From:	Chen, Lily (Fed)
To:	Nicky Mouha
Subject:	FW: [Crypto-club] Reminder - TODAY : Crypto Reading Club - August 3
Date:	Wednesday, August 3, 2016 9:56:00 AM
Attachments:	ATT00001.txt

From: crypto-club-bounces@nist.gov [mailto:crypto-club-bounces@nist.gov] **On Behalf Of** Sonmez Turan, Meltem (Assoc)
Sent: Wednesday, August 03, 2016 9:26 AM
To: CRYPTO-CLUB <CRYPTO-CLUB@nist.gov>
Subject: [Crypto-club] Reminder - TODAY : Crypto Reading Club - August 3

Dear all,

Date: August 3, 2016 TODAY

Time: 10AM-12PM

Place: **222 B263** (Our usual place is reserved for another training)

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