SEMINARIO

Seyma Bodur

Universidad de Valladolid

Private Information Retrieval Schemes Using Cyclic Codes

Abstract: Many protocols protect the user and server from third parties while accessing the data. Nevertheless, no security measure protects the user from the server. As a result of this demand, Private Information Retrieval (PIR) protocols emerged. A Private Information Retrieval (PIR) scheme allows users to retrieve data from a database without disclosing to the server information about the identity of the data retrieved. We consider in this work that data is stored in a Distributed Storage System (DSS) since, if data is stored in a single database, one can only guarantee information-theoretic privacy by downloading the full database, which has a high communication cost.

The use of a GRS, or an MDS code, requires working over a big base field. In order to address this issue, since binary base fields are desirable for practical implementations, in this work, we propose to use cyclic codes to construct PIR schemes. In 2018, R. Freij-Hollanti et al. proposed the scheme which considers a storage and retrieval code with a transitive group and provides binary PIR schemes with the highest possible rate. Reed-Muller codes were considered in that work, cyclic codes are considered in this work since they have a transitive group and can be defined over a binary field as well.

In this work, we provide a family of optimal binary PIR schemes. Our PIR schemes have the advantage, with respect to PIR schemes from MDS codes, that they can be defined over a binary field. Moreover, they provide a larger constellation of parameters than the binary PIR schemes using Reed-Muller codes and they even outperform them in some cases.

This talk is based on joint work with Edgar Martínez-Moro and Diego Ruano.

Seminario del IMUVa, Edificio LUCIA
Jueves 30 de Junio de 2022 (11:30)