
中国科大等发表量子保密通信综述论文

作者：writer 来源：中国科学院

本文原地址：<https://www.iikx.com/news/progress/9785.html>

本文仅供学习交流之用，版权归原作者所有，请勿用于商业用途！

5月26日，中国科学技术大学潘建伟及其同事徐飞虎、张强，与清华大学马雄峰、多伦多大学Hoi-Kwong Lo等，应邀在国际物理学综述期刊、美国物理学会的《现代物理评论》（Reviews of Modern Physics）上发表题为《基于现实器件的安全量子密钥分发》（Secure quantum key distribution with realistic devices

）的长篇综述论文。该论文系统阐述了量子密码的原理、理论和实验技术，并指出，经过全球学术界三十余年的共同努力，现实条件下量子密码的安全性已经建立起来，尤其是测量器件无关等量子密钥分发协议的提出，彻底关闭了量子密码在物理实现过程中可能出现的安全性风险，为实现基于现实器件的安全量子密码铺平了道路。此论文为量子密码的广泛应用以及标准化制定奠定了坚实基础。

量子通信是量子信息科学的重要分支，它是指利用量子比特作为信息载体来进行信息交互的通信技术。量子通信中最典型的应用方式之一是量子保密通信（量子密钥分发）。量子密钥分发可以提供一种原理上安全的通信手段，是迄今唯一的安全性得到严格证明的通信方式，也是首个从实验室走向实际应用的量子信息技术。它已经成为物理学最有活力的前沿研究方向之一。经过我国科学家的长期努力，成功发射了世界首颗量子科学实验卫星“墨子号”，并完成了国际上最大规模的量子保密通信光纤网络“京沪干线”。

近年来，随着量子密钥分发逐步走向实用化研究，量子密钥分发的现实安全性得到了国际上的广泛关注。主要研究实际系统中的器件并不完全符合协议的数学模型而引入的潜在安全性风险和解决方案。这其中涌现了很多关于量子安全攻防的研究，以及多个新型的量子密钥分发协议。其中，潘建伟团队在国际上首次实验实现多个重要的新型协议，包括诱骗态、测量器件无关和双场等协议，极大地推动了量子密钥分发的现实安全性。

潘建伟等受邀为《现代物理评论》撰写的综述论文长达60页。文章详细回顾了量子密码的发展历史，深入讨论了量子密钥分发的现实安全性，并展望了量子密钥分发技术的未来发展趋势。《现代物理评论》杂志专门发布评论指出：“在科学家的长期共同努力下，国际学术界在现实条件下量子密钥分发的理论和实验上都取得了重要的进展，现实安全性得到了彻底的提升”，“这篇论文描述了当前最优的量子安全理论，以及实际保证量子密码系统现实安全性的方法和关键技术。”

[论文链接](#)

研究团队单位：中国科学技术大学

更多 科学进展 请访问 <https://www.iikx.com/news/progress/>

本文版权归原作者所有，请勿用于商业用途，[爱科学iikx.com](http://www.iikx.com)转发