

Security of Voting Systems

Ronald L. Rivest

MIT CSAIL

L19-SecurityOfVoting

April 23, 2014

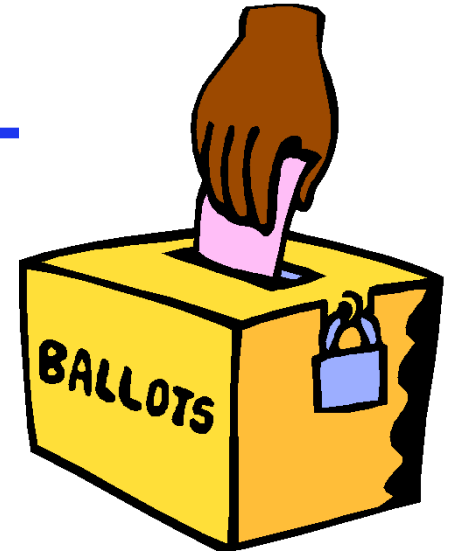


Outline

- ◆ 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...*

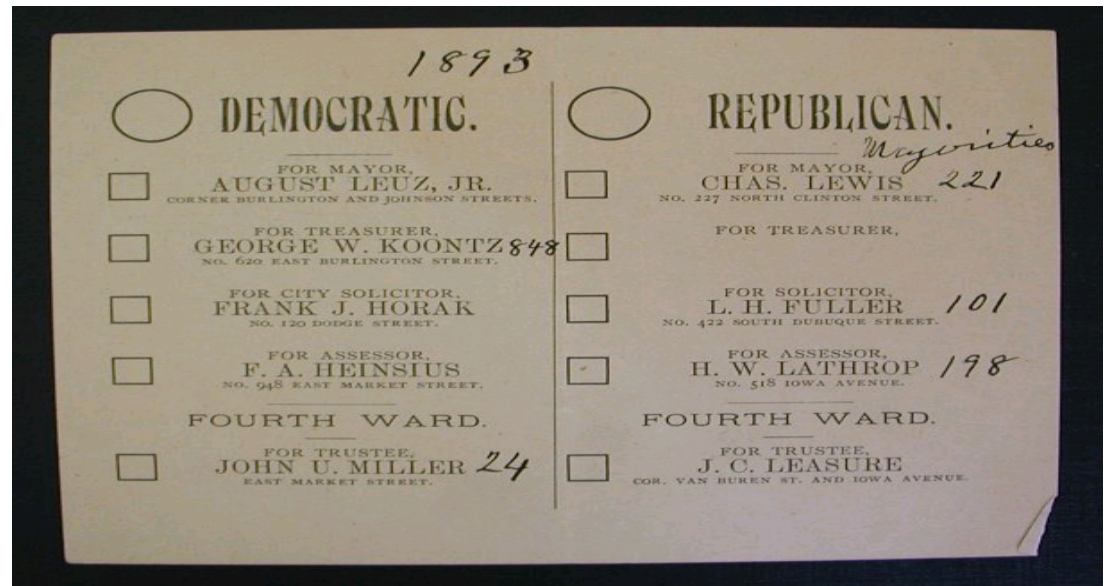
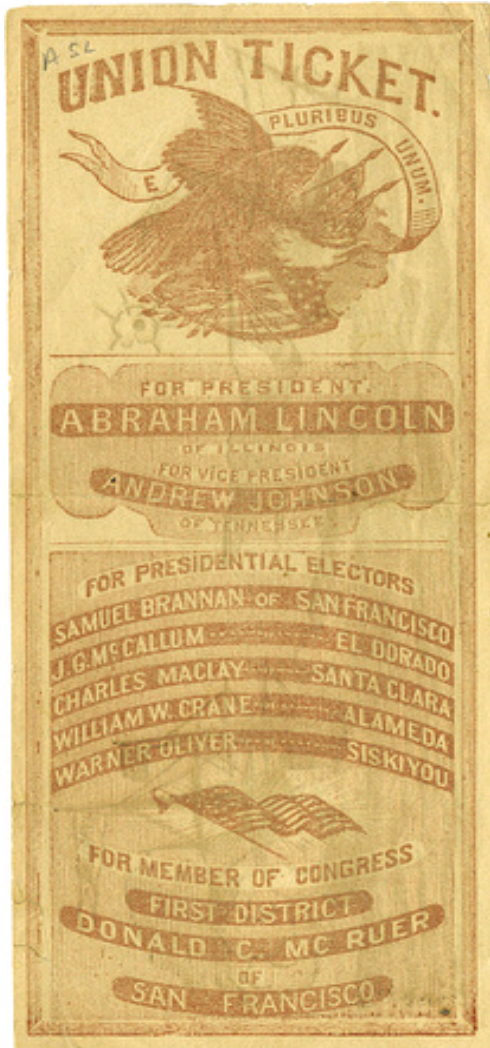


Public Voting



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.

DO NOT DETACH STUB-FOLD OVER

• 1	• 21	• 40	• 59	• 78	• 97	• 117	• 136	• 156	• 176	• 196	• 216
• 2	• 22	• 41	• 60	• 79	• 98	• 118	• 137	• 157	• 177	• 197	• 217
• 3	• 23	• 42	• 61	• 80	• 99	• 119	• 138	• 158	• 178	• 198	• 218
• 4	• 24	• 43	• 62	• 81	• 100	• 120	• 139	• 159	• 179	• 199	• 219
• 5	• 25	• 44	• 63	• 82	• 101	• 121	• 140	• 160	• 180	• 200	• 220
• 6	• 26	• 45	• 64	• 83	• 102	• 122	• 141	• 161	• 181	• 201	• 221
• 7	• 27	• 46	• 65	• 84	• 103	• 123	• 142	• 162	• 182	• 202	• 222
• 8	• 28	• 47	• 66	• 85	• 104	• 124	• 143	• 163	• 183	• 203	• 223
• 9	• 29	• 48	• 67	• 86	• 105	• 125	• 144	• 164	• 184	• 204	• 224
• 10	• 30	• 49	• 68	• 87	• 106	• 126	• 145	• 165	• 185	• 205	• 225
• 11	• 31	• 50	• 69	• 88	• 107	• 127	• 146	• 166	• 186	• 206	• 226
• 12	• 32	• 51	• 70	• 89	• 108	• 128	• 147	• 167	• 187	• 207	• 227
• 13	• 33	• 52	• 71	• 90	• 109	• 129	• 148	• 168	• 188	• 208	• 228
• 14	• 34	• 53	• 72	• 91	• 110	• 130	• 149	• 169	• 189	• 209	• 229
• 15	• 35	• 54	• 73	• 92	• 111	• 131	• 150	• 170	• 190	• 210	• 230
• 16	• 36	• 55	• 74	• 93	• 112	• 132	• 151	• 171	• 191	• 211	• 231
• 17	• 37	• 56	• 75	• 94	• 113	• 133	• 152	• 172	• 192	• 212	• 232
• 18	• 38	• 57	• 76	• 95	• 114	• 134	• 153	• 173	• 193	• 213	• 233
• 19	• 39	• 58	• 77	• 96	• 115	• 135	• 154	• 174	• 194	• 214	• 234
• 20	• 39	• 58	• 77	• 96	• 116	• 136	• 155	• 175	• 195	• 215	• 235

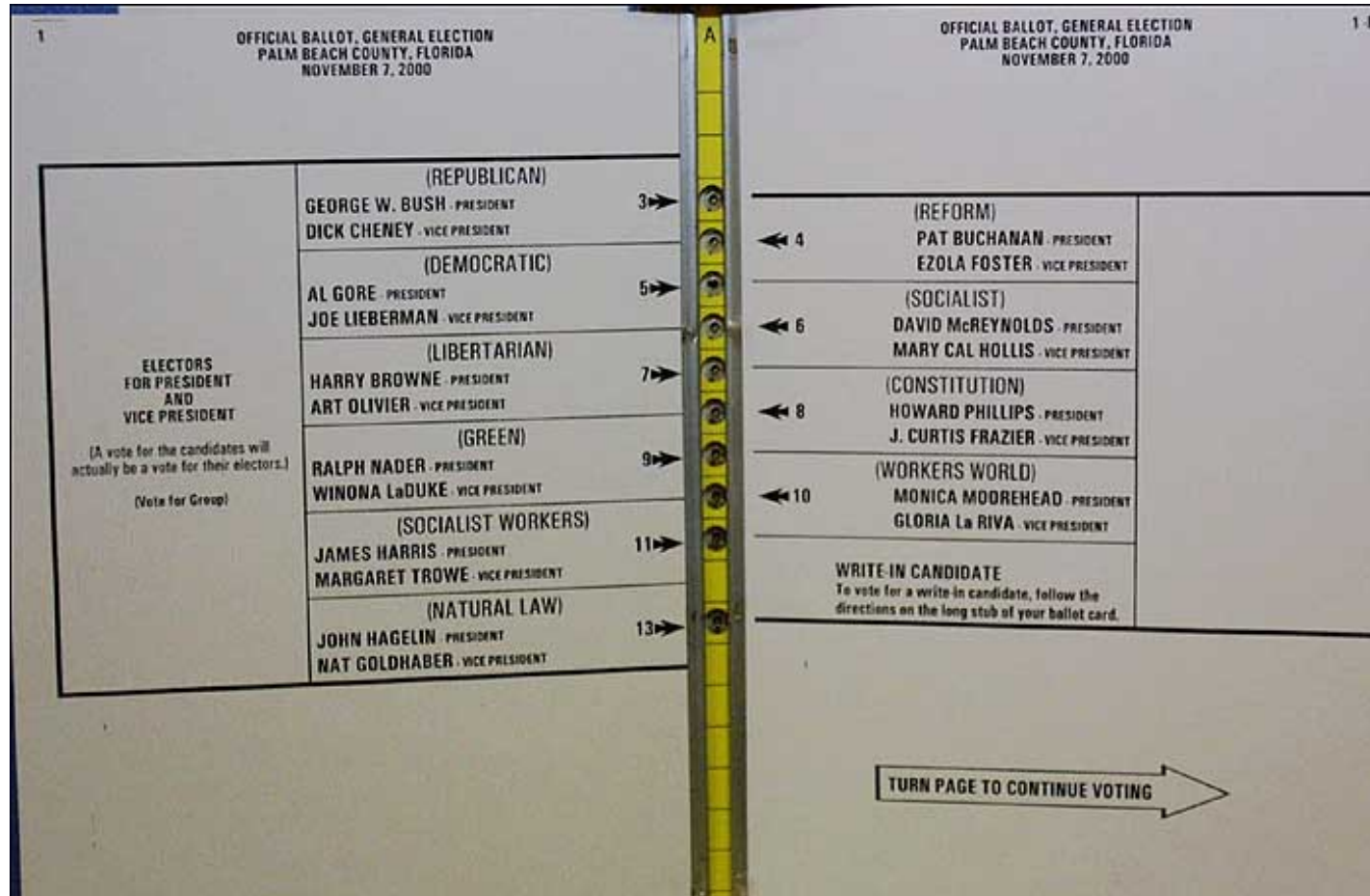
TO BE FILLED IN BY COUNTING BOARD ONLY

PRECINCT NO. _____

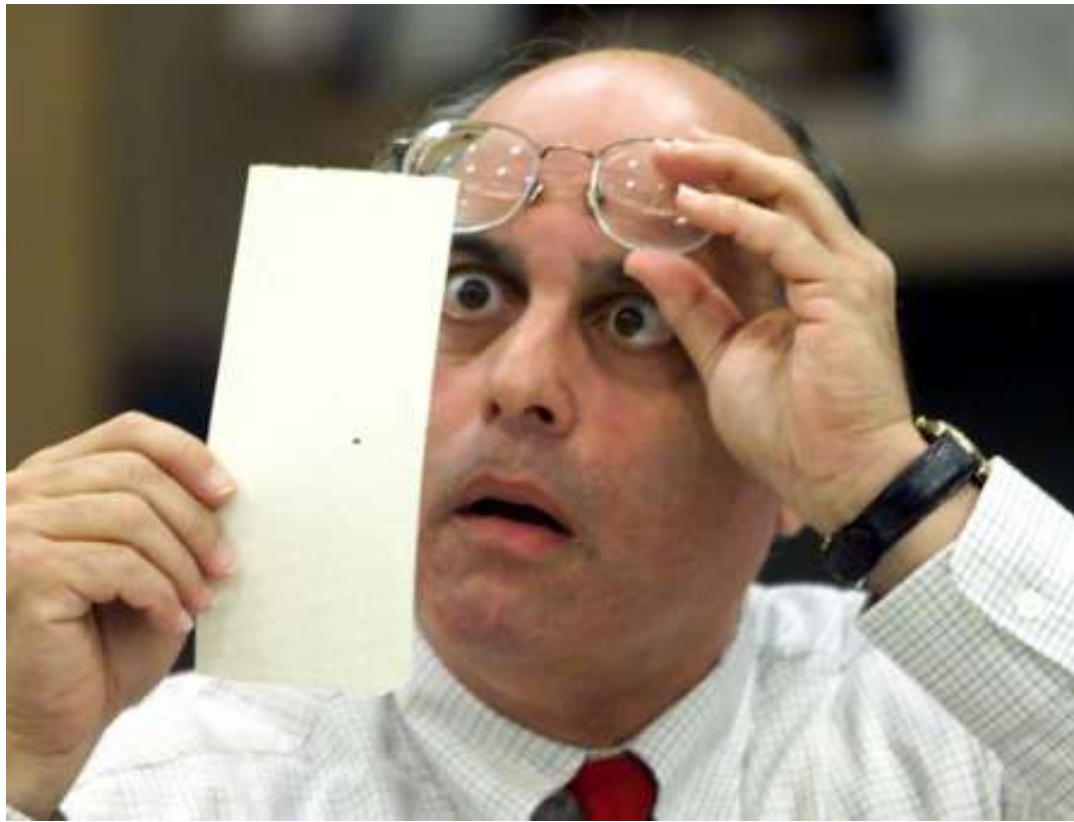
WRITE-IN NO. _____

4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80

The famous “butterfly ballot”



A “dimpled chad” ???



Optical scan ("opscan")

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



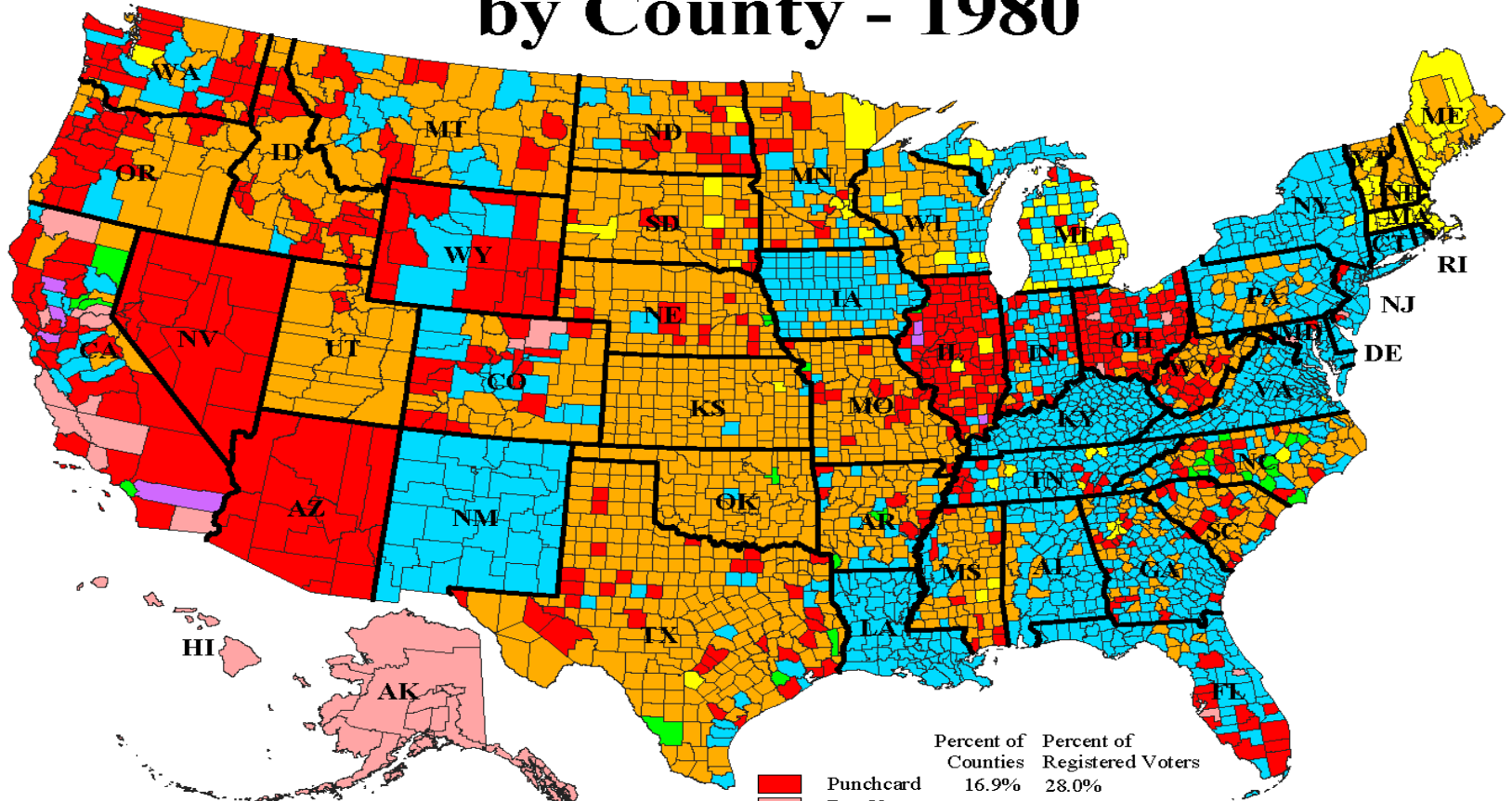
Internet voting (?)

- ◆ 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



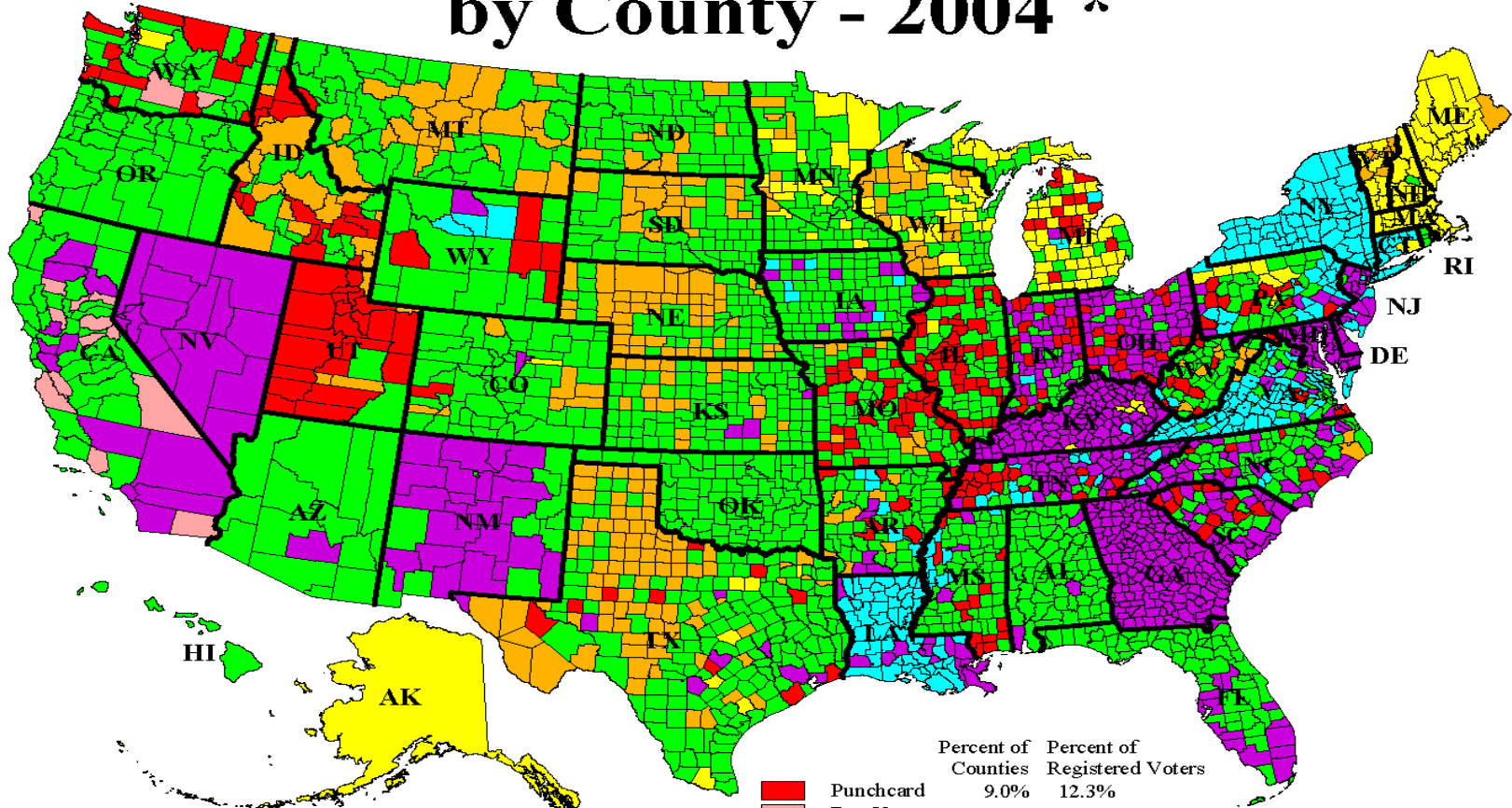
Alaska does not have counties.
DataVote system is used statewide
except for a few paper ballot precincts.

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.

	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%

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 *

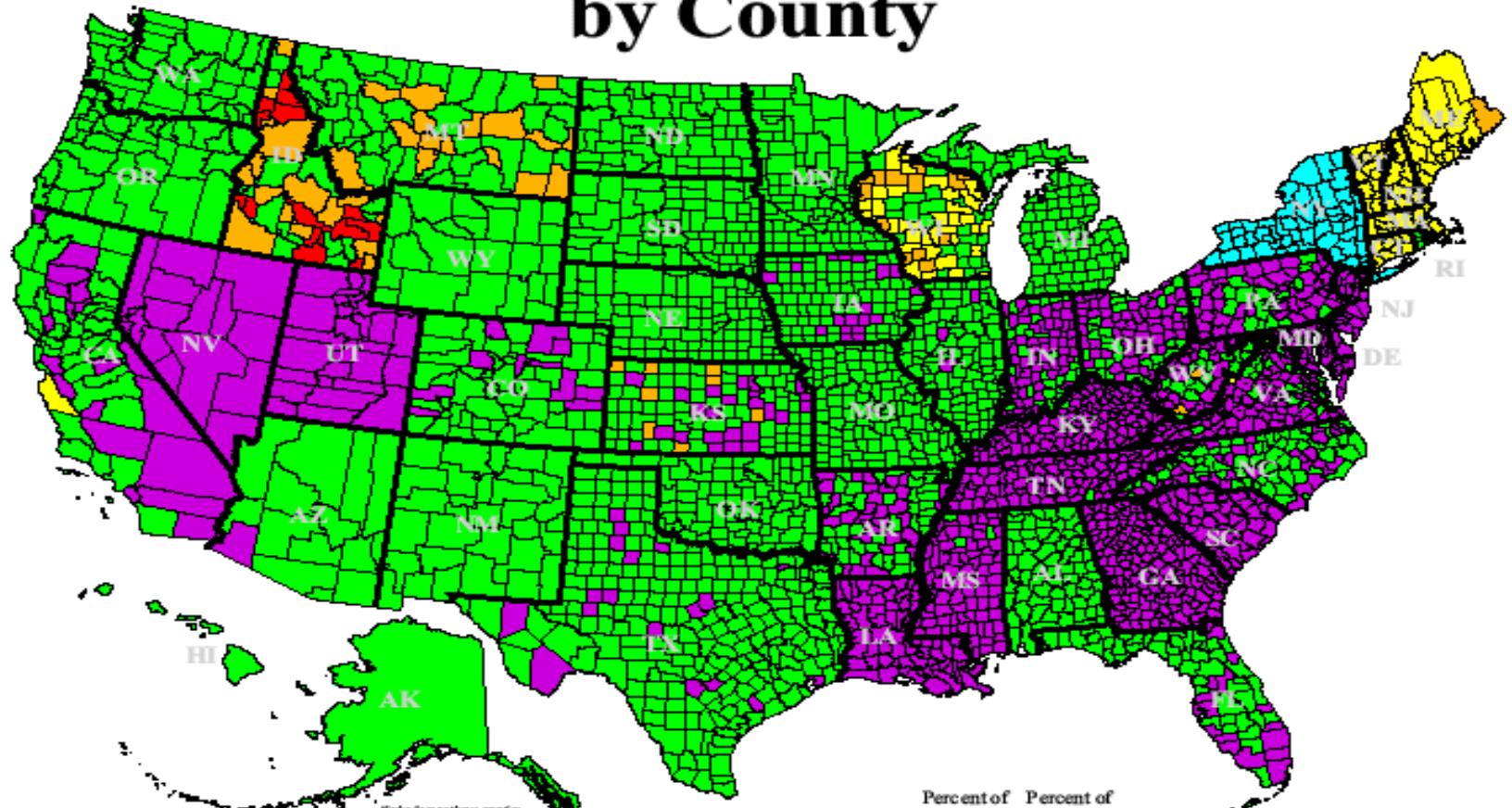


Alaska does not have counties.
AccessVote system is used statewide
except for a few paper ballot precincts.

	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.

November 2006 Voting Equipment Usage by County

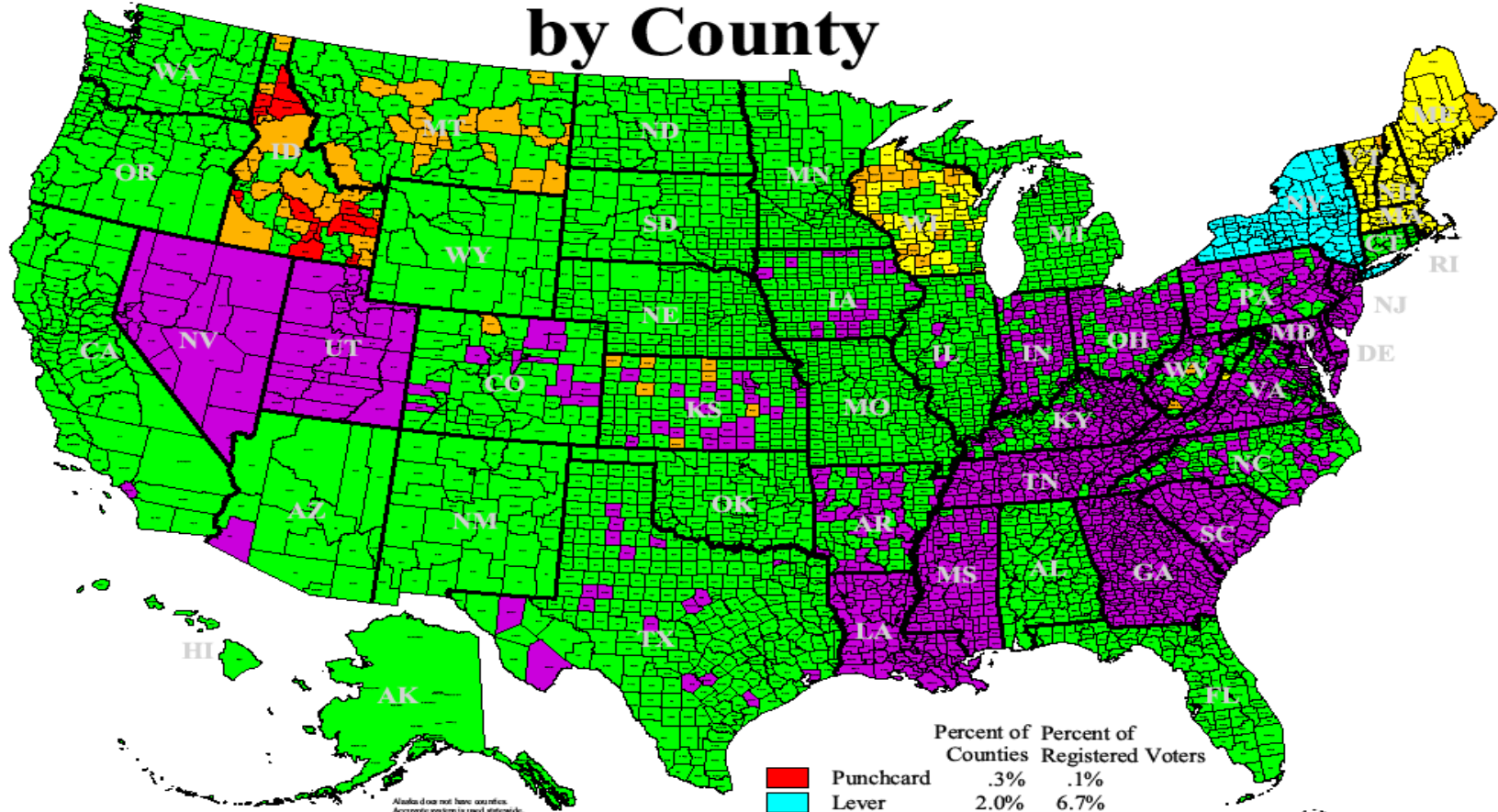


*Alaska does not have counties.
A statewide system is used statewide.*

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

	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%

November 2008 Voting Equipment Usage by County



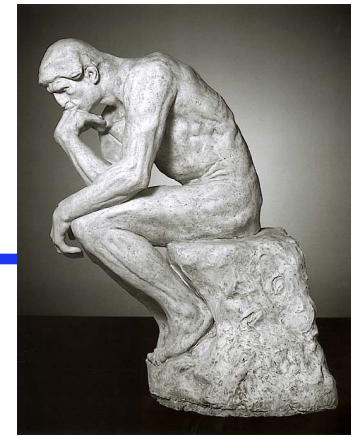
Alaska does not have counties.
Accurate system is used statewide.

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
■ 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%

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 $1-\alpha$ chance of finding corruption of this size or larger.
- ◆ Audit precinct i with probability $1 - \alpha^{v_i/M}$
- ◆ 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”

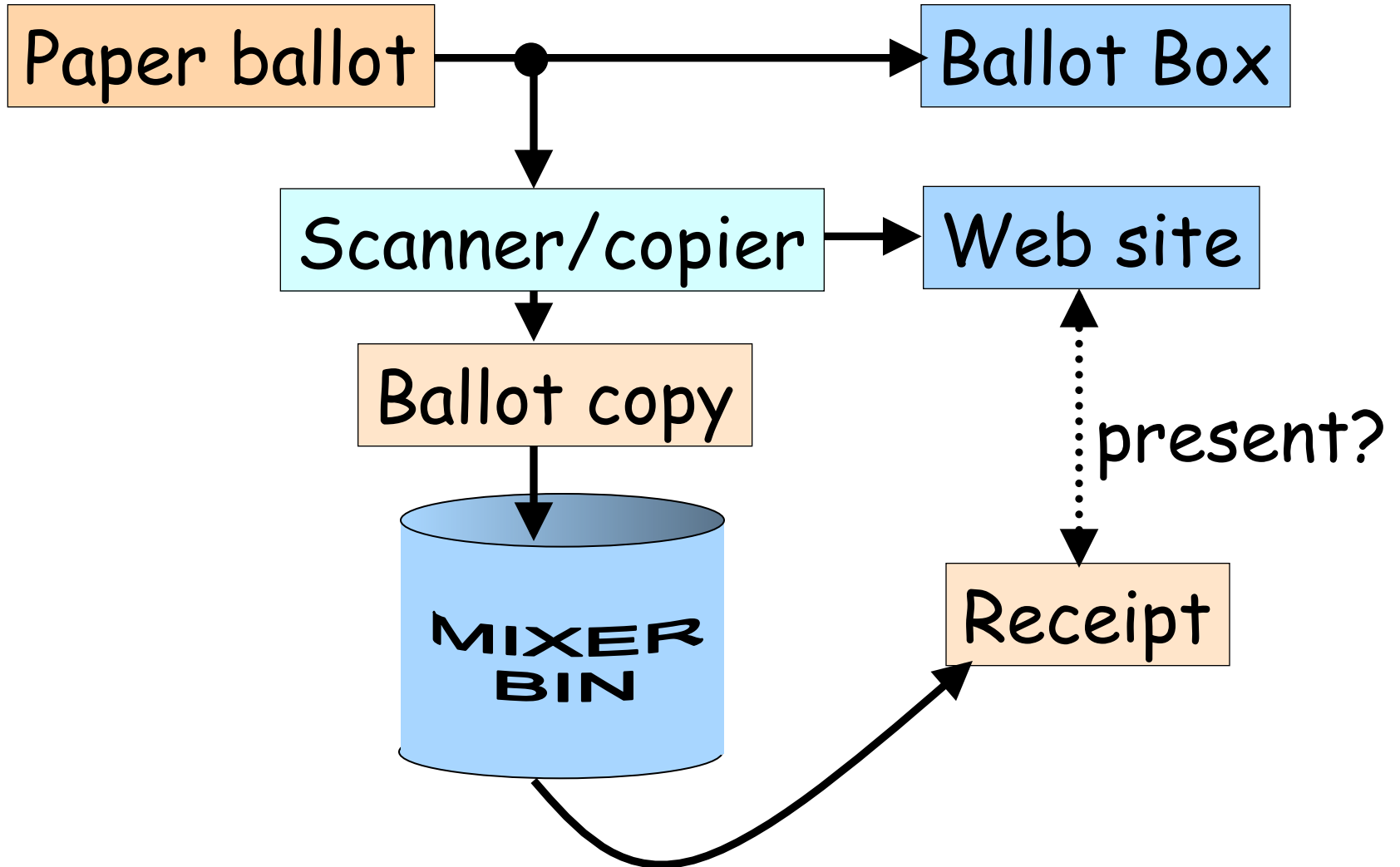
- ◆ Provide “end-to-end” integrity:
 - Votes verifiably “cast as intended”
 - Votes verifiably “collected as cast”
 - Votes verifiably “counted as collected”
- ◆ VVPAT only gets the *first* of these; once ballot is cast, what happens thereafter depends on integrity of “chain of custody” of ballots.
- ◆ “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

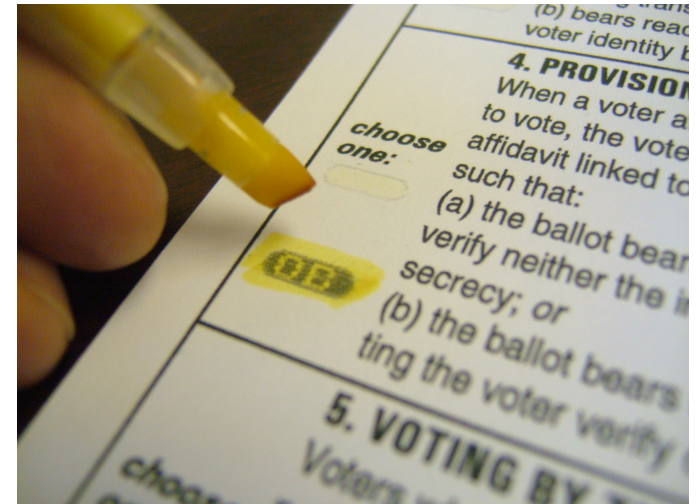


Twin integrity

- ◆ 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

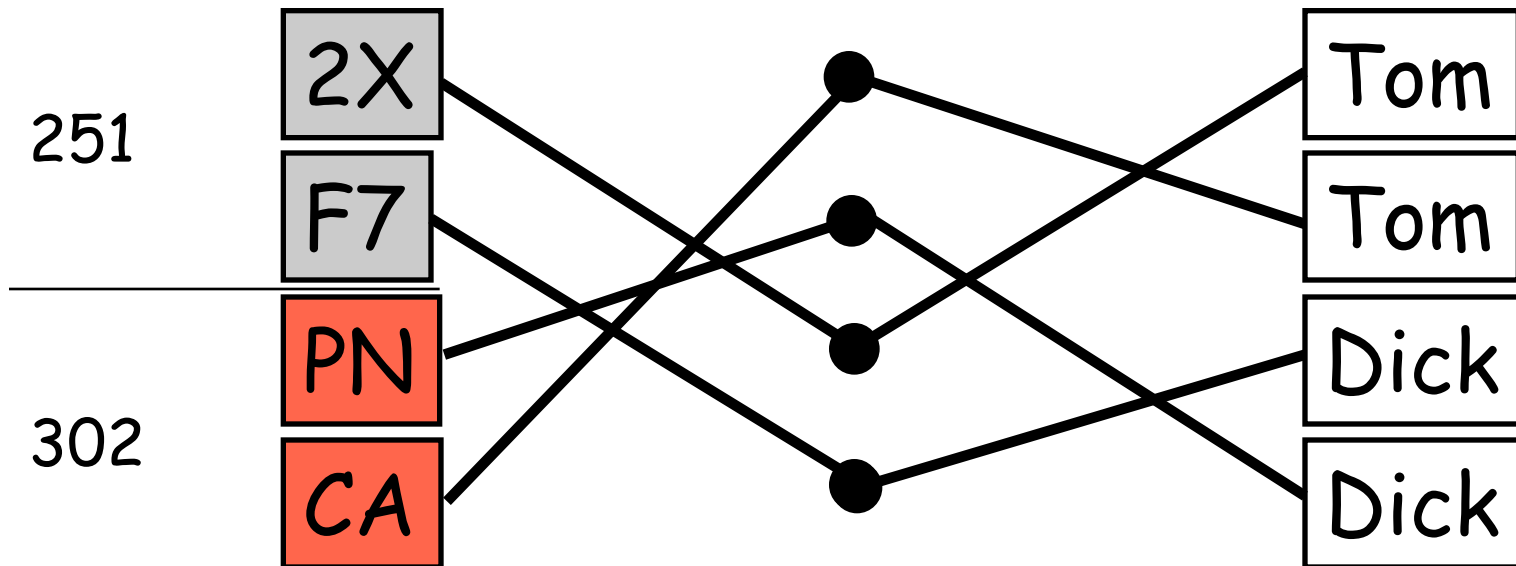
The logo consists of the letters 'F7' in a bold, white, sans-serif font, centered within a gray oval with a thin black border.

- ◆ 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

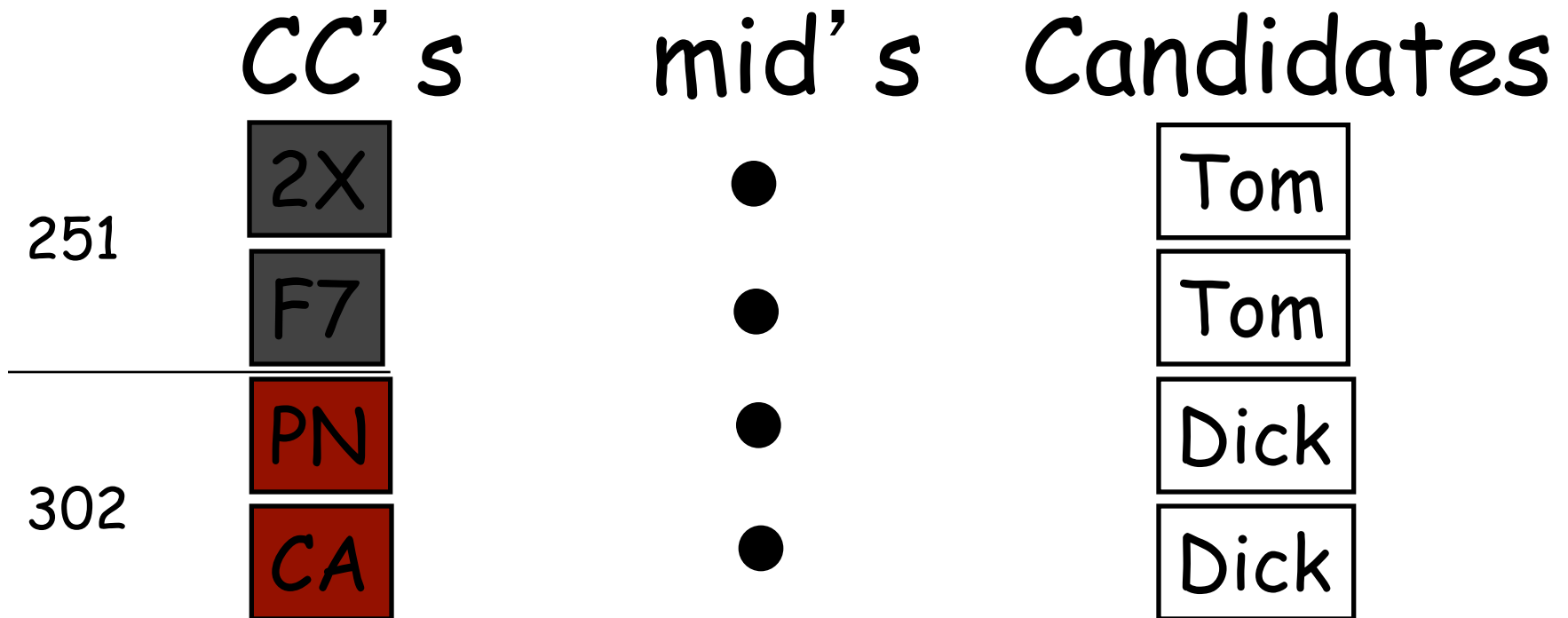
- ◆ Officials create two permutations:
 $CC's \rightarrow mid's \rightarrow candidates$

CC's mid's Candidates



Scantegrity II integrity

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



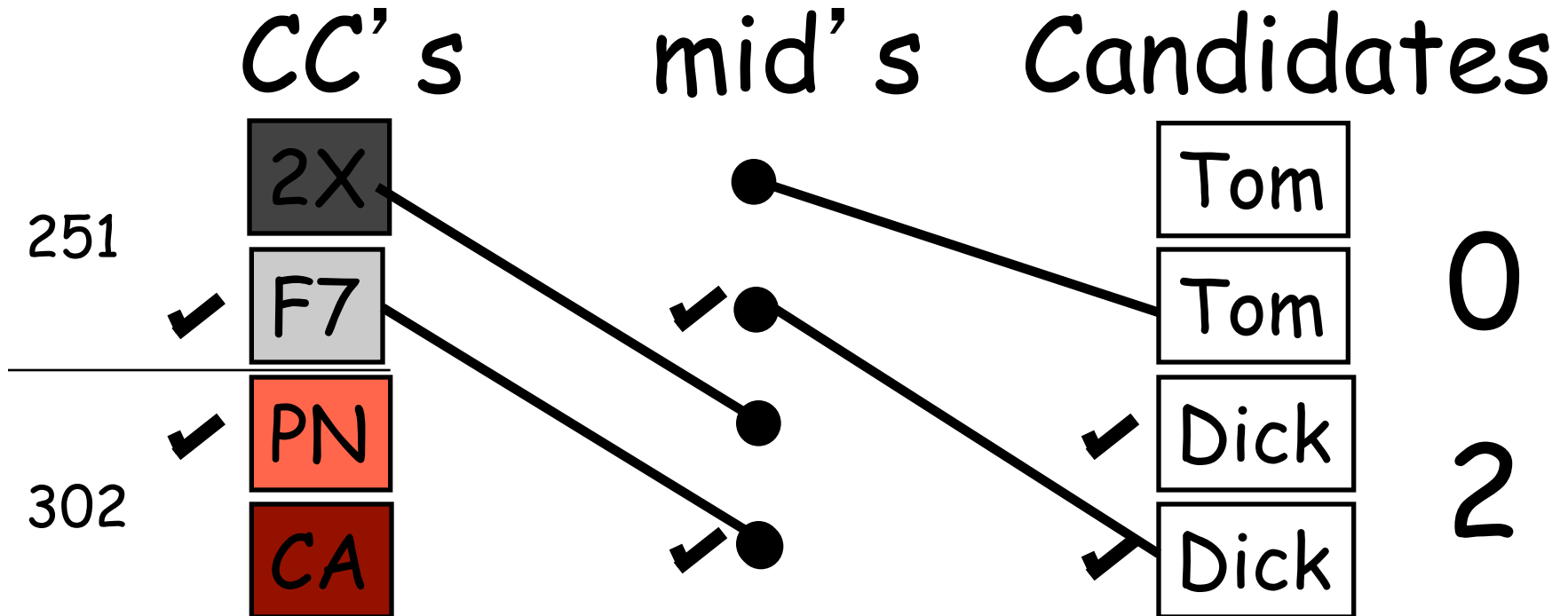
Scantegrity II integrity

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

	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

City of Takoma Park, Maryland
MUNICIPAL ELECTION
NOVEMBER 3, 2009

Cludad de Takoma Park, Maryland
ELECCIONES MUNICIPALES
3 DE NOVIEMBRE DE 2009

OFFICIAL BALLOT — WARD 3

BOLETA OFICIAL — DISTRITO ELECTORAL 3

Instructions: Vote for candidates by indicating your first-choice candidate, your second-choice candidate, and so on. You are free to rank only a first choice if you wish.

Instrucciones: Vote por los candidatos indicando el candidato que sea su primera opción, el candidato que sea su segunda opción, y así sucesivamente. Si lo desea, puede limitarse a seleccionar solamente al candidato que sea su primera opción.

Do not fill in more than one oval per column. Do not fill in more than one oval per candidate. Do not skip numbers in the ranking sequence.

No rellene más de una casilla por cada columna. No rellene más de una casilla por cada candidato. No salte números en la secuencia de clasificación por orden.

To vote for a person whose name is not printed on the ballot, write the name in the space provided and fill in one box in the column indicating your ranking of the write-in candidate.

Para votar por una persona cuyo nombre no está impreso en la boleta, escriba el nombre en el espacio provisto y rellene una casilla en la columna para indicar el orden de clasificación del candidato que se ha añadido.

If you make a mistake on your ballot, return it to the judge and get another.

Si usted comete un error en su boleta, devuélvasela al juez y otra.

Do not make any identifying marks on your ballot.

No haga marcas en su boleta que puedan identificarlo.

When you mark an oval to rank a candidate, a code will be revealed that you may later use to verify your vote online. See the instruction sheet in the voting booth.

Cuando usted marque la casilla para clasificar a un candidato, verá un código que podrá usar posteriormente para verificar su voto por Internet. Vea la hoja de instrucciones en la cabina de votación.

MAYOR ALCALDE			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
Roger B. Schlegel	0276		
Bruce Williams		0250	
Tom Smith		0281	
Write-In Candidate/Para añadir a un candidato			

CITY COUNCIL MEMBER WARD 3 MIEMBRO DEL CONSEJO DE LA CIUDAD DISTRITO ELECTORAL 3			
Rank candidates in order of choice Clasifique a los candidatos por orden de preferencia	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
Dan Robinson			0255
Write-In Candidate/Para añadir a un candidato			

3 - 972853
Online Verification Number
Número de Verificación por Internet

	1st choice 1ra opción	2nd choice 2da opción	3rd choice 3ra opción
cia	0276		
			0255
	0281		

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

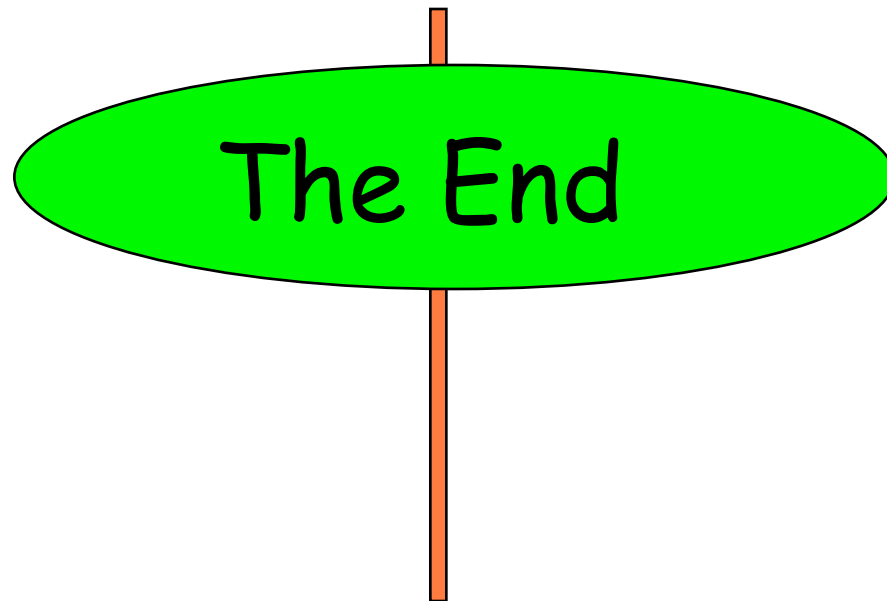
Lilley Coney

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!