Desiderata for Future Hash Functions

1. Research agenda for future hash functions?
   - Compression functions - “Provably secure” vs heuristic methods?
   - Iterative structures – Any improvements on Merkle-Damgård’s?
     - Parallelize; block length extension; resist multicollisions; prevent second pre-image and herding attacks, etc.
   - Countermeasures - Which are necessary for the future hash functions?
     - Dithering, output truncation, randomize, etc.
   - Other criteria – What should we explicitly specify for future hash functions?
2. Do we know enough yet?
   - Arguably, we began the AES process in 1997 knowing more about block ciphers than we know about hashes today
3. What is the best approach to develop the future hash standards?
   - A competition? What is the alternative?
   - How often does an implementation life cycle allow us to replace hash function?
   - Do we need alternative hash algorithms as a back up for the future attacks?
     - Can we make hash functions different enough to resist similar attacks?