HERVÉ SCHAUER CONSULTANTS
Cabinet de Consultants en Sécurité Informatique depuis 1989
Spécialisé sur Unix, Windows, TCP/IP et Internet

SSTIC
10 juin 2010

La sécurité des systèmes de vote

Frédéric Connes
<Frederic.Connes@hsc.fr>

Introduction

- « La sécurité des systèmes de vote »
  - Thèse en droit
  - Université Panthéon-Assas (Paris-II)
  - En 2009
  - Se trouve sur http://www.fconnes.org/
  - Bientôt disponible en ouvrage papier
- Aspects juridiques et techniques

Plan

- **La sécurité problématique des systèmes de vote automatisés**
- Proposition de protocole de vote électronique

Problèmes de l'automatisation

- Indisponibilité
  - Alimentation électrique, défaillances matérielles
  - Déni de service
- Atteintes à l'intégrité
  - Dysfonctionnement de l'autorisation
  - Problème d'interface (Floride 2000)
  - Altérations volontaires ou involontaires des résultats
- Absence d'auditabilité
  - Boîtes noires
- Disparition du secret
  - Signaux parasites compromettants, stockage de l'ordre de passage des votants, vote par Internet...

Recherche de solutions

- Recherche de protocoles de vote permettant
  - De garantir l'intégrité tout en préservant le secret
  - Sans remettre en cause la disponibilité et l'auditabilité
- Problème
  - Le secret empêche de détecter et de corriger les atteintes à l'intégrité
  - Atteintes non détectées si le nombre de suffrages est correct
  - Contrairement aux autres systèmes critiques
- Solution : référence indépendante préservant le secret

Trace papier

- Permet de comparer les résultats électroniques et papier
- Plusieurs formes
  - Électeur place lui-même le bulletin papier dans une urne
  - Inscription du vote sur un rouleau derrière une vitre (R. Mercuri)
  - Impression d'un bulletin à lecture optique (A. Rubin)
- Dans tous les cas
  - Comptabilisation principale sous forme électronique
  - Nécessite un décompte manuel à chaque fois pour valider
  - Rendrait l'automatisation superflue
- Dépouillements papier aléatoires
  - Doivent confirmer les résultats sinon problème de confiance

Reçu papier

- Certains experts recherchent des solutions fondées sur un reçu papier
- Référence non plus globale mais individuelle
- Avantages par rapport au vote traditionnel
  - Permet à chaque citoyen de faire valoir son vote en justice
  - Publication des votes sur un site web
  - Toute personne intéressée peut recompter
- Problème majeur : préserver le secret
- Exemples : ThreeBallot, VAV, Twin, Scantegrity...
- Souvent difficiles à comprendre et présentent certains défauts

Plan

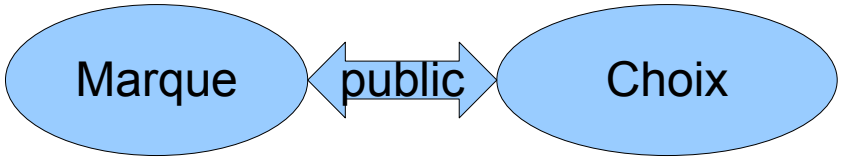
- La sécurité problématique des systèmes de vote automatisés
- **Proposition de protocole de vote électronique**

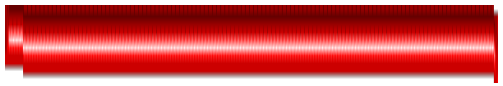
Proposition de protocole de vote

- Protocole présenté dans un article du 18 août 2008
  - Accessible sur ArXiv et http://www.fconnes.org/
  - Commenté sur la liste « Scantegrity »
- Version présentée ici :
  - Tient compte des remarques formulées et des simplifications imaginées depuis la thèse

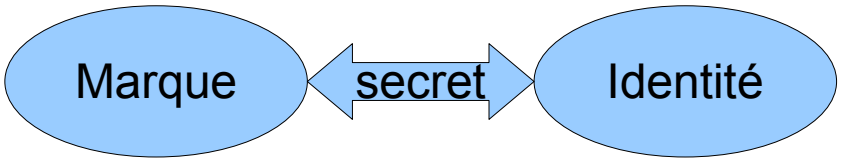
Principe

- Assigner une marque aléatoire à chaque votant
- Rendre **public** le lien
  - Publié sur le site web





- Garantir le **secret** du lien

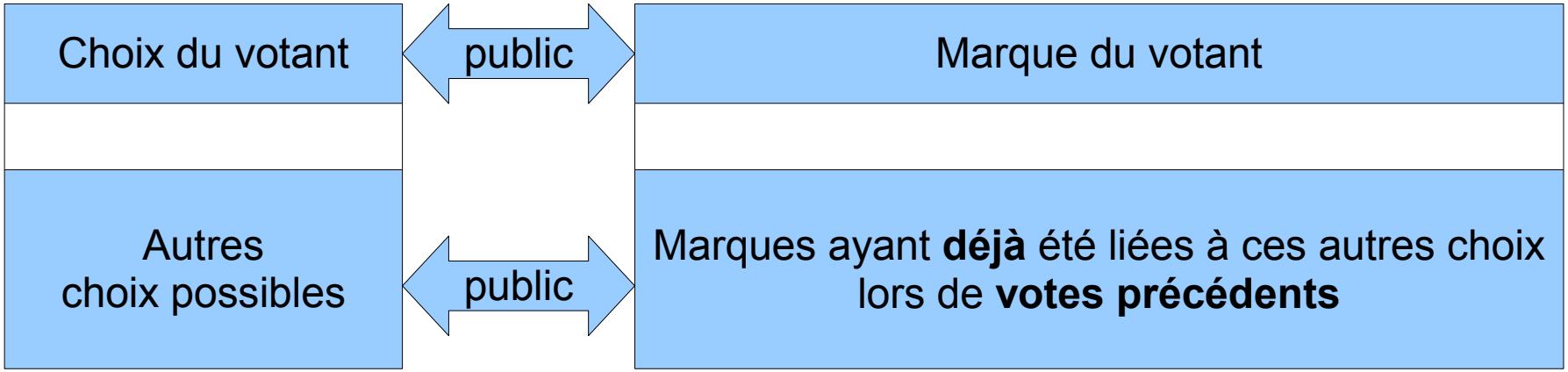


  - Ne doit pas survivre en dehors de l'isoloir
  - L'électeur doit être incapable de prouver à un tiers la marque allouée
  - L'électeur doit pouvoir déterminer sa marque à tout moment

Solution proposée

- Remettre un reçu au votant à l'issue de son vote

- Ce reçu associe :



- Sur le reçu, le choix du votant ne se distingue pas des autres

  => Secret

Exemple

- Élection opposant :
  - Alice
  - Bob
  - Carla
  - David
  - Sans oublier le vote blanc

- Notre électeur veut voter pour Bob

Exemple

- Reçu remis à notre électeur :

Alice	23482
Bob	17589
Carla	65459
David	42349
Vote blanc	34585

- Seul élément différenciant : 17589 est une marque nouvelle
  - Toutes les autres marques ont déjà été attribuées
- Mais un tiers n'a pas connaissance de cet élément (juge)
- Notre électeur peut toujours se souvenir de sa marque
  - Elle est inscrite en face de son vote

Exemple

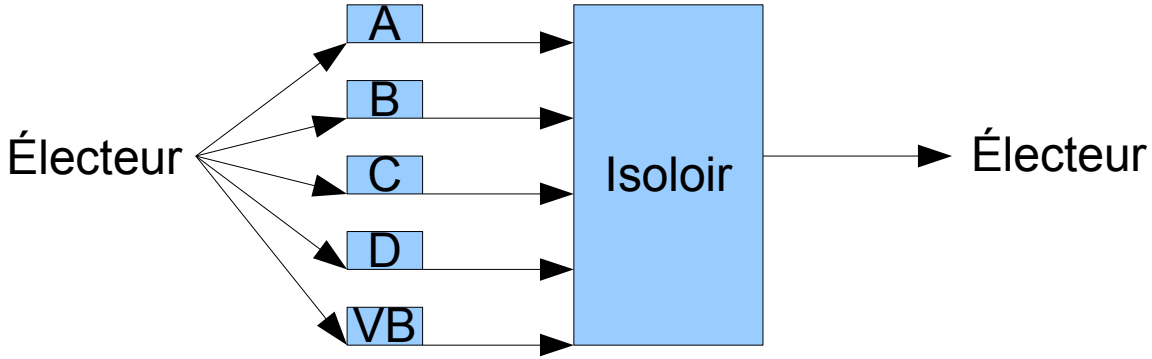
- Publication sur le web :

8234	Vote blanc
...	...
17589	Bob
...	...
23482	Alice
...	…
34585	Vote blanc
...	...
42349	David
...	...

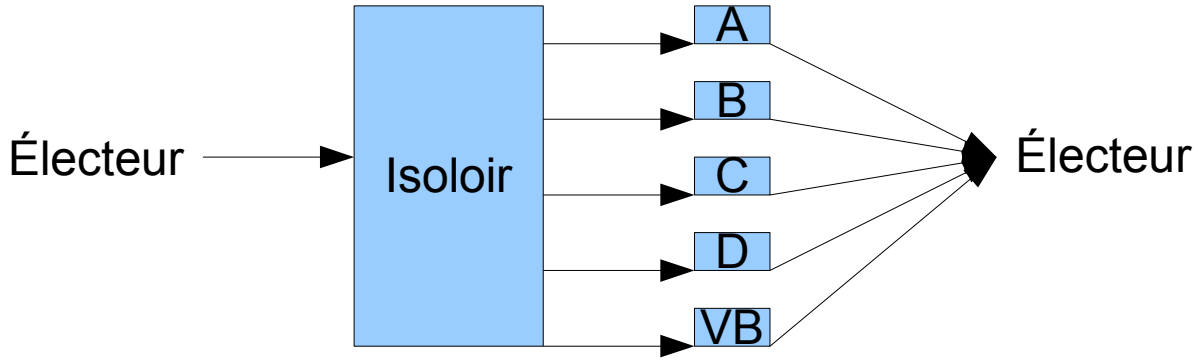
45698	Carla
...	...
65459	Carla
...	...
67895	David
...	...
83593	Alice
...	...
93452	Bob
...	...

Comparaison avec le vote traditionnel

- Dans le vote traditionnel :



- Dans le protocole proposé :

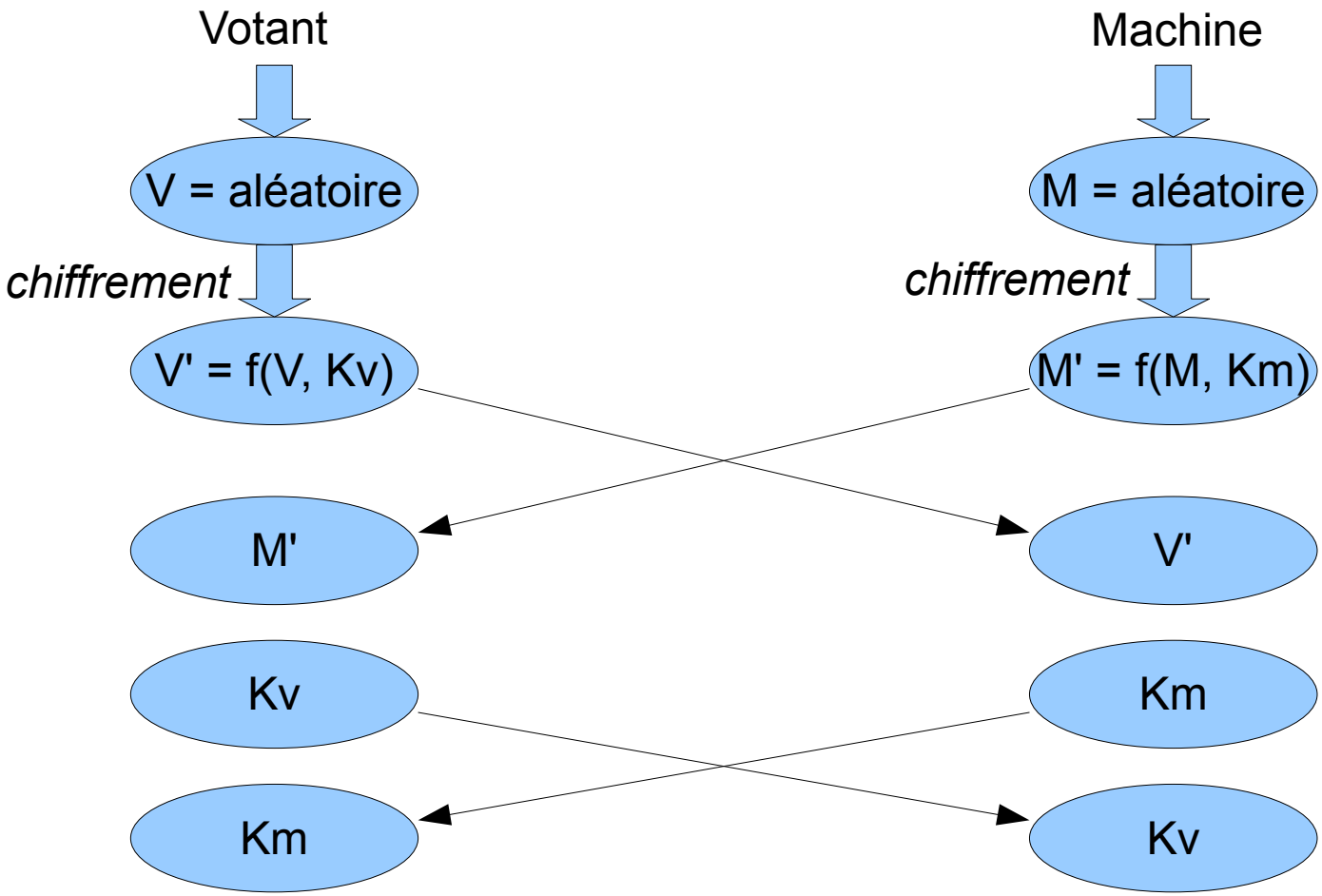


Génération de la marque du votant

- Problème :
  - La marque peut dissimuler une information permettant de la reconnaître
  - Exemple : résultat d'un calcul sur les chiffres qui la composent
- Solution proposée :
  - Ni la machine ni le votant ne doivent choisir la marque
  - Protocole de choix d'un nombre aléatoire sans tiers de confiance

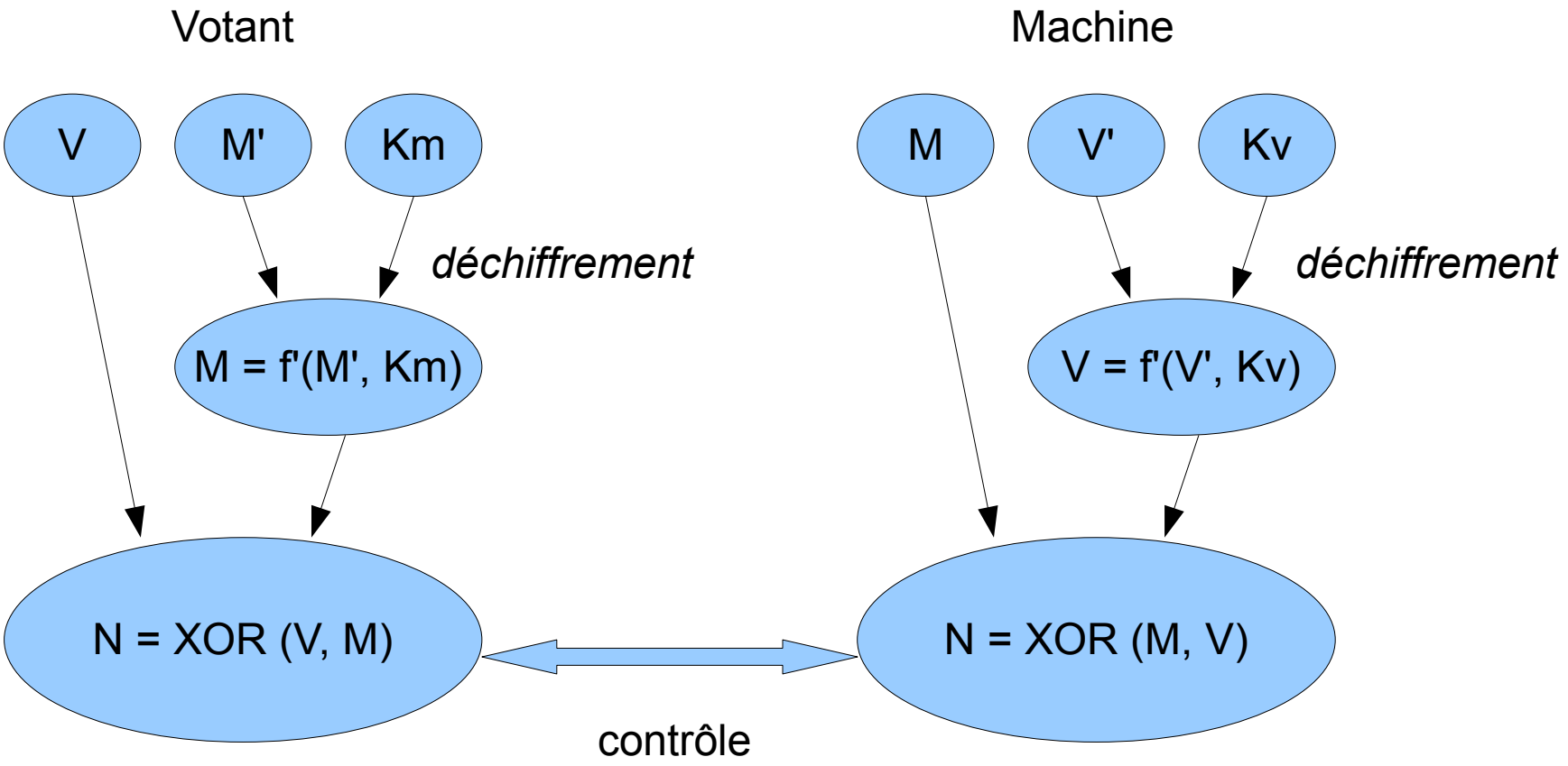
Génération de la marque du votant

- Protocole de génération proposé :



Génération de la marque du votant

- Protocole de génération proposé (suite) :



Génération des autres marques

- Problème :
  - La marque du votant peut être distinguée des autres marques
  - Exemple : chiffre des milliers le plus petit

- Solution proposée :
  - Déterminer les marques antérieures avant de déterminer la marque du votant
  - Mais déterminer les marques antérieures après le choix du votant
    - Sinon : 2 marques pour le choix du votant (antérieure + générée)
    - Ce serait un signe distinctif

Premier votant

- Problème :
  - Utilisation de votes antérieurs
  - Que se passe-t-il pour le premier votant ?
- Solution proposée :
  - Faire générer par la machine des votes antérieurs fictifs
  - Après le choix du premier votant
    - Sinon il resterait une marque « dans la nature » (choix du votant)
- Propriétés :
  - Vote d'une seule personne : son choix demeure secret
  - Jamais d'unanimité : protection du secret même si votes unanimes
  - Majorité = écart de 2 voix : caractère collectif de la décision

Comparaison de reçus

- Problème :
  - Une personne entre en possession de 2 reçus et connaît leur ordre
  - La même marque apparaît sur les 2 reçus :
    - Le second votant n'a pas voté pour le choix lié à la marque
- Solution proposée :
  - Rendre possible le fait qu'un nouveau vote soit associé à une marque antérieure (crée une incertitude)
  - Génération de 2 types de reçus :
    - « de contrôle » : choix associé à une nouvelle marque
    - « absolument secret » : choix associé à une marque antérieure
      - Ne permet pas un contrôle d'intégrité mais préserve le secret
      - Vote comptabilisé dans un registre séparé (comme actuellement)
      - Générer au moins un reçu de ce type (imposé par la machine)

Problèmes restant à résoudre

- Garantir au votant que les autres marques correspondent bien à des votes antérieurs
  - Ne doivent pas être « inventées » par la machine
  - Sinon : votes supplémentaires à déduire des résultats
- Risque que personne ne veuille voter en premier
  - Cacher le fait qu'on est le premier à voter
  - Plus facile avec le vote par Internet
- Possession de tous les reçus ordonnées depuis l'ouverture du scrutin
  - Marque nouvelle = nouveau vote
  - Ne fonctionne que si tous les premiers votants coopèrent
  - Un votant peut toujours demander un reçu « absolument secret »

Conclusion

- Vote électronique :
  - Se développe de plus en plus (certains avantages)
  - Mais gros problèmes de sécurité
  - Les citoyens pourraient massivement rejeter l'automatisation

- Protocole proposé :
  - Permet de vérifier l'intégrité des résultats (reçus, site web)
    - Avantage par rapport au vote traditionnel
  - Tout en préservant le secret et en restant compréhensible dans son principe