FACULTY OF SCIENCE

Bart Jacobs

Practical Issues in Electronic Voting

Radboud University Nijmegen

“It’s not the people who vote that count.

It’s the people who count the votes.”

Attributed to Joseph Stalin

Contents

I. Background and Plan

Who is this guy?

- Professor in software security & correctness, at Nijmegen & Eindhoven, in NL.
- Early work in logic, type theory, category theory, coalgebra
  (most cited papers still in this area)
- Later work on semantics and verification for Java, esp. on smart cards
- Gradual shift to ***Security***

Security work

- Distinctly non-theoretical focus
  (with some exceptions)
- Involvement in e-government / identity managment, like biometric passports, voting, chipcards, privacy
- Advisory role to government, both formally and informally
- Regular presence in societal debates/media
- Genuine interest in societal aspects of computer security.

Most recently

- Severe vulnerabilities found at Nijmegen in Mifare Classic chipcard (one billion sold)
- To appear at Esorics'08 (oct; Malaga)
- Producer NXP tried to stop publication via court case — but failed.
- Also here "hands on" approach: attacks have been implemented & demonstrated
  (e.g. in London Tube)

Disclaimer: no crypto, but software person

Own involvement in voting in NL

- For internet voting in EU-'04: advisor & contractor for vote counting software
- Auditor for regional waterboard elections (RIES, '04) & independent counter ('04, '06)
- Papers & lectures about this
- Member of government committee
  (named after chairman/ex-minister *Korthals Altes*)
- Chairman of technical expert group
- Supervision of two PhD theses, on *trust in technology* (2008) and *vote counting* (20??).

Main developments in NL

- Early adoption of voting machines (early 90s)
  (useage 97% in 2006; no controversy until then)
- Various field experiments with internet voting
  (regionally and nationally, for expats)
- Strong campaign by action group against e-voting in 2007
- Complete return to paper voting in 2008.

NL is early adopter & early abolisher

Why NL relevant?

- E-voting issues are universal
- Trust in technology underlying problem
- Societal & political debates (on transparancy or voting as pilar of democracy) recognisable
- Inside story always bound to particular situation
- Hopefully instructive (& entertaining)

II. Requirements and Techniques

Requirements / safeguards

- transparancy
- verifiability
- integrity
- eligibility
- unicity
- vote secrecy
- vote freedom
- accessibility

- Not all can hold absolutely: balance needed
- Poll station gives most guarantees
- . . . but may require exceptions for severely disabled and/or expatriats
  (like voting by proxy, or by internet)

Poll station characteristics

- Separate space, free from political messages
- Multi-person, independent supervision
- Simple procedure for checking eligibility & unicity (marking names on a list)
- Personal, isolated voting boots
- Transparant, one-way storage (protecting confidentiality and integrity)
- Counting done locally (or after limted accumulation), in public, in principle.

Poll station analysis

- Check 8 requirements . . .
  (Accessiblity ☹)
- Distributed & low-tech character gives protection
- Fraud more likely “higher up” the vote processing chain
- Manual counting is error-prone / time-consuming / boring (after a long day)
- Possible confidentiality threats from small cameras

Voting machines I, in NL

Nedap

Sdu

Voting machines II

- Introduced in NL since early 90s; early 2006 used almost everywhere
- Votes stored in digital memory; internal mechanics is secret
- US terminology: “Direct-Recording Electronic voting machine” (DRE)
- Evaluation is required, done by independent organisation (TNO); reports are secret (and also partly missing)
- No meaningful recounts possible.

The main concern . . .

"Let's see how my vote is counted" ©Automatisering Gids 2003.

Voting machines III

Advantages

- automatic processing of results: efficient and fast (especially for local organisers: municipalities)
- vote expression is unambiguous

Disadvantages

- Voter cannot verify that the vote is registered correctly
- Recount only possible on already processed votes

Back then . . .

- The introduction of these voting machines in NL since early 90s was uncontroversial
- Optimisation (not big change) of procedures
- Openness (of software) was not an issue
- Much trust in technology (and in the state!)
- By now we know better about the unreliability and vulnerability of software and networks
- International controversy since 2004 (esp. relevant in IRL) without much effect in NL, . . . *at first* . . .

Adding a paper trail?

- Popular proposal: let machine print (behind glass) the voter's choice
- Should protect against software errors
- In experiments: difference between "electronic" and "paper" vote, eg. through mechanical problems
- Not clear what to do then . . .
- Often, electronic outcome is chosen!
- Simple idea, but involves difficult dilemma.

Crypto based approaches

- ***Basic techniques***
  - Mix-nets
  - Homomorphic encryption
  - Blind signatures
- ***In practice simpler techniques***
  - PKI-based (Estonia)
  - Randomised ballots
  - Hashes (RIES in NL, see later)

Mix networks

- Introduced by Chaum, to achieve untraceability via different proxy servers
- Uses multiple encryptions, for successive servers that mix (the order of) messages:

$$\text{PubEnc}_{K_{S1}}(\text{PubEnc}_{K_{S2}}(\text{PubEnc}_{K_{S3}}(C)))$$

- Servers must be trusted not to log connections or to drop messages
- Used nowadays for anonymous mailing / surfing ("onion routing", as in Tor)

Homomorphic Encryption I

- Illustration for El Gamal, with generator g, secret key x, public key $h = g^x$.
- $\text{PubEnc}_h(m) = (g^r, h^r \cdot m)$, with r random
- Decryption of (a, b) is $\frac{b}{a^x}$.
- Then:

$$\begin{aligned}&\text{PubEnc}_h(m_1) \cdot \text{PubEnc}_h(m_2)\\ =\ &(g^{r_1+r_2}, h^{r_1+r_2} \cdot m_1 \cdot m_2).\end{aligned}$$

Homomorphic Encryption II

- Fix public G; votes $v \in \{-1, 1\}$ (as in [CGS97])
- Encrypted vote is $(g^r, h^r \cdot G^v)$
- For tallying, multiply encrypted results:
  $(g^{r_1}, h^{r_1} \cdot G^{v_1}) \cdot (g^{r_2}, h^{r_2} \cdot G^{v_2}) = (g^{r_1+r_2}, h^{r_1+r_2} \cdot G^{v_1+v_2})$
- After decryption multiplications with G or G^{-1} yields result
- Additional protection needed:
  - encrypted vote must by signed by voter
  - vote $\in \{-1, 1\}$ via zero knowledge proof
  - secret sharing against early decryption

Blind signatures [Chaum]

- Let (N, e) public RSA key, with secret (N, d), so that $\text{PubEnc}_{(N,e)}(m) = m^e \bmod N$ and $\text{Sign}_{(N,d)}(m) = m^d \bmod N$
- Blinding: ask signature on $m \cdot r^e$ and get signature on m.
- After eligibility check, get anonymous (blindly signed) voting ticket
- Such tickets can be sold . . .

PKI-based envelopes

- Used in Estonia, where citizens have identity smart card with PKI (and readers)
- Vote for candidate C is sent in by voter i as:

$$\text{Sign}_{K_i}(\text{PubEnc}_{K_{auth}}(C))$$

- Test in 2005 (10K participants), actual use in 2007 for parliament (30K = 6% participants)
- 4 days of e-voting; 1 day of paper voting
- Multiple-vote option, against family fraud.
- Pragmatic, non-ideological approach.

Randomised ballots I

- Prêt-à-voter by P. Ryan, with 2-part ballots:

Idefix	
Asterix	X
Obelix	
	3874670

encodes order of candidates

- After separation the RHS is scanned and a signed copy is returned
- All copies are published, together with key, for counting

Randomised ballots II

- Various other options possible
- E.g. in internet voting:
  - number candidates, differently for each voter
  - vote via entering numbers
  - protects against viruses.
  - used in NL in '04 for first internet voting.

III. Controversy in NL

The trigger

- March 2006: municipal elections in NL
- City of Amsterdam uses voting machines (from Sdu) for the first time
- One citizen was shocked: ***Rop Gonggrijp***
- . . . and started a foundation:

wijvertrouwenstem computersniet.nl

"*wedonottrustvotingcomputers.nl*"

Foundation's main points

- Not "voting machines" but "voting computers"
- Voting computers (Nedap & Sdu) are not protected against manipulation—like eg. game computers are
- Voting results are not verifiable
- Paper copy of each vote required.

Foundation's approach

- Set up very informative webpage
- Exploit *freedom of information legislation* and put all results on the web
- Start effective media campaign & newsletter
- Gather knowledgeable volunteers
- Take legal actions against every government move.

BJ: sympathy with goals, but no direct involvement

Foundation's main stunt

- Purchase of two Nedaps:

- Legal, from left-over after municipal merger
- Including all software ("ISS") for running an election.

Nedap deconstruction

- Motorola M68000 processor from 80s
- Two removable memory chips (EPROM) with OS & vote counting software
- Removable flash memory for holding votes
- Software was reverse-engineered, and new software written for:
  - chess playing on Nedap
  - "false" counting

Killer events

- TV program *EenVandaag*, 4/10/'06, showing:
  - Easy manipulation of Nedap software
  - Sloppy storage of 500 Nedaps in Rotterdam
- Tempest: electromagnetic radiation
  - Vote can be read from dozens of meters
  - Tension with vote secrecy requirement
  - Basis for legal action by Foundation.

Foundation's direct impact

- Approval of Sdu's withdrawn before NL parliament elections of nov. '06
  - Nedap tempest within ad hoc limits
  - Paper voting returned to Amsterdam
- Two government committees:
  - **Looking back:** "Hermans", with report *Stemmachines, een verweesd dossier*, 4/07
  - **Looking forward:** "Korthals Altes", with report *Stemmen met vertrouwen*, 9/07. (English version *Voting with Confidence* available)

IV. Two government committees

Looking back committee (Hermans), I

- Voting machine initiatives in 80s came from industry (Nedap, TNO), for higher accuracy
- Requirements for voting machines:
  - only in late 90s
  - no steering by ministry or election council
  - focus on safety, not security/transparancy
  - vote counting software never covered
- Security and reliability concerns (like in IRL) ignored in NL, both nationally and locally

Looking back committee (Hermans), II

- Election council too dependent on (loose cannon) software supplier
- About the ministry
  - lack of technical expertise
  - not in control: too dependent on external (commercial) parties
  - has ignored signals of concern
- TNO wrote requirements & had evaluation monopoly
- Local authorities only want convenience

Official reaction

- Humble acceptance of conclusions
- Shift of “voting” within ministry, to department with more technical expertise
  (from CZW to BPR)
- Immediate redrafting of requirements for voting machines
  - Foundation sees attempt to save Nedaps
- Await “looking forward” report.

Paranoia?

- ***Paper ballots*** are a bad idea because voters leave fingerprints and governments have databases of fingerprints these days and can thus read individual votes
- ***Computer-based*** voting is a bad idea because government (intelligence) services are best at reading tempest signals, and can thus read individual votes

Paranoia!

- Those things don't happen in a civilised country like NL. We should assume a minimal level of trust.
- But NL should set an example, also for countries where such trust is maybe not justified!

Looking forward: who were involved

- FLTR: Barendrecht, Meesters, Korthals Altes (chair), Jacobs, van der Wel
- Active from jan. to sept. 2007.

Looking forward: what was done

- Formulate requirements / safeguards
  (mentioned before)
- Perform threat analysis
  (threat = risk * impact on safequard)
- Decide on basic form (poll station); establish exceptions
- Compare options within poll station
  (tempest is issue on its own, see later)
- Organisational matters
  (mostly ommitted)

Own emphasis here on technical angle

On the far side of being wrong

- Imagine “vote pillar”, eg. in train station, with:
  - Voter recognition via (biometric) passport
  - Vote expression via touch screen
  - Electronic storage of vote
  - Transmission to central office at end
- Sounds cool & convenient . . .
- Two fundamental problems: device may
  - store ***link*** between voter and vote
  - store or count votes ***incorrectly***

Basic idea of committee

- Create separation between phases
  - *identification*
  - *vote expression*
  - *vote storage*

  with individual voter as only connection!
- ***Within*** these phases use ICT as much as you like, but ***not inbetween***.

Implementation: “voteprinter”

- Vote expression via touchscreen
- Device stores nothing, but only prints individual vote in human readable manner
- Voter checks correctness of print:
  - **OK**, then print is deposited in ballot box
  - **NOT OK**, voter may vote again
    (upon repeated errors device is replaced)
- In the end votes are counted automatically
  (using optical character recognition, OCR)

Advantages voteprinter

- Recounts are possible, manually if preferred
- Actual vote casting is physical act (deposit)
- Software faults are detectable, by voters
- After failures, device can be replaced without effect on already cast votes (no internal state)
- Device can present many possible elections: vote anywhere, nationwide
- Voteprinter is flexible, fancy pencil
- Voting proces is centered around the voter

Main disadvantage: tempest risk

- Uncomfortable situation:
  - Expertise secretive (esp. intelligence services)
  - No public, but secret (NATO), norms
  - High demands on environment
  - High cost & evaluation per item
- Pragmatic recommendation:
  - Best effort, affordable technical measures
  - Repressive measures (punishable)

Additional recommendations

- Internet voting:
  - Transparancy, verifiability, freedom & secrecy insufficiently guaranteed
  - Incomparable with internet banking etc.
  - Research dust has not come down yet
  - At this stage advised only for expats
  - Knowledge & experience remains present
- Independent audit of every election:
  - Report within 3 days for election council
  - Within 3 months analysis & recommendations

At the presentation of the report

Responsible junior minister (*staatssecretaris Bijleveld*) decides:

- Remaining (Nedap) voting machines are dropped
- Paper voting returns until new voteprinter is introduced

Cabinet reaction (11/07)

- Safeguards accepted
- Voting in polling stations (anywhere within city)
- Paper should be basis
- Voteprinter + counter appealing, but requires further investigation $\longrightarrow$ new Expert Group
- Internetvoting experiment (for expats), depending on costs (later: “Not in 2009”, also because Parliament demands strict regulation)
- More centralised control, by Ministry (confined role for commercial parties)

Election council:

- Additional safeguard: “independence” wrt. decisions in election process
  (party registration, final outcome)
- Too much control by ministry, too little independent steering.
- Tempest must be handled via preventive measures

New expert group I

- Headed by BJ; active jan-june 2007
- Tempest main issue, studied by company GBS
  - public norm developed
  - prototype “voteprinter” built, with 5 meter norm
  - weight: over 100kg, due to heavy metal case.
- Unpractical, military-style restrictions:
  - regular (re)testing of each device (eg. after bump)
  - no other devices (like GSMs, MP3s) in poll station
  - no nearby parking / empty adjacent rooms
  - special anti-tempest software (moving images)

New expert group II

- Conclusion: Voteprinter is not feasible
- Experiment with counting support:
  - After reading out paper vote, manual entry via touch screen by poll station worker
  - Alternatively: entry via barcode reader, on special ballot (only used for counting)
  - Partial results must be clearly visible on screen.
- Cabinet accepted these recommendations
  - No more e-voting in NL for general elections!

V. RIES Internet voting

Background

- RIES = Rijnland Internet Election System
- By Dutch authority for water management
- Goals
  - Simple, cheap but secure internet voting system
  - Increase election turnout
- System should be at least as secure as their older ordinary mail voting system
- Independent audits by TNO, Cryptomathic, SURFnet, Madison Gurka, RU, TU/e, Fox-IT

RIES actual use

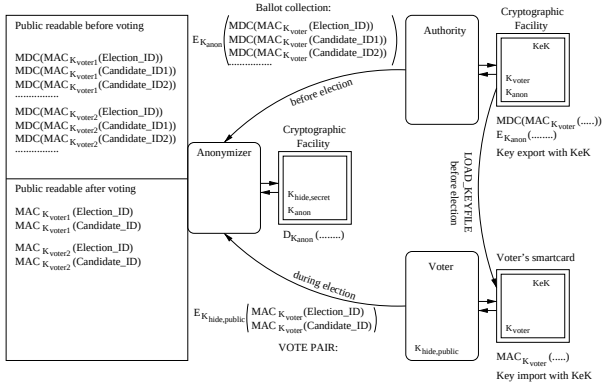
- In 2004/5 for regional waterboard elections (with > 1M possible voters; 100-200K actual)
- 2006: parliament elections, for expats (20K)
- 2008: intended for joint regional waterboards
  - But not deployed due to (action group) opposition and security vulnerabilities
- Among the largest used systems
- Produced valueable experience about how to run medium/large internet elections

The System I

- Designed by Maclaine Pont
- Based upon mastersthesis by Robers (1998)
- Clever but elementary use of hashes
  - MDC: key-less hash
  - MAC: hash with personal secret key
- Transparent
  - Pre-election and post-election tables imply verifiability
- Patented system

The System II

- Robers's smart card based system



The System III

- No smart cards by general public
- Crypto functionality replaced by Java Script
- Key-store functionality replaced by paper ballot, with printed voter key (56bit)
  (key must be entered manually in web form)
- Parallel ordinary mail voting system
- Different agents in each stage: TTPI, SURFnet, Voting office, Voters

Reference table & technical vote

Reference table
pre-election table

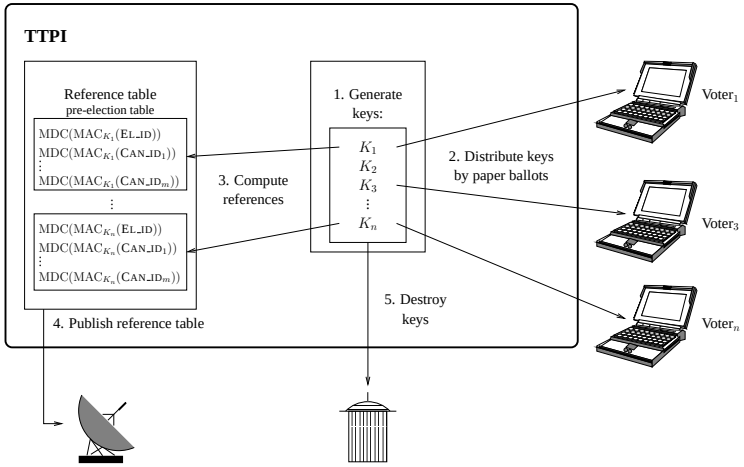
$\mathrm{MDC}(\mathrm{MAC}_{K_1}(\textsc{El\_id}))$
$\mathrm{MDC}(\mathrm{MAC}_{K_1}(\textsc{Can\_id}_1)) \simeq \textsc{Can\_id}_1$
$\mathrm{MDC}(\mathrm{MAC}_{K_1}(\textsc{Can\_id}_m)) \simeq \textsc{Can\_id}_m$

$\mathrm{MDC}(\mathrm{MAC}_{K_n}(\textsc{El\_id}))$
$\mathrm{MDC}(\mathrm{MAC}_{K_n}(\textsc{Can\_id}_1)) \simeq \textsc{Can\_id}_1$
$\mathrm{MDC}(\mathrm{MAC}_{K_n}(\textsc{Can\_id}_m)) \simeq \textsc{Can\_id}_m$

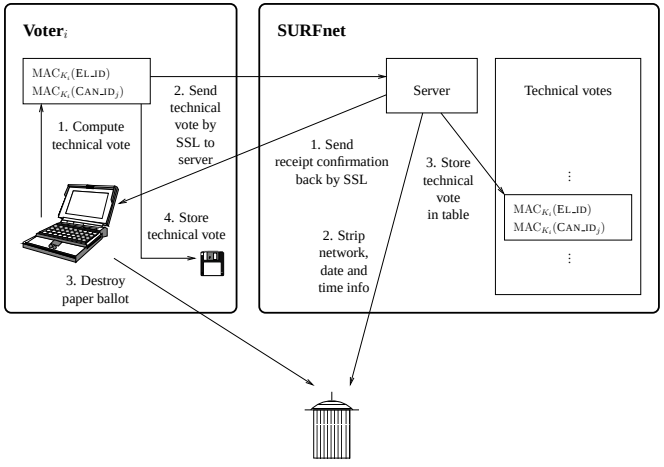
Technical vote

$\mathrm{MAC}_{K_i}(\textsc{El\_id})$
$\mathrm{MAC}_{K_i}(\textsc{Can\_id}_j)$

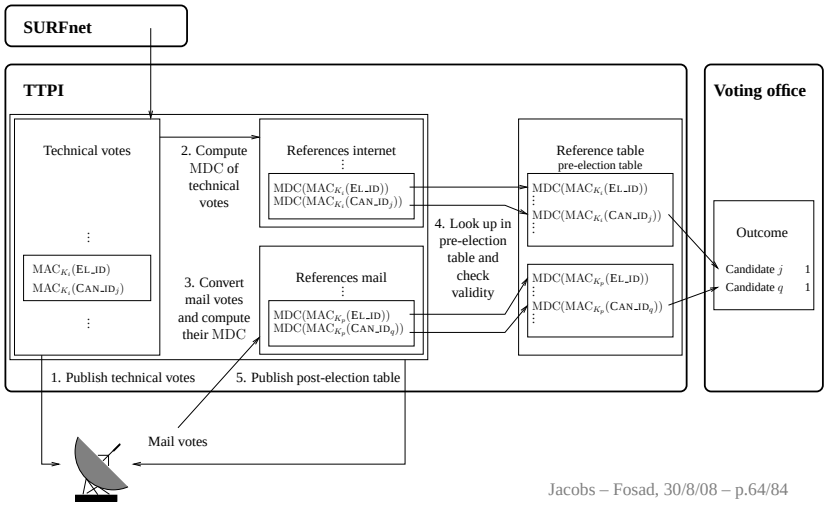
Before the voting



During the voting



After the voting



Verification I

- Voters can check their own vote by
  - Storing technical vote
  - Looking up technical vote in post-election table
  - Collecting hashed technical vote from post-election table
  - Looking up hashed technical vote in pre-election table
  - Checking candidate

Verification II

- Anyone can check total outcome by
  - Collecting all technical votes from post-election table
  - Computing MDC hash on each vote
  - Looking up hashed technical vote in pre-election table
  - Looking up candidate
  - Counting vote for this candidate
- DS group performed these checks and found identical outcomes.

Threats I

- Compromise vote integrity by local virus
  - \+ Modification can be detected
- Compromise privacy by local virus
  - \- Can only be prevented by a good firewall
- Compromise privacy from outside
  - \+ Secret keys do not leave client's machine
  - \+ No correlation between reference tables and specific voter

Threats II

- Compromise ‘public’ secrecy
  - \+ SSL connection prevents this
- Compromise ‘private’ secrecy
  - \- Purely the responsibility of the voter
- Family voting
  - \- Votings outside controlled environments always suffer from this

Threats III

- Compromise identity of vote server
  - \+ Certificates prevent this for `https://www.internetstemmen.nl`
  - \- But not for automatic redirecting `http://www.internetstemmen.nl`; user should go directly to `https` address
- Compromise integrity of vote server
  - \- Can never be prevented completely
  - \+ audit showed that SURFnet made this unlikely

Threats IV

- DDOS attack on vote server
  - \- Can never be prevented completely
  - \- DS audit showed that it is easy to drain disk storage by sending random data
  - \+ Overcapacity of 97% during elections
- Brute force attack
  - \- Personal keys are only 56bits long
  - \- Aug’08: Fox-IT showed: only 20 hours to get such key K_i from reference table entry $\mathrm{MDC}(\mathrm{MAC}_{K_i}(\textsc{El\_id}))$

Threats V

- Insider attacks
  - \- Insider attacks are possible on several places (abuse replacement votes; link votes . . .)
  - \+ Organisational controls
- Buying or selling votes
  - \- Voter can prove his vote, making buying or selling votes possible
  - \+ This situation is not worse than with the mail voting system

What went wrong?

- Fundamental design flaw: organisers can (in principle) vote on behalf of everyone
- Many organisational controls needed
- June'08: open source release showed vulnerabilities (like SQL injection, by Gonggrijp)
- Brute force vulnerability should have been noticed earlier (short key length is compromise)
- July'08: ministry decides not to allow RIES!

VI. Trust and technology

(after PhD Pieters)

Trust at stake

- It is essential for democracies that people trust the outcomes of elections
- Is opposition to new (electronic) forms of voting:
  - conservative, techno-fobic, luddite action?
  - rational, scientific attitude?
- Why is it so difficult to accept ICT-risks in voting (and less so in e.g. aviation software)?
- Focus here on security, not on safety

On trust, in general

- Common distinction:
  - **Rational trust**: based on risk evaluation and possible alternatives
  - **Blind trust**: no options available, risks unknown

  (Luhmann "confidence", to reduce social complexity)
- Security experts replace confidence by trust
- (Rational) trust does not involve objective, actual security
- Also security depends on perspective / context / formalisations / attacker model / . . .

Trust in voting systems

- Introduction of new (voting) techniques undermines confidence and requires trust
- Saying: “this voting system is secure” (or: “can be trusted”) is problematic
- Many (implicit) assumptions need to be made explicit — also for the negation
- Attacker models need to be updated constantly
- Permanent updates of security properties!

Technology & society

- New technologies (like GSM) do not just solve a (communication) problem
- They have profound social influence
- What is the influence of online voting?
- It will change our concept of democracy
  (and of autonomy & separation)
- Eg. direct links between candidate & voting sites: *not appropriate* or *convenient*?
- “Poll station ritual” versus “voting in your underwear” (while chatting)

Big questions about voting

- What are essential requirements, and what do they mean?
  - . . .
  - . . .
- What are the threats?
  - . . .
  - . . .
- Which techniques should be used to counter them?
  - . . .
  - . . .

VII. Seat distributions

(work in progress, with Wichers Schreur)

Background

- Calculating seat distributions in NL:
  - Performed by closed source software
  - never independently investigated
  - New open source software has now been commissioned, after heavy criticism
- Aims of this research
  - Formalise election law in logic (and remove ambiguities)
  - Establish appropriate properties of this formalisation
  - Generate executable code (reference implementation)

Basic properties

- Monotonicity: $\geq$ votes $\Rightarrow$ $\geq$ seats
- Neutrality: treat parties equally
- Completeness: allocate all available seats
- Challenges:
  - Sometimes: draw, resolved by chance
  - Modelled by (distribution) monad
  - Properties must be adapted accordingly

VIII. Conclusions

What we have seen

- E-voting broad, (scientifically) challenging topic: no dust down
- High profile, in media & politics
- NL early adopter . . . but also early abolisher
- Effective grass-root involvement in NL, against “wrong kind of ICT”
  (Which sector is next?)
- Killers: tempest & weak crypto
- Prevailing view: protection of individual autonomy remains necessary.

Thanks for your attention!