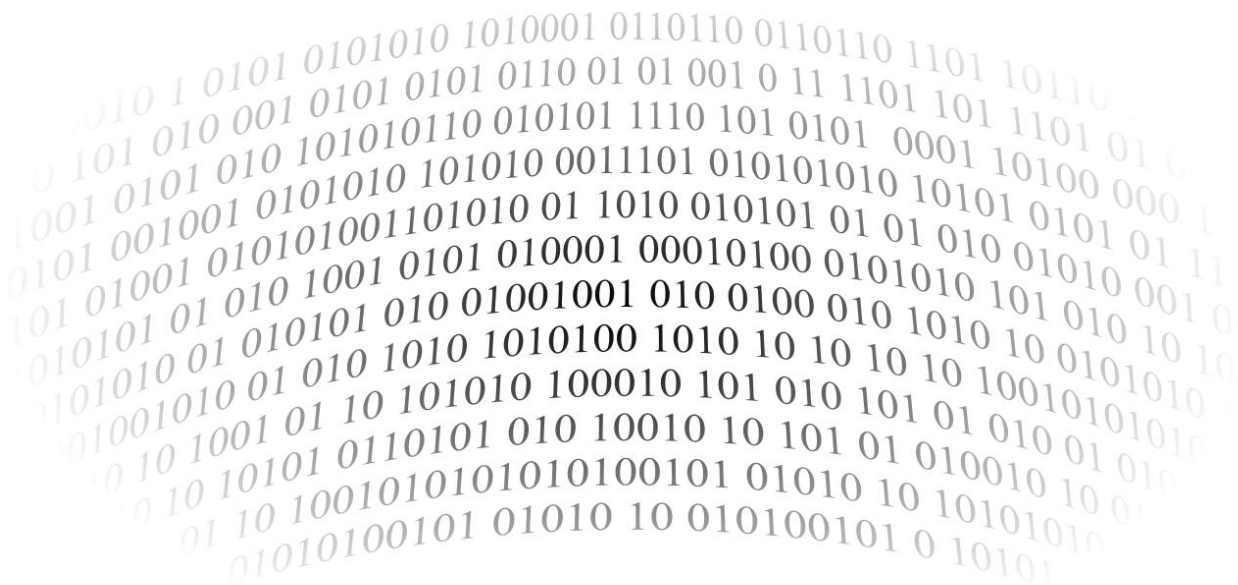

Conferencia

"Linealización de los generadores *shrinking* a través de CA"

Sara Díaz Cardell (Universidad de Alicante)

Resumen: Algunos generadores de secuencias cifrantes pueden ser modelizados como estructuras lineales basadas en autómatas celulares lineales. En este trabajo se presenta la modelización lineal de los generadores criptográficos *shrinking* y auto-*shrinking* a través de autómatas celulares lineales uniformes utilizando la ley 102 (o la 60). La linealidad de estos autómatas se puede utilizar para el criptoanálisis de estos generadores de secuencias.

Fecha: Martes 12 de mayo
Hora: 17.00 horas
Lugar: Seminario de Análisis y Estadística
Facultad de Ciencias II, Planta Baja
Información: clementa.alonso@ua.es
Departamento de Estadística e Investigación Operativa
Universidad de Alicante