QUANTUM INNOVATION 2023

CC-04-02

Numerical method for security analysis of quantum key distribution based on complementarity

Toshihiko Sasaki

The University of Tokyo

Abstract

The main goal of the security analysis in the quantum key distribution is to provide the security proof for general attacks in the finite-key regime. In recent years, it is also important to consider imperfections of the devices. It increases the number of parameters in the device models and makes security analysis complicated. One possible way to deal with this situation is to use numerical methods to provide the security analysis. The question is how to make it adaptable to a wide range of situations and how to achieve high key rate even in the finite-key regime. We will present recent progress in a numerical method for the security proof based on complementarity.