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?
Remote voting is widely used:

- Professional elections
- Trade union elections
- Associations
- University boards of directors
- Political primaries
Remote voting is widely used:

- Professional elections
- Trade union elections
- Associations
- University boards of directors
- Political primaries
... but also very high stakes

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.

STOP THE COUNT!

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

113.2K Retweets  292.1K Quote Tweets  683.6K Likes
Privacy

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

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

- **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.
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 countermeasure

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

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 countermeasure

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

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

**Complexity of the protocol**

Each voter receives two envelopes.
Vote&Check

Registrar → (a_i, V_i), σ_R(a_i, V_i)

σ_P(a_i, V_i)

(a_i, t_i), σ_R(a_i, t_i)

σ_P(a_i, V_i)

(a_i, c_i), σ_P(a_i, c_i)

Voter

(a_i, t_i), σ_R(a_i, t_i)

h(a_i), t_i, σ_R(h(a_i), t_i)

Voter

(a_i, c_i), σ_R(a_i, c_i), v_i, n_i

if σ_R ok : (c_i ⊕ t_i, v_i, n_i)

Cast Officer

all a_i in a random order

after the election:

Board

Léo Louistisserand
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

<table>
<thead>
<tr>
<th></th>
<th>Untrusted entities</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>At most 1</td>
</tr>
<tr>
<td>Individual verifiability</td>
<td>✓</td>
</tr>
<tr>
<td>Universal verifiability</td>
<td>✓</td>
</tr>
<tr>
<td>Eligibility</td>
<td>✓</td>
</tr>
<tr>
<td>Ballot secrecy</td>
<td>✗</td>
</tr>
<tr>
<td>Coercion resistance</td>
<td>✗</td>
</tr>
</tbody>
</table>
Thanks for your attention