From: Chen, Lily (Fed)
To: Moody, Dustin (Fed); Perlner, Ray A. (Fed); Jordan, Stephen P (Fed); Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu); Liu, Yi-Kai (Fed); Peralta, Rene C. (Fed)
Subject: RE: Upcoming PQC meetings
Date: Monday, June 13, 2016 1:25:35 PM

Hi, Dustin:
I think we can invite other members to attend for these two talks. How about “internal-crypto” or CRYPTO-CLUB (include externals and need visitor registration)?
Lily

From: Moody, Dustin (Fed)
Sent: Monday, June 13, 2016 12:41 PM
To: Perlner, Ray (Fed) <ray.perlner@nist.gov>; Chen, Lily (Fed) <lily.chen@nist.gov>; Jordan, Stephen P (Fed) <stephen.jordan@nist.gov>; Daniel C Smith (daniel-c.smith@louisville.edu) (daniel-c.smith@louisville.edu) <daniel-c.smith@louisville.edu>; Liu, Yi-Kai (Fed) <yi-kai.liu@nist.gov>; Peralta, Rene (Fed) <rene.peralta@nist.gov>
Subject: Upcoming PQC meetings
6/14 (tomorrow) Dustin will talk on the supersingular isogeny diffie-hellman
6/21 Gorjan Alagic will speak on:
Hidden shifts and quantum attacks on symmetric-key cryptography
---
It is well-known that large-scale quantum computers would devastate the current public-key cryptography infrastructure. Symmetric-key systems, on the other hand, are widely believed to be quantum-secure. However, this belief is predicated on various assumptions about the security model, some of which may be too strong. Kuwakado and Morii showed that, under a certain notion of ``quantum CPA,’’ many classically-secure symmetric-key schemes can be completely broken by a simple quantum adversary. The broken schemes include the 3-round Feistel cipher, the Even-Mansour cipher, the Encrypted-CBC-MAC, and many others. In this talk, we will begin by describing these attacks and the underlying security model. We will then propose a generic adaptation, which can be applied to all of the broken schemes, and which is likely to provide quantum security even in the ``quantum CPA’’ model. In particular, we will show that breaking some of the adapted schemes would imply efficient quantum algorithms for the Hidden Shift Problem. Based on joint work with Alex Russell.