DECISION PROCEDURE FOR TRACE EQUIVALENCE

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

18 October 2011

CONTEXT

- Cryptographic protocols

Most communications take place over a public network

Cryptographic protocols

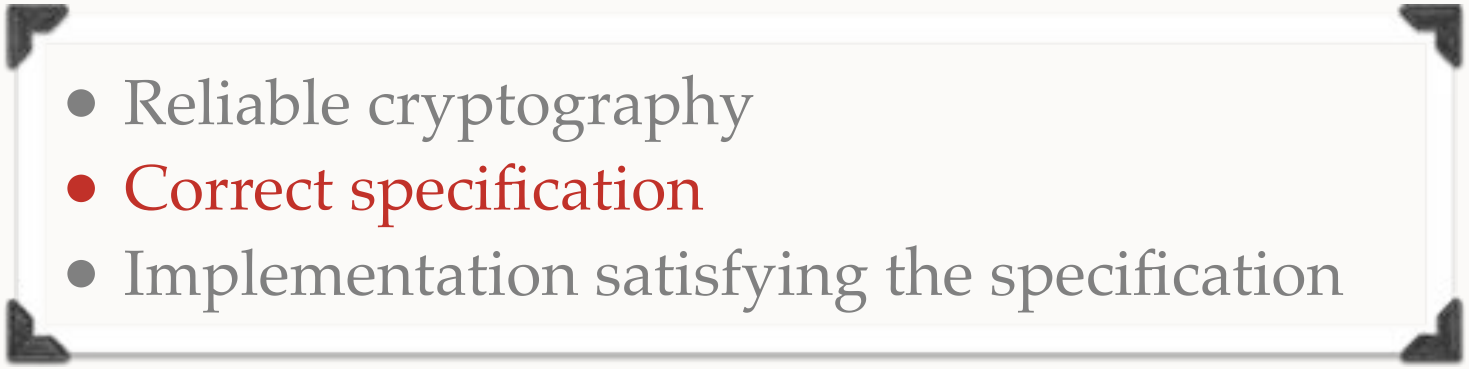
- small programs designed to secure communication (e.g. secrecy)
- use cryptographic primitives (e.g. encryption, signature)

It important to verify their security

CONTEXT

- Reliable cryptography
- Correct specification
- Implementation satisfying the specification

CONTEXT



- Reliable cryptography
- Correct specification
- Implementation satisfying the specification

- Some security properties

CONTEXT

- Reliable cryptography
- Correct specification
- Implementation satisfying the specification

- Some security properties

Reachability properties

- Secrecy, Authentication, ...

CONTEXT

- Reliable cryptography
- Correct specification
- Implementation satisfying the specification

- Some security properties

Reachability properties

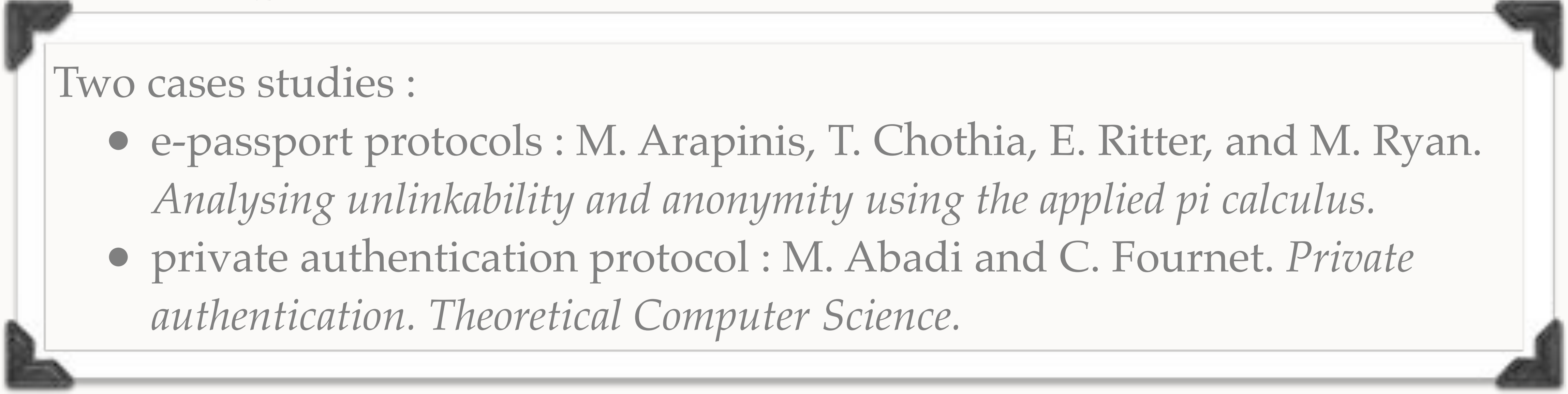
- Secrecy, Authentication, ...

Equivalence properties

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

CONTEXT

- Example



Two cases studies :

- 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.*

CONTEXT

- Example

Two cases studies :

- 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

Bob

CONTEXT

- Example

Two cases studies :

- 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

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

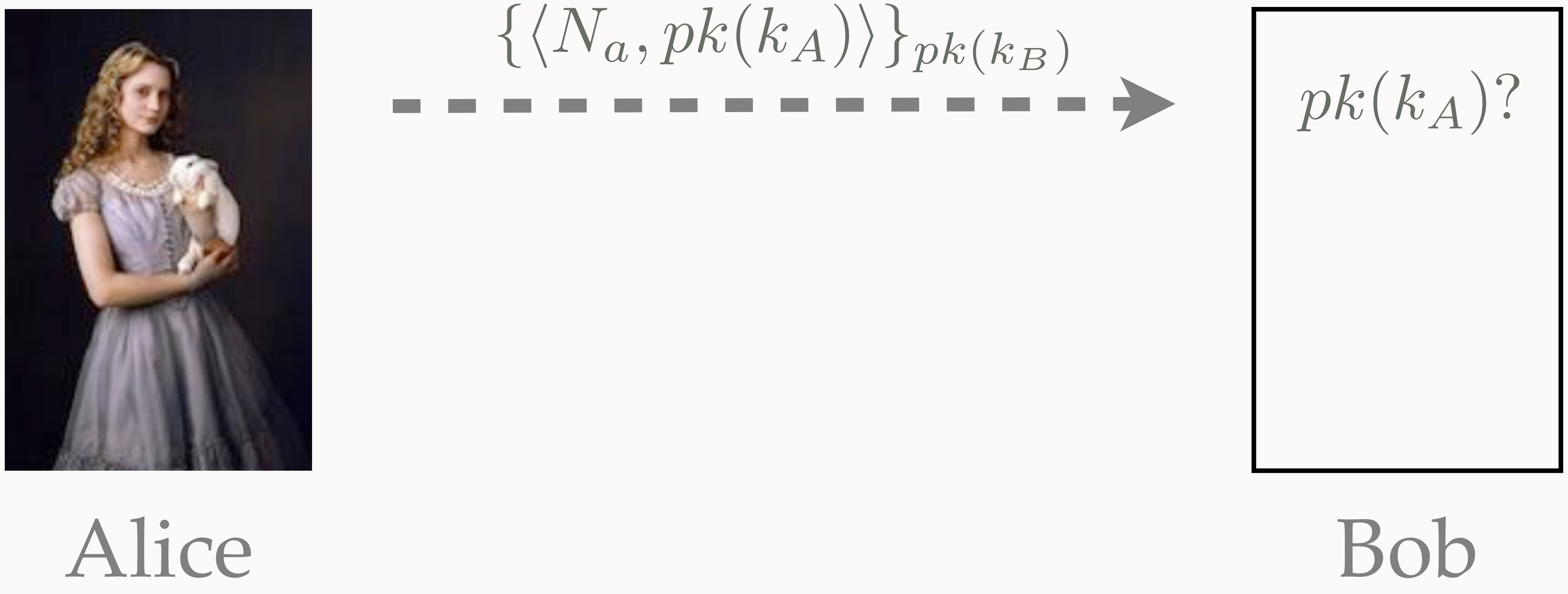
Bob

CONTEXT

- Example

Two cases studies :

- 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.*



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

$pk(k_A)?$

Alice

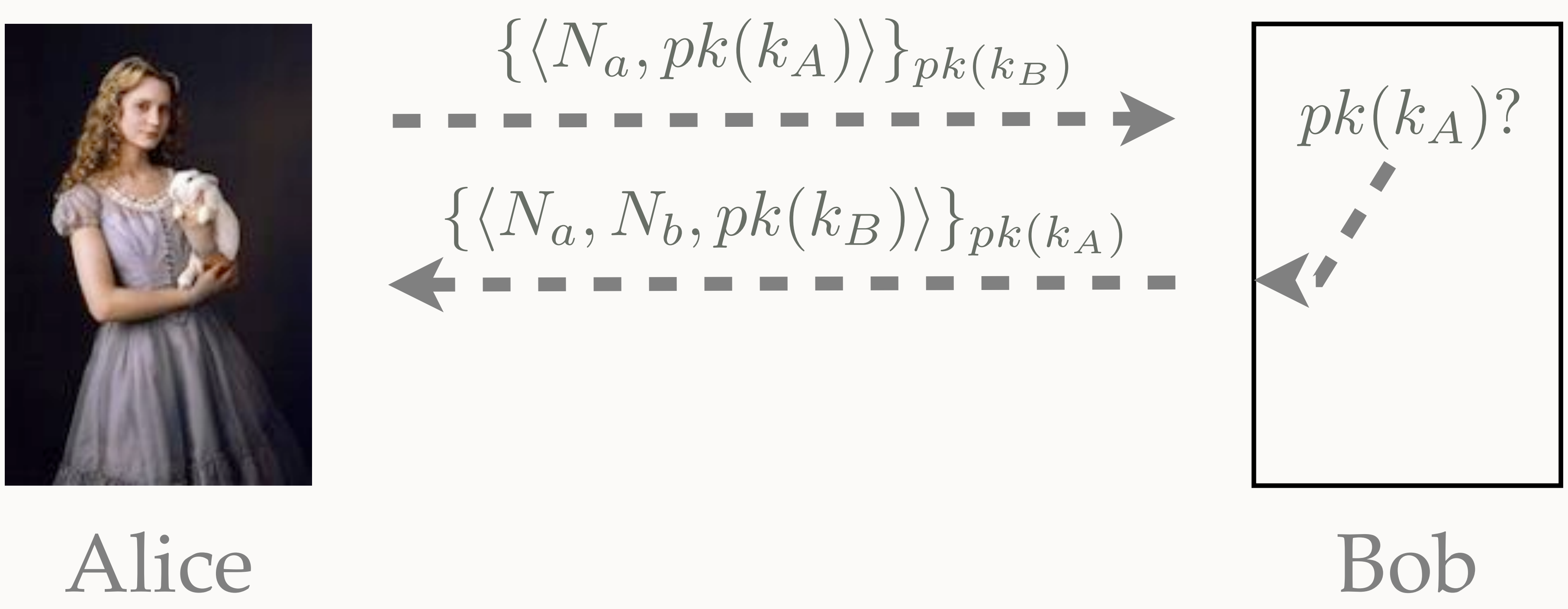
Bob

CONTEXT

- Example

Two cases studies :

- 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.*



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

$pk(k_A)?$

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

Alice

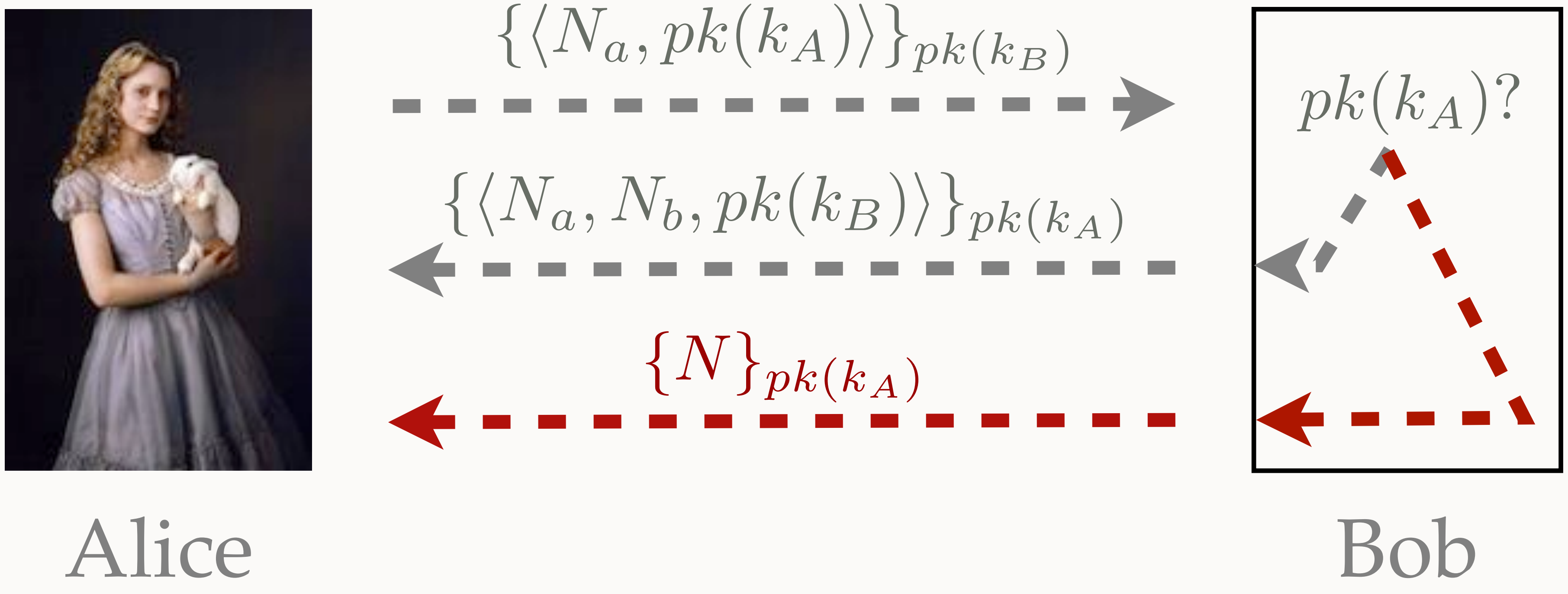
Bob

CONTEXT

- Example

Two cases studies :

- 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.*

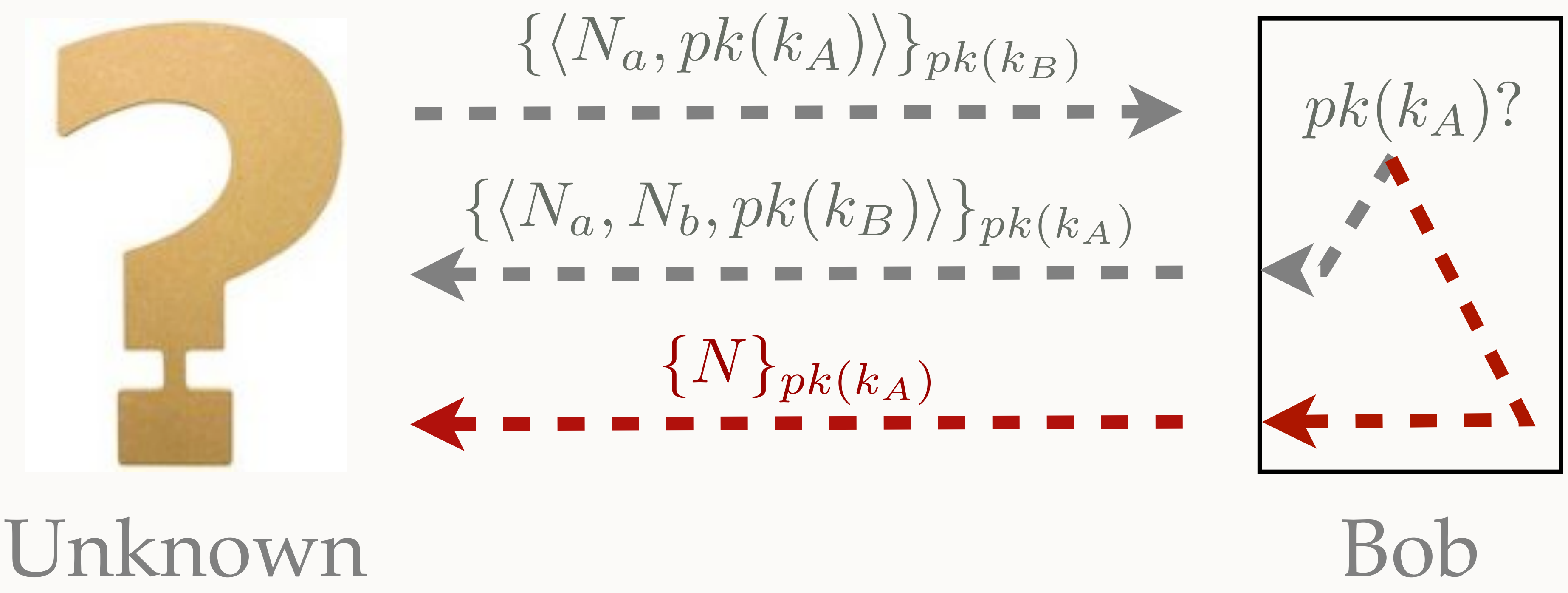

$\{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}$
$\{\langle N_a, N_b, pk(k_B)\rangle\}_{pk(k_A)}$
$\{N\}_{pk(k_A)}$
$pk(k_A)?$
Alice
Bob

CONTEXT

- Example

Two cases studies :

- 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.*



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

$pk(k_A)?$

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

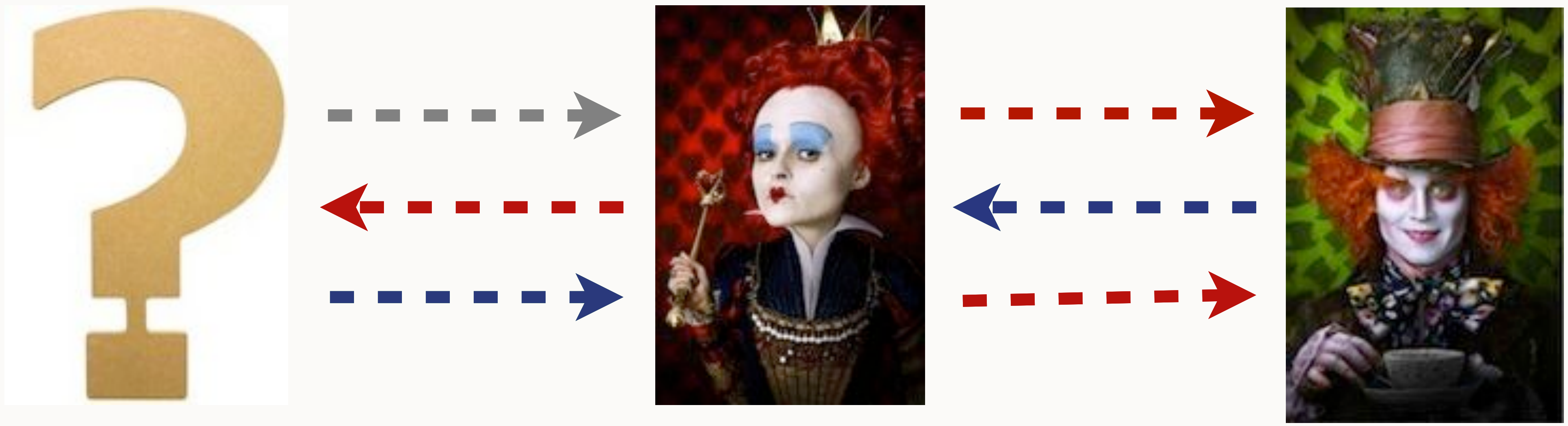
$\{N\}_{pk(k_A)}$

Unknown

Bob

CONTEXT

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



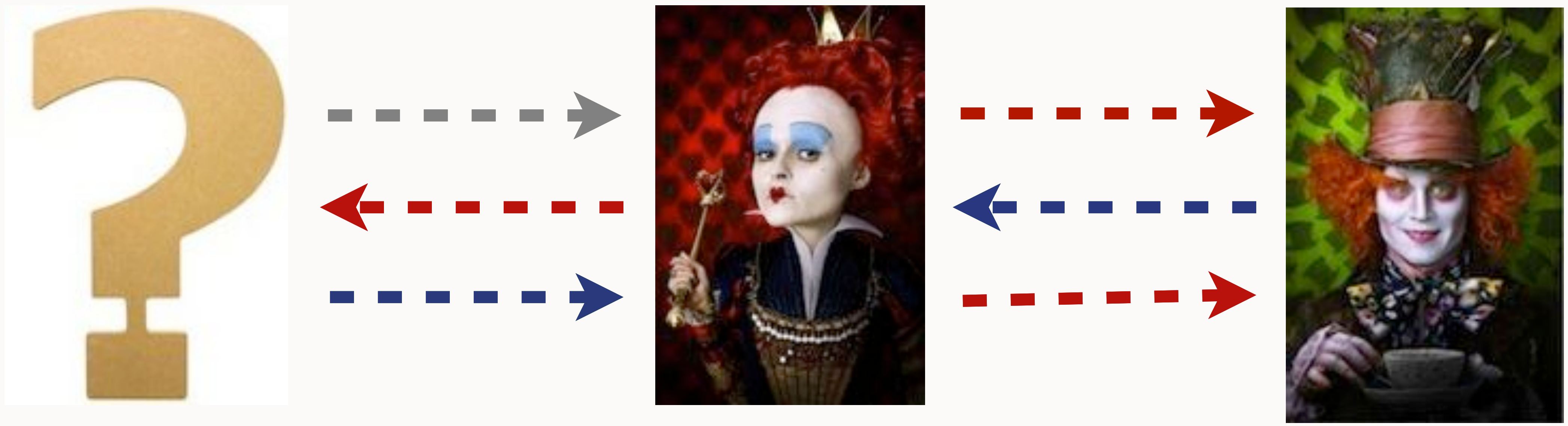
Unknown

Intruder

Bob

CONTEXT

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



Unknown

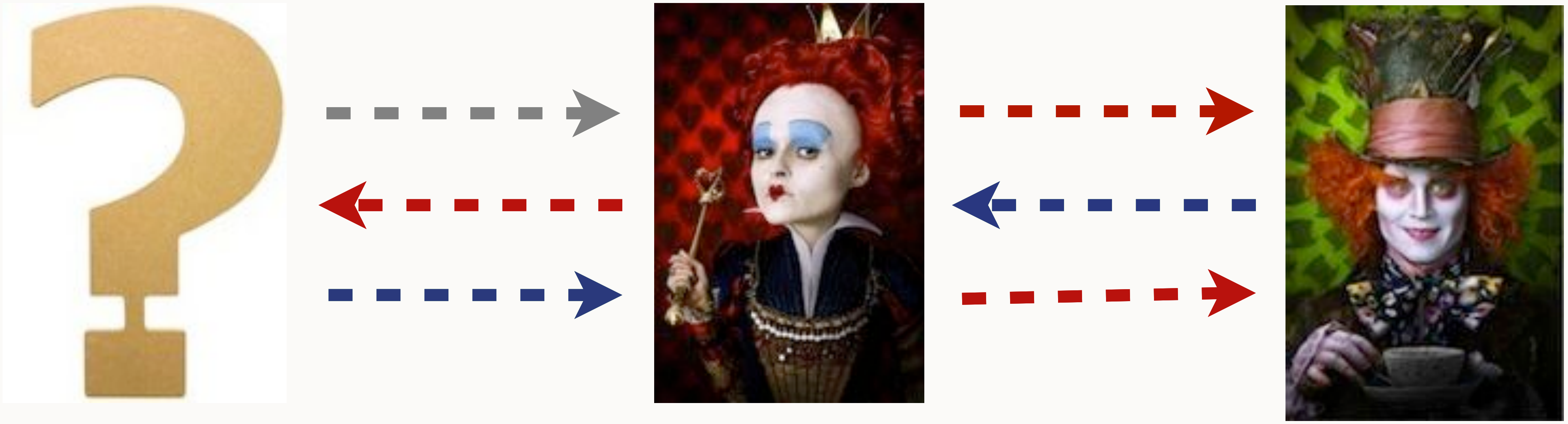
Intruder

Bob

Can the intruder deduce the unknown’s identity ?

CONTEXT

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



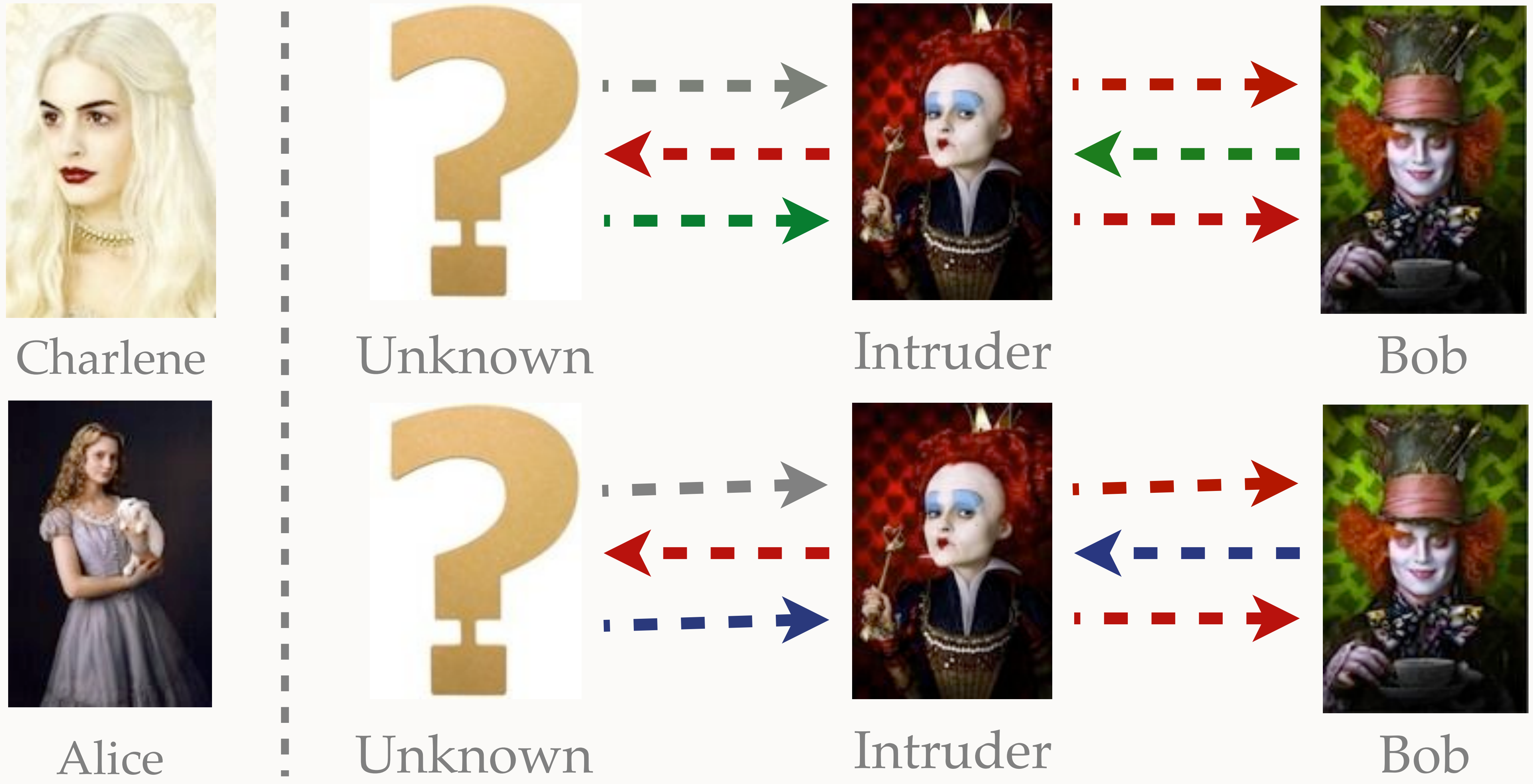
Unknown

Intruder

Bob

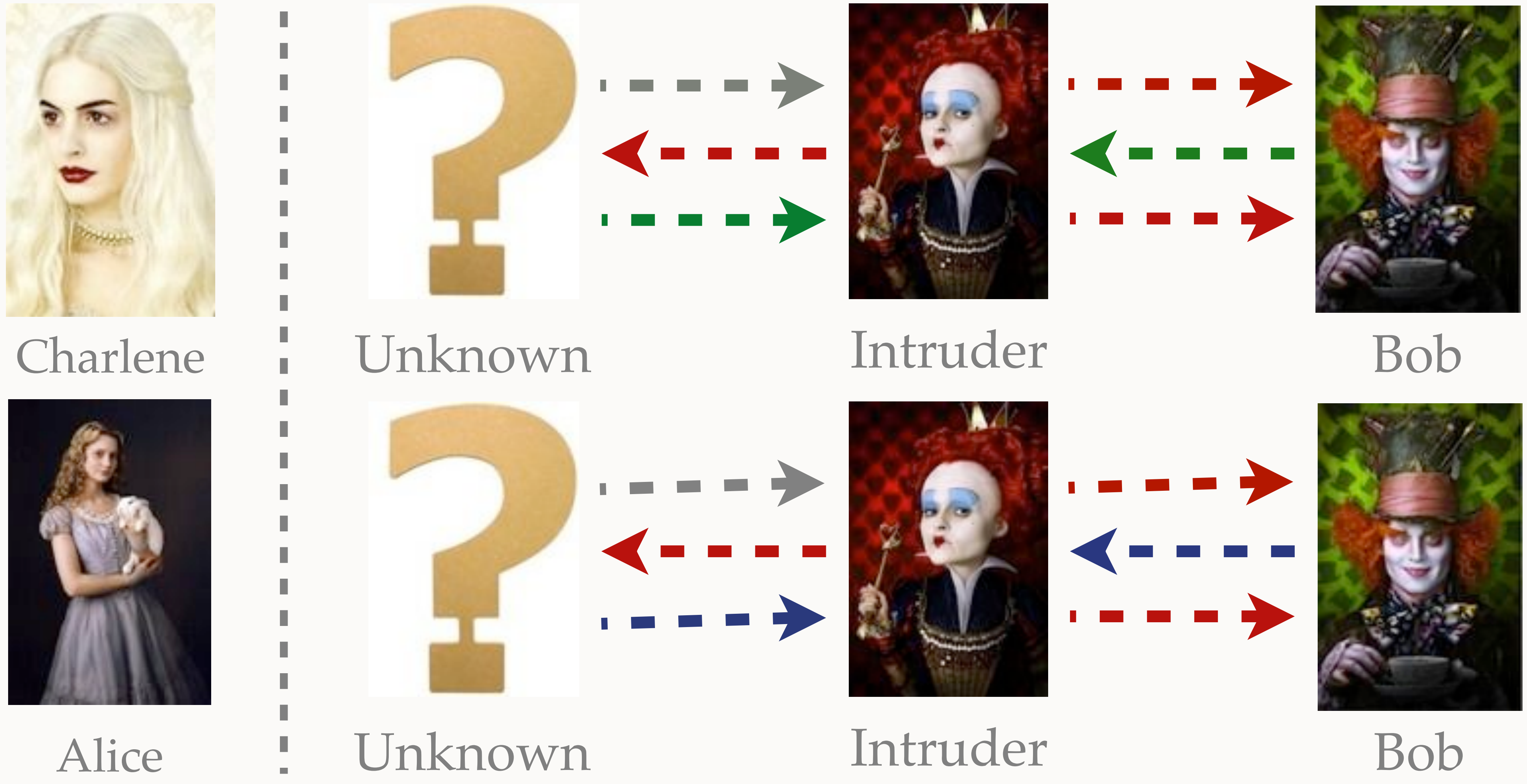
CONTEXT

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



CONTEXT

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



Charlene

Unknown

Intruder

Bob

Alice

Unknown

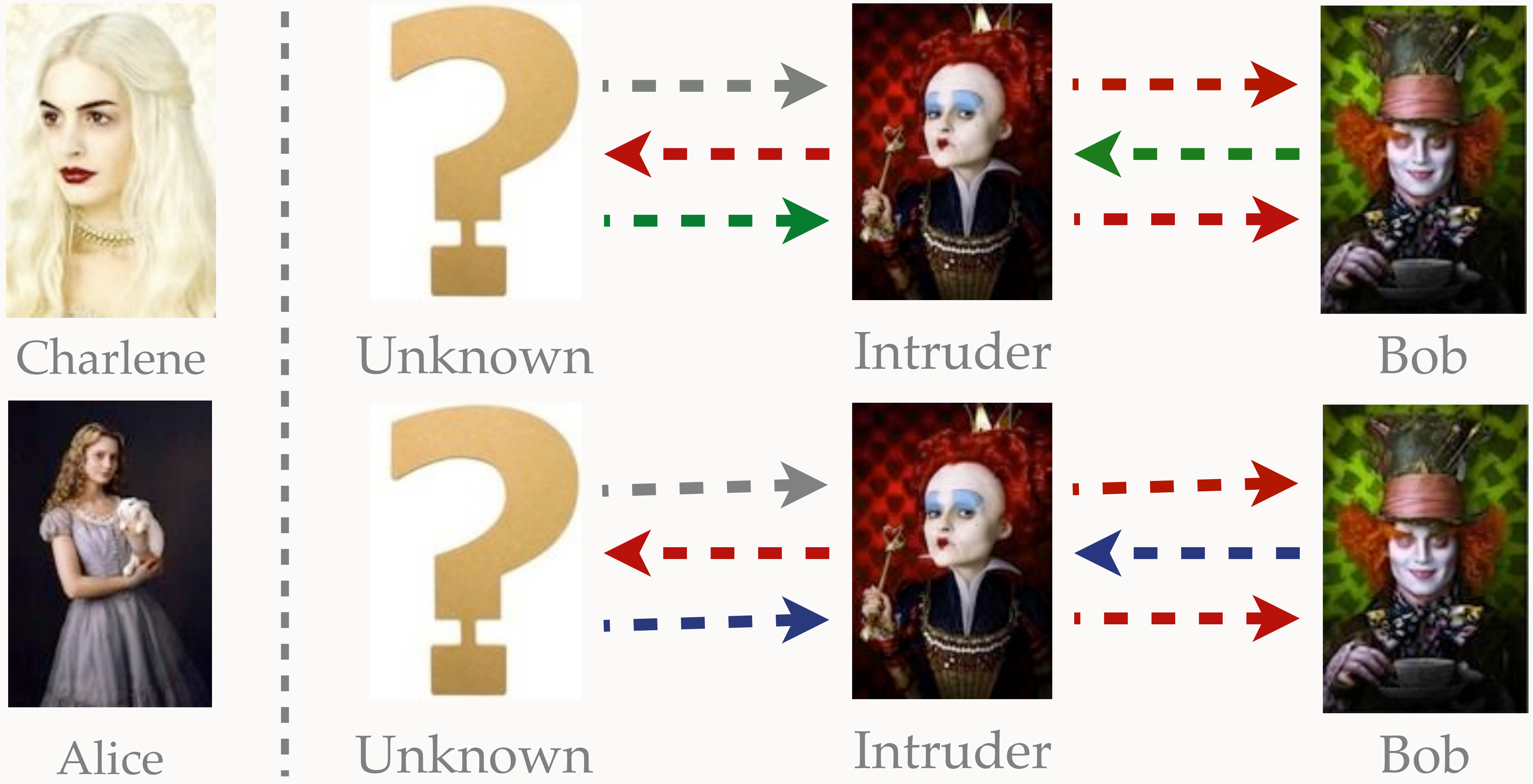
Intruder

Bob

Can the intruder distinguish the two situations ?

CONTEXT

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



Trace Equivalence

CONTEXT

- Trace equivalence on an example

Alice

Intruder

Bob

Charlene

Intruder

Bob

CONTEXT

- Trace equivalence on an example

Alice

Bob

Charlene

Bob

CONTEXT

- Trace equivalence on an example

Alice

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

Bob

Charlene

Bob

CONTEXT

- Trace equivalence on an example

Alice

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

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

Bob

Charlene

Bob

CONTEXT

- Trace equivalence on an example

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

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

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

Alice

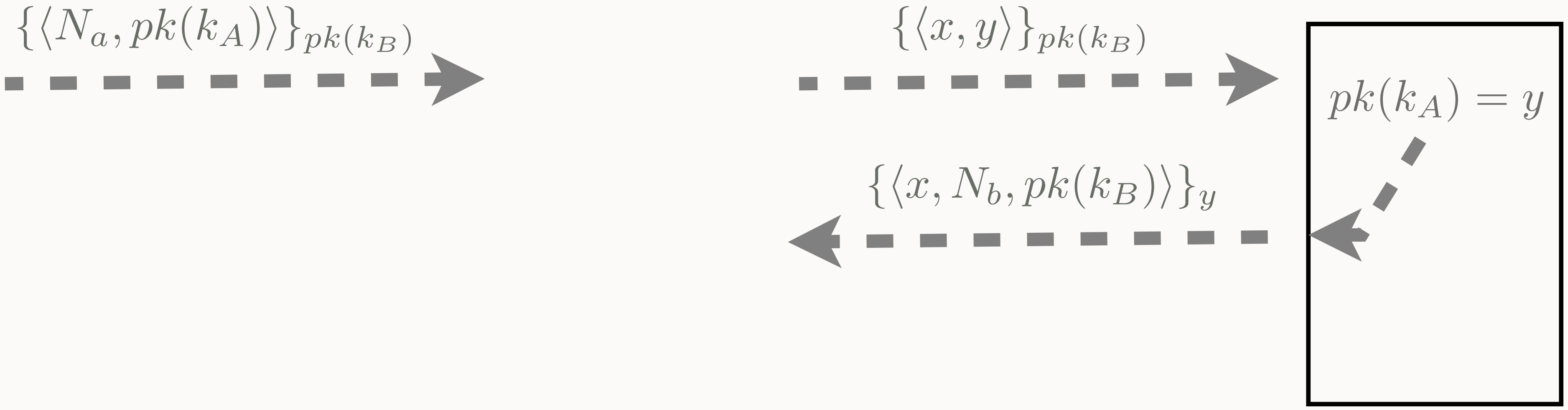
Bob

Charlene

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = y$

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

Alice

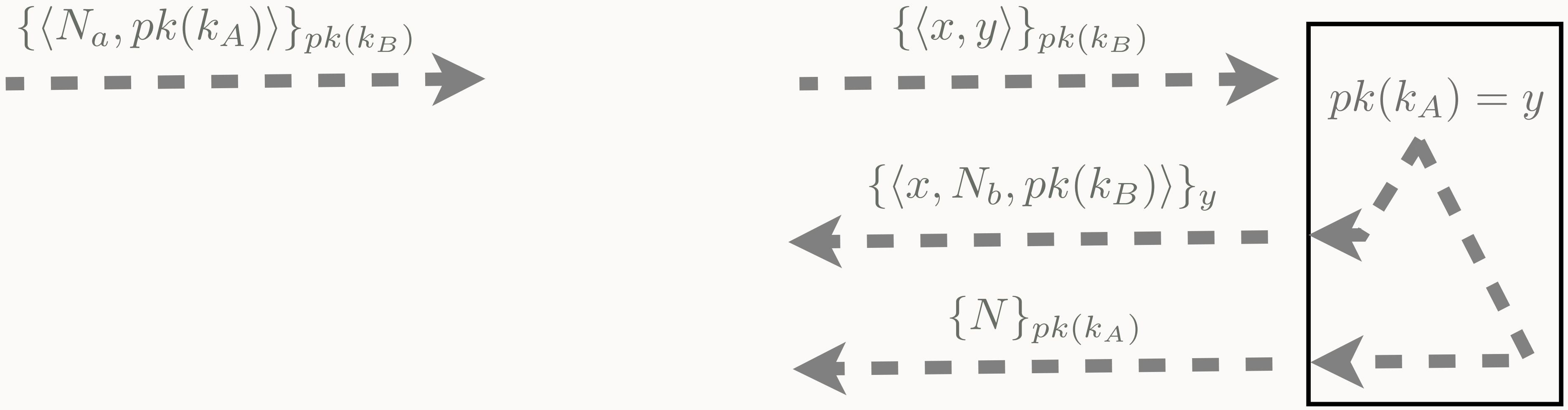
Bob

Charlene

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = y$

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

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

Alice

Bob

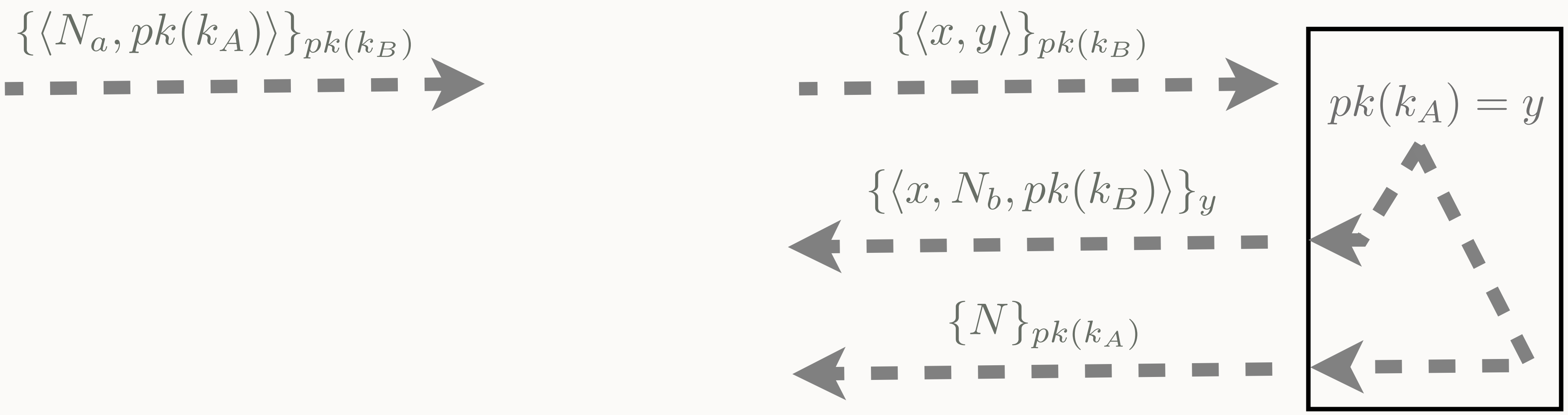
Charlene

Bob

CONTEXT

- Trace equivalence on an example

Alice



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

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

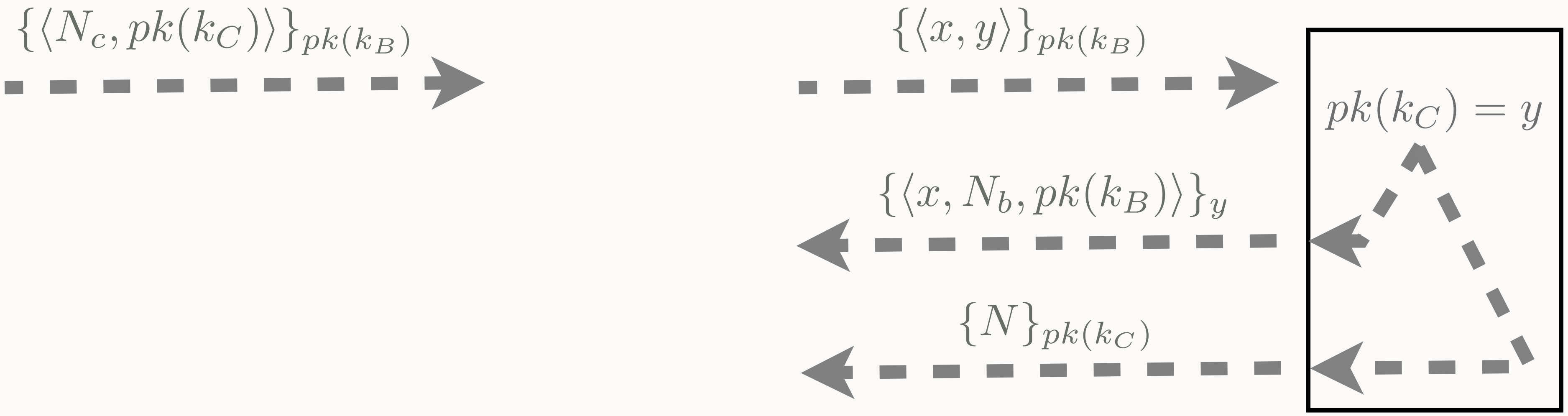
$pk(k_A) = y$

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

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

Bob

Charlene



$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

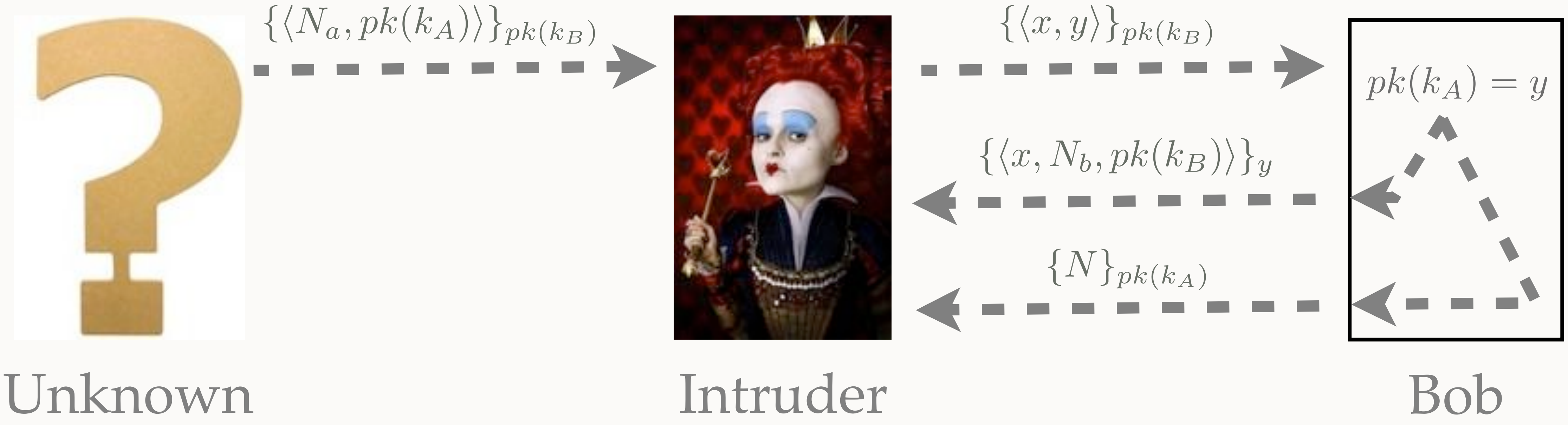
$\{\langle x, N_b, pk(k_B)\rangle\}_y$

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

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = y$

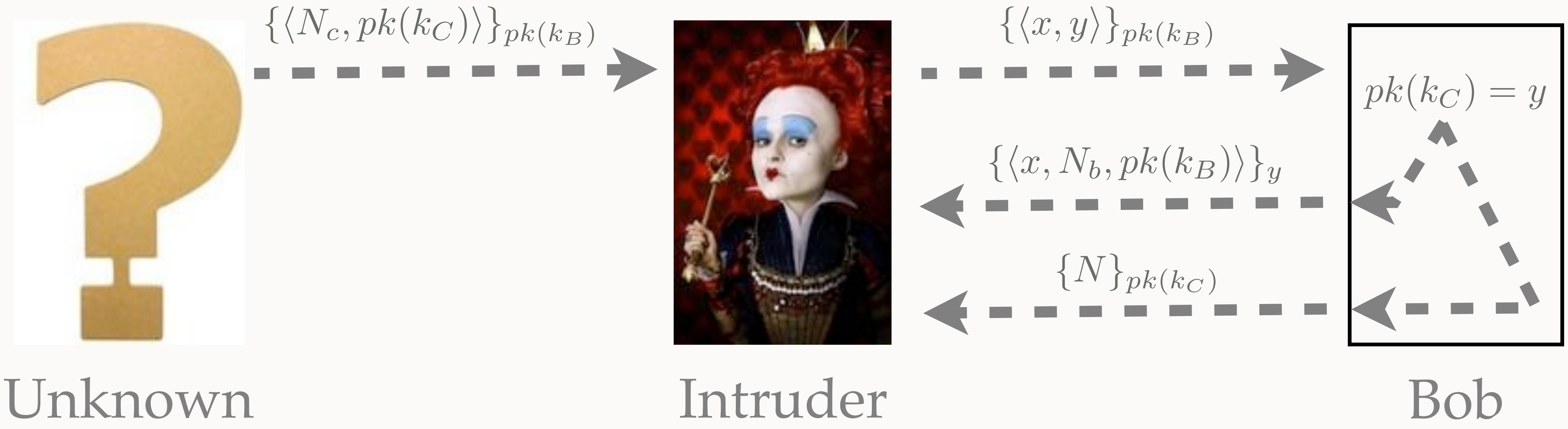
$\{\langle x, N_b, pk(k_B)\rangle\}_y$

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

Unknown

Intruder

Bob



$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

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

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

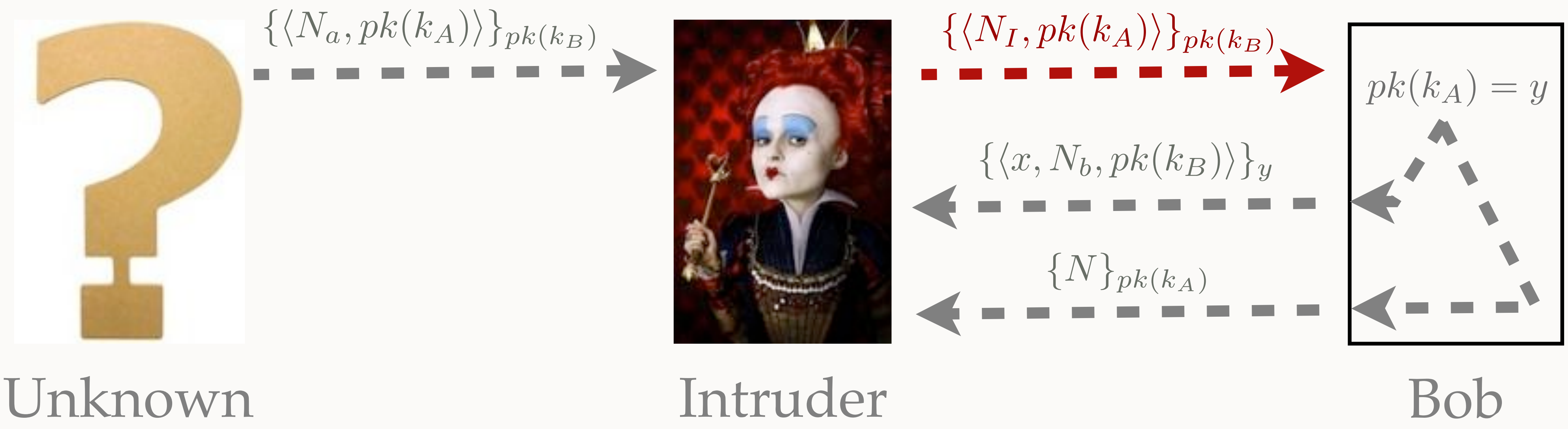
Unknown

Intruder

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = y$

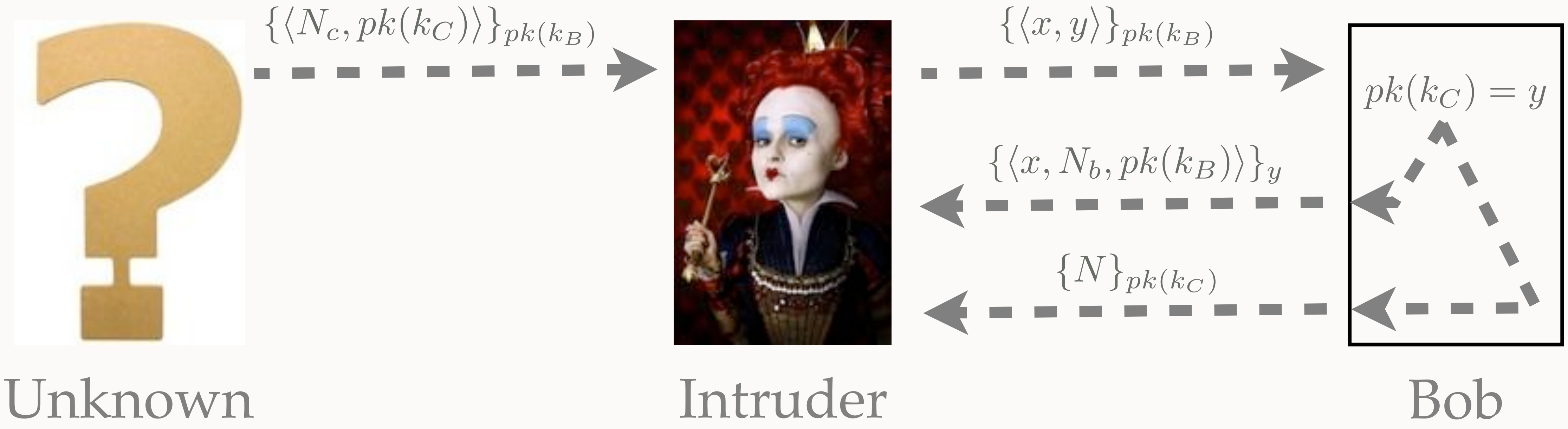
$\{\langle x, N_b, pk(k_B)\rangle\}_y$

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

Unknown

Intruder

Bob



$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

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

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

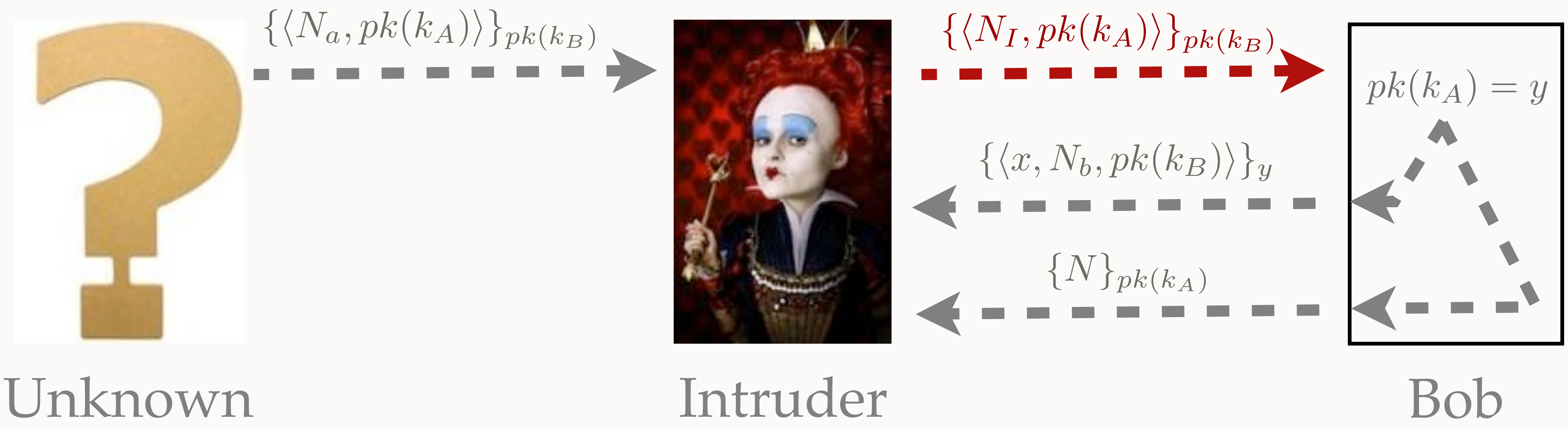
Unknown

Intruder

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = y$

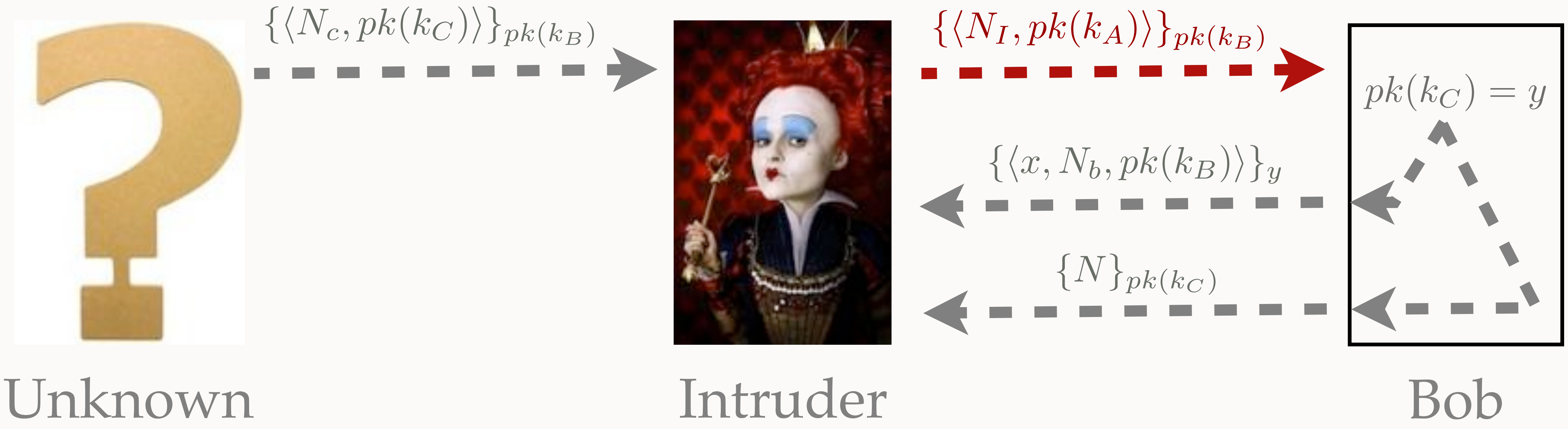
$\{\langle x, N_b, pk(k_B)\rangle\}_y$

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

Unknown

Intruder

Bob



$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

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

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

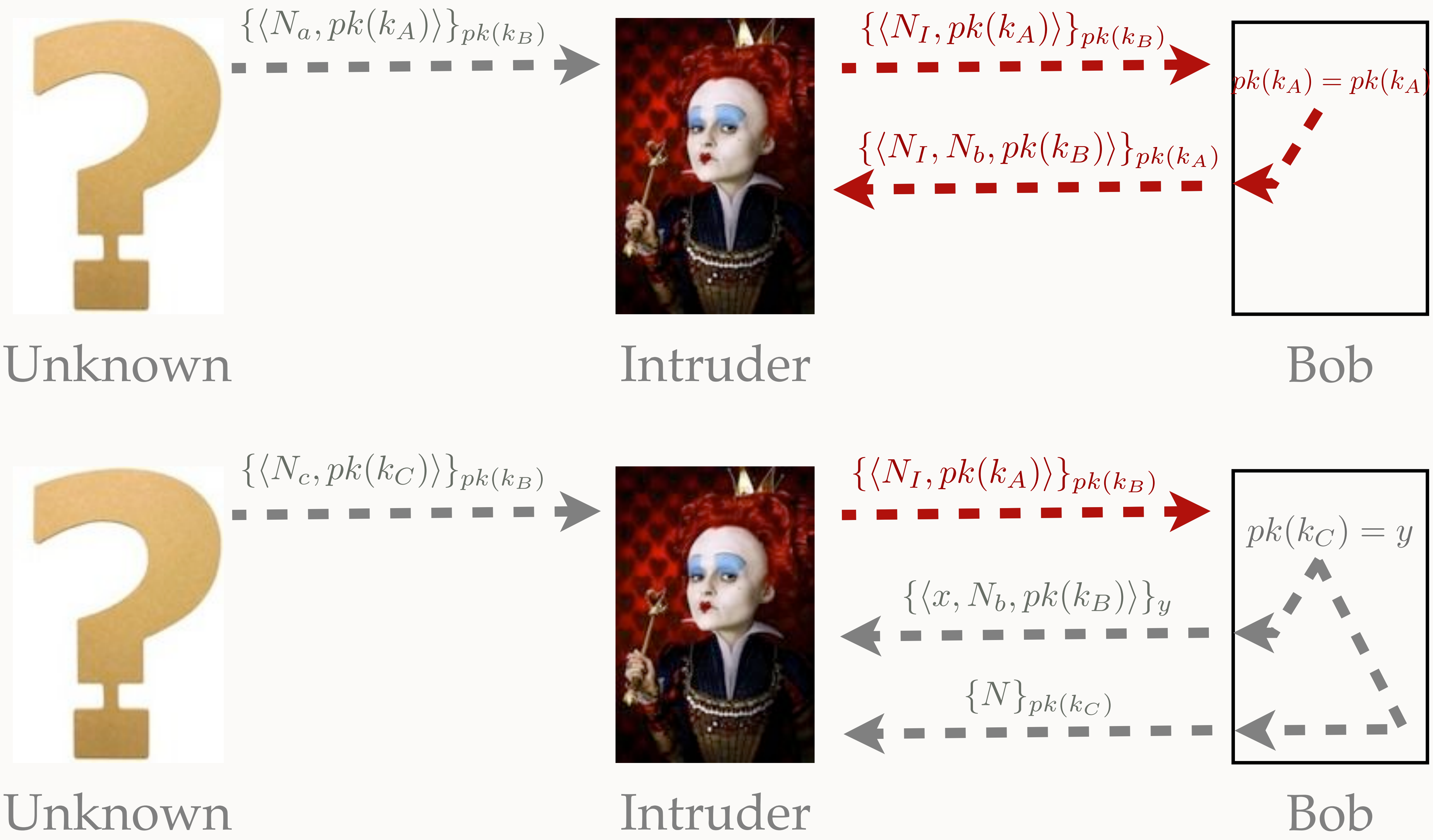
Unknown

Intruder

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = pk(k_A)$

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

Unknown

Intruder

Bob

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

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

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

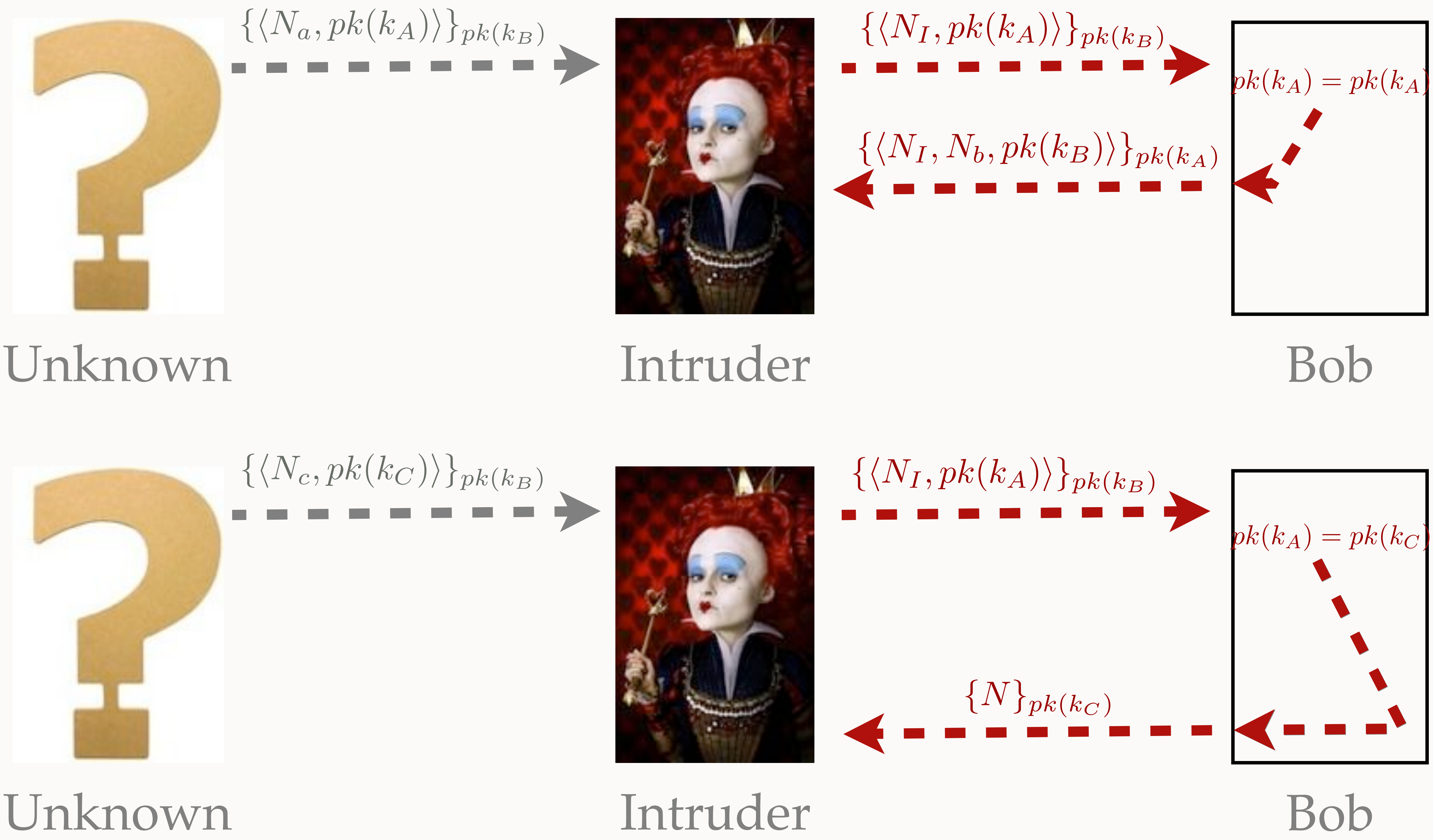
Unknown

Intruder

Bob

CONTEXT

- Trace equivalence on an example



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

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

$pk(k_A) = pk(k_A)$

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

Unknown

Intruder

Bob

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_A) = pk(k_C)$

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

Unknown

Intruder

Bob

PREVIOUS WORKS

Most of the previous works focus on stronger equivalence

- 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
- B. Blanchet, M. Abadi, and C. Fournet. *Automated verification of selected equivalences for security protocols.*

    ➡ Tool : B. Blanchet, *ProVerif*

Trace equivalence for simple processes without else branches

- V. Cortier and S. Delaune. *A method for proving observational equivalence.*

CONTRIBUTION

Decision procedure for verification of trace equivalence

- Infinitely many traces are represented by symbolic constraint system

+ Protocol possibly non-determinist and with non trivial else branches

+ Private channels

- Fixed set of cryptographic primitives : symmetric and asymmetric encryption, pairing and signature

- Bounded number of sessions (no replication in the process algebra)

CONSTRAINT SYSTEM

- One constraint system = several traces

Alice

Intruder

Bob

CONSTRAINT SYSTEM

- One constraint system = several traces

Alice

Intruder

Bob

$pk(k_A), pk(k_B), pk(k_C), N_I$

CONSTRAINT SYSTEM

- One constraint system = several traces

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

Alice

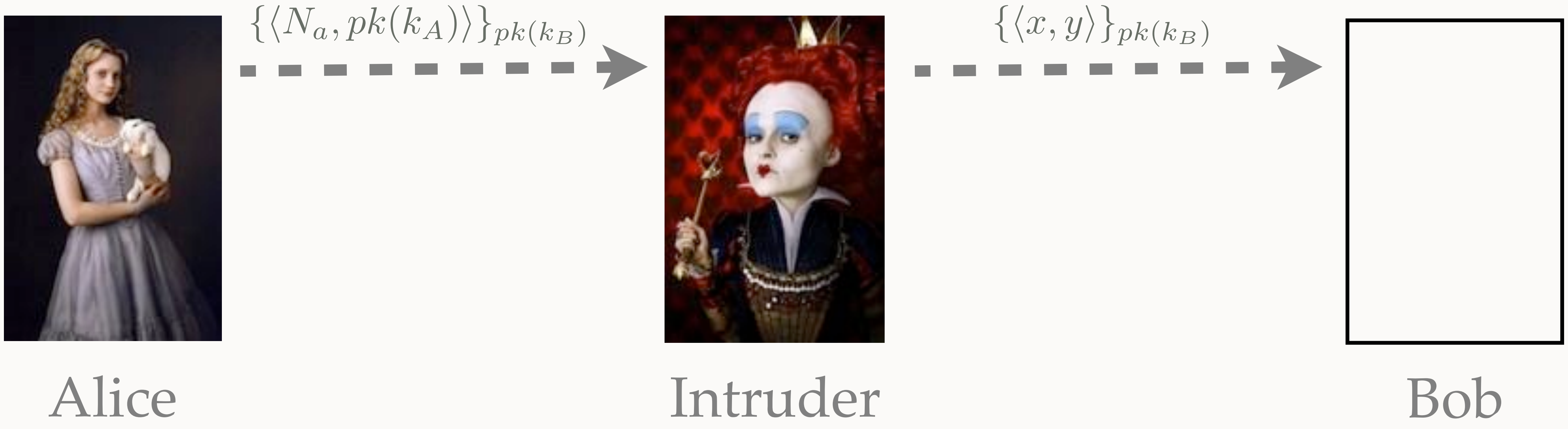
Intruder

Bob

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

CONSTRAINT SYSTEM

- One constraint system = several traces



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

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

Alice

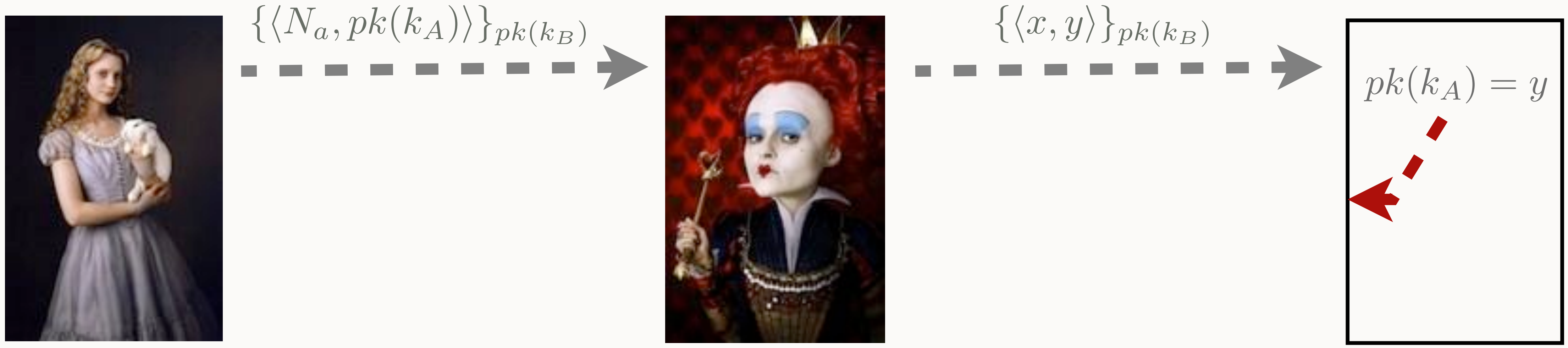
Intruder

Bob

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

CONSTRAINT SYSTEM

- One constraint system = several traces



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

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

$pk(k_A) = y$

Alice

Intruder

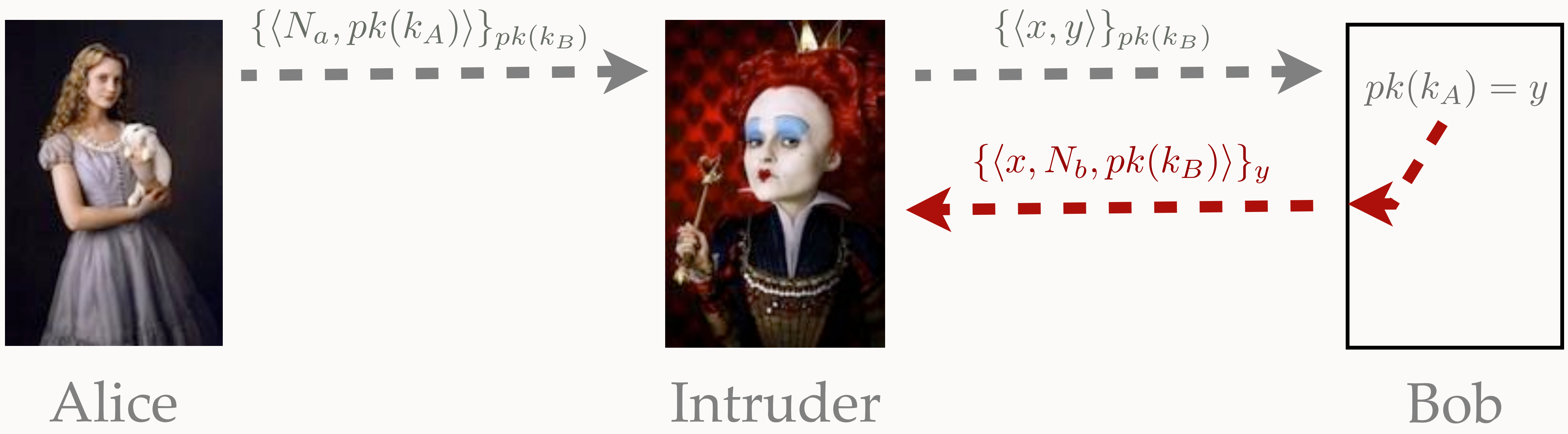
Bob

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

$$y \overset{?}{=} pk(k_A)$$

CONSTRAINT SYSTEM

- One constraint system = several traces



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

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

$pk(k_A) = y$

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

Alice

Intruder

Bob

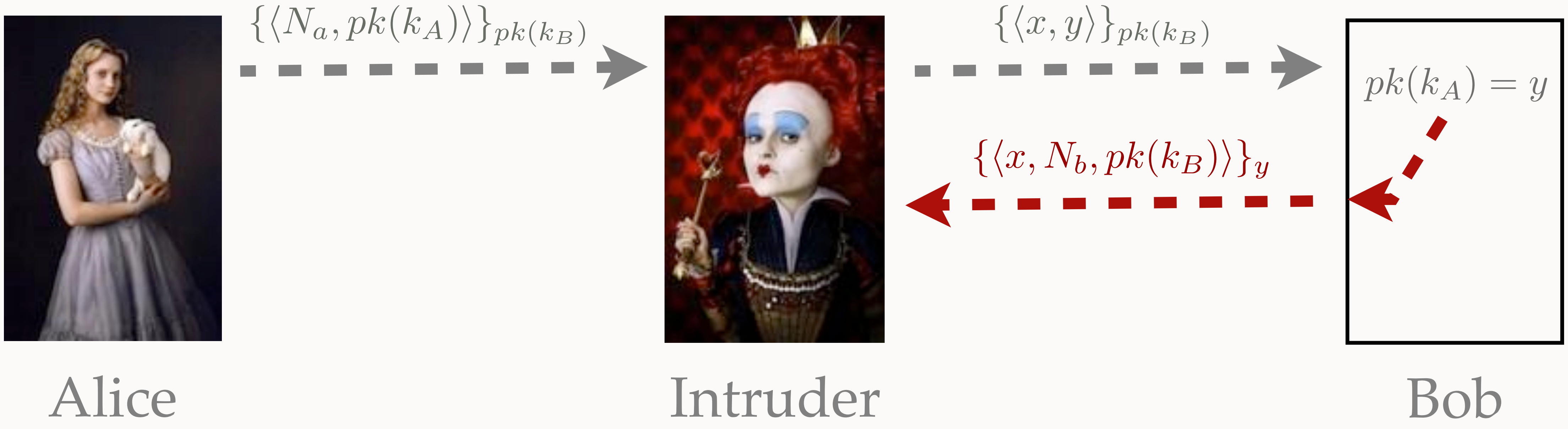
$$pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)} \overset{?}{\vdash} \{\langle x, y\rangle\}_{pk(k_B)}$$

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

$$y \overset{?}{=} pk(k_A)$$

CONSTRAINT SYSTEM

- One constraint system = several traces



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

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

$pk(k_A) = y$

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

Alice

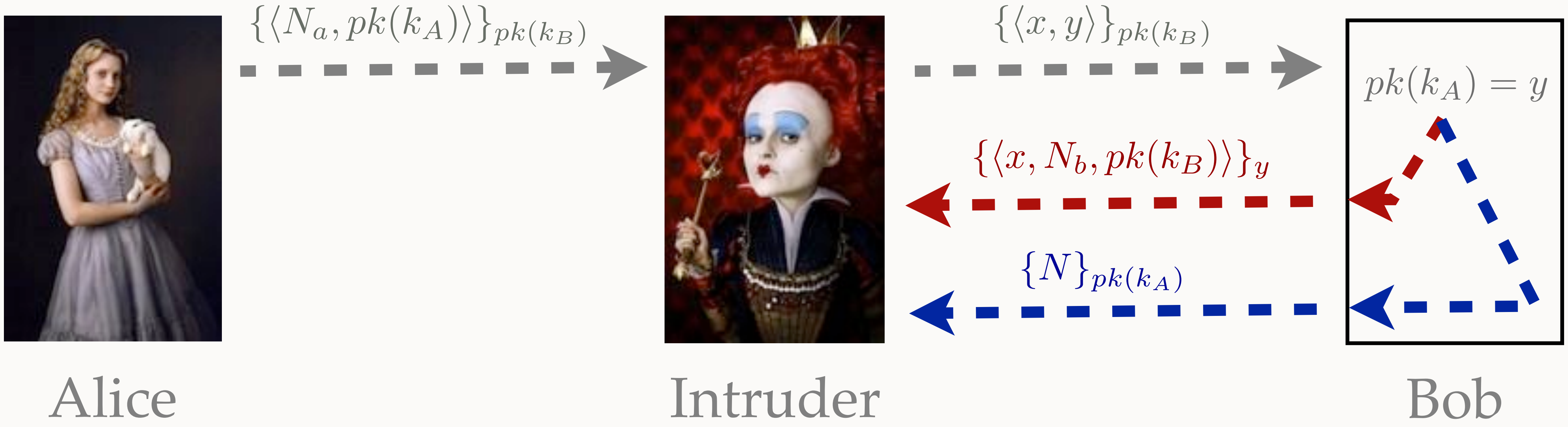
Intruder

Bob

$$
\begin{aligned}
D &: \; pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)} \overset{?}{\vdash} \{\langle x, y\rangle\}_{pk(k_B)} \\
\Phi &: \; pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}, \{\langle x, N_b, pk(k_B)\rangle\}_y \\
E &: \; y \overset{?}{=} pk(k_A)
\end{aligned}
$$

CONSTRAINT SYSTEM

- One constraint system = several traces



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

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

$pk(k_A) = y$

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

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

Alice

Intruder

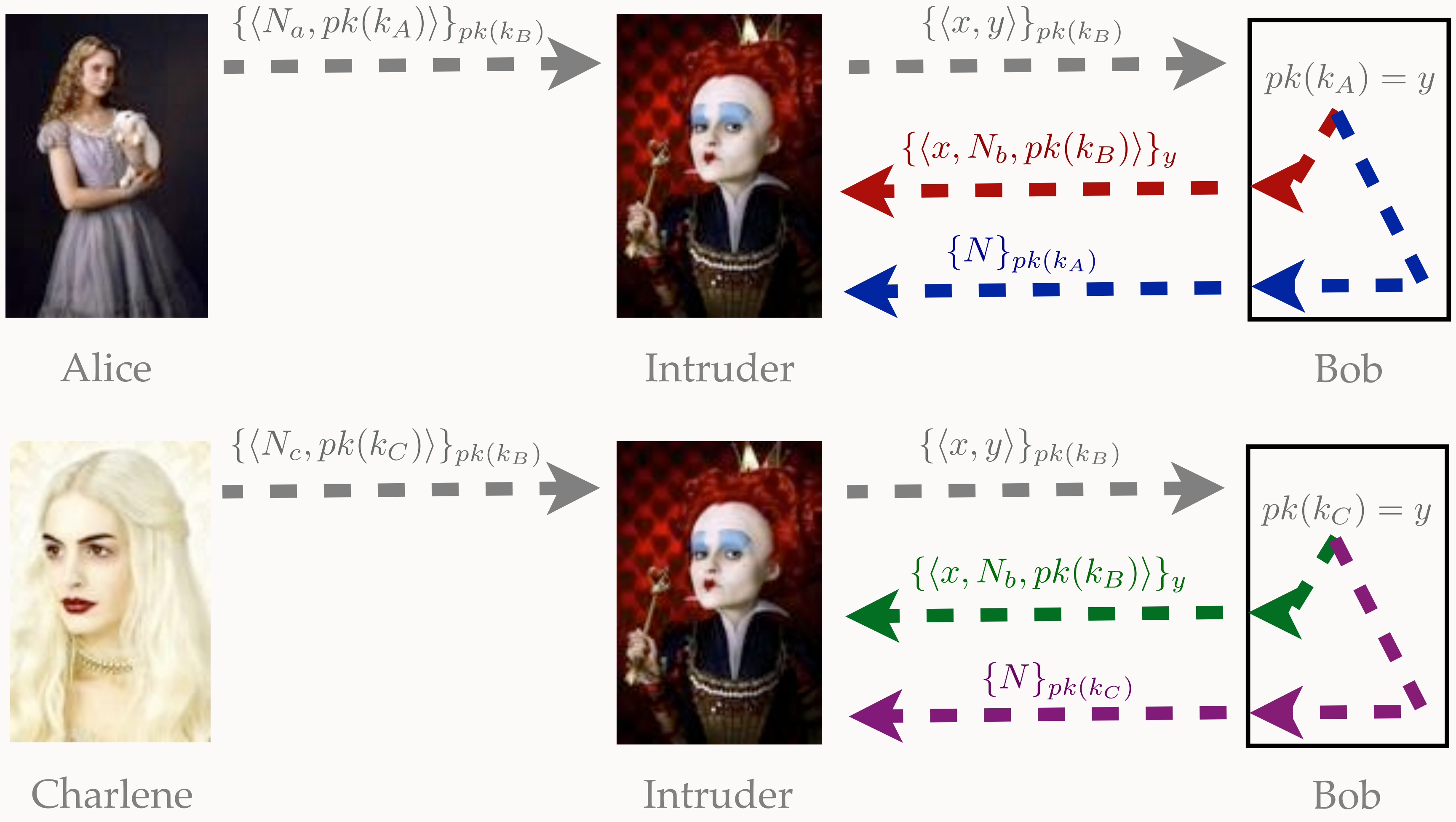
Bob

$$
\begin{aligned}
D &: \; pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)} \overset{?}{\vdash} \{\langle x, y\rangle\}_{pk(k_B)} \\
\Phi &: \; pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}, \{\langle x, N_b, pk(k_B)\rangle\}_y \\
E &: \; y \overset{?}{=} pk(k_A)
\end{aligned}
$$

$$
\begin{aligned}
D &: \; pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)} \overset{?}{\vdash} \{\langle x, y\rangle\}_{pk(k_B)} \\
\Phi &: \; pk(k_A), pk(k_B), pk(k_C), N_I, \{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}, \{N\}_{pk(k_A)} \\
E &: \; y \overset{?}{\neq} pk(k_A)
\end{aligned}
$$

CONSTRAINT SYSTEM

- Set of constraint systems



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

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

$pk(k_A) = y$

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

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

Alice

Intruder

Bob

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

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

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

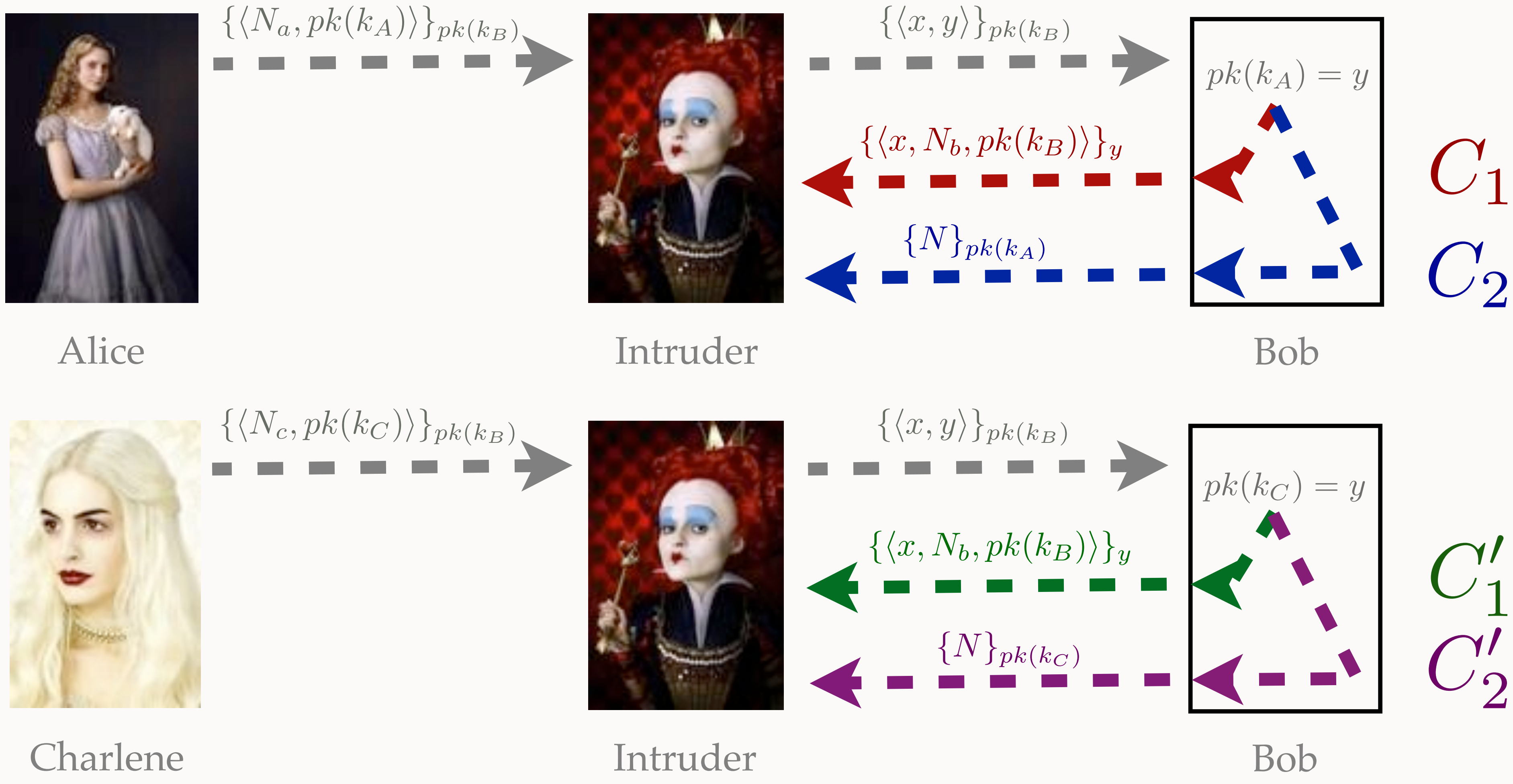
Charlene

Intruder

Bob

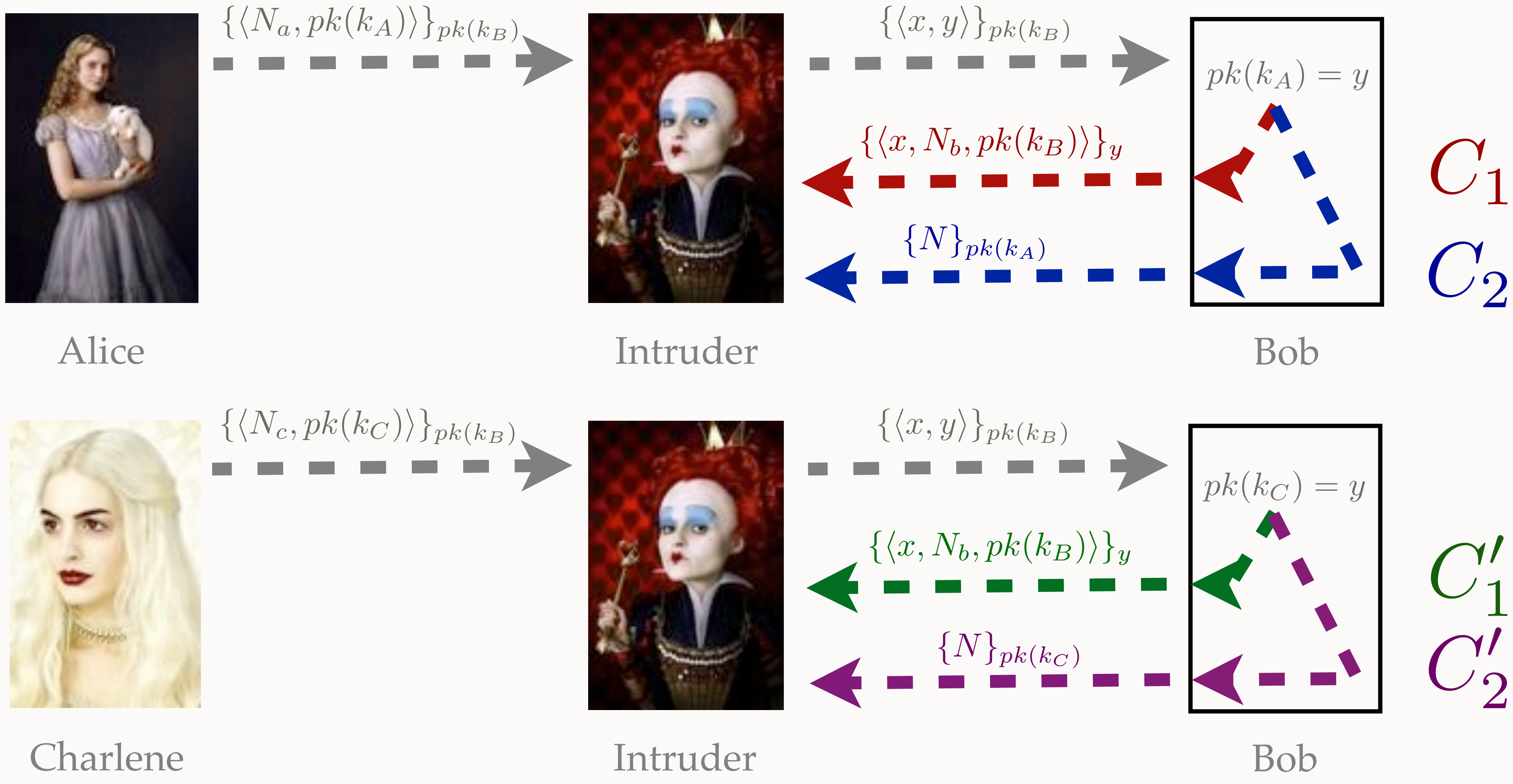
CONSTRAINT SYSTEM

- Set of constraint systems


$\{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}$
$\{\langle x, y\rangle\}_{pk(k_B)}$
$pk(k_A) = y$
$\{\langle x, N_b, pk(k_B)\rangle\}_y$
$\{N\}_{pk(k_A)}$
C_1
C_2
Alice
Intruder
Bob
$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$
$\{\langle x, y\rangle\}_{pk(k_B)}$
$pk(k_C) = y$
$\{\langle x, N_b, pk(k_B)\rangle\}_y$
$\{N\}_{pk(k_C)}$
C'_1
C'_2
Charlene
Intruder
Bob

CONSTRAINT SYSTEM

- Set of constraint systems



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

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

$pk(k_A) = y$

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

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

C_1

C_2

Alice

Intruder

Bob

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$pk(k_C) = y$

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

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

C'_1

C'_2

Charlene

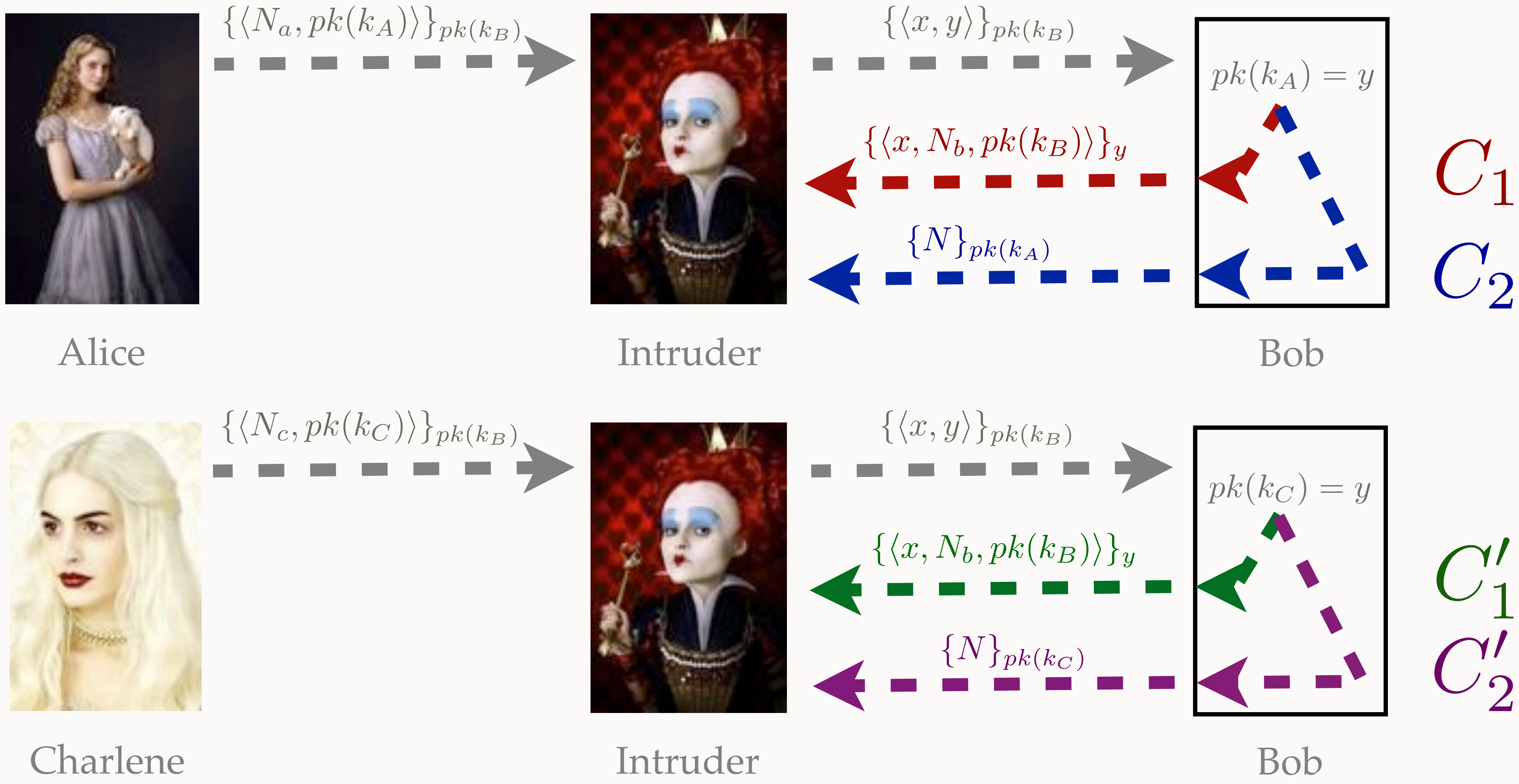
Intruder

Bob

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

CONSTRAINT SYSTEM

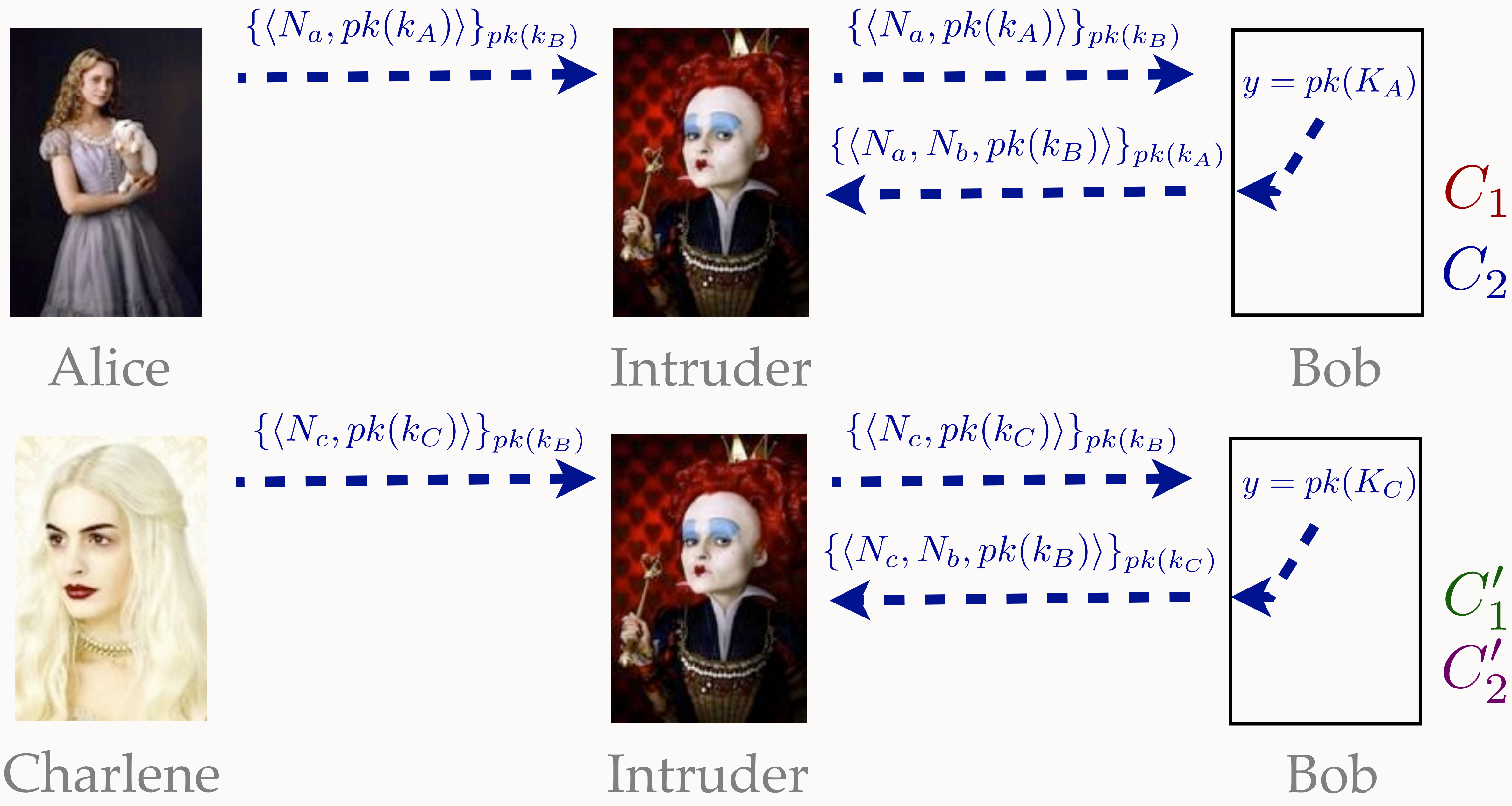
- Set of constraint systems


$\{\langle N_a, pk(k_A)\rangle\}_{pk(k_B)}$
$\{\langle x, y\rangle\}_{pk(k_B)}$
$pk(k_A) = y$
$\{\langle x, N_b, pk(k_B)\rangle\}_y$
C_1
$\{N\}_{pk(k_A)}$
C_2
Alice
Intruder
Bob
$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$
$\{\langle x, y\rangle\}_{pk(k_B)}$
$pk(k_C) = y$
$\{\langle x, N_b, pk(k_B)\rangle\}_y$
C'_1
$\{N\}_{pk(k_C)}$
C'_2
Charlene
Intruder
Bob

Symbolic equivalence between sets of constraint systems

CONSTRAINT SYSTEM

- Why sets of constraint systems are necessary ?



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

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

$y = pk(K_A)$

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

C_1

C_2

Alice

Intruder

Bob

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

$y = pk(K_C)$

$\{\langle N_c, N_b, pk(k_B)\rangle\}_{pk(k_C)}$

C'_1

C'_2

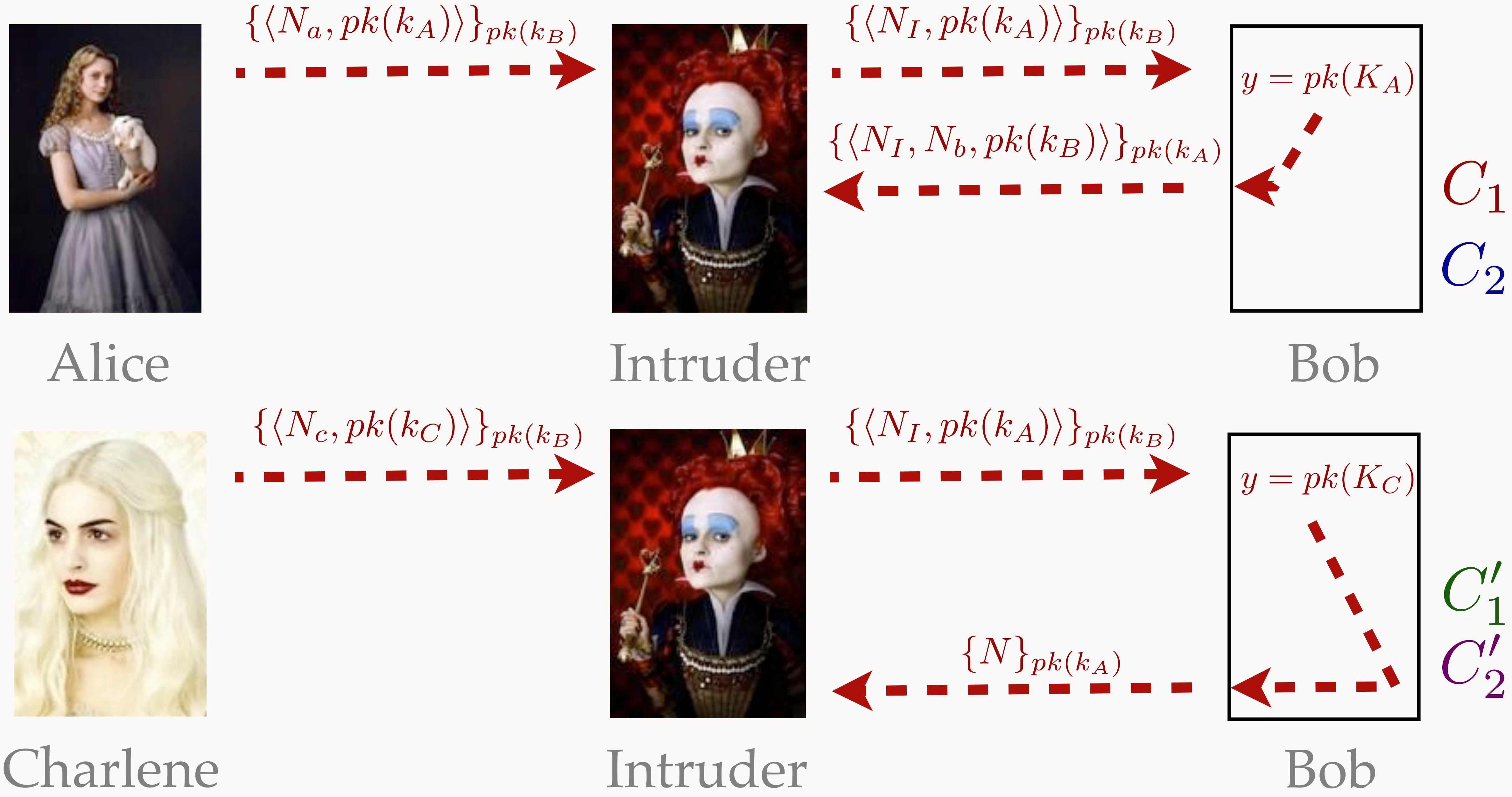
Charlene

Intruder

Bob

CONSTRAINT SYSTEM

- Why sets of constraint systems are necessary ?



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

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

$y = pk(K_A)$

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

C_1

C_2

Alice

Intruder

Bob

$\{\langle N_c, pk(k_C)\rangle\}_{pk(k_B)}$

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

$y = pk(K_C)$

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

C'_1

C'_2

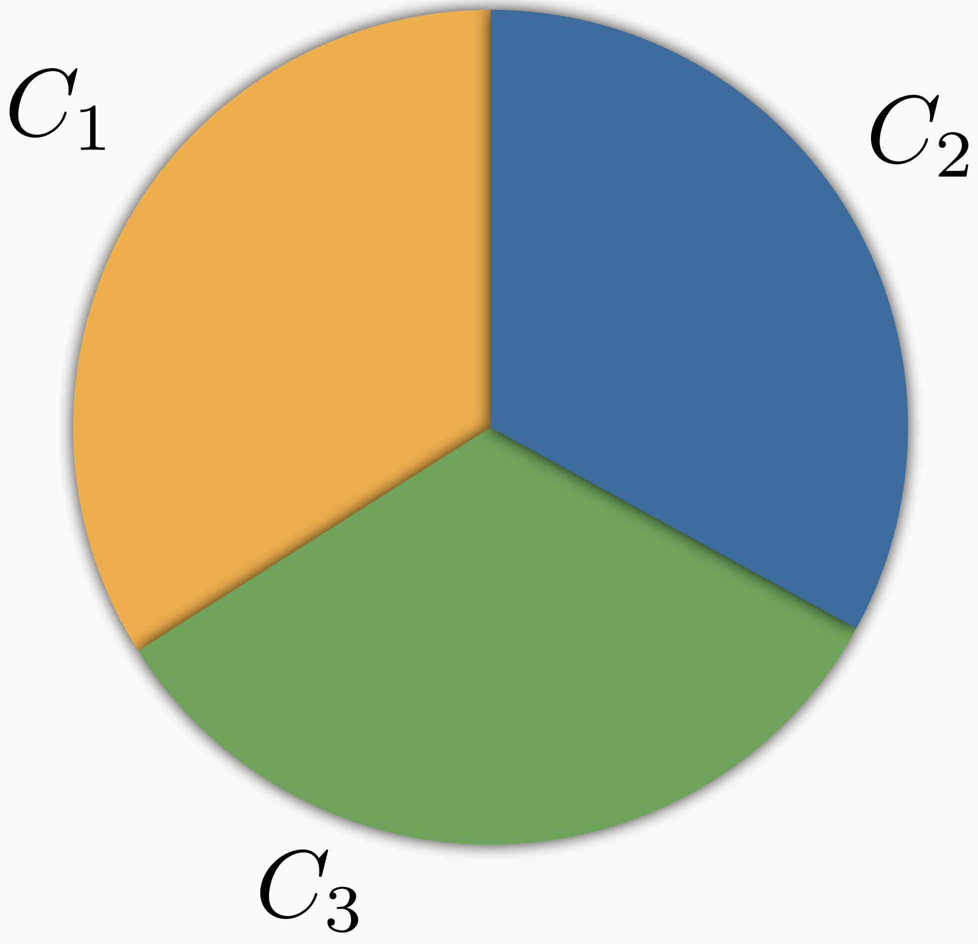
Charlene

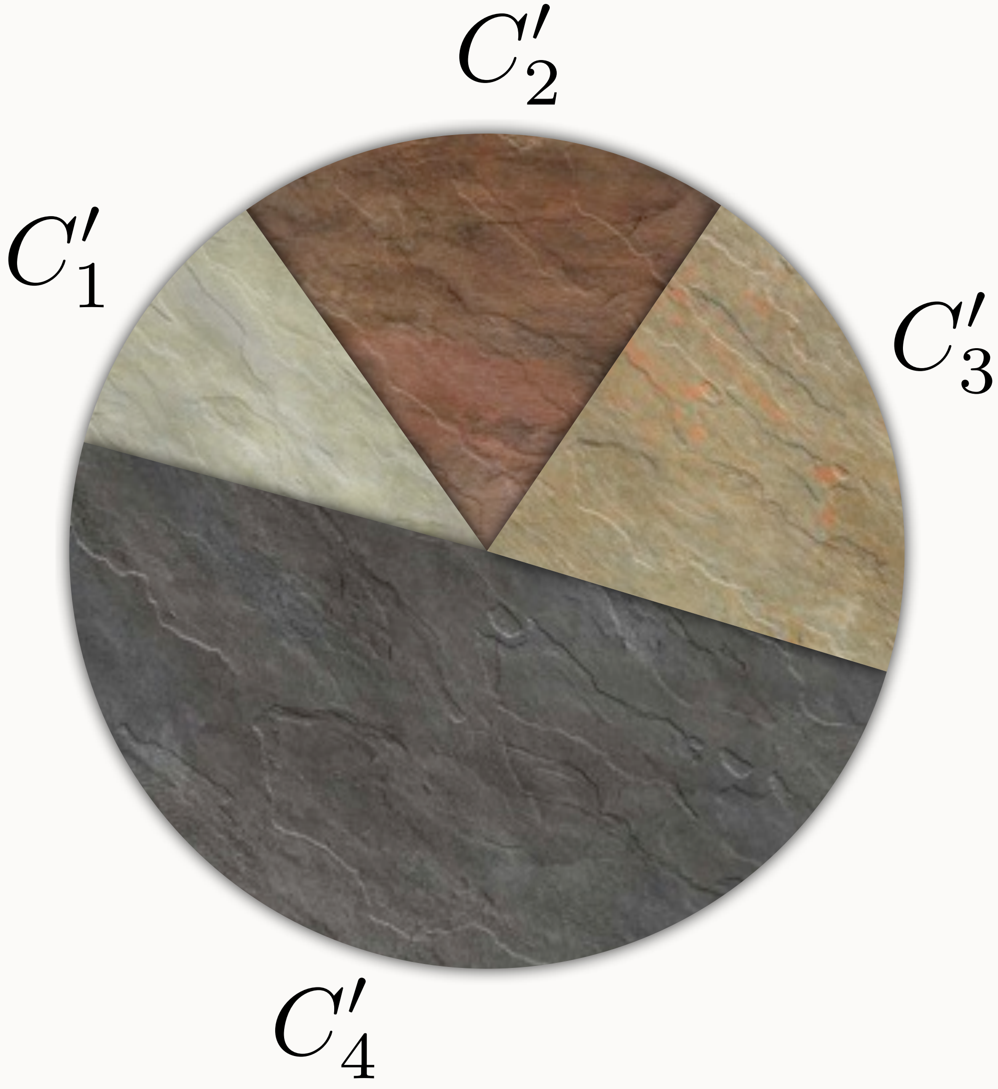
Intruder

Bob

CONSTRAINT SYSTEM

- Why sets of constraint systems are necessary ?





$$S = \{C_1; C_2; C_3\}$$

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

CONSTRAINT SYSTEM

- Previous works on constraint system

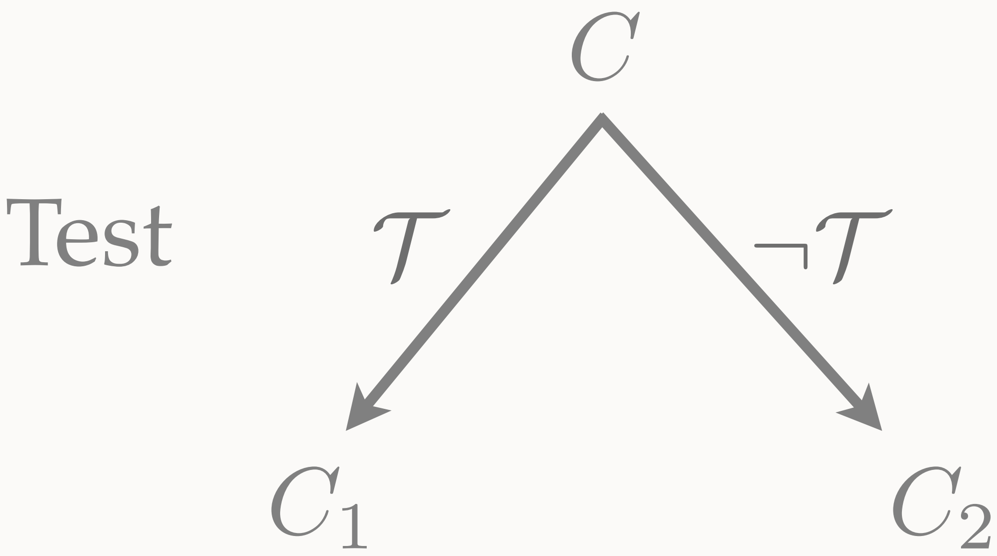
1. M. Baudet. *Sécurité des protocoles cryptographiques : aspects logiques et calculatoires.* Phd thesis
2. Y. Chevalier and M. Rusinowitch. *Decidability of equivalence of symbolic derivations.*
3. V. Cortier and S. Delaune. *A method for proving observational equivalence.*
4. A. Tiu and J. E. Dawson. *Automating open bisimulation checking for the spi calculus.*
5. V. Cheval, H. Comon-Lundh, S. Delaune. *Automating security analyss: symbolic equivalence of constraint systems*

Focus on :

- symbolic equivalence between two constraint systems (All)
- positive constraint system (no disequations) (All)
- subterm convergent equational theory (1,2 & 3)
- more restricted equational theory (4 & 5)

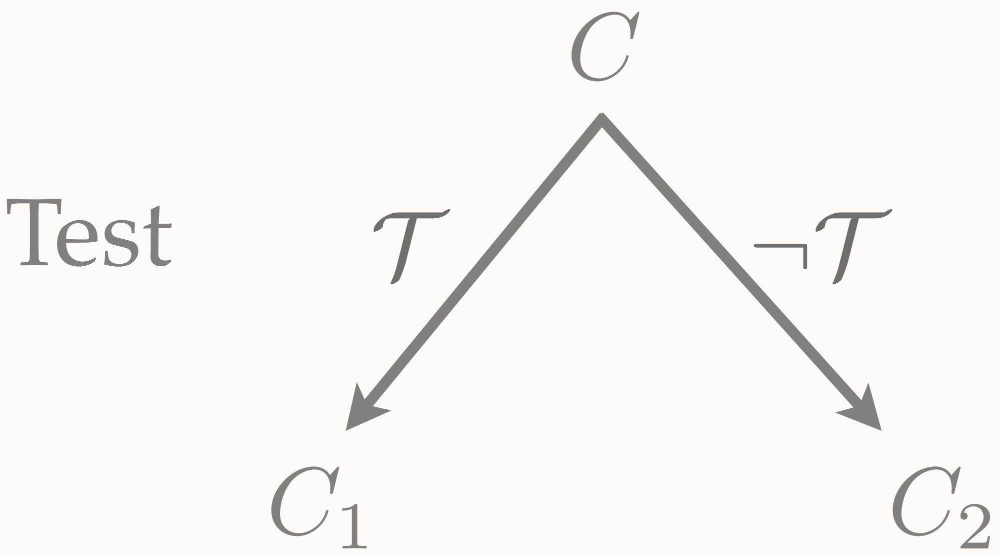
THE ALGORITHM

- Set of rules



THE ALGORITHM

- Set of rules



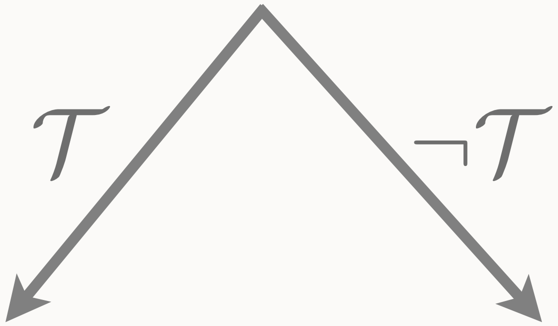
C

Test $\mathcal{T}$ $\neg\mathcal{T}$

C_1 C_2

- How to apply the rules :

$$\{C^1;\ C^2;\ \ldots\} \approx \{C^n;\ \ldots\}$$

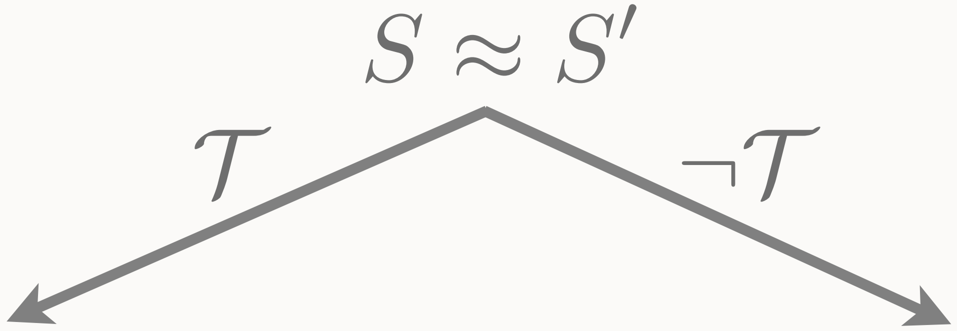


$\mathcal{T}$ $\neg\mathcal{T}$

$$\{C_1^1;\ C_1^2;\ \ldots\} \approx \{C_1^n;\ \ldots\} \qquad \{C_2^1;\ C_2^2;\ \ldots\} \approx \{C_2^n;\ \ldots\}$$

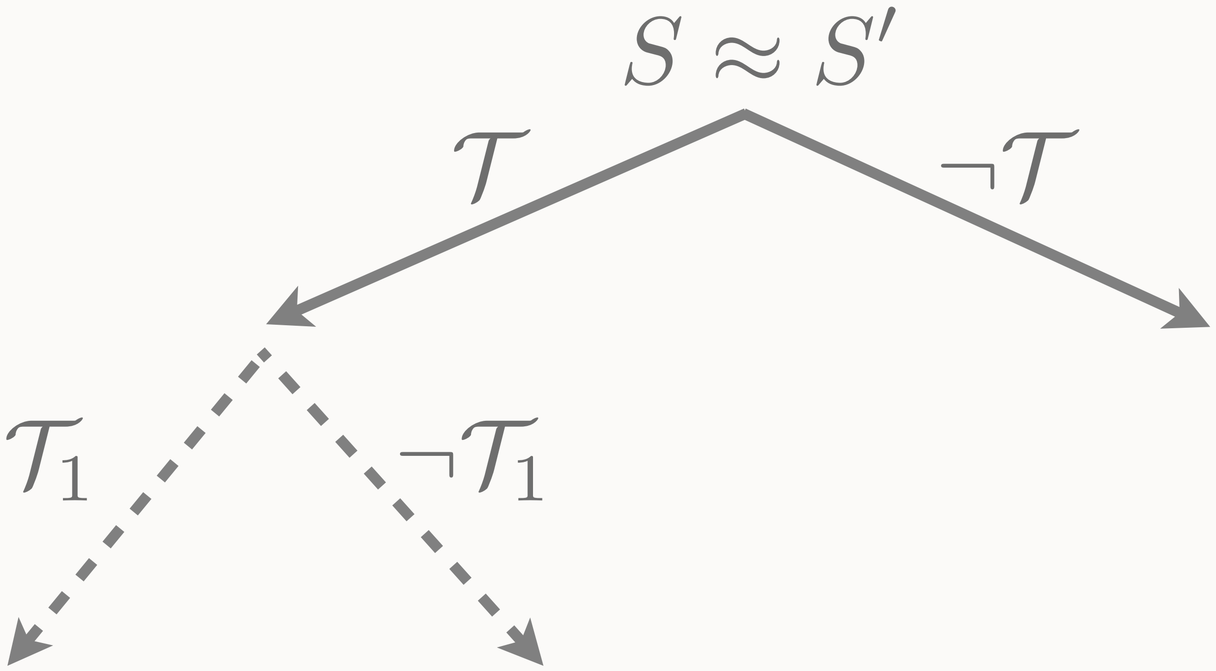
THE ALGORITHM

- A complete execution



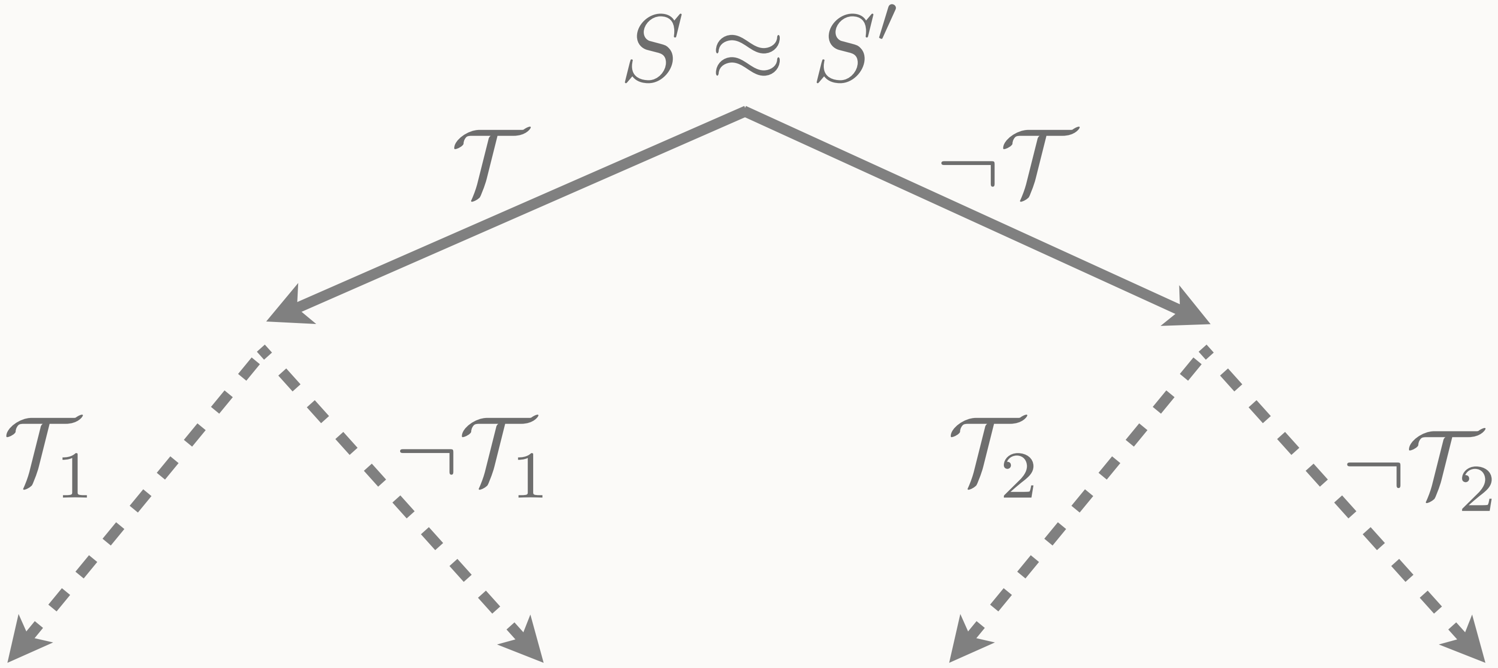
THE ALGORITHM

- A complete execution



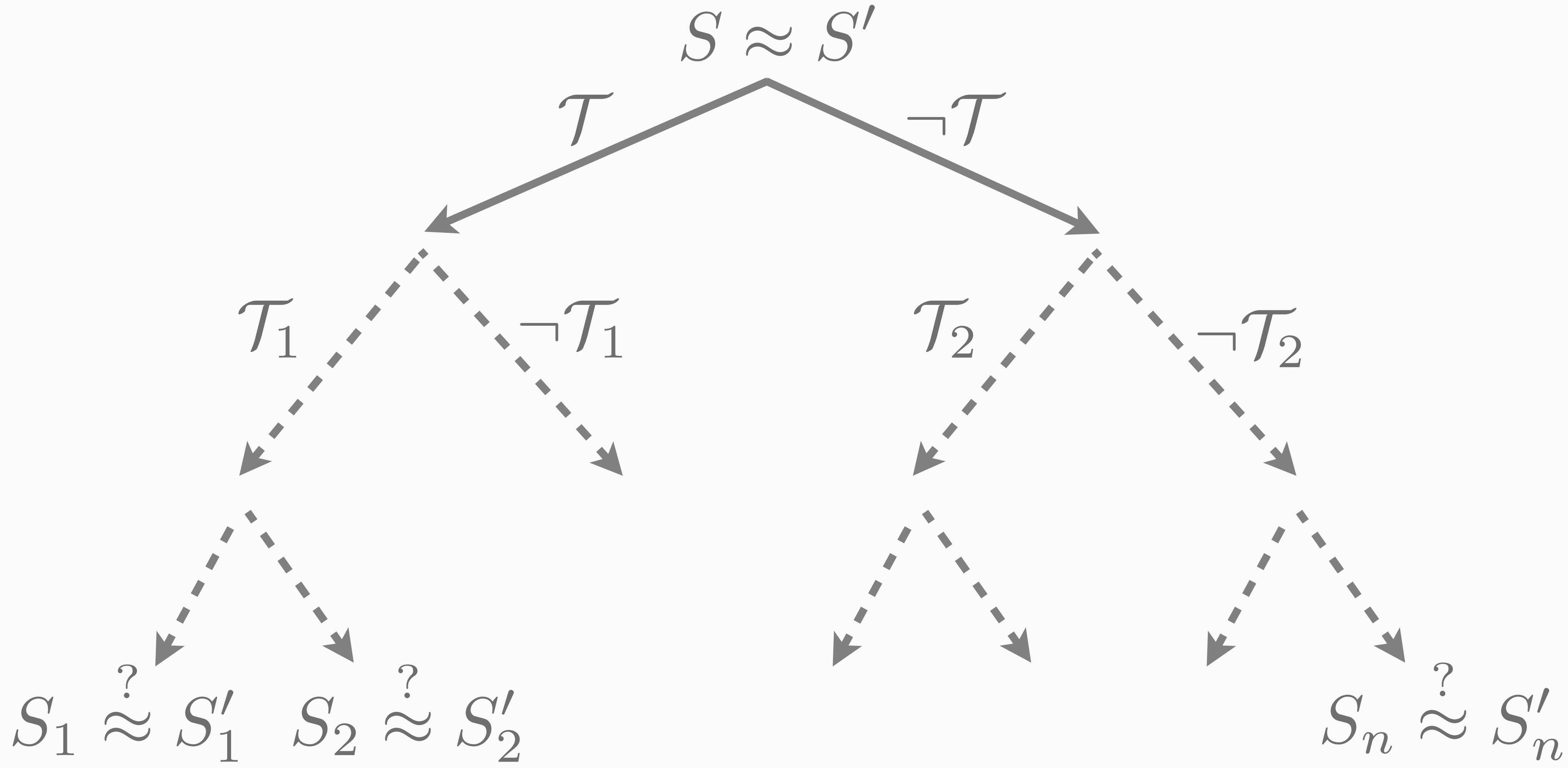
THE ALGORITHM

- A complete execution



THE ALGORITHM

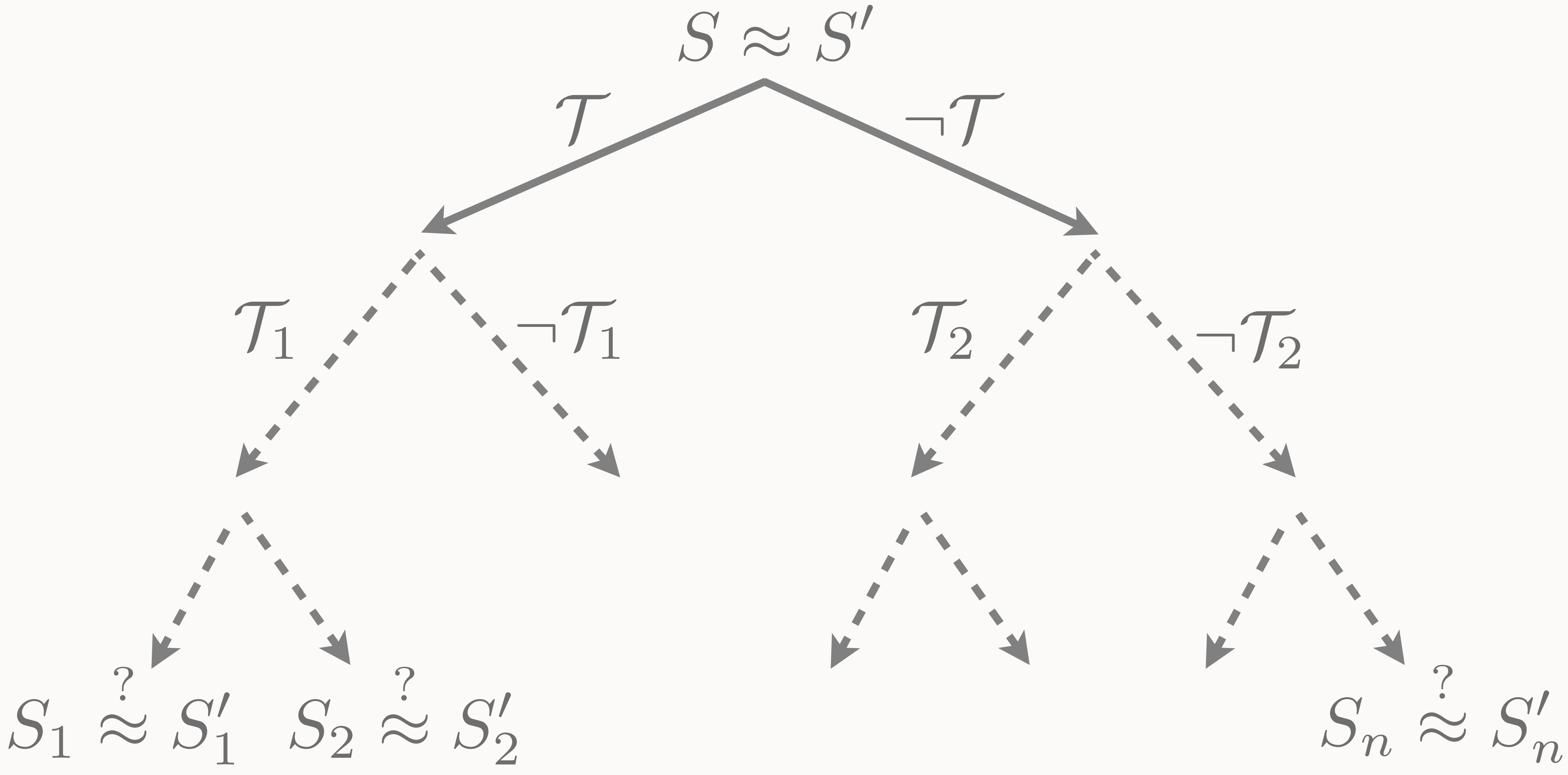
- A complete execution



The application of the rules creates a binary tree where each node is a pair of sets of constraint systems

THE ALGORITHM

- A complete execution



The symbolic equivalence is syntactically decided on each leaf

THE ALGORITHM

- The solved form difficulties
  - Existence of solutions (Reachability)

$$\boxed{\begin{array}{l} m_1, \ldots, m_n \vdash x \\ m_1, \ldots, m_n, \ldots, m_{n'} \vdash y \end{array}}$$

  - Matching solutions (including disequations)

$$\boxed{\begin{array}{l} a, b \vdash x \\ a, b, c \vdash y \\ x \neq y \end{array}} \qquad \boxed{\begin{array}{l} a, b \vdash x \\ a, b, c \vdash y \\ x \neq f(y) \end{array}}$$

  - Static equivalence

$$\boxed{\begin{array}{l} a, \{b\}_c \vdash x \\ a, \{b\}_c, c \vdash y \end{array}} \qquad \boxed{\begin{array}{l} a, b \vdash x \\ a, b, c \vdash y \end{array}}$$

RESULT

Let (S_0, S_0') be an initial pair of set of constraint systems, we have :

(S, S')

(S, S')

RESULT

Let (S_0, S'_0) be an initial pair of set of constraint systems, we have :

If all leaves (S, S') on the tree satisfy the testing condition then $S_0 \approx S'_0$.

(S, S')

RESULT

Let (S_0, S_0') be an initial pair of set of constraint systems, we have :

If all leaves (S, S') on the tree satisfy the testing condition then $S_0 \approx S_0'$.

If $S_0 \approx S_0'$ then all leaves (S, S') on the tree satisfy the testing condition.

RESULT

Let (S_0, S'_0) be an initial pair of set of constraint systems, we have :

If all leaves (S, S') on the tree satisfy the testing condition then $S_0 \approx S'_0$.

If $S_0 \approx S'_0$ then all leaves (S, S') on the tree satisfy the testing condition.

The strategy terminates

FUTURE WORK

- Contribution

Decision procedure for trace equivalence

- Infinitely many traces are represented by symbolic constraint system

+ Protocol possibly non-determinist and with non trivial else branches

+ Private channels

- Fixed set of cryptographic primitives : symmetric and asymmetric encryption, pairing and signature

- Bounded number of sessions (no replication in the process algebra)

- Future work
  - Experiment shows that the implementation is not efficient enough
  - More cryptographic primitives
  - Link with ProVerif

TERMINATION

- The disequations problem

$$\begin{array}{rl} & a, b \vdash x_1 \\ D: & a, b \vdash x_2 \\ & a, b \vdash y \end{array}$$

$$E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle$$

TERMINATION

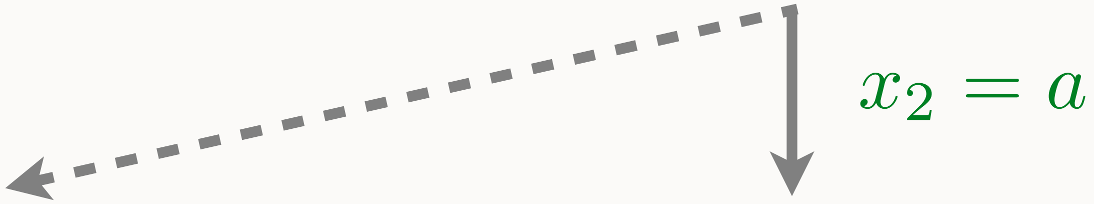
- The disequations problem

$$E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle$$

TERMINATION

- The disequations problem

$$E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b\rangle$$



$x_2 = a$

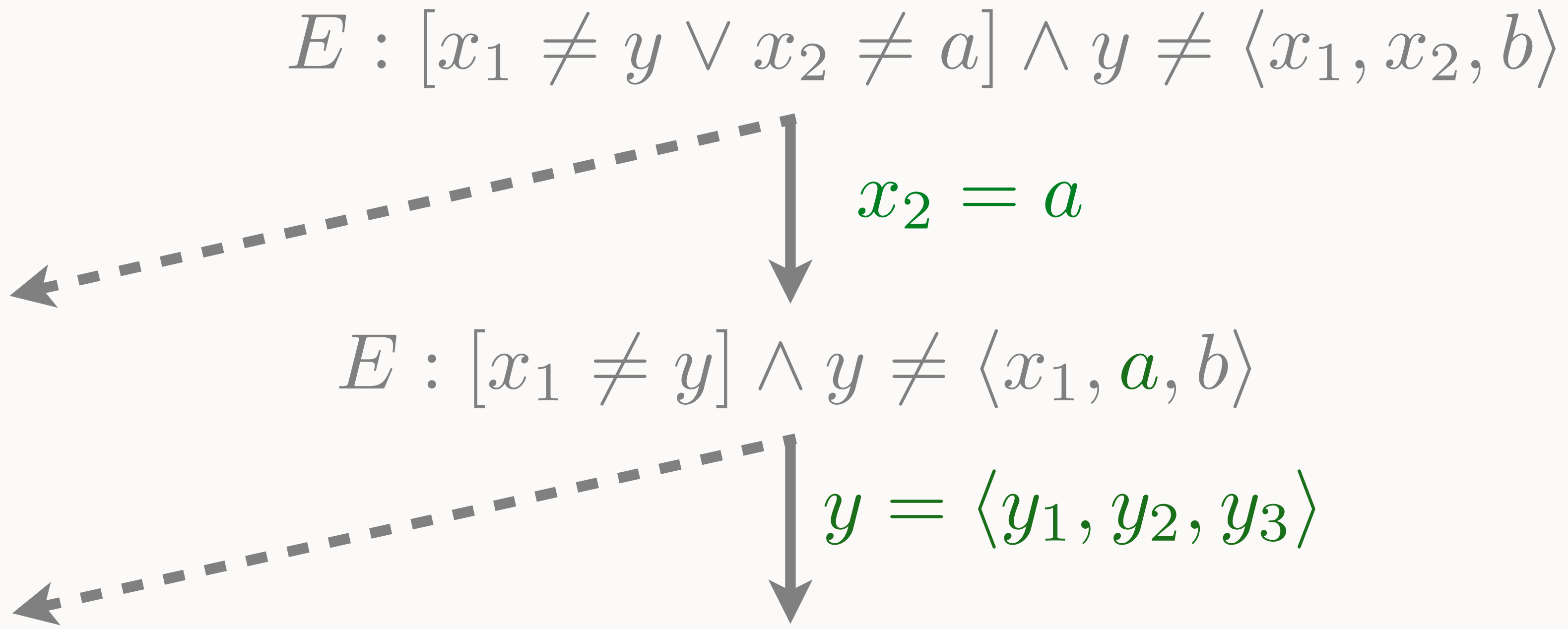
TERMINATION

- The disequations problem

$$\begin{tikzcd} & E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle \arrow[d, "x_2 = a"] \arrow[dl, dashed] \\ {} & E : [x_1 \neq y] \wedge y \neq \langle x_1, a, b \rangle \end{tikzcd}$$

TERMINATION

- The disequations problem



$$E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle$$

$$x_2 = a$$

$$E : [x_1 \neq y] \wedge y \neq \langle x_1, a, b \rangle$$

$$y = \langle y_1, y_2, y_3 \rangle$$

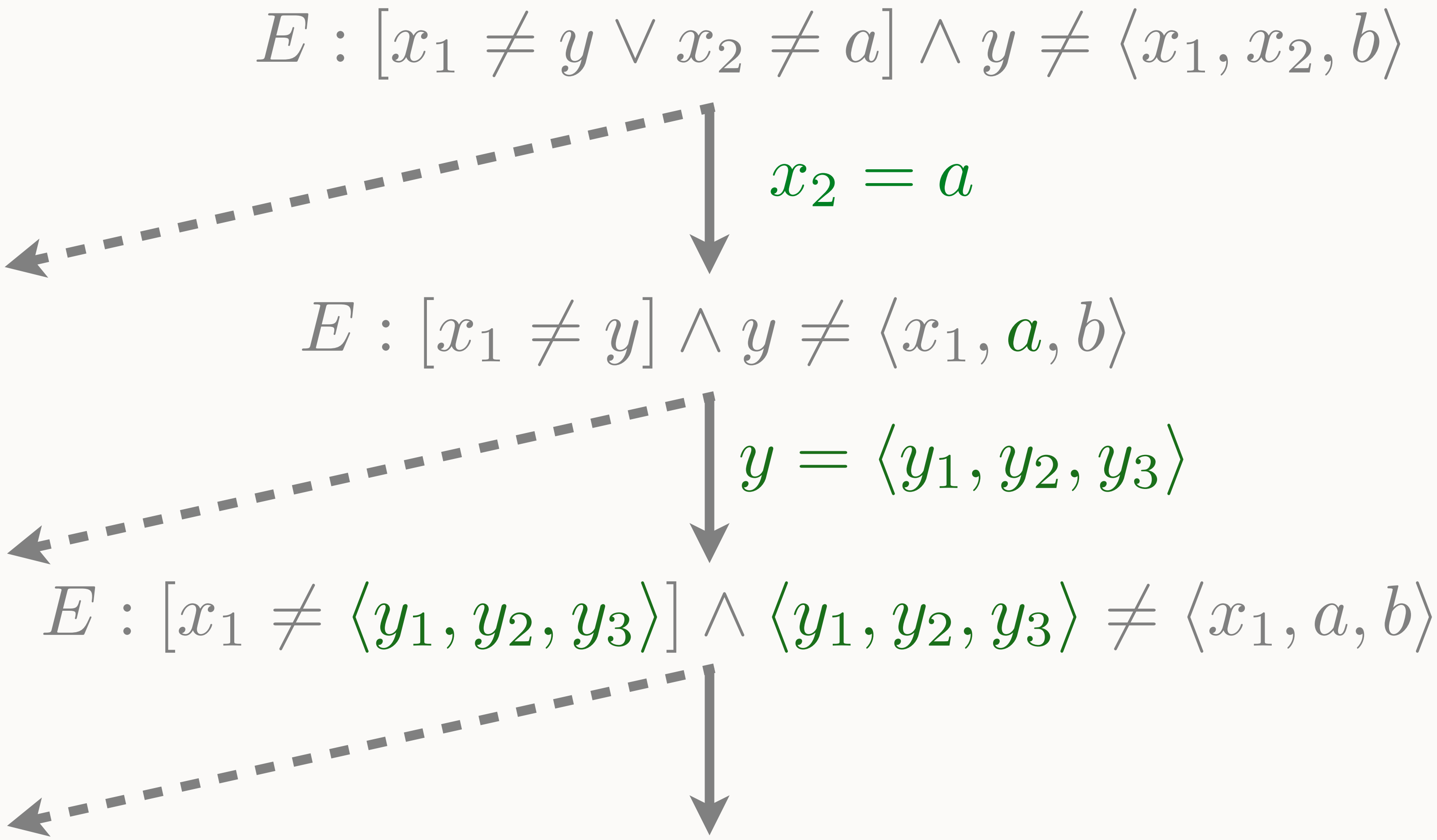
TERMINATION

- The disequations problem

$$\begin{tikzcd}
{} & E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle \arrow[d, "x_2 = a"] \arrow[dl, dashed] \\
{} & E : [x_1 \neq y] \wedge y \neq \langle x_1, a, b \rangle \arrow[d, "y = \langle y_1, y_2, y_3 \rangle"] \arrow[dl, dashed] \\
{} & E : [x_1 \neq \langle y_1, y_2, y_3 \rangle] \wedge \langle y_1, y_2, y_3 \rangle \neq \langle x_1, a, b \rangle
\end{tikzcd}$$

TERMINATION

- The disequations problem



$$E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b\rangle$$

$$x_2 = a$$

$$E : [x_1 \neq y] \wedge y \neq \langle x_1, a, b\rangle$$

$$y = \langle y_1, y_2, y_3\rangle$$

$$E : [x_1 \neq \langle y_1, y_2, y_3\rangle] \wedge \langle y_1, y_2, y_3\rangle \neq \langle x_1, a, b\rangle$$

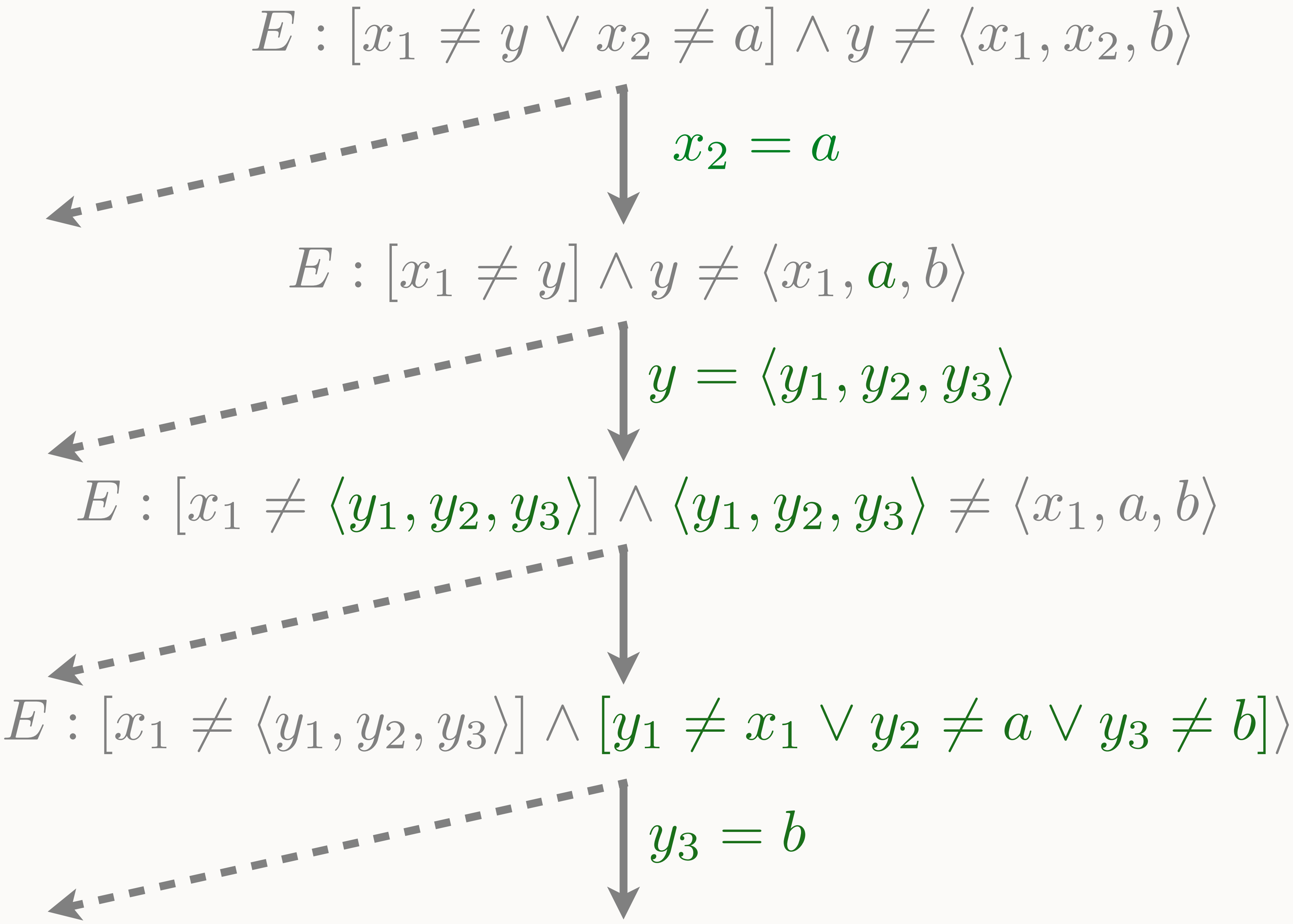
TERMINATION

- The disequations problem

$$\begin{tikzcd}
 & E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle \arrow[d, "x_2 = a"] \arrow[dl, dashed] \\
{} & E : [x_1 \neq y] \wedge y \neq \langle x_1, a, b \rangle \arrow[d, "y = \langle y_1, y_2, y_3 \rangle"] \arrow[dl, dashed] \\
{} & E : [x_1 \neq \langle y_1, y_2, y_3 \rangle] \wedge \langle y_1, y_2, y_3 \rangle \neq \langle x_1, a, b \rangle \arrow[d] \arrow[dl, dashed] \\
{} & E : [x_1 \neq \langle y_1, y_2, y_3 \rangle] \wedge [y_1 \neq x_1 \vee y_2 \neq a \vee y_3 \neq b]\rangle
\end{tikzcd}$$

TERMINATION

- The disequations problem



$$E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b\rangle$$

$$x_2 = a$$

$$E : [x_1 \neq y] \wedge y \neq \langle x_1, \mathbf{a}, b\rangle$$

$$y = \langle y_1, y_2, y_3\rangle$$

$$E : [x_1 \neq \langle y_1, y_2, y_3\rangle] \wedge \langle y_1, y_2, y_3\rangle \neq \langle x_1, a, b\rangle$$

$$E : [x_1 \neq \langle y_1, y_2, y_3\rangle] \wedge [y_1 \neq x_1 \vee y_2 \neq a \vee y_3 \neq b]\rangle$$

$$y_3 = b$$

TERMINATION

- The disequations problem

$$\begin{tikzcd}
{} & {E : [x_1 \neq y \vee x_2 \neq a] \wedge y \neq \langle x_1, x_2, b \rangle} \arrow[d, "x_2 = a"] \arrow[dl, dashed] \\
{} & {E : [x_1 \neq y] \wedge y \neq \langle x_1, a, b \rangle} \arrow[d, "{y = \langle y_1, y_2, y_3 \rangle}"] \arrow[dl, dashed] \\
{} & {E : [x_1 \neq \langle y_1, y_2, y_3 \rangle] \wedge \langle y_1, y_2, y_3 \rangle \neq \langle x_1, a, b \rangle} \arrow[d] \arrow[dl, dashed] \\
{} & {E : [x_1 \neq \langle y_1, y_2, y_3 \rangle] \wedge [y_1 \neq x_1 \vee y_2 \neq a \vee y_3 \neq b]\rangle} \arrow[d, "y_3 = b"] \arrow[dl, dashed] \\
{} & {E : [x_1 \neq \langle y_1, y_2, b \rangle] \wedge [y_1 \neq x_1 \vee y_2 \neq a]\rangle}
\end{tikzcd}$$