**From:** Jordan, Stephen P (Fed)
**To:** Perlner, Ray A. (Fed); Moody, Dustin (Fed); Liu, Yi-Kai (Fed); Chen, Lily (Fed); (b) (6)
**Cc:** Peralta, Rene C. (Fed); Bassham, Lawrence E. (Fed)
**Subject:** Re: PQC call for papers v4
**Date:** Wednesday, March 30, 2016 10:24:12 PM

---

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

(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'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