

From: [Moody, Dustin](#)
To: [Perlner, Ray](#); [Liu, Yi-Kai](#); [Jordan, Stephen P](#); [Peralta, Rene](#); [Chen, Lily](#); [Daniel C Smith \(daniel-c.smith@louisville.edu\)](#) ([daniel-c.smith@louisville.edu](#)); [Bassham, Lawrence E](#)
Subject: PQC Crypto Club Talk
Date: Thursday, January 14, 2016 10:50:35 AM
Attachments: [Challenges in PQC standardization - 11302015 dbm.pptx](#)
[PQC at UMD.pptx](#)
[QuantumSafeWhitepaper.pdf](#)

Everyone,

We're going to give the crypto-club talk on Feb. 3rd, at 10am, on our PQC project and its upcoming plans. I'm thinking we should plan for roughly 90 minutes of talking, which would leave ample time for questions. To ease the burden of preparing, I would like to break up the presentation, and have several of us give different parts of it. Here's my initial thought for how we could do this:

- 1) (10 min) Yi-Kai Introduction. Impact of quantum on PKC/NIST standards. What are quantum computers, Shor's algorithm, Grover's algorithm. What is post-quantum crypto. Difference with quantum crypto/QKD. NIST project/team. Why this all matters right now. Then lead into broad overview of the main candidates.
- 2) (10 min) Yi-Kai or Ray Lattice-based crypto summary
- 3) (10 min) Ray Code-based crypto summary
- 4) (10 min) Ray Hash-based signatures
- 5) (10 min) Rene Multivariate crypto summary
- 6) (5 min) Rene Other candidates (isogeny-based, maybe braid groups?)
- 7) (5 min) Rene Overall summary. Our table of key sizes / timings. No obvious drop-in replacement. Which criteria are most important?
- 8) (10 min) Stephen State of quantum computing. Recent advances. Estimates of future progress (time/cost)
- 9) (20 min) Dustin NIST's plans. Workshop recap. NSA announcement. Transition importance. NISTIR. Call for Proposals. Evaluation criteria. Process. Timeline. How this will affect the group.

Does this make sense to everyone? Any suggestions. Yi-Kai, Ray, Rene, Stephen, are you good to cover these topics on Feb. 3rd? I think everyone should make their own slides using powerpoint, and then we can combine them all into one. I've attached a few resources that might be helpful. Also, on our wiki page we have slides from most of our past presentations:

<http://nistpqc.wikispaces.com/>

Dustin