Relativistic & Non-Local Zero-Knowledge Proofs

Workshop on Quantum Information, Computation, and Foundation

Sept. 14-18, 2020

Claude Crépeau

McGill

Aly Ibrahim

Nan Yang

Workshop on Quantum Information, Computation, and Foundation

Sept. 14-18, 2020

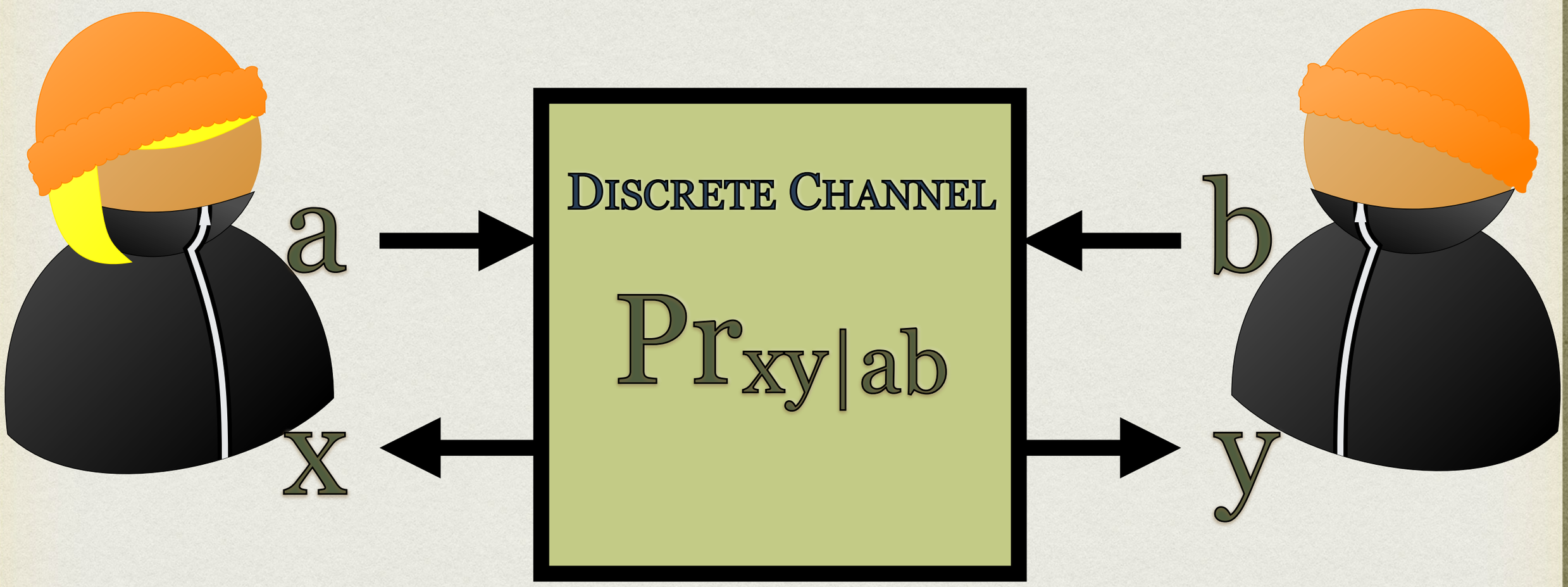
Claude Crépeau

McGill

INTRODUCTION

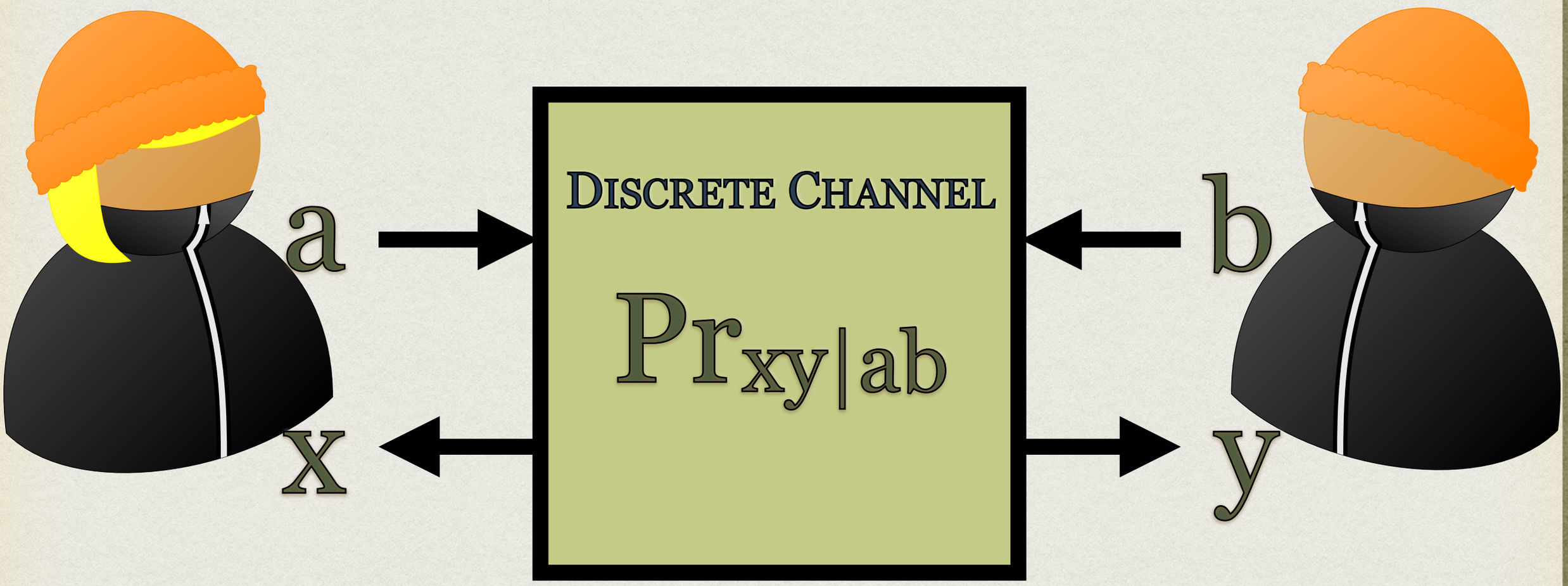
DISCRETE CHANNELS

DISCRETE CHANNELS



DISCRETE CHANNELS

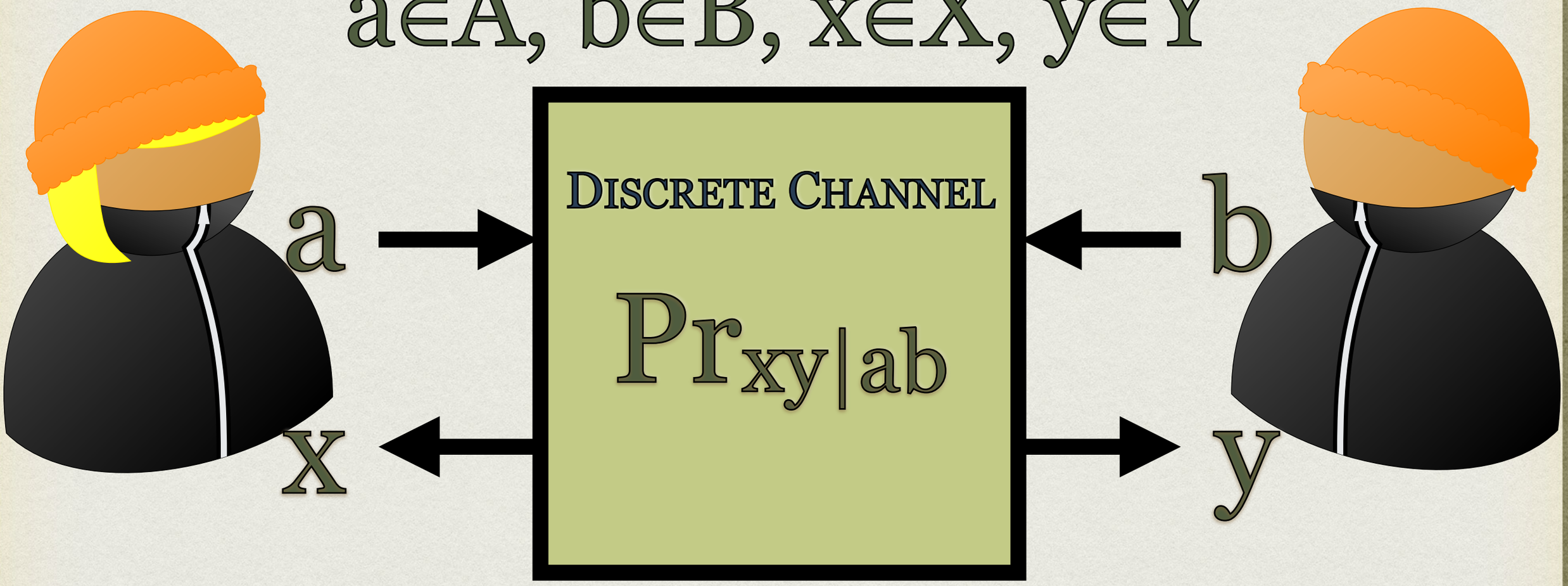
A,B,X,Y: finite sets



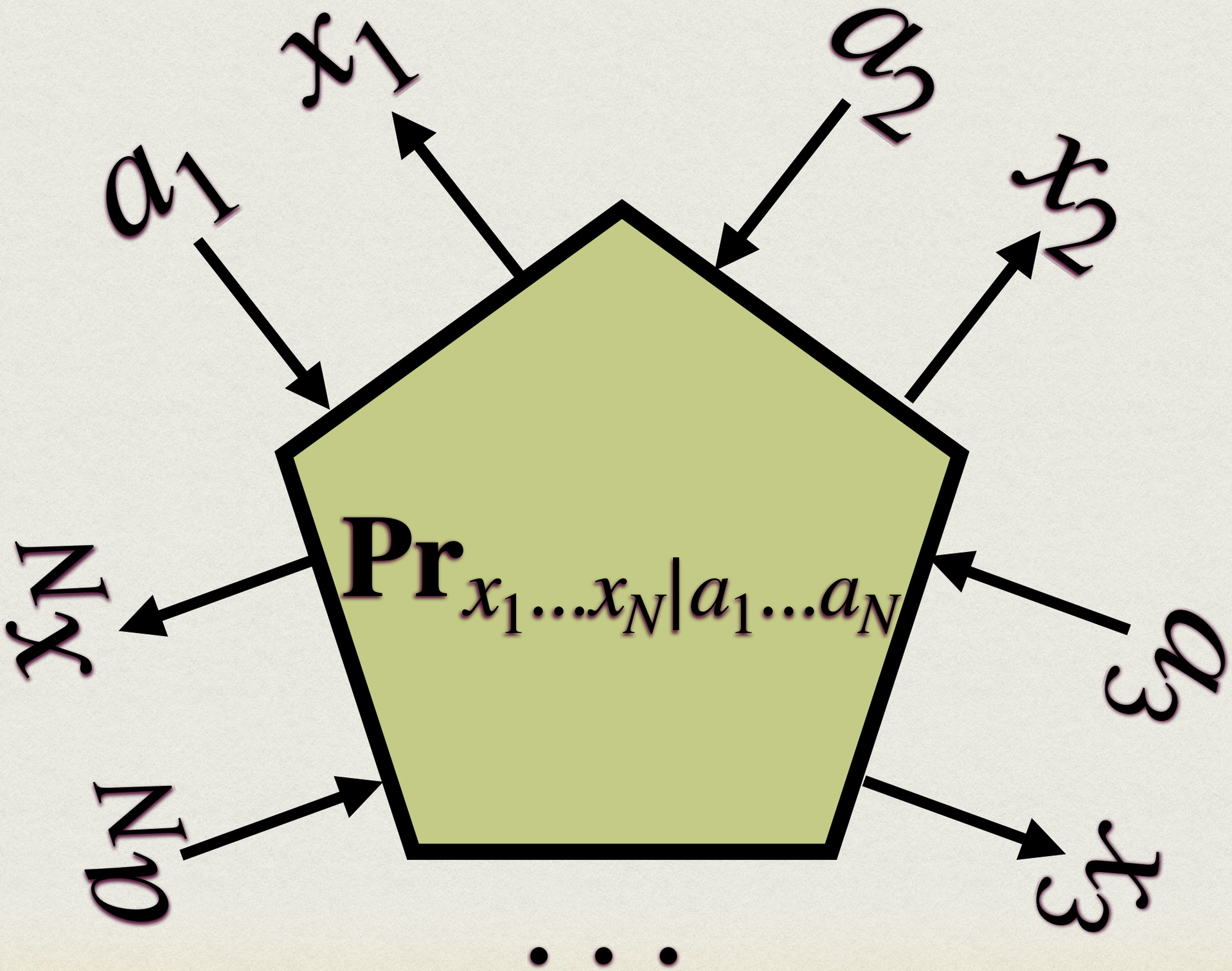
DISCRETE CHANNELS

A, B, X, Y: finite sets

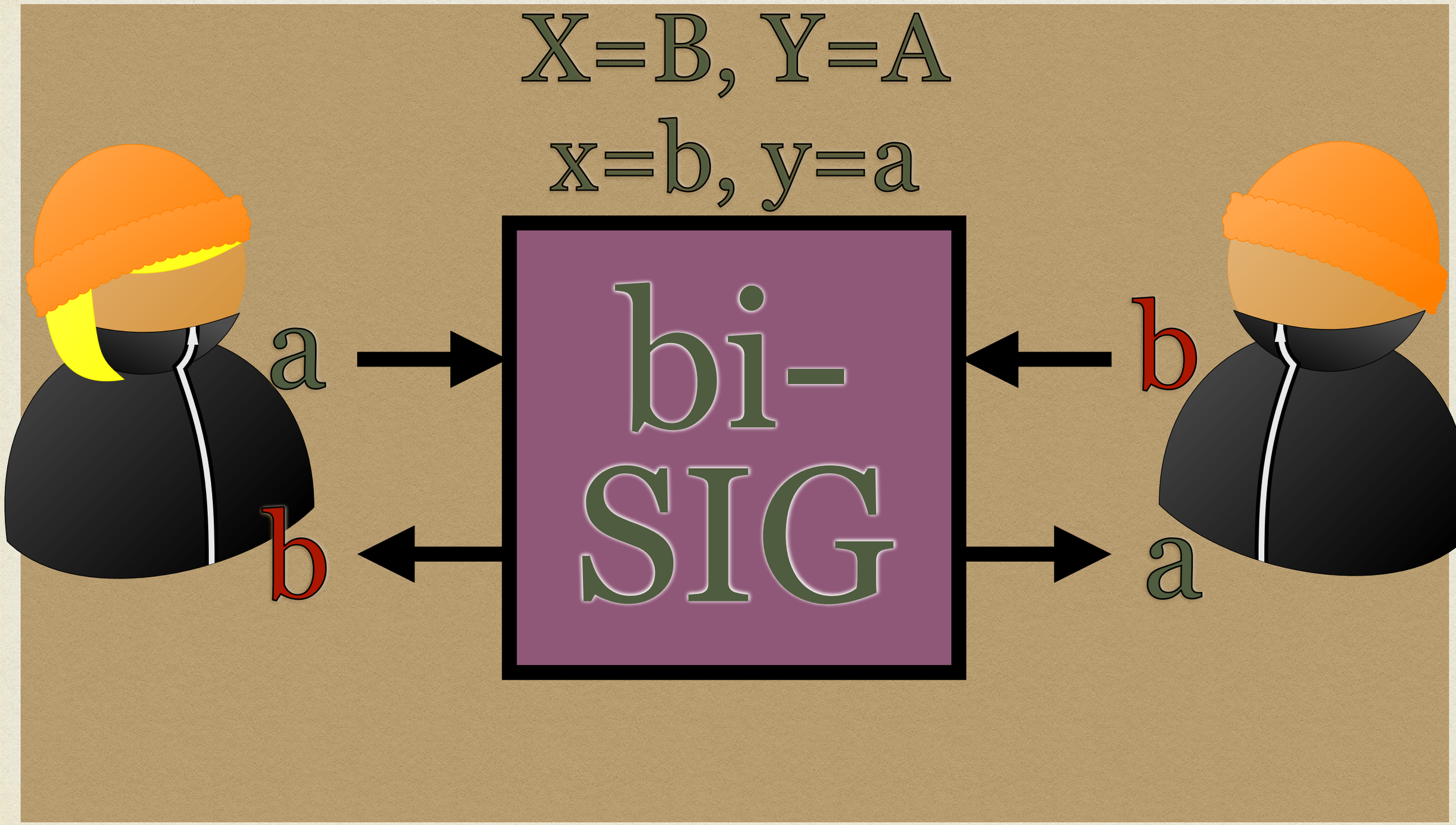
$a \in A$, $b \in B$, $x \in X$, $y \in Y$



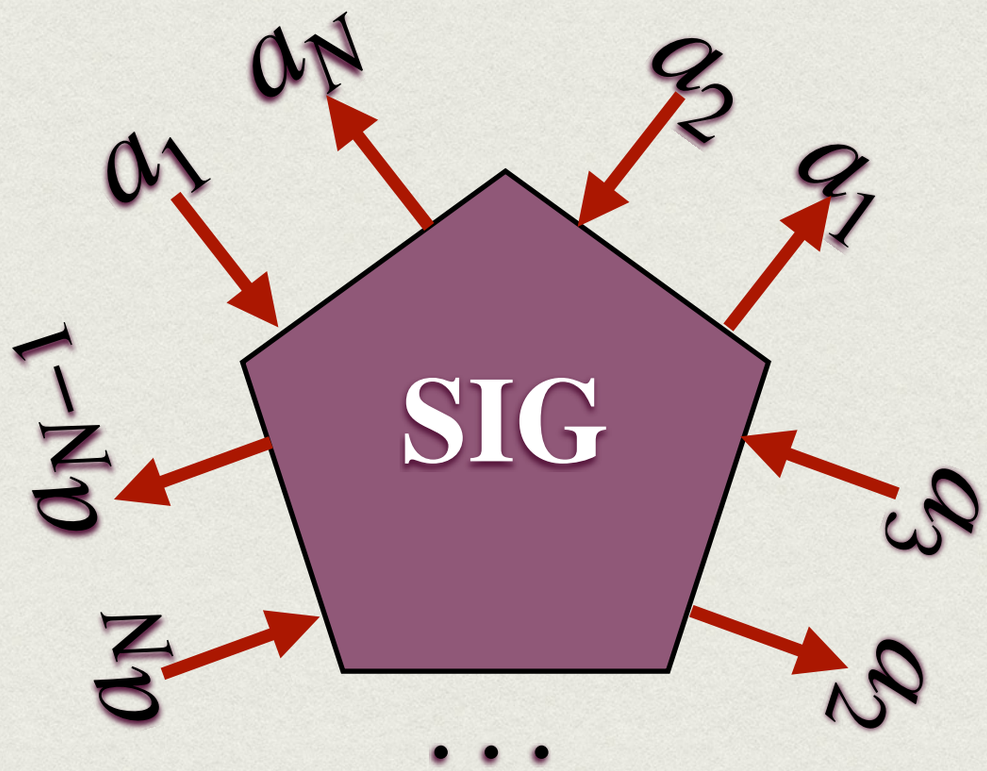
GENERAL CHANNELS

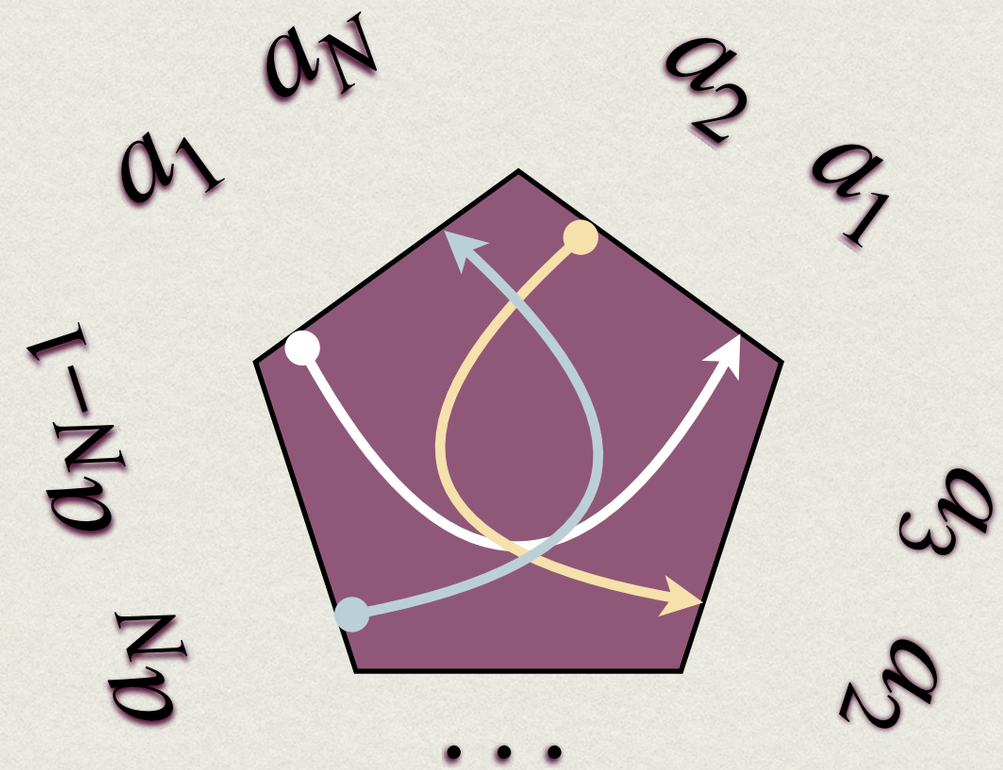


DISCRETE CHANNELS

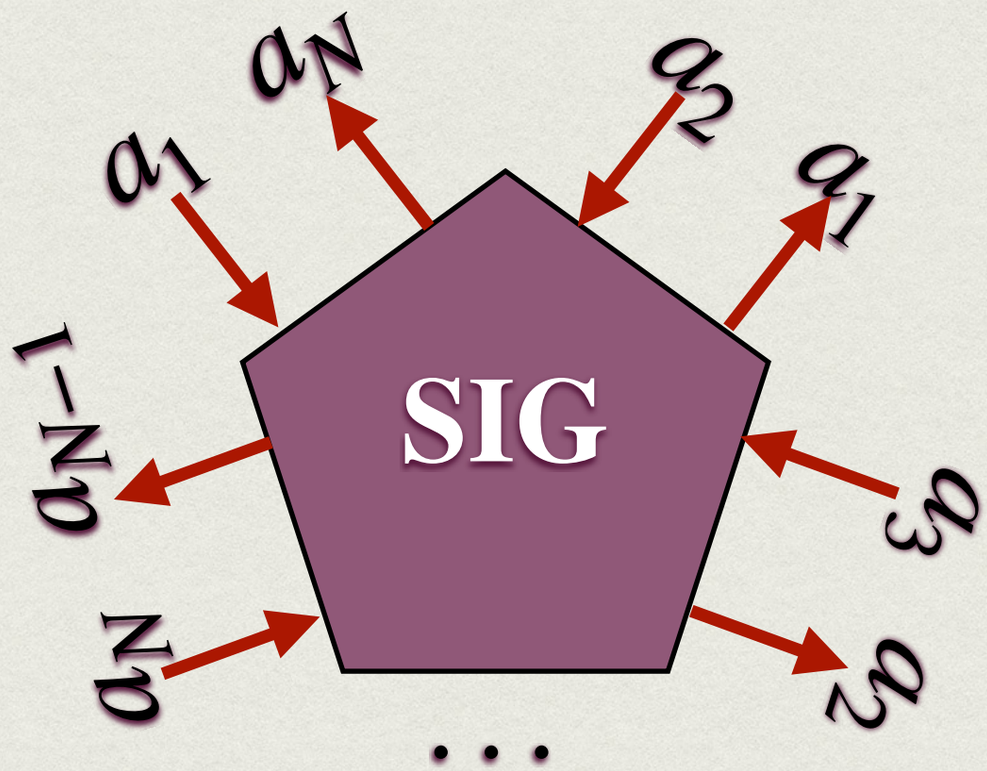


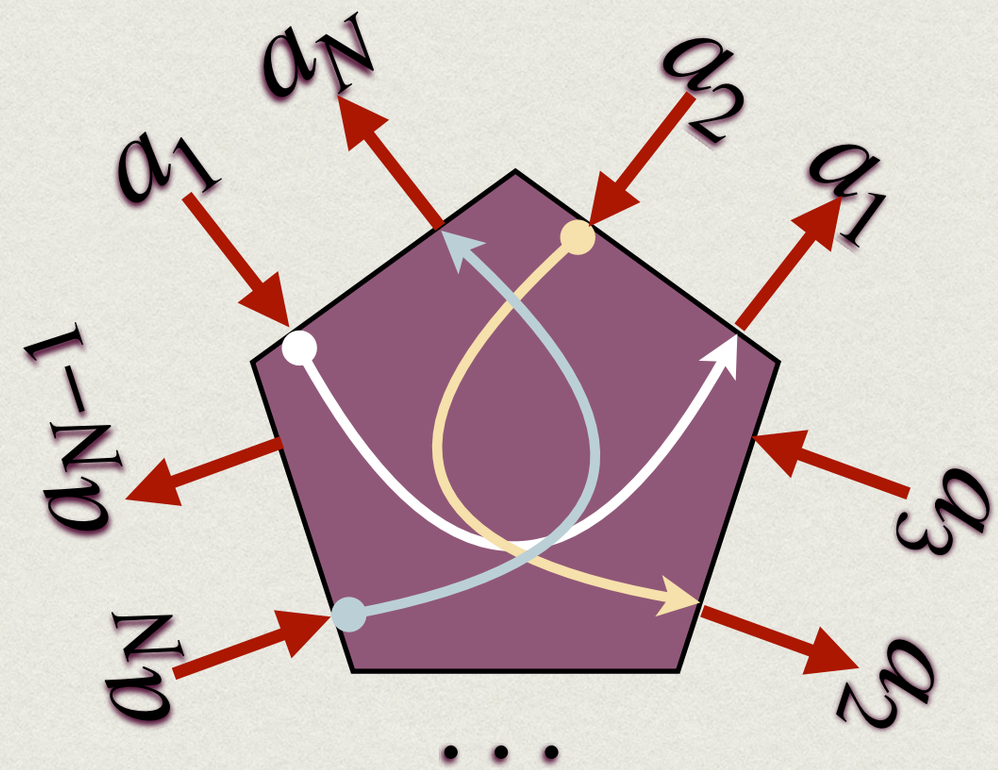
GENERAL **SIG** CHANNELS



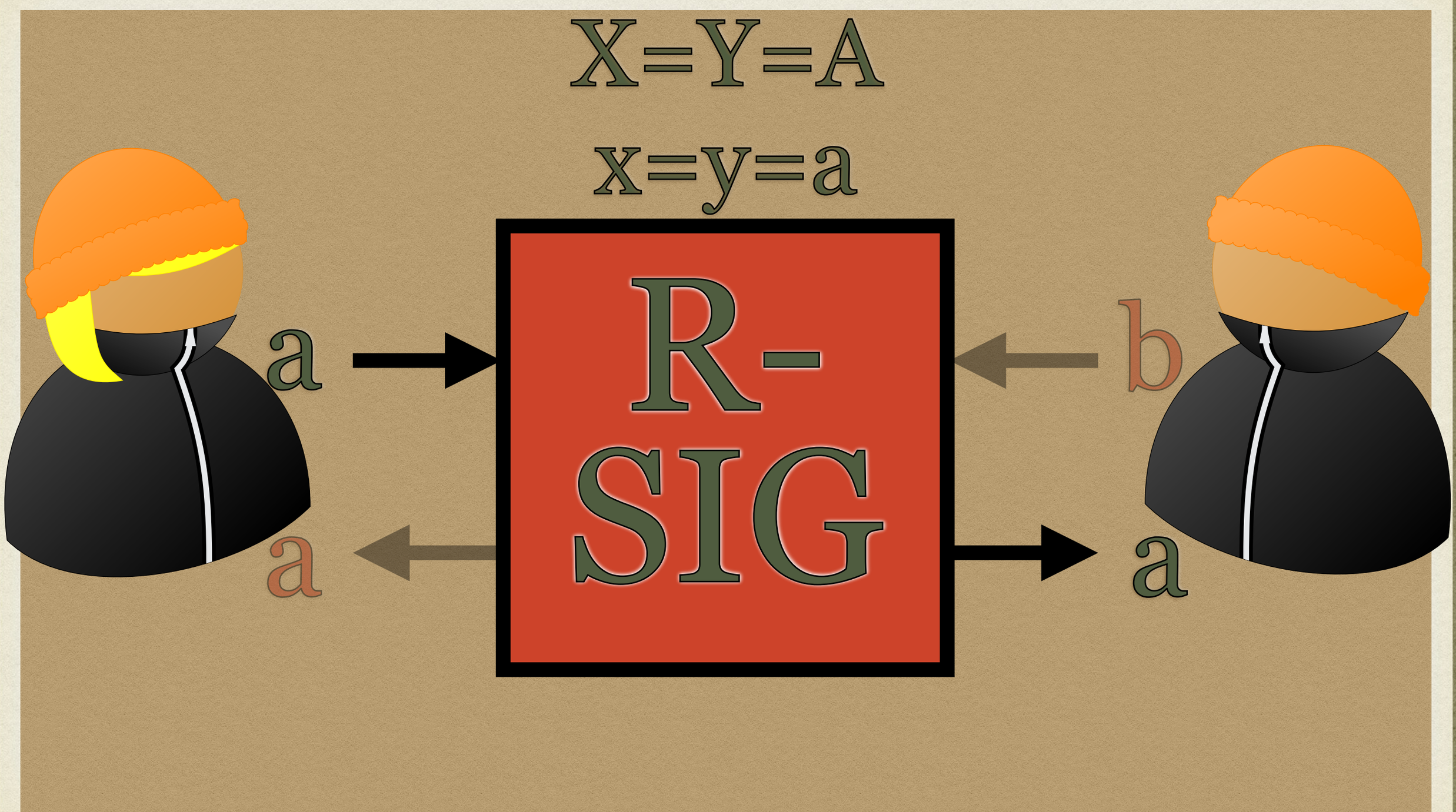


GENERAL **SIG** CHANNELS

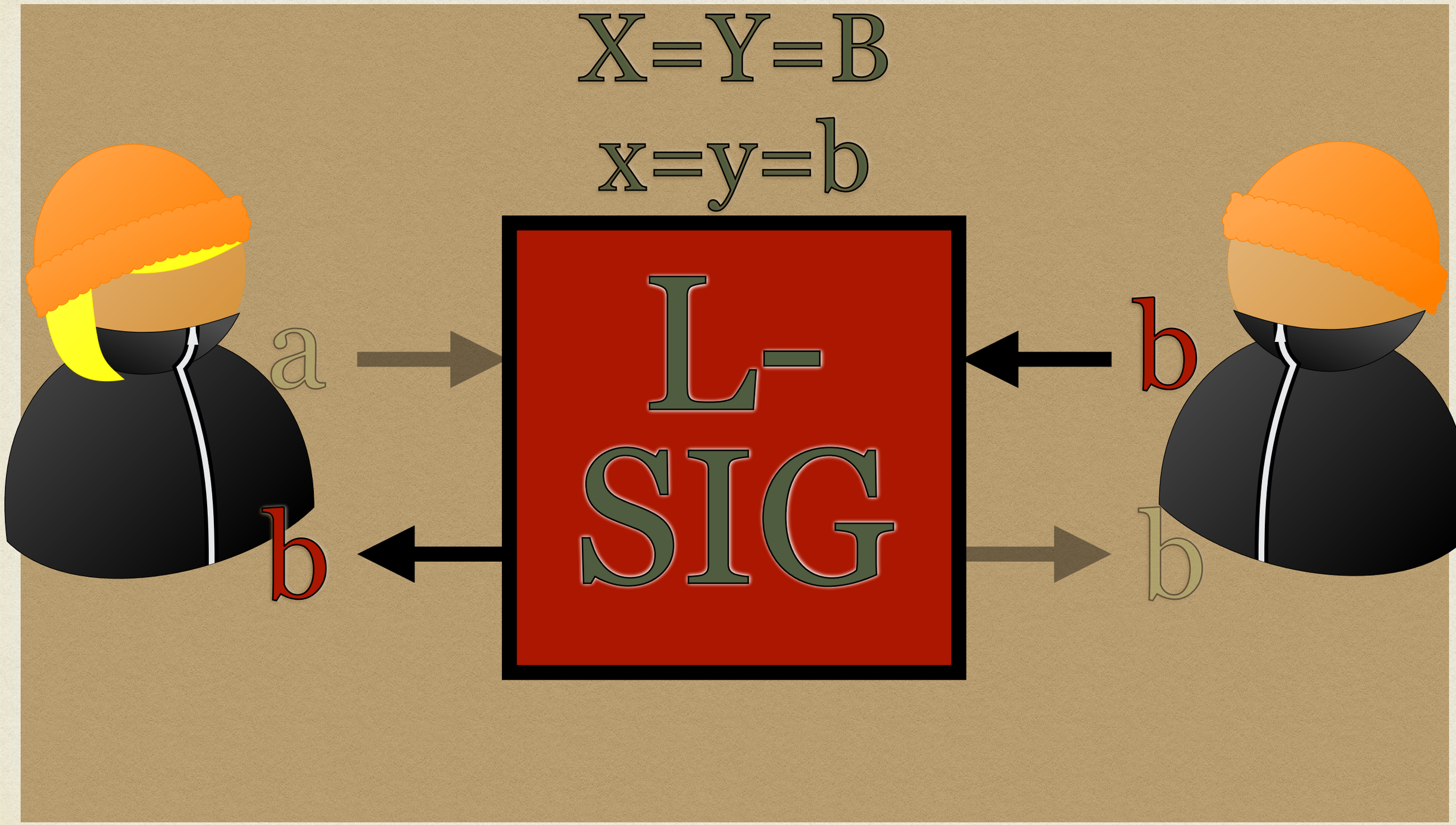




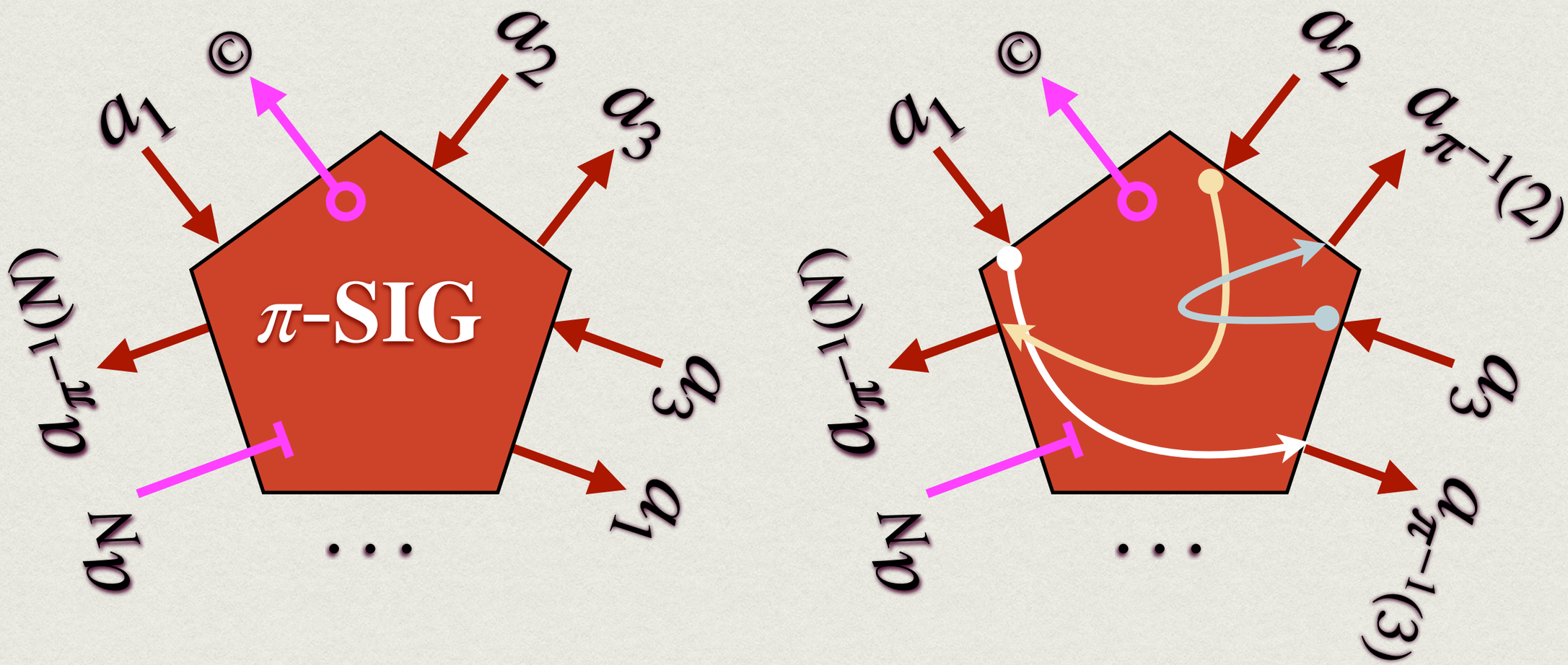
DISCRETE CHANNELS



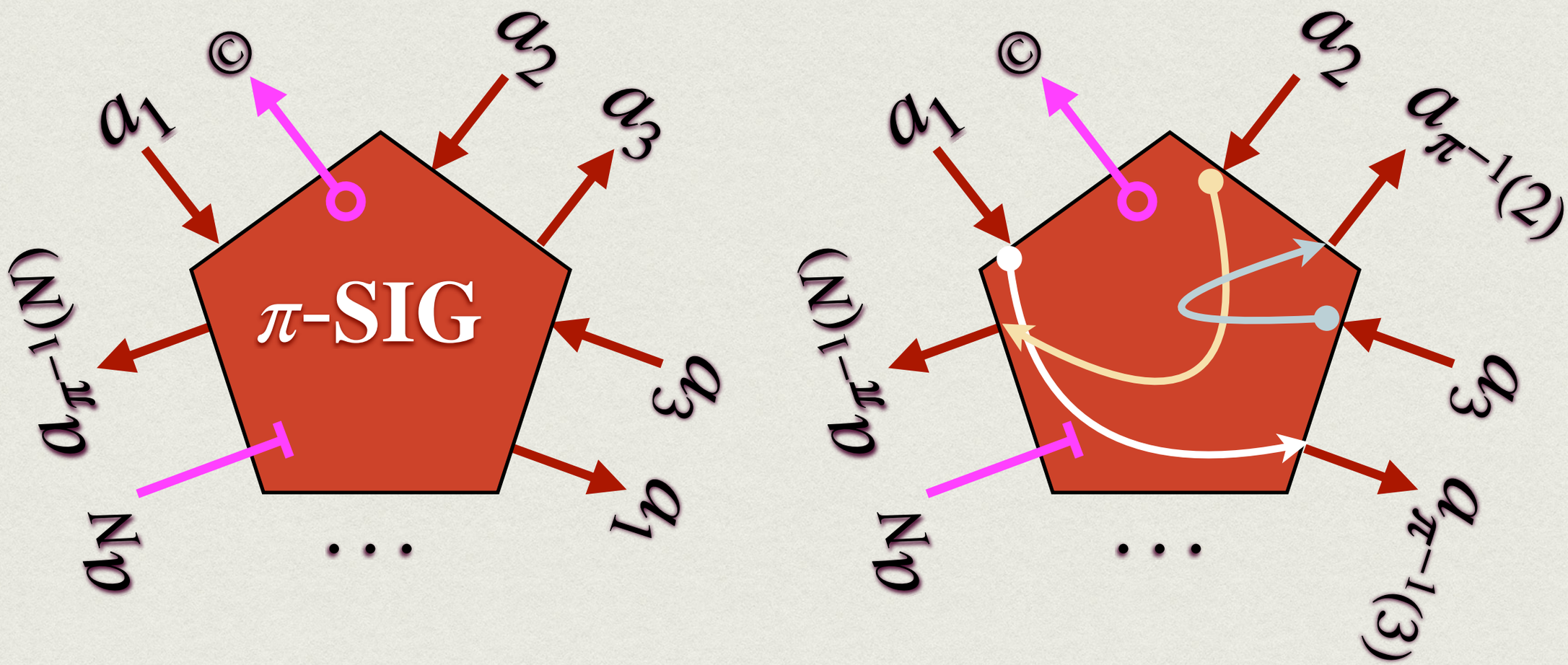
DISCRETE CHANNELS



GENERAL π-SIG CHANNELS



GENERAL π-SIG CHANNELS



$$i \blacktriangleright \pi(i) \blacktriangleright \pi^2(i) \blacktriangleright \ldots \blacktriangleright \pi^{N\text{-}1}(i)$$

DISCRETE CHANNELS

$A=B=X=Y=\mathbb{F}$

a

x

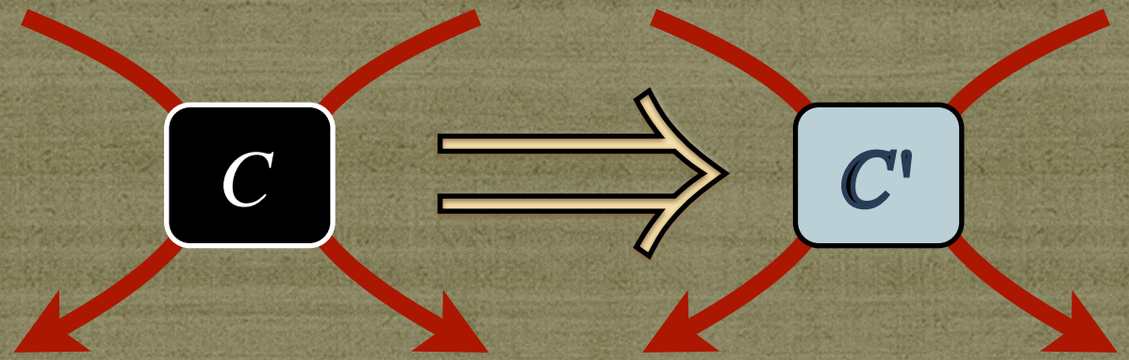
random x

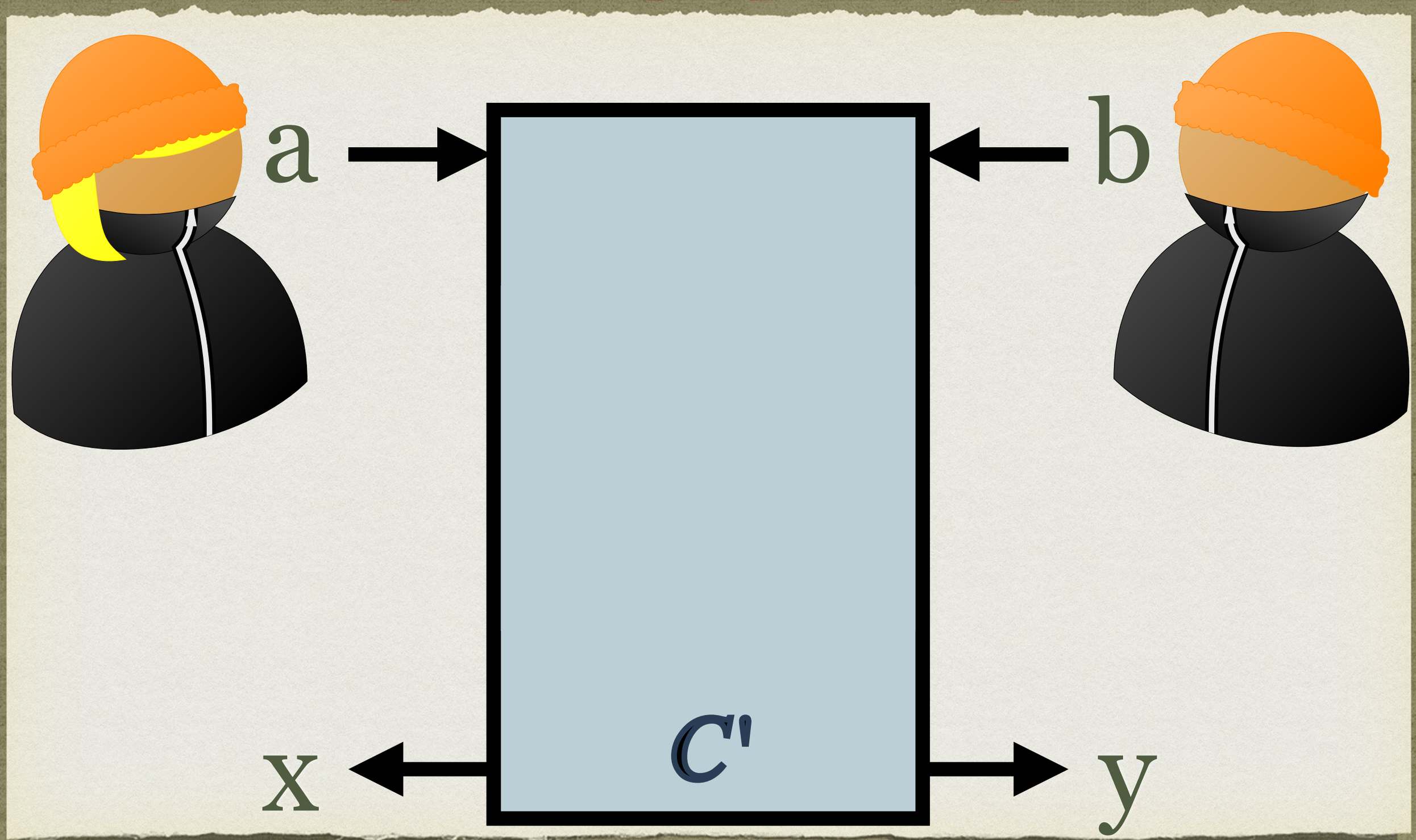
PR

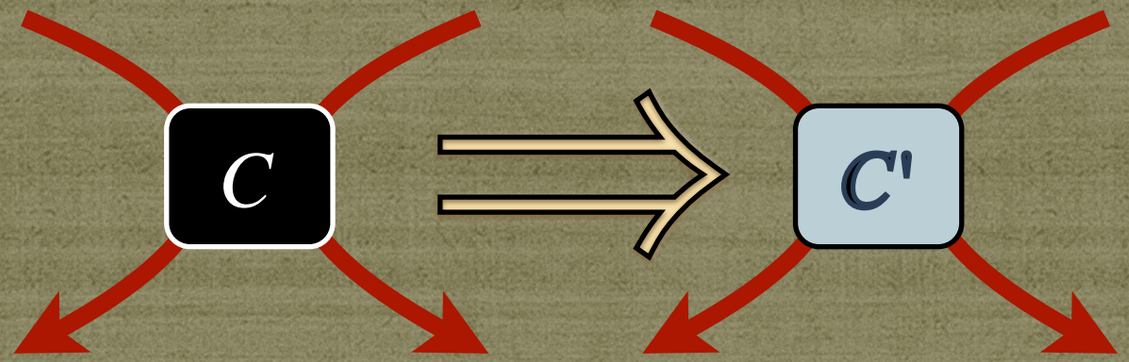
b

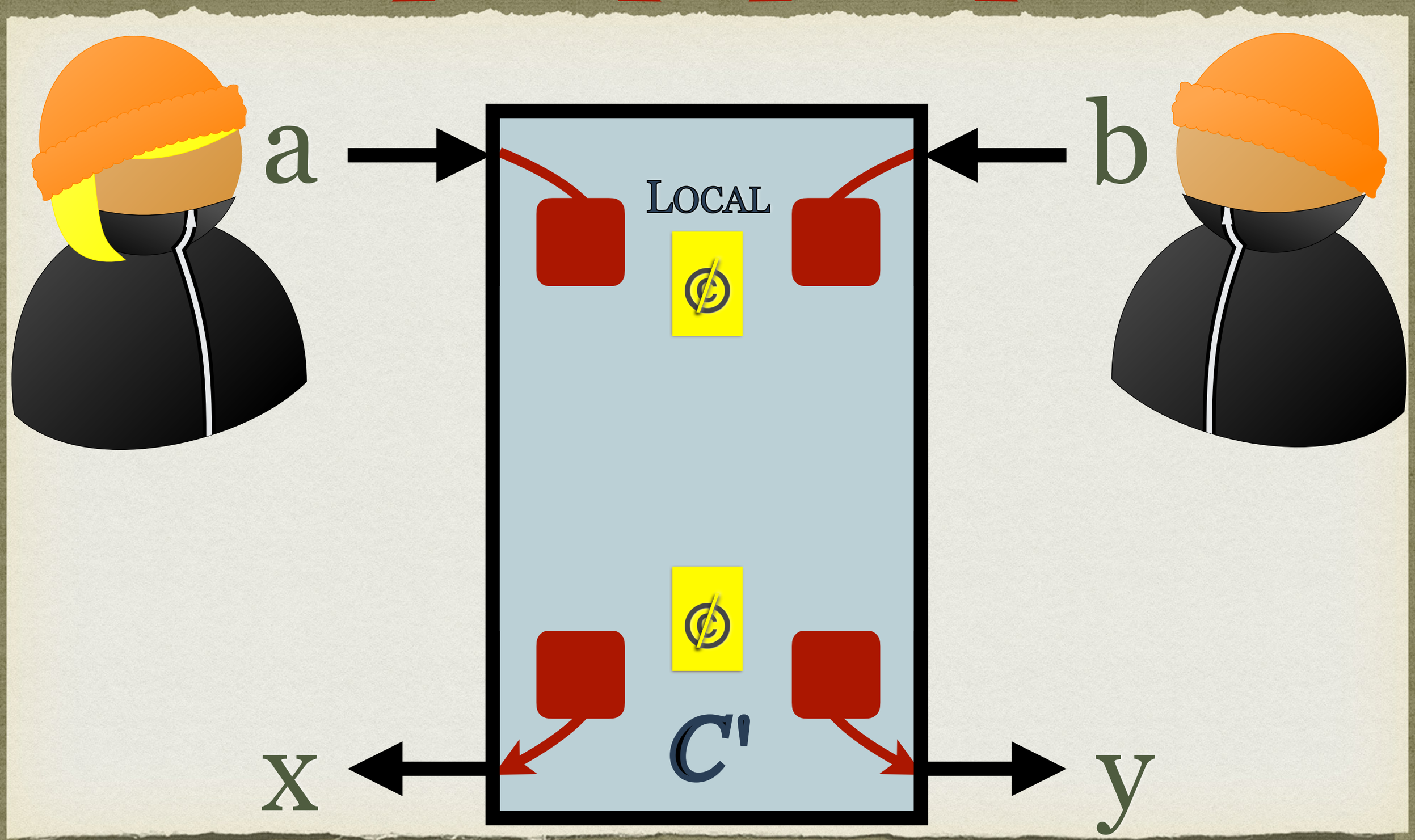
y

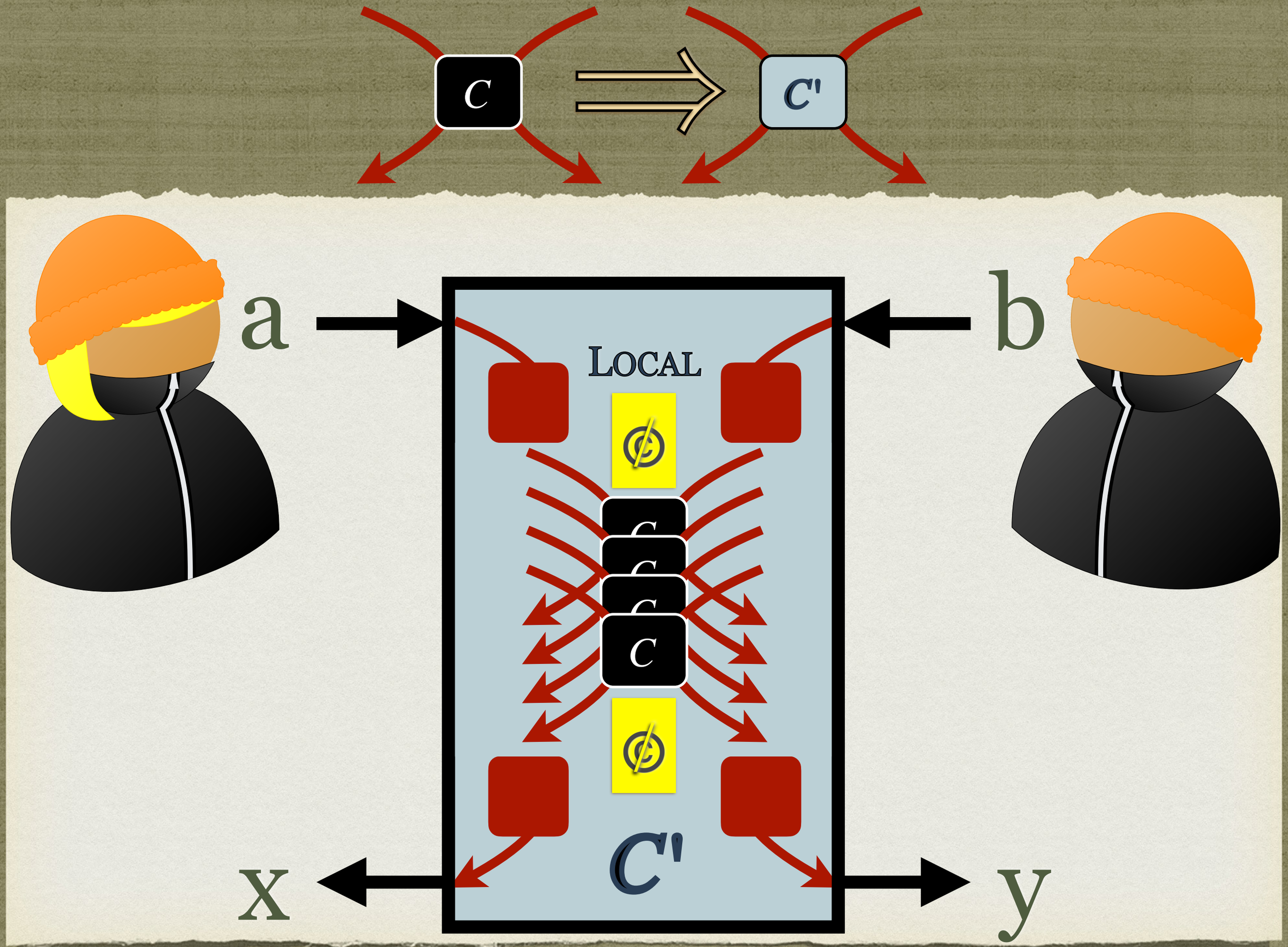
$y = a \cdot b + x$


c
c'

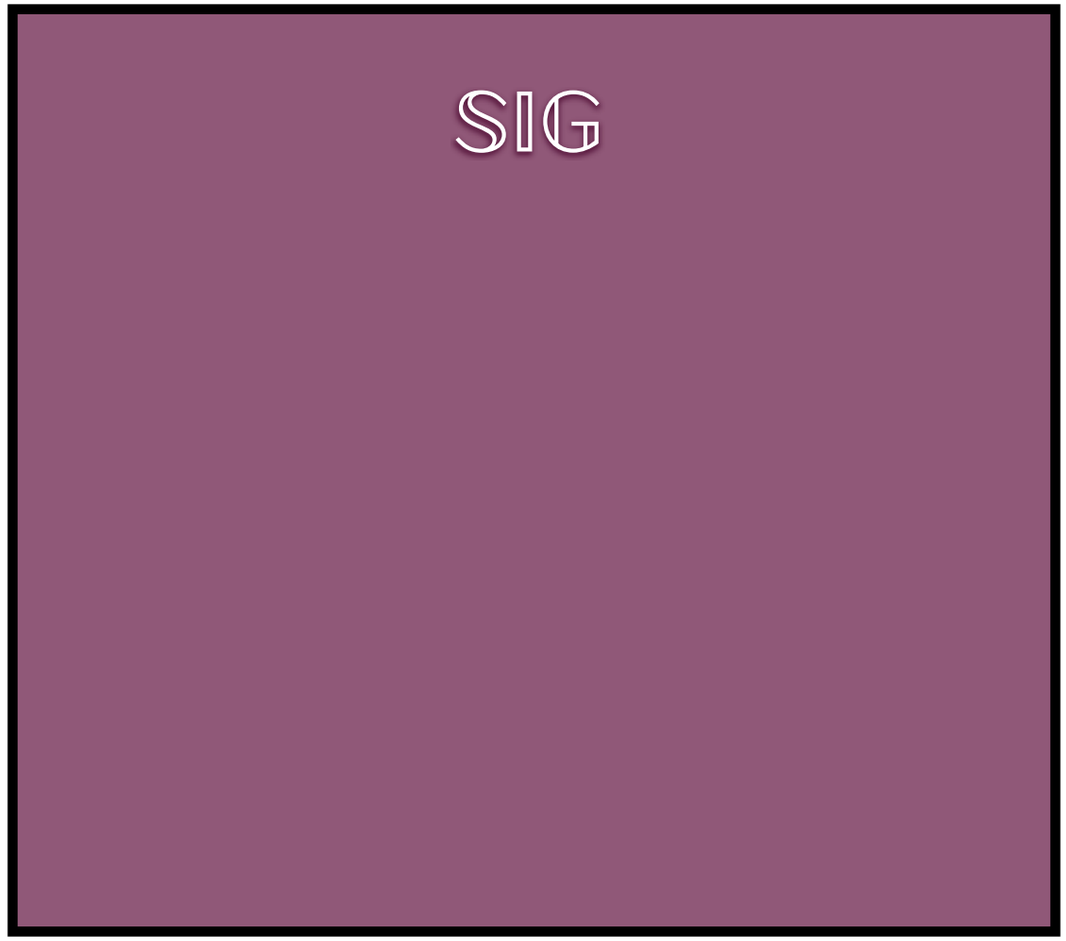

a
b
c'
x
y


c
c'


a
b
Local
c'
x
y

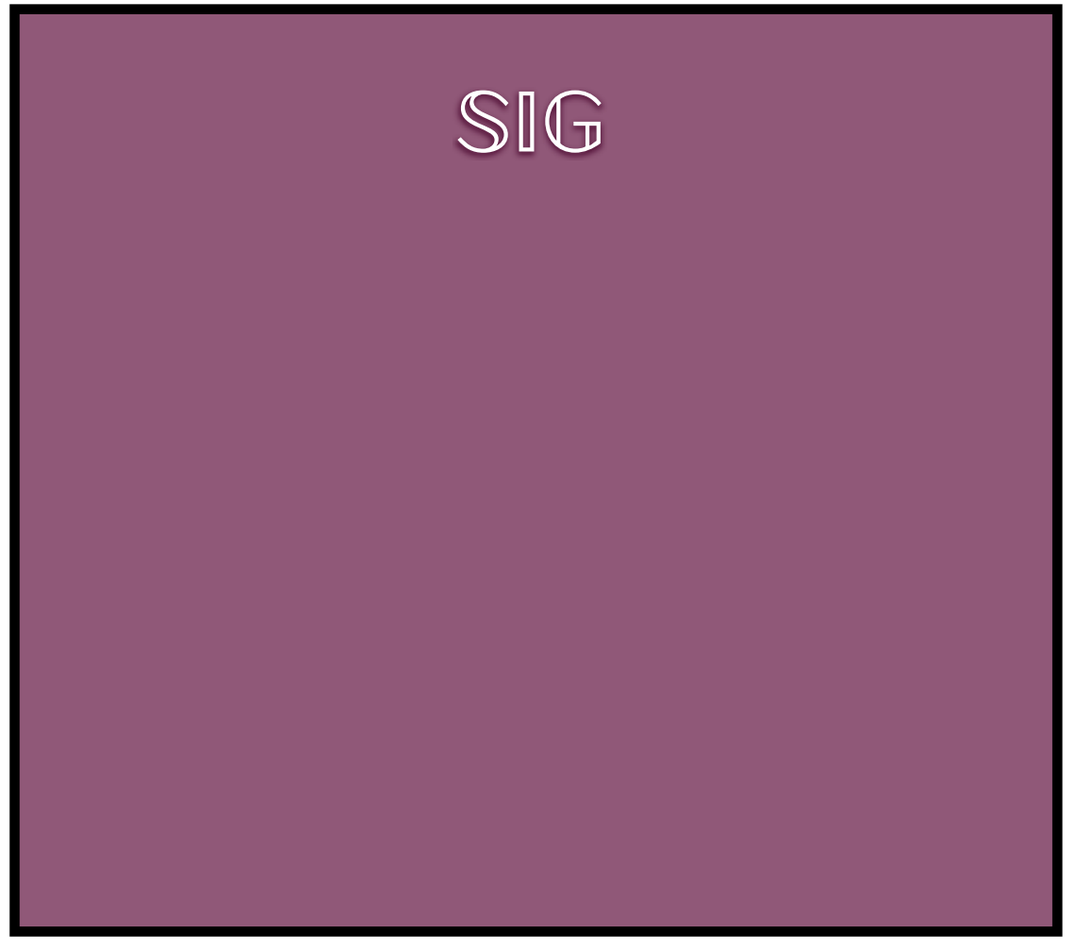

c
c'
a
b
Local
c
c
c
c
c'
x
y

2-PARTY NON-LOCALITY HIERARCHY



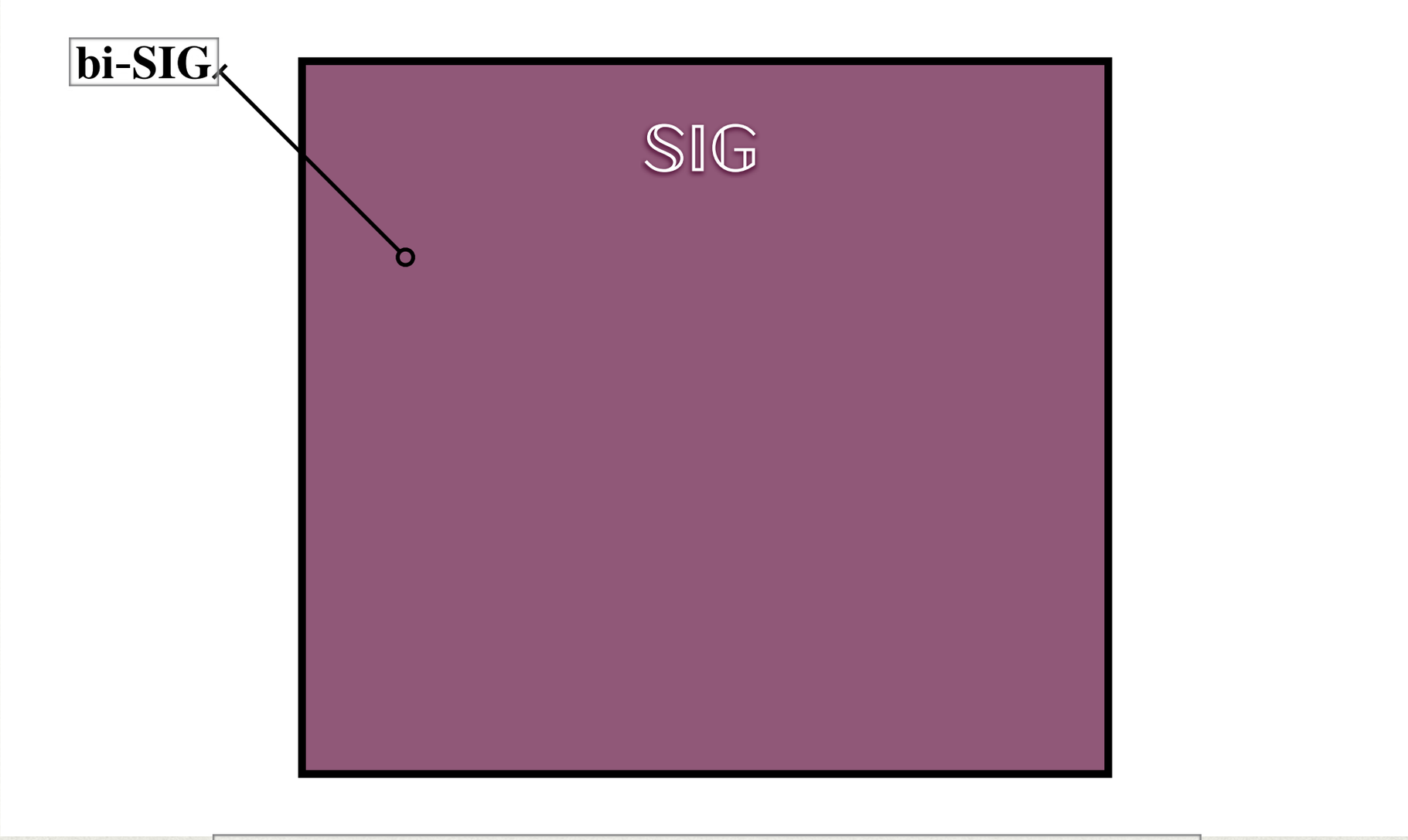
2-PARTY NON-LOCALITY HIERARCHY

$\mathbb{SIG}$ = all two-party correlations



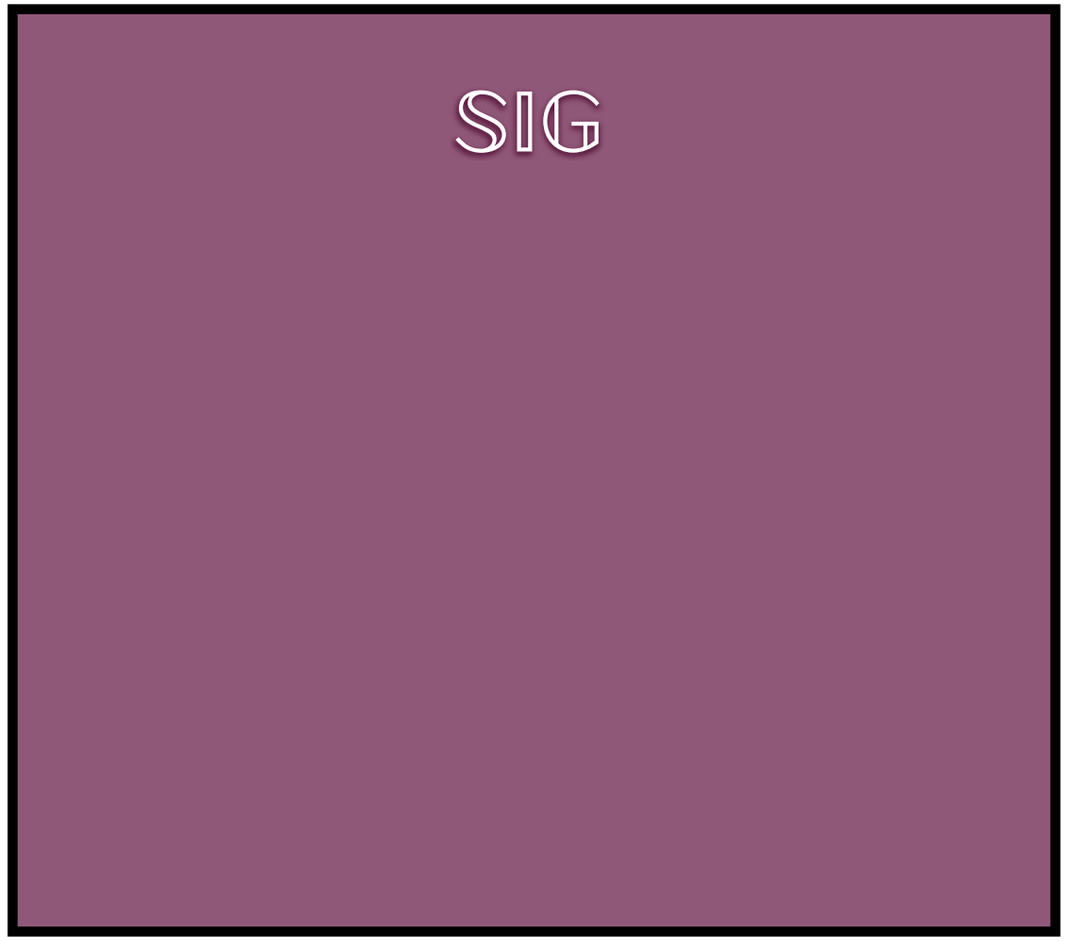
2-PARTY NON-LOCALITY HIERARCHY

$\mathbb{SIG}$ = all two-party correlations

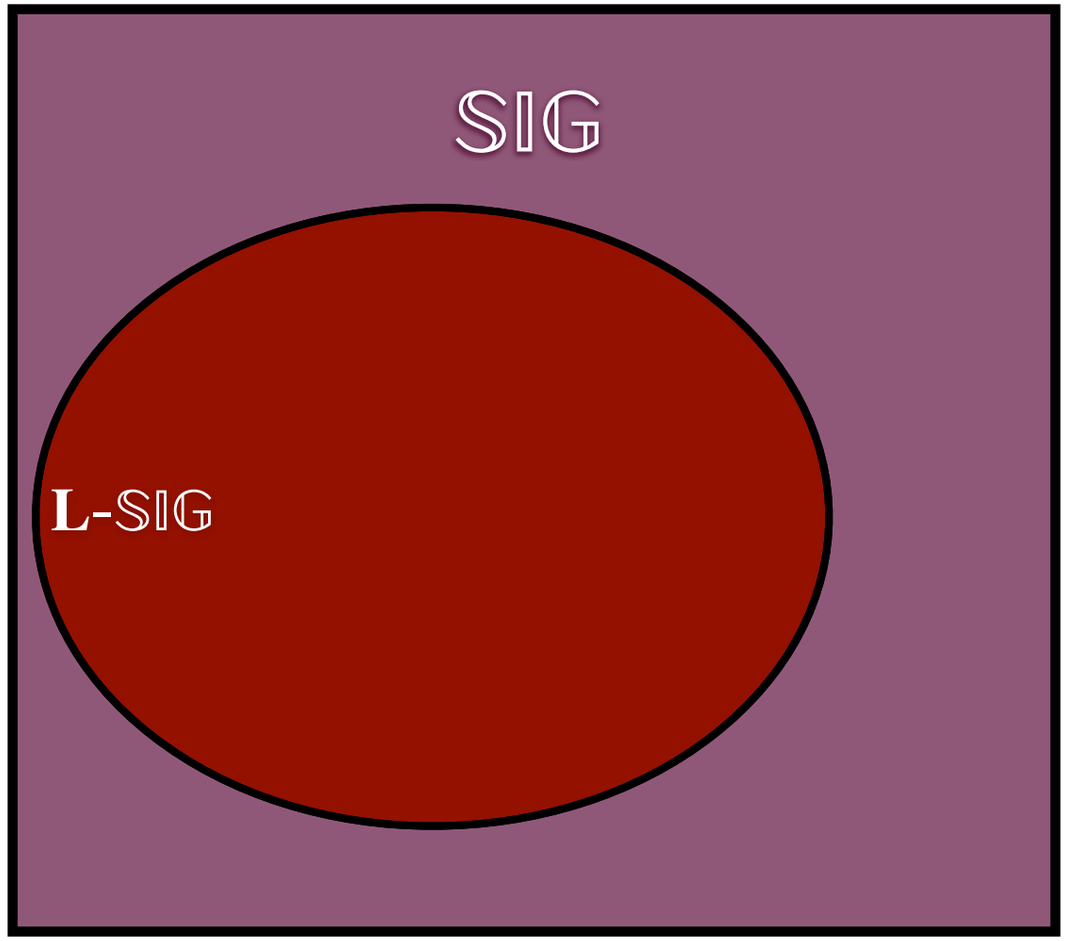


$\forall c \in \mathbb{SIG}$, **bi-SIG** $\implies c$

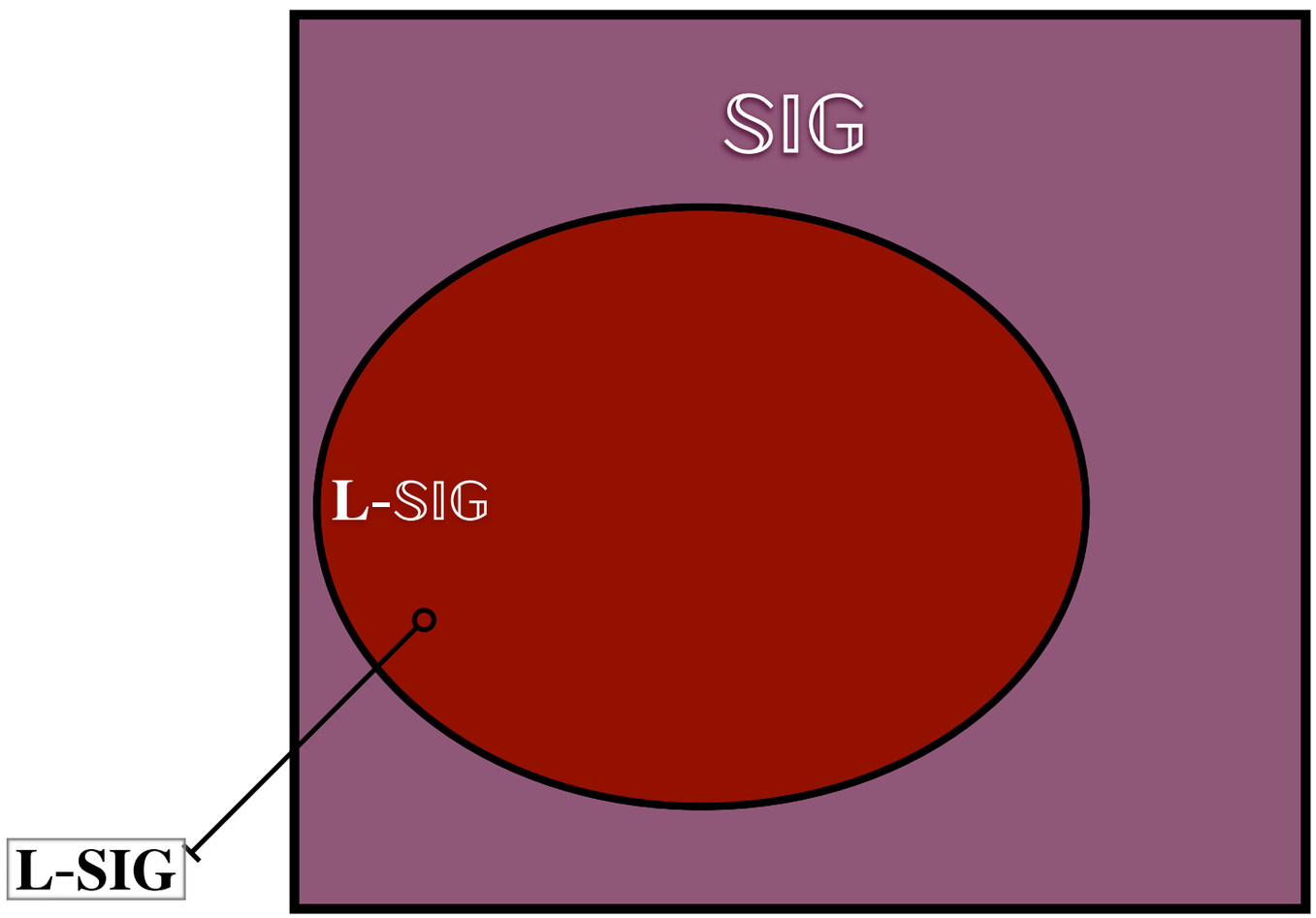
2-PARTY NON-LOCALITY HIERARCHY



2-PARTY NON-LOCALITY HIERARCHY

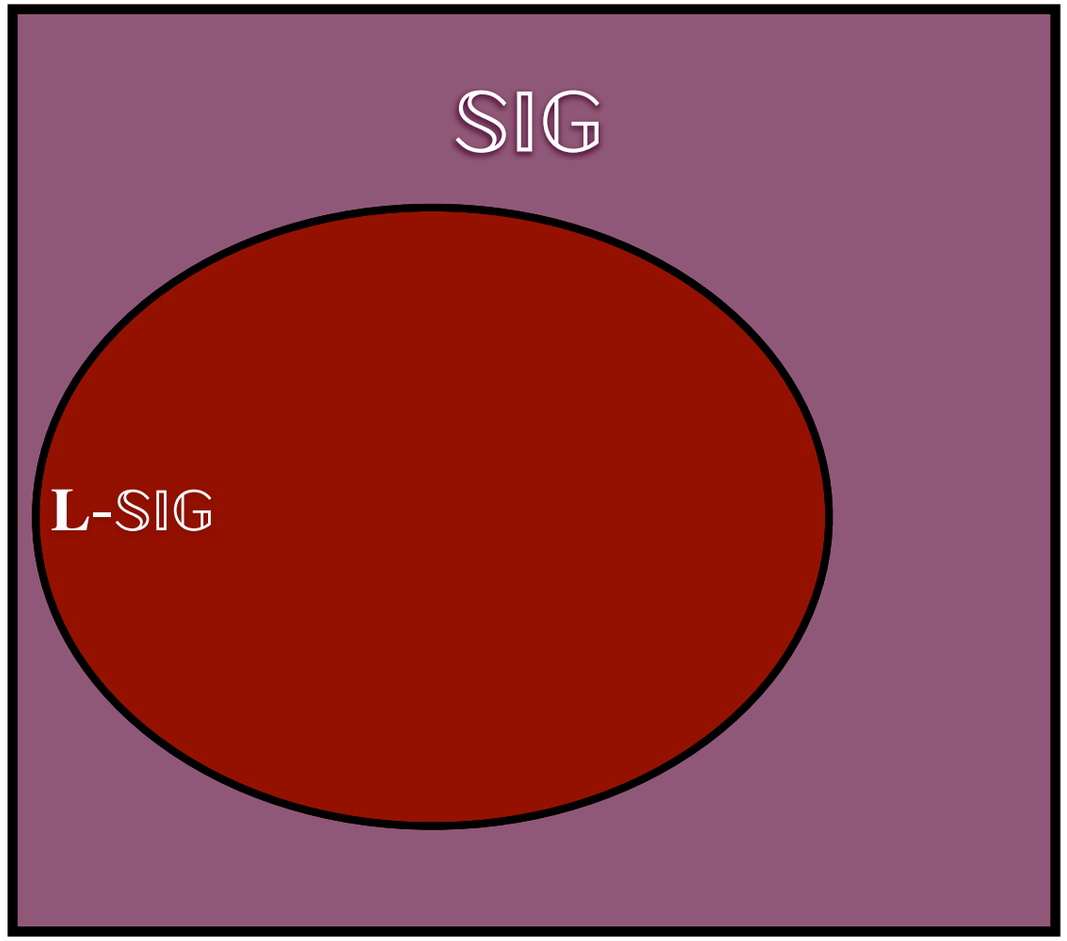


2-PARTY NON-LOCALITY HIERARCHY

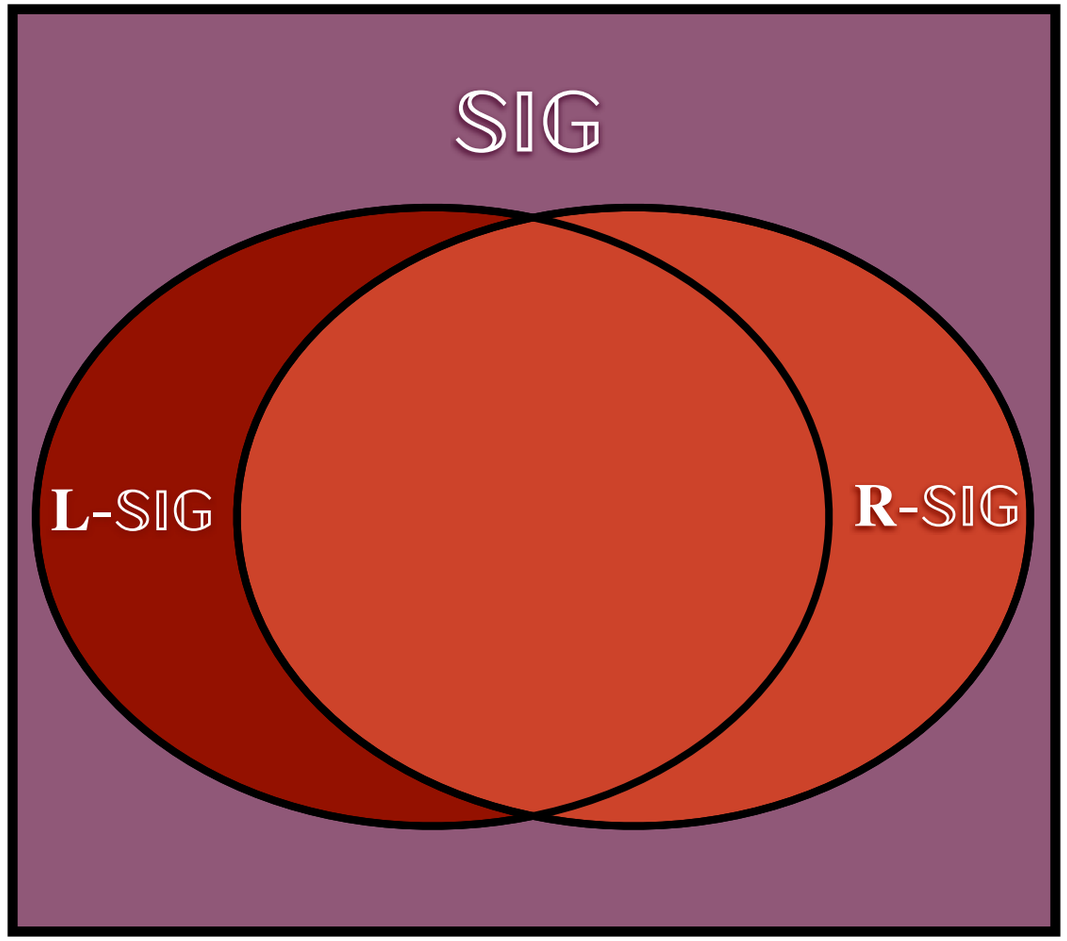


$$\forall c \in \textbf{L-}\mathbb{SIG}, \textbf{L-SIG} \implies c$$

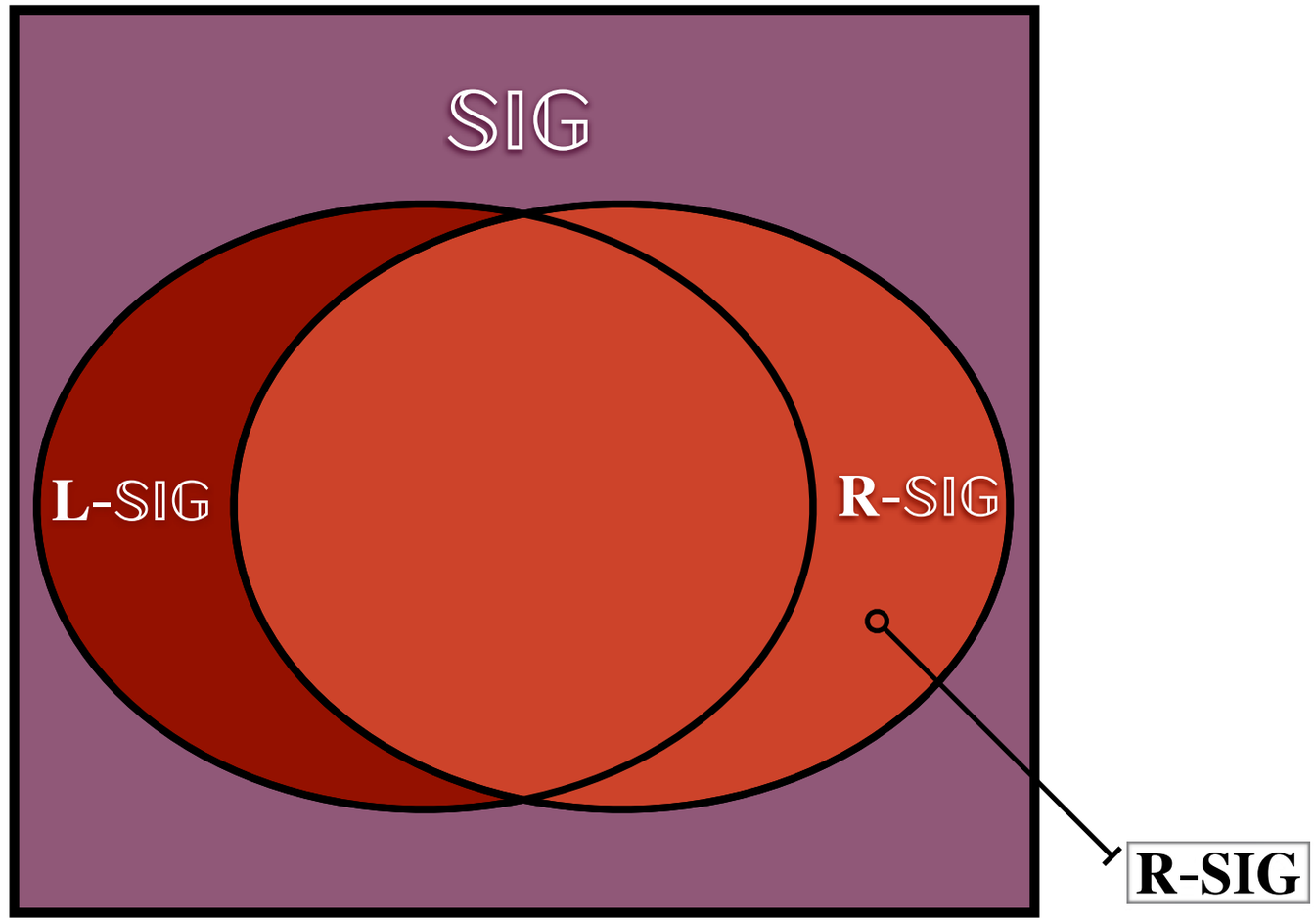
2-PARTY NON-LOCALITY HIERARCHY



2-PARTY NON-LOCALITY HIERARCHY

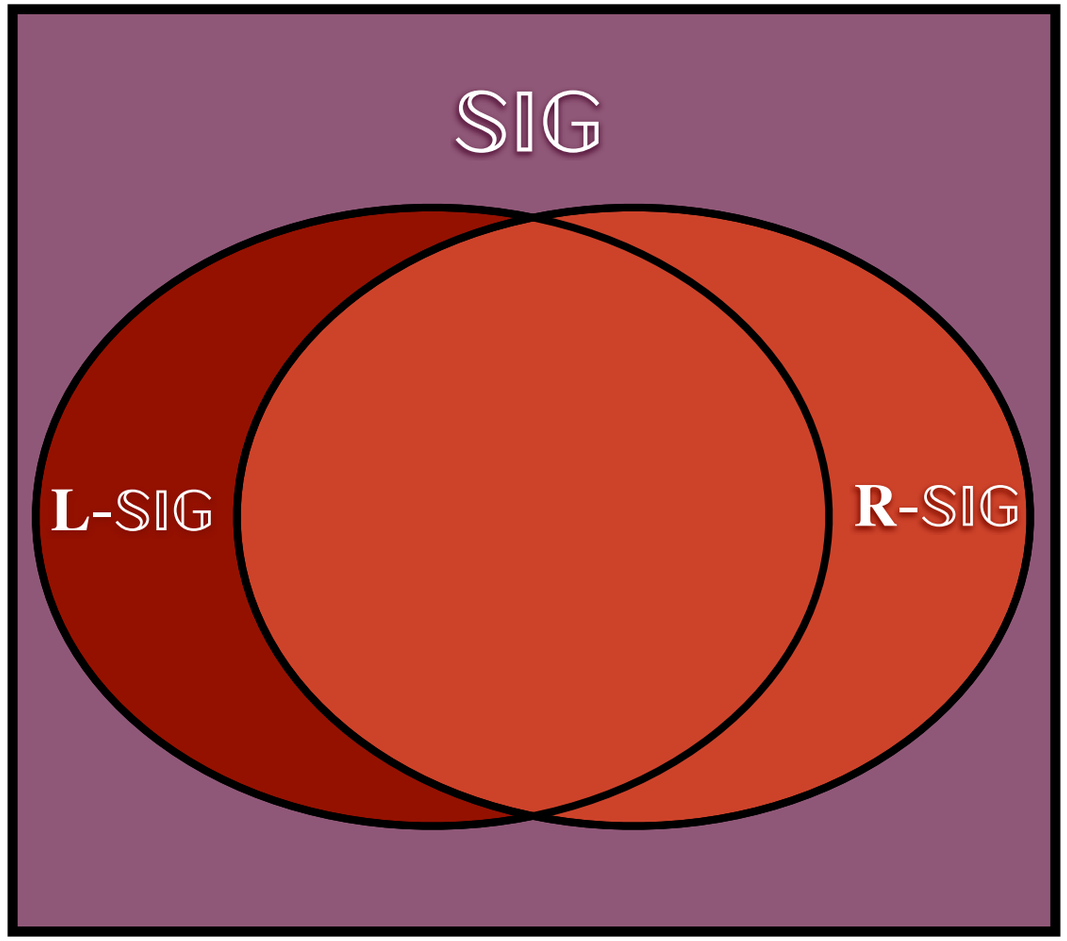


2-PARTY NON-LOCALITY HIERARCHY

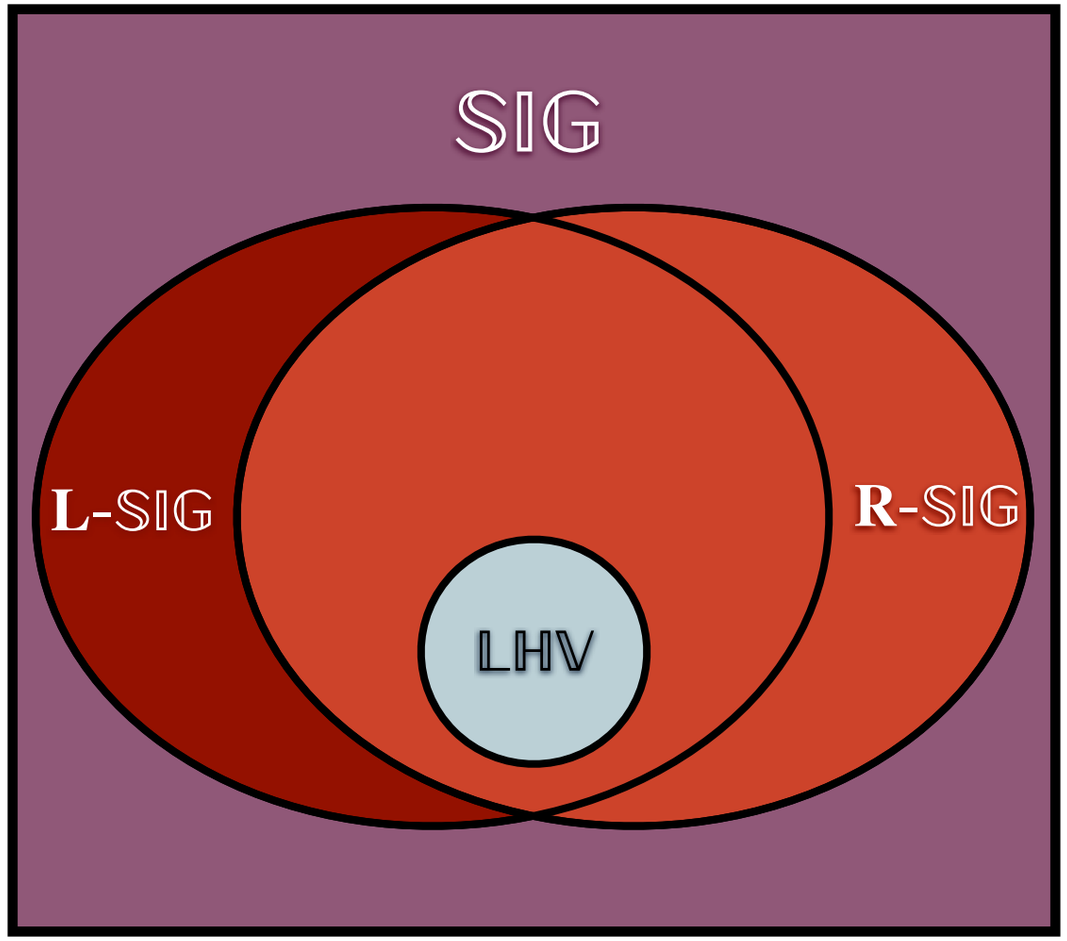


$$\forall c \in \textbf{R-}\mathbb{SIG}, \textbf{R-SIG} \implies c$$

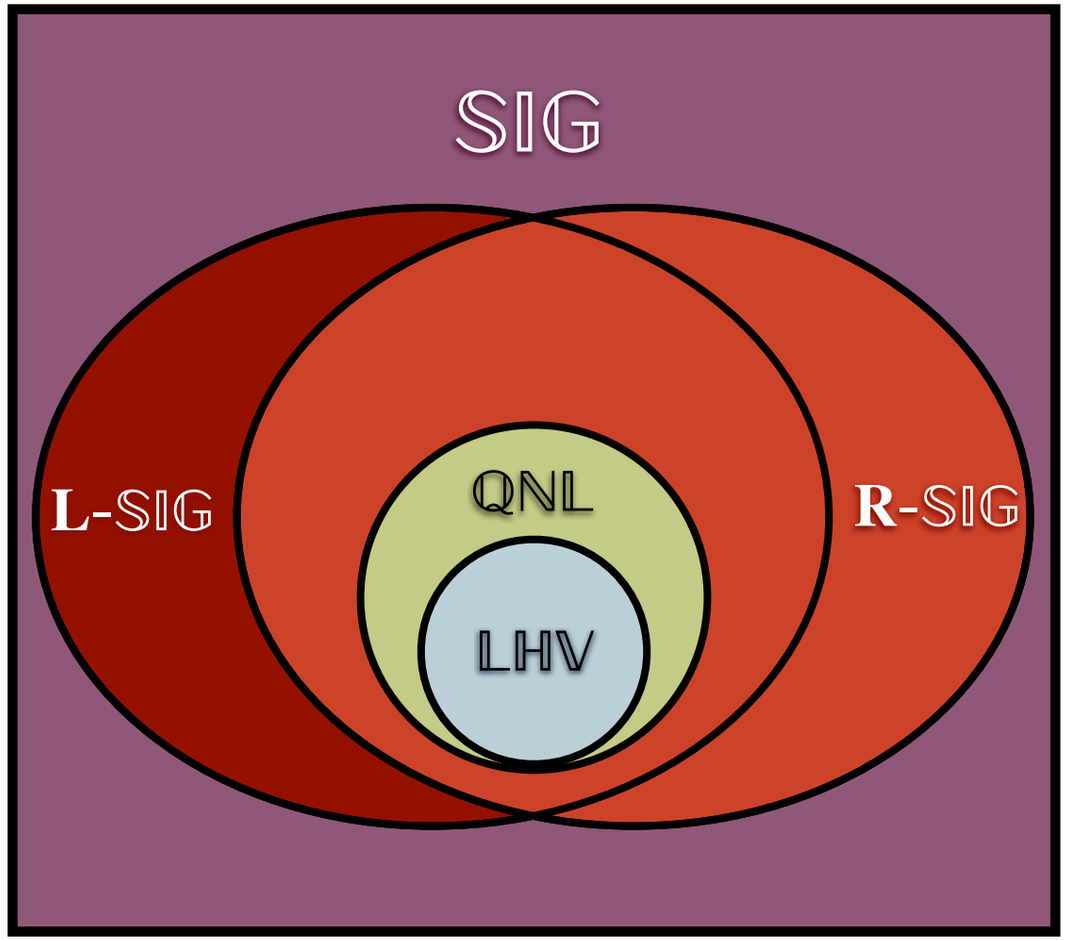
2-PARTY NON-LOCALITY HIERARCHY



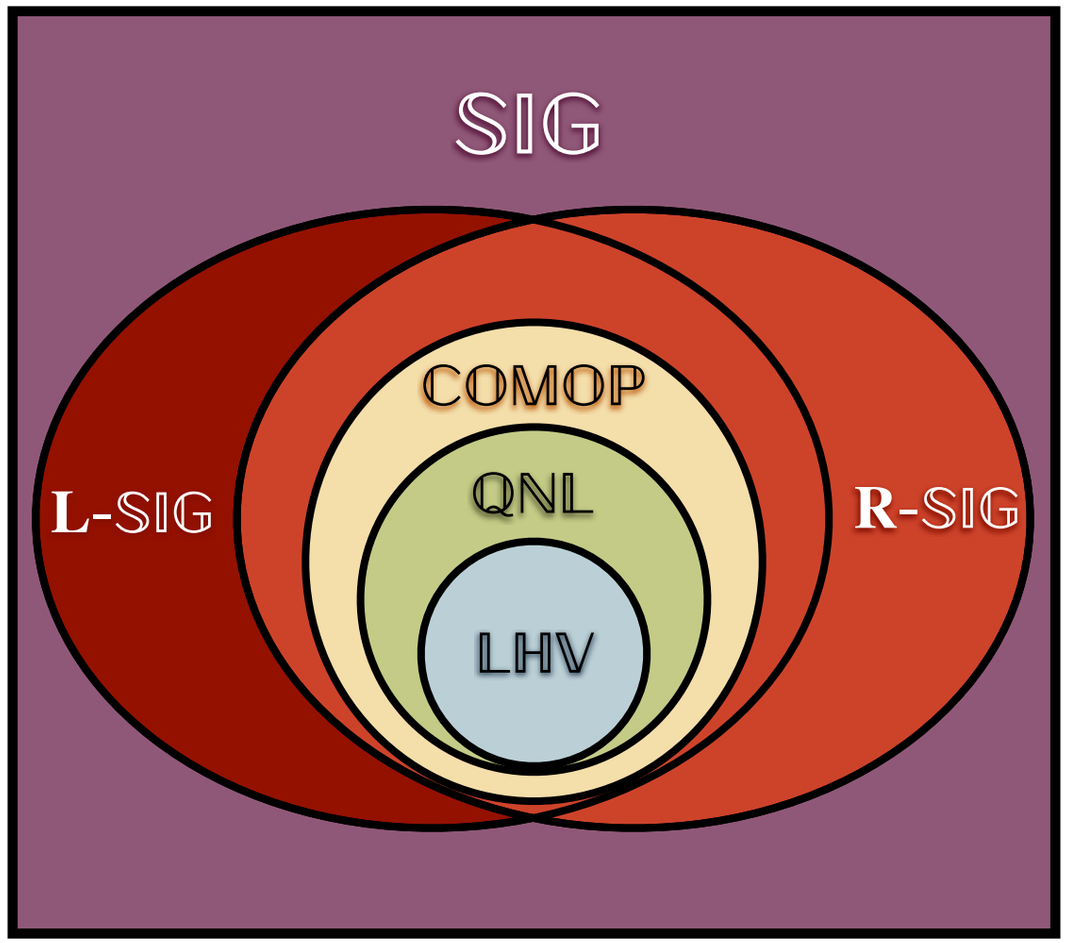
2-PARTY NON-LOCALITY HIERARCHY



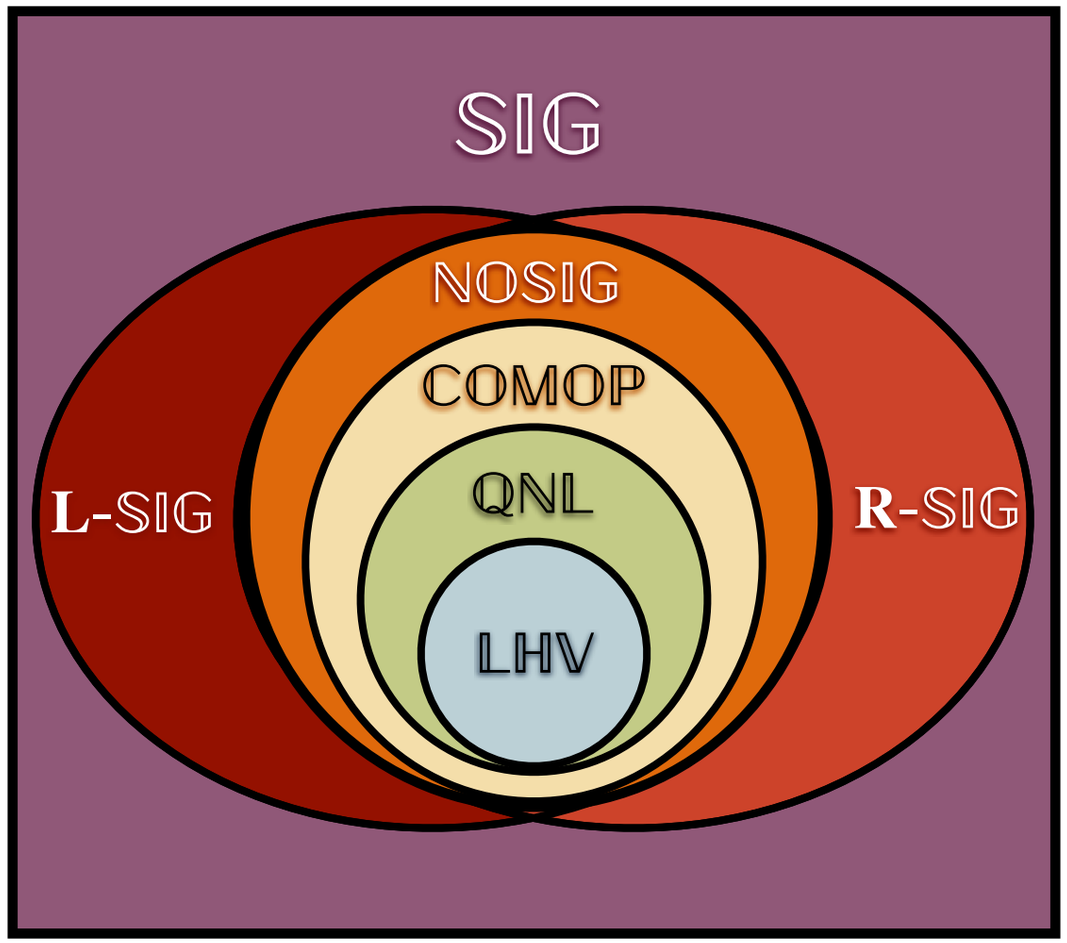
2-PARTY NON-LOCALITY HIERARCHY



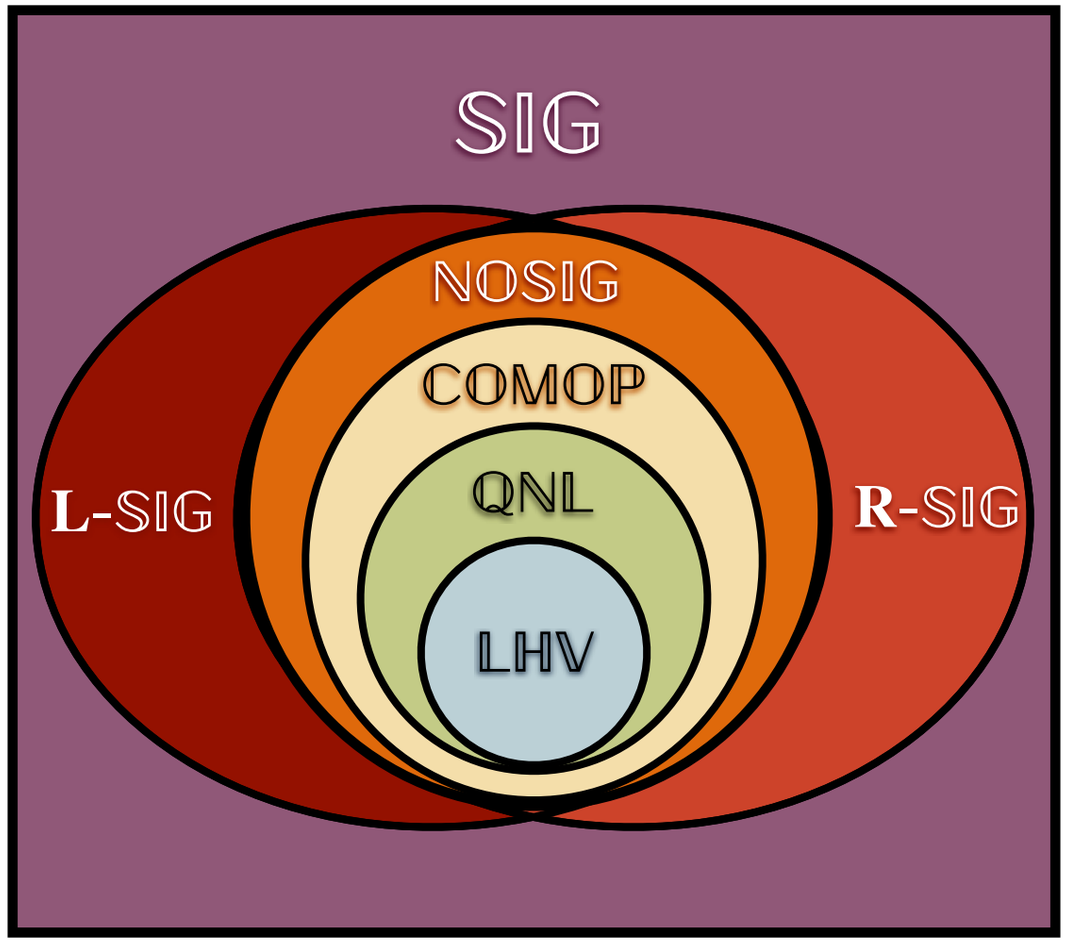
2-PARTY NON-LOCALITY HIERARCHY



2-PARTY NON-LOCALITY HIERARCHY

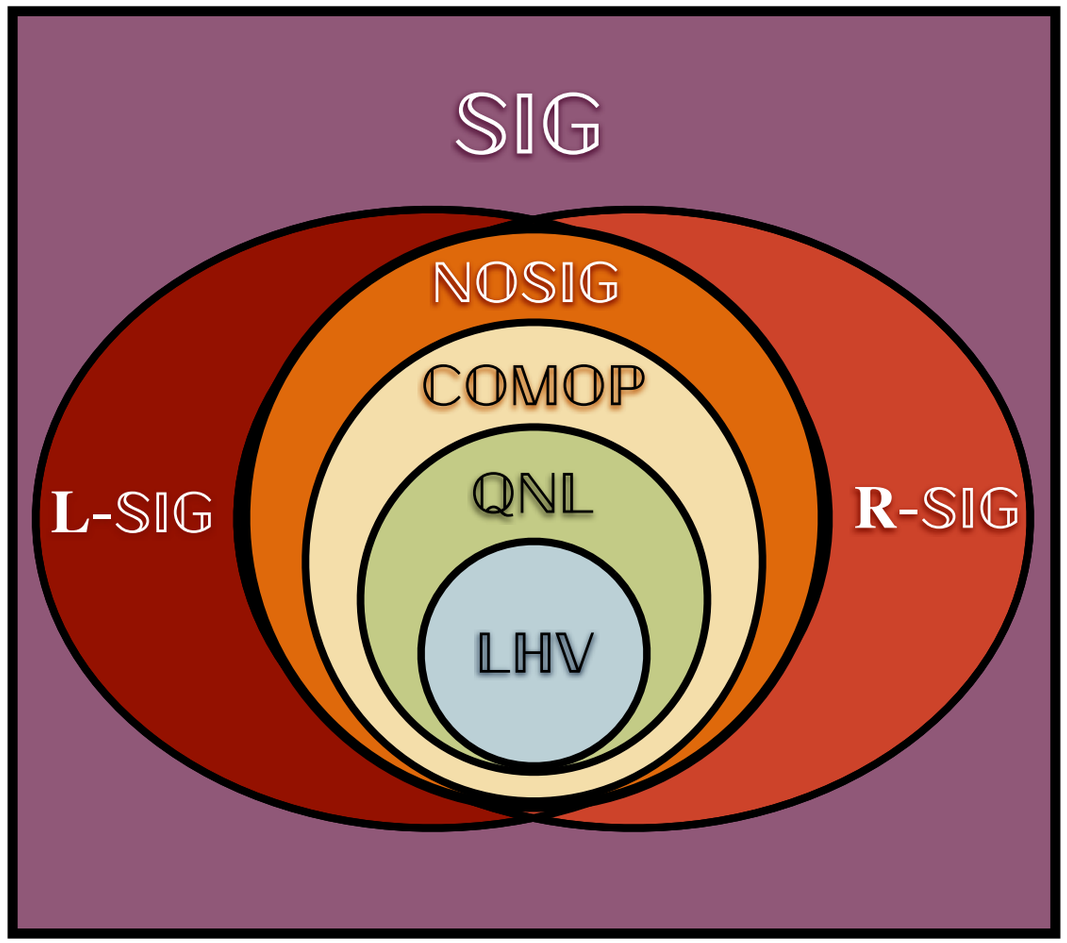


2-PARTY NON-LOCALITY HIERARCHY

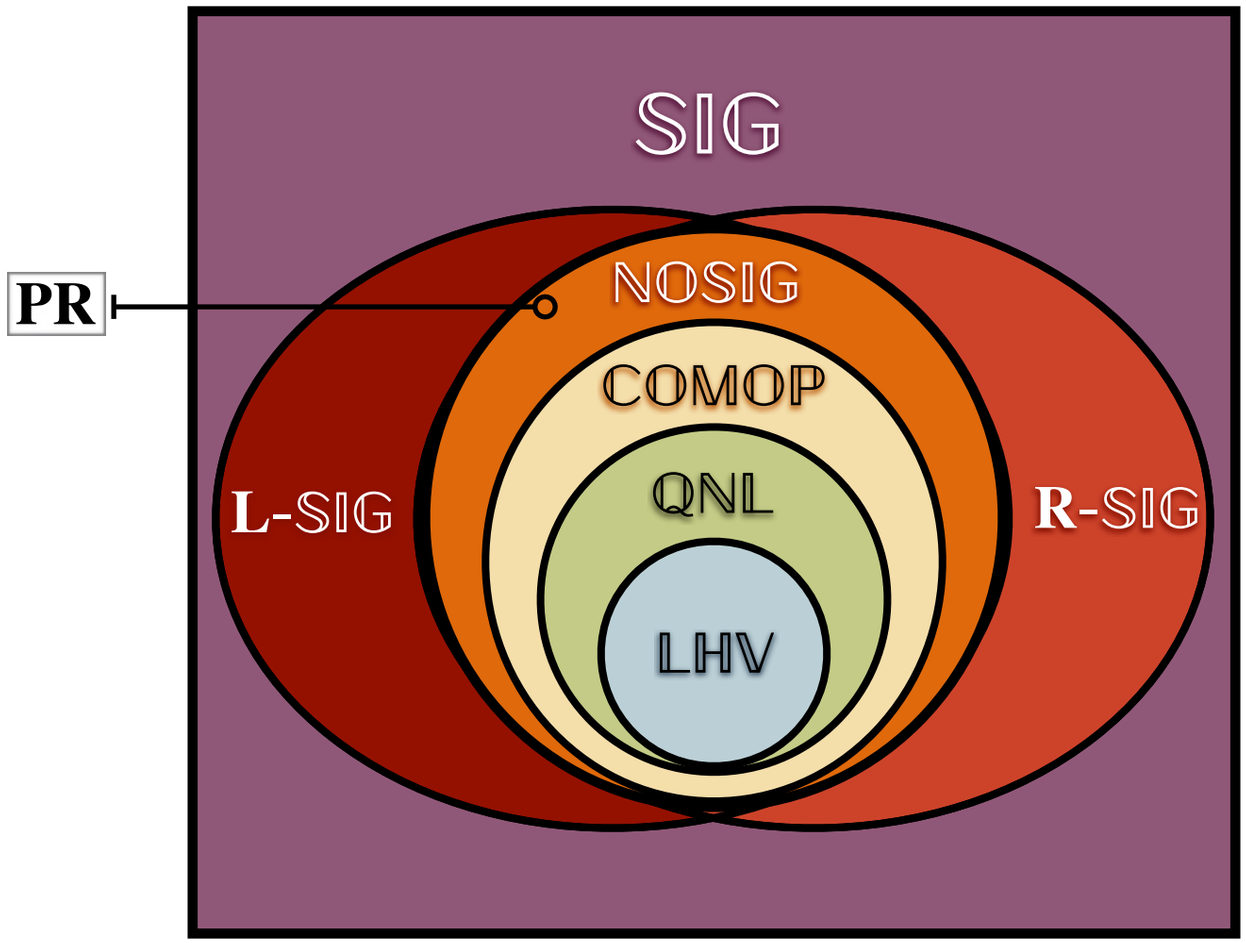


2-party NOSIG = L-SIG $\bigcap$ R-SIG

2-PARTY NON-LOCALITY HIERARCHY

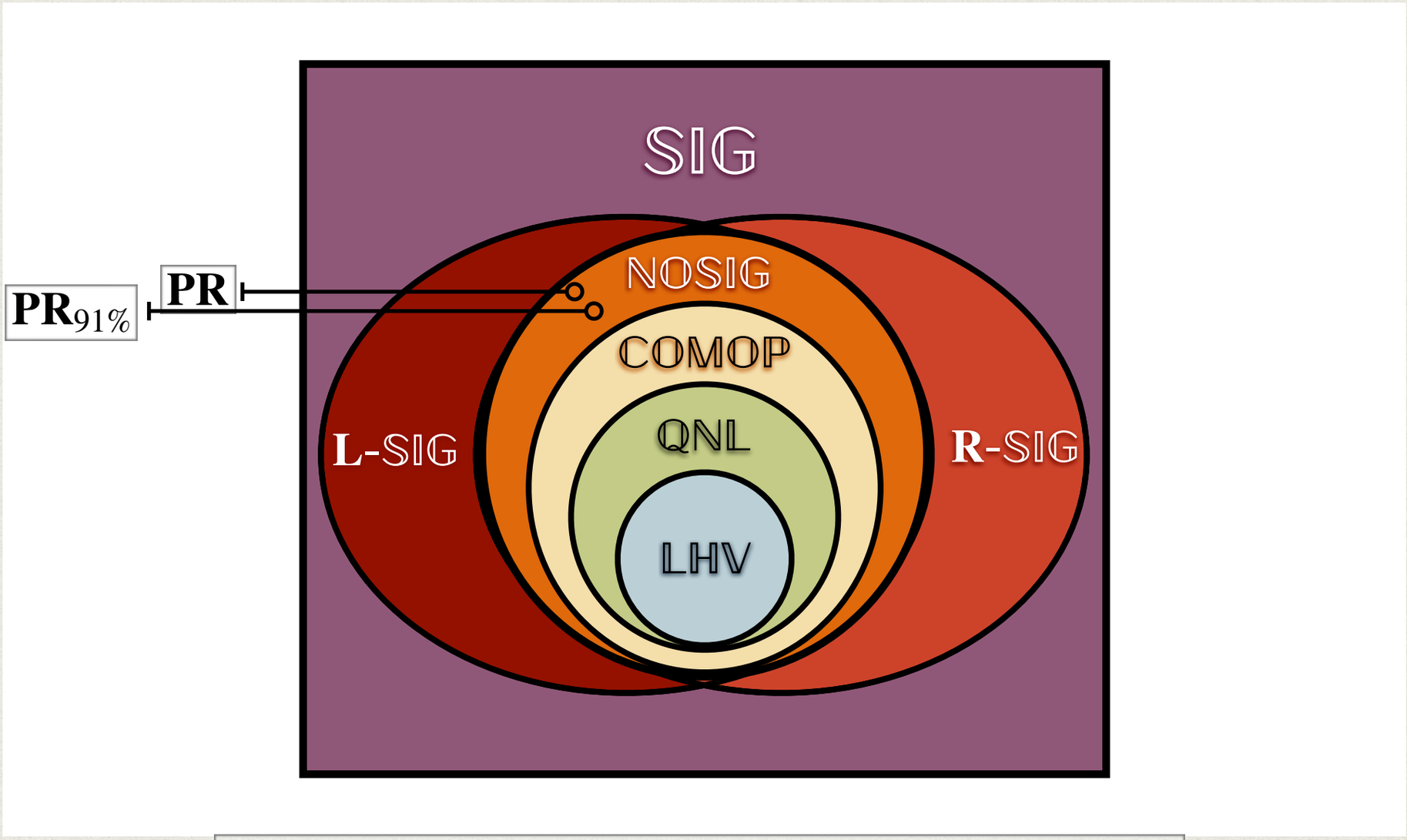


2-PARTY NON-LOCALITY HIERARCHY



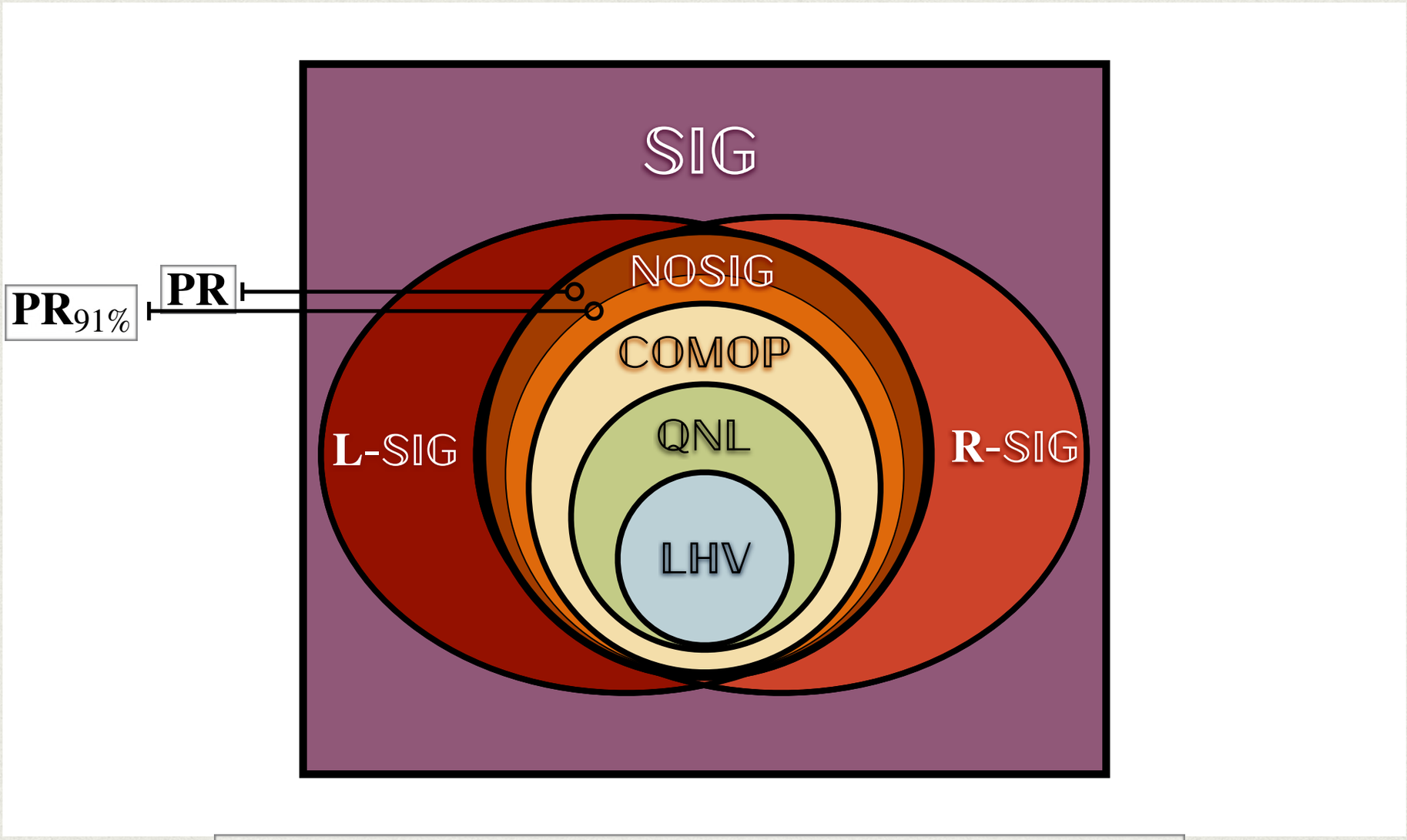
$$\forall c \in \mathbb{NOSIG}, \mathbf{PR} \implies c$$

2-PARTY NON-LOCALITY HIERARCHY



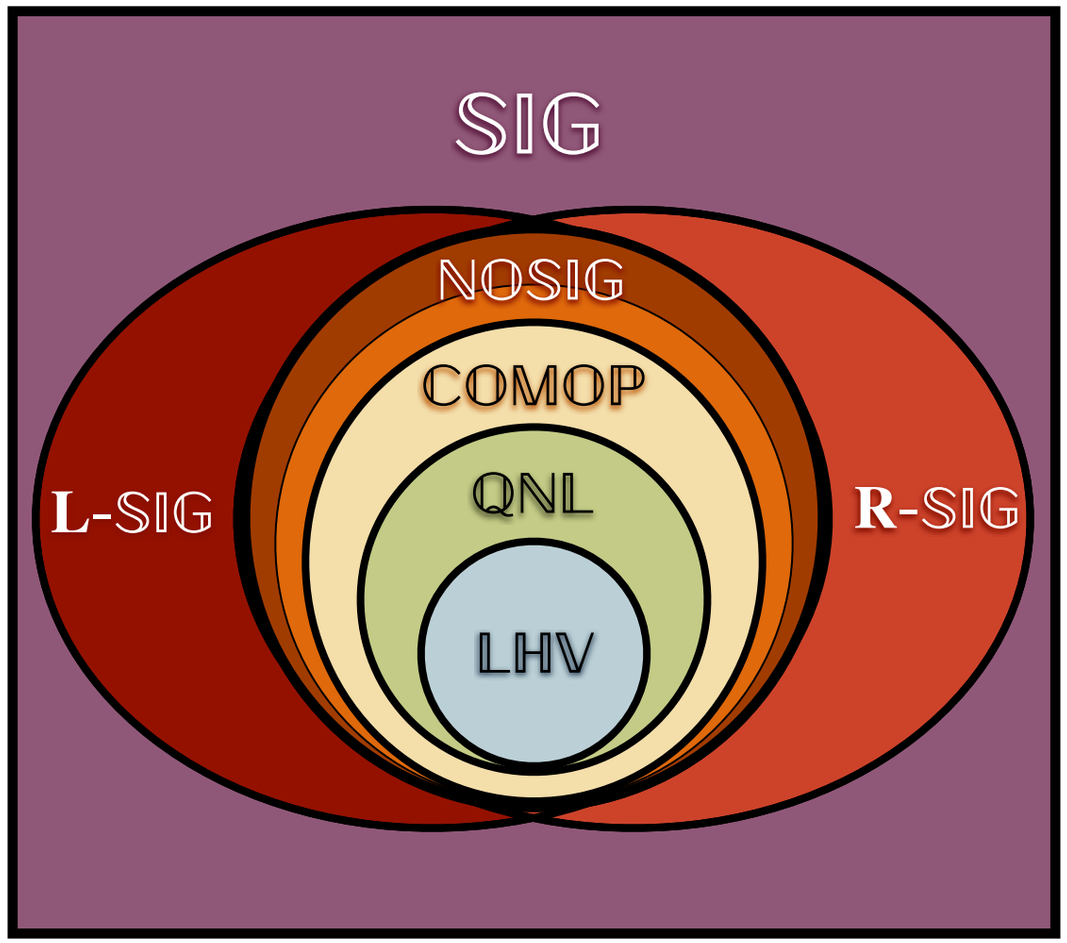
$\forall c \in \mathbb{NOSIG}, \mathbf{PR} \implies c$

2-PARTY NON-LOCALITY HIERARCHY

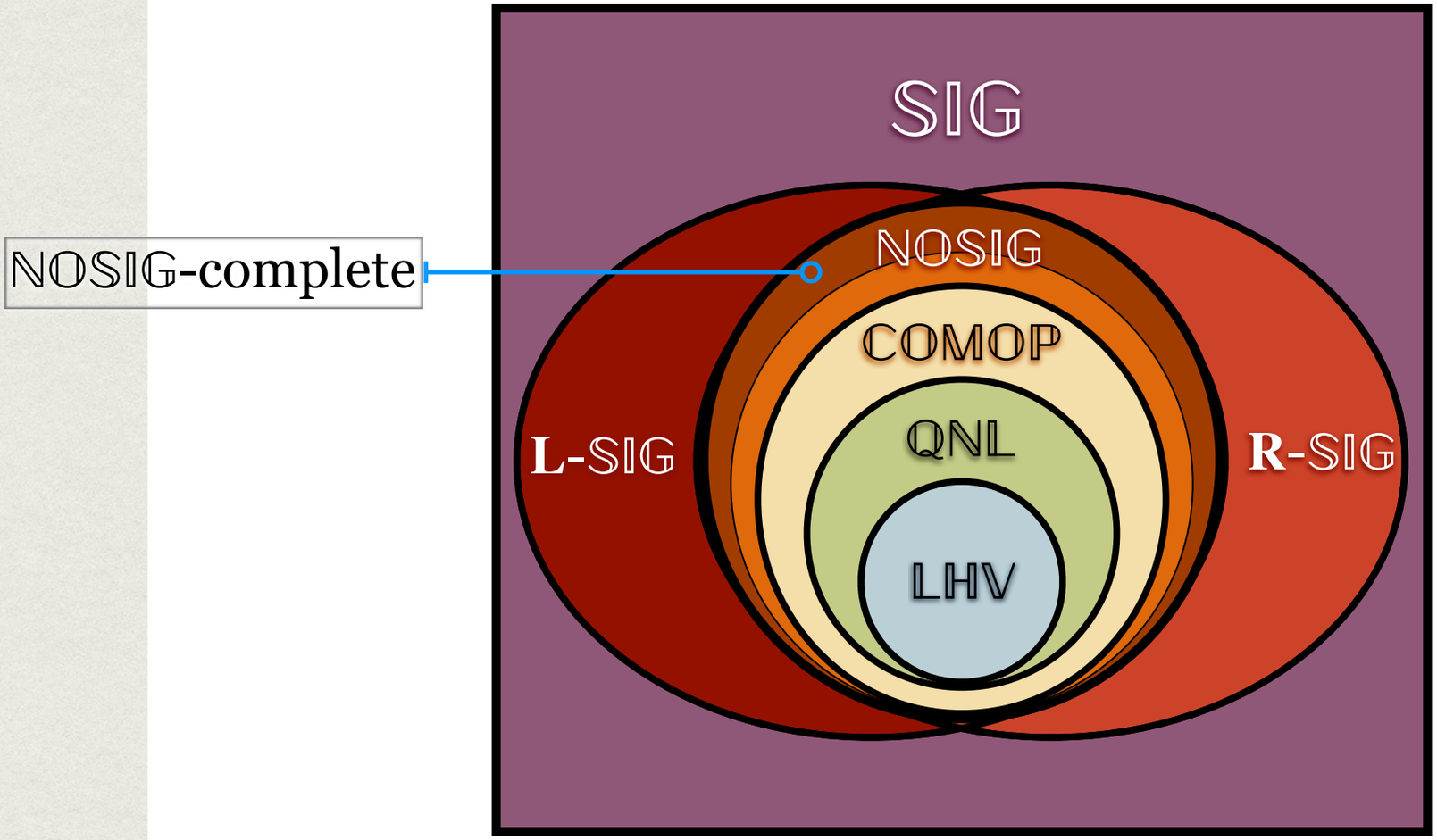


$\forall c \in \mathbb{NOSIG}, \mathbf{PR} \implies c$

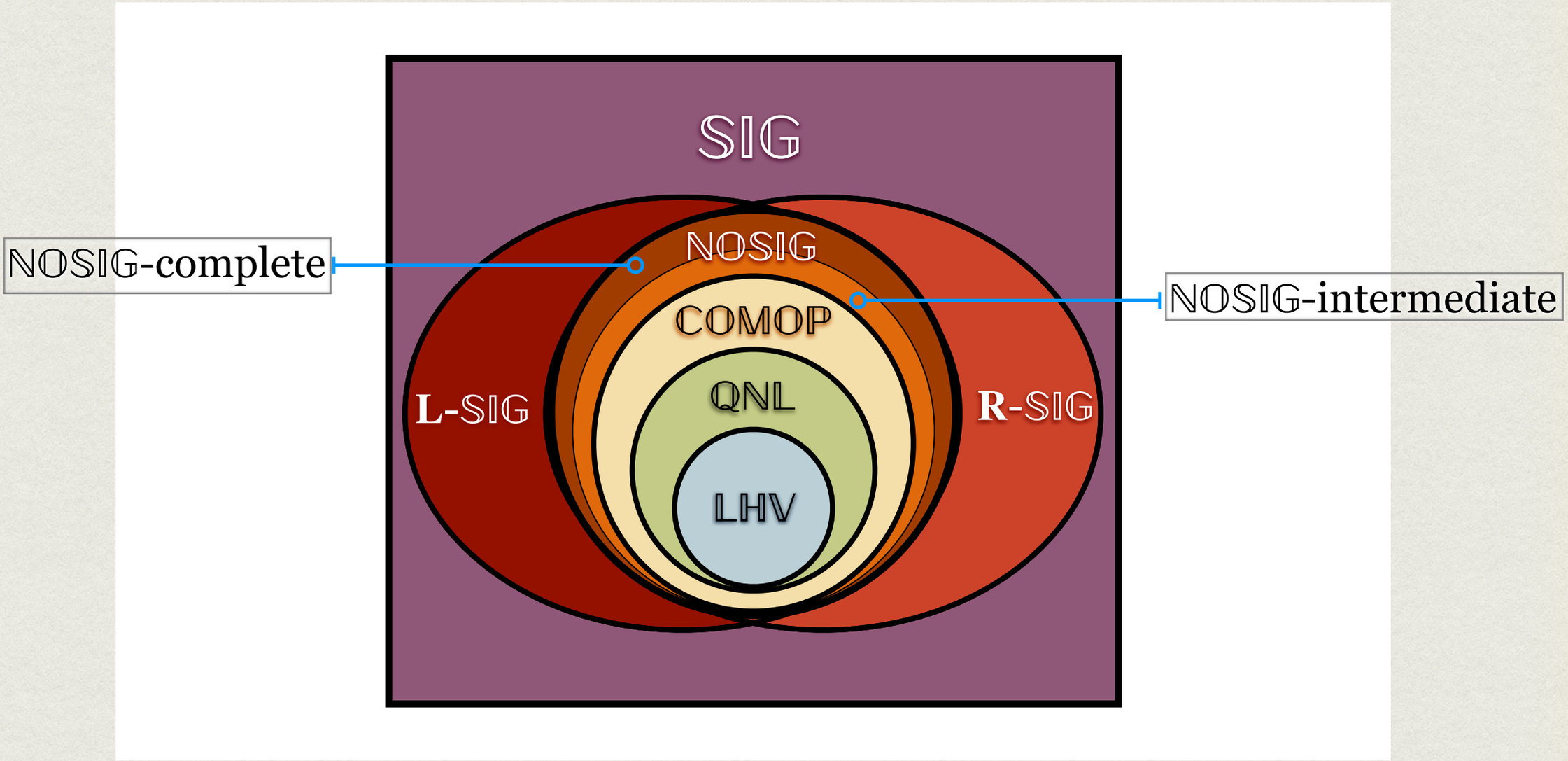
2-PARTY NON-LOCALITY HIERARCHY



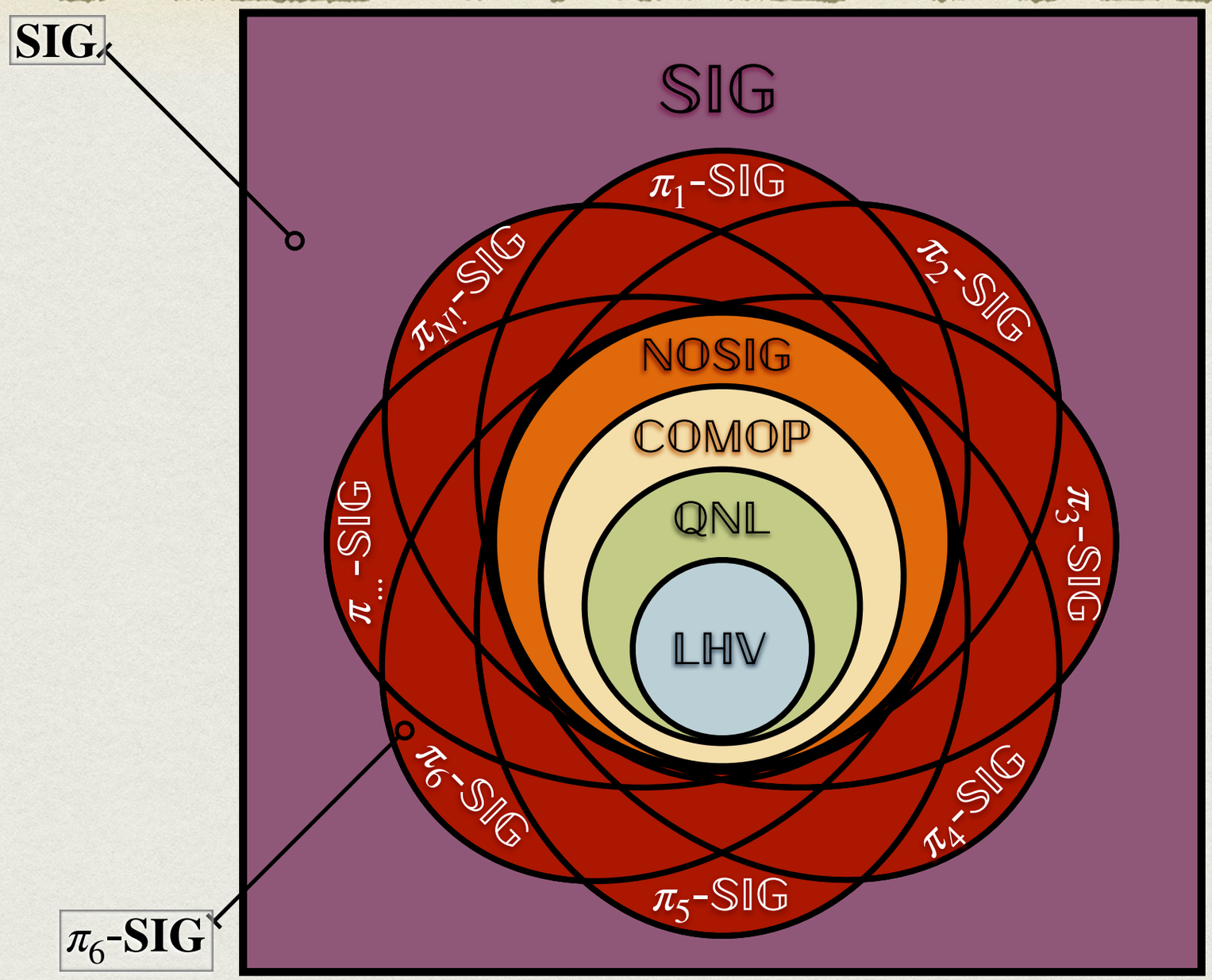
2-PARTY NON-LOCALITY HIERARCHY



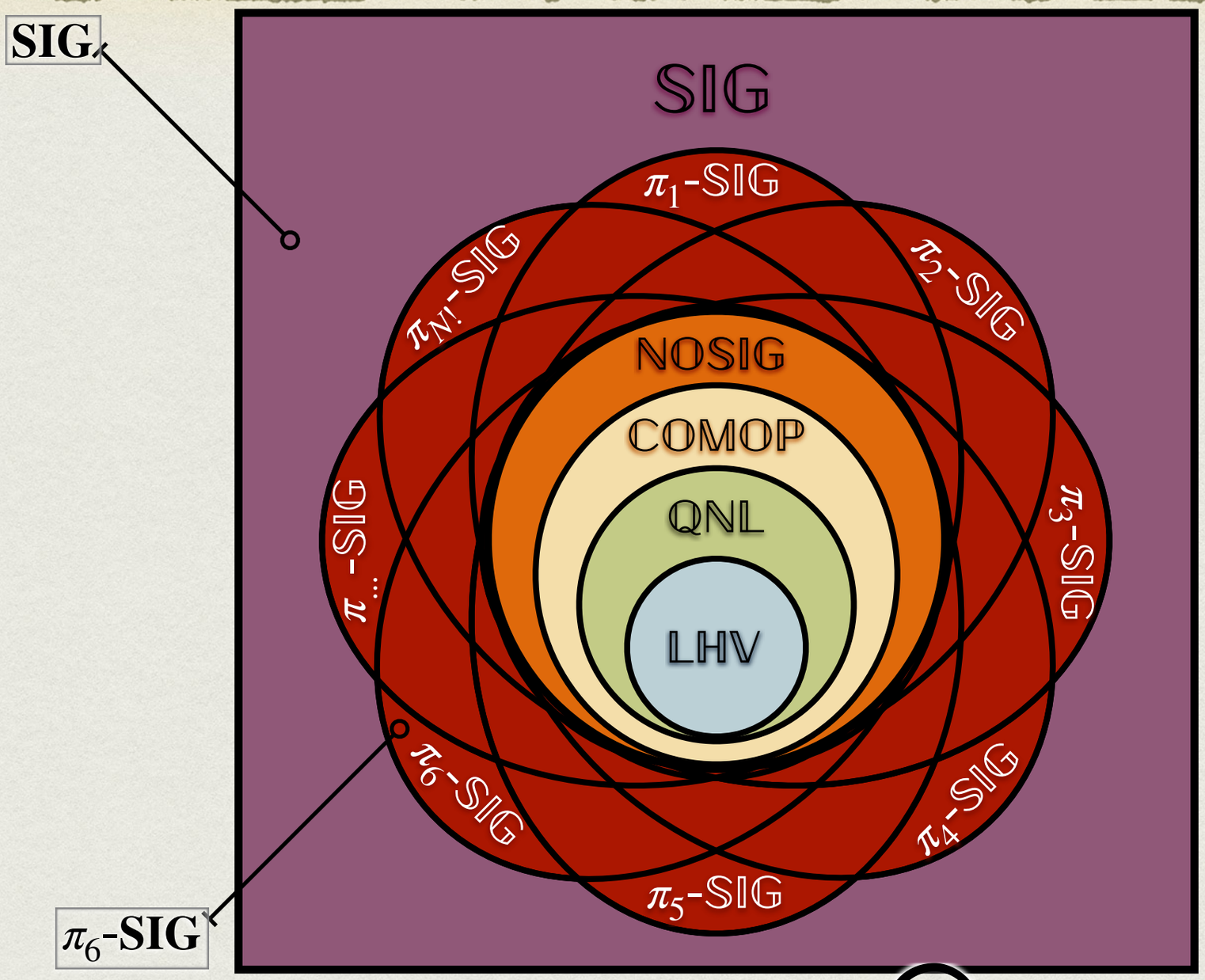
2-PARTY NON-LOCALITY HIERARCHY



N-PARTY NON-LOCALITY HIERARCHY

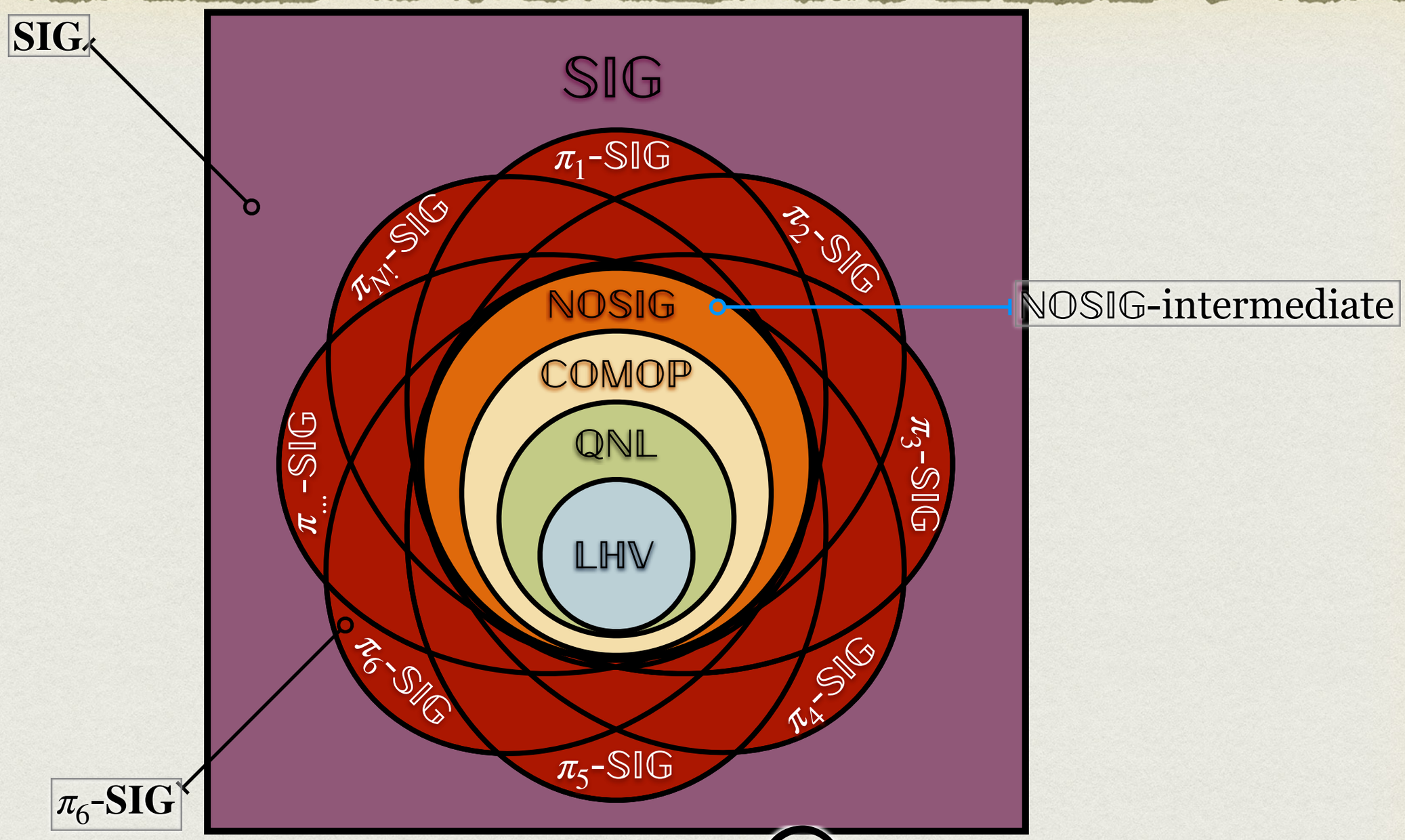


N-PARTY NON-LOCALITY HIERARCHY



$$N\text{-party NOSIG} = \bigcap_{\pi} \pi\text{-SIG}$$

N-PARTY NON-LOCALITY HIERARCHY



$$N\text{-party NOSIG} = \bigcap_{\pi} \pi\text{-SIG}$$

CHARACTERS

prover

CHARACTERS

prover

verifier

CHARACTERS

interactive proof

CHARACTERS

prover

verifier

CHARACTERS

prover

verifier

CHARACTERS

prover

verifier

judge

CHARACTERS

prover

verifier

judge

CHARACTERS

prover

verifier

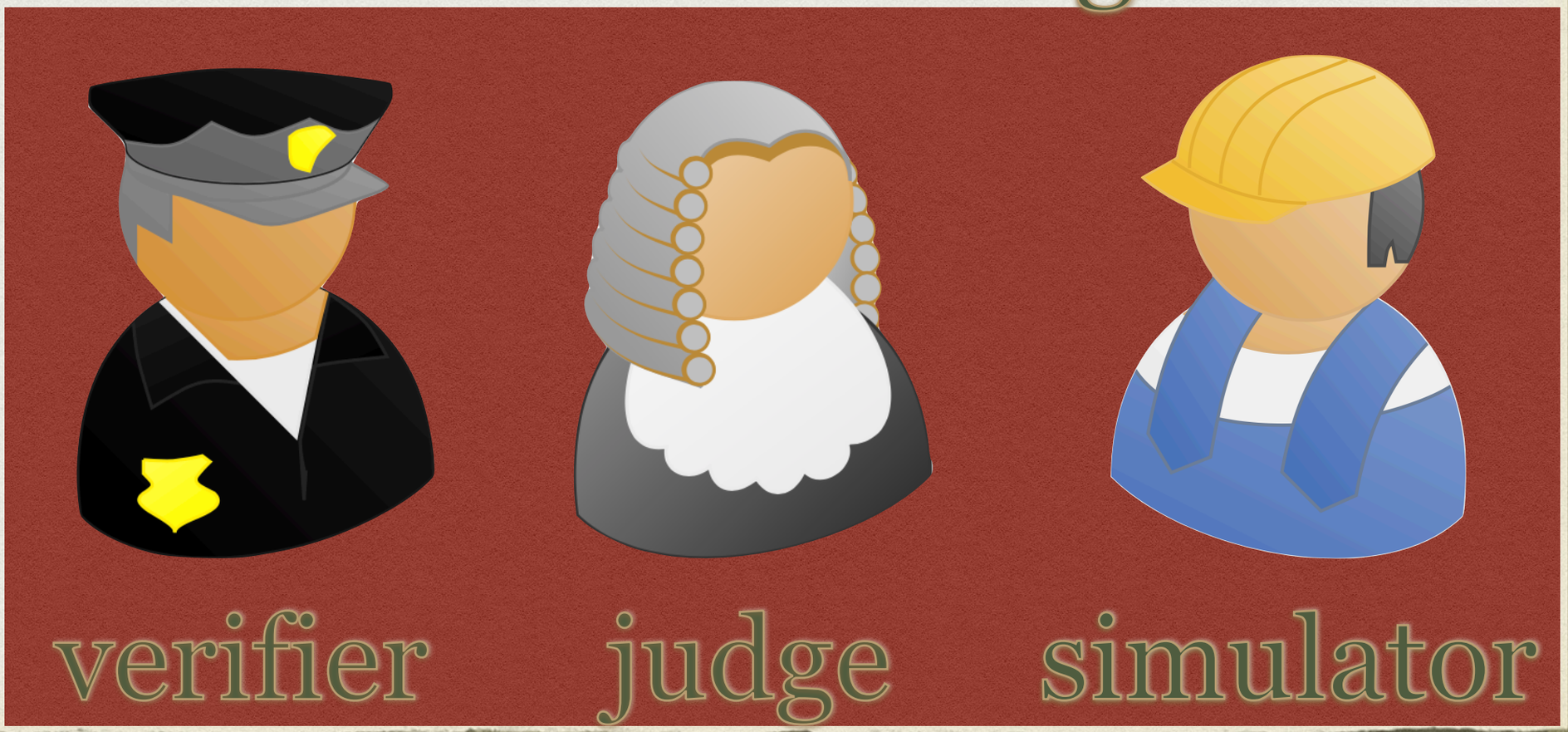
judge

simulator

CHARACTERS

zero-knowledge

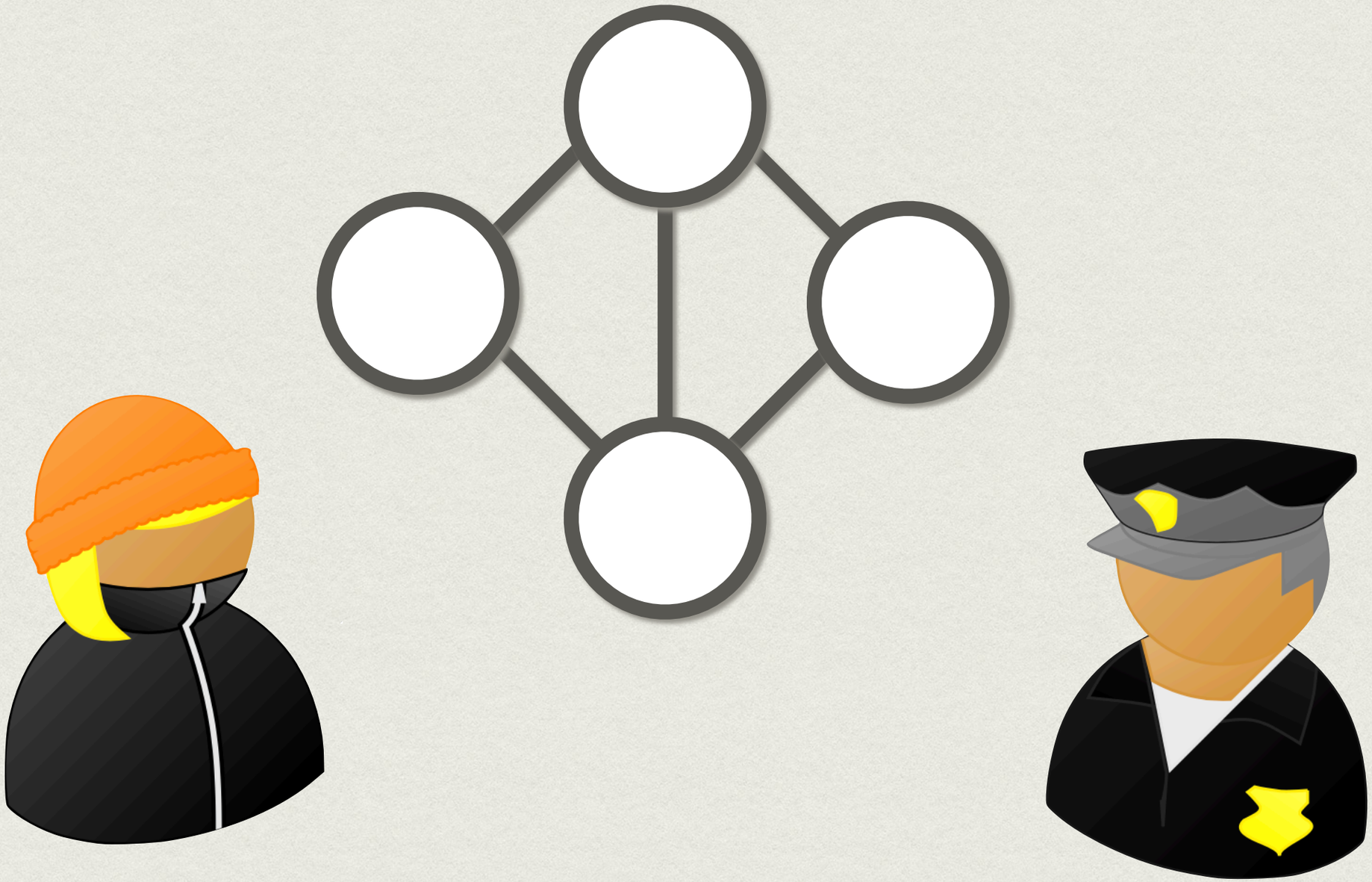
prover



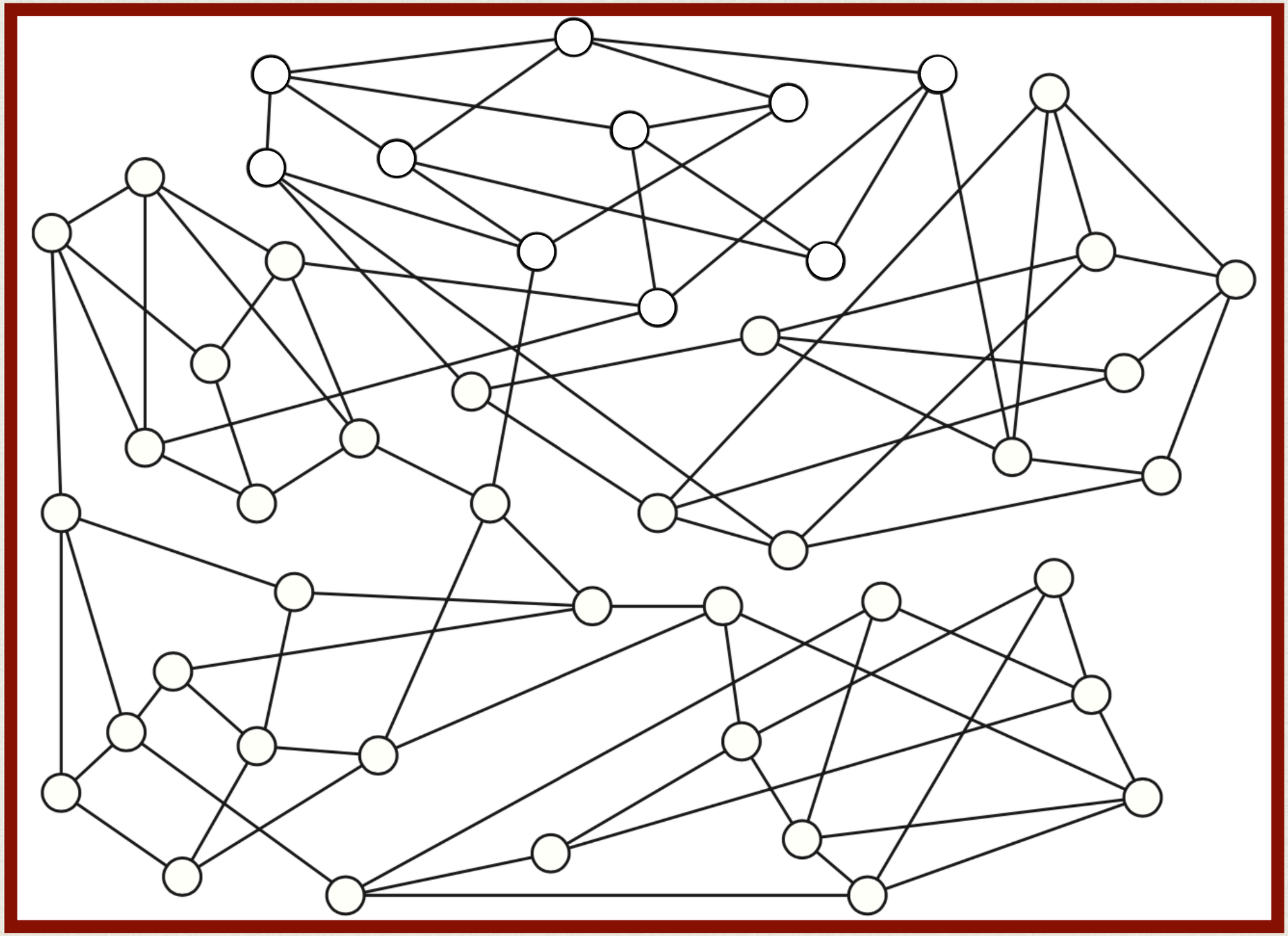
verifier judge simulator

TRADITIONAL PROOFS

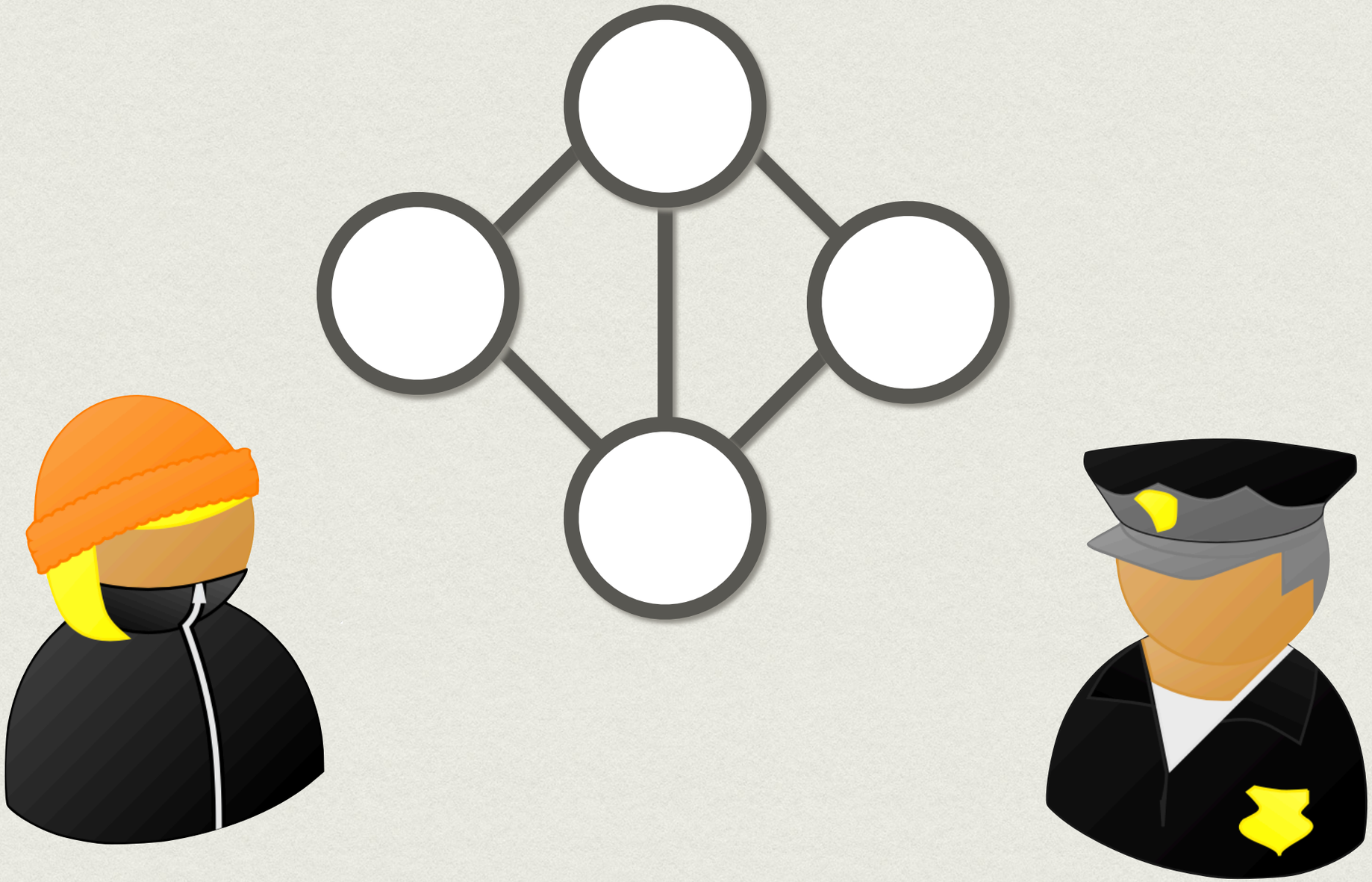
3-COL



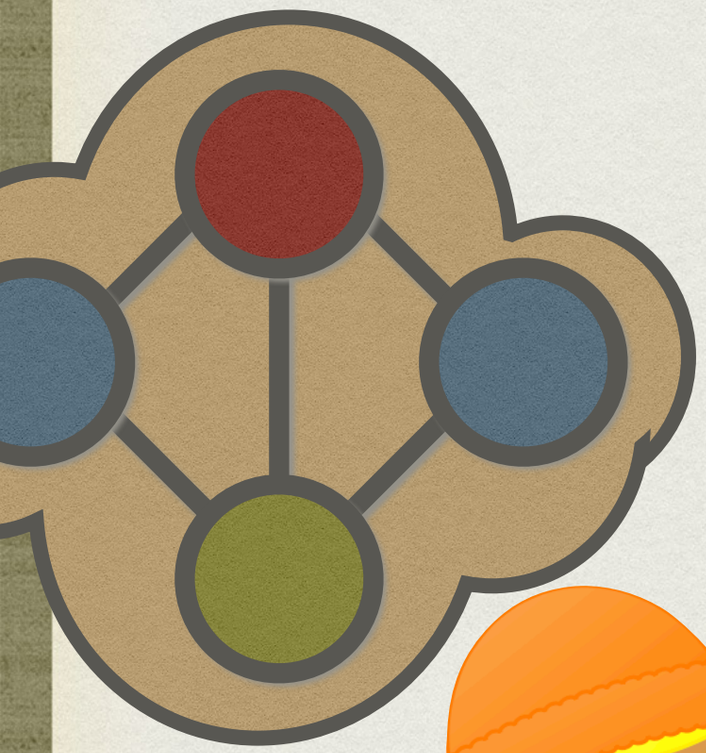
3-COL

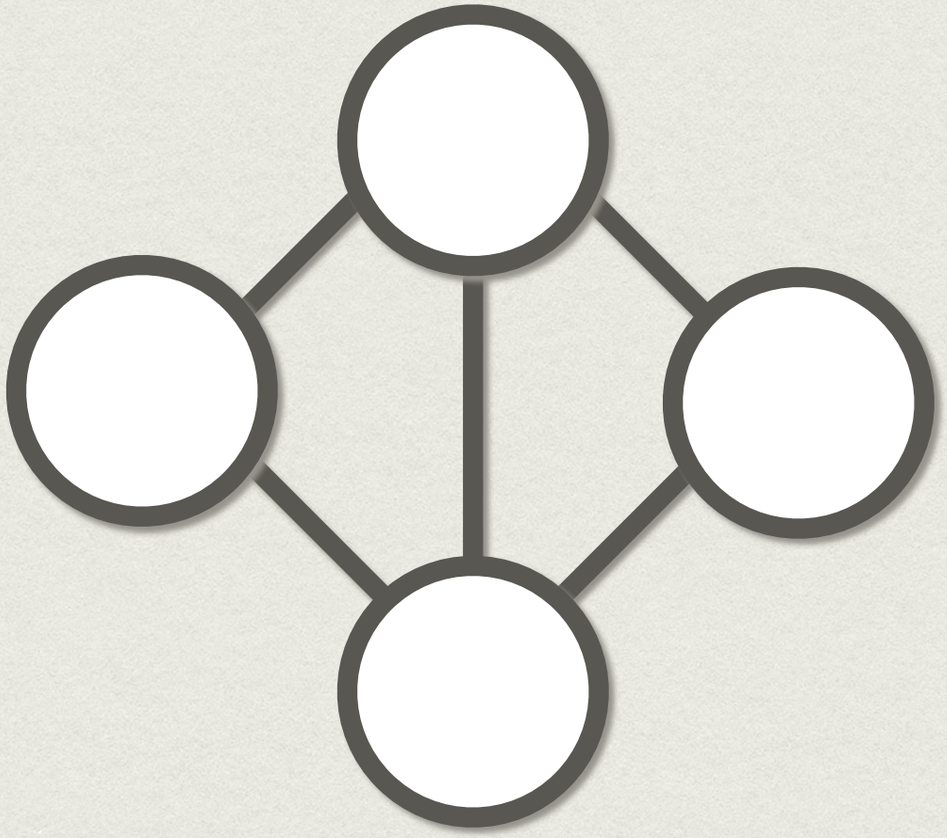


3-COL



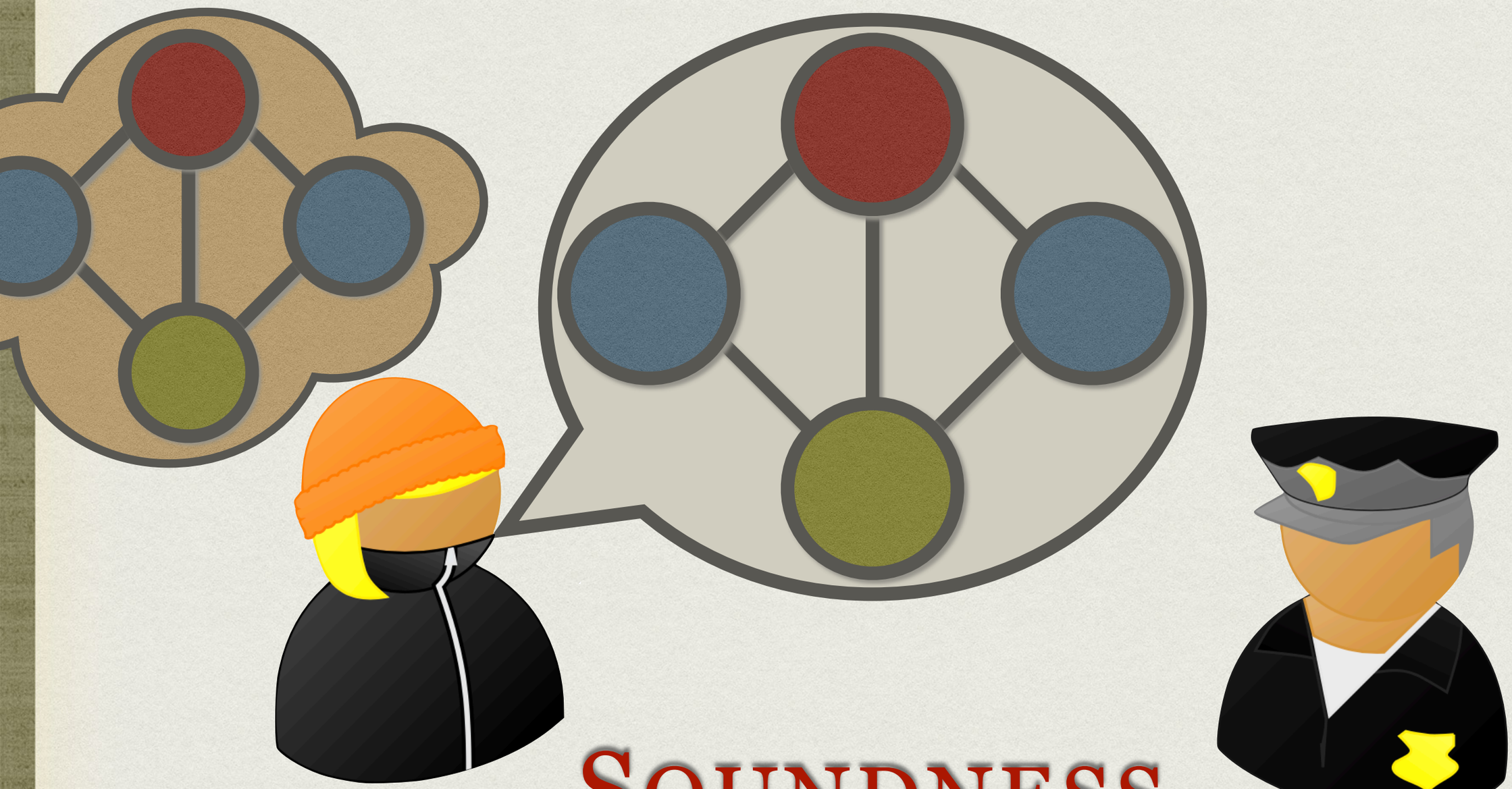
3-COL





3-COL

Completeness



Soundness

3-COL

COMPLETENESS

SOUNDNESS

INTERACTIVE PROOFS

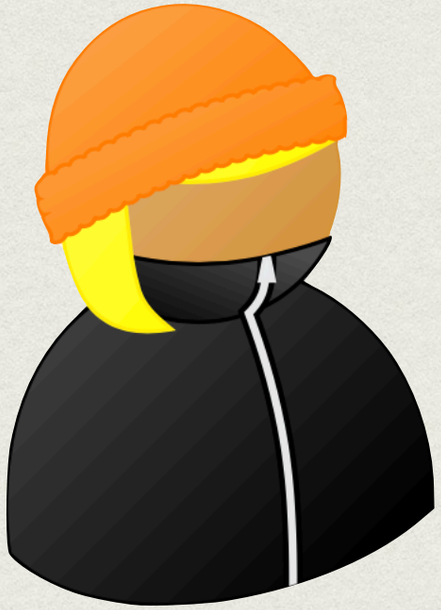
Goldwasser

Micali

Rackoff

1985

W



Goldwasser

Micali

Rackoff

1985

$w \in L$

Goldwasser

Micali

Rackoff

1985

$L \in IP$

$w \in L$

w

Goldwasser

Micali

Rackoff

1985

L∈IP

w∈L

Goldwasser

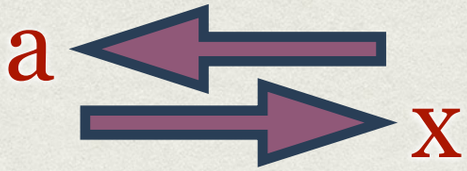
Micali

Rackoff

1985

L∈IP

w∈L



Goldwasser

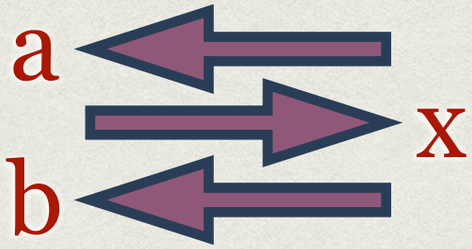
Micali

Rackoff

1985

L∈IP

w∈L



Goldwasser

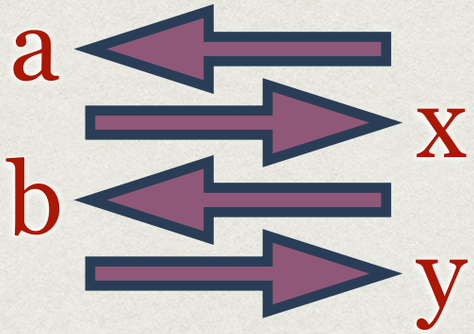
Micali

Rackoff

1985

L∈IP

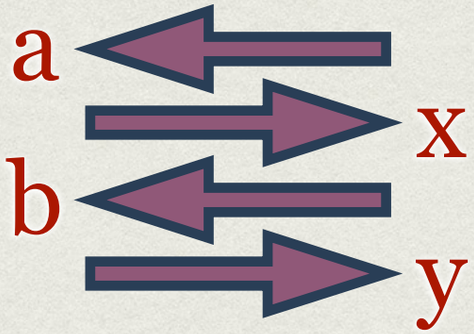
w∈L



Completeness

$\exists$ $\exists$ $\forall w \in L, \mathbf{Prob}[($ $:$ $)(w)$ accepts $] \geq 1 - \epsilon$

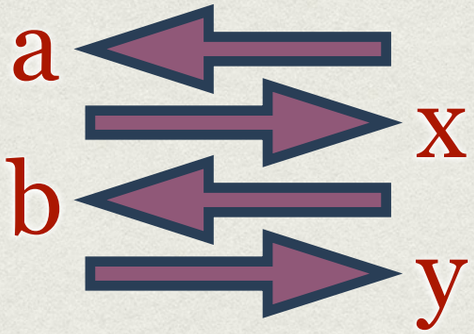
poly



Completeness

$\exists$ $\exists$ $\forall w \in L, \mathbf{Prob}[($ $:$ $)(w)$ accepts $] \geq 1 - \epsilon$

poly



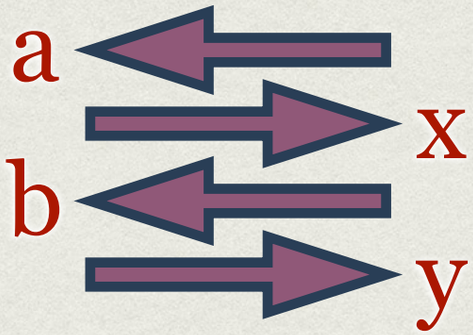
Soundness

$\exists$ $\exists$ $\forall w \in L, \mathbf{Prob}[($ $:$ $)(w)$ accepts $] \geq 1 - \epsilon$

poly

$\forall$ $, w \notin L, \mathbf{Prob}[($ $:$ $)(w)$ accepts $] \leq \epsilon$

W



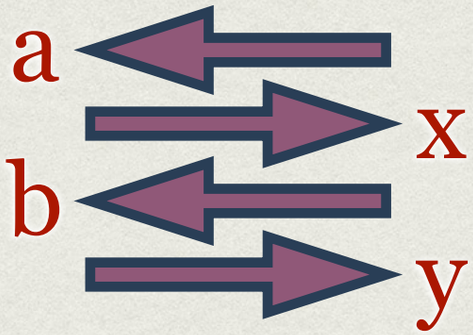
Soundness

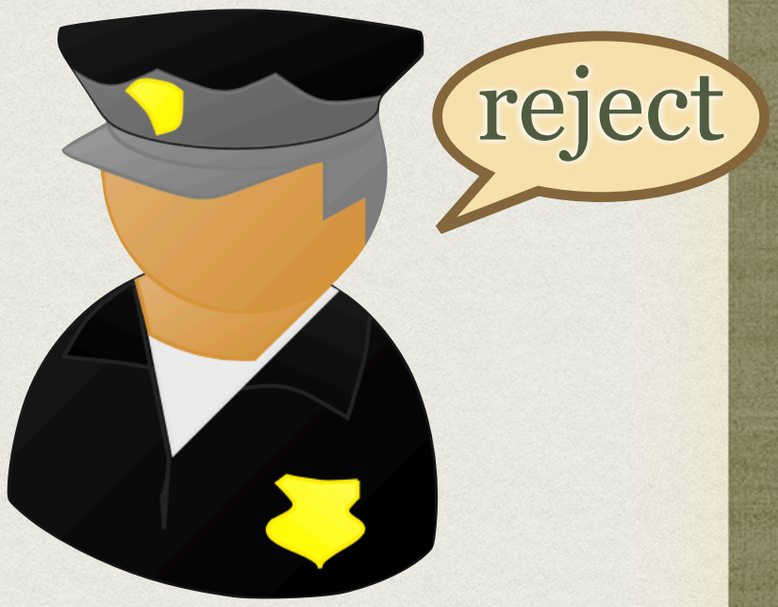
$\exists$ $\exists$ $\forall w \in L, \mathbf{Prob}[($ $:$ $)(w)$ accepts $] \geq 1 - \epsilon$

poly

$\forall$ $, w \notin L, \mathbf{Prob}[($ $:$ $)(w)$ accepts $] \leq \epsilon$

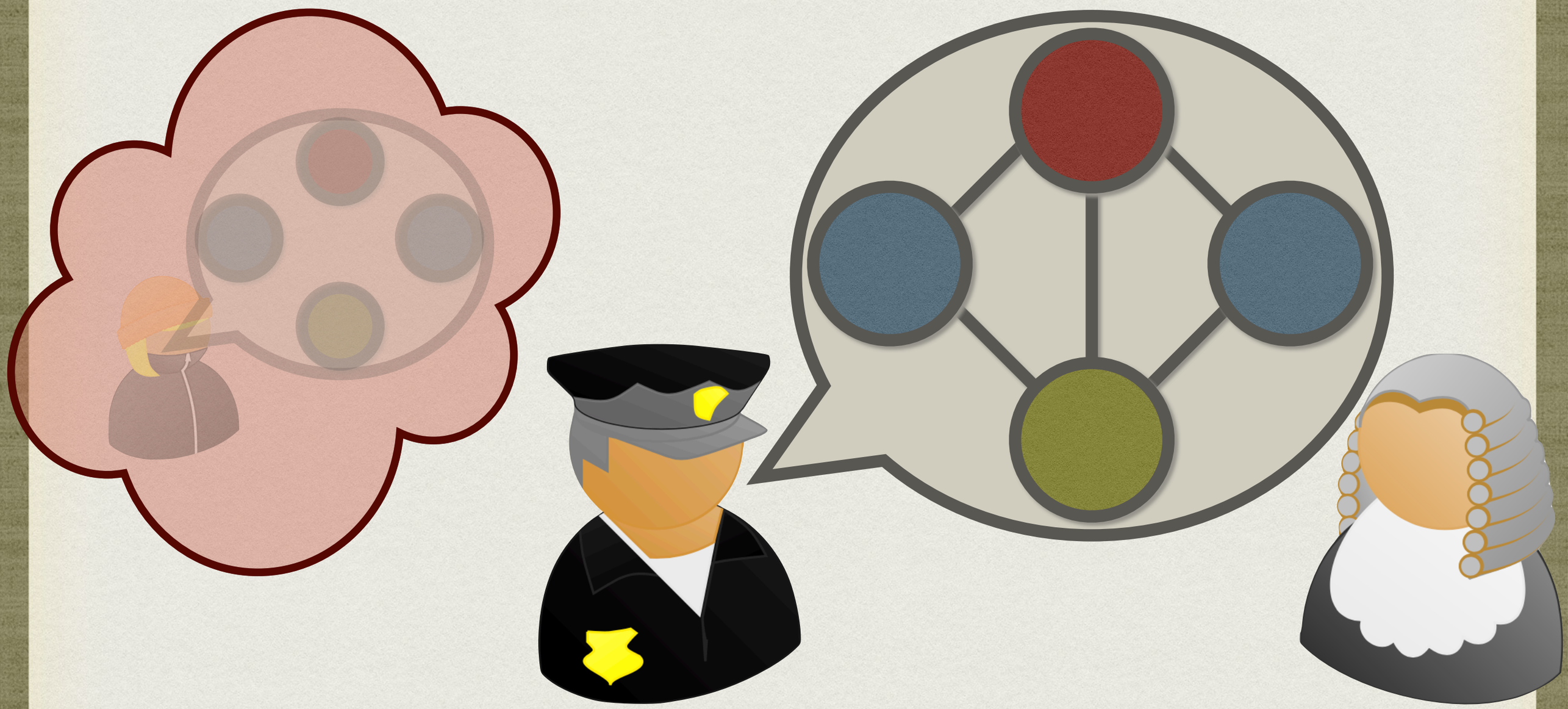
W





ZERO-KNOWLEDGE

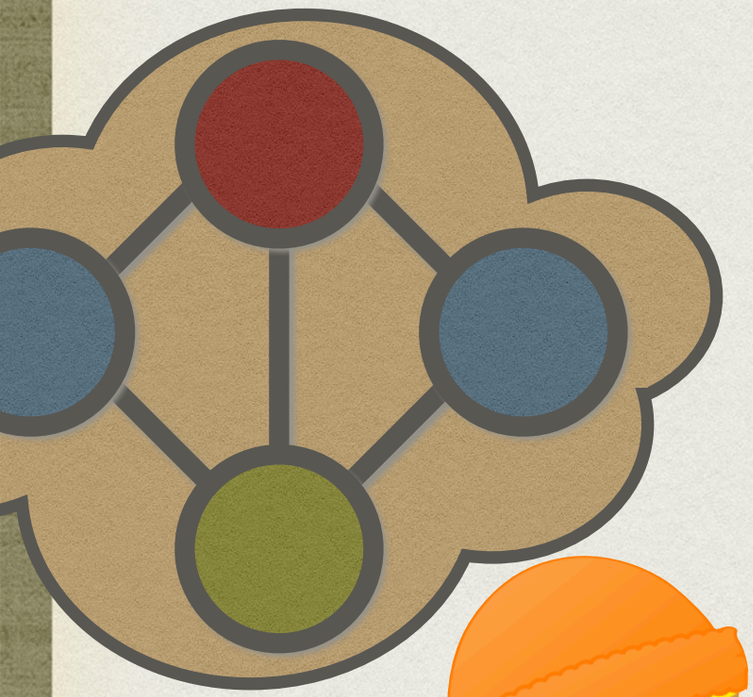
3-COL

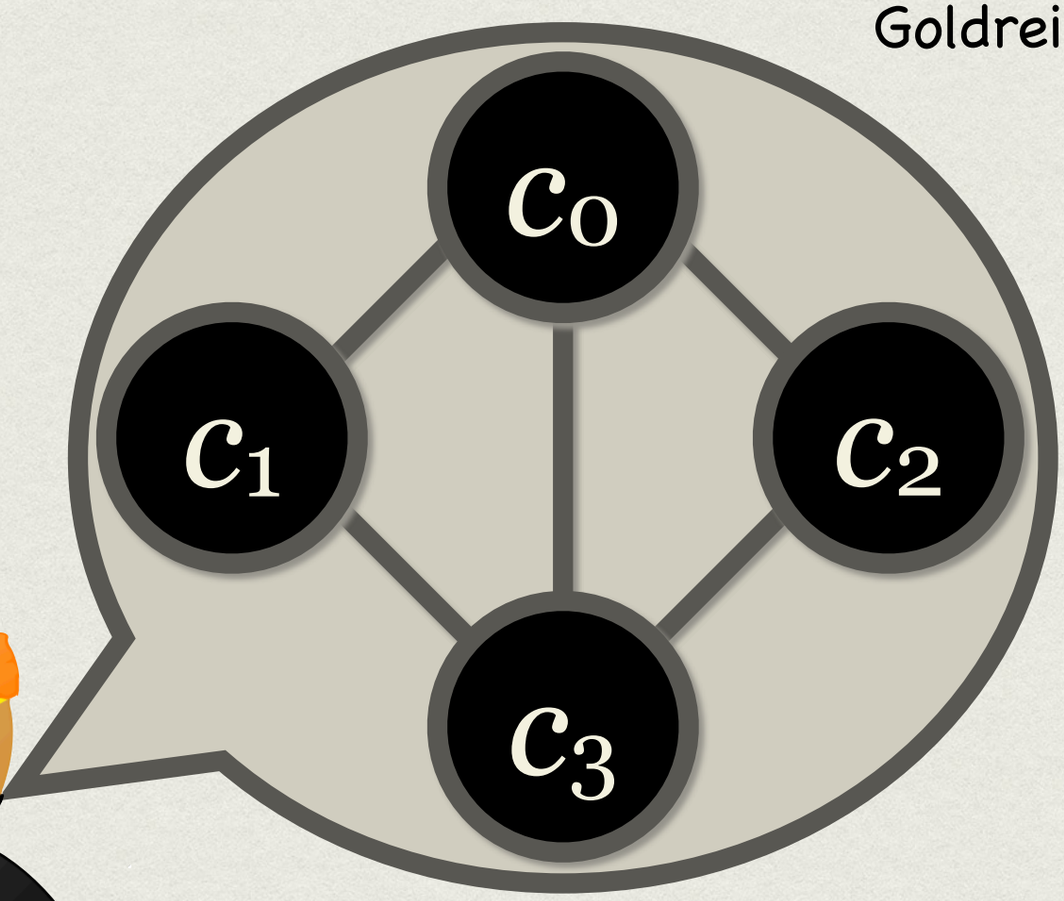


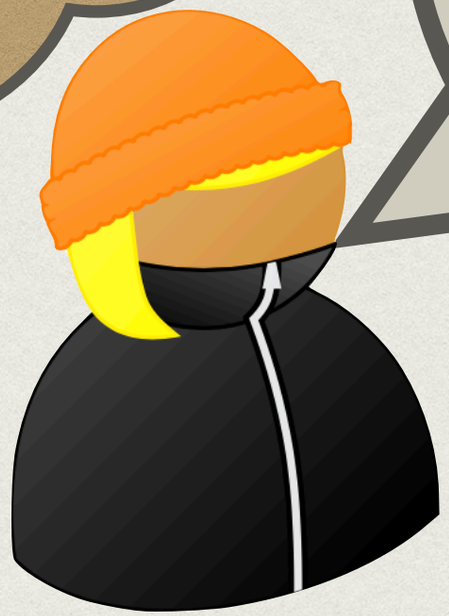
TRANSFERABLE

3-COL (86)

Goldreich Micali Wigderson

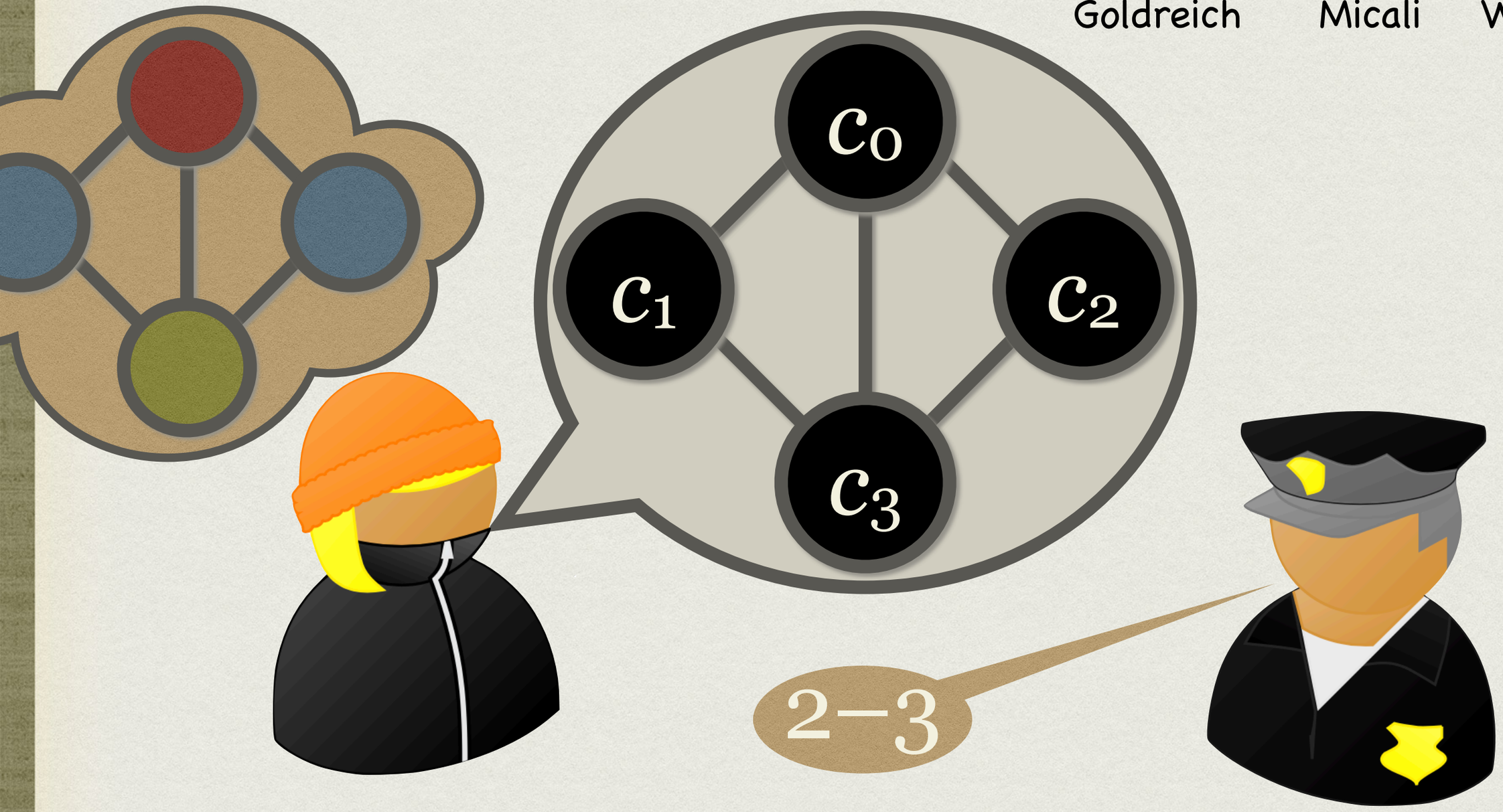




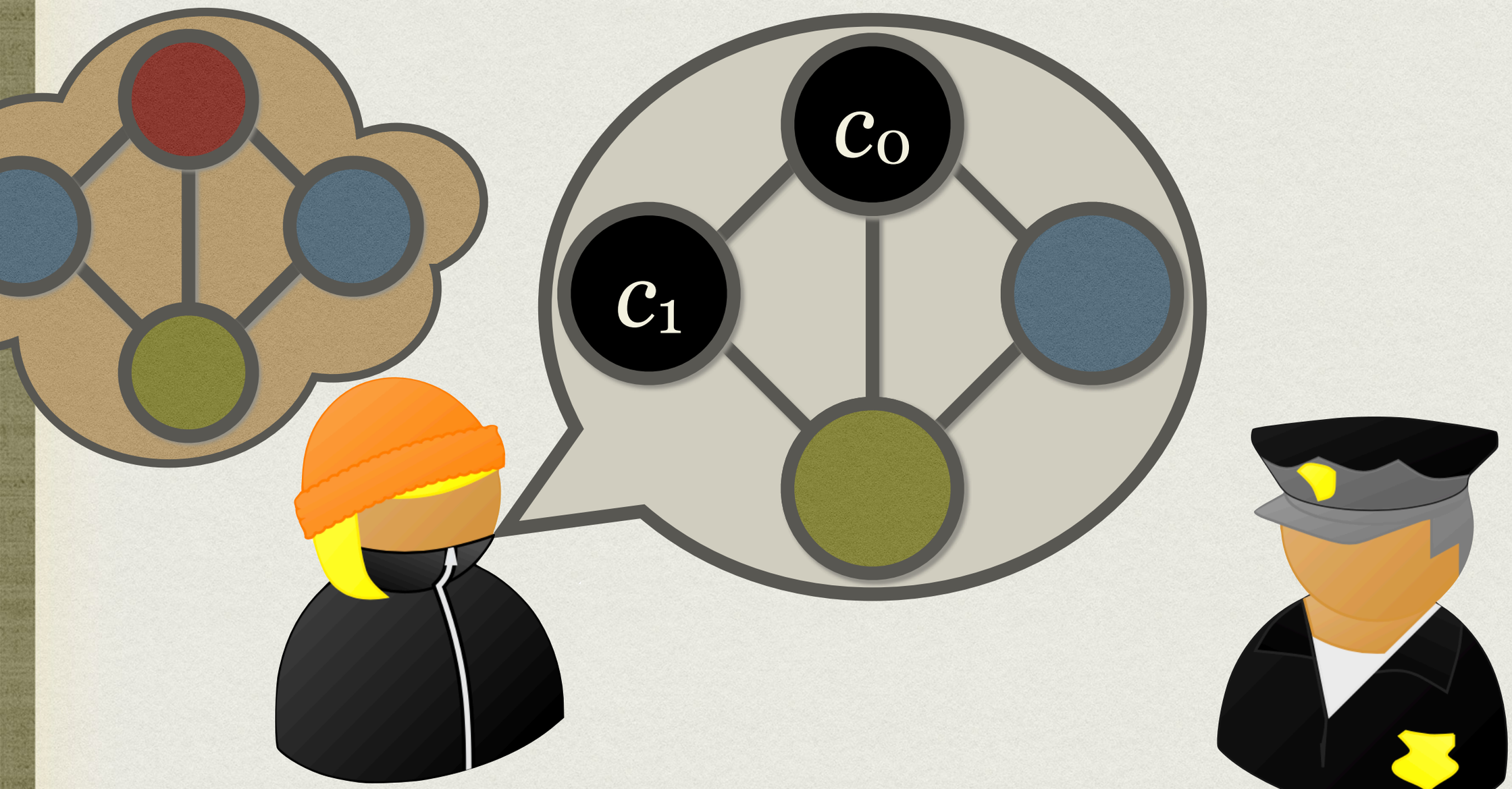


3-COL (86)

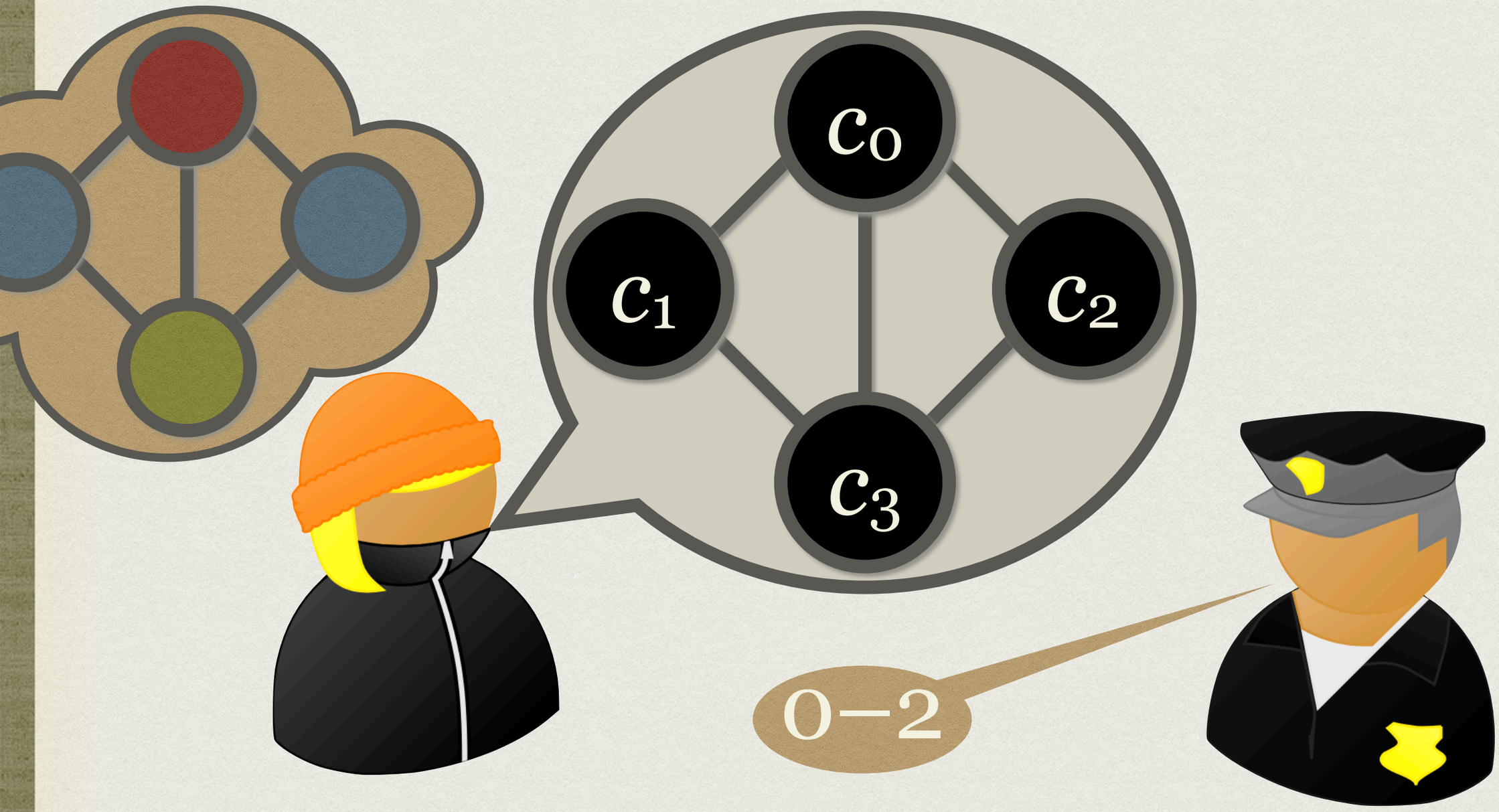
Goldreich Micali Wigderson



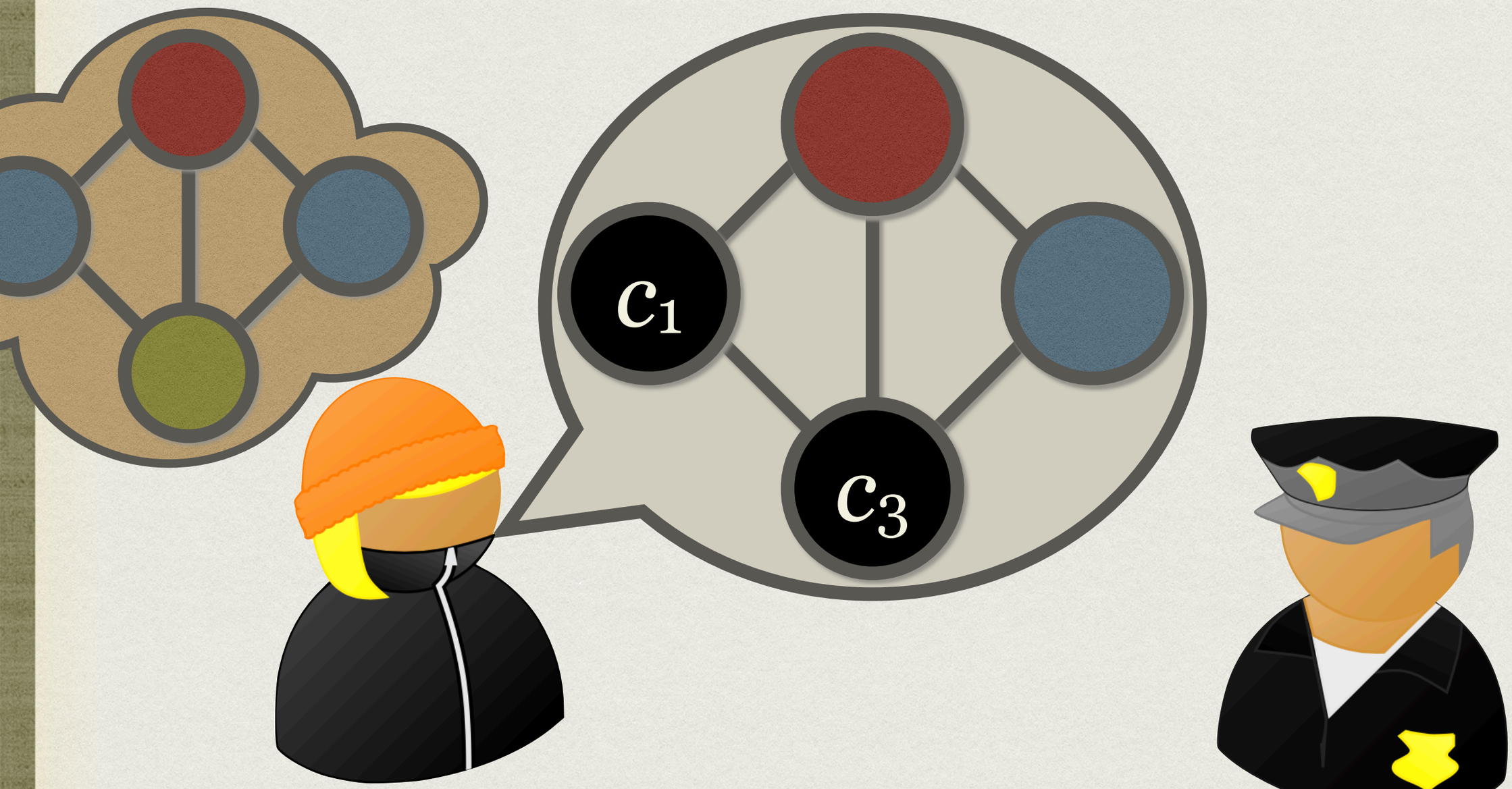
3-COL



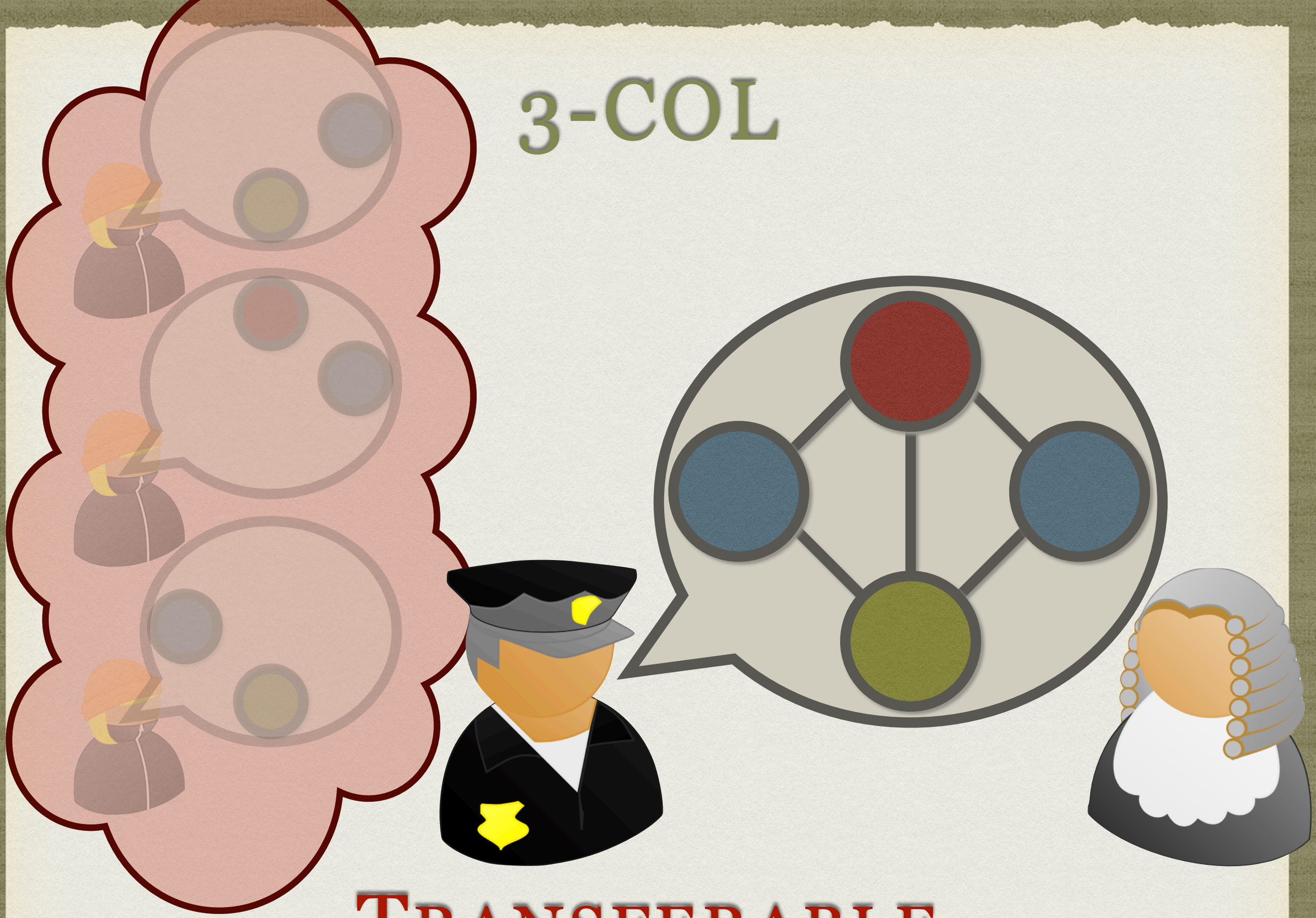
3-COL



3-COL

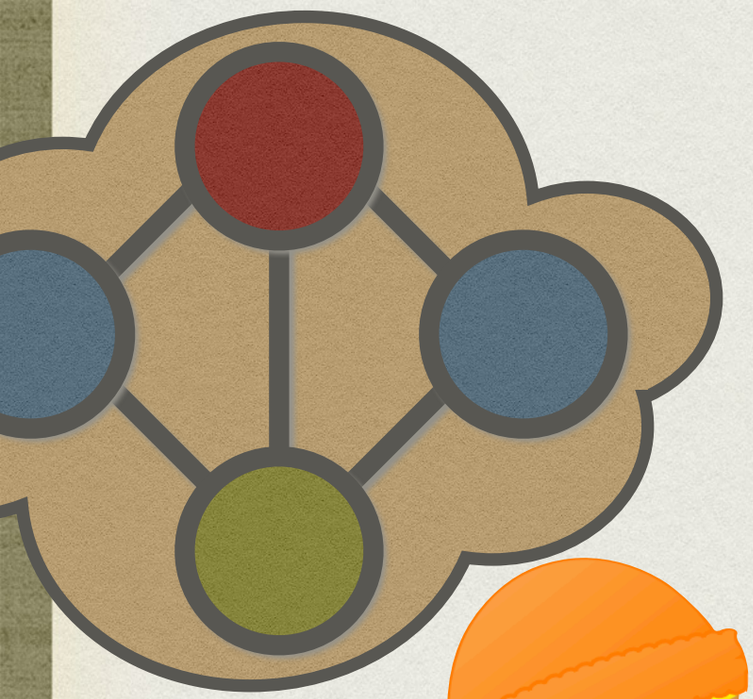


3-COL

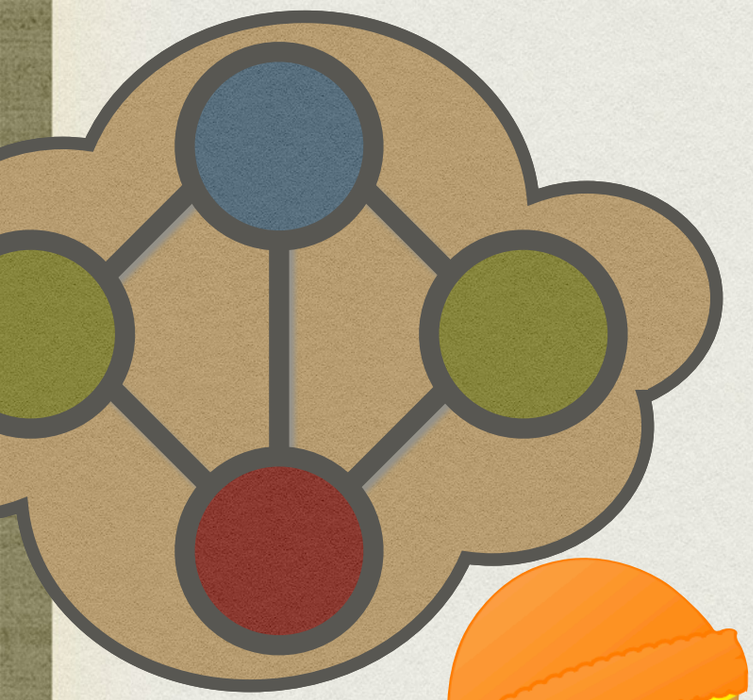


Transferable

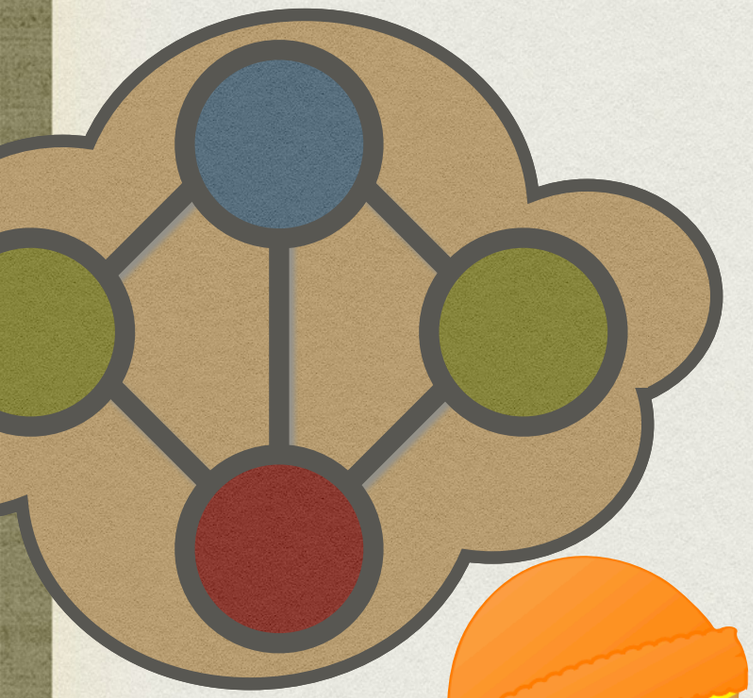
3-COL

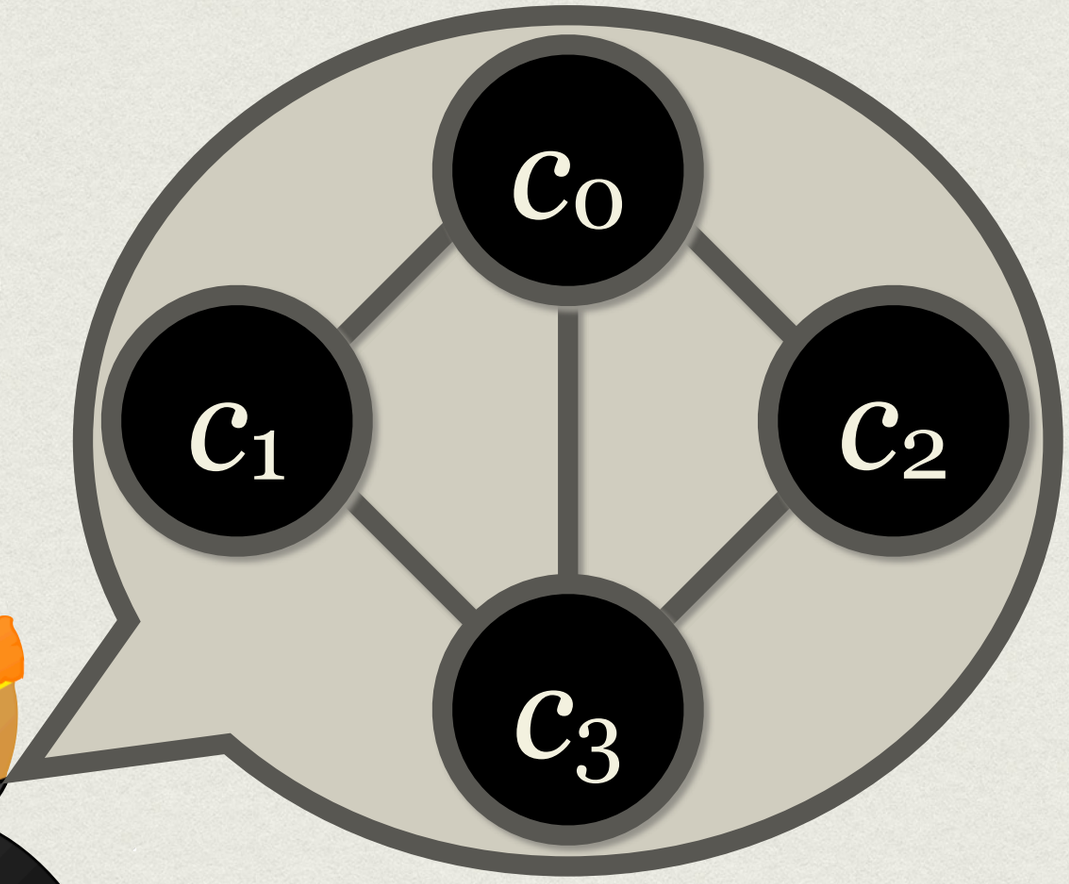


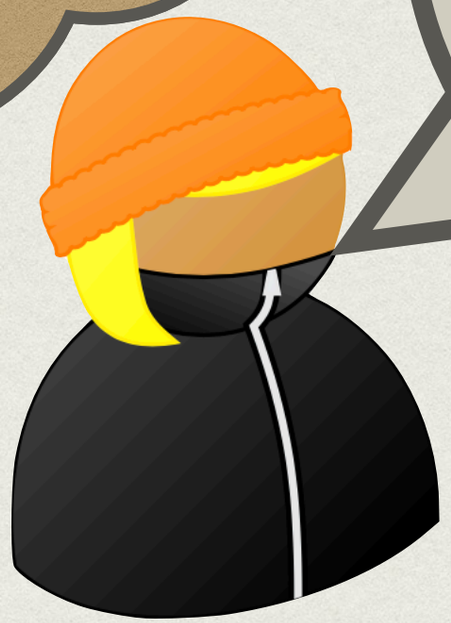
3-COL



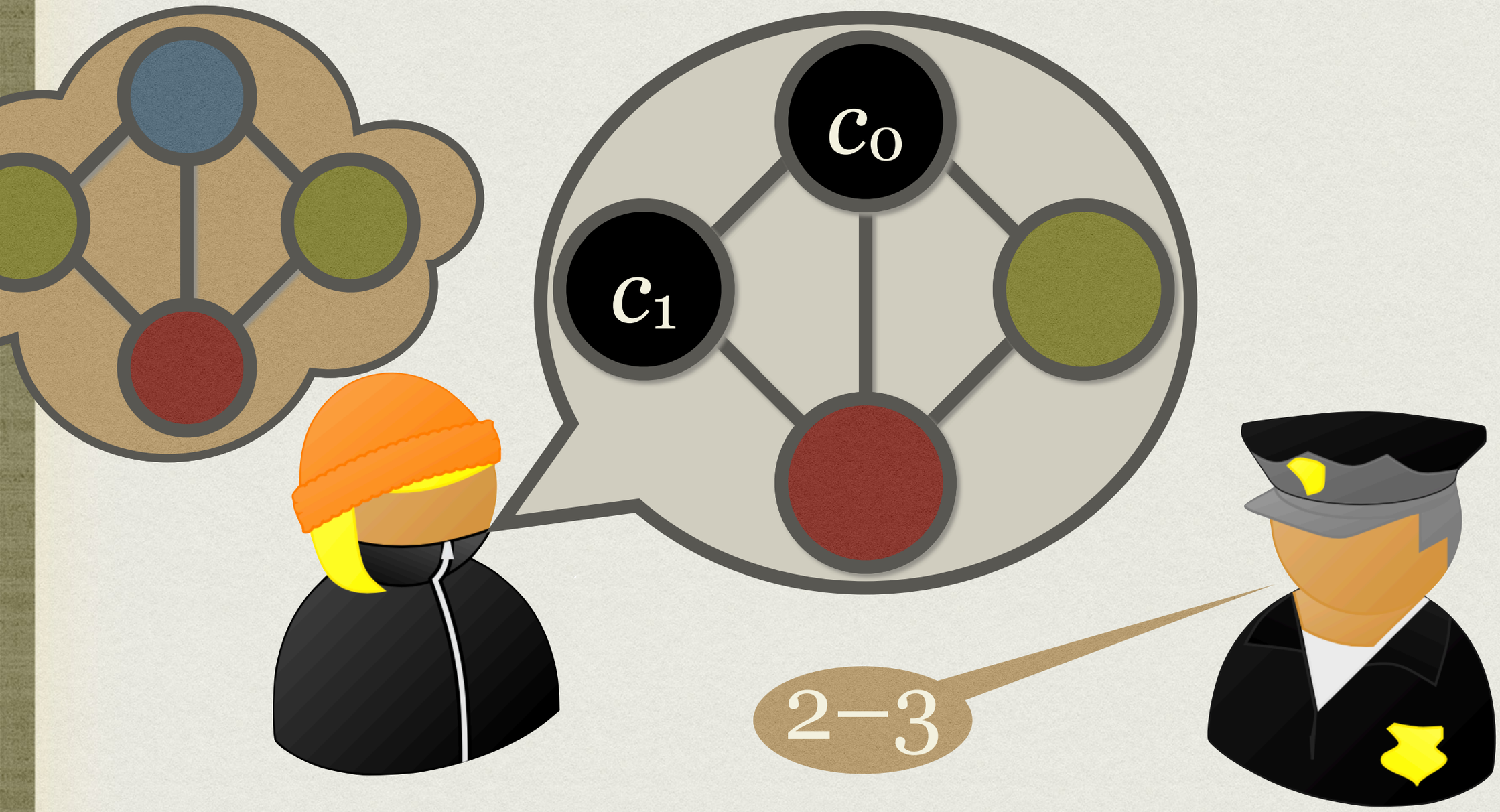
3-COL



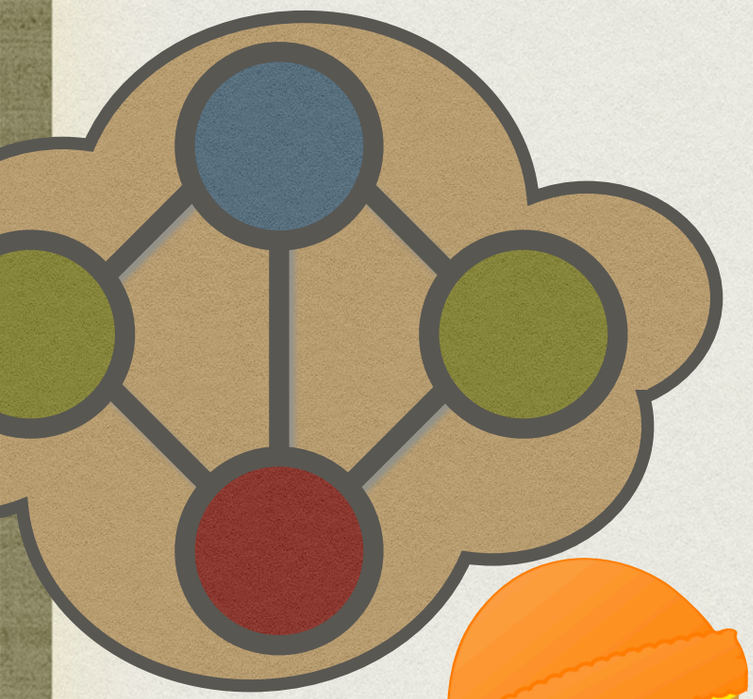




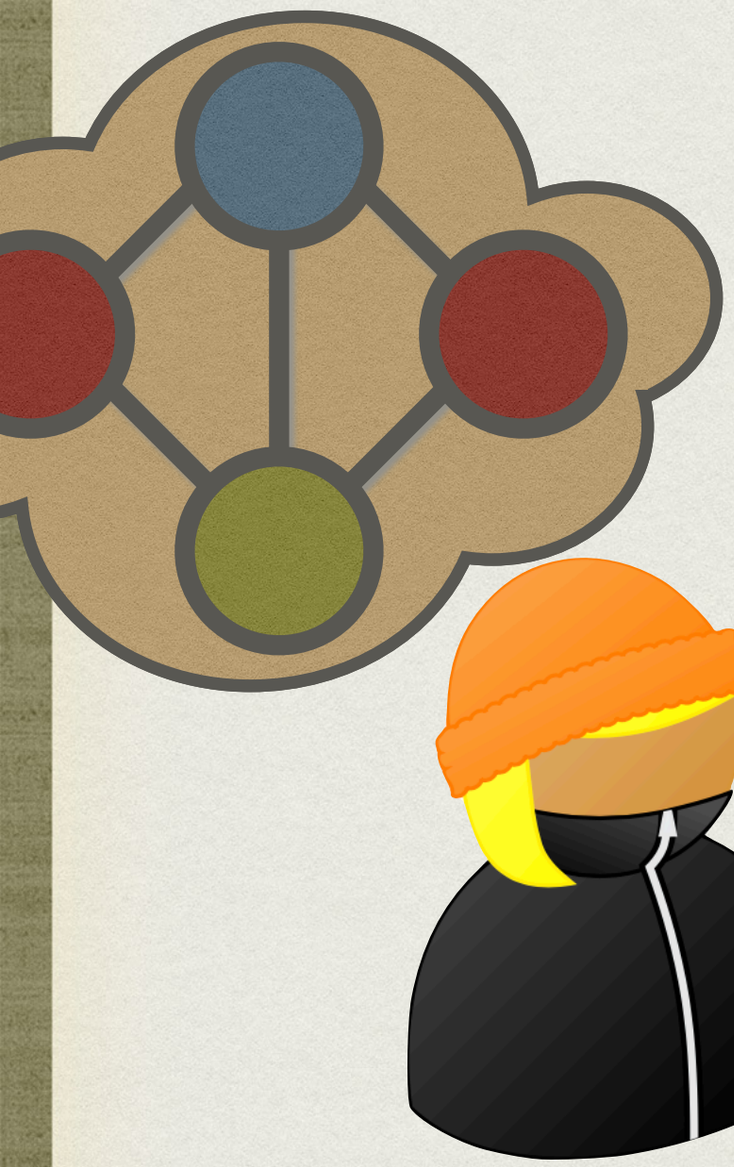
3-COL



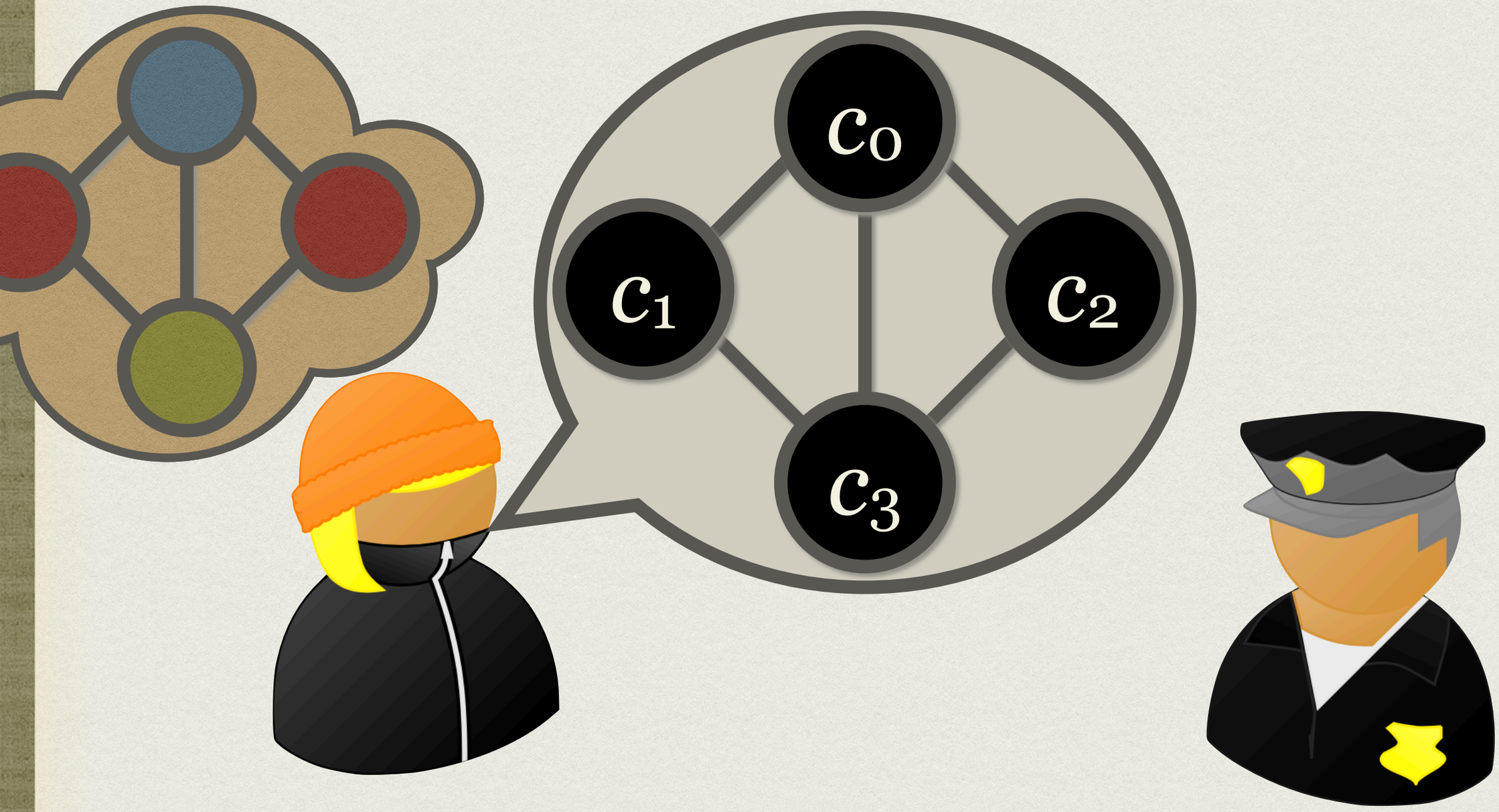
3-COL



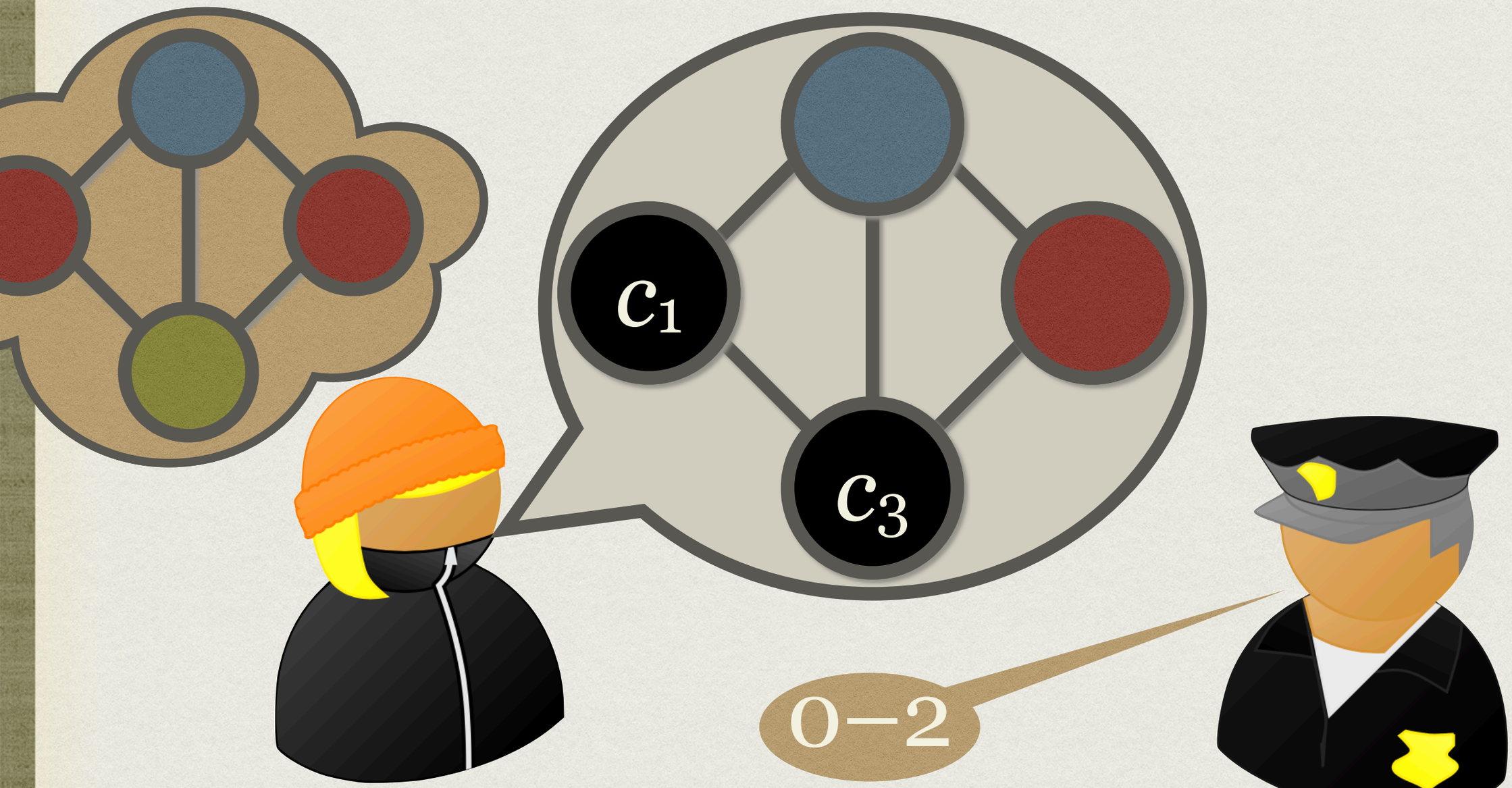
3-COL



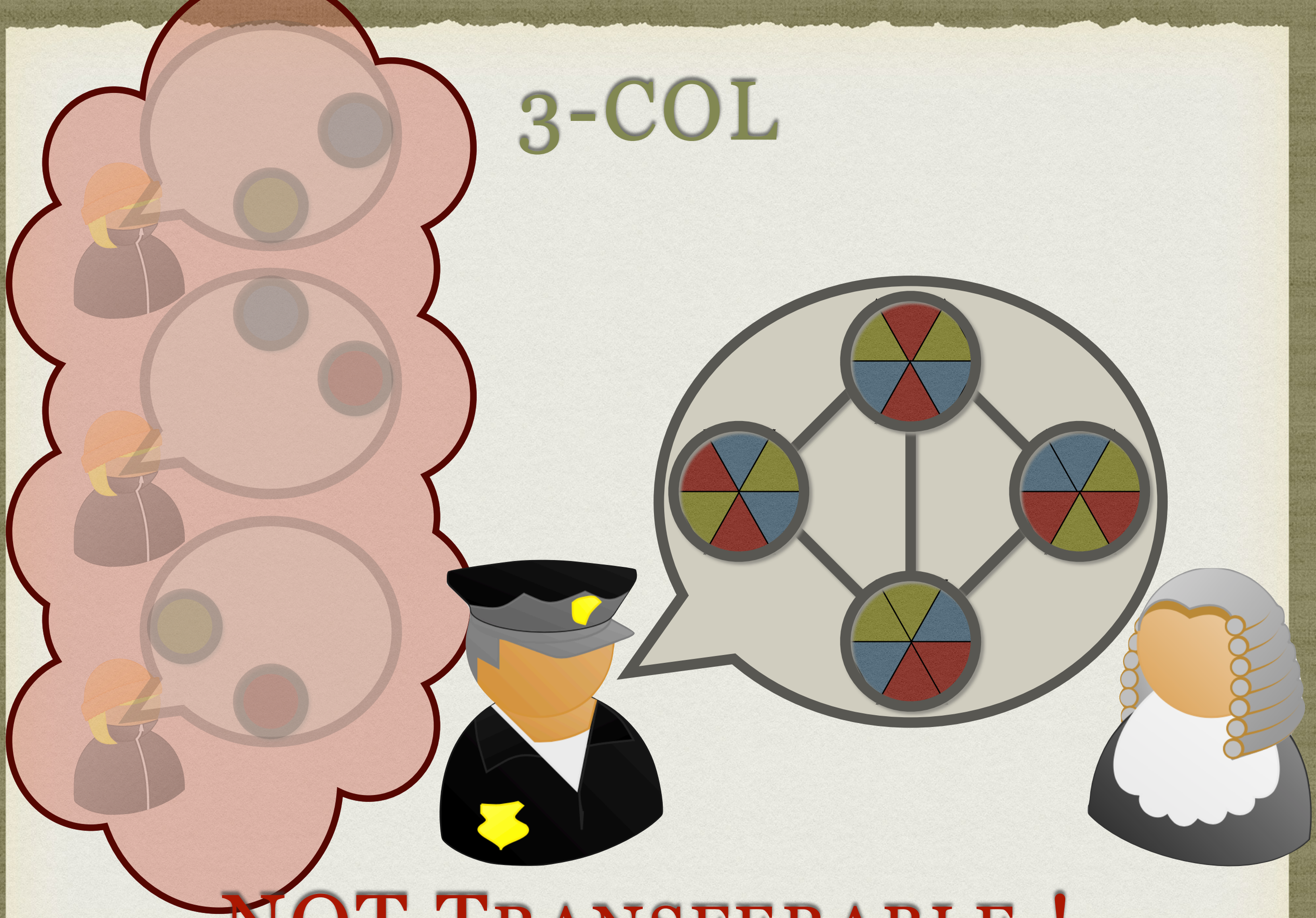
3-COL



3-COL

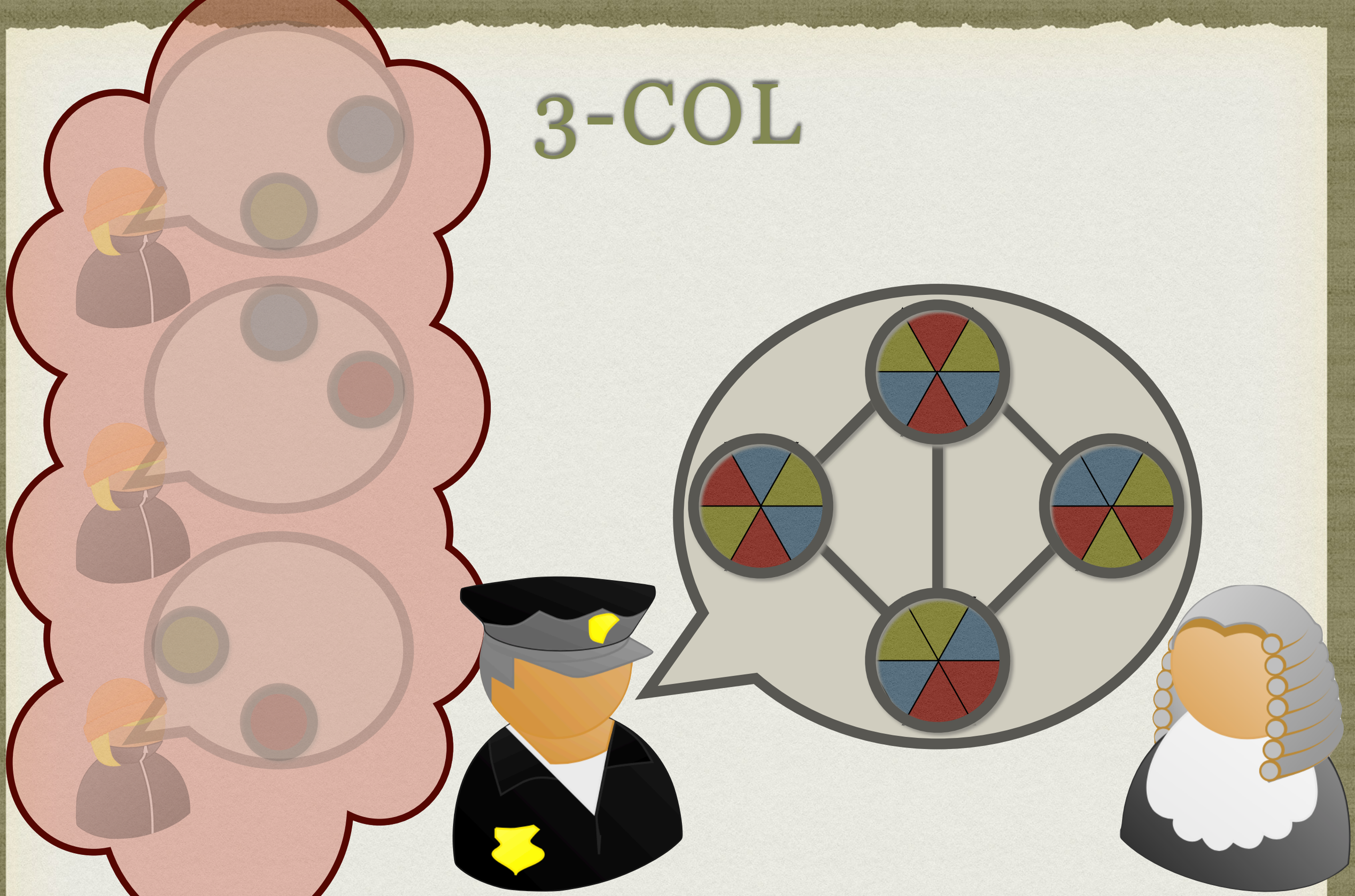


3-COL



NOT TRANSFERABLE !

3-COL



Zero-Knowledge

NON-ZERO-KNOWLEDGE

prover

verifier

judge

NON-ZERO-KNOWLEDGE

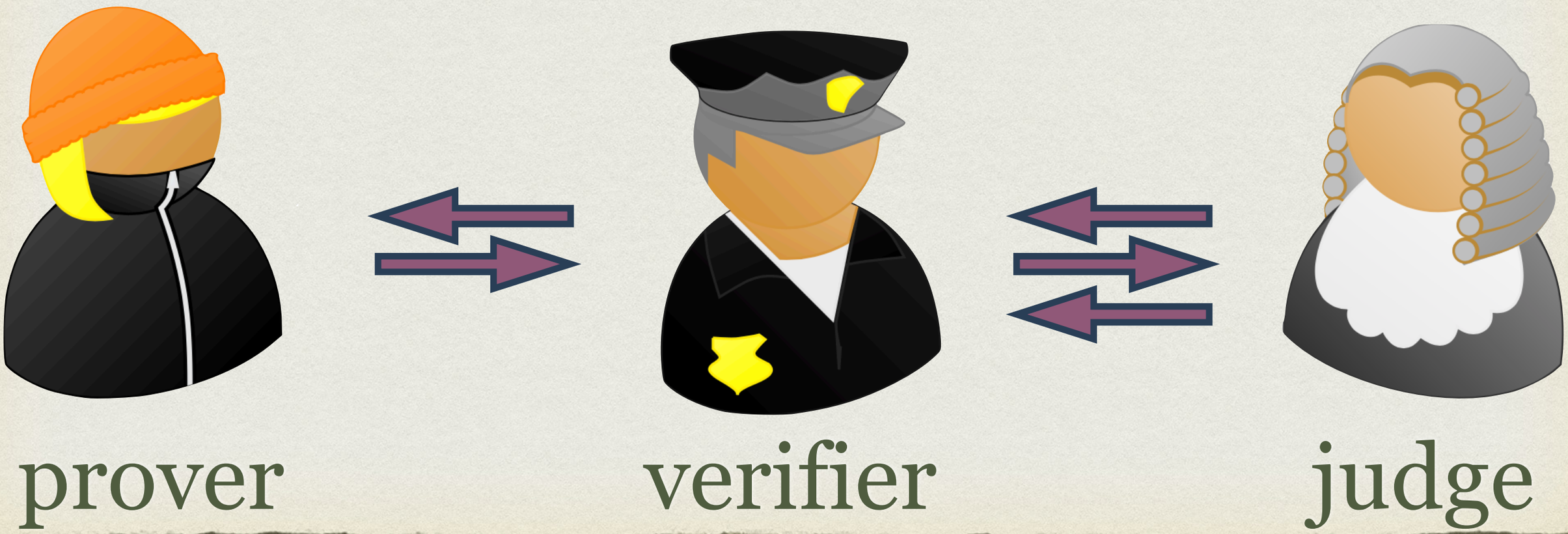
NON-ZERO-KNOWLEDGE

prover verifier judge

NON-ZERO-KNOWLEDGE

NON-ZERO-KNOWLEDGE

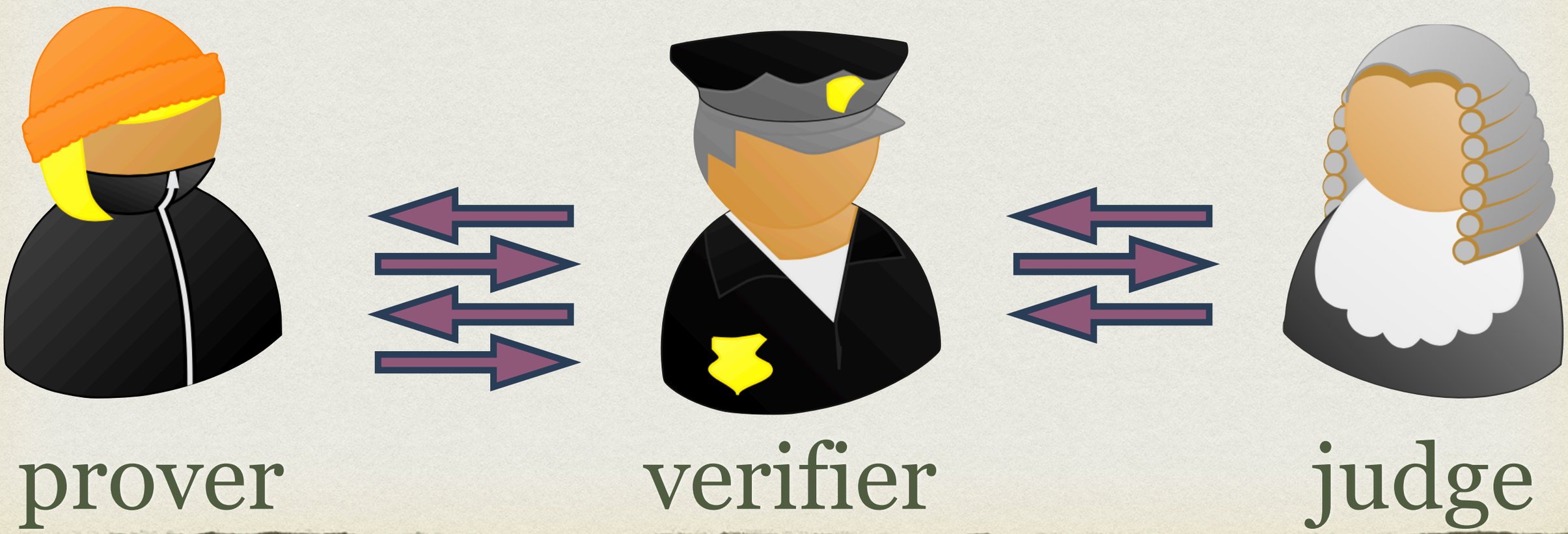
NON-ZERO-KNOWLEDGE



NON-ZERO-KNOWLEDGE

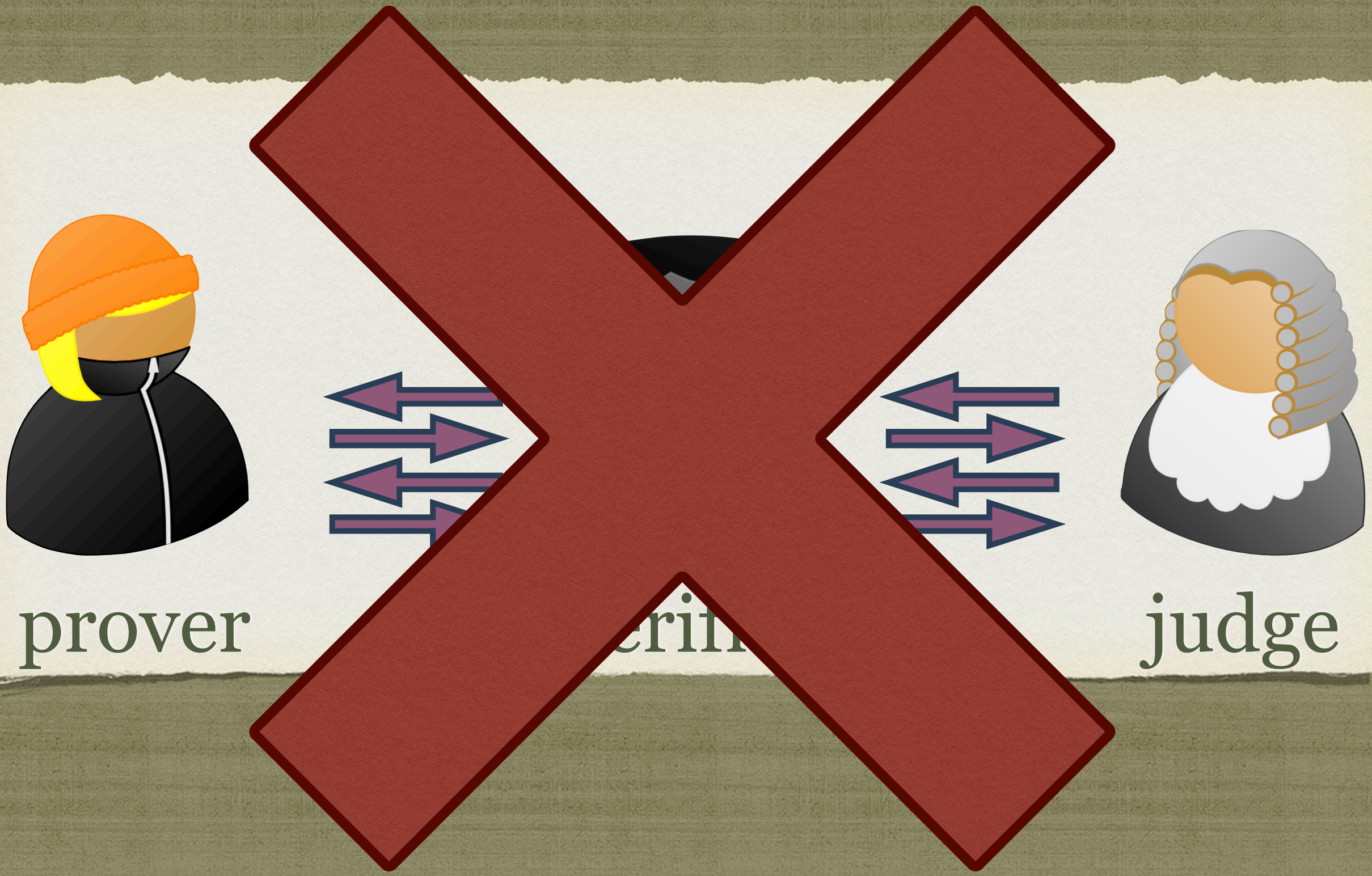
NON-ZERO-KNOWLEDGE

NON-ZERO-KNOWLEDGE



NON-ZERO-KNOWLEDGE

NON-ZERO-KNOWLEDGE



ZERO-KNOWLEDGE

prover

verifier

judge

ZERO-KNOWLEDGE

prover

verifier

aux input

judge

ZERO-KNOWLEDGE

prover

verifier

aux input

judge

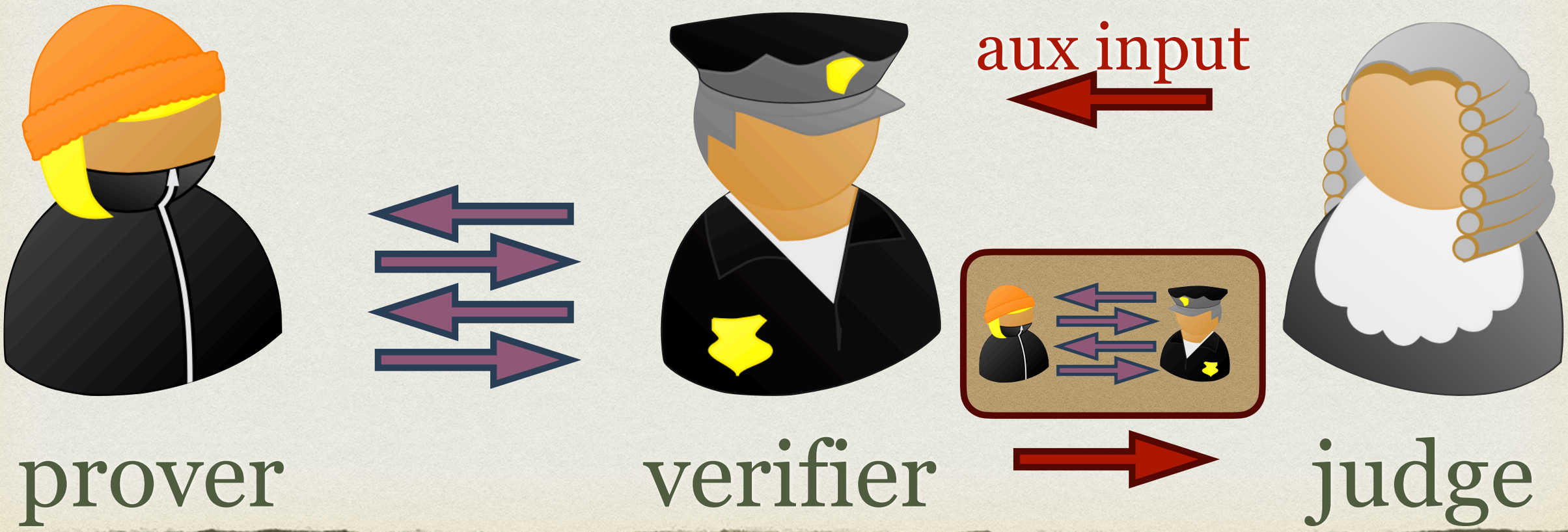
ZERO-KNOWLEDGE

prover verifier judge

ZERO-KNOWLEDGE

prover verifier judge

ZERO-KNOWLEDGE



ZERO-KNOWLEDGE

simulator

judge

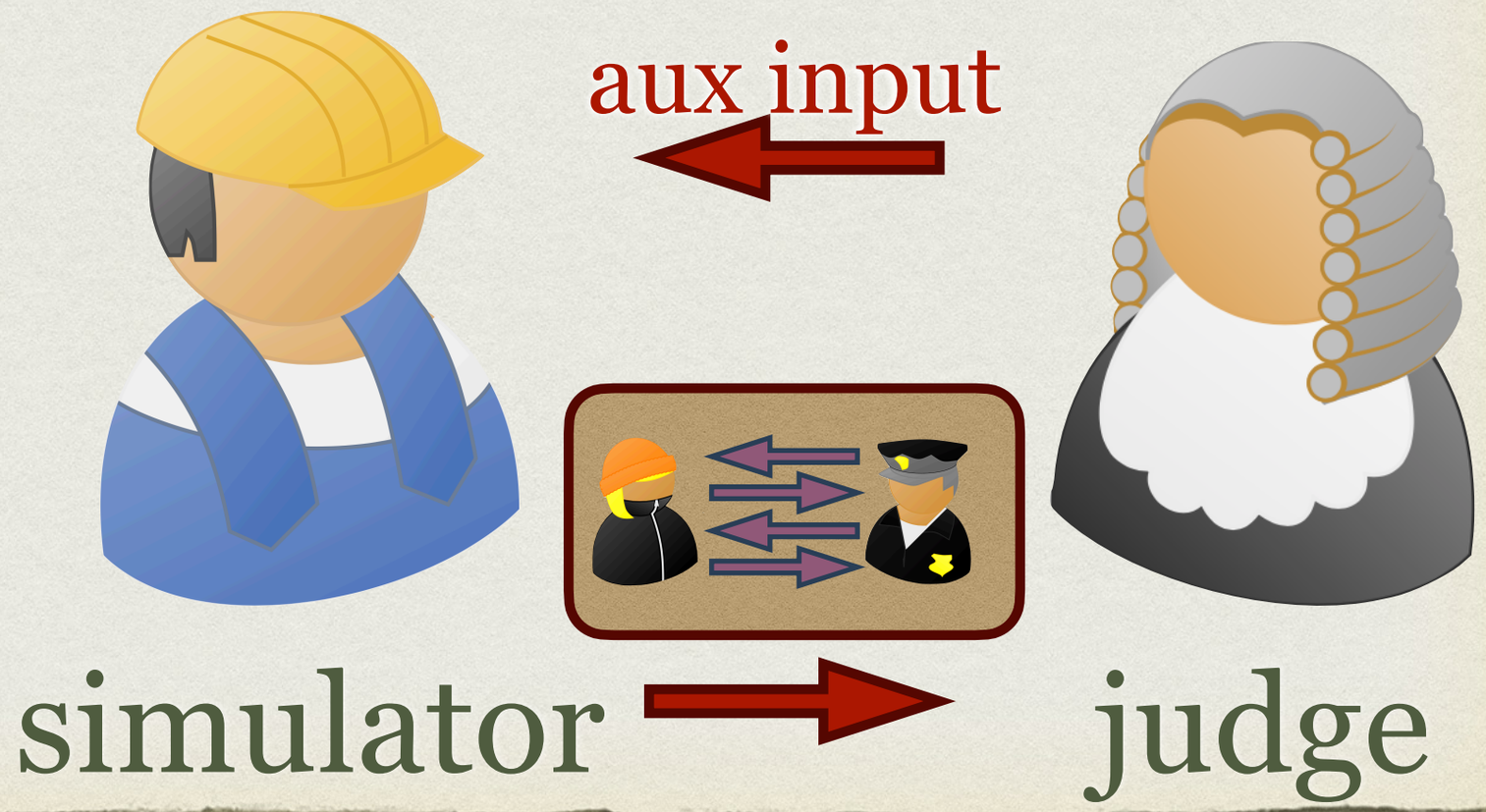
ZERO-KNOWLEDGE

aux input

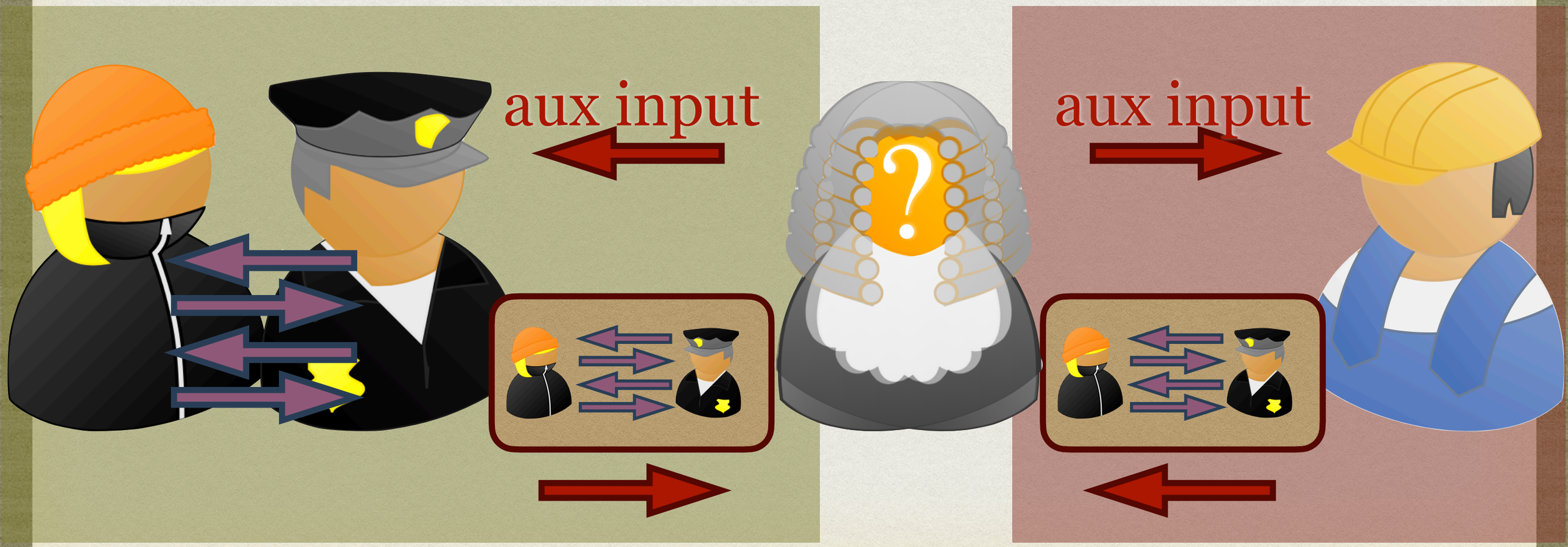
simulator

judge

ZERO-KNOWLEDGE



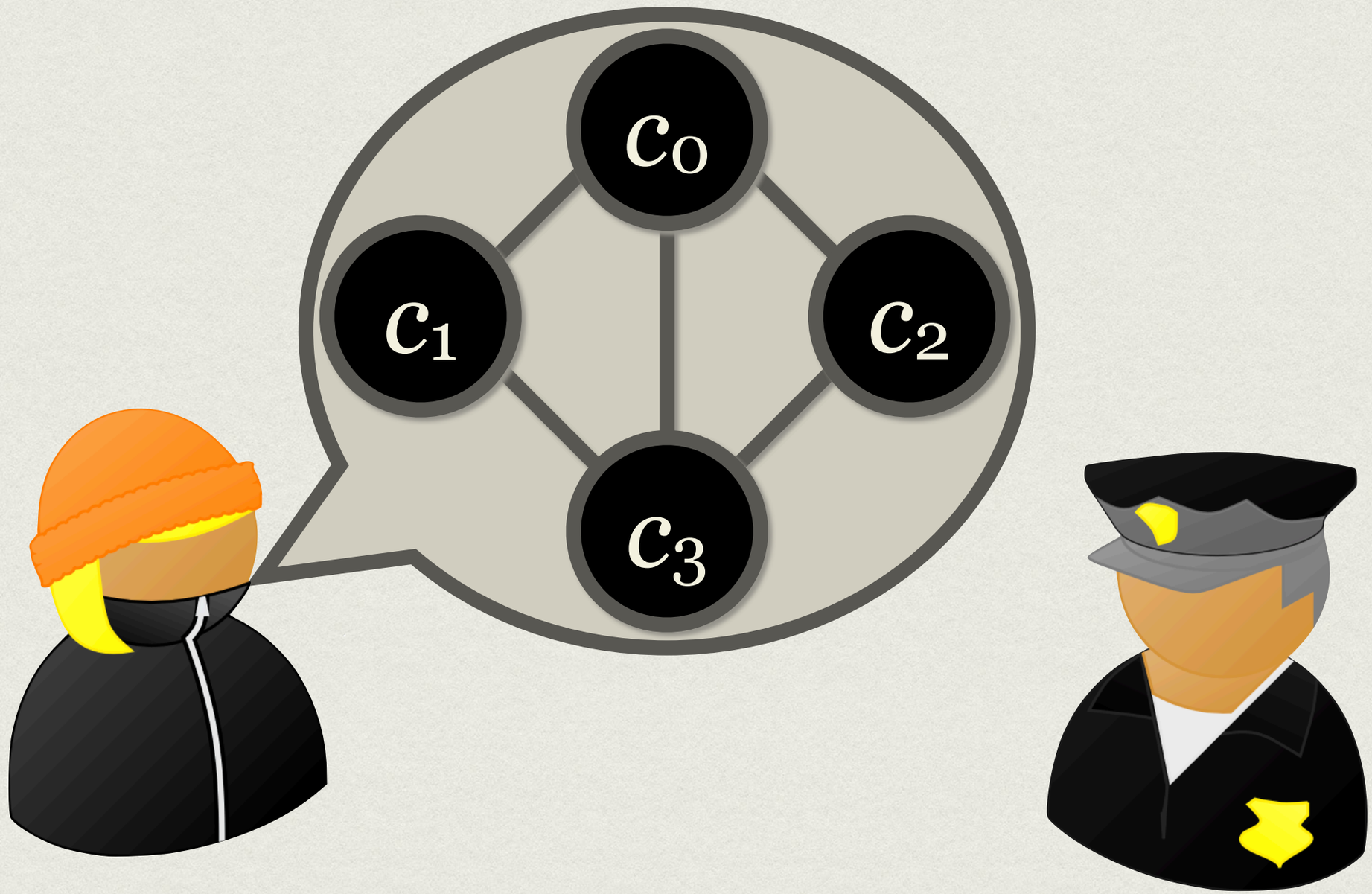
ZERO-KNOWLEDGE



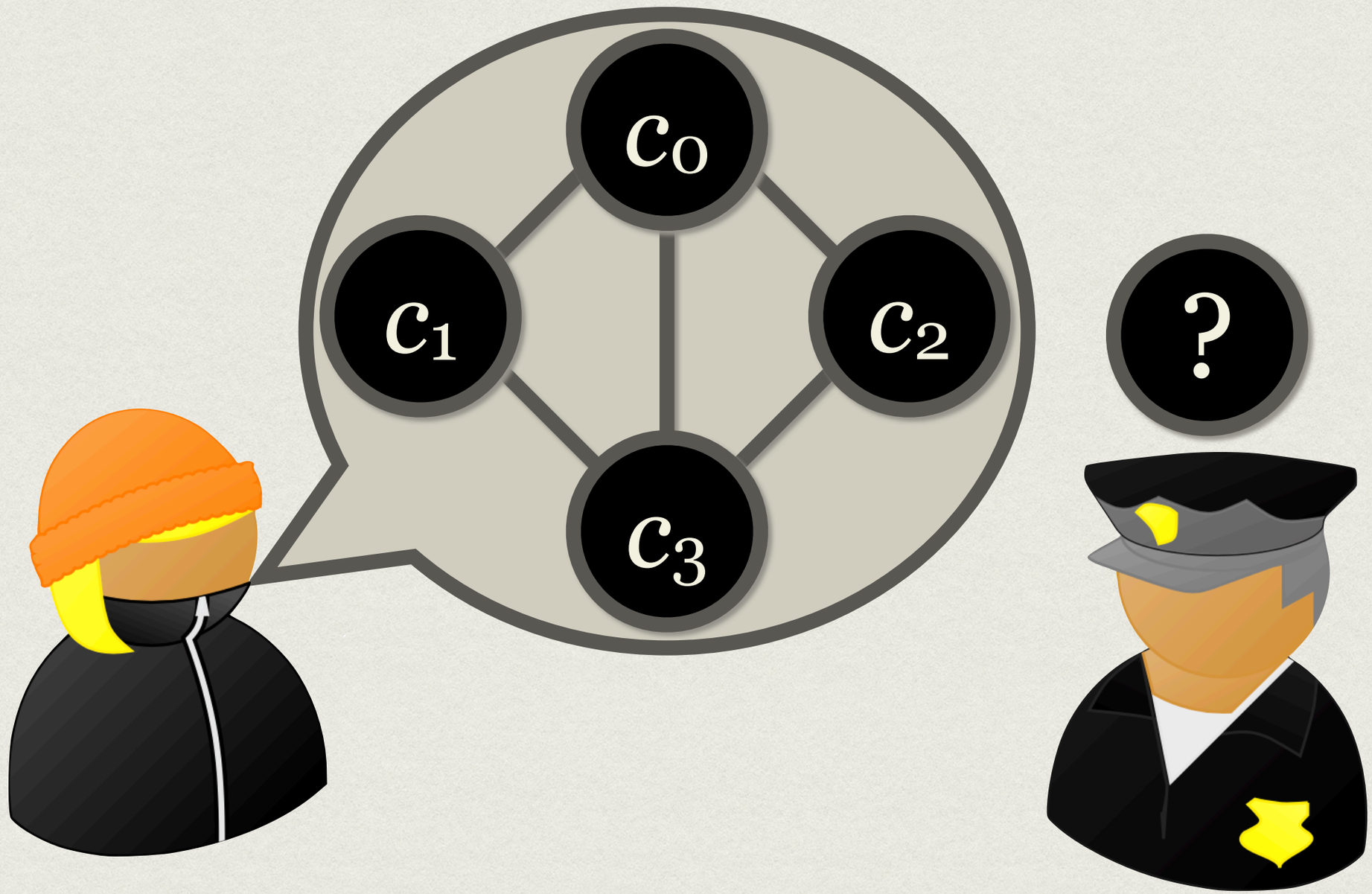
$\forall$ poly, $\exists$ poly, $\forall w \in L, \forall z,$

$[($ $:$ $)(w, z)] \approx [($ $)(w, z)]$

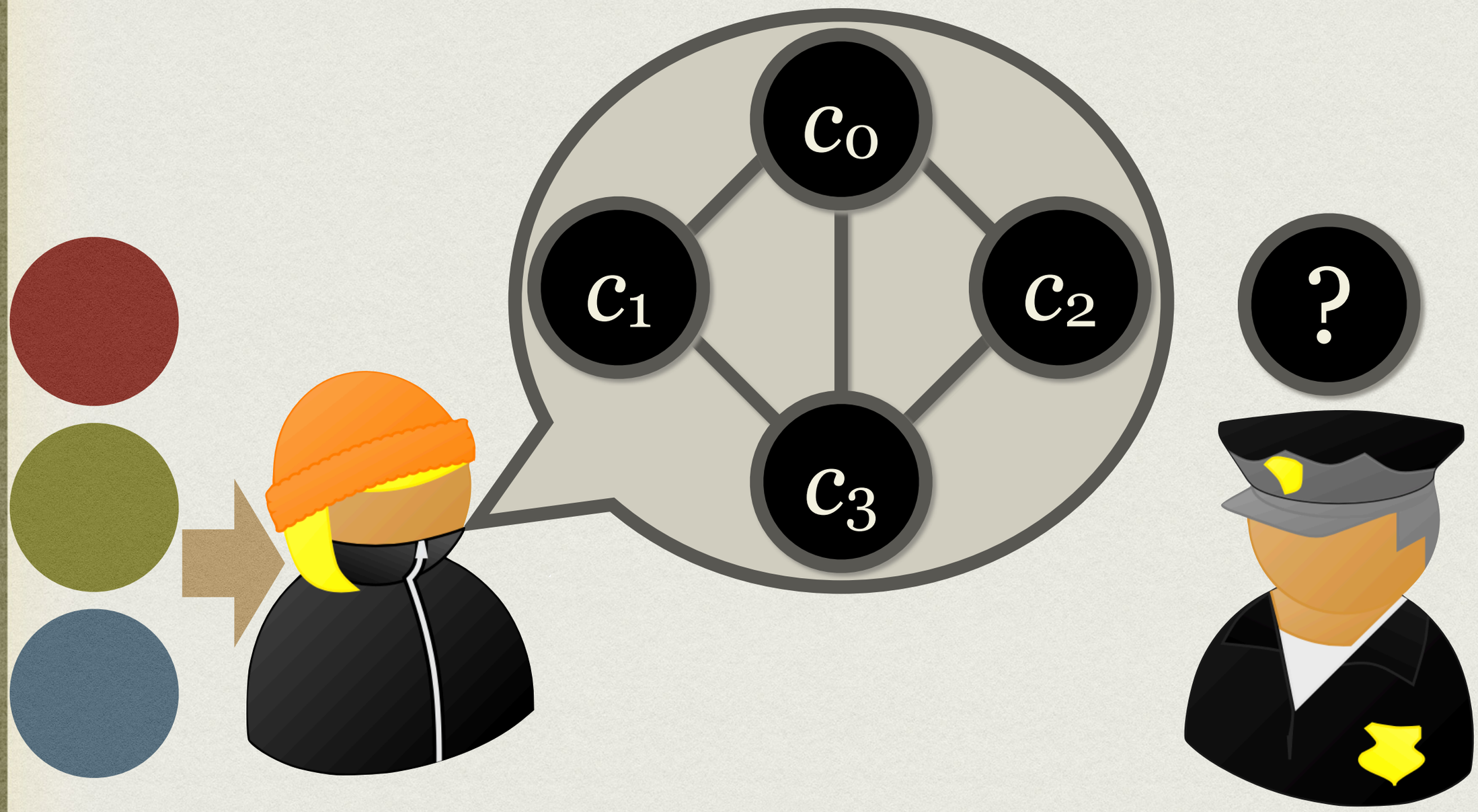
COMMITMENTS ??



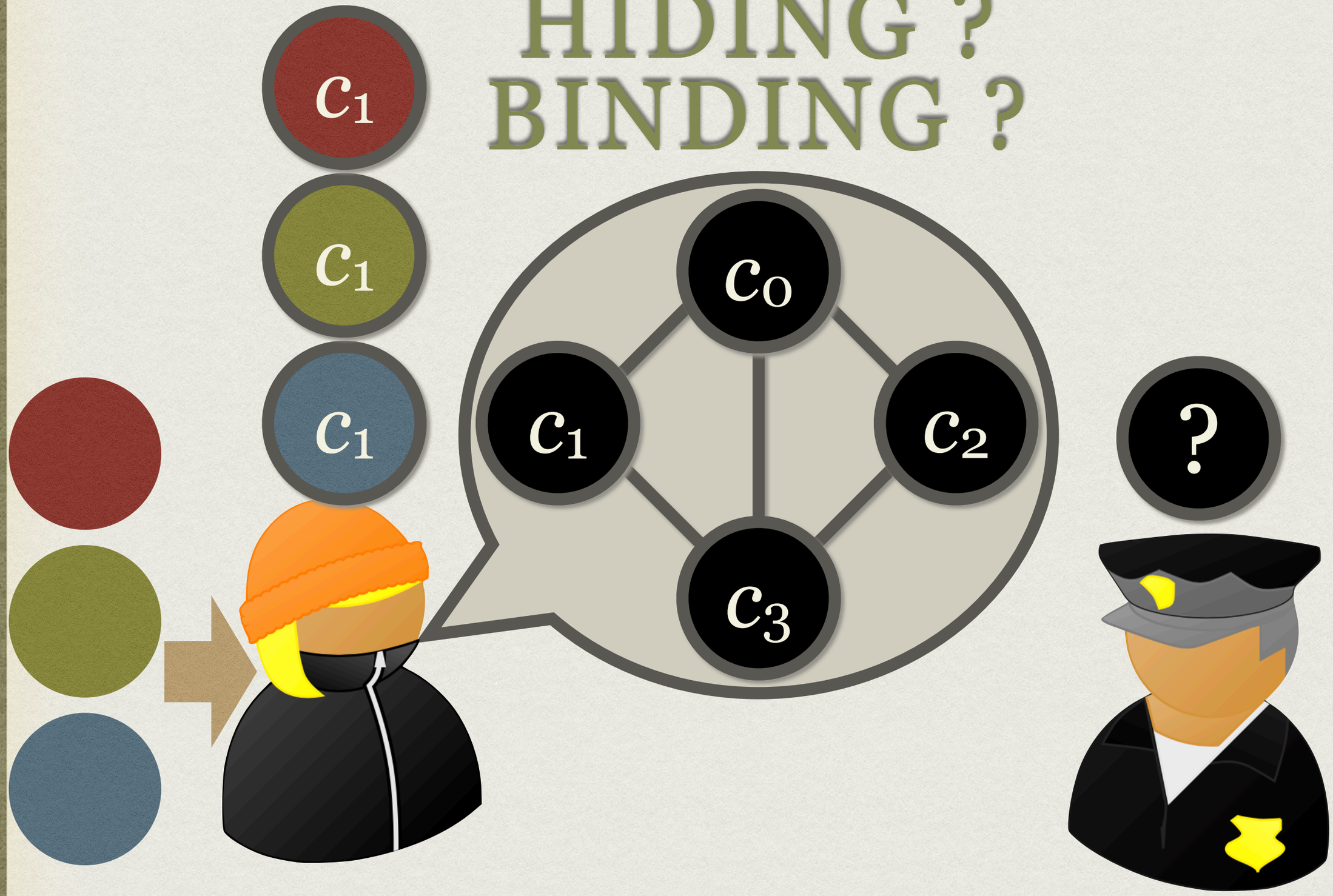
COMMITMENTS ??
HIDING ?



COMMITMENTS ??
HIDING ?
BINDING ?

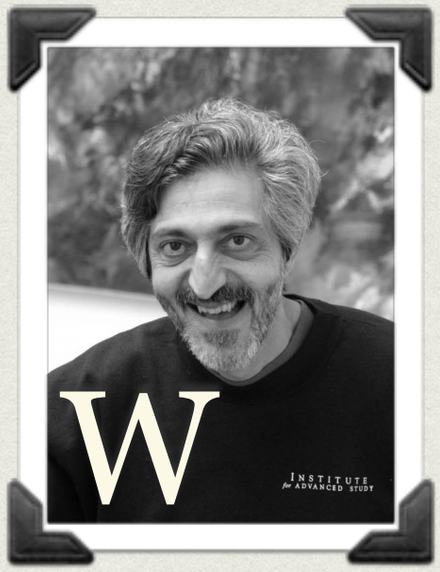


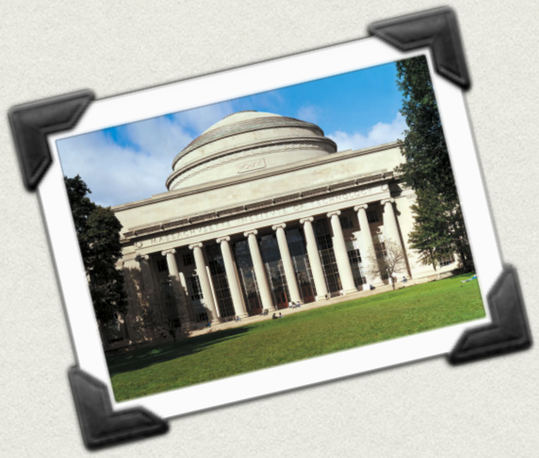
COMMITMENTS ??
HIDING ?
BINDING ?



MULTI-PROVERS

INTERACTIVE PROOFS

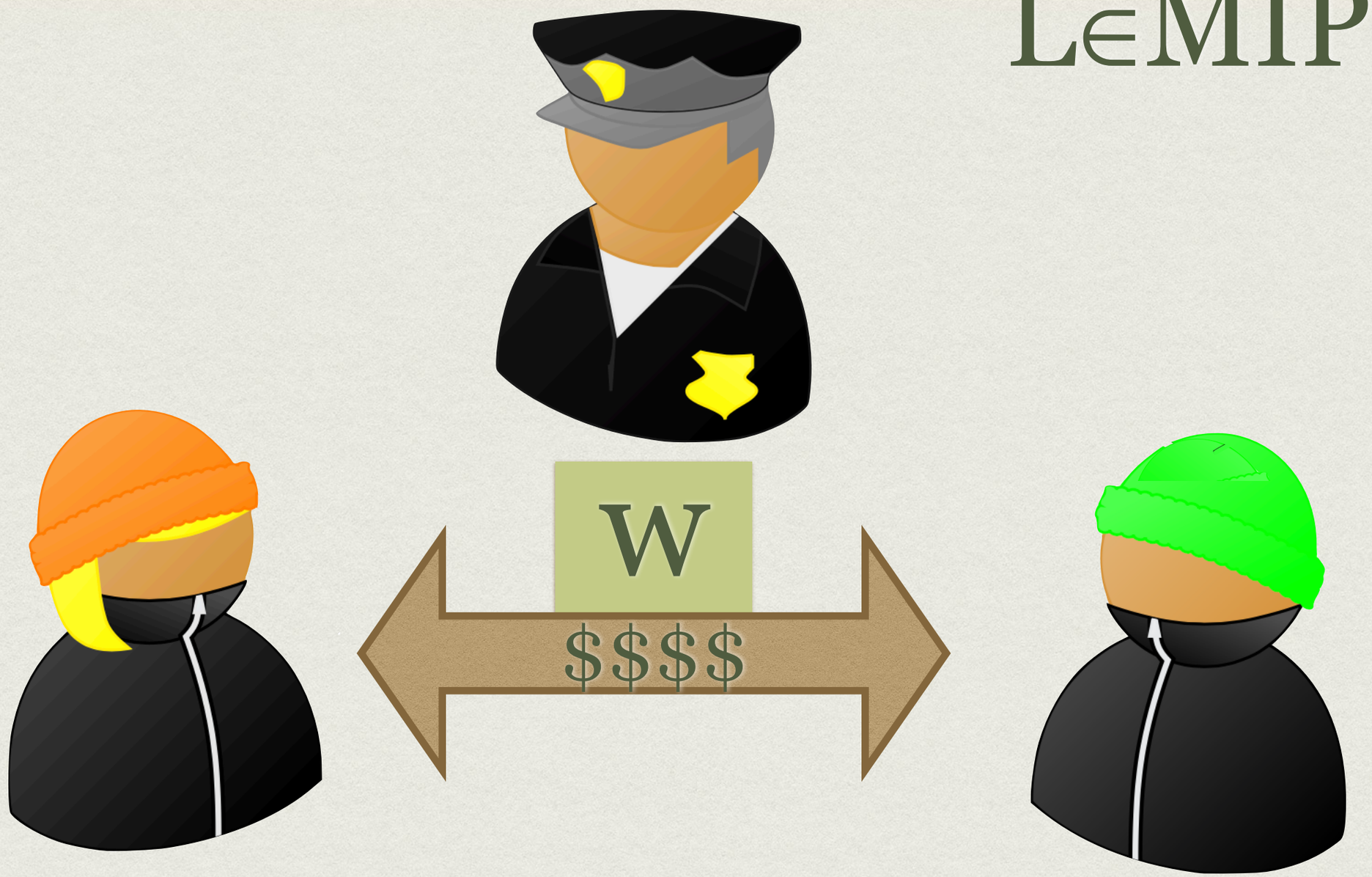




'88

BGKW88

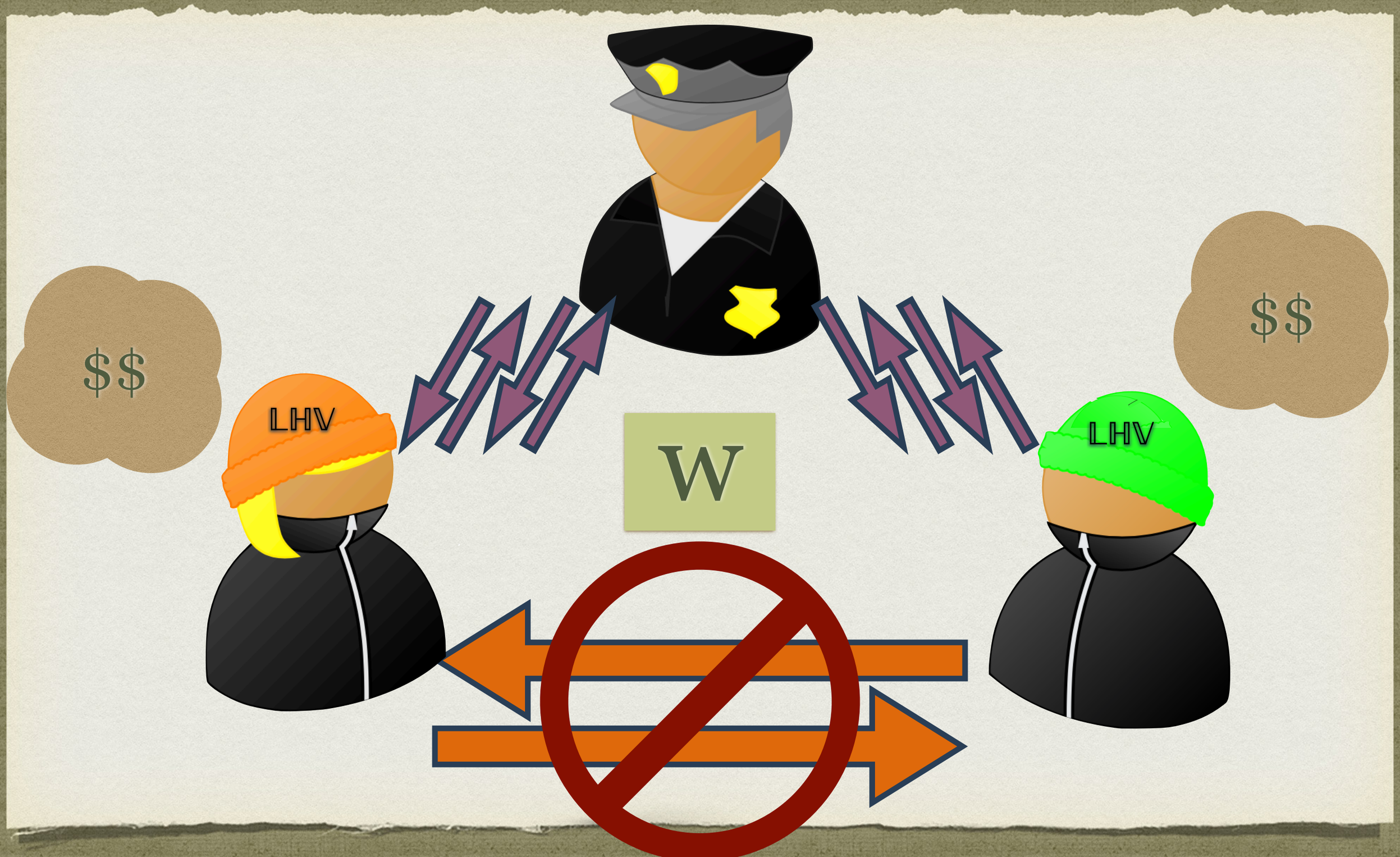
BGKW88



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

poly

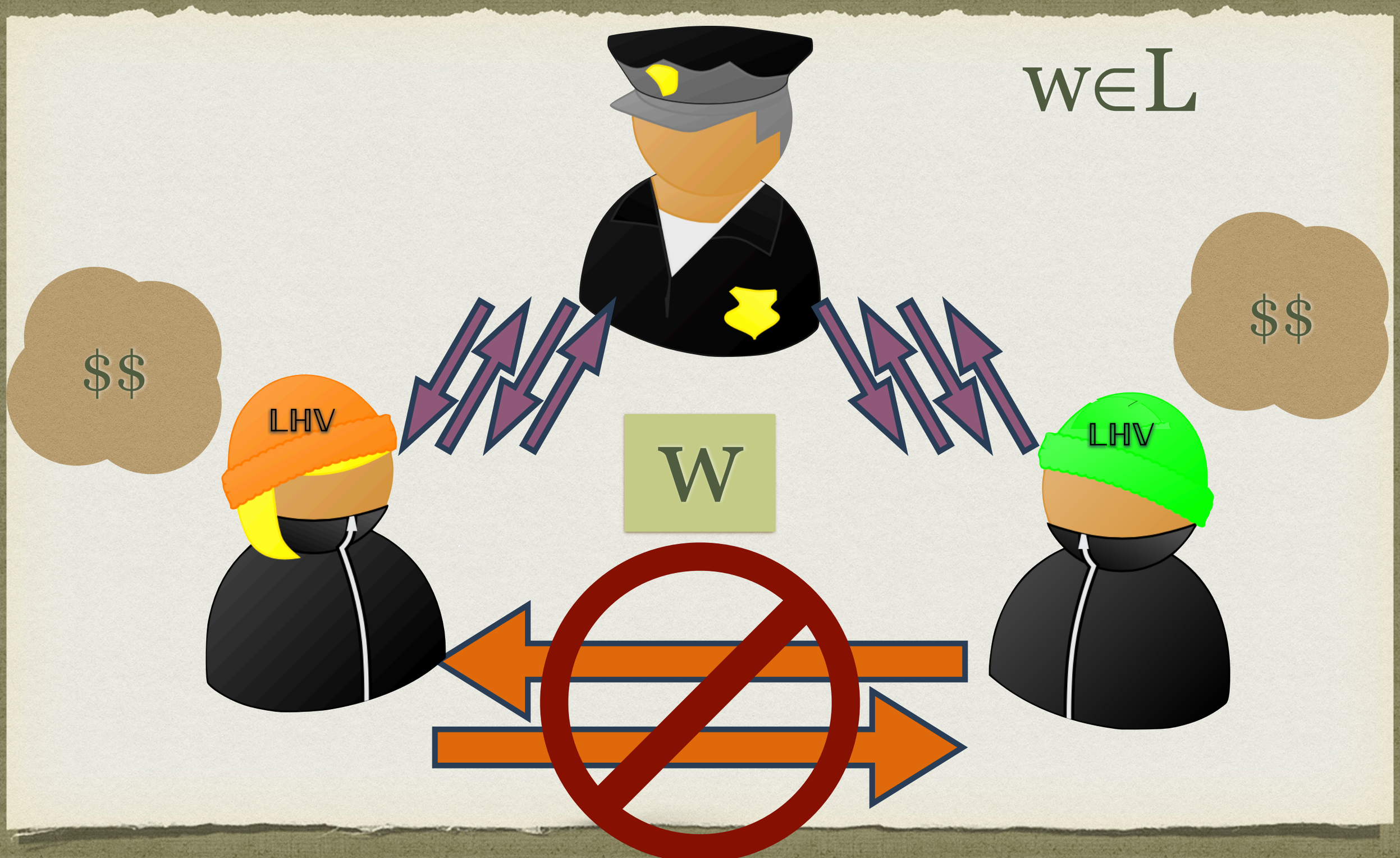
$$\textbf{Prob}[(\text{\textcircled{1}}:\text{\textcircled{2}}:\text{\textcircled{3}})(w) \text{ accepts }] \geq 1 - \epsilon$$



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

poly

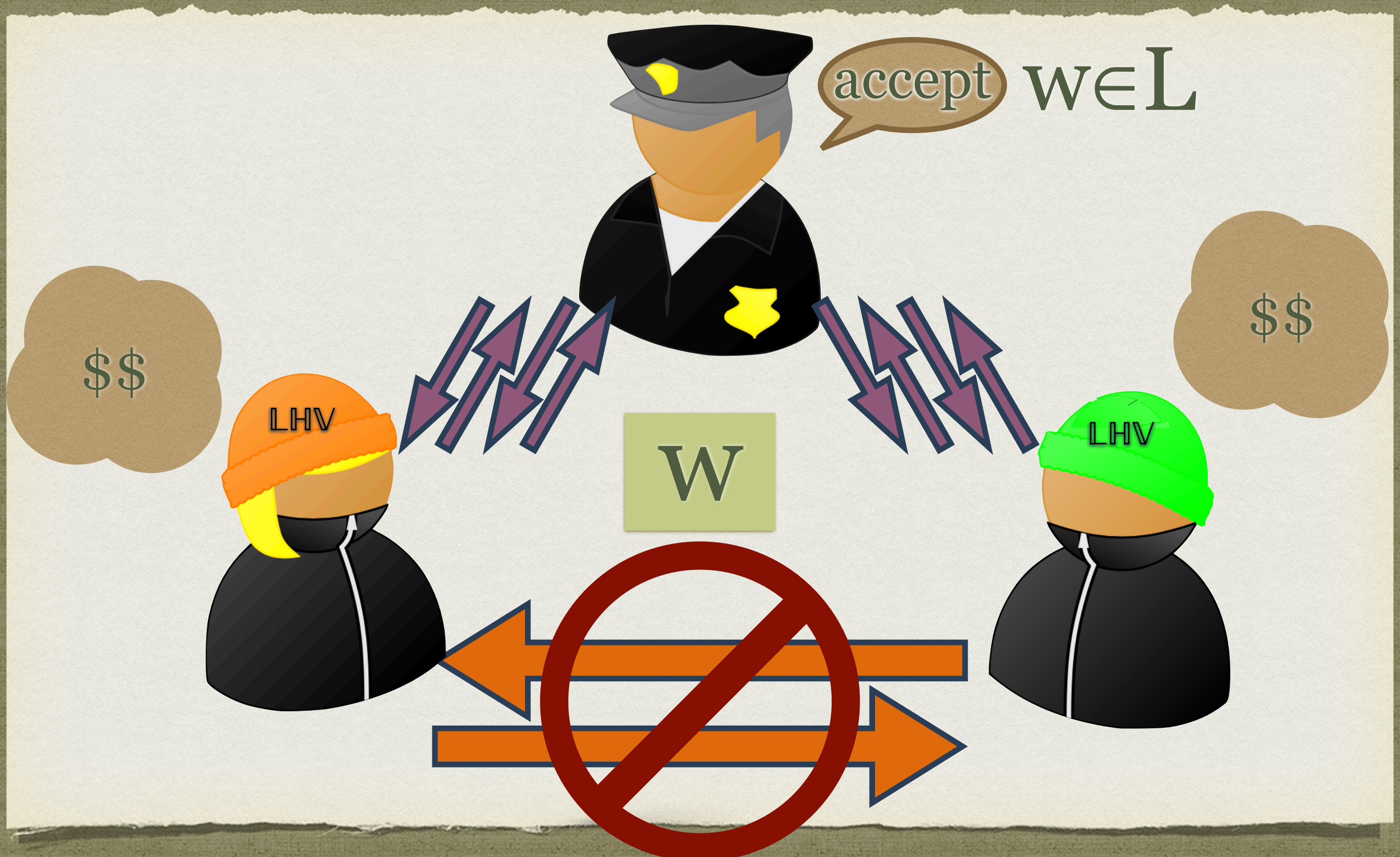
$$\textbf{Prob}[(\text{\textcircled{\raisebox{0.5ex}{\scriptsize\textbf{:}}}}:\text{\textcircled{\raisebox{0.5ex}{\scriptsize\textbf{:}}}}:\text{\textcircled{\raisebox{0.5ex}{\scriptsize\textbf{:}}}})(w) \text{ accepts }] \geq 1 - \epsilon$$



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

poly

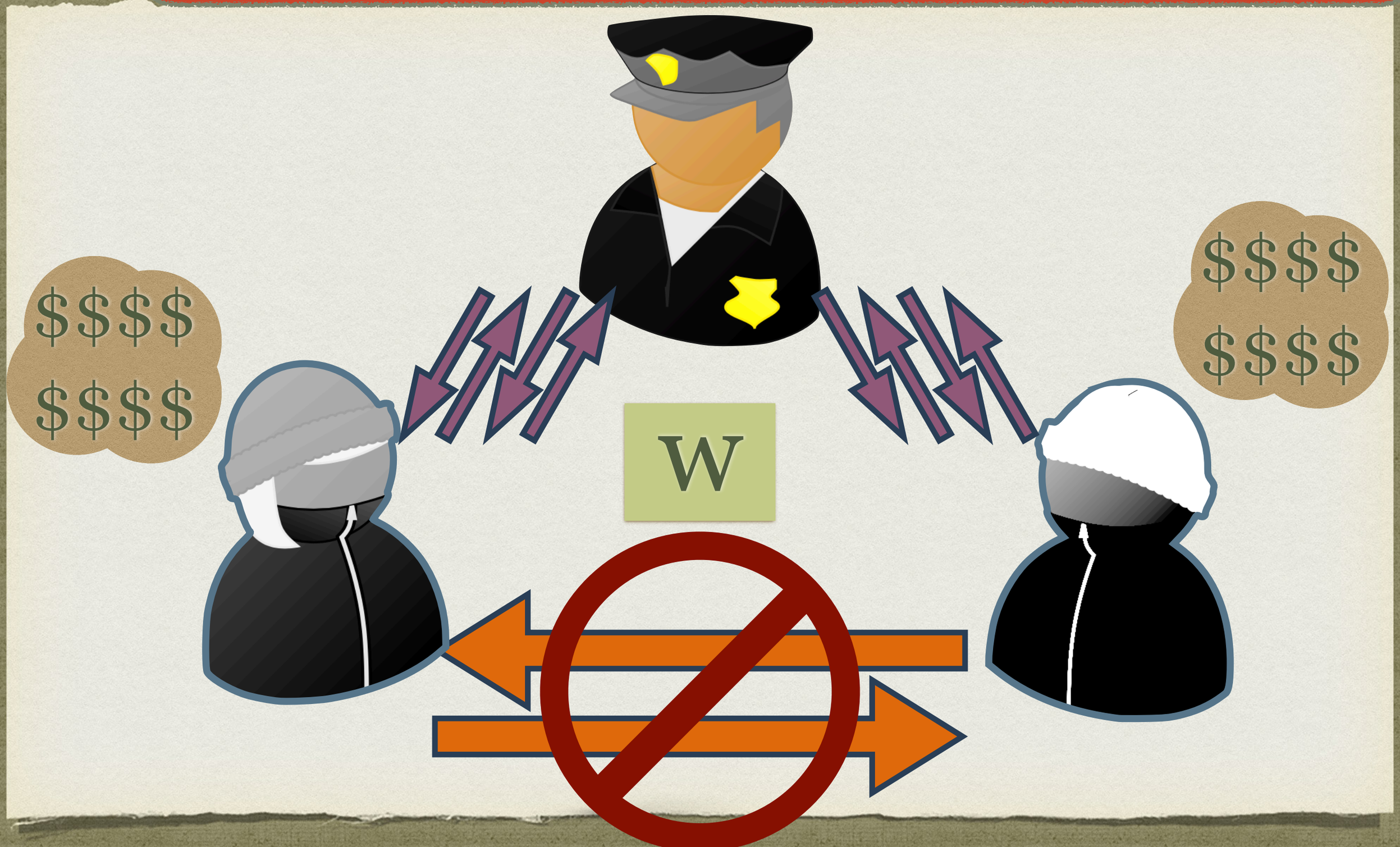
Prob[(: :)(w) accepts] $\geq 1 - \epsilon$



$\exists$ poly

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

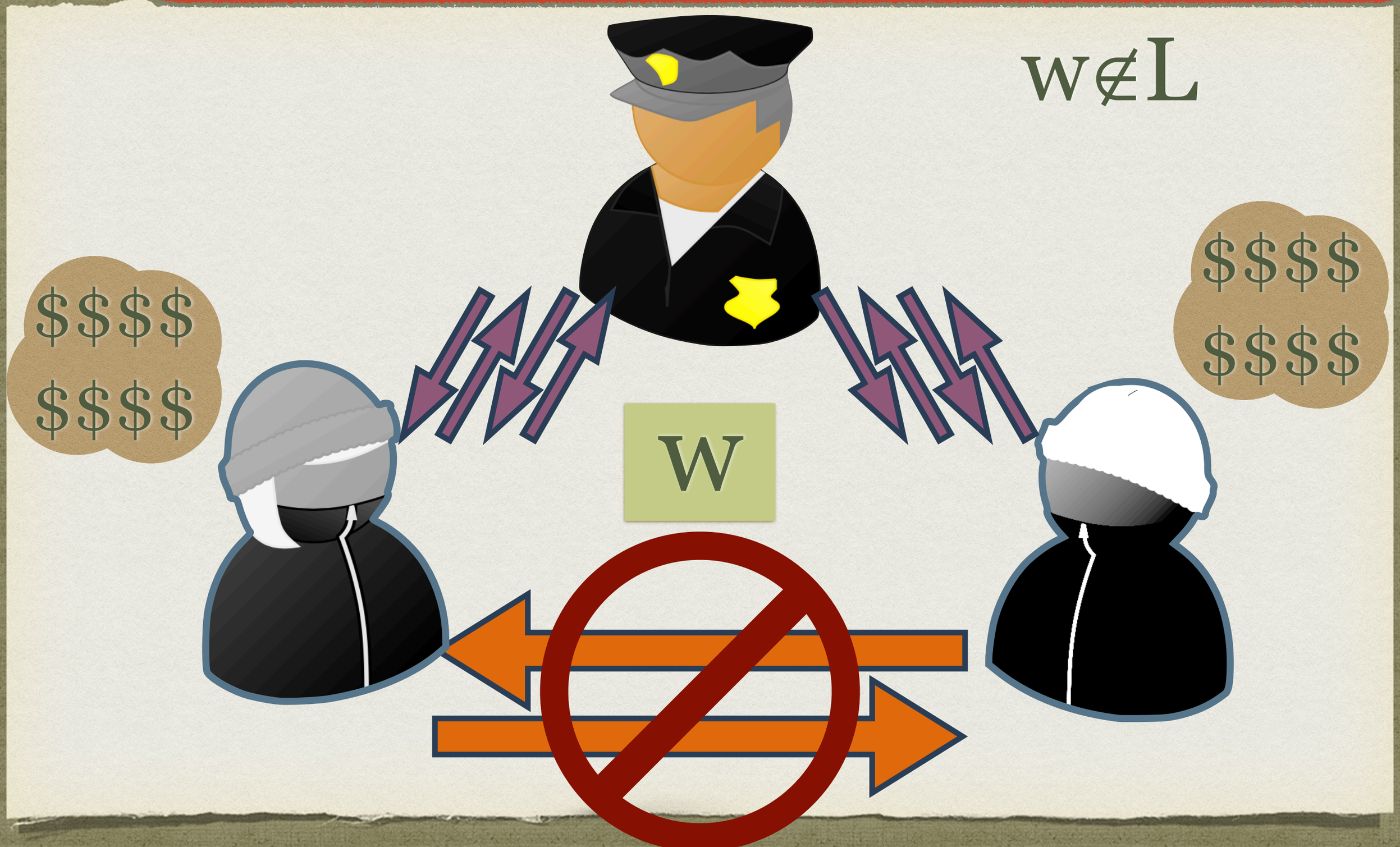
Prob[(: :)(w) accepts] $\leq \epsilon$



$\exists$ poly

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

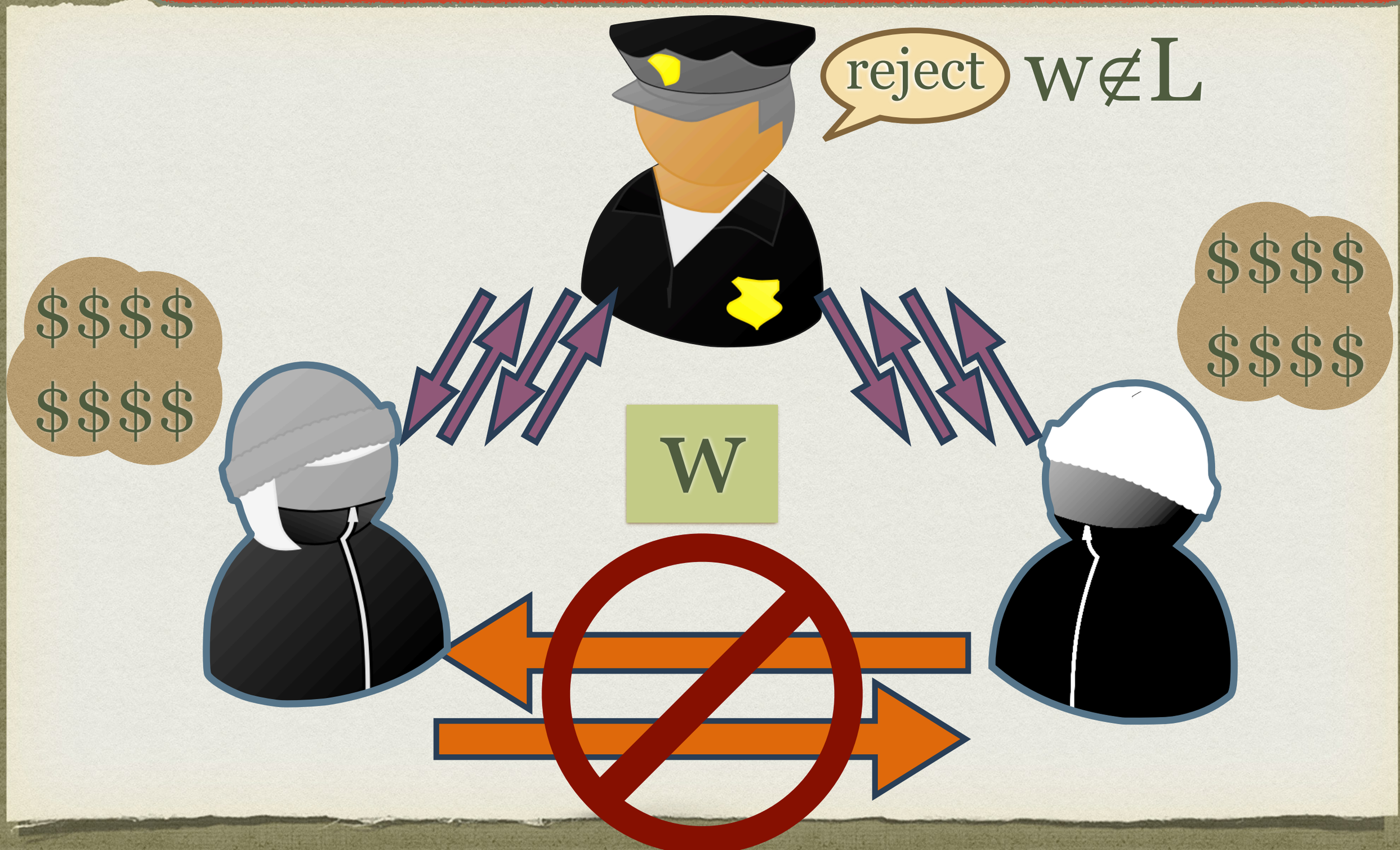
Prob[(: :)(w) accepts] $\leq \epsilon$



$\exists$ poly

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

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



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

poly poly

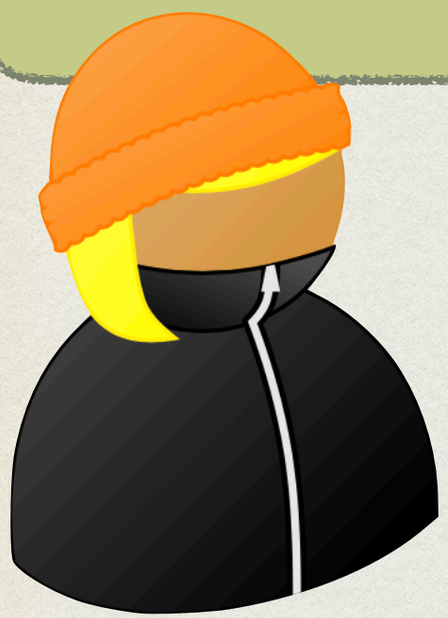
$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

ZERO-KNOWLEDGE

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

poly poly

$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$



provers

ZERO-KNOWLEDGE

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

poly poly

$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

verifier

provers

ZERO-KNOWLEDGE

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

poly poly

$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

verifier

judge

provers

ZERO-KNOWLEDGE

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

poly poly

$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

provers

verifier

aux input

judge

ZERO-KNOWLEDGE

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

poly poly

$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

aux input

provers

verifier

judge

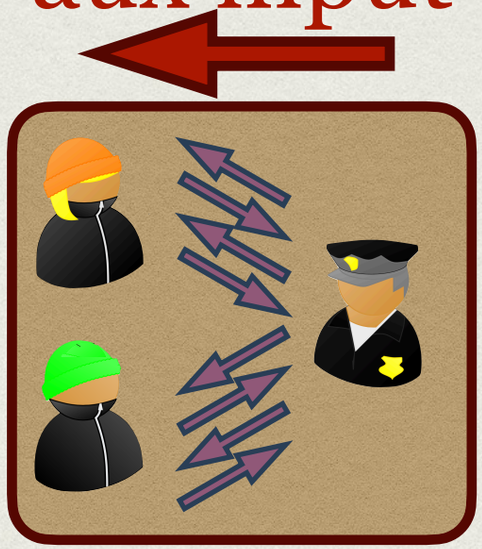
ZERO-KNOWLEDGE

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

poly poly

$[($ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

aux input



provers

verifier

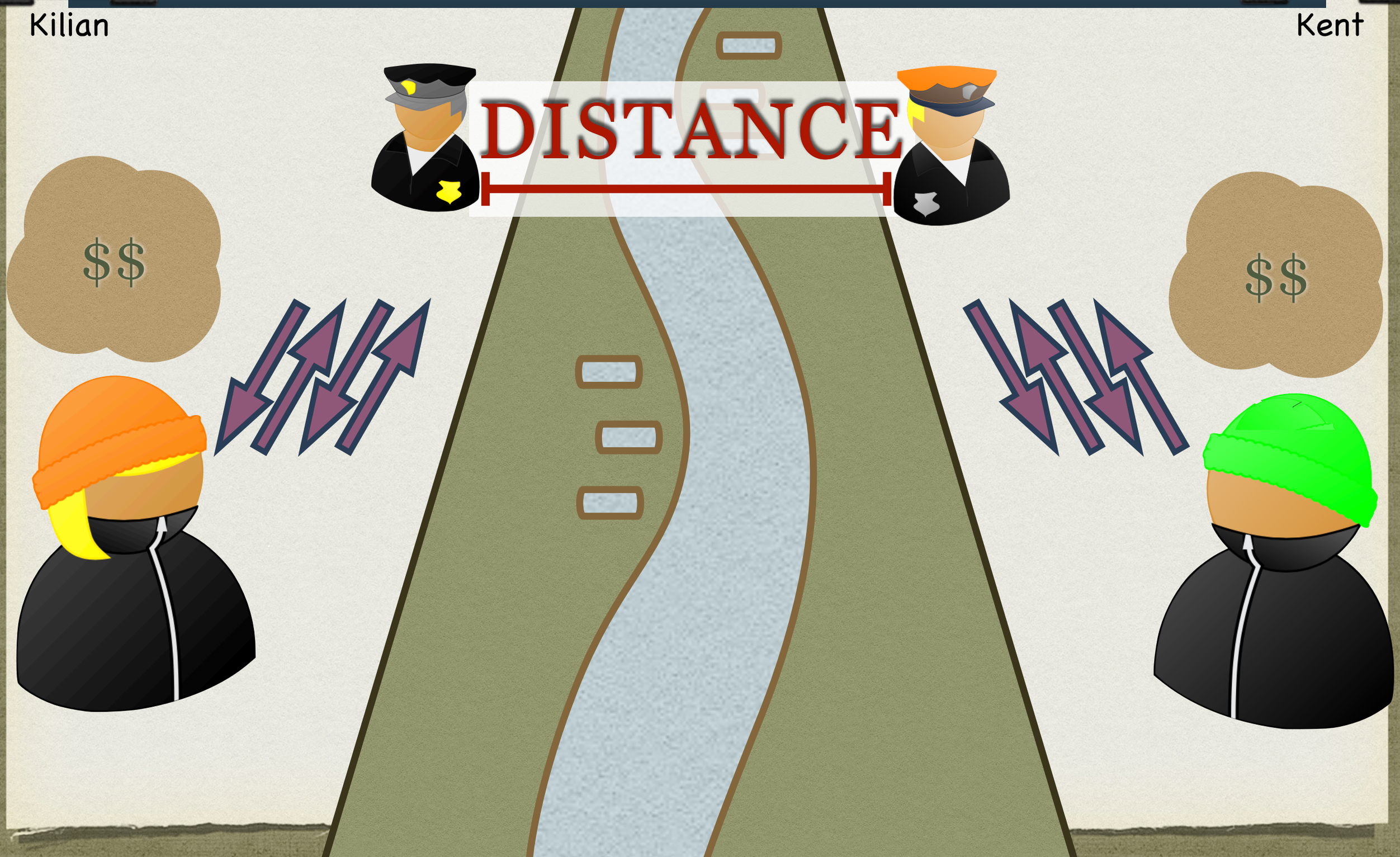
judge

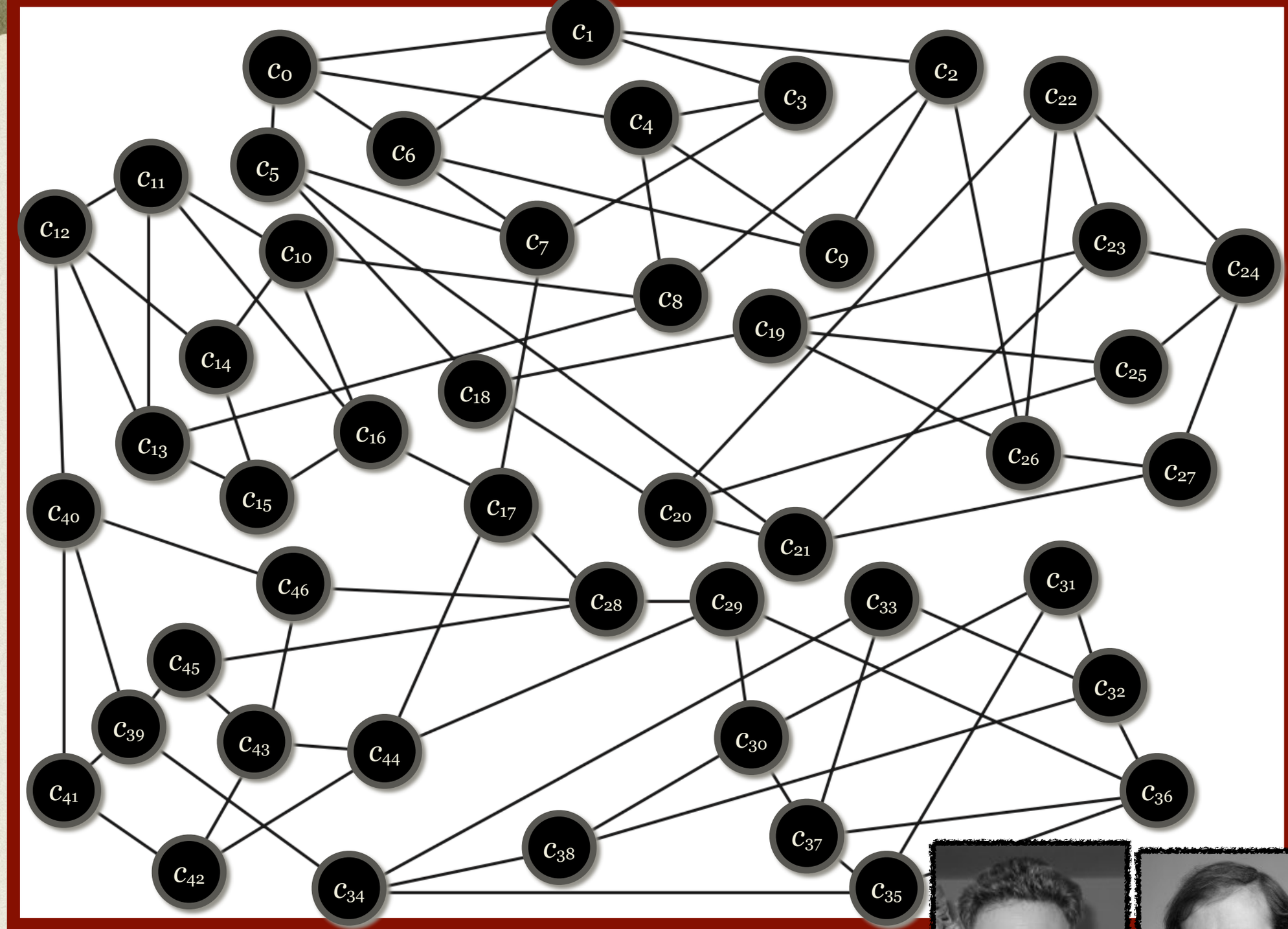
ZERO-KNOWLEDGE

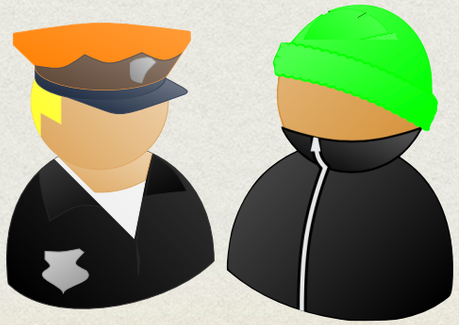
RELATIVISTIC MODEL

Kilian

Kent




c_0
c_1
c_2
c_3
c_4
c_5
c_6
c_7
c_8
c_9
c_{10}
c_{11}
c_{12}
c_{13}
c_{14}
c_{15}
c_{16}
c_{17}
c_{18}
c_{19}
c_{20}
c_{21}
c_{22}
c_{23}
c_{24}
c_{25}
c_{26}
c_{27}
c_{28}
c_{29}
c_{30}
c_{31}
c_{32}
c_{33}
c_{34}
c_{35}
c_{36}
c_{37}
c_{38}
c_{39}
c_{40}
c_{41}
c_{42}
c_{43}
c_{44}
c_{45}
c_{46}



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

poly poly

$[($: : : $)(w, z)] \approx [($ $)(w, z)]$

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

poly poly

$[($: : : $)(w, z)] \approx [($ $)(w, z)]$

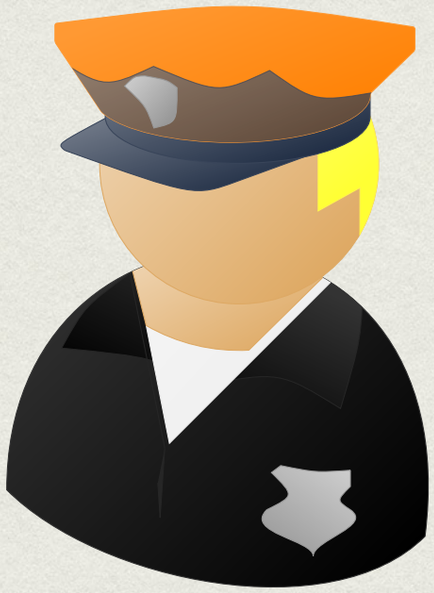
provers

$\forall$ $,$
poly

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

$[($ $:$ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

provers



verifiers

$\forall$ $,$
poly

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

$[($ $:$ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

judge

provers

verifiers

$\forall$,
poly

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

$[($: : : $)(w, z)] \approx [($ $)(w, z)]$

aux input

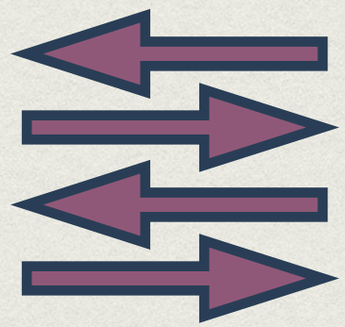
judge

provers

verifiers

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

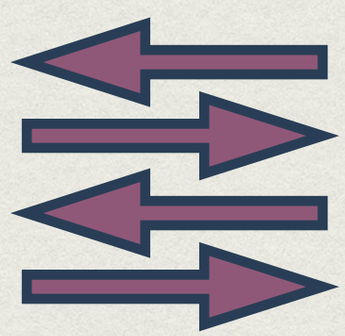
$[($ $)(w, z)] \approx [($ $)(w, z)]$



aux input

judge

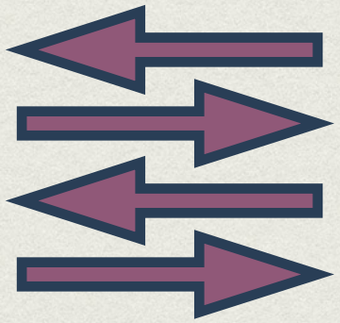
provers



verifiers

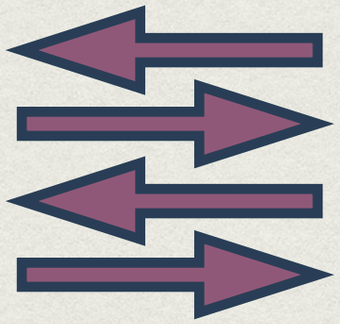
$\forall$ poly, $\exists$ poly $\forall w \in L, \forall z,$

$[($ $:$ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$



aux input

judge

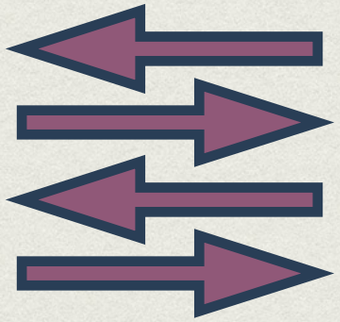


provers

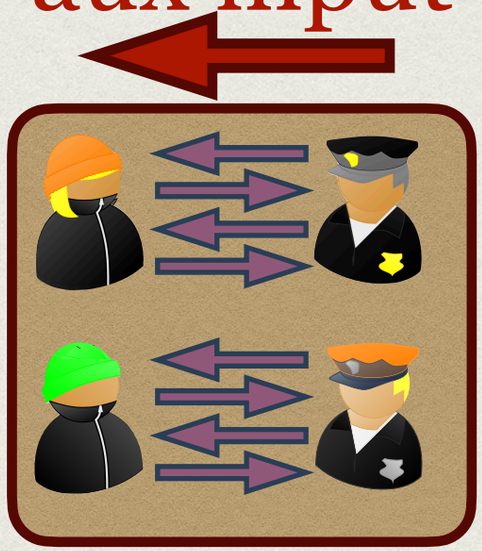
verifiers

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

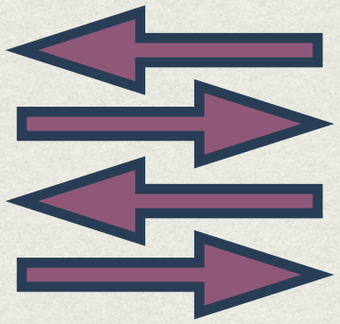
$[($ $:$ $:$ $:$ $)(w, z)] \approx [($ $)(w, z)]$

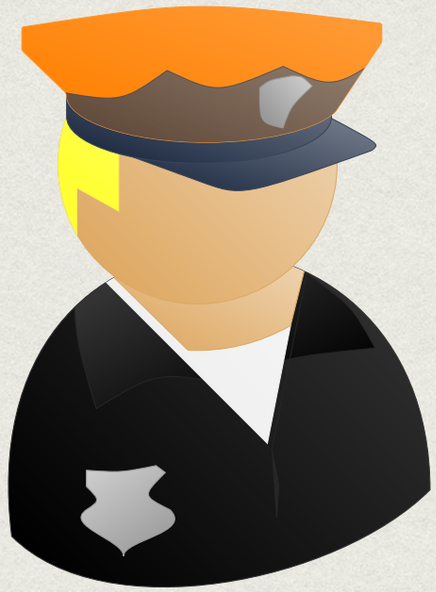


aux input



judge

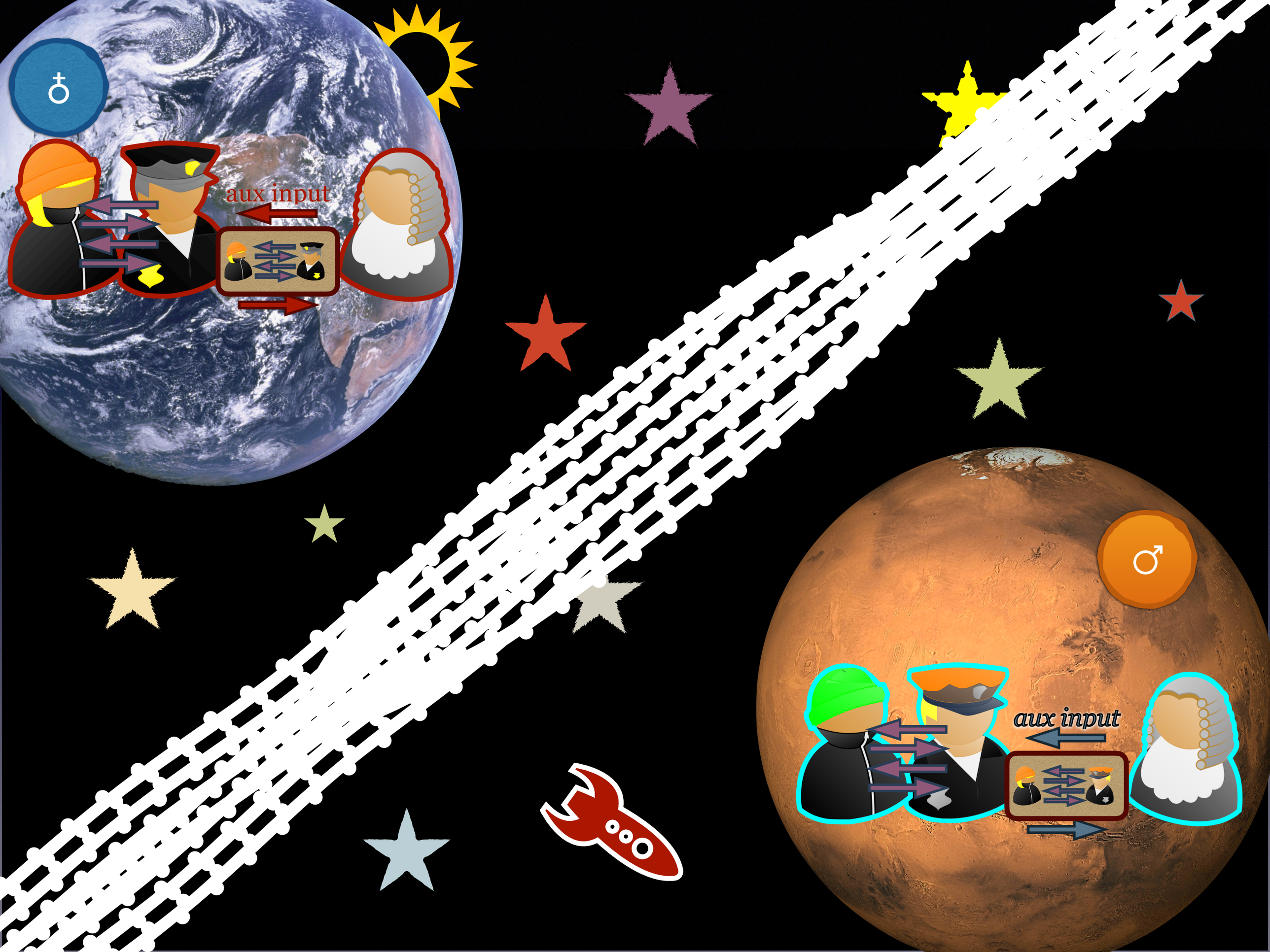




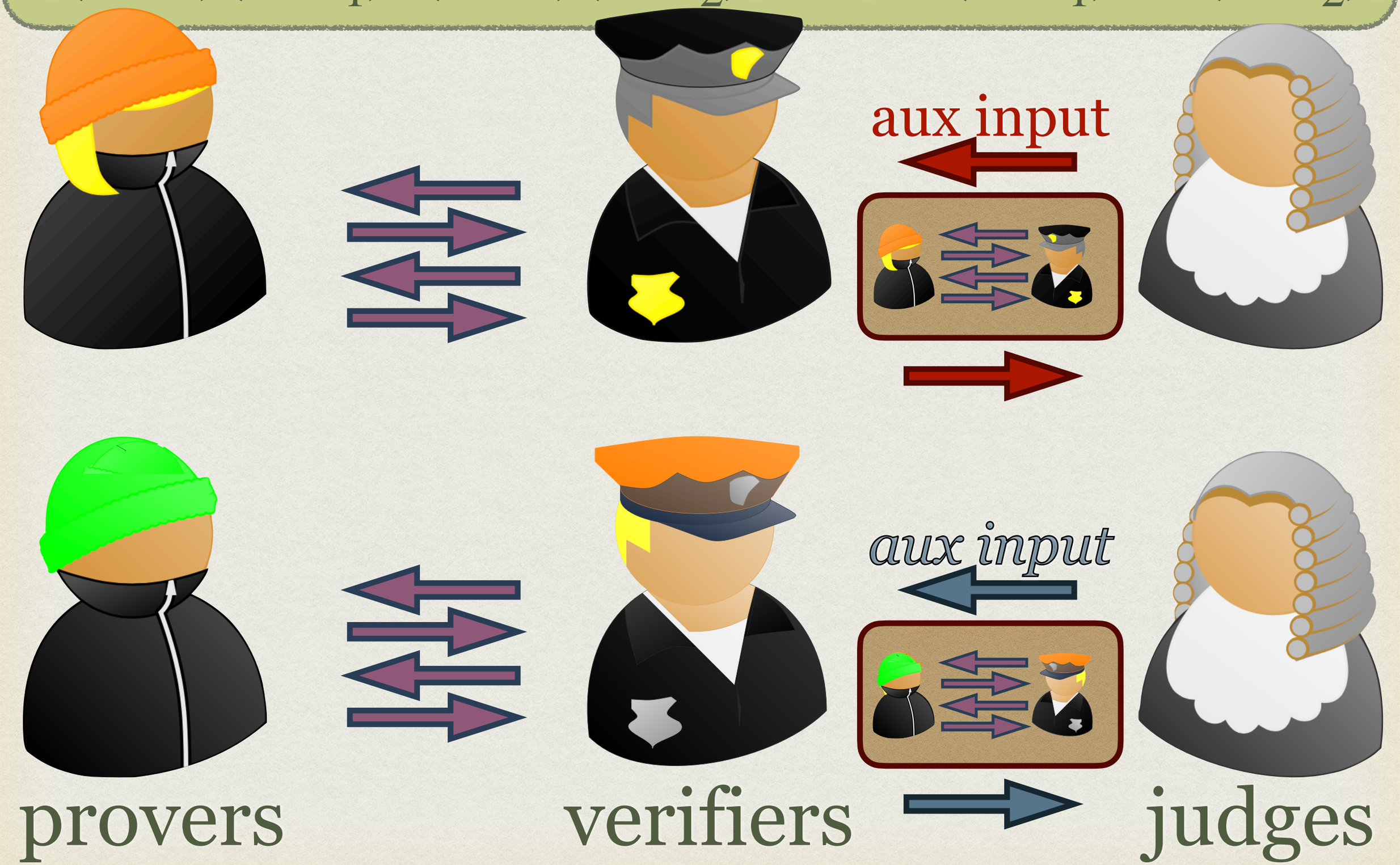
provers

verifiers

RELATIVISTIC ZERO-KNOWLEDGE

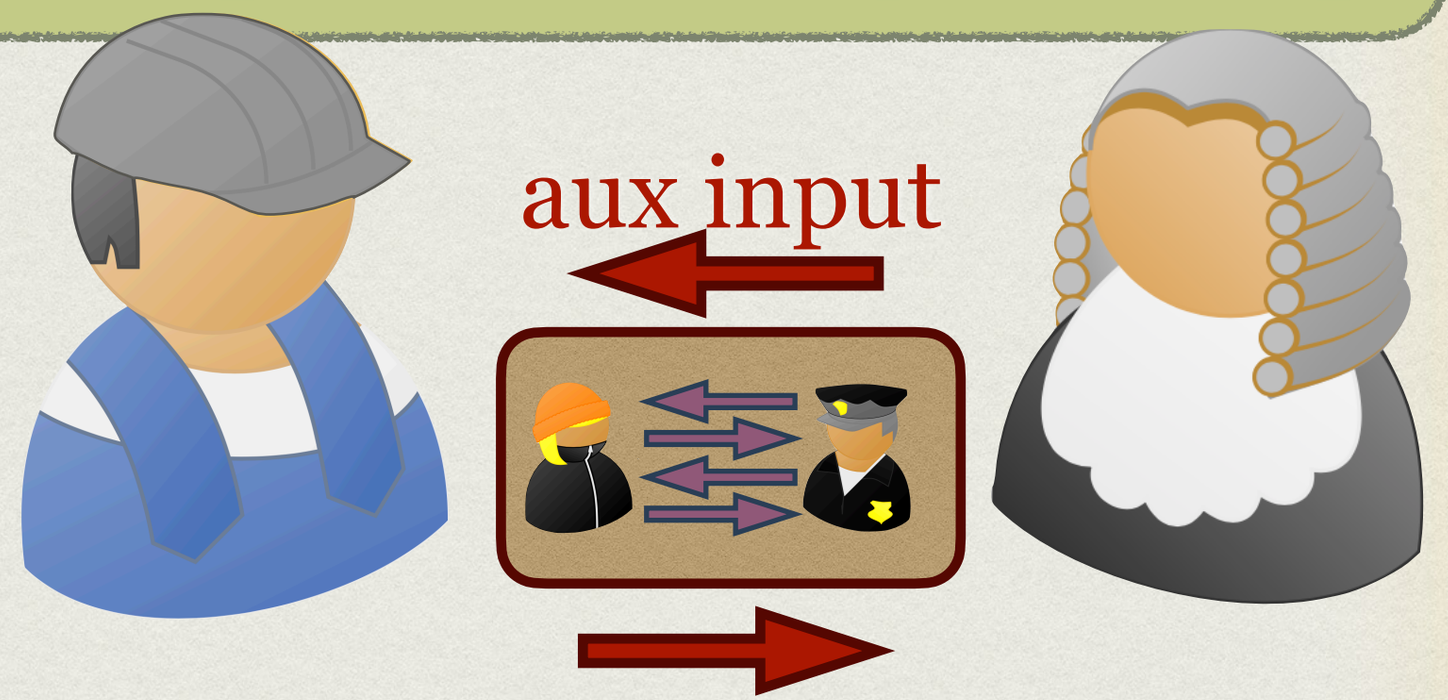

♁
aux input
♂
aux input

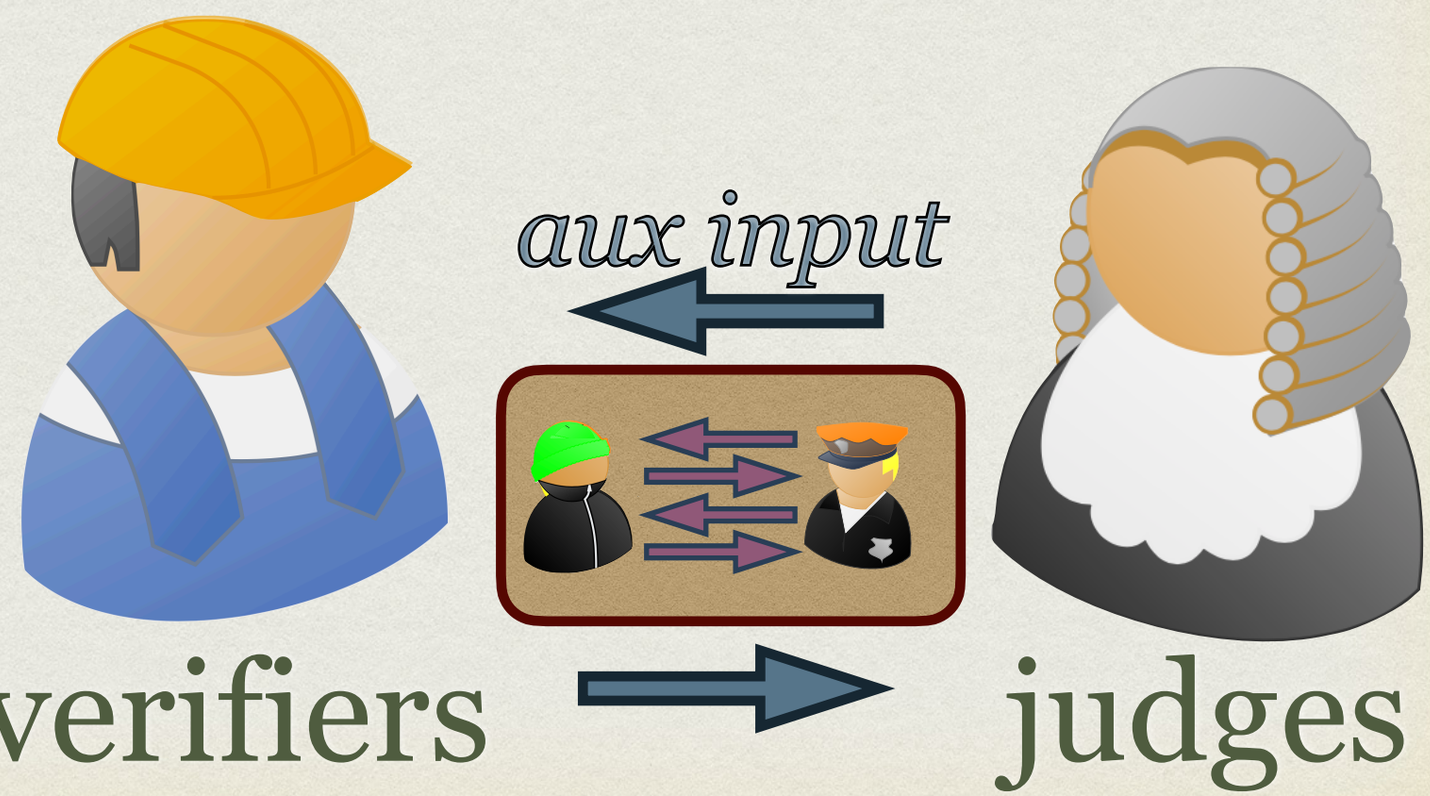
$$\forall \text{poly}, \text{poly} \; \exists \, , \, \forall w \in L, \forall z_1, z_2$$
$$[(\, : \,)(w, z_1), (\, : \,)(w, z_2)] \approx [\, (w, z_1), \, (w, z_2)]$$

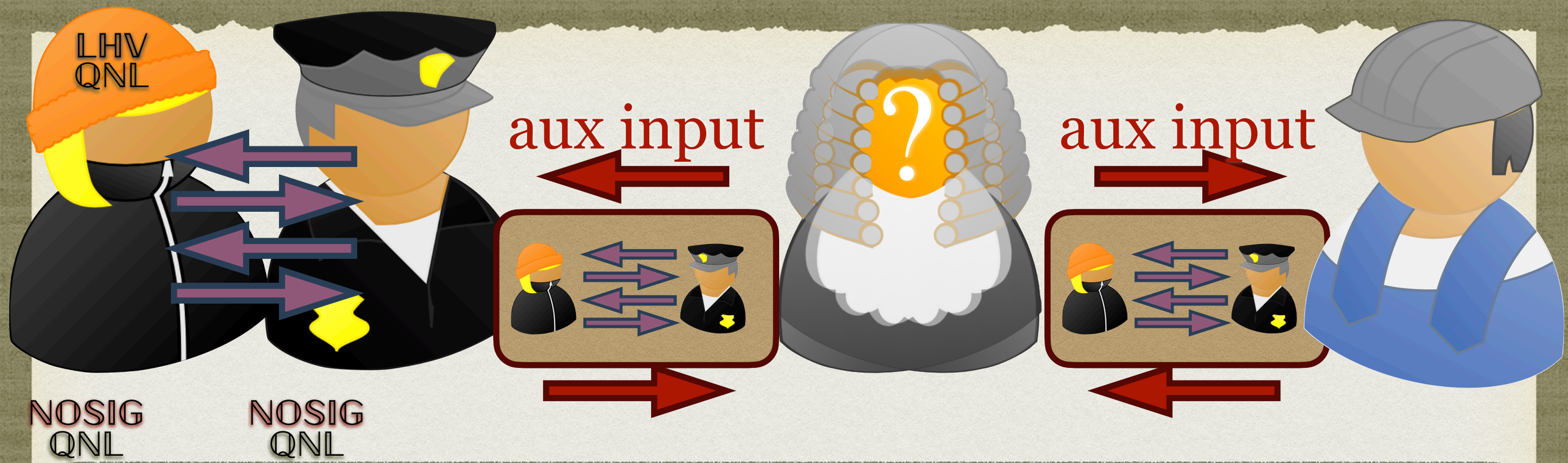


$\forall$, $\exists$, $\forall w \in L, \forall z_1, z_2$

$\overset{\text{poly}}{[(\ :\ )}(w, z_1), \overset{\text{poly}}{(\ :\ )}(w, z_2)] \approx [\ (w, z_1), \ (w, z_2)]$



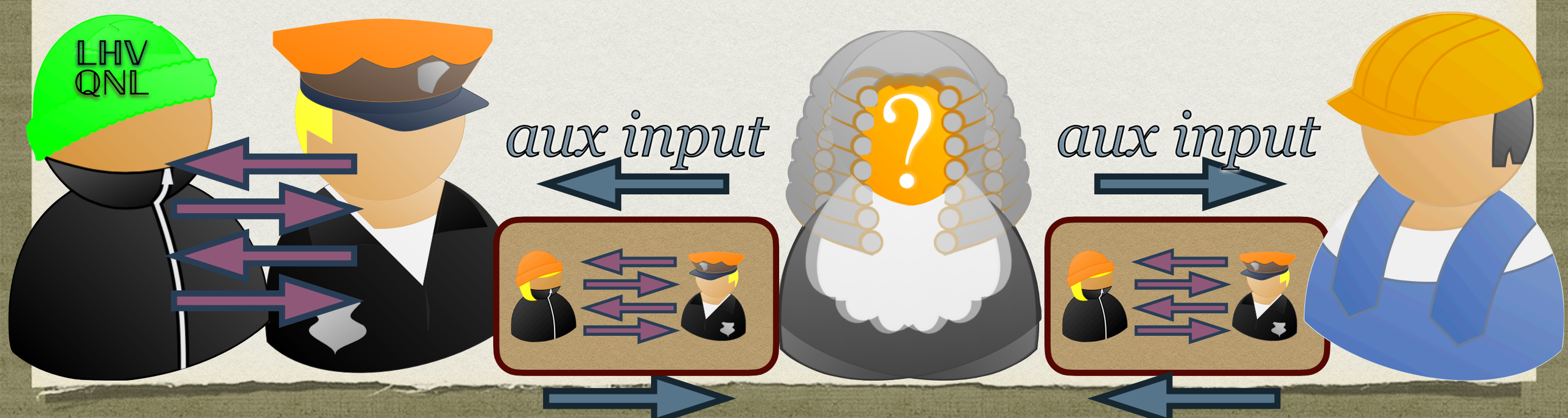


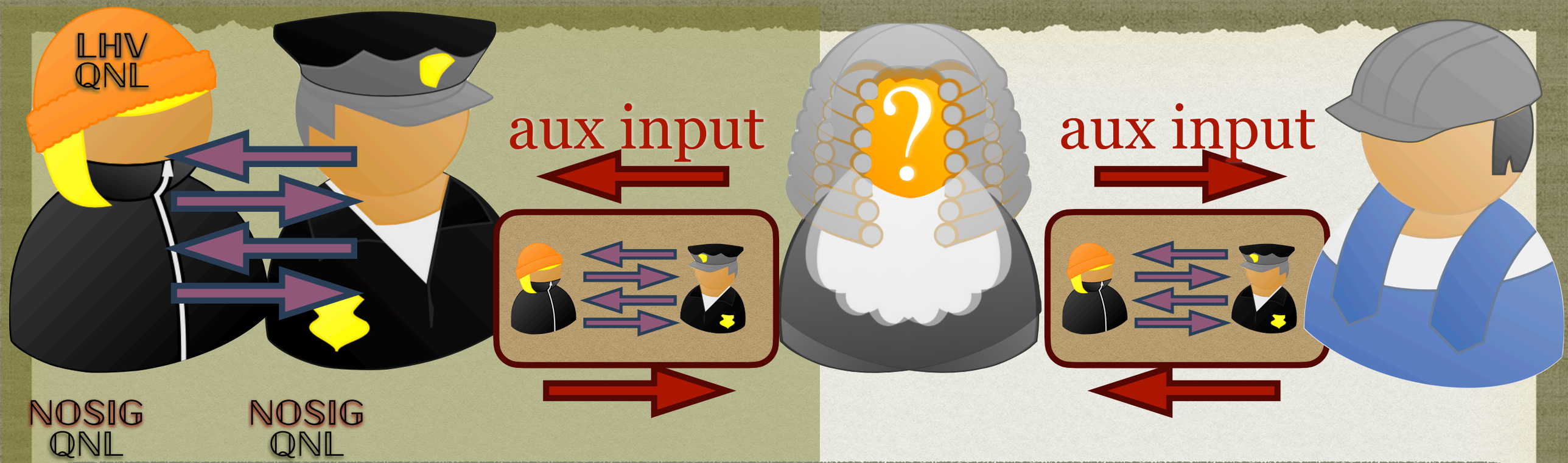


$$\forall \text{🧑}, \text{🧑}\ \exists \text{🧑}, \text{🧑}\ \forall w \in L, \forall z_1, z_2$$

$$[(\text{poly}\ \text{🧑}:\text{🧑})(w, z_1), (\text{poly}\ \text{🧑}:\text{🧑})(w, z_2)] \approx [\text{🧑}(w, z_1), \text{🧑}(w, z_2)]$$

RELATIVISTIC ZK

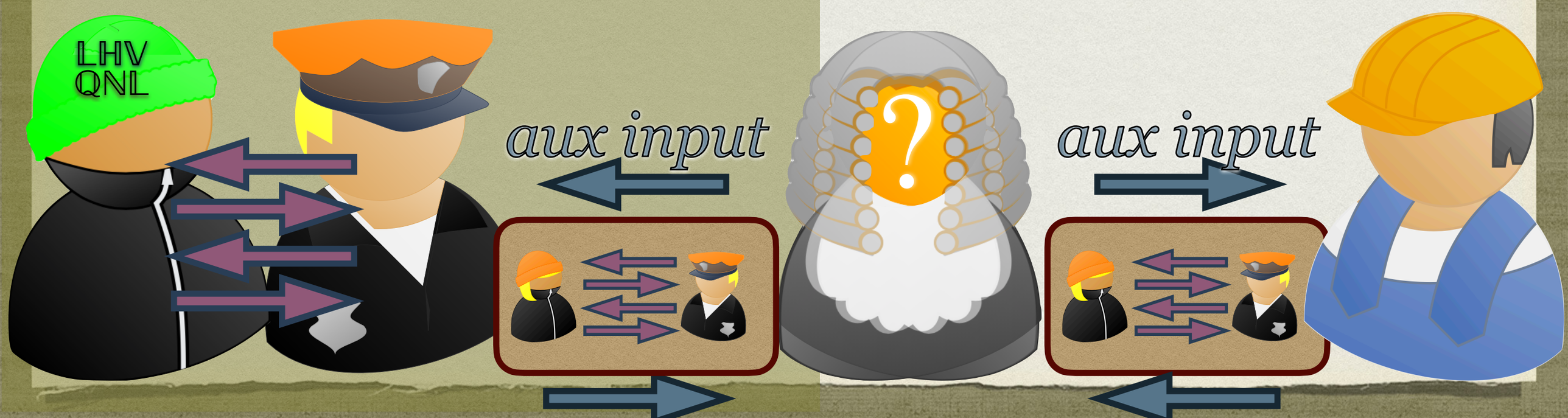


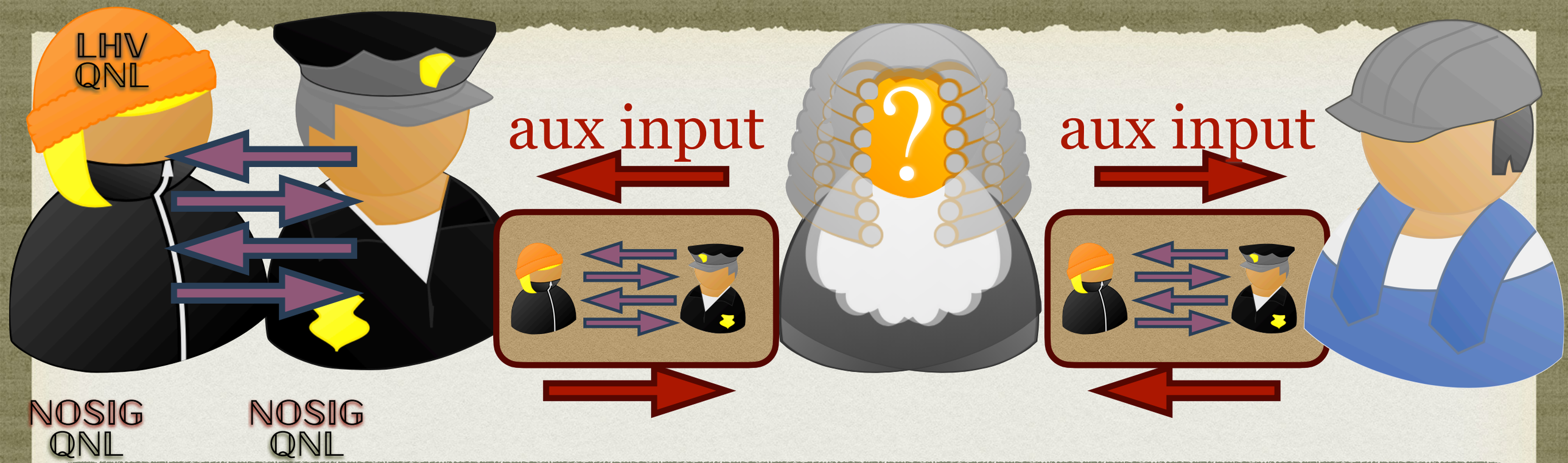


$$\forall \, , \, \exists \, , \, \forall w \in L, \forall z_1, z_2$$

$$[(\overset{\text{poly}}{\;}:\overset{\text{poly}}{\;})(w, z_1), (\;:\;)(w, z_2)] \approx [\;(w, z_1), \;(w, z_2)]$$

RELATIVISTIC ZK

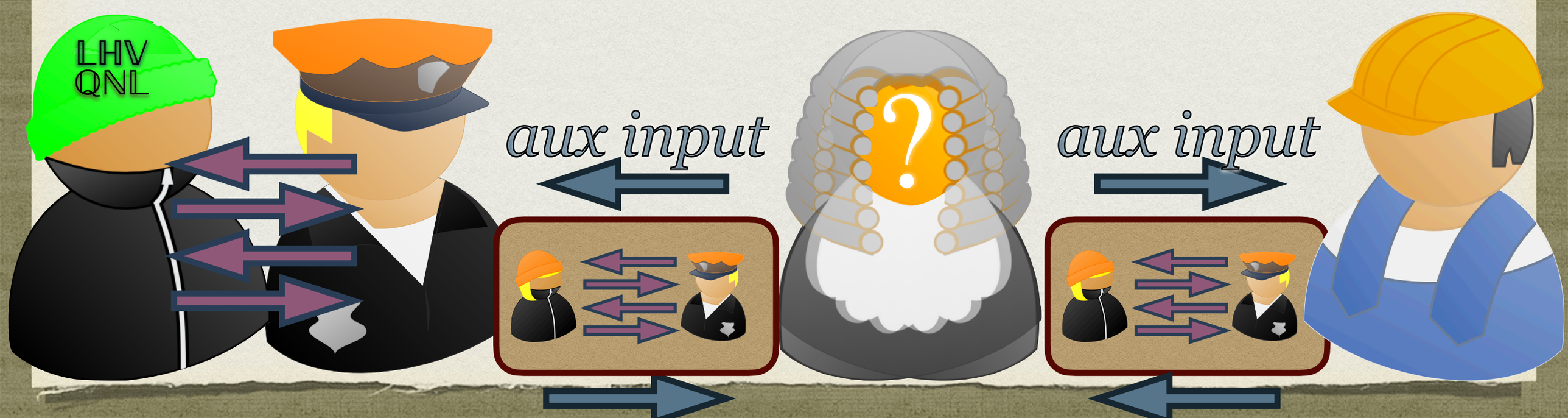


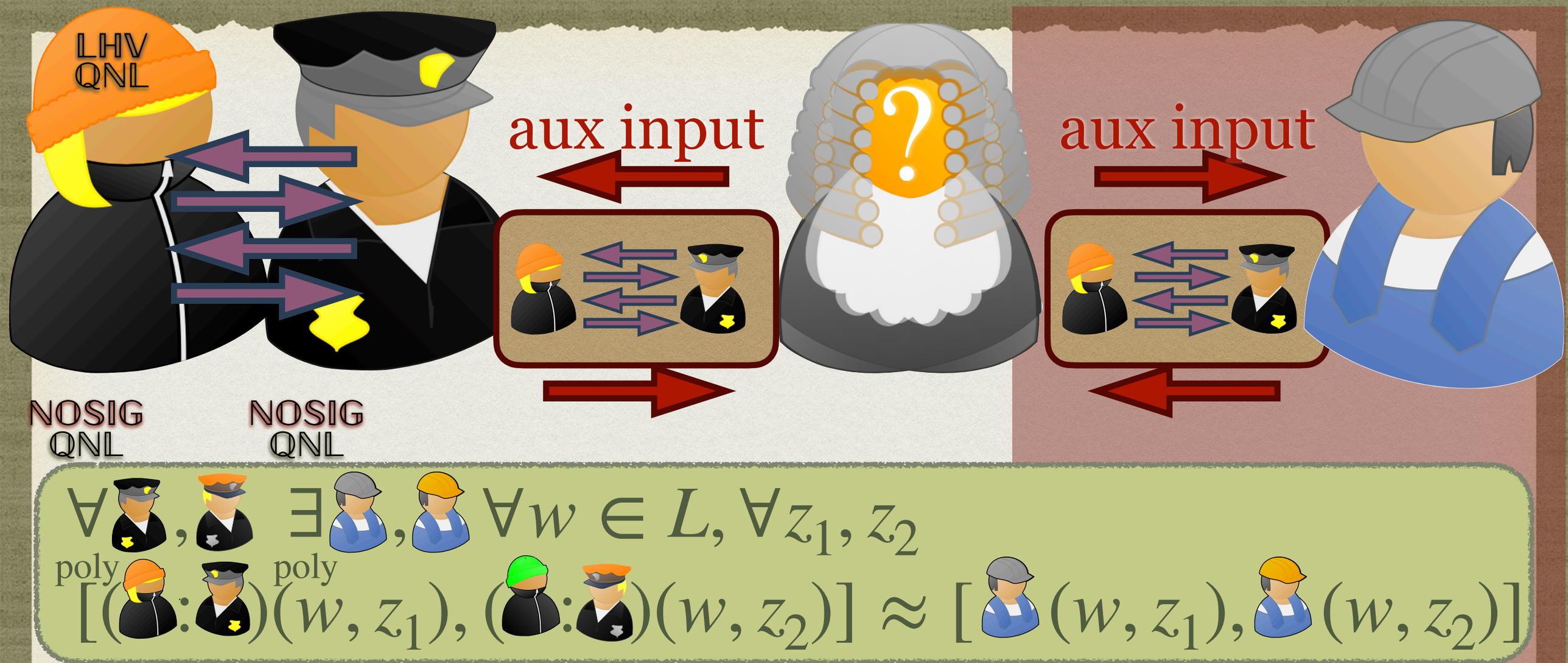


$$\forall \text{🧑}, \text{🧑}\ \exists \text{🧑}, \text{🧑}\ \forall w \in L, \forall z_1, z_2$$

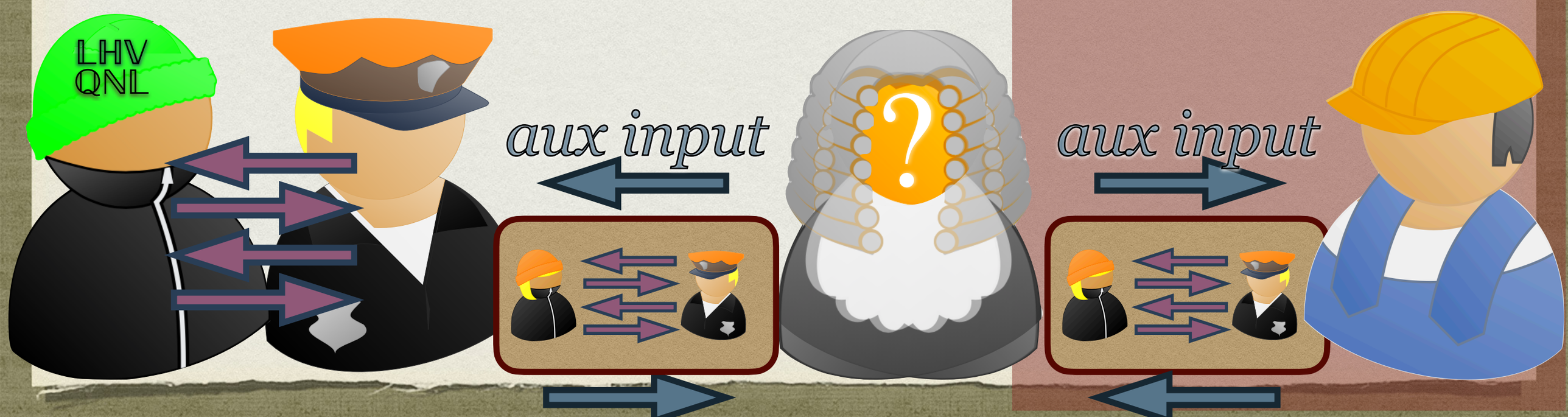
$$[(\text{poly}\ \text{🧑}:\text{🧑})(w, z_1), (\text{poly}\ \text{🧑}:\text{🧑})(w, z_2)] \approx [\text{🧑}(w, z_1), \text{🧑}(w, z_2)]$$

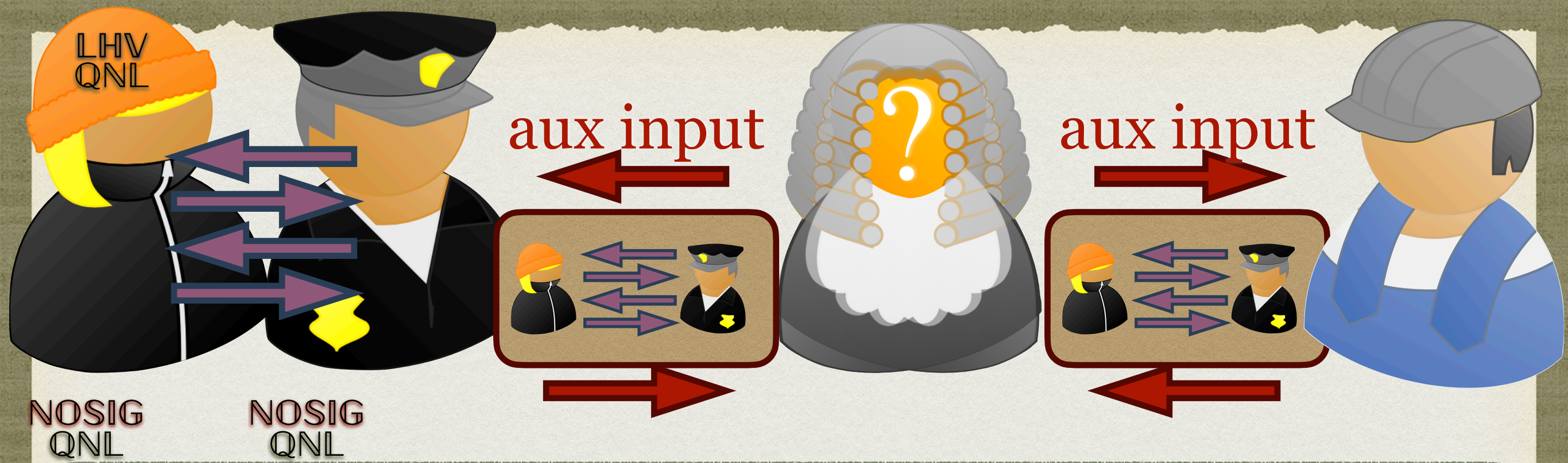
RELATIVISTIC ZK





RELATIVISTIC ZK

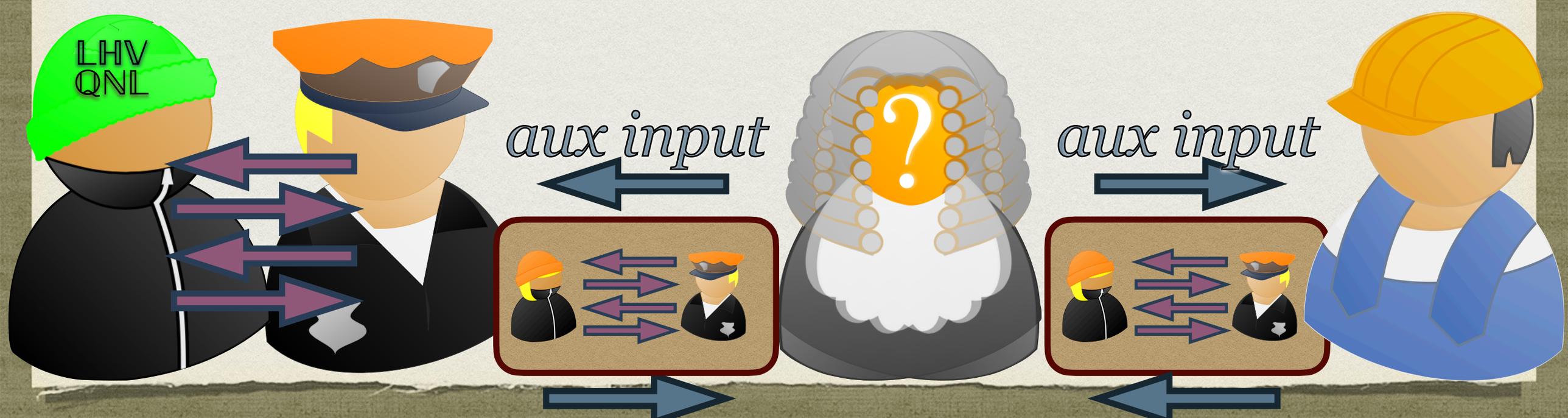




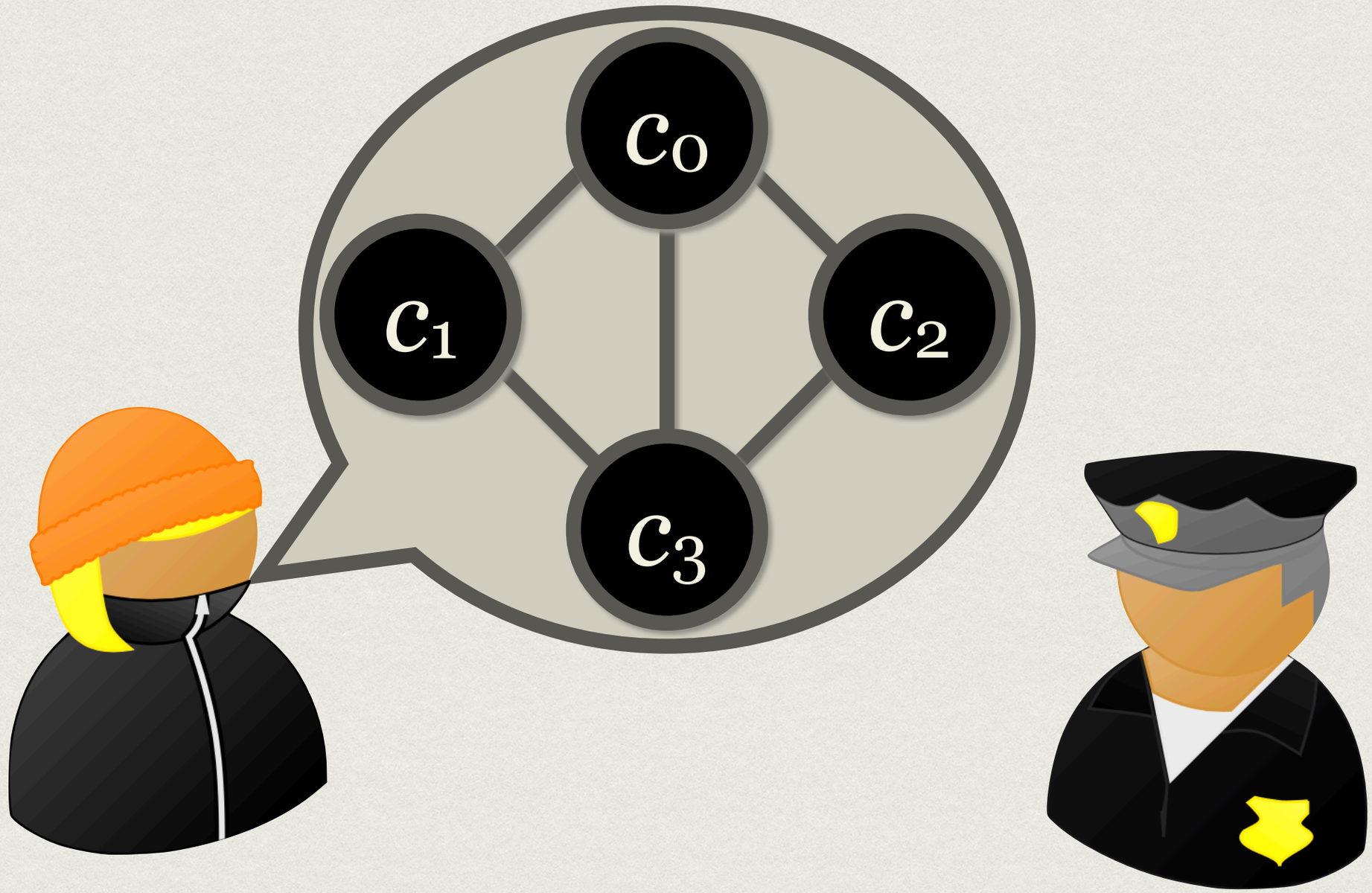
$$\forall \text{🧑}, \text{🧑}\ \exists \text{🧑}, \text{🧑}\ \forall w \in L, \forall z_1, z_2$$

$$[(\text{poly}\ \text{🧑}:\text{🧑})(w, z_1), (\text{poly}\ \text{🧑}:\text{🧑})(w, z_2)] \approx [\text{🧑}(w, z_1), \text{🧑}(w, z_2)]$$

RELATIVISTIC ZK



COMMITMENTS



COMMITMENT

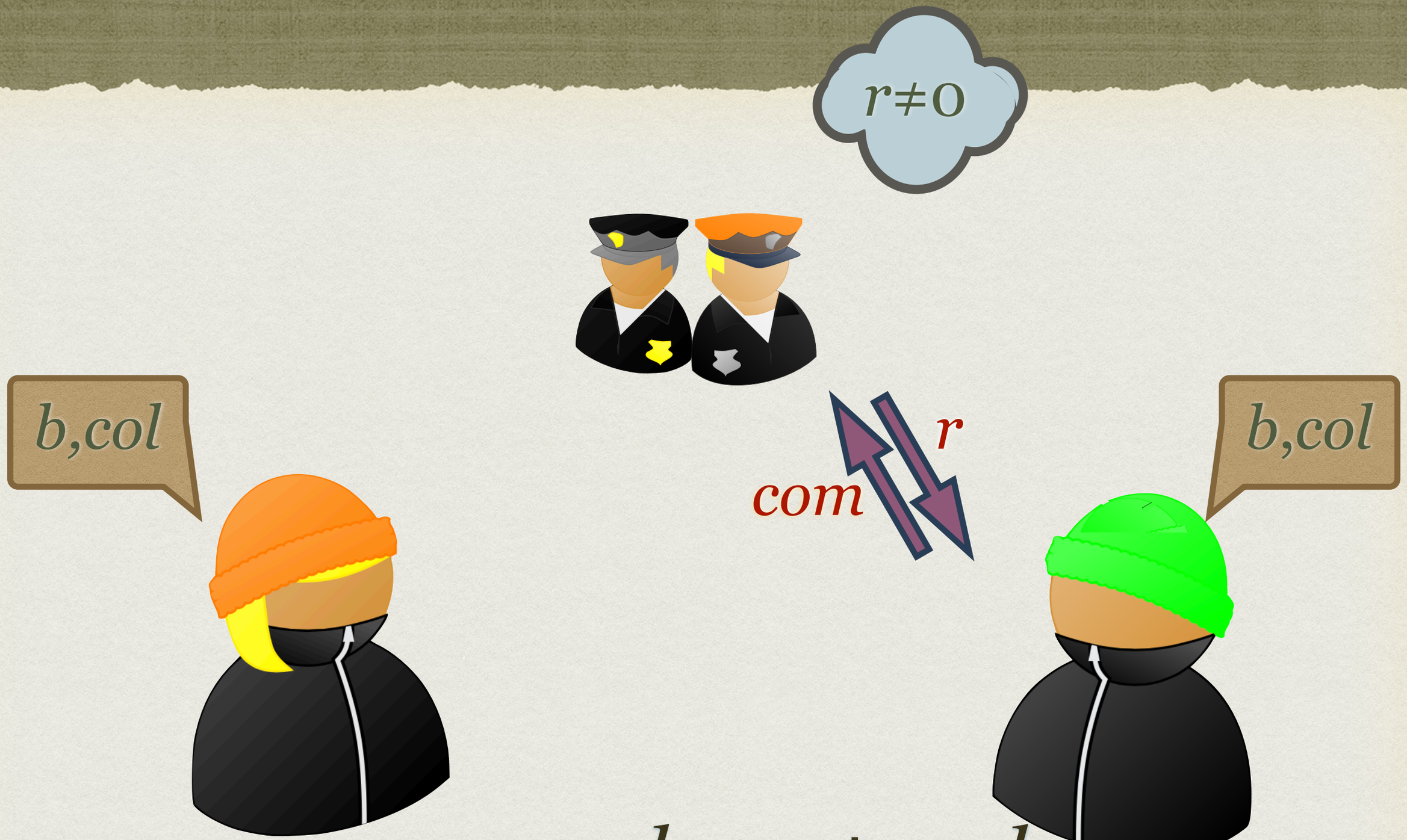
COMMITMENT

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

COMMITMENT

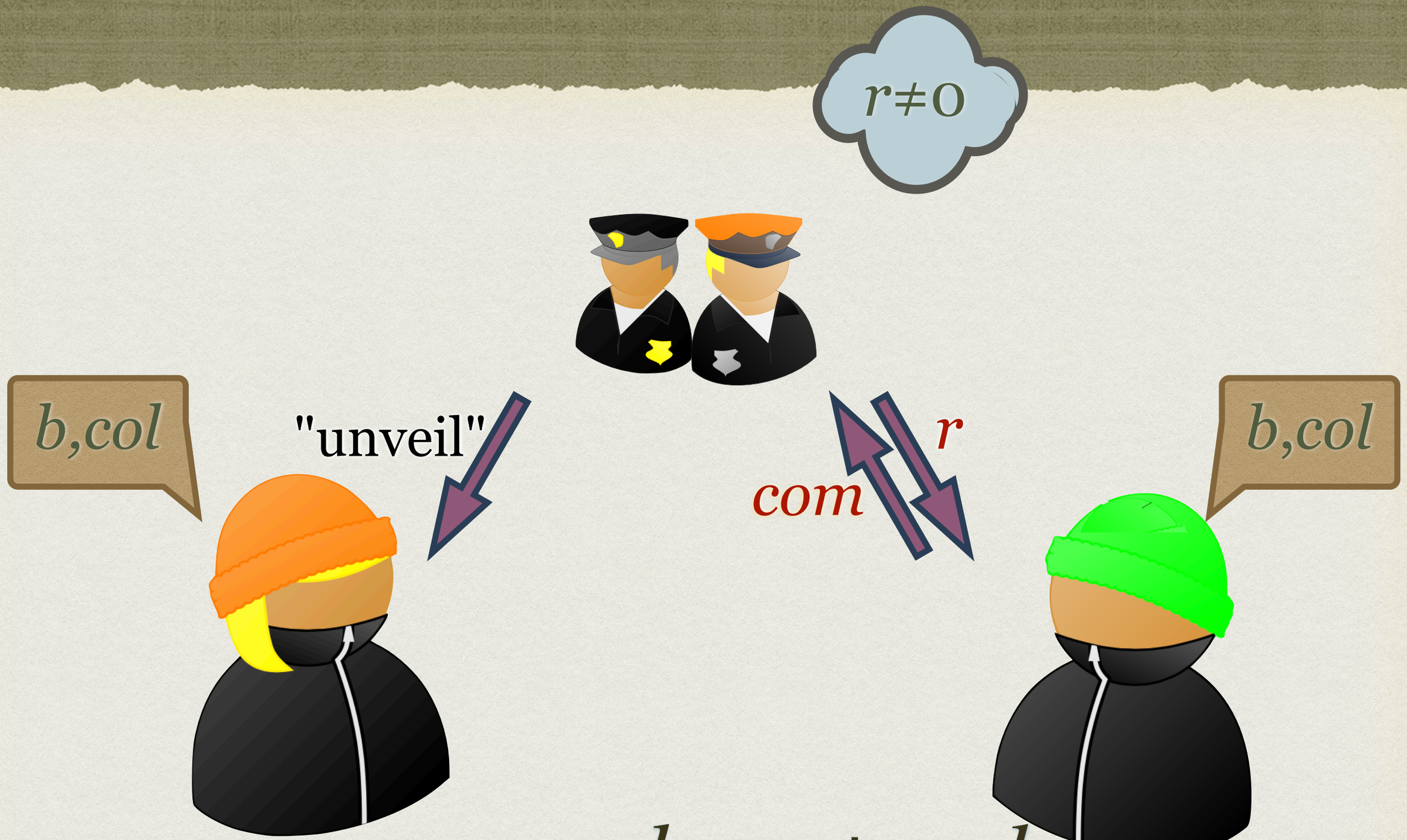
$$com := b \cdot r + col$$

COMMITMENT



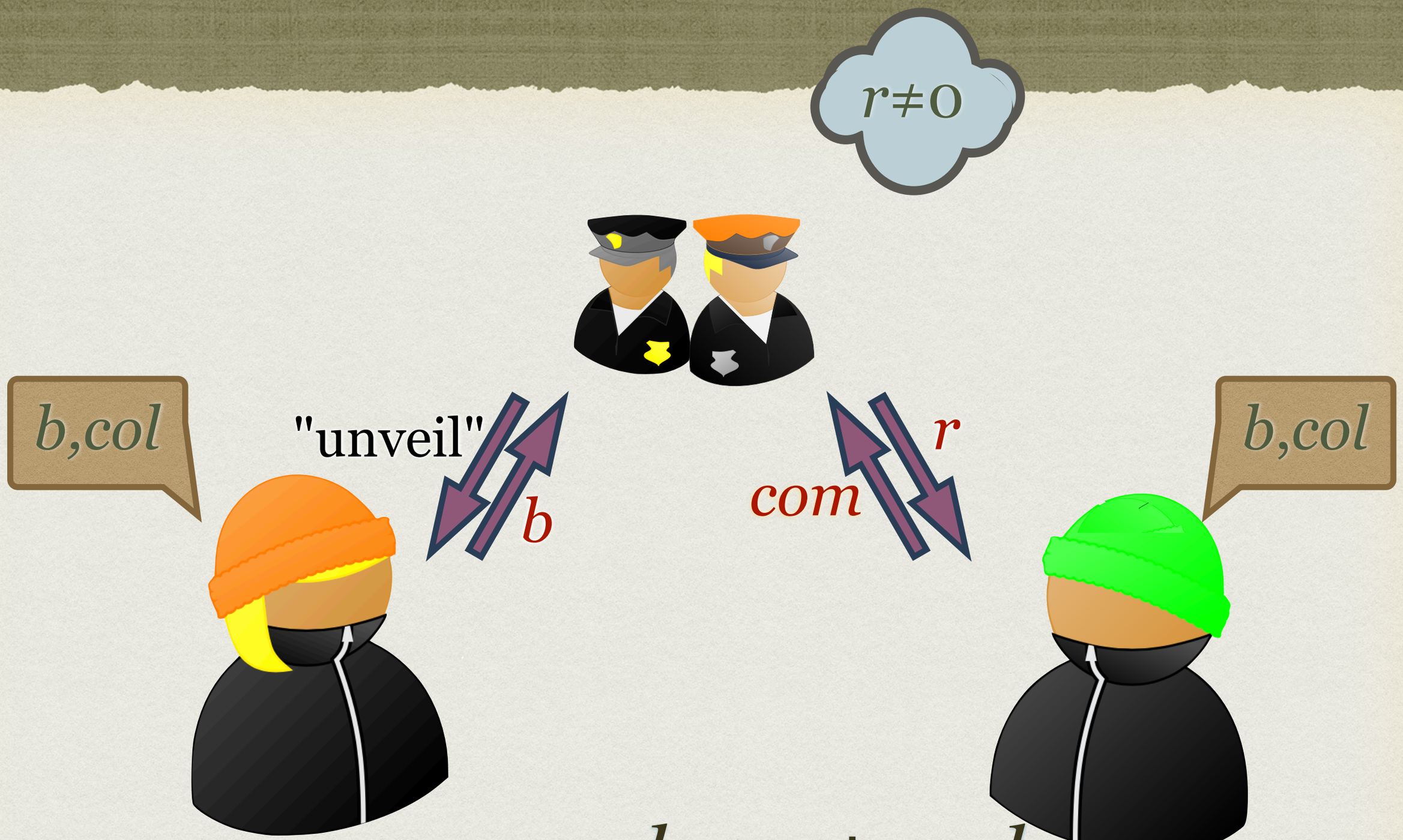
$$com := b \cdot r + col$$

COMMITMENT



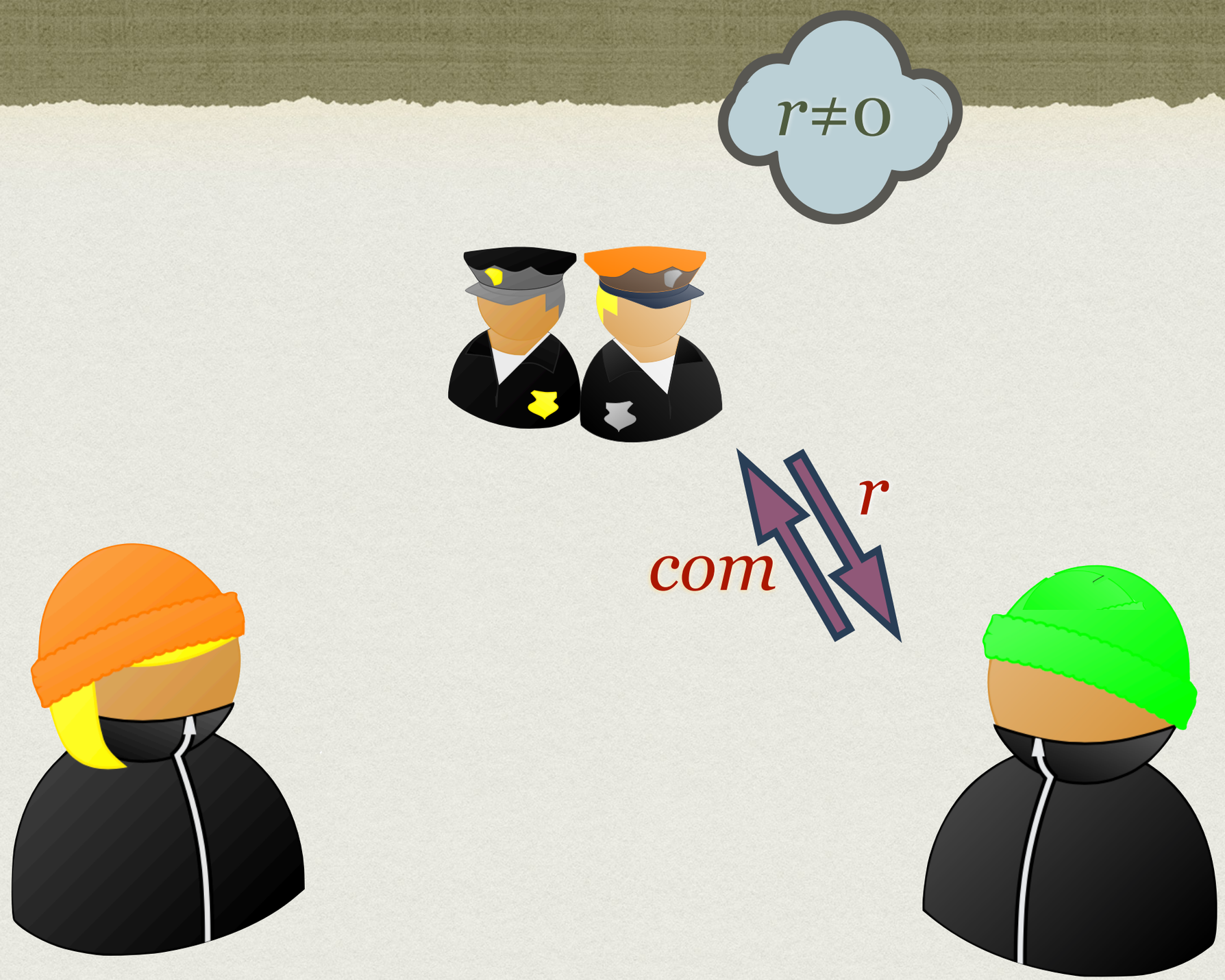
$$com := b \cdot r + col$$

COMMITMENT

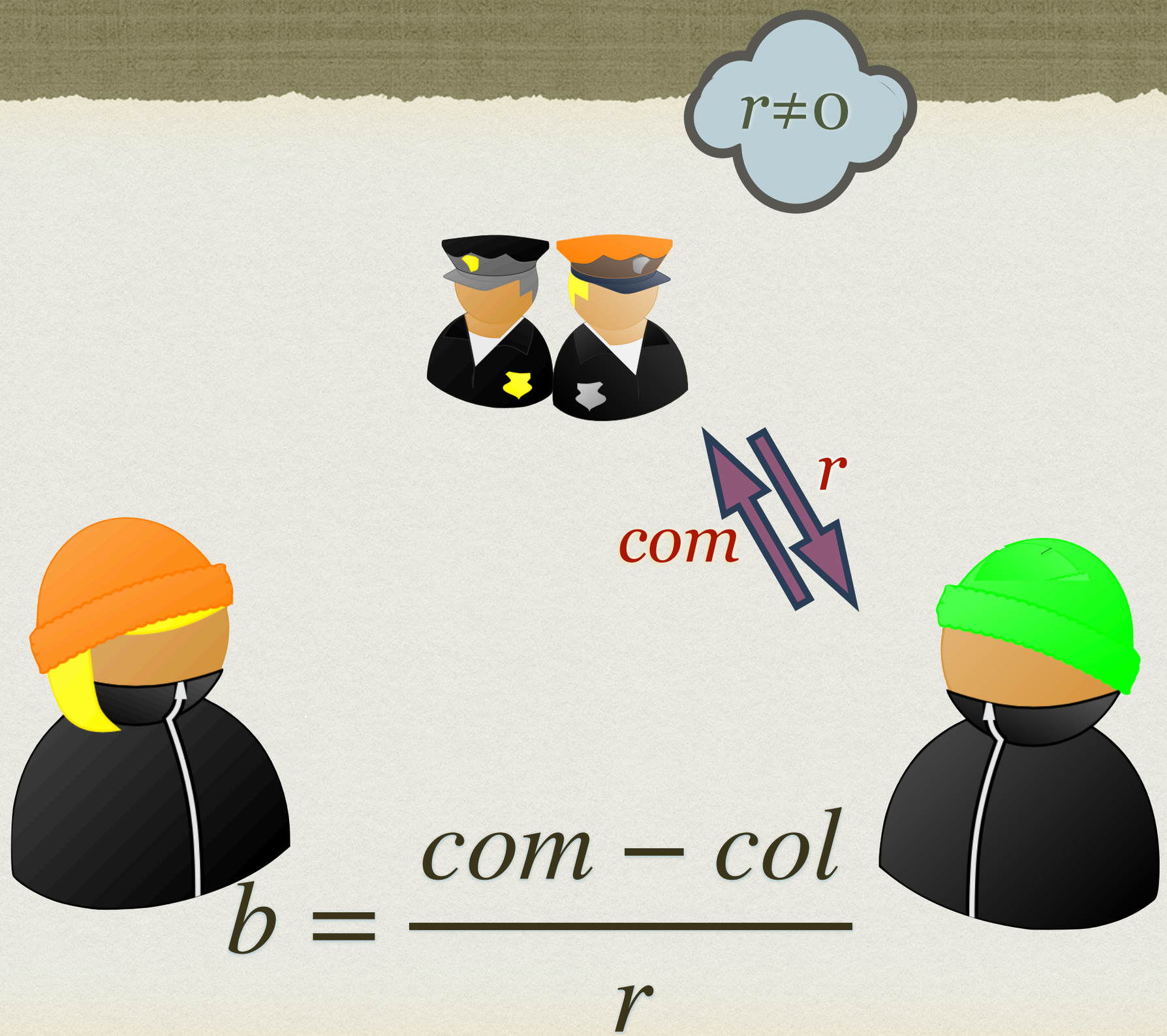


$$com := b \cdot r + col$$

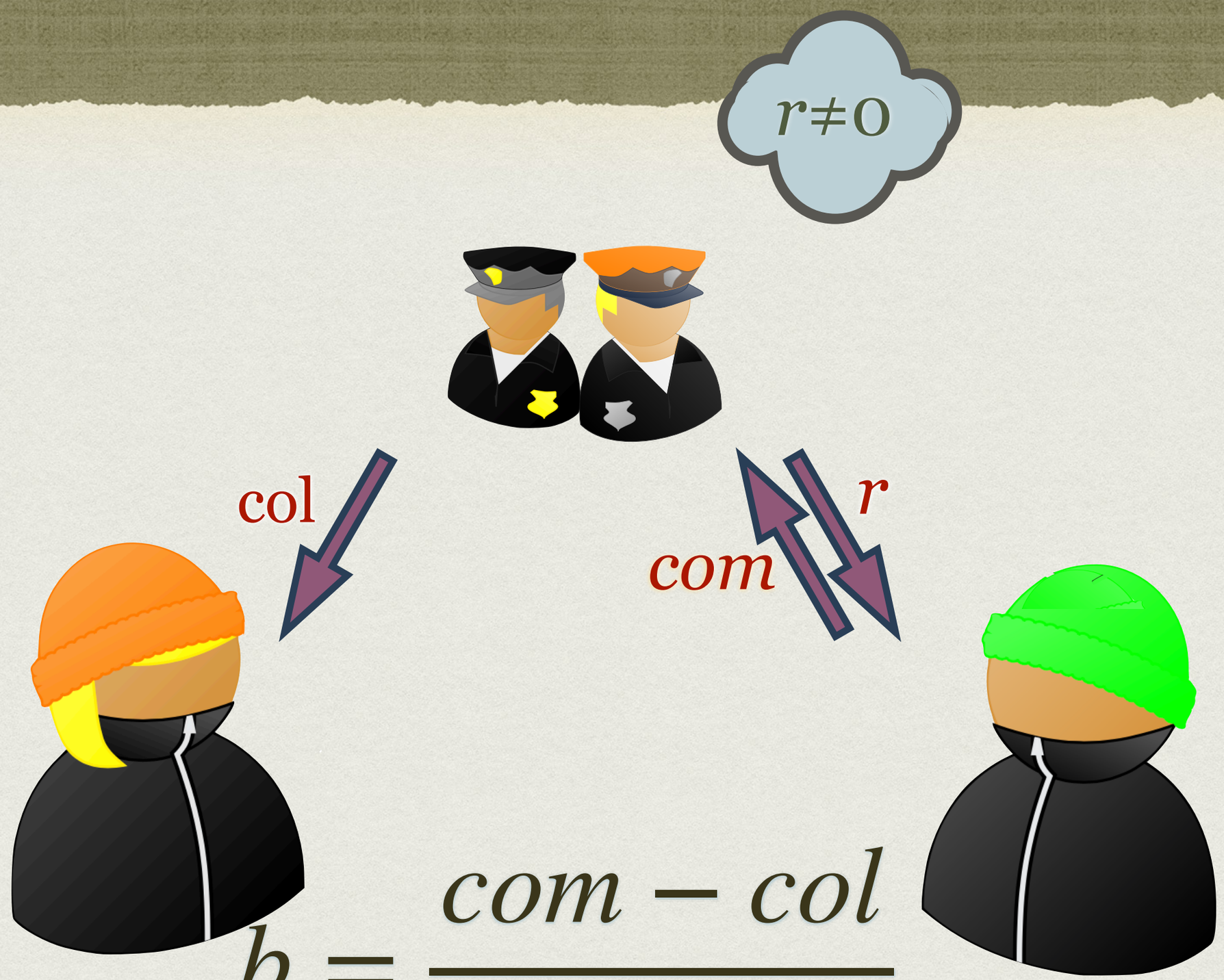
BINDING ?



BINDING ?

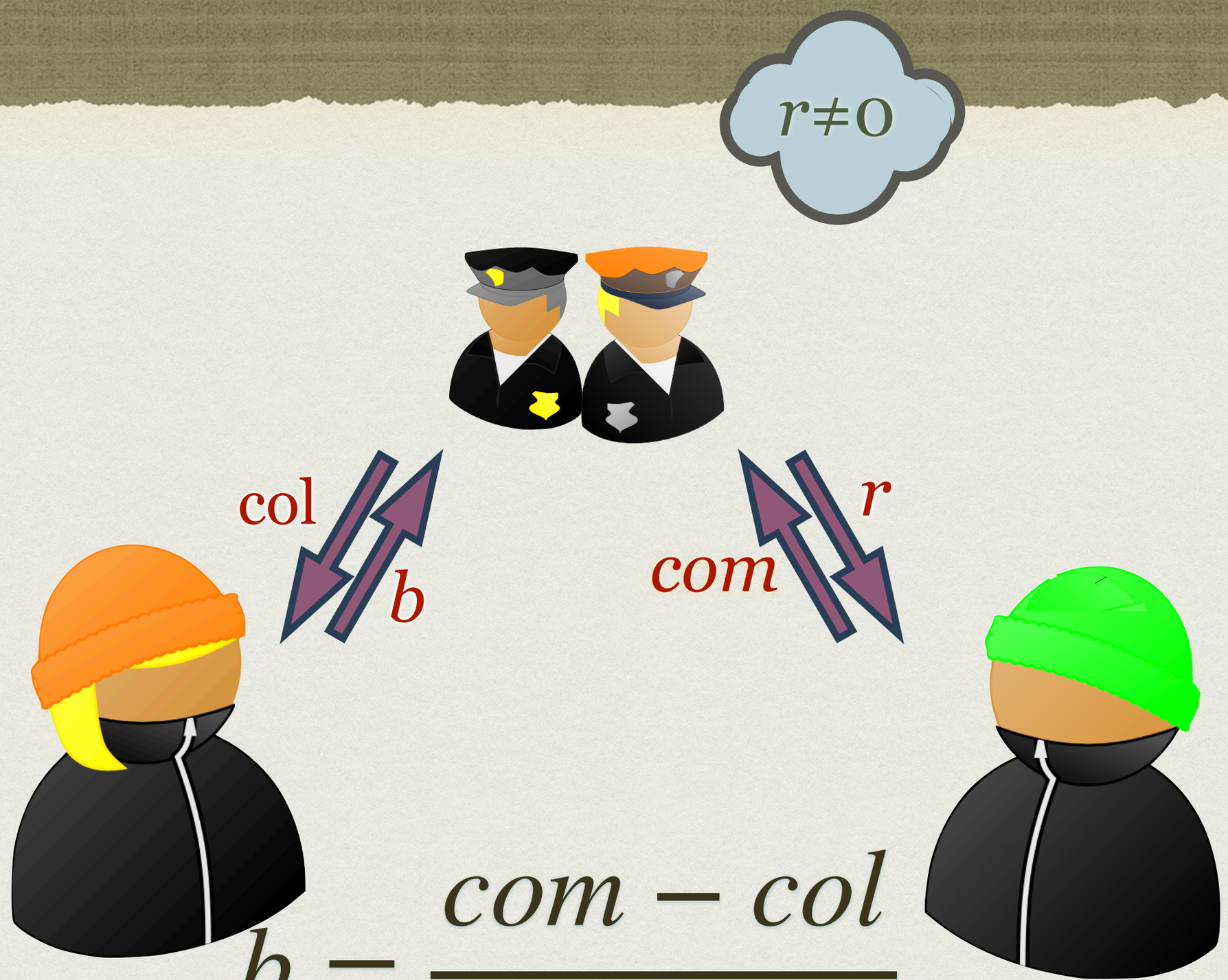


BINDING ?



$$b = \frac{com - col}{r}$$

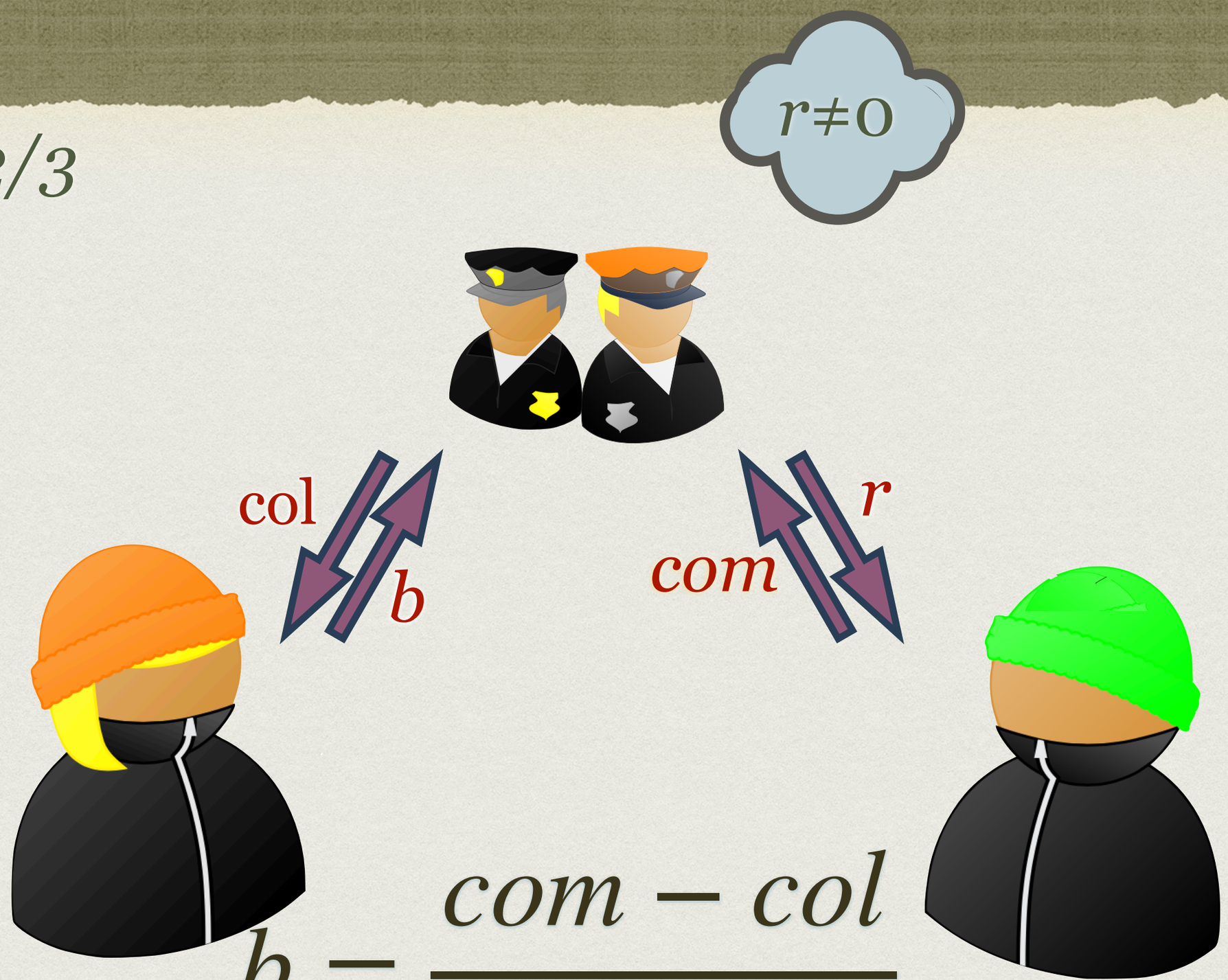
BINDING ?



$$b = \frac{com - col}{r}$$

BINDING ?

$\omega_{LHV} = 2/3$



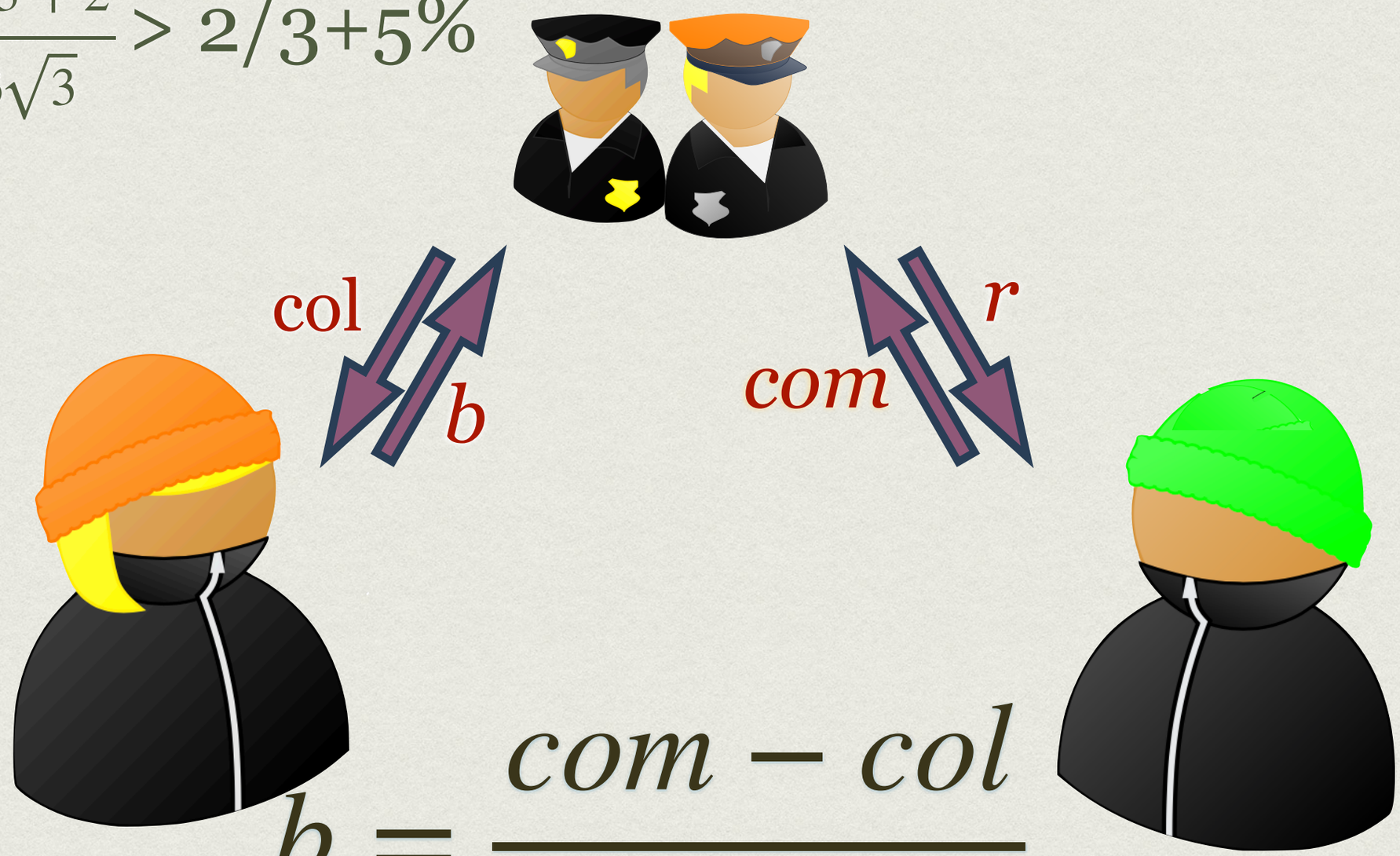
$$b = \frac{com - col}{r}$$

BINDING ?

$r \neq 0$

$\omega_{LHV} = 2/3$

$\omega_{QNL} = \frac{\sqrt{3}+2}{3\sqrt{3}} > 2/3 + 5\%$



$$b = \frac{com - col}{r}$$

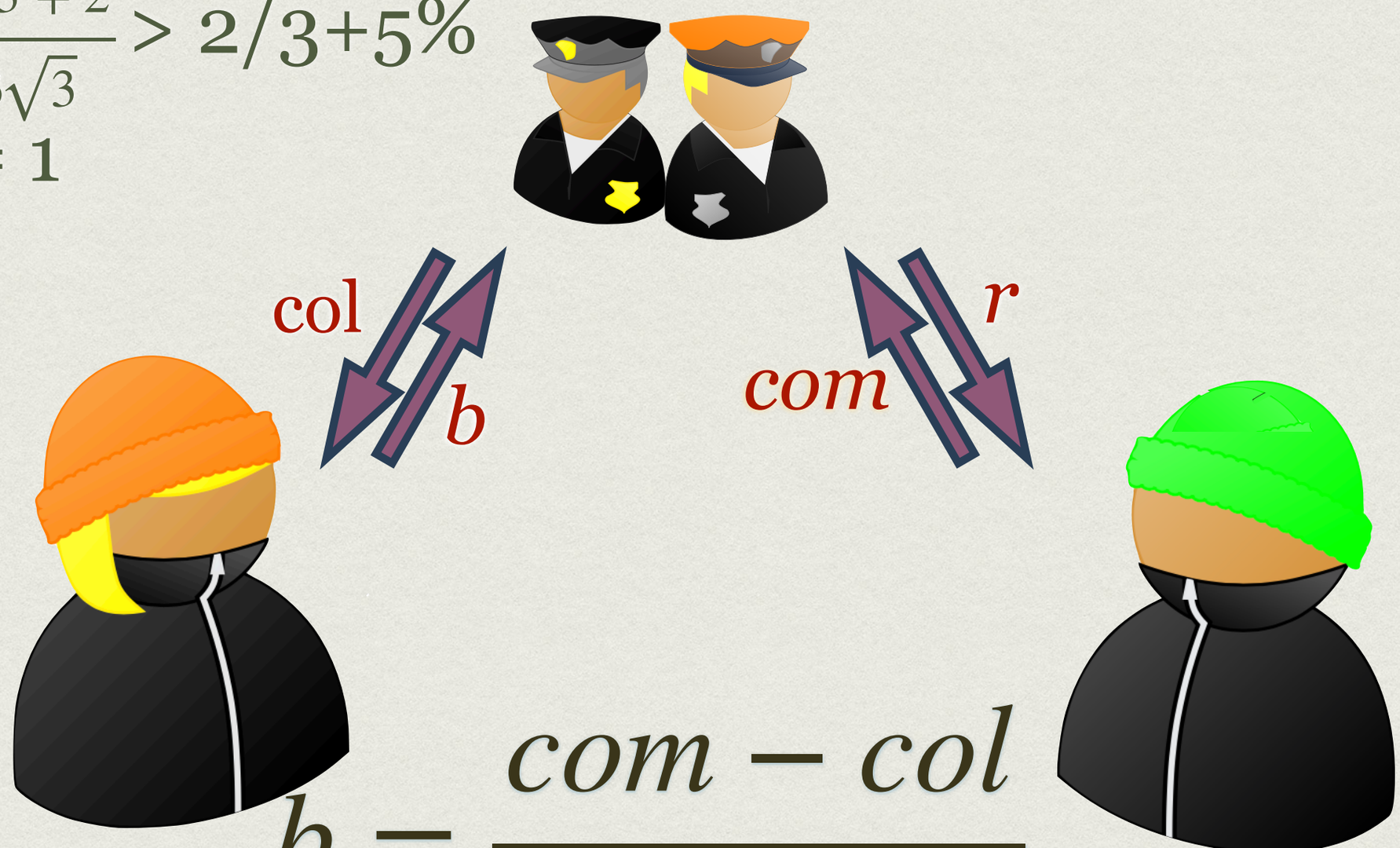
BINDING ?

$r \neq 0$

$\omega_{LHV} = 2/3$

$\omega_{QNL} = \frac{\sqrt{3}+2}{3\sqrt{3}} > 2/3 + 5\%$

$\omega_{NOSIG} = 1$



$$b = \frac{com - col}{r}$$

COMMITMENT

COMMITMENT

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

COMMITMENT

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

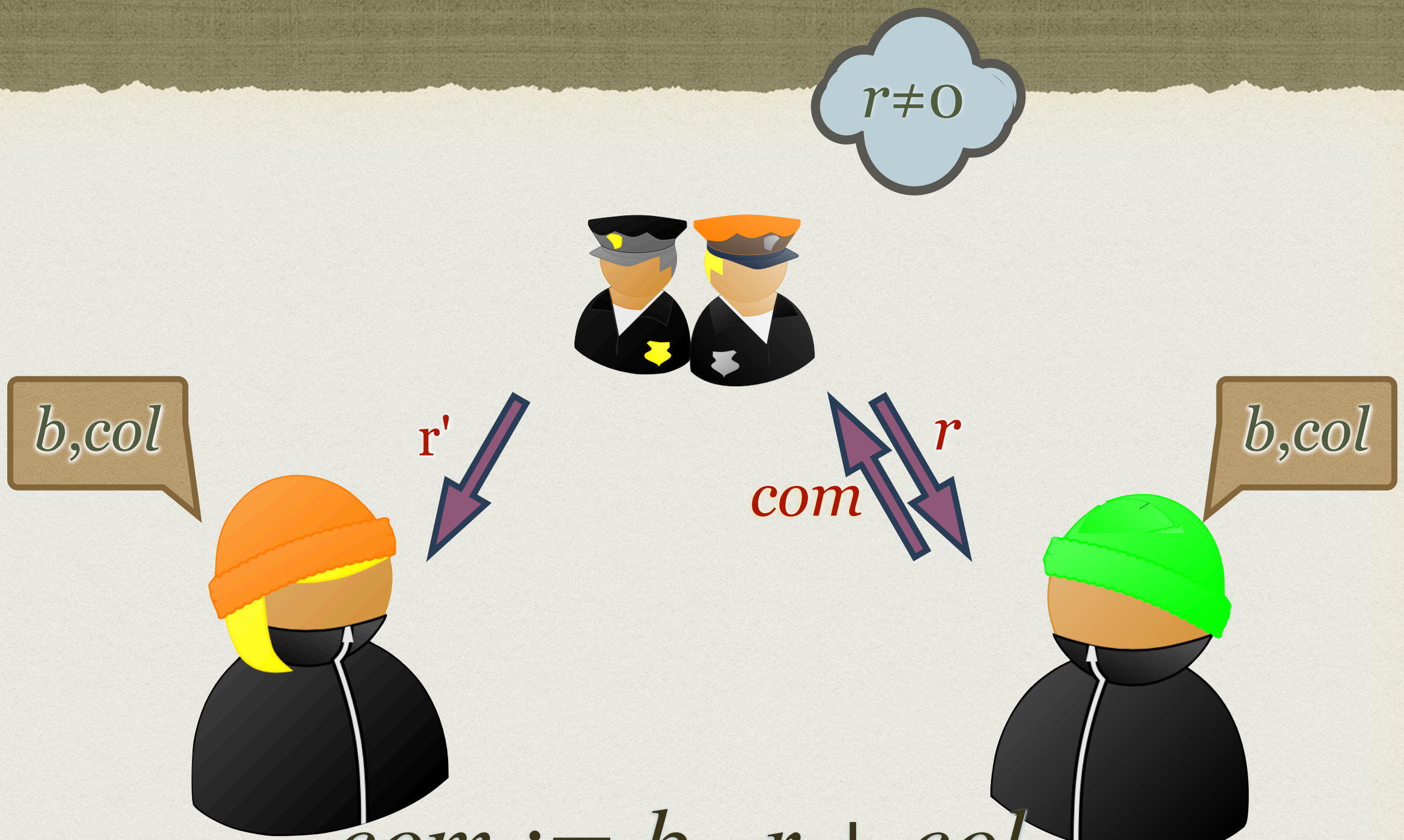
COMMITMENT

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

COMMITMENT

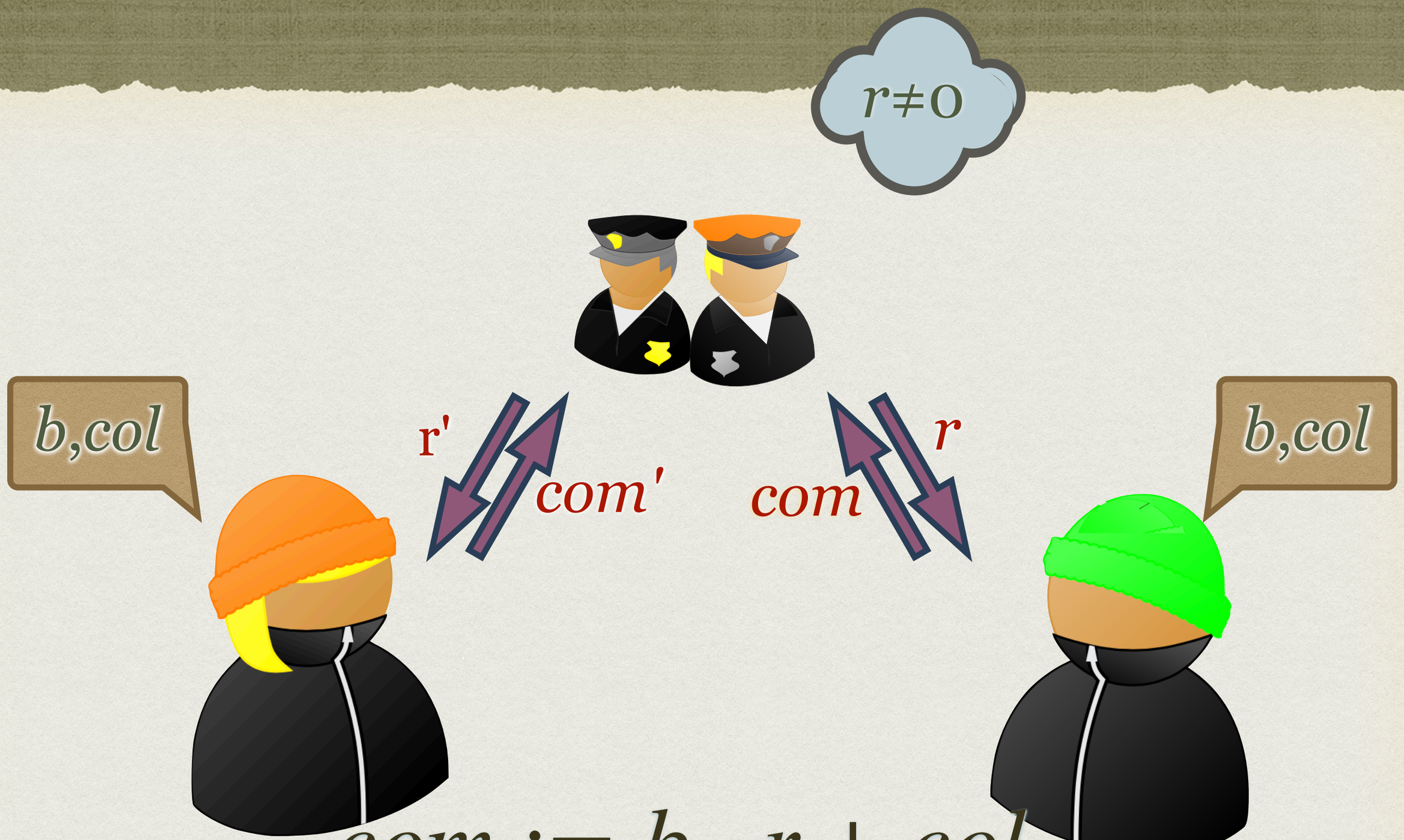
$$com := b \cdot r + col$$
$$com' := b \cdot r' + col$$

COMMITMENT



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

COMMITMENT

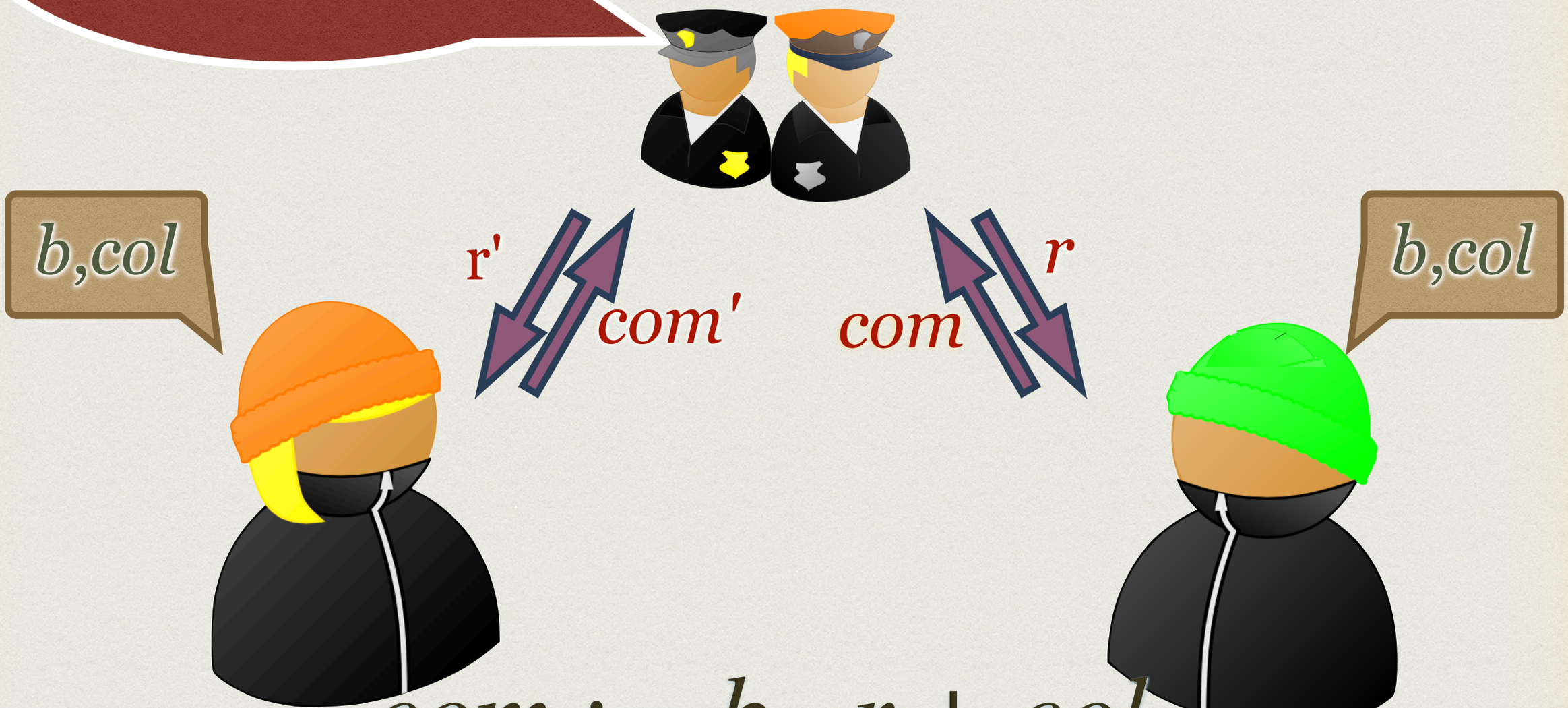


$$com := b \cdot r + col$$
$$com' := b \cdot r' + col$$

COMMITMENT

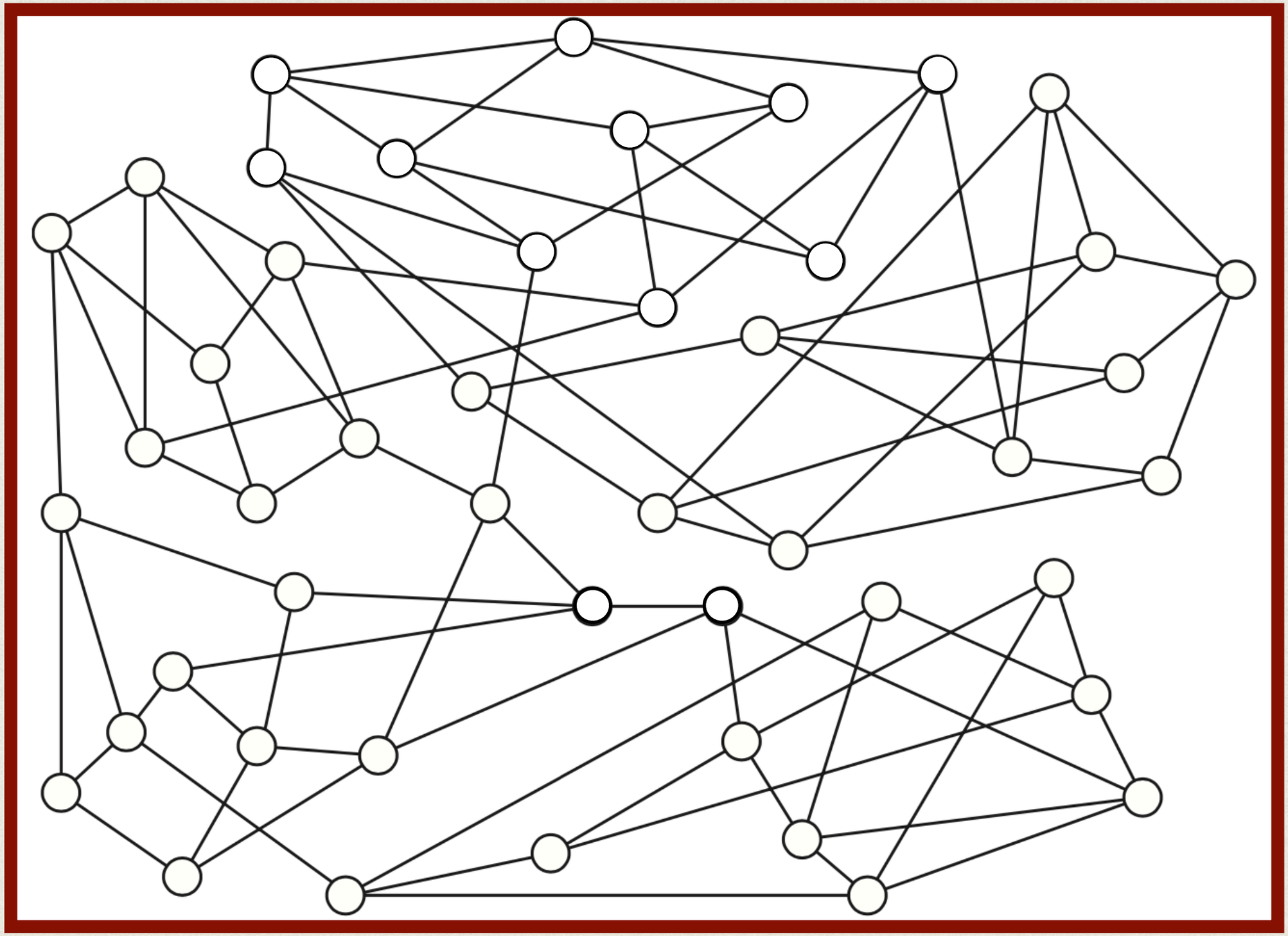
$$col = \frac{com \cdot r' - com' \cdot r}{r' - r}$$

$r \neq 0$

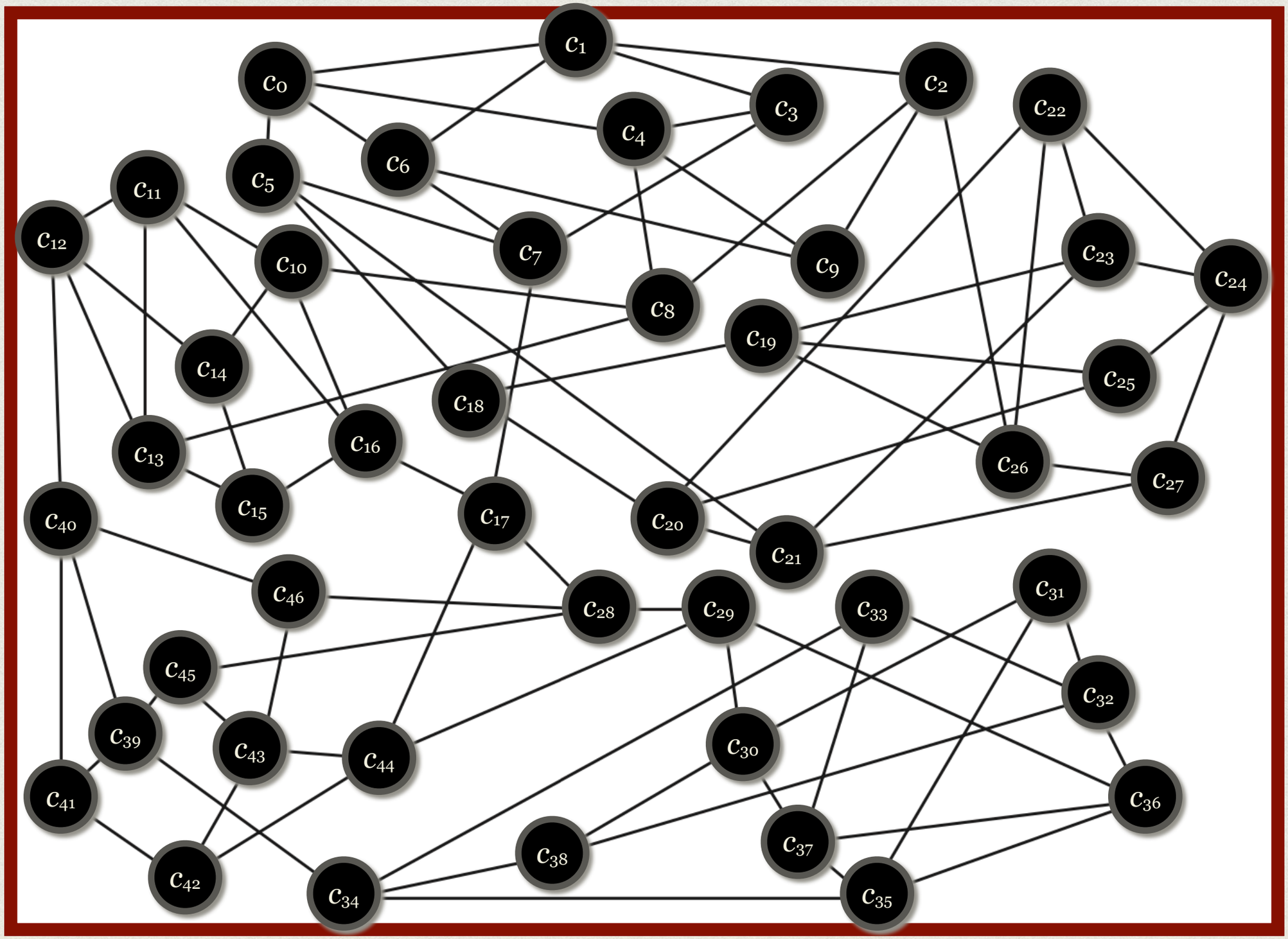


$$com := b \cdot r + col$$
$$com' := b \cdot r' + col$$

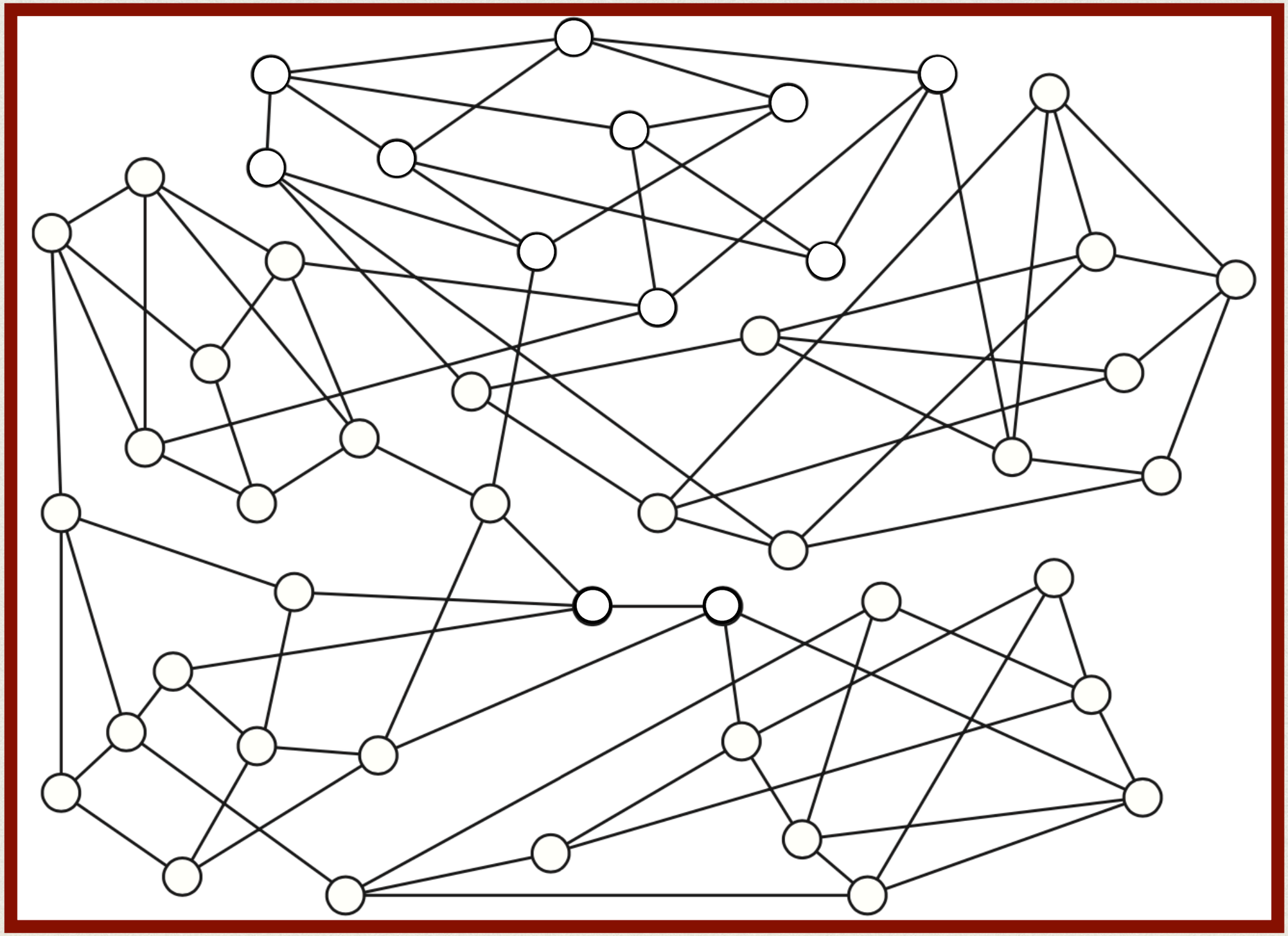
HONEST PROVERS: 3-COL



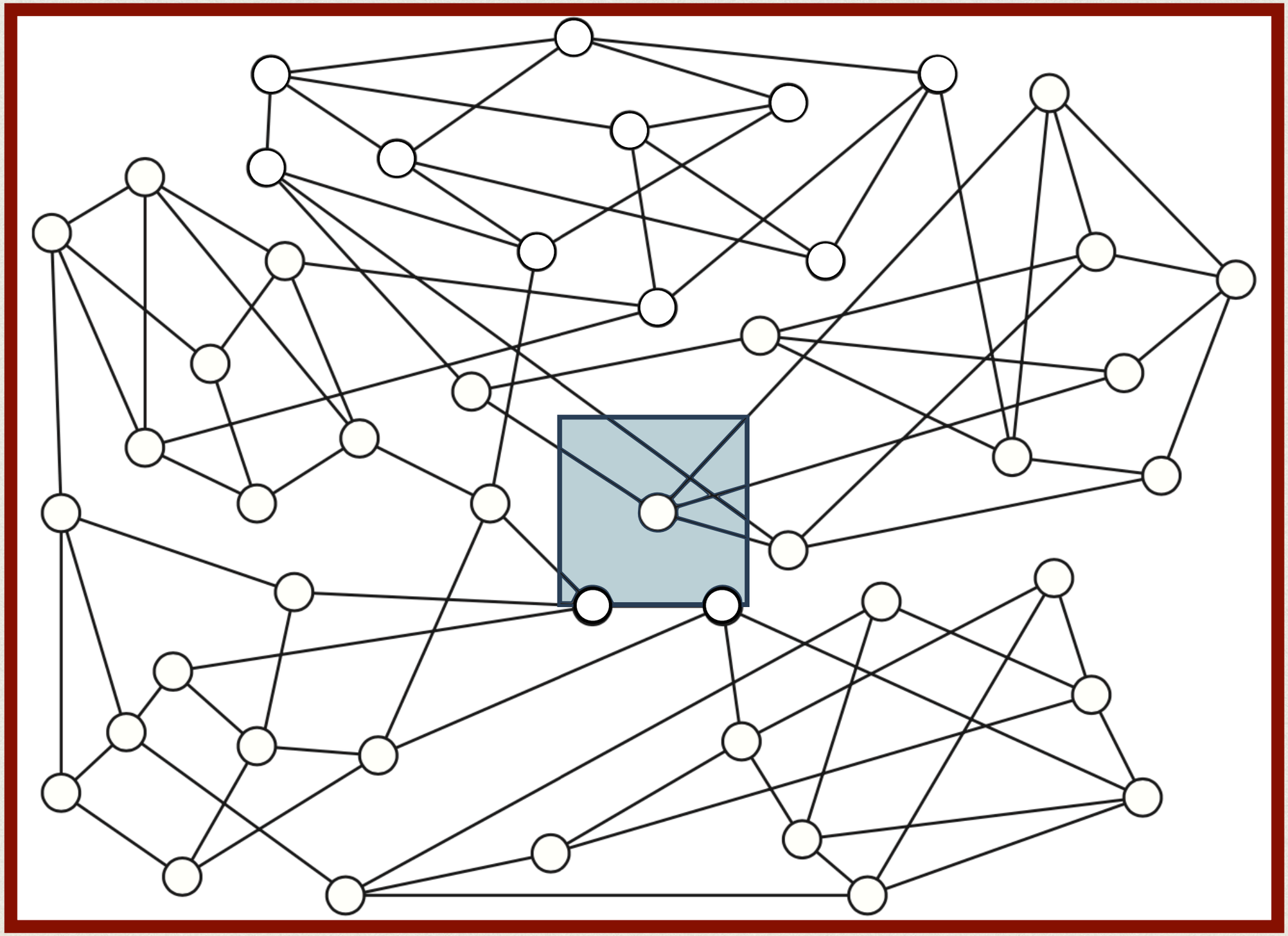
HONEST PROVERS: 3-COL



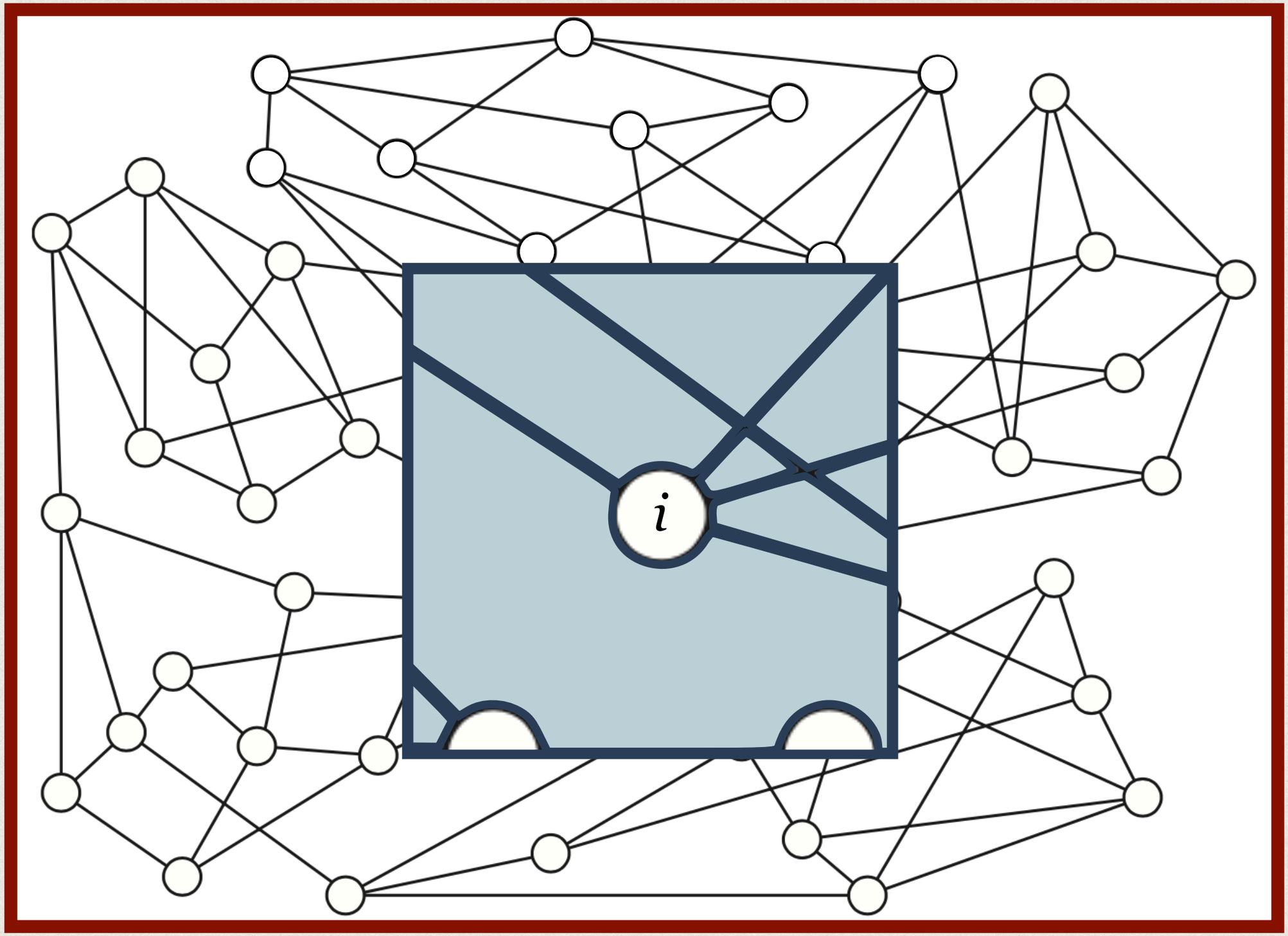
HONEST PROVERS: 3-COL



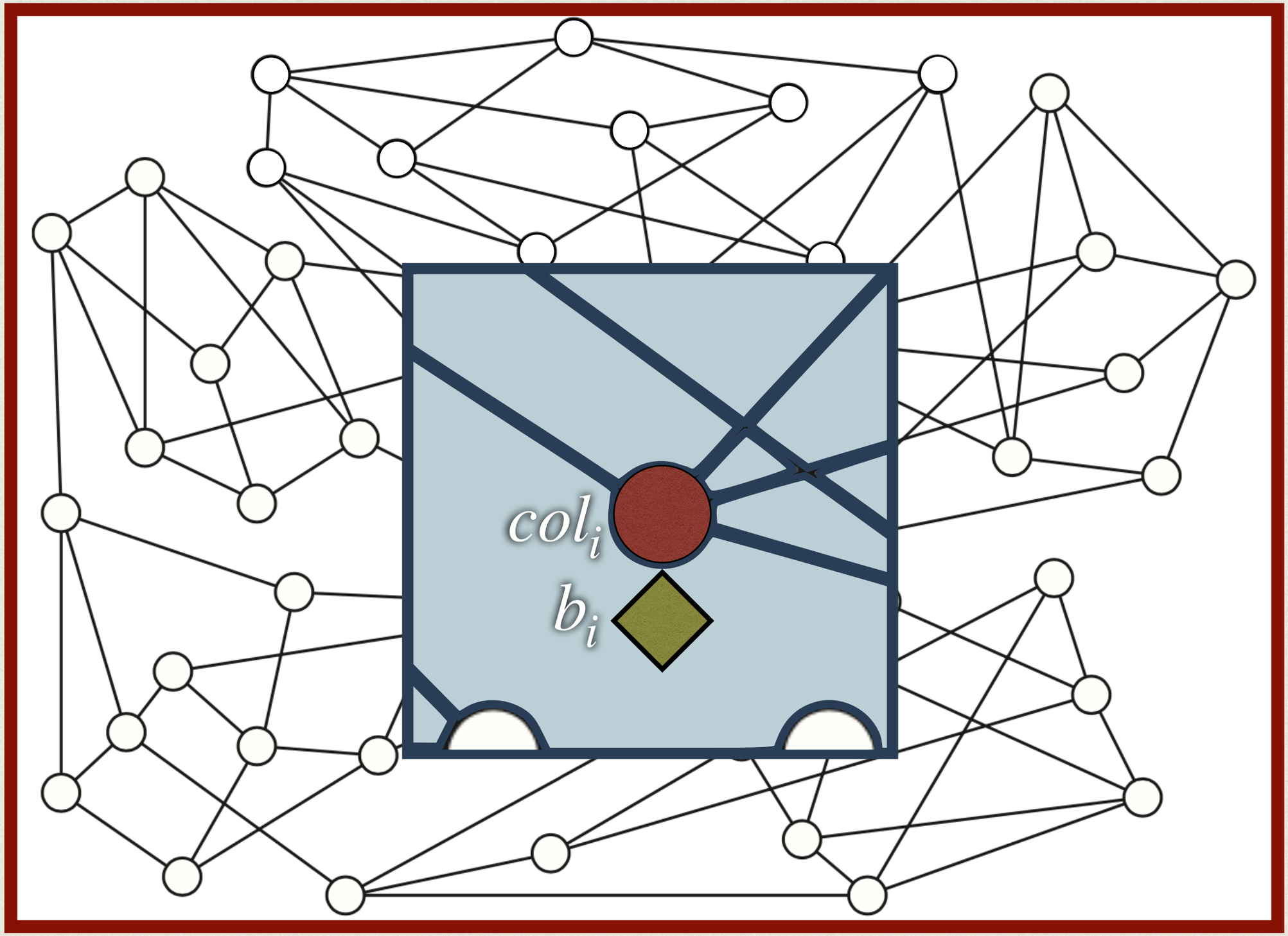
HONEST PROVERS: 3-COL



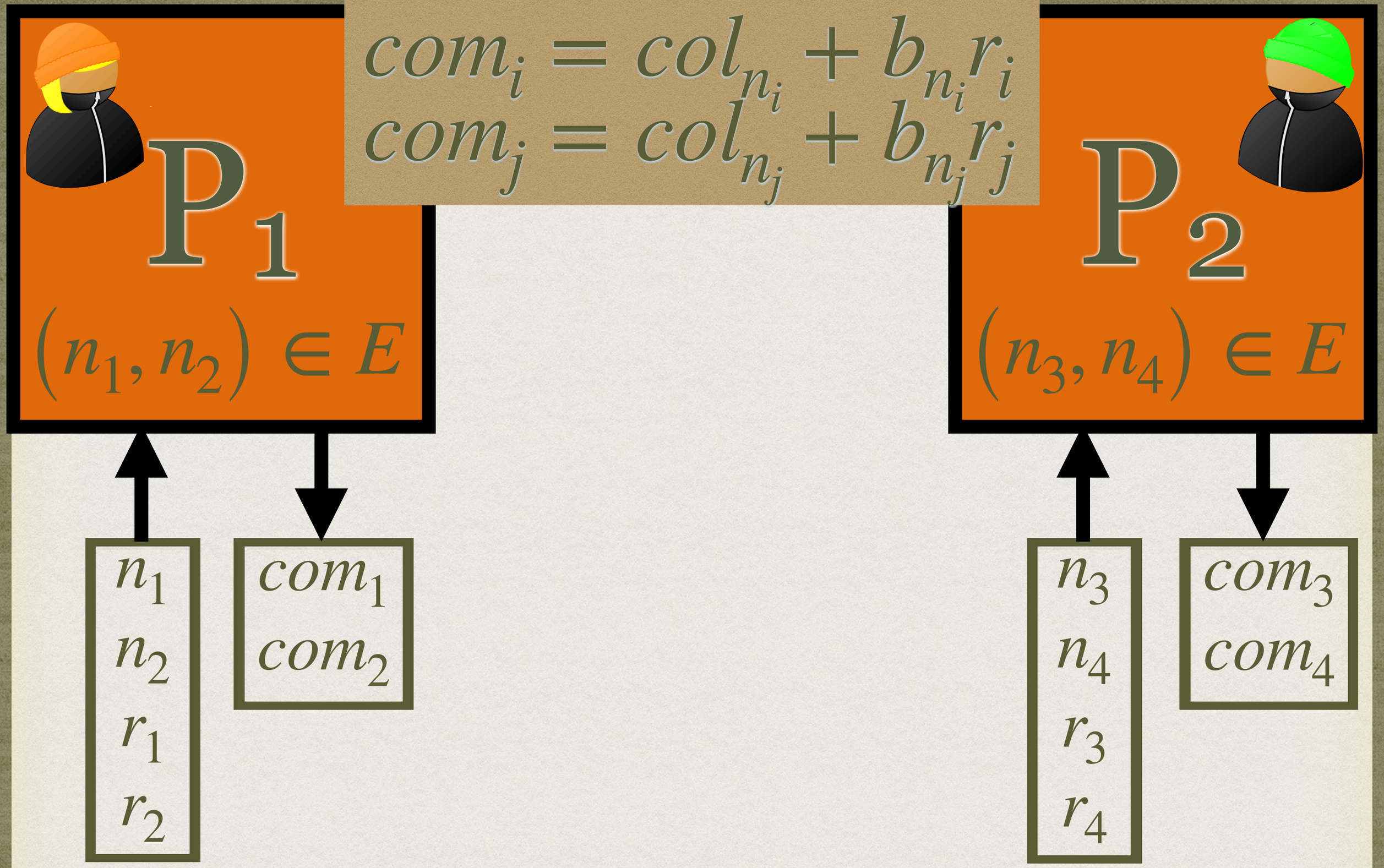
HONEST PROVERS: 3-COL



HONEST PROVERS: 3-COL



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



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

P_1

$(n_1, n_2) \in E$

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

P_2

$(n_3, n_4) \in E$

n_1
n_2
r_1
r_2

com_1
com_2

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.

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

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

n_1
n_2
r_1
r_2

com_1
com_2

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.

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

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

n_1
n_2
r_1
r_2

com_1
com_2

n_3
n_4
r_3
r_4

com_3
com_4

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

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

P_1

$(n_1, n_2) \in E$

P_2

$(n_3, n_4) \in E$

n_1
n_2
r_1
r_2

com_1
com_2

n_3
n_4
r_3
r_4

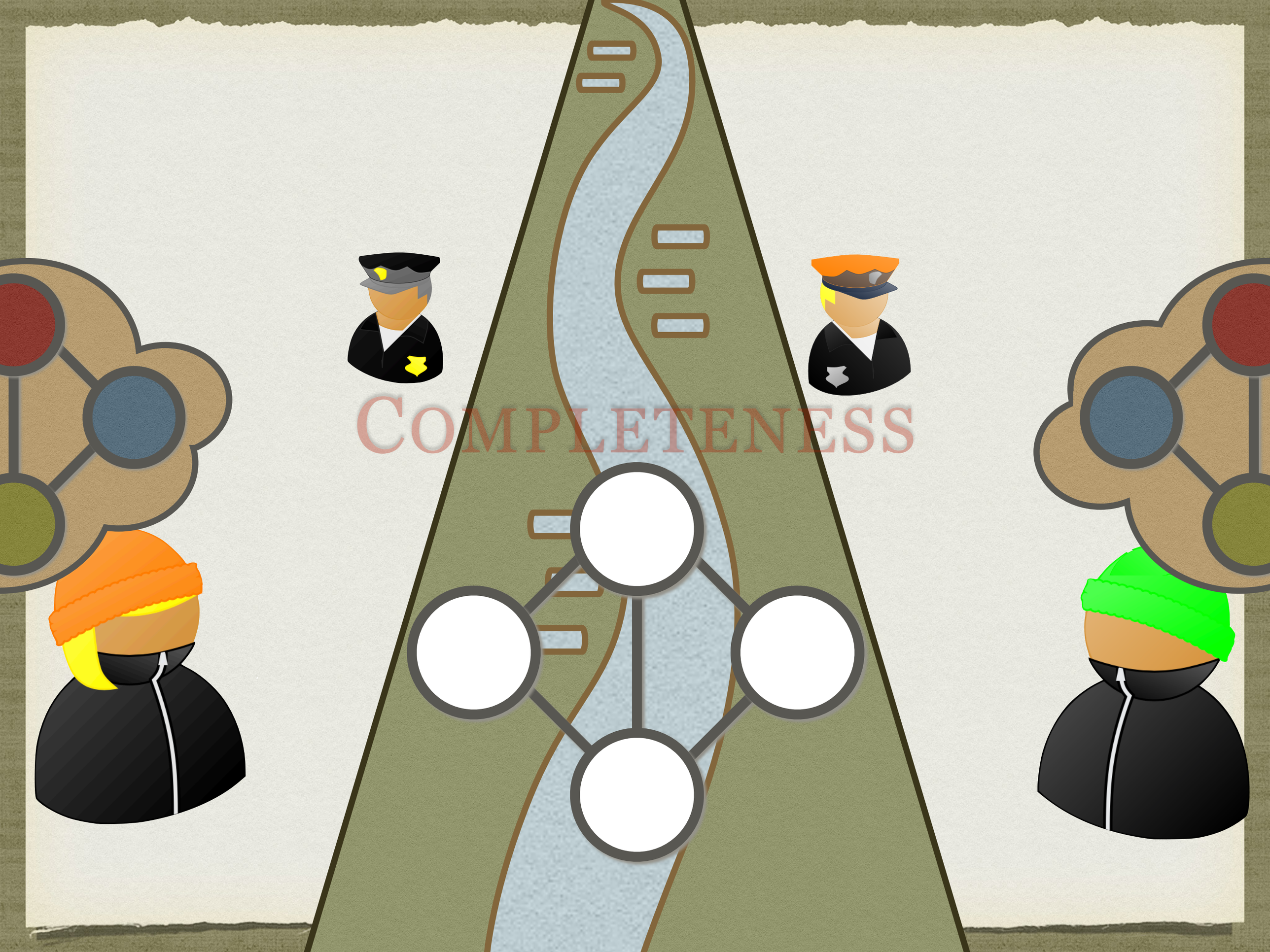
com_3
com_4

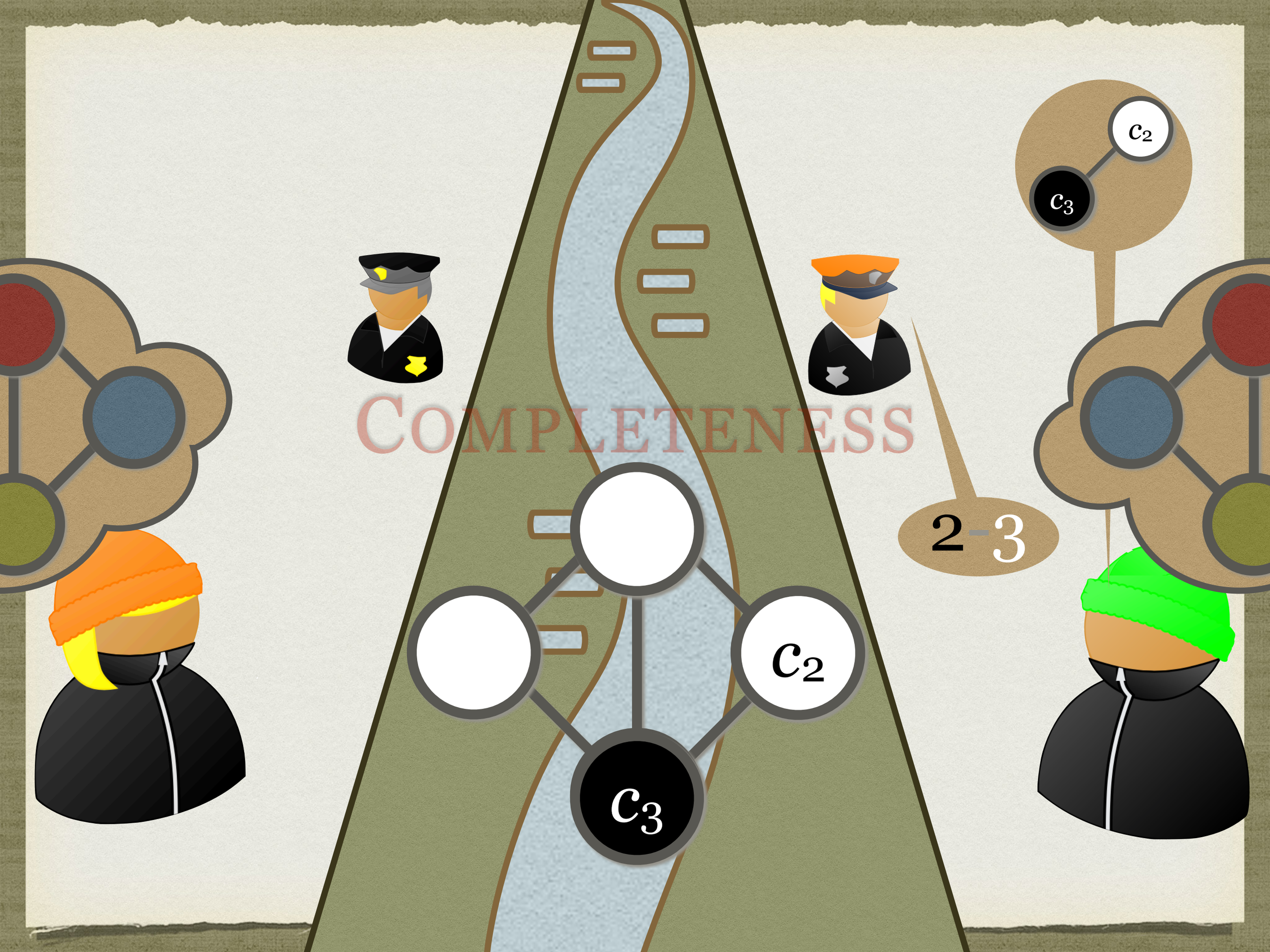
Asking two provers the same node with same r checks their consistency.

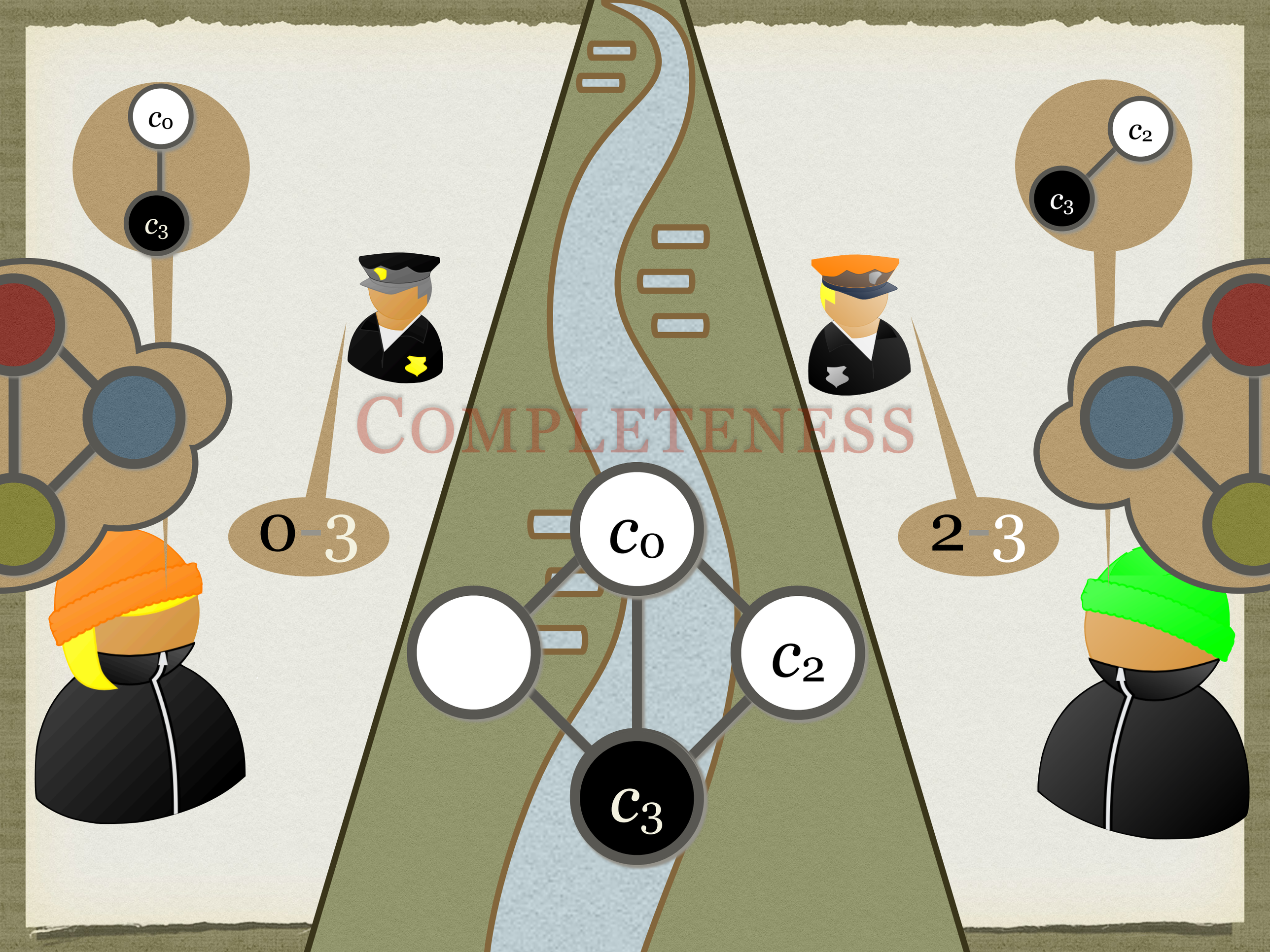
$$n_i = n_j \wedge r_i = r_j \implies com_i = com_j$$

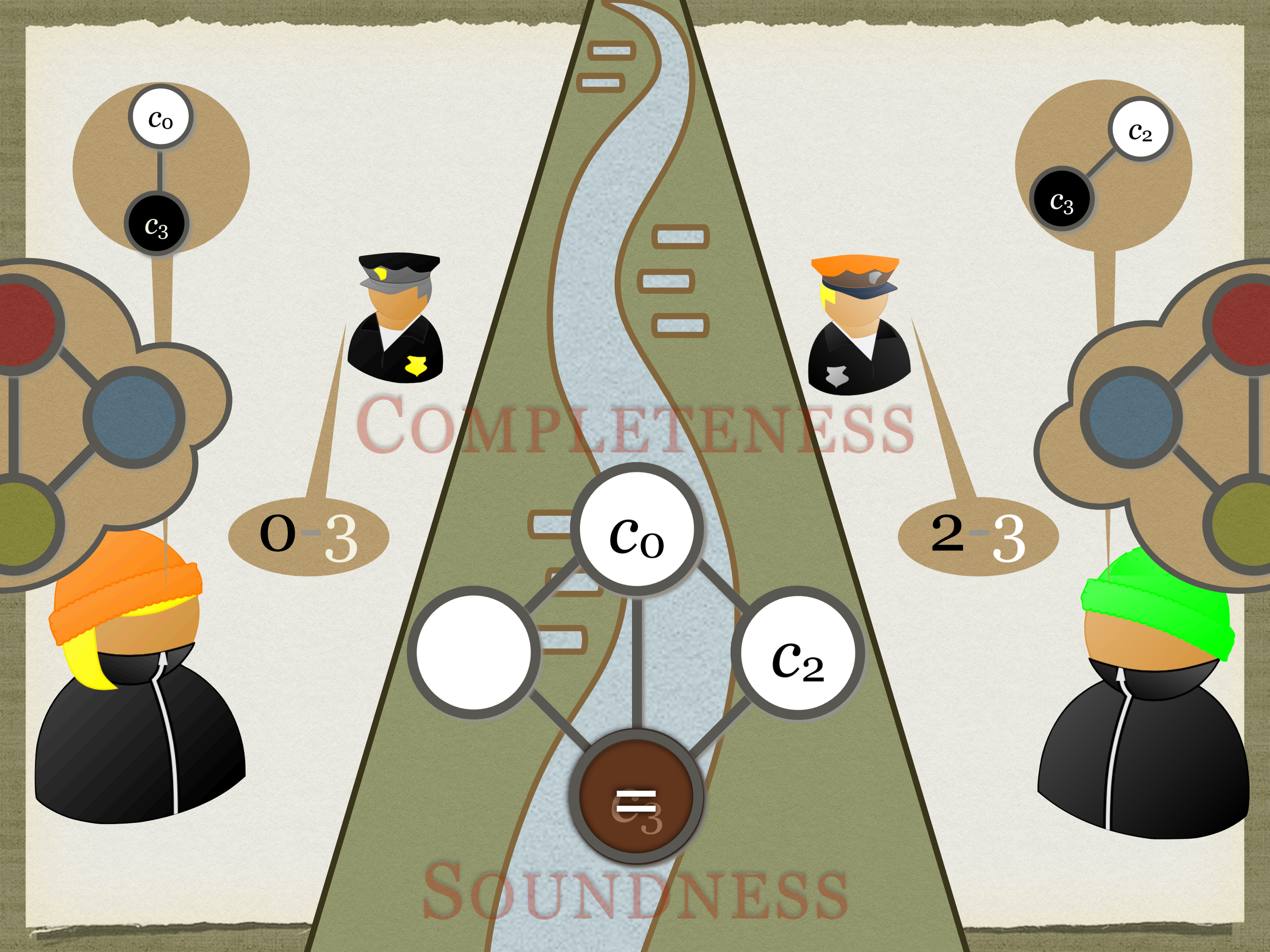
Asking two provers the same node with distinct r's unveils that node colour.

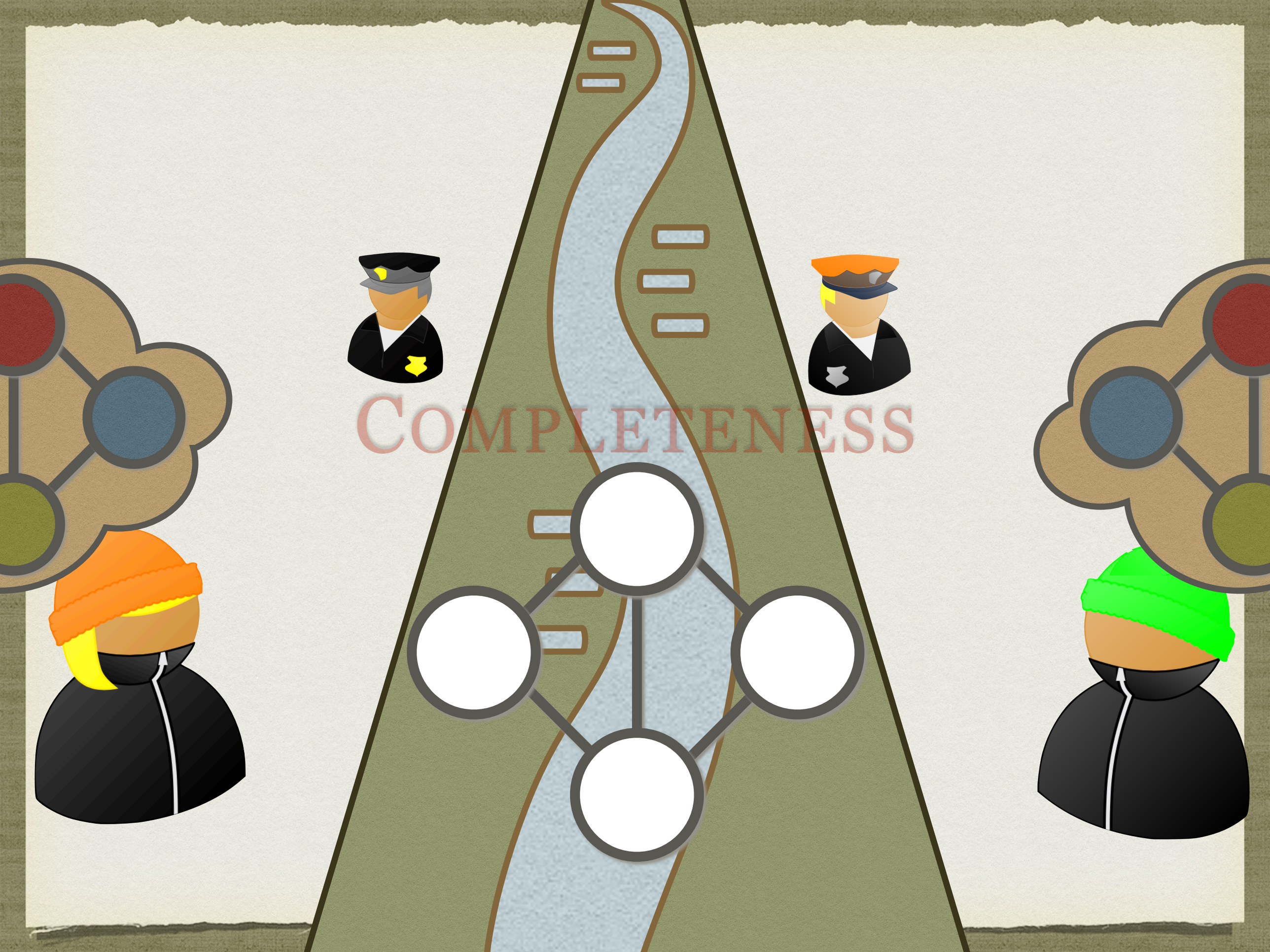
$$n_i = n_j \wedge r_i \neq r_j \implies col_{n_i} = com_i + com_j$$

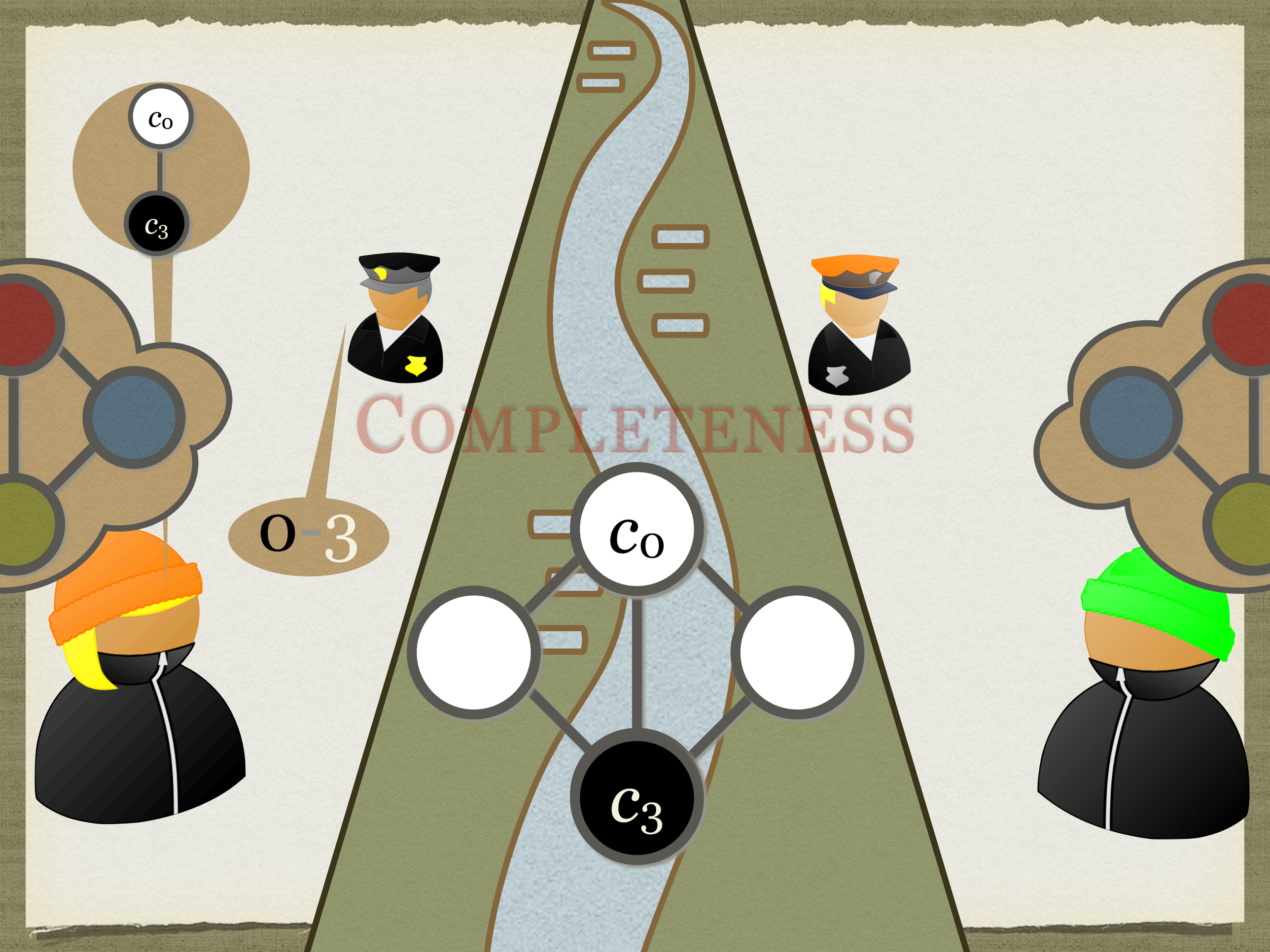

COMPLETENESS

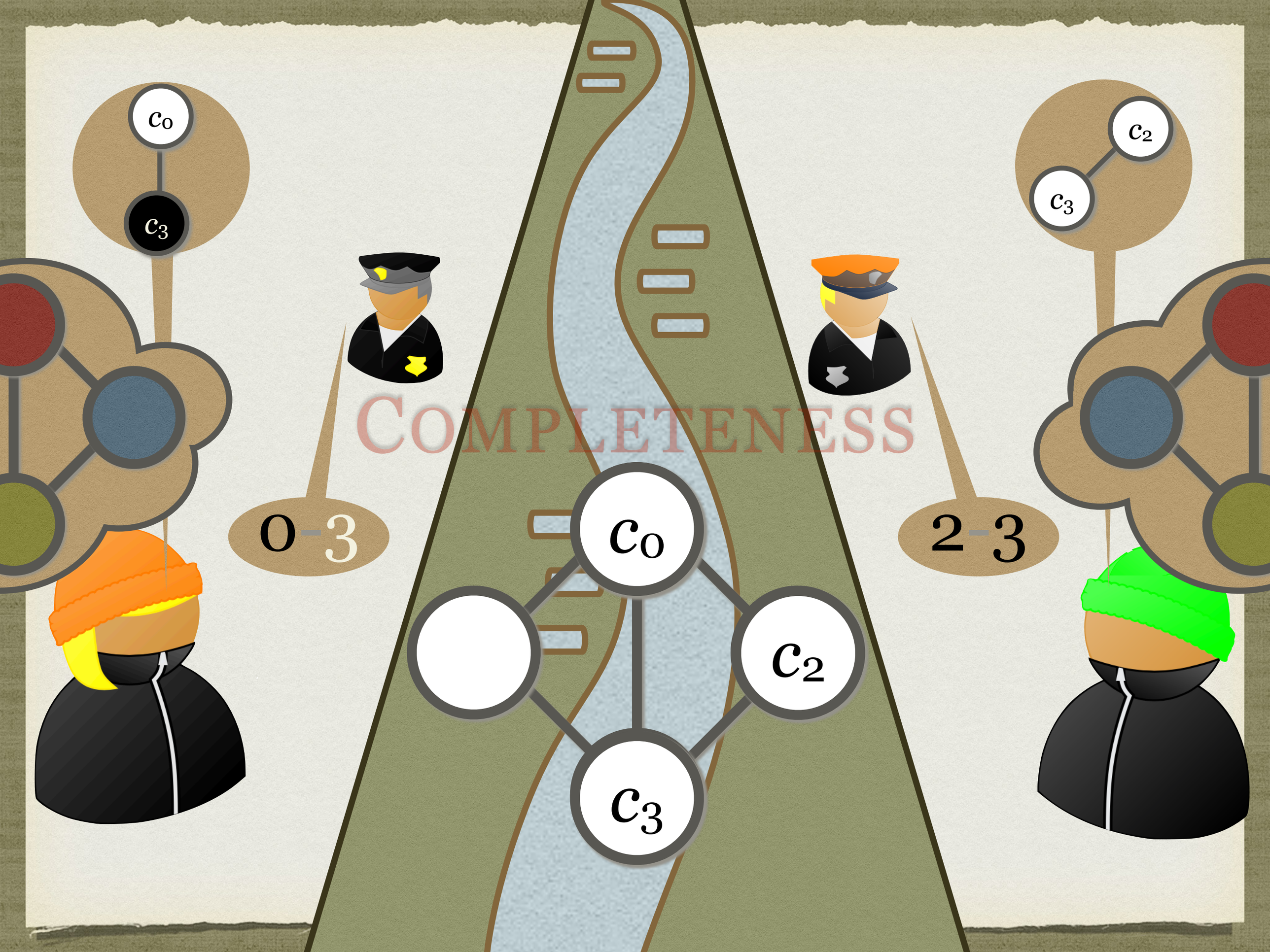

COMPLETENESS
c_2
c_3
2-3
c_2
c_3

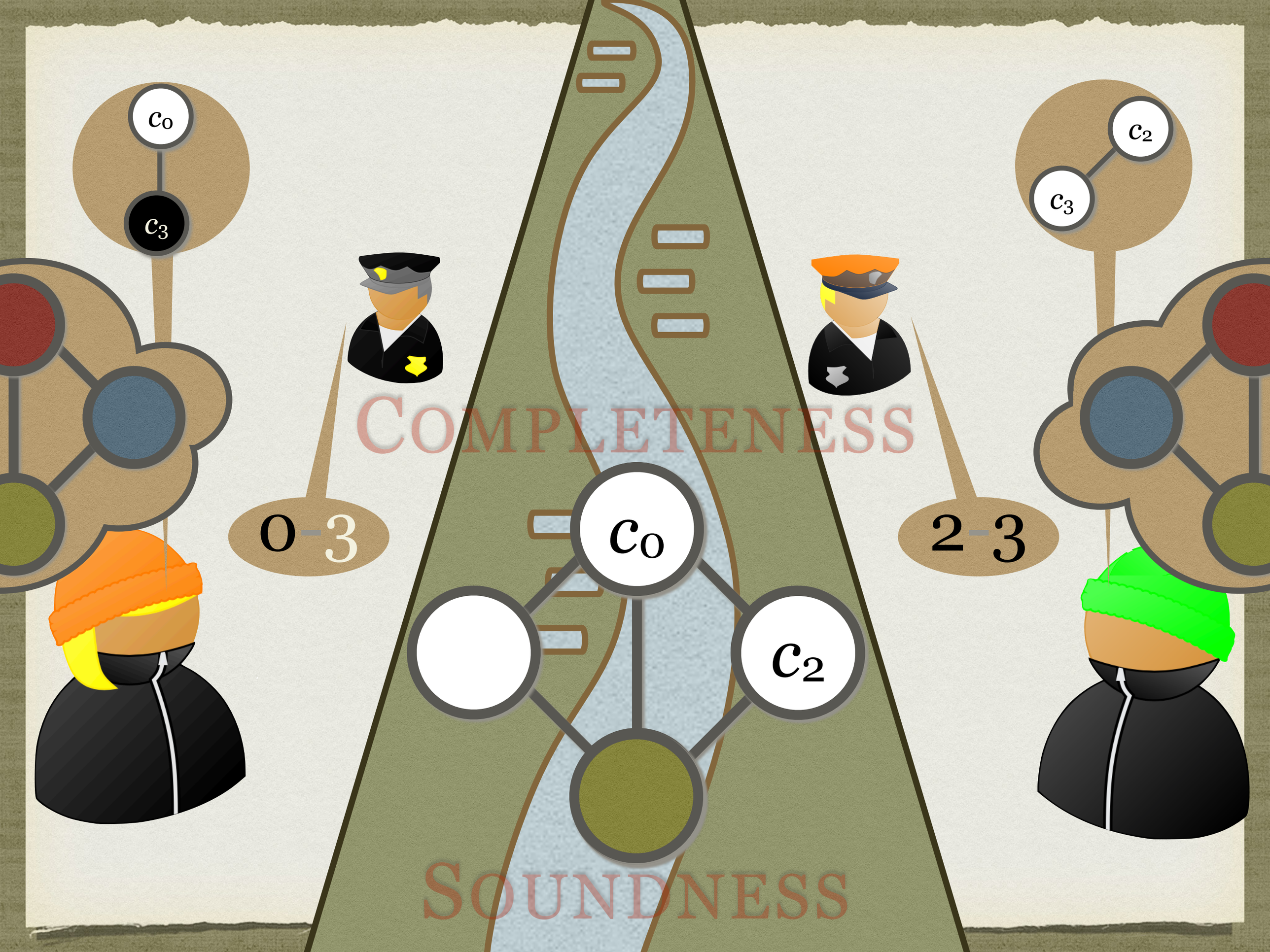

c_0
c_3
c_2
c_3
COMPLETENESS
0-3
2-3
c_0
c_2
c_3

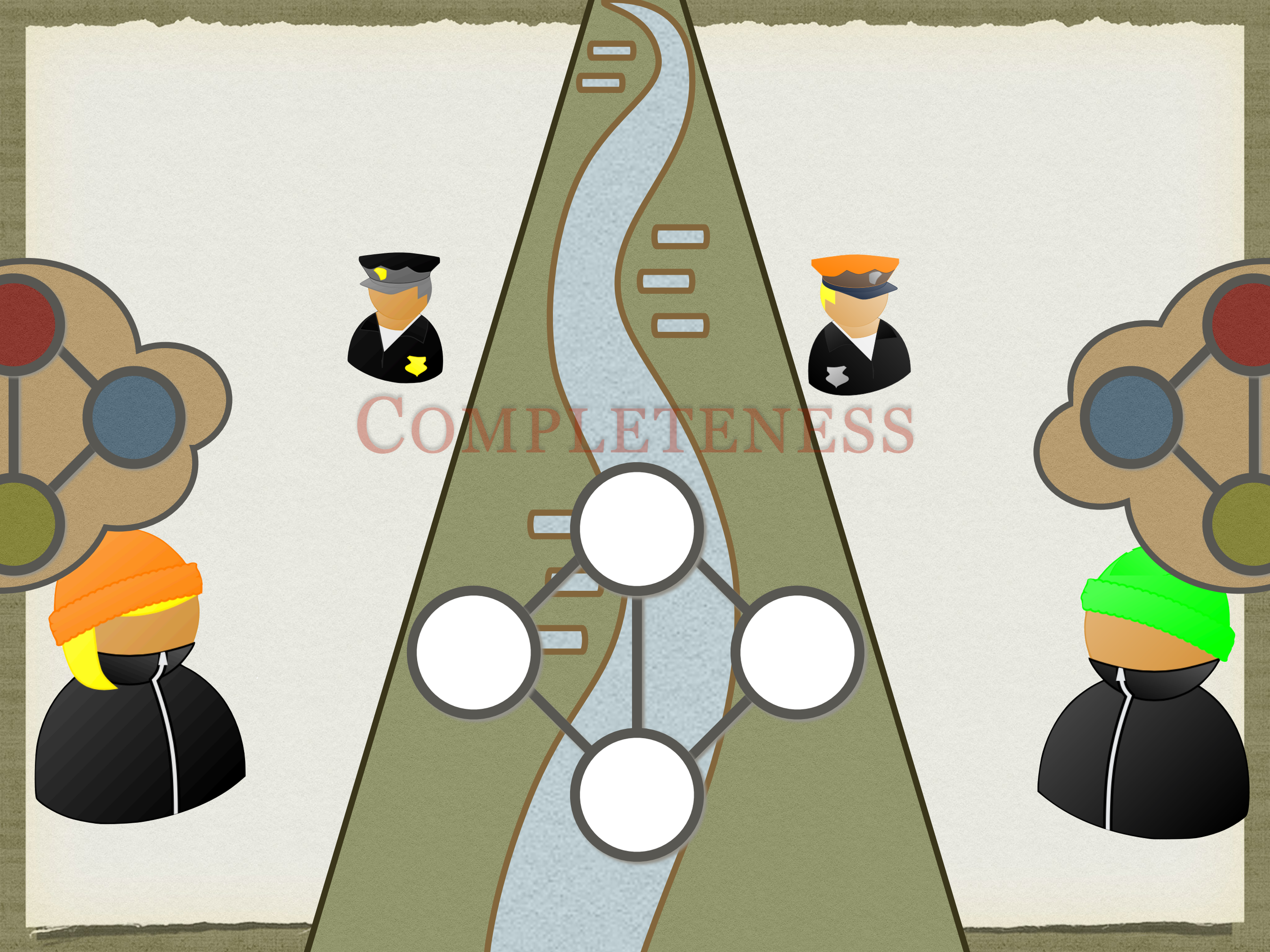

c_0
c_3
c_2
c_3
0-3
2-3
c_0
c_2
c_3
Completeness
Soundness

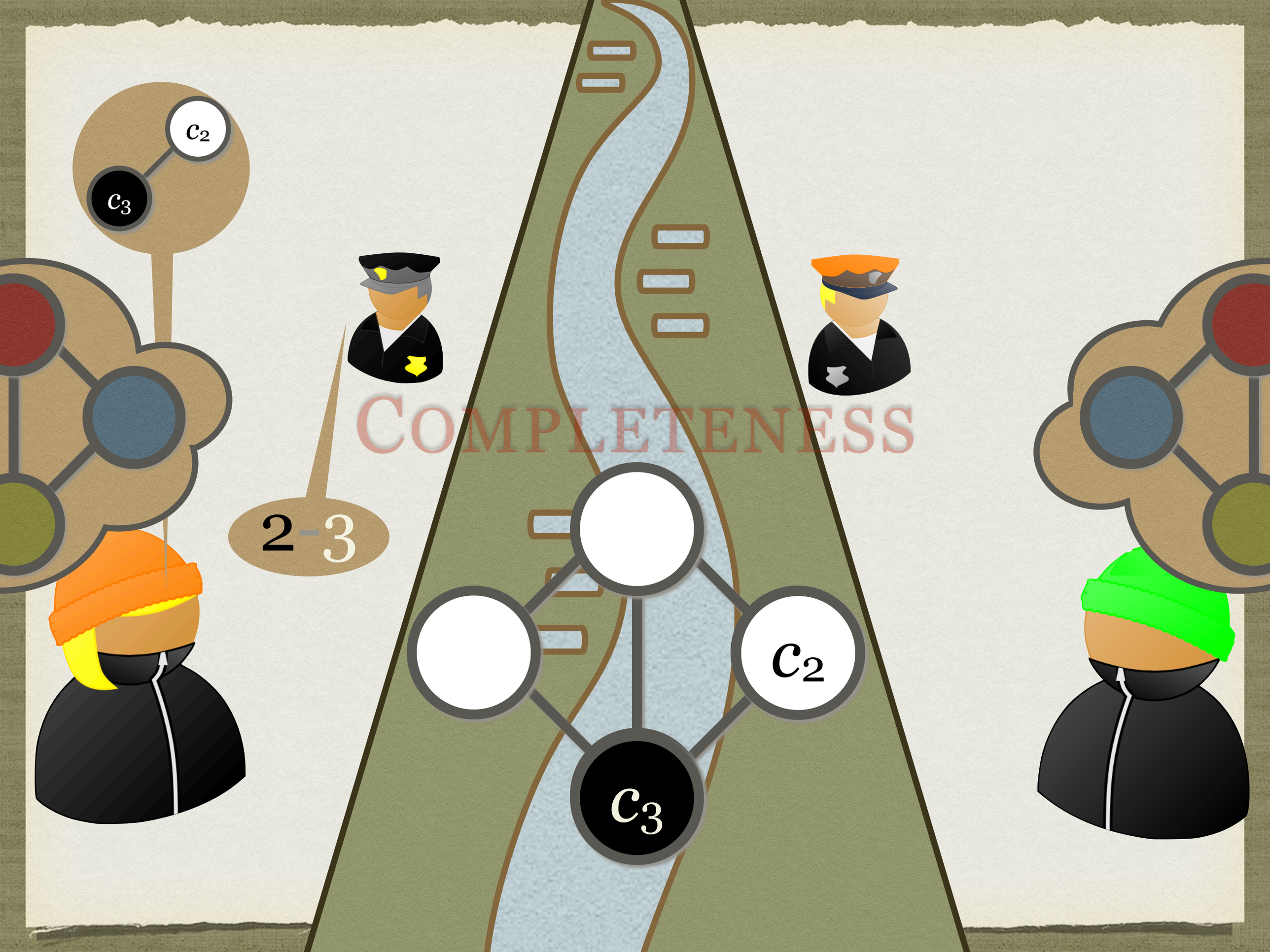

COMPLETENESS

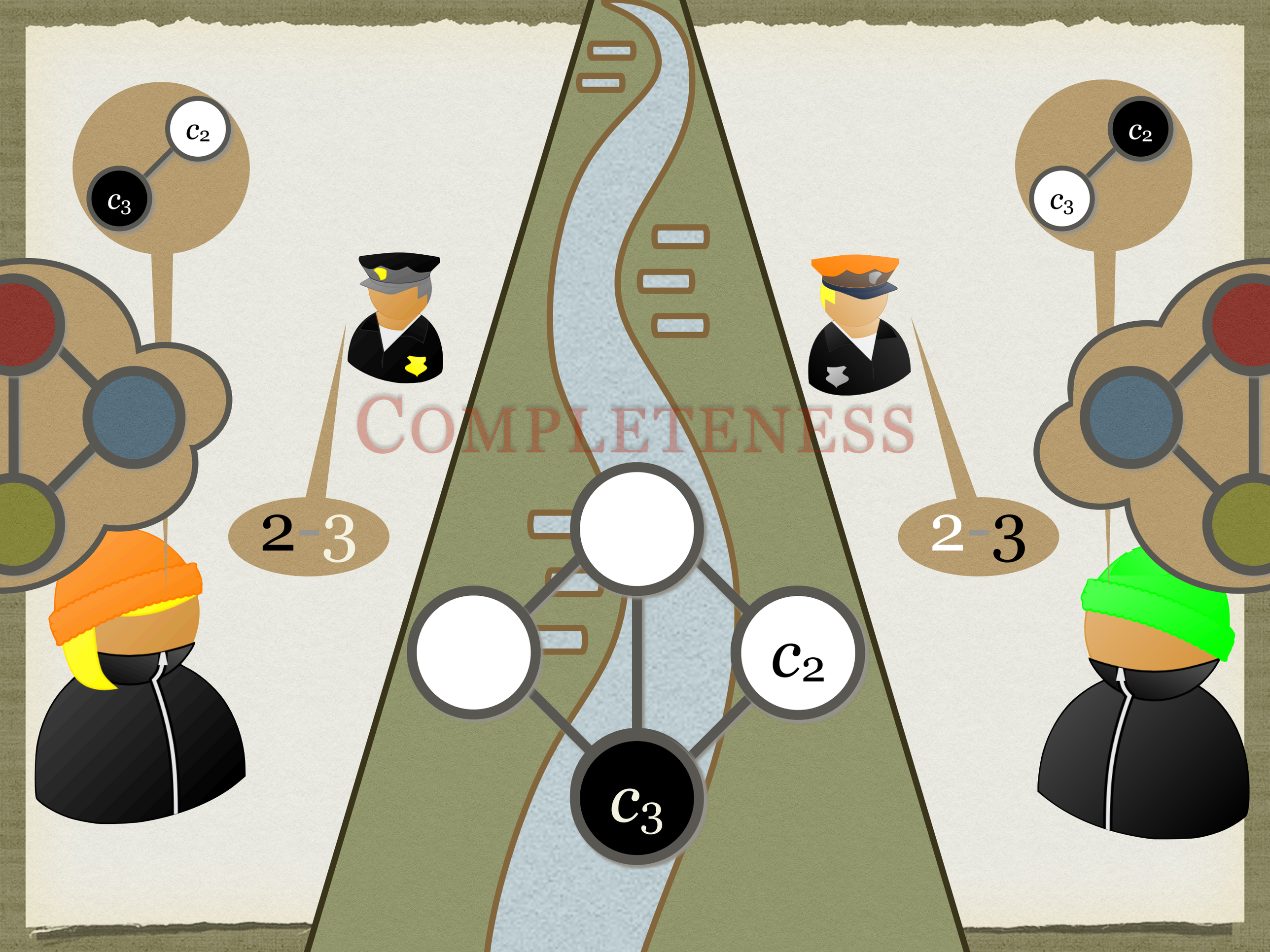

c_0
c_3
0-3
COMPLETENESS
c_0
c_3

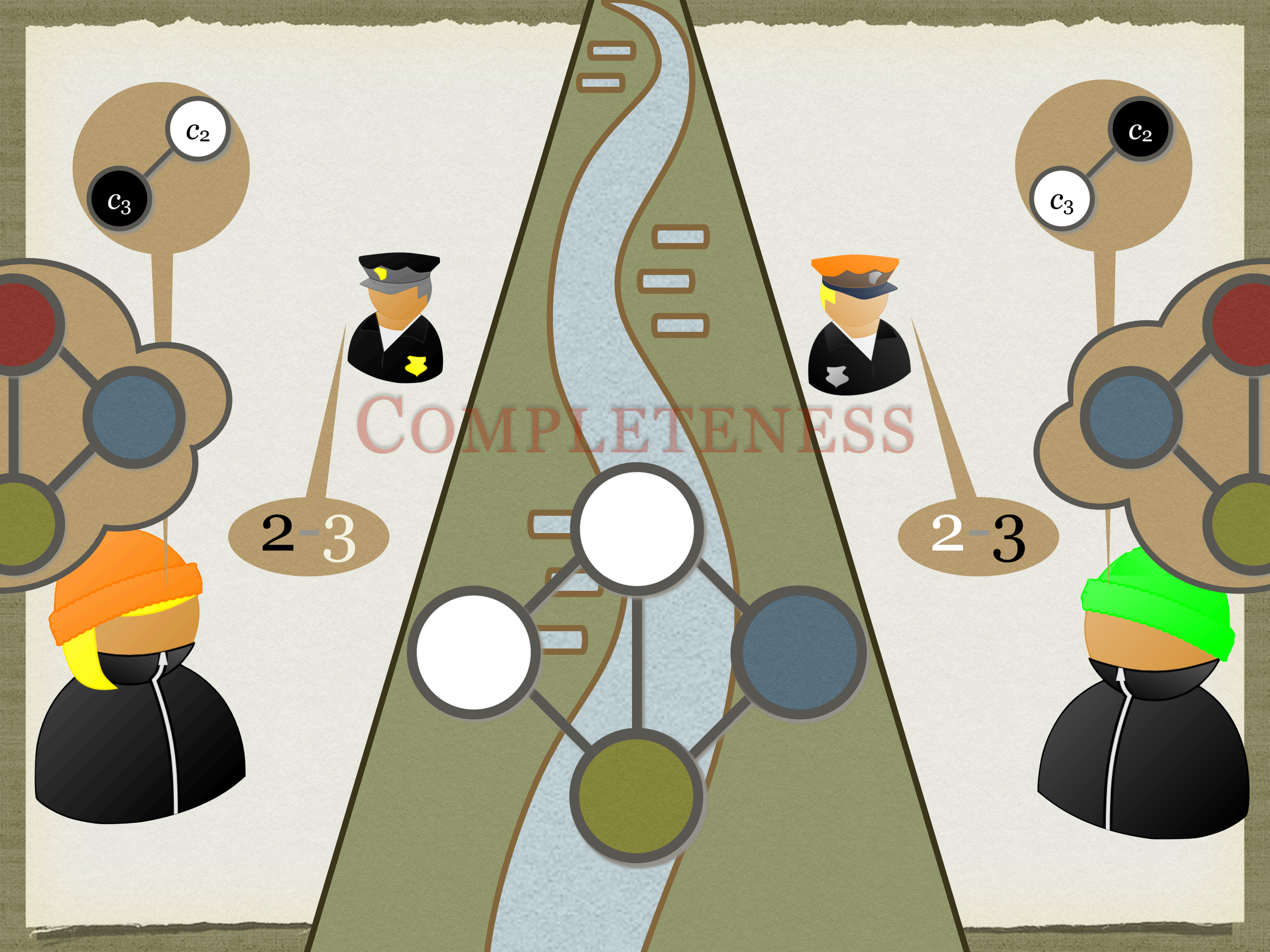

c_0
c_3
c_2
c_3
0-3
2-3
c_0
c_2
c_3
COMPLETENESS

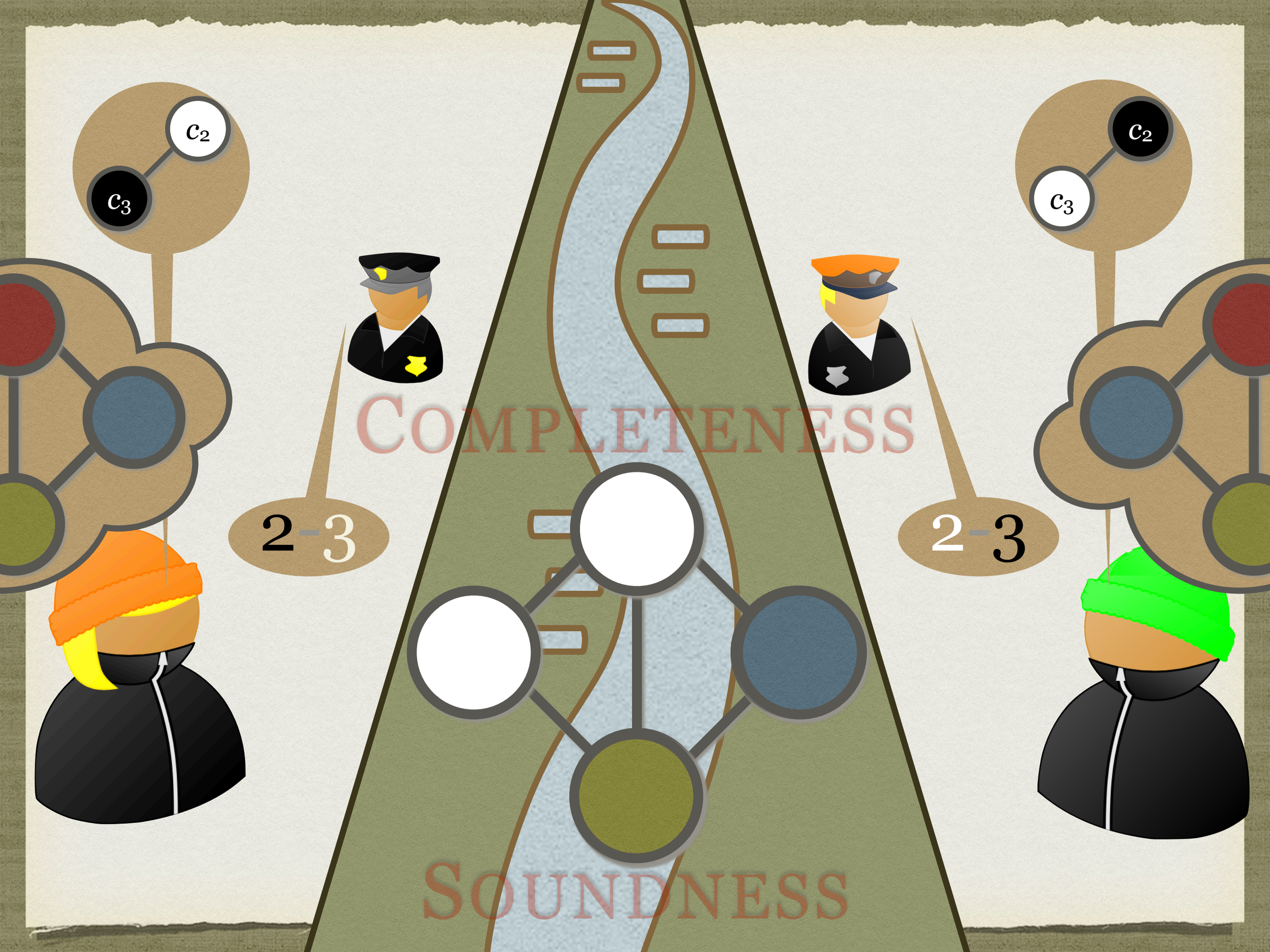

c_0
c_3
c_2
c_3
0-3
2-3
c_0
c_2
COMPLETENESS
SOUNDNESS


COMPLETENESS


c_2
c_3
2-3
COMPLETENESS
c_2
c_3


c_2
c_3
2-3
c_2
c_3
2-3
c_2
c_3
COMPLETENESS


c_2
c_3
2-3
COMPLETENESS
c_2
c_3
2-3


c_2
c_3
2-3
COMPLETENESS
SOUNDNESS
c_2
c_3
2-3

SOUNDNESS ANALYSIS

LHV

edge-verification test = 1/9

well-definition test = 8/9

SOUNDNESS ANALYSIS

LHV

edge-verification test = 1/9

well-definition test = 8/9

$$\omega_{LHV} \leq 1 - \frac{1}{9|E|}$$

SOUNDNESS ANALYSIS

LHV

edge-verification test = 1/9

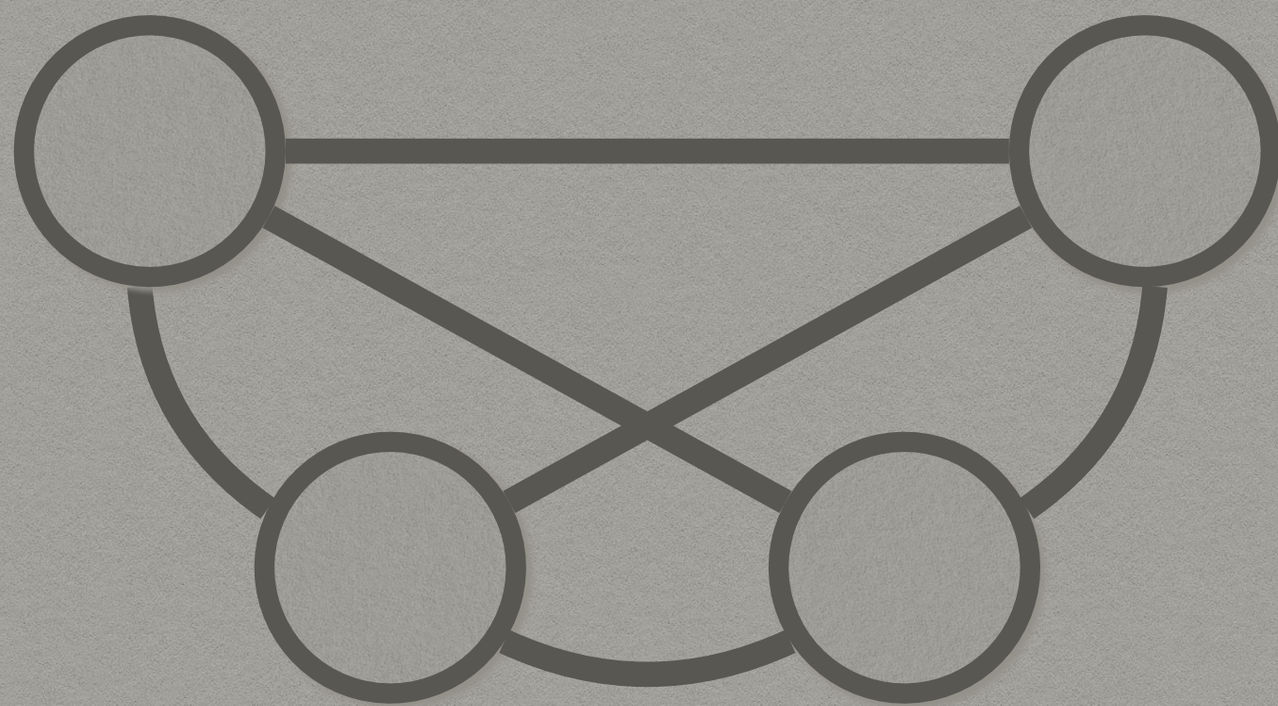
well-definition test = 8/9

$$\omega_{LHV} \leq 1 - \frac{1}{9|E|}$$

$9|E|k$ repetitions

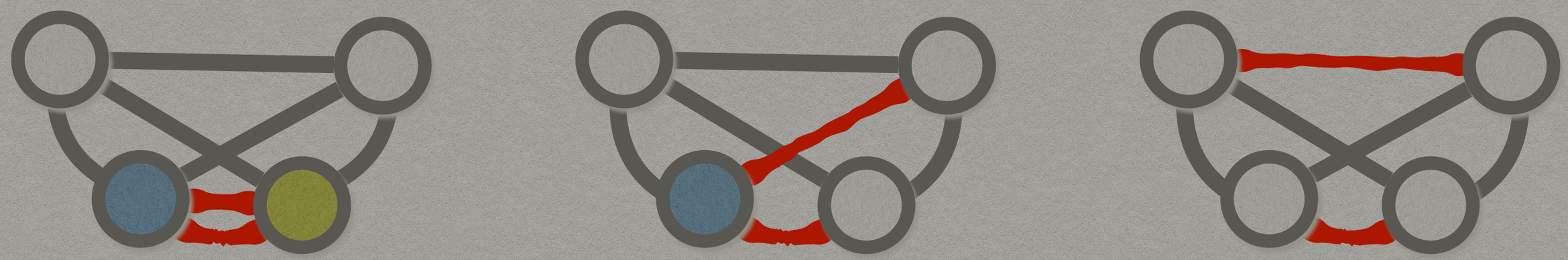
$$\omega_{LHV} \leq e^{-k}$$

ZK SIMULATION

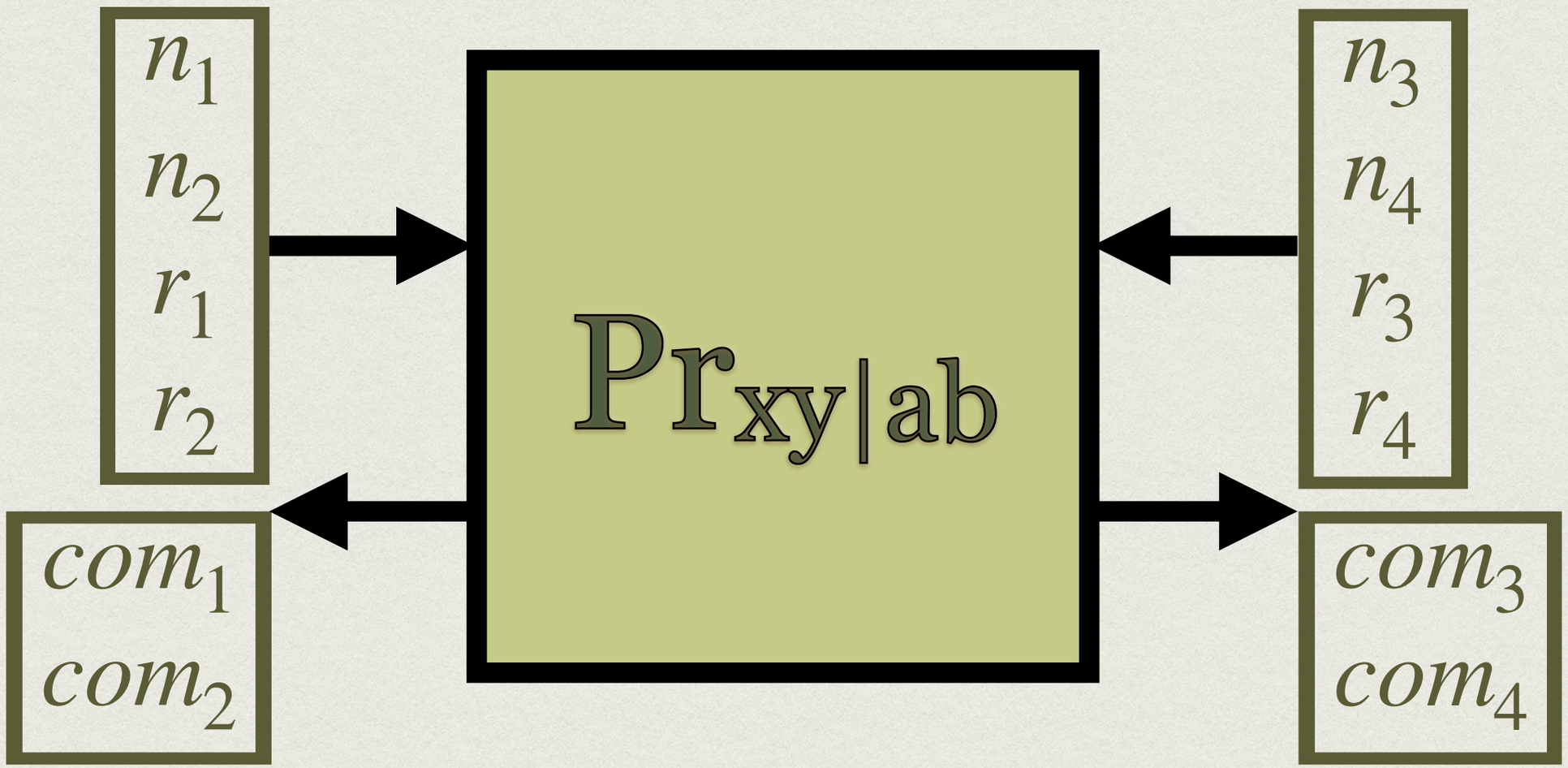


K_4

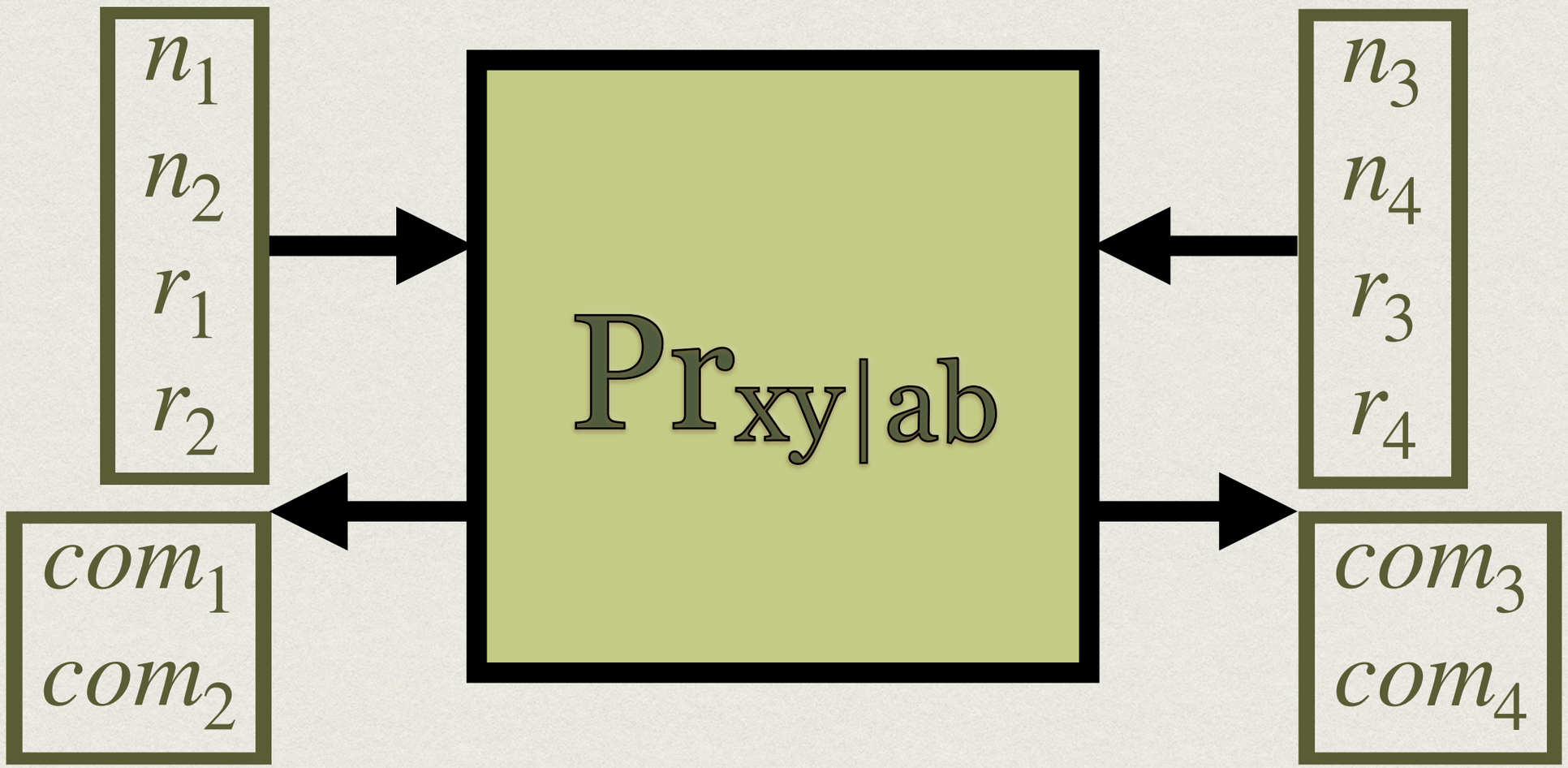
ZK SIMULATION



CASE ANALYSIS

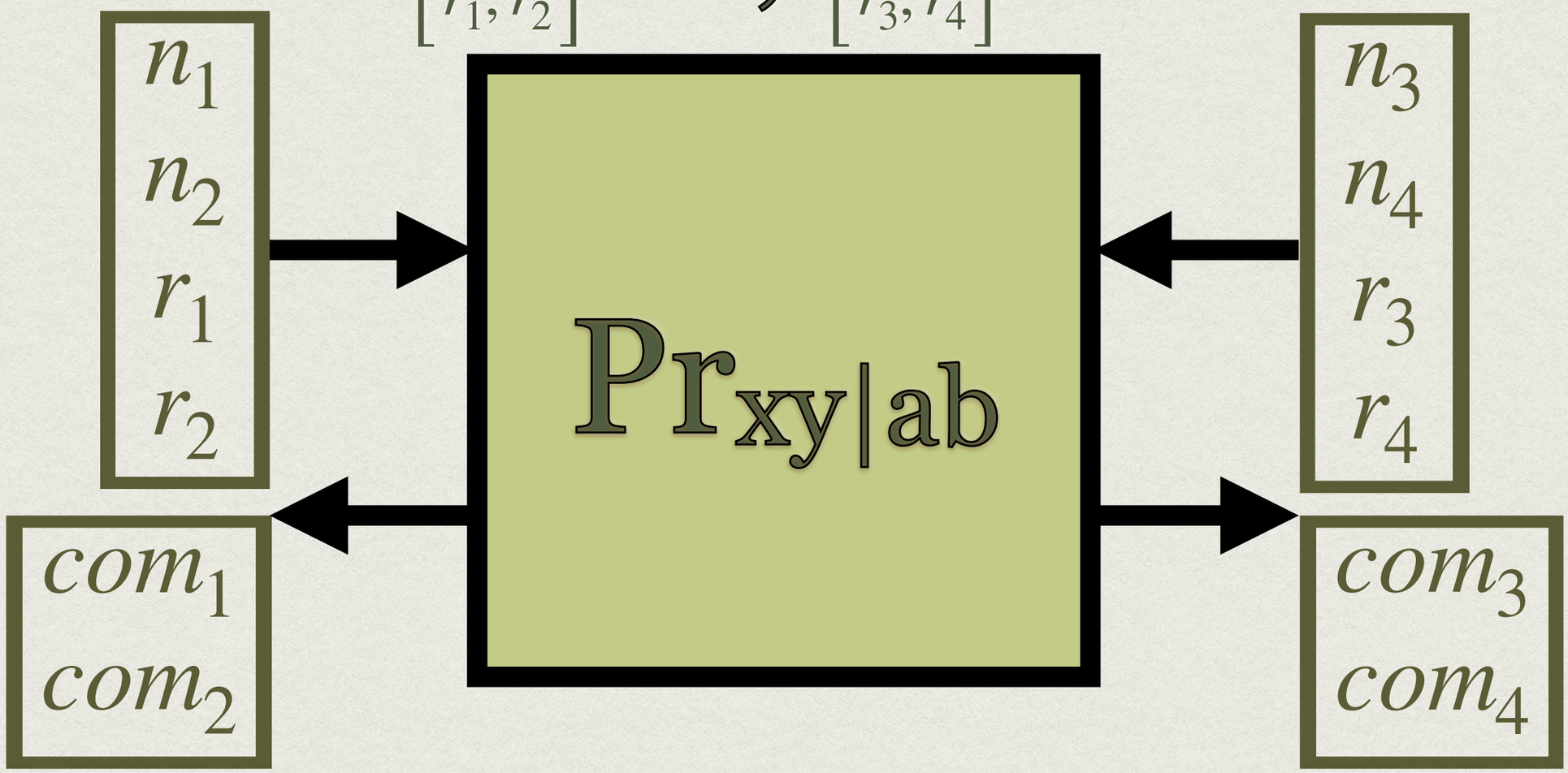

n_1
n_2
r_1
r_2
$\mathrm{Pr}_{xy|ab}$
n_3
n_4
r_3
r_4
com_1
com_2
com_3
com_4

A,B: <u>infinite</u> sets

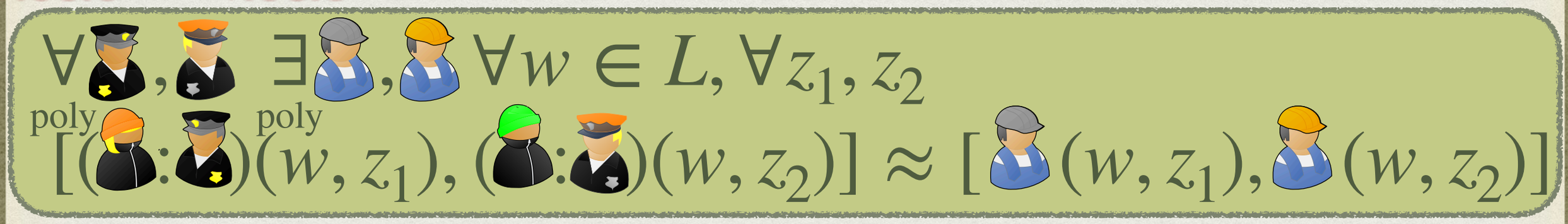


A,B: <u>infinite</u> sets

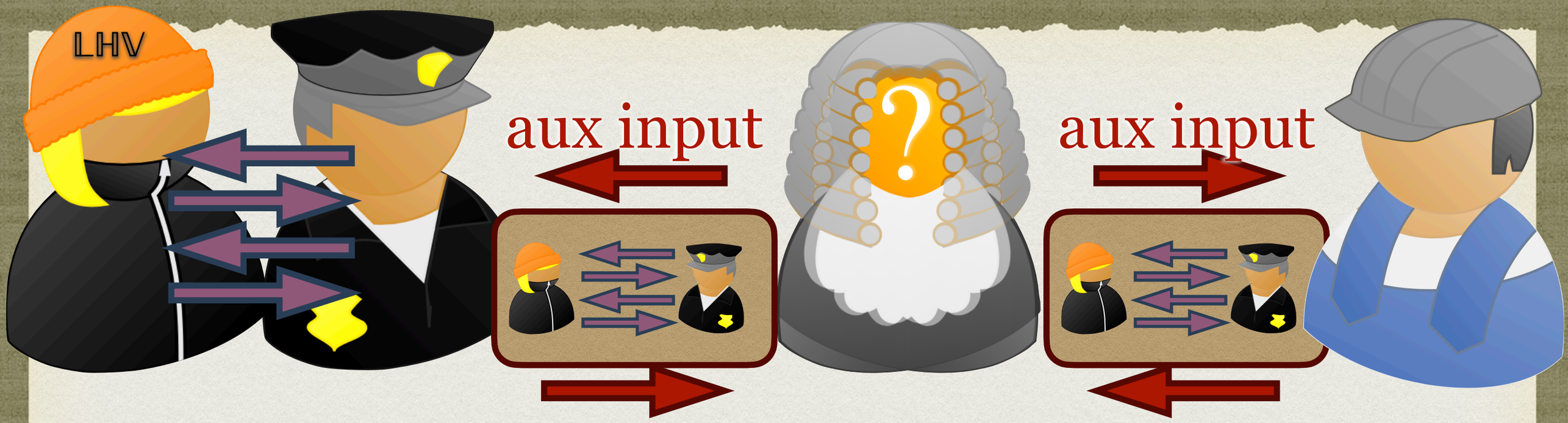
$$\begin{bmatrix} n_1, n_2 \\ r_1, r_2 \end{bmatrix} \in A, \quad \begin{bmatrix} n_3, n_4 \\ r_3, r_4 \end{bmatrix} \in B$$



NOSIG NOSIG



RELATIVISTIC ZK

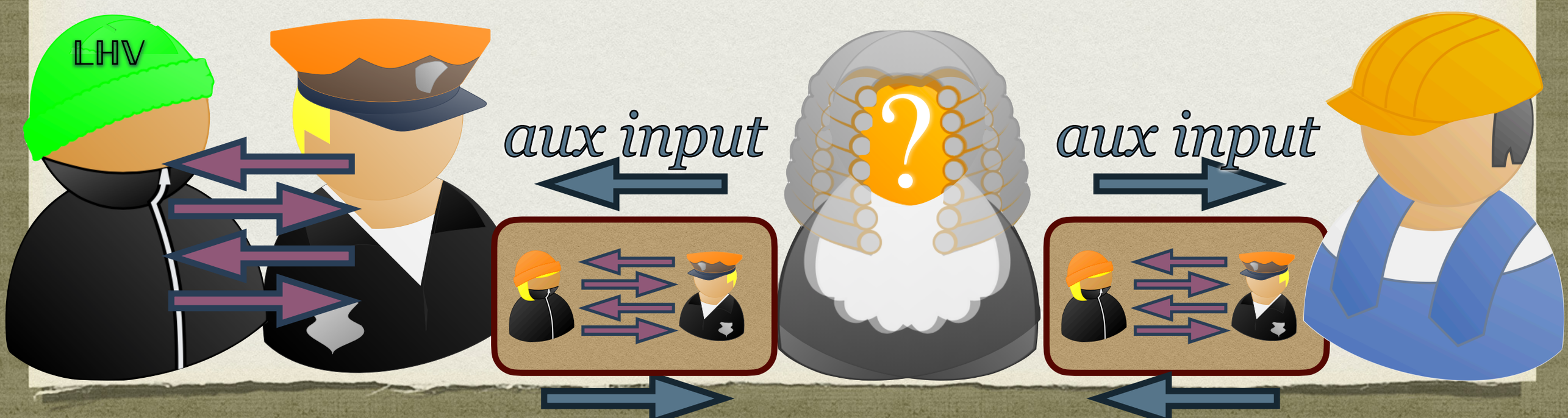


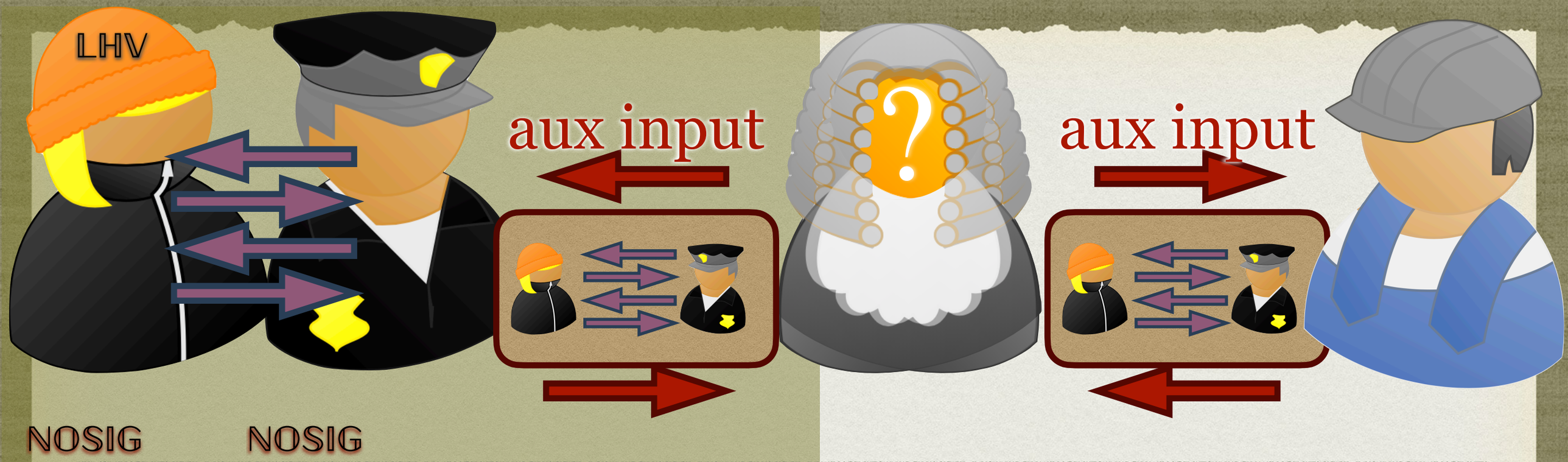
NOSIG NOSIG

$$\forall \text{\textcircled{\scriptsize P}}, \text{\textcircled{\scriptsize P}}\ \exists \text{\textcircled{\scriptsize V}}, \text{\textcircled{\scriptsize V}}\ \forall w \in L, \forall z_1, z_2$$

$$[(\overset{\text{poly}}{\text{\textcircled{\scriptsize P}}}:\text{\textcircled{\scriptsize P}})(w, z_1), (\overset{\text{poly}}{\text{\textcircled{\scriptsize P}}}:\text{\textcircled{\scriptsize P}})(w, z_2)] \approx [\text{\textcircled{\scriptsize V}}(w, z_1), \text{\textcircled{\scriptsize V}}(w, z_2)]$$

RELATIVISTIC ZK

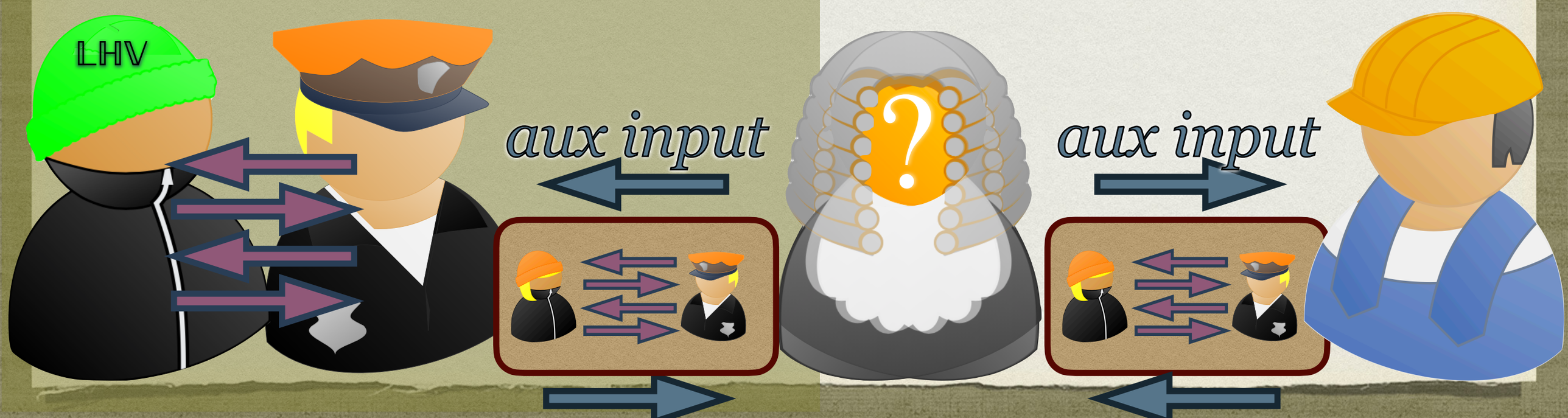


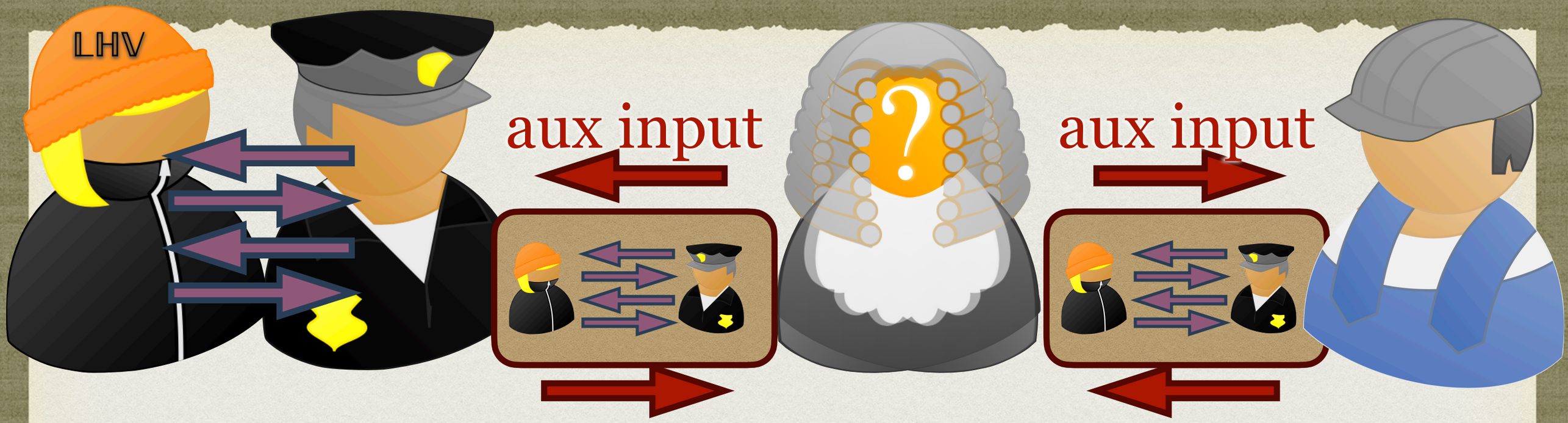


$$\forall \text{\textbf{A}}, \text{\textbf{B}}\ \exists \text{\textbf{C}}, \text{\textbf{D}}\ \forall w \in L, \forall z_1, z_2$$

$$[(\text{\textbf{A}}^{\text{poly}} : \text{\textbf{B}}^{\text{poly}})(w, z_1), (\text{\textbf{C}} : \text{\textbf{D}})(w, z_2)] \approx [\text{\textbf{C}}(w, z_1), \text{\textbf{D}}(w, z_2)]$$

RELATIVISTIC ZK



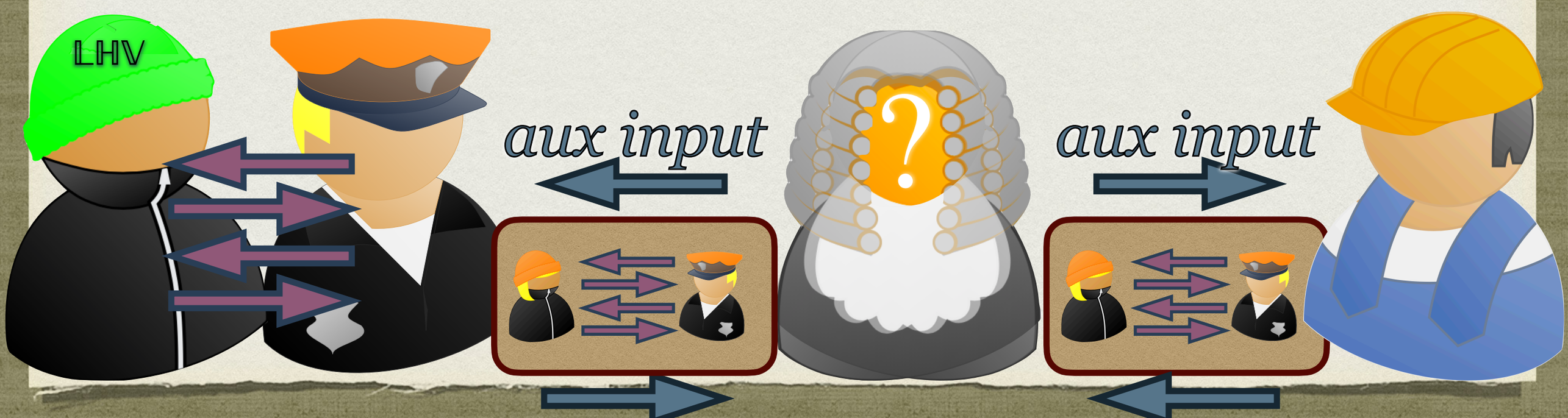


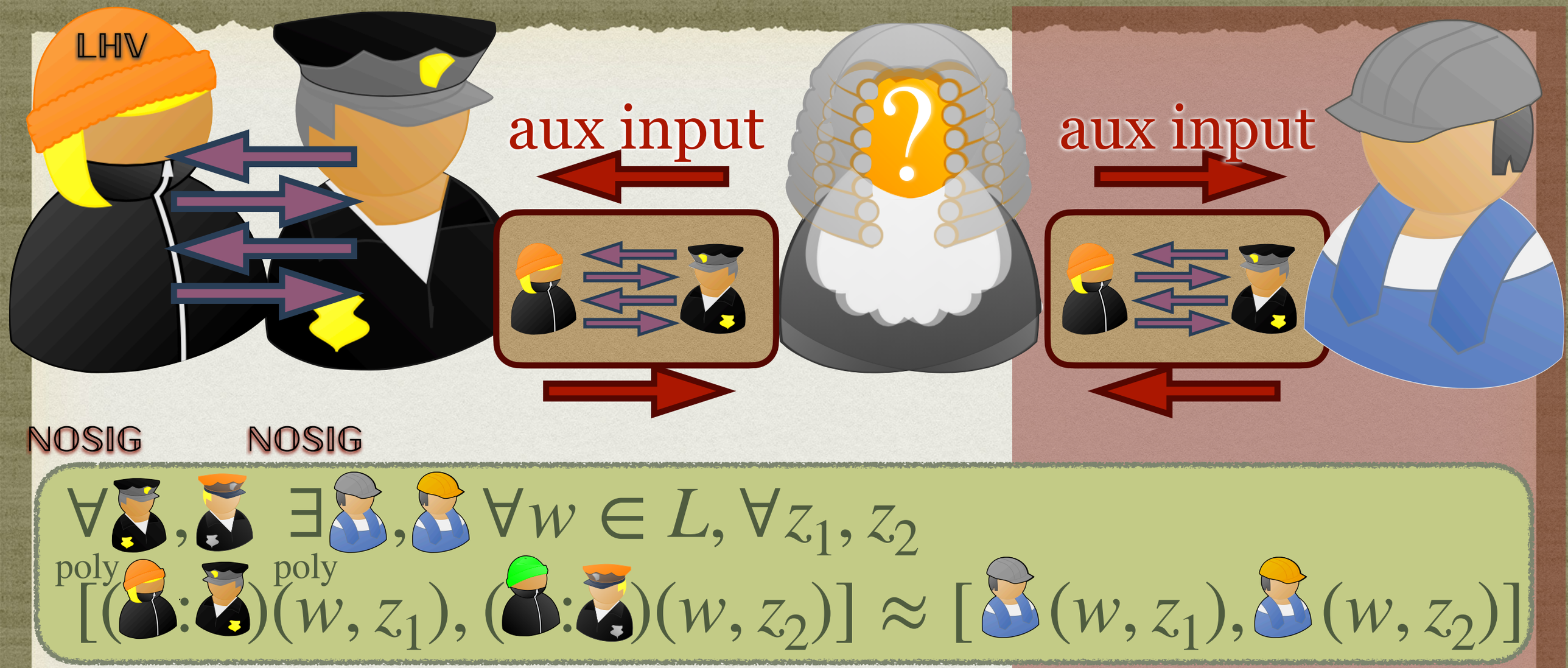
NOSIG NOSIG

$$\forall \text{\textcircled{\scriptsize P}}, \text{\textcircled{\scriptsize P}}\ \exists \text{\textcircled{\scriptsize V}}, \text{\textcircled{\scriptsize V}}\ \forall w \in L, \forall z_1, z_2$$

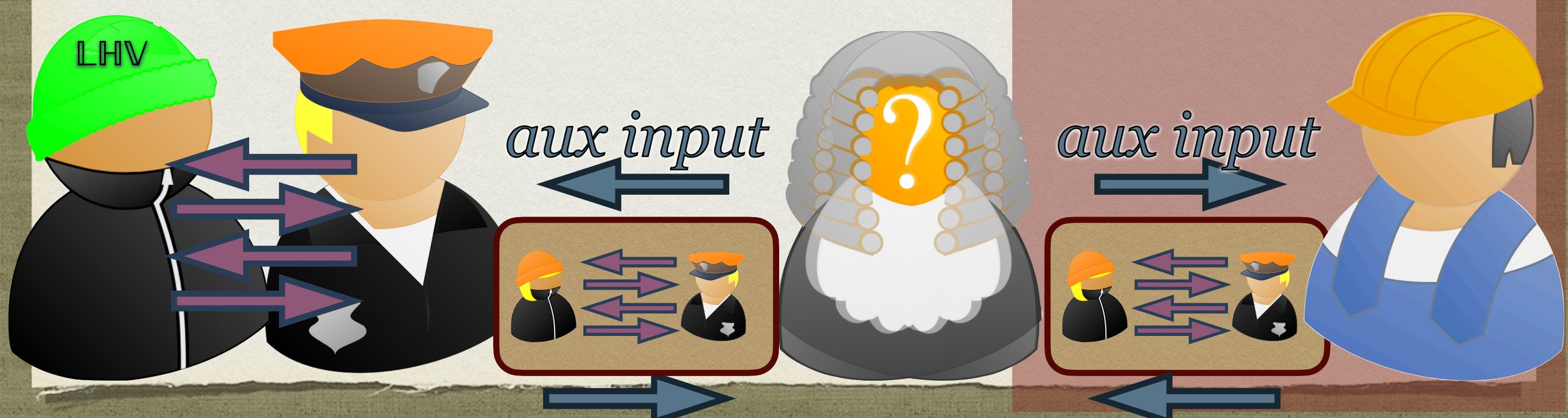
$$[(\overset{\text{poly}}{\text{\textcircled{\scriptsize P}}}:\text{\textcircled{\scriptsize P}})(w, z_1), (\overset{\text{poly}}{\text{\textcircled{\scriptsize P}}}:\text{\textcircled{\scriptsize P}})(w, z_2)] \approx [\text{\textcircled{\scriptsize V}}(w, z_1), \text{\textcircled{\scriptsize V}}(w, z_2)]$$

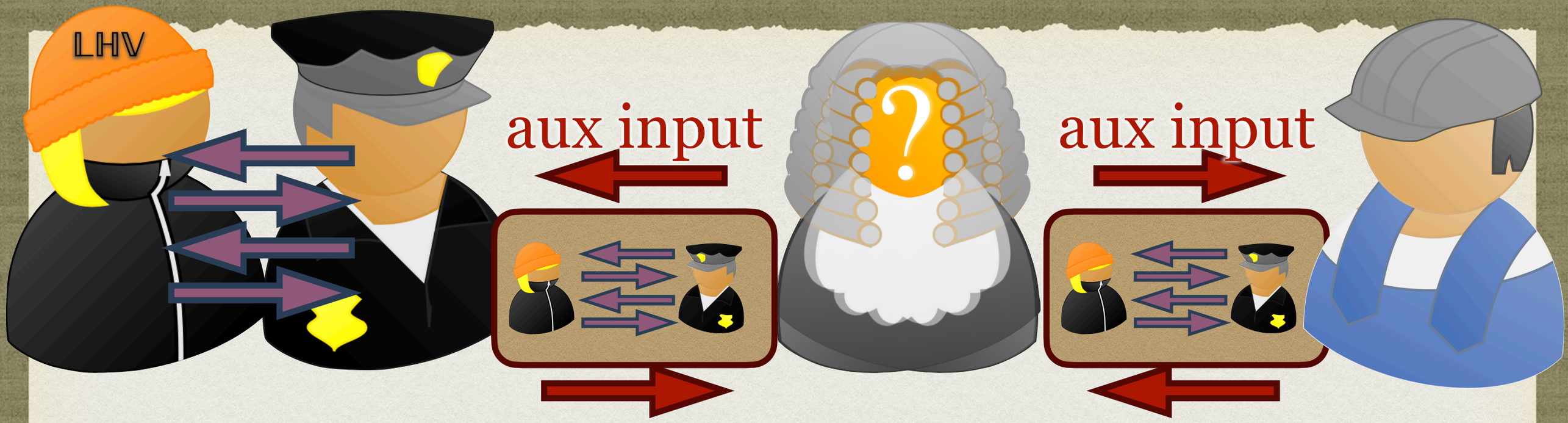
RELATIVISTIC ZK





RELATIVISTIC ZK



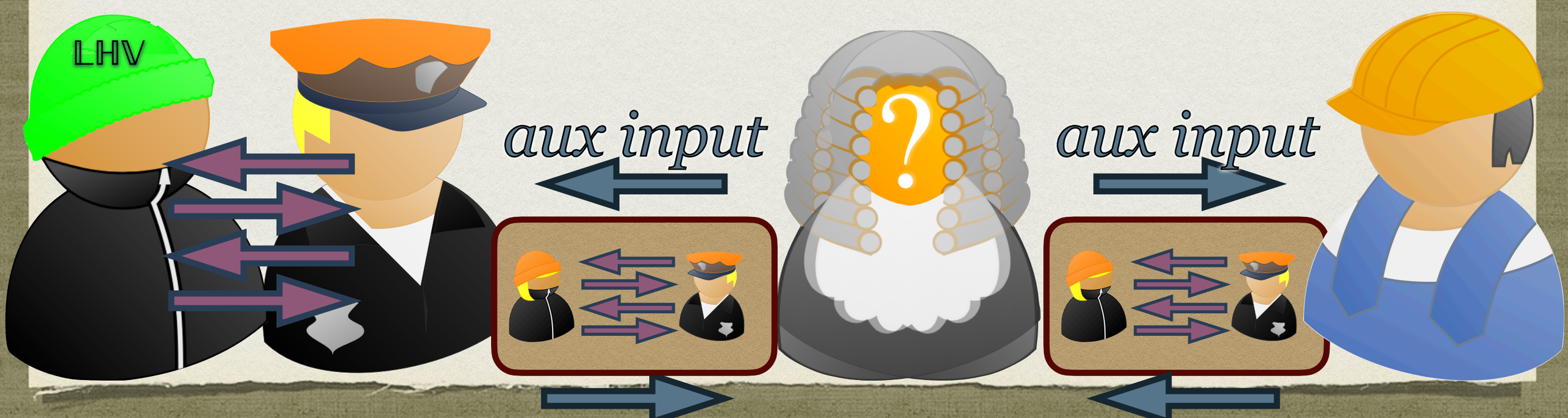


NOSIG NOSIG

$$\forall \text{\textcircled{\scriptsize P}}, \text{\textcircled{\scriptsize P}}\ \exists \text{\textcircled{\scriptsize V}}, \text{\textcircled{\scriptsize V}}\ \forall w \in L, \forall z_1, z_2$$

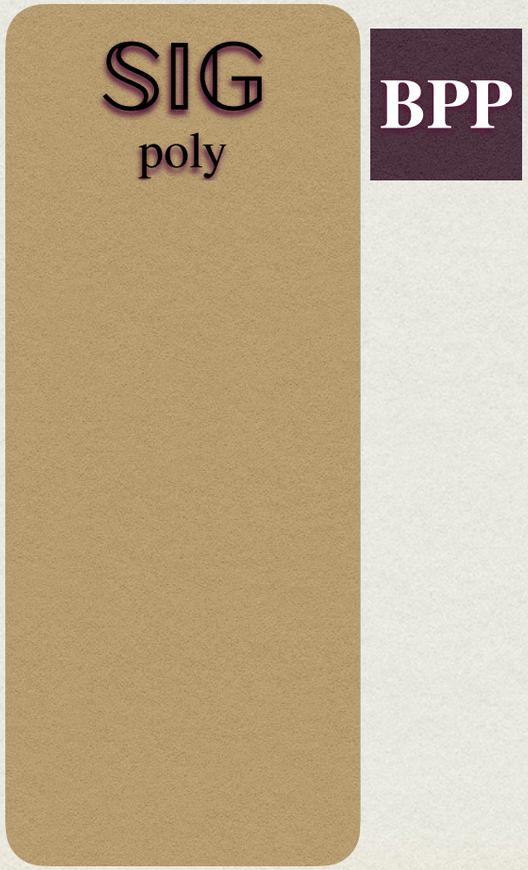
$$[(\overset{\text{poly}}{\text{\textcircled{\scriptsize P}}}:\text{\textcircled{\scriptsize P}})(w, z_1), (\overset{\text{poly}}{\text{\textcircled{\scriptsize P}}}:\text{\textcircled{\scriptsize P}})(w, z_2)] \approx [\text{\textcircled{\scriptsize V}}(w, z_1), \text{\textcircled{\scriptsize V}}(w, z_2)]$$

RELATIVISTIC ZK



POLYNOMIAL NON-LOCALITY

POLYNOMIAL NON-LOCALITY



POLYNOMIAL NON-LOCALITY

SIG poly	BPP
LHV poly	BPP
	BPP

POLYNOMIAL NON-LOCALITY

SIG poly	BPP
LHV poly	BPP
	BPP
QNL poly	BQP
	BQP

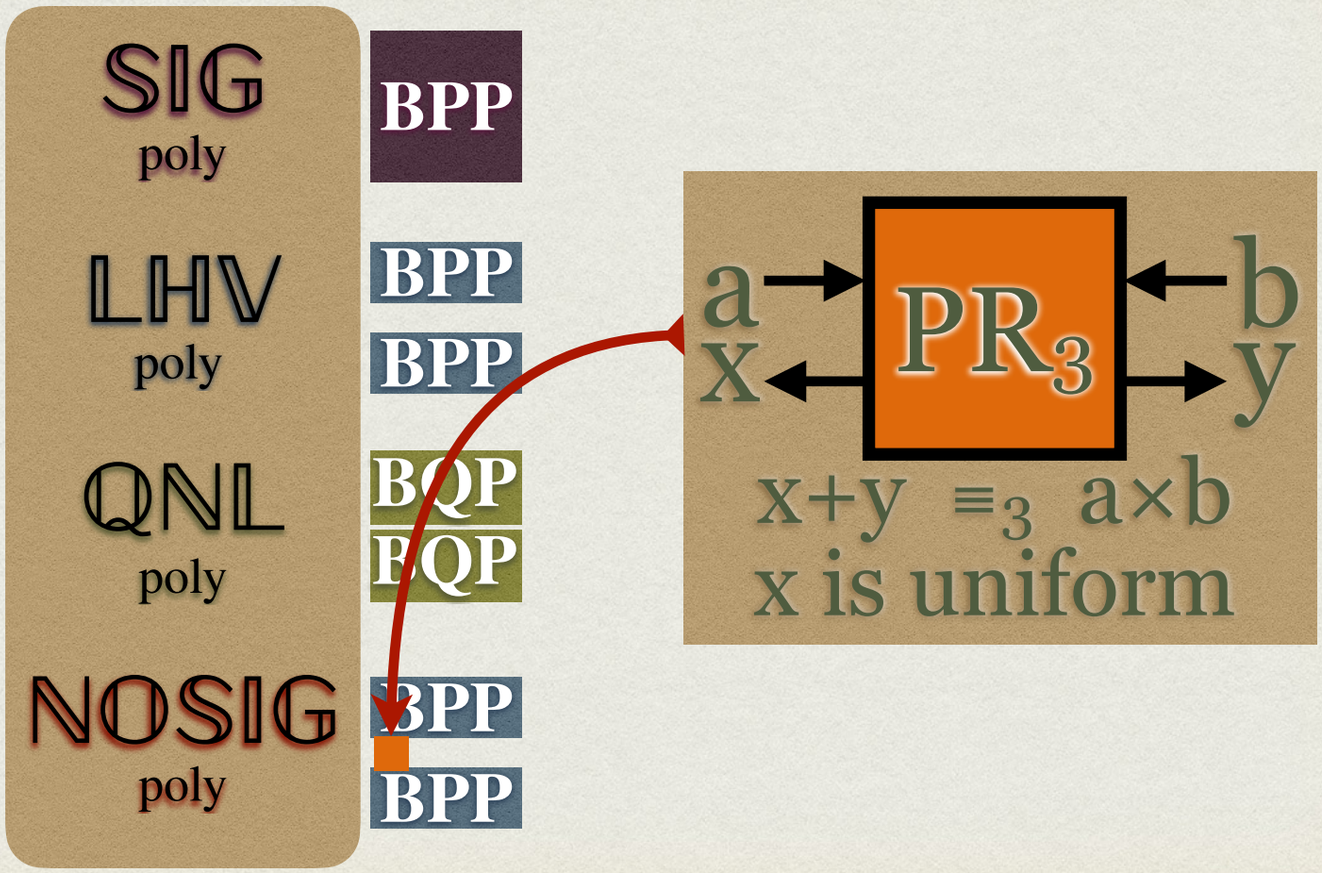
POLYNOMIAL NON-LOCALITY

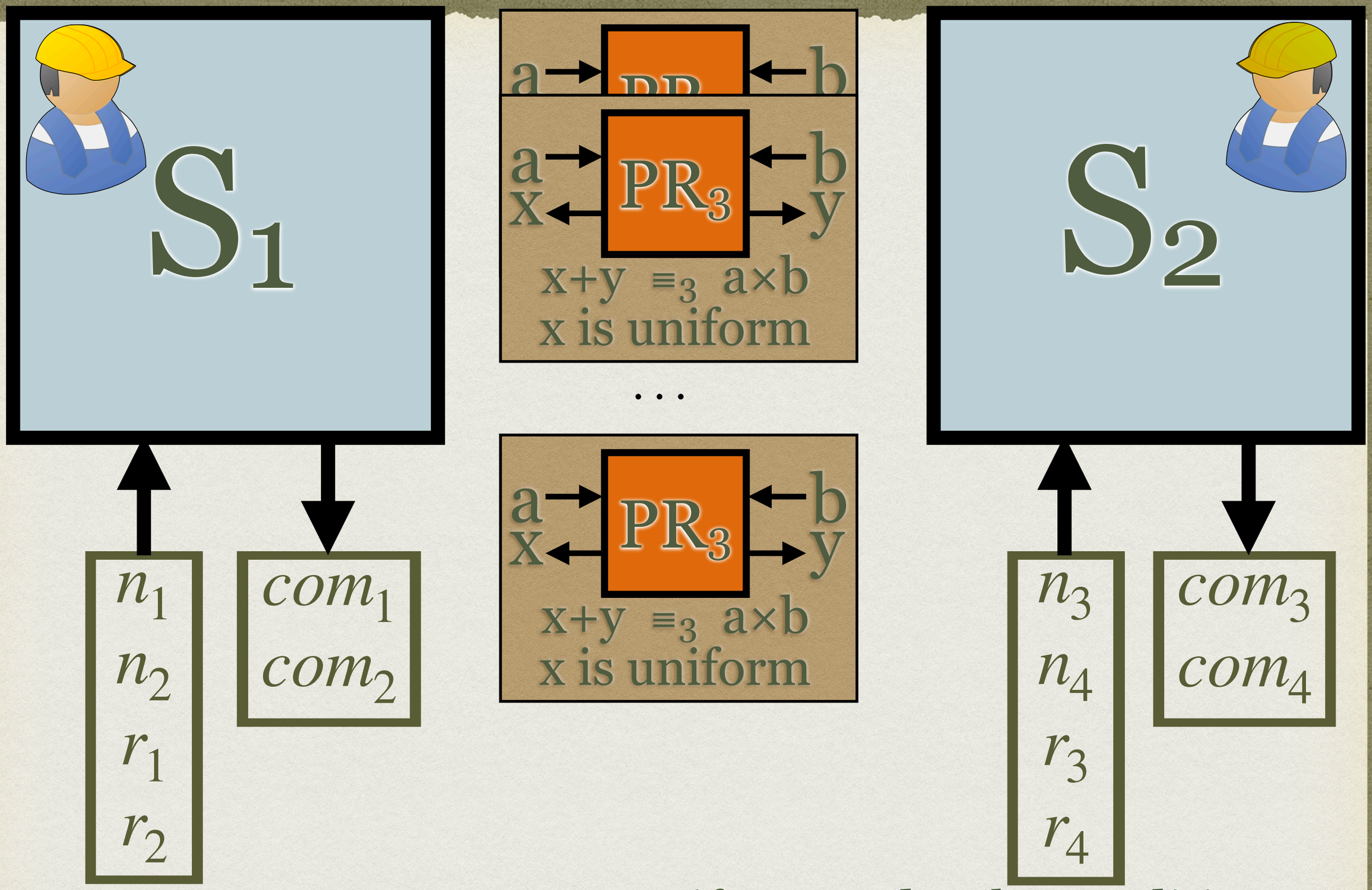
SIG poly	BPP
LHV poly	BPP BPP
QNL poly	BQP BQP
NOSIG poly	??? ???

POLYNOMIAL NON-LOCALITY

SIG poly	BPP
LHV poly	BPP BPP
QNL poly	BQP BQP
NOSIG poly	BPP BPP

POLYNOMIAL NON-LOCALITY



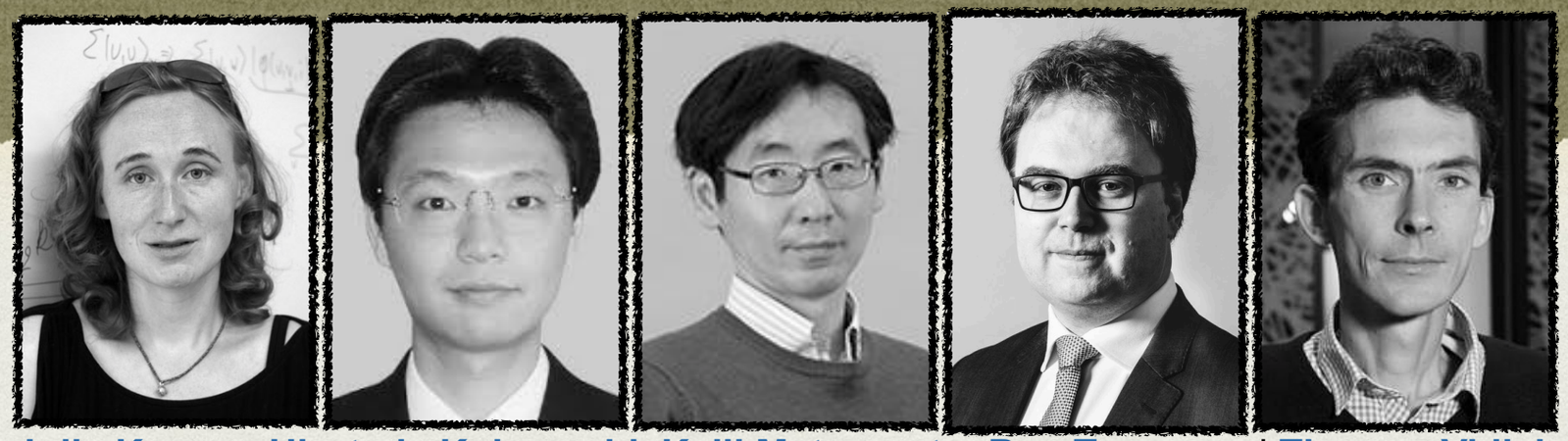


$com_1, com_2, \ldots, com_4$ are uniform under the conditions

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

$$n_i = n_j, r_i \neq r_j, n_k = n_\ell, r_k \neq r_\ell \implies com_i + com_j \neq com_k + com_\ell$$

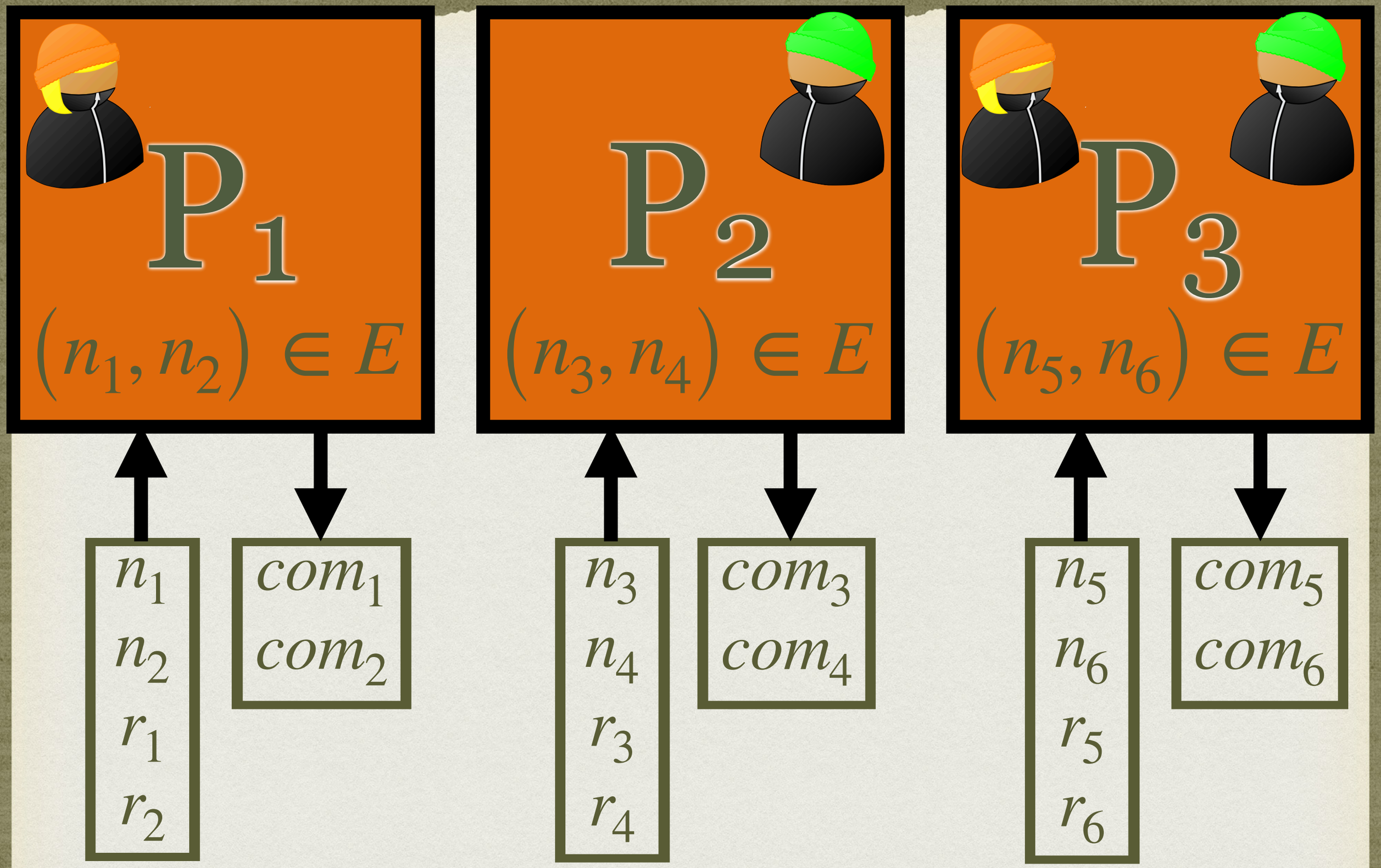
POWERFUL THEOREM



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

Entangled Games Are Hard to Approximate

- ▶ **Lemma 3** ([13], Lemma 17). *Let* $\Pi(x)$ *be a two-prover one-round symmetric game and let* $\Pi'(x)$ *be its modified version with three provers. If* $\omega^*(\Pi'(x)) > 1 - \varepsilon$ *then we always get* $\omega(\Pi(x)) > 1 - \varepsilon - 12|Q|\sqrt{\varepsilon}$ *where* Q *is the set of* V*'s possible questions to a prover in* Π.
- If (1-round) MIP is sound against *local* provers Then augmented MIP where 3rd prover mimics one of the first 2 is sound against *entangled* provers.



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

SOUNDNESS ANALYSIS

LHV

edge-verification test = 1/9

well-definition test = 8/9

SOUNDNESS ANALYSIS

LHV

edge-verification test = 1/9

well-definition test = 8/9

$$\omega_{QNL} \leq 1 - \frac{1}{(21|E|)^4}$$

SOUNDNESS ANALYSIS

LHV

edge-verification test = 1/9

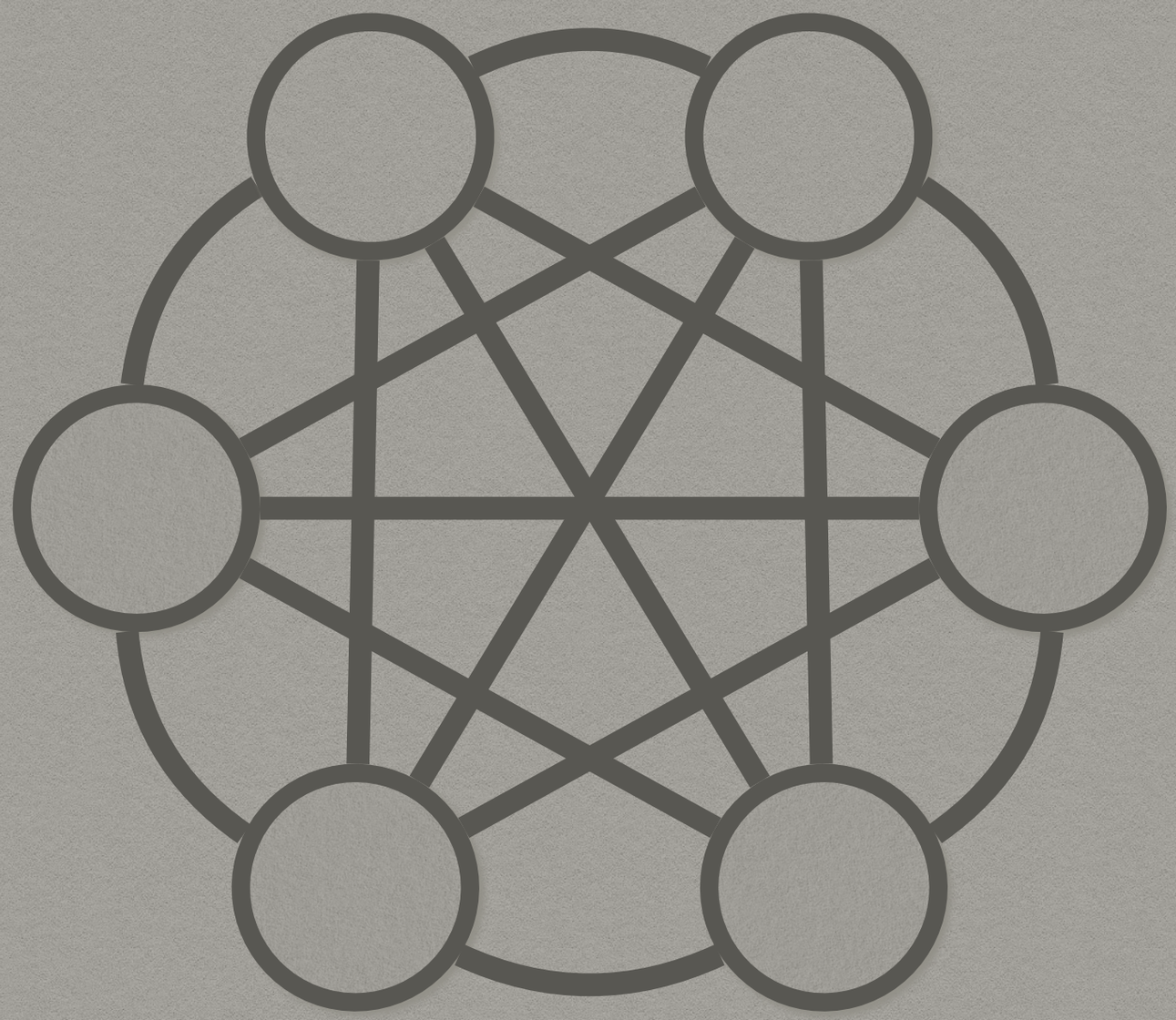
well-definition test = 8/9

$$\omega_{QNL} \leq 1 - \frac{1}{(21|E|)^4}$$

$(21|E|)^4 k$ rep.

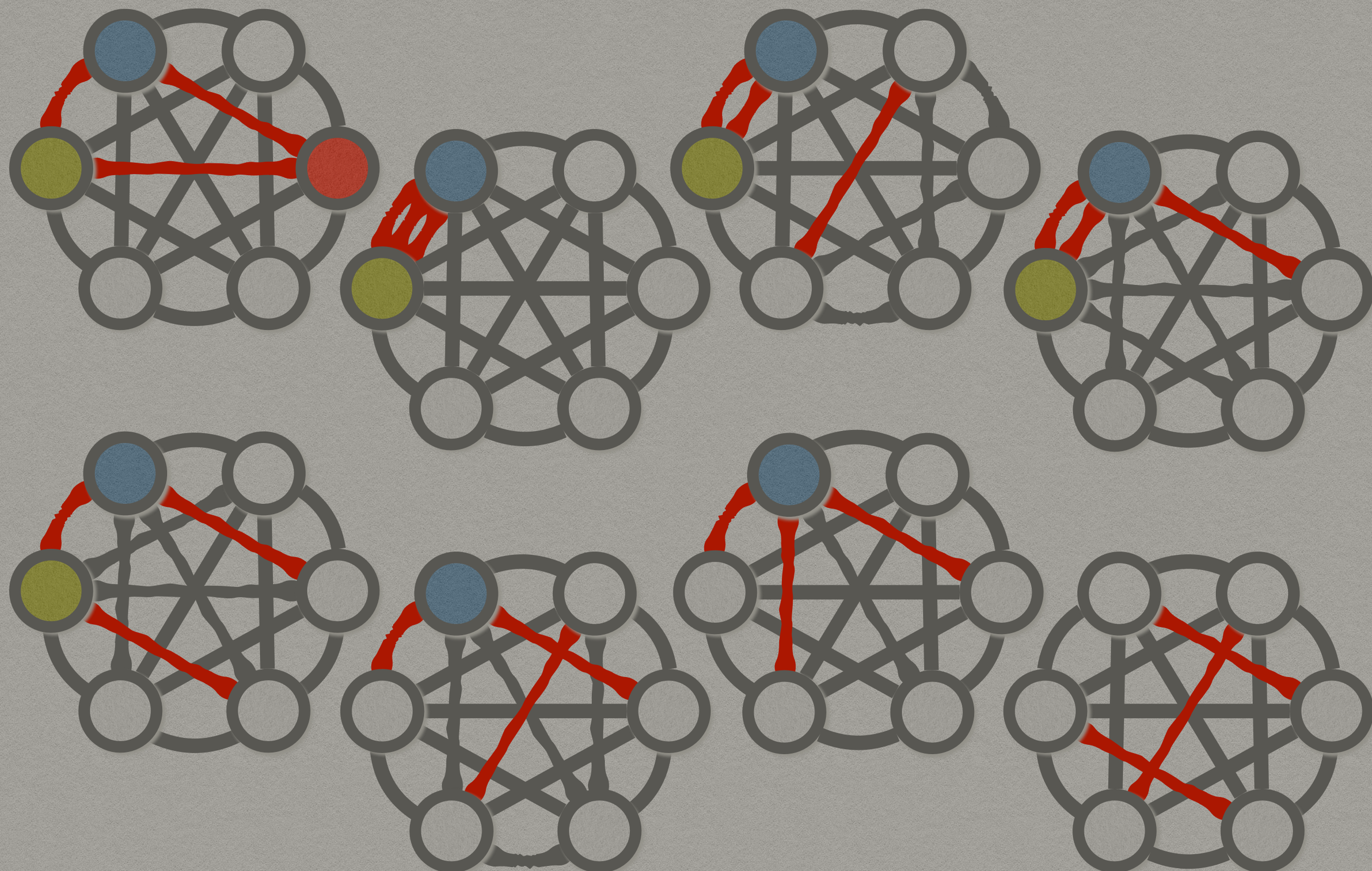
$$\omega_{QNL} \leq e^{-k}$$

ZK SIMULATION



K_6

ZK SIMULATION



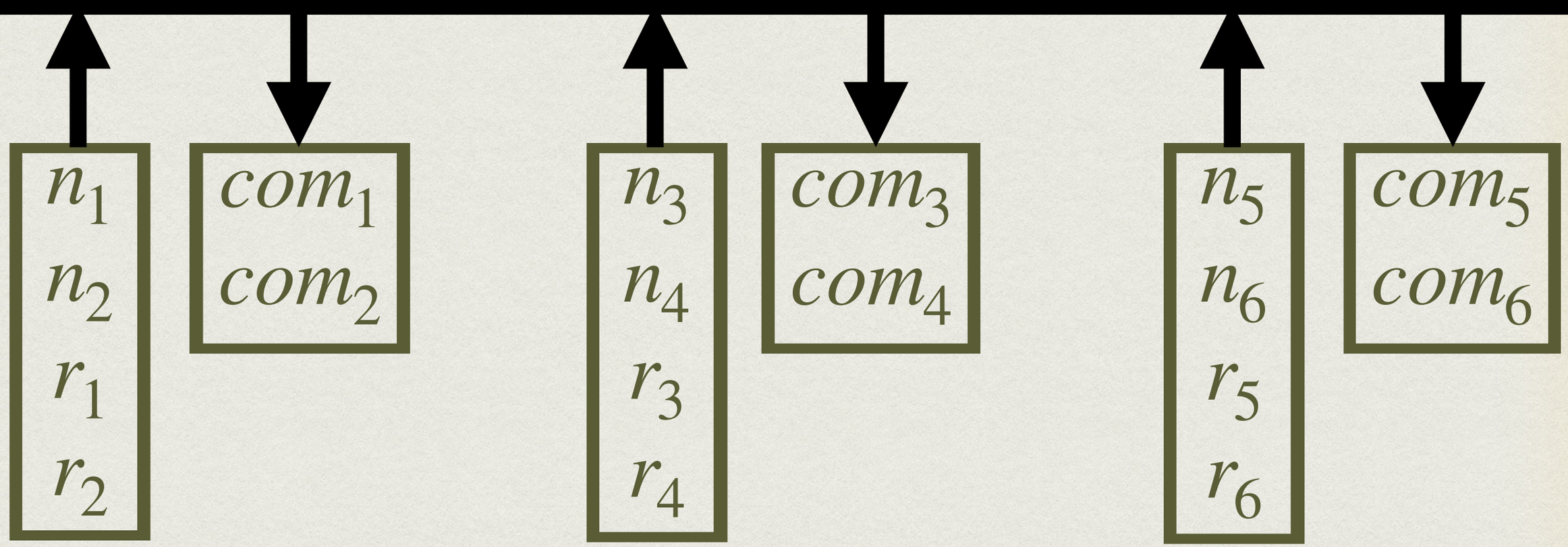
CASE ANALYSIS

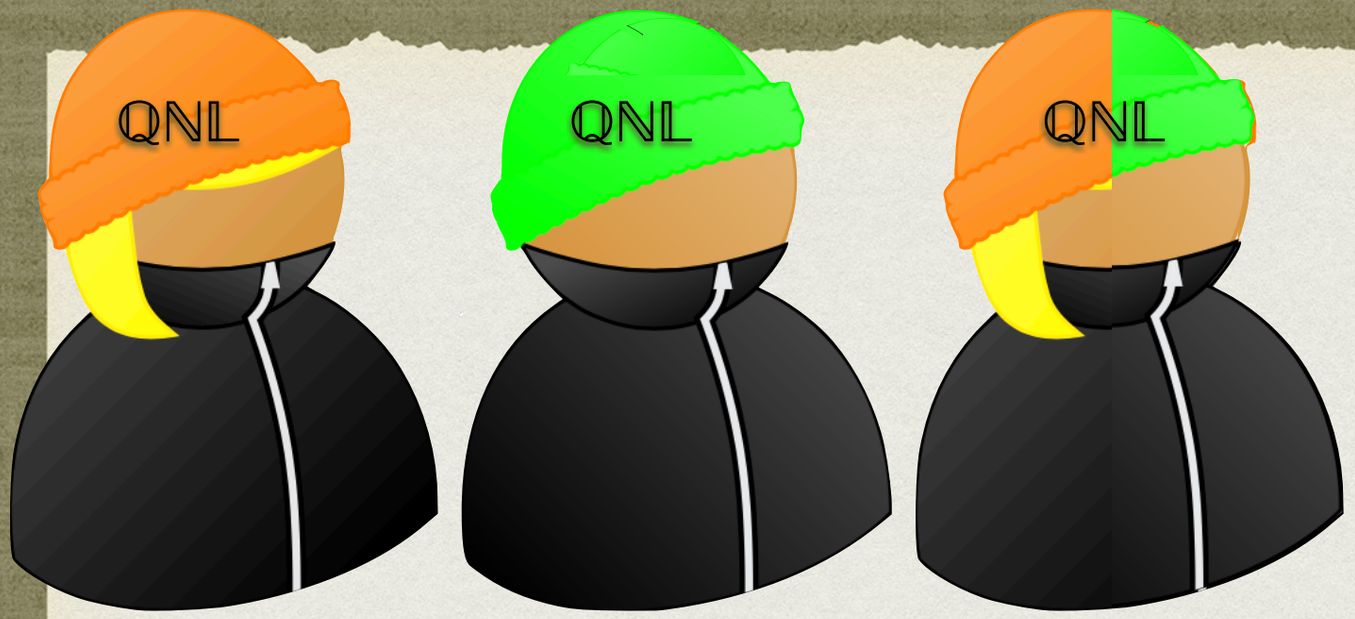
$com_1, com_2, \ldots, com_6$ are uniform under the conditions

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

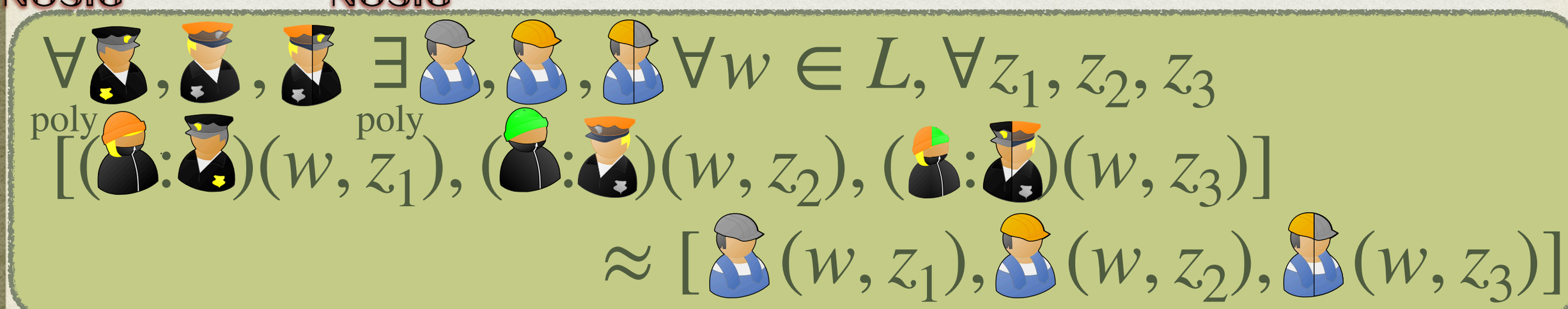
$$n_i = n_j, r_i \neq r_j, n_k = n_\ell, r_k \neq r_\ell \implies com_i + com_j \neq com_k + com_\ell$$

$$(n_1, n_2) \in E \qquad (n_3, n_4) \in E \qquad (n_5, n_6) \in E$$





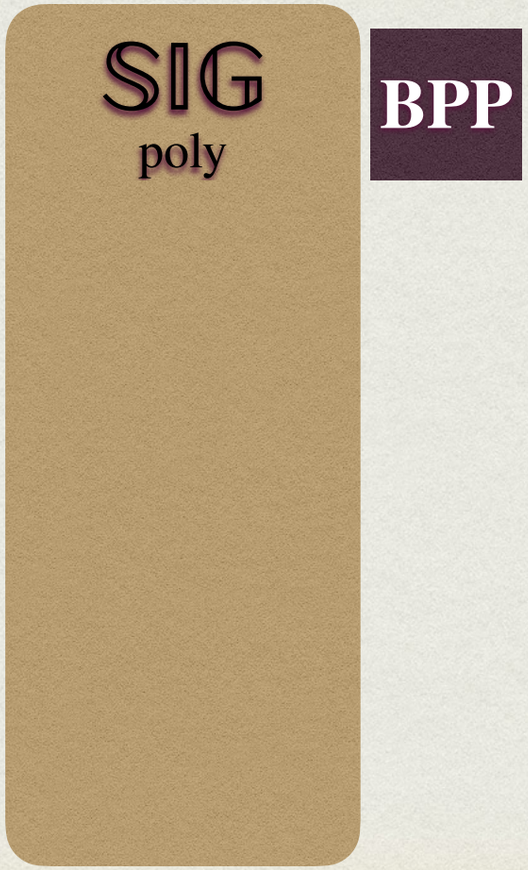
NOSIG NOSIG



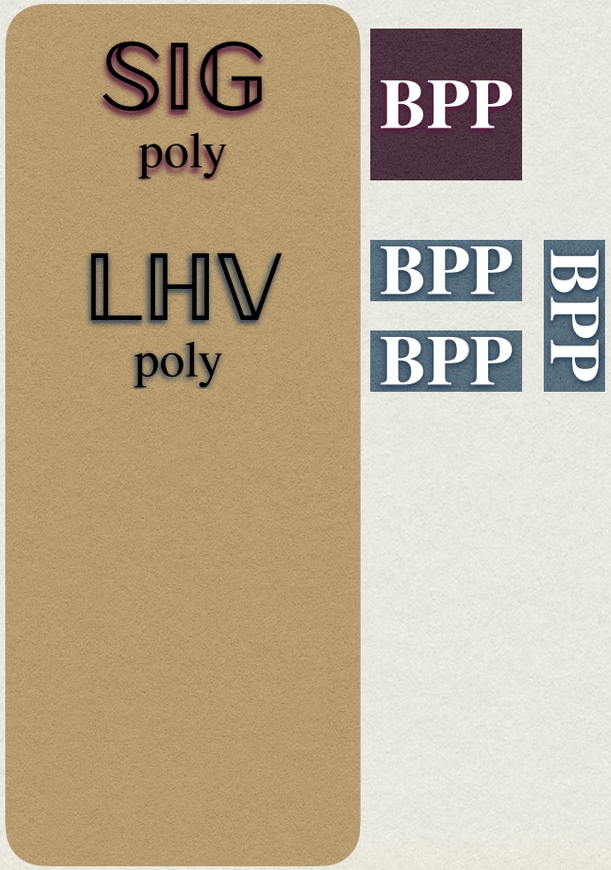
RELATIVISTIC ZK

POLYNOMIAL NON-LOCALITY

POLYNOMIAL NON-LOCALITY



POLYNOMIAL NON-LOCALITY

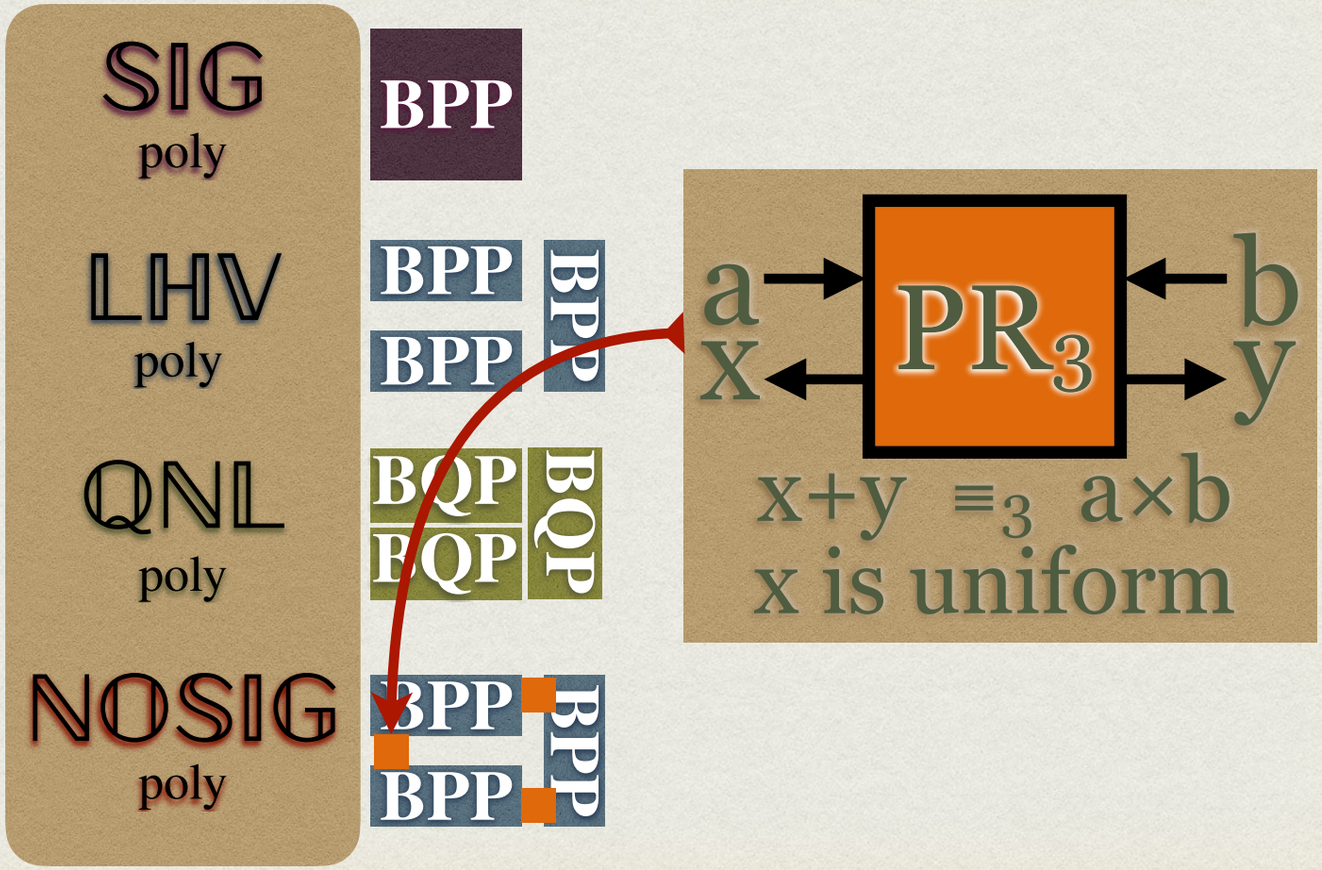


POLYNOMIAL NON-LOCALITY

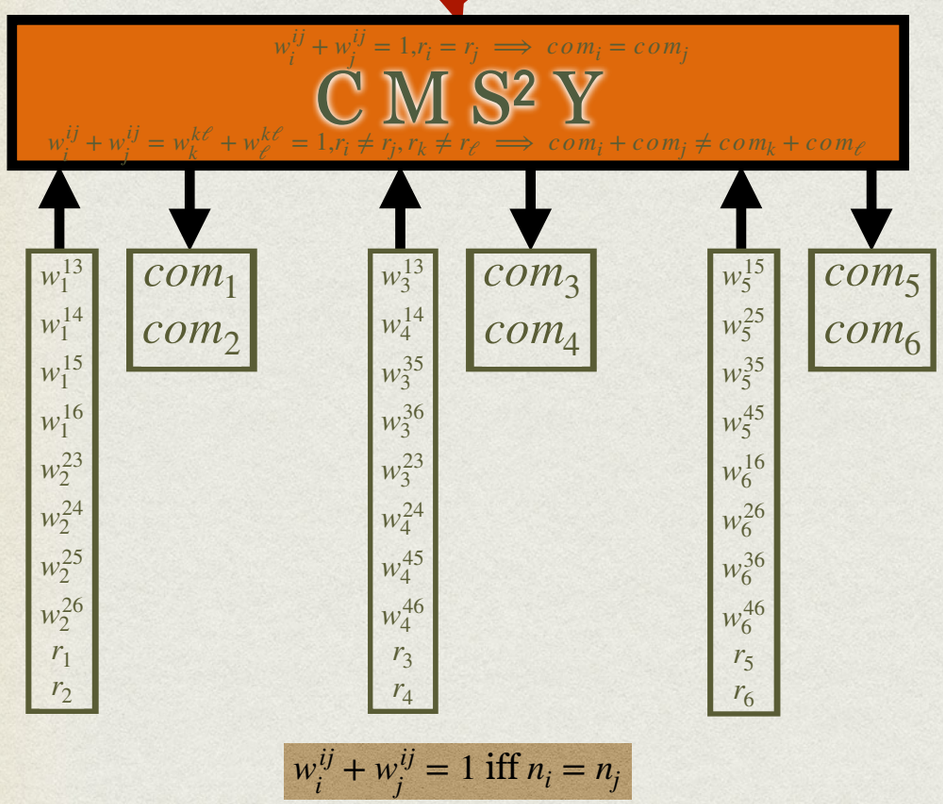
POLYNOMIAL NON-LOCALITY

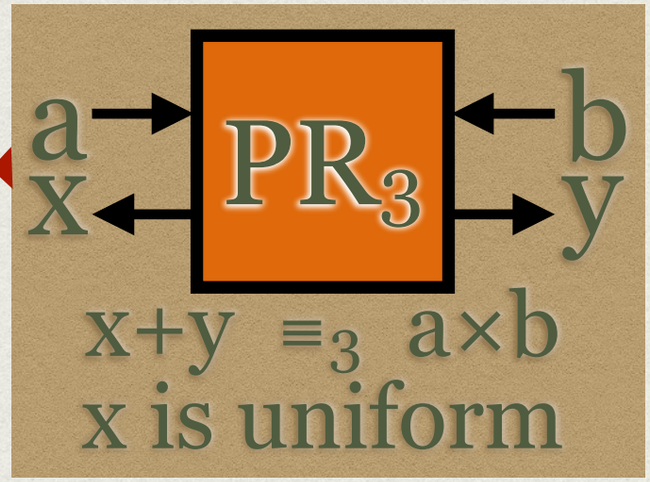
POLYNOMIAL NON-LOCALITY

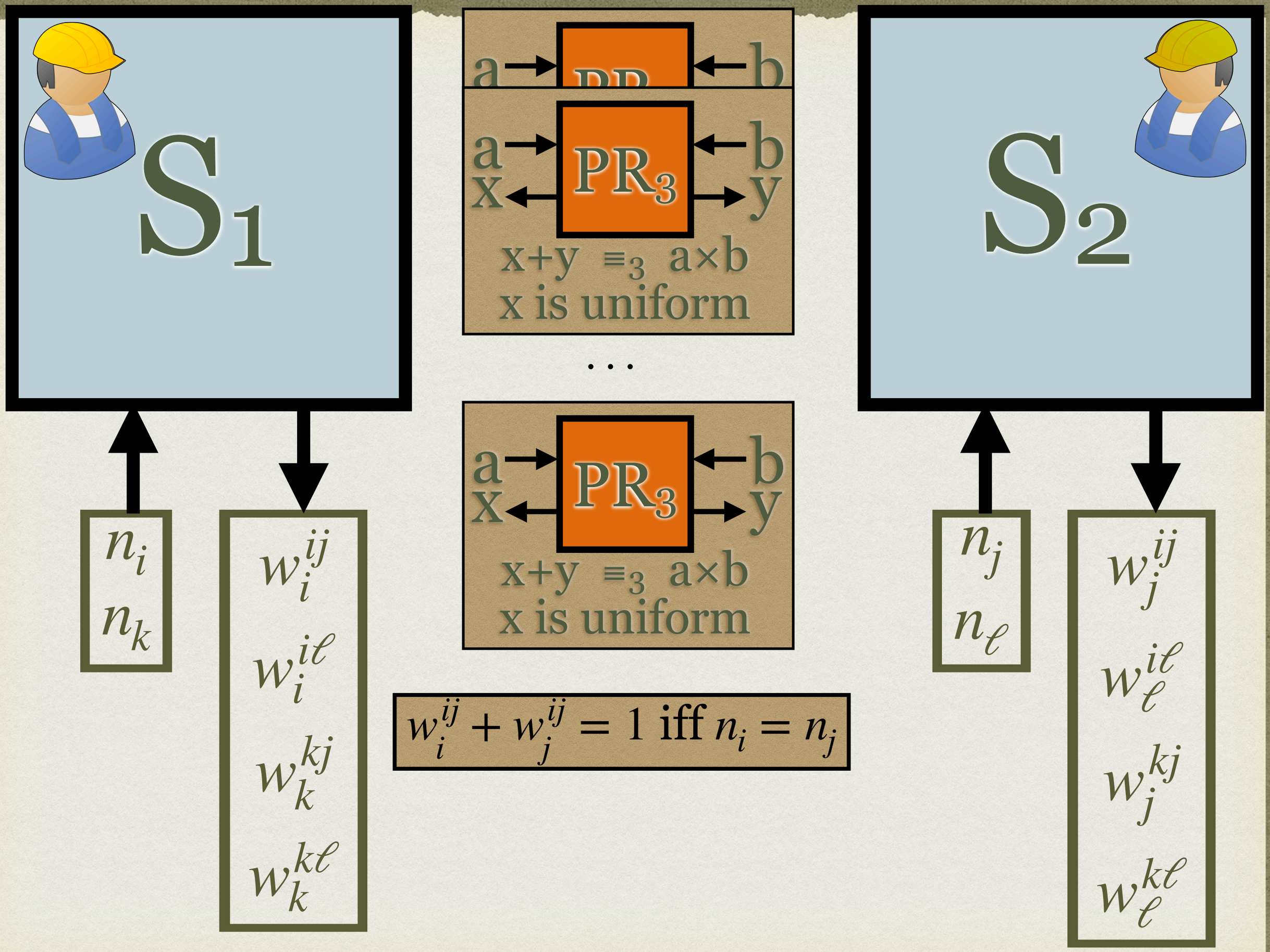
POLYNOMIAL NON-LOCALITY

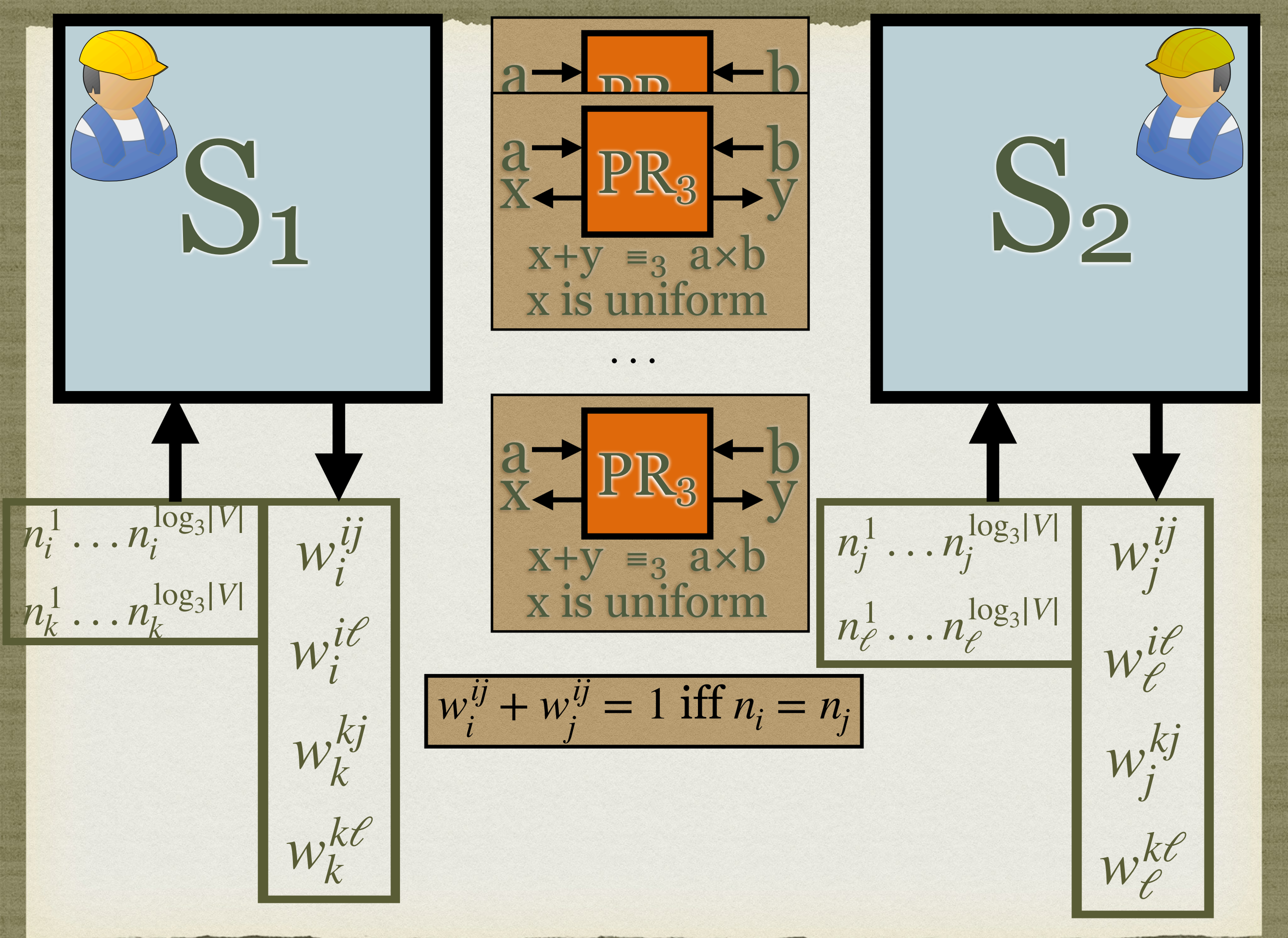


POLYNOMIAL NON-LOCALITY






S_1
S_2
a
b
PR_3
x
y
$x+y \equiv_3 a\times b$
x is uniform
. . .
n_i
n_k
w_i^{ij}
$w_i^{i\ell}$
w_k^{kj}
$w_k^{k\ell}$
n_j
n_ℓ
w_j^{ij}
$w_\ell^{i\ell}$
w_j^{kj}
$w_\ell^{k\ell}$
$w_i^{ij} + w_j^{ij} = 1 \text{ iff } n_i = n_j$


S_1
S_2
a
b
PR_3
x
y
$x+y \equiv_3 a\times b$
x is uniform
. . .
$n_i^1 \ldots n_i^{\log_3|V|}$
$n_k^1 \ldots n_k^{\log_3|V|}$
w_i^{ij}
$w_i^{i\ell}$
w_k^{kj}
$w_k^{k\ell}$
$n_j^1 \ldots n_j^{\log_3|V|}$
$n_\ell^1 \ldots n_\ell^{\log_3|V|}$
w_j^{ij}
$w_\ell^{i\ell}$
w_j^{kj}
$w_\ell^{k\ell}$
$w_i^{ij} + w_j^{ij} = 1 \text{ iff } n_i = n_j$

$$w_i^{ij} + w_j^{ij} = 1, r_i = r_j \implies com_i = com_j$$

C M S² Y

$$w_i^{ij} + w_j^{ij} = w_k^{k\ell} + w_\ell^{k\ell} = 1, r_i \neq r_j, r_k \neq r_\ell \implies com_i + com_j \neq com_k + com_\ell$$

w_1^{13}	com_1	w_3^{13}	com_3	w_5^{15}	com_5
w_1^{14}	com_2	w_4^{14}	com_4	w_5^{25}	com_6
w_1^{15}		w_3^{35}		w_5^{35}	
w_1^{16}		w_3^{36}		w_5^{45}	
w_2^{23}		w_3^{23}		w_6^{16}	
w_2^{24}		w_4^{24}		w_6^{26}	
w_2^{25}		w_4^{45}		w_6^{36}	
w_2^{26}		w_4^{46}		w_6^{46}	
r_1		r_3		r_5	
r_2		r_4		r_6	

$$w_i^{ij} + w_j^{ij} = 1, r_i = r_j \implies com_i = com_j$$

CMS²Y

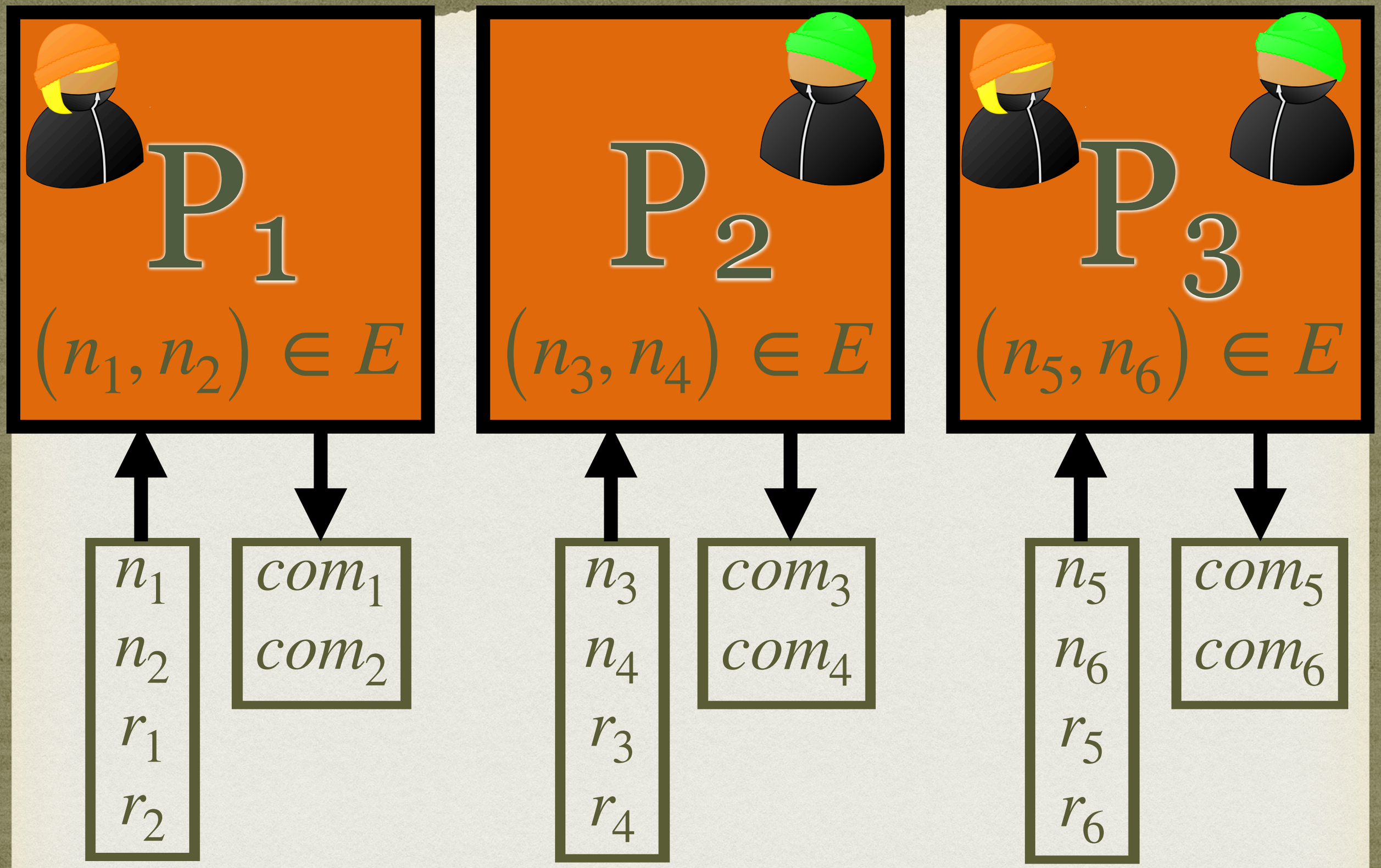
$$w_i^{ij} + w_j^{ij} = w_k^{k\ell} + w_\ell^{k\ell} = 1, r_i \neq r_j, r_k \neq r_\ell \implies com_i + com_j \neq com_k + com_\ell$$

w_1^{13}	com_1	w_3^{13}	com_3	w_5^{15}	com_5
w_1^{14}	com_2	w_4^{14}	com_4	w_5^{25}	com_6
w_1^{15}		w_3^{35}		w_5^{35}	
w_1^{16}		w_3^{36}		w_5^{45}	
w_2^{23}		w_3^{23}		w_6^{16}	
w_2^{24}		w_4^{24}		w_6^{26}	
w_2^{25}		w_4^{45}		w_6^{36}	
w_2^{26}		w_4^{46}		w_6^{46}	
r_1		r_3		r_5	
r_2		r_4		r_6	

$$w_i^{ij} + w_j^{ij} = 1, r_i = r_j \implies com_i = com_j$$

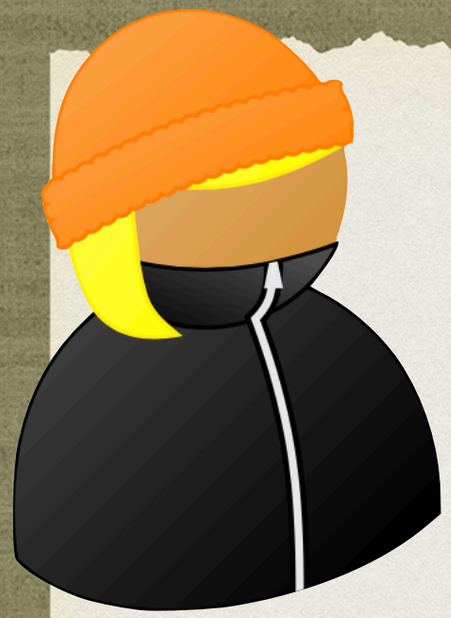
$$w_i^{ij} + w_j^{ij} = w_k^{k\ell} + w_\ell^{k\ell} = 1, r_i \neq r_j, r_k \neq r_\ell \implies com_i + com_j \neq com_k + com_\ell$$

w_1^{13}	com_1	w_3^{13}	com_3	w_5^{15}	com_5
w_1^{14}	com_2	w_4^{14}	com_4	w_5^{25}	com_6
w_1^{15}		w_3^{35}		w_5^{35}	
w_1^{16}		w_3^{36}		w_5^{45}	
w_2^{23}		w_3^{23}		w_6^{16}	
w_2^{24}		w_4^{24}		w_6^{26}	
w_2^{25}		w_4^{45}		w_6^{36}	
w_2^{26}		w_4^{46}		w_6^{46}	
r_1		r_3		r_5	
r_2		r_4		r_6	



Unsound against NOSIG Provers

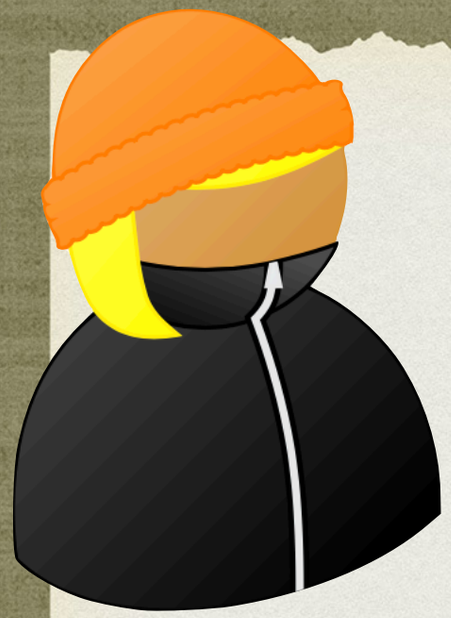
NON-LOCAL ZERO-KNOWLEDGE



NON-LOCAL ZK

$\forall \mathbb{V} \supseteq \mathbb{S},\ \forall_{\text{poly}\mathbb{V}}$ $,$ $\exists_{\text{poly}\mathbb{V}}$ $,$ $\forall w \in L, \forall z_1, z_2$

$[($ $:$ $)(w, z_1), ($ $:$ $)(w, z_2)] \approx [$ $(w, z_1),$ $(w, z_2)]$



NON-LOCAL ZK

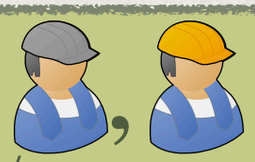
$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$\forall \mathbb{V} \supseteq \mathbb{S},\ \forall_{\text{poly}\mathbb{V}}$ $,$ $\exists_{\text{poly}\mathbb{V}}$ $,$ $\forall w \in L, \forall z_1, z_2$

$[($ $:$ $)(w, z_1), ($ $:$ $)(w, z_2)] \approx [$ $(w, z_1),$ $(w, z_2)]$

NON-LOCAL ZK

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathrm{HV}}$

$\forall \mathbb{V} \supseteq \mathbb{S},\ \forall_{\mathrm{poly}\mathbb{V}}$ $\exists_{\mathrm{poly}\mathbb{V}}$  $\forall w \in L, \forall z_1, z_2$

$[($ $:$$)(w, z_1), ($ $:$$)(w, z_2)] \approx [$ $(w, z_1),$ $(w, z_2)]$

Upper bound on dishonest Provers

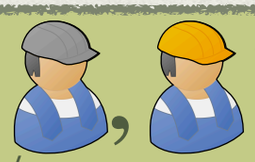
NON-LOCAL ZK

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

Honest Verifier class

$\mathbb{HV} \subsetneq \mathbb{P}$ is unusual.

$\mathbb{HV}$

$\forall \mathbb{V} \supseteq \mathbb{S},\ \forall_{\text{poly}\mathbb{V}}$ $\exists_{\text{poly}\mathbb{V}}$  $\forall w \in L, \forall z_1, z_2$

$[(\ :\ )(w, z_1), (\ :\ )(w, z_2)] \approx [\ (w, z_1), \ (w, z_2)]$

Upper bound on dishonest Provers

NON-LOCAL ZK

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

Honest Verifier class

$\mathbb{HV} \subsetneq \mathbb{P}$ is unusual.

$\mathbb{HV}$ $\mathbb{S}$ Upper bound on dishonest verifiers/simulators

$\forall \mathbb{V} \supseteq \mathbb{S}, \ \forall_{\text{poly}\mathbb{V}}$ $\exists_{\text{poly}\mathbb{V}}$ $\forall w \in L, \forall z_1, z_2$

$[($ $)(w, z_1), ($ $)(w, z_2)] \approx [$ $(w, z_1),$ $(w, z_2)]$

Upper bound on dishonest Provers

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{IP} = \mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{PSPACE}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{IP} = \mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{PSPACE}$$

$$\mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{SZK}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{IP} = \mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{PSPACE}$$

$$\mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{SZK}$$

$$\mathbf{MIP} = \mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{NEXP}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{IP} = \mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{PSPACE}$$

$$\mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{SIG}}_{\mathbb{SIG}} = \mathbf{SZK}$$

$$\mathbf{MIP} = \mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{NEXP}$$

$$\mathbf{ZKMIP} = \mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{SIG}} = \mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{NEXP}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{MIP}^{*} = \mathbf{ZKMIP}^{*} = \mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \boxed{\mathbf{RE}}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{MIP}^{*} = \mathbf{ZKMIP}^{*} = \mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{RE}$$

$$\mathbf{MIP}^{ns} = \mathbf{MIP}^{\mathbb{NOSIG}}_{\mathbb{LHV}} = \mathbf{EXP}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{MIP}^{*} = \mathbf{ZKMIP}^{*} = \mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{RE}$$

$$\mathbf{MIP}^{ns} = \mathbf{MIP}^{\mathbb{NOSIG}}_{\mathbb{LHV}} = \mathbf{EXP}$$

$$\mathbf{ZK}^{\mathbb{QNL}}\mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{ZK}^{\mathbb{NOSIG}}\mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{NEXP}$$

$\mathbf{ZK}^{\mathbb{S}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{HV}}$

$$\mathbf{MIP}^{*} = \mathbf{ZKMIP}^{*} = \mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}} = \mathbf{RE}$$

$$\mathbf{MIP}^{ns} = \mathbf{MIP}^{\mathbb{NOSIG}}_{\mathbb{LHV}} = \mathbf{EXP}$$

$$\mathbf{ZK}^{\mathbb{QNL}}\mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{ZK}^{\mathbb{NOSIG}}\mathbf{MIP}^{\mathbb{LHV}}_{\mathbb{LHV}} = \mathbf{NEXP}$$

$$\mathbf{NP} \subseteq \mathbf{ZK}^{\mathbb{NOSIG}}\mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}}$$

OPEN QUESTIONS:

OPEN QUESTIONS:

- $\mathbf{ZK}^{\mathsf{SIG}}\mathbf{MIP}^{\mathsf{NOSIG}}_{\mathsf{LHV}} \neq \mathbf{SZK}$?

OPEN QUESTIONS:

- $\mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{NOSIG}}_{\mathbb{LHV}} \neq \mathbf{SZK}$?
- $\exists \mathbb{P} \neq \mathbb{SIG}, \mathbf{ZK}^{\mathbb{P}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{P}} \neq \mathbf{SZK}$?

OPEN QUESTIONS:

- $\mathbf{ZK}^{\mathbb{SIG}}\mathbf{MIP}^{\mathbb{NOSIG}}_{\mathbb{LHV}} \neq \mathbf{SZK}$?
- $\exists \mathbb{P} \neq \mathbb{SIG}, \mathbf{ZK}^{\mathbb{P}}\mathbf{MIP}^{\mathbb{P}}_{\mathbb{P}} \neq \mathbf{SZK}$?
- $\mathbf{QMA} \subseteq \mathbf{ZK}^{\mathbb{NOSIG}}\mathbf{MIP}^{\mathbb{QNL}}_{\mathbb{LHV}}$?

Aly Ibrahim Nan Yang

Relativistic & Non-Local Zero-Knowledge Proofs

Workshop on Quantum Information, Computation, and Foundation

Sept. 14-18, 2020

Claude Crépeau

McGill