Aalto University
School of Science

School of Science
https://www.aalto.fi/school-of-science

Dissertation press release 07.02.2019

Providing user privacy for information retrieval

Title of the dissertation

Private Information Retrieval from Coded Storage

Contents of the dissertation

Along with the technological advancements and the remarkable growth of digital data storage, new challenges arise regarding the reliability of the digital data storage and the privacy of the users. A distributed storage system (DSS) can store big amounts of data for a long time over possibly unreliable servers. As for the privacy concern of the users, much effort has been spent in trying to find systems and schemes that allow users to communicate, search, upload and download files while maintaining their privacy. One of those schemes is private information retrieval (PIR).

PIR allows the users to hide the identity of files they request from a DSS. In other words, a PIR scheme allows the user to retrieve any file from a DSS without revealing the file identity to any of the servers. It goes without saying that, to achieve privacy, the user should download a bigger amount of data than the size of the desired file. The extra amount of data downloaded is quantified by the communication complexity of a PIR scheme. Naturally, downloading all the data from the DSS hides the identity of the desired file, but has a very high communication complexity, especially as the number of files in a DSS is typically very large. Moreover, this also raises the question of the server privacy, meaning that the user should not be able to retrieve any extra information about the undesired files while retrieving a certain file. Schemes taking into account the server privacy are called symmetric PIR (SPIR) schemes.

This thesis focuses on constructing PIR schemes for different DSSs with low communication cost. We study different DSSs, which reduce the storage cost of the system while providing reliability. We construct PIR schemes on such systems, where we consider both cases, the case where the servers in the DSS do not communicate, and the case where some subsets of the servers communicate in an effort to figure out the desired file identity. Moreover, we consider the SPIR problem, and consider the case where some servers may be unresponsive, such that they do not respond to the sent query, and the case where the servers may be malicious or unsynchronized and thus give false information to the user. Last but not least, this thesis also considers schemes providing privacy for users requesting data from a DSS over a random linear network.

Field of the dissertation

Mathematics

Doctoral candidate

Razane Tajeddine, M.Sc.
Born in 1990

Time of the defence

07.03.2019 at 14 (2 pm)

Place of the defence

Aalto University School of Science, lecture hall M1, Otakaari 1, Espoo

Opponent

Professor Simon Blackburn, Royal Holloway, University of London, UK

Custos

Professor Camilla Hollanti, Aalto University School of Science, Department of Mathematics and Systems Analysis

Doctoral candidate's contact information

Razane Tajeddine
Department of Mathematics and Systems Analysis
0503272485
rstajeddine@gmail.com
razane.tajeddine@aalto.fi

A doctoral dissertation is a public document and shall be available at Aalto University, School of Science's notice board in Konemiehentie 2, Espoo at the latest 10 days prior to public defense.