

安全技术

基于部分纠缠态的量子安全直接通信协议

徐红云1, 杨新元2, 马智2, 吕欣3

(1. 乌鲁木齐总医院, 乌鲁木齐 830000; 2. 信息工程大学应用数学系, 郑州 450002; 3. 国家信息中心, 北京 100045)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 提出一种新的带认证的三方量子安全直接通信协议。该方案利用共享的三粒子部分纠缠态和CNOT门来编码和译码, 两方可同时向第三方传递秘密消息, 共享的部分纠缠态可重复使用。在理想信道下, 协议对于非相干攻击是安全的。该方案通过认证可以验证客户端身份的合法性, 部分纠缠态在实际中容易制备和保存, 能够实现两方同时跟第三方直接通信。

关键词 [密码学](#); [量子密码学](#); [量子安全直接通信](#); [部分纠缠态](#)

分类号 [TN918.1](#)

DOI:

通讯作者:

作者个人主页: [徐红云1](#); [杨新元2](#); [马智2](#); [吕欣3](#)

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF\(92KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“\[密码学\]\(#\); \[量子密码学\]\(#\); \[量子安全直接通信\]\(#\); \[部分纠缠态\]\(#\)”的 相关文章](#)
- ▶ [本文作者相关文章](#)