From: Chen, Lily (Fed)
To: Alperin-Sheriff, Jacob (Fed)
Cc: Perlner, Ray A. (Fed); Moody, Dustin (Fed)
Subject: Re: Received Comments 9/1-18
Date: Monday, September 19, 2016 9:07:44 AM

Hi, Jacob and Ray:

By the way, I already included Bernstein's (received Saturday) and Lange's (Received Sunday). It will be very helpful to (1) put them together with their full name on the top; and (2) Generate a file which groups the comments under topics.

Some of them may not be able to be classified, which is fine.

Lily

From: Alperin-Sheriff, Jacob (Fed)
Sent: Monday, September 19, 2016 9:02 AM
To: Chen, Lily (Fed); Perlner, Ray (Fed); Moody, Dustin (Fed); Daniel C Smith (daniel-c.smith@louisville.edu); Liu, Yi-Kai (Fed); Peralta, Rene (Fed); Jordan, Stephen P (Fed); Miller, Carl A. (Fed)
Subject: Re: Received Comments 9/1-18
I will organize the rest of them (the ones not in by when I left on Friday) by section of the draft and then email it to everybody.

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Monday, September 19, 2016 at 8:05 AM
To: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Moody, Dustin (Fed)" <dustin.moody@nist.gov>, "Daniel C Smith (daniel-c.smith@louisville.edu)" <daniel-c.smith@louisville.edu>, "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Jordan, Stephen P (Fed)" <stephen.jordan@nist.gov>, "Alperin-Sheriff, Jacob M. (Fed)" <jacob.alperin-sheriff@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: Received Comments 9/1-18

During weekend, when I read the comments, I found that some of the comments are in txt version in the e-mails and hard to read. Then I converted to word version to read. I collected the comments received after September 1 in the attached zip file, for every one to read. I named them by commenter's last name except the one submitted by Microsoft, which is a PDF file.

The main commented areas are (in order of the number of comments). I think we will need to further separate the comments to the each topics.

1. Quantum security strength
2. Key exchange (KEM vs. DHish)
3. IPR
4. Hybrid mode

I did not look into comments received before September 1, which are not many. Please include if you can check the e-mails from August 2 to September 1. (I also might miss some after September 1)

Lily