From: Liu, Yi-Kai
To: Moody, Dustin
Subject: Re: PQC Crypto club talk
Date: Thursday, January 14, 2016 2:04:27 AM

Hi Dustin,

Thanks, that looks good! I think we should spend a fair amount of time on item 2, describing the different proposals for post-quantum cryptosystems, so that people have an idea of what are the pros and cons of the different candidates. Maybe we can borrow some text from the ETSI white paper?

Thanks -- let me know if you need help!

--Yi-Kai

From: Moody, Dustin
Sent: Wednesday, January 13, 2016 1:13 PM
To: Liu, Yi-Kai
Subject: PQC Crypto club talk

Yi-Kai,
Here's an outline I came up with for the crypto-club talk. Let me know if you can think of anything obvious I'm missing. Thanks,

Dustin

1) Introduction
   a. Impact of quantum computing on NIST standards
   b. What are quantum computers?
      i. Shor's algorithm, Grover's algorithm
   c. Post-quantum cryptography
      i. Difference with quantum crypto/qkd
      ii. NIST's team
   d. Why does this matter now?
2) Overview of potential solutions
   a. Broad families
   b. Table of key sizes / benchmarks show no obvious drop-in replacement
      i. Which evaluation criteria are most important?
   c. More details
      i. Lattices
      ii. Code-based
      iii. Multi-variate
      iv. Hash-based

v. Other

3) State of quantum computing

a. Overview of recent work

b. Estimates for future progress

i. Time/cost

4) NIST's plans

a. Our workshop recap

b. NSA's announcement

i. Transition importance

c. What we're doing now

i. NISTIR

ii. Call for proposals announcement at PQCrypto

iii. Evaluation criteria

1. Many questions here
2. Need public comment/workshops?
3. Security
4. IKE, TLS, X509 certs, etc…

iv. Process/timeline

v. How this might affect our group