From: Moody, Dustin (Fed)
To: (b) (6)
Subject: RE: PQC call for papers v4
Date: Thursday, April 7, 2016 9:12:00 AM

Okay. Just send me a hangout request, or an email when you're free.

From: Daniel Smith (b) (6)
Sent: Thursday, April 07, 2016 9:12 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Re: PQC call for papers v4

I have a meeting with the graduate studies committee today starting at 10. I'm not sure how long it will take, so I'm not sure if I can join, but I'll try.
On Thu, Apr 7, 2016 at 8:40 AM, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

> All the rooms are booked, so we will meet in Lily's office.
>
> **From:** Liu, Yi-Kai (Fed)
> **Sent:** Wednesday, April 06, 2016 8:18 PM
> **To:** Perlner, Ray (Fed) <ray.perlner@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith (b) (6)
>
> **Cc:** Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
> **Subject:** Re: PQC call for papers v4
>
> Hi everyone,
>
> I cleaned up section 2 -- see attached file. (Dustin: I was editing Ray's version from earlier in this email chain, and all of my changes were confined to section 2. If you have made any edits on your copy of the file, can you just take my section 2 and paste it into your file?)
>
> I think the first half of the document is in decent shape, so tomorrow we can just focus on the second half.
>
> Cheers,
>
> --Yi-Kai
>
> ---
>
> **From:** Perlner, Ray (Fed)
> **Sent:** Thursday, March 31, 2016 10:51:04 AM
> **To:** Jordan, Stephen P (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); Daniel Smith
> **Cc:** Peralta, Rene (Fed); Bassham, Lawrence E (Fed)
> **Subject:** RE: PQC call for papers v4
>
> Thanks for the comment, Stephen
> I'm glad someone else is looking carefully at our proposed evaluation criteria. That said, I don't think we should be overly concerned with submitters doing incorrect or biased security analysis.

The worst thing that would come of that is that they set their parameters incorrectly – something which I think is likely to be less fatal for the submissions in this process than it was in the SHA3 competition. If we like a submission but think the submitters set the parameters wrong, we should simply tell the submitters that we'd like them to tweak their parameters for the next round, and publicly state the same in the report. I'm also not convinced that counting elementary gates is any easier than the sort of analysis suggested by my text. Hopefully I am getting across the message that we would prefer an imprecise measurement of security in a realistic attack model to a precise measurement of security in an unrealistic attack model (which, by the way, is the opposite of the typical incentives when the primary goal is getting academic papers published, so I do think we need to be somewhat explicit to push the analysis in this direction.)

I think it's also important to emphasize that these security metrics are evaluation criteria, not instructions to the submitters, and so they primarily constrain how we analyze submissions. If we give a precise definition of security which does not include consideration of parallelism, relative cost of classical and quantum operations etc, then we have prevented ourselves from taking these factors into account when we analyze submissions.

Cheers, Ray

From: Jordan, Stephen P (Fed)
Sent: Wednesday, March 30, 2016 10:24 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Daniel Smith (b) (6)
Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: Re: PQC call for papers v4

I like the direction the security definition is heading, but my intuition is that we may wish to simplify it further. A danger is that different submitters may make incomparable security analyses. If we leave too much complexity people may make mistakes and if we leave wiggle room people will be likely to interpret things in a way that makes their own submission look more favorable, even if they are not doing it consciously. I'd be in favor of saying something totally simpleminded and mathematically well-defined like: "the best known quantum attack must use at least 2^80 elementary quantum gates" (where we replace 2^80 with a few different numbers for different security levels). If we worry that someone might discover a way to parallelize the quantum attacks I think it is better to compensate by replacing 2^80 with 2^90 (or something) rather than adding more complexity or malleability to the security definition. Furthermore, our assumptions about the relative cost of quantum vs classical operations can simply be baked into our choices of number bits of security for each rather than leaving this as an aspect of the security definition for the individual teams to decide for themselves.

Best regards,

Stephen

From: Perlner, Ray (Fed)
Sent: Wednesday, March 30, 2016 4:49 PM
To: Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Daniel Smith
Cc: Peralta, Rene (Fed); Bassham, Lawrence E (Fed)
Subject: RE: PQC call for papers v4

Here is my update. All changes are confined to section 4, except for one comment to section 3, pointing out that we cannot require submitted signature algorithms to take arbitrary-length messages, since SHA256 has a maximum input size.

I have offered two choices for section 4A.iv (a slightly modified version of what I wrote before and something more aligned with what I think Yi-Kai was looking for.) See which one you like better.

Thanks,

Ray

From: Moody, Dustin (Fed)
Sent: Wednesday, March 30, 2016 10:21 AM
To: Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Daniel Smith [redacted]
Cc: Peralta, Rene (Fed) <rene.peralta@nist.gov>; Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>
Subject: Re: PQC call for papers v4

I've added my fixes. I've also made some other small revisions throughout the document, so if you haven't yet started, please use the attached version. If you have already started writing, maybe you can copy/paste your sections you've edited into this document. Thanks.

Dustin

From: Liu, Yi-Kai (Fed)
Sent: Tuesday, March 29, 2016 4:32 PM
To: Chen, Lily (Fed); Moody, Dustin (Fed); Perlner, Ray (Fed); Jordan, Stephen P (Fed); Daniel Smith
Cc: Peralta, Rene (Fed); Bassham, Lawrence E (Fed)
Subject: PQC call for papers v4

Hi everyone,

Here is an updated version of the call for papers, after our discussion this morning. I cleaned up my section. Could you all take turns revising your sections? If we can get this cleaned up by Friday afternoon, that would be great!

> Thanks!
>
> --Yi-Kai