

From: [Liu, Yi-Kai](#)
To: [Moody, Dustin](#)
Subject: Re: PQC meeting tomorrow
Date: Wednesday, January 13, 2016 2:26:37 AM

Hi Dustin,

Sorry I wasn't able to reply to this today, I will get back to you sometime tomorrow (Wednesday).
Sorry for the delay!

--Yi-Kai

From: Moody, Dustin
Sent: Tuesday, January 12, 2016 2:32 PM
To: Liu, Yi-Kai
Subject: RE: PQC meeting tomorrow

Yi-Kai,

I know you have much on your plate this month, but I'm hoping to get some help.

- I think the NISTIR is under control. I made some edits after our meeting, and Ray will add some for Section 4. We can then re-send out for comments from our group, and to Donna/Matt, etc... I don't want to review this to death, because we want it published before the end of the month. I think it's pretty good right now, but I appreciated the feedback from the NSA and Donna, as they gave us a perspective I think we were lacking.
- We determined that we only really need to worry about slides for PQCrypto. I am fine to give the presentation. I'll start working on them, but if you can help me come up with an outline of what we want to cover, that would be extremely helpful.
- Andy told me the NSA wants to coordinate with us before PQCrypto, so they know what we are going to say. Sounds reasonable. I don't think we've told our NSA friends what our plans are? It'd probably be good to do so. We could invite them to our crypto-club talk? Or hold a meeting just to go over it with them?
- Lily would like us to give a crypto-club talk to the group, so they can know what we are doing, and get them a bit up to speed since some of them will probably be pulled in to help with this project in the future. This will be on Feb. 3rd. Should we do a group presentation? Or just have one person do the whole thing? We need to create slides for this as well. I think our NISTIR provides a good outline for what we should cover. What do you think?

Dustin

From: Liu, Yi-Kai
Sent: Tuesday, January 12, 2016 12:48 AM
To: Moody, Dustin <dustin.moody@nist.gov>
Cc: yikailiu00@gmail.com
Subject: Re: PQC meeting tomorrow

Hi Dustin,

If it helps, I can try to join by google hangout tomorrow morning! Let me know...

--Yi-Kai

From: Jordan, Stephen P

Sent: Monday, January 11, 2016 10:28 AM

To: Moody, Dustin; Chen, Lily; Peralta, Rene; Perlner, Ray; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Liu, Yi-Kai; Find, Magnus G.

Subject: Re: PQC meeting tomorrow

Actually we are in Banff for the QIP conference, but still accessible by email.

Best regards,

Stephen

From: Moody, Dustin

Sent: Monday, January 11, 2016 10:21 AM

To: Chen, Lily; Peralta, Rene; Perlner, Ray; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Jordan, Stephen P; Liu, Yi-Kai; Find, Magnus G.

Subject: PQC meeting tomorrow

Everyone,

We have an internal PQC meeting tomorrow at 10am in B345. We will review some comments we have received back on the NISTIR, as well as continue to work on the Call For Proposals.

Dustin

- Stephen has told me that he and Yi-Kai will be in College Park.