From: Dang, Quynh H. (Fed)
To: Moody, Dustin (Fed); internal-pqc; Daniel Smith-Tone
Subject: Re: PQC Round 2 report assignments
Date: Thursday, June 4, 2020 9:52:26 AM

Hi Dustin,

Since the content of that section has been put somewhere else. I don't see a lot of need for that section. We don't have to have the same sections as in the the first round report.

I am happy to write a sentence about IPR issue. But, I think Ray understands the details of the current IPRs that we are aware of than I do.

Hi Ray,

Could you consider to write about the IPR issue in our report ?

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 4, 2020 9:44 AM
To: internal-pqc <internal-pqc@nist.gov>; Daniel Smith-Tone <dcsmit11@exchange.louisville.edu>
Subject: Re: PQC Round 2 report assignments

Everybody,

Thanks for revising our Round 2 report. Most people finished yesterday, as desired. You are all improving it greatly. I've got some new assignments to keep this going. See below:

Ray - please edit/re-write the 1st four paragraphs of 2.2.1 so that it won't read as a carbon copy of what we had in the 1st round report. What you wrote at the end is good.

Quynh - David took a chunk of text out of 2.2.3, which is fine. But it leaves 2.2.3 needing some more work. If you want the 1st paragraph deleted, go ahead and do that. Perhaps mention factors that could hinder adoption (IPR) as one of the criteria we are considering in this section.

Daniel ST - it looks like you haven't finished your assignment. Please do so ASAP! This includes editing/re-writing 2.3 as well as the multivariate schemes in Section 3.

Angela - in Section 4 you added some good changes. Please continue to edit/re-write the entire section so that it doesn't read as a carbon copy of what we had in the 1st round report.

Everyone - add things in Section 3 to the submissions. strengths, weaknesses, key points, things we want the submitter to consider, etc. Several probably have enough, but there are lots that aren't.

Let's see if we can get all the above done by Friday. Thank you! Let me know if you have more specific questions. Thanks,

Dustin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, June 2, 2020 3:08 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC Round 2 report assignments

As a reminder, here are the assignments (due by tomorrow).

Thanks,
Dustin

>>>>>>>>>>>>>>>>>
Everyone,
We need to edit more our round 2 report. It is accessible on sharepoint at:
PQC Report on Round 2.docx

I'd like to give out some assignments as we continue our selection. There are two types:

1) I've already sort of written much of the text, mostly adapted straight from the round 1 report. We need to re-write it for the round 2 report, adding in relevant info. Feel free to propose adding new sections or info.

- Yi-Kai, Section 1 - Introduction
- Ray, Section 2.2.1 - Security
- David, Section 2.2.2 - Performance
- Quynh, Section 2.2.3 - Algorithm and implementation char.
- Daniel ST, Section 2.3 - selection of 3rd round candidates
- Angela, Section 4 - Conclusion. Maybe add in something about the on ramp idea (esp. for non-lattice general purpose signatures)

2) The most important part will be section 3, where we discuss each candidate. Please add info, either with bullet points or just writing it out. Address our evaluation criteria. Some

schemes already have this started. Here is where we need to justify our decisions.

- Gorjan, Kyber, Frodo, NTRU
- Yi-Kai, LAC
- Daniel A, New Hope, NTRUprime, Saber, 3 bears
- Angela, Round 5, Rollo, HQC
- Ray, Classic McEliece, Bike, LEDAcrypt, RQC
- Carl, qTesla, check falcon and dilithium
- Quynh, GeMSS
- Daniel ST, LUOV, MQDSS
- David, check sphincs+, picnic
- Rene, picnic, check SIKE
- John, (already done some), any you feel like

Of course, please do look at the whole report and make edits/comments any where you wish. Let's see if we can have everybody do this by next Wednesday (one week), so we will have a complete first draft. This is just a first step. Thanks everyone!

Dustin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, May 27, 2020 11:21 AM
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC Round 2 report assignments

Everyone,
We need to edit more our round 2 report. It is accessible on sharepoint at:
PQC Report on Round 2.docx

I'd like to give out some assignments as we continue our selection. There are two types:

1) I've already sort of written much of the text, mostly adapted straight from the round 1 report. We need to re-write it for the round 2 report, adding in relevant info. Feel free to propose adding new sections or info.

- Yi-Kai, Section 1 - Introduction
- Ray, Section 2.2.1 - Security
- David, Section 2.2.2 - Performance
- Quynh, Section 2.2.3 - Algorithm and implementation char.
- Daniel ST, Section 2.3 - selection of 3rd round candidates
- Angela, Section 4 - Conclusion. Maybe add in something about the on ramp idea (esp. for non-lattice general purpose signatures)

2) The most important part will be section 3, where we discuss each candidate. Please add info, either with bullet points or just writing it out. Address our evaluation criteria. Some schemes already have this started. Here is where we need to justify our decisions.

- Gorjan, Kyber, Frodo, NTRU
- Yi-Kai, LAC
- Daniel A, New Hope, NTRUprime, Saber, 3 bears
- Angela, Round 5, Rollo, HQC
- Ray, Classic McEliece, Bike, LEDAcrypt, RQC
- Carl, qTesla, check falcon and dilithium
- Quynh, GeMSS
- Daniel ST, LUOV, MQDSS
- David, check sphincs+, picnic
- Rene, picnic, check SIKE
- John, (already done some), any you feel like

Of course, please do look at the whole report and make edits/comments any where you wish. Let's see if we can have everybody do this by next Wednesday (one week), so we will have a complete first draft. This is just a first step. Thanks everyone!

Dustin