计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190500168

一种基于量子 GHZ 态的防窃听网络编码

徐光宪　崔俊杰
辽宁工程技术大学电子与信息工程学院　辽宁 葫芦岛 125105

摘　要　经典网络编码在传输过程中的编码效率低,容易被窃听。虽然 Hayashi 提出的在发送端共享 EPR 的方式提高了信息传输过程中的编码效率,但其不能实现传输信息的完全恢复,也没有对信息进行安全处理,信息很容易被窃听。为此,文中提出了基于 GHZ 三粒子最大纠缠态,利用量子的不可克隆定理及隐形传态技术来防止信息被窃听的量子网络编码方案。首先,从经典的蝶形网络编码出发,在发送端对待发送粒子与 GHZ 态粒子进行直积操作;其次,对运算后的粒子进行 Bell 测量,并根据测量结果得到预编码信息,再将预编码信息传输给中间节点;然后,在接收端引入用于测量的辅助粒子,对接收到的粒子进行量子纠缠运算,并对粒子簇进行联合幺正运算;最后,依据编码信息选取相应的酉矩阵对粒子簇进行恢复。实验数据表明,基于 GHZ 态的量子网络编码在单次传输成功率上有了明显的提高,在编码效率上只需 6 个量子比特即可完成量子信息在蝶形网络中的交叉传输;在安全性方面,其提升了信息是否被窃听的可检测概率。实验数据充分表明,所提方案提高了网络编码系统的编码效率,有效地解决了信息传输的窃听问题。

关键词:网络编码;不可克隆;隐形传态;量子网络编码;窃听攻击
中图法分类号　TP391.9

Anti-eavesdropping Network Coding Based on Quantum GHZ State

XU Guang-xian and CUI Jun-jie
School of Electronic and Information Engineering, Liaoning Technical University, Huludao, Liaoning 125105, China

Abstract　The coding efficiency of classical network coding is inefficient during transmission and easy to be bugged. Although Hayashi's proposal of sharing EPR at the transmitter improves the coding efficiency for information transmission, it can not realize the complete recovery of transmitted information, and the information is not safely disposed, so it is easy to be bugged. To this end, based on the three-particle maximally entangled GHZ state, a quantum network coding scheme is proposed to prevent information being eavesdropped by using the quantum no-cloning theorem and teleportation. Starting from the classical butterfly network coding, the direct product operation is carried out on particles to be sent and the GHZ state particles at the sending end. Then bell measurement is performed on the calculated particles, and the precoding information can be obtained according to the measurement results. The precoding information is transmitted to intermediate nodes, and auxiliary particles used for measurement are introduced at the receiving end. Then, quantum entanglement computation is performed on the received particles, and joint unitary operation is performed on particle clusters. Finally, based on the coding information, corresponding unitary matrix is selected to restore particle clusters. Experimental data shows that the single transmission success rate of GHZ-based quantum network coding has been significantly improved, in terms of encoding efficiency, the cross transmission of quantum information in the butterfly network can be completed with only 6 qubits. In terms of security, the probability of detecting whether the information is bugged has improved. It proves that the proposed scheme improves the coding efficiency of the network coding system and effectively solves the bugging problem of information transmission.

Keywords　Network coding, No-cloning, Teleportation, Quantum network coding, Eavesdropping attack

1　引言

早在 2000 年,Ahlswede 等在开创性论文[1]中就给出了网络编码的经典定义。网络编码的效用颇多,最为学者熟知的就是可以提高吞吐量;此外,还可以改善鲁棒性,降低复杂度,提高安全性[2]。信息传输过程中的安全问题一直都是各方学者关注的重点,在网络编码中主要涉及窃听问题和信息污染问题。近年来,由于通信技术的快速发展,越来越多的学

到稿日期:2019-05-29　返修日期:2019-08-26　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家科技支撑计划(2013BAH12F02);辽宁省高等学校杰出青年学者成长计划项目(LJQ2014029)
This work was supported by the National Science and Technology Support Program (2013BAH12F02) and Liaoning Province University Outstanding Young Scholar Growth Plan Project (LJQ2014029).
通信作者:徐光宪(flybirdxgx@sohu.com)

者对量子通信技术的关注度有了很大提高。2016 年 8 月 16 日 1 时 40 分，墨子号量子科学实验卫星在酒泉用长征二号丁运载火箭成功发射升空，就是量子通信技术成功应用于实际的一个很好的例子。

量子通信具有无条件的安全性[3]。与经典的信息传输相比，量子通信系统的安全性不是基于算法的复杂度，而是由量子物理的基本原理保障[4]：1）量子世界在本质上存在真实的随机性，这是产生真随机密钥的关键原因；2）承载有非正交信息的单量子不能被完美克隆，这一特性最先由 Wootters 等于 1982 年证明，而这一理论被学者们称作量子的不可克隆原理[5]。量子通信的主要研究内容包含量子密集编码、量子的隐形传态技术、量子网络编码和量子通信的保密等。

量子网络编码的基本思想主要是通过对共有量子通信信道的量子态粒子进行编码来提高信道传输的容量，降低编码的错误率及编解码的复杂程度[6]。量子网络传输中的量子比特通过酉操作来实现编码。针对量子比特进行加密的系统是量子密码系统中重要的一类，而可以加密量子信息的系统同样也可以用来加密经典信息，只是需要先将经典信息制备为对应的量子态。

1993 年，Bennt 等第一次定义了量子隐形传态技术的概念。量子隐形传态技术是保密传输量子信息的一个经典例子[7]。Hayashi 等对量子通信网络的组播传输技术进行了针对性的深入研究，并开发出了一种无损压缩和解压缩量子比特信息的算法。在隐形传态中，发送方首先要完成纠缠态的分发[8]；而后双方利用纠缠提纯协议得到接近完美的纠缠态，再利用纠缠态的特性进行联合测量并公布测量结果；最后将信息重新复现出来。初始的纠缠态分发类似于传统密码中的密码分发，可理解为 Alice 和 Bob 共享了一组“量子密钥”，其中不包含待传输量子态的任何信息。在后续的操作中，携带信息的待传输量子态并没有进入信道，窃听者根本没有机会接触到信息载体。

科学家们通过研究发现，在针对量子隐形传态技术设计的方案中，发送方无须将编码后的粒子回传给接收方也同样可以实现量子信息的安全传输[9]。研究人员针对蝶形网络系统中的量子比特传输问题进行了分析，并得出了以下结论：在允许近似的情况下，量子网络编码实现的概率很大，但是如果没有其他外部条件，量子比特协助下准确的传播理论是不可能实现的[10]。Iwama 等随后研究了各种不同拓扑结构的量子网络系统，也证实了上述结论[11]。在量子通信网络中，量子信道编码可以在不改变现有信道容量的基础上提高量子比特的传输速率[12]。Leung 等提出了一种利用发送端共享的纠缠对，提前实现蝶形网络拓扑中量子比特无错交叉传输的方案[13]。

基于量子隐形传态技术提出的蝶形量子网络编码能够实现交叉传输经典信息和未知量子态两种方案，而且这两种方案都可以不传输经典信息，所有用到的信道都采用的是量子信道，利用量子信道来传输信息可以使信息在传输过程中的安全性和效率得到有效的提高。2015 年，Ma 等提出了经典信道与量子信道共同存在的假设，并在这个假设的基础上进一步提出了一种以基于非最大纠缠态为辅助编码信道来交叉传输量子比特的方案[14]。虽然该方案的编码效率相比文献[17]有了很大的提高，但其并没有对编码过程进行加密，因此安全性很低。为此，本文提出了基于 GHZ 三粒子最大纠缠态，利用量子的不可克隆定理及隐形传态技术来防止信息被窃听的量子网络编码方案。

2 经典网络编码

2.1 网络编码的基本思想

经典网络编码是一种混合信息论和路由的交换技术[15]，网络中节点进行的编码被称为网络编码，其中编码是指由输入到输出的任意因果映射。大多数网络编码的基本思想就是在中间节点处通过局部编码核进行编码的映射，在接收端点处通过全局编码核来进行解码。网络编码主要可以用来提高组播通信网络的吞吐量，以解决实际网络中传输无法达到最大理论容量的问题，网络编码打破了传统网络中只允许中继节点转发数据的限制，是一种使用中继节点对接收到的数据包进行编码和组合等智能化处理的方式。

网络编码最为人熟知且最易解释的效用是提高吞吐量。吞吐量的提高由更有效的分包传输实现，即用更少的分包传输获取更多的信息。Ahlsw 等给出了这类例子，考虑了有线网络中的多播问题。这些例子通常被称为蝴蝶网。

2.2 蝶形网络的编码思想

蝶形网络具有一个信源节点到两个信宿或者目的节点的多播特性，两个信宿都想获得信源节点发送的全部信息。在考虑的约束网中，只有当中间节点打破分组网络中传统的复制转发路由方式并进行编码操作后，才能够建立所需的多播连接；该中间节点对接收到的两个包的内容进行二进制加法或者异或处理，得到一个新包，并将该新包输出。蝶形网络的编码示意图如图 1 所示。

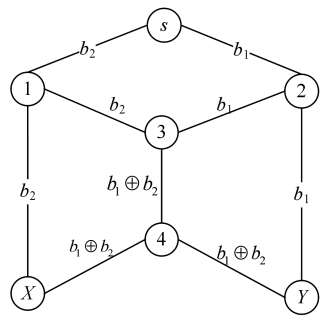

图 1 蝶形网络编码图

Fig. 1 Diagram of butterfly network coding

图 1 中，s 表示信源节点，X 和 Y 分别为信宿节点。如果两个接收包的内容分别为比特向量 b_1 和 b_2，则输出包为 $b_1 \oplus b_2$，即向量 b_1 和 b_2 的逐位异或。两信宿节点分别对其接收到的数据包进行进一步的编码处理，以实现解码。信宿节点 Y 对 b_1 和 $b_1 \oplus b_2$ 进行异或处理，解出 b_2；同样地，信宿节点 X 对 b_2 和 $b_1 \oplus b_2$ 进行异或处理，解出 b_1。蝶形通信网络显示，网络编码可以增加有线网络的多播吞吐量。

因此，网络编码的核心思想可以简述为：网络中具备编码条件的所有点对接收到的传输信息进行编码处理，然后传输给下一级网络节点，并依此类推，直到全部经过处理的信息都

汇聚到信宿节点上，在信宿节点上对其进行译码，就可得到信源端发出的原始信息。

3 量子网络编码

3.1 量子不可克隆原理

1982 年，Wootters 和 Zurek 提出了在量子力学系统中一个未知的量子态不可能被全部准确克隆的原理[16]，即量子不可克隆原理。下面对此定理进行证明，设未知量子态为：

$$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle,|\alpha|^2+|\beta|^2=1,\alpha\beta\neq0 \tag{1}$$

假设复制装置的初态为$|A\rangle$，则量子态被完全克隆的准确表达式为：

$$|A\rangle|\varphi\rangle\rightarrow|A_\varphi\rangle|\varphi\rangle|\varphi\rangle \tag{2}$$

其中，$|A_\varphi\rangle$为装置复制以后的状态，将其代入式(1)可得：

$$|A\rangle|\varphi\rangle=|A\rangle(\alpha|0\rangle+\beta|1\rangle)\rightarrow\alpha|A_0\rangle|0\rangle|0\rangle+\beta|1\rangle|1\rangle \tag{3}$$

而纯态为：

$$|\varphi\rangle|\varphi\rangle=(\alpha|0\rangle+\beta|1\rangle)(\alpha|0\rangle+\beta|1\rangle)\rightarrow(\alpha|0\rangle+\beta|\rangle1)^2 \tag{4}$$

由此可以得出结论：不存在能完美克隆任意未知量子态的量子克隆机。如果用于编码的量子态中包含非正交态，当窃听者通过量子操作来获得关于编码的信息时，接收方所收到的量子态和发送方原始制备的量子态就会有所不同，这就会导致其统计特性发生变化，从而使窃听被通信双方所察觉。量子不可克隆定理是量子密码学的一个重要基础，它保证了量子密码的安全性，使得窃听者 Eve 不可以通过克隆未知信息态来获得传输信息。将这一理论应用到蝶形网络编码上，就可以有效地防止传输信息被窃听，从而提高通信网络的安全性。

3.2 量子隐形传态

Alice 将两体纠缠态的一个模式通过信道发送给 Bob，而后双方利用纠缠态提纯协议得到接近完美的纠缠态。利用纠缠的特性，Alice 在本地对待传输量子态$|\varphi\rangle=\alpha|0\rangle+\beta|1\rangle$和纠缠态保留的模式进行联合测量，并公布测量结果，使得 Bob 手中纠缠态的另一个模式所塌缩到的量子比特系数与$\{\alpha,\beta\}$仅有一个可纠正的“符号”差异，这就实现了在$|\varphi\rangle$不经过信道的条件下，将其在 Bob 端重新复现出来。初始的纠缠态分发类似于传统密码中的密钥分发，可以理解为 Alice 和 Bob 共享了一组“量子密钥”，其不包含传输量子态的任何信息。在后续操作中，携带信息的待传输量子态并没有进入信道，窃听者根本没有机会接触信息载体。因此，这种传递信息的方式与窃听者的计算能力无关，是无条件安全的。

3.3 量子纠缠态

量子纠缠态是 Schrodinger 于 1935 年首次提出的。在量子通信网络中，量子信道编码可在现有信道的基础上提高量子比特的传输速率。量子纠缠是量子信息论中一个独特的概念，不能与经典理论相对应。如果一个复杂的系统不能写成它的子系统状态的张量积，那么它就处于纠缠态。量子密码学中应用最广泛的状态是双粒子系统的 Bell 态和三粒子系统的 GHZ 状态 。GHZ 态是一种比较独特的量子纠缠状态，可看作三粒子系统下的最大纠缠态。1998 年，量子纠缠交换技术第一次完成，实现了将两个不纠缠的光子纠缠在一起。这里，纠缠的本质原理其实就是经过不同的测量和组合，使得纠缠特性在粒子之间传递、交换的过程。

3.4 基于最大纠缠态的蝶形量子网络编码

2007 年，Hayashi 等提出了通过在发送两端共享 EPR 来实现对量子态信息传输的方案[17]，如图 2 所示。

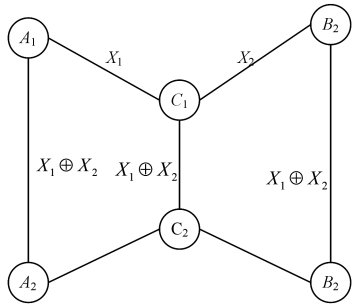

图 2 最大纠缠量子

Fig. 2 Maximum quantum entanglement

首先在发送端 A_i 与共享 EPR 粒子 φ 进行直接操作，随后进行 Bell 测量，并将酉操作 $U(X_i)^{-1}$ 作用于 $A_{i,i\oplus1}$ 上，其次将作用后的结果由 A_i 端发送给接收端 B_i，最后在 B_i 端对收到的预编码信息 $X_i\oplus X_{i\oplus1}$ 进行解码操作，从而恢复出粒子。

3.5 基于非最大纠缠态的蝶形量子网络编码

在一般的非实验环境中，人们常常制造的是非最大纠缠态的粒子对。对此，2015 年 Ma 等提出了经典信道与量子信道共同存在的假设，并在这个假设的基础上进一步提出了一种以基于非最大纠缠态为辅助编码信道来交叉传输量子比特的方案，如图 3 所示。

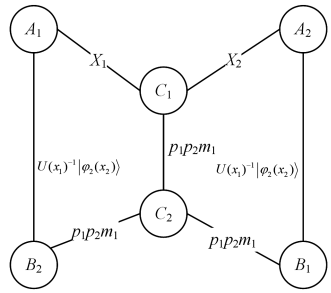

图 3 非最大纠缠态

Fig. 3 Non-maximal entanglement state

(1)在发送端 A_i 对准备发送的粒子$|\varphi_i\rangle$及本侧非最大纠缠对粒子 $A_{i'}$ 进行联合 bell 态测量。

(2)在传输端 A_i 将酉操作 $U_{x_i}^{-1}$ 作用于粒子$|\varphi_{i\oplus1}(X_{i\oplus1})\rangle$，并通过信道 $A_iB_{i\oplus1}$ 将作用后的粒子传输给接收端 $B_{i\oplus1}$。

(3)节点 C_1 将信息 $p_1p_2m_1$ 经过编码信道 C_1C_2 发送给节点 C_2，在此过程中进行的编码操作为 $p_1p_2=X_1\oplus X_2$，此后将粒子传送给接收端 B_1，B_2。

(4)接收端 B_i 根据预编码信息来选择对应的酉操作，并将其作用于$|\varphi_{i\oplus1}(X_{i\oplus1})\rangle$。若 $m_1=0$，则在 B_1 端采用酉操作 V_0；若 $m_1=p_1$，则在 B_2 端采用酉操作 V_1。

$$V_1=\begin{pmatrix}\frac{b_0}{b_1} & 0 & \sqrt{1-\frac{b_0^2}{b_1^2}} & 0\\ 0 & 1 & 0 & 0\\ \sqrt{1-\frac{b_0^2}{b_1^2}} & 0 & -\frac{b_0}{b_1} & 0\\ 0 & 0 & 0 & -1\end{pmatrix} \tag{5}$$

$$V_0=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & \frac{b_0}{b_1} & 0 & \sqrt{1-\frac{b_0^2}{b_1^2}}\\ 0 & 0 & -1 & 0\\ 0 & \sqrt{1-\frac{b_0^2}{b_1^2}} & 0 & -\frac{b_0}{b_1}\end{pmatrix} \tag{6}$$

则接收端 B_i 恢复 $|\varphi_i\rangle$ 的概率为 $2(b_0)^2$。

3.6 基于 GHZ 态的蝶形量子网络编码

蝶形量子网络编码(见图 4)这种通信方案采用的是经典的蝶形网络，可从两个方面加以说明：1)传输经典信息；2)传输未知量子态信息，下面基于蝶形量子网络编码来证明量子网络编码的防窃听性能。

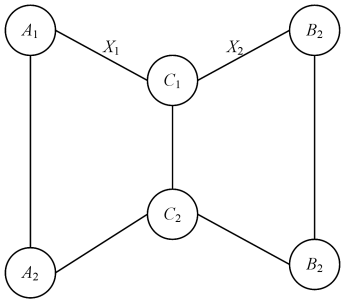

图 4 蝶形量子网络编码

Fig. 4 Butterfly quantum network coding

3.6.1 发送端预编码操作

假设待发量子比特为 $m_i(i=1,2)$，$|m_i\rangle=\alpha_i|0\rangle+\beta_i|1\rangle$，其中 $|\alpha|^2+|\beta|^2=1$，在发送端将待发送粒子 $|m_i\rangle$ 与该处所拥有的 GHZ 态粒子 $A_{i\bar{i}}$ 进行直积操作：

$$|GHZ\rangle_{A_{11}A_{21}G_1}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{A_{11}A_{21}G_1} \tag{7}$$

$$|GHZ\rangle_{A_{12}A_{22}G_2}=\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)_{A_{12}A_{22}G_2} \tag{8}$$

然后，在发送端 A_1 处对粒子 A_{11} 与 $|m_1\rangle$ 进行直积变换操作：

$$|\varphi\rangle_{A_{11}A_{21}G_1}=|m_1\rangle\otimes|GHZ\rangle_{A_{11}A_{21}G_1} \tag{9}$$

并进行 Bell 测量。预计测量结果如下：

$$\varphi_{00}^{+}=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{m_1A_{11}} \tag{10}$$

则可以确定粒子的状态为 $|\psi(00)\rangle=(\alpha_1|00\rangle+\beta_1|11\rangle)_{A_{21}G_1}$。

根据测量结果可得预编码信息 $M_i=n_ig_i(M_1=00)$，选择酉操作 U_{00}：

$$U_{00}|\Theta\rangle=U_{00}\otimes\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle) \tag{11}$$

在发送端 A_2 对粒子 A_{22} 与 $|m_2\rangle$ 进行直积操作的变换结果为：

$$|\varphi\rangle_{A_{12}A_{22}G_2}=|m_2\rangle\otimes|GHZ\rangle_{A_{12}A_{22}G_2} \tag{12}$$

对粒子进行 Bell 态测量，结果为：

$$\varphi_{01}^{-}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{m_2A_{22}} \tag{13}$$

粒子 A_{12} 和 G_2 的状态可以表示为：

$$|\psi(01)\rangle=(\alpha_1|00\rangle-\beta_1|11\rangle)_{A_{22}G_2} \tag{14}$$

若 $M_2=01$，则选取酉操作 U_{01}。

发送端 A_i 完成对粒子 $|m_i\rangle$ 和 $A_{i\bar{i}}$ 的 Bell 态测量之后，依据测量结果相对应的 M_i 值来选取相应酉操作的逆 $U_{M_i}^{-1}$，并将其作用于粒子 $A_{i,i\oplus1}$ 上，随后将其发送给接收端 $B_{i\oplus1}$，同时将预编码信息 M_i 传给节点 C_i，此处的操作为：

$$U_{00}=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\quad U_{10}=\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$$
$$U_{01}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\quad U_{11}=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} \tag{15}$$

3.6.2 中间节点的编码

中间节点 C 在接收到发送端 A_1 和 A_2 发送的纠缠态粒子并进行联合 Bell 态测量后，根据表 1 可以恢复出预编码信息：$M_1=00$，$M_2=01$。

表 1 预编码信息与 Bell 态测量结果的对应关系

Table 1 Correspondence between precoding information and measurement results in Bell state

预编码信息	Bell 态测量结果
00	$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)$
01	$\frac{1}{\sqrt{2}}(\|10\rangle+\|01\rangle)$
10	$\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)$
11	$\frac{1}{\sqrt{2}}(\|01\rangle-\|10\rangle)$

节点 C_2 通过信道 C_2B_1 与 C_2B_2 依次将以上比特信息发送给接收端 B_1 和 B_2。

3.6.3 中间节点的解码

接收端 B_2 对从节点 C 发来的粒子和本侧 EPR 粒子进行 Bell 测量，测量结果如下：

$$|\Theta_1\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)\,|\Theta_2\rangle=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle) \tag{16}$$

依据表 1 的对应关系，即可恢复编码信息 $b_1P_1P_2P_3=0010$。选取酉操作 U_{01} 作用于粒子 $A_{1,2}$ 上，$U_{01}|\psi(01)\rangle=(-\beta_2|01\rangle+\alpha_2|10\rangle)A_{1,2}G_2$ 为基态中的一种情况，只有通过解码操作，恢复的预编码信息为 $M_2=01$ 的粒子才能确定其为基态中的 $U_{01}|\psi(01)\rangle$，相似地在接收端 B_1 对 $|\Theta_3\rangle$ 和 $|\Theta_4\rangle$ 进行测量，通过解码操作恢复的预编码信息 $M_1=00$ 可以确定粒子 $A_{2,1}$ 为 $U_{00}|\varphi(00)\rangle$。

3.6.4 信息的恢复

为了能在接收端 B_i 恢复出即将发送的粒子，在此引入一个用于测量的辅助粒子，粒子的初始状态为 $|0\rangle_{b_i}$，对发送粒子进行量子纠缠运算，然后对粒子簇进行联合幺正运算。若 $g_1=0$，则在接收端 B_1 处将酉操作 V_0 作用于上述粒子簇；若 $g_1=p_1$，则在接收端 B_2 处将酉操作 V_1 作用于上述粒子簇。此处：

$$V_0=V_1=\begin{pmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & -1 & 0\\ 0 & 0 & 0 & -1\end{pmatrix} \tag{17}$$

在 B_i 处对引入的粒子进行测量。若测量结果为 $|0\rangle_{B_i}$，则说明粒子发送成功；若测量结果为 $|1\rangle_{B_i}$，则说明粒子发送失败。因此，B_i 端可恢复出发送粒子的初始态 $|\varphi\rangle_i$ 的概率为：

$$4\times\left(\frac{\frac{1}{\sqrt{2}}}{\frac{1}{\sqrt{2}}}\right)^2=1 \tag{18}$$

4 安全性分析

4.1 中间节点编码

网络中间节点编码的加密方式是，当信源产生原始消息之后，选取每个原始数据消息矩阵的最后一行元素进行加密，加密方式是引入 Logistic 混沌时间序列。

首先，需要将 α 作为初值生成 Logistic 混沌序列。Logistic 混沌时间序列的取值都是整数，表示为：

$$x_{n+1}=\mu x_n(2^n-x_n)/2^n,0\leqslant x_n<2^n \tag{19}$$

然后，用混沌序列 $Y(\alpha)$ 对最后一维数据 x_n 加密。

$$c_n=(x_{n1}+Y(\alpha),x_{n2}+Y(x_{n1},\alpha),\cdots,x_{nm}+Y(x_{n1},x_{n2},\cdots,x_{nm-1},\alpha)) \tag{20}$$

则加密后，原始消息就可以表示为：

$$X'=(x_1,x_2,\cdots,x_{n-1},c_n)^{\mathrm{T}}$$

第一步加密后，在中间节点构造全局编码矩阵。令全局编码矩阵为 $\boldsymbol{T_X}$，从生成矩阵 $\boldsymbol{T_X}$ 对角线上的元素入手，利用 m 序列扰动 Logistic 混沌序列，同样将生成的序列执行取整操作以构造矩阵 $\boldsymbol{T_X}$ 中对角线上的元素。首先，用 $t_i,i\in[1,n]$ 来表示对角线上的元素，m 序列可以表示为 $(m_1,m_2,\cdots,m_n)$。m 序列中的任一序列用 $m_i,i\in[1,n]$ 表示，它是在一个既定初值生成的 m 序列中，取连续 8 位伪随机数，用 $Y(\beta)$ 表示初值 β 产生的 Logistic 混沌时间序列经过 m 序列扰动 Logistic 序列生成的全局编码矩阵对角线元素为：

$$t_1=Y(\beta)\oplus m_1,t_2=Y(t_1)\oplus m_2,\cdots,t_n=Y(t_{n-1})\oplus m_n \tag{21}$$

其中，$\oplus$ 表示异或运算，即模二加运算。至此，全局编码矩阵 $\boldsymbol{T}_X$ 的对角线元素全部构造完毕。令该矩阵中最后一列除 t_n 以外的元素都由随机数 k 构成，矩阵中剩余元素用 0 表示，那么信源节点处的全局编码矩阵 $\boldsymbol{T}_X$ 就构造完成了。

$$\boldsymbol{T}_X=\begin{pmatrix}t_1&0&\cdots&k\\0&t_2&\cdots&k\\\vdots&\vdots&&\vdots\\0&0&\cdots&t_n\end{pmatrix} \tag{22}$$

全局编码矩阵 $\boldsymbol{T_X}$ 构造完之后，接着在信源节点处利用矩阵 $\boldsymbol{T_X}$ 与已加密的信源消息 X'' 进行线性运算，从而构造出加密消息 X'。

$$\boldsymbol{X'}=\boldsymbol{T_X}X''=\begin{pmatrix}t_1&0&\cdots&k\\0&t_2&\cdots&k\\\vdots&\vdots&&\vdots\\0&0&\cdots&t_n\end{pmatrix}\begin{pmatrix}x_1\\x_2\\\vdots\\c_n\end{pmatrix}=\begin{pmatrix}x_1'\\x_2'\\\vdots\\x_n'\end{pmatrix} \tag{23}$$

对于攻击者而言，在节点处加密后的传输消息矩阵 $\boldsymbol{X'}$ 和节点处的全局编码矩阵 $\boldsymbol{T_X}$ 是相互独立的。窃听者在截获了通信链路中传输的全部加密信息后，依然无法破译出正确的原始消息数据。

4.2 中间信道编码

在中间编码信道的设计上，根据量子态的特性选择“二次检测安全”的保障方案能够有效地防止攻击者对编码信息的窃听，保证了信息的安全传输，达到了设计的目的。在截听-重发窃听中，窃听者 Eve 想要在信道中截取发送者 Alice 发送的量子态信息，就必须随机选取一组基对量子态进行测量，然后把测量结果 $\{w_n\}$ 记录下来，再根据测量结果在该测量基下制备所对应的偏振量子态并发送给 Bob，即使选择了相同的基，Bob 端的数据与 Alice 端的数据也存在不一致的情况。

由于窃听者 Eve 事先并不知道 Alice 制备发送量子态时所选择的基，因此她只能随机地选择测量基。对于选对基的一半量子态，窃听者 Eve 能够准确地获得测量结果，因此其制备发送给 Bob 的量子态也是正确的，使得 Bob 的最终测量结果也是正确的。对于选错基的一半量子态，无论 Eve 得到哪个测量结果，其都要在错误的基组下去制备发送给 Bob 的量子态，因此，即使 Bob 的测量基与 Alice 的制备是一致的，其也有 50%的可能性得到错误结果。总体来看，Bob 端接收的数据中将有 50% * 50% = 25% 的数据与 Alice 端不同，即 Bob 与 Alice 不同。也就是说，Bob 和 Alice 的数据在基选择正确的情况下也有 25%的误码率，相比没有窃听者时接近 0 的误码，这样高的误码率非常容易区分，因此极易发现信息是否被窃听。

假设攻击者 Eve 可以通过窃听信道来截取传输的信息，由于采用的编码信道为量子信道，因此窃听者很有可能是通过直接攻击 $|\varepsilon_{a,b}\rangle$ 与信道粒子进行纠缠：

$$|\psi_{a,b,c}\rangle=\sum_{a,b\in0,1}|\varepsilon_{a,b}\rangle|a\rangle|b\rangle \tag{24}$$

其中，$|a\rangle$ 和 $|b\rangle$ 是 A_1 和 C 之间共享的 EPR 粒子。制备一个任意的量子比特：

$$|l\rangle=\cos\theta|0\rangle+e^{-i\theta}\sin\theta|1\rangle \tag{25}$$

作为探测粒子，将量子可控非门操作 $C_{a,t}$ 作用于探测粒子 $|l\rangle$ 及 A_i 侧的 EPR 纠缠对粒子上。

$$|l^{\mathrm{CNOT}}\rangle=C_{a,t}|\psi\rangle|l\rangle \tag{26}$$

Inamori(稻盛和夫)理论[18]，探测粒子满足正交性：

$$\sum_{a,b\in0,1}\langle\varepsilon_{a,b}|\varepsilon_{a,b}\rangle=1 \tag{27}$$

则窃听者 Eve 的探测操作对粒子的影响为：

$$\hat{E}|0,E\rangle\equiv\hat{E}|0\rangle_c|E\rangle=\alpha|0,\varepsilon_{00}\rangle+\beta|1,\varepsilon_{01}\rangle \tag{28}$$

$$\hat{E}|1,E\rangle\equiv\hat{E}|1\rangle_c|E\rangle=\alpha'|1,\varepsilon_{11}\rangle+\beta'|1,\varepsilon_{10}\rangle \tag{29}$$

其中，酉操作 $\hat{E}$ 为：

$$\hat{E}=\begin{pmatrix}\alpha&\beta'\\\beta&\alpha'\end{pmatrix} \tag{30}$$

因为探测操作是酉矩阵，所以一定满足以下的关系：

$$|\alpha|^2+|\beta|^2=1,|\alpha'|^2+|\beta'|^2=1,\alpha\beta^*+\alpha'^*\beta'=0 \tag{31}$$

由此，可以得到：

$$|\alpha'|^2=|\alpha|^2,|\beta'|^2=|\beta|^2 \tag{32}$$

探测操作可能出现的错误率如下：

$$\tau=|\beta|^2=|\beta'|^2=1-|\alpha|^2 \tag{33}$$

窃听者 Eve 可能截取窃听的最多传输信息量可以通过以下方式计算得出：在发送端 A_1 处，对本侧 EPR 粒子的测量结果为 $|1\rangle$，则由 A_1，C 与窃听者 Eve 所组成的粒子簇中的剩余粒子可表示为：

$$|\psi'\rangle=\hat{E}|0,E\rangle=\alpha|0,\varepsilon_{00}\rangle+\beta|1,\varepsilon_{01}\rangle \tag{34}$$

约化密度算子[19]：

$$\rho'=|\alpha|^2|0,\varepsilon_{00}\rangle\langle 0,\varepsilon_{00}|+|\beta|^2|1,\varepsilon_{01}\rangle<1,\varepsilon_{01}|+\alpha\beta^*|0,$$

$$\rho''=\begin{pmatrix}(p_0+p_3)|\alpha|^2 & (p_0-p_3)\alpha\beta^*\\ (p_0-p_3)\alpha^*\beta & (p_0+p_3)|\beta|^2\\ 0 & 0\\ 0 & 0\end{pmatrix}$$

$$\begin{pmatrix}0 & 0\\ 0 & 0\\ (p_1+p_2)|\alpha|^2 & (p_1-p_2)\alpha\beta^*\\ (p_1-p_2)\alpha^*\beta & (p_1+p_2)|\beta|^2\end{pmatrix} \tag{35}$$

其中，$p_0+p_1+p_2+p_3=1$。

依据 Von Neumann 理论[20]，从该矩阵 $\boldsymbol{\rho}''$ 表达中可以分离出的最大信息量为：$I_0=\sum_{i=0}^{3}-\lambda_i\log_2\lambda_i$。

这里，λ_i 为 ρ'' 的特征值：

$$\lambda_{0,1}=\frac{1}{2}(p_0+p_3)\pm\frac{1}{2}\sqrt{(p_0+p_3)^2-16p_0p_3(\tau-\tau^2)}$$

$$\lambda_{1,2}=\frac{1}{2}(p_1+p_2)\pm\frac{1}{2}\sqrt{(p_1+p_2)^2-16p_1p_2(\tau-\tau^2)}$$

当概率相等时，信息熵最大：

$$I_0=(1-\tau)\log_2\frac{1-\tau}{2}\tau\log_2\frac{\tau}{2}$$

对 $I_0=(1-\tau)\log_2\frac{1-\tau}{2}\tau\log_2\frac{\tau}{2}$ 进行求导以后，可以求得函数在 $\tau=1/2$ 时的最值。这意味着，如果攻击者 Eve 确实存在，那么她被检测到的概率 $\tau(I_0)>0$。假设可以完全得到想要获得的信息，即 $I_0=1$，则其可以被检测到的概率为 $\tau=1/2$。攻击者 Eve 为窃取编码信息，将酉矩阵作用在 $|\psi_{a,b,c}\rangle$ 上：

$$\begin{aligned}|l^{CNOT}\rangle=&\frac{1}{2}(\cos\theta|0_a0_c0_l\rangle+e^{-i\theta}\sin\theta|0_a0_c1_l\rangle\otimes|\varepsilon\rangle+\\&\frac{1}{2}(\cos\theta|0_a1_c0_l\rangle+e^{-i\theta}\sin\theta|0_a1_c1_l\rangle\otimes|\varepsilon\rangle+\\&\frac{1}{2}(\cos\theta|1_a0_c1_l\rangle+e^{-i\theta}\sin\theta|1_a0_c1_l\rangle\otimes|\varepsilon\rangle+\\&\frac{1}{2}(\cos\theta|1_a1_c1_l\rangle+e^{-i\theta}\sin\theta|1_a1_c0_l\rangle\otimes|\varepsilon\rangle\end{aligned} \tag{36}$$

在中间节点对接收到的粒子进行量子可控非门操作：

$$\begin{aligned}C_{a,t}(\hat{E}|\psi_{a,b,c}\rangle)|l\rangle=&\frac{1}{2}(\cos\theta|0_a0_c0_l\rangle+e^{-i\theta}\sin\theta|0_a0_c1_l\rangle\otimes\\&|\varepsilon\rangle+\frac{1}{2}(\cos\theta|0_a1_c0_l\rangle+e^{-i\theta}\sin\theta\\&|0_a1_c1_l\rangle\otimes|\varepsilon\rangle+\frac{1}{2}(\cos\theta|1_a0_c1_l\rangle+\\&e^{-i\theta}\sin\theta|1_a0_c0_l\rangle\otimes|\varepsilon\rangle+\frac{1}{2}(\cos\theta|\\&1_a1_c0_l\rangle+e^{-i\theta}\sin\theta|1_a1_c1_l\rangle\otimes|\varepsilon\rangle\end{aligned} \tag{37}$$

显然可以看出：$C_{a,t}(\hat{E}|\psi_{a,b,c}\rangle)|l\rangle\neq|\psi\rangle\otimes|l\rangle$。因此，并不能从 $|l^{CONT}\rangle$ 中得到粒子 $|l\rangle$。本文对原始矩阵 $\boldsymbol{X}$ 的最后一维进行加密，因此窃听者只能获取 $\boldsymbol{X}$ 的前 $m-1$ 维的数据，存在如下关系：$H(X_i'|x_1,x_2,\cdots,x_{m-1})=H(X_i)$，$i=1,2,3,\cdots,m-1$。当窃听者可以窃听到 $x_1,x_2,\cdots,x_{m-1}$ 时，窃听者得不到信源消息的任意一维 X_i，其中 $i=1,2,3,\cdots,m$。由于编码方案对最后一维进行了加密，因此窃听者得不到最后一维消息，我们只需证明窃听者窃听不到前 $m-1$ 维信息即可推出 $I(X_i;x_1,x_2,\cdots,x_{m-1})=0$。由 $H(X_i'|\rangle x_1,x_2,\cdots,x_{m-1})=\varepsilon_{00}\rangle<|1,\varepsilon_{01}\rangle+\alpha^*\beta|1,\varepsilon_{01}\rangle|0,\varepsilon_{00}|$

对本侧 EPR 粒子分别进行概率为 p_0，p_1，p_2 和 p_3 的酉矩阵操作 U_{00}，U_{01}，U_{10}，U_{11} 后其可整理为：

$H(X_i)$ 可以推出：

$$\begin{aligned}&H(X_i'|x_1,x_2,\cdots,x_{m-1})-H(X_i)\\&=I(X_i;x_1,x_2,\cdots,x_{m-1})\\&=I(X_i+iX_m;x_1,x_2\cdots x_{m-1})\\&=I(X_i,X_m;x_1,x_2\cdots x_{m-1})\end{aligned}$$

其中，$i=1,2,3,\cdots,m-1$。

由互信息量的非负性可知上式成立。由此可知本方案是安全的。

4.3 对攻击的分析

唯密文攻击的安全性能分析首先对唯密文攻击的安全方案进行评估。前文已经介绍了混沌序列具有不可逆的性质，因此可以认为产生的混沌序列是相互独立且均匀分布的。在本文安全方案中，利用混沌序列对信源消息 X 和信源处全局编码矩阵 $\boldsymbol{T_X}$ 进行加密能得到定理 1。

定理 1 在信源处经过加密后的传输消息矩阵 $\boldsymbol{X}'$ 和信源处的全局编码矩阵 $\boldsymbol{T_X}$ 对于攻击者而言是相互独立的。

定理 1 的推导过程如式(38)所示：

$$\begin{aligned}&Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}}|X'=\overrightarrow{X'})\\&=\frac{Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}},X'=\overrightarrow{X'})}{Pr(X'=\overrightarrow{X'})}\\&=\frac{Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}},X''=\overrightarrow{X''})}{Pr(X''=\overrightarrow{X''})}\\&=\frac{Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}})Pr(X''=\overrightarrow{X''})}{Pr(X''=\overrightarrow{X''}}\\&=Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}})\end{aligned} \tag{38}$$

其中，$\boldsymbol{T_X}$ 表示全局编码矩阵，$\boldsymbol{X}'$ 表示加密后的消息矩阵，两者互相独立；$Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}}|\rangle X'=\overrightarrow{X'})=\Pr(\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}})$，$\overrightarrow{\boldsymbol{T_X}}$ 和 $\overrightarrow{X'}$ 表示的是窃听者所窃听到的消息向量。为了确保信宿节点顺利解码，必须保证全局编码矩阵 $\boldsymbol{T_X}$ 是满秩矩阵。矩阵满秩同样也是可逆的。由于 $X'=\boldsymbol{T_X}\boldsymbol{X}''$，$\overrightarrow{X'}=\overrightarrow{\boldsymbol{T_X}}\overrightarrow{X''}$，$\boldsymbol{T_X}$ 和 $\overrightarrow{\boldsymbol{T_X}}$ 是可逆矩阵，根据 $\overrightarrow{X'}=\overrightarrow{\boldsymbol{T_X}}\overrightarrow{X''}$，矩阵 $\boldsymbol{T_X}=\overrightarrow{\boldsymbol{T_X}}$ 能够得到唯一的矩阵 $X'=\overrightarrow{X'}$，即 $Pr(X'=\overrightarrow{X'})=Pr(X''=\overrightarrow{X''})$。本文用到的混沌序列是相互独立且均匀分布的，那么运用混沌序列进行加密的矩阵也是相互独立的。根据上文对条件概率的推导可以证明，传输消息矩阵 $\boldsymbol{X}'$ 和信源处的全局编码矩阵 $\boldsymbol{T_X}$ 对于攻击者而言是相互独立的。由定理 1 可以进一步得出定理 2。

定理 2 具备窃听全局能力的窃听者在截获了通信链路中传输的全部加密信息后，依然无法破译出正确的原始消息数据。

证明：已知窃听者在网络拓扑中截获了全部加密数据消息 X'，但是不论窃听者的能力有多强大，由定理 1 可知，它都无法获得与信源处全局编码矩阵 $\boldsymbol{T_X}$ 相关的任何信息，即使

窃听者获取了全部密文，它也无法利用截获的密文推导出全局编码矩阵 $\boldsymbol{T_X}$；再者，原始的数据消息在信源端进行了加密操作，因此窃听者无法恢复出原始信息 $x_i=\vec{x_i}'$。推导过程如式(39)所示：

$$Pr(x_i=\vec{x_i}\,|\,x_i'=\vec{x_i}')=Pr(x_i=\frac{\vec{x_i}'-kc_n}{t_i})$$
$$=Pr(x_i=\vec{x_i}) \tag{39}$$

以上的分析证明，本文基于混沌序列的安全网络编码算法在面对唯密文攻击时能够保证信息的安全，窃听者即使截获了全部的加密数据消息，也无法解码成功。

已知明文攻击的安全性能分析：在本文中，已知明文攻击是指窃听者通过窃听知道了一段信源消息 x_i 以及该段信源消息加密后的密文 x_i'。当然，窃听者依然拥有全局窃听的能力，这样其窃听到的就不只是某段原始消息加密后的密文，而有可能窃听到全部密文。已知原始消息与加密后消息的关系如式(40)所示：

$$x_i'=t_i\cdot x_i+k\cdot c_n \tag{40}$$

通过式(40)可以看出：即使窃听者截获了一段明文，同时已知一段密文甚至全部密文，其也无法成功破译出全部原始信息，因为仍然有 3 个参数 t_i，k，c_n 是无法确定的。这样一来，窃听者依然无法通过所截获的部分原始消息来破译出全部原始数据。因此，所提方案在面对已知明文攻击时能够保证数据消息的安全。

接下来讨论最糟糕的情况，即窃听者不仅得到了原始消息加密后的一维数据，还知道了加密一维消息的所有参数。也就是说，窃听者截获了 c_n，也知道了随机数 k，通过关系式 $x_i'-k\cdot c_n=t_i\cdot x_i$，就可得到 t_ix_i 的值，t_ix_i 表示原始消息其他维数据的 t_i 倍。但是，定理 1 已经证明全局编码矩阵中的数值相对于窃听者而言是相互独立的，因此窃听者除了用穷举法之外，无法推断出 t_i 的取值。这样一来，信源消息依然不会被截获。

4.4 仿真分析

为了验证安全网络编码方案的有效性，分别对文本和图片进行加密/解密仿真操作，并利用 Matlab 来实现所提加密方案。仿真时，首先利用所提安全网络编码方案对文件进行加密处理，然后对加密后的文件进行解密操作，正确的加密操作是利用密钥进行解密，最后模仿窃听者在不知道全部密钥的情况下试图对文件进行解密操作。

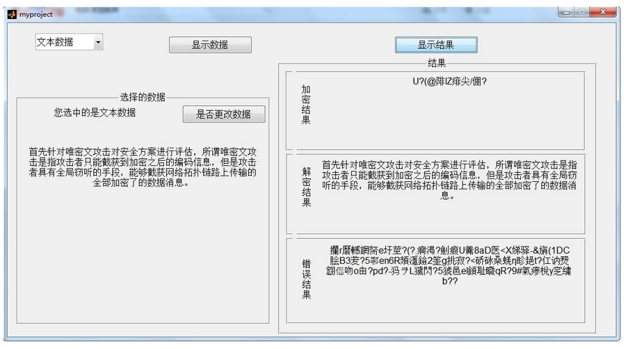

图 5 加密解密仿真结果 1

Fig. 5 Simulation result 1 of encryption and decryption

图 6 加密解密仿真结果 2

Fig. 6 Simulation results 2 of encryption and decryption

5 性能对比分析

5.1 传输成功率的对比

本方案的单次传输成功率相比文献[17]的方案有了明显的提高，单次传输成功率达到了 1，而文献[17]中方案的成功率为 $2(b_0)^2$。

文献[17]中接收端双对辅助粒子进行测量，若测量结果为 $|0\rangle_{B_i}$，则表明发送成功；若测量结果为 $|1\rangle_{B_i}$，则说明发送失败。由此可计算出接收端 B 恢复出初始态 $|\varphi_i\rangle$ 的概率为：

$$4\times\left(\frac{b_0}{\sqrt{2}}\right)^2=2b_0^2 \tag{41}$$

本方案采取量子 GHZ 态进行传输，其中 b_0 的取值为 $\left(\frac{1}{\sqrt{2}}\right)$，因此本方案接收端 B 恢复出初始态 $|\varphi_i\rangle$ 的概率为 1。

5.2 编码效率的对比

文献[14]中方案的中间编码信道需要传输 13 个经典比特才能实现 1 个量子信息的交叉传输，且成功传输的概率尚不足 1，这对该方案的编码效率造成了一定的影响。相比 Ma 方案中需要进行 13 个经典比特的传输，文献[17]中的方案需要 10 个经典比特的传输，在编码效率上有了一定的提升。本方案只需在中间编码信道进行 6 个量子比特的传输，即可完成量子信息在蝶形网络中的交叉传输过程。对比结果如图 7 所示。

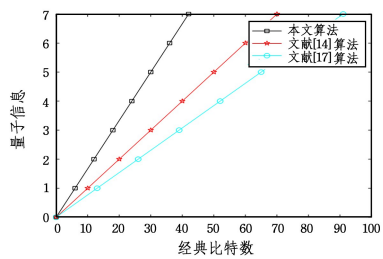

图 7 编码效率对比

Fig. 7 Comparison of coding efficiency

5.3 安全性对比

文献[14]和文献[17]中的方案并未考虑编码信道的安全性问题，不能有效地防范攻击者的窃听行为，从而不能保障量子比特信息的传输安全。本方案针对中间编码信道的特性设计了安全保障方案，使得窃听者很容易被检测到，因此能够有效地防范攻击者对编码信息的窃取行为。对比结果如图 8 所示。

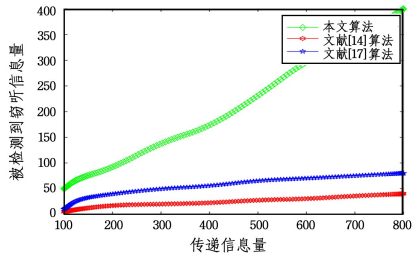

图 8　防窃听性能对比

Fig. 8　Comparison of anti-eavesdropping performance

结束语　本文针对信息传输的窃听问题，采用了一种基于三粒子纠缠 GHZ 辅助信道，利用量子的不可克隆原理和隐形传态技术完成了在经典蝶形网络中量子比特的无差别传输交叉。所提方案中采用的均是量子信道，与传统的量子网络编码相比实现了信道的一致，并且采用的是三粒子最大纠缠态进行操作，协助完成了网络编码操作。在辅助编码上，将辅助编码的粒子个数由两粒子的 Bell 态扩展到三粒子的 GHZ 态，在技术上实现了创新，并且在编码效率方面也有了很大幅度的提高。本方案的中间信道中只需要传输很少的量子比特就能够实现编码操作，而在解码的过程中采用了酉矩阵来进行量子比特的恢复。本文分析了中间信道的安全性，并利用量子直接通信技术对攻击者 Eve 进行检测，分析出 Eve 可被检测出的概率，证明了本文方案可以很好地防止信息在传输中被窃听的危险。

目前，针对量子网络编码的研究已经取得了不小的进展，但相比传统的经典网络编码来说还有着很大的进步空间，尤其是在网络编码安全方面。未来，针对量子网络编码安全问题有着以下规划：1）传统密码研究在量子密码中的对应，如与数字签名相对应的量子签名，与公钥密码相对应的量子公钥密码等；2）量子特性所带来的新应用，如对量子信息进行加密，使用量子态进行信息的量子安全直接通信，以及在量子通信网络构建中所独有的量子中继技术等；3）此外，网络编码的优化问题也是今后研究的方向。

参 考 文 献

[1] AHLSWEDE R，CAI N，LI S Y R，et al. Network information flow [J]. IEEE Transactions on Information Theory，2000，6(4)：1204-1216.

[2] MEI M D. Research on secure network coding [D]. Nanjing：Nanjing University of Posts and Telecommunications，2018.

[3] NGUYEN H V，BABAR Z，ALANIS D，et al. Towards the Quantum Internet：Generalised Quantum Network Coding for Large-scale Quantum Communication Networks[J]. IEEE Access，2017，PP(99)：17288-17308.

[4] GULATI M，SIDDHARTHA S，VEDI Y，et al. Genet-ic-Algorithm Based Planar Antenna Design[C]// International Conference on Wireless Communications，ignal Processing and Networking (WiSPNET). 2018：1-2.

[5] AKIBUE S，MURAO M. Network Coding for Distributed Quantum Computation Over Cluster and Butterfly Networks[J]. IEEE Transactions on Information Theory，2016，62(11)：6620-6637.

[6] JIANG M，ZHOU S，DING M X. Quantum network coding based on remote state preparation of arbitrary two-qubit states [C]// 2017 36th Chinese Control Conference (CCC). 2017：9757-9760.

[7] BENNETT C H，BRASSARD G，REPEAU C，et al. Teleportaion an Un known Quantum State oia Dual Claasical and EPR [J]. Physical Review Letters，1993，7(13)：1895-1899.

[8] QI S，ZHENG H，QIAOYAN W，et al. Quantum blind signature based on Two-State Vector Formalism[J]. Optics Communications，2010，283(21)：4408-4410.

[9] NISHIMURA H. Quantum Network Coding-How can network coding he applied to quantum information? [C]// 2013 International Symposium on Network Coding (NetCod). 2013：1-5.

[10] DURKOVIC S，CICA Z. Load balanced Birkhoff-von Neumann switch with output congestion detection[C]// 2017 13th International Conference on Advanced Technologies，Systems and Services in Telecommunications (TELSIKS). 2017：283-286.

[11] HAYASHI M，IWAMA K. Quantum network coding [M]// Thomas W，Weil P，eds. STACS 2007. Berlin：Springer，2007.

[12] LIU G J. An efficient security network coding scheme for anti-eavesdropping and anti-pollution [J]. Electronic Design Engineering，2008，7(26)：21-26.

[13] LEUNG D，OPPENHEIM J，WINTER A. Quantum Network Communication—The Butterfly and Beyond[J]. IEEE Transactions on Information Theory，2010，56(7)：3478-3490.

[14] MA S Y，CHEN X B，LUO M X. Probabilistic quantum network coding of M qubit states over the butterfly network[J]. Optics Communications，2010，283(3)：497-501.

[15] LIU G，LIU B，LIU X，et al. Low-complexity secure network coding against wiretapping using intra/inter-generation coding [J]. China Communications，2015，12(6)：116-125.

[16] PIRANDOLA S，EISERT J，WEEDBROOK C，et al. Advances in quantum teleportation[J]. Nature Photonics，2015，9(10)：641-652.

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

[18] INAMORI H，RALLAN L，VEDRAL V. Security of EPR-based Quantum Cryptography against Incoherent Symmetric Attacks [J]. Journal of Physics A General Physics，2001，34(35)：6913-6918.

[19] MICHAEL A，ISAAC L. quantum computation and quantum information [M]. Beijing：Tsinghua University Press，2004：65-66.

[20] HEN H，ZHANG J，ZHANG C. Chaos Updating Rotated Gates Quantum-inspired Genetic Algorithm [C]// International Conference on Communicattions，Circuits and Systems. 2004：1108-1112.

XU Guang-xian，born in 1977，Ph.D candidate，professor. His main research interests include network code and information processing.