Tools for proving equivalence

V.Cheval
LSV, ENS-Cachan, CNRS
School of computer science, University of Birmingham

FMATS2, Cambridge

05 February 2013

SECURITY PROPERTIES

Reachability properties

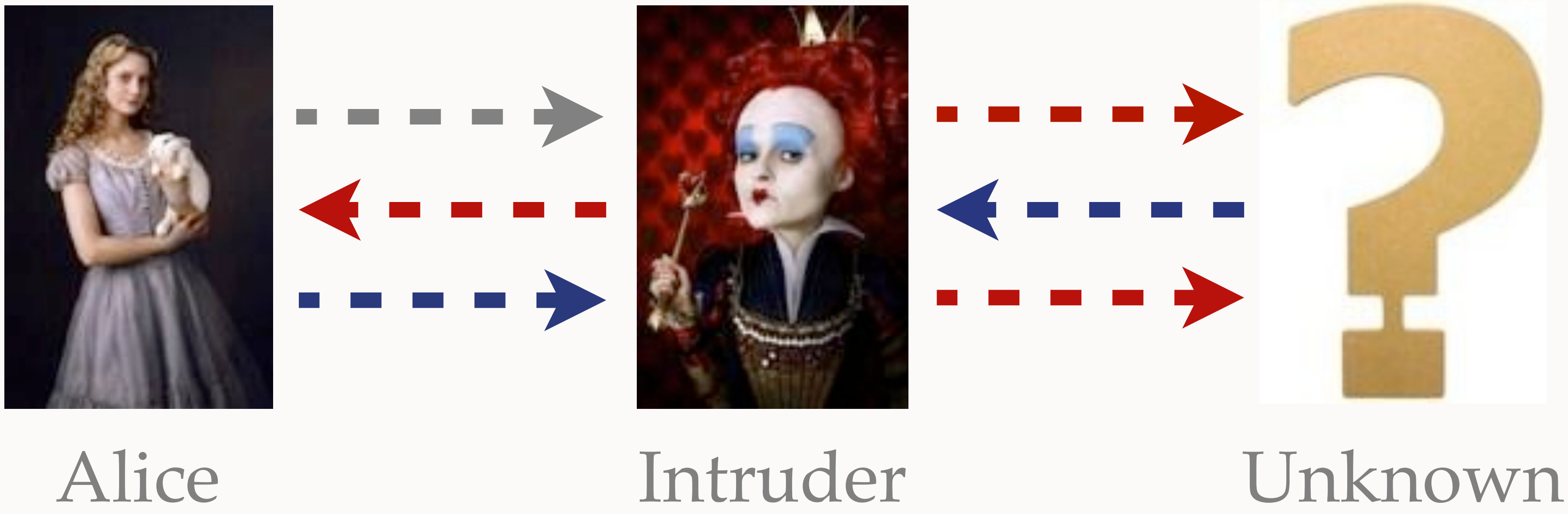
- Secrecy, Authentication, ...

Equivalence properties

- Anonymity, Privacy, Receipt-Freeness, ...

CONTEXT

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



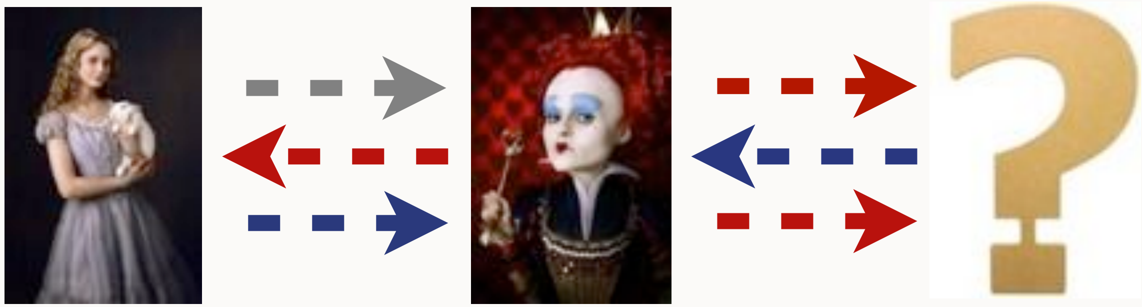
Alice

Intruder

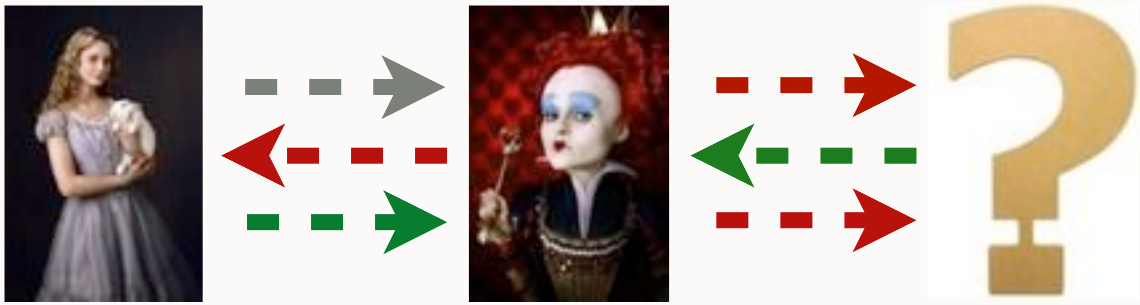
Unknown

CONTEXT

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



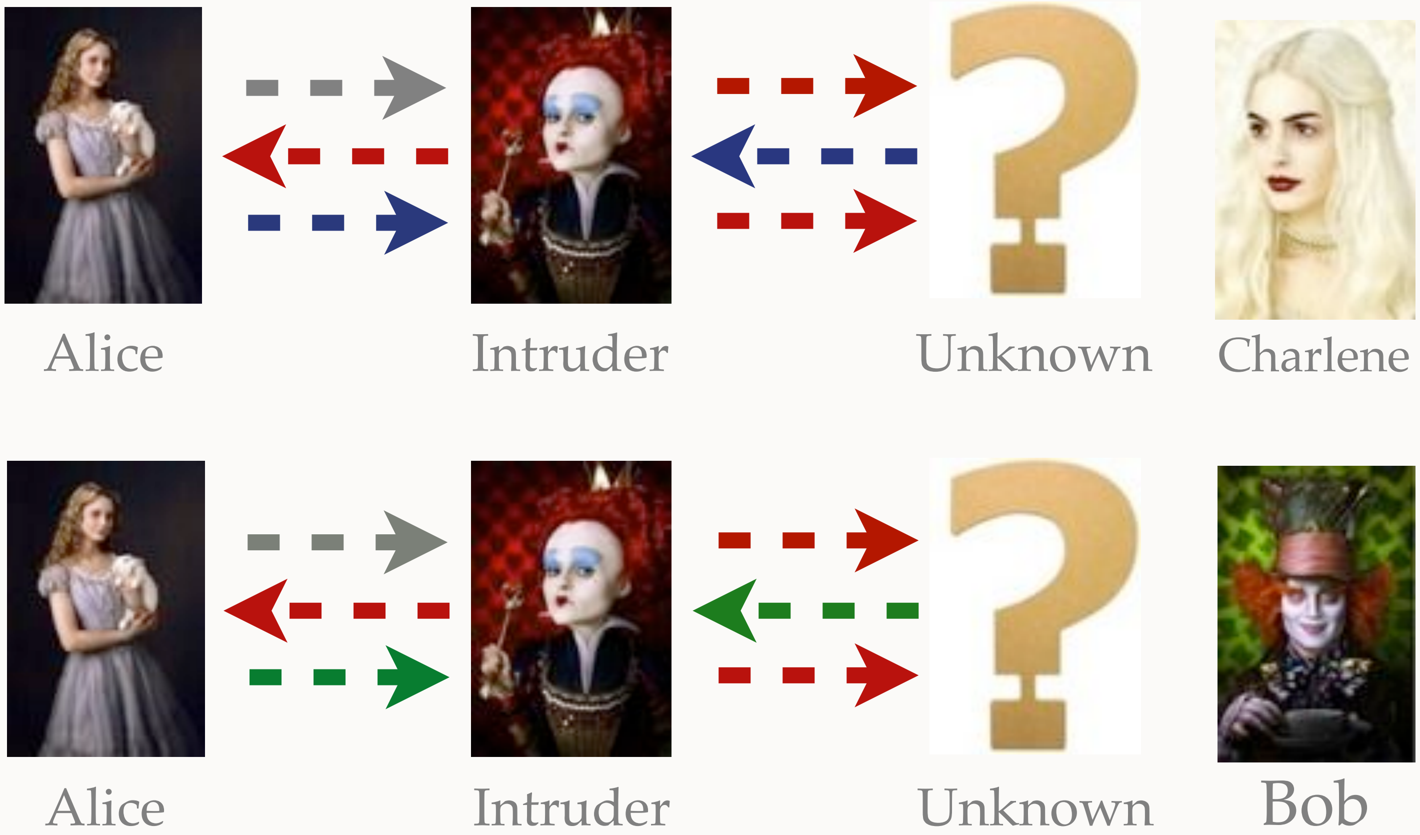
Alice Intruder Unknown



Alice Intruder Unknown

CONTEXT

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



Alice Intruder Unknown Charlene

Alice Intruder Unknown Bob

TOOLS

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.*

TOOLS

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.*

Extension of ProVerif

- Unbounded number of sessions
- Any cryptographic primitives
- Sound
- Possible false attack
- Does not always terminate
- No more biprocess !

APTE

- Bounded number of sessions
- Fixed set of cryptographic primitives
- Sound
- Complete
- Always terminate
- Can consider length of messages

TOOLS

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.*

Extension of ProVerif

- Unbounded number of sessions
- Any cryptographic primitives
- Sound
- Possible false attack
- Does not always terminate
- No more biprocess !

Useful to prove

APTE

- Bounded number of sessions
- Fixed set of cryptographic primitives
- Sound
- Complete
- Always terminate
- Can consider length of messages

Useful to find attacks

APTE

- Length of messages

$$\mathsf{enc}(x, y)$$

$$\ell_{\mathsf{enc}}(x, y) = \alpha + \beta_1 x + \beta_2 y$$

$$\begin{aligned}\ell(\mathsf{enc}(u, v)) &= \ell_{\mathsf{enc}}(\ell(u), \ell(v)) \\ &= \alpha + \beta_1 \ell(u) + \beta_2 \ell(v))\end{aligned}$$