



# Security of Voting Systems

---

Ronald L. Rivest  
MIT CSAIL



Given at:

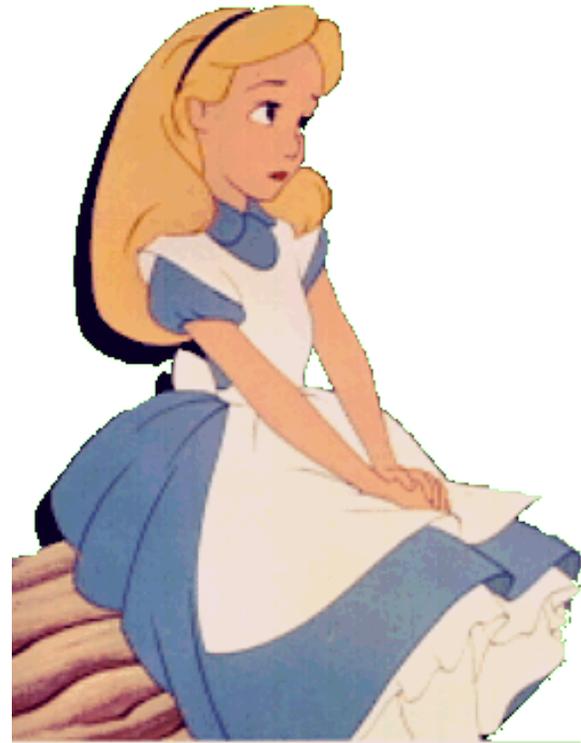
GWU Computer Science Dept.

November 9, 2009

# Voting is Easy... ???

---

- ◆ "What's one and one?"  
"I don't know," said Alice. "I lost count."  
"She can't do addition," said the Red Queen.



There are three kinds of people working on elections:

1. those who can count
2. and those who can't.



# Outline

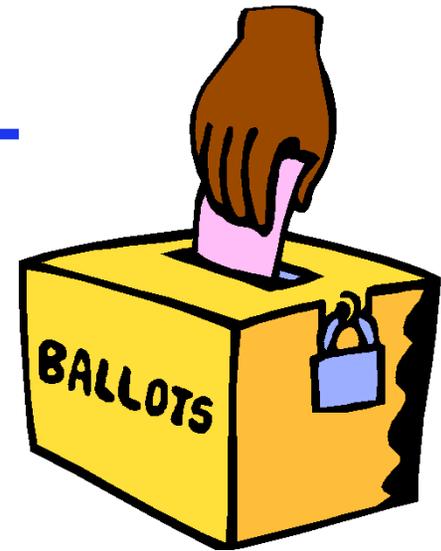
---

- ◆ 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...*



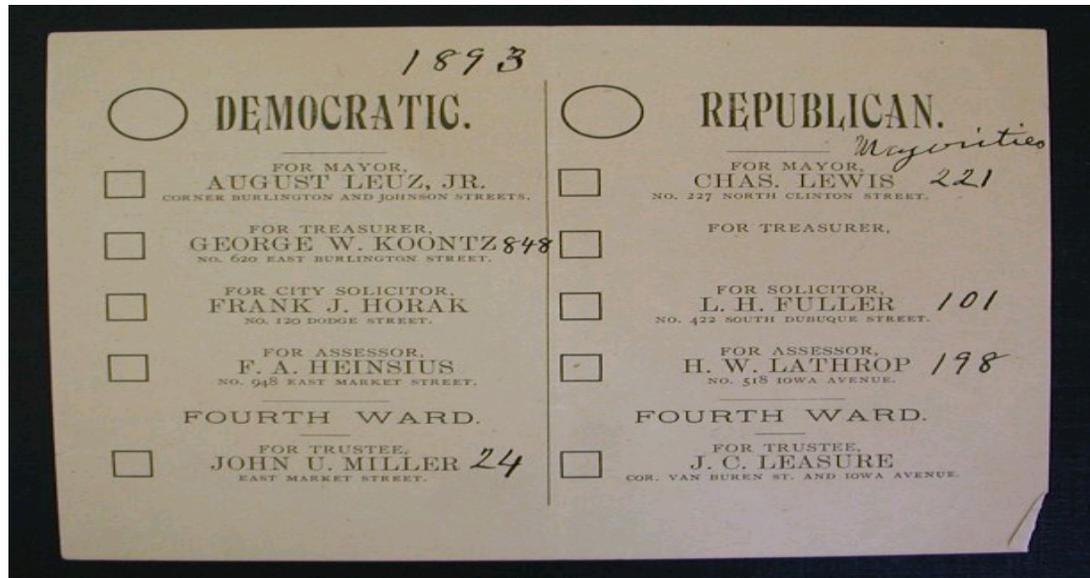
# Public Voting

---



The County Election. Bingham. 1846.

# Paper Ballots



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

# Lever Machines

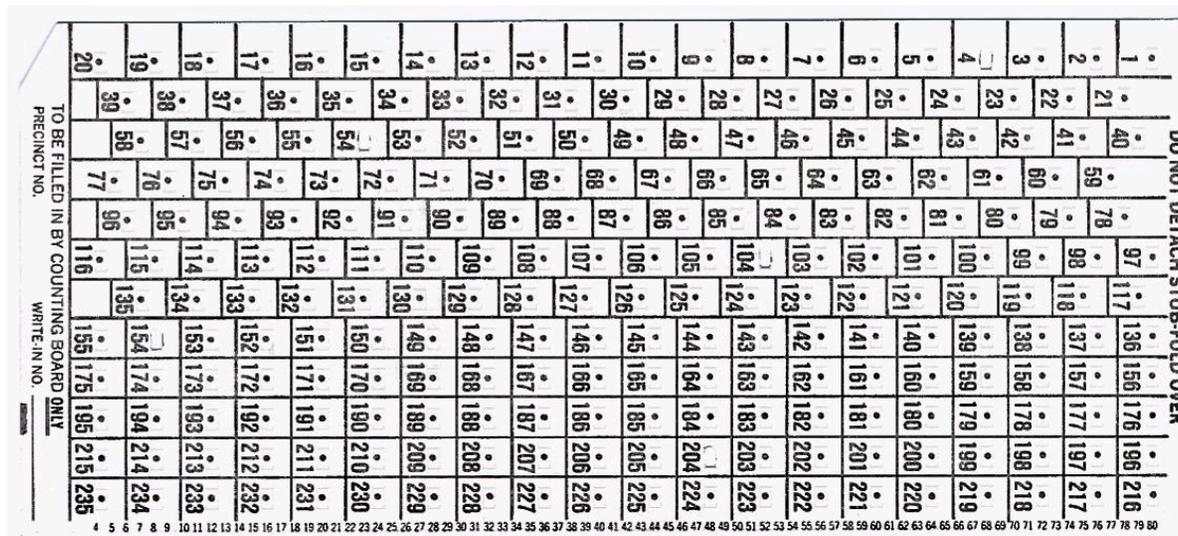
---



- ◆ 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"

1 OFFICIAL BALLOT, GENERAL ELECTION  
PALM BEACH COUNTY, FLORIDA  
NOVEMBER 7, 2000

ELECTORS FOR PRESIDENT AND VICE PRESIDENT  (A vote for the candidates will actually be a vote for their electors.)  (Vote for Group)	(REPUBLICAN) GEORGE W. BUSH - PRESIDENT DICK CHENEY - VICE PRESIDENT	3 →
	(DEMOCRATIC) AL GORE - PRESIDENT JOE LIEBERMAN - VICE PRESIDENT	5 →
	(LIBERTARIAN) HARRY BROWNE - PRESIDENT ART OLIVIER - VICE PRESIDENT	7 →
	(GREEN) RALPH NADER - PRESIDENT WINONA LaDUKE - VICE PRESIDENT	9 →
	(SOCIALIST WORKERS) JAMES HARRIS - PRESIDENT MARGARET TROWE - VICE PRESIDENT	11 →
	(NATURAL LAW) JOHN HAGELIN - PRESIDENT NAT GOLDHABER - VICE PRESIDENT	13 →

1-R OFFICIAL BALLOT, GENERAL ELECTION  
PALM BEACH COUNTY, FLORIDA  
NOVEMBER 7, 2000

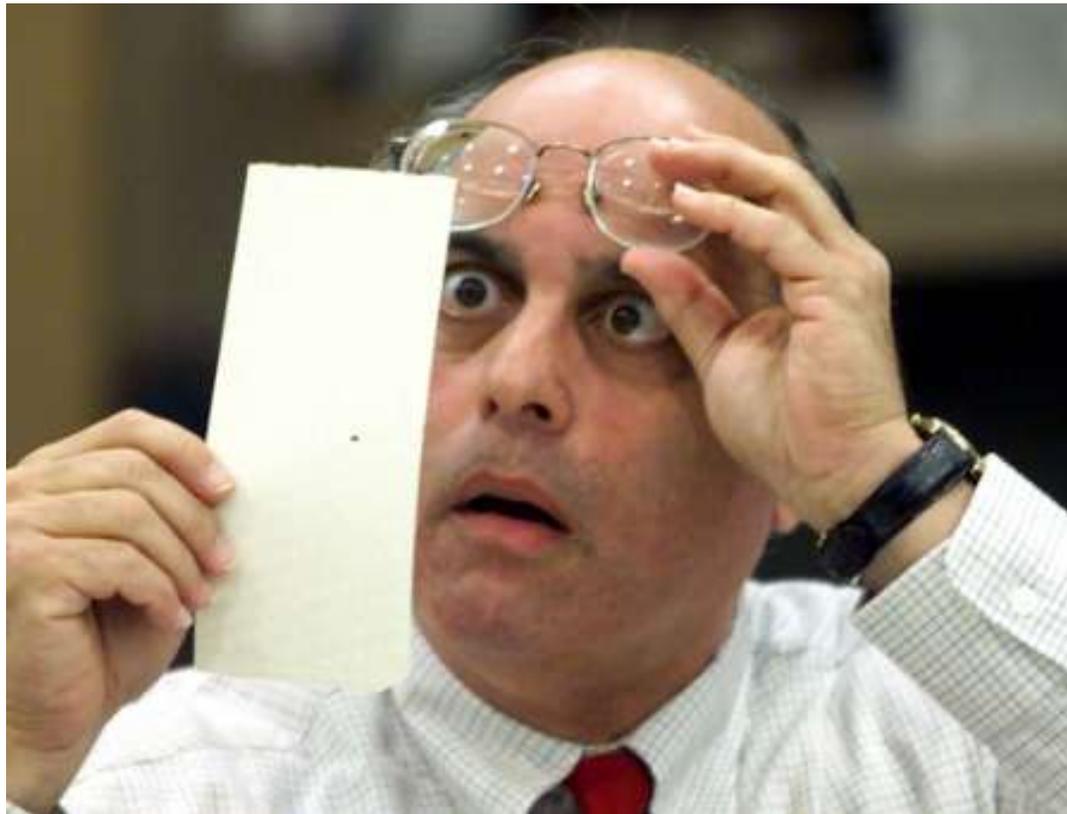
← 4	(REFORM) PAT BUCHANAN - PRESIDENT EZOLA FOSTER - VICE PRESIDENT
← 6	(SOCIALIST) DAVID McREYNOLDS - PRESIDENT MARY CAL HOLLIS - VICE PRESIDENT
← 8	(CONSTITUTION) HOWARD PHILLIPS - PRESIDENT J. CURTIS FRAZIER - VICE PRESIDENT
← 10	(WORKERS WORLD) MONICA MODREHEAD - PRESIDENT GLORIA La RIVA - VICE PRESIDENT

WRITE-IN CANDIDATE  
To vote for a write-in candidate, follow the  
directions on the long stub of your ballot card.

TURN PAGE TO CONTINUE VOTING →

A "dimpled chad" ???

---



# Optical scan ("opscan")

OFFICIAL BALLOT		
CONSOLIDATED GENERAL ELECTION		
SANTA BARBARA COUNTY, CALIFORNIA		
NOVEMBER 5, 2002		
<p><b>INSTRUCTIONS TO VOTERS:</b> 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: <input checked="" type="radio"/> <b>VOTE BOTH SIDES</b></p>		
<b>STATE</b>	<b>INSURANCE COMMISSIONER</b>	<b>FOR ASSOCIATE JUSTICE, COURT OF APPEAL</b>
<b>GOVERNOR</b>	<b>Vote for One</b>	<b>2nd APPELLATE DISTRICT, DIVISION TWO</b>
<b>Vote for One</b>	<input type="radio"/> DALE F. OGDEN Insurance Consultant/Actuary <i>Liberarian</i>	Shall ASSOCIATE JUSTICE JUDITH M. ASHMANN be elected to the office for the term prescribed by law? <input type="radio"/> YES <input type="radio"/> NO
<input type="radio"/> GARY DAVID COPELAND Chief Executive Officer <i>Liberarian</i>	<input type="radio"/> DAVID I. SHEIDLLOWER Financial Services Executive <i>Green</i>	
<input type="radio"/> BILL SIMON Businessman/Charity Director <i>Republican</i>	<input type="radio"/> GARY MENDOZA Businessman <i>Republican</i>	<b>FOR ASSOCIATE JUSTICE, COURT OF APPEAL</b> <b>2nd APPELLATE DISTRICT, DIVISION TWO</b>
<input type="radio"/> REINHOLD GULKE Electrical Contractor/Farmer <i>American Independent</i>	<input type="radio"/> JOHN GARAMENDI Rancher <i>Democratic</i>	
<input type="radio"/> GRAY DAVIS Governor of the State of California <i>Democratic</i>	<input type="radio"/> STEVE KLEIN Businessman <i>American Independent</i>	Shall ASSOCIATE JUSTICE KATHRYN DOI TODD be elected to the office for the term prescribed by law? <input type="radio"/> YES <input type="radio"/> NO
<input type="radio"/> IRIS ADAM Business Analyst <i>Natural Law</i>	<input type="radio"/> RAUL CALDERON, JR. Health Researcher/Educator <i>Natural Law</i>	
<input type="radio"/> PETER MIGUEL CAMEJO Financial Investment Advisor <i>Green</i>	<input type="radio"/> Write-In	<b>FOR PRESIDING JUSTICE, COURT OF APPEAL</b> <b>2nd APPELLATE DISTRICT, DIVISION THREE</b>
<input type="radio"/> Write-In	<b>MEMBER, STATE BOARD OF EQUALIZATION</b> <b>2<sup>ND</sup> District</b> <b>Vote for One</b>	
<b>LIEUTENANT GOVERNOR</b>	<b>Vote for One</b>	Shall PRESIDING JUSTICE JOAN DEMPSEY KLEIN be elected to the office for the term prescribed by law? <input type="radio"/> YES <input type="radio"/> NO
<b>Vote for One</b>	<input type="radio"/> TOM Y. SANTOS Tax Consultant/Realtor <i>Democratic</i>	
<input type="radio"/> PAT WRIGHT Ferret Legalization Coordinator <i>Liberarian</i>	<input type="radio"/> BILL LEONARD State Lawmaker/Businessman <i>Republican</i>	<b>FOR ASSOCIATE JUSTICE, COURT OF APPEAL</b> <b>2nd APPELLATE DISTRICT, DIVISION FOUR</b>
<input type="radio"/> PAUL JERRY HANNOSH Educator/Businessman <i>Reform</i>	<input type="radio"/> Write-In	
<input type="radio"/> BRUCE MC PHERSON California State Senator <i>Republican</i>	<b>UNITED STATES REPRESENTATIVE</b>	Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law? <input type="radio"/> YES <input type="radio"/> NO
<input type="radio"/> KALEE PRZYBYLAK Public Relations Director <i>Natural Law</i>	<b>24<sup>TH</sup> District</b>	
<input type="radio"/> CRUZ M. BUSTAMANTE Lieutenant Governor <i>Democratic</i>	<b>Vote for One</b>	Shall ASSOCIATE JUSTICE GARY HASTINGS be elected to the office for the term prescribed by law? <input type="radio"/> YES <input type="radio"/> NO
<input type="radio"/> JIM KING Real Estate Broker <i>American Independent</i>	<input type="radio"/> ELTON GALLEGLY U.S. Representative <i>Republican</i>	
<input type="radio"/> DONNA J. WARREN Certified Financial Manager <i>Green</i>	<input type="radio"/> Write-In	



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 (?)

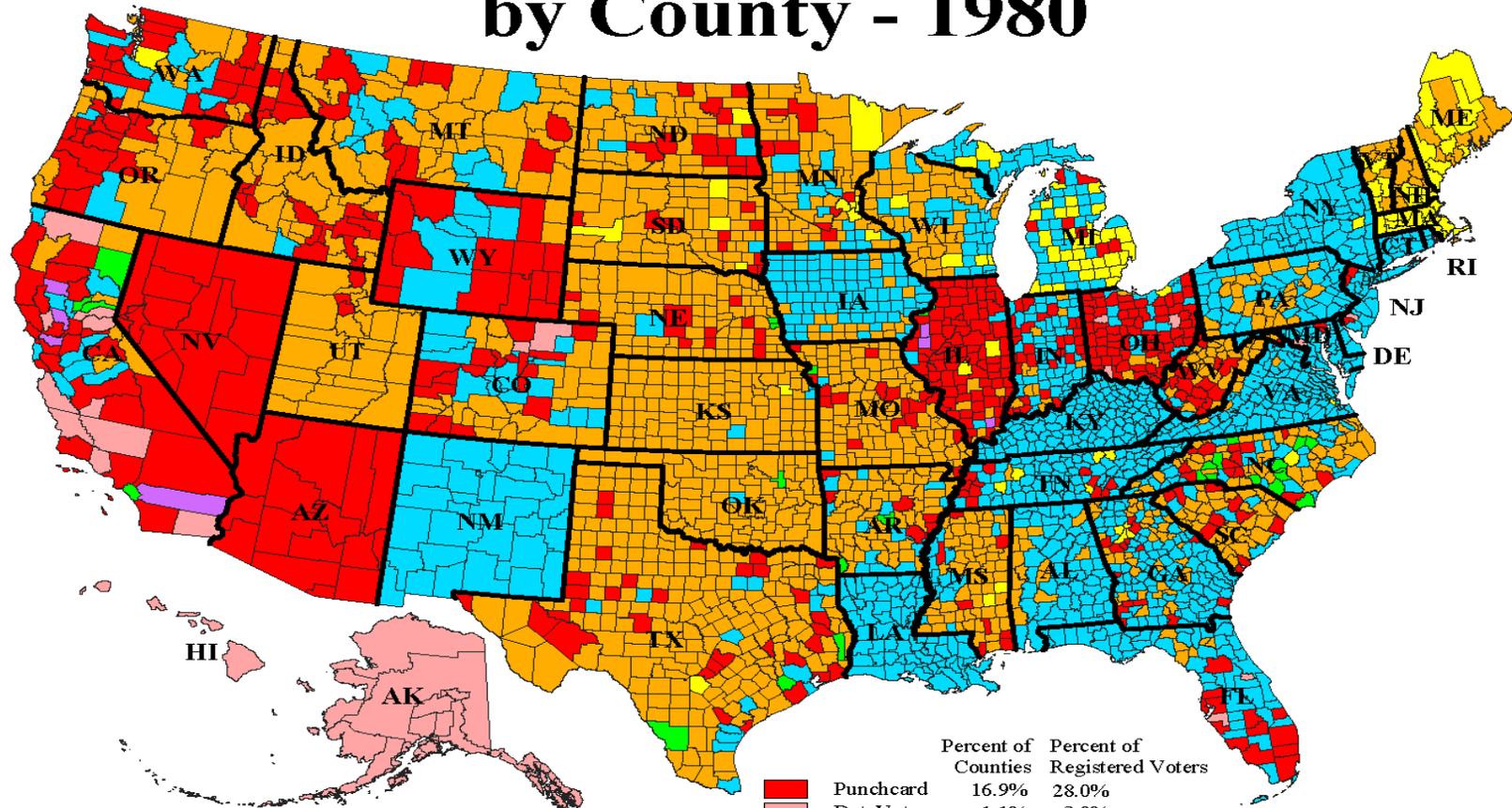
---

- ◆ 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 systems is used statewide  
except for a few paper ballot precincts.

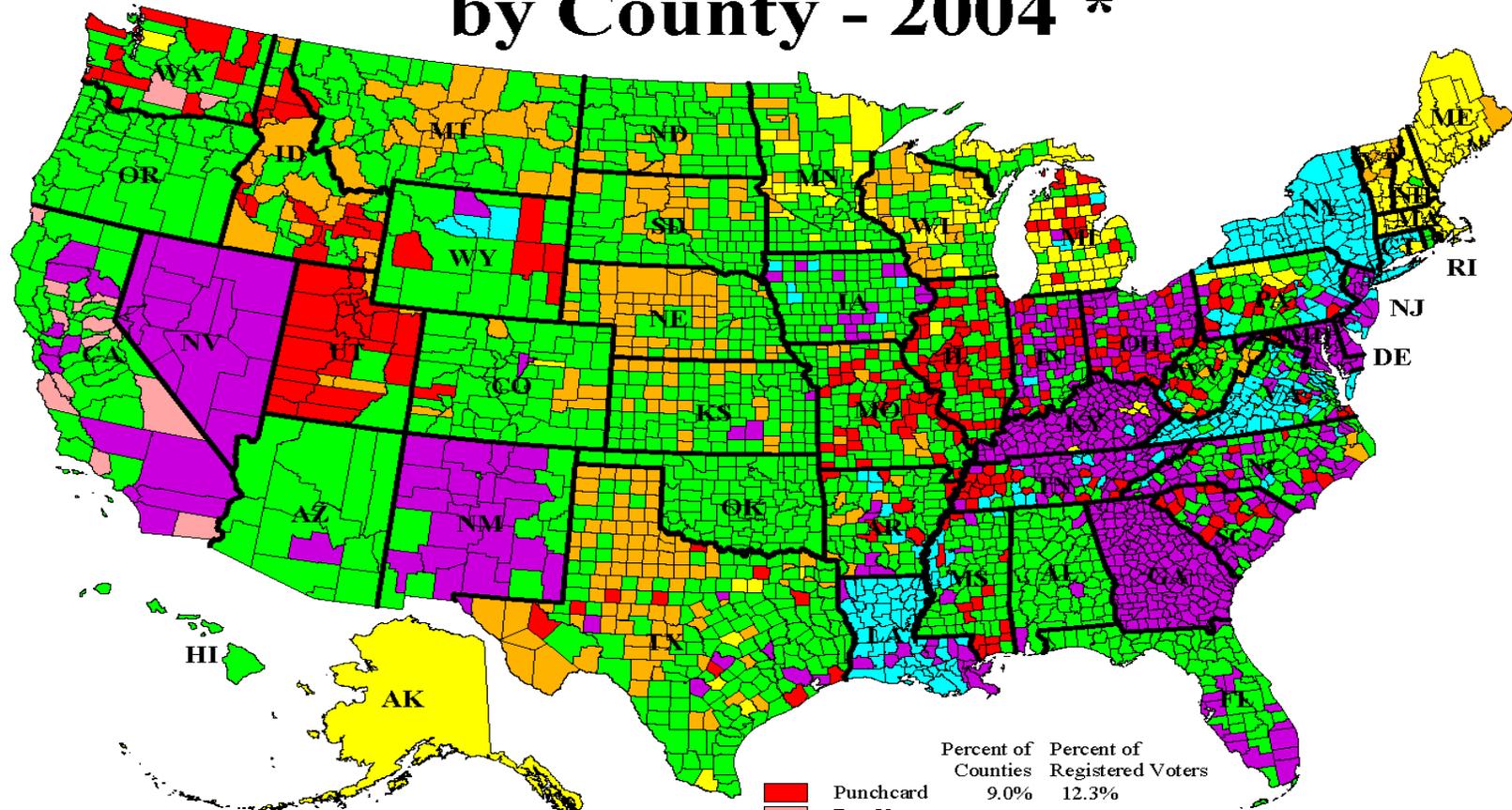
	Percent of Counties	Percent of Registered Voters
<span style="color: red;">■</span> Punchcard	16.9%	28.0%
<span style="color: #f08080;">■</span> DataVote	1.1%	3.0%
<span style="color: cyan;">■</span> Lever	36.9%	42.9%
<span style="color: orange;">■</span> Paper	41.0%	10.8%
<span style="color: green;">■</span> Optical	.8%	2.1%
<span style="color: purple;">■</span> Electronic	.2%	.7%
<span style="color: yellow;">■</span> 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.

Copyright © 2004 Election Data Services, Inc.  
Printed 5/4/2004.

**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.  
AccessVote system is used statewide  
except for a few paper ballot precincts.

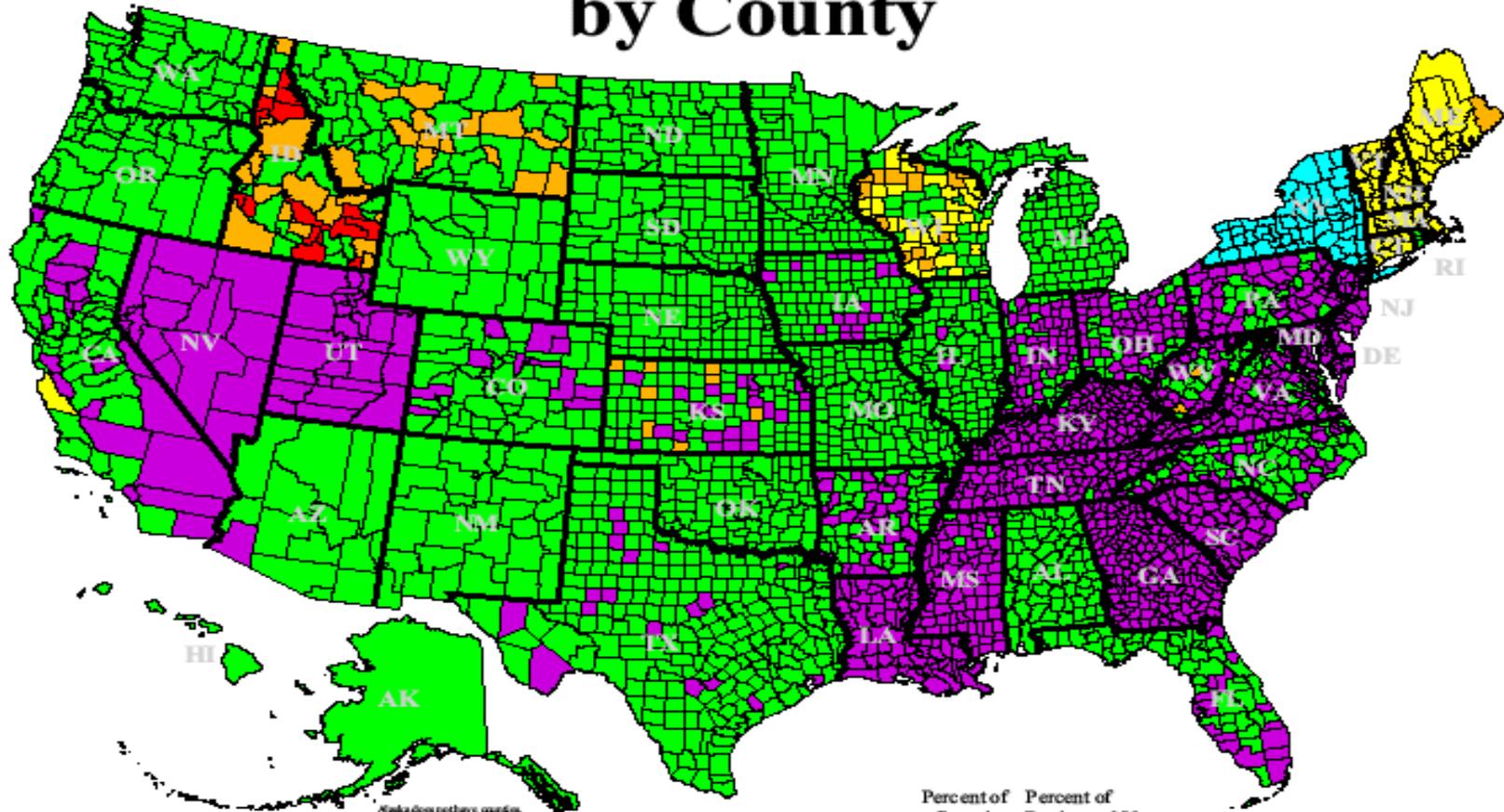
\* Equipment expected to be used  
in the November 2004 election as  
reported by state election officials.  
The map shows equipment used at polling  
places, not necessarily absentee balloting.

	Percent of Counties	Percent of Registered Voters
<span style="color: red;">■</span> Punchcard	9.0%	12.3%
<span style="color: pink;">■</span> DataVote	.8%	1.4%
<span style="color: cyan;">■</span> Lever	8.6%	13.9%
<span style="color: orange;">■</span> Paper	9.6%	.7%
<span style="color: green;">■</span> Optical	45.4%	33.7%
<span style="color: purple;">■</span> Electronic	21.7%	30.8%
<span style="color: yellow;">■</span> Mixed Systems	4.8%	7.2%

Copyright © 2004 Election Data Services, Inc.  
\*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



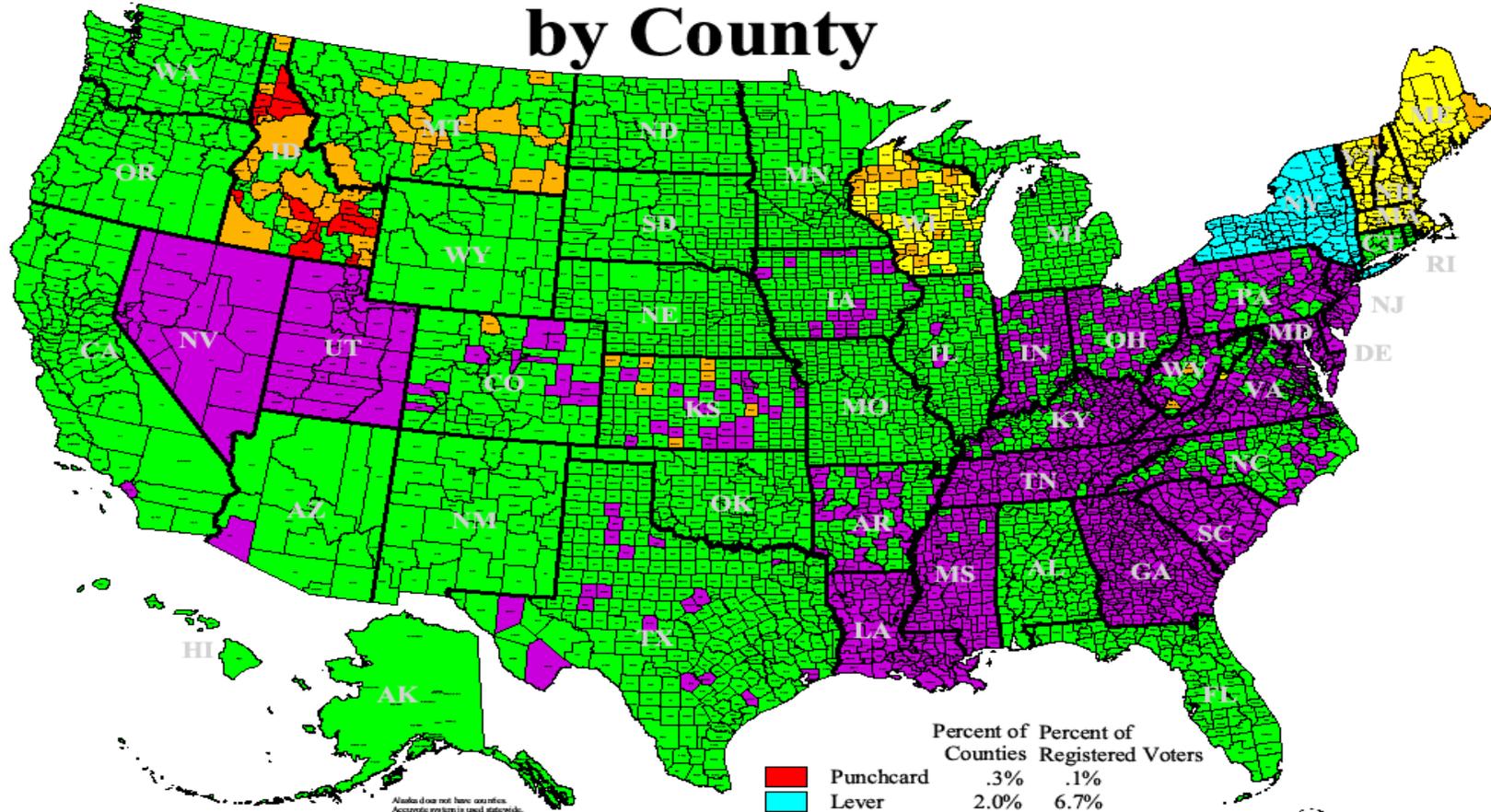
*Alaska does not have counties.  
A statewide system is used statewide.*

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.

Percent of Counties    Percent of Registered Voters

<span style="color: red;">■</span> Punchcard	.4%	.2%
<span style="color: cyan;">■</span> Lever	2.0%	6.8%
<span style="color: orange;">■</span> Paper	1.8%	.2%
<span style="color: green;">■</span> Optical	56.2%	48.9%
<span style="color: purple;">■</span> Electronic	36.6%	38.3%
<span style="color: yellow;">■</span> Mixed Systems	3.0%	5.5%

# November 2008 Voting Equipment Usage by County



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

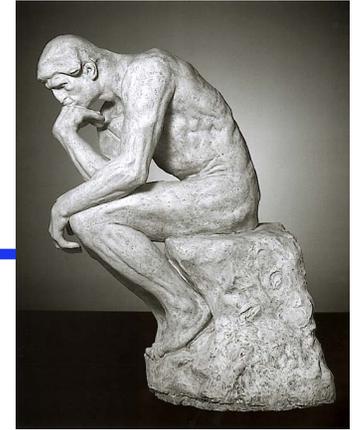
Equipment expected to be used in the November 2008 election as reported by state election officials and news media. The map shows equipment used at polling places, not necessarily absentee or disabled balloting.

	Percent of Counties	Percent of Registered Voters
<span style="color: red;">■</span> Punchcard	.3%	.1%
<span style="color: cyan;">■</span> Lever	2.0%	6.7%
<span style="color: orange;">■</span> Paper	1.8%	.2%
<span style="color: green;">■</span> Optical	58.9%	56.2%
<span style="color: purple;">■</span> Electronic	34.3%	32.6%
<span style="color: yellow;">■</span> Mixed Systems	2.7%	4.2%

# 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 (one team led by Matt Blaze) found serious problems of this sort...
- ◆ ...

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.

# 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 mathematics ("cryptography") 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)

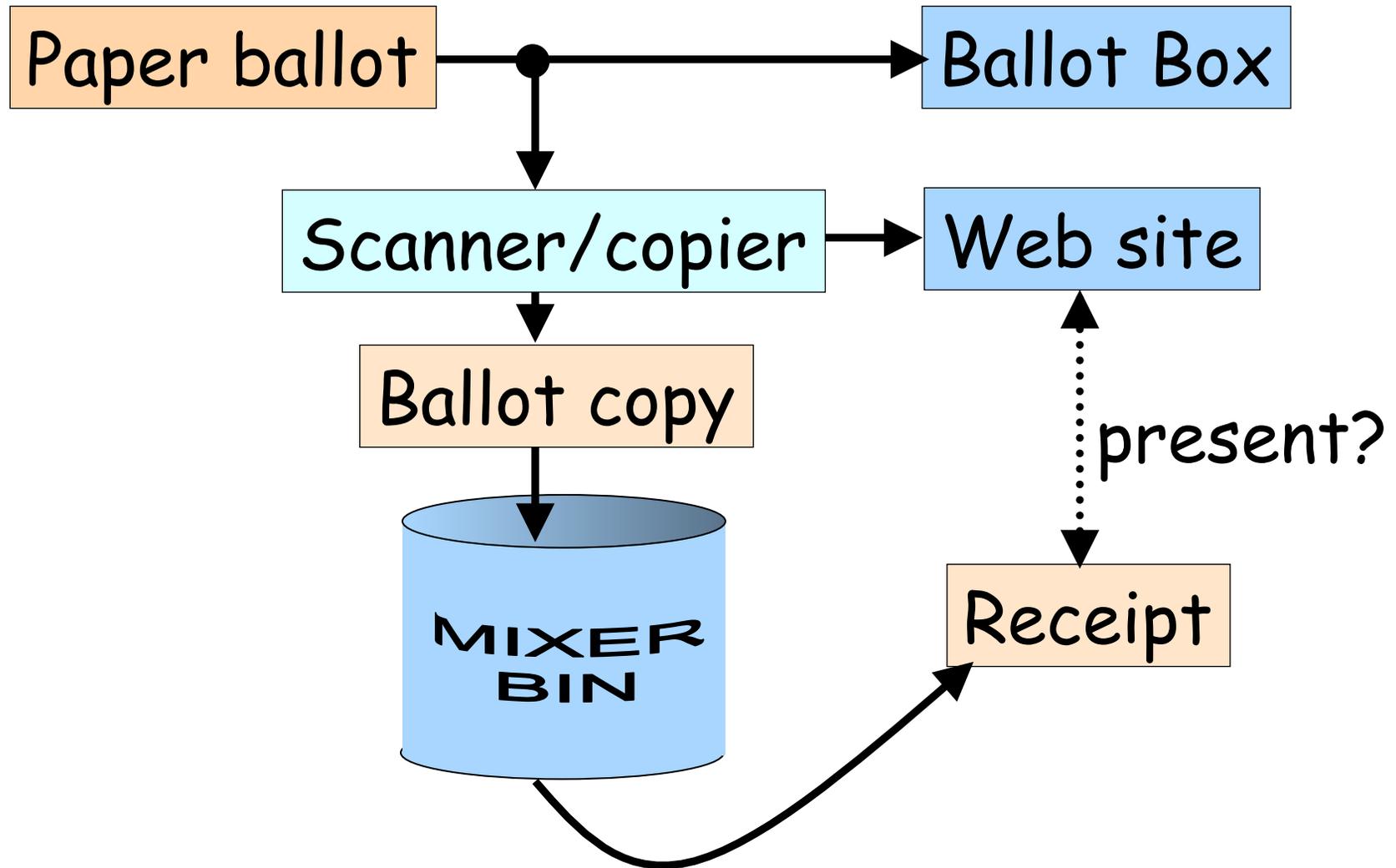
---

- ◆ "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

---



# 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 unproven

# 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.



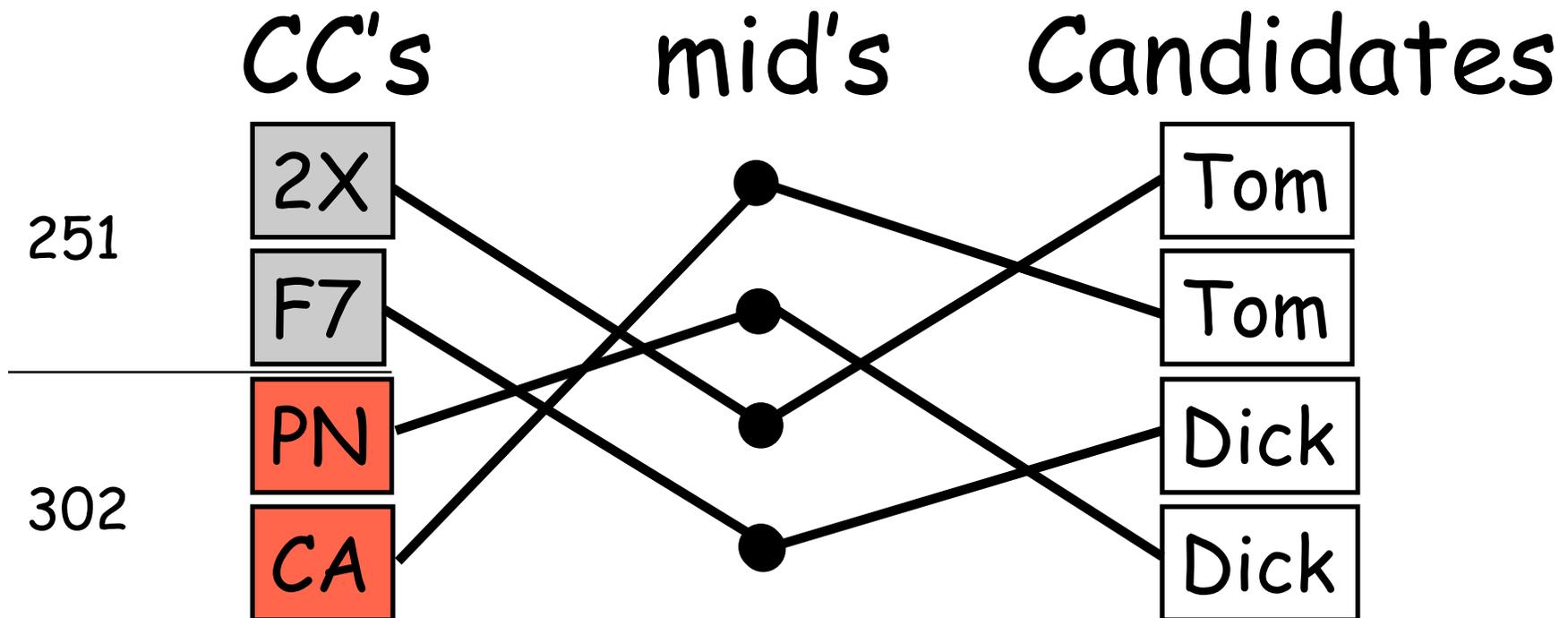
# Scantegrity II details



- ◆ 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.

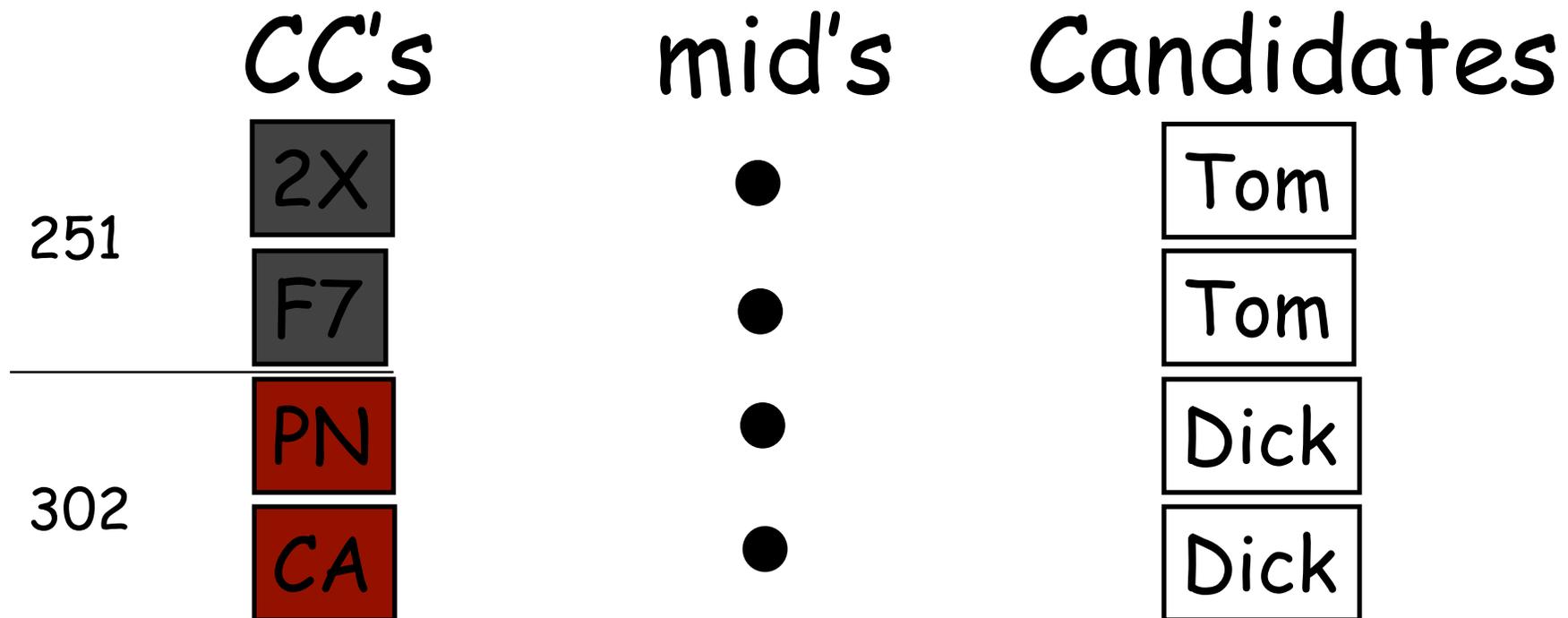
# Scantegrity II integrity

- ◆ Officials create two permutations:  
 $CC's \rightarrow mid's \rightarrow candidates$



# Scantegrity II integrity

- ◆ Election officials commit to (encrypt and post) all values and edges on web:



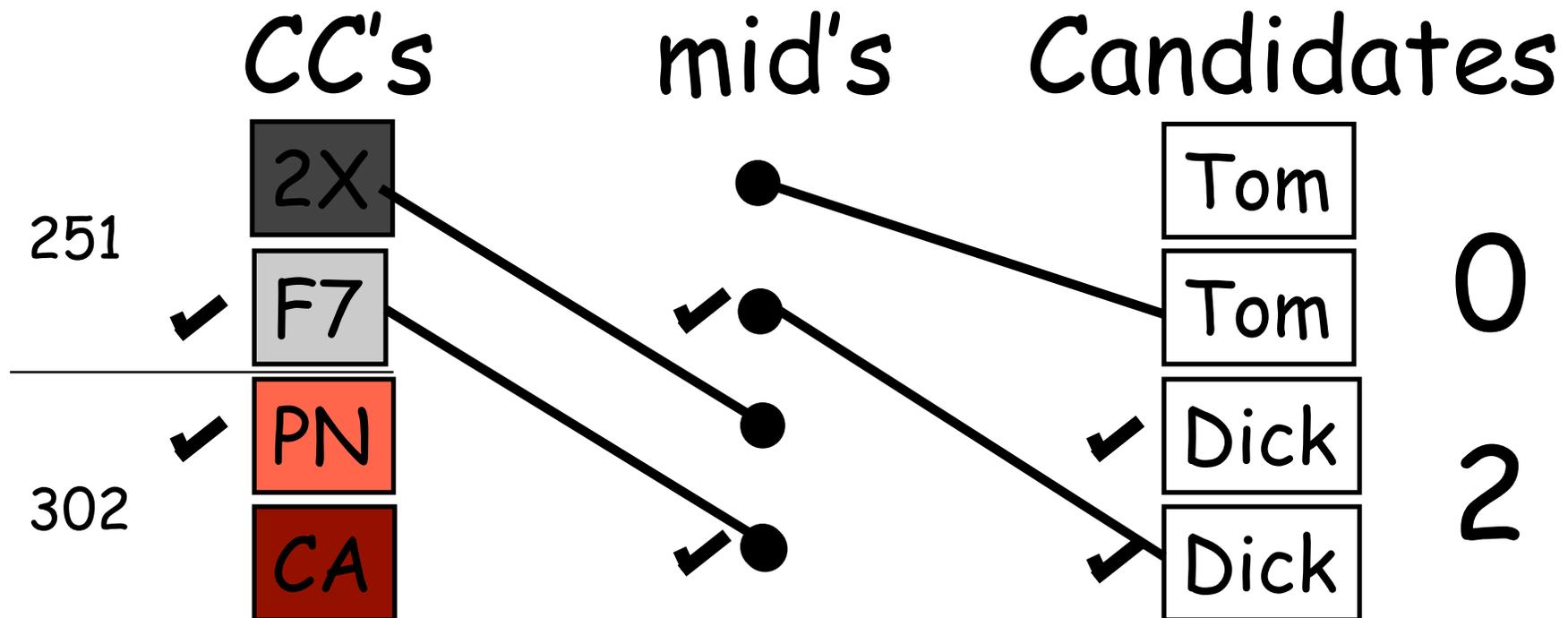
# Scantegrity II integrity

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

	CC's	mid's	Candidates	
251	2X	●	Tom	
✓	F7	✓●	Tom	0
<hr/>				
302	PN	●	✓ Dick	
	CA	✓●	✓ Dick	2

# 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

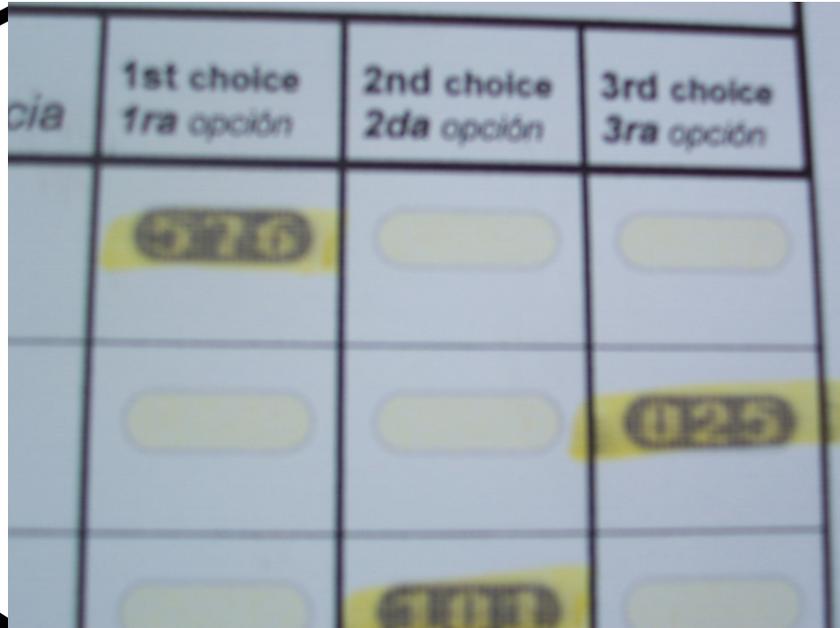
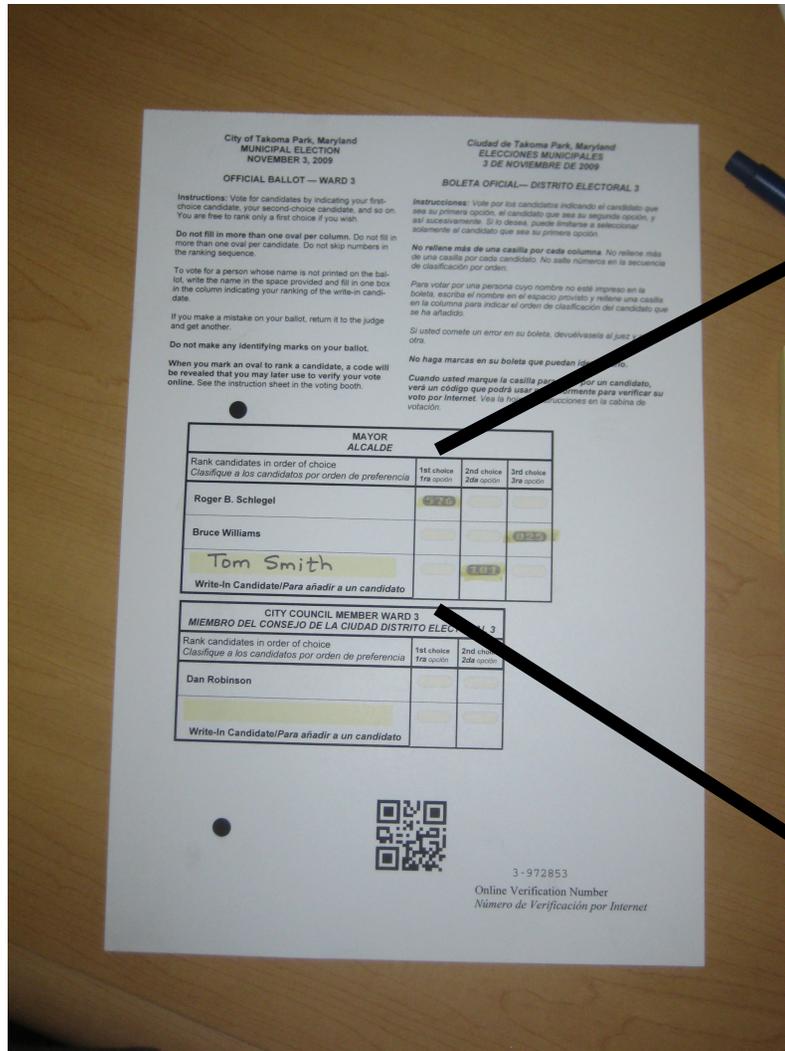
- ◆ Two races per ward; six wards.
- ◆ One poll site. 1722 voters.  
66 verified on-line.
- ◆ Election ran smoothly.
- ◆ Absentee votes; early votes;  
provisional votes; spoiled ballots;  
ballot audits; privacy sleeves; write-  
ins; IRV; external auditors; two  
scanners; spanish+english; ...

# 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

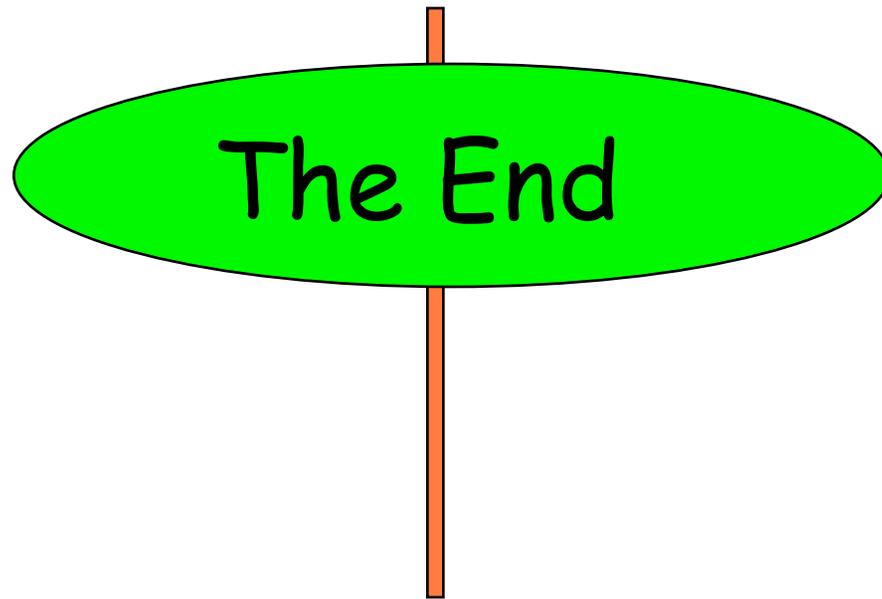
Filip Zagorski

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...



The End