The Transition from Classical to Post-Quantum Cryptography: draft-hoffman-c2pq

Paul Hoffman, ICANN
IETF 99, Prague, July 2017
Why the CFRG might care

• There is lots of good discussion of what algorithms the world should use to thwart future attacks from large-scale quantum computers

• There is an amazing dearth of discussion about when those computers might actually come into existence and, when they do, what the costs of running them will be

• Changing algorithms, particularly signing algorithms, is expensive and error-prone
draft-hoffman-c2pq

• **Is not** about post-quantum algorithms; **only** addresses the timing needed for the transition
• Addresses many audiences:
  – Execs who want to understand when the transition needs to happen
  – Security experts who want deeper information about how much quantum computers that can attack crypto will cost and how fast they can break keys
  – Cryptographers (and physicists!) who want something readable to point people to
The current draft is quite incomplete

- There are whole sections that need to be filled in with material and references
- It does not yet address the wide disparity in guesses that people have made about when some adversaries might be able to create an attack computer
- It might be too early to give any useful guesses, but we can at least be honest about that
Proposed way forward

• Adopt this as a CFRG work item
• I bug people people to fill in holes and suggest new parts
• Have it informally discussed at pqc events and general crypto meetings
• Finish in a year or so?
• Return to it some years later if we have better research on the difficulty of building large-scale quantum computers