CONFERENCIA

Viernes 22 marzo, 13h.

Aula B03, Facultad de Ciencias (Oviedo)

La futura navegación segura por internet ya está aquí: disección de los estándares post-cuánticos del NIST

IGNACIO FERNÁNDEZ RÚA

Catedrático de Álgebra,
Universidad de Oviedo

Navegar por internet y encontrarse una “nao” cuántica no será un peligro en el futuro: los algoritmos que nos protegerán en esos mares de superposición, entrelazamiento y ganancias cuánticas están listos para ser estandarizados. En esta charla realizaremos un análisis de las propuestas del NIST del pasado mes de agosto: ML-KEM y ML-DSA. No será necesario que traigas EPI: la disección será solamente superficial, no nos meteremos con sus vísceras, solamente con su diseño de alto nivel.

Financiado por la Unión Europea NextGenerationEU