From: Perlner, Ray (Fed)
To: (b) (6)
Subject: FW: Slides for CBC2019
Date: Tuesday, April 30, 2019 4:59:00 PM
Attachments: Code based Crypto in the NIST competition.pptx

From: Kelsey, John M. (Fed)
Sent: Tuesday, April 30, 2019 4:56 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: Re: Slides for CBC2019

Ray,

I looked through your slides. They generally looked good, but I had a couple comments:

First, several slides had ***really*** small print on my screen—I think those will be unreadable on a slide. The ones I noticed were 2, 12, 19, 20, 22, 29, 38, 43, and 46. Several of those had equations in really small print, which is just evil. I'm not sure if that's something Powerpoint was specifically doing on my Mac, but if that's what the slides will look like on the screen, you might want to work on making the print bigger!

Second, several of your slides were just too wordy—I think you need to split them into two slides so they're not so dense. I noticed this especially for slides 20, 21, 45, and 46.

Third, I wonder if you could explain what you mean by the security definitions on slide 8 in your talk—even just a very brief reminder for the listeners might be nice. Also on slide 32, you use SD for syndrome decoding in the title—probably you should expand that to the actual words the first time you use it, like you do for a bunch of other terms (ISD, for example).

Thanks,

--John

From: "Perlner, Ray (Fed)" <ray.perlner@nist.gov>
Date: Tuesday, April 30, 2019 at 16:30
To: internal-pqc <internal-pqc@nist.gov>
Subject: Slides for CBC2019

Hi all. I'm giving an invited talk at the Eurocrypt associated event CBC2019 in Darmsdadt on May 18th. Here are my slides. I'm sending them now because I will be away at PQCrypto next week. Please let me know if you have any comments or suggestions.
Thanks,
Ray