From: Sonmez Turan, Meltem (Assoc)
To: Smith-Tone, Daniel C. (Fed)
Subject: RE: Crypto Reading Club - Aug. 3
Date: Monday, August 1, 2016 2:01:05 PM

Thanks !

From: Smith-Tone, Daniel (Fed)
Sent: Monday, August 01, 2016 1:57 PM
To: Sonmez Turan, Meltem (Assoc) <meltem.turan@nist.gov>
Subject: RE: Crypto Reading Club - Aug. 3

Hi, Meltem,

I will talk on the following:

Title: 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.

Thanks, Meltem.

Cheers,

Daniel

From: Sonmez Turan, Meltem (Assoc)
Sent: Monday, August 01, 2016 9:19 AM
To: Smith-Tone, Daniel (Fed) <daniel.smith@nist.gov>
Cc: Dworkin, Morris J. (Fed) <morris.dworkin@nist.gov>
Subject: Crypto Reading Club - Aug. 3

Daniel,

Thanks for volunteering to give a reading club talk on Wednesday. Please send you title/abstract today.

Meltem