From: Moody, Dustin
To: Liu, Yi-Kai
Subject: pqc stuff
Date: Thursday, January 21, 2016 12:20:04 PM
Attachments: PQCrypto 2016.pptx

Yi-Kai,

I didn't end up coming into work today, so I won't be dropping by. I was just going to go over things with you, since it feels like we have so much going on right now.

- I attached a first draft of my slides for PQCrypto. Let me know what you think. Then we can send them out to the group. I'll probably use some variation for my part of the crypto-club talk.
- Nobody has given me back any comments on the last round of the NISTIR. I gave everyone a deadline of yesterday, but got no responses. Should I send another email reminding people? We want to get this out this month if possible.
- Our next meeting with the NSA, we'll also tell them of our plans. I'll probably just use whatever version of the attached slides we have at that point. Hopefully they have some good pointers. We can also share with them our NISTIR.
- Feb 2nd, we have Michael Groves from the CESG in UK coming. He's one of the guys behind the soliloquy stuff. We met him on our trip to Germany last month, and invited him. He'll share with us some stuff ETSI has going on, and we can update him on our plans (probably using the slides)
- Feb 3rd we have our crypto-club talk. Daniel says he can do the multi-variate part, if we do it early. So after your introduction, it might be nice to let Daniel be the first person to talk. Or maybe after you do lattices? His constraint is that he is teaching at 11. I hope everyone is preparing. I have confirmed with everyone they will give their assigned parts. Should we practice it at some point? When?

Anything else you can think of?

Dustin