Instituto Universitario de Investigación de Matemáticas y Aplicaciones Universidad Zaragoza

Departamento de Matemáticas Universidad Zaragoza

Seminario Geometría y Topología

Conferencia

por

Martín Avendaño

Centro Universitario de la Defensa

Título:

"Un análisis del criptosistema post-cuántico DME"

RESUMEN:
Los sistemas criptográficos de clave pública (basados en la dificultad del problema de factorizar enteros) son vulnerables frente a la hipotética computadora cuántica, cuya realización parece inminente. Cualquiera que esté capturando en este momento mensajes que hayan sido cifrados con estos criptosistemas, podrá en el futuro (quizás no muy lejano) decifrarlos sin problemas. La pregunta que surge naturalmente es si existen sistemas criptográficos de clave pública que no sean vulnerables a ataques con máquinas cuánticas. La agencia americana NIST abrió recientemente una convocatoria pidiendo propuestas de tales sistemas. El objetivo principal de esta charla es describir el sistema DME propuesto por el profesor Ignacio Luengo de la Universidad Complutense de Madrid. Este sistema cambia el problema de factorizar enteros, por el de factorizar un cierto mapa polinomial como composición de tres mapas lineales y dos exponenciales. Veremos también que aunque el sistema no ha sido quebrado aún en su forma mas general, puede ser vulnerable a ataques algebraicos. En un trabajo reciente (en conjunto con Miguel Angel Marco-Buzunariz de la Universidad de Zaragoza), hemos probado que ciertas instancias del DME pueden romperse calculando intersecciones de variedades lineales con una variedad tórica afín. En la charla también presentaré las ideas principales de este tipo de ataques.

Fecha: Miércoles, 3 de abril de 2019
Hora: 11:00 horas
Lugar: Edificio de Matemáticas, Aula 13