VERIFYING PRIVACY-TYPE PROPERTIES IN A MODULAR WAY

M.Arapinis (1), V.Cheval (2), S. Delaune (2)
(1) School of Computer Science, Birmingham, UK
(2) LSV, ENS Cachan, CNRS, INRIA Saclay

25th IEEE Computer Security Foundations Symposium

25 June 2012

CONTEXT

To verify security properties on protocols,
we model protocols in isolation

Protocols are never alone

Possible problems:

- Protocols may share same keys
- Protocols may share same cryptographic primitives
- Tools may not be able to prove the security property

CONTEXT

Our goal

Verifying **S** on **P** and Verifying **S** on **Q**

↓

Verifying **S** on **P** and **Q** running in parallel

where

- **P** and **Q** may share secrets and cryptographic primitives
- **S** is a security property

CONTEXT

Security properties

CONTEXT

Security properties

Reachability properties

- Secrecy, Authentication, ...

CONTEXT

Security properties

Reachability properties

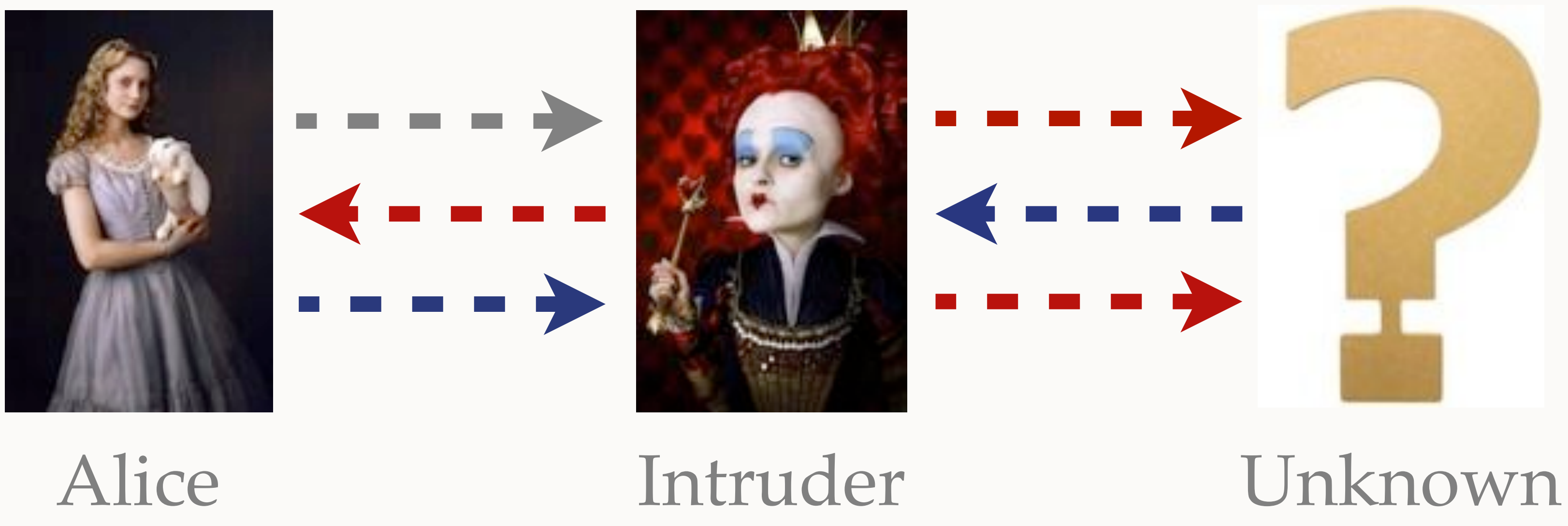
- Secrecy, Authentication, ...

Equivalence properties

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

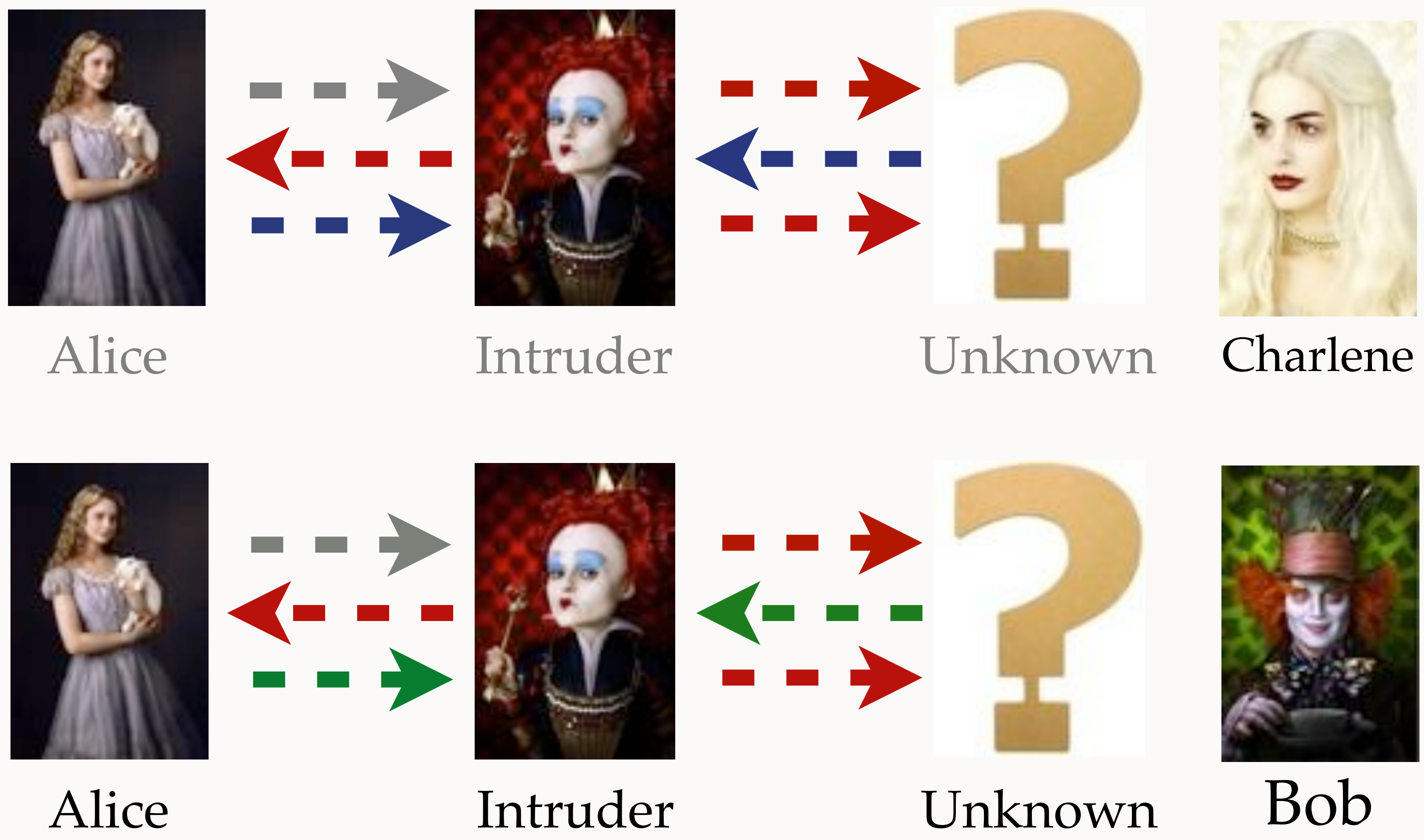
CONTEXT

Example of equivalence property : anonymity



CONTEXT

Example of equivalence property : anonymity



Can the intruder distinguish the two situations ?

PREVIOUS WORKS

- On reachability properties
  - J.D. Guttman and F.J. Thayer. *Protocol independence through disjoint encryption.*
  - S. Ciobâca and V. Cortier. *Protocol composition for arbitrary primitives.*
  - S. Andova, C. Cremers, K. Gosteen, S. Mauw. S. M. Isnes and S. Radomirovic. *A framework for compositional verification of security protocols.*

- On equivalence properties : Tagged protocol
  - S. Delaune, S. Kremer and M.D. Ryan. *Composition of password-based protocols.*
  - C. Chevalier, S. Delaune and S. Kremer. *Transforming password protocols to compose.*

MOTIVATION

Privacy-type properties: Anonymity and unlinkability

Concrete example: e-passport protocols

- Basic Access Control (BAC) : establishes sessions keys between reader and a passport
- Passive Authentication (PA)
- Active Authentication (AA)

Passive Authentication and Active Authentication are executed in parallel

FORMALISM

Composition context for anonymity

$$P: \quad A \to S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$

FORMALISM

Composition context for anonymity

$$P: \quad A \rightarrow S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$

Definition from : M. Arapinis, T. Chothia and M. Ryan. *Analysing unlinkability and anonymity using the applied pi calculus.*

FORMALISM

Composition context for anonymity

$$P: \quad A \rightarrow S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$

$$C'[\_] \stackrel{\mathsf{def}}{=} \texttt{new}\ k_S.\ !\texttt{new}\ id_A.\ !\_$$

$$C[\_1, \_2] \stackrel{\mathsf{def}}{=} \texttt{new}\ k_S.((!\texttt{new}\ id_A.\ !\_1)\ |!\_2)$$

$$C[P, P\{^{id_O}/_{id_A}\}] \approx C'[P]$$

Definition from : M. Arapinis, T. Chothia and M. Ryan. *Analysing unlinkability and anonymity using the applied pi calculus.*

FORMALISM

Composition context for anonymity

$$P : \quad A \rightarrow S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$

$$C'[\_] \stackrel{\mathsf{def}}{=} \mathtt{new}\ k_S.\ !\mathtt{new}\ id_A.\ !\_$$

$$C[\_1, \_2] \stackrel{\mathsf{def}}{=} \mathtt{new}\ k_S.((!\mathtt{new}\ id_A.\ !\_1) \ |!\_2)$$

$$C[P, P\{^{id_O}/_{id_A}\}] \approx C'[P]$$

$$C[Q, Q\{^{id_O}/_{id_A}\}] \approx C'[Q]$$

Definition from : M. Arapinis, T. Chothia and M. Ryan. *Analysing unlinkability and anonymity using the applied pi calculus.*

FORMALISM

Composition context for anonymity

$$P: \quad A \to S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$

$$C'[\_] \overset{\mathsf{def}}{=} \mathtt{new}\ k_S.\ !\mathtt{new}\ id_A.\ !\_$$

$$C[\_1, \_2] \overset{\mathsf{def}}{=} \mathtt{new}\ k_S.((!\mathtt{new}\ id_A.\ !\_1) \mid !\_2)$$

$$C[P, P\{^{id_O}/_{id_A}\}] \approx C'[P]$$

$$C[Q, Q\{^{id_O}/_{id_A}\}] \approx C'[Q]$$

$$C[Q \mid P, (Q \mid P)\{^{id_O}/_{id_A}\}] \approx C'[Q \mid P]$$

Definition from : M. Arapinis, T. Chothia and M. Ryan. *Analysing unlinkability and anonymity using the applied pi calculus.*

CONDITIONS

No shared key revealed

$$P: \quad A \rightarrow S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$
$$Q: \quad S \rightarrow A : k_S$$

P preserves the anonymity of A
Q preserves the anonymity of A

$P \mid Q$ does not preserve the anonymity of A

CONDITIONS

Tag shared cryptographic primitives

$$P: \quad A \to S : \{id_A\}^r_{\mathsf{pk}(k_S)}$$

$$Q: \quad A \to S : \{N_a\}^r_{\mathsf{pk}(k_S)}$$
$$S \to A : N_a$$

P preserves the anonymity of A
Q preserves the anonymity of A

$P \mid Q$ does not preserve the anonymity of A

CONDITIONS

Public key revealed at the beginning

$$P_i : \quad A \rightarrow S : \{\mathsf{tag}_a(id_i)\}_{\mathsf{pk}(k_S)}$$

$$Q : \quad S \rightarrow A : \mathsf{pk}(k_S)$$

$$C[\_] \overset{\mathsf{def}}{=} \mathtt{new}\ k_S.\ \_$$

CONDITIONS

Public key revealed at the beginning

$$P_i : \quad A \rightarrow S : \{\mathsf{tag}_a(id_i)\}_{\mathsf{pk}(k_S)}$$

$$Q : \quad S \rightarrow A : \mathsf{pk}(k_S)$$

$$C[\_] \stackrel{\mathsf{def}}{=} \mathtt{new}\ k_S.\ \_$$

$$C[P_1] \approx C[P_2] \quad \text{and} \quad C[Q] \approx C[Q]$$

But $C[P_1 \mid Q] \not\approx C[P_2 \mid Q]$

MAIN THEOREM

$$\frac{C[P_A] \approx C'[P'_A] \qquad C[P_B] \approx C'[P'_B]}{C[P_A \mid P_B] \approx C'[P'_A \mid P'_B]}$$

If :

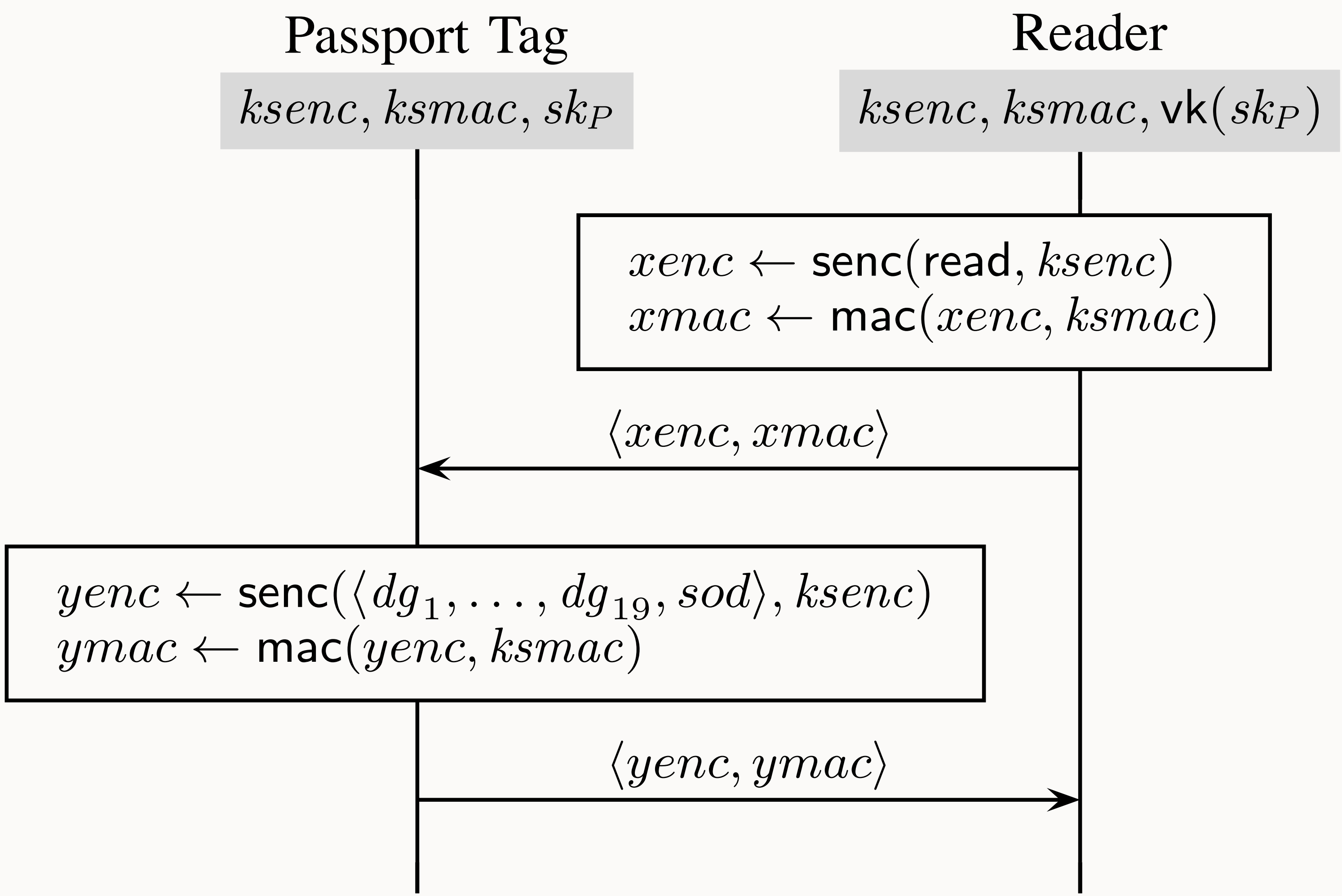
-The shared keys of C and C′ are not revealed

-The public keys are revealed at the beginning

-The protocols A and B are tagged

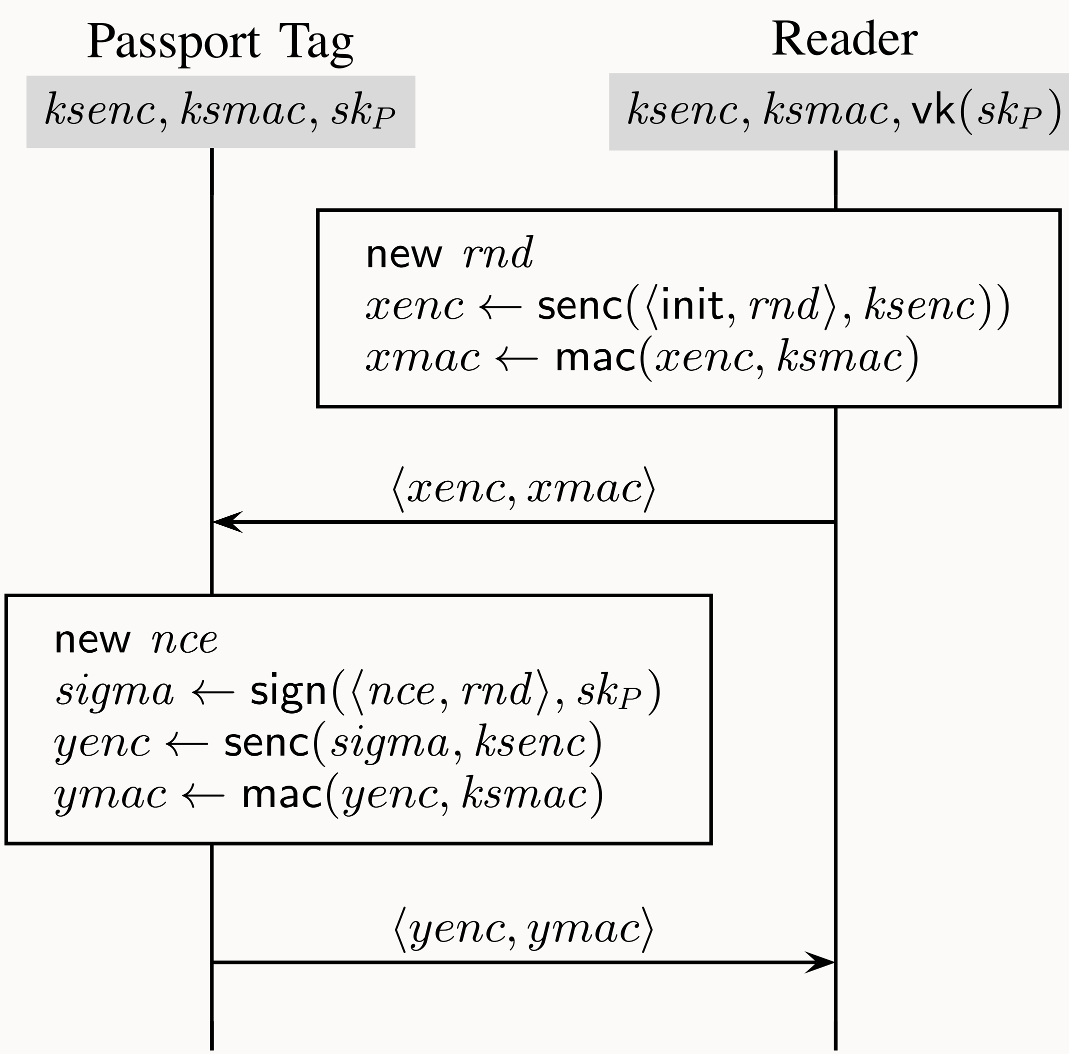
E-PASSPORT

Passive Authentication (PA)



E-PASSPORT

Active Authentication (AA)



E-PASSPORT

Result

With ProVerif,

- we prove anonymity for AA
- we can not prove anonymity for PA
- we can not prove anonymity for $PA \mid AA$

E-PASSPORT

Result

With ProVerif,

- we prove anonymity for *AA*
- we can not prove anonymity for *PA*
- we can not prove anonymity for *PA* | *AA*

> proving anonymity for *PA*
>
> implies
>
> proving anonymity for *PA* | *AA*

SKETCH OF PROOF

$C[P_A] \approx C'[P'_A]$ and $C[P_B] \approx C'[P'_B]$

SKETCH OF PROOF

$$C[P_A] \approx C'[P'_A] \quad \text{and} \quad C[P_B] \approx C'[P'_B]$$

$$\Downarrow$$

$$C[P_A] \mid C[P_B] \approx C'[P'_A] \mid C'[P'_B]$$

SKETCH OF PROOF

$C[P_A] \approx C'[P'_A]$ and $C[P_B] \approx C'[P'_B]$

↓

$$C[P_A] \mid C[P_B] \approx C'[P'_A] \mid C'[P'_B]$$

$$C[P_A \mid P_B] \approx C'[P'_A \mid P'_B]$$

SKETCH OF PROOF

$$C[P_A] \approx C'[P'_A] \quad \text{and} \quad C[P_B] \approx C'[P'_B]$$

$$\Downarrow$$

$$C[P_A] \mid C[P_B] \approx C'[P'_A] \mid C'[P'_B]$$

$$\approx$$

$$C[P_A \mid P_B]$$

SKETCH OF PROOF

$$C[P_A] \approx C'[P'_A] \quad \text{and} \quad C[P_B] \approx C'[P'_B]$$

$$\Downarrow$$

$$C[P_A] \mid C[P_B] \approx C'[P'_A] \mid C'[P'_B]$$

$$\approx$$

$$C'[P'_A \mid P'_B]$$

SKETCH OF PROOF

$$C[P_A] \approx C'[P'_A] \quad \text{and} \quad C[P_B] \approx C'[P'_B]$$

$$\Downarrow$$

$$C[P_A] \mid C[P_B] \approx C'[P'_A] \mid C'[P'_B]$$

$$\approx \qquad\qquad \approx$$

$$C[P_A \mid P_B] \approx C'[P'_A \mid P'_B]$$

SKETCH OF PROOF

$$C[P_A] \mid C[P_B] \approx C[P_A \mid P_B]$$

$$\texttt{new}\ k.[P_A \mid P_B]$$

$$\texttt{new}\ k.P_A \mid \texttt{new}\ k.P_B$$

SKETCH OF PROOF

$$C[P_A] \mid C[P_B] \approx C[P_A \mid P_B]$$

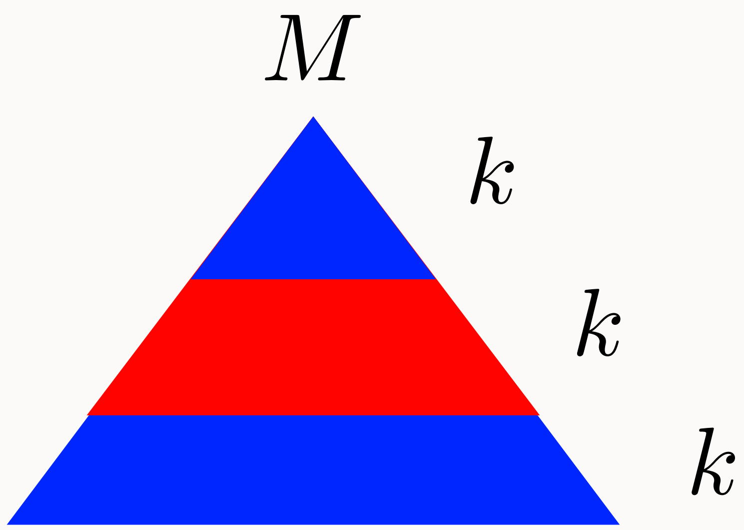
$$\mathtt{new}\ k.[P_A \mid P_B] \longrightarrow P_1 \dashrightarrow P_n$$

$$\mathtt{new}\ k.P_A \mid \mathtt{new}\ k.P_B$$

SKETCH OF PROOF

$C[P_A] \mid C[P_B] \approx C[P_A \mid P_B]$

$\mathtt{new}\ k.[P_A \mid P_B] \longrightarrow P_1 \dashrightarrow P_n$

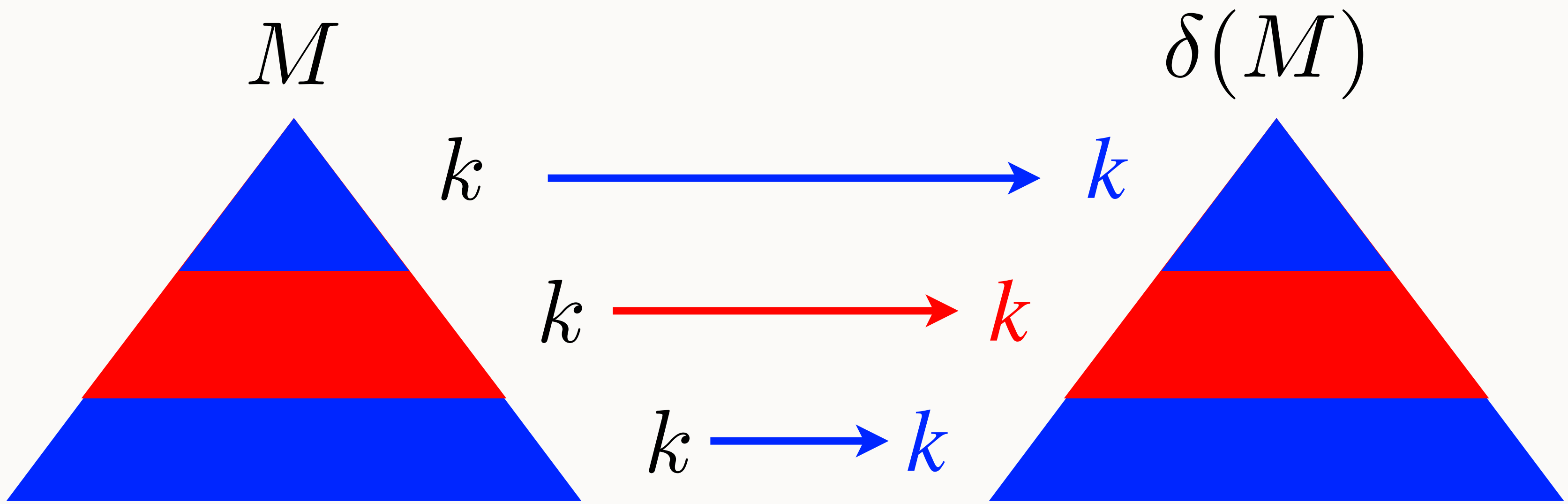


$\mathtt{new}\ k.P_A \mid \mathtt{new}\ k.P_B$

SKETCH OF PROOF

$$C[P_A] \mid C[P_B] \approx C[P_A \mid P_B]$$

$\texttt{new}\ k.[P_A \mid P_B] \longrightarrow P_1 \dashrightarrow P_n$

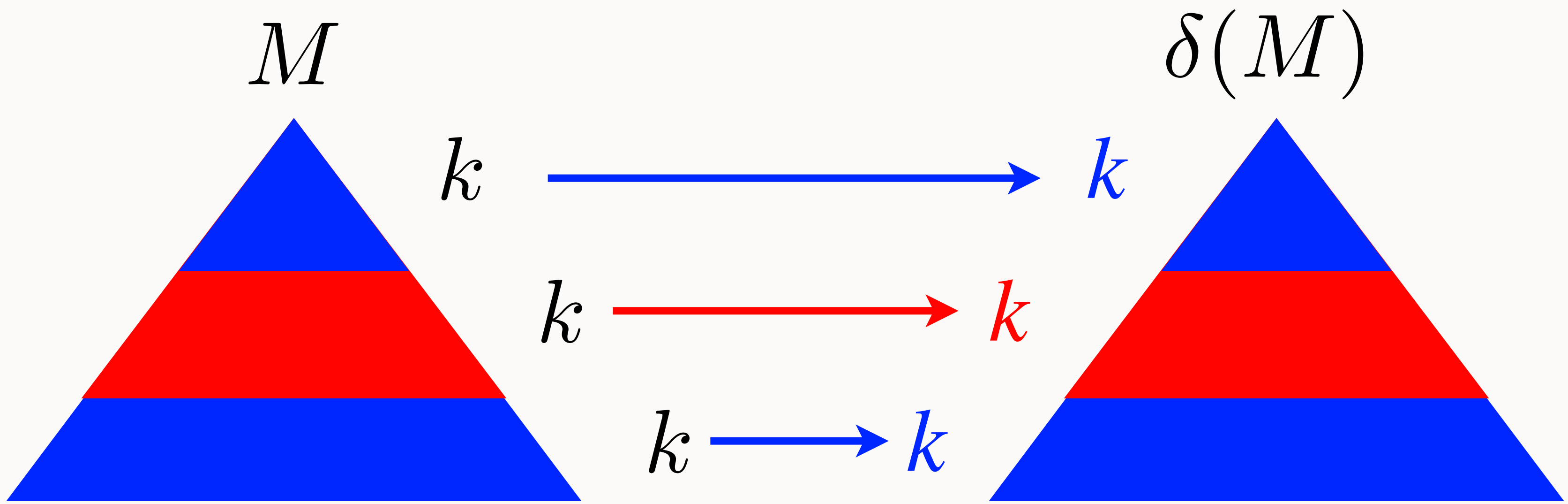


$\texttt{new}\ k.P_A \mid \texttt{new}\ k.P_B$

SKETCH OF PROOF

$C[P_A] \mid C[P_B] \approx C[P_A \mid P_B]$

$\texttt{new}\ k.[P_A \mid P_B] \longrightarrow P_1 \dashrightarrow P_n$



$\texttt{new}\ k.P_A \mid \texttt{new}\ k.P_B \longrightarrow \delta(P_1) \dashrightarrow \delta(P_n)$

CONCLUSION & FUTURE WORK

- Parallel composition theorem for equivalence properties

Conditions:

- The shared keys are not revealed
- The public keys are revealed at the beginning
- The protocols are tagged

- Future work : Sequential composition

E-passport protocols

- Basic Access Control (BAC) : establishes sessions keys between reader and a passport
- Passive Authentication (PA)
- Active Authentication (AA)

- Future work : Removing the tags

- Tags imply heavy transformation of the protocol
- Almost no current protocol tags all their message
- Protocols may behave as if they were tagged (ex: nonce exchange)