论文

基于集体噪声信道三量子比特纠缠态测量相关性的鲁棒量子对话

叶天语*

浙江工商大学信息与电子工程学院, 杭州 310018

*联系人, E-mail: happyty@aliyun.com

收稿日期: 2014-12-31; 接受日期: 2015-01-28; 网络出版日期: 2015-02-11

国家自然科学基金资助项目(批准号: 61402407, 11375152)

摘要 利用三量子比特纠缠态作为初始量子资源, 提出两个分别运行在集体退相位噪声信道和集体旋转噪声信道上的鲁棒量子对话(Quantum Dialogue, QD)协议. Alice 制备一系列三量子比特纠缠态, 将它们分成一个物理量子比特序列和一个逻辑量子比特序列, 然后将逻辑量子比特序列发送给 Bob. 接着, Alice 和 Bob 分别对物理量子比特序列和逻辑量子比特序列进行测量. 根据他的测量结果, Bob 制备新的没有测量过的逻辑量子比特序列, 并利用逻辑酉操作编码他的秘密消息. 接着, Bob 将编码的逻辑量子比特序列发送回 Alice. 最后, Alice 对编码的逻辑量子比特序列施加逻辑酉操作以编码她的秘密消息并公布她对其的测量结果. 这样, Alice 和 Bob 就能解码出彼此的秘密消息. 借助于三量子比特纠缠态的测量相关性, 两个参与者秘密地共享信息逻辑量子比特的初态. 这样, 信息泄露问题被克服. 所提出的协议只需要单光子测量. 与之前提出的可运行在集体噪声信道上的 QD 协议相比, 所提出的协议具有最高的信息论效率.

关键词 量子对话(Quantum Dialogue, QD), 集体退相位噪声, 集体旋转噪声, 测量相关性, 信息泄露

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

doi: 10.1360/SSPMA2014-00510

1 引言

众所周知, 量子安全直接通信(Quantum Secure Direct Communication, QSDC)的目标是通过量子信号的传输实现秘密消息的直接通信. 许多优秀的 QSDC 协议^[1-12]已经实现秘密消息从一个参与者到另一个参与者的单向通信. 显然, 秘密消息的双向通信更接近于实际对话. 如果秘密消息在两个参与者之

间的双向通信能够得到实现, 这将会更有益. 在 2004 年, Nguyen^[13]和 Zhang 等人^[14,15]分别独立提出量子对话(Quantum Dialogue, QD)这一新概念从而使得这一梦想成真. 从那时起, 许多研究者专注于从不同角度构造 QD 协议^[16-25]. 2008 年, Gao 等人^[26,27]发现, QD 中存在信息泄露安全漏洞. 与此同时, Tan 和 Cai^[28]发现, QD 中存在经典相关现象. Gao 等人^[26,27]以及 Tan 和 Cai^[28]的发现成功地改变了 QD 的研究焦

引用格式: 叶天语. 基于集体噪声信道三量子比特纠缠态测量相关性的鲁棒量子对话. 中国科学: 物理学 力学 天文学, 2015, 45: 050301
Ye T Y. Robust quantum dialogue based on the measurement correlation of three-qubit entangled states over collective noise channels (in Chinese). Sci Sin-Phys Mech Astron, 2015, 45: 050301, doi: 10.1360/SSPMA2014-00510

点. 换句话说, 研究者们开始将他们的注意力转向如何解决 QD 的信息泄露问题. 这样, 许多抗信息泄露的 QD 协议被设计出来^[29-41]. 在对上述抗信息泄露 QD 协议进行仔细观察后可以发现, 它们忽略了实际量子信道噪声的存在, 因而只能工作在一个理想信道. 文献[42,43]已经指出, 只要光子在一个比噪声源变化还快的时间窗里传输, 信道噪声就可以被建模为集体噪声. 主要有两种集体噪声, 分别是集体退相位噪声和集体旋转噪声. 由于无消相干(Decoherence-Free, DF)态^[42-55]具有抗集体噪声不变性, 它们已经成为一种对抗集体噪声的有效手段.

基于以上分析, 本文利用三量子比特纠缠态作为初始量子资源, 提出两个分别运行在集体退相位噪声信道和集体旋转噪声信道上的鲁棒 QD 协议. 借助于三量子比特纠缠态的测量相关性, 两个参与者秘密地共享信息逻辑量子比特(即两量子比特 DF 态)的初态. 这样, 信息泄露问题被克服. 所提出的协议只需要单光子测量. 与之前提出的可运行在集体噪声信道上的 QD 协议相比, 所提出的协议具有最高的信息论效率.

2 可运行在集体退相位噪声信道上的鲁棒 QD 协议

当光子的水平极化态 $|0\rangle$ 和垂直极化态 $|1\rangle$ 分别在集体退相位噪声信道上传输时, 前者总是被保持不变, 后者总是被改变为 $e^{i\varphi}|1\rangle$ ^[44], 其中 φ 是随时间变化的噪声参数. 可以直接得到两个逻辑量子比特, $|0_{dp}\rangle = |01\rangle$ 和 $|1_{dp}\rangle = |10\rangle$, 对这类噪声免疫^[44]. 它们的叠加态,

$$|\pm_{dp}\rangle = \frac{1}{\sqrt{2}}(|0_{dp}\rangle \pm |1_{dp}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle) = |\psi^\pm\rangle,$$

也总是不受这类噪声影响^[46]. $Z_{dp} = \{|0_{dp}\rangle, |1_{dp}\rangle\}$ 和 $X_{dp} = \{|+\rangle, |-\rangle\}$ 是这类噪声下的两个逻辑测量基. 显然, 有以下关系存在^[50]:

$$\begin{aligned} U_{dp}^0 |0_{dp}\rangle &= |0_{dp}\rangle, \quad U_{dp}^0 |1_{dp}\rangle = |1_{dp}\rangle, \\ U_{dp}^1 |0_{dp}\rangle &= |1_{dp}\rangle, \quad U_{dp}^1 |1_{dp}\rangle = -|0_{dp}\rangle, \end{aligned} \quad (1)$$

其中, $U_{dp}^0 = I_1 \otimes I_2$ 和 $U_{dp}^1 = (-i\sigma_y)_1 \otimes (\sigma_x)_2$ 是两个逻辑酉操作. 这里, $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $-i\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1|$

和 $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$ 是 3 个原始酉操作, 数字下标代表它所施加的物理量子比特.

这里, 作为初始量子资源的三量子比特纠缠态可被描述为^[43]

$$|\Phi_{dp}^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle|0_{dp}\rangle + |1\rangle|1_{dp}\rangle)_{AB}. \quad (2)$$

根据式(2), 如果 Z 基 ($Z = \{|0\rangle, |1\rangle\}$) 测量和 Z_{dp} 基测量被分别施加在物理量子比特 A 和逻辑量子比特 B 上, $|\Phi_{dp}^+\rangle_{AB}$ 将以每个 1/2 的概率被坍塌为 $|0\rangle_A |0_{dp}\rangle_B$ 和 $|1\rangle_A |1_{dp}\rangle_B$. 而且, 如果物理量子比特 A 被坍塌为 $|0\rangle_A$ ($|1\rangle_A$), 逻辑量子比特 B 将相应地被坍塌为 $|0_{dp}\rangle_B$ ($|1_{dp}\rangle_B$). 换句话说, 逻辑量子比特 B 的 Z_{dp} 基测量结果与物理量子比特 A 的 Z 基测量结果高度相关. 这个性质在这里被称为“三量子比特纠缠态 $|\Phi_{dp}^+\rangle_{AB}$ 的测量相关性”.

假设 Alice 拥有 N 比特秘密消息 $\{k_1, k_2, \dots, k_N\}$, Bob 拥有 N 比特秘密消息 $\{i_1, i_2, \dots, i_N\}$, 其中 $k_n, i_n \in \{0, 1\}$, $n \in \{1, 2, \dots, N\}$. 可运行在集体退相位噪声信道上的鲁棒 QD 协议被详细说明如下.

步骤 1 Alice 制备 $N+Q$ 个都处于 $|\Phi_{dp}^+\rangle_{AB}$ 的三量子比特纠缠态. 然后她将这些三量子比特纠缠态分成两个有序粒子序列, S_A 和 S_B , 其中 S_A 是由所有物理量子比特 A 构成, S_B 是由所有逻辑量子比特 B 构成, 也就是 $S_A = \{A_1, A_2, \dots, A_{N+Q}\}$ 和 $S_B = \{B_1, B_2, \dots, B_{N+Q}\}$. 最后, 她以块传输的方式^[1]将 S_B 发送给 Bob 并将 S_A 保留在她自己手中.

步骤 2 在 Bob 告知 Alice 他已收到 S_B 后, 他们一起开始利用与文献[3]的第一次安全检测方法类似的样本检测方法执行窃听检测. Bob 首先从 S_B 随机选择 Q 个逻辑量子比特作为样本逻辑量子比特. 然后, 他随机利用 Z_{dp} 基或 $X \otimes X$ 基

$$\left(X = \{|+\rangle, |-\rangle\}, |\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \right)$$

测量每个样本逻辑量子比特. 接着, Bob 告诉 Alice 这些样本逻辑量子比特的的位置和测量基. 这样, Alice 从

Z 基和 X 基中选择恰当的测量基来测量 S_A 中相应的样本物理量子比特. 如果不存在窃听, 根据式(3), 他们的测量结果应当存在确定的相关性^[43]. 相应地, 通信被继续; 否则, 通信被终止.

$$\begin{aligned} |\Phi_{dp}^+\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0\rangle_A |01\rangle_{B_1 B_2} + |1\rangle_A |10\rangle_{B_1 B_2}) \\ &= \frac{1}{\sqrt{2}} \left[|+\rangle_A (|++\rangle - |--\rangle)_{B_1 B_2} \right. \\ &\quad \left. + |-\rangle_A (|-+\rangle - |- -\rangle)_{B_1 B_2} \right]. \end{aligned} \quad (3)$$

步骤 3 Alice 和 Bob 分别丢弃 S_A 和 S_B 中的 Q 个样本物理量子比特和 Q 个样本逻辑量子比特. 这样, S_A 和 S_B 被分别转变为 S'_A 和 S'_B , 其中, $S'_A = \{A_1, A_2, \dots, A_N\}$, $S'_B = \{B_1, B_2, \dots, B_N\}$. Alice 和 Bob 分别用 Z 基和 Z_{dp} 基测量 A_n 和 B_n ($n=1, 2, \dots, N$). 根据三量子比特纠缠态 $|\Phi_{dp}^+\rangle_{AB}$ 的测量相关性, Alice 和 Bob 能推断出彼此的测量结果. 根据他自己的测量结果, Bob 重新制备一个新的没有进行过测量的 B_n . 然后, 为了编码他的一比特秘密消息 i_n , Bob 对新的 B_n 施加逻辑酉操作 $U_{dp}^{i_n}$. 这样, 新的 B_n 被转变为 $U_{dp}^{i_n} B_n$. 接着, 为了确保传输安全性, Bob 采用诱骗光子技术^[56,57]. 也就是, Bob 制备足够的随机处于 $\{|0_{dp}\rangle, |1_{dp}\rangle, |+\rangle, |-\rangle\}$ 4 个态之一的诱骗逻辑量子比特并将它们随机插入 S'_B . 相应地, S'_B 被转变为一个新序列 S''_B . 最后, Bob 以块传输方式^[1]将 S''_B 发送给 Alice.

步骤 4 在 Alice 告知 Bob 她已收到 S''_B 后, Bob 告诉 Alice 那些诱骗逻辑量子比特的位置和相应的制备基. Alice 用 Bob 的制备基测量诱骗逻辑量子比特并告诉 Bob 她的测量结果. 通过对比诱骗逻辑量子比特的初态和 Alice 的测量结果, Bob 能判断出量子信道是否安全. 如果量子信道是安全的, 通信被继续; 否则, 通信被终止.

步骤 5 Alice 丢弃 S''_B 中的诱骗逻辑量子比特. 这样, S''_B 被转变回 S'_B . 然后, 为了编码她的一比特秘密消息 k_n , Alice 对逻辑量子比特 $U_{dp}^{i_n} B_n$ 施加逻辑酉操作 $U_{dp}^{k_n}$. 这样, $U_{dp}^{i_n} B_n$ 被转变为 $U_{dp}^{k_n} U_{dp}^{i_n} B_n$. 然后, Alice 用 Z_{dp} 基测量 $U_{dp}^{k_n} U_{dp}^{i_n} B_n$ 并向 Bob 公布她的测量结果. 根据他自己的逻辑酉操作 $U_{dp}^{i_n}$ 、他自己对 B_n 的

Z_{dp} 基测量结果和 Alice 的公布, Bob 能读出 Alice 的一比特秘密消息 k_n . 与此同时, 既然 Alice 能从她自己对 A_n 的 Z 基测量结果推断出 Bob 对 B_n 的 Z_{dp} 基测量结果, 根据她自己的逻辑酉操作 $U_{dp}^{k_n}$, Alice 也能推断出 Bob 的一比特秘密消息 i_n .

显然, 文献[38]的 Bell 态版本协议将传输量子态进行单向传送, 而以上协议将传输量子态进行来回传送. 然而, 通过忽略传送模式的差异, 以上协议仍能被视为文献[38]的 Bell 态版本协议在集体退相位噪声情形下的推广. 这是因为它们都是基于量子纠缠态的测量相关性. 而且, 前者将对集体退相位噪声免疫的逻辑量子比特代替后者的单光子作为传输量子态以进行编码.

另外, 这里进一步考虑上述协议涉及的量子测量. 在上述协议中, 只有步骤 4 需要 X_{dp} 基测量, 因为那里一些诱骗逻辑量子比特被制备处于 $\{|+\rangle, |-\rangle\}$. 在 Hadamard 操作被施加在每个物理量子比特后, $|+\rangle$ 被转变为 $|\phi^-\rangle = (1/\sqrt{2})(|00\rangle - |11\rangle)$ 而 $|-\rangle = |\psi^-\rangle = (1/\sqrt{2})(|01\rangle - |10\rangle)$ 被保持不变^[50]. 因为 $|\phi^-\rangle$ 和 $|\psi^-\rangle$ 对于它们各自的两个光子具有不同的宇称, $|+\rangle$ 和 $|-\rangle$ 能通过 Hadamard 操作被施加在每个物理量子比特后的 $Z \otimes Z$ 基测量所区分. 因此, 上述协议只需要单光子测量.

为清晰起见, 用一个例子进一步解释以上协议. 假设 $k_n = 1$ 和 $i_n = 0$. 而且, 不失一般性, 假设步骤 3 在 Alice 的 Z 基测量和 Bob 的 Z_{dp} 基测量后, A_n 和 B_n 被分别坍塌为 $|0\rangle_A$ 和 $|0_{dp}\rangle_B$. 相应地, Bob 重新制备一个新的处于 $|0_{dp}\rangle_B$ 的 B_n . 这样, 新的 B_n 会经历以下演化:

$$\begin{aligned} |0_{dp}\rangle_B &\Rightarrow U_{dp}^0 \otimes |0_{dp}\rangle_B \\ &= |0_{dp}\rangle_B \Rightarrow U_{dp}^1 \otimes |0_{dp}\rangle_B = |1_{dp}\rangle_B. \end{aligned} \quad (4)$$

根据 3 个已知的信息: 被宣布的测量结果 $|1_{dp}\rangle_B$ 、他自己对 B_n 的 Z_{dp} 基测量结果以及他自己的逻辑酉操作 U_{dp}^0 , Bob 能够知道 k_n 为 1. 同样地, 根据她自己的逻辑酉操作 U_{dp}^1 和她自己对 A_n 的 Z 基测量结果, Alice 也能推断出 i_n 为 0.

3 可运行在集体旋转噪声信道上的鲁棒 QD 协议

当光子的水平极化态 $|0\rangle$ 和垂直极化态 $|1\rangle$ 分别在集体旋转噪声信道传输时, 前者总是被改变为 $\cos\theta|0\rangle + \sin\theta|1\rangle$, 后者总是被改变为 $-\sin\theta|0\rangle + \cos\theta|1\rangle$ [46], 其中 θ 是随时间变化的噪声参数. 可以直接得到两个逻辑量子比特,

$$|0_r\rangle = |\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

和

$$|1_r\rangle = |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle),$$

对这类噪声免疫 [46]. 它们的叠加态,

$$|+\rangle_r = \frac{1}{\sqrt{2}}(|0_r\rangle + |1_r\rangle) \equiv |\Phi^+\rangle$$

和

$$|-\rangle_r = \frac{1}{\sqrt{2}}(|0_r\rangle - |1_r\rangle) \equiv |\Psi^-\rangle,$$

也总是不受这类噪声影响 [48]. $Z_r = \{|0_r\rangle, |1_r\rangle\}$ 和 $X_r = \{|+\rangle_r, |-\rangle_r\}$ 是这类噪声下的两个逻辑测量基. 显然, 有以下关系存在 [50]:

$$\begin{aligned} U_r^0|0_r\rangle &= |0_r\rangle, \quad U_r^0|1_r\rangle = |1_r\rangle, \\ U_r^1|0_r\rangle &= |1_r\rangle, \quad U_r^1|1_r\rangle = -|0_r\rangle, \end{aligned} \quad (5)$$

其中, $U_r^0 = I_1 \otimes I_2$ 和 $U_r^1 = I_1 \otimes (-i\sigma_y)_2$ 是两个逻辑酉操作. 这里, 数字下标代表它所施加的物理量子比特.

这里, 作为初始量子资源的三量子比特纠缠态可被描述为 [43]

$$|\Phi_r^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0_r\rangle + |1\rangle_A|1_r\rangle)_{AB}. \quad (6)$$

根据式(6), 如果 Z 基测量和 Z_r 基测量被分别施加在物理量子比特 A 和逻辑量子比特 B 上, $|\Phi_r^+\rangle_{AB}$ 将以每个 $1/2$ 的概率被坍塌为 $|0\rangle_A|0_r\rangle_B$ 和 $|1\rangle_A|1_r\rangle_B$. 而且, 如果物理量子比特 A 被坍塌为 $|0\rangle_A(|1\rangle_A)$, 逻辑量子比特 B 将相应地被坍塌为 $|0_r\rangle_B(|1_r\rangle_B)$. 换句话说, 逻辑量子比特 B 的 Z_r 基测量结果与物理量子比特 A 的 Z 基测量结果高度相关. 这个性质在这里被称为

“三量子比特纠缠态 $|\Phi_r^+\rangle_{AB}$ 的测量相关性”.

假设 Alice 和 Bob 分别拥有 N 比特秘密消息 $\{k_1, k_2, \dots, k_N\}$ 和 N 比特秘密消息 $\{i_1, i_2, \dots, i_N\}$, 其中 $k_n, i_n \in \{0, 1\}$, $n \in \{1, 2, \dots, N\}$. 在具备以下不同之处后, 第 2 部分的可运行在集体退相位噪声信道上的鲁棒 QD 协议可直接转化为可运行在集体旋转噪声信道上的版本.

步骤 1 Alice 制备的 $N+Q$ 个三量子比特纠缠态都处于 $|\Phi_r^+\rangle_{AB}$.

步骤 2 Bob 随机利用 Z_r 基或 $Y \otimes Y$ 基

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

测量从 S_B 中随机选择的每个样本逻辑量子比特, 而 Alice 从 Z 基和 Y 基中选择恰当的测量基来测量 S_A 中相应的样本物理量子比特. 在没有窃听的情况下, 他们的测量结果之间的确定相关性如式(7)所示 [43].

$$\begin{aligned} |\Phi_r^+\rangle_{AB} &= \frac{1}{2} \left[|0\rangle_A(|00\rangle + |11\rangle)_{B_1B_2} + |1\rangle_A(|01\rangle - |10\rangle)_{B_1B_2} \right] \\ &= \frac{1}{\sqrt{2}} \left(|+y\rangle_A |+y\rangle_{B_1} |-y\rangle_{B_2} + |-y\rangle_A |-y\rangle_{B_1} |+y\rangle_{B_2} \right). \end{aligned} \quad (7)$$

步骤 3 Alice 和 Bob 分别用 Z 基和 Z_r 基测量 A_n 和 B_n ($n=1, 2, \dots, N$). 根据他自己的测量结果, Bob 重新制备一个新的没有进行过测量的 B_n . 接着, Bob 对新的 B_n 施加逻辑酉操作 $U_r^{i_n}$ 以编码他的一比特秘密消息 i_n 从而得到 $U_r^{i_n} B_n$. 另外, Bob 制备的诱骗逻辑量子比特为随机处于 $\{|0_r\rangle, |1_r\rangle, |+\rangle_r, |-\rangle_r\}$ 4 个态之一.

步骤 4 在 Alice 告知 Bob 她已收到 S_B'' 后, Bob 告诉 Alice 那些诱骗逻辑量子比特的位置和相应的制备基. Alice 用 Bob 的制备基测量诱骗逻辑量子比特并告诉 Bob 她的测量结果. 通过对比诱骗逻辑量子比特的初态和 Alice 的测量结果, Bob 能判断出量子信道是否安全. 如果量子信道是安全的, 通信被继续; 否则, 通信被终止.

步骤 5 Alice 对逻辑量子比特 $U_r^{i_n} B_n$ 施加逻辑酉操作 $U_r^{k_n}$ 以编码她的一比特秘密消息 k_n 从而得到 $U_r^{k_n} U_r^{i_n} B_n$. 然后, Alice 用 Z_r 基测量 $U_r^{k_n} U_r^{i_n} B_n$ 并向 Bob

公布她的测量结果. Bob 利用 $U_r^{i_n}$ 、他自己对 B_n 的 Z_r 基测量结果和 Alice 的公布解码出 k_n . Alice 先从她自己对 A_n 的 Z 基测量结果推断出 Bob 对 B_n 的 Z_r 基测量结果, 再利用 $U_r^{k_n}$ 解码出 i_n .

以上协议将传输量子态进行来回传送. 与第 2 部分提出的协议类似, 通过忽略传送模式的差异, 以上协议仍能被视为文献[38]的 Bell 态版本协议在集体旋转噪声情形下的推广. 这是因为它们都是基于量子纠缠态的测量相关性以及前者将对集体旋转噪声免疫的逻辑量子比特代替后者的单光子作为传输量子态以进行编码.

另外, 这里进一步考虑上述协议涉及的量子测量. 上述协议的步骤 2, 3 和 5 都需要进行 $|0_r\rangle$ 和 $|1_r\rangle$ 之间的区分, 步骤 4 需要进行 $|0_r\rangle$ 和 $|1_r\rangle$ 之间的区分以及 $|+_r\rangle$ 和 $|-_r\rangle$ 之间的区分. 因为 $|0_r\rangle = |\phi^+\rangle$ 和 $|1_r\rangle = |\psi^-\rangle$ 对于它们各自的两个光子具有不同的宇称, 它们能通过 $Z \otimes Z$ 基测量进行区分. 另一方面, 在 Hadamard 操作被施加在第二个物理量子比特后, $|+_r\rangle = |\Phi^+\rangle$ 和 $|-_r\rangle = |\Psi^-\rangle$ 被分别转变为

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

和

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad [50].$$

因为 $|\phi^-\rangle$ 和 $|\psi^+\rangle$ 对于它们各自的两个光子具有不同的宇称, $|+_r\rangle$ 和 $|-_r\rangle$ 之间的区分能通过 Hadamard 操作被施加在第二个物理量子比特后的 $Z \otimes Z$ 测量所完成. 因此, 上述协议只需要单光子测量.

4 安全性分析

不失一般性, 这里以所提出的可运行在集体退相位噪声信道上的鲁棒 QD 协议为例进行安全性分析.

4.1 信息泄露问题

以第 2 部分的例子分析信息泄露问题. 根据三量子比特纠缠态 $|\Phi_{dp}^+\rangle_{AB}$ 的测量相关性, Alice 能从她自己对 A_n 的 Z 基测量结果推断出 Bob 关于 B_n 的 Z_{dp} 基测量结果. 这样, Bob 就没必要向 Alice 宣布他自己关

于 B_n 的 Z_{dp} 基测量结果, 使得 Eve 没有机会知道新的 B_n 的状态. 因此, 被 Alice 宣布的测量结果 $|1_{dp}\rangle_B$ 包含来自于两个参与者的 4 种逻辑酉操作组合. 换句话说, Alice 和 Bob 有 4 种可能的秘密信息, 即 $\{k_n=1, i_n=0\}$, $\{k_n=0, i_n=1\}$, $\{k_n=0, i_n=0\}$ 和 $\{k_n=1, i_n=1\}$. 从 Shannon 的信息论^[58]的角度来看, 对于 Eve 来说, 这包含

$$-\sum_{i=1}^4 p_i \log_2 p_i = -4 \times \frac{1}{4} \log_2 \frac{1}{4} = 2$$

比特信息. 因此, 信息泄露问题不存在. 显然, 三量子比特纠缠态 $|\Phi_{dp}^+\rangle_{AB}$ 的测量相关性帮忙克服信息泄露问题.

4.2 Eve 的主动攻击

在所提出的协议中, 由于每个信息逻辑量子比特在两个参与者之间经历来回传送, 首先应当考虑来自 Eve 的木马攻击, 包括不可见光子窃听^[59]和延迟光子木马攻击^[60]. 正如文献[61]所建议的, Bob 能使用过滤器滤除不可见光子和光子数分离器(Photon number Splitter, PNS)监测延迟光子. 这样, 这两种木马攻击的影响就能被消除.

另外, 所提出的协议需要两次窃听检测来确保来回传送的安全性. 在第二次传送中, 诱骗光子技术^[56,57]被用来保证其安全性. Eve 没有机会知道诱骗逻辑量子比特的真实位置和它们正确的逻辑测量基. 这样, 她将不可避免地在它们上面留下痕迹从而将被第二次安全检测检测到. 事实上, 即使她截获传输序列, 由于她不知道信息逻辑量子比特的真实位置以及它们的初态, Eve 仍然不能得到关于 Alice 和 Bob 的秘密消息的任何有用信息, 并同时最终被第二次安全检测检测到. 因此, 只要第一次传送的安全性被确保, 所提出协议最终将是安全的.

在第一次安全检测中, 物理量子比特 A 和逻辑量子比特 B 之间的确定性纠缠相关性被用于检测 S_B 从 Alice 到 Bob 的传输安全性. 事实上, 只要将 $|\Phi_{dp}^+\rangle_{AB}$ 的逻辑量子比特 B 当成一个 Bell 态的第二个粒子看待, 这种安全检测方法就可被视为等同于文献[3]的第一次安全检测方法. 既然文献[3]的第一次安全检测方法已经被证明能有效确保传输安全性, 所提出协议的第一次传输的安全性就自然地能由第

表 1 与之前提出的可运行在集体噪声信道上的 QD 协议的对比

Table 1 Comparisons with previous QD protocols workable over collective-noise channels

对比项目	文献[52]的协议	文献[53]的协议	文献[55]的协议	本文提出的协议
初始量子资源	两个原始 Bell 态的乘积态	逻辑量子比特	逻辑 Bell 态	三量子比特纠缠态
量子测量	Bell 基测量	单光子测量	Bell 基测量	单光子测量
信息论效率	40%	33.3%	40%	50%
信息泄露问题	无	无	无	无

一次安全检测来保证. 可以得出结论, 所提出的协议在原理上是完全安全的.

5 讨论

5.1 信息论效率

Cabello 的信息论效率^[62]被定义为 $\eta = b_s / (q_t + b_t)$, 其中 b_s , q_t 和 b_t 分别是期望收到的秘密比特数、所使用的量子比特数以及两个参与者之间交换的经典比特数. 在所提出的可运行在集体退相位(集体旋转)噪声信道上的鲁棒 QD 协议, 每个

$$|\Phi_{dp}^+\rangle_{AB} \left(|\Phi_r^+\rangle_{AB} \right)$$

被用来交换 Alice 的一比特和 Bob 的一比特, 同时一比特被消耗于 Bob 对最终编码后的逻辑量子比特的宣布. 也就是, 有 $b_s = 2$, $q_t = 3$ 和 $b_t = 1$. 这样, 所提出的可运行在集体退相位(集体旋转)噪声信道上的协议的信息论效率为

$$\eta = \frac{2}{3+1} \times 100\% = 50\%.$$

5.2 与之前提出的可运行在集体噪声信道上的 QD 协议的对比

文献[52,53,55]的 QD 协议可在集体噪声信道上运行. 这里将所提出的协议与它们在初始量子资源、量子测量、信息论效率以及信息泄露问题 4 个方面进行对比. 对比结果被总结在表 1 中. 根据表 1, 所提出的协议具有最高的信息论效率. 而且, 所提出的协议比文献[52,55]的协议在量子测量上更占有优势.

6 结论

本文利用三量子比特纠缠态作为初始量子资源提出两个鲁棒 QD 协议. 所提出协议的亮点在于: (1) 它们分别适用于集体退相位噪声信道和集体旋转噪声信道; (2) 它们利用三量子比特纠缠态的测量相关性使两个参与者秘密地共享信息逻辑量子比特的初态从而避免信息泄露问题; (3) 它们只使用单光子测量作为量子测量; (4) 与之前提出的可运行在集体噪声信道上的 QD 协议相比, 它们具有最高的信息论效率.

参考文献

- Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A, 2002, 65: 032302
- Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. Phys Rev Lett, 2002, 89: 187902
- Deng F G, Long G L, Liu X S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. Phys Rev A, 2003, 68: 042317
- Deng F G, Long G L. Secure direct communication with a quantum one-time pad. Phys Rev A, 2004, 69: 052319
- Wang C, Deng F G, Li Y S, et al. Quantum secure direct communication with high-dimension quantum superdense coding. Phys Rev A, 2005, 71: 044305
- Wang C, Deng F G, Long G L. Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state. Opt Commun, 2005, 253: 15-20
- Li X H, Li C Y, Deng F G, et al. Quantum secure direct communication with quantum encryption based on pure entangled states. Chin Phys, 2007, 16: 2149-2153
- Chen X B, Wen Q Y, Guo F Z, et al. Controlled quantum secure direct communication with W state. Int J Quant Inform, 2008, 6: 899-906
- Gu B, Huang Y G, Fang X, et al. A two-step quantum secure direct communication protocol with hyperentanglement. Chin Phys B, 2011, 20: 100309

- 10 Liu D, Chen J L, Jiang W. High-capacity quantum secure direct communication with single photons in both polarization and spatial-mode degrees of freedom. *Int J Theor Phys*, 2012, 51: 2923–2929
- 11 Ren B C, Wei H R, Hua M, et al. Photonic spatial Bell-state analysis for robust quantum secure direct communication using quantum dot-cavity systems. *Eur Phys J D*, 2013, 67: 30–37
- 12 Chang Y, Xu C X, Zhang S B, et al. Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad. *Chin Sci Bull*, 2014, 59: 2541–2546
- 13 Nguyen B A. Quantum dialogue. *Phys Lett A*, 2004, 328: 6–10
- 14 Zhang Z J, Man Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. *arXiv:quant-ph/0403215v1*
- 15 Zhang Z J, Man Z X. Secure bidirectional quantum communication protocol without quantum channel. *arXiv:quant-ph/0403217v4*
- 16 Man Z X, Zhang Z J, Li Y. Quantum dialogue revisited. *Chin Phys Lett*, 2005, 22: 22–24
- 17 Jin X R, Ji X, Zhang Y Q, et al. Three-party quantum secure direct communication based on GHZ states. *Phys Lett A*, 2006, 354: 67–70
- 18 Man Z X, Xia Y J. Controlled bidirectional quantum direct communication by using a GHZ state. *Chin Phys Lett*, 2006, 23: 1680–1682
- 19 Ji X, Zhang S. Secure quantum dialogue based on single-photon. *Chin Phys*, 2006, 15: 1418–1420
- 20 Man Z X, Xia Y J, Nguyen B A. Quantum secure direct communication by using GHZ states and entanglement swapping. *J Phys B-At Mol Opt Phys*, 2006, 39: 3855–3863
- 21 Man Z X, Xia Y J. Improvement of security of three-party quantum secure direct communication based on GHZ states. *Chin Phys Lett*, 2007, 24: 15–18
- 22 Chen Y, Man Z X, Xia Y J. Quantum bidirectional secure direct communication via entanglement swapping. *Chin Phys Lett*, 2007, 24: 19–22
- 23 Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons. *Sci China Ser G-Phys Mech Astron*, 2007, 50: 558–562
- 24 Shan C J, Liu J B, Cheng W W, et al. Bidirectional quantum secure direct communication in driven cavity QED. *Mod Phys Lett B*, 2009, 23: 3225–3234
- 25 Ye T Y, Jiang L Z. Improvement of controlled bidirectional quantum secure direct communication by using a GHZ state. *Chin Phys Lett*, 2013, 30: 040305
- 26 Gao F, Qin S J, Wen Q Y, et al. Comment on: “Three-party quantum secure direct communication based on GHZ states”. *Phys Lett A*, 2008, 372: 3333–3336
- 27 Gao F, Guo F Z, Wen Q Y, et al. Revisiting the security of quantum dialogue and bidirectional quantum secure direct communication. *Sci China Ser G-Phys Mech Astron*, 2008, 51: 559–566
- 28 Tan Y G, Cai Q Y. Classical correlation in quantum dialogue. *Int J Quant Inform*, 2008, 6: 325–329
- 29 Shi G F, Xi X Q, Tian X L, et al. Bidirectional quantum secure communication based on a shared private Bell state. *Opt Commun*, 2009, 282: 2460–2463
- 30 Shi G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles. *Opt Commun*, 2010, 283: 5275–5278
- 31 Gao G. Two quantum dialogue protocols without information leakage. *Opt Commun*, 2010, 283: 2288–2293
- 32 Shi G F, Xi X Q, Hu M L, et al. Quantum secure dialogue by using single photons. *Opt Commun*, 2010, 283: 1984–1986
- 33 Shi G F, Tian X L. Quantum secure dialogue based on single photons and controlled-not operations. *J Mod Opt*, 2010, 57: 2027–2030
- 34 Yin X R, Ma W P, Liu W Y, et al. Efficient bidirectional quantum secure communication with two-photon entanglement. *Quantum Inf Process*, 2013, 12: 3093–3102
- 35 Ye T Y. Large payload bidirectional quantum secure direct communication without information leakage. *Int J Quant Inform*, 2013, 11: 1350051
- 36 Ye T Y, Jiang L Z. Quantum dialogue without information leakage based on the entanglement swapping between any two Bell states and the shared secret Bell state. *Phys Scripta*, 2014, 89: 015103
- 37 Ye T Y. Quantum secure dialogue with quantum encryption. *Commun Theor Phys*, 2014, 62: 338–342
- 38 Ye T Y. Quantum dialogue without information leakage using a single quantum entangled state. *Int J Theor Phys*, 2014, 53: 3719–3727
- 39 Zheng C, Long G F. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. *Sci China-Phys Mech Astron*, 2014, 57: 1238–1243
- 40 Zhou N R, Hua T X, Wu G T, et al. Single-photon secure quantum dialogue protocol without information leakage. *Int J Theor Phys*, 2014,

53: 3829–3837

- 41 Luo Y P, Lin C Y, Hwang T. Efficient quantum dialogue using single photons. *Quantum Inf Process*, 2014, 13: 2451–2461
- 42 Li X H, Deng F G, Zhou H Y. Efficient quantum key distribution over a collective noise channel. *Phys Rev A*, 2008, 78: 022321
- 43 Li X H, Zhao B K, Sheng Y B, et al. Fault tolerant quantum key distribution based on quantum dense coding with collective noise. *Int J Quant Inform*, 2009, 7: 1479–1489
- 44 Walton Z D, Abouraddy A F, Sergienko A V, et al. Decoherence-free subspaces in quantum key distribution. *Phys Rev Lett*, 2003, 91: 087901
- 45 Boileau J C, Gottesman D, Laflamme R, et al. Robust polarization-based quantum key distribution over a collective-noise channel. *Phys Rev Lett*, 2004, 92: 017901
- 46 Zhang Z J. Robust multiparty quantum secret key sharing over two collective-noise channels. *Physica A*, 2006, 361: 233–238
- 47 Gu B, Pei S X, Song B, et al. Deterministic secure quantum communication over a collective-noise channel. *Sci China Ser G-Phys Mech Astron*, 2009, 52: 1913–1918
- 48 Gu B, Mu L L, Ding L G, et al. Fault tolerant three-party quantum secret sharing against collective noise. *Opt Commun*, 2010, 283: 3099–3103
- 49 Yang C W, Tsai C W, Hwang T. Fault tolerant two-step quantum secure direct communication protocol against collective noises. *Sci China-Phys Mech Astron*, 2011, 54: 496–501
- 50 Gu B, Zhang C Y, Cheng G S, et al. Robust quantum secure direct communication with a quantum one-time pad over a collective-noise channel. *Sci China-Phys Mech Astron*, 2011, 54: 942–947
- 51 Lin J, Hwang T. Bell state entanglement swappings over collective noises and their applications on quantum cryptography. *Quantum Inf Process*, 2013, 12: 1089–1107
- 52 Yang C W, Hwang T. Quantum dialogue protocols immune to collective noise. *Quantum Inf Process*, 2013, 12: 2131–2142
- 53 Ye T Y. Information leakage resistant quantum dialogue against collective noise. *Sci China-Phys Mech Astron*, 2014, 57: 2266–2275
- 54 Ye T Y. Fault tolerant quantum steganography over collective-noise channels. *Sci Sin-Phys Mech Astron*, 2015, 45: 010301 (in Chinese) [叶天语. 集体噪声信道上错误容忍量子隐写. *中国科学: 物理学 力学 天文学*, 2015, 45: 010301]
- 55 Ye T Y. Robust quantum dialogue based on a shared auxiliary logical Bell state against collective noise (in Chinese). *Sci Sin-Phys Mech Astron*, 2015, 45: 040301 [叶天语. 基于一个共享辅助逻辑 Bell 态的抗集体噪声鲁棒量子对话. *中国科学: 物理学 力学 天文学*, 2015, 45: 040301]
- 56 Li C Y, Zhou H Y, Wang Y, et al. Secure quantum key distribution network with Bell states and local unitary operations. *Chin Phys Lett*, 2005, 22: 1049–1052
- 57 Li C Y, Li X H, Deng F G, et al. Efficient quantum cryptography network without entanglement and quantum memory. *Chin Phys Lett*, 2006, 23: 2896–2899
- 58 Shannon C E. Communication theory of secrecy system. *Bell Syst Tech J*, 1949, 28: 656–715
- 59 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A*, 2006, 351: 23–25
- 60 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 74: 145–195
- 61 Li X H, Deng F G, Zhou H Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys Rev A*, 2006, 74: 054302
- 62 Cabello A. Quantum key distribution in the Holevo limit. *Phys Rev Lett*, 2000, 85: 5635–5638

Robust quantum dialogue based on the measurement correlation of three-qubit entangled states over collective noise channels

YE TianYu^{*}

College of Information & Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018, China

In this paper, two robust quantum dialogue (QD) protocols over collective-dephasing noise channel and collective-rotation noise channel are proposed, respectively, by using three-qubit entangled states as the initial quantum resource. Alice generates a series of three-qubit entangled states and divides them into a physical qubit sequence and a logical qubit sequence. Then, Alice sends the logical qubit sequence to Bob. Afterward, Alice and Bob measure the physical qubit sequence and the logical qubit sequence, respectively. According to his measurement result, Bob generates a new logical qubit sequence with no measurement performed. Then, Bob encodes his secret messages on the new logical qubit sequence by performing logical unitary operations on it. Afterward, Bob sends the encoded logical qubit sequence back to Alice. Finally, Alice encodes her secret messages on the encoded logical qubit sequence from Bob by performing logical unitary operations on it and publishes her measurement. As a result, Alice and Bob can decode out each other's secret messages. By virtue of the measurement correlation of three-qubit entangled states, two participants share the initial states of message logical qubits privately. In this way, the information leakage problem is overcome. The proposed protocols only need the single-photon measurements. Compared with previous QD protocols workable over collective noise channels, the proposed protocols have the highest information-theoretical efficiency.

quantum dialogue (QD), collective-dephasing noise, collective-rotation noise, measurement correlation, information leakage

PACS: 03.67.Dd, 03.67.Hk, 03.67.Pp

doi: 10.1360/SSPMA2014-00510