Vote by mail

Design and verification of a secure protocol

Léo Louistisserand
Supervisors : Véronique Cortier & Pierrick Gaudry

INRIA Nancy

30/03/2023

Motivations

Why be interested in postal voting?

Medium stakes ballots

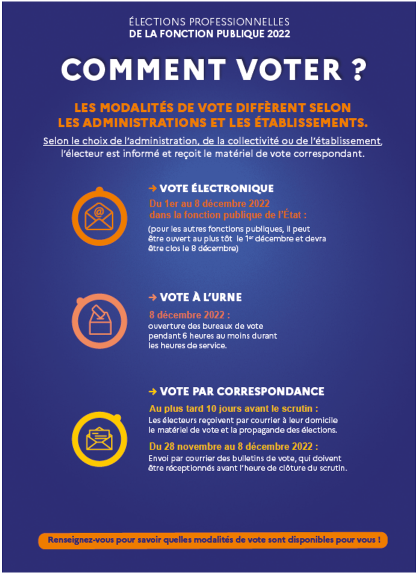
Remote voting is widely used:

- Professional elections
- Trade union elections
- Associations
- University boards of directors
- Political primaries

Medium stakes ballots

Remote voting is widely used:

- Professional elections
- Trade union elections
- Associations
- University boards of directors
- Political primaries



ÉLECTIONS PROFESSIONNELLES
DE LA FONCTION PUBLIQUE 2022

COMMENT VOTER ?

LES MODALITÉS DE VOTE DIFFÈRENT SELON LES ADMINISTRATIONS ET LES ÉTABLISSEMENTS.

Selon le choix de l'administration, de la collectivité ou de l'établissement, l'électeur est informé et reçoit le matériel de vote correspondant.

→ **VOTE ÉLECTRONIQUE**

Du 1er au 8 décembre 2022 dans la fonction publique de l'État :

(pour les autres fonctions publiques, il peut être ouvert au plus tôt le 1er décembre et devra être clos le 8 décembre)

→ **VOTE À L'URNE**

8 décembre 2022 :

ouverture des bureaux de vote pendant 6 heures au moins durant les heures de service.

→ **VOTE PAR CORRESPONDANCE**

Au plus tard 10 jours avant le scrutin :

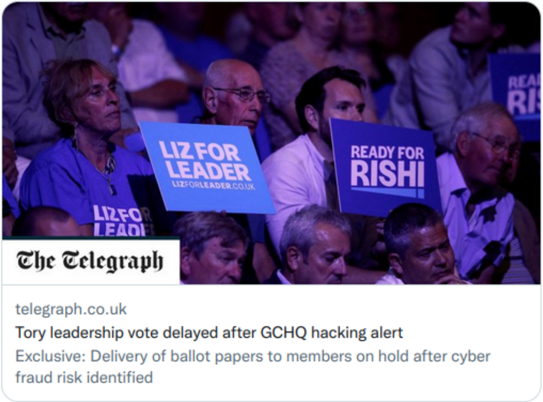
Les électeurs reçoivent par courrier à leur domicile le matériel de vote et la propagande des élections.

Du 28 novembre au 8 décembre 2022 :

Envoi par courrier des bulletins de vote, qui doivent être réceptionnés avant l'heure de clôture du scrutin.

Renseignez-vous pour savoir quelles modalités de vote sont disponibles pour vous !

… but also very high stakes



telegraph.co.uk

Tory leadership vote delayed after GCHQ hacking alert

Exclusive: Delivery of ballot papers to members on hold after cyber fraud risk identified

2022 Conservative Party leadership election

Objectives

- Voters must be able to vote without a computer. It may be required to conduct verifications.
- The protocol must be at least as good as that of the current one.

Objectives

- Voters must be able to vote without a computer. It may be required to conduct verifications.
- The protocol must be at least as good as that of the current one.

Question

What does ''good'' mean?

Objectives

- Voters must be able to vote without a computer. It may be required to conduct verifications.
- The protocol must be at least as good as that of the current one.

Question

What does ''good'' mean?

Some properties measure the quality of a protocol.

Verifiability

A transparent protocol ensures a legitimate result.

Verifiability

A transparent protocol ensures a legitimate result.

- **Individual verifiability:** my ballot is in the ballot box and contains my vote.

Verifiability

A transparent protocol ensures a legitimate result.

- **Individual verifiability:** my ballot is in the ballot box and contains my vote.
- **Eligibility:** each valid ballot in the ballot box comes from a legitimate voter.

Verifiability

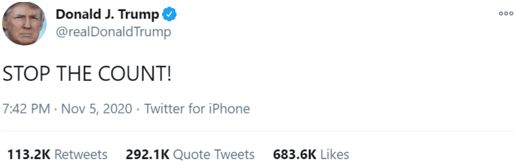
A transparent protocol ensures a legitimate result.

- **Individual verifiability:** my ballot is in the ballot box and contains my vote.
- **Eligibility:** each valid ballot in the ballot box comes from a legitimate voter.
- **Universal verifiability:** the result corresponds to the ballot box's content.

Verifiability

A transparent protocol ensures a legitimate result.

- **Individual verifiability:** my ballot is in the ballot box and contains my vote.
- **Eligibility:** each valid ballot in the ballot box comes from a legitimate voter.
- **Universal verifiability:** the result corresponds to the ballot box's content.



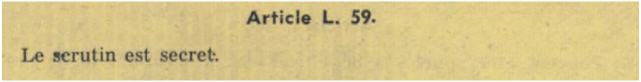
Donald J. Trump
@realDonaldTrump

STOP THE COUNT!

7:42 PM · Nov 5, 2020 · Twitter for iPhone

113.2K Retweets **292.1K** Quote Tweets **683.6K** Likes

Privacy

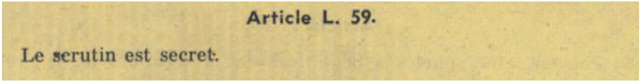


Article L. 59.

Le scrutin est secret.

- **Secrecy:** no one can know my vote.

Privacy

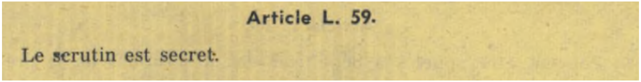


Article L. 59.

Le scrutin est secret.

- **Secrecy:** no one can know my vote.
- **Coercion resistance:** no one can know my vote, *even with my help*.

Privacy



Article L. 59.

Le scrutin est secret.

- **Secrecy:** no one can know my vote.
- **Coercion resistance:** no one can know my vote, *even with my help*.

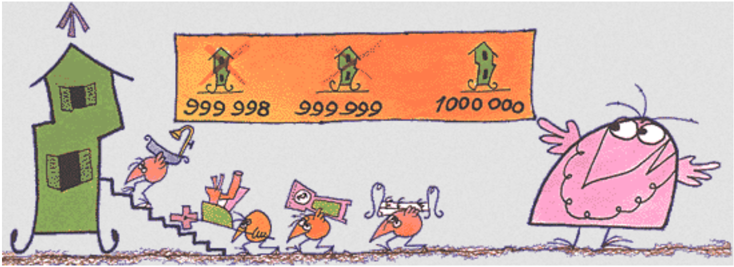
Other properties

- **Accessibility:** Voters can easily vote, get the result of the election, do the checks, etc.

Other properties

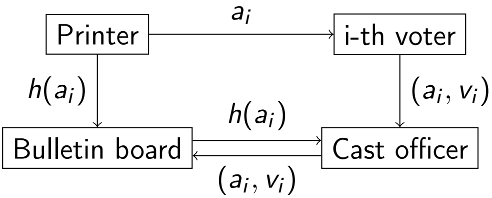
- **Accessibility:** Voters can easily vote, get the result of the election, do the checks, etc.
- **Accountability:** In case of problems, it is possible:
  - for the witness to support their denunciation.
  - for each entity to prove that it has followed the protocol.

Design of a protocol



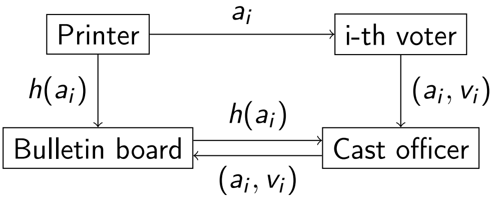
Trial and error

First attempt



Idea: each voter receives a token a_i to track their ballot.

First attempt

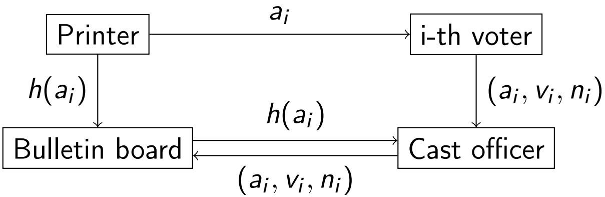


Idea: each voter receives a token a_i to track their ballot.

Clash attack

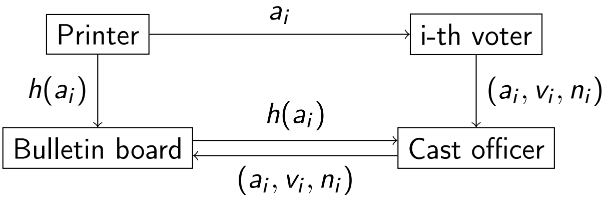
A dishonest printer may send the same token to different voters.

First contermeasure



Idea: each voter adds a number of their choice n_i to their ballot.

First contermeasure



Printer

a_i

i-th voter

$h(a_i)$

(a_i, v_i, n_i)

$h(a_i)$

Bulletin board

Cast officer

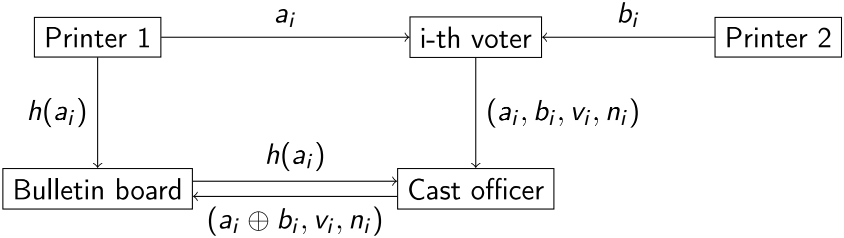
(a_i, v_i, n_i)

Idea: each voter adds a number of their choice n_i to their ballot.

Honest but curious attacker

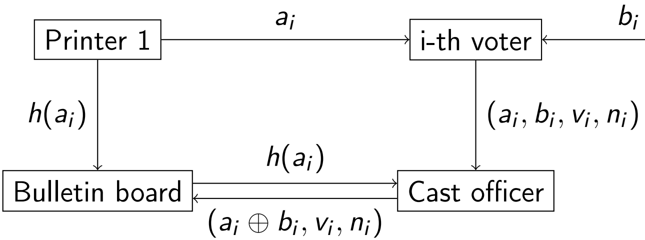
The printer knows everyone's vote.

Second contermeasure



Idea: split the printer to share the secret between two entities.

Second contermeasure

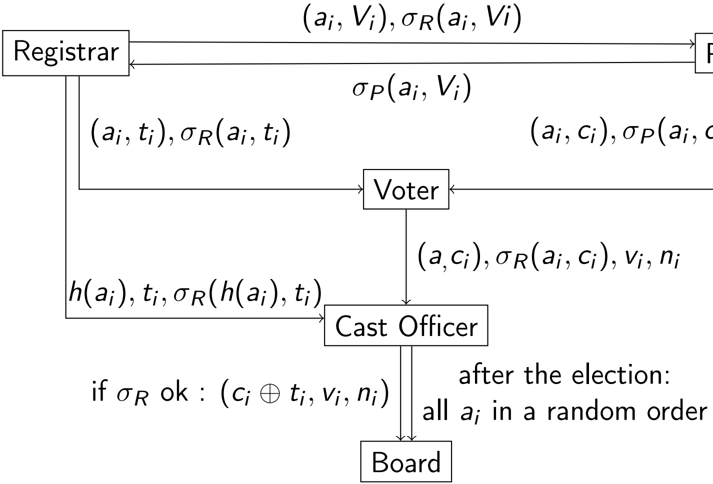


Idea: split the printer to share the secret between two entities.

Complexity of the protocol

Each voter receives two envelopes.

Vote&Check


$(a_i, V_i), \sigma_R(a_i, Vi)$
Registrar
Printer
$\sigma_P(a_i, V_i)$
$(a_i, t_i), \sigma_R(a_i, t_i)$
$(a_i, c_i), \sigma_P(a_i, c_i)$
Voter
$(a_, c_i), \sigma_R(a_i, c_i), v_i, n_i$
$h(a_i), t_i, \sigma_R(h(a_i), t_i)$
Cast Officer
if σ_R ok : $(c_i \oplus t_i, v_i, n_i)$
after the election:
all a_i in a random order
Board

Security properties

Verifiability

- Individual verifiability holds even if all the entities are dishonest.
- The eligibility holds if the registrar is honest or if the printer and the cast officer are honest.
- Universal verifiability always holds.

Security properties

Verifiability

- Individual verifiability holds even if all the entities are dishonest.
- The eligibility holds if the registrar is honest or if the printer and the cast officer are honest.
- Universal verifiability always holds.

Privacy

- The secrecy holds if the registrar and at least one of the two other entities are honest.
- The coercion resistance never holds.

Overview table

	Untrusted entities		
	At most 1	2 but not reg.	2 including reg.
Individual verifiability	✓	✓	✓
Universal verifiability	✓	✓	✓
Eligibility	✓	✓	✗
Ballot secrecy	✗	✗	✗
Coercion resistance	✗	✗	✗

Thanks for your attention