Networked public sphere

- democratization of political activism
- Attempts to censor Internet and countermeasures
- Electronic elections

- Technology and political activism
  - Benkler pp. 220-225, the story of Sinclair Broadcasting
  - Ease of communicating, gathering and creating political action: media eliminated as intermediary
- Attempts of non-democratic governments to censor Internet
  - China and search engines

- Falun Gong
- Psiphon
  - How do ISPs work
  - Technical idea: proxy, traffic encoding
  - Why it can operate

Technology and political change

- Importance of
  - Social networking
  - mobile phones
- Twitter: Iran, Tunisia

Electronic elections

- Why is this important
- From "electronizing" the current poll/ballot system to "networked" elections
- The Brazilian experience
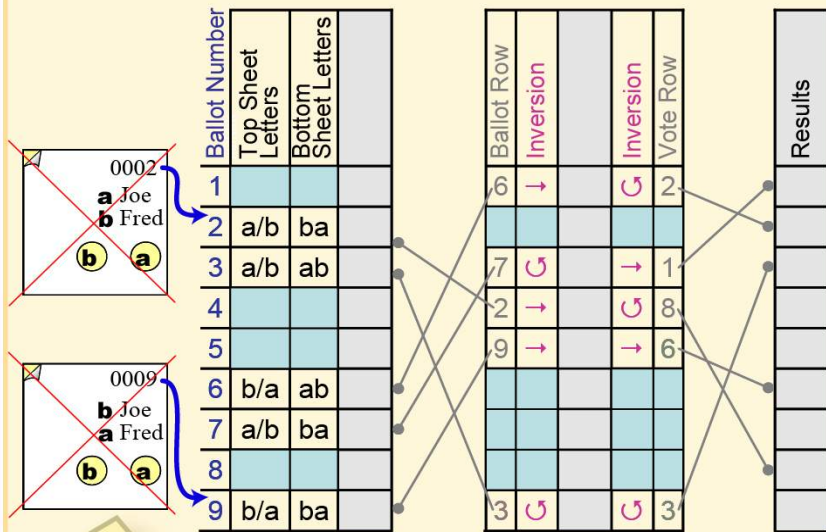- The PunchScan system

Punchscan

- Video http://www.punchscan.org/
- Main features:
  - Integrity: secret ballot
  - Proof of vote and verification that vote recorded correctly
  - Impossible to buy votes
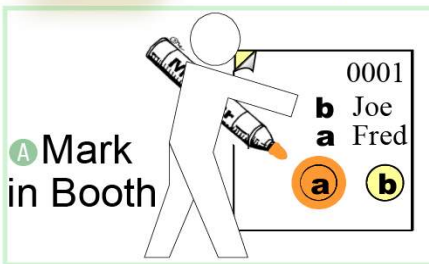 - Simple, technologically inexpensive

Technical elements

- Two page ballots
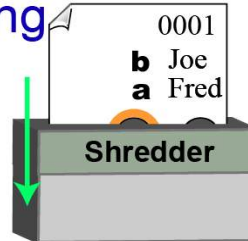- Daubing
- Shredding
- Verification

❶ Pre-Election Audit

Ballot Number	Top Sheet Letters	Bottom Sheet Letters		Ballot Row	Inversion	Inversion	Vote Row	Results
1				6	→	↺	2	
2	a/b	ba						
3	a/b	ab		7	↺	→	1	
4				2	→	↺	8	
5				9	→	→	6	
6	b/a	ab						
7	a/b	ba						
8								
9	b/a	ba		3	↺	↺	3	

0002
a Joe
b Fred
b a

0009
b Joe
a Fred
b a

❷ Polling-Place Voting

0001
b Joe
a Fred
a b

Ⓐ Mark in Booth

Ⓑ Shred — Shredder

0001
b Joe
a Fred

❸ Post-Election Audit

0001
a b

Ballot Number	Top Sheet Letters	Bottom Sheet Letters	Marked Left or Right Side		Ballot Row	Inversion	Intermediate Positions	Inversion	Vote Row	Joe Fred
1		ab	●				●	→	5	●
4	b/a		●		8	→	●			●
5	a/b		●				●	↺	7	●
8		ba	●		4	↺				●

0005
a Joe
b Fred
○ ○

❹ Verifying at Home

Scanner 0001 a b

0001

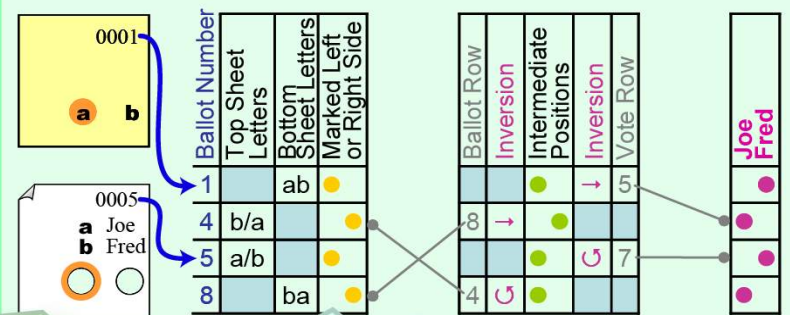Ⓒ Scan, Check, Cast

0001 a b

0001 a b

(e.g., ballot "0002") the row includes one "straight through" arrow and one "inversion" loop arrow (so the orange dot would switch columns when it became a purple results dot, as will be explained); and if such a mark should have resulted in a vote for "Joe" (e.g., ballot "0009"), it includes either two straight-through or two inversion arrows.

❷ **Polling-Place Voting:** Those ballots not decrypted in audit (ballot numbers 1, 4, 5, 8, in the example) are printed and supplied to each voter at the polling place.

Ⓐ **Mark in Booth:** The voter uses an ink dauber to mark the symbol through the hole that matches the symbol labeling the voter's choice of candidate ("Fred" in the example shown). The dauber marks with colored ink both the top sheet around the hole and the
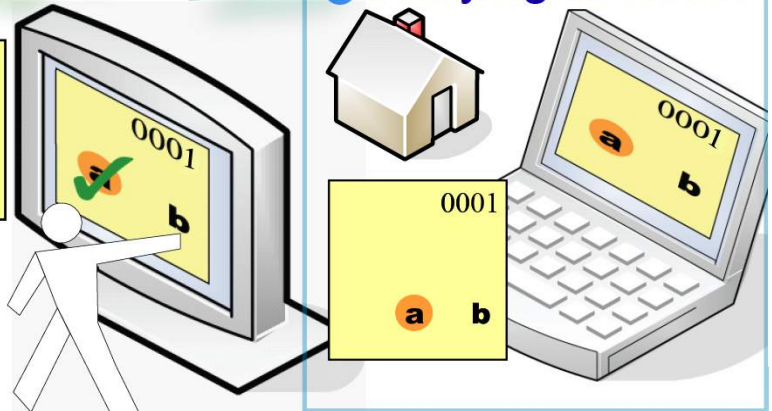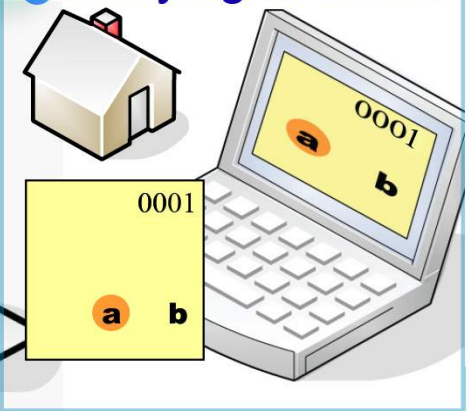
bottom sheet through the hole.

Ⓑ **Shred:** One sheet, freely chosen from the two by the voter (the top sheet, shown as white in the example), is shredded by the voter.

Ⓒ **Scan, Check, Cast:** The voter then scans the remaining sheet and compares it with its scanned image. Green checkmarks on the display indicate the ink marks recognized. Unless the voter wants to spoil the ballot and try again, the scanned image is "cast." The voter keeps the sheet as a receipt—which "locks-in" but does not reveal the vote.

❸ **Post-Election Audit:** After polls close, columns of orange dots record the side, left or right, of each mark scanned. Also, the letters that should be printed on the receipt are decrypted. The results are posted, for anyone to count, as purple dots. Audit is by decrypting

❶ **Pre-Election Audit:** Two tables are posted online, with the content of each table entry encrypted (blue rectangles). Auditors randomly select rows of the first table for decryption (ballot numbers 2, 3, 6, 7, 9, shown after selection with blue removed). This reveals details of ballots (examples shown with red "X") that would have been printed had those rows not been audited. Rows of the second table are then decrypted (rows 1, 3, 4, 5, 9, blue removed) to reveal what would have been the corresponding randomized transformations from ballots to results. Anyone can then check that if a mark on the left side of a ballot should have yielded a vote for "Fred"

randomly either the left or right side of second-table rows (in the example: right, left, right, left). Anyone can then check that green dots are on the same side of the column as the corresponding orange or purple dots for straight-through arrows, and on opposite sides for loop arrows. Randomness in the audit, not encryption, ensures with very high probability that *posted marks* are tallied correctly—but without linking results to ballots.

❹ **Verifying at Home:** To check that his or her vote was *posted correctly*, a voter can use a browser to go to an election website and enter the serial number from the receipt. The image of the receipt should then be provided for download. Voters check that the two match and that marks are in the same positions on the display as on the paper receipt. ◗●◗

Discussion

- Encryption used to keep votes secret
- Correctness is
  - Pre-election audit shows (with very high probability) that the ballots are encoded correctly
  - by randomness of the audit, i.e. post-election audit audit provides a very high probability that votes as registered are counted correctly
  - See "An Introduction to PunchScan" by Popovenius and Hosp, in SpringerLink in e-library

Web as a medium

- Publishing contents on the web and:
  - Freedom of speech
  - Existing laws constraining it:
    - Hate propaganda
    - Anti-pornography, anti-pedophilia
  - "small" *vs* "large"
- Anonymity on the web