论文

基于一个共享辅助逻辑 Bell 态的抗集体噪声鲁棒量子对话

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: yetianyu@mail.zjgsu.edu.cn

收稿日期: 2014-07-28; 接受日期: 2014-09-10; 网络出版日期: 2015-01-30

国家自然科学基金资助项目(批准号: 61402407, 11375152)

摘要 本文分别提出两个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. 在每个提出的 QD 协议中, 每个由 4 物理量子比特构成的 4 个逻辑 Bell 态被用于对抗集体噪声. 信息泄露问题通过从一个通信方向另一个通信方直接两步传送辅助逻辑 Bell 态来克服. Bell 态测量而非 4 量子比特联合测量被用于解码. 抵抗窃听者主动攻击(如截获-重发攻击、测量-重发攻击、纠缠-测量攻击和木马攻击)的有效性能得到保证.

关键词 量子对话, 信息泄露, 逻辑 Bell 态, 集体退相位噪声, 集体旋转噪声, Bell 态测量

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

doi: 10.1360/SSPMA2014-00289

1 前言

众所周知, 量子安全直接通信(Quantum Secure Direct Communication, QSDC)能够利用量子信号从一个发送者向一个接收者直接传送秘密信息. 在 2002 年, Long 和 Liu^[1]提出第一个 QSDC 协议, 即基于量子态编码的两步 QSDC 协议. 同年, Bostrom 和 Felbinger^[2]利用 Einstein-Podolsky-Rosen(EPR)对提出著名的 ping-pong 协议. 在 2003 年, Deng 等人^[3]提出一个基于酉操作编码的两步 QSDC 协议. 在 2004 年, Deng 和 Long^[4]提出一个量子一次一密(One-Time Pad, OTP) QSDC 协议. 在 2005 年, Wang 等人^[5]提出一个

基于高维量子超密编码的 QSDC 协议. 同年, Wang 等人^[6]利用多粒子 Green-Horne-Zeilinger (GHZ)态提出一个多步 QSDC 协议. 在 2007 年, Li 等人^[7]提出一个量子加密 QSDC 协议. 在 2008 年, Chen 等人^[8]提出一个基于 W 态的受控 QSDC 协议. 在 2010 年, Cao 等人^[9]提出一个基于团簇态的 QSDC 协议. 在 2011 年, Gao 等人^[10]提出一个基于 3×3 维 Bell 态纠缠交换的高容量 QSDC 协议. 在 2012 年, Sun 等人^[11]提出一个基于 2 光子 4 量子比特团簇态的 QSDC 协议. 在 2013 年, Ren 等人^[12]利用光子空间 Bell 态分析提出一个鲁棒两步 QSDC 协议.

与此同时, 确定性安全量子通信(Deterministic

引用格式: 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

YE TianYu. Robust quantum dialogue based on a shared auxiliary logical Bell state against collective noise (in Chinese). Sci Sin-Phys Mech Astron, 2015, 45: 040301, doi: 10.1360/SSPMA2014-00289

Secure Quantum Communication, DSQC)也被提出来. 与 QSDC 不同的是, 接收者需要借助至少 1 比特经典信息的辅助传送才能读取秘密信息. 在 2002 年, Beige 等人^[13]提出第一个 DSQC 协议. 在 2004 年, Yan 和 Zhang^[14]提出一个基于 EPR 对和量子隐形传态的 DSQC 协议. 在 2005 年, Man 等人^[15]提出一个基于 Bell 态纠缠交换的 DSQC 协议. 在 2006 年, Li 等人^[16]提出一种基于纯纠缠态的 DSQC 协议. 在 2009 年, Xiu 等人^[17]提出一种基于 4 粒子纠缠态纠缠交换的 DSQC 协议. 接着, Qin 等人^[18]指出文献[17]的协议存在安全漏洞, 即窃听者可通过纠缠一个辅助粒子提取部分秘密信息而不被发现, 并且做了相应的改进. 同年, Xiu 等人^[19]利用五粒子量子纠缠态提出一个受控 DSQC 协议. 接着, Qin 等人^[20]指出, 在文献[19]的协议中控制者的角色可被去除, 而且窃听者可通过纠缠一个辅助粒子提取部分秘密信息而不被发现. 然后, Xiu 等人^[21]利用传输光子顺序重排和两步安全检测来修正 Qin 等人^[20]在文献发现的安全漏洞. 在 2013 年, Wang 等人^[22]提出一个基于 EPR 对和单光子的新颖的 DSQC 协议. 在 2014 年, Yuan 等人^[23]提出一个基于三粒子 GHZ 态的 DSQC 协议.

最近, 一种新颖的被称之为量子对话(Quantum Dialogue, QD)的 QSDC 得到研究者们极大的关注. QD 在 2004 年首次被 Nguyen^[24], Zhang 和 Man^[25,26]独立提出. 在 Nguyen 的协议^[24]中, Bob 首先产生足够的处于 $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ 的 EPR 对, 其中 $|0\rangle$ 和 $|1\rangle$ 分别代表光子的水平和垂直偏振态. Bob 通过对 $|\psi^+\rangle$ 施加酉操作 C_{k_n, l_n} 编码自己的 2 比特 $(k_n, l_n) (k_n, l_n \in \{0, 1\})$. 然后, Bob 将第 2 个量子比特传送给 Alice. Alice 收到后, 对第 2 个量子比特施加酉操作 C_{i_n, j_n} 来编码自己的 2 比特 $(i_n, j_n) (i_n, j_n \in \{0, 1\})$. 然后, Alice 将它传送回 Bob. Bob 收到后, 对 2 个量子比特进行 Bell 态测量, 并且等待 Alice 告诉他这是处于信息模式还是控制模式. 如果是信息模式, Bob 公布他的 Bell 态测量结果 (x_n, y_n) , 然后他们利用 $x_n = i_n \oplus k_n$ 和 $y_n = j_n \oplus l_n$ 各自解码出对方的 2 比特 ($\oplus$ 为模 2 加运算); 如果是控制模式, Alice 将她所编码的 2 比特 (i_n, j_n) 告诉 Bob 以检测量子信道的安全性.

显然, 与单向 QSDC 不同的是, 在 QD 中, 通信者同时扮演了发送者和接收者的角色. 由 2 个 QSDC 或 1 个 QSDC 和 1 个 DSQC 组成的安全量子对话, 有一些实际的应用. 目前, 许多 QD 协议^[24-36]已经被提出来以致于 QD 也得到快速发展.

对于量子保密通信, 通信安全性和实用性是它的两个主要焦点. QD 也不例外. 在 QD 的通信安全性上, Gao 等人^[37,38]在 2008 年发现 QD 总是存在信息泄露问题. 事实上, QD 中信息泄露问题的产生可被归因于 Tan 和 Cai^[39]在 2008 年发现的经典相关现象. 自从那时起, 特殊的注意力已经被集中在解决 QD 的信息泄露问题. 这样, 几种方法已经被提出用于克服它, 如 Bell 态的相关提取性^[40]、2 个 Bell 态之间纠缠交换后的测量相关性^[41]、直接传送辅助量子态^[42-45]、量子加密共享^[46]和两次 QSDC 传送^[47]. 在 QD 的实用性上, 噪声的影响应当被考虑, 因为光纤双折射的波动导致光子不可避免地被打扰. 通常, 信道噪声被视为集体噪声. 其原因在于: 光子在一个比噪声变化还快的时间窗里传输, 将受同样的噪声影响^[48,49]. 因为无消相干(Decoherence-Free, DF)态^[48-58]几乎不受集体噪声影响, 它们在对抗集体噪声上备受称誉. 特别是, DF 态也已经被引入到 QD 以使 QD 能够在集体噪声信道上工作. 例如, 在 2013 年, Yang 和 Hwang^[57]利用 2 个 2 量子比特 DF 态的乘积态来构建 2 个抗集体噪声的无信息泄露 QD 协议. 在 2014 年, Ye^[58]利用 2 量子比特 DF 态提出两个抗集体噪声的无信息泄露 QD 协议.

本文利用逻辑 Bell 态(即 4 量子比特 DF 态)分别提出两个抵抗集体退相位噪声和集体旋转噪声的鲁棒 QD 协议. 信息泄露问题通过从一个通信方向另一个通信方直接两步传送辅助逻辑 Bell 态来克服. Bell 态测量而非 4 量子比特联合测量被用于解码. 抵抗窃听者主动攻击(如截获-重发攻击、测量-重发攻击、纠缠-测量攻击和木马攻击)的有效性能得到保证.

2 QD 协议说明

2.1 基于一个共享辅助逻辑 Bell 态的抗集体退相位噪声的鲁棒 QD 协议

当极化光子 $|0\rangle$ 和 $|1\rangle$ 遭遇集体退相位噪声的变化时, 它们被分别转化为 $|0\rangle$ 和 $e^{i\varphi}|1\rangle$, 其中 φ 是随时

间变化的集体退相位噪声的参数^[51]. 为了抵抗集体退相位噪声, 每个由反宇称的两物理量子比特构成的 2 个逻辑量子比特可被定义为 $|0_{dp}\rangle = |01\rangle$ 和 $|1_{dp}\rangle = |10\rangle$ ^[51]. 这 2 个逻辑量子比特的叠加态为 $|\pm_{dp}\rangle = \frac{1}{\sqrt{2}}(|0_{dp}\rangle \pm |1_{dp}\rangle) = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, 也不受集体退相位噪声的影响^[53]. 公式(1)定义的 4 个逻辑 Bell 态^[55] 也不受集体退相位噪声的影响, 其中 $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$ 和 $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ 是 4 个逻辑 Bell 态. 显然, 这 4 个逻辑 Bell 态彼此之间可通过对第 1 和第 3 个量子比特、第 2 和第 4 个量子比特施加 2 个 Bell 态测量来区分^[55].

$$\begin{aligned}
|\Phi_{dp}^+\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|0_{dp}\rangle + |1_{dp}\rangle|1_{dp}\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|01\rangle|01\rangle + |10\rangle|10\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|00\rangle|11\rangle + |11\rangle|00\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\phi^+\rangle - |\phi^-\rangle|\phi^-\rangle)_{1234}, \\
|\Phi_{dp}^-\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|0_{dp}\rangle - |1_{dp}\rangle|1_{dp}\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|01\rangle|01\rangle - |10\rangle|10\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|00\rangle|11\rangle - |11\rangle|00\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|\phi^-\rangle|\phi^+\rangle - |\phi^+\rangle|\phi^-\rangle)_{1234}, \\
|\Psi_{dp}^+\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|1_{dp}\rangle + |1_{dp}\rangle|0_{dp}\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|01\rangle|10\rangle + |10\rangle|01\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|01\rangle|10\rangle + |10\rangle|01\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|\psi^+\rangle|\psi^+\rangle - |\psi^-\rangle|\psi^-\rangle)_{1234}, \\
|\Psi_{dp}^-\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_{dp}\rangle|1_{dp}\rangle - |1_{dp}\rangle|0_{dp}\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|01\rangle|10\rangle - |10\rangle|01\rangle)_{1234}
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{\sqrt{2}}(|01\rangle|10\rangle - |10\rangle|01\rangle)_{1234} \\
&= \frac{1}{\sqrt{2}}(|\psi^-\rangle|\psi^+\rangle - |\psi^+\rangle|\psi^-\rangle)_{1234}. \quad (1)
\end{aligned}$$

定义为公式(2)的 4 个复合酉操作能将一个逻辑 Bell 态以表 1 的方式映射到另一个^[55,56], 其中 $I = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_x = |1\rangle\langle 0| + |0\rangle\langle 1|$, $U_y = |0\rangle\langle 1| - |1\rangle\langle 0|$ 和 $U_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ 是 4 个普通的酉操作, 每个复合酉操作的下标代表 2 比特信息.

$$\begin{aligned}
\Omega_0 &= \Omega_I = I_1 \otimes I_2, \quad \Omega_{01} = \Omega_z = U_{z1} \otimes I_2, \\
\Omega_{10} &= \Omega_x = U_{x1} \otimes U_{x2}, \quad \Omega_{11} = \Omega_y = U_{y1} \otimes U_{x2}. \quad (2)
\end{aligned}$$

假设 Alice 的 $2N$ 比特秘密信息为 $\{(i_1, j_1)(i_2, j_2) \dots (i_n, j_n) \dots (i_N, j_N)\}$, Bob 的 $2N$ 比特秘密信息为 $\{(k_1, l_1)(k_2, l_2) \dots (k_n, l_n) \dots (k_N, l_N)\}$, 其中 $i_n, j_n, k_n, l_n \in \{0, 1\}$, $n \in \{1, 2, \dots, N\}$. 他们利用以下 QD 协议来在一个集体退相位噪声信道上同时交换他们的秘密信息. 该协议采用了融合块传输^[1]和两步传输^[3]的传输模式.

步骤 1 Alice 对传输量子态的制备和对第一次窃听检测的准备. Alice 产生一个由 $2N$ 个逻辑 Bell 态组成的传输量子态序列, 即 $S = \{(A_1, B_1), (A_2, B_2), \dots, (A_t, B_t), \dots, (A_{2N}, B_{2N})\}$, 其中 A_t 和 B_t ($t = 1, 2, \dots, 2N$) 分别为第 t 个逻辑 Bell 态的第 1 和第 2 个逻辑量子比特. 而且, Alice 事先使每 2 个相邻的逻辑 Bell 态 (A_{2n-1}, B_{2n-1}) 和 (A_{2n}, B_{2n}) ($n = 1, 2, \dots, N$) 处于相同的量子态(随机处于 4 个量子态 $\{|\Phi_{dp}^+\rangle, |\Phi_{dp}^-\rangle, |\Psi_{dp}^+\rangle, |\Psi_{dp}^-\rangle\}$ 之一). Alice 从每个逻辑 Bell 态挑选出第 1 个逻辑量子比特来组成一个新的序列 $S_A = \{A_1, A_2, \dots, A_{2N-1}, A_{2N}\}$.

表 1 集体退相位噪声下 4 个逻辑 Bell 态之间的映射关系
Table 1 Mapping of the four logical Bell states under the collective-dephasing noise

	$ \Phi_{dp}^+\rangle$	$ \Phi_{dp}^-\rangle$	$ \Psi_{dp}^+\rangle$	$ \Psi_{dp}^-\rangle$
Ω_I	$ \Phi_{dp}^+\rangle$	$ \Phi_{dp}^-\rangle$	$ \Psi_{dp}^+\rangle$	$ \Psi_{dp}^-\rangle$
Ω_z	$ \Phi_{dp}^-\rangle$	$ \Phi_{dp}^+\rangle$	$ \Psi_{dp}^-\rangle$	$ \Psi_{dp}^+\rangle$
Ω_x	$ \Psi_{dp}^+\rangle$	$ \Psi_{dp}^-\rangle$	$ \Phi_{dp}^+\rangle$	$ \Phi_{dp}^-\rangle$
Ω_y	$ \Psi_{dp}^-\rangle$	$ \Psi_{dp}^+\rangle$	$ \Phi_{dp}^-\rangle$	$ \Phi_{dp}^+\rangle$

剩余的逻辑量子比特构成另一个新的序列 $S_B = \{B_1, B_2, \dots, B_{2N-1}, B_{2N}\}$. 为了窃听检测, Alice 制备足够的随机处于 4 个量子态 $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$ 之一的诱骗逻辑量子比特. 然后, Alice 将它们与 S_B 随机地混合来构成一个新序列 S'_B . 最后, Alice 将 S'_B 发送给 Bob, 并将 S_A 保留在自己手中.

步骤 2 第 1 次窃听检测. 在 Alice 确认 Bob 成功收到后, 他们开始公开讨论. Alice 向 Bob 公开那些诱骗逻辑量子比特的位置和制备基. 然后, Bob 用 Alice 告诉的基测量那些诱骗逻辑量子比特, 并向 Alice 宣布他的测量结果. Alice 能容易地通过比较那些诱骗逻辑量子比特的初态和 Bob 对它们的测量结果估计出错误率. 如果错误率不合理地高, 通信被放弃; 否则, 通信被继续.

步骤 3 Alice 的编码和对第 2 次窃听检测的准备. 根据她的 2 比特秘密信息 (i_n, j_n) , Alice 对逻辑量子比特 A_{2n-1} 施加复合酉操作 $\Omega_{i_n j_n}$ 进行编码. 相应地, S_A 被转变为 $S'_A = \{\Omega_{i_1 j_1} A_1, A_2, \dots, \Omega_{i_n j_n} A_{2n-1}, A_{2n}, \dots, \Omega_{i_N j_N} A_{2N-1}, A_{2N}\}$. 为了窃听检测, Alice 制备足够的随机处于 4 个量子态 $\{|0_{dp}\rangle, |1_{dp}\rangle, |+_{dp}\rangle, |-_{dp}\rangle\}$ 之一的诱骗逻辑量子比特, 并将它们与 S'_A 随机混合来构成一个新序列 S''_A . 然后, Alice 将 S''_A 传送给 Bob.

步骤 4 第 2 次窃听检测. 在 Alice 确认 Bob 成功收到后, 他们执行第 2 次窃听检测. Alice 向 Bob 公开那些诱骗逻辑量子比特的位置和制备基. 然后, Bob 用 Alice 告诉的基测量那些诱骗逻辑量子比特, 并向 Alice 宣布他的测量结果. Alice 能容易地通过比较那些诱骗逻辑量子比特的初态和 Bob 对它们的测量结果估计出错误率. 如果错误率不合理地高, 通信被放弃; 否则, 通信被继续.

步骤 5 Bob 的编码和他们的解码. Bob 分别丢弃 S'_B 和 S''_A 中所有的诱骗逻辑量子比特. 这样, S'_B 和 S''_A 被分别改变为 S_B 和 S'_A . 然后, 根据他的 2 比特秘密信息 (k_n, l_n) , Bob 对 S'_A 中的逻辑量子比特 $\Omega_{i_n j_n} A_{2n-1}$ 施加复合酉操作 $\Omega_{k_n l_n}$ 进行编码. 相应地, S'_A 被转变为 $S'''_A = \{\Omega_{k_1 l_1} \Omega_{i_1 j_1} A_1, A_2, \dots, \Omega_{k_n l_n} \Omega_{i_n j_n} A_{2n-1}, A_{2n}, \dots, \Omega_{k_N l_N} \Omega_{i_N j_N} A_{2N-1}, A_{2N}\}$. 在手上拥有 2 个序列 S_B 和 S'''_A 后, Bob 按

顺序从每个序列挑选出 1 个逻辑量子比特, 并将 2 个相邻的逻辑 Bell 态保存为一组. 也就是说, 第 n 组为 $\{(\Omega_{k_n l_n} \Omega_{i_n j_n} A_{2n-1}, B_{2n-1}), (A_{2n}, B_{2n})\}$. 对于第 n 组的每个逻辑 Bell 态, Bob 对第 1 和第 3 个量子比特、第 2 和第 4 个量子比特施加 2 个 Bell 态测量. 然后, Bob 公开他对第 1 个逻辑 Bell 态的测量结果. 根据 Bob 的公布和她的复合酉操作 $\Omega_{i_n j_n}$, Alice 从表 1 能够解码出 Bob 的 2 比特秘密信息, 既然她自己制备 (A_{2n-1}, B_{2n-1}) . 类似地, Bob 从表 1 能读出 Alice 的 2 比特秘密信息, 因为他从对 (A_{2n}, B_{2n}) 的测量知道 (A_{2n-1}, B_{2n-1}) 的初态. 例如, 假设 (i_1, j_1) 和 (k_1, l_1) 分别是 (0,0) 和 (0,1). 而且, 假设 (A_1, B_1) 和 (A_2, B_2) 都处于 $|\Phi_{dp}^+\rangle$. 这样, 在 Alice 和 Bob 都编码后, (A_1, B_1) 被转变为 $|\Phi_{dp}^-\rangle$, 而 (A_2, B_2) 保持不变. 当 Bob 公布 (A_1, B_1) 的最终编码后的状态, Alice 能容易知道 (k_1, l_1) 为 (0,1). 同样地, Bob 能容易推断出 (i_1, j_1) 为 (0,0).

至此完成了对基于一个共享辅助逻辑 Bell 态的抗集体退相位噪声的鲁棒 QD 协议的描述. 文献[42]的 QD 协议仅在理想信道假设下可行. 所提出的 QD 协议用对集体退相位噪声免疫的逻辑 Bell 态代替文献[42]QD 协议使用的原始 Bell 态使得它在一个集体退相位噪声信道运行良好.

2.2 基于一个共享辅助逻辑 Bell 态的抗集体旋转噪声的鲁棒 QD 协议

当极化光子 $|0\rangle$ 和 $|1\rangle$ 遭遇集体旋转噪声的变化时, 它们被分别转化为 $\cos\theta|0\rangle + \sin\theta|1\rangle$ 和 $-\sin\theta|0\rangle + \cos\theta|1\rangle$, 其中 θ 是随时间变化的集体旋转噪声的参数^[53]. 为了抵抗集体旋转噪声, 每个由两物理量子比特构成的 2 个逻辑量子比特可被定义为 $|0_r\rangle = |\phi^+\rangle$ 和 $|1_r\rangle = |\psi^-\rangle$ ^[53]. 这 2 个逻辑量子比特的叠加态为 $|\pm_r\rangle = \frac{1}{\sqrt{2}}(|0_r\rangle \pm |1_r\rangle) = \frac{1}{\sqrt{2}}(|\phi^+\rangle \pm |\psi^-\rangle)$, 也不受集体旋转噪声的影响^[55]. 公式(3)定义的 4 个逻辑 Bell 态^[55]也不受集体旋转噪声的影响. 显然, 这 4 个逻辑 Bell 态彼此之间可通过对第 1 和第 3 个量子比特、第 2 和第 4 个量子比特施加 2 个 Bell 态测量

来区分^[55].

$$\begin{aligned}
 |\Phi_r^+\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle + |1_r\rangle|1_r\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\phi^+\rangle + |\psi^-\rangle|\psi^-\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\phi^+\rangle + |\psi^-\rangle|\psi^-\rangle)_{1324}, \\
 |\Phi_r^-\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_r\rangle|0_r\rangle - |1_r\rangle|1_r\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\phi^+\rangle - |\psi^-\rangle|\psi^-\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^-\rangle|\phi^-\rangle + |\psi^+\rangle|\psi^+\rangle)_{1324}, \\
 |\Psi_r^+\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_r\rangle|1_r\rangle + |1_r\rangle|0_r\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\psi^-\rangle + |\psi^-\rangle|\phi^+\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^-\rangle|\psi^+\rangle - |\psi^+\rangle|\phi^-\rangle)_{1324}, \\
 |\Psi_r^-\rangle_{1234} &= \frac{1}{\sqrt{2}}(|0_r\rangle|1_r\rangle - |1_r\rangle|0_r\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\psi^-\rangle - |\psi^-\rangle|\phi^+\rangle)_{1234} \\
 &= \frac{1}{\sqrt{2}}(|\phi^+\rangle|\psi^-\rangle - |\psi^-\rangle|\phi^+\rangle)_{1324}.
 \end{aligned} \quad (3)$$

定义为公式(4)的 4 个复合酉操作能将一个逻辑 Bell 态以表 2 的方式映射到另一个^[55,56], 其中每个复合酉操作的下标代表 2 比特信息.

$$\begin{aligned}
 \Theta_{00} &= \Theta_I = I_1 \otimes I_2, \quad \Theta_{01} = \Theta_z = U_{z1} \otimes U_{z2}, \\
 \Theta_{10} &= \Theta_x = U_{x1} \otimes U_{x2}, \quad \Theta_{11} = \Theta_y = I_1 \otimes U_{y2}. \quad (4)
 \end{aligned}$$

假设 Alice 的 $2N$ 比特秘密信息为 $\{(i_1, j_1)(i_2, j_2) \cdots (i_n, j_n) \cdots (i_N, j_N)\}$, Bob 的 $2N$ 比特秘密信息为 $\{(k_1, l_1)(k_2, l_2) \cdots (k_n, l_n) \cdots (k_N, l_N)\}$, 其中 $i_n, j_n, k_n, l_n \in \{0, 1\}$, $n \in \{1, 2, \cdots, N\}$. 显然, 2.1 节的 QD 协议在根据以下几点进行修改后能被用于抵抗集体旋转噪声:

(1) 在 2.1 节 QD 协议的步骤 1, 每 2 个相邻逻辑 Bell 态 (A_{2n-1}, B_{2n-1}) 和 (A_{2n}, B_{2n}) ($n=1, 2, \cdots, N$) 被 Alice 事先制备处于相同的量子态(随机处于 4 个量子态 $\{|\Phi_r^+\rangle, |\Phi_r^-\rangle, |\Psi_r^+\rangle, |\Psi_r^-\rangle\}$ 之一), 诱骗逻辑量子比特

表 2 集体旋转噪声下 4 个逻辑 Bell 态之间的映射关系

Table 2 Mapping of the four logical Bell states under the collective-rotation noise

	$ \Phi_r^+\rangle$	$ \Phi_r^-\rangle$	$ \Psi_r^+\rangle$	$ \Psi_r^-\rangle$
Θ_I	$ \Phi_r^+\rangle$	$ \Phi_r^-\rangle$	$ \Psi_r^+\rangle$	$ \Psi_r^-\rangle$
Θ_z	$ \Phi_r^-\rangle$	$ \Phi_r^+\rangle$	$ \Psi_r^-\rangle$	$ \Psi_r^+\rangle$
Θ_x	$ \Psi_r^+\rangle$	$ \Psi_r^-\rangle$	$ \Phi_r^+\rangle$	$ \Phi_r^-\rangle$
Θ_y	$ \Psi_r^-\rangle$	$ \Psi_r^+\rangle$	$ \Phi_r^-\rangle$	$ \Phi_r^+\rangle$

被 Alice 制备随机处于 4 个量子态 $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ 中的一个;

(2) 在步骤 3, 复合酉操作 $\Theta_{i_n j_n}$ 被 Alice 施加在逻辑量子比特 A_{2n-1} 上进行编码, 诱骗逻辑量子比特被 Alice 制备随机处于 4 个态 $\{|0_r\rangle, |1_r\rangle, |+_r\rangle, |-_r\rangle\}$ 之一;

(3) 在步骤 5, 复合酉操作 $\Theta_{k_n l_n}$ 被 Bob 施加在 S'_A 的逻辑量子比特 $\Theta_{i_n j_n} A_{2n-1}$ 上进行编码, 表 2 被 Alice 和 Bob 用于解码.

至此完成了对基于一个共享辅助逻辑 Bell 态的抗集体旋转噪声的鲁棒 QD 协议的描述. 文献[42]的 QD 协议仅在理想信道假设下可行. 所提出的 QD 协议用对集体旋转噪声免疫的逻辑 Bell 态代替文献[42]QD 协议使用的原始 Bell 态使得它在一个集体旋转噪声信道运行良好.

3 安全性分析

不失一般性, 仅对 2.1 节的 QD 协议进行安全性分析.

(1) 信息泄露问题分析.

不失一般性, 以 2.1 节的例子分析信息泄露问题. 显然, (A_2, B_2) 扮演一个共享的辅助逻辑 Bell 态的角色, 使得 Bob 知道 Alice 制备的 (A_1, B_1) 的初态. 这样, Eve 就不能知道 (A_1, B_1) 的初态. 因此, 根据表 1, 对于 Eve, Bob 对 (A_1, B_1) 最终编码后的状态的宣布对应 16 种可能性. 根据 Shannon 信息论的观点^[59], 对于 Eve, 它共包含了 $-\sum_{i=1}^{16} p_i \log_2 p_i = -16 \times \frac{1}{16} \log_2 \frac{1}{16} = 4$ 比特信息, 正好等于 2 个通信者秘密信息的总数. 可

以得出结论, 辅助逻辑 Bell 态 (A_2, B_2) 帮助所提出的 QD 协议防止信息泄露问题.

(2) 对 Eve 主动攻击的分析.

在所提出的 QD 协议中, Alice 分两步将来自于逻辑 Bell 态的 2 个逻辑量子比特序列传送给 Bob. 显然, 直到第 1 个序列被确保安全地被 Bob 接收, 第 2 个逻辑量子比特序列才被传出去. 事实上, 在第 2 次传输中, Eve 只能干扰 S'_A 的传送而不能提取任何有用信息, 因为没有人能靠仅拥有一个逻辑量子比特来区分一个逻辑 Bell 态. 其原因在于: 逻辑量子比特 A 总是处于一个完全混合态, 由于它的约化密度矩阵为 $\rho_A = \text{tr}_B \{ |\Phi_{dp}^\pm\rangle\langle\Phi_{dp}^\pm| \} = \text{tr}_B \{ |\Psi_{dp}^\pm\rangle\langle\Psi_{dp}^\pm| \} = (1/2)I$. 因此, 所提出 QD 协议的安全性决定于 S'_B 的传送.

在 S'_B 的传送中, 尽管 Eve 期望仅对携带秘密信息的传输逻辑量子比特施加她的攻击, 她将不可避免地施加攻击于诱骗逻辑量子比特, 既然她不知道它们的真实位置. 因此, Eve 的主动攻击能通过第 1 次窃听检测使用的诱骗光子技术^[60,61]被检测到.

(1) 截获-重发攻击.

Eve 事先制备一个假的由随机处于 4 个态 $\{|0_{dp}\rangle, |1_{dp}\rangle, |+\rangle, |-\rangle\}$ 之一的逻辑量子比特构成的逻辑量子比特序列. 在截获 S'_B 后, 她将假的逻辑量子比特序列代替 S'_B 发送给 Bob. 因为 Bob 对假的逻辑量子比特序列的测量结果并不总是与真实的一样, Eve 能以 50% 的概率被检测到^[58].

(2) 测量-重发攻击.

在截获 S'_B 后, Eve 随机选择 2 个测量基 $\{|0_{dp}\rangle, |1_{dp}\rangle\}$ 和 $\{|+\rangle, |-\rangle\}$ 之一来测量它, 并将它重发给 Bob. 因为 Eve 并不总是选择与 Alice 对诱骗逻辑量子比特的制备基相同的测量基, 她的攻击能以 25% 的概率被检测到^[58].

(3) 纠缠-测量攻击.

Eve 通过一个酉操作 U_E 将她的辅助光子 $E = \{|E_1\rangle, |E_2\rangle, \dots, |E_i\rangle, \dots\}$ 与 S'_B 中的逻辑量子比特相纠缠. 这样, 量子系统被转变为^[57]

$$U_E |01\rangle |E_i\rangle = \alpha_{00} |00\rangle |e_0 e_0\rangle + \alpha_{01} |01\rangle |e_0 e_1\rangle + \alpha_{10} |10\rangle |e_1 e_0\rangle + \alpha_{11} |11\rangle |e_1 e_1\rangle,$$

$$U_E |10\rangle |E_i\rangle = \beta_{00} |00\rangle |e'_0 e'_0\rangle + \beta_{01} |01\rangle |e'_0 e'_1\rangle + \beta_{10} |10\rangle |e'_1 e'_0\rangle + \beta_{11} |11\rangle |e'_1 e'_1\rangle,$$

$$U_E |\psi^+\rangle |E_i\rangle = \frac{1}{\sqrt{2}} (U_E |01\rangle |E_i\rangle + U_E |10\rangle |E_i\rangle) = \frac{1}{2} \begin{pmatrix} \langle\phi^+| (\alpha_{00} |e_0 e_0\rangle + \alpha_{11} |e_1 e_1\rangle + \beta_{00} |e'_0 e'_0\rangle + \beta_{11} |e'_1 e'_1\rangle) \\ \langle\phi^-| (\alpha_{00} |e_0 e_0\rangle - \alpha_{11} |e_1 e_1\rangle + \beta_{00} |e'_0 e'_0\rangle - \beta_{11} |e'_1 e'_1\rangle) \\ \langle\psi^+| (\alpha_{01} |e_0 e_1\rangle + \alpha_{10} |e_1 e_0\rangle + \beta_{01} |e'_0 e'_1\rangle + \beta_{10} |e'_1 e'_0\rangle) \\ \langle\psi^-| (\alpha_{01} |e_0 e_1\rangle - \alpha_{10} |e_1 e_0\rangle + \beta_{01} |e'_0 e'_1\rangle - \beta_{10} |e'_1 e'_0\rangle) \end{pmatrix},$$

$$U_E |\psi^-\rangle |E_i\rangle = \frac{1}{\sqrt{2}} (U_E |01\rangle |E_i\rangle - U_E |10\rangle |E_i\rangle) = \frac{1}{2} \begin{pmatrix} \langle\phi^+| (\alpha_{00} |e_0 e_0\rangle + \alpha_{11} |e_1 e_1\rangle - \beta_{00} |e'_0 e'_0\rangle - \beta_{11} |e'_1 e'_1\rangle) \\ \langle\phi^-| (\alpha_{00} |e_0 e_0\rangle - \alpha_{11} |e_1 e_1\rangle - \beta_{00} |e'_0 e'_0\rangle + \beta_{11} |e'_1 e'_1\rangle) \\ \langle\psi^+| (\alpha_{01} |e_0 e_1\rangle + \alpha_{10} |e_1 e_0\rangle - \beta_{01} |e'_0 e'_1\rangle - \beta_{10} |e'_1 e'_0\rangle) \\ \langle\psi^-| (\alpha_{01} |e_0 e_1\rangle - \alpha_{10} |e_1 e_0\rangle - \beta_{01} |e'_0 e'_1\rangle + \beta_{10} |e'_1 e'_0\rangle) \end{pmatrix}, \quad (5)$$

其中 $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = |\beta_{00}|^2 + |\beta_{01}|^2 + |\beta_{10}|^2 + |\beta_{11}|^2 = 1$, $|e_0 e_0\rangle$, $|e_0 e_1\rangle$, $|e_1 e_0\rangle$ 和 $|e_1 e_1\rangle$ 是 Eve 的探测态. 为了通过第一次窃听检测, Eve 应当使得

$$\alpha_{00} = \alpha_{10} = \alpha_{11} = \beta_{00} = \beta_{01} = \beta_{11} = 0, \quad (6)$$

如果诱骗逻辑量子比特是 $|0_{dp}\rangle$ 或 $|1_{dp}\rangle$; Eve 应当使得

$$\alpha_{01} |e_0 e_1\rangle - \alpha_{10} |e_1 e_0\rangle + \beta_{01} |e'_0 e'_1\rangle - \beta_{10} |e'_1 e'_0\rangle = \alpha_{01} |e_0 e_1\rangle + \alpha_{10} |e_1 e_0\rangle - \beta_{01} |e'_0 e'_1\rangle - \beta_{10} |e'_1 e'_0\rangle = \mathbf{0}, \quad (7)$$

其中 $\mathbf{0}$ 是一个零向量, 如果诱骗逻辑量子比特是 $|+\rangle$ 或 $|-\rangle$. 显然, 只有当(6)和(7)式都成立, Eve 才将不会被检测到. 在将(6)代入(7)式后, 可得到

$$\alpha_{01} |e_0 e_1\rangle = \beta_{10} |e'_1 e'_0\rangle. \quad (8)$$

(8)式意味着 Eve 不能区分 $\alpha_{01} |e_0 e_1\rangle$ 和 $\beta_{10} |e'_1 e'_0\rangle$. 这样, Eve 也无法区分 $|0_{dp}\rangle$ 和 $|1_{dp}\rangle$. 因此, Eve 通过测量她的辅助光子将不能得到任何有用的东西. 另一方面, 如果 Eve 试图通过使 $\alpha_{01} |e_0 e_1\rangle \neq \beta_{10} |e'_1 e'_0\rangle$ 来区分她的辅助光子以得到部分有用信息, 根据(7)式, 她将干扰诱骗逻辑量子比特 $|+\rangle$ 和 $|-\rangle$, 从而无疑将在第一次窃听检测被 Alice 和 Bob 检测到^[57].

(4) 木马攻击.

因为没有逻辑量子比特在所提出的 QD 协议被

来回传送, 这就没必要去担心木马攻击策略, 包括不可见光子窃听^[62]和延迟光子木马攻击^[63]. 换句话说, 所提出的 QD 协议对木马攻击策略具有完美的安全性.

4 讨论

(1) 信息论效率.

在文献 [64] 中, Cabello 定义信息论效率为 $\eta = b_s / (q_t + b_t)$, 其中 b_s , q_t 和 b_t 分别是期望收到的秘密比特数、使用的量子比特数和通信者间交换的经典比特数. 在所提出的抗集体退相位噪声(集体旋转噪声)QD 协议中, 不考虑窃听检测, 每 2 个相邻的逻辑 Bell 态 (A_{2n-1}, B_{2n-1}) 和 (A_{2n}, B_{2n}) 能被用于编码四经典比特(即 Alice 的 2 比特和 Bob 的 2 比特). 而且, 对 $(\Omega_{k_n l_n} \Omega_{i_n j_n} A_{2n-1}, B_{2n-1}) ((\Theta_{k_n l_n} \Theta_{i_n j_n} A_{2n-1}, B_{2n-1}))$ 测量结果的宣布需要消耗两经典比特. 相应地, 可以得到 $b_s = 4$, $q_t = 8$ 和 $b_t = 2$. 因此, 所提出的抗集体退相位噪声(集体旋转噪声)QD 协议的信息论效率为 $\eta = 4 / (8 + 2) \times 100\% = 40\%$.

表 3 与之前的抗集体噪声的无信息泄露 QD 协议的对比
Table 3 Comparisons of previous information leakage resistant QD protocols against collective noise

	文献[57]的 协议	文献[58]的 协议	本文提出的 QD 协议
初始量子资源	2 个 Bell 态的 乘积态	逻辑量子比特	逻辑 Bell 态
量子测量	Bell 态测量	单粒子测量	Bell 态测量
信息论效率	40%	33.3%	40%
量子信道容量	每轮 2 比特	每轮 2 比特	每轮 4 比特

(2) 与之前的无信息泄露 QD 协议的对比.

尽管文献[40–47]的 QD 协议不存在信息泄露问题, 它们仅工作在理想信道假设下. 可以直接得到, 所提出的 2 个 QD 协议在集体噪声信道的实际可行性上胜过它们.

而且, 不考虑窃听检测过程, 这里再对所提出的 QD 协议和之前的抗集体噪声的无信息泄露 QD 协议之间在初始量子资源、量子测量、信息论效率和量子信道容量方面进行对比. 对比结果被列在表 3. 从表 3 可以看出, 所提出的 QD 协议在量子信道容量上胜过文献[57]的协议而输了初始量子资源, 因为逻辑 Bell 态的制备比 2 个 Bell 态的乘积态的制备更复杂. 另一方面, 所提出的 QD 协议在信息论效率和量子信道容量上都胜过文献[58]的协议而输了初始量子资源和量子测量.

5 结论

本文分别提出两个抵抗集体退相位噪声和集体旋转噪声的鲁棒 QD 协议. 在每个提出的 QD 协议中, 每个由 4 物理量子比特构成的 4 个逻辑 Bell 态被用于对抗集体噪声. 信息泄露问题通过从一个通信方向另一个通信方直接两步传送辅助逻辑 Bell 态来克服. Bell 态测量而非 4 量子比特联合测量被用于解码. 抵抗窃听者主动攻击(如截获-重发攻击、测量-重发攻击、纠缠-测量攻击和木马攻击)的有效性能得到保证. 本文的 2 个 QD 协议在理论上是可行的. 虽然目前的技术在实际中制备和保存 4 量子比特纠缠态还存在困难, 但随着量子技术的进步, 这些实际执行上的困难将会逐步被克服.

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

- 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 Cao W F, Yang Y G, Wen Q Y. Quantum secure direct communication with cluster states. *Sci China-Phys Mech Astron*, 2010, 53: 1271–1275
- 10 Gao G, Fang M, Yang R M. Quantum secure direct communication by swapping entanglements of 3x3-dimensional Bell states. *Int J Theor Phys*, 2011, 50: 882–887
- 11 Sun Z W, Du R G, Long D Y. Quantum secure direct communication with two-photon four-qubit cluster states. *Int J Theor Phys*, 2012, 51: 1946–1952
- 12 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
- 13 Beige A, Englert B G, Kurtsiefer C, et al. Secure communication with a publicly known key. *Acta Phys Pol A*, 2002, 101: 357–368
- 14 Yan F L, Zhang X Q. A scheme for secure direct communication using EPR pairs and teleportation. *Eur Phys J B*, 2004, 41: 75–78
- 15 Man Z X, Zhang Z J, Li Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. *Chin Phys Lett*, 2005, 22: 18–21
- 16 Li X H, Deng F G, Li C Y, et al. Deterministic secure quantum communication without maximally entangled states. *J Korean Phys Soc*, 2006, 49: 1354–1359
- 17 Xiu X M, Dong H K, Dong L, et al. Deterministic secure quantum communication using four-particle genuine entangled state and entanglement swapping. *Opt Commun*, 2009, 282: 2457–2459
- 18 Qin S J, Wen Q Y, Lin S, et al. Cryptanalysis and improvement of a DSQC using four-particle entangled state and entanglement swapping. *Opt Commun*, 2009, 282: 4017–4019
- 19 Xiu X M, Dong L, Gao Y J, et al. Controlled deterministic secure quantum communication using five-qubit entangled states and two-step security test. *Opt Commun*, 2009, 282: 333–337
- 20 Qin S J, Wen Q Y, Meng L M, et al. Comment on “Controlled DSQC using five-qubit entangled states and two-step security test”. *Opt Commun*, 2009, 282: 2656–2658
- 21 Xiu X M, Dong L, Gao Y J, et al. A revised controlled deterministic secure quantum communication with five-photon entangled state. *Opt Commun*, 2010, 283: 344–347
- 22 Wang C, Liu J W, Liu X, et al. A novel deterministic secure quantum communication scheme with Einstein-Podolsky-Rosen pairs and single photons. *Commun Theor Phys*, 2013, 60: 397–404
- 23 Yuan H, Zhang Q, Hong L, et al. Scheme for deterministic secure quantum communication with three-qubit GHZ state. *Int J Theor Phys*, 2014, 53: 2558–2564
- 24 Nguyen B A. Quantum dialogue. *Phys Lett A*, 2004, 328: 6–10
- 25 Zhang Z J, Man Z X. Secure direct bidirectional communication protocol using the Einstein-Podolsky-Rosen pair block. *arXiv: quant-ph/0403215v1*
- 26 Zhang Z J, Man Z X. Secure bidirectional quantum communication protocol without quantum channel. *arXiv: quant-ph/0403217v4*
- 27 Man Z X, Zhang Z J, Li Y. Quantum dialogue revisited. *Chin Phys Lett*, 2005, 22: 22–24
- 28 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
- 29 Man Z X, Xia Y J. Controlled bidirectional quantum direct communication by using a GHZ state. *Chin Phys Lett*, 2006, 23: 1680–1682
- 30 Ji X, Zhang S. Secure quantum dialogue based on single-photon. *Chin Phys*, 2006, 15: 1418–1420
- 31 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
- 32 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
- 33 Chen Y, Man Z X, Xia Y J. Quantum bidirectional secure direct communication via entanglement swapping. *Chin Phys Lett*, 2007, 24: 19–22
- 34 Yang Y G, Wen Q Y. Quasi-secure quantum dialogue using single photons. *Sci China Ser G-Phys Mech Astron*, 2007, 50: 558–562
- 35 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
- 36 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
- 37 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
- 38 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
- 39 Tan Y G, Cai Q Y. Classical correlation in quantum dialogue. *Int J Quant Inform*, 2008, 6: 325–329
- 40 Shi G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles. *Opt Commun*, 2010, 283: 5275–5278
- 41 Gao G. Two quantum dialogue protocols without information leakage. *Opt Commun*, 2010, 283: 2288–2293
- 42 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
- 43 Shi G F, Xi X Q, Hu M L, et al. Quantum secure dialogue by using single photons. *Opt Commun*, 2010, 283: 1984–1986
- 44 Ye T Y. Large payload bidirectional quantum secure direct communication without information leakage. *Int J Quant Inform*, 2013, 11: 1350051
- 45 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
- 46 Ye T Y. Quantum secure dialogue with quantum encryption. *Commun Theor Phys*, 2014, 62: 338–342
- 47 Zheng C, Long G F. Quantum secure direct dialogue using Einstein-Podolsky-Rosen pairs. *Sci China-Phys Mech Astron*, 2014, 57: 1238–1243
- 48 Li X H, Deng F G, Zhou H Y. Efficient quantum key distribution over a collective noise channel. *Phys Rev A*, 2008, 78: 022321
- 49 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
- 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 Walton Z D, Abouraddy A F, Sergienko A V, et al. Decoherence-free subspaces in quantum key distribution. *Phys Rev Lett*, 2003, 91: 087901
- 52 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
- 53 Zhang Z J. Robust multiparty quantum secret key sharing over two collective-noise channels. *Phys A*, 2006, 361: 233–238
- 54 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
- 55 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
- 56 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
- 57 Yang C W, Hwang T. Quantum dialogue protocols immune to collective noise. *Quantum Inf Process*, 2013, 12: 2131–2142
- 58 Ye T Y. Information leakage resistant quantum dialogue against collective noise. *Sci China-Phys Mech Astron*, 2014, 57(12): 2266–2275
- 59 Shannon C E. Communication theory of secrecy system. *Bell Syst Tech J*, 1949, 28: 656–715
- 60 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
- 61 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
- 62 Cai Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys Lett A*, 2006, 351: 23–25
- 63 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. *Rev Mod Phys*, 2002, 74: 145–195
- 64 Cabello A. Quantum key distribution in the Holevo limit. *Phys Rev Lett*, 2000, 85: 5635–5638

Robust quantum dialogue based on a shared auxiliary logical Bell state against collective noise

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 presented, respectively. In each of the proposed QD protocols, four logical Bell states, each of which is made up of four physical qubits, are used to combat collective noise. The information leakage problem is overcome by directly transmitting the auxiliary logical Bell states in two steps from one communication party to the other. For decoding, Bell state measurements rather than four-qubit joint measurements are used. The effectiveness against an eavesdropper's active attacks such as the intercept-resend attack, the measure-resend attack, the entangle-measure attack and the Trojan horse attack can be guaranteed.

quantum dialogue (QD), information leakage, logical Bell state, collective-dephasing noise, collective-rotation noise, Bell state measurement

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

doi: 10.1360/SSPMA2014-00289