New Notions of Security:
Universal Composability without Trusted Setup

Manoj Prabhakaran & Amit Sahai
Princeton University

To appear in STOC'04

Defining Security

- Central Problem in Cryptography
- Understanding what we want
- and what we can get

Evolution of Security Notions

Early 80's

Fundamental Ideas
(Basic tasks. Stand-alone situations.)

Complex tasks

Adaptive Adversaries

Sequential/Parallel/ Concurrent Composition

Malleability

The "Grand Unification"

Early 00's

Environmental Security

[C,PW]

- Comprehensive Security of a general task...
- ... in a general environment
- Essential to be applicable in a networked/multi-tasking setting
- "Universally Composable": can achieve complex tasks in a modular way

However...

- Too strong?
- Sweeping impossibility results
- No commitment/ZK/Multi-Party Computation protocol is Environmentally Secure [C,CF,CKL,L]
- Things possible: encryption, honest-majority MPC, or using a trusted setup (CRS- common reference string) [CF,CLOS,...]
- No notion of provable security for any protocol in the "plain model" in the presence of an environment!

New Notions of Security: An Overview

Environmental Security [C]

Composable
Not realizable

Generalized Environmental Security

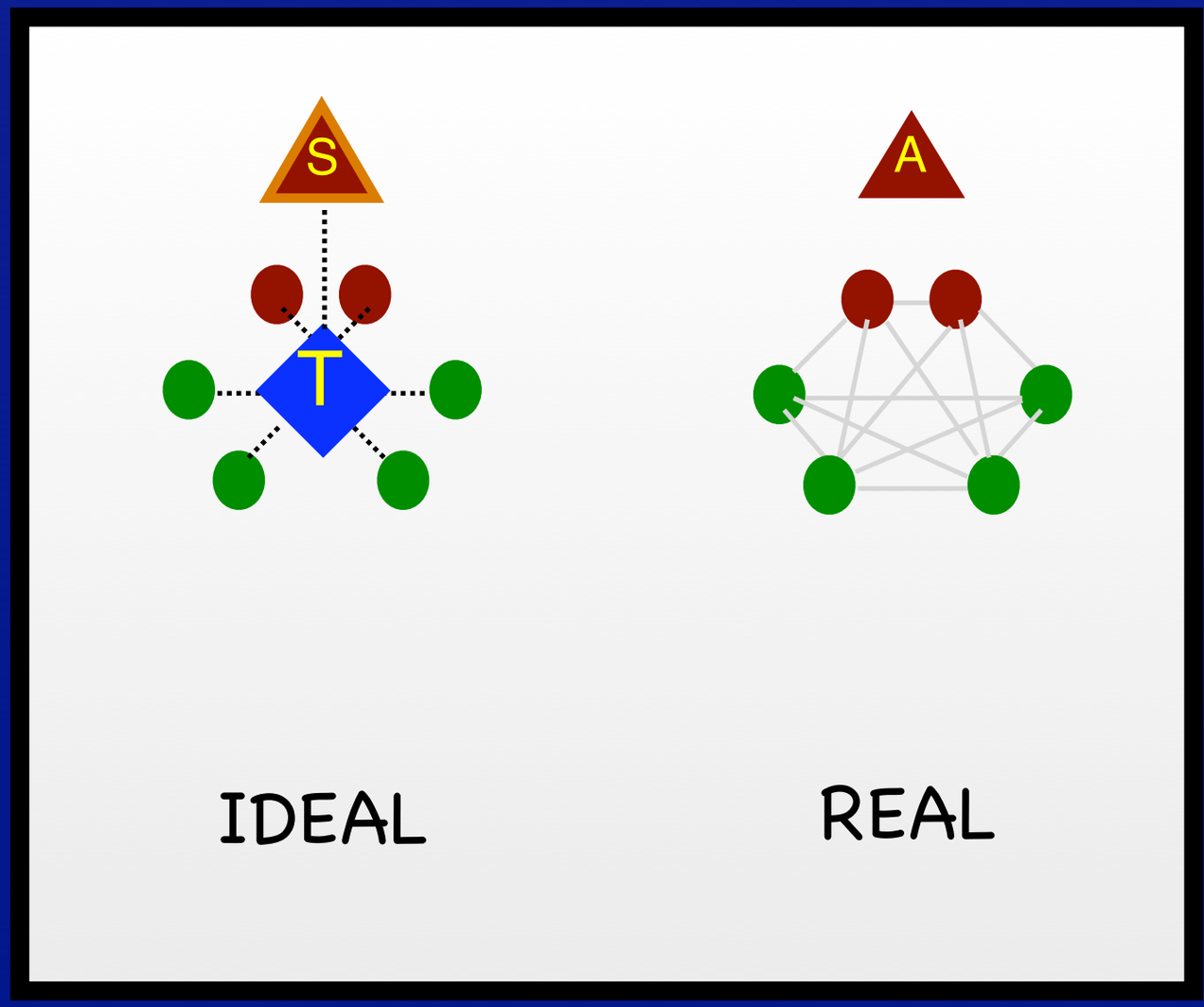
Composable
Realizable

Relaxed Environmental Security

Realizable
Not composable

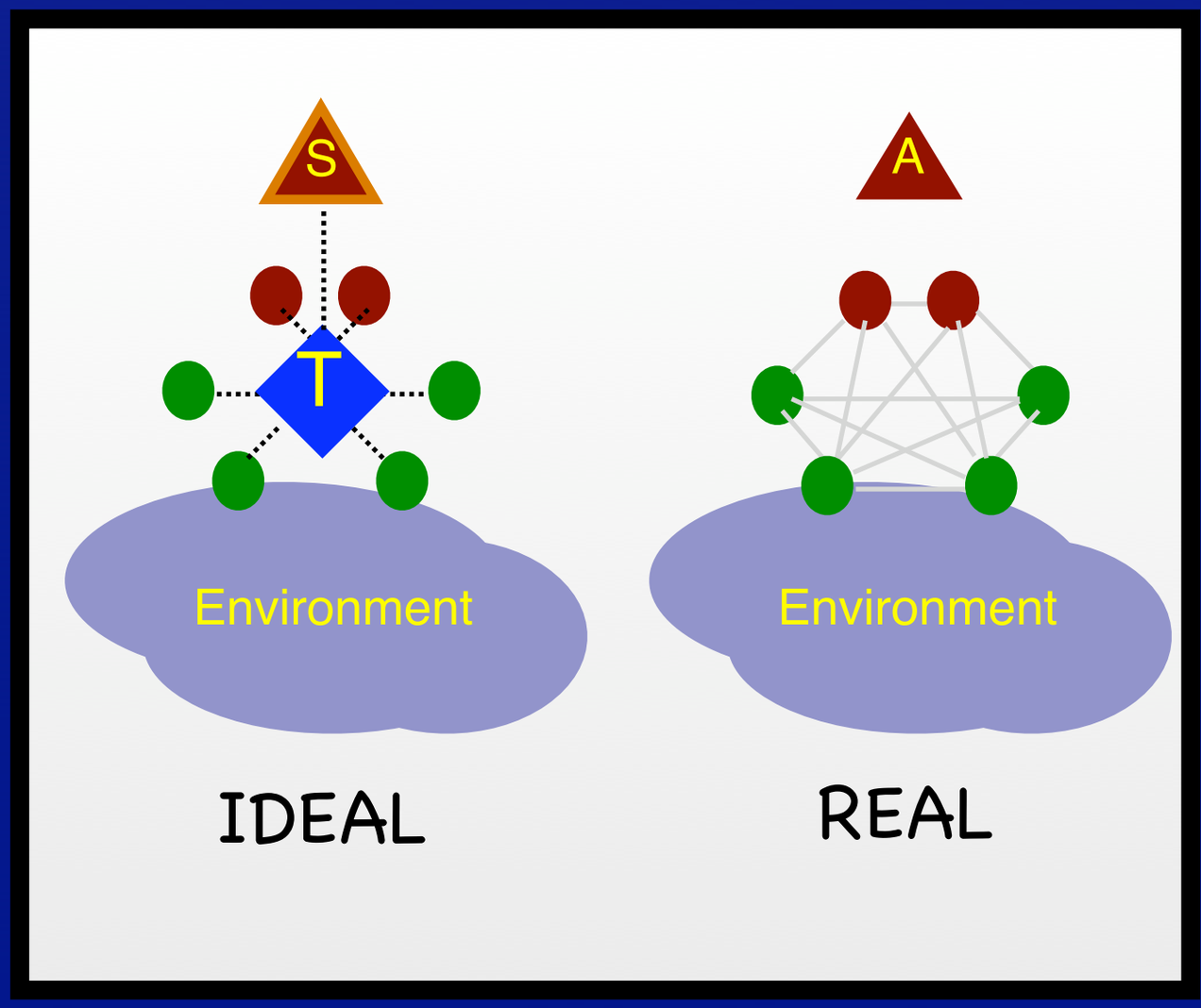
Security as Achieving the IDEAL

- Envision the IDEAL security notion- using trusted parties and secure channels to them
- A protocol in the REAL world is secure if whatever can happen in the REAL world could have happened in the IDEAL world

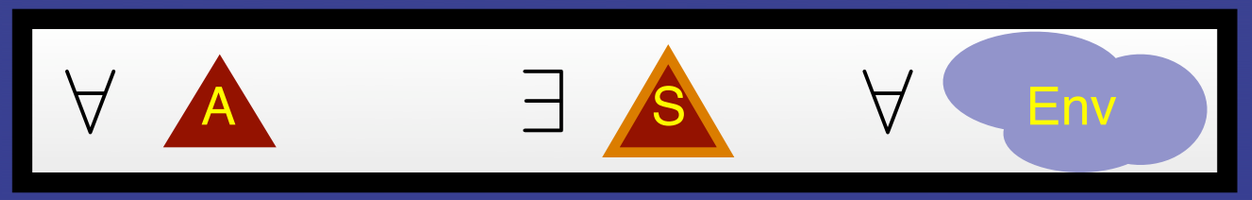


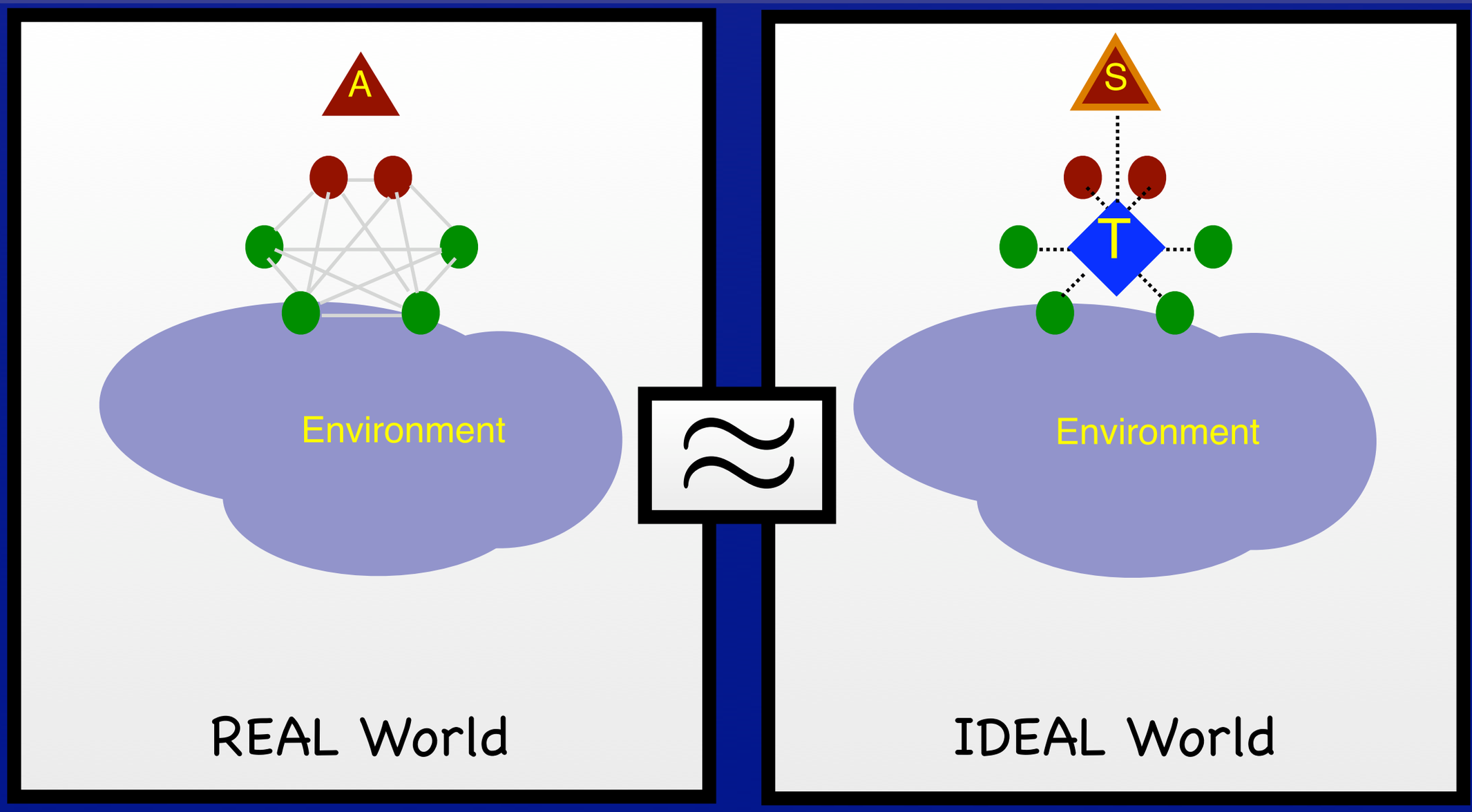
Environmental Security

- Interactive Environment present
- Environment cannot distinguish between being in REAL execution and being in IDEAL execution



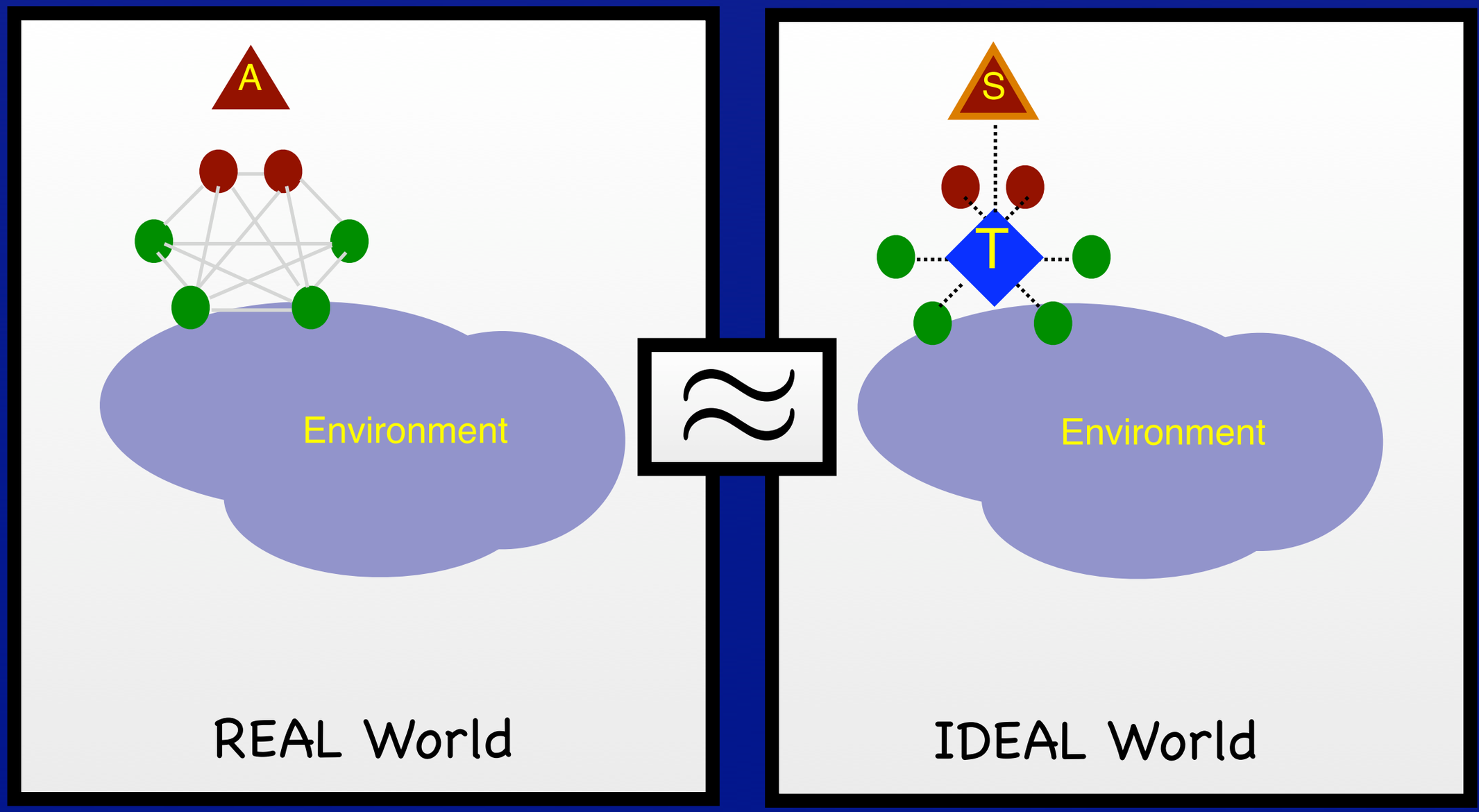
Environmental Security





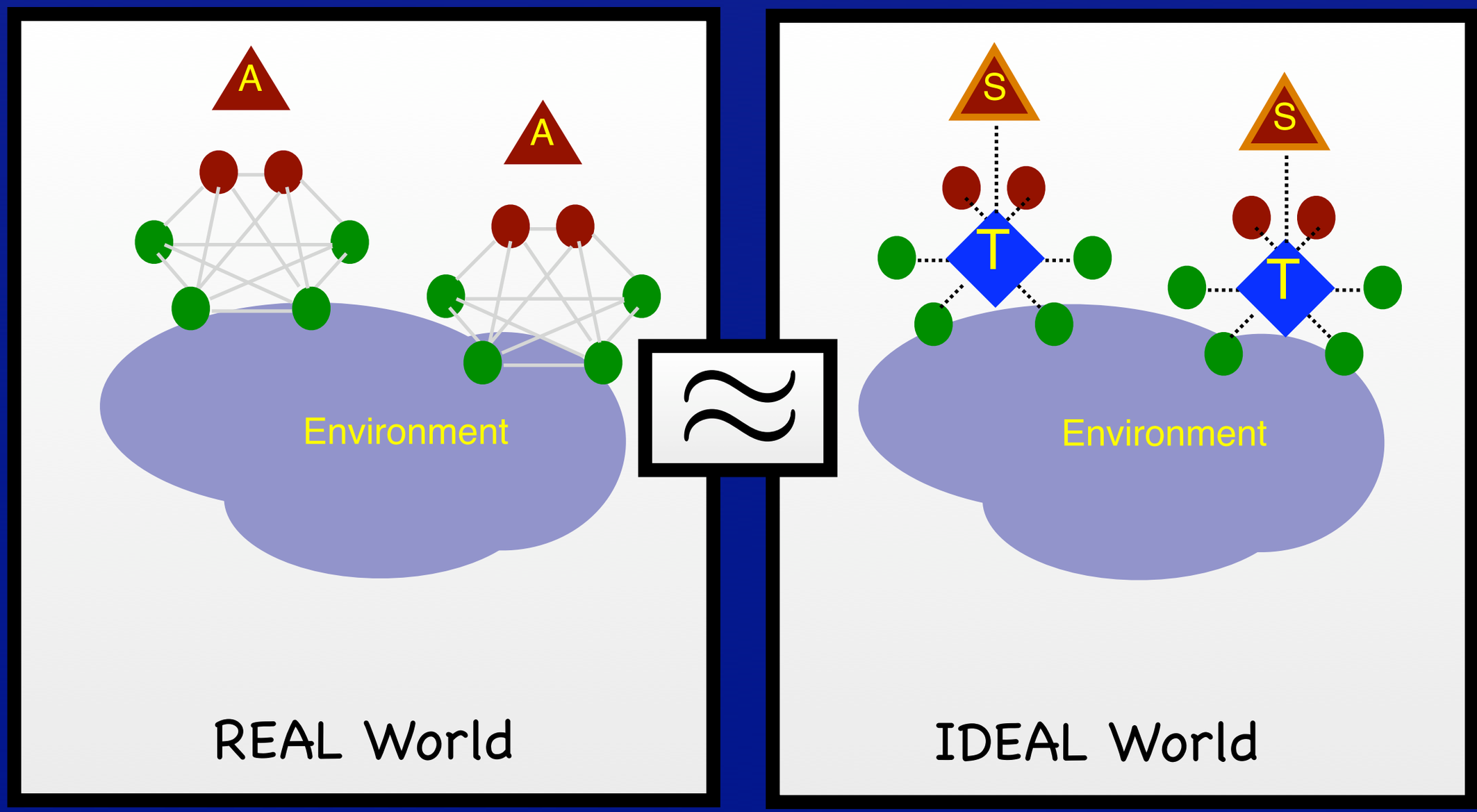
Universal Composability Theorem [C]

If



Universal Composability Theorem [C]

Then



Environmental Security Not Realizable

- Very general impossibility results [C,CF,L,CKL...]
- No commitment, ZK, multi-party computation
- Impossibility holds whenever environment can internally run the IDEAL adversary

- Same condition for Universal Composition to hold!

New Notions of Security: An Overview

Environmental Security [C]

Composable
Not realizable

Generalized Environmental Security

Composable
Realizable

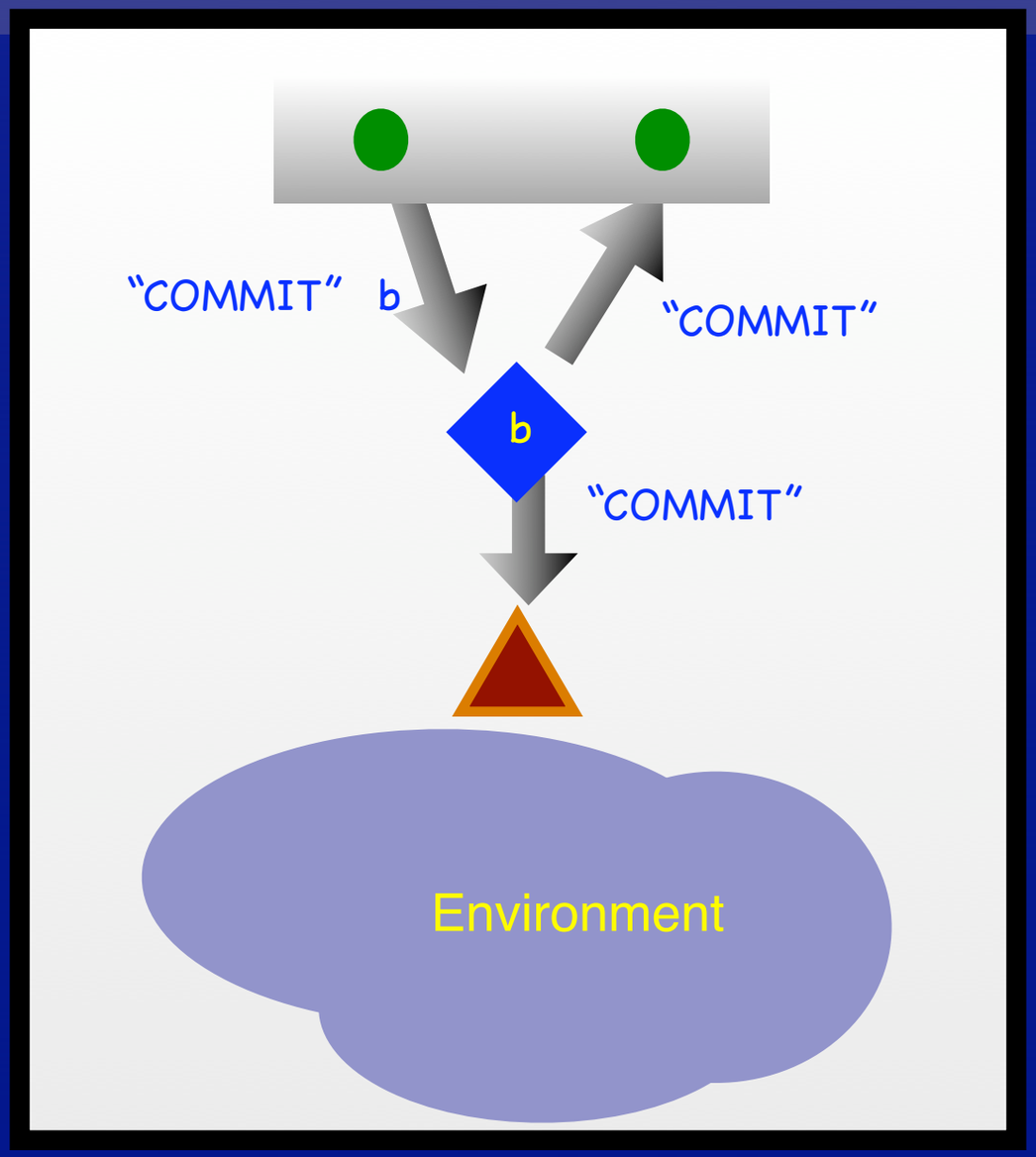
Relaxed Environmental Security

Realizable
Not composable

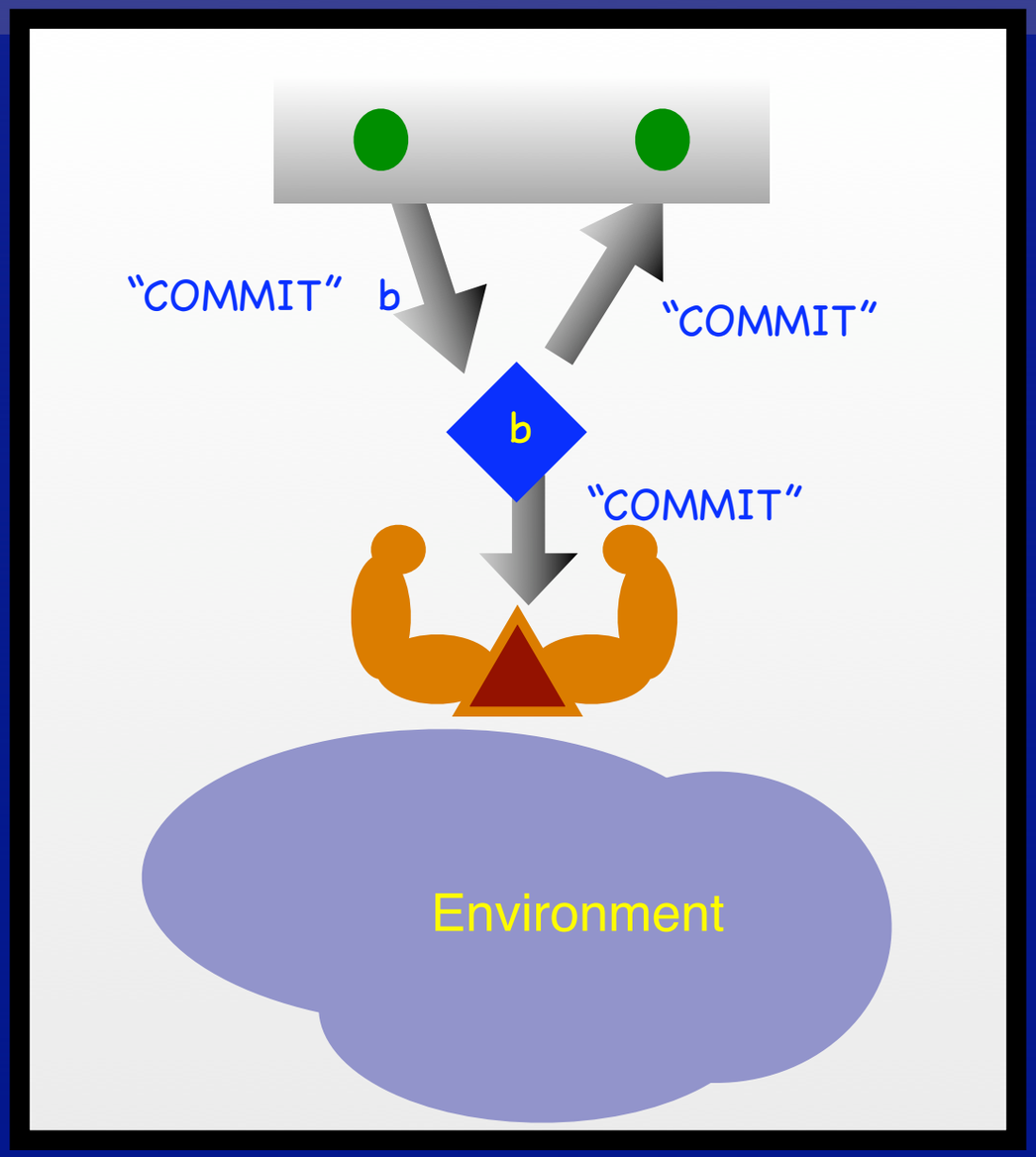
Coming Up...

ES Reloaded

Commitment IDEAL



Commitment IDEAL

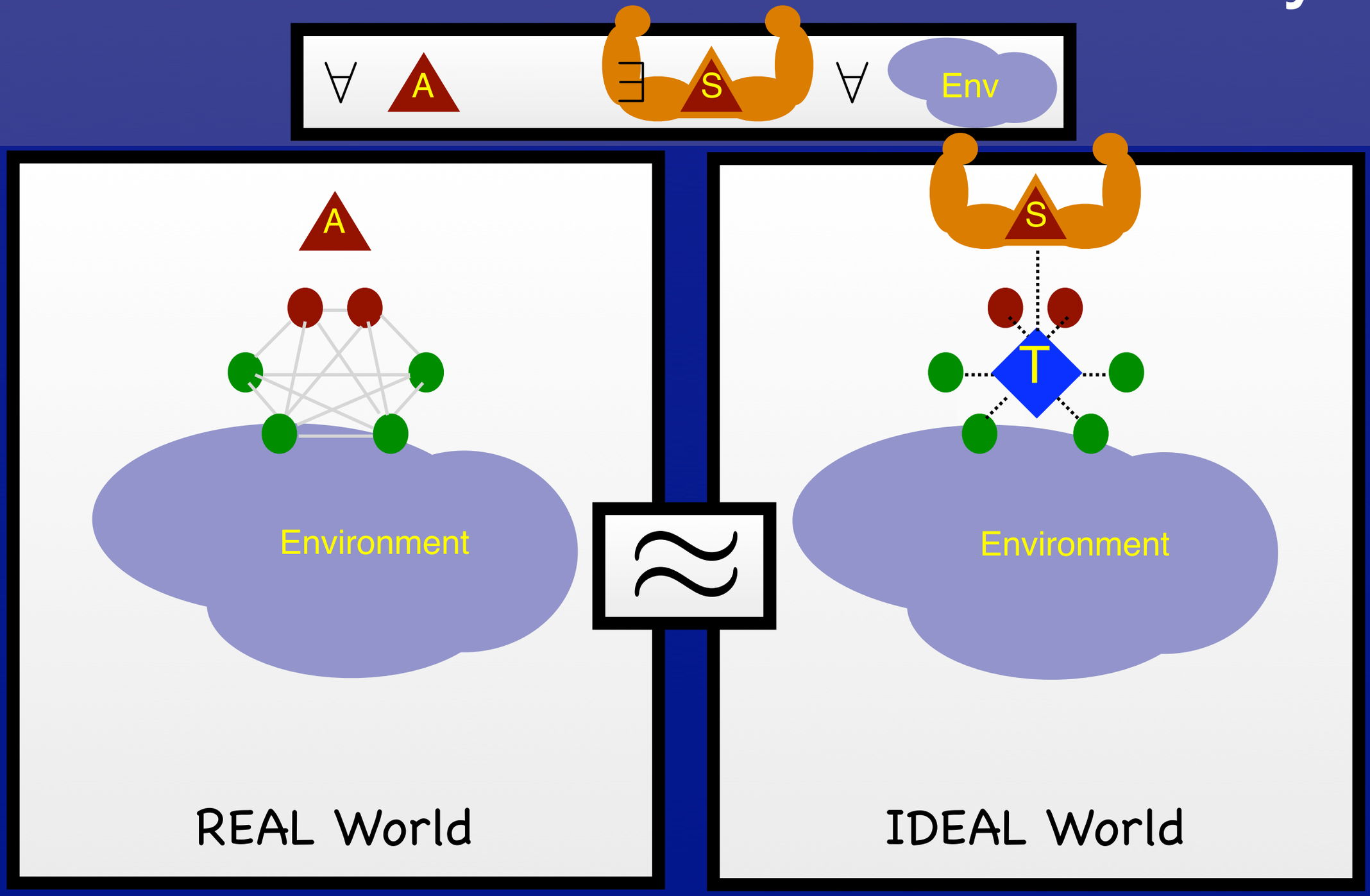


Still ideal!

Relaxed Environmental Security

- In the IDEAL world, adversary has exponential computational power
- Still IDEAL: no extra information to compute with

Relaxed Environmental Security



Relaxed ES

- Suffices in most cases of interest- when notion of security is information theoretic
- IDEAL not satisfactory for some situations (e.g. playing an online game)
  - Fixed in Generalized Environmental Security
- Easily implies traditional strong notions of security (concurrent, non-malleable, CCA2 secure) for many tasks (commitment, encryption, WI proofs,...)
- Similar ideas previously for simpler situations

Relaxed Environmental Security

Not Composable!

Too Relaxed?

New Notions of Security: An Overview

Environmental Security [C]

Composable
Not realizable

Generalized Environmental Security

Composable
Realizable

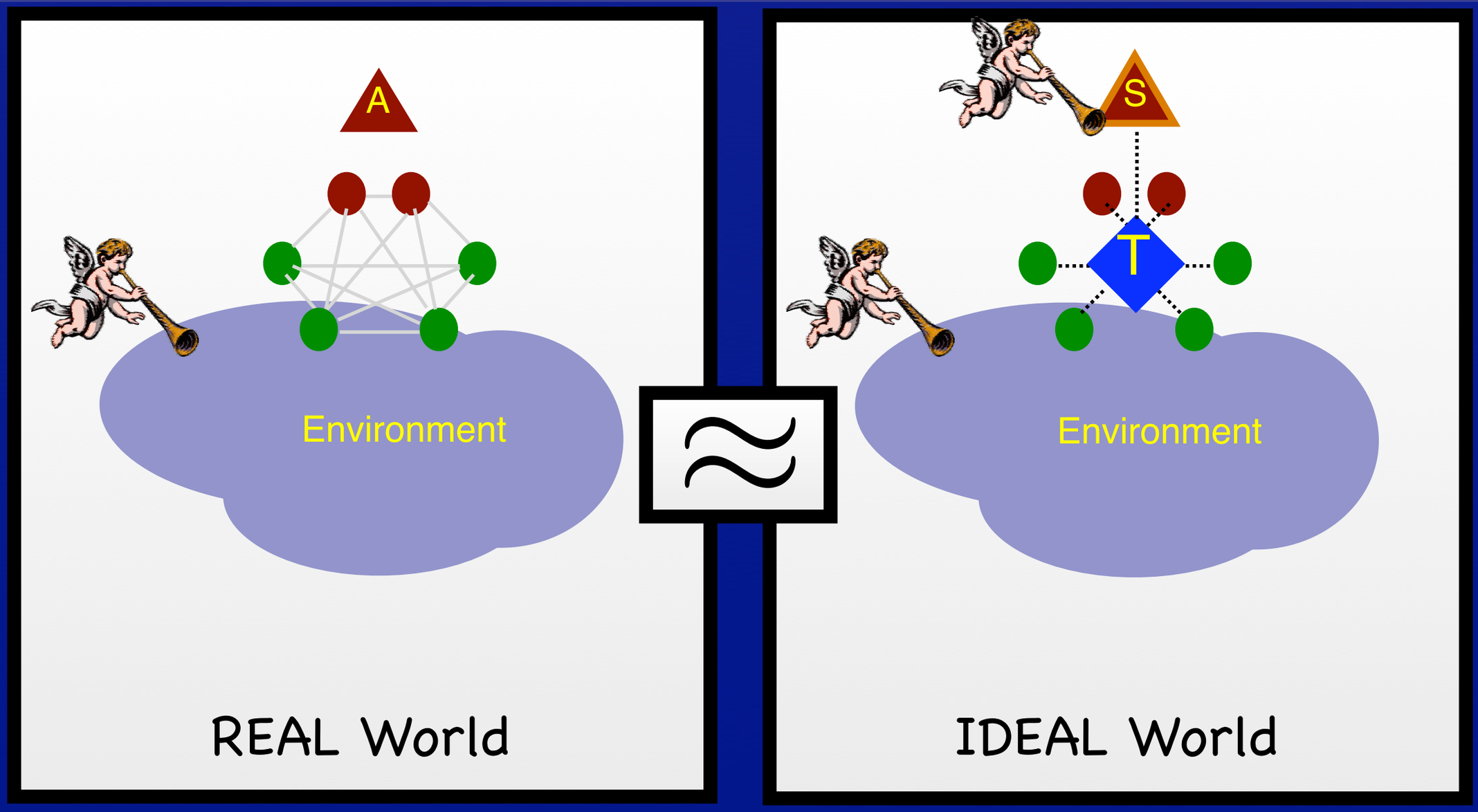
Relaxed Environmental Security

Realizable
Not composable

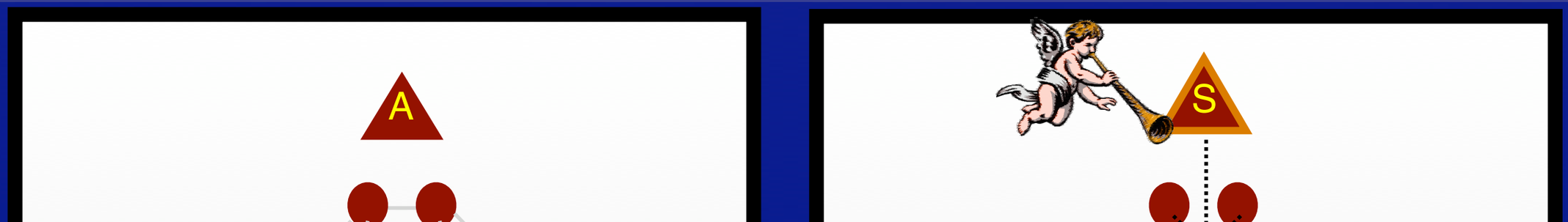
Generalized Environmental Security

- Implies Relaxed Environmental Security
- IDEAL adversary and Environment have access to "The Angel"
- The Angel is exponential-time Oracle with a simple filter to decide whether to answer or not
- Filter depends on the set of corrupted parties
- Gives restricted access to exponential computational power: helps break corrupted parties' security, but not honest parties'

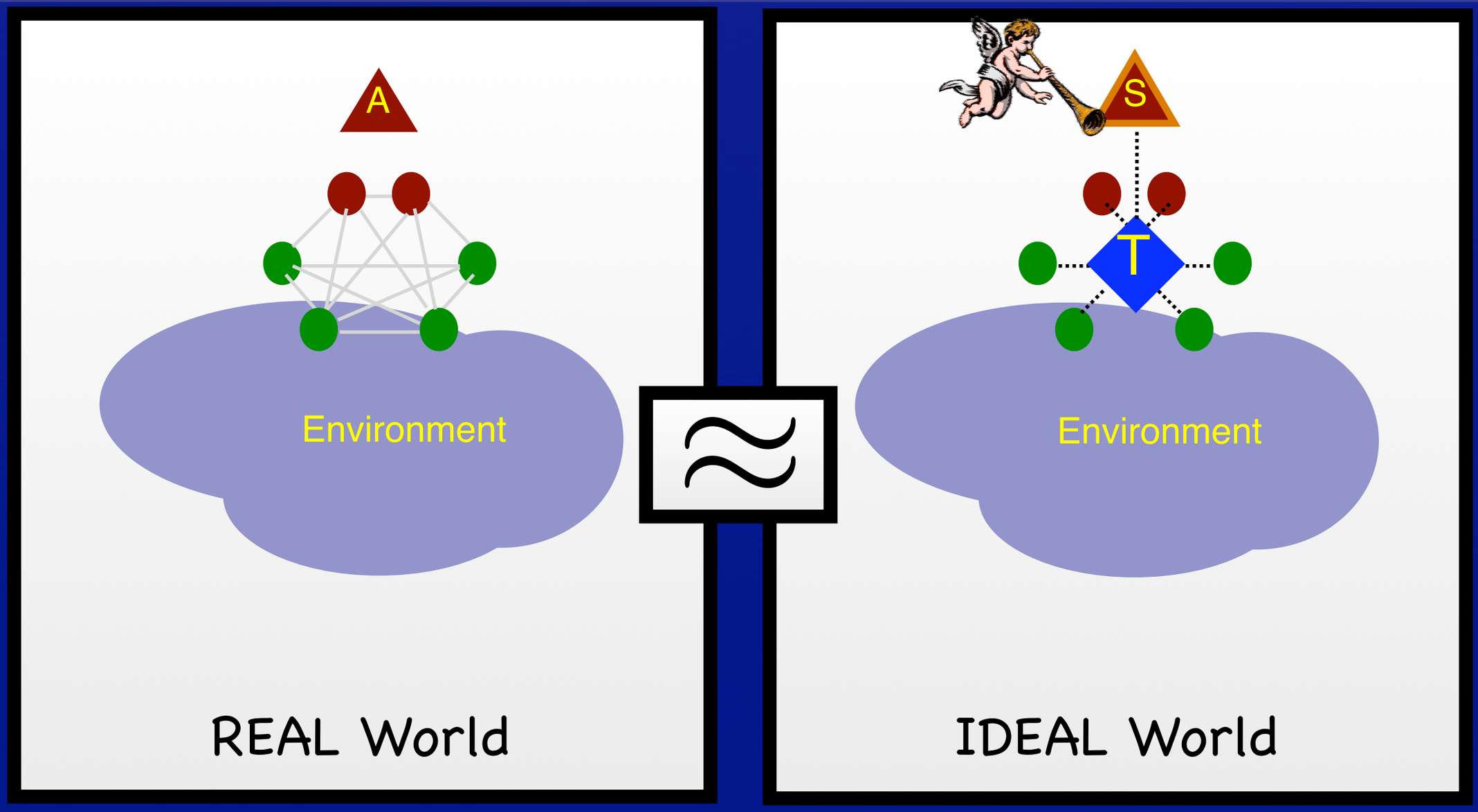
Generalized ES



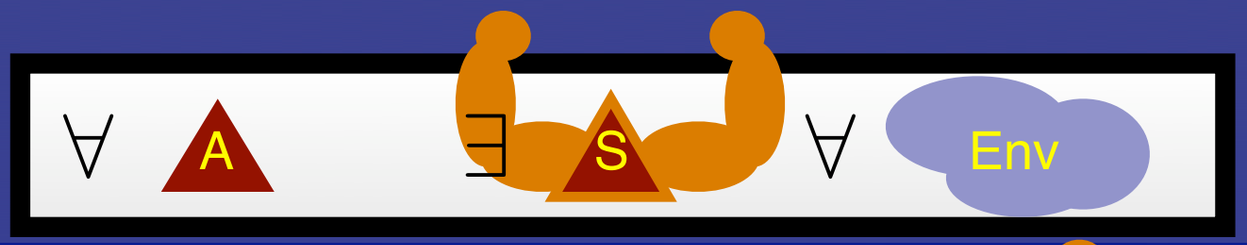
Generalized ES ⇒ Relaxed ES

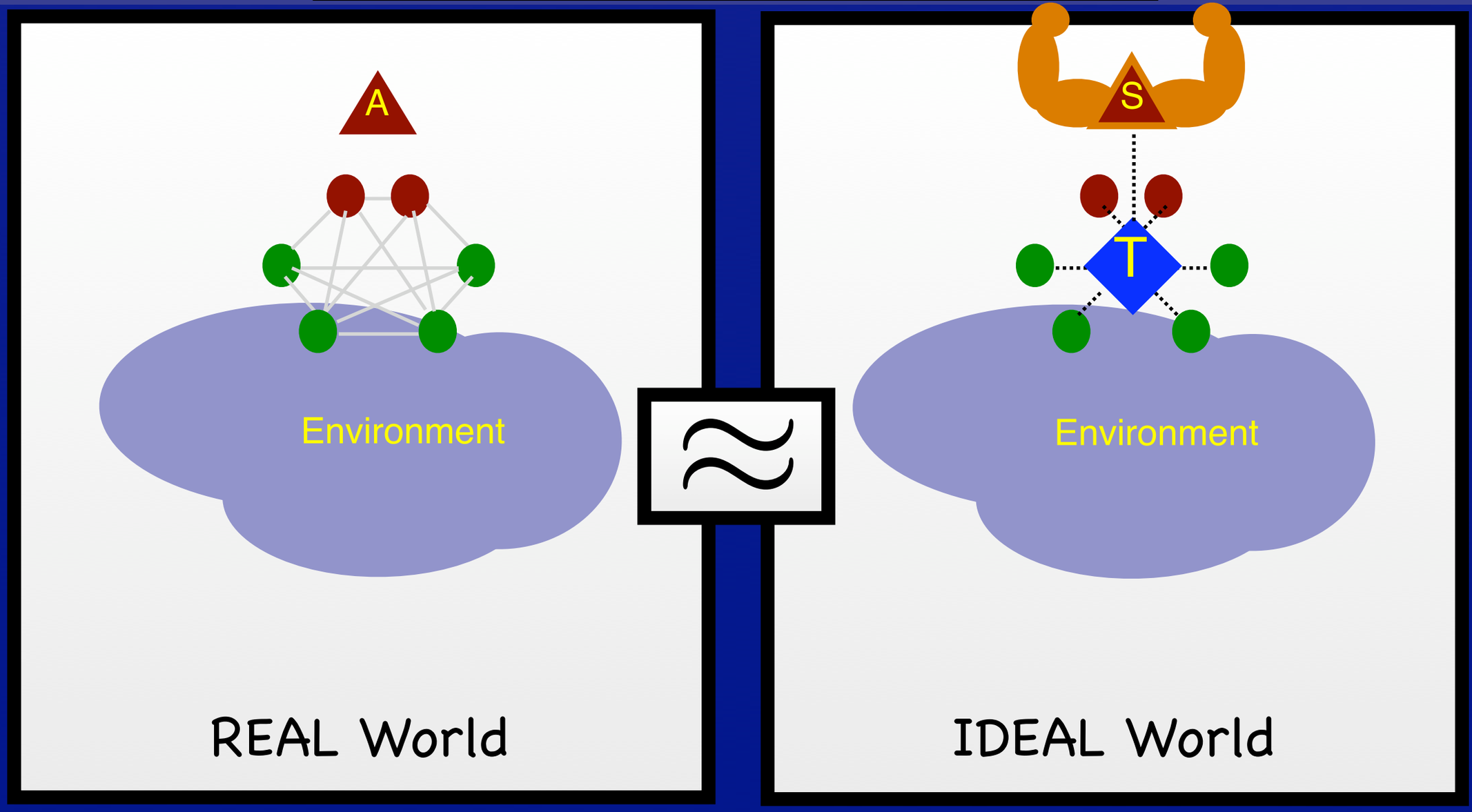


Generalized ES ⇒ Relaxed ES



Generalized ES ⇒ Relaxed ES





What is this Angel?

- Our Angel gives collisions in a hash function
- Alternative models possible with different Angels
- i.e., can instantiate the generalized ES framework with different Angels
- Using "null-Angel" gives the original ES model of [C]

Generalized ES results

- For any exponential-time Angel X,
  gES(X) ⇒ relaxed ES

- For any Angel X, gES(X) protocols are Universally Composable

- There is an Angel X* such that there are gES(X*) protocols for commitment, ZK, and for realizing any efficient trusted party

Realizing a General Trusted Party

New!

Commitment Semi-Functionality

ZK Proof Semi-Functionality

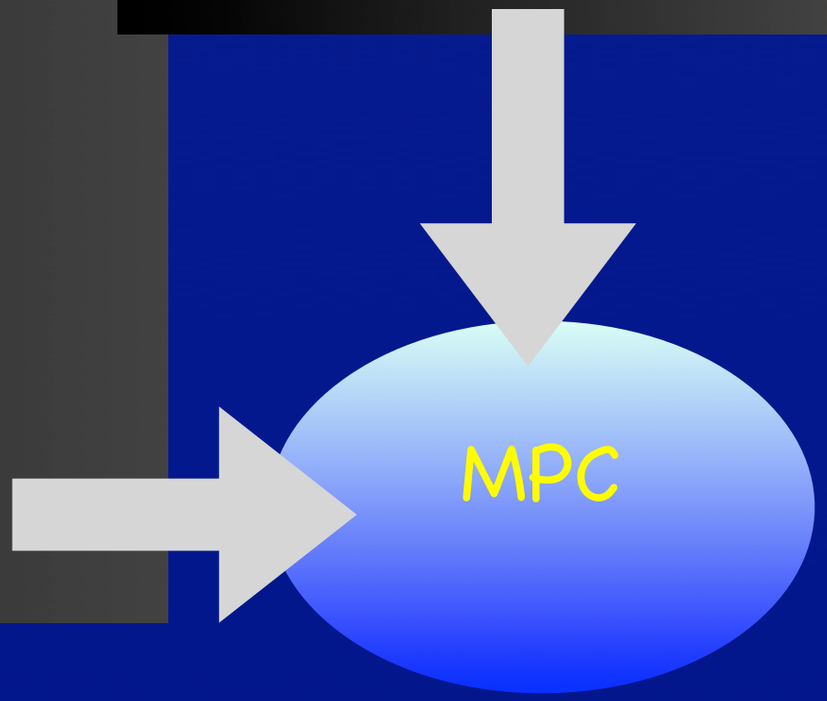
Commitment

ZK Proof

Commit & Prove
(one-many)

Protocol Compiler
(semi-honest to malicious)

Semi-Honest MPC

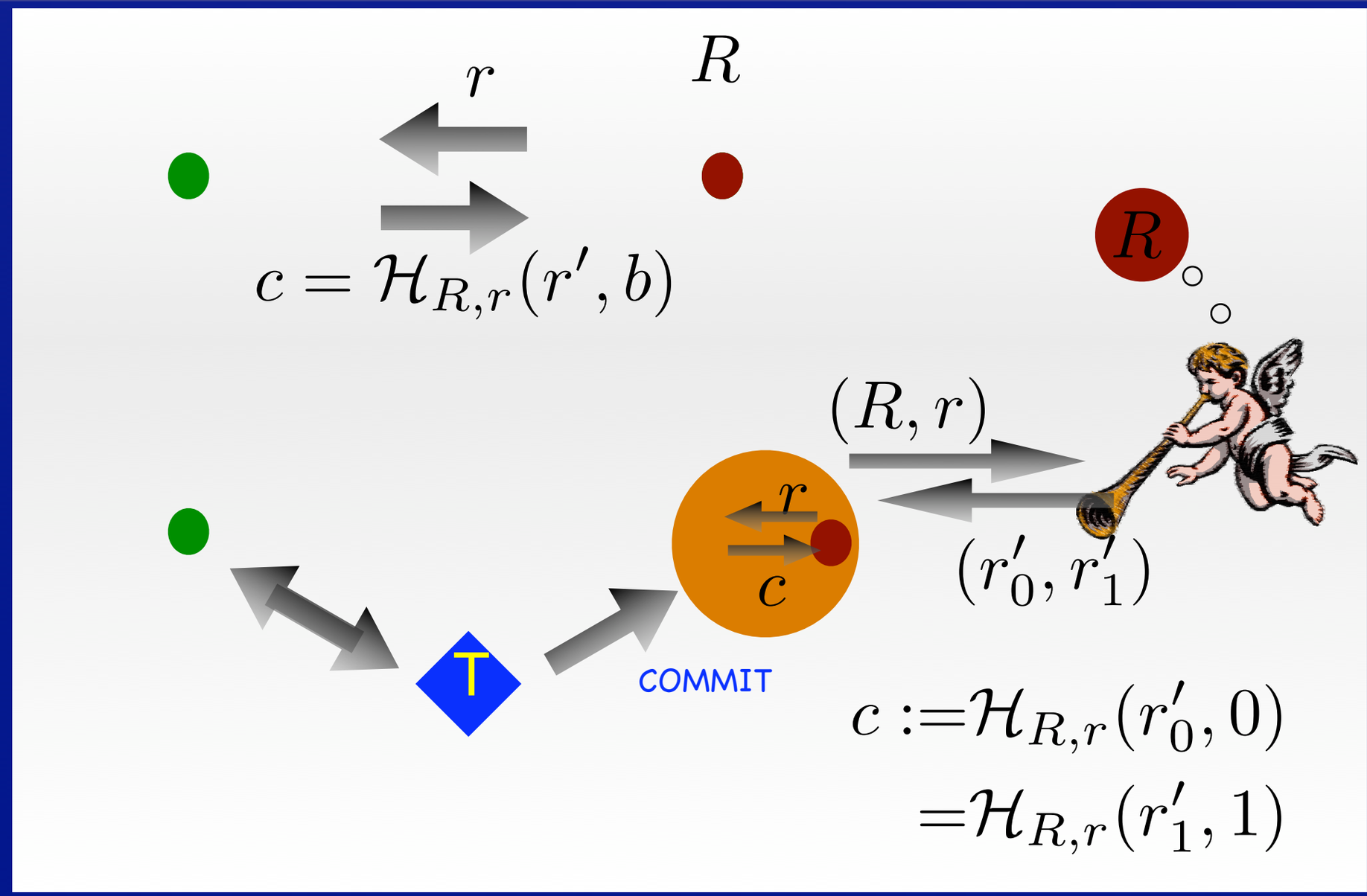


Currently, all results for Static Adversaries

“The Angel” in Action

Protocol

IDEAL

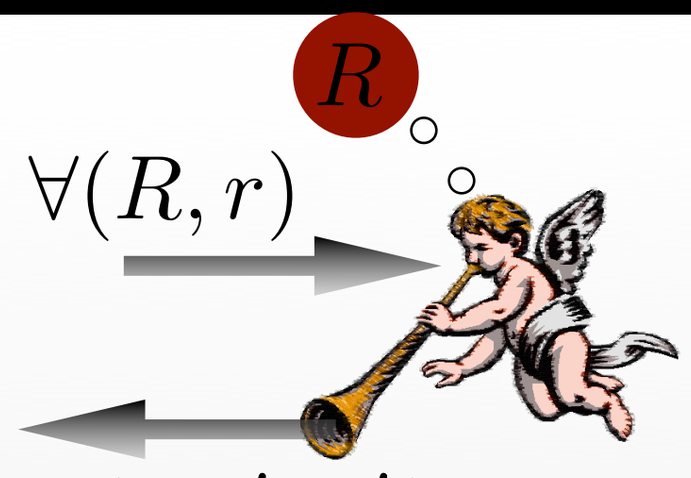


Assumptions

r'

$$(\mathcal{H}_{R,r}(r',0),r') \approx (c,r'_0)$$

$$(\mathcal{H}_{R,r}(r',1),r') \approx (c,r'_1)$$



$$(c,r'_0,r'_1)$$

$c := \mathcal{H}_{R,r}(r'_0,0)$
$= \mathcal{H}_{R,r}(r'_1,1)$

R

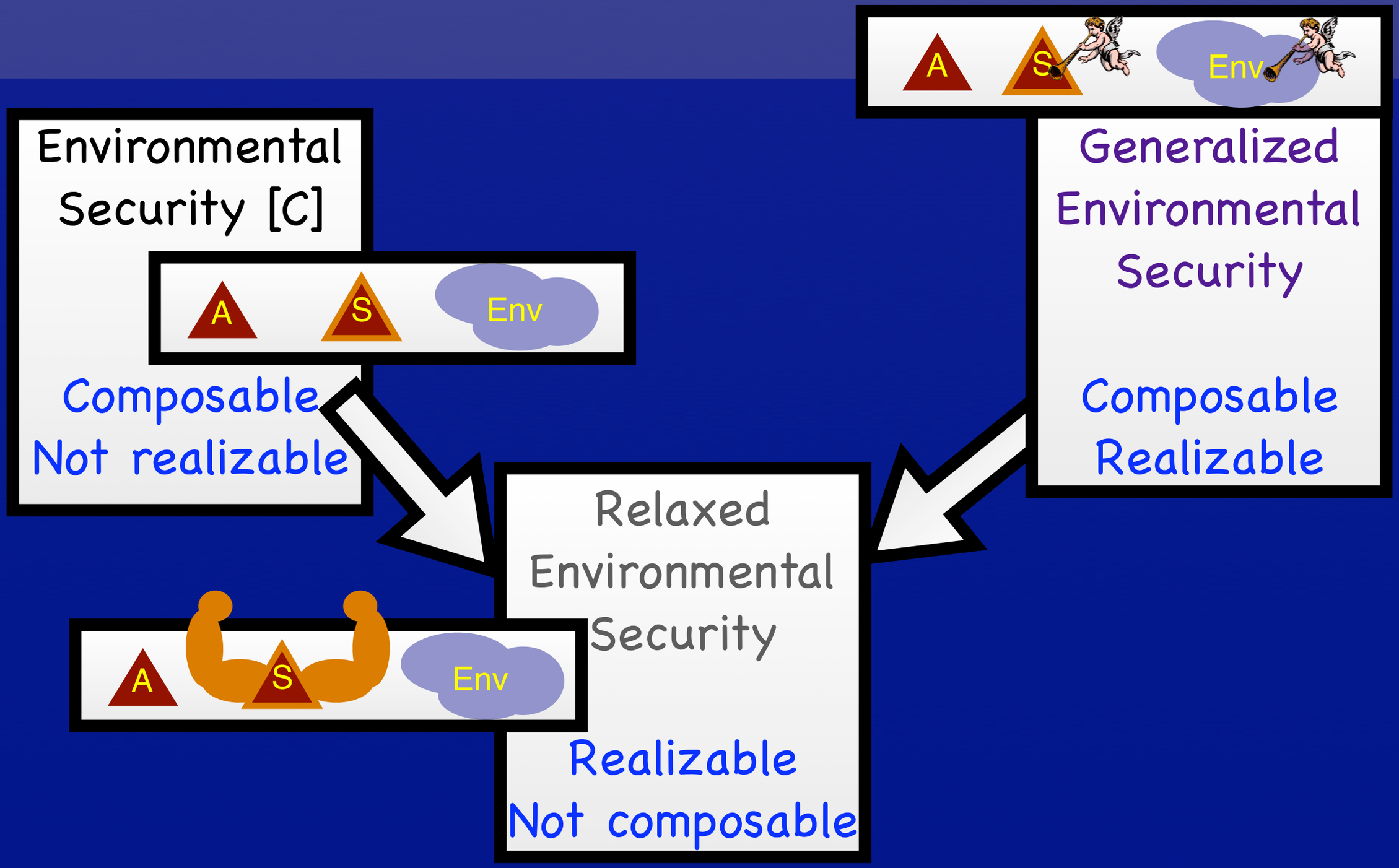
r

(r'_0,r'_1)

$$\mathcal{H}_{R,r}(r'_0,0) \neq \mathcal{H}_{R,r}(r'_1,1)$$

Trapdoor Permutation

Recap


A
S
Env
Environmental Security [C]
Composable
Not realizable
A
S
Env
Generalized Environmental Security
Composable
Realizable
Relaxed Environmental Security
A
S
Env
Realizable
Not composable

More work needed

- Investigate/simplify the assumptions
- Extend to Adaptive Adversaries
- Get simpler/more efficient protocols
- Even more realistic Environmental Security model

Thank You!