New Tricks for Coercion-Resistant E-Voting

(from Jeremy Clark)

Rolf Haenni

http://e-voting.bfh.ch

Seminar, E-Voting Group, BFH

March 25th, 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 with public parameters p, q, g
  - → 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 σ_i
  - → Voter obtains σ_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

Registration Board

- The public registration board 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 $c_j \in C$
  - → $Z_j =$ NIZKP of knowledge of σ_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 σ_j

Voting Board

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

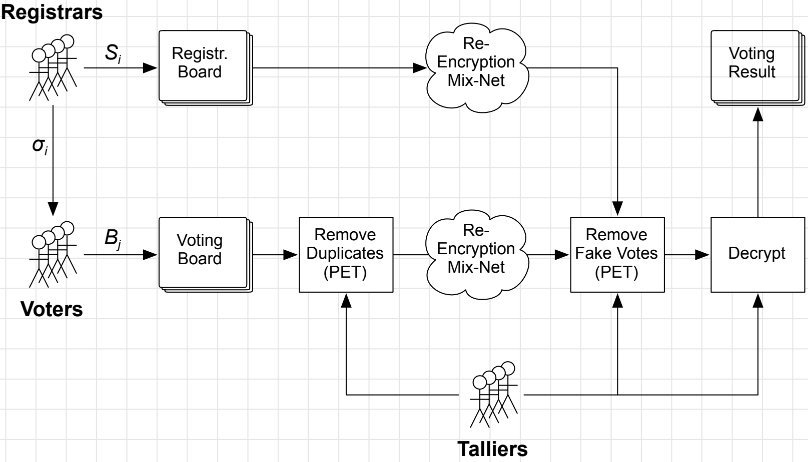
i	V_i	S_i
1	Wolf	$E(\sigma_1)$
2	Dwarf	$E(\sigma_2)$
3	Gretel	$E(\sigma_3)$
$\vdots$	$\vdots$	$\vdots$
n	Witch	$E(\sigma_n)$

j	X_j	Y_j	Z_j
1	$E(\bar{\sigma}_1)$	Y_1	Z_1
2	$E(\bar{\sigma}_2)$	Y_2	Z_2
3	$E(\bar{\sigma}_3)$	Y_3	Z_3
4	$E(\bar{\sigma}_4)$	Y_4	Z_4
$\vdots$	$\vdots$	$\vdots$	$\vdots$
N	$E(\bar{\sigma}_N)$	Y_N	Z_N

Tallying

- Votes with invalid NIZKP 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

Removing Duplicates

- Setup: as before
- Registration: as before, but the registrars publish $S_i = E(g^{\sigma_i})$ instead of $S_i = E(\sigma_i)$
- Vote casting: $B_j = (X_j, Y_j, Z_j)$ as before, but
  - → $X_j = g^{\sigma_j}$ instead of $X_j = E(\sigma_j)$
  - → Z_j includes modified NIZKP of knowledge of σ_j
- Tallying: ballots with identical values X_j are removed (keep the most recent one)
  - → runs in linear time
- Problem: Ballots can be linked across multiple voting events

Modified Voting Board

- Voting Event 1: n voters and N votes

i	V_i	S_i
1	Wolf	$E(g^{\sigma_1})$
2	Dwarf	$E(g^{\sigma_2})$
$\vdots$	$\vdots$	$\vdots$
n	Witch	$E(g^{\sigma_n})$

j	X_j	Y_j	Z_j
1	$g^{\bar{\sigma}_1}$	Y_1	Z_1
2	$g^{\bar{\sigma}_2}$	Y_2	Z_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
N	$g^{\bar{\sigma}_N}$	Y_N	Z_N

- Voting Event 2: n' voters and N' votes

i	V_i	S_i
1	Wolf	$E(g^{\sigma_1})$
2	Dwarf	$E(g^{\sigma_2})$
$\vdots$	$\vdots$	$\vdots$
n'	King	$E(g^{\sigma_{n'}})$

j	X_j	Y_j	Z_j
1	$g^{\bar{\sigma}_1}$	Y_1	Z_1
2	$g^{\bar{\sigma}_2}$	Y_2	Z_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
N'	$g^{\bar{\sigma}_{N'}}$	$Y_{N'}$	$Z_{N'}$

Outline

Election Setup

- To solve the linkability problem, an Election Setup phase is introduced between registration and vote casting
- The trick is to derive an electoral board from the registration board by switching the generator from g to $\hat{g}$
- Idea: perform the "SH10-Trick" (without shuffling)
  - → Initialize $\hat{g} := g$ and $\hat{S}_i := S_i$
  - → Each of r trustees selects a random value $\alpha_j \in \mathbb{Z}_q$
  - → ...and computes $\hat{g} := \hat{g}^{\alpha_j}$ and $\hat{S}_i := \hat{S}_i^{\alpha_j}$ (with NIZKP)
  - → Finally, $\hat{g} = g^{\alpha_1 \cdots \alpha_r}$ and $\hat{S}_i = S_i^{\alpha_1 \cdots \alpha_r}$ are published on the electoral board
  - → Note that $\hat{S}_i = E(g^{\sigma_i})^{\alpha_1 \cdots \alpha_r} = E(g^{\sigma_i \alpha_1 \cdots \alpha_r}) = E(\hat{g}^{\sigma_i})$

Electoral Board

- Voting Event 1: n voters and N votes

i	V_i	$\hat{S}_i$
1	Wolf	$E(\hat{g}_1^{\sigma_1})$
2	Dwarf	$E(\hat{g}_1^{\sigma_2})$
$\vdots$	$\vdots$	$\vdots$
n	Witch	$E(\hat{g}_1^{\sigma_n})$

j	X_j	Y_j	Z_j
1	$\hat{g}_1^{\bar{\sigma}_1}$	Y_1	Z_1
2	$\hat{g}_1^{\bar{\sigma}_2}$	Y_2	Z_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
N	$\hat{g}_1^{\bar{\sigma}_N}$	Y_N	Z_N

- Voting Event 2: n' voters and N' votes

i	V_i	$\hat{S}_i$
1	Wolf	$E(\hat{g}_2^{\sigma_1})$
2	Dwarf	$E(\hat{g}_2^{\sigma_2})$
$\vdots$	$\vdots$	$\vdots$
n'	King	$E(\hat{g}_2^{\sigma_{n'}})$

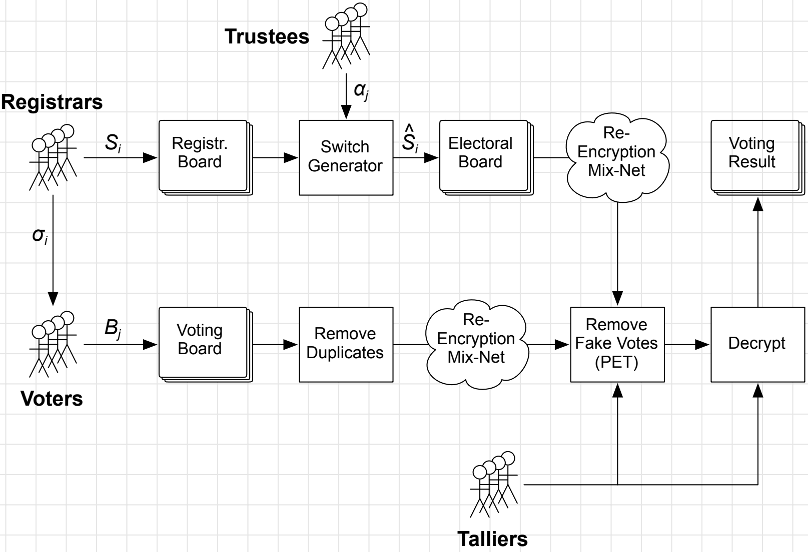
j	X_j	Y_j	Z_j
1	$\hat{g}_2^{\bar{\sigma}_1}$	Y_1	Z_1
2	$\hat{g}_2^{\bar{\sigma}_2}$	Y_2	Z_2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
N'	$\hat{g}_2^{\bar{\sigma}_{N'}}$	$Y_{N'}$	$Z_{N'}$

Outline

Anonymity Set

- Removing fake votes during tallying is based on random anonymity sets
- During vote casting, each voter j
  - → computes $\hat{S}'_j = ReRandomize(\hat{S}_j, r_j)$
  - → selects randomly $S \subseteq \{\hat{S}_1, \dots, \hat{S}_n\}$ s.t. $\hat{S}_j \in S$ and $|S| = \beta$
  - → generates NIZKP that $\hat{S}'_j$ is a re-randomization of 1-out-of-β elements of S
  - → $\hat{S}'_j$ and NIZKP are added to ballot: $B_j = (X_j, Y_j, Z'_j, \hat{S}'_j)$
- During tallying, ballots $PET(X_j, \hat{S}'_j) = false$ are removed
  - → runs in linear time
- Disadvantage: expensive proof left to voters (if β is large)

Protocol Overview



Outline

Conclusion

- Linear-time removal of duplicates without Smith/Weber
- Linear-time removal of fake votes with anonymity set of size β, re-encryption of S_j, 1-out-of-β NIZKP
- Board flooding attacks are still possible
- More details available in:

J. Clark and U. Hengartner
Selections: Internet Voting with Over-the-Shoulder Coercion Resistance.
FC'11, 15th International Conference on Financial Cryptography and Data Security, St. Lucia 2011

- Clark's solution includes "Panic Password System" on top