From: Alperin-Sheriff, Jacob (Fed)
To: Moody, Dustin (Fed)
Subject: Re: PQC docs
Date: Wednesday, October 26, 2016 3:48:36 PM

Let me try to start reading about it.

On 10/26/16, 3:39 PM, "Moody, Dustin (Fed)" <dustin.moody@nist.gov> wrote:

>I would welcome such a system. Its hard for me to keep track of as well, especially since I have to often combine the changes that people have made almost simultaneously. For example, Lily sent in comments today and Yi-Kai sent revisions. I had to combine the 2 documents. Not a huge deal, but it does take time.
>
>I believe Office 365 (which we all have on our computers) has this capability, but I haven't explored it.
>
>-----Original Message-----
>From: Alperin-Sheriff, Jacob (Fed)
>Sent: Wednesday, October 26, 2016 3:32 PM
>To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Daniel Smith-Tone <daniel-c.smith@louisville.edu>
>Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
>Subject: Re: PQC docs
>
>Slightly off topic, but is there a good reason we don't use some kind of concurrent version system software for writing these? I'm getting a little overwhelmed as to what the "current" revision is ...
>
>
>
>On 10/26/16, 3:22 PM, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov> wrote:
>
>>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>; Perlner, Ray (Fed)
>><ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Daniel
>>Smith-Tone <daniel-c.smith@louisville.edu>; Alperin-Sheriff, Jacob
>>(Fed) <jacob.alperin-sheriff@nist.gov>
>>Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Jordan, Stephen P
>>(Fed) <stephen.jordan@nist.gov>; Bassham, Lawrence E (Fed)
>><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
>>