ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

inf | Informatik
Computer Science

Efficient Vote Authorization in Coercion-Resistant Internet Voting

Michael Schläpfer, Rolf Haenni, Reto Koenig and Oliver Spycher

Michael Schläpfer
Information Security Group
September 29, 2011

Motivation

- There exist already coercion-resistant approaches, but they lack efficiency or applicability
- Recent improvements require expensive operations on the voter's side
- We present a simple and efficient approach with fewer computational requirements on the voter's side

Outline

Remote Internet Voting

Some of the main problems of remote voting include:

- No voting booth
- No privacy
- Prone to coercion attacks of all kinds
  - Randomization attacks
  - Forced abstention attacks
  - Simulation attacks

Establishing Privacy

To establish voter privacy in remote settings, two concepts must be provided to the voter:

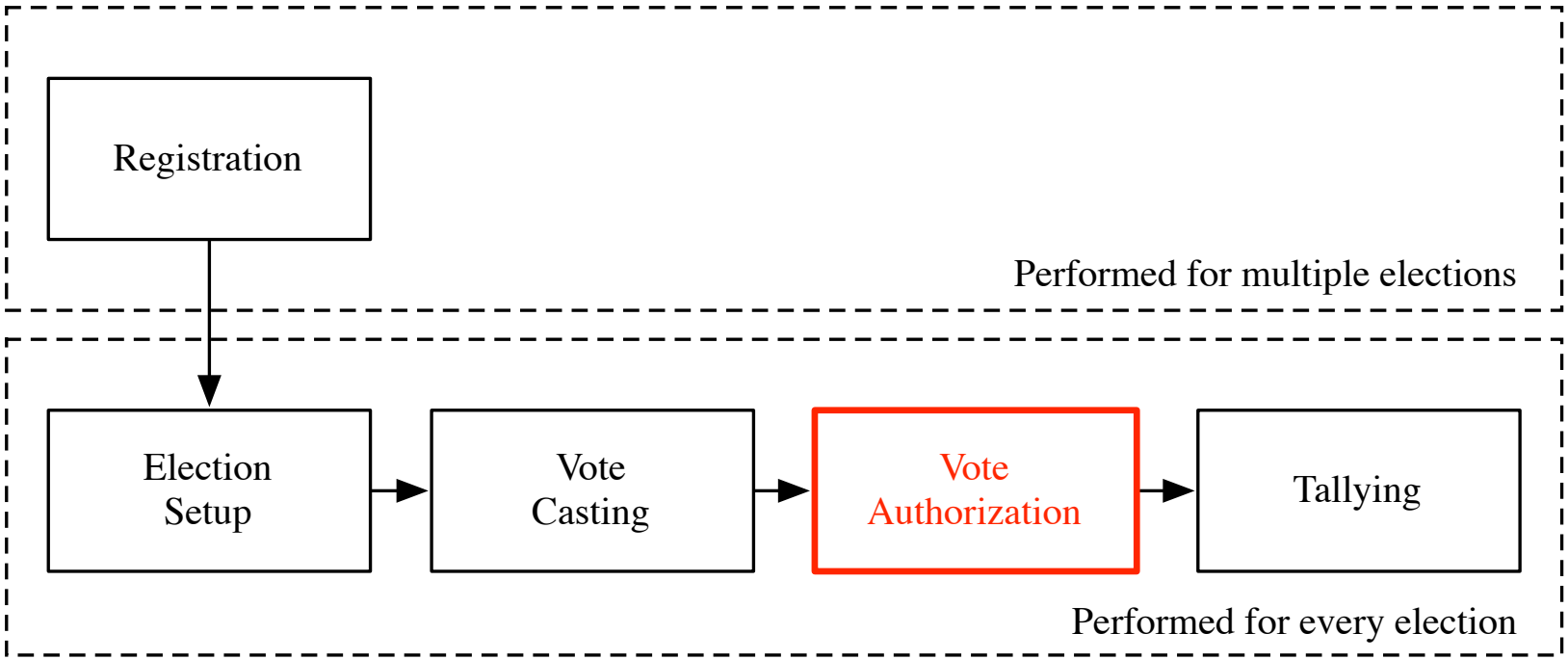
- Ability to create and cast fake votes, the coercer cannot distinguish from valid ones
- Ability to cast multiple votes

This possibly leads to:

- Improperly constructed ballots
- Duplicate ballots with the same credentials
- Fake ballots with invalid credentials

Phases of Coercion-Resistant Internet Voting

All approaches generally follow these phases:



Vote Authorization

Vote authorization includes the following steps:

Invalid Votes Elimination: Remove ballots that are not created properly (e.g., incorrect proofs, invalid format)

Duplicate Votes Elimination: Remove ballots with the same credential (enforce “one-voter-one-vote” principle)

Fake Votes Elimination: Remove ballots with fake credentials

Outline

Approaches

First approach presented by Juels, Catalano and Jakobsson (JCJ) in 2005 and implemented by Clarkson et al. (CIVITAS):

- Vote authorization using plaintext equivalence tests (PET)
- Quadratic work load in the number of submitted ballots
- Not applicable for large-scale settings as shown by Clarkson
- Various improvements presented during the last years, none is a solution to the full

Anonymity-Set-Based Approaches

At FC '11, Clark and Hengartner presented SELECTIONS:

- Voter randomly defines an anonymity set of β public credentials including his own
- Hence, voter is anonymous w.r.t a subset of the electorate

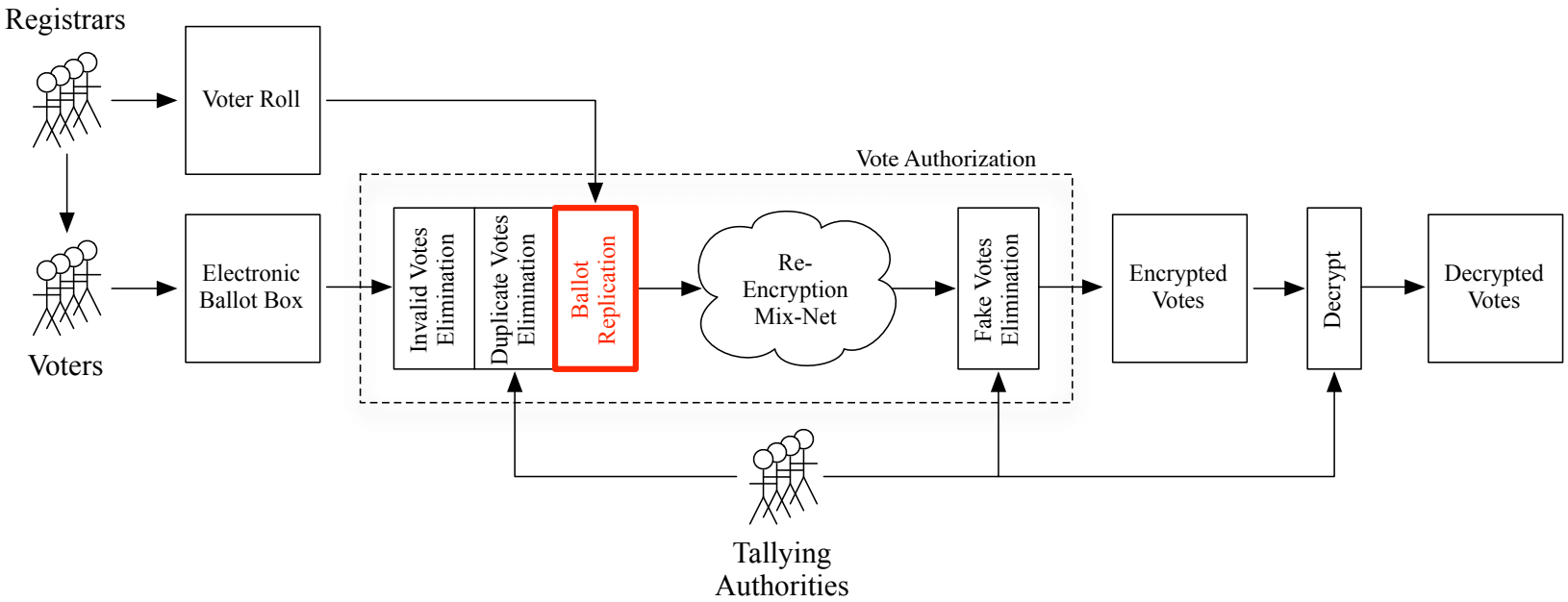
Problem:

Voter must provide an (expensive) additional proof!
Example: Simple yes/no question with $\beta = 50$ requires the voter to perform more than 200 exponentiations.

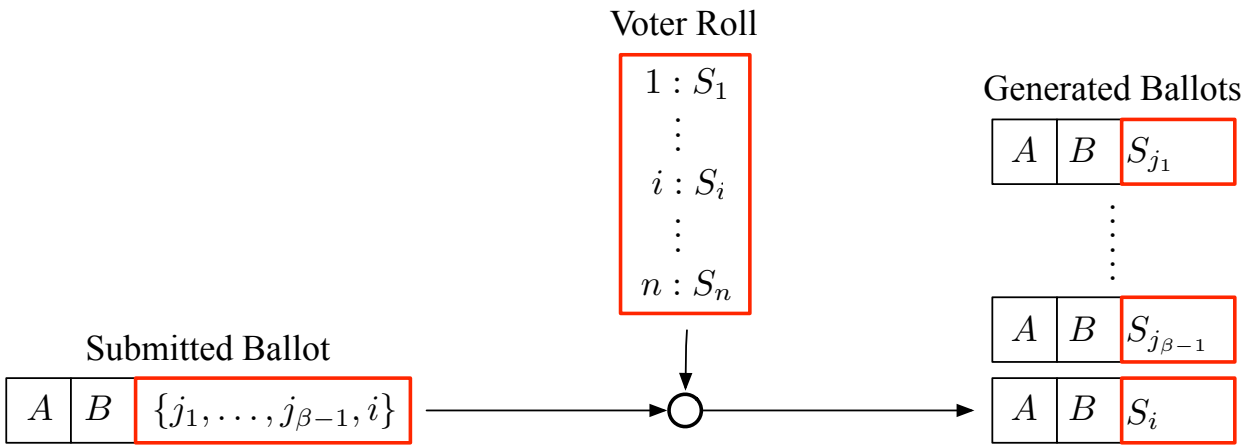
Outline

An Enhanced Anonymity-Set-Based Protocol

- Relates strongly to JCJ
- Additional ballot replication step
- Voter is not forced to perform additional proofs (example from before: 11 exponentiations)

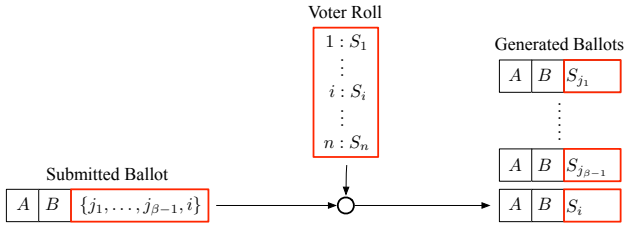


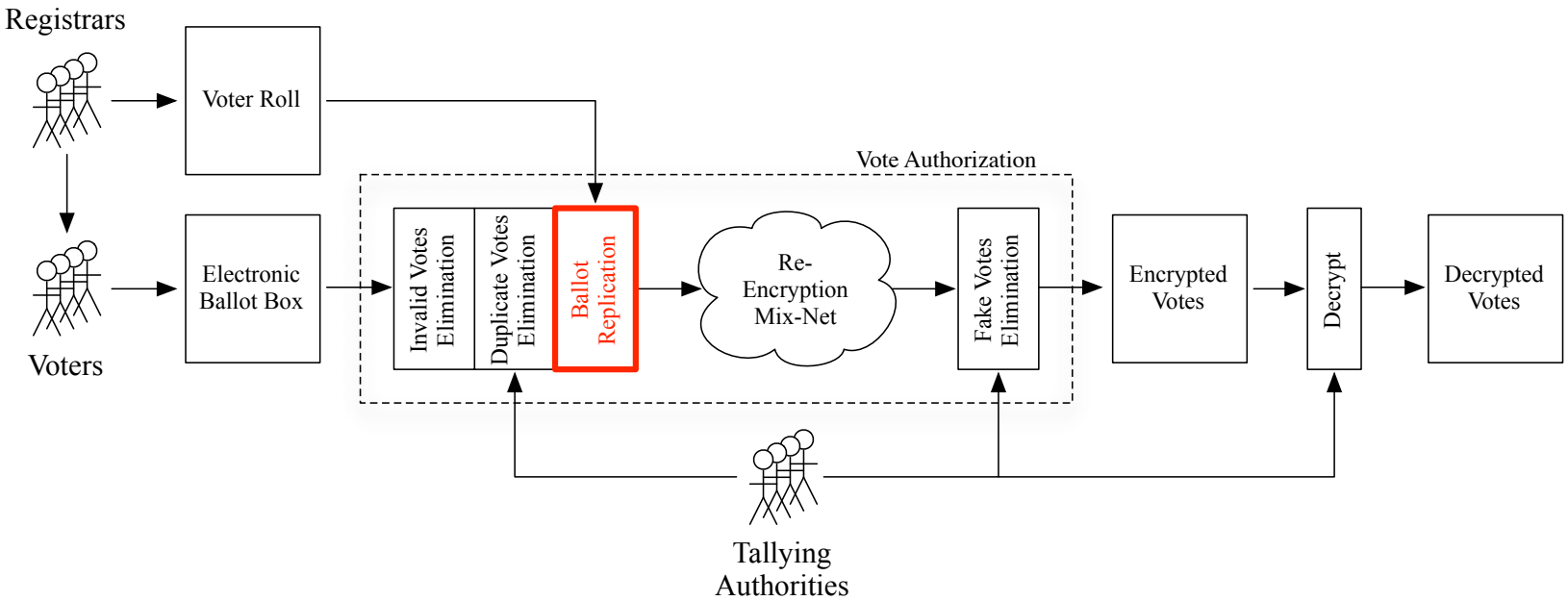
Ballot Replication Step



- $A = Enc_\epsilon(\sigma, \alpha_A)$ (voter's encrypted credential σ)
- $B = Enc_\epsilon(c \in \mathcal{C}, \alpha_\mathcal{B})$ (chosen candidate c of all valid candidates $\mathcal{C}$)
- Voter defines set of distinct voter roll indices of size β including his own
- NIZKP (knowledge of σ and $c \in \mathcal{C}$)

Ballot Replication Step





Security Considerations

Three interesting cases regarding β:

Case 1: ($\beta = n$)
Degree of coercion-resistance corresponds to JCJ, but vote authorization quadratic in n

Case 2: (β fixed, e.g., $\beta = 50$)
Non-negligible, but small advantage for coercer, coercion-resistance not given to the full, but to a reasonable extent

Case 3: ($\beta_i \geq \beta$, e.g., $\beta_i \geq 50$)
Vote authorization again quadratic in n

Performance

		JCJ (CIVITAS)	Clark et al. (SELECTIONS)	Our Protocol
Election Setup		–	$(4n+2)T$	–
Vote Casting		$4m+3$	$4\beta+4m+2$	$4m+3$
Vote Authorization	Eliminate Invalid Votes	$(4m+2)N$	$(4\beta+4m+2)N$	$(4m+2)N$
	Elim. Duplicate Votes	$\frac{7}{2}(N^2-N)T$	0	$7NT$
	1st Mixing of Ballots	$12NT$	$18NT$	$18\beta NT$
	Eliminate Fake Votes	$7nNT$	$7NT$	$7\beta NT$
Verification	Election Setup	–	$4(n+1)T$	–
	Eliminate Invalid Votes	$(4m+2)N$	$(4\beta+4m+2)N$	$(4m+2)N$
	Elim. Duplicate Votes	$4(N^2-N)T$	0	$8NT$
	1st Mixing of Ballots	$8NT$	$12NT$	$12\beta NT$
	Eliminate Fake Votes	$8nNT$	$8NT$	$8\beta NT$

Table: Performance comparison by counting the number of modular exponentiations required in each phase.

Outline

Conclusion

- Anonymity-set-based approaches offer a new way for efficient vote authorization
- Efficiency comes with a price, i.e., coercion-resistance only to a certain degree
- Our new protocol, based on ballot replication, can also be applied on limited voting devices, but at the cost of more workload on the authority's side