MISG 2016 Graduate Workshop

e-vota

J. W. Sanders

AIMS South Africa & SUN

The problem

Election by vote: from clubs to nations.
Many *voting protocols* are in common use and their features are well known (and perhaps surprising at first).

However all voting *systems* share important properties, including:

- voter authentication
- confidentiality of vote
- accountability of result.

Can we design a distributed voting system?

Characteristics of this problem

What characterises a typical MISG problem?

How this problem is similar; and different.

What is required: a *design*; its correctness and efficiency.

What is not required: a *program*; testing it in various cases.

The maths is *pure*, *discrete* and perhaps unfamiliar.

Specification

Assume the voting protocol is given by a 'black box' procedure.
Concentrate on the rest of the system.

Our system is *specified* by its

- functionality
  (reflects the voting protocol)
- extra features
  (authentication, confidentiality, anonymity,
  + security?, + robustness?)

Design techniques

- Describing a distributed design.
  Modularity.
  Information flow by shared variables or message passing.
- Reasoning about distributed behaviour.
  Each module must be autonomous.
  Invariant properties.
- Public key encryption.
  Secure communication. Digital signatures.
- Mathematical notation.
  Z formalism.

Example: the voting protocol

$$Voters$$
$$Candidates$$

$$\begin{aligned} Rankings &:= perms(Candidates) \\ Votes &:= Voters \to Rankings \\ VProtocol &:= Votes \to Rankings \end{aligned}$$

Concerns

1. Modelling: how to abstract (what is 'observable'?).
2. Does the distributed e-format offer *new* possibilities for a voting system?
3. Correctness?
4. Efficiency?

References

- *Survey on electronic voting schemes*, Laure Fouard, Mathilde Duclos and Pascal Lafourcade. 65 pages.
- *Design and analysis of a practical e-voting protocol*, Marián Novotný. 14 pages.
- *Analysis of an Electronic Voting System*, Tadayoshi Kohno, Adam Stubblefield, Aviel Rubin and Dan Wallach. 23 pages.