

**From:** [Moody, Dustin](#)  
**To:** [Perlner, Ray](#); [Liu, Yi-Kai](#); [Jordan, Stephen P](#); [Daniel C Smith \(daniel-c.smith@louisville.edu\) \(daniel-c.smith@louisville.edu\)](#); [Peralta, Rene](#)  
**Cc:** [Chen, Lily](#)  
**Subject:** Slides for our Crypto Club talk  
**Date:** Wednesday, January 27, 2016 9:30:01 AM  
**Attachments:** [PQC NISTIR v2.docx](#)  
[CNSA-Suite-and-Quantum-Computing-FAQ.pdf](#)

---

Everyone,

I hope everyone is doing alright with all the snow. I have a sore back from lots of shoveling, but am otherwise good. As a reminder, we are giving the crypto club talk next Wednesday, Feb 3rd, at 10am. Could everyone please finish their portion of the slides **by this Friday**? Then we can send them around to everyone for comments/suggestions before we give the talk. Mine will be essentially the slides I sent around for the PQCrypto announcement. Thanks,

One more thing. We were going to meet with the NSA yesterday, but NIST was closed. The NSA still wants to meet with us soon for us to give them an update on what we will be saying at PQCrypto. I'm still checking with them, but it might work out for us to meet tomorrow (Thursday) at 1pm, right before we all meet with Carl Miller. This is just a heads up that we might have a last minute meeting at that time. If so, we'll just go over the slides for PQCrypto with them, and get their input. They also gave me a new FAQ for their announcement about transitioning to PQCrypto. (attached)

Dustin

P.S. - Any last comments on the NISTIR (attached)? If not, we can start the process of getting it published.