ANNE BROADBENT, University of Ottawa

Specious Adversaries and Quantum Private Information Retrieval

Private information retrieval is a cryptographic scheme that allows a client to secretly query a database. We show that information-theoretic single-server quantum private information retrieval requires a linear amount of communication to be secure against specious adversaries, which are the quantum analog of honest-but-curious adversaries. We also stress the importance of adequate comparison between classical and quantum adversaries—unfair comparisons might lead to an unjustified advantage for the quantum case.