University of Puerto Rico Mayaguez Campus
Faculty of Arts and Sciences
Department of Mathematical Sciences
call box 9000, Mayagüez, P.R. 00681

THE DEPARTMENT OF MATHEMATICAL SCIENCES PROUDLY PRESENTS

COLLOQUIUM

Fall 2012

Asymptotic behavior of the exponential sum of distortions of symmetric polynomials

Dr. Luis A. Medina
UPR-Río Piedras
Sept 25th, 2012

Abstract: We consider distortions of symmetric boolean functions $\sigma_{n,k_1} + \cdots + \sigma_{n,k_s}$ in n-variable and degree k_s. Here, $\sigma_{n,k}$ represents the elementary symmetric polynomial of degree k in n variables. We compute the asymptotic behavior of boolean functions of the type

$$\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(X_1, \ldots, X_j)$$

for j fixed. In particular, we characterize all the boolean functions of the type

$$\sigma_{n,k_1} + \cdots + \sigma_{n,k_s} + F(X_1, \ldots, X_j)$$

that are asymptotic balanced. Balanced boolean functions are very important in some applications of cryptography.

Monzón Building, Room 201, 10:45 AM
Refreshments will be served
15 minutes before the colloquium, M203