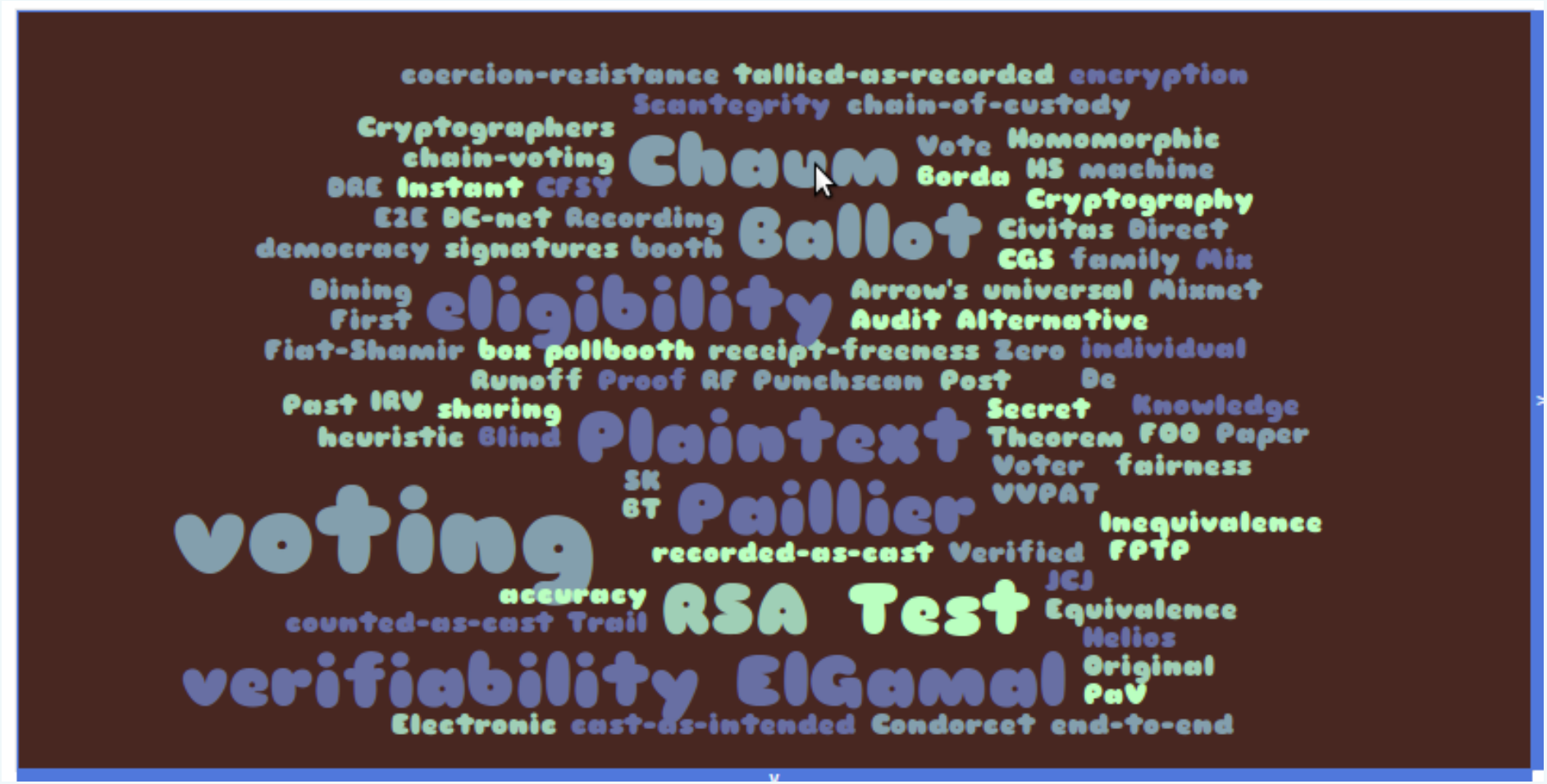
A Glossary of Voting Terminology

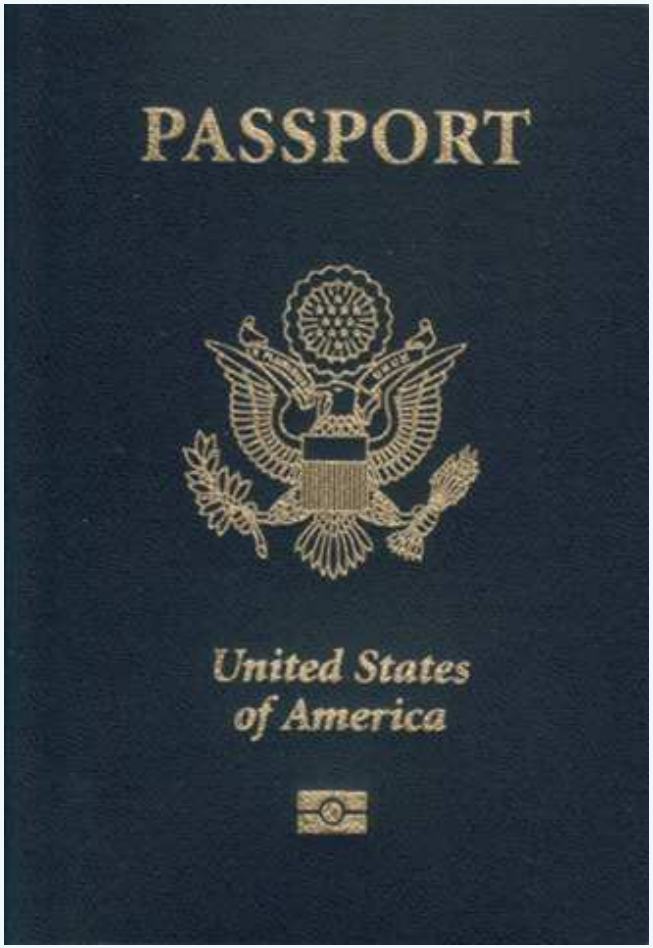


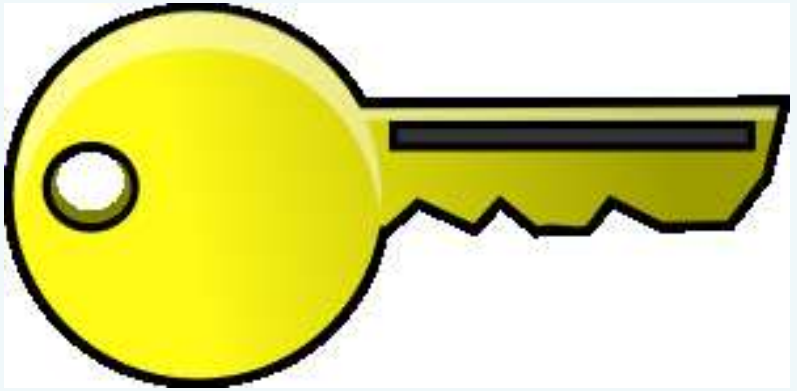
Structure

- Terms from actual elections
- Requirements
- Attacks
- Cryptography
- Determining the winner
- Some academic systems of renown

Actual election terminology

- Voter credentials





Actual election terminology

- Ballot

Actual election terminology

- Ballot box

Actual election terminology

- Booth / Voting Booth / Pollbooth

Actual election terminology

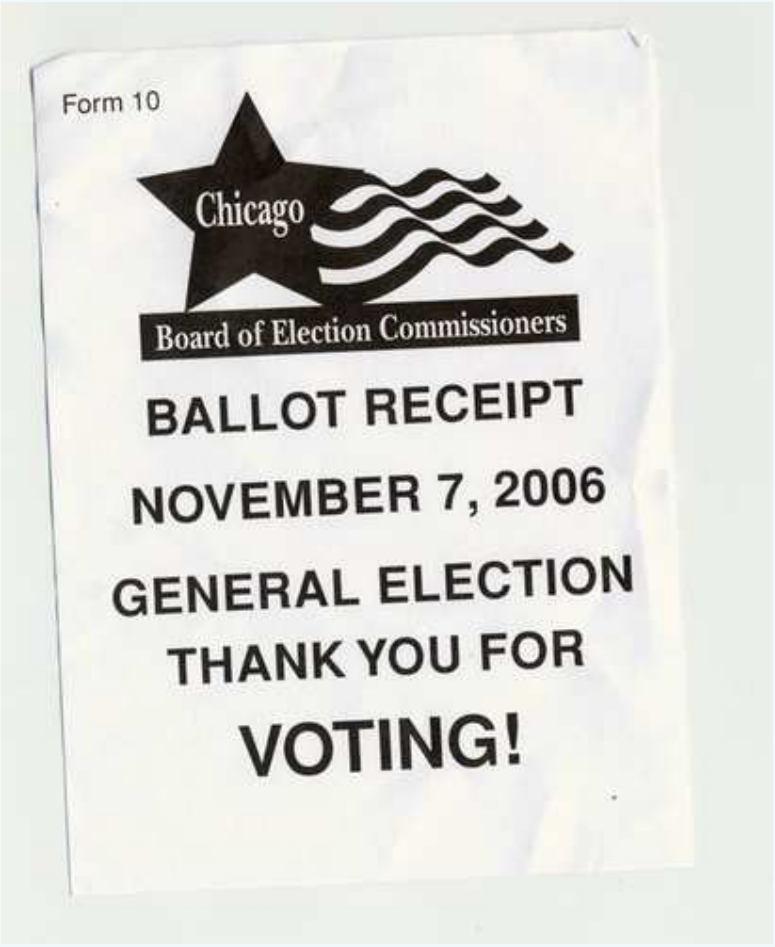
- DRE = **D**irect **R**ecording **E**lectronic (voting machine)

Diebold (USA)

Nedap (NL)

Actual election terminology

- VVPAT = **V**oter **V**erified **P**aper **A**udit **T**rail



Actual election terminology

- HAVA = **H**elp **A**merica **V**ote **A**ct

Actual election terminology

- chain of custody

Requirements

- **eligibility**
  only individuals belonging to the group may vote.

- **democracy**
  only eligible voters may vote, and they may only vote once.

- **accuracy**
  - result depends on *all* cast votes,
  - result depends on *nothing more* than cast votes,
  - result depends on cast votes *as they were cast*.

- **fairness**
  no intermediate results.

Requirements - verifiability

- **universal verifiability**
  given the set of cast votes, anyone can verify that the announced result is correct.

- **individual verifiability**
  a voter can verify that her vote counts for the correct candidate.

- **eligibility verifiability**
  anyone can verify that the set of cast votes originates only from eligible voters.

Requirements - privacy

- **anonymity**
  no observer can learn how a voter voted.

- **receipt-freeness**
  the voter cannot prove how she voted.

- **coercion-resistance (JCJ05)**

  receipt-freeness + resistance to:

  - forced randomised voting,
  - forced abstention,
  - voting in the voter's stead.

Requirements - end-to-end

End-to-end verifiability:

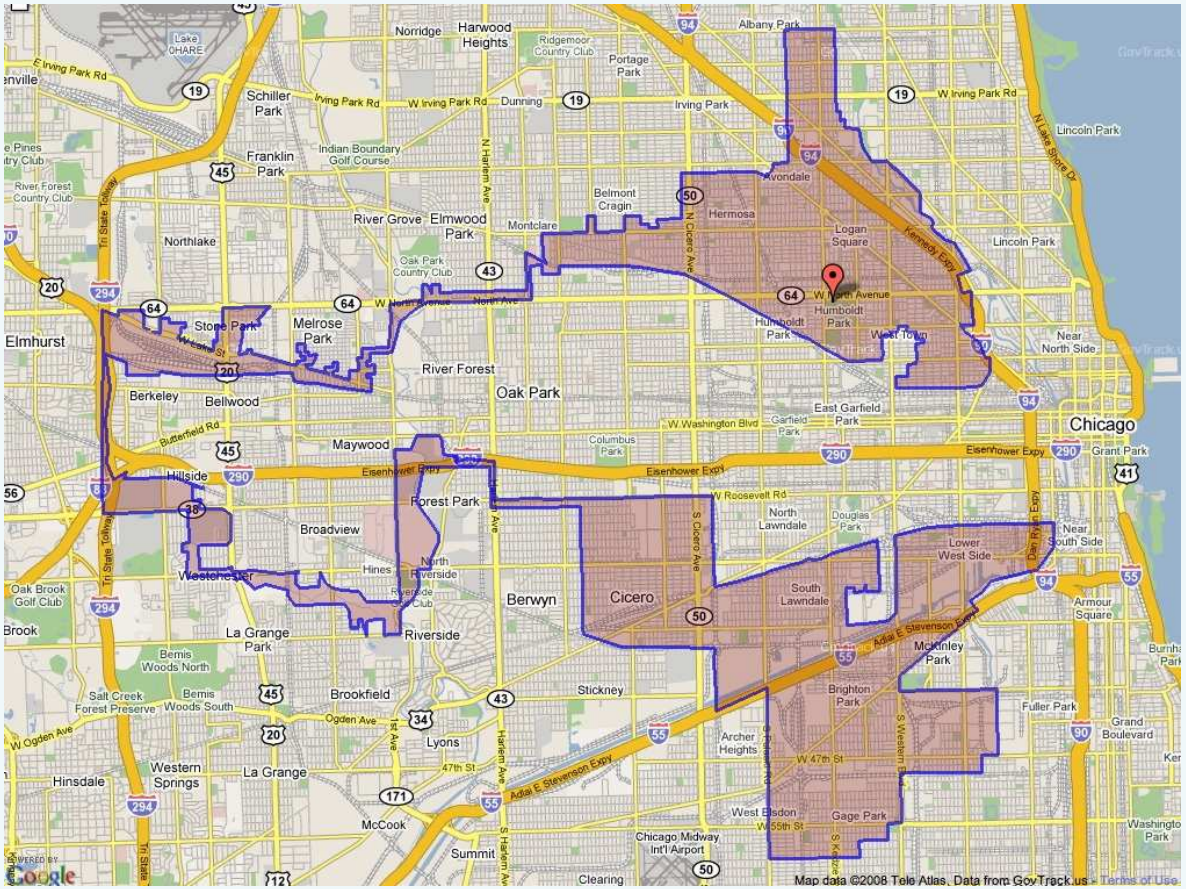
- **cast-as-intended** a voter can verify that her input to the process matches her intent.
- **recorded-as-cast** a voter can verify that the record of her vote matches what she gave as input.
- **tallied-as-recorded** anyone can verify that the announced result matches the public records of votes cast.
- **counted-as-cast** a voter can verify that her vote counts in favour of the candidate for whom she cast it.

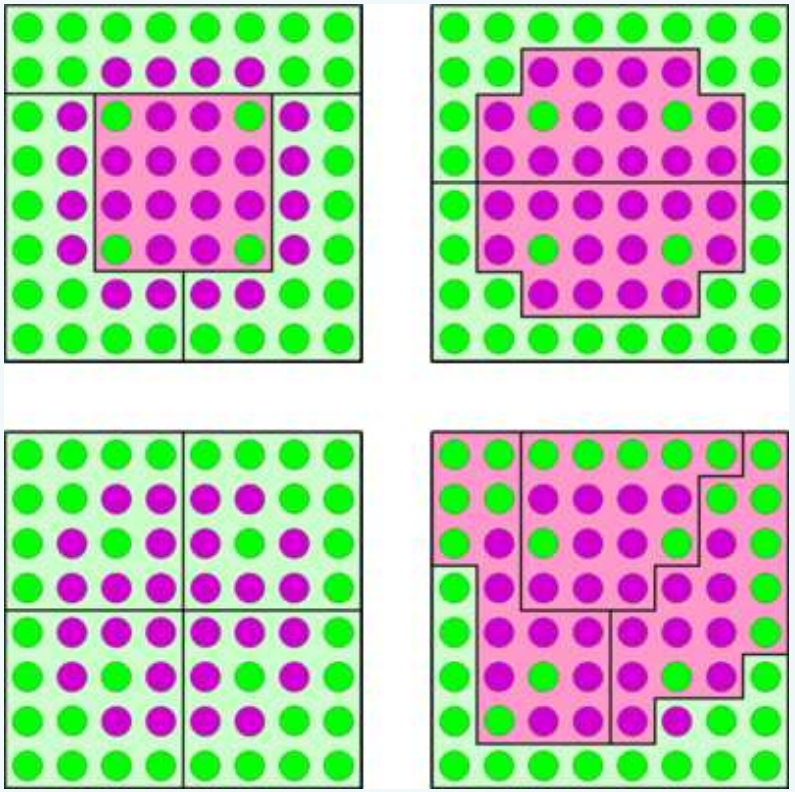
Attacks

- ~~Italian~~Luxembourgian attack.
- chain voting.

Attacks

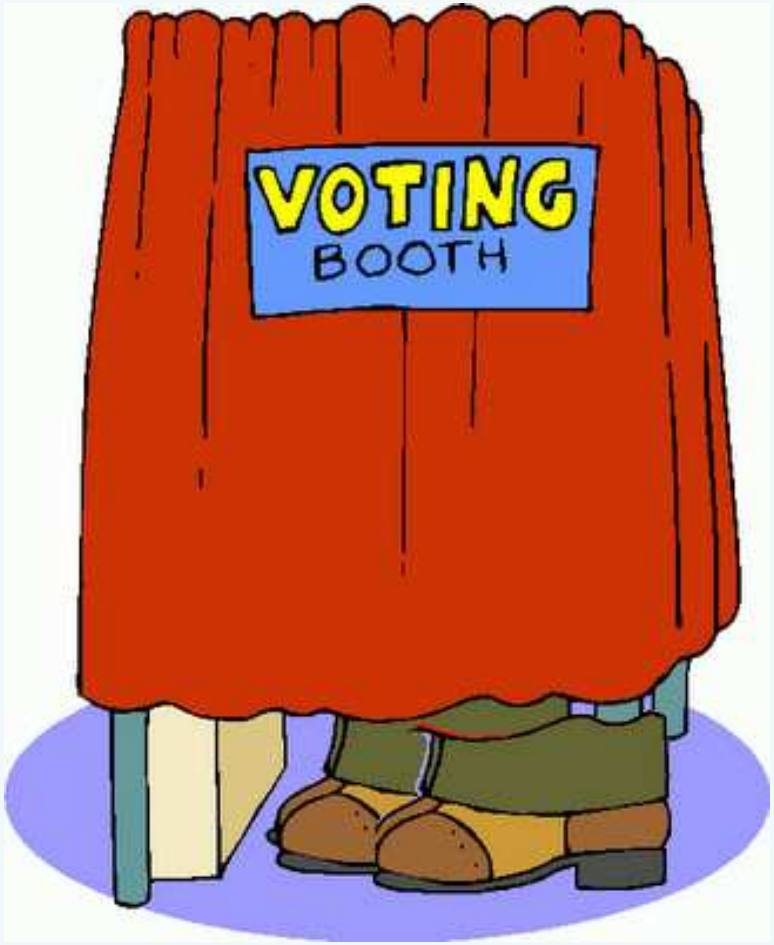
- gerrymandering.





Attacks

- Family voting.



Attacks

- chain voting.

Cryptography

- blind signatures:

$$deblind(sign_A(blind(msg, k))) = sign_A(msg).$$

- homomorphic encryption:

$$enc(msg_a, k) \otimes enc(msg_b, k) = enc(msg_a \oplus msg_b, k).$$

  - RSA78
  - ElGamal85
  - Paillier99
  - ...

Cryptography

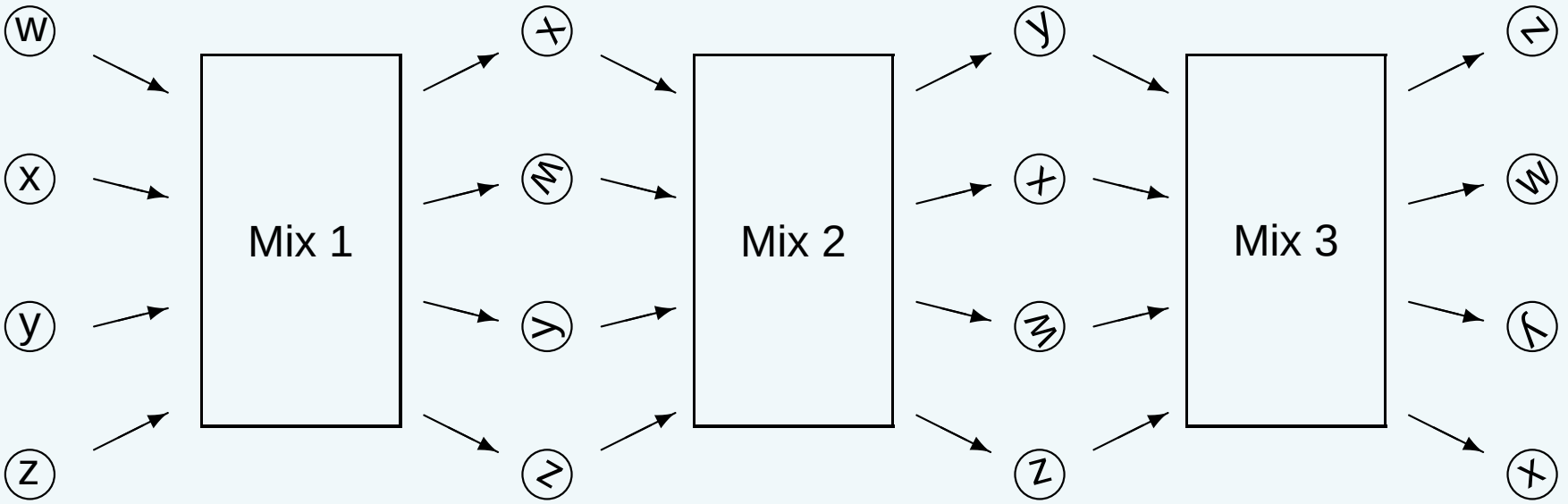
- commitments.
- proofs:
  - (interactive) Zero Knowledge Proof (ZKP)
  - Designated Verifier Proofs (DVP)
- Fiat-Shamir heuristic:

  Make interactive proofs non-interactive.

Cryptography

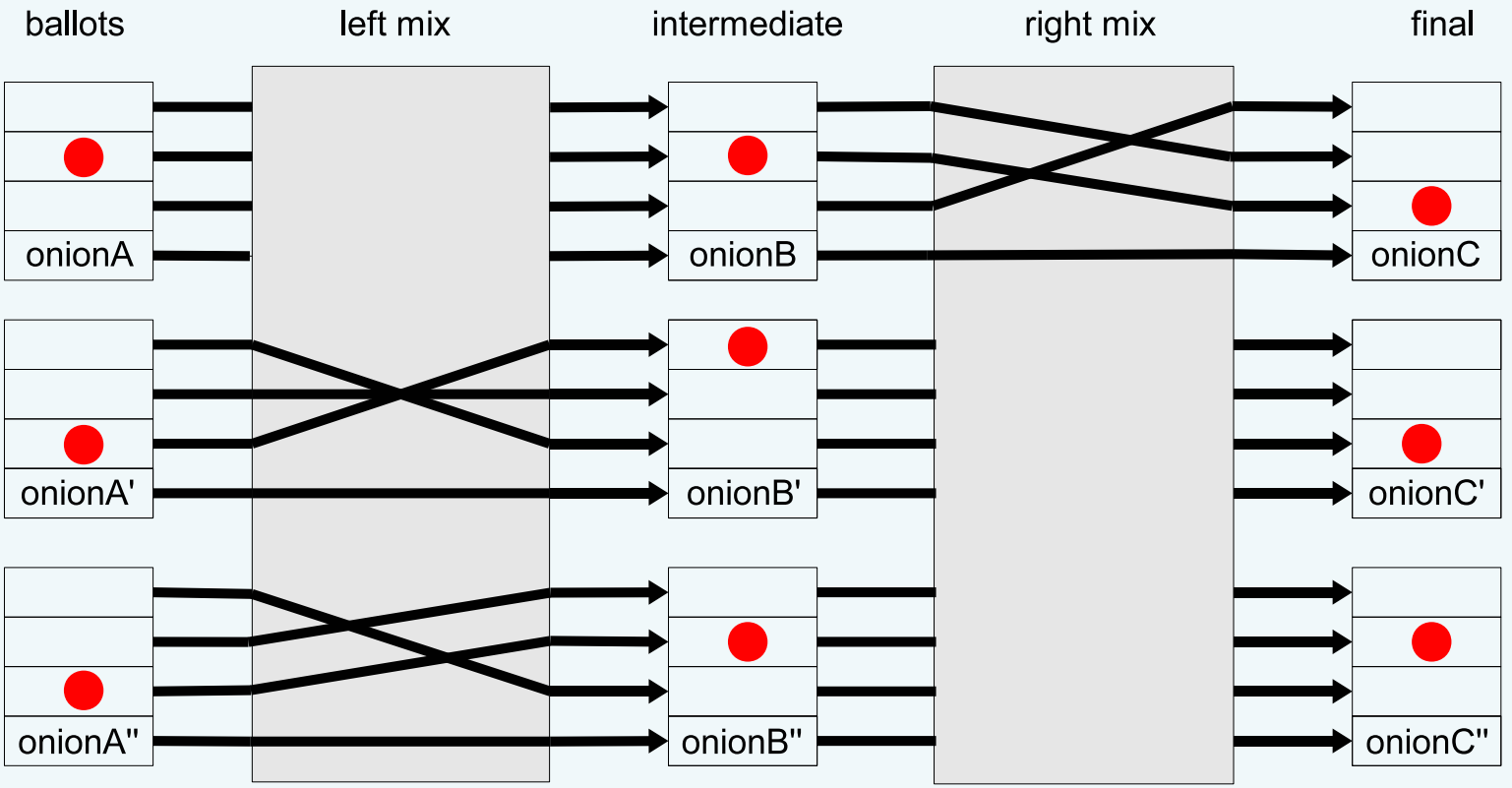
- Plaintext Equivalence Test:
  $enc(msg_a, k) \stackrel{?}{=} enc(msg_b, k)$.
- Plaintext Inequivalence Test:
  $enc(msg_a, k) \stackrel{?}{<} enc(msg_b, k)$.

- Mixnets



— adapted from [HS00]

- Randomized Partial Auditing / Checking [JJR02]



How to fill in the ballot / determining the winner

- Plurality voting (single winner)
- FPTP = **F**irst **P**ast **T**he **P**ost
  winner = candidate with most votes.
- Instant Runoff / Alternative Vote
- Approval voting
- Range voting
- Condorcet
  Winner = pairwise most preferred candidate.
- Borda count
  rank candidates, most preferred wins.

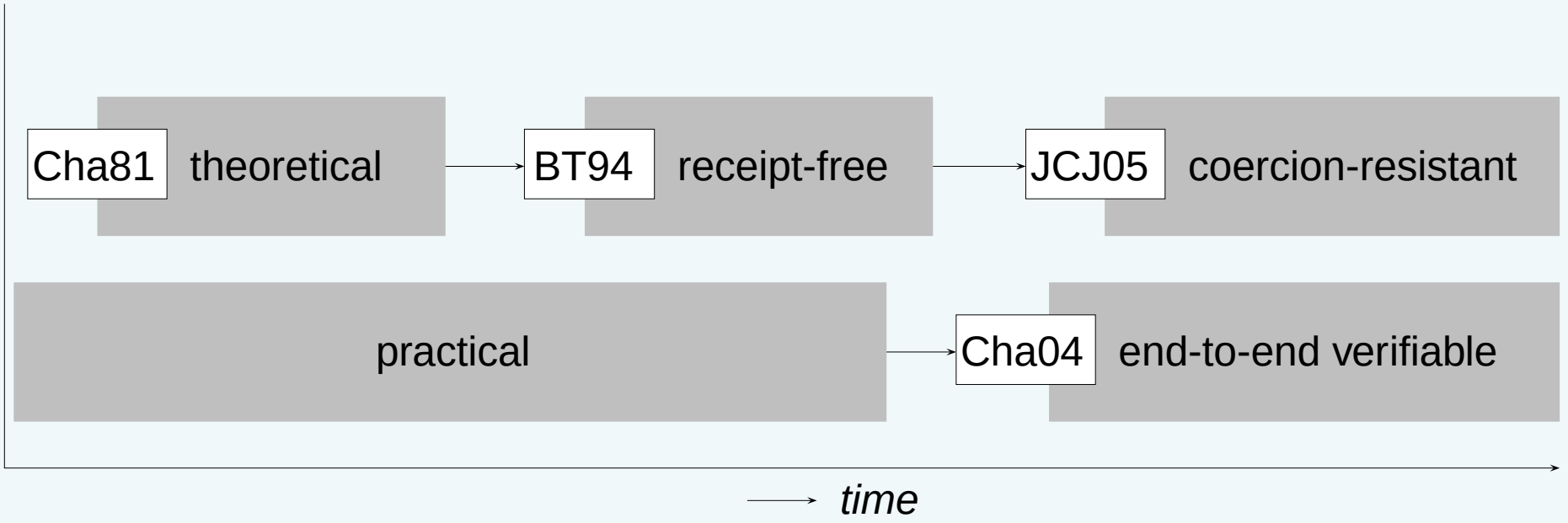
Determining the winner

- Arrow's Theorem

  No system such that:

  - if every voter prefers A to B, then the group prefers A to B.
  - if no voter's preference between A and B is changed if C is added, then the group's preference between A and B also remains unchanged.
  - no single voter can determine the group's preference.

Some influential systems



Theoretical:

- **Chaum81**
- FOO92
- CFSY96
- CGS97
  - Helios

RF / CR:

- **BT94**
- SK95
- HS00
- JCJ05
  - Civitas

End-to-end:

- Chaum04
- Prêt à Voter
- Punchscan
- Scantegrity (I, II)
- Code Voting

Done!

Thanks for your attention!