

Private Subset Retrieval: Performance Bounds and Achievability Schemes

Alex Sprintson

Texas A&M University

We study private subset retrieval, a variant of the multi-message Private Information Retrieval (PIR) problem, where a user requests a subset of messages from a predefined set system over X . This set system is represented as a hypergraph, where vertices correspond to messages and hyperedges define the permissible subsets that a user can request. In this setting, the capacity—the maximum achievable ratio of the information retrieved by the user to the total amount of data downloaded from the servers—depends on the structure of the hypergraph. We establish a lower bound on the capacity of the private subset retrieval problem and propose several achievability schemes, including a sequential retrieval scheme, where messages are retrieved one by one and a linear programming framework for identifying near-optimal vector-linear solutions for a given hypergraph. These results provide insights into the fundamental limits of private subset retrieval and offer strategies for efficient data retrieval under constrained query sets.

In Special Session 40 on Network Coding and Related Fields at the Mathematical Congress of the Americas 2025.