Electronic elections, winter 2007

MICHAEL NÜSKEN

6. Exercise sheet
Bring your solutions Wednesday, 6 February 2008, 11^{30}, to the course.

Exercise 6.1 (Further properties). (7 points)

For our selected schemes we have considered the properties

- accuracy (scheme works as desired),
- eligibility (only voters can vote and only once),
- anonymity/privacy,
- individual verifiability,
- global verifiability,
- robustness.

Consider

- dispute-free,
- long-term privacy,
- fairness (no partial tallies possible),
- receipt-free,
- incoercible,
- scalable,
- practical.

For each property identify one mechanism that is used to ensure it in one of our selected election schemes. 7

Exercise 6.2 (Implementation). (0 points)

Suppose you have to implement an electronic election scheme. (Pick one of our selected schemes when appropriate.) Which major difficulties do you expect?

Exercise 6.3 (Your choice). (0 points)

(i) Which scheme would you choose as a basis?

(ii) Which additional features would you require?