论文

基于逻辑量子比特和控制非操作的鲁棒量子对话

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: 2014-11-18; 接受日期: 2014-12-18; 网络出版日期: 2015-01-20

国家自然科学基金资助项目(批准号: 61402407, 11375152)

摘要 本文利用逻辑量子比特和控制非(Controlled-Not, CNOT)操作提出两个分别抵抗集体退相位噪声和集体旋转噪声的鲁棒量子对话(Quantum Dialogue, QD)协议. 制备方产生逻辑量子比特作为传输态以抵抗集体噪声. 另一方借助于 CNOT 操作知道逻辑量子比特的初始制备态, 并在制备方发送过来的一个经典信息序列的帮助下解码出制备方的秘密信息. 制备方借助于量子安全直接通信读出另一方的秘密信息. 这样, 信息泄露风险被有效地避免. 在所提出的协议中, 只有单光子测量被需要用于量子测量. 与之前的抗噪声 QD 协议相比, 所提出的协议具有最高的信息论效率. 与作者最近设计的需要将两个相邻的逻辑量子比特制备处于相同的量子态的 QD 协议相比, 所提出的协议在实验上更加容易执行, 因为它们没有这种特殊的要求.

关键词 量子对话, 逻辑量子比特, 控制非操作, 集体退相位噪声, 集体旋转噪声, 信息泄露

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

doi: 10.1360/SSPMA2014-00444

1 前言

在 2002 年, Long 和 Liu^[1]提出第一个量子安全直接通信(Quantum Secure Direct Communication, QSDC)协议, 意味着利用量子信号将秘密信息从一方直接传送到另一方的梦想变为现实. 然后, 许多好的 QSDC 协议从不同角度被构造出来^[2-11]. 自然地, 一个人希望通过量子信道与另一个人进行对话. 在 2004 年, Nguyen^[12]和 Zhang 等人^[13,14]使这个梦想变成现实, 当他们独立提出称为量子对话(Quantum Dialogue, QD)的新概念. 也就是说, QD 能够让双方

自由地交换信息. 然后, 一些 QD 协议被设计出来^[15-24]. 然而, 在 2008 年, Gao 等人^[25,26]指出 QD 总是存在称为信息泄露的风险. 这意味着任何其他人能直接推断出部分秘密信息而无需进行任何窃听. 同年, Tan 和 Cai^[27]发现 QD 存在称为经典相关的现象. 事实上, 信息泄露和经典相关属于同一回事. 自从那时起, 许多好的无信息泄露 QD 协议根据不同的执行途径被提出来^[28-37]. 然而, 它们只能假设量子信道是理想的. 事实上, 由于光纤双折射的波动, 光子易受量子信道噪声的干扰. 量子信道噪声可被视为集体噪声, 只要光子在一个比噪声源变化还快的时间窗

引用格式: 叶天语. 基于逻辑量子比特和控制非操作的鲁棒量子对话. 中国科学: 物理学 力学 天文学, 2015, 45: 030301

Ye T Y. Robust quantum dialogue based on logical qubits and controlled-not operations (in Chinese). Sci Sin-Phys Mech Astron, 2015, 45: 030301, doi: 10.1360/SSPMA2014-00444

里传输^[38,39]. 众所周知的是, 无消相干(Decoherence-Free, DF)态^[38-50]是一种有效的消除集体噪声干扰的手段, 因为它们总是对于集体噪声具有不变性. 特别地, DF 态已经被用来设计抗噪声 QD 协议^[47,49,50]. 在文献[47], 对集体噪声免疫的两个原始 Bell 态的乘积态(两量子比特 DF 态的乘积态)被作为传输量子态. 在文献[49], 逻辑量子比特(2 量子比特 DF 态)被用作传输量子态以抵抗集体噪声. 在文献[50], 逻辑 Bell 态(4 量子比特 DF 态)被用作传输量子态以克服集体噪声.

基于以上分析, 本文利用逻辑量子比特和控制非(Controlled-Not, CNOT)操作提出两个分别抵抗集体退相位噪声和集体旋转噪声的鲁棒 QD 协议. 制备方产生逻辑量子比特作为传输态以抵抗集体噪声. 另一方借助于 CNOT 操作知道逻辑量子比特的初始制备态, 并在制备方发送过来的一个经典信息序列的帮助下解码出制备方的秘密信息. 制备方借助于量子安全直接通信读出另一方的秘密信息. 这样, 信息泄露风险被有效地避免. 在所提出的协议中, 只有单光子测量被需要用于量子测量. 与之前的抗噪声 QD 协议^[47,49,50]相比, 所提出的协议具有最高的信息论效率. 与最近的文献[49]的需要将两个相邻的逻辑量子比特制备处于相同的量子态的 QD 协议相比, 所提出的协议在实验上更加容易执行, 因为它们没有这种特殊的要求.

2 抗集体退相位噪声的鲁棒 QD 协议

一个量子信道上的集体退相位噪声能使光子的水平极化态 $|0\rangle$ 保持不变和使光子的垂直极化态 $|1\rangle$ 改变为 $e^{i\varphi}|1\rangle$ ^[40], 其中 φ 是随时间变化的噪声参数. 显然, 定义为 $|0_{dp}\rangle = |01\rangle$ 和 $|1_{dp}\rangle = |10\rangle$ 的两个逻辑量子比特能抵抗这类噪声^[40]. 这两个逻辑量子比特能通过 $Z \otimes Z$ -基测量进行区分, 其中 $Z = \{|0\rangle, |1\rangle\}$. 它们的叠加态, 即

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

也能抵抗这类噪声^[42]. 这样就形成了这类噪声下的两个逻辑测量基. 也就是, $Z_{dp} = \{|0_{dp}\rangle, |1_{dp}\rangle\}$ 和 $X_{dp} =$

$\{|+_{dp}\rangle, |-_{dp}\rangle\}$. 在定义两个逻辑酉操作为 $U_{dp}^0 = I_1 \otimes I_2$ 和 $U_{dp}^1 = (-i\sigma_y)_1 \otimes (\sigma_x)_2$ 后, 以下关系便存在^[46]:

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

其中 $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $-i\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1|$ 和 $\sigma_x = |1\rangle\langle 0| + |0\rangle\langle 1|$ 是 3 个原始酉操作, 每个原始酉操作的数字下标表示它所施加的物理量子比特. 从式(1)可以明显看出, 逻辑酉操作 U_{dp}^1 只能在每个逻辑测量基内翻转它的两个量子态, 但不能改变每个逻辑测量基本身. 这个性质是文献[4]描述的理想情况下的性质在集体退相位噪声情形下的推广.

假设 Alice 拥有 N 比特秘密信息 $\{k_1, k_2, \dots, k_i, \dots, k_N\}$, Bob 拥有 N 比特秘密信息 $\{l_1, l_2, \dots, l_i, \dots, l_N\}$, 其中 $k_i, l_i \in \{0, 1\}$ ($i = 1, 2, \dots, N$). 抗集体退相位噪声的 QD 协议由下列步骤组成.

步骤 1 制备和第一次传输. Alice 制备 N 个随机处于两个态 $\{|0_{dp}\rangle, |1_{dp}\rangle\}$ 之一的信息逻辑量子比特 $\{|L_1\rangle, |L_2\rangle, \dots, |L_i\rangle, \dots, |L_N\rangle\}$ ($i = 1, 2, \dots, N$). 为了第一次安全检测, 她采用诱骗光子技术^[51,52]. 也就是, 她制备 $\delta_1 + \delta_2$ 个随机处于 4 个态 $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$ 之一的诱骗逻辑量子比特并将它们与 N 个信息逻辑量子比特随机地混合. 然后, 她将这个量子态序列发送给 Bob.

步骤 2 第一次安全检测. 在 Bob 告知 Alice 他已收到后, 他们一起完成第一次安全检测: (1) Alice 告诉 Bob δ_1 个诱骗逻辑量子比特的位置和制备基; (2) Bob 利用 Alice 的制备基测量 δ_1 个诱骗逻辑量子比特并告诉 Alice 他的测量结果; (3) Alice 通过比较 δ_1 个诱骗逻辑量子比特的初态和 Bob 的测量结果判断 Eve 是否存在. 如果存在 Eve, 他们放弃通信; 否则, 通信被继续.

步骤 3 Bob 的编码和第二次传输. Bob 丢弃 δ_1 个诱骗逻辑量子比特. 这样, 他手中的序列就由 N 个信息逻辑量子比特和 δ_2 个诱骗逻辑量子比特组成. 然后 Bob 向 Alice 询问 δ_2 个诱骗逻辑量子比特的位置. Bob 在 Alice 的指导下从他手中的序列挑选出 δ_2 个诱

骗逻辑量子比特. 然后, Bob 制备 N 个单光子 $\{|B_1\rangle, |B_2\rangle, \dots, |B_i\rangle, \dots, |B_N\rangle\}$ ($i=1, 2, \dots, N$) 都处于 $|0\rangle$. 接着, Bob 以 $|L_i\rangle$ 的第一个物理量子比特作为控制量子比特和 $|B_i\rangle$ 作为目标量子比特对 $|L_i\rangle$ 和 $|B_i\rangle$ 施加 CNOT 操作. 显然, 如果 $|L_i\rangle$ 是 $|0_{dp}\rangle$, $|B_i\rangle$ 在 CNOT 操作后将被保持不变; 如果 $|L_i\rangle$ 是 $|1_{dp}\rangle$, $|B_i\rangle$ 在 CNOT 操作后将被转变为 $|1\rangle$. 然后, Bob 按顺序保存每个 $|B_i\rangle$ 用于之后的解码.

另外, Bob 通过对 $|L_i\rangle$ 施加逻辑酉操作 $U_{dp}^{l_i}$ 对其编码他的一比特 l_i . 这样, $|L_i\rangle$ 被转变为 $U_{dp}^{l_i}|L_i\rangle$. Bob 通过相应的逻辑酉操作也对 δ_2 个诱骗逻辑量子比特编码他的检测信息. 然后, Bob 将 δ_2 个编码后的诱骗逻辑量子比特随机插入 N 个编码后的信息逻辑量子比特并将新序列传送给 Alice.

步骤 4 第二次安全检测. 在 Alice 告知 Bob 她已收到后, 他们一起完成第二次安全检测: (1) Bob 告诉 Alice δ_2 个编码后的诱骗逻辑量子比特的位置; (2) Alice 利用相应的制备基测量 δ_2 个编码后的诱骗逻辑量子比特以解码出它们携带的检测信息并向 Bob 宣布她的测量结果; (3) Bob 通过比较他的检测信息和 Alice 公布的测量结果判断是否存在 Eve. 如果存在 Eve, 他们放弃通信; 否则, 通信被继续.

步骤 5 双向通信的实现. Alice 丢弃 δ_2 个编码后的诱骗逻辑量子比特. 然后, 根据她的秘密信息和 N 个制备的信息逻辑量子比特, Alice 发送给 Bob 一个由 N 个比特组成的经典信息序列 T . 具体地讲, 如果第 i 个信息逻辑量子比特 $|L_i\rangle$ 处于 $|0_{dp}\rangle$, 经典信息序列 T 的第 i 比特 t_i 将与 Alice 的第 i 比特秘密信息 k_i 一样; 如果 $|L_i\rangle$ 处于 $|1_{dp}\rangle$, t_i 将是 k_i 的取非值. 为了解码 k_i , Bob 用 Z 基测量 $|B_i\rangle$ 并计算 $|B_i\rangle$ 的测量结果所代表的经典比特 b_i 和 t_i 的模 2 加值. 这里, $|B_i\rangle$ 的测量结果以如下方式代表一个经典比特: $|0\rangle$ ($|1\rangle$) 对应经典比特 0(1). 另一方面, Alice 通过利用 $Z \otimes Z$ -基测量 $U_{dp}^{l_i}|L_i\rangle$ 能直接读出 Bob 的一比特 l_i .

这里进一步解释 Alice 和 Bob 解码彼此秘密信息的原理. 在步骤 3, Bob 通过对 $|L_i\rangle$ 施加 $U_{dp}^{l_i}$ 对其编码

l_i 从而使 $|L_i\rangle$ 被转变为 $U_{dp}^{l_i}|L_i\rangle$, 然后把它传送给 Alice. 在步骤 5, Alice 通过利用 $Z \otimes Z$ -基测量 $U_{dp}^{l_i}|L_i\rangle$ 直接读出 l_i . 这样, Alice 就借助于量子安全直接通信的方式直接读出 Bob 的秘密信息. 另外, 利用表 1 可以清楚地看出 Bob 如何解码 Alice 的秘密信息. 从表 1 可以知道, Bob 借助于 CNOT 操作知道 Alice 制备的逻辑量子比特的初态, 并在 Alice 发送过来的一个经典信息序列的帮助下解码出 Alice 的秘密信息.

另外, 所提出的协议可被视为文献[32]的协议在集体退相位噪声情形下的推广. 其理由有以下两个方面: (1) 它们俩都借助于 CNOT 操作; (2) 后者采取单光子作为传输量子态, 而前者采用对集体退相位噪声免疫的逻辑量子比特作为传输量子态.

为清晰起见, 在忽略安全检测时, 一个具体的例子被用来进一步阐述双向通信过程. 假设 $|L_i\rangle = |1_{dp}\rangle$, $k_i = 1$ 和 $l_i = 0$. 在步骤 1, Alice 发送 $|L_i\rangle$ 给 Bob. 在步骤 3, Bob 制备 $|B_i\rangle$ 处于 $|0\rangle$ 并以 $|L_i\rangle$ 的第一个物理量子比特作为控制量子比特和 $|B_i\rangle$ 作为目标量子比特实施 CNOT 操作. 这样, $|B_i\rangle$ 被改变为 $|1\rangle$. 另外, Bob 对 $|L_i\rangle$ 施加 U_{dp}^0 以编码 l_i . 结果, $|L_i\rangle$ 被保持不变. 在步骤 5, Alice 将 k_i 的取非值(即经典比特 0)发送给 Bob. 为了解码, Bob 用 Z 基测量 $|B_i\rangle$ 从而知道 $|B_i\rangle$ 为 $|1\rangle$. 然后, Bob 通过计算 $1 \oplus 0$ 能读出 k_i 是 1. 与此同时, Alice 通过利用 $Z \otimes Z$ -基测量 $|L_i\rangle$ 能知道 l_i 为 0.

另一方面, 这里进一步考虑下所提出协议的量子测量. 在步骤 5, Z -基测量和 $Z \otimes Z$ -基测量被使用. 然而, 在步骤 2 和步骤 4, 除了 $Z \otimes Z$ -基测量外,

表 1 Bob 解码 Alice 秘密消息的原理

Table 1 Principle of Bob's decoding on Alice's secret messages

物理量	量子态或经典比特			
$ L_i\rangle$ 的初态	$ 0_{dp}\rangle$		$ 1_{dp}\rangle$	
$ B_i\rangle$ 的初态	$ 0\rangle$		$ 0\rangle$	
CNOT 操作后 $ B_i\rangle$ 的状态	$ 0\rangle$		$ 1\rangle$	
b_i	0		1	
k_i	0	1	0	1
t_i	0	1	1	0
$b_i \oplus t_i$	0	1	0	1

还需要 Bell 态测量, 因为 $\delta_1 + \delta_2$ 个诱骗逻辑量子比特中的一些被 Alice 制备处于两个态 $\{|+\rangle, |-\rangle\}$ 中的一个. 在 Hadamard 操作被施加在每个物理量子比特后, $|+\rangle$ 被转变为

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

且

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

被保持不变^[46]. 显然, $|\phi^-\rangle$ 和 $|\psi^-\rangle$ 通过 $Z \otimes Z$ -基测量能被轻易区分, 因为它们各自的两个光子具有不同的宇称. 因此, 步骤 2 和 4 中 $|+\rangle$ 和 $|-\rangle$ 需要的 Bell 态测量能被 Hadamard 操作被施加在每个物理量子比特后的单光子测量所代替. 可以得出结论, 所提出的协议仅需要单光子测量.

3 抗集体旋转噪声的鲁棒 QD 协议

一个量子信道上的集体旋转噪声能使光子的水平极化态 $|0\rangle$ 和光子的垂直极化态 $|1\rangle$ 分别改变为 $\cos\theta|0\rangle + \sin\theta|1\rangle$ 和 $-\sin\theta|0\rangle + \cos\theta|1\rangle$ ^[42], 其中 θ 是随时间变化的噪声参数. 显然, 定义为

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

和

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

的两个逻辑量子比特能抵抗这类噪声^[42]. 它们的叠加态, 即

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

和

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

也能抵抗这类噪声^[44]. 这样就形成了这类噪声下的两个逻辑测量基. 也就是, $Z_r = \{|0_r\rangle, |1_r\rangle\}$ 和 $X_r = \{|+\rangle, |-\rangle\}$. 在定义两个逻辑酉操作为 $U_r^0 = I_1 \otimes I_2$ 和 $U_r^1 = I_1 \otimes (-i\sigma_y)$ 后, 以下关系便存在^[46]:

$$\begin{aligned} U_r^1|0_r\rangle &= |1_r\rangle, U_r^1|1_r\rangle = -|0_r\rangle, \\ U_r^1|+\rangle &= -|-\rangle, U_r^1|-\rangle = |+\rangle, \end{aligned} \quad (2)$$

其中每个原始酉操作的数字下标表示它所施加的物理量子比特. 从式(2)可以明显看出, 逻辑酉操作 U_r^1 只能在每个逻辑测量基内翻转它的两个量子态, 但不能改变每个逻辑测量基本身. 这个性质是文献[4]描述的理想情况下的性质在集体旋转噪声情形下的推广.

假设 Alice 和 Bob 分别拥有 N 比特秘密信息 $\{k_1, k_2, \dots, k_i, \dots, k_N\}$ 和 N 比特秘密信息 $\{l_1, l_2, \dots, l_i, \dots, l_N\}$, 其中 $k_i, l_i \in \{0, 1\}$ ($i = 1, 2, \dots, N$). 只要具备以下不同之处, 抗集体旋转噪声的 QD 协议就可直接由抗集体退相位噪声的 QD 协议转变而来.

步骤 1: Alice 制备的 N 个信息逻辑量子比特 $\{|L_1\rangle, |L_2\rangle, \dots, |L_i\rangle, \dots, |L_N\rangle\}$ ($i = 1, 2, \dots, N$) 都随机处于两个态 $\{|0_r\rangle, |1_r\rangle\}$ 之一, $\delta_1 + \delta_2$ 个诱骗逻辑量子比特都随机处于四个态 $\{|0_r\rangle, |1_r\rangle, |+\rangle, |-\rangle\}$ 之一.

步骤 2: 第一次安全检测. 这步的描述与第 2 部分提出的 QD 协议的步骤 2 一样.

步骤 3: Bob 以 $|L_i\rangle$ 的两个物理量子比特作为控制量子比特和 $|B_i\rangle$ 作为目标量子比特对 $|L_i\rangle$ 和 $|B_i\rangle$ 施加双重 CNOT 操作. 显然, 如果 $|L_i\rangle$ 是 $|0_r\rangle$, $|B_i\rangle$ 在双重 CNOT 操作后将被保持不变; 如果 $|L_i\rangle$ 是 $|1_r\rangle$, $|B_i\rangle$ 在双重 CNOT 操作后将被转变为 $|1\rangle$. 然后, Bob 通过对 $|L_i\rangle$ 施加逻辑酉操作 $U_r^{l_i}$ 对其编码他的一比特 l_i . 这样, $|L_i\rangle$ 被转变为 $U_r^{l_i}|L_i\rangle$.

另外, Bob 通过对 $|L_i\rangle$ 施加逻辑酉操作 $U_r^{l_i}$ 对其编码他的一比特 l_i . 这样, $|L_i\rangle$ 被转变为 $U_r^{l_i}|L_i\rangle$. Bob 通过相应的逻辑酉操作也对 δ_2 个诱骗逻辑量子比特编码他的检测信息. 然后, Bob 将 δ_2 个编码后的诱骗逻辑量子比特随机插入 N 个编码后的信息逻辑量子比特并将新序列传送给 Alice.

步骤 4: 第二次安全检测. 这步的描述与第 2 部分提出的 QD 协议的步骤 4 一样.

步骤 5: Alice 发送给 Bob 的由 N 个比特组成的经典信息序列 T 与她的秘密信息和 N 个制备的信息

逻辑量子比特的关系如下: 如果第 i 个信息逻辑量子比特 $|L_i\rangle$ 处于 $|0_r\rangle$, 经典信息序列 T 的第 i 比特 t_i 将与 Alice 的第 i 比特秘密信息 k_i 一样; 如果 $|L_i\rangle$ 处于 $|1_r\rangle$, t_i 将是 k_i 的取非值. Alice 利用 Bell 态测量从 $U_r^i |L_i\rangle$ 解码出 Bob 的一比特 l_i .

这里进一步解释 Alice 和 Bob 解码彼此秘密信息的原理. 在步骤 3, Bob 通过对 $|L_i\rangle$ 施加 U_r^i 对其编码 l_i 从而使 $|L_i\rangle$ 被转变为 $U_r^i |L_i\rangle$, 然后把它传送回 Alice. 在步骤 5, Alice 通过对 $U_r^i |L_i\rangle$ 进行 Bell 态测量直接读出 l_i . 这样, Alice 就借助于量子安全直接通信的方式直接读出 Bob 的秘密信息. 另外, 从表 2 可以知道, Bob 借助于双重 CNOT 操作知道 Alice 制备的逻辑量子比特的初态, 并在 Alice 发送过来的一个经典信息序列的帮助下解码出 Alice 的秘密信息.

另外, 所提出的协议可被视为文献[32]的协议在集体旋转噪声情形下的推广. 其理由有以下两个方面: (1) 它们俩都借助于 CNOT 操作; (2) 后者采取单光子作为传输量子态, 而前者采用对集体旋转噪声免疫的逻辑量子比特作为传输量子态.

另一方面, 这里进一步考虑下所提出协议的量子测量. 步骤 5 需要区分 $|0_r\rangle$ 和 $|1_r\rangle$. 步骤 2 和步骤 4 都既需要区分 $|0_r\rangle$ 和 $|1_r\rangle$ 又需要区分 $|+_r\rangle$ 和 $|-_r\rangle$. 显然, $|0_r\rangle = |\phi^+\rangle$ 和 $|1_r\rangle = |\psi^-\rangle$ 容易通过 $Z \otimes Z$ -基测量进行区分, 因为它们各自的两个光子具有不同的宇称. 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 $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ [46].

表 2 Bob 解码 Alice 秘密信息的原理

Table 2 Principle of Bob's decoding on Alice's secret messages

物理量	量子态或经典比特			
$ L_i\rangle$ 的初态	$ 0_r\rangle$	$ 1_r\rangle$		
$ B_i\rangle$ 的初态	$ 0\rangle$	$ 0\rangle$		
双重 CNOT 操作后 $ B_i\rangle$ 的状态	$ 0\rangle$	$ 1\rangle$		
b_i	0	1		
k_i	0	1	0	1
t_i	0	1	1	0
$b_i \oplus t_i$	0	1	0	1

显然, $|\phi^-\rangle$ 和 $|\psi^+\rangle$ 容易通过 $Z \otimes Z$ -基测量进行区分, 因为它们各自的两个光子具有不同的宇称. 因此, 步骤 2 和步骤 4 中 $|+_r\rangle$ 和 $|-_r\rangle$ 之间的区分可通过 Hadamard 操作被施加在第二个物理量子比特后的单光子测量所代替. 可以得出结论, 所提出的协议仅需要单光子测量.

4 安全性分析

不失一般性, 所提出的抗集体退相位噪声的协议被用来进行安全性分析.

(1) 信息泄露问题.

明显的是, Bob 的秘密信息通过 QSDC 的方式被传送给 Alice, 其中没有经典通信被需要用于解码. Eve 不清楚 $|L_i\rangle$ 和 $U_{dp}^i |L_i\rangle$ 的量子态, 因为她无法知道它们在传输序列中的真实位置. 在这种情形下, l_i 被安全地没有任何泄露地从 Bob 传送到 Alice. 另一方面, 借助于 $|B_i\rangle$ 和来自 Alice 的经典信息序列的第 i 比特 t_i , Bob 能够准确知道 k_i 是什么. 然而, 尽管 Eve 从 Alice 收到经典信息序列的第 i 比特 t_i , 她仍然不能知道 k_i 是什么, 因为她不清楚 Bob 对 $|B_i\rangle$ 的测量结果. 这样, k_i 被安全地无泄露地从 Alice 传送到 Bob. 因此, 可以得出结论, 没有任何信息泄露发生.

(2) Eve 的主动攻击.

在所提出的协议中, 每个信息逻辑量子比特在双方之间来回传送. 这样, 两次安全检测被用来确保来回传送的安全性. 在第二次传送中, Eve 不清楚 δ_2 个编码的诱骗逻辑量子比特的真实位置. 而且, 她不能给它们选择正确的逻辑测量基, 即使她知道它们的真实位置. 这样, 她的攻击将不可避免地在它们上留下痕迹, 从而被采用信息认证的第二次安全检测检测到. 另一方面, Eve 不能得到任何秘密信息即使她截获传输序列, 因为她不能知道 N 个编码的信息逻辑量子比特的真实位置和它们的初始制备态. 可以得出结论, 所提出协议的安全性取决于第一次传送和第一次安全检测.

第一次安全检测利用随机处于四个态 $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_dp\rangle, |-_dp\rangle\}$ 之一的诱骗逻辑量子比特来检测

Eve 的存在性. Eve 的截获-重发攻击和测量-重发攻击能分别以 50% 和 25% 的概率被检测到^[49]. 同样地, 正如文献[47]所详细证明的, Eve 的纠缠-测量攻击要么不能有效地窃听到有用的信息, 要么被第一次安全检测检测到. 由于每个信息逻辑量子比特在双方之间经历了一个来回传输, Eve 的木马攻击, 包括不可见光子窃听^[53]和延迟光子木马攻击^[54], 也应当被进一步考虑. 正如文献[55]所指出的, 为了抵抗不可见光子窃听, 当他在步骤 2 接收到 $\delta_1 + \delta_2$ 个诱骗逻辑量子比特与 N 个信息逻辑量子比特相混合的量子态序列后, Bob 可以在他的装置前再插入一个过滤器滤除带有不合理波长的光子信号; 为了抵抗延迟光子木马攻击, 在步骤 2, 对于每个诱骗逻辑量子比特, Bob 采用一个光子数分离器(Photon Number Splitter, PNS)分割每个物理量子比特并统计光子数. 如果多光子率高得不合理, 通信被终止, 否则通信继续. 另外, 利用两个不同量子比特或同一个量子比特在不同时间之间的关系来提取有用信息的相关提取(Correlation-Elicitation, CE)攻击^[56], 应当也被考虑. 第一种 CE 攻击是 Eve 以两个物理量子比特作为控制量子比特和她的辅助光子作为目标量子比特对每个逻辑量子比特和她的辅助光子施加双重 CNOT 操作. 文献[49]已证实, 尽管这种 CE 攻击能通过第一次安全检测, Eve 仍然对每个逻辑量子比特的初态一点也不清楚. 第二种 CE 攻击是 Eve 以两个物理量子比特中的任何一个作为控制量子比特和她的辅助光子作为目标量子比特对每个逻辑量子比特和她的辅助光子施加一个 CNOT 操作. 文献[47]已证实, 这种 CE 攻击能以 25% 的概率被检测到.

5 讨论

(1) 信息论效率.

在文献[57]中, 信息论效率被定义为 $\eta =$

$b_s / (q_i + b_i)$, 其中 b_s , q_i 和 b_i 分别是期望收到的秘密比特数、所使用的量子比特数以及 Alice 和 Bob 之间交换的经典比特数. 在每个所提出的协议中, 在经典信息序列的第 i 比特的帮助下, $|L_i\rangle$ 和 $|B_i\rangle$ 被用于传送 k_i 和 l_i . 相应地, $b_s = 2$, $q_i = 3$ 和 $b_i = 1$. 因此, 每个所提出的协议的信息论效率为 $\eta = 2 / (3 + 1) = 50\%$.

(2) 与之前抗噪声 QD 协议的对比.

显然, 文献[47,49,50]的 QD 协议是抗噪声的. 在这种情况下, 有必要将所提出的协议与它们进行对比. 对比结果被总结在表 3 中. 从表 3 容易知道, 在初始量子资源和量子测量方面, 所提出的协议战胜文献[47,50]的协议. 而且, 所提出的协议具有最高的信息论效率.

另一方面, 文献[49]的协议也采用逻辑量子比特作为传输态, 但需要将两个相邻的逻辑量子比特制备处于相同的量子态. 幸运的是, 所提出的协议没有这种特殊的要求. 在这种意义上, 与文献[49]的协议相比, 所提出的协议在实验上更加容易执行.

6 结论

本文基于逻辑量子比特和 CNOT 操作设计两个鲁棒 QD 协议. 制备方产生逻辑量子比特作为传输态以抵抗集体噪声. 另一方借助于 CNOT 操作知道逻辑量子比特的初始制备态, 并在制备方发送过来的一个经典信息序列的帮助下解码出制备方的秘密信息. 制备方借助于量子安全直接通信读出另一方的秘密信息. 所提出协议的亮点在以下几个方面:

- (1) 它们分别在集体退相位噪声信道和集体旋转噪声信道上可行;
- (2) 它们能成功防止信息泄露问题;
- (3) 它们只需要单光子测量用于量子测量;
- (4) 与之前的抗噪声 QD 协议相比, 它们具有最

表 3 与之前的抗噪声 QD 协议的对比

Table 3 Comparisons of previous antinoise QD protocols

对比项目	文献[47]的协议	文献[49]的协议	文献[50]的协议	本文的协议
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	逻辑量子比特和单光子
量子测量	Bell 态测量	单光子测量	Bell 态测量	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

高的信息论效率;

(5) 与最近的基于逻辑量子比特的 QD 协议^[49]相比,

它们在实验上更加容易执行, 因为它们不需要制备两个相邻的逻辑量子比特处于相同的量子态.

参考文献

- 1 Long G L, Liu X S. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys Rev A*, 2002, 65: 032302
- 2 Bostrom K, Felbinger T. Deterministic secure direct communication using entanglement. *Phys Rev Lett*, 2002, 89: 187902
- 3 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
- 4 Deng F G, Long G L. Secure direct communication with a quantum one-time pad. *Phys Rev A*, 2004, 69: 052319
- 5 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
- 6 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
- 7 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
- 8 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
- 9 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 Nguyen B A. Quantum dialogue. *Phys Lett A*, 2004, 328: 6–10
- 13 Zhang Z J, Man Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. *arXiv:quant-ph/0403215*
- 14 Zhang Z J, Man Z X. Secure bidirectional quantum communication protocol without quantum channel. *arXiv:quant-ph/0403217*
- 15 Man Z X, Zhang Z J, Li Y. Quantum dialogue revisited. *Chin Phys Lett*, 2005, 22: 22–24
- 16 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
- 17 Man Z X, Xia Y J. Controlled bidirectional quantum direct communication by using a GHZ state. *Chin Phys Lett*, 2006, 23: 1680–1682
- 18 Ji X, Zhang S. Secure quantum dialogue based on single-photon. *Chin Phys*, 2006, 15: 1418–1420
- 19 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
- 20 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
- 21 Chen Y, Man Z X, Xia Y J. Quantum bidirectional secure direct communication via entanglement swapping. *Chin Phys Lett*, 2007, 24: 19–22
- 22 Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons. *Sci China Ser G-Phys Mech Astron*, 2007, 50: 558–562
- 23 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
- 24 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
- 25 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
- 26 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
- 27 Tan Y G, Cai Q Y. Classical correlation in quantum dialogue. *Int J Quant Inform*, 2008, 6: 325–329
- 28 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

- 29 Shi G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles. *Opt Commun*, 2010, 283: 5275–5278
- 30 Gao G. Two quantum dialogue protocols without information leakage. *Opt Commun*, 2010, 283: 2288–2293
- 31 Shi G F, Xi X Q, Hu M L, et al. Quantum secure dialogue by using single photons. *Opt Commun*, 2010, 283: 1984–1986
- 32 Shi G F, Tian X L. Quantum secure dialogue based on single photons and controlled-not operations. *J Mod Opt*, 2010, 57: 2027–2030
- 33 Ye T Y. Large payload bidirectional quantum secure direct communication without information leakage. *Int J Quant Inform*, 2013, 11: 1350051
- 34 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 Scr*, 2014, 89: 015103
- 35 Ye T Y. Quantum secure dialogue with quantum encryption. *Commun Theor Phys*, 2014, 62: 338–342
- 36 Ye T Y. Quantum dialogue without information leakage using a single quantum entangled state. *Int J Theor Phys*, 2014, 53: 3719–3727
- 37 Zheng C, Long G F. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. *Sci China-Phys Mech Astron*, 2014, 57: 1238–1243
- 38 Li X H, Deng F G, Zhou H Y. Efficient quantum key distribution over a collective noise channel. *Phys Rev A*, 2008, 78: 022321
- 39 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
- 40 Walton Z D, Abouraddy A F, Sergienko A V, et al. Decoherence-free subspaces in quantum key distribution. *Phys Rev Lett*, 2003, 91: 087901
- 41 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
- 42 Zhang Z J. Robust multiparty quantum secret key sharing over two collective-noise channels. *Physica A*, 2006, 361: 233–238
- 43 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
- 44 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
- 45 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
- 46 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
- 47 Yang C W, Hwang T. Quantum dialogue protocols immune to collective noise. *Quantum Inf Process*, 2013, 12: 2131–2142
- 48 Lin J, Hwang T. Bell state entanglement swappings over collective noises and their applications on quantum cryptography. *Quantum Inf Process*, 2013, 12: 1089–1107
- 49 Ye T Y. Information leakage resistant quantum dialogue against collective noise. *Sci China-Phys Mech Astron*, 2014, 57: 2266–2275
- 50 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(4): 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(4): 040301]
- 51 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
- 52 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
- 53 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A*, 2006, 351: 23–25
- 54 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 74: 145–195
- 55 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
- 56 Gao F, Wen Q Y, Zhu F C. Comment on “Quantum exam”. *Phys Lett A*, 2007, 360: 748–750
- 57 Cabello A. Quantum key distribution in the Holevo limit. *Phys Rev Lett*, 2000, 85: 5635–5638

Robust quantum dialogue based on logical qubits and controlled-not operations

YE TianYu *

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

In this paper, two robust quantum dialogue (QD) protocols against collective-dephasing noise and collective-rotation noise are proposed, respectively, by virtue of logical qubits and controlled-not (CNOT) operations. The party in charge of preparation produces logical qubits as travelling states to combat collective noise. The other party knows the initial prepared states of logical qubits with resort to the CNOT operations, and decodes out the preparation party's secret messages with the help of a classical information string sent from the preparation party. The preparation party reads out the other party's secret messages by virtue of quantum secure direct communication. In this way, the risk of information leakage is effectively avoided. Throughout the proposed protocols, only the single-photon measurements are needed for quantum measurements. Compared with previous antinoise QD protocols, the proposed protocols have the highest information-theoretical efficiency. Compared with the recent QD protocols designed by the author which need to prepare two adjacent logical qubits in the same quantum state, the proposed protocols are more experimentally feasible, as they do not have this special requirement.

quantum dialogue (QD), logical qubits, controlled-not (CNOT) operation, collective-dephasing noise, collective-rotation noise, information leakage

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

doi: 10.1360/SSPMA2014-00444