CS-438 Decentralized Systems Engineering

Week 14

E-voting — E-democracy

- Election phases:
  - Marking ballots
  - Casting ballots
  - ---------- deadline ----------
  - Shuffling ballots
  - Counting ballots

- Toolbox:
  - Privacy: / verifiable shuffles
    - homomorphic / SMPC
  - Integrity: / code voting (Swiss) "cast-as-intended"
    - cut-and-choose (Benaloh challenge)
    - re-voting
  - Anti-coercion: / false credentials (JCJ)

Requirements

- Authentication / authorization
- Inclusion
- One person one vote
- Integrity: correct result
- Privacy: ballot secrecy
- Clear, well-defined set of valid ballots
- Transparency: Convincing voters that result is correct
- Coercion / vote-buying resist.

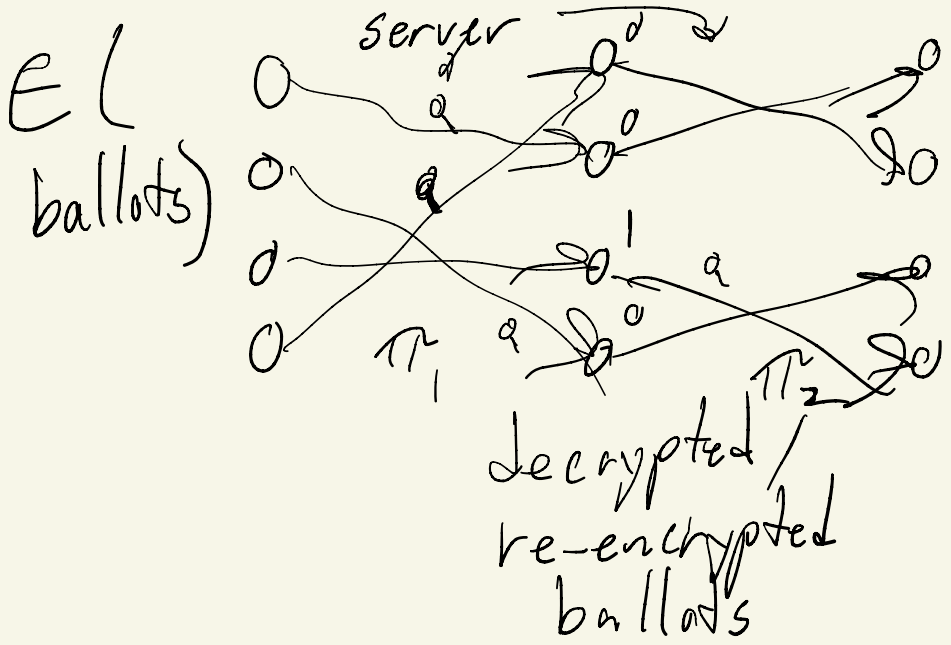
Voting systems

- In-person, electronically-assisted voting (ballot marking devices (BMD))
  - Usability / inclusion, reduced voter errors, screen reading
  - Scantegrity (2009), STAR-Vote: "coercion-resistance", cast-as-intended verif., paper trail, auditable
- Remote / Internet voting
  - Estonia: cast-as-intended verifiability, coercion-resistance
    NOT full E2E verifiability
    revoting: only the last vote cast counts
    weakness: keep voters under control / surveillance until deadline
    last-minute voting
  - False credentials (JCJ)
    real credentials cast counting votes
    indistinguishable after registration

- Verifiable shuffles / MIX-nets

- Scantegrity: trying to be simple/understandable

cut-and-choose



server:

1. permutes x2
2. commits to all (on BB/ blockchain...)
3. challenger: pick 1 random coin per interm. ballot

- H(all commits)
- Verifiable random func, public randomness (RandHound, drand)

- ZK shuffle proofs (specialized)
  - Neff (2001) - ElGamal encryptions
  - Wikstom, Fujikawa, Groth, ...
- Gen: ZK-SNARKS, ...