

CONTRACT SIGNING

Rohit Chadha, John Mitchell, Andre Scedrov,
Vitaly Shmatikov

Contract signing (fair exchange)

- ◆ Two parties want to exchange signatures on an already agreed upon contract text
- ◆ Parties adversarial
- ◆ Both parties want to sign a contract
- ◆ Neither wants to sign first
- ◆ Fairness: each party gets the other's signature or neither does
- ◆ Timeliness: No player gets stuck

Optimism

- ◆ Fairness requires a third party, T
 - Even 81
 - FLP
- ◆ Trivial protocol
 - Send signatures to T which then completes the exchange
- ◆ Optimistic 3-party protocols
 - T contacted only for error recovery
 - Avoids communication bottlenecks
- ◆ Optimistic player
 - Prefers not to go to T

General protocol outline



- ◆ Trusted third party can force or abort contract
 - Third party can declare contract binding if presented with first two messages.

Model and fairness

- ◆ Call the two participants P and Q
- ◆ Definitions lead to game-theoretic notions
 - If P follows strategy, then Q cannot achieve win over P
 - Or, P follows strategy from some class ...
- ◆ Need timeouts in the model "waiting"
- ◆ **Fairness** for P
 - If Q has P 's contract, then P has a strategy to get Q 's contract

Silent strategies

- ◆ A strategy of Q is P -silent if it succeeds whenever P does nothing
- ◆ Define two values, $rslv_P$ and $rslv_Q$ on reachable states S :
 - $rslv_P(S) = 2$ if P has a strategy to get honest Q 's signature,
 - $= 1$ if P has a Q -silent strategy to reach a state S' such that $rslv_P(S') = 2$,
 - $= 1/2$ if there is a state S' reachable from S that does not involve Q such that $rslv_P(S') = 2$,
 - $= 0$ otherwise

Optimism and timeliness

- ◆ Protocol is **optimistic for Q** if, assuming Q controls the timeouts of both Q and P, then and honest Q has a strategy to get honest P's contract without any messages to/from T
- ◆ A protocol is **timely for Q** if
 - For all reachable states, S, Q has a (P -silent) strategy to drive the protocol to a state S' such that $rslv_Q(S')=2$ or $rslv_P(S')=0$
- ◆ A protocol is **timely** if it is timely for both Q and P

Optimistic participant

- ◆ Honest P is said to be **optimistic** if
 - Whenever P can choose between
 - waiting for a message from Q
 - contacting TTP for any purpose P waits and allows Q to move next
- ◆ Modeled by giving the control of timeouts to Q

[Chadha, Mitchell, Scedrov, Shmatikov]

Abort and resolve strategies

- ◆ Q is said to have a (P-silent) **abort strategy at S** if
 - Q has a (P-silent) strategy to drive the protocol to a state S' such that $rslv_p(S')=0$
- ◆ Q is said to have a (P-silent) **resolve strategy at S** if
 - Q has a (P-silent) strategy to drive the protocol to a state S' such that $rslv_Q(S')=2$

Advantage

- ◆ Q is said to have the **power to abort** against an **optimistic P** the protocol in S
 - if Q has an abort strategy
- ◆ Q is said to have the **power to resolve** against an **optimistic P** the protocol in S
 - if Q has a resolve strategy
- ◆ Q has **advantage** against an **optimistic P** if Q has both the power to abort and the power to complete

Advantage flow

B

C

O-adv

I am willing to sell at this price

O-adv

O-adv

I am willing to buy at this price

Here is my signature

Here is my signature

Impossibility Theorem

- ◆ In any optimistic, fair, and timely contract-signing protocol, any potentially dishonest participant will have an advantage at some non-initial point if the other participant is optimistic
- ◆ 4-valued version of:
 - Even's impossibility of deterministic two-party contract signing
 - Fischer-Lynch-Paterson impossibility of consensus in distributed systems

Proof Outline

- ◆ Pick an optimistic flow: S_0, \dots, S_n . $\text{rslv}_Q(S_n)=2$
 - ◆ $\text{rslv}_Q(S_0)=0$ and $\text{rslv}_Q(S_n)=2$
 - Pick i such that $\text{rslv}_Q(S_i)=0$ and $\text{rslv}_Q(S_{i+1}) > 0$
 - ◆ Protocol is timely for P
 - Q has a P -silent abort strategy at S_i
 - ◆ Transition from S_i to S_{i+1} is a transition of P
 - ◆ Let S, S' be reachable states such that
 - Q_i has a P -silent abort strategy at S
 - S' is obtained from S using a transition of P that does not send any messages to T
- Then Q has a P -silent abort strategy at S'

Proof outline contd..

- ◆ Q has a P -silent abort strategy at S_{i+1}
- ◆ Let S be a reachable state such that Q has an P -silent abort strategy at S
 - Then Q also an abort strategy if P does not send any messages to T
- ◆ Q also an abort strategy at S_{i+1} if P does not send any messages to T
- ◆ Q has power to abort against an optimistic P at S_{i+1}
- ◆ Q has power to resolve against an optimistic P at S_{i+1}
- ◆ Q has an advantage against optimistic P

No evidence of advantage

◆ If

- Q can provide evidence of P's participation to an outside observer X,

then

- Q does not have advantage against an optimistic P

◆ Evidence: what does X *know*

◆ X *knows* fact φ in state σ

- φ is true in any state consistent with X's observations in σ

Conclusions and further work

- ◆ Formal definitions of fairness, optimism, timeliness and advantage were given
- ◆ Impossibility result
 - any fair, timely and optimistic protocol necessary gives advantage
- ◆ Define abuse-freeness precisely using epistemic logic
- ◆ Other properties like trusted-third party accountability need to be investigated
- ◆ Multiparty contract signing protocols need to be investigated
- ◆ Use of automated theorem provers based on rewriting techniques need to be explored