Verification of Indistinguishability Properties

Stéphanie Delaune

LSV, CNRS & ENS Cachan & INRIA Saclay Île-de-France, France

Thursday, October 11th, 2012

VIP in a nutshell

$\longrightarrow$ ANR project - programme JCJC (Jan. 2012 - Dec. 2015)

`http://www.lsv.ens-cachan.fr/Projects/anr-vip/`

Ressources

Travel + Equipment: 53,5 kE
Pôle Systematic: 10 kE **??**
1 PhD student (Rémy Chrétien)+ 1 post-doc

Permanent members:

- Stephanie Delaune (80%)
- Steve Kremer (35%)
- Graham Steel (35%)

VIP in a nutshell

$\longrightarrow$ ANR project - programme JCJC (Jan. 2012 - Dec. 2015)

`http://www.lsv.ens-cachan.fr/Projects/anr-vip/`

Ressources

Travel + Equipment: 53,5 kE
Pôle Systematic: 10 kE **??**
1 PhD student (Rémy Chrétien)+ 1 post-doc

Permanent members:

- Stephanie Delaune (80%)
- Steve Kremer (35%) $\longrightarrow$ Cassis team in Nancy since Sept. 2011
- Graham Steel (35%) $\longrightarrow$ ProSecco team in Paris since Sept. 2012

Context: cryptographic protocols

PayPal™

Cryptographic protocols

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

The network is unsecure!

Communications take place over a public network like the Internet.

Context: cryptographic protocols

PayPal™

Cryptographic protocols

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

Context: cryptographic protocols

PayPal™

Cryptographic protocols

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

It becomes more and more important to protect our privacy.

Example: electronic passport

$\longrightarrow$ studied in [Arapinis *et al.*, 10]

An electronic passport is a passport with an RFID tag embedded in it.

The RFID tag stores:

- the information printed on your passport,
- a JPEG copy of your picture.

Example: electronic passport

$\longrightarrow$ studied in [Arapinis *et al.*, 10]

An electronic passport is a passport with an RFID tag embedded in it.

The RFID tag stores:

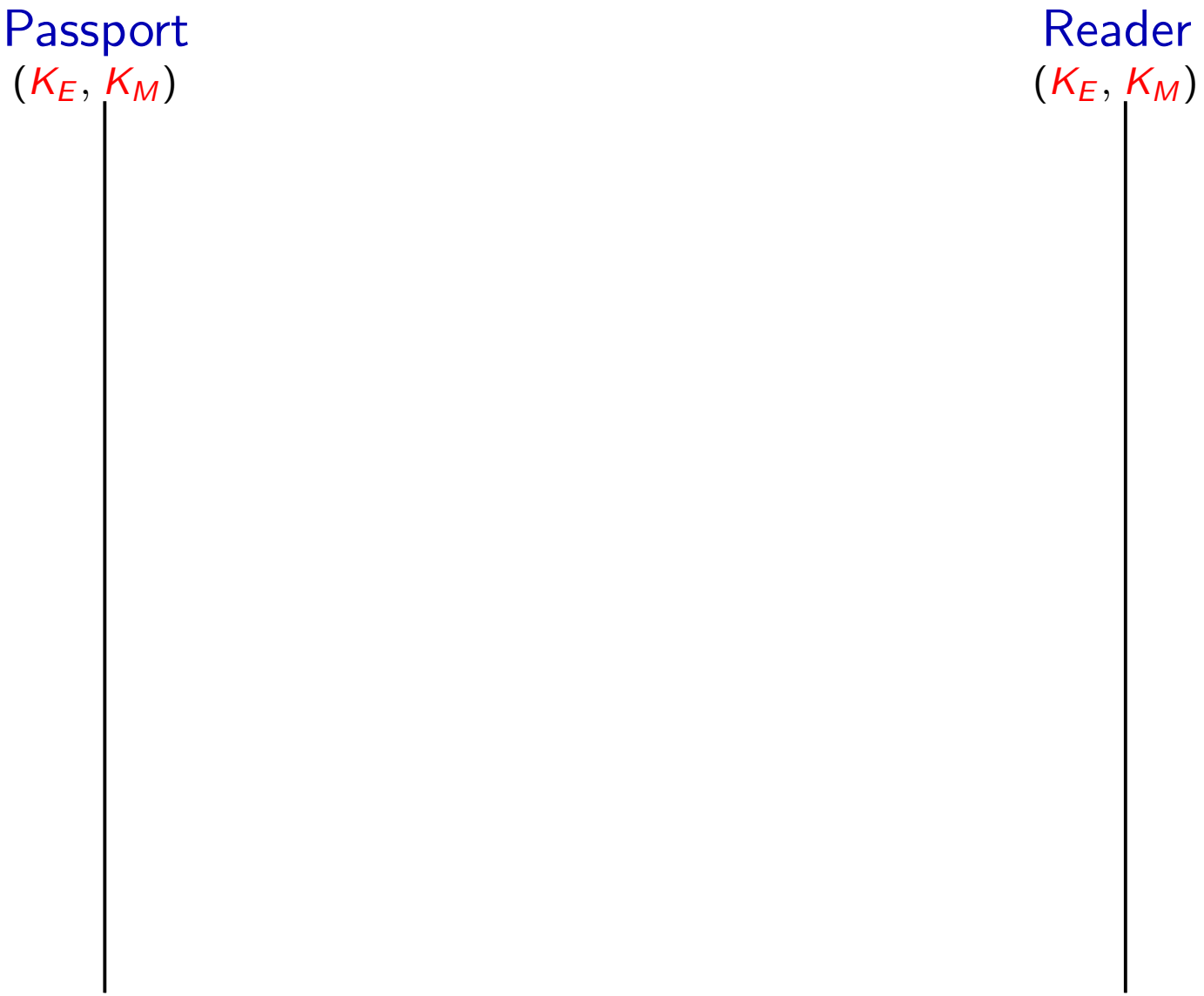
- the information printed on your passport,
- a JPEG copy of your picture.

The Basic Access Control (BAC) protocol is a key establishment protocol that has been designed to also ensure unlinkability.

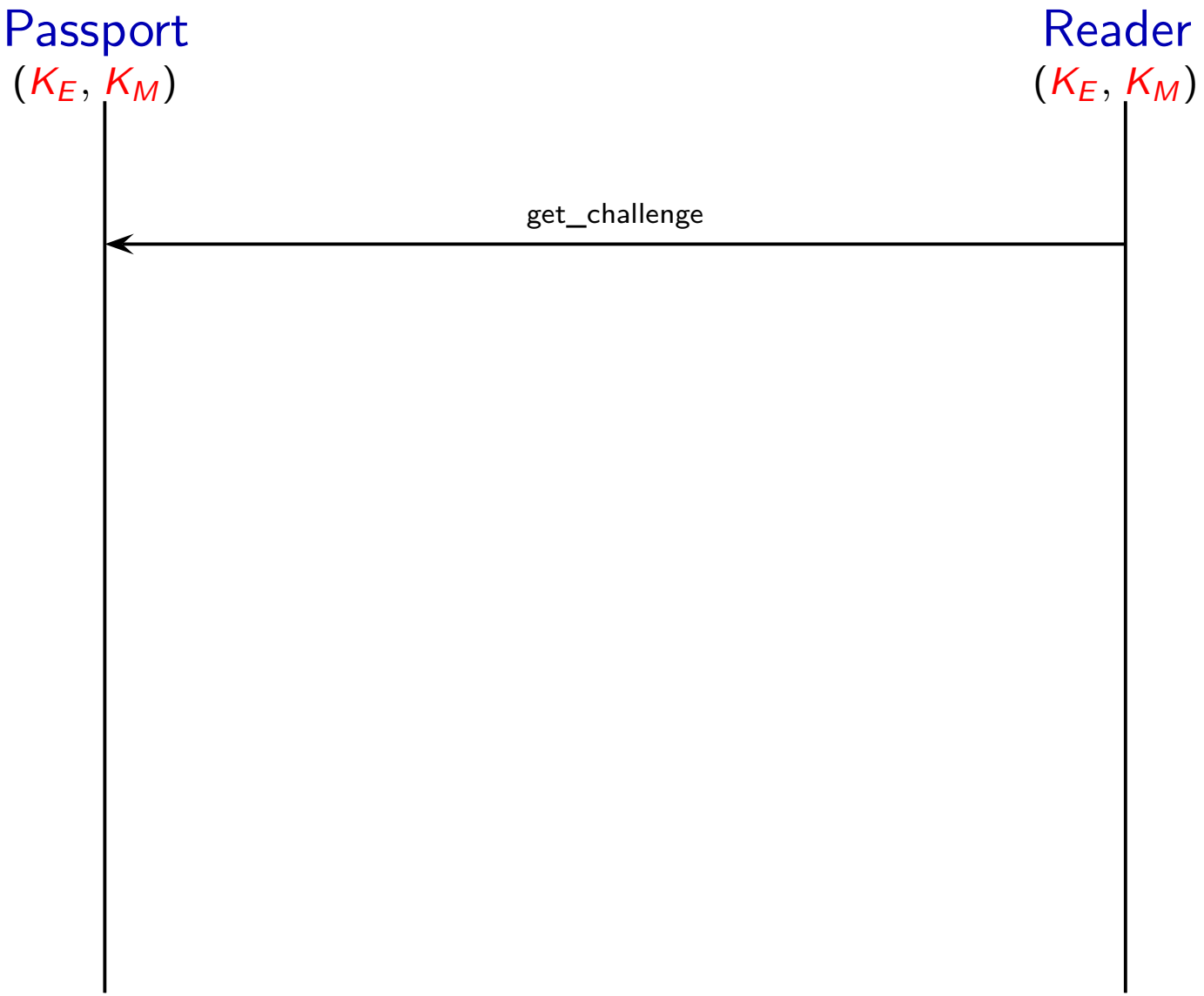
ISO/IEC standard 15408

Unlinkability aims to ensure *that a user may make multiple uses of a service or resource without others being able to link these uses together.*

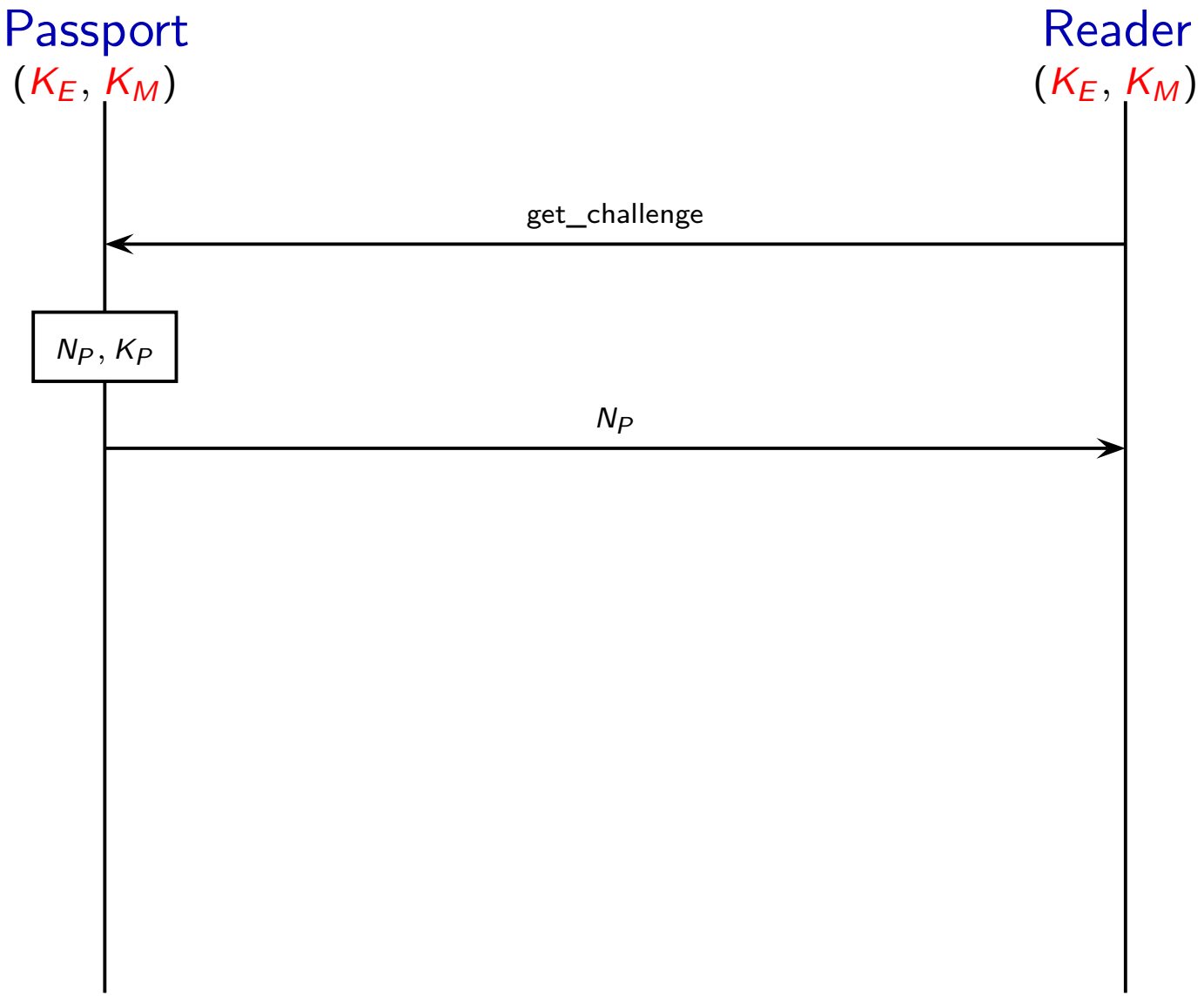
The electronic passport protocol



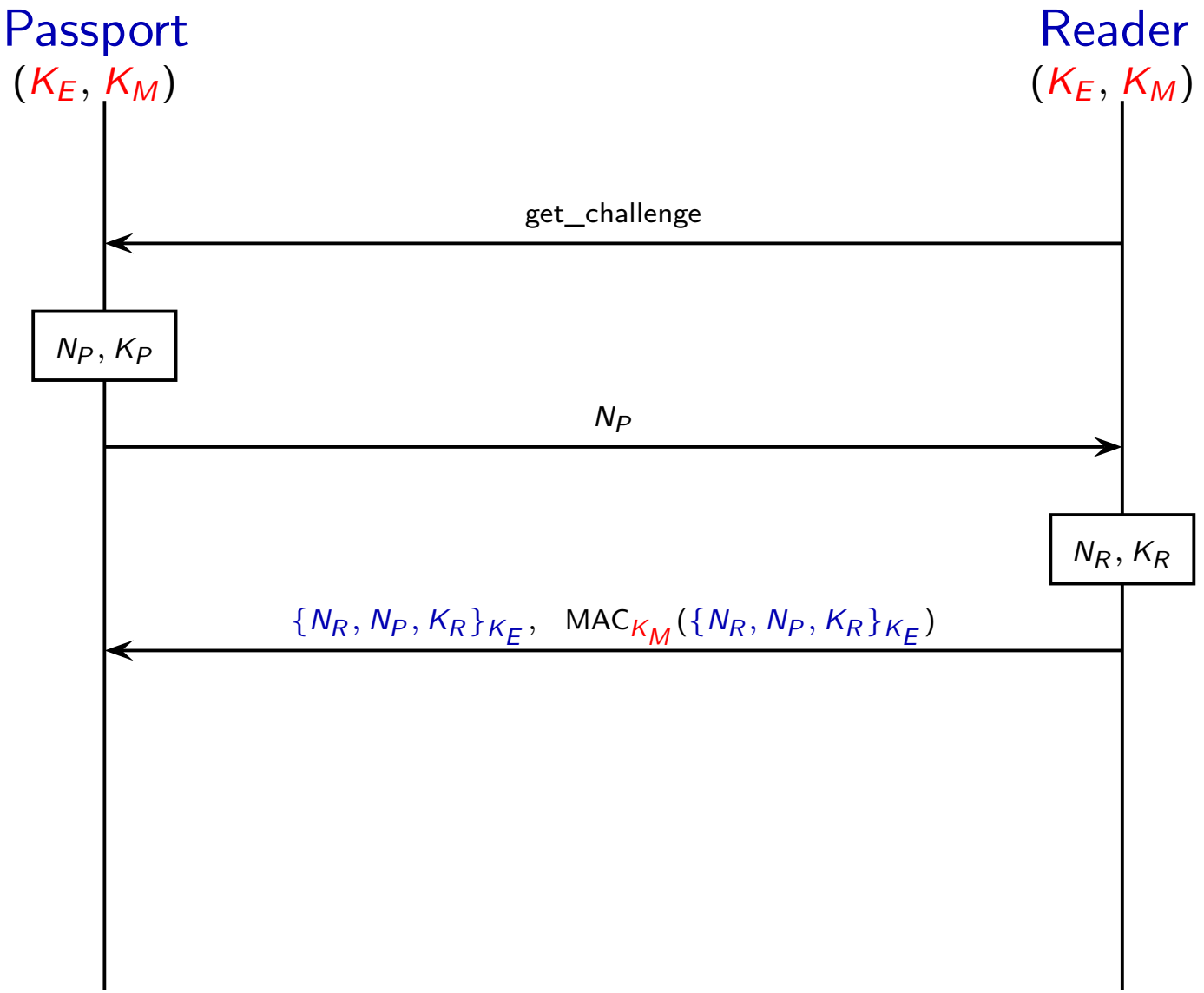
The electronic passport protocol



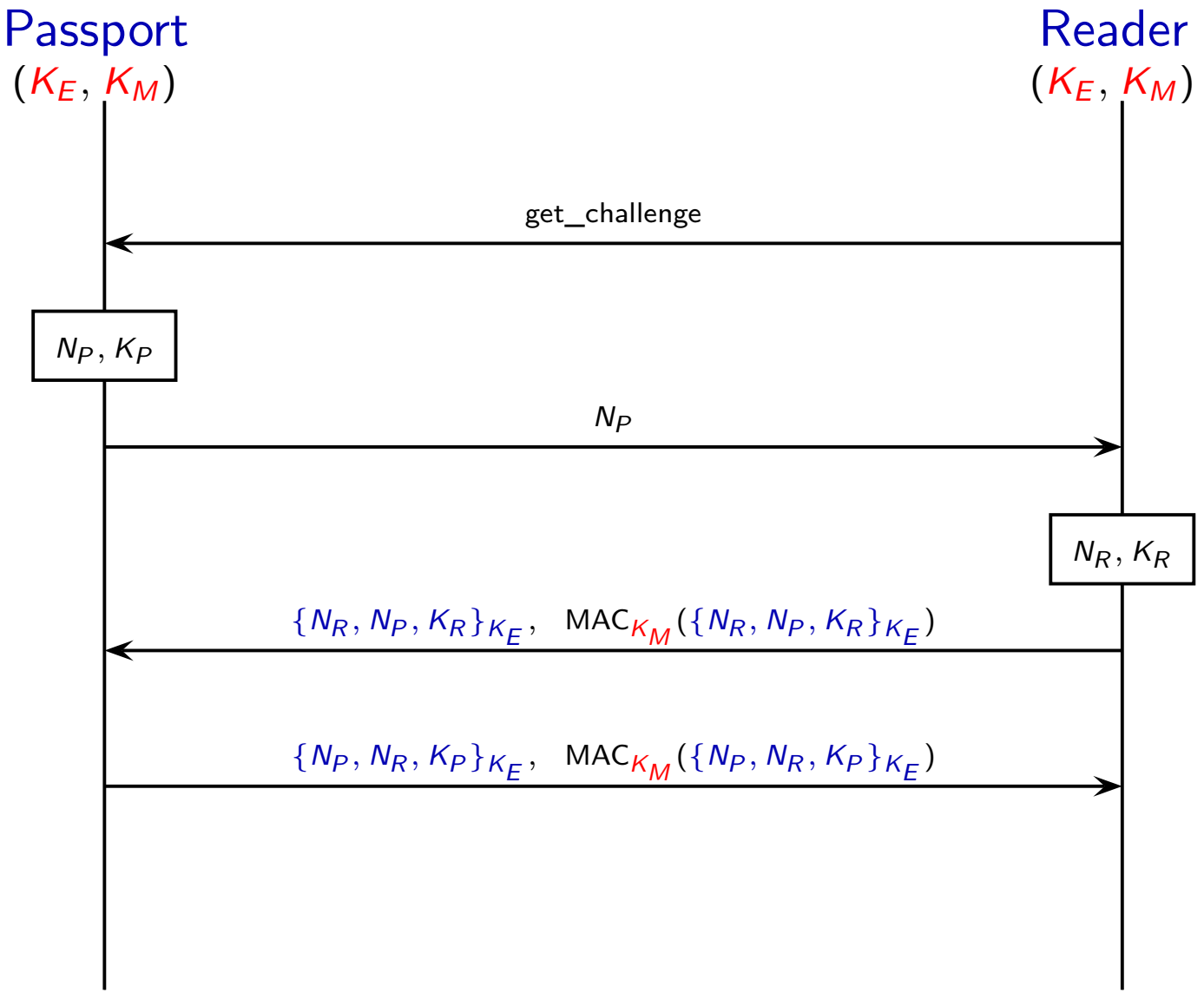
The electronic passport protocol



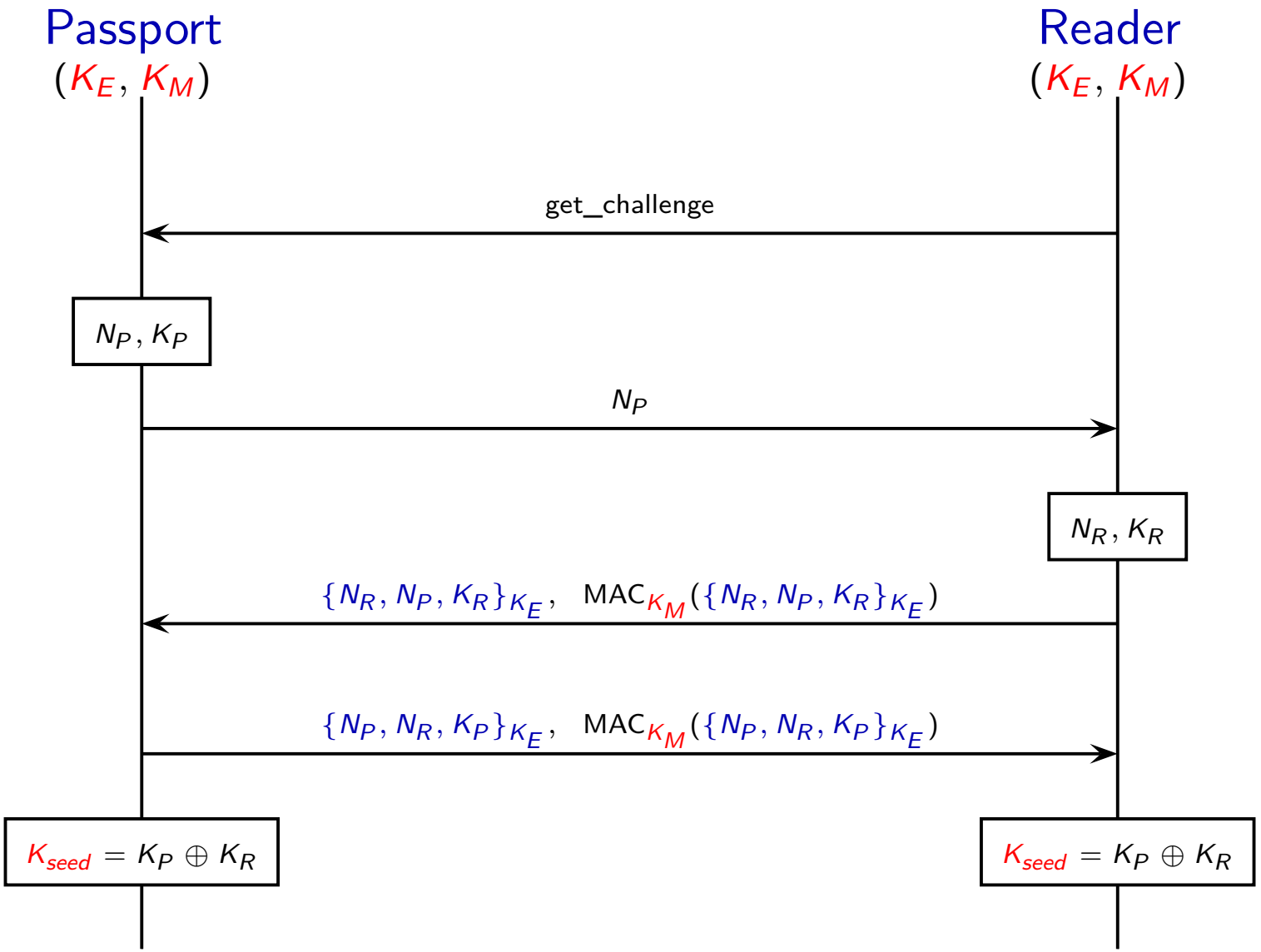
The electronic passport protocol



The electronic passport protocol



The electronic passport protocol



How cryptographic protocols can be attacked?

Some famous examples

The Serge Humpich case (1997)

He factorizes the number (320 bits) used to protect credit cards and he builds a false credit card. (the « YesCard »).

$\longrightarrow$ this makes it possible to withdraw a bank account that does not exist!

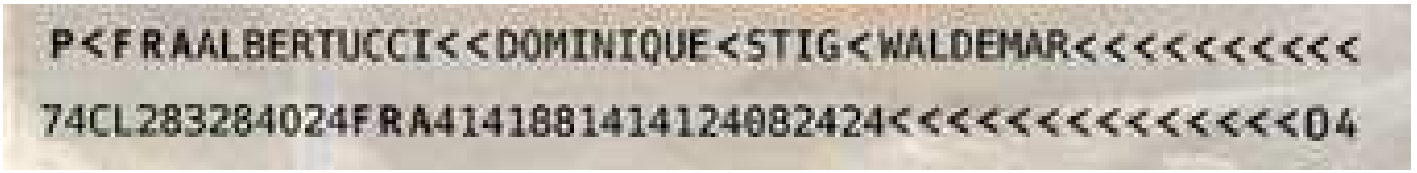
Some famous examples

The Serge Humpich case (1997)

He factorizes the number (320 bits) used to protect credit cards and he builds a false credit card. (the « YesCard »).

$\longrightarrow$ this makes it possible to withdraw a bank account that does not exist!

Attack on the Belgian e-passport (2006)



$\longrightarrow$ this makes it possible to obtain the personnal data of the user (*e.g.* the signature)

How cryptographic protocols can be attacked?

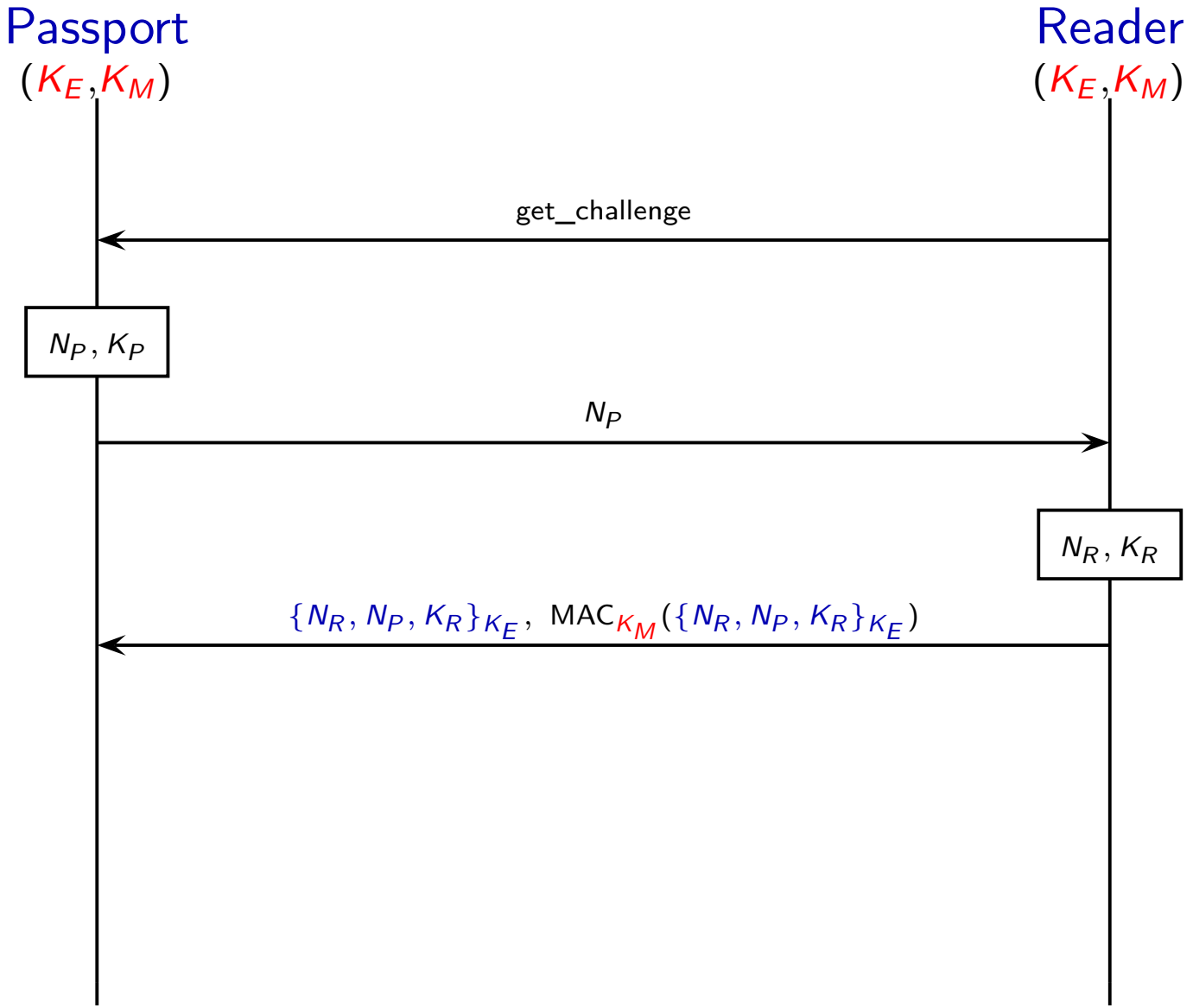
How cryptographic protocols can be attacked?

Logical attacks

- can be mounted even assuming perfect cryptography,
  $\hookrightarrow$ replay attack, man-in-the middle attack, ...
- are numerous,
  $\hookrightarrow$ a flaw discovered in 2008 in Single Sign On Protocols used in Google App (Avantssar european project)
- subtle and hard to detect by "eyeballing" the protocol

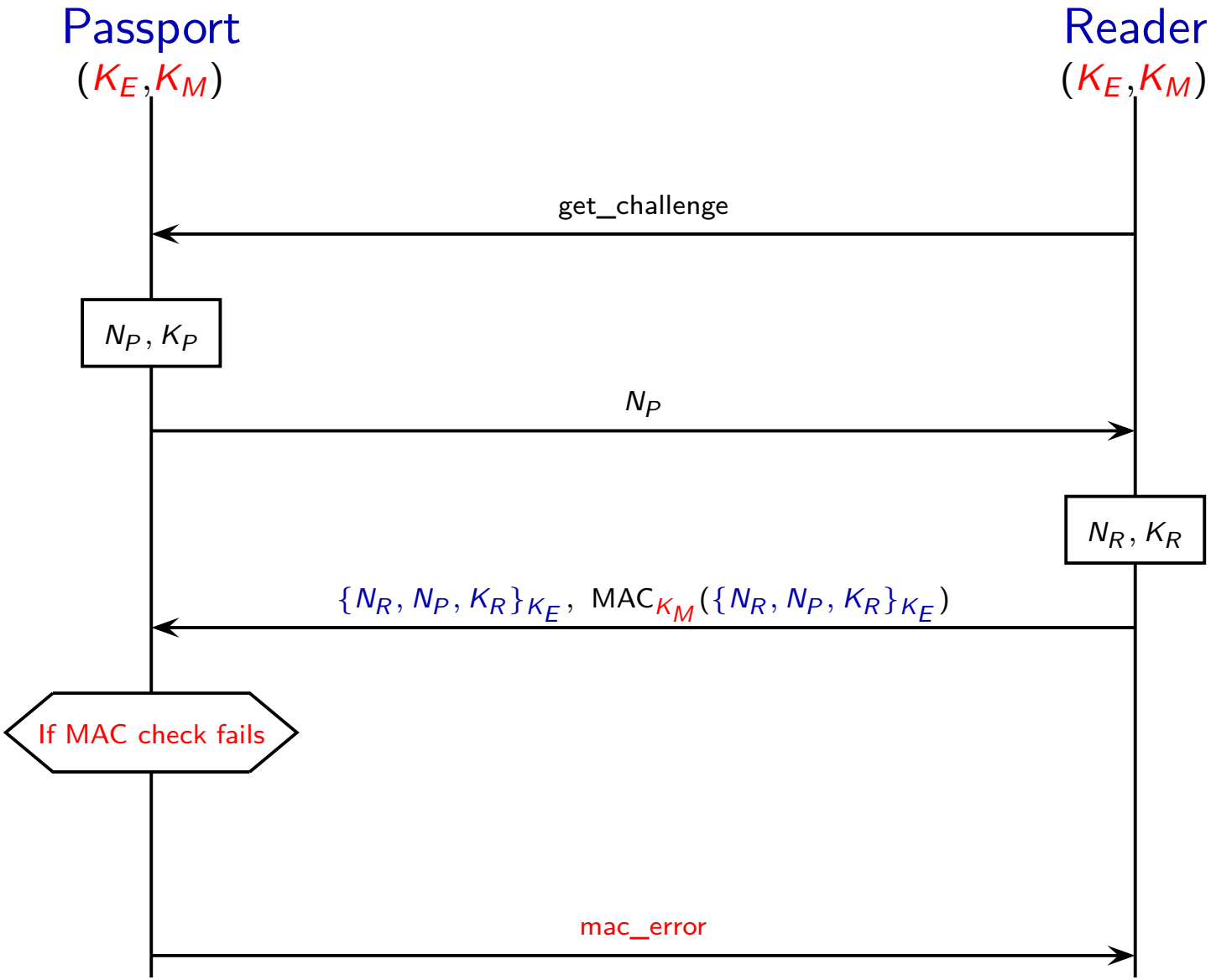
French electronic passport

$\longrightarrow$ the passport must reply to all received messages.



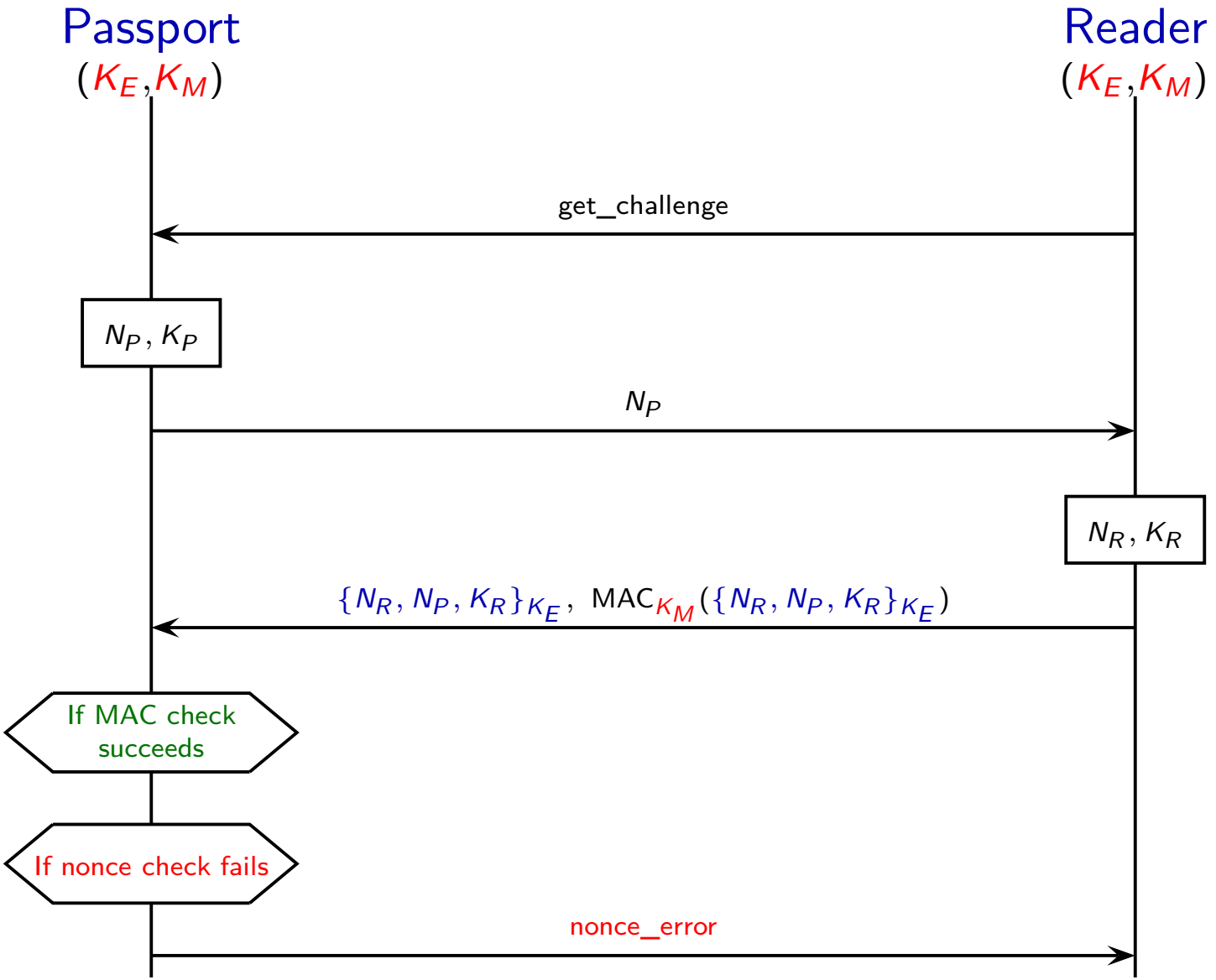
French electronic passport

$\longrightarrow$ the passport must reply to all received messages.



French electronic passport

$\longrightarrow$ the passport must reply to all received messages.



An attack on the French passport [Chothia & Smirnov, 10]

Attack against unlinkability

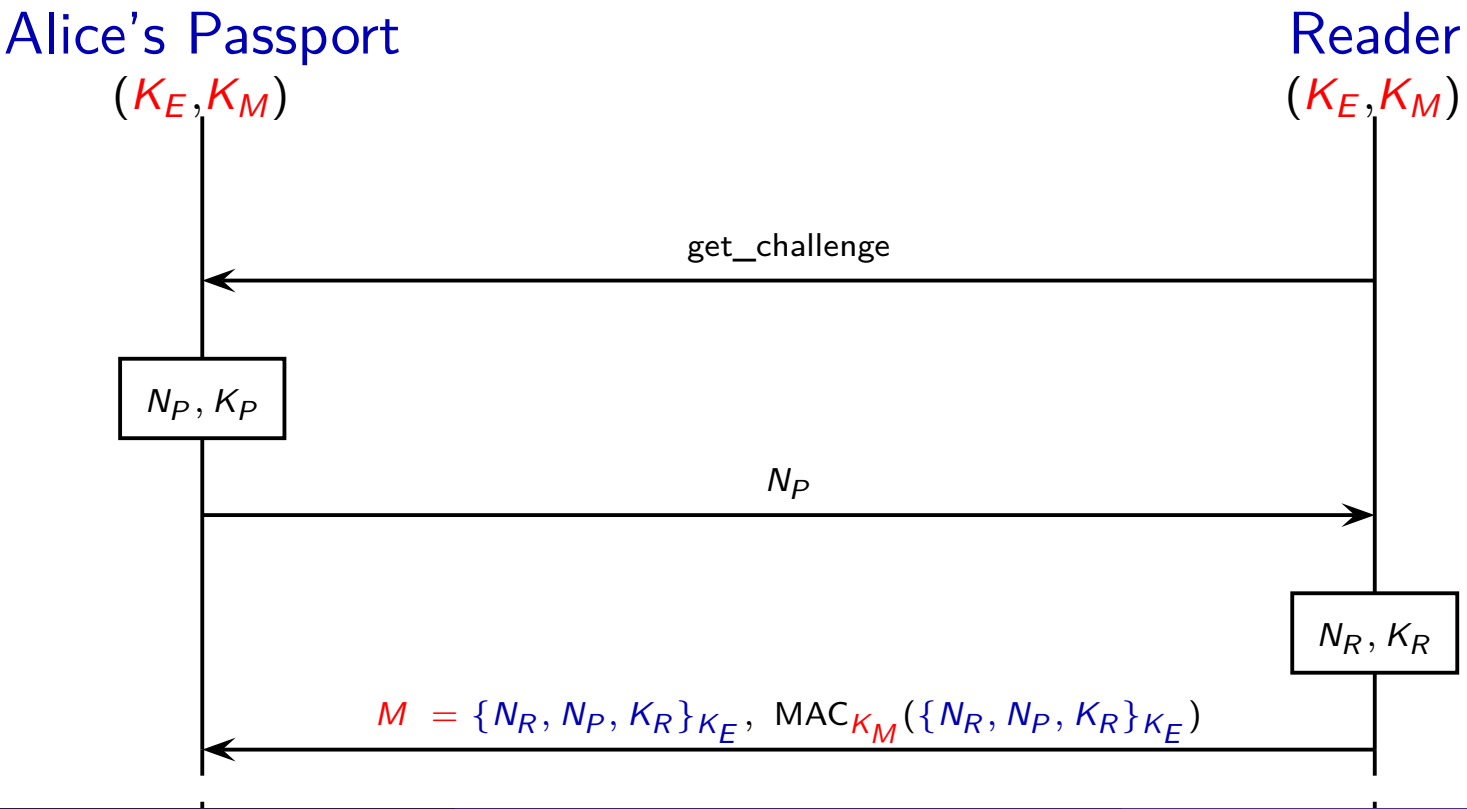
An attacker can track a French passport, provided he has once witnessed a successful authentication.

An attack on the French passport [Chothia & Smirnov, 10]

Attack against unlinkability

An attacker can track a French passport, provided he has once witnessed a successful authentication.

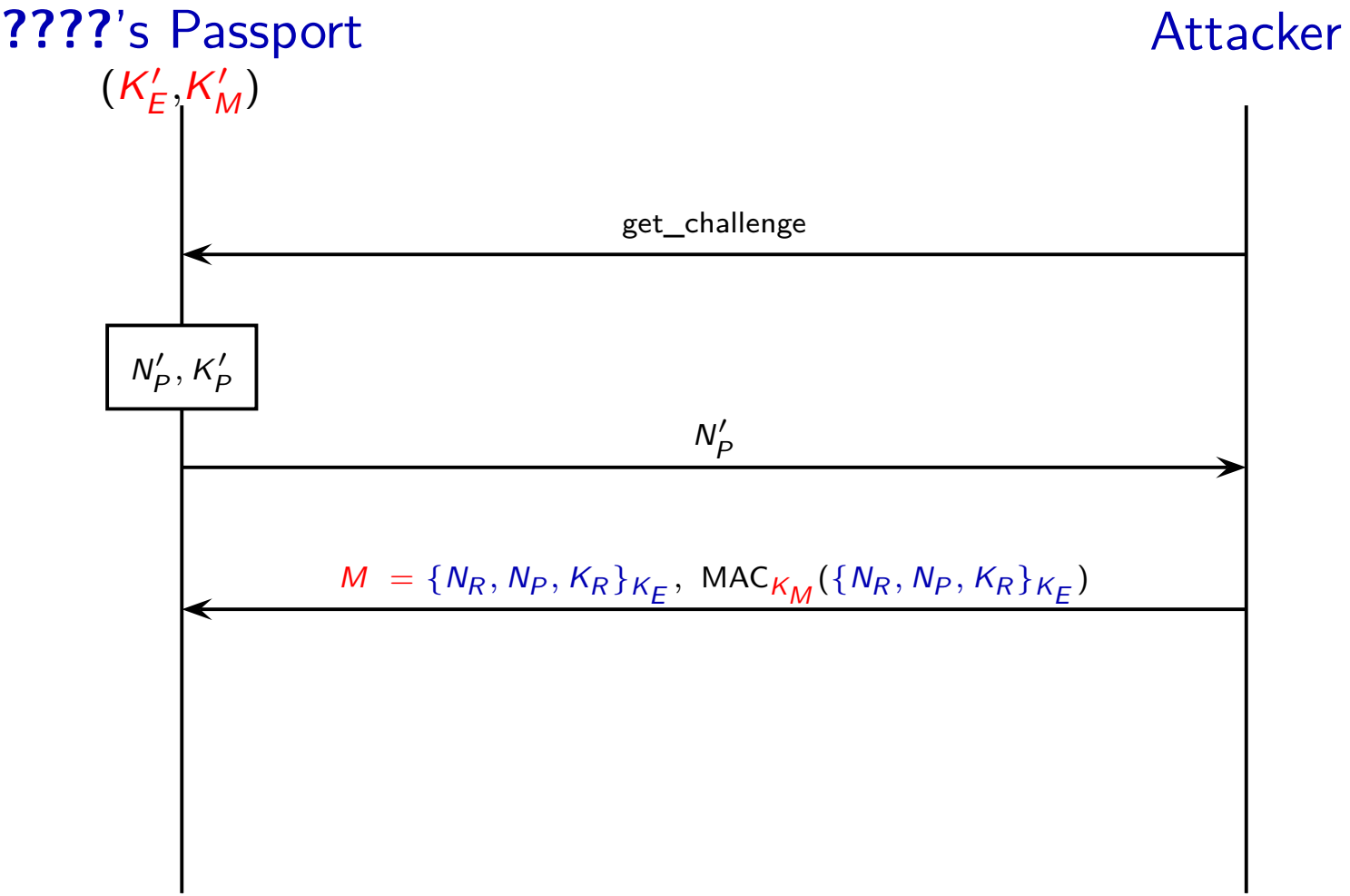
Part 1 of the attack. The attacker eavesdropes on Alice using her passport and records message M.



An attack on the French passport [Chothia & Smirnov, 10]

Part 2 of the attack.

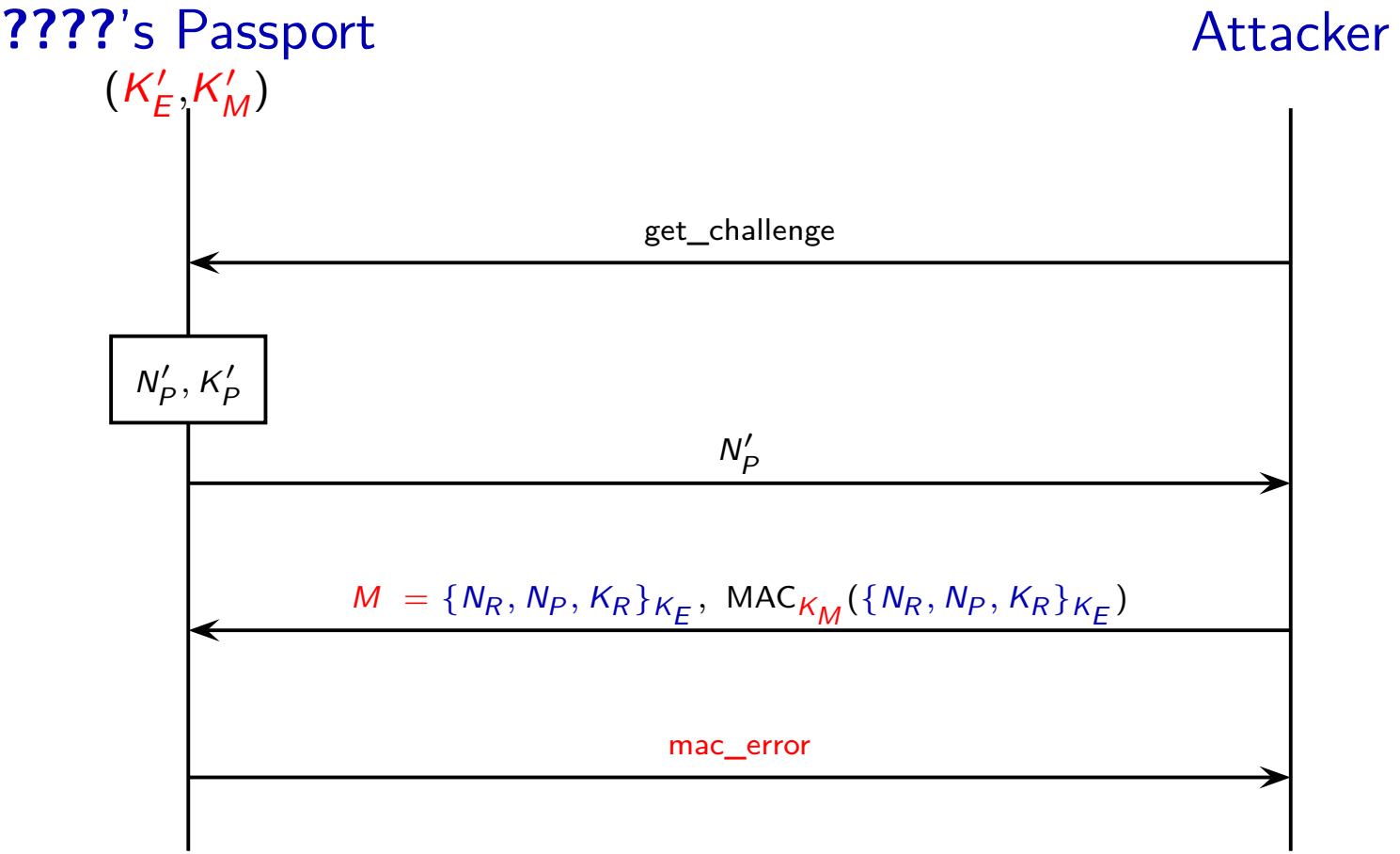
The attacker replays the message M and checks the error code he receives.



An attack on the French passport [Chothia & Smirnov, 10]

Part 2 of the attack.

The attacker replays the message M and checks the error code he receives.

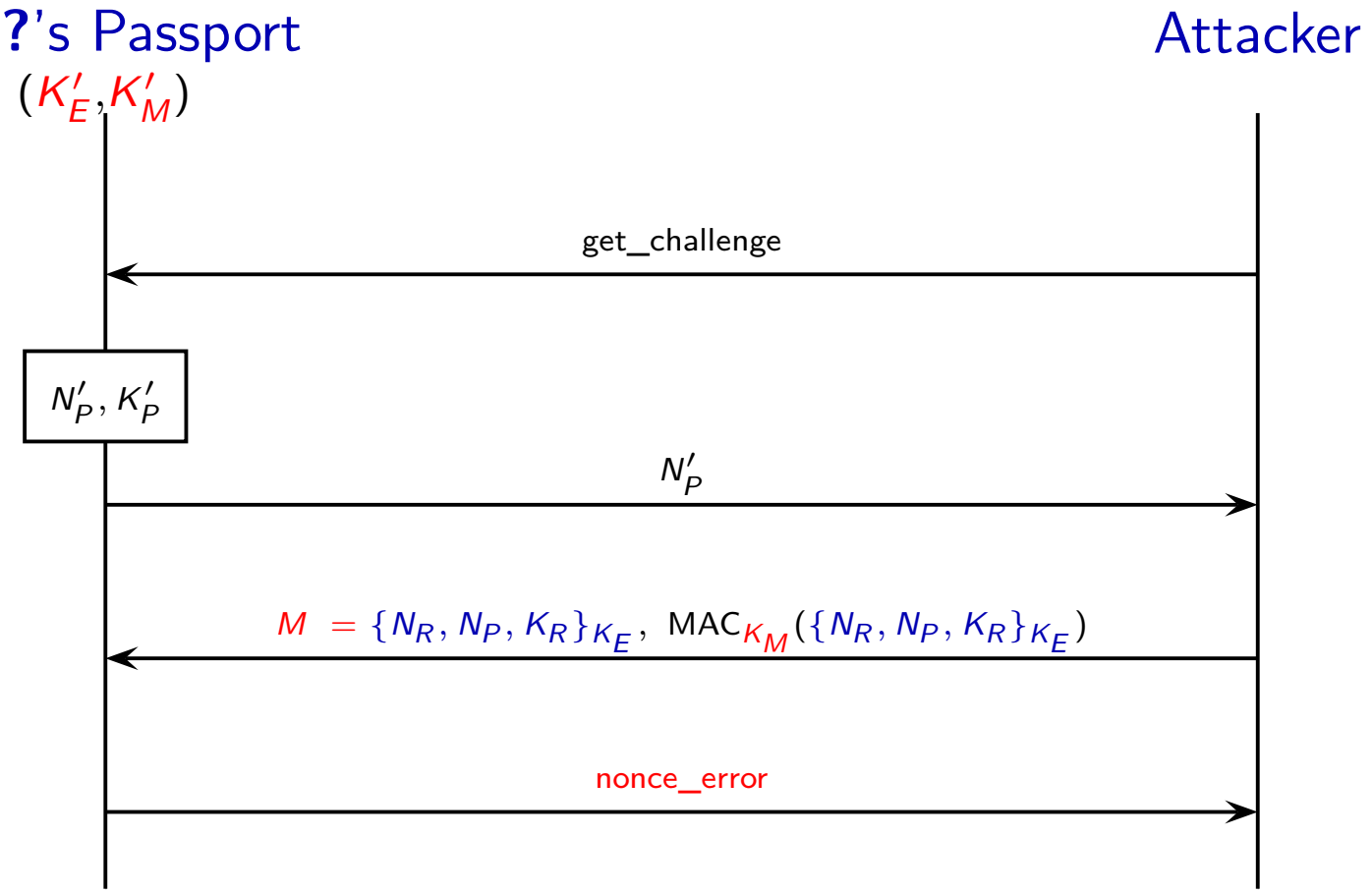


$\Longrightarrow$ MAC check failed $\Longrightarrow$ $K'_M \neq K_M$ $\Longrightarrow$ **????** is not Alice

An attack on the French passport [Chothia & Smirnov, 10]

Part 2 of the attack.

The attacker replays the message M and checks the error code he receives.



$\Longrightarrow$ MAC check succeeded $\Longrightarrow$ $K'_M = K_M$ $\Longrightarrow$???? is Alice

Objectives of the project

Automatic verification of privacy-type security properties
(in the symbolic model)

Target applications: electronic voting protocols, RFID protocols, routing protocols, vehicular ad hoc networks, electronic auction protocols, ...

Objectives of the project

Automatic verification of privacy-type security properties
(in the symbolic model)

Target applications: electronic voting protocols, RFID protocols, routing protocols, vehicular ad hoc networks, electronic auction protocols, ...

Main tasks of the project:

- Task 2. A taxonomy for privacy-type properties
- Task 3. Algorithmic and decidability issues
- Task 4. Modularity issues

$\longrightarrow$ Tool development (Task 5) + Case studies (Task 6)

Outline

1. Task 2. A taxonomy for privacy-type properties
2. Task 3. Algorithmic and decidability issues
3. Task 4. Modularity issues (composition / combination)

Outline

What does privacy mean?

A general concept that is not so easy to formalize.

Main difficulties

1. its formalization depends on the underlying application
   $\longrightarrow$ e-voting, e-passport, ...
2. several notions of privacy for a same application
   $\longrightarrow$ anonymity, unlinkability, vote-privacy, ...

Formalising privacy-type properties

Equivalence-based properties

An observer cannot observe any difference between P and Q

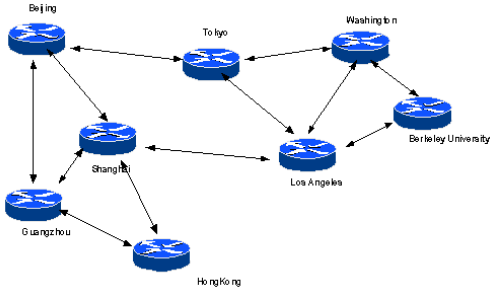
Recently, some formal definitions have been proposed:

- privacy properties in e-voting [Delaune *et al.*, 2008],
- unlinkability in RFID systems [Arapinis *et al.*, 2010], [Bruso *et al.*, 2010],

. . . but some definitions are still missing for many applications (*e.g.* anonymous routing protocols, e-auction protocols, safety critical application in vehicular ad hoc networks, . . .)

Work in progress

With Rémy Chrétien: formalizing privacy-type properties (indistiguishability, unlinkability, anonymity) in routing protocols.

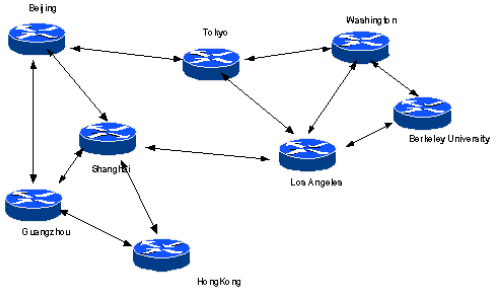


Main difficulty: it is important to assume "enough traffic"

$\longrightarrow$ submitted at POST'13

Work in progress

With Rémy Chrétien: formalizing privacy-type properties (indistiguishability, unlinkability, anonymity) in routing protocols.



Main difficulty: it is important to assume "enough traffic"

$\longrightarrow$ submitted at POST'13

With Graham Steel and Malika Izabachène: a real case study

The Navigo pass

Main difficulty: to obtain the protocol specification !!

Perspectives (possibly)

Some other applications and/or case studies

Examples: e-auction application, protocols used to protect online social networks and/or electronic health record systems

ARC CAPPRIS

- CAPPRIS = Collaborative Action on the Protection of Privacy Rights in the Information Society
- Themes: from privacy analysis to legal and social issues
- Application areas: online social networks, location based services, electronic health record systems

Outline

Algorithms for checking equivalences

trace equivalence is undecidable in general

Algorithms for checking equivalences

trace equivalence is undecidable in general

Bounded number of sessions

e.g. [Baudet, 05], [Dawson & Tiu, 10], [Chevalier & Rusinowitch, 10], ...

$\longrightarrow$ this allows us to decide trace equivalence between simple processes with trivial else branches. [Cortier & Delaune, 09]

Algorithms for checking equivalences

trace equivalence is undecidable in general

Bounded number of sessions

e.g. [Baudet, 05], [Dawson & Tiu, 10], [Chevalier & Rusinowitch, 10], ...

$\longrightarrow$ this allows us to decide trace equivalence between simple processes with trivial else branches. [Cortier & Delaune, 09]

Unbounded number of sessions [Blanchet, Abadi & Fournet, 05]

ProVerif tool [Blanchet, 01] `http://www.proverif.ens.fr/`

- \+ unbounded number of sessions; various cryptographic primitives;
- − termination is not guaranteed; diff-equivalence (too strong)

$\longrightarrow$ ProSwapper extension [Smyth, 10]

Algorithms for checking equivalences

trace equivalence is undecidable in general

Bounded number of sessions

e.g. [Baudet, 05], [Dawson & Tiu, 10], [Chevalier & Rusinowitch, 10], ...

$\longrightarrow$ this allows us to decide trace equivalence between simple processes with trivial else branches. [Cortier & Delaune, 09]

Unbounded number of sessions [Blanchet, Abadi & Fournet, 05]

ProVerif tool [Blanchet, 01] `http://www.proverif.ens.fr/`

- \+ unbounded number of sessions; various cryptographic primitives;
- − termination is not guaranteed; diff-equivalence (too strong)

$\longrightarrow$ ProSwapper extension [Smyth, 10]

$\longrightarrow$ None of these results is able to analyse the e-passport protocol.

A recent contribution

$\longrightarrow$ V. Cheval, H. Comon-Lundh, and S. Delaune CCS 2011

Main result

A procedure for deciding trace equivalence for a large class of processes.

A recent contribution

$\longrightarrow$ V. Cheval, H. Comon-Lundh, and S. Delaune CCS 2011

Main result

A procedure for deciding trace equivalence for a large class of processes.

Our class of processes:

- + non-trivial else branches, private channels, and non-deterministic choice;
- − but no replication, and a fixed set of cryptographic primitives (signature, encryption, hash function, mac).

$\longrightarrow$ this allows us in particular to deal with the e-passport example

A recent contribution

$\longrightarrow$ V. Cheval, H. Comon-Lundh, and S. Delaune CCS 2011

Main result

A procedure for deciding trace equivalence for a large class of processes.

Main idea:

- we propose a symbolic semantics to avoid infinite branching
  $\longrightarrow$ we keep track of the choice of the attacker in a constraint system
- we design an algorithm to decide symbolic equivalence between sets of constraint systems.

Another contribution

$\longrightarrow$ S. Delaune, S. Kremer, and D. Pasaila IJCAR 2012

Main result

Algorithm for deciding symbolic equivalence of constraint systems for monoidal equational theories (*e.g.* exclusive-or, Abelian group, ...)

Another contribution

$\longrightarrow$ S. Delaune, S. Kremer, and D. Pasaila IJCAR 2012

Main result

Algorithm for deciding symbolic equivalence of constraint systems for monoidal equational theories (*e.g.* exclusive-or, Abelian group, ...)

Main idea: we rely on the isomorphism between group theories and rings.

1. we reduce the problem under study to the problem of deciding whether the solutions of a system of linear equations are included in the set of solutions of a system of equation;
2. we rely on some existing results to conclude.

Another contribution

$\longrightarrow$ S. Delaune, S. Kremer, and D. Pasaila IJCAR 2012

Main result

Algorithm for deciding symbolic equivalence of constraint systems for monoidal equational theories (*e.g.* exclusive-or, Abelian group, ...)

Limitations:

- a restricted class of protocols (simple processes with trivial else branches only),
- monoidal theories do not allow us to model encryptions, signatures, hash functions ...

Work in progress

With Rémy Chrétien and Véronique Cortier: (un)decidability results for processes with replication (Master thesis)

- an undecidability result for a simple class of processes (known to be decidable for reachability properties)
- a decidability result with further restrictions (a very restricted class !)

$\longrightarrow$ see Rémy's talk (November 7th)

Work in progress

With Rémy Chrétien and Véronique Cortier: (un)decidability results for processes with replication (Master thesis)

- an undecidability result for a simple class of processes (known to be decidable for reachability properties)
- a decidability result with further restrictions (a very restricted class !)

$\longrightarrow$ see Rémy's talk (November 7th)

With Apoorva Deshpande and Steve Kremer: a procedure for trace equivalence in presence of more equational theories

- our aim is to extend the procedure by R. Chadha, S. Ciobaca, and S. Kremer (ESOP'12) to deal with equatinonal theories having the finite variant property;
- add this feature in the AKISS tool (at least) for some equational theories (*e.g.* exclusive-or + subterm convergent theory)

Some perspectives

Could we improve ProVerif to conclude in more cases ?

- More equational theories: *e.g.* those having the finite variant property as done in [R. Küsters, T. Truderung, 08 & 09] for reachability properties
- Beyond diff-equivalence: propose some transformations to "help" ProVerif to conclude as the one implemented in the ProSwapper tool [B. Smyth] for observational equivalence properties

Outline

Task 4.1 Combination

Motivation

Protocols rely on many cryptographic primitives.

$\longrightarrow$ a need for **combination results**

Main goal:

Decision procedure for E_1 + Decision procedure for E_2
+ some conditions (*e.g.* disjoint/hierarchical)

implies

Decision procedure for $\mathsf{E}_1 \cup \mathsf{E}_2$.

Starting points:

- the special case of guessing attacks; and
- the existing combination algorithms for reachability properties [Chevalier and Rusinowitch, 05 & 06] and static equivalence [Cortier and Delaune, 07].

Task 4.2 Composition

Some motivations

- Existing tools allow us to verify **relatively small** protocols and sometimes only for a **bounded number of sessions**
- Most often, we verify them in **isolation**

$\longrightarrow$ a need for **composition results**

Task 4.2 Composition

Some motivations

- Existing tools allow us to verify **relatively small** protocols and sometimes only for a **bounded number of sessions**
- Most often, we verify them in **isolation**

$\longrightarrow$ a need for **composition results**

Example:

$$P_1 : \quad A \to B : \quad \{A\}^r_{\mathsf{pub}(B)}$$

What about the anonymity of A?

Task 4.2 Composition

Some motivations

- Existing tools allow us to verify **relatively small** protocols and sometimes only for a **bounded number of sessions**
- Most often, we verify them in **isolation**

$\longrightarrow$ a need for **composition results**

Example:

$$P_1 : \quad A \to B : \quad \{A\}^r_{\mathrm{pub}(B)}$$

$$P_2 : \quad A \to B : \quad \{N_a\}^r_{\mathrm{pub}(B)}$$
$$B \to A : \quad N_a$$

What about the anonymity of A?

Task 4.2 Composition

Our goals

investigate sufficient conditions to ensure that protocols (that may share some keys) can be safely used in an environment where:

1. other sessions of the same protocol may be executed;
2. other sessions of another protocol may be executed as well.

Task 4.2 Composition

Our goals

investigate sufficient conditions to ensure that protocols (that may share some keys) can be safely used in an environment where:

1. other sessions of the same protocol may be executed;
2. other sessions of another protocol may be executed as well.

Several results already exist for sequential/parallel composition, *e.g.*:

- parallel composition using tagging
  $\longrightarrow$ [Guttman & Thayer, 2000], [Cortier *et al.*, 2007]
- sequential composition for arbitrary primitives
  $\longrightarrow$ [Ciobaca & Cortier, 2010]

Task 4.2 Composition

Our goals

investigate sufficient conditions to ensure that protocols (that may share some keys) can be safely used in an environment where:

1. other sessions of the same protocol may be executed;
2. other sessions of another protocol may be executed as well.

Several results already exist for sequential/parallel composition, *e.g.*:

- parallel composition using tagging
  $\longrightarrow$ [Guttman & Thayer, 2000], [Cortier *et al.*, 2007]
- sequential composition for arbitrary primitives
  $\longrightarrow$ [Ciobaca & Cortier, 2010]

None of them are well-suited for analysing privacy-type properties

A recent contribution

$\longrightarrow$ M. Arapinis, V. Cheval, and S. Delaune CSF 2012

Main result

A composition result that allows us to analyse privacy-type properties in a modular way.

- we consider processes that may share some keys and also some primitives provided that they are tagged (syntactic condition);
- we consider parallel composition only;

$\longrightarrow$ this allows us to analyse the passive/active authentication protocols of the e-passport application in a modular way

Some perspectives

Relaxing the tagging condition

$\longrightarrow$ we could consider an implicit disjointness criterion as done in [Küsters & Tuengerthal, 2011]

Some perspectives

Relaxing the tagging condition

$\longrightarrow$ we could consider an implicit disjointness criterion as done in [Küsters & Tuengerthal, 2011]

Other kinds of composition:

This will be useful to analyse the whole e-passport application in a modular way (*e.g.* *BAC* protocol followed by *PA* & *AA* protocols)

Some perspectives

Relaxing the tagging condition

$\longrightarrow$ we could consider an implicit disjointness criterion as done in [Küsters & Tuengerthal, 2011]

Other kinds of composition:

This will be useful to analyse the whole e-passport application in a modular way (*e.g.* *BAC* protocol followed by *PA* & *AA* protocols)

From few sessions to many:

$$\begin{array}{c} \text{Unlinkability for } P_1 \mid P_2 \\ + \\ \text{some conditions ?} \end{array} \quad \Rightarrow \quad \text{Unlinkability for } !P_1 \mid !P_2 \mid \ldots \mid !P_n$$

Conclusion

ANR JCJC - VIP project
(Jan. 2012 - Dec 2015)
`http://www.lsv.ens-cachan.fr/Projects/anr-vip/`

It remains a lot to do for analysing privacy-type properties:

- formal definitions of some privacy-type security properties
- algorithms (and tools!) for checking automatically trace equivalence for various cryptographic primitives;
- more combination/composition results.