

Computational Soundness for Strategy-Based Properties

Mihhail Aizatulin^{1,2} Henning Schnoor² Thomas Wilke²

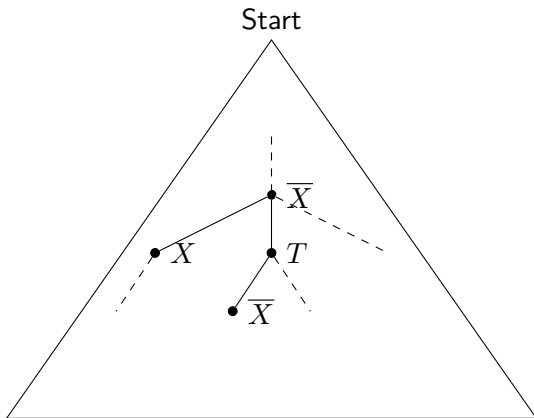
¹Open University

²Christian-Albrechts-Universität zu Kiel,
`mai@informatik.uni-kiel.de, {schnoor|wilke}@ti.informatik.uni-kiel.de`

Cryptoforma, October 02, 2009

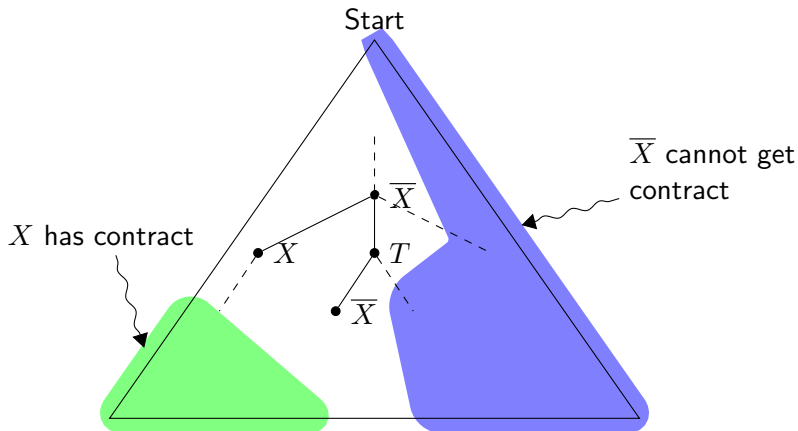
Contract Signing: The Goal

Contract signing is a network game:



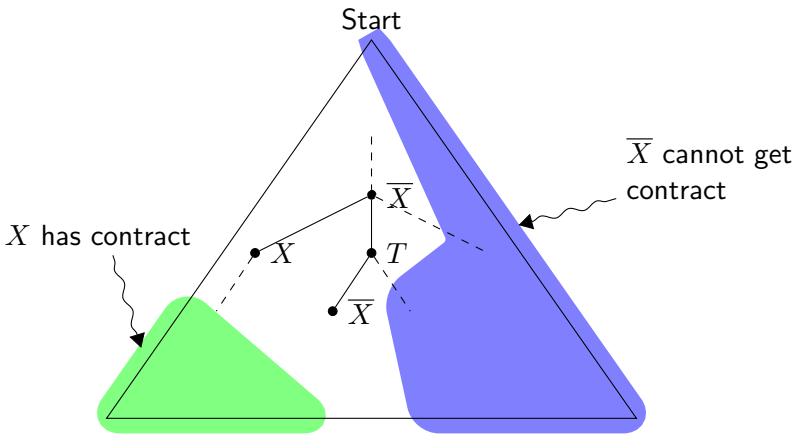
Contract Signing: The Goal

Contract signing is a network game:



Contract Signing: The Goal

Contract signing is a network game:

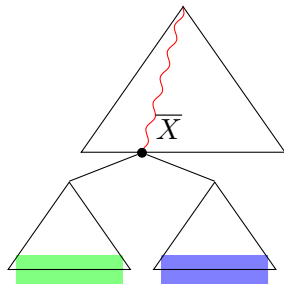


Fairness: $\blacksquare \cap \blacksquare = \emptyset$.

Timeliness: $\langle\langle X \rangle\rangle \diamond (\blacksquare \cup \blacksquare)$.

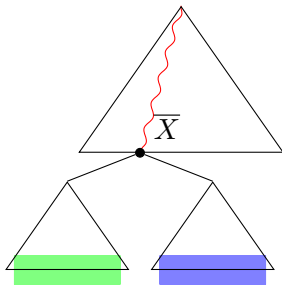
The Problem: Unbalance

In all previous protocols [Asokan *et al.*, 2000; Garay *et al.*, 1999] the dishonest player had too much control:



The Problem: Unbalance

In all previous protocols [Asokan *et al.*, 2000; Garay *et al.*, 1999] the dishonest player had too much control:

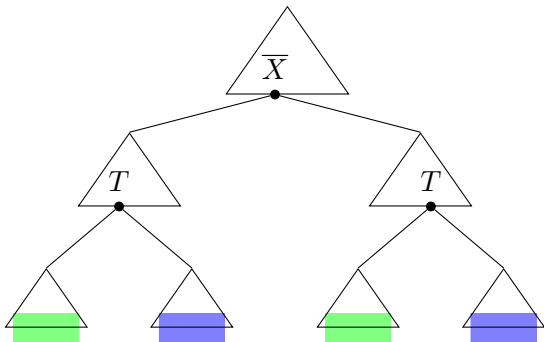


Formally:

$$\langle\langle X, \bar{X}, T \rangle\rangle \diamond (\langle\langle \bar{X} \rangle\rangle \diamond \blacksquare \wedge \langle\langle \bar{X} \rangle\rangle \diamond \blacksquare).$$

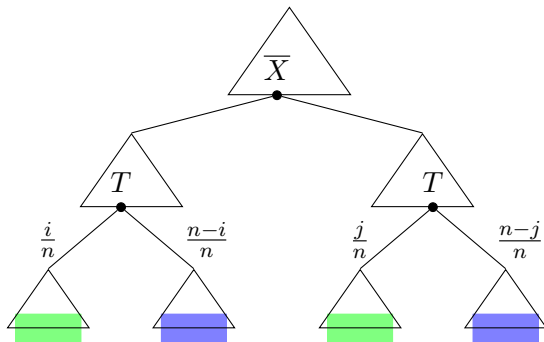
Our Solution

To achieve balance we let the TTP decide the outcome in some cases:



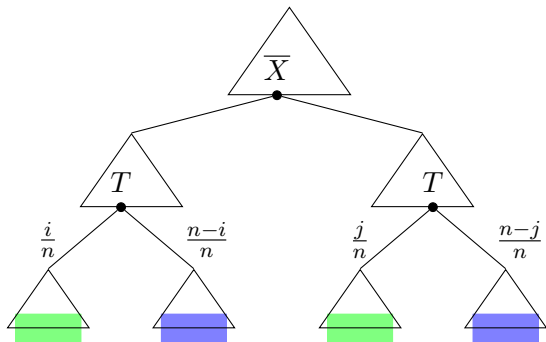
Adding Probabilities

We study n -round protocols with probabilities.



Adding Probabilities

We study n -round protocols with probabilities.

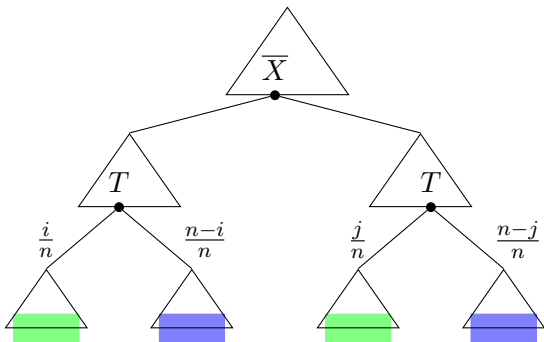


ATL* with probabilities [Chen and Lu, 2007]:

$$\langle\langle X, \bar{X}, T \rangle\rangle^{>0} \diamond \left(\langle\langle \bar{X} \rangle\rangle^{\geq p_r} \diamond \blacksquare \wedge \langle\langle \bar{X} \rangle\rangle^{\geq p_a} \diamond \blacksquare \right).$$

Adding Probabilities

We study n -round protocols with probabilities.



ATL* with probabilities [Chen and Lu, 2007]:

$$\langle\langle X, \bar{X}, T \rangle\rangle^{>0} \diamond \left(\langle\langle \bar{X} \rangle\rangle^{\geq p_r} \diamond \blacksquare \wedge \langle\langle \bar{X} \rangle\rangle^{\geq p_a} \diamond \blacksquare \right).$$

New result 1: for an n -round protocol $p_r + p_a \leq 1 + \frac{1}{n}$ at all times.

New Result 2: Computational Soundness for ATL*

We define a symbolic and a computational interpretation of pATL^* [Aizatulin *et al.*, 2009].

Theorem (Computational Soundness)

If $\text{Game}^{\text{symb}} \models \varphi$ then there exists a negligible function ϵ such that for all security parameters η ,

$$\text{Game}^{\text{comp}, \eta} \models \varphi^{\epsilon(\eta)},$$

where the strategy probabilities in $\varphi^{\epsilon(\eta)}$ are shifted by $\epsilon(\eta)$.

We define a symbolic and a computational interpretation of pATL^* [Aizatulin *et al.*, 2009].

Theorem (Computational Soundness)

If $\text{Game}^{\text{symb}} \models \varphi$ then there exists a negligible function ϵ such that for all security parameters η ,

$$\text{Game}^{\text{comp}, \eta} \models \varphi^{\epsilon(\eta)},$$

where the strategy probabilities in $\varphi^{\epsilon(\eta)}$ are shifted by $\epsilon(\eta)$.

Limitations: only signatures and only finite games.

Main Open Problem

We would like to extend the result to infinite games (multiple sessions, auctions).

Main Open Problem

We would like to extend the result to infinite games (multiple sessions, auctions).

But computational games stop early, so how do we preserve liveness?



Mihhail Aizatulin, Henning Schnoor, and Thomas Wilke.

Computationally sound analysis of a probabilistic contract signing protocol.

In Michael Backes and Peng Ning, editors, *ESORICS*, volume 5789 of *Lecture Notes in Computer Science*, pages 571–586. Springer, 2009.



N. Asokan, Victor Shoup, and Michael Waidner.

Optimistic fair exchange of digital signatures.

IEEE Journal on Selected Areas in Communications, 18(4):593–610, 2000.



Taolue Chen and Jian Lu.

Probabilistic alternating-time temporal logic and model checking algorithm.

In *FSKD (2)*, pages 35–39, 2007.



Juan A. Garay, Markus Jakobsson, and Philip D. MacKenzie.

Abuse-free optimistic contract signing.

In *CRYPTO '99: Proceedings of the 19th Annual International Cryptology Conference on Advances in Cryptology*, pages 449–466, London, UK, 1999. Springer-Verlag.