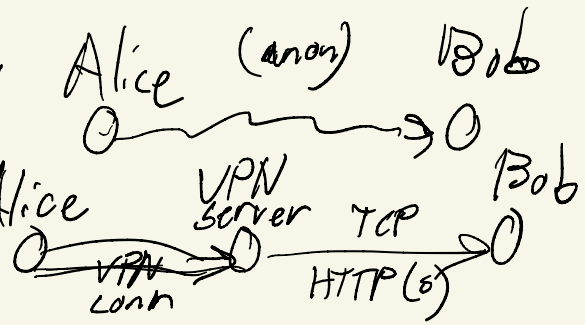
CS-438 Decentralized Systems Engineering

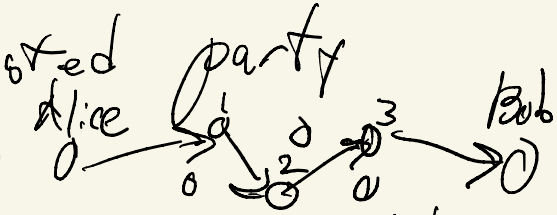
Week 11

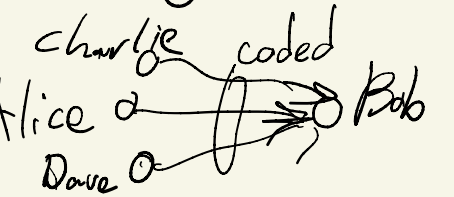
Anonymous Communication

Motivations:
- political dissidents (in authoritarian regime)
- isolate work & personal
- protect freedoms of speech, association
- voting: ballots are anonymous
- hide criminal activity from law enforcement

Approaches:
- "Natural" anonymity: "feel" of anonymity
- IP addresses, phone numbers, ...
- Proxies, Virtual Private Network (VPN)
  weakness: proxy is a centralized, trusted party
- Multi-hop relaying: MIX-nets Tor (onion routing) (David Chaum)
- Dining Cryptographers (DC-nets): information coding

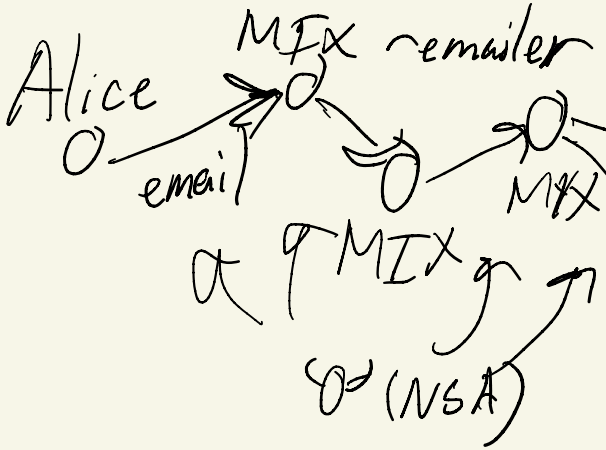






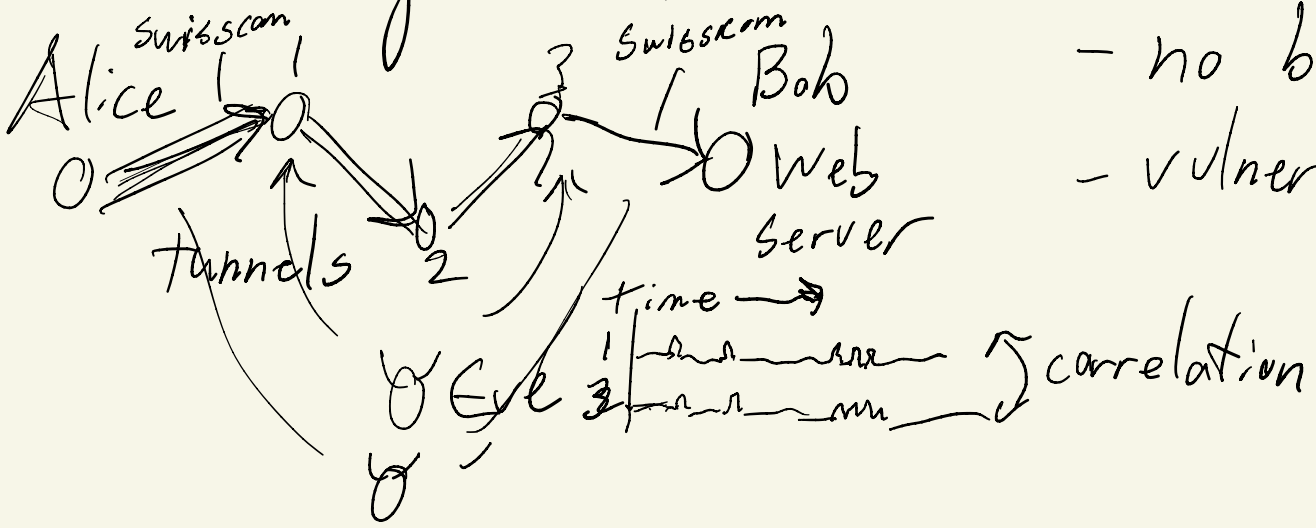
Relaying approaches

- MIX-nets (Chaum): high-latency, delay-tolerant messages ("USENET, Email")



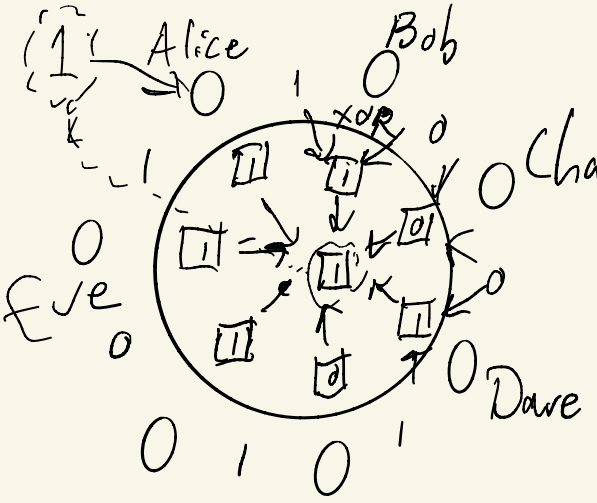
- low trust in each MIX
- traffic analysis resistance
- batching, delays
- low usability (non-interactive)

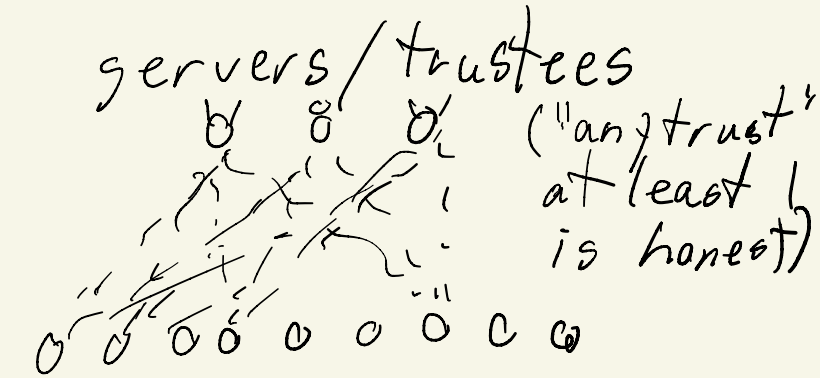
- Onion routing (Tor): low-latency, interactive (web)

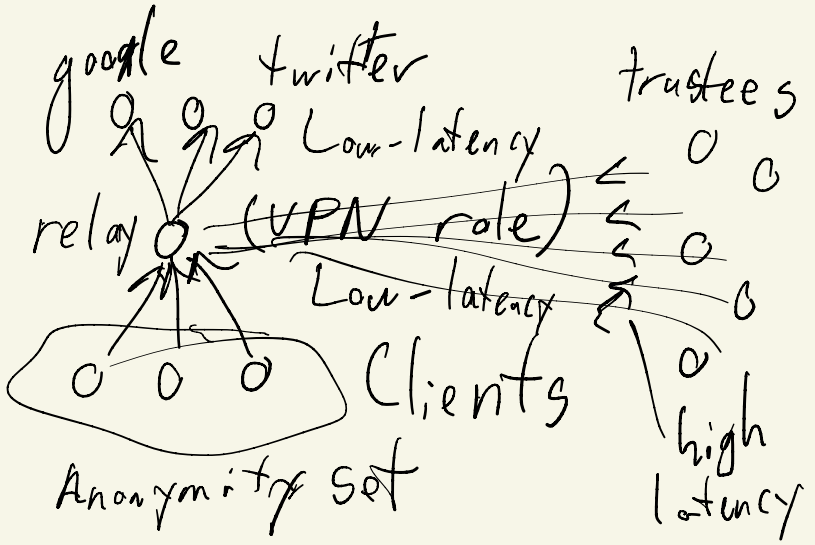


- no batching, added delays
- vulnerable to traffic analysis (by adversaries w/ multiple vantage points)

Information coding: Dining Cryptographers (DC-nets)







- Multiple bits? - use larger symbols
  - parallel instances
- Anyone can lie - disruption - XOR in random bits
  - (re)form different groups, see which groups "work"
  - intersection attack
  - "trap" or "blame" mechanisms w/ anonymous scheduling
  - Zero-knowledge proofs (verdict)
- Security: want all-to-all coin sharing
  - $O(n^2)$ - less scalable
- Promise: low-latency DC-nets?
  - PriFi (Ludovic Barman et al)