# CS-234
# Technologies for societal self-organization

## Week 10

# Technologies for identity & anonymity

Identification technologies:

- IP addresses, phone/SMS verification, ...
- KYC identity checking services, e-ID
- Social media identities, federated ID (tequila)
  login w/ Facebook, Google, etc

Anonymous communication

- Signal, WhatsApp, Telegram – pseudonymous (phone#) } weak
- SpeakUp, Piazza, 4chan, slashdot, ... }
- VPNs – trusted, centralized

Anonymous identity

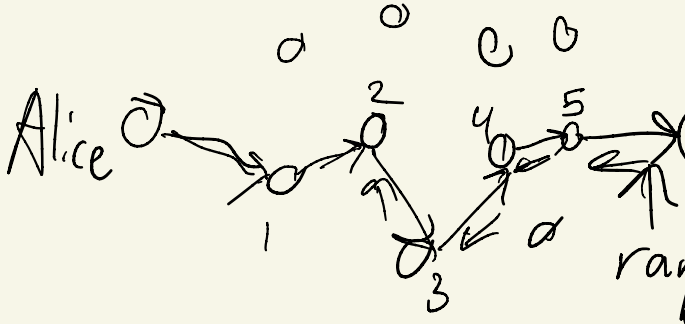
Anonymous reputation / currency

# Stronger anonymous communication

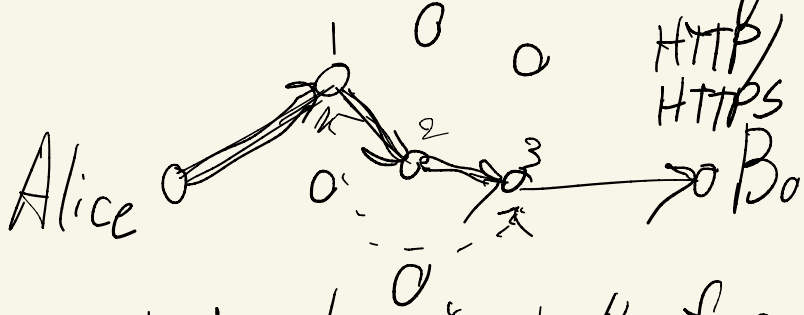
Mix networks – 1st-generation anonymous relaying
- David Chaum – message-oriented: USENET, Email

high-latency, delay-tolerant

goal: protection unless all relays compromized

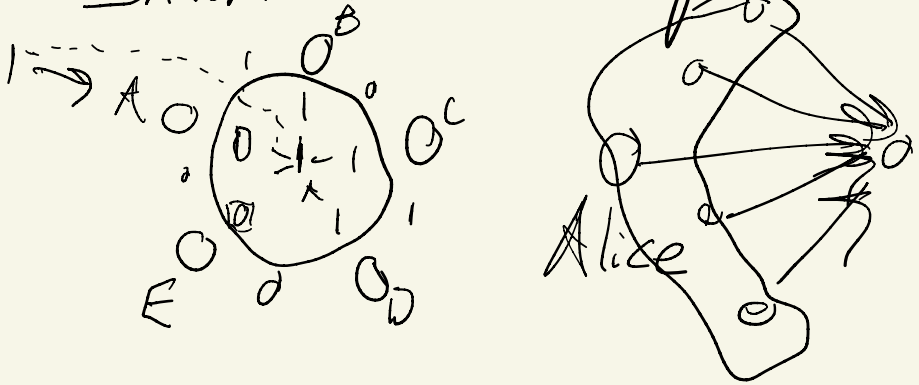



- Tor – onion routing – low latency, interactivity (Web)
  - no delays, batching
  - goal: protection against single compromised relay
  - vulnerable to traffic analysis



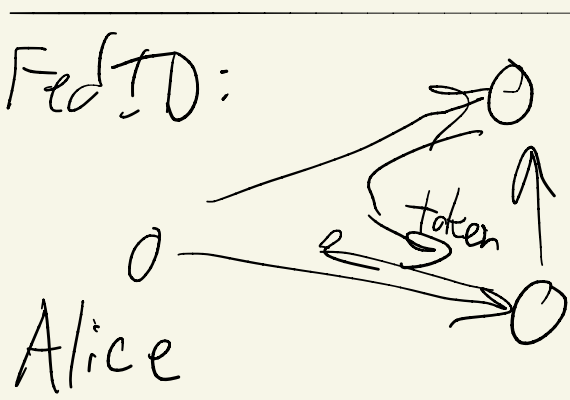

encrypted tunnels – "onion" of encryption

- Information coding – "Dining cryptographers" (David Chaum)
  - information-theoretic privacy
  - parallel, not serial



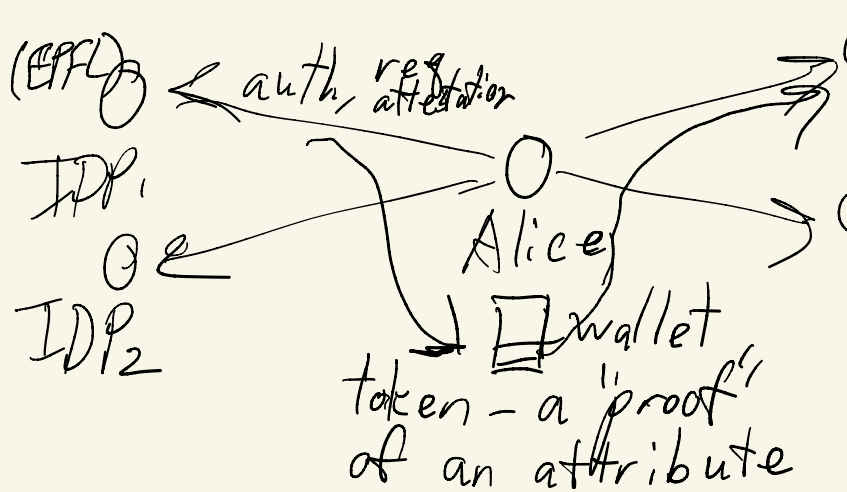
# Federated & self-sovereign ID

Fed ID:




token: attests
- that IDP "knows" you
- gives RP access to certain attributes

Self-sovereign ID: more decentralized, "user in charge"




- attributes:
  - name, address
  - age
  - degrees
  - citizenship
  - badges
  - ...

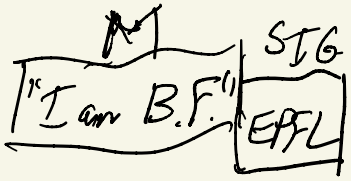
Sovrin, ...

Issues: Hacking / compromise / theft of wallet tokens
- time-limited tokens, revocation lists, blockchain

Backup / renewal after device loss
- reintroduce centralization

# Cryptographic signatures

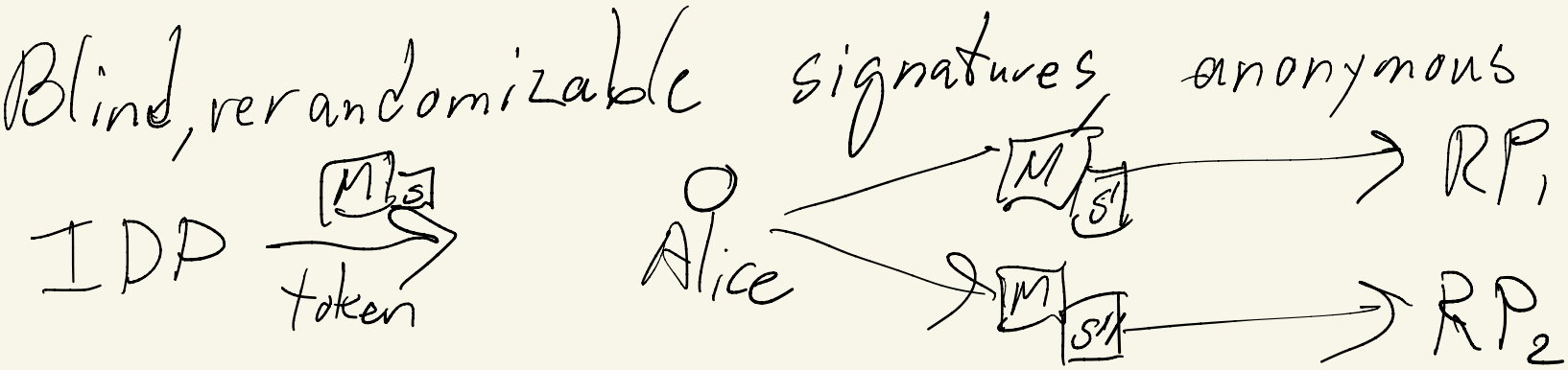
Basic: public/private key pair

Self-Sovereign ID: token = 

(IDP)

---

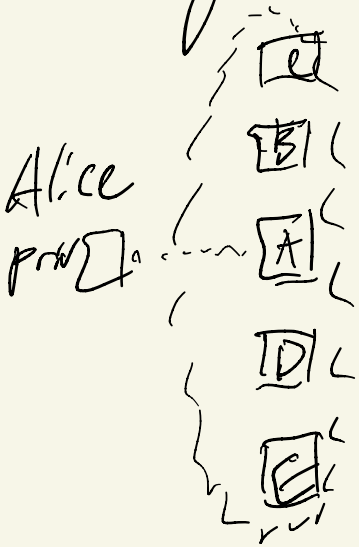
Blind, rerandomizable signatures, anonymous credentials




---

Ring signatures, linkable ring signatures

→ pseudonymous, 1-to-1




→ ring sig: proof that signer is an anonymous member of ring