Voters, Computers, and Trust: Designing Verifiable Elections

Stuart M. Shieber
Ben Adida
Greg Morrisett

Center for Research on Computation and Society

October 18, 2008
Secure Voting
• Voting is particularly challenging: requires secrecy and public auditability.

• Computer science enables qualitatively novel solutions.

• Cryptography can reconcile seemingly contradictory requirements.
"That's for me and a button to know."

Joe, the plumber.
Does e-voting need paper trails?

By Anne Broache
Staff Writer, CNET News.com
Published: October 31, 2006, 4:00 AM PST
Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: Oct

State sued over lack of paper trail for ballots

By AMAN BATHEJA
STAR-TELEGRAM STAFF WRITER
Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: Oct

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

Wed Nov 1, 2006 6:37am ET
Does e-voting need paper trails?

By Anne Broache
Staff Writer, New York Times
Published: Oct 18, 2006

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

© Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin
Reporting
Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: Oct 31, 2006

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

© Nov 1, 2006 10:54 pm US/Pacific
California E-Voting Machine Allows Multiple Votes

Allen Martin
Reporting

OCTOBER 31, 2006
Hugo Chavez in the Voting Machine
Does e-voting need paper trails?

By Anne Broache
Staff Writer,
Published: October 31, 2006

State sued over lack of paper trail for ballots

HBO documentary irks voting technology firm

© Nov 1, 2006 10:54 pm US/Pacific

California E-Voting Machine Allows Multiple Votes

Allen Martin
Reporting

OCTOBER 31, 2006

Hugo Chavez in the Voting Machine

Originally published October 26, 2006

Your vote will count
Hype over hacking shouldn't shatter confidence

By Paul DeGregorio
McCLATCHY-TRIBUNE
“When I finally saw the results of our tests, I thought I was going to throw up.”

Sec. of State, Ohio, last week.
Fashionable Voting
Fashionable Voting
Fashionable Voting

http://www.cs.uiowa.edu/~jones/voting/pictures/
Fashionable Voting
Fashionable Voting
Fashionable Voting

http://www.cs.uiowa.edu/~jones/voting/pictures/
Fashionable Voting

http://www.cs.uiowa.edu/~jones/voting/pictures/
Fashionable Voting
Voting is a fundamentally difficult problem.
1 person, 1 vote
Enforced Privacy to ensure each voter votes in his/her own interest
1892 - Australian Ballot

1893

**DEMOCRATIC.**

- FOR MAYOR,
  - AUGUST LEUZ, JR.
  - CORNER BURLINGTON AND JOHNSON STREETS.
- FOR TREASurer,
  - GEORGE W. KOONTZ
  - NO. 620 EAST BURLINGTON STREET.
- FOR CITY SOLICITOR,
  - FRANK J. HORAK
  - NO. 120 DODGE STREET.
- FOR ASSESSOR,
  - F. A. HEINSIUS
  - NO. 948 EAST MARKET STREET.
- FOR TRUSTEE,
  - JOHN U. MILLER
  - EAST MARKET STREET.

**REPUBLICAN.**

- FOR MAYOR,
  - CHAS. LEWIS
  - NO. 227 NORTH CLINTON STREET.
- FOR TREASurer,
- FOR SOLICITOR,
  - L. H. FULLER
  - NO. 422 SOUTH DUBUQUE STREET.
- FOR ASSESSOR,
  - H. W. LATHROP
  - NO. 518 IOWA AVENUE.
- FOR TRUSTEE,
  - J. C. LEASURE
  - COR. VAN BUREN ST. AND IOWA AVENUE.

**Majorities**

- 1892 - 221
- 1893 - 198
The Ballot Handoff

Alice the Voter

McCain
The Ballot Handoff

McCain

Alice the Voter
The Ballot Handoff

Alice the Voter
The Ballot Handoff

Alice the Voter
The Ballot Handoff

Alice the Voter

McCain

Obama

McCain
The Ballot Handoff

Alice the Voter

Black Box

McCain
Obama
McCain
Chain of Custody
Chain of Custody

/*
 * source
 * code
 */
if (...}

Vendor
Chain of Custody

Voting Machine

Vendor

```c
/*
 * source
 * code
 */
if (...)
Chain of Custody

Polling Location  →  Voting Machine  →  Vendor

Vendor

if (...

/*
  * source
  * code
  */
Chain of Custody

1. Vendor
2. Voting Machine
3. Polling Location
4. Alice
Chain of Custody

1. Vendor

2. Voting Machine

/*
 * source
 * code
 */

if (...

3. Polling Location

4. Alice
Chain of Custody

1. Vendor
2. Voting Machine
3. Polling Location
4. Alice
5. Ballot Box Collection

/* source code */
if (...)
Chain of Custody

1. Vendor
2. Voting Machine
3. Polling Location
4. Alice
5. Ballot Box Collection
6. Results

/* source code */
if (...)
Chain of Custody

Polling Location → 3 → Voting Machine → 2 → Vendor

/*
 * source
 * code
 */

if (...)

Alice → 4 → Ballot Box Collection

Black Box → Results

.....
Computers have only obscured the process.
Computers have only obscured the process.

What about computer science?
Cryptography
solving problems that initially appear to have conflicting requirements.
Public-Key Encryption

Customer
Public-Key Encryption

Customer ➔ public key ➔ amazon.com
Public-Key Encryption

Customer

← public key

enc(cc number) →

amazon.com
Public Ballots

Bob: McCain

Carol: Obama
Public Ballots

Bob: McCain
Carol: Obama

Alice
Public Ballots

Alice: Obama
Bob: McCain
Carol: Obama

Alice
Public Ballots

**Alice:** Obama

**Bob:** McCain

**Carol:** Obama

**Tally**

Obama: 2
McCain: 1
Encrypted Public Ballots

Alice: Rice
Bob: Clinton
Carol: Rice

Tally: Obama....2
McCain....1
Encrypted Public Ballots

Alice: Rice
Bob: Clinton
Carol: Rice

Tally:
Obama....2
McCain....1

Alice verifies her vote.
Encrypted Public Ballots

Alice: Rice
Bob: Clinton
Carol: Rice

Tally:Obama....2
McCain....1

Alice verifies her vote
Everyone verifies the tally
How can we verify operations on encrypted data?

Mathematical Proofs.
Zero-Knowledge Proof

Vote For: Obama

Vote For: Obama
Zero-Knowledge Proof
Zero-Knowledge Proof

Vote For: Obama

This last envelope likely contains “Obama”
Zero-Knowledge Proof

Open envelopes don’t prove anything after the fact.