SEMINARIO

Seyma Bodur

Universidad de Valladolid

Private Information Retrieval Protocols

Abstract: A Private Information Retrieval (PIR) scheme allows users to access data from a database without disclosing to the server information about the identity of the data retrieved. The analysis of these protocols involves two main approaches: considering that the information is stored in one or several servers. For the several servers approach, one may consider information-theoretic privacy and they are secure against unlimited computation sources. A single-server PIR scheme is based on computational privacy and assumes computers have limited power. Therefore, it requires computational difficulty. When a system consists of a single server, it is possible to achieve information-theoretic privacy by transmitting the entire database. However, this approach is not feasible. The first computational PIR scheme based on coding theory is presented by Holzbaur, Hollanti, and Wachter-Zeh in [2]. However, Bordage and Lavauzelle presented an attack that occurs in polynomial time and with high probability. We present a single-server PIR scheme using codes over rings that utilize the coding theory perspective of Holzbaur, Hollanti, and Wachter-Zeh, which provides resistance against the attack described in [1]. This talk is based on a joint work with Edgar Martínez-Moro and Diego Ruano.

[1] Sarah Bordage and Julien Lavauzelle (2020). On the privacy of a code-based single-server computational PIR scheme. Cryptogr. Commun.,13:519–526 .

[2] Holzbaur L, Hollanti C, Wachter-Zeh A. (2020). Computational Code-Based Single-Server Private Information Retrieval.IEEE International Symposium on Information Theory, ISIT 2020 - Proceedings. IEEE. 2020. p. 1065-1070.

Seminario del IMUVa, edificio LUCIA
Jueves 27 de Junio de 2024 (10:00)