UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

POSGRADO

Criptografía Post-Cuántica y HPC: Desafíos y Oportunidades

Sandra Catalán Pallarés
Universidad Jaume I, Castellón

Facultad de Informática
Sala de Grados - jueves 16 de octubre de 2025 - 16:00
Entrada libre hasta completar el aforo

Resumen:

La inminente llegada de los computadores cuánticos plantea una amenaza sin precedentes a los sistemas criptográficos tradicionales, especialmente aquellos basados en RSA y curvas elípticas. Frente a este panorama, la criptografía post-cuántica surge como un campo crítico para garantizar la seguridad de la información en el futuro. Sin embargo, la adopción de estos nuevos algoritmos no está exenta de retos: su complejidad computacional y los requisitos de rendimiento hacen imprescindible el uso de infraestructuras de High-Performance Computing (HPC). En este contexto, el HPC desempeña un papel clave al permitir acelerar la validación de propuestas criptográficas, evaluar su escalabilidad y preparar su implementación a gran escala. Casos de uso recientes, pruebas de rendimiento y estudios comparativos muestran cómo estas arquitecturas de cómputo paralelo impulsan la investigación y el desarrollo de soluciones resilientes a la computación cuántica, consolidando un nuevo paradigma en la seguridad de la información y abriendo oportunidades de innovación en la comunidad científica y tecnológica.

Sobre Sandra Catalán Pallarés:

Sandra Catalán es ingeniera en Informática y obtuvo el título de doctorado en la misma disciplina en la Universitat Jaume I (UJI). Actualmente, es investigadora postdoctoral Ramón y Cajal en el grupo High Performance Computing and Architectures. Sandra ha desarrollado su investigación postdoctoral en el Barcelona Supercomputing Center (BSC), y en la Universidad Complutense de Madrid (UCM). Por otro lado, ha trabajado para diferentes proyectos a nivel autonómico, nacional y europeo. Su investigación se centra en el ahorro energético en clústers de escala moderada y procesadores de bajo consumo, algoritmos y bibliotecas paralelas de álgebra lineal y arquitecturas asimétricas. Las estancias de investigación que ha realizado en otros centros como el BSC, The University of Texas en Austin e IBM Research Zurich, le han permitido profundizar en estos campos.