Prêt à Voter with Confirmation Codes

Peter Y A Ryan
Université du Luxembourg

Outline

- End-to-end verifiable voting.
- Outline of Prêt à Voter (polling station).
- Outline of Pretty Good Democracy (internet).
- Prêt à Voter with confirmation codes (polling station).
- Discussion.
- Conclusions.

The Design Philosophy

- Verify the election, not the system!
- Assurance should be based on transparency and auditability, not on claims of correctness of code.
- We transform the problem to one of verifying the correctness of a mathematical computation.
- As simple and understandable as possible.

Key Requirements

- Integrity/accuracy: the count accurately reflects votes cast.
- Ballot secrecy: the way a voter cast their vote should only be known to the voter.
- Coercion resistance: voters cannot prove to a third party how they voted, even if they cooperate with the coercer.
- Availability, accessibility etc. etc....

E2E verifiability

- Voters can confirm that their vote is accurately counted, without violating ballot secrecy.
- Voters are provided with an encrypted ballot.
- These ballots are posted to a secure web bulletin board. Voters can verify that their receipt is correctly posted.
- A (universally) verifiable, anonymising tabulation is performed on the receipts.

Prêt à Voter

- Uses familiar, paper ballot forms.
- The candidate list is independently randomised on each ballot form.
- Information defining the candidate order is encrypted on the ballot (or committed to the WBB).

Prêt à Voter Ballot

Obelix	
Idefix	
Abraracourix	
Asterix	
Panaromix	X
Falbala	
	7490012

The voting "ceremony"

- Voter enters the polling station, pre-registers and takes a ballot form at random, sealed in an envelope.
- Enters a booth, extracts the ballot, marks her choice and destroys the Left Hand portion.
- She leaves the booth with the receipt (the RH portion), and re-registers with an official.
- The receipt is scanned, digitally signed and franked and posted to the bulletin board.
- The voter heads off clutching her receipt.

Tabulation

- Voters can visit the WBB and confirm that their receipt appears correctly.
- A verifiable, anonymising mix or homomorphic tabulation is performed on the posted receipts.
- All steps are subject to (random) audits.

Remarks

- The receipt reveals nothing about the vote
- Voter experience simple and familiar.
- Votes are not directly encrypted, hence voters do not communicate their choice to a device. This neatly sidesteps many side-channel threats.
- Ballot auditing rather clean.
- Can be adapted to deal with ranked voting, AV etc.

Code Voting

- Due to Chaum (2001?).
- Voters get a code sheet with random voting and acknowledgement codes against each candidate.

Code sheet

	Vote code	Ack code
Odin	74522	89043
Thor	22916	60344
Hel	89321	6754
Forseti	29945	59684
		39772510

Voting

- Voter logs onto a server and provides the serial number of their code sheet along with the voting code for their candidate of choice.
- The server returns the corresponding ack code.
- The ack code serves to authenticate the server and confirm receipt of the correct code, but non end-to-end verifiability.

Pretty Good Democracy

- Code voting side-steps many insecurities of the internet but does not provide E2E verifiability.
- Knowledge of the codes is secret shared amongst a set of Trustees.
- For receipt-freeness we use a single ack code per code sheet.

PGD Code sheet

Candidate	Voting code
Asterix	4098
Idefix	3990
Obelix	6994
Panoramix	2569
Serial number	49950284926
Acknowledgement code	4482094

Pretty Good Democracy

- Voter logs on and provides the serial number and vote code for the candidate of choice.
- A threshold set of the trustees cooperate to validate the code, register it and reveal the ack code.
- Receipt of the correct ack code confirms that the correct vote code has been registered by a threshold set of the Trustees.

Security properties

- Tabulation much as in Prêt à Voter.
- Violation of secrecy of codes can violate accuracy (undetectably).
- Need to assume absence of colluding threshold set of trustees.
- Receipt free due to single ack code per code sheet.

Prêt à Voter with Confirmation Codes

- Combines ideas from Prêt à Voter and PGD: introduce a PGD style confirmation code into Prêt à Voter.
- The vote is registered by a threshold set of trustees at the time of casting and a code returned immediately.

Set-up

- Initially we need to set up a table each row of which corresponds to a ballot:
- $i, (\{CC_{i1}\}, \{\pi_i(1)\}), (\{CC_{i2}, \{\pi_i(2)\}),.....(\{CC_{in}\},\{\pi_i(n)\})$
- Each cell is a pair: an encryption of the code and of a candidate index.
- The candidate indices are permuted in each row.
- Audit for consistency.

Example

- 488213, ({4723}, {2}), ({9022},{1}), ({3726},{4}), ({2551},{3})

Candidate	Vote	Confirmation
Idefix		4723
Asterix		9022
Pamoramix		3726
Obelix		2551
		488213

Ballot forms

Candidate	Vote	Confirmation
Thor		
Odin	X	
Forseti		
Hermod		
		890032146

The ceremony

- In the booth, the voter marks her x and destroys the LH portion as usual, leaving the scratch strips intact.
- She then casts her vote, which is registered by the trustees and the confirmation code returned.
- She reveals the appropriate code on the ballot and checks that it matches.

Tabulation

- Once the election is over, the flagged, encrypted candidate indices are extracted and tabulated in the usual, verifiable fashion.

Discussion

- Voters don't now have to visit the WBB, but still have the option.
- Note: distinct codes for each candidate.
- Could we drop the receipt altogether?
- More convenient.
- More conducive of trust?

Distributed construction

- We have a nice distributed construction for the information posted to the WBB such that no single entities knows any codes.
- But the need to decrypt, print and distribute this information via the code sheets undermines this.

Distributed printing

- Is there an effective way of distributing the printing of the codes and candidates?
- Could use Alex et al's "How to print a secret" techniques.
- In the paper I suggest having a different Clerk for each digit of the codes, using scratch strips or invisible ink techniques.

Conclusions

- Potentially a interesting extension of Prêt à Voter.
- Arguably more secure, more convenient, most conducive of trust.
- Could we dispense with receipts, perhaps with a VEPAT (hash chained?) and/or use a Scantegrity approach?
- Link to VoteBox?

Thanks to

- Steve Schneider, David Chaum, Ron Rivest, James Heather, Vanessa Teague, Chris Culnane, Joson Zia,.....
- Fonds Nationale de Research (FNR) Luxembourg