Contribution ID : **9** Type : **not specified**

Masahito Hayashi: Two-Server Oblivious Transfer for Quantum Messages

Tuesday, 13 June 2023 15:00 (60)

Oblivious transfer is considered as a cryptographic primitive task for quantum information processing over a quantum network. It is an essential building block for secure multiparty computation. It is known that one-server oblivious transfer is impossible. When the task is the transmission of classical messages, protocols for two-server oblivious transfer exist, i.e., existing protocols work under the assumption that two servers do not communicate with each other. However, when the task is the transmission of a quantum state, no existing method works even under the above two-server assumption. We propose two-server oblivious transfer protocols for quantum messages for the first time.
The full paper is available from https://arxiv.org/abs/2211.03308