

Analysis of a Fair Exchange Protocol

Vitaly Shmatikov John Mitchell
Stanford University

Agreement in Hostile Environment

- Cannot trust the communication channel
- Cannot trust the other party in the protocol
- Trusted third party may exist
 - Last resort: use only if something goes wrong

Contract Signing

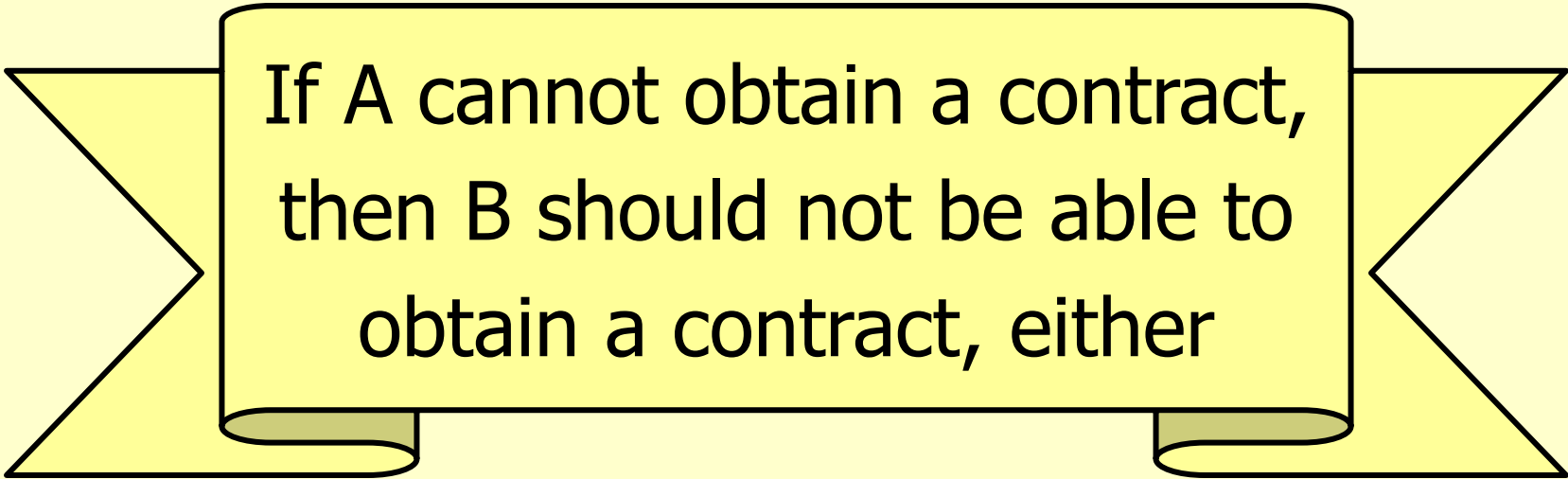


Immunity
deal



- Both parties want to sign the contract
- Neither wants to commit first

Fairness



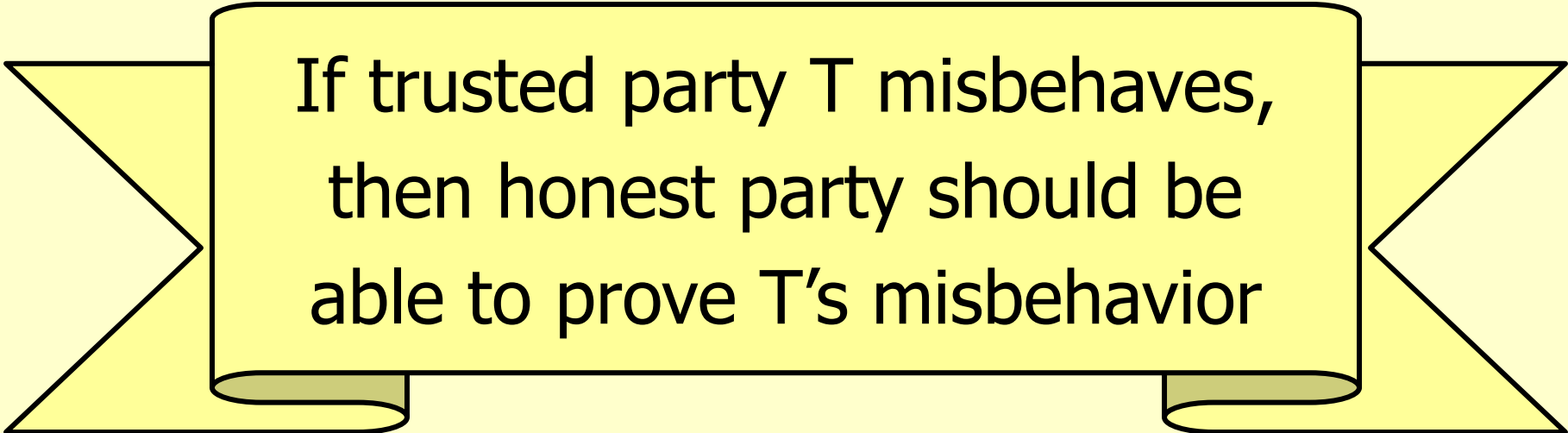
If A cannot obtain a contract,
then B should not be able to
obtain a contract, either

(and vice versa)

Example (Alice buys a house from Bob)

If Alice cannot obtain a deed for the property,
Bob should not be able to collect Alice's money

Accountability

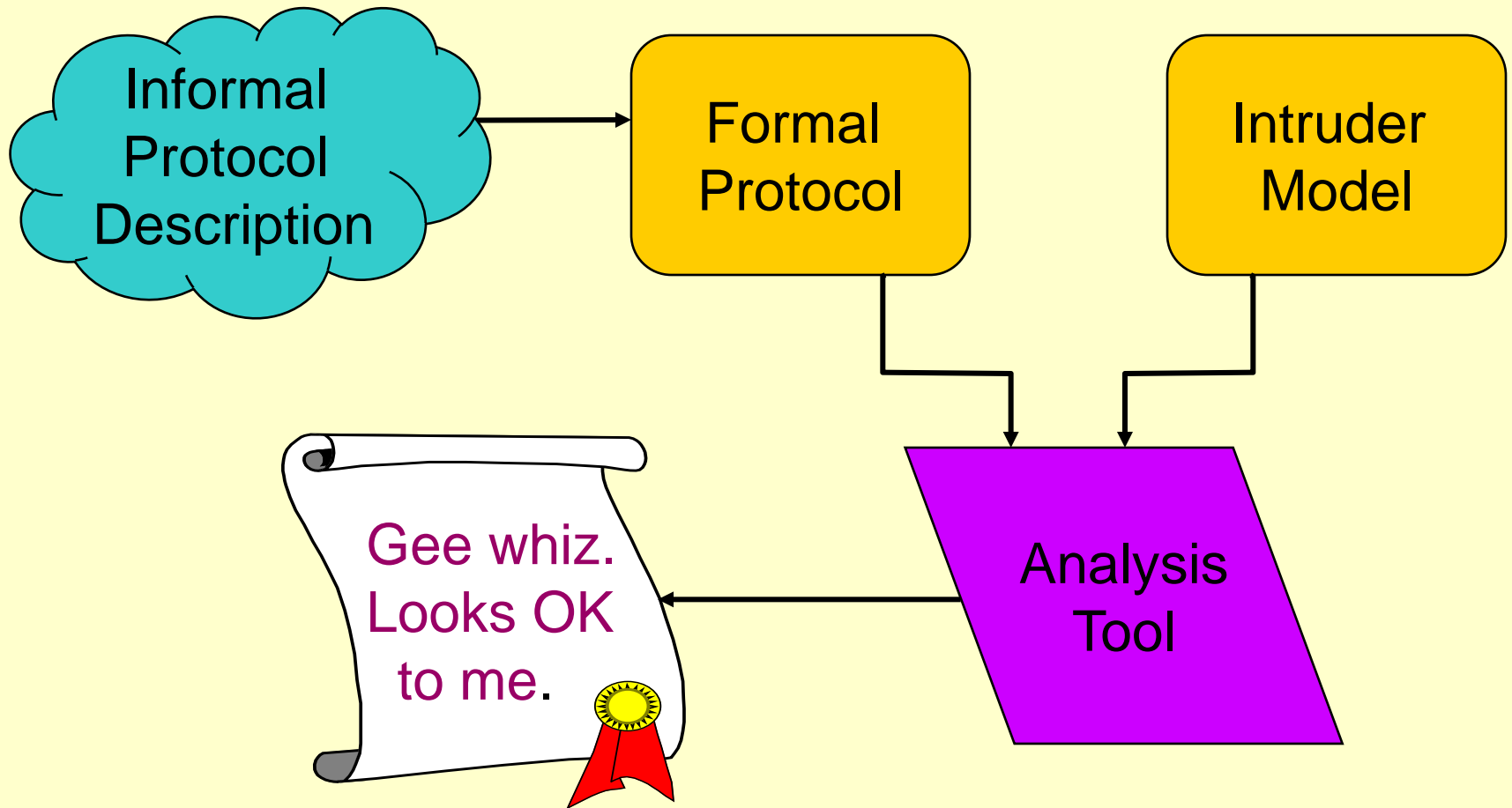


If trusted party T misbehaves,
then honest party should be
able to prove T's misbehavior

Example (Alice buys a house from Bob)

If escrow service gives Bob Alice's money without giving Alice the deed, Alice should be able to prove to a judge that escrow service is cheating

Formal Protocol Analysis



Mur ϕ

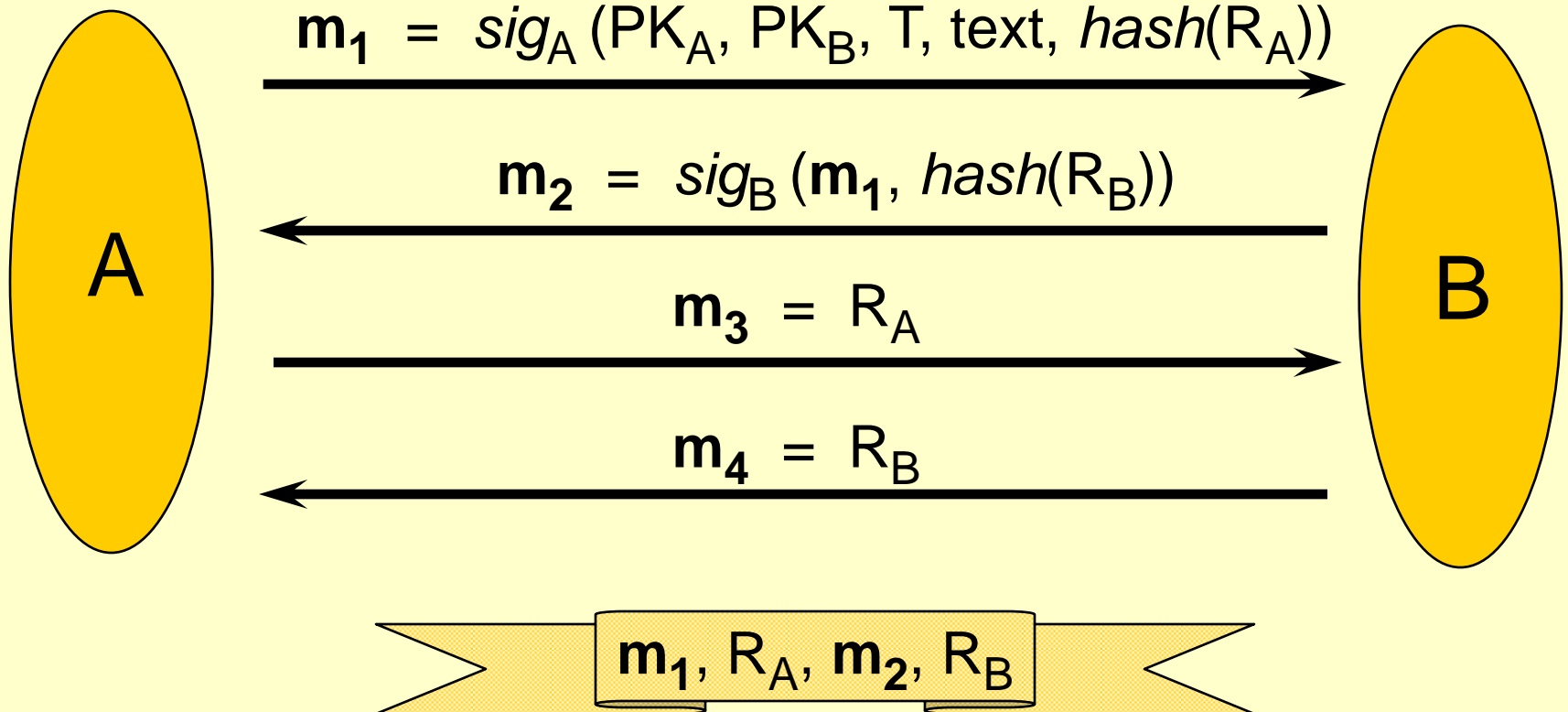
[Dill et al.]

- Describe finite-state system
 - State variables with initial values
 - Transition rules
 - Communication by shared variables
 - Scalable: choose system size parameters
- Specify correctness condition
- Automatic exhaustive state enumeration
 - Hash table to avoid repeating states

Success with research, industrial protocol verification

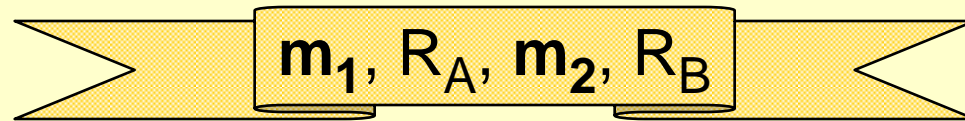
Optimistic Contract Signing

[Asokan, Shoup, Waidner]



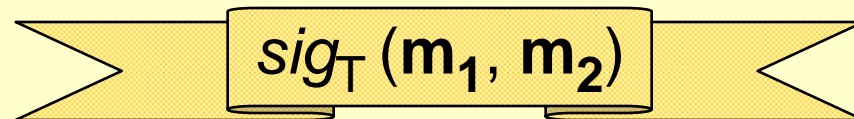
Several Forms of Contract

- Contract from normal execution



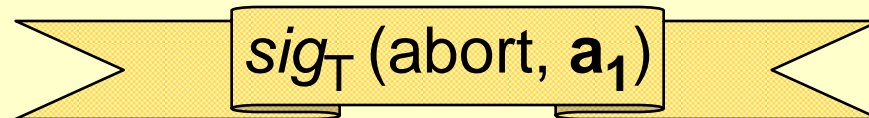
m_1, R_A, m_2, R_B

- Contract issued by third party



$sig_T(m_1, m_2)$

- Abort token issued by third party

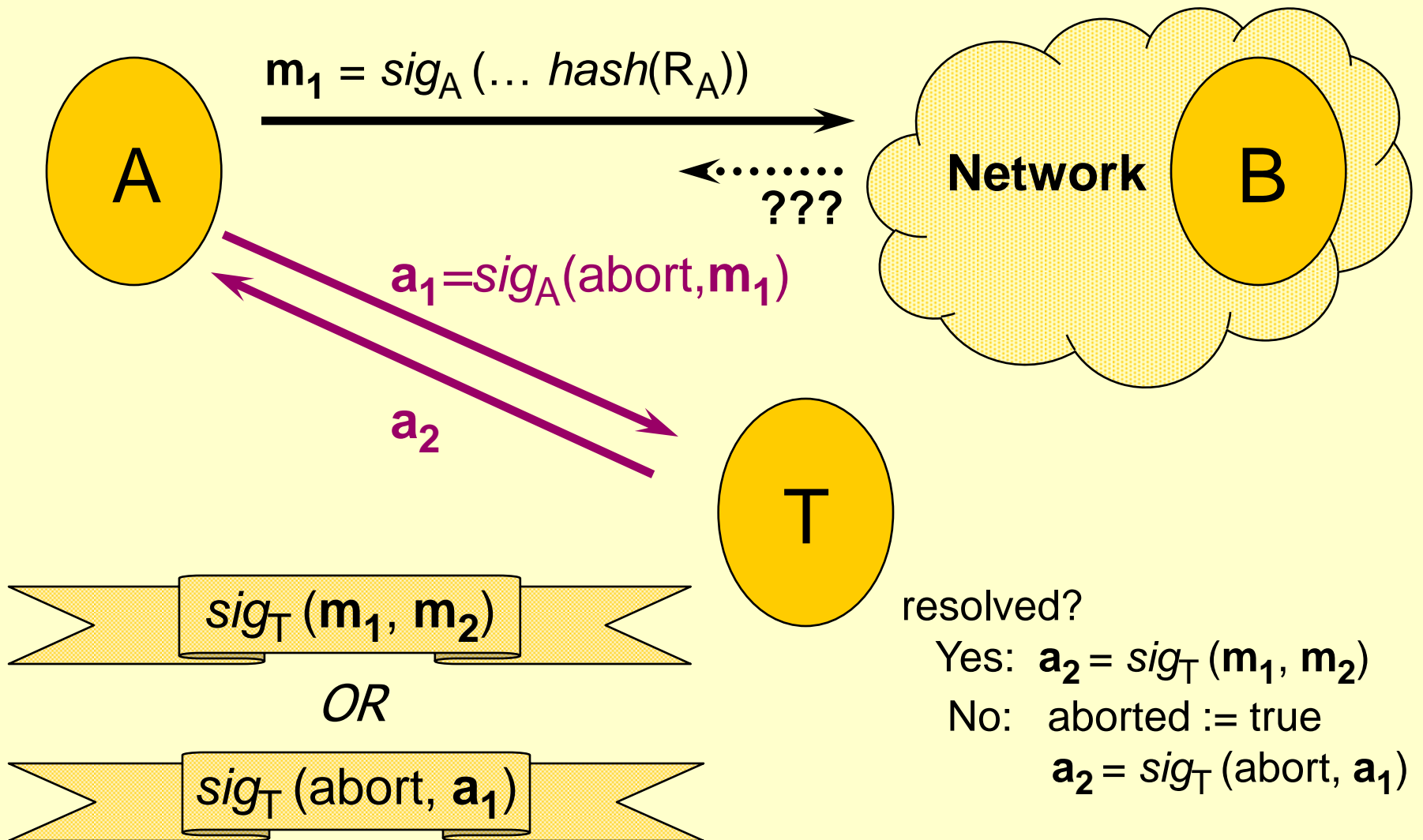


$sig_T(\text{abort}, a_1)$

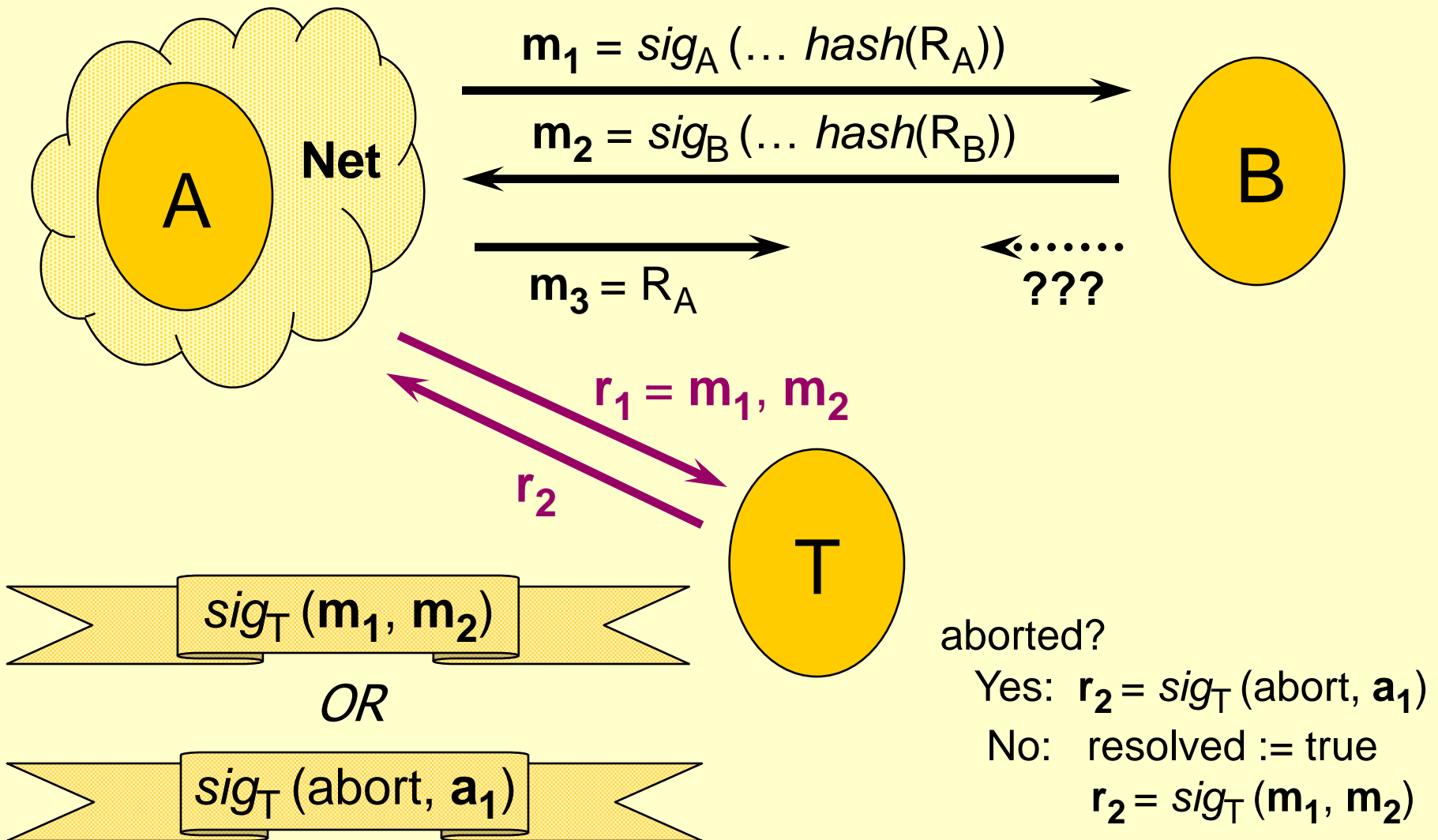
Role of Trusted Third Party

- T can issue an *abort token*
Promise not to resolve the protocol in the future
- T can issue a *replacement contract*
Proof that both parties are committed
- T decides whether to abort or resolve on the first-come-first-serve basis
- T only gets involved if requested by A or B

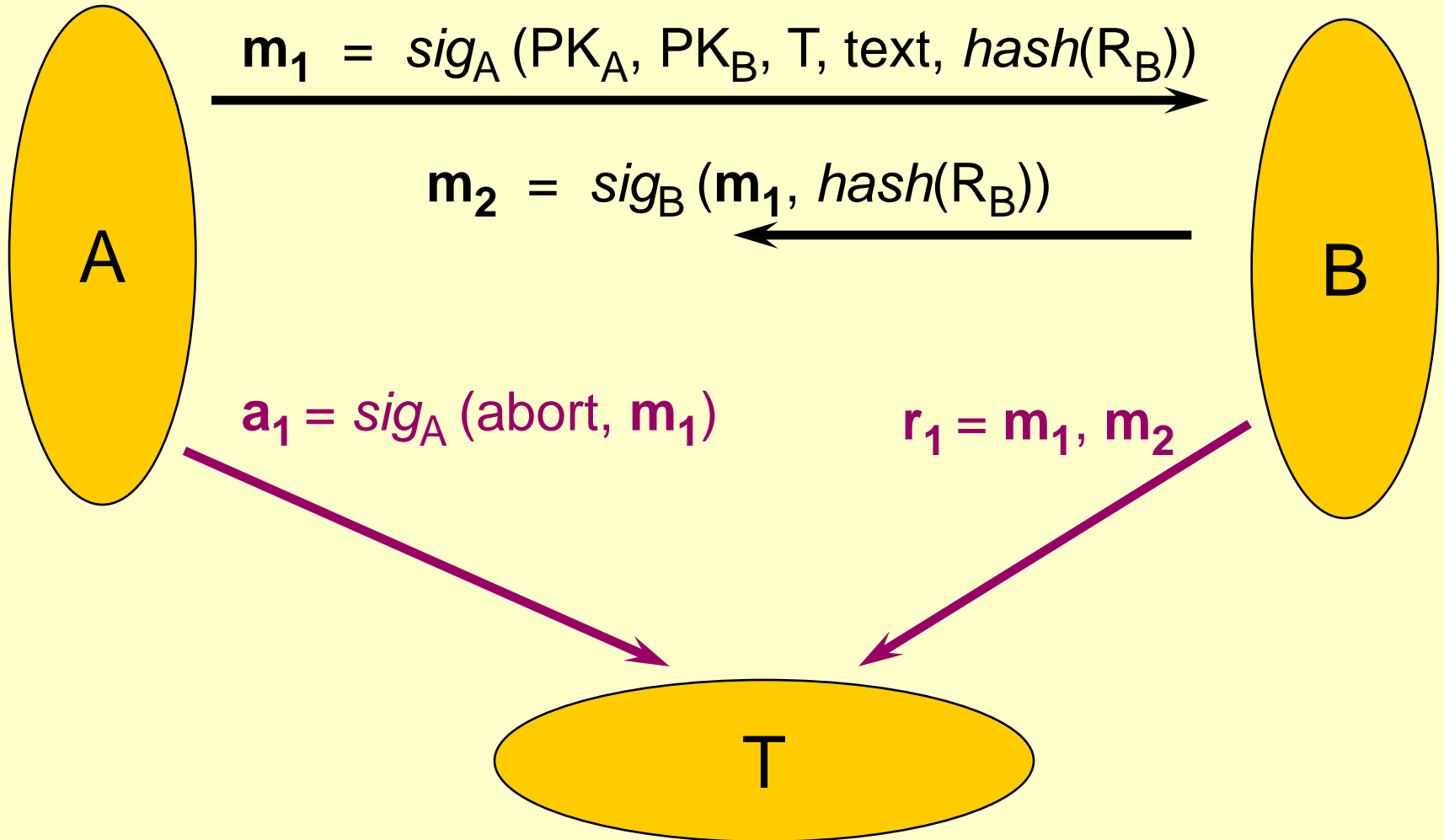
Abort Subprotocol



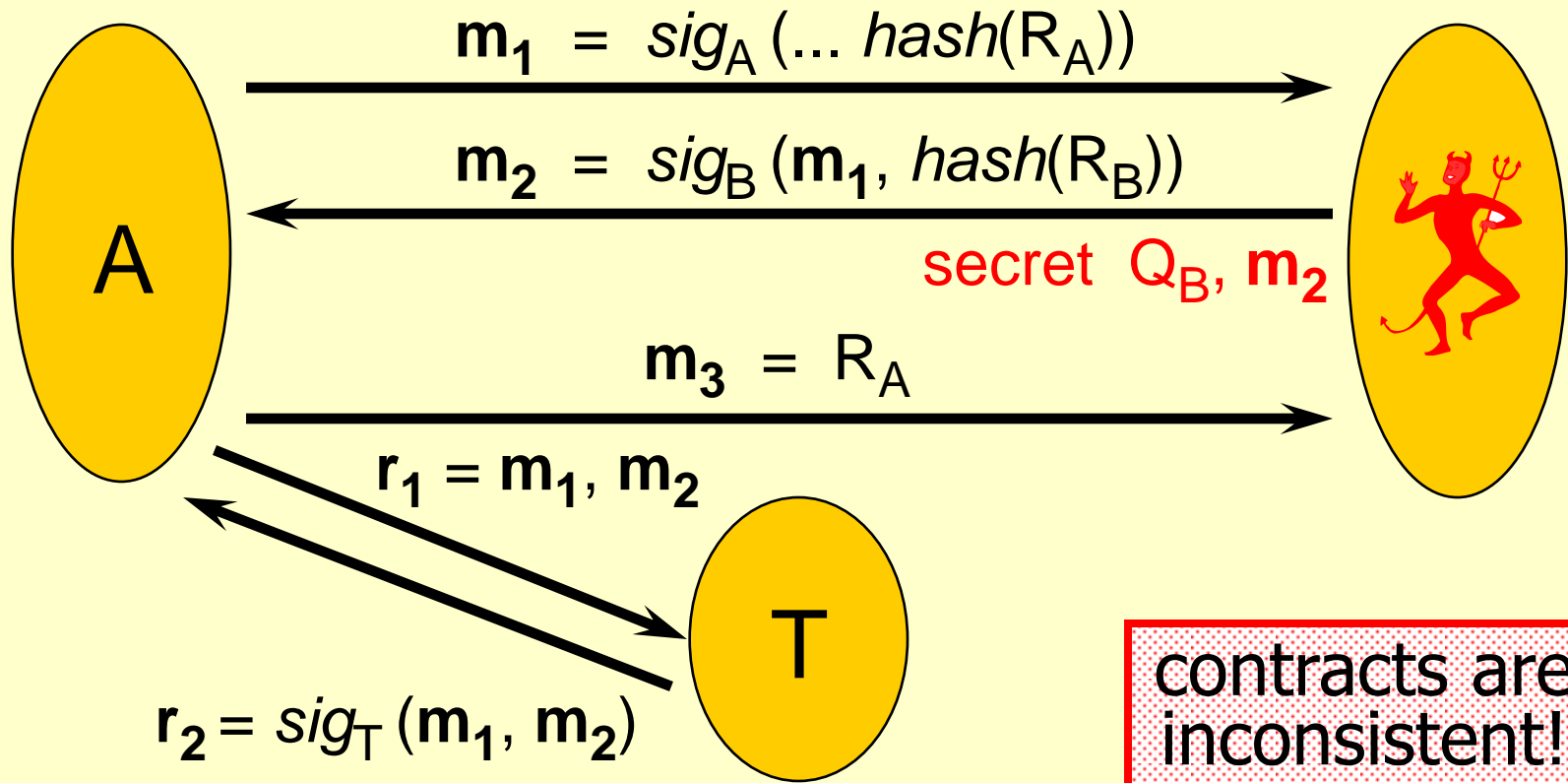
Resolve Subprotocol



Race Condition



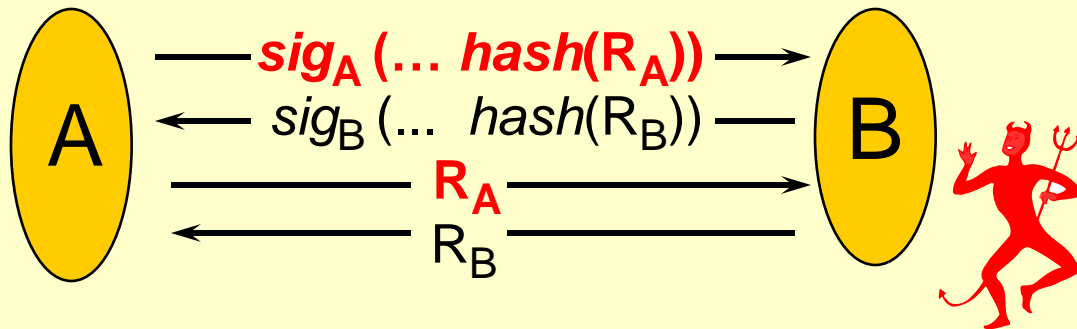
Attack



$sig_T (m_1, m_2)$

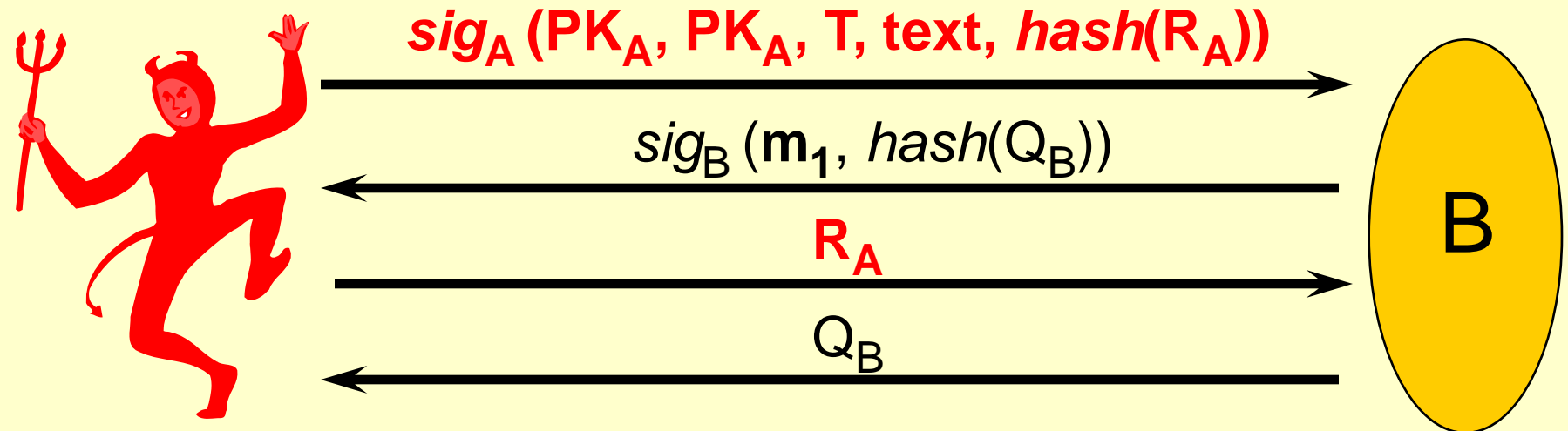
m_1, R_A, m_2, Q_B

Replay Attack

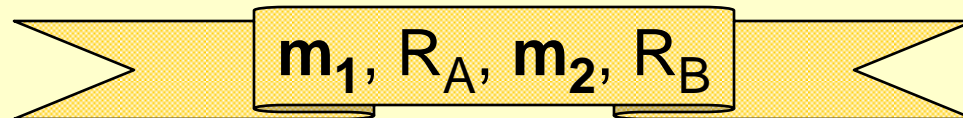
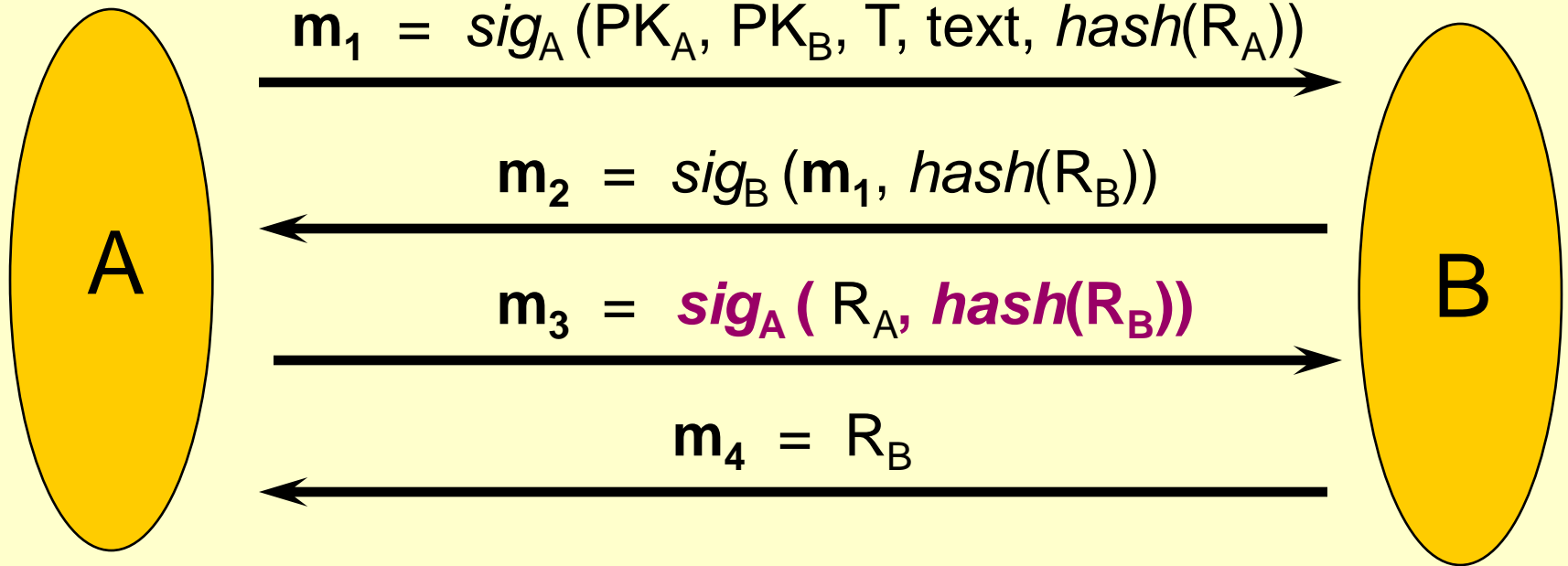


Intruder causes B to commit to old contract with A

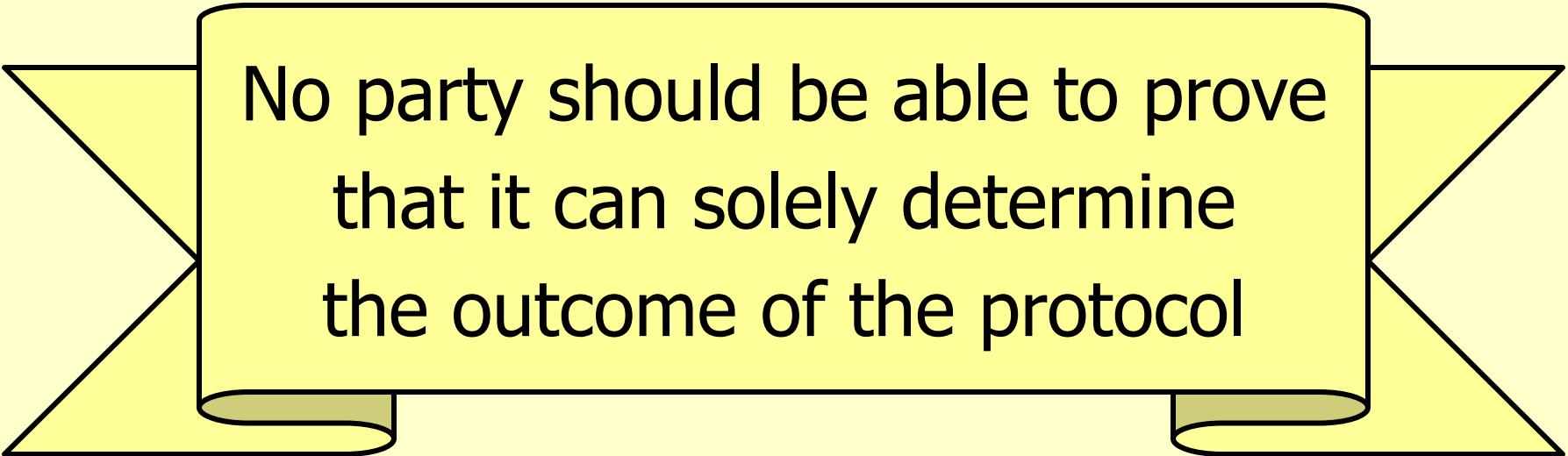
Later ...



Repairing the Protocol



Another Property: Abuse-Freeness



No party should be able to prove that it can solely determine the outcome of the protocol

Example (Alice buys a house from Bob)

Bob should not be able to show Alice's offer to Cynthia so that he can convince Cynthia to pay more

Conclusions

- Fair exchange protocols are subtle
 - Correctness conditions are hard to formalize
 - Unusual constraints on communication channels
- Several interdependent subprotocols
 - Many cases and interleavings
- Finite-state tools are useful for case analysis