From:	Miller, Carl A. (Fed)
To:	Moody, Dustin (Fed)
Subject:	Re: PQC seminar
Date:	Friday, March 24, 2017 4:34:59 PM

Hi Dustin –

Here's my abstract for the talk next week. (Apologies that it is fairly broad – I can make it more specific if you'd like after I've developed the talk a little more.)

Have a great weekend!

-Carl

TITLE: Groebner bases for multivariate cryptography schemes

ABSTRACT: This talk will discuss computing Groebner bases as an attack on multivariate cryptography schemes. The goal is to discuss specific multivariate protocols and also to incorporate general concepts from commutative algebra. This talk will be a learning experience for me and hopefully for some of the audience as well.

—————

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, March 24, 2017 at 7:52 AM
To: "Alperin-Sheriff, Jacob (Fed)" <jacob.alperin-sheriff@nist.gov>, "Bassham, Lawrence E (Fed)" <lawrence.bassham@nist.gov>, "Chen, Lily (Fed)" <lily.chen@nist.gov>, Daniel Smith-Tone <daniel-c.smith@louisville.edu>, "Dworkin, Morris J. (Fed)" <morris.dworkin@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>, "Peralta, Rene (Fed)" <rene.peralta@nist.gov>, "Perlner, Ray (Fed)" <ray.perlner@nist.gov>, "Smith-Tone, Daniel (Fed)" <daniel.smith@nist.gov>, "Dang, Thinh H. (Fed)" <thinh.dang@nist.gov>, "Dang, Quynh (Fed)" <quynh.dang@nist.gov>
Cc: Daniel Smith (b) (6)
Subject: PQC seminar

This is a placeholder to reserve space on your calendar for our PQC seminar meetings.