From: Moody, Dustin (Fed)
To: Kerman, Sara J. (Fed)
Cc: Chen, Lily (Fed); Perlner, Ray A. (Fed)
Subject: Links to FAQ
Date: Monday, July 18, 2016 11:15:54 AM

Sara,

Okay, I've described below the links that we can add into the CFP, that will link to the relevant question in the FAQ as Lily suggested. Since the CFP isn't completely final, I'm not sure how much you can do at this point, but this will probably be unaffected by what the lawyers give us. A quick google search seems to indicate we can create a link that points to a specific place within a pdf. Anyway:

- FAQ #1 (on hybrid modes). In the CFP, the last paragraph before Section 2 uses "hybrid modes" in quotes twice. Each of these should link to this FAQ question.
- FAQ #2 (rationale to convert time and space…). In Section 4.A.4, Target Security Strengths, there is a paragraph with the sentence "To make this statement precise, however, one must choose appropriate units for measuring computational complexity, memory requirements etc." I think this would be the best place for the link to this FAQ question.
- FAQ #3 (why are hash functions assigned fewer bits….). In Section 4.A.4, Target Security Strengths, there is a paragraph with the sentence "Likewise, parameter sets meeting security strengths 2 and 4 should remain secure roughly as long as brute-force collision attacks against SHA-256/ SHA3-256 and SHA-384/SHA3-384, respectively, remain infeasible." I think this is the best place for a link to this FAQ question.
- FAQ #4 (stateful hash-based signatures). In the fourth paragraph of Section 1, the term "hash-based signatures" is used. You can link it to this FAQ question .

Dustin