Modernizing Electronic Elections
The DemTech Project

Carsten Schürmann

May I introduce myself

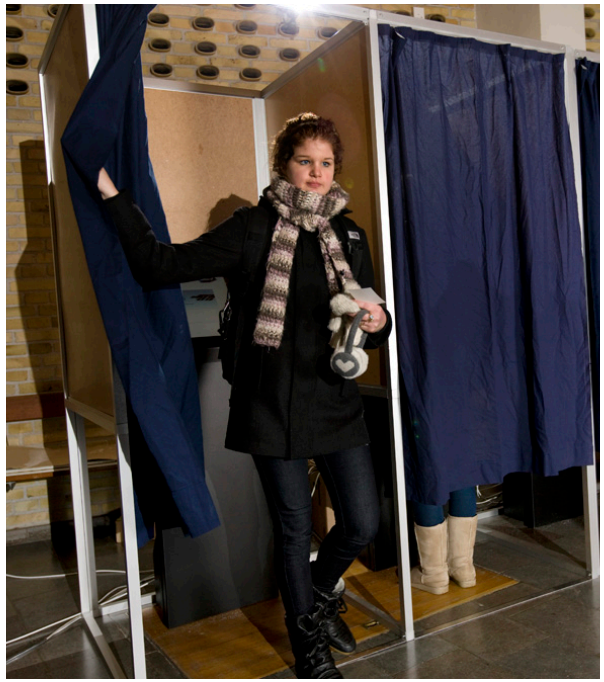
- Diplom Informatik (Karlsruhe, 1993)
- M.S. in Logic and Computation (CMU, 1995)
- PhD. in Pure and Applied Logic (CMU, 2000)
- Assistant Professor (Yale, 2000)
- Associate Professor (ITU, 2005)
- Director of PhD School (ITU, 2008)

Every Vote Matters

Tiny Systematic Vote Manipulation Can Swing Elections

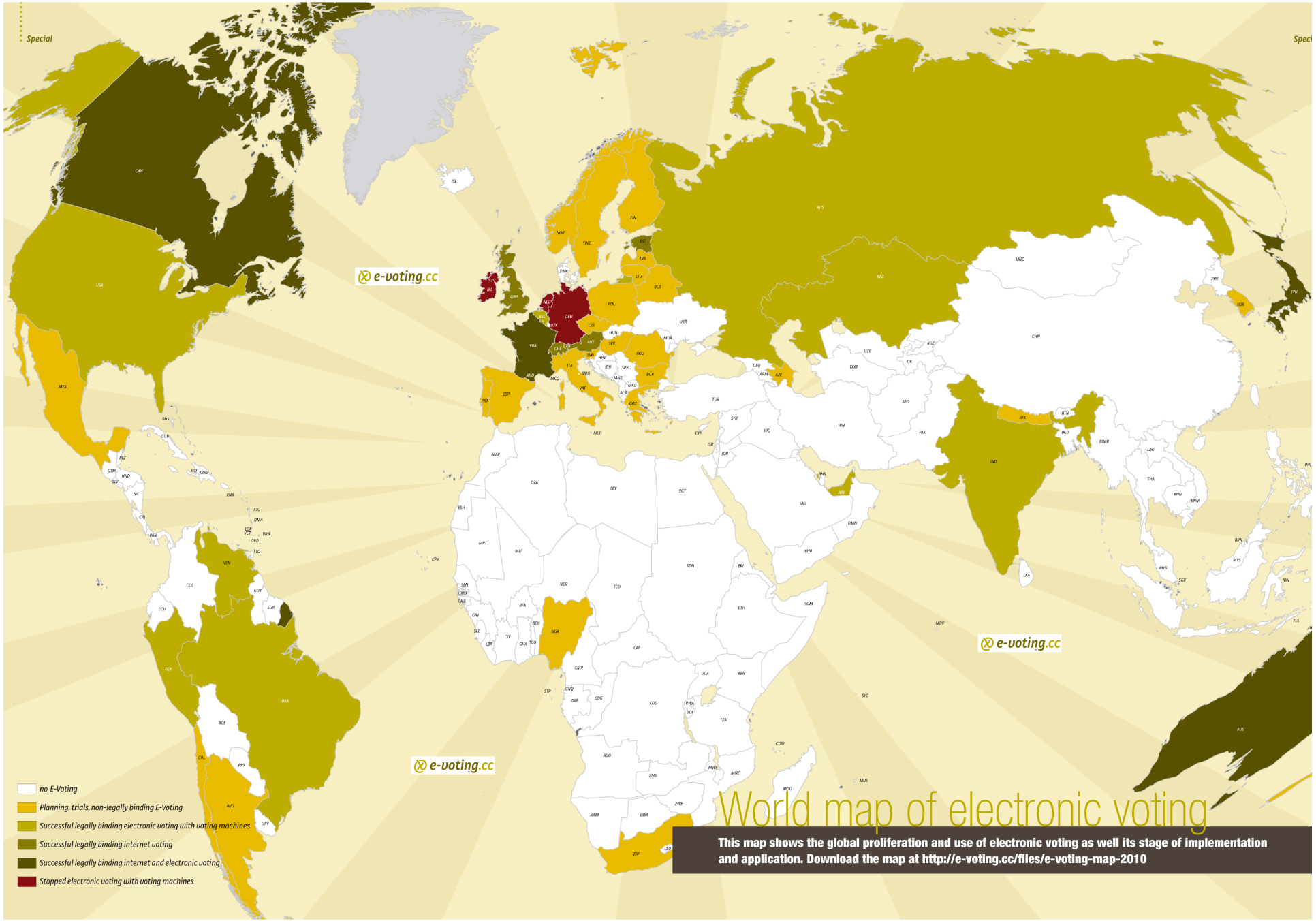
[Di Franco, Petro, Shear, Vladimirov 2001, Yale Technical Report 1285]

Traditional Election



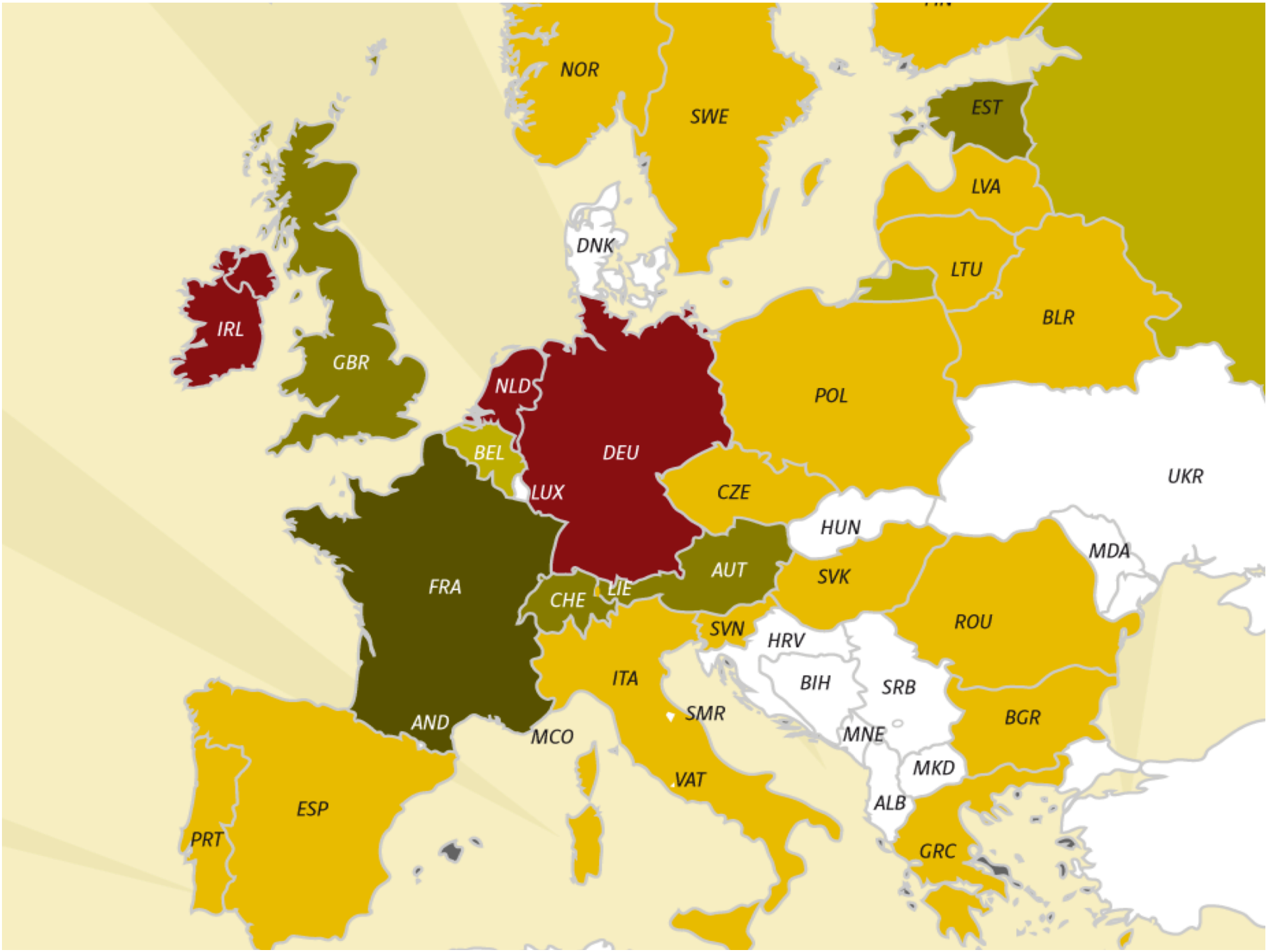
Electronic Election

Internet Election/Remote Voting



World map of electronic voting

This map shows the global proliferation and use of electronic voting as well its stage of implementation and application. Download the map at http://e-voting.cc/files/e-voting-map-2010


NOR
SWE
EST
LVA
LTU
DNK
BLR
IRL
GBR
NLD
POL
BEL
DEU
UKR
LUX
CZE
HUN
MDA
AUT
SVK
FRA
CHE
LIE
ROU
SVN
HRV
ITA
BIH
SRB
SMR
BGR
AND
MCO
MNE
MKD
VAT
ALB
ESP
PRT
GRC

Evolution Danish Democratic Process

[1849] Danish Election Law, show of hands

[1901] Secret ballots

[1915] Women's right to vote

[1920] Vote by letter (for sailors), relaxed '53

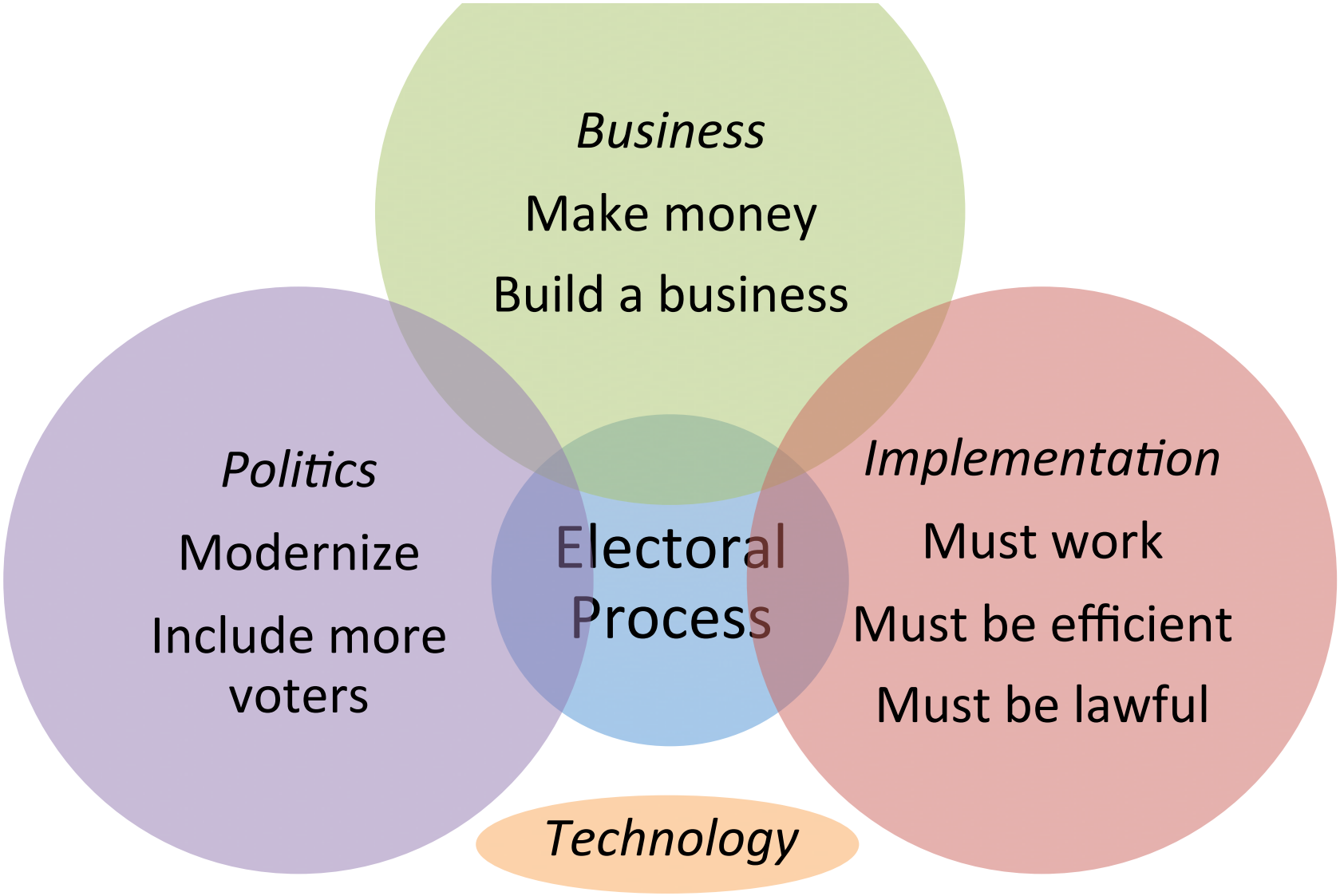
[1953] Folketinget (Parliament)

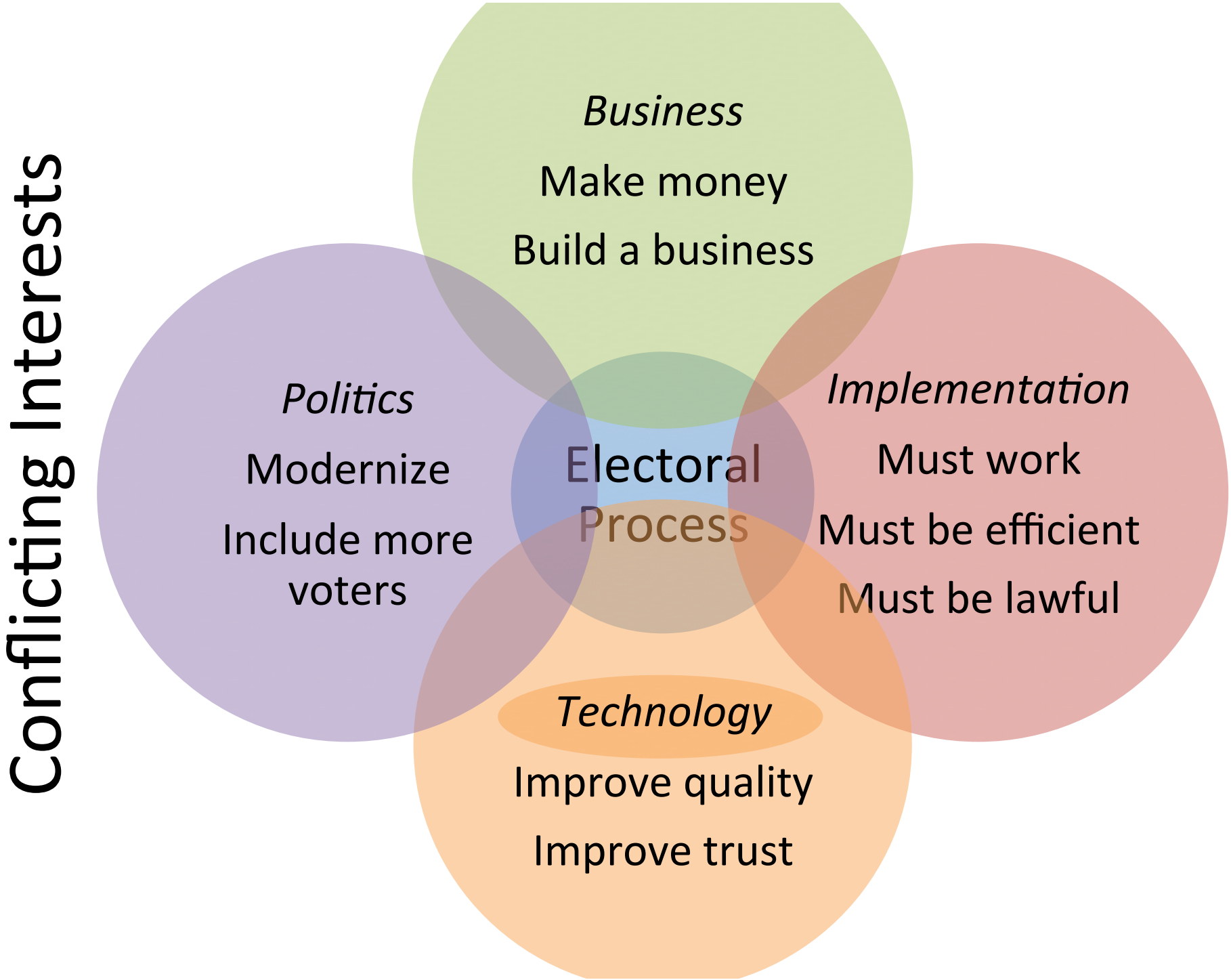
[1970] Danish abroad, right to vote for Folketinget

[1978] Legal voting age: 18

[1984] Rosengreens software for seat assignment

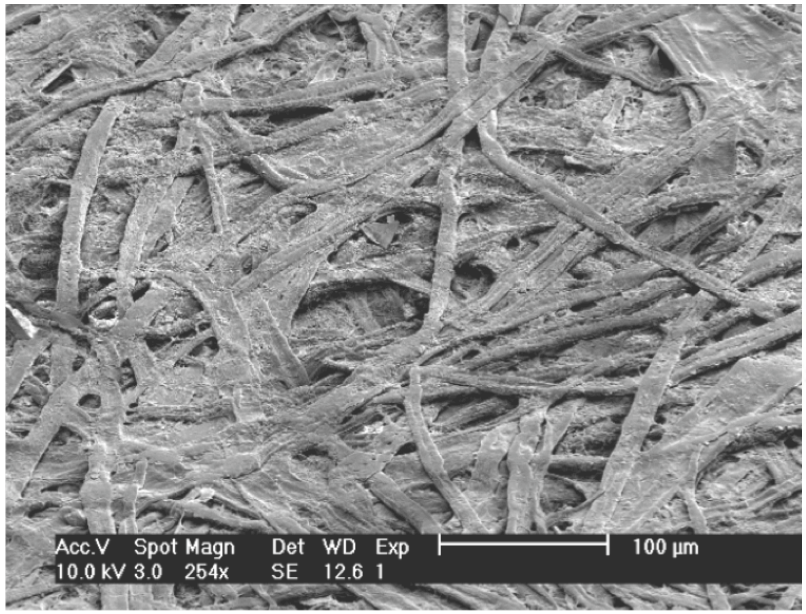
Conflicting Interests




Conflicting Interests
Business
Make money
Build a business
Politics
Modernize
Include more voters
Electoral Process
Implementation
Must work
Must be efficient
Must be lawful
Technology
Improve quality
Improve trust

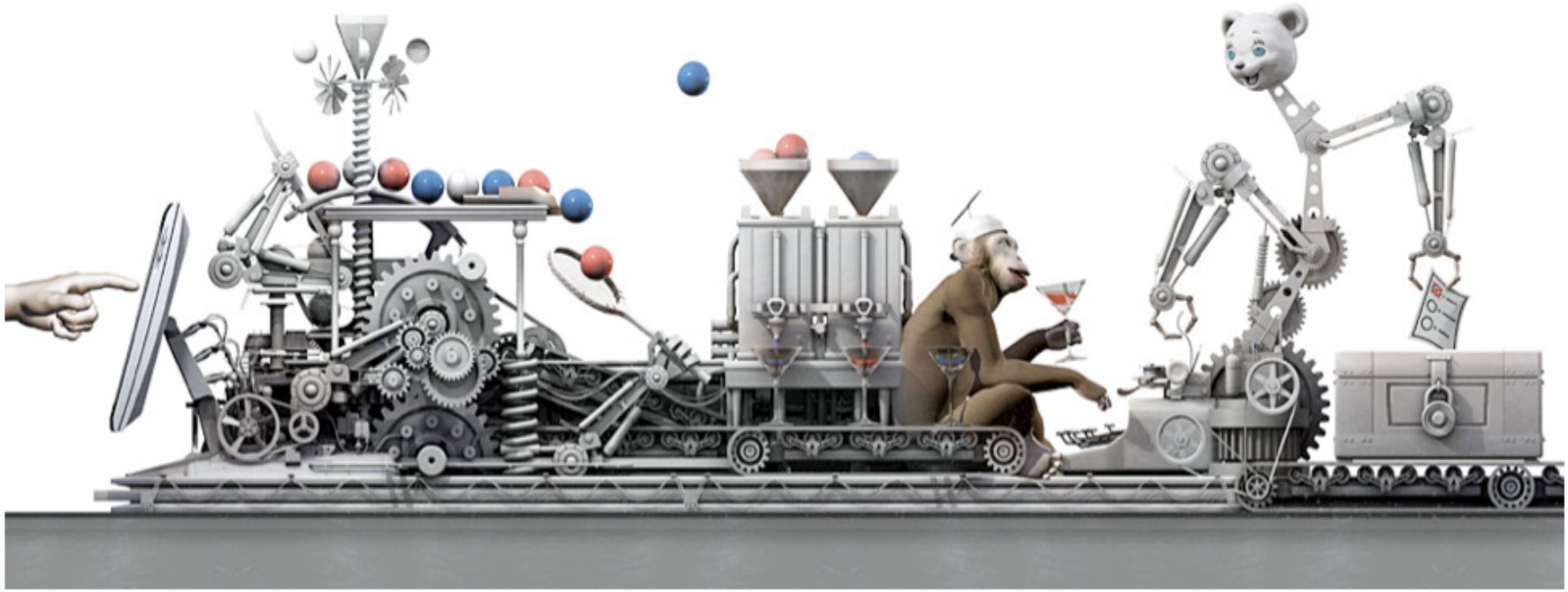
Power of Information Technology

Invalidates old assumptions



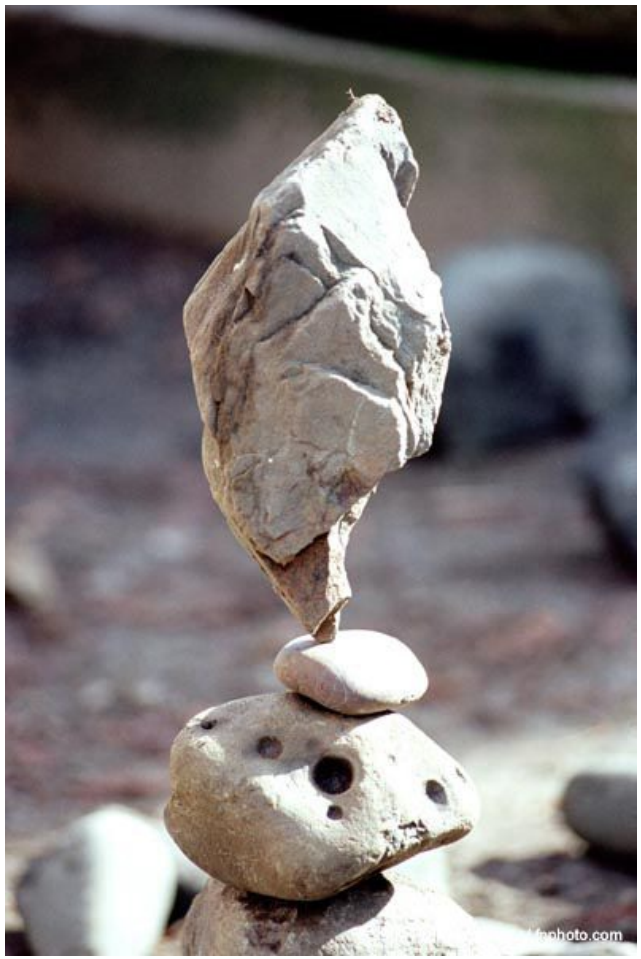
Power of Information Technology

Enables new solutions



Hypothesis

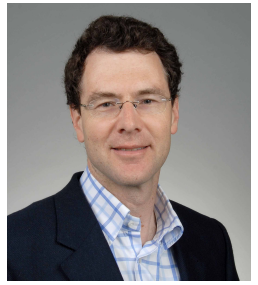
It is possible to modernize the electoral process while balancing the trust of the people on the trustworthiness of the deployed technology.



DemTech Objectives

- Consult decision makers wrt. risk analysis
- Evolve the democratic process
- Certification technology
- Help solve a “global” problem
- Be constructive
- Conduct cutting-edge security research
- Produce results that have an impact
- Build models of trust
- Evaluate our findings empirically

Consortium



External Advisory Board

1. Independent panel
2. Reviews progress
3. Allows election stakeholders to take ownership

Composition

Nicoline Nyholm Miller

Jørgen Elklit

Kasper Møller Hansen

…

Focus Area 1

Theory

Logical Frameworks

Programming Languages

Problem:

800 million transistors

> 89 million loc

Windows 7

> 50 million loc

Auditability/Accountability

Idea #1

The vote casting device is a computer, but not a general purpose one. It, and its software, should be as absolutely simple as possible. It should not be nearly as complex as a standard PC, for example. It needs only a touch screen, a slow processor and bus, minimal working RAM, and only one or two kinds of I/O port (e.g. serial, USB, or PCMCIA); it needs no rotating storage devices, no network card, no sound card (except for units for the handicapped), no advanced graphics, and no clock, no keyboard, and no mouse.

[Bruck, Jeffersen, Rivest, 2001]

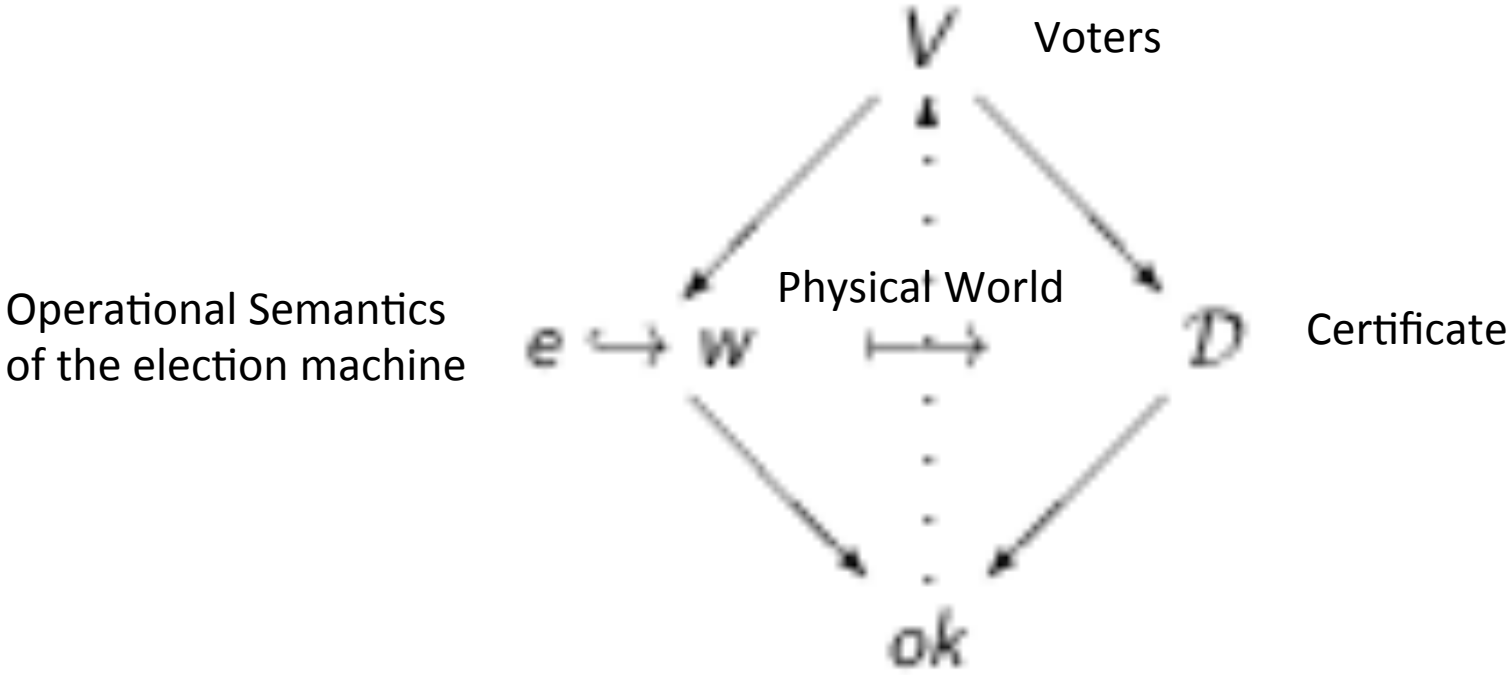
Idea #2
Software Independence

A voting system is software-independent if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome.

Rivest, Ron and Wack, John (2006) ***On the notion of "software independence" in voting systems***

Idea #3

- Certificates [CS '09]
- Trace emitting computations
- Simple certificate checker (< 2000 loc)



Election Domain Specific Language

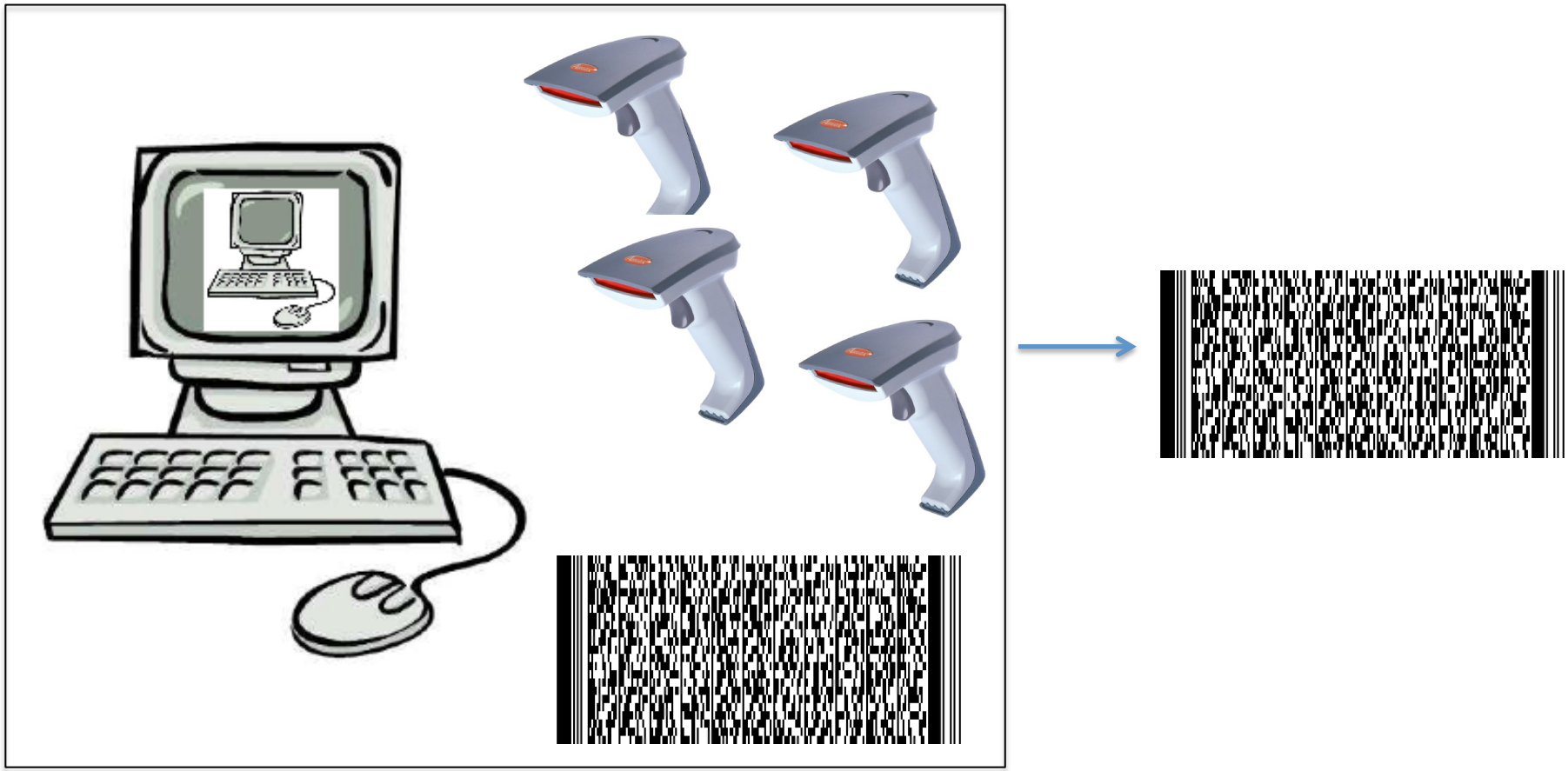
```
evcasea:
   {E:exp} {E1:exp} {W:val} {E2:exp}
        eval E a* ->
        eval E1 W ->
        eval (case E E1 E2) W.

evcaseb:
  {E:exp} {E2:exp} {W:val} {E1:exp}
        eval E b* ->
        eval E2 W ->
        eval (case E E1 E2) W.

evlam:
   {E:val -> exp}
       eval (lam ([x:val] E x)) (lam* ([x:val] E x)).
```

Definition

- Logical Framework LF
- Atomic steps
- Published ahead elections
- Known by all



From Law To Software

Example: Irish Voting Law

- Single Transferable Vote
- Law = Specification
- Software (Re)certification?

Related Work [Kiniry et al ‘10]

- Translate into JML
- Check with ESC Java
- Huge conceptual gap

Idea #4

- Linear/Concurrent Logic [Cervesato et al 01]
- Specification and Programming Language

$$A^-, B^- ::= P^- \mid \forall x{:}\tau.\, A^- \mid A^+ \multimap \{B^+\}$$
$$A^+, B^+ ::= A^+ \otimes B^+ \mid \mathbf{1} \mid !A^- \mid A^-$$

- Celf System [Schack-Nielsen 11]

http://www.twelf.org/~celf

```
c/1 : count-ballots S H (s U) *
      uncounted-ballot C L *
      hopeful C N *
      !quota Q * !nat-less (s N) Q
        -o {counted-ballot C L *
            hopeful C (s N) *
            count-ballots S H U}.

c/2 : count-ballots (s (s S)) (s H) (s U) *
      uncounted-ballot C L * hopeful C N *
      !quota Q * !nat-lesseq Q (s N) *
      winners W
        -o {counted-ballot C L *
            !elected C *
            winners (cons C W) *
            count-ballots (s S) H U}.

c/3 : count-ballots (s z) H U *
      uncounted-ballot C L *
      hopeful C N *
      !quota Q * !nat-lesseq Q (s N) *
      winners W
        -o {counted-ballot C L *
            !elected C *
            winners (cons C W) *
            !defeat-all}.
```

```
c/4_1 : count-ballots S H U *
        uncounted-ballot C (cons C' L) *
        !elected C
          -o {uncounted-ballot C' L *
              count-ballots S H U}.

c/4_2 : count-ballots S H U *
        uncounted-ballot C (cons C' L) *
        !defeated C
          -o {uncounted-ballot C' L *
              count-ballots S H U}.
```

PR-STV

[deYoung + CS]

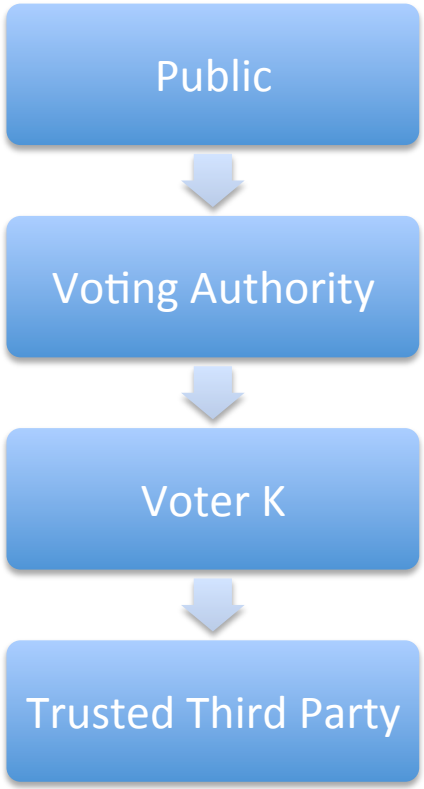
```
c/5_1 : count-ballots S H (s U) *
        uncounted-ballot C nil *
        !elected C
          -o {count-ballots S H U}.

c/5_2 : count-ballots S H (s U) *
        uncounted-ballot C nil *
        !defeated C
          -o {count-ballots S H U}.

c/6 : count-ballots S H z
        -o {defeat-min S H z}.
```

Idea #5: Epistemic Logic

- Knowledge, possession, assertion
- A la Proof carrying FS [Garg, Pfenning]
- Lattice of trust relationships
- Declassification
- Work in progress [with DeYoung]



Vote Casting

$$
\begin{array}{ll}
 & [K]\langle K\rangle \text{vote-for } L \\
\otimes & \langle va\rangle \text{is-registered } K \\
\otimes & [va]\text{voting} \\
\otimes & !\langle va\rangle \text{is\_candidate } L \\
\multimap & \{[va]\text{vote } L \\
 & \otimes [va]\text{voting}\}
\end{array}
$$

Election Closing

$$
\begin{array}{ll}
 & [K]\langle K\rangle \text{close} \\
\otimes & \langle va\rangle \text{may-close } K \\
\otimes & [va]\text{voting} \\
\multimap & \{[va]\text{close}\}
\end{array}
$$

Counting

$$
\begin{array}{ll}
 & [K]\text{count } L\ N \\
\otimes & [va]\text{may-count } K \\
\otimes & [va]\text{close} \\
\otimes & [va]\text{vote } L \\
\multimap & \{[va]\text{close} \\
 & \otimes [K]\text{count } L\ (N+1)\},
\end{array}
$$

Focus Area 2

Cryptography

(Full) Homomorphic Encryption

- Encryption
- Lax Logic: sec α
- Idea: due to Gentry
- HynML
- Voting machine:
  - no decryption keys
  - Slow

```
let
  double (x:sec int) =
    let (enc y) = x
    in case y
         of z => z
          | (s y) =>
            let (enc w) =
                double (enc y)
            in enc (s (s w))
in
  double (enc 3)
end
```

uni.lu ETH

Focus Area 3

Software Engineering

Trust by Design

Why do people trust?

- Public control
- User Verifiability

Challenge:

- Software Engineering
- User Interfaces Design

Goal:

Electronic process as trustworthy as the traditional process

ETH SIEMENS

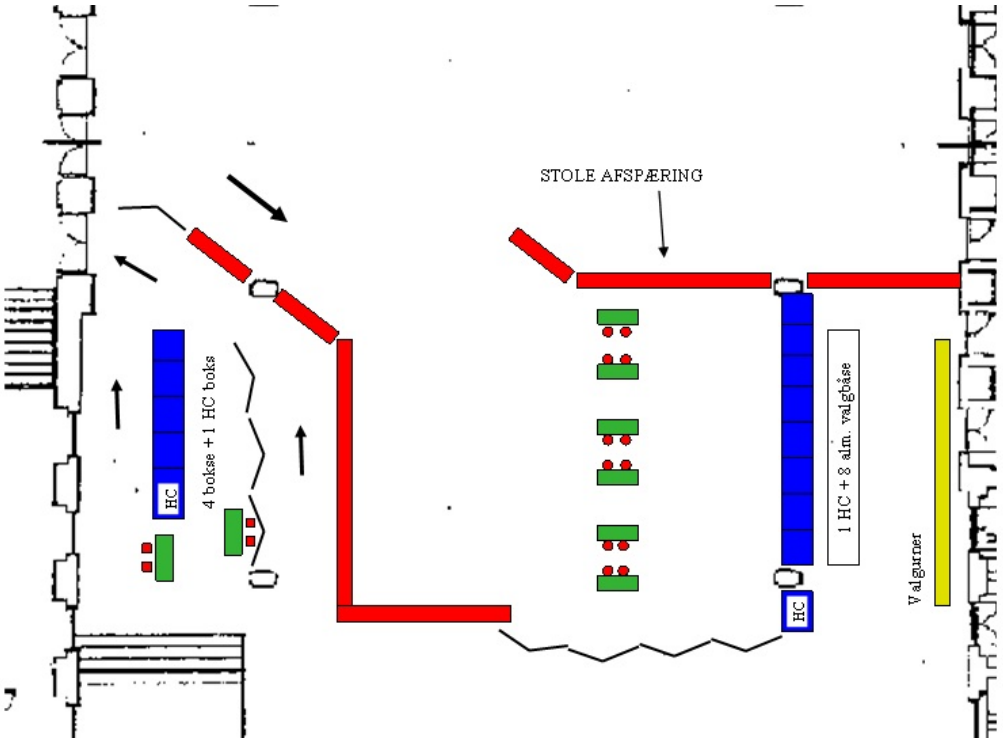
Focus Area 4

Social Science

Political Science

Studies of Science and Technology

- Ethnographies
- History of trust
- Models of trust
  - Qualitative
  - Quantitive
- User Studies



Evaluation

History

[2007] Students build a machine

[2008] University Board Member Election

[2009] Interior ministry forbids experimentation Municipality/Parliamentary Elections

[2010] Invited speaker at E-Elections Conference in Parliament

[2010] Consultant to the governmental “Board of Technology”

From the Minister of the Interior Bertel Haarder, May 13,2011

Thank you for your letter of 28 March 2011 with information on the DemTech project, and for your kind offer to provide your services in relation to the political process and further public discussions on the future of e-voting in Denmark.

I agree with you that more research particularly on how to preserve trust and ensure a sufficient level of security throughout digital election processes will be most useful to enlighten the debate and ensure that we – if we should one day decide to embark on e-voting pilot projects in Denmark – will be able to do so on a sufficiently enlightened background.

Concerning the recommendations from the Board of Technology working group, I believe it is a useful outset for further discussions, albeit the report still leaves a number of issues unresolved, which require careful consideration and investigation before any concrete projects can be initiated. Among these issues are how to ensure a sufficiently high level of security, and how to exercise public control in a black box polling setup. Therefore, the government wishes to encourage the building up of relevant expertise and know-how based on already established national election rituals and culture and drawing on international experiences. In this respect, I believe that the DemTech project shows good prospect of being of great value to the further public debate and political process.

I know that you are already in close contact with the officials in my ministry responsible for the election administration, and that they are following your research project closely. I trust that this already established cooperation will prove to be fruitful to both parties. I wish you the very best of luck with your endeavours and look forward to be informed of your findings.

Real Elections

[2013] Municipalitiy (possibly Luxembourg parliament)

- Wider tests if permitted by minister of the interior

[2014] European Government Election

- If we agree then maybe pilot projects

[2015] Folketinget (Parliament)

- If we agree then maybe pilot projects

Statistics

- 4 Focus areas
  - PL, Crypto, Software Engineering, Social Science
- Generously funded
  - Thanks to the Research Council for Strategic Research
  - IT University of Copenhagen
- Start date 7/1/2011
- End date 6/30/2016
- 4 PostDoc positions, 3 years each
- 6 PhD positions

Thank you

www.demtech.dk

Related Projects

Voting Technology Project

- MIT, CalTech
- Rivest, Katz, et al. (affiliated Ryan)

Accurate Project

- Berkeley, Johns Hopkins, Rice, Stanford, SRI
- Rubin, Wallach, Dill, Wagner et al.

True Voter Verifiable Elections

- Chaum

…