Quantum Byzantine Agreement for Any Number of Dishonest Parties

Vicent Cholvi
Departament de Llenguatges i Sistemes Informàtics, Universitat Jaume I, Campus Rius Sec s/n, Castelló, 12071 Spain

Reaching agreement in the presence of arbitrary faults is a fundamental problem in distributed computation, which has been shown to be unsolvable if one-third of the processes can fail, unless signed messages are used. In this paper, we propose a solution to a variation of the original BA problem, called Detectable Byzantine Agreement (DBA), that does not need to use signed messages. The proposed algorithm uses what we call *Q-correlated lists*, which are generated by a *quantum source device*. Once each process has one of these lists, they use them to reach the agreement in a classical manner. Although, in general, the agreement is reached by using $m + 1$ rounds (where m is the number of processes that can fail), if less than one-third of the processes fail it only needs one round to reach the agreement.

This paper has been published in *Quantum Information Processing* 21, 151 (2022). It is available in open access at https://doi.org/10.1007/s11128-022-03492-y.

This work has been partially funded by the Spanish Ministry of Science and Innovation grant PID2019-109805RB-I00 (ECID) cofunded by FEDER, and by the Departament de Llenguatges i Sistemes Informàtics of the Universitat Jaume I.