From: Liu, Yi-Kai (Fed)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed)
Subject: Re: PQC docs
Date: Thursday, October 27, 2016 5:02:57 PM
Attachments: final CFP v4.3 YKL.docx

Sure, I am fine with everything Ray has suggested.

Regarding the 2nd paragraph of 4.A.5, I agree with Ray that it is a bit confusing, however I don't want to delete it entirely, because it explains some of the motivation that is behind the security strength categories. Can we cut the confusing parts but keep the rest, like this? (I also inserted this in the Word document, see attachment.)

"Because of these uncertainties, NIST is taking a conservative approach in laying out its security requirements. NIST is formulating these requirements in a way that will ensure security in a variety of scenarios, representing a broad range of possibilities regarding the future development of both classical and quantum computing technologies. In addition, NIST recommends that submitters exceed these minimum requirements by some suitable margin, in order to account for possible uncertainties in their own estimates of security strength."

Cheers,

--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Thursday, October 27, 2016 3:09:23 PM
To: Perlner, Ray (Fed); Liu, Yi-Kai (Fed)
Subject: Re: PQC docs

Yi-Kai,

Do you agree with Ray?

From: Perlner, Ray (Fed)
Sent: Thursday, October 27, 2016 3:03:58 PM
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed)
Subject: RE: PQC docs

Hi all.

FWIW, I am leaning towards putting the heuristic description of our security strengths in the FAQ (since they do look a bit out of place in the document as written.) That said, it might be helpful if you can find a convenient place in the CFP to stick in a sentence or two implying that such heuristics exist.

Also worth pointing out: Two of the Q&A questions have been pretty much entirely put back in the CFP (the one about how we measure quantum security and the one about the strength of our symmetric key algorithms according those metrics.) Presumably they can be taken out of the FAQ.

Thanks,
Ray

From: Moody, Dustin (Fed)
Sent: Thursday, October 27, 2016 2:24 PM

To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>
Subject: Re: PQC docs

Yi-Kai and Ray.

I cleaned up Ray's comments on Yi-Kai's revision, and added references in the footnotes, etc. The ball is back in Yi-Kai's court. Can you take a look at Ray's outstanding comments (there aren't too many), and see if what he proposes is acceptable. Also, decide if the end of 4.A.5 stays or goes in the FAQ. I've also attached the FAQ so you can see what it currently has. Thanks,

Dustin

From: Perlner, Ray (Fed)
Sent: Wednesday, October 26, 2016 5:24:17 PM
To: Liu, Yi-Kai (Fed); Chen, Lily (Fed); Moody, Dustin (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc: Peralta, Rene (Fed); Jordan, Stephen P (Fed); Bassham, Lawrence E (Fed)
Subject: RE: PQC docs

Here are my comments on Yi-Kai's edits to section 4.A.5. For the most part, I like them, but I did think some stuff should be moved to footnotes, and there was about a paragraph worth of material in the intro which seemed confusing, and looked like it could be eliminated without doing too much damage. As for the stuff concerning simple heuristics for assigning security categories, if you just know the classical security strength, and that there are only generic quantum speedups, I think it can be moved to the FAQ, but at the same time, I worry that not everyone will read the FAQ, and I'd like to at least allude in the CFP to the fact that, if you're just concerned about making sure you're in the appropriate security strength category, and not about quantifying your security margin, it isn't so hard to do it.

-----Original Message-----
From: Liu, Yi-Kai (Fed)
Sent: Wednesday, October 26, 2016 3:22 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov<mailto:ray.perlner@nist.gov>>; Chen, Lily (Fed) <lily.chen@nist.gov<mailto:lily.chen@nist.gov>>; Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>; Daniel Smith-Tone <daniel-c.smith@louisville.edu<mailto:daniel-c.smith@louisville.edu>>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov<mailto:jacob.alperin-sheriff@nist.gov>>
Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov<mailto:rene.peralta@nist.gov>>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov<mailto:stephen.jordan@nist.gov>>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov<mailto:lawrence.bassham@nist.gov>>
Subject: Re: PQC docs

Hi everyone,

I made some edits to the CFP and FAQ, mainly having to do with quantum security.

Ray, I didn't change any of your meanings, I just revised the text to make it clearer. What do you think?

In particular, I'm much more comfortable now with your approach to measuring quantum security. But it really requires a lot of explanation to see why it makes sense. This was hard to follow in the earlier drafts of the CFP and the FAQ, but I think it is much clearer now.

Lily, sorry I didn't see your comments while I was editing the draft. Anyway, we can still edit some more.

--Yi-Kai

From: Perlner, Ray (Fed)
Sent: Wednesday, October 26, 2016 2:05 PM
To: Chen, Lily (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Daniel Smith-Tone; Alperin-Sheriff, Jacob (Fed)
Cc: Peralta, Rene (Fed); Jordan, Stephen P (Fed); Bassham, Lawrence E (Fed)
Subject: RE: PQC docs

1) KEM-KWS is actually using the KEM terminology the same way as we are using it in the CFP. Specifically it is a KEM combined with a key wrapping scheme to make a public key encryption scheme. The KEM is composed of RSASVE and an approved KDF. Again, while RSA-KEM-KWS is not itself a KEM, it is composed of two components, one of which is a KEM, and the other of which is a KWS.

2) Security strength 2 does not mean 0% Groverizer effect. If there is a larger Groverizer effect, it simply means that you need more classical security than 128 bits to get the appropriate quantum security.

From: Chen, Lily (Fed)
Sent: Wednesday, October 26, 2016 11:58 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov<mailto:dustin.moody@nist.gov>>; Perlner, Ray (Fed) <ray.perlner@nist.gov<mailto:ray.perlner@nist.gov>>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov<mailto:yi-kai.liu@nist.gov>>; Daniel Smith-Tone <daniel-c.smith@louisville.edu<mailto:daniel-c.smith@louisville.edu>>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov<mailto:jacob.alperin-sheriff@nist.gov>>
Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov<mailto:rene.peralta@nist.gov>>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov<mailto:stephen.jordan@nist.gov>>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov<mailto:lawrence.bassham@nist.gov>>
Subject: Re: PQC docs

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