From:	Alperin-Sheriff, Jacob (Fed)
To:	Chen, Lily (Fed); Perlner, Ray A. (Fed); Moody, Dustin (Fed); Daniel C Smith (daniel-c.smith@louisville.edu); Liu, Yi-Kai (Fed); Peralta, Rene C. (Fed); Jordan, Stephen P (Fed); Miller, Carl A. (Fed)
Subject:	Re: Received Comments 9/1-18
Date:	Monday, September 19, 2016 10:16:08 AM
Attachments:	Bernstein and Lange.docx Organized Draft Comments.docx

The following two documents contain

1. [Bernstein and Lange] the comments by the dynamic duo of D.J. Bernstein and Tanja Lange, whose complete comments are put together one after another in a separate file per Lily's request
2. [Organized Draft Comments] All of our received comments (including those of Bernstein and Lange, as well as the nonsensical comments by our buddy Mr. W1SD0M) have been organized to the best of my ability by which part of the draft they refer to, and should make it a little easier to wade through them and incorporate the good ones over the next few months.

(If I should PDF them, let me know. I mean Microsoft itself sent us a PDF …)

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