DECISION PROCEDURE FOR TRACE EQUIVALENCE

V. Cheval, H. Comon-Lundh, S. Delaune
LSV, ENS Cachan, CNRS, INRIA Saclay

27 June 2011
Analysing the security of cryptographic protocols

- Alice
- Intruder
- Bob

The intruder can
- intercept all messages
- transmit or modify messages
- test equality between messages
- initiate several sessions
Can the intruder deduce the unknown’s identity?

Equivalence properties: strong secret, anonymity,...
Can the intruder distinguish the two situations?
GOAL

Decision procedure for trace equivalence
• A. Tiu and J. E. Dawson. *Automating open bisimulation checking for the spi calculus*.

Observational equivalence is used in:


Equivalent to trace equivalence for *simple processes* without else branch:

PREVIOUS WORKS

- Observational equivalence is used in:

- Equivalent to trace equivalence for *simple processes* without else branch:

- Existing tool: ProVerif
  - B. Blanchet, M. Abadi, and C. Fournet. *Automated verification of selected equivalences for security protocols.*
MOTIVATION

Why trace equivalence?

Two problematic examples:
MOTIVATION

Why trace equivalence?

Two problematic examples:

Decision procedure for trace equivalence
RESULT

Decision procedure for trace equivalence

• between two processes
  * possibly non deterministic
  * possibly with non trivial else branches
  * possibly with private channels
  * with bounded number of sessions
• complete and sound
• terminate