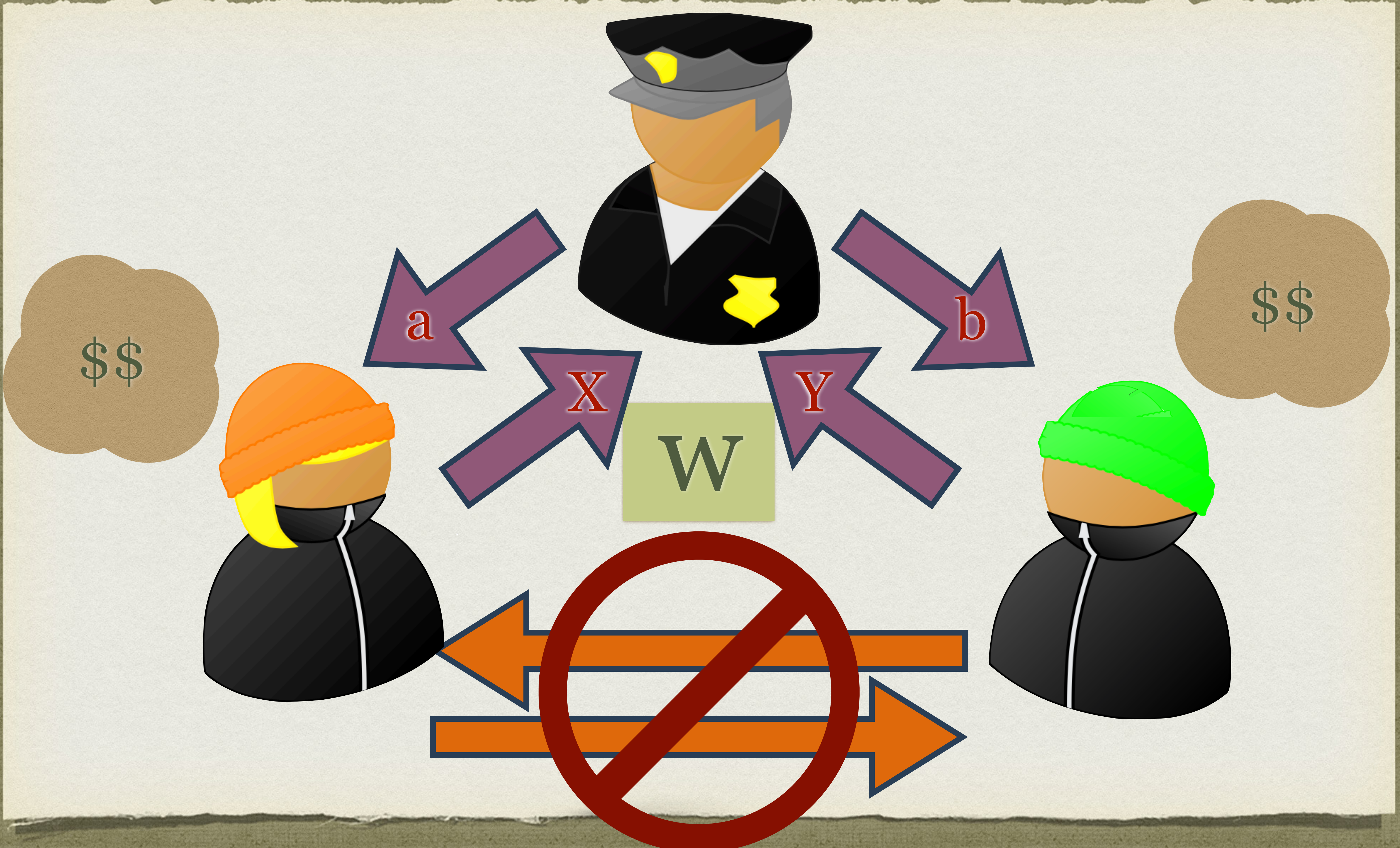
BGKW88

$L \in \mathrm{MIP}$



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

Prob[(👤:👮:👤) accepts] $\geq 1 - \epsilon$



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

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

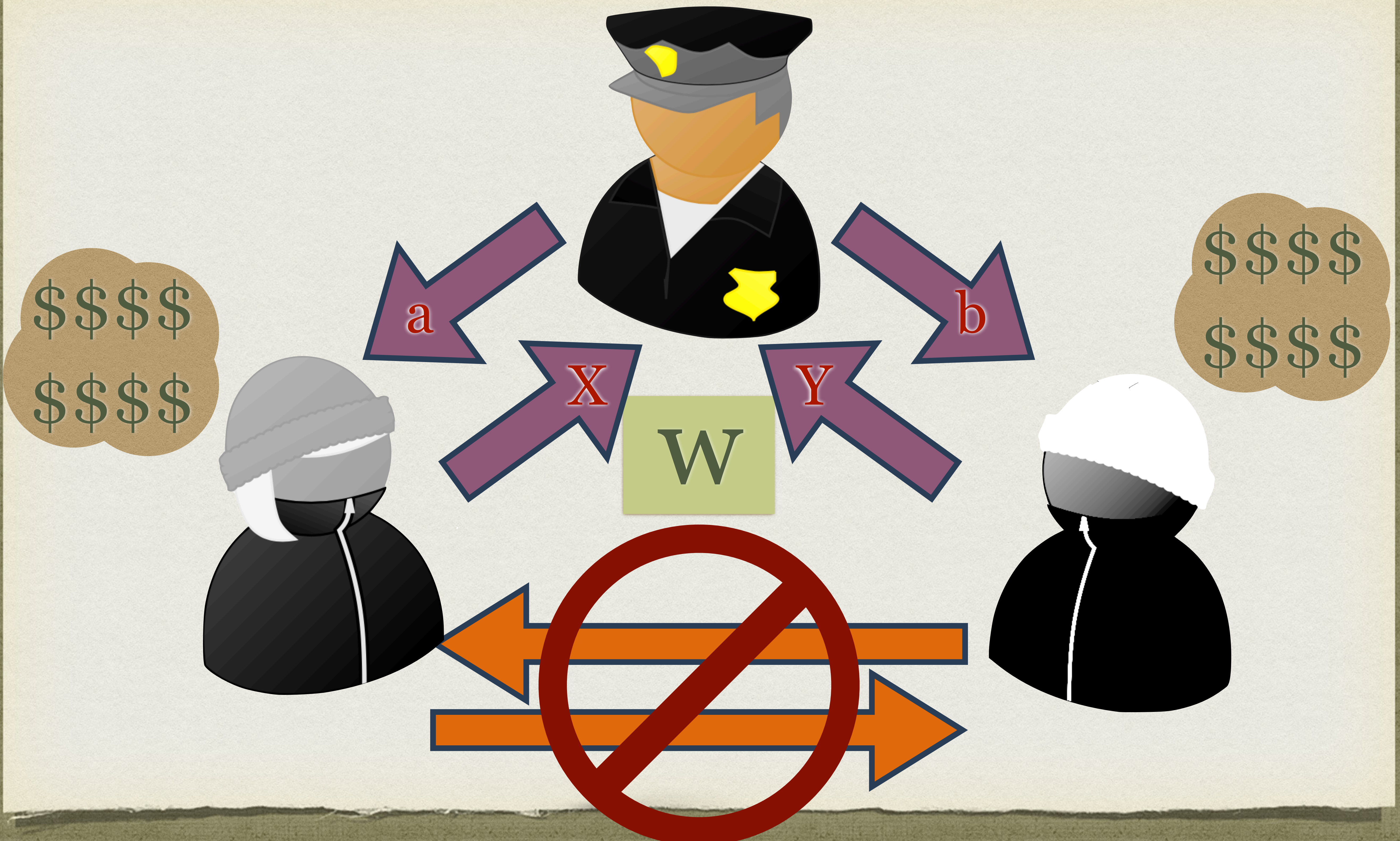
$\exists$ 👮, $\exists$ 👤, 👤, $\forall w \in L$,

Prob[(👤:👮:👤) accepts] $\geq 1 - \epsilon$

∃👮, ∃

and ∀ 👤, 👤, ∀$w \notin L$,

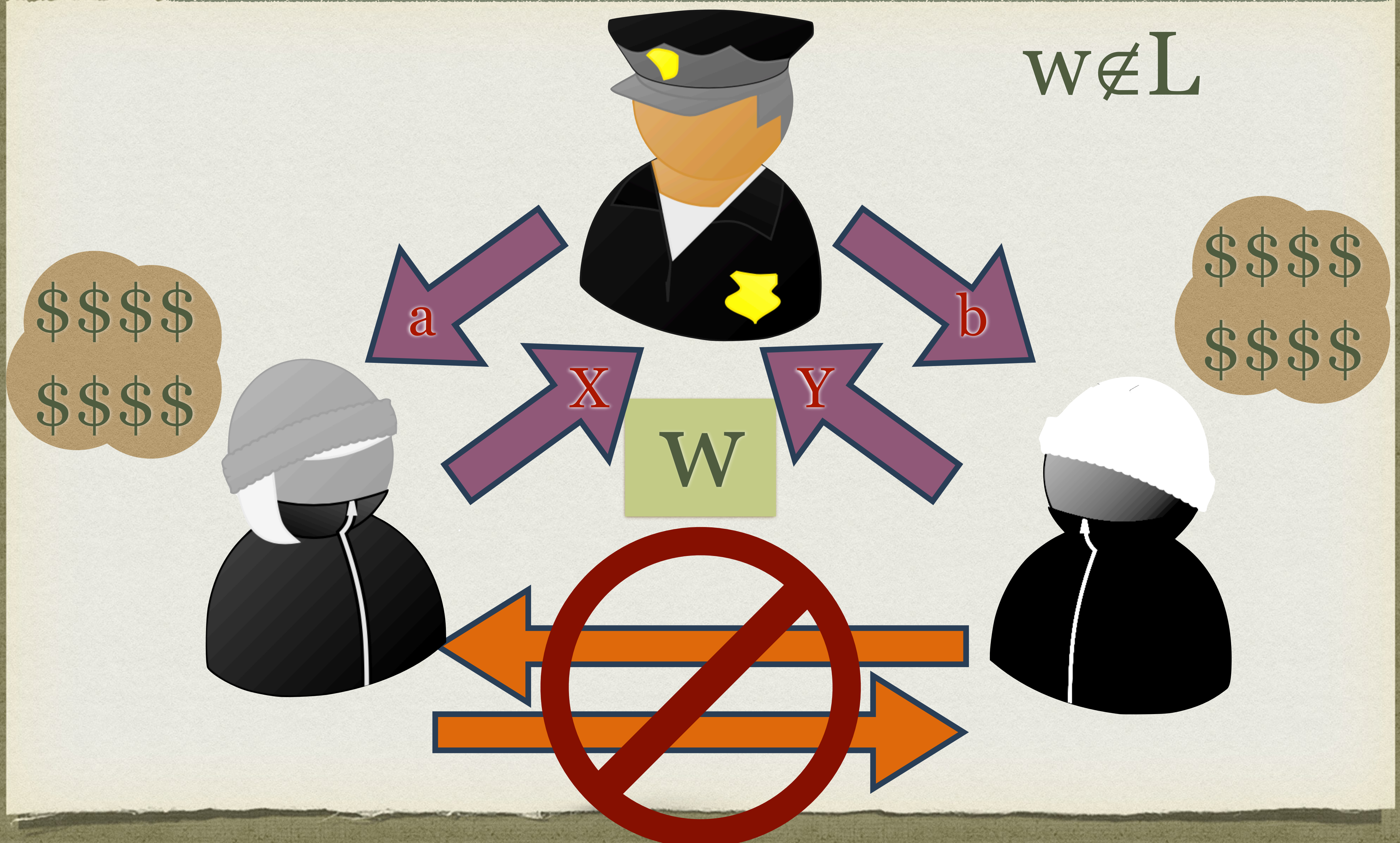
Prob[(👤:👮:👤) accepts] $\leq \epsilon$



$\exists$,

and $\forall$, , $\forall w \notin L$,

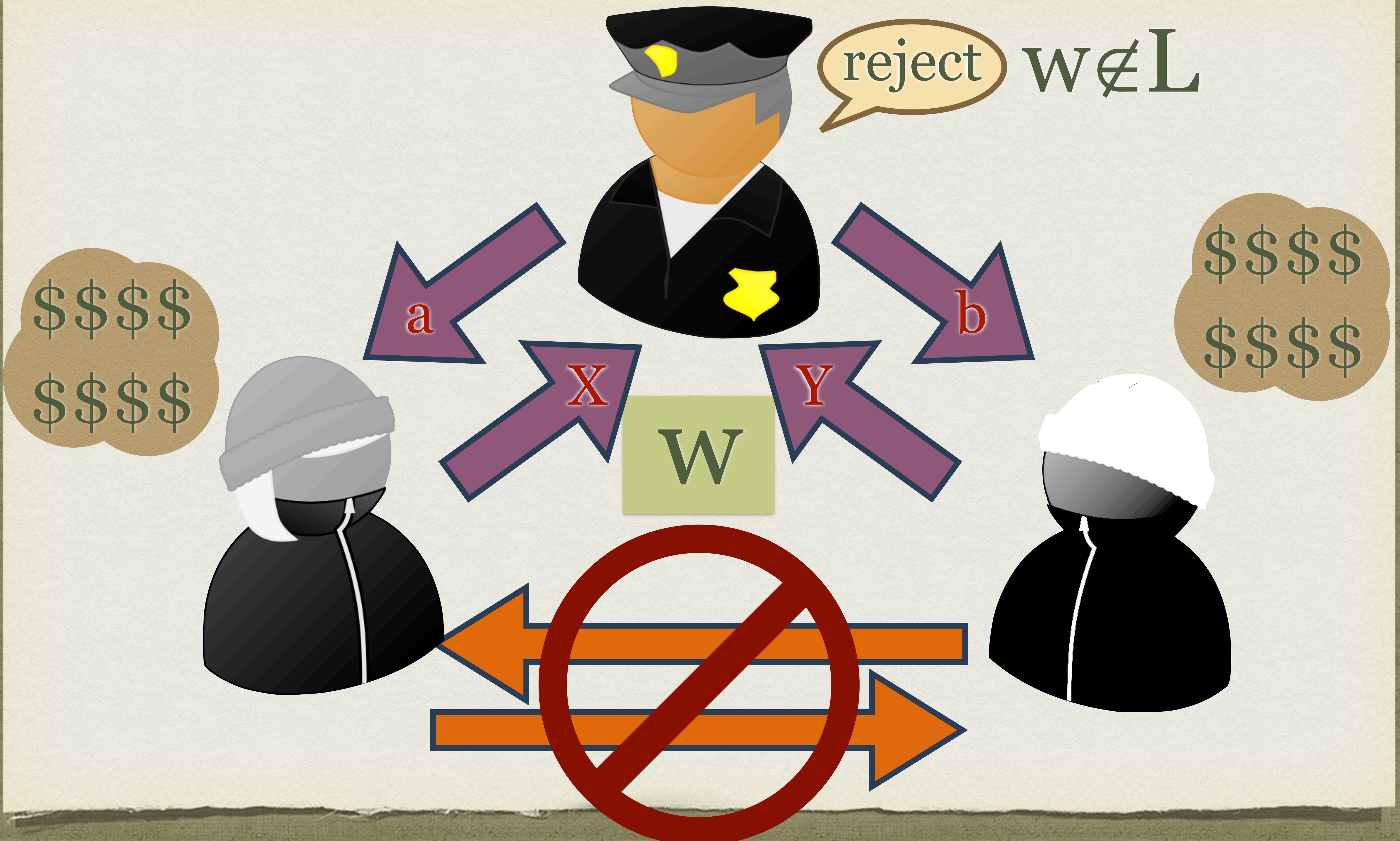
Prob[(: :) accepts] $\leq \epsilon$



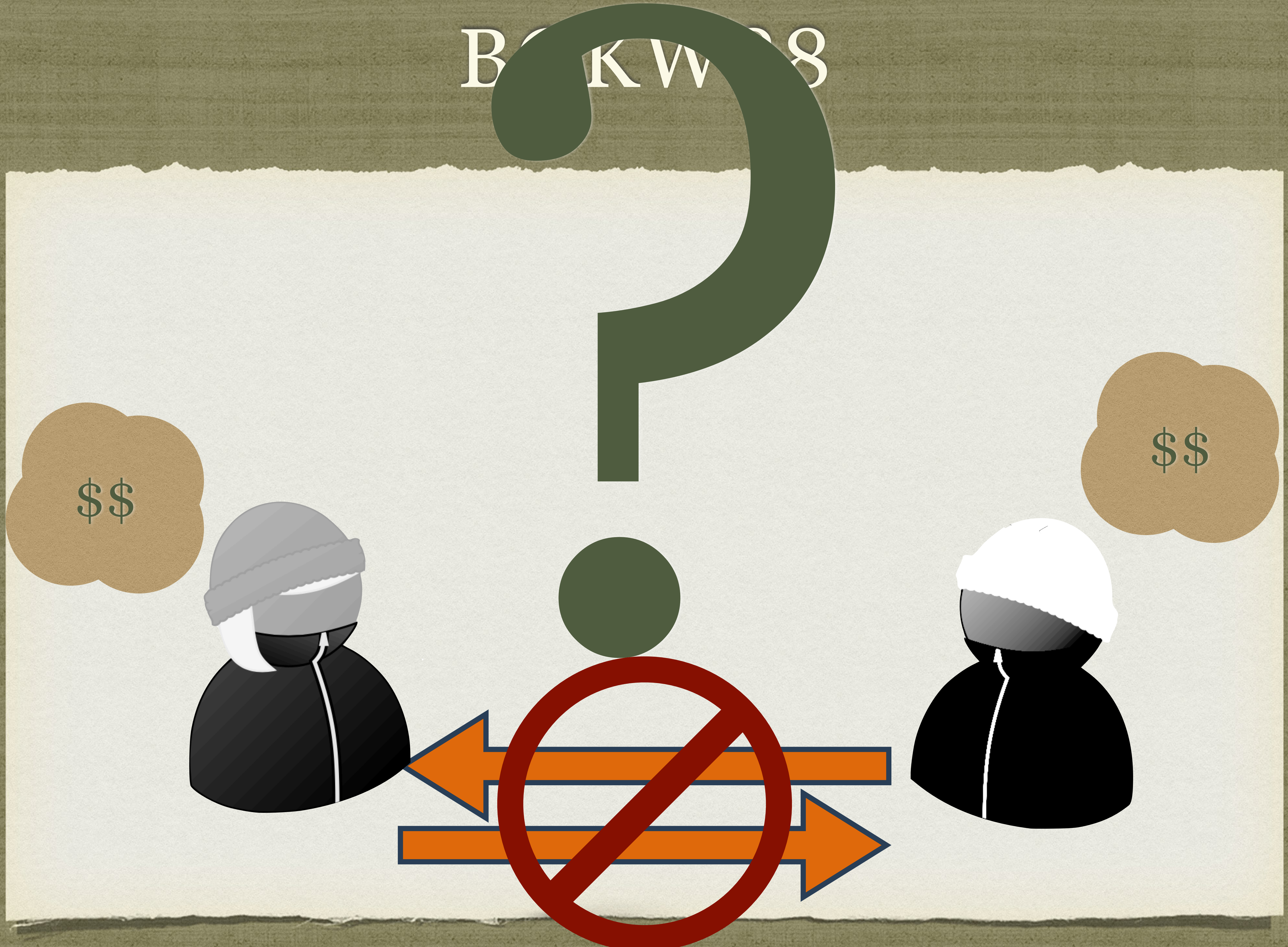
∃👮, ∃

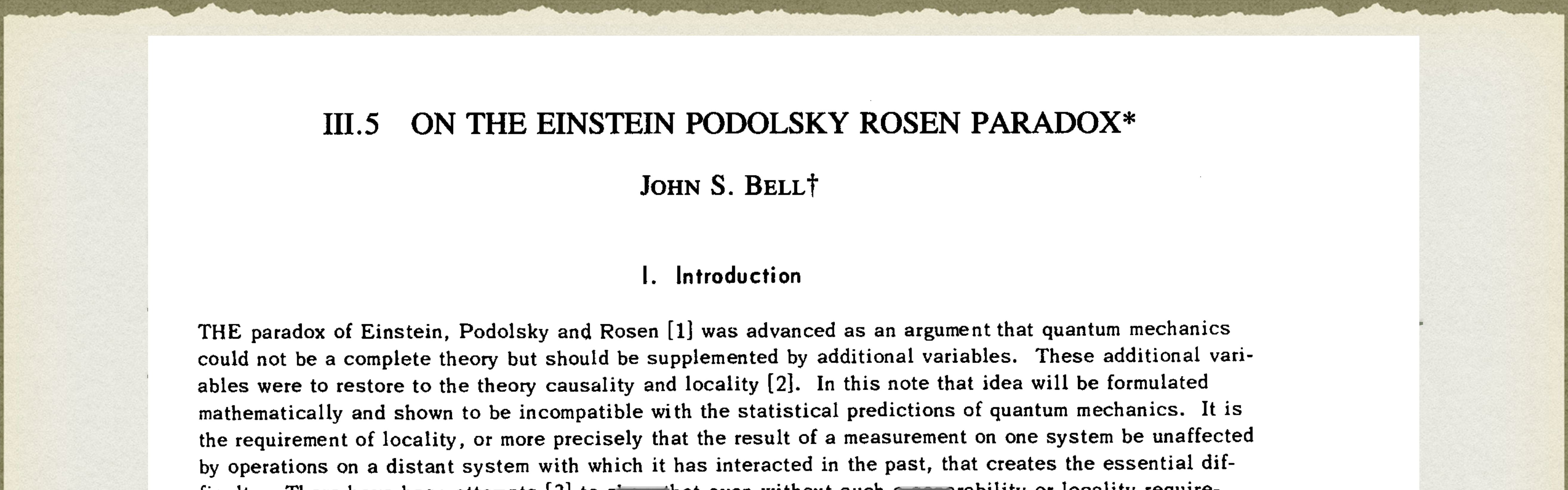
and ∀👤, 👤, $\forall w \notin L$,

Prob[(👤:👮:👤) accepts] $\leq \epsilon$



B KW 8



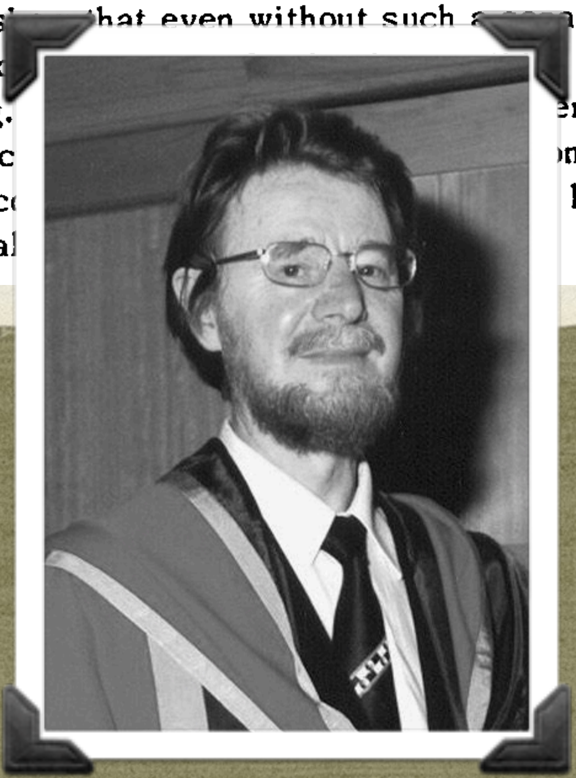


III.5 ON THE EINSTEIN PODOLSKY ROSEN PARADOX*

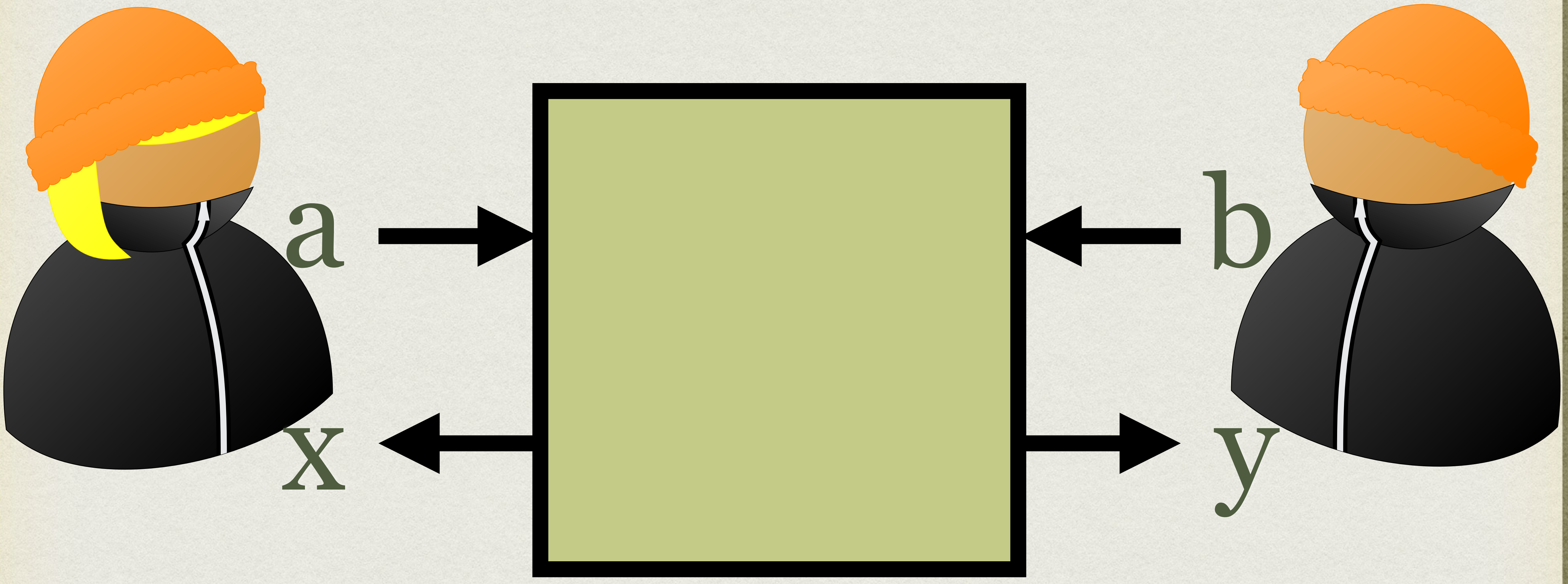
JOHN S. BELL†

I. Introduction

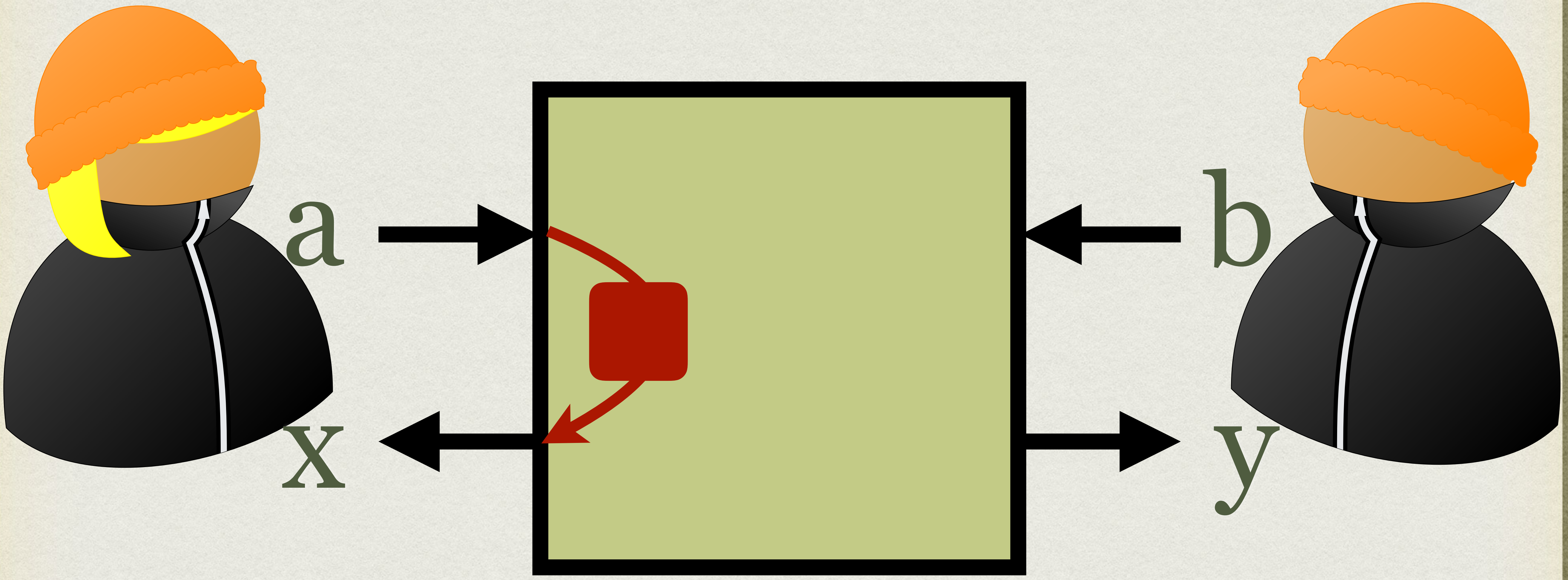
THE paradox of Einstein, Podolsky and Rosen [1] was advanced as an argument that quantum mechanics could not be a complete theory but should be supplemented by additional variables. These additional variables were to restore to the theory causality and locality [2]. In this note that idea will be formulated 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 hat even without such a arability or locality requirement no "hidden variable" interpretation These attempts have been examined elsewhere [4] and found wanting. rpretation of elementary quantum theory [5] has been explicitly construc n has indeed a grossly nonlocal structure. This is characteristic, ac here, of any such theory which reproduces exactly the quantum mechanical



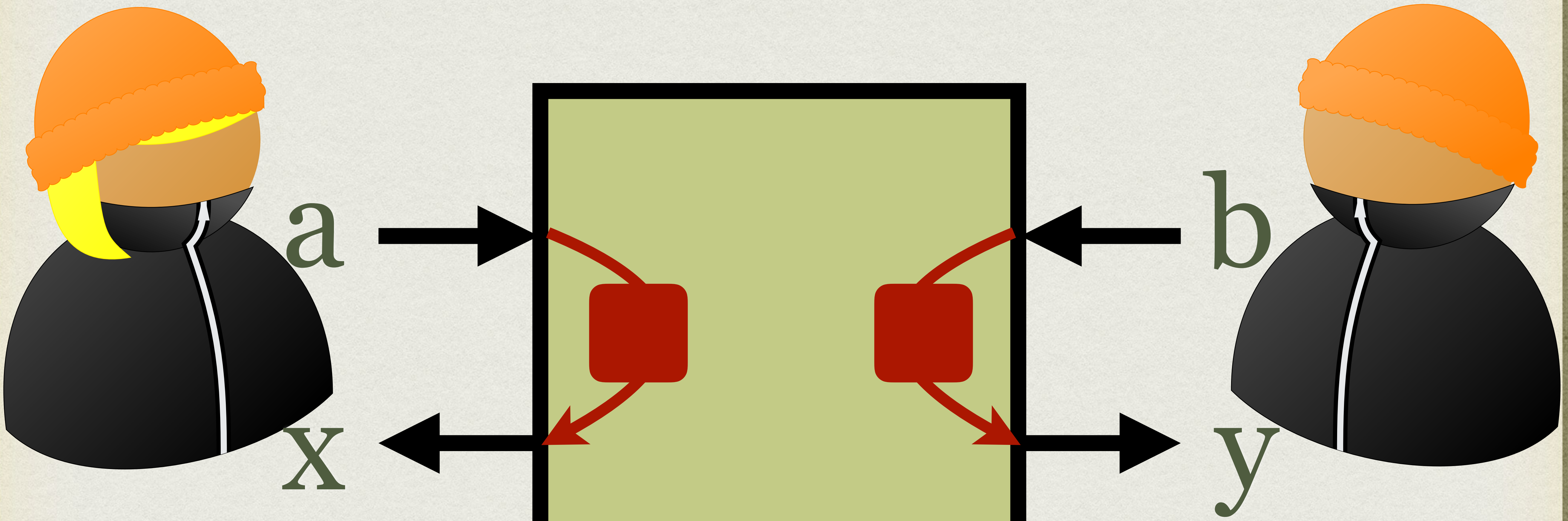
LOCALITY



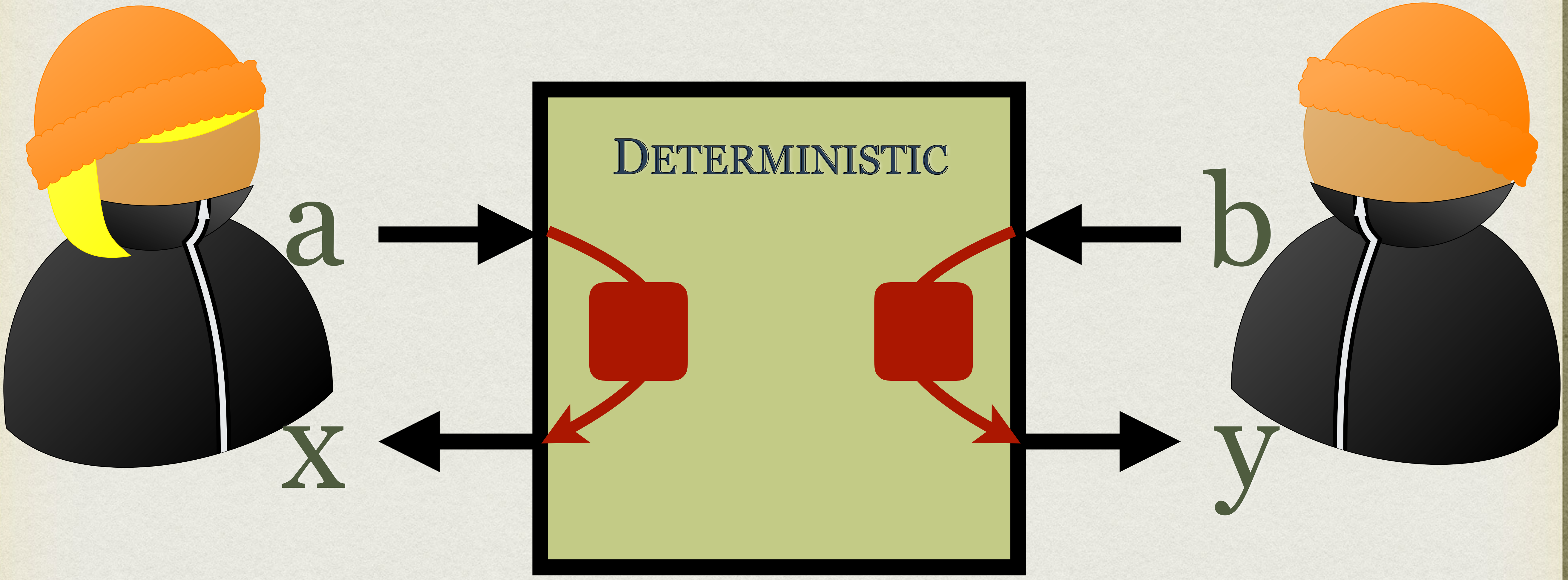
LOCALITY



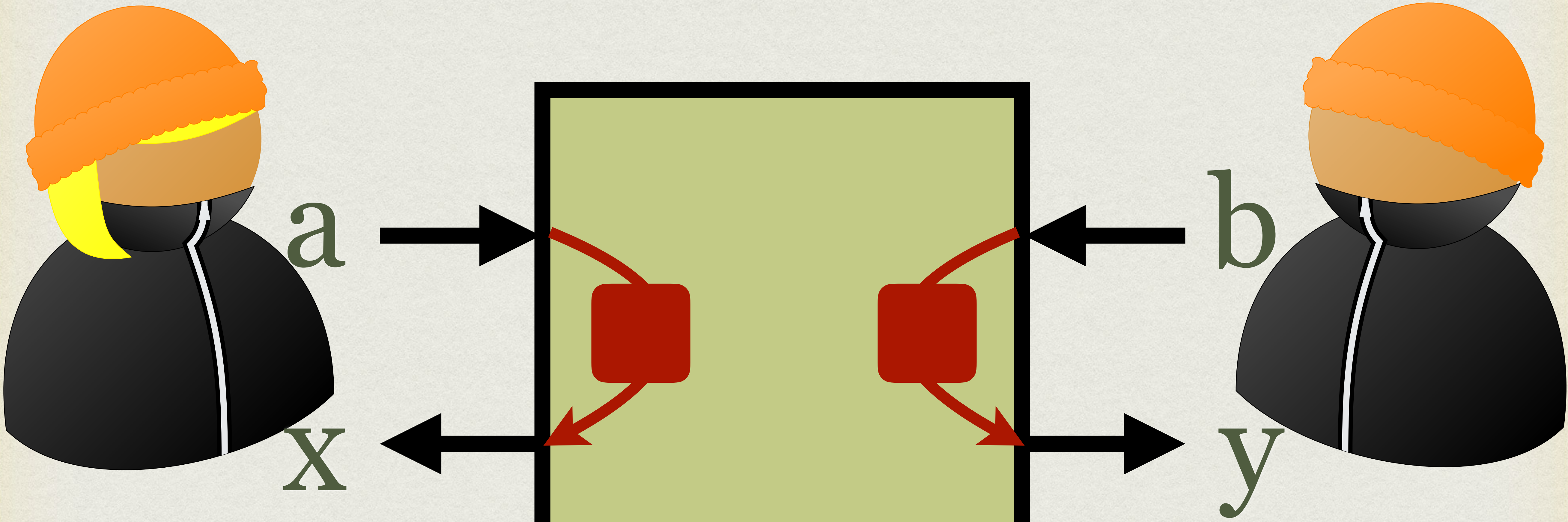
LOCALITY



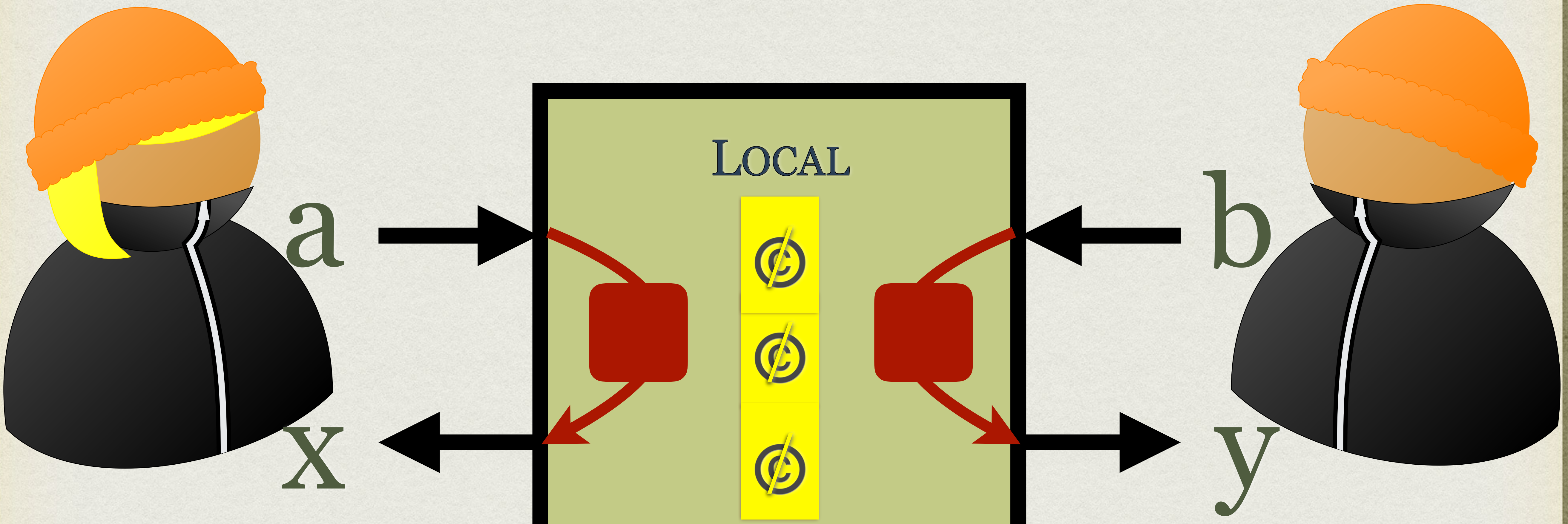
LOCALITY



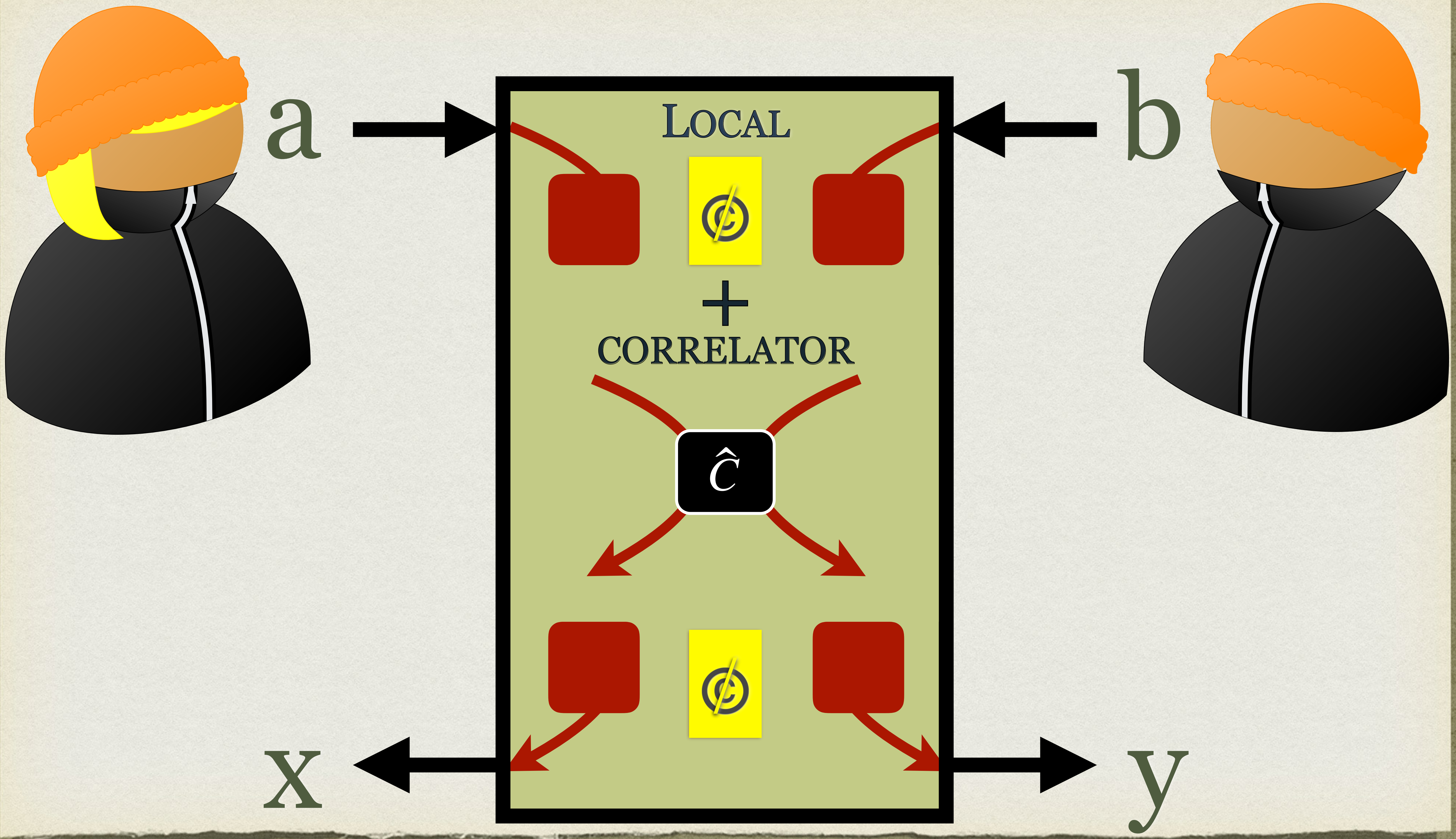
LOCALITY



LOCALITY

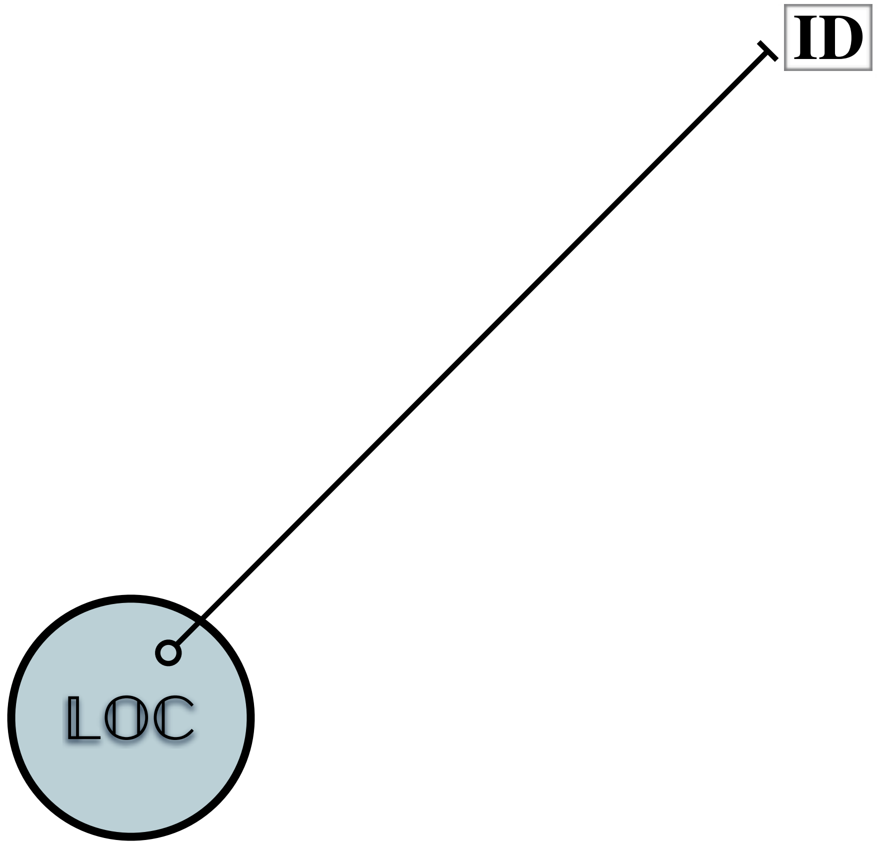


NON-LOCALITY HIERARCHY

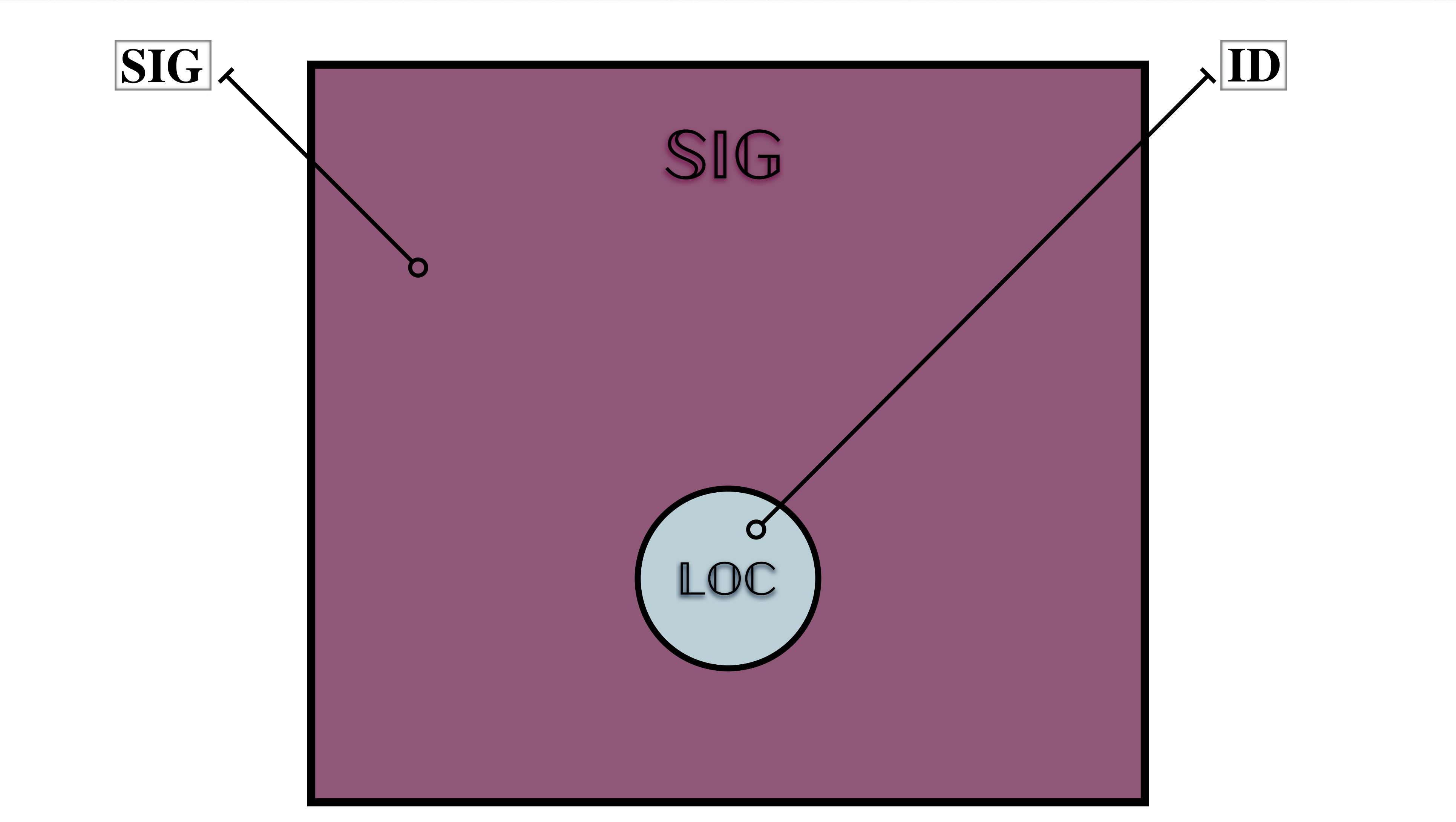


NON-LOCALITY HIERARCHY

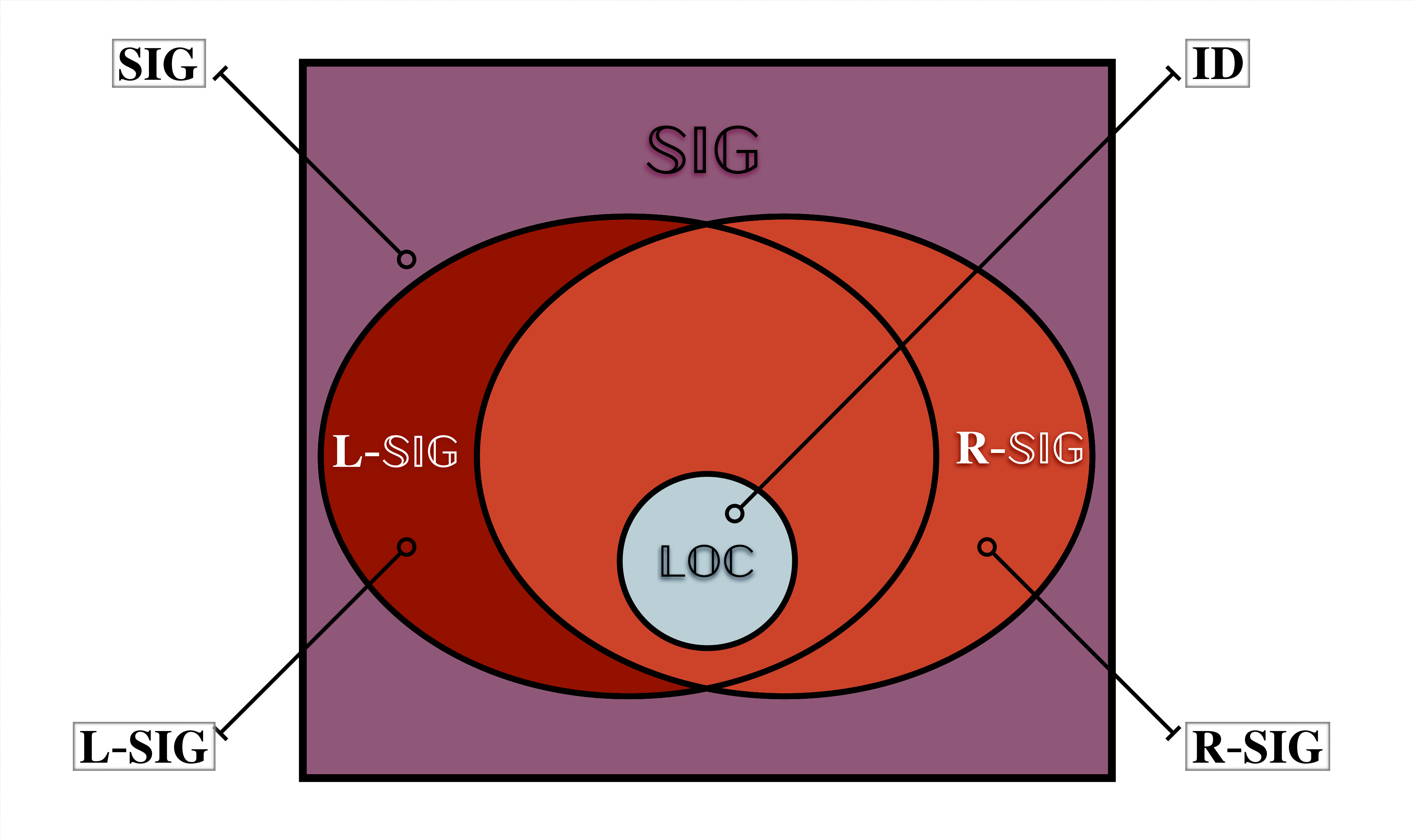
NON-LOCALITY HIERARCHY



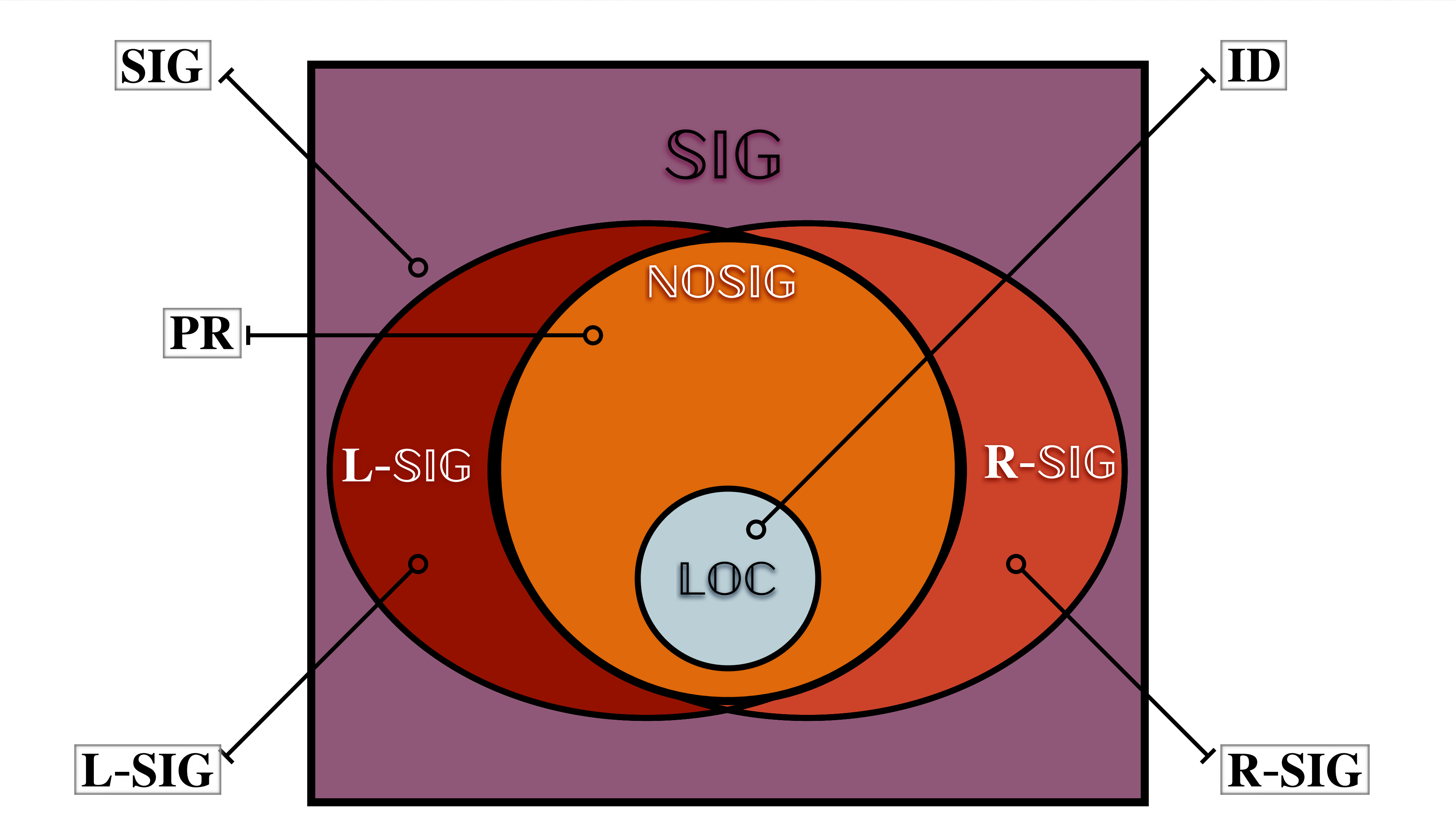
NON-LOCALITY HIERARCHY



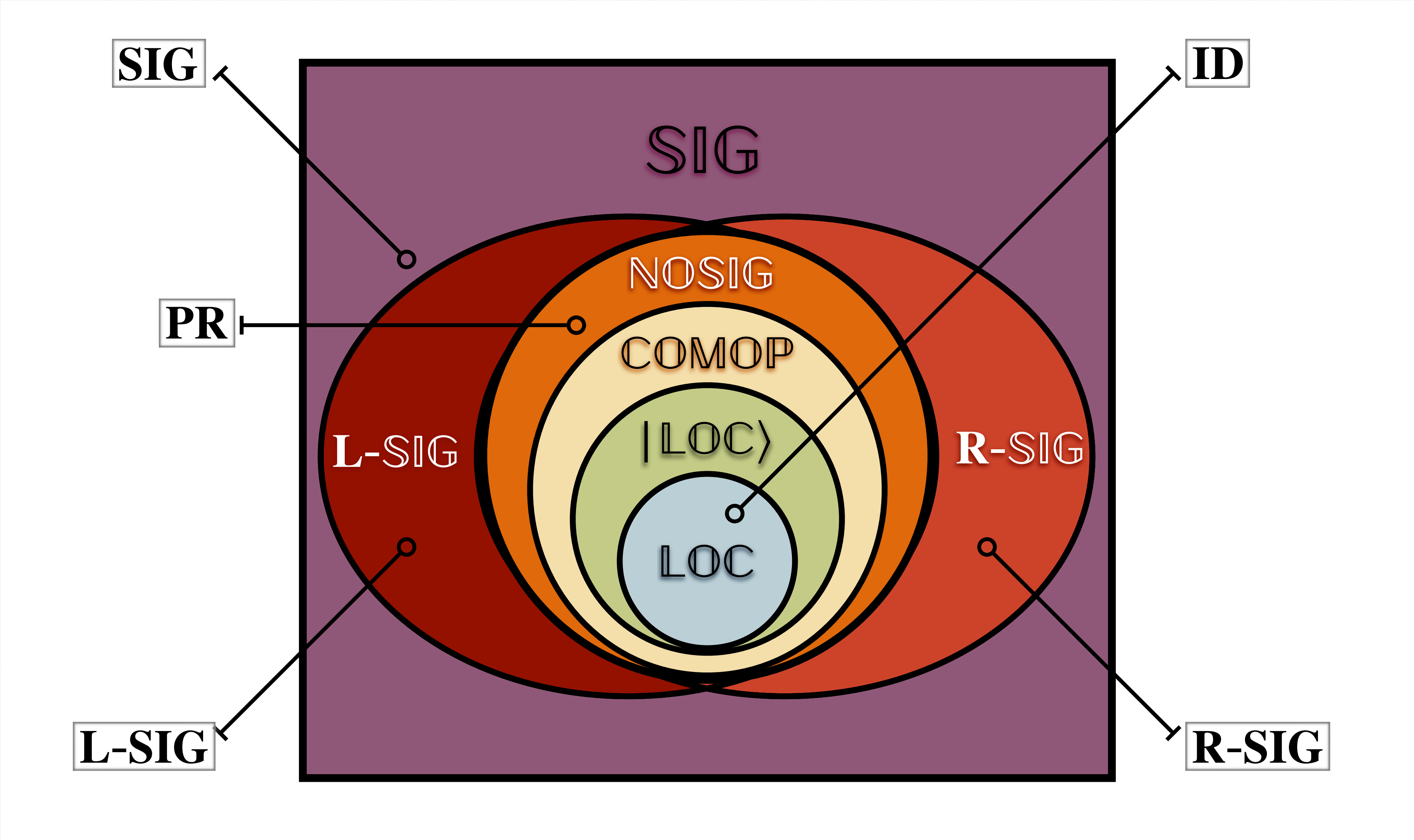
NON-LOCALITY HIERARCHY



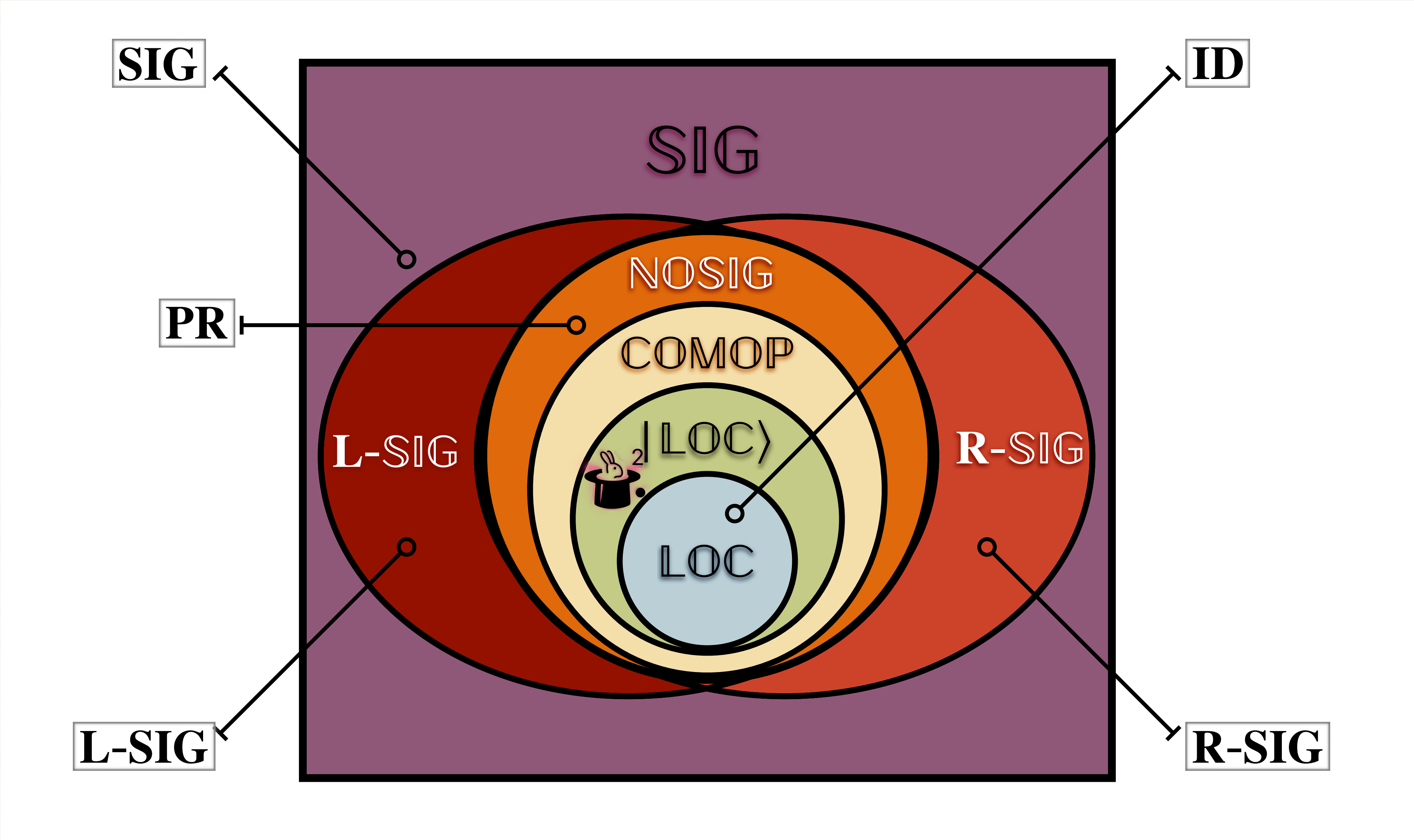
NON-LOCALITY HIERARCHY



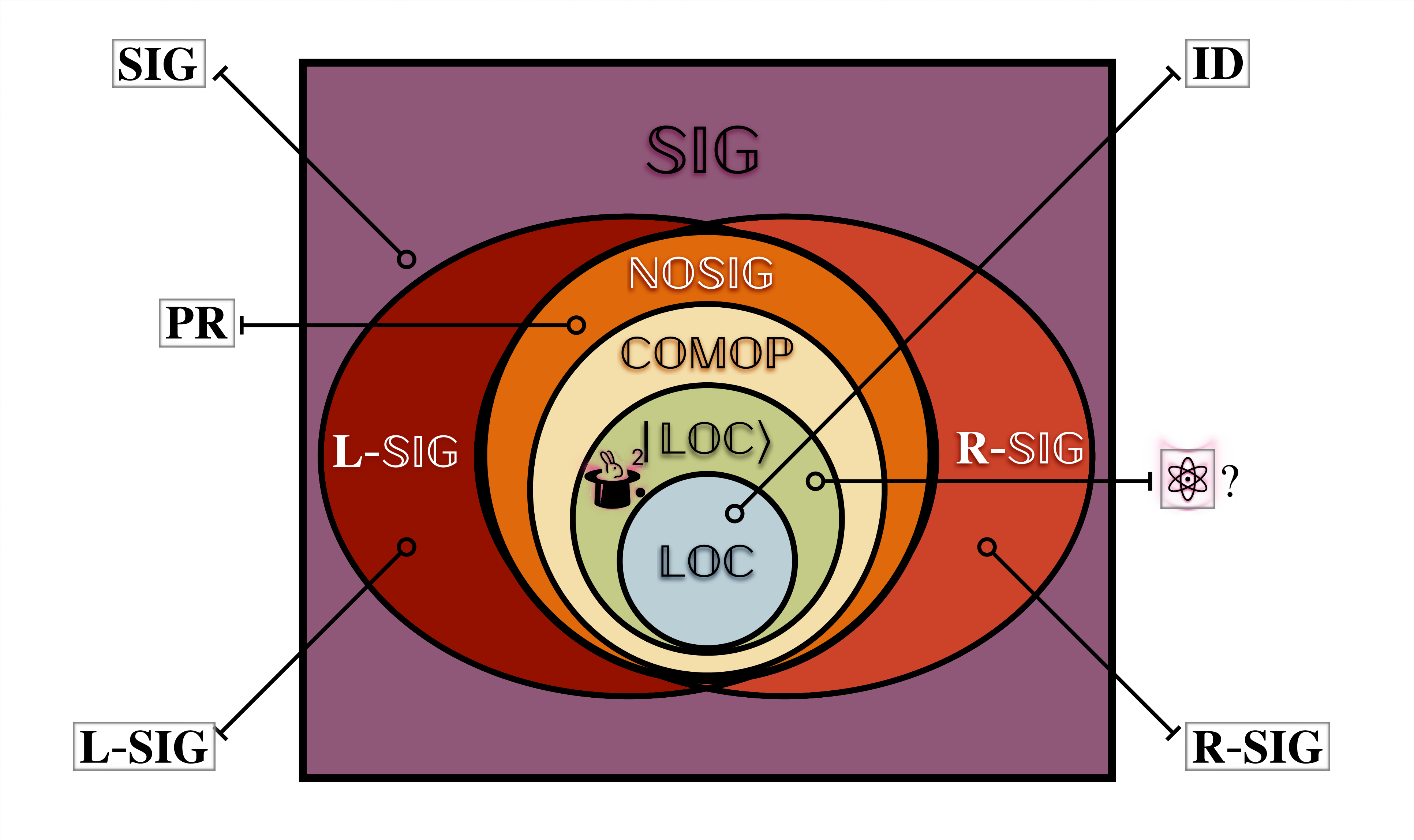
NON-LOCALITY HIERARCHY



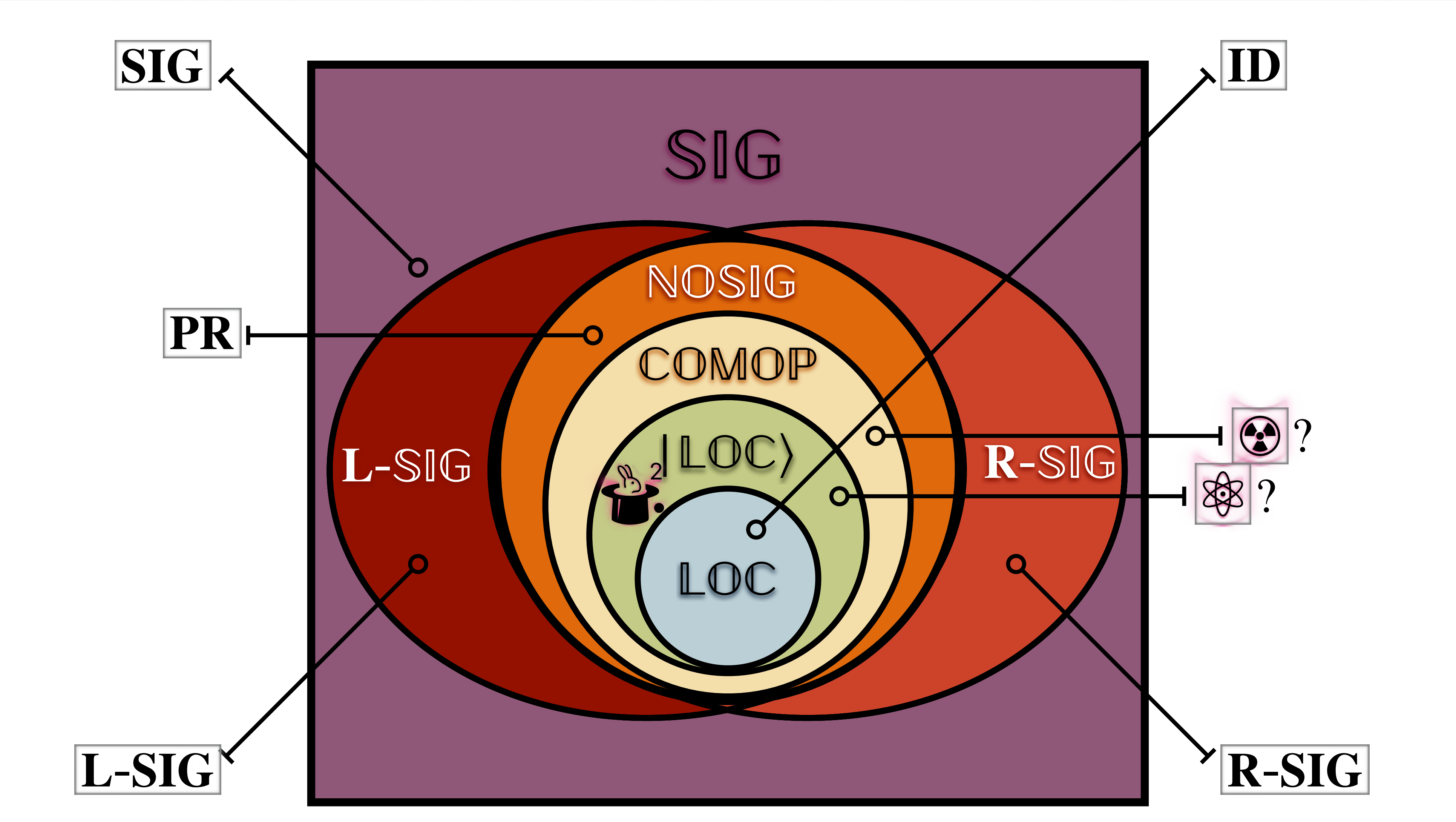
NON-LOCALITY HIERARCHY

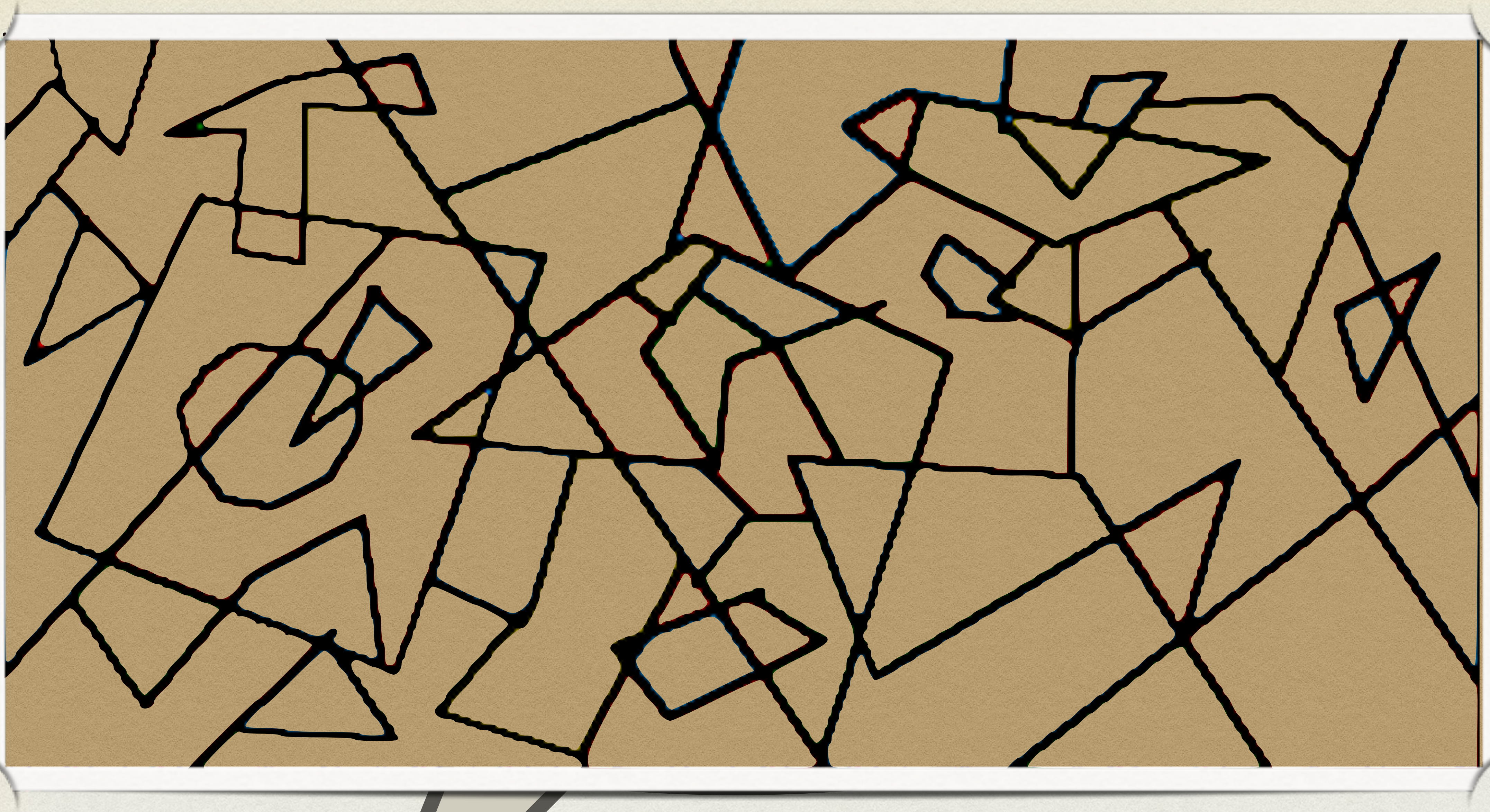


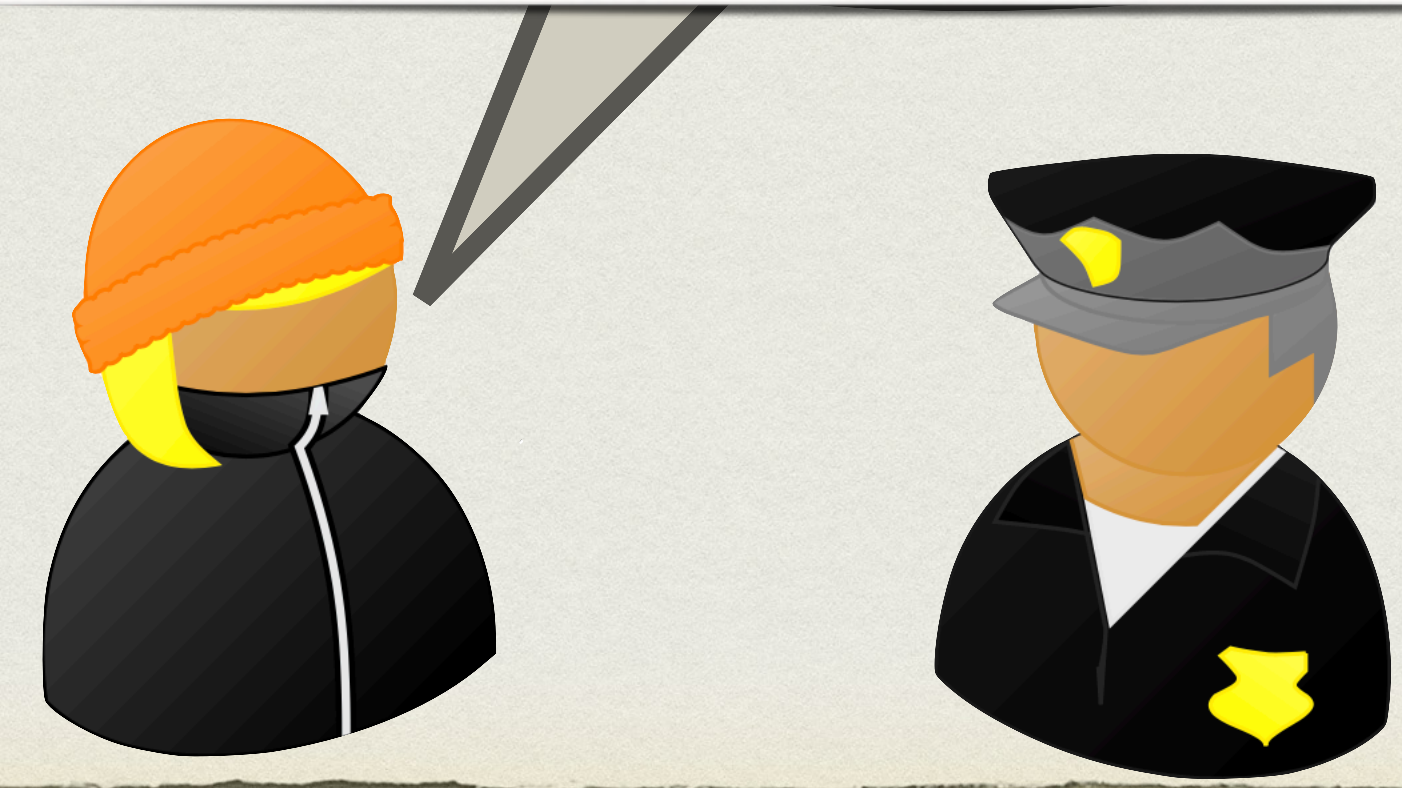
NON-LOCALITY HIERARCHY

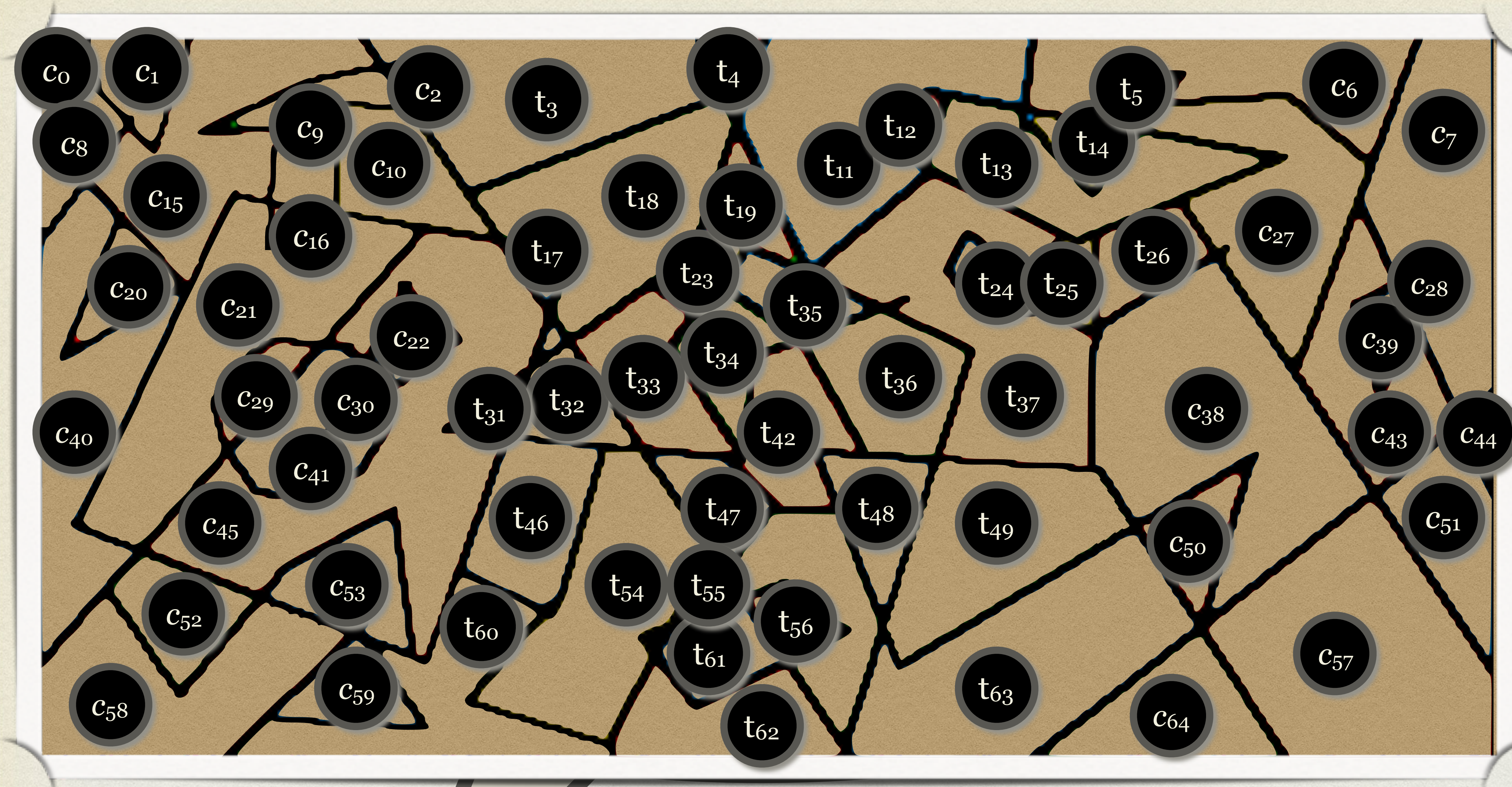


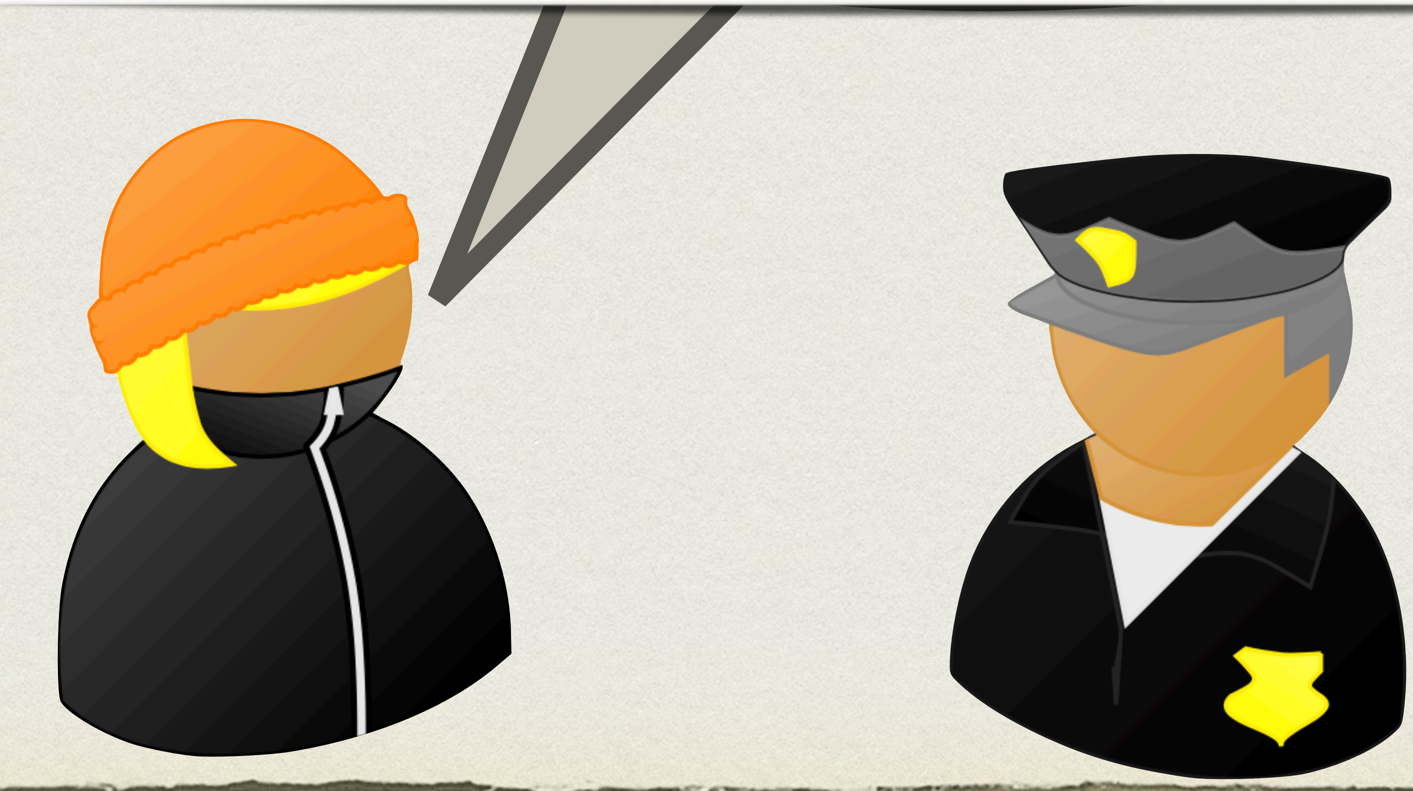
NON-LOCALITY HIERARCHY



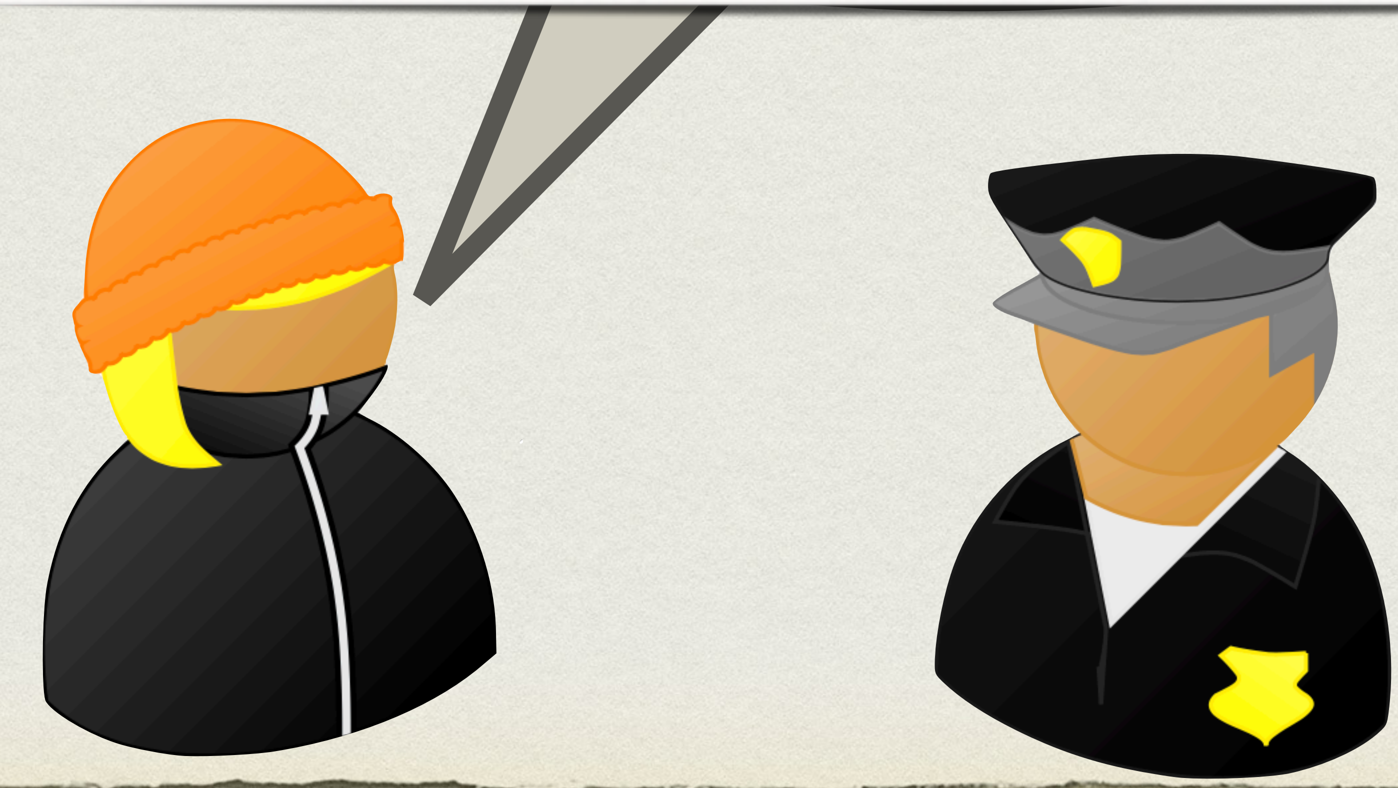


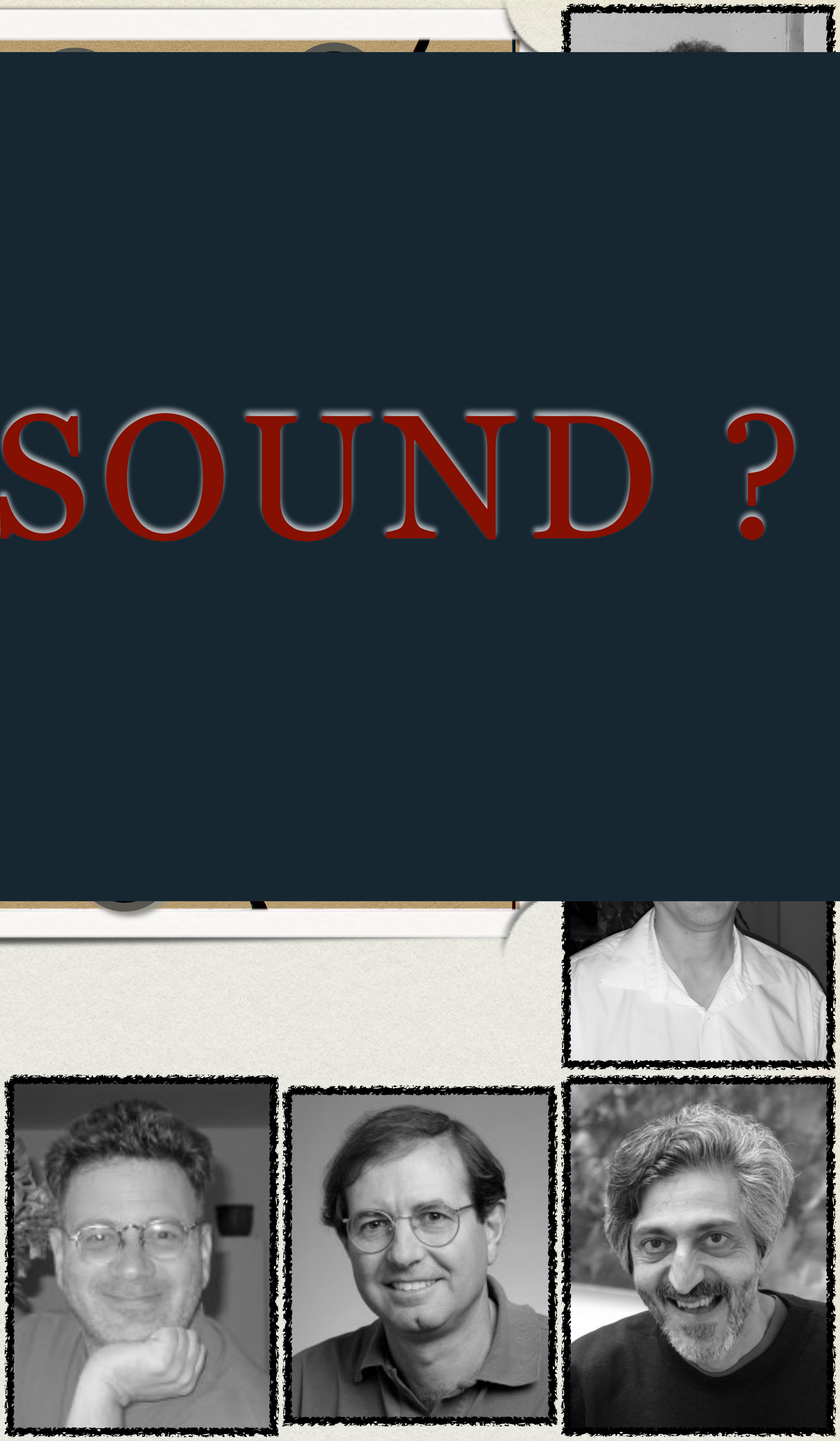


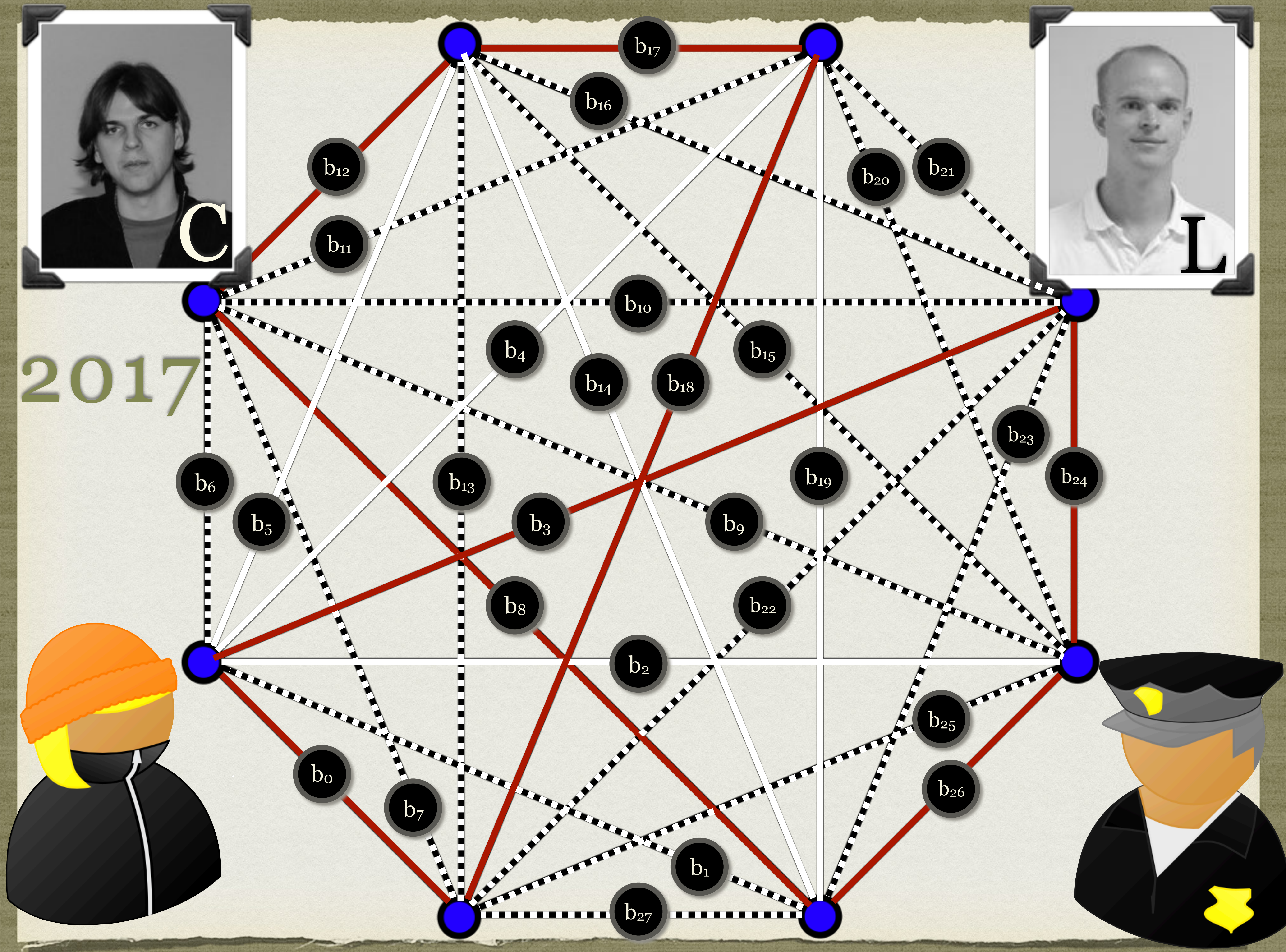

c_0
c_1
c_2
t_3
t_4
t_5
c_6
c_7
c_8
c_9
c_{10}
t_{11}
t_{12}
t_{13}
t_{14}
c_{15}
c_{16}
t_{17}
t_{18}
t_{19}
c_{20}
c_{21}
c_{22}
t_{23}
t_{24}
t_{25}
t_{26}
c_{27}
c_{28}
c_{29}
c_{30}
t_{31}
t_{32}
t_{33}
t_{34}
t_{35}
t_{36}
t_{37}
c_{38}
c_{39}
c_{40}
c_{41}
t_{42}
c_{43}
c_{44}
c_{45}
t_{46}
t_{47}
t_{48}
t_{49}
c_{50}
c_{51}
c_{52}
c_{53}
t_{54}
t_{55}
t_{56}
c_{57}
c_{58}
c_{59}
t_{60}
t_{61}
t_{62}
t_{63}
c_{64}



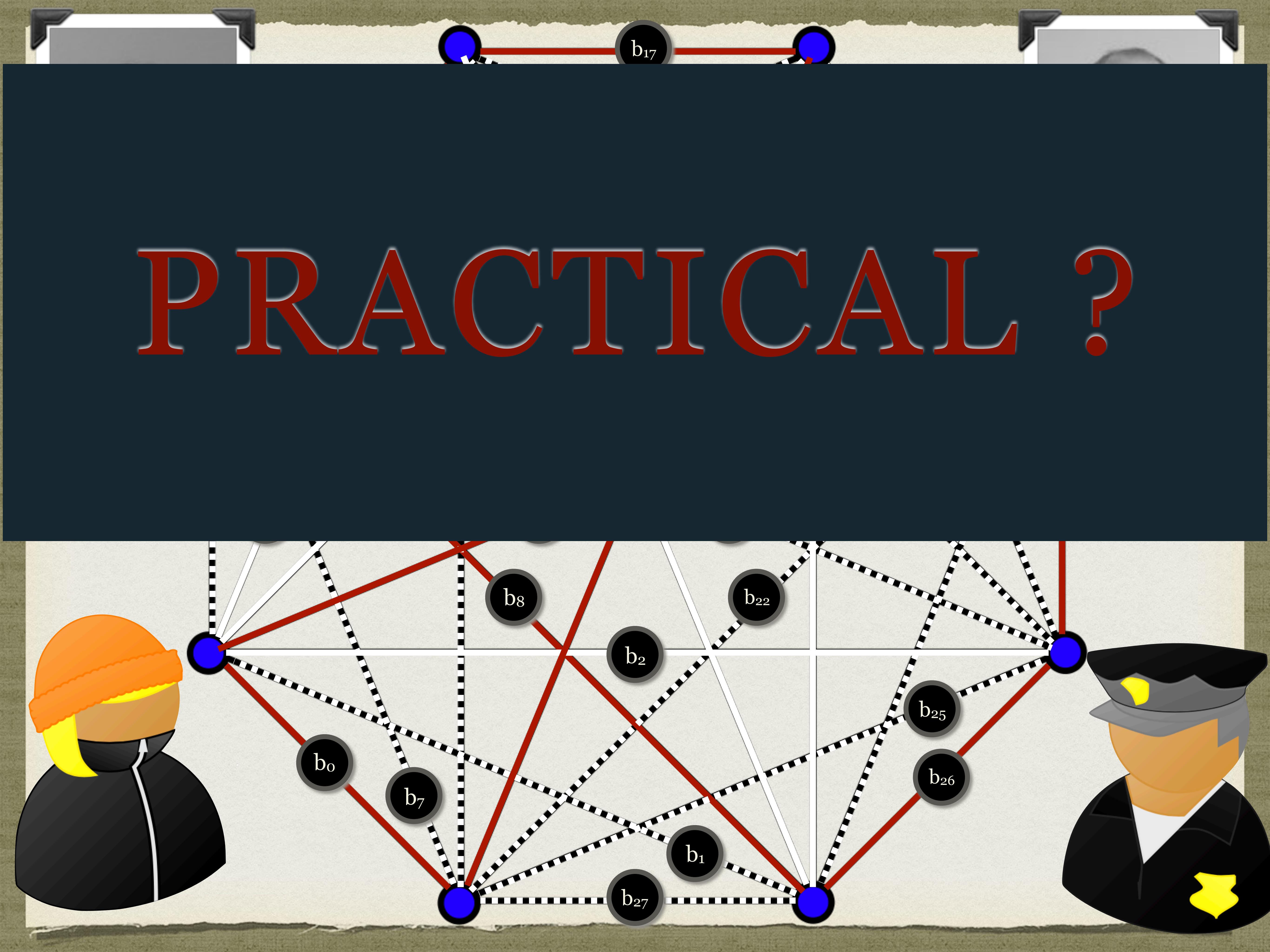
ENTANGLED SOUND ?





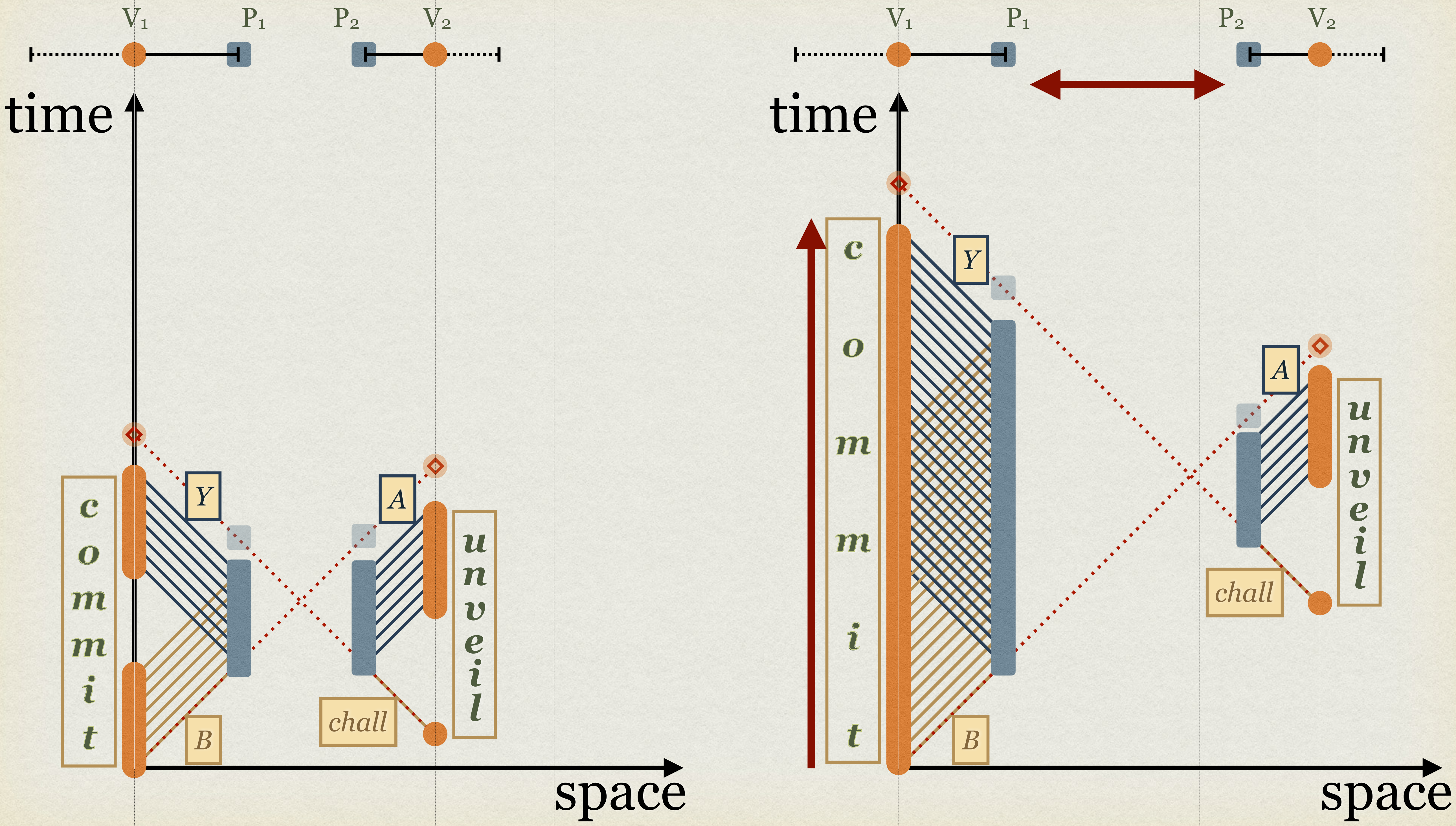

C
L
b17
b16
b12
b11
b20
b21
b10
b4
b14
b18
b15
b23
b24
b6
b13
b19
b5
b3
b9
b8
b22
b2
b25
b0
b7
b26
b1
b27

2017



PRACTICAL ?

CHAILLOUX-LEVERRIER

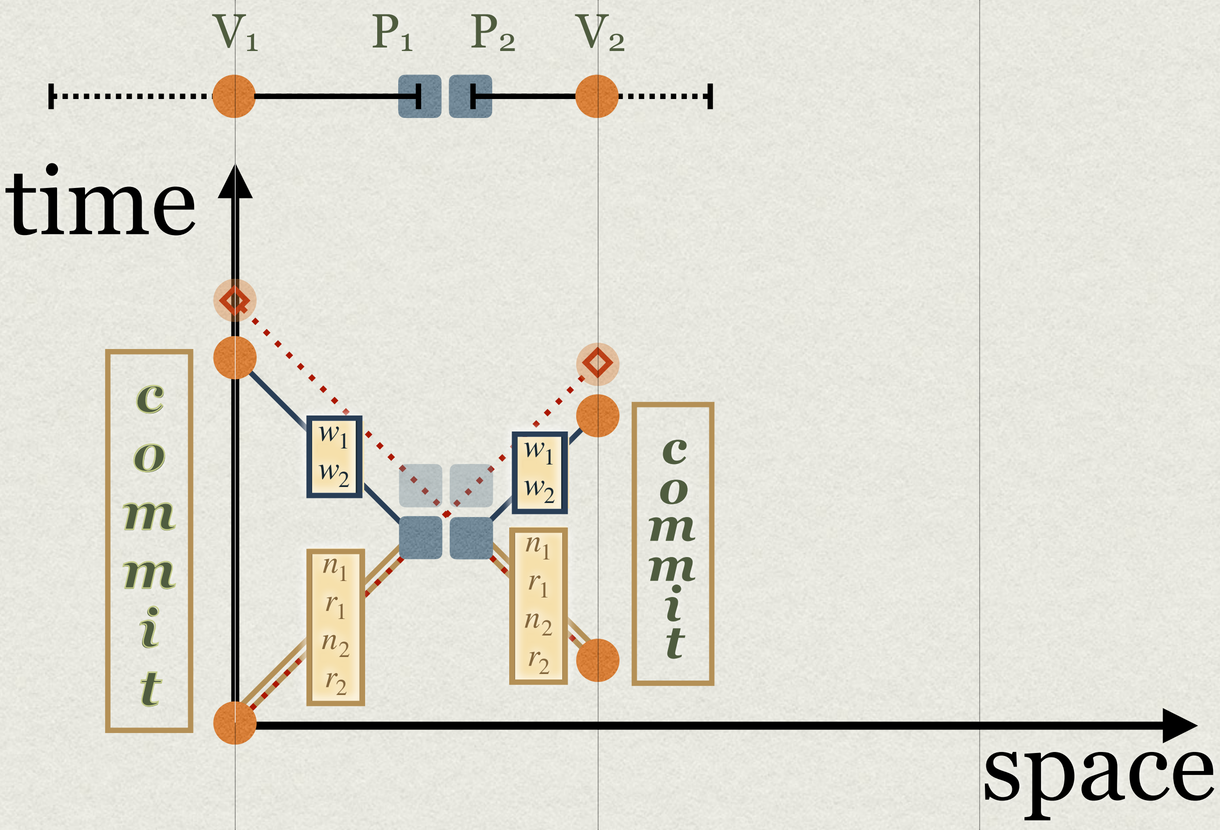


Massenet

Salvail

Stinchcombe

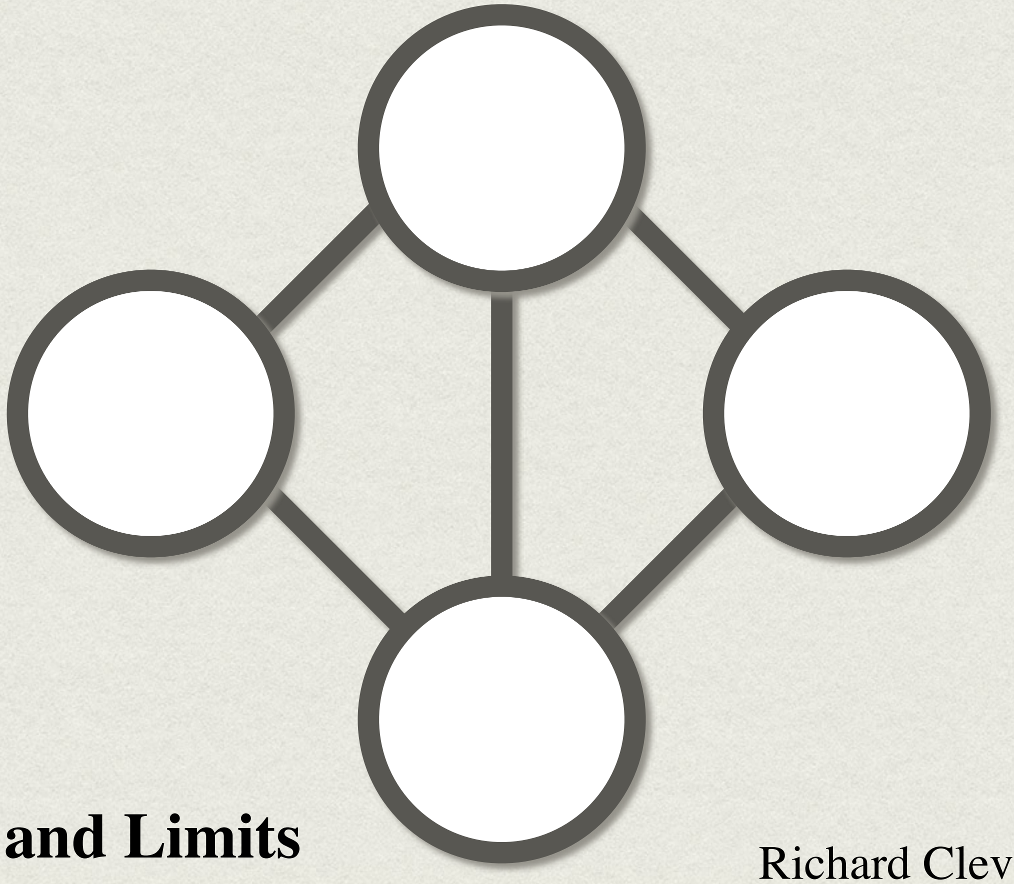
Yang

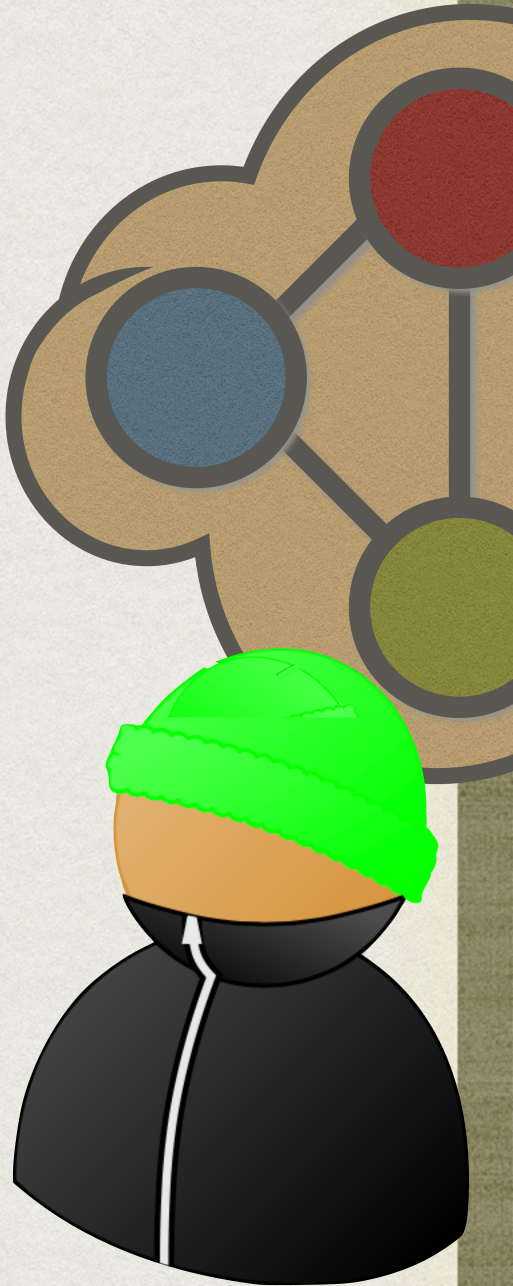


OUR APPROACH

(ZK)MIPs

2004
COMPLETENESS

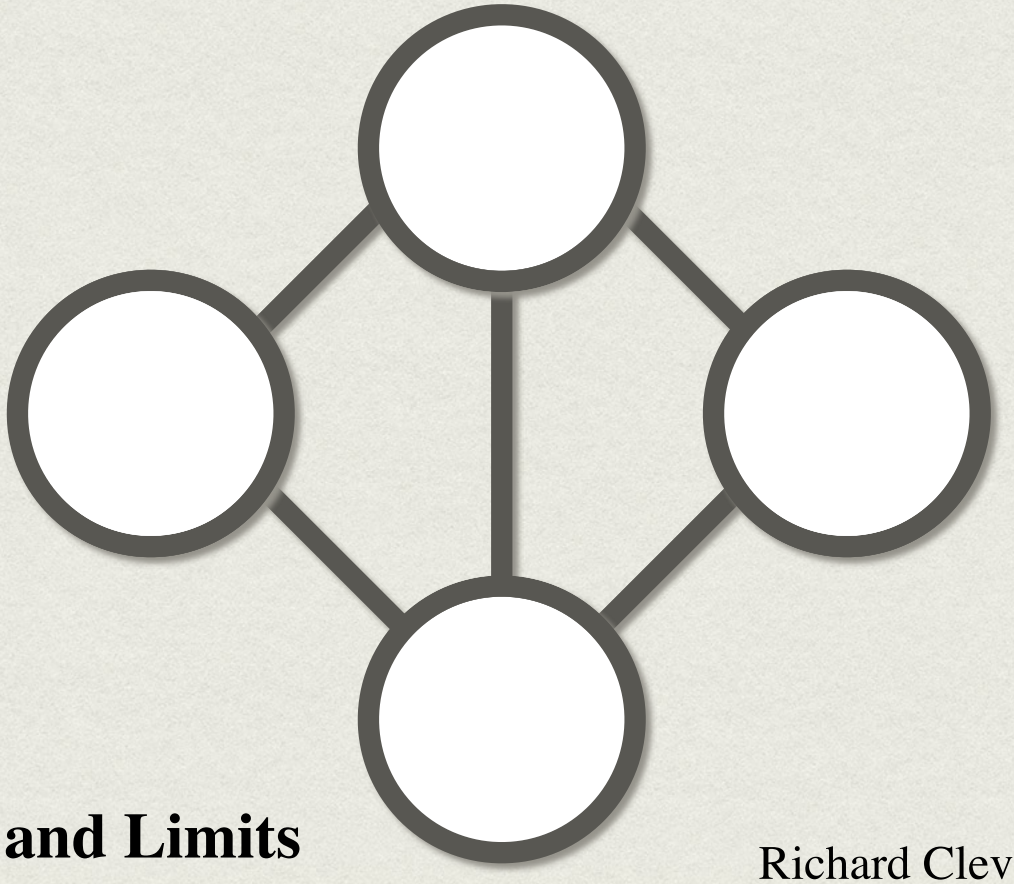




Consequences and Limits of Nonlocal Strategies

Richard Cleve Peter Høyer
Benjamin Toner John Watrous

2004
COMPLETENESS

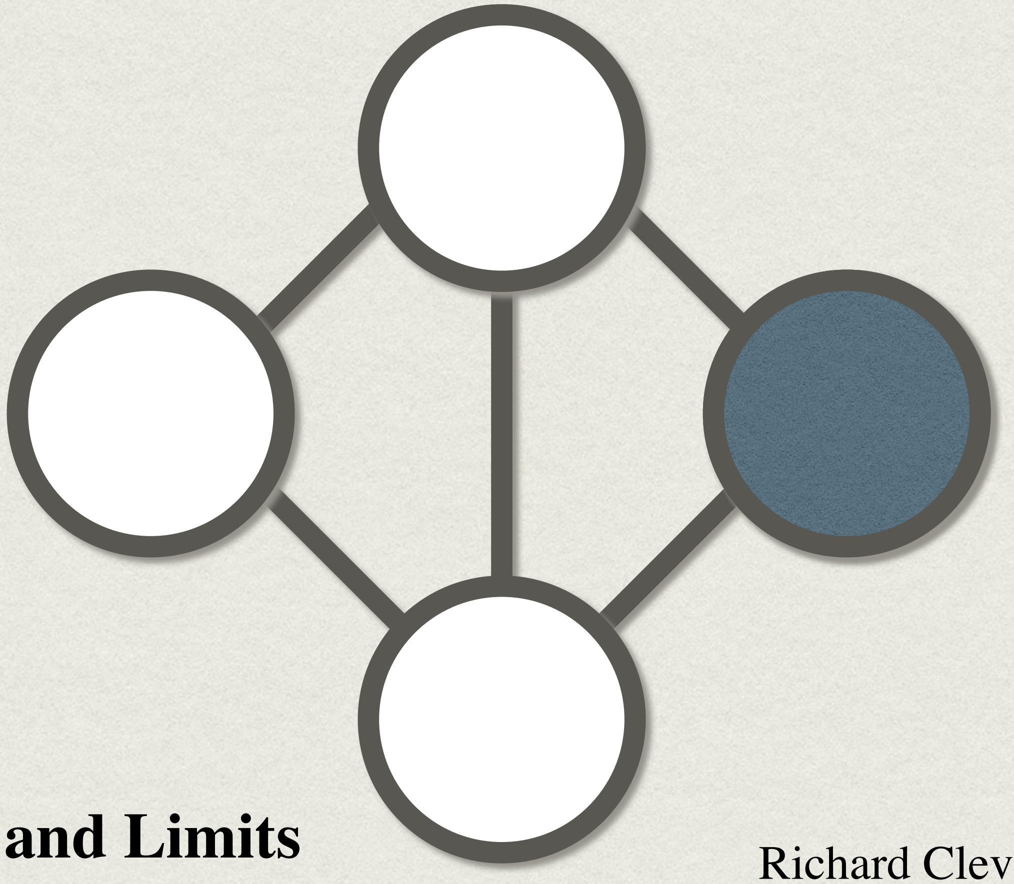


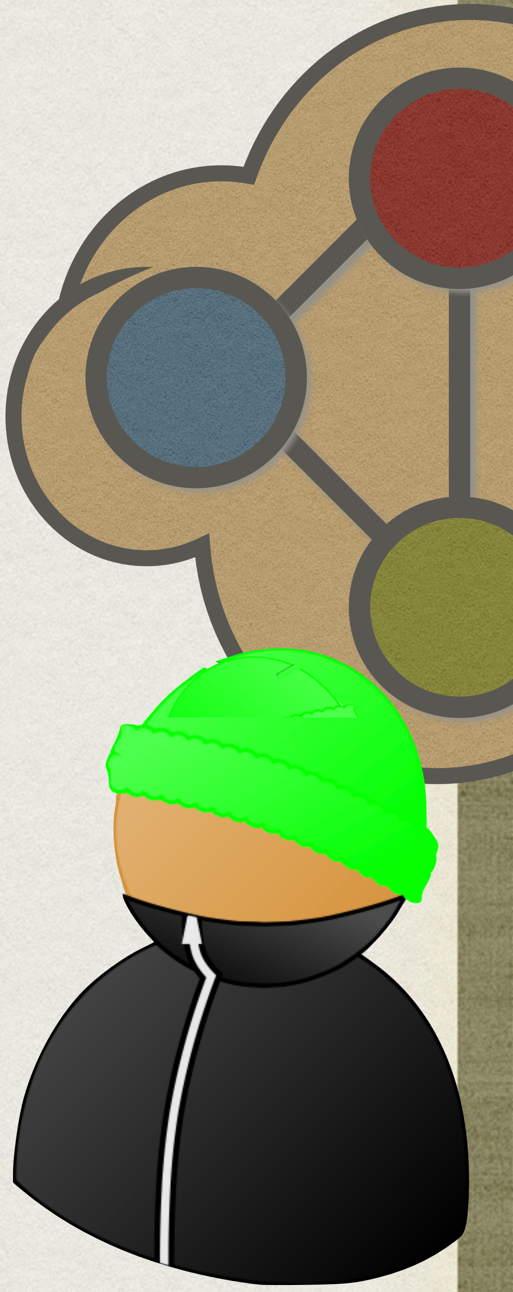
Consequences and Limits of Nonlocal Strategies

Richard Cleve Peter Høyer
Benjamin Toner John Watrous

2004

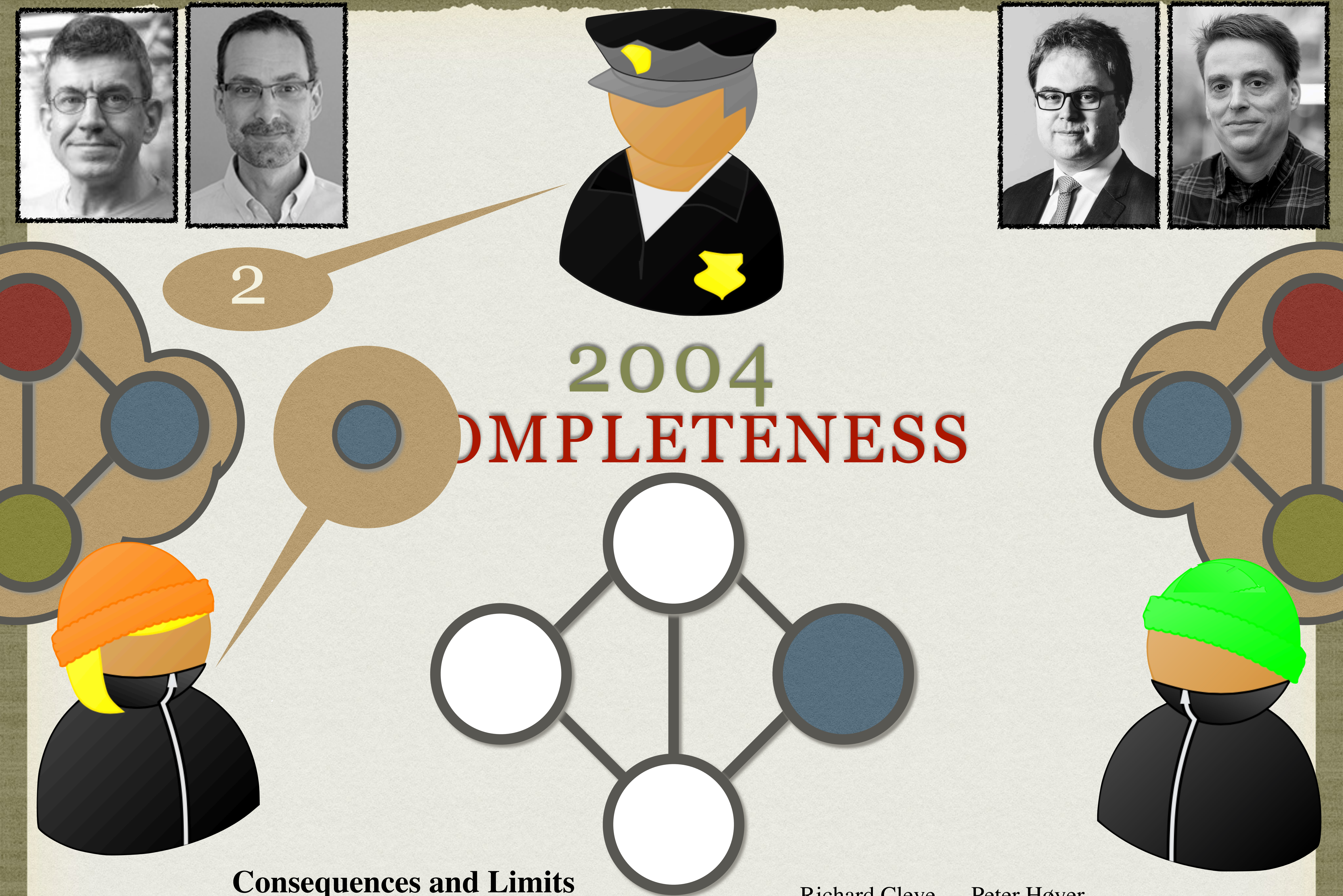
COMPLETENESS





Consequences and Limits of Nonlocal Strategies

Richard Cleve Peter Høyer
Benjamin Toner John Watrous



2004

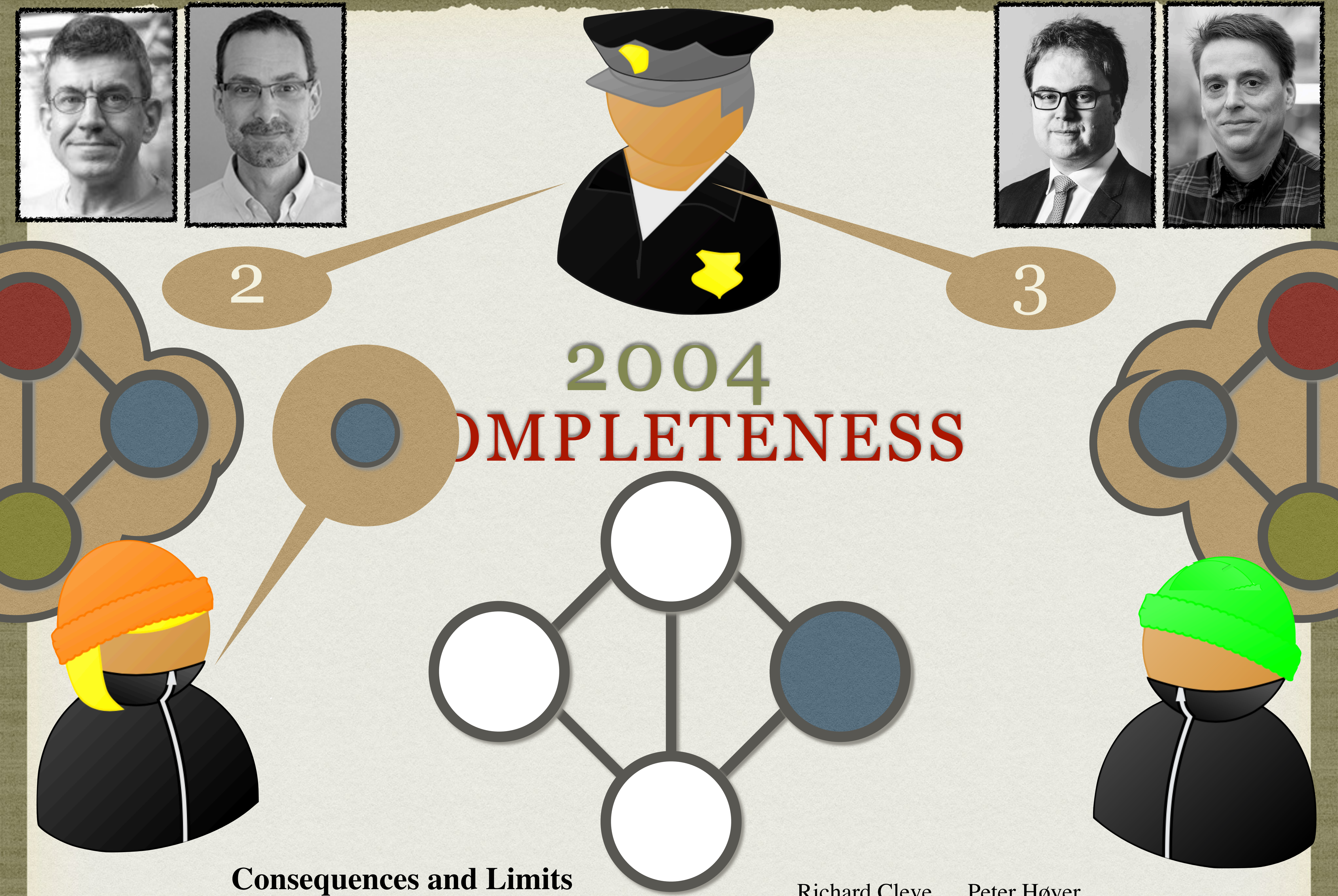
OMPLETENESS

Consequences and Limits

of Nonlocal Strategies

Richard Cleve Peter Høyer

Benjamin Toner John Watrous

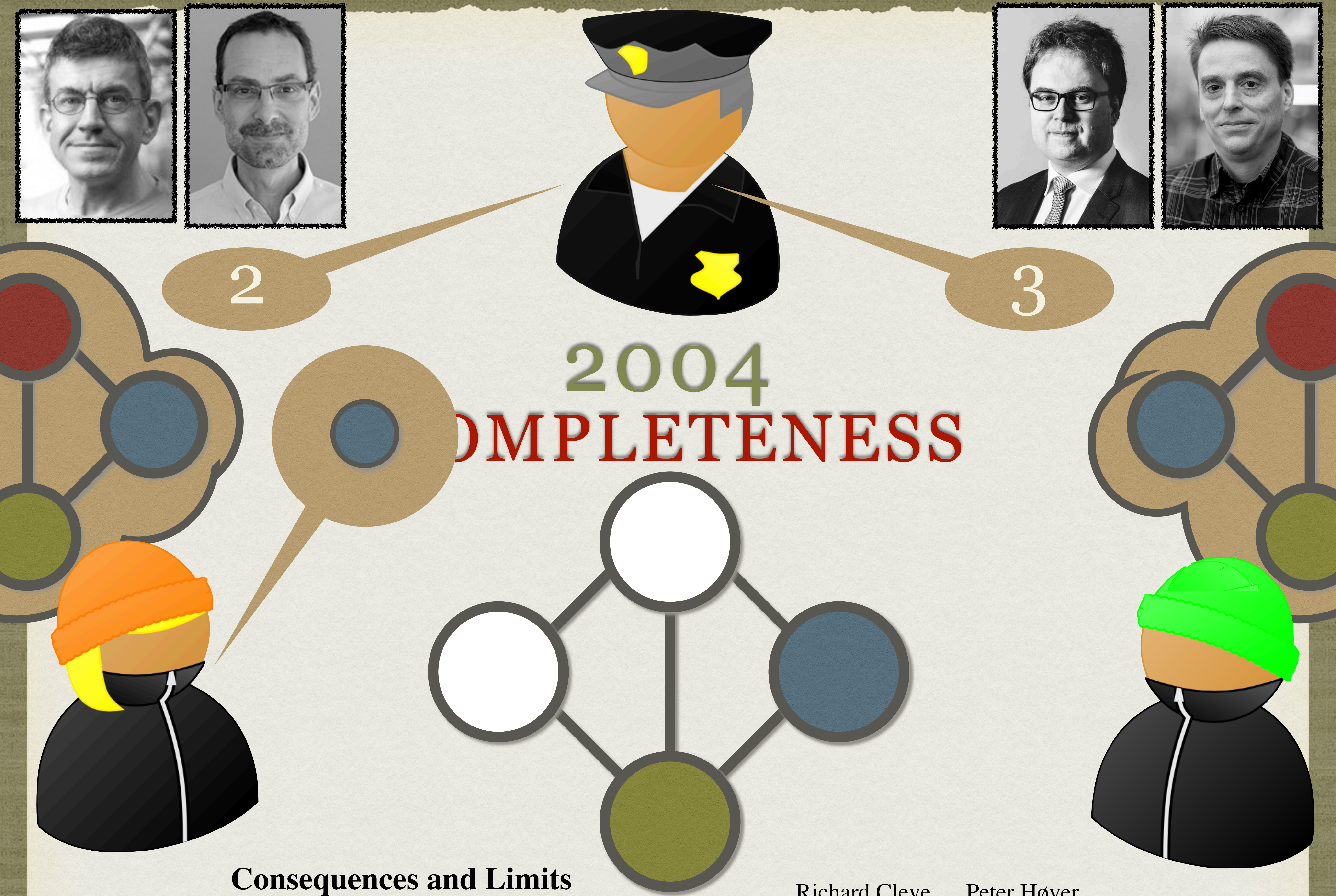


2004

OMPLETENESS

Consequences and Limits of Nonlocal Strategies

Richard Cleve   Peter Høyer
Benjamin Toner   John Watrous

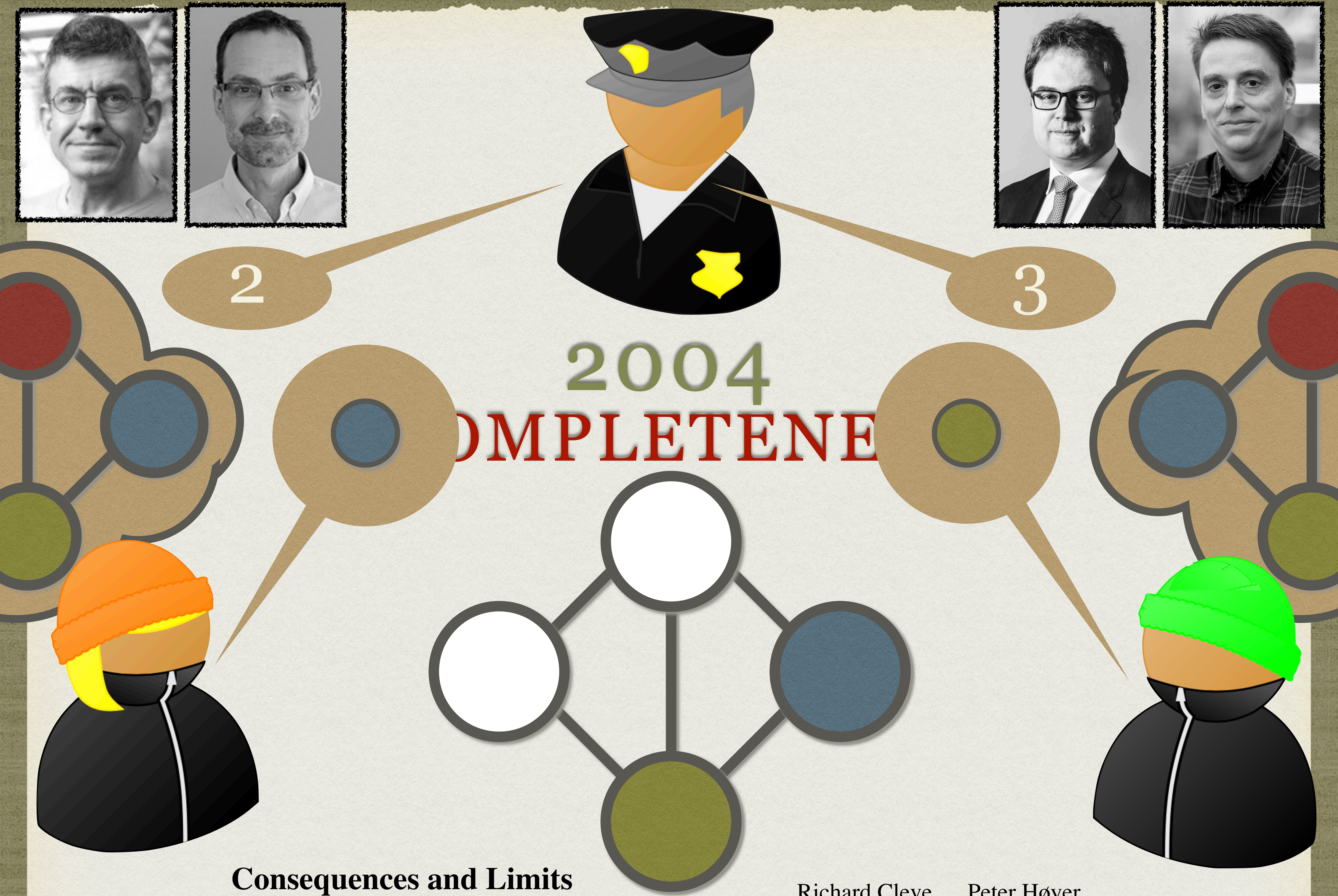


2004

OMPLETENESS

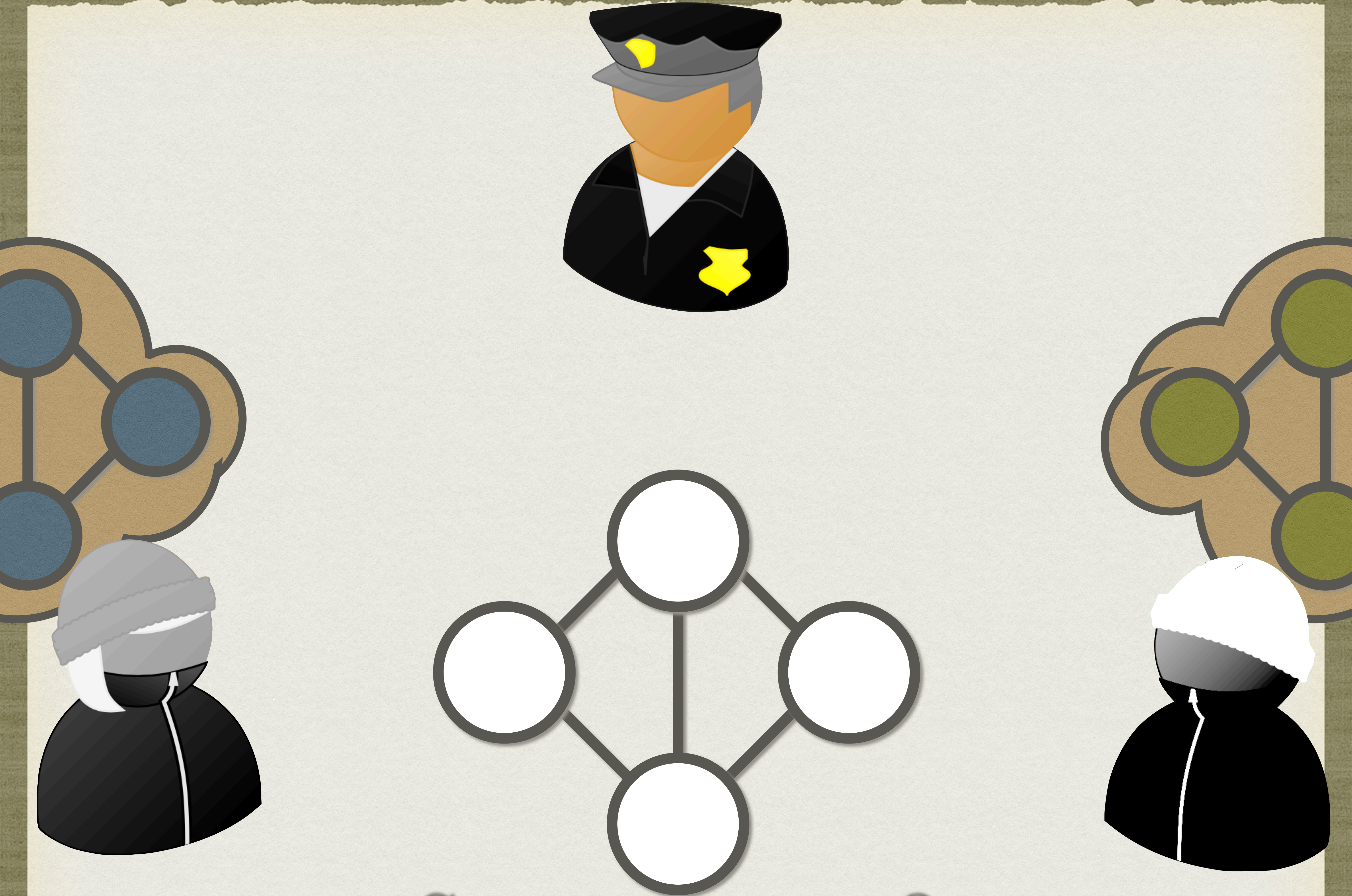
Consequences and Limits of Nonlocal Strategies

Richard Cleve Peter Høyer
Benjamin Toner John Watrous

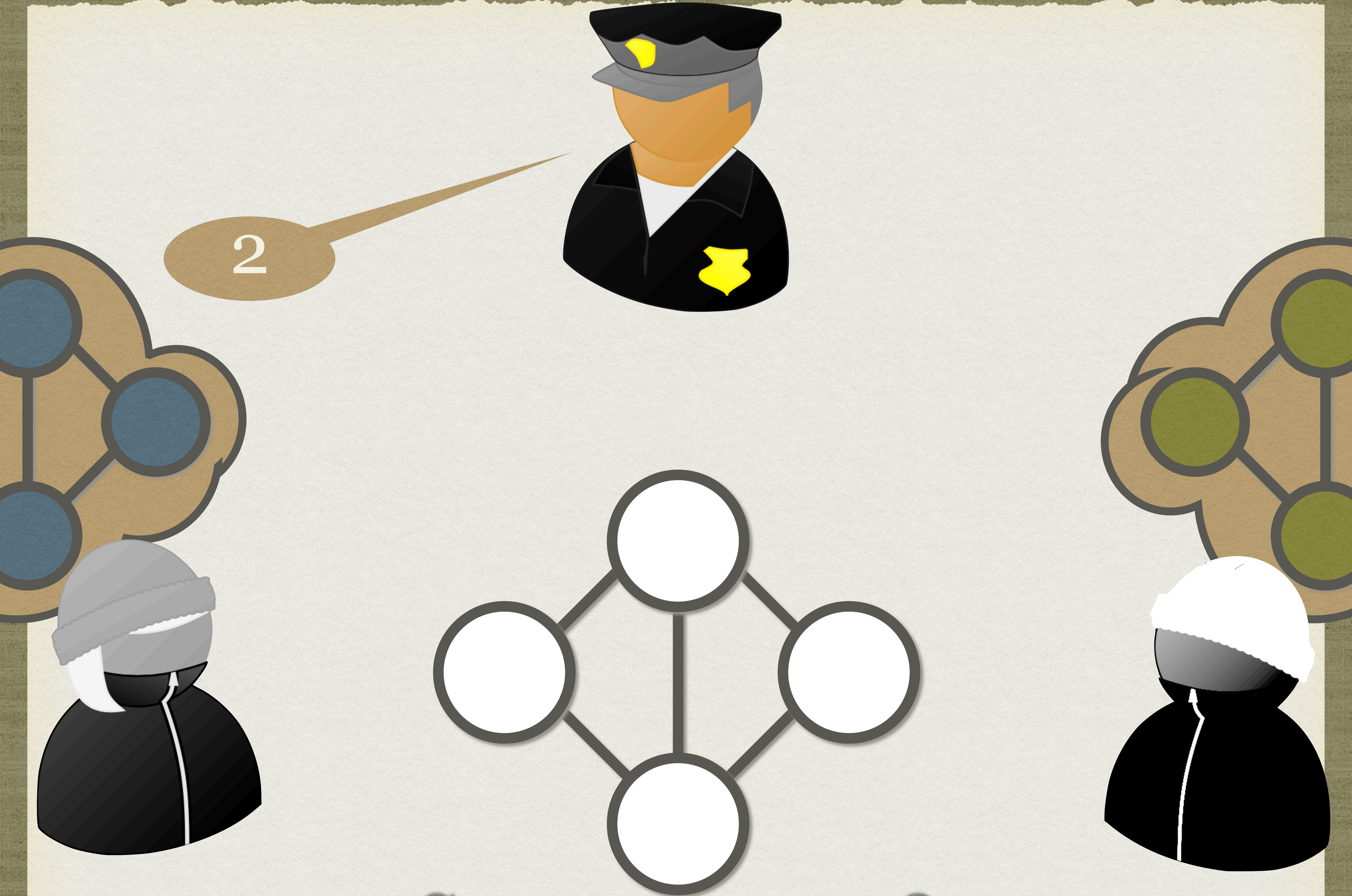


Consequences and Limits of Nonlocal Strategies

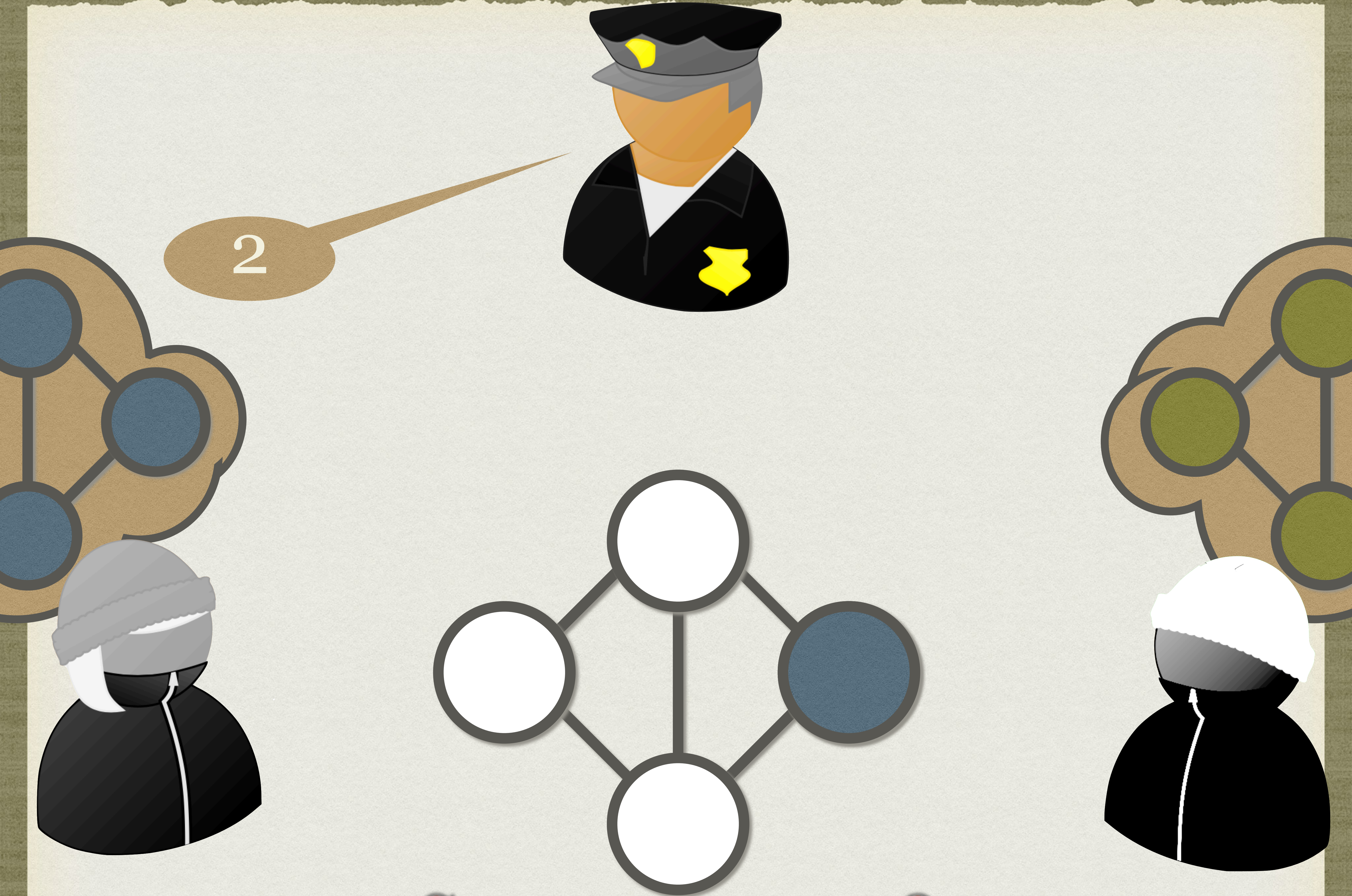
Richard Cleve
Peter Høyer
Benjamin Toner
John Watrous



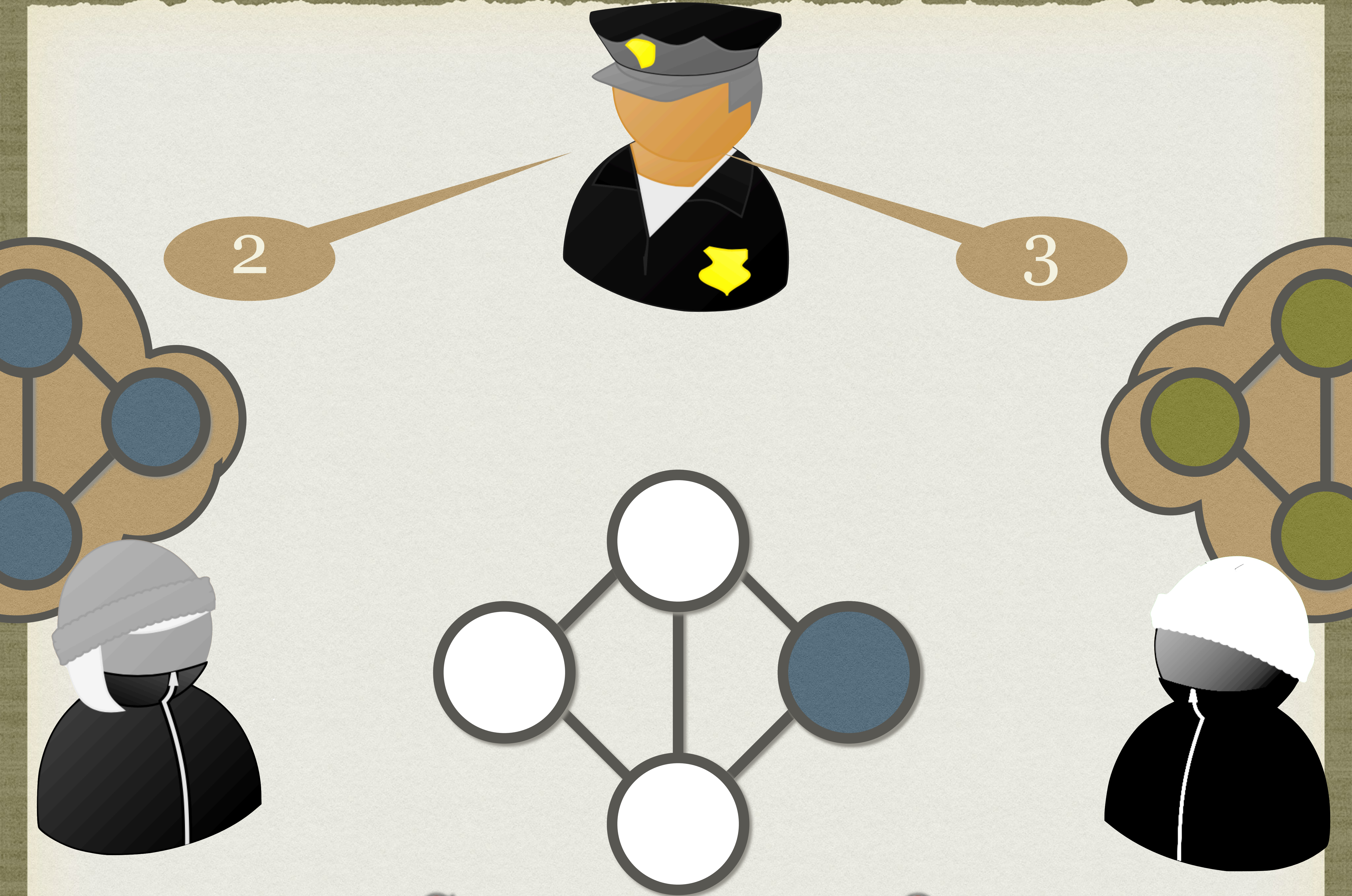
Soundness ?



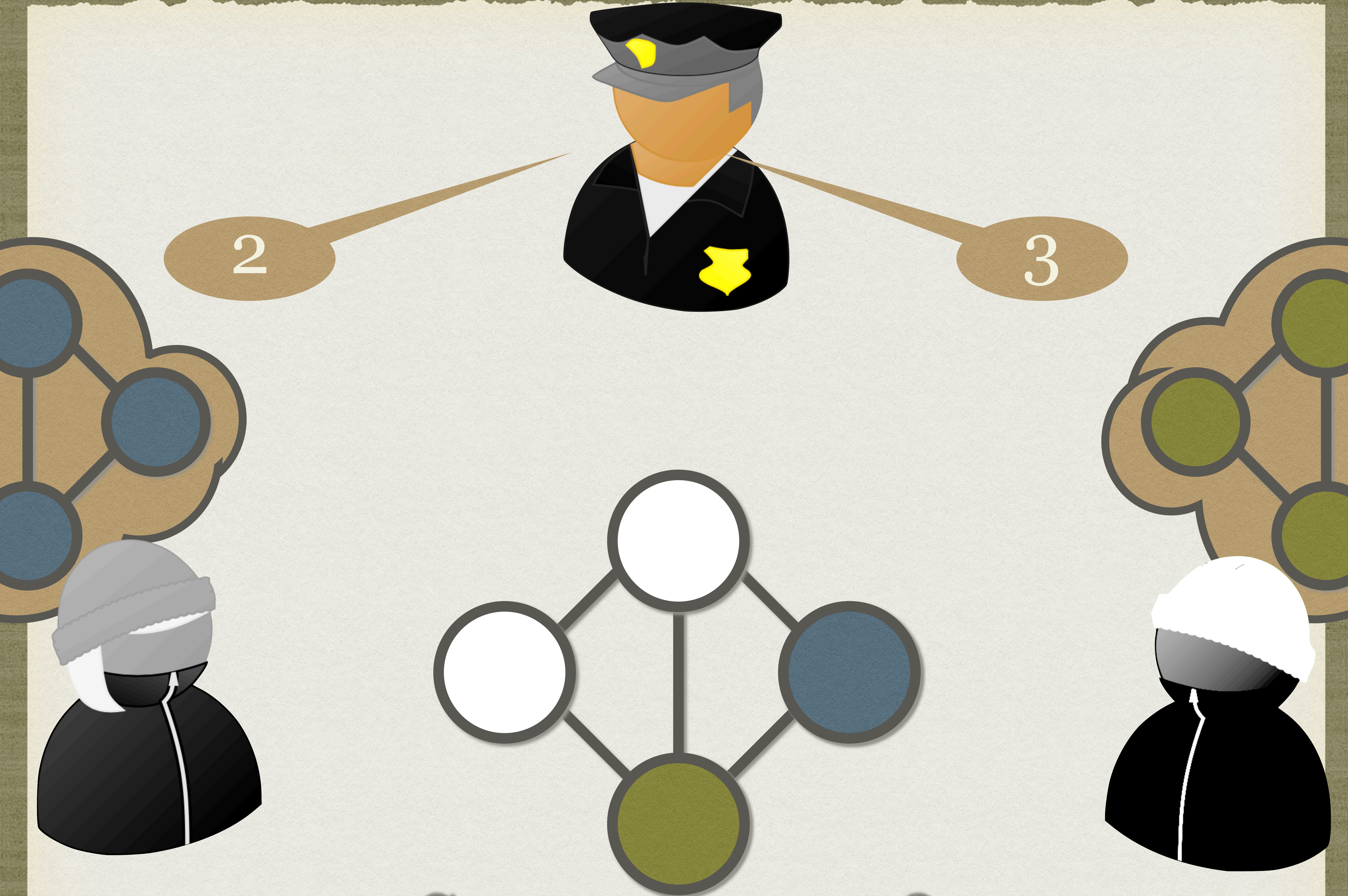
Soundness ?



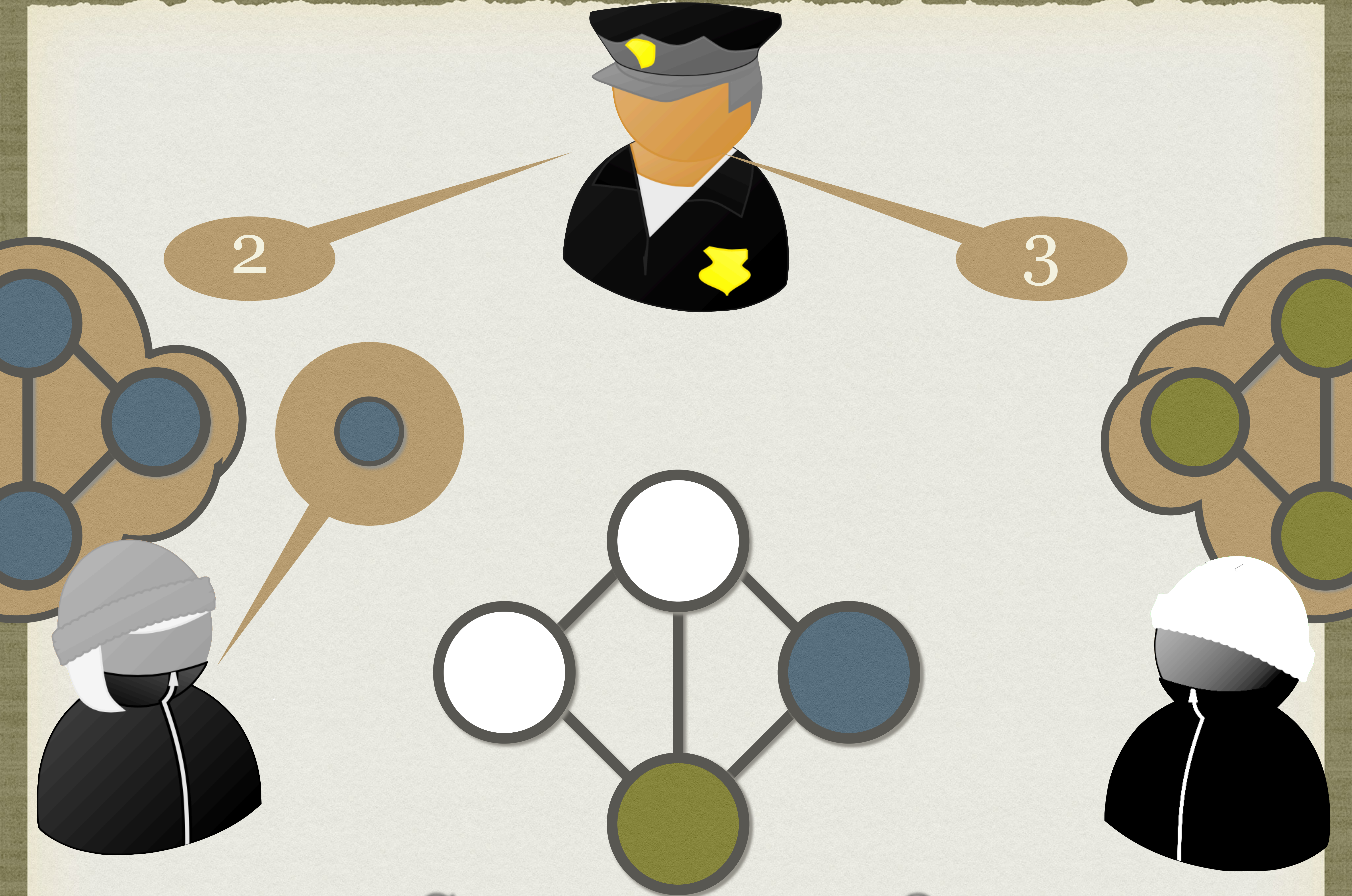
SOUNDNESS ?



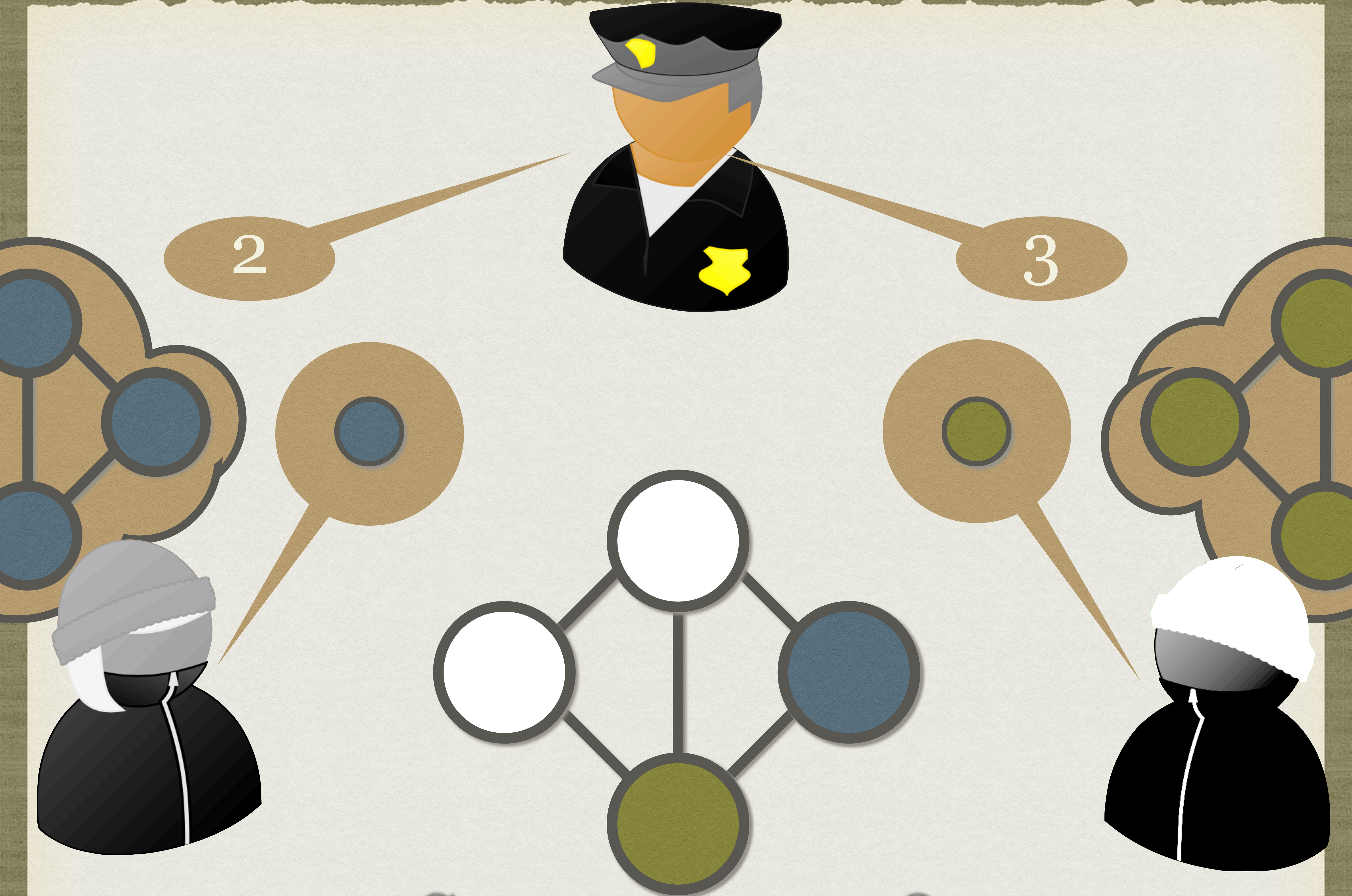
SOUNDNESS ?



SOUNDNESS ?

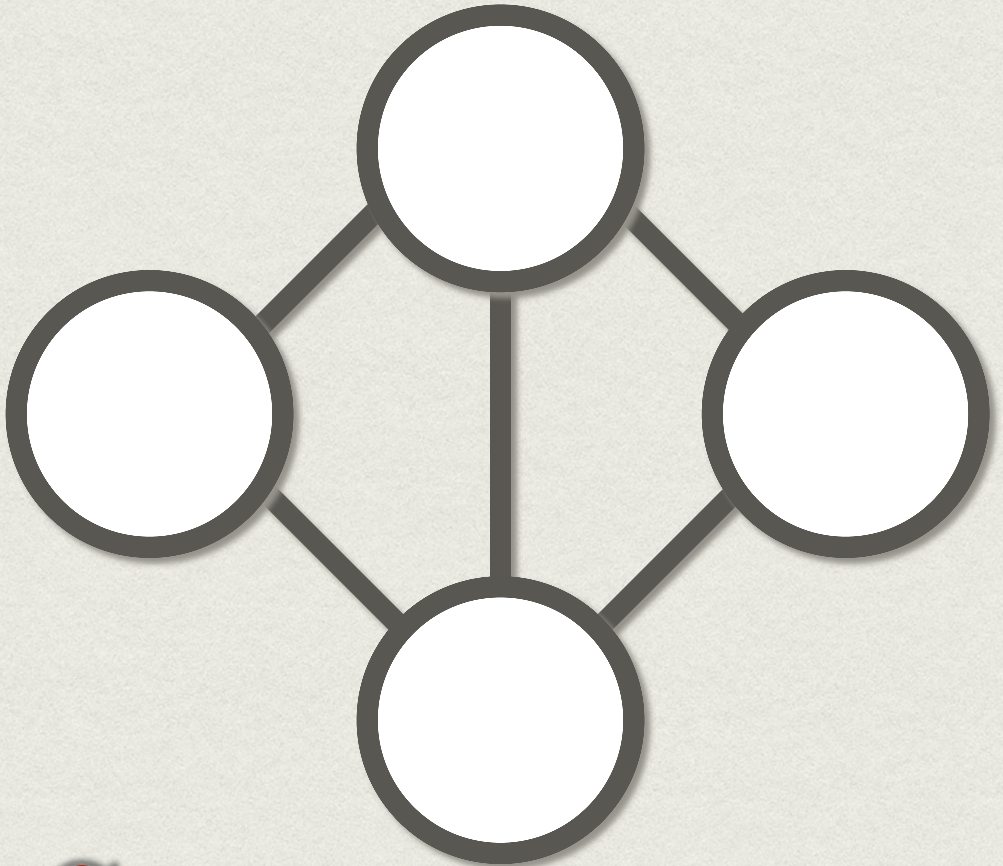


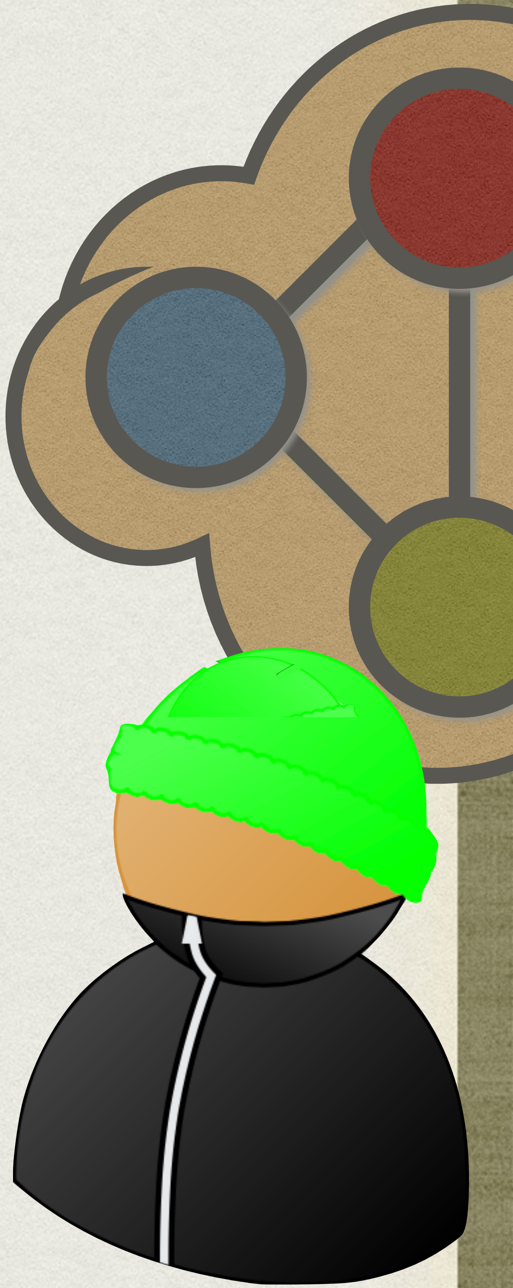
SOUNDNESS ?



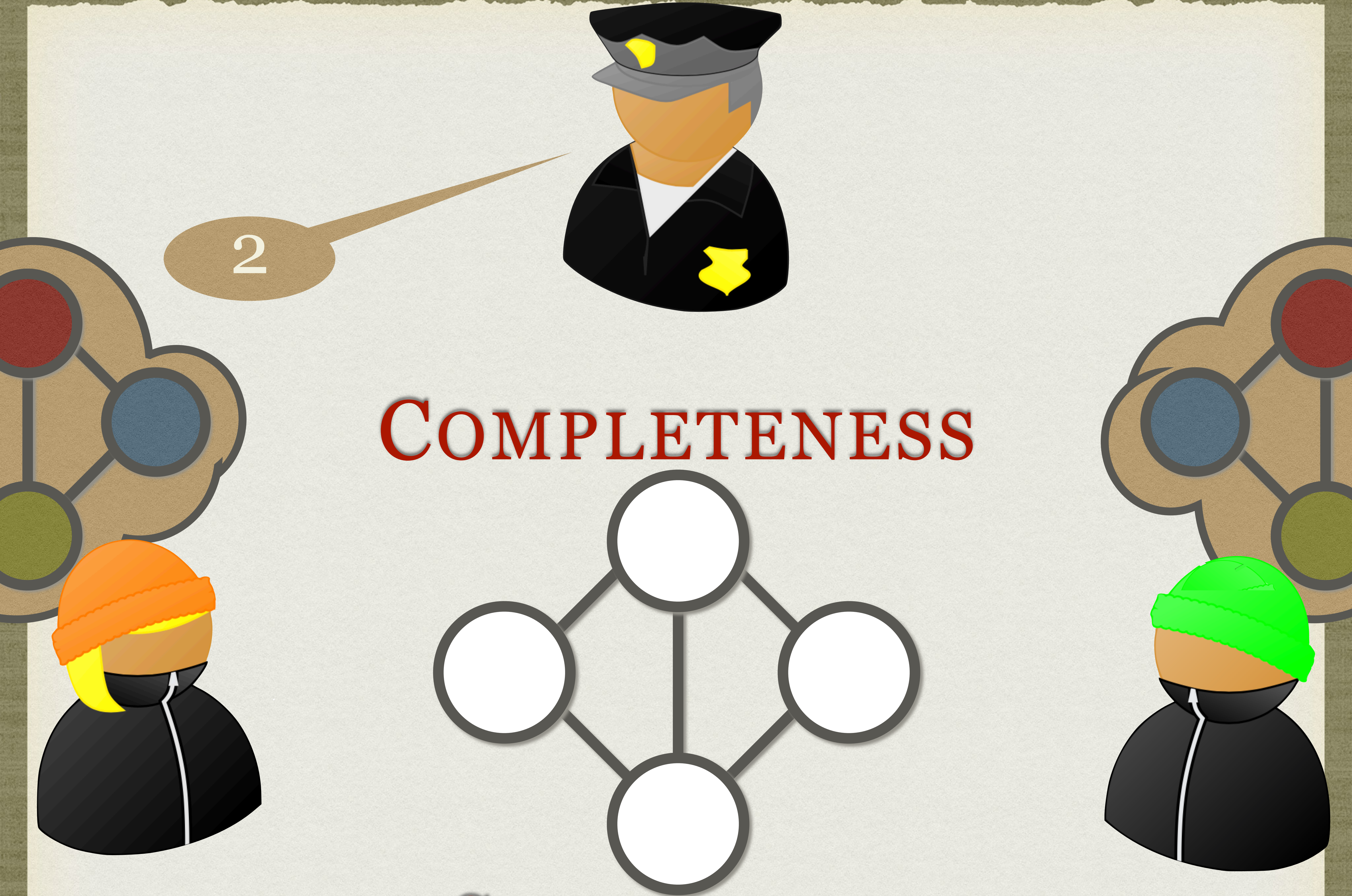
SOUNDNESS ?

Completeness



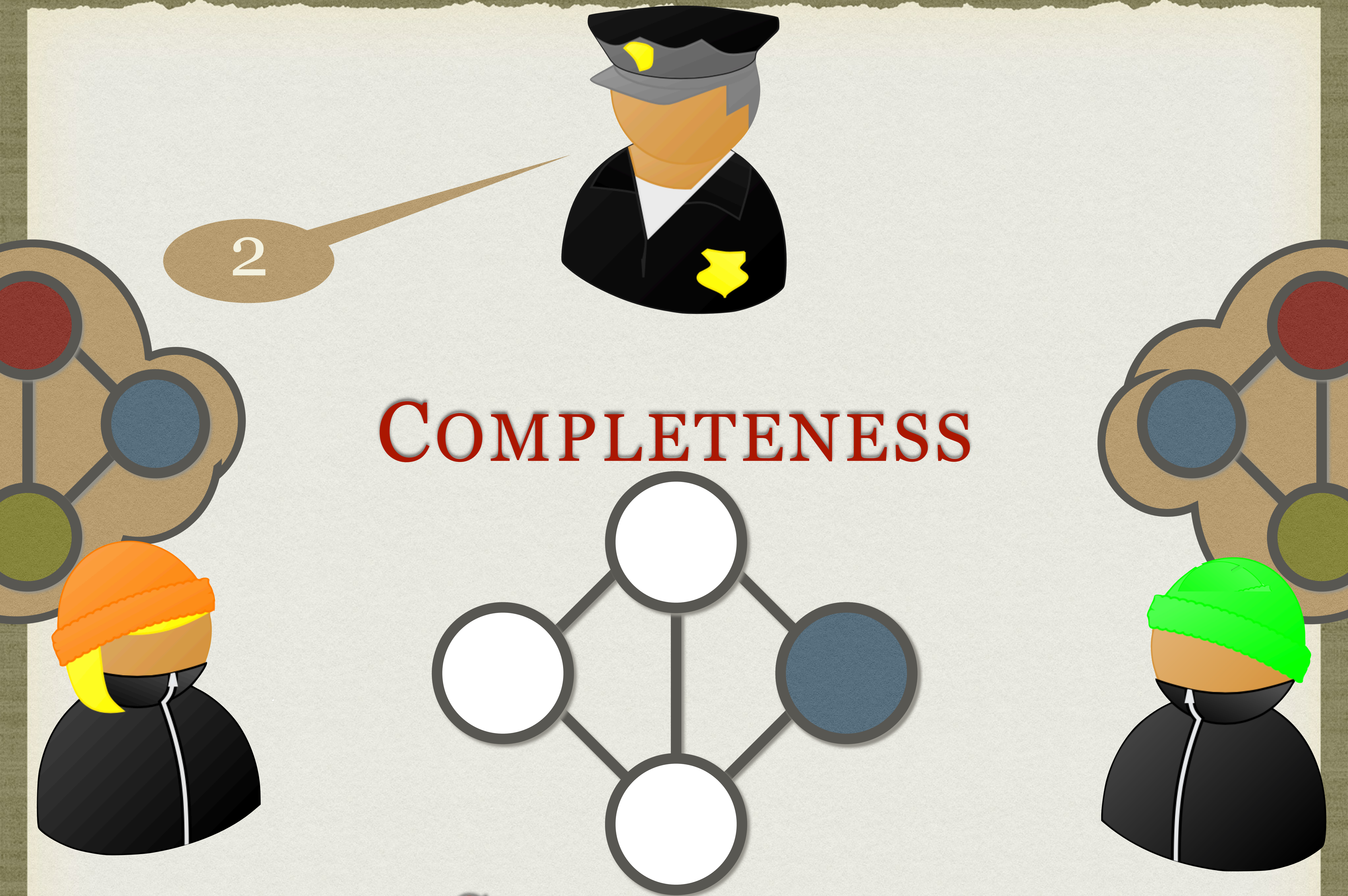


Soundness



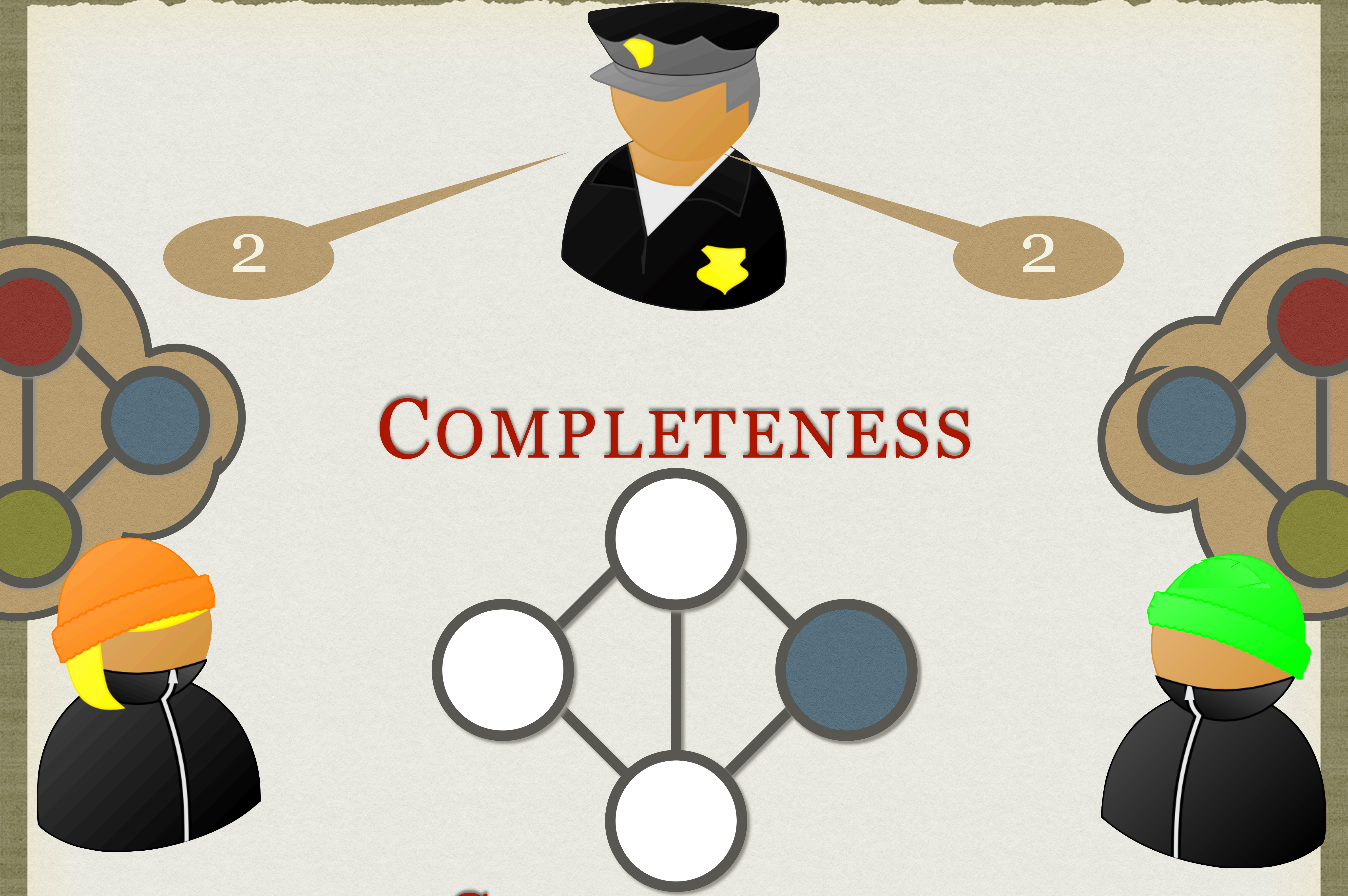
Completeness

Soundness



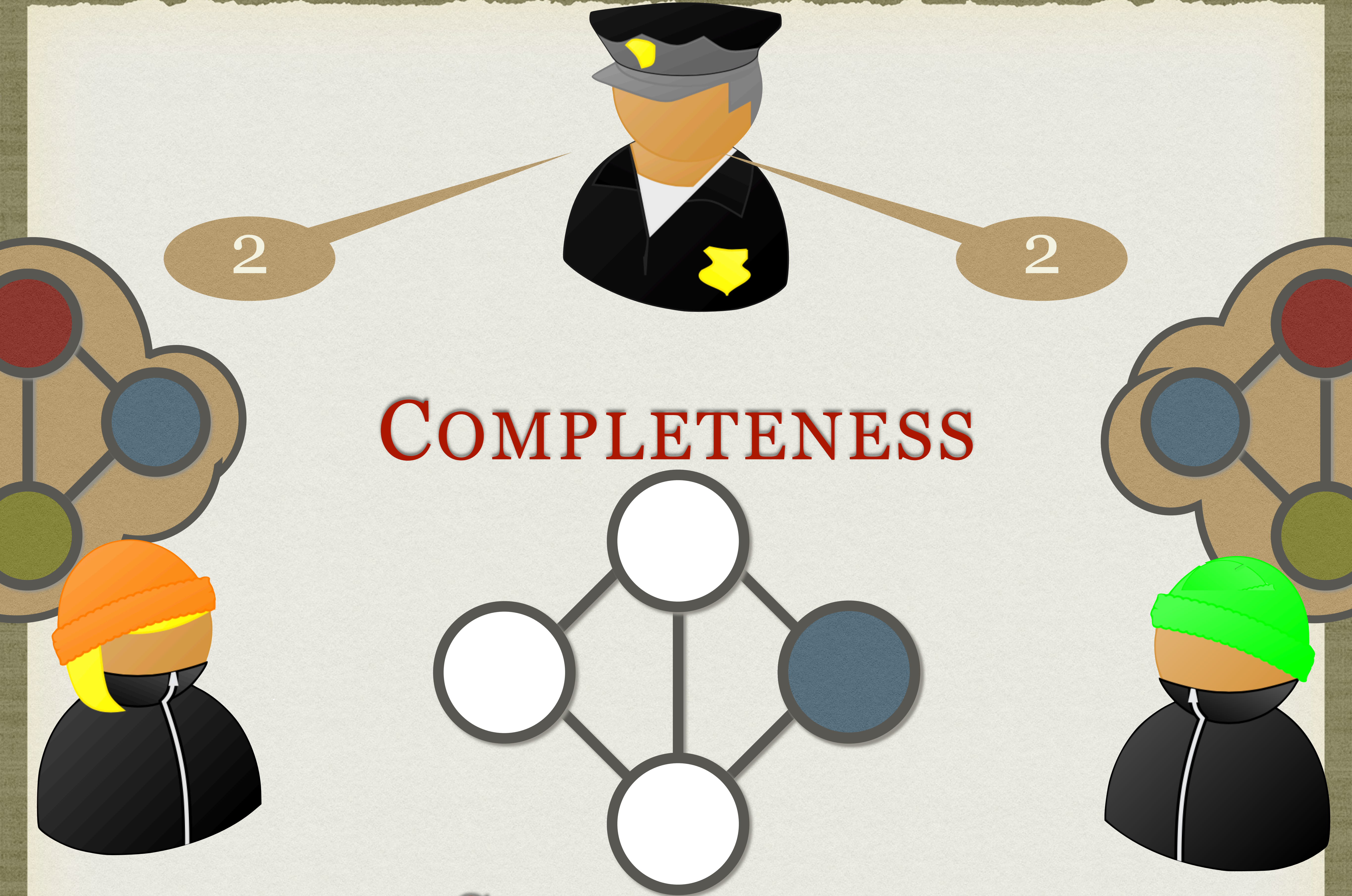
Completeness

Soundness



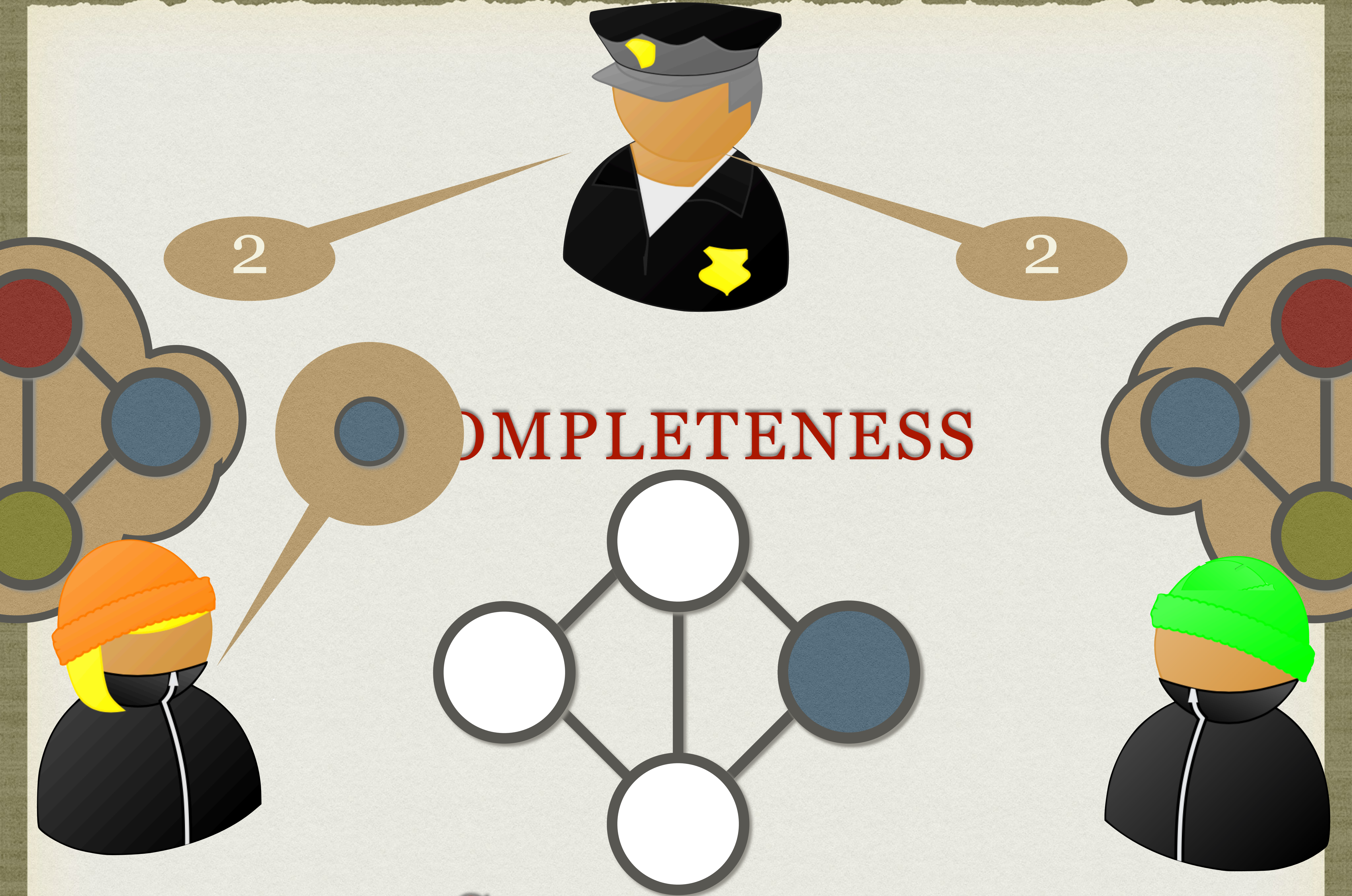
COMPLETENESS

SOUNDNESS



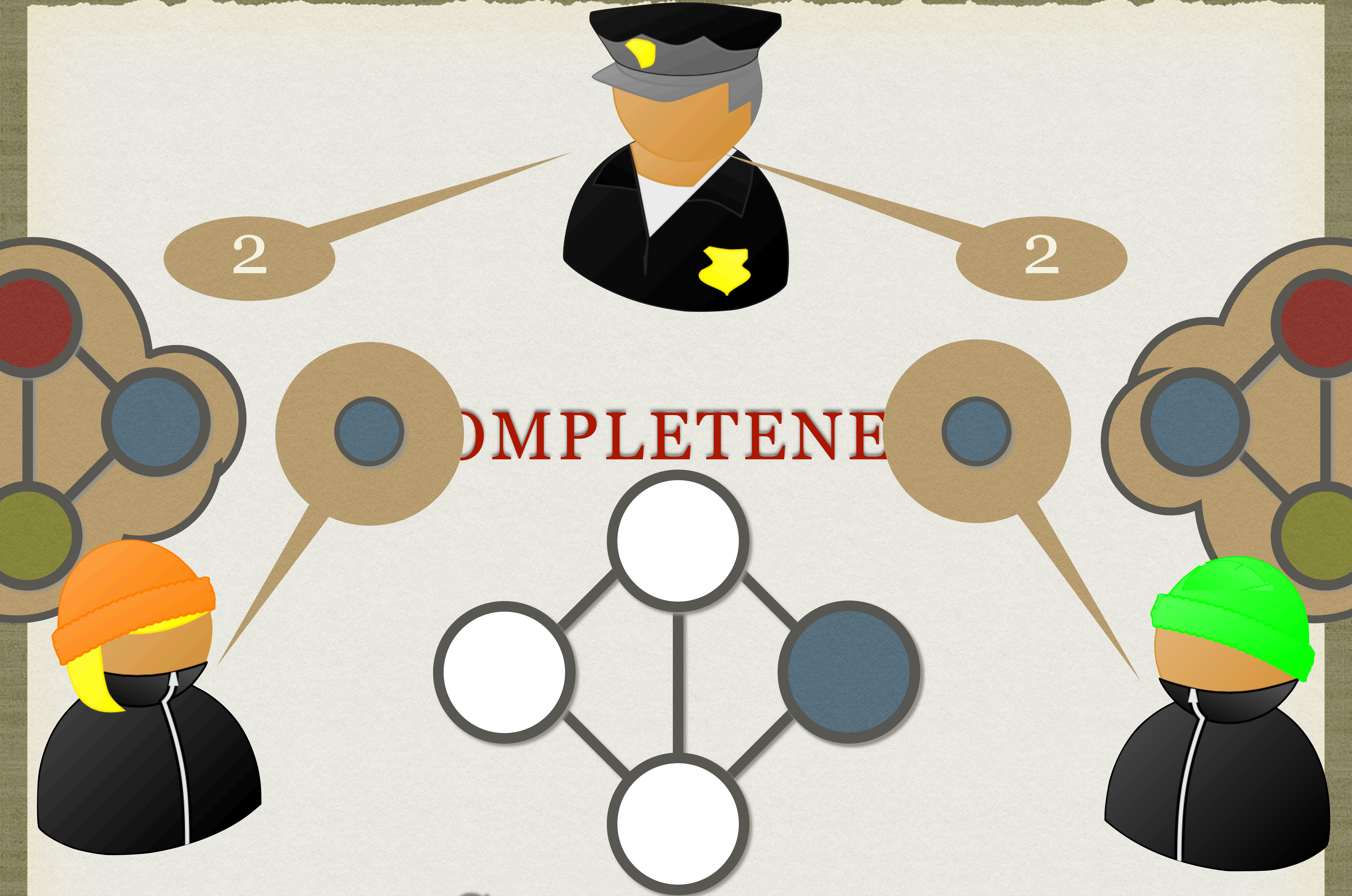
Completeness

Soundness



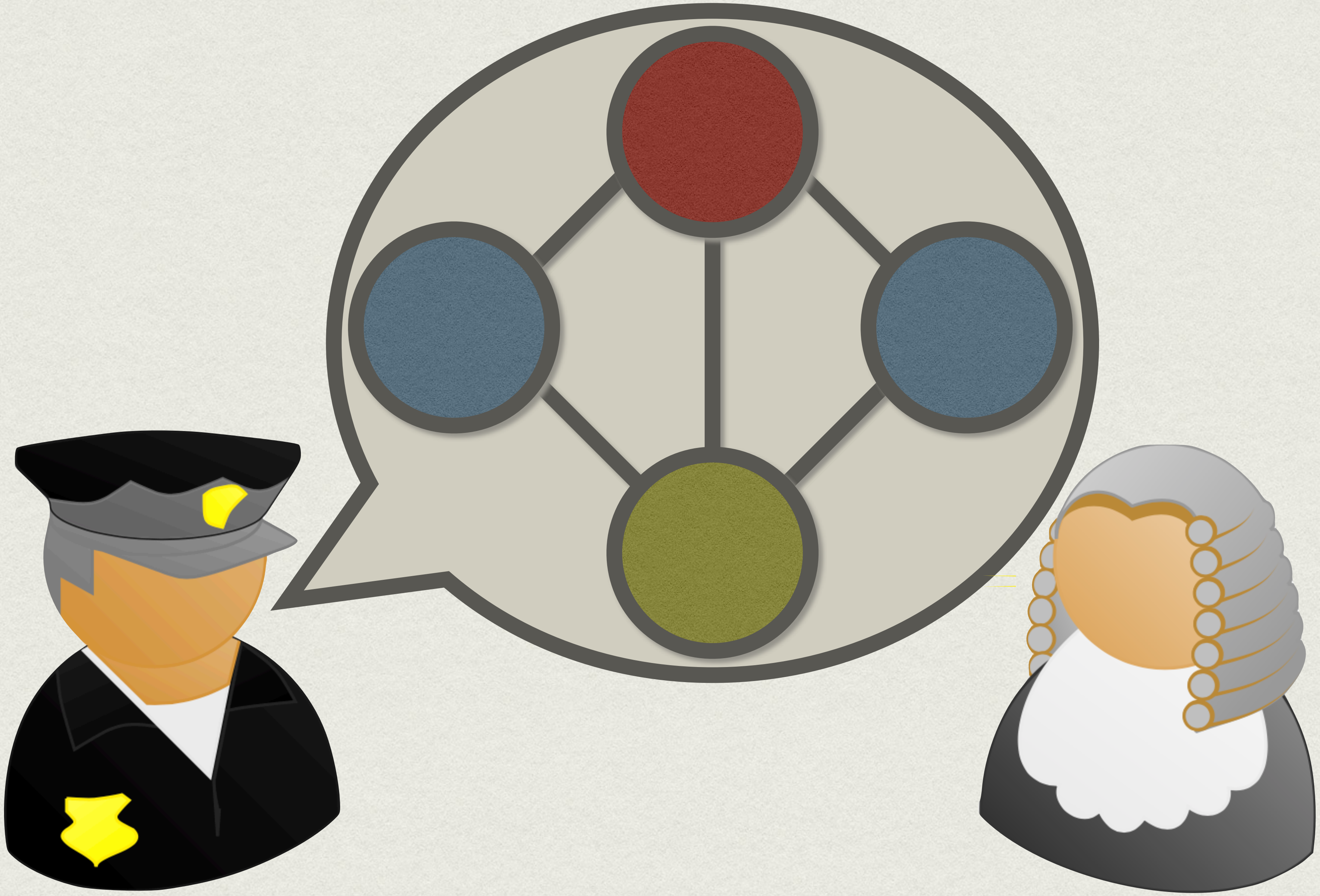
ompleteness

Soundness

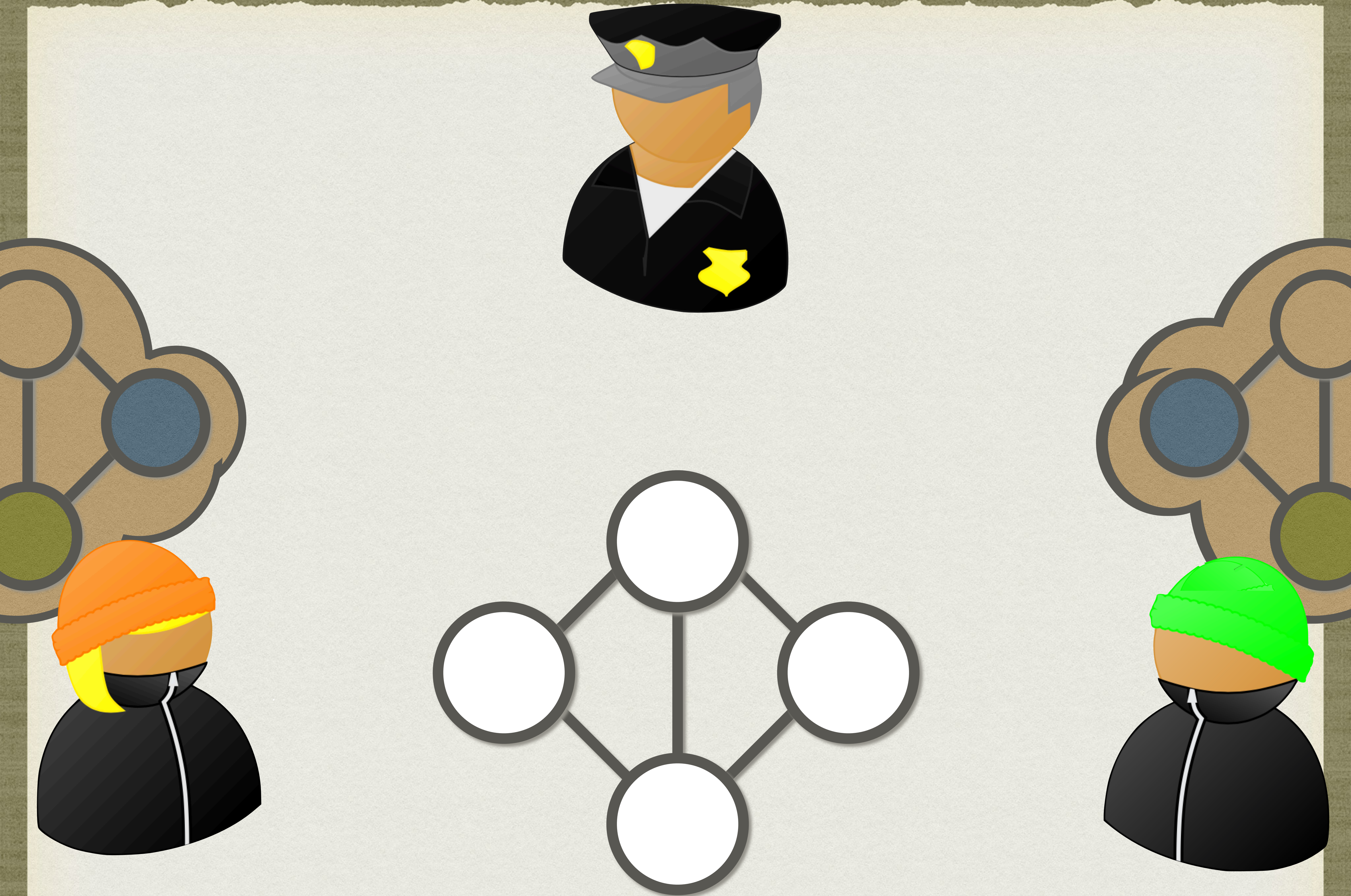


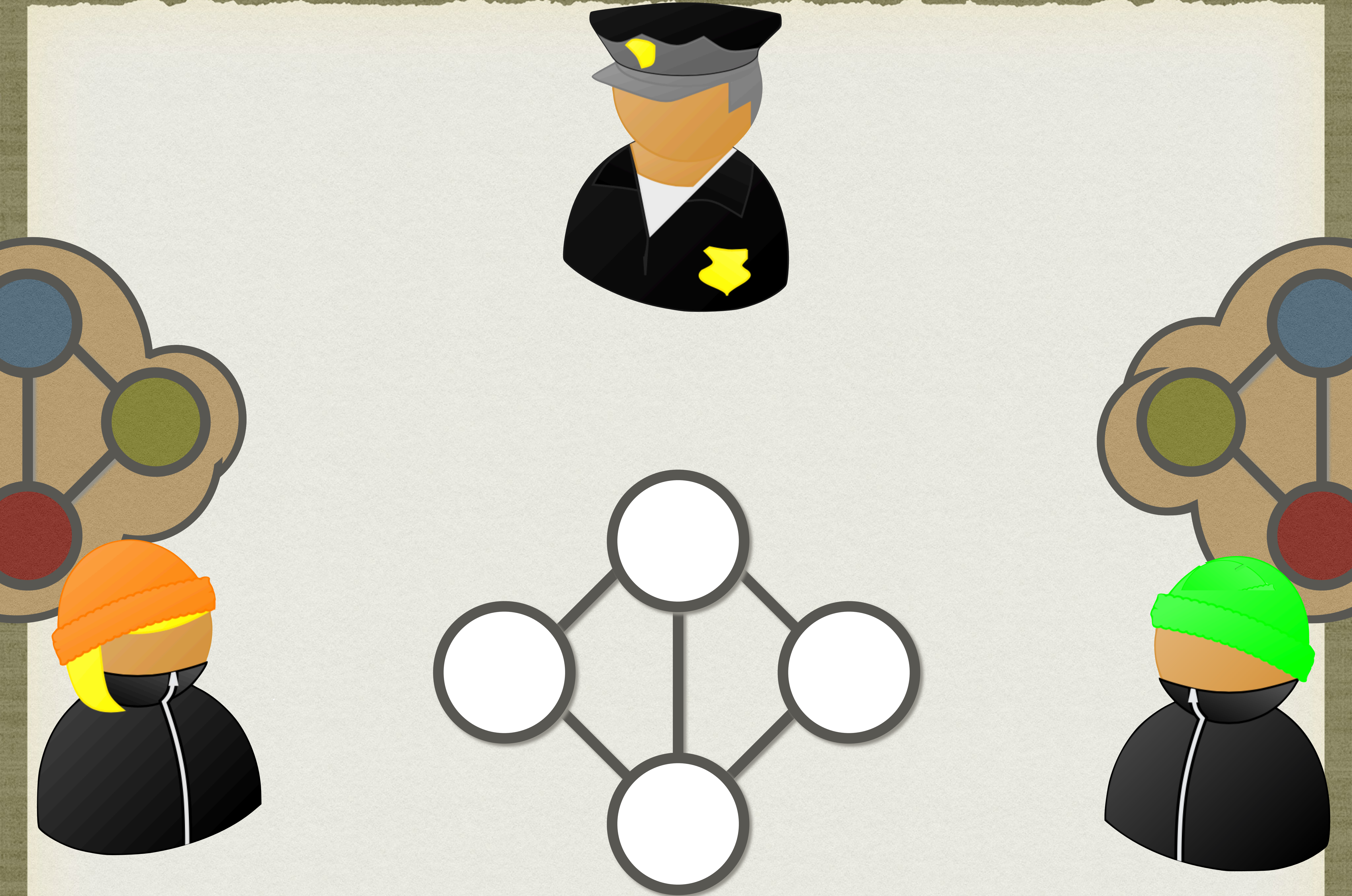
OMPLETENE

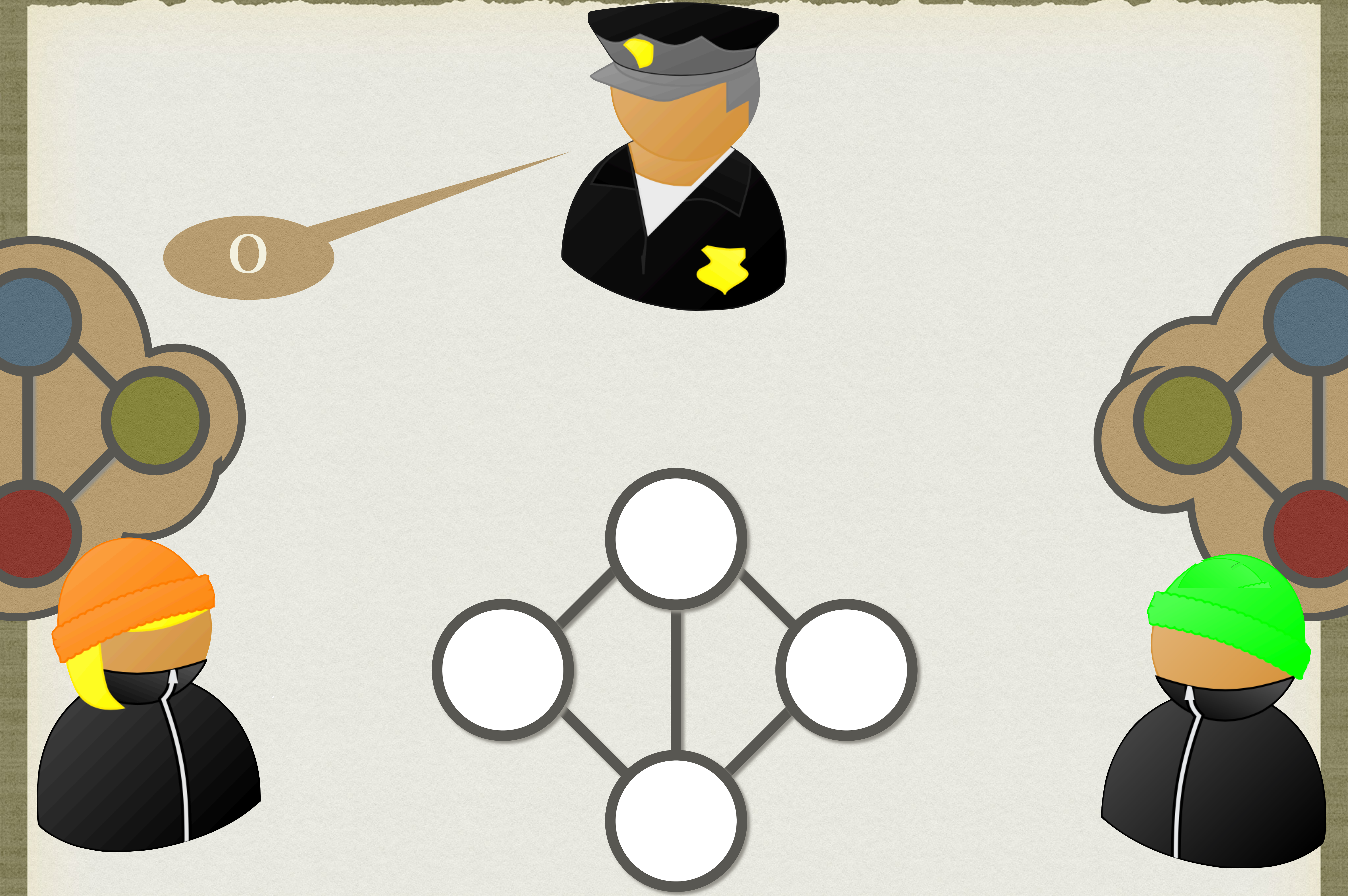
SOUNDNESS



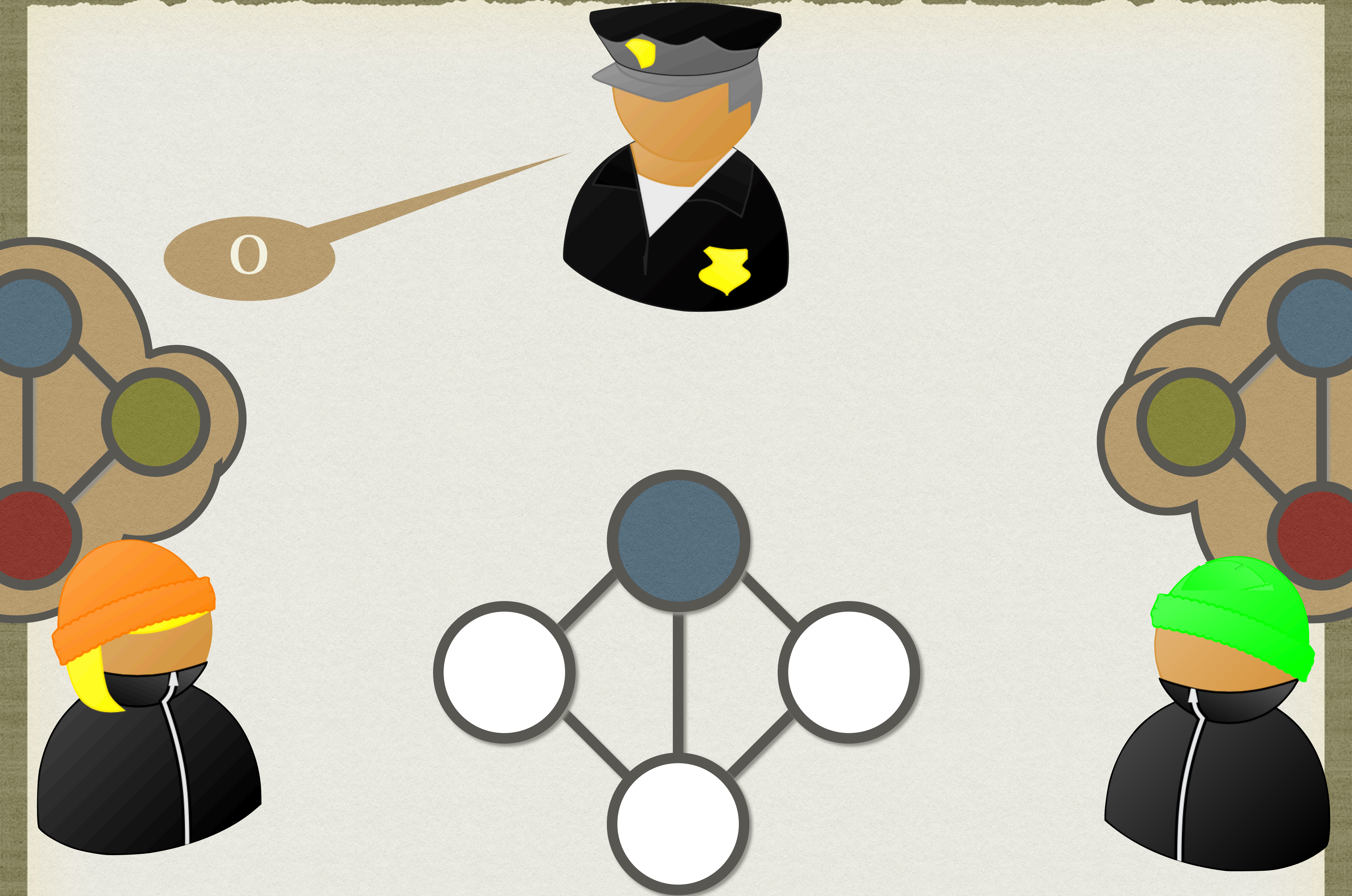
TRANSFERABLE

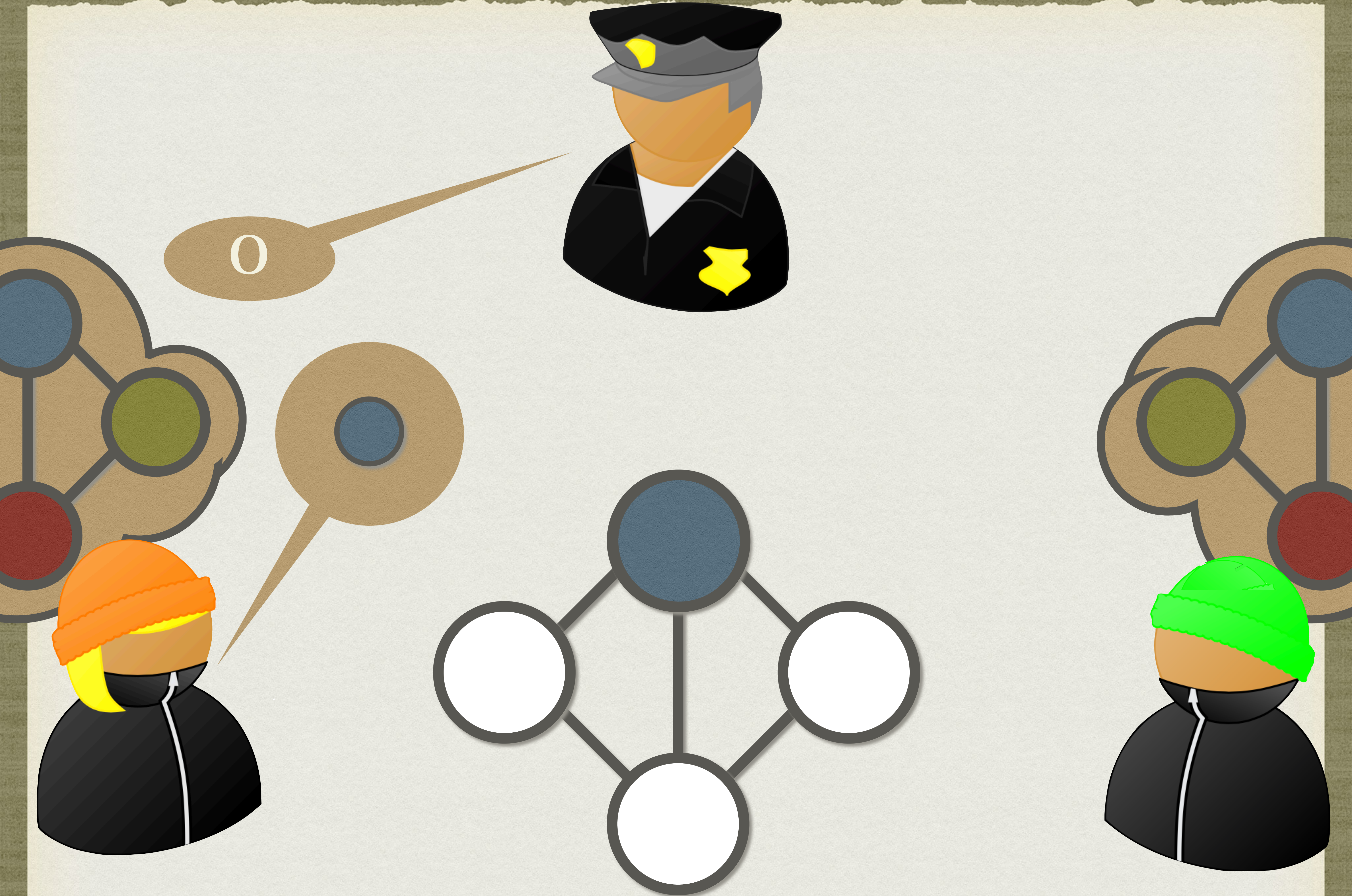


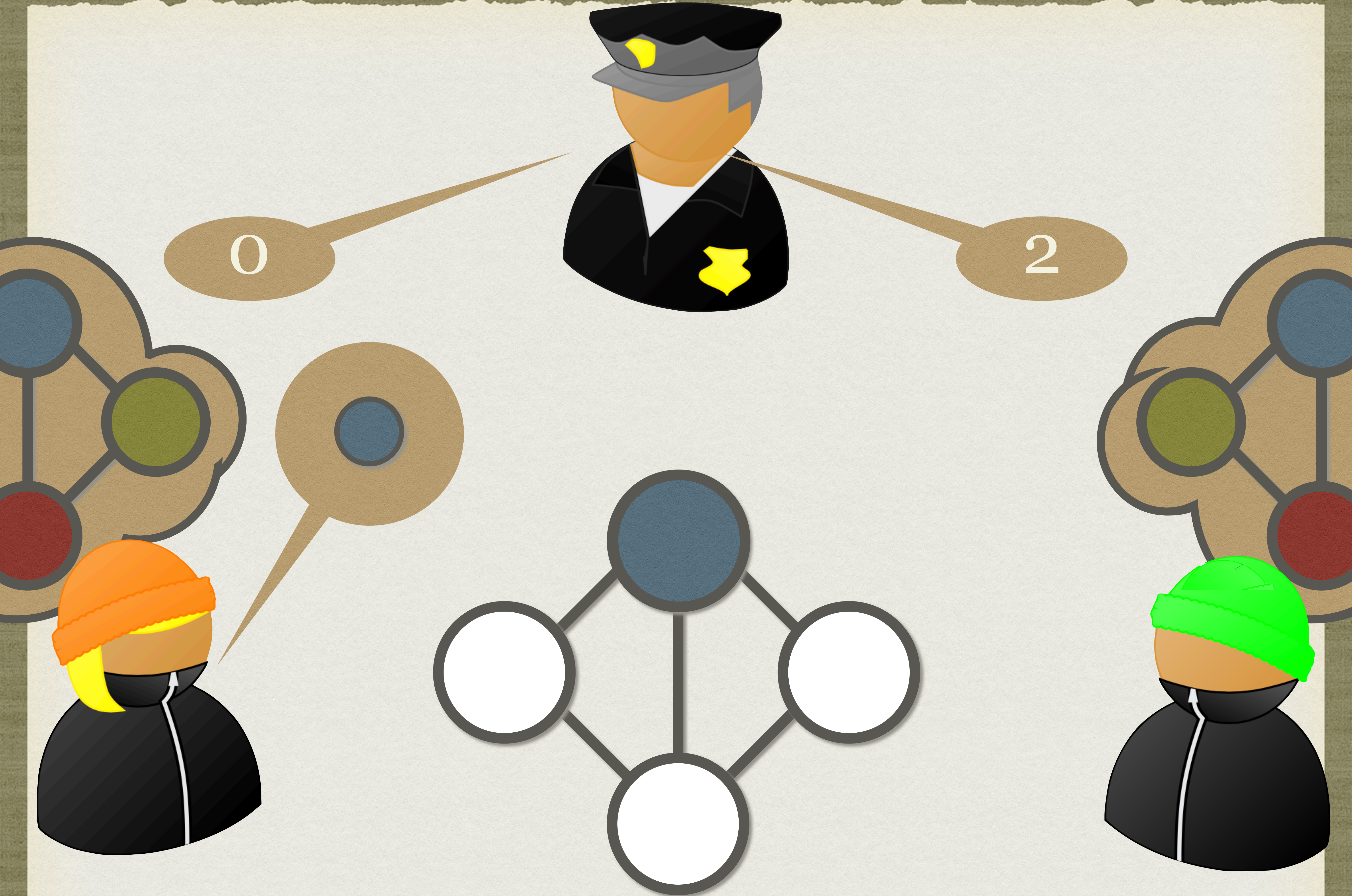


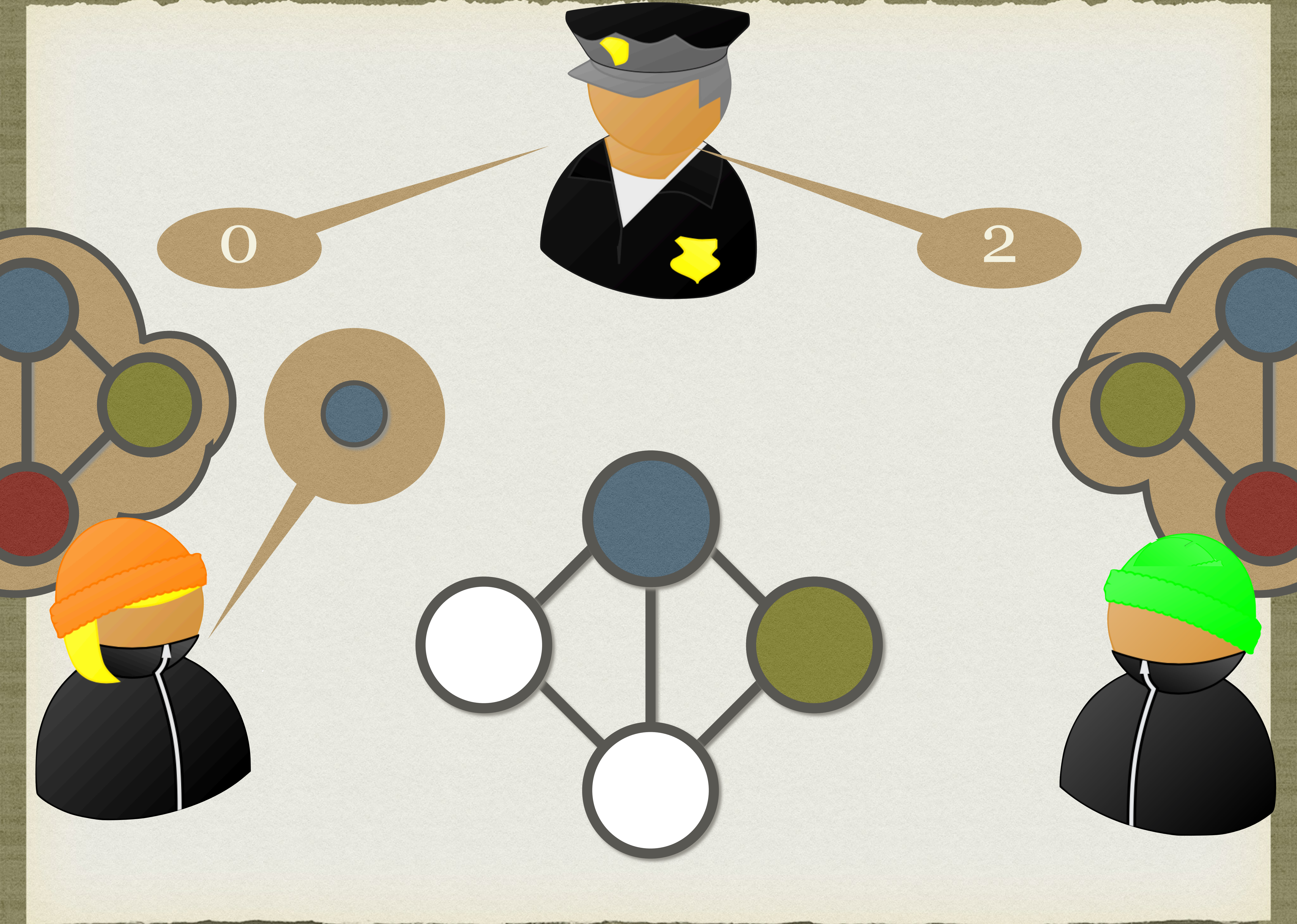


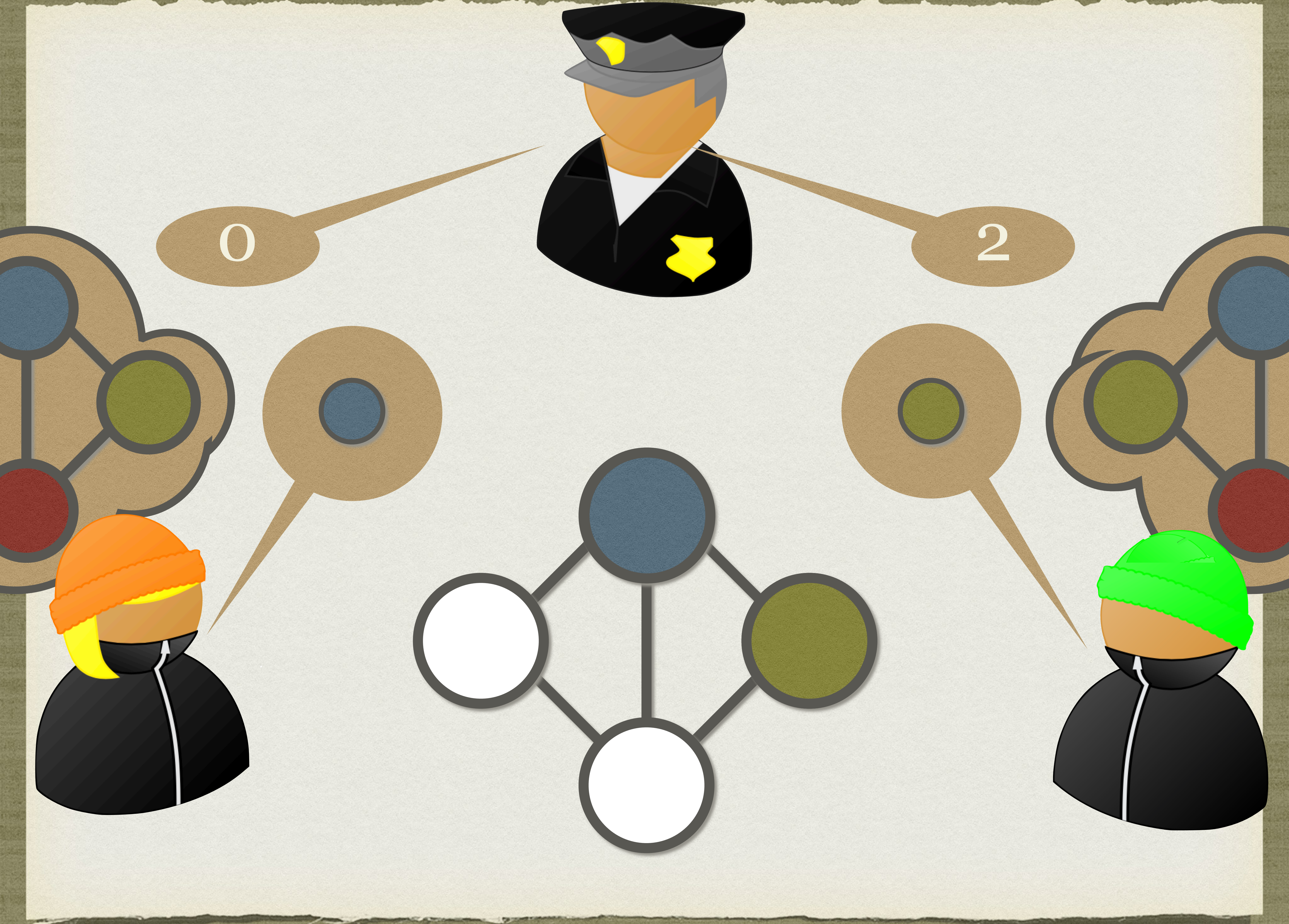
0

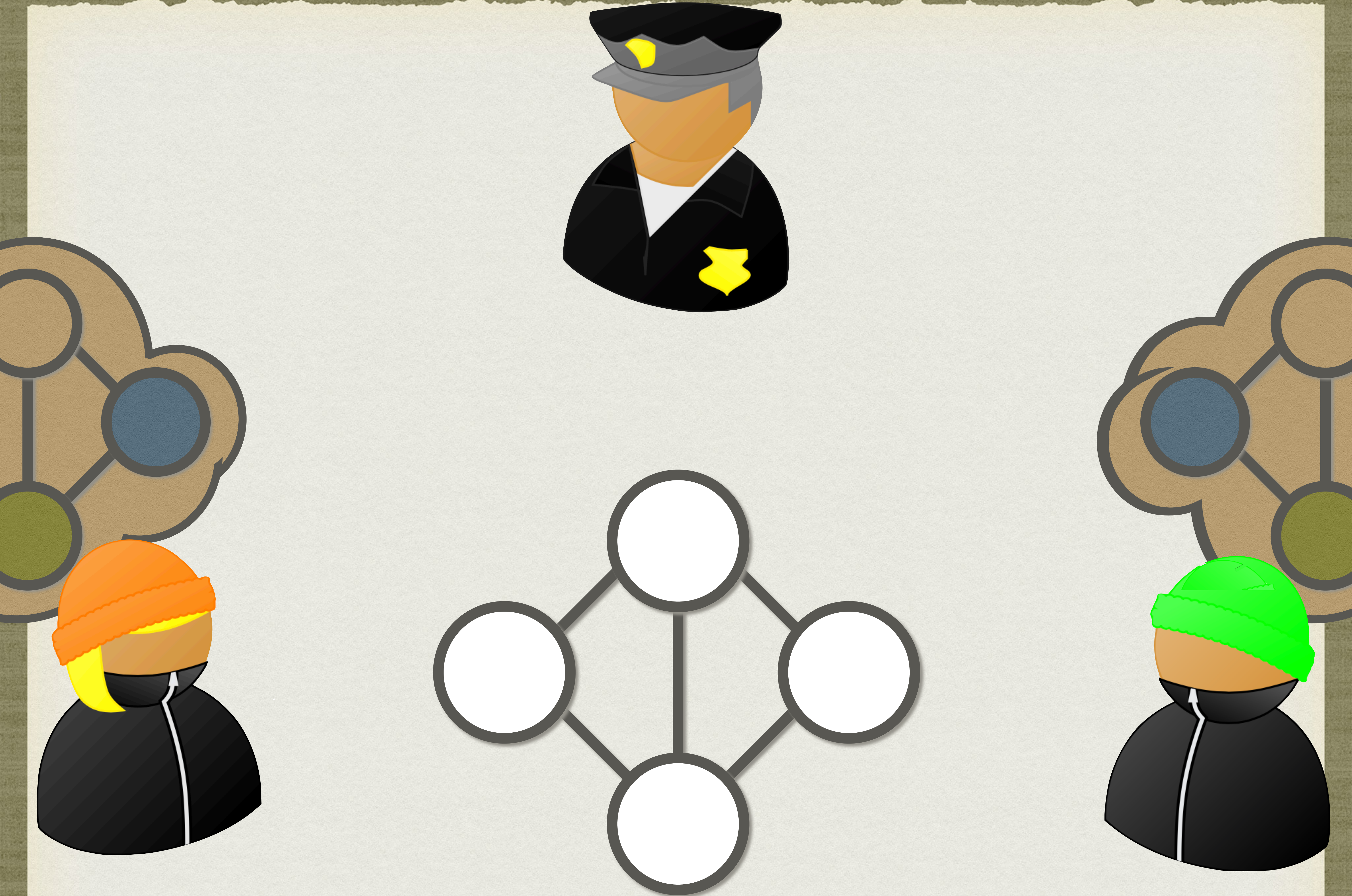

0

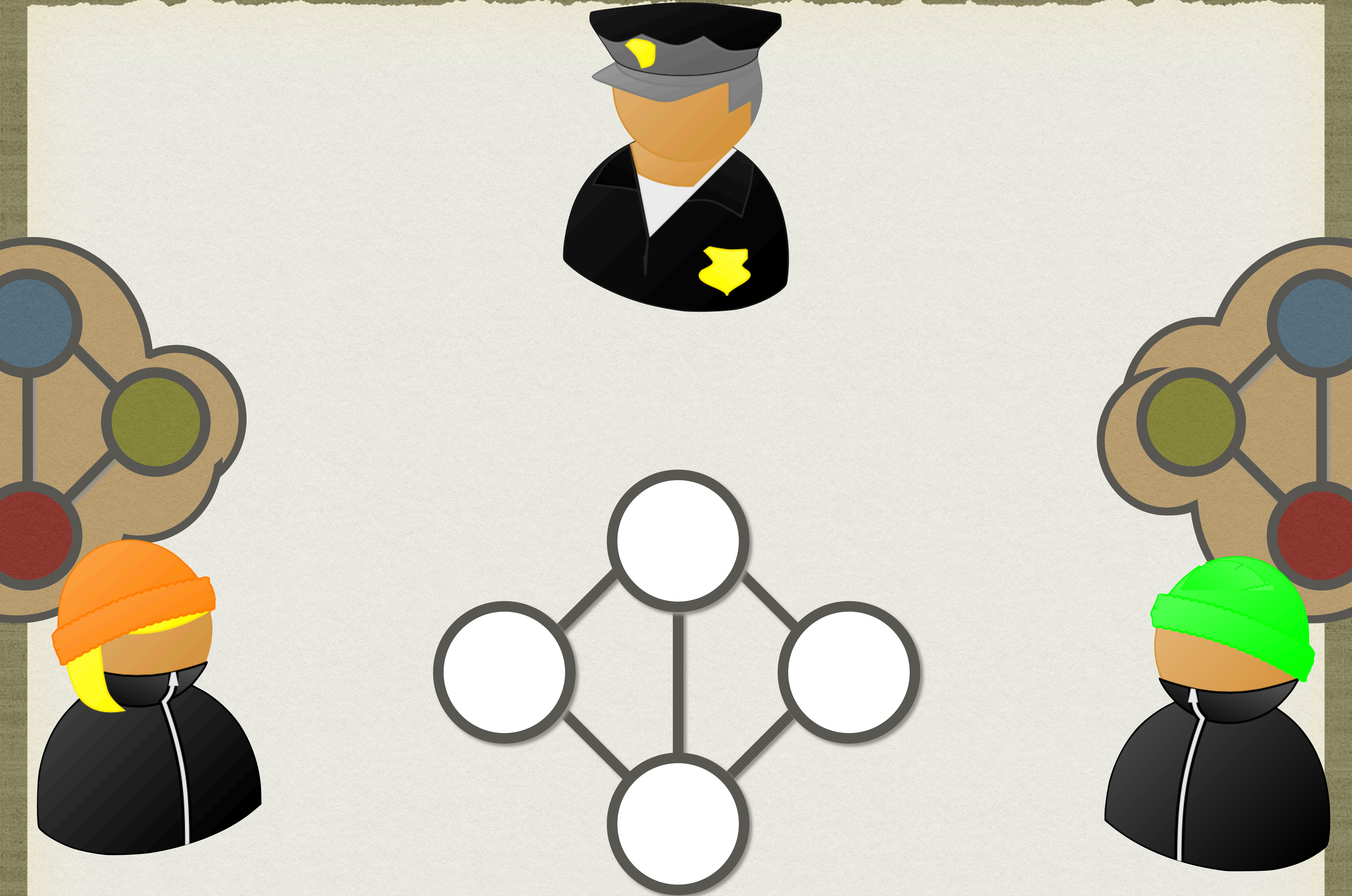

0

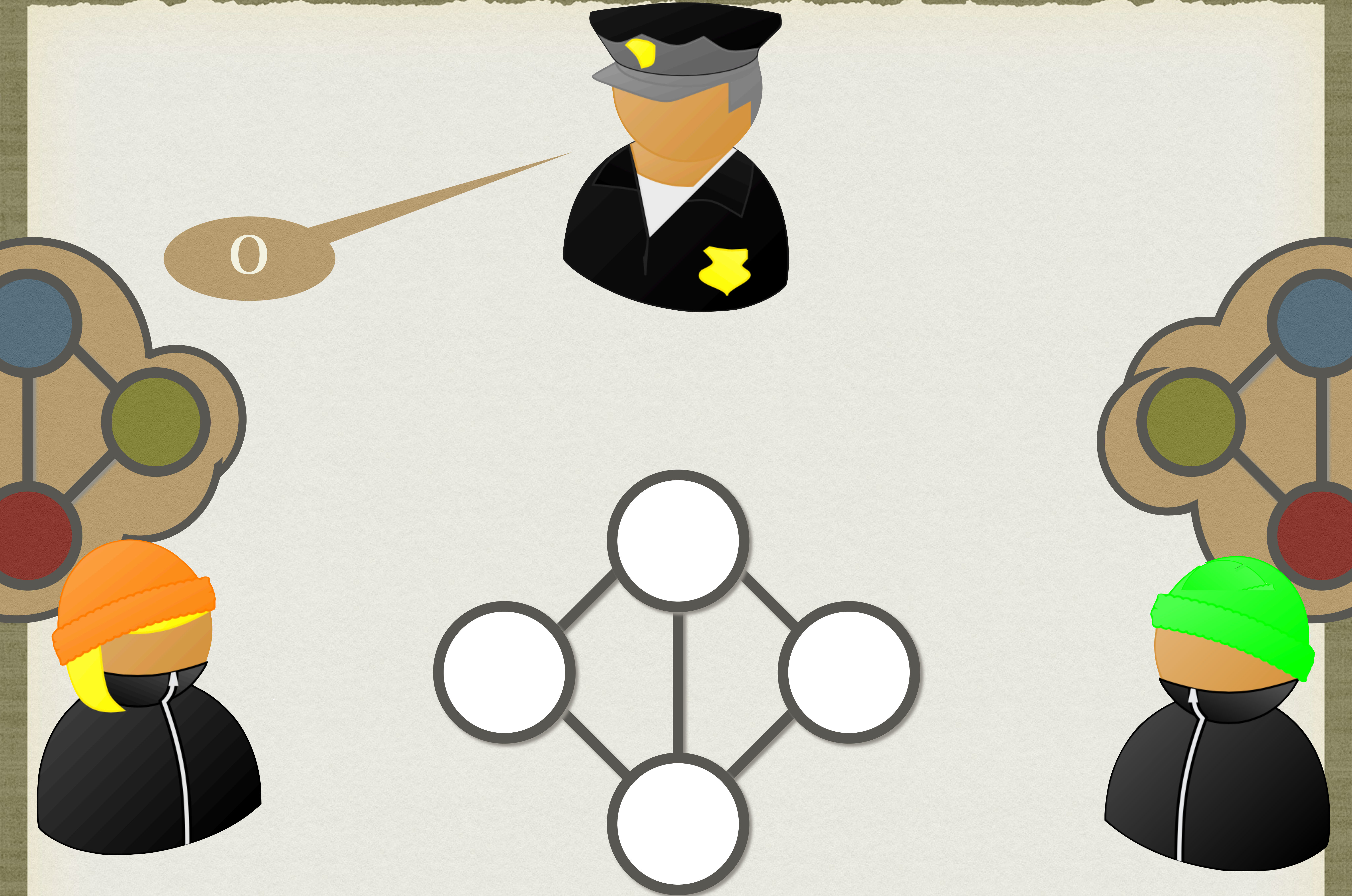

0
2

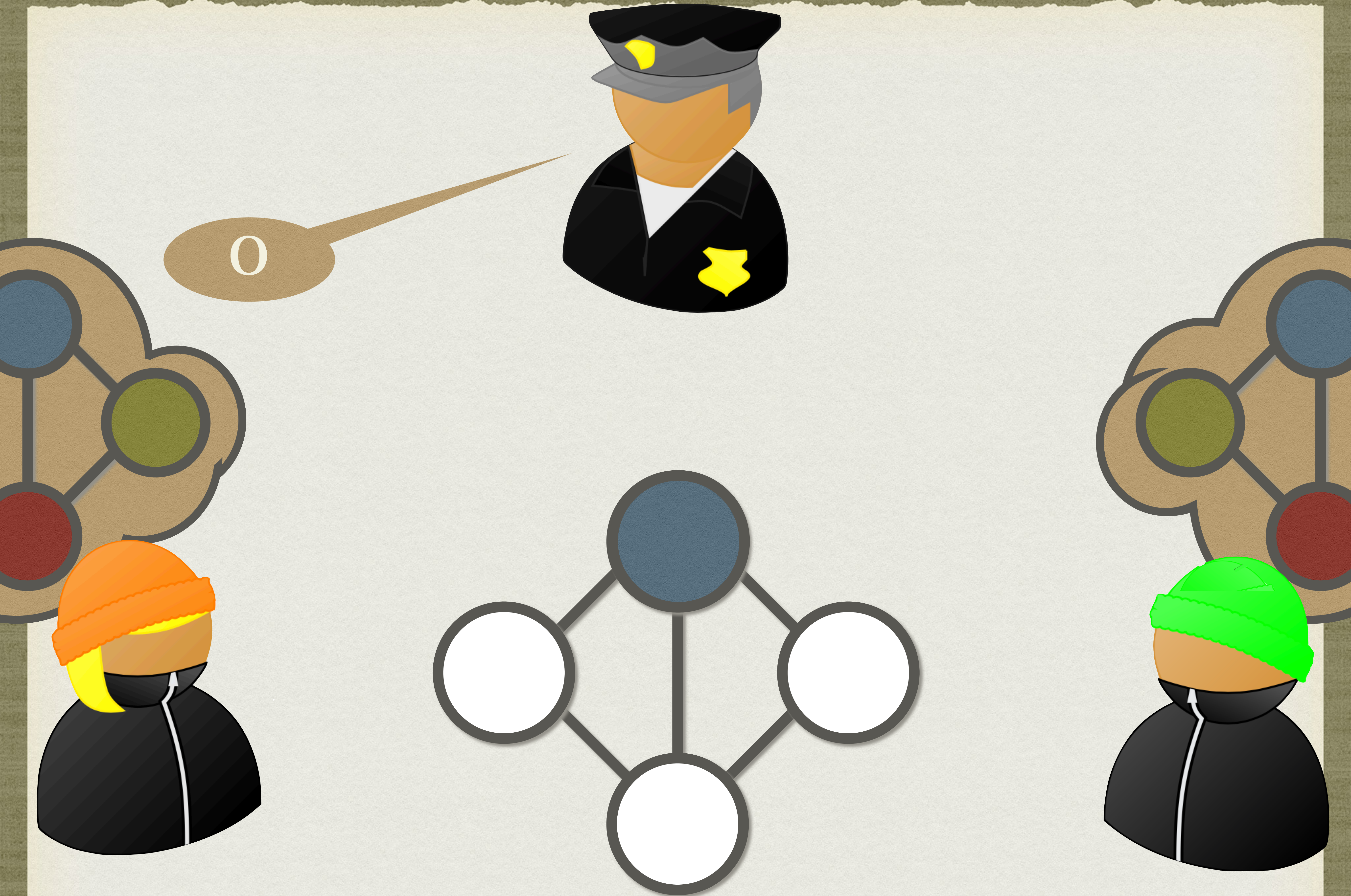

0
2

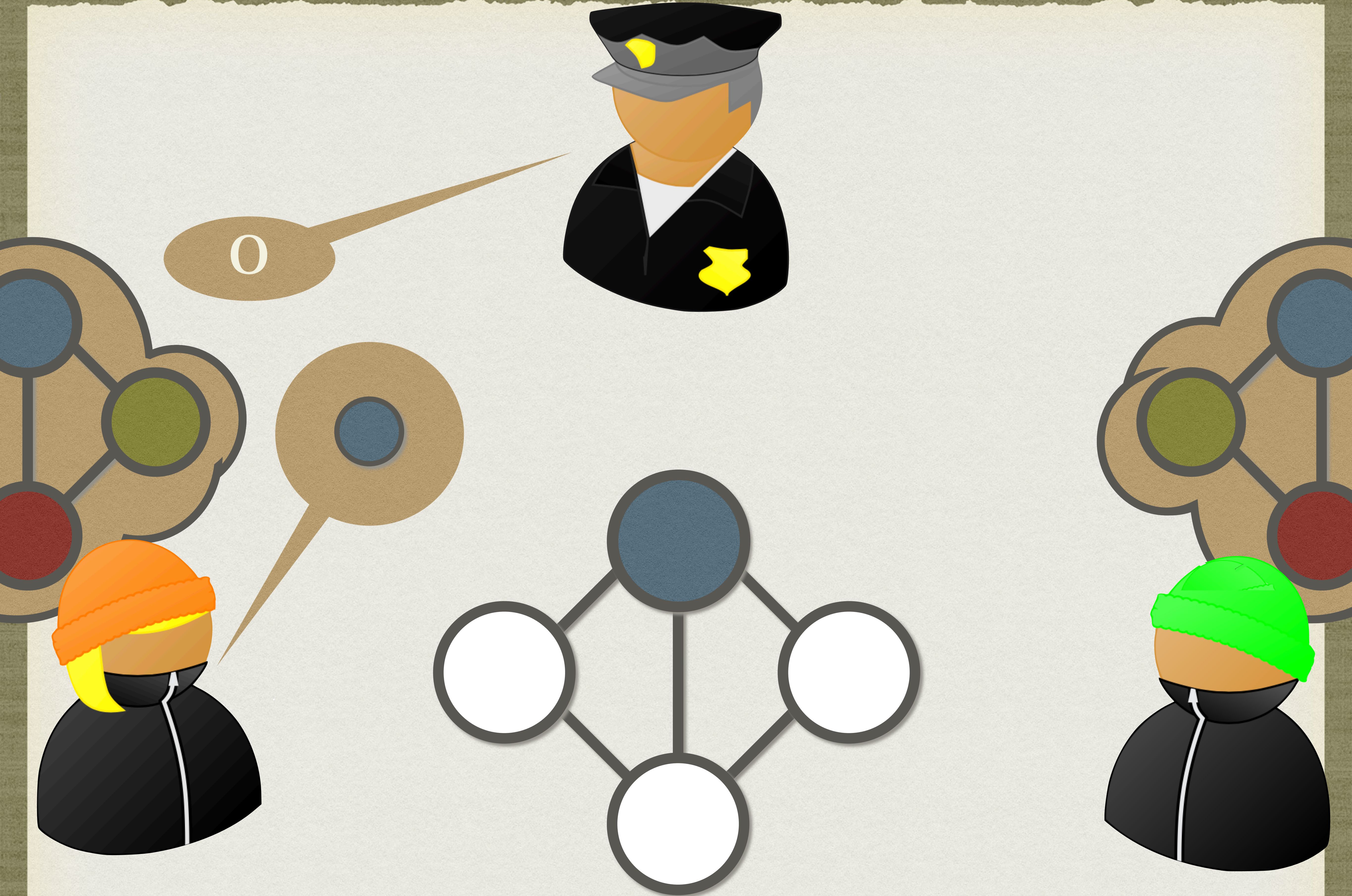

0
2

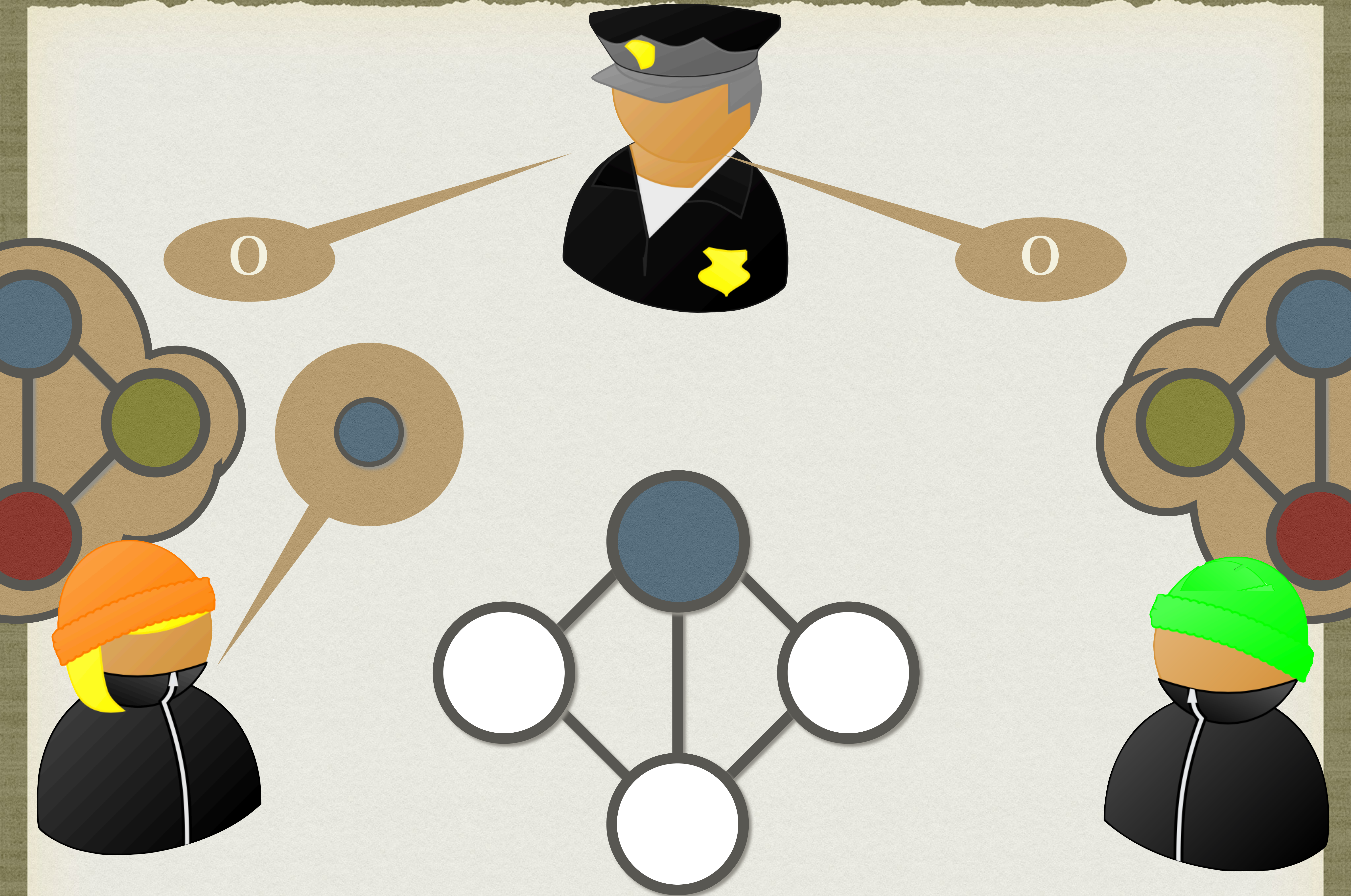


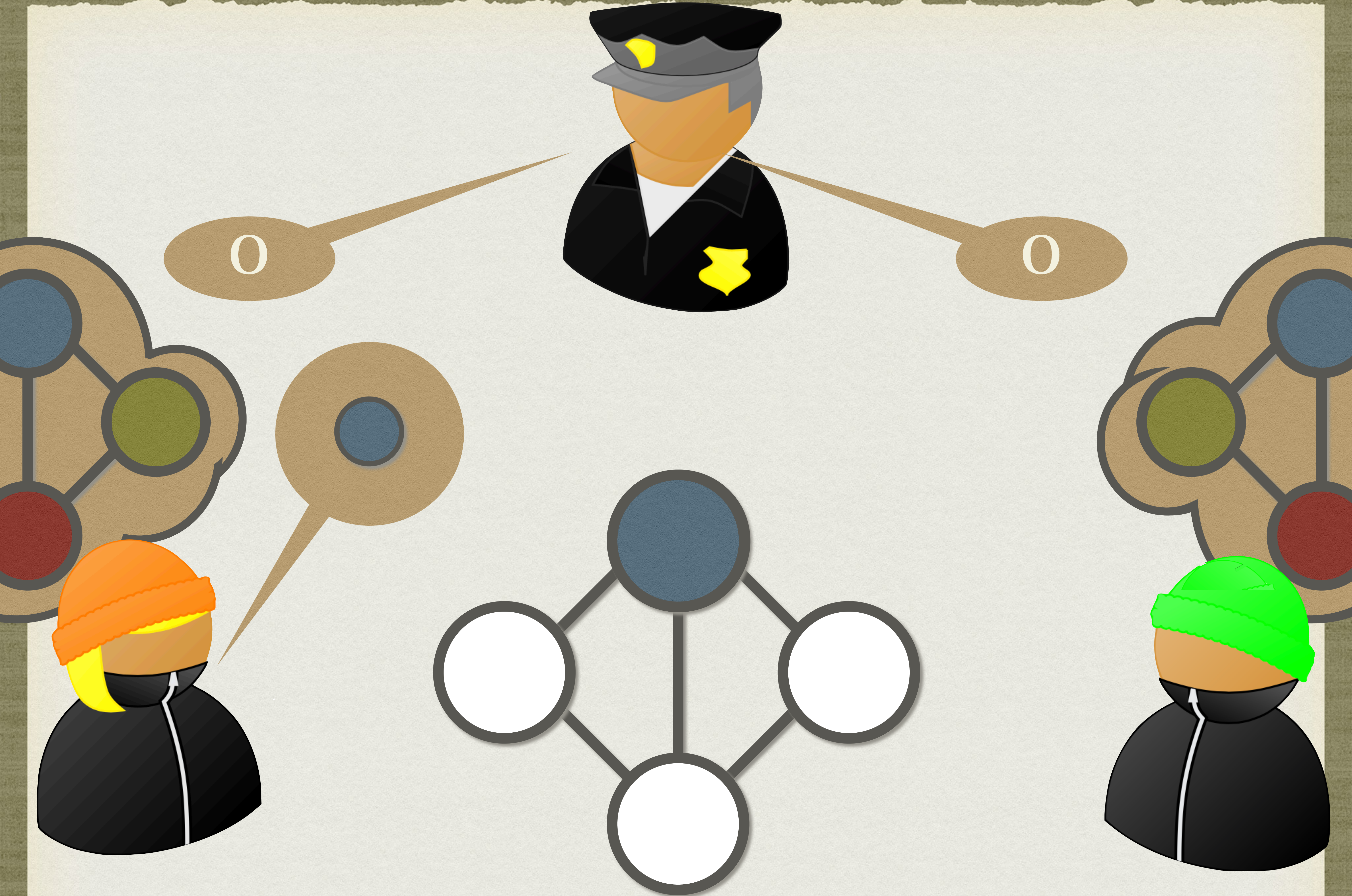


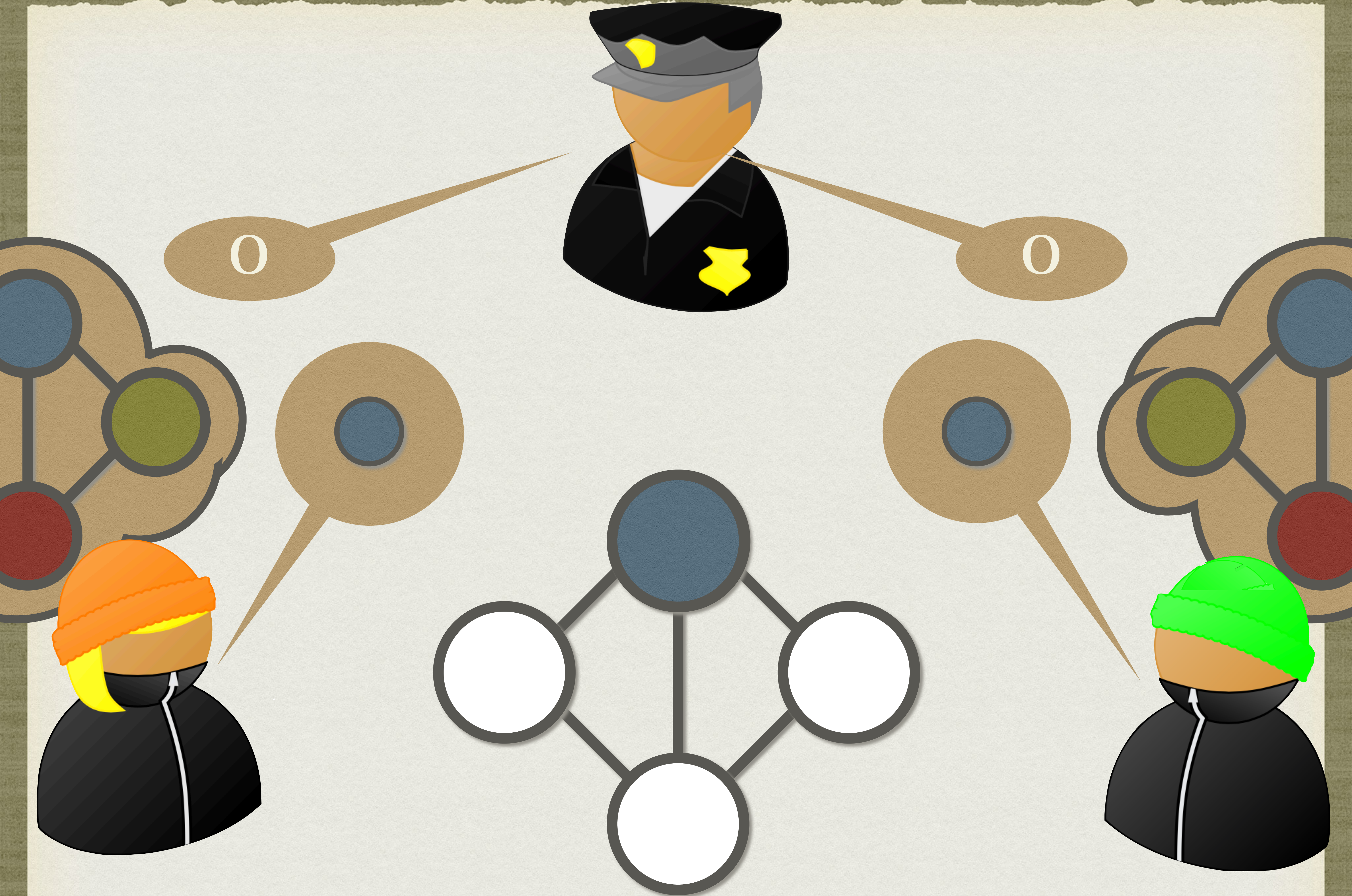

0

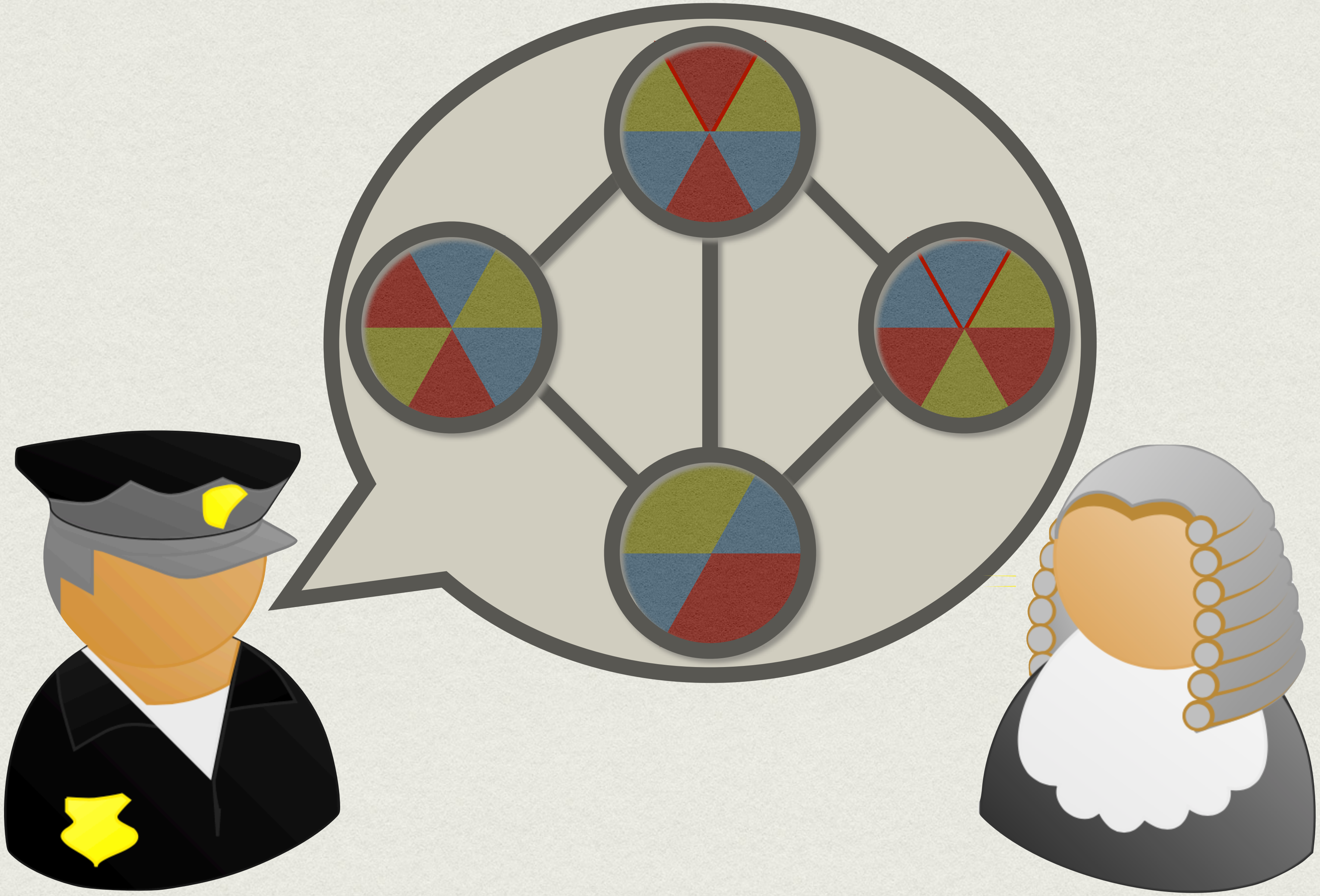

0


0

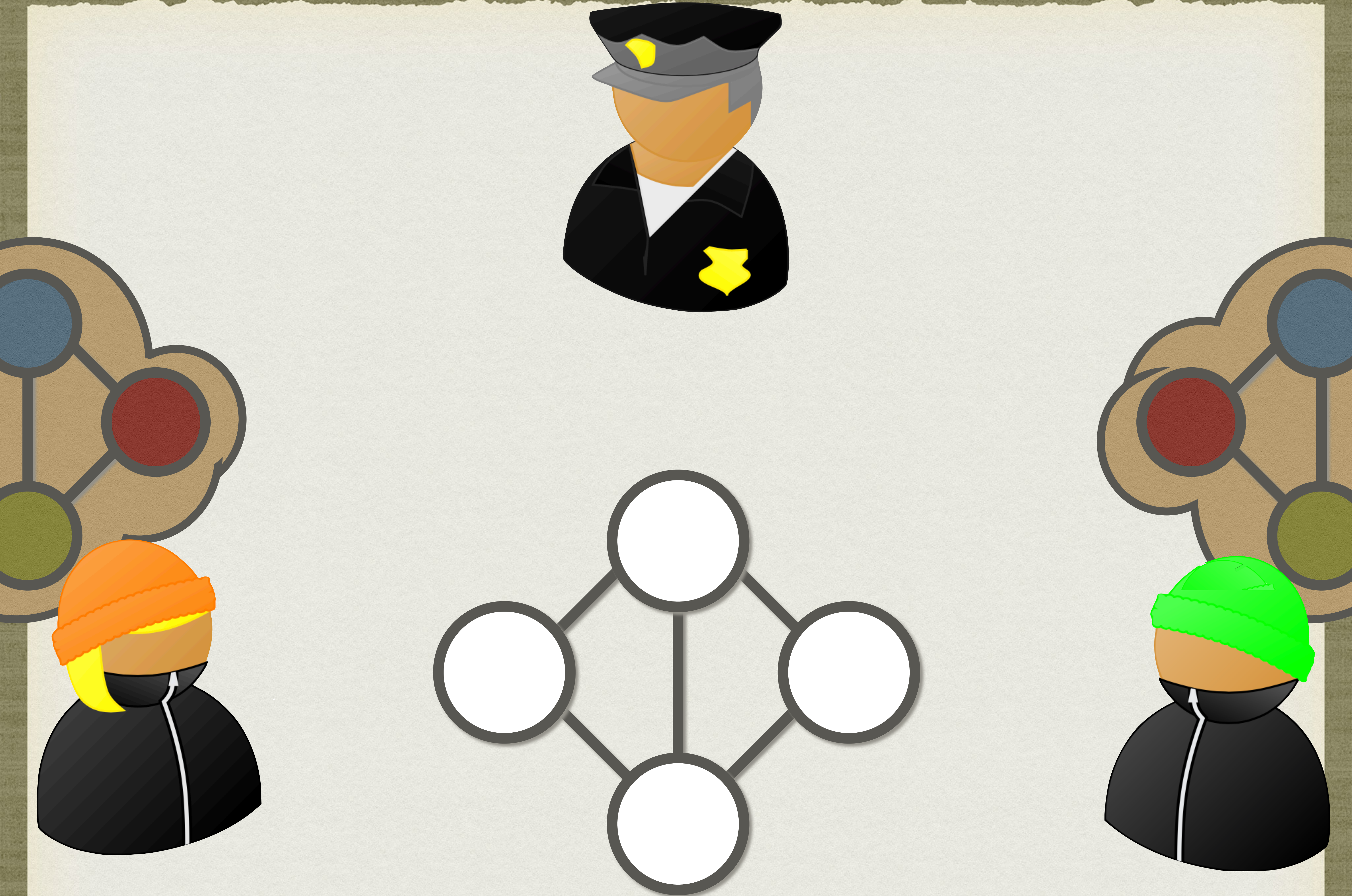

0
0

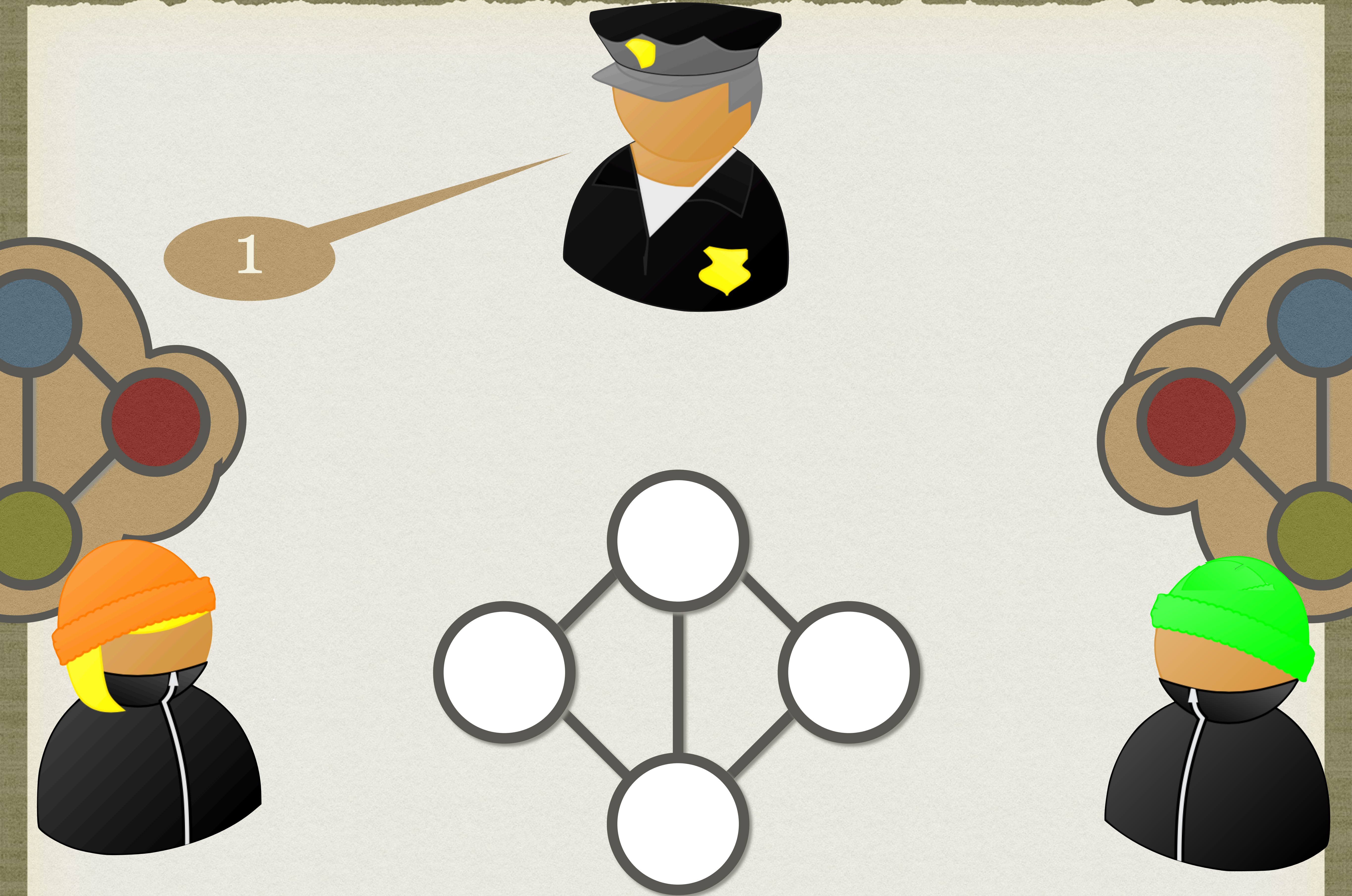

0
0

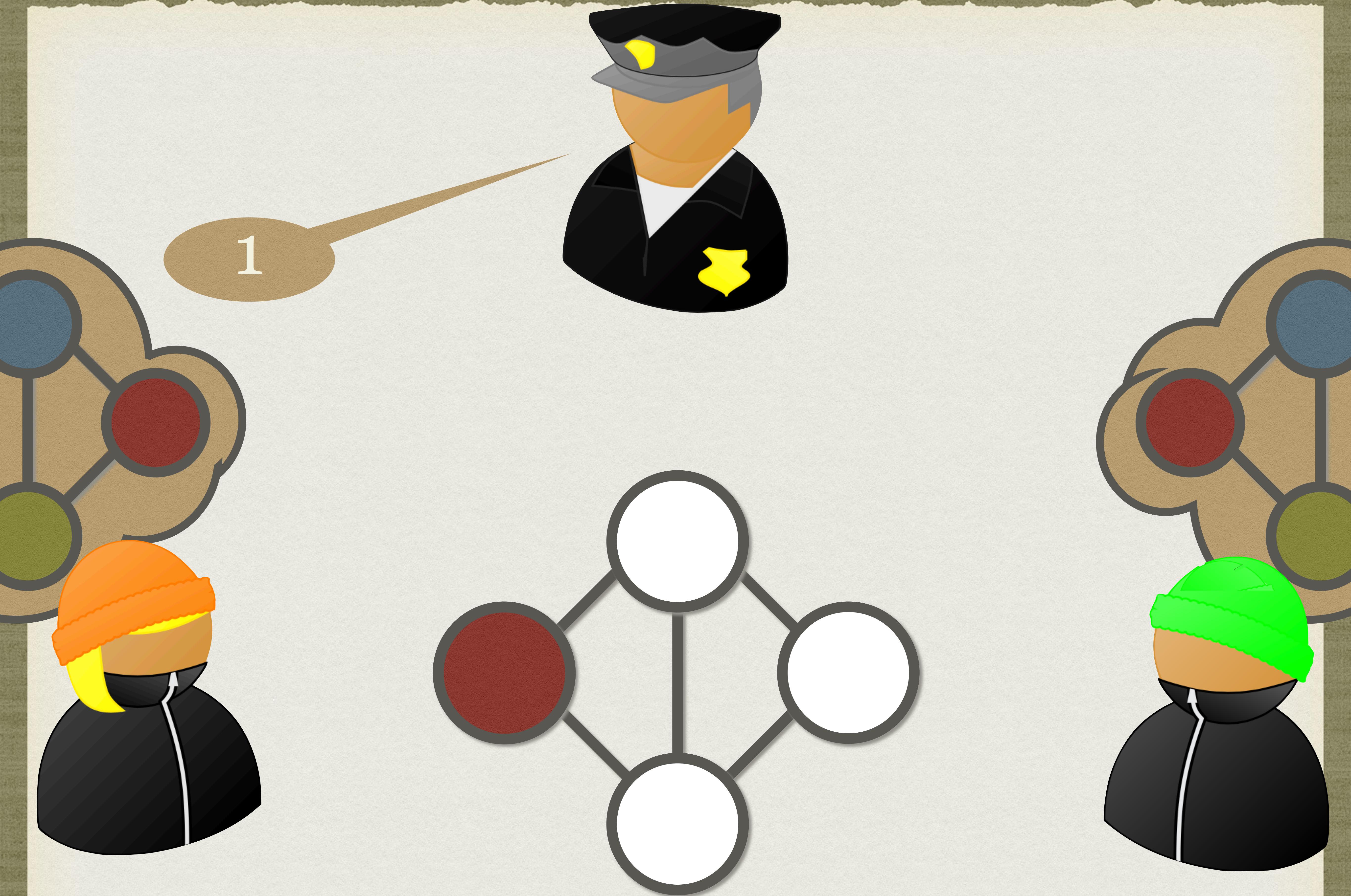

0
0

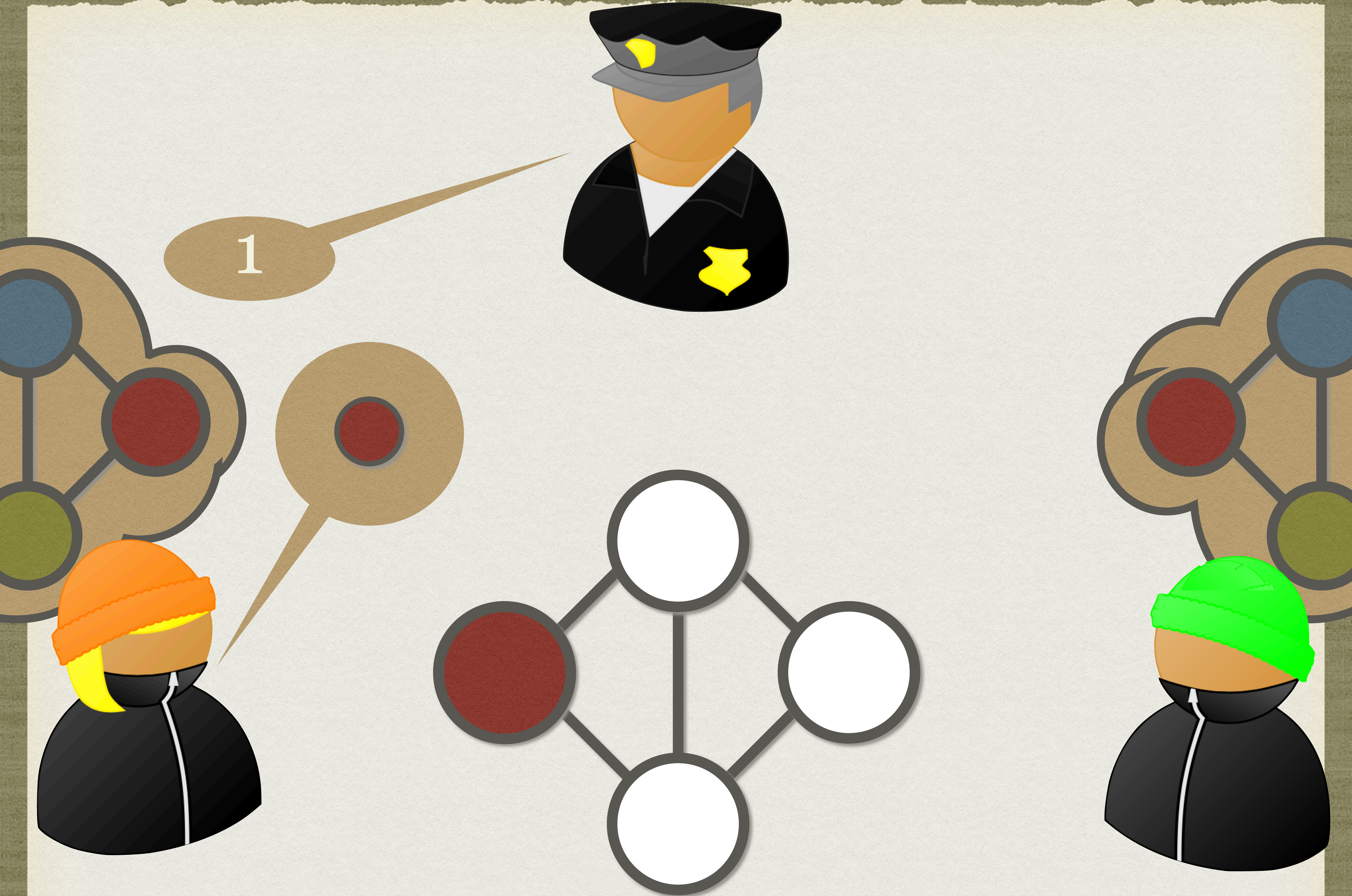


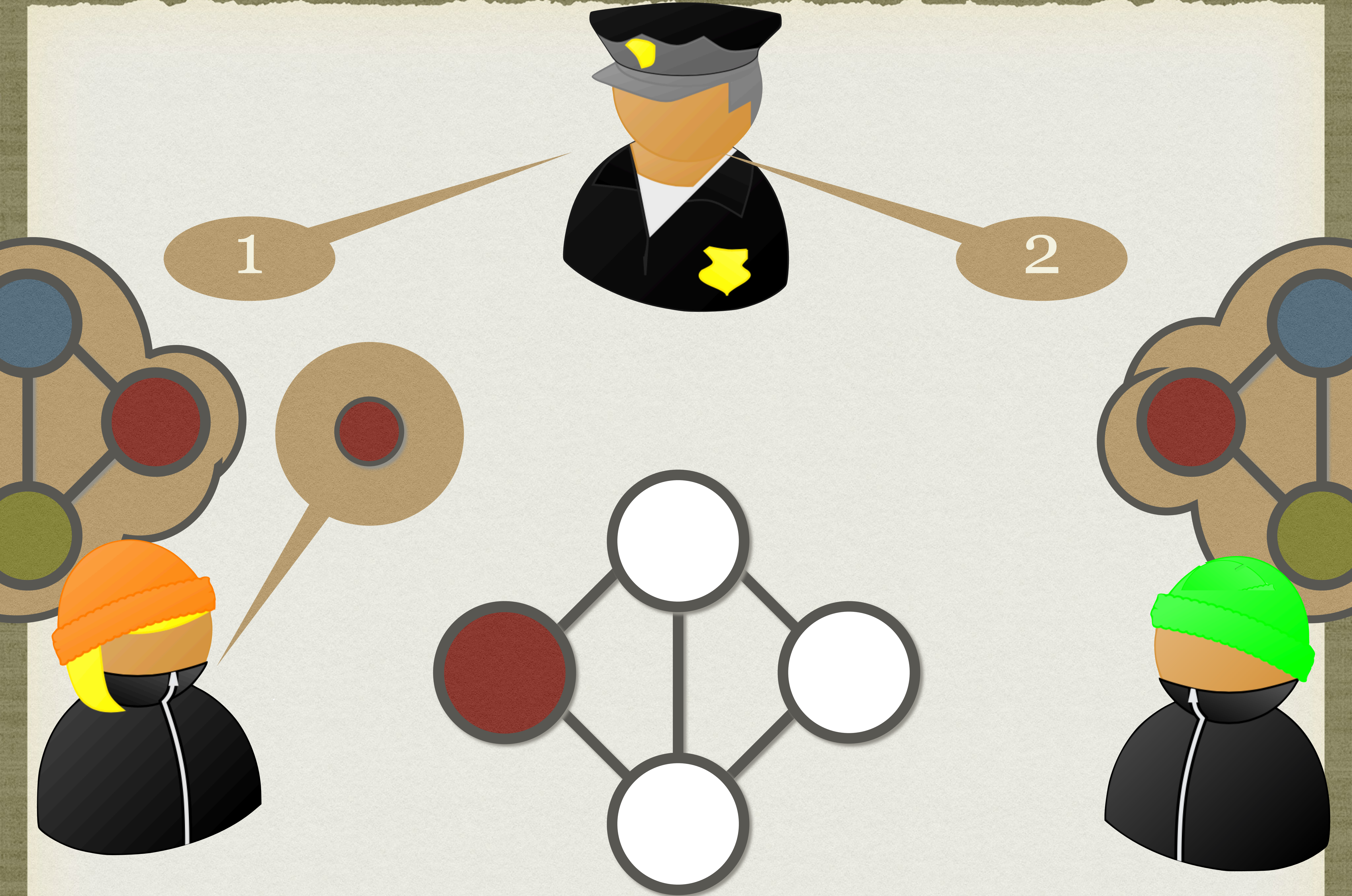
HONEST-VERIFIER ZK

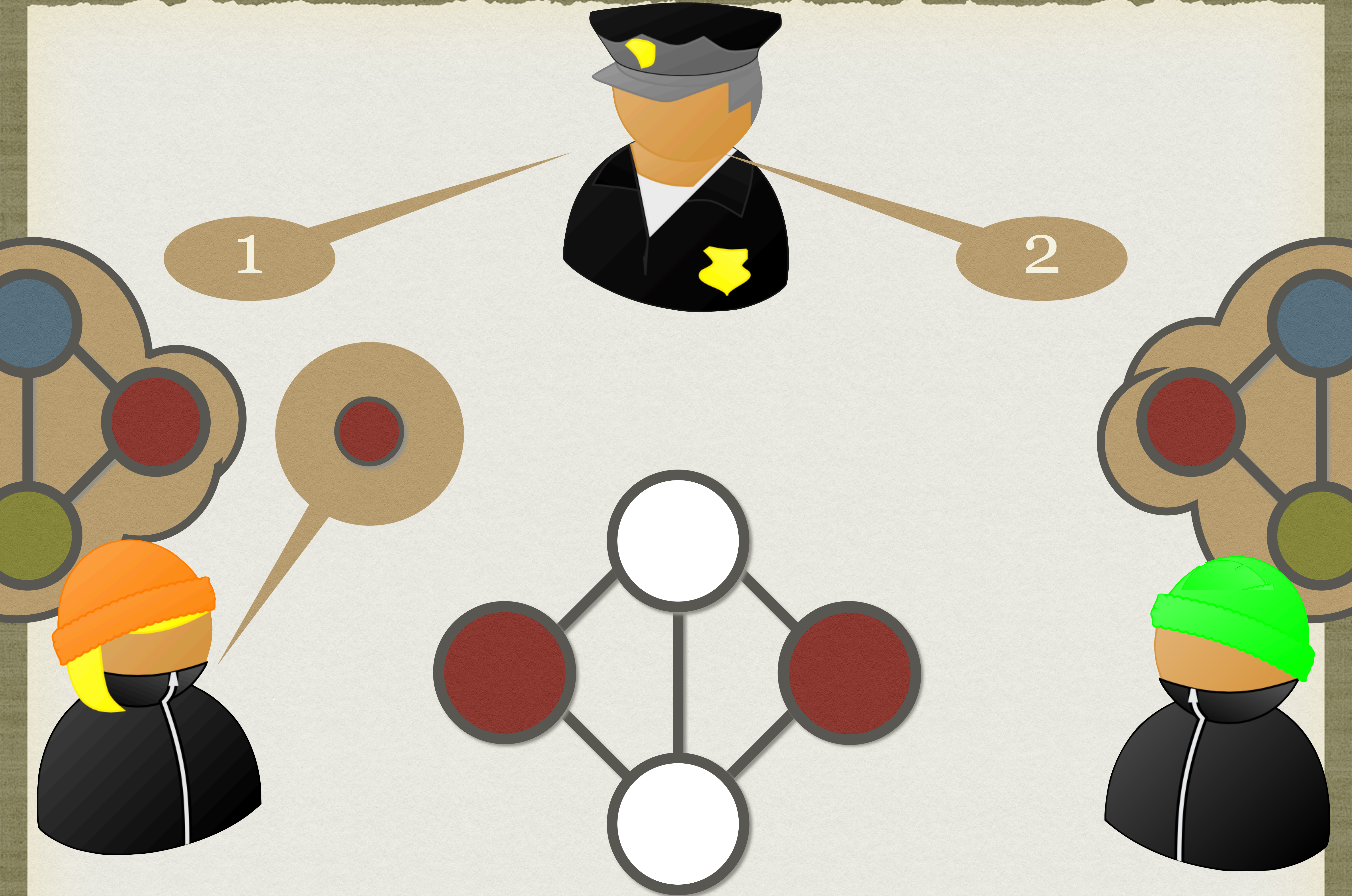


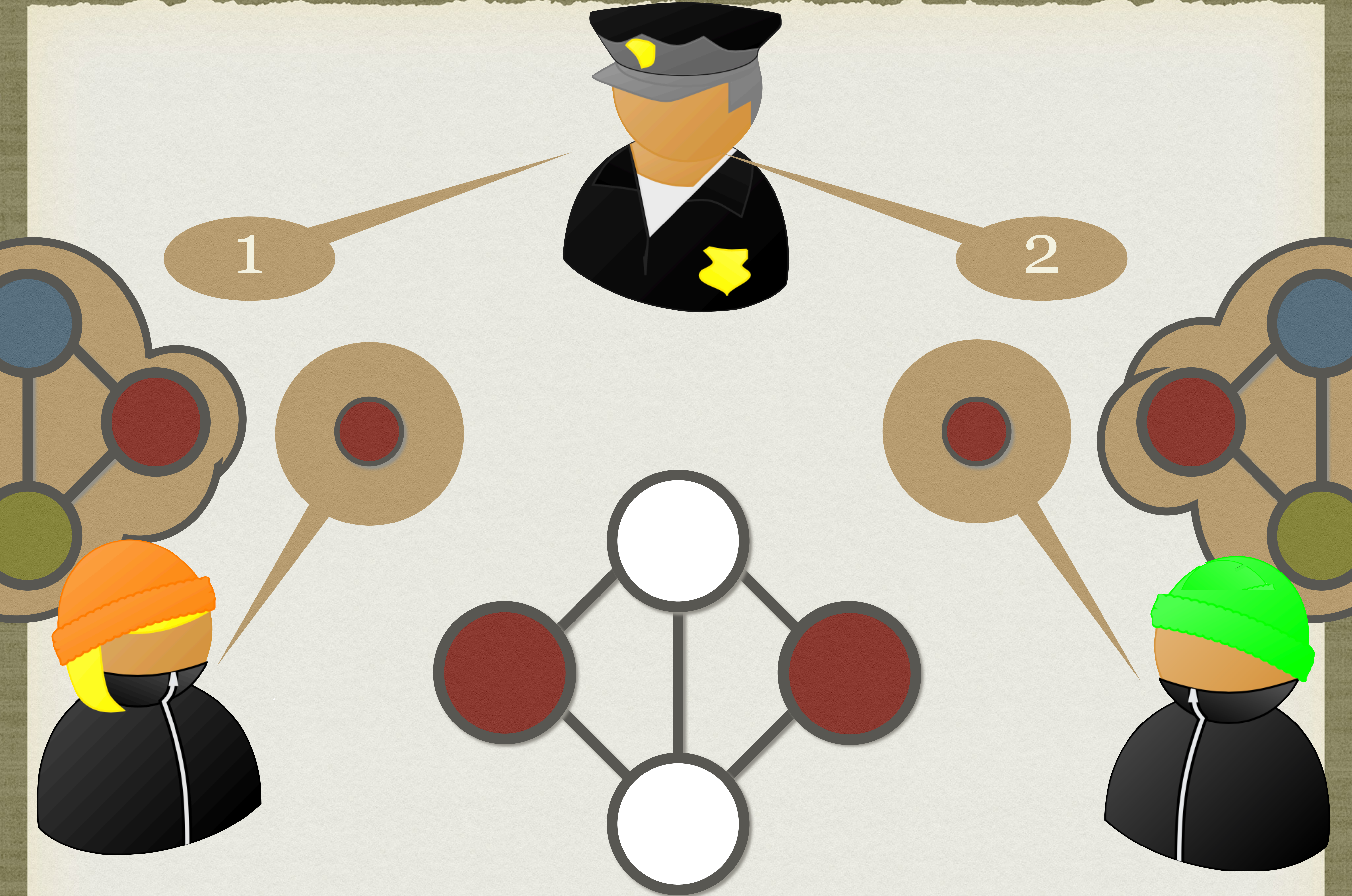

1

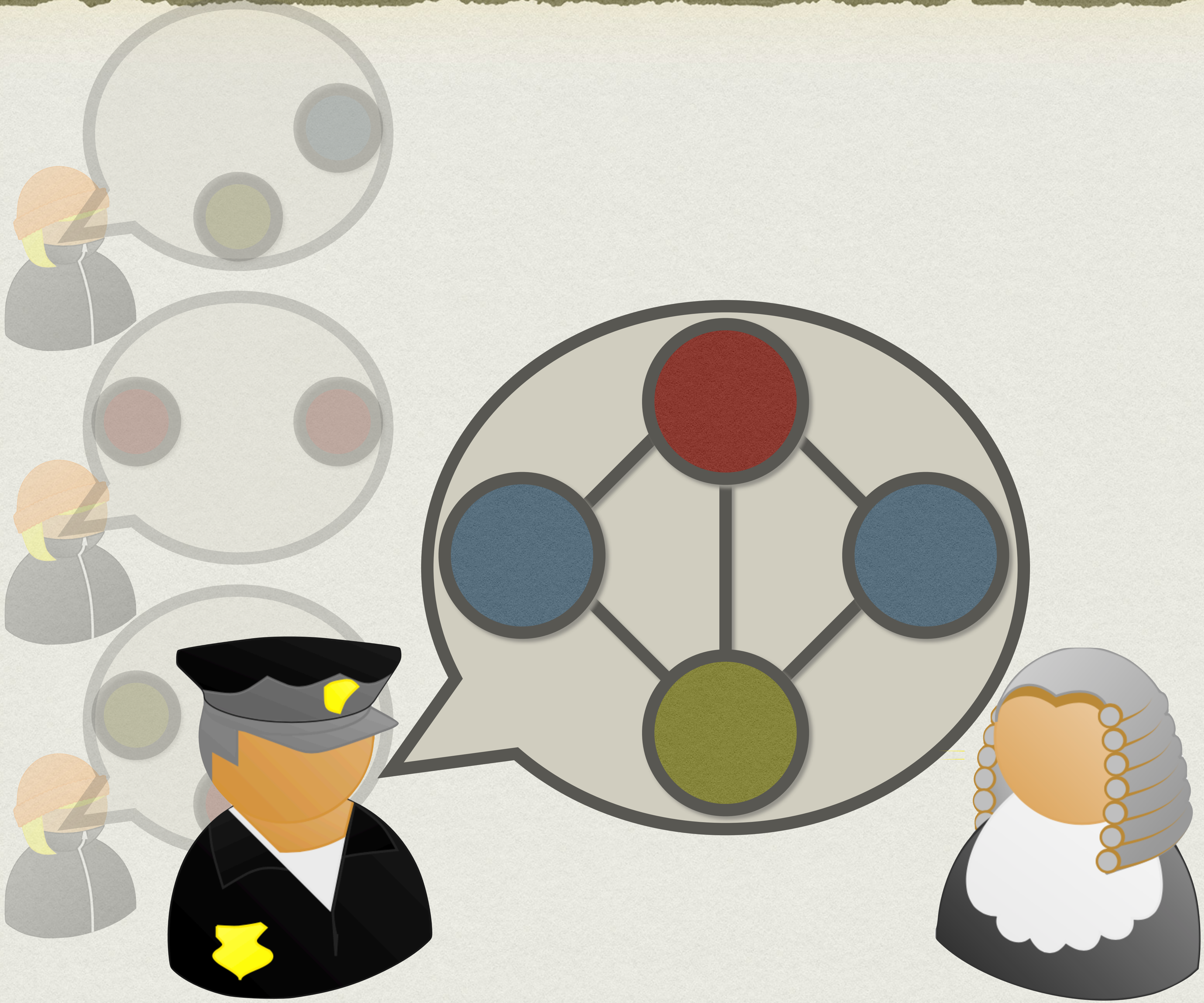

1


1


1
2


1
2

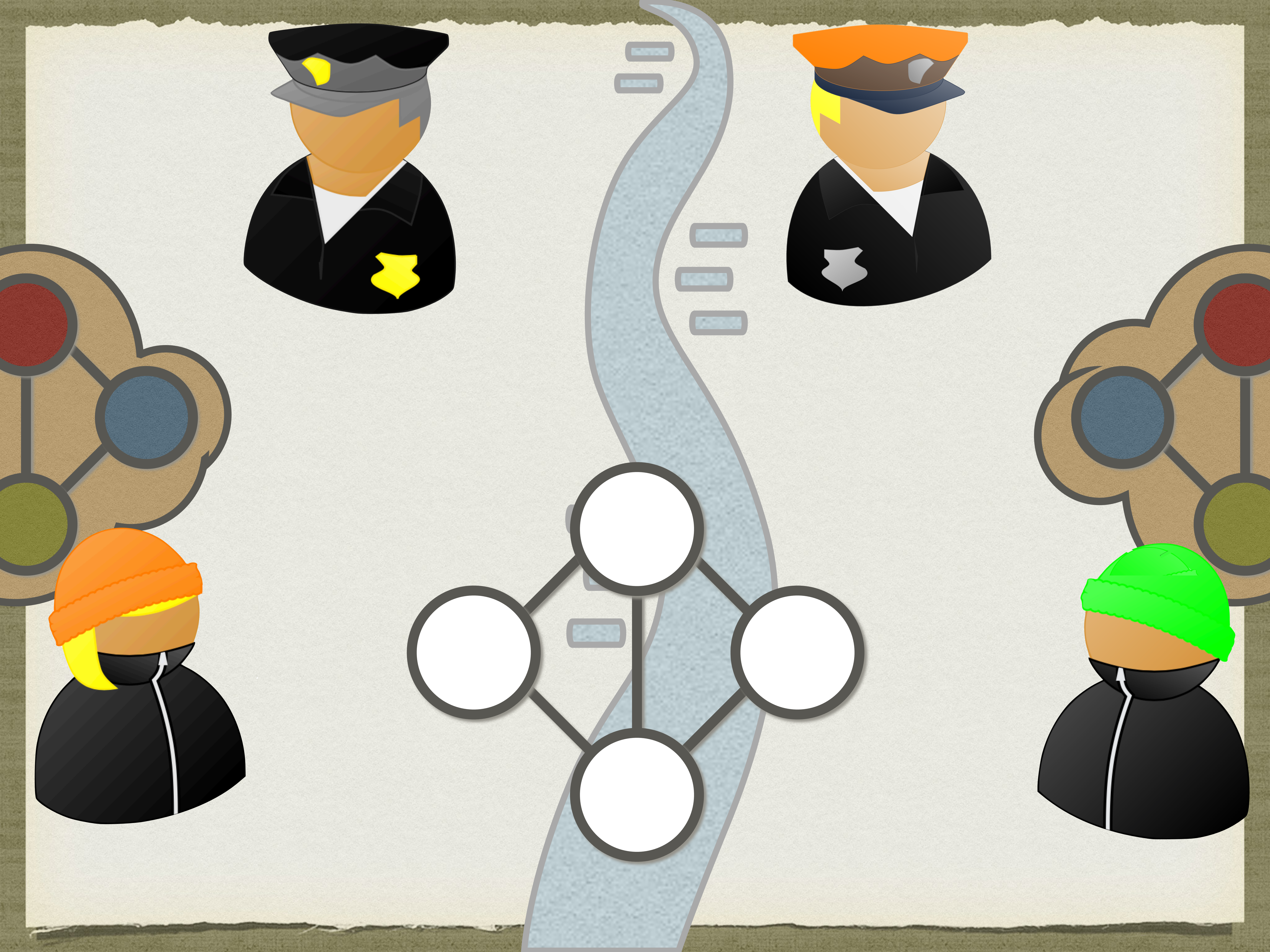

1
2

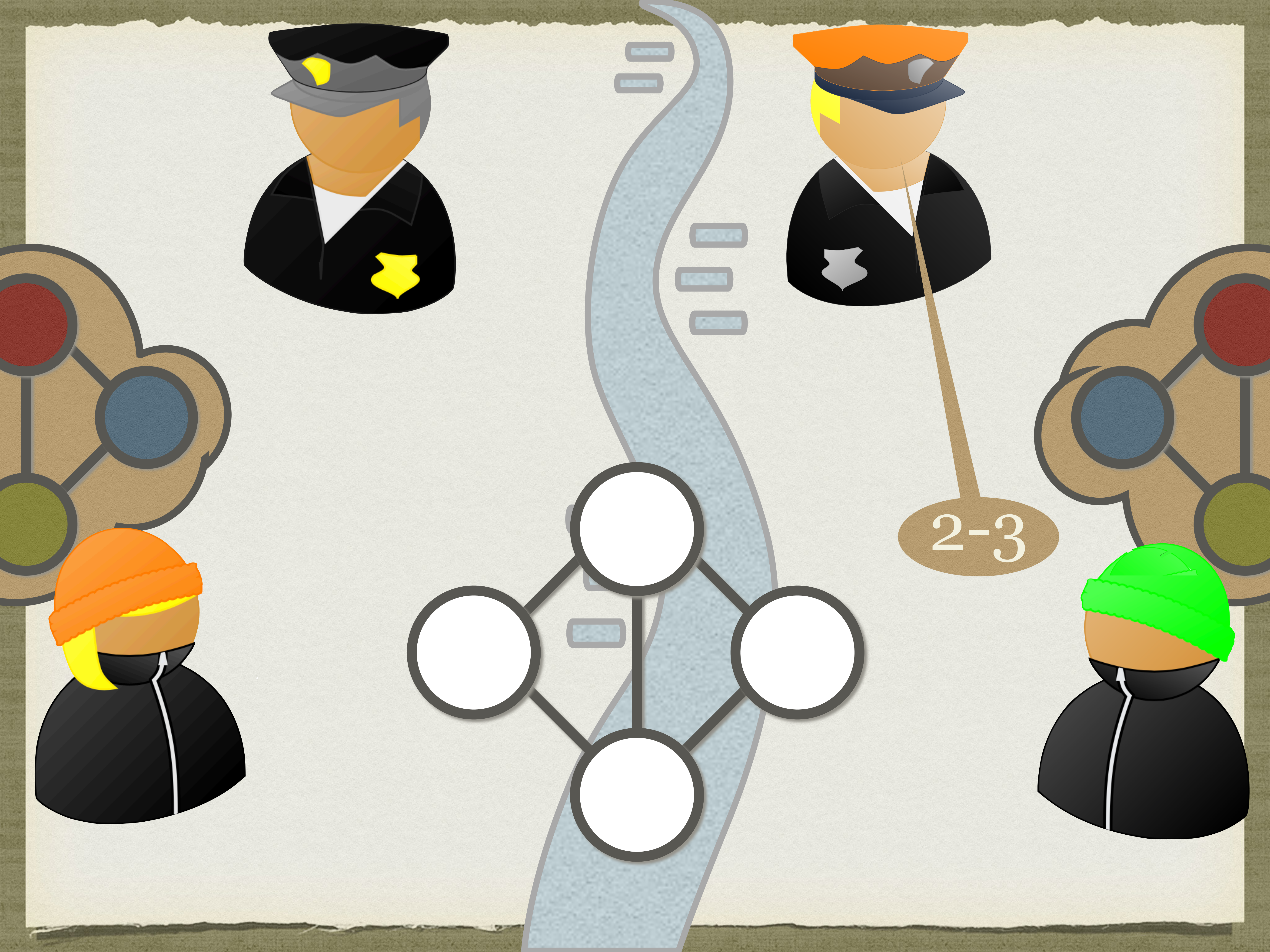


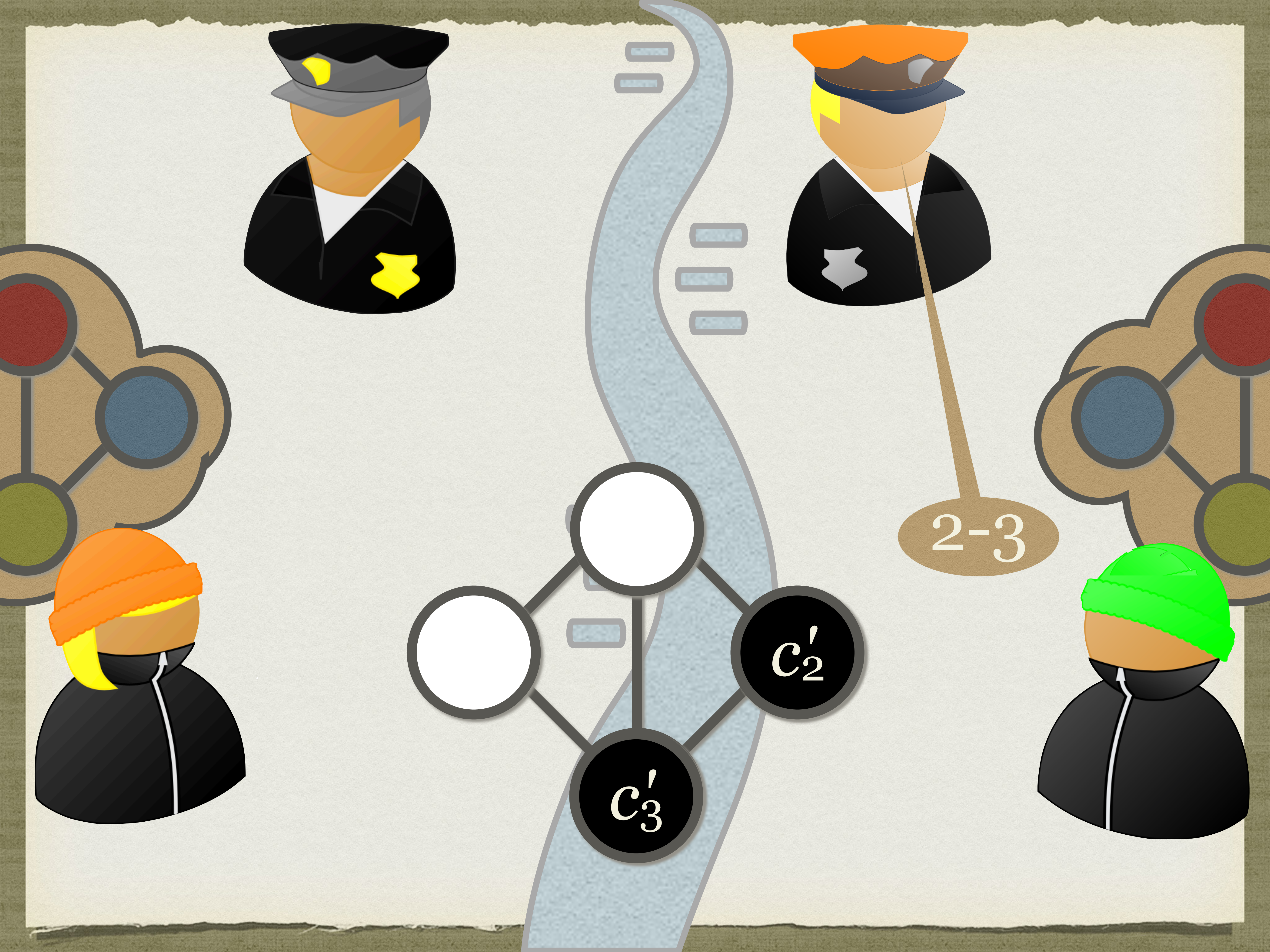
TRANSFERABLE

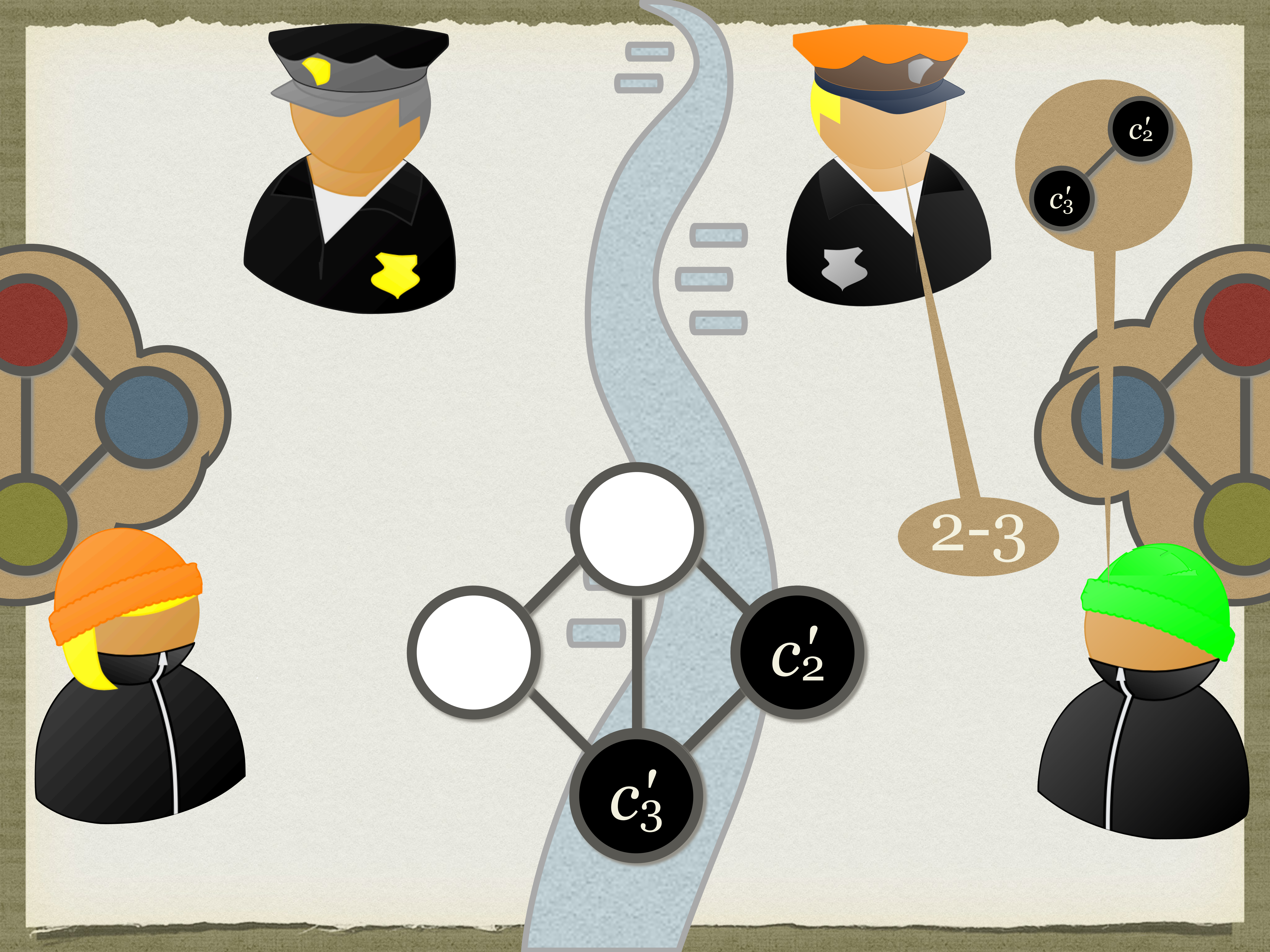
NEW IDEAS

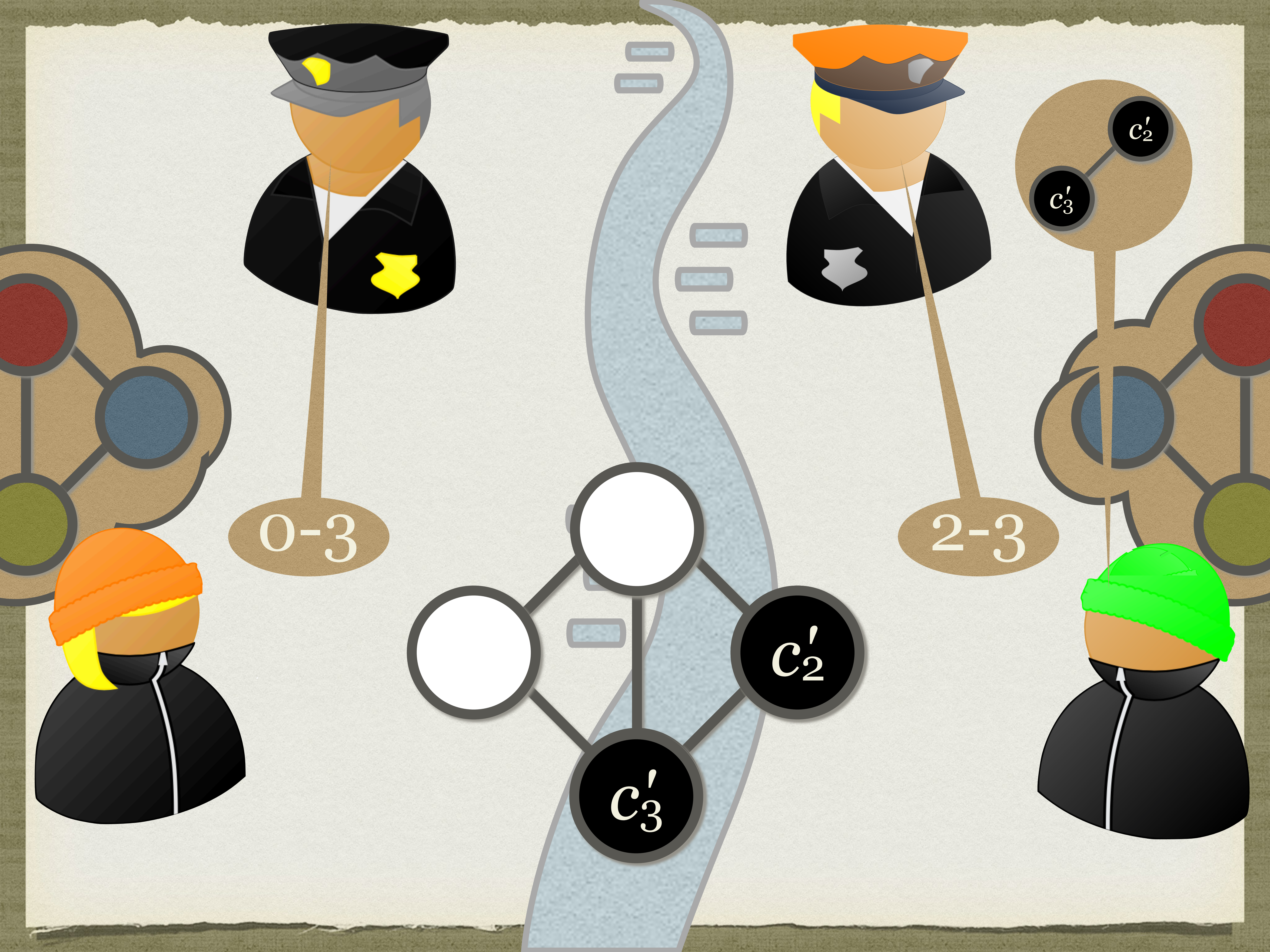
(ZK)MIPs

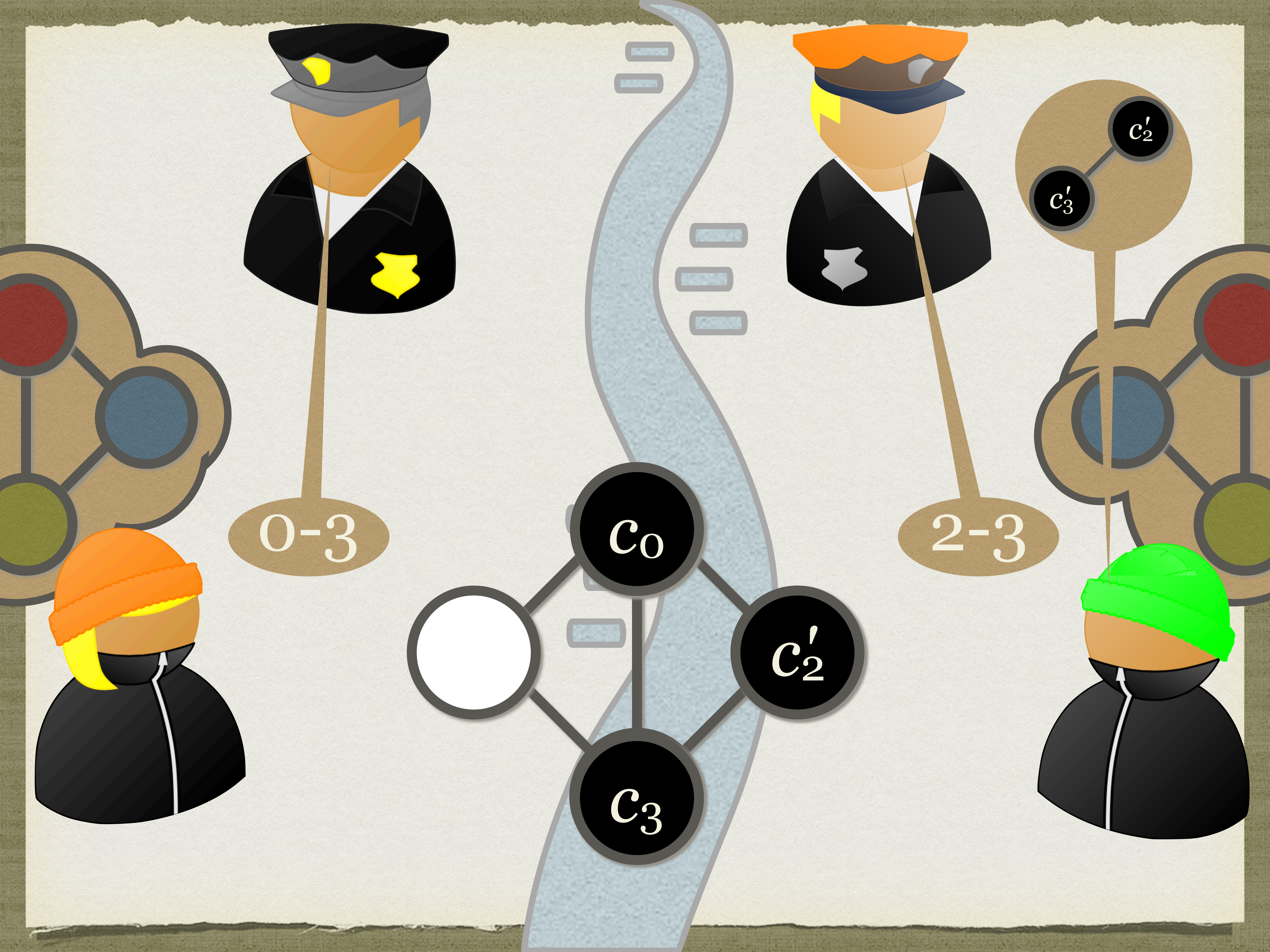


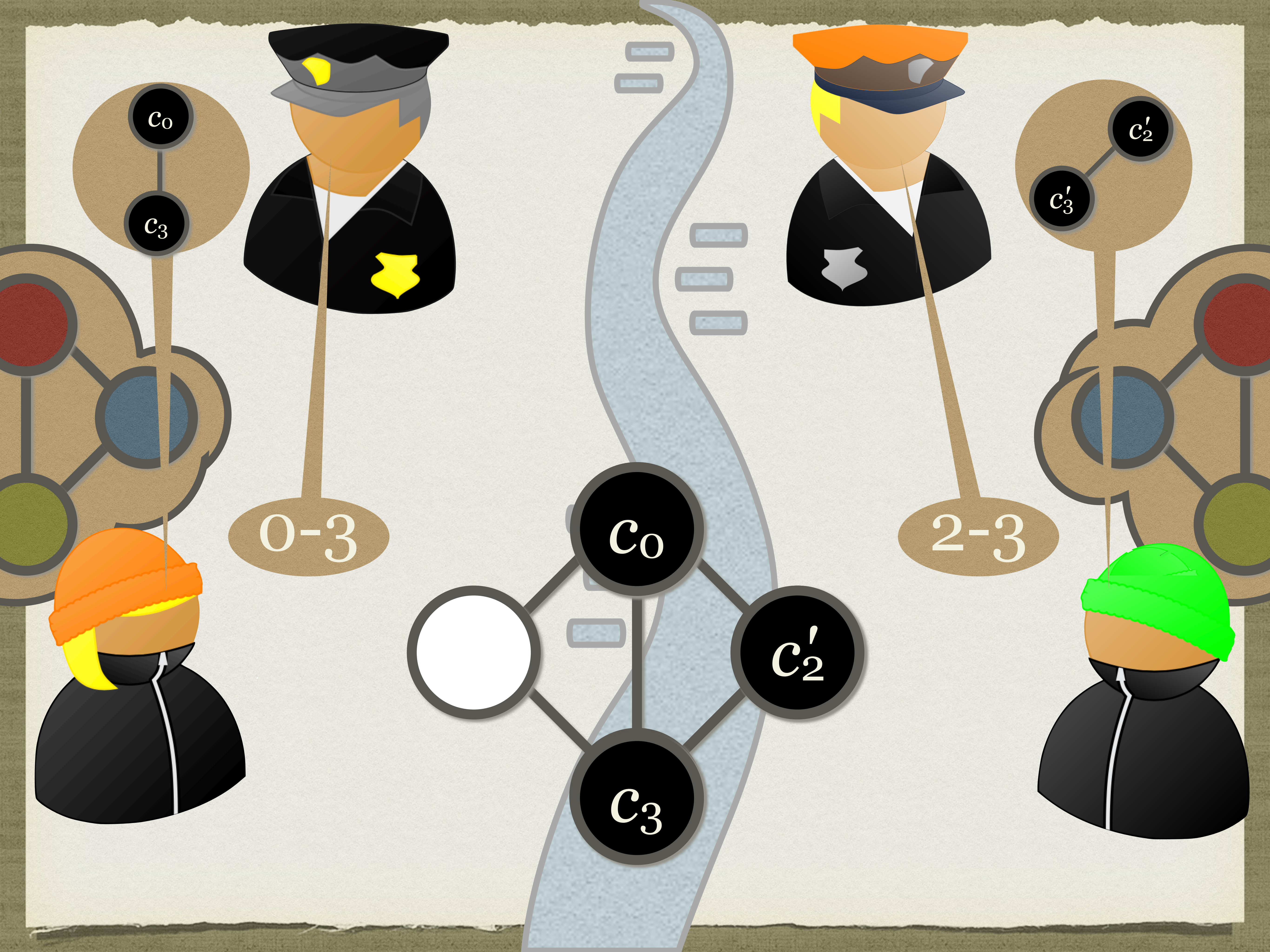

2-3


2-3
c_2'
c_3'

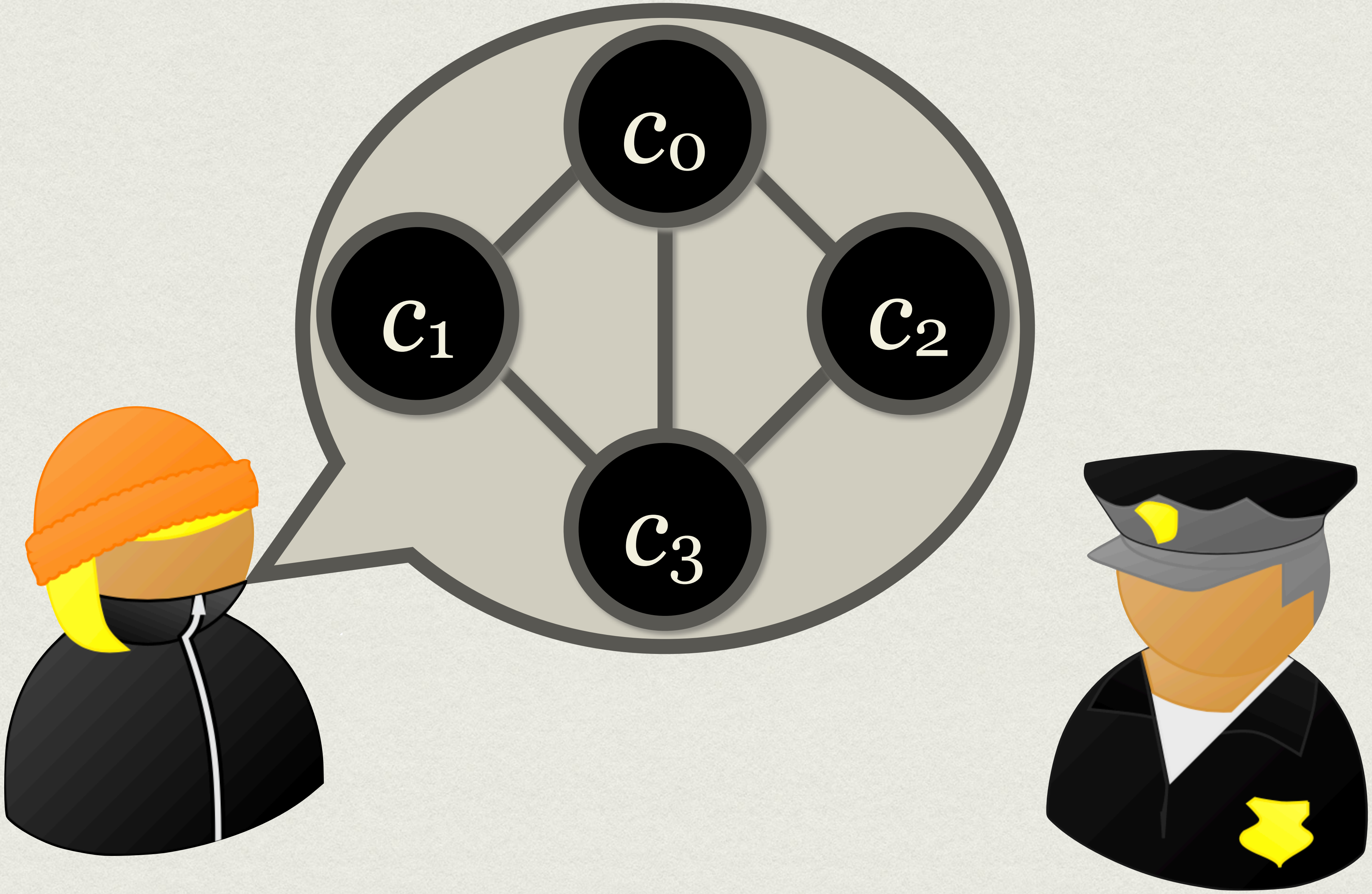

c'_2
c'_3
2-3
c'_2
c'_3


c'_2
c'_3
0-3
2-3
c'_2
c'_3


0-3
2-3
c'_2
c'_3
c_0
c'_2
c_3

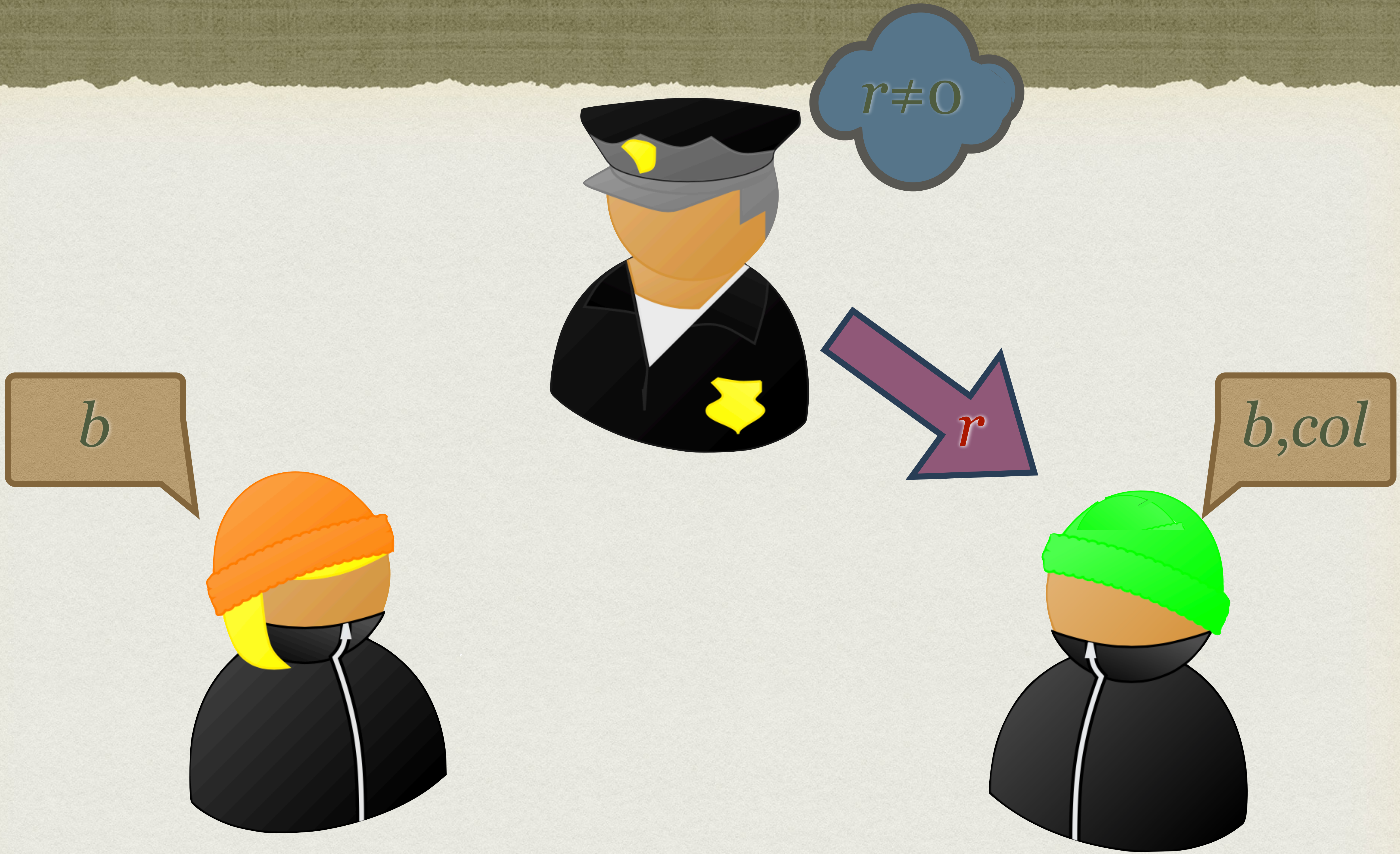

c_0
c_3
0-3
c'_2
c'_3
2-3
c_0
c'_2
c_3

COMMITMENTS ??



COMMITMENT

COMMITMENT



COMMITMENT

$$com := b \cdot r + col$$

COMMITMENT

$$com := b \cdot r + col$$

COMMITMENT

$$com := b \cdot r + col$$

COMMITMENT

$$com := b \cdot r + col$$

COMMITMENT

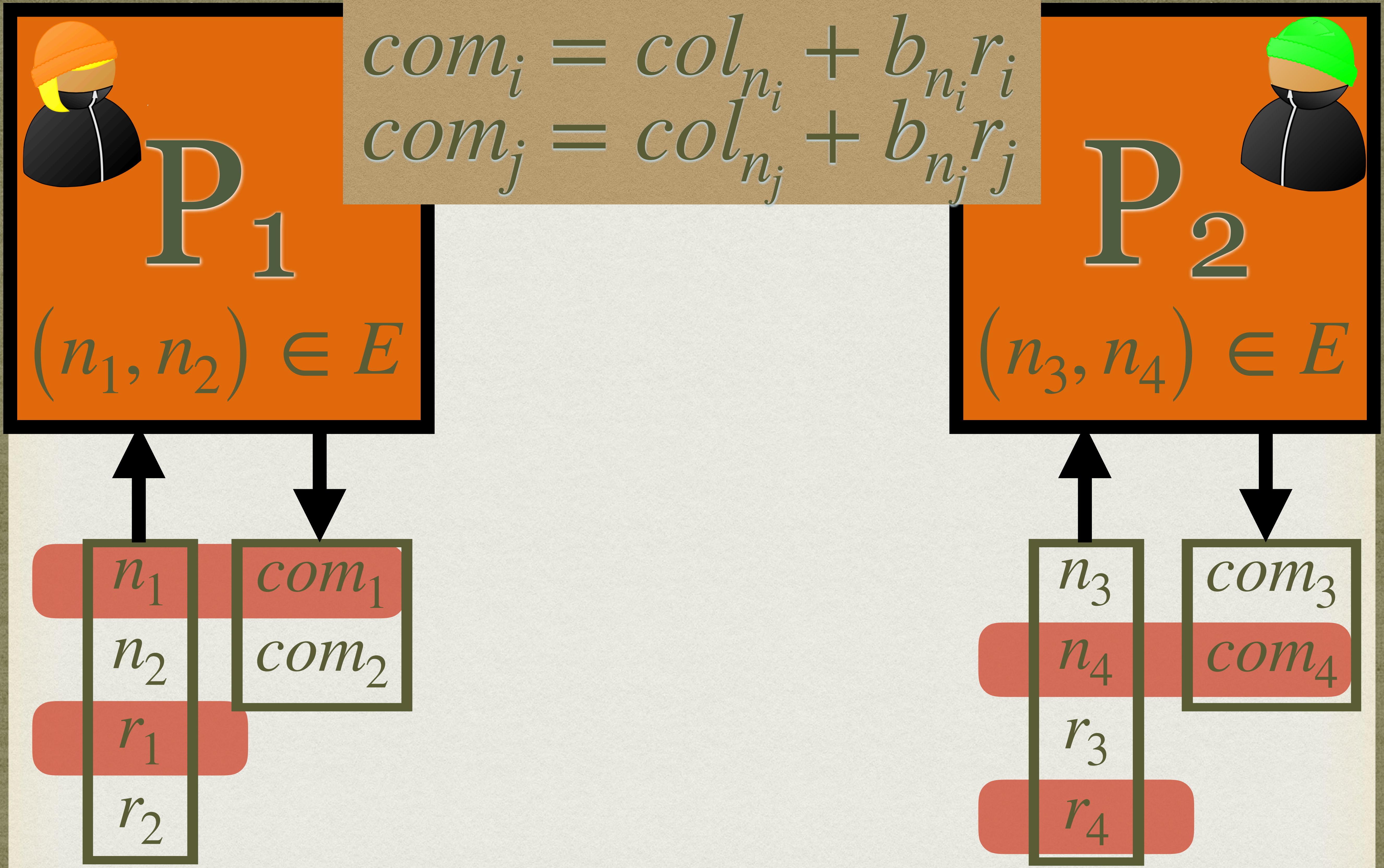
THE

UNVEIL VIA COMMIT

PRINCIPLE

$$com_i = col_{n_i} + b_{n_i} r_i$$

$$com_j = col_{n_j} + b_{n_j} r_j$$



P$_1$

$(n_1, n_2) \in E$

n_1

n_2

r_1

r_2

com_1

com_2

P$_2$

$(n_3, n_4) \in E$

n_3

n_4

r_3

r_4

com_3

com_4

P_1

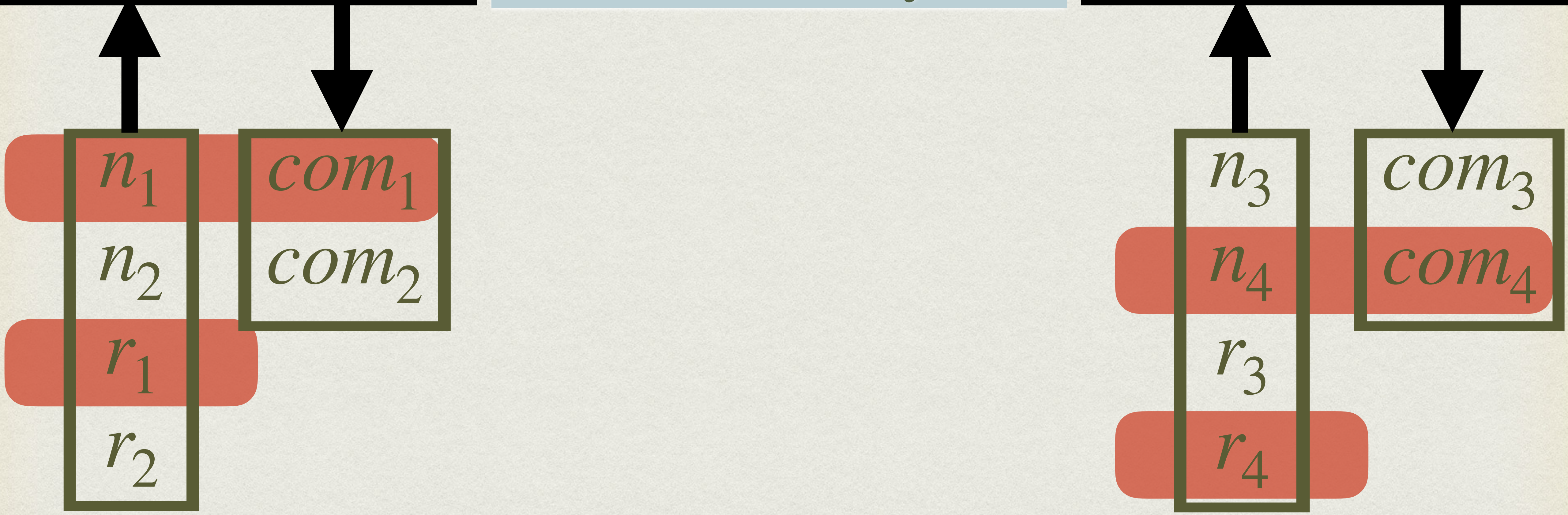
$(n_1, n_2) \in E$

$$com_i = col_{n_i} + b_{n_i} r_i$$
$$com_j = col_{n_j} + b_{n_j} r_j$$

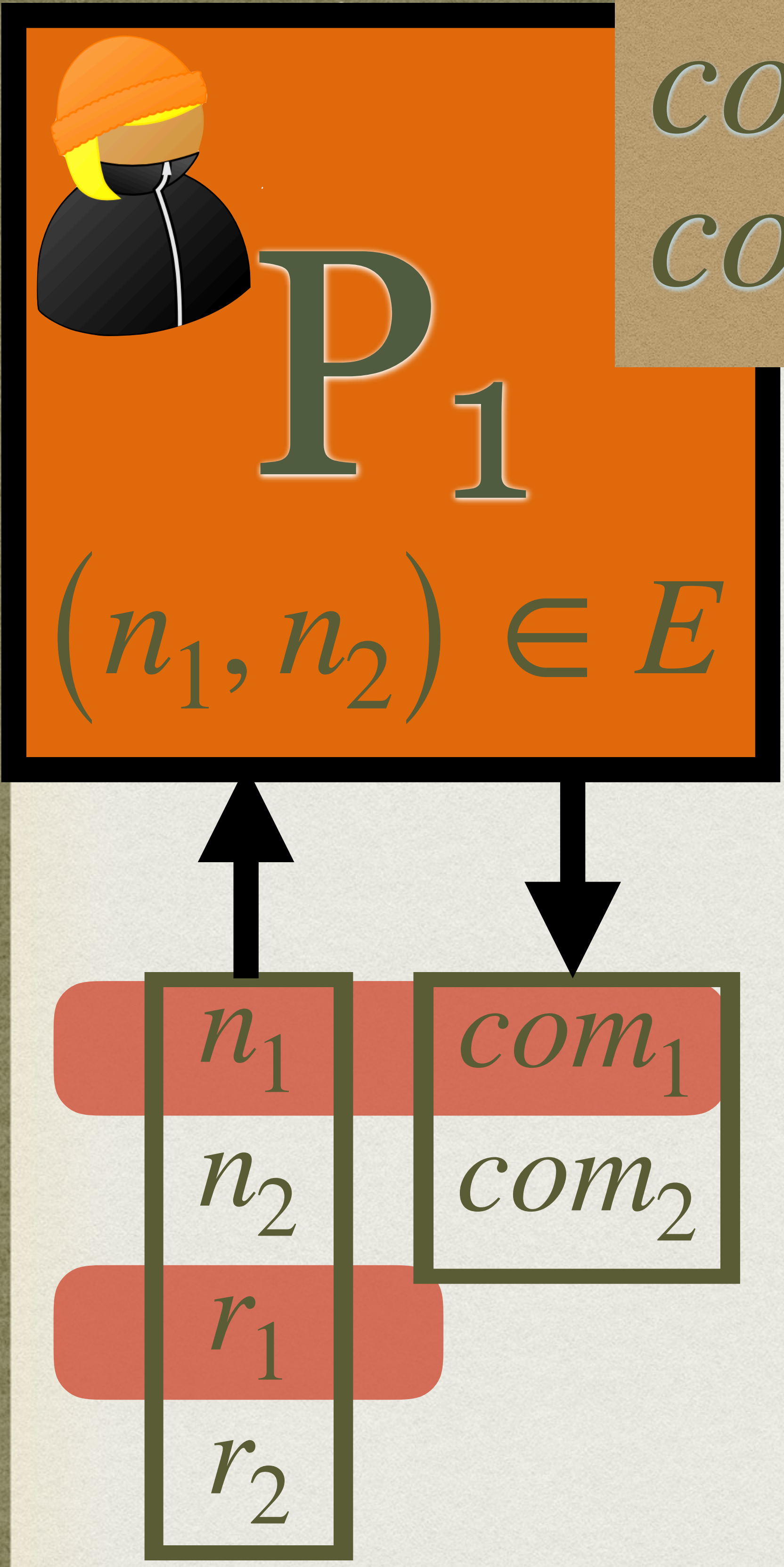
Asking two provers the same node with same *r* checks their consistency.

P_2

$(n_3, n_4) \in E$



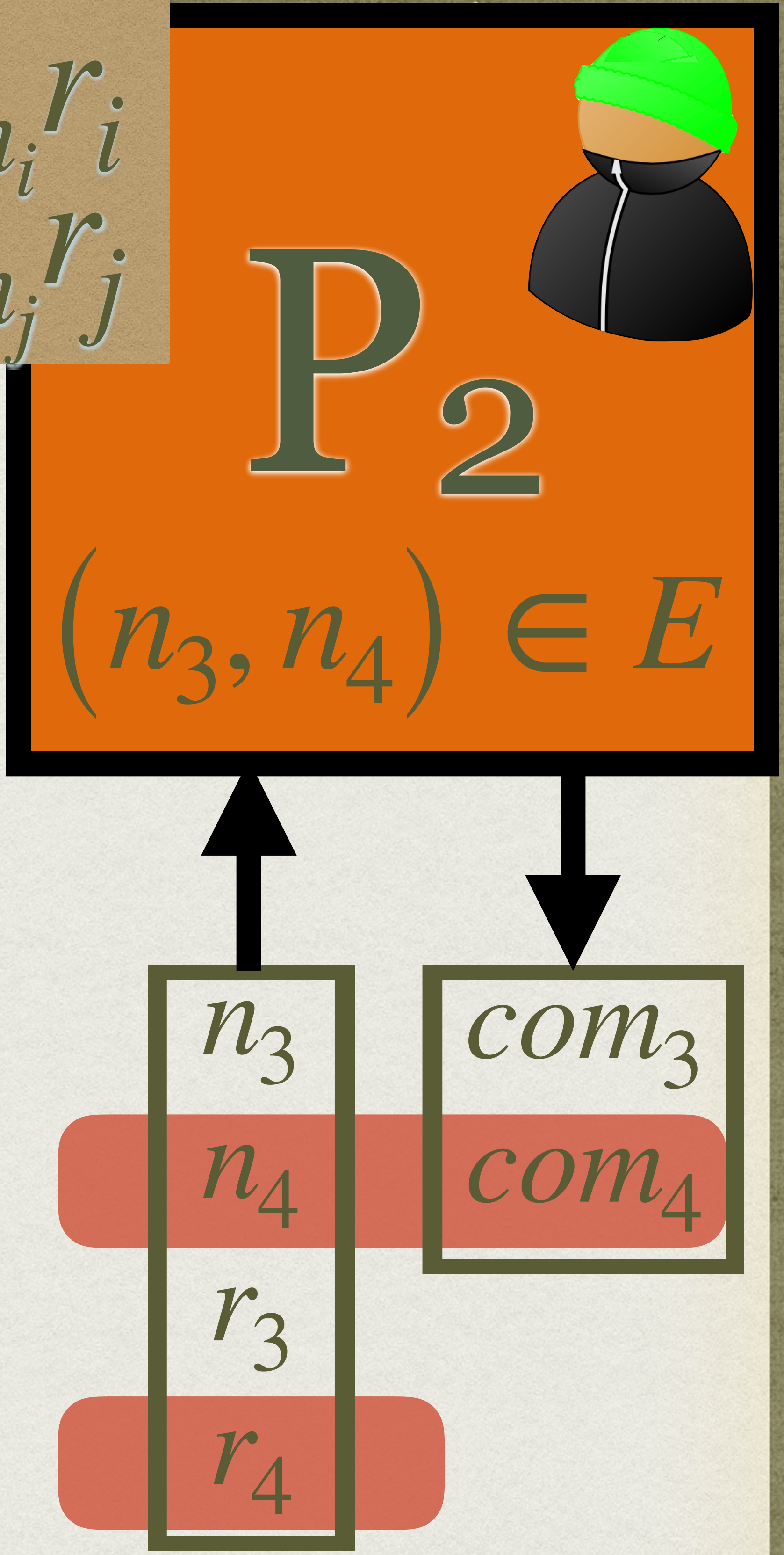
$$com_i = col_{n_i} + b_{n_i} r_i$$
$$com_j = col_{n_j} + b_{n_j} r_j$$



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

$$n_i = n_j \wedge r_i = r_j$$
$$\implies com_i = com_j$$

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



$$com_i = col_{n_i} + b_{n_i} r_i$$
$$com_j = col_{n_j} + b_{n_j} r_j$$

P_1

$(n_1, n_2) \in E$

n_1
n_2
r_1
r_2

com_1
com_2

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

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

$$n_i = n_j \wedge r_i = r_j$$
$$\implies com_i = com_j$$

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

P_2

$(n_3, n_4) \in E$

n_3
n_4
r_3
r_4

com_3
com_4

$$com_i = col_{n_i} + b_{n_i} r_i$$
$$com_j = col_{n_j} + b_{n_j} r_j$$

P_1

$(n_1, n_2) \in E$

P_2

$(n_3, n_4) \in E$

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

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

$$n_i = n_j \wedge r_i = r_j$$
$$\implies com_i = com_j$$

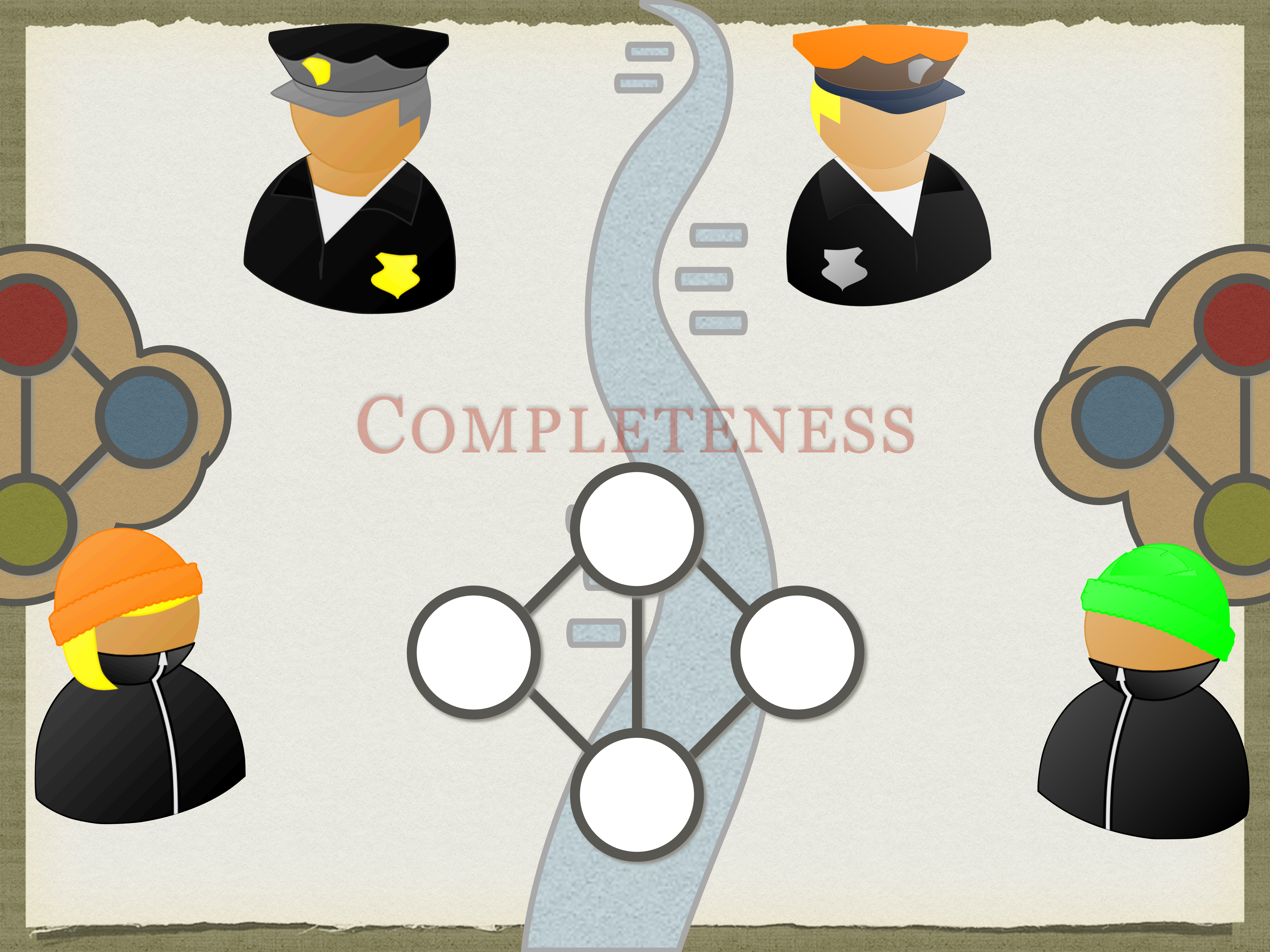
Asking two provers the same node with distinct *r*'s unveils that node colour.

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

$$n_i = n_j \wedge r_i \neq r_j \implies col_{n_i} = com_j + com_i$$

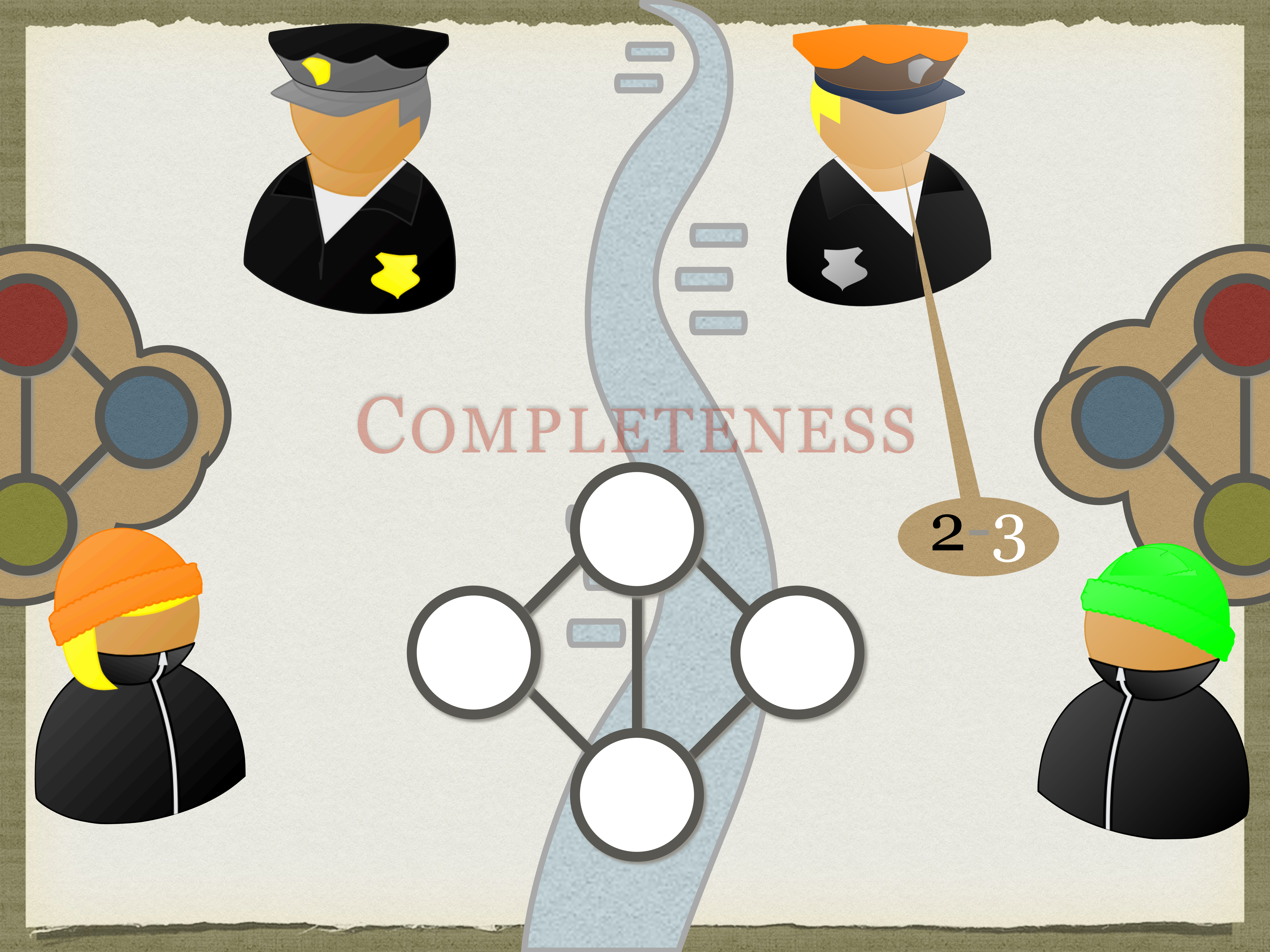
n_1	com_1
n_2	com_2
r_1	
r_2	

n_3	com_3
n_4	com_4
r_3	
r_4	

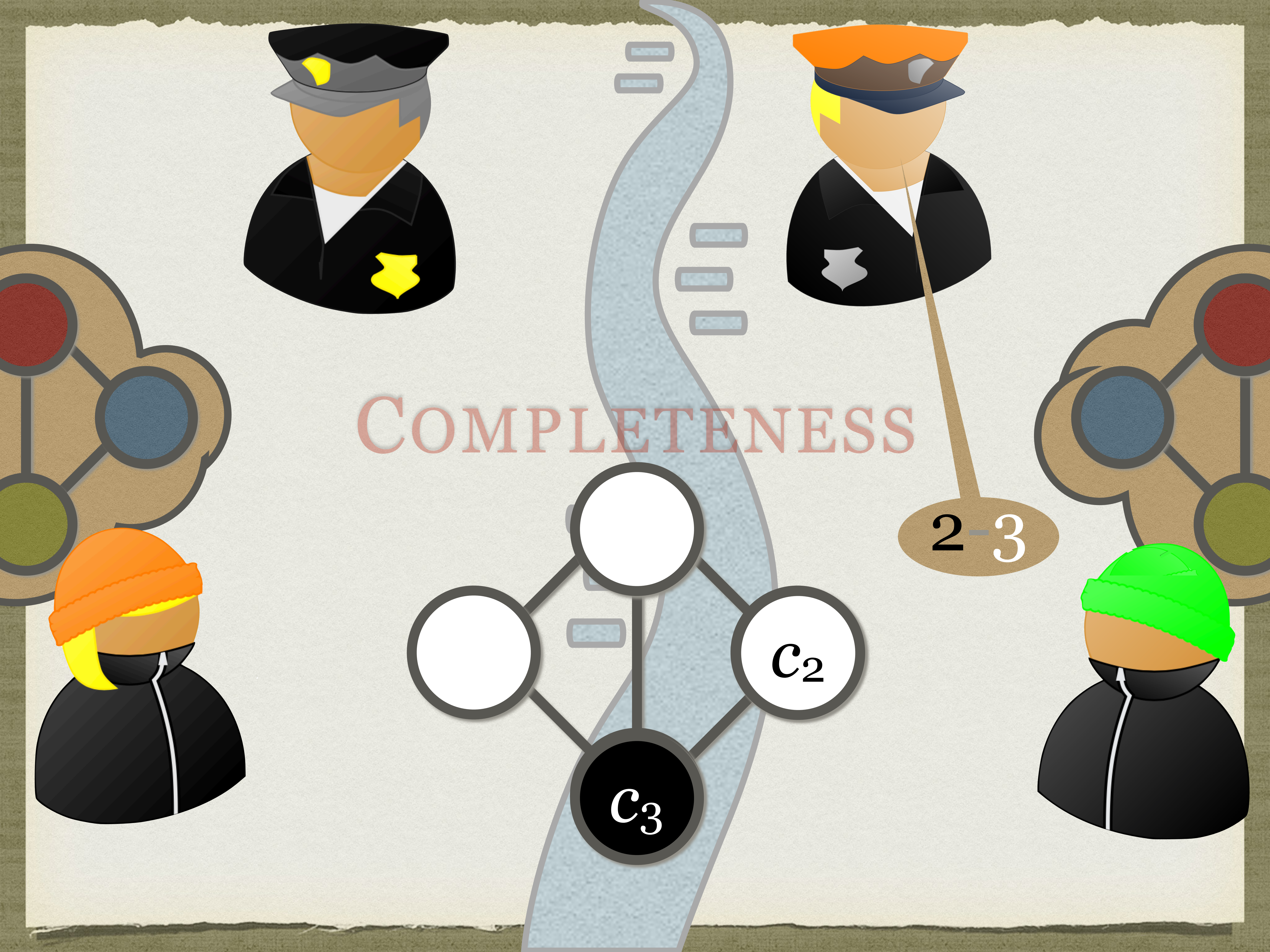


Completeness

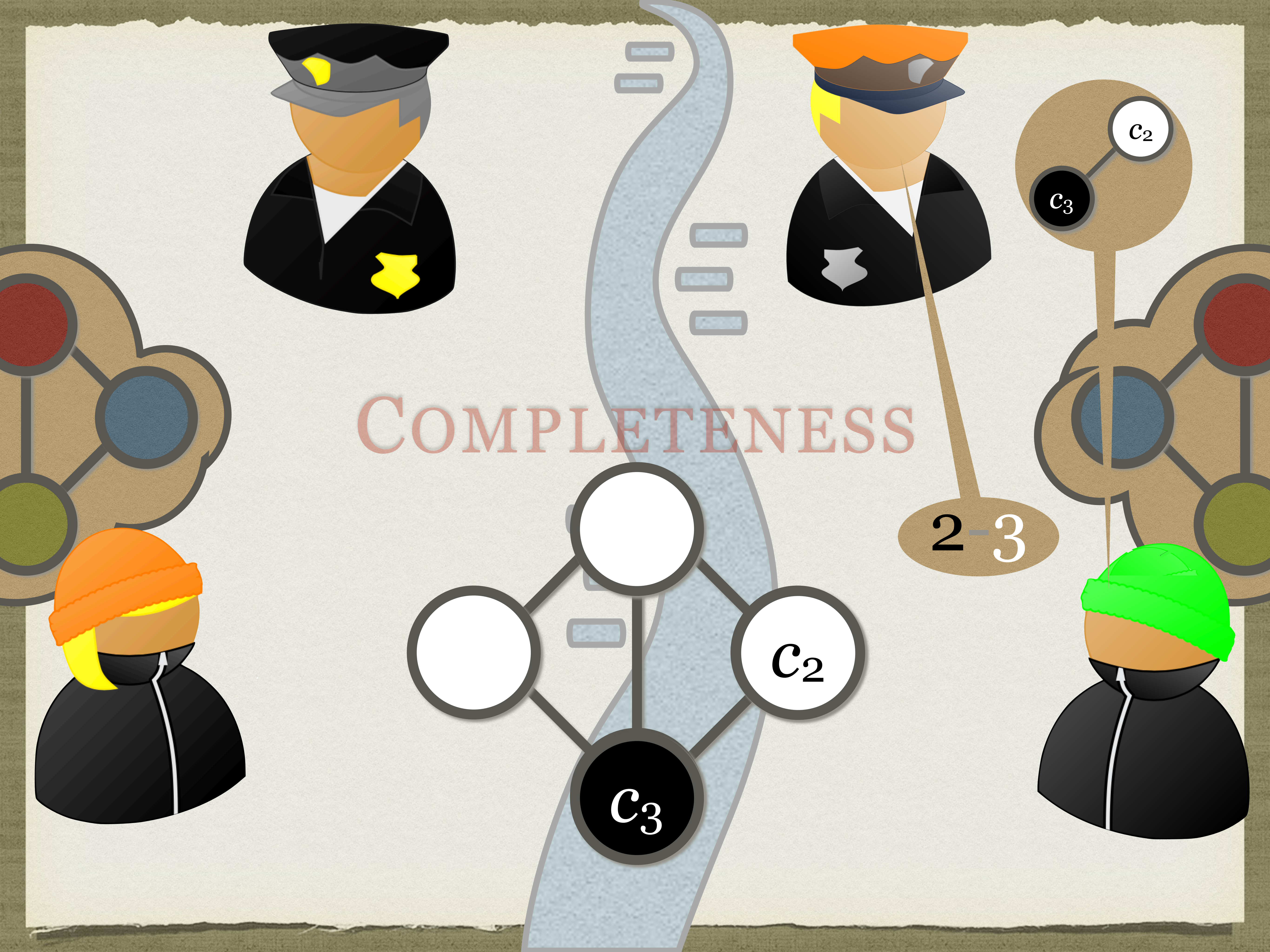
COMPLETENESS



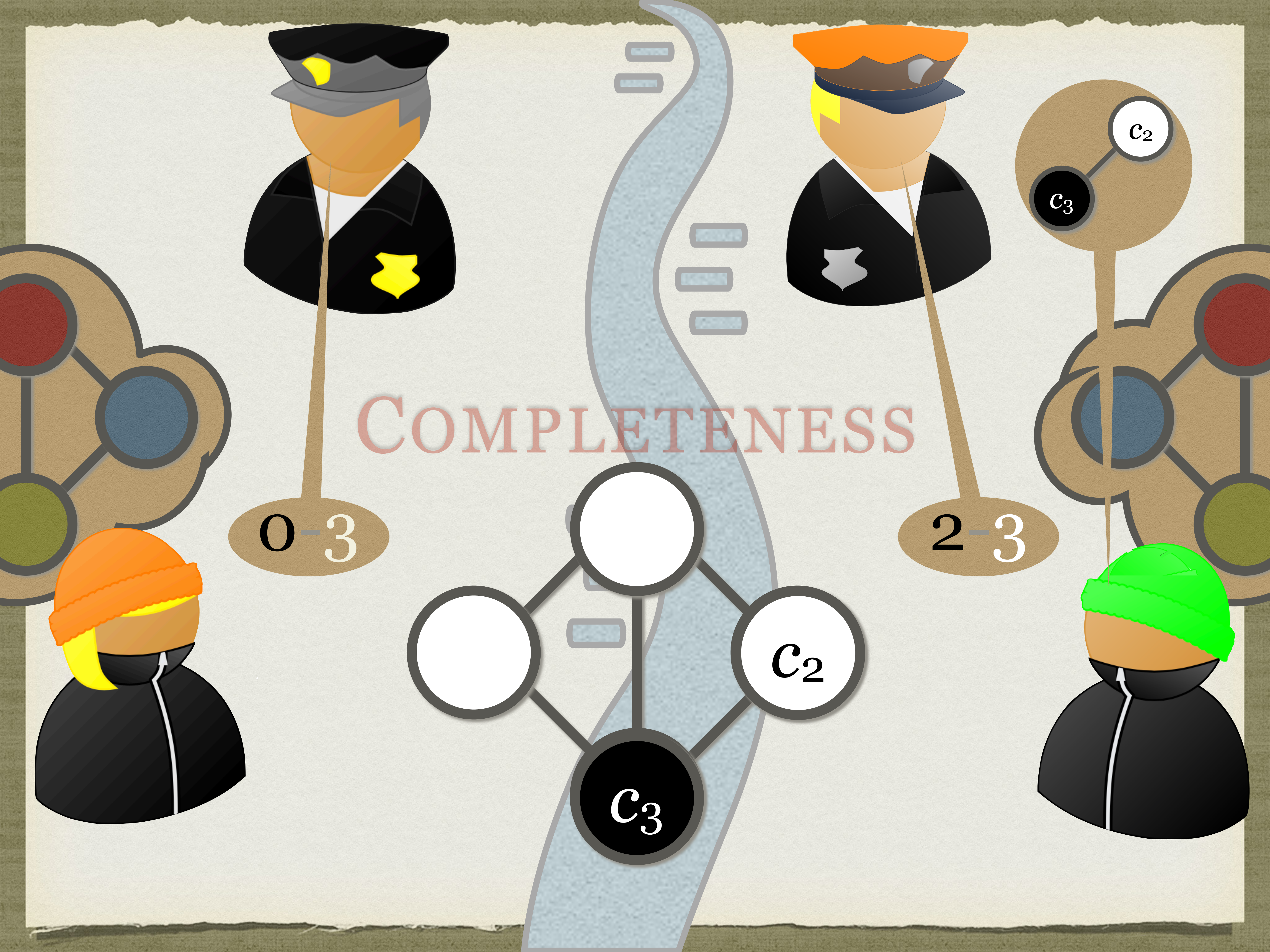
COMPLETENESS



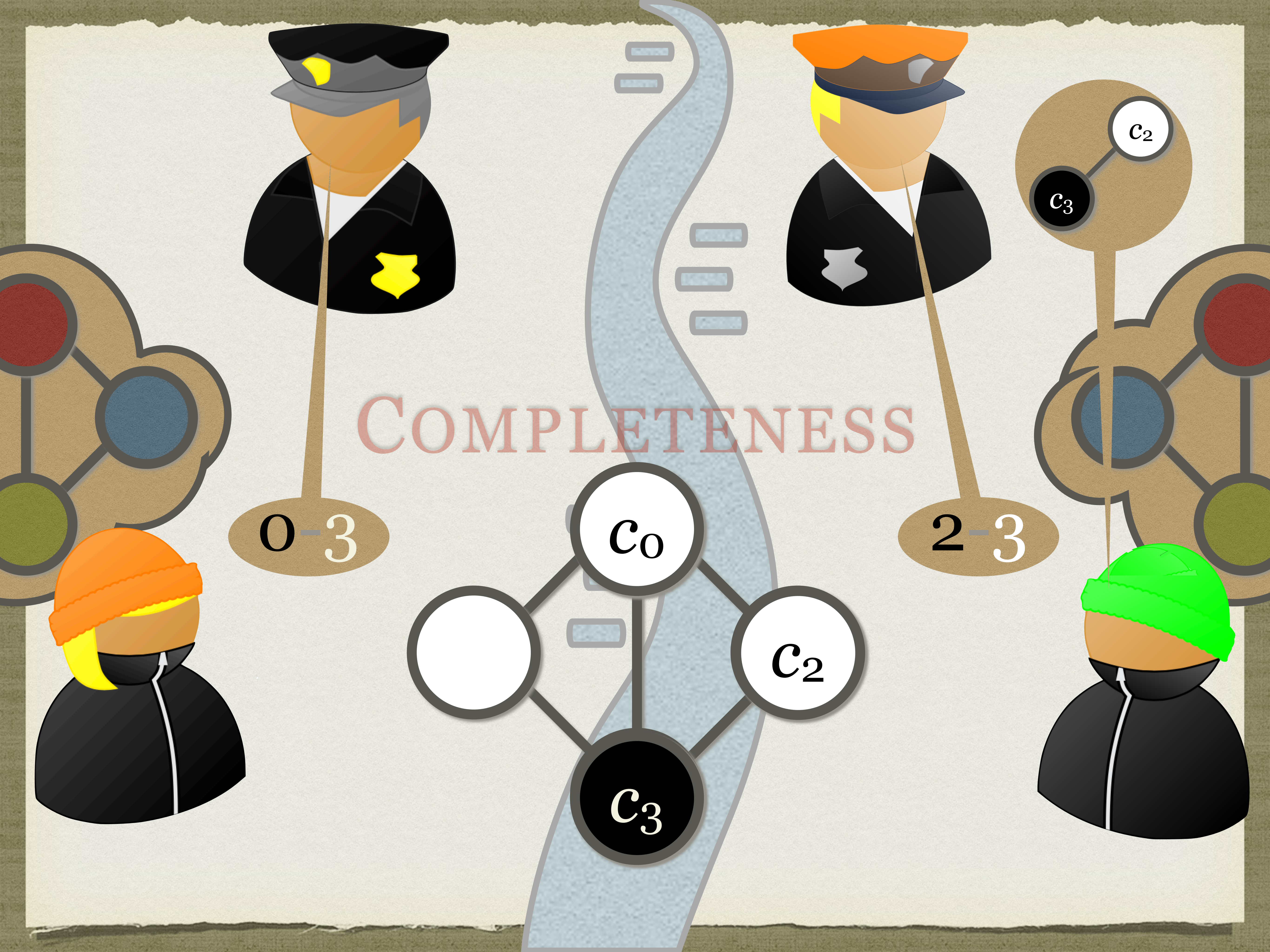
COMPLETENESS



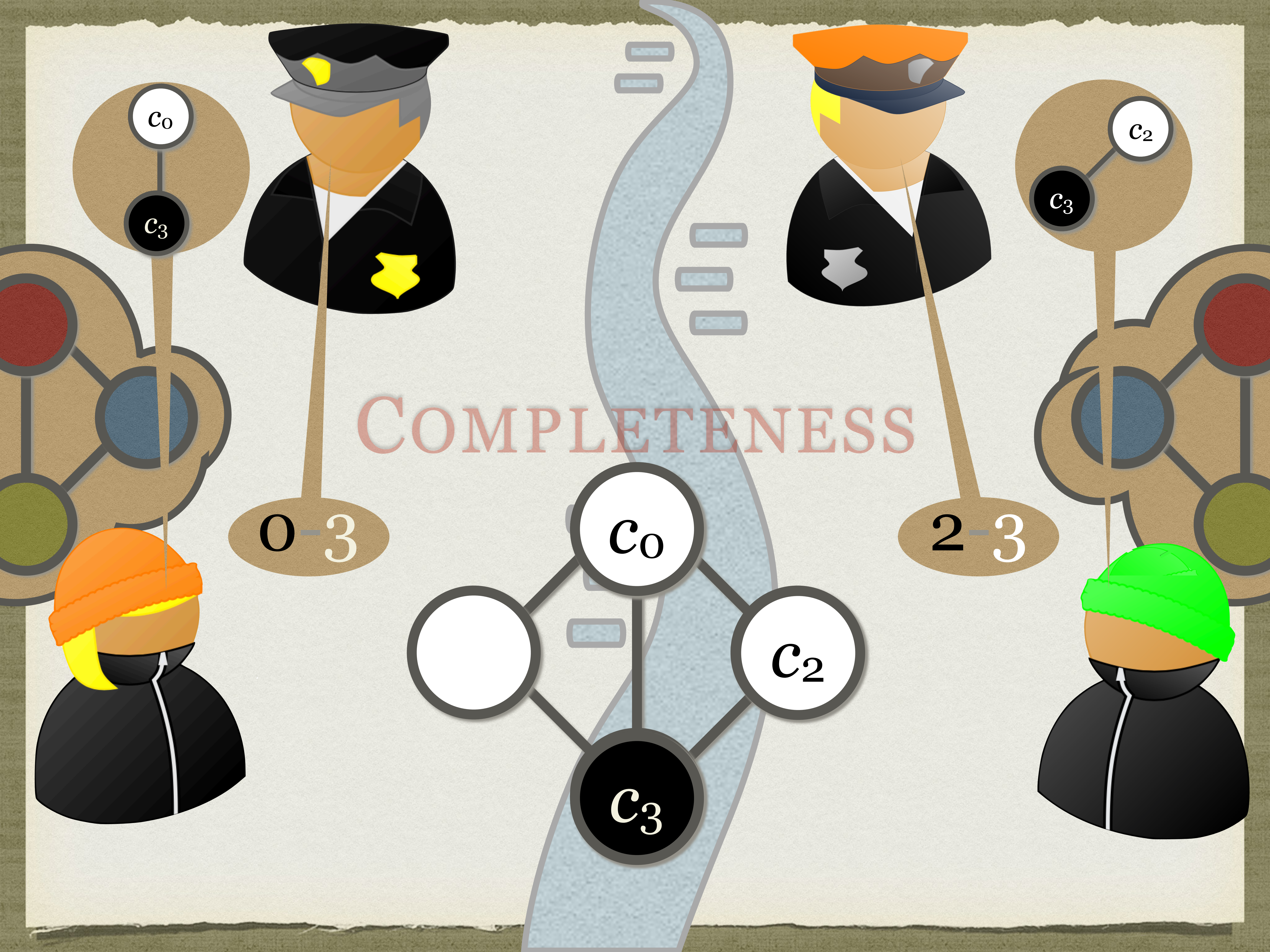
COMPLETENESS



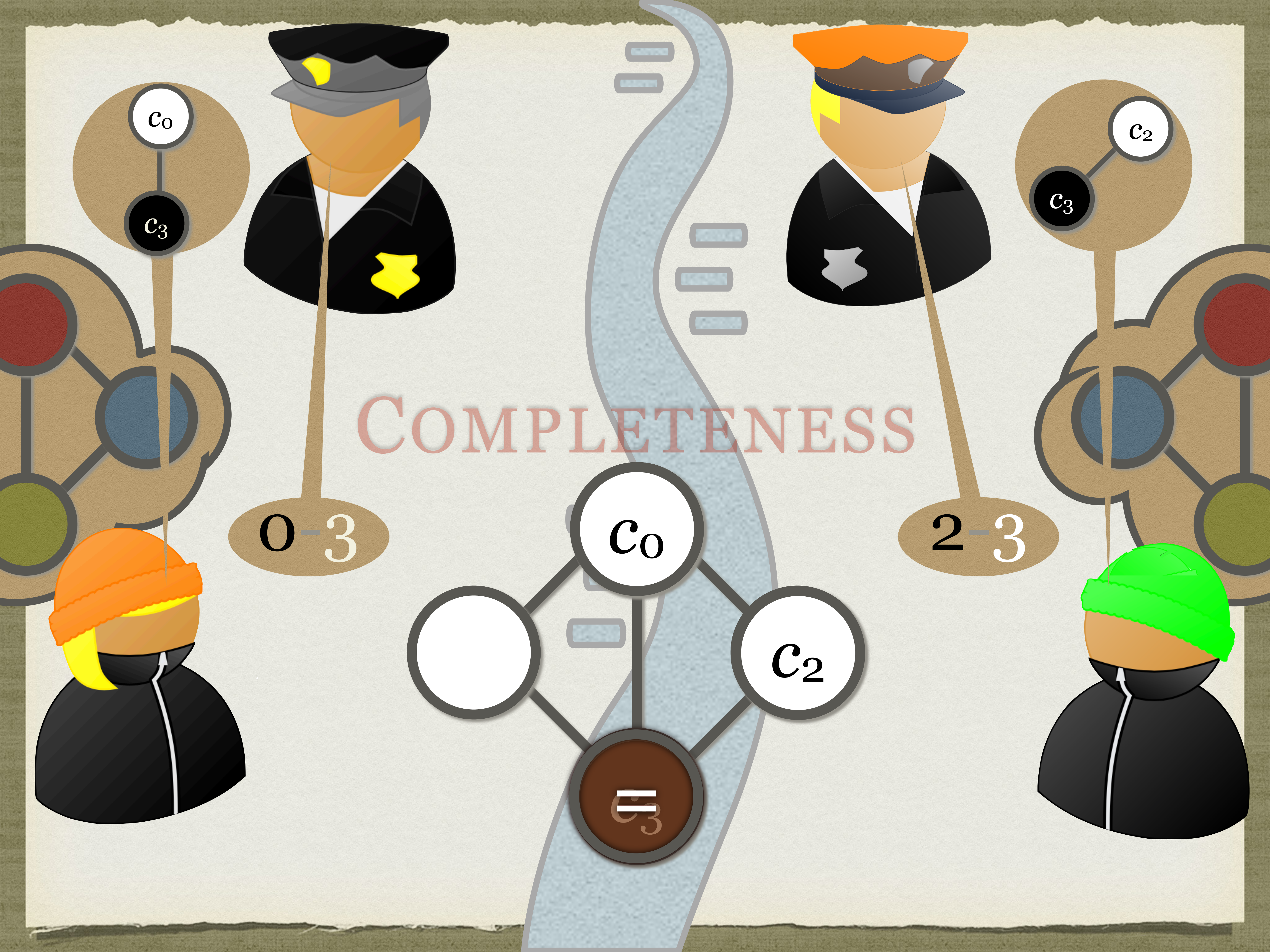
Completeness

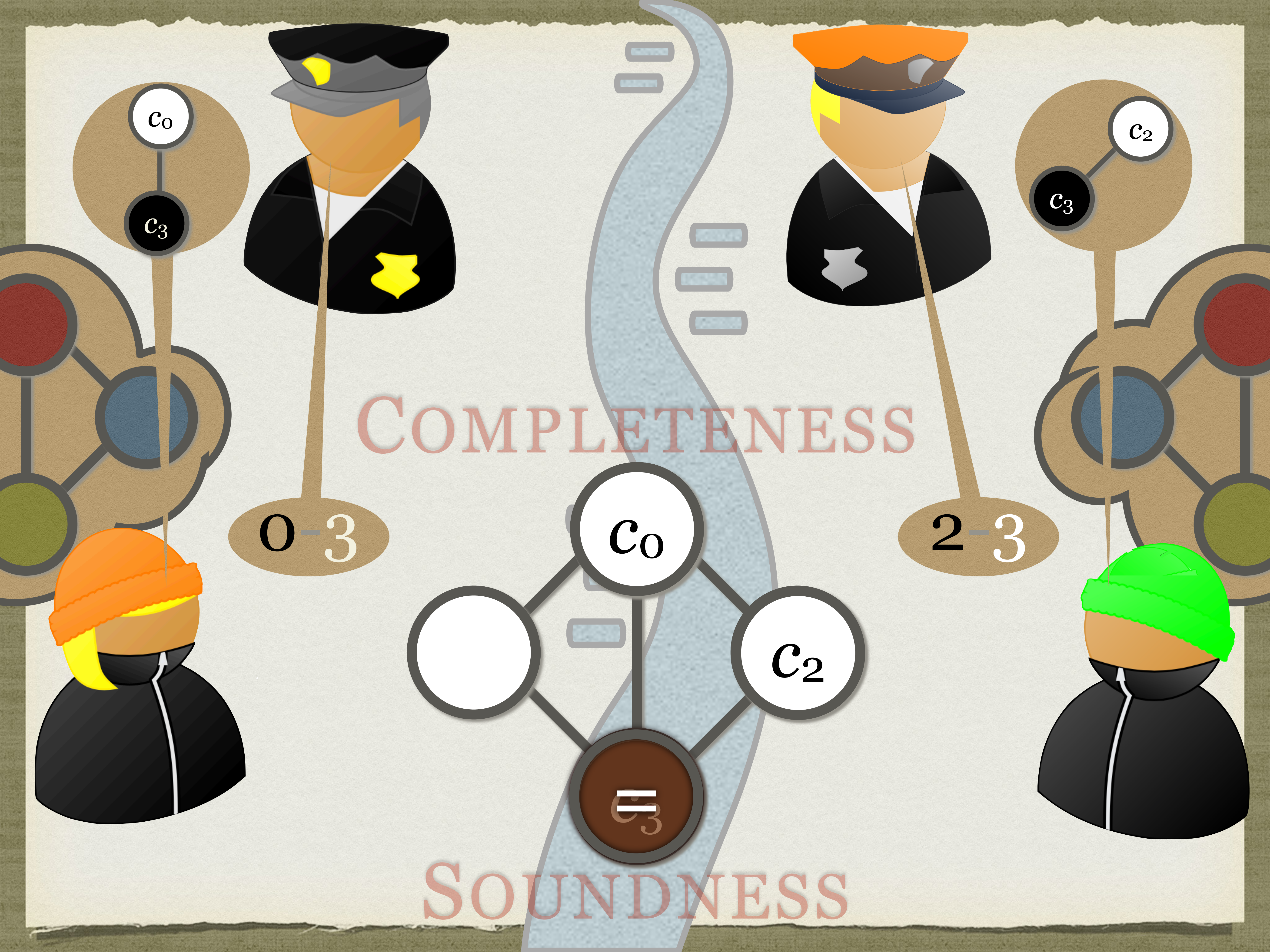


COMPLETENESS



COMPLETENESS

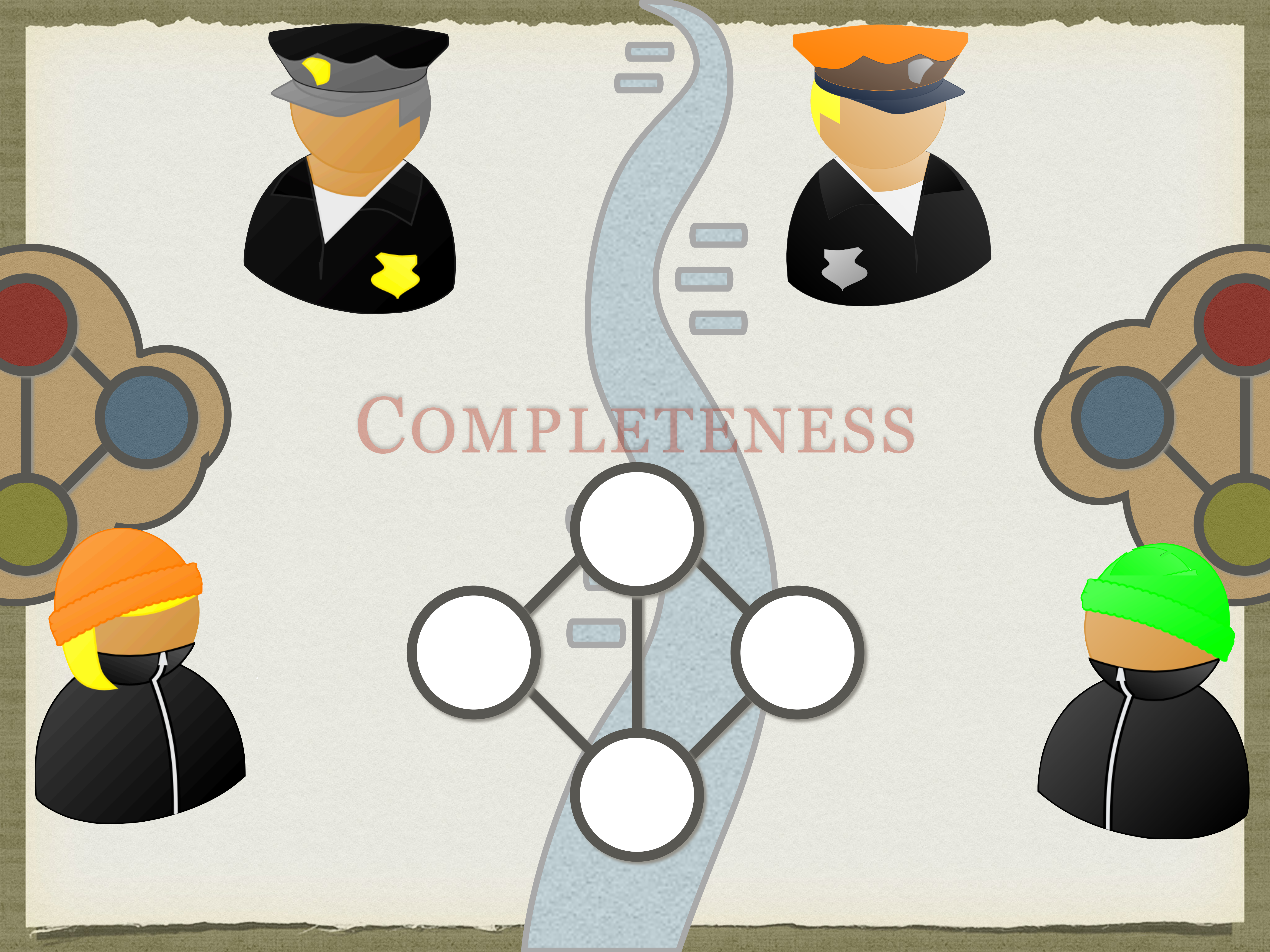


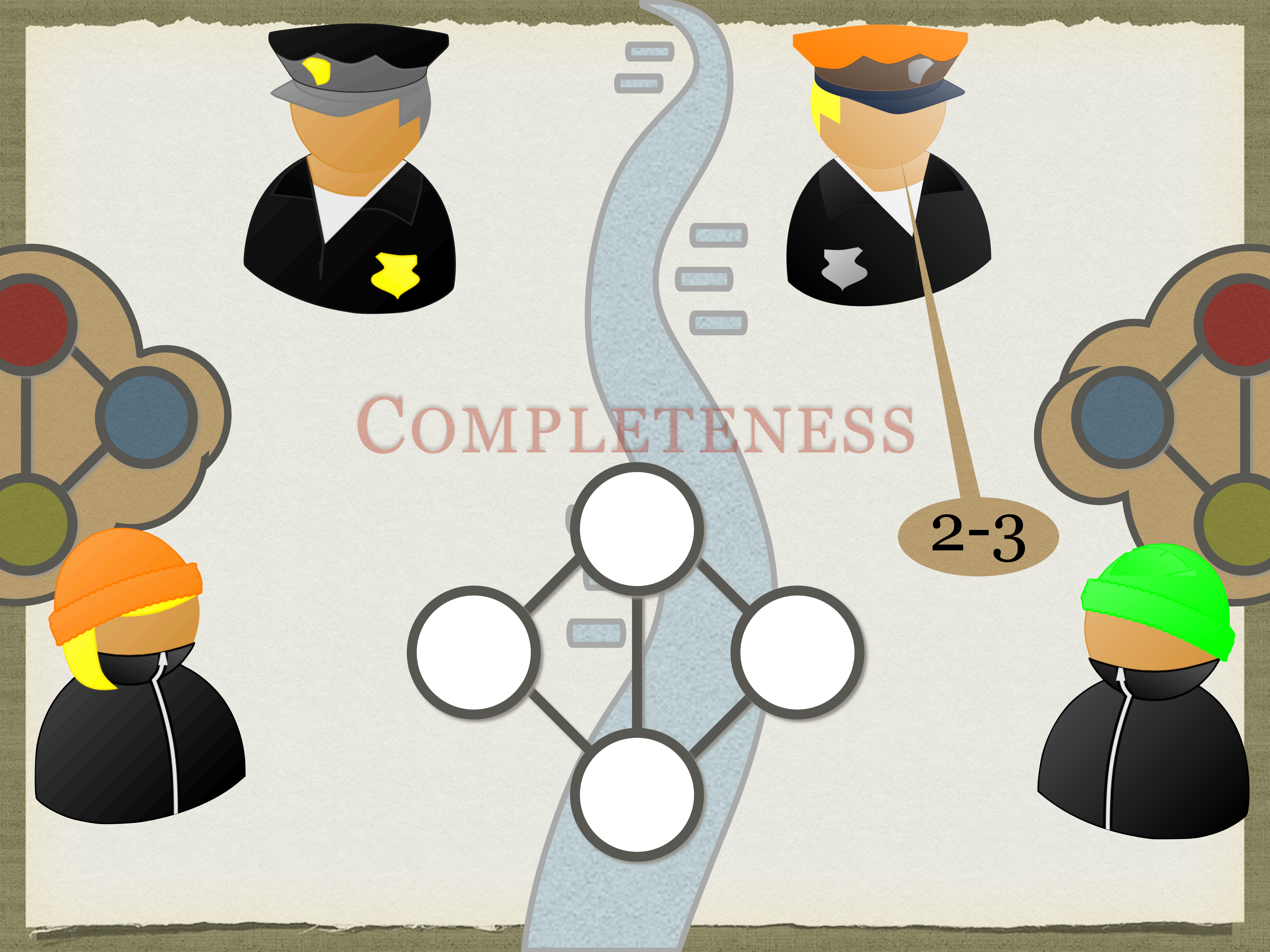


COMPLETENESS

SOUNDNESS

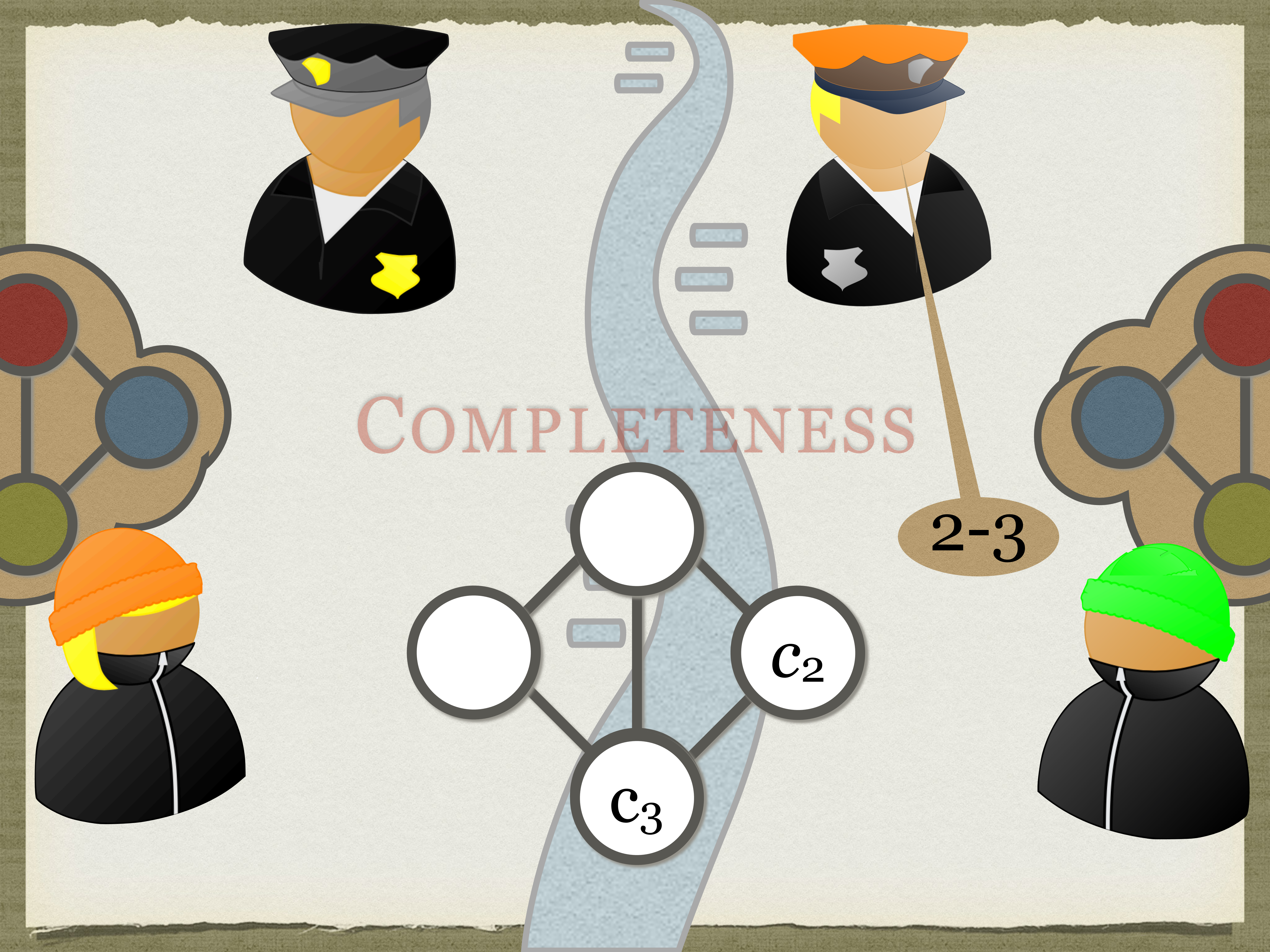
COMPLETENESS



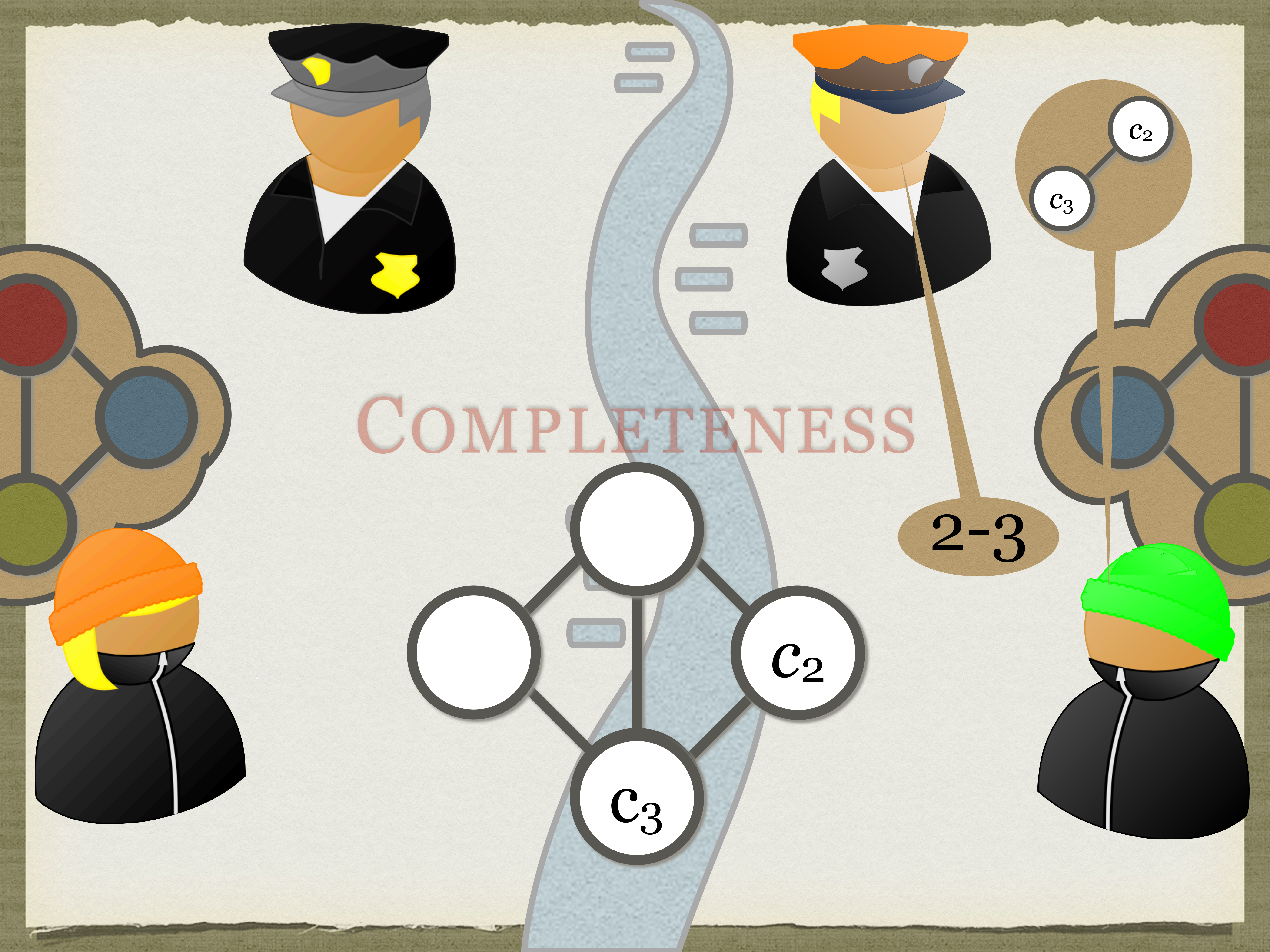


COMPLETENESS

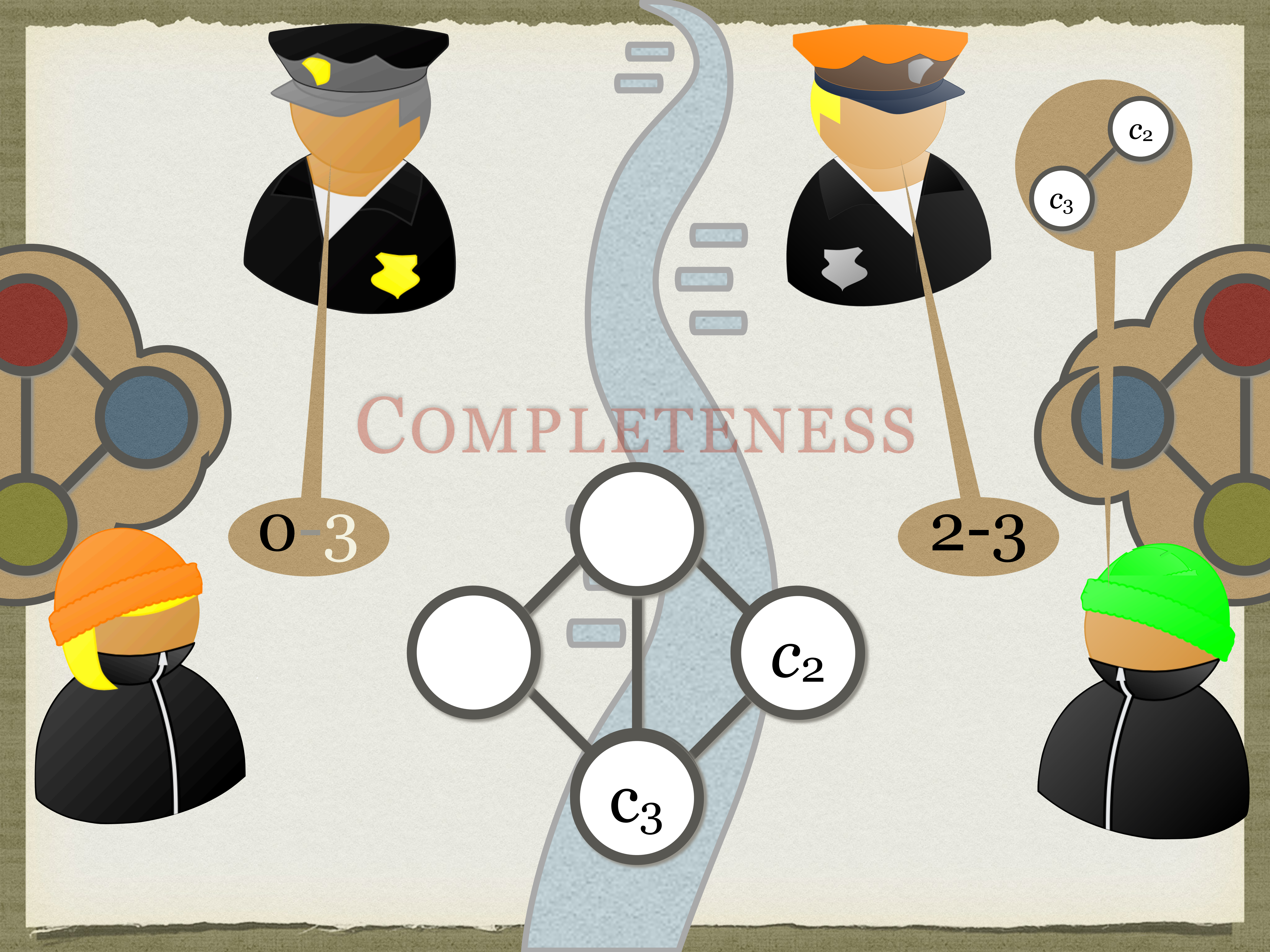
COMPLETENESS



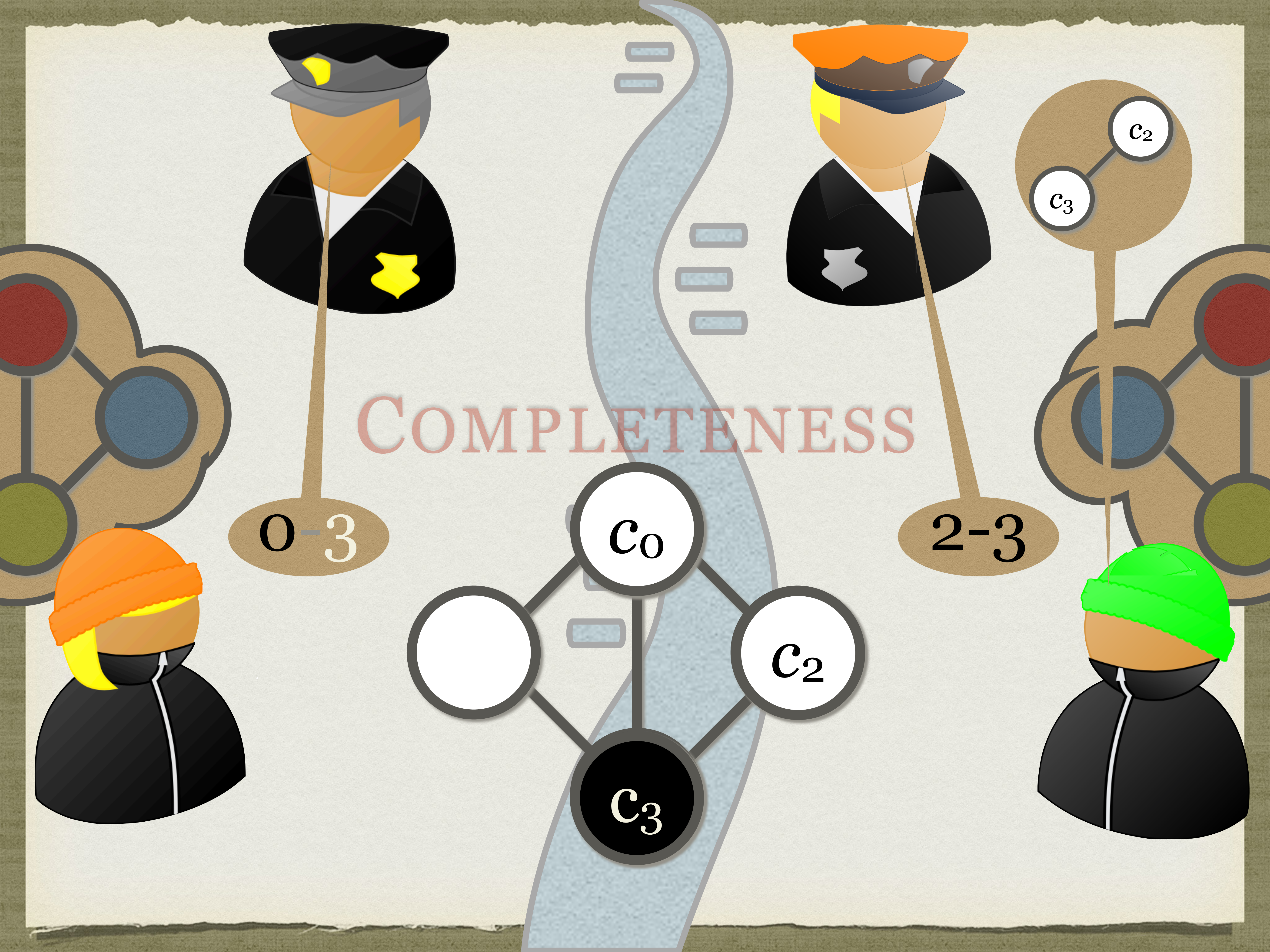
COMPLETENESS



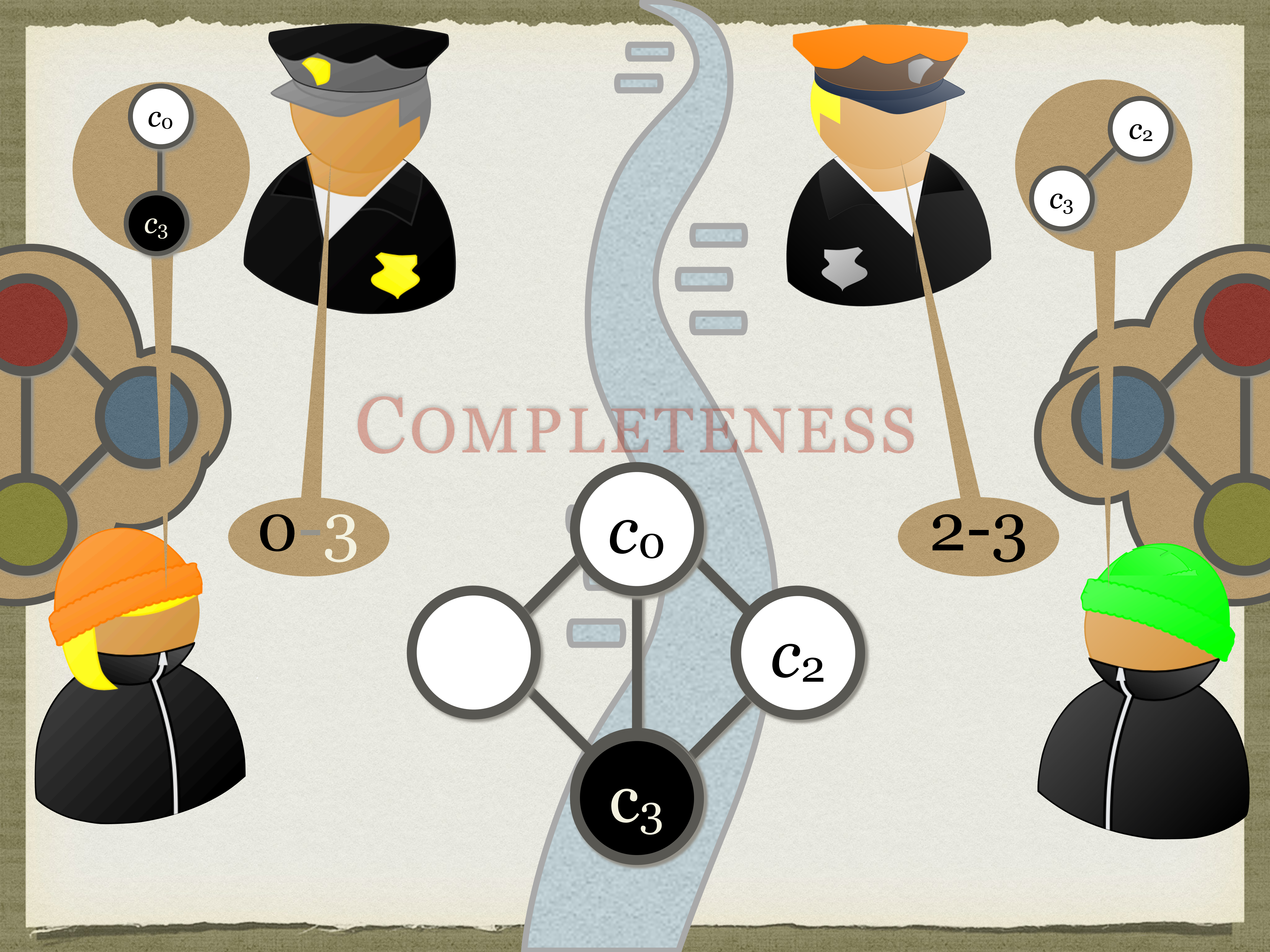
COMPLETENESS



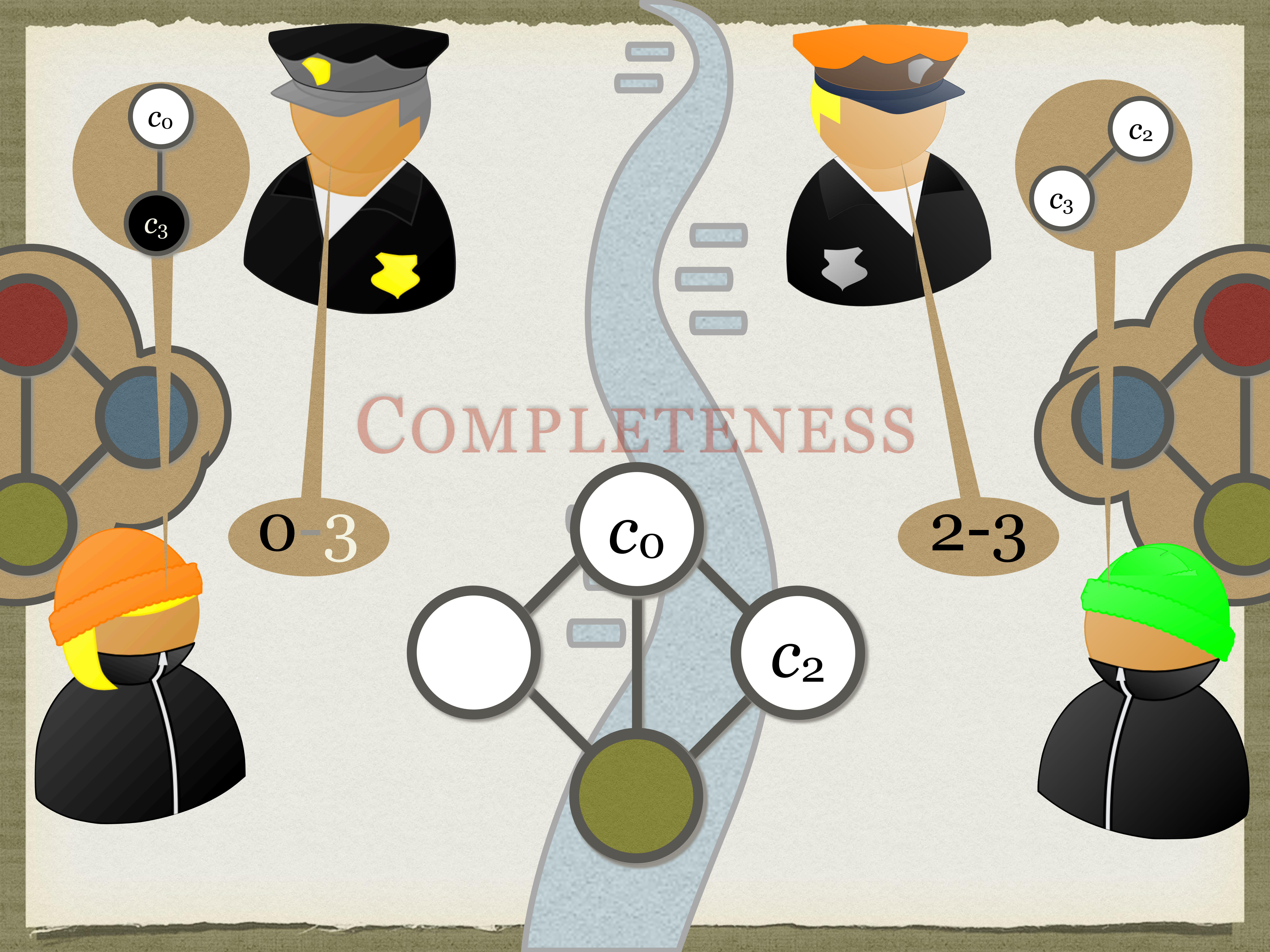
Completeness

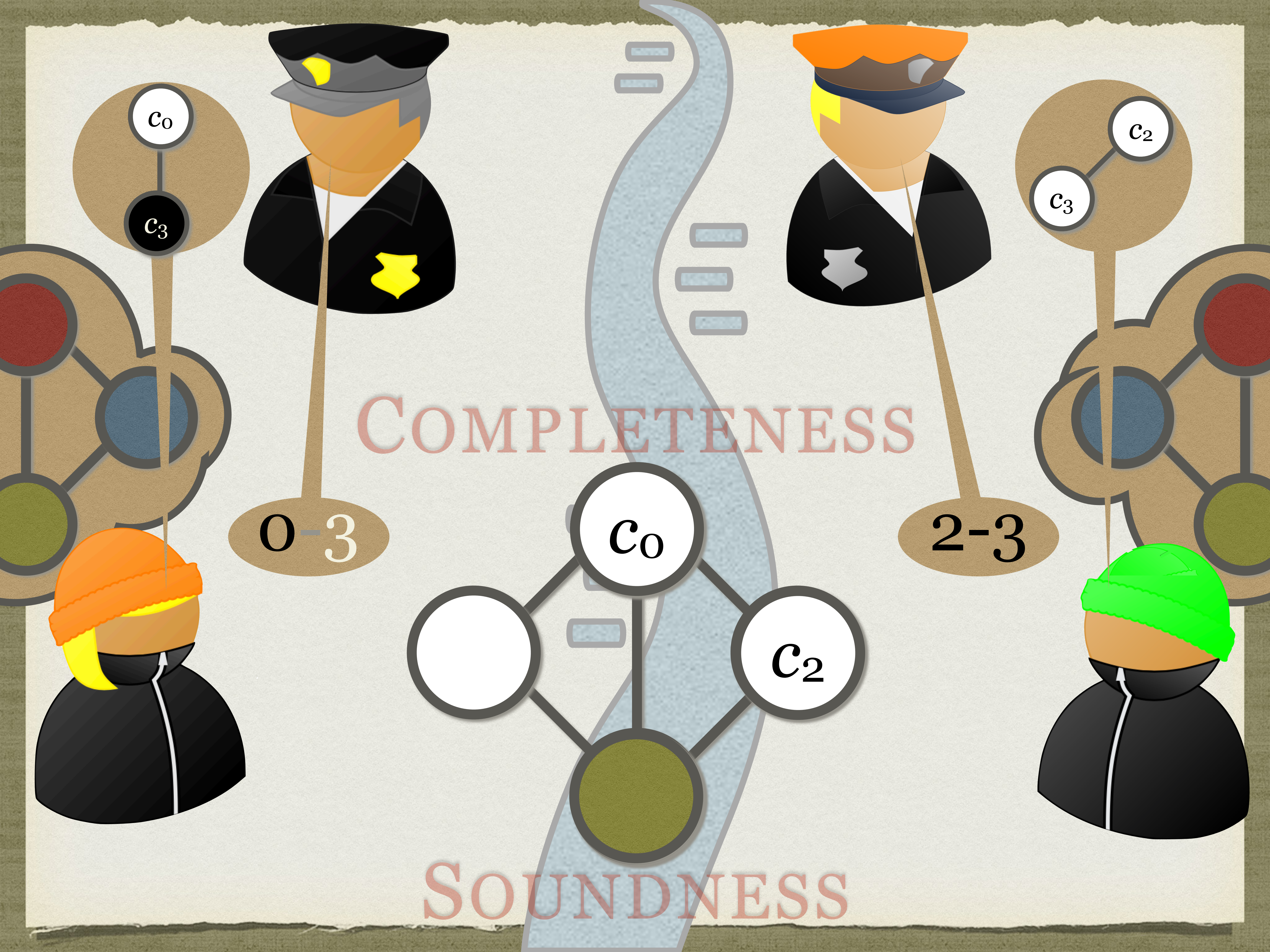


COMPLETENESS



Completeness

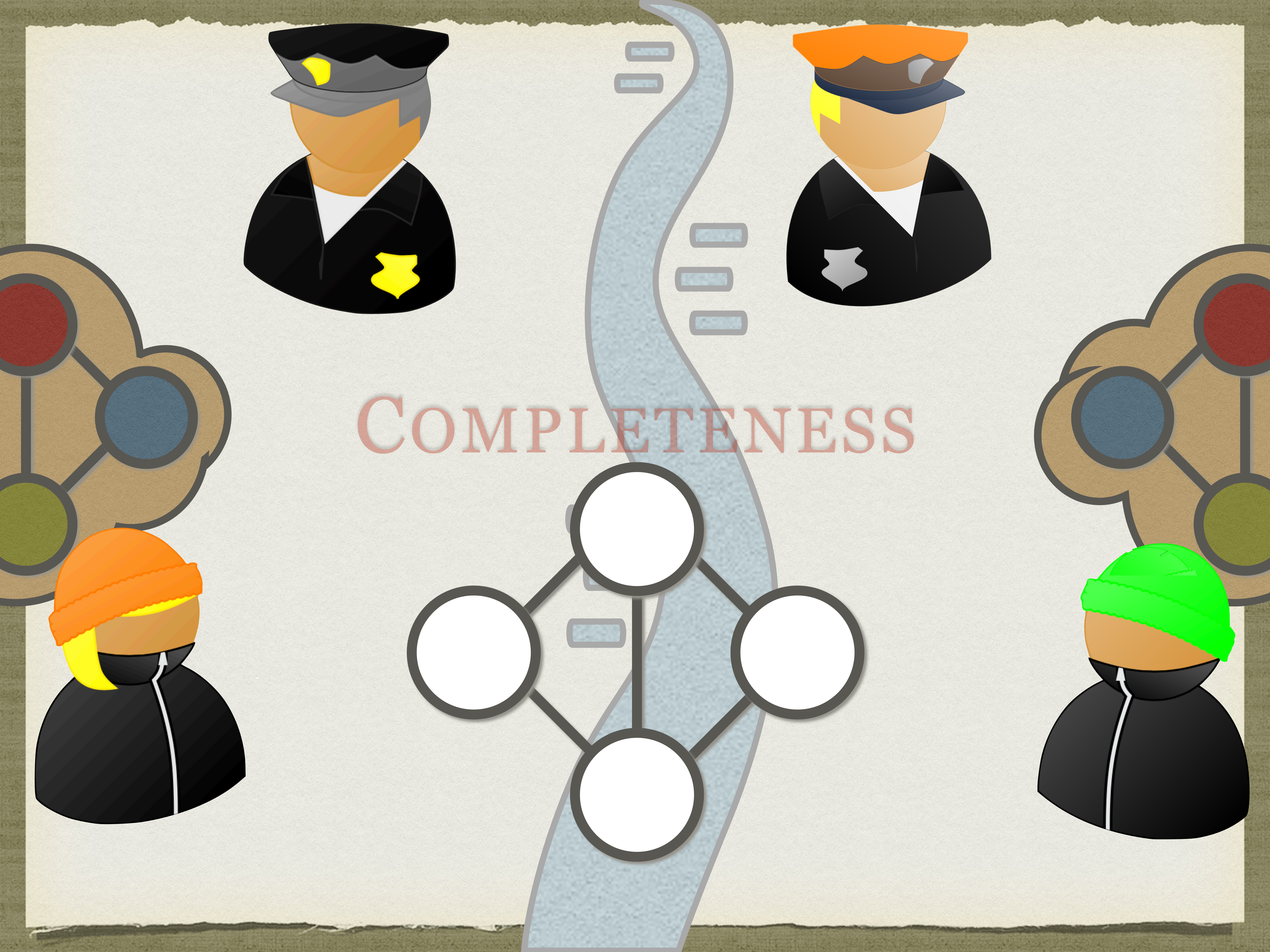




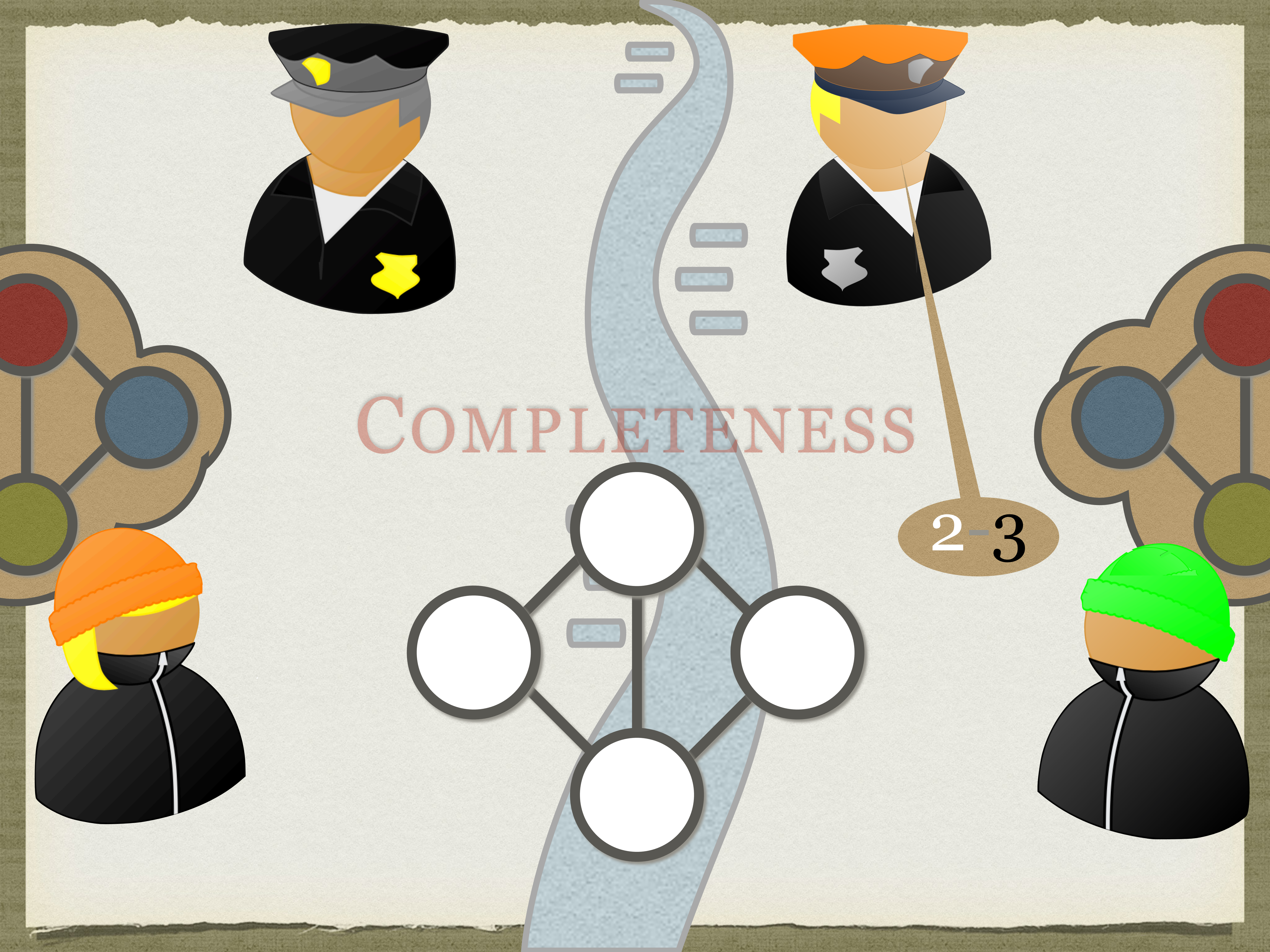
COMPLETENESS

SOUNDNESS

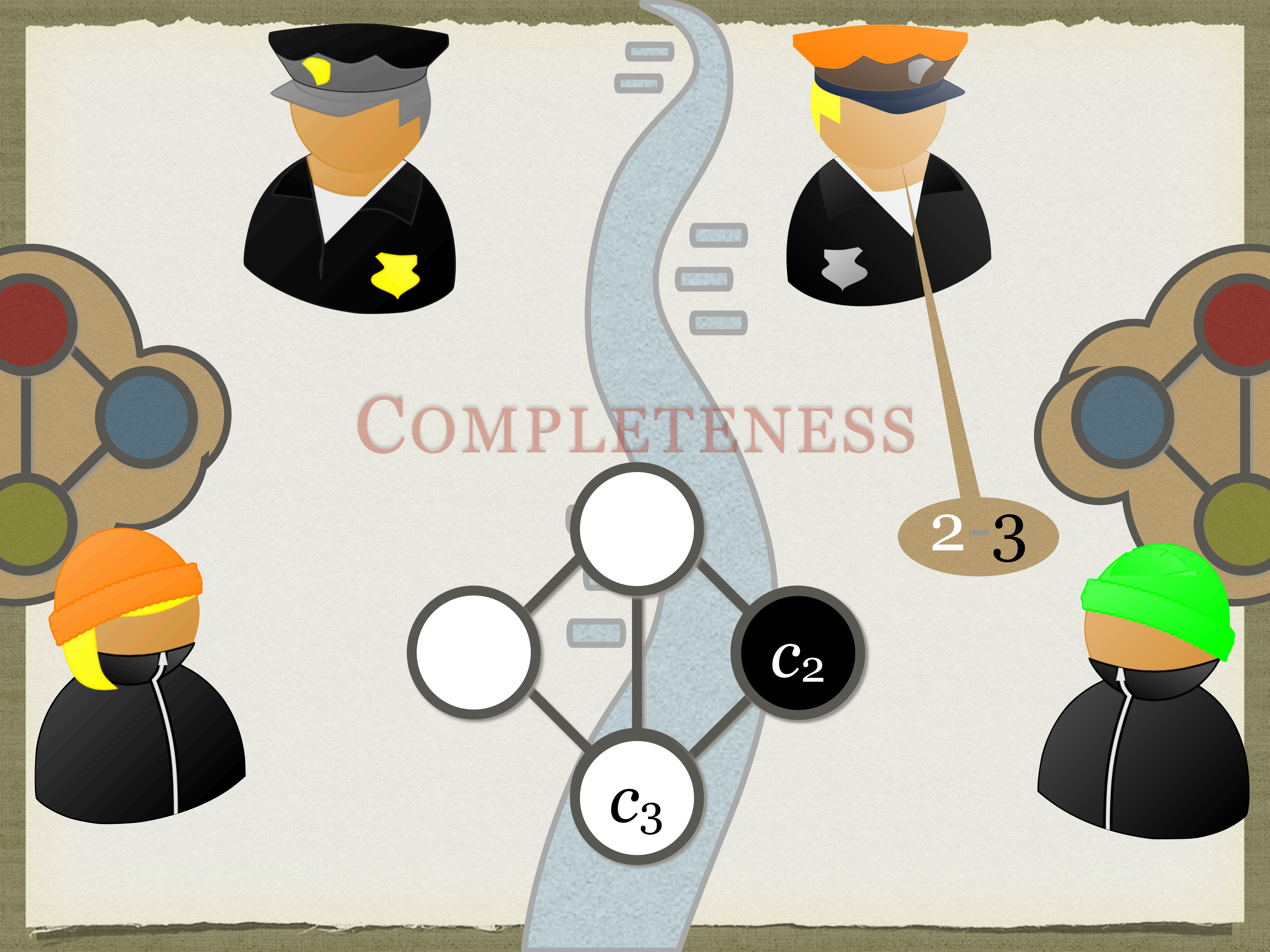
Completeness



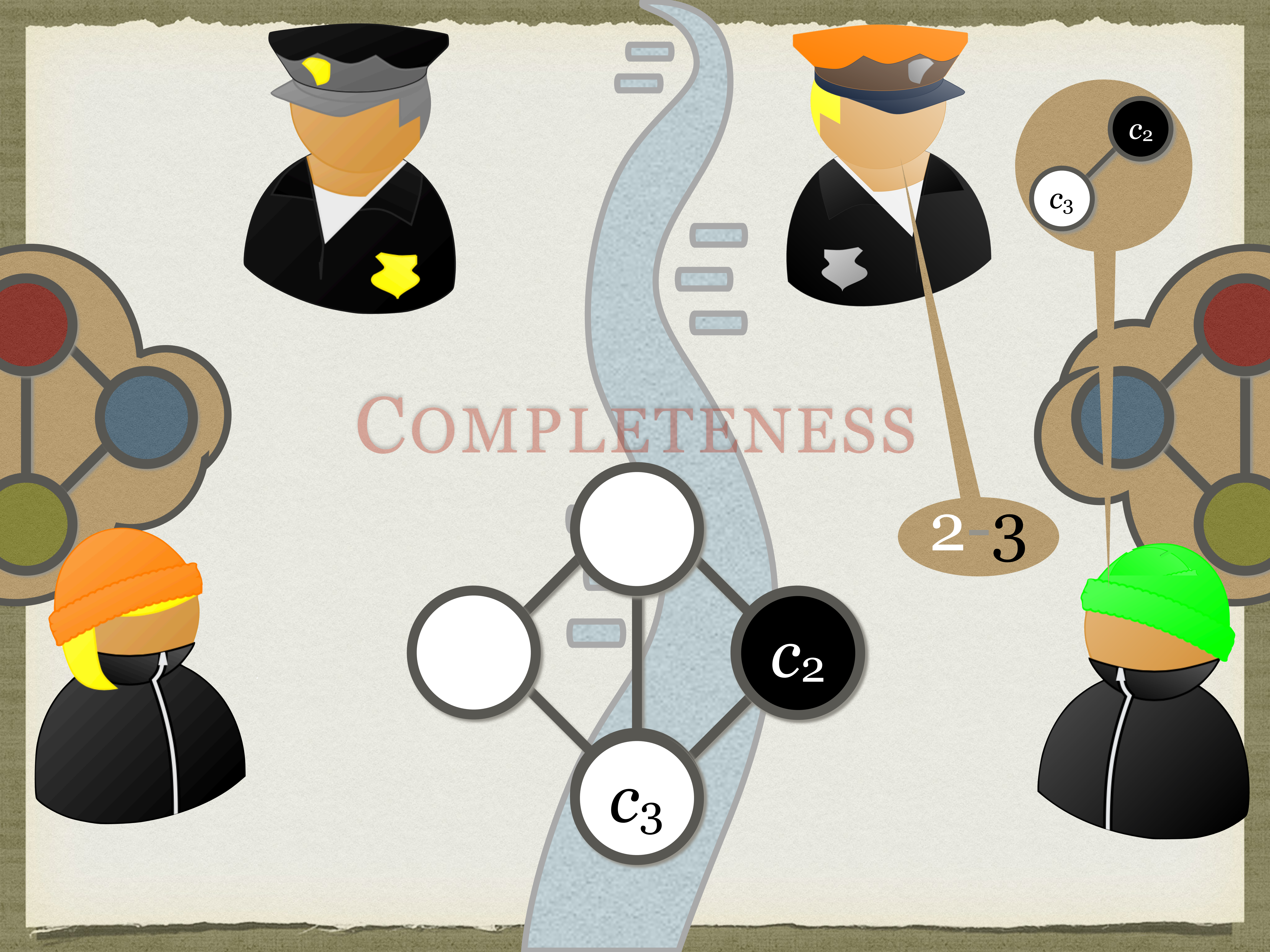
Completeness



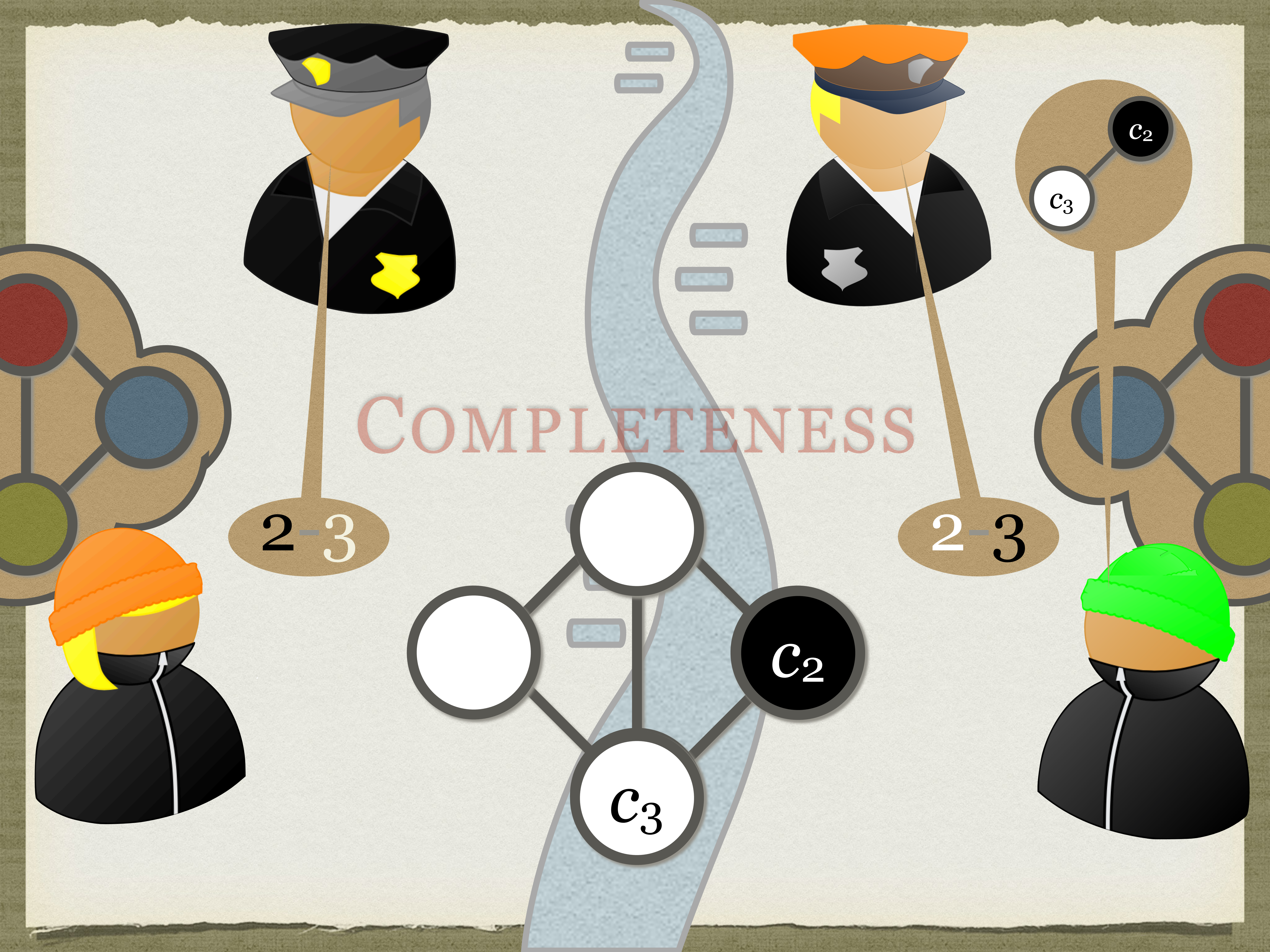
Completeness



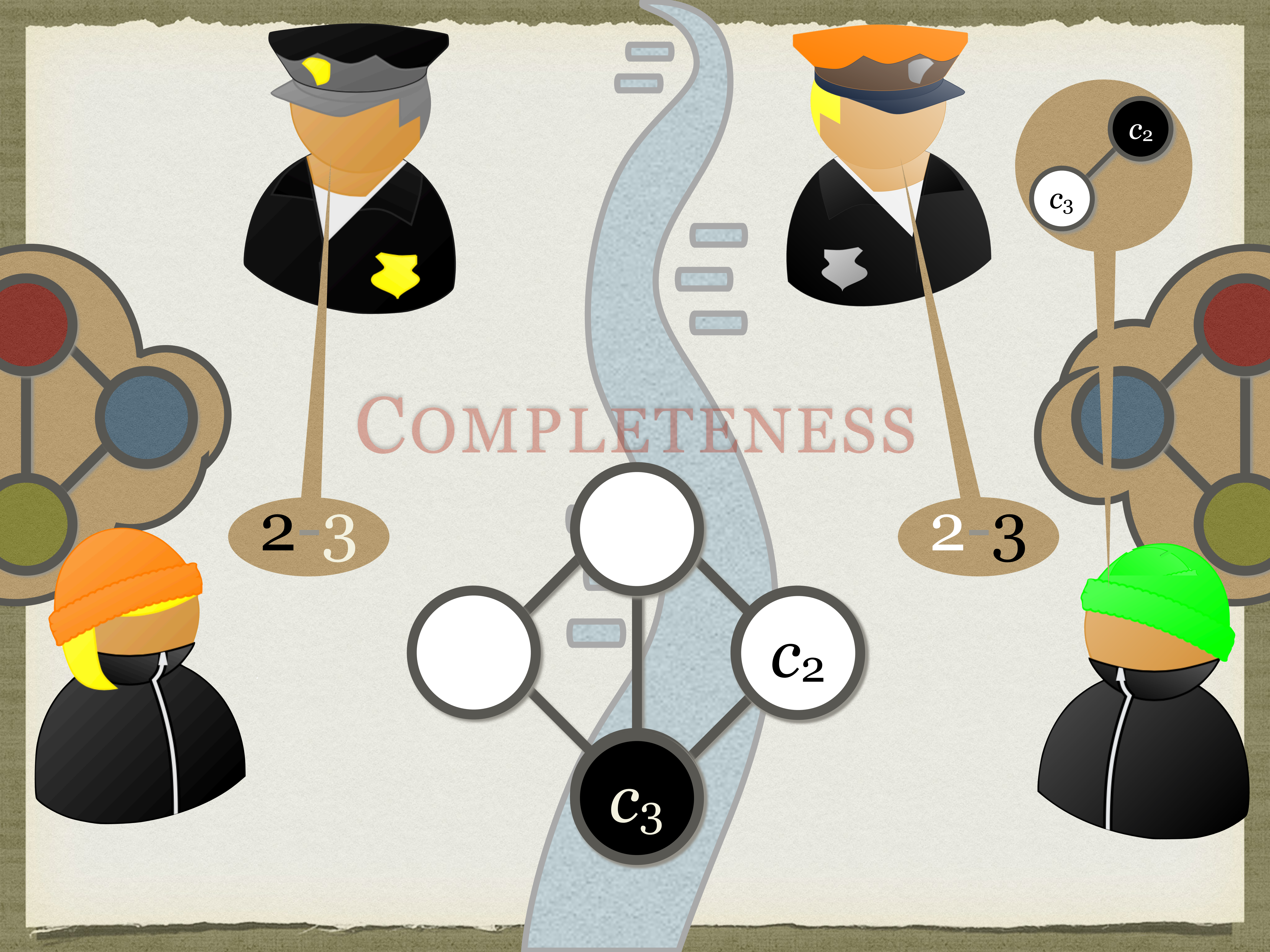
COMPLETENESS



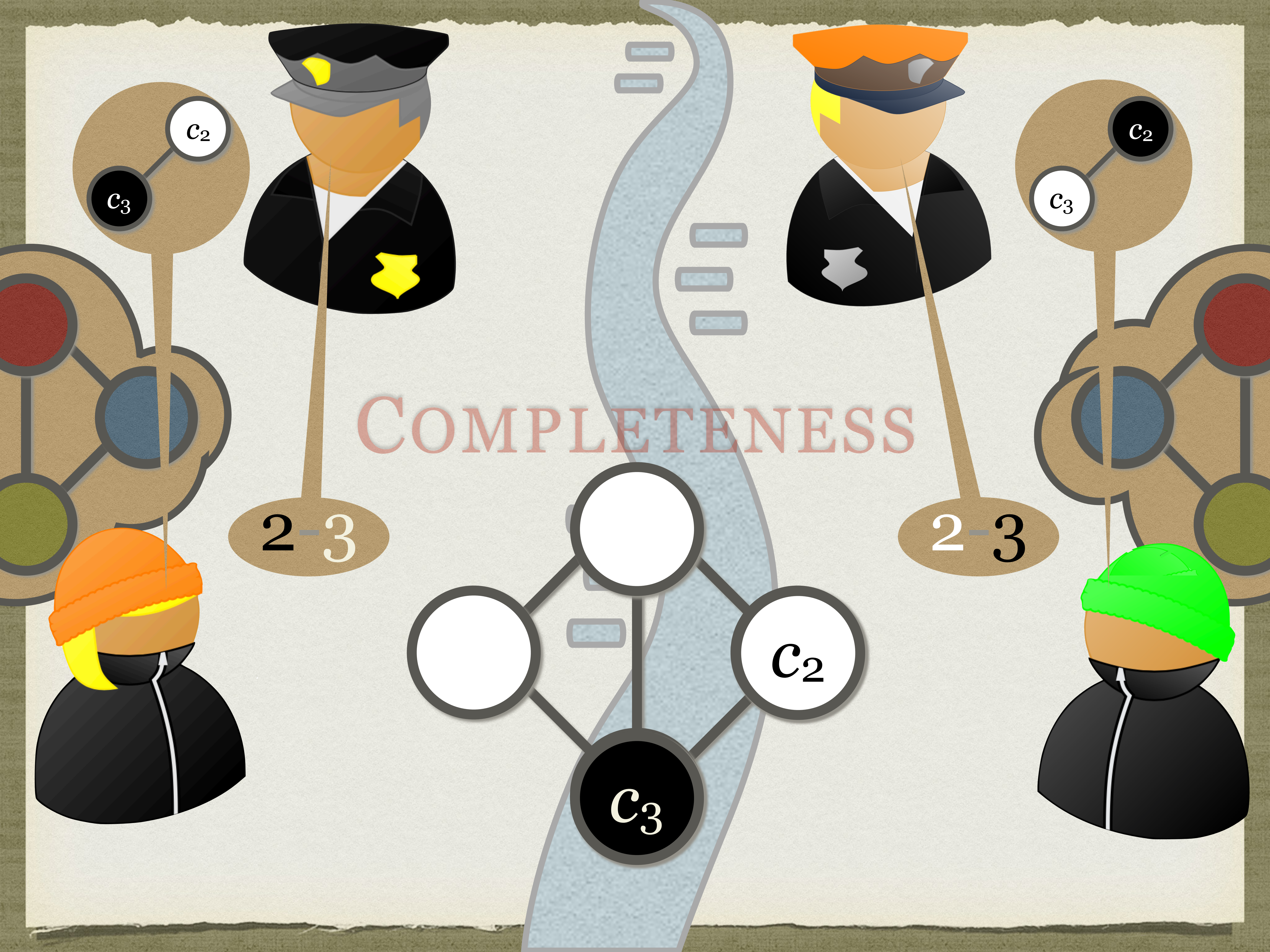
COMPLETENESS



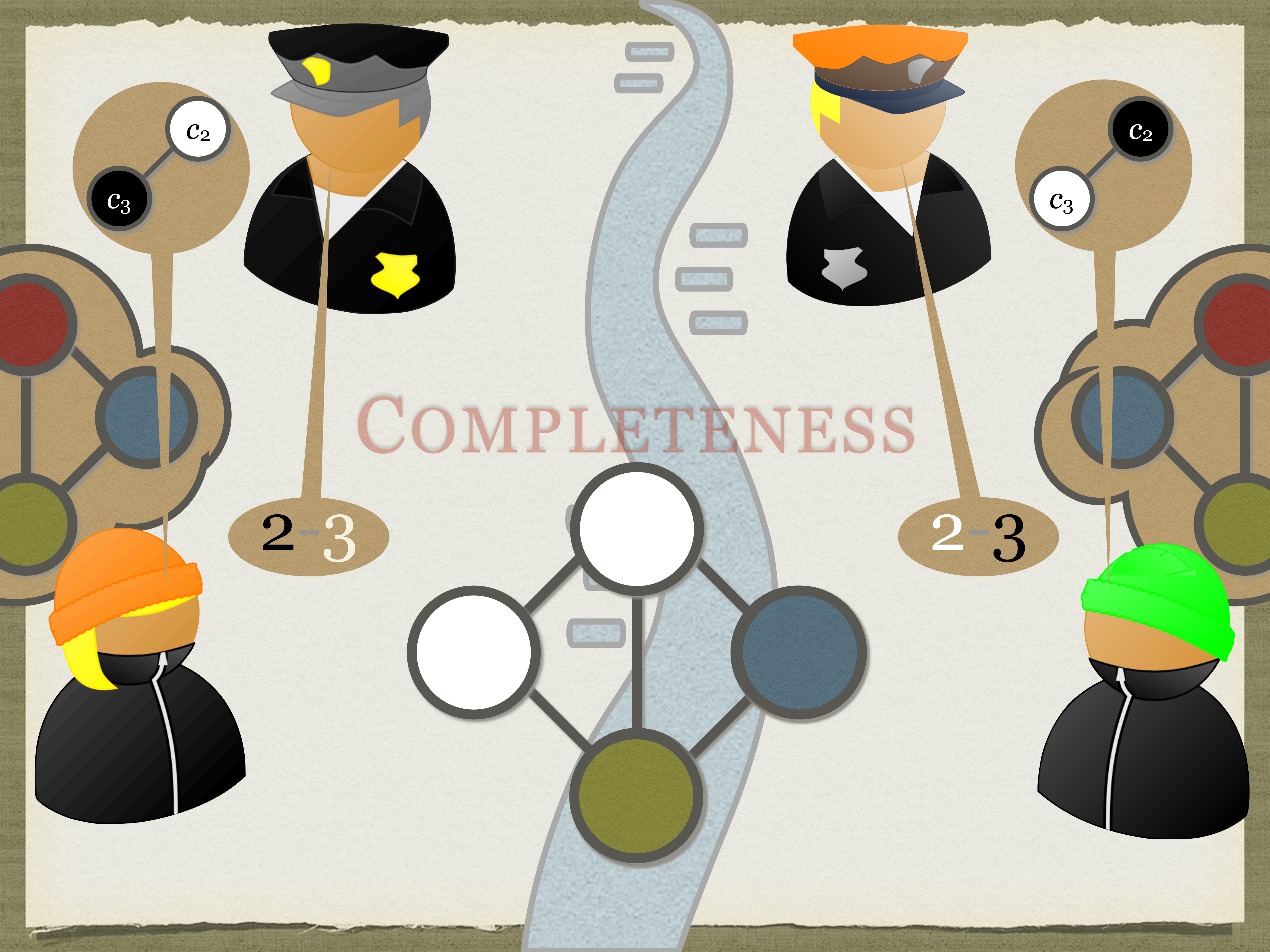
COMPLETENESS

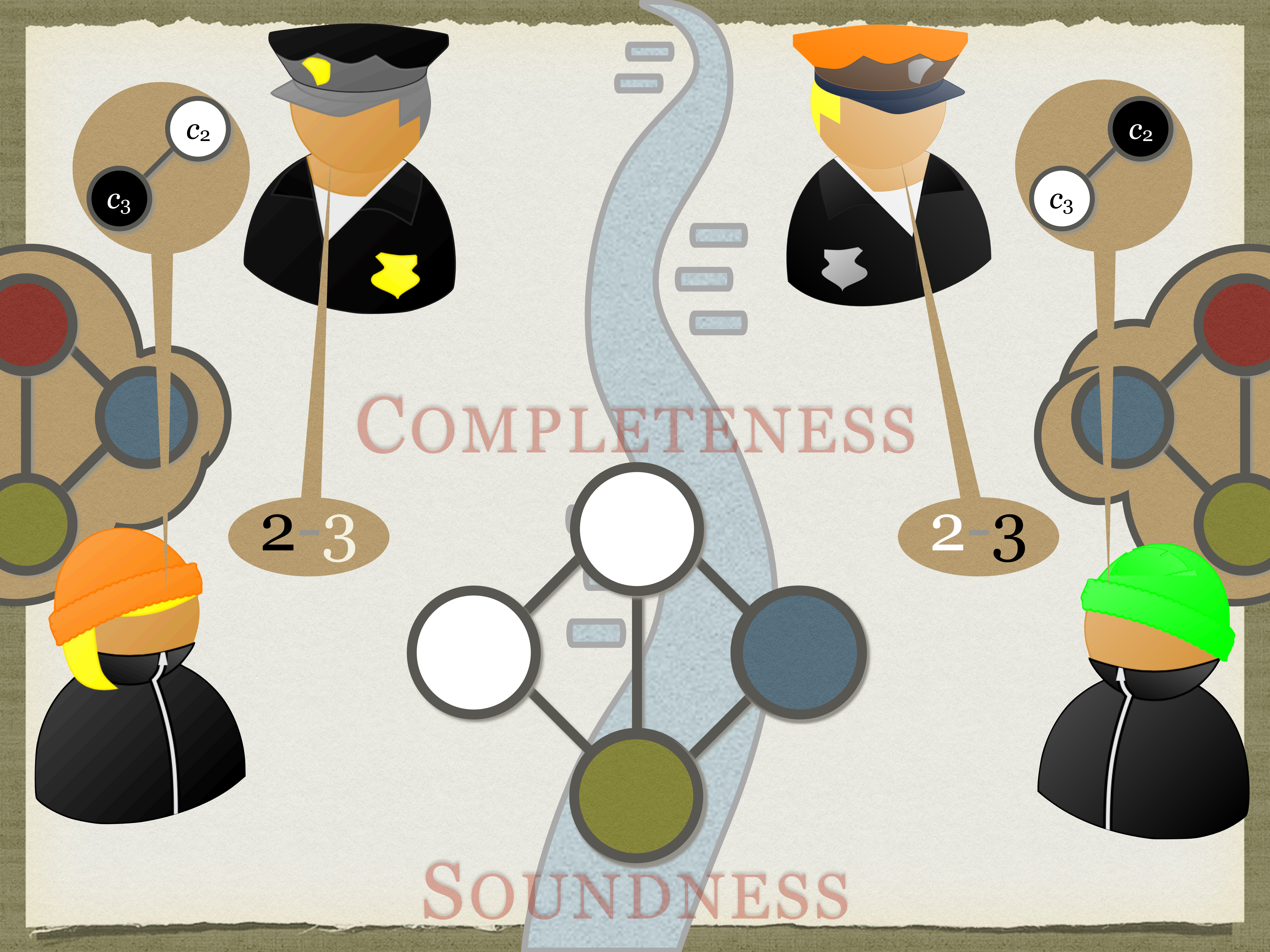


COMPLETENESS



COMPLETENESS





Completeness

Soundness

(LOCAL) SOUNDNESS

HONEST:

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

CASE ANALYSIS

(LOCAL) SOUNDNESS

HONEST:

$$COM^k[n_i, r_i, n_j, r_j] = (col_{n_i} + b_{n_i} r_i \; , \; col_{n_j} + b_{n_j} r_j)$$

DISHONEST:

CASE ANALYSIS

(LOCAL) SOUNDNESS

HONEST:

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

DISHONEST:

$$COM^k[n_i, r_i, n_j, r_j] = \text{arbitrary}$$

CASE ANALYSIS

(LOCAL) SOUNDNESS

HONEST:

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

DISHONEST:

$$COM^k[n_i, r_i, n_j, r_j] = \text{arbitrary}$$

$$COM[n_i, r_i] = \text{well-defined}$$

CASE ANALYSIS

(LOCAL) SOUNDNESS

HONEST:

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

DISHONEST:

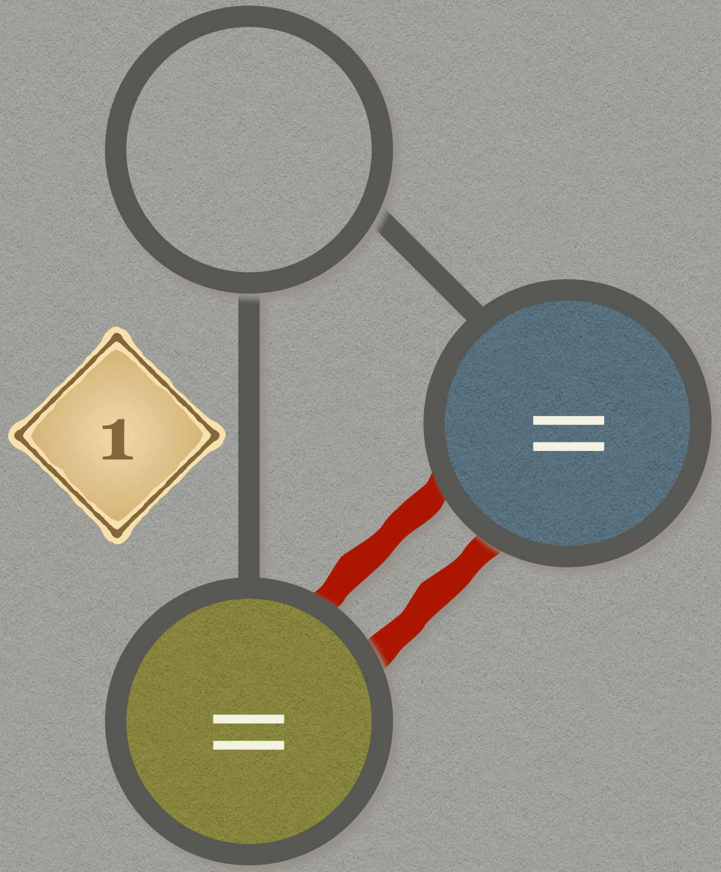
$COM^k[n_i, r_i, n_j, r_j]$ = arbitrary

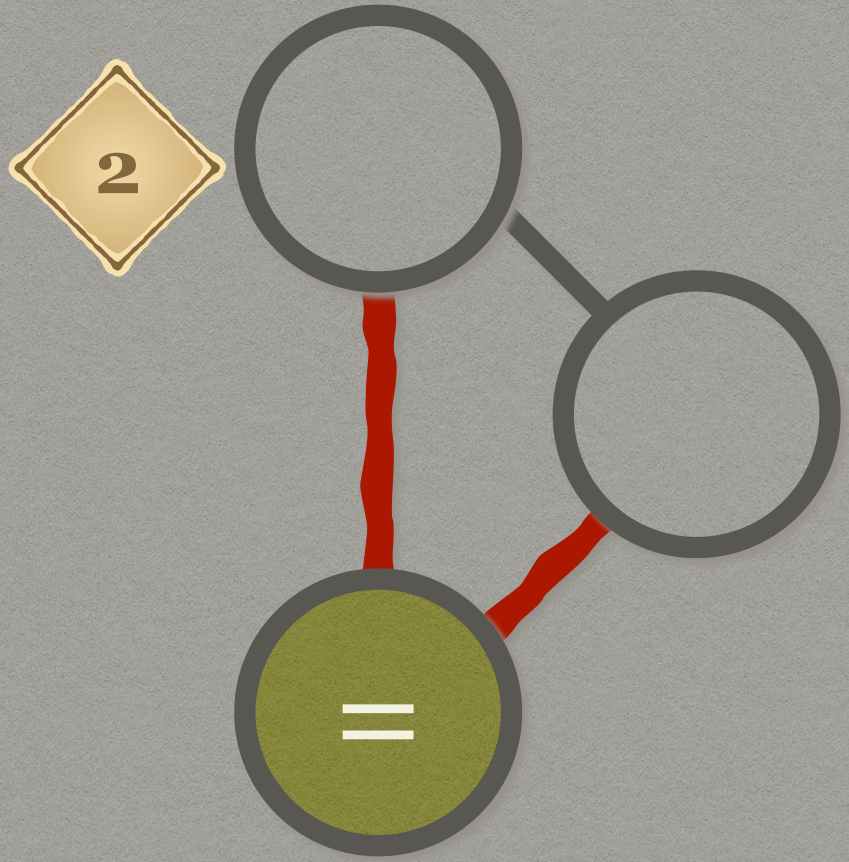
$COM[n_i, r_i]$ = well-defined

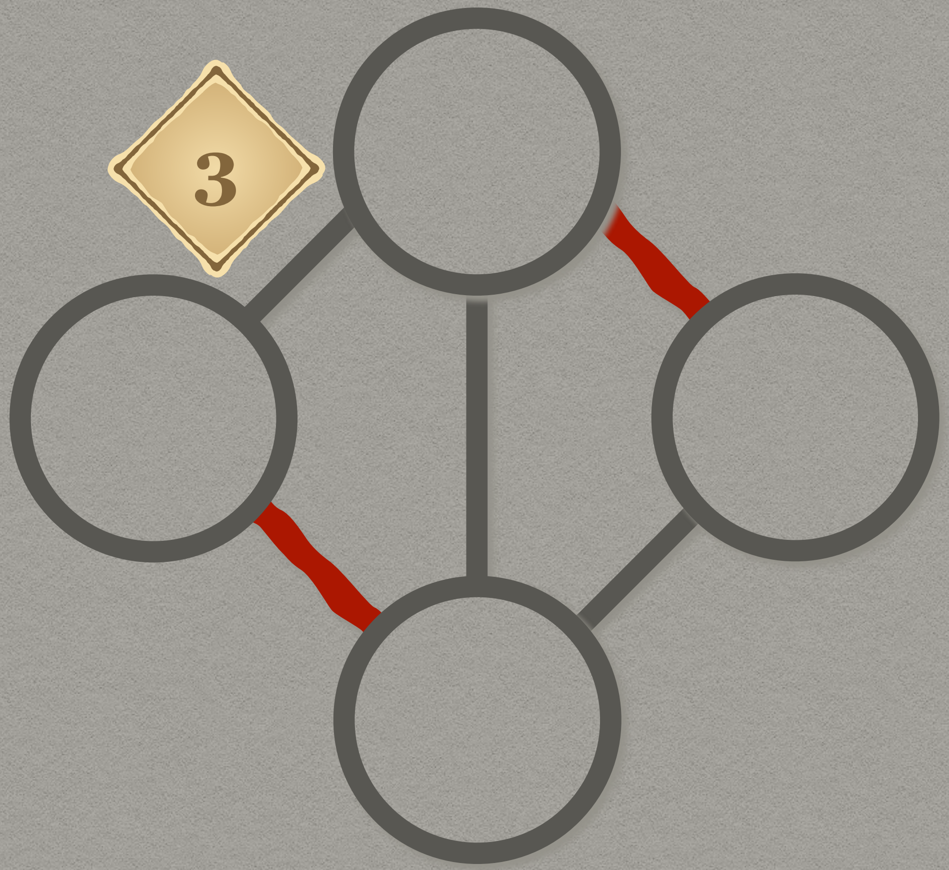
$COL[n_i]$ = well-defined

CASE ANALYSIS

ZK SIMULATION

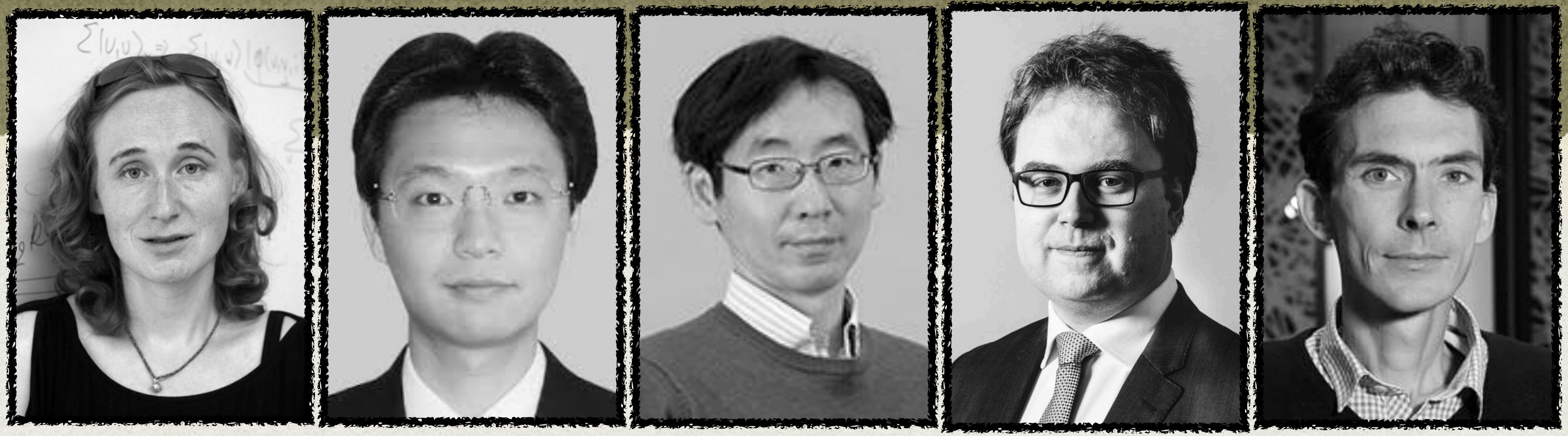






CASE ANALYSIS

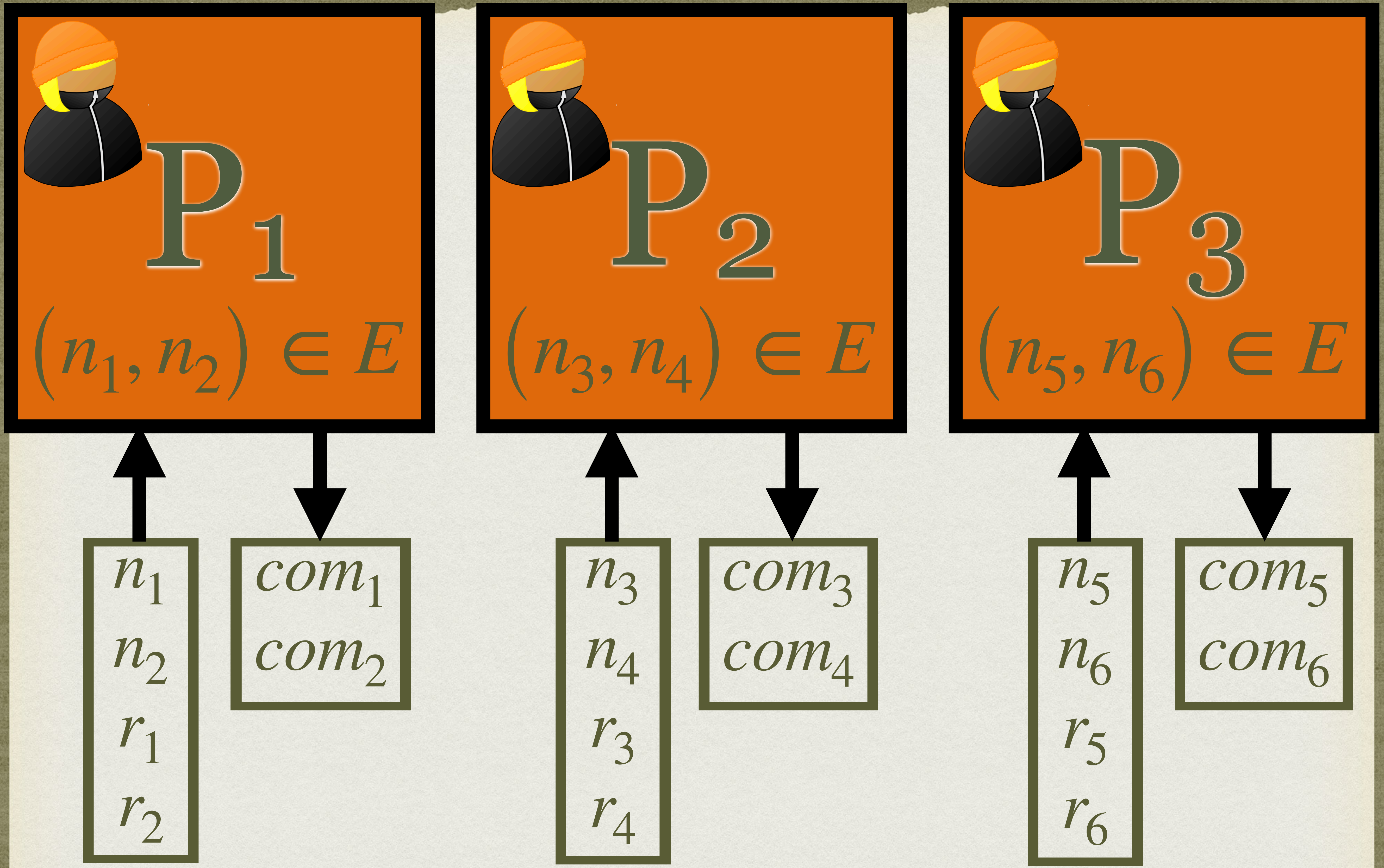
POWERFUL THEOREM



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

Entangled Games Are Hard to Approximate

- If (Single-Round) IP is sound against *local* provers
- Then augmented (S-R) IP where 3rd prover mimics one of the first 2 is sound against *entangled* provers
- Then also 2-out-of-3 version.



P_1

$(n_1, n_2) \in E$

n_1
n_2
r_1
r_2

com_1
com_2

P_2

$(n_3, n_4) \in E$

n_3
n_4
r_3
r_4

com_3
com_4

P_3

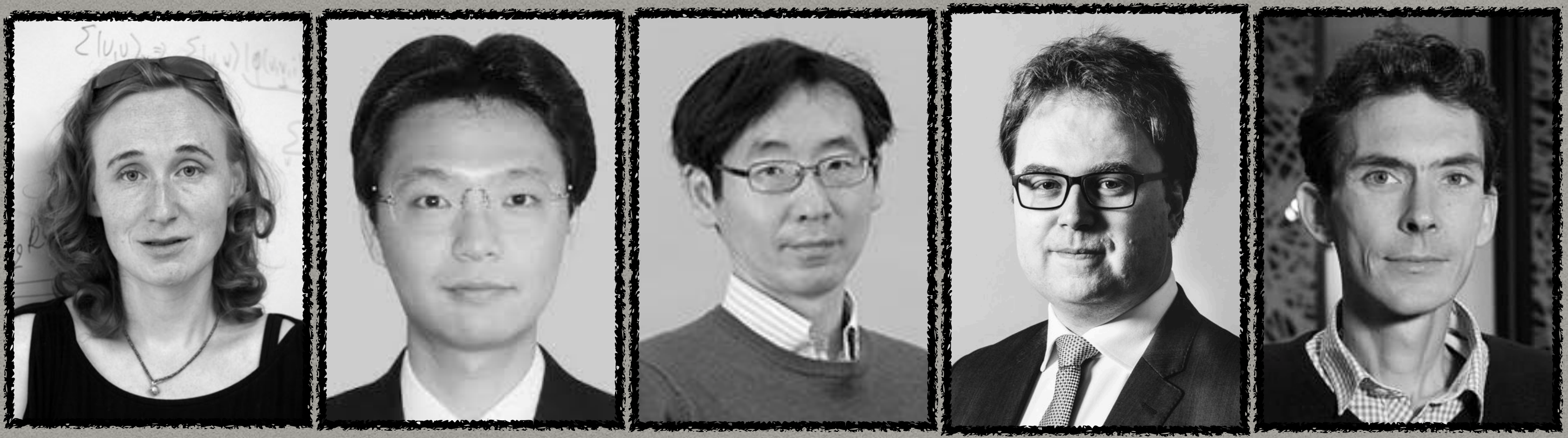
$(n_5, n_6) \in E$

n_5
n_6
r_5
r_6

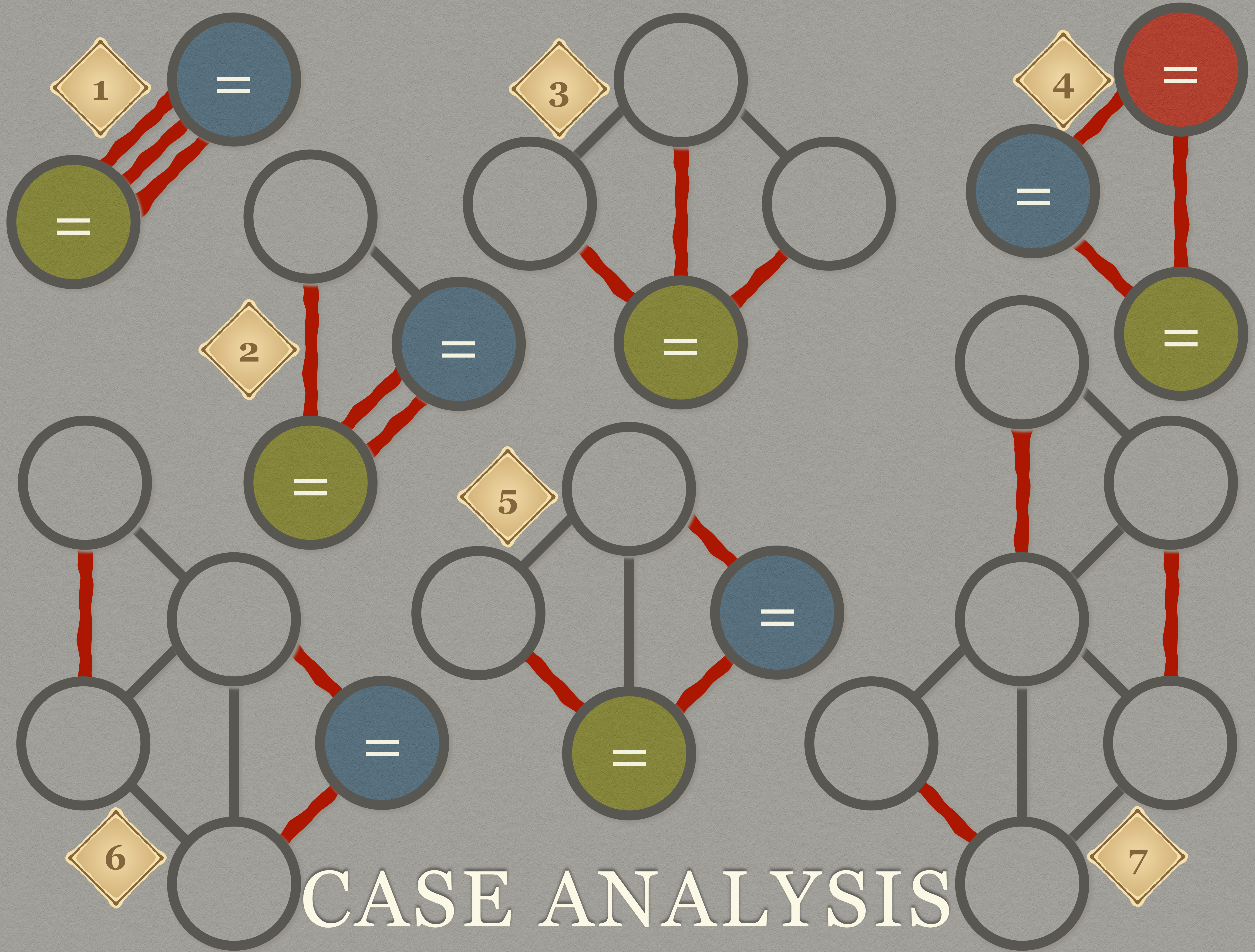
com_5
com_6

$$com_i = b_{n_i} r_i + col_{n_i}$$

(ENTANGLED) SOUNDNESS



CASE ANALYSIS



QUANTUM TECHNOLOGIES GROUP UNIVERSITÉ DE GENÈVE

OPEN QUESTION: ANALOGOUS THEOREM?

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

OPEN QUESTION: ANALOGOUS THEOREM?

- If IP is sound against *local/Entangled* provers

OPEN QUESTION: ANALOGOUS THEOREM?

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

- If IP is sound against *local/Entangled* provers
- Then augmented (S-R) IP where *N* provers mimic existing ones sound against *No-Signalling* provers ?

OPEN QUESTION: ANALOGOUS THEOREM?

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

- If IP is sound against *local/Entangled* provers
- Then augmented (S-R) IP where *N* provers mimic existing ones sound against *No-Signalling* provers ?
- Zero-Knowledge ?

Demonstrating that a Public *Graph* can be *3-Coloured* Without Revealing Any *Knowledge* About How

Claude Crépeau

McGill