Measuring Voter-controlled Privacy

Hugo Jonker

in collaboration with Sjouke Mauw and Jun Pang

hugo.jonker@uni.lu
SaToSS group, University of Luxembourg
Luxembourgnian elections

Luxembourgnian ballot:

<table>
<thead>
<tr>
<th></th>
<th>ADR</th>
<th></th>
<th></th>
<th>KPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>J. Henckes</td>
<td></td>
<td></td>
<td>P. Back</td>
</tr>
<tr>
<td>1-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-21</td>
<td>F. Zeutzius</td>
<td></td>
<td></td>
<td>M. Tani</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Luxembourgian elections

**Luxembourgian ballot:**

<table>
<thead>
<tr>
<th></th>
<th>ADR</th>
<th></th>
<th></th>
<th>KPL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>J. Henckes</td>
<td>■</td>
<td>■</td>
<td>...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-21</td>
<td>F. Zeutzius</td>
<td>□</td>
<td>□</td>
<td>...</td>
</tr>
</tbody>
</table>
Luxembourguian elections

Luxembourguian ballot:

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ADR</td>
<td>...</td>
<td>...</td>
<td>7</td>
</tr>
<tr>
<td>1-1</td>
<td>J. Henckes</td>
<td></td>
<td></td>
<td>7-1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-21</td>
<td>F. Zeutzius</td>
<td></td>
<td></td>
<td>7-21</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ways to complete this ballot:

\[
\binom{292}{19} = 314,269,098,408,967,151,724,980,483,800
\]
Privacy is more than “for whom you voted”.

Privacy depends on all knowledge you have.
helpful voters
- Privacy is more than “for whom you voted”.
- Privacy depends on all knowledge you have.
- Subjects may seek to reduce/renounce privacy.
- Quantify privacy.
- Taking conspiring voters into account.
- Based on the intruder’s knowledge.
choice group $c_{g,v}$:
contains all candidates, that a voter $v$ might have chosen.
**quantifying privacy**

**choice group** $cg_v$:
contains all candidates, that a voter $v$ might have chosen.

Example:
$C = \{Vike - Freiberga, Balkenende, Juncker\}$.

- results: Balkenende 0 votes
  \[ \forall v \in V : \text{Balkenende} \notin cg_v(\mathcal{V}S). \]

- $v$ voted for a man
  \[ cg_v(\mathcal{V}S) \subseteq \{\text{Balkenende, Juncker}\}. \]
Extra info: what the intruder doesn’t know.

The intruder sees communications.

So: initial/final knowledge, untappable channels.
Indistinguishability:
a list of events $t$ is indistinguishable from a list $t'$ if “the intruder cannot distinguish them”.
in a nutshell

- voters, authorities $\rightarrow$ communicating processes
- processes communicate terms
- communication events $\rightarrow$ trace
- trace $\overset{intruder}{\rightarrow}$ privacy
Syntax

- voters $\mathcal{V}$, candidates $\mathcal{C}$
- choice function $\gamma: \mathcal{V} \rightarrow \mathcal{C}$

Terms:

$$\varphi ::= \text{var} \in \text{Vars} \mid c \in \mathcal{C} \mid n \in \text{Nonces} \mid k \mid (\varphi_1, \varphi_2) \mid \{\varphi\}_k.$$
When can the intruder distinguish $Tr(\mathcal{VS}^\gamma_1)$ from $Tr(\mathcal{VS}^\gamma_2)$?

When he cannot **reinterpret** $t$ as $t'$. 
Definition 1 (reinterpretation (adapted from GHPR05))

Let $\rho$ be a permutation on the set of terms $\text{Terms}$ and let $K_I$ be a knowledge set. The map $\rho$ is a **semi-reinterpretation under $K_I$** if it satisfies the following.

\[
\begin{align*}
\rho(p) &= p, \text{ for } p \in \mathcal{C} \cup \text{Keys} \\
\rho((\varphi_1, \varphi_2)) &= (\rho(\varphi_1), \rho(\varphi_2)) \\
\rho(\{\varphi\}_k) &= \{\rho(\varphi)\}_k, \text{ if } K_I \vdash \varphi, k \lor K_I \vdash \{\varphi\}_k, k^{-1}
\end{align*}
\]

Map $\rho$ is a **reinterpretation under $K_I$** iff it is a semi-reinterpretation and its inverse $\rho^{-1}$ is a semi-reinterpretation under $\rho(K_I)$. 

Traces $t, t'$ are indistinguishable for the intruder, notation $t \sim t'$ iff there exists a reinterpretation $\rho$ such that

$$obstr(t') = \rho(obstr(t)) \land \overline{K_I^t} = \rho(\overline{K_I^{t'}}).$$
Given voting system \( \mathcal{VS} \), choice functions \( \gamma_1, \gamma_2 \) are indistinguishable to the intruder, notation \( \gamma_1 \sim_{\mathcal{VS}} \gamma_2 \) iff

\[
\forall t \in Tr(\mathcal{VS}^{\gamma_1}) \colon \exists t' \in Tr(\mathcal{VS}^{\gamma_2}) : t \sim t' \quad \land \\
\forall t \in Tr(\mathcal{VS}^{\gamma_2}) \colon \exists t' \in Tr(\mathcal{VS}^{\gamma_1}) : t \sim t'
\]
Possible choices for $\mathcal{VS}, \gamma$:

$$cg(\mathcal{VS}, \gamma) = \{ \gamma' \mid \gamma \simeq_{\mathcal{VS}} \gamma' \}.$$  

Possible choices for $\nu$ then:

$$cg_{\nu}(\mathcal{VS}, \gamma) = \{ \gamma'(\nu) \mid \gamma' \in cg(\mathcal{VS}, \gamma) \}.$$
goals

✓ privacy > “for whom you voted”

✓ depends on knowledge

? conspiring voter
goals

✓ privacy > “for whom you voted”
✓ depends on knowledge
?

conspiring voter

\[ \text{goals} \]

\[ \checkmark \text{privacy} > \text{“for whom you voted”} \]
\[ \checkmark \text{depends on knowledge} \]

? conspiring voter

\[
\begin{align*}
1. \text{classic-rf} & \quad \text{vote-priv} \\
2. \text{start-rf} & \quad \text{vote-priv}
\end{align*}
\]

(i)

\[
\begin{align*}
c. \text{rf-relay} & \quad \text{vote-priv} \\
a. \text{rf-share} & \quad \text{vote-priv} \\
b. \text{rf-witness} & \quad \text{vote-priv}
\end{align*}
\]

(ii)
conspiracy-resistance

classical notion:

$$\forall v, \gamma: \left| cg^1_v(\mathcal{VS}, \gamma) \right| > 1.$$ 

New: conspiracy-dependent notion:

\textbf{\$\mathcal{VS}\$ is conspiracy-resistant for conspiring behaviour} $i \in \{1, 2, a, b, c\}$ iff

$$\forall v \in \mathcal{V}, \gamma \in \mathcal{V} \rightarrow \mathcal{C}: cg^i_v(\mathcal{VS}, \gamma) = cg_v(\mathcal{VS}, \gamma).$$
concluding

- we can quantify privacy in voting
- possibility to detect new attacks
- choice group aids reasoning about privacy

Future work:

- conspiring authorities
- defense strategies
- automated verification
- extend with probabilism (election result)
Thank you for your attention.

Questions?