Published Attacks So Far

- What are the most worrying attacks on each of the finalists?
    - Distinguishers
    - Reduced-round collisions
    - Preimages
- Do any of these seriously call a finalist into question?
- What should we be learning about the finalists from these attacks?

Understanding the Security

- What finalists would you say are ***most*** understood, in security terms?
  - Security proofs?
  - Lots of cryptanalysis?
  - Similarity to other well-studied things?
  - Bounds on attacks?
- What finalists would you say are ***least*** understood, in security terms?
  - Are some designs inherently hard to analyze?
  - Are some too complex to ever be understood?

Side Channels

- Which finalists have the ***most serious*** problems with side-channels?
  - Grostl without AES instructions?
  - ARX?
- Which finalists are ***least worrying*** w.r.t. side channel attacks?
- How much should we worry about this?
  - Is it really just an implementation issue?

SHA-3 Selection

- Should we try to get something very different from SHA-2?
  - In performance profile?
  - In terms of internal operations?
- Should we care about extras?
  - Big tweakable block cipher
  - Authenticated encryption mode

Questions for the Audience

- Are there any finalists we explicitly shouldn't pick?
    - Now's the time to make your case!
- What are we missing?
    - What should we be thinking about that we haven't discussed?
- Individual designers: Other than your algorithm, what would you pick?
- Non-designer, non-NIST people: What candidate would you pick if it were your choice?