Lorenzo Maccone

Department of Physics, University of Pavia
Via Bassi 6 - 27100 Pavia, Italy
maccone@unipv.it

Blind Computation

L. Maccone, V. Giovannetti, T. Morimae, T.G. Rudolph

We give a cheat sensitive protocol for blind universal quantum computation that is efficient in terms of computational and communication resources: it allows one party to perform an arbitrary computation on a second party's quantum computer without revealing either which computation is performed, or its input and output. The first party's computational capabilities can be extremely limited: she must only be able to create and measure single-qubit superposition states. The second party is not required to use measurement-based quantum computation. The protocol requires the (optimal) exchange of O(J log N) single-qubit states, where J is the computational depth and N is the number of qubits needed for the computation.

This talk is based on the paper arXiv:1306.2724 from which this abstract is taken.