Securing Digital Democracy

Lecture 9 | *Using Technology Wisely*

J. Alex Halderman
University of Michigan

Criteria

Transparency

Voters can **observe** and **understand** the process.

A fully transparent election system supports **accountability** as well as **public oversight**, **comprehension** and **access** to the entire process.

Definitions adopted from Joseph Lorenzo Hall
http://josephhall.org/papers/jhall-phd.pdf

Verifiability

Voters have means to convince themselves that the outcome is correct **without having to blindly trust** the technology or the election authorities.

Auditability

The system can be **manually checked** after the election to ensure that the votes have been counted properly.

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.

See: Rivest and Wack, "On the Notion of Software Indepdence in Voting Systems"
http://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

Post-Election Auditing

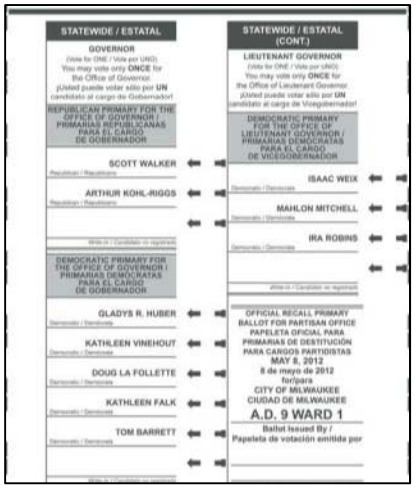
Manual Recounts

What?

When?

Cost?

Redundant Records



AUDIT =?

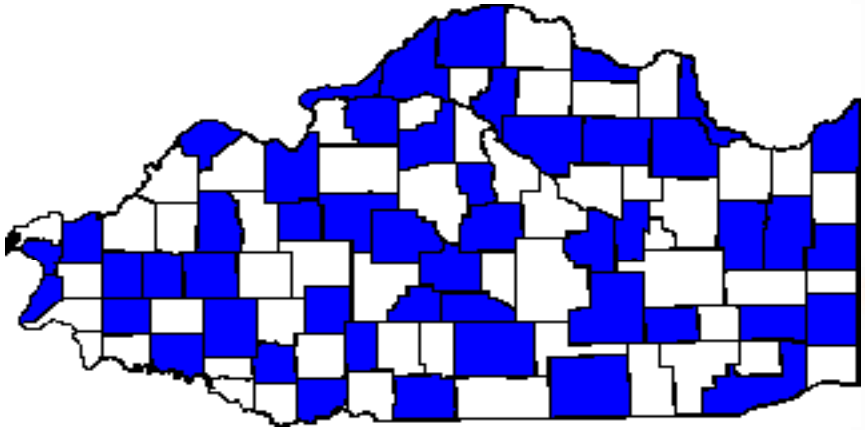
Slow/ex … tally

Redundancy + Different failure modes = Greater security

Verified by voter … Unverified

But…Redundancy only helps if we use both records!

Post-Election Audits



Pick some precincts **randomly** for paper recount.

If electronic tallies disagree, recount everywhere.

How much to Audit?

Standard practice:

Fixed Fraction of Precincts
(e.g., 10%)

Recommended practice:

Fixed Level of Confidence
(e.g., 99%)

Statistical Risk-Limiting Audits

Establish, with high statistical confidence, that hand-counting *all* of the paper records would yield the same winner as the electronic tally.

Audit Example

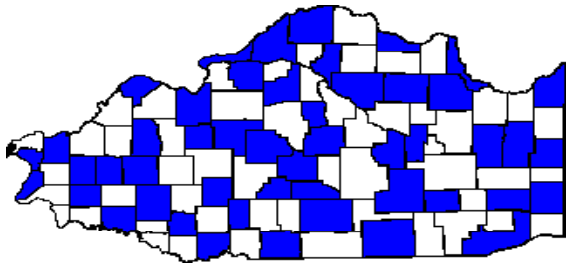
Goal: Reject hypothesis that ≥ 5% of ballots differ between electronic and paper

For 95% confidence, hand-audit 60 precincts

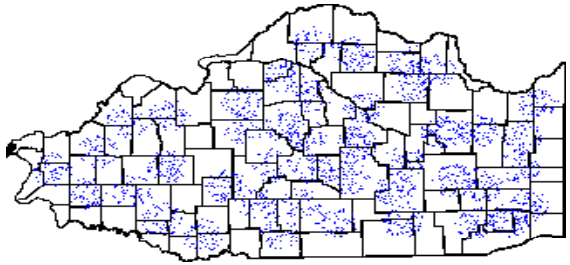
Cost: about $100,000

An Alternative Approach

Precinct-based auditing
(standard practice)



Ballot-based auditing



100 marbles, 10% blue

6300 beads, 10% blue

How large a sample do we need to detect an error?

Example due to Andrew Appel. http://www.cs.princeton.edu/~appel/voting/

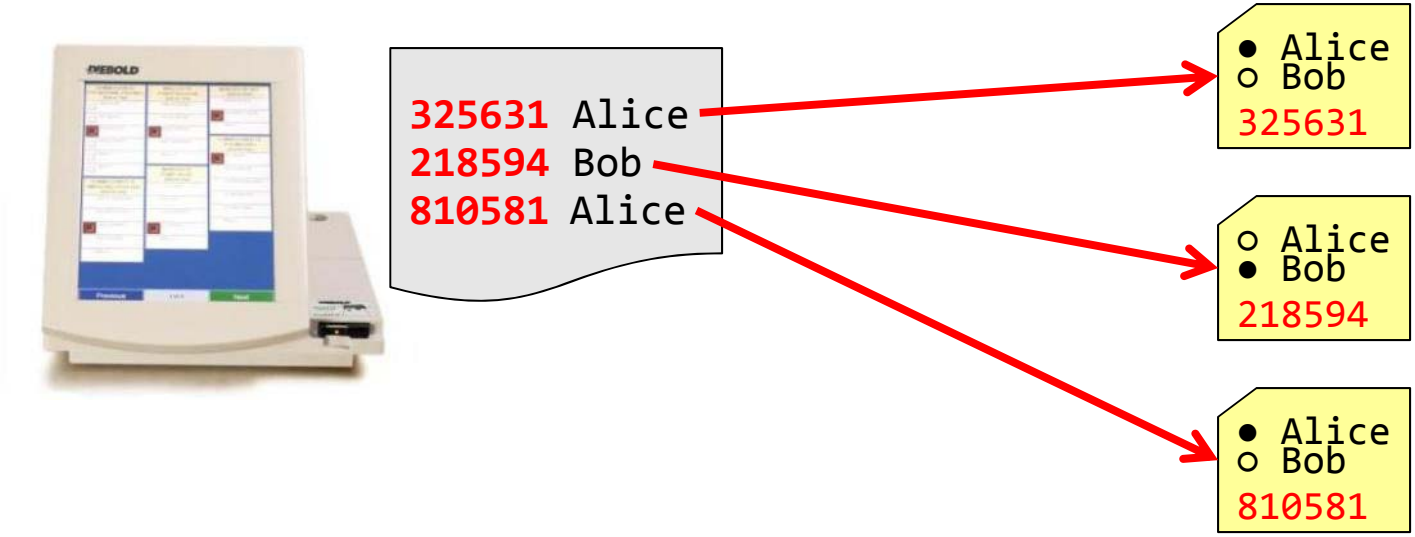
Audit Example

Goal: Reject hypothesis that ≥ 5% of ballots differ between electronic and paper

For 95% confidence, hand-audit 60 ~~precincts~~ ballots

Cost: about ~~$100,000~~ $1,000

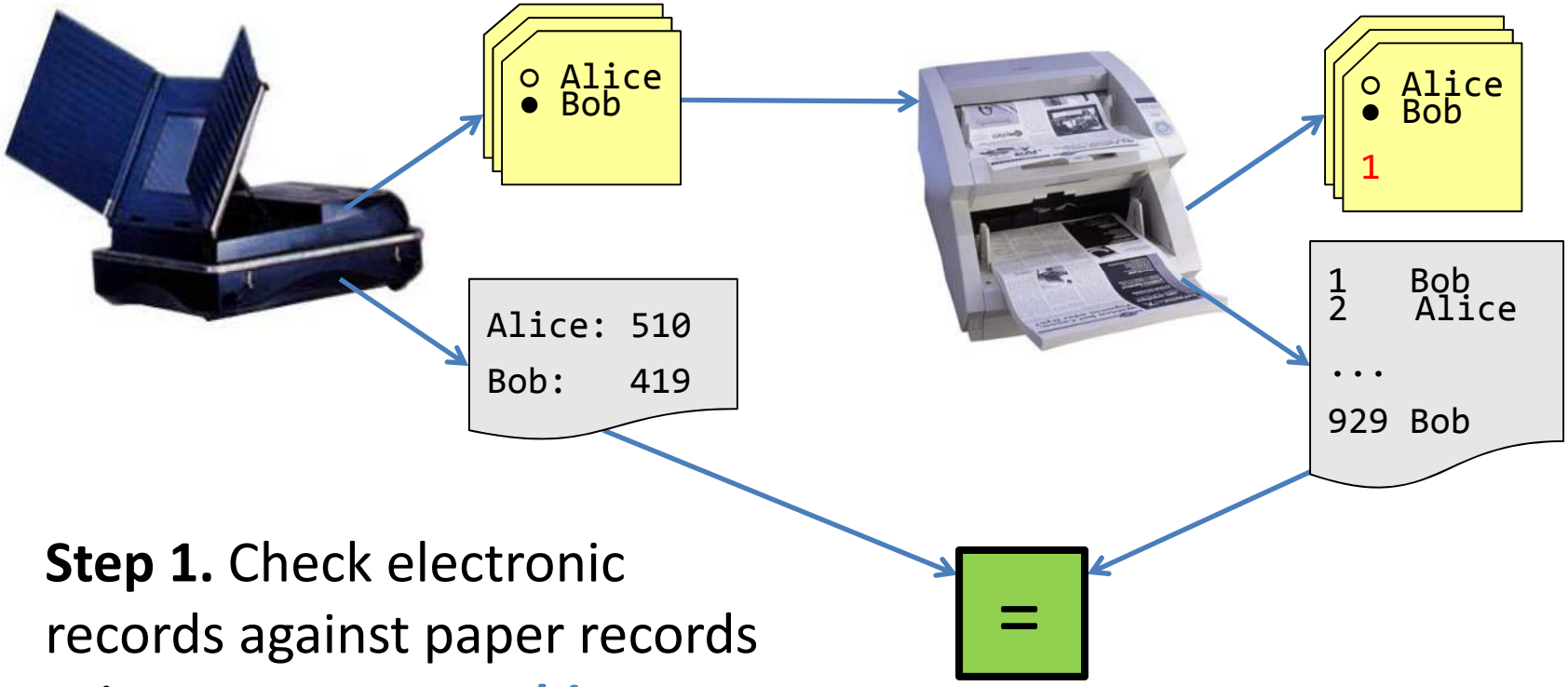
Why Not Ballot-based?



Need to match up electronic with paper ballots.

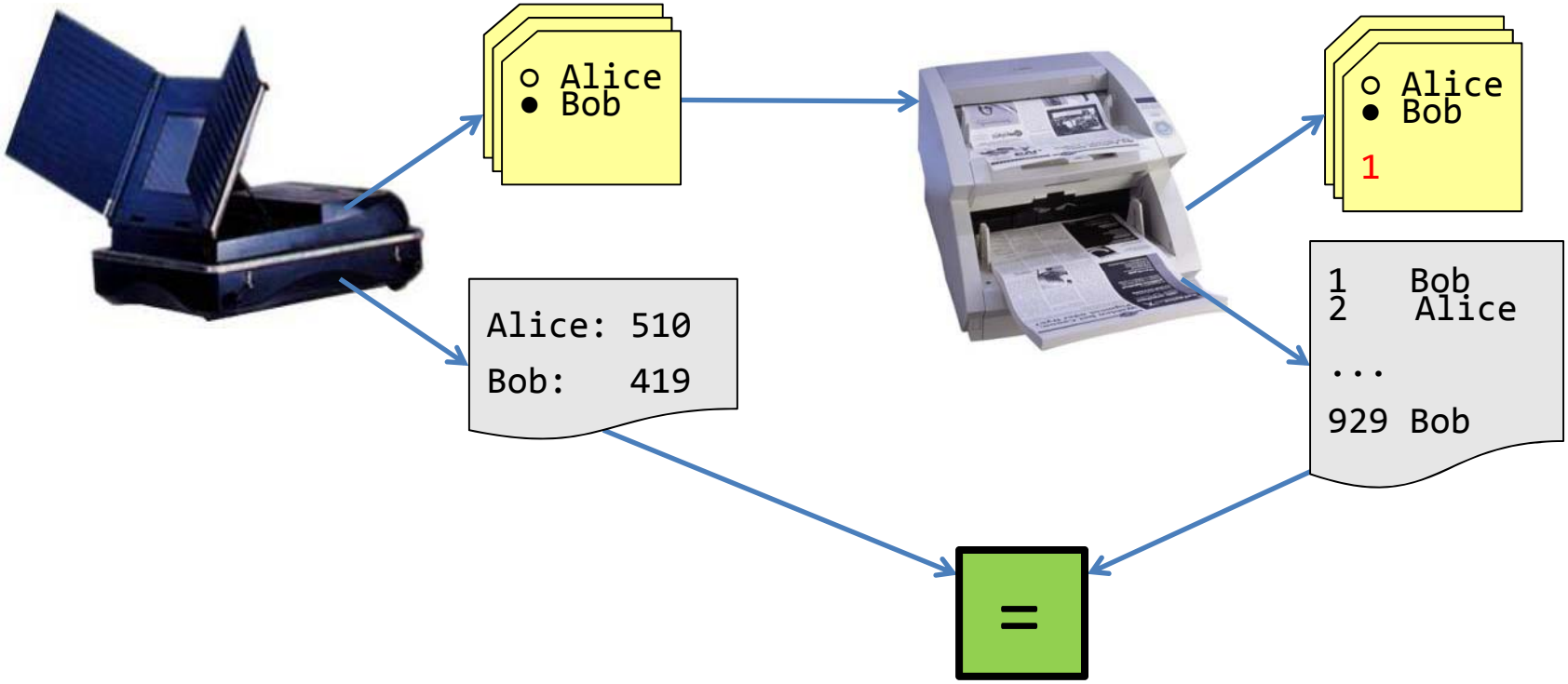
Difficult without compromising the secret ballot!

Machine-Assisted Auditing

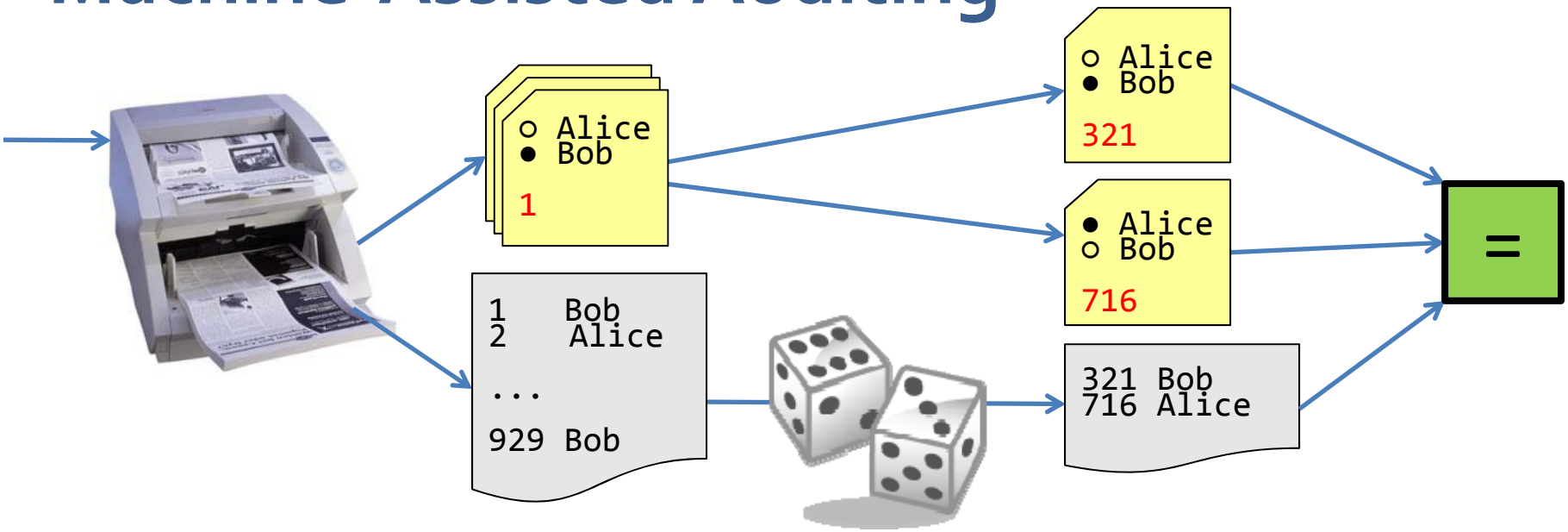


Step 1. Check electronic records against paper records using a **recount machine**.

Machine-Assisted Auditing

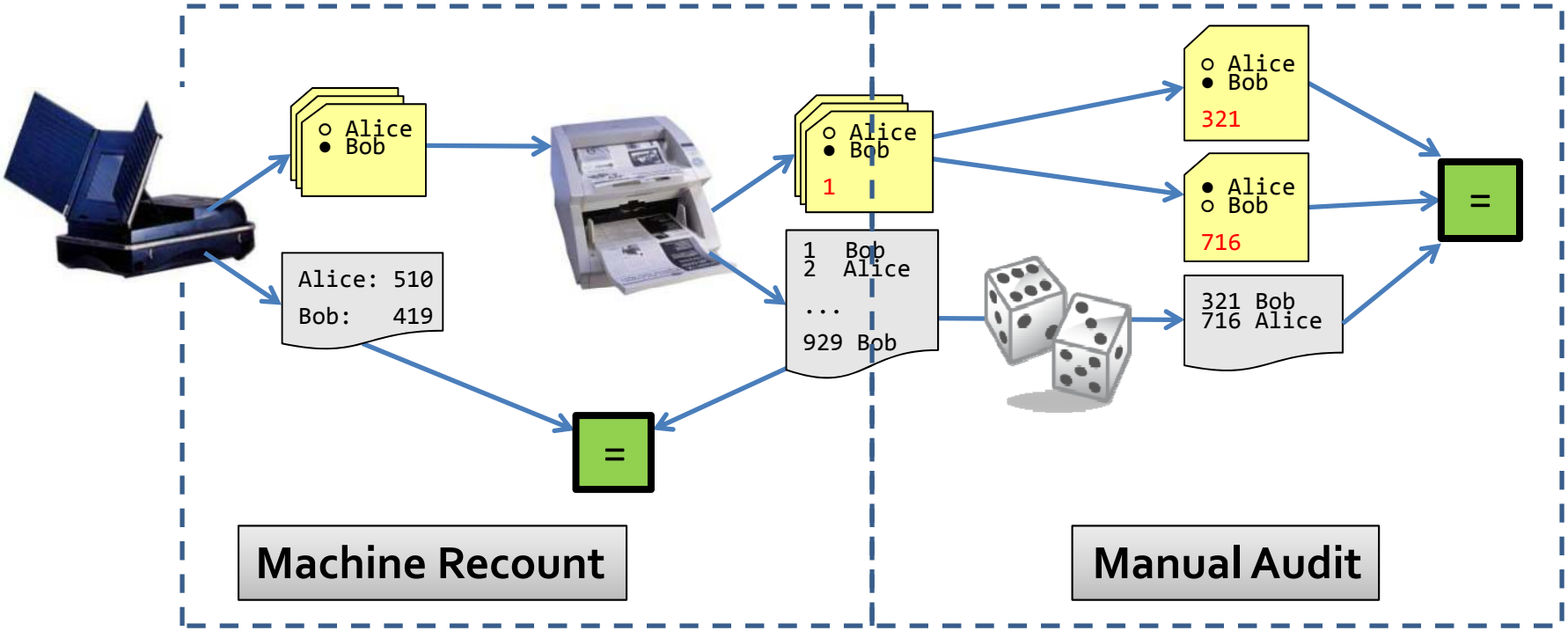


Machine-Assisted Auditing



Step 2. Audit the recount machine by selecting random ballots for human inspection.

Machine-Assisted Auditing



We can use a machine without having to trust it!

More Efficient Audits

2006 Virginia U.S. Senate race
0.3% margin of victory
We want 99% confidence

	Precinct Based	**Machine Assisted**
# Ballots	1,141,900	**2,339**
# Precincts	1,252	**1,351**

See Calandrino, Halderman, and Felten, "Machine-Assisted Election Auditing." EVT 2007.
https://jhalderm.com/pub/papers/audit-evt07.pdf

The Gold-Medal Standard

Precinct-Count Optical Scan

+

Mandatory Risk-Limiting Audits

End-to-End Verifiable Voting

This segment adapted from Josh Benaloh, with permission.

9.3 End-to-End Verifiable Voting

End-to-End (E2E) Voter-Verifiability

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.

Not a secret ballot!

Alice Johnson, 123 Main . . **YES**
Bob Ramirez, 79 Oak . . . . . **NO**
Carol Wilson, 821 Market . **NO**

End-to-End Voter-Verifiability

As a voter, I can be sure that:

- My vote is cast as I intended.
- My vote is counted as cast.
- All votes are counted as cast.
- No voter can demonstrate how he or she voted to a third party.

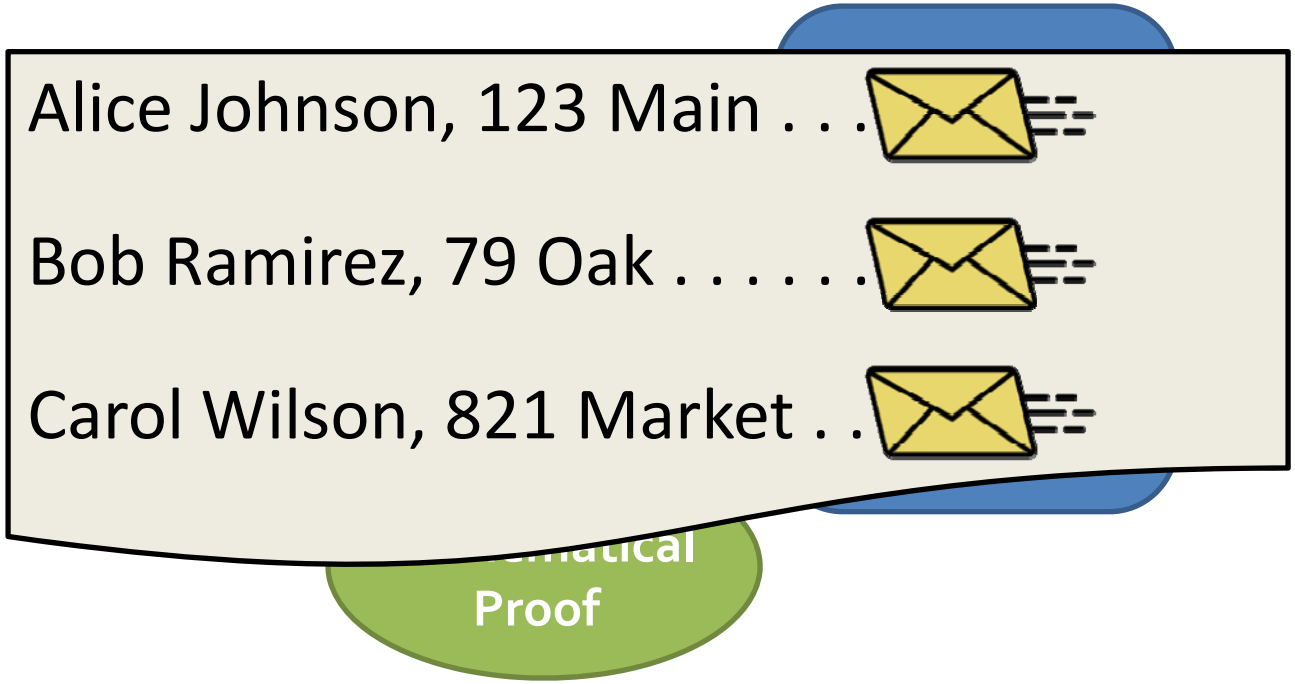
A Verifiable Receipt

Alice Johnson, 123 Main . . .

Bob Ramirez, 79 Oak . . . . . .

Carol Wilson, 821 Market . .

Checking the Result



End-to-End Verifiable Elections

Anyone who cares to do so can:

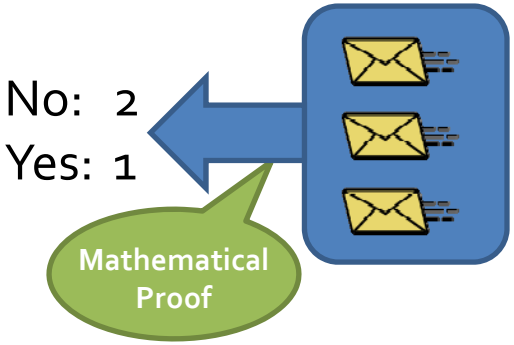
Check that their own encrypted votes are correctly listed.

Alice Johnson, 123 Main .

Bob Ramirez, 79 Oak . . . .

Carol Wilson, 821 Market

Check that other voters are legitimate.



Check the mathematical proof of the correctness of the tally.

The Voter's Perspective

Voters can …

- Use their receipts to check that their results are properly recorded.
- Throw their receipts in the trash.

- Verify the accuracy of the election with apps they wrote themselves.
- Download apps from sources of their choice to verify the election.
- Believe verifications done by their political parties.
- Accept the results without question.

Lots of Details to Get Right!

How do voters know that their **receipt matches their choices?**

How are voters convinced that the published encrypted votes **correspond to the announced tally?**

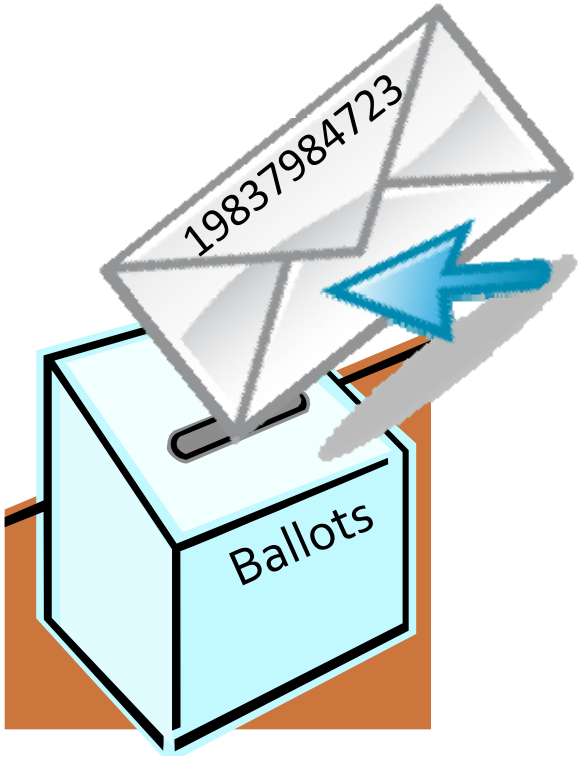
Voter-Initiated Auditing

Encrypted Vote

Voter's choice: **Cast** or **Challenge**

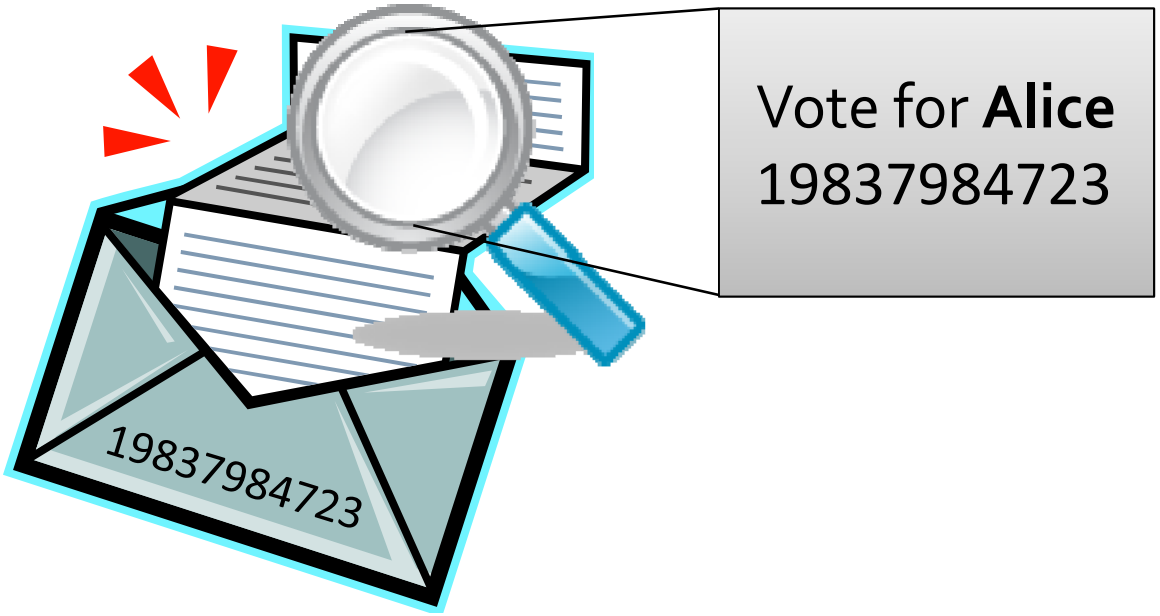
Voter-Initiated Auditing

Cast



Voter-Initiated Auditing

Challenge

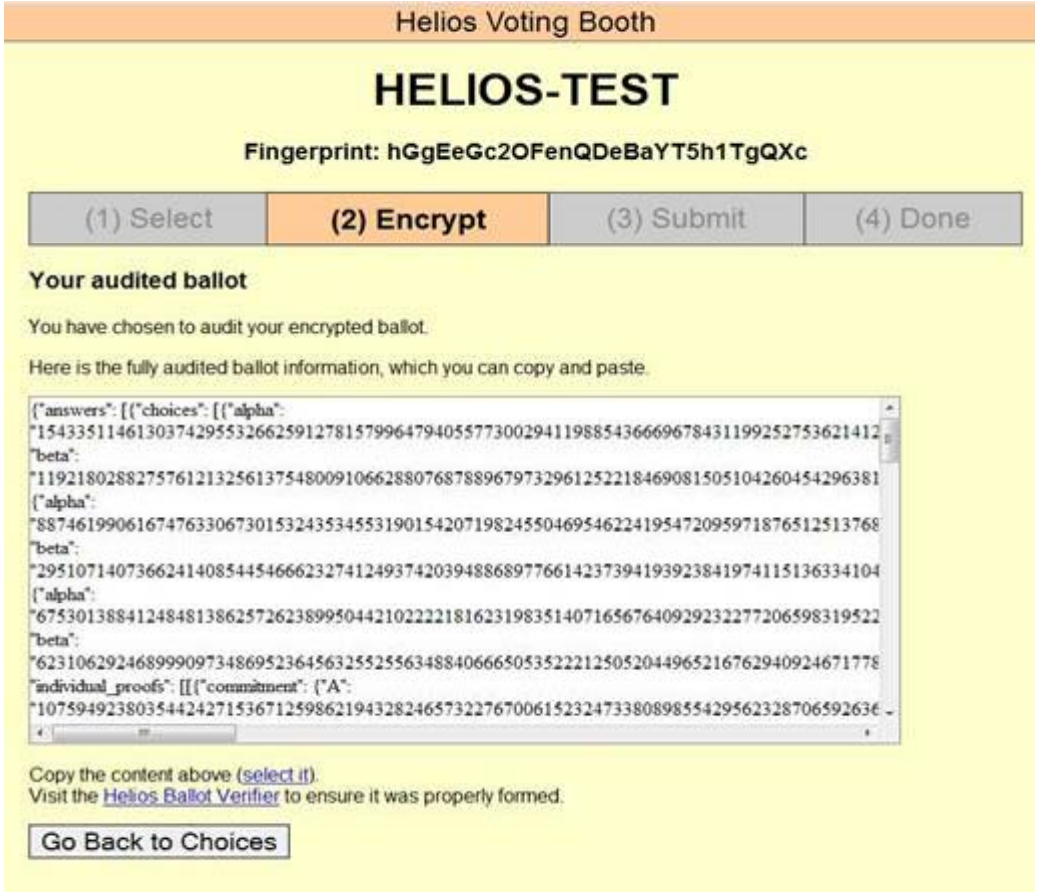


Scantegrity

Optical Scan + E2E

http://www.scantegrity.org/

Helios

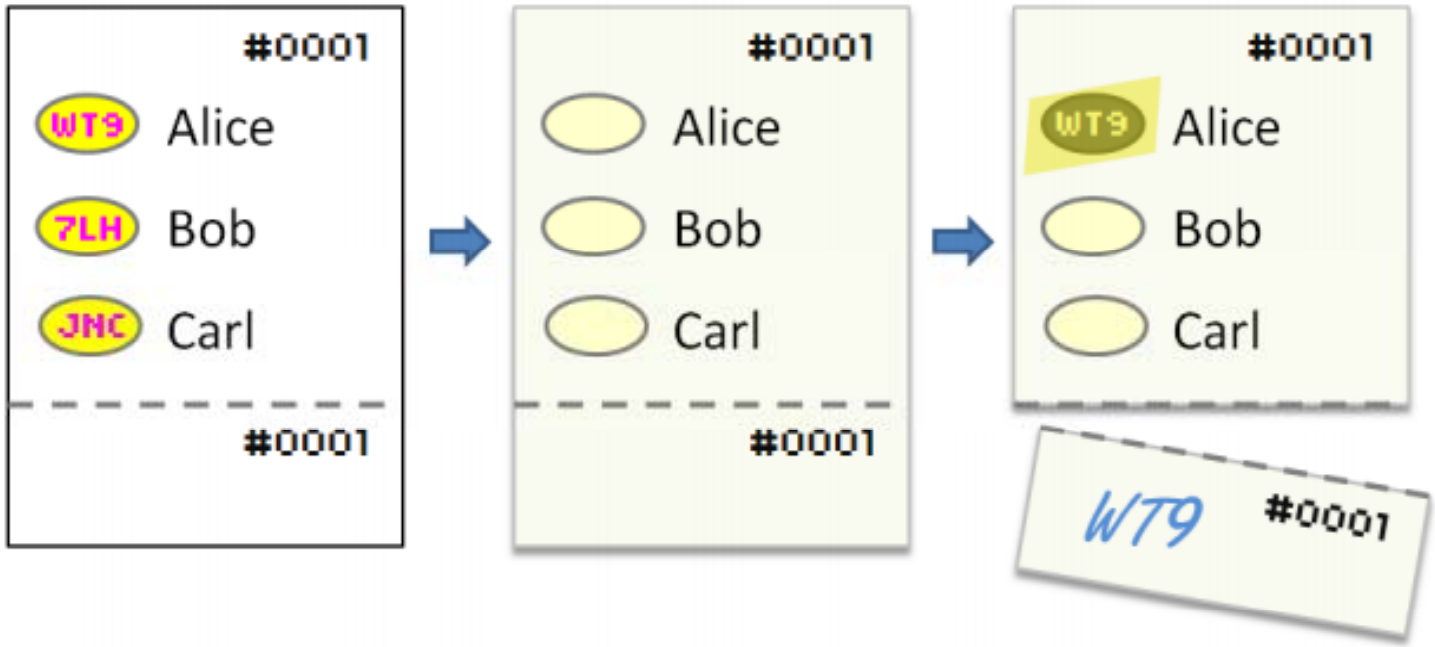


E2E Internet Voting

http://heliosvoting.org/

Verifying an E2E Result

Scantegrity



See: Chaum, et al., "Scantegrity II: End-to-End Verifiability for Optical Scan Election Systems using Invisible Ink Confirmation Codes". EVT 2008.
http://static.usenix.org/event/evt08/tech/full_papers/chaum/chaum.pdf

Verifiable Tallying

Confirmation Code Table

Ballot	A	B
B1	7LC	WTX
B2	J31	TC0
B3	KWA	H7L

Correspondence Table

	VOTE?	
B3:A		R2:YES
B1:B		R3:NO
B2:A		R1:YES
B1:A		R2:NO
B2:B		R1:NO
B3:B		R3:YES

Voted Choice Table

Result	YES	NO
R1		
R2		
R3		

Verifiable Tallying

Confirmation Code Table

	Ballot	A	B
Yes	B1	7LC	WTX
No	B2	J31	TC0
No	B3	KWA	H7L

Correspondence Table

	VOTE?	
B3:A		R2:YES
B1:B		R3:NO
B2:A		R1:YES
B1:A	X	R2:NO
B2:B	X	R1:NO
B3:B	X	R3:YES

Voted Choice Table

Result	YES	NO
R1		✓
R2		✓
R3	✓	

Verifiable Tallying

Confirmation Code Table

Ballot	A	B
B1	7LC	
B2		TC0
B3		H7L

Correspondence Table

	VOTE?	
	X	
	X	
	X	

Voted Choice Table

Result	YES	NO
R1		✓
R2		✓
R3	✓	

No: 2
Yes: 1

Verifiable Tallying

Confirmation Code Table

Ballot	A	B
B1	7LC	
B2		TC0
B3		H7L

Correspondence Table

	VOTE?	
B3:A		R
		R3:NO
		R1:YES
B1:A	X	R
	X	R1:NO
B3:B	X	R

Voted Choice Table

Result	YES	NO
R1		✓
R2		✓
R3	✓	

Check that revealed codes are marked with an X

Check that voted choices are marked with an X

Questions for E2E?

Complexity?

Usability?

Comprehensibility?

Security?

Securing Digital Democracy

Lecture 9 | *Using Technology Wisely*

J. Alex Halderman
University of Michigan