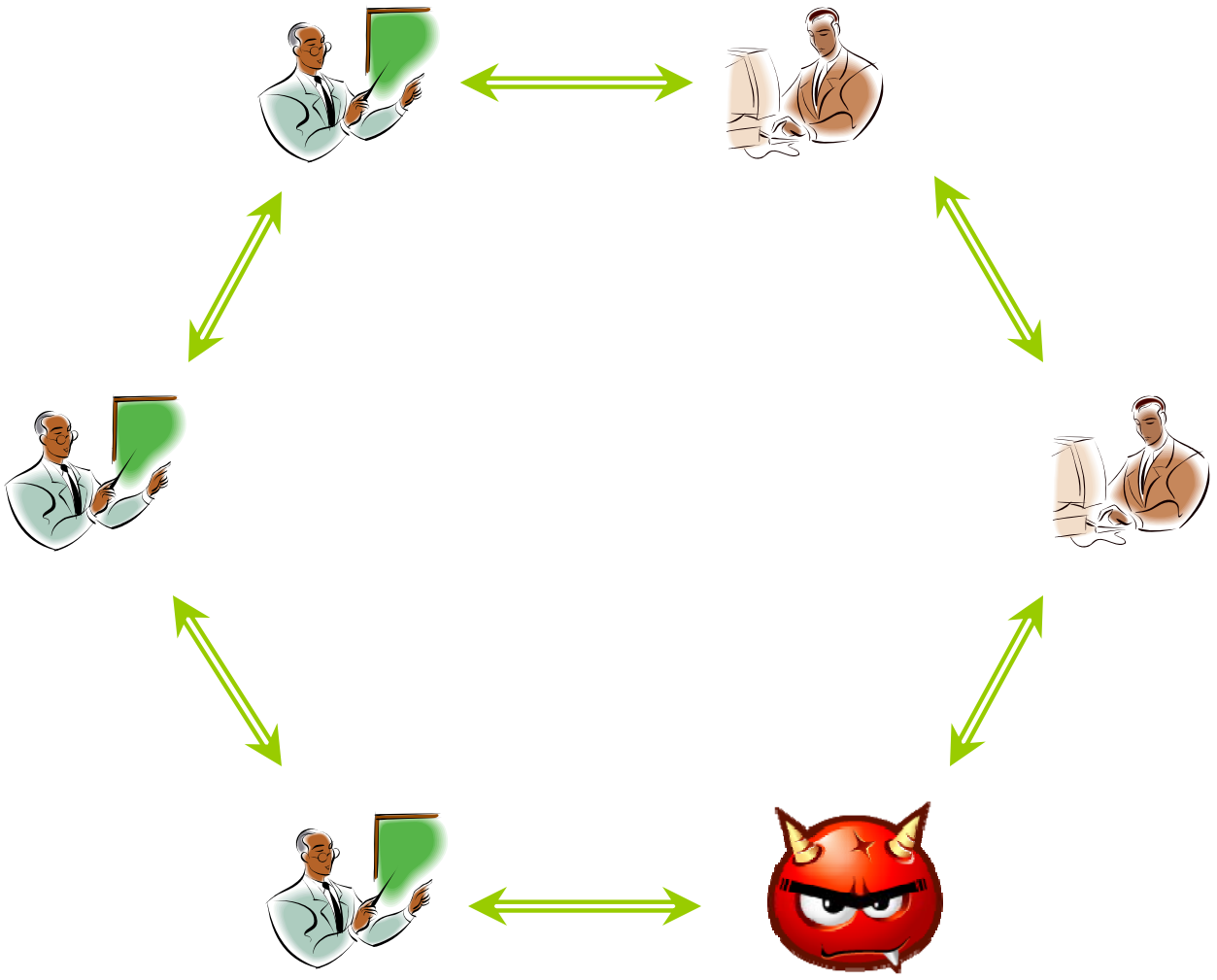
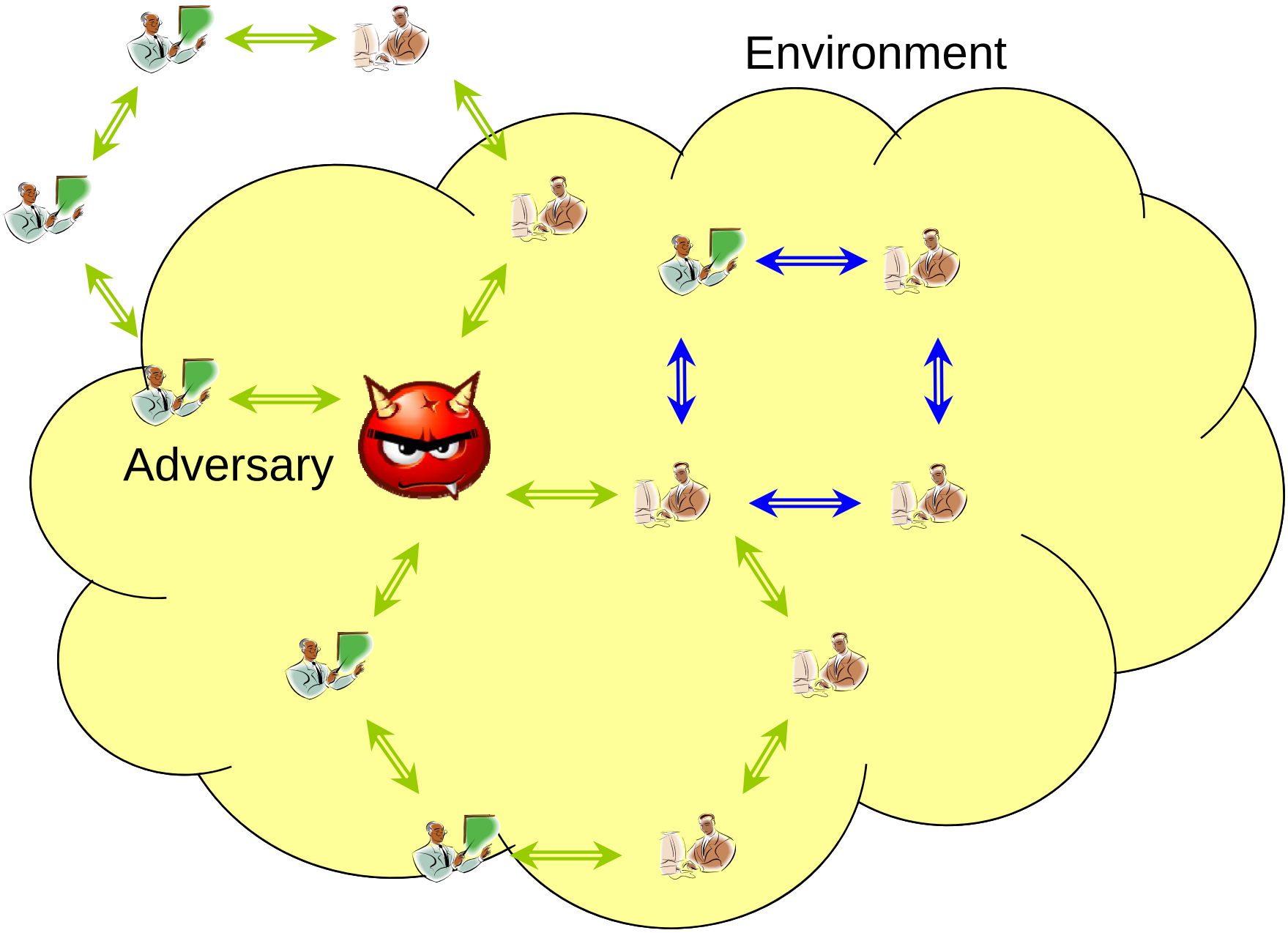
Unified framework for Secure Multiparty Computation

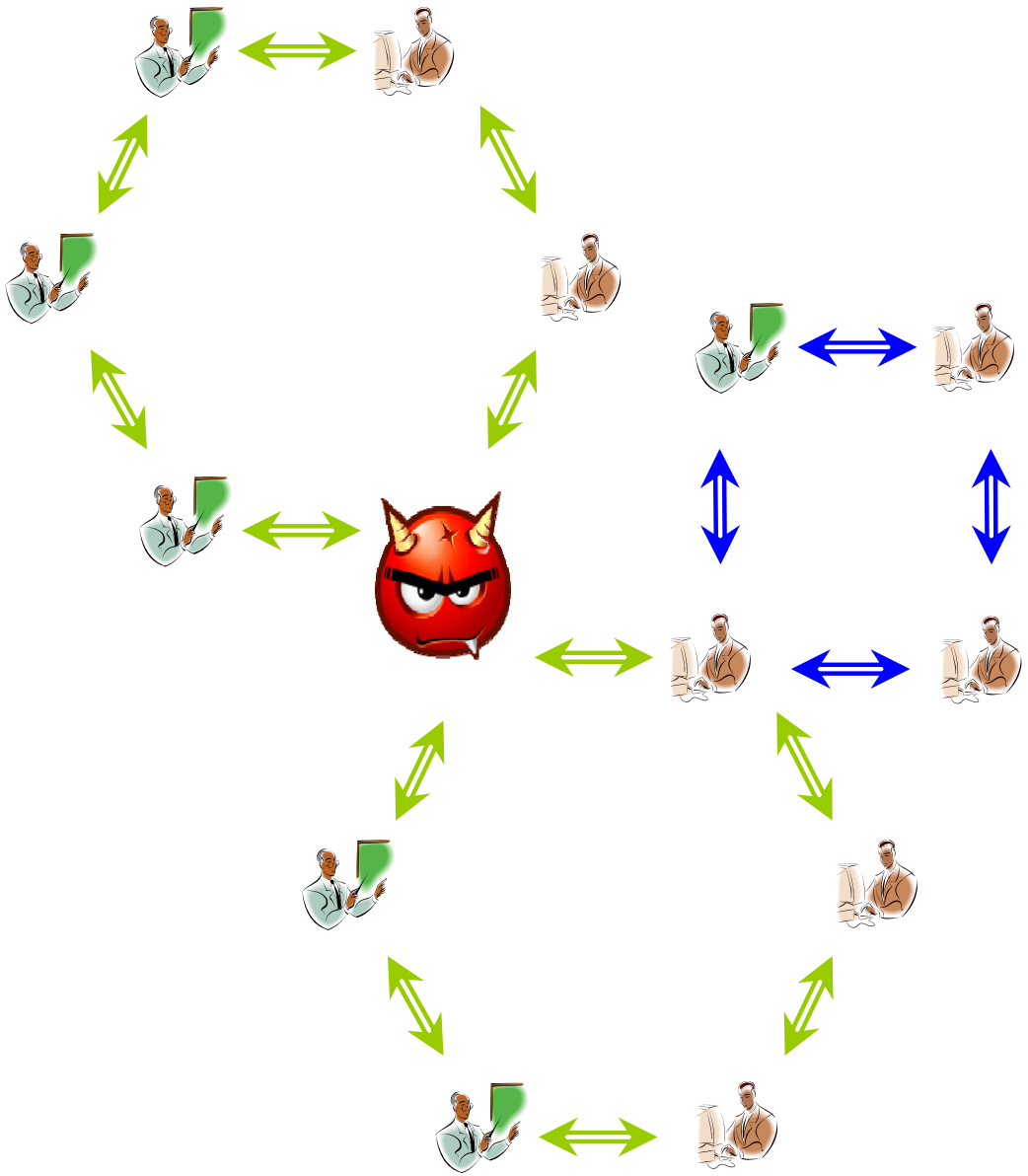
Huijia Lin

Rafael Pass

Muthu Venkitasubramaniam

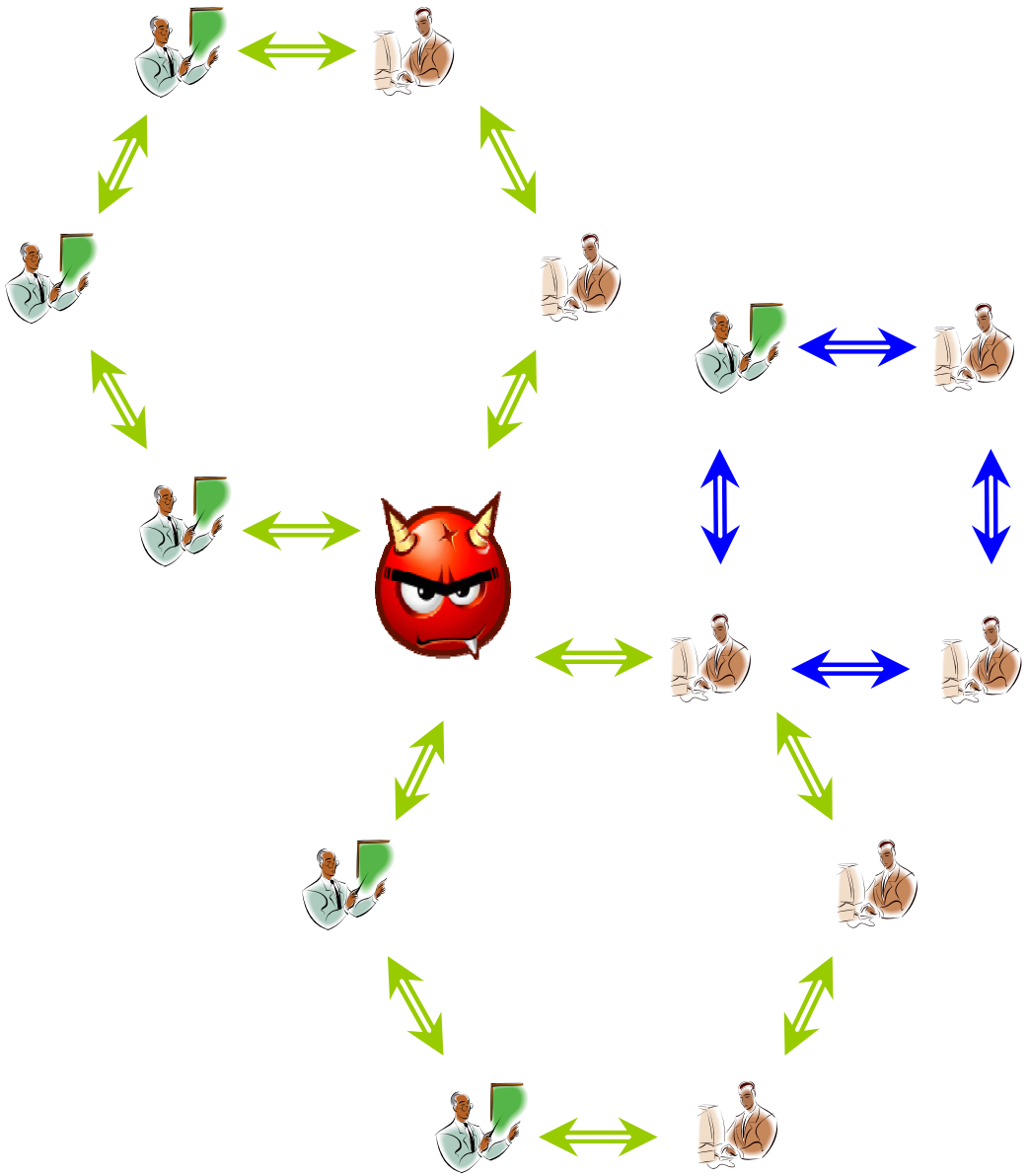



Environment
Adversary



UC model [C01]

concurrent
different protocols



UC model [C01]

concurrent
different protocols

Unrealizable

Timing model
[KLP05]

CRS model
[CLOS02]

Setup

Sunspot model
[CPS07]

Timing model
[KLP05]

CRS model
[CLOS02]

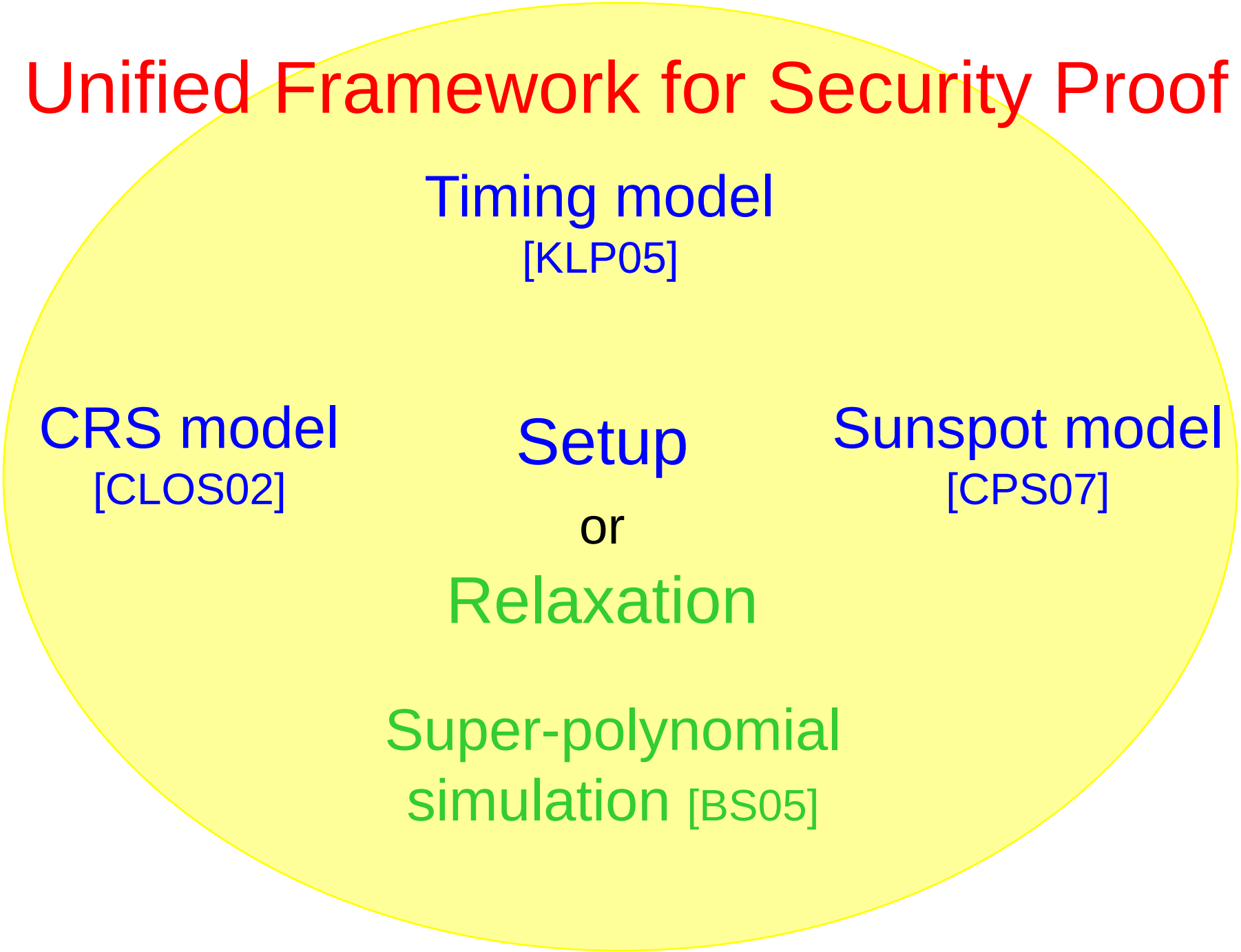
Setup

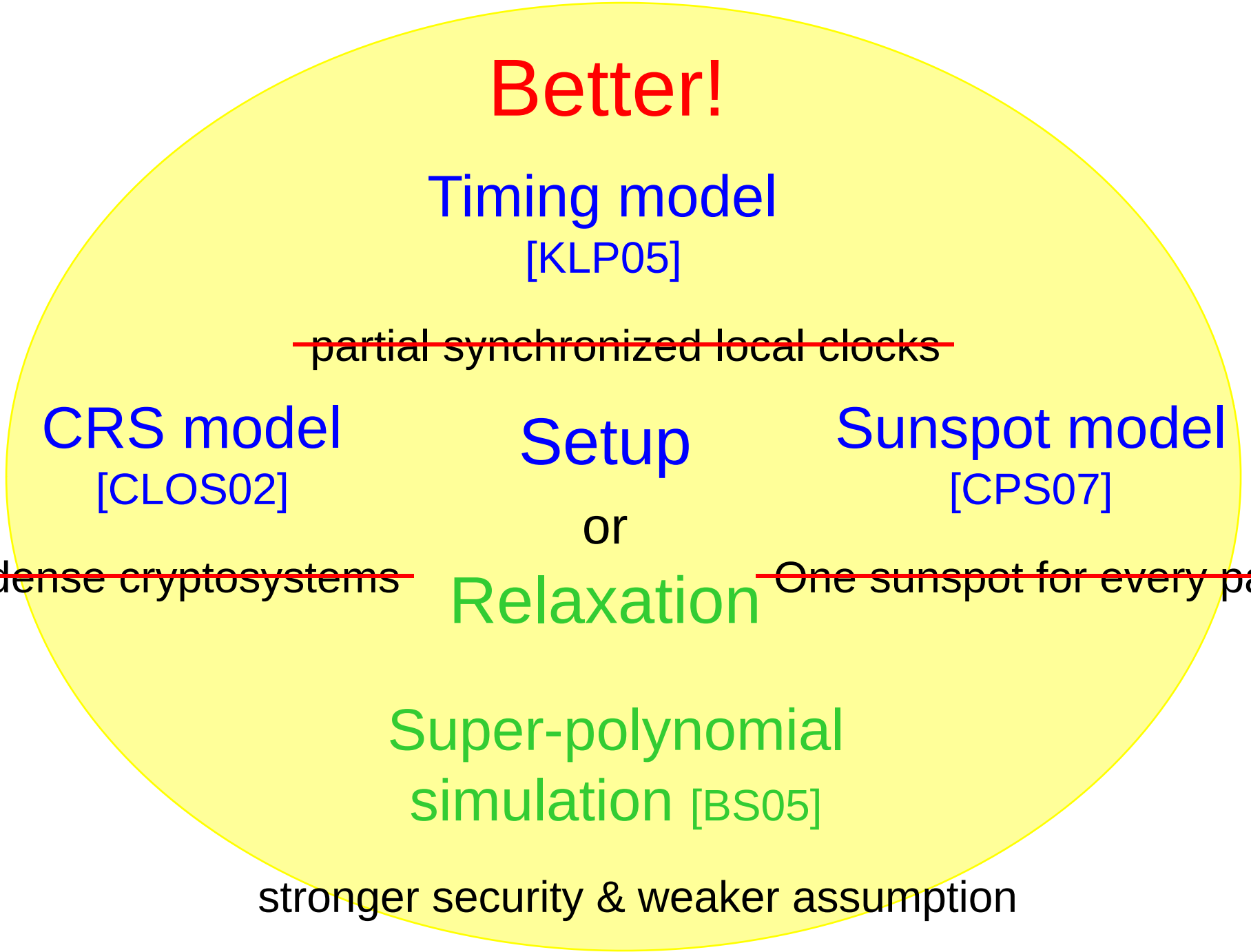
or

Relaxation

Super-polynomial simulation [BS05]

Sunspot model
[CPS07]


Unified Framework for Security Proof
Timing model
[KLP05]
CRS model
[CLOS02]
Setup
or
Relaxation
Sunspot model
[CPS07]
Super-polynomial
simulation [BS05]


Better!
Timing model
[KLP05]
partial synchronized local clocks
CRS model
[CLOS02]
dense cryptosystems
Setup
or
Relaxation
Sunspot model
[CPS07]
One sunspot for every pair
Super-polynomial simulation [BS05]
stronger security & weaker assumption

Stand-alone Model:

O(*log* n) —ETDP→ O(*log log* n)

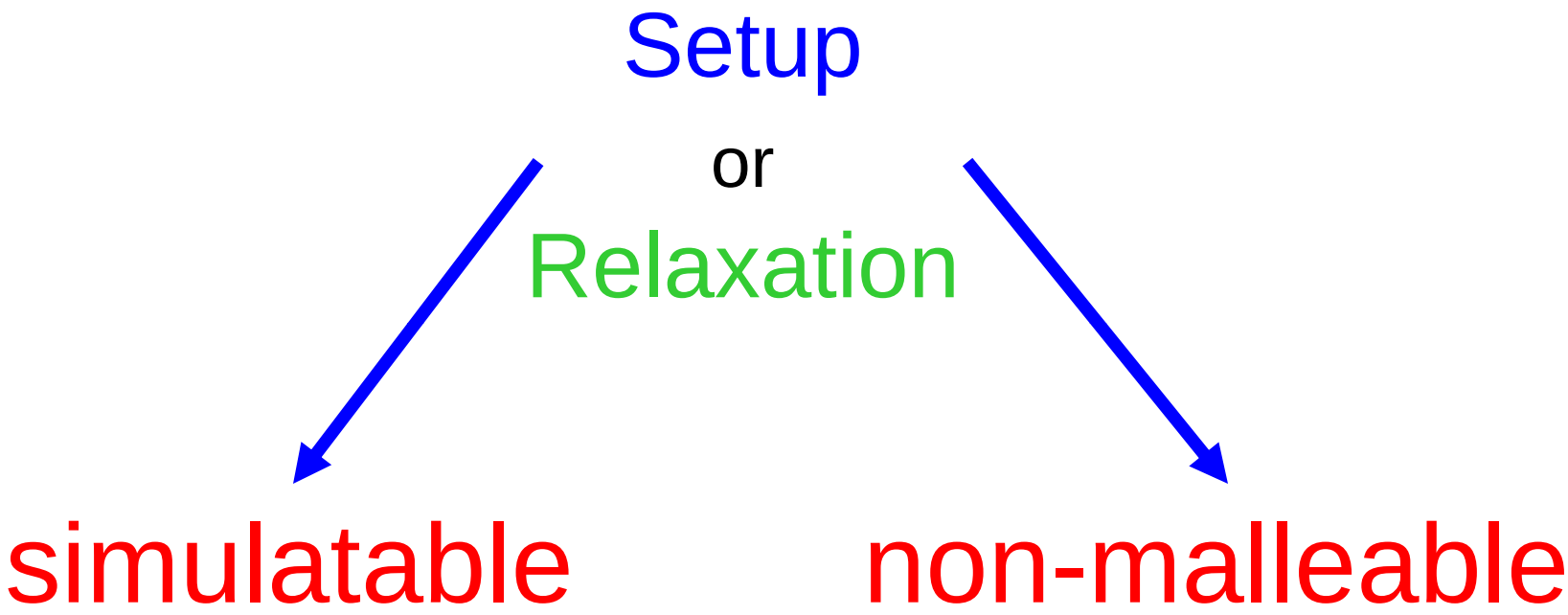
dense cryptosystem ~~dense cryptosystem~~

—CRH→ O(1)

Timing Model:

O(n) —ETDP→ O(*log* n)

—CRH→ O(1)


Setup
or
Relaxation
simulatable
non-malleable

Setup

or

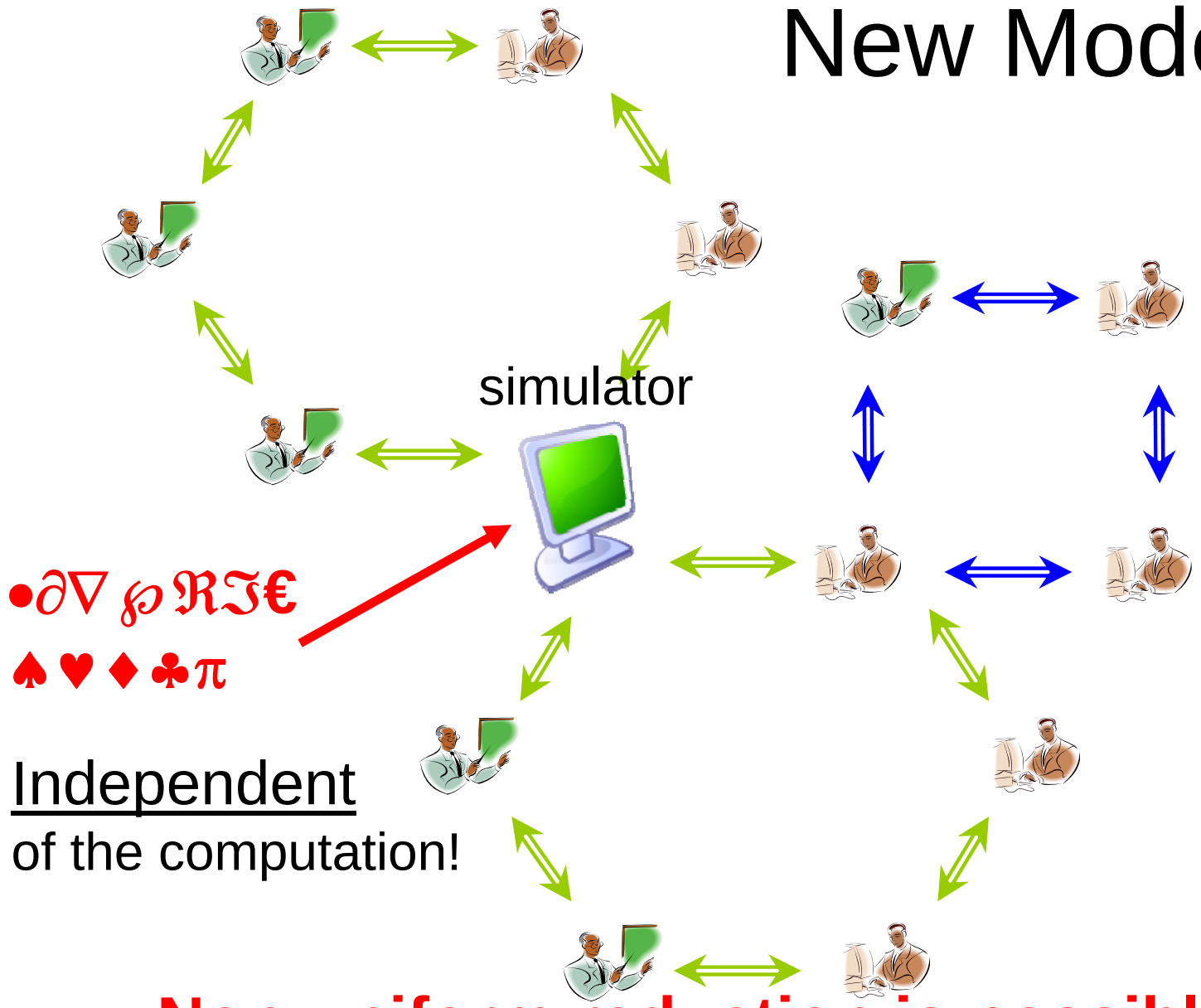
Relaxation

simulatable

Stand-alone
non-malleable
commitment

non-malleable

New Model



Independent
of the computation!

Non-uniform reduction is possible!