CONFERENCIA

Martes 12 diciembre, 13h.

Sala de grados, Facultad de Ciencias (Oviedo)

CRIPTOGRAFÍA SEGURA FRENTE A ADVERSARIOS CUÁNTICOS [UNA GUÍA PARA EL OSADO PRINCIPIANTE]

Mª Isabel González Vasco

Catedrática de la Universidad
Carlos III de Madrid

El avance de las tecnologías cuánticas impulsa hoy enormes avances en diferentes ámbitos. En criptografía, este avance se percibe a la vez como una terrible amenaza y una gran oportunidad. En esta charla, intentaremos dar respuesta a alguna de las preguntas que se plantean en este campo, ¿cómo se aborda, desde las matemáticas, el diseño de herramientas y protocolos criptográficos seguros frente a adversarios cuánticos? ¿qué tipo de criptografía podremos utilizar en el futuro? ¿es sensato empezar ya la transición hacia una nueva criptografía? Sin entrar en demasiados detalles técnicos, intentaremos presentar las ideas y herramientas que pueden ayudar a responder a estas cuestiones.

Financiado por la Unión Europea NextGenerationEU