From:	Kelsey, John M. (Fed)
To:	Peralta, Rene C. (Fed); Moody, Dustin (Fed); internal-pqc
Cc:	Dang, Thinh H. (Fed)
Subject:	Re: PQC meeting summary + updated assignments
Date:	Friday, June 12, 2020 5:31:30 PM

I think we need to at least more-or-less talk about the path to standardization, but I agree we shouldn't bind ourselves to standardizing anything.

--John

From: "Peralta, Rene C. (Fed)" <rene.peralta@nist.gov>
Date: Friday, June 12, 2020 at 15:11
To: "Kelsey, John M. (Fed)" <john.kelsey@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, internal-pqc <internal-pqc@nist.gov>
Cc: "Dang, Thinh H. (Fed)" <thinh.dang@nist.gov>
Subject: Re: PQC meeting summary + updated assignments

Is there value in having this on the document, as opposed to it being our internal consensus as of today? Anything we say in the document is really hard to retract later.

Rene.

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Friday, June 12, 2020 3:08 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Cc: Dang, Thinh H. (Fed) <thinh.dang@nist.gov>
Subject: Re: PQC meeting summary + updated assignments

Everyone,

I've added a short summary of what I think is the path to standardization for each algorithm in [[double square brackets]]. The text isn't polished, but I think we somehow need to get these ideas into the sections.

Thanks,

--John

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Friday, June 12, 2020 at 15:04
To: internal-pqc <internal-pqc@nist.gov>
Cc: "Dang, Thinh H. (Fed)" <thinh.dang@nist.gov>
Subject: PQC meeting summary + updated assignments

Everyone,

Thanks for a good meeting today. We covered many points. Let us continue to keep polishing our report:

 PQC Report on Round 2.docx

While everything could still use more checking, the main things I want to call attention to:

- Section 2.3 Selection of the Third Round Candidates. I made some changes based on our meeting. This is a very important explanation we need to make sure is good. Please review and make changes/suggestions.
- We need to edit and make more uniform our individual candidate write ups. In general, they should consist of
    - Summary of algorithm, including security and performance
    - Anything to note that occurred in round 2. (tweaks they made, etc...)
    - Areas of concern, or that we want more study on, etc
    - Finish with the reason behind our decision, and possibly some mention of the path to standardization if its not clear from the text yet.

- As you go, please add in the citations that you know. At the end of the report is the references section. Don't worry about the numbering. Just stick the citation at the end of the list. When we are ready to finalize, we will get the ordering right.

Here are some updated assignments for our 2nd draft. As usual, everybody should read and edit everything, but here they are. Some people have already done this, but I'm repeating the info anyway.

1) For the body of the report, check if the main points are covered. Are we missing anything?

- Carl, Section 1 - Introduction
- Gorjan, Section 2.2.1 - Security
- John, Section 2.2.2 - Performance
- Angela, Section 2.2.3 - Algorithm and implementation char.
- Yi-Kai, Section 2.3 - selection of 3rd round candidates
- Rene, Section 4 - Conclusion.

2) Edit the candidate specific write-ups, following the formula above

- Gorjan, Saber, NTRUprime, qTESLA
- Yi-Kai, NewHope, Dilithium, Falcon
- Daniel A, LAC, Kyber, Round5, Picnic
- Angela, BIKE, LEDAcrypt, RQC
- Ray, GeMSS, Rainbow, LUOV, MQDSS
- Carl, ThreeBears, HQC
- Quynh, NTRU, FrodoKEM
- Daniel ST, HQC, Rollo
- David, Picnic, SPHINCS+
- Rene, SIKE, MQDSS, LUOV
- John, Classic McEliece, Picnic

In particular, NTRU Prime, NewHope, and Three Bears need to be more high level. Please try and do some revising before Tuesday, where we can meet again to discuss the report.

Also take a look at:


Round 3 Announcements.docx

which has a pqc-forum announcement, detailed instructions for tweaks, and a general call for our 3rd workshop.

Thanks everyone!

Dustin