Trusted Parties and Their Twins

Manoj Prabhakaran & Mike Rosulek

Splittability!
(The Disney Version)

Haley Mills was indistinguishable from two coordinating copies of herself

Splittability! (The Disney Version)

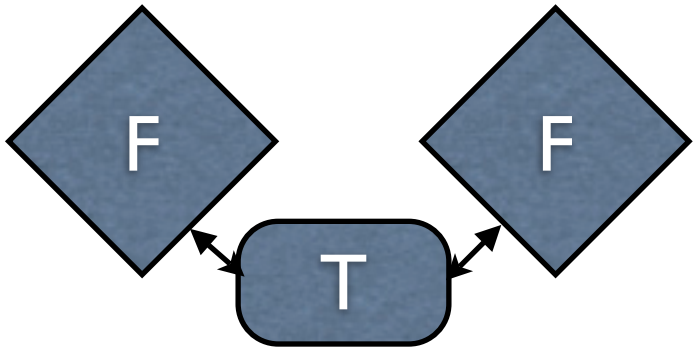
Haley Mills was indistinguishable from two coordinating copies of herself

Splittability! (The Disney Version)

Haley Mills was indistinguishable from two coordinating copies of herself

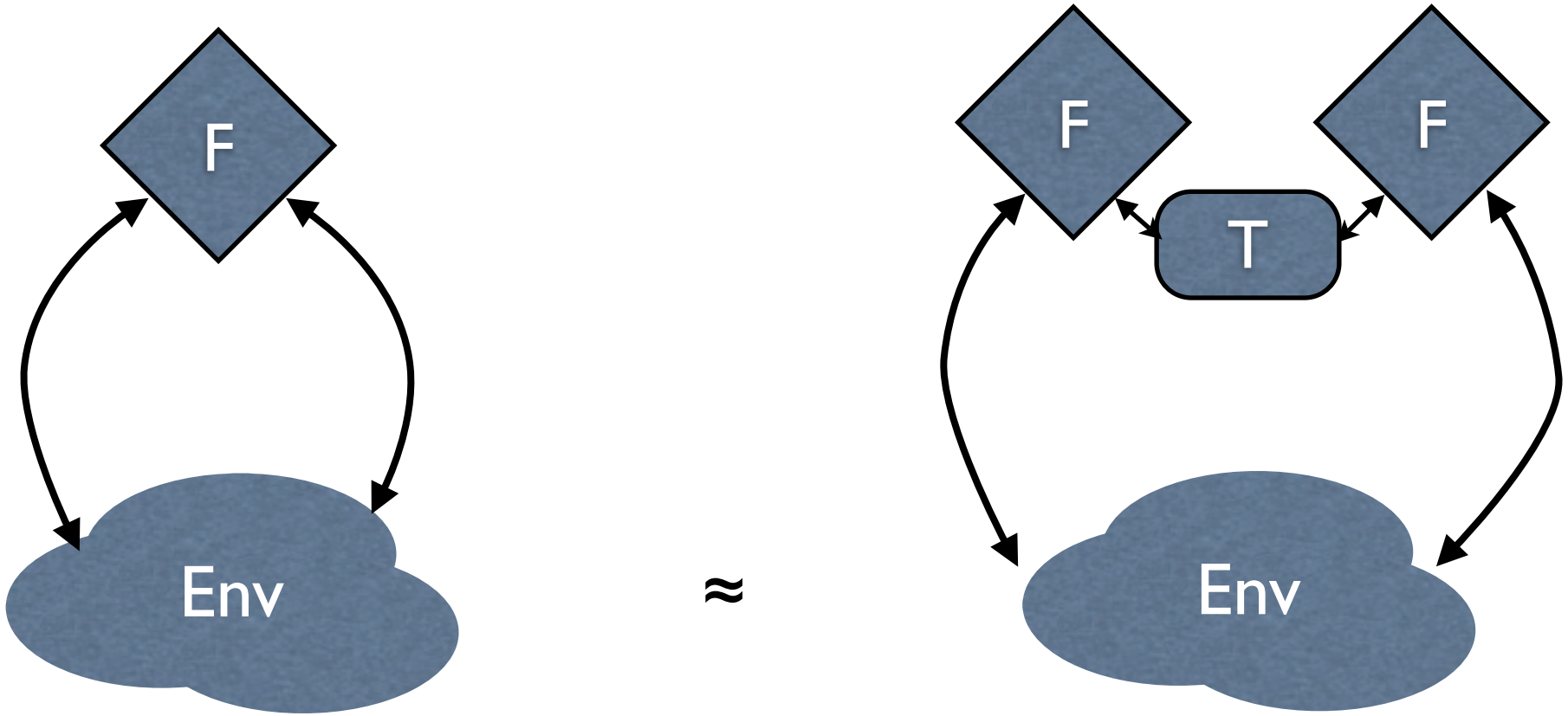
≈

Splittability!
(The Disney Version)

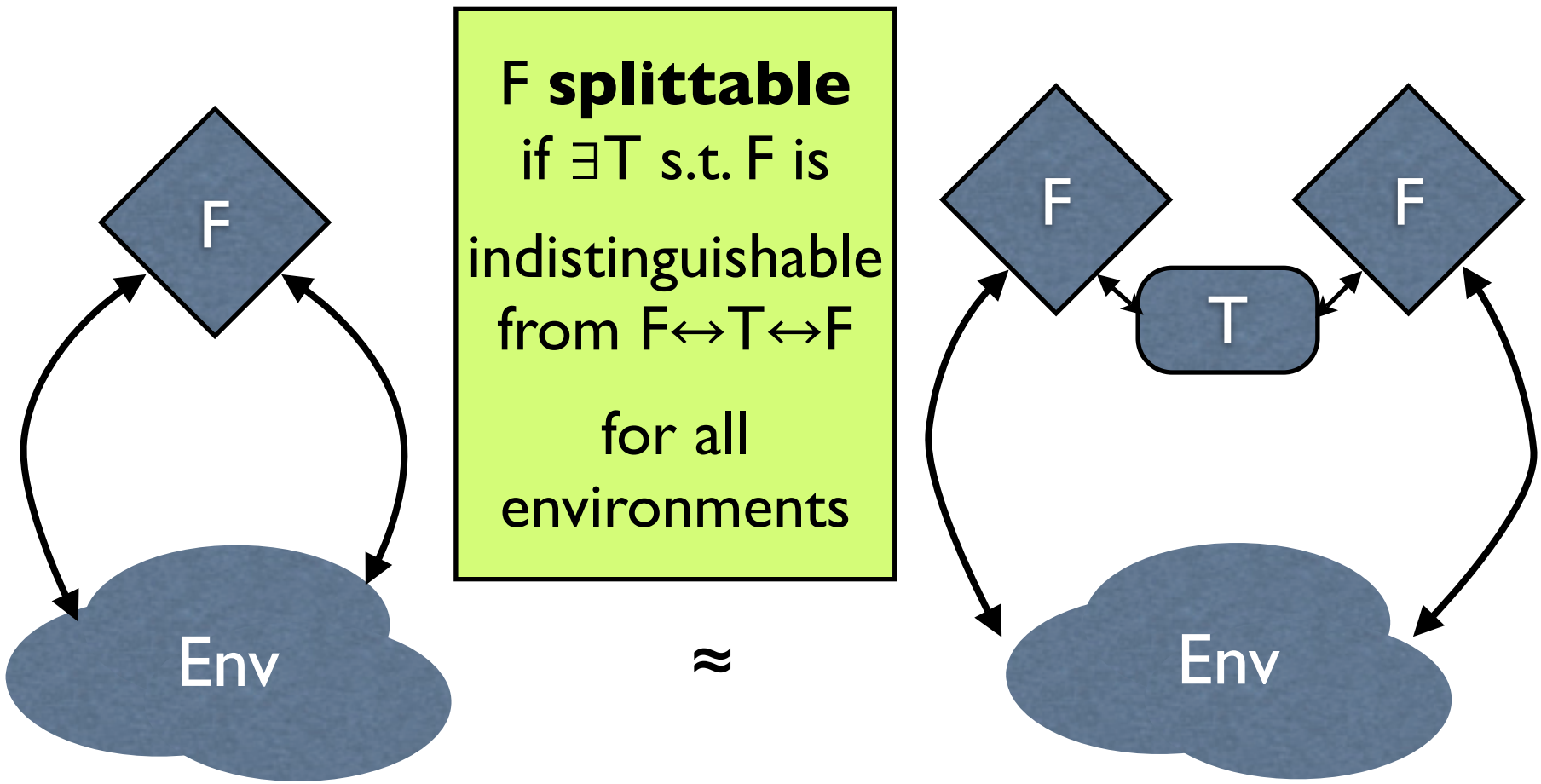


≈

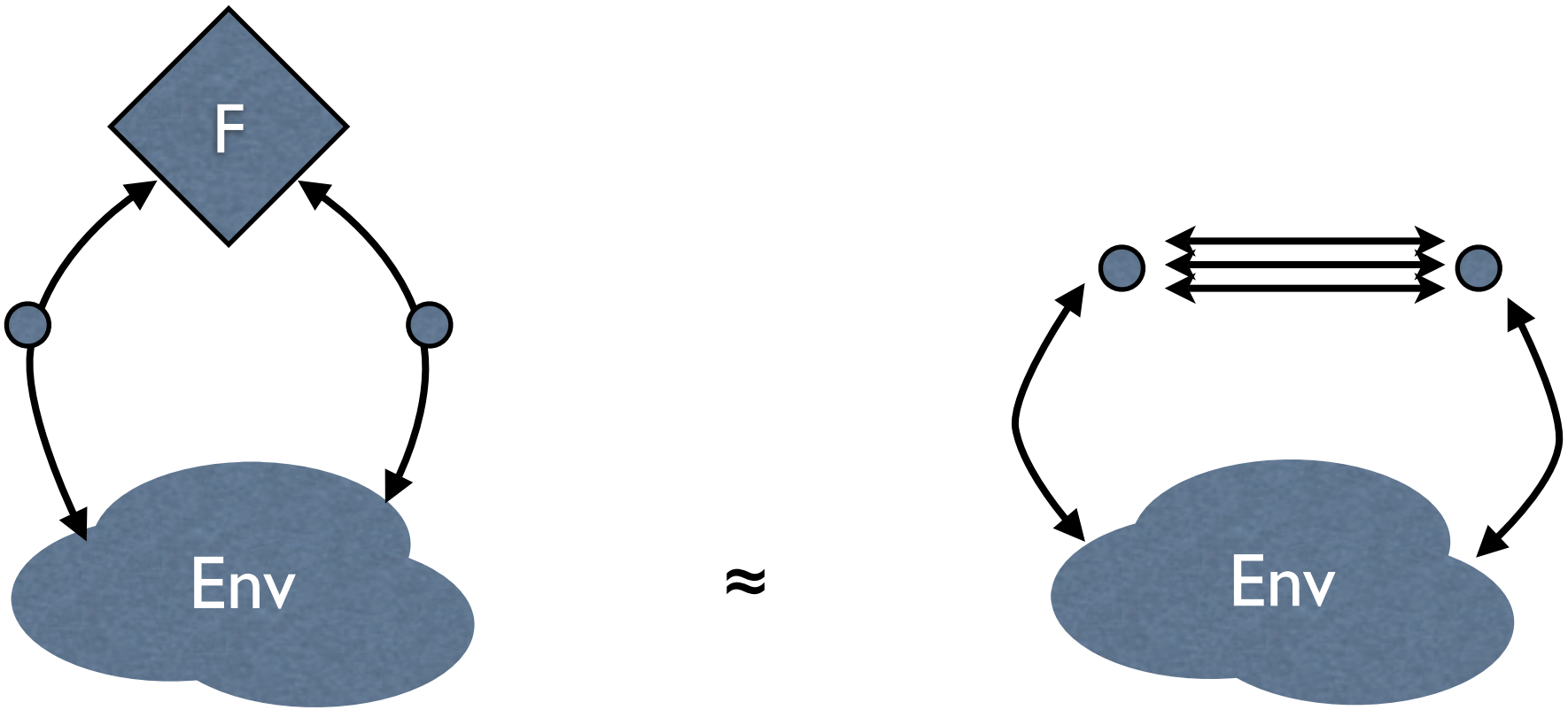
Splittability!



Splittability!



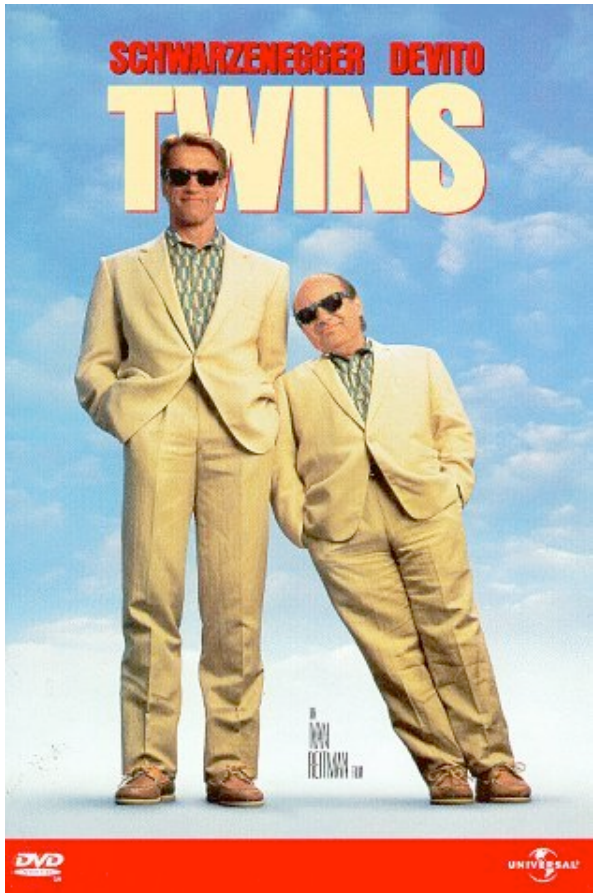
Theorem:
Splittable = Realizable



When is there no protocol possible?

When is there no protocol possible?

If there's no way to keep the trusted party synchronized with its twin



Using our characterization

- Easy to show impossibility of:
  - Commitment, simultaneous exchange, oblivious transfer, coin-flipping, ...
- Explicit and exact characterization for 2-party non-reactive functionalities
  - Subsumes impossibility of Canetti-Kushilevitz-Lindell'06
- Characterization holds also for m-party, reactive, randomized functionalities.
- Intriguing gaps/results for m-party (m>2) settings

Generalization: Splittability Partial Order

- Extends to a partial order F < G ("F splits w.r.t. G")
  - Gives results on realizability of F w.r.t G
  - Complete characterization when G is self-splittable (G<G) !
- Other cute things...

Hiding Functionalities

- Functionality version of one-way functions
  - e.g. oblivious transfer
- Can construct hardcore predicates for HFs
  - Then use to realize commitment, etc. (everything?)
  - Goldreich-Levin predicate for HFs!
  - Several open questions