

From: [Peralta, Rene \(Fed\)](#)
To: [Daniel C Smith \(daniel-c.smith@louisville.edu\)](#) ([daniel-c.smith@louisville.edu](#))
Cc: [Moody, Dustin \(Fed\)](#); [Perlner, Ray A. \(Fed\)](#); [Chen, Lily \(Fed\)](#)
Subject: Re: Reminder - PQC meeting this Friday at 1pm
Date: Friday, September 30, 2016 12:08:53 PM

I'll have to miss this. But it looks like your work is having some impact.
That's great!

Rene.

From: pqc-bounces@nist.gov <pqc-bounces@nist.gov> on behalf of Moody, Dustin (Fed) <dustin.moody@nist.gov>
Sent: Wednesday, September 28, 2016 1:29 PM
To: pqc
Subject: [Pqc] Reminder - PQC meeting this Friday at 1pm

Everyone,

We will have a PQC talk next week, on Friday, Sept. 30th, at 1pm. Note - this is after lunch, and not before lunch like we typically do. Daniel Smith-Tone will talk on some of Jintai Ding's ideas on extension field schemes. I think the paper is:

<https://eprint.iacr.org/2015/1184.pdf>

[Extension Field Cancellation: a New Central Trapdoor for ...](#)

eprint.iacr.org

Extension Field Cancellation: a New Central Trapdoor for Multivariate Quadratic Systems Alan Szepieniec^{1,2}, Jintai Ding³ and Bart Preneel¹ Department of Electrical ...

Thanks,

Dustin

Brad/Dave/Jerry, let me know who I need to register