Instituto Universitario de Investigación de Matemáticas y Aplicaciones Universidad Zaragoza

Departamento de Matemáticas Universidad Zaragoza

Facultad de Ciencias Universidad Zaragoza

Seminario de Doctorado IUMA
Conferencia

por

Sofía Sirón Barluenga

Universidad de Zaragoza

Título:

Fully Homomorphic Encryption based on ring learning with errors.

Resumen:

El *Fully Homomorphic Encryption* (FHE) se define como un esquema de encriptación que permite evaluar circuitos arbitrarios C sobre datos cifrados, satisfaciendo

$$\text{Decrypt}(\text{Eval}(C, \text{Encrypt}(m))) = \text{Eval}(C, m).$$

La relevancia del *Fully Homomorphic Encryption* radica en su capacidad para permitir computación segura sobre datos confidenciales sin necesidad de descifrado. La técnica de *bootstrapping*, introducida por Craig Gentry, garantiza que la evaluación pueda extenderse a circuitos de profundidad arbitraria.

En la criptografía post-cuántica (PQC), la seguridad no depende exclusivamente de asunciones de complejidad algorítmica clásica, sino del estudio riguroso de problemas matemáticos subyacentes. Los esquemas postcuánticos basados en retículos constituyen uno de los paradigmas de seguridad más robustos frente a los ataques cuánticos.

En esta charla, comenzaremos estudiando un problema de criptografía basada en retículos, el *Ring Learning With Errors* (RLWE), formulado sobre anillos cociente de la forma $R_q = \mathbb{Z}_q[x]/\langle \Phi_n(x) \rangle$, con $\Phi_n(x)$, cierto polinomio irreducible. Veremos cómo la seguridad del criptosistema depende de la dificultad de distinguir muestras ruidosas de distribuciones uniformes en R_q. Finalmente, explicaremos la construcción de esquemas FHE basados en el problema RLWE.

Fecha: Jueves, 16 de abril de 2026.
Hora: 17:00 horas.
Lugar: Seminario Rubio de Francia. Primera planta, Edificio B, Facultad de Ciencias.
Meet: `https://meet.google.com/zjj-cnyf-euk`