物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

噪声情况下的量子网络直接通信

马鸿洋　秦国卿　范兴奎　初鹏程

Quantum network direct communication protocol over noisy channel

Ma Hong-Yang　Qin Guo-Qing　Fan Xing-Kui　Chu Peng-Cheng

引用信息 Citation: Acta Physica Sinica, 64, 160306 (2015)　DOI: 10.7498/aps.64.160306
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.160306
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I16

专题: 量子精密计量与操控

噪声情况下的量子网络直接通信*

马鸿洋[1)†] 秦国卿[2)] 范兴奎[1)] 初鹏程[1)]

1) (青岛理工大学理学院, 青岛 266033)

2) (清华大学物理系, 北京 100084)

(2015 年 4 月 28 日收到; 2015 年 5 月 25 日收到修改稿)

提出和研究了噪声情况下的量子网络直接通信. 通信过程中所有量子节点共享多粒子 Greenberger-Horne-Zeilinger (GHZ) 量子纠缠态; 发送节点将手中共享的 GHZ 态的粒子作为控制比特、传输秘密信息的粒子作为目标比特, 应用控制非门 (CNOT) 操作; 每个接收节点将手中共享 GHZ 态的粒子作为控制比特、接收到的秘密信息粒子作为目标比特, 再次应用 CNOT 门操作从而获得含误码的秘密信息. 每个接收节点从秘密信息中提取部分作为检测比特串, 并将剩余的秘密信息应用奇偶校验矩阵纠正其中存在的比特翻转错误, 所有接收节点获得纠正后的秘密信息. 对协议安全、吞吐效率、通信效率等进行了分析和讨论.

关键词: 噪声, 量子安全直接通信, 量子网络, 量子纠错码

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud **DOI:** 10.7498/aps.64.160306

1 引 言

量子网络是由多个量子节点利用量子效应运行事先指定任务的分布式通信系统, 其中量子节点具备存储和运算量子信息的能力. 量子网络使用量子通信协议运行, 著名的通信协议有 Bennett 和 Brassard 的利用四个量子态的 BB84 协议 [1]、Ekert 的利用 EPR 纠缠态的 E91 通信协议 [2]、Bennett 的利用两个非正交量子态的 B92 通信协议 [3]. 这三个协议是一个发送节点对一个接收节点的量子通信协议; 随着量子网络通信需求的提升, 多个发送节点对多个接收节点的量子通信协议的研究得到发展 [4]. 例如, Yan 和 Gao [5] 提出了在特定量子网络中的多个量子节点之间的通信协议. Ma 等 [6] 提出了利用中心节点作为桥联接的多个量子节点通信协议. 文献 [7—22] 研究了多个量子节点的通信协议.

量子安全直接通信 (QSDC) 的安全性是基于量子信息的非定域关联性、不可克隆、测不准等理论, 利用该种通信方式的一对一或者多对多的量子节点不需要预先生成密钥, 而是使用量子信道直接传输秘密信息. 2000 年, Long 和 Liu [23] 提出第一个两粒子 Bell 态的高效量子安全直接通信协议; 2002 年, Boström 和 Felbinger [24] 提出利用纠缠对的确定性量子通信方案; 2003 年, Deng 等 [25] 提出利用 Bell 态的两步安全直接编码通信协议; 2004 年, Deng 和 Long [26] 提出了基于单光子的量子一次便笺方案 (或 DL04) 方案; 2005 年, Wang 等 [27] 提出高维两步量子安全直接通信协议; 2006 年, Li 等 [28] 提出利用 Einstein-Podolsky-Rosen (EPR) 纠缠的两步量子网络安全直接通信协议; 同年, Deng 等 [29] 提出利用 EPR 纠缠的双向量子安全通信协议; 2007 年, Wen 和 Long [30] 提出单方量子纠错的量子安全通信协议; 2014 年, Zhou 等 [31] 提出单光子无信息泄露的量子对话协议. 多个研究组在该方向开展了深入研究 [32−38]. 2015 年, 山西大学 Hu 等 [38] 首次在国际上实现单光子 DL04 量子

* 国家自然科学基金 (批准号: 61173056, 11304174) 资助的课题.

† 通信作者. E-mail: hongyang_ma@aliyun.com

安全直接通信.

在实际通信环境中存在信道噪声、非理想信号源、误差操作等客观问题, 为了实现安全量子通信需从多个方面努力. 例如, 优化量子控制消除噪声[39,40]、制备高纯度纠缠源[41]、浓缩方法提高纠缠源纠缠度[42]、私密放大方法避免部分信息泄露[43,44]. 在更一般的情况下, 量子纠错码[45]进行编码纠正某种类型的量子错误.

本文研究噪声情况下量子网络直接通信协议, 该协议基于文献[37]的量子汇报协议, 量子汇报协议采用了文献[7]中的量子信道加密技术. 在通信协议中, $1+N$ 个量子节点分享多粒子Greenberger-Horne-Zeilinger (GHZ)量子纠缠态, 其中一个量子节点是发送节点, 具有特权, 是老板, 其他 N 个量子节点是接收节点, 是用户. 发送节点以手中的GHZ粒子作为控制比特, 对自己的通信粒子进行控制非门(control NOT gate, CNOT)操作, 然后将通信粒子传给接收节点; 接收节点再以自己手中的粒子作为控制比特、对发送节点传输过来的粒子, 进行CNOT操作从而读出发送节点传输过来的秘密信息. 接收节点对接收的秘密信息进行检测, 判定是否存在Eve窃听, 并对秘密信息利用量子CSS码纠正比特翻转错误. 在本文工作中, 我们首先将该协议推广使得共享GHZ态的 $1+N$ 个量子节点地位平等, 它们之间任意两者之间都可以进行直接通信; 其次, 该协议考虑噪声环境, 利用量子纠错编码使该协议能在有噪声的环境下工作.

2 相关理论基础

2.1 量子CNOT门

在本协议中多个量子节点之间需要使用CNOT门. 该量子门包含两个量子比特(控制比特 $|x\rangle$ 与目标比特 $|y\rangle$), 其特性: 当 $|x\rangle$ 为 $|0\rangle$ 时, 它不改变 $|y\rangle$ 的状态; 当 $|x\rangle$ 为 $|1\rangle$ 时, 它将翻转 $|y\rangle$ 的状态; 其表达式:

$$\mathrm{CNOT}(|x\rangle|y\rangle)=|x\rangle|x\oplus y\rangle, \tag{1}$$

其中 $x,y\in\{0,1\}$. 用矩阵表示为

$$\mathrm{CNOT}=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}.$$

2.2 量子纠错码

量子纠错码是具备纠正量子态错误能力的量子码, 其中包括CSS量子码、稳定子量子码、Turbo量子码等. 针对本通信协议涉及信道噪声所产生的量子态误码是比特翻转错误, 需要使用CSS量子码. CSS量子码是由两个线性编码 C_1 与 C_2 构成, C_1 与 C_2 映射至Hilbert空间, 采用一定的编码规范纠正 $t\leqslant t_0$ 位的比特翻转和相位翻转错误. 其表达式:

$$|v+C_2\rangle=\frac{1}{2^{k_2/2}}\sum_{w\in C_2}|v+w\rangle, \tag{2}$$

其中, (2)式右边符合模2运算规则. $v\in C_1$; n 是 C_1, C_2 的总位数; k_1, k_2 是 C_1, C_2 的码元数目.

3 噪声情况下的量子网络直接通信

在该协议中的量子节点数为 $1+N$, 分别表示为 $S_0,S_1,\cdots,S_i,\cdots,S_N$ $(i=1,2,\cdots,N)$. S_0 是发送节点, S_i 是接收节点, 如图1. $1+N$ 个量子节点之间通信使用量子与经典信道, 其中, 量子信道使用纠缠态与量子门传输量子信息, 经典信道使用“0”, “1”比特传输经典信息.

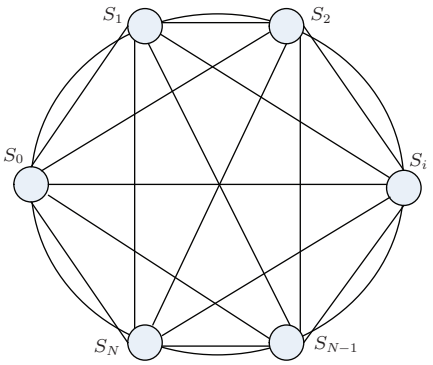

图1 可扩展的量子网络的架构

Fig. 1. The extensible quantum network architecture.

为研究讨论方便, 首先假设 $N=2$, 如图2, 对于多个量子节点的情况, 其通信过程与 $N=2$ 相同.

步骤1 初始化阶段

S_0, S_1, S_2 共享 $2n+\delta$ 个GHZ态, 表达式为

$$|\varphi\rangle^m_{S_0S_1S_2}=\frac{1}{\sqrt{2}}\left(|000\rangle_{\gamma_0\gamma_1\gamma_2}+|111\rangle_{\gamma_0\gamma_1\gamma_2}\right), \tag{3}$$

其中 S_0, S_1, S_2 分别对应粒子 γ_0, γ_1, γ_2, m 表示第 m 个纠缠态, $m=1,2,\cdots,2n+\delta$.

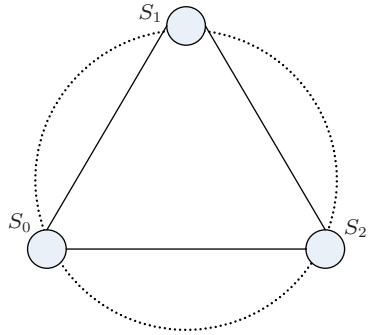

图 2 简化的扩展量子网络的架构

Fig. 2. The simplified quantum network architecture.

步骤 2 发送节点通信阶段

S_0 与 S_1 进行直接通信, 目的是传输 n 位比特的秘密信息串, 记为 Δ_1. 为了检测 Eve 和消除信道噪声, S_0 实际是需要制备 $2n+\delta$ 位的秘密信息串, 记为 ρ_0, 其生成方式为: 从集合 $\{0,1\}$ 中随机选取 n 位的经典比特, 作为检测比特串, 记做 Δ_2, Δ_2 的长度为 n, 将 Δ_1 随机地插入 Δ_2, 构建成 ρ_0, 即

$$\rho_0 = \{\rho_{01}, \rho_{02}, \cdots, \rho_{0(2n+\delta)}\},$$

其中 $\rho_{0j} \in \{0,1\}$, $j \in \{1,2,\cdots,2n+\delta\}$. S_0 使用量子比特 γ 承载经典信息, 当承载的经典信息为“0”时, γ 对应的量子态 $|\psi\rangle = |0\rangle$; 反之, γ 的量子态为 $|\psi\rangle = |1\rangle$. 对于 ρ_0 和相应发送的量子态只有 S_0 自己掌握, 其他量子节点无法获取相关信息. S_0 依次选取纠缠态 $|\varphi\rangle^m_{S_0S_1S_2}$ 中的粒子 γ_0 (每个 GHZ 态只使用一次) 与 γ, 应用 CNOT 门, 其中粒子 γ_0 是控制比特, γ 是目标比特, 其操作表示如下:

$$\begin{aligned}&\mathrm{CNOT}\left\{\left[\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)\right]\otimes|0\rangle\right\}_{\gamma_0\gamma_1\gamma_2\gamma}\\ =&\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)_{\gamma_0\gamma_1\gamma_2\gamma}, \qquad (4)\\ &\mathrm{CNOT}\left\{\left[\frac{1}{\sqrt{2}}(|000\rangle+|111\rangle)\right]\otimes|1\rangle\right\}_{\gamma_0\gamma_1\gamma_2\gamma}\\ =&\frac{1}{\sqrt{2}}(|0001\rangle+|1110\rangle)_{\gamma_0\gamma_1\gamma_2\gamma}, \qquad (5)\end{aligned}$$

然后将粒子 γ 发送给节点 S_1.

步骤 3 接收节点通信阶段

接收节点 S_1 对其共享的粒子 γ_1 与 γ, 应用 CNOT 门, 其中粒子 γ_1 是控制比特, γ 是目标比特, 其操作表示如下:

$$\begin{aligned}&\mathrm{CNOT}\left[\frac{1}{\sqrt{2}}(|0000\rangle+|1111\rangle)\right]_{\gamma_0\gamma_1\gamma_2\gamma}\\ =&\frac{1}{\sqrt{2}}(|0000\rangle+|1110\rangle)_{\gamma_0\gamma_1\gamma_2\gamma}\\ =&\frac{1}{\sqrt{2}}(|000\rangle_{\gamma_0\gamma_1\gamma_2}+|111\rangle_{\gamma_0\gamma_1\gamma_2})|0\rangle_\gamma, \qquad (6)\\ &\mathrm{CNOT}\left[\frac{1}{\sqrt{2}}(|0001\rangle+|1110\rangle)\right]_{\gamma_0\gamma_1\gamma_2\gamma}\\ =&\frac{1}{\sqrt{2}}(|0001\rangle+|1111\rangle)_{\gamma_0\gamma_1\gamma_2\gamma}\\ =&\frac{1}{\sqrt{2}}(|000\rangle_{\gamma_0\gamma_1\gamma_2}+|111\rangle_{\gamma_0\gamma_1\gamma_2})|1\rangle_\gamma. \qquad (7)\end{aligned}$$

S_1 通过 (6) 与 (7) 式可获得发送节点发送的量子态. S_1 获得量子态后, 向 S_0 返回数据确认帧 (acknowledgement frame, ACK). 这样, S_0 与 S_1 之间依次重复步骤 2 与步骤 3, 将 $2n+\delta$ 量子态传输完毕, $|0\rangle$ 与 $|1\rangle$ 分别表示编码“0”, “1”, 与经典信息对应编码生成 $2n+\delta$ 位的秘密信息串, 记为 ρ_1, 即

$$\rho_1 = \{\rho_{11}, \rho_{12}, \cdots, \rho_{1(2n+\delta)}\},$$

其中 $\rho_{1j} \in \{0,1\}$, $j \in \{1,2,\cdots,2n+\delta\}$. 注意因为存在 Eve 和信道噪声, ρ_1 与 ρ_0 是不一样的. 同时, S_0 与 S_2 进行直接通信, 操作如步骤 2 与步骤 3, 生成 $2n+\delta$ 位的秘密信息串, 记为 ρ_2, 即

$$\rho_2 = \{\rho_{21}, \rho_{22}, \cdots, \rho_{2(2n+\delta)}\},$$

其中 $\rho_{2j} \in \{0,1\}$, $j \in \{1,2,\cdots,2n+\delta\}$. 还是因为存在 Eve 和信道噪声, ρ_2, ρ_1, ρ_0 也是不一样的. 而且, 在该通信协议中, S_0, S_1, S_2 三者的地位实际上是相等的, 同样的通信过程适用于任意两个量子节点. 在协议中, 步骤 1 和 2 没有经典信息的传递, 发送节点实现量子比特传输以后, S_1, S_2 利用 CNOT 直接读出发送节点拟要传输的秘密信息. 当然, 为了防止 S_1, S_2 无限制地等待下一个量子态, 本通信协议增加了 ACK 部分.

步骤 4 检测阶段

在共享了 $2n+\delta$ 位的秘密信息串后, S_0 在经典信道中公开 Δ_2. 依据 Δ_2, S_1 对照自己手中的 ρ_1 中的检测比特位置, 与 Δ_2 一一比对, 计算其误码数目 t_1, 如果 $t_1 \leqslant t_0$, 则进行下一步, 否则, 认为存在 Eve 或者信道噪声过大, 终止该通信过程. 同时, S_2 也进行同样操作, 将自己手中的 ρ_2 中的检测比特位与 Δ_2 一一比对, 计算其误码数目 t_2.

步骤 5 纠错阶段

S_1 与 S_2 将剩余的 $n+\delta$ 位秘密信息串, 分别记为 v_1 与 v_2, 一般情况下假设是第 i 个量子节点, 对应的比特串记为 v_i, 对应的量子态写为 $|v_i + C_2\rangle$.

根据 (2) 式可知,

$$|v_i + C_2\rangle = \frac{1}{2^{k_2/2}} \sum_{w \in C_2} |v_i + w\rangle, \tag{8}$$

针对一般情况下信道噪声引起的比特翻转错误和相位翻转错误, CCS 量子码能够准确指出错误位并能有序纠正错误. 而本协议中对应的量子态, 只存在比特翻转错误, 用 e_i 表述. 因存在 e_i, 所以 (8) 式变形为

$$\frac{1}{2^{k_2/2}} \sum_{w \in C_2} (-1)|v_i + w + e_i\rangle. \tag{9}$$

利用经典信道通信, S_1 选用 $\boldsymbol{H}_1$, 将 (9) 式中的 $v_i + w + e_i$ 与 $\boldsymbol{H}_1$ 相乘, 其中 $\boldsymbol{H}_1$ 是 C_1 的奇偶校验矩阵.

$$(v_i + w + e_i)\boldsymbol{H}_1 = e_i\boldsymbol{H}_1, \tag{10}$$

根据 $e_i\boldsymbol{H}_1$ 可算出存在比特反转错误的位置, 随之反转就可得到正确的量子比特, 从而获得秘密信息串 Δ_1. 从步骤 4 和 5 可知, 该协议通信过程除了检测与纠错阶段, 其他阶段不需要交换额外经典信息. 另外, 在本通信协议过程中, 因 S_0, S_1, S_2 之间编码的特点, Eve 或信道噪声所引起的量子态的错误只存在比特翻转错误, 而不会存在相位翻转错误, 所以该通信协议的纠错比一般的量子纠错要简单.

4 扩展到多量子节点的量子汇报

在上述通信过程中, 量子节点 $N = 2$. 这个协议可以扩展到量子节点 $N \geqslant 3$ 的情况. 这时 N 个量子节点所分享的最大纠缠态为

$$|\varphi\rangle_{S_0 \cdots S_N} = \frac{1}{\sqrt{2}} \left(|00\cdots0\rangle_{\gamma_0 \cdots \gamma_N} + |11\cdots1\rangle_{\gamma_0 \cdots \gamma_N}\right), \tag{11}$$

其通信方案与 $N = 2$ 相同. 并且, 任意两个量子节点都可以根据上面的方案进行通信.

5 协议安全、吞吐效率、通信效率分析

5.1 协议安全分析

1) 考虑 S_0, S_1, S_2 三者构成 GHZ 态, 表达式如下:

$$|\phi\rangle = \frac{1}{\sqrt{2}} \left(|000\rangle_{\gamma_0\gamma_1\gamma_2} + |111\rangle_{\gamma_0\gamma_1\gamma_2}\right).$$

S_0 使用粒子 γ_0 作为控制比特、γ 作为目标比特进行 CNOT 操作, 再考虑 S_1 使用的粒子 γ_1, S_2 使用的粒子 γ_2, 共计四个粒子. 该四个粒子共享 GHZ 态的表达式如下:

$$|\Psi\rangle = \frac{1}{2} \left(|0000\rangle + |1111\rangle\right)_{\gamma_0\gamma_1\gamma_2\gamma}.$$

为讨论方便, 这里只选取 $|\psi\rangle = |0\rangle$ 的情况. S_1 和 S_2 在接收秘密信息的时候, 分别以 γ 作为目标比特进行 CNOT 操作, 获得正确的量子态

$$|\Psi\rangle = \frac{1}{2} \left(|000\rangle + |111\rangle\right) \otimes |0\rangle_{\gamma_0\gamma_1\gamma_2\gamma}.$$

为检测是否存在 Eve, S_0, S_1, S_2 需要用旋转矩阵进行三边变换, 其旋转矩阵表达式为

$$\boldsymbol{R}(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

如果 Eve 对此传输信息过程窃听成功, 以 γ 作为控制变量, 对自己的量子态做 CNOT, 把 γ 的信息传递给 S_1, S_2, 这样使 S_0, S_1, S_2 和 Eve 四者形成了纠缠. 然而, Eve 不知道自己截获的态的具体信息 (只能取得上一次截获的信息的取值), 也无法确定自己与哪一个态进行了纠缠, 所以为了检测信息是否被窃听, S_0, S_1, S_2 要做三边旋转 (在 S_0 做 CNOT 之前). 如果 Eve 没有窃听到信息的话, $|\phi\rangle$ 以及所传递的信息都不会发生变化, 得到正确信息的量子态为

$$\begin{aligned} &|\Psi\rangle_{\gamma_0\gamma_1\gamma_2\gamma} \\ =& \frac{1}{\sqrt{2}} \big(\cos^3\theta|0000\rangle - \sin\theta\cos^2\theta|1001\rangle \\ &+ \sin^2\theta\cos\theta|1101\rangle - \sin\theta\cos^2\theta|0100\rangle \\ &+ \sin^2\theta\cos\theta|1001\rangle - \sin\theta\cos^2\theta|0000\rangle \\ &- \sin^3\theta|1101\rangle - \sin^2\theta\cos\theta|0100\rangle \\ &+ \cos^3\theta|1111\rangle + \sin\theta\cos^2\theta|1101\rangle \\ &+ \sin^2\theta\cos\theta|0100\rangle + \sin\theta\cos^2\theta|0110\rangle \\ &+ \sin^2\theta\cos\theta|1001\rangle + \sin\theta\cos^2\theta|1011\rangle \\ &+ \sin^3\theta|0000\rangle + \sin^2\theta\cos\theta|0010\rangle \big). \end{aligned} \tag{12}$$

当 $\theta = \pi/2$, (12) 式变为 $|\Psi\rangle_{\gamma_0\gamma_1\gamma_2\gamma} = \frac{1}{\sqrt{2}} \left(|0000\rangle - |1101\rangle\right)$.

若存在 Eve 窃听, 则变换后的量子态为

$$\begin{aligned} &|\Psi\rangle_{\mathrm{ABCE}} \\ =& \frac{1}{\sqrt{2}} \big(\cos^3\theta|0000\rangle - \sin\theta\cos^2\theta|1000\rangle \end{aligned}$$

$$
\begin{aligned}
&+\sin^2\theta\cos\theta|1100\rangle-\sin\theta\cos^2\theta|0100\rangle\\
&+\sin^2\theta\cos\theta|1000\rangle-\sin\theta\cos^2\theta|0000\rangle\\
&-\sin^3\theta|1100\rangle-\sin^2\theta\cos\theta|0100\rangle\\
&+\cos^3\theta|1111\rangle+\sin\theta\cos^2\theta|1101\rangle\\
&+\sin^2\theta\cos\theta|0101\rangle+\sin\theta\cos^2\theta|0111\rangle\\
&+\sin^2\theta\cos\theta|1001\rangle+\sin\theta\cos^2\theta|1011\rangle\\
&+\sin^3\theta|0001\rangle+\sin^2\theta\cos\theta|0011\rangle\big). \qquad (13)
\end{aligned}
$$

当 $\theta=\pi/2$, (13) 式变为 $|\Psi\rangle_{\gamma_0\gamma_1\gamma_2\gamma}=\frac{1}{\sqrt{2}}(|0001\rangle-|1100\rangle)$. 所以, S_1, S_2 根据旋转矩阵中选取角度, 根据该角度计算得到的不同量子态, 可以确定是否存在窃听.

2) 该部分在量子节点的数目在 $N=2$ 的情况下进行讨论, 其结论适用于多个量子节点的情况. S_1, S_2 接收的量子态位均为 $n+\delta$, 为了讨论方便 δ 忽略不计, 所以, S_1, S_2 联合共计的量子位的总位数是 $2n$. 根据文献 [22] 可知, S_1, S_2 表达式等价带两个参数 x 与 z 的 $\mathrm{CSS}_{x,z}(C_1,C_2)$:

$$
|v_1+C_2\rangle=\frac{1}{2^{k_2/2}}\sum_{w\in C_2}(-1)^{z\cdot w}|x+v_1+w\rangle, \qquad (14)
$$

$$
|v_2+C_2\rangle=\frac{1}{2^{k_2/2}}\sum_{w\in C_2}(-1)^{z\cdot w}|x+v_2+w\rangle, \qquad (15)
$$

根据文献 [21] 可知, S_1, S_2 的混合态表达式为

$$
\frac{1}{2^n2^{k_2/2}}\sum_{z\in F_n^2}\Big[\sum_{w_1,w_2\in C_2}(-1)^{(w_1+w_2)z}|x+v_1+w\rangle\langle x+v_1+w|\Big], \qquad (16)
$$

$$
\frac{1}{2^n2^{k_2/2}}\sum_{z\in F_n^2}\Big[\sum_{w_1,w_2\in C_2}(-1)^{(w_1+w_2)z}|x+v_2+w\rangle\langle x+v_2+w|\Big], \qquad (17)
$$

根据 (16), (17) 式, S_1, S_2 的联合混合态表达式为

$$
\begin{aligned}
&\frac{1}{2^n2^{k_2/2}}\sum_{z\in F_n^2}\Big(\sum_{w_1,w_2\in C_2}(-1)^{(w_1+w_2)z}|x+v_1+w\rangle|x+v_2+w\rangle\langle x+v_1+w|\langle x+v_2+w|\Big)\\
=&\frac{1}{2^{k_2/2}}\sum_{w\in C_2}|x+v_1+w\rangle|x+v_2+w\rangle\langle x+v_1+w|\langle x+v_2+w|, \qquad (18)
\end{aligned}
$$

(18) 式等价于 S_1, S_2 分别发送随机选取的 x 和 z 所确定的 CSS 码字. S_0 根据 x 和 z, 从而确定 $v_i\in C_1$ 的选择, 纠正其产生的比特翻转错误.

5.2 吞吐效率分析

吞吐效率 η (throughput efficiency) 是描述经典通信系统性能的重要参数, 其定义为在单位时间内被成功接收的信息位数与发送信息位数的比值. 本文参照该定义, 计算通信协议的吞吐效率.

在本协议中 S_0 与各节点之间共享 GHZ 纠缠态、随机选取 $n+\delta$ 位的比特均为检测比特串, 并将其与 n 位比特的密钥信息串混合. 发送节点 S_0 应用 CNOT 门的时间为 t_{CNOT_0}, 不同量子节点应用 CNOT 门的时间是不一样的, 各个节点所应用 CNOT 门的时间表示为 t_{CNOT_i}, 为了计算方便, 选取 t_{CNOT_i} 的最大值, 即为 $t_{\mathrm{CNOT}}=\max\{t_{\mathrm{CNOT}_i}\}$, $i=1,2,\cdots,N$. 接收节点 S_i 返回数据确认帧 ACK 的通信时延为 t_{ACK}. 发送节点 S_0 发送 $2n+\delta$ 所用的时间 T_1:

$$
T_1=t_{\mathrm{CNOT}_0}+t_{\mathrm{CNOT}}+t_{\mathrm{ACK}}.
$$

接收节点 S_i 取 n 位检查信道的安全性, 利用纠错码获得 $n+\delta$ 位的秘密信息, 由于利用纠错码纠错不涉及通信的时间, 可忽略不计.

所以, 该协议的吞吐效率为

$$
\begin{aligned}
\eta&=\frac{n+\delta}{T_1}\\
&=\frac{n+\delta}{(t_{\mathrm{CNOT}_0}+t_{\mathrm{CNOT}}+t_{\mathrm{ACK}})(2n+\delta)}. \qquad (19)
\end{aligned}
$$

根据协议情况 $\delta\to 0$, (19) 式简化为

$$
\eta=\frac{1}{2(t_{\mathrm{CNOT}_0}+t_{\mathrm{CNOT}}+t_{\mathrm{ACK}})}. \qquad (20)
$$

因此, 提高本协议通信的吞吐效率, 需要提高 CNOT 门的处理时间和确认帧 ACK 的通信时延.

5.3 通信效率分析

在本通信协议中, 在不考虑重传和数据丢失的情况下, 发送节点 S_0 实际传输的秘密信息串的位

数是$2n+\delta$, 在完成检测和纠错过程后, 获得正确的秘密信息串的位数是$n+\delta$, 所以该协议的通信效率为

$$\Gamma = \frac{n+\delta}{2n+\delta} \approx \frac{1}{2}. \tag{21}$$

而在噪声条件下, 基于CCS 码的BB84协议[22], 发送端拟发送的量子位是$4n+\delta$, 其丢弃测量基不同的量子位就损耗一半, 再剩余的一半用于纠错, 其效率为1/4. 所以, 根据(21)式可知, 在考虑噪声的情况下本协议有较高通信效率.

6 结束语

本文提出噪声情况下量子网络直接通信协议, 该协议中任意两点都可以作为发送节点和接收节点, 发送节点、接收节点依次分别使用CNOT门, 传输并生成$2n+\delta$的秘密信息; 在$2n+\delta$中提取n位用于检测是否存在Eve; 对于$n+\delta$应用奇偶校验矩阵纠正其中存在的误码; 所有量子节点从而获得共享的$n+\delta$位秘密信息. 并对协议安全、吞吐效率、通信性能等方面进行分析. 该协议的优点是噪声情况的量子网络之间通信, 但是该噪声情况限定在只能引起秘密信息的误码的范围, 并且秘密信息不能丢失. 而在更一般的网络通信中的确存在秘密信息的丢失的问题, 对于这一问题的较好解决也是下一步需要考虑的.

参考文献

[1] Bennett C H, Brassard G 1984 *Proceedings of IEEE International Conference on Computers, System and Signal Processing* Bangalore, India, December 1984 pp75–179

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[4] Zhou N R, Cheng H L, Tao X Y, Gong L H 2014 *Quantum Inf. Process* **13** 513

[5] Yan F L, Gao T 2005 *Phys. Rev. A* **72** 012304

[6] Ma H, Chen B, Guo Z, Li H 2008 *Can. J. Phys.* **86** 1097

[7] Zhang Y S, Li CF, Guo G C 2001 *Phys. Rev. A* **64** 024302

[8] Zhao Z, Chen Y A, Zhang A N, Yang T, Briegel H J, Pan J W 2004 *Nature* **430** 54

[9] Matsumoto R 2007 *Phys. Rev. A* **76** 62316

[10] Chen L B, Zheng C H, Ma H Y, Shan C J 2014 *Opt. Commun.* **328** 73

[11] Guo B H, Yang L, Xiang C, Guan C, Wu L A, Liu S H 2013 *Acta Phys. Sin.* **62** 130303 (in Chinese) [郭邦红, 杨理, 向憧, 关翀, 吴令安, 刘颂豪 2013 物理学报 **62** 130303]

[12] Chen L B, Yang W 2014 *Laser Phys. Lett.* **11** 105201

[13] Zhang P, Zhou X Q, Li Z W 2014 *Acta Phys. Sin.* **63** 130301 (in Chinese) [张沛, 周小清, 李智伟 2014 物理学报 **63** 130301]

[14] Qiu T H, Yang G J 2014 *Phys. Rev. A* **89** 052312

[15] Zhang C M, Song X T, Treeviriyanupab P, Li M, Wang C, Li H W, Han Z F 2014 *Chin. Sci. Bull.* **59** 2825

[16] Su X L 2014 *Chin. Sci. Bull.* **59** 1083

[17] Wang C, Guo H, Ren J, Cao Y, Peng C, Liu W 2014 *Sci. China: Phys. Mech. Astron.* **57** 1233

[18] Gao F, Fang W, Wen Q Y 2014 *Sci. China: Phys. Mech. Astron.* **57** 1244

[19] Gong L H, Song H C, He C S, Liu Y, Zhou N R 2014 *Phys. Scr.* **89** 035101

[20] Li C Y, Zhou H Y, Wang Y, Deng F G 2005 *Chin. Phys. Lett.* **22** 1049

[21] Sheng Y B, Zhou L, Cheng W W, Gong L Y, Wang L, Zhao S M 2013 *Chin. Phys. B* **22** 030314

[22] Shor P W, Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[23] Long G L, Liu X S 2002 *Phys. Rev. A* **65** 032302

[24] Boström K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 187902

[25] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 042317

[26] Deng F G, Long G L 2004 *Phys. Rev. A* **69** 052319

[27] Wang C, Deng F G, Li Y S, Liu X S, Long G L 2005 *Phys. Rev. A* **71** 044305

[28] Li X H, Zhou P, Liang Y J, Li C Y, Zhou H Y, Deng F G 2006 *Chin. Phys. Lett.* **23** 108

[29] Deng F G, Li X H, Li C Y, Zhou P, Zhou H Y 2006 *Phys. Lett. A* **359** 359

[30] Wen K, Long G L 2010 *Int. J. Quantum. Info.* **8** 697

[31] Zhou N R, Hua T X, Wu G T, He C S, Zhang Y 2014 *Intern. J. Theor. Phys.* **53** 3829

[32] Long G L, Deng F G, Wang C, Li X H, Wen K, Wang W Y 2007 *Front. Phys. China* **2** 251

[33] Chang Y, Xu C, Zhang S, Yan L 2014 *Chin. Sci. Bull.* **59** 2541

[34] Chang Y, Xu C, Zhang S, Yan L 2013 *Chin. Sci. Bull.* **58** 4571

[35] Zou X F, Qiu D W 2014 *Sci. China: Phys Mech. Astron.* **57** 1696

[36] Zheng C, Long G F 2014 *Sci. China: Phys. Mech. Astron.* **57** 1238

[37] Deng F G, Li X H, Li C Y, Zhou P, Liang Y J, Zhou H Y 2006 *Chin. Phys. Lett.* **23** 1676

[38] Hu J Y, Yu B, Jing M Y, Xiao L T, Jia S T 2015 arXiv:1503.00451

[39] Li S, Ma H Q, Wu L A, Zhai G J 2013 *Acta Phys. Sin.* **62** 084214 (in Chinese) [李申, 马海强, 吴令安, 翟光杰 2013 物理学报 **62** 084214]

[40] Jing J, Wu L A 2015 *Sci. Bull.* **60** 328

[41] Heilmann R, Gräfe M 2015 *Sci. Bull.* **60** 96

[42] Sheng Y B, Liu J Z, Sheng Y, Wang L, Zhou L 2014 *Chin. Phys. B* **23** 080305

[43] Deng F G, Long G L 2006 *Commun. Theor. Phys.* **46** 443

[44] Hao L, Wang C, Long G L 2010 *J. Phys. B: At. Mol. Opt. Phys.* **43** 125502

[45] Nebendahl V 2015 *Phys. Rev. A* **91** 022332

SPECIAL ISSUE — Quantum metrology and control

Quantum network direct communication protocol over noisy channel*

Ma Hong-Yang[1)†] Qin Guo-Qing[2)] Fan Xing-Kui[1)] Chu Peng-Cheng[1)]

1) (*School of Sciences, Qingdao Technological University, Qingdao 266033, China*)

2) (*Department of Physics, Tsinghua University, Beijing 100084, China*)

(Received 28 April 2015; revised manuscript received 25 May 2015)

Abstract

The direct communication protocol of quantum network over noisy channel is proposed and investigated in this study. In communication process, all quantum nodes share multiparticle Greenberger-Horne-Zeilinger (GHZ)-states. The sending node takes the GHZ-state particle in the hand as the control qubit and the particle for sending secret information as the target qubit, which carries out the CNOT gate operation for the control and target qubit. Each receiving node takes the GHZ-state particle in the hand as the control qubit and the particle of the received secret information as the target qubit, in which the CNOT gate operation is repeated to obtain the secret information that contains the bit error. Each receiving node uses the extracted part of qubits as the checking qubits, and then corrects the bit-flip errors using parity check matrix together with the rest part of qubits. As a result, all receiving nodes obtain rectified secret information. In addition to the high security analysis, this study also presents the detailed analyses of the throughput efficiency and the communication performance.

Keywords: noisy, quantum secure direct communication, quantum network, quantum error coding

PACS: 03.67.Hk, 03.67.Dd, 03.65.Ud **DOI:** 10.7498/aps.64.160306

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61173056, 11304174).

† Corresponding author. E-mail: hongyang_ma@aliyun.com