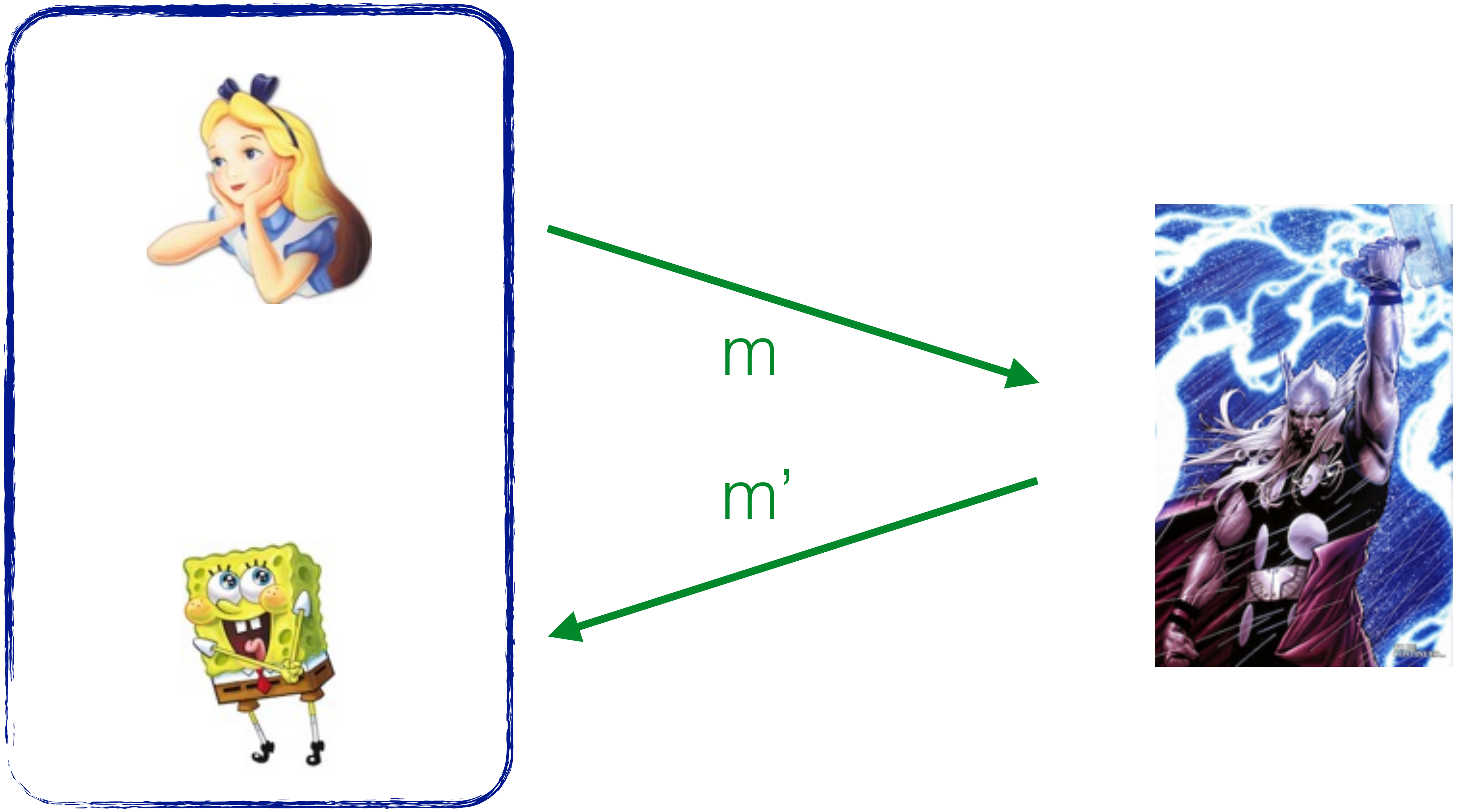
How the internal communication of the applied-pi calculus is messing with equivalence properties.

Kushal Babel, Vincent Cheval, Steve Kremer

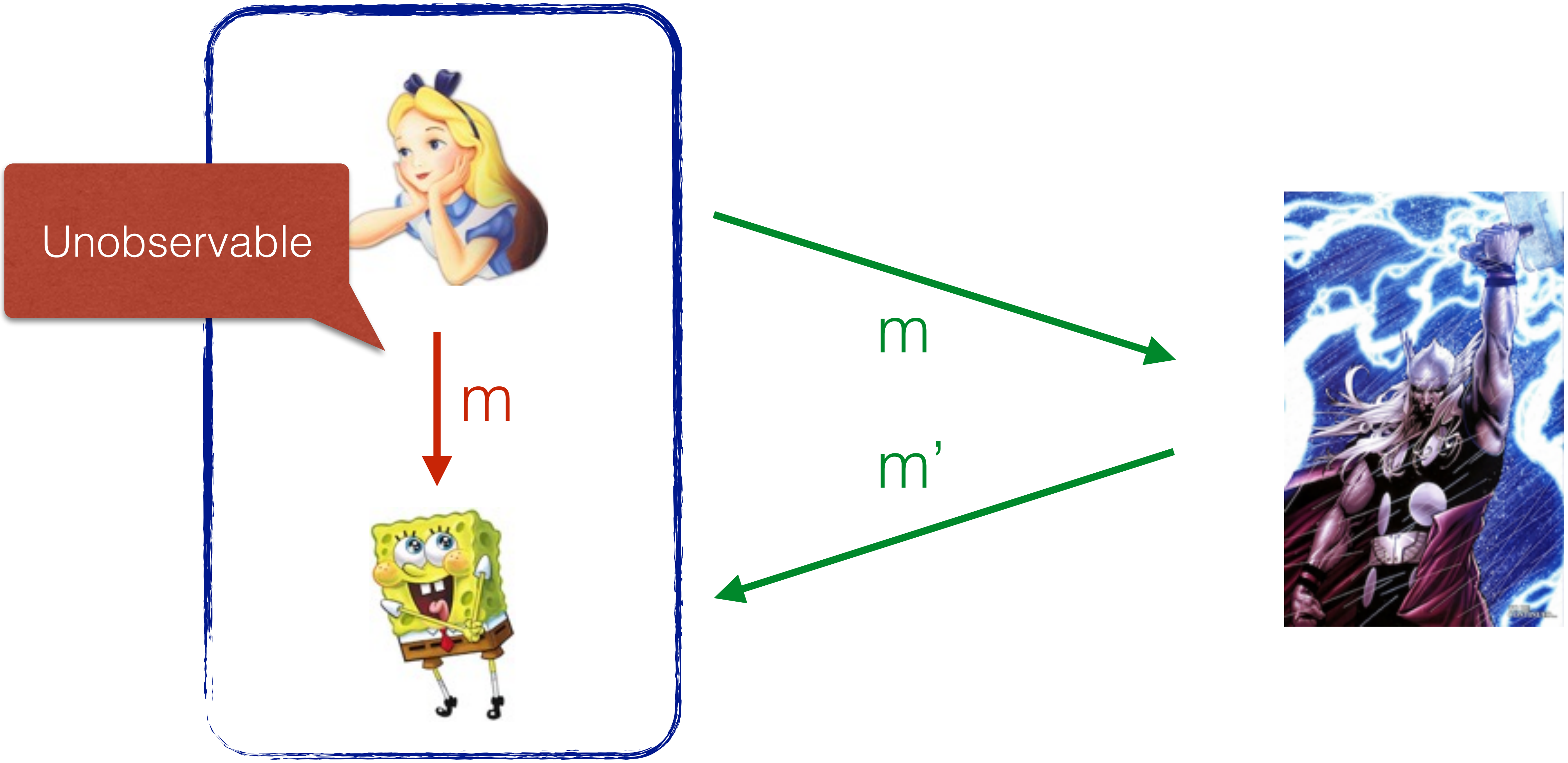
5 min talk
30/06/2016
INRIA, LORIA

I'm almighty ! I can control the ~~lightning~~ network



m

m’

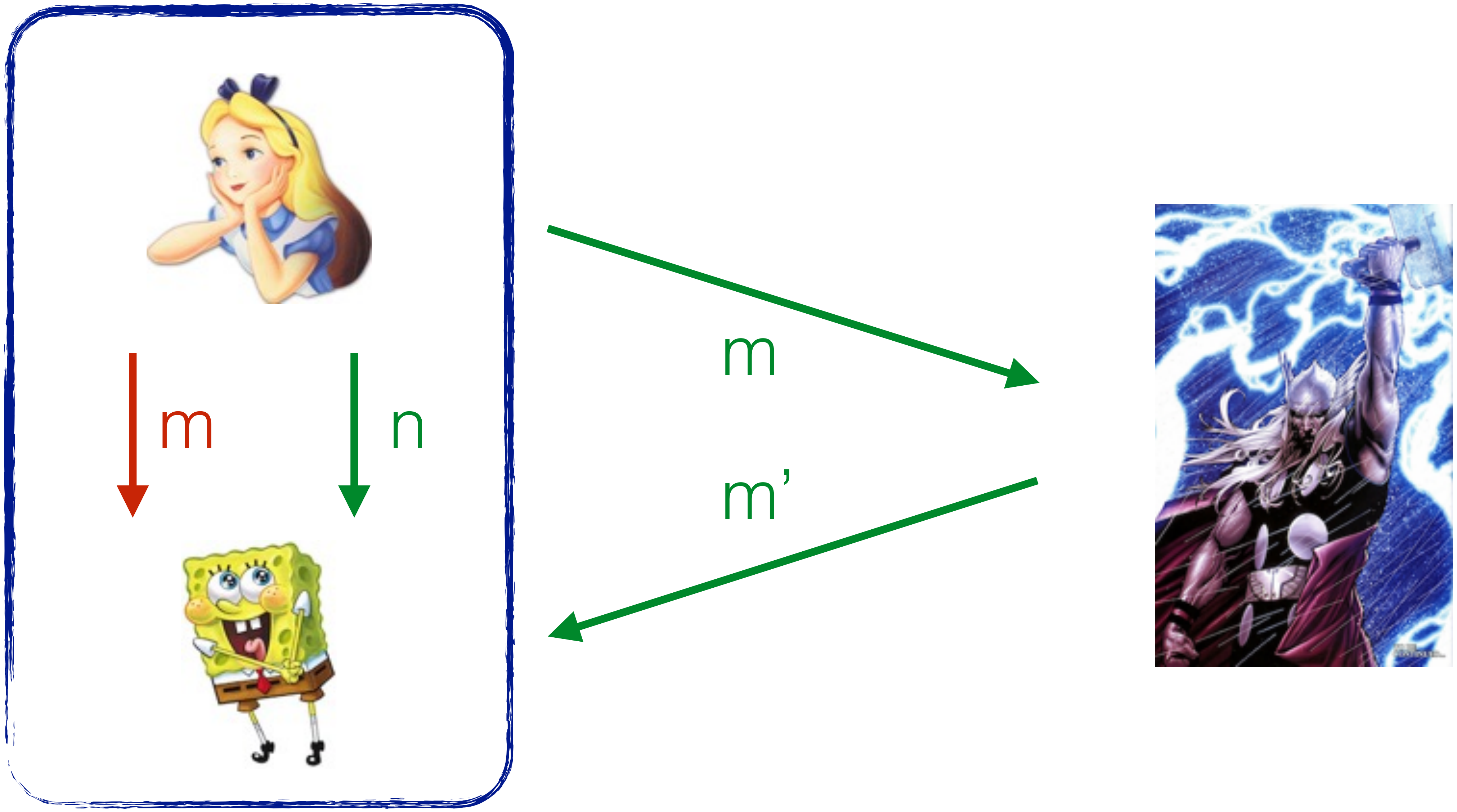


Unobservable

m

m

m’

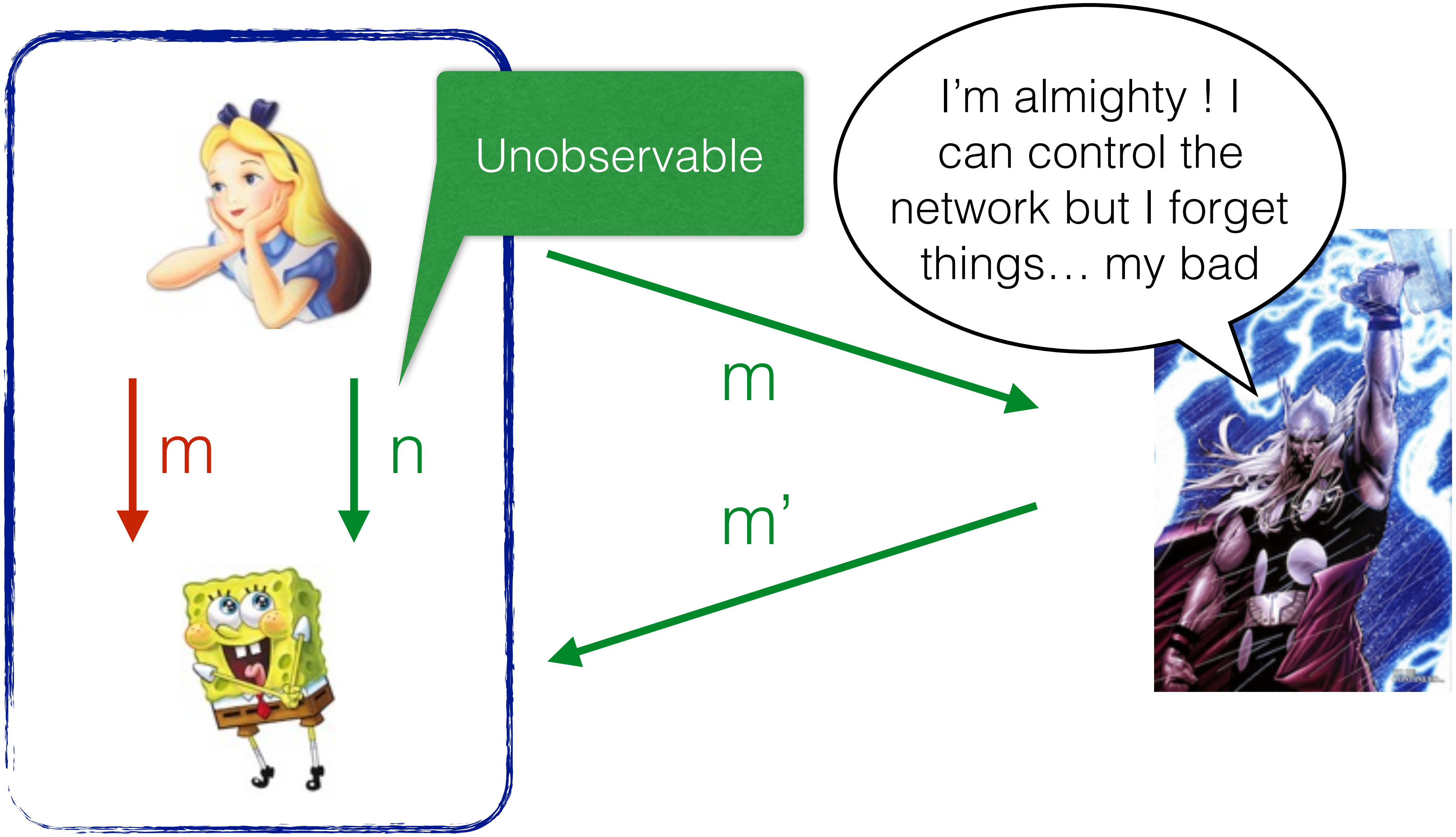


m

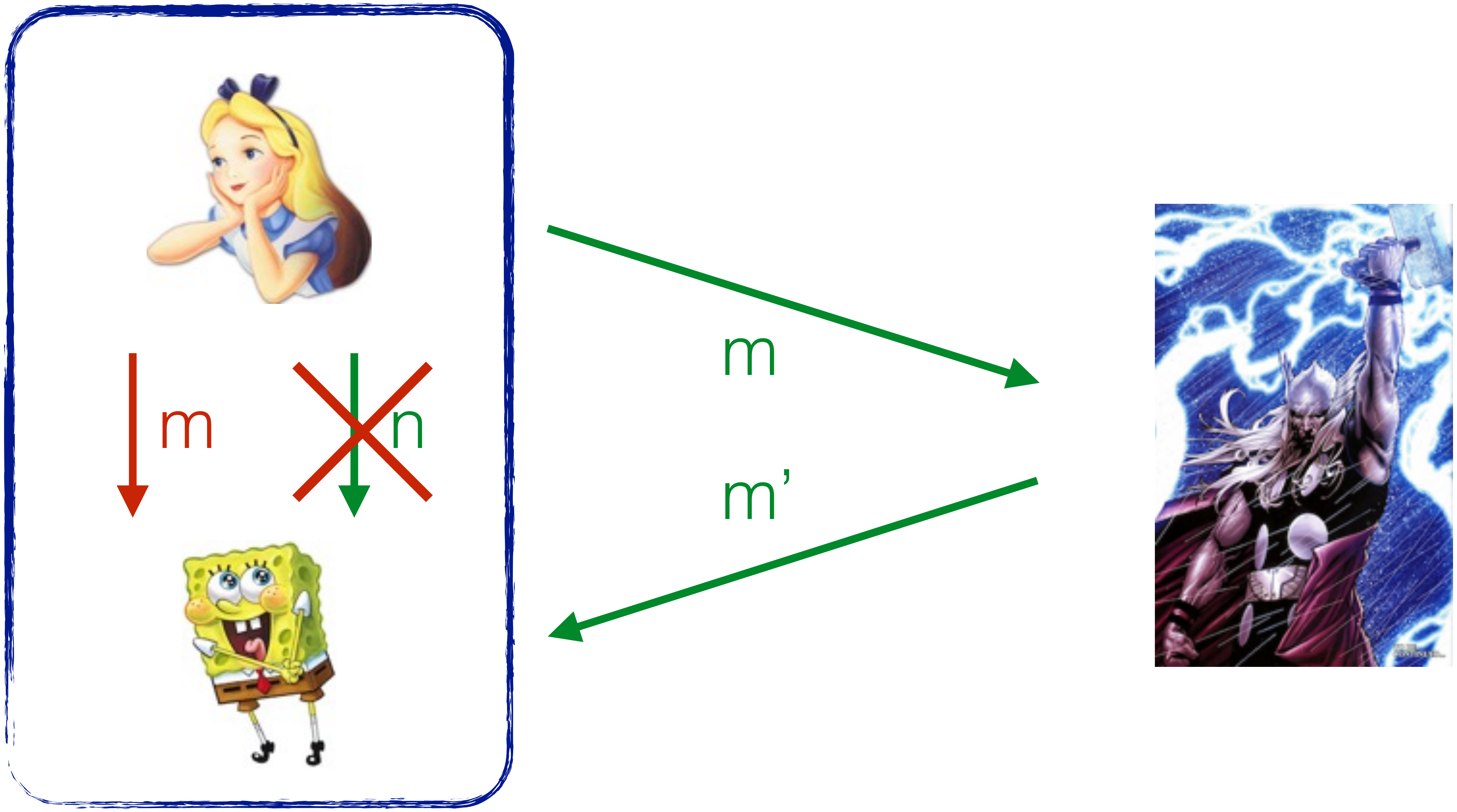
n

m

m’

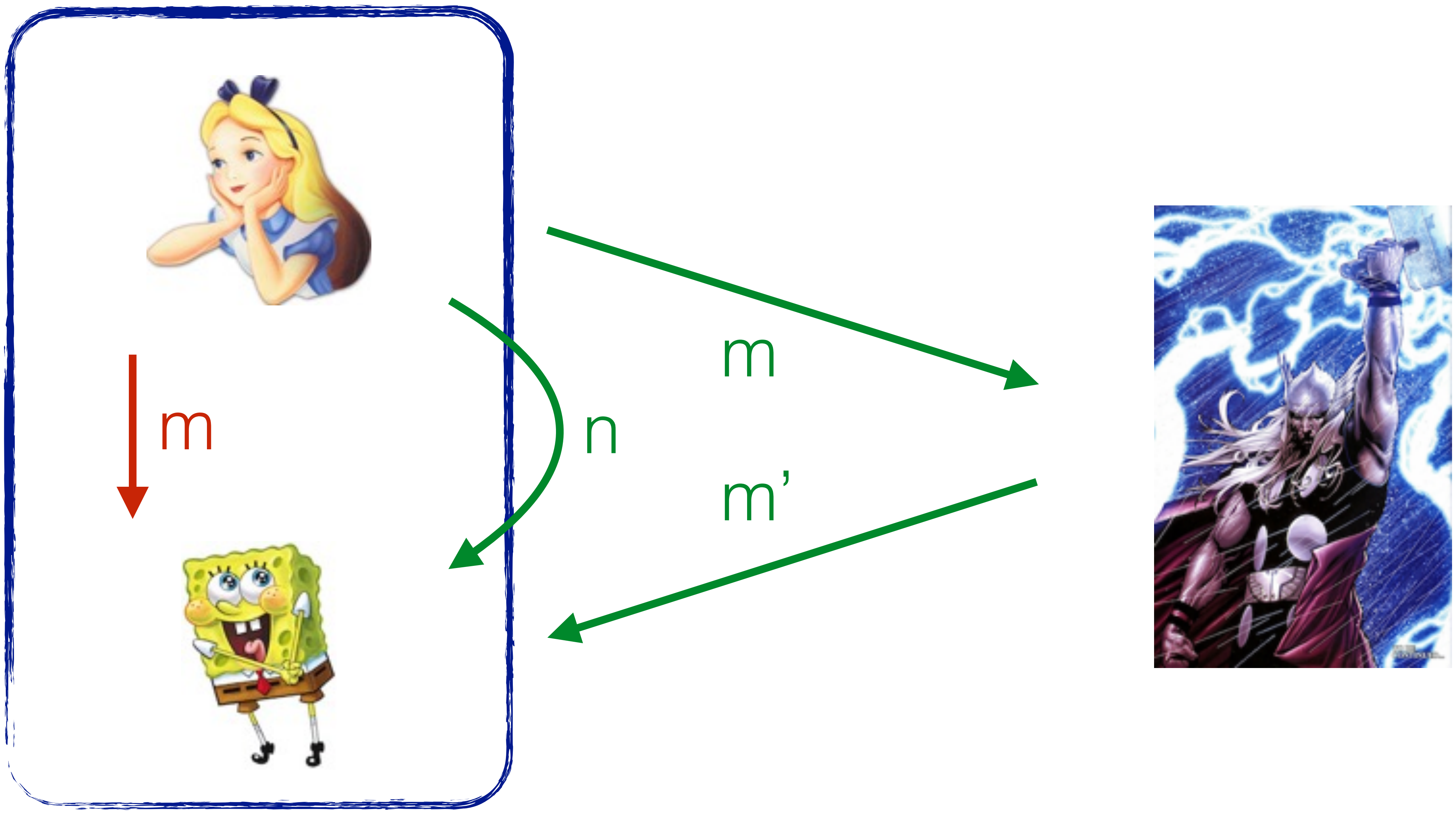

Unobservable
m
n
m
m’
I’m almighty ! I can control the network but I forget things… my bad

Applied pi :
Unobservable internal communication



Applied pi :
Unobservable internal communication

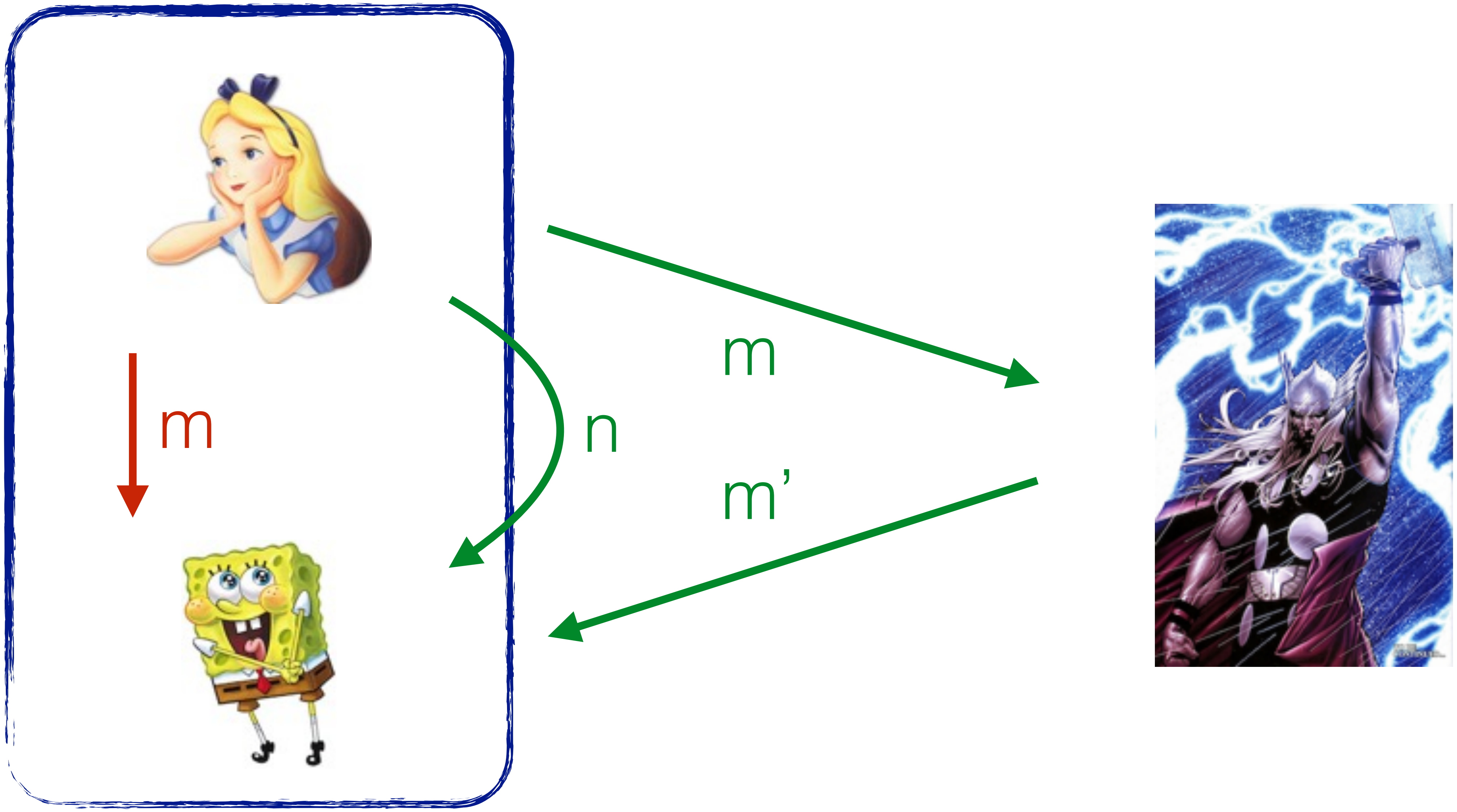
No internal communication on public channel



Observable public internal communication

Applied pi : Unobservable internal communication

No internal communication on public channel



Observable public internal communication

Applied pi : Unobservable internal communication

No internal communication on public channel

Equivalence: $\approx_o \quad \subset \quad \approx \quad \subset \quad \approx_n$

$A \approx_n B$ but $A \not\approx B$

$$\begin{aligned} P_1(x) = \quad & \mathtt{if}\ x = s_1\ \mathtt{then}\ \overline{d}\langle s_2 \rangle \\ & \mathtt{else\ if}\ x = s_2\ \mathtt{then}\ \overline{d}\langle a \rangle \end{aligned}$$

$$P_2(x) = \quad \mathtt{if}\ x = s_1\ \mathtt{then}\ \overline{d}\langle s_2 \rangle$$

Protocol A

$$\nu s_1.\nu s_2.(\overline{c}\langle s_1\rangle.c(x).P_1(x) \mid c(x).P_2(x))$$

Protocol B

$$\nu s_1.\nu s_2.(\overline{c}\langle s_1\rangle.c(x).P_2(x) \mid c(x).P_1(x))$$