Seminario conjunto ACGO y Matemáticas Discretas

Speaker
Carla Rafols (Ruhr Universitt Bochum)

Title
Hard-core predicates and list decoding

Abstract:

A hard-core predicate P of a one-way function f is a predicate of the input of f which is not leaked by f. There are many classical results regarding hard-core predicates of the most common cryptographically useful one-way functions such as RSA, discrete exponentiation or the Rabin function. A classical result by Goldreich and Levin states that every one-way function has a hard-core predicate.

At FOCS 2003, Akavia, Goldwasser and Safra gave a coding theoretic interpretation of Goldreich and Levin's result and an elegant list decoding methodology to prove that a predicate is a hard-core of a one-way function. Additionally, they showed how to use the methodology to get a simpler proof of many classical works on hard-core predicates, although their result did not apply to important results like the one that says that the bits in the middle of RSA, Rabin or the discrete exponentiation problem are hard-core (Hstad and Nslund, 1996).

In this talk I will explain this connection between list decoding and hard-core predicates of Akavia et al. I will also explain how, in joint work with Paz Morillo, we extended their results to the middle bits of these functions. The talk is aimed at a general public interested in theoretical computer science (not necessarily cryptographically savvy).

Host: Marcos Kiwi

Date: Friday May 09, 2014 - 16:15. Place: Sala de seminarios del CMM