Electronic Voting with Fully Distributed Trust and Maximized Flexibility Regarding Ballot Design

Oksana Kulyk
Motivation

- **Common setting**
  - Voters need to trust the central infrastructure (trustees, mix nodes etc.)
  - Trust is distributed among the set of entities (9 in Norway, 7 in Estonia)

- **Ideal setting**
  - Trust is distributed among all the voters
  - In many scenarios, not appropriate

→ Appropriate in small-scale elections
Boardroom voting

- Board of directors
- Party congress
- University governing body
Goals

- Design secure boardroom voting protocol

- Implement it as smartphone application
Security requirements

- **Eligibility** – only eligible votes accepted
- **Fairness** – no partial results revealed
- **Vote secrecy** – no link between voter and vote
- **Integrity** – no way to modify cast votes
- **Verifiability** – possible to verify the integrity
- **Robustness** – availability of the result
Project Settings

- No central voting infrastructure
- Common mobile devices
- Remote participation
- Ballot flexibility
- Dynamic groups of voters
Challenges from this setting

- Low network quality
- Low computational power
Voting Stages

1. Voter selection
2. PKI establishment
3. Election key generation
4. Ballot initiation
5. Vote casting
6. Vote anonymization
7. Tallying
Voter selection

- Voter selection
- PKI establishment
- Election key generation
- Ballot initiation
- Vote casting
- Vote anonymization
- Tallying
PKI Establishment

- Voter keys generation and exchange
- Options
  - Certificate authority
  - Web of trust
  - Short authentication strings
- Criteria: dynamic groups of voters
Election Key Generation

- Generation of public key and shares of private key
- Options
  - Single dealer key generation
  - Multiple independent party key generation
  - Multiple dealer key generation
- Criteria: Trust distribution
PKI establishment and election key generation

Voter selection → PKI establishment → Election key generation → Ballot initiation → Vote casting → Vote anonymization → Tallying

The keys have been generated and exchanged.

Please read out the following security phrase aloud:

*treadmill penetrate basalt*

The other voters will check if their security phrase matches yours.
Ballot Initiation

Voter selection
PKI establishment
Election key generation
Ballot initiation
Vote casting
Vote anonymization
Tallying
Vote Casting

1. Voter selection
2. PKI establishment
3. Election key generation
4. Ballot initiation
5. Vote casting
6. Vote anonymization
7. Tallying
Vote Casting

- Encrypt vote with public election key
- Broadcast the encrypted vote

- Voter selection
- PKI establishment
- Election key generation
- Ballot initiation
- Vote casting
- Vote anonymization
- Tallying
Vote Anonymization

- Remove link between voter and individual vote

- Options
  - Homomorphic tallying
  - Decryption mix net
  - Reencryption mix net

- Criteria: ballot complexity, low network quality
Vote Anonymization

- Prove the validity of mixing

- Options
  - Randomized partial checking
  - Zero-knowledge proof
    - Groth 10
    - Terelius-Wikström 10
    - ...

- Criteria: low computational power
Tallying

- Distributed decryption
- Options
  - Reconstruct key
  - Produce partial decryptions
- Criteria: trust distribution

- Voter selection
- PKI establishment
- Election key generation
- Ballot initiation
- Vote casting
- Vote anonymization
- Tallying
Tallying

- Voter selection
- PKI establishment
- Election key generation
- Ballot initiation
- Vote casting
- Vote anonymization
- Tallying
Efficiency

- Android App as prototype
- Efficiency tests with Samsung Galaxy S3
  - Independent from ballot type
  - ~2 minutes for 4 voters
  - Estimated: ~12 minutes for 25 voters
Security assumptions

- More than half of voters honest
- Devices of honest voters reliable
- Network communications between honest voters reliable
- No coercion
Conclusion and future work

- Designed secure boardroom voting protocol
- Implemented it as smartphone application

Future work
- Efficiency improvements
- Robustness improvements
- Usability studies
References

