量子信息科技学术研讨会 **(2018.9.17-21)**

报告

免于侧信道攻击的只用若相干态光源的量子密钥分发方案

Towards Practical Long Distance Side-channel-free Quantum Key Distribution with Coherent states only

王向斌教授 | 清华大学物理系

讲者介绍 Biography

PhD from National University of Singapore
2000-2006 Postdoctoral Researcher in JST Japan
2006- Professor of Physics in Tsinghua University

报告摘要 Abstract

We show that a side-channel-free (SCF) source does not have to be an ideal source from which all states are identical in the side-channel space by introducing the idea of mapping from ideal source. We propose a 3-state sending-or-not-sending protocol and its twin-field form for quantum key distribution (QKD). We show that, the protocol is secure and side-channel-free (i.e., both source side channel free and measurement device independent) provided that the source satisfies two conditions in the simple operational space only: phase randomization and the lower bound of single-photon fraction. Calculation shows that one can reach a side-channel-free secure distance over 300 km using only coherent-state source. We use worst-case analysis which takes no limitation to the channel or detection loss for security. Our protocol is immune to all adverse due to side channels such as the photon frequency spectrum, emission time, propagation direction, spatial angular moment, and so on. Numerical simulations show that our scheme can reach a side-channel-free result for quantum key distribution over a distance longer than 200 km given the single-photon-interference misalignment error rate of 30%, and a distance longer than 300 km given the single-photon-interference misalignment error rate of 10%. Effects of imperfection in phase randomization is also discussed.