Fonctionnement de Belenios

Véronique Cortier, Pierrick Gaudry et Stéphane Glondu

Caramba et Pesto – LORIA UMR 7503
CNRS, Université de Lorraine, Inria

https://www.belenios.org/

rédigé le 17 mars 2021

Propriétés attendues d'un système de vote

Avant d'envisager les **attaques**, il est important d'expliciter les **propriétés** à préserver.

Propriété	À l'urne	Postal	Internet
Secret du vote	✓	?	?
Légitimité des électeurs	✓	?	?
Garantie de résultat correct	✓	?	?
Accessibilité, facilité d'utilisation	✓	?	?
Pas de coercition ni achat de vote	✓	?	?

Le **vote à l'urne traditionnel** est une remarquable solution offrant un excellent compromis (quand il est bien mis en œuvre).

Malheureusement, il est parfois impossible à déployer et l'on doit se rabattre sur du **vote à distance**.

Secret du vote

Propriété très souvent **souhaitée** (mais pas toujours).

Difficile à mettre en œuvre (même avec le vote à l'urne !)

Vote à distance :

- L'expression du vote arrive en même temps que l'identité de l'électeur (pour vérifier la présence sur la liste électorale).
- Solutions pour le vote par correspondance : utiliser des alias (numéro d'électeur aléatoire), 2 ou 3 envoloppes imbriquées, ...
- Solution pour le vote par Internet : **chiffrement**, avec clé répartie en plusieurs autorités.

Le secret s'appuie alors sur la **confiance** en une ou plusieurs entités qu'il faut pouvoir clairement identifier.

Légitimité des électeurs

Liste électorale : c'est ce qui différencie une élection d'un sondage.

L'**usurpation d'identité** est un **risque majeur** du vote à distance.

Le point faible est principalement l'**envoi du matériel de vote** :

- Adresse postale fiable ?
- Adresse e-mail fiable ?
- Numéro de portable (SMS) fiable ?

Disposer d'un **canal de communication** vers chaque électeur où les messages arrivent toujours (pas forcément de manière privée) peut suffire pour réduire le risque. (e.g. envoi de mail de confirmation "a voté").

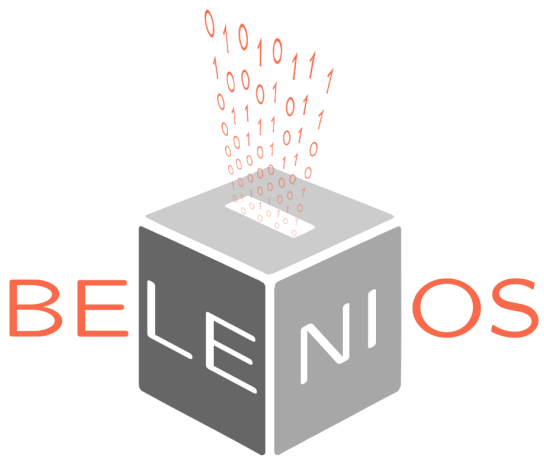
Selon les circonstances, le vote électronique peut être mieux que le vote par correspondance sur ce point.

Garantie de résultat correct

Quelques points qui peuvent **fausser le résultat** :

- Lors du **vote**, je crois voter A, mais je vote B.
  - Par correspondance : parfois on sélectionne un numéro plutôt que le candidat pour protéger le secret.
  - Par Internet : le navigateur peut me montrer “A”, mais chiffrer “B”.
- Bulletins manipulés lors du **transport**.
  (transport physique, ou transport virtuel)
- Manipulations lors du **dépouillement**.
  Vote par correspondance : on doit avoir confiance.
  Vote électronique : il existe des protocoles où cette partie-là ne demande pas de tiers de confiance.

Protocole de vote Belenios



- Développé au Loria, équipes Caramba et Pesto
  Développeur principal : Stéphane Glondu
- Utilisé dans plus de 1400 élections en 2020 (au sein d'universités, d'associations, etc.)

`https://www.belenios.org/`

Particularité : l'urne est publique, accessible depuis une page web. Tout le monde peut consulter les bulletins chiffrés.

Un peu de cryptographie pour commencer

Les votes ne sont pas envoyés en clair mais sont chiffrés.

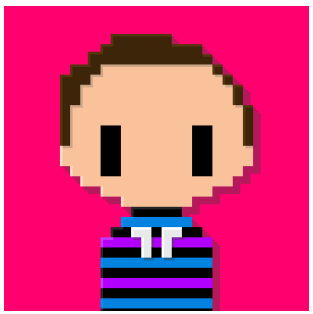
Chiffrement à clé publique, à seuil

- Tout le monde peut chiffrer avec la **clé publique** de l'élection
- Il faut plusieurs clés pour déchiffrer, comme pour ouvrir le coffre-fort d'un magasin.
- Les clés de déchiffrement sont **réparties** entre plusieurs autorités.
- On peut définir un seuil. Par exemple 3 parmi 5 autorités suffisent pour déchiffrer.

Belenios, phase de vote (simplifiée)

Notations : $\{v\}_{\text{pub}_E}$: vote v chiffré par la clé publique pub_E.

pub_E : clé publique de l'élection, les clés de déchiffrement sont réparties entre les autorités.



Urne (page web publique)

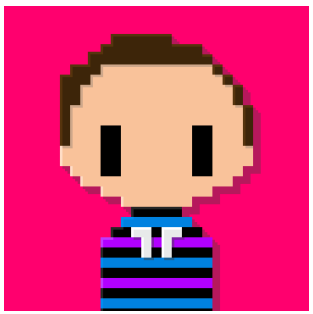
$\{v_A\}_{\text{pub}(E)}$
$\{v_B\}_{\text{pub}(E)}$
$\{v_C\}_{\text{pub}(E)}$

- Lorsque David arrive, certains électeurs ont déjà voté. Leurs bulletins sont visibles dans l'urne.

Belenios, phase de vote (simplifiée)

Notations : $\{v\}_{\text{pub}_E}$: vote v chiffré par la clé publique pub_E.

pub_E : clé publique de l'élection, les clés de déchiffrement sont réparties entre les autorités.



Urne (page web publique)

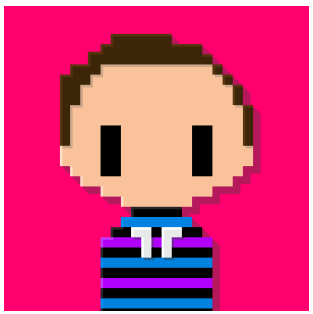
$\{v_A\}_{\text{pub}(E)}$
$\{v_B\}_{\text{pub}(E)}$
$\{v_C\}_{\text{pub}(E)}$

- Lorsque David arrive, certains électeurs ont déjà voté. Leurs bulletins sont visibles dans l'urne.
- David sélectionne son vote et son ordinateur **chiffre son vote**. L'ordinateur affiche également un **numéro de suivi**, l'empreinte (le haché) du bulletin.

Belenios, phase de vote (simplifiée)

Notations : $\{v\}_{\text{pub}_E}$: vote v chiffré par la clé publique pub_E.

pub_E : clé publique de l'élection, les clés de déchiffrement sont réparties entre les autorités.



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

Urne (page web publique)

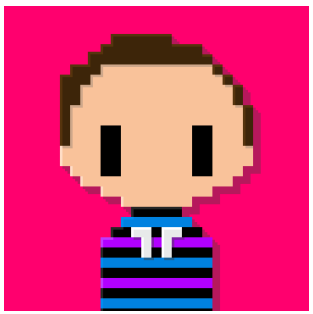
$\{v_A\}_{\text{pub}(E)}$
$\{v_B\}_{\text{pub}(E)}$
$\{v_C\}_{\text{pub}(E)}$

- Lorsque David arrive, certains électeurs ont déjà voté. Leurs bulletins sont visibles dans l'urne.
- David sélectionne son vote et son ordinateur **chiffre son vote**. L'ordinateur affiche également un **numéro de suivi**, l'empreinte (le haché) du bulletin.
- David envoie son vote chiffré en s'authentifiant.

Belenios, phase de vote (simplifiée)

Notations : $\{v\}_{\text{pub}_E}$: vote v chiffré par la clé publique pub_E.

pub_E : clé publique de l'élection, les clés de déchiffrement sont réparties entre les autorités.



Urne (page web publique)

$\{v_A\}_{\text{pub}(E)}$
$\{v_B\}_{\text{pub}(E)}$
$\{v_C\}_{\text{pub}(E)}$
$\{v_D\}_{\text{pub}(E)}$

- Lorsque David arrive, certains électeurs ont déjà voté. Leurs bulletins sont visibles dans l'urne.
- David sélectionne son vote et son ordinateur **chiffre son vote**. L'ordinateur affiche également un **numéro de suivi**, l'empreinte (le haché) du bulletin.
- David envoie son vote chiffré en s'authentifiant.
- David peut vérifier que son bulletin est dans l'urne en comparant les **numéros de suivi**.

Dépouillement

Le chiffrement a la propriété d'être **homomorphe**.
En « multipliant » les chiffrés, on obtient un bulletin chiffré qui contient la somme des votes, pour chaque candidat.

$$\{v_1\}_{\mathsf{pub}(E)} \times \cdots \times \{v_n\}_{\mathsf{pub}(E)} = \{v_1 + \cdots + v_n\}_{\mathsf{pub}(E)}$$

$\rightarrow$ Seul le résultat final doit être déchiffré !

Dépouillement

Le chiffrement a la propriété d'être **homomorphe**.
En « multipliant » les chiffrés, on obtient un bulletin chiffré qui contient la somme des votes, pour chaque candidat.

$$\{v_1\}_{\mathsf{pub}(E)} \times \cdots \times \{v_n\}_{\mathsf{pub}(E)} = \{v_1 + \cdots + v_n\}_{\mathsf{pub}(E)}$$

$\rightarrow$ Seul le résultat final doit être déchiffré !

Les autorités de déchiffrement déchiffrent collectivement le chiffré du résultat et **prouvent** qu'elles ont correctement déchiffré.

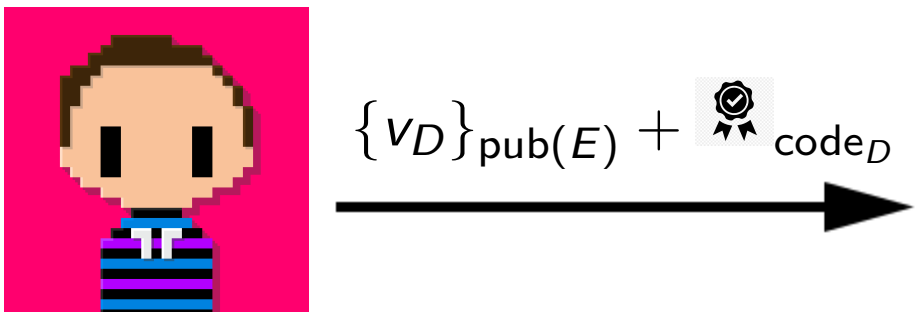
$$\{v_1 + \cdots + v_n\}_{\mathsf{pub}(E)} \rightsquigarrow v_1 + \cdots + v_n + \textbf{preuve}$$

Cette preuve est vérifiable par tous : il est impossible de fournir autre chose que le résultat de l'élection à l'intérieur du chiffré.
Cela repose sur des preuves à divulgation nulle de connaissance (zero-knowledge proofs).

Belenios, phase de vote (avec code de vote)

Pour éviter le bourrage d'urne par le serveur de l'élection lui-même, Belenios comprend deux formes d'authentification de l'électeur :

- Authentification classique par login et mot de passe, contrôlée par le serveur
- Signature des bulletins par un **code de vote**. Le serveur ne connait que les parties publiques des codes de vote.



David rentre son code de vote au moment du vote et envoie son vote chiffré et signé.

Les codes de vote sont envoyés par une autorité tierce.

Sécurité de Belenios

Propriété	À l'urne	Postal	Internet	Belenios
Secret du vote	✓	?	?	✓
Légitimité des électeurs	✓	?	?	✓
Garantie de résultat correct	✓	?	?	✓
Accessibilité	✓	?	?	?
Pas d'achat de vote	✓	?	?	×

Belenios **ne protège pas contre l'achat de vote** : un électeur peut vendre ses identifiants (mot de passe), son code de vote.

Un électeur peut également prouver pour qui il a voté en fournissant tous les aléas utilisés lors de la formation du bulletin.

La sécurité a un prix !

Secret du vote : **à condition que les clés de déchiffrement soient réparties** entre plusieurs autorités. Sinon, le serveur a la capacité technique de savoir qui a voté quoi.
Vous pouvez consulter la liste des autorités sur la page principale de l'élection (zone grisée).

La sécurité a un prix !

Secret du vote : **à condition que les clés de déchiffrement soient réparties** entre plusieurs autorités. Sinon, le serveur a la capacité technique de savoir qui a voté quoi.
Vous pouvez consulter la liste des autorités sur la page principale de l'élection (zone grisée).

Légitimité des électeurs : **à condition que les codes de vote soient envoyés par une autorité externe**. Sinon, le serveur a la capacité technique d'ajouter des bulletins.
Vous pouvez savoir qui envoie les codes de vote sur la page principale de l'élection (zone grisée).

La sécurité a un prix !

Secret du vote : **à condition que les clés de déchiffrement soient réparties** entre plusieurs autorités. Sinon, le serveur a la capacité technique de savoir qui a voté quoi.
Vous pouvez consulter la liste des autorités sur la page principale de l'élection (zone grisée).

Légitimité des électeurs : **à condition que les codes de vote soient envoyés par une autorité externe**. Sinon, le serveur a la capacité technique d'ajouter des bulletins.
Vous pouvez savoir qui envoie les codes de vote sur la page principale de l'élection (zone grisée).

Garantie de résultat correct

- Si les électeurs vérifient que leur bulletin est bien dans l'urne. **Faites-le !**
- Si l'urne est effectivement surveillée (vérification des preuves de bon déchiffrement).

Soyez critiques !

Un processus d'élection est **complexe**.
Les considérations de sécurité sont **multiples**.

Mais **soyez critiques** partout :

- Lors du vote **à l'urne**. Surveillance effective ?
- Lors du vote par **correspondance**. À qui je fais confiance ?
- Lors du vote par **internet**. À qui je fais confiance ?