Quantifying voter-controlled privacy

Hugo Jonker

in collaboration with Sjouke Mauw and Jun Pang

hugo.jonker@uni.lu

SaToSS group, University of Luxembourg

Dutch elections

Dutch ballot:

1. CDA			...	18. SGP		
1-1.	X	☐	...	18-1.	X'	☐
	⋮		⋮		⋮	
1-13.	Y	☐		18-13.	Y'	☐
	⋮		⋮			
1-45.	Z	☐	...			

Parties: CDA, VVD, PvdA, SP, Groenlinks, Wilders, LPF, Christenunie, SGP, ...

lesson

- Privacy is more than “for whom you voted”.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	...	7. KPL
1-1. J. Henckes ☐ ☐	...	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	...	7-21. M. Tani ☐ ☐

Luxembourgian elections

Luxembourgian ballot:

1. ADR	···	7. KPL
1-1. J. Henckes ☐ ☐	···	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	···	7-21. M. Tani ☐ ☐

- voter marks 21 boxes.

Luxembourgian elections

Luxembourgian ballot:

1.	ADR			···		7.	KPL	
1-1.	J. Henckes	■	■	···		7-1.	P. Back	☐ ☐
⋮				⋮		⋮		
1-21.	F. Zeutzius	☐	☐	···		7-21.	M. Tani	☐ ☐

- voter marks 21 boxes.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	⋯	7. KPL
1-1. J. Henckes ■ ■	⋯	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	⋯	7-21. M. Tani ☐ ☐

- voter marks 21 boxes.
- pick 2. That leaves $\binom{292}{19} =$ 314,269,098,408,967,151,724,980,483,800 ways to fill in ballot.

lesson

- Privacy is more than “for whom you voted”.
- Privacy depends on all knowledge you have.

helpful voters

lesson

- Privacy is more than “for whom you voted”.
- Privacy depends on all knowledge you have.
- Subjects may seek to reduce/renounce privacy.

approach

- Quantify privacy.
- Taking conspiring voters into account.
- Based on the intruder's knowledge.

overview

- Privacy is tricky (examples)
- Understanding privacy
- Define privacy
- Use definitions
- What did we miss?

Dutch elections

Dutch ballot:

1. CDA			...	18. SGP		
1-1.	X	☐	...	18-1.	X'	☐
	⋮		⋮		⋮	
1-13.	Y	☐		18-13.	Y'	☐
	⋮		⋮			
1-45.	Z	☐	...			

Parties: CDA, VVD, PvdA, SP, Groenlinks, Wilders, LPF, Christenunie, SGP, ...

lesson

- Privacy is more than “for whom you voted”.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	⋯	7. KPL
1-1. J. Henckes ☐ ☐	⋯	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	⋯	7-21. M. Tani ☐ ☐

Luxembourgian elections

Luxembourgian ballot:

1. ADR	⋯	7. KPL
1-1. J. Henckes ☐ ☐	⋯	7-1. P. Back ☐ ☐
⋮	⋮	⋮
1-21. F. Zeutzius ☐ ☐	⋯	7-21. M. Tani ☐ ☐

- voter marks 21 boxes.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	⋯	7. KPL
1-1. J. Henckes ■ ■	⋯	7-1. P. Back □ □
⋮	⋮	⋮
1-21. F. Zeutzius □ □	⋯	7-21. M. Tani □ □

- voter marks 21 boxes.

Luxembourgian elections

Luxembourgian ballot:

1. ADR	⋯	7. KPL
1-1. J. Henckes ■ ■	⋯	7-1. P. Back □ □
⋮	⋮	⋮
1-21. F. Zeutzius □ □	⋯	7-21. M. Tani □ □

- voter marks 21 boxes.
- pick 2. That leaves $\binom{292}{19} =$ 314,269,098,408,967,151,724,980,483,800 ways to fill in ballot.

lesson

- Privacy is more than “for whom you voted”.
- Privacy depends on all knowledge you have.

helpful voters

lesson

- Privacy is more than “for whom you voted”.
- Privacy depends on all knowledge you have.
- Subjects may seek to reduce/renounce privacy.

approach

- Quantify privacy.
- Based on the intruder's knowledge.
- Taking conspiring voters into account.

quantifying privacy

choice group:
contains all candidates, that a voter might have chosen.

quantifying privacy

choice group:
contains all candidates, that a voter might have chosen.

Example:
$\mathcal{C} = \{Merkel, Berlusconi, Sarkozy\}$.

- results: Berlusconi 0 votes
  $\Longrightarrow \forall v \in \mathcal{V}\colon cg_v(\mathcal{VS}) = \{Sarkozy, Merkel\}$.
- v voted for a man
  $\Longrightarrow cg_v(\mathcal{VS}) = \{Berlusconi, Sarkozy\}$.

intruder knowledge

Indistinguishability:
a series of events t is indistinguishable from a series t' if
“the intruder cannot distinguish them”.

intruder knowledge

Indistinguishability:
a series of events t is indistinguishable from a series t' if
"the intruder cannot distinguish them".

Example:
$\{c\}_k \sim \{c'\}_k$, if the intruder does not know k.
$\{n\}_k \sim \{n'\}_k$, always.

conspiring voters

- Only advantage: what the intruder doesn't know.
- The intruder sees all communications.
- So: initial knowledge, final knowledge, untappable channels.

choice function

choice function: a function $\gamma : \mathcal{V} \to \mathcal{C}$.

choice function

choice function: a function $\gamma : \mathcal{V} \to \mathcal{C}$.

Example:

$\gamma_1(Melanie) = Merkel.$

$\gamma_2(Melanie) = Sarkozy.$

modelling privacy

When can the intruder distinguish $Tr(\mathcal{VS}^{\gamma_1})$ from $Tr(\mathcal{VS}^{\gamma_2})$?

When he can reinterpret t as t'.

reinterpretation

Definition 1 (reinterpretation (GHPR05)) *Let ρ be a permutation on the set of terms $Terms$ and let K_I be a knowledge set. The map ρ is a semi-reinterpretation under K_I if it satisfies the following.*

$$\begin{aligned} \rho(p) &= p, \text{ for } p \in \mathcal{C} \cup Nonces \cup Keys \\ \rho((\varphi_1, \varphi_2)) &= (\rho(\varphi_1), \rho(\varphi_2)) \\ \rho(\{\varphi\}_k) &= \{\rho(\varphi)\}_k, \text{ if } K_I \vdash \varphi, k \vee K_I \vdash \{\varphi\}_k, k^{-1} \end{aligned}$$

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

indistinguishability

Definition 2 (trace indistinguishability) *Traces t, t' are indistinguishable for the intruder, notation $t \sim t'$ iff there exists a reinterpretation ρ such that*

$$obstr(t') = \rho(obstr(t)) \ \wedge \ \overline{K_I^t} = \rho(\overline{K_I^{t'}}).$$

Definition 3 (choice indistinguishability) *Given voting system $\mathcal{VS}$, choice functions γ_1, γ_2 are indistinguishable to the intruder, notation $\gamma_1 \simeq_{\mathcal{VS}} \gamma_2$ iff*

$$\forall t \in Tr(\mathcal{VS}^{\gamma_1}) : \exists t' \in Tr(\mathcal{VS}^{\gamma_2}) : t \sim t' \quad \wedge$$
$$\forall t \in Tr(\mathcal{VS}^{\gamma_2}) : \exists t' \in Tr(\mathcal{VS}^{\gamma_1}) : t \sim t'$$

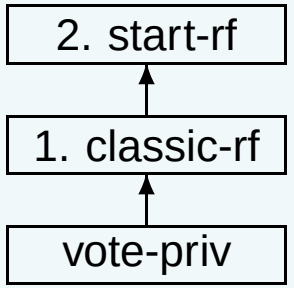
Definition 4 (choice group) *The choice group for a voting system $\mathcal{VS}$ and a choice function γ is given by*

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

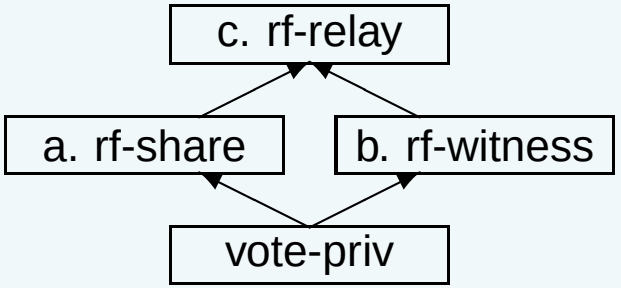
The choice group for a particular voter v, i.e. the set of candidates indistinguishable from v's chosen candidate, is given by

$$cg_v(\mathcal{VS}, \gamma) = \{\gamma'(v) \mid \gamma' \in cg(\mathcal{VS}, \gamma)\ \}.$$

conspiracy

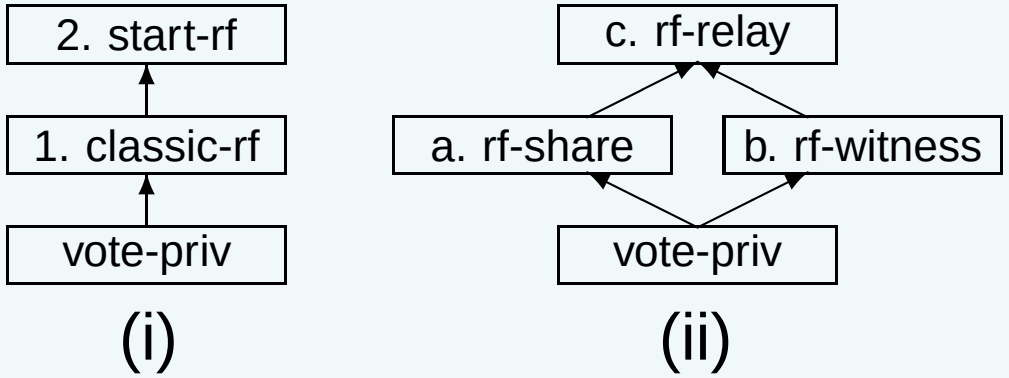


(i)



(ii)

conspiracy



- transform processes using Θ_i, where $i \in \{1, 2, a, b, c\}$.
- transform events using θ_i
- coercion-resistance i:
  $\forall v, \gamma : cg_v^i(\mathcal{VS}, \gamma) = cg_v(\Theta_i(v, \mathcal{VS}), \gamma)$

event transformation

- $\theta_a(v, ev) =$

$$\begin{cases} ur(ag, v, \varphi) \ . \ is(v, \varphi) & \text{if } ev = ur(ag, v, \varphi) \\ ev & \text{otherwise} \end{cases}$$

event transformation

- $\theta_a(v, ev) =$

$$\begin{cases} ur(ag, v, \varphi) \ . \ is(v, \varphi) & \text{if } ev = ur(ag, v, \varphi) \\ ev & \text{otherwise} \end{cases}$$

- $\theta_b(v, ev) =$

$$\begin{cases} is(v, \mathrm{vars}(v, \varphi)) \ . \ ir(v, \mathrm{vars}(v, \varphi')) \ . \ us(v, ag, \varphi') \\ \qquad \text{if } ev = us(v, ag, \varphi), \text{ for } \varphi' = \mathrm{freshvars}(v, \varphi) \\ ev \qquad \text{otherwise} \end{cases}$$

event transformation

- $\theta_a(v, ev) =$

$$\begin{cases} ur(ag, v, \varphi) \ . \ is(v, \varphi) & \text{if } ev = ur(ag, v, \varphi) \\ ev & \text{otherwise} \end{cases}$$

- $\theta_b(v, ev) =$

$$\begin{cases} is(v, \mathrm{vars}(v, \varphi)) \ . \ ir(v, \mathrm{vars}(v, \varphi')) \ . \ us(v, ag, \varphi') \\ \qquad \text{if } ev = us(v, ag, \varphi), \text{ for } \varphi' = \mathrm{freshvars}(v, \varphi) \\ ev \qquad \text{otherwise} \end{cases}$$

- $\theta_c(v, ev) = \theta_b(v, \theta_a(v, ev))$

process transformation

$$\Theta_2(v, P) = is(knw_v).P$$

$$\Theta_i(v, P) =$$

$$\begin{cases} \delta & \text{if } i \neq 1 \wedge P = \delta \\ is(v, knw_v).\delta & \text{if } i = 1 \wedge P = \delta \\ \\ \theta_i(v, ev).\Theta_i(v, P) & \text{if } P = ev.P \\ \Theta_i(v, P_1) + \Theta_i(v, P_2) & \text{if } P = P_1 + P_2 \\ \Theta_i(v, P_1) \lhd \varphi_1 = \varphi_2 \rhd \Theta_i(v, P_2) & \text{if } P = P_1 \lhd \varphi_1 = \varphi_2 \rhd \\ & \text{for } \varphi_1, \varphi_2 \in Terms \\ \\ \theta_i(v, ev).Y(\varphi_1, \ldots, \varphi_n), & \text{for fresh } Y(\mathsf{var}_1, \ldots, \mathsf{var}_n) = \Theta_i(\\ & \text{if } P = X(\varphi_1, \ldots, \varphi_n) \wedge X(\mathsf{var}_1, \ldots, \mathsf{var}_n) \end{cases}$$

conspiracy-resistance

classical notion:

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

Our definition:

Definition 5 (conspiracy-resistance) *We call voting system $\mathcal{VS}$ conspiracy-resistant for conspiring behaviour $i \in \{1, 2, a, b, c\}$ iff*

$$\forall v \in \mathcal{V}, \gamma \in \mathcal{V} \to \mathcal{C} : cg_v^i(\mathcal{VS}, \gamma) = cg_v(\mathcal{VS}, \gamma).$$

concluding

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

concluding

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

Future work:

- consider transformations of authorities
- defense strategies
- automated application
- extend with probabilism (election result)

final slide

Thank you for your attention.

Questions?