Joint Math Colloquium

Millersville University and Franklin & Marshall College

Speaker: **Dr. Ting Gu,**
Assistant Professor of Computer Science
Department of Computer Science
Elizabethtown College

Title: **Analysis of the Statistical Power of Correlation Attacks on Nonlinear Combiners**

Date: **October 19, 2017 (Thursday)**

Time: **4:00 pm – 5:00 pm**

Place: **Room 201, Wickersham Hall, Millersville University**

Contact: **Baoling Ma** **(717) 871-4263** **Baoling.Ma@millersville.edu**
Kevin S. Robinson **(717) 871-7313** **krobinson@millersville.edu**

Abstract:

Pseudorandom sequences generated by linear feedback shift registers (LFSRs) with nonlinear combining functions have been widely used as running key generators in stream ciphers. However, in 1985 Siegenthaler showed that if the keystream is correlated to (at least) one of the LFSR sequences, then a correlation attack against the individual LFSR sequence can significantly reduce the work needed for a brute-force attack. Since then, correlation attacks on nonlinear combining functions have been intensively investigated. Recently, Wei et al. (2011) and Gu et al. (2016) have modified Siegenthaler's attack by using nonlinear correlation functions. In this talk, I will explain Siegenthaler's classic attack and present a general framework for different statistical models that are used in correlation attacks and propose a more powerful test statistic based on the maximum likelihood ratio test. Our statistical model achieves better performance than those presented in Wei's and Gu's papers. More importantly, we prove that, for a nonlinear combiner that is correlation-immune of order k, then among all correlation functions that depends on k+1 variables, linear functions maximize the statistical power of classical correlation attacks.

Millersville University
COLLEGE OF SCIENCE AND TECHNOLOGY

Elizabethtown College