From: Chen, Lily (Fed)
To: Moody, Dustin (Fed); internal-pqc; Kelsey, John M. (Fed)
Subject: RE: Here"s a second draft
Date: Wednesday, July 19, 2017 1:03:00 PM

I do not have further comments.

Thanks,

Lily

From: Moody, Dustin (Fed)
Sent: Wednesday, July 19, 2017 9:53 AM
To: internal-pqc <internal-pqc@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Subject: FW: Here's a second draft

Any comments? We will also still add:

"If the scheme uses a cryptographic primitive that has not been approved by NIST, the submitter shall provide an explanation for why a NIST-approved primitive would not be suitable."

From: Perlner, Ray (Fed)
Sent: Wednesday, July 19, 2017 9:50 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: FW: Here's a second draft

From: Perlner, Ray (Fed)
Sent: Wednesday, July 19, 2017 9:46 AM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Here's a second draft

Q: How should submitters choose symmetric algorithms for their submissions?

A: While NIST will permit submitters to choose any NIST approved cryptographic algorithm for their submission if they feel it is necessary to achieve the desired security and performance, a number of potential submitters have asked us to offer default options for common symmetric cryptographic primitives. As such, here are our suggestions:

1. Hash functions: SHA512 is likely sufficient to meet the requirements of any of our five security strength categories and gives good performance in software, especially for 64 bit architectures. Submitters seeking a variable length output, good performance in hardware, or

multiple input strings, may instead prefer to use TupleHash256 (specified in SP 800-185.)

2. XOFs: We would recommend SHAKE256
3. Authenticated encryption: We'd suggest AES256-GCM with a random IV.
4. PRFs: Where security proofs can accommodate something that is not indifferentiable from a random oracle, John's AES-based seed-expander will offer excellent performance. Otherwise, KMAC256 (specified in SP 800-185) will be a good choice.

From: Perlner, Ray (Fed)
Sent: Tuesday, July 18, 2017 5:17 PM
To: Moody, Dustin (dustin.moody@nist.gov) <dustin.moody@nist.gov>
Subject: Here's text summarizing what we said in our meeting. Note that John will need to expand on his advice regarding "seed expander"

Q: How should submitters choose symmetric algorithms for their submissions?

A: While NIST will permit submitters to choose any NIST approved cryptographic algorithm for their submission if they feel it is necessary to achieve the desired security and performance, a number of potential submitters have asked us to offer default options for common symmetric cryptographic primitives. As such, here are our suggestions:

1. Hash functions: SHA512 is likely sufficient to meet the requirements of any of our five security strength categories and gives good performance in software, especially for 64 bit architectures. Submitters seeking a variable length output or good performance in hardware may instead prefer to use SHAKE256.
2. Authenticated encryption: We'd suggest AES256-GCM with a random IV.
3. KDFs: Where security proofs can accommodate something that is not indifferentiable from a random oracle, John's AES-based seed-expander will offer excellent performance. Otherwise, KMAC256 will be a good choice.