From:	Miller, Carl A. (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: PQC presentations
Date:	Monday, July 30, 2018 2:50:52 PM

No problem.

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, July 30, 2018 at 2:50 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: RE: PQC presentations

Thanks – sorry for the trouble!

From: Miller, Carl A. (Fed)
Sent: Monday, July 30, 2018 2:50 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC presentations

I can do lizard.

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, July 30, 2018 at 2:44 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>

Subject: RE: PQC presentations

You have great luck – Jacob took Falcon not very long ago. Here's the ones I have remaining:

nts-kem
ntru hrss kem, ntruencrypt
hila5
lotus
lac
lizard
titanium
Giophantus (there is an attack on it, but it still seems interesting)

From: Miller, Carl A. (Fed)
Sent: Monday, July 30, 2018 2:38 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC presentations

How about falcon?

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, July 30, 2018 at 1:58 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: RE: PQC presentations

He hasn't gotten back to me yet – but maybe it would be easiest if you picked a different one. Do any of them look good to you?

From: Miller, Carl A. (Fed)
Sent: Monday, July 30, 2018 1:55 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>

Subject: Re: PQC presentations

Ok – that's fine if so (he knows a lot more than I do). You can let me know, and I'll pick something else.

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Monday, July 30, 2018 at 8:13 AM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Subject: RE: PQC presentations

Carl,
Thanks – I think John Kelsey was going to do sphincs and gravity sphincs – I should have mentioned them. Let me check with him.

Dustin

From: Miller, Carl A. (Fed)
Sent: Friday, July 27, 2018 5:04 PM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: Re: PQC presentations

Hi Dustin –

I can do sphincs / gravity sphincs. A possible date would be August 14th. (I'm flexible to move to a nearby date also.)

-Carl

—————
Carl A. Miller
Mathematician, Computer Security Division
National Institute of Standards and Technology
Gaithersburg, MD

From: "Moody, Dustin (Fed)" <dustin.moody@nist.gov>
Date: Friday, July 27, 2018 at 2:07 PM
To: internal-pqc <internal-pqc@nist.gov>
Subject: PQC presentations

Everyone,

It'd be nice to finish up the remaining presentations in the next month or two. Can everybody please sign up to do one (or two)– that'd just about take care of it. The ones remaning:

- kyber
- sphincs/gravity sphincs
- falcon
- ntru hrss kem/ntruencrypt
- hila5
- kcl
- lac
- lizard
- titanium
- lotus
- Ledakem/pkc
- nts-kem

I've grouped a few together, since it'd be easy to do them in the same presentation. Ones which haven't been presented, but have been attacked are: DME, compact LWE, lepton, racoss, giophantus, and pqsigrm. These are a lower priority.

Dates available:

Tuesdays: July 31, Aug 7, Aug 14, Aug 21, Aug 28
Fridays: Aug 3, Aug 10, Aug 17, Aug 24, Aug 31

Please let me know what you can do. Thanks! After we finish the presentations, we can start comparing similar types of schemes….

Dustin