From: Peralta, Rene (Fed)
To: (b) (6) ; Perlner, Ray A. (Fed)
Cc: Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E. (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Smith-Tone, Daniel C. (Fed); Regenscheid, Andrew R. (Fed)
Subject: Re: Slides for RWC talk
Date: Tuesday, January 3, 2017 4:57:31 PM

Thanks, I fixed PKC -> PKE on slide 3 and added code-based signatures (my intention is to say that we are agnostic on what is good at this point, and that the "..."s mean I am not listing everything).

I meant to use key-agreement instead of KEM. I only have 20 minutes, so can't go much into details.

Rene.

From: Daniel Smith (b) (6)
Sent: Tuesday, January 3, 2017 11:42 AM
To: Perlner, Ray (Fed)
Cc: Peralta, Rene (Fed); Alperin-Sheriff, Jacob (Fed); Bassham, Lawrence E (Fed); Chen, Lily (Fed); Jordan, Stephen P (Fed); Liu, Yi-Kai (Fed); Miller, Carl A. (Fed); Moody, Dustin (Fed); Smith-Tone, Daniel (Fed); Regenscheid, Andrew (Fed)
Subject: Re: Slides for RWC talk

I agree with point 1. I'm not an expert on the code-based stuff, but I think that the code-based signatures have a better foundation than multivariate encryption, so if only one is to be listed, it should be the other way around. I think that if it is not too inconvenient, both should be listed. Efficient and secure schemes within both frameworks are entirely plausible, even if we are very unlikely to develop sufficient trust in them within our timeline.

On Tue, Jan 3, 2017 at 11:14 AM, Perlner, Ray (Fed) <ray.perlner@nist.gov> wrote:

> I have two nitpicks. Not sure either is worth changing though.
>
> 1) You have Multivariate listed for both signature and PKE, but code-based is only listed for PKE. The way I'd describe the current situation is that code-based is mostly for PKE and multivariate is mostly for signature, but each has some plausible proposals for obtaining the other functionality. I wouldn't necessarily say that code-based signature proposals are any worse than multivariate encryption proposals, so it seems a little odd to list one but not the other. That said, it's really a judgement call.
> 2) On slides 3 and 7, you use the following terms: "key agreement" "key establishment" and "PKC" (On slide 3: you probably mean PKE here.) The CFP primarily uses PKE and KEM, which have standard security and correctness definitions, although KEM may be unfamiliar to your audience.

Each is then allowed to be submitted for ephemeral-ephemeral only, or for both ephemeral-ephemeral and static-ephemeral. You probably at least want to change PKC to PKE on slide 3. Not sure you care about being ultra-precise with the rest of your terminology, though.

From: Peralta, Rene (Fed)
Sent: Tuesday, January 03, 2017 8:17 AM
To: Alperin-Sheriff, Jacob (Fed) <jacob.alperin-sheriff@nist.gov>; Daniel Smith (b) (6); Bassham, Lawrence E (Fed) <lawrence.bassham@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Miller, Carl A. (Fed) <carl.miller@nist.gov>; Moody, Dustin (Fed) <dustin.moody@nist.gov>; Perlner, Ray (Fed) <ray.perlner@nist.gov>; Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Cc: Regenscheid, Andrew (Fed) <andrew.regenscheid@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Slides for RWC talk

Dear all,

I managed to delete all copies of my talk in Hanoi, so I made a new set of slides for tomorrow's talk at RWC (attached).

Any comments are most welcome.

Happy New Year, Rene.