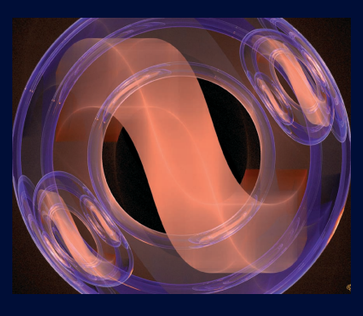
imdea matemáticas



imdea seminar

March 7, 2008

Módulo C-IX, sala 405
Facultad de Ciencias - UAM
Ciudad Universitaria de Cantoblanco
28049 Madrid
How to get there: www.imdea.org

Matemáticas, la llave para el conocimiento, el desarrollo y la innovación
Mathematics, the key for knowledge, development & innovation

10:30 · 11:30 Signcryption or How to Kill Two Birds in One Stone

Yuliang ZHENG
University of North Carolina at Charlotte

Signcryption is a public key cryptographic technique that simultaneously fulfills data unforgeability and confidentiality with significantly smaller overhead than that required by "digital signature followed by public key encryption". This talk introduces examples of signcryption, surveys the current state of the art in the field and motivates future research directions.

11:30 · 12:00 Coffee break

12:00 · 13:00 Kleptography: Using Cryptography Against Cryptography

Moti YUNG
Columbia University and Google

Traditionally in the practice of cryptography, tamper proof hardware which passes some testing was considered as a guarantor of "trust" (and security) in cryptosystems implementations. We will review our work on Kleptography, an area which contradicts this common belief and deals with attacks on "black box" cryptographic implementations (e.g., tamper-proof hardware implementation). Kleptographic attacks enable a designer and implementor of an algorithm to cause leaking of secrets, employing alternative algorithms, in a way which is (1) un-noticeable; and (2) exclusive. Namely, No one else can tell whether the "black-box" implementation contains the kleptographic attack or not, and only the attacker gets the advantage of the leakage (even if another party reverse-engineer the device in the future). We will discuss kleptographic algorithms attacking Factoring based and Discrete Logarithm based systems, and will also review recent developments. This is based on joint work with Adam Young.