Seminario de Álgebra, Geometría algebraica y Singularidades - ULL
La Laguna, 1 de julio de 2021, 15:30 horas (GMT+1)

Códigos correctores de errores en computación segura

Ignacio Cascudo Pueyo
Instituto IMDEA Software, Madrid[1]

En esta charla hablaré algunos usos de los códigos de errores en criptografía. Aunque su utilización más conocida es para el cifrado, con los conocidos esquemas de McEliece y Niederreiter, los códigos correctores de errores han encontrado también en los últimos años varias aplicaciones interesantes en el terreno de la computación segura, que permite a varios participantes colaborar para realizar algún tipo de cálculo que involucre sus datos privados, pero sin revelar estos datos al resto de participantes. En esta charla hablaré de su uso en este área, así como en algunas de las herramientas que se utilizan en ella como son esquemas de compartición de secretos y pruebas de conocimiento cero. Este tipo de aplicaciones motiva nuevas cuestiones acerca de los códigos correctores de errores como son el estudio de las propiedades del denonimado cuadrado del código (definido como el código generado por los productos coordenada a coordenada de cada par de palabras del código original).

[1]Instituto IMDEA Software
Madrid
ignacio.cascudo@imdea.org