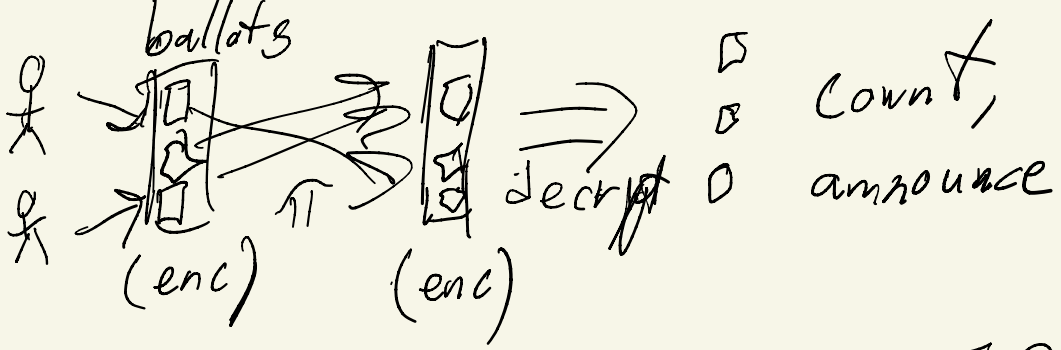
# CS-234
# Technologies for societal self-organization

## Week 14

# E-voting, as part of "E-democracy"

- Research: digital voting algorithms
  - Verifiable shuffle / Mix-nets (Neff) - to shuffle ballots 2001




  - E-voting systems esp. E2E-verifiable Scantegrity (2005), ...
  - Estonia (2005)
  - Switzerland (200?) - certain cantons
  - "Blockchain voting" - US (Voatz) (2019?)

# Motivations

- Faster, more precise counting
- increase participation / turnout
- Convenience, usability
- Inclusion - disabilities
- Expats - voting from abroad

short-term / pragmatic ↖ ↗ long-term

- increase - continuous participation
  - depth of:
    - liquid democracy
    - (online) deliberative polls, juries
    - iterative collective choice
- E-voting as stepping-stone

# Challenges / Requirements

- Strong validation / correctness
- Vote privacy (encryption)
- Coercion-resistance (vote-buying)
- High availability (time-critical)
- Authentication / authorization
- Education
- Integrity: Correctness
- Trust / perception of legitimacy
  - transparency

- Toolbox (technologies, algorithms, methods)

---

- Encryption, cryptography (Signing, ZK proofs)
  - Weaknesses: buggy SW (app, OS, supply chain)
  - Weakness: long-term privacy - cryptographic breakthroughs
    - quantum computers
  - Challenge: long-term / post-quantum crypto
- Verifiable shuffles: encrypt, shuffle, decrypt, tally
  - advantage: general - works for <u>any</u> ballot type, election method
  - disadvantage: privacy/coercion-resistance: rich-information ballots
- Homomorphic encryption, SMPC: encrypt, collect, tally, decrypt result
  - advantage: less privacy leakage, coercion risk
  - disadvantages: slower/costly for complex computations

additive homomorphism: $\in_y(M_1) + \in_y(M_2) = \in_y(M_1 + M_2)$

(El Gamal)

# Coercion-resistance

- "it's illegal, so people won't do it" (Switzerland)
  (remote vote-buying)
- Estonia: limited coercion-resistance: re-voting
  - disadvantages: last-minute voting
- false credentials (JCJ)
  - real & false credentials indistinguishable
  - research, practical challenges