引用本文：常利伟，张宇青，田晓雄，等. 集体噪声信道中错误容忍的可控量子对话[J]. 光通信技术，2020，44(9)：7–12.

集体噪声信道中错误容忍的可控量子对话

常利伟，张宇青，田晓雄，白增亮

（山西财经大学 信息学院，太原 030006）

摘要：量子通信中信道噪声将会影响信息传输的可靠性和有效性。设计了 2 个能够分别抵抗集体退相位噪声和集体旋转噪声的可控量子对话(CQD)协议。分析表明：该协议不仅可以避免集体噪声的影响，具有更强的实用性，还可以避免信息泄露，且能有效减少控制方的在线时间，同时能够抵抗外部和内部攻击。

关键词：集体噪声；逻辑簇态；量子对话；信息泄露；内部攻击

中图分类号：TN918.1　**文献标志码**：A　**文章编号**：1002-5561(2020)09-0007-06

DOI：10.13921/j.cnki.issn1002–5561.2020.09.002　**开放科学(资源服务)标识码(OSID)**：

Fault tolerant controlled quantum dialogue in collective noise channel

CHANG Liwei, ZHANG Yuqing, TIAN Xiaoxiong, BAI Zengliang

(College of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China)

Abstract: In quantum communication, channel noise will affect the reliability and effectiveness of information transmission. Two controllable quantum dialogue(CQD) protocols are designed, which can resist collective-dephasing noise and collective-rotation dialogue noise respectively. The comparative analysis shows that the protocol can not only avoid the impact of collective noise, but also avoid information leakage, and effectively reduce the online time of the controller, and can resist external and internal attacks.

Key words: collective noise; logical cluster states; quantum dialogue; information leakage; internal attacks

0 引言

量子保密通信的安全性基于量子力学基本原理，具有理论上的无条件安全性。量子对话(QD)[1–5]作为量子保密通信的一个重要分支，是一种允许通信双方同时直接交换秘密信息的通信方式。第三方可控量子对话(CQD)在 QD 中加入了控制方以监督通信双方秘密信息的交换。2006 年，Man 等人[6]提出了第一个 CQD 协议，之后 Ye 和 Liu 等人[7–9]从信息论角度分析、讨论了如何避免 CQD 协议存在的信息泄露问题。2013 年，Yang 等人[10]利用五粒子布朗态作为载体实现了效率较高的 CQD 协议。2016 年，Kao 等人[11–12]发现一种普遍存在于 CQD 协议中的共谋攻击并设计出能够抵抗此类攻击的 CQD 协议。同时，他们也指出一个安全的 CQD 协议必须满足 3 个安全性条件：①通信双方的秘密信息不能泄露给包括控制方在内的任何人；②通信双方只有在获得控制方允许后才能得到对方的秘密信息；③没有控制方的允许，通信双方不能共谋获得对方信息。2019 年，Liu 等人[13–14]指出文献[11–12]中协议还存在来自不诚信控制方的攻击，也就是不同初始态(DIS)攻击和拒绝服务(DoS)攻击，并且设计出了改进协议以及提出了一个新的安全性条件：通信双方必须具备能够抵抗不诚信控制方攻击的能力。

然而，以上 CQD 协议都是基于理想环境设计的。由于光子旅行的时间窗比噪声源变化短，光子在实际量子信道中传输时必然会受到噪声的影响，其势必导致信息载体发生改变以至于引入错误。而窃听者则可

收稿日期：2019–12–04。

基金项目：山西省自然科学基金(批准号：201801D221159)资助；山西省高校科技创新基金(批准号：2019L0470、2019L0479)资助；山西省教育科学“十三五”规划项目(批准号：GH–17035)资助；山西重点研发计划项目(批准号：201903D421003)资助。

作者简介：常利伟(1986—)，男，山西怀仁人，博士，副教授，硕士生导师，中国计算机学会会员，中国密码学会会员，山西省区块链研究会理事。主要研究方向是经典密码算法、量子保密通信和网络安全态势感知。参与国家级项目 4 项，负责完成或在研省部级项目 3 项；获省部级教学成果一等奖。

以在噪声的掩盖下窃取甚至破坏秘密信息。集体噪声是主要的噪声源之一，但是，目前集体噪声下 CQD 协议[15-16]的相关研究成果较少。因此，本文提出 2 个集体噪声信道上错误容忍的 CQD 协议：一个用来抵抗集体退相位噪声；另一个用来抵抗集体旋转噪声。

1 CQD 协议

1.1 集体退相位噪声信道中错误容忍的 CQD 协议

在集体退相位噪声环境下，光子的水平极化状态 $|0\rangle$ 不发生变化，而光子的垂直极化状态 $|1\rangle$ 将被改变为 $e^{i\varphi}|1\rangle$（φ 是随时间波动的噪声参数）。为了避免这类噪声对量子态的影响，本文构造了 2 个逻辑量子比特：$|0_{dp}\rangle=|01\rangle$ 和 $|1_{dp}\rangle=|10\rangle$。这 2 个逻辑量子比特的叠加态 $|+_{dp}\rangle=\frac{1}{2}(|0_{dp}\rangle+|1_{dp}\rangle)$ 和 $|-_{dp}\rangle=\frac{1}{2}(|0_{dp}\rangle-|1_{dp}\rangle)$ 在该噪声信道中也不发生变化。因此，集体退相位噪声下的 2 组测量基可选为 $\{|0_{dp}\rangle,|1_{dp}\rangle\}$ 和 $\{|+_{dp}\rangle,|-_{dp}\rangle\}$。为了使测量基的基底可以相互转换，本文选用了 2 个逻辑幺正变换 $U_0^{dp}=I_1\otimes I_2$ 和 $U_1^{dp}=(-\sigma_x)_1\otimes(-i\sigma_y)_2$，其中下角标 1 和 2 分别表示逻辑量子比特的第一个和第二个量子比特，且 $I=|0\rangle\langle 0|+|1\rangle\langle 1|$，$\sigma_x=|0\rangle\langle 1|+|1\rangle\langle 0|$ 和 $-i\sigma_y=|1\rangle\langle 0|-|0\rangle\langle 1|$ 是 3 个幺正变换。幺正变换 U_1^{dp} 对每个逻辑量子比特的影响可表示为：$U_1^{dp}|0_{dp}\rangle=|1_{dp}\rangle$，$U_1^{dp}|1_{dp}\rangle=-|0_{dp}\rangle$，$U_1^{dp}|+_{dp}\rangle=-|-_{dp}\rangle$ 和 $U_1^{dp}|-_{dp}\rangle=|+_{dp}\rangle$。

假定通信双方为 Alice 和 Bob，控制方为 Charlie。集体退相位噪声信道中错误容忍的第三方 CQD 协议的工作流程如图 1 所示，其由以下 8 个步骤构成：

①分发逻辑量子态。Alice 向 Charlie 发送通信请求。Charlie 制备 $2N$ 个逻辑簇态：

$$\begin{aligned}|\Xi_{dp}\rangle=&\frac{1}{2}(|0_{dp}0_{dp}0_{dp}0_{dp}\rangle+|0_{dp}0_{dp}1_{dp}1_{dp}\rangle+\\&|1_{dp}1_{dp}0_{dp}0_{dp}\rangle-|1_{dp}1_{dp}1_{dp}1_{dp}\rangle)_{A_1B_1A_2B_2}\\=&\frac{1}{2}(|01010101\rangle+|01011010\rangle+\\&|10100101\rangle-|10101010\rangle)_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}\end{aligned}\quad(1)$$

首先，将其划分为 2 个量子比特序列 S_A 和 S_B，其中序列 S_A 由所有的逻辑量子比特 A_1 和 A_2 组成，序列 S_B 则由所有的逻辑量子比特 B_1 和 B_2 组成。随后，Charlie 对逻辑量子比特 A_2 实施随机的幺正变换 U_0^{dp} 或者 U_1^{dp} 形成 S'_A 并记录该操作生成许可。最后，Charlie 在 S'_A 和 S_B 中随机插入足够数量的诱骗态得到新的序列 Q_A 和 Q_B 并分别发送给 Alice 和 Bob，其中每个诱骗态随机地处于 $\{|0_{dp}\rangle,|1_{dp}\rangle,|+_{dp}\rangle,|-_{dp}\rangle\}$ 4 个态之一。

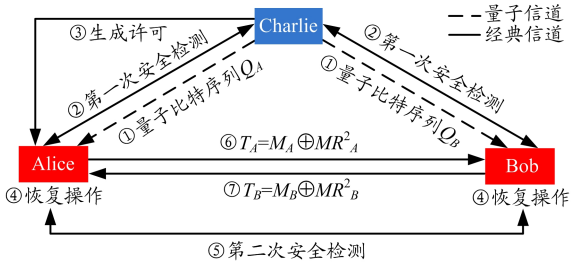

图 1 集体退相位噪声信道中错误容忍的第三方 CQD 协议

②第一次安全检测。在收到 Q_A 和 Q_B 后，Alice 和 Bob 分别与 Charlie 公开讨论序列中的诱骗态。若错误率低于阈值，则他们认为此次通信安全并丢弃诱骗态，否则中止通信。

③生成许可。若 Charlie 允许 Alice 和 Bob 进行通信，他将告诉 Alice 他的许可，即他在第 1 步实施的幺正变换，之后 Alice 实施与 Charlie 相同的幺正变换以还原初始的量子比特序列 S_A 和 S_B。

④恢复四粒子簇态。集体退相位噪声下四粒子簇态的恢复过程线路图如图 2 所示。图中横线从上到下分别表示量子比特 A_1^1、A_1^2、B_1^1、B_1^2、A_2^1、A_2^2、B_2^1 和 B_2^2。Alice 以逻辑量子比特 $A_1(A_2)$ 中的 $A_1^1(A_2^1)$ 为控制比特，$A_1^2(A_2^1)$ 为目标比特实施 CNOT 操作。同时，Bob 以逻辑量子比特 $B_1(B_2)$ 中的 $B_1^1(B_2^1)$ 为控制比特，$B_1^2(B_2^2)$ 为目标比特实施 CNOT 操作。此时逻辑簇态 $|\Xi_{dp}\rangle$ 将转变为：

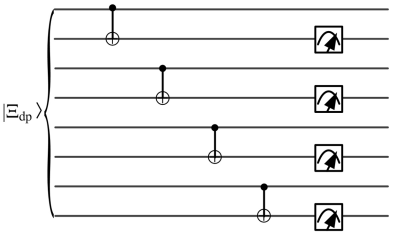

图 2 集体退相位噪声下四粒子簇态的恢复过程线路图

$$\begin{aligned}|\Theta_{dp}\rangle=&\frac{1}{2}(|01010101\rangle+|01011111\rangle+|11110101\rangle-\\&|11111111\rangle)_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}\end{aligned}\quad(2)$$

最后，Alice(Bob) 对量子比特 $A_1^2(B_1^2)$ 和 $A_2^2(B_2^2)$ 分别执行 Z 基测量，$|\Theta_{dp}\rangle$ 将塌缩为 $|\zeta\rangle=\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{A_1^1B_1^1A_2^1B_2^1}$，显然他们成功地恢复并共享了四粒子簇态。为了表达简洁且便于理解，本文将用 $A_1B_1A_2B_2$ 代替下角标 $A_1^1B_1^1A_2^1B_2^1$。

⑤第二次安全检测。为了检测 Charlie 是否诚信，Bob 随机从序列 S_B 中选择 N 个量子比特，并且通知 Alice 从序列 S_A 中选择对应位置的量子比特。四粒子簇态在不同测量基下测得的结果是不同的(如 Z 基、Z 基、X 基和 X 基；X 基、X 基、Z 基和 Z 基)，因此 Bob 随机选择一组测量基进行测量并将选择的测量基告诉 Alice。之后，Alice 和 Bob 根据式(3)比较它们的测量结果，并判断 Charlie 是否诚信。如果错误率低于阈值，则 Alice 和 Bob 认为 Charlie 是诚信的并继续下一步，否则此次通信被中止。其中，四粒子簇态在不同测量基下可表示为：

$$\begin{aligned}|\zeta\rangle=&\frac{1}{2}(|0000\rangle+|0011\rangle+|1100\rangle-\\&|1111\rangle)_{A_1B_1A_2B_2}\\=&\frac{1}{2}(|00{+}{+}\rangle+|00{-}{-}\rangle+|11{+}{-}\rangle+\\&|11{-}{+}\rangle)_{A_1B_1A_2B_2}\\=&\frac{1}{2}(|{+}{+}00\rangle+|{-}{-}00\rangle+|{+}{-}11\rangle+\\&|{-}{+}11\rangle)_{A_1B_1A_2B_2}\end{aligned}\tag{3}$$

⑥传输 Alice 的信息。Alice 用 Z 基测量量子比特 A_1 以及用 X 基测量量子比特 A_2，测量结果分别被表示为 MR_A^1 和 MR_A^2，其中用 0 表示测量结果 $|0\rangle$ 和 $|+\rangle$，用 1 表示测量结果 $|1\rangle$ 和 $|-\rangle$。之后，Alice 传输经典信息 $T_A=MR_A^2\oplus M_A$ 给 Bob，其中 M_A 是 Alice 的秘密信息。

⑦传输 Bob 的信息。类似于 Alice，Bob 用 Z 基测量量子比特 B_1 并用 X 基测量量子比特 B_2，测量结果分别被表示为 MR_B^1 和 MR_B^2。之后，Bob 传输经典信息 $T_B=M_B\oplus MR_B^2$ 给 Alice，其中 M_B 是 Bob 的秘密信息。

⑧获取秘密信息。Alice 根据自己的测量结果 MR_A^1 和 MR_A^2，以及式(3)可以推断出 MR_B^2，各量子比特的测量结果之间的关系以及解码规则如表 1 所示。Alice 由此可以根据 Bob 公布的经典信息 T_B 推断出 Bob 的秘密信息为 $M_B=MR_B^2\oplus T_B$。类似地，Bob 也能够推断出 Alice 的秘密信息 $M_A=MR_A^2\oplus T_A$。

表 1 各量子比特测量结果之间的关系以及解码规则

测量数据属性	解码规则			
MR_A^1	$0(\|0\rangle)$	$0(\|0\rangle)$	$1(\|1\rangle)$	$1(\|1\rangle)$
MR_B^1	$0(\|0\rangle)$	$0(\|0\rangle)$	$1(\|1\rangle)$	$1(\|1\rangle)$
MR_A^2	$0(\|+\rangle)$	$1(\|-\rangle)$	$0(\|+\rangle)$	$1(\|-\rangle)$
MR_B^2	$0(\|+\rangle)$	$1(\|-\rangle)$	$1(\|-\rangle)$	$0(\|+\rangle)$

1.2 集体旋转噪声信道中错误容忍的 CQD 协议

偏振光子 $|0\rangle$ 和 $|1\rangle$ 在集体旋转噪声信道中传输时将不可避免地分别被改变为 $U_r|0\rangle=\cos\theta|0\rangle+\sin\theta|1\rangle$ 和 $U_r|1\rangle=-\sin\theta|0\rangle+\cos\theta|1\rangle$($\theta$ 是集体旋转噪声参数并且随时间波动)。事实上，2 个 Bell 态 $|\varphi^+\rangle$ 和 $|\psi^-\rangle$ 具有抗集体旋转噪声功能，其在集体旋转噪声环境下状态不发生改变。因此，在集体旋转噪声下可构造 2 个逻辑量子比特和 $|0_r\rangle=|\varphi^+\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$、$|1_r\rangle=|\psi^-\rangle=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)$ 来免疫此类噪声。同时，这 2 个逻辑量子比特的叠加态 $|+_r\rangle=\frac{1}{\sqrt{2}}(|0_r\rangle+|1_r\rangle)$ 和 $|-_r\rangle=\frac{1}{\sqrt{2}}(|0_r\rangle-|1_r\rangle)$ 也能够免疫该噪声。因此，集体旋转噪声下的 2 组测量基可表示为 $\{|0_r\rangle,|1_r\rangle\}$ 和 $\{|+_r\rangle,|-_r\rangle\}$。为了使每组测量基的基底可以相互转换，本文选用 2 个逻辑幺正变换 $U_0^r=I_1\otimes I_2$ 和 $U_1^r=I_1\otimes(-i\sigma_y)_2$，其中下角标 1 和 2 分别表示逻辑量子比特的第一个和第二个量子比特，且 $I=|0\rangle\langle0|+|1\rangle\langle1|$ 和 $-i\sigma_y=|1\rangle\langle0|-|0\rangle\langle1|$ 是 2 个幺正变换。幺正变换 U_1^r 对每个逻辑量子比特的影响为：$U_1^r|0_r\rangle=|1_r\rangle$，$U_1^r|1_r\rangle=-|0_r\rangle$，$U_1^r|+_r\rangle=-|-_r\rangle$ 和 $U_1^r|-_r\rangle=|+_r\rangle$。

整体而言，集体旋转噪声下的 CQD 协议类似于上一节所提的集体退相位噪声下的 CQD 协议，其不同之处主要体现在 2 个方面：初始逻辑簇态的分发方式和四粒子簇态的恢复方式。

◆分发逻辑量子态。Alice 向 Charlie 发送通信请求。Charlie 制备 $2N$ 个逻辑簇态如下：

$$\begin{aligned}|\Xi_r\rangle=&\frac{1}{2}(|0_r0_r0_r0_r\rangle+|0_r0_r1_r1_r\rangle)+|1_r1_r0_r0_r\rangle-\\&|1_r1_r1_r1_r\rangle)_{A_1B_1A_2B_2}\\=&\frac{1}{8}[(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)\otimes\\&(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)+\\&(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)\otimes\\&(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)+\\&(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)\otimes\\&(|00\rangle+|11\rangle)(|00\rangle+|11\rangle)-\\&(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)\otimes\\&(|01\rangle-|10\rangle)(|01\rangle-|10\rangle)]_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}\end{aligned}\tag{4}$$

随后，Charlie 随机实施幺正变换 U_0^r 或者 U_1^r 生成的许可并在 2 个序列中随机插入足够数量的诱骗态，每个诱骗态随机地处于 $\{|0_r\rangle,|1_r\rangle,|+_r\rangle,|-_r\rangle\}$ 4 个态之一。

◆恢复四粒子簇态。集体旋转噪声下四粒子簇态的恢复过程如图 3所示，图中横线从上到下分别表示量子比特 A_1^1、A_1^2、B_1^1、B_1^2、A_2^1、A_2^2、B_2^1、B_2^2。首先，Alice 以逻辑量子比特 $A_1(A_2)$ 中的 $A_1^2(A_2^2)$ 为控制比特、$A_1^1(A_2^1)$ 为目标比特实施 CNOT 操作。同时，Bob 以逻辑量子比特 $B_1(B_2)$ 中的 $B_1^2(B_2^2)$ 为控制比特、$B_1^1(B_2^1)$ 为目标比特实施 CNOT 操作。然后，Alice 以逻辑量子比特 $A_1(A_2)$ 中的 $A_1^1(A_2^1)$ 为控制比特、$A_1^2(A_2^2)$ 为目标比特实施 Controlled-U_z($CU_z=|0\rangle\langle 0|\otimes I+|1\rangle\langle 1|\otimes\sigma_z$)操作，其中 $\sigma_z=|0\rangle\langle 0|-|1\rangle\langle 1|$。Bob 以逻辑量子比特 $B_1(B_2)$ 中的 $B_1^1(B_2^1)$ 为控制比特、$B_1^2(B_2^2)$ 为目标比特实施 CU_z 操作。此时逻辑簇态 $|\Xi_r\rangle$ 将转变为：

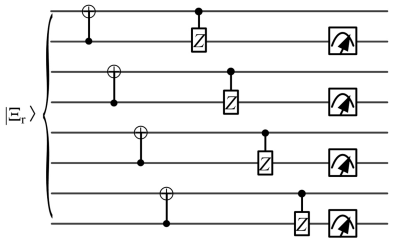

图 3 集体旋转噪声下四粒子簇态的恢复过程

$$
\begin{aligned}
|\Gamma_r\rangle=\frac{1}{8}\,[&\,|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)\otimes\\
&|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)+\\
&|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)|1\rangle(|0\rangle+|1\rangle)\otimes\\
&|1\rangle(|0\rangle+|1\rangle)+|1\rangle(|0\rangle+|1\rangle)|1\rangle\otimes\\
&(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)|0\rangle(|0\rangle+|1\rangle)-\\
&|1\rangle(|0\rangle+|1\rangle)|1\rangle(|0\rangle+|1\rangle)|1\rangle(|0\rangle+|1\rangle)\otimes\\
&|1\rangle(|0\rangle+|1\rangle)\,]_{A_1^1A_1^2B_1^1B_1^2A_2^1A_2^2B_2^1B_2^2}
\end{aligned}
\tag{5}
$$

最后，Alice(Bob)对量子比特 $A_1^2(B_1^2)$ 和 $A_2^2(B_2^2)$ 分别执行 X 基测量，$|\Gamma_r\rangle$ 将塌缩为 $|\zeta_r\rangle=1/2(|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{A_1^1B_1^1A_2^1B_2^1}$，显然它们成功恢复并共享了四粒子簇态。

2 安全性分析

安全性是衡量协议性能的重要指标，安全的 CQD 协议不仅能够避免信息泄露问题，同时还能够抵抗外部攻击和内部攻击。在集体退相位噪声和集体旋转噪声下，本文提出的协议的工作流程相似，因此将以集体退相位噪声下的 CQD 协议为例分析 CQD 协议的安全性。

2.1 信息泄露问题

通信双方在 1.1 节内容中的步骤⑥和步骤⑦的公布经典信息 T_A 和 T_B 后，Eve 或 Charlie 可尝试据此推测通信双方传输的秘密信息。例如，假设 Alice 公布经典信息 T_A=0，Eve 和 Charlie 猜测 $\{MR_A^2=0,M_A=0\}$ 或者 $\{MR_A^2=1,M_A=1\}$，显然秘密信息将有 2 种可能。从信息论的角度分析，这 2 种可能性意味着有 $-2\times\frac{1}{2}\log_2\frac{1}{2}=1$ 比特的秘密信息是 Eve 或 Charlie 不能获得的。而事实上，协议中 Alice 只传 1 比特秘密信息给 Bob，这将使得 Eve 和 Charlie 无法准确获得 Alice 所传输的秘密信息。同理，Bob 发送给 Alice 的秘密信息也是安全的。因此本文协议能够有效地避免信息泄露。

2.2 外部攻击

在通信过程中，外部敌手 Eve 通过拦截传输的量子比特并实施某种操作以窃取通信双方的秘密信息，统称外部攻击，其主要包括截获-重发攻击、纠缠-测量攻击和修改攻击等攻击策略。

◆截获-重发攻击。假设 Eve 截获了步骤①中传输的所有逻辑量子比特进行测量，并根据测量结果发送新的逻辑量子比特给 Alice。由于诱骗态是由 Charlie 随机插入到序列 S_A 中的且随机地处于 $\{|0_{dp}\rangle,|1_{dp}\rangle,|+_{dp}\rangle,|-_{dp}\rangle\}$ 4 个态之一，Eve 在不知道诱骗态的测量基和位置的情况下，她制备的诱骗态将会以 $1-\left(\frac{3}{4}\right)^n$ 的概率被检测出来，而当 n 足够大时，被检测出的概率将趋于 1。因此，本文协议能够抵抗 Eve 发起的截获-重发攻击。

◆纠缠-测量攻击。为了获取通信双方的秘密信息，Eve 拦截步骤①中传输的所有逻辑量子比特，并通过实施幺正变换 U_e 使她的辅助量子比特与其形成纠缠。随后，Eve 便可通过测量辅助量子比特来获得秘密信息。然而，Eve 对逻辑量子比特实施的幺正变换将会使传输序列中的诱骗态发生改变。她在不知道诱骗态的状态和位置的情况下进行测量势必会对量子系统产生扰动，以至于她的攻击必将在步骤②的安全检测中被发现。如果 Eve 想避免被检测出来，她将无法通过测量辅助量子比特来获得任何有用的量子态信息，更无法推断通信双方交换的秘密信息。

◆修改攻击。本文协议秘密信息的交换主要依赖于四粒子簇态的确定性纠缠关系，若 Eve 截获所有的

逻辑量子比特并实施幺正变换 U_1^{dp} 使逻辑簇态的纠缠关系发生改变，通信双方必将获得错误的秘密信息。而事实上,Charlie 在传输序列 S_A 和 S_B 之前随机插入了足够数量的诱骗态。对于 Eve 而言,如果她不知道诱骗态的位置,她实施的幺正变换在改变簇态纠缠关系的同时也会改变诱骗态,最终导致她的攻击将在步骤②的安全检测中被发现。

2.3 内部攻击

内部攻击者包括通信双方和控制方。在通信过程中,通信双方企图绕过控制方直接进行通信,通常称为共谋攻击;不诚信的控制方企图窃听通信双方传输的秘密信息或者干扰他们的正常通信,通常包括共谋攻击、DIS 攻击和 DoS 攻击。

◆共谋攻击。基于簇态的确定性纠缠关系 $|\zeta\rangle=1/2\ (|0000\rangle+|0011\rangle+|1100\rangle-|1111\rangle)_{A_1B_1A_2B_2}$ 必然存在量子比特 $A_1=B_1$ 且 $A_2=B_2$。因此 Alice 和 Bob 可根据自己的测量结果和簇态的确定性纠缠关系共谋获取对方的秘密信息。然而 Charlie 在步骤①随机实施了幺正变换 U_0^{dp} 或者 U_1^{dp} 生成许可。当幺正变换 U_1^{dp} 作用在逻辑量子比特 A_2 上时,逻辑簇态将被改变并在步骤④塌缩为 $|\omega\rangle=1/2(|0010\rangle-|0001\rangle+|1110\rangle+|1101\rangle)_{A_1B_1A_2B_2}=1/2(|00+-\rangle-|00-+\rangle+|11++\rangle-|11--\rangle)_{A_1B_1A_2B_2}$。显然,如表 2 所示,此时簇态各量子比特测量结果之间的关系将发生改变，这将使得 Alice 和 Bob 无法获得正确的秘密信息。以 Bob 为例,当 Charlie 对逻辑量子比特 A_2 实施幺正变换 U_1^{dp} 且 Alice 和 Bob 没有获得 Charlie 许可时,如果 Bob 的测量结果为 $MR_B^1=0$ 和 $MR_B^2=0$,他将根据自己的测量结果推测 $MR_A^2=0$。此时如果 Alice 公布其传输的经典信息 $T_A=0$，那么 Bob 将推测 Alice 的秘密信息 $M_A=0$。而事实上 Alice 的测量结果应为 $MR_A^2=1$,且他真正传输的秘密信息 $M_A=1$。由此可见,Bob 在这种情况下将获得错误的秘密信息。由于协议中幺正变换 U_0^{dp} 和 U_1^{dp} 是随机被实施的，如果没有 Charlie 的许可,Alice 和 Bob 都只能以 1/2 的概率获得对方传输的秘密信息,这个概率无异于随机猜测。因此本文协议能够有效地免疫于共谋攻击。

表 2 执行 U_1^{dp} 后各量子比特测量结果之间的关系以及解码规则

测量数据属性	解码规则			
MR_A^1	$0(\|0\rangle)$	$0(\|0\rangle)$	$1(\|1\rangle)$	$1(\|1\rangle)$
MR_B^1	$0(\|0\rangle)$	$0(\|0\rangle)$	$1(\|1\rangle)$	$1(\|1\rangle)$
MR_A^2	$0(\|+\rangle)$	$1(\|-\rangle)$	$0(\|+\rangle)$	$1(\|-\rangle)$
MR_B^2	$1(\|-\rangle)$	$0(\|+\rangle)$	$0(\|+\rangle)$	$1(\|-\rangle)$

◆DIS 攻击。为了获取秘密信息,不诚信的控制方制备纠缠态 $|Y_{dp}\rangle$ 代替真实逻辑簇态 $|\Xi_{dp}\rangle$,在步骤④执行恢复操作后,纠缠态 $|Y_{dp}\rangle$ 将塌缩为 $|\xi\rangle=1/2(|00++\rangle|e_{00}\rangle+|00--\rangle|e_{01}\rangle+|11+-\rangle|e_{10}\rangle+|11-+\rangle|e_{11}\rangle)_{A_1B_1A_2B_2D}$,其中 $|e_{00}\rangle$、$|e_{01}\rangle$、$|e_{10}\rangle$ 和 $|e_{11}\rangle$ 能够被控制方准确区分。控制方将测量这 4 个量子态,推断通信双方的测量结果并获取秘密信息。然而,步骤⑤的安全检测能够成功地阻止控制方的 DIS 攻击。具体而言,在步骤⑤的安全检测中,若 Bob 选择的测量基为 Z 基、Z 基、X 基和 X 基,在检测过程中将不会引入错误；而 Bob 选择的测量基为 X 基、X 基、Z 基和 Z 基时,对比式(3)可知,控制方的攻击将会以 3/4 的概率被检测出来。当 Bob 选择第二组测量基时,纠缠态 $|\xi\rangle$ 可被表示为：

$$\begin{aligned}|\xi\rangle=\frac{1}{8}[&(|++00\rangle+|--00\rangle+|+-11\rangle+|-+11\rangle)\otimes\\&(|e_{00}\rangle+|e_{01}\rangle+|e_{10}\rangle+|e_{11}\rangle)+\\&(|++01\rangle+|--01\rangle+|+-10\rangle+|-+10\rangle)\otimes\\&(|e_{00}\rangle-|e_{01}\rangle-|e_{10}\rangle+|e_{11}\rangle)+\\&|++10\rangle+|--10\rangle+|+-01\rangle+|-+01\rangle)\otimes\\&(|e_{00}\rangle-|e_{01}\rangle+|e_{10}\rangle-|e_{11}\rangle)+\\&|++11\rangle+|--11\rangle+|+-00\rangle+|-+00\rangle)\otimes\\&(|e_{00}\rangle+|e_{01}\rangle-|e_{10}\rangle-|e_{11}\rangle)]_{A_1B_1A_2B_2D}\end{aligned}\tag{6}$$

如果不诚信的控制方想要避免自己的攻击被检测出来，他必须设定 $(|e_{00}\rangle-|e_{01}\rangle-|e_{10}\rangle+|e_{11}\rangle)=(|e_{00}\rangle-|e_{01}\rangle+|e_{10}\rangle-|e_{11}\rangle)=(|e_{00}\rangle+|e_{01}\rangle-|e_{10}\rangle-|e_{11}\rangle)=\vec{0}$,也就是 $(|e_{00}\rangle=|e_{01}\rangle=|e_{10}\rangle=|e_{11}\rangle)$,因而他将不能正确地区分这 4 个量子态，更不能通过测量这 4 个量子态来获取通信双方的测量结果。显然,本文协议能够成功抵抗控制方的 DIS 攻击。

◆DoS 攻击。不诚信的控制方故意宣布错误的许可而使通信双方获得错误的信息。具体而言,不诚信的控制方公布的错误许可可分为 2 类：一类是真实许可为0而控制方公布 1;另一类是真实许可为 1 而控制方公布0。但无论哪种情况,一旦控制方公布了错误的许可,Alice 在步骤③实施与控制方公布的许可对应的幺正变换后,逻辑簇态都将转变为 $|\Omega_{dp}\rangle=1/2\times(|0_{dp}0_{dp}1_{dp}0_{dp}\rangle-|0_{dp}0_{dp}0_{dp}\ 1_{dp}\rangle+|1_{dp}1_{dp}1_{dp}\ 0_{dp}\rangle+|1_{dp}1_{dp}0_{dp}\ 1_{dp}\rangle)_{A_1B_1A_2B_2}$,在步骤④执行恢复操作后,该逻辑簇态将塌缩为 $|\omega\rangle=1/2(|0010\rangle-|0001\rangle+|1110\rangle+|1101\rangle)_{A_1B_1A_2B_2}=$

$1/2(|00+-\rangle-|00-+\rangle+|11++\rangle-|11--\rangle)_{A_1B_1A_2B_2}=1/2(|++10\rangle+|--10\rangle-|+-01\rangle-|-+01\rangle)_{A_1B_1A_2B_2}$。显然,此时各量子比特测量结果之间的关系将完全不同于式(3)。因而,只要不诚信的控制方公布了错误的许可,控制方的 DoS 攻击在步骤⑤的安全检测中一定能够被通信双方发现。因此,本文协议在这类攻击下也是安全的。

3 与其它代表性 CQD 协议的比较

为了突显本文协议的优势,本文从多个方面综合地比较了本文协议与其它具有代表性的 CQD 协议,结果如表 3 所示。

表 3 与具有代表性的可控量子对话协议的比较

协议	避免信息泄露	抵抗噪声	抵抗共谋攻击	抵抗 DIS 攻击	抵抗 DoS 攻击	控制方在线等待	量子资源
文献[7]	否	否	否	是	否	是	GHZ 态
文献[10]	是	否	否	否	否	是	Brown 态
文献[11]	是	否	是	否	否	是	GHZ 态+Bell 态
文献[12]	是	否	是	否	否	否	簇态
文献[14]	是	否	是	是	是	否	簇态
文献[15]	是	是	是	是	否	是	逻辑单量子比特
本文协议	是	是	是	是	是	否	逻辑簇态

由表 3 可知, 相比以上具有代表性的 CQD 协议,本文协议具有更好的安全性和更强的实用性。

4 结束语

本文基于逻辑簇态设计了 2 个集体噪声下错误容忍的 CQD 协议,能够有效抵抗集体退相位噪声和集体旋转噪声。QD 中控制方角色的加入能够拓展 QD 协议的应用场景。类似文献[16]中逻辑态的构造方法,逻辑簇态理论上可由控制方对几个特定的叠加态实施多次不同的受控幺正变换构造。通过安全性分析显示:本文协议能够有效地抵抗各类攻击,尤其是近几年被探究发现的共谋攻击、DIS 攻击和 DoS 攻击,这些攻击对协议的安全性都产生了极大的威胁。在量子保密通信的实用化进程中,噪声环境下第三方 CQD 协议具有很高的应用价值。在协议的实用化进程中必然会受到诸多因素的影响,因此我们后续的工作应该以现有工作为基础, 充分考虑现实环境中的影响因素,设计更加实用的量子保密通信协议。

参考文献:

[1] QI J M, XU G, CHEN X B, et al. Two authenticated quantum dialogue protocols based on three-particle entangled states [J]. Quantum Information Processing, 2018. DOI: https://doi.org/10.1007/s11128–018–2005–8.

[2] ZHANG M H, CAO Z W, PENG J Y, et al. Fault tolerant quantum dialogue protocol over a collective noise channel[J]. The European Physical Journal D, 2019. DOI: https://doi.org/10.1140/epjd/e2019–90481–9.

[3] ZHANG M H, PENG J Y, CAO Z W. Quantum dialogue protocol with four-mode continuous variable GHZ state [J]. Modern Physics Letters B, 2019. DOI: 10. 1142/S0217984919500337.

[4] PAN H M. Quantum Dialogue Based on Entanglement Swapping and Hadamard Operation via Cavity QED [J]. Inter national Journal of Theoretical Physics, 2019, 58(3): 1017–1027.

[5] LANG Y F. Fault Tolerant Authenticated Quantum Dialogue Based on Logical Qubits and Controlled-Not Operations[J]. International Journal of Theoretical Physics, 2019, 58(2): 531–542.

[6] MAN Z X, XIA Y J. Controlled bidirectional quantum direct communication by using a GHZ state [J]. Chinese Physics Letters, 2006, 23(7): 1680–1682.

[7] YE T Y, JIANG L Z. Improvement of controlled bidirectional quantum direct communication using a GHZ state [J]. Chinese Physics Letters, 2013. DOI: 10.1088/0256-307X/30/4/040305.

[8] LIU Z H, CHEN H W. Comment on "Improvement of controlled bidirectional quantum direct communication using a GHZ state"[J]. Chinese Physics Letters, 2013. DOI: 10. 1088/0256-307X/30/7/079901.

[9] YE T Y, JIANG L Z. Reply to the Comment on "Improvement of Controlled Bidirectional Quantum Direct Communication Using a GHZ State" [J]. Chinese Physics Letters, 2013. DOI: 10.1088/0256-307X/30/7/079902.

[10] YANG Y F, YE Z Q, TU C L. Controlled Secure Quantum Dialogue by Using Brown States [J]. Acta Photonica Sinica, 2013, 4(11): 1305–1310 .

[11] KAO S H, HWANG T. Controlled quantum dialogue robust against conspiring users[J]. Quantum Information Processing, 2016, 15(10): 4313–4324.

[12] KAO S H, HWANG T. Controlled quantum dialogue using cluster states [J]. Quantum Information Processing, 2017. DOI: https://doi. org/10.1007/s11128-017–1597-8.

[13] LIU Z H, CHEN H W. Security loopholes in the controlled quantum dialogue robust against conspiring users protocol [J]. Quantum Information Processing, 2019. DOI: https://doi.org/10.1007/s11128-019–2343-1

[14] LIU Z, CHEN H. Cryptanalysis and improvement in controlled quantum dialogue using cluster states[J]. Quantum Information Processing, 2019. DOI: https://doi.org/10.1007/s11128-019–2214-9.

[15] XIAO M, LIU G. Fault-tolerant controlled quantum dialogue using logical qubit[J]. Chinese Journal of Electronics, 2018, 27(2): 263–269.

[16] CHANG L W, ZHANG Y Q, TIAN X X, et al. Fault tolerant controlled quantum dialogue against collective noise[J]. Chinese Physics B, 2020.DOI: 10.1088/1674-1056/ab5786.