Protocoles cryptographiques…
les méthodes formelles à la rescousse!

Alexandre Debant
(équipe PESTO)

Université de Lorraine, CNRS, Inria, LORIA,
Nancy, France

Nancy, 18 janvier 2023

Loria
Laboratoire lorrain de recherche en informatique et ses applications

Inria

Quel sont leurs points communs ?

Navigation sur internet

App. d’authentication

Paiement bancaires

Vote électronique

Quel sont leurs points communs ?

Navigation sur internet

App. d’authentication

Paiement bancaires

Vote électronique

1. **Manipulation de données sensibles**
   - login/passwords
   - codes bancaires
   - données médicales
   - opinions politiques
   - ….

Quel sont leurs points communs ?

Navigation sur internet

Paiement bancaires

App. d'authentication

Vote électronique

1. **Manipulation de données sensibles**
   - login/passwords
   - codes bancaires
   - données médicales
   - opinions politiques
   - ….
2. **Elles implémentent des protocoles cryptographiques pour assurer diverses propriétés de sécurité**
   - confidentialité
   - intégrité
   - authentification
   - ….

Quel sont leurs points communs ?

Navigation sur internet

App. d'authentication

Paiement bancaires

Vote électronique

1. **Manipulation de données sensibles**
   - login/passwords
   - codes bancaires
   - données médicales
   - opinions politiques
   - ….
2. **Elles implémentent des protocoles cryptographiques pour assurer diverses propriétés de sécurité**
   - confidentialité
   - intégrité
   - authentification
   - ….
3. **Elles sont toutes sujettes à des attaques !**

Quel sont leurs points communs ?

Freak attack [Beurdouche *et al* 2015]
Logjam attack [Adrian *et al* 2015]

Navigation sur internet

Authentication flaw
[Armand *et al* 2008]

App. d'authentication

YES Card attack [Murdoch *et al* 2010]
PIN by-pass attacks [Basin et al 2021]

Paiement bancaires

Helios is broken [Cortier *et al* 2011]
Attacks against Swiss systems
[Culnane et al 2019] [Cortier et al 2022]

Vote électronique

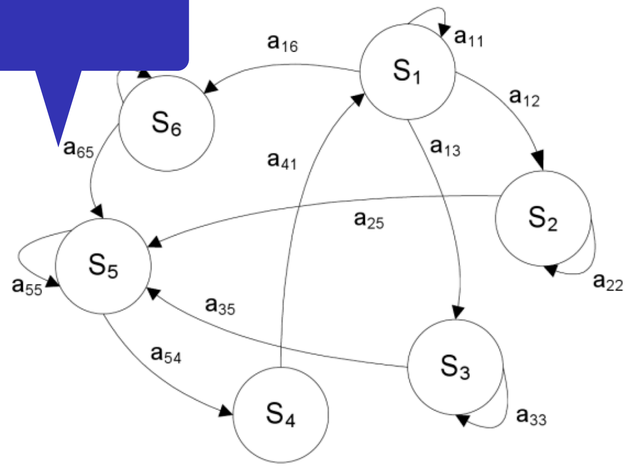
1. **Manipulation de données sensibles**
   - login/passwords
   - codes bancaires
   - données médicales
   - opinions politiques
   - ….
2. **Elles implémentent des protocoles cryptographiques pour assurer diverses propriétés de sécurité**
   - confidentialité
   - intégrité
   - authentification
   - ….
3. **Elles sont toutes sujettes à des attaques !**

Comment prouver
la sécurité d'un système?

Comment prouver la sécurité d'un système?

Modèle du système

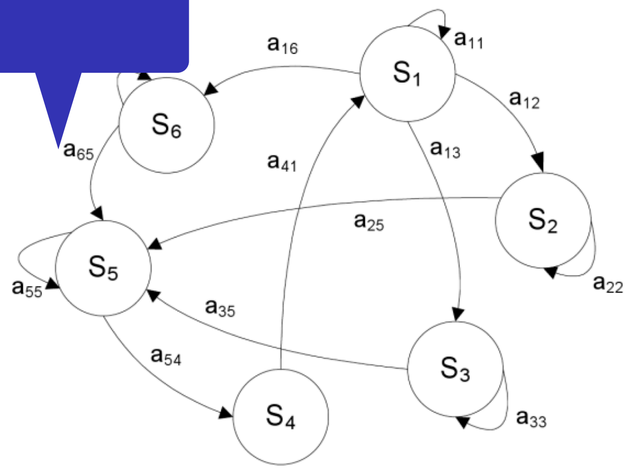
- Entrées/sorties
- Calculs et opérations effectués
- Scénarios à étudier (e.g. quel est le nombre d'agents ?)
- …



Comment prouver la sécurité d'un système?

Modèle du système

- Entrées/sorties
- Calculs et opérations effectués
- Scénarios à étudier (e.g. quel est le nombre d'agents ?)
- …



ϕ

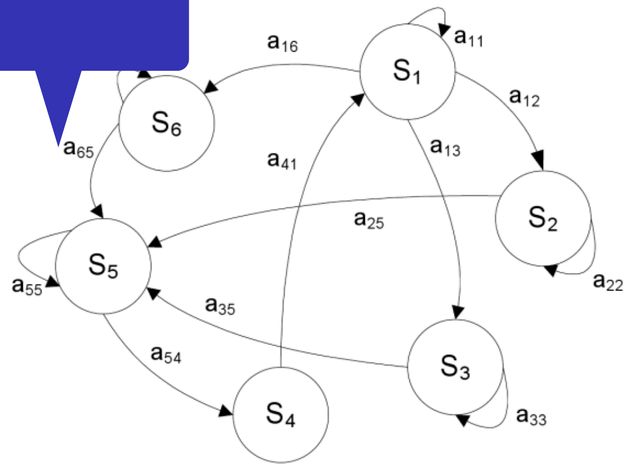
Propriété de sécurité

- Quels sont les objectifs de sécurité ?
- Que voulons-nous garantir?

Comment prouver la sécurité d'un système?

Modèle du système

- Entrées/sorties
- Calculs et opérations effectués
- Scénarios à étudier (e.g. quel est le nombre d'agents ?)
- …



Modèle de l'attaquant

- Qui peut être compromis ?
- Qu'est-ce que l'attaquant peut faire sur le réseau ?
- Qu'est-ce que l'attaquant peut déduire à partir d'un message ?
- …

ϕ

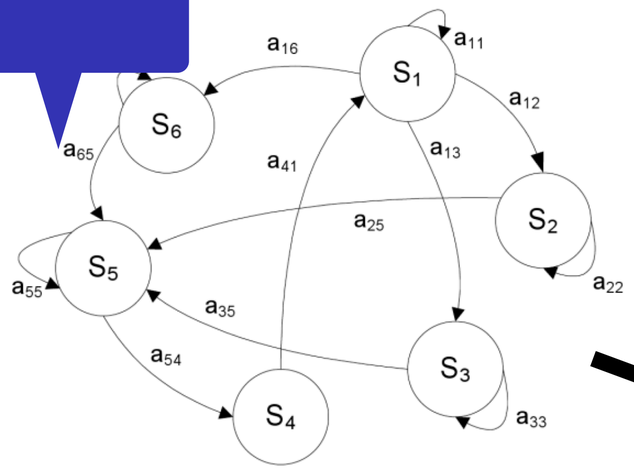
Propriété de sécurité

- Quels sont les objectifs de sécurité ?
- Que voulons-nous garantir?

Comment prouver la sécurité d'un système?

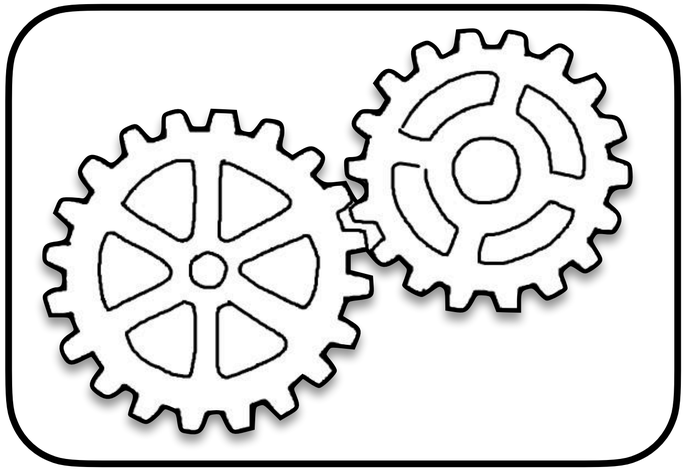
Modèle du système

- Entrées/sorties
- Calculs et opérations effectués
- Scénarios à étudier (e.g. quel est le nombre d'agents ?)
- …



Un outil (automatique)

- Efficace en pratique
- Prouvé correct



ϕ

Modèle de l'attaquant

- Qui peut être compromis ?
- Qu'est-ce que l'attaquant peut faire sur le réseau ?
- Qu'est-ce que l'attaquant peut déduire à partir d'un message ?
- …

Propriété de sécurité

- Quels sont les objectifs de sécurité ?
- Que voulons-nous garantir?

Primitives cryptographiques

chiffrement/déchiffrement

fonction de hachage

signature numérique

preuve zero-knowledge

Primitives cryptographiques

chiffrement/déchiffrement

$\texttt{enc}(x, k)$

$\texttt{dec}(c, k')$

$\texttt{dec}(\texttt{enc}(x, k), k) = x$

fonction de hachage

signature numérique

preuve zero-knowledge

Primitives cryptographiques

chiffrement/déchiffrement

$\texttt{enc}(x, k)$

$\texttt{dec}(c, k')$

$\texttt{dec}(\texttt{enc}(x, k), k) = x$

fonction de hachage

signature numérique

$\texttt{sign}(x, sk)$

$\texttt{verify}(m, \sigma, pk)$

$\texttt{verify}(m, \texttt{sign}(m, sk), \texttt{pk}(sk)) = true$

preuve zero-knowledge

Primitives cryptographiques

chiffrement/déchiffrement

$\texttt{enc}(x, k)$

$\texttt{dec}(c, k')$

$\texttt{dec}(\texttt{enc}(x, k), k) = x$

fonction de hachage

$\texttt{h}(x)$

signature numérique

$\texttt{sign}(x, sk)$

$\texttt{verify}(m, \sigma, pk)$

$\texttt{verify}(m, \texttt{sign}(m, sk), \texttt{pk}(sk)) = true$

preuve zero-knowledge

ça dépend...

Primitives cryptographiques

chiffrement/déchiffrement

$\texttt{enc}(x, k)$

$\texttt{dec}(c, k')$

$\texttt{dec}(\texttt{enc}(x, k), k) = x$

fonction de hachage

$\texttt{h}(x)$

La cryptographie est parfaite 😇

signature numérique

$\texttt{sign}(x, sk)$

$\texttt{verify}(m, \sigma, pk)$

$\texttt{verify}(m, \texttt{sign}(m, sk), \texttt{pk}(sk)) = true$

preuve zero-knowledge

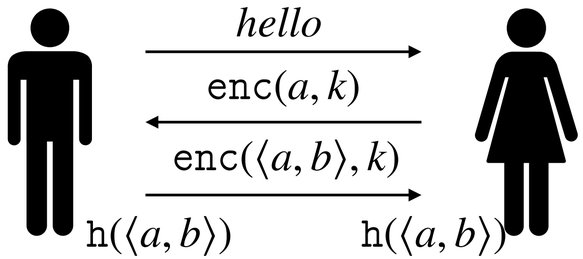
ça dépend...

Protocoles

Comment les messages sont échangés ?

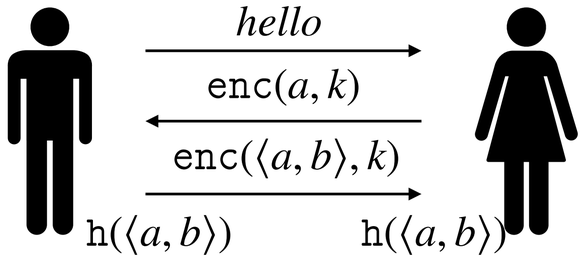
Protocoles

Comment les messages sont échangés ?



Protocoles

Comment les messages sont échangés ?

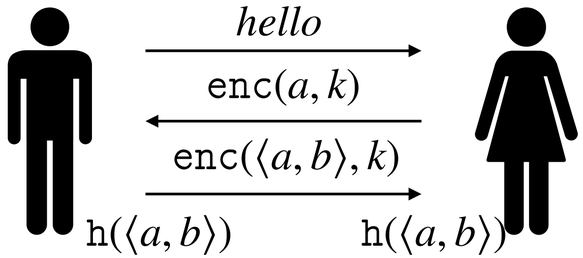


$$
\begin{array}{rl}
P := & in(c, x) \\
\mid & out(c, m) \\
\mid & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid & (P \mid Q) \\
\mid & !P \\
\mid & \ldots
\end{array}
$$

An operational semantics $P \to Q$

Protocoles

Comment les messages sont échangés ?



$$
\begin{aligned}
P := \quad & in(c, x) \\
\mid \; & out(c, m) \\
\mid \; & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid \; & (P \mid Q) \\
\mid \; & !P \\
\mid \; & \dots
\end{aligned}
$$

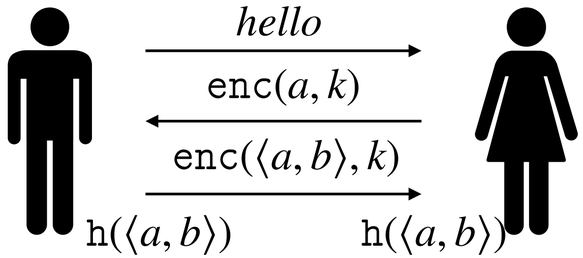
An operational semantics $P \to Q$

Example

$Bob := \quad out(c, hello);$

Protocoles

Comment les messages sont échangés ?



$$
\begin{aligned}
P := \quad & in(c, x) \\
\mid \; & out(c, m) \\
\mid \; & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid \; & (P \mid Q) \\
\mid \; & !P \\
\mid \; & \dots
\end{aligned}
$$

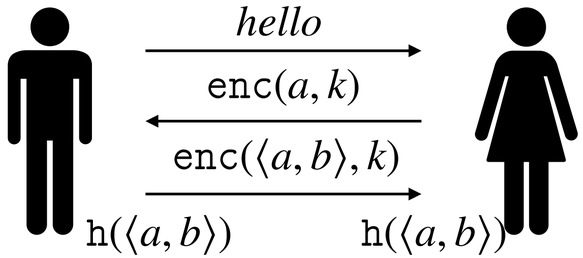
An operational semantics $P \to Q$

Example

$$
\begin{aligned}
Bob := \quad & out(c, hello); \\
& in(c, x);
\end{aligned}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{aligned}
P := \quad & in(c, x) \\
\mid \; & out(c, m) \\
\mid \; & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid \; & (P \mid Q) \\
\mid \; & !P \\
\mid \; & \ldots
\end{aligned}
$$

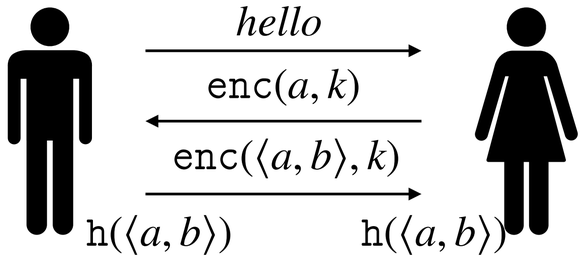
An operational semantics $P \to Q$

Example

$$
\begin{aligned}
Bob := \quad & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in
\end{aligned}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{array}{rl}
P := & in(c, x) \\
\mid & out(c, m) \\
\mid & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid & (P \mid Q) \\
\mid & !P \\
\mid & \ldots
\end{array}
$$

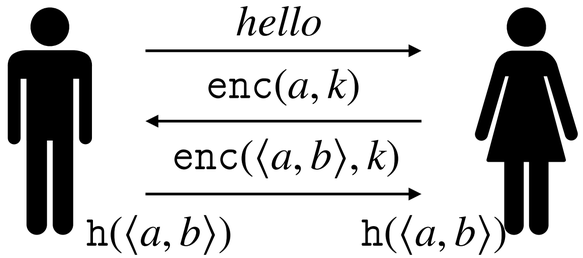
An operational semantics $P \rightarrow Q$

Example

$$
\begin{array}{rl}
Bob := & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in \\
& new\ b;
\end{array}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{aligned}
P := \quad & in(c, x) \\
\mid \; & out(c, m) \\
\mid \; & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid \; & (P \mid Q) \\
\mid \; & !P \\
\mid \; & \ldots
\end{aligned}
$$

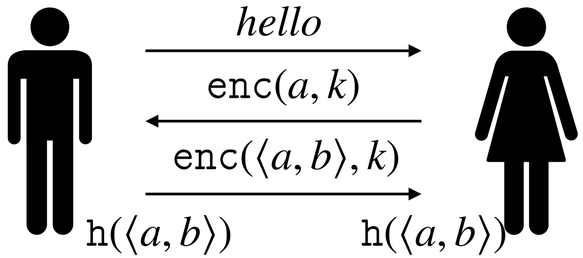
An operational semantics $P \to Q$

Example

$$
\begin{aligned}
Bob := \quad & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in \\
& new\ b; \\
& out(c, \mathtt{enc}(\langle x_a, b \rangle, k));
\end{aligned}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{aligned}
P := \quad & in(c, x) \\
\mid \; & out(c, m) \\
\mid \; & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid \; & (P \mid Q) \\
\mid \; & !P \\
\mid \; & \ldots
\end{aligned}
$$

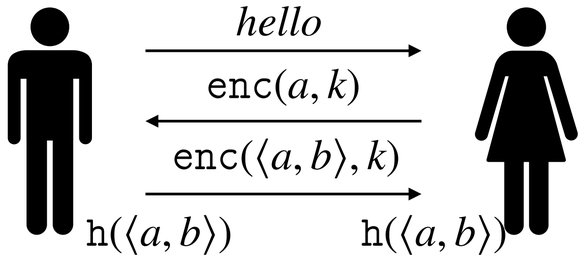
An operational semantics $P \to Q$

Example

$$
\begin{aligned}
Bob := \quad & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in \\
& new\ b; \\
& out(c, \mathtt{enc}(\langle x_a, b \rangle, k)); \\
& let\ k_{session} = \mathtt{h}(\langle x_a, b \rangle)\ in\ \ldots
\end{aligned}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{aligned}
P := \quad & in(c, x) \\
\mid \; & out(c, m) \\
\mid \; & \textit{if } b \textit{ then } P \textit{ else } Q \\
\mid \; & (P \mid Q) \\
\mid \; & !P \\
\mid \; & \ldots
\end{aligned}
$$

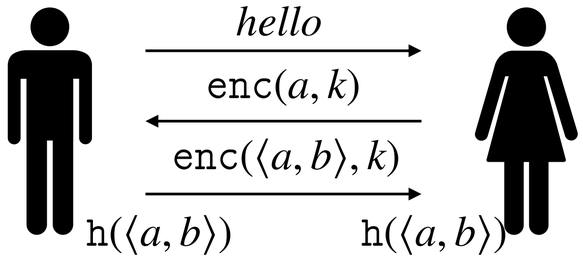
An operational semantics $P \to Q$

Example

$$
\begin{aligned}
Bob := \quad & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in \\
& new\ b; \\
& out(c, \mathtt{enc}(\langle x_a, b \rangle, k)); \\
& let\ k_{session} = \mathtt{h}(\langle x_a, b \rangle)\ in\ \ldots \\
\\
Alice := \quad & \ldots
\end{aligned}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{array}{rl}
P := & in(c, x) \\
\mid & out(c, m) \\
\mid & \mathit{if}\ b\ \mathit{then}\ P\ \mathit{else}\ Q \\
\mid & (P \mid Q) \\
\mid & !P \\
\mid & \ldots
\end{array}
$$

An operational semantics $P \to Q$

$$attacker(x) \ \wedge \ attacker(y) \Rightarrow attacker(\mathtt{enc}(x, y))$$

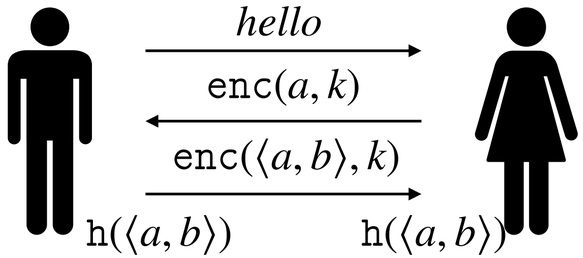
$$mess(c, enc(x, y)) \ \wedge \ mess(x, y) \Rightarrow mess(c, x)$$

Example

$$
\begin{array}{rl}
Bob := & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in \\
& new\ b; \\
& out(c, \mathtt{enc}(\langle x_a, b\rangle, k)); \\
& let\ k_{session} = \mathtt{h}(\langle x_a, b\rangle)\ in\ \ldots \\
\\
Alice := & \ldots
\end{array}
$$

Protocoles

Comment les messages sont échangés ?



$$
\begin{array}{rl}
P := & in(c, x) \\
\mid & out(c, m) \\
\mid & \text{if } b \text{ then } P \text{ else } Q \\
\mid & (P \mid Q) \\
\mid & !P \\
\mid & \ldots
\end{array}
$$

An operational semantics $P \to Q$

$$attacker(x) \ \wedge \ attacker(y) \Rightarrow attacker(\mathtt{enc}(x, y))$$

$$mess(c, enc(x, y)) \ \wedge \ mess(x, y) \Rightarrow mess(c, x)$$

Example

$$
\begin{array}{rl}
Bob := & out(c, hello); \\
& in(c, x); \\
& let\ x_a = dec(x, k)\ in \\
& new\ b; \\
& out(c, \mathtt{enc}(\langle x_a, b\rangle, k)); \\
& let\ k_{session} = \mathtt{h}(\langle x_a, b\rangle)\ in\ \ldots
\end{array}
$$

$$Alice := \quad \ldots$$

Bob

$$\Rightarrow mess(c, hello)$$

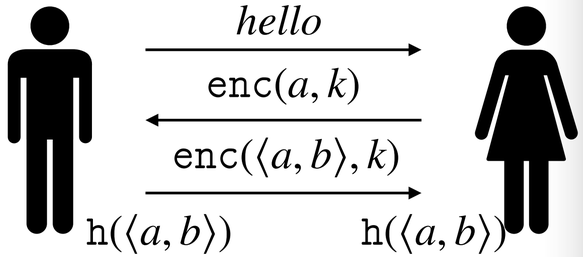
$$mess(c, \mathtt{enc}(a, k)) \Rightarrow mess(c, \mathtt{enc}(\langle a, b\rangle, k))$$

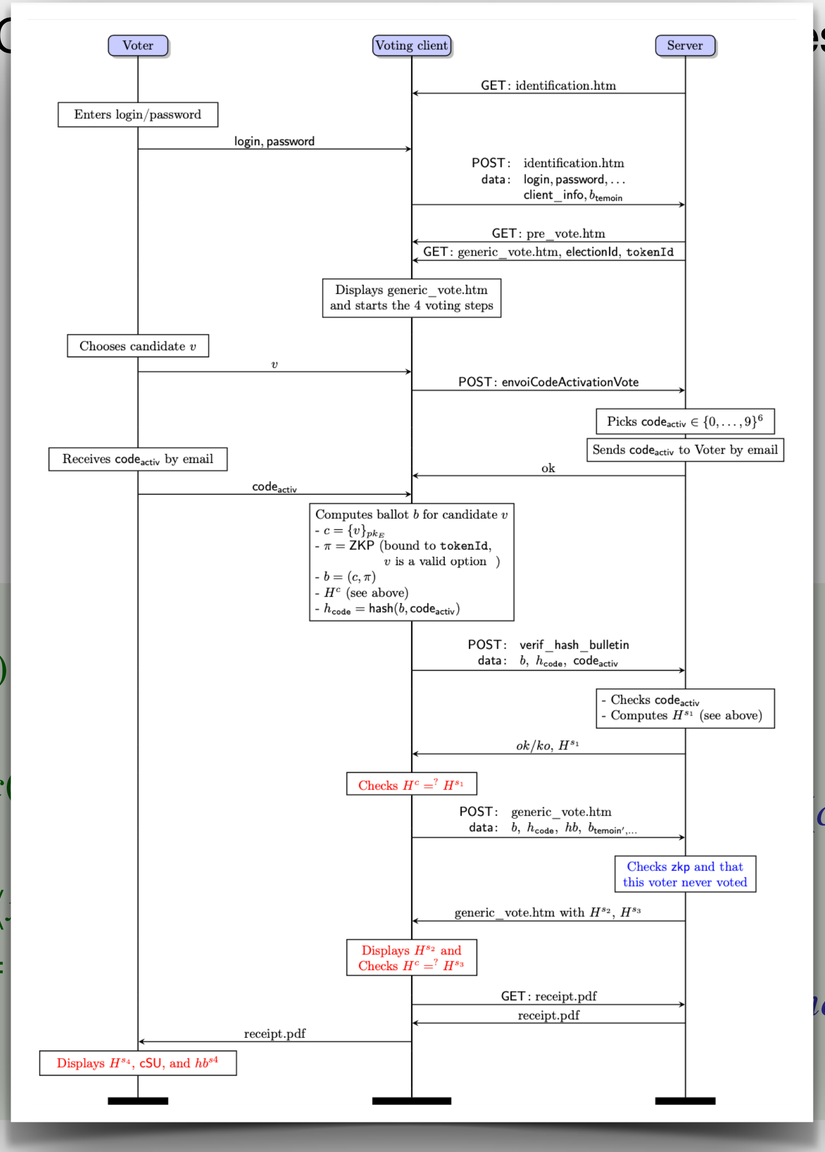
Alice

$$mess(c, hello) \Rightarrow mess(c, \mathtt{enc}(a, k))$$

Protocoles

C ... es ?





$attacker(x) \ \wedge \ attacker(y) \Rightarrow attacker(\mathtt{enc}(x, y))$

$mess(c, enc(x, y)) \ \wedge \ mess(x, y) \Rightarrow mess(c, x)$

Example

$Bob := \ out(c, hello)$

$in(c, x);$

$let \ x_a = dec($

$new \ b;$

$out(c, \mathtt{enc}(\langle$

$let \ k_{session} =$

$Alice := \ \ldots$

$\Rightarrow mess(c, hello)$

$c, \mathtt{enc}(a, k)) \Rightarrow mess(c, \mathtt{enc}(\langle a, b\rangle, k))$

$ess(c, hello) \Rightarrow mess(c, \mathtt{enc}(a, k))$

Propriétés de sécurité

Propriété de trace : un protocole P satisfait une propriété ϕ si pour tout attaquant A, et trace $tr = P\,|\,A \rightarrow Q_1 \rightarrow \ldots \rightarrow Q_n$, nous avons $\phi(tr) = true$.

Exemples:

Authentification Confidentialité Intégrité

Propriété d'équivalence : P et Q sont indistinguable si pour tout attaquant A et trace tr_P de $P\,|\,A$ il existe une trace tr_Q de $Q\,|\,A$ telle que $tr_P \approx tr_Q$.

Exemples:

Secret fort Non-traçabilité

Propriétés de sécurité

Propriété de trace : un protocole P satisfait une propriété ϕ si pour tout attaquant A, et trace $tr = P\,|\,A \rightarrow Q_1 \rightarrow \ldots \rightarrow Q_n$, nous avons $\phi(tr) = true$.

Exemples:

Authentification Confidentialité Intégrité

Propriété d'équivalence : P et Q sont indistinguable si pour tout attaquant A et trace tr_P de $P\,|\,A$ il existe une trace tr_Q de $Q\,|\,A$ telle que $tr_P \approx tr_Q$.

Exemples:

Secret fort Non-traçabilité

Prouver la sécurité d'un protocole est un problème indécidable en général

(i.e. pour des classes de protocoles et de scénarios étudiées)

Propriétés de sécurité

Propriété de trace : un protocole P satisfait une propriété ϕ si pour tout attaquant A, et trace $tr = P\,|\,A \rightarrow Q_1 \rightarrow \ldots \rightarrow Q_n$, nous avons $\phi(tr) = true$.

Exemples:

Authentification Confidentialité Intégrité

Propriété d'équivalence : P et Q sont indistinguable si pour tout attaquant A et trace tr_P de $P\,|\,A$ il existe une trace tr_Q de $Q\,|\,A$ telle que $tr_P \approx tr_Q$.

Exemples:

Secret fort Non-traçabilité

Prouver la sécurité d'un protocole est un problème indécidable en général

(i.e. pour des classes de protocoles et de scénarios étudiées)

Mais des outils efficaces en pratique existent :

DEEPSEC (Pesto, Inria Paris)

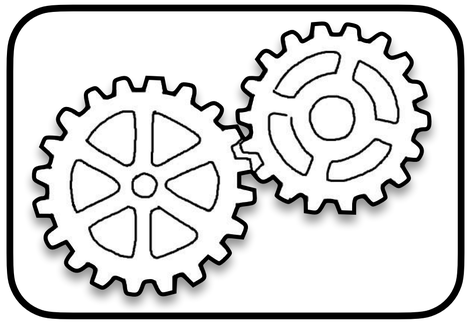
AKiSs (Pesto)

ProVerif (Inria Paris, Pesto)

TAMARIN Tamarin prover interactive mode (ETH Zurich, CISPA, Pesto)

Concrètement
on fait quoi ?

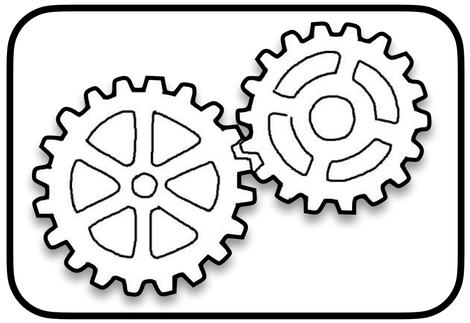
Concrètement
on fait quoi ?



1. Développements théoriques

- définitions de nouveaux modèles et formalisation des propriétés de sécurité
- conception/développement d'outils, e.g. Deepsec, Akiss, ProVerif, Tamarin
- mise en place de résultats de réduction, d'abstraction, pour l'étude de nouvelles classes de protocoles (e.g., temps, probabilités)

Concrètement
on fait quoi ?



1. Développements théoriques

- définitions de nouveaux modèles et formalisation des propriétés de sécurité
- conception/développement d'outils, e.g. Deepsec, Akiss, ProVerif, Tamarin
- mise en place de résultats de réduction, d'abstraction, pour l'étude de nouvelles classes de protocoles (e.g., temps, probabilités)

2. Étude et conception de protocoles pour la vie réelle (non exhaustif)

- protocoles de paiement sans contact **[Debant *et. al.*, 2019 & 2020]**
- protocoles d'authentification Google 2-step and FIDO U2F **[Kremer et. al., 2018]** ou encore LAKE-EDHOC **[Kremer *et. al.*, 2022]**

- protocoles de communication 5G **[Hirschi et. al., 2018 & 2019]**
- **protocoles de vote électroniques**

Le vote électronique

Contexte

Machine à voter

Vote par internet

Contexte

Machine à voter

Vote par internet

Pays utilisant des machines à voter :

- USA (>50% des états)
- France (~1M votants)
- Belgique (100% des communes)
- Brésil
- ….

Contexte

Machine à voter

Vote par internet

Pays utilisant des machines à voter :

- USA (>50% des états)
- France (~1M votants)
- Belgique (100% des communes)
- Brésil
- ….

Pays utilisant (ou ayant utilisé) le vote par internet :

- Estonie
- Suisse
- France (français de l'étranger, i.e. ~1,5M votants)
- ….

Contexte

Machine à voter

Vote par internet

Pays utilisant des machines à voter :

- USA (>50% des états)
- France (~1M votants)
- Belgique (100% des communes)
- Brésil
- ….

Pays utilisant (ou ayant utilisé) le vote par internet :

- Estonie
- Suisse
- France (français de l'étranger, i.e. ~1,5M votants)
- ….

De plus en plus utilisé dans la société en France :

- primaires présidentielles (EELV, LR, Primaire populaire)
- élections professionnelles
- élections d'associations…

Contexte

Machine à vo **ote par internet**

Quelles garanties avons-nous ?

Pays utilisant des machines à v **yant utilisé) le vote par internet :**

- USA (>50% des états)
- France (~1M votants)
- Belgique (100% des communes)
- Brésil
- ….

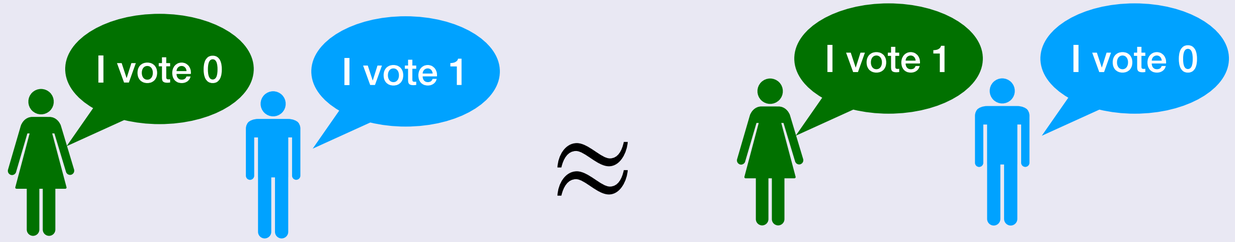
- Estonie
- Suisse
- France (français de l'étranger, i.e. ~1,5M votants)
- ….

De plus en plus utilisé dans la société en France :

- primaires présidentielles (EELV, LR, Primaire populaire)
- élections professionnelles
- élections d'associations…

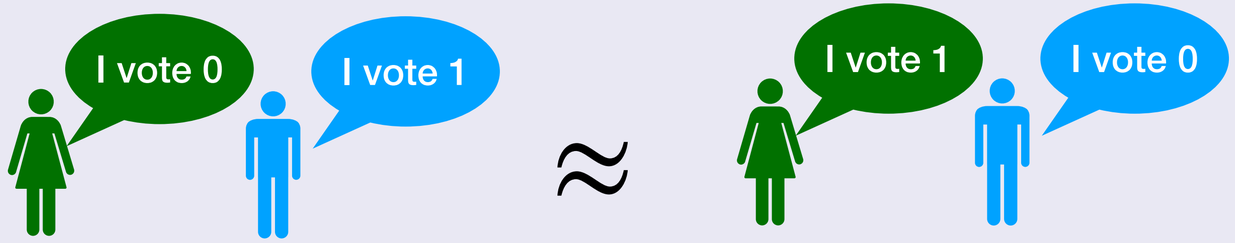
Propriétés de sécurités

Secret du vote - personne ne doit savoir pour qui j'ai voté !



Propriétés de sécurités

Secret du vote - personne ne doit savoir pour qui j'ai voté !



Vérifiabilité - personne ne peut modifier le résultat !

- Éligibilité : les bulletins comptés ont été soumis par des votants éligibles
- Vérifiabilité individuelle : je peux vérifier que mon bulletin a bien été ajouté dans l'urne
- Vérifiabilité universelle : le résultat de l'élection correspond au contenu de l'urne

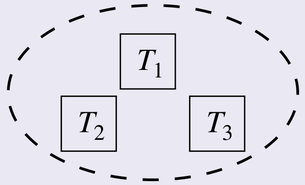
Des analyses complexes…

De nombreux agents… avec des roles très différents…

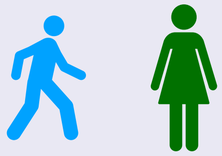
Administrateur

Tableau de bord public

Serveur de vote



Autorités de déchiffrement



Votants

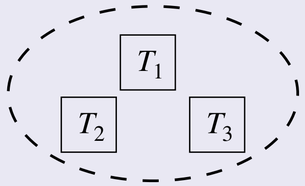
Des analyses complexes…

De nombreux agents… avec des roles très différents…

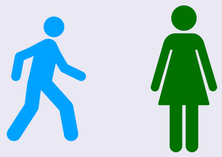
Administrateur

Tableau de bord public

Serveur de vote



Autorités de déchiffrement

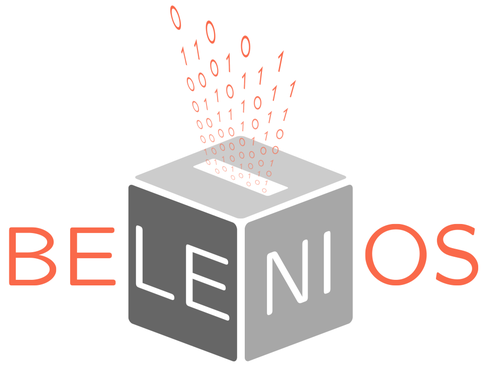


Votants

Et des scénarios complexes…

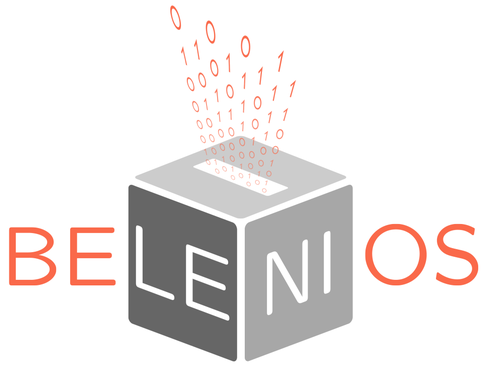
- Re-vote
- Élections à 2-tours
- Multiple urnes (*e.g.*, une par bureau de vote)

Quelques protocoles étudiés



- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : secret et vérifiabilité
  (CNIL niveau 2)

Quelques protocoles étudiés



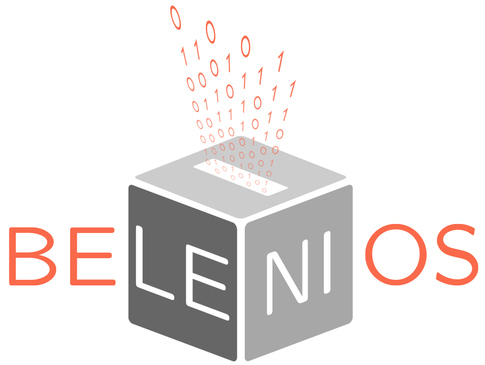
- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : secret et vérifiabilité (CNIL niveau 2)

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

VOXALY
UNE MARQUE DE DOCAPOSTE

- Dev. : Voxaly Docapost
- Cible : élections législatives français (français de l'étranger seulement)
- Sécurité : secret et vérifiabilité (CNIL niveau 3)

Quelques protocoles étudiés



- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : secret et vérifiabilité (CNIL niveau 2)

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

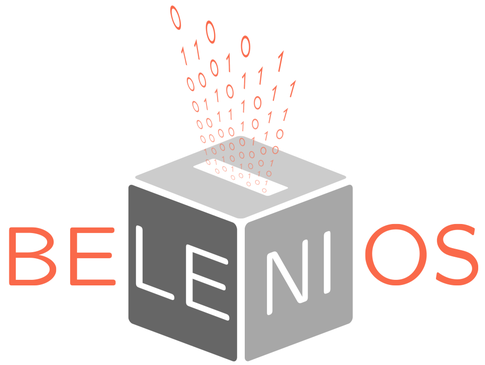
VOXALY
UNE MARQUE DE DOCAPOSTE

- Dev. : Voxaly Docapost
- Cible : élections législatives français (français de l'étranger seulement)
- Sécurité : secret et vérifiabilité (CNIL niveau 3)

SWISS POST

- Dev. : Swiss Post
- Cible : élections politiques suisses
- Sécurité : secret et vérifiabilité (avec respect de l'intention)

Quelques protocoles étudiés



- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : ~~secret~~ et vérifiabilité (CNIL niveau 2)

Attaque

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

VOXALY
UNE MARQUE DE DOCAPOSTE

- Dev. : Voxaly Docapost
- Cible : élections législatives français (français de l'étranger seulement)
- Sécurité : ~~secret~~ et ~~vérifiabilité~~ (CNIL niveau 3)

Attaques

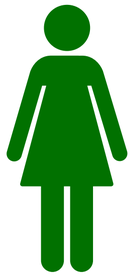
SWISS POST

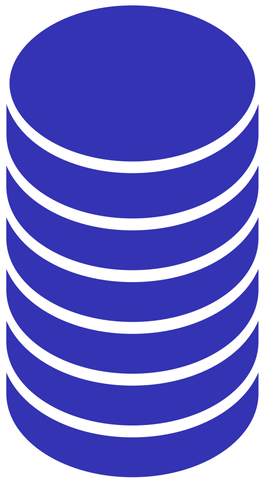
- Dev. : Swiss Post
- Cible : élections politiques suisses
- Sécurité : ~~secret~~ et vérifiabilité (avec respect de l'intention)

Attaque

Élections législatives 2022

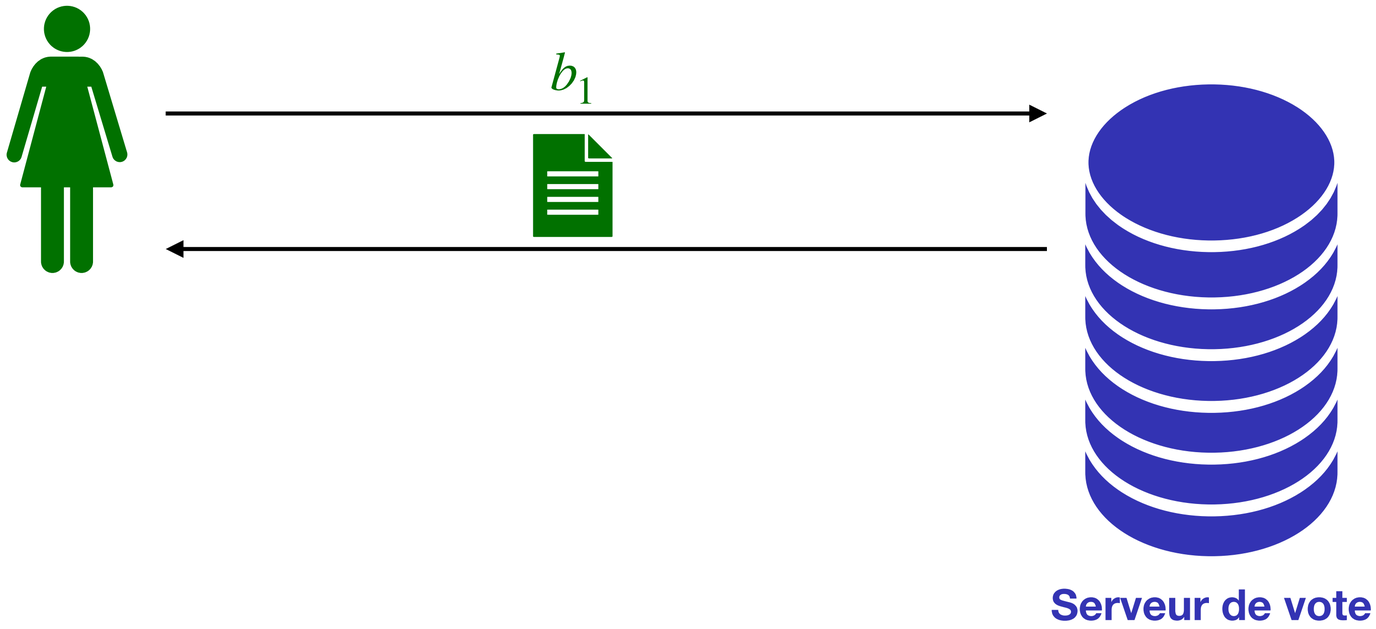
Élections législatives 2022



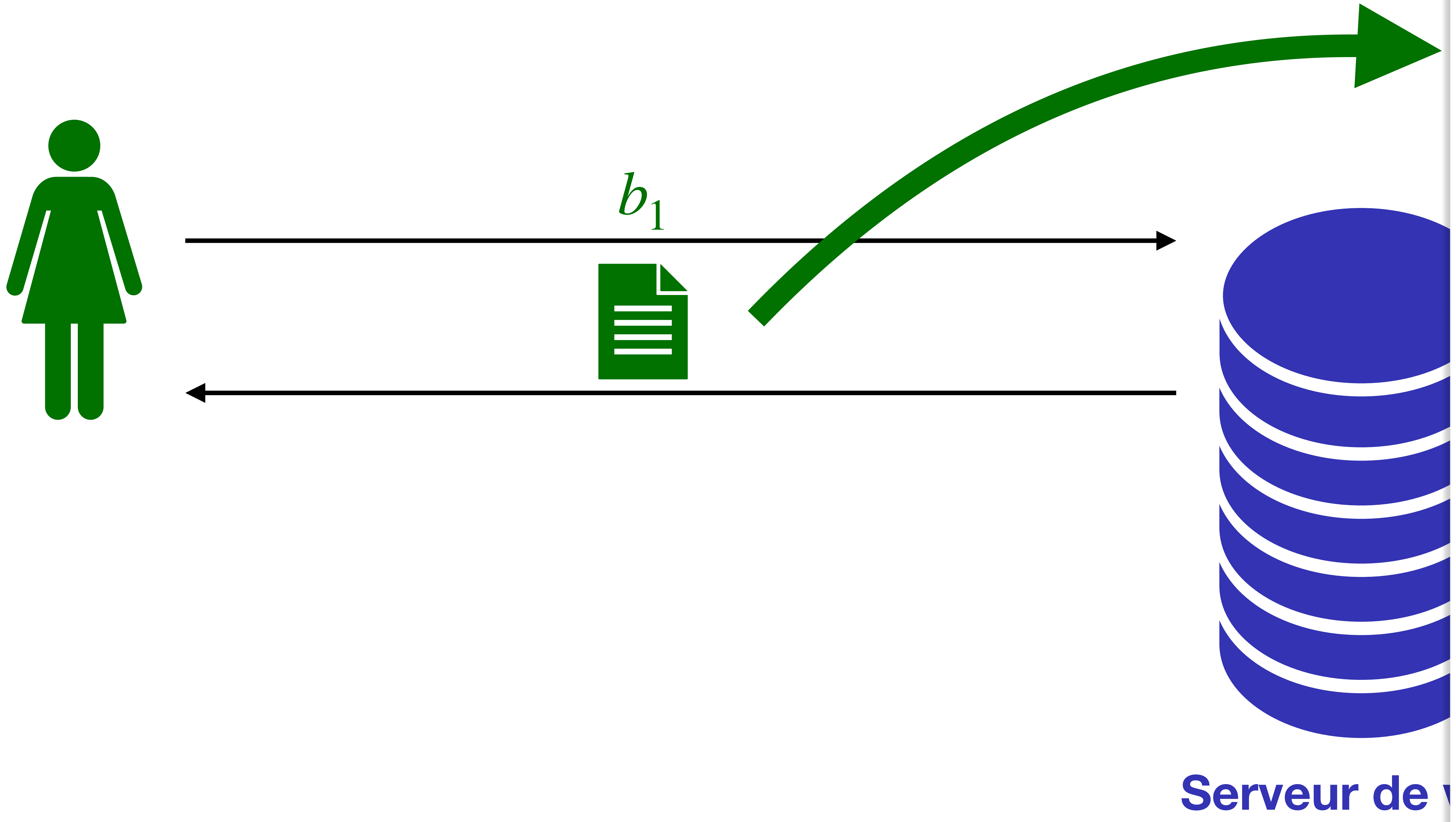


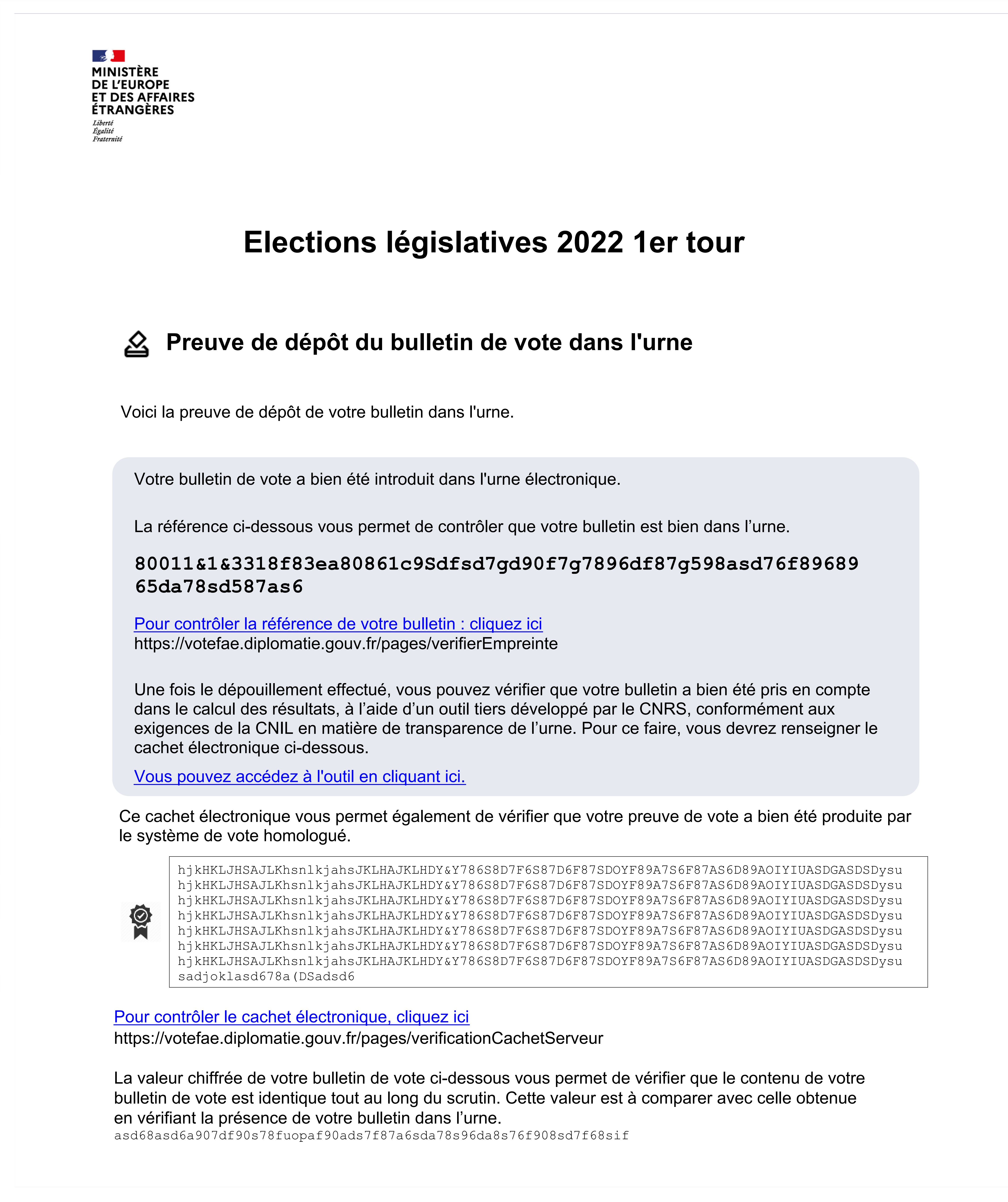
Serveur de vote

Élections législatives 2022



Élections législati




MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689 65da78sd587as6

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

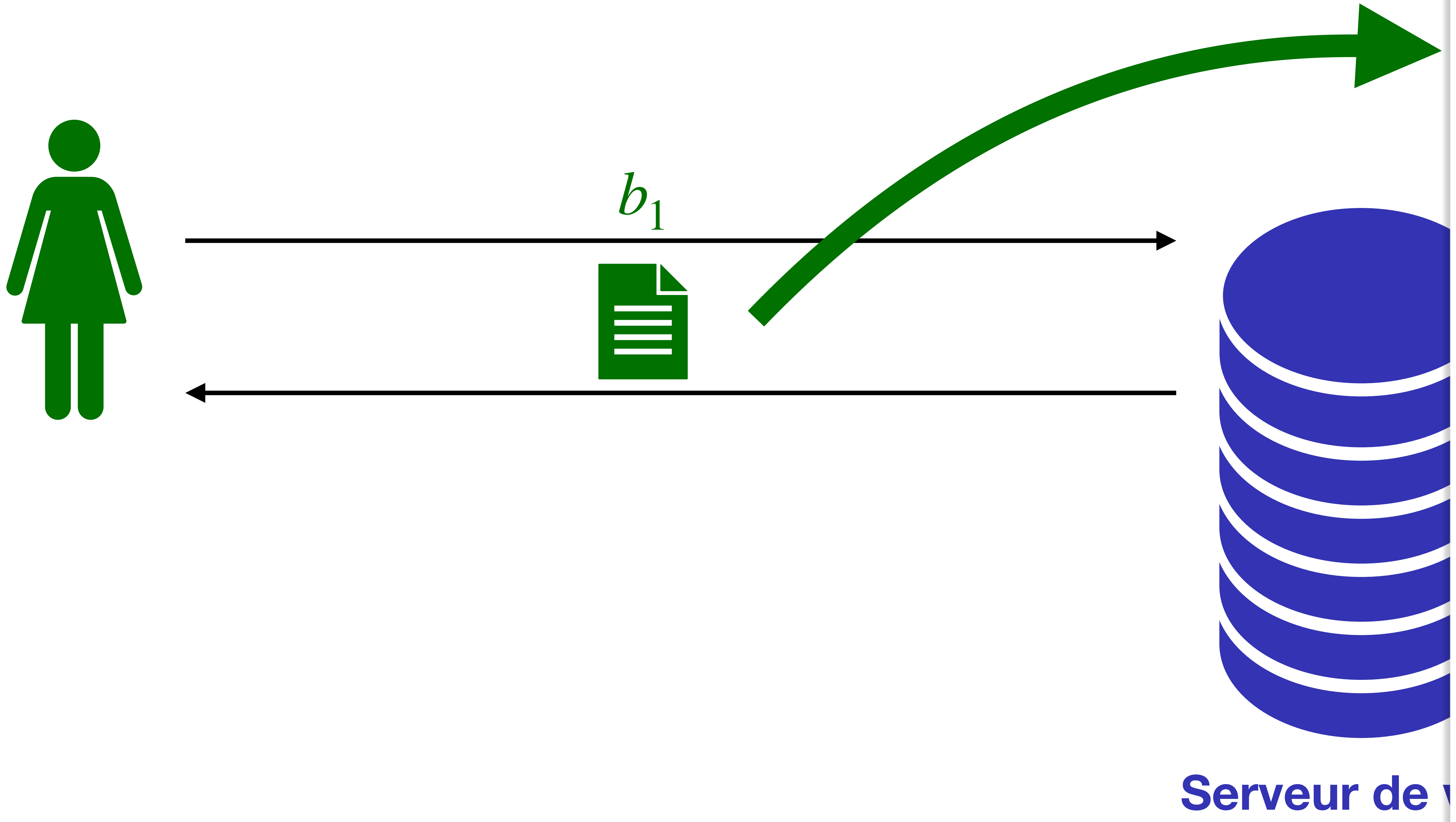
Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif

Élections législati



MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

**80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689
65da78sd587as6**

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

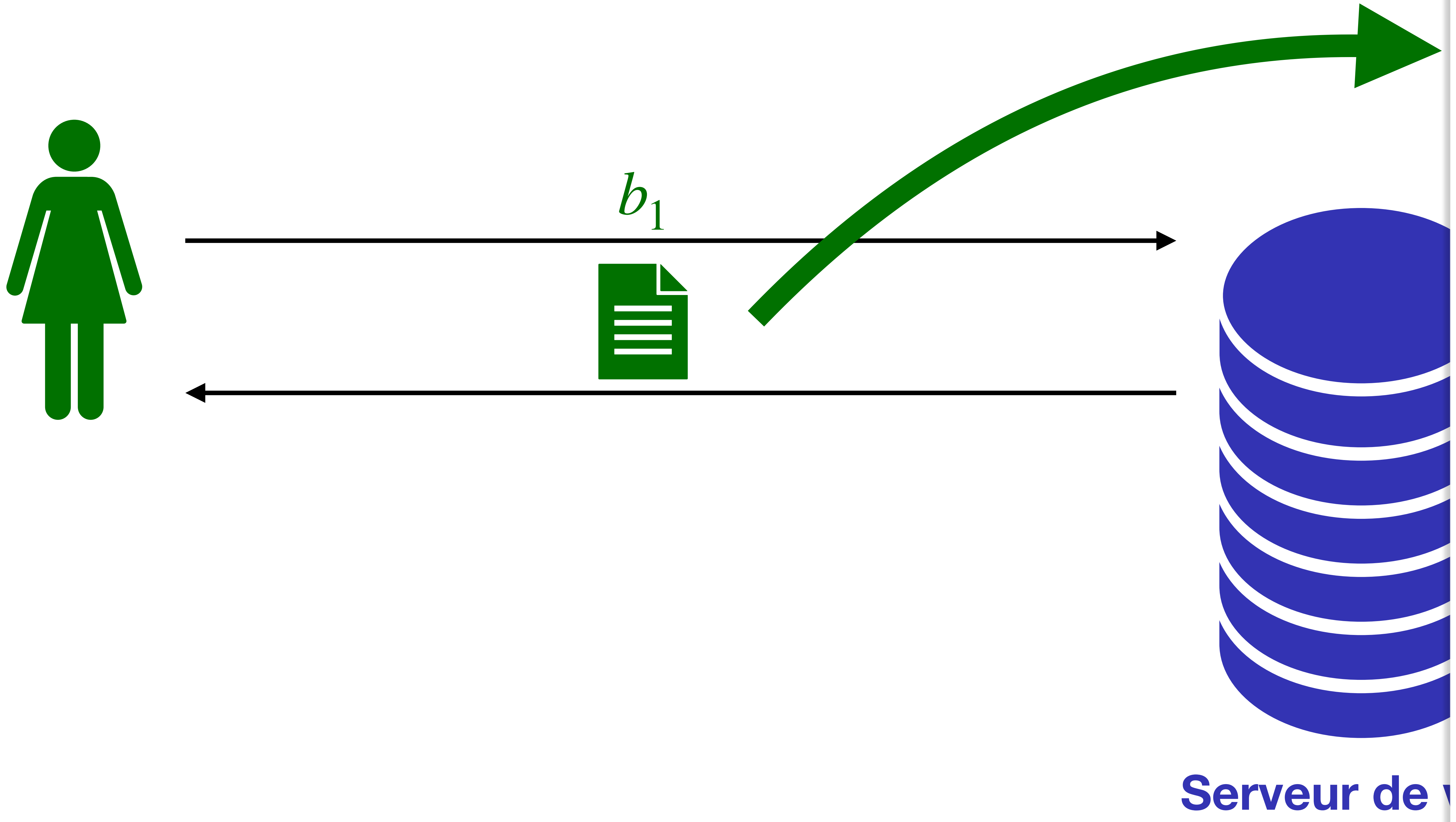
Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif

Élections législati



MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

Elections législatives 2022 1er tour

Preuve de dépôt du bulletin de vote dans l'urne

Voici la preuve de dépôt de votre bulletin dans l'urne.

C'est faux !

Votre bulletin de vote a bien été introduit dans l'urne électronique.

La référence ci-dessous vous permet de contrôler que votre bulletin est bien dans l'urne.

**80011&1&3318f83ea80861c9Sdfsd7gd90f7g7896df87g598asd76f89689
65da78sd587as6**

Pour contrôler la référence de votre bulletin : cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verifierEmpreinte

Une fois le dépouillement effectué, vous pouvez vérifier que votre bulletin a bien été pris en compte dans le calcul des résultats, à l'aide d'un outil tiers développé par le CNRS, conformément aux exigences de la CNIL en matière de transparence de l'urne. Pour ce faire, vous devrez renseigner le cachet électronique ci-dessous.

Vous pouvez accédez à l'outil en cliquant ici.

Ce cachet électronique vous permet également de vérifier que votre preuve de vote a bien été produite par le système de vote homologué.

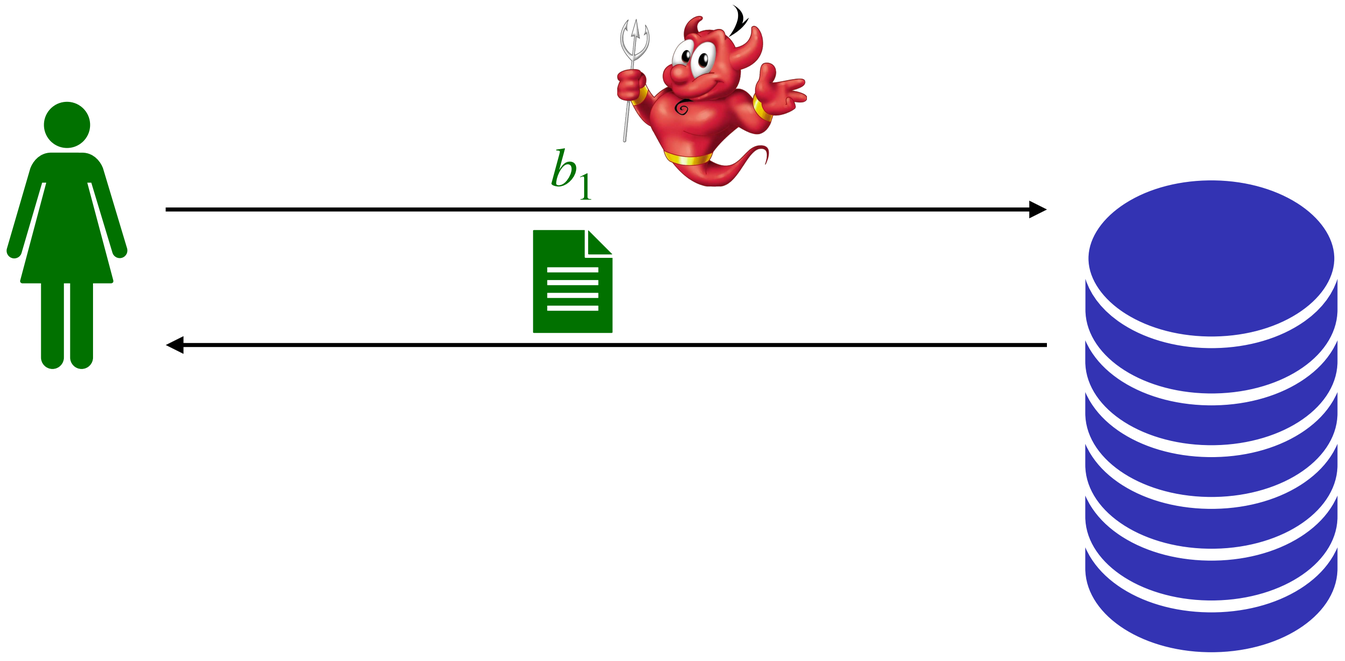
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
hjkHKLJHSAJLKhsnlkjahsJKLHAJKLHDY&Y786S8D7F6S87D6F87SDOYF89A7S6F87AS6D89AOIYIUASDGASDSDysu
sadjoklasd678a(DSadsd6

Pour contrôler le cachet électronique, cliquez ici
https://votefae.diplomatie.gouv.fr/pages/verificationCachetServeur

La valeur chiffrée de votre bulletin de vote ci-dessous vous permet de vérifier que le contenu de votre bulletin de vote est identique tout au long du scrutin. Cette valeur est à comparer avec celle obtenue en vérifiant la présence de votre bulletin dans l'urne.
asd68asd6a907df90s78fuopaf90ads7f87a6sda78s96da8s76f908sd7f68sif

Élections législatives 2022

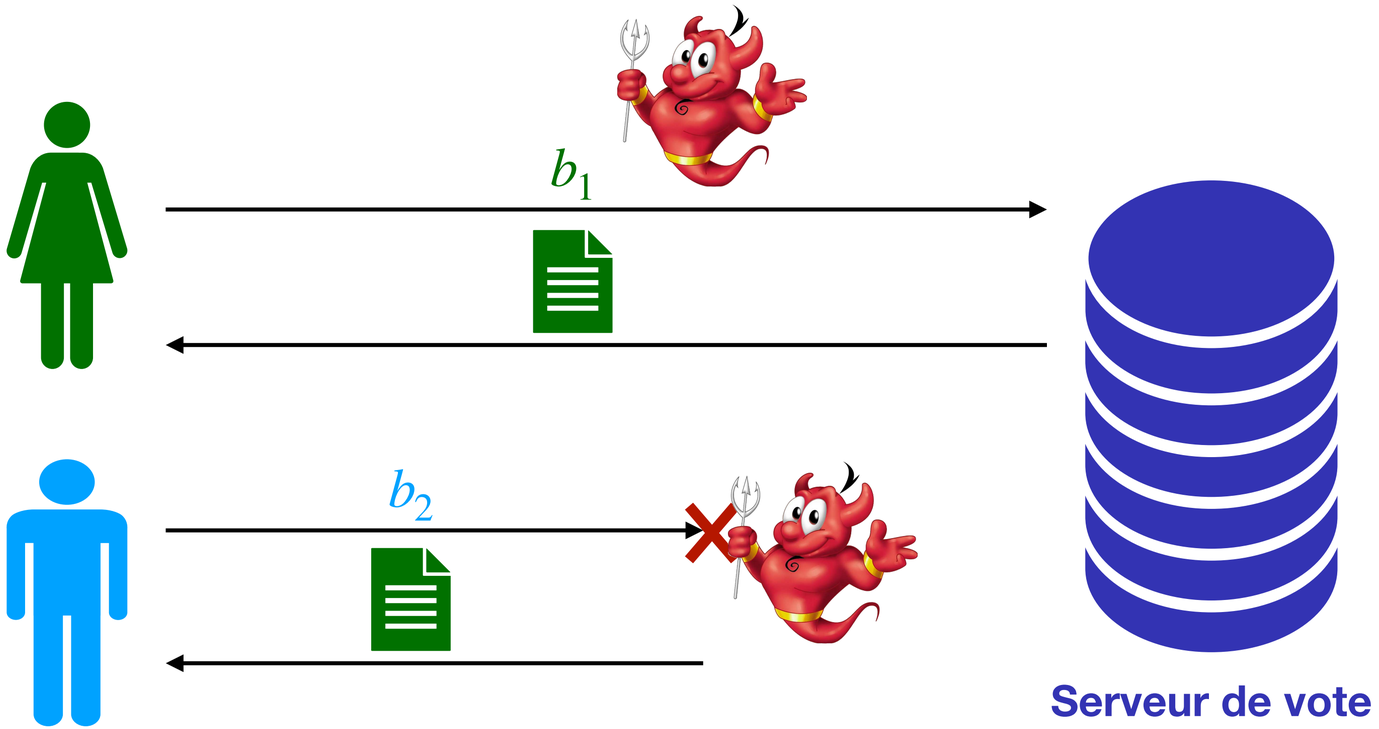
(attaque)



Étape 1 : Alice vote normalement

Élections législatives 2022

(attaque)

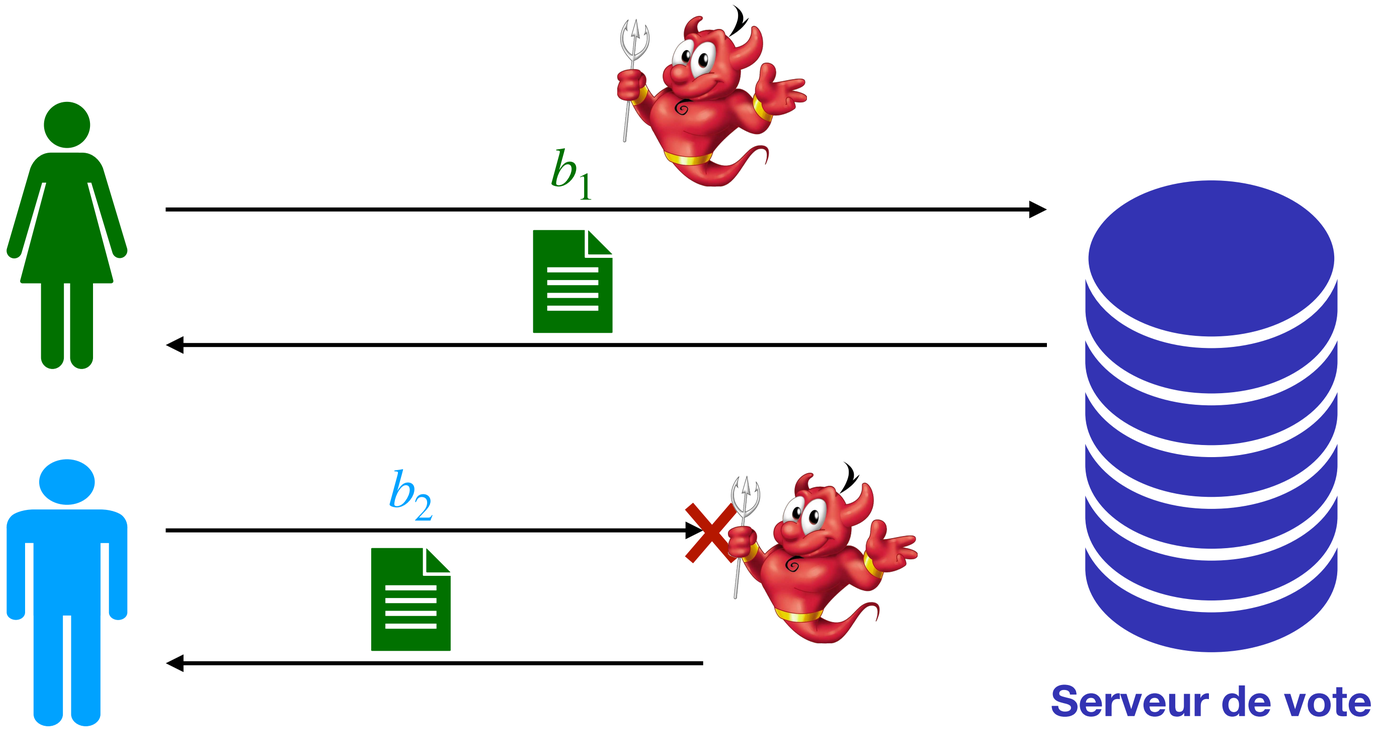


Étape 1 : Alice vote normalement

Étape 2 : l'attaquant intercepte le bulletin de Bob et répond en utilisant le reçu d'Alice

Élections législatives 2022

(attaque)



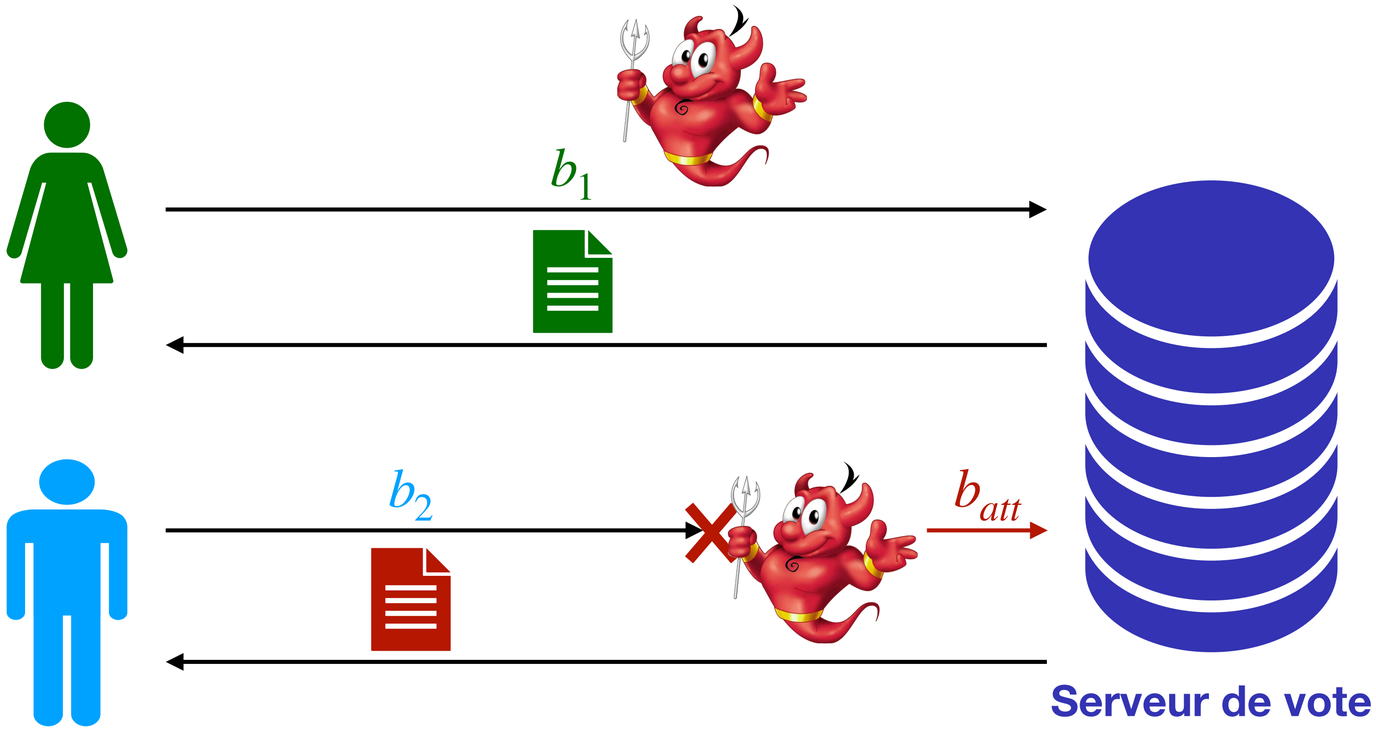
Étape 1 : Alice vote normalement

Étape 2 : l'attaquant intercepte le bulletin de Bob et répond en utilisant le reçu d'Alice

Résultat: le bulletin de Bob est jeté… mais Bob ne s'est aperçu de rien !

Élections législatives 2022

(attaque)



Étape 1 : Alice vote normalement

Étape 2 : l'attaquant intercepte le bulletin de Bob et répond en utilisant le reçu d'Alice

Résultat: le bulletin de Bob est jeté… mais Bob ne s'est aperçu de rien !

Amélioration : l'attaquant peut remplacer le bulletin par un autre !

Quelques protocoles étudiés

BELENIOS

- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : secret et vérifiabilité (CNIL niveau 2)

Attaque

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

VOXALY
UNE MARQUE DE DOCAPOSTE

- Dev. : Voxaly Docapost
- Cible : élections législatives français (français de l'étranger seulement)
- Sécurité : secret et vérifiabilité (CNIL niveau 3)

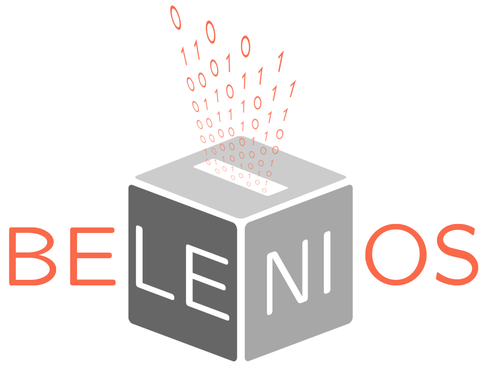
Attaques

SWISS POST

- Dev. : Swiss Post
- Cible : élections politiques suisses
- Sécurité : secret et vérifiabilité (avec respect de l'intention)

Attaque

Quelques protocoles étudiés



- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : secret et vérifiabilité (CNIL niveau 2)

✅ **Correctif proposé et prouvé**

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

VOXALY
UNE MARQUE DE DOCAPOSTE

- Dev. : Voxaly Docapost
- Cible : élections législatives français (français de l'étranger seulement)
- Sécurité : secret et vérifiabilité (CNIL niveau 3)

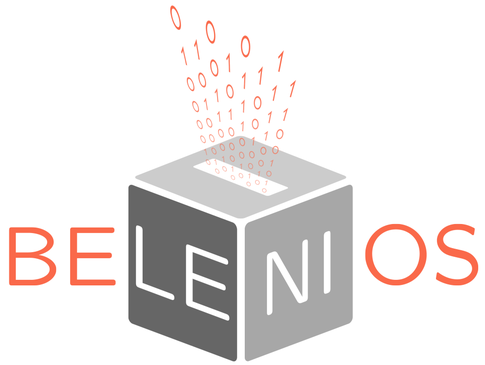
✅ **Correctifs proposés**

SWISS POST

- Dev. : Swiss Post
- Cible : élections politiques suisses
- Sécurité : secret et vérifiabilité (avec respect de l'intention)

✅ **Correctif proposé et prouvé**

Quelques protocoles étudiés



- Dev. : Loria et Inria
- Cible : associations et entreprises
- +1400 élections par an
- gratuit
- Sécurité : secret et vérifiabilité (CNIL niveau 2)

✅ **Correctif proposé et prouvé**

MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

VOXALY UNE MARQUE DE DOCAPOSTE

- Dev. : Voxaly Docapost
- Cible : élections législatives français (français de l'étranger seulement)
- Sécurité : secret et vérifiabilité (CNIL niveau 3)

✅ **Correctifs proposés**

SWISS POST

- Dev. : Swiss Post
- Cible : élections politiques suisses
- Sécurité : secret et vérifiabilité (avec respect de l'intention)

✅ **Correctif proposé et prouvé**

Chaque analyse ouvre de nouvelles questions de recherche

Exemples de problèmes ouverts

Exemples de problèmes ouverts

1. Que se passe-t-il si l'ordinateur du votant est corrompu ?

- Aujourd'hui : pas de garantie…
- Demain : - secret ? Probablement non…
  - vérifiabilité ? Oui

Exemples de problèmes ouverts

1. Que se passe-t-il si l'ordinateur du votant est corrompu ?

- Aujourd'hui : pas de garantie…
- Demain : - secret ? Probablement non…
  - vérifiabilité ? Oui

2. Pouvons-nous rendre responsables de leurs actes les différents agents?

- Aujourd'hui : un reçu invalide n'est PAS une preuve d'attaque,
- Demain : - reçu invalide ⇒ preuve d'attaque ? Oui
  - reçu invalide ⇒ preuve d'attaque & identité d'un responsable ? Idéalement

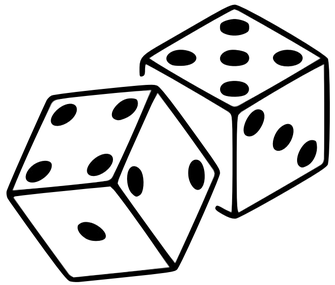
Exemples de problèmes ouverts

1. Que se passe-t-il si l'ordinateur du votant est corrompu ?

- Aujourd'hui : pas de garantie…
- Demain : - secret ? Probablement non…
  - vérifiabilité ? Oui

2. Pouvons-nous rendre responsables de leurs actes les différents agents?

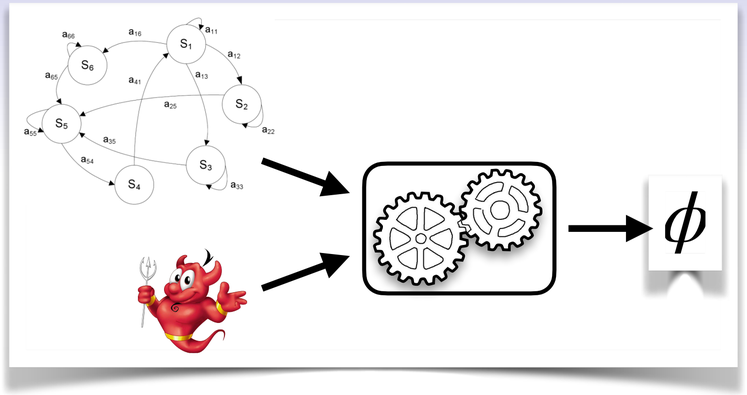
- Aujourd'hui : un reçu invalide n'est PAS une preuve d'attaque,
- Demain : - reçu invalide ⇒ preuve d'attaque ? Oui
  - reçu invalide ⇒ preuve d'attaque & identité d'un responsable ? Idéalement



3. Comment modéliser et analyser des protocoles incluant des choix aléatoires ?

- Aujourd'hui : impossible…
- Demain : de nouveaux modèles et outils automatiques ?

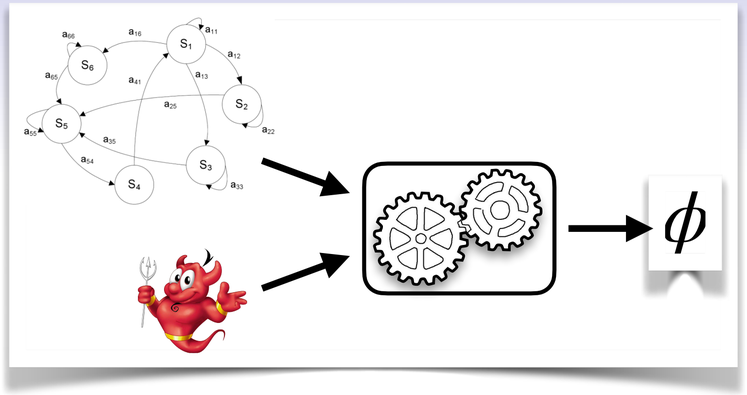
D’autres applications des méthodes formelles



1. Protocoles cryptographiques

- vote électronique, protocoles de communication, paiement, authentification, etc.

D’autres applications des méthodes formelles

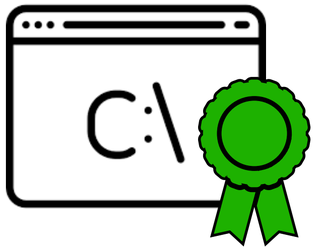


1. Protocoles cryptographiques

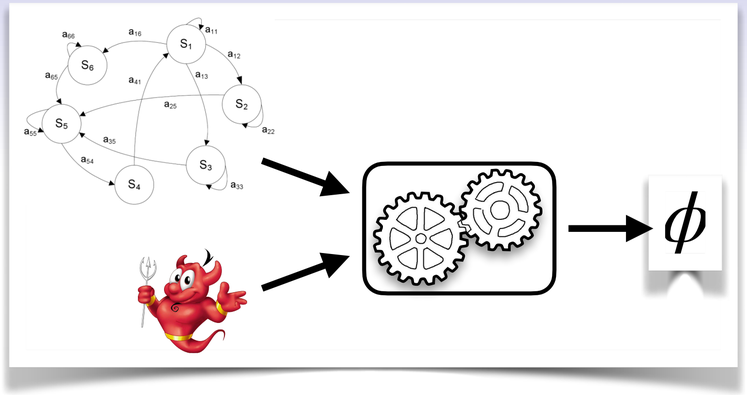
- vote électronique, protocoles de communication, paiement, authentification, etc.

2. Preuve de programmes critiques

- Preuve d’absence de bugs, deadlocks, constant-time etc.
- Correction de la compilation
- Applications : aéronautique, aérospatial, métro automatiques, centrales nucléaires, etc.



D’autres applications des méthodes formelles

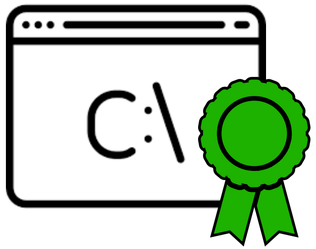


1. Protocoles cryptographiques

- vote électronique, protocoles de communication, paiement, authentification, etc.

2. Preuve de programmes critiques

- Preuve d’absence de bugs, deadlocks, constant-time etc.
- Correction de la compilation
- Applications : aéronautique, aéropatial, métro automatiques, centrales nucléaires, etc.



3. Recherche de bugs (fuzzing, testing)

- Pas une preuve mais une aide à la conception
- Applications : librairies crypto, implémentations de protocoles, etc.