Voting for IACR

Some low-tech options

Antoine Joux
Current voting system

Send ballots to voters

Ballot → Inner env. → Signed env.

Count ballots
Announce results

Election officers
Weaknesses and Vulnerabilities

- Few returned ballots (many late/lost ?)
- Vote coercion/buying/stealing easy
  - But may be irrelevant, could create new members
- Cost of system (postal fees for IACR and members)
- Workload for election officers
- Need to trust election officers
  - For correctness and anonymity
Possible hybrid system

Individual ballot
- Number
  - X: OTP
  - Y: OTP ...
  - (+abstain)

Mix and Send to voters (snail mail)

Web interface
- Enter ballot number
- Enter OTP for each vote
  - (possible including abstain(s))

Online web interface

Voter

Offline Archive/Counting
Quick security facts

- Need to trust mixing
- Need to trust outgoing postal service
  - Intercepted ballots can be used by Adversary
- Vote Coercion/Buying still possible
- Viruses on user's computer useless
  - Except to attack availability
Possible additional security measures

- Error detection to help OTP input
- Allow returning ballots by snail-mail for improved availability
- Return signed receipts to user to allow checking that ballots indeed arrived
- Write received ballots on write-only devices

- **Careful counting** (remove invalid votes, remove exact duplicates, cancel multiple voting, priority to snail-mail ballots)
Motivations

• Simple scheme to benchmark proposals
  – Security, cost, ...

• Removes need for securing computing device on user's side

• Clearly unsuitable for political elections (do not scale, easy coercion, ...)

• This is fun but probably not original
  – references anyone?