Capacity of Quantum Private Information Retrieval with Multiple Servers

Masahito Hayashi
Nagoya University

Abstract: We study the capacity of quantum private information retrieval (QPIR) with multiple servers.In the QPIR problem with multiple servers, a user retrieves a classical file by downloading quantum systems from multiple servers each of which containing the whole classical file set, without revealing the identity of the retrieved file to any individual server. The QPIR capacity is defined as the maximum rate of the file size over the whole dimension of the downloaded quantum systems. When the preexisting entanglement among servers are assumed,we prove that the QPIR capacity with multiple servers is 1 regardless of the number of servers and files. We propose a rate-one protocol which can be implemented by using only two servers.This capacity-achieving protocol outperforms its classical counterpart in the sense of the capacity, server secrecy, and upload cost.The strong converse bound is derived concisely without using any secrecy condition. We also prove that the capacity of multi-round QPIR with multiple servers is 1.In addition, we discuss the case with collusion of all but one of servers.

The contents are available from arXiv:1903.10209 and 1903.12556. This study is based on joint work with Seunghoan Song.