Applications of CloudProxy

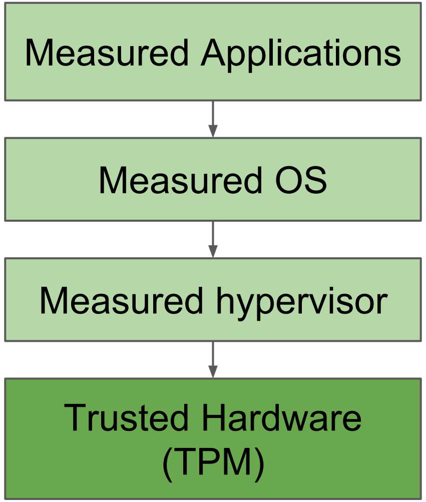
(Albert’s intern projects)

Albert Kwon, Sid Telang, John Manferdelli

11/28/16

CloudProxy

- Recursive protection of applications
  - Root of trust in hardware (TPM)
- “Trustworthy” computing
  - Attest the whole stack
- Main objectives
  - Develop CloudProxy applications
  - Security audit



Outline

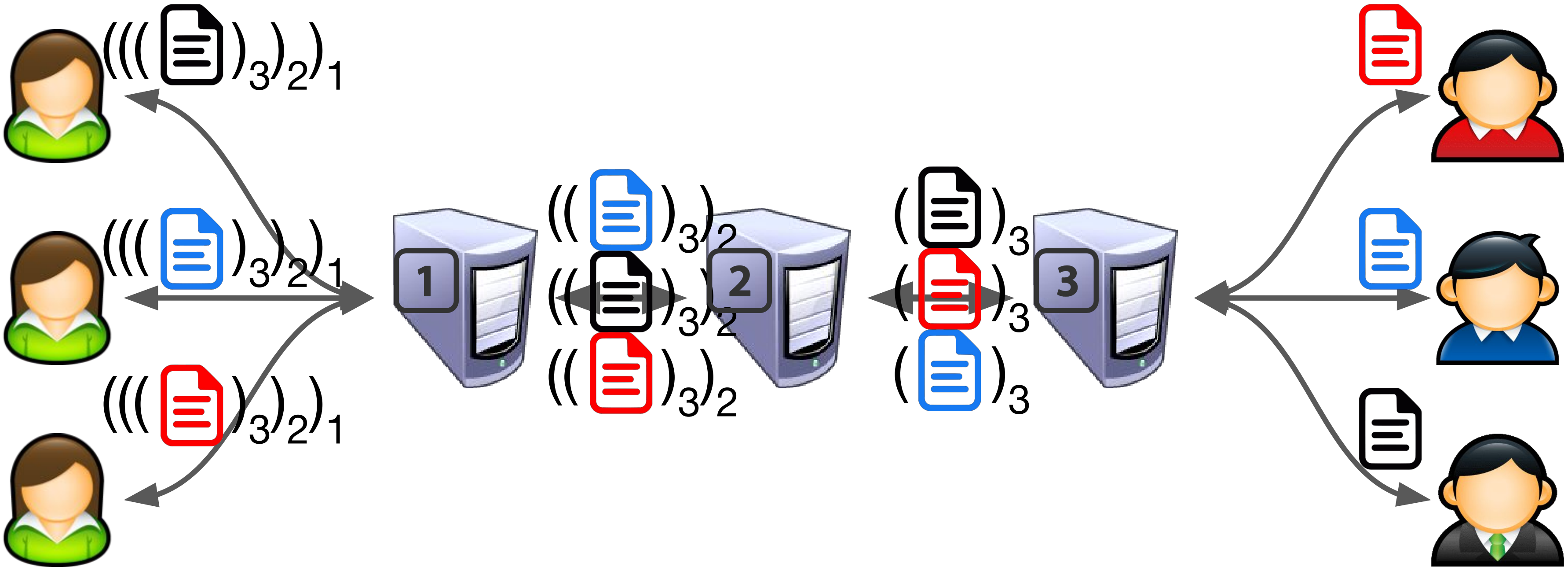
- Mix-networks
- Time on CloudProxy
- Ongoing & Future work

Mix-network

- Network of servers that collects and “mixes” messages
- Provides sender anonymity for the users

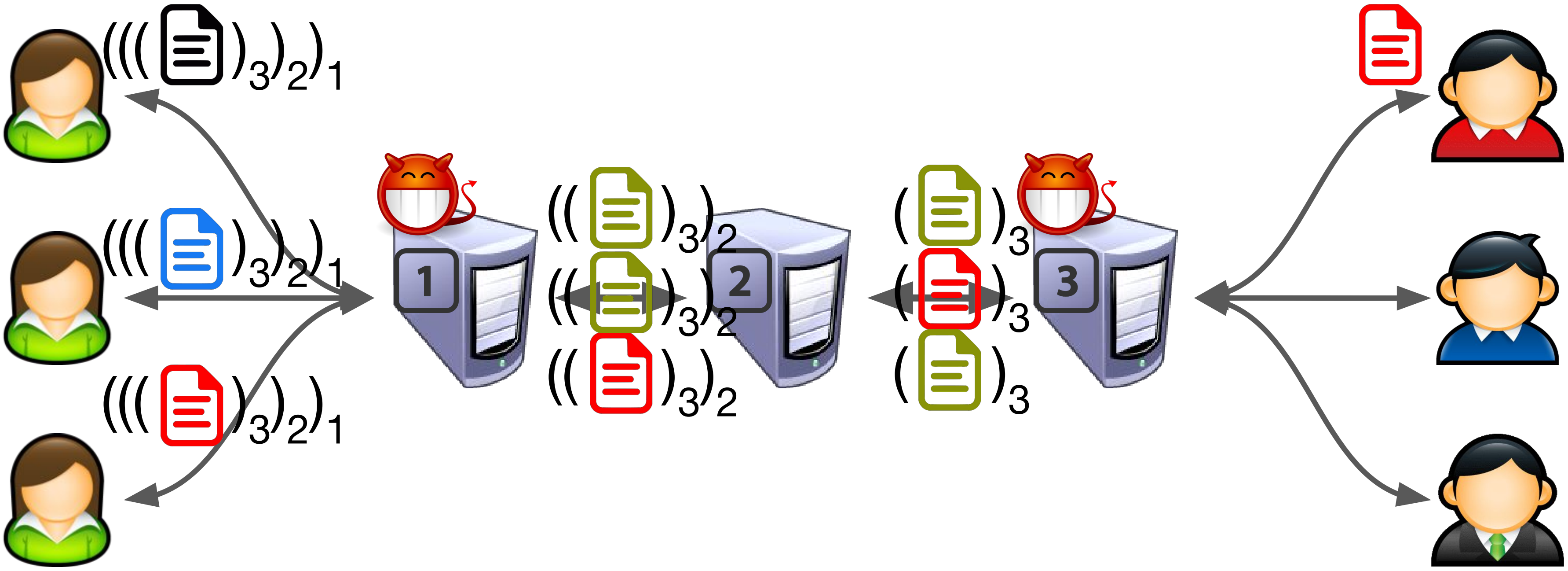
Cascade Mix-network

$(\quad)_j$: pub key enc for server j

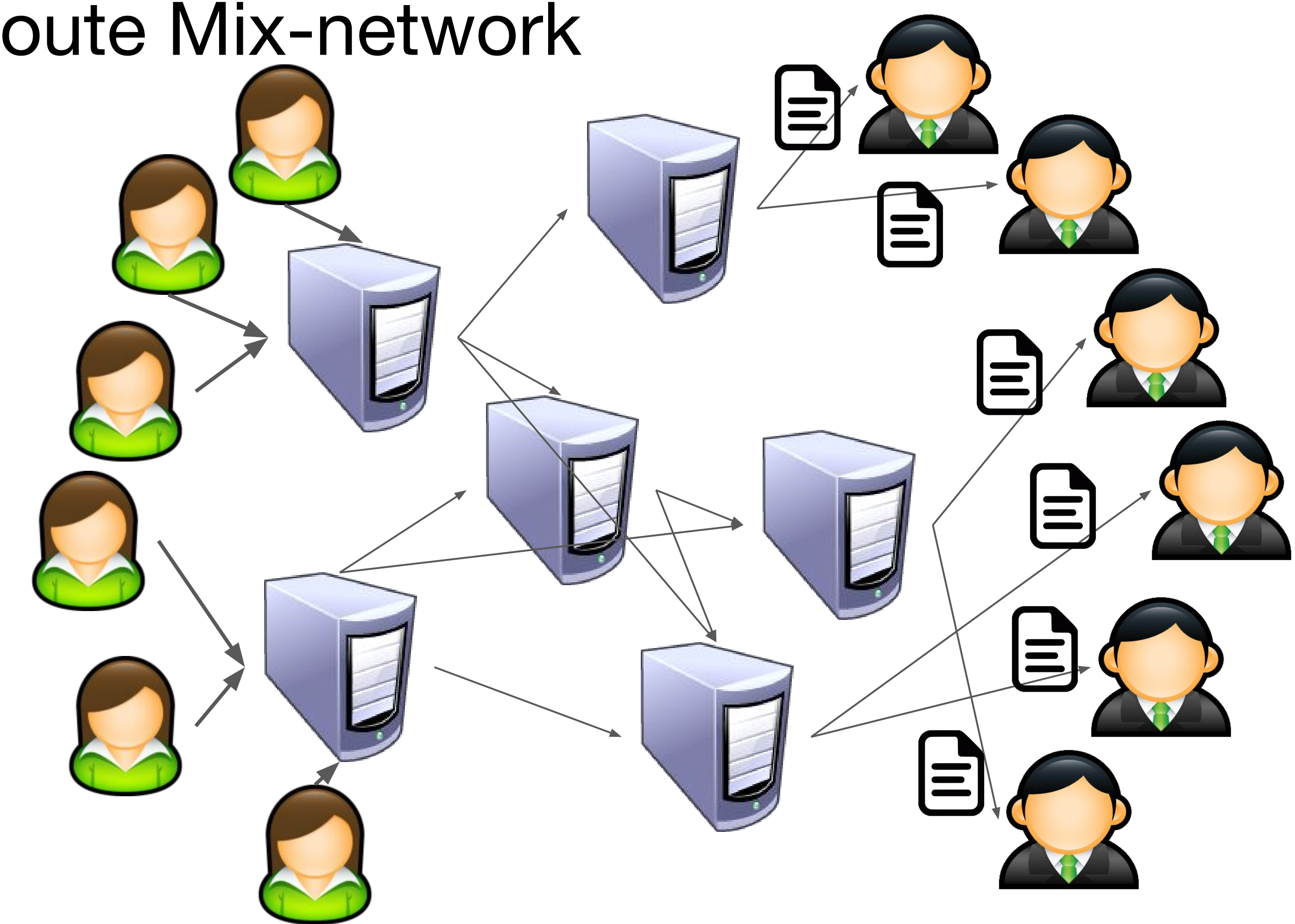


Cascade Mix-network

( )$_j$: pub key enc for server j



Free-route Mix-network



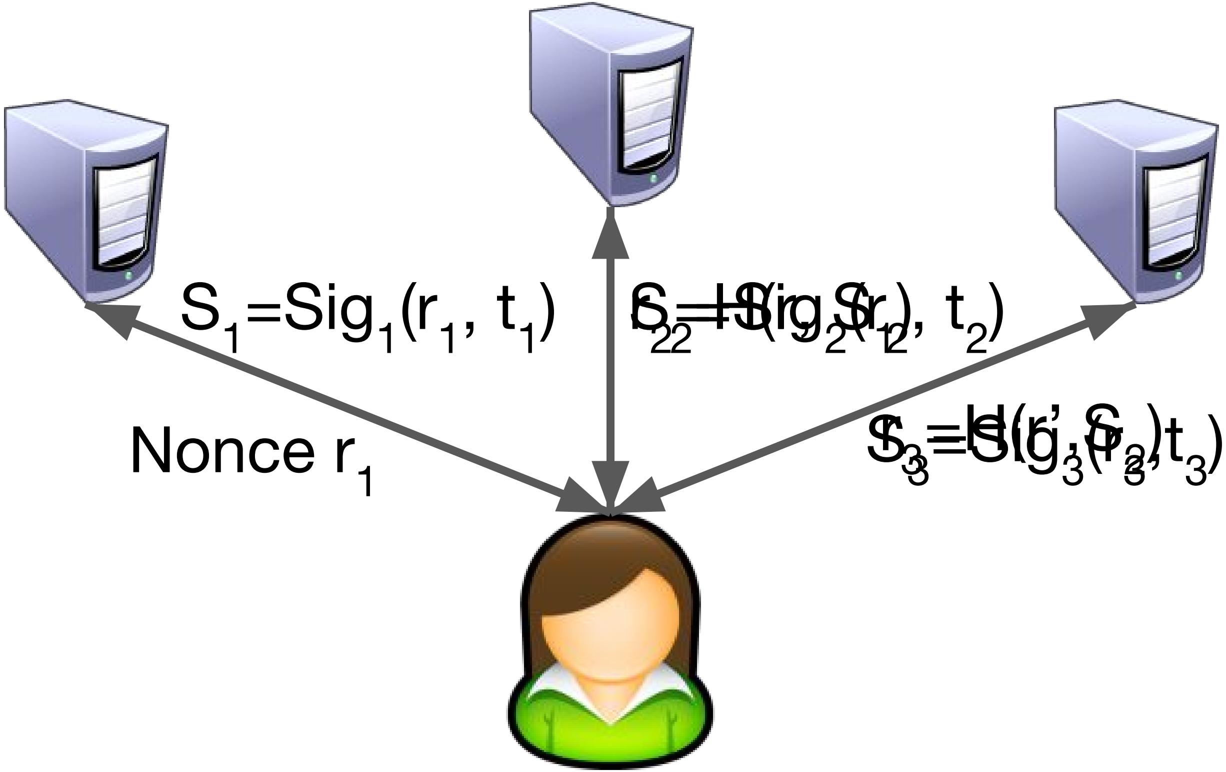
Mix-network Status

- Implemented in Go
- Tested on Google Cloud Platform
- Academic paper coming

Trustworthy Time: Server

- Many application depends on time
  - E.g., ~25% of Chrome certificate error from wrong client time
- NTP is not very secure
  - No good way to cross-verify
- Adam Langley's Roughtime
  - Signed responses of servers
  - Can detect when the servers misbehave

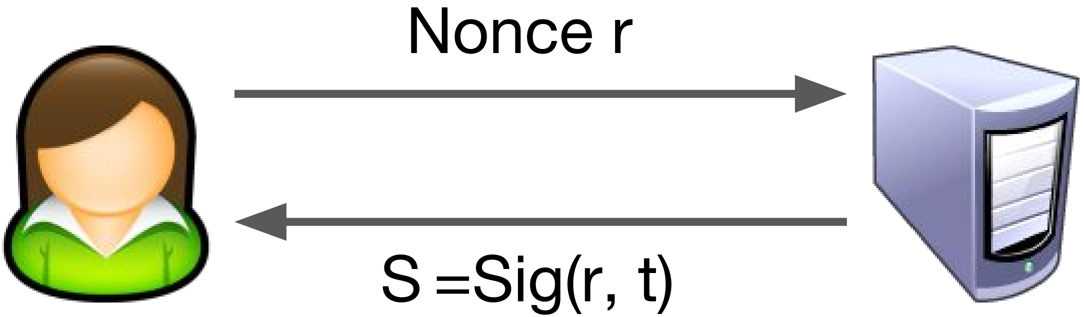
Roughtime



S_1=Sig$_1$(r_1, t_1)
S_2=Sig$_2$(r_2, t_2)
r_2=H(r', S_1)
Nonce r_1
r_3=H(r', S_2)
S_3=Sig$_3$(r_3, t_3)

Roughtime on CloudProxy

- Only needs to communicate with one server
- Could probe multiple servers for accuracy
- Written in Go

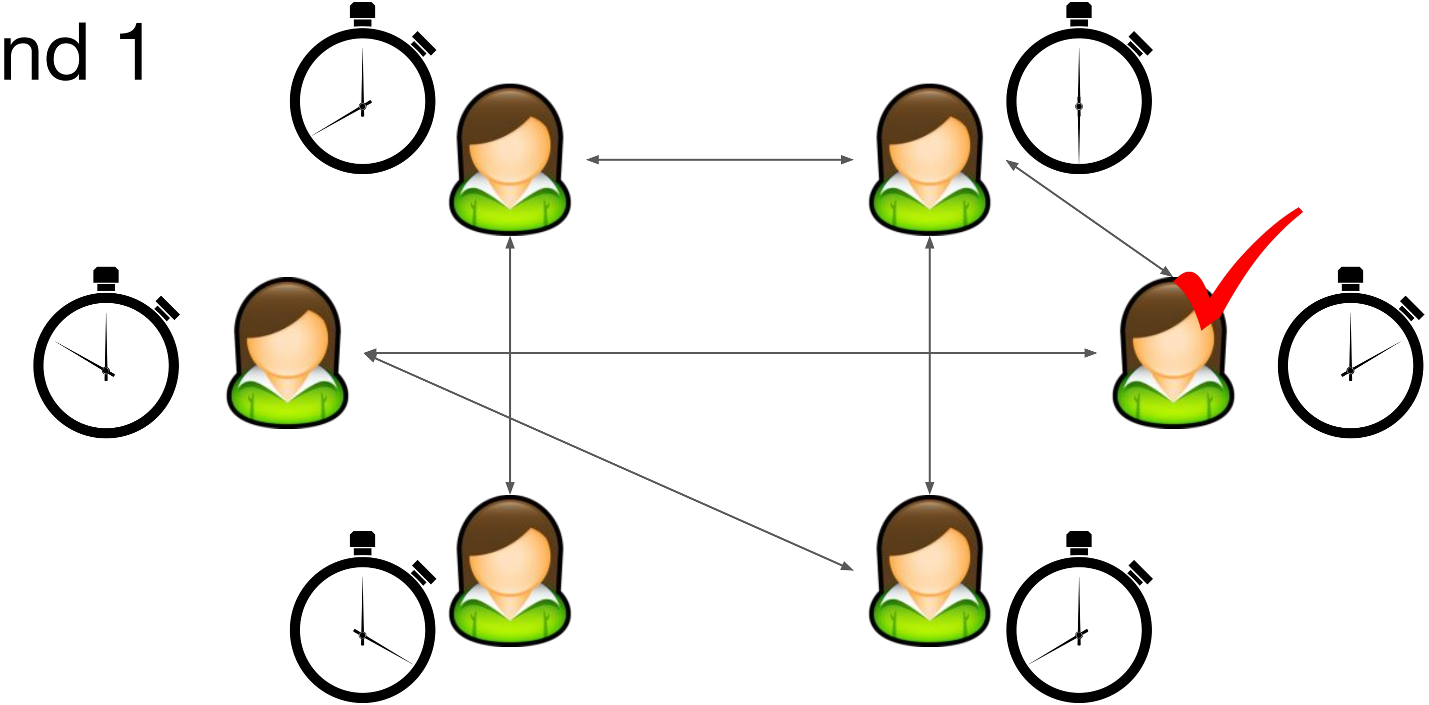


Trustworthy Time: Clients

- What can we do if clients/users are trustworthy?
- Distributed permissionless consensus protocol
  - Leader election
  - Replace proof-of-work with “proof-of-elapsed-time”

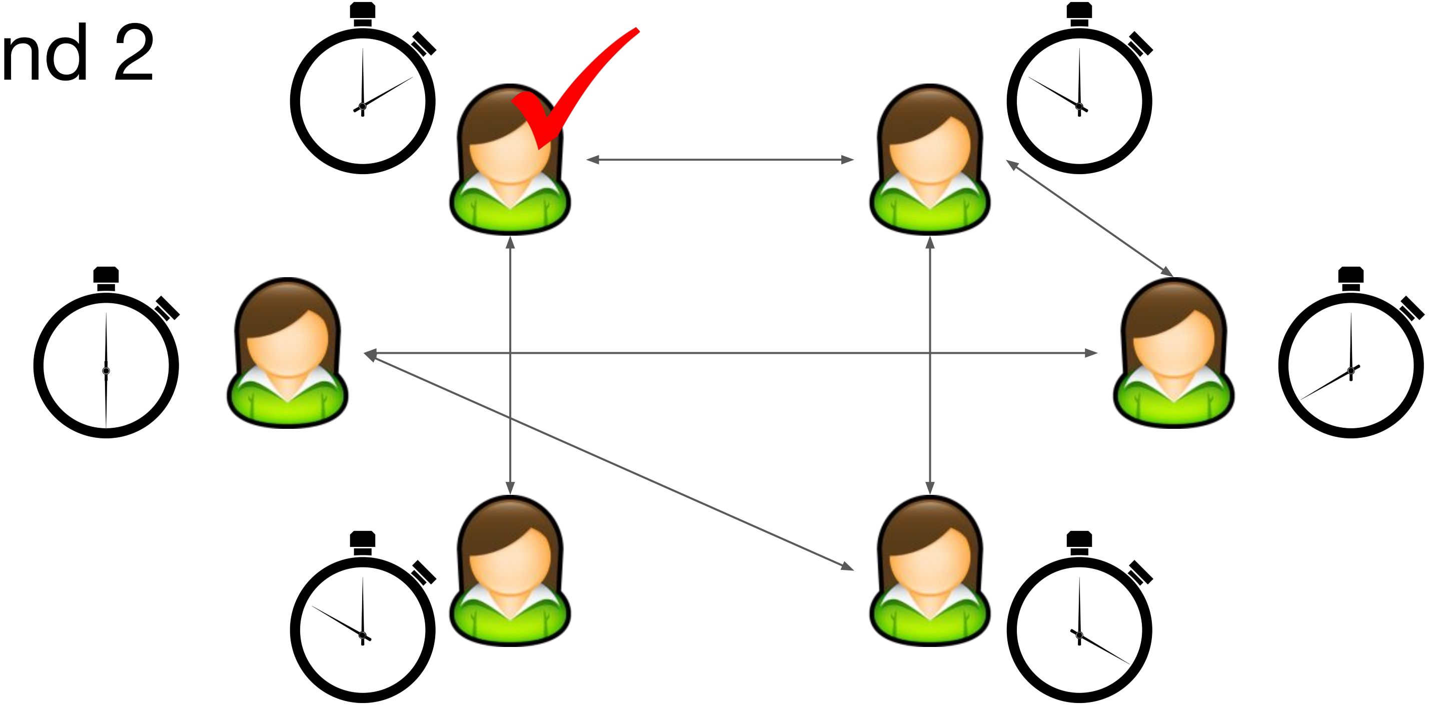
Proof-of-Elapsed-Time

Round 1



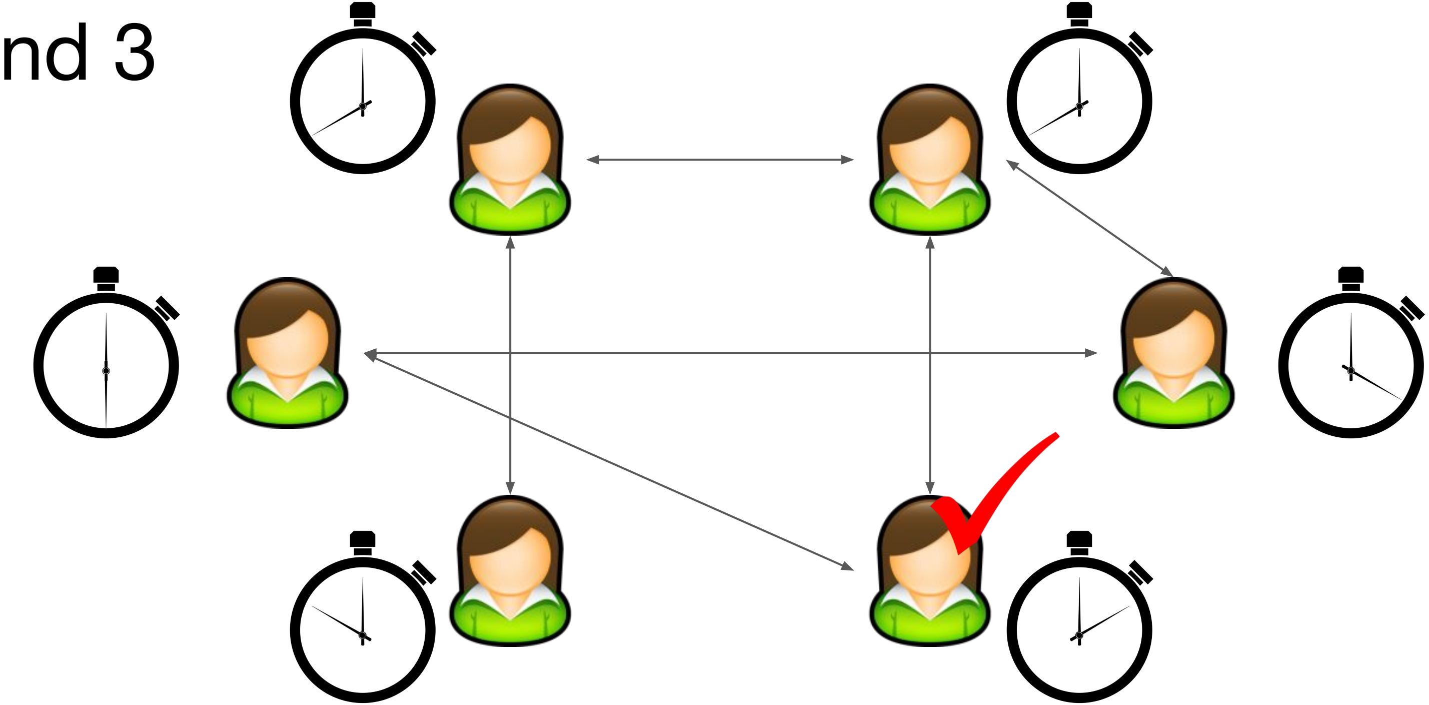
Proof-of-Elapsed-Time

Round 2



Proof-of-Elapsed-Time

Round 3



PoET Status

- Simple proof-of-concept done
- Tested locally for 100s of clients
- Tested across machines for ~20 clients

What’s next?

- Mix-net paper
- Documentation
- Security audit