



Electronic Voting

Ronald L. Rivest

MIT Laboratory for Computer Science



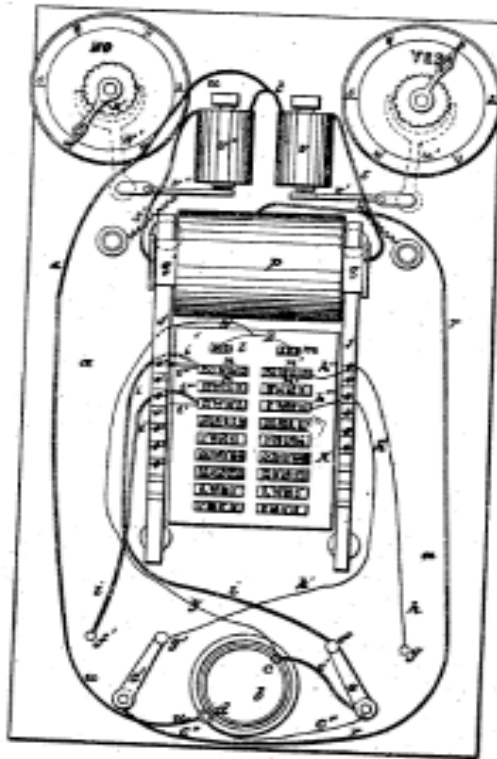
Edison's 1869 Voting Machine

T. A. EDISON.

Electric Vote-Recorder.

No. 90,646.

Patented June 1, 1869.



Intended for use
in Congress;
never adopted
because it was
"too fast" !

The famous "butterfly ballot"

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

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

ELECTORS FOR PRESIDENT AND VICE PRESIDENT	
(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 →

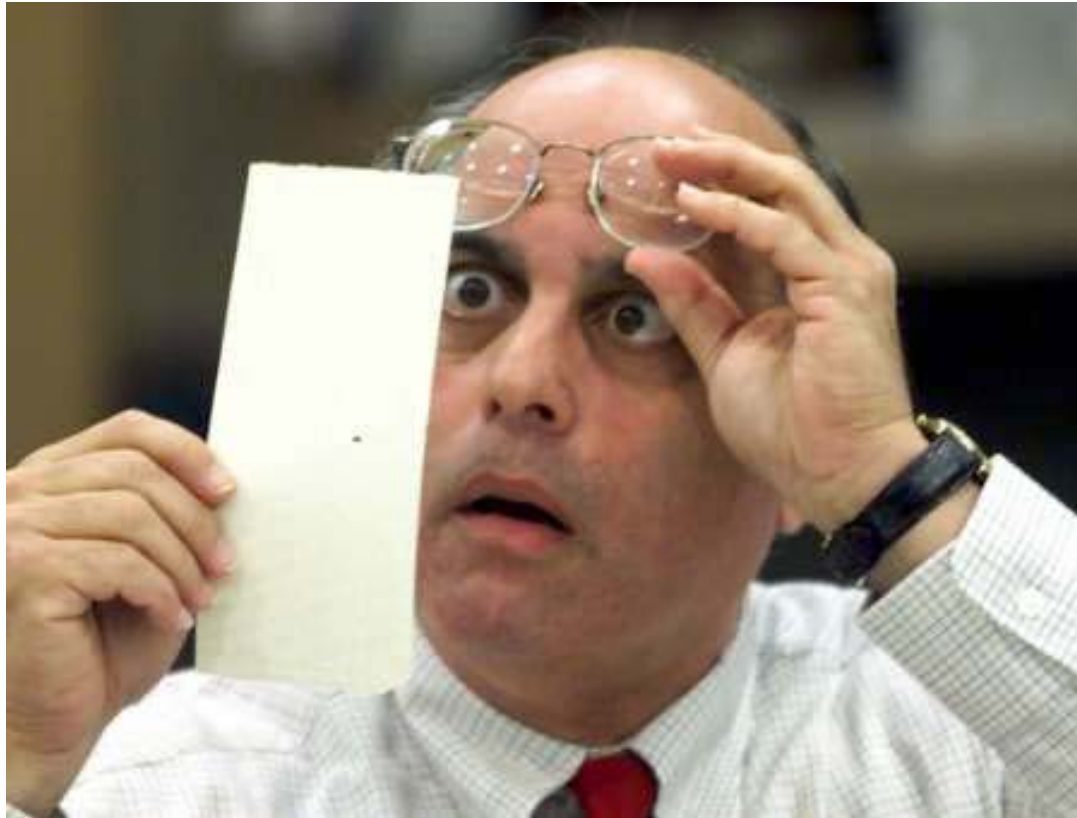
(A vote for the candidates will actually be a vote for their electors.)
(Vote for Group)

← 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" ???



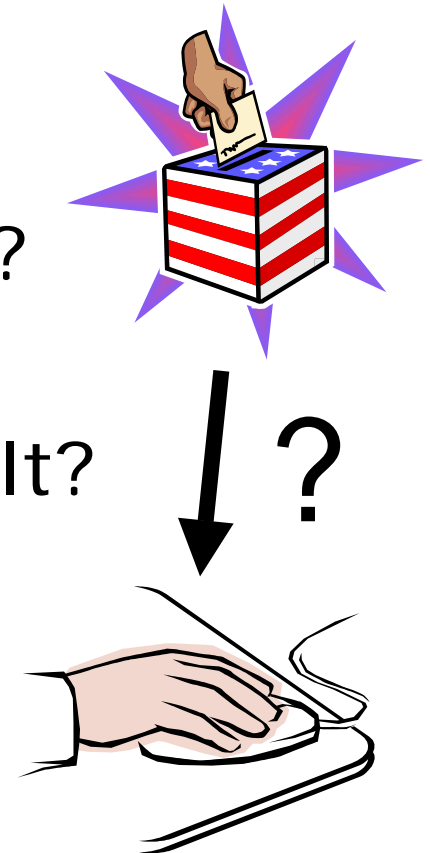
Voting Technology Study



- ◆ MIT and CalTech have begun a joint study of alternative voting technologies.
- ◆ Companion to Carter/Ford commission on political issues in voting systems.
- ◆ Initial work funded by the Carnegie Foundation.
- ◆ Electronic voting schemes will be included in study.

Electronic Voting

- ◆ *Could the U.S. presidential elections be held on the Internet?*
- ◆ Why bother?
 - Increased voter convenience?
 - Increased voter turnout?
 - Increased confidence in result?
 - "Because we can"?

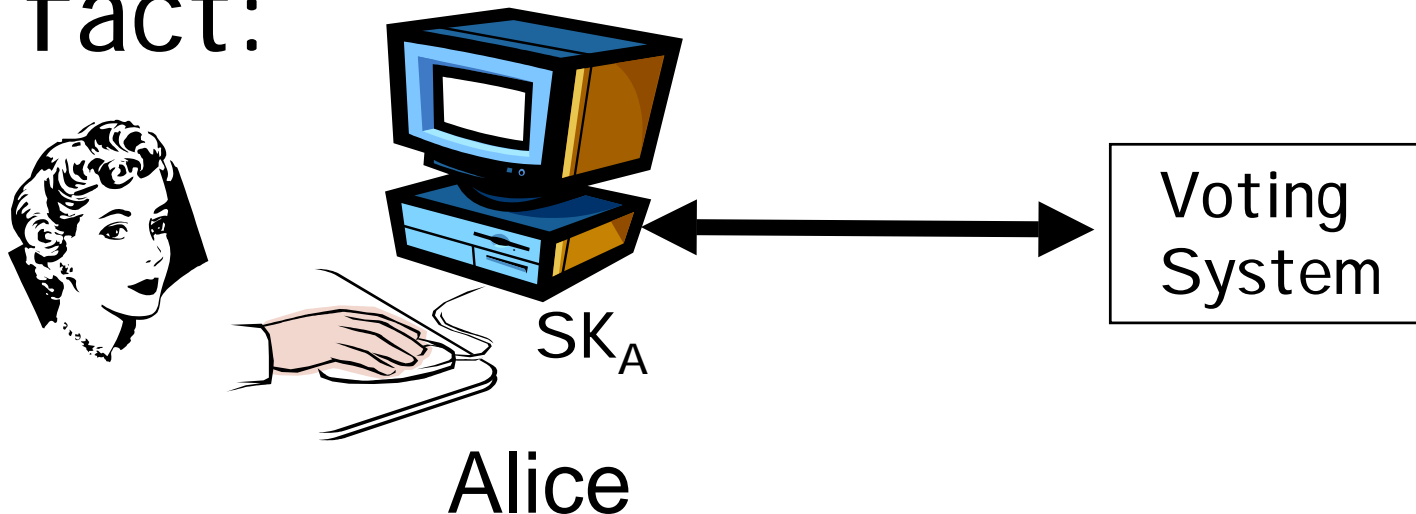


The "Secure Platform Problem"

In theory:



In fact:



Where's the financial angle?

- ◆ Buying and selling votes!!
- ◆ Casting a vote is a bit like depositing an electronic coin...?
- ◆ Getting absentee ballot like getting disposable credit card number...?
- ◆ Congress and states may allocate mucho \$\$ to upgrade voting equipment... (costs are \$5K per precinct just to *lease*).
- ◆ Anonymous political contributions...

Some personal opinions

- ◆ More important that *no one has their thumb on the scale* than having *scale easy to use or very accurate.*
- ◆ Can I convince my mom that system is trustworthy?
- ◆ Physical ballots (e.g. paper) can provide better audit trails than electronic systems.

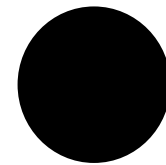
More personal opinions:

- ◆ Precinct-based decisions on voting technology has benefits: lack of uniformity allows for experimentation and makes large-scale fraud harder.
- ◆ Ability to handle disabled voters will become increasingly important.
- ◆ Biggest security problem has got to be the problem of *absentee ballots*.

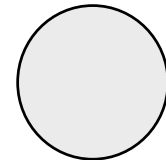
My favorite technology (today)

- ◆ Fill-in bubbles on paper ballots.
Optically scan ballots at polling site,
before ballot is deposited.

Anguilla



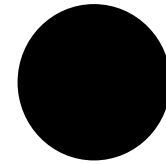
Grand Cayman



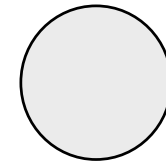
(THE END)

Financial Crypto '02

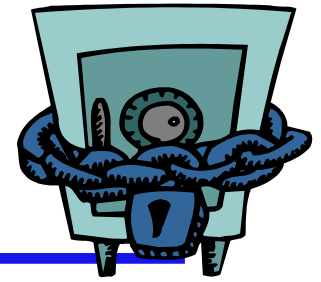
Anguilla



Grand Cayman



Security Requirements



- ◆ All eligible voters should be able to vote.
 - Therefore: can at best augment current system, not replace it.
 - May need to close electronic voting early.
- ◆ Votes should be private (anonymous).
 - May be difficult to ensure at home.
- ◆ Voters should not be able to sell their votes!
 - Voting should be private and “receipt-free”
- ◆ Integrity and verifiability of result; no vulnerability to large-scale fraud.

The “Alice abstraction”

- ◆ *Assumes* Alice can create and keep secret her secret key SK_A , while still being able use it.
- ◆ There is a fundamental conflict between
 - *secrecy* of a secret key, and
 - the *usability* of that secret key

Where does Alice keep SK_A ?

- ◆ An important question!
 SK_A is Alice's "cyber-soul";
theft of SK_A is "identity theft".
- ◆ Modern OS's (Windows, Unix) are too complex to be adequately secure (viruses, Trojan horses).
- ◆ *But*: we need modern OS to support applications and satisfactory UI.
Conflict!

Can Alice use a smart card?

- ◆ A smart card storing SK_A is vulnerable to power-analysis, timing, and chosen-message attacks.
- ◆ Worse, there is no UI on a smart card: it must trust the device into which it is inserted to compose message to be signed.



Needed: a secure platform

- ◆ One that Alice can trust to:
 - Store her secret key SK_A securely
 - Use her secret key to sign messages, without revealing any information about SK_A
 - Reliably show her what she is about to sign (trusted user interface)
 - *Not be vulnerable to Trojan horses and viruses.*

Perhaps a smart phone?



- ◆ Promising, but starting to look too much like a desktop PC in terms of complexity and consequent vulnerability...
- ◆ Maybe with a special SIM card just for voting...?
- ◆ Problems would remain: vote-selling (allow voting multiple times, where last one counts!)