Towards Secure Internet e-Voting

Yvo Desmedt\textsuperscript{1,2}  Stelios Erotokritou\textsuperscript{1}  Rebecca Wright\textsuperscript{3}

\textsuperscript{1} Department of Computer Science
University College London, UK

\textsuperscript{2} Research Center for Information Security (RCIS)
AIST, Japan

\textsuperscript{3} Computer Science Department and DIMACS
Rutgers University

August 17, 2010
1. **CODE VOTING**

**IACR Election Voting Codes**

<table>
<thead>
<tr>
<th>Name</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antoine</td>
<td>7556144853</td>
</tr>
<tr>
<td>Bart</td>
<td>6899798021</td>
</tr>
<tr>
<td>Christian</td>
<td>6077258430</td>
</tr>
<tr>
<td>Helena</td>
<td>2450694286</td>
</tr>
<tr>
<td>Josh</td>
<td>9093806830</td>
</tr>
<tr>
<td>Thomas</td>
<td>4448934855</td>
</tr>
<tr>
<td>Tsutomu</td>
<td>2536721542</td>
</tr>
</tbody>
</table>

**Yvo Desmedt**

Department of Computer Science
Gower Street
London WC1E 6BT
United Kingdom

Yvo Desmedt
Department of Computer Science
Gower Street
London WC1E 6BT
United Kingdom

Andrew Yao
Centre for Quantum Information and Quantum Control
University of Toronto
Toronto, ON M5S 3H6
Canada

Rebecca Wright
Rensselaer Polytechnic Institute
215 W. Phila. St.
Poughkeepsie, NY 12604
USA
IACR Election
Please enter your string below:

Rebecca Wright
Rutgers University
96 Frelinghuysen Road
Piscataway, NJ 08854
USA

<table>
<thead>
<tr>
<th>Voting Codes</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Antoine</td>
<td>8173472492</td>
</tr>
<tr>
<td>Bart</td>
<td>9287374672</td>
</tr>
<tr>
<td>Christian</td>
<td>0198291639</td>
</tr>
<tr>
<td>Helena</td>
<td>2373919017</td>
</tr>
<tr>
<td>Josh</td>
<td>2638939283</td>
</tr>
<tr>
<td>Thomas</td>
<td>1923872622</td>
</tr>
<tr>
<td>Tsutomu</td>
<td>8294729027</td>
</tr>
</tbody>
</table>
2. Advantages/Disadvantages

Advantages of Code Voting: secure even if voter’s machine hacked.

Disadvantages:

• requires IACR to send random numbers by postal mail, and

• no collusion between postal system (or sender of envelopes) and the party receiving the vote.
Ballot stuffing with Code Voting

IACR Election Voting Codes
Antoine - 7556144953
Bart  - 6899798021
Christian  - 6077258430
Helena  - 2450694286
Josh   - 9093806830
Thomas - 4448934855
Tsutomu - 2536721542
### 3. Voting Using Our Solution

<table>
<thead>
<tr>
<th>IACR Election Voting Codes</th>
<th>Antoine</th>
<th>Bart</th>
<th>Christian</th>
<th>Helena</th>
<th>Tsutomu</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2613</td>
<td>9384</td>
<td>8173</td>
<td>6734</td>
<td>4832</td>
</tr>
<tr>
<td>IACR Election Voting Codes</td>
<td>Antoine</td>
<td>Bart</td>
<td>Christian</td>
<td>Helena</td>
<td>Tsutomu</td>
</tr>
<tr>
<td></td>
<td>1827</td>
<td>9394</td>
<td>0238</td>
<td>9187</td>
<td>1829</td>
</tr>
<tr>
<td>IACR Election Voting Codes</td>
<td>Antoine</td>
<td>Bart</td>
<td>Christian</td>
<td>Helena</td>
<td>Tsutomu</td>
</tr>
<tr>
<td></td>
<td>1872</td>
<td>3627</td>
<td>9283</td>
<td>7562</td>
<td>5147</td>
</tr>
<tr>
<td>IACR Election Voting Codes</td>
<td>Antoine</td>
<td>Bart</td>
<td>Christian</td>
<td>Helena</td>
<td>Tsutomu</td>
</tr>
<tr>
<td></td>
<td>8163</td>
<td>2837</td>
<td>9287</td>
<td>6473</td>
<td>2517</td>
</tr>
<tr>
<td>IACR Election Voting Codes</td>
<td>Antoine</td>
<td>Bart</td>
<td>Christian</td>
<td>Helena</td>
<td>Tsutomu</td>
</tr>
<tr>
<td></td>
<td>7283</td>
<td>2938</td>
<td>9263</td>
<td>1717</td>
<td>2839</td>
</tr>
</tbody>
</table>

©Yvo Desmedt and Stelios Erotokritou
3. Voting using our solution

IACR Election Voting Codes
Antoine - 2613
Bart - 9384
Christian - 8173
Helena - 6734
Tsutomu - 4832

IACR Election Voting Codes
Antoine - 1827
Bart - 9394
Christian - 0238
Helena - 9187
Tsutomu - 1829

IACR Election Voting Codes
Antoine - 1872
Bart - 3627
Christian - 9283
Helena - 7562
Tsutomu - 5147

IACR Election Voting Codes
Antoine - 8163
Bart - 2837
Christian - 9287
Helena - 6473
Tsutomu - 2517

IACR Election Voting Codes
Antoine - 7283
Bart - 2938
Christian - 9263
Helena - 1717
Tsutomu - 2839

6734  9187  7562  6473  1717

over $\mathbb{Z}_{10}^4$

9453
3. Voting using our solution
So main **requirement** for the voter:
So main **requirement** for the voter:

is to be able to add numbers mod 10.
So main requirement for the voter:

is to be able to add numbers mod 10.

Cryptographers should be able to do this (otherwise they should not vote!).
4. **Avoiding Mod 10**

<table>
<thead>
<tr>
<th>List of Candidates</th>
<th>Do not vote without</th>
<th>Do not vote without</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antoine</td>
<td>Sheet 1 covering</td>
<td>Sheet 2 covering</td>
</tr>
<tr>
<td>Bart</td>
<td>this area</td>
<td>this area</td>
</tr>
<tr>
<td>Christian</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Helena</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tsutomu</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Avoiding Mod 10

Put this edge against "Candidate list edge"

Put this edge against Arrow Sheet 2

List of Candidates

- Antoine
- Bart
- Christian
- Helena
- Tsutomu

Do not vote without Sheet 2 covering this area
4. AVOIDING MOD 10

List of Candidates

- Antoine
- Bart
- Christian
- Helena
- Tsutomu

Put this edge against "Candidate list edge"

Put this edge against Arrow Sheet 2

Put against "Voting Bullets"

Put against "Voting Bullets"

Sheet 1

Sheet 2
4. **Avoiding Mod 10**

List of Candidates

- Antoine
- Bart
- Christian
- Helena
- Tsutomu
5. **Correctness and Details**

Using different secret sharing schemes and PSMT protocols, we can achieve 100% correctness against a $t$-limited adversary.

New *primitives* to achieve all this:

- (P)SMT with a Human, and
- Private Anonymous Communication.