



# Spooky Voting at a Distance

Peter Y A Ryan  
University of Newcastle



# Outline

- The problem.
- Voter-verifiability.
- Outline of (Classical) Prêt à Voter.
- Vulnerabilities of the classical scheme.
- Exploiting quantum phenomena.
- Distributed generation of ballot forms.
- Remote, Coercion-resistant Prêt à Voter.



# “The Computer Ate my Vote”

- In last year’s US presidential election, ~30% of the electorate were using DRE, touch screen devices.
- Aside from the “thank you for your vote for Kerry, have a nice day” what assurance do voters have that their vote will be accurately counted?
- What do you do if the vote recording and counting process is called into question?



# Technical Requirements

- Key requirements:
  - Integrity/accuracy: count (sufficiently) accurately reflects votes cast.
  - Ballot secrecy: the way a voter cast their vote should only be known to the voter.
  - Anonymity: permuting the voters ids is indistinguishable.
  - Voter verifiability: the voter should be able to confirm that their vote is accurately included in the count and prove to a 3<sup>rd</sup> party if it is not (whilst not revealing their vote).
  - Coercion resistance: there should be no way for the voter to prove to a coercer which way they voted even if the voter cooperates.
  - Availability: all eligible voters should be able to cast their vote without let or hindrance throughout the voting period.
  - Transparency and minimal trust.
  - Ease of use, public trust, etc. etc.....



# Why quantum voting?

- A fun intellectual exercise!
- It does seem that quantum phenomena can provide some properties that are very useful here: information erasure, no cloning etc.
- Unconditional guarantees of privacy!?
- But also some downsides: difficult to maintain any form of quantum audit trail.
- And as for persuading the electorate to trust Uncle Heisenberg.....

# Assumptions

- For the purposes of the talk I will make many sweeping assumptions, e.g.,:
  - An accurate electoral register is maintained.
  - Mechanisms are in place to ensure that voters can be properly authenticated.
  - Mechanisms are in place to prevent double voting.
  - Existence of a secure Web Bulletin Board.
  - Etc.



# Voter-verifiability in a nutshell

- Voters cast an encrypted “receipt”.
- Copies of the receipts are posted to a secure web bulletin board. Voters can verify that their (encrypted) receipt is correctly posted.
- Tellers perform a robust anonymising mix and decryption on the batch of posted receipts, revealing the decrypted votes at the end. Results posted to a secure WBB.
- Checks are performed at each stage to detect any attempt to decouple the encryption on the receipt from the decryption performed by the tellers.



# Prêt à Voter “Classic”

- Supervised.
- Uses pre-prepared ballot forms that encode the vote in familiar form (e.g., ✕ against the chosen candidate).
- The candidate list is (independently) randomised for each ballot form.
- Information allowing the candidate list to be reconstructed is buried cryptographically in an “onion” on each ballot form.
- An excess number of forms are generated to allow for random auditing, before, during and after the election.



# Typical Ballot Sheet

Epicurus	
Democritus	
Aristotle	
Socrates	
Plato	
	\$rJ9*mn4R&8



# Voter marks their choice

Epicurus	
Democritus	x
Aristotle	
Socrates	
Plato	
	\$rJ9*mn4R&8



# Voter's Ballot Receipt

x
\$rJ9*mn4R&8

# Remarks

- Note that the receipt reveals nothing about the vote.
- The onion carries the crypto seed, encrypted with the teller's public keys, that (a subset of) the tellers use to reconstruct the permutation of the candidate list.
- Without all of these secret keys (or an appropriate subset) the candidate list cannot be reconstructed and hence the vote value cannot be recovered.
- Vote is not directly encrypted, rather the frame of reference, i.e., the candidate list, is randomised and information defining the frame is encrypted.
- Works for ranked, approval, STV etc.



# Anonymisation and tabulation

- Once the election has closed and all receipts have been posted to the WBB, a set of tellers perform a robust anonymising mix on the receipts:
  - Receipts go through a sequence of anonymising mixes followed by threshold decryption steps. Intermediate stages are also posted to the WBB for audit.
  - Final column of the WBB shows the votes in the clear.
  - Any link between the original receipts and the decrypted values will be lost.



# What can go wrong...

- For the accuracy requirement:
  - Ballot forms may be incorrectly constructed, leading to incorrect decryption of the vote.
  - Ballot receipts could be corrupted before they are entered in the tabulation process.
  - Tellers may perform the mix/decryption incorrectly.

# Auditing ballot forms

- The current version of Prêt à Voter uses pre-committed and pre-audited forms to detect and deter corrupt forms.
- In the quantum context, it may be more interesting to explore on-demand creation of ballot material along with a voter cut-and-choose protocol. This allows post auditing.
- Here, the voter could be provided with a commitment to two (or maybe more) ballot forms. One is chosen for casting, the others are retained (as part of the receipt) for audit.



# Recording and transmission

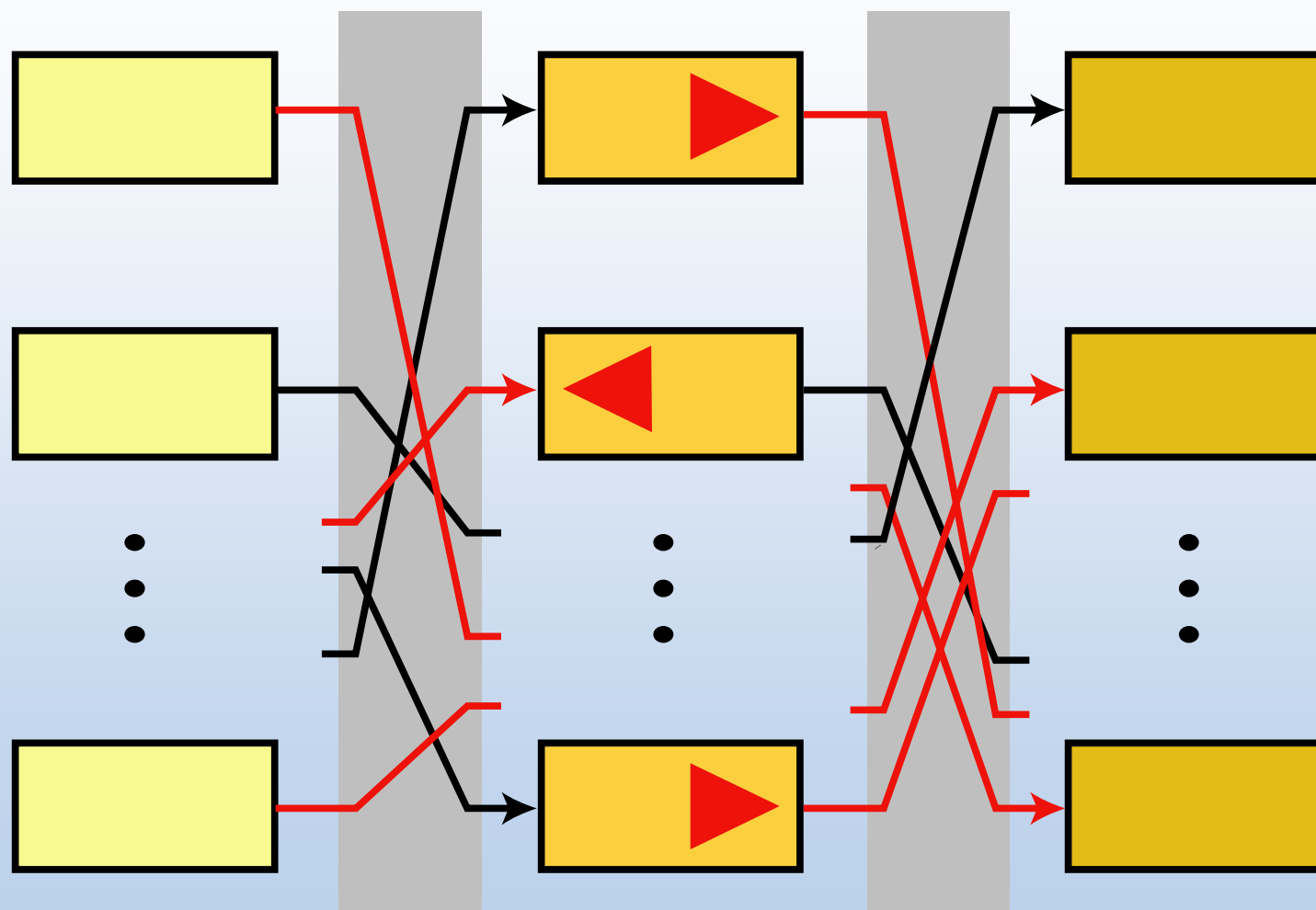
- To check that receipts are accurately recorded and input into the mix:
  - Voters can visit the WBB and check that their receipt appears correctly recorded.
  - Voter checks can be supplemented by independent audit authorities checking the WBB against the VVPAT style record of ballot receipts. Also helps counter ballot stuffing.
  - Voter signatures on receipts to counter ballot stuffing!?



# Auditing the Tellers

- All the intermediate mix steps are posted to the web site. Partial Random Checking can be used to detect any corruption in the mixes with high probability.
- The auditing of the WBB information has to be carefully controlled to avoid revealing any full links through the mix. This can be done by, for each object on the WBB, randomly selecting for audit either the incoming or outgoing link, but never both.
- ZK techniques can also be used with ElGamal type “onions”, see Neff.

# Random auditing of the tellers





# Advantages of Prêt à Voter

- Voter experience simple and familiar.
- No need for voters to have personal keys or computing devices.
- Votes are not directly encrypted, just the frame of reference in which votes encoded. Hence:
  - The vote recording device doesn't get to learn the vote.
  - No need for ZK proofs of correctly formed encrypted receipts. (but onus of proof shifts to the well-formedness of the ballot forms).
  - Avoids subliminal channels and social engineering attacks (see Karlof et al for Chaum and Neff schemes).
- Flexible.



# Classical vulnerabilities

- Need to trust “The Authority” (for secrecy).
- Need to protect ballot form information (chain of custody).
- Enforcing the destruction of LH strips.
- Need to constrain the WBB audits, i.e, reveal only L or R links.
- Separation of teller modes, i.e., ensure that each ballot form is processed only once (either cast and counted or audited).



# Protecting ballot forms

- Authority knowledge of ballot information/leakage of ballot form info.
- Mitigation.
- Classical:
  - Ballot forms in sealed envelopes.
  - Distributed generation of material.
  - on-demand generation of crypto material.
  - Alternative, mixed sources of entropy.
- Quantum:
  - Spooky voting at a distance, e.g., ballot forms composed of entangled q-bits?



# Enforcing destruction of LHS

- Mitigation.
  - Classical:
    - Procedural.
    - Mechanical.
    - Decoy strips.
  - Quantum:
    - Quantum mechanical: collapse of wave functions. Voter marking ballot erases candidate list information.



# Confusion of teller modes

- Mitigation.
- Classical:
  - Procedural: ballot checking and vote casting under official supervision.
  - Note: vote selection could be done in isolation whilst ballot receipt could be cast in presence of an official, French/Greek style.
  - Mechanical: forms invalidated once used, e.g., scratch cards.
- Quantum:
  - Quantum mechanical-no cloning theorem!?



# Remote, coercion-resistant Prêt à Voter

- The scheme described so far is designed for a supervised context: vote casting in enforced isolation in a booth at a polling station.
- Recent work (joint with Michael Clarkson and Andrew Myers, Cornell) has explored adapting Prêt à Voter to the remote context in which isolation during the vote casting cannot be assumed.
- The challenge now is to prevent coercion of the voters.

# Coercion resistance

- Definition (informal): the voter should have no way to prove to the coercer which way they voted, even if they are prepared to cooperate with the coercer.
- Coercer can observe virtually all steps of the protocol, the WBB and even demand the voter to reveal keys, dictate any randomness or choices available to the voter, but the voter should be able to lie undetected.
- Need to postulate at least a window in which the voter can interact with the voting system unobserved.
- Need to assume availability of anonymous channels.
- Need to assume that the voter's private (authentication) key remains secret during registration phase?

# Remote Prêt à Voter

- Naïve approach: casting vote by just submitting an onion and index value. Open to coercion.
- More sophisticated, coercion resistant version (à la Juels et al and Clarkson, Myers): supply voters with a capability, onion and encrypted candidate list.
- Capabilities constructed like onions but with “valid” flag and serial number at the centre.
- Casting: voter sends off a triple:  
(index, onion, capability)
- Coerced voter can corrupt their capability. Invalidity only revealed after the anonymising mixes.
- Designated verifier proof (DVP) to convince the voter, and only the voter, of the validity of their capability.

# Capabilities

- Construction similar to ElGamal “onions”, but with registrar signature on a “valid” string along with a nonce:

$$\varepsilon_x(\text{Sig}_{\text{Reg}}(\text{valid}, \text{nonce}))$$

- Delivered to the voters along with a non-interactive, designated verifier proof (DVP) of validity.
- Designed to go through the mix and be decrypted along with the associated ballot.
- Need to ensure that each voter gets exactly one valid capability.



# Capabilities

- Ideally we would like to construct these capabilities in such a way that no single entity knows their values or the association with voter ids.
- We would also like to have the voters participate in their construction to counter official ballot stuffing, whilst preserving anonymity.
- At the moment it is not clear how to achieve this without some level of trust in a (distributed) registrar and some secure (e.g., anonymous) channel.
- Need to assume voters have private/public key pairs.

# Quantum opportunities

- Enforcing audit constraints:
  - There are several places in the classical scheme where we want to enforce the revealing of only one of two complementary pieces of information:
    - The voter's choice of ballot form: the seed for the form used for casting the vote must be kept secret, the seed for the form for audit should be revealed for audit.
    - Similarly with the random auditing of the mix information on the WBB: either the incoming or the outgoing link information should be revealed but never both.
  - If these paired pieces of information could be coded up as conjugate variables, then Heisenberg uncertainty could enforce these requirements.



# Information erasure

- Erasure of information:
- It is essential for coercion resistance that certain items be erased after use, in particular the candidate list once the voter has made their selection on the ballot form.
- Could we exploit quantum phenomena to ensure that the act of “marking” the ballot form automatically erases the candidate list information?

# Quantum entropy

- On-demand creation or revealing of crypto information:
  - To avoid problems of chain of custody and chain voting etc, it would be desirable to ensure that crypto information is revealed only at the last possible moment, i.e., when the voter is about to cast their vote. Better still, if this information doesn't exist until the last possible moment. This suggests using quantum states as the source of crypto material. Crypto seeds would then only come into existence at the moment that the classical measurements on the qbits are made.
  - The real challenge here is to find a way to check that quantum ballot forms are well formed, e.g., that pairs of qbits are appropriately entangled.



# Quantum tabulation

- Classical schemes tend to use either anonymising mixes (as described here) or exploit homomorphic crypto primitives to perform anonymous tabulation of the votes.
- Could quantum interference phenomena be used to tabulate q-votes?
- Can this be done robustly, i.e., guaranteeing the accuracy of the result with minimal trust in the devices and processes performing the tabulation?



# Vote teleportation

- Spooky voting at a distance.
- One can envisage providing voters with q-ballot forms comprising q-bits entangled with q-bits held by a registrar.
- Vote casting could then be performed by suitably chosen measurement on the voter's q-bits.
- Tabulation might then be performed by a quantum interference process.
- Quite appealing but difficult to see how to do this in a robust way.

# Quantum anonymous channels

- In order to achieve coercion resistance it is often necessary to assume the existence of anonymous (and sometimes also untappable) channels.
- Classically this can be very difficult. Quantum techniques, e.g., using entangled q-bits, may provide a nice way of doing this.

# Conclusions/questions

- Exploiting quantum phenomena in voting schemes may allow us to avoid some of the vulnerabilities of the classical schemes.
- There appear to be several places in the classical schemes that are crying out for quantum phenomena to enforce certain properties.
- It seems quite feasible to come up with plausible quantum voting schemes as long as significant trust is placed in agents, for example, preparing entangled qbits. Coming up with schemes that achieve the goals without needing any such trust assumptions (in the spirit of the classical schemes) is very challenging.
- Perhaps we just have to trade one set of assumptions for another?
- Can quantum phenomena help us get around some of the classical impossibility results? But how does this play against the quantum impossibility results, e.g., bit commitment, coin flipping.

# Future work

- Beyond the current scheme:
  - Finalise (classical) remote, coercion resistant version.
  - Establish minimal assumptions.
  - Explore alternative sources of entropy: Voters, optical fibres in the paper, quantum...?
  - Protocols for distributed and on-demand generation and checking of ballot forms, e.g., authenticated onion and capability establishment.
  - Alternative robust mixes, e.g., ZK shuffle proofs.
  - Quantum variants.



# Acknowledgements

- With thanks to:
  - Ran Canetti
  - David Chaum
  - Michael Clarkson
  - James Heather
  - Michael Jackson
  - Marcus Jakobsson
  - Andrew Myers
  - Thea Peacock
  - Brian Randell
  - Ron Rivest
  - Steve Schneider
  - Nigel Smart
  - .....

# References

- David Chaum, Secret-Ballot receipts: True Voter-Verifiable Elections, IEEE Security and Privacy Journal, 2(1): 38-47, Jan/Feb 2004.
- J W Bryans & P Y A Ryan “A Dependability Analysis of the Chaum Voting Scheme”, Newcastle Tech Report CS-TR-809, 2003.
- J W Bryans & P Y A Ryan, “Security and Trust in a Voter-verifiable Election Scheme”, FAST 2003.
- P Y A Ryan & J W Bryans “A Simplified Version of the Chaum Voting Scheme”, Newcastle TR 2004
- P Y A Ryan, Towards a Dependability Case for the Chaum Voting Scheme, DIMACS June 2004.
- P Y A Ryan, “E-voting”, presentation to the Caltech/MIT workshop on voting technology, MIT Boston 1-2 October 2004.
- P Y A Ryan, “A Variant of the Chaum Voter-verifiable Election scheme”, WITS, 10-11 January 2005 Long Beach Ca.
- D Chaum, P Y A Ryan, S A Schneider, “A Practical, Voter-Verifiable Election Scheme”, Newcastle TR 880 December 2004, Proceedings ESORICS 2005, LNCS 3679.
- B Randell, P Y A Ryan, “Trust and Voting Technology”, NCL CS Tech Report 911, June 2005, to appear IEEE Security and Privacy Magazine.
- P Y A Ryan, T Peacock, “Prêt à Voter, A Systems Perspective”, NCL CS Tech Report 929, September 2005, submitted to IEEE Computer Security Foundations Workshop 2006.
- Clarkson and Myers, “Coercion-resistant Remote Voting using Decryption Mixes”, at FEE 2005.  
<http://www.win.tue.nl/~berry/fee2005/>