Microsoft Research Faculty Summit 2012

ADVANCING THE STATE OF THE ART
Verifiable Election Technologies

Josh Benaloh
Senior Cryptographer, Microsoft Research

July 16, 2012
Traditional Voting Methods
Traditional Voting Methods

- Hand-Counted Paper

Vote for one option.

- [ ] Joe Smith
- [x] John Citizen
- [ ] Jane Doe
- [ ] Fred Rubble
- [ ] Mary Hill
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
- Touch-Screen Terminals
Traditional Voting Methods

- Hand-Counted Paper
- Punch Cards
- Lever Machines
- Optical Scan Ballots
- Electronic Voting Machines
- Touch-Screen Terminals
- Various Hybrids
All of these systems have substantial vulnerabilities.

All of these systems require trust in the honesty and expertise of election officials (and usually the equipment vendors as well).

Can we do better?
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective
The Voter’s Perspective

• As a voter, you don’t really know what happens behind the curtain.
• You have no choice but to trust the people working behind the curtain.
• You don’t even get to choose the people who you will have to trust.
Fully-Verifiable Election Technologies

(aka End-to-End Verifiable)

Allow voters to track their individual (sealed) votes and ensure that they are properly counted...

... even in the presence of faulty or malicious election equipment ...

... and/or careless or dishonest election personnel.
Voters can check...

... that their (sealed) votes have been properly recorded

... and that all recorded votes have been properly counted

This is *not* just checking a claim that the right steps have been taken...

This is actually a check that the counting is correct.
Where is My Vote?
Where is My Vote?

Alice Johnson, 123 Main – YES

Bob Ramirez, 79 Oak – NO

Carol Wilson, 821 Market – NO
End-to-End Voter-Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
  - Counted as cast
- All votes are counted as cast

... without having to trust anyone or anything.
But wait ...

This isn’t a *secret-ballot* election.
Quite true, but it’s enough to show that voter-verifiability is possible
... and also to falsify arguments that electronic elections are inherently untrustworthy.
Privacy

The only ingredient missing from this transparent election is privacy – and the things which flow from privacy (e.g. protection from coercion).

Performing tasks while preserving privacy is the bailiwick of cryptography.

Cryptographic techniques can enable fully-verifiable elections while preserving voter privacy.
Where is My Vote?

Alice Johnson, 123 Main –

Bob Ramirez, 79 Oak –

Carol Wilson, 821 Market –
Where is My Vote?

Alice Johnson, 123 Main –

Bob Ramirez, 79 Oak –

Carol Wilson, 821 Market –
Where is My Vote?
Where is My Vote?
Where is My Vote?

No – 2

Yes – 1
Where is My Vote?

No – 2
Yes – 1

Mathematical Proof
End-to-End Voter-Verifiability

As a voter, I can be sure that

- My vote is
  - Cast as intended
  - Counted as cast
- All votes are counted as cast

... without having to trust anyone or anything.
The Voter’s Perspective

Verifiable election systems can be built to look exactly like current systems ...

... with one addition ...
A Verifiable Receipt

Precinct 37 – Machine 4
Nov. 6, 2012  1:39PM

Vote receipt tag:
7A34ZR9K4BX

***VOTE CONFIRMED***
The Voter’s Perspective

Voters can ...

- Use their receipts to check that their results are properly recorded on a public web site.
- Throw their receipts in the trash.
- Verify the accuracy of the election with apps they wrote themselves.
- Download apps from sources of their choice to verify the election.
- Believe verifications done by their political parties, LWV, ACLU, etc.
- Accept the results without question.
End-to-End Verifiable Elections

Anyone who cares to do so can

- Check that their own *encrypted* votes are correctly listed
- Check that other voters are legitimate
- Check the cryptographic proof of the correctness of the announced tally
Yes ...

... but there are lots of details to get right.
Two questions must be answered ...

· How do voters turn their preferences into encrypted votes?

· How are voters convinced that the published set of encrypted votes corresponds to the announced tally?
Many tools are available ...

... including “homomorphic encryption”:

\[ A \text{ is an encryption of } a \]
\[ B \text{ is an encryption of } b \]
\[ A \otimes B \text{ is an encryption of } a \oplus b \]
# Homomorphic Tallying

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>
## Homomorphic Tallying

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ \Sigma = \]
Homomorphic Tallying

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

\[ \Sigma = 2 \]
## Homomorphic Tallying

<table>
<thead>
<tr>
<th>Name</th>
<th>Tally</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>
Homomorphic Tallying

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Bob</th>
<th>Carol</th>
<th>David</th>
<th>Eve</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
# Homomorphic Tallying

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
</tr>
</tbody>
</table>

\[ \bigotimes = 2 \]
Homomorphic Tallying

<table>
<thead>
<tr>
<th></th>
<th>Alice</th>
<th>Bob</th>
<th>Carol</th>
<th>David</th>
<th>Eve</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Bob</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Carol</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>David</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Eve</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

\[\otimes = 2\]
Most pre-2000 verifiable election protocols:

**Step 1**

Encrypt your vote.

**How?**
How do Humans Encrypt?

If voters encrypt their votes with devices of their own choosing, they are subject to coercion and compromise.

If voters encrypt their votes on “official” devices, how can they trust that their intentions have been properly captured?
We need to find ways to engage humans in an interactive proof process to ensure that their intentions are accurately reflected in encrypted ballots cast on their behalf.
<table>
<thead>
<tr>
<th></th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>
# MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>367</td>
<td>248</td>
<td>792</td>
<td>141</td>
<td>390</td>
<td>863</td>
<td>427</td>
<td>015</td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
<td></td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Alice</td>
<td>Bob</td>
<td>Carol</td>
<td>David</td>
<td>Eve</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>----------------</td>
<td>-------------</td>
<td>------------</td>
<td>------------</td>
<td>-----------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>367</td>
<td>248</td>
<td>792</td>
<td>141</td>
<td>390</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>248</td>
<td>792</td>
<td>141</td>
<td>390</td>
<td>863</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>792</td>
<td>141</td>
<td>390</td>
<td>863</td>
<td>427</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>141</td>
<td>390</td>
<td>863</td>
<td>427</td>
<td>015</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>390</td>
<td>863</td>
<td>427</td>
<td>015</td>
<td>367</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>863</td>
<td>427</td>
<td>015</td>
<td>367</td>
<td>248</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>427</td>
<td>015</td>
<td>367</td>
<td>248</td>
<td>792</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>015</td>
<td>367</td>
<td>248</td>
<td>792</td>
<td>141</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Device commitment to voter: “You’re candidate’s number is 863.”
### MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>

Device commitment to voter: “You’re candidate’s number is 863.”
Voter challenge: “Decrypt column number 5.”
### MarkPledge Ballot

<table>
<thead>
<tr>
<th>Alice</th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
</tbody>
</table>

Device commitment to voter: “You’re candidate’s number is 863.”

Voter challenge: “Decrypt column number 5.”
# MarkPledge Ballot

<table>
<thead>
<tr>
<th></th>
<th>367</th>
<th>248</th>
<th>792</th>
<th>141</th>
<th>390</th>
<th>863</th>
<th>427</th>
<th>015</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td>629</td>
<td>523</td>
<td>916</td>
<td>504</td>
<td>129</td>
<td>077</td>
<td>476</td>
<td>947</td>
</tr>
<tr>
<td>Carol</td>
<td>285</td>
<td>668</td>
<td>049</td>
<td>732</td>
<td>859</td>
<td>308</td>
<td>156</td>
<td>422</td>
</tr>
<tr>
<td>David</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
<td>863</td>
</tr>
<tr>
<td>Eve</td>
<td>264</td>
<td>717</td>
<td>740</td>
<td>317</td>
<td>832</td>
<td>399</td>
<td>441</td>
<td>946</td>
</tr>
<tr>
<td>Prêt à Voter Ballot</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alice</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17320508</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Eve</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carol</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alice</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>David</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17320508
Prêt à Voter Ballot

X

17320508
PunchScan Ballot

Y – Alice
X – Bob

#001
PunchScan Ballot

Y – Alice
X – Bob

#001
PunchScan Ballot

X – Alice
Y – Bob

#001
PunchScan Ballot

X – Alice
Y – Bob

#001

Y
X

#001
Scantegrity

5. Voters
Choose one:
(a) the
(b) the

6. Voters
Choose one:
(a) the
(b) the

Identify
for other
the record
the record

Voter can use “any” device to make selections (touch-screen DRE, OpScan, etc.)

After selections are made, voter receives an encrypted receipt of the ballot.
Voter-Initiated Auditing

Voter choice: Cast or Challenge
Voter-Initiated Auditing

Cast

734922031382

Encrypted Vote

Ballots
Challenge

Vote for Alice
Random # is 28637582738
Real-World Deployments

Helios ([www.heliosvoting.org](http://www.heliosvoting.org)) – Ben Adida and others
  · Remote electronic voting system using voter-initiated auditing and homomorphic backend.
  · Used to elect president of UC Louvain, Belgium.
  · Used in Princeton University student government.
  · Used to elect IACR Board of Directors.

Scantegrity II ([www.scantegrity.org](http://www.scantegrity.org)) – David Chaum, Ron Rivest, many others.
  · Optical scan system with codes revealed by invisible ink markers and “plugboard-mixnet” backend.
  · Used for municipal elections in Takoma Park, MD.
Front End
There is great value in continuing work on the user-facing front end.
The front end should be
· Simpler to use
· Simpler to understand
· Higher assurance
Back End

Simple counting methods are well-understood with effective techniques. More complex counting methods create substantial challenges –

- Maintaining strong privacy
- Keeping computations efficient
Election Technologies – Today and Tomorrow

Lillie Coney,
Electronic Privacy Information Center
J. Alex Halderman,
University of Michigan
Josh Benaloh,
Microsoft Research

July 16, 2012