Publicly-Verifiable Elections

How Voters can Check Election Integrity

Josh Benaloh

Senior Cryptographer
Microsoft Research

Risk-Limiting & Bayesian Audits

Internal administrative audits can detect many important errors and malicious behaviors…

… but they do not protect against all ills.

Administrative Audits

Internal administrative are ineffective if election administrators …

- are careless or malicious,
- fail to maintain good chain-of-custody of ballots,
- use auditing tools that are not independent of counting software, or
- are simply not trusted by constituents.

What is Possible?

Technology exists that enables *any* inaccuracies and tampering of election tallies to be detected …

… not just by election officials, but also by any candidate, media outlet, voter, or other observer …

… and not just external tampering, but corruption by election officials, equipment vendors, and others.

This is known as *End-to-End (E2E) Verifiability*.

End-to-End Verifiable Elections

An election is *end-to-end verifiable* if

1. Voters can verify that their own selections have been correctly recorded.
2. Anyone can verify that the recorded votes have been correctly tallied.

I’d love to describe *how* …

… but I could easily spend 90 minutes. ☹

Here’s the 90 second version. ☺

Privacy *must* be Enforced

- Voters must be *unable* to disclose their votes to others.
- Open-ballot elections would be sooo… much easier to secure.

Elections Prior to Secret Ballots

The County Election – George Caleb Bingham 1852

A Public Election Ledger

Voter Name	Vote
Alice Smith	Jefferson
Bob Williams	Adams
Carol James	Adams
David Fuentes	Jefferson
Ellen Chu	Jefferson

Totals	
Jefferson	3
Adams	2

An End-to-End Verifiable Election

Voter Name	Vote
Alice Smith	Jefferson
Bob Williams	Adams
Carol James	Adams
David Fuentes	Jefferson
Ellen Chu	Jefferson

Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

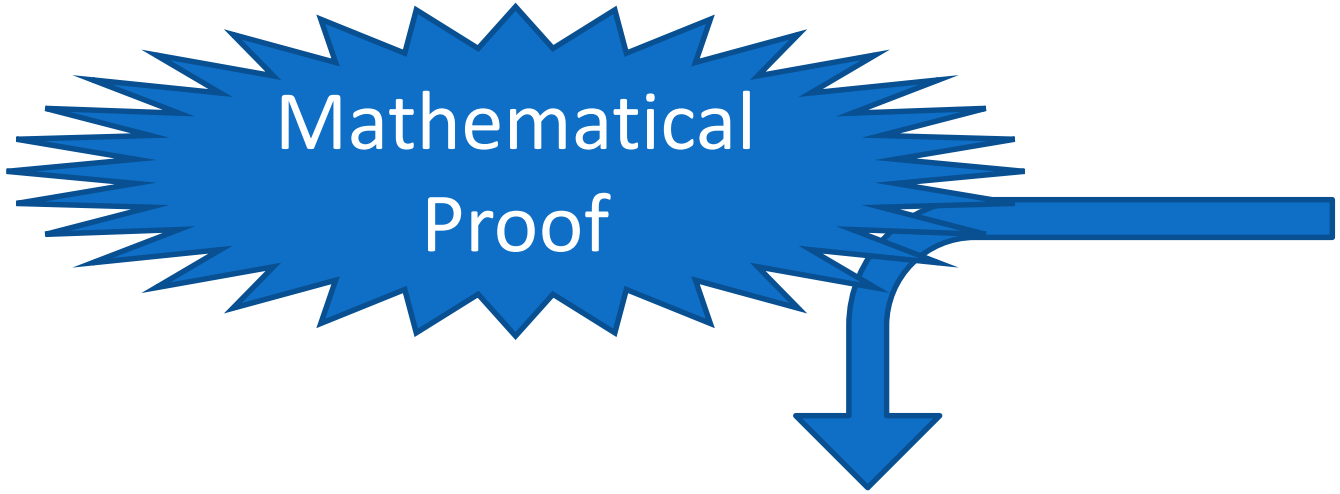
Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election

X37BM6YPM
2J8CNF2KQ
VRSF5JQWZ
MW5B2VA7Y
8VPPS2L39

Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election



X37BM6YPM
2J8CNF2KQ
VRSF5JQWZ
MW5B2VA7Y
8VPPS2L39

Totals	
Jefferson	3
Adams	2

Homomorphic Tallying

Voter Name	Vote
Alice Smith	<1,0,0;1,0;0,1;0,0,1>
Bob Williams	<0,1,0;1,0;1,0;1,0,0>
Carol James	<0,1,0;0,1;1,0;1,0,0>
David Fuentes	<1,0,0;1,0;0,1;0,0,1>
Ellen Chu	<1,0,0;1,0;0,1;0,1,0>

Homomorphic Tallying

Voter Name	Vote
Alice Smith	<1,0,0;1,0;0,1;0,0,1>
Bob Williams	<0,1,0;1,0;1,0;1,0,0>
Carol James	<0,1,0;0,1;1,0;1,0,0>
David Fuentes	<1,0,0;1,0;0,1;0,0,1>
Ellen Chu	<1,0,0;1,0;0,1;0,1,0>
	+
Tally	<3,2,0;4,1;2,3;2,1,2>

Homomorphic Tallying

Voter Name	Vote	
Alice Smith	<1,0,0;1,0;0,1;0,0,1>	X37BM6YPM
Bob Williams	<0,1,0;1,0;1,0;1,0,0>	2J8CNF2KQ
Carol James	<0,1,0;0,1;1,0;1,0,0>	VRSF5JQWZ
David Fuentes	<1,0,0;1,0;0,1;0,0,1>	MW5B2VA7Y
Ellen Chu	<1,0,0;1,0;0,1;0,1,0>	8VPPS2L39

Homomorphic Tallying

Voter Name	Vote	
Alice Smith	<1,0,0;1,0;0,1;0,0,1>	X37BM6YPM
Bob Williams	<0,1,0;1,0;1,0;1,0,0>	2J8CNF2KQ
Carol James	<0,1,0;0,1;1,0;1,0,0>	VRSF5JQWZ
David Fuentes	<1,0,0;1,0;0,1;0,0,1>	MW5B2VA7Y
Ellen Chu	<1,0,0;1,0;0,1;0,1,0>	8VPPS2L39
	+	⊕
Tally	<3,2,0;4,1;2,3;2,1,2>	**41R7DDY7M**

Homomorphic Tallying

Voter Name	Vote	
Alice Smith	<1,0,0,1,0,0,1,0,0,1>	X37BM6YPM
Bob Williams	<0,1,0,1,0,1,0,1,0,0>	2J8CNF2KQ
Carol James	<0,1,0,0,1,1,0,1,0,0>	VRSF5JQWZ
David Fuentes	<1,0,0,1,0,0,1,0,0,1>	MW5B2VA7Y
Ellen Chu	<1,0,0,1,0,0,1,0,1,0>	8VPPS2L39

Homomorphic Tallying

Voter Name	Vote	
Alice Smith	<1,0,0,1,0,0,1,0,0,1>	X37BM6YPM
Bob Williams	<0,1,0,1,0,1,0,1,0,0>	2J8CNF2KQ
Carol James	<0,1,0,0,1,1,0,1,0,0>	VRSF5JQWZ
David Fuentes	<1,0,0,1,0,0,1,0,0,1>	MW5B2VA7Y
Ellen Chu	<1,0,0,1,0,0,1,0,1,0>	8VPPS2L39
		⊕
Tally		**41R7DDY7M**

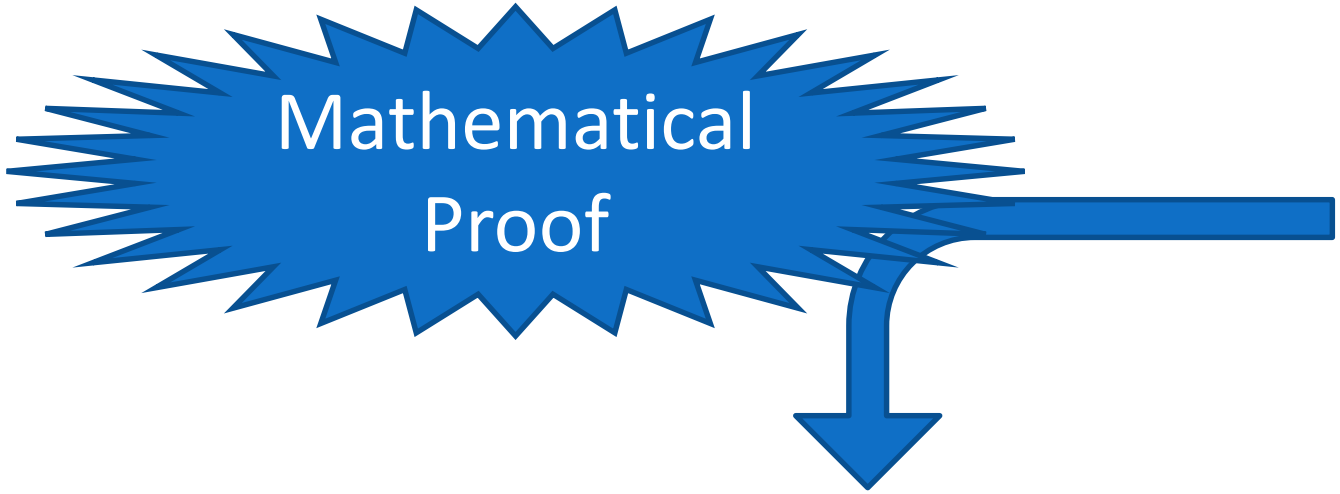
Homomorphic Tallying

Voter Name	Vote	
Alice Smith	<1,0;1,0;0,1;0,0,1>	X37BM6YPM
Bob Williams	<0,1;0,1;0,1;0,1,0>	2J8CNF2KQ
Carol James	<0,1;0,0,1;1,0,1;0,1,0>	VRSF5JQWZ
David Fuentes	<1,0;1,0;0,1;0,0,1>	MW5B2VA7Y
Ellen Chu	<1,0;1,0;0,1;0,1,0>	8VPPS2L39
		⊕
Tally	<3,2,0;4,1;2,3;2,1,2>	**41R7DDY7M**

Homomorphic Tallying

Voter Name	Vote	
Alice Smith	<1,0,0;1,0;0,1;0,0,1>	X37BM6YPM
Bob Williams	<0,1,0;1,0;1,0;1,0,0>	2J8CNF2KQ
Carol James	<0,1,0;0,1;1,0;1,0,0>	VRSF5JQWZ
David Fuentes	<1,0,0;1,0;0,1;0,0,1>	MW5B2VA7Y
Ellen Chu	<1,0,0;1,0;0,1;0,1,0>	8VPPS2L39
	+	⊕
Tally	<3,2,0;4,1;2,3;2,1,2>	**41R7DDY7M**

A Secret-Ballot E2E-V Election



X37BM6YPM
2J8CNF2KQ
VRSF5JQWZ
MW5B2VA7Y
8VPPS2L39

Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

Totals	
Jefferson	3
Adams	2

A Secret-Ballot E2E-V Election

Voter Name	Vote	
Alice Smith	Jefferson	X37BM6YPM
Bob Williams	Adams	2J8CNF2KQ
Carol James	Adams	VRSF5JQWZ
David Fuentes	Jefferson	MW5B2VA7Y
Ellen Chu	Jefferson	8VPPS2L39

Totals	
Jefferson	3
Adams	2

Current Technology

This is not speculative new technology.

- The basic techniques have existed for decades …

  … and there are several ways to realize them.

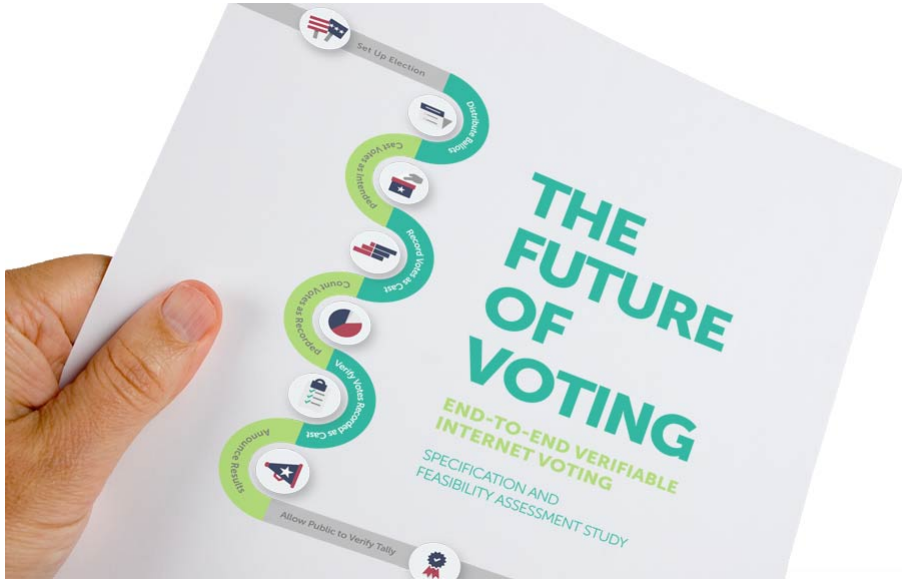
- But new refinements are now making this practical …

  … just at a time when the need is being appreciated.

Real-World Deployments

- Helios (www.heliosvoting.org) – Adida and others
  - Used to elect president of UC Louvain, Belgium.
  - Used in Princeton University student government.
  - Used by ACM, IACR, and other professional societies.
- Scantegrity II (www.scantegrity.org) – Chaum, Rivest, many others
  - Used for 2009 & 2011 municipal elections in Takoma Park, MD.
- STAR-Vote – Benaloh, Byrne, Eakin, Kortum, McBurnett, Pereira, Stark, Wallach
  - Designed for use in Travis County, Texas.

2015 U.S. Vote Foundation study



Internet voting in public elections should *never* be done *without* E2E-verifiability.

New (draft) 2018 EAC standards (VVSG):

U.S. Election Assistance Commission

Compliant systems must *either* be paper-based *or* E2E-verifiable.

Public vs. Administrative Audits

- Administrative (risk-limiting and Bayesian) audits are
  - vulnerable to careless/malicious administrators
  - more cumbersome to administer
- Public (E2E-verifiable) audit systems are
  - harder to build
  - harder to understand and explain

Audit Technology Comparison

Voting Medium	RLAs and Bayesian Audits	E2E-verifiability
In-person, hand-marked paper	✓	✓
In-person, BMDs	✓	✓
In-person, paperless	✗	✓
Vote-by-Mail	✓	✗
Internet voting	✗	✓

Thank you.

What About Blockchain Voting?

Can blockchain technology be used to enable secure online voting?

Applications of Blockchains

- Distributed Currency
- Contracts
- Distributed Public Ledger Applications
- Voting?

Blockchains and Elections

- Elections have central authorities.
  - Set the ballot contents
  - Set and maintain eligibility requirements
  - Set start/end time of election
- Note that authority need not be trusted!

Blockchains and Elections

An election’s designated central authority can simply post the same information (digitally signed) on a public web site.

Blockchains and Elections

- Blockchains do not provide anonymity and authentication.
- These can be provided with cryptography.
- But once the cryptography is added, the blockchains become superfluous.

Blockchains and Elections

Blockchains don’t solve fundamental problems with online voting.

- Client malware can change votes.
- Targeted DoS can disenfranchise voters.
- Voters are subject to coercion.

Blockchains and Elections

Blockchains create new problems.

- There is no accountability.
- There is no certainty.
- A mining majority has total control.

Variations?

Not all blockchains look like bitcoin.

- *Private* rather than *public* blockchains
- Proof of *stake* rather than proof of *work*
- *DAGs* rather than *chains*