量子信息科技学术研讨会 (2018.9.17-21)

报告

利用 McDiarmid 不等式增加秘密密鑰率

Improving the Secret Key Rate without Changing the Experimental Setup by McDiarmid Inequality

周海峰教授 | 香港大学物理学系教授

讲者介绍 Biography

Professor Chau has been working on quantum information science since 1996 shortly after the announcement of the Shor algorithm. He is an expert in quantum cryptography.

报告摘要 Abstract

The foci of quantum key distribution researches are making it practical, reliable, error-tolerant and most importantly fast. To achieve a high provably secret key rate in practical situation with a finite raw key length, most works to date focus on either better protocol, better experiments or better theories to deal with issues of imperfect apparatus. Is it possible that the secret key rate of a current experiment is actually higher than the one given by existing proofs? Here I show that this is indeed the case in the finite raw key length situation. I first point out why existing proofs are ineffective in this aspect; and then I introduce powerful method from classical statistics community to tackle the problem. In particular, I show how to use McDiarmid inequality to increase the provably secure key rate of the BB84 scheme with decoy through a realistic optical fiber channel by at least 30% without changing existing experimental setup and classical processing procedure. Details of this work can be found in arVix:1806.05073.