

量子密钥分发 (QKD)
 的
 安全性
 分析
 与
 应用
 前景

Thursday, 1 June 2023 16:05 (35 minutes)

量子密钥分发 (QKD) 是一种利用量子力学原理实现密钥分发的技术。其安全性基于量子力学的基本原理，如量子态的不可克隆性和量子纠缠等。QKD 可以分为基于单光子的 QKD 和基于连续变量的 QKD 两种类型。本文主要介绍基于单光子的 QKD 的安全性分析。

在 QKD 过程中，发送方 (Alice) 和接收方 (Bob) 通过量子信道传输量子态。由于量子态的不可克隆性，任何窃听者 (Eve) 试图窃取密钥都会引入扰动，从而被 Alice 和 Bob 检测到。因此，QKD 的安全性依赖于量子力学原理，而不是计算复杂性。

本文首先介绍 QKD 的基本原理，然后分析其安全性。我们将讨论 QKD 的安全性分析模型，包括信道模型、窃听模型和攻击模型。我们将分析 QKD 的安全性，并讨论其应用前景。

本文的研究结果表明，QKD 是一种安全的密钥分发技术，其安全性基于量子力学原理。QKD 的应用前景广阔，包括量子通信、量子网络和量子计算等。

Presenter: 张三, 李四, 王五