# A New Approach Towards Coercion-Resistant Remote E-Voting in Linear Time


Rolf Haenni

Oliver Spycher, Reto Koenig, Michael Schläpfer
http://e-voting.bfh.ch



15th International Conference on Financial Cryptography

March 1st, 2011

# Outline

# Outline

# A Good Voting System

- Correctness
  - → Only authorized voters can vote
  - → No voter can vote more than once
  - → Valid votes can not be altered
  - → All valid votes are counted
- Privacy
  - → Votes can not be linked to voters (not even with the help of the voters)
  - → No premature or partial results are revealed
- Verifiability
  - → Correctness is publicly verifiable

# Coercion-Resistance

- Voters can not be urged (neither by offering a reward nor by intimidation) ...
  - → to vote in a particular way
  - → to vote at random
  - → not to vote at all
  - → to give away private keying material
- Coercion-resistance means that the adversary can not decide whether a voter complies with the demands [JCJ05]

# Outline

# Introduction

- Original protocol from 2005

  A. Juels, D. Catalano, and M. Jakobsson
  *Coercion-resistant electronic elections*. WPES'05, 4th ACM Workshop on Privacy in the Electronic Society, 2005

- Offers correctness, privacy, verifiability and coercion-resistance under realistic assumptions
  - → Untappable (offline) channel during registration
  - → Sender-anonymous channel for vote casting
  - → Public bulletin board
  - → Majority of trustworthy authorities (registrars, talliers)
- Problems
  - → Quadratic-time tallying procedure (w.r.t. number of votes)
  - → Unrestricted number of votes (board flooding attacks)
  - → Secure platform

# Setup and Registration

- Setup
  - → ElGamal cryptosystem (modified version with two generators)
  - → Key pair for registrars (common public key, shared private key)
  - → Key pair for talliers (common public key, shared private key)
  - → Candidate list $C$
- Registration
  - → Registrars jointly determine at random secret credential $\sigma_i$
  - → Voter obtains $\sigma_i$ from registrars (upon proof of eligibility)
  - → Registrars publish $S_i = E(\sigma_i)$ on bulletin board
  - → Registrars prove towards voter correctness of $S_i$

## Voter Roll

- The public voter roll results from the registration phase
- Example with $n$ voters

| $i$ | $V_i$ | $S_i$ |
|---|---|---|
| 1 | Wolf | $E(\sigma_1)$ |
| 2 | Dwarf | $E(\sigma_2)$ |
| 3 | Gretel | $E(\sigma_3)$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $n$ | Witch | $E(\sigma_n)$ |

# Vote Casting

- Voter posts ballot $B_j = (X_j, Y_j, Z_j)$ to public voting board through anonymous channel
  - → $X_j = E(\sigma_j)$
  - → $Y_j = E(c_j)$ for candidate choice $c_j \in C$
  - → $Z_j =$ zero-knowledge proofs of knowledge of $\sigma_j$ and $c_j \in C$
- To deceive the adversary, a coerced voter ...
  - → selects a fake credential $\sigma'_j \neq \sigma_j$
  - → follows the coercer's instructions
  - → secretly casts the proper vote using $\sigma_j$

# Voting Board

- At the end of the voting period, the public bulletin board may contain three types of invalid votes containing ...
  - → invalid proofs
  - → duplicate credentials
  - → fake credentials
- Example with $n$ voters and $N$ votes

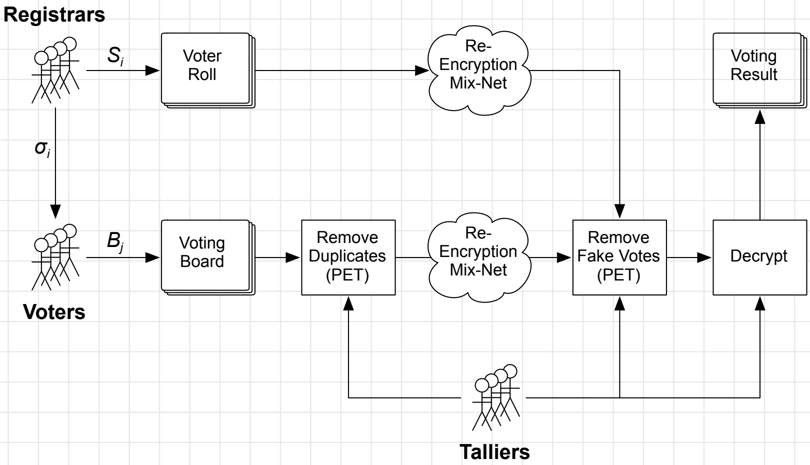
| $i$ | $V_i$ | $S_i$ |
|---|---|---|
| 1 | Wolf | $E(\sigma_1)$ |
| 2 | Dwarf | $E(\sigma_2)$ |
| 3 | Gretel | $E(\sigma_3)$ |
| $\vdots$ | $\vdots$ | $\vdots$ |
| $n$ | Witch | $E(\sigma_n)$ |

| $j$ | $X_j$ | $Y_j$ | $Z_j$ |
|---|---|---|---|
| 1 | $E(\bar{\sigma}_1)$ | $E(c_1)$ | $\cdots$ |
| 2 | $E(\bar{\sigma}_2)$ | $E(c_2)$ | $\cdots$ |
| 3 | $E(\bar{\sigma}_3)$ | $E(c_3)$ | $\cdots$ |
| 4 | $E(\bar{\sigma}_4)$ | $E(c_4)$ | $\cdots$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $N$ | $E(\bar{\sigma}_N)$ | $E(c_N)$ | $\cdots$ |

## Tallying

- Votes with invalid proofs are removed
- To remove duplicates, talliers perform $\mathcal{O}(N^2)$ many plaintext equivalence tests (PET) for all distinct pairs $(X_j, X_k)$
- To remove fake votes, talliers perform $\mathcal{O}(n \cdot N)$ many PETs for all remaining pairs $(S_i, X_j)$
- To sustain privacy, both the $S_i$ and the $(X_j, Y_j)$ lists must be shuffled in a verifiable re-encryption mix-net
- The remaining values $Y_j$ are decrypted and counted
- The whole procedure runs in $\mathcal{O}(N^2)$ time

# Protocol Overview



# Outline

# Smith/Weber's Method

- Smith (2005) and Weber (2006) proposed a method to avoid expensive PETs
  - → Talliers share secret random number $b$
  - → Talliers jointly compute $D(S_i^b) = \sigma_i^b$ and $D(X_j^b) = \bar{\sigma}_j^b$
  - → Duplicates and fake votes are removed in linear time using hash tables
- This method turned out to be insecure
  - → Posting votes with $E(\bar{\sigma}_j)$ and $E(\bar{\sigma}_j^2)$ leads to $\bar{\sigma}_j^b$ and $(\bar{\sigma}_j^b)^2$
  - → This undermines the anonymity of the mix-net
- However, removing duplicates (performed before mixing) with Smith/Weber's method is safe

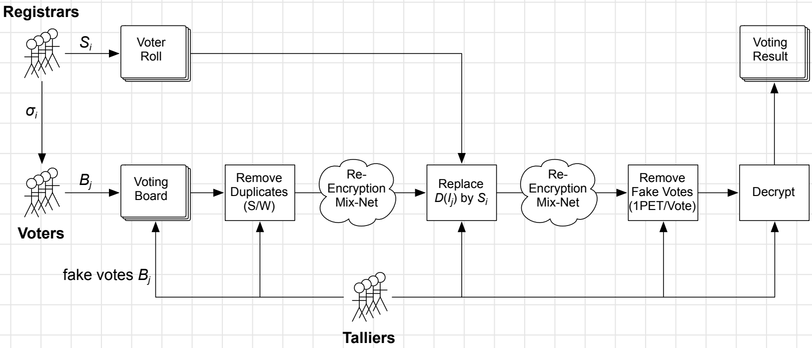
# The Modified Protocol

- Setup (unchanged)
- Registration (unchanged)
- Vote casting
  - → Extended ballot $B_j = (X_j, Y_j, Z_j, I_j)$ with $X_j, Y_j, Z_j$ unchanged
  - → $I_j = E(i)$ for index $i$ on voter roll
- Authorities insert a random number of additional fake votes for each index $i$
  - → Necessary to conceal the existence of a proper vote with index $i$
  - → Enables voters to deny the fact of having posted a proper vote
  - → The number of inserted fake votes must be kept secret

# Modified Tallying

- Votes with invalid proofs are removed
- Duplicate votes are removed using Smith/Weber's method
- Remaining votes $(X_j, Y_j, I_j)$ are mixed (1st mix-net)
- Talliers decrypt $i = D(I_j)$, votes with invalid $i$ are deleted
- Voter roll entry $S_i$ is adjoined to $(X_j, Y_j)$
- Remaining votes $(S_i, X_j, Y_j)$ are mixed (2nd mix-net)
- Talliers remove votes for which PET on $(S_i, X_j)$ returns false
- The remaining values $Y_j$ are decrypted and counted
- Modified tallying runs in $\mathcal{O}(N)$ time

# Modified Protocol Overview



# Outline

# Conclusion

- In the paper, we argue that the modified protocol is as coercion-resistance as JCJ (without changing the underlying trust assumptions)
- Tallying in the modified protocol runs in linear time
- Smith/Weber's method helps removing duplicate votes
- Additional fake votes are necessary to conceal the existence of a proper vote
- Board flooding attacks are still possible

# Outlook

- Work out formal proof
- Implementation (student project)
- Solution for preventing board flooding attack

  R. Koenig, R. Haenni, S. Fischli
  *Preventing board flooding attacks in coercion-resistant electronic voting schemes*. SEC'11, 26th IFIP International Information Security Conference, Lucerne, Switzerland, 2011

  (paper available online on http://e-voting.bfh.ch)
- Two more linear-time protocols in pipeline