CFRG Agenda

- Introduction and Welcome
- CFRG status
- Hash-based passwords (15 minutes, Bellovin)
  - draft-bellovin-hpw-01
- Password Authenticated Key Exchange (25 minutes, Harkins)
- PAKE discussion (5 minutes)
- Ciphers in Use on the Internet (10 minutes, Shen)
  - draft-irtf-cfrg-cipher-catalog-00
- OCBv3 (20 minutes, Rogaway)
  - draft-krovetz-ocb-03
- Elliptic curve considerations (20 minutes, Struik)
- CFRG review of IETF uses of crypto (time permitting)