基于量子纠错码的小型量子网络路由通信协议

马鸿洋[1,2],郭忠文[2],范兴奎[1],王淑梅[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: 在小型量子网络中采用量子隐形传态通信从物理机制上保证通信信息的绝对安全,但是由于量子信道存在噪声,干扰信息的正确性从而产生误码.为保证通信信息的可靠性,本文提出基于量子纠错码的小型量子网络路由通信协议.根据小型量子网络的路由特点构建路由表;依据路由表实现源量子节点到一跳、两跳目的量子节点的量子隐形传态;利用量子纠错码纠正因噪声产生的误码信息;对该协议的安全性进行理论证明.

关键词: 量子纠错码; 小型量子网络; 量子隐形传态; 一跳; 两跳
中图分类号: TN918.91 **文献标识码:** A **文章编号:** 0372-2112 (2015)01-0171-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2015.01.027

The Routing Communication Protocol for Small Quantum Network Based on Quantum Error Correction Code

MA Hong-yang[1,2], GUO Zhong-wen[2], FAN Xing-kui[1], WANG Shu-mei[1]
(1. *School of Sciences, Qingdao Technological University, Qingdao, Shandong* 266033, *China*;
2. *College of Information Science and Engineering, Ocean University of China, Qingdao, Shandong* 266100, *China*)

Abstract: In small quantum network, the security of communication information can be guaranteed physically by the application of quantum teleportation, the noise of quantum channel will be bound to interfere with the communication information, leading to the error of code. In order to guarantee the reliability of information communication, a routing protocol of small quantum network is proposed based on quantum error correcting code. According to the routing characteristics of small quantum network, corresponding routing tables are made. On the basis of these routing tables, quantum teleportation can be realized from source quantum node to the nodes within one-hop or two-hop. Correct the errors of code resulting from noise of quantum channel based on error correcting code theory, and handle it accordingly, to ensure the reliability of communication information at data link layer. The security of the protocol is proved in theory.

Key words: quantum error correction code; small quantum network; teleportation; one-hop; two-hop

1 引言

量子网络[1~5]是由若干随机部署量子节点组成的通信模型,通信主要方式是在经典通道配合下的量子信道隐形传态.国内外相关研究成果较多.2012 年,余旭涛等提出融合量子隐形传态的无线自组织量子网络路由协议[6],依照路由度量选择传输路径,用量子隐形传态实现无线自组织量子通信网络的数据通信;2012 年,杨小琳等提出利用量子隐形传态的方法进行数据链路层的选择重传通信协议[7],发送方把量子比特分为若干数据帧,接收方利用经典信息判断是否收到正确的数据帧.文献[6,7]考虑了量子网络中如何进行量子隐形传态通信,然而实际通信系统中信道噪声是不可避免的,对噪声误码纠正好坏直接关系到通信质量的优劣.

本文在前人讨论的基于量子隐形传态的量子网络路由通信协议的基础上,首次提出基于量子纠错码的小型量子网络路由通信协议,依据路由表实现源量子节点到一跳、两跳目的量子节点的量子隐形传态,采用量子纠错码理论来实现对误码的纠正,确保数据链路层量子信息传输的可靠性.

2 小型量子网络通信模型

网络中 N 个量子节点,分为源量子节点 S_0 与目的量子节点 $S_j(j=1,2,\cdots,N-1)$.源量子节点 S_0 到目的

收稿日期:2013-09-06;修回日期:2014-01-02;责任编辑:李勇锋
基金项目:国家自然科学基金(No.61173056,No.11304174);山东省高等学校科技计划(No.J11LG07);青岛市科技计划基础研究(No.12-1-4-4-(6)-JCH)

量子节点 S_j 经典信道数据流按路由表的指定方向传输,在路由表中从源量子节点 S_0 到目的量子节点 S_j 的中转节点最多不超过一个.

S_j 分两类:第一类与 S_0 直接相连,定义为一跳目的量子节点,记为 S_j^1;第二类与 S_0 通过中转节点相连,定义为两跳目的量子节点,记为 S_j^2;其中上角标 1,2 表示为一跳、两跳,下角标 j 表示为第 j 个目的量子节点.在图 1 中一跳目的量子节点 S_1、S_2、S_3、S_4,两跳目的量子节点 S_5,从 S_0 到 S_5 的中转节点为 S_2、S_3.节点间通信信道有量子信道与经典信道.量子信道利用纠缠态传输量子信息,用虚线表示;经典信道利用 "0"、"1"码来传递通信信息,用实线表示.

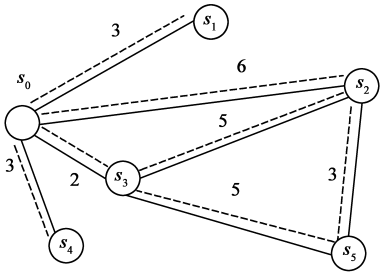

图1 小型量子网络通信模型

3 协议

本通信协议由单跳、两跳的量子隐形传态构成,其中量子通信需要经典信道配合,而经典信息的通信必须依靠传统的路由协议,即距离向量选择的路由信息协议.

3.1 小型量子网络构建路由表过程

3.1.1 路由初始化过程

为配合量子通信必须先构造经典信息通信路由表,路由表内容是每个量子节点的最小距离向量表.该表由三列组成,第一列去往量子节点列表;第二列代价表,包含与之直接相连节点距离,即一跳节点的距离.与之不直接相连节点距离,即两跳节点距离,用无穷大表示;第三列下一个量子节点列表,见图 2.

3.1.2 路由信息更新过程

距离向量表中有一跳节点的距离,源量子节点可以直接获取;但没有两跳节点的距离,源量子节点需要通过共享邻居量子节点的路由距离来间接获取.以图 2 为例,S_0 不知道两跳节点 S_5 的路由距离,但是 S_0 知道一跳节点 S_3 的路由距离,通过共享 S_3 的距离向量表中信息,S_0 就知道自己到 S_5 的路由距离.S_0 从 S_3 的距离向量表中抽取第二列,将该列信息与 S_0 到 S_3 的代价值相加,构建成新的第二列;再将新的第二列与其旧的第二列比较,保留最小值.完成共享路由信息,形成 S_0 的新表.按照共享路由信息步骤,其它量子节点依次更新距离向量表,如图 3.

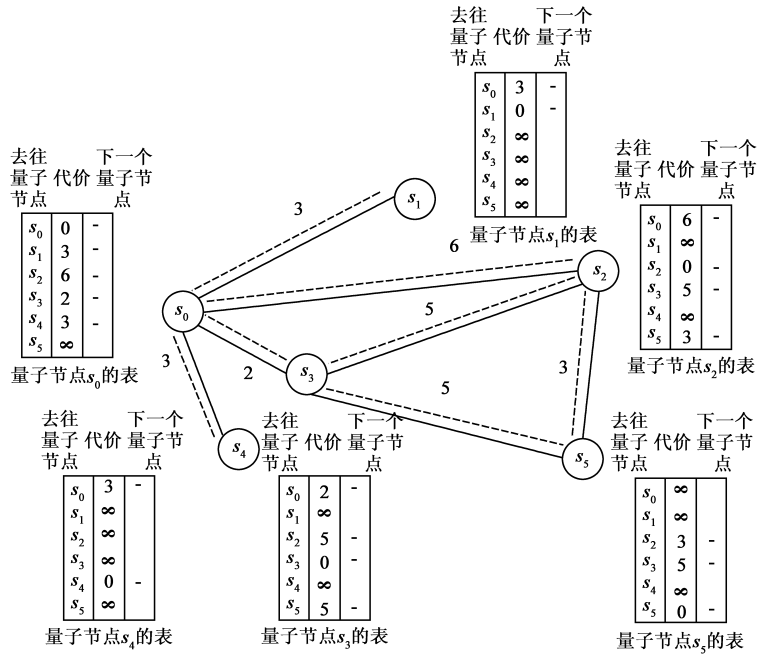

图2 小型量子网络初始化路由选择表

3.2 依照路由表构建节点之间的通信

依照路由表进行一跳节点、两跳节点的量子通信.

3.2.1 通信的初始化阶段

①源量子节点 S_0 发送 $2n$ 个量子比特流,并标记其发送序列,其中第 i 个量子比特表达式为 $|\Psi\rangle_i = \alpha_i|0\rangle_a^i + \beta_i|1\rangle_a^i$, $|\alpha_i|^2 + |\beta_i|^2 = 1$, $i = 1,\cdots,2n$,发送序列记表达式为 $\lambda = \{\lambda_1,\lambda_2,\cdots,\lambda_{2n}\}$.

②S_0 从发送序列中随机选取长度为 n 子集,记为 P,其中 $P \subset \lambda$, $|P| = n$,作为校验量子比特,用于检测信道噪声.

3.2.2 一跳与两跳的节点间通信阶段

③目的量子节点分为一跳目的量子节点 S_j^1 和两跳目的量子节点 S_j^2,与之对应的通信分为一跳目的量子节点通信和两跳目的量子节点通信两部分.

若与一跳目的量子节点通信,以图 1 为例,在 4 个一跳节点 S_1、S_2、S_3、S_4 中任选一个作为通信目的量子节点,假设为 S_1. S_0 与 S_1 构建 $2n$ 个 EPR 纠缠对作为量子信道,其表达式为 $K = \{|k_1\rangle, |k_2\rangle, \cdots, |k_{2n}\rangle\}$,其中 $|k_i\rangle = \frac{1}{\sqrt{2}}(|0\rangle_b^i|1\rangle_c^i - |1\rangle_b^i|1\rangle_c^i)$. S_0 手中的两个量子比特,S_1 手中的一个量子比特,所构建的三个量子比特系统,表达式:

$$|\Omega_i\rangle_{abc} = (\alpha_i|0\rangle_a^i + \beta_i|1\rangle_a^i) \otimes \frac{1}{\sqrt{2}}(|0\rangle_b^i|1\rangle_c^i - |1\rangle_b^i|0\rangle_c^i) \quad (1)$$

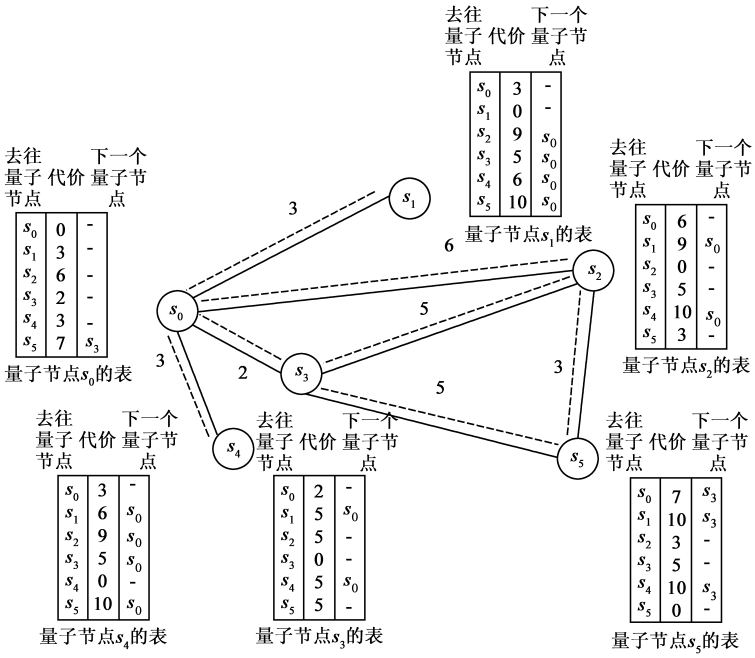

图3　小型量子网络通信距离向量路由选择表

式(1)中下角标 a、b 表示 S_0 手中的第一个、第二个量子比特，c 表示 S_1 手中的量子比特.将式(1)变形为

$$|\Omega_i\rangle_{abc}=\frac{1}{2}[|\Psi^-\rangle_{ab}^i(-\alpha_i|0\rangle_c^i-\beta_i|1\rangle_c^i)+|\Psi^+\rangle_{ab}^i(-\alpha_i|0\rangle_c^i+\beta_i|1\rangle_c^i)]$$
$$+\frac{1}{2}[|\Phi^-\rangle_{ab}^i(\beta_i|0\rangle_c^i+\alpha_i|1\rangle_c^i)+|\Phi^+\rangle_{ab}^i(-\beta_i|0\rangle_c^i+\alpha_i|1\rangle_c^i)] \tag{2}$$

其中,4 个 Bell 基表达式:

$$|\Phi^\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle^i|0\rangle^i\pm|1\rangle^i|1\rangle^i),$$
$$|\Psi^\pm\rangle=\frac{1}{\sqrt{2}}(|0\rangle^i|1\rangle^i\pm|1\rangle^i|0\rangle^i).$$

S_0 对粒子 a、b 做 Bell 测量,若测量结果为 $|\Psi^-\rangle_{ab}^i$ 时,一跳目的量子节点 S_1 对粒子 c 施以幺正变换 $-I$,得到 $(\alpha_i|0\rangle_c^i+\beta_i|1\rangle_c^i)$;同理,为 $|\Psi^+\rangle_{ab}^i$ 时,施以幺正变换 $-Z$,得到 $(\alpha_i|0\rangle_c^i+\beta_i|1\rangle_c^i)$;为 $|\Phi^-\rangle_{ab}^i$ 时,施以幺正变换 X,得到 $(\alpha_i|0\rangle_c^i+\beta_i|1\rangle_c^i)$;为 $|\Phi^+\rangle_{ab}^i$ 时,施以幺正变换 $-iY$,得到 $(\alpha_i|0\rangle_c^i+\beta_i|1\rangle_c^i)$.

若与两跳目的量子节点通信,以图 1 为例,只有一个两跳的节点为 S_5,中转节点为 S_3.S_0 与 S_3 构建 $2n$ 个 EPR 纠缠对作为量子信道,表达式 $K'=\{|k_1'\rangle,|k_2'\rangle,\cdots,|k_{2n}'\rangle\}$,其中 $|k_i'\rangle=\frac{1}{\sqrt{2}}(|0\rangle_b^i|1\rangle_c^i-|1\rangle_b^i|0\rangle_c^i)$;$S_3$ 与 S_5 构建 $2n$ 个 EPR 纠缠对作为量子信道,表达式 $K''=\{|k_1''\rangle,|k_2''\rangle,\cdots,|k_{2n}''\rangle\}$,其中 $|k_i''\rangle=\frac{1}{\sqrt{2}}(|0\rangle_d^i|1\rangle_e^i-|1\rangle_d^i|0\rangle_e^i)$.$S_0$ 手中两个量子比特,S_3 手中两个量子比特,S_5 手中的一个量子比特,所构建的五个量子比特系统,其表达式:

$$\begin{aligned}|\Omega_i\rangle_{abcde}&=(\alpha_i|0\rangle_a^i+\beta_i|1\rangle_a^i)\\&\otimes\frac{1}{\sqrt{2}}(|0\rangle_b^i|1\rangle_c^i-|1\rangle_b^i|0\rangle_c^i)\\&\otimes\frac{1}{\sqrt{2}}(|0\rangle_d^i|1\rangle_e^i-|1\rangle_d^i|0\rangle_e^i)\\&=\frac{1}{2}(\alpha_i|0\rangle_a^i+\beta_i|1\rangle_a^i)\\&\otimes(|0\rangle_b^i|1\rangle_c^i|0\rangle_d^i|1\rangle_e^i-|0\rangle_b^i|1\rangle_c^i|1\rangle_d^i|0\rangle_e^i\\&-|1\rangle_b^i|0\rangle_c^i|0\rangle_d^i|1\rangle_e^i+|1\rangle_b^i|0\rangle_c^i|1\rangle_d^i|0\rangle_e^i)\end{aligned} \tag{3}$$

式(3)中下角标 a、b 表示 S_0 手中第一、第二个量子比特，c、d 表示 S_3 手中第一、第二个量子比特，e 表示 S_5 手中量子比特.

S_0 和 S_3 分别对手中的第一个量子比特应用 *CONT* 门与 H 门,则式(3)可变化为:

$$\begin{aligned}|\Omega_i'''\rangle=\frac{1}{2\sqrt{2}}[&-|0\rangle_a^i|0\rangle_c^i|\Phi^-\rangle_{bd}^i(\alpha|0\rangle_e^i+\beta|1\rangle_e^i)+|1\rangle_a^i|1\rangle_c^i|\Phi^+\rangle_{bd}^i(\alpha|0\rangle_e^i+\beta|1\rangle_e^i)\\&+|0\rangle_a^i|0\rangle_c^i|\Psi^-\rangle_{bd}^i(\alpha|1\rangle_e^i+\beta|0\rangle_e^i)-|1\rangle_a^i|1\rangle_c^i|\Psi^+\rangle_{bd}^i(\alpha|1\rangle_e^i+\beta|0\rangle_e^i)\\&+|0\rangle_a^i|1\rangle_c^i|\Phi^+\rangle_{bd}^i(\alpha|0\rangle_e^i-\beta|1\rangle_e^i)-|1\rangle_a^i|0\rangle_c^i|\Phi^-\rangle_{bd}^i(\alpha|0\rangle_e^i-\beta|1\rangle_e^i)\\&-|0\rangle_a^i|1\rangle_c^i|\Psi^+\rangle_{bd}^i(\alpha|1\rangle_e^i-\beta|0\rangle_e^i)+|1\rangle_a^i|0\rangle_c^i|\Psi^-\rangle_{bd}^i(\alpha|1\rangle_e^i-\beta|0\rangle_e^i)]\end{aligned} \tag{4}$$

从式(4)可知,S_0、S_3 的量子比特是 $|0\rangle_a|0\rangle_c$,$|\Phi^-\rangle_{bd}^i$,S_5 对粒子 e 施以幺正变换 $-I$,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|1\rangle_a|1\rangle_c$、$|\Phi^+\rangle_{bd}^i$ 时,施以幺正变换 I,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|0\rangle_a|0\rangle_c$、$|\Psi^-\rangle_{bd}^i$ 时,施以幺正变换 X,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|1\rangle_a|1\rangle_c$、$|\Psi^+\rangle_{bd}^i$ 时,施以幺正变换 $-X$,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|0\rangle_a|1\rangle_c$、$|\Phi^+\rangle_{bd}^i$ 时,施以幺正变换 Z,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|1\rangle_a|0\rangle_c$、$|\Phi^-\rangle_{bd}^i$ 时,施以幺正变换 $-Z$,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|0\rangle_a|1\rangle_c$、$|\Psi^+\rangle_{bd}^i$ 时,施以幺正变换 $-iY$,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$;同理,是 $|1\rangle_a|0\rangle_c$、$|\Psi^-\rangle_{bd}^i$ 时,施以幺正变换 iY,得到 $(\alpha_i|0\rangle_e^i+\beta_i|1\rangle_e^i)$.

依照上面方式,$2n$ 个量子密钥流依次从 S_0 利用隐形传态发送给一跳或两跳的目的量子节点.

④一跳或两跳目的量子节点 S_j 开始接收量子比

特,标记其接收序列,表达式为 $\rho_j=\{\rho_{j1},\rho_{j2},\cdots,\rho_{j(2n)}\}$,下角标 j 表示为第 j 个目的量子节点;S_j 要考虑量子比特的存储,现在量子比特存储已有较好办法[8].

3.3 节点间的经典通信阶段

⑤ S_j 依次接受完 $2n$ 个量子密钥流后,根据域内路由协议所构建的路由表,经过经典信道向源量子节点返回一个数据确认帧.其中,如果 S_j 是一跳目的量子节点 S_j^1,可直接向 S_0 返回 ACK;如果 S_j 是两跳目的量子节点 S_j^2,则经过中间节点向 S_0 返回数据确认帧.

⑥ S_0 收到 ACK 后,宣布 P,根据 P 对应的检测位,公布其对应量子比特信息.随之将 P 和对应的量子比特信息,构建成相应数据包,通过路由表发送给 S_j.

⑦ S_j 接受完数据包后,根据 P,寻找在 ρ_j 中对应的检测位,再根据对应的检测位公布其对应量子比特信息.将 S_0 与 S_j 公布的量子比特进行比对,计算其误码数:$E_j=\{m\in P\mid|\Psi\rangle_{\lambda_m}\neq|\varphi\rangle_{\rho_{jm}}\}$,其中 E_j 表示第 j 个目的量子节点公布的检测位的错误数,$|\Psi\rangle_{\lambda_m}$ 表示 S_0 发送序列中第 m 个比特,$|\Psi\rangle_{\rho_{jm}}$ 表示 S_j 接收序列中第 m 个比特.如果 $E_j>t$,根据域内路由协议构建的路由表,经过经典信道向源量子节点返回一个否定确认帧,启动量子数据流的重传操作.如果,$E_j\leqslant t$,则进行下一步.

3.4 节点误码纠错阶段

⑧ S_j 从接收的 $2n$ 个量子比特流中除去已作为检测位的 n 个量子比特,将剩余 n 个量子比特,记为 v_j,表达式为:

$$\frac{1}{2^{k_2/2}}\sum_{w\in C_2}|v_j+w\rangle \tag{5}$$

在 v_j 中有比特翻转和相位翻转,分别表示为 e_b、e_p.根据 $E_j\leqslant t$ 可知,v_j 中误码位数不超过 t,可用 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2^{\mathrm{T}}$ 纠正.步骤如下,因存在误码所以式(5)变形为:

$$\frac{1}{2^{k_2/2}}\sum_{w\in C_2}(-1)^{(v_i+w)\cdot e_p}|v_i+w+e_b\rangle \tag{6}$$

S_0 根据路由表,经过经典信道向 S_j 发送校验矩阵 $\boldsymbol{H}_1$,将 $|v_j+w+e_b\rangle$ 中 v_j+w+e_b 与 $\boldsymbol{H}_1$ 相乘,依据伴随式可算出存在比特反转错误的位置,再采用反转操作得到纠正后的比特.修正 e_b 后,式(6)变化为只有相位翻转错误 e_p 形式:

$$\frac{1}{2^{k_2/2}}\sum_{w\in C_2}(-1)^{(v_i+w)\cdot e_p}|v_j+w\rangle \tag{7}$$

对其各个比特实施 H 门操作,利用 $\boldsymbol{H}_2^{\mathrm{T}}$ 对信息进行比特检测和错误纠正处理,得到纠正后量子信息.其中 $\boldsymbol{H}_2^{\mathrm{T}}$ 的表达式为 $\boldsymbol{H}_2^{\mathrm{T}}=\left(\boldsymbol{h}_1^{\mathrm{T}},\ \cdots,\ \boldsymbol{h}_{n-\dim C_2}^{\mathrm{T}}\right)$,这是 $C_2^{\perp}$ 的奇偶校验矩阵.这样,利用路由表发送过来的 $\boldsymbol{H}_1$ 和 $\boldsymbol{H}_2^{\mathrm{T}}$,纠正了最大可能出现 t 位错误的 v_j,最终获得传输过来的正确数据.

4 安全性分析

该通信协议安全性取决于源量子节点和目的量子节点通信的安全.假设窃听者 Eve 参与并想截获相关信息,它要与源量子节点、目的量子节点组成三个粒子 *GHZ* 态,三者拥有的粒子分别表示为 E、S、A,表达式:$|\Psi\rangle=\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{SAE}$.

源量子节点向目的量子节点发送 $2n$ 个量子密钥流,窃听者 Eve 从量子密钥流中任选一个量子密钥 $(\alpha_j|0\rangle+\beta_j|1\rangle)_a$,$a$、$S$、$A$、$E$ 组成的四个量子比特系统:

$$\begin{aligned}|\Omega_{aSAE}&=(\alpha_j|0\rangle+\beta_j|1\rangle)_a\otimes\frac{1}{\sqrt{2}}(|000\rangle-|111\rangle)_{SAE}\\&=\frac{1}{2}[|\Psi^-\rangle_{aS}(-\beta_j|00\rangle_{AE}-\alpha_j|11\rangle_{AE})\\&\quad+|\Psi^+\rangle_{aS}(\beta_j|00\rangle_{AE}-\alpha_j|11\rangle_{AE})]\\&\quad+\frac{1}{2}[|\Phi^-\rangle_{aS}(\alpha_j|00\rangle_{AE}+\beta_j|11\rangle_{AE})\\&\quad+|\Phi^+\rangle_{aS}(\alpha_j|00\rangle_{AE}-\beta_j|11\rangle_{AE})]\end{aligned} \tag{8}$$

从式(8)可知,源量子节点在 Bell 基测量操作下,目的量子节点与 Eve 组成状态有四种可能:$-\beta_j|00\rangle_{AE}-\alpha_j|11\rangle_{AE}$,$\beta_j|00\rangle_{AE}-\alpha_j|11\rangle_{AE}$,$\alpha_j|00\rangle_{AE}+\beta_j|11\rangle_{AE}$,$\alpha_j|00\rangle_{AE}-\beta_j|11\rangle_{AE}$.Eve 从四种可能中获得 $(\alpha_j|0\rangle+\beta_j|1\rangle)_a$,必须在源量子节点、目的量子节点共同协助下才能获得.但是,源量子节点是不会对其提供协助的,所以,Eve 是无法得到有用信息.

文献[9]知源量子节点 S_0 发送密钥信息 v_j+w 在 $\frac{1}{2^{k_2/2}}\sum_{w\in C_2}(-1)^{z\cdot w}|x+v_j+w\rangle\in Q_{xy}$ 中,并推出其互信息为:

$$I(v_j;E\mid X=x,Z=z\mid)\leqslant 2d^{-nE+o(n)}[n((E+R)-o(n)]$$

其中,E 表示 Eve 引入的误码,$R=n^{-1}\log_d\dim Q_{xz}$.依据文献[10]所提及好码和 $n\to\infty$ 条件其互信息接近为零,可知道其 Eve 获得的有用信息极少,从而表明对窃听必能进行有效的抵御.

5 结束语

本文提出基于量子纠错码的小型量子网络路由通信协议,根据小型量子网络的路由特点构建相应路由表,依据路由表实现源量子节点到一跳、两跳之内目的量子节点的量子隐形传态.本文解决了利用隐形传态传输信息的网络中误码纠错的问题,但是能纠错的网络模型较为简单,只限定在一跳和两跳的目的量子节点,对于更加复杂的网络即多跳网络的纠错仍需要进

一步研究.

参考文献

[1] Koashi M. Simple security proof of quantum key distribution via uncertainty principle[J]. New Journal of Physics, 2009, 11: 045018.

[2] 周小清,邬云文.量子隐形传态网络的广播与组播[J].物理学报,2012,61(17):170303.
Zhou Xiao-qing, Wu Yun-wen. Broadc ast and multicast in quantum teleportat ion internet[J]. Acta Physica Sinica, 2012, 61(17): 170303. (in Chinese)

[3] Ma Hong-yang, Chen Bing-quan, Guo Zhong-wen, et al. Development of quantum network based on multiparty quantum secret sharing[J]. Canadian Journal of Physics, 2008, 86(9): 1097 – 1101.

[4] 温晓军,田原,牛夏牧.一种基于秘密共享的量子强盲签名协议[J].电子学报,2010,38(3):720 – 724.
Wen Xiao-jun, Tian Yuan, Niu Xia-mu. A strong blind quantum signature protocol based on secret sharing[J]. Acta Electronica Sinica, 2010, 38(3): 720 – 724. (in Chinese)

[5] Nielsen M A, Chuang I L. Quantum Computation and Quantum Information [M]. Cambridge: Cambridge University Press, 2000. 596 – 603.

[6] 余旭涛,徐进,张在琛.基于量子远程传态的无线自组织量子通信网络路由协议[J].物理学报,2012,61(22):220303.
Yu Xu-tao, Xu Jin, Zhang Zai-chen. The routing protocol for wireless and hoc quantum communication network based on quantum teleportation[J]. Acta Physica Sinica, 2012, 61(22): 220303. (in Chinese)

[7] 杨小琳,周小清,赵晗,等.基于量子隐形传态的数据链路层选择重传协议[J].物理学报,2012,61(2):020303.
Yang Xiao-lin, Zhou Xiao-qing, Zhao Han, et al. Data link layer of selective repeat protocol based on quantum teleportation [J]. Acta Physica Sinica, 2012, 61(2): 020303. (in Chinese)

[8] Bao X H, Andreas R, Dietrich P, et al. Efficient and long-lived quantum memory with cold atoms inside a ring cavity[J]. Nature Physics, 2012, 8(7): 517.

[9] Hamada M. J. Reliability of Calderbank-Shor-Steane codes and security of quantum key distribution[J]. Journal of Physics A: Mathematical and General, 2004, 37(34): 8303 – 8328.

[10] Calderbank A R, Shor P W. Good quan-tum error-correcting codes exist[J]. Physical Review A, 1996, 54(2): 1098 – 1105.

作者简介

马鸿洋　男,1976 年 9 月出生,山东青岛人.1998 年于曲阜师范大学获理学学士,2006 年和 2011 年在中国海洋大学获工学硕士与工学博士学位.现为青岛理工大学副教授、硕士生导师,主要从事通信安全理论、量子信息与量子通信等方面的研究工作.
E-mail: hongyang_ ma@aliyun.com

郭忠文　男,1965 年 7 月,黑龙江双鸭山人.教授、博士生导师.1987 年在同济大学获工学学士学位,1996 年和 2005 年在中国海洋大学获工学硕士与工学博士学位.现为中国海洋大学信息科学与工程学院副院长,主要从事网络通信安全理论、海洋信息分布式处理技术等方面的研究工作.
E-mail: guozhw@ouc.edu.cn