From:	Smith-Tone, Daniel C. (Fed)
To:	Chen, Lily (Fed); Peralta, Rene C. (Fed); Moody, Dustin (Fed); Kelsey, John M. (Fed); Cooper, David (Fed); internal-pqc
Subject:	RE: Commenting on 3rd round report
Date:	Friday, March 11, 2022 10:11:44 AM

Hi,

For the multivariate section, I used the language “intractable”, since that’s what we mean. Our statements aren’t related to asymptotic statements at all, so I would prefer to not overload the term “hard” that much. It might be misinterpreted as being related to these NP-hard problems.

Cheers,
Daniel

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Monday, March 7, 2022 3:15 PM
To: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Commenting on 3rd round report

Yes, Rene, you are correct. The original sentence was “This does not guarantee that cryptographic instantiations are NP hard.” Even breaking the systems cannot be NP-Hard.
Lily

From: Peralta, Rene C. (Fed) <rene.peralta@nist.gov>
Sent: Monday, March 7, 2022 2:54 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Commenting on 3rd round report

>>
This does not guarantee that breaking cryptographic instantiations ~~are~~ is NP hard.”
>>

Instantiations cannot be NP-hard, as this is an asymptotic notion only.
Maybe we could just remove "NP"?

René

From: Chen, Lily (Fed) <lily.chen@nist.gov>

Sent: Monday, March 7, 2022 2:44 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: RE: Commenting on 3rd round report

These are the comments I have so far. I will continue to use the same format, if it is okay.

Lily

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Monday, March 7, 2022 2:40 PM
To: Kelsey, John M. (Fed) <john.kelsey@nist.gov>; Cooper, David A. (Fed) <david.cooper@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Commenting on 3rd round report

I'd agree with David that we should just use the commenting feature at this point. If you want to make comments some other way, just send an email, and we can insert them into Overleaf for you.

Please regularly go check for comments and help resolve any that you can. I'll try to directly contact you if I think you could provide some feedback for a particular comment and you haven't addressed it.

Great job by everyone - we've almost got it done. Thanks,

Dustin

From: Kelsey, John M. (Fed) <john.kelsey@nist.gov>
Sent: Monday, March 7, 2022 2:36 PM
To: Cooper, David A. (Fed) <david.cooper@nist.gov>; internal-pqc <internal-pqc@nist.gov>
Subject: Re: Commenting on 3rd round report

Everyone,

I can't seem to get the commenting feature to work--maybe because I'm using a weird browser (Brave)? Maybe I'll just write comments separately and email them or something if I can't figure it out, but it seems kind of awkward.

On 3/7/22, 14:31, "Cooper, David A. (Fed)" <david.cooper@nist.gov> wrote:

> Hi all,
>
> I would like to suggest that anyone wishing to comment on the 3rd round report at this point use Overview's commenting feature rather than

inserting comments into the body of the document.

I am concerned that comments inserted into the body of the document at this late stage will be missed and will accidentally end up in the final document.

Thanks,

David