La cryptographie au secours du vote électronique

Marc Girault (avec **Jacques Traoré**)
France Télécom
Division R&D – Site de Caen

Symposium SSTIC - 1er juin 2007

Précision

- Cet exposé est également inspiré de La Lettre Techniques de l'Ingénieur – Sécurité des Systèmes d'Information
  - numéro de mai 2007, édité par F. Veysset
  - remerciements à D. Arditti, C. Blancher, G. Grattard, M. Chochois, P. Chauvaud et E. Bruillon

Sommaire

1 Introduction

Définition

- Un système de vote est dit électronique s'il implique le recours à des moyens électroniques au moins lors de l'enregistrement du suffrage
  - cf. Recommandation du Conseil de l'Europe, 30 septembre 2004
  - pas d'urne matérielle
  - pas de comptage humain

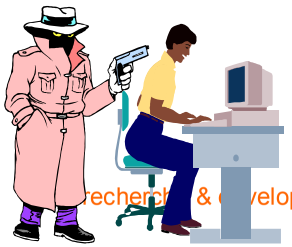
- Les autres phases (inscription sur les listes électorales, identification/émargement, expression du choix) peuvent être manuelles, électroniques ou mixtes

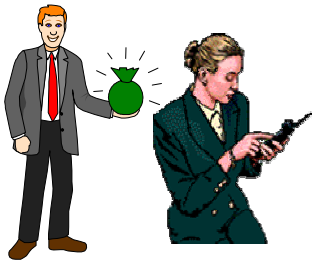
Classification

- Vote hors-ligne
  - contrôlé par une autorité électorale
  - machines à voter autonomes

- Vote hybride
  - contrôlé par une autorité électorale
  - machines à voter reliées en réseau

- Vote en ligne (à distance)
  - non contrôlé par une autorité électorale
  - (typiquement) par réseau Internet ou mobile





Arguments

- Réduction de coûts (personnel, papier)
- Dépouillement : facilité, rapidité, fiabilité
- Recul de l'abstention
- Augmentation du nombre de consultations
- Facilitation pour les handicapés
- Modernité
- …

Le contexte national (1)

- Vote hors-ligne 
  - autorisé pour des élections politiques depuis le décret n° 69-419 du 10 mai 1969
  - mis en oeuvre par plusieurs communes lors du référendum sur la constitution européenne en mai 2005 et des élections présidentielles 2007
  - utilisation très encadrée :
    - CNIL : recommandation du 1er juillet 2003
    - Ministère de l'Intérieur : réglementation technique comportant 114 exigences à respecter
    - seulement 3 types de machines à voter agréés

Le contexte national (2)

- Vote hybride 
  - pourrait-être autorisé à moyen terme pour des élections politiques

- Vote en ligne 
  - assimilé au vote par correspondance (interdit depuis 1975)
  - autorisé toutefois, depuis 2003, pour les élections consulaires et prud'hommales

Le contexte international

- Vote hors-ligne 
  - Belgique, Brésil, Etats-Unis
- Vote hybride 
  - Italie : utilisation de bornes de vote E-Poll pour un scrutin local (Ladispoli)
- Vote en ligne (par Internet) 
  - Estonie : à l'échelle nationale lors des élections municipales d'octobre 2005
  - Corée : élections majeures d'ici 2012
  - Suisse : expérimentations lors de référendums entre 2003 et 2005

Vote hors ligne : l'existant (1)

- Plusieurs systèmes, dont 3 homologués en France :
  - Nedap – France Election
  - ES&S – Datamatique
  - Indra Systemas

- Objections
  - systèmes opaques (codes-sources indisponibles, résultats invérifiables)
  - systèmes non certifiés (malgré l'existence d'un profil de protection)

Vote hors ligne : l'existant (2)

- Attaques (en vrac)
  - Pays-Bas, France : introduction (ou substitution) de faux composants (cartes électroniques)
  - Princeton : introduction d'un programme malicieux en < 1mn
  - Arkansas : un candidat n'a recueilli aucun suffrage alors qu'il a voté pour lui
  - Belgique : nombre de votants >> nombre d'inscrits

Propriétés de sécurité (1)

- Conformité aux listes électorales [CONF]
  - tout électeur inscrit peut voter une et une seule fois
- Anonymat [ANO]
  - parfait ou non
  - non révocable
- Vote sans contraintes [CONT]
  - personne n'est capable de contraindre ou soudoyer un électeur
- Vote sans preuve [PRV]
  - un électeur est incapable de prouver pour qui il a voté

Propriétés de sécurité (2)

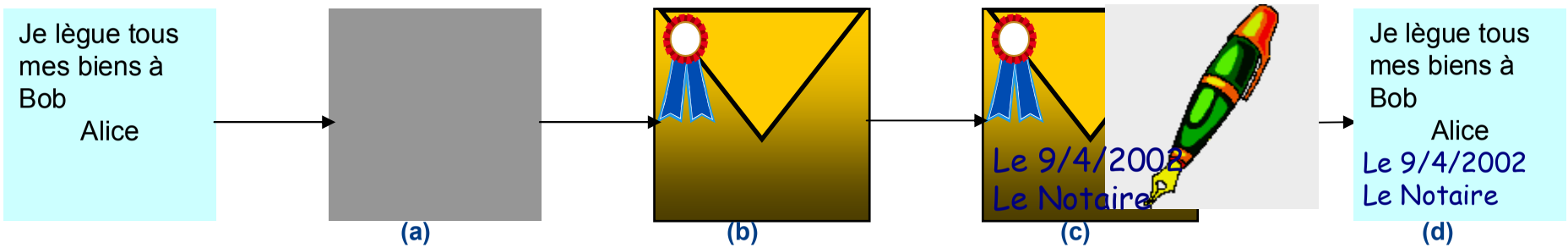
- Vérification (individuelle) du vote [VER1]
  - l'électeur peut vérifier que son vote a été pris en compte…
- Vérification (universelle) du vote [VER2]
  - … ainsi que tous les autres votes
- Pas de résultats partiels [PAR]
  - personne ne peut obtenir de résultats partiels

La question de la confiance

- Assurer ces propriétés est une chose
- Démontrer qu'on les assure en est une autre
  - "What you see is what you vote for"
  - Comment en convaincre l'électeur ?
- Deux approches
  - amont : certification (critères d'évaluation)
  - aval : tests de conformité par "prélèvements"

2 Signatures aveugles

Principe



a) Alice superpose une feuille de papier carbone

b) Alice insère le tout dans une enveloppe qu'elle cachète

c) Le notaire appose sa signature sur l'enveloppe

d) Alice décachète l'enveloppe et récupère le message signé

Avec RSA

Utilisateur

Signataire
PK = (n,e)
SK = d

r, m

$x = mr^e \pmod n$

x

$y = x^d = m^d r^{ed} = m^d r \pmod n$

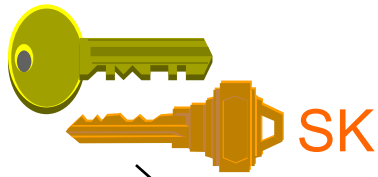
y

$s = y/r = m^d \pmod n$

non-corrélable

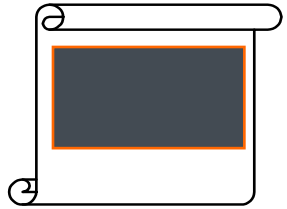
(m,s) ⟷ (x,y)

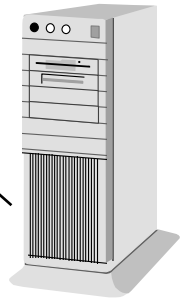
Authentification/vote



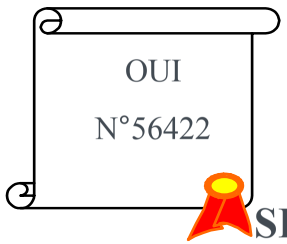
Liste Electorale

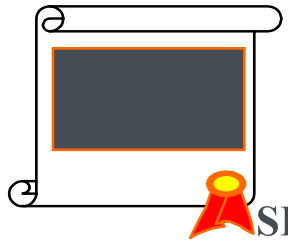
Mr Dupond
Mr Dupont
Mr Durand
.
.
Miss Alice X

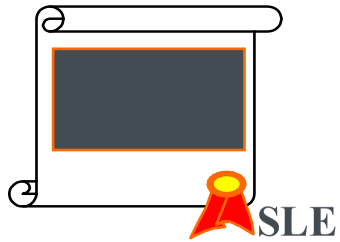




Serveur de liste électorale

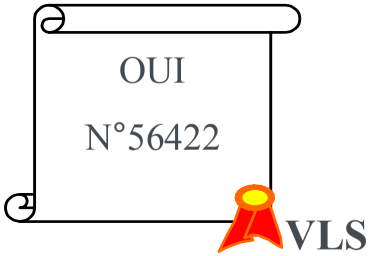




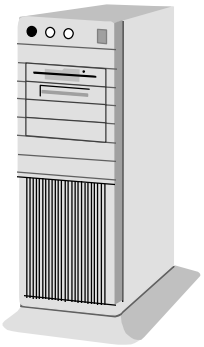


Signe en aveugle

Dépôt du bulletin



Canal Anonyme



Urne

Propriétés de Sécurité

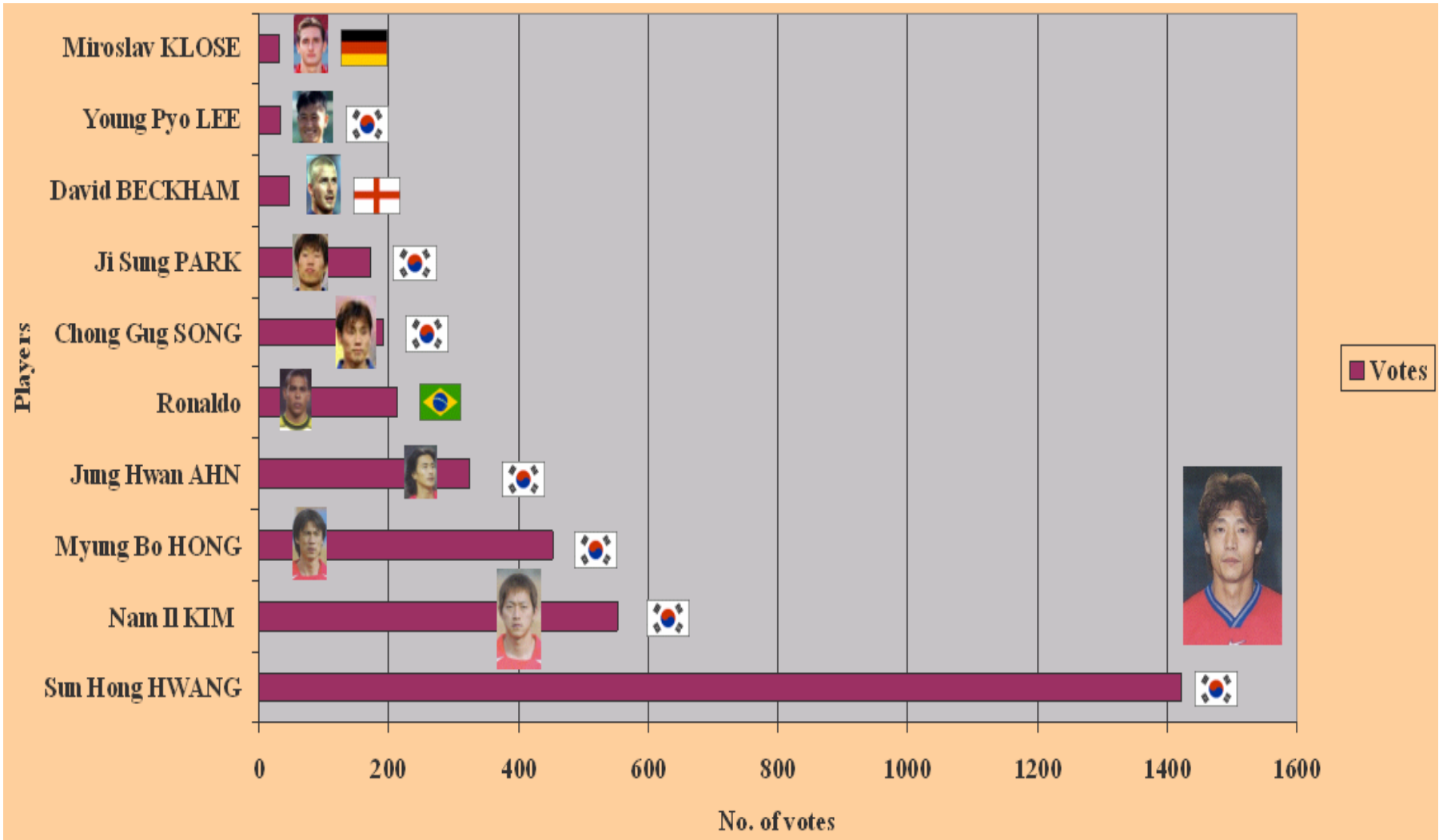
- [CONF] ✓
  - authentification des votants
  - signatures aveugles non falsifiables
- [ANO] ✓
  - Anonymat parfait (si canal parfaitement anonyme)
- [CONT] ✗ [PRV] ✗
- [VER1] ✓ [VER2] ✗
  - vérifiabilité individuelle seulement.
- [PAR] ✗

Sensus - Votopia

- Sensus
  - Université de Washington
  - le vote est de surcroît chiffré avec un algorithme à clé secrète
    - avantage : la propriété [PAR] est satisfaite
    - inconvénient : vote en **trois** étapes au lieu de deux

- Votopia
  - Projet coréen – japonais
  - Expérimenté lors du Mundial 2002
  - Quelques failles de sécurité
    - Canard-Gaud-Traoré 2006
    - nécessité de signatures aveugles "équitables"

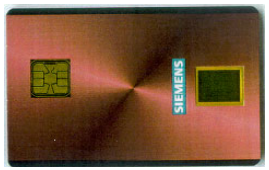
Votopia : résultats



3662 votants : 3474 de la Corée and 90 du Japon

E-Poll

- Projet européen de vote électronique : (2001 – 2005)
  - Ministère de l'intérieur français, France Télécom, Siemens, Ministère de l'intérieur italien et Vodafone
- Vote hybride
  - assisté par ordinateur
  - dans un bureau de vote (pour le vote institutionnel)
  - nomadisme autorisé
- Authentification biométrique

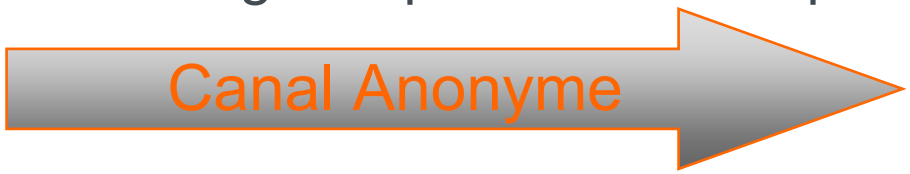


- Expérimentations françaises (entre 3000 et 20000 votants):
  - Votes doublons : Avellino, Mérignac (Présidentielles 2002), Campobasso, Vandoeuvre (Législatives 2002), Issy les Moulineaux (Référendum 2005)
  - Votes exclusifs : Cremona, Ladispoli, Czestochova, Ladispoli (sept. 2004), Université de Lyon II et Nantes (déc. 2004 et 2006)

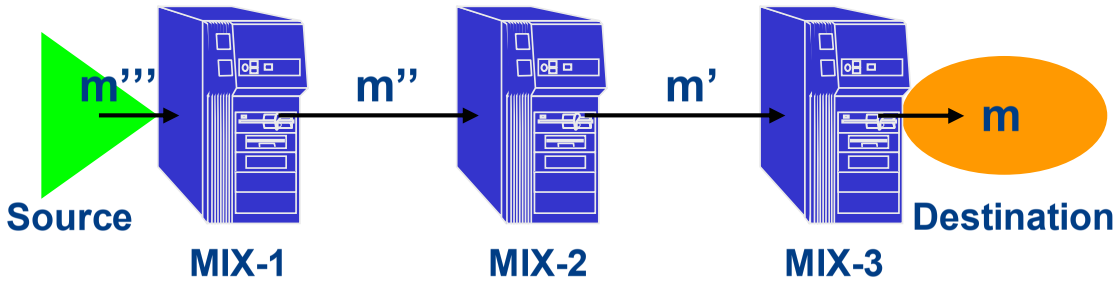
3 Réseaux de mélangeurs

Principe

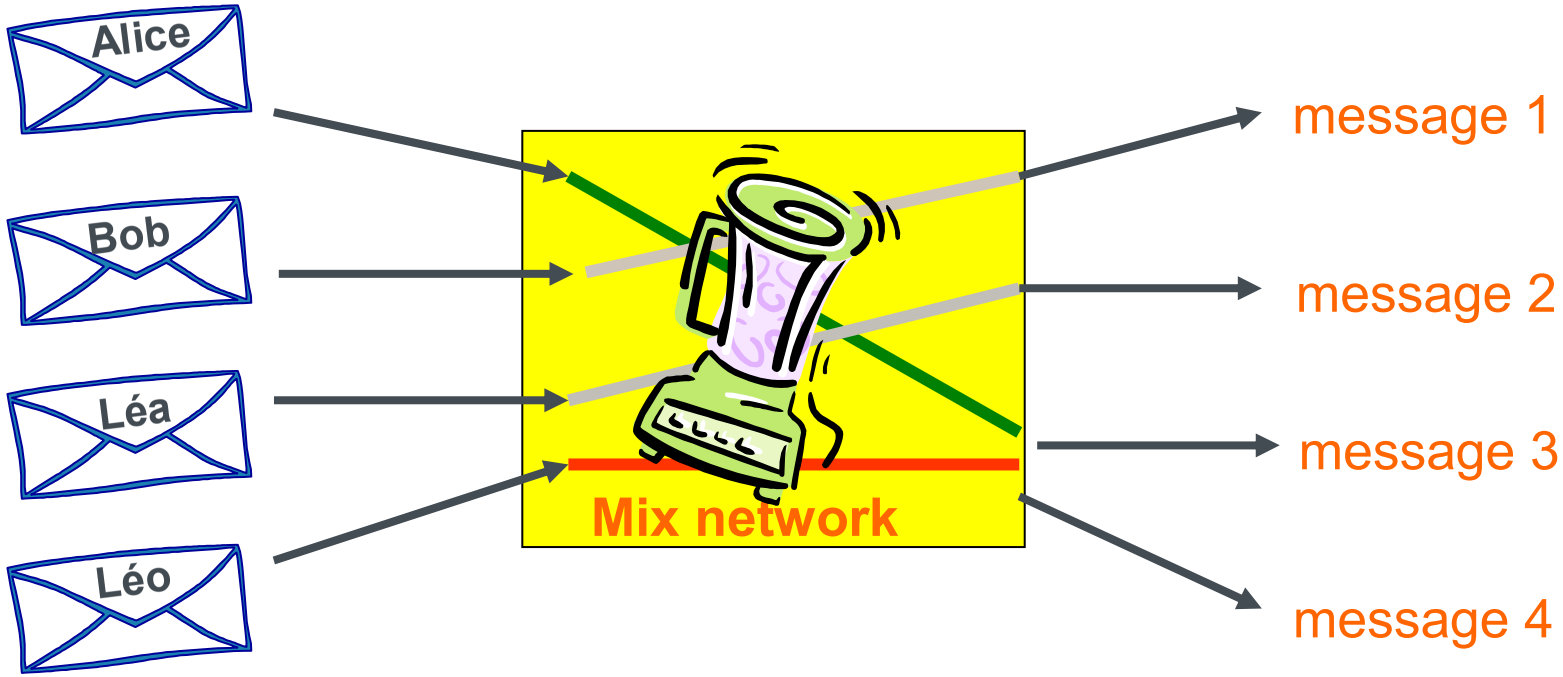
- Les réseaux de mélangeurs permettent d'implémenter un



- Chaque mélangeur (MIX)
  - permute l'ordre dans lequel il reçoit les messages
  - transforme le message reçu de sorte qu'entrée et sortie soient indissociables



Ce qui donne…

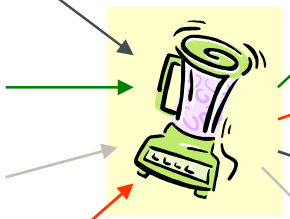

Alice
Bob
Léa
Léo
Mix network
message 1
message 2
message 3
message 4

Exemple avec El-Gamal

Assesseur

Dépouilleur(s)

$$(g^a \bmod p,\ v_1 h^a \bmod p)$$
$$(g^b \bmod p,\ v_2 h^b \bmod p)$$
$$(g^c \bmod p,\ v_3 h^c \bmod p)$$
$$(g^d \bmod p,\ v_4 h^d \bmod p)$$



$$(g^b \boldsymbol{g^{r_2}} \bmod p,\ v_2 h^b \boldsymbol{h^{r_2}} \bmod p)$$
$$(g^d \boldsymbol{g^{r_4}} \bmod p,\ v_4 h^d \boldsymbol{h^{r_4}} \bmod p)$$
$$(g^a \boldsymbol{g^{r_1}} \bmod p,\ v_1 h^a \boldsymbol{h^{r_1}} \bmod p)$$
$$(g^c \boldsymbol{g^{r_3}} \bmod p,\ v_3 h^c \boldsymbol{h^{r_3}} \bmod p)$$

Dépôt dans l'urne

Ouverture de l'urne

- Le MIX-net "rechiffre" et permute les bulletins
- Le(s) dépouilleur(s) les déchiffre(nt)

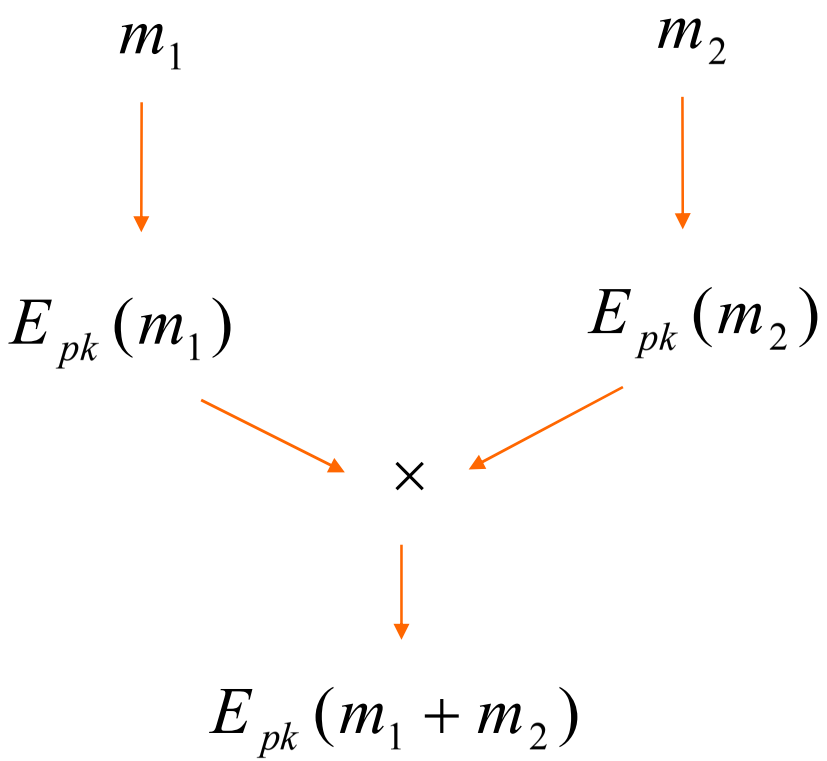
Propriétés de Sécurité

- [CONF] ✓
  - authentification des votants
- [ANO] ✓
  - si au moins un des mélangeurs est honnête
  - anonymat non parfait
- [CONT] ✗ [PRV] ✗
- [VER1] ✓ [VER2] ✓
- [PAR] ✓
  - si au moins un des dépouilleurs est honnête

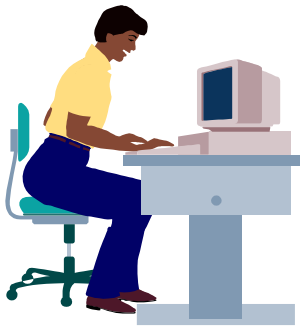
4 Chiffrement homomorphique

Définition

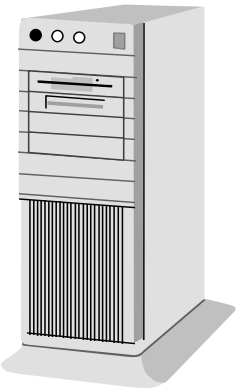
- Algorithme de chiffrement homomorphique



Phase de vote : le cas du référendum
(v = 0 ou 1)



$$E_{PK}(v) = (g^a \bmod p, f^v h^a \bmod p)$$



Votant

Urne

L'envoi doit être complété d'une preuve que $v \in \{0;1\}$

→ technique mal adaptée si beaucoup de candidats

Dépouillement

Dépouilleur

$E_{PK}(v_1)$

$E_{PK}(v_2)$

$E_{PK}(v_3)$

.

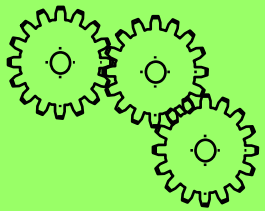
.

.

$E_{PK}(v_n)$

Urne (après mélange)

$E_{PK}(v_1 + v_2 + v_3 + \ldots + v_n)$



Déchiffrement

$\Sigma\, v = v_1 + v_2 + v_3 + \ldots + v_n$

Dépouillement avec El-Gamal

$$E_{PK}(v_1) = (g^{a_1} \bmod p, f^{v_1} h^{a_1} \bmod p)$$

$$E_{PK}(v_2) = (g^{a_2} \bmod p, f^{v_2} h^{a_2} \bmod p)$$

$$E_{PK}(v_3) = (g^{a_3} \bmod p, f^{v_3} h^{a_3} \bmod p)$$

.

.

.

$$E_{PK}(v_n) = (g^{a_n} \bmod p, f^{v_n} h^{a_n} \bmod p)$$

$$\Rightarrow E_{PK}(\sum v) = (g^{\sum a} \bmod p, f^{\sum v} h^{\sum a} \bmod p)$$

Propriétés de Sécurité

- [CONF] ✓
  - authentification des votants
- [ANO] ✓
  - si au moins un des dépouilleurs est honnête
  - anonymat non parfait
- [CONT] ✗ [PRV] ✗
- [VER1] ✓ [VER2] ✓
- [PAR] ✓
  - si au moins un des dépouilleurs est honnête

EADS - VoteHere

- EADS Matra Systèmes & Information
  - solution issue du projet européen Cybervote (BT, Nokia, etc.)
  - expérimentations : CCI, scrutin octobre – novembre 2004
  - organisation de l'élection des représentants de l'Assemblée des Français de l'Etranger, juin 2006, 525 000 électeurs potentiels

- VoteHere
  - start-up américaine
  - solution identique à celle issue du projet européen Cybervote

5 Progrès récents

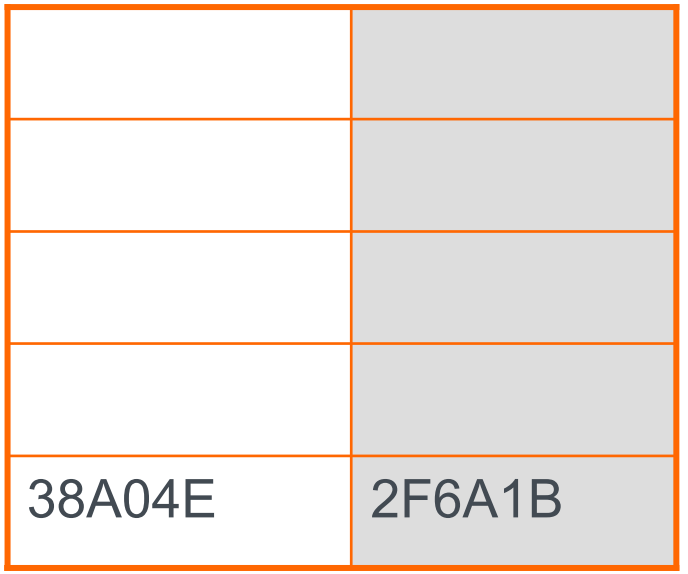
Trois challenges

- Challenge A
  - Comment vérifier la machine sans la certifier ?
- Challenge B
  - Comment associer anonymat (parfait) et vérifiabilité (universelle) ?
- Challenge C
  - Comment associer vote en ligne et vote sans contrainte ?

Challenge A – Pret A Voter (1)

- Comment vérifier la machine sans la certifier ?
  - Chaum(-Ryan-Schneider), 2003 et ensuite

- Notations :
  - ***N*** : nombre de candidats
  - ***s*** : permutation circulaire de [1.. ***N***])



- Bulletin de vote :
  - 38A04E est le chiffrement de ***s*** destiné à la machine à voter
  - 2F6A1B est le chiffrement de ***s*** destiné à l'autorité de vote

Challenge A – Pret A Voter (2)

- La machine à voter lit optiquement le volet de gauche
- La machine à voter
  - retrouve ***s*** en déchiffrant 38A04E
  - imprime la liste permutée des candidats
- Le votant marque un X en face du candidat de son choix
- Le votant
  - détache le volet de gauche et quitte l'isoloir
  - place le volet de droite devant un lecteur optique en présence des assesseurs
- Les votes sont mélangés (mix-net)

Democritus	
Plato	X
Socrates	
Thales	
38A04E	2F6A1B

Challenge A – Pret A Voter (3)

- Comment vérifier (le bon fonctionnement de) la machine ?
- Réclamer deux bulletins (imprimés recto verso) puis :
  - remplir l'un (par ex.verso)
  - donner le recto à l'autorité de vote pour vérification
- Si la machine triche *k* fois, elle sera détectée avec probabilité $1-2^{-k}$

Democritus	
Plato	
Socrates	
Thales	
38A04E	2F6A1B

(recto)

Challenge B

- Comment associer anonymat (parfait ?) et vérifiabilité (universelle ?)
- Facile à résoudre si l'anonymat ne doit pas être parfait (par ex. avec du chiffrement homomorphique)
- *Impossible* à résoudre sinon (en environnement "normal")
  - Chevallier-Mames-Fouque-Pointcheval-Stern-Traoré, 2006

Challenge C

- Comment associer vote en ligne et vote sans contrainte ?
  (Juels-Catalano-Jakobsson, 2005)

- Ingrédients de base
  - un vote peut être valide ou non
  - un attaquant est incapable de savoir si un vote est valide ou non
  - un votant peut voter plusieurs fois (mais un seul vote sera pris en compte)

- Idée de base
  - pour berner un attaquant, le votant envoie des votes invalides tant qu'il se trouve en situation de contrainte
  - dès qu'il dispose d'un instant de liberté, il émet un vote valide

6 Conclusion

Conclusion

- Le vote électronique est déjà une réalité dans certains pays
  - Brésil, Estonie, Etats-Unis, etc.
  - en France, évolution d'abord timide puis brutale (élections politiques 2007)
- Systèmes actuels peu satisfaisants
- En dépit du résultat d'impossibilité, on peut espérer l'émergence d'un système à la fois pratique, sûr et de confiance dans un avenir proche, même pour le vote en ligne