吉林大学学报(工学版)　2008 38 (06): 1480-1484　ISSN: 1671-5497　CN: 22-1341/T

对两个使用Bell测量基的量子密钥分配协议的分析与改进

李恕海，明洋，王育民

西安电子科技大学 综合业务网络国家重点实验室，西安 710071

收稿日期 2007-7-3　修回日期　网络版发布日期 2008-10-25　接受日期

摘要

对两个使用EPR对和Bell测量基的量子密钥分配协议的安全性进行了分析，从测量不同位置的量子比特的拓扑结构出发，证明了这两个协议的等价性。指出了协议执行双方使用Bell测量基在两个量子比特上的检错策略的合理性，但在有效确定错误数量方面却有一个缺陷，即不能够检测到出现在所有量子上同样类型的错误，从而构成安全性的一个隐患。并利用|0+>,|0->,|1+>,|1->测量基解决了这个缺陷，同时不需要目前还比较难以实现的完全Bell测量，并给出了安全性证明。

关键词　信息处理技术；量子密码学；密钥分配；完全Bell基测量；纠缠转移

分类号　TN918. 1

Security analysis and improvements of two QKD protrocols using complete Bell state measurements

LI Shu-hai，MING Yang，WANG Yu-min

State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China

Abstract

Security analysis for two quantum key distribution protocols was presented by using EPR pair and complete Bell state measurements. It is also shown that those two protocols are totally equivalent from the point of view of the topological structures on how to measure the corresponding qubits at random. The paper proved that Bell state measurement basis can detect some special eavesdropping behaviors, but not all of them. Thus, this enables all same errors occurring on the sampling qubits undetected, which impairs the security of quantum key distribution protocols. |0+>, |0->, |1+>, |1-> measurement basis was used to replace complete Bell state basis, which can avoid the incomplete error detecting strategy. And unconditionally security was guaranteed bythe improved protocol.

Key words information processing；quantum cryptography key distribution complete Bell state measurement entanglement swapping

DOI:

通讯作者 王育民 ymwang@xidian.edu.cn

扩展功能

本文信息

- Supporting info
- PDF(671KB)
- [HTML全文](0KB)
- 参考文献

服务与反馈

- 把本文推荐给朋友
- 复制索引
- 文章反馈
- 浏览反馈信息

相关信息

- 本刊中 包含“信息处理技术；量子密码学；密钥分配；完全Bell基测量；纠缠转移 ”的 相关文章
- 本文作者相关文章
  - 李恕海
  - 明洋
  - 王育民