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 10:03:16 AM

OK.

Quynh.

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Thursday, June 4, 2020 10:00 AM
To: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>; internal-pqc <internal-pqc@nist.gov>; Daniel Smith-Tone <dcsmit11@exchange.louisville.edu>
Subject: Re: PQC Round 2 report assignments

Quynh,

In our CFP we identified 3 main evaluation areas: security, performance, and algorithm and implementation characteristics. I think we should have this section still. It doesn't need to be long. See below for what we wrote about this in the original CFP for algorithm and implementation characteristics. Just write a short summary of this. Relative to round 2 we could add that we have seen some experiments looking into whether the schemes can be incorporated into existing protocols.

For IPR, I don't want much about this in the report, certainly not specific details. Just a sentence mentioning that this topic is a factor in our decision making process.

Is that alright?

Dustin

4.C.1 Flexibility Assuming good overall security and performance, schemes with greater flexibility will meet the needs of more users than less flexible schemes, and therefore, are preferable.
Some examples of "flexibility" may include (but are not limited to) the following:

a. The scheme can be modified to provide additional functionalities that extend beyond the minimum requirements of public-key encryption, KEM, or digital signature (e.g., asynchronous or implicitly authenticated key exchange, etc.).
b. It is straightforward to customize the scheme's parameters to meet a range of security targets and performance goals.
c. The algorithms can be implemented securely and efficiently on a wide variety of platforms, including constrained environments, such as smart cards.

d. Implementations of the algorithms can be parallelized to achieve higher performance.
e. The scheme can be incorporated into existing protocols and applications, requiring as few changes as possible.

4.C.2 Simplicity The submitted scheme will be judged according to its relative design simplicity.

4.C.3 Adoption Factors that might hinder or promote widespread adoption of an algorithm or implementation will be considered in the evaluation process, including, but not limited to, intellectual property covering an algorithm or implementation and the availability and terms of licenses to interested parties. NIST will consider assurances made in the statements by the submitter(s) and any patent owner(s), with a strong preference for submissions as to which there are commitments to license, without compensation, under reasonable terms and conditions that are demonstrably free of unfair discrimination.

From: Dang, Quynh H. (Fed) <quynh.dang@nist.gov>
Sent: Thursday, June 4, 2020 9:52 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; internal-pqc <internal-pqc@nist.gov>; Daniel Smith-Tone <dcsmit11@exchange.louisville.edu>
Subject: Re: PQC Round 2 report assignments

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