From: Liu, Yi-Kai (Fed)
To: Moody, Dustin (Fed)
Subject: Re: 1st cut as Asiacrypt slides
Date: Thursday, November 16, 2017 1:18:05 PM

Looks good! If you like, you could also mention Tor and Signal as possible applications... they are not so commonly used, but they might be early adopters of PQC.

Cheers,

--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Thursday, November 16, 2017 11:32:36 AM
To: Liu, Yi-Kai (Fed)
Subject: RE: 1st cut as Asiacrypt slides

Yi-Kai, I added slide 27. Let me know what you think.

Dustin

-----Original Message-----
From: Liu, Yi-Kai (Fed)
Sent: Monday, November 13, 2017 6:05 PM
To: Moody, Dustin (Fed) <dustin.moody@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>
Subject: Re: 1st cut as Asiacrypt slides

Cool! I think the slides look fine. One suggestion would be to make a slide that shows the complete hardware/software "stack" for post-quantum crypto. Maybe, something like this:

Upper layer: Web browsers, certificates. Higher level protocols like TLS and IKE. Other applications that use PQC, such as software updates and secure boot.

Middle layer: Post-quantum encryption, signatures and key exchange. (Also, hybrid modes with elliptic curve crypto.)

Lower layer: Libraries like NTL and GMP. Block ciphers like AES. Hash functions like SHA-3. Random number generators, provided by operating system or hardware. (Also, hardware support for maintaining state for hash-based signatures.)

Cheers,

--Yi-Kai

From: Moody, Dustin (Fed)
Sent: Monday, November 13, 2017 1:22:12 PM
To: Liu, Yi-Kai (Fed); (b) (6) ; Perlner, Ray (Fed); Alperin-Sheriff, Jacob (Fed); (b) (6) ; daniel-c.smith@louisville.edu
Subject: 1st cut as Asiacrypt slides

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