Decentralized Systems Engineering

CS-438 – Fall 2023

DEDIS

Bryan Ford and Pierluca Borsò-Tan

EPFL

Credits: B. Ford, P. Borsò-Tan

E-Voting

Decentralized Systems for Democracy

Election Phases

- Voter registration
- Prepare ballots
- Mark ballots
- Cast ballots
- Count ballots

Requirements

- Authentication / authorization
- Inclusion / accessibility
- Equality / fairness – 1 person, 1 vote
- Integrity – mark, cast, counted
- Privacy – ballot, participation
- Transparency – E2E verifiability
- Resistant to coercion & vote-buying

In-person Voting

- Why not just paper ?
  - Validating user choices
  - Inclusion / accessibility (e.g. visual impairments)
  - Counting efficiency
  - Convenience

- What types ?
  - Direct-recording electronic (DRE) voting machines
  - Paper-based – Ballot Marking Device (BMD), Optical scan

Remote online e-voting (or i-voting)

- Ballots are marked electronically on voter's device
- Transmitted over the internet
- No paper trail

- Voter hopes (verifies?) the vote is counted correctly

- Switzerland: various trials since 2003
- Estonia: since 2005, >50% votes cast online in 2023

Remote E-Voting Phases

- Registration → decide on voter roster
- Open election
- Cast ballot → encryption, transmission
- Close election
- Shuffling → randomize order of encrypted ballots
- Counting → decryption of ballots or tallies

End-to-end Verifiability

Key desirable properties:

- Cast-as-intended
  Verifiably: voter's intent → encrypted, transmitted ballot

- Recorded-as-cast
  Verifiably: encrypted ballot → ledger of cast ballots
  Approach: public bulletin board, tamper-evident log, ledger/blockchain

- Counted-as-recorded
  Verifiably: all encrypted ballots → (shuffled, decrypted,) counted

Cast-as-intended: Challenges

- Availability – network connectivity
  - Swiss fallback: postal voting, in-person
- Man-in-the-Middle – ballot manipulation
  - Requires strong user authentication
- Compromised voter device
  - Benolah challenge
  - Code voting (e.g., Switzerland)
  - Cross-device verification (Votegral)

Counted-as-recorded: Approaches

Shuffle-and-decrypt

- Classic mix-nets

  ballots → Mix1 → Mix2 → ... → MixN → decrypt ballots

  (verifying at each step)

- Cryptographic verifiable shuffles

  Neff shuffle (ElGamal encryption)

  Generalized zk-SNARKs

- Cut-and-choose (Scantegrity, assigned reading)

Coercion resistance: Challenges

Two broad approaches:

- Re-voting
  - Only the last vote counts

- Fake credentials
  - Juels-Catalano-Jakobsson (JCJ) scheme
  - cf. “Coercion-Resistant Electronic Elections” (optional reading)

Next steps

Mandatory reading:

- Scantegrity: End-to-End Voter-Verifiable Optical-Scan Voting

Optional readings:

- STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System
- Verifiable Internet Voting in Estonia
- Coercion-Resistant Electronic Elections (JCJ)
- ... and a few more ☺