From: Miller, Carl A. (Fed)
To: Moody, Dustin (Fed)
Subject: Re: PQC Round 2 report assignments
Date: Tuesday, June 9, 2020 11:39:19 AM

Hi Dustin –

Ok, I'll take a look at the Falcon and Dilithium discussions some time soon.

-Carl

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, June 8, 2020 at 4:25 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: Re: PQC Round 2 report assignments

Carl,
I wrote up something for Dilithium and Falcon. Please take a look and add anything you think needs to be brought up, or correct anything you see fit.

Thanks,

Dustin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, June 8, 2020 2:24 PM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC Round 2 report assignments

Reminder -

- Please take a look, and edit:
  Round 3 Announcements.docx
- So far, 10 of the 26 second round schemes have write-ups. Please try to finish the remainder of these by tomorrow COB at the latest. Here's what we still need:
  - LAC - Yi-Kai
  - NewHope - Daniel A
  - NTRU Prime - Daniel A
  - Round 5 - Angela
  - SABER - Daniel A

- Three Bears - Daniel A
- Classic McEliece - Ray
- BIKE - Ray
- LEDAcrypt - Ray
- RQC - Ray
- Dilithium - Carl/Dustin
- Falcon - Carl/Dustin
- MQDSS - Quynh/Daniel ST
- Rainbow - Quynh/Daniel ST
- Picnic - David/John
- SPHINCS+ - David/John

I appreciate those who have been editing and completing their assignments.

Dustin

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Friday, June 5, 2020 9:44 AM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC Round 2 report assignments

Everyone,
In addition to our report, I've written some other text we'll need: An announcement for the pqc-forum (or maybe even for any press release), some more detailed instructions about round 3 tweaks, and a CFP for our 3rd workshop. All of these are modeled on what we did at the end of round 2. I tried to add in some of what we've discussed recently.

Please take a look, and edit:
Round 3 Announcements.docx

One way we could phrase our 2 tracks is call the first "Finalists" and call the other algorithms moving on as "candidates". I used that in the announcement, and I think it makes sense and is easy to understand.

Please continue working on our report. A few of the schemes have had their bullet points converted into text. Thanks to those who wrote them! Let's keep doing this for all the schemes. It would be great if by Tuesday we have these all done - at least a first draft of them. We need to decide if the level of detail we have is what we want for section 3.

Dustin

From: David A. Cooper <david.cooper@nist.gov>

Sent: Thursday, June 4, 2020 12:22 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: PQC Round 2 report assignments

Hi John,

I did mention that in Section 2.2.2 (perhaps that is what you were referring to). Where else in the document do you think it bears mentioning?

Thanks,

David

On 6/4/20 12:19 PM, Kelsey, John M. (Fed) wrote:

> Would it make sense to specifically call out the large key, small ciphertext/signature thing as a separate performance profile? Classic McEliece, Rainbow, and GeMSS all fit this profile. There's a little test in the document now, but I wonder if it makes sense to call this out as its own thing
>
> --John