From:	Chen, Lily (Fed)
To:	Moody, Dustin (Fed); Regenscheid, Andrew R. (Fed); Scholl, Matthew A. (Fed)
Subject:	Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process
Date:	Monday, June 29, 2020 3:24:54 PM

The responses to Dustin's e-mail from the team show that a general statement about a possibility can trigger a lot of different understandings. Signature candidates are differently from KEM. For KEM, we have NTRU as a IPR fall back and Classic McEliece as a backup for lattice. For signatures, we do not have real backups.

Lily

From: Dustin Moody <dustin.moody@nist.gov>
Date: Monday, June 29, 2020 at 11:17 AM
To: "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>, Matthew Scholl <matthew.scholl@nist.gov>
Cc: Lily Chen <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Okay, I can take it out of the footnote and put it in the main body.

Dustin

From: Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Sent: Monday, June 29, 2020 11:11 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

To be fair, I've been concerned about that text around SPHINCS+ (and more generally, standardizing "second-track" candidates) for a while now. I brought it up earlier- I just held my tongue after there was a group consensus that made SPHINCS+ an alternate.

Procedurally, I definitely think its best if we intend to standardize an "alternate" right away, we should elevate them to a finalist first so there's no surprise.

I looked through your changes. They all seem fine with me. The one thing I'd change, though, is that you added that new sentence to a footnote, rather than the body. I'm generally anti-footnote except in some limited cases. I just pull it up into the body.

-Andy

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, June 29, 2020 10:46 AM
To: Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>; Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Andy,

I made some changes based on your suggestions. Take a look, and let me know what you think. The key one was adding in the sentence (in two places):

"It is possible that new analysis could result in an alternate candidate being elevated to being a finalist, in the case that NIST's confidence in the security of any of the finalists is greatly reduced."

Take a look. If we like it, I think we need to mention/discuss this idea with the team. I don't think they'll have a problem with it, but they will wonder where it comes from. When we've talked about this sort of situation in our meetings, we've said that if something breaks a finalist we would probably regroup and figure out what to do at that point. I don't want to start anything too major within the group if possible, as that will only prolong our announcement.

Dustin

From: Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Sent: Monday, June 29, 2020 9:43 AM
To: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Personally, I don't think that goes far enough to avoid another SHA3-like situation. And I'm also not sure what your new sentence is a good idea to include. The problem we face isn't that someone would try to mount a legal challenge that we broke the rules- it's that if we did something unexpected it might impact public confidence in the process. I think it would be much better to try to explain *what* might change.

I continue to think it would be a bad idea to immediately standardize an alternate candidate.

Now, obviously if there's something extreme, like a break of lattice-based signatures, then probably everyone would conclude everything is on the table. But short of that, we could find ourselves in a difficult situation. What if there's no break, but substantial interest in a non-lattice option?

The main thing I'd recommend is including text that says we may elevate alternates to finalists based on analysis that comes out during the third round. That would let us avoid directly standardizing an alternate.

But, in the interest of keeping all options open, I would suggest expanding the text were we suggest alternates wouldn't get standardized until after a 4th round. Presumably SPHINCS+ and Frodo would both potentially fall in to that category.

I'm attaching my comments on the report. All-in-all, I think its in great shape once we deal with this "alternates" and SPHINCS+ issue.

-Andy

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Friday, June 26, 2020 1:41 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Yes I think it does

-------- Original Message --------
From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Fri, June 26, 2020 1:39 PM -0400
To: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>
CC: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Relevant lines in the report:

- in the SPHINCS+ writeup:

> NIST sees SPHINCS+ as an extremely conservative choice for standardization. If NIST's confidence in better performing signature

algorithms is shaken by the end of the third round, SPHINCS+ could provide an immediately available algorithm for standardization. Further, if NIST sees the need for an additional signature algorithm for applications that need very high security and can tolerate larger and slower signatures, NIST may decide to standardize SPHINCS+ in the future.

(note that we say it could be immediately available if needed)

- in a few places we mention the alternate candidates are still being considered for standardization, although "most likely after another round". We were careful to not exclude the possibility of standardizing one after the 3rd round.
- In our announcement, we have the line:

  "Note – These are NIST's current plans. NIST reserves the right to modify the process in the future."

I added the sentence "NIST also reserves the right to modify the process in the future, should circumstances warrant." into the conclusion of the report.

Does this seem sufficient for what we expect?

Dustin

From: Scholl, Matthew A. (Fed) <matthew.scholl@nist.gov>
Sent: Thursday, June 25, 2020 3:32 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Regenscheid, Andrew R. (Fed) <andrew.regenscheid@nist.gov>
Cc: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: Re: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Thank you all,
This looks great. Is it possible to do a quick call, perhaps tomorrow (perhaps not so quick).

I would like to discuss the potential to move Sphincs+ up into the finalist from alternative.

I have been read in but,……. . I would be the manager making a call if needed, on the grounds of IP concerns but want to hear and discuss.
Sorry for this late notice item and the potential consternation this might cause
Matt

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Wednesday, June 24, 2020 at 3:02 PM
To: "Regenscheid, Andrew R. (Fed)" <andrew.regenscheid@nist.gov>
Cc: "Scholl, Matthew A. (Fed)" <matthew.scholl@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>
Subject: draft Status Report on the 2nd Round of the NIST PQC Standardization Process

Andy (and Lily and Matt),

Our PQC team has finally finished our draft of the 2nd round report, and will be starting the process of getting it approved/WERB'ed (meaning I've sent it to Jim and Sara). I've attached a clean copy of it, which will hopefully facilitate a speedier publication. Let me know of any comments or suggestions.

Thanks,

Dustin