CC1. Arantxa Zapico (UNC)

El problema de "learning with errors"

Debido a la aparición del Algoritmo de Shor para factorizar números naturales con computadoras cuánticas, la criptografía se ha visto obligada a buscar problemas alternativos al de factorización en los cuáles basar su seguridad en un futuro posible. Entre los sistemas más prometedores, se encuentran los basados en lattices. En esta charla, abordaremos el problema de "Learning with errors" (LWE) y algunos sistemas criptográficos inspirados en éste. Además, presentaremos reducciones del LWE a problemas de lattices, lo que representa hoy en día su mayor prueba de seguridad.