# Brittle and Resilient Verifiable Voting Systems

Philip B. Stark

Department of Statistics
University of California, Berkeley

Verifiable Voting Schemes Workshop:
from Theory to Practice
Interdisciplinary Centre for Security, Reliability and Trust
University of Luxembourg
Luxembourg
21–22 March 2013

## Fundamental Rule of Applied Work

In theory, there's no difference between theory and practice.
But in practice, there is.
Jan L.A. van de Snepscheut

## Fundamental Rule Election Integrity

If you tell vendors or LEOs that there are three essential things they must do to ensure integrity, often they will do both of those things.

## Fundamental Rule of Election Integrity in Action

- Recent examples: Clear Ballot, Sacramento County
- What are the consequences for traditional voting systems?
- What are the consequences for E2E voting systems?

## Wallach's Insight

The purpose of an election is to convince the loser he lost.
Dan Wallach

## Evidence-Based Elections

Elections officials should provide convincing evidence that the outcomes are right, or say that no such evidence is forthcoming.

## (Strong) Software Independence

Undetected change or error in its software cannot produce an undetectable change or error in the results (and possible to reconstruct the correct result without re-running the election). Rivest & Wack

- Property of election, not equipment
- System can produce wonderful voter-verified paper trail and still not be SI, if paper trail is not curated adequately
- SSI guarantees that the right outcome can be found without re-running the election, but you still gotta look and do the work

## E2E

Voter can verify that her vote was counted as cast.
Anyone can verify that the published votes were tabulated correctly.

- Property of election, not equipment

## Resilient Canvass Framework

Large (minimum) chance that, at the end of the canvass, the declared outcome is correct—or a declaration that no such guarantee can be made.
Benaloh et al.

- Capture idea that system should be self-correcting or admit that the "perturbation" may have exceeded its fault tolerance
- Property of election, not equipment

## What do we want election audits to do?

- Ensure that the electoral outcome is correct.
- If outcome is wrong, correct it before it's official.

## Risk-limiting Audit

Large (minimum) chance of correcting the outcome if the outcome is wrong.

- Property of audit, not a particular recipe
- Gives quantitative, statistical evidence
- Generally relies on random samples from the audit trail
- Presumes that the audit trail is sufficiently intact that a full hand count would reveal the correct outcome

## Compliance Audit

Check whether the audit trail is sufficiently intact that a full hand count would show the real outcome.

- Gives qualitative evidence—like legal standards.
- "Convincing to a reasonable person."
- Ballot accounting, checks of chain of custody, security seals, etc.

## Risk-Limiting Audits

- Guaranteed minimum chance of correcting the outcome if the outcome is wrong
- Minimum is over all ways the outcome could be wrong: random error, equipment failure, fraud
- Many ways to accomplish
- Basic strategies: comparison and ballot-polling

# Ballot-polling Audits and Comparison Audits

- Ballot polling audit: sample ballots until there is strong evidence that looking at all of them would show the same election outcome.
  Like an exit poll—but of ballots, not voters.
- Comparison audit:
  1. Commit to vote subtotals (or CVRs), e.g., precinct-level results
  2. Check that the subtotals add up exactly to contest results
  3. Check subtotals by hand until there is strong evidence the outcome is right

  For both, sample size is random: sampling continues until evidence is strong enough.
  Depends on which ballots are drawn; for comparison audit, depends on errors found.

# Tradeoffs

- Ballot polling audit
  - Virtually no set-up costs
  - Requires nothing of voting system
  - Need a ballot manifest to draw sample
  - Preserves voter anonymity except possibly for sampled ballots
  - Requires more counting than ballot-level comparison audit
  - Does not check tabulation: outcome could be right because errors cancel
- Comparison audit
  - Heavy demands on voting system for reporting and data export
  - Requires LEO to commit to subtotals
  - Requires ability to retrieve ballots that correspond to CVRs or subtotals
  - May compromise voter privacy
  - Most efficient (ballot-level) not possible w/ current systems: requires rescan
  - Checks tabulation (but not for transitive audits unless subtotals are cross checked as well)
  - Ballot-level comparison audits require least hand counting

# Pilot Risk-Limiting Audits

- 17 pilot audits in CA, CO, and OH; another 13 planned.
- EAC funding for pilots in CA and CO and Cuyahoga County, OH
- CO has law; CA has pilot law
- simple measures, super-majority, multi-candidate, vote-for-$n$
- multiple contests audited simultaneously with one sample
- contest sizes: 200 ballots to 121,000 ballots
- counting burden: 16 ballots to 7,000 ballots
- cost per audited ballot: nil to about \$0.55
- several jurisdictions have audited on their own—no statistician required

# What hasn't been tried?

- Cross-jurisdictional contests
- IRV/RCV

# Ballot-polling Audits are often Cheap for Big Contests

**255 state-level U.S. presidential contests, 1992–2011, 10% risk limit**

BPA expected to examine fewer than 308 ballots for half the contests.

Work expands as margins shrink, but we could get a lot of election integrity at low cost—with any paper-based system.

# Workload estimate: Ballot-Polling Audit, 2 Candidates, 10% Risk Limit

| Winner's True Share | Ballots drawn | | |
|---|---|---|---|
| | median | 90th percentile | Mean |
| 70% | 22 | 60 | 30 |
| 65% | 38 | 108 | 53 |
| 60% | 84 | 244 | 119 |
| 58% | 131 | 381 | 184 |
| 55% | 332 | 974 | 469 |
| 54% | 518 | 1,520 | 730 |
| 53% | 914 | 2,700 | 1,294 |
| 52% | 2,051 | 6,053 | 2,900 |
| 51% | 8,157 | 24,149 | 11,556 |
| 50.5% | 32,547 | 96,411 | 46,126 |

# Making it simple is hard—but possible

## Very simple rules and tools for ballot-level audits

Crucial that calculations be simple and reproducible by observers.
Have approaches easy enough for pencil and paper.

- Comparison: At 10% risk, need 5/margin ballots if no errors are found
  Sample until #good $+\alpha_1 \cdot$#under $-\alpha_2 \cdot$#over $> \alpha_3$
- Ballot-polling: sample until $\alpha_1^{\omega} \alpha_2^{\ell} < \rho$
  $\forall$(winner, loser) pairs.

## Evidence-based Elections

$$\text{Evidence} = \text{Auditability} + \text{Auditing}$$

- strongly software-independent voting system
- compliance audit to check integrity of audit trail: is system still SSI?
- risk-limiting audit to check outcomes
- puts incentives in the right place: better procedures and equipment mean less work for LEOs

Current elections are procedure-based: equipment certification and election process.

## End-to-End Verifiable Elections and Paper Evidence-Based Elections

- Goal of both is to have convincing evidence that outcomes are right—or know that the evidence isn't convincing
- Differ in the nature of evidence, in who generates the evidence, in whom voters need to trust, and for what they must be trusted
- Also differ in ability to recover from corruption of portions of the evidence trail
- Examine differences and impact on strength of evidence and anonymity of votes
- Suggest ways to combine and to make E2E more resilient

## E2E

- Focus on bulletin-board systems
- Voter can obtain strong evidence that her vote was cast as intended and counted as cast, and that all posted ballots were correctly tabulated
- Enforce vote anonymity using cryptography and procedures (voter cannot prove to anyone how she voted)
- Aggregate votes using homomorphic encryption or mixnet
- Protect voter privacy using randomized threshold public key encryption (requires collusion among officials to break anonymity)

## EBE

- Focus on paper-based systems with risk-limiting audits
- Voters can obtain strong evidence that vote was cast as intended
- Auditors can obtain strong evidence that outcomes are correct
- Enforce anonymity through equipment and procedures
- Small lapses can break anonymity to elections officials
- Some proposals (e.g., posting digital images of all ballots) could break anonymity to the public

## E2E v EBE

- To have strong evidence that outcomes are correct, need evidence that votes were recorded accurately, tabulated accurately, and reported accurately.
- Voters, public, and elections officials have different roles in that process in E2E and paper-based EBE
- Examine consequences of the approaches for software independence and strong software independence, privacy, verifiability

## What does it take to make an E2E election resilient?

- Basic E2E like tamper-evident seal: SI, not SSI
- can tell that something went wrong, but not how badly; generally can't recover
- How can we enhance basic strategy to make it easier to recover from errors?

## Tradeoffs

| | E2E | | paper | |
|---|---|---|---|---|
| own cast as intended | self | hard | voter | easy |
| others' cast as intended | others | hard | others | easy |
| own counted as cast | self/public | easy | auditors | easy |
| others' counted as cast | self/public | easy | auditors | easy |
| only authorized voters | self/public | hard | LEO | easy |

chain of custody versus direct visibility

definition of "any voter"

## STAR-Vote

- Combine crypto with paper
- Might lose E2E property for some voters, but keep resilient canvass framework
- Also protects against loss of some paper or loss of some crypto-data

## Which really matters?

1. Under laboratory conditions, can the vote tabulation system—as delivered from the manufacturer—count votes with a specified level of accuracy?
2. As maintained, deployed, and used in the current election, did the vote tabulation system find the true winners?

Certification can cost millions and take years. Addresses Q 1.

Audits address Q 2.

## Role and consequences of certification

Current certified systems make audits more expensive and less transparent than necessary.
Maintenance costs high; systems not agile; stupefying inertia.

Certification still useful for some things, e.g., to ensure accessibility and creation of durable audit trail.

Need to push for easily auditable systems using COTS components and free/open/cheap software.

Travis County TX and Los Angeles County CA are leaders.