From: Moody, Dustin (Fed)
To: Sonmez Turan, Meltem (Fed)
Subject: Re: pqc round 2 report
Date: Wednesday, June 17, 2020 12:15:15 PM

Thanks, Meltem.

You bring up a good point. We've debated what to call the tracks. We did agree to call the 7 most promising ones "Finalists". For the others, we never completely settled on one name. I preferred "third round candidates", while John prefers "alternate candidates". You're right that what is in the report calls these second track schemes a few different names. I'll try to clear that up.

Yep, the references section is still a mess, but you should have seen it yesterday! It was even worse. I just gave us a deadline of next Friday June 26th to be done with the report.

While it's nice to have a big group to lean on to write a report like this, it's also tricky to manage. Many different authors, with different opinions and styles, and we want to combine it to read like one cohesive document. Your lightweight report writing process is probably simpler!

Dustin

From: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Sent: Wednesday, June 17, 2020 11:57 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: pqc round 2 report

Hi Dustin,

I just briefly went over the status report. Congratulations! It looks very good.

I like the idea of having two tracks and separating more promising ones from the alternates. However, I have a minor comment to eliminate possible confusion. The document uses different names for the candidates such as finalists, third-round finalists, additional candidates, alternate candidates, third-round candidates etc. When I read it, it was not clear to me if additional/alternate candidates part of finalists, or part of third-round candidates? If there is a possibility of a fourth round, can these candidates be called finalists as well at later time?

Maybe you can simplify this and call all of the remaining the candidates as ‘third round candidates’ and mark seven of them as focus or promising. eStream stream cipher competition had a similar approach and phase 2 candidates were partitioned into ‘Phase 2 cipher’ and ‘Focus Phase 2 cipher’. Then, you would not really need an additional name as ‘alternate’ or ‘additional’ for the remaining algorithms.

Minor additional comments:

- In section 2.2.1 listing ‘certificates’ as an example for application looks a little odd to me.
- References section might benefit from editorial check.

Cheers,
Meltem

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, June 17, 2020 9:43 AM
To: Sonmez Turan, Meltem (Fed) <meltem.turan@nist.gov>
Subject: pqc round 2 report

Meltem,

I'm attaching a current draft of our report. I'm curious your take on a few things. I forget how much I've told you, since we haven't been able to talk much (or practically at all). We are advancing algorithms in 2 tracks. The first are the finalists, which are the most promising ones. We'll likely select 1 (or 2) of both the KEMs and signatures. We then are keeping several alternate candidates into the third round, which have a variety of different reasons for keeping them, but for not being a finalist. Our main explanation of this is in section 2.3.

I was wondering if our rationale makes sense to somebody who is aware of our process, but not into all the details. Let me know what you think. Thanks!

I guess we'll talk this afternoon at our CTG re-group.

Dustin