From: Liu, Yi-Kai
To: Moody, Dustin
Subject: Re: Latest version of NISTIR and other documents for PQC
Date: Wednesday, January 27, 2016 4:28:18 PM
Attachments: PQC NISTIR v2 YKL.docx

Hi Dustin,

Wow, that was a double fail on my part -- editing a stale version of the document, and then forgetting to attach it to the email. Here are my edits, now applied to the current version of the document, and hopefully I will remember to attach it this time!

Cheers,

--Yi-Kai

From: Moody, Dustin
Sent: Wednesday, January 27, 2016 8:36 AM
To: Liu, Yi-Kai
Subject: Re: Latest version of NISTIR and other documents for PQC

Yi-Kai,
I didn't see any file attached. Also, from your email it sounds like you might not have my latest version. See the attached, which is my latest version.

Dustin

From: Liu, Yi-Kai
Sent: Monday, January 25, 2016 5:34 PM
To: Peralta, Rene; Perlner, Ray; Moody, Dustin; Chen, Lily; Jordan, Stephen P; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: Re: Latest version of NISTIR and other documents for PQC

Hi Dustin,

I took another look at the NISTIR. Is this the latest version? It has a bunch of comments by Donna and the NSA people, and I remember we discussed those comments at one of our meetings, but I don't know if we updated the NISTIR after that discussion?

Anyway, I made a few more comments in the Word file: I edited the abstract to make it clearer, and I suggested splitting section 4 into two sections (one on the timing of the transition to post-quantum cryptography, and one on the development of standards for post-quantum cryptography). What do

you think?

Cheers,

--Yi-Kai

From: Peralta, Rene
Sent: Thursday, January 14, 2016 11:32 AM
To: Perlner, Ray; Moody, Dustin; Chen, Lily; Jordan, Stephen P; Liu, Yi-Kai; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Cc: Peralta, Rene
Subject: Re: Latest version of NISTIR and other documents for PQC

Have I mentioned how much I hate Word?

I'd like to make a bunch of punctuation or style changes (eliminate misplaced commas and break run-on sentences). When is the best time to do that?

Rene.

From: Perlner, Ray
Sent: Wednesday, January 13, 2016 5:24 PM
To: Moody, Dustin; Chen, Lily; Peralta, Rene; Jordan, Stephen P; Liu, Yi-Kai; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: RE: Latest version of NISTIR and other documents for PQC

Here's my text in section 4

From: Moody, Dustin
Sent: Tuesday, January 12, 2016 9:02 AM
To: Chen, Lily; Perlner, Ray; Peralta, Rene; Jordan, Stephen P; Liu, Yi-Kai; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu)
Subject: Latest version of NISTIR and other documents for PQC

The latest version of the PQC NISTIR (with comments from NSA and Donna) is attached. Also the current Call For Proposals, as well as a list of topics to be addressed in the Call for Proposals.

Dustin