From: Moody, Dustin (Fed)
To: Cooper, David (Fed)
Subject: RE: PQCrypto talk
Date: Tuesday, April 30, 2019 2:45:00 PM

Thanks – I'll make those changes.

From: David A. Cooper <david.cooper@nist.gov>
Sent: Tuesday, April 30, 2019 2:36 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQCrypto talk

On 4/30/19 9:16 AM, Moody, Dustin (Fed) wrote:

> Everyone,
> I'll be giving a talk (45 minutes) at PQCrypto next week. Here's a first draft of slides.
> Let me know of any comments/suggestions, etc… Thanks,

Hi Dustin,

Just a couple of comments.

I think some clarification is needed on the cryptanalysis of LAC on slide 32. The text could be interpreted to mean that the LAC spec was broken and needed to be modified. However, if I understand correctly, the attack was just against the particular (non-constant-time) implementation, and the fix was just to modify the implementation to be constant time.

Slide 36 - LMS is now RFC 8554: https://mailarchive.ietf.org/arch/msg/cfrg/K-BxrBhh_VEL4F32_N1UPfiVlqQ

Thanks,

Dave