From: Moody, Dustin (Fed)
To: Perlner, Ray A. (Fed)
Subject: Re: PQC talk
Date: Thursday, May 26, 2016 7:08:30 AM

Ray,
Thanks for the comments!

Dustin

From: Perlner, Ray (Fed)
Sent: Wednesday, May 25, 2016 5:13:08 PM
To: Moody, Dustin (Fed)
Subject: RE: PQC talk

Comments
Slide 3:

- Superposition – ability of quantum system to be in multiples states at the same time

Delete the s at the end of "multiples." I also think this bullet may be slightly misleading, but I'm not sure there's a way to not be misleading without going into the full formalism of probability amplitudes.
Slide 7:

- Finding discrete logarithms in abelian groups

Is the phrase "in abelian groups" really necessary. Doesn't the existence of a discrete log generally imply that the relevant group elements are part of an abelian subgroup anyway? If I were going to add a qualifier I would mention something someone with a passing familiarity with crypto might have heard of (e.g. elliptic curves, prime fields/modular arithmetic.)
Slide 16:
Why is there a table with performance estimates for signatures, but no corresponding table for encryption?
Slide 20:

- How long will a car in the field?

Check this sentence for grammar. I'm not sure what it's supposed to mean.

From: Moody, Dustin (Fed)
Sent: Wednesday, May 25, 2016 1:38 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>
Subject: PQC talk

Lily, Ray, Yi-Kai, Stephen,
Next week I'll be giving a talk to the automotive industry about post-quantum cryptography. I've attached my slides. I was hoping someone could take a quick look through them and make sure I am not saying anything really wrong, since I have a few on quantum computers, which are not my area of expertise. I used our NIST crypto club talk as a source of inspiration, and took some of the slides/ideas from that. Thanks!
Dustin