The Transition from Classical to Post-Quantum Cryptography: draft-hoffman-c2pq-02

Paul Hoffman, ICANN

IETF 100, Singapore, 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

Changes since IETF 99

- -02 is based on lots of good input from a few dedicated reviewers
- The draft was announced at the rump session at Crypto in Santa Barbara
- Little has happened since, even though there are still many noted holes in the draft

But it needs more

- Is there interest in CFRG in this type of work?
  - CFRG (and the IETF) don’t talk about “when” very often
- Do people who understand Shor’s algorithm and the recent papers want to help?

Proposed way forward

- Adopt this as a CFRG work item
- People in CFRG fill in holes and suggest new parts
- People in CFRG bug their colleagues 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