University of Fribourg

Bern University of Applied Sciences

Coercion-Resistant Hybrid Voting Systems

Oliver Spycher, Rolf Haenni, Eric Dubuis

July 24th, 2010

Outline

Outline

Internet E-Voting Systems in Practice

- Literature on e-voting protocols usually assumes 1 channel for voting.
- This assumption seems unrealistic.

Internet E-Voting Systems in Practice

- Literature on e-voting protocols usually assumes 1 channel for voting.
- This assumption seems unrealistic.
  - → Governments need to avoid the risk of introducing new technology in a big bang.

Internet E-Voting Systems in Practice

- Literature on e-voting protocols usually assumes 1 channel for voting.
- This assumption seems unrealistic.
  - → Governments need to avoid the risk of introducing new technology in a big bang.
  - → Not all voters have access to the internet.

Internet E-Voting Systems in Practice

- Literature on e-voting protocols usually assumes 1 channel for voting.
- This assumption seems unrealistic.
  - → Governments need to avoid the risk of introducing new technology in a big bang.
  - → Not all voters have access to the internet.
  - → Not all voters are able to handle a computer.

Internet E-Voting Systems in Practice

- Literature on e-voting protocols usually assumes 1 channel for voting.
- This assumption seems unrealistic.
  - → Governments need to avoid the risk of introducing new technology in a big bang.
  - → Not all voters have access to the internet.
  - → Not all voters are able to handle a computer.
  - → Voters do not neccessarily like e-voting systems.
- As a matter of fact, the traditional, paper-based channel is preserved as an alternative channel.
  - → *Example*: Swiss Cantons of Geneva, Zurich and Neuchatel.
  - → *Example*: Estonia.

Integrate Traditional and Electronic Voting

- It is not possible to run both the traditional and the electronic channel independently.

Minimal requirement for integrated voting systems

- Ensure that at most one vote is cast per voter.

Note, that the integrated system is only as secure as the weaker voting channel.

What are the features of a good voting channel?

A Good Voting Channel (some aspects)

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)

A Good Voting Channel (some aspects)

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)
- Privacy (Nobody should be able to find out how any of the voters voted.)

A Good Voting Channel (some aspects)

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)
- Privacy (Nobody should be able to find out how any of the voters voted.)
- Uniqueness and Eligibility (Only eligible voters are able to cast a vote, one at most.)

A Good Voting Channel (some aspects)

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)
- Privacy (Nobody should be able to find out how any of the voters voted.)
- Uniqueness and Eligibility (Only eligible voters are able to cast a vote, one at most.)
- Universal Verifiability (Everybody is able to verify the accuracy of the tally.)

A Good Voting Channel (some aspects)

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)
- Privacy (Nobody should be able to find out how any of the voters voted.)
- Uniqueness and Eligibility (Only eligible voters are able to cast a vote, one at most.)
- Universal Verifiability (Everybody is able to verify the accuracy of the tally.)
- Individual Verifiability (Each voter can verify that his vote is counted.)

A Good Voting Channel (some aspects)

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)
- Privacy (Nobody should be able to find out how any of the voters voted.)
- Uniqueness and Eligibility (Only eligible voters are able to cast a vote, one at most.)
- Universal Verifiability (Everybody is able to verify the accuracy of the tally.)
- Individual Verifiability (Each voter can verify that his vote is counted.)
- Coercion-Resistance (Voter coercion and vote buying are infeasible.)

A Good Voting Channel

- Accuracy (The result of the tally reflects the collection of cast votes correctly.)
- Privacy (Nobody should be able to find out how any of the voters voted.)
- Uniqueness and Eligibilty (Only eligible voters are able to cast a vote, one at most.)
- Universal Verifiability (Everybody is able to verify the accuracy of the tally.)
- Individual Verifiability (Each voter can verify that his vote is counted.)
- Coercion-Resistance (Voter coercion and vote buying are infeasible.)

These requirements are very hard to meet simultaneously in the e-voting channel of an integrated system.

Individual Verifiability vs. Coercion-Resistance

- *Individual Verifiability* grounds on an electronic bulletin board.
- Unfortunatelly, the voter can generally reproduce the encryption procedure to demonstrate to an adversary (voter coercer or vote buyer) how he voted.
- The information a voter needs to do so is called a voter's *receipt*.
- *Receipt-freeness* of the electronic voting channel is thus a precondition to *coercion-resistance* of the *integrated system*.

Individual Verifiability vs. Coercion-Resistance

- *Individual Verifiability* grounds on an electronic bulletin board.
- Unfortunatelly, the voter can generally reproduce the encryption procedure to demonstrate to an adversary (voter coercer or vote buyer) how he voted.
- The information a voter needs to do so is called a voter's *receipt*.
- *Receipt-freeness* of the electronic voting channel is thus a precondition to *coercion-resistance* of the *integrated system*.
- Unfortunatelly, *receipt-freeness* is very difficult to achieve with e-voting systems over the internet.
- We propose *hybrid systems* to solve the dilemma of simultaneously providing *Individual Verifiability* and *Coercion-Resistance* in *integrated systems*.

Outline

Coercion-Resistance in Hybrid Voting Systems

- Voters can revoke and replace their electronic vote at the polling station.
- It is infeasible for an adversary (voter coercer or vote buyer) to verify whether voters have revoked their vote.
- Thus, a voter's receipt for the electronic vote published on the bulletin board has no value for adversaries.

Coercion-Resistance in Hybrid Voting Systems

- Voters can revoke and replace their electronic vote at the polling station.
- It is infeasible for an adversary (voter coercer or vote buyer) to verify whether voters have revoked their vote.
- Thus, a voter's receipt for the electronic vote published on the bulletin board has no value for adversaries.

Benefits

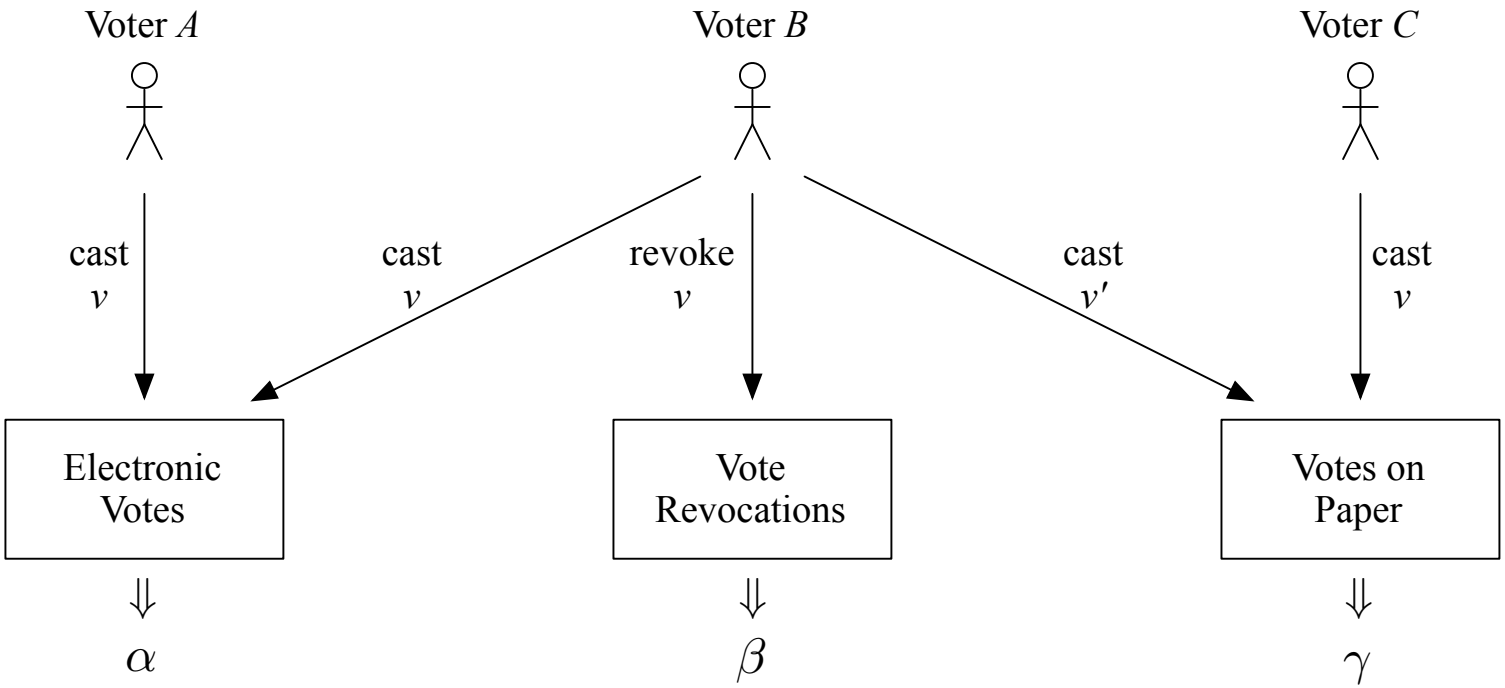
- *Individual Protection*: Voters that were put under pressure can still express their real political opinion.
- *Universal Protection*: Attacks will not influence the outcome of the vote, since adversaries must assume that voters revoke.

  Thus, launching an attack in the first place seems unattractive.

Revoking Votes in Hybrid Voting Systems

We need an additional ballot-box (β) to contain the revoked votes.

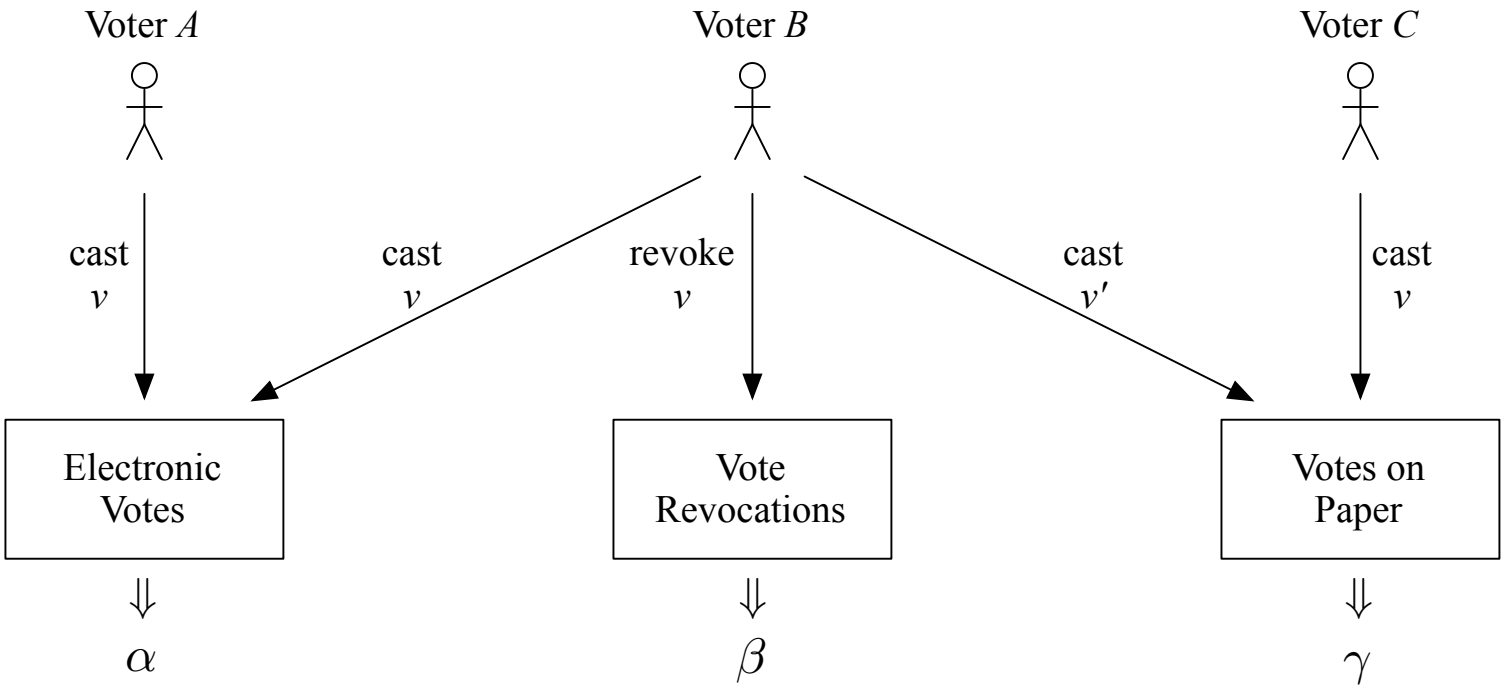
- *Remember*: The ballot-box of the electronic voting channel is public.



Revoking Votes in Hybrid Voting Systems

We need an additional ballot-box (β) to contain the revoked votes.

- *Remember*: The ballot-box of the electronic voting channel is public.



$$\mathit{FinalTally} = \mathit{Tally}(\alpha) - \mathit{Tally}(\beta) + \mathit{Tally}(\gamma)$$

Outline

Requirements on Hybrid Voting Systems

1. The traditional channel opens after the electronic channel closes.

Requirements on Hybrid Voting Systems

1. The traditional channel opens after the electronic channel closes.
2. An anonymous ballot box (the β-box) that contains the revoked votes.

Requirements on Hybrid Voting Systems

1. The traditional channel opens after the electronic channel closes.
2. An anonymous ballot box (the β-box) that contains the revoked votes.
3. Requirements on the electronic channel.

Requirements on Hybrid Voting Systems

1. The traditional channel opens after the electronic channel closes.
2. An anonymous ballot box (the β-box) that contains the revoked votes.
3. Requirements on the electronic channel.
4. Requirements on the traditional voting channel.

Requirements on Hybrid Voting Systems

1. The traditional channel opens after the electronic channel closes.
2. An anonymous ballot box (the β-box) that contains the revoked votes.
3. Requirements on the electronic channel.
4. Requirements on the traditional voting channel.
5. A procedure that defines the revocation process in the polling station.

Requirements on Electronic Channel

1. **Proof of Eligibility**: Voters at the polling station must be able to prove that their electronic vote has not been cast.
2. **Proof of Ownership**: Voters at the polling station who own an electronic vote must be able to identify its encryption on the bulletin board and prove that they have done so truthfully.

Requirements on Electronic Channel

1. **Proof of Eligibility**: Voters at the polling station must be able to prove that their electronic vote has not been cast.
2. **Proof of Ownership**: Voters at the polling station who own an electronic vote must be able to identify its encryption on the bulletin board and prove that they have done so truthfully. $\longrightarrow$*vote identifier*.

Requirements on Traditional Channel

To allow the definition of an appropriate revocation procedure, the traditional voting channel must comply with the following requirements.

1. The traditional voting infrastructure consists of a polling station.

Requirements on Traditional Channel

To allow the definition of an appropriate revocation procedure, the traditional voting channel must comply with the following requirements.

1. The traditional voting infrastructure consists of a polling station.
2. The traditional voting procedure at the polling station (checking the identity of voters, opening the ballot box, counting the votes, etc.) is sufficiently secure.

Outline

Revocation Procedure 1

- Voters own a receipt for their electronic vote.
- The β-box is defined as a traditional ballot box.

Definition

1. The voter uses the receipt to locate the encrypted electronic vote in the α-box and to reveal it to the voting officials.
2. The voting officials prepare a revocation paper ballot containing the same vote and hand it over to the voter.
3. The voting officials verify that the voter drops the revocation paper ballot into the β-box.
4. The voter is granted access to the γ-box to cast the final paper vote.

Revocation Procedure 1 - Discussion

- By defining the β-box as a traditional ballot box, the procedure appeals to e-voting doubters.

Revocation Procedure 1 - Discussion

- By defining the β-box as a traditional ballot box, the procedure appeals to e-voting doubters.
- The voting officials could notify the adversary that voters have revoked their vote. However, they cannot prove it.

Revocation Procedure 1 - Discussion

- By defining the β-box as a traditional ballot box, the procedure appeals to e-voting doubters.
- The voting officials could notify the adversary that voters have revoked their vote. However, they cannot prove it.
- Additional measures could be applied to prevent the voting authorities from knowing the vote to be revoked.

Revocation Procedure 2 - Prerequisites

- The second revocation procedure does not require voters to own a receipt for their electronic vote. It is sufficient to own a vote identifier.

Revocation Procedure 2 - Prerequisites

- The second revocation procedure does not require voters to own a receipt for their electronic vote. It is sufficient to own a vote identifier.
- The β-box is defined as an anonymous public bulletin board.

Revocation Procedure 2 - Prerequisites

- The second revocation procedure does not require voters to own a receipt for their electronic vote. It is sufficient to own a vote identifier.
- The β-box is defined as an anonymous public bulletin board.
- The encryption of the electronic votes in the α-box need to allow re-encryption. (ElGamal cryptosystem would comply.)

Revocation Procedure 2 - Prerequisites

- The second revocation procedure does not require voters to own a receipt for their electronic vote. It is sufficient to own a vote identifier.
- The β-box is defined as an anonymous public bulletin board.
- The encryption of the electronic votes in the α-box need to allow re-encryption. (ElGamal cryptosystem would comply.)
- The re-encryption function needs to allow the construction of a non-transferable zero-knowledge proof of correct re-encryption. (Σ-protocols would comply together with ElGamal cryptosystem.)

Revocation Procedure 2

Definition

1. The voter generates a re-encryption of the encrypted vote in the α-box.
2. The voter generates a non-transferable proof of correct re-encryption, designated to the officials at the polling station.

Revocation Procedure 2

Definition

1. The voter generates a re-encryption of the encrypted vote in the α-box.
2. The voter generates a non-transferable proof of correct re-encryption, designated to the officials at the polling station.
3. The voter approaches the voting officials and uses the vote identifier to identify the encrypted vote in the α-box.
4. The voter hands the re-encryption and the corresponding non-transferable proof over to the voting officials.
5. If the delivered proof is valid, the voting officials post the re-encrypted vote to the β-box.
6. The voter is granted access to the γ-box to cast the final paper vote.

Revocation Procedure 2 - Discussion

- The voter does not have to reveal the plaintext of the encrypted vote in the α-box at any time.

Revocation Procedure 2 - Discussion

- The voter does not have to reveal the plaintext of the encrypted vote in the α-box at any time.
- Although the β-box is defined as a public bulletin board, an adversary cannot tell which voters have revoked.

Revocation Procedure 2 - Discussion

- The voter does not have to reveal the plaintext of the encrypted vote in the α-box at any time.
- Although the β-box is defined as a public bulletin board, an adversary cannot tell which voters have revoked.
- Again, the voting officials could notify the adversary that voters have revoked their vote. However, they cannot prove it, since the proof of correct re-encryption is non-transferable.

Outline

Conclusion

- Traditional voting systems will be used along with internet e-voting systems.

Conclusion

- Traditional voting systems will be used along with internet e-voting systems.
- It is hard to make the electronic channel of an integrated system coercion-resistant.

Conclusion

- Traditional voting systems will be used along with internet e-voting systems.
- It is hard to make the electronic channel of an integrated system coercion-resistant.
- Yet to achieve coercion-resistance of the integrated system, we allow voters to revoke and replace their vote in a secure manner. Such an integrated system we call a *hybrid system*.

Conclusion

- Traditional voting systems will be used along with internet e-voting systems.
- It is hard to make the electronic channel of an integrated system coercion-resistant.
- Yet to achieve coercion-resistance of the integrated system, we allow voters to revoke and replace their vote in a secure manner. Such an integrated system we call a *hybrid system*.
- Thus, the electronic channel alone does not require any measures to ban receipts. Instead, it can offer *individual verifiability* to voters unconditionally.

Thank You

Questions / Remarks

Find
"*A Novel Protocol to Allow Revocation of Votes in a Hybrid Voting System*" by Oliver Spycher / Prof. Rolf Haenni in

www.e-voting.ti.bfh.ch