

Inria
INVENTEURS DU MONDE NUMÉRIQUE



Big Brother
won't watch us !

ENS Cachan



- ▶ 17 départements d'enseignement: mathématiques, informatique, chimie, génie mécanique, sciences sociales, . . .
- ▶ 14 laboratoires de recherche:

Laboratoire Spécification & Vérification



La recherche au LSV

Ennemi public numéro 1: le **bug** !



La recherche au LSV

Ennemi public numéro 1: le **bug** !



→ accroître notre confiance dans les **logiciels critiques**

Ennemi public numéro 1: le bug !



—> 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 !

Dans la vie quotidienne !



Sonde Mars Climate Orbiter - 26 septembre 1999



Perte de la sonde due ...

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.



- ▶ 6 membres temporaires
- ▶ 6 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

« XQLWKH RX FDIH »

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**.

*Tant que nous ne sommes pas capables de résoudre ce problème d'une façon **efficace**, la méthode de chiffrement RSA sera considérée sûre.*

Mais chiffrer ne suffit pas toujours !

La carte bancaire



Le vote électronique



Le passeport électronique

La carte bancaire

La carte bancaire est protégée par un grand nombre public dont on ne connaît pas la **factorisation**.



La carte bancaire

La carte bancaire est protégée par un grand nombre public dont on ne connaît pas la **factorisation**.



Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
4165008583957746445088405009430865999

La carte bancaire

La carte bancaire est protégée par un grand nombre public dont on ne connaît pas la **factorisation**.



Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
4165008583957746445088405009430865999

Affaire Serge Humpich (1997)

il factorise ce nombre de 96 chiffres et conçoit de fausses cartes bleues (les « **YesCard** »).

Le protocole de paiement



- ▶ Le client CI insère sa carte C dans le terminal T .
 - ▶ Le marchand saisit le montant M de la transaction.
-
- ▶ Le terminal vérifie qu'il s'agit d'une « vraie carte ».
 - ▶ Le client entre son code.
Si $M \geq \text{€}100$, alors dans 20% des cas,
 - ▶ Le terminal contacte la banque B .
 - ▶ La banque donne (ou pas) son autorisation.



En détails (1/2)

4 acteurs: la Banque *B* , le Client *Cl*, la Carte *C* et le Terminal *T*



En détails (1/2)

4 acteurs: la Banque B , le Client Cl , la Carte C et le Terminal T

La **Banque** possède

- ▶ une **clef privée** – $\text{priv}(B)$
- ▶ une **clef publique** – $\text{pub}(B)$
- ▶ une **clef symétrique secrète** partagée avec la carte – K_{CB}

En détails (1/2)

4 acteurs: la Banque B , le Client Cl , la Carte C et le Terminal T

La **Banque** possède

- ▶ une **clef privée** – $\text{priv}(B)$
- ▶ une **clef publique** – $\text{pub}(B)$
- ▶ une **clef symétrique secrète** partagée avec la carte – K_{CB}

La **Carte** possède

- ▶ des données **Data**: nom du propriétaire, date d'expiration, ...
- ▶ la signature de ces données – $\{\text{Data}\}_{\text{priv}(B)}$
- ▶ la clef K_{CB} , clef secrète partagée avec la banque.

En détails (1/2)

4 acteurs: la Banque B , le Client Cl , la Carte C et le Terminal T

La **Banque** possède

- ▶ une **clef privée** – $\text{priv}(B)$
- ▶ une **clef publique** – $\text{pub}(B)$
- ▶ une **clef symétrique secrète** partagée avec la carte – K_{CB}

La **Carte** possède

- ▶ des données *Data*: nom du propriétaire, date d'expiration, ...
- ▶ la signature de ces données – $\{\text{Data}\}_{\text{priv}(B)}$
- ▶ la clef K_{CB} , clef secrète partagée avec la banque.

Le **Terminal** possède

- ▶ la **clef publique** de la banque – $\text{pub}(B)$

En détails (2/2)

Le terminal T lit la carte C :

1. $C \rightarrow T : Data, \{Data\}_{\text{priv}(B)}$

En détails (2/2)

Le terminal T lit la carte C :

1. $C \rightarrow T$: $Data, \{Data\}_{priv(B)}$

Le terminal T demande le code:

2. $T \rightarrow CI$: $code?$

3. $CI \rightarrow C$: 1234

4. $C \rightarrow T$: code bon

En détails (2/2)

Le terminal T lit la carte C :

1. $C \rightarrow T$: $Data, \{Data\}_{priv(B)}$

Le terminal T demande le code:

2. $T \rightarrow C$: $code?$

3. $C \rightarrow T$: 1234

4. $C \rightarrow T$: code bon

Le terminal T demande l'autorisation à la banque B :

5. $T \rightarrow B$: $autorisation?$

6. $B \rightarrow T$: 45289

7. $T \rightarrow C$: 45289

8. $C \rightarrow T$: $\{45289\}_{K_{CB}}$

9. $T \rightarrow B$: $\{45289\}_{K_{CB}}$

10. $B \rightarrow T$: ok

Attaques sur la carte bleue

Initialement la sécurité été assurée par :

- ▶ cartes difficilement répliquables,
- ▶ secret des clefs et du protocole.



Attaques sur la carte bleue

Initialement la sécurité été assurée par :

- ▶ cartes difficilement répliquables,
- ▶ secret des clefs et du protocole.



Mais il y a des failles !

- ▶ le chiffrement n'est pas sûr (les clefs de 320 bits ne sont plus sûres);
- ▶ on peut faire des fausses cartes.

→ “YesCard” fabriquées par Serge Humpich (1997).

La « YesCard »: Comment ça marche ?

Faible logique

1. $C \rightarrow T$: $\text{Data}, \{\text{Data}\}_{\text{priv}(B)}$

2. $T \rightarrow Cl$: *code?*

3. $Cl \rightarrow C$: 1234

4. $C \rightarrow T$: *ok*

La « YesCard »: Comment ça marche ?

Faible logique

1. $C \rightarrow T$: $\text{Data}, \{\text{Data}\}_{\text{priv}(B)}$
2. $T \rightarrow Cl$: *code?*
3. $Cl \rightarrow C'$: **2345**
4. $C' \rightarrow T$: *ok*

La « YesCard »: Comment ça marche ?

Faible logique

1. $C \rightarrow T$: **Data**, $\{\text{Data}\}_{\text{priv}(B)}$
2. $T \rightarrow Cl$: *code?*
3. $Cl \rightarrow C'$: **2345**
4. $C' \rightarrow T$: *ok*

Ajout d'une fausse signature sur une fausse carte

1. $C' \rightarrow T$: **XXX**, $\{\text{XXX}\}_{\text{priv}(B)}$
2. $T \rightarrow Cl$: *code?*
3. $Cl \rightarrow C'$: 0000
4. $C' \rightarrow T$: *ok*

Corrections apportées

Utilisation de plus grands nombres pour sécuriser les cartes bancaires

→ 232 chiffres au lieu des 96 chiffres utilisés en 1997.

Corrections apportées

Utilisation de plus grands nombres pour sécuriser les cartes bancaires

→ 232 chiffres au lieu des 96 chiffres utilisés en 1997.

Europay, MasterCard et Visa (EMV) ont produit 3 nouveaux protocoles:

1. SDA: Static Data Authentication

→ Ce système est le plus couramment utilisé.

2. DDA: Dynamic Data Authentication

→ Ce système devrait permettre de lutter efficacement contre l'utilisation des "YesCards".

3. CDA: Combined Data Authentication

→ conçus en 2004 et déployés en 2006.



Le passeport électronique



Passeport électronique

Un passeport électronique est un passeport contenant une **puce RFID**.

→ ils sont délivrés en France depuis l'été 2006.



Passeport électronique

Un passeport électronique est un passeport contenant une **puce RFID**.

→ 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**.

→ 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 !

Aucun mécanisme de sécurité pour protéger les informations personnelles



Aucun mécanisme de sécurité pour protéger les informations personnelles



→ possibilité de récupérer la signature manuscrite du porteur en interrogeant le passeport à distance

Aucun mécanisme de sécurité pour protéger les informations personnelles



→ 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 émis à partir de 2006 en **France**,
en Belgique, ...



Protocole BAC - objectif



Le Basic Access Control (BAC) protocole est un protocole d'établissement de clef qui doit assurer la protection de nos données personnelles ainsi que la **non traçabilité** du passeport.

Protocole BAC - objectif



Le Basic Access Control (BAC) protocole est un protocole d'établissement de clef qui doit assurer la protection de nos données personnelles ainsi que la **non traçabilité** du passeport.

ISO/IEC standard 15408

La **non traçabilité** a pour but d'assurer qu'un utilisateur peut utiliser plusieurs fois un service ou une ressource sans permettre à un tiers de faire un lien entre ces différentes utilisations.

Protocole BAC



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.

Attaque sur le passeport Français

DÉMO

(merci à Myrto Arapinis, Tom Chothia, et Vincent Cheval
... et à tous ceux qui m'ont prêté leur passeport.)

Attaque découverte en 2010 par T. Chothia et V. Smirnov





SAC : Passeport 3e génération

Une nouvelle dimension dans la sécurité du passeport électronique

Je cite: « Ce mécanisme offre des **propriétés de sécurité supérieures** à celle du mécanisme BAC et garantit ainsi une très haute protection de l'anonymat du porteur. Il assure les propriétés de: **non liable, non transférable, et intraçable.** »

Vote électronique

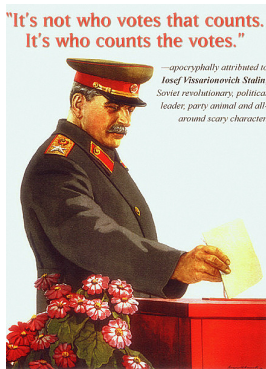


Vote électronique

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 isolements;
- ▶ mécanisme d'authentification externe (*e.g.* carte d'identité)

Deux grandes familles



Machines à voter

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

→ 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 isolements;
- ▶ mécanisme d'authentification externe (e.g. carte d'identité)

→ 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 isolements;
- ▶ mécanisme d'authentification externe (e.g. carte d'identité)

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

Vote par Internet

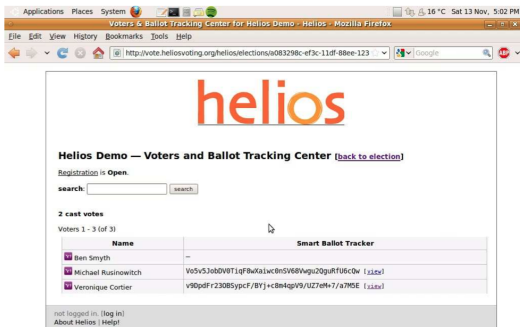
- ▶ possibilité de voter de **chez soi** avec son ordinateur personnel;

→ utilisé en Estonie (législatives 2011), en Suisse (depuis 2004), en France (e.g. **élections prud'homales**)



Helios

→ développé par Ben Adida *et al.*



The screenshot shows a web browser window with the title "Voters & Ballot Tracking Center for Helios Demo - Helios - Mozilla Firefox". The address bar shows the URL "http://vote.heliosvoting.org/helios/elections/a083298c-ef3c-11df-88ee-123". The page content includes the "helios" logo, the heading "Helios Demo — Voters and Ballot Tracking Center" with a link to "back to election", and the status "Registration is Open." Below this is a search bar with a "search" button. A section titled "2 cast votes" shows a list of voters with their names and unique identifiers. At the bottom, there is a footer with "not logged in. [log in]" and "About Helios | Help!".

Name	Smart Ballot Tracker
Ben Smyth	--
Michael Rusinowitch	Vo5v5Job0VBT1qf8wXaIwc0n5V68Vagu20guRfU6cQw [x12x]
Veronique Cortier	v90pdFr23085ypcF/BYj+cBm4qpV9/UZ7etf+7/a7MDE [x12x]

→ utilisé lors de plusieurs élections: à l'UCL, à l'Université de Princeton, ...

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

Équité

Vérifiabilité individuelle

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 ?

→ 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

<i>Alice</i>	$\{v_A\}_{\text{pub}(S)}$
<i>Bob</i>	$\{v_B\}_{\text{pub}(S)}$
<i>Chris</i>	$\{v_C\}_{\text{pub}(S)}$



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	$\{v_C\}_{\text{pub}(S)}$
-------	---------------------------

$\{v_D\}_{\text{pub}(S)}$

←



Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

<i>Alice</i>	$\{v_A\}_{\text{pub}(S)}$
<i>Bob</i>	$\{v_B\}_{\text{pub}(S)}$
<i>Chris</i>	$\{v_C\}_{\text{pub}(S)}$
<i>David</i>	$\{v_D\}_{\text{pub}(S)}$



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 homomorphe

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

→ Ainsi seul le résultat final sera déchiffré.

Protocole Helios (version simplifiée)

Phase de vote: (valeur 0 ou 1)

Tableau d'affichage

Alice	$\{v_A\}_{pub(S)}$
Bob	$\{v_B\}_{pub(S)}$
Chris	$\{v_C\}_{pub(S)}$
David	$\{v_D\}_{pub(S)}$



Phase de comptage: utilisation du chiffrement homomorphe

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

→ 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	$\{v_A\}_{pub(S)}$
Bob	$\{v_B\}_{pub(S)}$
Chris	$\{v_C\}_{pub(S)}$
David	$\{v_D\}_{pub(S)}$



Phase de comptage: utilisation du chiffrement homomorphe

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

→ Ainsi seul le résultat final sera déchiffré.

Un votant malhonnête pourrait tricher !

$\{v_D\}_{pub(S)}$ " + " 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
→ 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
→ il est possible d'obtenir un reçu de son vote
- ▶ **Helios ne satisfait même pas l'anonymat !**
→ 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

MERCI

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

EURIPIDE 480-406 av. J.-C.