Ces protocoles qui nous protègent ...

Stéphanie Delaune

Chargée de Recherche CNRS affectée au LSV
Équipe-Projet SecSI

L'enseignement en informatique à l'ENS Cachan

$\longrightarrow$ formation tournée vers les **fondements de l'informatique**

L'enseignement en informatique à l'ENS Cachan

$\longrightarrow$ formation tournée vers les **fondements de l'informatique**

- Les bases: calculabilité et logique, algorithmique, complexité, langages formels, programmation, ...
- Des enseignements plus poussés: preuves assistées par ordinateur, démonstration automatique, bioinformatique, ...

L'enseignement en informatique à l'ENS Cachan

$\longrightarrow$ formation tournée vers les **fondements de l'informatique**

- Les bases: calculabilité et logique, algorithmique, complexité, langages formels, programmation, ...
- Des enseignements plus poussés: preuves assistées par ordinateur, démonstration automatique, bioinformatique, ...

« La science informatique n'est pas plus la science des ordinateurs que l'astronomie n'est celle des téléscopes »

E. Dijkstra

La recherche au LSV

Ennemi public numéro 1: le bug !

La recherche au LSV

Ennemi public numéro 1: le bug !

$\longrightarrow$ accroître notre confiance dans les logiciels critiques

La recherche au LSV

Ennemi public numéro 1: le bug !

$\longrightarrow$ accroître notre confiance dans les logiciels critiques

- logiciel: texte relativement long écrit dans un langage spécifique et qui sera exécuté par un ordinateur
- critique: une défaillance peut avoir des conséquences désastreuses en termes humains ou économiques

Dans la vie quotidienne ...

Zune : le bug de l'an 2009 !

Il redémarre tout seul puis reste figé sur l'écran de démarrage.

Dans la vie quotidienne ... ou presque !

Sonde Mars Climate Orbiter - 26 septembre 1999

Perte de la sonde due ...

Dans la vie quotidienne ... ou presque !

Sonde Mars Climate Orbiter - 26 septembre 1999

Perte de la sonde due ... à un problème d'unité de mesure !

Équipe projet SECSI

Sécurité des Systèmes d'Information

- 4 permanents: H. Comon-Lundh, S. Delaune, J. Goubault-Larrecq, et G. Steel.




- 3 membres temporaires
- 4 doctorants

Protocoles cryptographiques

PayPal™

- petits programmes destinés à sécuriser nos communications (*e.g.* confidentialité, authentification)
- omniprésents dans notre vie quotidienne.

Protocoles cryptographiques

PayPal™

- petits programmes destinés à sécuriser nos communications (*e.g.* confidentialité, authentification)
- omniprésents dans notre vie quotidienne.

Protocoles cryptographiques

PayPal™

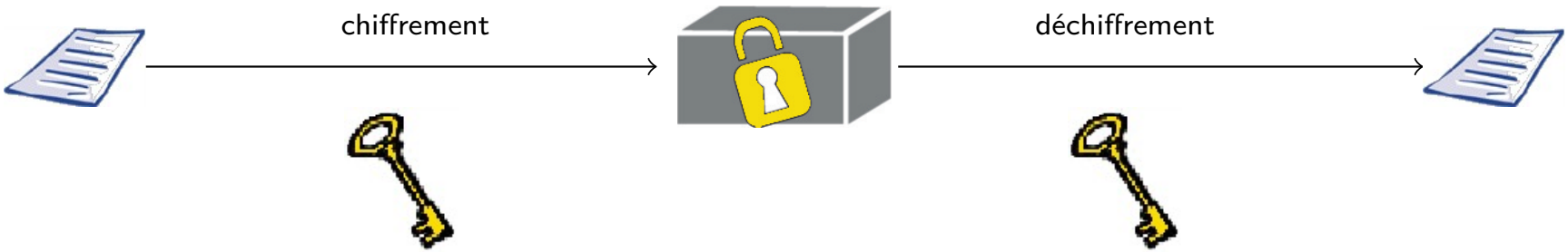
- petits programmes destinés à sécuriser nos communications (*e.g.* confidentialité, authentification)
- omniprésents dans notre vie quotidienne.

Nos informations personnelles sont en danger !

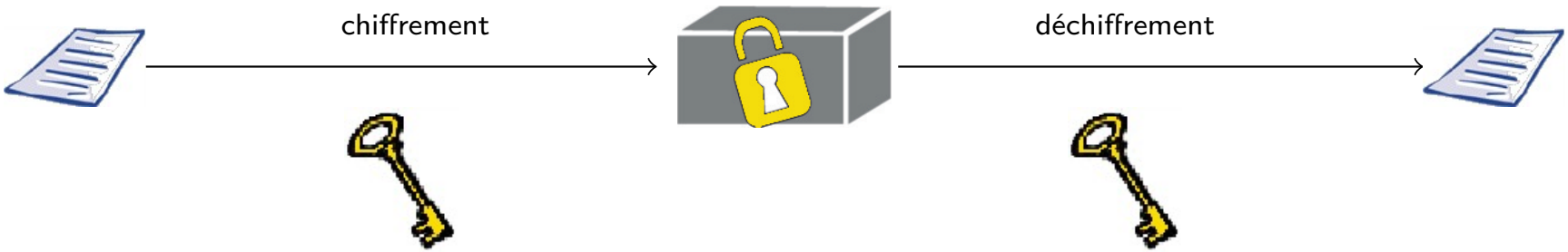
Le chiffrement

« HQVFD FKDQ »

Chiffrement symétrique



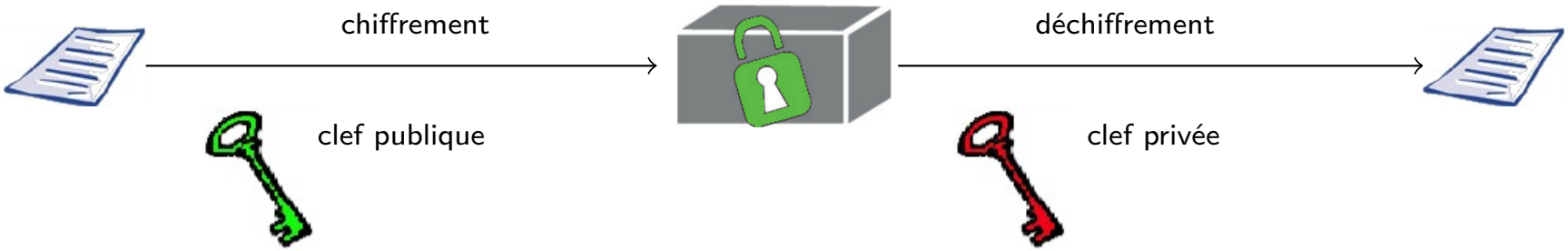
Chiffrement symétrique



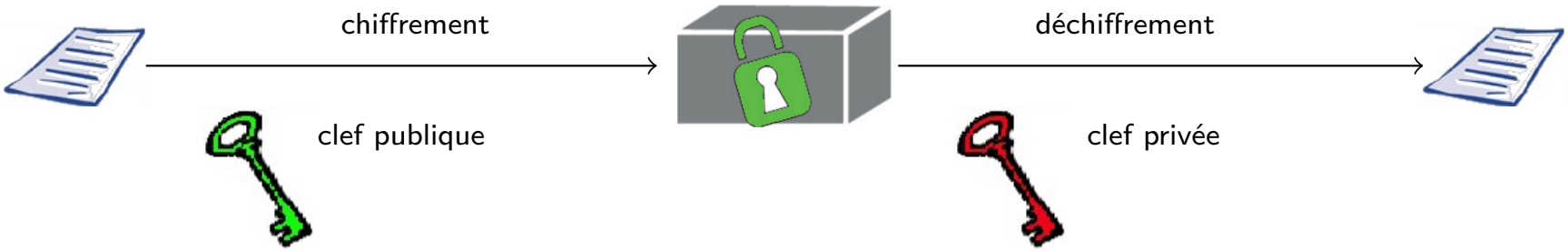
Quelques dates repères:

- 2000 avant J.-C.: traces de son utilisation par les Égyptiens
- 1920: machine Enigma
- 1977: Data Encryption Standard (DES)
- 2000: Advanced Encryption Standard (AES)

Chiffrement asymétrique (ou à clefs publiques)



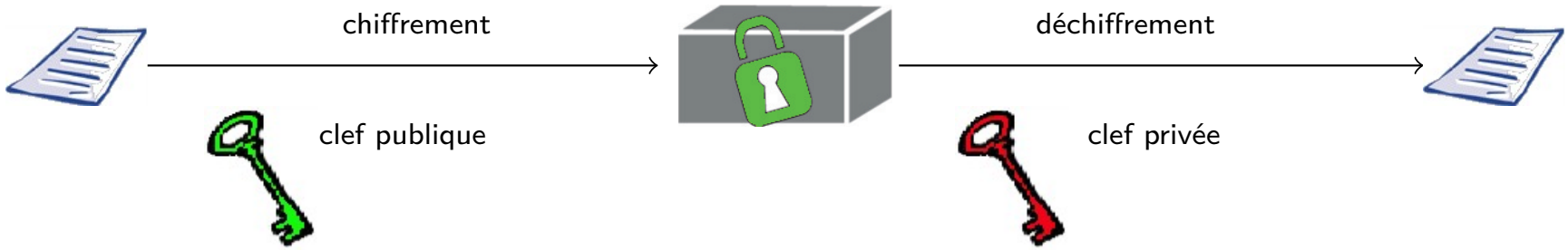
Chiffrement asymétrique (ou à clefs publiques)



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- cette méthode de chiffrement repose sur un problème mathématique bien connu: le problème de la factorisation.

Chiffrement asymétrique (ou à clefs publiques)



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- cette méthode de chiffrement repose sur un problème mathématique bien connu: le problème de la factorisation.

Nombre à 96 chiffres

$\longrightarrow$ utilisé pour sécuriser les cartes bancaires dans les années 80 et 90.

213598703592091008239502270499962879705109534182
641740644252416500858395774644508840500943086599 9

Mais chiffrer ne suffit pas toujours !

Le passeport électronique

Le vote électronique

La carte bancaire

Le smartphone

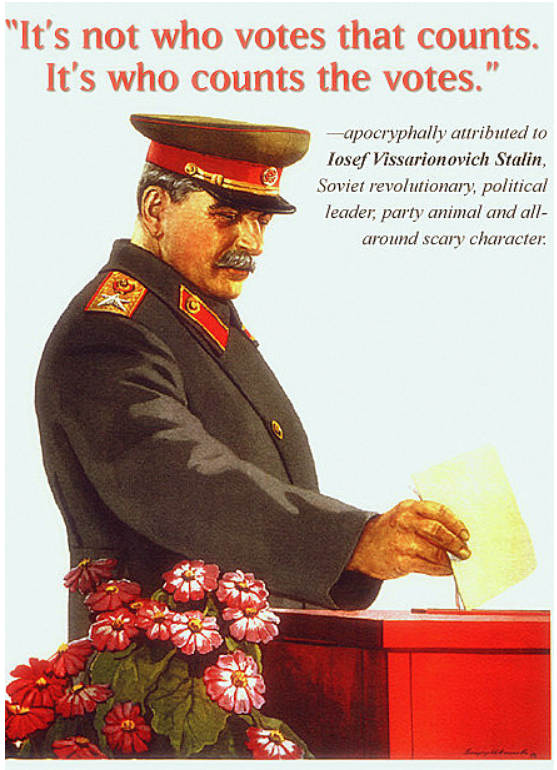
Vote électronique

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 / isoloirs;
- mécanisme d'authentification externe (*e.g.* carte d'identité)

Deux grandes familles

Machines à voter

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

$\longrightarrow$ utilisées dans 82 communes - élections présidentielles 2007

Deux grandes familles

Machines à voter

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

$\longrightarrow$ utilisées dans 82 communes - élections présidentielles 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 / isoloirs;
- mécanisme d'authentification externe (*e.g.* carte d'identité)

$\longrightarrow$ utilisées dans 82 communes - élections présidentielles 2007

Vote par Internet

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

$\longrightarrow$ 11 députés à l'Assemblée nationale ont été élus par voie électronique - élections législatives juin 2012

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

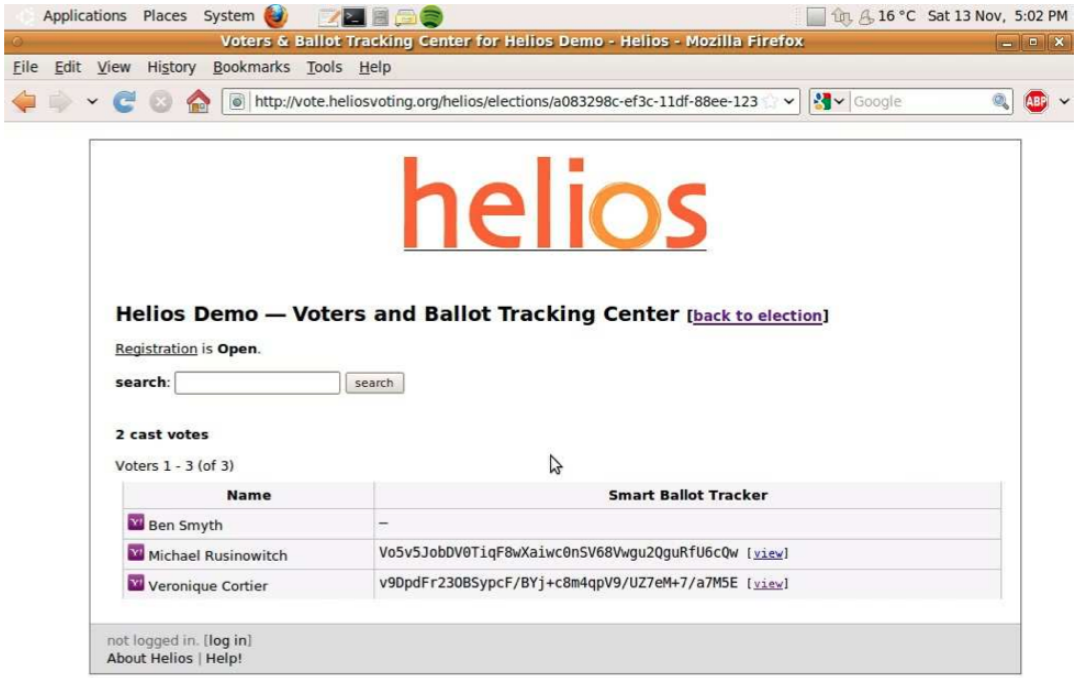
Anonymat

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.

Helios

$\longrightarrow$ développé par Ben Adida *et al.* (2009)



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

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	$\{v_A\}_{\text{pub}(S)}$
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.

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 !

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

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

1936: une telle machine n'existe pas (Alan Turing)

... même dans le cas particulier des protocoles cryptographiques.

Mais alors, que faisons-nous ?

Le problème n'a pas de solution ....

Mais alors, que faisons-nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Mais alors, que faisons-nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Différentes pistes:

- résoudre le problème dans de nombreux cas intéressants
- proposer des procédures approchées

Mais alors, que faisons-nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

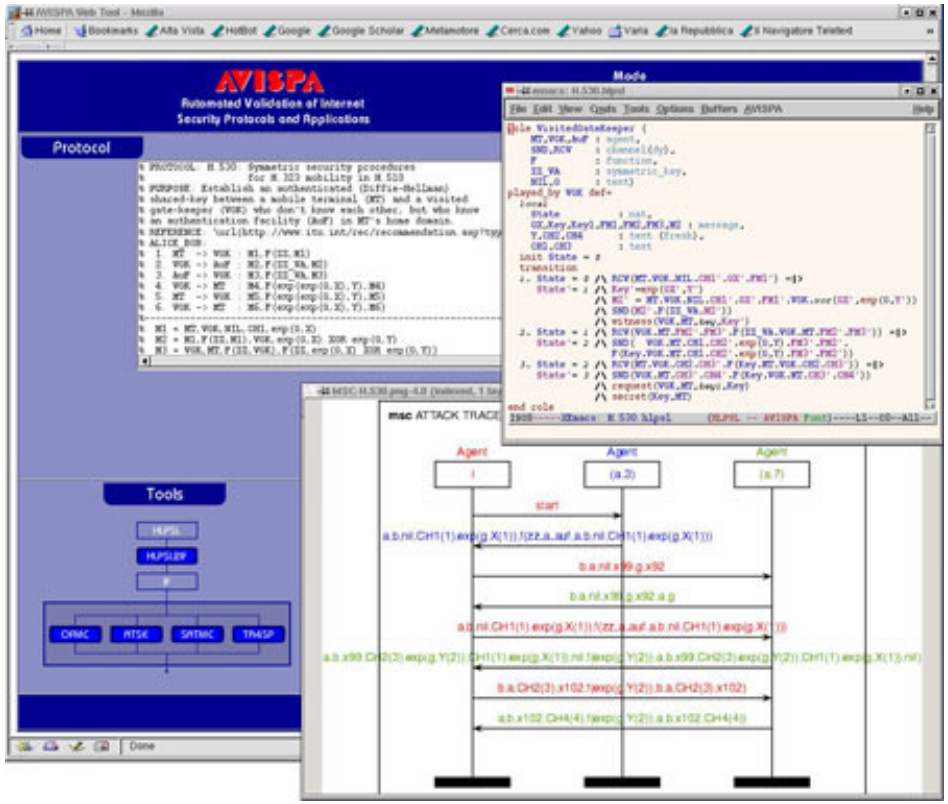
Différentes pistes:

- résoudre le problème dans de nombreux cas intéressants
- proposer des procédures approchées

$\longrightarrow$ **Prix Turing** décerné à Joseph Sifakis en 2007 pour ses travaux sur le model-checking.

Outil de vérification AVISPA

Outil disponible en ligne: `http://www.avispa-project.org/`



$\longrightarrow$ Projet Européen (France, Italie, Allemagne, Suisse)

Conclusion

Les méthodes formelles permettent une bonne analyse des protocoles cryptographiques.

- découverte de failles à l'aide d'outil de vérification;
- des preuves formelles de sécurité peuvent être obtenues automatiquement (sans intervention humaine).

Conclusion

Les méthodes formelles permettent une bonne analyse des protocoles cryptographiques.

- découverte de failles à l'aide d'outil de vérification;
- des preuves formelles de sécurité peuvent être obtenues automatiquement (sans intervention humaine).

Il reste cependant beaucoup à faire:

- savoir analyser différentes propriétés de sécurité
  $\longrightarrow$ l'anonymat sous toutes ses formes!
- prendre en compte les propriétés mathématiques du chiffrement (e.g. chiffrement homomorphique)
- réaliser ses analyses formelles dans des modèles plus réalistes.

MERCI