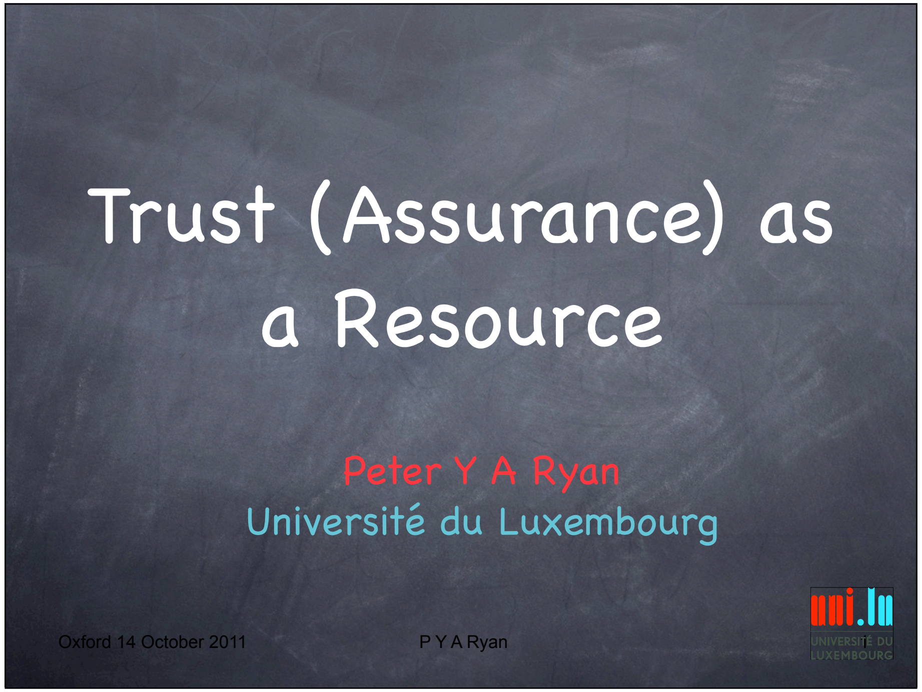


Trust (Assurance) as a Resource

Peter Y A Ryan
Université du Luxembourg

Outline

- Some ramblings
- Trust and trustworthiness
- End-to-end verifiable voting
- Outline of Prêt à Voter
- Design decisions
- Discussion/Conclusions (some more ramblings)

The spirit of the workshop!?

- So what is a “resource” anyway?
  - Something valuable.
  - Something with limited availability.
  - Something to be controlled.
  - ....

Other possible topics

- High grade entropy as a resource
- Attack resources as a measure of security? Security hierarchies?
- bootstrapping entropy, e.g. PAKEs.
- Spooky voting at a distance.
- Boardroom voting.

Trust

- Here, by “trust”, I just mean the user’s confidence in the security guarantees.
- Trust is a valuable resource: hard to acquire and easy to lose (ask Blackberry!)
- Sometimes we want trust to be non-transferable.
- May have to trade trust off against other resources.

Trust and trustworthiness

- It is not enough for a system to be trustworthy, it must also be trusted.
- And this is not just a question of uptake, lack of trust and understanding of security mechanisms can undermine security.
- True of all security critical systems, but especially true of voting systems.

Secure Voting

- Voting is the foundation of democracy.
- The outcome should not only be correct, but universally demonstrably correct.
- Everyone should be persuaded of the correctness of the outcome, especially the losers!

Trust in elections

- Traditionally voters are expected to trust in the honesty and competence of voting officials.
- With electronic voting machines they have to trust vendors, certifiers etc.
- Often officials and voters are expected to trust in code that is kept proprietary and secret.
- Sadly, they often do is seems.

and mistrust!

Verifiable Voting

- 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.
- The system should be as simple and understandable as possible.

Key Requirements

- Integrity/accuracy: the count accurately reflects (legitimate) 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....

End-to-end Verifiability

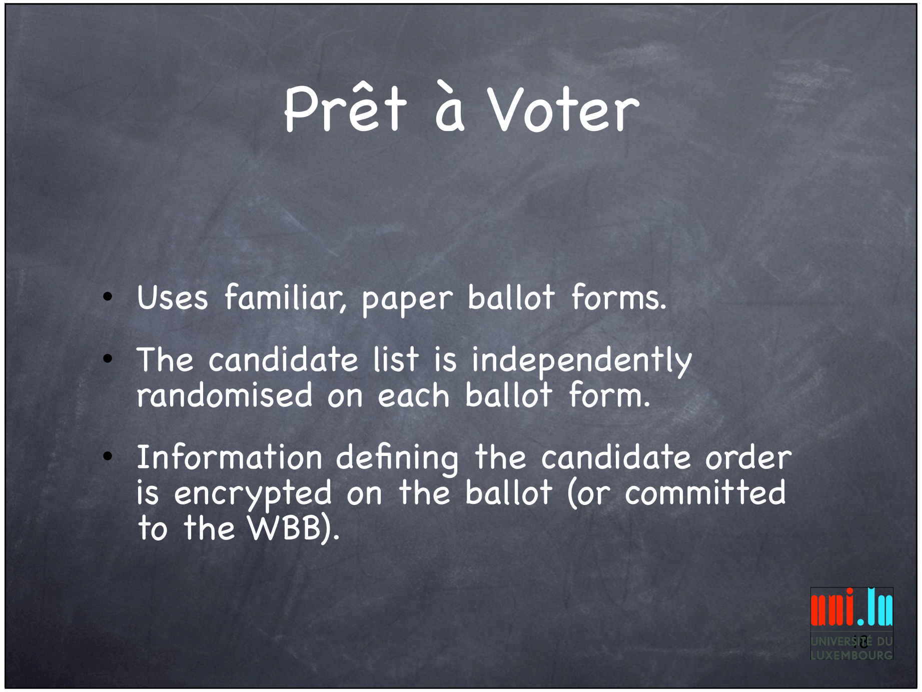
- Goal: voters can confirm that their vote is accurately counted, without violating ballot secrecy.
- Voters are provided with an encrypted ballot.
- The ballots are posted to a secure web bulletin board. Voters can verify that their receipt is correctly posted.
- A (universally) verifiable, anonymising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

Coercion resistance

- The really tricky bit is how to create the encryption of the vote in a such a way as the voter is confident that the encryption is correct but this conviction must not be transferable.
- This is the key difference with Secure Distributed Computation.

Coercion resistance

- We don't really want the randomisation to be provided just by the system or just by the voter (or voter's client).
- Typically have a some form of cut-and-choose or random auditing of ballots.
- Designated Verifier Proofs.
- Or MarkPledge.....

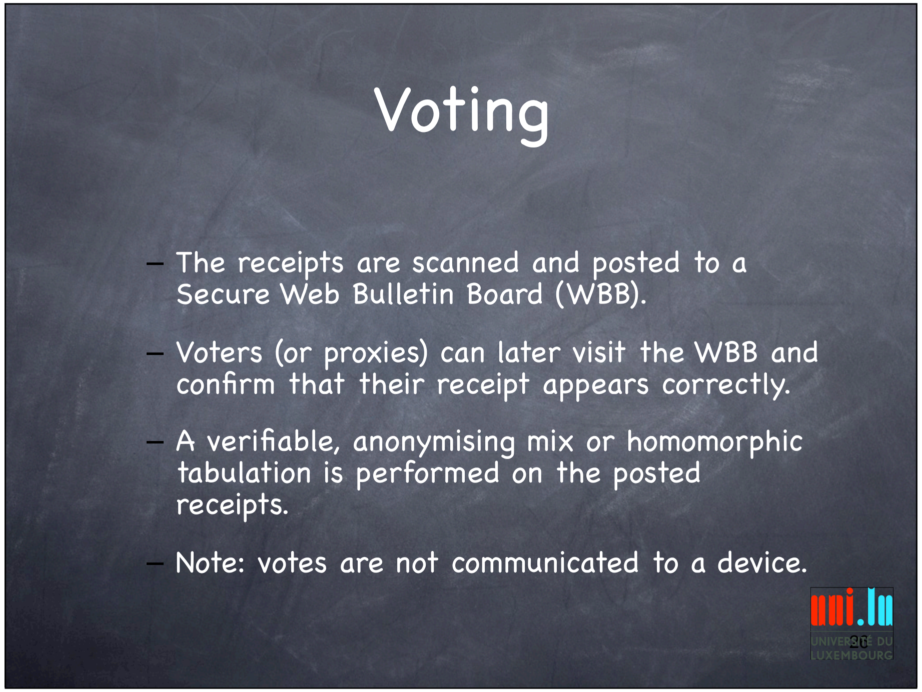


Prêt à Voter

- 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



Voting

- The receipts are scanned and posted to a Secure Web Bulletin Board (WBB).
- Voters (or proxies) can later visit the WBB and confirm that their receipt appears correctly.
- A verifiable, anonymising mix or homomorphic tabulation is performed on the posted receipts.
- Note: votes are not communicated to a device.

Verifiability

- We need to guarantee the following to demonstrate accuracy:
  - Votes are correctly encoded in the encrypted ballots.
  - All legitimately cast ballots are included in the tabulation, and only these.
  - All ballots input to the tabulation are correctly mixed and decrypted.

Auditing

- For the first we need to ensure that Ballots are well-formed-achieved via random audits.
- For the second voters can check their receipts on the WBB (maybe back-up with a VEPAT).
- For the mixing and decryption we can use standard random audits and Zero-Knowledge proofs etc. Essentially SDC at this stage.

Trustworthiness

- Prêt à Voter has been extensively analyzed and appears to be quite secure.
- some threats remain but counters exist, no absolute security!
- seems clear that it is at least as secure as "conventional" voting.
- But the arguments and mechanisms are subtle.
- So are people going to trust it?

Some known attacks

- Chain voting
- Randomisation
- Psychological
- Retention of candidate list
- Kleptographic
- Social engineering……

Paradoxes of Trust

- People have a charmingly inclination to trust totally untrustworthy systems.
- Introducing greater verifiability and auditability may in fact undermine trust.
- People prefer not to contemplate the possibility of something going wrong.

Design decisions

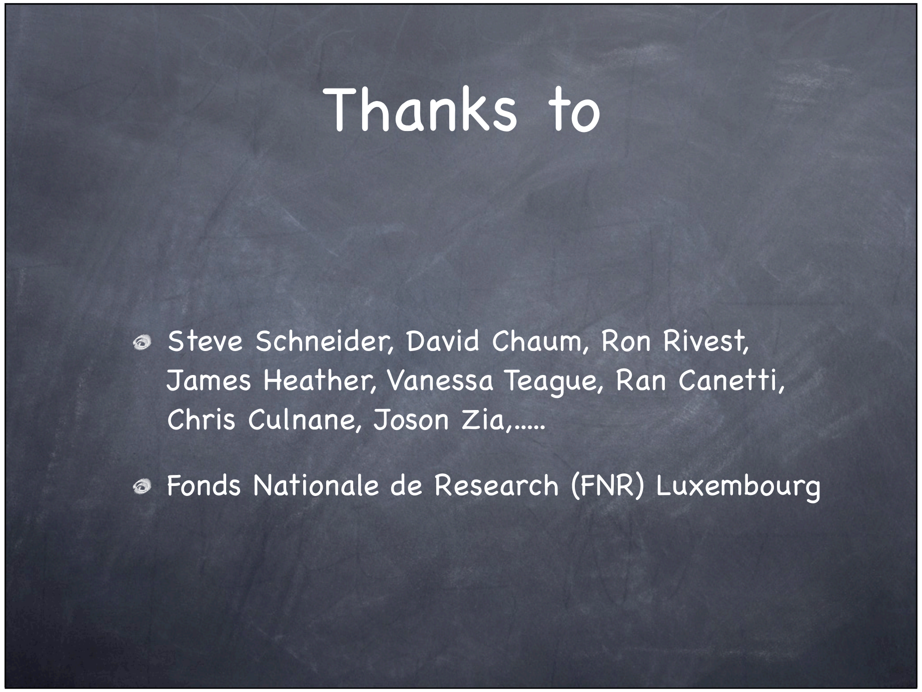
- Do we allow voters to perform ballot audits or just independent auditors?
- Pre-printed or print-on-demand ballots?
- Homomorphic vs mix tabulation?
- Everlasting privacy?
- Verified Encrypted Paper Audit Trail or confirmation codes in place of voter receipts?

Entropy as a resource

- High grade entropy is a scarce and valuable resource.
- needed for keys, for auditing.
- Not enough for it to be indistinguishable from random-needs to be impossible to manipulate.
- Verifiable Random Functions (Micali).

Q-voting

- Can quantum phenomena help enforce some of the assumptions of the classical scheme? e.g.:
  - Destructions of LHS of ballots.
  - Mutual exclusion of voting and auditing ballots.
  - Q-auditing (enforce destruction of "conjugate" info)
  - Revealing info to the voter.
  - Cast and recorded via entanglement.
  - Q-tabulation (cf homomorphic tabulation).



Thanks to

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