University of Fribourg

The SH E-Voting Protocol

Oliver Spycher

September 29th, 2010

Outline

Motivation - Hybrid Scheme

SH Protocol

Baloti E-Voting Platform

Outline

Motivation - Hybrid Scheme

SH Protocol

Baloti E-Voting Platform

A Good Voting Scheme

- Accuracy (Casted as intended, tallied as casted)
- Uniqueness and Eligibility
- Verifiability (Individual, Universal, Eligibility)
- Privacy (No link vote - voter)
- Receipt-Freeness (Not enough)
- Coercion-Resistance (Voter coercion and vote buying are infeasible)

A Good Voting Scheme

- Accuracy (Casted as intended, tallied as casted)
- Uniqueness and Eligibility
- Verifiability (Individual, Universal, Eligibility)
- Privacy (No link vote - voter)
- Receipt-Freeness (Not enough)
- Coercion-Resistance (Voter coercion and vote buying are infeasible)

In Practice

- ?Accuracy? (Casted as intended, tallied as casted)
- ?Uniqueness? and ?Eligibility?
- ~~Verifiability (Individual, Universal, Eligibility)~~
- ?Privacy? (No link vote - voter)
- ?Receipt-Freeness? (Not enough)
- ?Coercion-Resistance? (Voter coercion and vote buying are infeasible)

SH in a Hybrid Scheme

- Accuracy (Casted as intended, tallied as casted)
- Uniqueness and Eligibility
- Verifiability (Individual, Universal, Eligibility)
- Privacy (No link vote - voter)
- Receipt-Freeness (Not enough)
- Coercion-Resistance (Voter coercion and vote buying are infeasible)

Hybrid Scheme: Revoke at Polling Station

Outline

PKI Setup for DSA

Voters are assigned their

- private key $s \in \mathbb{Z}_q$ safe
- public key $S = g^s \in \mathbb{G}_q$

Group Threshold

A First Naive Approach without Privacy

Voter Roll			
1: Hugo			
2: Mark			
3: Peter			

A First Naive Approach without Privacy

Voter Roll	Public		
1: Hugo	$S_1 = g^{s_1}$		
2: Mark	$S_2 = g^{s_2}$		
3: Peter	$S_3 = g^{s_3}$		

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	Signature of Enc
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_1, g)$
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_2, g)$
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_3, g)$

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	Signature of Enc
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_1, g)$
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_2, g)$
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_3, g)$

- Proof of eligibility: simple

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	Signature of Enc
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_1, g)$
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_2, g)$
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_3, g)$

- Proof of eligibility: simple
- Proof of ownership: simple

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	Signature of Enc
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_1, g)$
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_2, g)$
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_3, g)$

- Proof of eligibility: simple
- Proof of ownership: simple
- Hugo needs to revoke his vote before casting a paper vote
  1. Choose uniformly random z from $[1, .., q]$
  2. Compute $re\text{-}enc(w_1, z) = (h^{k_1} \cdot h^z, yes \cdot e^{k_1} \cdot e^z)$ and proof
  3. Have polling station authorities sign both
  4. Cast $re\text{-}enc(w_1, z)$, proof and signature to revocation board

A First Naive Approach without Privacy

Voter Roll	Public	Encryption of Vote	Signature of Enc
1: Hugo	$S_1 = g^{s_1}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_1, g)$
2: Mark	$S_2 = g^{s_2}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_2, g)$
3: Peter	$S_3 = g^{s_3}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_3, g)$

- Proof of eligibility: simple
- Proof of ownership: simple
- Hugo needs to revoke his vote before casting a paper vote
  1. Choose uniformly random z from $[1, .., q]$
  2. Compute $re\text{-}enc(w_1, z) = (h^{k_1} \cdot h^z, yes \cdot e^{k_1} \cdot e^z)$ and proof
  3. Have polling station authorities sign both
  4. Cast $re\text{-}enc(w_1, z)$, proof and signature to revocation board

What about Privacy?

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

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

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

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

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

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
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

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
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym		
$\hat{S}_1 = \hat{g}^{s_2}$		
$\hat{S}_2 = \hat{g}^{s_3}$		
$\hat{S}_3 = \hat{g}^{s_1}$		

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

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
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	

Introduction of Pseudonyms for Privacy

Mixing authorities jointly compute pseudonyms.

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
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

Revocation

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

Revocation

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

- Proof of eligibility
  1. Hugo reveals his pseudonym $\hat{S}_3$
  2. He proves $ZKP[(s_1) : S_1 = g^{s_1} \wedge \hat{S}_3 = \hat{g}^{s_1}]$

Revocation

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

- Proof of eligibility
  1. Hugo reveals his pseudonym $\hat{S}_3$
  2. He proves $ZKP[(s_1) : S_1 = g^{s_1} \wedge \hat{S}_3 = \hat{g}^{s_1}]$
- Proof of ownership: simple

Revocation

Voter Roll	Public
1: Hugo	$S_1 = g^{s_1}$
2: Mark	$S_2 = g^{s_2}$
3: Peter	$S_3 = g^{s_3}$

Pseudonym	Encryption of Vote	Signature of Enc
$\hat{S}_1 = \hat{g}^{s_2}$	$w_1 = (h^{k_1}, yes \cdot e^{k_1})$	$sign(w_1, s_2, \hat{g})$
$\hat{S}_2 = \hat{g}^{s_3}$	$w_2 = (h^{k_2}, yes \cdot e^{k_2})$	$sign(w_2, s_3, \hat{g})$
$\hat{S}_3 = \hat{g}^{s_1}$	$w_3 = (h^{k_3}, yes \cdot e^{k_3})$	$sign(w_3, s_1, \hat{g})$

- Proof of eligibility
  1. Hugo reveals his pseudonym $\hat{S}_3$
  2. He proves $ZKP[(s_1) : S_1 = g^{s_1} \wedge \hat{S}_3 = \hat{g}^{s_1}]$
- Proof of ownership: simple
- Revoke encrypted vote: same as in naive version

Outline

Motivation - Hybrid Scheme

SH Protocol

Baloti E-Voting Platform

The Baloti Project

Baloti is an online platform that incorporates SH.

- Immigrants participate in federal referendums.

The Baloti Project

Baloti is an online platform that incorporates SH.

- Immigrants participate in federal referendums.

www.baloti.ch

- Explains political processes in 11 languages.
- Informs on political issues and disputes.
- Runs referenda