Practical Approach to Anonymity in Large Scale Electronic Voting Schemes

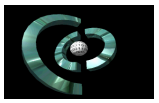
NDSS '99 — San Diego CA, February 1999

Andreu Riera, Joan Borrell

Combinatorics and Digital Communication Group

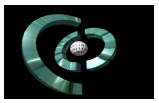
Universitat Autònoma de Barcelona — Catalonia, Spain

E-mail: ariera@ccd.uab.es



Contents

- Electronic voting schemes: Security requirements
- Mix-nets in voting schemes
- Large scale voting schemes
- Our proposal: Preliminary, voting and shuffling phases
- Conclusions

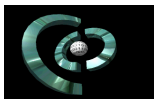


Electronic voting schemes: Security requirements

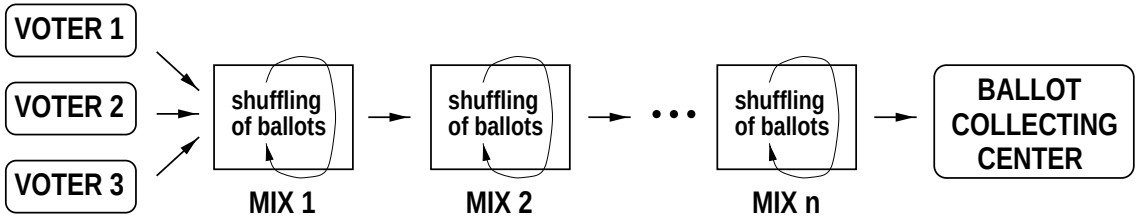
- Accuracy
- Democracy
- Privacy $\rightarrow$ Anonymity
- Verifiability

Anonymity is normally treated by assuming the existence of an anonymous channel, either

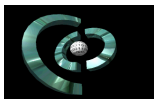
1. Without caring about its actual implementation, or
2. Using an already operating remailer system, based on the mix concept.



Mix-nets in voting schemes



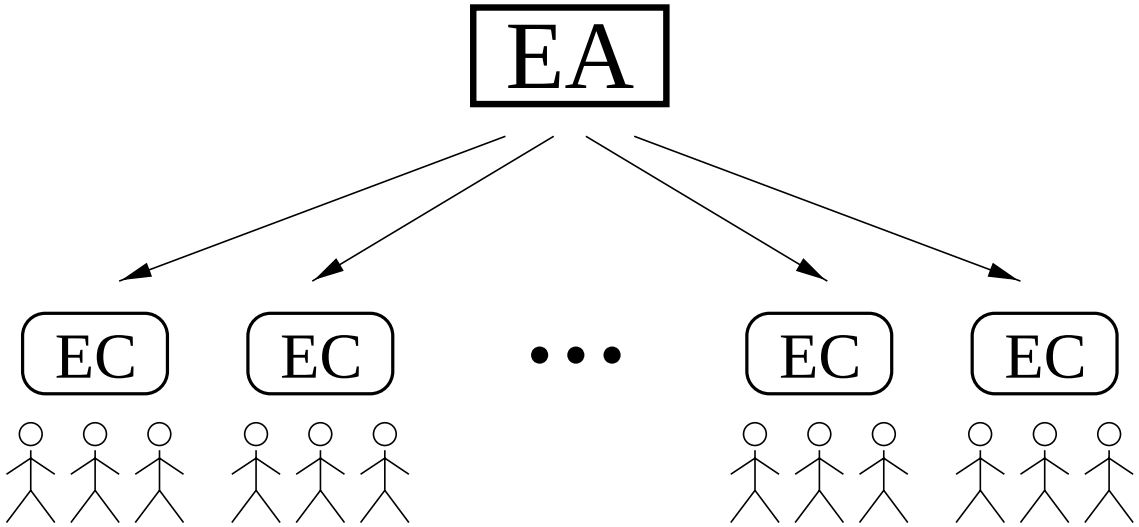
- Two sessions are required to cast a ballot
- Possibility of half–abstentions
- Anonymity can be defeated by the ballot collecting center under low traffic conditions
- Difficulty to assure fairness
- Dependence of the voting system on a set of external entities

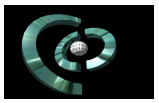


Large scale voting schemes

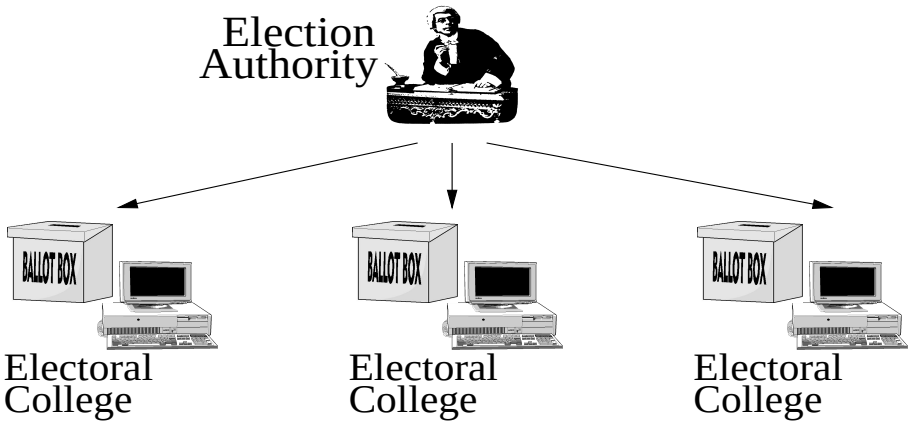
There must be a set of distributed Electronic Electoral Colleges operating concurrently.

The hierarchical relationship is the most suitable for coordination tasks.

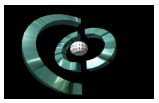




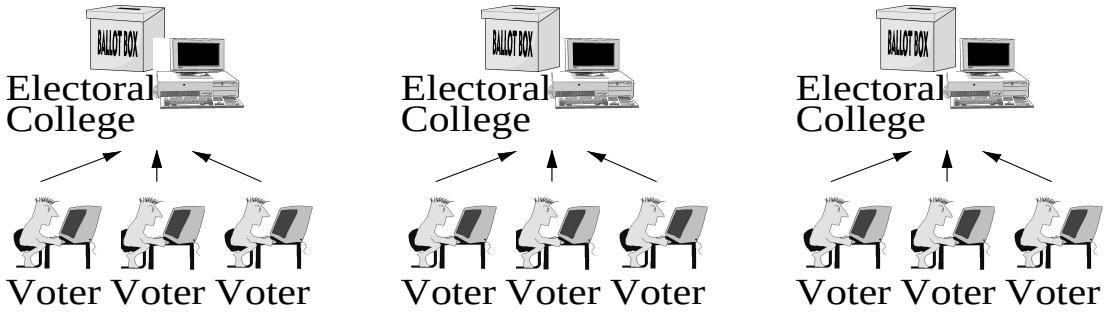
Preliminary phase



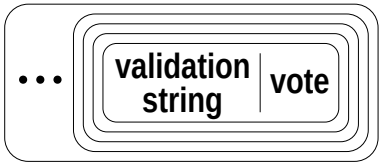
1. Certification of asymmetric key pairs
2. Creation of the Electoral Roll by the EA
3. Generation by the EA of n asymmetric key pairs for each EC, which will be used for anonymity purposes

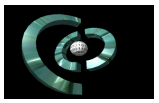


Voting phase

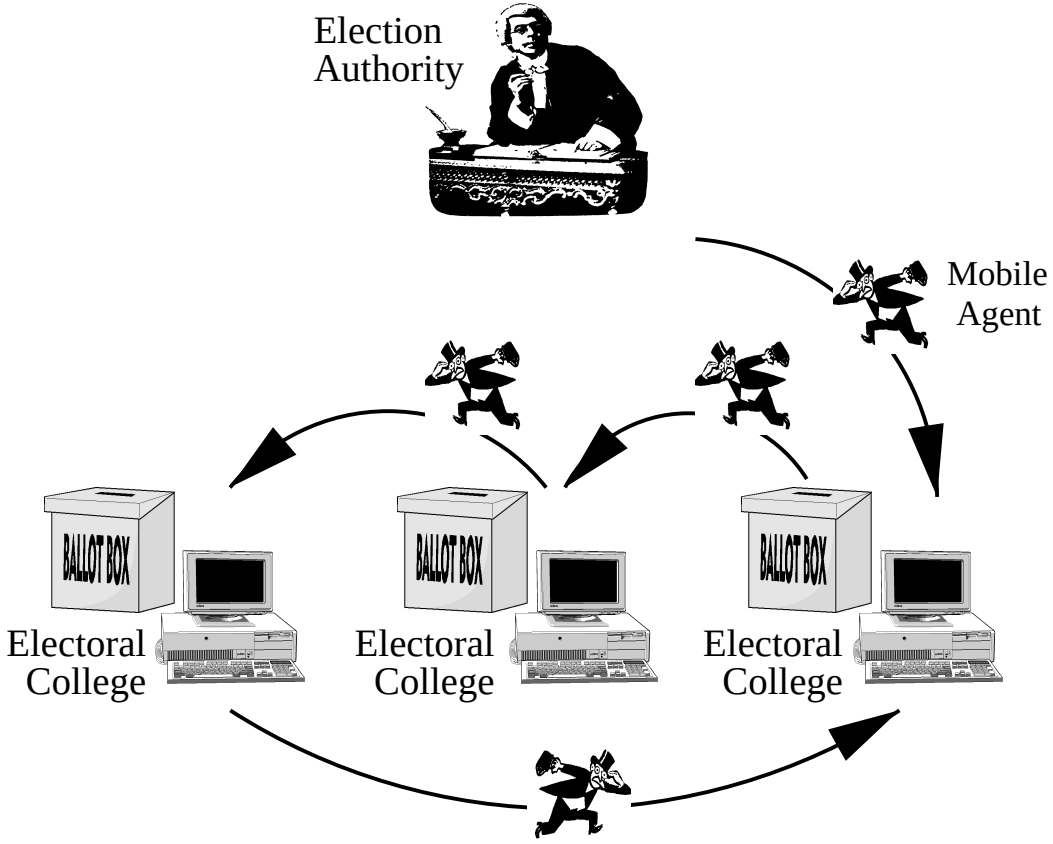


1. Security context establishment
2. Use of D.Chaum's blind signature mechanism
3. Ballot as a pair (vote, validation string) into a recursive digital envelope

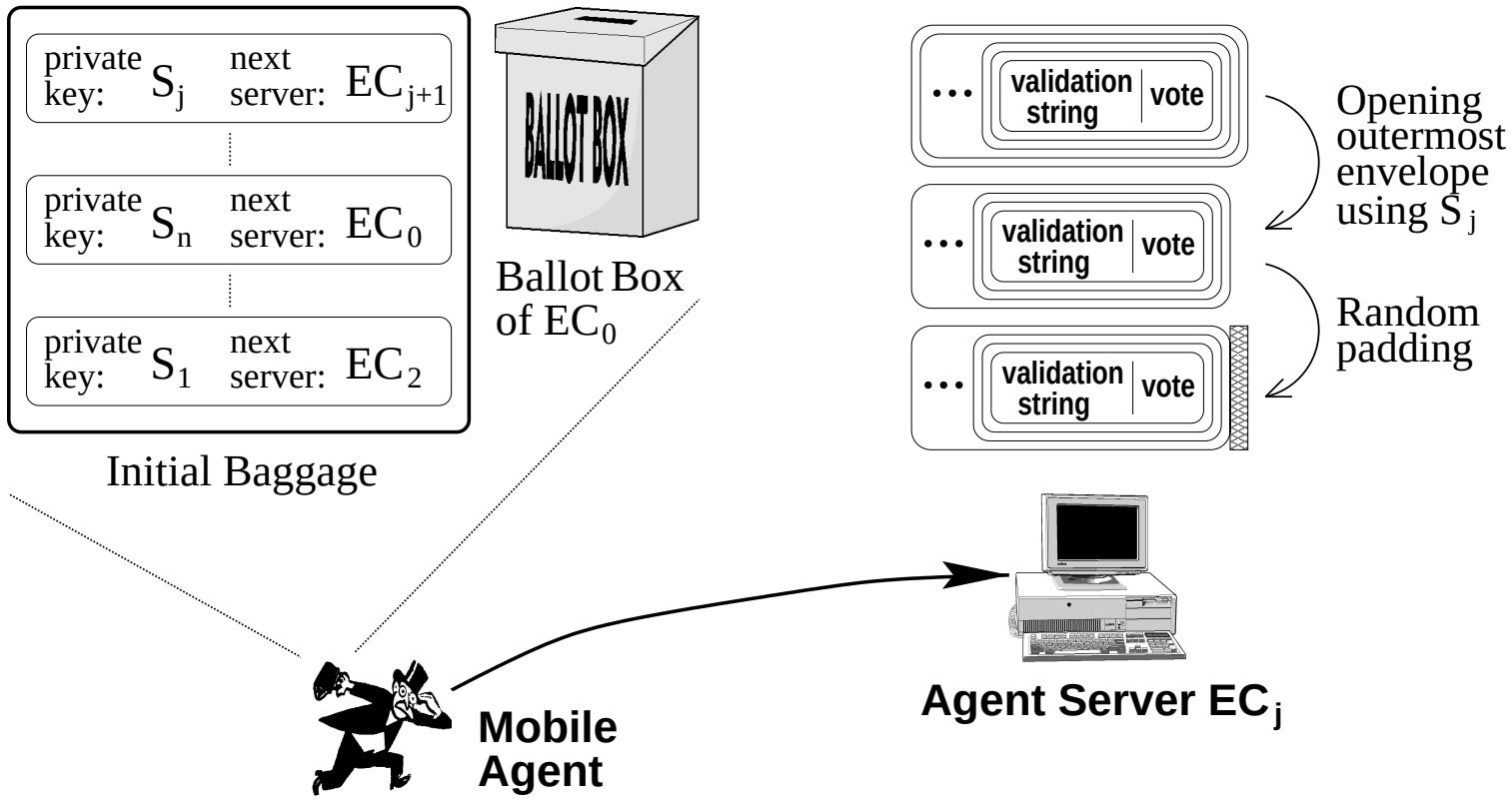




Shuffling phase: Overview



Shuffling phase: Processing at agent servers



Conclusions

- Regarding anonymity, the security offered by our scheme is equivalent to that provided by a mix-net. In addition, all presented problems are solved
- Passive and active attacks against a single honest agent server may be detected and corrected
- The design of the agents' baggage format tries to reduce the risk of collusion of malicious servers
- The voting scheme fulfills all commonly accepted security requirements