From: Lily Chen
To: Moody, Dustin (Fed)
Subject: Re: 1st cut as Asiacrypt slides
Date: Wednesday, November 15, 2017 6:12:43 PM

Hi, Dustin,

Thanks for sending the draft. It covers every aspect on our PQC “competition”. Here are a few comments.

Page 2 RSA and factoring may be changed to RSA on factoring to be consistent with the bullet above.

Page 4 check font and sentence.

Page on standards activities,change three six months to four six months.

Lily

On Tue, 11/14/17, Moody, Dustin (Fed) <dustin.moody@nist.gov> wrote:

Subject: 1st cut as Asiacrypt slides
To: "Liu, Yi-Kai (Fed)" <yi-kai.liu@nist.gov>, (b) (6) "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, (b) (6) "daniel-c.smith@louisville.edu" <dcsmit11@exchange.louisville.edu>
Date: Tuesday, November 14, 2017, 2:22 AM

Yi-Kai, Ray, Jacob, Lily,
Daniel,
I’m
slated to give a 50 minute talk at Asiacrypt at the start of December. I figure it should be 45 minutes + 5 minutes for questions or so. I put together some slides for my first draft. Can you take a look and tell me what you think? I only have 36 slides, so I could certainly expand on some areas that I maybe only mentioned on one side. Let me know also if there are things I put in, that you don’t think need to be there. Is there anything I didn’t talk about that you think should get covered? Thanks,

Dustin