Blinding ballot copying in Helios: from Condorcet to IACR

Yvo Desmedt Pyrros I.P. Chaidos

University College London, UK

August 16, 2011

What do Helios Ballots look like...

- Suppose: an election for 2 seats with 10 candidates. Helios represents a voter's choice as $v_i \in \{0, 1\}, i = 0..10$ with $\sum v_i \leq 2$. Then each v_i is encrypted with ElGamal.

What do Helios Ballots look like...

- Suppose: an election for 2 seats with 10 candidates. Helios represents a voter's choice as $v_i \in \{0, 1\}, i = 0..10$ with $\sum v_i \leq 2$. Then each v_i is encrypted with ElGamal.
- To keep the voter honest Helios forces the voter to prove that:
  - $(v_i = 0)$ **OR** $(v_i = 1)$ for every i.
  - $(\sum v_i = 0)$ **OR** $(\sum v_i = 1)$ **OR** $(\sum v_i = 2)$
- Helios uses disjunctive proofs for that, and the Fiat-Shamir trick to keep them non-interactive.

... and what will we do with them.

- We want to copy them.

... and what will we do with them.

- We want to copy them. Without being obvious.
- Bob trusts Alice, especially when it comes to politics. He decides to vote the same as she does.
- Alice wants to help Bob, but will not reveal her vote.
- Bob could copy her ballot *verbatim* (as by Courtier & Smyth), but that's detectable.

A better approach to copying.

Alice will help Bob make a blinded copy of her ballot. When they're done:

- Alice's vote will stay secret.
- Bob will be confident his ballot is equivalent to Alice's vote.
- Not even Alice will know whether Bob's submitted vote is a "copied" vote.

Copying in practice

- Alice gets the encryption randomness from her browser before casting her vote.
- Bob can blind the ElGamal ciphertext himself but needs help in creating the proofs. For this we use divertible proofs.
- Some difficulties we had to overcome:
  - Divertible proofs prove the original claim. Here, however, Bob wants to blind Alice's ciphertext.
  - Applying the Fiat-Shamir trick now (on Bob's ciphertext) will give new queries. To solve this, we let Alice and Bob interact.
  - There were no divertible proofs for disjunctive proofs before our work.

Why copy?

One of the problems of plurality is the "spoiler effect." This means, votes to unelectable candidates may imply that some unpopular candidate wins.
This was already observed by Condorcet, a French scientist.

- Copying votes can limit the impact of the spoiler effect, improving fairness for other parties. So, Helios may help fight the spoiler effect.
- We realize, that a voting block may imply their candidates be over-represented. Since Helios is malleable, this might be negative.

Example election: IACR 2011

- The French seem to know Condorcet's work well!

Example election: IACR 2011

- The French seem to know Condorcet's work well!
- Indeed, 4 out the 9 IACR BoD elected directors are French!

Example election: IACR 2011

- The French seem to know Condorcet's work well!
- Indeed, 4 out the 9 IACR BoD elected directors are French!
- For these concerned about this, we expect to have a vote copying server live before the 2011 IACR elections.

Future work

Can we replace Alice by a "distributed voter"?

In other words:

> *Essentially a group of respected members could hold their own primary election, and then allow others to copy the result. This gives an instant voting bloc!*