From: Peralta, Rene (Fed)
To: Moody, Dustin (Fed)
Cc: Peralta, Rene C. (Fed)
Subject: Re: Slides for RWC talk
Date: Tuesday, January 3, 2017 9:42:47 AM

After your email this is what I dug up:

"Post-quantum key exchange for the TLS protocol
from the ring learning with errors problem"

Rene.

From: Moody, Dustin (Fed)
Sent: Tuesday, January 3, 2017 9:39 AM
To: Peralta, Rene (Fed)
Subject: RE: Slides for RWC talk

It started with Jintai Ding's scheme, which was improved upon by Chris Peikert. It's similar to Diffie-Hellman, and based on lattices.

From: Peralta, Rene (Fed)
Sent: Tuesday, January 03, 2017 9:37 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: Slides for RWC talk

I didn't know that, thanks!

Rene.

From: Moody, Dustin (Fed)
Sent: Tuesday, January 3, 2017 9:17 AM
To: Peralta, Rene (Fed)
Subject: RE: Slides for RWC talk

Rene,
Thanks for giving this talk. You may want to mention on your slide 7, that there are some lattice-based key agreement methods, not just PKE and isogeny-based.

Dustin

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.