From: Moody, Dustin (Fed)
To: Chen, Lily (Fed)
Subject: Re: slides for ICMC
Date: Wednesday, August 25, 2021 11:15:57 AM
Attachments: PQC ICMC 2021.pptx

Thanks, Lily.

I made the suggested changes.

From: Chen, Lily (Fed) <lily.chen@nist.gov>
Sent: Tuesday, August 24, 2021 5:25 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: slides for ICMC

Hi, Dustin,

The slides are good. Blue is my favorite color . Here are some comments.

- Page 6, "Classic McEliece, the ~~other~~ finalist, is code-based" – may remove "other" or say "Finalist Classic McEliece is code based. (The title is "The Other KEMs". Maybe too many "other".)
- Page 6: "The ~~final~~ alternate SIKE is based on isogenies of elliptic curves" (remove "final").
- Maybe page 7 and page 8 can coordinate better. "The signatures (page 7)" and "The status of the signatures (page 8). The attacks on multivariate signatures can be moved to page 7. Use page 8 to discuss diversity issues of signatures.
- Page 8: Under "Jan 2021 pqc-forum post from NIST", make the second bullet relate to the next page's onramp.
- Page 9: I am wondering whether "Announcements" is needed. The 4th round and on ramp will be explained in the next page.
- Page 10: It may be helpful to separate 4th round and onramp to two high level bullets.
- Page 13: The text is good. Can we verbally say something like NIST will consider the IPR impact when making selections? Actually, even though we did not receive a lot feedback, it is clear that the candidates with IPR issues would not be adopted.
- Page 16: Change "Oct '20" to "Oct. 2020"
- Page 16: Change "ISO/IEC JTC 1 SC27 WG2 is also studying stateful-hash based signatures" to "ISO/IEC JTC 1 SC27 WG2 also initiated a project to standardize stateful-hash based signatures as in ISO/IEC 14888-4"

Lily

From: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Tuesday, August 24, 2021 12:15 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Subject: slides for ICMC

Lily,

Here's the slides I made for the ICMC talk.

Dustin