doi:10.3969/j.issn.1000-436x.2014.07.023

抗特洛伊木马攻击的量子密钥多播通信协议

马鸿洋[1,2]，范兴奎[1]

(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)

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 $2n+\delta$ 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 $n+\delta$ 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。

关键词：量子信道；多播；特洛伊木马；量子网络

中图分类号：TN918.91 **文献标识码**：A **文章编号**：1000-436X(2014)07-0193-06

Multicast communication protocol based on quantum key distribution against trojan horse attacking

MA Hong-yang[1,2]，FAN Xing-kui[1]

(1.School of Sciences, Qingdao Technological University, Qingdao 266033, China;
2. College of Information Science and Engineering, Ocean University of China, Qingdao 266100, China)

Abstract: 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 $2n+\delta$ 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 $n+\delta$ 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.

Key words: quantum channel; multicast; Trojan horse; quantum network

1 引言

量子网络[1~4]中最简单的模型，单个源量子节点 Alice 发送信息给单个目的量子节点 Bob，其数量关系是一对一。随着量子通信需求的提高，要求单个源量子节点 Alice 发送给多个目的量子节点 Bobs，其数量关系是一对多，这是复杂量子网络多播通信。量子网络多播通信模型来自经典计算机网络通信模式。在经典计算机网络中，多播通信的研究成果较多。文献[5]提出在光通信网络中基于网络编码与多核点共享树融合的多播路由协议，以启发式矩阵的方法实现对多源节点的多播信息传输，仿真结果显示该协议能获得较好的网络负载性能。文献[6]提出在卫星通信中多播密钥通信方案，根据多

收稿日期：2014-03-31；**修回日期**：2014-04-30

基金项目：山东省高等学校科技计划基金资助项目(J11LG07);青岛市科技计划基础研究基金资助项目(12-1-4-4-(6)-JCH);国家自然科学基金资助项目(61173056，11304174)

Foundation Items: The Science and Technology Program of High Education of Shandong (J11LG07); The Qingdao Science and Technology Program-Fundamental Research (12-1-4-4-(6)-JCH); The National Natural Science Foundation of China (61173056, 11304174)

播源节点通信能力对接入用户进行相应分组，构建多播密钥管理图，合理控制多播密钥，仿真结果说明该方案有较好的安全性能。文献[7]提出水下传感器网络多播通信协议，在海洋特殊环境中传输同等数据量最大限度减少节点能量消耗，仿真表明该协议通信效率较高。文献[8]提出在无线 Mesh 网络中基于万有引力的启发式多播通信协议，根据邻居节点引力大小来选择合适节点，获得较高的安全性能，较小的通信抗干性。文献[5~8]研究光通信网络、卫星通信网络、水下传感器网络、无线 Mesh 网络的多播通信，均没有研究量子网络多播通信。

量子网络多播通信众多学者进行了深入研究。文献[9]提出量子网络的广播与多播通信，根据目的地址 3 类情况解析地址进行相应的量子信息的多播通信。文献[10]提出利用零拍测量对连续性量子密钥分配的攻击策略，插入不同的光脉冲信息，获得相应的量子密钥。该协议考虑零拍测量攻击可行性及其应对对策，文献[11]提出在量子广域网中基于多阶量子隐形传态路由通信协议，各通信节点进行量子门控制与量子测量，构建通信路由。该协议考虑了量子通信网络中如何进行量子门控制和量子测量，实际上量子信息的多播是在量子网络中不可缺少的通信模式。

本文在前人讨论的量子网络的广播与多播通信协议的基础上，针对量子信道中的特洛伊木马攻击，首次提出抵抗特洛伊木马攻击的多播通信协议，确保数据链路层量子信息传输的可靠性。

2 相关基础理论

2.1 量子网络广播模型

该量子网络中有 N+M 个通信节点，其中分为 2 类。第一类，一个源量子节点（N=1），表示为 S_1，其中，源量子节点的地址是单播地址。第二类，M 个目的量子节点，表示为 G_{1j}，其中下角标 1 表示一个组群，下角标 j 表示同一个组群内的不同量子节点（$j=1,2,\cdots,M$），其中，目的量子节点的地址是组地址，属于 D 类地址[11]。IP 地址分为 IPv4 或 IPv6，本文取 32 位的 IPv4，前 4 个比特表示地址类型，用 1110 表示；后 28 个比特表示具体的多播地址。本协议目的量子节点的组地址为永久性的。经典信息的多播通信分为距离矢量多播路由通信协议与因特网管理通信协议，在图 1 中经典信息多播通信的数据是采用单向箭头带三框图表示，三框图中内涵源量子节点的地址与目的量子节点的地址。

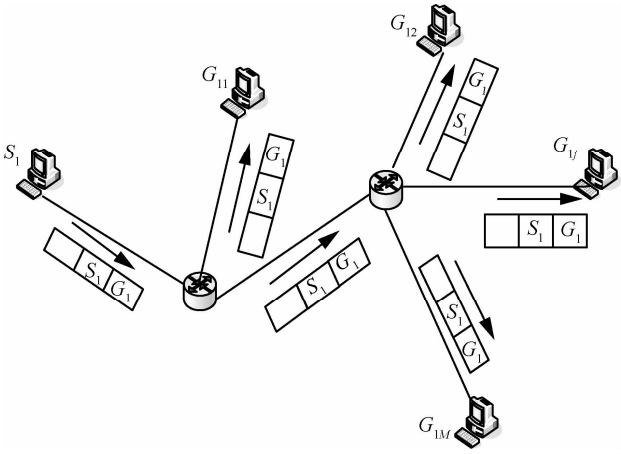

图 1 量子网络多播通信模型

2.2 量子信息群发 N 对 M 的传输模式

量子信息群发 N 对 M 的传输模式，需要对量子态进行大量复制，依据量子不可克隆定理可知量子态的精确复制是无法处理的，所以复制信息只能采用量子态的不精确克隆[12]，其复制信息的质量用量子信息保真度 ζ 来衡量。其中，$\zeta=\left[M(N+1)+N\right]/\left[M(N+2)\right]$，$N$ 为源量子节点数目，$N=1$；M 为目的量子节点数目，$N<M$。当 M 较多时，ζ 最大为 $\frac{2}{3}$，在本协议中目的量子节点数目较多，所以能保证每个目的量子节点接收到的量子信息质量均相同。

2.3 特洛伊木马攻击的基本理论

特洛伊木马攻击是窃听者将程序预先嵌入到合法的计算机系统中，利用系统的合法环境执行程序说明书中没有注明的功能，将系统内部信息隐藏传输给外部窃听者，这些病毒的后缀是 Trojan。根据区分信息能力的不同特洛伊木马分为经典特洛伊木马和量子特洛伊木马。经典特洛伊木马是通过计算机常规“0”、“1”程序指令代码，利用计算机系统漏洞非法进入体系潜伏隐藏起来，并在某个时间触发向外部窃听者泄漏本机用户的敏感信息。量子特洛伊木马[13]是在量子计算机或者量子通信设备未经许可的情况下植入小型量子系统，该小型量子系统能精确区分本征态 $|0\rangle$ 和 $|1\rangle$，对量子计算机或者量子通信设备进行非法操作，将本征态信息泄露给外部窃听者。

3　量子信道上抗特洛伊木马攻击的多播通信协议

假设目的量子节点较多，量子网络为密集拓扑结构。在该拓扑结构中，节点之间有量子信道与经典信道。其中，量子信道是操作量子态信息的传递；经典信道是操作常规“0”、“1”程序指令代码信息的传递，经典信息的广播通信采用距离矢量多播路由通信协议。

3.1　多播通信的启动阶段

根据距离矢量多播路由协议，源量子节点向目的量子节点发送多播通信启动数据帧，该数据帧中包含 S_1 的地址和 G_{1j} 的地址。

3.2　量子信息拷贝操作阶段

在数据链路层中，源量子节点将 $2n+\delta$ 个 EPR 纠缠对作为初步的多播密钥，其中每一个 EPR 纠缠对表达式为

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|00\rangle_{S_1G_1}+|11\rangle_{S_1G_1}\right) \tag{1}$$

用发送序列 $\lambda=\{\lambda_1,\lambda_2,\cdots,\lambda_{2n+\delta}\}$ 标记 $2n+\delta$ 个 EPR 纠缠对，在发送序列中随机抽取子集 $P\subset\{1,\cdots,2n+\delta\}$，其中 $|P|=n$。将子集对应的 EPR 纠缠对利用不精确克隆向每个目的量子节点发送一份拷贝信息。

3.3　利用 CHSH 不等式进行信道检测阶段

每个目的量子节点接受其拷贝的 EPR 纠缠信息，将其接受到的子集 P 对应的光子每三个为一组，进行随机测量。源量子节点与第 j 个目的量子节点选择的测量基 $a_i\,(i=1,2,3)$ 和 $b_{jk}\,(k=1,2,3)$，其偏振关联系数

$$E(a_i,b_{jk})=P_{00}(a_i,b_{jk})+P_{11}(a_i,b_{jk})-P_{01}(a_i,b_{jk})-P_{10}(a_i,b_{jk}) \tag{2}$$

其中，$P_{uv}(a_i,b_{jk})$（$u,v=0,1$）是源量子节点与第 j 个目的量子节点的测量结果为 u,v 的概率。根据局域隐变量的相关理论与 CHSH 不等式，定义其关联函数

$$S=\left|E(a_1,b_{j1})-E(a_1,b_{j3})\right|+\left|E(a_3,b_{j1})+E(a_3,b_{j3})\right| \tag{3}$$

在定域实在理论中计算关联函数 S 不会大于 2，但是在本文设定的情况下，初始态是纯纠缠态没有窃听者干扰的条件下 $S=2\sqrt{2}$。将子集 P 对应的光子测量 $L=[n/3]$ 次，如果均满足上式，则向 S_1 发送确认帧，否则停止。

3.4　纠缠对变形共享密钥阶段

CHSH 不等式满足 $S=2\sqrt{2}$，将发送序列中剩余的数记为集合 B，其中 $|B|=n+\delta$，将其对应的 EPR 纠缠对变形为

$$\left|\Phi^+\right\rangle=\frac{1}{\sqrt{2}}\left(|++\rangle_{S_1G_1}+|--\rangle_{S_1G_1}\right) \tag{4}$$

其中，$|\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle\pm|1\rangle)$。第 j 个目的量子节点构建变形算子序列 $\rho_j=\{\rho_{j1},\rho_{j2},\cdots,\rho_{j(n+\delta)}\}$，其中 $j\in B$。其中，取 0 时使用变形算子 $\boldsymbol{I}=\begin{bmatrix}1&0\\0&1\end{bmatrix}$，反之使用变形算子 $\boldsymbol{H}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$。

利用不同的变形算子，将式（4）进一步变形为：$|\varphi_1\rangle=I\left|\Phi^+\right\rangle=\left|\Phi^+\right\rangle$，$|\varphi_2\rangle=H\left|\Phi^+\right\rangle$。其中，$|\varphi_2\rangle=\frac{1}{\sqrt{2}}\left(|1+\rangle_{S_1G_1}+|0-\rangle_{S_1G_1}\right)=\frac{1}{\sqrt{2}}\left(|+1\rangle_{S_1G_1}+|-0\rangle_{S_1G_1}\right)$。这样，$|\varphi_1\rangle$ 与 $|\varphi_2\rangle$ 合计数目是 $n+\delta$ 个，这 $n+\delta$ 个作为最后的广播密钥。因为 $\langle\varphi_1|\varphi_2\rangle\neq0$，所以能抵抗量子特洛伊木马的攻击。

3.5　明文信息的通信阶段

广播明文信息 Q，长度为 W 位，分为 r 组（每组 $n+\delta$ 位），每组均用 $n+\delta$ 位的广播密钥加密。其中每组的量子态表示为：$\otimes_{q=0}^{n+\delta-1}\left|\psi_q\right\rangle=\otimes_{q=0}^{n+\delta-1}\left(\alpha_q|0\rangle+\beta_q|1\rangle\right)_a$ 其中，$|\alpha_q|^2+|\beta_q|^2=1$，$q$ 为广播信息量子态的载体粒子。其密文为

$$\otimes_{q=0}^{n+\delta-1}\left|\Psi_q^c\right\rangle \tag{5}$$

其中，

$$\left|\Psi_q^c\right\rangle\in\left\{\left|\Psi_q^c\right\rangle_{\{|K\rangle=|\varphi_1\rangle\}},\left|\Psi_q^c\right\rangle_{\{|K\rangle=|\varphi_2\rangle\}}\right\}$$

$$\left|\Psi_q^c\right\rangle_{\{|K\rangle=|\varphi_1\rangle\}}=C_m\left|\varphi_1\right\rangle\left|\psi_q\right\rangle=\alpha|00\rangle_{S_1G1}\otimes\left|\psi_q\right\rangle+\beta|+1\rangle_{S_1G_1}\otimes X_m\left|\psi_q\right\rangle$$

$$\left|\Psi_q^c\right\rangle_{\{|K\rangle=|\varphi_2\rangle\}}=D_m\left|\varphi_2\right\rangle\left|\psi_q\right\rangle=\beta|-0\rangle_{S_1G_1}\otimes\left|\psi_q\right\rangle+\alpha|11\rangle_{S_1G_1}\otimes X_m\left|\psi_q\right\rangle$$

这里，C_m、D_m 表示为作用在粒子 m 和源量子节点

S_1 的粒子上的量子受控非门，X_m 表示作用在粒子 m 上的量子 X 门，$C_m=\begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix}$，$D_m=\begin{pmatrix} \sigma_x & 0 \\ 0 & I \end{pmatrix}$，$\sigma_x=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$，$\boldsymbol{I}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$。将式（5）利用不精确克隆拷贝 M 份，分别发送给每个目的量子节点；每个目的量子节点接到后再利用量子受控非门逆操作，依次解密 r 组数据分组，最终获得广播明文信息 W。

4 吞吐量、信道利用率与安全性分析

4.1 吞吐量分析

在本多播通信协议中，假设待传送的初步多播密钥串包含 $Q=2n+\delta$ 个，在信息拷贝操作阶段，假设每个发送时延为 t_a，从 S_1 到 $G_{1j}(j=1,2,\cdots,M)$的传播时延为 t_{p1}，G_{1j} 接收数据帧所需的处理时间为 $t_{prj}(j=1,2,\cdots,M)$，考虑各个目的节点 G_{1j} 对信息处理能力的不同，该部分的处理时间取 $t_{pr1}=\max\{t_{prj}\}, j=1,2,\cdots,M$。该阶段的通信时间为 $t_{f1}=t_a+t_{p1}+t_{pr1}$。针对本通信协议采用 EPR 纠缠，因其通信的瞬时特性 t_{p1}=0，所以 $t_{f1}=t_a+t_{pr1}$。为了讨论方便在每个传输过程中出错及丢失的概率均为 p=0，故该部分的通信时间 $T_1=nt_{f1}$。

在信道检测阶段，G_{1j} 对子集 P 对应的光子进行测量，处理时间 $t_{pcj}(j=1,2,\cdots,M)$，因 G_{1j} 信息处理能力的不同，取 $t_{pc1}=\max\{t_{pcj}\}, j=1,2,\cdots,M$。再考虑 G_{1j} 回复 ACK 的发送与传播时延为 t_b，S_1 处理确认帧的时间取 t_c，则该部分的通信时间 $T_2=t_{pc1}+t_c$。

在共享密钥阶段，$n+\delta$ 个密钥变形处理时间为 $T_3=t_d$。而在信息拷贝操作阶段、信道检测阶段，可同时处理好密钥变形，所以在计算整个通信时间 T_3=0。

在明文信息的通信阶段，r 组量子比特依次发送。每个发送时延为 t_a，其中包括不同量子门的作用时间。从 S_1 到 $G_{1j}(j=1,2,\cdots,M)$的传播时延为 t_{p2}，G_{1j} 接收数据帧所需的处理时间为 t_{prj} $(j=1,2,\cdots,M)$，考虑各个目的节点 G_{1j} 对信息处理能力的不同，该部分的处理时间取 $t_{pr2}=\max\{t_{prj}\}, j=1,2,\cdots,M$，其中也是包括不同量子门逆操作时间。该阶段的通信时间为 $t_{f2}=t_a+t_{p2}+t_{pr2}$。在该部分通信时间中 $t_{p2}\neq 0$，设每个信息在传输过程中出错及丢失的概率均为 $p=0$，故该部分的通信时间 $T_4=r(n+\delta)\ t_{f2}$。

整体考虑，成功加密发送 W 位的 r 组数据帧所需的时间 T 为

$$T=T_1+T_2+T_3+T_4=(n+nr+n\delta)\ t_a+n\ t_{pr1}+t_{pc1}+t_b+t_c+(rn+r\delta)\ t_{p2}+(rn+r\delta)\ t_{pr2} \tag{6}$$

考虑 δ 很小，可将式(6)化简为

$$T=(n+nr)\ t_a+n\ t_{pr1}+t_{pc1}+t_b+t_c+rn\ t_{p2}+rn\ t_{pr2} \tag{7}$$

在本协议设定的情况下正确传送一组数据帧所需的平均时间为

$$t_{av}=\frac{T}{r}=\frac{(n+nr)t_a+nt_{pr1}+t_{pc1}+t_b+t_c+rn(t_{p2}+t_{pr2})}{r} \tag{8}$$

在 S_1 处于饱和状态下，最大吞吐量为

$$\lambda_{\max}=\frac{r}{(n+nr)t_a+nt_{pr1}+t_{pc1}+t_b+t_c+rn(t_{p2}+t_{pr2})} \tag{9}$$

4.2 信道利用率分析

r 组数据帧，数据长度为 $l_d=n+\delta$，控制信息长度为 l_h，T 时间内发送 r 组数据帧，其中有效数据率 $D=\lambda_{\max}l_d$，链路带宽为 $C=rl_f/T=r(l_d+l_h)/T$，在本协议设定的情况下信道利用率 U_0

$$U_0=\frac{D}{C}=\frac{rl_d}{rl_d+rl_h} \tag{10}$$

考虑 δ 很小，

$$U_0=\frac{rn}{rn+rl_h} \tag{11}$$

从式(11)可知，提高信道利用率需要减少控制信息长度。

4.3 安全性分析

该广播协议的安全性取决于源量子节点和目的量子节点通信的每个过程。本协议分为多播通信的启动阶段、量子信息拷贝操作阶段、利用 CHSH 不等式进行信道检测阶段、纠缠对变形共享密钥阶段、明文信息的通信阶段等 5 部分。其中，经典信息处理阶段是常规的数据通信，明文信息是通过量子信道传输的，所以在这一段没有涉密信息。量子信息拷贝处理阶段的安全性是通过量子态的不精确克隆处理完成，其安全证明见文献[14]。下面着

重分析抵御高低不同水平窃听者的情况以及量子特洛伊木马的情况。

1) 高水平窃听者 Eve 构建三粒子纠缠态的攻击分析

在利用 CHSH 不等式进行信道检测阶段，存在高水平窃听者 Eve。为了获得密钥已经探听到源量子节点与第 j 个目的量子节点选择的测量基，她将 EPR 对截获并重新制备想控制源量子节点与第 j 个目的量子节点的三粒子纠缠态——GHZ 态，其中 Eve、源量子节点与第 j 个目的量子节点三者手中的粒子分别为 E 、 A 、 B ，其表达式

$$|\psi\rangle=\frac{1}{\sqrt{2}}\left(|000\rangle+|111\rangle\right)_{ABE} \tag{12}$$

可将式（12）变化为

$$\begin{aligned}|\psi\rangle=&\frac{1}{\sqrt{2}}\Big[\left(|+x\rangle_A|+x\rangle_B+|-x\rangle_A|-x\rangle_B\right)\left(|0\rangle_E+|1\rangle_E\right)+\\&\left(|+x\rangle_A|-x\rangle_B+|-x\rangle_A|+x\rangle_B\right)\left(|0\rangle_E-|1\rangle_E\right)\Big]\\=&\frac{1}{\sqrt{2}}\Big[\left(|+y\rangle_A|+x\rangle_B+|-y\rangle_A|-x\rangle_B\right)\left(|0\rangle_E-i|1\rangle_E\right)+\\&\left(|+y\rangle_A|-x\rangle_B+|-y\rangle_A|+x\rangle_B\right)\left(|0\rangle_E+i|1\rangle_E\right)\Big]\\=&\frac{1}{\sqrt{2}}\Big[\left(|+x\rangle_A|+y\rangle_B+|-x\rangle_A|-y\rangle_B\right)\left(|0\rangle_E-i|1\rangle_E\right)+\\&\left(|+x\rangle_A|-y\rangle_B+|-x\rangle_A|+y\rangle_B\right)\left(|0\rangle_E+|1\rangle_E\right)\Big]\\=&\frac{1}{\sqrt{2}}\Big[\left(|+y\rangle_A|+y\rangle_B+|-y\rangle_A|-y\rangle_B\right)\left(|0\rangle_E-|1\rangle_E\right)+\\&\left(|+y\rangle_A|-y\rangle_B+|-y\rangle_A|+y\rangle_B\right)\left(|0\rangle_E+|1\rangle_E\right)\Big]\end{aligned} \tag{13}$$

其中， $|\pm x\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle\pm|1\rangle\right)$ ， $|\pm y\rangle=\frac{1}{\sqrt{2}}\left(|0\rangle\pm i|1\rangle\right)$ ，$|0\rangle=\frac{1}{\sqrt{2}}\left(|+x\rangle+|-x\rangle\right)$ ， $|1\rangle=\frac{1}{\sqrt{2}}\left(|+x\rangle-|-x\rangle\right)$ 。

从式（13）可得，在 $+x$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$ ；在 $+x$ 与 $-x$ 方向测量 A 、 B ， E 量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$ ；在 $+y$ 与 $+x$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle-i|1\rangle\right)$ ；在 $+y$ 与 $-x$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle+i|1\rangle\right)$ ；在 $+x$ 与 $+y$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle-i|1\rangle\right)$ ；在 $+x$ 与 $-y$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle+i|1\rangle\right)$ ；在 $+y$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$ ；在 $+y$ 与 $-y$ 方向测量 A 、 B ， E 的量子态是 $\frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$ 。 分析得知 Eve 要得到正确的测量结果，必须在源量子节点与第 j 个目的量子节点的帮助下才完成，但是在实际情况中，让在源量子节点与第 j 个目的量子节点为一个不知名的节点提供核心信息的帮助，是不可能的。

2) 低水平窃听者 Eve 截获伪造信息的攻击分析

在利用 CHSH 不等式进行信道检测阶段，存在低水平窃听者 Eve，没有能力制备 GHZ 态，仅是在检测器 a_i （ $i=1,2,3$ ）与 b_{jk} （ $k=1,2,3$ ）方向上截获光子，并在检测到粒子自旋方向上再次发送伪造的 2 个粒子，但是式 (3)的关联系数将变化为 $-\sqrt{2}\leqslant S'\leqslant\sqrt{2}$ ，其安全性详细证明见文献[14,15]。这样不满足没有窃听者干扰的条件下 $S=2\sqrt{2}$ ，所以该窃听者必定被检测出。

3) 窃听者 Eve 抵抗量子特洛伊木马攻击的分析

窃听者 Eve 预先将量子特洛伊木马 γ_i （ $i=1,2,\cdots,n+\delta$ ）植入量子网络中，其中 γ_i 是作用在第 i 个广播的共享密钥上。因为量子特洛伊木马能精确地识别 EPR 纠缠对中本征态 $|0\rangle$ 和 $|1\rangle$ ，对于原先式 (1)中纠缠态复制传输给目的节点后能识别 $|0\rangle$ 和 $|1\rangle$ ，继续用式(1)中纠缠态做密钥是不安全的，所以在利用 CHSH 不等式进行信道检测阶段之后就利用变形算子序列，将其变形为 $n+\delta$ 个 $|\varphi_1\rangle$ 与 $|\varphi_2\rangle$ ，作为密钥。如果受到特洛伊木马攻击，其密文 $\otimes_{q=0}^{N-1}\left|\Psi_q^c\right\rangle$ 变化为

$$\left|\Psi_q^c\right\rangle\in\left\{\left|\Psi_q^c\right\rangle(\gamma_i)_{\{|K\rangle=|\varphi_1\rangle\}},\ \left|\Psi_q^c\right\rangle(\gamma_i)_{\{|K\rangle=|\varphi_2\rangle\}}\right\}$$

$$\begin{aligned}&\left|\Psi_q^c\right\rangle(\gamma_i)_{\{|K\rangle=|\varphi_1\rangle\}}\\=&\alpha\left|00(h_{//})\right\rangle_{S_1G_1}\otimes\left|\psi_q\right\rangle+\beta\left|+1(h_?')\right\rangle_{S_1G_1}\otimes X_m\left|\psi_q\right\rangle\\&\left|\Psi_q^c\right\rangle(\gamma_i)_{\{|K\rangle=|\varphi_2\rangle\}}\\=&\beta\left|-0(h_?)\right\rangle_{S_1G_1}\otimes\left|\psi_q\right\rangle+\alpha\left|11(h_\perp)\right\rangle_{S_1G_1}\otimes X_m\left|\psi_q\right\rangle\end{aligned}$$

其中， $h_?$ 和 $h_?'$ 表示非确定性反馈信息。

这种密钥变形的核心是由 2 组非共轭的本征态 $\{|0\rangle,|1\rangle\}$ 和 $\{|+\rangle,|-\rangle\}$ 构建，所以量子特洛伊木马是无法精确识别的，也就是无法破译的，从而保证了密钥的安全性。

5 结束语

本文提出一个源量子节点与 M 个目的量子节点组成的网络中多播通信协议，源量子节点构建 $2n+\delta$ 个 EPR 纠缠对，从中随机选取 n 个作为检测光子，利用量子态的不精确克隆理论向 M 个目的节点发送，使用 CHSH 不等式进行信道检测，判断有没有窃听者的存在，进一步为了防止特洛伊木马的攻击，将 $n+\delta$ 个 EPR 纠缠对编码为非正交的信息，并对其信息进行接收，从而实现网络中一对多的通信加密。在本通信协议中，目的量子节点是无法增减的，如何动态地处理还需要进一步深入研究。

参考文献：

[1] ZHOU N R, CHENG H L, *et al*. Three-party quantum network communication protocols based on quantum teleportation[J]. International Journal of Theoretical Physics, 2014, 53(4):1387-1403.

[2] 曾贵华. 特洛依木马攻击下的量子密码安全性(英文)[J]. 软件学报, 2004, 19(8):1259-1264.
ZENG G H. Security of quantum cryptography against Trojan horse attacking[J]. Journal of Software, 2004, 19(8):1259-1264.

[3] GONG L H, LIU Y, ZHOU N R. Novel quantum virtual private network scheme for PON via quantum secure direct communication[J]. International Journal of Theoretical Physics, 2013, 52(9): 3260-3268.

[4] MA H Y, CHEN B Q, *et al*. Development of quantum network based on multiparty quantum secret sharing[J]. Canadian Journal of Physics, 2008, 86(9):1097-1101.

[5] 刘焕淋, 岁蒙, 邓朗. 基于多核点共享树的多源光多播路由方法[J]. 光子学报, 2014, 43(2):0127001.
LIU H L, SUI M, DENG L. A method of multi-source optical multicast routing based on multi-core node shared trees [J]. Acta Photonica Sinica. 2014, 43(2):0127001.

[6] 孙雁鸣, 马恒太, 郑刚等.卫星多播多组共享密钥管理方案[J]. 宇航学报, 2013, 34(6):824-832.
SUN Y M, MA H T, ZHENG G, *et al*. Multiple group shared key management for satellite multicast[J]. Journal of Astronautics, 2013, 34(6):824-832.

[7] CHEN Y S, LIN Y W. Mobicast routing protocol for underwater sensor networks[J]. IEEE Sensors Journal, 2013, 13(2):737-1403.

[8] 肖春静, 刘明, 龚海刚等. 无线 Mesh 网络低干扰多播[J]. 软件学报, 2013, 24(6):1295-1309.
XIAO C J, LIU M, GONG H G , *et al*. Low-interference multicast in wireless mesh networks [J]. Journal of Software,2013, 24(6): 1295-1309.

[9] 周小清, 邬云文, 赵晗. 量子隐形传态网络的广播与多播[J].物理学报, 2012, 61(17):22-27.
ZHOU X Q, WU Y W, ZHAO H. Broadcast and multicast in quantum teleportation internet [J]. Acta Physica Sinica,2012, 61(17):22-27.

[10] JONATHAN D, PLENIO M B, VEDRAL V, *et al*. Quantum hacking on quantum key distribution using homodyne detection[J]. Physical Review A, 2014, 89(3):032304.

[11] 刘晓慧, 聂敏, 裴昌幸. 量子无线广域网构建与路由策略[J]. 物理学报, 2013, 62(20):200304.
LIU X H, NIE M, PEI C X. Quantum wireless wide-area networks and routing strategy [J]. Acta Physica Sinica, 2013, 62(20):200304.

[12] GHIU I. Asymmetric quantum telecloning of d-level systems and broadcasting of entanglement to different locations using the “many-to-many” communication protocol[J]. Physical Review A, 2003, 67(1):012323.

[13] 李超, 聂敏. 基于特洛伊木马攻击的多用户树型量子信令损伤模型及修复策略[J]. 光子学报, 2012, 40(10):1256-1260.
LIU C, NIE M. Damage model of quantum signaling of multi-user based on malicious attack and repair strategy [J]. Acta Photonica Sinica, 2012, 40(10):1256-1260.

[14] YUAN Z S, BAO X H, LUA C Y, *et al*. Entangled photons and quantum communication[J]. Physics Reports, 2010, 497(1):1-40.

[15] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Physical Review Letters,1991, 67(6):661-663.

作者简介：

马鸿洋（1976-），男，山东青岛人，博士，青岛理工大学副教授、硕士生导师，主要研究方向为通信安全理论、量子信息的安全理论、量子通信协议等。

范兴奎（1970-），男，山东嘉祥人，博士，青岛理工大学副教授，主要研究方向为量子纠错码、代数群论、量子通信协议等。