Write-ins for Prêt à Voter

Steve Schneider
University of Surrey, UK
Outline of talk

- Context: Electronic voting issues and challenges
- Pret a Voter Design Overview
- Handling write-ins
“The Write-in”, Hogarth 1755

Hogarth: The Polling (1755)
Electronic voting (2005)
Write-ins (2010)

United States Senator
(vote for one)

- McAdams, Scott T.
- Miller, Joe
- Carter, Tim
- Gianoutsos, Ted
- Haase, Fredrick "David"
- Write-in

United States
Representative

©2010 www.kath.tv

www.surrey.ac.uk
Issues with electronic voting

• On 3rd August 2007 the state of California decertified all four electronic voting machines currently in use.
  – susceptibility of the machines to viruses that propagate between voting machines, or between voting machines and the election management system, that could maliciously cause votes to be recorded incorrectly or miscounted.

• Lack of transparency.

• Complexity means that systems and processes are harder for the voting public to understand.

• Security vulnerabilities and threats.

• Need to trust the manufacturer.

» The situation has not improved (2011)
Electronic voting

• What if you suspect your vote was altered, or not counted?
Lawyers poised as US vote hit by technical glitches

Corruption and terrorism top of voters’ concerns
Fight for closely-contested states energises electorate

Julian Borger Washington
Ed Pilkington Evansville, Indiana

Americans turned out in force yesterday to vote in a bitterly fought election to decide who will control Congress for the last two years of the Bush era, but the poll was marred by technical glitches and accusations of fraud.

Patrick Wintour Political editor

Tony Blair and Gordon Brown last night convened an unprecedented meeting of 60 ministers in a bid to put the government back on track after Labour’s recent infighting. The summit was seen as an attempt by the government to draw a line under the party’s difficulties, and set out a challenging policy agenda for the next 10 years. The involvement of both the prime minister and the chancellor alongside senior civil servants was taken as a sign they realise they must cooperate if the party is to overcome its most serious midterm poll decline since it came to power in 1997.
Desiderata for a(n electronic) voting system

- Secrecy of the ballot.
- Integrity: Correctness of the tally.
- Auditability: end to end verifiability.
  - In Prêt à Voter, the votes themselves and how they have been processed is public and auditable.
  - More than just checking the equipment.
- Can handle a variety of election systems (first past the post, approval, STV…)
- Usability.
Verifying your vote

• In current UK (non-electronic) elections, you have no way of checking that your vote was counted, and no way of challenging the system if you don’t think it was. You (have to) trust the system.
• What if your vote was lost?
• What if your vote was spoiled during counting?

• Compare: for financial transactions, this approach of trusting the system would be unthinkable.
  – No receipts.
  – No bank statements.
  – No way of challenging mistakes (or fraud).

• How can verification mechanisms be introduced into voting systems?
End to end verifiability

• End to end verifiability is being able to verify that the vote that has been cast really was included in the final tally.
  – Voters’ intent is reflected in the final result, and this can be verified.

• End to end verifiability already exists in particular contexts:
  – for example, it is achieved in parliament by listing all of the voters (MPs) and how they have voted.
  – Shareholders meetings.

• Issues around public record of all votes:
  – loss of privacy;
  – vulnerable to coercion.
Voter evidence: Receipts

• To check and challenge the public record, voters need some evidence that they can use after the election if necessary. Such evidence is called a receipt.
  – More than just evidence of casting some vote.
  – A receipt should provide evidence of the vote that has been cast.
  – (cf evidence of purchase, vs a receipt for the amount involved).
• Privacy: a receipt must not give away who the vote was for.
  – Need to break the link between the actual vote, and the receipt of the ballot form. (cf a `gift receipt’)
• Cryptography can provide this.
Desiderata for an electronic voting system

• Secrecy of the ballot.
• Integrity: Correctness of the tally.
• Auditability: end to end verifiability.
  – Of the election information itself, not the processes.
• Receipt freeness.
  – The voter should not have a receipt that indicates how the vote was cast. (otherwise vote selling, coercion are possible)
• Coercion resistance.
• Usability.
• Can handle a variety of election systems (first past the post, STV, Borda, Condorcet…).
Voting with Prêt à Voter

- Place X against desired candidate. (candidates in random order)
- Separate left hand side.
- Destroy left hand side.
- Cast (scan) vote.
- Take receipt home.

- Key point: the receipt could match a vote for anyone.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Alice</td>
<td></td>
</tr>
<tr>
<td>2. Bob</td>
<td></td>
</tr>
<tr>
<td>3. Crystal</td>
<td></td>
</tr>
<tr>
<td>4. Diane</td>
<td></td>
</tr>
<tr>
<td>5. Elaine</td>
<td></td>
</tr>
</tbody>
</table>

6QakL5sR
Voting with Prêt à Voter

- Place X against desired candidate. (candidates in random order)
- Separate left hand side.
- Destroy left hand side.
- Cast (scan) vote.
- Take receipt home.

- Key point: the receipt could match a vote for anyone.

---

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

6QakL5sR
Voting with Prêt à Voter

• Place X against desired candidate. (candidates in random order)
• Separate left hand side.
• Destroy left hand side.
• Cast (scan) vote.
• Take receipt home.

• Key point: the receipt could match a vote for anyone.

<table>
<thead>
<tr>
<th>1. Alice</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Bob</td>
</tr>
<tr>
<td>3. Crystal</td>
</tr>
<tr>
<td>4. Diane</td>
</tr>
<tr>
<td>5. Elaine</td>
</tr>
</tbody>
</table>

6QakL5sR
Voting with Prêt à Voter

- Place X against desired candidate. (candidates in random order)
- Separate left hand side.
- Destroy left hand side.
- Cast (scan) vote.
- Take receipt home.

- Key point: the receipt could match a vote for anyone.

6QakL5sR
Voting with Prêt à Voter

- Place X against desired candidate. (candidates in random order)
- Separate left hand side.
- Destroy left hand side.
- Cast (scan) vote.
- Take receipt home.

- Key point: the receipt could match a vote for anyone.
Voting with Prêt à Voter

- Place X against desired candidate. (candidates in random order)
- Separate left hand side.
- Destroy left hand side.
- Cast (scan) vote.
- Take receipt home.

- Key point: the receipt could match a vote for anyone.
Publish the ballots cast

Public bulletin board of votes cast.

Voter’s receipt

Thursday, 2 February 12
Publish the ballots cast

Public bulletin board of votes cast.

Voter’s receipt

Thursday, 2 February 12
Publish the ballots cast

- Voter receipts prevent election officials from discarding votes.

Voter’s receipt
Publish the ballots cast

- Voter receipts prevent election officials from discarding votes.
- Voters confirm inclusion of their vote

Voter’s receipt

Public bulletin board of votes cast.

Thursday, 2 February 12
Tallying

When the votes are cast:

• Publish the votes cast (newspaper, or web bulletin board)
  – these should match the receipts, and voters can check.
• Mix up the votes (see next slide), so resulting votes are not linked to input votes (which correspond to receipts):
  – Decryption - mix and decrypt together
  – or Re-encryption - mix but don’t decrypt yet
• Publish the resulting votes.
  – Decrypt if still encrypted;
  – or combine ‘homomorphically’ while still encrypted
• Count the votes.
  – Tally decrypted votes
  – or decrypt homomorphic tally
Mix nets (Chaum)

- Can audit random links without linking receipts to votes (Randomised partial checking)
- Alternatively, tellers can provide `proofs of shuffles`
- Decryption or re-encryption mixing
Prêt à Voter in one slide

Voters → Ballot Casting → Encrypted Votes → Ballot Shuffling by mixnet → Encrypted Votes → Decrypt and Count → Results

- Verify by receipts
- Verify by audit/checks
- Verify by public information

End-to-end verifiability

www.surrey.ac.uk
Write-ins

• ‘A dumb idea... necessary to offset other dumb ideas’
  Charles Stewart III
Pret a Voter ballot form with write-ins

<table>
<thead>
<tr>
<th></th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daniel</td>
<td></td>
</tr>
<tr>
<td>Ben</td>
<td></td>
</tr>
<tr>
<td>Ali</td>
<td></td>
</tr>
<tr>
<td>Write-In</td>
<td></td>
</tr>
<tr>
<td>Cathy</td>
<td></td>
</tr>
</tbody>
</table>

write-in name here

E(Daniel,r_{14,d})
E(Ben,r_{14,b})
E(Ali,r_{14,a})
E(Write-in,r_{14,w})
E(Cathy,r_{14,c})
Completing the ballot 1

• X against listed name
• No name written in

• This is a vote for Cathy
Completing the ballot 2

• X against `write-in’
• Name written in

• This is a vote for Bobbie
Completing the ballot 3

- X against listed name
- Name written in

- This is a vote for Cathy

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Daniel</td>
<td></td>
</tr>
<tr>
<td>Ben</td>
<td></td>
</tr>
<tr>
<td>Ali</td>
<td></td>
</tr>
<tr>
<td><strong>Write-In</strong></td>
<td></td>
</tr>
<tr>
<td>Cathy</td>
<td>X</td>
</tr>
<tr>
<td>write-in name here</td>
<td></td>
</tr>
</tbody>
</table>

Bobbie

7xf2w-4j8yt
Completing the ballot 4

- X against `write-in'
- No name written in
- This is a spoiled ballot
Receipt with named write-in

- Could be a vote for a listed candidate
- Could be a vote for the named candidate
- Consistent with vote for any listed candidate
- or with a vote for Rob

write-in name here

Rob

7xf2w-4j8yt
Receipt with blank write-in

• Could be a vote for a listed candidate
• Could be a spoiled ballot (i.e. vote for `write-in’)
• Consistent with vote for any listed candidate
• but not with any write-in candidate
Mix 1

- The code, e.g. $E(\text{Cathy}, r_{14}, c)$, for the encoded selection is an input to the mix.
- The serial number e.g. 14 of the ballot paper is an input to the mix, paired with the selection.

- Shuffle and re-encrypt (keep pairs together).
- Decrypt selection (can tally non-write-ins).
- Serial numbers remain encrypted at this stage.
Mix 1

E(Null, r₄) → E(Write-In, r₃') → Write-In
E(4, 1) → E(3, s₃')

E(Write-In, r₅) → E(Write-In, r₁') → Write-In
E(5, 1) → E(i, s₁')

E(Write-In, rᵢ) → E(Null, r₄') → Null
E(i, 1) → E(4, s₄')

Encode Write-Ins  Shuffle and re-encrypt  Decrypt candidates  serial number  write-in

Thursday, 2 February 12
• Encode ‘Write-in’ as E(1,1)
• Code up anything else (e.g. ‘Cathy’) as E(0,1)

• Pair with encrypted serial numbers
• Shuffle and re-encrypt pairs
• Decrypt serial numbers
Mix 2

Write-in
E(3,s_3') → E(1,1)
E(3,s_3')

E(1,t_0)

E(1,t_0)

Write-in
E(i,s_i') → E(1,1)
E(i,s_i')

E(0,t_4)

E(0,t_4)

Null
E(4,s_4') → E(0,1)
E(4,s_4')

E(1,t_5)

E(1,t_5)

E(4,s_4')

E(5,s_5')

E(5,s_5')

encode votes shuffle and re-encrypt decrypt indexes
Write-in tally

- Allocate the written-in names against candidates
  - (this can be done in parallel with the mixes)
- Collect together the encrypted $E(0,r)$ and $E(1,r)$ for each candidate
- Homomorphically tally, for those candidates where it is appropriate
Receipt-freeness

- Can vote for any listed candidate, and emerge with any receipt

- BUT not receipt-free for write-ins:
  - Blank receipt means no write-in
  - Filled in write-in means no other write-in candidate received the vote
Solution: Null (dummy) ballots
Voters given valid and null ballot form

<table>
<thead>
<tr>
<th>Write-in name</th>
<th>Daniel</th>
<th>Ben</th>
<th>Ali</th>
<th>Write-In</th>
<th>Cathy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Write-In</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid W-I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Write-in name
fr5sq-j69iu
Complete both ballots: both processed independently

<table>
<thead>
<tr>
<th>Daniel</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ben</td>
<td></td>
</tr>
<tr>
<td>Ali</td>
<td></td>
</tr>
<tr>
<td>Write-In</td>
<td></td>
</tr>
<tr>
<td>Cathy</td>
<td>X</td>
</tr>
</tbody>
</table>

- write-in name here
- 7xf2w-4j8yt

<table>
<thead>
<tr>
<th>Null</th>
<th>67</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td></td>
</tr>
<tr>
<td>Null</td>
<td></td>
</tr>
<tr>
<td>Null</td>
<td></td>
</tr>
</tbody>
</table>

- write-in name here
- 8sf12-hrp9j

- Donald

Thursday, 2 February 12
Conclusion: Receipt-freeness, coercion-resistance

- Receipt-freeness: any receipt is consistent with any cast vote, including write-ins
- Issues around handwriting (i.e. receipts on bulletin board are recognisable)
- Issues around unique (recognisable) names from coercer, on both ballot forms... solved by allowing voters any number of null forms
- Crypto analysis...?
“The Write-in”, Hogarth 1755

Hogarth: The Polling (1755)