From:	Chen, Lily (Fed)
To:	Moody, Dustin (Fed); Perlner, Ray A. (Fed); Liu, Yi-Kai (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc:	Peralta, Rene C. (Fed); Jordan, Stephen P (Fed); Bassham, Lawrence E. (Fed)
Subject:	Re: PQC docs
Date:	Wednesday, October 26, 2016 11:57:33 AM
Attachments:	llc-final CFP v4.docx

Attached please see my comments on CFPv4. I noticed that we added a fairly amount of details and explanations. The details and explanations help people understand what we are asking for. On the other hand, the details often need to be handled more carefully and think about the impacts. Here are two places I feel we shall check.

1. KEM concept. In the current draft, we consider an ephemeral DH like scheme (e.g. New Hope) as a KEM. Then converting KEM to a public-key encryption is not intuitive at all. I cannot see why we need it other than security proofs. The recipient will need to send something in order to receive "public key encrypted" something. Usually, for public key encryption, we use static public key, not ephemeral public key. Furthermore, we have to assume an authenticated encryption (like GCM), which in my opinion, is not very reasonable. What we really need is (1) public key encryption (use either ephemeral or static public key) (2) Key agreement (like ephemeral DH). In practice, we may need to convert (1) to (2) (use one time public key), not from (2) to (1).
Please notice that, in 56B KEM-KWS is to use RSA to "encapsulate" a value, then derive a key from the "value" and used it to do key wrap. The KEM in 56B is different from what we called KEM.

2. Quantum security levels (1, 3, 5) vs. (2, 4).
I understand that for two algorithms A and B with parameter sets providing 128 bit classical security. If A satisfies level 1 quantum security while B satisfies level 2 quantum security, then we are in favor of algorithm B. However, A and B must be from different families, they will not be compared only on quantum security levels in the future but other properties. I also feel that level 2 is a special case of level 1. Level 1 means Groverizer effect less than 100%, assuming 100% is to make

square root of classical security level, while Level 2 means Groverizer effect equal to 0% meaning no effect at all. Again, a give algorithm will fit into either (1, 3, 5) or (2, 4) with parameter choices. A given algorithm will never reasonably provide 1, 2, 3, 4, 5 levels with different selection of parameters. Introducing levels 2 and 4 complicated our statement.

Let's think about.

Lily

From: Moody, Dustin (Fed)
Sent: Tuesday, October 25, 2016 12:56:27 PM
To: Perlner, Ray (Fed); Liu, Yi-Kai (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc: Peralta, Rene (Fed); Jordan, Stephen P (Fed); Chen, Lily (Fed); Bassham, Lawrence E (Fed)
Subject: PQC docs

Ray, Daniel, Jacob, and Yi-Kai,

Attached are the most recent versions of the FAQ and CFP. Please use them as you edit. Here are the assignments:

Daniel – edit your FAQ bullet

Ray – write a post summarizing our approach to quantum security in the CFP for the pqc-forum

Yi-Kai – edit Ray's FAQ bullets on quantum security, in addition to 4.A.5

Dustin – write a post summarizing our changes dealing with KEMs, along with the API to be posted in the pqc-forum

Jacob – write a summary of the comments and how we responded to them

Daniel, Ray, Yi-Kai (and myself). Please get these done this week. Next week we hit November.

Thanks!

Dustin