基于单控制方的可控量子网络编码方案

尚 涛,赵晓杰,王 朝,刘建伟
(北京航空航天大学电子信息工程学院,北京 100191)

摘 要: 本文提出了基于单控制方的可控量子网络编码方案,实现对传统量子网络编码方案中接收方的解码控制.该方案以经典 XQQ(Crossing Two Qubits)协议为基础,引入可控隐形传态的控制方到网络编码模型当中,对两个接收方的解码实现控制.方案分析表明,这种新型方案实现了在没有控制方允许的情况下,即使攻击者获得了接收方全部信息也无法解码获得传输的量子信息,从而提高了量子网络中信息传输的安全性.

关键词: 可控隐形传态; 量子网络编码; XQQ 协议; 安全
中图分类号: TP393 **文献标识码:** A **文章编号:** 0372-2112 (2014)10-1913-05
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2014.10.007

Controlled Quantum Network Coding Scheme Based on Single Controller

SHANG Tao, ZHAO Xiao-jie, WANG Chao, LIU Jian-wei
(*School of Electronic and Information Engineering, Beihang University, Beijing* 100191, *China*)

Abstract: This paper proposes a controlled quantum network coding scheme based on single controller so as to control the decoding operation at the receivers for traditional quantum network coding schemes. This scheme is designed based on the paradigm XQQ(Crossing Two Qubits) protocol, and it can control the decoding process of two receivers simultaneously by means of introducing the controller in controlled teleportation. Scheme analyses show that without the permission of the controller, any attacker cannot decode and acquire the quantum information from the senders in this scheme, even if he can get all the information of the receivers. Thus our scheme can enhance the security of transferring quantum information in quantum networks.

Key words: controlled teleportation; quantum network coding; XQQ protocol; security

1 引言

近年来网络编码技术因其可以提高网络吞吐量的特性[1,2],而被逐渐引入到量子网络中.针对蝶形网络结构,量子网络编码已取得突破性进展,可分为传输经典信息和未知量子态两类方案.2006 年 Hayashi 等人[3]利用蝶形网络实现了两个任意量子态交叉概率性传输,使量子网络编码成为可能,并提出了著名的 XQQ(Crossing Two Qubits)协议.2007 年 Hayashi[4]又从新的角度将量子隐形传态(Quantum Teleportation)应用于量子网络编码中,设计了基于发送方预共享纠缠态(Prior Entanglement)的量子网络编码方案,实现了量子态的完美传输.2010 年 Ma 等人[5]在 Hayashi 研究成果基础上,提出了基于发送者共享非最大纠缠态(Non-maximally entangled state)实现 M-qudit 交叉传输的协议.2012 年,闫帅帅等人[6]利用两个发送方之间共享两对非最大化 GHZ 纠缠粒子作为传输信道,实现了传输 2-level 量子纠缠态的量子网络编码方案,提高了蝶形网络中量子信息传输的效率.2013 年 Nishimura[7]明确了基于蝶形网络的量子网络编码中可达速率的界限.

随着量子网络的迅速发展,研究人员开始关注传输信息的安全性,并致力于利用量子信道直接传输消息,即量子安全直接通信(Quantum Security Direct Communication, QSDC).研究发现,基于量子隐形传态的 QSDC 方案,发送方无需将编码后的粒子回传给接收方也可以实现信息的安全传输[8].该方案最后阶段依赖于经典信息进行解码,依然存在着安全问题.由于可控隐形传态加入了控制方,使得接收方在没有控制方允许情况下,即使获得了接收方的信息,仍无法独自解码获得接收的未知量子态,因此它可以很好地解决 QSDC 经典信息传递

收稿日期:2013-10-23;修回日期:2014-01-22;责任编辑:郭游
基金项目:国家重点基础研究发展计划(973 计划)(No.2012CB315905);国家自然科学基金(No.61272501);北京市自然科学基金(No.4132056);中央高校基本科研业务费(No.YWF14DZXY012);Research Promotion Grant-in-Aid for KUT Graduates of Special Scholarship Program.

时的安全问题,保证了信息传递的安全性.因此,本文在此思想基础上,将可控隐形传态应用于蝶形量子网络中,设计了可控量子网络编码方案,保证接收方必须在控制方参与下才能解码获得所接收的量子态,来增强蝶形网络中量子信息传输的安全性.

2 相关研究

2.1 可控隐形传态

1993 年 Bennett 等人首次提出了量子隐形传态的概念[9].在此基础上,Zhou 等人[10]首次提出了可控隐形传态的方案.与量子隐形传态相比,可控隐形传态在发送方、接收方基础上添加了一个控制方.它们三者共享三粒子的 GHZ 态,并用此纠缠态作为量子通道来传输单粒子态.如果不是三者都同意,则无法完成单粒子态的隐形传输,即若没有控制方的测量信息,接收方无法对接收的量子态进行解码.具体说明如下[11].

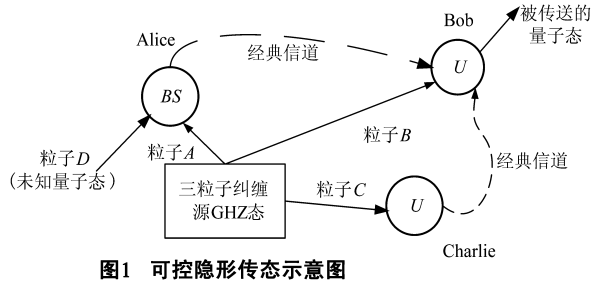


图1 可控隐形传态示意图

假设要传送的粒子 D 的未知量子态为 $|\varphi\rangle_D=\alpha|0\rangle_D+\beta|1\rangle_D$,其中 α 和 β 是未知的复系数,且满足归一化条件 $|\alpha|^2+|\beta|^2=1$. Alice, Bob, Charlie(分别拥有粒子 A、B、C)三方共享三粒子 GHZ 态作为量子信道,三粒子 GHZ 态如式(1)所示:

$$|\varphi\rangle_{ABC}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{ABC} \tag{1}$$

总的粒子体系的量子态为:

$$|\psi\rangle=|\varphi\rangle_{ABC}\otimes|\phi_D\rangle \tag{2}$$

将(2)展开为式(3):

$$\begin{aligned}|\psi\rangle=\frac{1}{2}[&|\phi^+\rangle_{AD}(\alpha|00\rangle_{BC}+\beta|11\rangle_{BC})+|\phi^-\rangle_{AD}\\&(\alpha|00\rangle_{BC}-\beta|11\rangle_{BC})+|\psi^+\rangle_{AD}(\alpha|11\rangle_{BC}\\&+\beta|00\rangle_{BC})+|\psi^-\rangle_{AD}(\alpha|11\rangle_{BC}-\beta|00\rangle_{BC})]\end{aligned} \tag{3}$$

定义下列一组算子:

$$U_0=|0\rangle\langle0|+|1\rangle\langle1|=\begin{pmatrix}1&0\\0&1\end{pmatrix}=I$$

$$U_1=|0\rangle\langle0|-|1\rangle\langle1|=\begin{pmatrix}1&0\\0&-1\end{pmatrix}=\sigma_Z$$

$$U_2=|1\rangle\langle0|+|0\rangle\langle1|=\begin{pmatrix}0&1\\1&0\end{pmatrix}=\sigma_X$$

$$U_3=|0\rangle\langle1|-|1\rangle\langle0|=\begin{pmatrix}0&1\\-1&0\end{pmatrix}=i\sigma_Y \tag{4}$$

可控隐形传态的具体步骤如下:

第一步,Alice 对粒子 A 和 D 进行 Bell 基测量,得到四个 Bell 态的其中一个,并将测量结果通过经典信道告诉 Bob,粒子 B 和 C 将会塌缩到对应的状态.以测量结果 $|\varphi^+\rangle_{AD}$ 为例,则粒子 B 和粒子 C 状态将会变成纠缠态:$|\psi\rangle_{BC}=\alpha|00\rangle_{BC}+\beta|11\rangle_{BC}$.

第二步,假设 Charlie 同意 Bob 获得信息,它可以对自己的粒子 C 实施 Hadamard 变换:

$$H|0\rangle_C=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)_C\quad H|1\rangle_C=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)_C$$

变换后粒子 B 和 C 的量子态变为:

$$|\psi'\rangle_{BC}=(\alpha|0\rangle_B+\beta|1\rangle_B)|0\rangle_C+(\alpha|0\rangle_B-\beta|1\rangle_B)|1\rangle_C$$

第三步,Charlie 此时对粒子 C 进行测量,并把测量结果告诉 Bob. Bob 根据粒子 C 的测量结果选用式(4)中一个合适的算子对粒子 B 进行 U 操作以恢复得到要传输的未知量子态.具体操作如下:

(1)当测量结果是 $|0\rangle_C$ 时,B 粒子状态为 $\alpha|0\rangle_B+\beta|1\rangle_B$,恰好为要接收的未知量子态,不必进行 U 操作变换;

(2)当测量结果为 $|1\rangle_C$ 时,B 粒子状态为 $(\alpha|0\rangle_B-\beta|1\rangle_B)$,对其进行适当的 $U(\sigma_z)$ 变换,即可得到未知量子态.

这样就实现了在第三方的控制下接收未知量子态.

2.2 基于蝶形网络的 XQQ 协议

鉴于量子信息不同于经典信息的性质,量子网络编码设计存在着两个难题:量子态编码困难和量子态不可复制.由 Hayashi 等人提出的 XQQ 协议[3]很好地解决了相关问题.XQQ 协议主要通过引入 Tetra 测量将量子态离散化,完成对中间节点处量子态的编码,并且利用 UC 克隆完成对量子态的复制.在图 2 所示的蝶形网络结构中,XQQ 协议通过在中间节点传递一个量子比特信息,使得接收方 B_1、B_2 能够以一定概率各自同时获得一个未知量子态.其中所有信道均为量子信道.

如图 2 所示,两个发送方 A_1、A_2 分别要传输信息到接收方 B_1、B_2. A_1 输入未知量子态 $|\varphi_1\rangle$,A_2 输入未知量子态 $|\varphi_2\rangle$.

XQQ 协议的主要步骤可以概括如下:

第一步,在节点 A_1 处,$(Q_1,Q_2)=UC(|\varphi_1\rangle)$;在节点 A_2 处,$(Q_3,Q_4)=UC(|\varphi_2\rangle)$;

第二步,在节点 C_1 处,$Q_5=GR(Q_2,TTR(Q_3))$;

第三步,在节点 C_2 处,$(Q_6,Q_7)=UC(Q_5)$;

第四步,在节点 B_1 和 B_2 处解码分别输出 ρ_1、ρ_2,

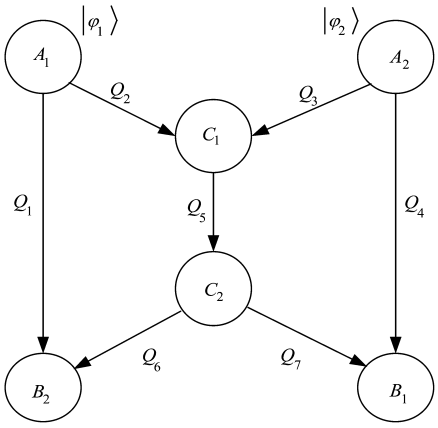


图2　XQQ协议的信息传递

其中 $\rho_1 = GR(Q_7, TTR(Q_4))$, $\rho_2 = BM(Q_1, Q_6)$.

其中 *UC* 运算引用了 Bužek 等人[12]提出的通用克隆. *TTR* 指对量子态执行 Tetra 测量,如第二步中的 *TTR*(Q_3)是对 Q_3 执行 Tetra 测量,得到两个经典比特 r_1r_2. r_1r_2 被用于选择四个不同的 Pauli 算子($I, \sigma_Z, \sigma_X, \sigma_Y$), r_1r_2 与 Q_3 一一对应,即 r_1r_2 是唯一的. *GR*(Q_2, *TTR*(Q_3))是利用 r_1r_2 选择的 Pauli 算子对 Q_2 进行 U 操作. 这个 Pauli 算子称为 *GR* 算子.

在节点 B_1 处,假设 $r_1r_2 \rightarrow U_x$(U_x 为四个 Pauli 算子之一),则 $Q_6 = Q_7 = U_x \cdot |\varphi_1\rangle$,则 $\rho_1 = U_x(Q_7, TTR(Q_4)) = U_x \cdot U_x|\varphi_1\rangle = |\varphi_1\rangle$.

在节点 B_2 处,通过比较 $Q_1 = |\varphi_1\rangle$ 和 $Q_6 = U_x \cdot |\varphi_1\rangle$,即通过 *BM* 测量,可以得到 r_1r_2,由 r_1r_2 可以得到 Q_3,从而得到 $|\varphi_2\rangle$,这样就完成了量子态的交叉传输.

3　可控量子网络编码方案

XQQ 协议关键是将 $|\varphi_2\rangle$ 进行离散化并对 $|\varphi_1\rangle$ 进行编码操作,这样在两个接收方处的解码都要依靠 $|\varphi_1\rangle$. 如果可以加入一个控制方来控制 $|\varphi_1\rangle$ 的传输,那么就可以同时控制两个接收方的解码.

如图 3 所示,本方案在 XQQ 协议基础上,添加一个控制方 Con,并与发送方 A_1 共享一个三粒子 GHZ 纠缠对:

$$|\varphi\rangle_{A_{1,2}A_{1,3}C} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)_{A_{1,2}A_{1,3}C}$$

其中,A_1 拥有粒子 $A_{1,2}$和 $A_{1,3}$,控制方 Con 拥有粒子 C.控制方 Con 到接收方 B_1、B_2 有两条经典信道,可以传输经典信息,Con 与 A_1 之间可以自由传输经典信息.

假设要传输的未知量子态 $|\varphi_1\rangle = \alpha|0\rangle + \beta|1\rangle$,则本方案的具体步骤如下:

第一步,在节点 A_1 处,$(Q_1, Q_2) = UC(|\varphi_1\rangle)$;在节点 A_2 处,$(Q_3, Q_4) = UC(|\varphi_2\rangle)$.

其中,在 A_1 处,经过 *UC* 克隆后,产生两个 $|\varphi_1\rangle$ 的复制态,一个复制态(Q_1)传输到 B_2 处,另外一个复制态(Q_2,这里将 Q_2 记为粒子 D)参与可控隐形传态.则 A_1 与 Con 总的粒子体系为:$|\psi\rangle = |\varphi\rangle_{A_{1,2}A_{1,3}C} \otimes |\varphi_1\rangle_D = \frac{1}{2}[|\varphi^+\rangle_{A_{1,2}D}(\alpha|00\rangle_{A_{1,3}C} + \beta|11\rangle_{A_{1,3}C}) + |\varphi^-\rangle_{A_{1,2}D}(\alpha|00\rangle_{A_{1,3}C} - \beta|11\rangle_{A_{1,3}C}) + |\psi^+\rangle_{A_{1,2}D}(\alpha|11\rangle_{A_{1,3}C} + \beta|00\rangle_{A_{1,3}C}) + |\psi^-\rangle_{A_{1,2}D}(\alpha|11\rangle_{A_{1,3}C} - \beta|00\rangle_{A_{1,3}C})]$

第二步,A_1 对粒子 $A_{1,2}$和 D 进行测量,得到四个 Bell 态的一个,并将该测量结果对应成经典信息 r_1r_2 ($00 \rightarrow |\phi^+\rangle$, $10 \rightarrow |\phi^+\rangle$, $01 \rightarrow |\Psi^+\rangle$, $11 \rightarrow |\Psi^-\rangle$),传输给控制方 Con,相应地粒子 $A_{1,3}$和粒子 C 将会变成一个纠缠态.这里假设粒子 $A_{1,2}$和 D 测量结果为 $|\varphi^+\rangle_{A_{1,2}D}$,那么 $r_1r_2 = 00$, $|\psi\rangle_{A_{1,3}C} = \alpha|00\rangle_{A_{1,3}C} + \beta|11\rangle_{A_{1,3}C}$.

第三步,控制方对粒子 C 实施 Hadamard 变换,对 C 进行测量,得到测量结果.并把测量结果对应为经典信息 r_3:$0 \rightarrow |0\rangle_C$, $1 \rightarrow |1\rangle_C$.这里不妨设测量结果为 $|1\rangle_C$,根据可控隐形传态,只要对粒子 $A_{1,3}$实施 U_1(见式 4)操作,变为 $|\varphi_1\rangle$,即 $|\varphi\rangle_{A_{1,3}} = (U_1)^{-1}|\varphi_1\rangle$.

第四步,在节点 A_1 处,$Q_2' = |\varphi\rangle_{A_{1,3}} = (U_1)^{-1}|\varphi_1\rangle$.

第五步,在节点 C_1 处,$Q_5 = GR(Q_2', TTR(Q_3))$.

第六步,在节点 C_2 处,$(Q_6, Q_7) = UC(Q_5)$.

第七步,在节点 B_1,解码输出 ρ_1, $\rho_1 = GR(Q_7, TTR(Q_4))$.

这里假设第四步经过 $TTR(Q_3)$选择的 *GR* 算子为 σ_Z,即 $Q_5 = GR(Q_2, TTR(Q_3)) = \sigma_Z \cdot |\varphi\rangle_{A_{1,3}}$,则 $\rho_1 = GR(Q_7, TTR(Q_4)) = \sigma_Z \cdot \sigma_Z \cdot |\varphi\rangle_{A_{1,3}} = |\varphi\rangle_{A_{1,3}}$.与 XQQ 协议有所不同,若此时解码获得的量子态 $|\varphi\rangle_{A_{1,3}}$并非要传输的 $|\varphi_1\rangle$,则两个接收方 B_1、B_2 都无法解码成功.

第八步,若控制方 Con 同意接收方获得未知量子态,则将测量结果 $r_1r_2r_3$ 通过经典信道分别传给 B_1、B_2,将 $|\varphi\rangle_{A_{1,3}}$ 恢复到 $|\varphi_1\rangle$ 来完成最后解码.具体操作如下:

表 1　各粒子测量结果与 U_x 关系

$\|\varphi\rangle_{A_{1,2}D}$	$\|\varphi\rangle_C$	$\|\varphi\rangle_{A_{1,3}}$	$r_1r_2r_3$	U_x
$\|\phi^+\rangle_{A_{1,2}D}$	$\|0\rangle_C$	$\alpha\|0\rangle + \beta\|1\rangle$	000	U_0
	$\|1\rangle_C$	$\alpha\|0\rangle - \beta\|1\rangle$	001	U_1
$\|\phi^-\rangle_{A_{1,2}D}$	$\|0\rangle_C$	$\alpha\|0\rangle - \beta\|1\rangle$	100	U_1
	$\|1\rangle_C$	$\alpha\|0\rangle + \beta\|1\rangle$	101	U_0
$\|\psi^+\rangle_{A_{1,2}D}$	$\|0\rangle_C$	$\alpha\|1\rangle + \beta\|0\rangle$	010	U_2
	$\|1\rangle_C$	$\alpha\|1\rangle - \beta\|0\rangle$	011	U_3
$\|\psi^-\rangle_{A_{1,2}D}$	$\|0\rangle_C$	$\alpha\|1\rangle - \beta\|0\rangle$	110	U_3
	$\|1\rangle_C$	$\alpha\|1\rangle + \beta\|0\rangle$	111	U_2

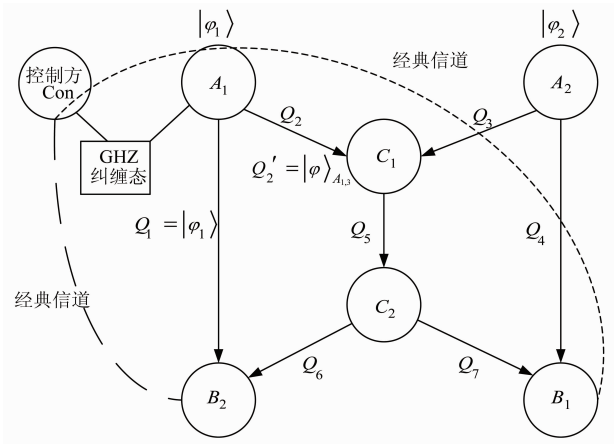


图3 可控量子网络编码方案

B_1、B_2 根据 Con 的测量结果 $r_1r_2r_3 = 000$ 决定对接收的量子态要进行的 U 操作为 U_1. 在 B_1 处解码输出 $\rho_{out}{}^1 = (U_1)\cdot GR(Q_7, TTR(Q_4)) = (U_1)\cdot|\varphi\rangle_{A_{1,3}} = (U_1)(U_1)^{-1}|\varphi_1\rangle = |\varphi_1\rangle$. 在 B_2 处，$\rho_2 = BM((U_1)^{-1}\cdot Q_1, Q_6) = (|\varphi_1\rangle, \sigma_Z\cdot|\varphi\rangle_{A_{1,3}}) \rightarrow |\varphi_1\rangle$.

在其他情况下，各粒子的测量结果 $r_1r_2r_3$ 与接收方选用的 U 操作算子 U_x 之间的对应关系如表 1 所示.

4 方案分析

从保真度、资源消耗、传输速率区域以及安全性等方面对本方案进行详细的分析.

1)保真度分析

假设输入量子态为 $|\psi_0\rangle$，输出量子态为 ρ，则保真度定义如下：

$$F = \langle\psi_0|\rho|\psi_0\rangle$$

由于 XQQ 协议中引入了近似克隆来解决量子态的不可克隆问题，显然会导致量子态失真，使得方案保真度小于 1. 本方案中引入的可控隐形传态可以实现量子态的完美传输，不会对保真度产生影响，即本方案的保真度等于 XQQ 协议的保真度. 因此，容易得到定理 1.

定理 1 令 $F_1(F_2)$ 为 $t_1(t_2)$ 处输出量子态的保真度，则有 $\frac{1}{2} < F_1(F_2) < 1$.

2)资源消耗分析

在该方案中，由于加入了控制方，它与发送方之间共享的三粒子纠缠态会增加更多的资源消耗. 并且为了控制接收方的解码，增加了两条经典信道. 在一次传输过程中，需要由控制方分别向接收方额外传送 3 个比特的经典信息才能完成解码操作.

3)传输速率区域分析

蝶形网络的速率区域定义如下[7]：假设一个协议使用蝶形网络和其他允许的资源 n 次，可以分别将 $n(r_1-\delta_n)$，$n(r_2-\delta_n)$位的比特/量子比特的信息 m_1, m_2 以至少 $1-\xi_n$ 的保真度交叉传输，则可达到的速率对 (r_1, r_2)，可达到的速率区域为所有速率对的集合，其中 $\delta_n, \xi_n \rightarrow 0$.

假设每条信道一次可传输 1 量子比特或 2 经典比特信息. 显然，XQQ 协议的传输速率区域为 $\{(r_1, r_2)\mid r_1, r_2 \leqslant 1\}$. 本方案为交叉传输两量子比特需要分别向两接收方传输 3 比特的经典信息 $r_1r_2r_3$，则需要使用图 3 中的两条经典信道 1.5 次，即 $(r_1, r_2) = \left(\frac{2}{3}, \frac{2}{3}\right)$，则传输速率区域为 $\left\{(r_1, r_2) \mid r_1, r_2 \leqslant \frac{2}{3}\right\}$.

4)安全性分析

在本方案中，可将 U_x 看成一个解码所必须的密钥，只有控制方才拥有这个密钥. 如图 4 所示，假设攻击者可以窃听获取接收方 B_1 处全部信息，如 Q_4、Q_7. 在控制方不同意解码的情况下，攻击者无法获得 U_x，只能获得 $(U_x)^{-1}|\varphi_1\rangle = |\varphi\rangle_{A_{1,3}}$. 因此，在控制方与接收方之间通信安全的前提下，该方案可以有效的抵御窃听攻击.

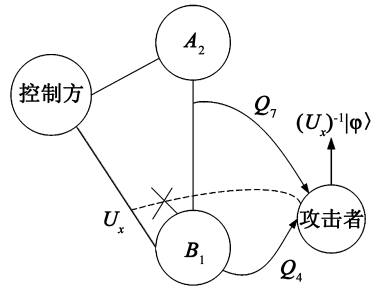


图4 窃听攻击模型

5)方案对比分析

通过以上分析可知，本文中的方案需额外消耗一个 GHZ 纠缠态和两条经典信道，来提高传输的安全性. 与 XQQ 协议相比，本方案保真度不变，传输速率区域由 $\{(r_1, r_2)\mid r_1, r_2 \leqslant\}$ 下降到 $\left\{(r_1, r_2) \mid r_1, r_2 \leqslant \frac{2}{3}\right\}$，见表 2.

表 2 方案对比

指标 / 方案	保真度	传输速率区域	GHZ 态
XQQ 协议	<1	$\{(r_1, r_2)\mid r_1, r_2 \leqslant 1\}$	0
本方案	<1	$\left\{(r_1, r_2) \mid r_1, r_2 \leqslant \frac{2}{3}\right\}$	1

6)讨论

本文提出的可控量子网络编码方案的保真度小于 1，不能实现信息的完美传输. 接收方要获得 1 量子比特的信息，就需要控制方的测量结果对应的 3 比特的经典信息. 显然，经典信道会限制整个方案的传输速率和效

率.如果将从控制方到发送方代表测量结果的3比特经典信息用量子信息进行密集编码并用量子信道进行传输,那么将会大大提高方案中量子信息的传输效率和安全性.另外,在控制方与接收方之间可以引入身份认证机制,只有在控制方确认接收方身份合法的前提下,才把测量结果告诉给接收方,则本方案可以作为一个安全的量子密钥分发模型,为量子网络编码分发密钥,从而提高量子网络编码的安全性.

5　结论

本文通过将可控隐形传态引入到量子网络编码中,设计了一种安全可控的量子网络编码方案,通过一个控制方实现了对量子网络编码模型中两个接收方的解码控制.而且,本方案可以与 QSDC 协议或者身份认证机制等相结合,进一步提高量子网络编码的安全性.

参考文献

[1] 黄辰,王芙蓉,戴彬,杨军,张波.基于网络编码的无线自组织网数据分发机制[J].电子学报,2010,38(8):1852 – 1857.
HUANG Chen, WANG Fu-rong, DAI Bin, YANG Jun, ZHANG Bo. Network Coding Based Data Dissemination in Wireless Ad Hoc Network[J]. Acta Electronica Sinica, 2010, 38(8):1852 – 1857.

[2] 田贤忠,周前伟.一种基于流内与流间网络编码的无线路由算法[J].电子学报,2013,41(2):395 – 401.
TIAN Xian-zhong, ZHOU Qian-wei. An Algorithm of Wireless Routing Based on Intra-Flow and Inter-Flow Network Coding [J]. Acta Electronica Sinica, 2013, 41(2):395 – 401.

[3] Hayashi M, Iwama K, Nishimura H, et al. Quantum Network Coding[A]. Proc of the 24th International Symposium on Theoretical Aspects of Computer Science[C]. Berlin: Springer, 2007:610 – 621.

[4] Hayashi M. Prior entanglement between senders enables perfect quantum network coding with modification[J]. Physical Review A, 2007, 76(4):040301.

[5] Ma S Y, Chen X B, Luo M X, et al. Probabilistic quantum network coding of M-qudit states over the butterfly network[J]. Optics Communications, 2010, 283(3):497-501.

[6] 闫帅帅,匡红艳,郭迎.基于可控量子隐形传态的蝶形网络量子编码研究[J].中国科技论文在线精品论文,2012,5(20):1996 – 2001.

[7] Nishimura H, Quantum Network Coding-How can network coding be applied to quantum information? [A]. Proc of the IEEE International Symposium on Network Coding[C]. Calgary, Canada, 2013:1 – 5.

[8] 温巧燕,郭奋卓,朱甫臣.量子保密通信协议的设计与分析[M].北京:科学出版社,2009.

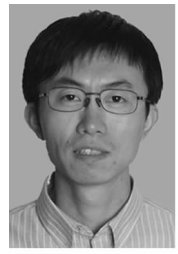
[9] Bennett C H, Brassard G, Crepeau C, et al. Teleportaion an Unknown Quantum State via Dual Claasical and EPR Channels [J]. Phys Rev Lett, 1993, 70(13):1895 – 1899.

[10] Zhou J, Hou G, Wu S, et al. Controlled Quantum Teleportaion [J]. arXiv preprint quant-ph/0006030, 2000.

[11] 叶俊.量子通信中的量子隐形传态技术研究[D].华中科技大学硕士论文,2007.

[12] Bužek V, Hillery M. Quantum copying: Beyond the no-cloning theorem[J]. Physical Review A, 1996, 54(3):1844 – 1852.

作者简介



尚　涛　男,1976 年出生于辽宁营口,博士,北京航空航天大学电子信息工程学院副教授,硕士生导师,主要研究方向为网络编码、网络安全等.
E-mail: shangtao@buaa.edu.cn

赵晓杰　男,1991 年出生于山东省临沂,硕士研究生,主要研究方向为量子网络编码及安全等.
E-mail: zhaoxiaojie0415@126.com

王　朝　男,1983 年出生于河北省保定,博士研究生,主要研究方向为量子密码学、网络安全等.
E-mail: wangchaobuaa@126.com

刘建伟　男,1964 年出生于山东莱州,博士,北京航空航天大学教授,博士生导师,主要研究方向为密码学、信息安全、网络安全等.
E-mail: liujianwei@buaa.edu.cn