Invited talk: Formal Verification of Quantum Protocols

Yuxin Deng

East China Normal University

Summary

We introduce two formal methods of verifying quantum communication protocols. One is to take advantage of quantum process algebras and the other is to make use of theorem provers. With a suitable notion of behavioural equivalence and a decision method, we can determine if an implementation of a protocol is consistent with its specification. Ground bisimulation is a convenient behavioural equivalence for quantum processes because of its associated coinduction proof technique. We exploit this technique to design and implement two on-the-fly algorithms for the strong and weak versions of ground bisimulation to check if two given processes in quantum CCS are equivalent. We have developed a tool that can verify interesting quantum protocols such as the BB84 quantum key distribution scheme. At a low level, quantum protocols can be implemented by quantum circuits. We propose a symbolic approach to reasoning about the functional correctness of quantum circuits. It is based on a small set of laws involving some basic manipulations on vectors and matrices. This symbolic reasoning scales well and is suited to be automated in Coq, as demonstrated with some typical examples.

FAVPQC 2022: International Workshop on Formal Analysis and Verification of Post-Quantum Cryptographic Protocols, October 24, 2022, Madrid, Spain