Seminario de Doctorado IUMA

Conferencia

por

Alba Larraya Sancho

Basque Center for Applied Mathematics (BCAM) y
Universidad del País Vasco / Euskal Herriko Unibertsitatea (UPV/EHU)

Título:

PQC: Ataques CCA en sistemas de cifrado basados en LWE

Resumen:

Los sistemas criptográficos basados en lattices son considerados prometedores para la criptografía post-cuántica debido a su resistencia a los ataques de ordenadores cuánticos. Sin embargo, como cualquier sistema criptográfico, son vulnerables a una variedad de ataques, incluidos los ataques de texto cifrado elegido (CCA), que representan un desafío significativo para su seguridad. Esta charla presenta resultados recientes que hemos obtenido sobre la vulnerabilidad de los sistemas criptográficos basados en redes a los ataques CCA. Comenzaremos con una introducción a lattices y los problemas difíciles que se conocen y sobre los que se basa la seguridad de los esquemas de cifrado, como el Problema del Vector Más Corto (SVP) y el Learning With Errors (LWE). Luego presentaremos los ataques CCA que hemos diseñado para atacar estos sistemas. En particular hablaremos del esquema Crystals-Kyber y como atacar la versión CPA-segura. Veremos la eficiencia de estos ataques y hablaremos de las medidas que se pueden tomar para evitarlos. El objetivo de esta charla es proporcionar una visión general de la investigación actual sobre la seguridad de la criptografía basada en redes, así como las implicaciones más amplias para los sistemas criptográficos en la era post-cuántica.

Fecha: Jueves, 14 de noviembre de 2024.
Hora: 17:00 horas.
Lugar: Seminario Rubio de Francia. Primera planta, Edificio B, Facultad de Ciencias.