

Trustworthy Elections: Evidence and Dispute Resolution

2019 Def Con
Las Vegas, NV

Philip B. Stark

9 August 2019

University of California, Berkeley

Suitably designed and operated paper-based voting systems can be strongly software independent, contestable, and defensible, and they can make risk-limiting audits and evidence-based elections possible. (These terms will be defined.) Not all paper-based voting systems have these properties. Systems that rely on ballot-marking devices and voter verifiable paper audit trails produced by electronic voting machines generally do not, because they cannot provide appropriate evidence for dispute resolution, which has received scant attention. An ideal system allows voters, auditors, and election officials to provide public evidence of any problems they observe—and can provide convincing public evidence that the reported electoral outcomes are correct despite any problems that might have occurred, if they are correct.

Many collaborators including (most recently) Andrew Appel, Josh Benaloh, Matt Bernhard, Rich DeMillo, Steve Evans, Alex Halderman, Mark Lindeman, Kellie Ottoboni, Ron Rivest, Peter Ryan, Vanessa Teague, Poorvi Vora, Dan Wallach

Did the reported winner really win?

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
 - sterile scalpel v. patient's condition

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
 - sterile scalpel v. patient's condition
- Check equipment? Or check outcomes?

Did the reported winner really win?

- Procedure-based vs. evidence-based elections
 - sterile scalpel v. patient's condition
- Check equipment? Or check outcomes?
- Whom must we trust, and for what?

Why audit?

- *Any* way of counting votes can make mistakes
- *Every* electronic system is vulnerable to bugs, configuration errors, & hacking
- **Did error/bugs/hacking cause losing candidate(s) to appear to win?**

Security properties of paper

- tangible/accountable
- tamper evident
- human readable
- large alteration/substitution attacks generally require many accomplices

Security properties of paper

- tangible/accountable
- tamper evident
- human readable
- large alteration/substitution attacks generally require many accomplices

Not electronic systems.

- If there's a reliable, voter-verified paper trail, can check whether reported winner really won.
- If you permit a small “risk” of not correcting the reported outcome if it is wrong, generally don't need to look at many ballots if outcome is right.

A risk-limiting audit has a known chance of correcting the reported outcome if the reported outcome is wrong (and doesn't change correct outcomes).

A risk-limiting audit has a known chance of correcting the reported outcome if the reported outcome is wrong (and doesn't change correct outcomes).

Risk limit: largest possible chance of *not* correcting reported outcome, if reported outcome is wrong.

- Audit enough to have strong evidence reported winner really won.

- Audit enough to have strong evidence reported winner really won.
- “Spoonful of soup”: small sample often enough (depends on margin)

- Audit enough to have strong evidence reported winner really won.
- “Spoonful of soup”: small sample often enough (depends on margin)
- Should be routine, no matter how big the margin

Tools for Comparison Risk-Limiting Election Audits

To hide or show everything but the tools, [click this link](#).

Initial sample size

Initial sample size

Contest information

Ballots cast in all contests: Smallest margin (votes): 61. Diluted margin: 0.86%.

Contest 1. Contest name:

Winners:

Reported votes:

Candidate 1 Name:	<input type="text" value="Juliana Brannen"/>	Votes:	<input type="text" value="1772"/>
Candidate 2 Name:	<input type="text" value="Mark Luce"/>	Votes:	<input type="text" value="2808"/>
Candidate 3 Name:	<input type="text" value="Mark Van Garder"/>	Votes:	<input type="text" value="1833"/>

Audit parameters

Risk limit:

Expected ratio of differences (as decimal numbers):

Overstatements. 1-vote: 2-vote:

Understatements. 1-vote: 2-vote:

Starting size

☒ Round up 1-vote differences. ☐ Round up 2-vote differences. 623.



Requirements

- Voter-verified paper trail
 - Any jurisdiction with paper can do an RLA
 - Need to ensure the paper trail is trustworthy
 - Some equipment makes it *easier*, but replacing equipment isn't necessary

Requirements

- Voter-verified paper trail
 - Any jurisdiction with paper can do an RLA
 - Need to ensure the paper trail is trustworthy
 - Some equipment makes it *easier*, but replacing equipment isn't necessary
- “Ballot manifest”: description of how ballots are stored
 - Should be routine
 - “It’s the day after the election. Do you know where your ballots are?”

Requirements

- Voter-verified paper trail
 - Any jurisdiction with paper can do an RLA
 - Need to ensure the paper trail is trustworthy
 - Some equipment makes it *easier*, but replacing equipment isn't necessary
- “Ballot manifest”: description of how ballots are stored
 - Should be routine
 - “It’s the day after the election. Do you know where your ballots are?”
- Manually inspect randomly selected paper ballots
 - individual ballots, batches, unstratified, stratified, w/ or w/o replacement
 - polling audits: just need ballots
 - comparison audits: also need to export data & check totals

Requirements

- Voter-verified paper trail
 - Any jurisdiction with paper can do an RLA
 - Need to ensure the paper trail is trustworthy
 - Some equipment makes it *easier*, but replacing equipment isn't necessary
- “Ballot manifest”: description of how ballots are stored
 - Should be routine
 - “It’s the day after the election. Do you know where your ballots are?”
- Manually inspect randomly selected paper ballots
 - individual ballots, batches, unstratified, stratified, w/ or w/o replacement
 - polling audits: just need ballots
 - comparison audits: also need to export data & check totals
- Routine in CO and soon RI; pilots in 9 states and Denmark
- laws in TX, VA, CA?

- “electronic pen”

- “electronic pen”
- can present ballots in many languages, “accessible” interface

- “electronic pen”
- can present ballots in many languages, “accessible” interface
- what if they malfunction?

- research so far:
 - few voters check
 - checks so brief unlikely to help
 - voters can't remember selections

- if astute voter catches error:
 - might get a fresh ballot
 - has no evidence to show malfunction, only claim
 - presumption will be voter error, not machine error
 - fresh ballot doesn't ensure correct outcome overall

- if astute voter catches error:
 - might get a fresh ballot
 - has no evidence to show malfunction, only claim
 - presumption will be voter error, not machine error
 - fresh ballot doesn't ensure correct outcome overall
- if pollworker convinced, what recourse is there?
 - new election? (no way to find correct outcome)
 - "wolf!"

BMDs need to be designed to allow disputes to be resolved

- If voter observes malfunction, should be able to prove it to others*

BMDs need to be designed to allow disputes to be resolved

- If voter observes malfunction, should be able to prove it to others*
- If LEO has evidence that the outcome is still correct, should be able to prove it to public*

(*Without compromising the anonymity of votes.)

- BMD printout might not match what voters indicated to the BMD.
- RLA of elections conducted on BMDs may confirm the wrong winner.
- “Parallel testing” requires unworkable sample sizes (& labor, training, equipment, infrastructure).

- BMD printout might not match what voters indicated to the BMD.
- RLA of elections conducted on BMDs may confirm the wrong winner.
- “Parallel testing” requires unworkable sample sizes (& labor, training, equipment, infrastructure).

Current BMDs can be hacked undetectably and alter outcomes: not *software independent*.

Useful ideas for election integrity and security

- (Strong) software independence

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability
- Contestability

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability
- Contestability
- Defensibility

Useful ideas for election integrity and security

- (Strong) software independence
- Risk-limiting audit
- Evidence-based elections
- End-to-end verifiability
- Contestability
- Defensibility

5 Cs

- *Create* durable, trustworthy record of voter intent
 - ideally, hand-marked paper ballots + BMDs for voters who benefit from them
- *Care* for the paper record
 - verifiable chain of custody, 2-person custody rules, ballot accounting, good seal protocols, etc.
- *Compliance* audit: establish whether paper trail is trustworthy
 - ballot accounting including VRDB, pollbooks, etc.; check chain of custody logs, video, etc.; eligibility
- *Check* reported outcome against the paper by auditing
- *Correct* the reported outcome if it is wrong