University of Fribourg

Bern University of Applied Sciences

A Novel Protocol to Allow Revocation of Votes in a Hybrid Voting System

Oliver Spycher, Rolf Haenni

August 3rd, 2010

Outline

Motivation - Integrated Voting Systems

Hybrid Voting Systems

The Protocol

Conclusion

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 (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 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

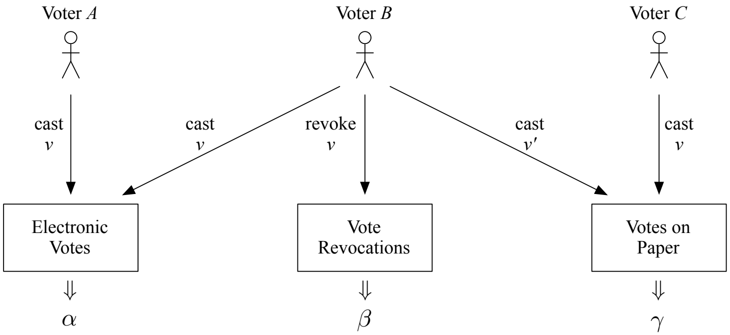
- *Individual Protection*: Voters that were put under pressure can still express their real political opinion.
- *Universal Protection*: Attacks will not influence the outcome of the vote, since adversaries must assume that voters revoke.

  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.

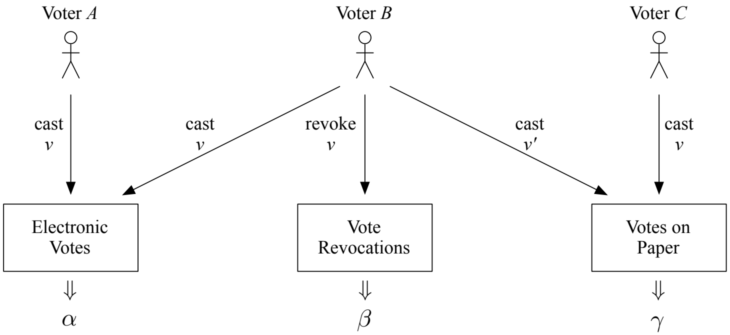
- *Remember*: The ballot-box of the electronic voting channel is public.



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.



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

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. $\rightarrow$*vote identifier*.

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.
   $\rightarrow$*vote identifier*.
   $\rightarrow$*receipt* $\Rightarrow$ *vote identifier*.

Outline

Secret Credential and Public Credential

Voters are assigned their

- *secret credential* $s \mod q$
- *public credential* $S = g^s \mod p \qquad (p = 2q + 1)$

Secret Credential and Public Credential

Voters are assigned their

- *secret credential* $s \mod q$
- *public credential* $S = g^s \mod p \qquad (p = 2q + 1)$

Voters can prove that they know the secret credential that matches their *public credential*. (Zero-Knowledge Proof)

Secret Credential and Public Credential

Voters are assigned their

- *secret credential* $s \mod q$
- *public credential* $S = g^s \mod p \qquad (p = 2q + 1)$

Voters can prove that they know the secret credential that matches their *public credential*. (Zero-Knowledge Proof)

Distribution

Voting Officials jointly create and publish the *public credential* and secretly reveal their share of the secret credential to the Voter.

Secret Credential and Public Credential

Voters are assigned their

- *secret credential* $s \mod q$
- *public credential* $S = g^s \mod p$ $\qquad (p = 2q + 1)$

Voters can prove that they know the secret credential that matches their *public credential*. (Zero-Knowledge Proof)

Distribution

Voting Officials jointly create and publish the *public credential* and secretly reveal their share of the secret credential to the Voter.
$\rightarrow$ R. Gennaro, Jarecki, Krawczyk, T. Rabin: Eurocrypt 1999

Secret Credential and Public Credential

Voters are assigned their

- *secret credential* $s \mod q$
- *public credential* $S = g^s \mod p \qquad (p = 2q + 1)$

Voters can prove that they know the secret credential that matches their *public credential*. (Zero-Knowledge Proof)

Distribution

Voting Officials jointly create and publish the *public credential* and secretly reveal their share of the secret credential to the Voter.
$\rightarrow$ R. Gennaro, Jarecki, Krawczyk, T. Rabin: Eurocrypt 1999

This only has to be done once.

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll			
Marianne			
Hein			
Marijke			

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**		
Marianne	$S_1 = g^{s_1}$		
Hein	$S_2 = g^{s_2}$		
Marijke	$S_3 = g^{s_3}$		

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**	**E(vote)**$= (c, d)$	
Marianne	$S_1 = g^{s_1}$	$(h^{s_1}, vote_1 \cdot e^{s_1})$	
Hein	$S_2 = g^{s_2}$	$(h^{s_2}, vote_2 \cdot e^{s_2})$	
Marijke	$S_3 = g^{s_3}$	$(h^{s_3}, vote_3 \cdot e^{s_3})$	

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**	**E(vote)**$= (c, d)$	**Proof** $ZKP[]$
Marianne	$S_1 = g^{s_1}$	$(h^{s_1}, vote_1 \cdot e^{s_1})$	$(s_1) : S_1 = g^{s_1} \wedge c = h^{s_1}$
Hein	$S_2 = g^{s_2}$	$(h^{s_2}, vote_2 \cdot e^{s_2})$	$(s_2) : S_2 = g^{s_2} \wedge c = h^{s_2}$
Marijke	$S_3 = g^{s_3}$	$(h^{s_3}, vote_3 \cdot e^{s_3})$	$(s_3) : S_3 = g^{s_3} \wedge c = h^{s_3}$

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**	**E(vote)**$= (c, d)$	**Proof** $ZKP[]$
Marianne	$S_1 = g^{s_1}$	$(h^{s_1}, vote_1 \cdot e^{s_1})$	$(s_1) : S_1 = g^{s_1} \wedge c = h^{s_1}$
Hein	$S_2 = g^{s_2}$	$(h^{s_2}, vote_2 \cdot e^{s_2})$	$(s_2) : S_2 = g^{s_2} \wedge c = h^{s_2}$
Marijke	$S_3 = g^{s_3}$	$(h^{s_3}, vote_3 \cdot e^{s_3})$	$(s_3) : S_3 = g^{s_3} \wedge c = h^{s_3}$

Proof of Eligibility: Simple

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**	**E(vote)**$= (c, d)$	**Proof** $ZKP[]$
Marianne	$S_1 = g^{s_1}$	$(h^{s_1}, vote_1 \cdot e^{s_1})$	$(s_1) : S_1 = g^{s_1} \wedge c = h^{s_1}$
Hein	$S_2 = g^{s_2}$	$(h^{s_2}, vote_2 \cdot e^{s_2})$	$(s_2) : S_2 = g^{s_2} \wedge c = h^{s_2}$
Marijke	$S_3 = g^{s_3}$	$(h^{s_3}, vote_3 \cdot e^{s_3})$	$(s_3) : S_3 = g^{s_3} \wedge c = h^{s_3}$

Proof of Eligibility: Simple
Proof of Ownership: Simple

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**	**E(vote)**$= (c, d)$	**Proof** $ZKP[]$
Marianne	$S_1 = g^{s_1}$	$(h^{s_1}, vote_1 \cdot e^{s_1})$	$(s_1) : S_1 = g^{s_1} \wedge c = h^{s_1}$
Hein	$S_2 = g^{s_2}$	$(h^{s_2}, vote_2 \cdot e^{s_2})$	$(s_2) : S_2 = g^{s_2} \wedge c = h^{s_2}$
Marijke	$S_3 = g^{s_3}$	$(h^{s_3}, vote_3 \cdot e^{s_3})$	$(s_3) : S_3 = g^{s_3} \wedge c = h^{s_3}$

Proof of Eligibility: Simple
Proof of Ownership: Simple
Use s_i **to disclose vote for revocation**:

1. Marijke computes $z = e^{s_3}$ and proves its correctness with ZKP.
2. Authorities compute $vote = \frac{d}{z}$.

A First Naive Approach wihout Privacy

This is the public bulletin board.

Voter Roll	**Public**	**E(vote)**$= (c, d)$	**Proof** $ZKP[]$
Marianne	$S_1 = g^{s_1}$	$(h^{s_1}, vote_1 \cdot e^{s_1})$	$(s_1) : S_1 = g^{s_1} \wedge c = h^{s_1}$
Hein	$S_2 = g^{s_2}$	$(h^{s_2}, vote_2 \cdot e^{s_2})$	$(s_2) : S_2 = g^{s_2} \wedge c = h^{s_2}$
Marijke	$S_3 = g^{s_3}$	$(h^{s_3}, vote_3 \cdot e^{s_3})$	$(s_3) : S_3 = g^{s_3} \wedge c = h^{s_3}$

Proof of Eligibility: Simple
Proof of Ownership: Simple
Use s_i to disclose vote for revocation:

1. Marijke computes $z = e^{s_3}$ and proves its correctness with ZKP.
2. Authorities compute $vote = \frac{d}{z}$.

So what about Privacy?

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)
3. Compute Pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)
3. Compute Pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Voter Roll		
Marianne		
Hein		
Marijke		

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)
3. Compute Pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Voter Roll	**Public**	
Marianne	$S_1 = g^{s_1}$	
Hein	$S_2 = g^{s_2}$	
Marijke	$S_3 = g^{s_3}$	

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)
3. Compute Pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Voter Roll	Public	Pseudonym
Marianne	$S_1 = g^{s_1}$	$\hat{S}_1 = \hat{g}^{s_2}$
Hein	$S_2 = g^{s_2}$	$\hat{S}_2 = \hat{g}^{s_3}$
Marijke	$S_3 = g^{s_3}$	$\hat{S}_3 = \hat{g}^{s_1}$

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)
3. Compute Pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Voter Roll	Public	Pseudonym
Marianne	$S_1 = g^{s_1}$	$\hat{S}_1 = \hat{g}^{s_2}$
Hein	$S_2 = g^{s_2}$	$\hat{S}_2 = \hat{g}^{s_3}$
Marijke	$S_3 = g^{s_3}$	$\hat{S}_3 = \hat{g}^{s_1}$

E(vote)$= (c, d)$	
$(h^{s_2}, vote_{Hein} \cdot e^{s_2})$	
$(h^{s_3}, vote_{Marijke} \cdot e^{s_3})$	
$(h^{s_1}, vote_{Marianne} \cdot e^{s_1})$	

Introduce Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms $\hat{S}_{\pi(i)} = \hat{g}^{s_i}$

1. Select random α from $\mathbb{Z}_q$
2. Publish $\hat{g} = g^{\alpha} \mod p$ (Pseudonym Generator)
3. Compute Pseudonym $\hat{S}_{\pi(i)} = S_i^{\alpha} (= \hat{g}^{s_i})$

Voter Roll	**Public**	**Pseudonym**
Marianne	$S_1 = g^{s_1}$	$\hat{S}_1 = \hat{g}^{s_2}$
Hein	$S_2 = g^{s_2}$	$\hat{S}_2 = \hat{g}^{s_3}$
Marijke	$S_3 = g^{s_3}$	$\hat{S}_3 = \hat{g}^{s_1}$

E(vote)$= (c, d)$	**Proof** $ZKP[]$
$(h^{s_2}, vote_{Hein} \cdot e^{s_2})$	$(s_2) : \hat{S}_1 = \hat{g}^{s_2} \wedge c = h^{s_2}$
$(h^{s_3}, vote_{Marijke} \cdot e^{s_3})$	$(s_3) : \hat{S}_2 = \hat{g}^{s_3} \wedge c = h^{s_3}$
$(h^{s_1}, vote_{Marianne} \cdot e^{s_1})$	$(s_1) : \hat{S}_3 = \hat{g}^{s_1} \wedge c = h^{s_1}$

Revocation

Voter Roll	Public	Pseudonym
Marianne	$S_1 = g^{s_1}$	$\hat{S}_1 = \hat{g}^{s_2}$
Hein	$S_2 = g^{s_2}$	$\hat{S}_2 = \hat{g}^{s_3}$
Marijke	$S_3 = g^{s_3}$	$\hat{S}_3 = \hat{g}^{s_1}$

E(vote)$= (c, d)$	**Proof** $ZKP[]$
$(h^{s_2}, vote_{Hein} \cdot e^{s_2})$	$(s_2) : \hat{S}_1 = \hat{g}^{s_2} \wedge c = h^{s_2}$
$(h^{s_3}, vote_{Marijke} \cdot e^{s_3})$	$(s_3) : \hat{S}_2 = \hat{g}^{s_3} \wedge c = h^{s_3}$
$(h^{s_1}, vote_{Marianne} \cdot e^{s_1})$	$(s_1) : \hat{S}_3 = \hat{g}^{s_1} \wedge c = h^{s_1}$

Proof of Eligibility:

1. Marijke reveals her Pseudonym $\hat{S}_2$.
2. She proves $ZKP[(s_3) : S_3 = g^{s_3} \wedge \hat{S}_2 = \hat{g}^{s_3}]$

Proof of Ownership: Simple

Use s_i to disclose vote for revocation: Same as in naive version.

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*.
- It is safe to offer individual verifiability unconditionally.

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*.
- It is safe to offer individual verifiability unconditionally.
- The presented protocol complies with the requirements on a hybrid voting system: Voters can reveal their vote even if a coercer casted it.

Thank You

Questions / Remarks

Find
"*Coercion-Resistant Hybrid Voting Systems*"
by Oliver Spycher / Prof. Rolf Haenni in

www.e-voting.ti.bfh.ch