

Ensimag 1^{ère} année

TD n°3 — Vote électronique

Le but de ce TD est de s'intéresser aux propriétés qu'on peut attendre d'un protocole de vote électronique et comment ceux-ci peuvent être implémentés. On étudiera en particulier le protocole Bélénios utilisé par exemple à l'Ensimag pour les dernières élections au conseil d'école. Nous allons déjà essayer d'en construire un, définir les propriétés attendues et étudier leur encodage dans Bélénios.

1 Pour s'échauffer

On considère un ensemble de votants V , une autorité A assurant le vote et un ensemble de candidats C désignés par un numéro.

Question 1 *Quelles sont les menaces contre lesquelles on veut se protéger ?*

Question 2 *Lister quelques propriétés attendues d'une procédure de vote électronique en terme de secret (confidentialité), intégrité et légitimité.*

Donner d'autres propriétés attendues.

2 Une première solution

Question 3 *Au vu des premiers TDs/TPs proposez des solutions cryptographiques pour les besoins suivants :*

1. *la sécurité des communications*
2. *l'identité du votant (à préciser ce qu'on entend par là)*
3. *la représentation de l'urne qui doit stocker les votes*

On considère le protocole suivant :

1. L'autorité de vote A génère une clé publique pour l'élection.
2. chaque votant chiffre son vote en utilisant cette clé et l'envoie à A par l'intermédiaire d'un canal sécurisé.

3. La phase de vote terminée A déchiffre tous les votes et annonce le résultat.

Question 4 1. Expliquer pourquoi au pas 2 un canal sécurisé doit être utilisé (alors qu'il y a déjà le chiffrement par la clé publique de A).

2. Quelles sont les propriétés garanties par ce protocole ? Quelles sont ses faiblesses ?
3. Qui peut soumettre un vote ? Proposer une amélioration.
4. Quelles hypothèses devons-nous faire pour que les votes restent secrets ?
5. Comment peut-on avoir confiance dans le résultat de l'élection ?

Question 5 En sécurité lors d'opérations particulièrement sensibles (comme ici le calcul du résultat) on cherche à appliquer deux principes importants : le moindre privilège et la séparation des responsabilités. Quelles solutions pourrait-on mettre en place ?

3 Etude de Bélénios

Le protocole Bélénios¹ s'appuie sur le schéma de chiffrement clé publique/clé privée El Gamal.

Rappel :

Soit G un groupe d'ordre q (ses éléments sont les entiers de l'intervalle $[0, q - 1]$) dont g est un générateur. On supposera ces paramètres bien choisis. Une clé privée x est un entier entre 0 et $q - 1$ (bornes incluses) et la clé publique associée est $y = g^x$. Le chiffrement et le déchiffrement se font par les deux opérations ci-dessous :

$E(m)$: choisir un entier aléatoire $r \in [0, q - 1]$, appelé *aléa*. Le chiffré de m est la paire $(g^r, m * y^r)$.

$D(c_1, c_2)$: calculer $m' = c_2 * c_1^{-x}$

Question 6 Montrer que l'algorithme de déchiffrement fonctionne correctement.

Le protocole de vote Bélénios comporte 3 phases : la distribution du matériel (clé privée/publique et mot de passe pour chaque votant), la phase de vote et la phase de dépouillement. On s'intéresse ici à la phase de vote, décrite sur la figure 1.

sk et vk désignent respectivement la clé secrète et la clé publique d'un votant (d'identifiant id , ayant pour mot de passe pwd) et ps la clé publique du serveur.

v est la valeur du vote, il est représenté par un entier dans $[0, q - 1]$, r est l'aléa. enc est le schéma de chiffrement de la question précédente dans lequel on explicite r et ps . Le bulletin de vote b contient notamment c avec sa signature s .

Question 7

1. Expliquer ce qu'envoie le votant
2. Peut-on voter plusieurs fois ? Justifier les vérifications faites par le serveur.
3. à quoi sert le journal (\parallel désigne la concaténation) ?
4. Peut-on faire du rejeu ? Si oui, quel est son effet ?
5. Pourquoi garder s et vk dans l'urne ? Que peut vérifier un votant ?

1. <http://www.belenios.org/>

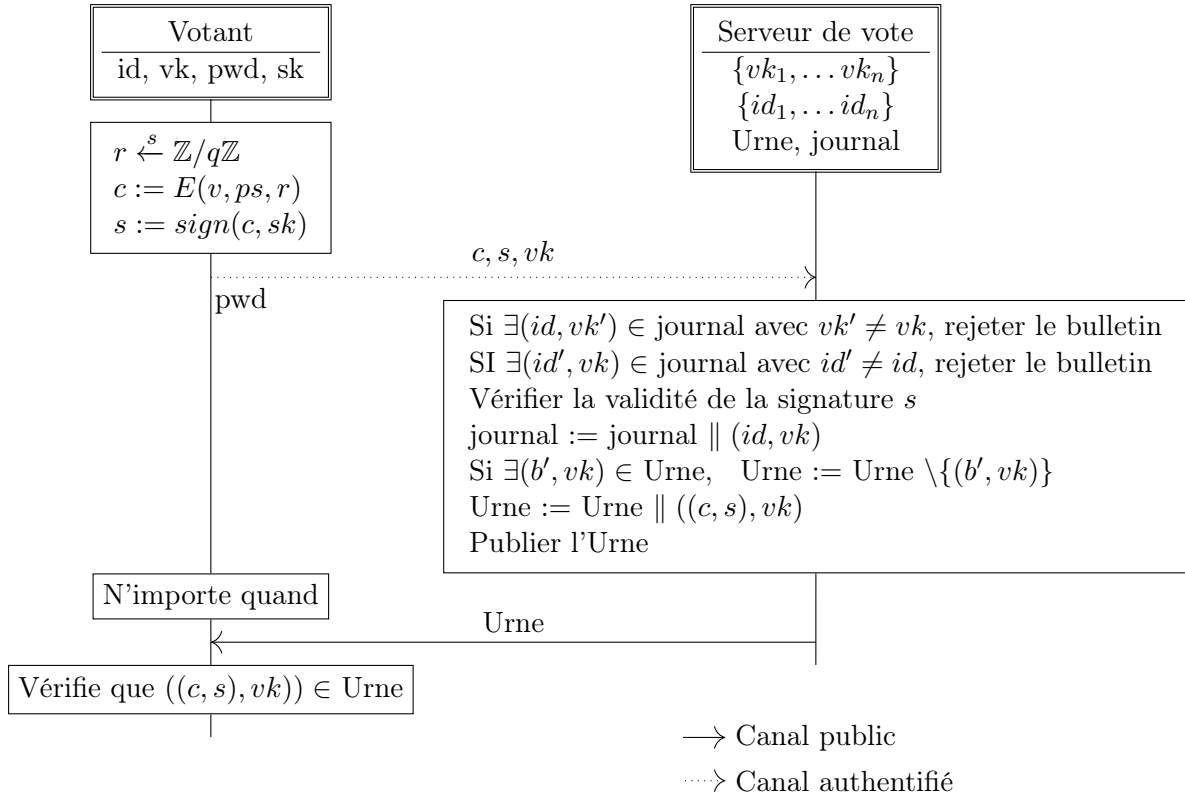


FIGURE 1 – Phase de vote dans Béliénios

On s'intéresse maintenant à la phase de dépouillement et de calcul du score. On suppose qu'on est dans le cas où il n'y a que 2 candidats, de numéros 0 et 1.

Question 8 On suppose que les votes sont encodés sous la forme g^v où v est le numéro d'un candidat. Montrer la propriété suivante (appelée chiffrement homomorphique) du chiffrement El Gamal (preuve facultative) :

$$\text{enc}(g^{v_1}, y, r_1) * \text{enc}(g^{v_2}, y, r_2) = \text{enc}(g^{v_1+v_2}, y, r_1 + r_2)$$

- On considère un vote à 2 candidats de numéros respectifs 0 et 1. Expliquer comment cette propriété peut être utilisée lors du dépouillement et son intérêt
- Est-on sûr du résultat ?

Question 9 Discuter les points suivants :

- Béliénios pourrait-il être utilisé pour remplacer des élections nationales ? Lister les propriétés garanties et celles qui font défaut.
- Pensez-vous que les électeurs doivent maîtriser la cryptographie pour adopter un système de vote électronique ?