Security of Voting Systems

Ronald L. Rivest

MIT CSAIL

Given at:

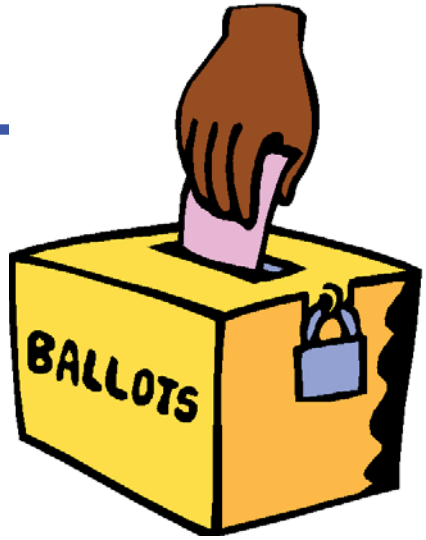
Collège de France

March 23, 2011

Outline

- Voting technology survey
- What is being used now ?
- Voting Requirements
- Security Threats
- Security Strategies and Principles
- New voting systems proposals: "Twin" and "Scantegrity II"

Voting Tech Survey

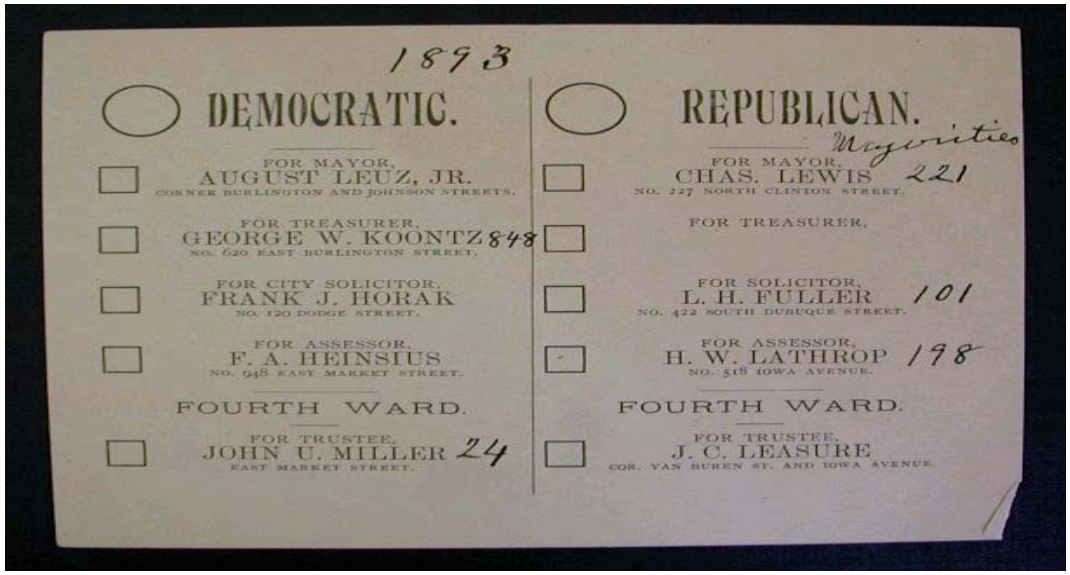


- Public voting
- Paper ballots
- Lever machines
- Punch cards
- Optical scan
- DRE (Touch-screen)
- DRE + VVPAT (paper audit trail)
- Vote by mail (absentee voting)
- Internet voting (?)
- *New voting methods ("end-to-end"), involving invisible ink, multiple ballots, scratch-off, cryptography, and other innovations…*

Public Voting

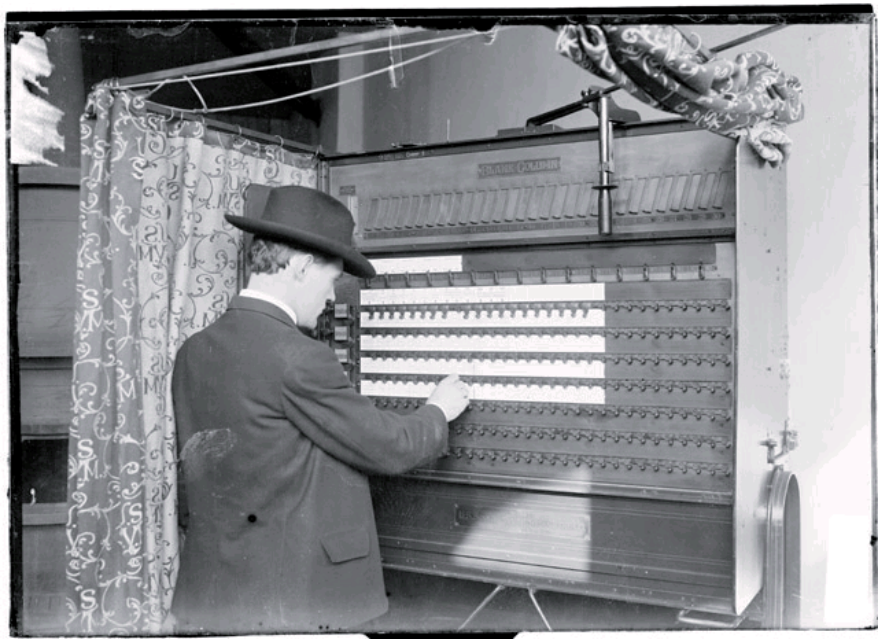
The County Election. Bingham. 1846.

Paper Ballots



- Lincoln ballot, 1860, San Francisco
- "Australian ballot", 1893, Iowa city

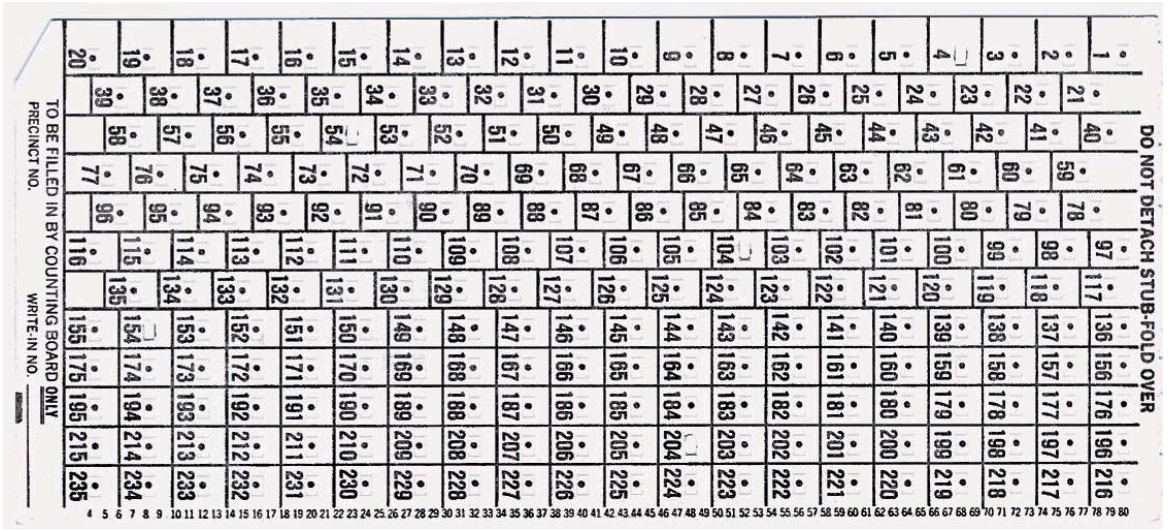
Lever Machines



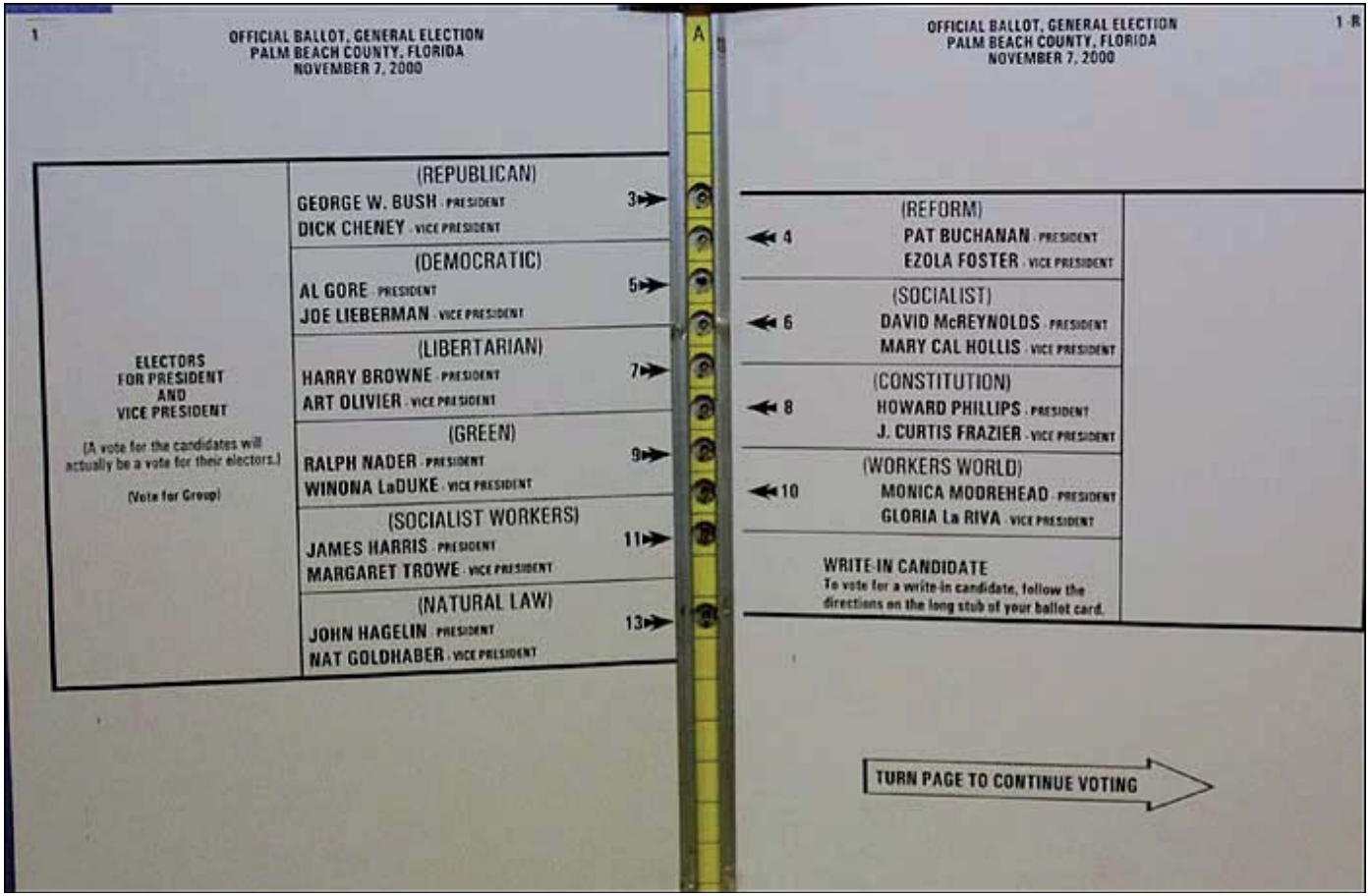
- Invented in 1892.
- Production ceased in 1982.
- See "Behind the Freedom Curtain" (1957)

Punch card voting

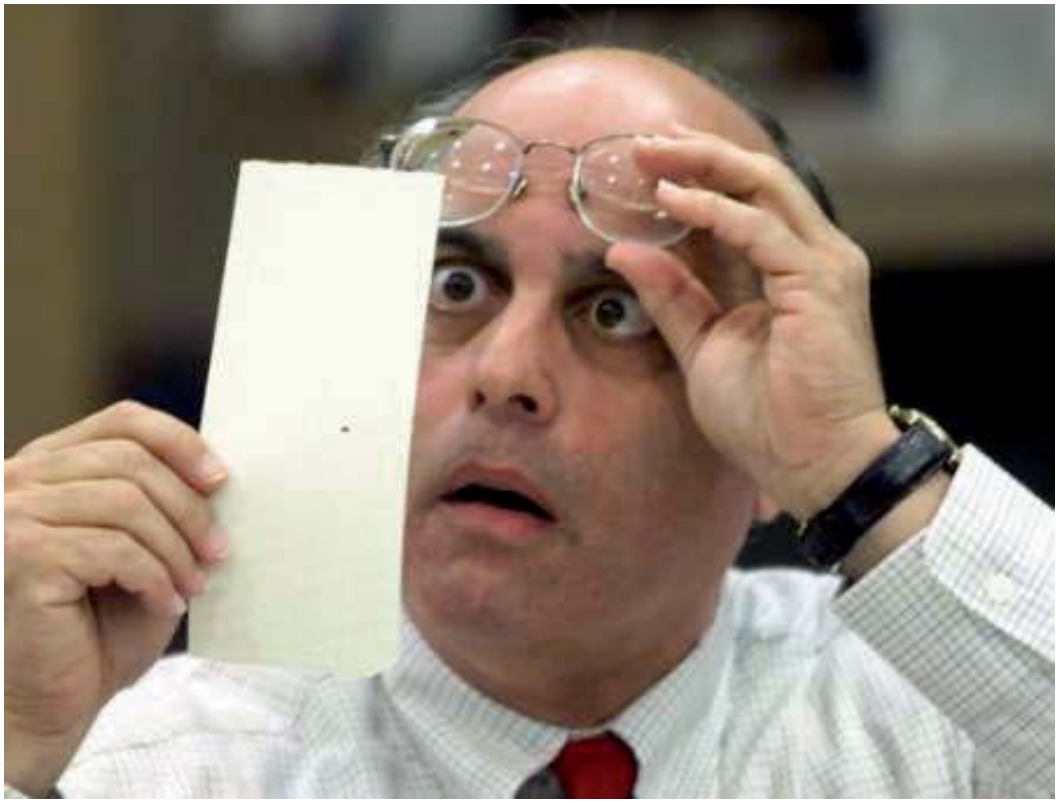
- Invented 1960's, based on computerized punch card.
- Now illegal, by HAVA (Help America Vote Act) of 2002.



The famous "butterfly ballot"



A "dimpled chad" ???



Optical scan ("opscan")

OFFICIAL BALLOT

CONSOLIDATED GENERAL ELECTION

SANTA BARBARA COUNTY, CALIFORNIA

NOVEMBER 5, 2002

INSTRUCTIONS TO VOTERS: To vote for the candidate of your choice, completely fill in the OVAL to the LEFT of the candidate's name. To vote for a person whose name is not on the ballot, darken the OVAL next to and write in the candidate's name on the Write-in line. To vote for a measure, darken the OVAL next to the word "Yes" or the word "No". All distinguishing marks or erasures are forbidden and make the ballot void. If you tear, deface, or wrongly mark this ballot, return it and get another. VOTE LIKE THIS: ● **VOTE BOTH SIDES**

STATE

GOVERNOR
Vote for One

- ◯ GARY DAVID COPELAND — Chief Executive Officer — Libertarian
- ◯ BILL SIMON — Businessman/Charity Director — Republican
- ◯ REINHOLD GULKE — Electrical Contractor/Farmer — American Independent
- ◯ GRAY DAVIS — Governor of the State of California — Democratic
- ◯ IRIS ADAM — Business Analyst — Natural Law
- ◯ PETER MIGUEL CAMEJO — Financial Investment Advisor — Green
- ◯ Write-In

LIEUTENANT GOVERNOR
Vote for One

- ◯ PAT WRIGHT — Ferret Legalization Coordinator — Libertarian
- ◯ PAUL JERRY HANNOSH — Educator/Businessman — Reform
- ◯ BRUCE MC PHERSON — California State Senator — Republican
- ◯ KALEE PRZYBYLAK — Public Relations Director — Natural Law
- ◯ CRUZ M. BUSTAMANTE — Lieutenant Governor — Democratic
- ◯ JIM KING — Real Estate Broker — American Independent
- ◯ DONNA J. WARREN — Certified Financial Manager — Green
- ◯ Write-In

INSURANCE COMMISSIONER
Vote for One

- ◯ DALE F. OGDEN — Insurance Consultant/Actuary — Libertarian
- ◯ DAVID I. SHEIDLOWER — Financial Services Executive — Green
- ◯ GARY MENDOZA — Businessman — Republican
- ◯ JOHN GARAMENDI — Rancher — Democratic
- ◯ STEVE KLEIN — Businessman — American Independent
- ◯ RAUL CALDERON, JR. — Health Researcher/Educator — Natural Law
- ◯ Write-In

MEMBER, STATE BOARD OF EQUALIZATION
2ND District
Vote for One

- ◯ TOM Y. SANTOS — Tax Consultant/Realtor — Democratic
- ◯ BILL LEONARD — State Lawmaker/Businessman — Republican
- ◯ Write-In

UNITED STATES REPRESENTATIVE
24TH District
Vote for One

- ◯ ELTON GALLEGLY — U.S. Representative — Republican

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE JUDITH M. ASHMANN be elected to the office for the term prescribed by law?
◯ YES ◯ NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION TWO

Shall ASSOCIATE JUSTICE KATHRYN DOI TODD be elected to the office for the term prescribed by law?
◯ YES ◯ NO

FOR PRESIDING JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION THREE

Shall PRESIDING JUSTICE JOAN DEMPSEY KLEIN be elected to the office for the term prescribed by law?
◯ YES ◯ NO

FOR ASSOCIATE JUSTICE, COURT OF APPEAL 2nd APPELLATE DISTRICT, DIVISION FOUR

Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law?
◯ YES ◯ NO

First used in 1962

DRE ("Touchscreen")

- Direct Recording by Electronics
- First used in 1970's
- Essentially, a stand-alone computer

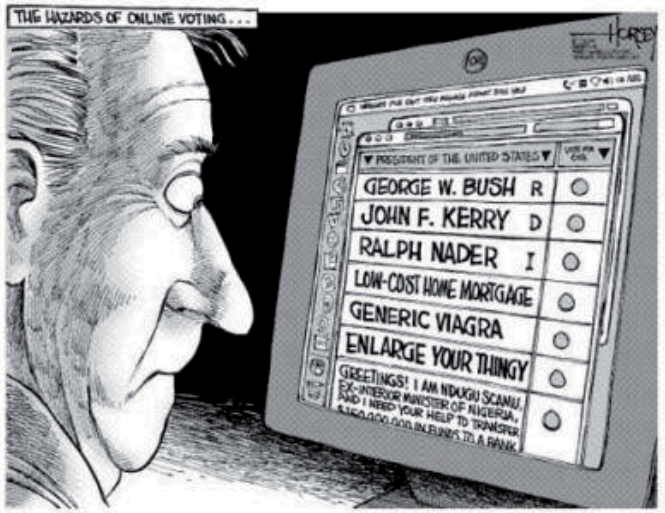
DRE + VVPAT

- DRE+Voter-Verified Paper Audit Trail.
- First used in 2003.

Vote By Mail

- Often used for absentee voting, but some states use it as default.
- Typically uses opscan ballots.

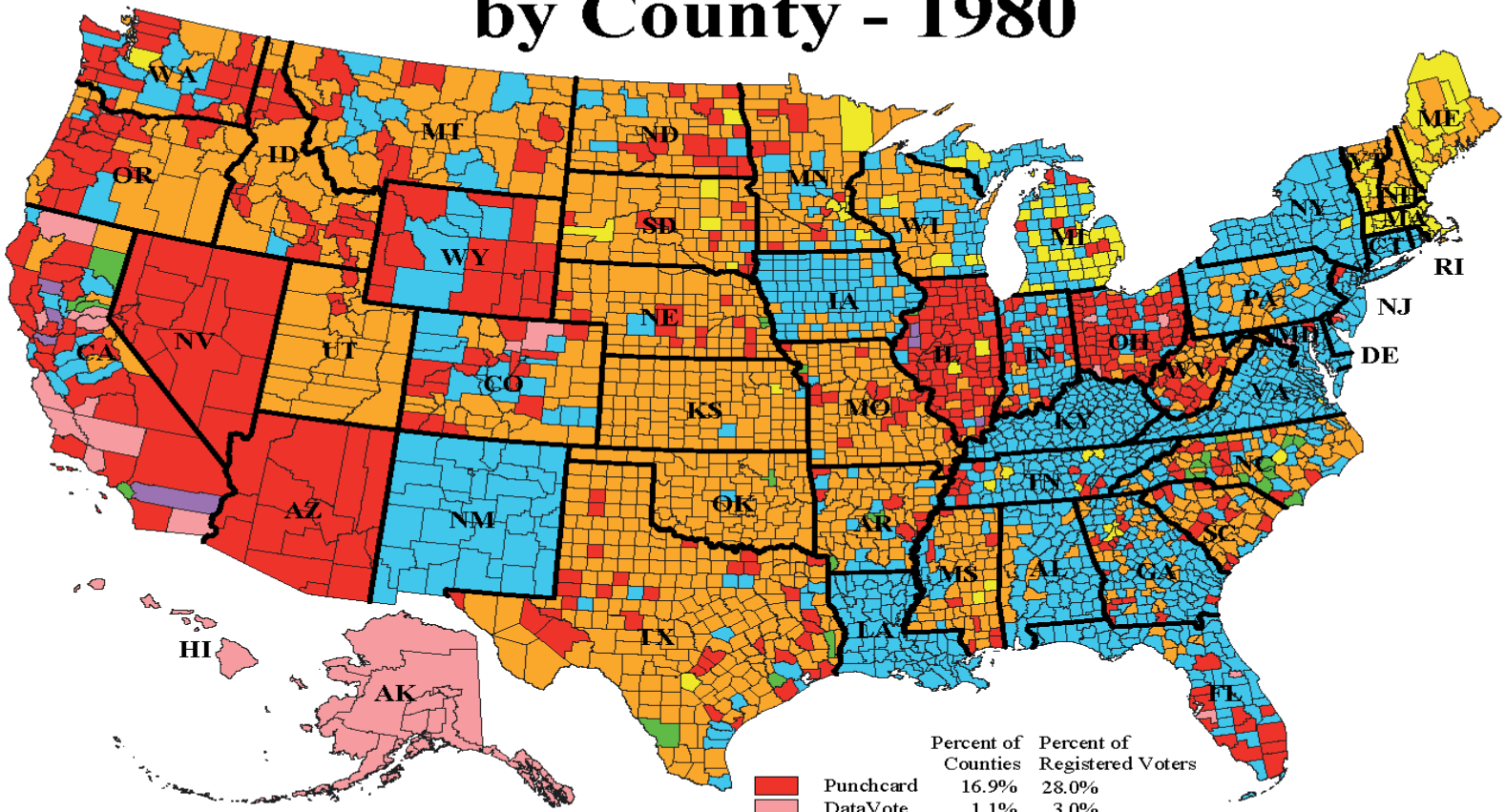
Internet voting (?)



- Risks combining the worst features of vote-by-mail (voter coercion) with the problems of DRE's (software security) and then adding new vulnerabilities (DDOS attacks from foreign powers?)…
- Why?? Because we can ?????
- Still, interesting experiments being carried out (e.g. Helios [Adida], Civitas [Clarkson/Chong/Myers]).

What is being used?

Type of Voting Equipment by County - 1980



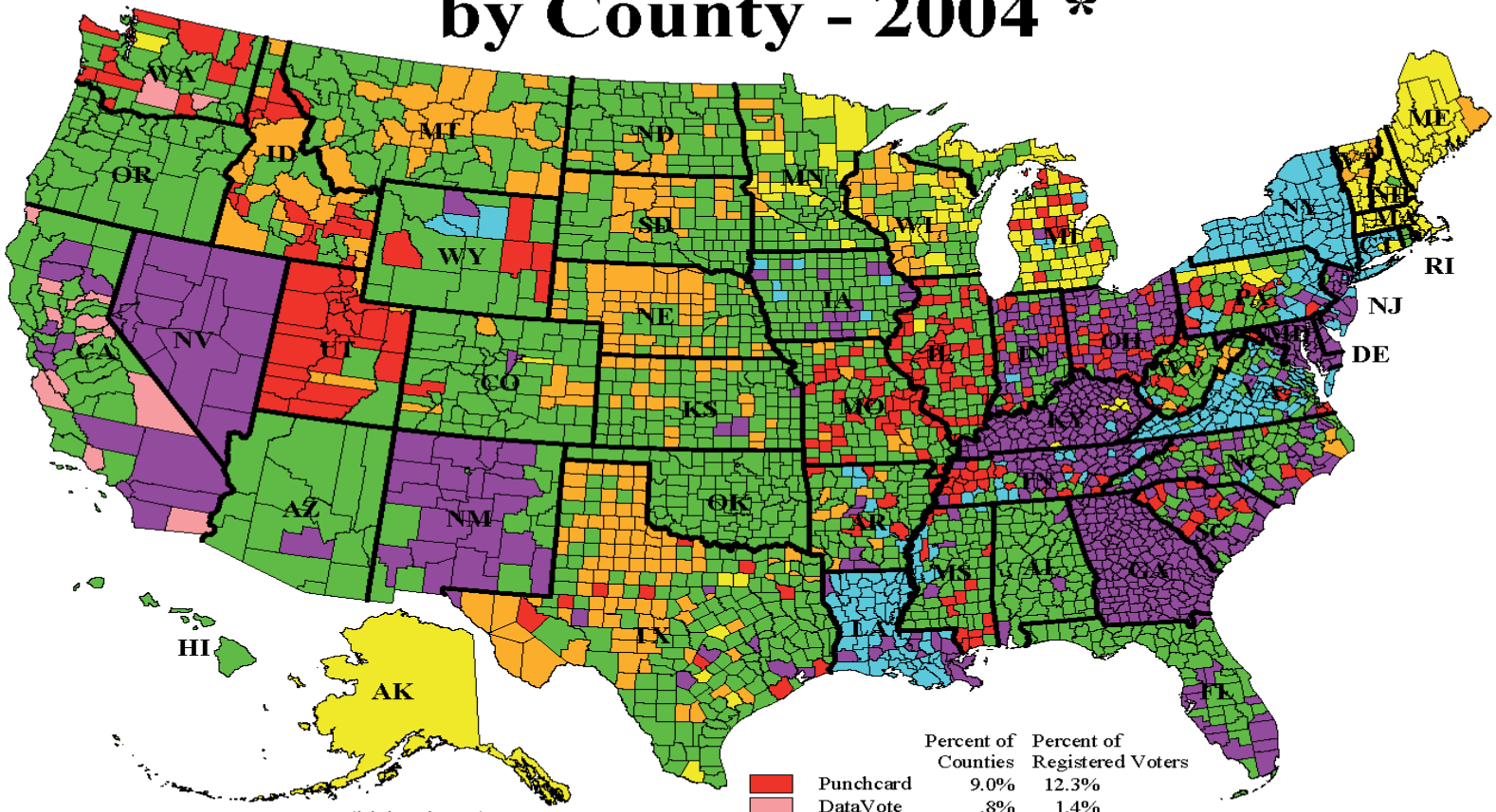
Alaska does not have counties.
Datavote system is used statewide
except for a few paper ballot precincts.

	Percent of Counties	Percent of Registered Voters
Punchcard	16.9%	28.0%
DataVote	1.1%	3.0%
Lever	36.9%	42.9%
Paper	41.0%	10.8%
Optical	.8%	2.1%
Electronic	.2%	.7%
Mixed Systems	3.0%	12.5%

Equipment used in the November 1980 election as reported by state election officials. The map shows equipment used at polling places, not necessarily absentee balloting.

Election Data Services
(202) 789-2004
1401 K Street NW, Suite 500
Washington, DC 20005-3417
www.ElectionDataServices.com

Type of Voting Equipment by County - 2004 *



Alaska does not have counties.
Accuvote system is used statewide
except for a few paper ballot precincts.

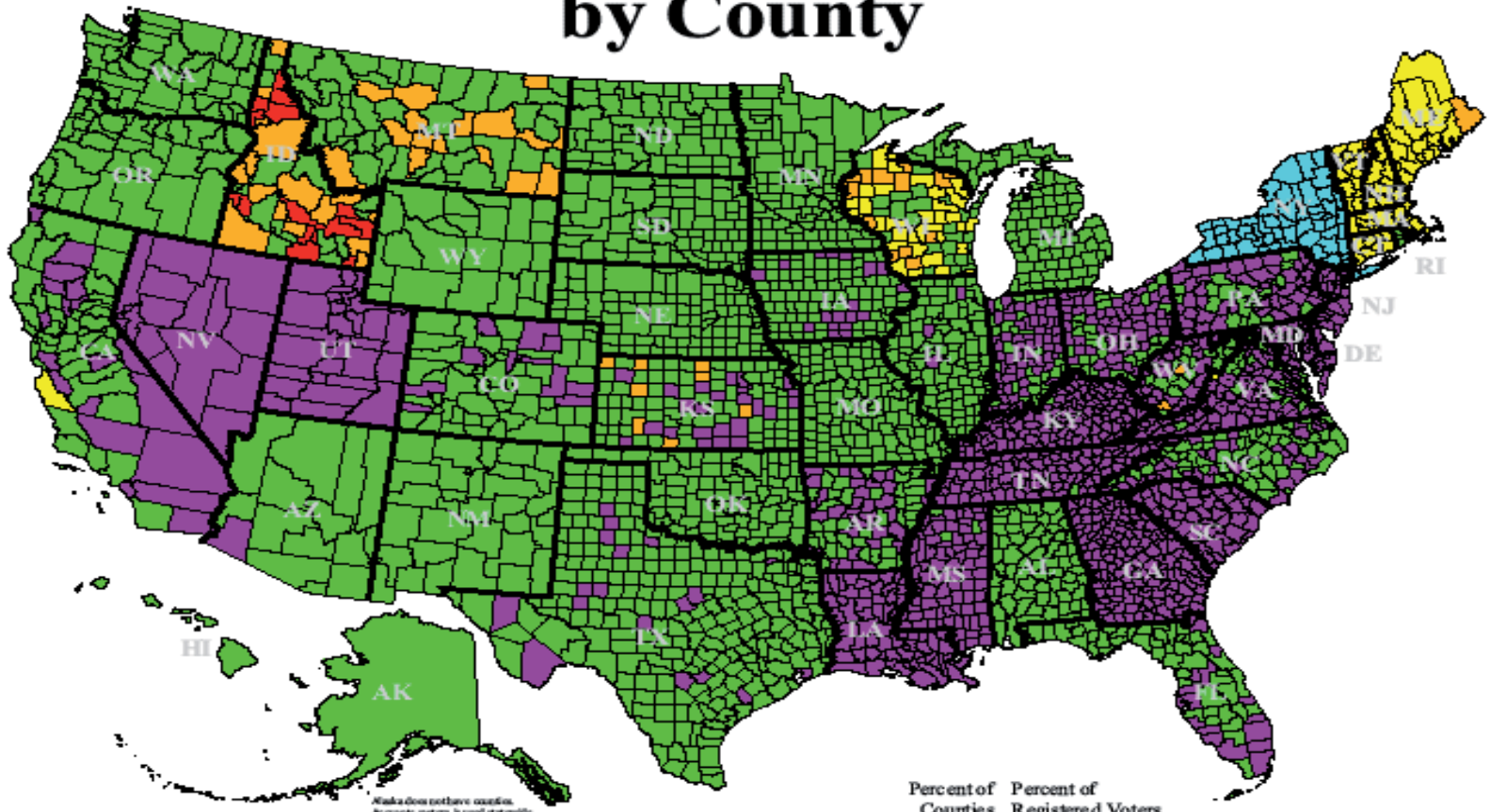
	Percent of Counties	Percent of Registered Voters
Punchcard	9.0%	12.3%
DataVote	.8%	1.4%
Lever	8.6%	13.9%
Paper	9.6%	.7%
Optical	45.4%	33.7%
Electronic	21.7%	30.8%
Mixed Systems	4.8%	7.2%

* Equipment expected to be used in the November 2004 election as reported by state election officials. The map shows equipment used at polling places, not necessarily absentee balloting.

*Printed with information available as of 5/3/2004.

Election Data Services
(202) 789-2004
1401 K Street NW, Suite 500
Washington, DC 20005-3417
www.ElectionDataServices.com

November 2006 Voting Equipment Usage by County



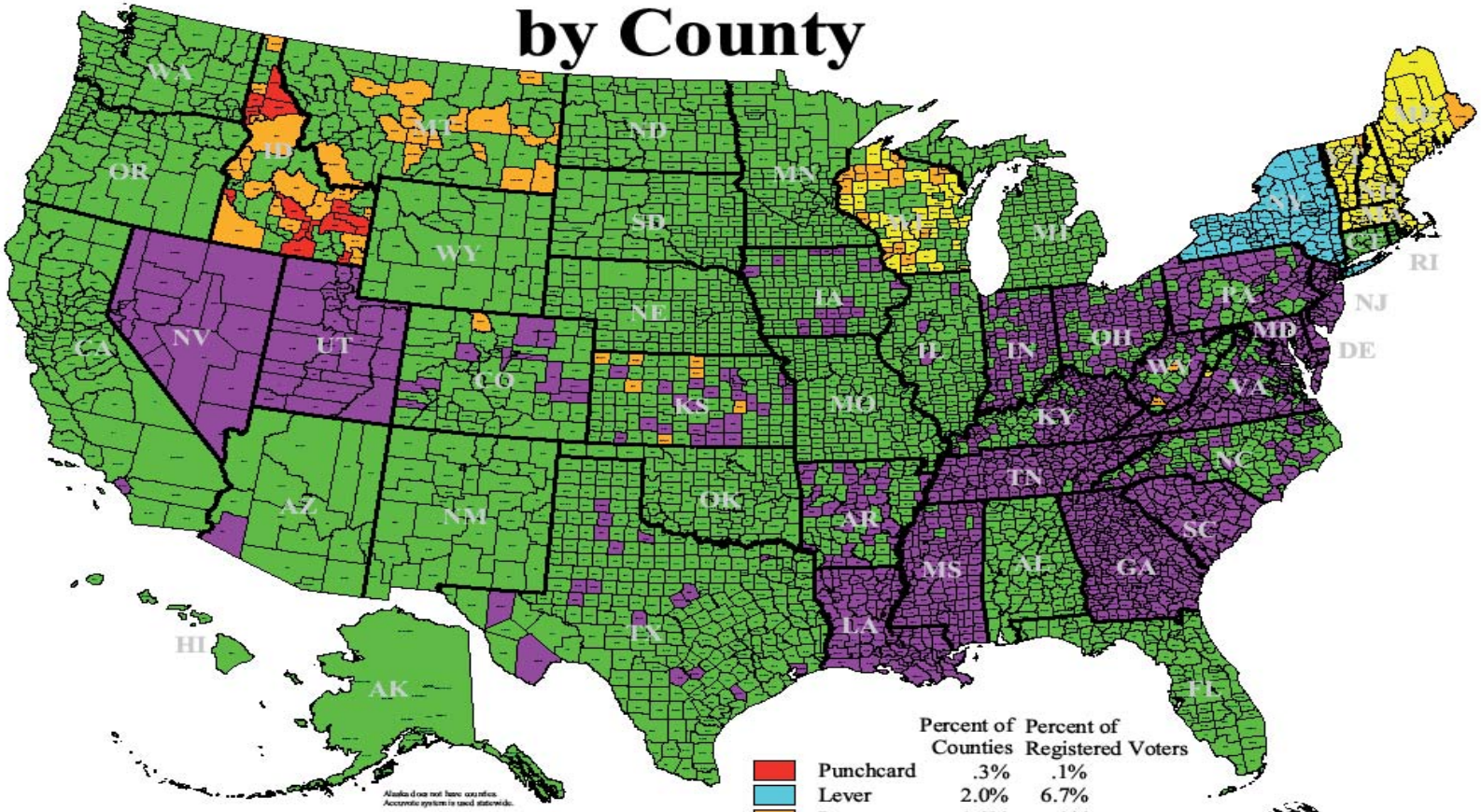
Alaska does not have counties. Accurate system is used statewide.

	Percent of Counties	Percent of Registered Voters
Punchcard	.4%	.2%
Lever	2.0%	6.8%
Paper	1.8%	.2%
Optical	56.2%	48.9%
Electronic	36.6%	38.3%
Mixed Systems	3.0%	5.5%

Equipment expected to be used in the November 2006 election as reported by state election officials. The map shows equipment used at polling places, not necessarily absentee or disabled balloting.

Election Data Services
(202) 789-2004
1400 I St NW, Suite 400
Washington, DC 20005
www.ElectionDataServices.com

November 2008 Voting Equipment Usage by County



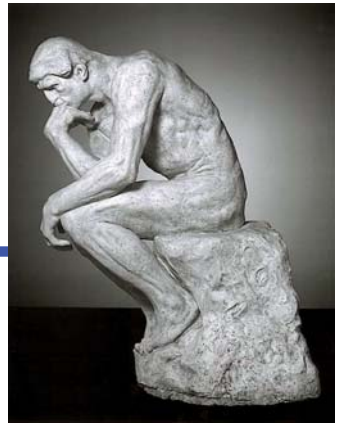
	Percent of Counties	Percent of Registered Voters
Punchcard	.3%	.1%
Lever	2.0%	6.7%
Paper	1.8%	.2%
Optical	58.9%	56.2%
Electronic	34.3%	32.6%
Mixed Systems	2.7%	4.2%

Equipment expected to be used in the November 2008 election as reported by state election officials and news media. The map shows equipment used at polling places, not necessarily absentee or disabled balloting.

Election Data Services
(202) 789-2004
6171 Emerywood Court
Manassas, VA 20112-3078
www.ElectionDataServices.com

Voting System Requirements

Voting is a hard problem



- **Voter Registration** - each eligible voter votes at most once
- **Voter Privacy** – no one can tell how any voter voted, even if voter wants it; no "receipt" for voter
- **Integrity** – votes can't be changed, added, or deleted; tally is accurate.
- **Availability** – voting system is available for use when needed
- **Ease of Use**
- **Accessibility** – for voters with disabilities
- **Assurance** – verifiable integrity

Security threats

Who are potential adversaries?

- Political zealots (want to fix result)
- Voters (may wish to sell their votes)
- Election officials (may be partisan)
- Vendors (may have evil "insider")
- Foreign powers (result affects them too!)

Really almost anybody!

Threats to Voting Security

- Dead people voting
- Ballot-box stuffing
- Coercion/Intimidation/Buying votes
- Replacing votes or memory cards
- Mis-counting
- Malicious software
- Viruses on voting machines
  - California top-to-bottom review found serious problems of this sort…
- … *See Brennan Center Report, "The Machinery of Democracy"…*

Some possible strategies…

Can't voter have a "receipt"?

- Why not let voter take home a "receipt" confirming how she voted?
- *A receipt showing her choices would allow a voter to sell her vote (or to be coerced).*
- Not acceptable!
- Note weakness in vote-by-mail…
- Need to ban cell-phone cameras!

Why not all-electronic voting?

- DRE's contain large amounts of software (e.g. 500,000 lines of code, not counting code for Windows CE, etc.)
- Software is exceedingly hard to build, test, and evaluate. Particularly if someone malicious is trying to hide their tracks.
- In the end, hard to provide assurance that votes are recorded as the voter intended.

Voter-Verified Paper Audit Trails

- Examples: opscan, DRE+VVPAT, electronic ballot markers
- Allow voter to verify, without depending on software, that at least one (paper) record of her vote is correct. This paper record is, of course, not taken home, but cast.
- Paper trail allows for *recounts* and *audits*.
- *Post-election audit* can compare statistical sample of paper ballots with corresponding electronic records.

Auditing (APR08 - Negexp)

- Margin of victory is *M*
- Precinct *i* has v_i voters?
- Adversary wants to pick precincts to corrupt with total size *M*
- Auditor wants 1-α chance of finding corruption of this size or larger.
- Audit precinct *i* with probability

$$1 - \alpha^{vi/M}$$

- Hand-count paper in precincts picked

Software Independence

- Notion introduced by TGDC for new voting system standards ("VVSG") for the EAC.
- TGDC = Technical Guidelines Development Committee
- VVSG = Voluntary Voting System Guidelines
  = federal certification standards
- EAC = Election Assistance Commission
- Proposed standard mandates that all voting systems be software independent.

Software Independence

- A voting system is "*software dependent*" if an undetected error in the software can cause an undetectable change in the reported election outcome.
- A voting system is "software independent" (SI) if it is not software dependent.
- With SI system, you can't rig election just by changing the software.
- VVPAT systems are SI.
- There are others (e.g. "end-to-end")

New voting system proposals

New voting systems: "end to end"

- Uses web so voter can check that her ballot was counted as she intended (this is hard to do right---she shouldn't be able to "sell her vote").
- May use math (crypto) to enable such verification without violating voter privacy.

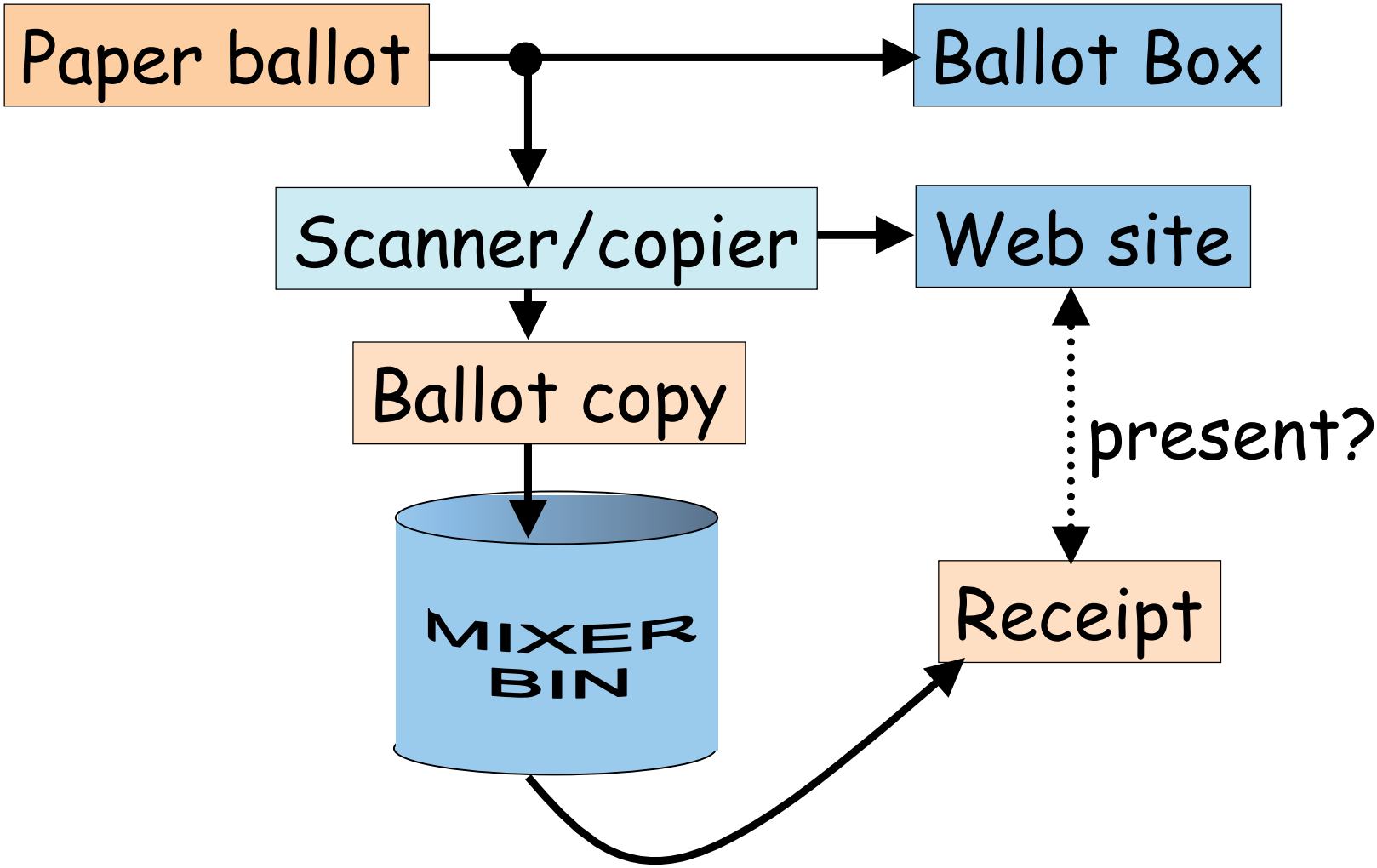
New voting systems: "end-to-end"

- Provide "end-to-end" integrity:
  - Votes *verifiably* "cast as intended"
  - Votes *verifiably* "collected as cast"
  - Votes *verifiably* "counted as collected"
- VVPAT only gets the *first* of these; once ballot is cast, what happens thereafter depends on integrity of "chain of custody" of ballots.
- "End-to-end" systems provide SI + verifiable chain of custody and tally.

"Twin" (Rivest & Smith)

- "academic" proposal
- NYT op-ed 1/7/08 by Poundstone in favor
- Each paper ballot has a copy ("twin") made that is put in "mixer bin"
- Voter casts original paper ballot (which is scanned and published on web), and takes home from mixer bin a copy of *some previous voter's ballot* as a "receipt".
- Voter may check that receipt is on web.

Twin

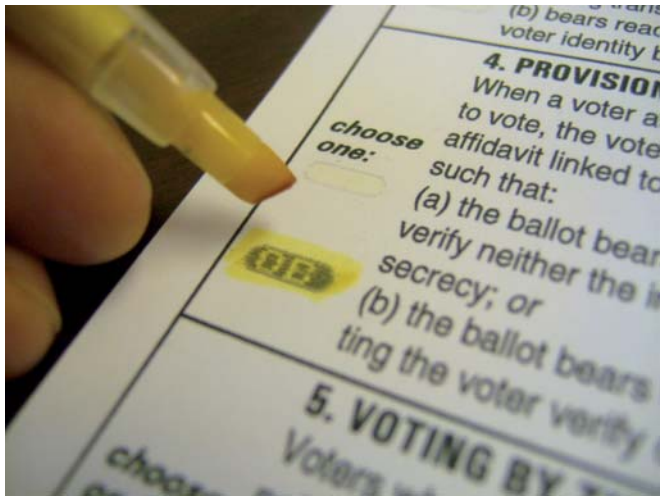

Paper ballot
Ballot Box
Scanner/copier
Web site
Ballot copy
present?
MIXER BIN
Receipt

Twin integrity

- Verifiably cast as intended
- Verifiably collected as cast: voters check that earlier voter's ballot is posted
- Verifiably counted as collected: anyone can tally posted ballots
- Usability … dubious…

Scantegrity II (Chaum, et al.)

- Marries traditional opscan with modern cryptographic (end-to-end) methods.
- Uses:
  - Invisible ink for "confirmation codes"
  - Web site
  - Crypto (back end)
- Ballots can be scanned by ordinary scanners.
- Ballots can be recounted by hand as usual.
- Takoma Park 11/03/09.

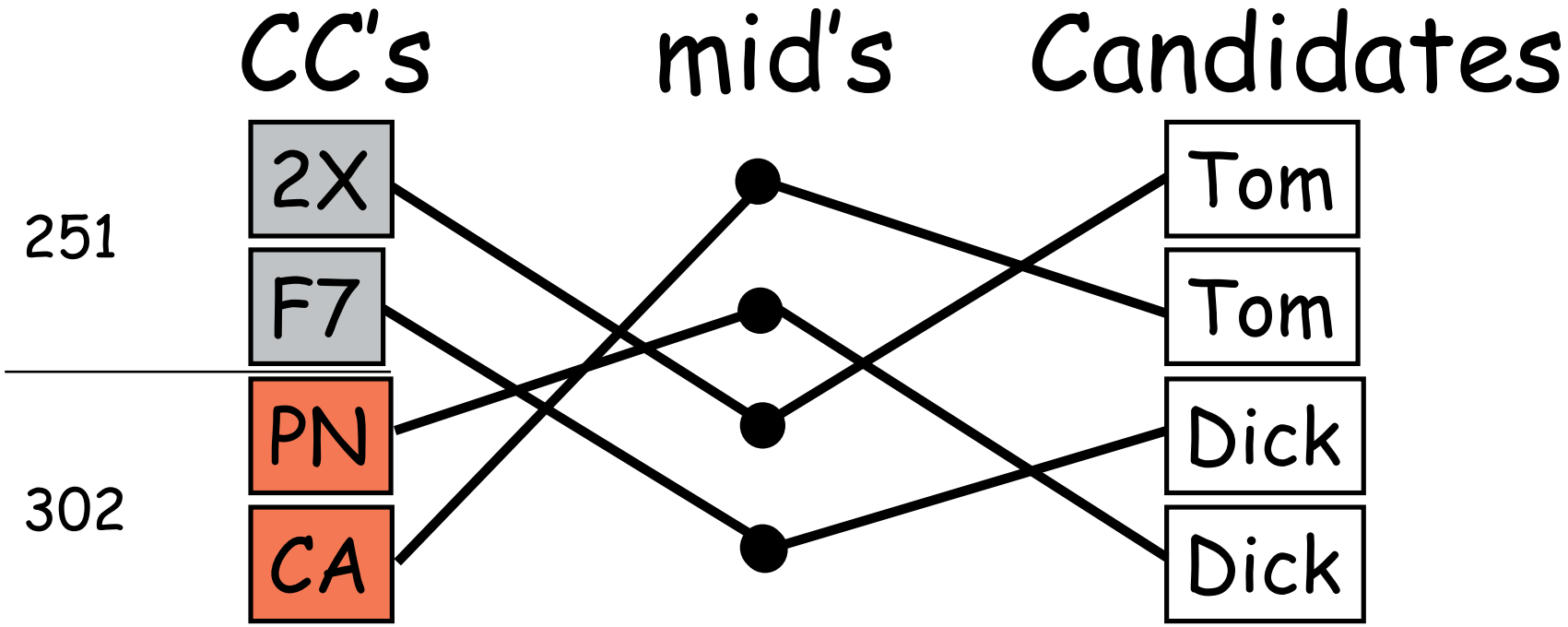


Scantegrity II details

- Special pen marks oval, but shows previously invisible confirmation code.
- CC's are random.
- Voter can copy & take home CC's.
- Officials also post revealed CC's.
- Voters can confirm posting (uses ballot serial number for lookup), and protest if incorrect.

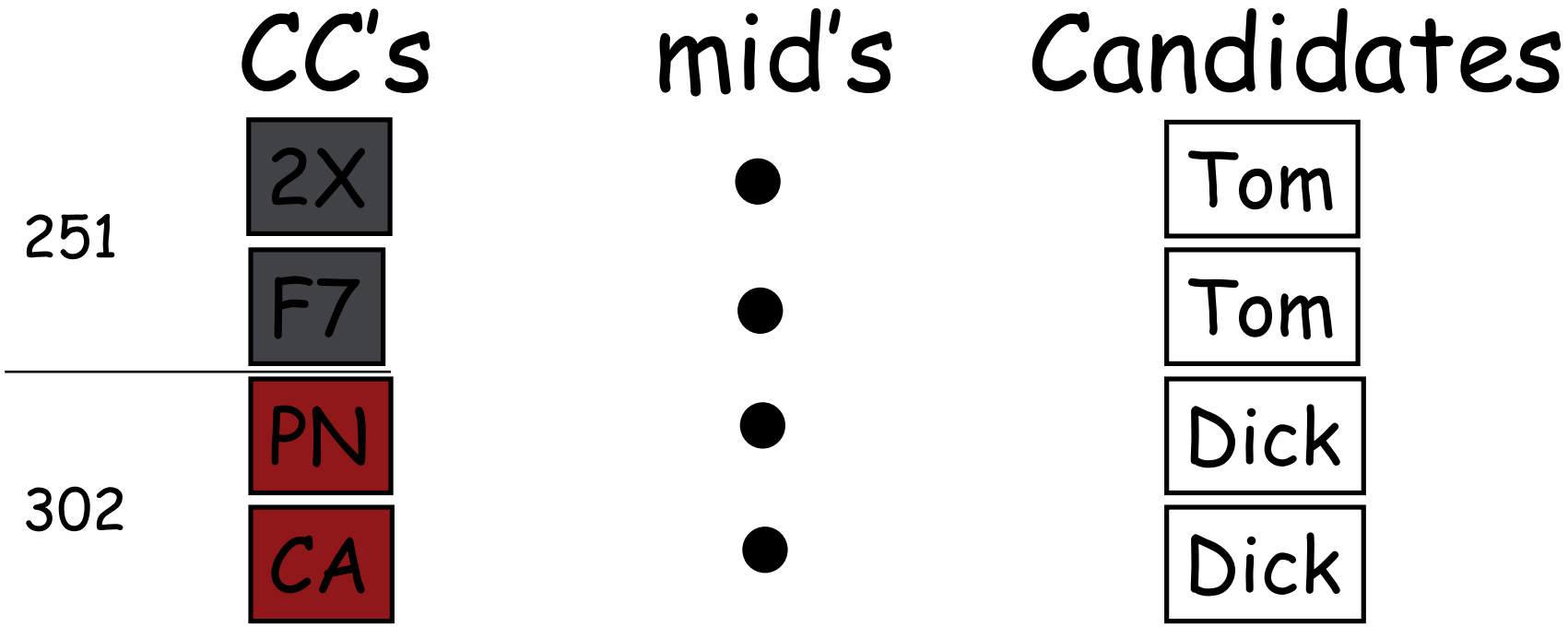
Scantegrity II integrity

- Officials create two permutations: CC's→mid's→candidates



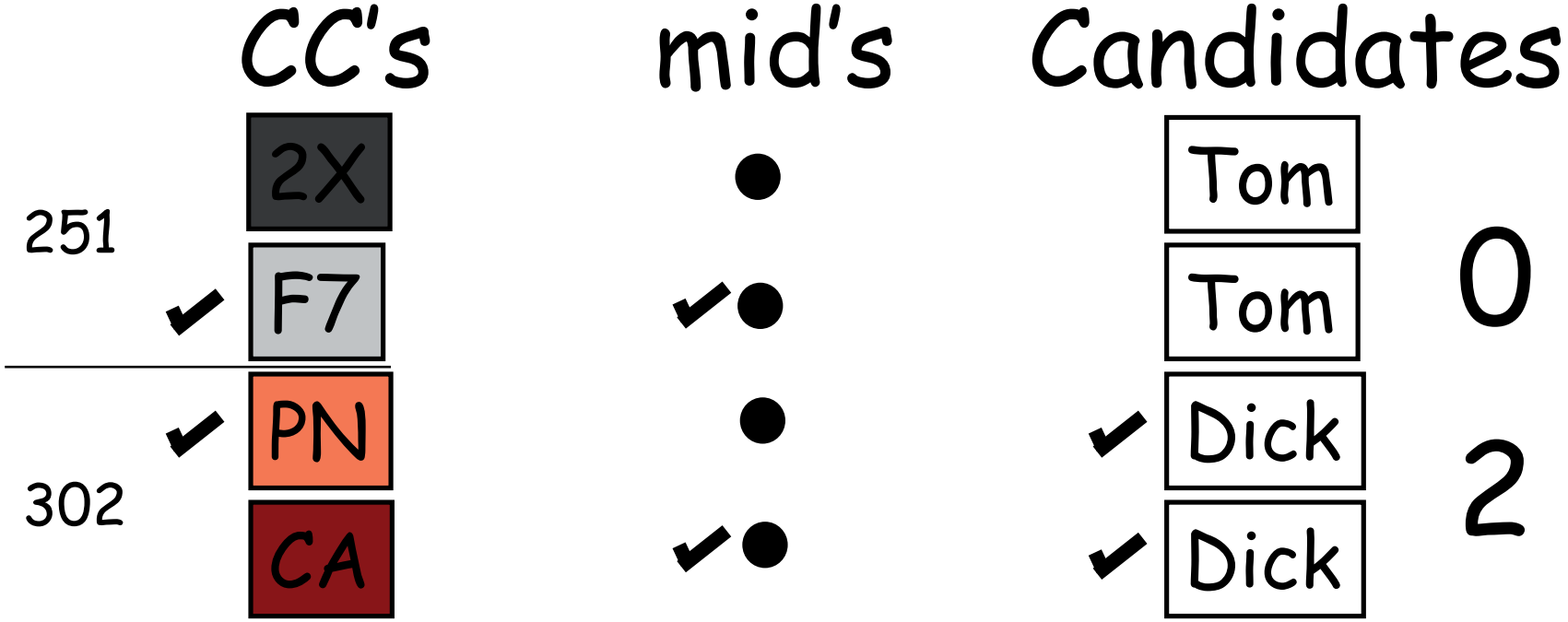
Scantegrity II integrity

- Election officials post commitments to all values and edges on web:



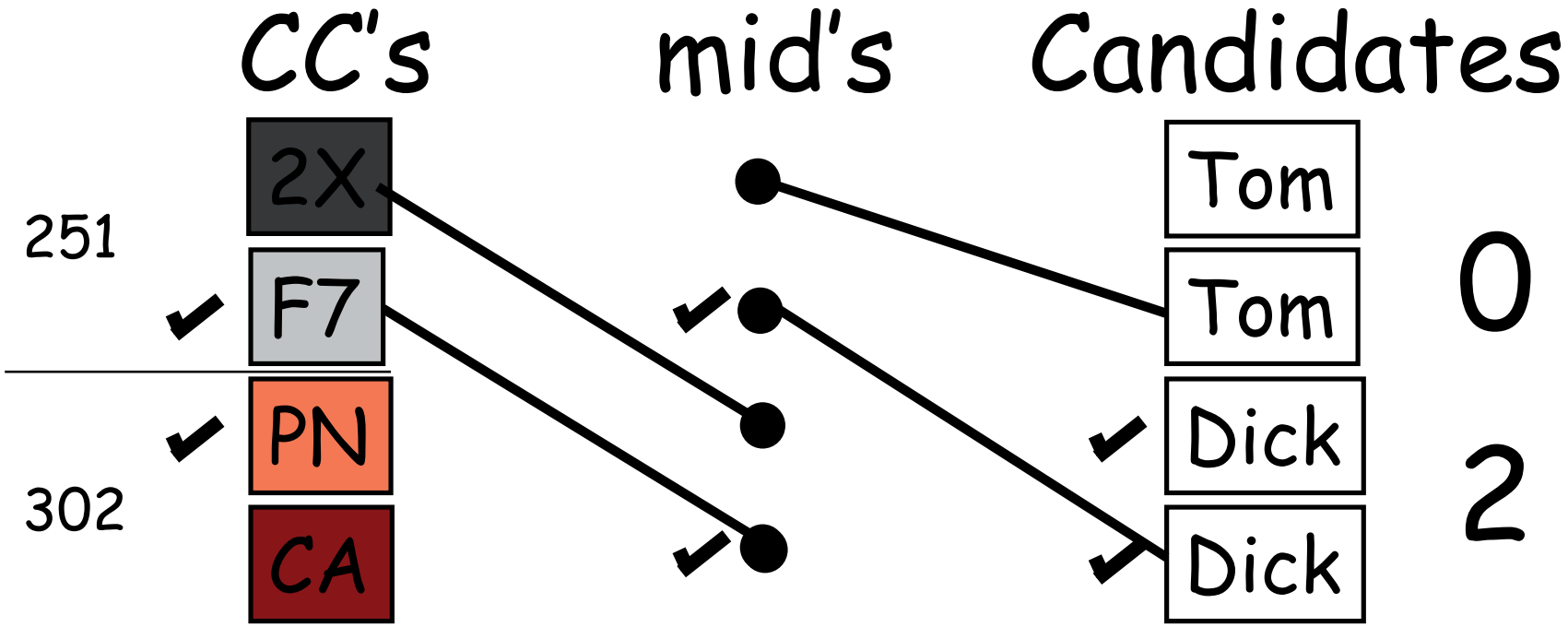
Scantegrity II integrity

- EO's open chosen CC's and mark related nodes; post tally; voter checks CC's and tally.



Scantegrity II integrity

- "randomized partial checking" confirms check marks consistent



Scantegrity II integrity

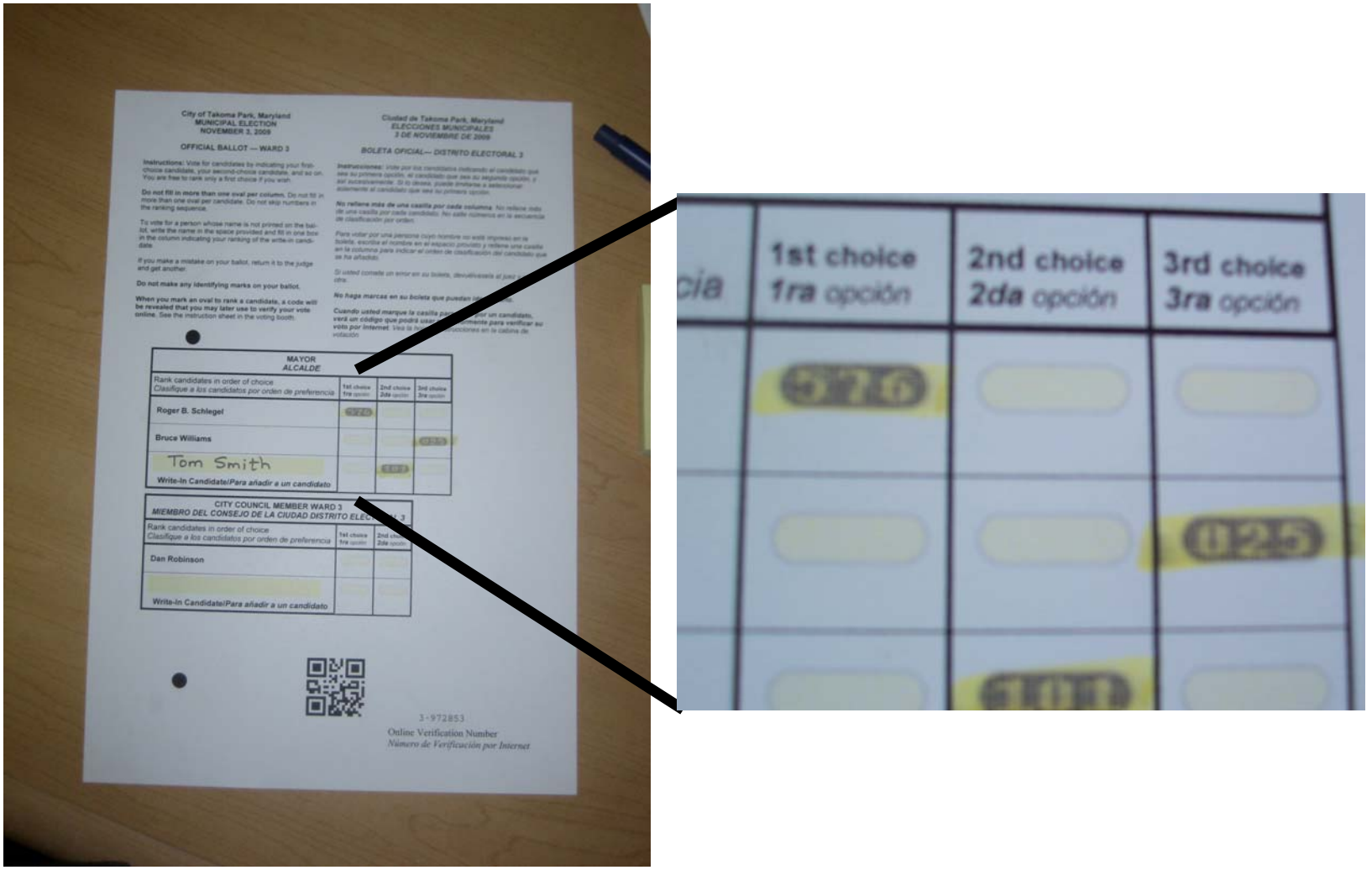
- *Cast as intended:* as in opscan
- *Collected as cast:* voter can check that his CC's are posted correctly.
- *Counted as cast:* ballot production audit, checkmark consistency check, and public tally of web site give verifiably correct result.

Takoma Park election 11/3/09

- Two races per ward; six wards.
- One poll site. 1722 voters.
  66 verified on-line.
- Election ran smoothly.
- Absentee votes; early votes; provisional votes; spoiled ballots; ballot audits; privacy sleeves; write-ins; IRV; external auditors; two scanners; spanish+english; …

David Chaum + scanner

Ballot and confirmation codes



Scantegrity II team

David Chaum
Rick Carback
Jeremy Clark
John Conway
Aleks Essex
Alex Florescu
Cory Jones
Travis Mayberry
Stefan Popoveniuc
Vivek Relan
Ron Rivest
Peter Ryan
Jan Rubio
Emily Shen
Alan Sherman
Bhushan Sonawane
Poorvi Vora
…

TP officials:

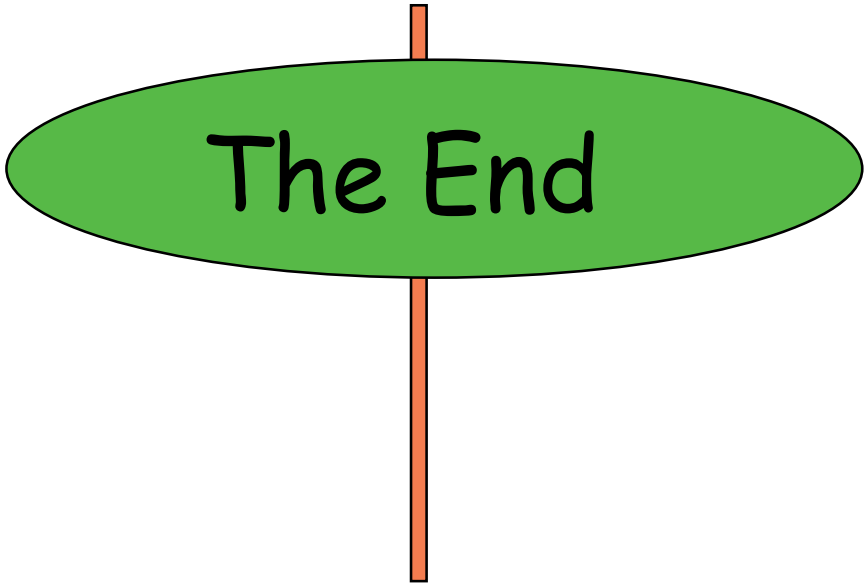
Jessie Carpenter
Anne Sergeant
Jane Johnson
Barrie Hoffman

Auditors & survey:

Ben Adida
Lilley Coney
Filip Zagorski
Lynn Baumeister

Summary

- "End-to-end" voting systems promise more verifiable integrity than we have seen to date in voting systems: they "verify the election outcome", and don't depend on "verifying the equipment & software".
- These systems have become practical, although more research and development is needed for scalability, accessibility, etc…



Thanks for your attention!