FYI. Comments received between September 1 and September 18.

Lily

From: Chen, Lily (Fed)
Sent: Monday, September 19, 2016 8:05 AM
To: 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); Alperin-Sheriff, Jacob (Fed); Miller, Carl A. (Fed)
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