From: Chen, Lily (Fed)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed)
Subject: Re: ICMC slides
Date: Tuesday, April 30, 2019 4:15:50 PM
Attachments: ICMC2019-chen-04292019dm-changed - Read-Only.pptx

Hi, Dustin and Ray,

Thank you for the comments. I accepted all of them. The last bullet on page 12 was intent to say that we want to hear different preferences for the tradeoffs. Please check if what I put there makes sense.

Lily

From: Dustin Moody <dustin.moody@nist.gov>
Date: Tuesday, April 30, 2019 at 12:36 PM
To: Lily Chen <lily.chen@nist.gov>, Ray Perlner <ray.perlner@nist.gov>
Subject: RE: ICMC slides

Lily,
See the attached. Looks good.

Dustin

From: Chen, Lily (Fed)
Sent: Tuesday, April 30, 2019 9:07 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>
Subject: ICMC slides

Hi, Dustin and Ray,

Can you please review the slides and let me know your comments? The talk is 30 minutes and the audience are more industry people (crypto module). I tried not to talk specific for each second round candidates but hope to give them a general picture. One thing I am struggling with is whether to give some examples on key size, signature size, ciphertext, processing time (cycles), etc. those can be implementation specific. Would you think those could mislead people?

Thanks,

Lily