Electronic Voting

Mohammed Awad

Ernst L. Leiss
coscel@cs.uh.edu

Partially funded under NSF Grant #1241772
Any opinions, findings, conclusions, or recommendations expressed herein are those of the authors and do not reflect the views of the National Science Foundation

Outline

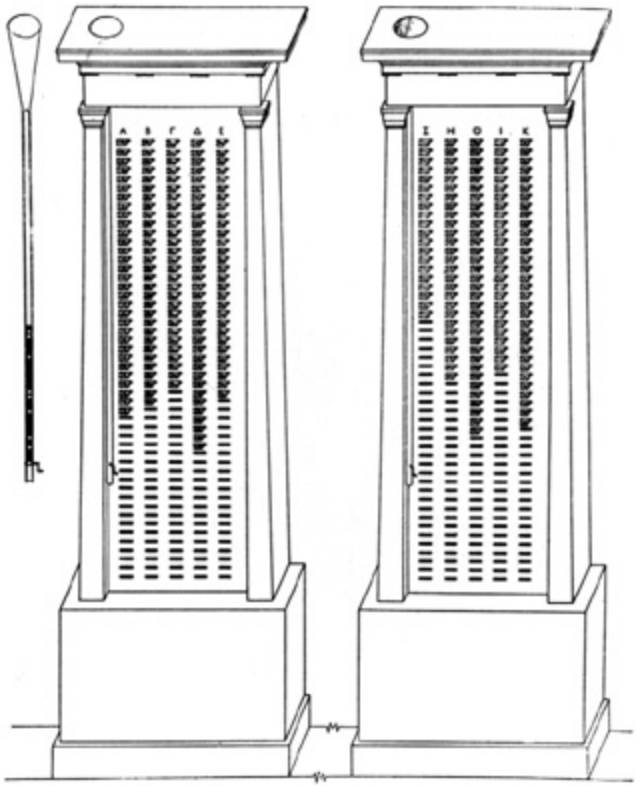
- Introduction to Voting
- Electronic Voting
- Paper Ballots
- Using Cryptography
- Internet Voting
- Using Biometrics

Introduction to Voting

History, principles, and requirements

Voting History

- In the museum of the Agora in Athens, there are the remains of ancient voting machines, the *kleroterion*
- Made of marble, they had columns with narrow slots for tokens or cards



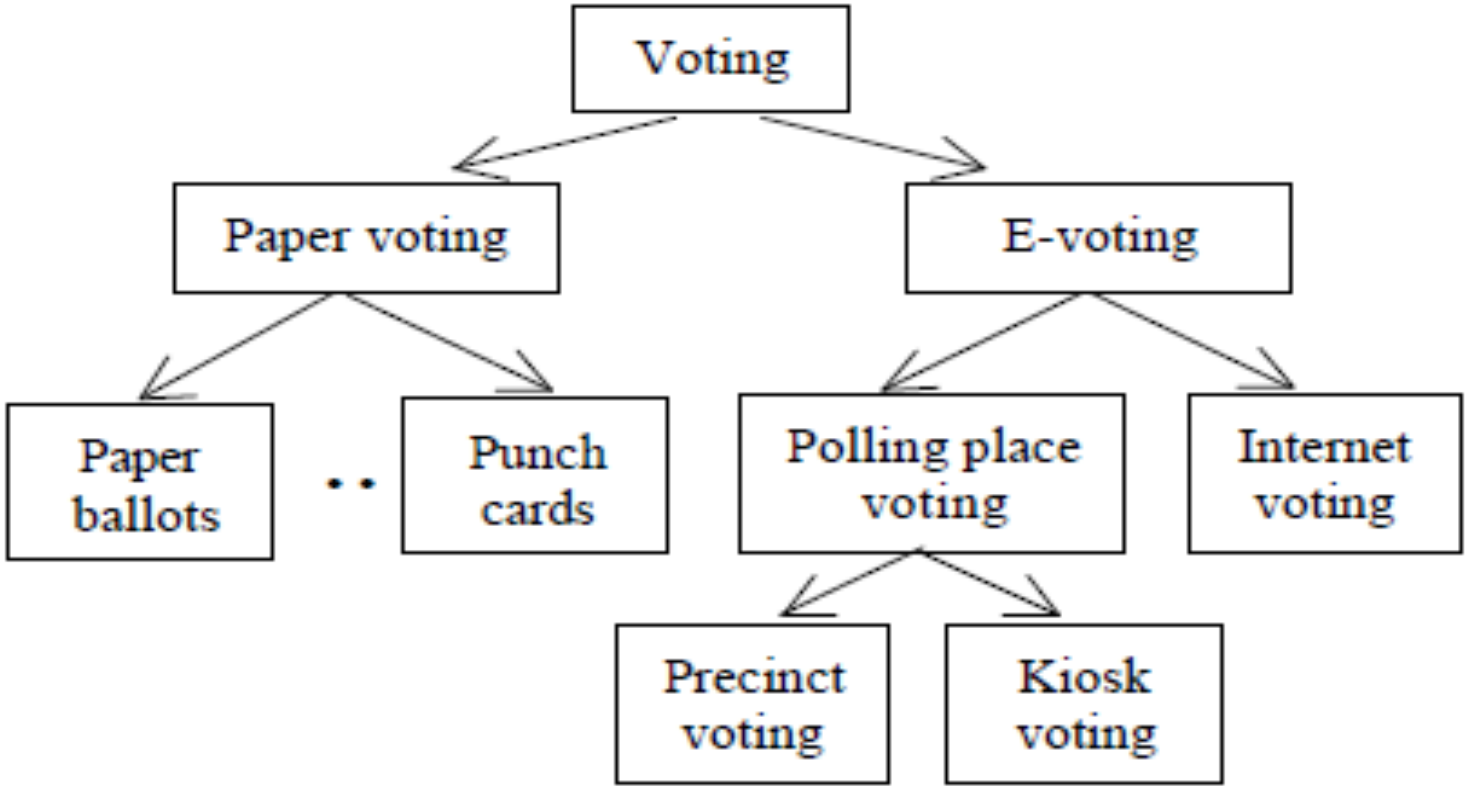
“Good” voting system criteria

- Preserve the *anonymity* of a voter’s ballot
- Is *tamper-resistant* to thwart a wide range of attacks
- Is comprehensible to and usable by the *entire* voting population

Election Transparency

- The fundamental basis of election integrity
- Handling and counting ballots are completely open to public view
- Except, of course, each individual's voting choices

Voting Technology



- E-voting system: Election data are handled (stored, counted, etc.) digitally

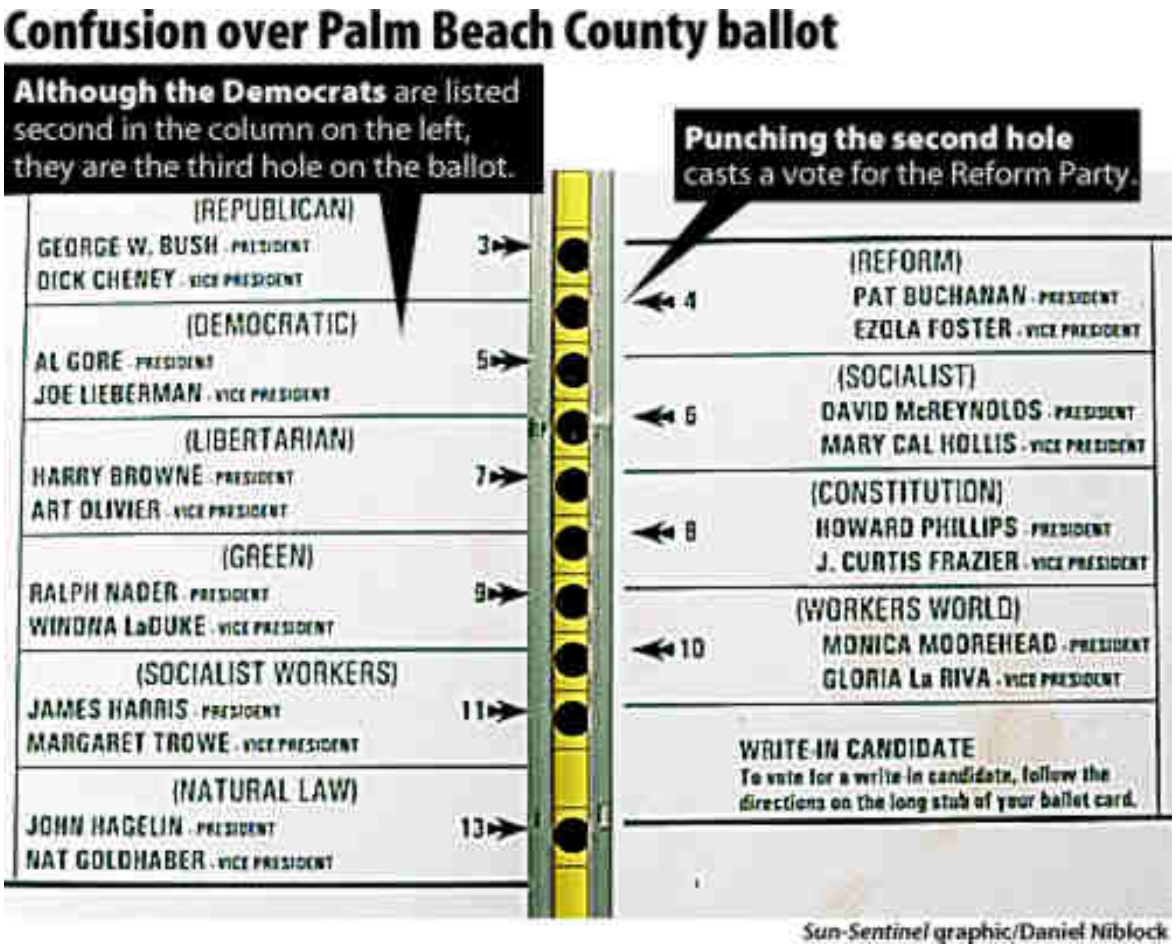
The Electoral Process

- Voter Registration
- Voter Authentication
- Vote Collection
- Vote Tabulation

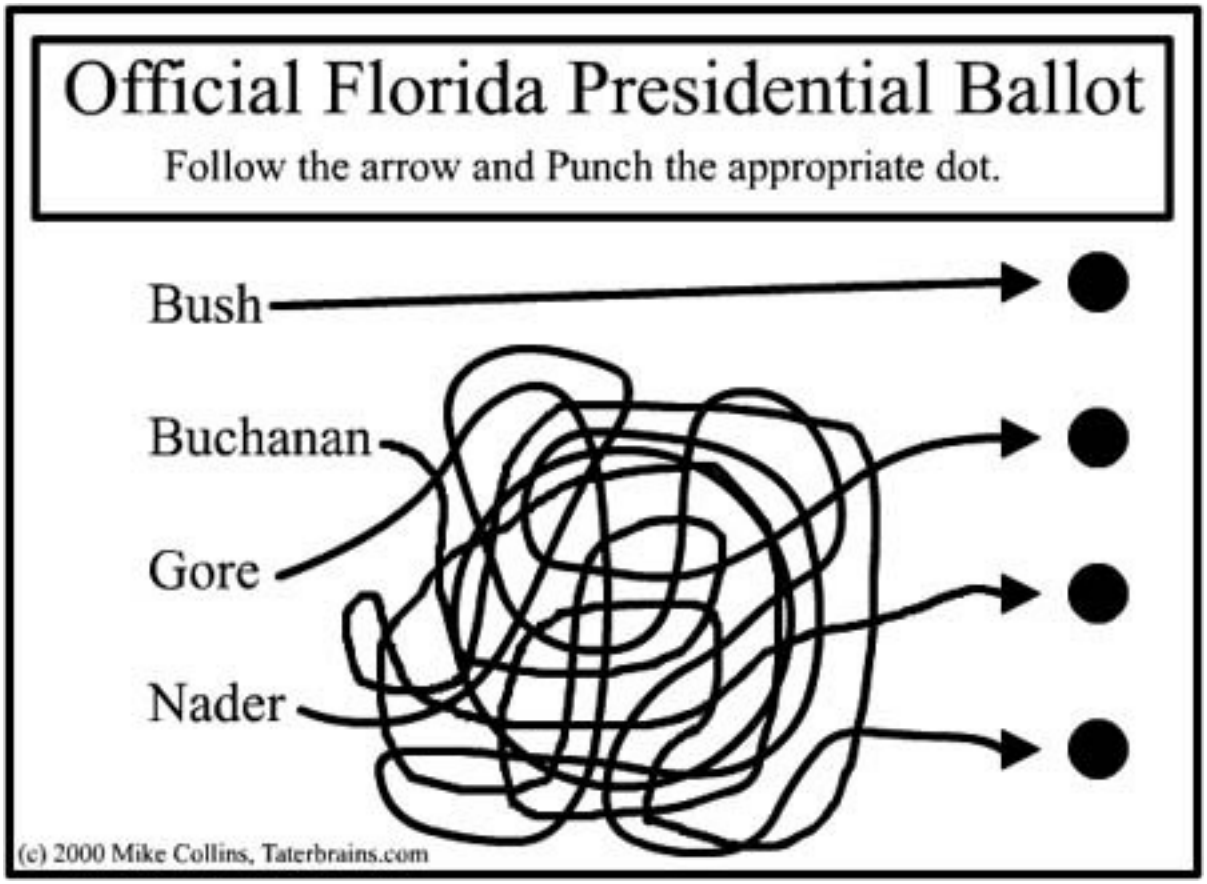
The Election Principles

- Universality
- Equality
- Freedom of Choice
- Secrecy
- Security
- Directness
- Trust

Florida US Presidential Election, 2000



Ballot Criticized



How Did it All Start?

- The Butterfly Ballot
  - Confusing design
  - Resulted in overvoting and undervoting
  - Gore's rejected ballots were 10 times more than the winning margin
- Almost 2 million ballots were disqualified in the 2000 elections due to overvoting or undervoting

Electronic Voting

As a solution?

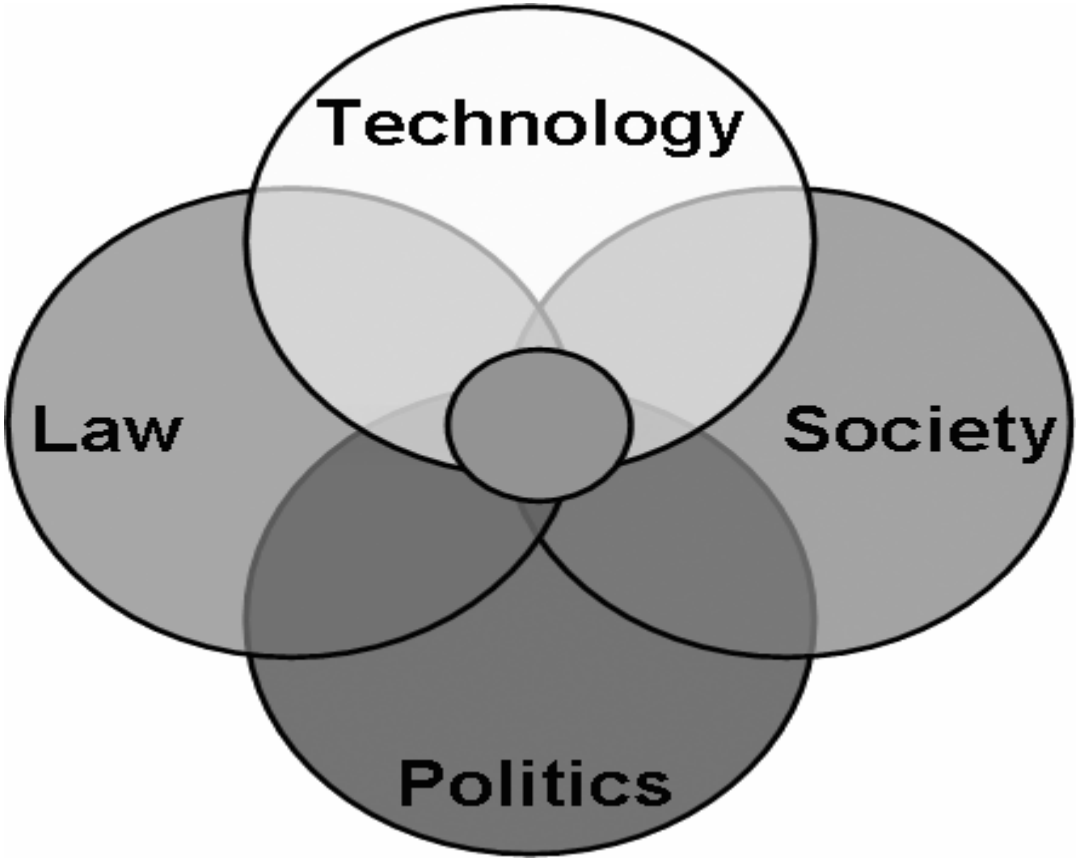
Proposed Solution

- Help America Vote Act (HAVA)
  - Signed into law in 2002
  - Multi-million dollar budget
  - Goal: upgrade voting systems by replacing
    - Punched Card Voting Systems
    - Lever Voting Systems
  - Did it backfire?

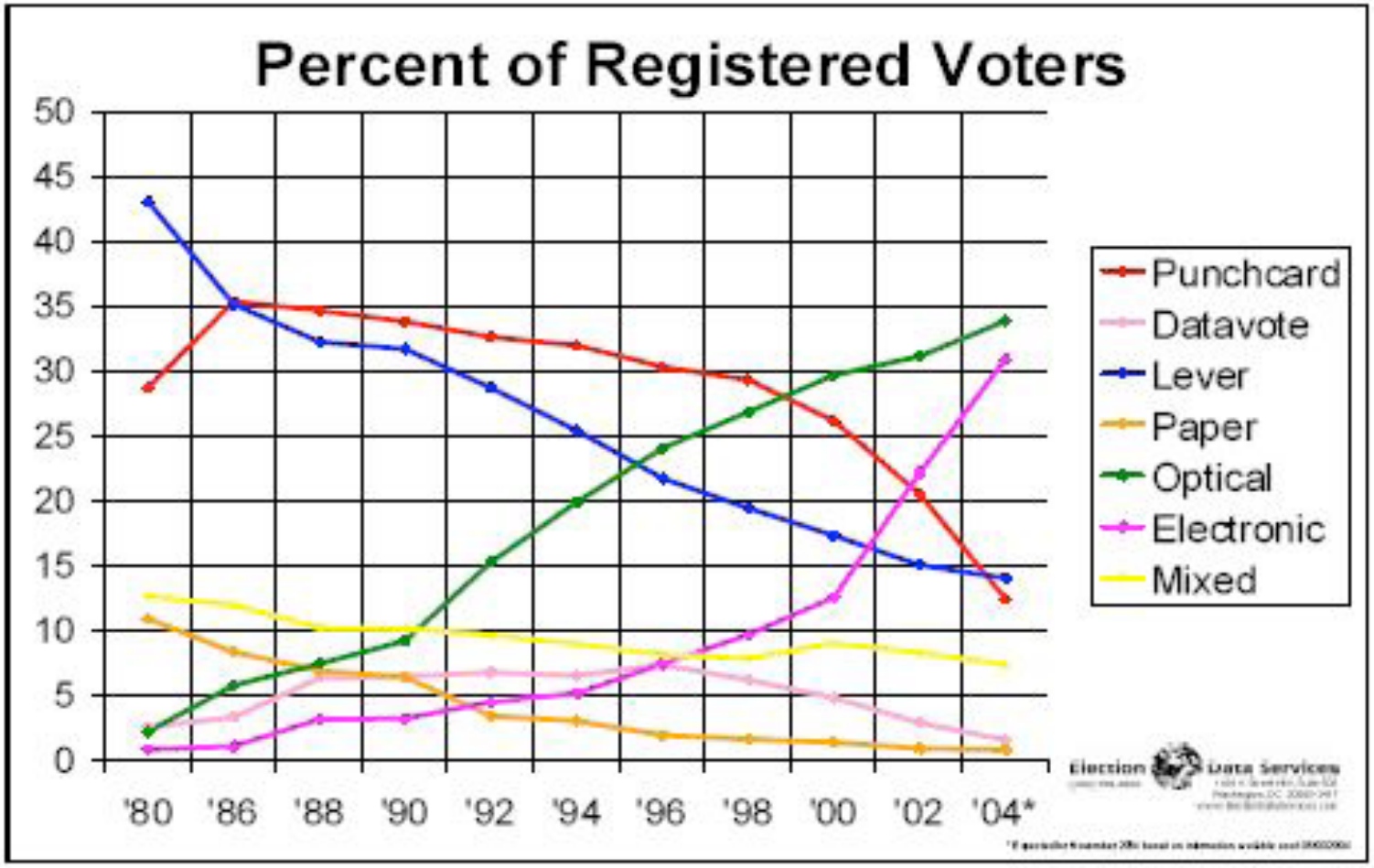
E-voting Advantages

- Speed
  - Around 117 million ballots were cast in the US presidential election (Nov. 2012)
- Increase voter turnout
  - Provides Convenience?
- New potentials:
  - Supporting people with disabilities
  - Providing ballots in several languages
  - Solving the overseas voting issues

Dimensions of E-voting



Voting Technology Used (US)



No Transparency in E-voting

- Electronic processes that record and count the votes are not open to public scrutiny
- Courts have ruled that election software is a trade secret
- Recording and tallying the votes are performed in secret

E-voting Implementations

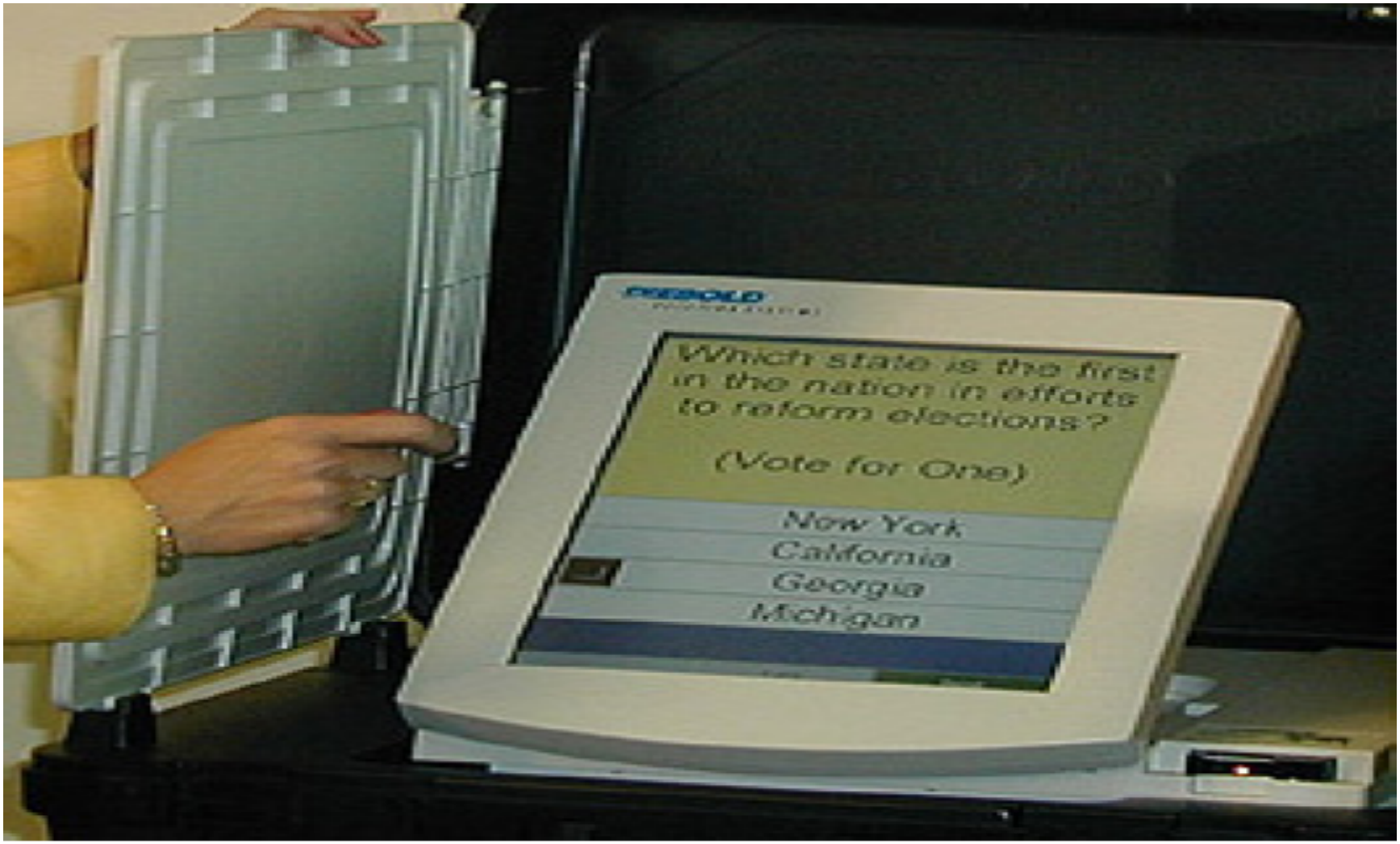
1. Voting at a supervised poll-site using electronic equipment
2. Voting at an unsupervised electronic kiosk
3. Remote voting using the voter's equipment (at a place of the voter’s choosing)

Direct Recording Electronic

- DRE systems completely eliminate paper ballots from the voting process

1. Voter goes to his home precinct
2. Voter is given a token
3. Voter enters the token
4. Voter votes
5. Vote is confirmed

DIEBOLD Voting System



DRE problem

- The most fundamental problem with such a voting system is that the entire election hinges on the correctness, robustness, and security of the software within the voting terminal

Let's Paraphrase

- Secrecy vs. Accuracy
- Election hinges on the correctness, robustness, and security of the software within the voting terminal.
- Viable solution: Voter-Verifiable Audit Trail (VVAT)
  - To provide manual auditing feature

VVAT is Not The Optimal Solution

- NJIT Study:
  - Paper jams
  - Security flaws
  - Performance issues

- Rice University Study:
  - 63% of voters failed to notice errors on summary screens and paper trails.

Obscure is Secure!

- Diebold's AccuVote-TS source code was mysteriously released
- Announced by Bev Harris and discussed in her book, *Black BoxVoting*
- Used in 37 states
- The 2nd largest DRE vendor in the US

AccuVote-TS Analysis & Findings

- Written in C++ and runs on Windows CE
- Voters can easily program their own smartcards
- The protocols do not use cryptographic techniques to authenticate either end of the connection nor do they check the integrity of the data in transit

More Analysis

- Cryptography, when used at all, is used incorrectly
- No evidence of any change control process that might restrict a developer's ability to insert arbitrary patches into the code

Possible Attacks

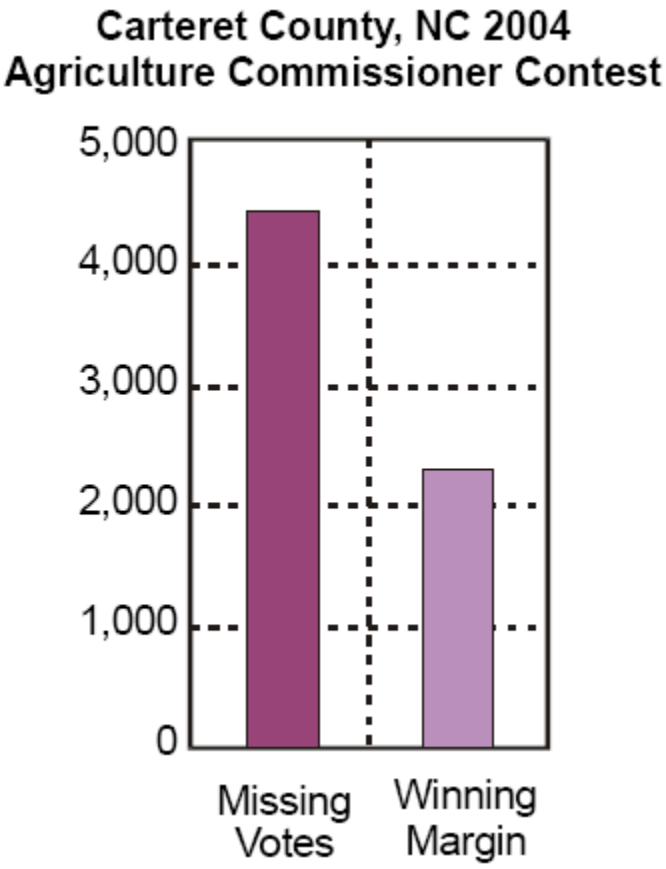
	Voter (with forged smartcard)	Poll Worker (with access to storage media)	Poll Worker (with access to network traffic)	Internet Provider (with access to network traffic)	OS Developer	Voting Device Developer
Vote multiple times using forged smartcard	•	•	•			
Access administrative functions or close polling station	•	•			•	•
Modify system configuration		•			•	•
Modify ballot definition (e.g., party affiliation)		•	•	•	•	•
Cause votes to be miscounted by tampering with configuration		•	•	•	•	•
Impersonate legitimate voting machine to tallying authority		•	•	•	•	•
Create, delete, and modify votes		•	•	•	•	•
Link voters with their votes		•	•	•	•	•
Tamper with audit logs		•			•	•
Delay the start of an election		•	•	•	•	•
Insert backdoors into code					•	•

2004 Concerning Outcomes

Some Problems in 2004 Elections

1. New election needed after E-voting failures

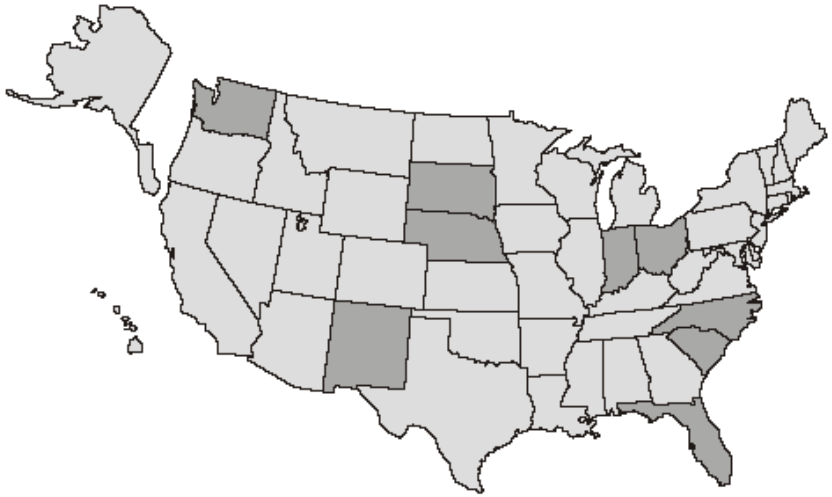
- Supposed to store 10,500 votes
- **Stored only 3,005 votes**



Problems cont.

2. "Phantom" Votes
   Added by Electronic Voting Machines

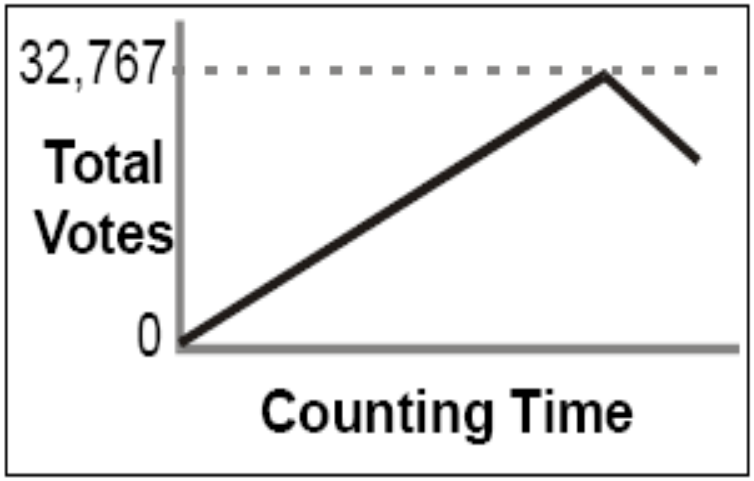
- Mecklenburg County, North Carolina
- **3,000 extra votes**



Problems cont.

3. Software Counts to 32,767 and then Counts Backwards

- Broward County, Florida.
- **ES&S vote-tallying software loses 70,000 votes**



Problems cont.

4. Votes Jump to the Opponent on the Screen.

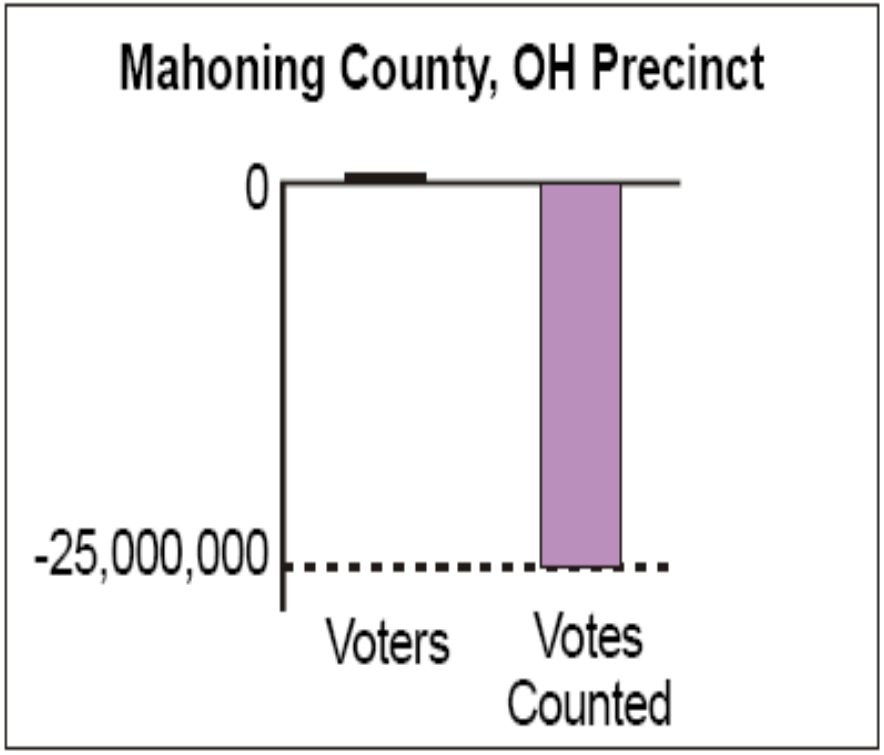
- Bernalillo County, New Mexico

5. DREs Present Incorrect Ballots to Voters

- The U.S. Senate contest was omitted from ballots in three counties of Maryland in March 2004.

Problems cont.

6. Totals Dip into the Negative Numbers



Problems cont.

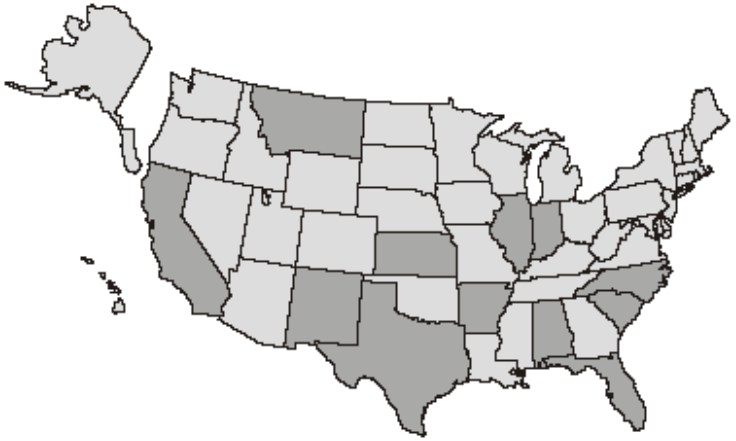
7. DREs Pass Pre-Election Testing, Fail on Election Day.

- Touch-screen voting machines malfunctioned in Mercer County, Pennsylvania.

Problems cont.

8. Programming Errors Give Votes to the Wrong Candidate

- Errors in ballot programming
- How touches on a screen or marks on a ballot are translated into votes



Errors in optical scan ballot programming have caused counting errors in recent elections in these states ... that we know of.

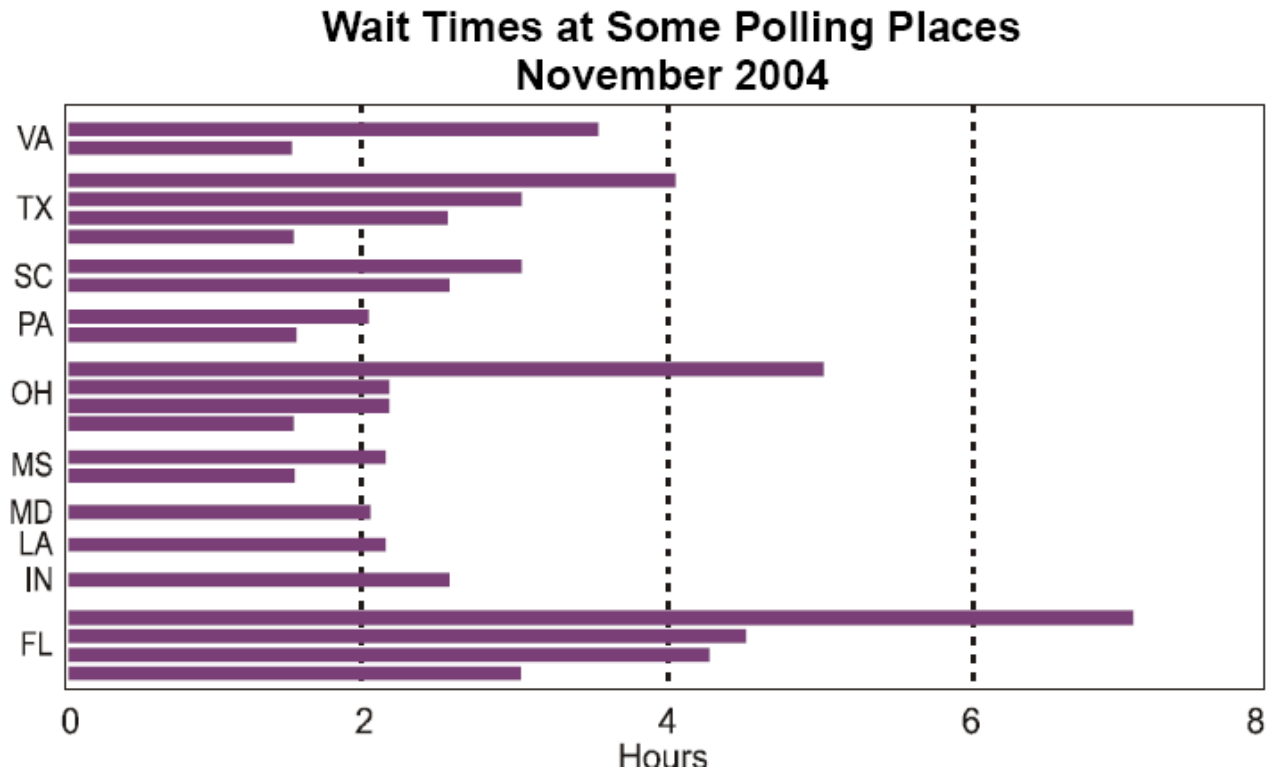
Problems cont.

9. Some DREs Don't Provide the Accessibility they Promise

- A survey of blind voters in Santa Clara County, California

Problems cont.

10. DREs Breakdown Cause Long Lines During the Election



Back to Paper Ballots

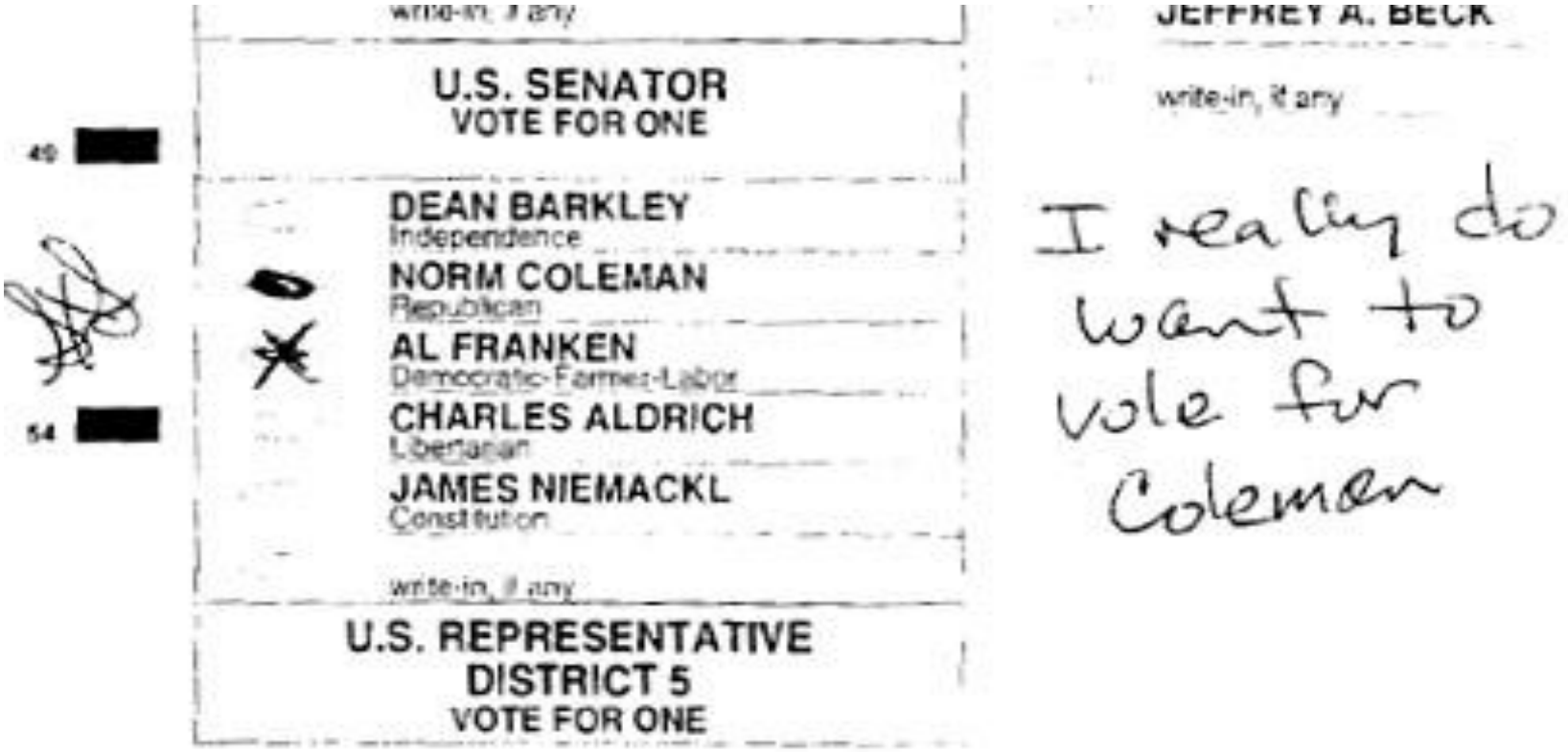
The safest approach?

What Can Go Wrong?

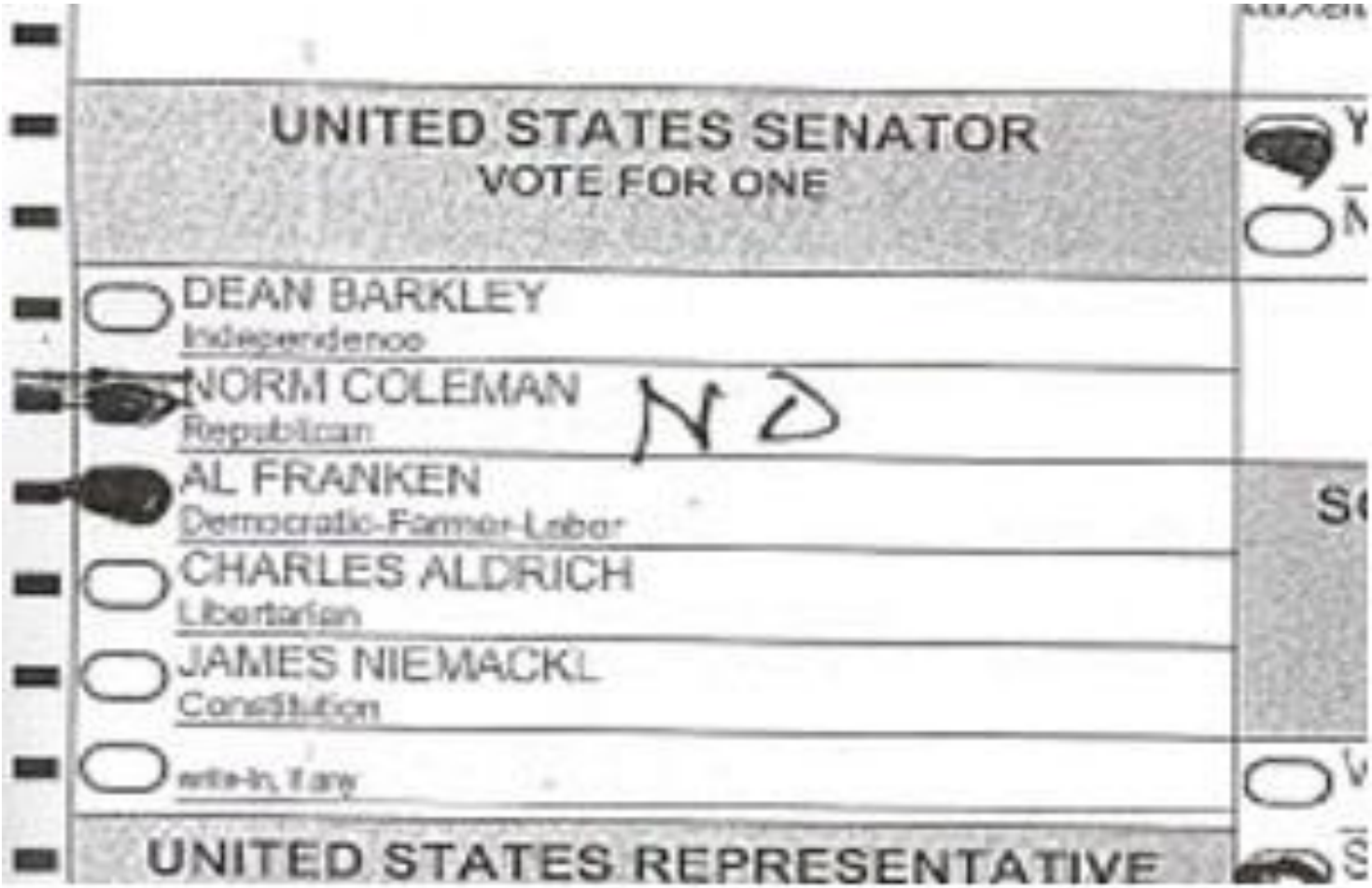
MN Senate Race 2008

- Candidates:
  - Norm Coleman (Republican Party)
  - Al Franken (Democratic Party)
- 2,920,214 Voters
- Coleman won by 215 votes (0.0075%)
  - Triggered automatic recount
- 3 weeks recount, Coleman won by 188 votes
- Over 6,500 challenged ballots

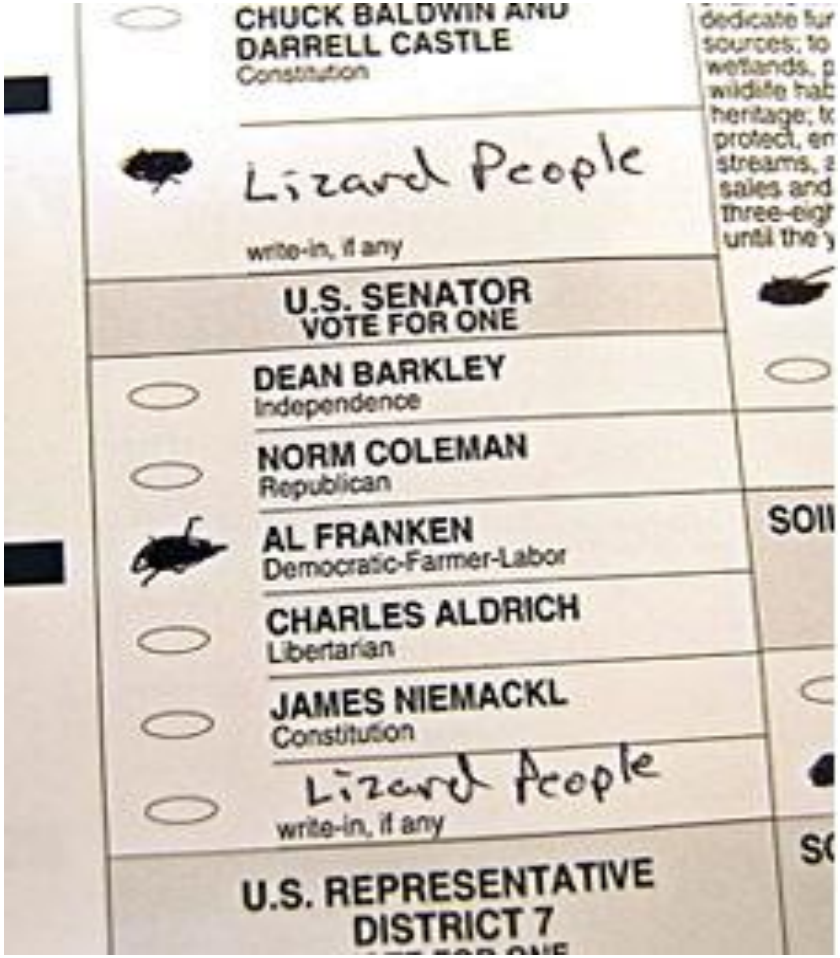
Actual Challenged Ballots I



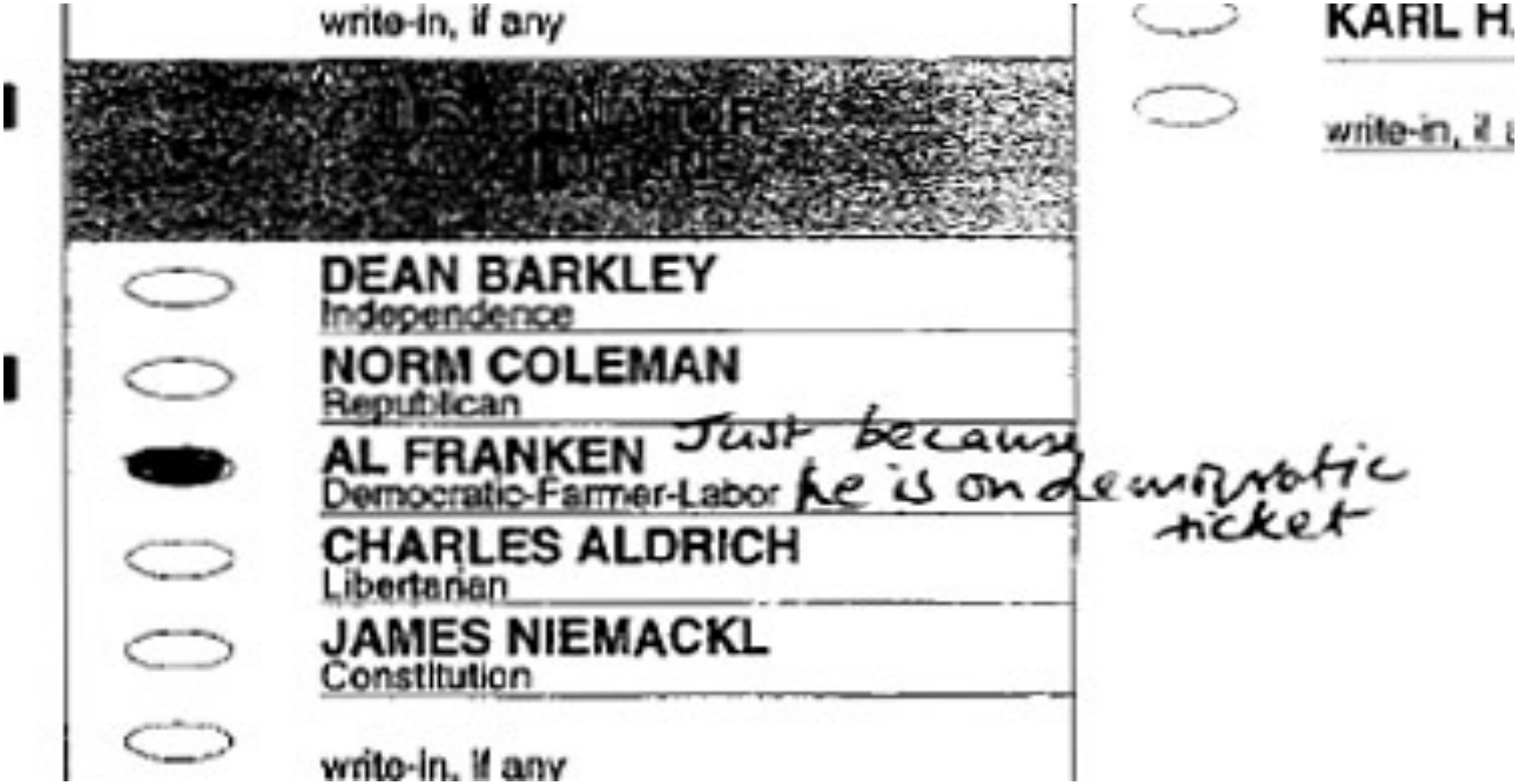
Actual Challenged Ballots II



Actual Challenged Ballots III



Actual Challenged Ballots IV

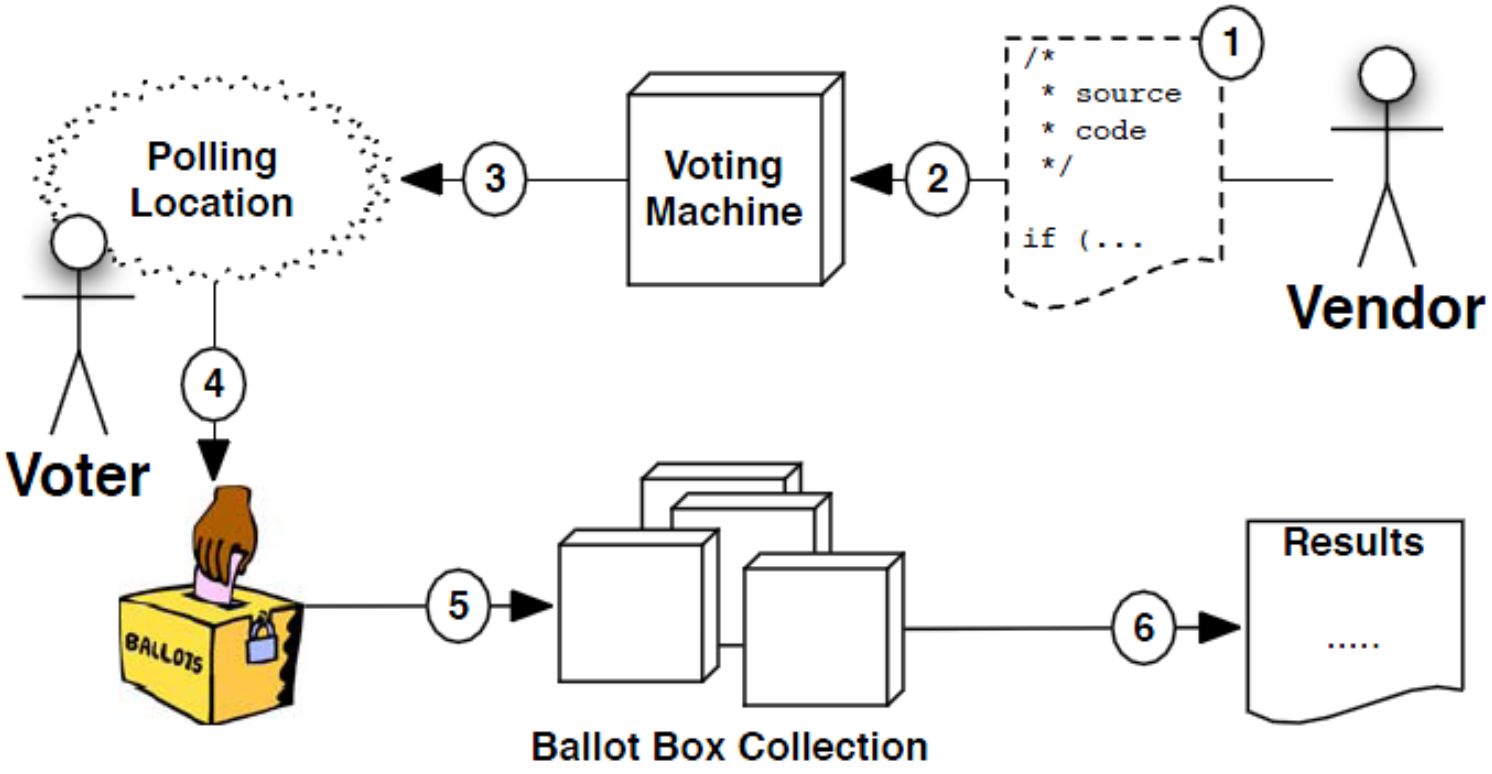


Actual Challenged Ballots V

MN Senate Race 2008 Cont.

- Challenged ballots reduced
- On January 5th 2009; Franken ahead by 255 votes
- On January 6th 2009, Coleman filed for an election contest (trial announced Franken win by 312 votes)
- Coleman appealed to the MN Supreme Court
- MN Supreme Court rejected the appeal on June 30th 2009

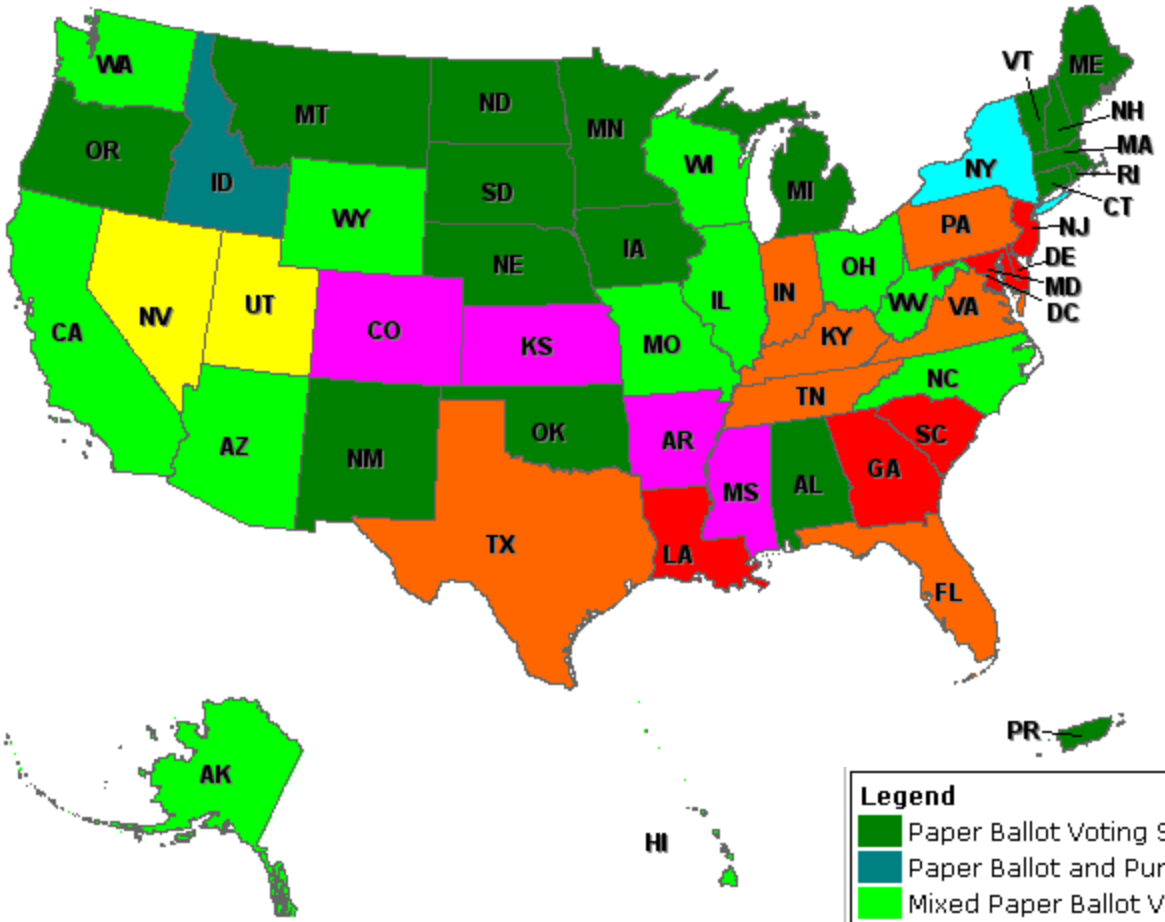
Chain of Custody Voting



Possible Solutions

- Voter Verifiable Audit Trails (VVAT)
  - Paper trails
- Cryptography
- Paper Records and Electronic Audits

2008 Election Equipment



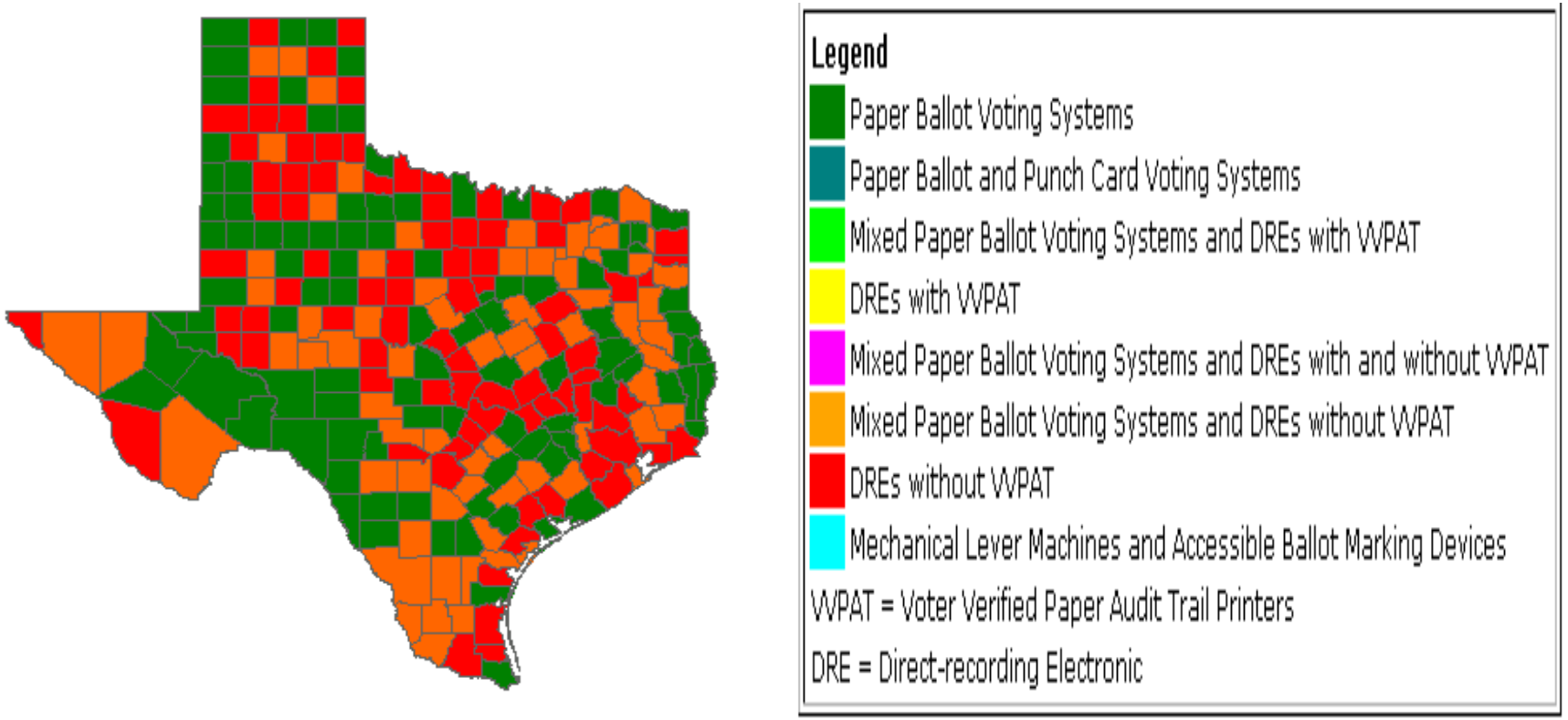
Legend

- Paper Ballot Voting Systems
- Paper Ballot and Punch Card Voting Systems
- Mixed Paper Ballot Voting Systems and DREs with VVPAT
- DREs with VVPAT
- Mixed Paper Ballot Voting Systems and DREs with and without VVPAT
- Mixed Paper Ballot Voting Systems and DREs without VVPAT
- DREs without VVPAT
- Mechanical Lever Machines and Accessible Ballot Marking Devices

VVPAT = Voter Verified Paper Audit Trail Printers

DRE = Direct-recording Electronic

For Example: Texas Election Equipment



Closer look at Texas Election Equipment

Harris county

HART Intercivic eSlate Voting System

- **DRE without VVAT**

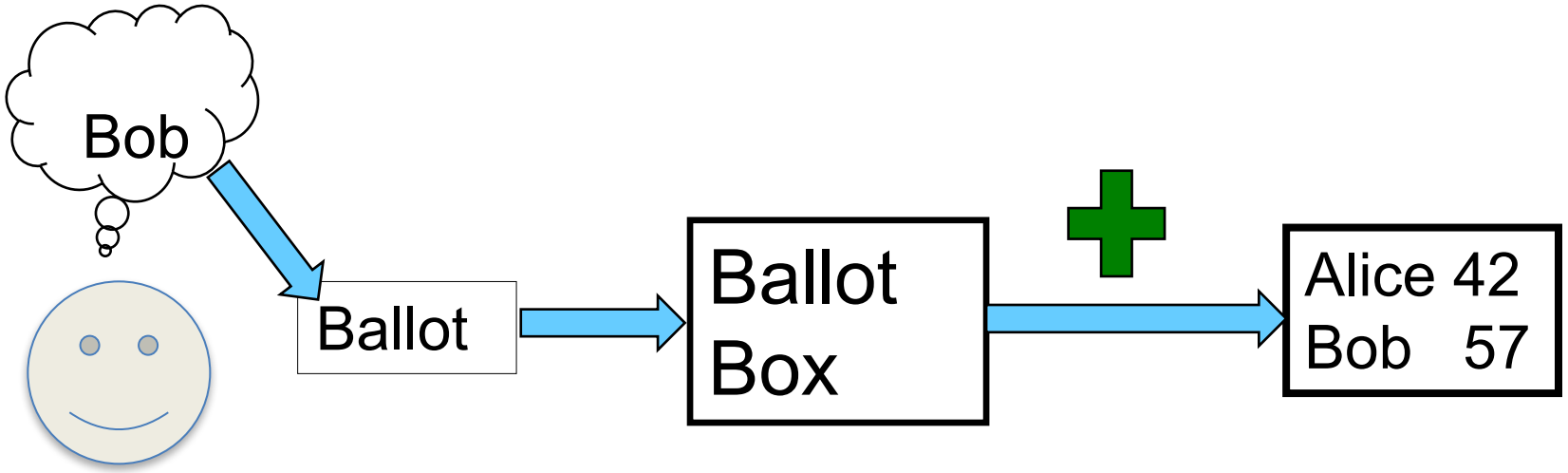
Using Cryptography

To provide the needed assurance

Cryptography as a Solution

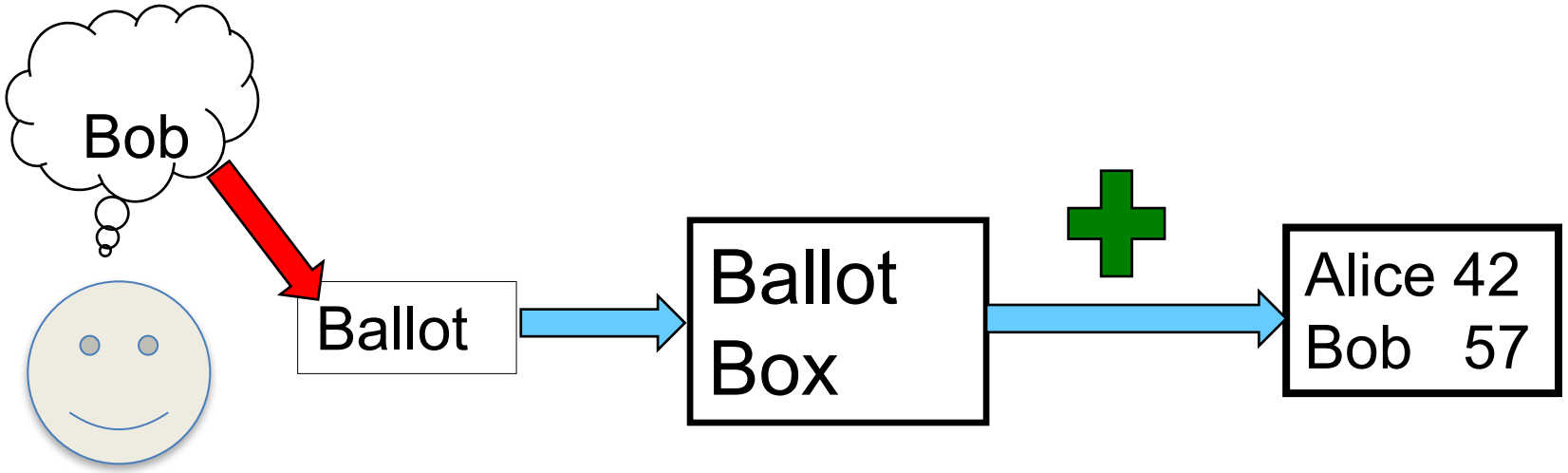
- Provides Ballots Casting Assurance:
  - Direct Verification
    - Cast as intended
    - Counted as cast
  - Universal Verification (E2E)
    - A tally at the end of the elections with plaintext voters names and their encrypted ballots

Cryptography in E-voting

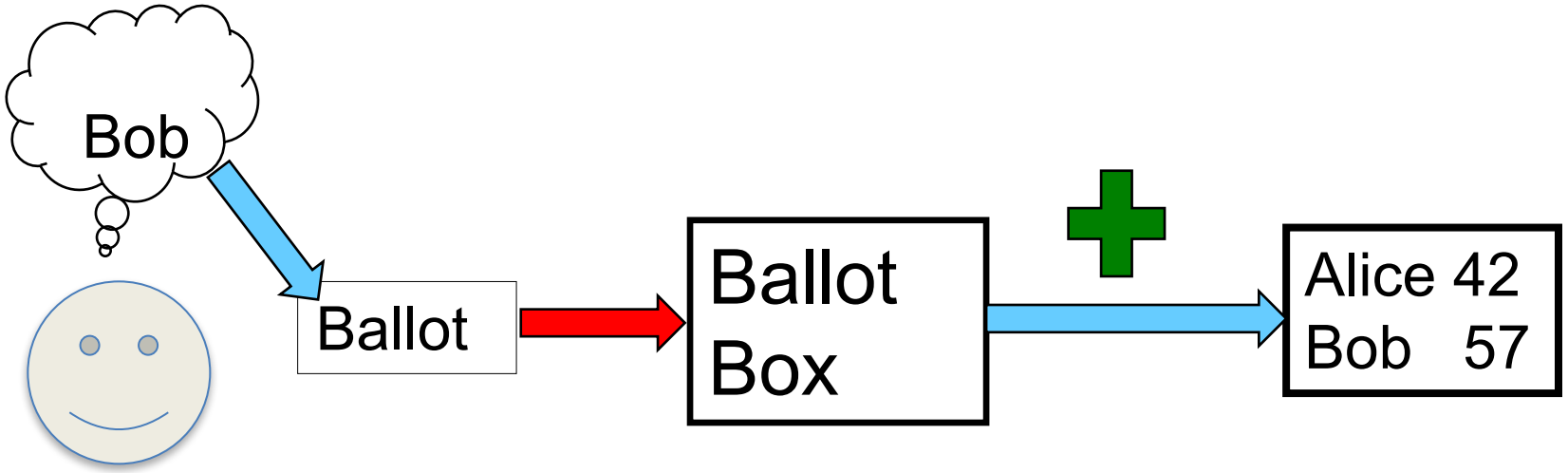


End-to-End Verifiability

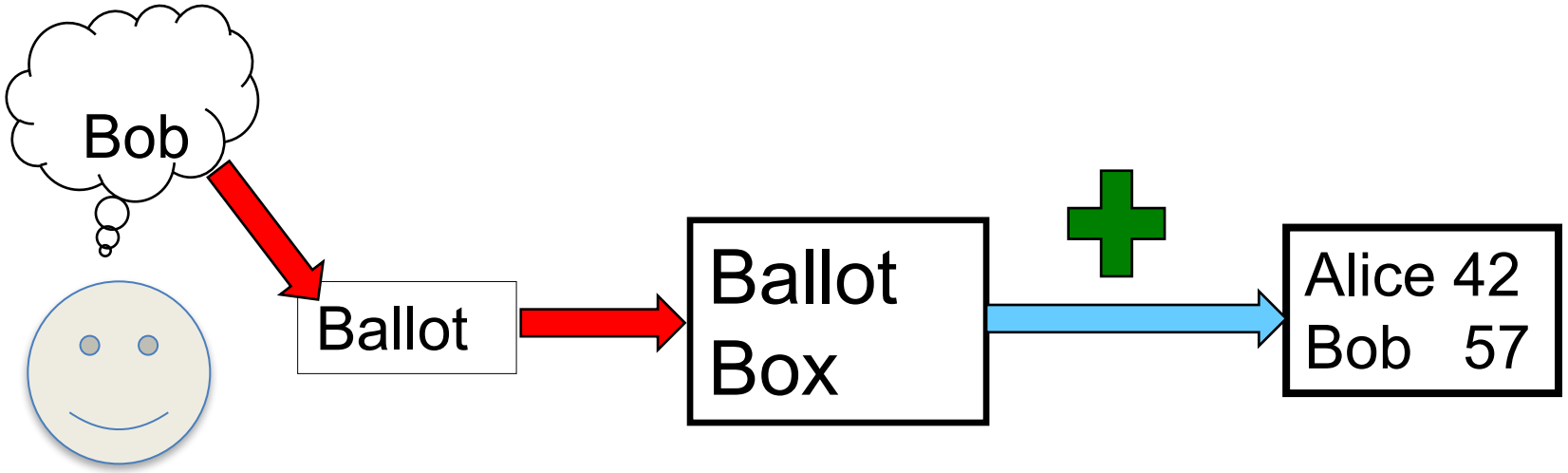
Cast as Intended



Recorded as Cast

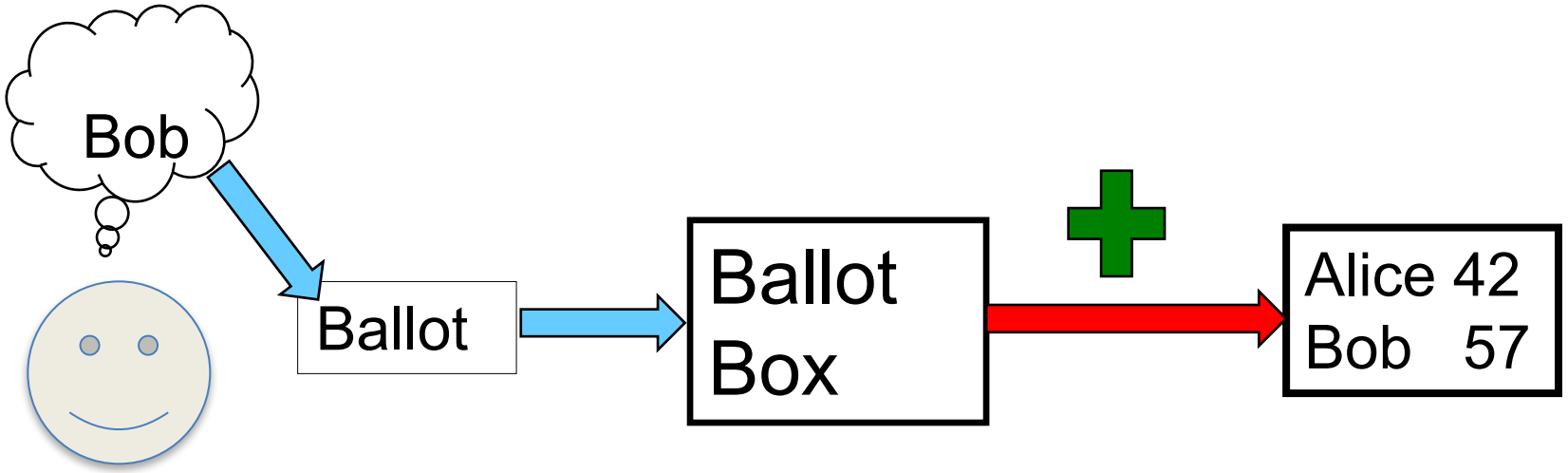


Recorded as Cast



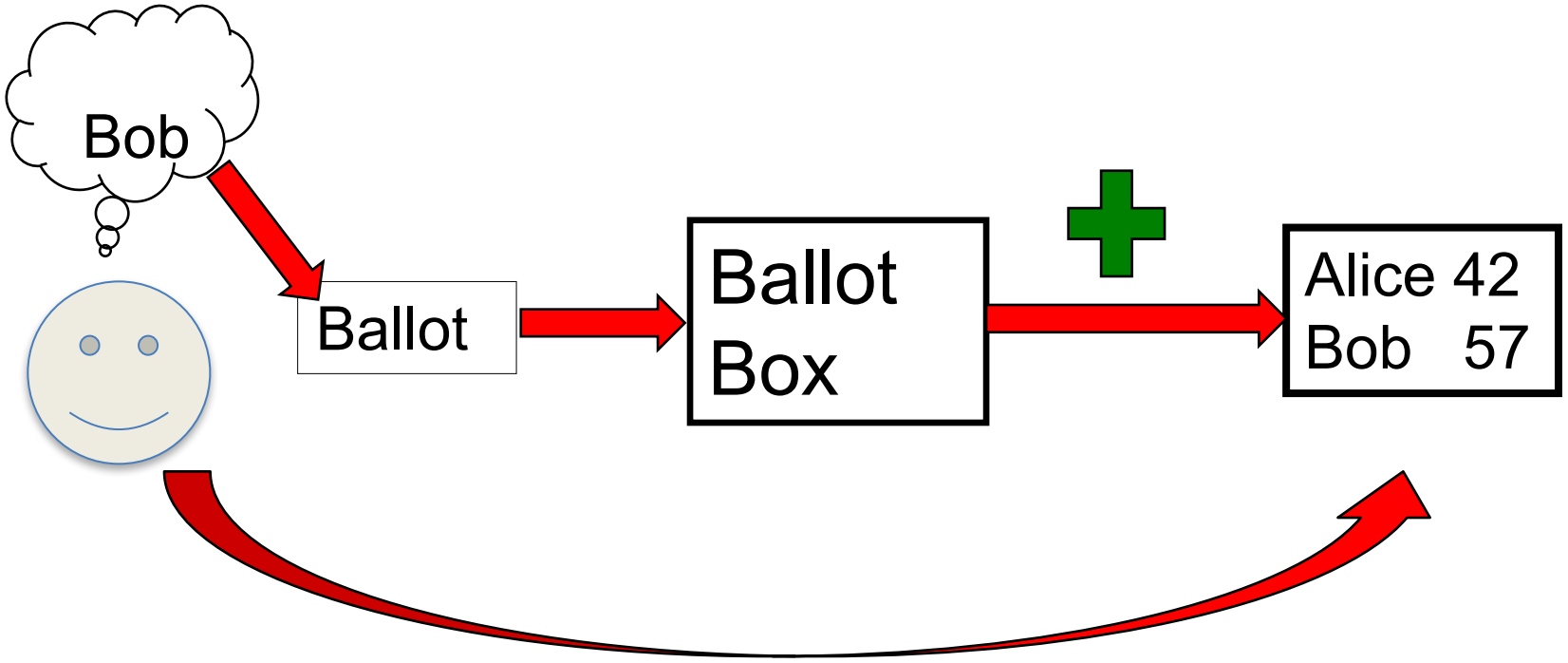
- Ballot casting assurance
- Verified by the voter

Counted as Recorded



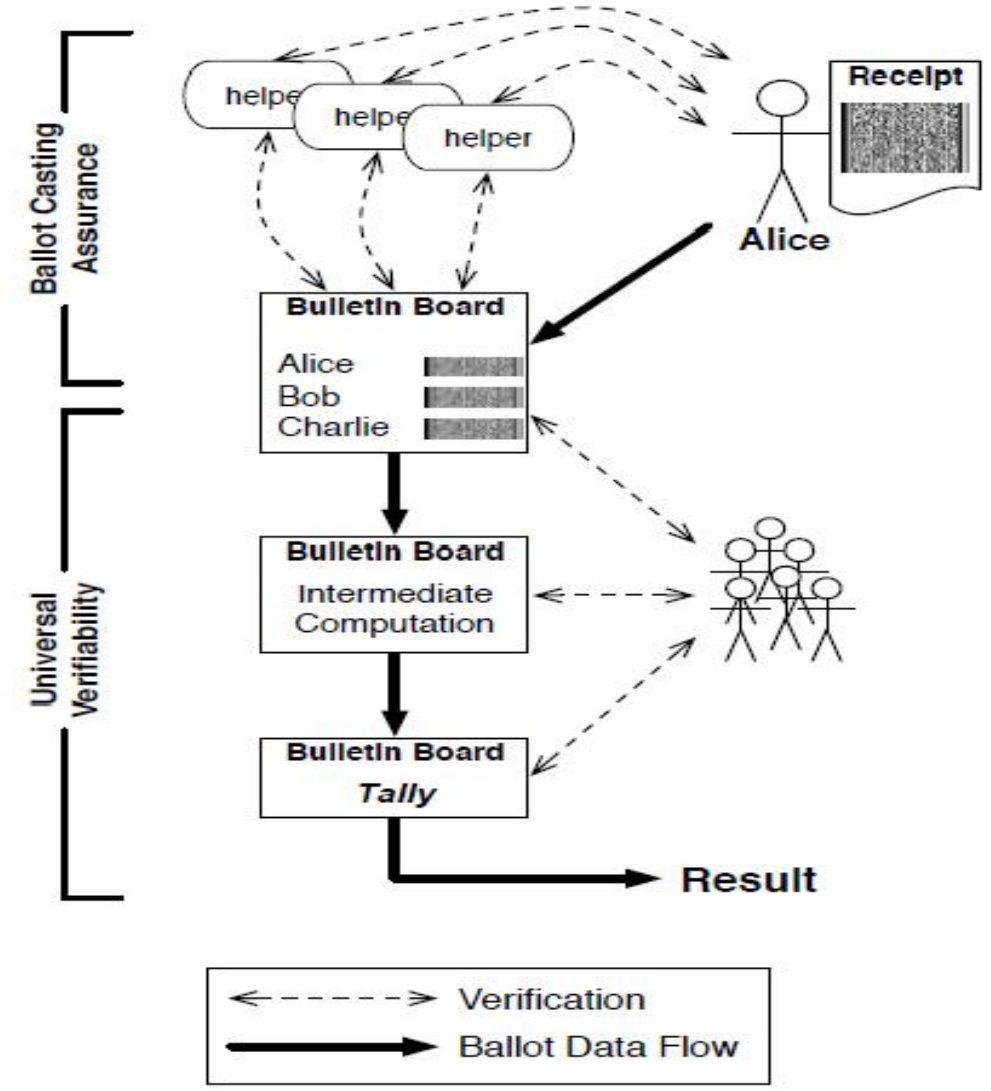
- Universal assurance
- Verified by anyone

Verifiable Outcome

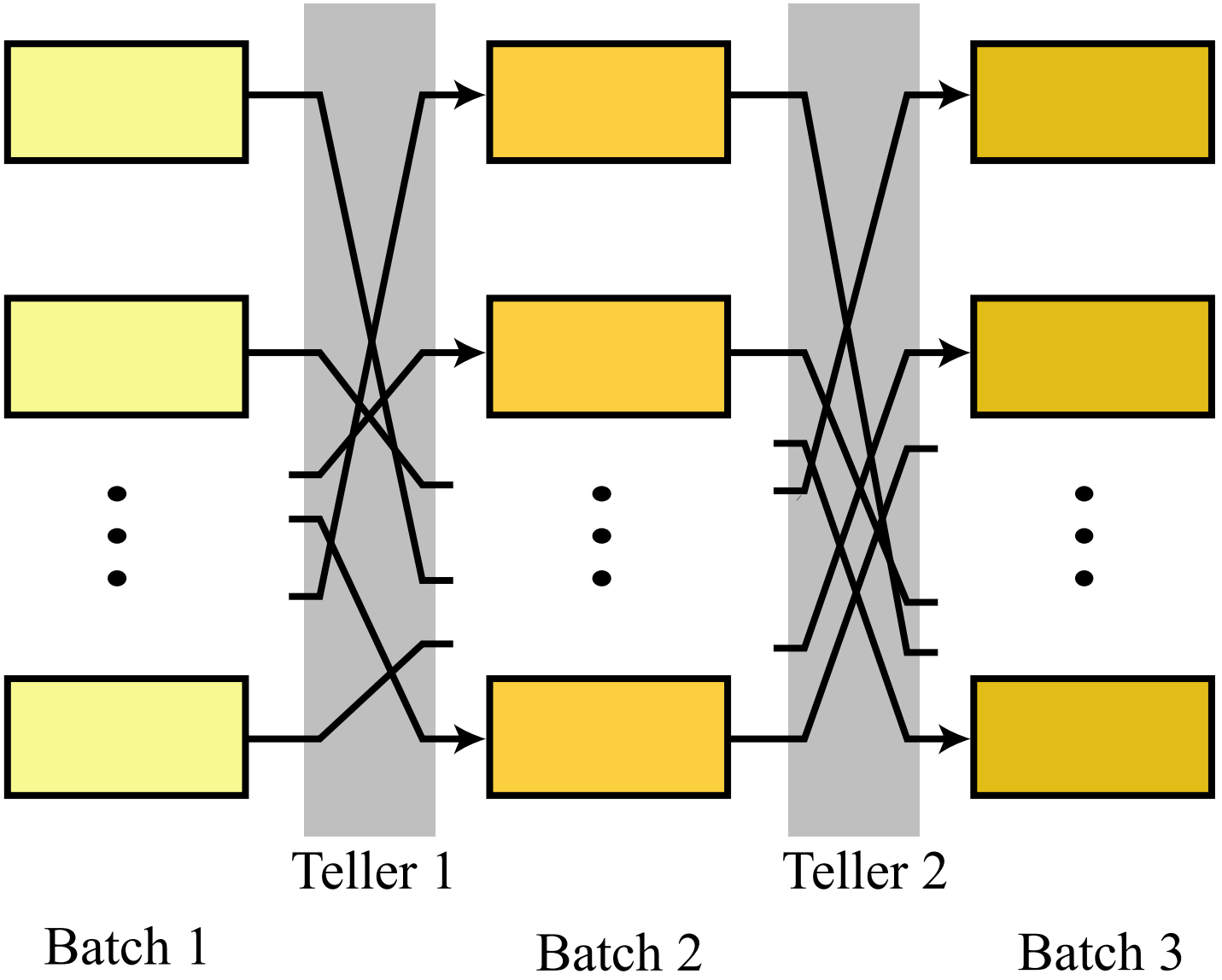


No need to trust the software

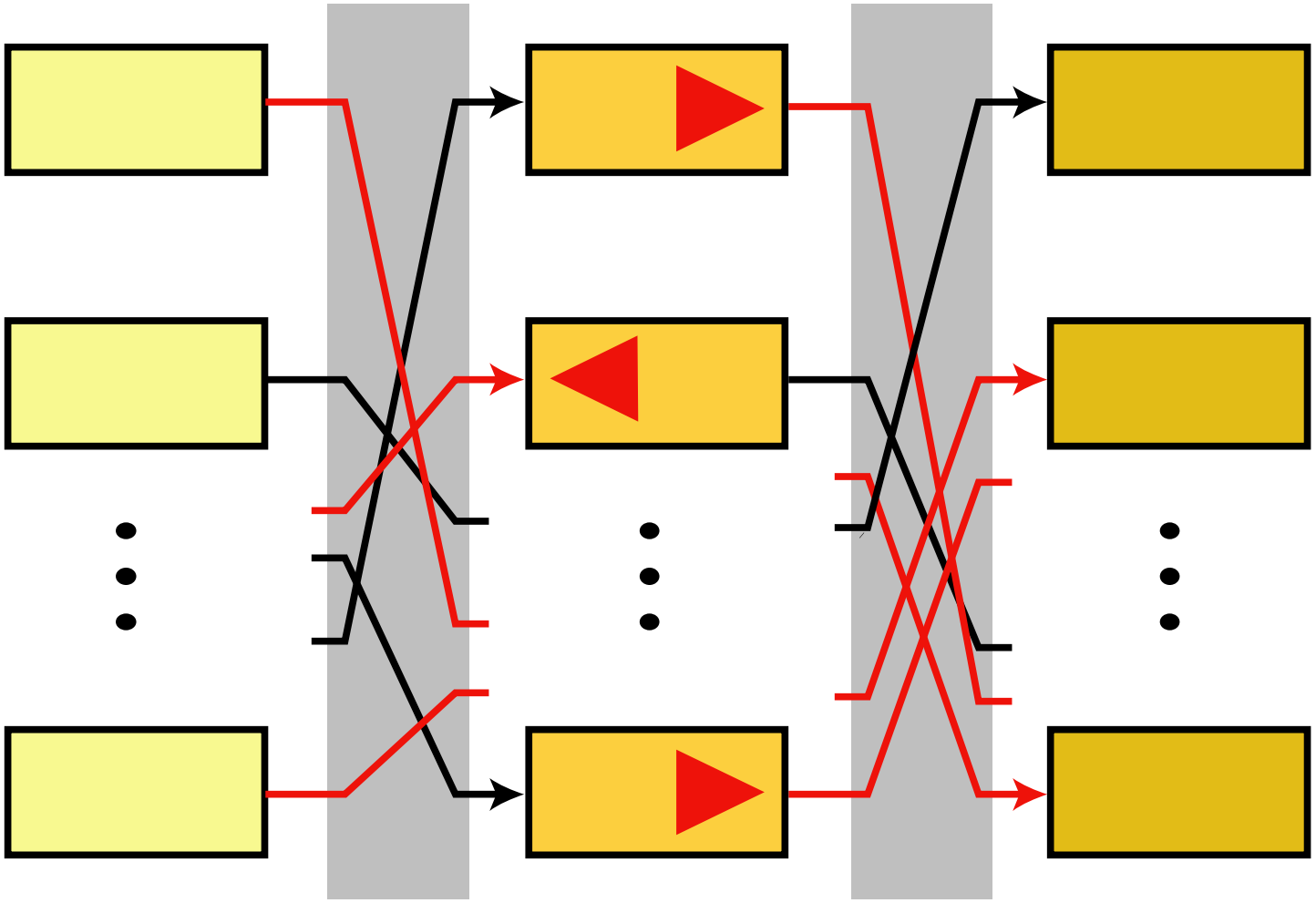
End-to-End Verifiability



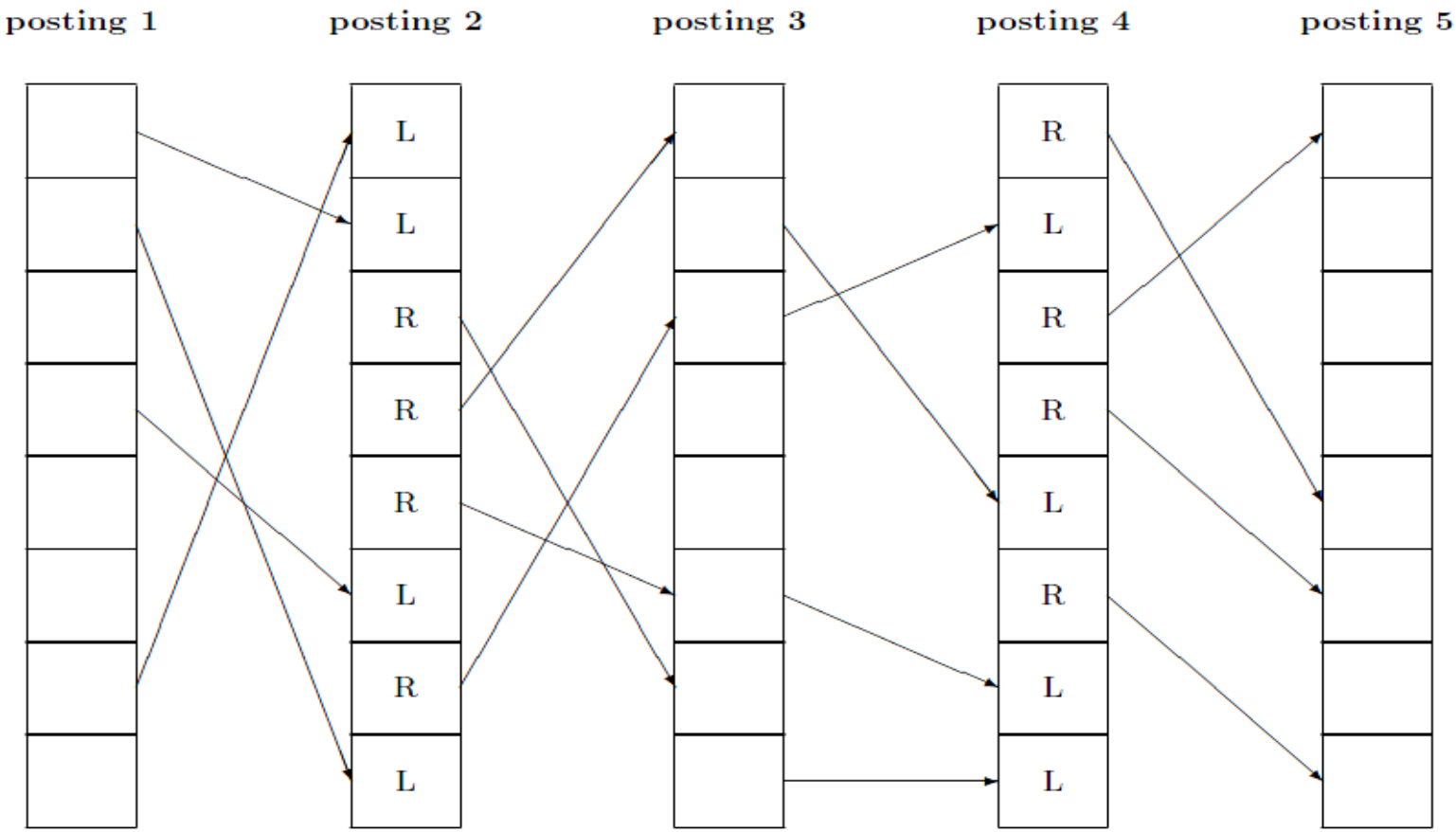
Mix Networks



Auditing the Tellers

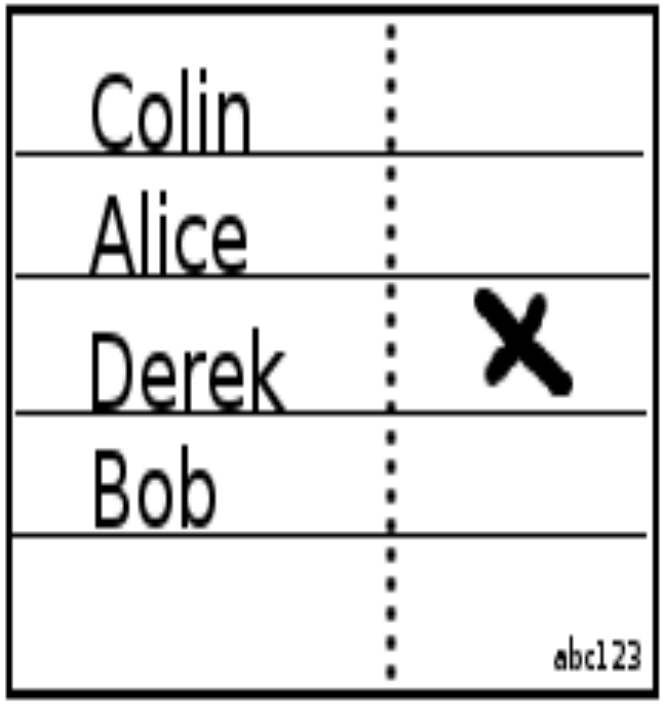


Mix Network


posting 1
posting 2
posting 3
posting 4
posting 5
L
L
R
R
R
L
R
L
R
R
R
L
R
L
L

Prêt à Voter: E2E System

- Cryptography Protocols:
  - Threshold cryptography
  - Cut and choose
  - Mix networks
    - Partial decryption
    - Re-encryption



Example: Prêt à Voter

Ballot Sheet

Derek	
Colin	
Bob	
Alice	
	ab1234

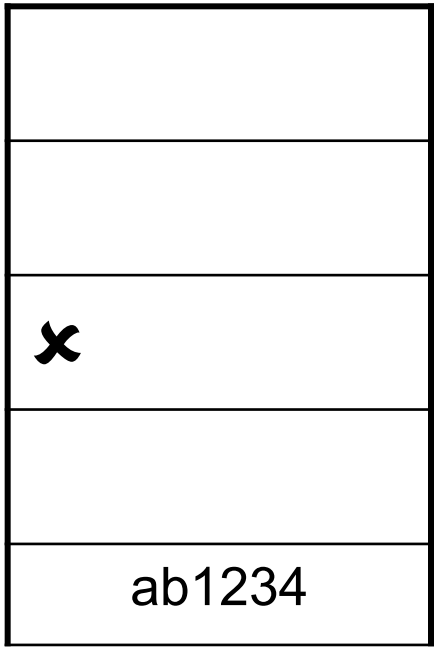
Candidates are randomly ordered

Voter Marks His Choice

Derek	
Colin	
Bob	✘
Alice	
	ab1234

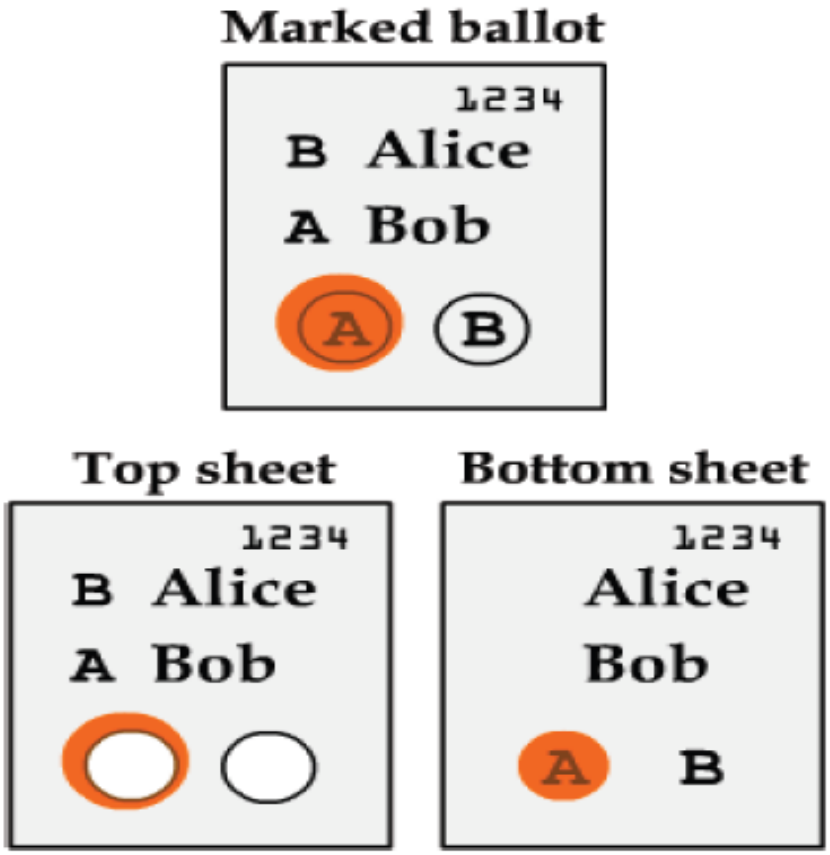
Left half Right half

Voter's Ballot Receipt

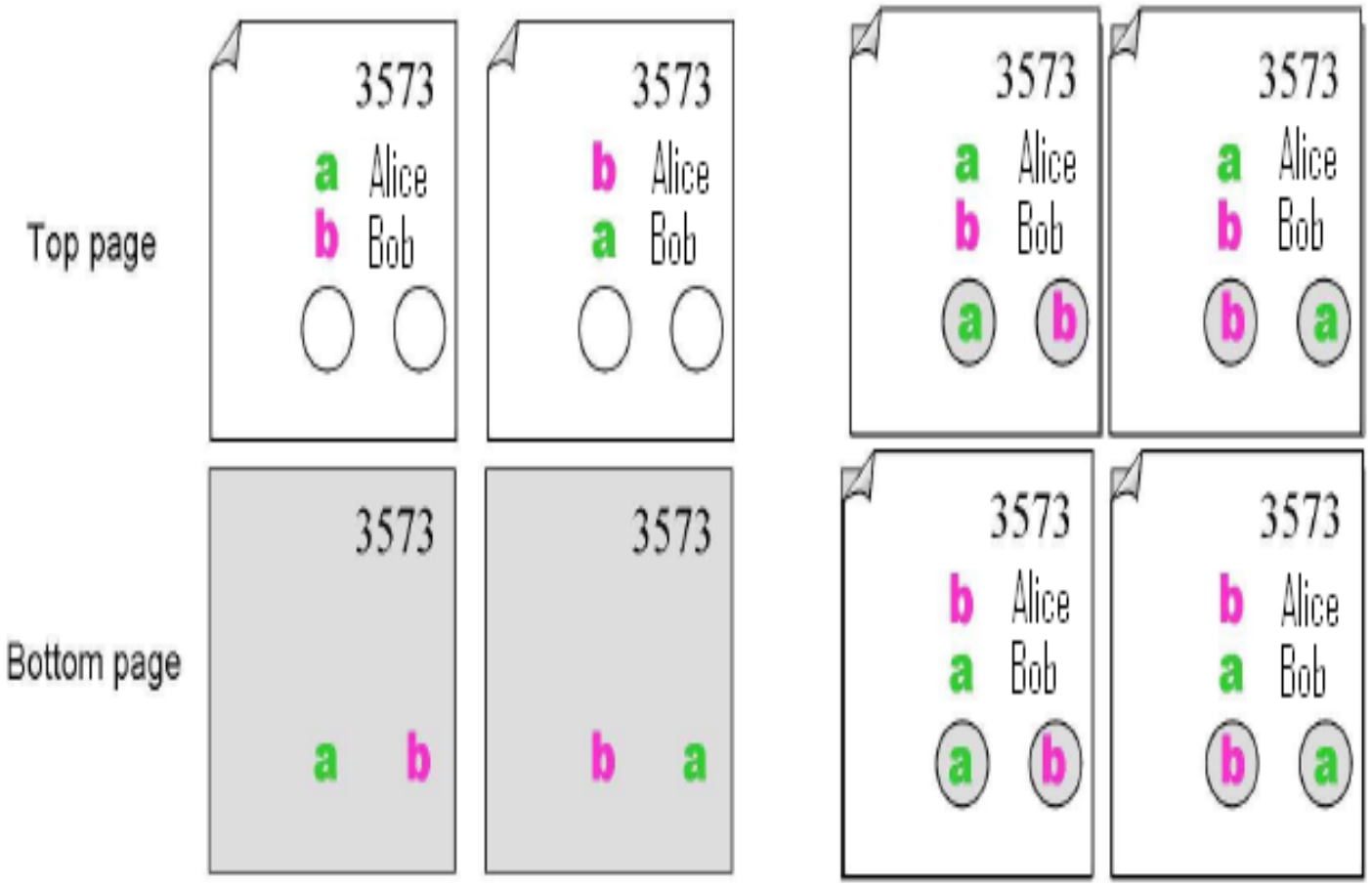


Encrypted receipt

PunchScan Voting System



PunchScan Possible Combinations



Cryptography Related Issues

- Complexity makes it hard to trust
- What if there were hidden data to link the vote to the voter?
- Limitations:
  - Doesn't support write-ins
  - Doesn't meet other requirements
- Threats and attacks:
  - Coercion
  - Randomization and contract attacks
  - Recovery?

Cryptography for Auditing

ElGamal Encryption

ElGamal Encryption

- Let **p** be a large prime
- Select a special number **g**
  - The number g must be a **primitive element** modulo **p**
- Choose a private key **x**
  - This can be any number bigger than 1 and smaller than **p**-1
- Compute public key **y** from **x**, **p** and **g:**

$$\mathbf{y} = \mathbf{g}^{\mathbf{x}} \bmod \mathbf{p}$$

ElGamal Encryption

The first job is to represent the plaintext as a series of numbers modulo p. Then:

1. Generate a random number k
2. Compute two values C_1 and C_2, where

$$\mathbf{C_1 = g^k \bmod p} \quad \text{and} \quad \mathbf{C_2 = y^k M \bmod p}$$

3. Send the ciphertext C, which consists of the two separate values C_1 and C_2

ElGamal Decryption

$$C_1 = g^k \bmod p \qquad C_2 = y^k M \bmod p$$

The receiver using his private key:

$$C_1^{-x} * C_2 \bmod p = M$$

Note: $C_1^{-x} = (g^k)^{-x} = (g^x)^{-k} = (y)^{-k}$

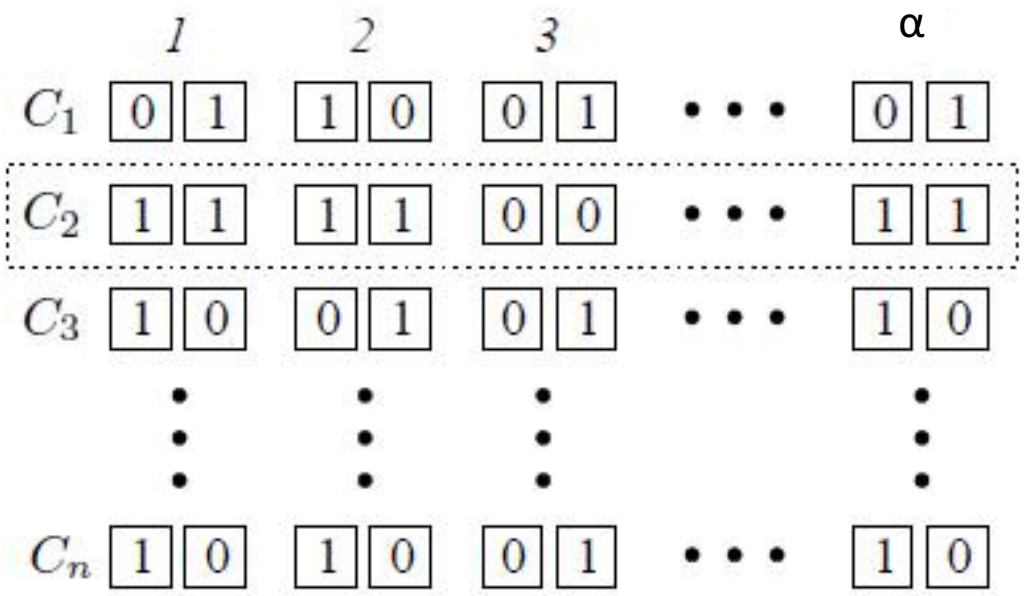
Exponential ElGamal Encryption

- Exponential ElGamal encryption of m is the normal ElGamal encryption of $\mathbf{g^m}$
- The Exponential ElGamal encryptions of 0 is the ElGamal encryption of 1
- The Exponential ElGamal encryption of 1 is the ElGamal encryption of g

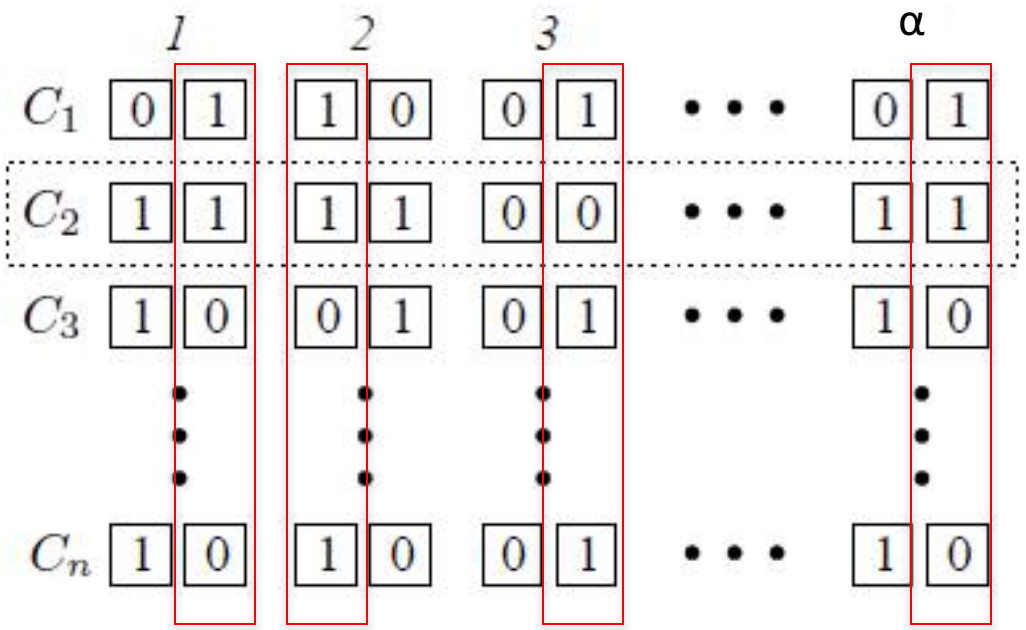
Special Form of Bit Encryption

- $\text{BitEnc}_{pk}(b) = \{[u_i, v_i]\}_{i \in [0, \alpha-1]}$, where α is the sequence length
- $b = \{\text{Dec}_{sk}(u_i) \oplus \text{Dec}_{sk}(v_i)\}_{i \in [0, \alpha-1]}$
- b = 1, then each pair encodes either [0, 0] or [1, 1]
- b = 0, then each pair encodes either [0, 1] or [1, 0]

Using BitEnc()



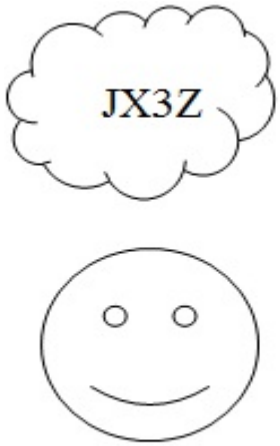
Using BitEnc()



Challenge String: 1 0 1 … 1

Using BitEnc()

Electronic Voting Protocol	
Alice	BitEnc(0)
Bob	BitEnc(1) JX3Z
Charles	BitEnc(0)
David	BitEnc(0)



Receipt	
Challenge NF3G	
Alice	MB12
Bob	JX3Z
Charles	H7GV
David	Y34C

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Commit to c

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice		
Bob		
Colin		
Derek		

Vote/Receipt Verification

Poll station voting (inside the voting booth)

Voter

Vote Machine

Printer

Commit to c

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice		
Bob		
Colin		
Derek		

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Voter

Wants to vote for Bob

Vote Machine

Commit to c

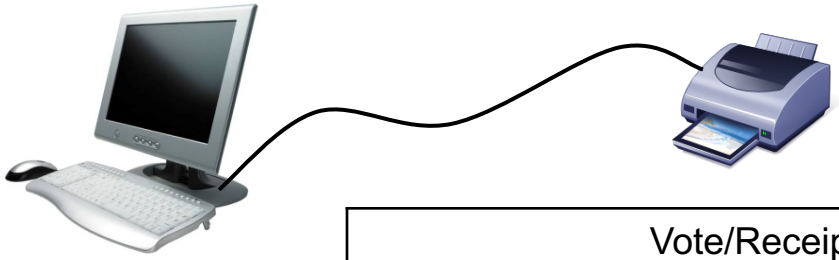
Printer

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice		
Bob		
Colin		
Derek		

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Voter

Vote Machine



Printer

Commit to c

Bob

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice	BitEnc(0)	
Bob	BitEnc(1)$_{JRF2}$	
Colin	BitEnc(0)	
Derek	BitEnc(0)	

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Voter

Vote Machine

Printer

Commit to c

Bob

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice	BitEnc(0)	
Bob	BitEnc(1)$_{JRF2}$	
Colin	BitEnc(0)	
Derek	BitEnc(0)	

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Voter

Vote Machine

Printer

Random Challenge (c)

Commit to c

Bob

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice	BitEnc(0)	
Bob	$\text{BitEnc}(1)_{\text{JRF2}}$	
Colin	BitEnc(0)	
Derek	BitEnc(0)	

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Voter

Vote Machine

Printer

Commit to c

Bob

Random Challenge (c)

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice	BitEnc(0)	
Bob	BitEnc(1)$_{JRF2}$	
Colin	BitEnc(0)	
Derek	BitEnc(0)	

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Voter

Vote Machine

Printer

Commit to c

Bob

Random Challenge (c)

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice	BitEnc(0)	W3EX
Bob	BitEnc(1)$_{JRF2}$	**JRF2**
Colin	BitEnc(0)	R59S
Derek	BitEnc(0)	KMZC
		Challenge = c

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Commit to c

Bob

Random Challenge (c)

Vote/Receipt		
Candidates	Vote Encryption (BitEnc)	Vote Receipt (OpenBitEnc)
Alice	BitEnc(0)	W3EX
Bob	$\text{BitEnc}(1)_{\text{JRF2}}$	**JRF2**
Colin	BitEnc(0)	R59S
Derek	BitEnc(0)	KMZC
		Challenge = c

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Commit to c

Bob

Random Challenge (c)

Vote/Receipt		
Candidates		Vote Receipt (OpenBitEnc)
Alice		W3EX
Bob		**JRF2**
Colin		R59S
Derek		KMZC
		Challenge = c

Vote/Receipt Verification
Poll station voting (inside the voting booth)

Commit to c

Bob

Random Challenge (c)

Vote/Receipt		
Candidates		Vote Receipt (OpenBitEnc)
Alice		W3EX
Bob		JRF2
Colin		R59S
Derek		KMZC
		Challenge = c

After the election end:

1. The Vote Machine publishes the encrypted receipts.
2. External organizations verify the correctness of the published data.
3. The voter verify his receipt (and correct his vote if necessary).
4. The votes are tallied using a protocol with counted-as-cast verification.

Internet Voting

Remote voting to provide ease?

Acronyms

- VOI: Voting Over the Internet
- UOCAVA: Uniformed and Overseas Citizens Absentee Voting Act
- FVAP: Federal Assistance Voting Program
- DoD: Department of Defense
- FPCA: Federal Post Card Application

Absentee Voting

- Voters covered by UOCAVA obtain, complete, and send an FPCA
- FPCA serves as both an absentee voter registration and a request for an absentee ballot
- Once the county officials approve the received FPCA, they send an absentee ballot to the voter

Internet Voting in the States

- Alaska's Republicans (2000)
- Arizona's Democrats (2000)
- VOI (2000)
  - Voting Over the Internet
- SERVE (2004)
  - Secure Electronic Registration and Voting Experiment
- BRAVO (2008)
  - Bring Remote Access to Voters Overseas

Alaska 2000

- Straw poll for the republican party
- A suitable state to implement I-voting
- 3,500 potential voter
- 35 actual voter
- I-votes changed the outcome
- Many questions and concerns

Arizona 2000

- First Democratic Primary in Arizona
- Too late to matter in election
- All potential voters received a PIN in the mail
- 35,786 voted using a remote connection
- Many technical difficulties
- No solid evaluation

Arizona's Conclusions

Counties with more

1. Elderly people
2. Non-whites
3. Unemployed
4. Rural population

were less likely to use I-voting

Before VOI Project

- Voters covered by UOCAVA obtain, complete, and send an FPCA
- FPCA serves as both an absentee voter registration and a request for an absentee ballot
- Once the county officials approve the received FPCA, they send an absentee ballot to the voter

VOI Project

- FPCA was confusing
- VOI was launched by FVAP
- Estimated cost: $6.2 million

VOI Scenario

1. Voters were sent a CD-ROM
2. Voters had to have a DoD issued digital certificate
3. To vote, voters need to login into a central server that authenticates their digital certificate
4. An electronic FPCA appears on the voters screen

VOI Scenario Cont.

5. FPCA is submitted to the appropriate local election office as an encrypted object
6. Once the FPCA is approved, voter can initiate voting session similar to the registration process
7. When the local election office receives the E ballot, the voter is sent an electronic return receipt

VOI Assessment

- 127 volunteers in 12 countries
- 91 registered voters
- 84 actually voted
- Cost per vote was $74,000
- No evidence of suffering from security violations
- Low participation made it impossible to evaluate the effectiveness of the system

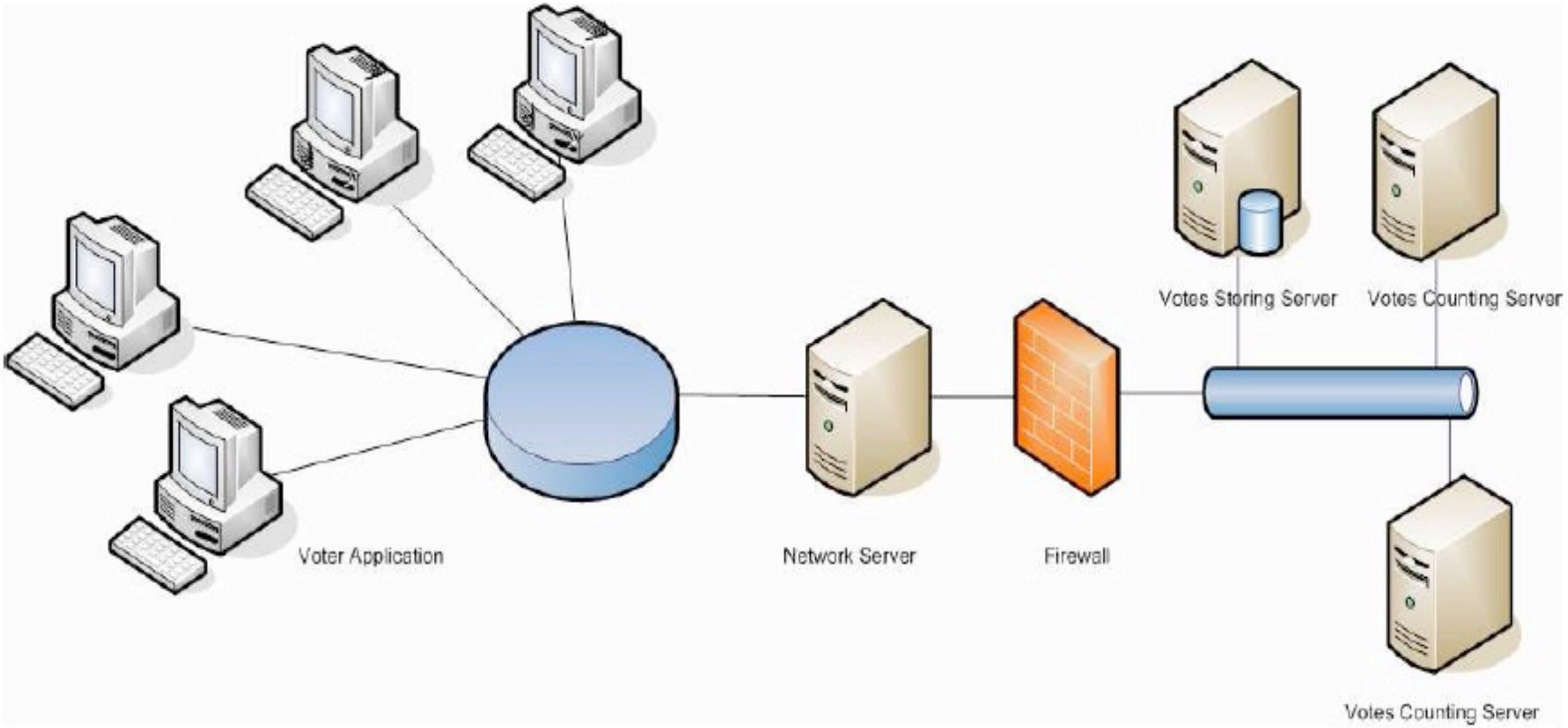
VOI Remarks

- VOI help desk received 71 calls, but they were all resolved
- Voting took around 15 minutes on average
- VOI had no serious glitches and no significant problems that led to loss of votes

SERVE

- Secure Electronic Registration and Voting Experiment
- Goal: Facilitate registration and voting over the Internet for overseas military and citizens
- Terminated in 2004
- Plans to apply it in 2008 general elections were put on hold

SERVE Infrastructure



SERVE Scenario

1. Voter enrolls in SERVE
2. Voter registers
3. Voter is given a username and a password
4. Connection is established
5. Candidate list generated
6. VA encrypts the vote
7. Network server verifies the encrypted vote
8. Vote is transferred to the Vote Storing Server (VSS)
9. A separate copy of the vote and the voter info are sent to the appropriate Vote Counting Server (VCS)

SERVE Threats

Threat	Skill needed	Consequences	Realistic?	Countermeasures
denial of service attack (various kinds)	low	disenfranchisement (possibly selective disenfranchisement)	common on the Internet	no simple tools; requires hours of work by network engineers; launchable from anywhere in the world
Trojan horse attack on PC to prevent voting	low	disenfranchisement	There are a million ways to make a complex transaction such as voting fail.	can mitigate risk with careful control of PC software; reason for failure may never be diagnosed
on-screen electioneering	low	voter annoyance, frustration, distraction, improper influence	trivial with today's web	nothing voter can do to prevent it; requires new law
spoofing of SERVE (various kinds)	low	vote theft, privacy compromise, disenfranchised voters	Web spoofing is common and relatively easy	none exist; likely to go undetected; launchable by anyone in the world
client tampering	low	disenfranchisement	one example: change permissions on cookie file. Many other trivial examples	none exist for all possible mechanisms. Too difficult to anticipate all attacks; likely never diagnosed.
insider attack on system servers	medium	complete compromise of election	Insider attacks are the most common, dangerous, and difficult to detect of all security violations	none within SERVE architecture; voter verified ballots needed, e.g. Appendix C; likely undetected

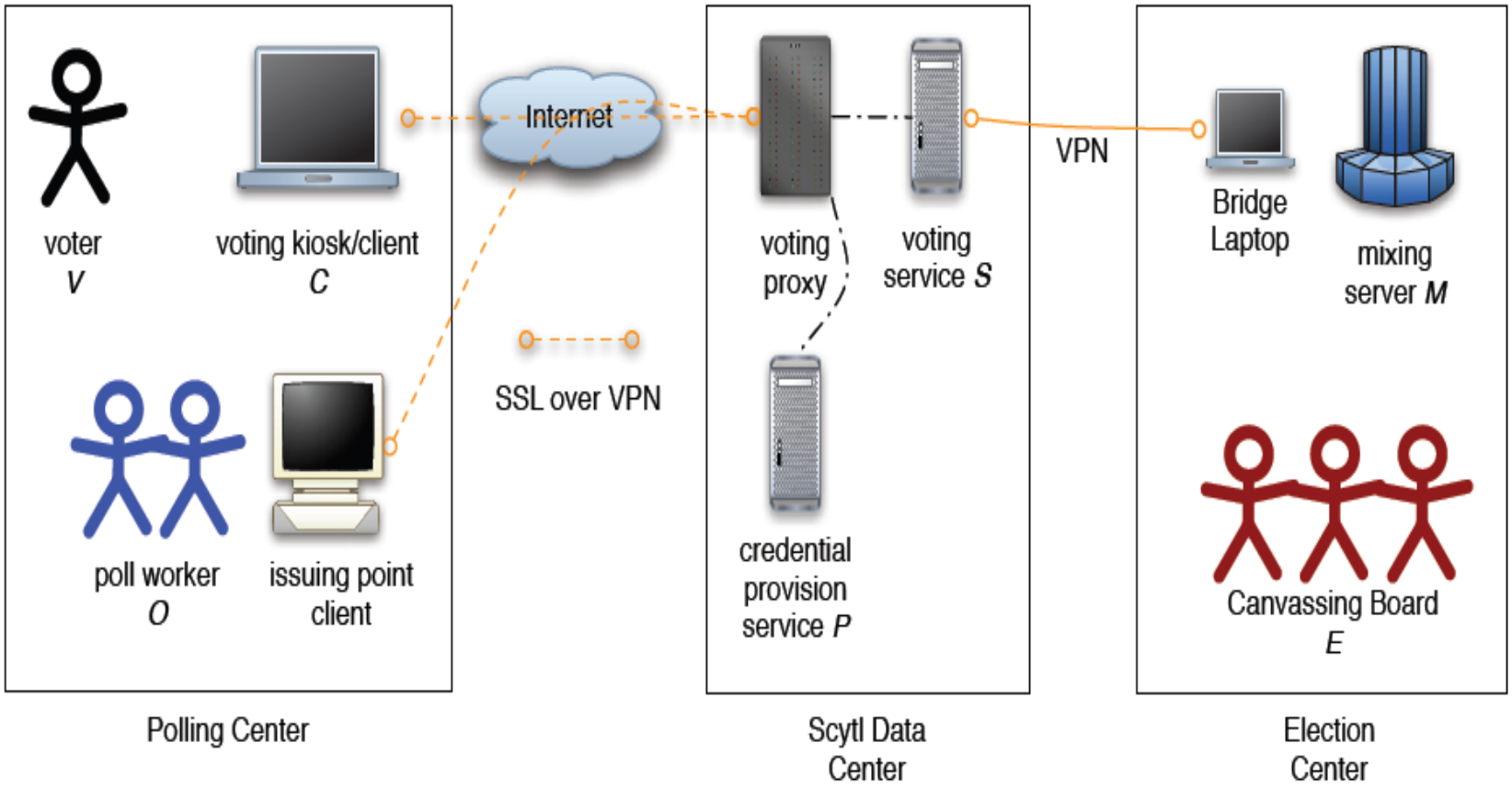
SERVE Threats II

automated vote buying/selling	medium	disruption of democracy	very realistic, since voter willingly participates	none exist; buyers may be out of reach of U.S. law
coercion	medium	disruption of democracy	harder to deploy than vote buying/selling, but man in the middle attacks make it achievable with average skill	none exist; likely to go undetected.
SERVE-specific virus	medium or high	vote theft, privacy compromise, disenfranchised voters	Some attacks require only experimentation with SERVE; others require leak of SERVE specs or code and resourceful attacker	virus checking software can catch known viruses, but not new ones; likely to go undetected
Trojan horse attack on PC to change votes or spy on them	high	vote theft, privacy compromise	widely available spyware would be a good starting point	can mitigate risk with careful control of PC software; harder to control at cybercafe, or other institutionally managed networks; attack likely to go undetected

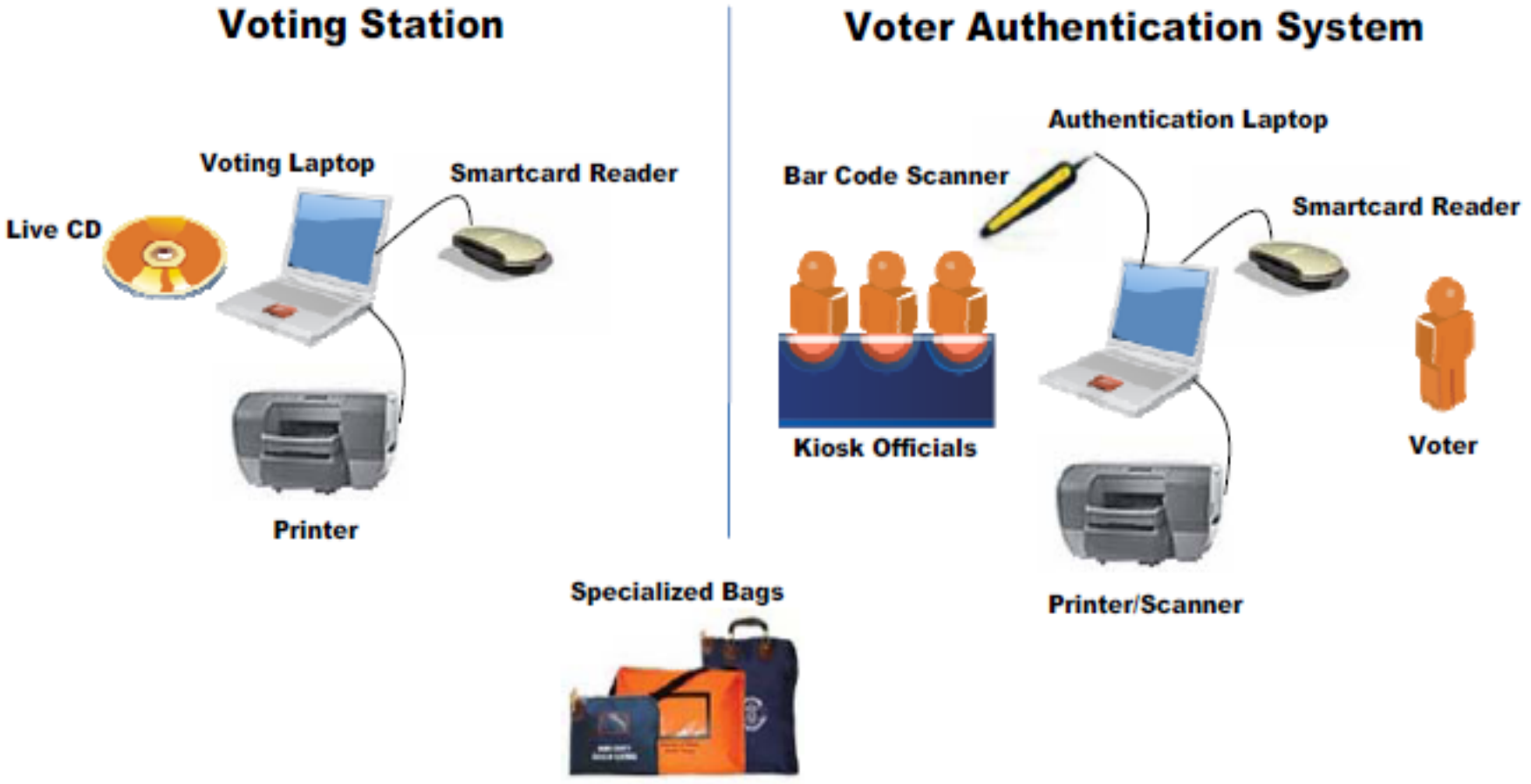
Operation BRAVO (2008)

- Okaloosa County, Florida
- Scytl Secure Electronic Voting
- SAIT Laboratory, Florida State University
- 3 overseas distance balloting sites
- 10 days voting period
- 900 self-selected voters

BRAVO Diagram



Absentee Voting Kiosk



SAIT Findings

- Complete life-cycle documentation
- The cryptographic protocol specification
- Occasional inaccuracies
- Ballot secrecy
- Programming languages used
- “Counted as cast” receipts

Internet Voting in Estonia

Estonia Cornerstones

- Penetration of the ID-card ~ 90% amongst eligible voters
- 5 years of experience with ID-card
- Municipal elections in 2005
- Everyday Internet usage ~ 63%
- Technology-savy people (No. 1 in the world of spending on ITC compared to GDP)
- Size of the country

Usage of the ID-card

- Major ID-document
- Replacement of
  - Transportation tickets
  - Library cards
  - Healthh insurance card
  - Driving documents
  - Etc.
- Authentication token for all major e-services
- Digital signature tool

I-voting Main Principles

- All major principles of paper-voting are followed
- I-voting is allowed during period before Voting Day
- The user uses ID-card
  - System authenticates the user
  - Voter confirms his choice with digital signature
- Repeated I-voting is allowed
  - Only last e-ballot is counted
- Manual re-voting is allowed
  - If vote is casted in paper during absentee voting days, I-vote(s) will be revoked

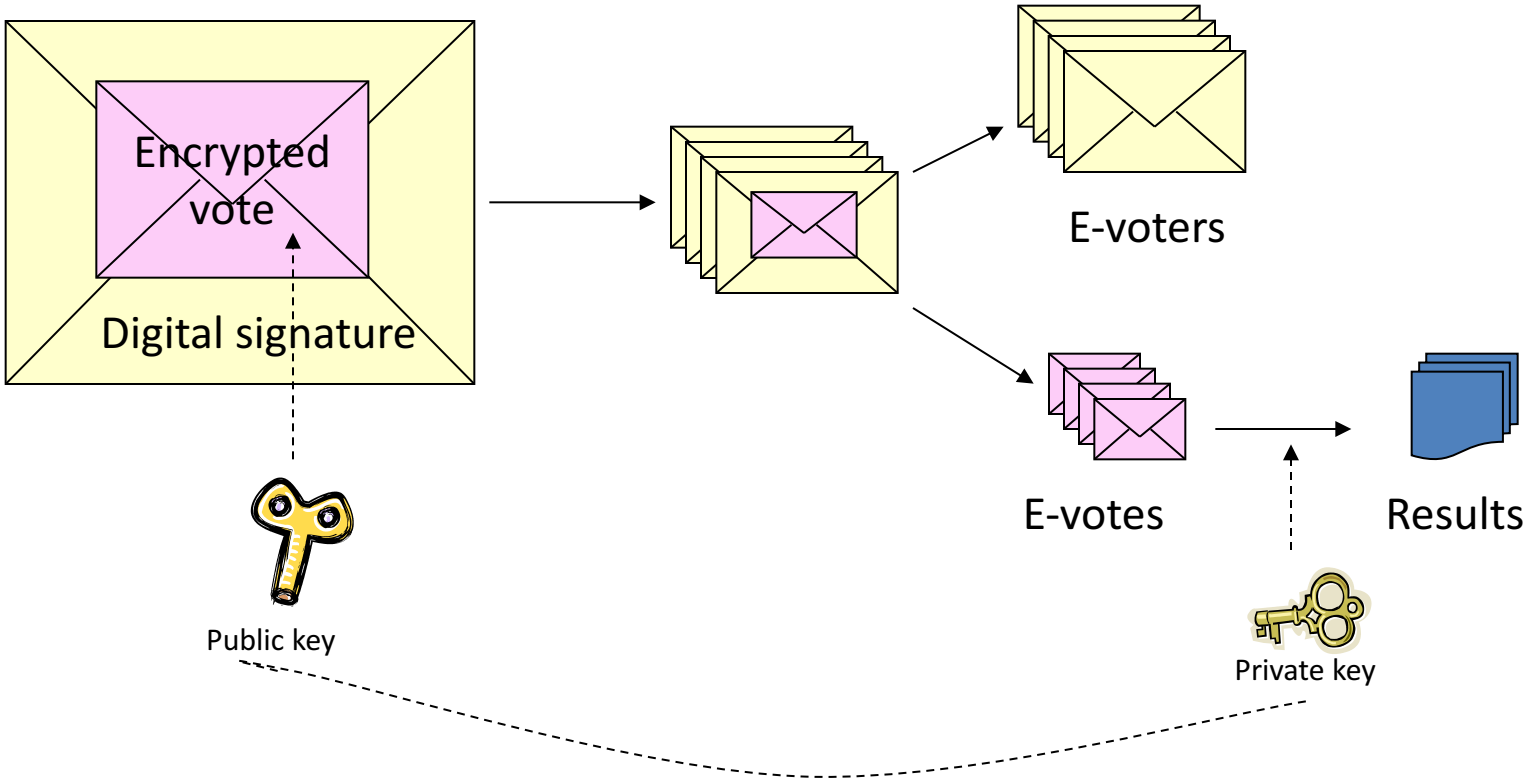
To vote via Internet the voter needs:

- An Estonian ID-card with valid certificates and PIN-codes

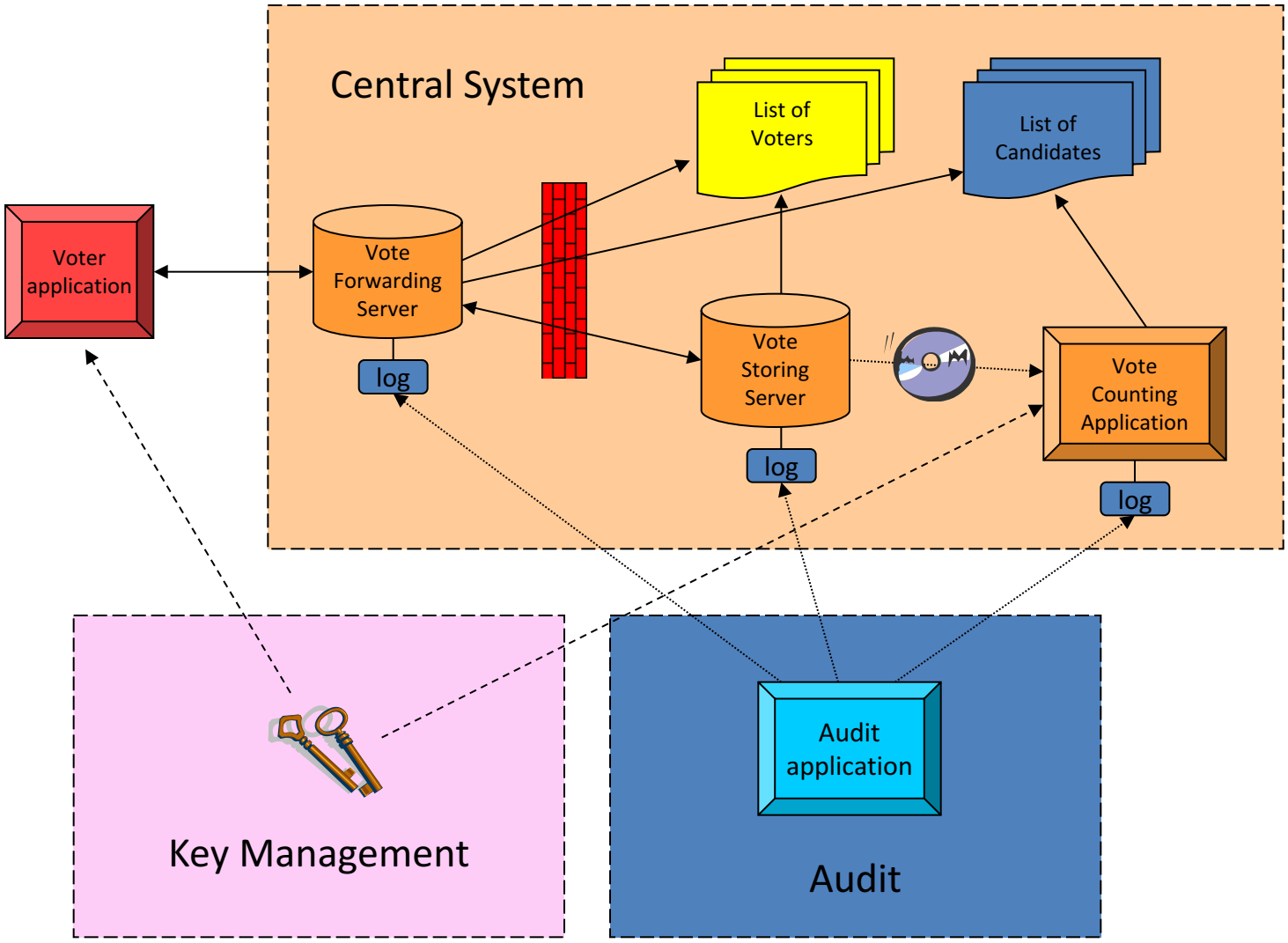
Computer used for I-voting must have:

- Smartcard reader
- Base software for the ID-card
- Windows, Linux, or MacOS X operating system
- Internet connection

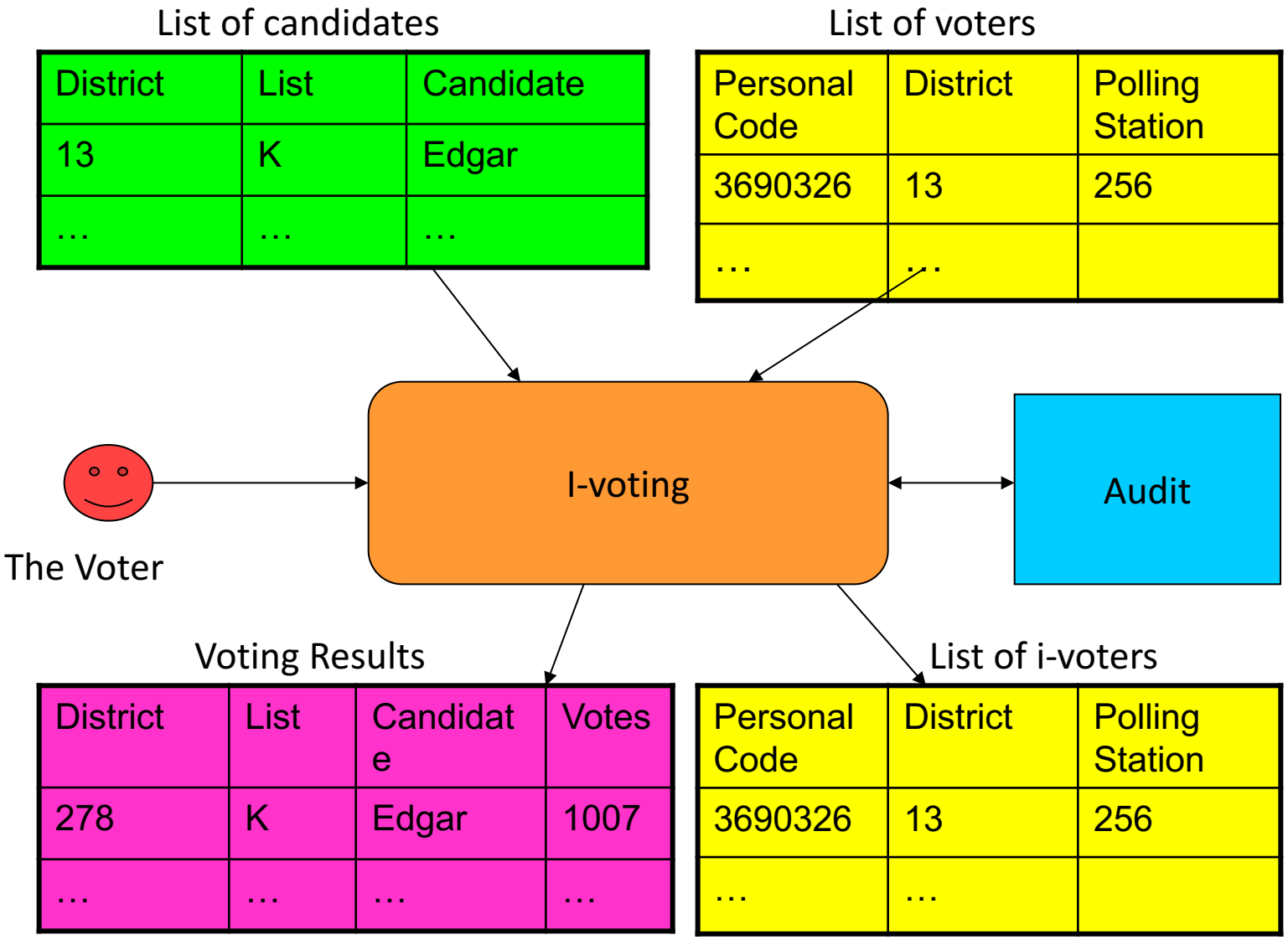
Envelope Scheme



Architecture



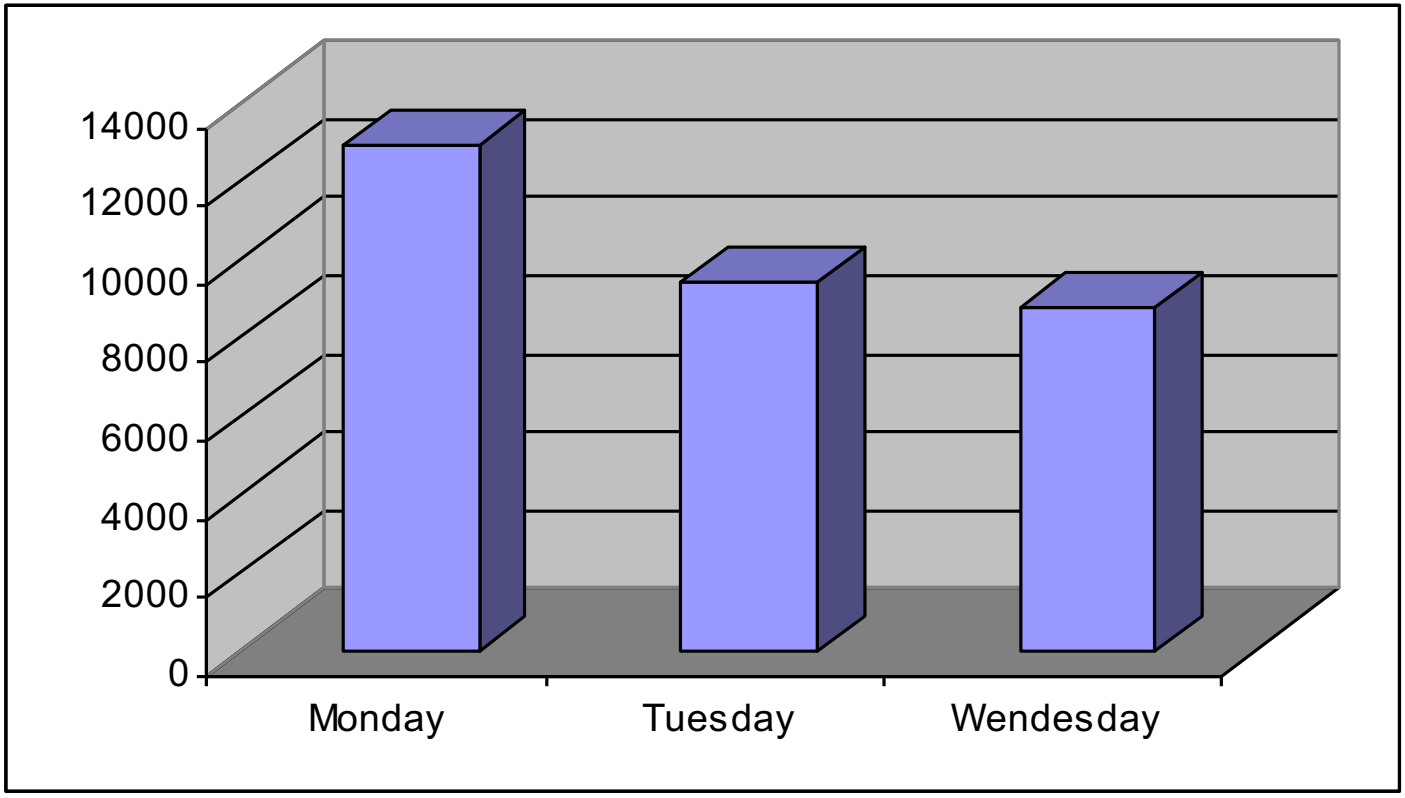
Scope of I-voting



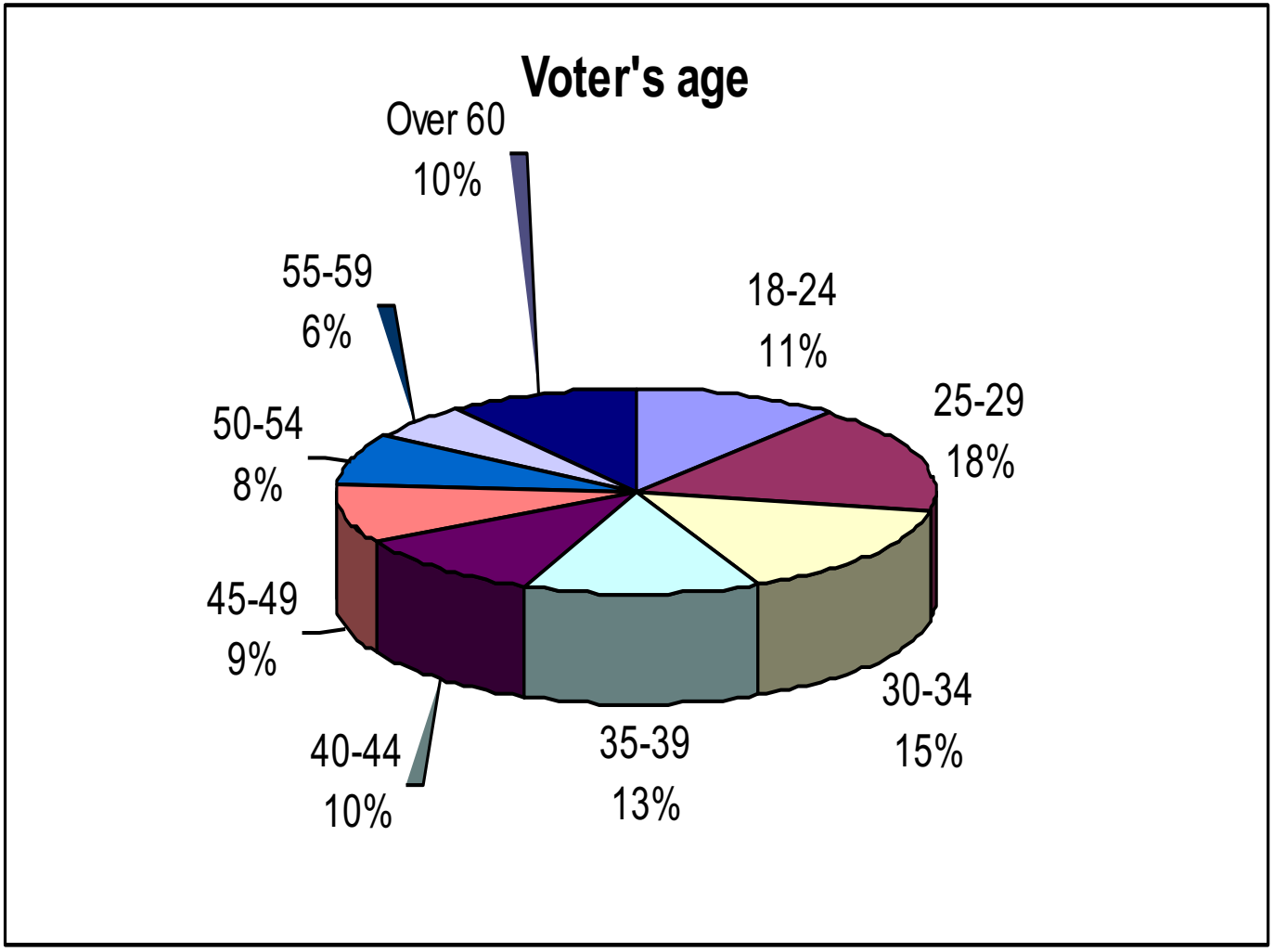
Results of 2007 (2005)

- I-voters: 30 275 (9 317)
- I-votes: 31 061 (9 681)
- First-time ID-card users: 11 894 (5 774)
- Percentage of i-voters amongst votes collected during absentee voting: 18% (7%)
- Certificates renewed Mon-Wed: 5994

Activity By Day



How old is the I-voter ?



Estonian System vs. SERVE

	Characteristic	The Estonian e-voting system	SERVE
1)	The period of e-voting	The e-voting is implemented within a period before the Election Day	The e-voting is implemented within a period before the Election Day and on the Election Day
2)	Revoting process in the polling station	Yes	No
3)	National Public Key Infrastructure	Yes	No
4)	A voter signs the encrypted ballot	Yes	No
5)	The state of votes in Votes Storing Server	Encrypted ballot	No encrypted ballot
6)	The state of Votes Counting Server	Offline	Online
7)	Log files system	Yes	No

Voting in Europe

- Many other countries experimented with I-voting: UK, Switzerland, and Germany
  - With various degrees of success
- National government plays a great role
- Simple Electoral Process
- Simple registration approach
- Simple ballots
- Experiments were on a small scale

Using Biometrics to Safeguard E-voting

Electoral Process Phases

- Voter Registration
- Voter Authentication
- Vote Collection
- Vote Tabulation

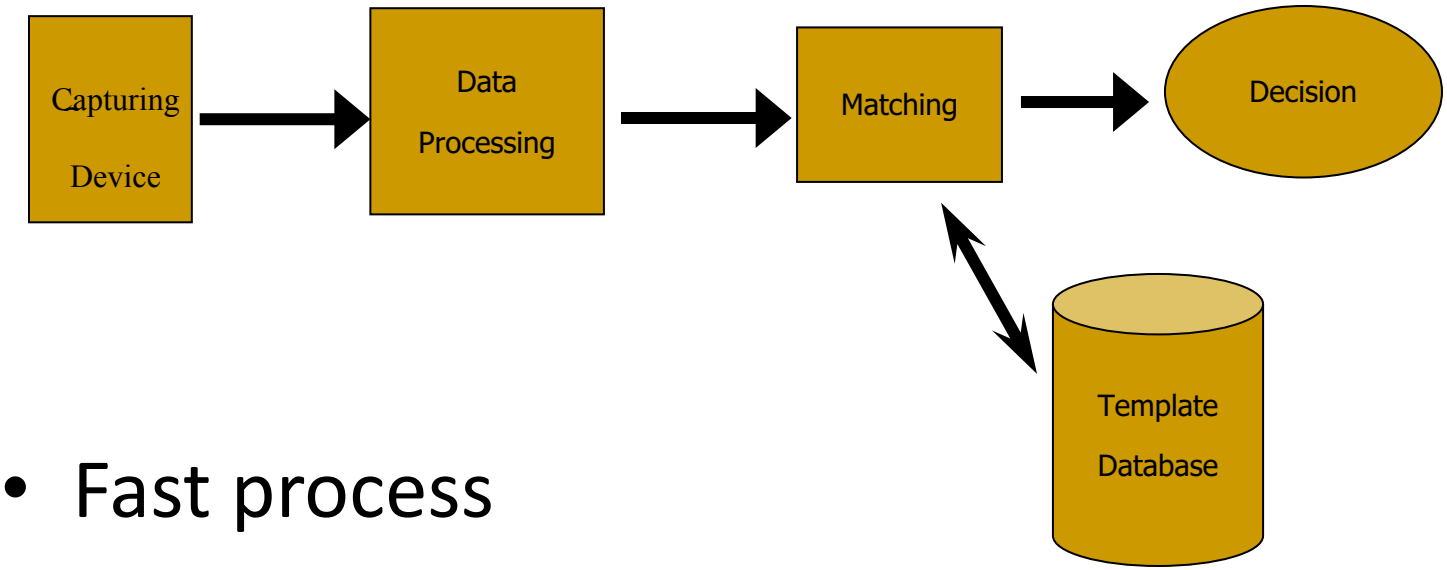
Motivation

- US provisional ballot procedure
- Provisional ballots rejected:
  - 35.5% in 2004
  - 20.5% in 2006
- Reasons:
  - Lack of ID
  - Incomplete registration form
  - Missing signature

Biometrics as a Solution

- Uses individuals' traits for identification purposes
- Physical traits:
  - Fingerprint
  - Voice
  - Face recognition
  - Iris scan
  - Retina scan
- Behavioral traits: Signature or writing style

Biometrics for Voter Authentication



- Fast process
- Prevents fraud (mistakes)
- Reduces the number of provisional ballots

Threats and Concerns

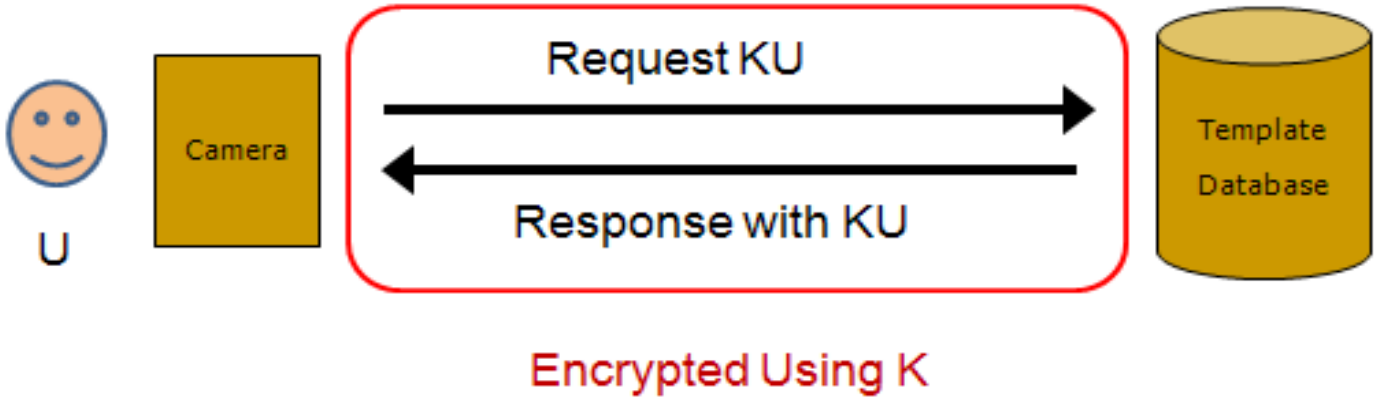
- Equality vs. similarity
- Biometrics are not flexible
- Stealing the measurements would be tragic
- Risky to transmit over the Internet
  - Simple intercept attacks
  - Sniff and suppress attacks

Safeguarding From Simple Intercepts

- Third party intercepts the captured measurement
- Encrypt measurements before transmission
- Store every successful match
- Decision making:
  - Similarity to the template
  - Equality to all previous successful matches

Handling "Sniff and Suppress"

- Previous approach permits single access
- Use a specific key K
- KU changes (every authentication attempt)



- Solves simple intercepts

Conclusion

- Paper ballots have their own flaws too
- Paper trails are not the ultimate solution
- Current e-voting methods are not very popular in the U.S. and many other places
- E2E provides promising features, but still has a long way to go

“It's Not the People Who Vote that Count; It's the People Who Count the Votes”

— Stalin