Balanced Contract Signing

Mihhail Aizatulin

Open University

Cryptoforma, 29 January 2009
1 Introduction
2 Properties
3 Protocols
4 Conclusion
A contract-signing protocol allows two parties to exchange tokens that represent a binding contract between them.

- The actual form of the tokens may depend on the protocol.
- Basic property is *fairness*: in the end either both parties should get a contract, or neither of them.
- Fairness is impossible with only two participants [Even and Yacobi, 1980], so a trusted third party (TTP) is required.
Important Properties

Threat model: a dishonest participant collaborates with a Dolev-Yao attacker, but cannot delay messages forever.

- **Optimism**: two honest participants have a strategy to sign the contract without sending messages to the TTP.

- **Timeliness**: each participant always has a strategy to unilaterally terminate the session.

- **Balance**: a (potentially dishonest) participant never has a strategy to unilaterally determine the outcome of the session.

Previously existing protocols: optimistic and timely, but not balanced.

**New result**: a protocol with all 3 properties [Aizatulin, 2008].
Main subprotocol:
\[ O \rightarrow R: \text{CMT}_O, \]
\[ R \rightarrow O: \text{CTR}_R, \]
\[ O \rightarrow R: \text{CTR}_O. \]

Resolve subprotocol:
\[ R \rightarrow T: \langle \text{CMT}_O, \text{CTR}_R \rangle, \]
\[ T \rightarrow R: \text{R-CTR}, \]
\[ T \rightarrow O: \text{CTR}_R. \]

Which properties hold?
Level II: Optimism + Timeliness

Prior state of the art [Asokan et al., 2000, Garay et al., 1999]:

Main subprotocol:
\[ O \rightarrow R : \text{CMT}_O, \]
\[ R \rightarrow O : \text{CMT}_R, \]
\[ O \rightarrow R : \text{CTR}_O, \]
\[ R \rightarrow O : \text{CTR}_R. \]

Resolve subprotocol for \( X \in \{O, R\} \):
\[ X \rightarrow T : \langle \text{CMT}_O, \text{CMT}_R \rangle, \]
\[ T \rightarrow X : \text{R-CTR}. \]

Abort subprotocol:
\[ O \rightarrow T : \text{abort-request}, \]
\[ T \rightarrow O : \text{abort-token}. \]

How do you attack balance here?
New idea: first exchange *preliminary commitments*. Those will be rejected by the TTP in 50% of the cases.

The main flow, together with resolve and abort chances for $R$:

<table>
<thead>
<tr>
<th>Step</th>
<th>resolve</th>
<th>abort</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$O \rightarrow R$: P-CMT$_O$</td>
<td>0.5</td>
<td>1</td>
</tr>
<tr>
<td>$R \rightarrow O$: P-CMT$_R$</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>$O \rightarrow R$: CMT$_O$</td>
<td>1</td>
<td>0.5</td>
</tr>
<tr>
<td>$R \rightarrow O$: CMT$_R$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$O \rightarrow R$: CTR$_O$</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$R \rightarrow O$: CTR$_R$</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

The hard part is correct behavior of the TTP to prevent cheating...
Figure: Specification of $T$ as an automaton.
Remarks

- Our protocol is *TTP-accountable*: if a corrupt TTP violates fairness, the cheated participant can prove that.

- The properties cannot be expressed by simple quantification over runs, in particularly not in LTL or CTL. Instead we develop a logic based on alternating-time temporal logic (ATL) [Alur et al., 2002, Kähler, 2008]:

\[
\text{balanced}(O) = \langle\langle\rangle\rangle_{O \text{-honest}} \square \neg (\langle\langle R, N\rangle\rangle_{O \text{-honest}} \Diamond c_R)
\]

\[
\land (\langle\langle R, N\rangle\rangle_{O \text{-honest}} \Diamond \langle\langle\rangle\rangle_{R \text{-silent}} \square \neg c_O).
\]

- Informal specification of properties can be very ambiguous, for instance a small change in wording makes balance impossible [Chadha et al., 2005]. This highlights the need of formal logics for specifications.
Two main contributions:

- Precise specification of properties using formal logics.
- New, more secure protocol.
Thank you!
Mihhail Aizatulin.
A timely and balanced optimistic contract-signing protocol.

Rajeev Alur, Thomas A. Henzinger, and Orna Kupferman.
Alternating-time temporal logic.

N. Asokan, Victor Shoup, and Michael Waidner.
Optimistic fair exchange of digital signatures.
Rohit Chadha, John C. Mitchell, Andre Scedrov, and Vitaly Shmatikov.

Contract signing, optimism, and advantage.


S. Even and Y. Yacobi.

Relations among public key signature schemes.

Technical Report 175, Computer Science Department, Technion, Israel, 1980.


Abuse-free optimistic contract signing.

Detlef Kähler.

*Strategy Properties for Cryptographic Protocols.*