From: Chen, Lily
To: Jordan, Stephen P; Perlner, Ray; Moody, Dustin; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Peralta, Rene; Liu, Yi-Kai
Subject: RE: Final call for changes to NISTIR
Date: Friday, January 29, 2016 10:27:19 AM
Attachments: llc-PQC NISTIR v3 Ray and Stephen Comments.docx

Attached please see my comments (use Stephen commented version). I noticed that we did not explicitly refer NIST public key cryptography standards. I think we should. We also use different terms for the categories of public key cryptography. In some places, we consider three functionalities: public key encryption, key exchange and signature, while in other place, we categorized as key establishment and signature. Let's try to be consistent.

Lily

From: Jordan, Stephen P
Sent: Thursday, January 28, 2016 8:14 PM
To: Perlner, Ray; Moody, Dustin; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Peralta, Rene; Chen, Lily; Liu, Yi-Kai
Subject: Re: Final call for changes to NISTIR

I have also added my comments. The attached file should have both mine and Ray's.

Best regards,

Stephen

From: Perlner, Ray
Sent: Thursday, January 28, 2016 4:20 PM
To: Moody, Dustin; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Peralta, Rene; Chen, Lily; Liu, Yi-Kai; Jordan, Stephen P
Subject: RE: Final call for changes to NISTIR

Here are my comments

From: Moody, Dustin
Sent: Thursday, January 28, 2016 3:44 PM
To: Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Perlner, Ray; Peralta, Rene; Chen, Lily; Liu, Yi-Kai; Jordan, Stephen P
Subject: Final call for changes to NISTIR

Everyone,

I've tried to incorporate in the suggestions received. On Monday I'm going to send the NISTIR out to Jim Foti, who will prepare it for publication. Matt has suggested that we put it out for 30 days of public comments. So, any last comments need to be given before Monday. Thanks! I appreciate all the help and input from everyone.

Dustin

Reminder – next Tuesday we meet with Michael Groves and Wednesday is our crypto club talk. Please send me your slides by the end of the day tomorrow (Friday). Thanks!