# Les protocoles cryptographiques: sommes-nous bien protégés ?

Stéphanie Delaune

LSV, CNRS & ENS Cachan, France

Jeudi 26 Juin 2014

# Cryptographic protocols everywhere !


## Cryptographic protocols

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

## The network is unsecure!

Communications take place over a public network like the Internet.

# Cryptographic protocols everywhere !



## Cryptographic protocols

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

**It becomes more and more important to protect our privacy.**




# Security properties

- **Secrecy**: May an intruder learn some secret message between two honest participants?
- Authentication: Is the agent Alice really talking to Bob?
- Anonymity: Is an attacker able to learn something about the identity of the participants who are communicating?
- Non-repudiation: Alice sends a message to Bob. Alice cannot later deny having sent this message. Bob cannot deny having received the message.
- ...

# How does a cryptographic protocol work (or not)? (1/2)

**cryptographic primitives = basic building blocks**

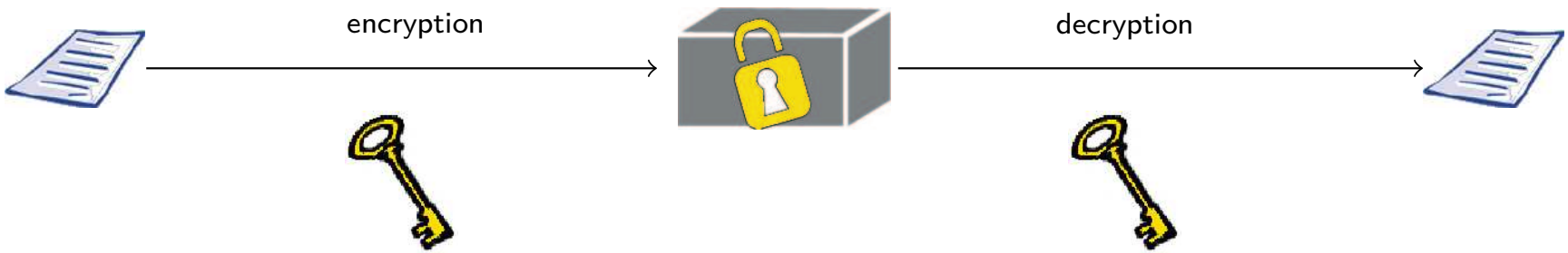
$\longrightarrow$ symmetric/ asymmetric encryption, signature, hash function, ...

# How does a cryptographic protocol work (or not)? (1/2)

**cryptographic primitives = basic building blocks**

$\longrightarrow$ symmetric/ asymmetric encryption, signature, hash function, ...

## Symmetric encryption

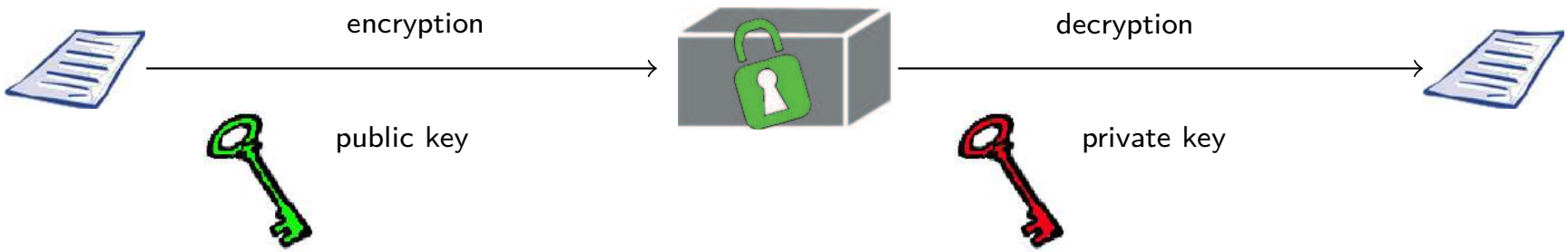


# How does a cryptographic protocol work (or not)? (1/2)

**cryptographic primitives = basic building blocks**

$\longrightarrow$ symmetric/ asymmetric encryption, signature, hash function, ...

## Asymmetric encryption ($\sim$ 70s)

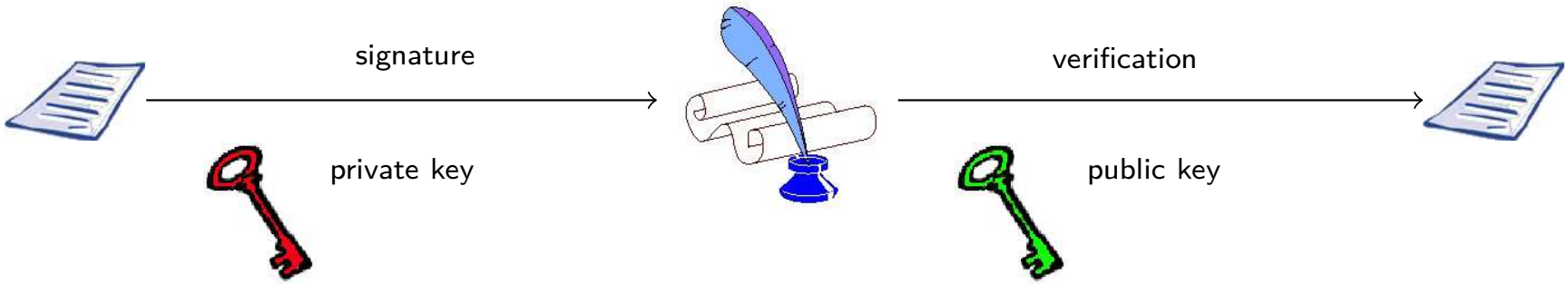


# How does a cryptographic protocol work (or not)? (1/2)

**cryptographic primitives = basic building blocks**

$\longrightarrow$ symmetric/ asymmetric encryption, signature, hash function, ...

## Signature



# How does a cryptographic protocol work (or not)? (2/2)

**protocol = small programs explaining how to exchange messages**

$\longrightarrow$ key-exchange protocols, authentication protocols, e-voting protocols, Bitcoin protocol, ...

# How does a cryptographic protocol work (or not)? (2/2)

**protocol = small programs explaining how to exchange messages**

$\longrightarrow$ key-exchange protocols, authentication protocols, e-voting protocols, Bitcoin protocol, ...

Example: A simplified version of the Denning-Sacco protocol (1981)

$$\begin{array}{lcl} A \to B & : & \mathsf{aenc}(\mathsf{sign}(k, \mathsf{priv}(A)), \mathsf{pub}(B)) \\ B \to A & : & \mathsf{senc}(s, k) \end{array}$$

What about secrecy of $s$ ?

# How does a cryptographic protocol work (or not)? (2/2)

**protocol = small programs explaining how to exchange messages**

$\longrightarrow$ key-exchange protocols, authentication protocols, e-voting protocols, Bitcoin protocol, ...

Example: A simplified version of the Denning-Sacco protocol (1981)

$$\begin{array}{lcl} A \to B & : & \mathsf{aenc}(\mathsf{sign}(k, \mathsf{priv}(A)), \mathsf{pub}(B)) \\ B \to A & : & \mathsf{senc}(s, k) \end{array}$$

What about secrecy of $s$ ?
Consider a scenario where $A$ starts a session with $C$ who is dishonest.

$$1.\ A \to C : \mathsf{aenc}(\mathsf{sign}(k, \mathsf{priv}(A)), \mathsf{pub}(C))$$

# How does a cryptographic protocol work (or not)? (2/2)

**protocol = small programs explaining how to exchange messages**

$\longrightarrow$ key-exchange protocols, authentication protocols, e-voting protocols, Bitcoin protocol, ...

Example: A simplified version of the Denning-Sacco protocol (1981)

$$\begin{array}{lcl} A \to B & : & \mathsf{aenc}(\mathsf{sign}(k, \mathsf{priv}(A)), \mathsf{pub}(B)) \\ B \to A & : & \mathsf{senc}(s, k) \end{array}$$

What about secrecy of $s$ ?
Consider a scenario where $A$ starts a session with $C$ who is dishonest.

1. $A \to C$ : $\mathsf{aenc}(\mathsf{sign}(k, \mathsf{priv}(A)), \mathsf{pub}(C))$

2. $C(A) \to B$ : $\mathsf{aenc}(\mathsf{sign}(k, \mathsf{priv}(A)), \mathsf{pub}(B))$
3. $B \to A$ : $\mathsf{senc}(s, k)$ Attack !

# Verification of cryptographic protocols (symbolic models)

$\longrightarrow$ Various models (*e.g.* [Dolev & Yao, 81]) having some common features

# Verification of cryptographic protocols (symbolic models)

$\longrightarrow$ Various models (*e.g.* [Dolev & Yao, 81]) having some common features

**Messages**

They are abstracted by terms together with an equational theory.

# Verification of cryptographic protocols (symbolic models)

$\longrightarrow$ Various models (*e.g.* [Dolev & Yao, 81]) having some common features

**Messages**

They are abstracted by terms together with an equational theory.

Examples:

$\rightarrow$ symmetric encryption/decryption: $\mathrm{dec}(\mathrm{enc}(x, y), y) = x$

$\rightarrow$ exclusive or operator:

$$\begin{array}{rcl} (x \oplus y) \oplus z & = & x \oplus (y \oplus z) \\ x \oplus y & = & y \oplus x \end{array} \qquad \begin{array}{rcl} x \oplus x & = & 0 \\ x \oplus 0 & = & x \end{array}$$

# Verification of cryptographic protocols (symbolic models)

$\longrightarrow$ Various models (*e.g.* [Dolev & Yao, 81]) having some common features

## Messages

They are abstracted by terms together with an equational theory.

## The attacker

# Verification of cryptographic protocols (symbolic models)

$\longrightarrow$ Various models (*e.g.* [Dolev & Yao, 81]) having some common features

## Messages

They are abstracted by terms together with an equational theory.

## The attacker

# Verification of cryptographic protocols (symbolic models)

$\longrightarrow$ Various models (*e.g.* [Dolev & Yao, 81]) having some common features

## Messages

They are abstracted by terms together with an equational theory.

## The attacker

- may read every message sent on the network,
- may intercept and send new messages according to its deduction capabilities.
  $\longrightarrow$ only symbolic manipulations on terms.

# Concevoir et vérifier les protocoles de sécurité est difficile

Le protocole doit “marcher”

- pour un nombre arbitraire de sessions et de participants;
- en présence d'agents malhonnêtes;
- en présence d'autres protocoles pouvant entrer en interaction avec le protocole étudié
  *e.g.* utilisation d'une même clef/mot de passe pour différentes applications

## Some automatic verification tools

- AVISPA platform [Armando *et al.*, 05]
  $\longrightarrow$ state-of-the-art for bounded verification
- ProVerif tool [Blanchet, 01]
  $\longrightarrow$ quite flexible to model cryptographic primitives

# Attaque sur le protocole Single Sign On

## Protocole Single Sign On

- permet de s'authentifier une seule fois pour plusieurs services;
- utilisé par exemple dans Google app


## Description de l'attaque

$\longrightarrow$ découverte en 2008 avec la platforme de vérification AVISPA

1. un attaquant propose une nouvelle application (amusante ou intéressante);
2. des clients s'authentifient auprès de cette application malhonnête;
3. l'attaquant peut alors accéder à toutes les autres applications du client, y compris *e.g.* Gmail ou Google Calendar.

# Should we worry about our privacy?


E-passport

E-voting

# Le passeport électronique

# Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

# Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

La puce RFID permet de stocker:

- les informations écrites sur le passeport,
- votre photo numérisée.

# Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

La puce RFID permet de stocker:

- les informations écrites sur le passeport,
- votre photo numérisée.

**Il est interrogeable à distance à l'insu de son propriétaire !**

# Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

# Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles


$\longrightarrow$ possibilité de récupérer la signature manuscrite du porteur en interrogeant le passeport à distance

# Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles


$\longrightarrow$ possibilité de récupérer la signature manuscrite du porteur en interrogeant le passeport à distance

"Faille" découverte sur les passeports belges

Passeport émis entre 2004 et 2006 en Belgique

# Passeport électronique — 2ème Génération

Passeport émis à partir de 2006 en France, en Belgique, . . .

# Passeport électronique — 2ème Génération

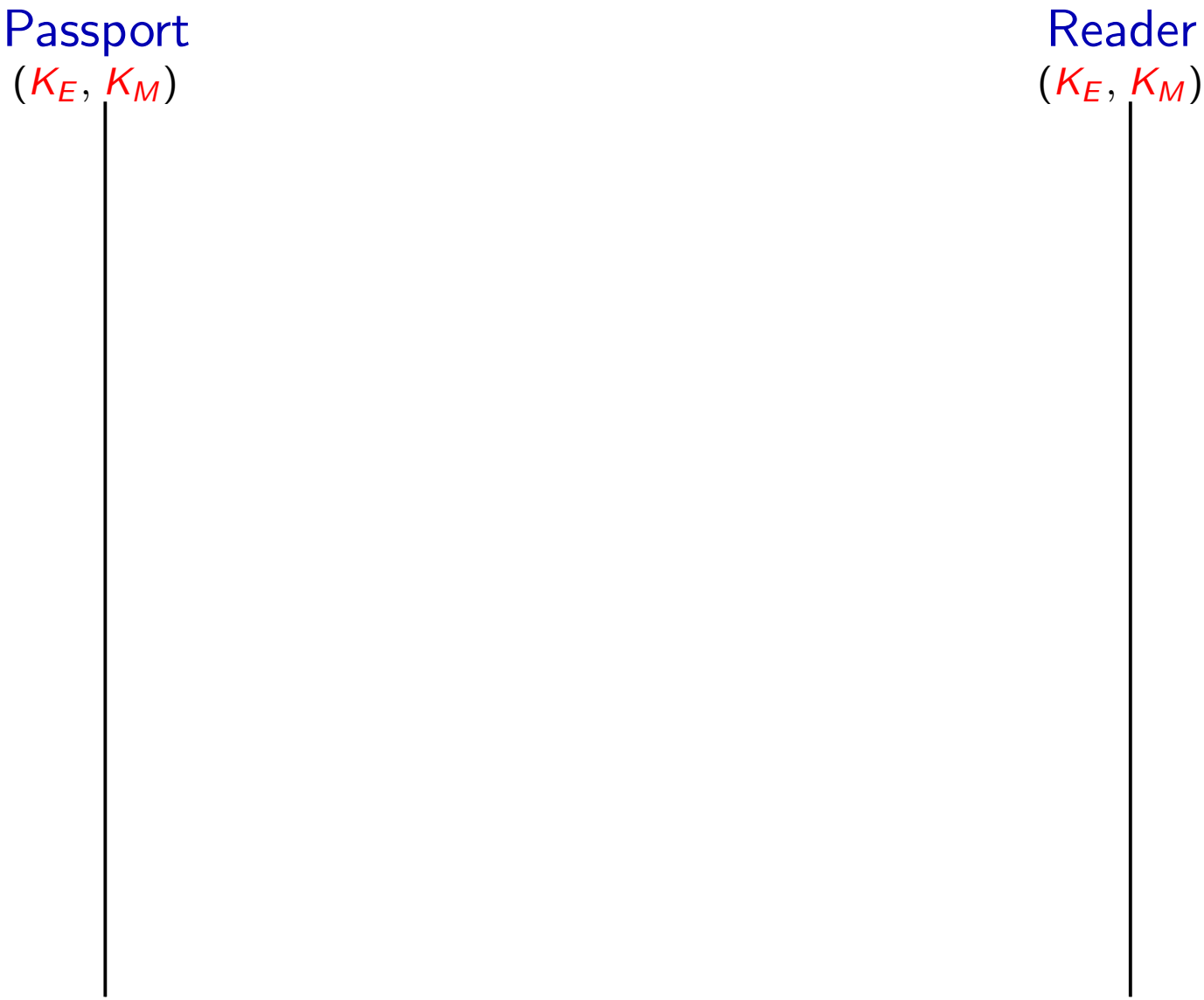
Passeport émis à partir de 2006 en France, en Belgique, . . .


$\longrightarrow$ mis en place d'un mécanisme (protocole BAC) qui permet de protéger nos informations personnelles. The BAC protocol is a key establishment protocol that has been designed to also ensure unlinkability.

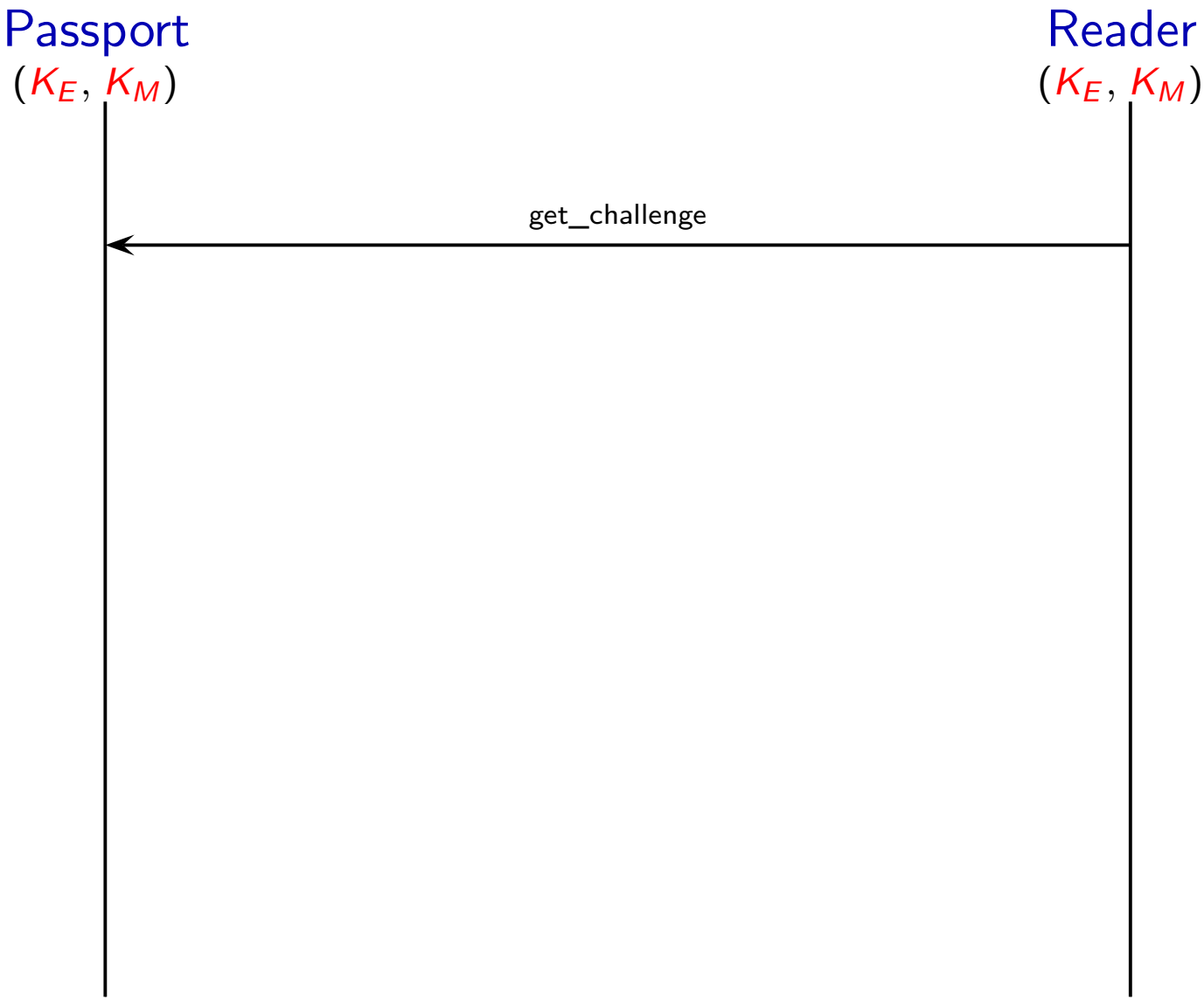
## ISO/IEC standard 15408

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.*

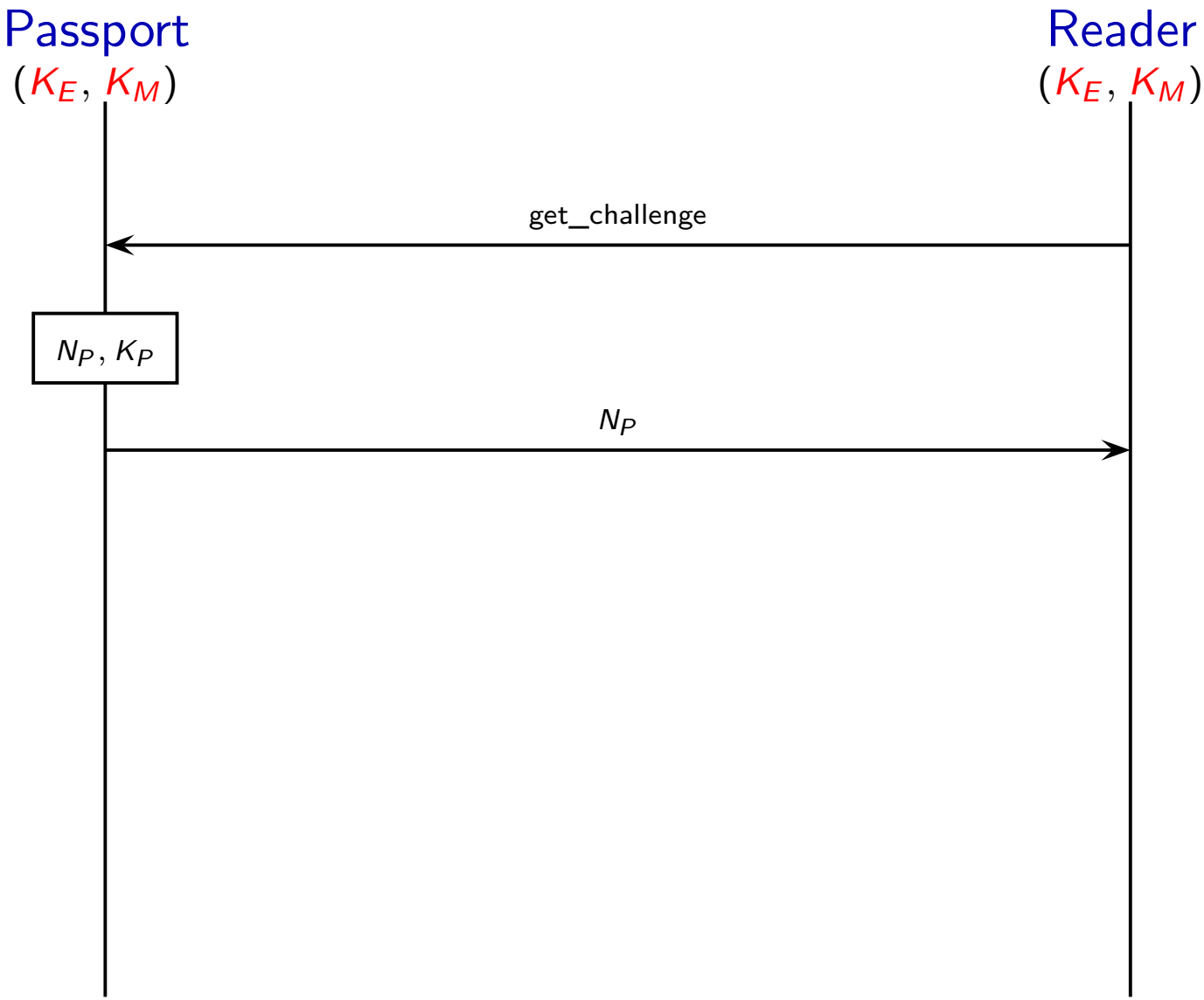
# BAC protocol



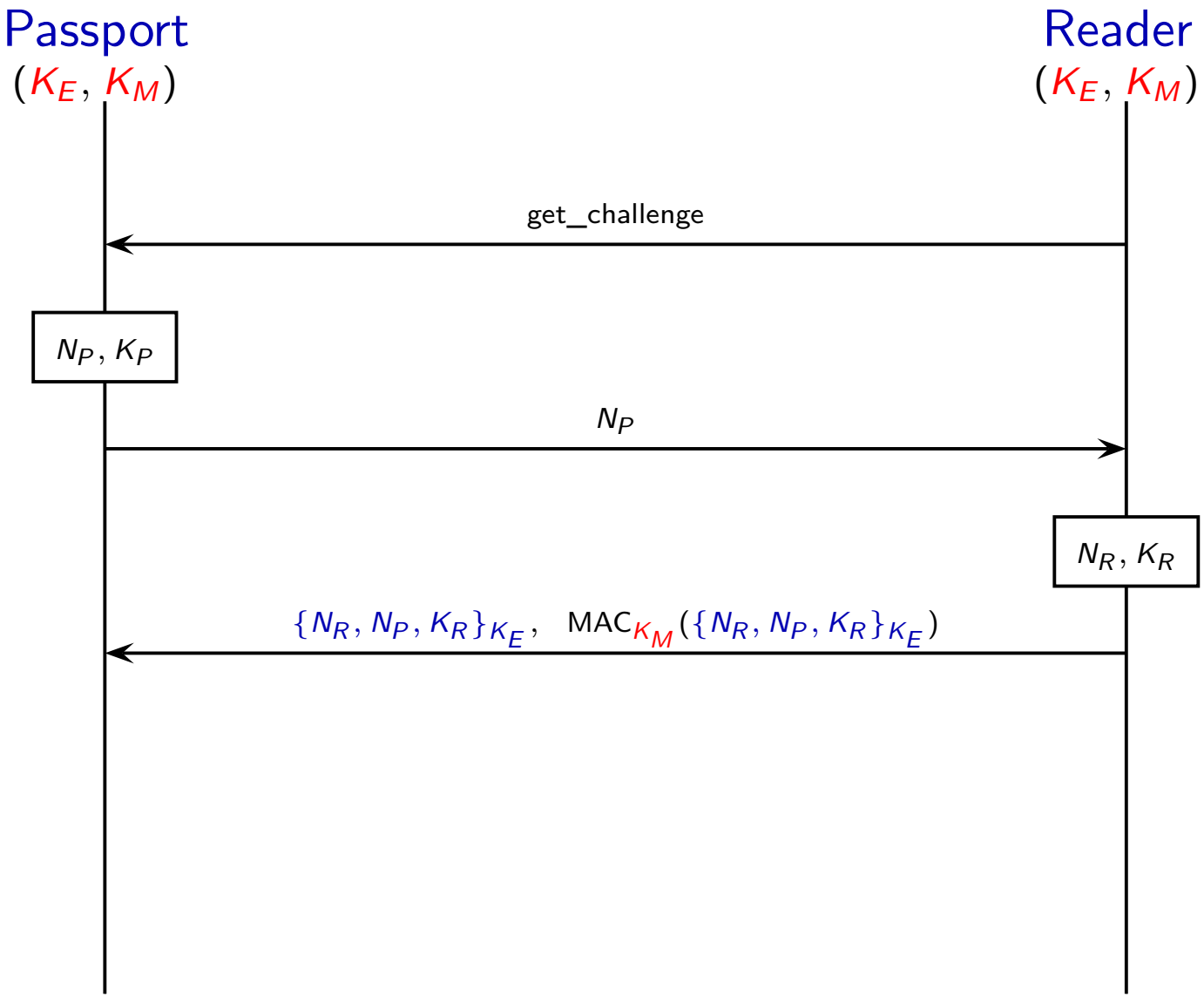
# BAC protocol



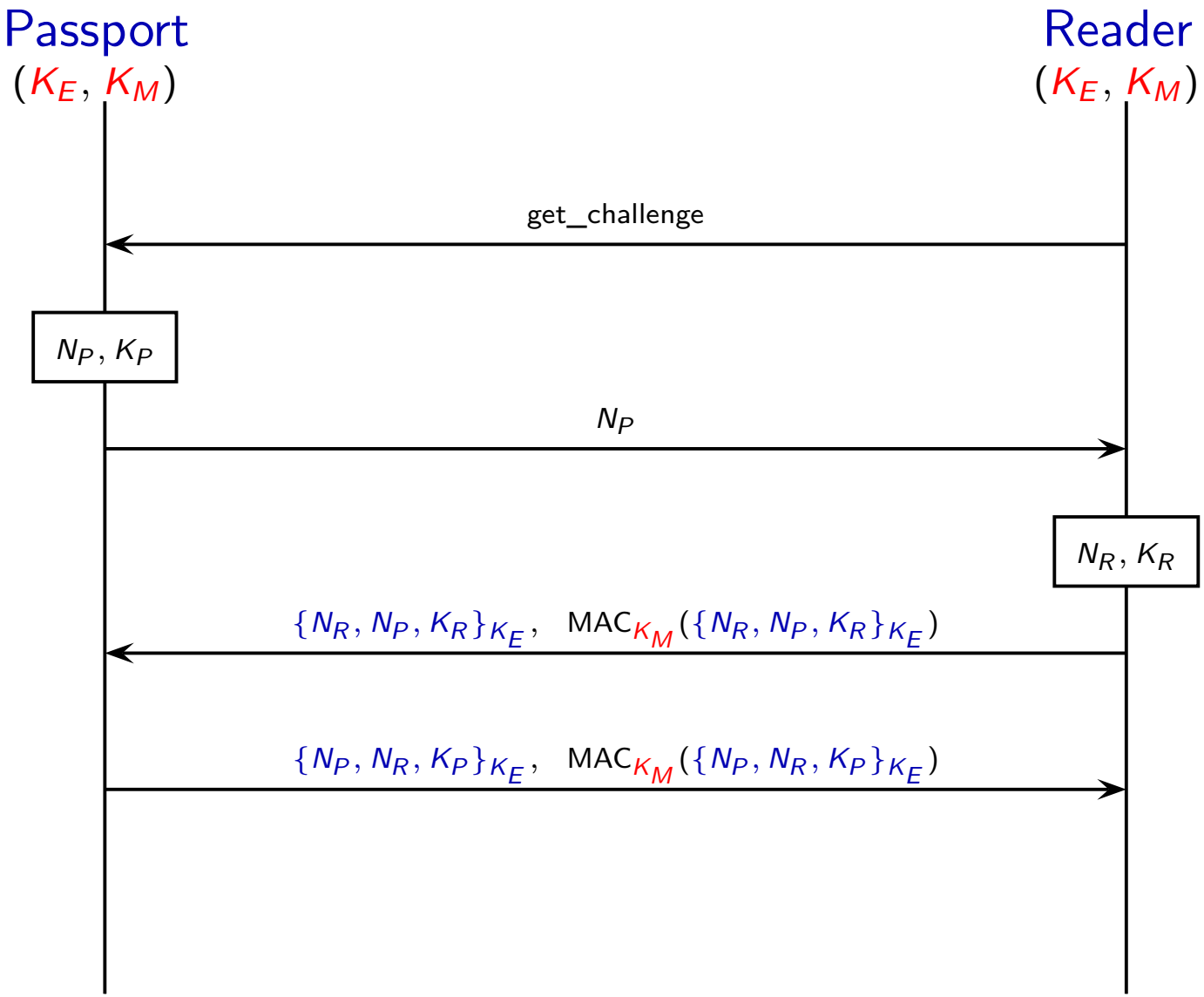
# BAC protocol



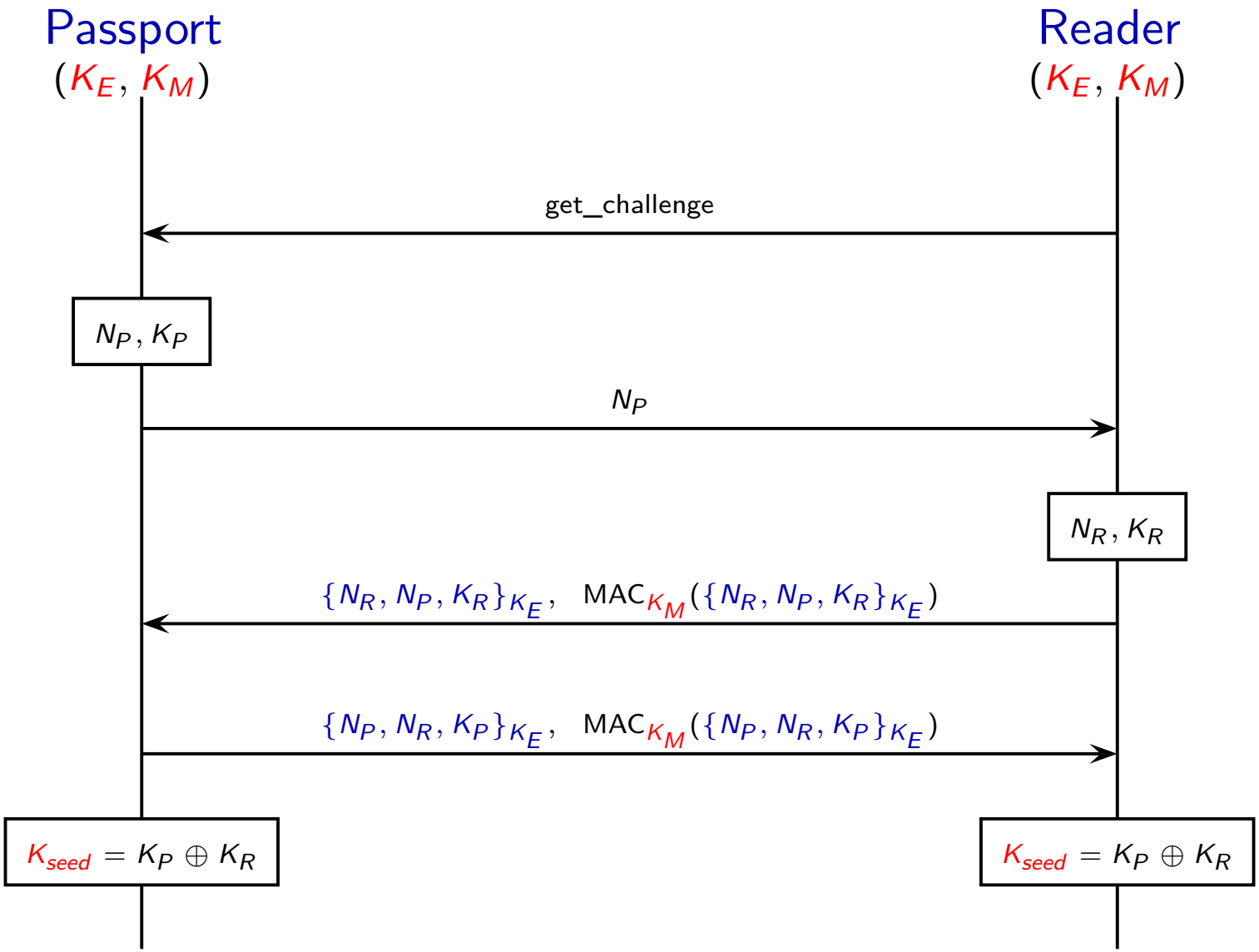
# BAC protocol



# BAC protocol



# BAC protocol



# Protocole BAC

Dans la description du protocole:

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) mais ...

# Protocole BAC

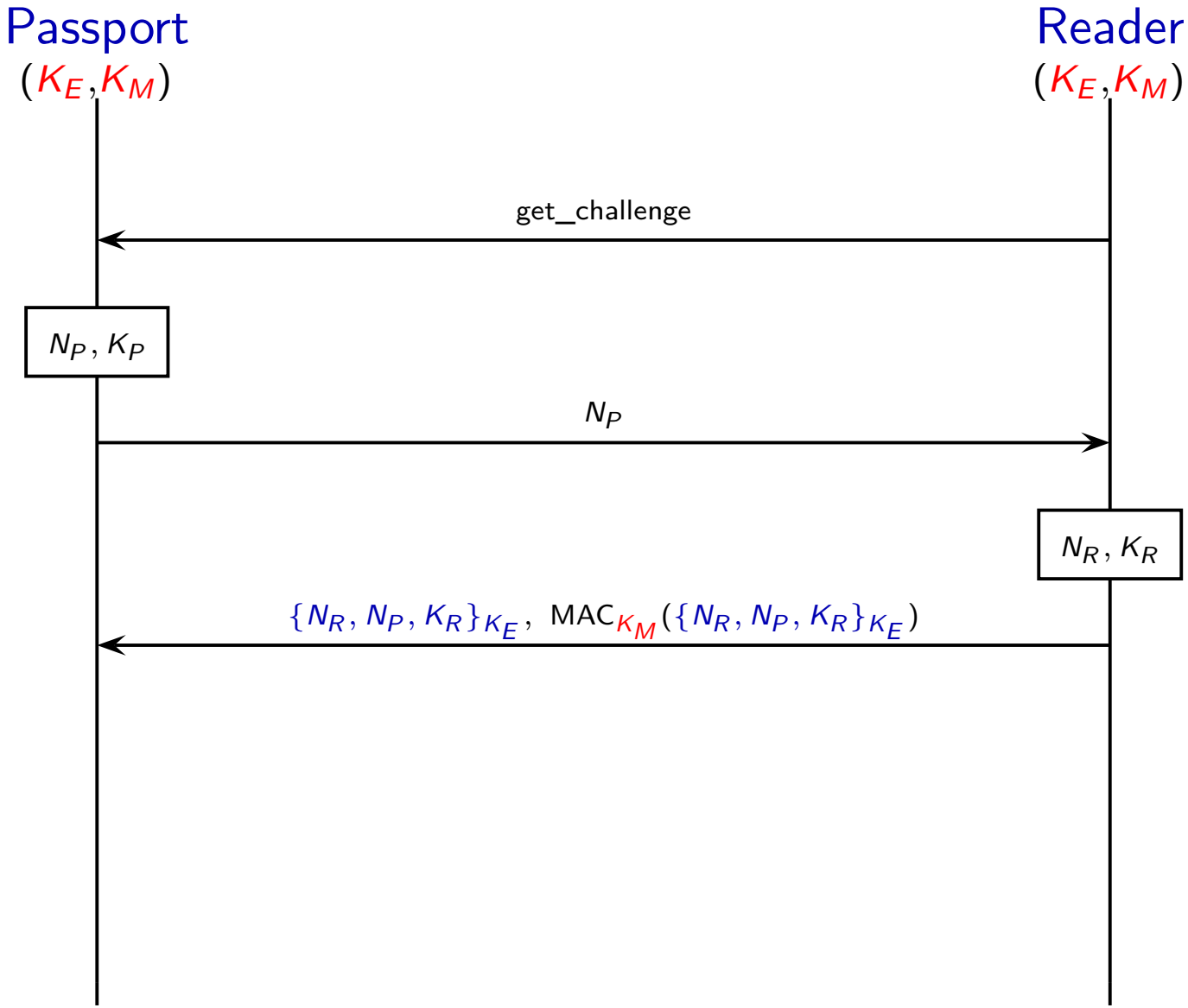
Dans la description du protocole:

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) mais ...
- ... ces messages d'erreurs ne sont pas précisés.

Il en résulte une implémentation différentes selon les nations.

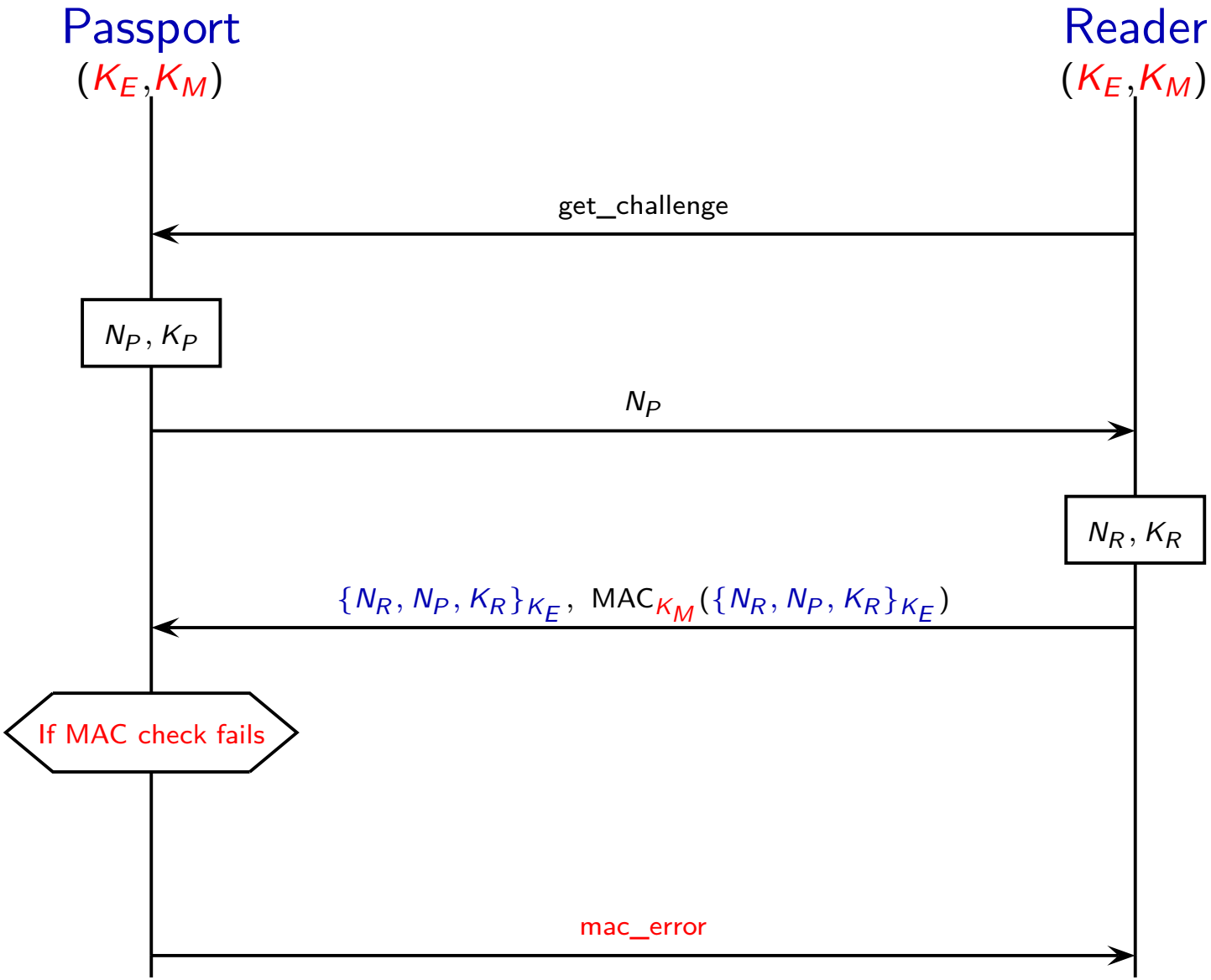
# French electronic passport

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



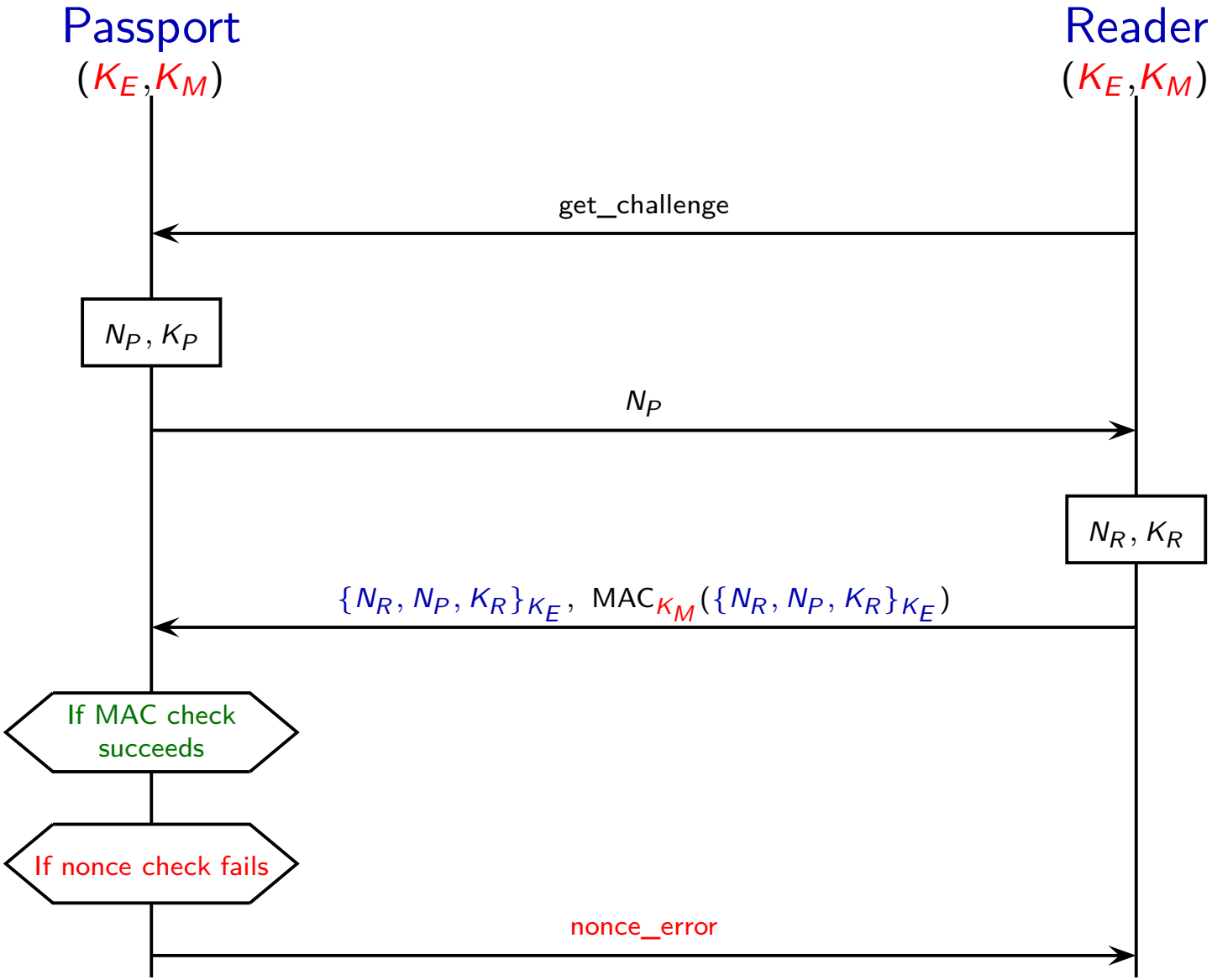
# French electronic passport

$\longrightarrow$ 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

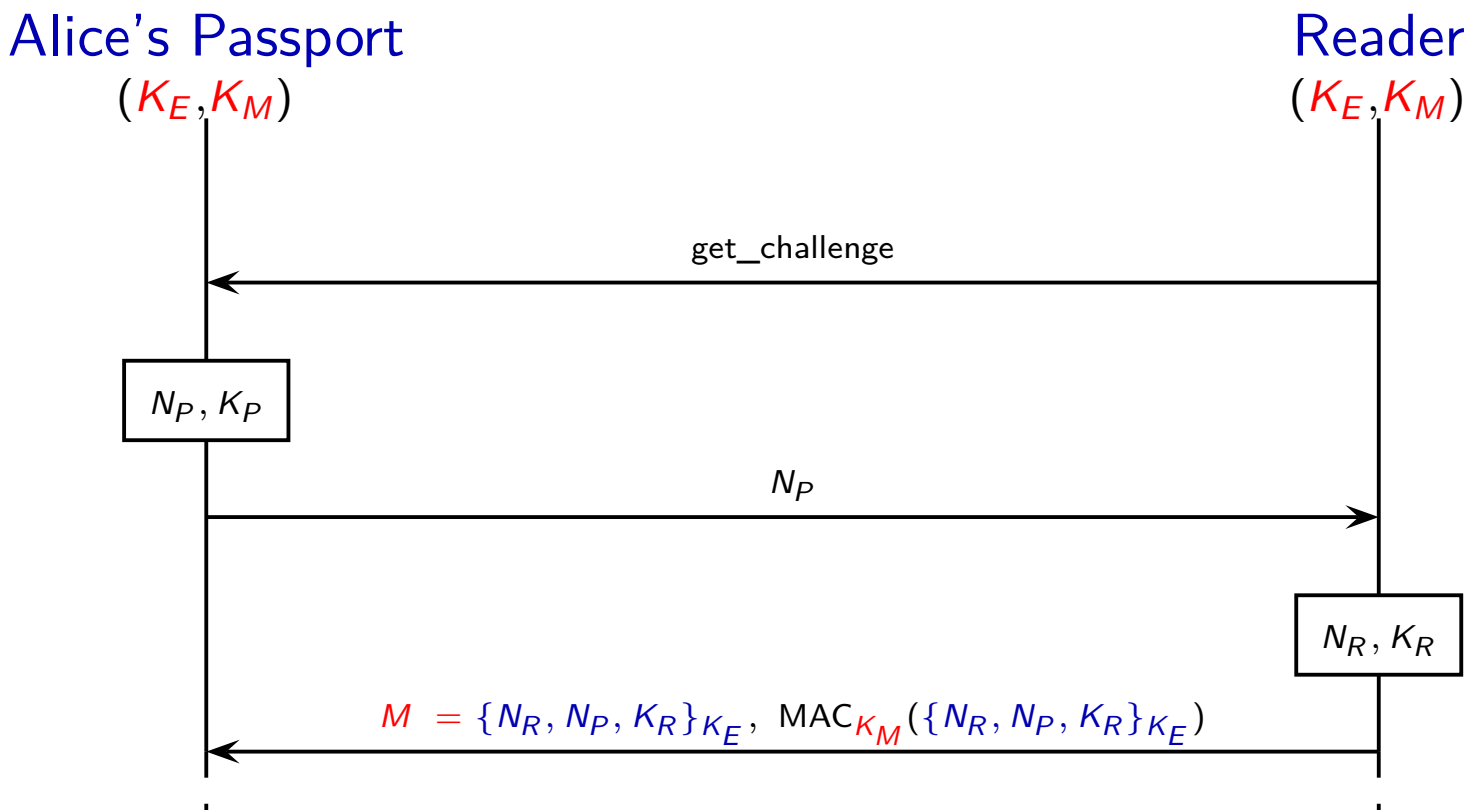
An attacker can track a French passport, provided he has once witnessed a successful authentication.

# 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.

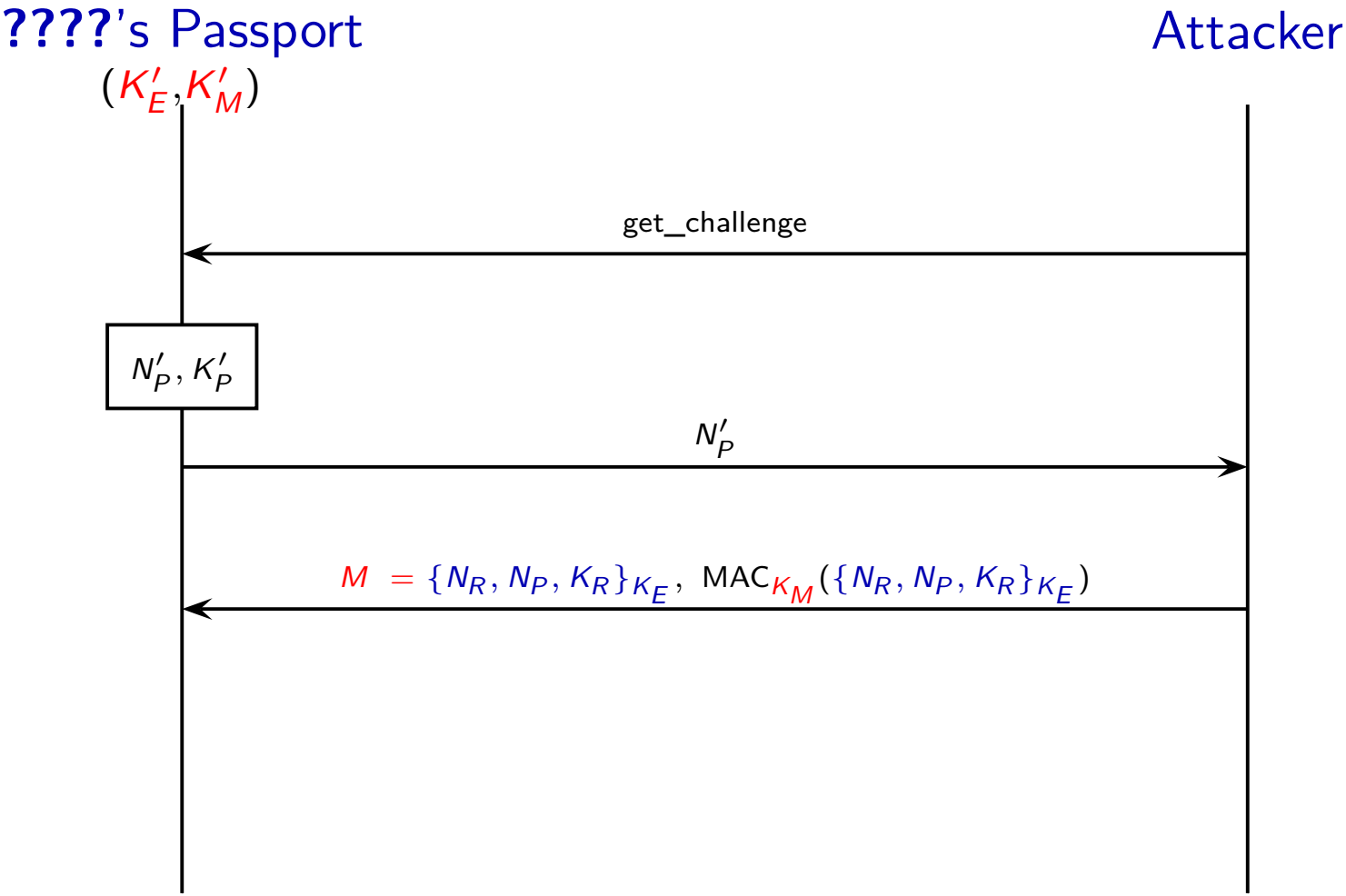
Part 1 of the attack. The attacker eavesdropes on Alice using her passport and records message $M$.



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

Part 2 of the attack.

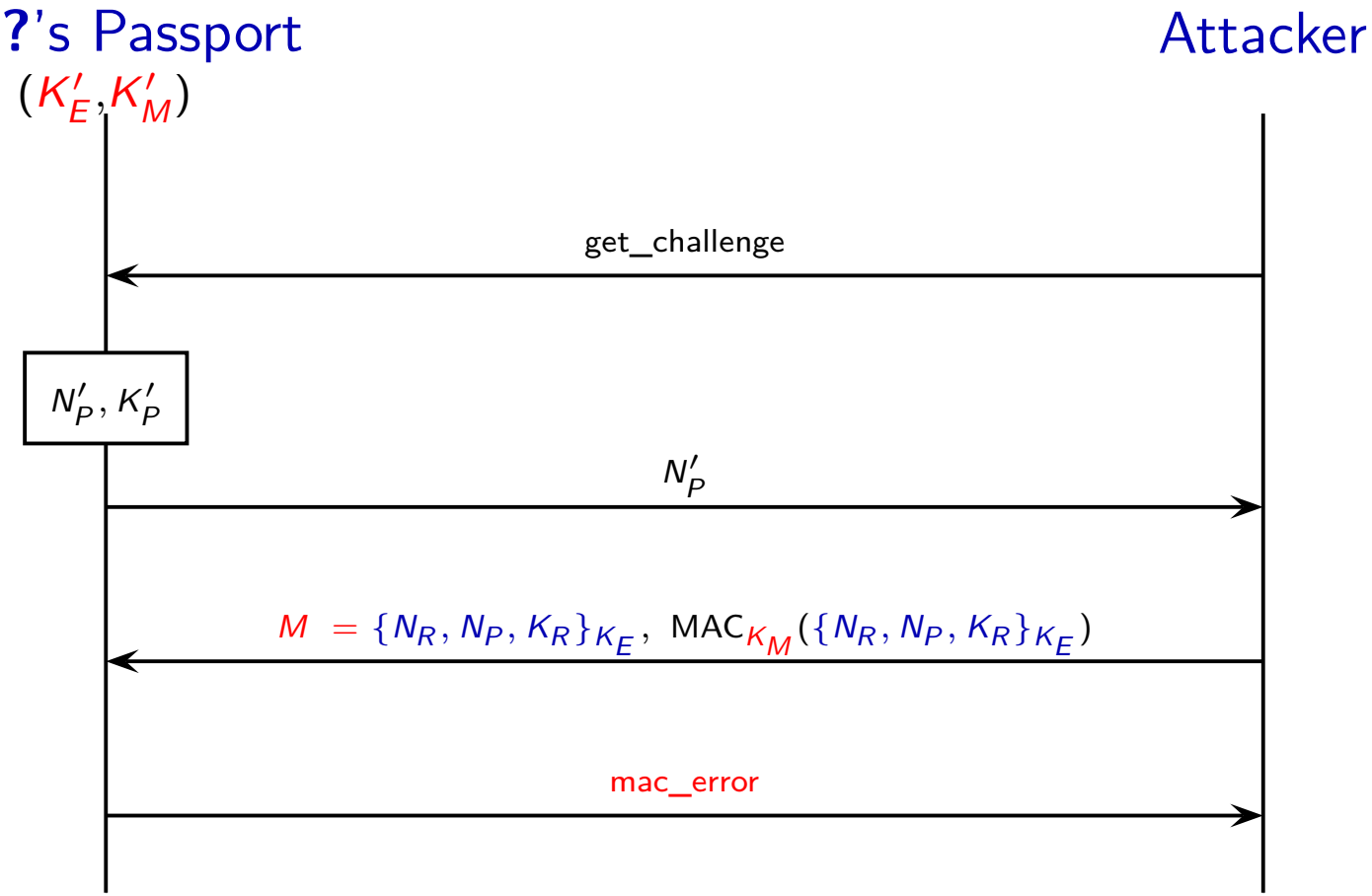
The attacker replays the message $M$ and checks the error code he receives.



# 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.

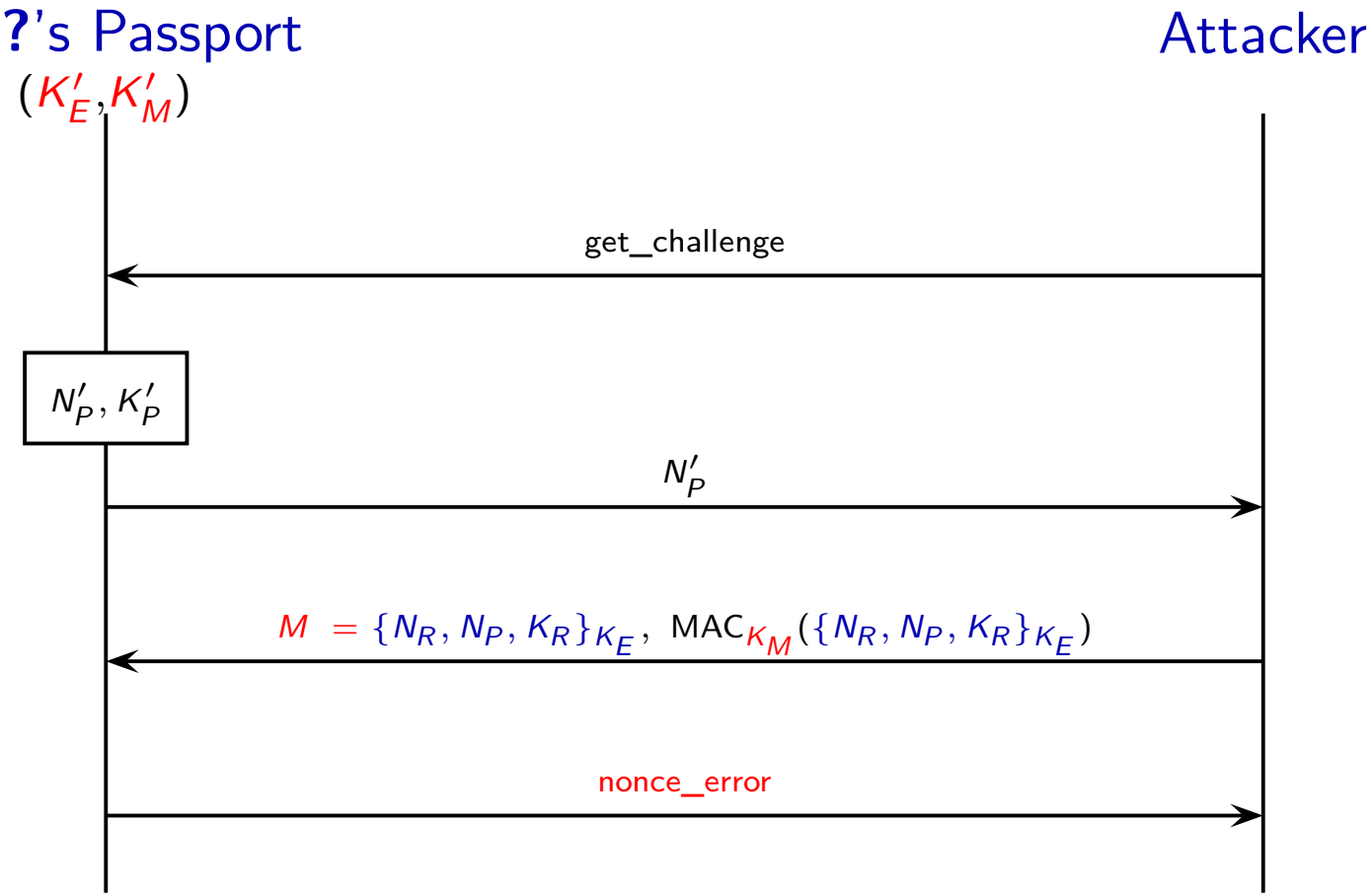



$\Longrightarrow$ MAC check failed $\Longrightarrow$ $K'_M \neq K_M$ $\Longrightarrow$ **????** is not Alice

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

Part 2 of the attack.

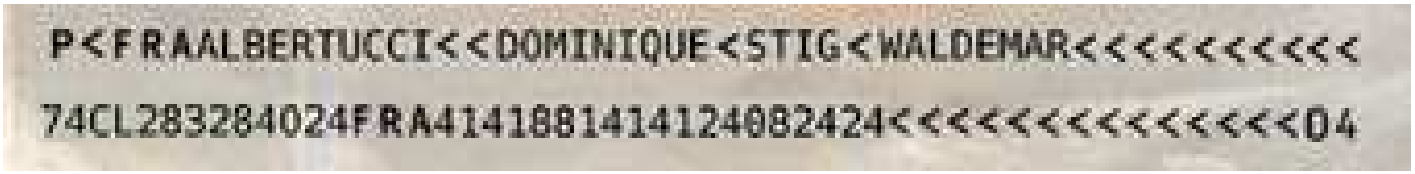
The attacker replays the message $M$ and checks the error code he receives.




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

# Et les Belges dans tout ça !

Possibilité de “deviner” les deux lignes codées.




$\longrightarrow$ les numéros des passeports ne sont pas attribués aléatoirement et sont particulièrement facile à deviner.

Gildas Avoine, Kassem Kalach, et Jean-Jacques Quisquater
Chercheurs à l'UCL, Belgique - Août 2007

# Some challenges for formal verification

**for analysing privacy-type security properties**

1. designing appropriate (and efficient) verification algorithms to analyse privacy-type properties
2. a need of composition results to be able to analyse *e.g.* the e-passport application and not only the BAC protocol

Some encouraging results:

- a prototype tool, called APTE, developed by Vincent Cheval.

  `http://projects.lsv.ens-cachan.fr/APTE/` [Cheval, 2014]

- some composition results to derive privacy guarantees on the whole application from the analysis of its components

  *e.g.* [Arapinis et al., 2012]

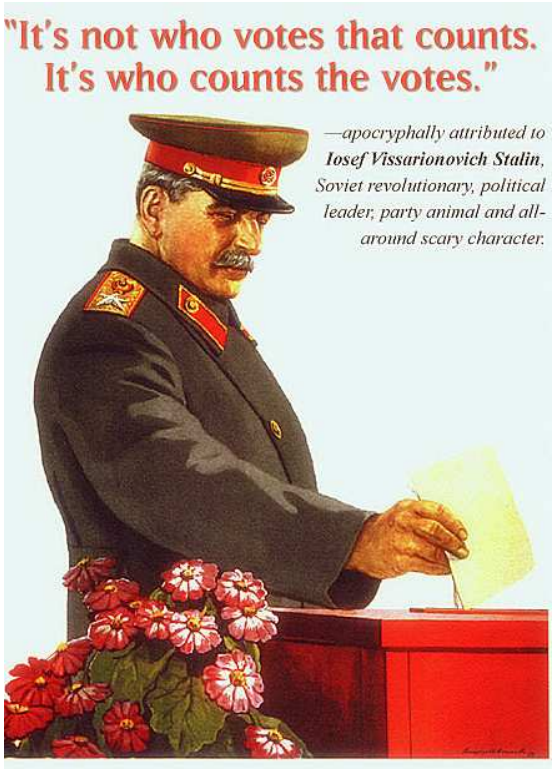
# Le vote électronique

# Vote électronique

**La démocratie est-elle en péril ?**

Avantages:

- pratique: différents types de scrutins, possibilité de voter de chez soi, ...
- décompte efficace des bulletins.




... mais il est souvent **opaque** et **invérifiable** !

# Deux grandes familles

## Machines à voter

- utilisation des bureaux de vote et des isoloirs;
- mécanisme d'authentification externe (*e.g.* carte d'identité)

# Deux grandes familles

## Machines à voter

- utilisation des bureaux de vote et des isoloirs;
- mécanisme d'authentification externe (*e.g.* carte d'identité)

$\longrightarrow$ machines NEDAP utilisées en France lors de scrutins nationaux (*e.g.* élection présidentielle de 2007)

# Deux grandes familles

## Machines à voter

- utilisation des bureaux de vote et des isoloirs;
- mécanisme d'authentification externe (*e.g.* carte d'identité)

$\longrightarrow$ machines NEDAP utilisées en France lors de scrutins nationaux (*e.g.* élection présidentielle de 2007)

## Vote par Internet

- possibilité de voter de chez soi avec son ordinateur personnel;

# Deux grandes familles

## Machines à voter

- utilisation des bureaux de vote et des isoloirs;
- mécanisme d'authentification externe (*e.g.* carte d'identité)

$\longrightarrow$ machines NEDAP utilisées en France lors de scrutins nationaux (*e.g.* élection présidentielle de 2007)

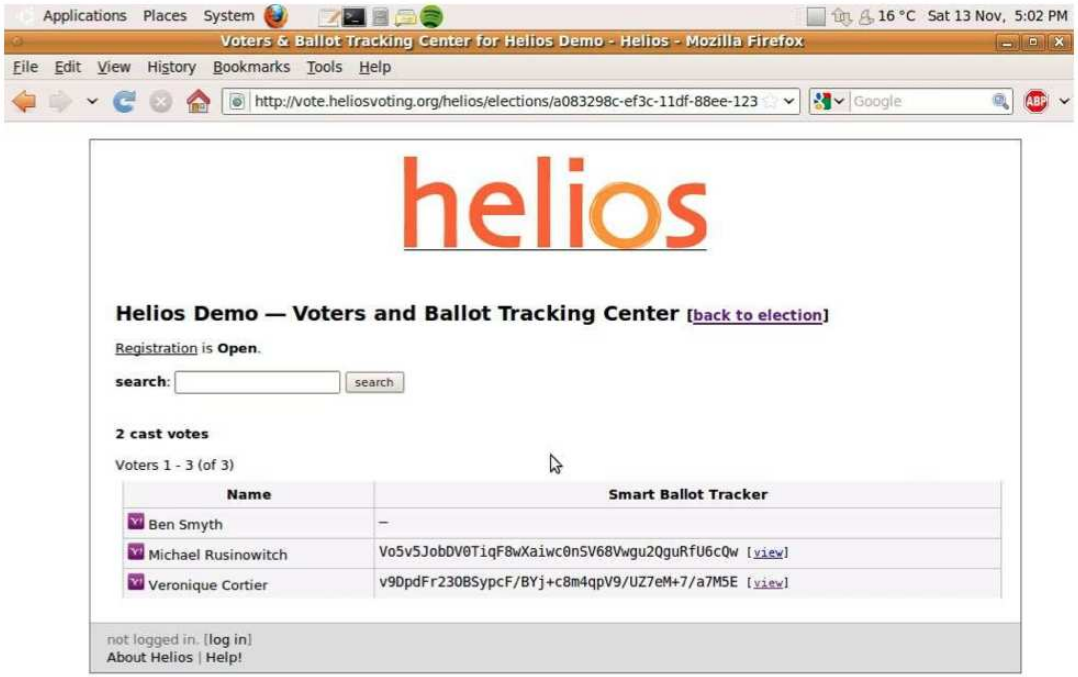
## Vote par Internet

- possibilité de voter de chez soi avec son ordinateur personnel;


$\longrightarrow$ utilisé en Suisse (depuis 2004), en Estonie (législatives 2011), en France pour des scrutins nationaux (*e.g.* élections législatives de 2012).

# Helios

$\longrightarrow$ développé par Ben Adida *et al.*




$\longrightarrow$ utilisé lors de plusieurs élections: à l'UCL, à l'Université de Princeton, ...

# Qu'est-ce qu'un bon protocole de vote ?

Vérifiabilité individuelle

Équité

Absence de reçu

Résistance à la coercition

Vérifiabilité universelle

Éligibilité

Anonymat

# Qu'est-ce qu'un bon protocole de vote ?

**Vérifiabilité individuelle**

Équité

Absence de reçu

**Résistance à la coercition**

Vérifiabilité universelle

Éligibilité

Anonymat

Est-ce qu'un bon protocole de vote existe ?

# Qu'est-ce qu'un bon protocole de vote ?

**Vérifiabilité individuelle**

Équité

Absence de reçu

**Résistance à la coercition**

Vérifiabilité universelle

Éligibilité

Anonymat

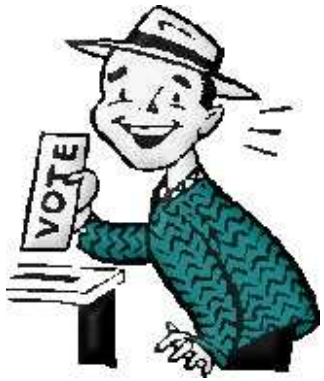
Est-ce qu'un bon protocole de vote existe ?

$\longrightarrow$ protocoles souvent complexes, utilisant des mécanismes cryptographiques « exotiques » et ne satisfaisant qu'un sous-ensemble des propriétés de sécurité ci-dessus.

# Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

| Tableau d'affichage | |
|---|---|
| *Alice* | $\{v_A\}_{\mathsf{pub}(S)}$ |
| *Bob* | $\{v_B\}_{\mathsf{pub}(S)}$ |
| *Chris* | $\{v_C\}_{\mathsf{pub}(S)}$ |

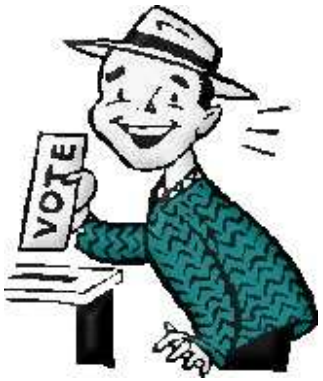


# Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

| Tableau d'affichage | |
|---|---|
| *Alice* | $\{v_A\}_{\mathsf{pub}(S)}$ |
| *Bob* | $\{v_B\}_{\mathsf{pub}(S)}$ |
| *Chris* | $\{v_C\}_{\mathsf{pub}(S)}$ |

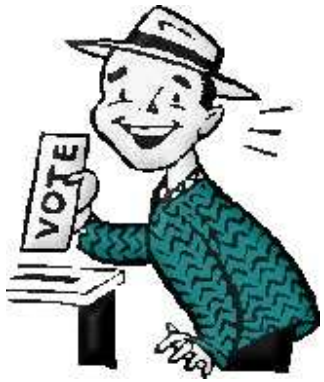
$\{v_D\}_{\mathsf{pub}(S)}$ ←



# Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

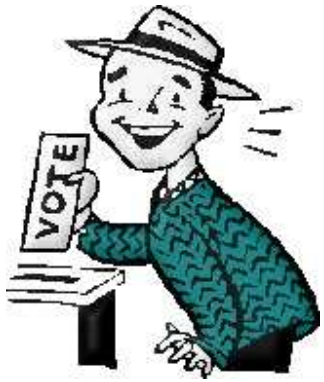
| Tableau d'affichage | |
|---|---|
| *Alice* | $\{v_A\}_{\mathsf{pub}(S)}$ |
| *Bob* | $\{v_B\}_{\mathsf{pub}(S)}$ |
| *Chris* | $\{v_C\}_{\mathsf{pub}(S)}$ |
| *David* | $\{v_D\}_{\mathsf{pub}(S)}$ |



# Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

| Tableau d'affichage | |
|---|---|
| *Alice* | $\{v_A\}_{\mathrm{pub}(S)}$ |
| *Bob* | $\{v_B\}_{\mathrm{pub}(S)}$ |
| *Chris* | $\{v_C\}_{\mathrm{pub}(S)}$ |
| *David* | $\{v_D\}_{\mathrm{pub}(S)}$ |




Phase de comptage: utilisation du chiffrement homomorphique

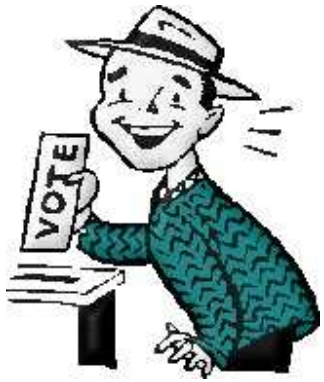
$$\{v_A\}_{\mathrm{pub}(S)} \times \{v_B\}_{\mathrm{pub}(S)} \times \ldots = \{v_A + v_B + \ldots\}_{\mathrm{pub}(S)}$$

$\longrightarrow$ Ainsi seul le résultat final sera déchiffré.

# Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

| Tableau d'affichage | |
|---|---|
| *Alice* | $\{v_A\}_{\mathrm{pub}(S)}$ |
| *Bob* | $\{v_B\}_{\mathrm{pub}(S)}$ |
| *Chris* | $\{v_C\}_{\mathrm{pub}(S)}$ |
| *David* | $\{v_D\}_{\mathrm{pub}(S)}$ |




Phase de comptage: utilisation du chiffrement homomorphique

$$\{v_A\}_{\mathrm{pub}(S)} \times \{v_B\}_{\mathrm{pub}(S)} \times \ldots = \{v_A + v_B + \ldots\}_{\mathrm{pub}(S)}$$

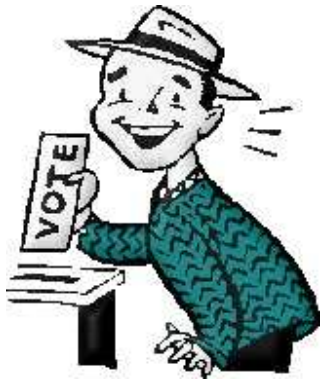
$\longrightarrow$ Ainsi seul le résultat final sera déchiffré.

**Un votant malhonnête pourrait tricher !**

# Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

| Tableau d'affichage | |
|---|---|
| *Alice* | $\{v_A\}_{\text{pub}(S)}$ |
| *Bob* | $\{v_B\}_{\text{pub}(S)}$ |
| *Chris* | $\{v_C\}_{\text{pub}(S)}$ |
| *David* | $\{v_D\}_{\text{pub}(S)}$ |




Phase de comptage: utilisation du chiffrement homomorphique

$$\{v_A\}_{\text{pub}(S)} \times \{v_B\}_{\text{pub}(S)} \times \ldots = \{v_A + v_B + \ldots\}_{\text{pub}(S)}$$

$\longrightarrow$ Ainsi seul le résultat final sera déchiffré.

**Un votant malhonnête pourrait tricher !**

$\{v_D\}_{\text{pub}(S)}$ " + " preuve que $v_D$ est égal à 0 ou 1

# Protocole Helios

## Vérifiabilité individuelle et universelle

Helios satisfait a priori les différentes formes de vérifiabilité.

# Protocole Helios

## Vérifiabilité individuelle et universelle

Helios satisfait a priori les différentes formes de vérifiabilité.

## Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote

# Protocole Helios

## Vérifiabilité individuelle et universelle

Helios satisfait a priori les différentes formes de vérifiabilité.

## Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote
- **Helios ne satisfait même pas l'anonymat !**
  $\longrightarrow$ il est possible de rejouer un message et de voter comme une autre votant de son choix (sans pour autant connaître la valeur de son vote)

Attaque découverte en 2011 par B. Smyth et V. Cortier

# Some challenges for formal verification

**for analysing e-voting protocols**

1. formal definitions of all the requirements (*e.g.* receipt-freeness, coercion-resistance)
2. designing verification algorithms that take into account the properties of the cryptographic primitives (e.g. homomorphic encryption).
3. obtaining guarantees in a more realistic model

# Merci de votre attention

« [...] j'envie parmi les hommes quiconque sans péril mena jusqu'au terme une existence anonyme et obscure. »

EURIPIDE 480-406 av. J.-C.