From: Chen, Lily (Fed)
To: Mehta, Ketan L. (Fed); Sonmez Turan, Meltem (Fed)
Subject: Re: Reminder: Crypto Reading Club - May 24 - @NCCoE
Date: Wednesday, May 24, 2017 10:36:46 AM

Hi, Ketan:

We did not set up a dial in option. Sorry.

Lily

From: "Mehta, Ketan (Fed)" <ketan.mehta@nist.gov>
Date: Wednesday, May 24, 2017 at 9:47 AM
To: "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>, Lily Chen <lily.chen@nist.gov>
Subject: RE: Reminder: Crypto Reading Club - May 24 - @NCCoE

Hi Meltem / Lily – Is there a dial-in number?

-Ketan

From: crypto-club-bounces@nist.gov [mailto:crypto-club-bounces@nist.gov] **On Behalf Of** Sonmez Turan, Meltem (Assoc)
Sent: Tuesday, May 23, 2017 4:39 PM
To: CRYPTO-CLUB <CRYPTO-CLUB@nist.gov>
Subject: [Crypto-club] Reminder: Crypto Reading Club - May 24 - @NCCoE

Hi everyone,

I would like to remind you that tomorrow Jintai Ding from U. of Cincinnati is going to give a talk titled "RLWE-based authentication and key reuse for RLWE-based key exchanges".

Abstract: In this talk, we will present new authentication schemes, where a prover tries to proves that he or she knows a secret solution to the RLWE problem without revealing any information on the solution. For an interactive scheme, we can prove the zero-knowledge property. We will also present a non-interactive scheme, and show how it can be used to build RLWE based key exchanges, where key reuse is also secure.

Date: May 24, 2017
Place: National Cybersecurity Center of Excellence, 9700 Great Seneca Hwy, Rockville, MD 20850, Room number:3D Hall 1
Time: 10:00AM-12:00PM

Regards,
Meltem