**Seminario: Criptografía pos-cuántica basada en reticulados**

Descripción:

El desarrollo de criptosistemas resistentes a la computación cuántica es de gran importancia para las comunicaciones y el comercio. En los últimos años, los criptosistemas basados en reticulados y el problema LWE han atraído mucho interés por su flexibilidad y egficiencia, especialmente con las competiciones de NIST para la estandarización de protocolos pos-cuánticos, con 3 de los primeros 4 finalistas utilizando este paradigma como base de su seguridad (Kyber, Saber y Dilithium). Además, el criptosistema NTRU (el sistema que inició el interés en este uso de los reticulados) puede ser utilizado para criptografía homomorfica, permitiendo computaciones en datos encriptados, lo que es de gran utilidad para el análisis de bases de datos confidenciales, etc.

Temas principales:

- La computación cuántica: potenciales y limitaciones

- Introducción a los reticulados en anillos de polinomios

- El problema LWE y otros problemas relacionados en reticulados

- La aritmética eficiente para criptosistemas basados en reticulados

- Los protocolos de intercambios de llaves Kyber y Saber

- El protocolo de firmas Dilithium

- NTRU y la criptografía homomorfica