ThreeBallot, VAV, and Twin

Ronald L. Rivest - MIT CSAIL
Warren D. Smith - CRV

Talk at EVT’07 (Boston)
August 6, 2007
Outline

- End-to-end voting systems
- ThreeBallot
- VAV
- Twin
“End-to-end” voting systems

- Voter composes and casts ballot as usual, except cast ballot may be encrypted.
- Cast ballots posted on public bulletin board (PBB).
- Voter gets “receipt” allowing her to confirm & correct posting of her ballot; receipt is typically copy of cast ballot as it should be posted.
- Tally is computed by election officials from ballots on PBB (proof of correctness also computed and posted).
End-to-end voting systems

- **VM**: Voter
- **PBB**: Cast Ballot
- **EO**: Confirm Posting
- **Result**: Verify Tally

Voter → PBB → EO → Result

Voter receives Receipt from PBB and EO.
End-to-end voting systems

Cast Ballot
“Cast as intended?”

Confirm Posting
“Posted as cast?”

Verify Tally
“Counted as posted?”
Crypto end-to-end voting systems

- Cast ballots are encrypted.
- With encrypted ballots, need to ensure they are “cast as intended” [challenging].
- With receipts, need to ensure that they don’t reveal how voter voted [not so hard].
- With tally, need to ensure that election result is publicly verifiable [manageable].
- Examples: Punchscan, PretAVoter, Scratch&Vote, ...
Crypto-free end-to-end systems

- Is it possible to have an end-to-end voting system without using cryptography?
Crypto-free end-to-end systems

- Is it possible to have an end-to-end voting system without using cryptography?
  - Yes. ThreeBallot.
  - Yes. VAV.
  - Yes. Twin.
ThreeBallot
Voting w/o crypto -- ThreeBallot

- Each voter casts three plaintext ballots
- All three cast ballots go on PBB.
- Voter takes home copy of arbitrarily-chosen one as receipt.
- Receipt does not indicate how she voted, but serves as integrity check on PBB.
Each row has 1 or 2 marks. Not 0, not 3.
All three ballots cast and posted on PBB.
Voter takes home copy of one as “receipt”.

<table>
<thead>
<tr>
<th>Ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>President</strong></td>
</tr>
<tr>
<td>Alice</td>
</tr>
<tr>
<td>Bob</td>
</tr>
<tr>
<td>Charles</td>
</tr>
<tr>
<td><strong>Vice President</strong></td>
</tr>
<tr>
<td>David</td>
</tr>
<tr>
<td>Erica</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>President</strong></td>
</tr>
<tr>
<td>Alice</td>
</tr>
<tr>
<td>Bob</td>
</tr>
<tr>
<td>Charles</td>
</tr>
<tr>
<td><strong>Vice President</strong></td>
</tr>
<tr>
<td>David</td>
</tr>
<tr>
<td>Erica</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>President</strong></td>
</tr>
<tr>
<td>Alice</td>
</tr>
<tr>
<td>Bob</td>
</tr>
<tr>
<td>Charles</td>
</tr>
<tr>
<td><strong>Vice President</strong></td>
</tr>
<tr>
<td>David</td>
</tr>
<tr>
<td>Erica</td>
</tr>
</tbody>
</table>
ThreeBallot

- Each row has 1 or 2 marks. Not 0, not 3.
- All three ballots cast and posted on PBB.
- Voter takes home copy of one as “receipt”.

<table>
<thead>
<tr>
<th>Ballot</th>
<th>Ballot</th>
<th>Ballot</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>President</strong></td>
<td><strong>President</strong></td>
<td><strong>President</strong></td>
</tr>
<tr>
<td>Alice</td>
<td>Alice</td>
<td>Alice</td>
</tr>
<tr>
<td>Bob</td>
<td>Bob</td>
<td>Bob</td>
</tr>
<tr>
<td>Charles</td>
<td>Charles</td>
<td>Charles</td>
</tr>
<tr>
<td><strong>Vice President</strong></td>
<td><strong>Vice President</strong></td>
<td><strong>Vice President</strong></td>
</tr>
<tr>
<td>David</td>
<td>David</td>
<td>David</td>
</tr>
<tr>
<td>Erica</td>
<td>Erica</td>
<td>Erica</td>
</tr>
</tbody>
</table>

r9>k*@0e!4$%
*t3]a&;nzs^_= u)*/8c$@.?( 
Tallying in ThreeBallot

- Tally as usual: each candidate receives $n$ extra votes ($n =$ number of voters), but election outcome is unchanged.
- Works for (or can be adapted for) ordinary plurality voting, approval voting, and range voting, but not for IRV or other schemes where voter must rank-order choices.
- Also doesn’t work for write-in votes.
Casting ballots

- Votes are cast in a physical ballot box; order of casting is lost, and it is should be impossible to figure out which three ballots originally formed a ballot triple.
Ensuring valid votes

- Need way to ensure that votes are valid -- voter doesn’t vote zero or three times for anyone.

- Voter casts ballots through a checker machine that checks validity of ballot triple before allowing them to be cast.
Making receipts

- Voter may arbitrarily choose one ballot to be copied as her receipt.
- No record kept of which was copied.
- Can integrate copying with checker (Shamos checker).
- Receipts should be “unforgeable”.

Diagram: Ballot Box -> Checker Machine -> Receipt
Confirming Posting

- Ballots aren’t posted on PBB until polls are closed.
- Each ballot should have a unique ID (matching ID on receipt copy), so that ID can be looked up on PBB.
- Voters should not see (and/or not be able to memorize) ID’s for ballots that were not copied (to prevent vote-selling).
Short Ballot Assumption (SBA)

- Since ballots are published in plaintext, voters must not be able to identify their ballots by the selection of choices made.

- Short Ballot Assumption: ballot is short enough so that each possible arrangement of choices likely to have been made by several voters.

- Can separate ballot into several short ones to ensure SBA.

- SBA also prevents reconstruction attacks.
Integrity of PBB

- Since no one knows *which* ballots posted on PBB have been copied for receipts, any significant tampering with PBB is likely to be detectable.
Coercion-freeness

- Voter can bring home an arbitrary-looking receipt, independent of her choices. Thus, voter can’t sell vote using her receipt.
- Adversary (or voter) can’t determine which three ballots were in original triple from PBB and receipt.
Usability

- Not so good! Voting three ballots would be confusing to many!
- Note: Can mix “OneBallot” (ordinary ballots) with ThreeBallot:
  - OneBallot voters don’t get receipts.
  - But their ballots posted on PBB are protected along with ThreeBallots.
ThreeBallot is end-to-end

- ThreeBallot provides end-to-end security:
  - Voter is confident her ballot is cast as intended.
  - Voter can check that her ballot is included in collection of ballots being tallied.
  - Voters can check that tampering with collection has not occurred.
  - Anyone can add up ballots on PBB to obtain correct election result.
(Vote // Anti-Vote // Vote)
VAV = ThreeBallot Variation

- Like ThreeBallot: each voter casts three ballots and takes home copy of one as a receipt.
- But VAV works for any vote-tallying system (e.g. IRV), not just plurality, approval, and range-voting.
- Key idea: one ballot may cancel another ballot. Of three ballots cast, two of them must cancel each other.
**VAV Example Ballots**

<table>
<thead>
<tr>
<th>Ballot</th>
<th>President</th>
<th>Vice President</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alice 1</td>
<td>David 2</td>
</tr>
<tr>
<td></td>
<td>Bob 3</td>
<td>Erica 1</td>
</tr>
<tr>
<td></td>
<td>Charles 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4765239014119052</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ballot</th>
<th>President</th>
<th>Vice President</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alice 1</td>
<td>David 2</td>
</tr>
<tr>
<td></td>
<td>Bob 3</td>
<td>Erica 1</td>
</tr>
<tr>
<td></td>
<td>Charles 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>155236349001341</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Ballot</th>
<th>President</th>
<th>Vice President</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alice 3</td>
<td>David 1</td>
</tr>
<tr>
<td></td>
<td>Bob 1</td>
<td>Erica 2</td>
</tr>
<tr>
<td></td>
<td>Charles 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>144578232133782</td>
<td></td>
</tr>
</tbody>
</table>

- **Second (Anti-) ballot cancels first ballot, since they are identical except for A/V notations.**
- **As in ThreeBallot, voter can take home copy of any one ballot as her receipt.**
Tallying VAV ballots

- Tallier finds pairs of V/A ballots that cancel, and removes such pairs from further consideration. (The ballots in a pair don’t need to have originated with the same voter.)
- Remaining ballots are tallied to determine election results.
- VAV handles any voting system.
- VAV also provides end-to-end security.
Twin
Key Idea for Twin

- With ThreeBallot, voter could not use take-home receipt to sell her vote, because it copied only a part of her ballot.
- With Twin, voter can not use take-home receipt to sell her vote, because it is copy of some other voter’s ballot.
- Single original may be copied more than once, or not at all.
- Simple!
“Mixing up” voter receipts

- Voter places her receipt into the bin, and receives a copy of some previous voter’s receipt from the bin.
- First 10 voters don’t get take-home receipt.
- Voter checks PBB with her take-home receipt.
- At end of day, bin has all original receipts; enables additional check on PBB.
“Mixing up” voter receipts

- Voter places her receipt into the bin, and receives a *copy* of some previous voter’s receipt from the bin.
- First 10 voters don’t get take-home receipt.
- Voter checks PBB with her take-home receipt.
- At end of day, bin has all original receipts; enables additional check on PBB.
“Mixing up” voter receipts

- Voter places her receipt into the bin, and receives a copy of some previous voter's receipt from the bin.
- First 10 voters don’t get take-home receipt.
- Voter checks PBB with her take-home receipt.
- At end of day, bin has all original receipts; enables additional check on PBB.
“Mixing up” voter receipts

- Voter places her receipt into the bin, and receives a copy of some previous voter’s receipt from the bin.
- First 10 voters don’t get take-home receipt.
- Voter checks PBB with her take-home receipt.
- At end of day, bin has all original receipts; enables additional check on PBB.
“Mixing up” voter receipts

- Voter places her receipt into the bin, and receives a copy of some previous voter’s receipt from the bin.
- First 10 voters don’t get take-home receipt.
- Voter checks PBB with her take-home receipt.
- At end of day, bin has all original receipts; enables additional check on PBB.
“Mixing up” voter receipts

- Voter places her receipt into the bin, and receives a *copy* of some previous voter's receipt from the bin.
- First 10 voters don’t get take-home receipt.
- Voter checks PBB with her take-home receipt.
- At end of day, bin has all original receipts; enables additional check on PBB.
Properties of Twin

- **[Exchange]** Voter gets a copy of *some other voter’s* receipt as her take-home receipt.
- **[Anonymity]** Voter does not know which other voter she received copy from.
- **[Collusion-Resistance]** Adversary has no good way of collecting *all* copies of some receipt.
- **[Coverage]** Constant fraction of all receipts are copied as take-home receipts, with high probability.
- **[End-to-end security]** Twin provides end-to-end security.
- Twin is similar to “Farnel” protocol, except we are applying it to receipts, not ballots, and we distribute *copies* rather than originals.
Conclusions

- End-to-end voting systems provide improved assurance of correctness of election outcome.
- It is possible to implement end-to-end voting systems without using cryptography.
(The End)