From:	Miller, Carl A. (Fed)
To:	Sonmez Turan, Meltem (Fed); Chen, Lily (Fed)
Cc:	Dworkin, Morris J. (Fed)
Subject:	Re: [Crypto-club] Crypto Reading Club - August 3
Date:	Monday, August 1, 2016 3:10:10 PM

Thanks.

-Carl

From: "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>
Date: Monday, August 1, 2016 at 3:09 PM
To: "Chen, Lily (Fed)" <lily.chen@nist.gov>, "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Cc: "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>
Subject: RE: [Crypto-club] Crypto Reading Club - August 3

Done.

From: Chen, Lily (Fed)
Sent: Monday, August 01, 2016 3:02 PM
To: Miller, Carl A. (Fed) <carl.miller@nist.gov>
Cc: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Subject: RE: [Crypto-club] Crypto Reading Club - August 3
Hi, Meltem and Morrie:
Can we add Carl?
Thanks,
Lily

From: Miller, Carl A. (Fed)
Sent: Monday, August 01, 2016 3:01 PM
To: Chen, Lily (Fed) <lily.chen@nist.gov>
Cc: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>; Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Subject: Re: [Crypto-club] Crypto Reading Club - August 3
Hi Lily —
I don't think I'm on the crypto-club list, it would be great to be added.
-Carl

From: "Chen, Lily (Fed)" <lily.chen@nist.gov>
Date: Monday, August 1, 2016 at 2:59 PM
To: "Miller, Carl A. (Fed)" <carl.miller@nist.gov>
Cc: "Dworkin, Morris J. (Fed)" <morris.dworkin@nist.gov>, "Sonmez Turan, Meltem (Assoc)" <meltem.turan@nist.gov>
Subject: FW: [Crypto-club] Crypto Reading Club - August 3
Hi, Carl:
Are you on the crypto-club mailing list? If not, would you like to be on? Meltem and Morrie can add you on?

Lily

From:crypto-club-bounces@nist.gov [mailto:crypto-club-bounces@nist.gov] **On Behalf Of** Sonmez Turan, Meltem (Assoc)
Sent: Monday, August 01, 2016 2:53 PM
To: CRYPTO-CLUB <CRYPTO-CLUB@nist.gov>
Subject: [Crypto-club] Crypto Reading Club - August 3

Hi everyone,

Our next crypto reading club is scheduled on August 3. Daniel Smith-Tone will give a talk titled *Multivariate Cryptography with "Big" Algebraic Structures*.

Abstract:*Since near the beginning of the history of multivariate public key cryptography there have been two basic strategies for constructing multivariate digital signatures and multivariate public key encryption schemes. These classes are often characterized as "Big Field" or "Small Field" schemes. Relaxing the definitions slightly we can encompass some more recent constructions, changing the moniker "Big Field" schemes to "Big Structure" schemes. We will discuss some of the basic techniques used to construct multivariate schemes, some of the new ideas for potentially achieving efficient encryption, and the main cryptanalytic techniques in this area. If there is sufficient time for preparation, we can play around with some computational examples*.

Date: August 3, 2016
Time: 10AM-12PM
Place: **222 B263** (Our usual place is reserved for another training)

Regards,
Meltem