AUTOMATIC TOOLS TO PROVE PRIVACY-TYPE PROPERTIES

Vincent Cheval
School of Computer Science, University of Birmingham

February 22, 2013

Context

Most communications take place over a public network

It is important to ensure their security

Cryptographic protocols

Cryptographic protocols

- small programs designed to secure communication (e.g. secrecy)
- use cryptographic primitives (e.g. encryption, signature)

Cryptographic protocols

Cryptographic protocols

- small programs designed to secure communication (e.g. secrecy)
- use cryptographic primitives (e.g. encryption, signature)

What do we need to build a secure protocol ?

Cryptographic protocols

Cryptographic protocols

- small programs designed to secure communication (e.g. secrecy)
- use cryptographic primitives (e.g. encryption, signature)

What do we need to build a secure protocol ?

- Reliable cryptography
- Correct protocol specification
- Implementation satisfying the specification

Cryptographic protocols

Cryptographic protocols

- small programs designed to secure communication (e.g. secrecy)
- use cryptographic primitives (e.g. encryption, signature)

What do we need to build a secure protocol ?

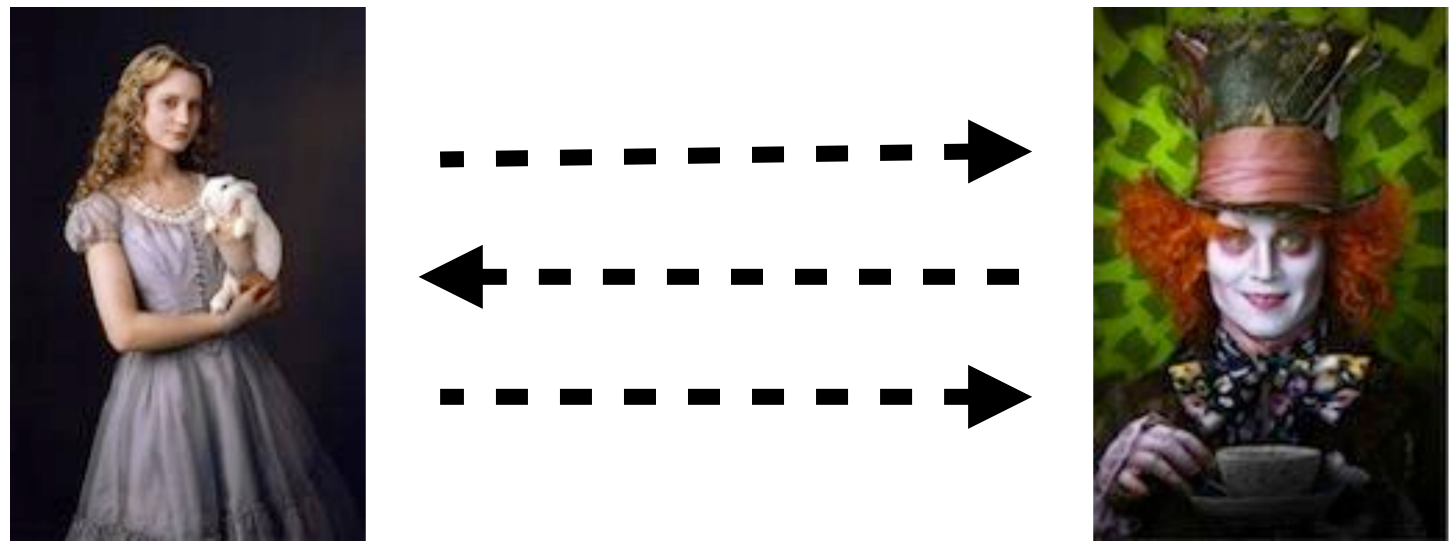
- Reliable cryptography
- Correct protocol specification
- Implementation satisfying the specification

Symbolic model

Alice

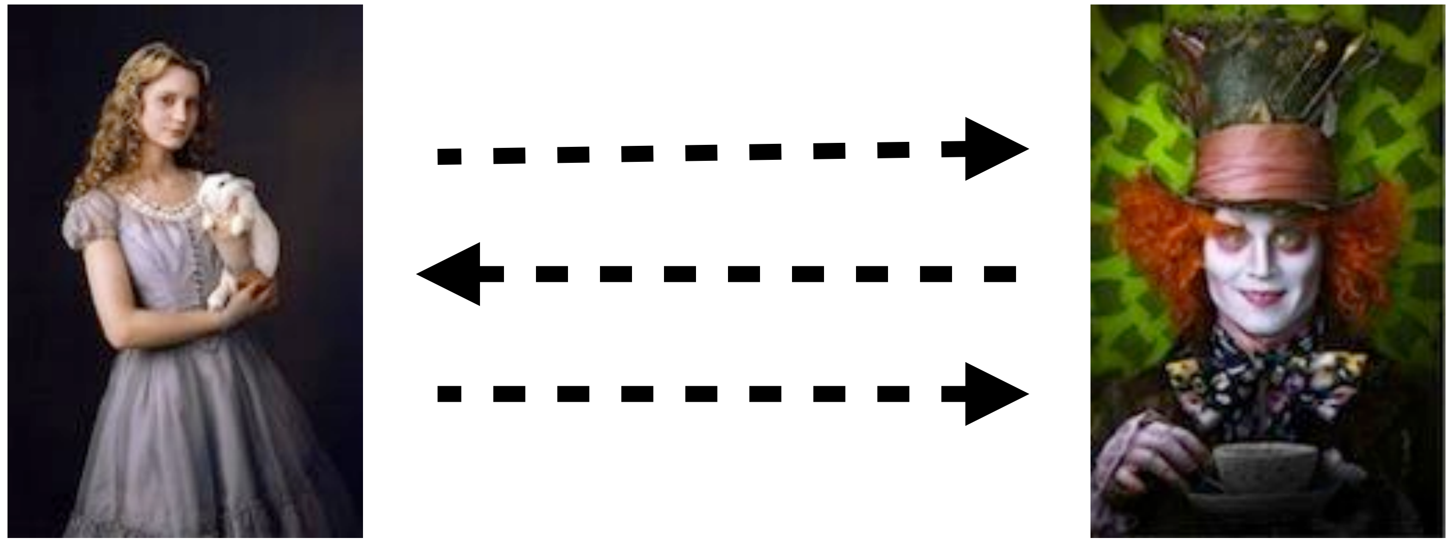
Bob

Symbolic model



Alice Bob

Symbolic model



Alice Bob

- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M \rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

Symbolic model

Alice

Attacker

Bob

- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M\rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

Symbolic model

Alice

Attacker

Bob

- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M \rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

The attacker can

- intercept all messages
- transmit or modify messages
- test equality between messages

Symbolic model

Alice

Attacker

Bob

- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M \rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

The attacker can

- intercept all messages
- transmit or modify messages
- test equality between messages

Symbolic model

Alice

Attacker

Bob

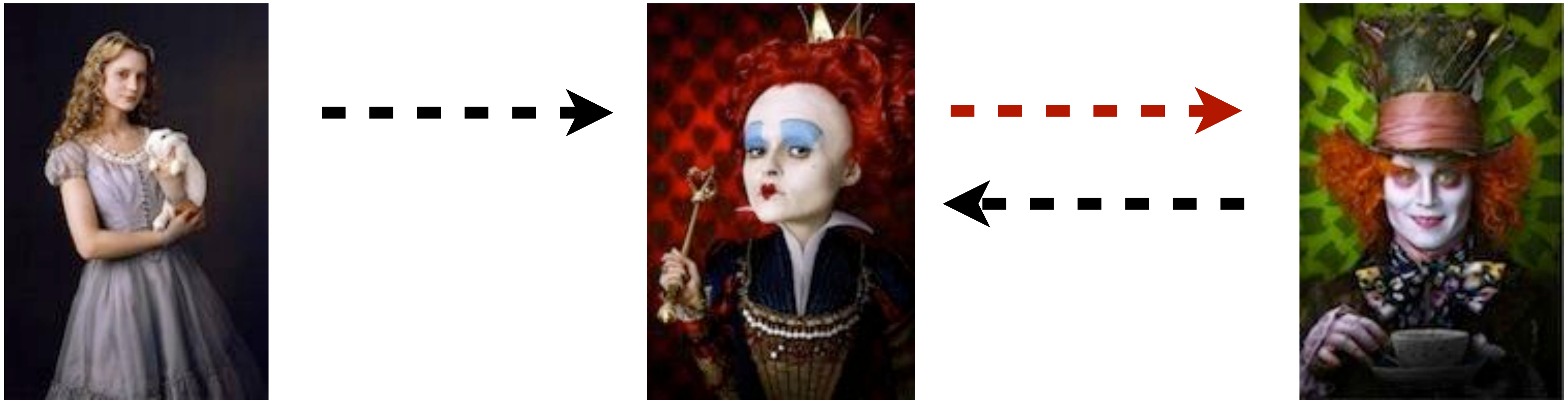
- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M\rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

The attacker can

- intercept all messages
- transmit or modify messages
- test equality between messages

Symbolic model



Alice | Attacker | Bob

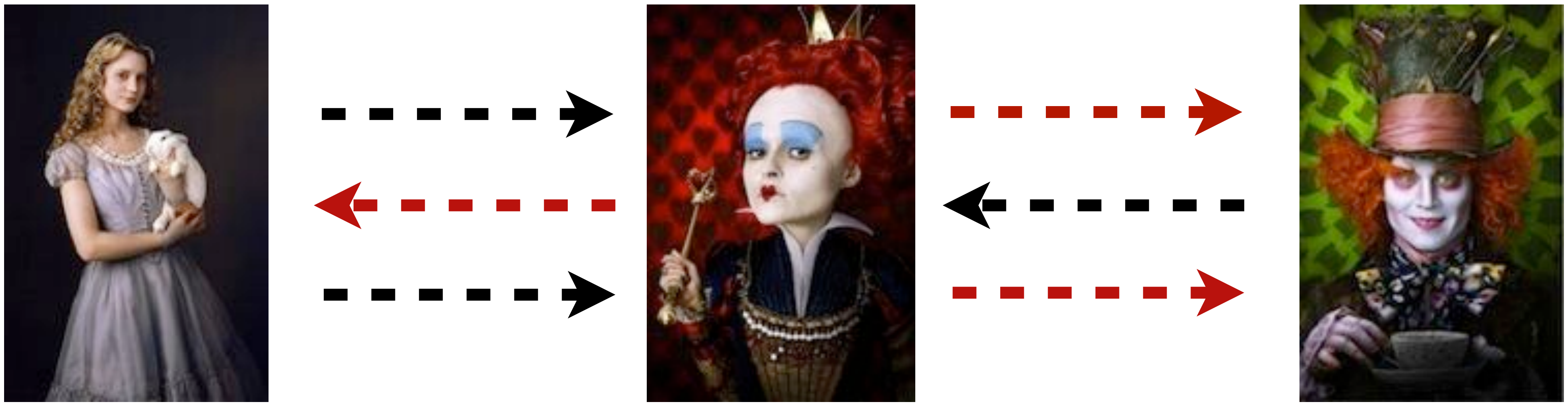
- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M\rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

The attacker can

- intercept all messages
- transmit or modify messages
- test equality between messages

Symbolic model



Alice Attacker Bob

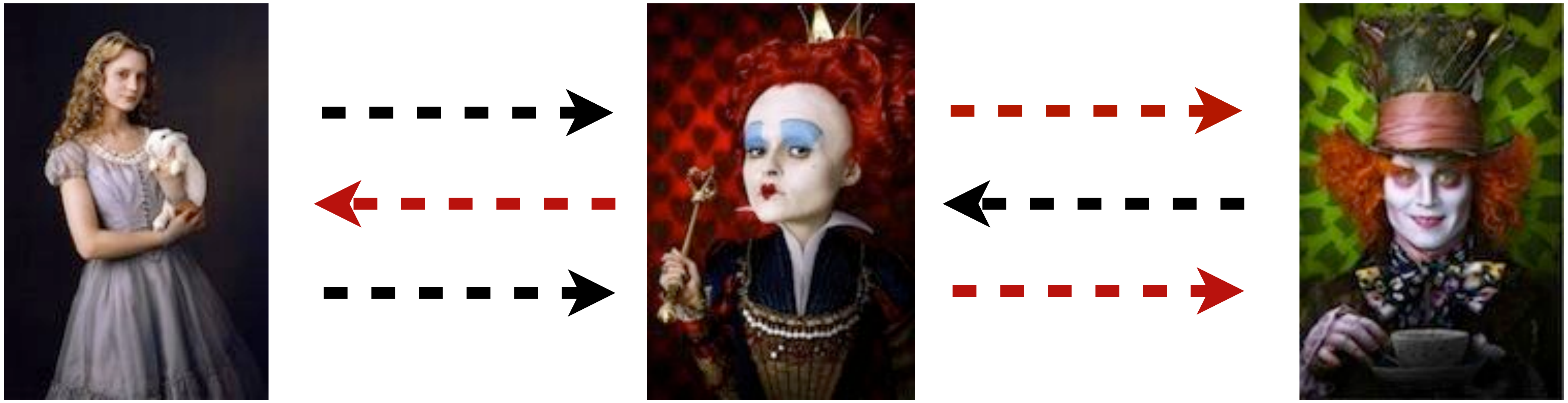
- We assume perfect cryptographic primitives
- Messages are represented by terms

$$\{N\}_{\mathsf{pk}(k)} \qquad \langle N, M \rangle \qquad \mathsf{adec}(\{N\}_{\mathsf{pk}(k)}, k)$$

The attacker can

- intercept all messages
- transmit or modify messages
- test equality between messages

Symbolic model



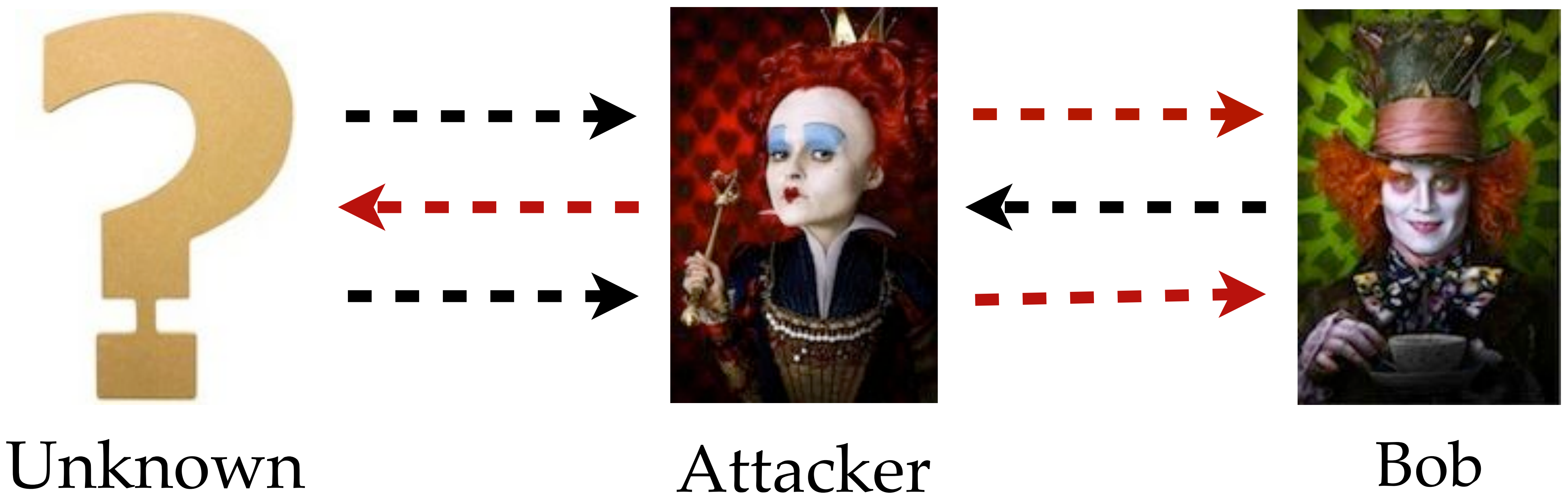
Alice | Attacker | Bob

Security properties:

- Reachability properties
- Equivalence properties

Security properties

Equivalence properties: anonymity

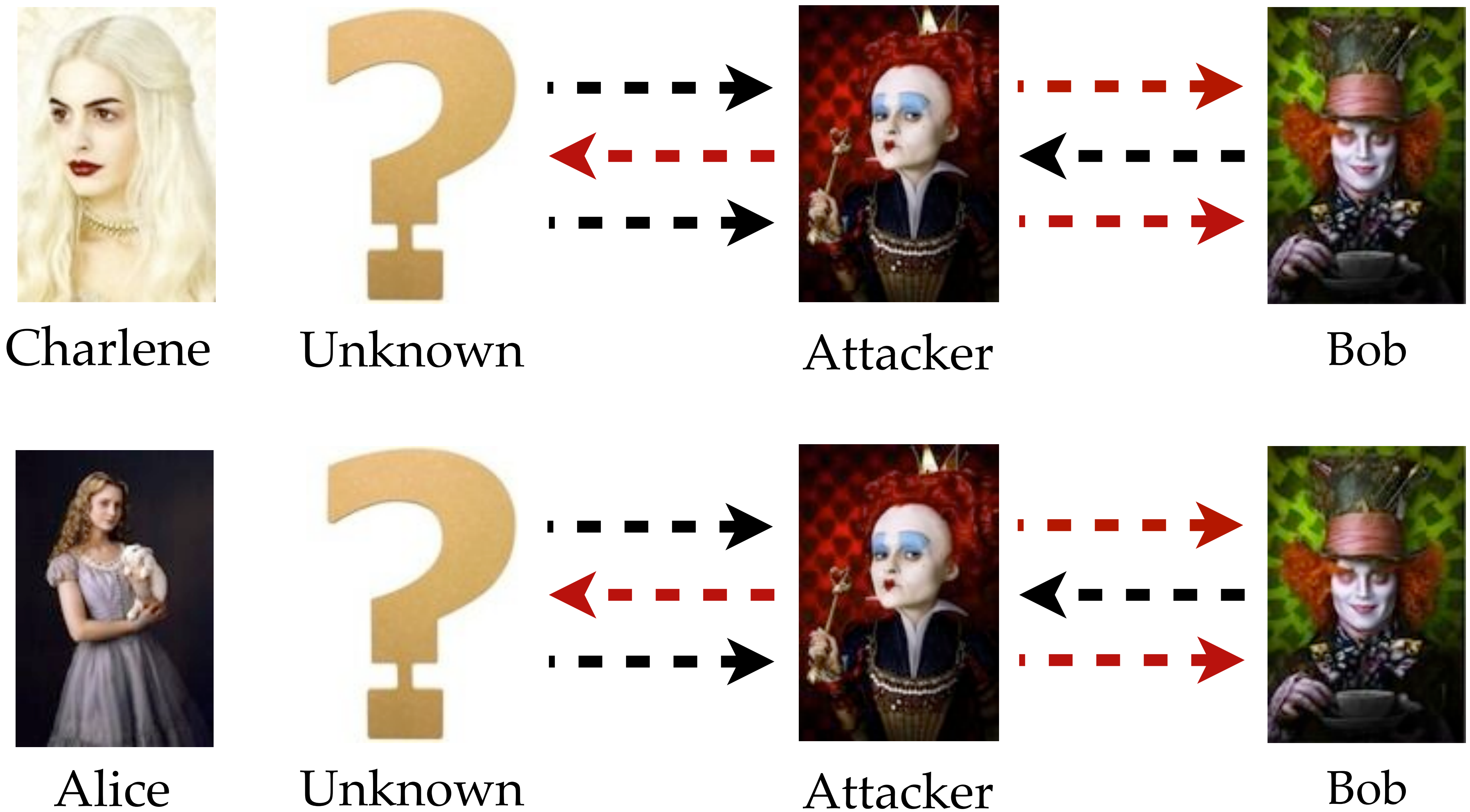


Security properties

Equivalence properties: anonymity

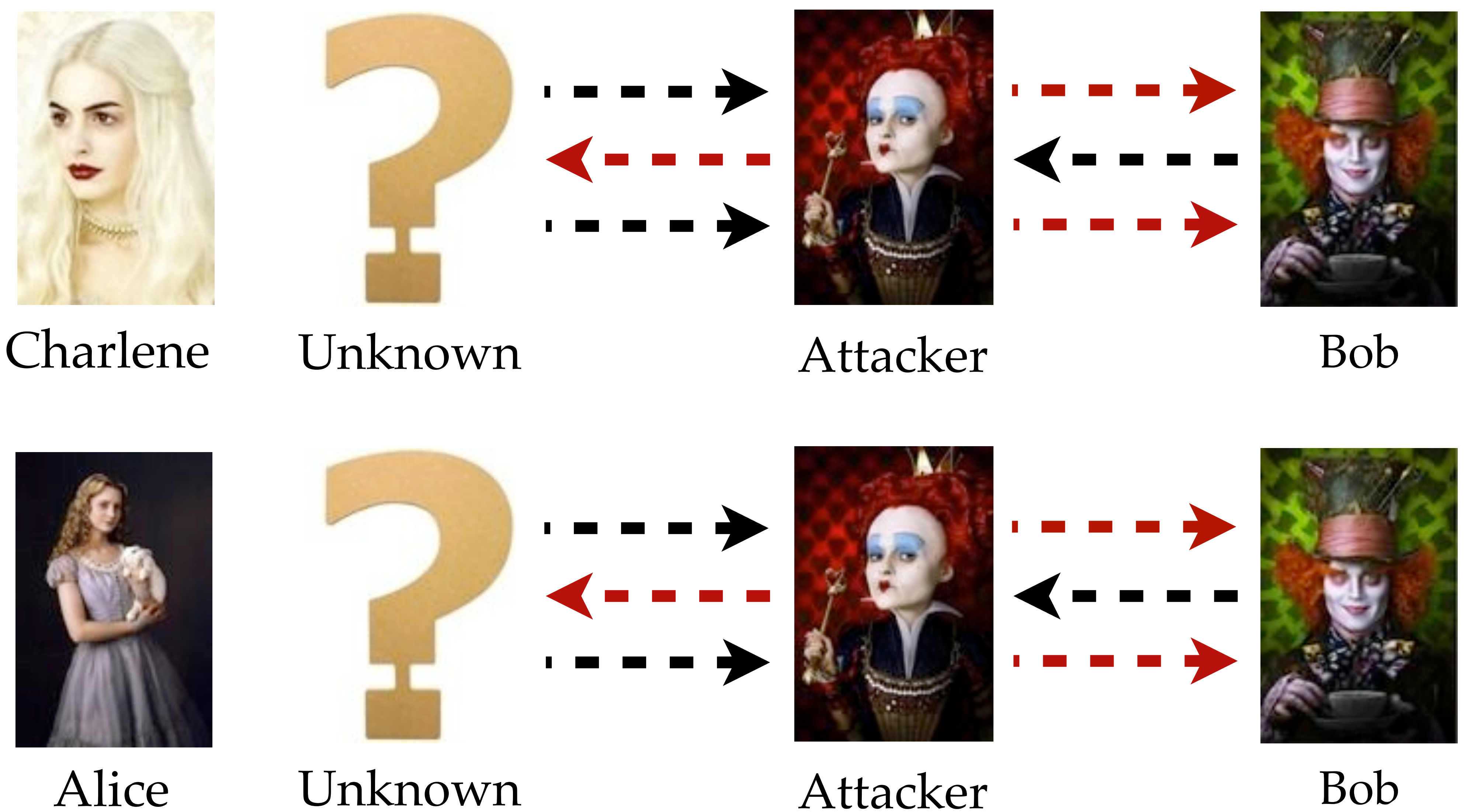
Security properties

Equivalence properties: anonymity



Security properties

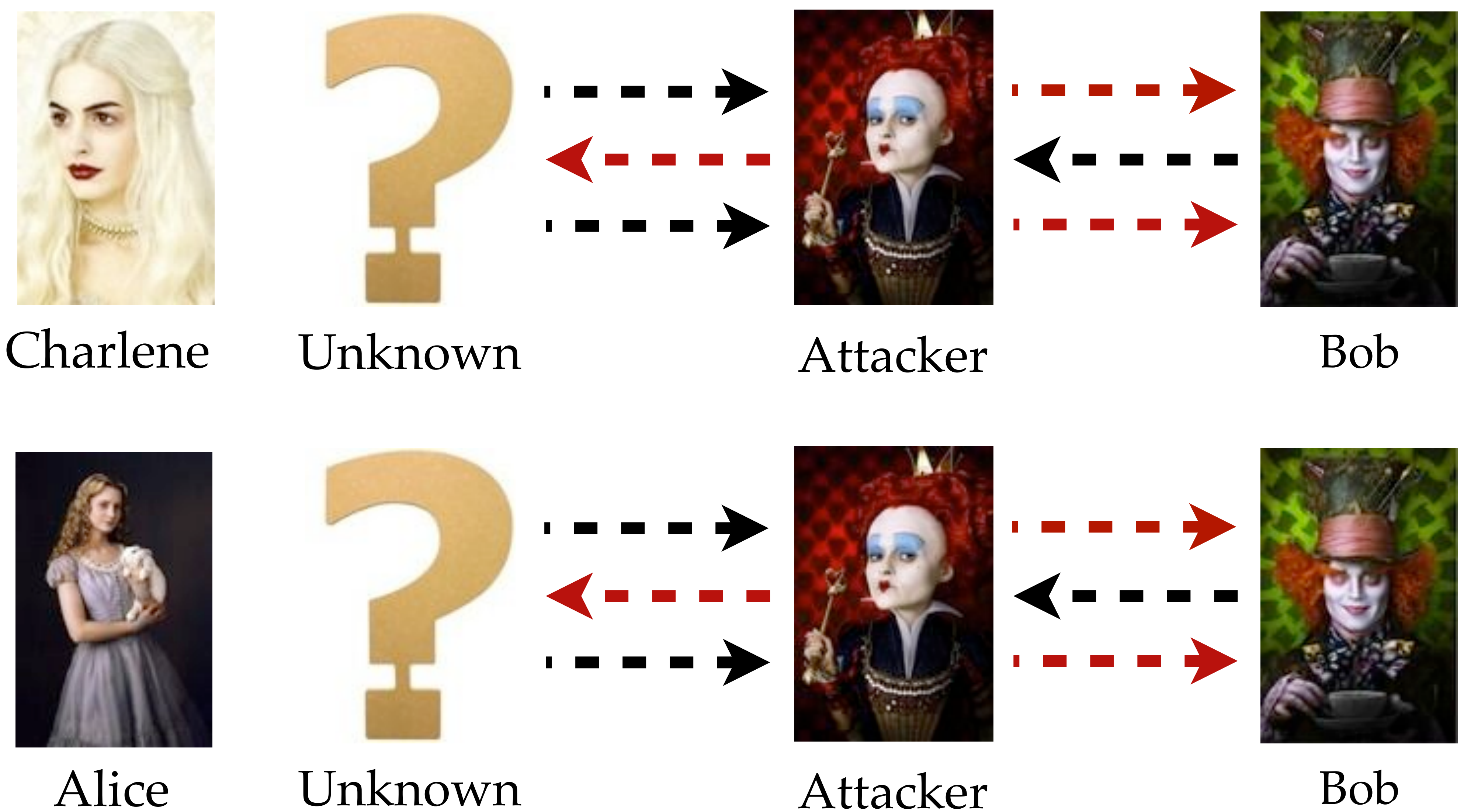
Equivalence properties: anonymity



Can the intruder distinguish the two situations ?

Security properties

Equivalence properties: anonymity



Trace equivalence

Examples

Private authentication protocol

Examples

Private authentication protocol

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

Alice

Bob

Examples

Private authentication protocol

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

Alice

$\mathsf{pk}(k_A)?$

Bob

Examples

Private authentication protocol

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

$\mathsf{pk}(k_A)?$

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

Alice

Bob

Examples

Private authentication protocol

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

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

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

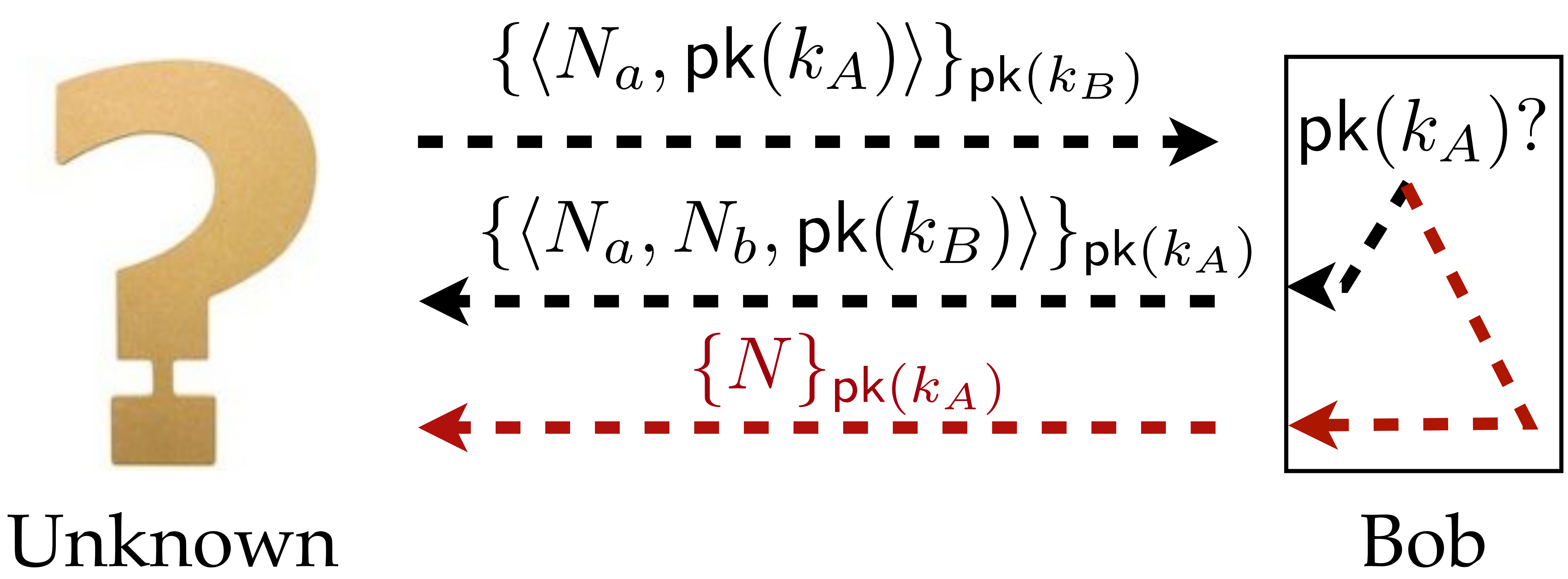
$\mathsf{pk}(k_A)?$

Alice

Bob

Examples

Private authentication protocol



Automatic tools

- For reachability properties

  Avispa, CSP/FDR, ProVerif, Scyther, Maude-NPA, ...

Automatic tools

- For reachability properties

  Avispa, CSP/FDR, ProVerif, Scyther, Maude-NPA, ...

- For equivalence properties

  • **ProVerif:** Bruno Blanchet. *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules.*
  • **SPEC:** Alwen Tiu and Jeremy E. Dawson. *Automating open bisimulation checking for the spi calculus.*
  • **AKiSs:** Ştefan Ciobâcă. *Automated Verification of Security Protocols with Applications to Electronic Voting.*

Automatic tools

- For reachability properties

  Avispa, CSP/FDR, ProVerif, Scyther, Maude-NPA, ...

- For equivalence properties

  - **ProVerif:** Bruno Blanchet. *An Efficient Cryptographic Protocol Verifier Based on Prolog Rules.*
  - **SPEC:** Alwen Tiu and Jeremy E. Dawson. *Automating open bisimulation checking for the spi calculus.*
  - **AKiSs:** Ştefan Ciobâcă. *Automated Verification of Security Protocols with Applications to Electronic Voting.*

Do not handle private authentication protocol and e-passport protocol

Outline

1. Proving more equivalence with ProVerif

2. APTE: Decision procedure for trace equivalence

3. Demo Time !

Proverif

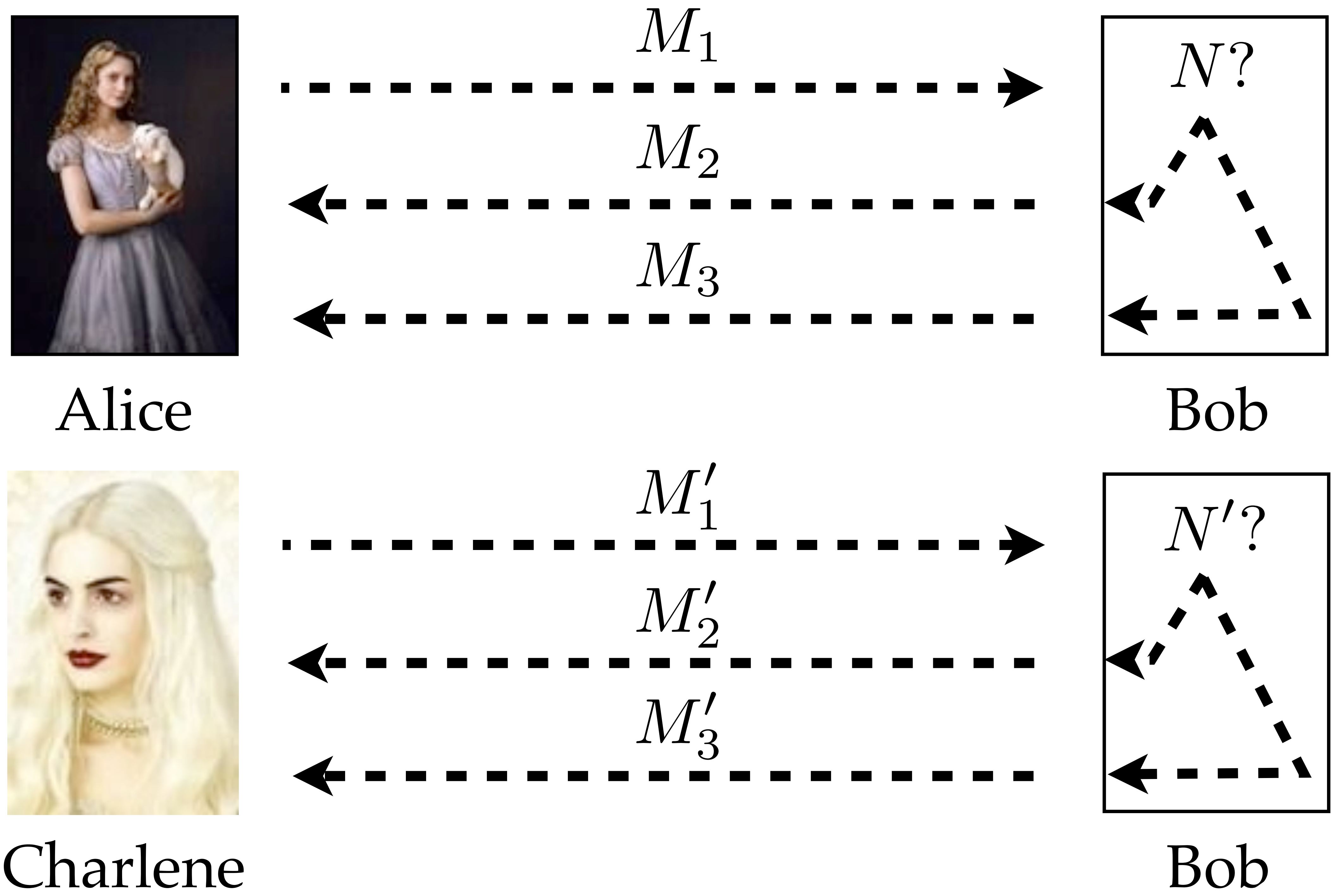
ProVerif was first an analyzer for reachability properties based on Horn clauses.

- Handle reachability and equivalence properties
- Cryptographic primitives described by equational theory and/or rewriting rules
- Handle processes with replication
- Possible false attack
- Does not always terminate

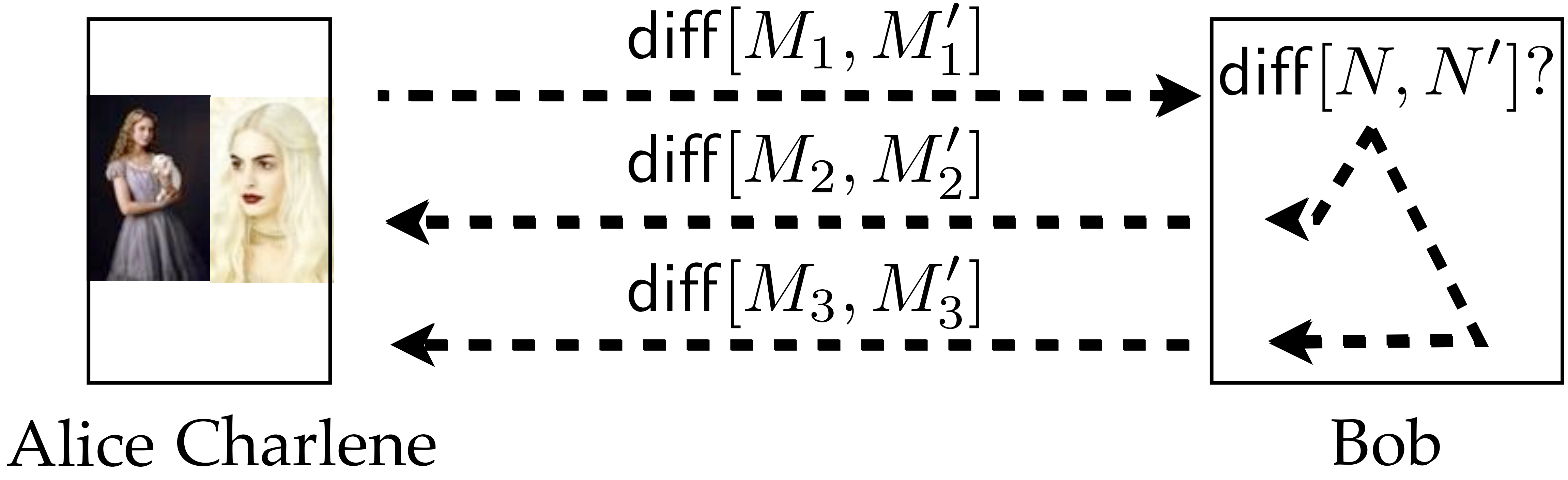
Processes

$$
\begin{aligned}
P, Q := \quad & 0 \\
& \mathsf{in}(c, x); P \\
& \mathsf{out}(c, M); P \\
& P \mid Q \\
& !\, P \\
& \mathsf{new}\ a; P \\
& \mathsf{let}\ x = D\ \mathsf{in}\ P\ \mathsf{else}\ Q
\end{aligned}
$$

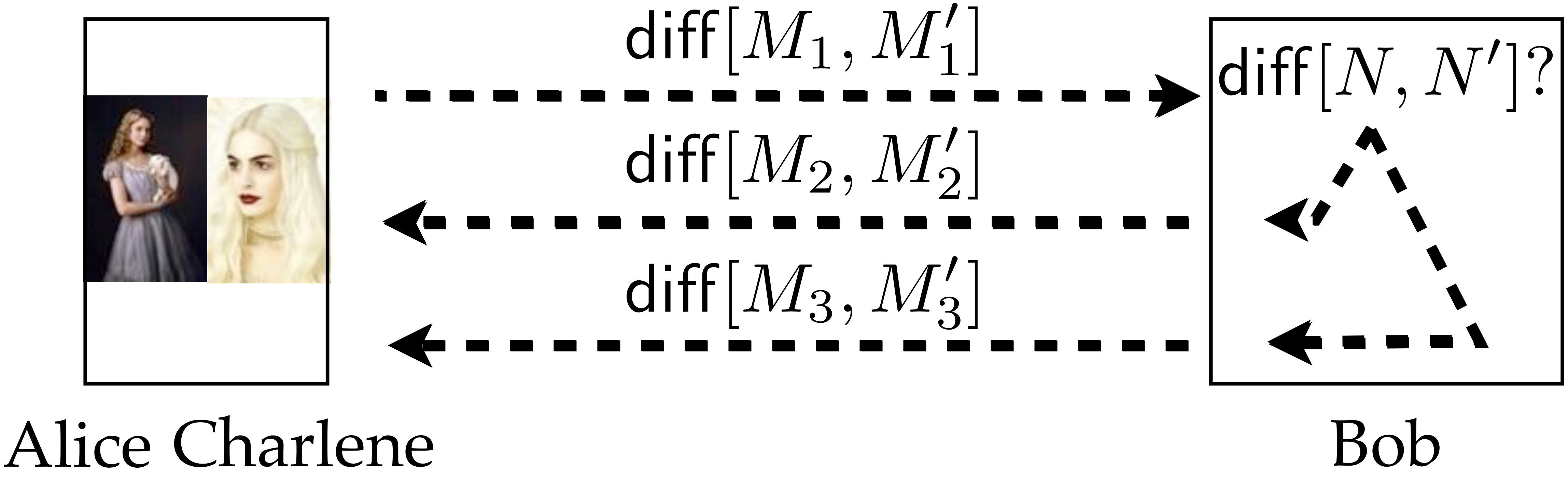
Biprocesses



Biprocesses



Biprocesses



Equivalence too strong: possible false attack

Motivation

The private authentication protocol

Alice

Attacker

Bob

Charlene

Attacker

Bob

Motivation

The private authentication protocol

Alice

Bob

Charlene

Bob

Motivation

The private authentication protocol

Alice

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

$\{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$

Bob

Charlene

Bob

Motivation

The private authentication protocol

Alice

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

$\{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$

$\mathsf{pk}(k_A) = y$

Bob

Charlene

Bob

Motivation

The private authentication protocol

Alice

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

$\{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$

$\mathsf{pk}(k_A) = y$

$\{\langle x, N_b, \mathsf{pk}(k_B)\rangle\}_y$

Bob

Charlene

Bob

Motivation

The private authentication protocol

Alice

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

$\{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$ →

$\mathsf{pk}(k_A) = y$

← $\{\langle x, N_b, \mathsf{pk}(k_B)\rangle\}_y$

← $\{N\}_{\mathsf{pk}(k_A)}$

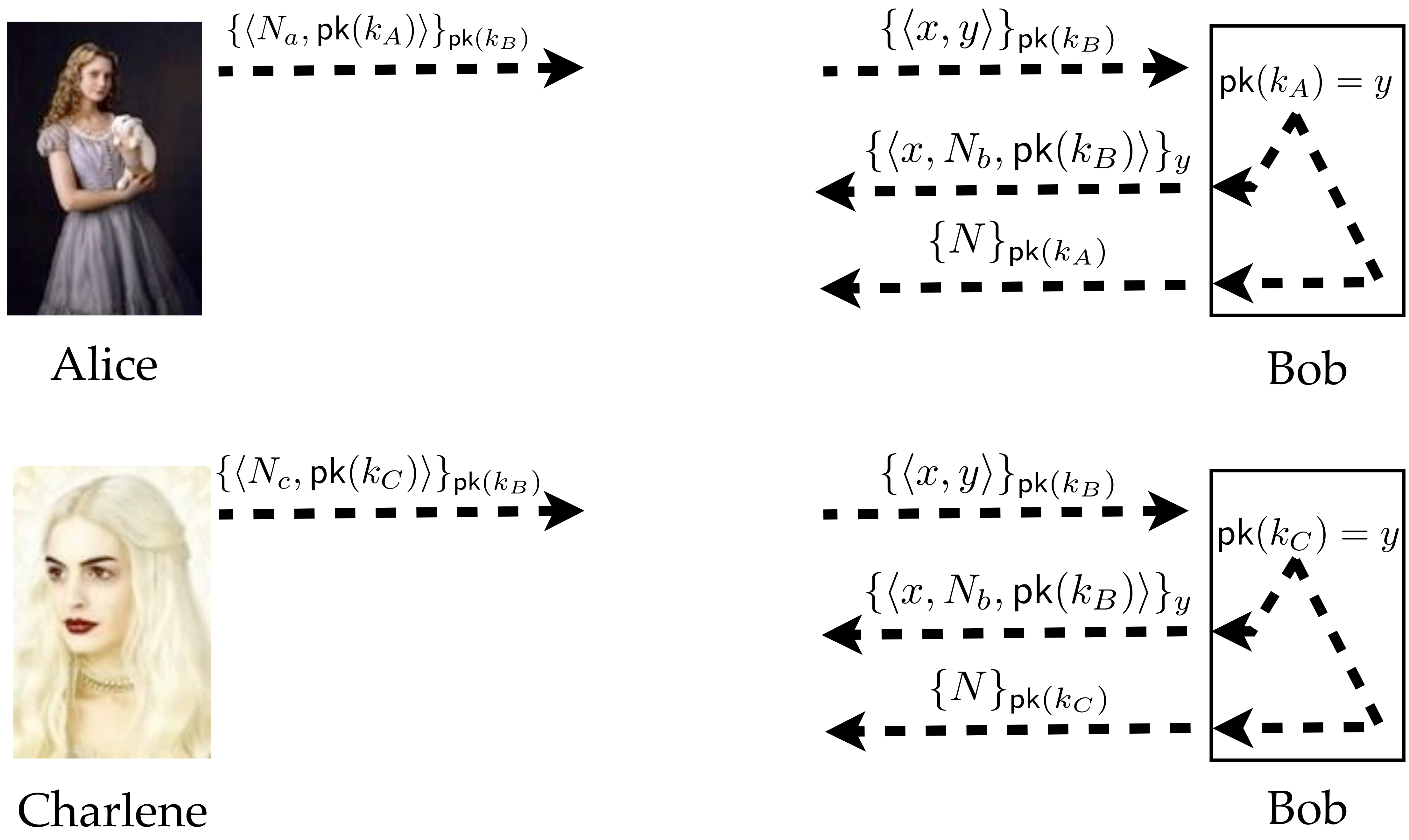
Bob

Charlene

Bob

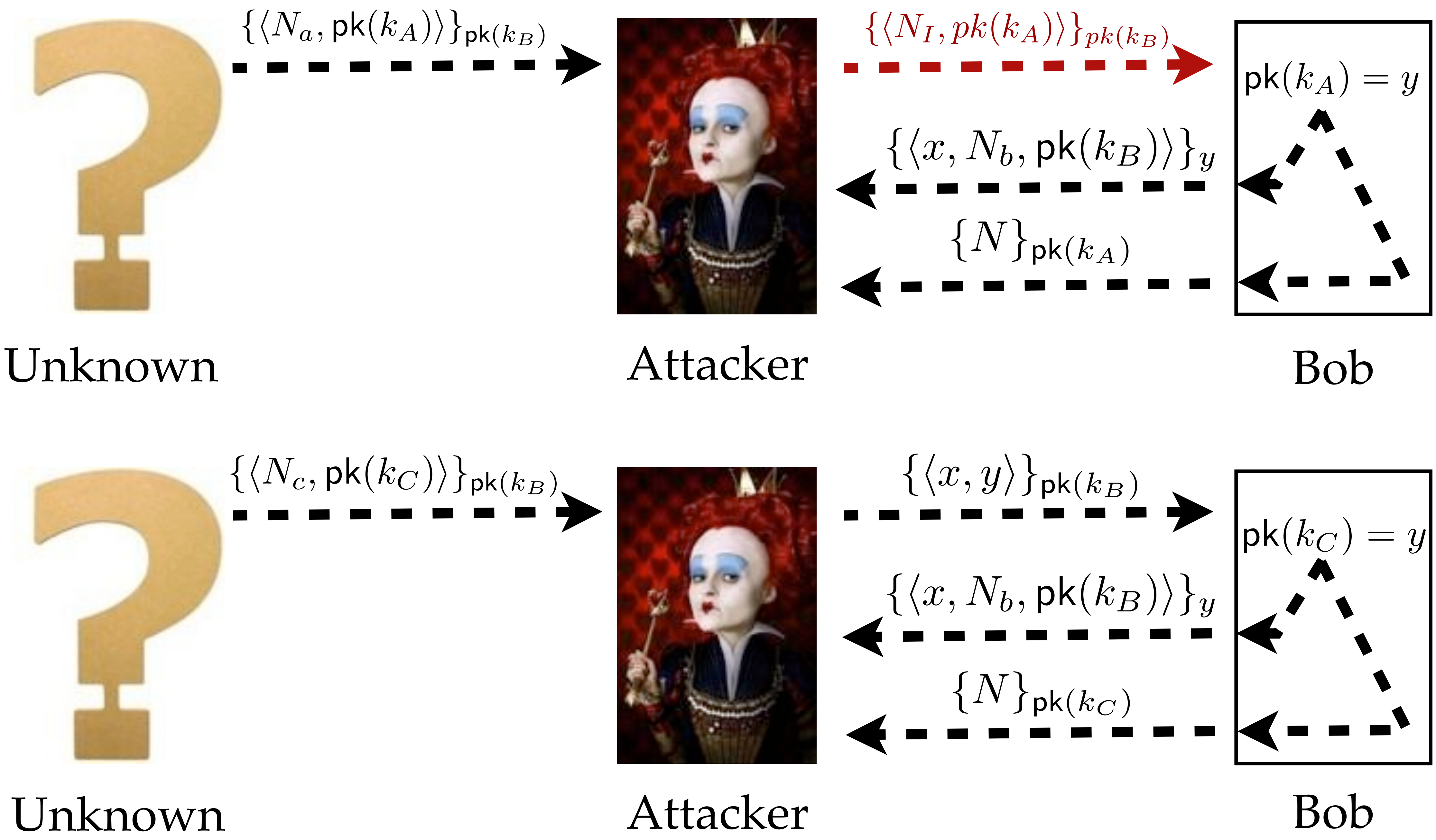
Motivation

The private authentication protocol



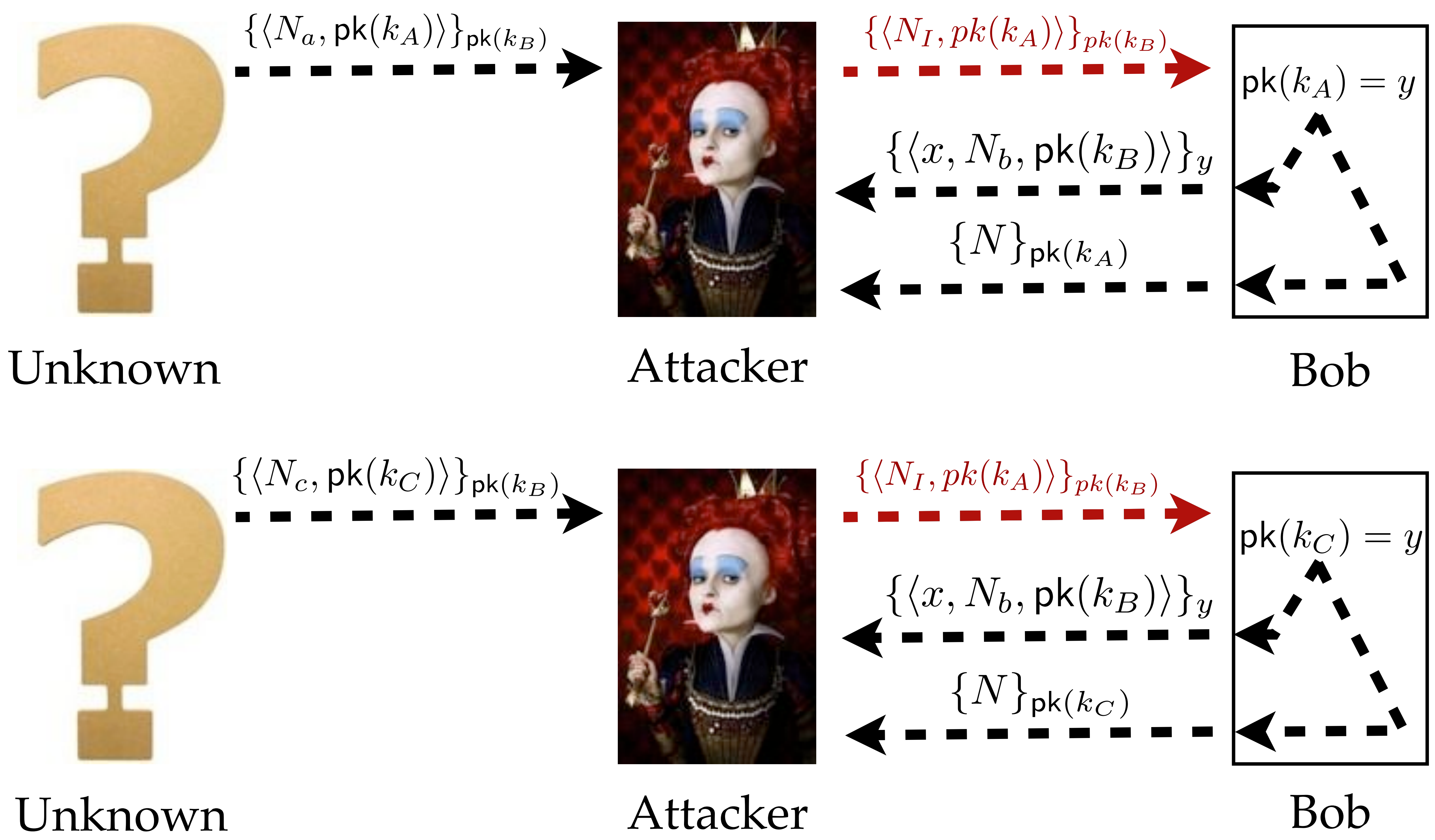
Motivation

The private authentication protocol



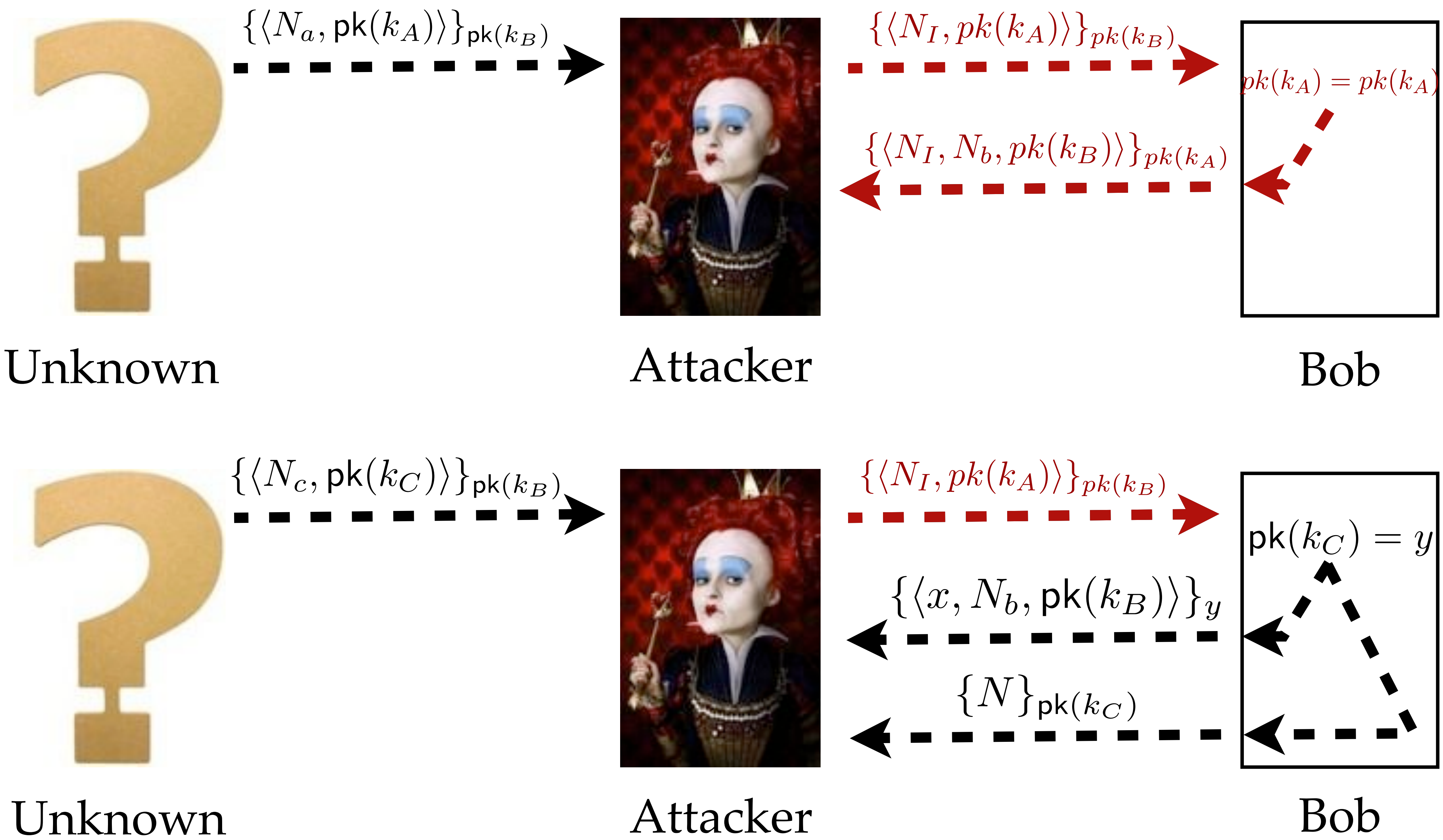
Motivation

The private authentication protocol



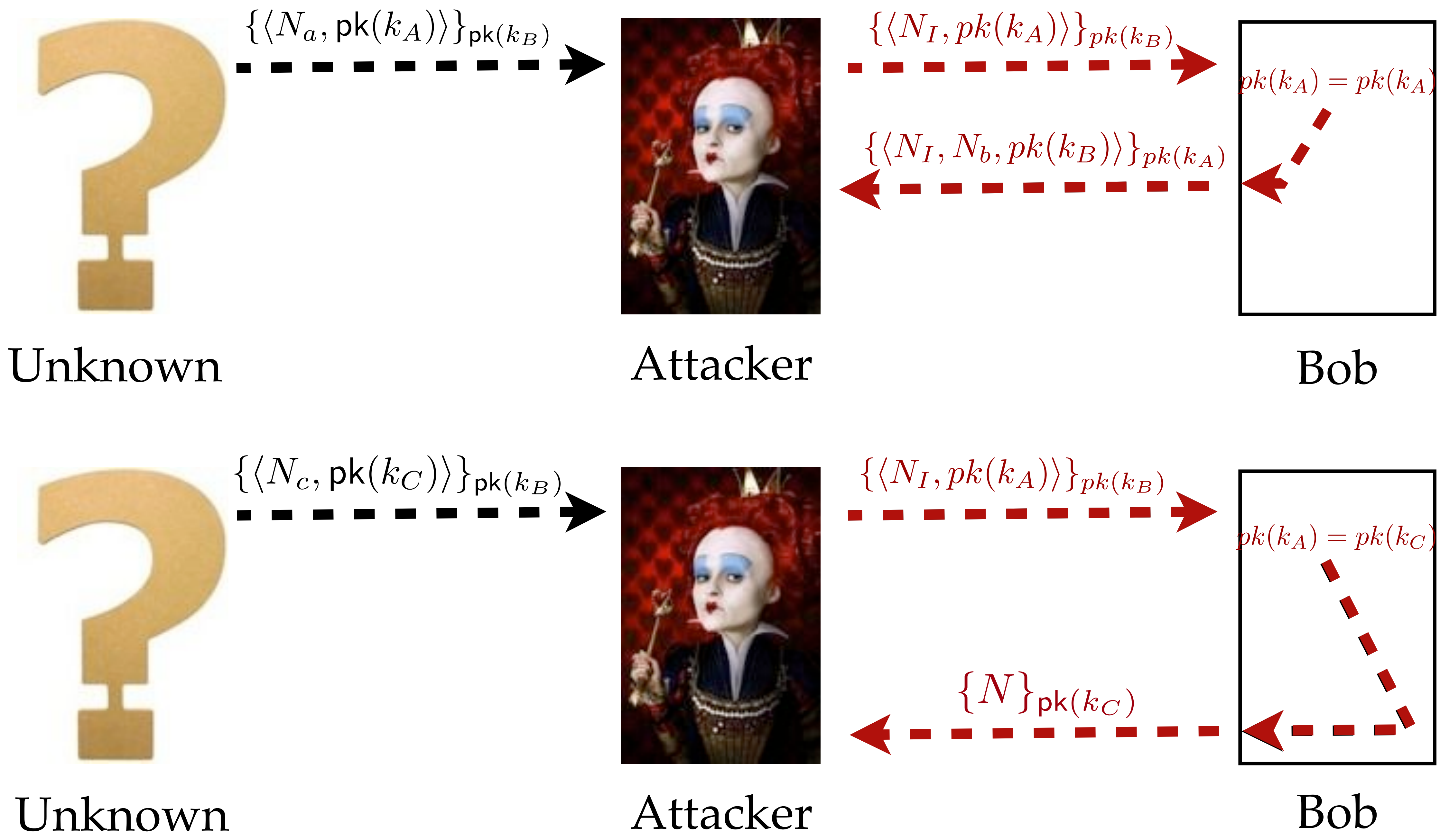
Motivation

The private authentication protocol



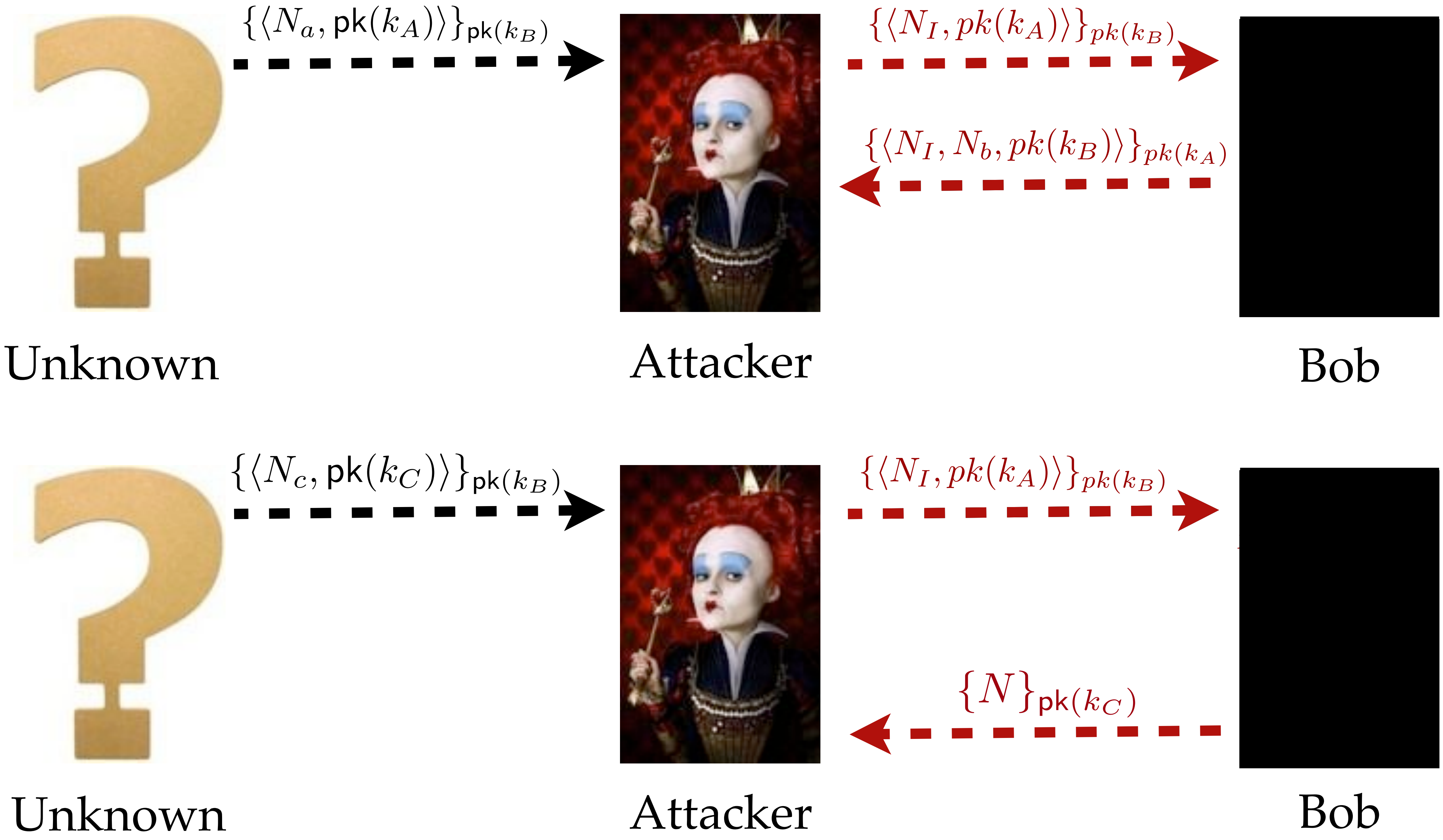
Motivation

The private authentication protocol



Motivation

The private authentication protocol



Contribution

Introduction of destructors with tests between terms

Contribution

Introduction of destructors with tests between terms

The *If-then-else* destructor:

$$\mathsf{ifthenelse}(x, x, z, t) \rightarrow z$$

$$\mathsf{ifthenelse}(x, y, z, t) \rightarrow t \quad \text{with} \quad x \neq y$$

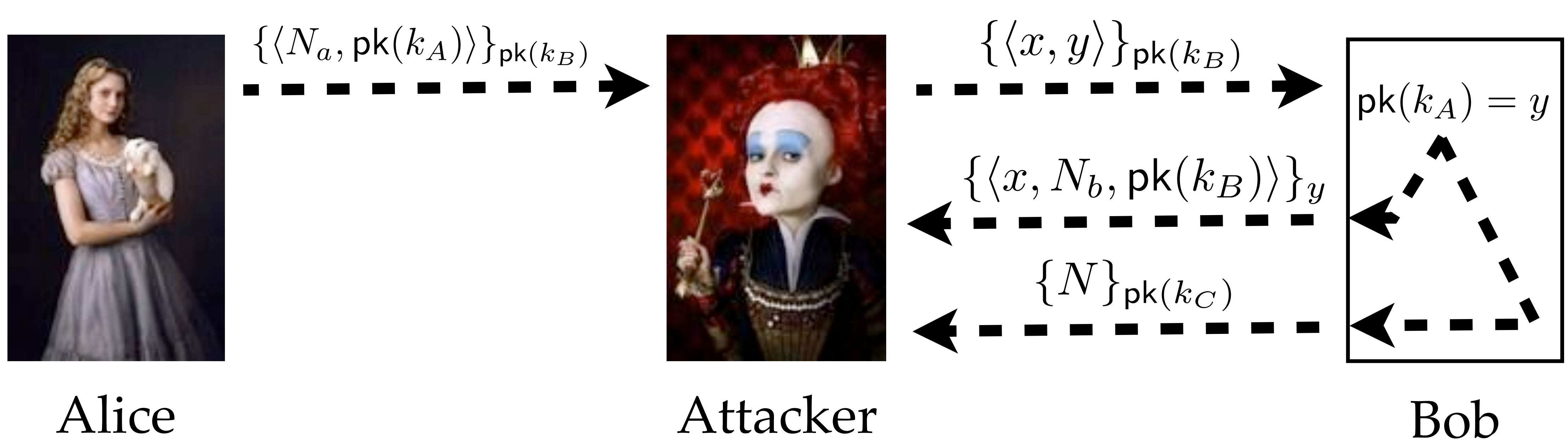
Contribution

Introduction of destructors with tests between terms

The *If-then-else* destructor:

$$\mathsf{ifthenelse}(x, x, z, t) \to z$$

$$\mathsf{ifthenelse}(x, y, z, t) \to t \quad \text{with} \quad x \neq y$$



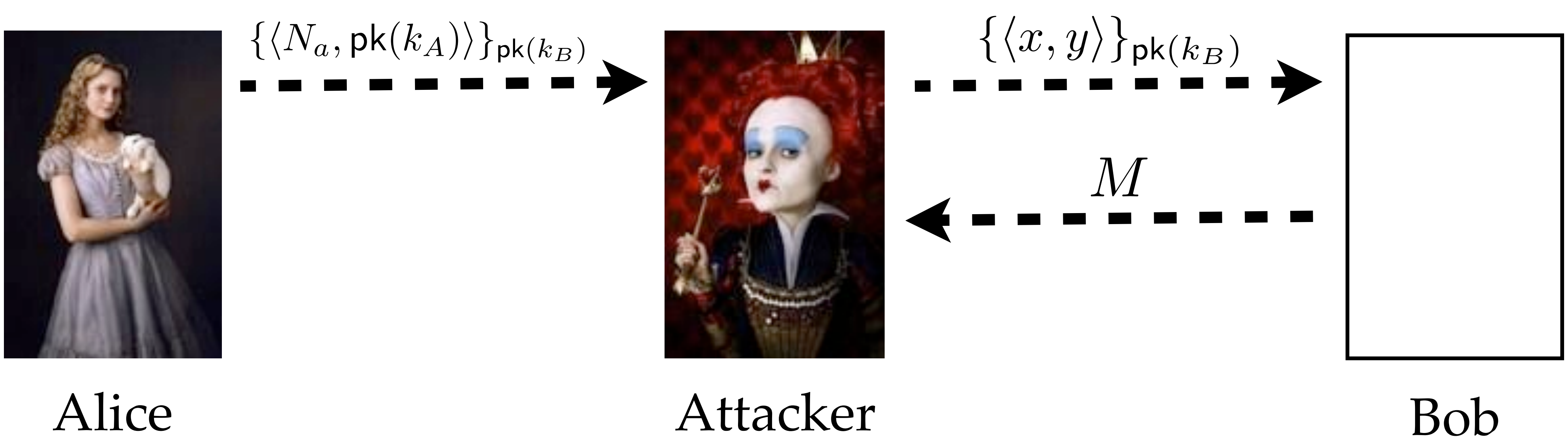
Contribution

Introduction of destructors with tests between terms

The *If-then-else* destructor:

$$\mathsf{ifthenelse}(x, x, z, t) \rightarrow z$$

$$\mathsf{ifthenelse}(x, y, z, t) \rightarrow t \quad \text{with} \quad x \neq y$$



$$M = \mathsf{ifthenelse}(y, \mathsf{pk}(k_A), \{x, N_b, \mathsf{pk}(k_B)\}_y, \{N\}_{\mathsf{pk}(k_A)})$$

Contribution

Introduction of destructors with tests between terms

The *If-then-else* destructor:

$$\mathsf{ifthenelse}(x, x, z, t) \rightarrow z$$

$$\mathsf{ifthenelse}(x, y, z, t) \rightarrow t \quad \text{with} \quad x \neq y$$

Automatic transformation: *simpl*

For all processes P, $simpl(P) \approx P$

Implementation

Beta release:

ProVerif version 1.87beta

http://prosecco.gforge.inria.fr/personal/bblanche/proverif/

Content:

- Rewrite rules with tests
- Automatic transformation of biprocesses
- Equivalence between processes with different control structures

Results:

- Prove anonymity for private authentication protocol (unbounded number of sessions)

Outline

1. Proving more equivalence with ProVerif
2. APTE: Decision procedure for trace equivalence
3. Demo Time !

Constraint systems

One constraint system = several traces

Alice

Attacker

Bob

$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I$

Constraint systems

One constraint system = several traces

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

Alice

Attacker

Bob

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

Constraint systems

One constraint system = several traces

Alice

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

Attacker

$\{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$

Bob

$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)} \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$$

Constraint systems

One constraint system = several traces

Alice

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

Attacker

$\{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$

$y = \mathsf{pk}(k_A)$

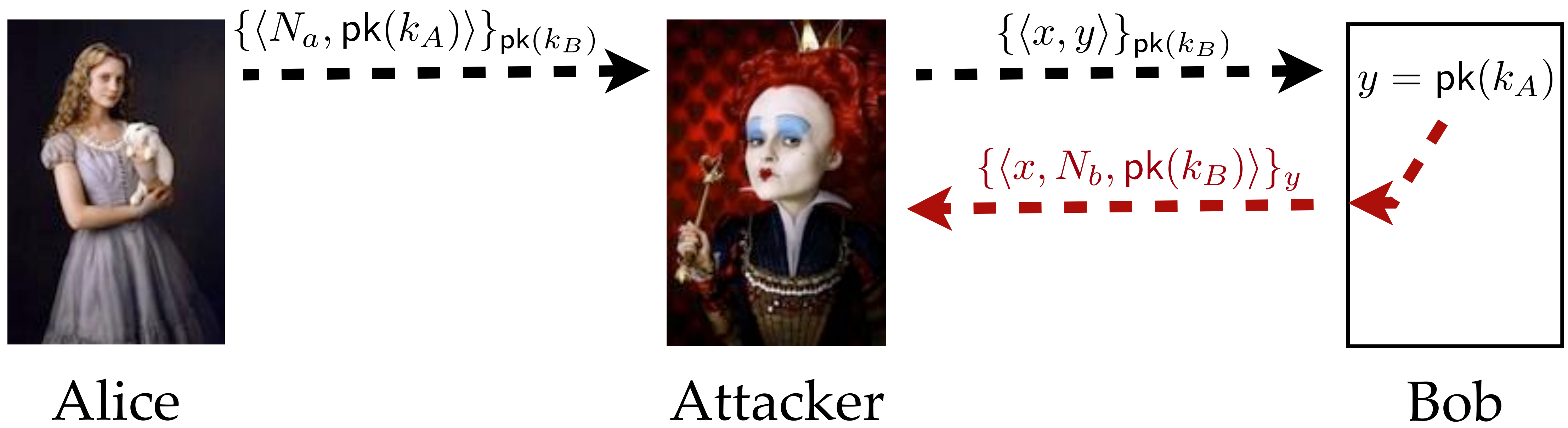
Bob

$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)} \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$$

$$y = \mathsf{pk}(k_A)$$

Constraint systems

One constraint system = several traces



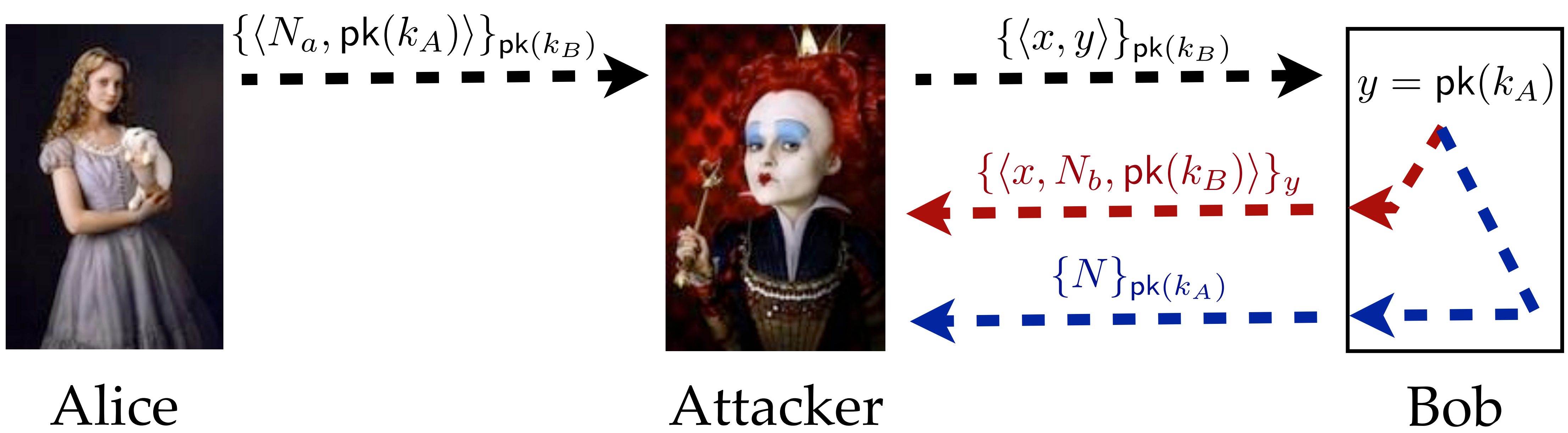
$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)} \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$$

$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)}, \{\langle x, N_b, \mathsf{pk}(k_B)\rangle\}_y$$

$$y = \mathsf{pk}(k_A)$$

Constraint systems

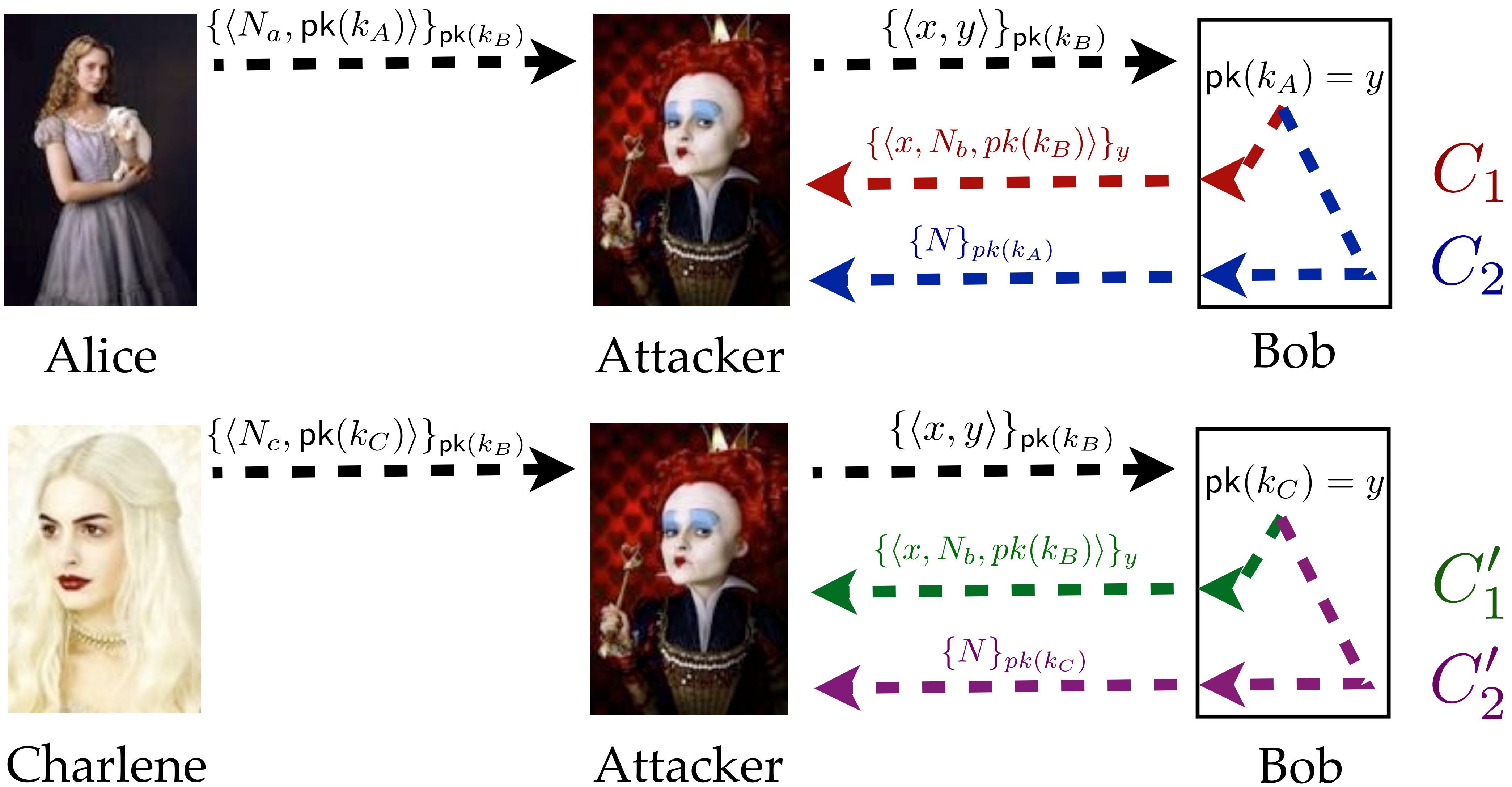
One constraint system = several traces



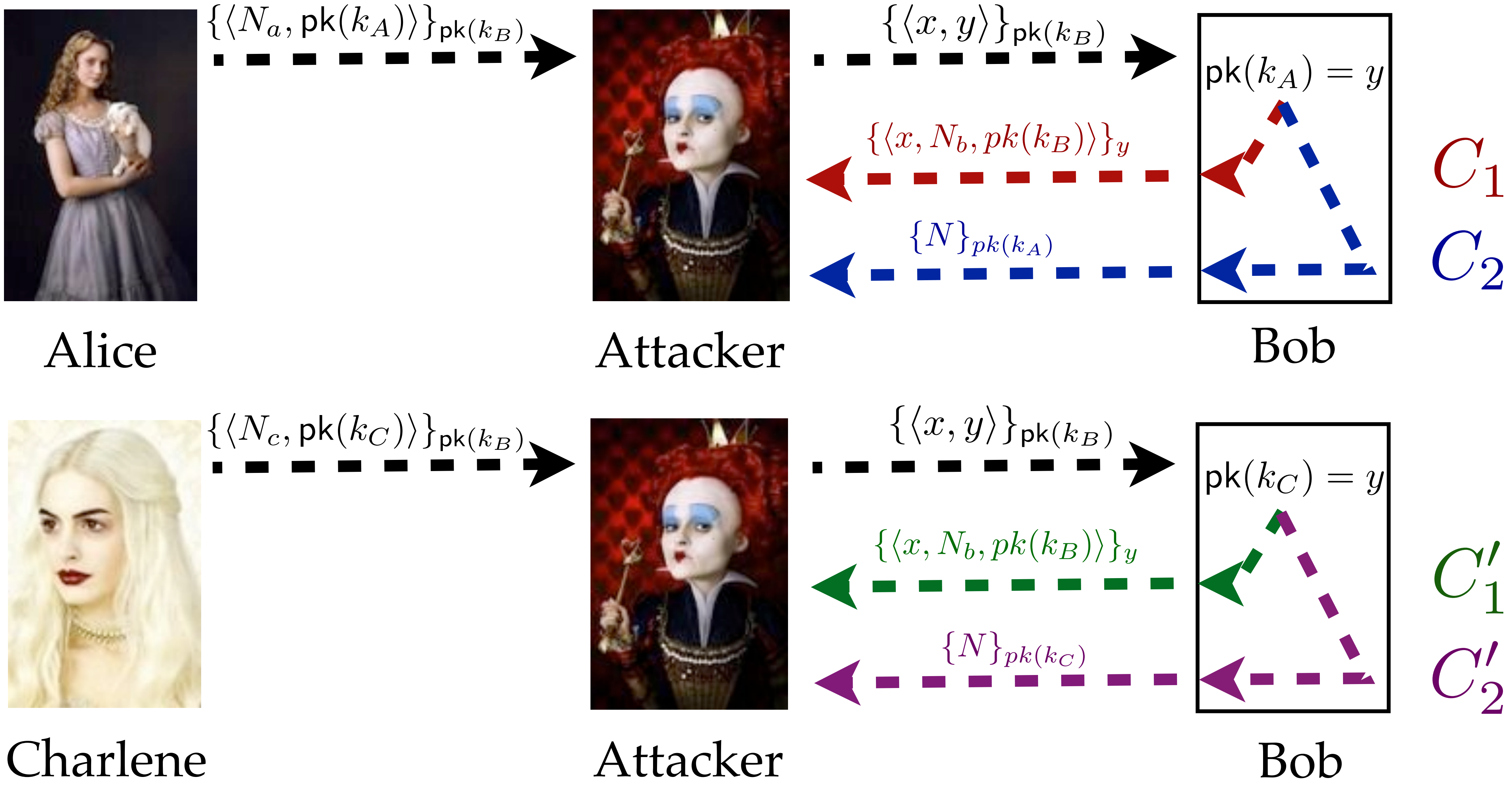
$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)} \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$$
$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)}, \{\langle x, N_b, \mathsf{pk}(k_B)\rangle\}_y$$
$$y = \mathsf{pk}(k_A)$$

$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)} \vdash \{\langle x, y\rangle\}_{\mathsf{pk}(k_B)}$$
$$\mathsf{pk}(k_A), \mathsf{pk}(k_B), \mathsf{pk}(k_C), N_I, \{\langle N_a, \mathsf{pk}(k_A)\rangle\}_{\mathsf{pk}(k_B)}, \{N\}_{\mathsf{pk}(k_A)}$$
$$y \neq \mathsf{pk}(k_A)$$

Sets of constraint systems

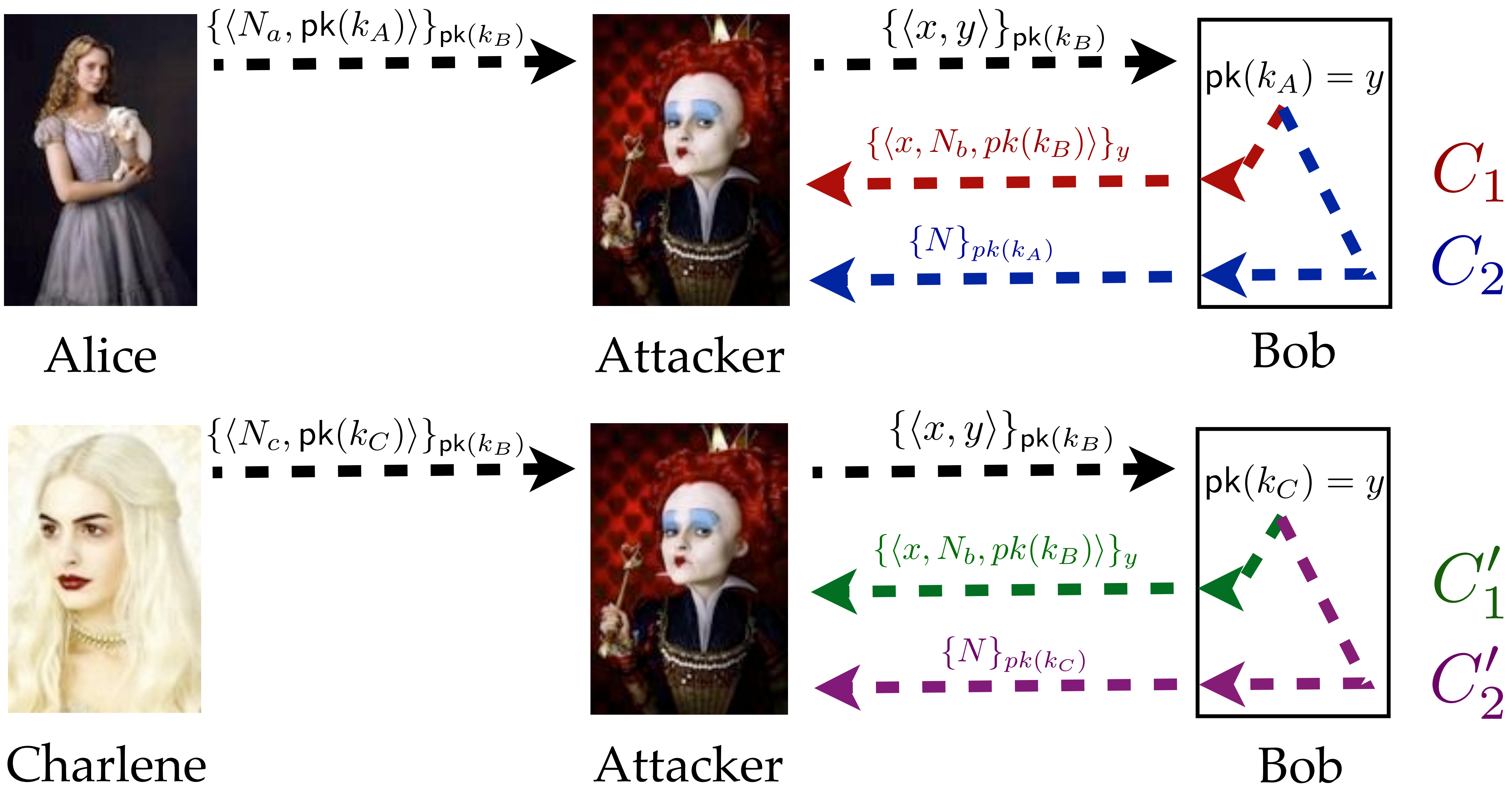


Sets of constraint systems



$$\{C_1;\ C_2\} \approx \{C'_1;\ C'_2\}$$

Sets of constraint systems



Symbolic equivalence between sets of constraint systems

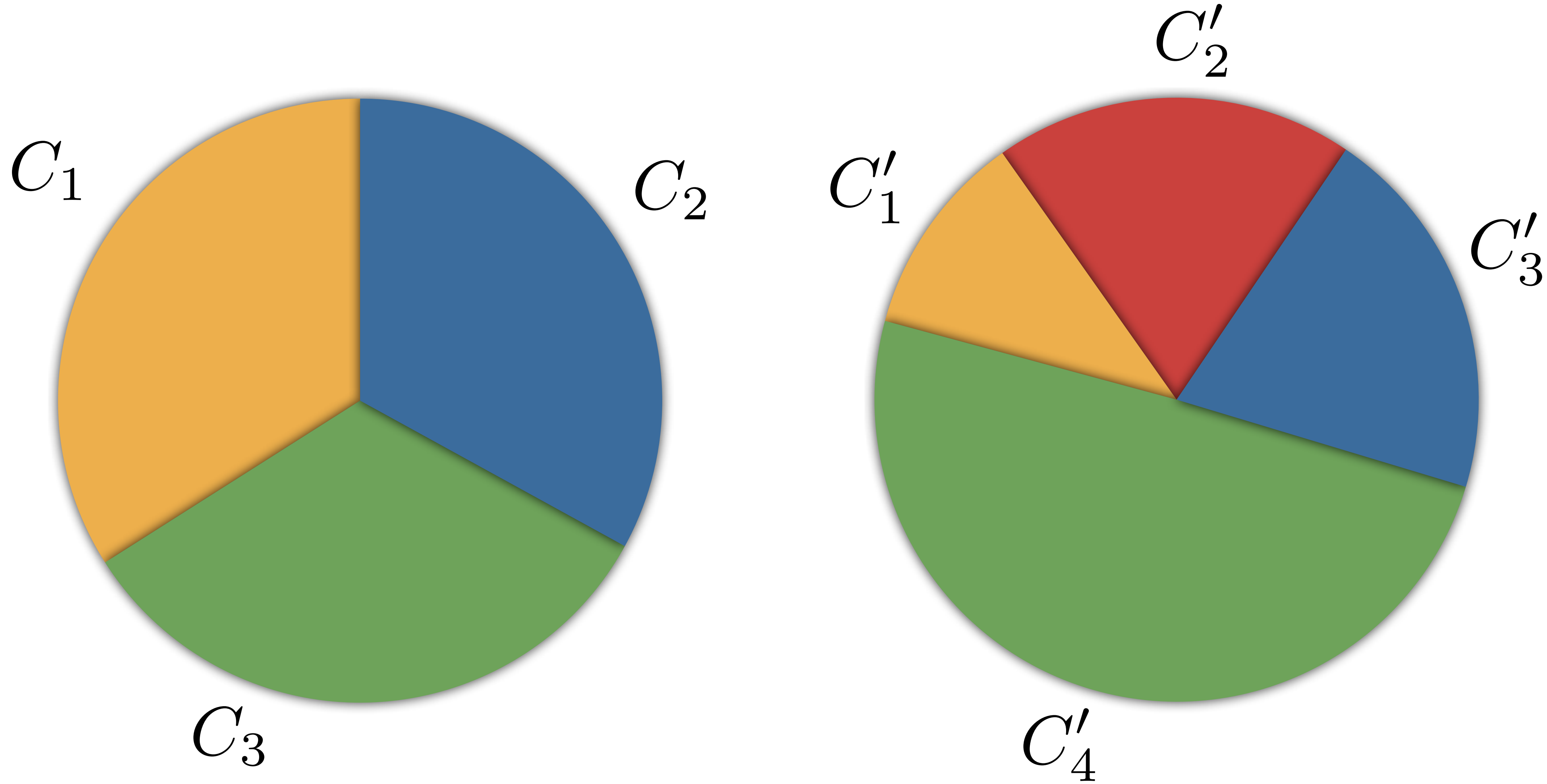
Previous works

1. M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires*. Phd thesis (2007)
2. Y. Chevalier and M. Rusinowitch. *Decidability of equivalence of symbolic derivations*. JAR (2012)
3. A. Tiu and J. E. Dawson. *Automating open bisimulation checking for the spi calculus*. CSF (2010)

- Do not handle set of constraint systems
- Do not handle inequations
- Do not handle non-deterministic processes

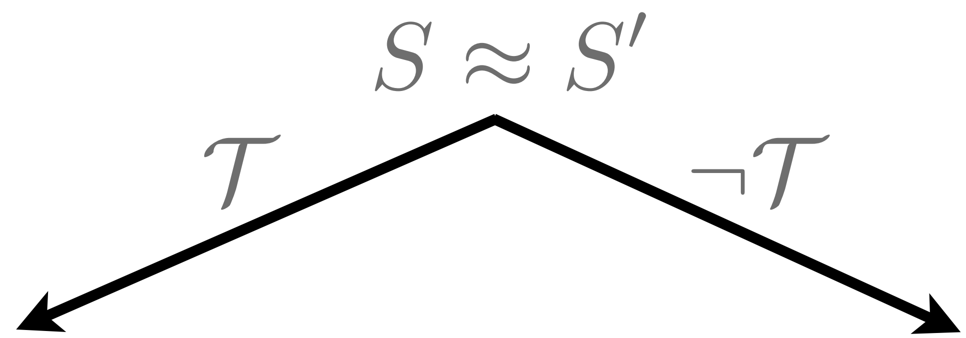
Sets of constraint systems

Why are they necessary ?

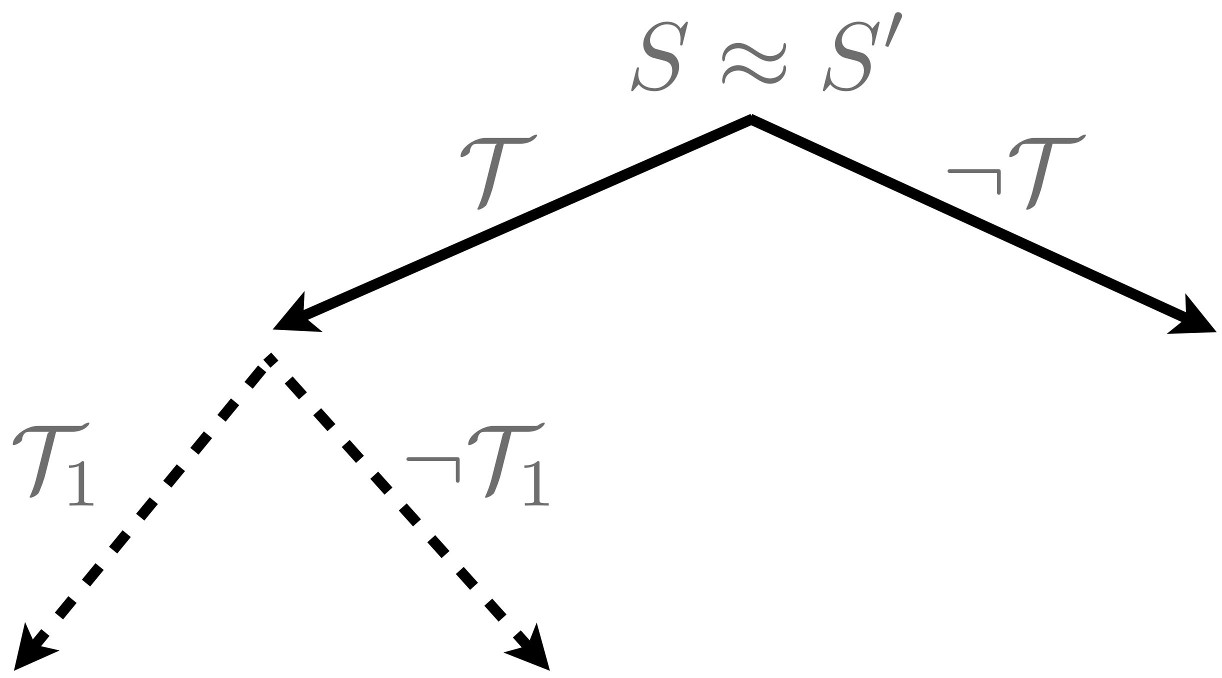


$S = \{C_1; C_2; C_3\}$ $S' = \{C'_1; C'_2; C'_3; C'_4\}$

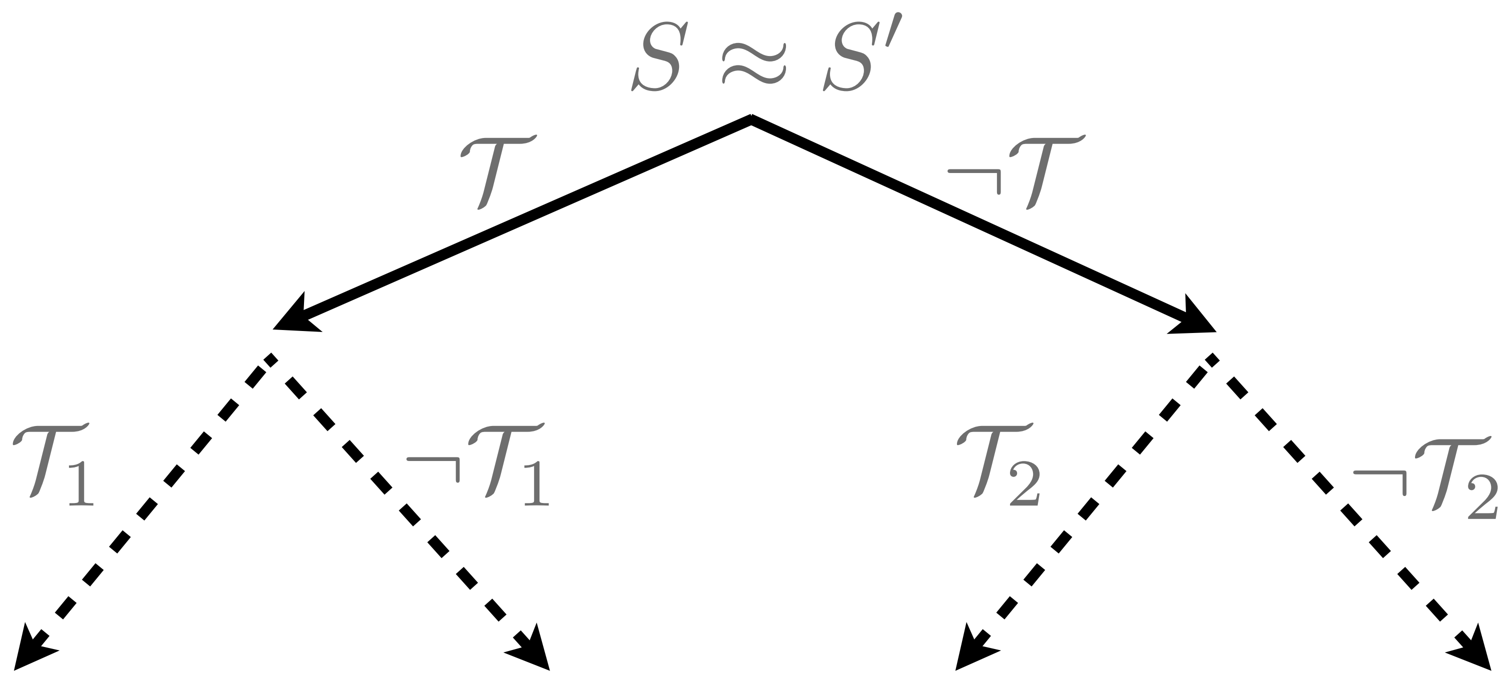
The Algorithm



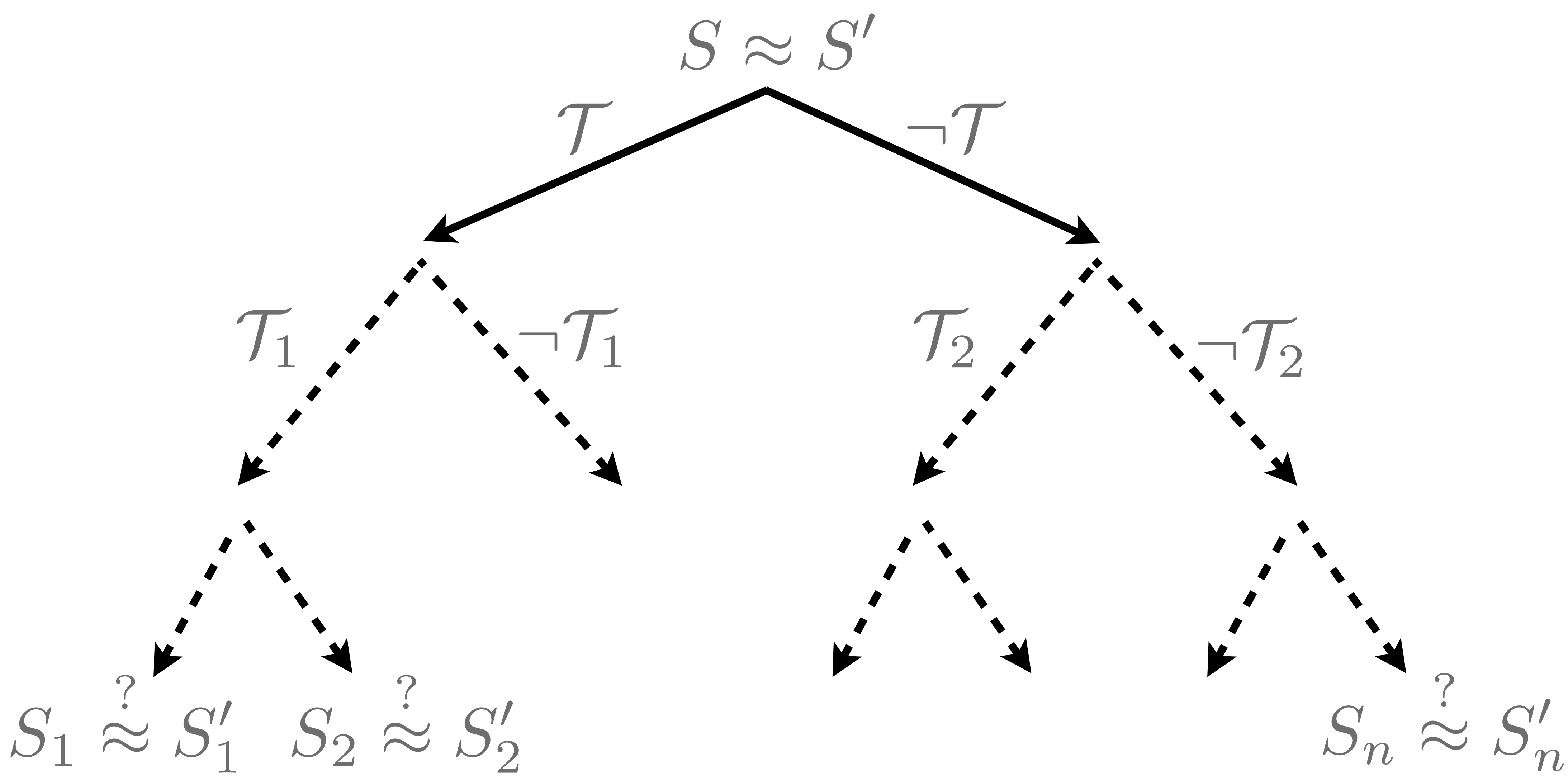
The Algorithm



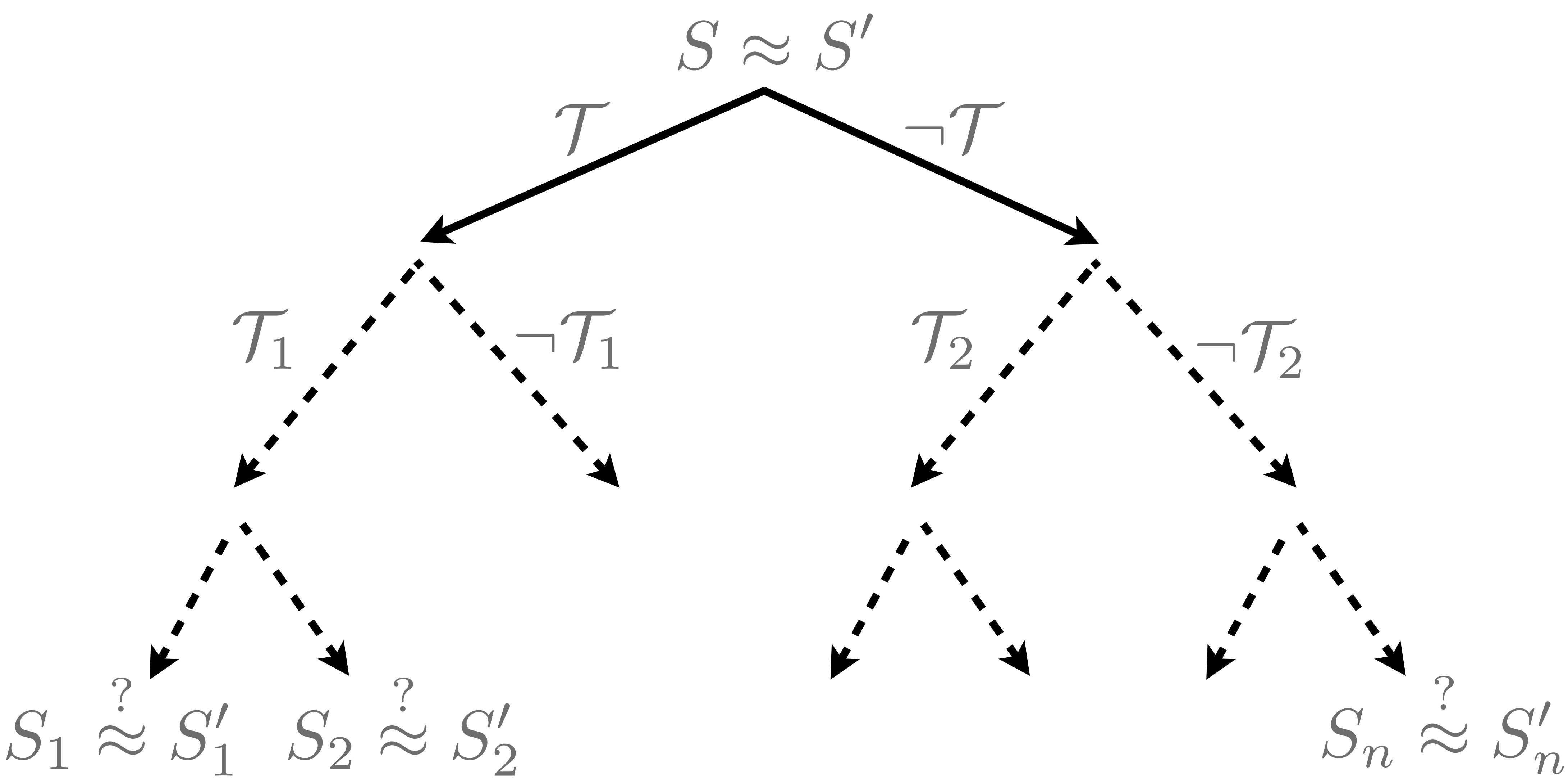
The Algorithm



The Algorithm



The Algorithm



The symbolic equivalence is syntactically decided on each leaf

Results

Decision procedure for proving trace equivalence for bounded number of sessions.

Class of accepted processes:

- Non-deterministic (e.g. private channel) with else-branches
- Classic cryptographic primitives (symmetric and asymmetric encryption, signature, pairing, hash)

Include:

- E-passport protocols
- Private authentication protocols

Length of messages

Example

Alice

Attacker

Bob

Charlene

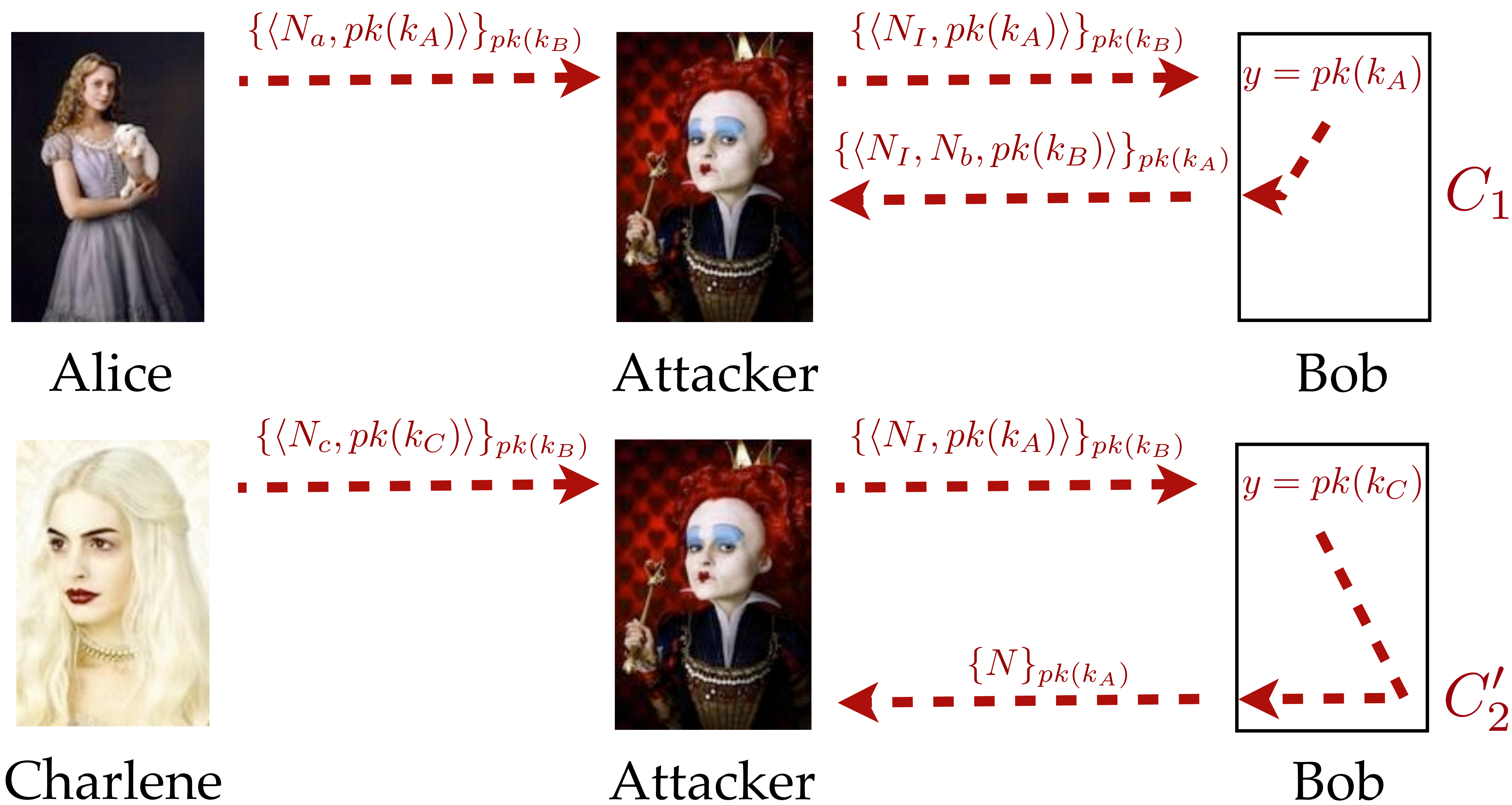
Attacker

$y = pk(k_C)$

Bob

Length of messages

Example



Length of messages

Linear length functions

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

$$\langle x, y \rangle \qquad \ell_{\langle\ \rangle}(x, y) = \alpha' + \beta_1' x + \beta_2' y$$

Length of messages

Linear length functions

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

$$\langle x, y \rangle \qquad \ell_{\langle\ \rangle}(x, y) = \alpha' + \beta'_1 x + \beta'_2 y$$

$$\ell(\mathsf{enc}(\langle n, n \rangle, k)) = \ell_{\mathsf{enc}}(\ell(\langle n, n \rangle), \ell(k))$$

Length of messages

Linear length functions

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

$$\langle x, y \rangle \qquad \ell_{\langle\ \rangle}(x, y) = \alpha' + \beta'_1 x + \beta'_2 y$$

$$\begin{aligned}\ell(\mathsf{enc}(\langle n, n \rangle, k)) &= \ell_{\mathsf{enc}}(\ell(\langle n, n \rangle), \ell(k)) \\ &= \alpha + \beta_1 \ell(\langle n, n \rangle) + \beta_2 \ell(k))\end{aligned}$$

Length of messages

Linear length functions

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

$$\langle x, y \rangle \qquad \ell_{\langle\ \rangle}(x, y) = \alpha' + \beta_1' x + \beta_2' y$$

$$\begin{aligned}
\ell(\mathsf{enc}(\langle n, n \rangle, k)) &= \ell_{\mathsf{enc}}(\ell(\langle n, n \rangle), \ell(k)) \\
&= \alpha + \beta_1 \ell(\langle n, n \rangle) + \beta_2 \ell(k)) \\
&= \alpha + \beta_1 \ell_{\langle\rangle}(n, n) + \beta_2 \ell(k))
\end{aligned}$$

Length of messages

Linear length functions

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

$$\langle x, y \rangle \qquad \ell_{\langle\ \rangle}(x, y) = \alpha' + \beta'_1 x + \beta'_2 y$$

$$\begin{aligned}
\ell(\mathsf{enc}(\langle n, n \rangle, k)) &= \ell_{\mathsf{enc}}(\ell(\langle n, n \rangle), \ell(k)) \\
&= \alpha + \beta_1 \ell(\langle n, n \rangle) + \beta_2 \ell(k)) \\
&= \alpha + \beta_1 \ell_{\langle\rangle}(n, n) + \beta_2 \ell(k)) \\
&= \alpha + \beta_1 (\alpha' + \beta'_1 \ell(n) + \beta'_1 \ell(n)) \\
&\quad + \beta_2 \ell(k)
\end{aligned}$$

Implementation

Alpha version:

APTE v0.2alpha
http://www.cs.bham.ac.uk/~chevavfp/tools/apte/

Content:

- Front-end similar to ProVerif
- Handle equivalence between processes without replication
- Display witness of non-equivalence
- Handle equivalences between sequences of messages
- Handle reachability properties for processes without replication
- Handle equivalence with respect to length of messages

Outline

1. Proving more equivalence with ProVerif

2. APTE: Decision procedure for trace equivalence

3. Demo Time !