

# Contract Signing, Optimism and Advantage

Rohit Chadha University of Sussex  
 John Mitchell Stanford University  
 Andre Scedrov University of Pennsylvania (formerly at UPenn)

Vitaly Shmatikov SRI International

Partially supported by CIP/SW URI "Software Quality and Infrastructure Protection for Diffuse Computing" through ONR grant N00014-01-1-0795

## The Contract Signing Problem

- Two parties agree on the text of the contract
- Each will sign if the other will sign
- Exchange of signatures on asynchronous network
  - Unreliable communication channels
  - Adversarial, malicious parties
  - Unlike the real world, cannot write signatures "in parallel"
- Need fairness and timeliness

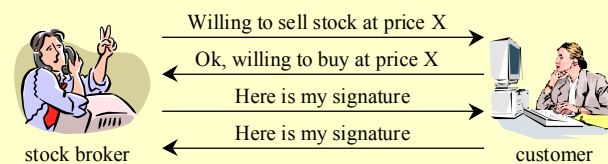
Both players get what they want, or neither does

No player is ever "stuck": protocol always gives some answer

## Contract Signing: State of the Art

- Two-party fair contract signing is impossible
  - Related to impossibility of distributed consensus [Eliasson and Yacobi '80], [Pagnia and Gaumer '90]
- Online trusted third party (TTP) is impractical
- Possible solution: gradual release of signatures
  - Fairness depends on the number of rounds [Damgård '95], [Boneh and Naor '00]
- Our focus is optimistic contract signing
  - TTP used only if something goes wrong
  - Fixed number of rounds; efficient if both parties are honest
  - Non-probabilistic fairness guarantees

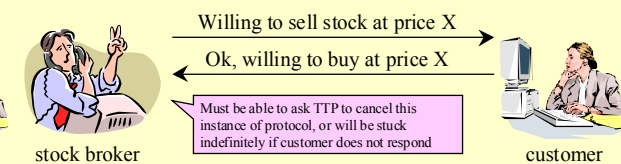
## Optimistic Contract Signing



Trusted third party (TTP) can declare contract binding if presented with the first two messages

Roughly based on [Asokan, Shoup, Waidner Eurocrypt '98], [Garay, Jakobsson, MacKenzie Crypto '99], and dozens of similar protocols

## Is This a Good Protocol?



Can go ahead and complete the sale, OR can still ask TTP to cancel (TTP doesn't know customer has responded)

Optimistically waits for broker to respond ...

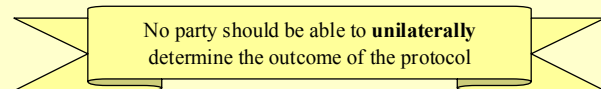
Chooses whether deal will happen: does not have to commit stock for sale, can cancel if sale looks unprofitable

Cannot back out of the deal: must commit money for stock

## Optimism

- An optimistic participant waits for some time before asking the trusted third party for help
  - We use set-of-traces semantics to model optimism in an untimed, nondeterministic, asynchronous model
- Optimistic contract signing assumes that participants are optimistic
  - Otherwise, no better than a trivial protocol with online trusted third party
- What can a contract signing protocol guarantee to an optimistic participant?

## Balance

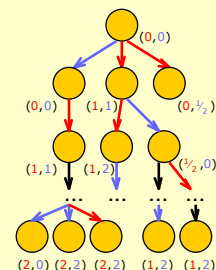


Balance may be violated even if basic fairness is satisfied!

Stock sale example: there is a point in the protocol where the broker can unilaterally choose whether the sale happens or not

Can a timely, optimistic protocol be fair AND balanced?

## Game-Theoretic Model



- Every possible trace of the protocol is a path in this tree
  - Nodes correspond to reachable states
  - Every edge is associated with one of the players or trusted third party
- Standard notion of strategy
  - A has a strategy for getting B's signature if, for any move that B can make, A has a response move s.t. game always ends in some state in which A has B's signature
- A pair of "resolve values" is associated with every node

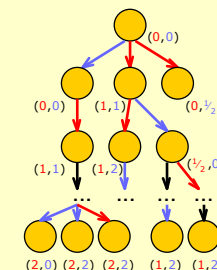
## Resolve Values

Defined in each state, characterize each player's control over the outcome of the protocol game

- $rslv_A(S)=2$  A has a strategy to obtain B's signature regardless of what B does
- $=1$  A has a strategy to obtain B's signature if B does not do anything ("B-silent" strategy)
- $=1/2$  There is a possibility (i.e., a valid protocol trace) that A obtains B's signature if B does not do anything
- $=0$  A cannot obtain B's signature without B's involvement

Subtle distinction: 1 means A wins if he can prevent B from sending messages  
 1/2 means A wins if some race condition is resolved favorably (e.g., if TTP receives A's message before B's message)

## Fairness, Timeliness, Balance



- Fairness (for B)
    - In every  $(2, \dots)$  state, B has strategy to reach a  $(\dots, 2)$  state with TTP's help
  - Timeliness (for B)
    - In every state, B has A-silent strategy to reach  $(0, \dots)$  or  $(\dots, 2)$  state
  - Balance (for B)
    - A never has a strategy to reach  $(2, \dots)$  AND a strategy to reach  $(\dots, 0)$
- If A has a strategy to obtain B's signature AND a strategy to prevent B from getting A's signature, then A can unilaterally choose the outcome

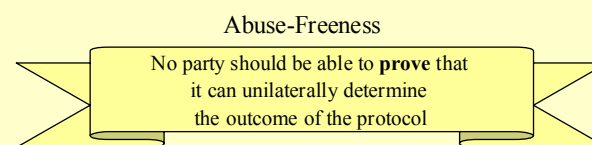
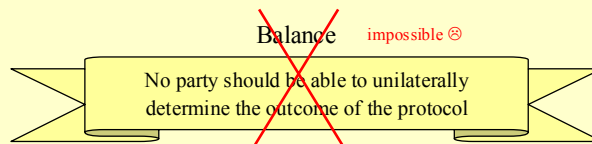
## Modeling Optimism

- An optimistic player waits for some time before asking the trusted third party for help
- Our model: optimistic player asks TTP for help only after receiving special signal from opponent
  - This "out-of-band" signal does not model real communication!
  - This is simply a technical device to restrict our model to the right set of traces
  - Enables us to reason about optimistic play in an untimed, asynchronous communication model

## Impossibility Result

- No optimistic, fair, timely protocol is balanced for the optimistic player
  - Dishonest player can always choose the outcome unilaterally
  - Does not matter which role is played by the optimistic player (this is not first-mover advantage)
  - Similar to impossibility results for distributed consensus
- Bad news for e-commerce
  - Honest party must commit merchandise or money, while dishonest party chooses whether to go ahead with the deal
  - Need an online trusted party in every transaction, or sacrifice timeliness, or abandon purely asynchronous setting

## Abuse-Freeness



[Garay, Jakobsson, MacKenzie Crypto '99]

## Formalization of Abuse-Freeness

- C knows F in state S if
  - F is true in S, and
  - F is true in every state S' indistinguishable from S, given C's observations of the protocol up to this point
  - Standard concept of knowledge from epistemic logic
- Inspired by Joe Halpern's work on logics of knowledge
- Proof of F = evidence causing C to know F
- Abuse-free protocol does not give the player any evidence that can be used to prove the other player's participation in the protocol
  - Useful for auctions: seller cannot prove to potential buyers that some bidder has already submitted a bid

## What Did We Achieve?

- Game-theoretic model for fair exchange
  - Formal definitions of fairness, timeliness, balance
  - Set-of-traces semantics for optimistic behavior
- Impossibility result
  - In any fair, timely, optimistic protocol, dishonest opponent always has advantage against optimistic player
  - Addition of trusted third party does not guarantee balance unless TTP is involved in every instance of the protocol
- Precise definition of abuse-freeness
  - Standard techniques from epistemic logic