Computational Soundness for Strategy-Based Properties

Mihhail Aizatulin\textsuperscript{1,2}  Henning Schnoor\textsuperscript{2}  Thomas Wilke\textsuperscript{2}

\textsuperscript{1}Open University

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

Cryptoforma, October 02, 2009
Contract signing is a network game:

\[
\text{Start}
\]

\[
X \quad \overline{X} \quad T
\]

Fairness: \( \cap = \emptyset \).

Timeliness: \( \langle \langle \cup \rangle \rangle \).
Contract signing is a network game:

- \( X \) cannot get contract
- \( X \) has contract

Start

Fairness: \( \cap \) = \( \emptyset \)
Timeliness: \( \langle \langle X \rangle \rangle (\cup) \)

Mihhail Aizatulin, Henning Schnoor, Thomas Wilke
Computational Soundness for Strategy-Based Properties
Contract signing is a network game:

- $X$ cannot get contract
- $X$ has contract

Fairness: $\square \cap \Diamond = \emptyset$
Timeliness: $\langle\langle X\rangle\rangle \Diamond (\square \cup \Diamond)$
In all previous protocols [Asokan et al., 2000; Garay et al., 1999] the dishonest player had too much control:
In all previous protocols [Asokan et al., 2000; Garay et al., 1999] the dishonest player had too much control:

Formally:

\[ \langle\langle X, \overline{X}, T \rangle\rangle \diamond (\langle\langle \overline{X} \rangle\rangle \diamond \text{green} \land \langle\langle \overline{X} \rangle\rangle \diamond \text{blue}) . \]
To achieve balance we let the TTP decide the outcome in some cases:
We study $n$-round protocols with probabilities.

\[ \langle \langle X \rangle \rangle \geq p_r \land \langle \langle X \rangle \rangle \geq p_a \]

**New result 1:** for an $n$-round protocol $p_r + p_a \leq 1 + \frac{1}{n}$ at all times.
We study $n$-round protocols with probabilities.

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

$$\langle\langle X, X, T \rangle \rangle >^0 \Diamond (\langle\langle X \rangle \rangle \geq p_r \Diamond \text{green} \land \langle\langle X \rangle \rangle \geq p_a \Diamond \text{blue}) .$$
We study $n$-round protocols with probabilities.

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

$$\langle X, \overline{X}, T \rangle > 0 \diamond (\langle \overline{X} \rangle \geq p_r \diamond \text{[Green]} \land \langle X \rangle \geq p_a \diamond \text{[Blue]})$$.

New result 1: for an $n$-round protocol $p_r + p_a \leq 1 + \frac{1}{n}$ at all times.
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 $\epsilon$ such that for all security parameters $\eta$,

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

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

Limitations: only signatures and only finite games.
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 $\varepsilon$ such that for all security parameters $\eta$,

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

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

Limitations: only signatures and only finite games.
We would like to extend the result to infinite games (multiple sessions, auctions).
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.


N. Asokan, Victor Shoup, and Michael Waidner.

Optimistic fair exchange of digital signatures.

Taolue Chen and Jian Lu.

Probabilistic alternating-time temporal logic and model checking algorithm.


Abuse-free optimistic contract signing.