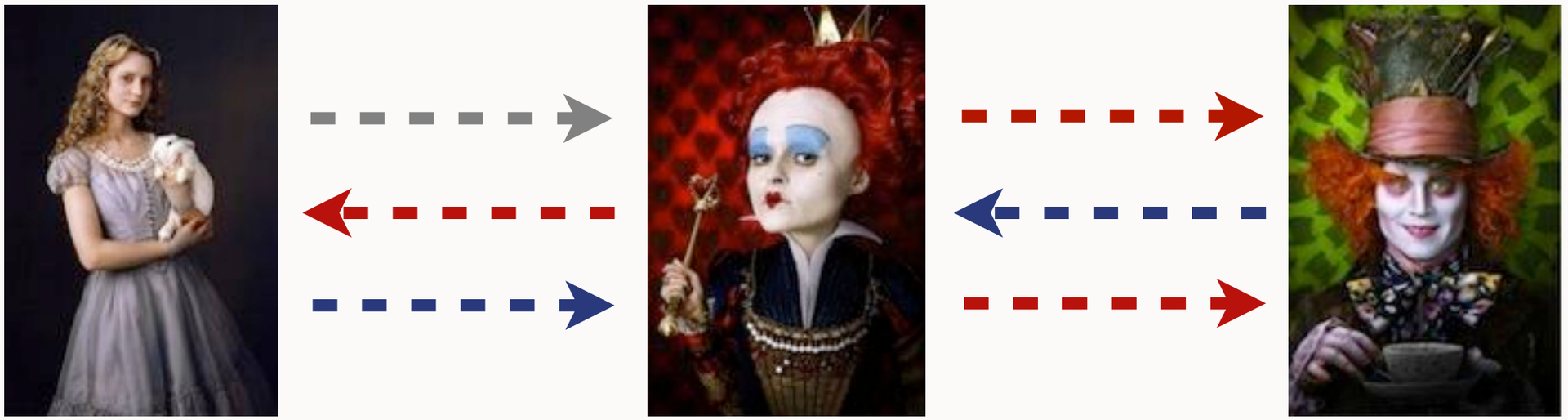
Decision procedure for trace equivalence

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

27 June 2011

CONTEXT

- Analysing the security of cryptographic protocols



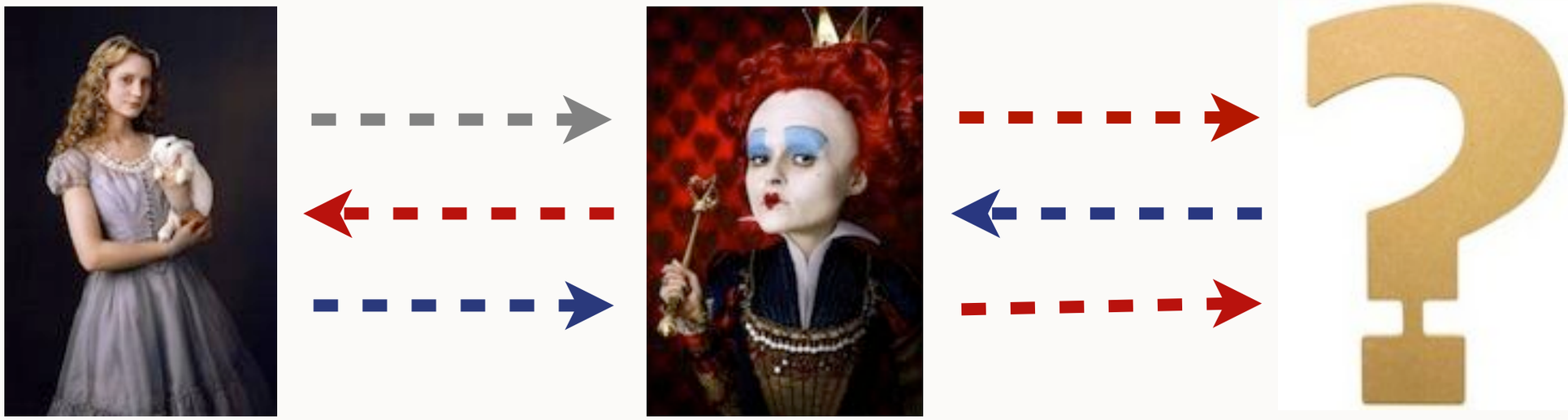
Alice Intruder Bob

The intruder can

- intercept all messages
- transmit or modify messages
- test equality between messages
- initiate several sessions

CONTEXT

- Equivalence properties : strong secret, anonymity,...

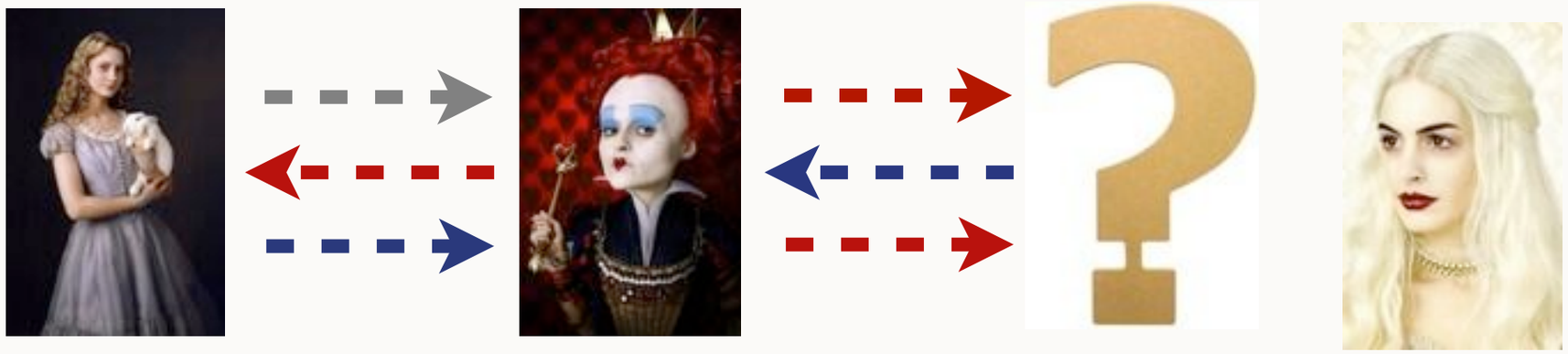


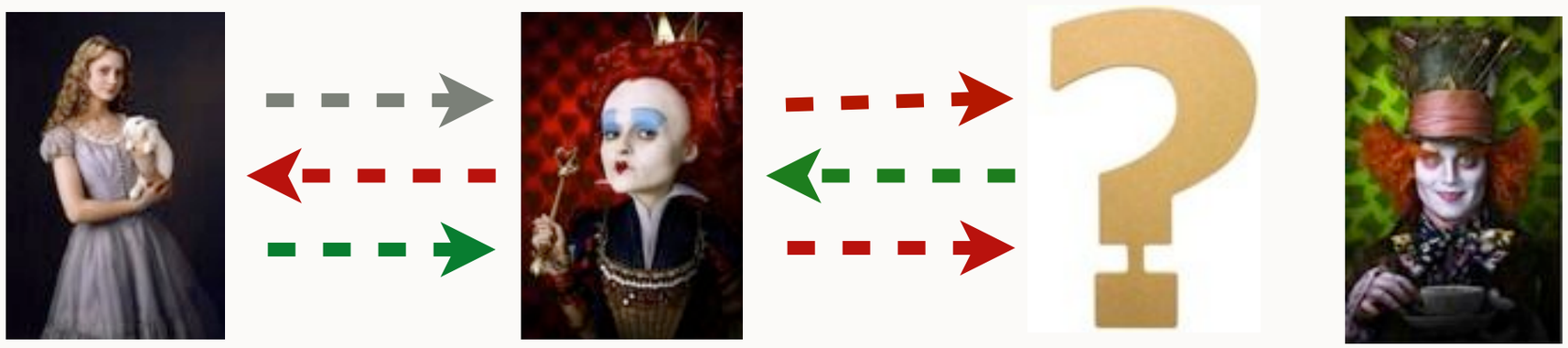
Alice Intruder Unknown

Can the intruder deduce the unknown's identity ?

CONTEXT

- Equivalence properties : strong secret, anonymity,...





Can the intruder distinguish the two situations ?

GOAL

Decision procedure for trace equivalence

PREVIOUS WORKS

- Observational equivalence is used in :
  - A. Tiu and J. E. Dawson. *Automating open bisimulation checking for the spi calculus.*
  - M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires.* Phd thesis

PREVIOUS WORKS

- Observational equivalence is used in :
  - A. Tiu and J. E. Dawson. *Automating open bisimulation checking for the spi calculus.*
  - M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires.* Phd thesis
- Equivalent to trace equivalence for *simple processes* without else branch :
  - V. Cortier and S. Delaune. *A method for proving observational equivalence.*

PREVIOUS WORKS

- Observational equivalence is used in :
  - A. Tiu and J. E. Dawson. *Automating open bisimulation checking for the spi calculus.*
  - M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires.* Phd thesis

- Equivalent to trace equivalence for *simple processes* without else branch :
  - V. Cortier and S. Delaune. *A method for proving observational equivalence.*

- 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 :

- e-passport protocols : M. Arapinis, T. Chothia, E. Ritter, and M. Ryan. *Analysing unlinkability and anonymity using the applied pi calculus.*
- private authentication protocol : M. Abadi and C. Fournet. *Private authentication. Theoretical Computer Science.*

MOTIVATION

- Why trace equivalence ?

Two problematic examples :

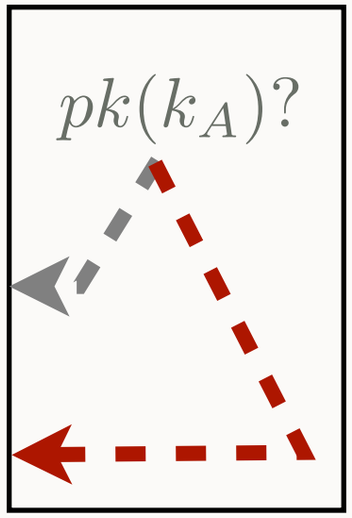
- e-passport protocols : M. Arapinis, T. Chothia, E. Ritter, and M. Ryan. *Analysing unlinkability and anonymity using the applied pi calculus.*
- private authentication protocol : M. Abadi and C. Fournet. *Private authentication. Theoretical Computer Science.*

Alice

$\{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}$

$\{\langle N_a, N_b, pk(k_B)\rangle\}_{pk(k_A)}$

$\{N\}_{pk(k_A)}$



Bob

RESULT

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