From:	Moody, Dustin (Fed)
To:	Petzoldt, Albrecht R. (IntlAssoc)
Subject:	RE: PQC relevant talk
Date:	Wednesday, January 11, 2017 9:41:00 AM

Great!

From: Petzoldt, Albrecht R. (IntlAssoc)
Sent: Wednesday, January 11, 2017 9:41 AM
To: Moody, Dustin (Fed) <dustin.moody@nist.gov>
Subject: RE: PQC relevant talk

Thank you for the reminder. I will come to the talk. I know where it is.

From: Moody, Dustin (Fed)
Sent: Wednesday, January 11, 2017 9:37 AM
To: Petzoldt, Albrecht R. (IntlAssoc) <albrecht.petzoldt@nist.gov>
Subject: PQC relevant talk

Albrecht,

If you are here, there is a talk today at 10 by Bill Fefferman, a postdoc at the Univ. of Maryland, which you may be interested in attending. I'll stop by and show you where it is.

Dustin

===
Title:

Characterizing the power of quantum computation

Abstract:

More than two decades after Shor's discovery of an efficient quantum factoring algorithm, we still do not have a complete knowledge of the power of quantum computation. In fact, despite the prevailing belief that quantum computers are more powerful than their classical counterparts, this still remains a conjecture backed by little mathematical evidence. Likewise, we cannot rule out the possibility that quantum computers can efficiently solve problems far harder than factoring. Obtaining a better understanding of this power will therefore be crucial to understanding cryptography in the near future. In this talk we will both introduce new capabilities for quantum computers and rigorously characterize the limitations of their power.