首页　　|期刊简介|编委会|投稿须知|期刊订阅|资料下载|编委论坛

抗特洛伊木马攻击的量子密钥多播通信协议

Multicast communication protocol based on quantumkey distribution against trojan horse attacking

作者	单位
马鸿洋，范兴奎	1. 青岛理工大学 理学院，山东 青岛 266033；2. 中国海洋大学 信息科学与工程学院，山东 青岛 266100

中文摘要：

　　提出在一个源量子节点与M个目的量子节点组成的网络中抗量子特洛伊木马攻击的多播通信协议，源量子节点构建2n+δ个EPR纠缠对，并用发送序列标记；在发送序列中随机选取n个作为检测纠缠对，利用CHSH不等式进行信道检测；发送序列中剩余n+δ个EPR纠缠对变形为非正交的量子态作为密钥，将广播明文信息分组编码成密文，利用量子态的不精确克隆复制M份发送给每个目的节点；目的节点接收密文逆向解密。分析了通信的吞吐量、信道的利用率、协议的安全性等问题。通过分析，证明该协议能有效防止特洛伊木马攻击，保证多播信息的安全。

英文摘要：

　　A multicast communication protocol over quantum channel against Trojan horse attacking was proposed, in the network with one source quantum node and M target quantum nodes. The source quantum node is to build 2n+δ quantum EPR state, and to send sequence tags. In the sending sequence, n are selected randomly as the test states. Channel test is carried out with the inequality of CHSH. The rest n+δ of sending sequence transform into non-orthogonal state as the key. The key is block encoded as cipher text which is to be copied into M with optimal universal quantum cloning and sent to each target quantum node. After target quantum node receiving cipher text, decoding is conducted. The communication protocols of throughput, channel utilization, security?proof were analyzed theoretically. By analyzing, the protocol can effectively counter Trojan horse attacking, guarantee the multicast communication information safely.

查看全文　查看/发表评论　下载PDF阅读器

关闭