From:	Chen, Lily (Fed)
To:	Smith-Tone, Daniel C. (Fed); Perlner, Ray A. (Fed); Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed); Kerman, Sara J. (Fed)
Cc:	internal-pqc
Subject:	RE: Posting Our Attack Thoughts?
Date:	Thursday, December 21, 2017 2:46:23 PM

We need to determine when will be "eventually". In SHA-3 case, we have the first round report, which include public analysis and also NIST team's analysis.

Can you please clarify "I don't think that we should put the comments on the site initially." Which comments?

For minor issues, would we have included in the acceptance letter to the submitters?

Lily

From: Smith-Tone, Daniel (Fed)
Sent: Thursday, December 21, 2017 2:38 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: RE: Posting Our Attack Thoughts?

I don't know if you agree, but I think that we should take our summary document from the sharepoint site and modify it to be more discrete and eventually make it available. I don't think that we should put the comments on the site initially. We risk being viewed as biased even though the science is on our side. Especially if the issue with some scheme is minor.

I think that we should let the community find these things, but keep a nice-for-public-view document of our comments that proves that we are on top of things. Do you agree?

Cheers,
Daniel

From: Chen, Lily (Fed)
Sent: Thursday, December 21, 2017 2:21 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: RE: Posting Our Attack Thoughts?

If they are existing papers, we probably do not need to do anything. Do we?

Lily

From: Perlner, Ray (Fed)
Sent: Thursday, December 21, 2017 2:18 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: RE: Posting Our Attack Thoughts?

What about cases where we're aware of existing papers claiming to break published prior version the submission
e.g. WalnutDSA and RVB?

From: Chen, Lily (Fed)
Sent: Thursday, December 21, 2017 2:16 PM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: RE: Posting Our Attack Thoughts?

Well, I say for official comments from our team and also **any non-official discussions** on individual submission, we shall consider our early access advantage. Please hold off.

Please discuss if you have different opinions.

Lily

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, December 21, 2017 2:13 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kerman, Sara J. (Fed) <sara.kerman@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Posting Our Attack Thoughts?

That's for conference-type publications only though, no?

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Thursday, December 21, 2017 at 2:12 PM
To: "Kerman, Sara J. (Fed)" <sara.kerman@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Re: Posting Our Attack Thoughts?

I suppose we should keep in mind what Daniel was discussing yesterday as well, in regards to this.

From: Kerman, Sara J. (Fed)
Sent: Thursday, December 21, 2017 2:11:19 PM
To: Alperin-Sheriff, Jacob (Fed); Moody, Dustin (Fed)
Cc: internal-pqc
Subject: RE: Posting Our Attack Thoughts?

I think that would qualify as an "OFFICIAL COMMENT". So yes, you should click the link so it's "official". Periodically I will compile them into a PDF and link via the "View Comments".

Does that help?
Sara

From: Alperin-Sheriff, Jacob (Fed)
Sent: Thursday, December 21, 2017 2:01 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Cc: internal-pqc <internal-pqc@nist.gov>
Subject: Posting Our Attack Thoughts?

I assume we'll post them under "Submit Comment?" Or are we posting them elsewhere? Let us know.

—Jacob Alperin-Sheriff