# Empowering Anonymity: Delegatable Anonymous Credentials.

PI: Anna Lysyanskaya
Brown University

- Participants in a DelCred system: authorities and users
- What participants do: anonymously obtain credentials from authorities, anonymously delegate credentials to other users, anonymously prove possession of credentials.
- What was known:
  - DelCreds for long delegation chains from Groth-Sahai NIZK proofs and structure-preserving sigs [BCCKLS09,CKLM14]
  - DelCreds for short chains from general assumptions [CL06]
- What is needed:
  - Direct constructions that don't rely on NIZK
  - Incorporating credential attributes, conditional anonymity, revocation
  - Modular constructions from signature schemes with the "right" properties
- Our results so far:
  - Direct construction without NIZK [CL17]
  - Lends itself to attributes [CL17a]
  - New results on revocation of anonymous credentials [BCDLRSY17]