From: Moody, Dustin (Fed)
To: Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E. (Fed); Chen, Lily (Fed); Daniel Smith-Tone; Dworkin, Morris J. (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Peralta, Rene C. (Fed); Perlner, Ray A. (Fed); Smith-Tone, Daniel C. (Fed); Kelsey, John M. (Fed)
Cc: daniel-c.smith@louisville.edu
Subject: A few PQCrypto tidbits
Date: Monday, July 3, 2017 1:41:07 PM

Everyone,

Daniel, Ray, and I attended PQCrypto last week, and did a Q+A session for people to answer questions. While many of the questions were more straightforward to answer, there were a few that we thought merited some more discussion amongst ourselves. I'll probably schedule a meeting for next week (I believe Daniel will be here) to discuss some of these. Or feel free to add your thoughts via email. Some of them included:

- When will our 2nd workshop be?
- Can we give easy to understand definitions of who is owner, submitter, etc.. and who is required to sign (and who isn't)
- Should we recommend specific symmetric key primitives to limit the number of options? For example, is there ONE hash function we'd recommend to use?
- For the 2nd round, we have said that changes will be allowed, but no "major changes". What sort of changes will this be? Do the submitters need our blessing/permission on their changes?

We also talked a little with Dan about randombytes. He's still waiting for something from Larry (who's waiting for something from John?). Dan's concerned that using AES to expand the seed to get more bytes might not satisfy some people, as for some security proofs you need indifferentiability to use certain transforms, and AES doesn't give indifferentiability.

Dustin