Seminario de Álgebra, Geometría algebraica y Singularidades
La Laguna, 31 de octubre de 2023, 16:00 horas (GMT+0)

Private Information Retrieval with codes

Julien Lavauzelle
Université Paris 8[1]

Private information retrieval (PIR) allows to query an entry from a remote database, without revealing the identity of the desired entry to the servers storing the database. One usually wants to build protocols with low communication complexity, low computation, and low storage overhead.

In this talk, I will give an overview of several constructions of information-theoretically secure PIR schemes. As a common feature, these constructions share the use of coding techniques in order to model queries and/or to pre-encode the database. Constructions vary depending on the way the database is stored (replicated or encoded), or on the parameters one wants to optimize (communication, computation, or storage).

[1]LAGA
Université Paris 8
Francia
julien.lavauzelle@univ-paris8.fr