Advanced Tools from Modern Cryptography

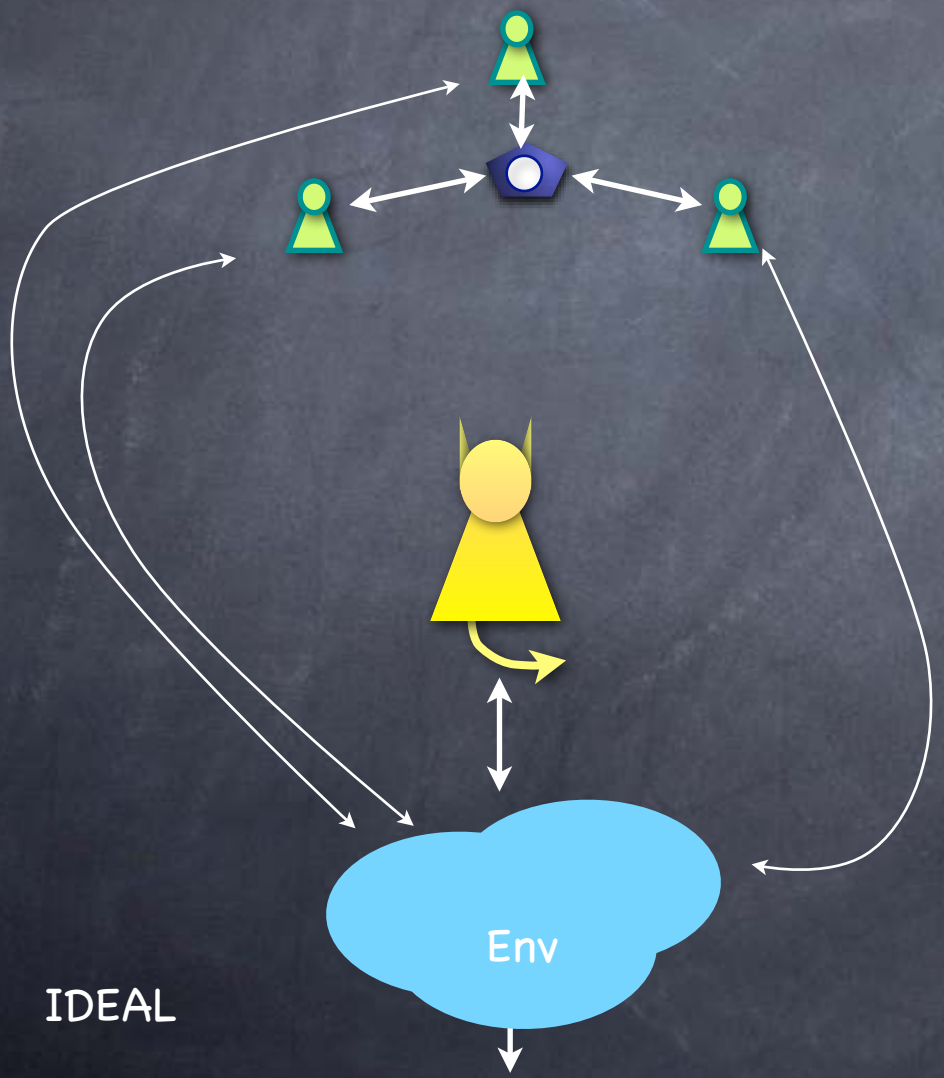
Lecture 11

MPC: UC Theorem. UC Limitations.

RECALL

UC Security

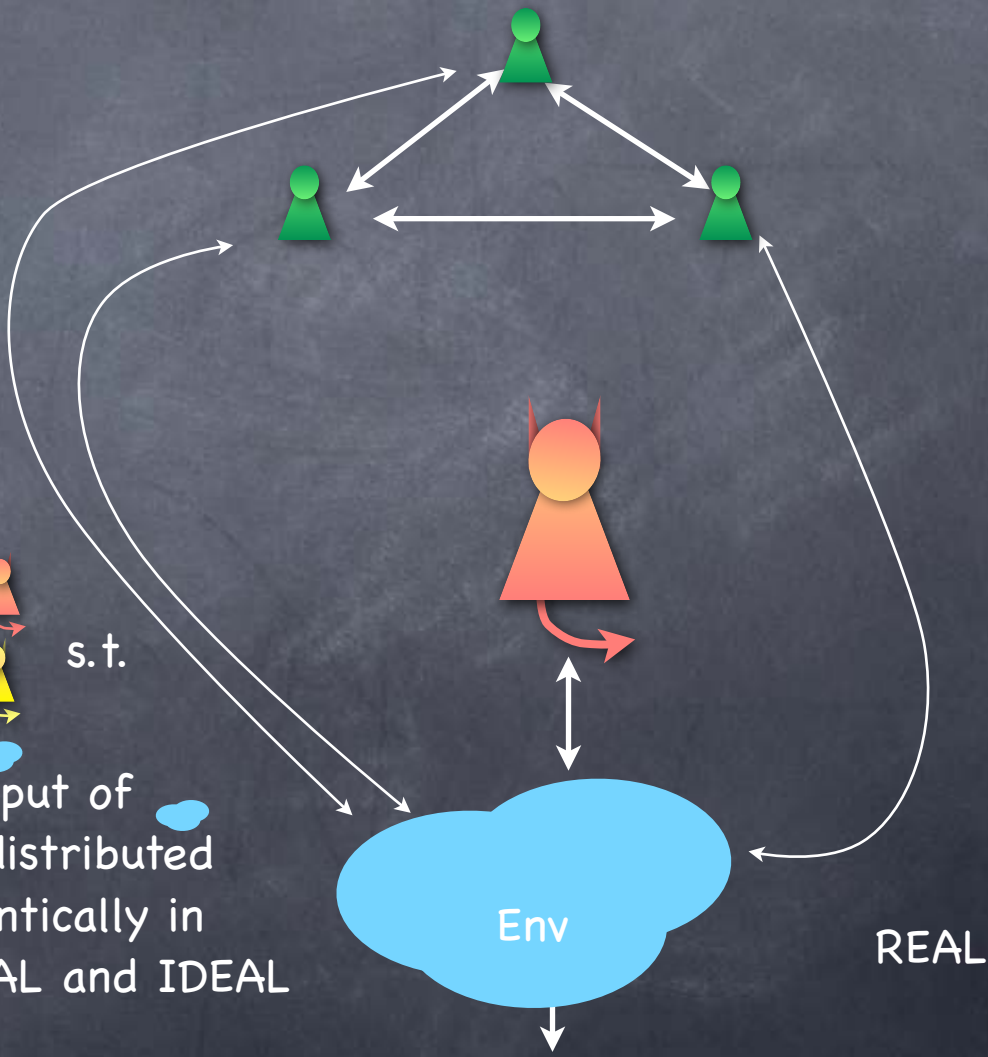
REAL is as secure as IDEAL if:



IDEAL

$\forall$ $\exists$ $\forall$ s.t.

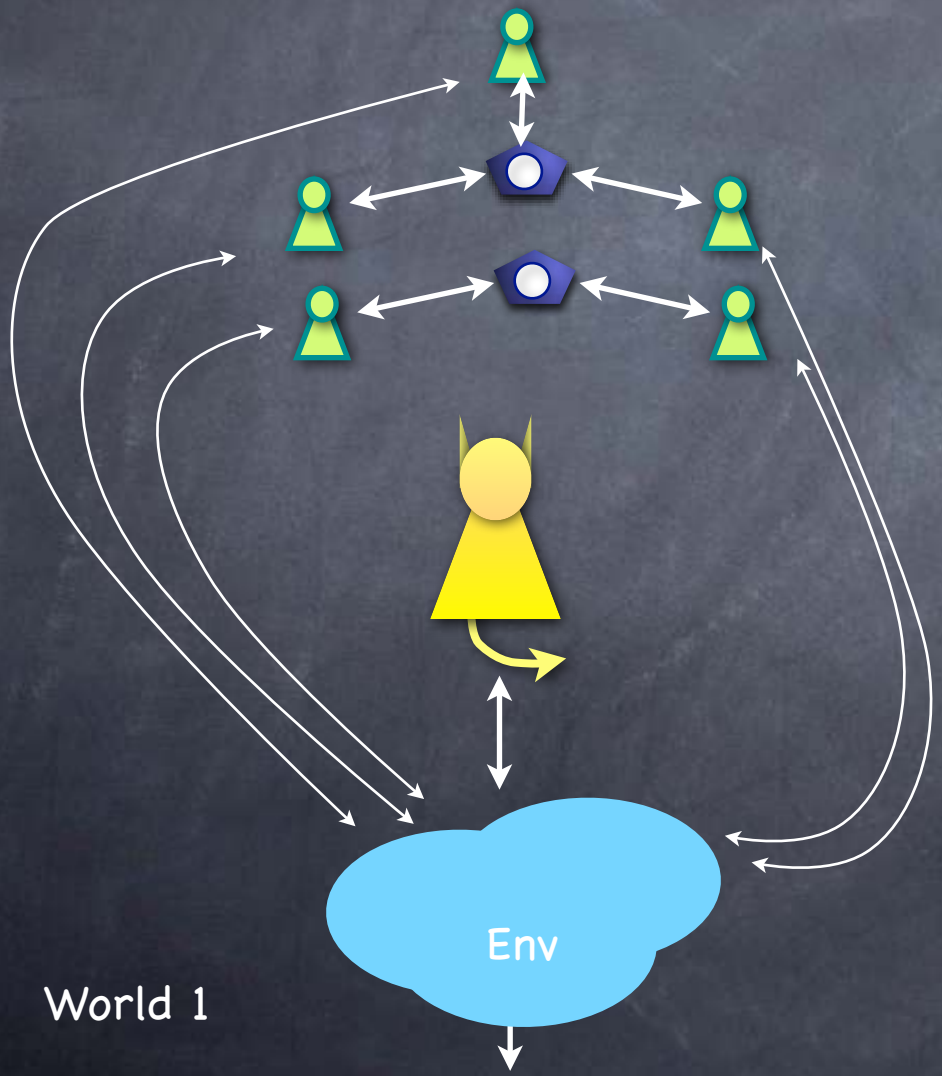
output of
is distributed
identically in
REAL and IDEAL

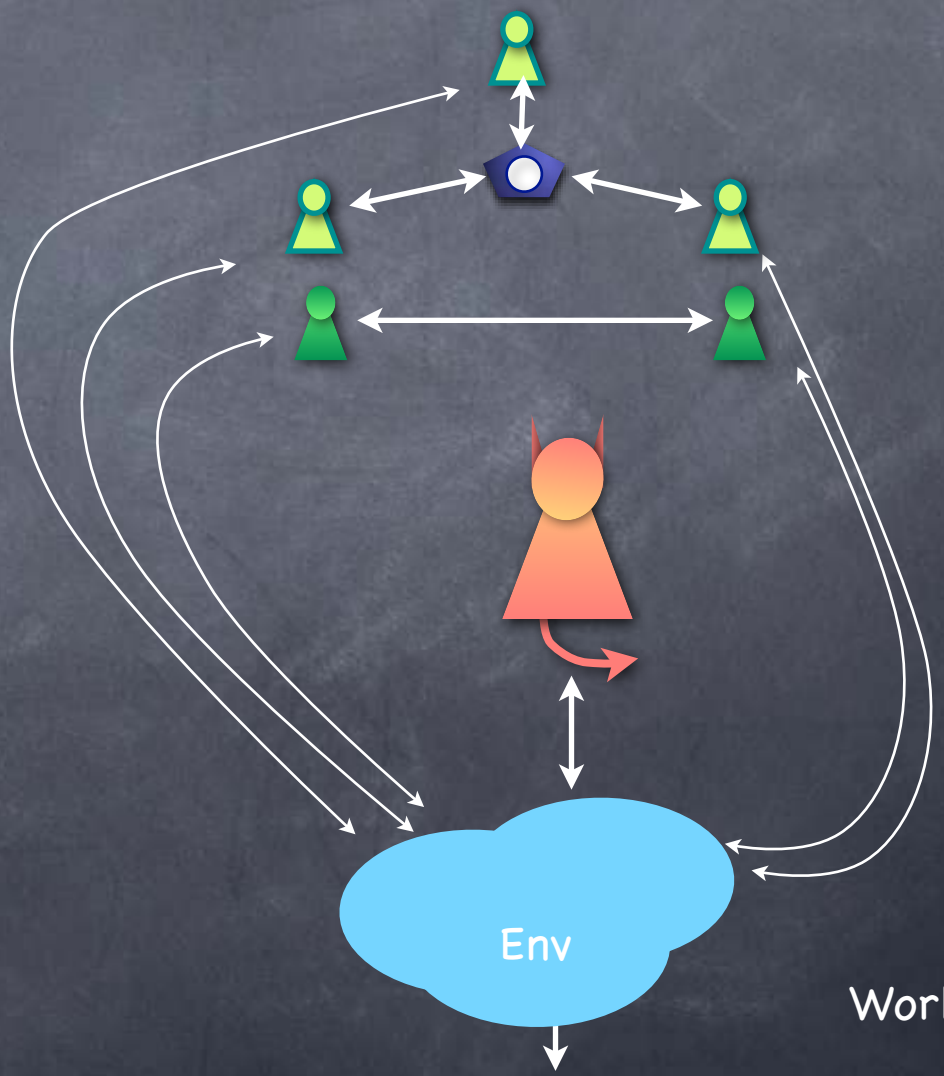


REAL

Universal Composition

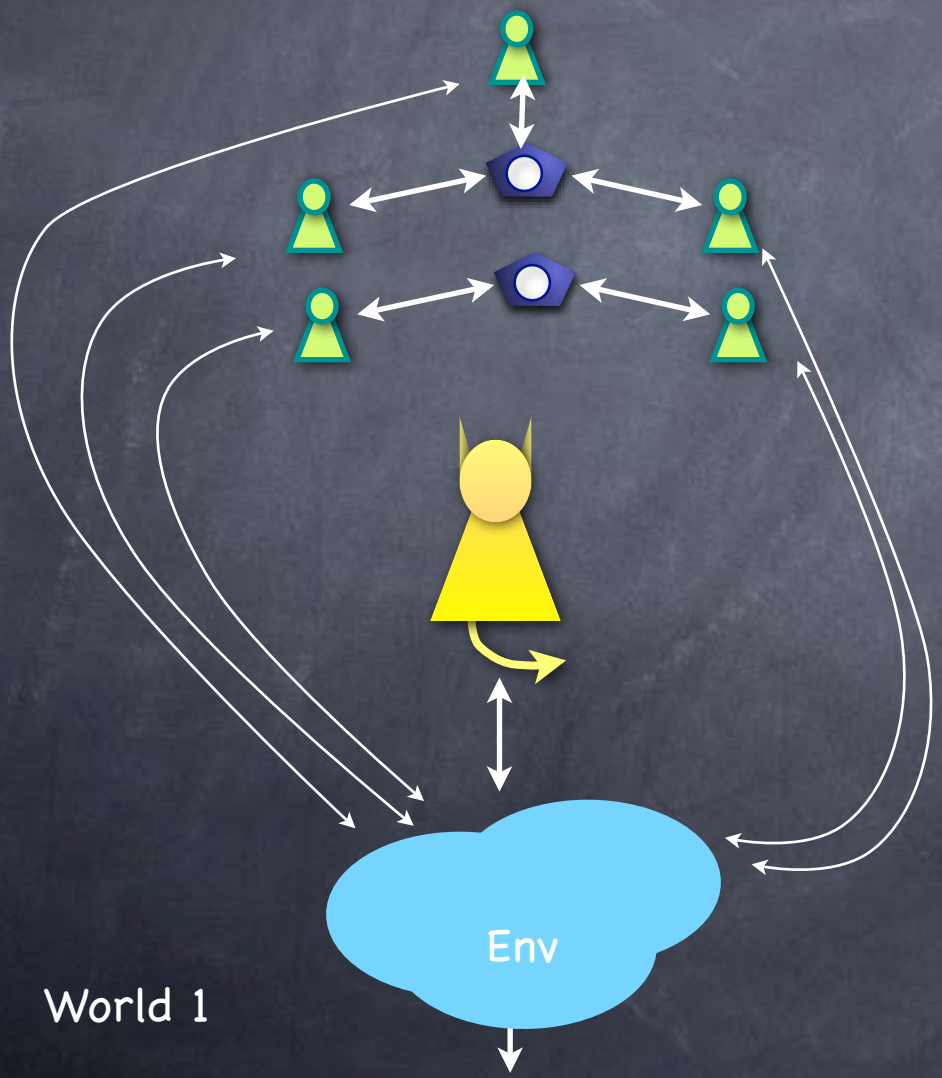
Replace protocol  with  which is as secure, etc.



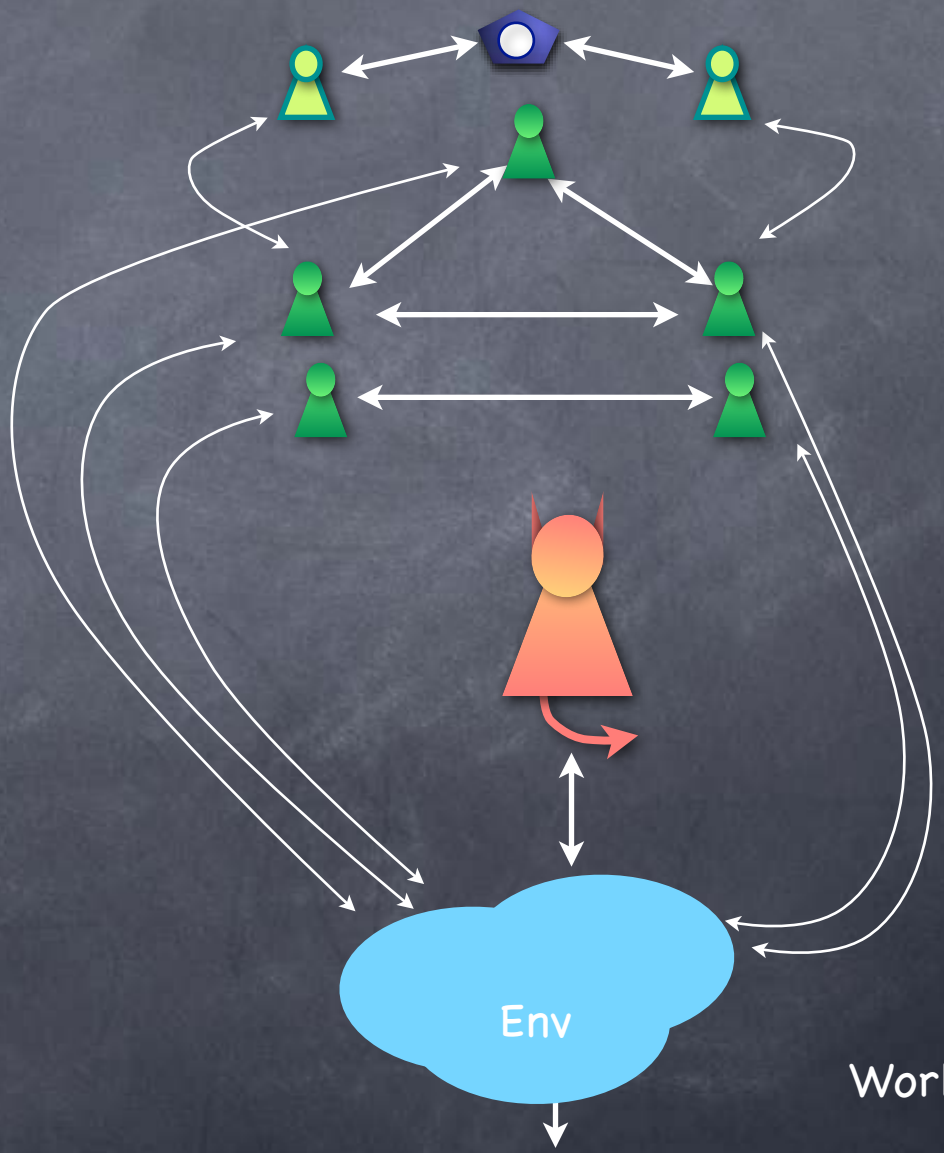


Universal Composition

Replace protocol  with  which is as secure, etc.



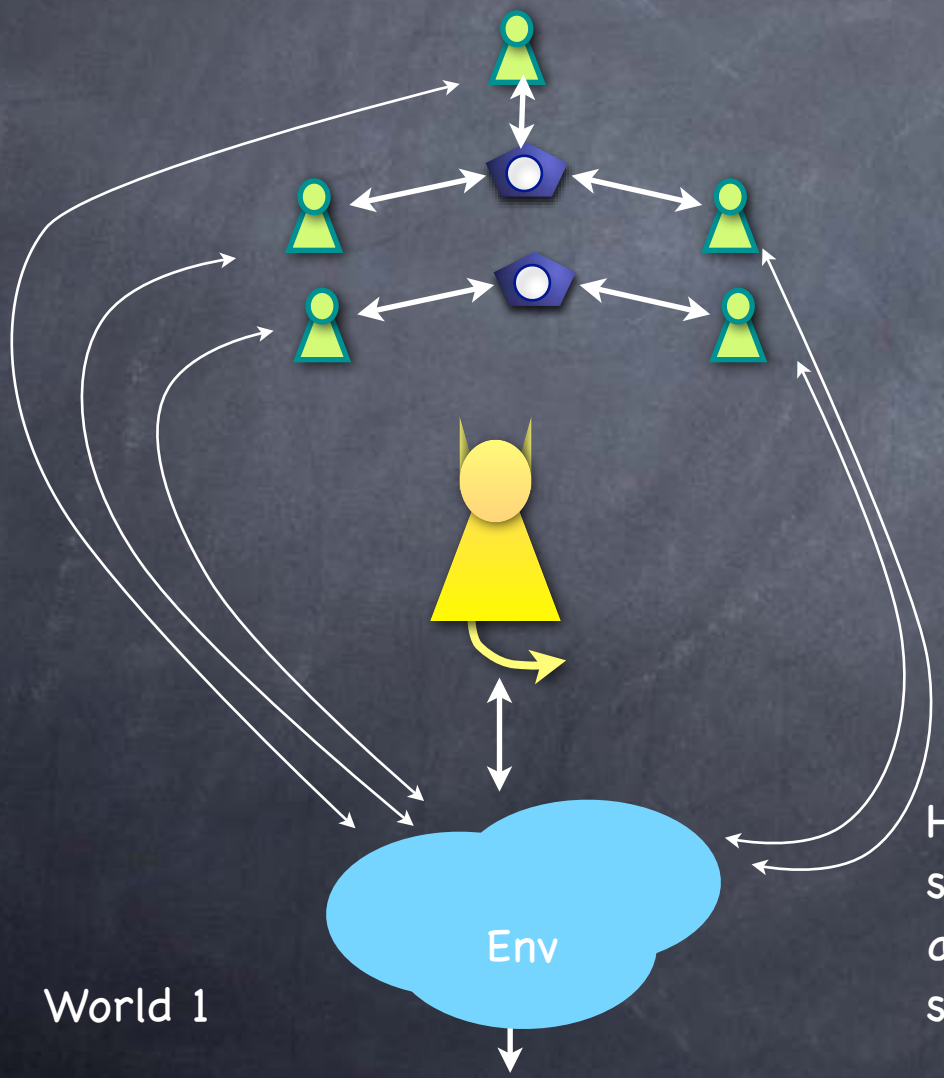
World 1



World 3

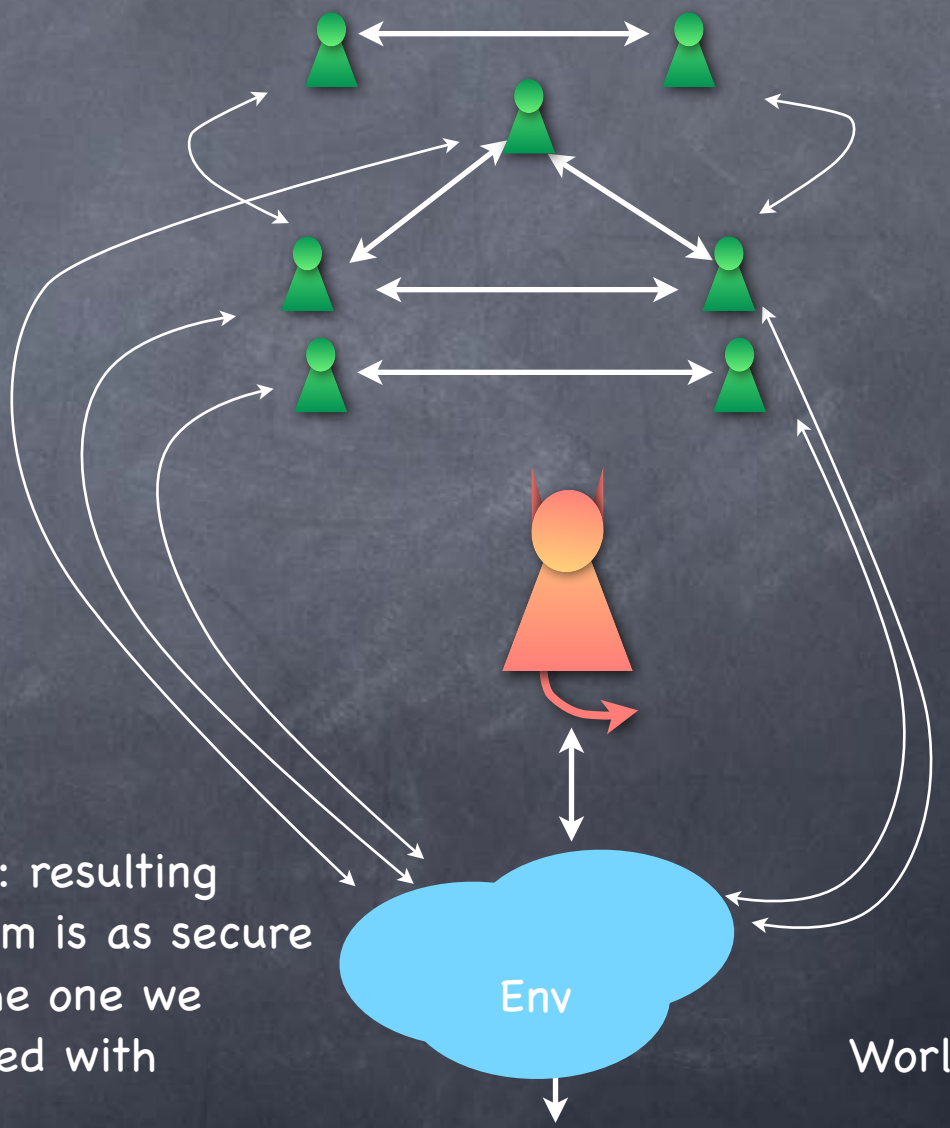
Universal Composition

Replace protocol  with  which is as secure, etc.



World 1

Hope: resulting system is as secure as the one we started with



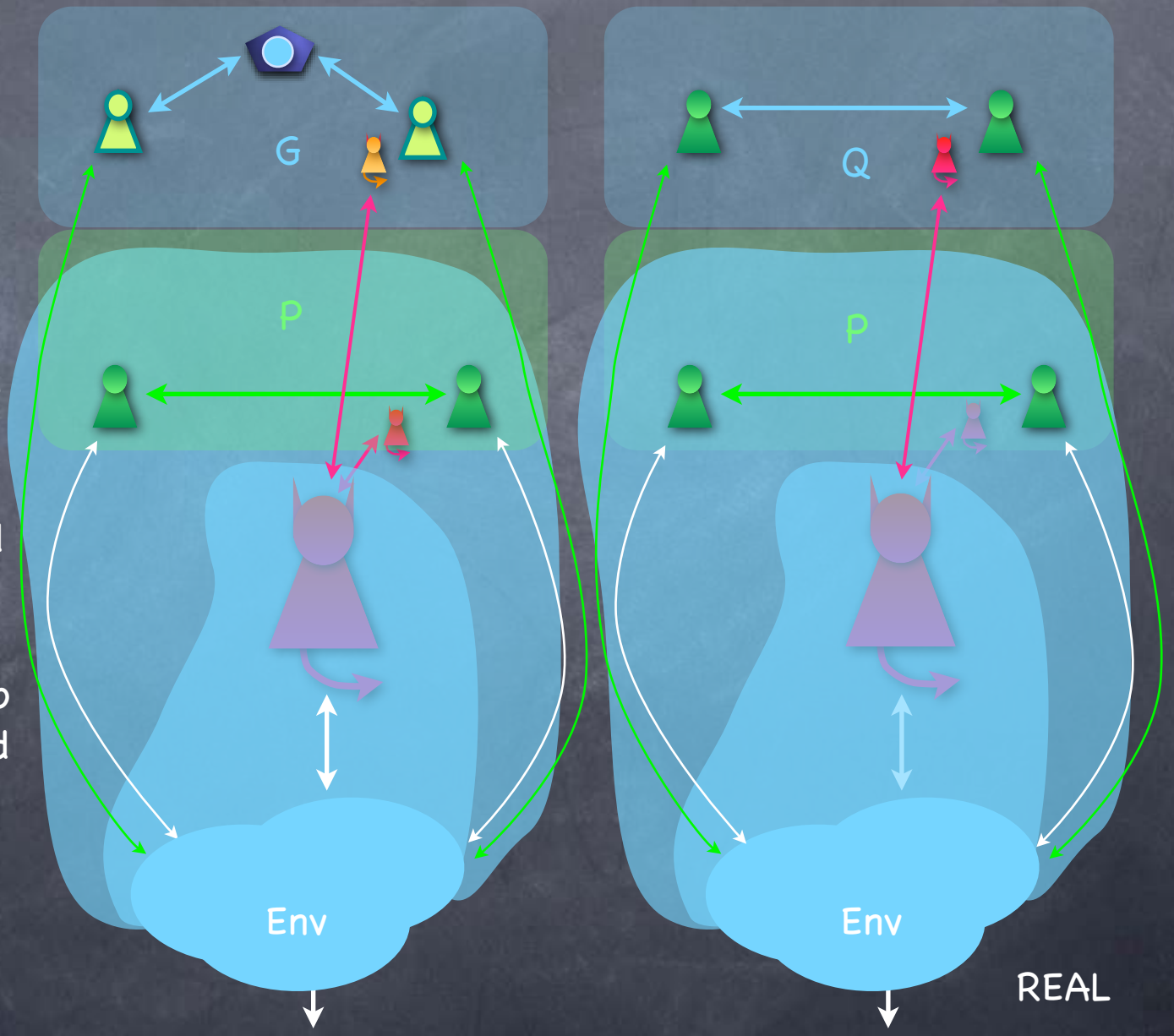
World 4

Universal Composition

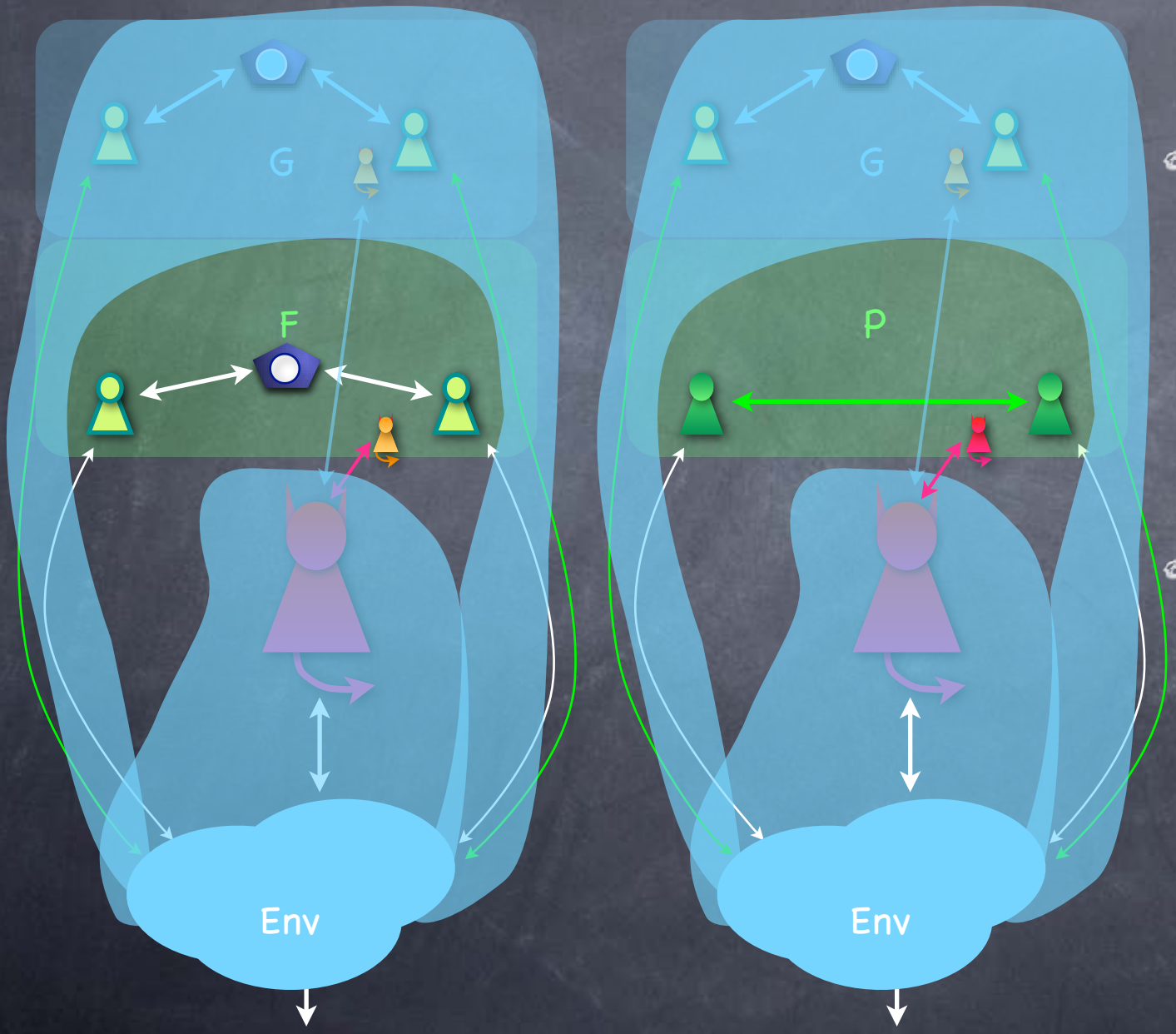
- Start from world A (think "IDEAL")
  - Repeat (for any poly number of times):
    - For some 2 "protocols" (that possibly make use of ideal functionalities) I and R such that R is as secure as I, substitute an I-session by an R-session
  - Say we obtain world B (think "REAL")
  - UC Theorem: Then world B is as secure as world A
- Gives a modular implementation of the IDEAL world

Proving the UC theorem

- Consider environment which runs the adversary internally, and depends on "dummy adversaries" to interface with the protocols
- Now consider new environment s.t. only Q (and its adversary) is outside it
- Use "Q is as secure as G" to get a new world with G and a new adversary

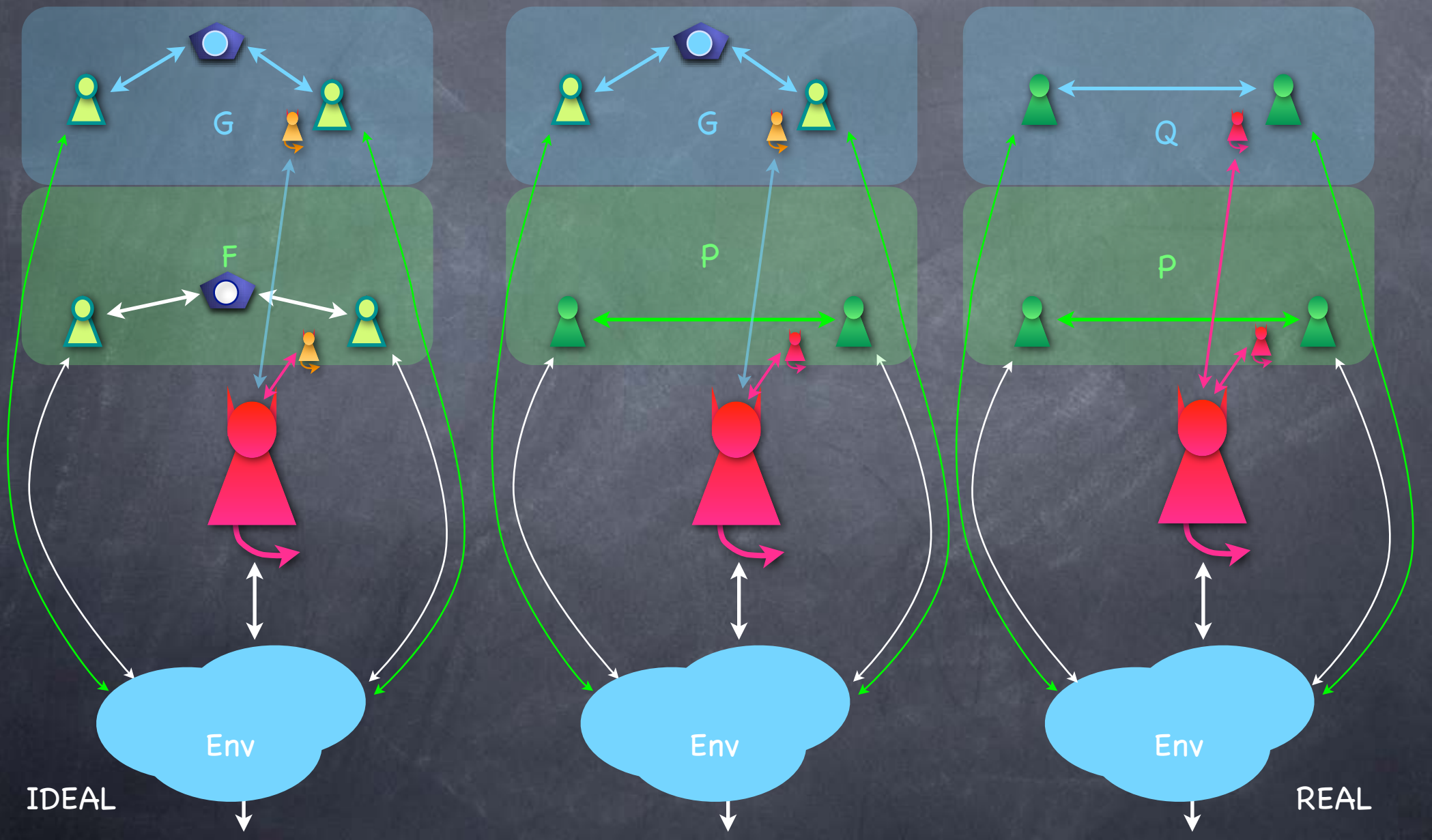


Proving the UC theorem

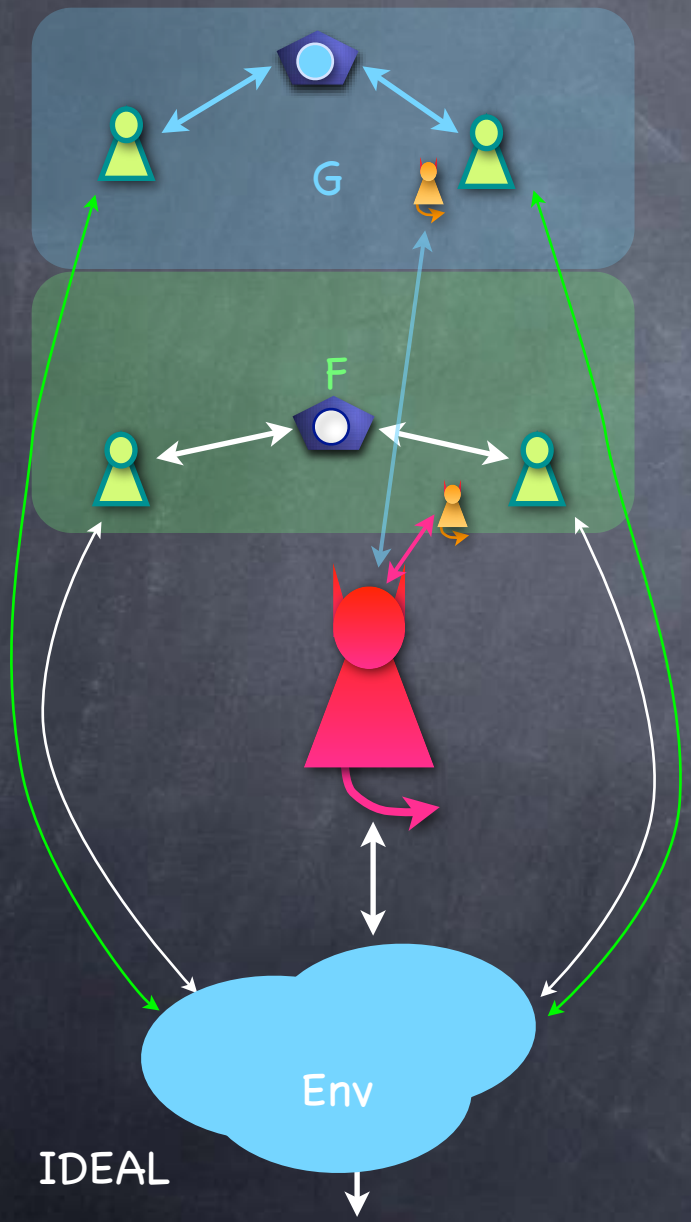


- Now consider new environment s.t. only P (and adversary) is outside it
  - Note: G and simulator for Q/G are inside the new environment
- Use "P is as secure as F" to get a new world with F and a new adversary

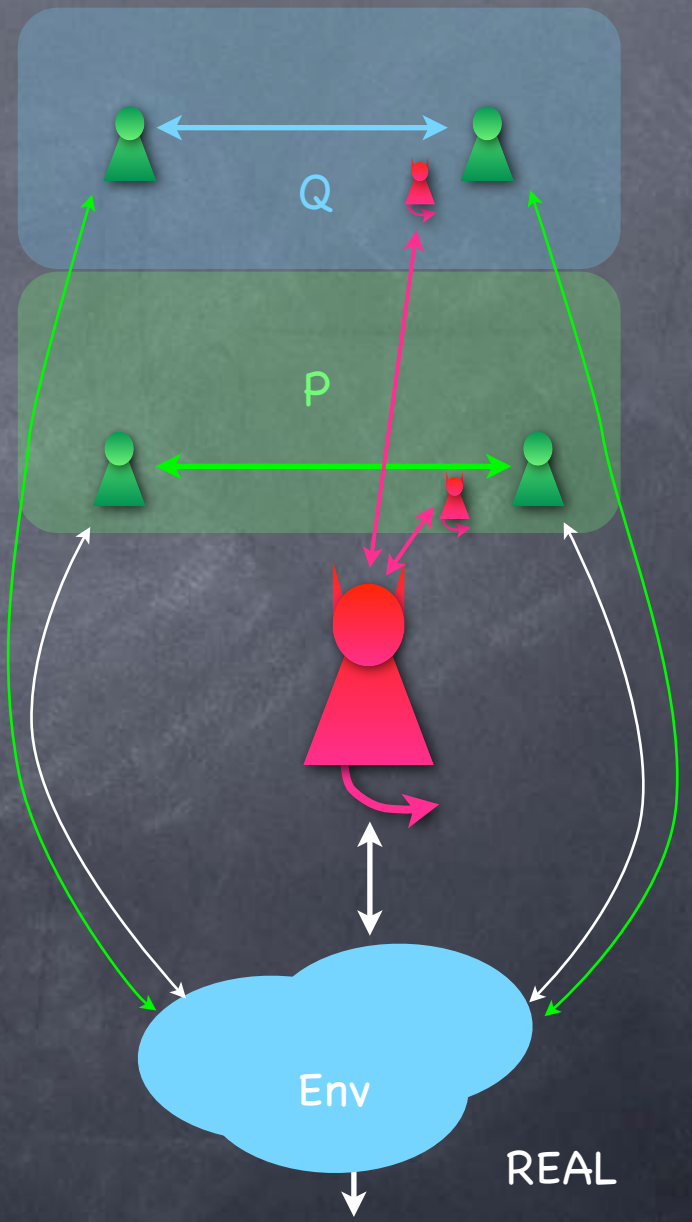
Proving the UC theorem



Proving the UC theorem



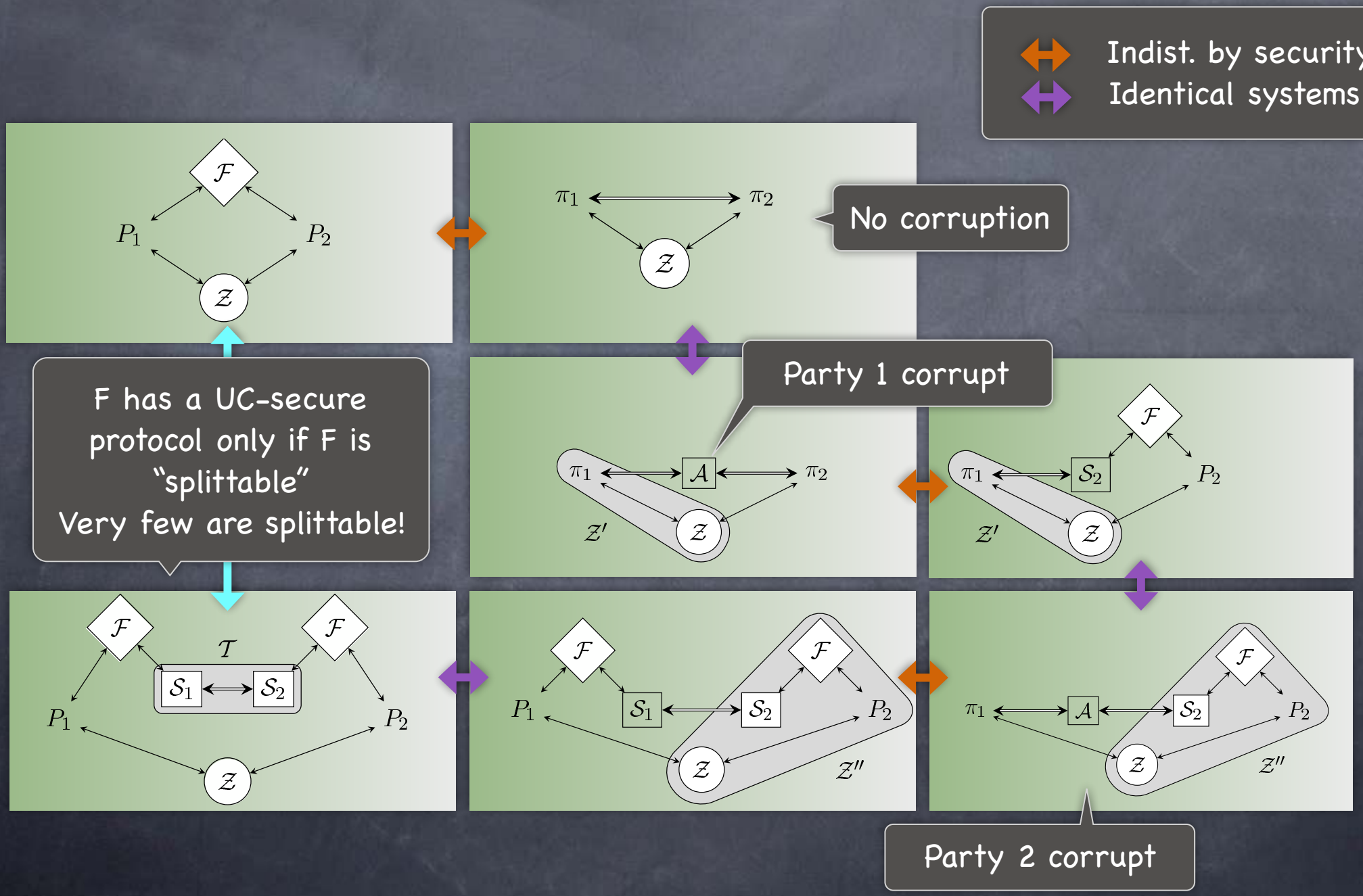
- Hence REAL ≈ IDEAL
- Main idea: Environment can model other sessions (real or ideal)



UC Secure MPC?

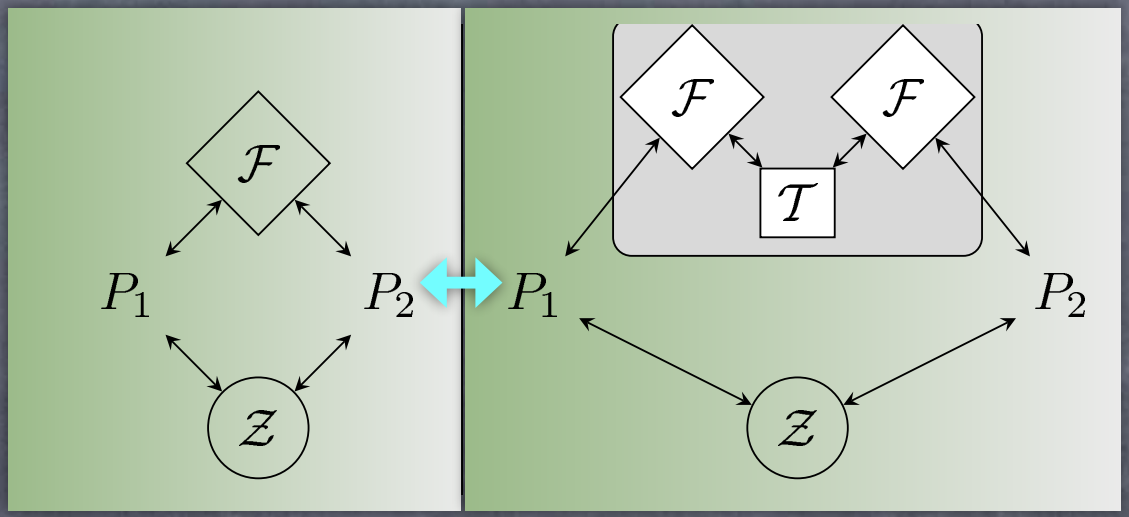
- UC-security is a strong security definition, and also enjoys the UC property
- But impossible to have "non-trivial" SIM-secure MPC!
- Universal Composition possible when:
  - Passive corruption, or
  - Honest majority, or
  - Given trusted setups (e.g., OT), or
  - Using alternate security definitions
    (e.g., "Angel-aided simulation": still meaningful and UC)

Impossibility of UC Security



Splittable Functionalities

- F splittable if ∃T ∀Z the outputs of Z in the following two experiments are negligibly far from each other:



- Splittable functionality essentially involve only communication and local computation. All splittable functionalities have UC-secure protocols.

- Most interesting functionalities are unsplittable. E.g., coin-tossing, commitment, XOR, OT, ...