UNIVERSIDAD COMPLUTENSE MADRID

**Facultad de Informática**

# ANUNCIO DE CONFERENCIA

## Secuencias, un número detrás de otro

Dr. Domingo Gómez Pérez
Universidad de Cantabria

Facultad de Informática
Sala de Grados • 1 de abril de 2016 • 18:00
*Entrada libre hasta completar el aforo*

Resumen:

Las secuencias de elementos son utilizadas en diversas áreas con diferentes usos. Son fundamentales para la aproximación numérica de integrales, en criptografía, para la localización de objetos en radar.... Dada la multitud de usos, muchas veces se requieren propiedades muy diversas e incluso contradictorias. Por ello, existen múltiples construcciones, adaptadas a resolver cada uno de los diferentes problemas. El objetivo de esta charla es dar una visión general de los usos de las secuencias. Esta charla estará dividida en tres bloques: En el primer bloque, se introducirá el estudio de secuencias desde el punto de vista de sus propiedades pseudo aleatorias con aplicaciones a la seguridad de la información. Esto incluye la generación de claves seguras eficientemente. Se discutirá la definición de pseudo aleatoriedad en múltiples dimensiones y la generación eficiente. En el segundo bloque se hablará de las secuencias para la aproximación numérica, utilizando muestreo automático. Esto es de especial aplicación en métodos quasi-Monte Carlo con aplicación a la matemática financiera y en la predicción de varianza de estimadores sistemáticos. En el último bloque se hablará de las secuencias utilizadas en la localización de objetos mediante la técnica radar.

Sobre Domingo Gómez:

Domingo Gómez Pérez es profesor contratado doctor en el departamento de Matemáticas, Estadística y Computación en la Universidad de Cantabria. Estudió en la Universidad de Cantabria, donde recibió su doctorado con calificación Cum Laude y mención de "Doctorado Europeo" en el año 2006. Trabajó como investigador Postdoctoral en el centro Johann Radon Institute for Computational and Applied Mathematics en Austria. Posteriormente, ha realizado estancias en diversos centros de investigación entre los que destacan Philips Research Eindhoven (2011-2012), Macquarie University (2013) y University of New South Wales (2014). Entre sus intereses se encuentran el estudio de secuencias con aplicaciones en seguridad informática, radar y sonar, medidas de pseudo aleatoriedad, métodos Monte Carlo y quasi-Monte Carlo y teoría de cuerpos finitos. Ha participado en varios proyectos de investigación a nivel nacional e internacional. Colaboró con la empresa Philips Research en el diseño y desarrollo del protocolo HIMMO destinado al intercambio seguro de claves en redes de sensores. Cuenta con más de 50 publicaciones científicas en diversas áreas y también ha formado parte del comité organizador de diversas conferencias de matemática discreta y criptografía. Durante este último año ha estado involucrado en la realización del HIMMO Challenge, en el desarrollo del Software CountEm para la estimación de manifestantes en fotografías aeréas y en la organización del Workshop on Mathematics in Communications 2016.