SEMINARIO

Seyma Bodur

Universidad de Valladolid

Single Server Private Information Retrieval Schemes over Rings

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. Information-theoretic privacy and computational privacy are two different approaches to this protocol. The schemes based on information theoretic privacy is secure against unlimited computational sources and are only possible in a Distributed Storage System (DSS) with more than one server. If there is one server in a system, information-theoretic privacy can be provided by sending the whole database, but this is an infeasible method. The PIR scheme based on computational privacy assumes computers have limited power. And hence, it requires computational difficulty.

The first computational PIR scheme based on coding theory is presented in [Lukas Holzbaur, Camilla Hollanti, and Antonia Wachter-Zeh. Computational code-based single-server private information retrieval. In 2020 IEEE International Symposium on Information Theory (ISIT), pages 1065–1070, 2020.]. However, Bordage and Lavauzelle presented an attack that occurs in polynomial time and with high probability [Sarah Bordage and Julien Lavauzelle. On the privacy of a code-based single-server computational PIR scheme. Cryptogr. Commun., 13:519–526, 2020.].

We consider in this work that data is stored in a single database and again used the coding theory perspective of the scheme Holzbaur, Hollanti and Wachter-Zeh but for codes over rings where the attack in [Sarah Bordage and Julien Lavauzelle. On the privacy of a code-based single-server computational PIR scheme. Cryptogr. Commun., 13:519–526, 2020.] is not feasible. We present a single server computational PIR scheme based on cyclic codes over Z_m, where m is a composite number.

Joint work with Edgar Martínez-Moro and Diego Ruano

Seminario del IMUVa, edificio LUCIA
Miércoles 28 de Junio de 2023 (9:30)