Bocconi

13 OCTOBER 2022
12:00 PM

Bocconi University
Room 3.E4.SR03
Via Röntgen 1 Milano (3rd floor)

Efficient Verification of Quantum Computation

Speaker

GIULIO MALAVOLTA
UC Berkeley

Abstract

Can the result of a quantum computation be verified more efficiently than redoing the computation from scratch? In this talk we describe how, using suitable cryptographic tools, one can verify the validity of any quantum computation in time poly-logarithmic in the runtime of the original computation. Furthermore, the verification procedure is entirely classical. As a central technical ingredient, we develop a complete “Heisenberg-like” proof of soundness for a protocol to classically verify quantum operations. We then discuss the computational assumptions needed for constructing the necessary cryptographic machinery, and we outline some outstanding open problems that remain. Based on the following work: https://arxiv.org/pdf/2206.14929.pdf (Crypto’22).

Università Bocconi
DEPARTMENT OF COMPUTING SCIENCES