No More Excuses: Automated Synthesis of Practical and Verifiable Vote-counting Programs for Complex Voting Schemes

Lyria Bennett Moses [1] Rajeev Goré [2] Ron Levy [3] Dirk Pattinson[2] Mukesh Tiwari [2]

E-Vote-ID, 26 October 2017

High(est) Level

Voting Systems: Requirements

1. each person's vote must be counted correctly
2. the system must be practicable, usable and secure
3. subjective trust in the process by the electorate
4. subjective trust should have objective basis

This talk.

- what does *trust* really mean?
- non-technical aspects of trust
- technical realisation

Aspects of Trust

Transparency

- doesn't necessarily increase subjective trust
- does promote public trust

Public Accountability.

- give account or explanation to public
- also needs enforcement

Two Sides of Transparency

- process transparency: usually achieved by legislation
- procedural transparency: execution of process is transparent

Electronic vs Paper Ballots: Tallying Votes

Paper Ballots.

- procedural transparency through scrutineers
- public confidence as candidates may nominate scrutineers
- transparency reduces risk of error and fraud

Electronic Ballots.

- should be held to the same standards
- should go further by overcoming physical limitations
- verifiable systems should achieve procedural and process transparency

Transparency: State of the Art

Open Source Counting.

- provides *some* level of procedural transparency
- in practice, largely hypothetical

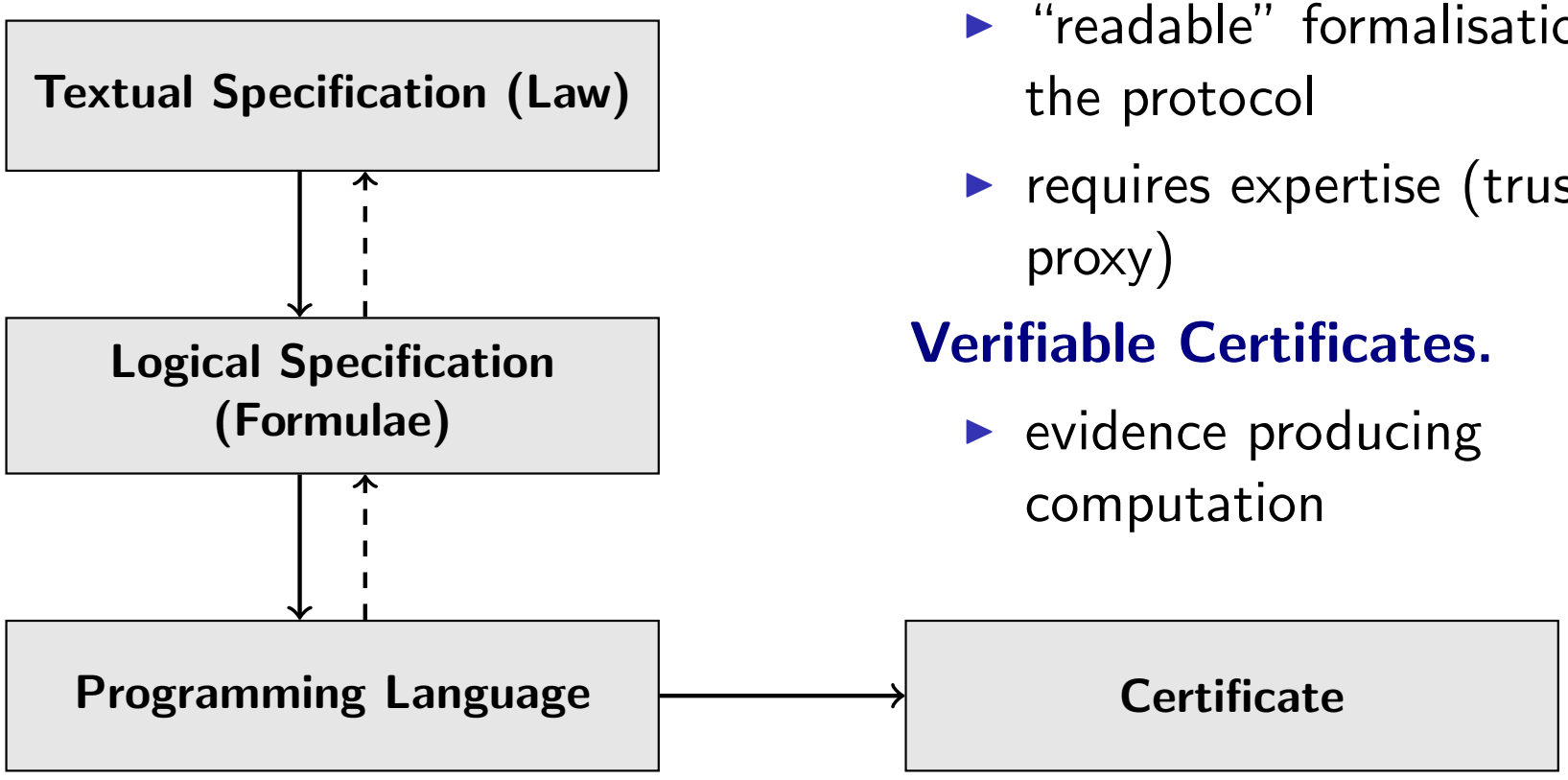
Closed Source Counting.

- no procedural transparency at all
- in practice, often commercial in confidence

Our Contribution.

- procedural transparency through *verifiable certificates*
- process transparency through *open specification*
- evidence of feasibility through *implemented prototype*

Overview



Open Specification

- "readable" formalisation of the protocol
- requires expertise (trust by proxy)

Verifiable Certificates.

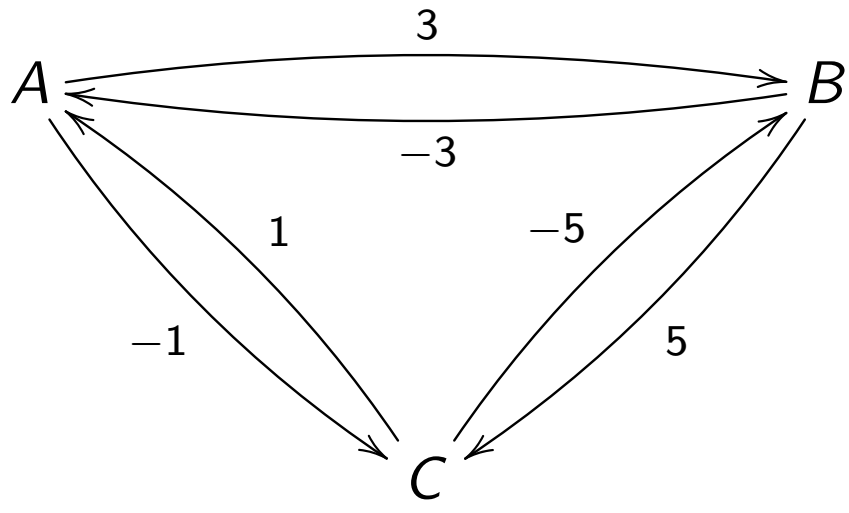
- evidence producing computation

Case Studies

- single transferable vote (last talk)
- Schulze counting (this talk)
- works for millions of ballots

The Schulze Method

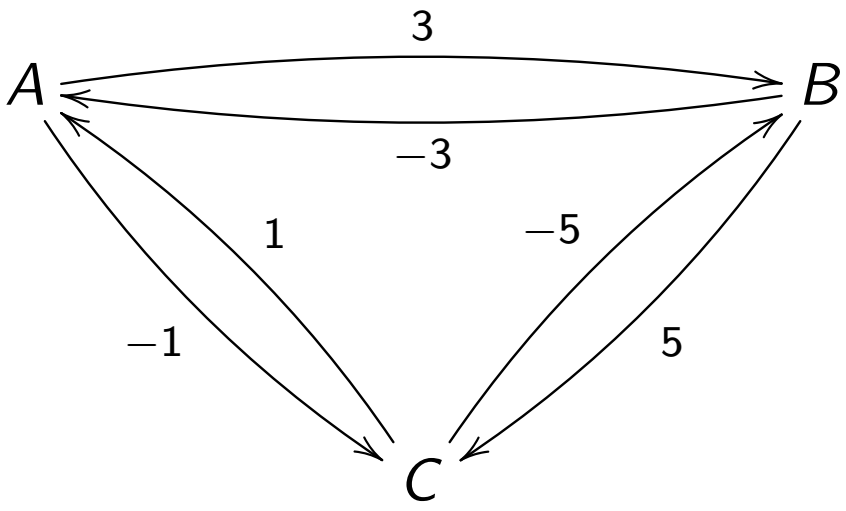
- Collective preferences can be cyclic (Condorcet paradox)

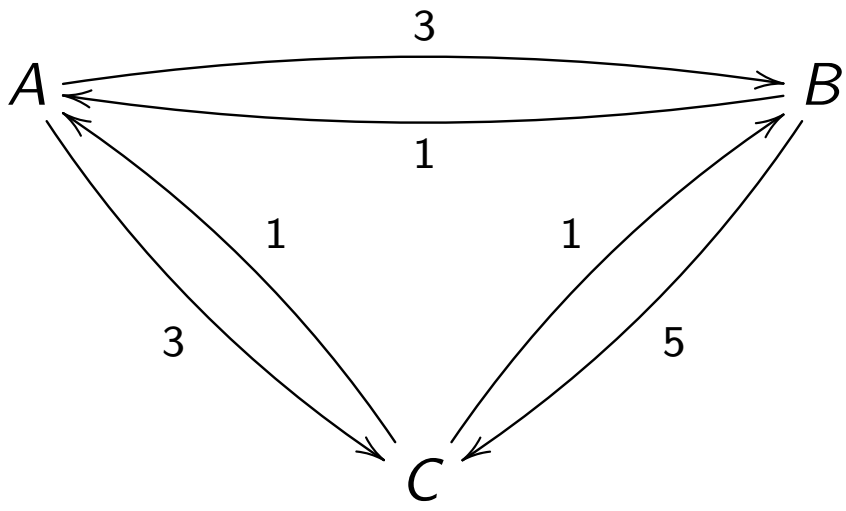


$$m(x, y) = \sharp\{\text{no of voters that prefer } x \text{ over } y\} - \sharp\{\text{no of voters that prefer } y \text{ over } x\}$$

- resolve cycles using transitive prefereces

Resolving Condorcet Cycles





Margin (left) and generalised margin (right)

Open Specification: Example

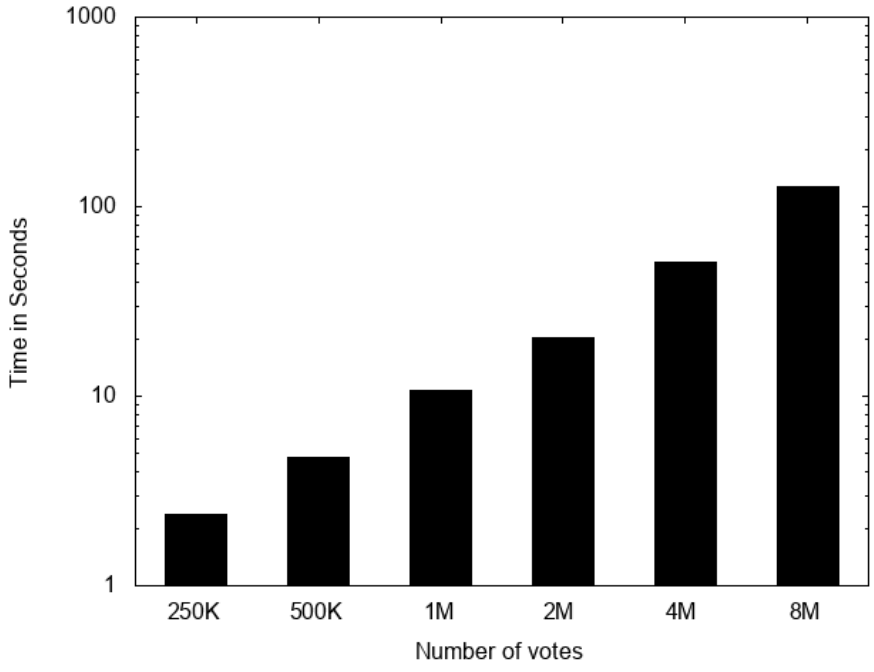
```
{- Winning: candidates that cannot be beaten -}
Definition wins_prop (c: cand) :=
  forall d : cand, exists k : Z,
   Path k c d /\
   (forall l, Path l d c -> l <= k).
```

```
{- Losing: candidates that can be beaten -}
Definition loses_prop (c : cand) :=
  exists k: Z, exists  d: cand,
   Path k d c /\
   (forall l, Path l c d -> l < k).
```

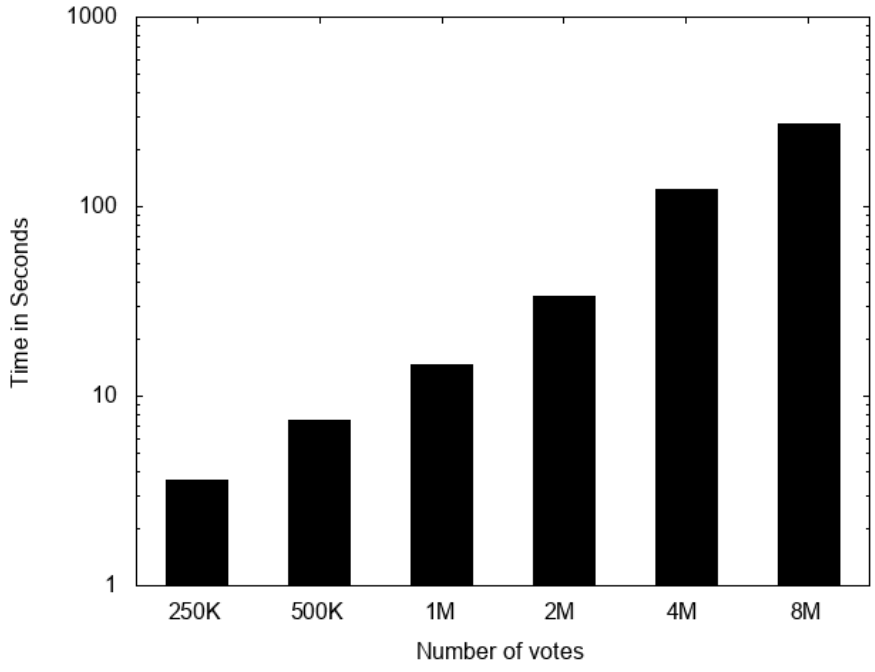
Extraction: Example Certificate

```
V: [A1 B2 C3,..], I:  [], M: [AB:0 AC:0 BC:0]
-----------------------------------------
V: [A1 B2 C3,..], I:  [], M: [AB:1 AC:1 BC:1]
-----------------------------------------
             . . .
-----------------------------------------
V: [A2 B3 C1], I:  [], M: [AB:2 AC:0 BC:6]
-----------------------------------------
V: [], I: [], M: [AB:3 AC:-1 BC:5]
----------------------------------
winning: A
   for B: path A -> B of strenght 3, 4-coclosed set:
     [(A,A),(B,A),(B,B),(C,A),(C,B),(C,C)]
   for C: path A -> B -> C of strenght 3, 4-coclosed set:
     [(A,A),(B,A),(B,B),(C,A),(C,B),(C,C)]
losing: B
   exists A: path A -> B of strength 3, 3-coclosed set:
     [(A,A),(B,A),(B,B),(C,A),(C,B),(C,C)]
losing: C
   exists A: path A -> B -> C of strength 3, 3-coclosed set:
     [(A,A),(B,A),(B,B),(C,A),(C,B),(C,C)]
```

Experimental Results: 4 candidates, commodity desktop



without producing certificates



with producing certificates

Conclusions

Many Aspects of Trust

- transparency: process and procedural
- accountability: *opposite* of "no signs of irregularities"

Procedural Transparency

- usually enshrined in legislation
- can and needs to be formalised with small gap

Process Transparency

- software independence
- externally verifiable certificates

Case Studies

- (more) transparency can be achieved
- in realistic scenarios