集体噪声信道上带身份认证的无信息泄露的量子对话协议*

吴贵铜[1)] 周南润[2)†] 龚黎华[2)] 刘三秋[1)]

1) (南昌大学物理系, 南昌 330031)

2) (南昌大学电子信息工程系, 南昌 330031)

(2013 年 6 月 10 日收到; 2013 年 10 月 6 日收到修改稿)

在集体噪声条件下提出三个带身份认证的量子对话协议, 两个量子对话协议分别用于抵抗集体消相干噪声和集体旋转噪声, 另一个用于同时抵抗这两种集体噪声. 通信双方通过广义幺正变换将自己的秘密信息编码到量子态中; 并根据自己的秘密信息和携带秘密信息的粒子的初末两量子态, 便可推知对方的秘密信息实现量子对话. 协议的效率、安全性和无信息泄露等性能分析表明了协议的有效性.

关键词: 集体噪声, 身份认证, 量子对话, 无信息泄露

PACS: 03.67.–a, 42.50.Ar, 42.79.Sz, 95.75.Kk **DOI:** 10.7498/aps.63.060302

1 引 言

量子安全直接通信(quantum secure direct communication, QSDC)是以量子态作为信息载体, 在量子信道中不依赖事先共享密钥直接传输秘密信息的量子通信模式. 2002 年 Beige 等[1] 首先提出“量子安全直接通信”新概念. Boström 和 Felbinger[2] 借鉴量子密集编码的思想提出一种基于 Einstein-Podolsky-Rosen (EPR) 纠缠态的 QSDC 协议, 简称“乒乓”协议或 BF 协议, 该协议操作简便, 但存在缺陷[3−5]. 例如 2003 年 Wojcik[3] 指出, 如果量子信道中存在噪声, 攻击者 Eve 可以窃听到 BF 协议的部分秘密信息; Cai[4] 指出, BF 协议无法抵抗 Eve 的拒绝服务攻击; 2004 年 Cai 和 Li[5] 提出 BF 协议的通信容量可以进一步提高. 2003 年 Deng 等[6] 提出了基于 EPR 纠缠态的两步 QSDC 协议, 简称“两步”协议, 其安全性得到了证实[7]. “乒乓”协议和“两步”协议成为 QSDC 中最基本的两种通信模式. 基于这两种思想相继提出了各种 QSDC 协议[8−14]. 除了这两种通信模式外, 2007 年王剑等[15] 基于单光子序列的顺序重排, 提出了多方控制 QSDC 协议, 接收者只有在征得所有控制者同意的情况下才可读取发送方的秘密信息. 然而, 在王天银等[16] 提出的攻击方法下, 该 QSDC 协议是不安全的——接收方不需任何控制者同意的情况下也可获得发送方的秘密消息.

量子对话(QD)是双向的 QSDC. 2004 年, Nguyen[17] 提出了 QD 协议的概念, 利用 EPR 纠缠态作为量子信道. 许多 QD 相继被提出[18,19]. 2007 年, Wen 等[19] 提出安全量子电话, 其通信过程包括拨号部分和通话部分, 其实质分别是通过第三方验证通信双方的合法身份和受第三方控制的 QD 协议. 2008 年, Gao 等[20] 指出 Nguyen 的 QD 协议存在严重的信息泄露问题, 即通信双方所交换的秘密信息将有一半的秘密信息无意中泄露给窃听者. 文献 [18] 和 [19] 同样存在信息泄露问题. 随后, 人们提出了各种无信息泄露的 QD 协议[21−25]. 2010 年, Gao[21] 提出了两个无信息泄露的 QD 协议, 一个基于“两步”协议的思想, 一个基于“ 乒乓”协议的思

* 国家自然科学基金 (批准号: 10647133)、江西省青年科学家培养对象计划项目 (批准号: 20122BCB23002) 和江西省教育厅科技项目 (批准号: GJJ13057) 资助的课题.

† 通讯作者. E-mail: znr21@163.com

想. 2010 年, Shi[22] 提出了基于 Bell 态和辅助粒子的双向 QSDC 协议, 并从信息论角度分析证明该协议无信息泄露. 2011 年, Gao 等[23] 结合“乒乓”协议的思想提出了基于 4 粒子最大纠缠态无信息泄露的 QD 协议. 2012 年, 王鹤等利用 two-qutrit 纠缠态作为量子信道提出高效无信息泄露的 QD 协议[24] 和两个无信息泄露的 QD 协议[25], 分别基于 Bell 态和 two-qutrit 纠缠态.

以上 QD 协议[17−25] 都是基于理想量子信道, 即无任何噪声干扰的量子信道. 实用的量子信道大多是光纤, 光纤具有双折射的波动性, 光子在量子信道中传输会受到噪声的影响. 光子旅行的时间窗比噪声源变化短, 因此, 这些光子都将受到相同噪声的影响, 这就是集体噪声的定义[11]. 在量子通信中, 集体噪声是主要的噪声源, 它包括集体消相干噪声和集体旋转噪声. 设计量子通信协议抵抗集体噪声影响的简单方法是构造一个无消相干子空间 (decoherence free subspace, DFS), 该空间的所有量子态在集体噪声环境影响下保持不变. DFS 的这一特性已被应用于构建集体噪声信道下的 QSDC 协议[11−13].

集体噪声是一种常见的噪声, 它存在于许多实际量子系统中. 本文基于“两步”协议和集体噪声的思想, 提出集体噪声信道上无信息泄露的 QD 协议, 该协议利用 DFS 可免疫集体噪声影响的特性, 构造广义纠缠态. 该协议在第一次安全性检测中加入身份认证, 从某种意义上来说, 不仅提高协议的安全性, 还提高协议的效率. 结合信息论对该协议的效率和安全性进行了详细分析.

2 集体噪声信道上的 QD 协议

集体消相干噪声和集体旋转噪声对量子态的影响分别用幺正算子 $U_{\rm d}$ 和 $U_{\rm r}$ 表示[11−13]:

$$U_{\rm d}=\begin{pmatrix}1 & 0\\ 0 & {\rm e}^{{\rm i}\theta}\end{pmatrix}, \tag{1}$$

$$U_{\rm r}=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}. \tag{2}$$

其对单粒子态作用如下:

$$U_{\rm d}|0\rangle=|0\rangle,\quad U_{\rm d}|1\rangle={\rm e}^{{\rm i}\theta}|1\rangle, \tag{3}$$

$$U_{\rm r}|0\rangle=\cos\theta|0\rangle+\sin\theta|1\rangle,$$

$$U_{\rm r}|1t\rangle=-\sin\theta|0\rangle+\cos\theta|1\rangle, \tag{4}$$

其中 $|0\rangle$, $|1\rangle$ 分别代表水平和垂直极化量子态, θ 表示集体噪声的参数, 它随时间而波动.

2.1 抵抗集体消相干噪声的 QD 协议

由 (3) 式可知, 任一单粒子量子态在集体消相干噪声信道中传输, 只改变量子态的相位, 而模保持不变. 根据集体消相干噪声对量子态的影响特性, 构造可免疫该噪声的逻辑量子比特为[11−13]

$$|L\rangle=|01\rangle_{\rm AB},\quad |V\rangle=|10\rangle_{\rm AB}, \tag{5}$$

其中 $|L\rangle$, $|V\rangle$ 分别代表逻辑比特 0 和 1; $\{|L\rangle,|V\rangle\}$ 作为一组测量基, 一个安全的量子通信协议至少需要两个非正交的测量基[13]. 另一个测量基可选为

$$\begin{aligned}|\pm\rangle&=\frac{1}{\sqrt{2}}(|L\rangle\pm|V\rangle)\\&=\frac{1}{\sqrt{2}}(|01\rangle\pm|10\rangle)=|\psi^{\pm}\rangle,\end{aligned} \tag{6}$$

显然 $|\langle+|L\rangle|^2=|\langle+|V\rangle|^2=|\langle-|L\rangle|^2=|\langle-|V\rangle|^2$, 因此, $\{|L\rangle,|V\rangle\}$ 和 $\{|+\rangle,|-\rangle\}$ 可构成集体消相干噪声信道上的两组无偏的基. 选用幺正变换 U_0 和 U_1 使每组测量基中的基底可以相互转换:

$$\begin{aligned}&U_0=I_{\rm A}\otimes I_{\rm B}=|L\rangle\langle L|+|V\rangle\langle V|,\\&U_1=(\sigma_x)_{\rm A}\otimes(-{\rm i}\sigma_y)_{\rm B}=|V\rangle\langle L|-|L\rangle\langle V|,\end{aligned} \tag{7}$$

其中, 下标 A 和 B 表示幺正变换分别作用于光子 A 和 B,

$$\begin{aligned}I&=|0\rangle\langle0|+|1\rangle\langle1|,\\\sigma_x&=|1\rangle\langle0|+|0\rangle\langle1|,\\-{\rm i}\sigma_y&=|1\rangle\langle0|-|0\rangle\langle1|.\end{aligned} \tag{8}$$

幺正变换 U_1 对测量基的变换为

$$U_1|L\rangle=|V\rangle,\quad U_1|V\rangle=-|L\rangle, \tag{9}$$

$$U_1|+\rangle=-|-\rangle,\quad U_1|-\rangle=|+\rangle. \tag{10}$$

Alice 和 Bob 事先商定 $|L\rangle(|0\rangle)$, $|V\rangle(|1\rangle)$ 分别代表 0 和 1; 并协商幺正变换 U_0, U_1 分别代表 0 和 1. 并构造 5 粒子广义 Greenberger-Horne-Zeilinger (GHZ) 态 $|\Psi\rangle_{ab_1b_2}$:

$$|\Psi\rangle_{ab_1b_2}=\frac{1}{\sqrt{2}}(|0LL\rangle+|1VV\rangle)_{ab_1b_2}, \tag{11}$$

其中 a, b_1 和 b_2 分别有 1, 2 和 2 个粒子.

2.2 抵抗集体旋转噪声的 QD 协议

由 (4) 式可知, 任一单粒子量子态传输都无法免疫集体旋转噪声的影响. 因此利用单粒子量子比特是无法实现量子信息的安全传输. 但是量子比

特系统中存在多个量子纠缠态在该噪声信道中不受影响, 例如, $|\phi^+\rangle$ 和 $|\psi^-\rangle$ 两个Bell态可免疫该噪声的影响. 因此, 在该噪声信道下, 逻辑量子比特可选为[11−13]

$$|L'\rangle = |\phi^+\rangle_{\rm AB} = \frac{1}{\sqrt{2}}(|0\rangle_{\rm A}|0\rangle_{\rm B} + |1\rangle_{\rm A}|1\rangle_{\rm B}),$$
$$|V'\rangle = |\psi^-\rangle_{\rm AB} = \frac{1}{\sqrt{2}}(|0\rangle_{\rm A}|1\rangle_{\rm B} - |1\rangle_{\rm A}|0\rangle_{\rm B}), \quad (12)$$

其中 $|L'\rangle$, $|V'\rangle$ 分别代表逻辑比特0和1; $\{|L'\rangle, |V'\rangle\}$ 可作为一组测量基, 另一个测量基可选为

$$|\pm'\rangle = \frac{1}{\sqrt{2}}(|L'\rangle \pm |V'\rangle), \quad (13)$$

显然 $|\langle +'|L'\rangle|^2 = |\langle +'|V'\rangle|^2 = |\langle -'|L'\rangle|^2 = |\langle -'|V'\rangle|^2$, 因此, $\{|L'\rangle, |V'\rangle\}$ 和 $\{|+'\rangle, |-'\rangle\}$ 可构成集体旋转噪声信道上的两组无偏的基. 选用幺正变换 U_0' 和 U_1' 使每组测量基中的基底可以相互转换:

$$U_0' = I_{\rm A} \otimes I_{\rm B} = |L'\rangle\langle L'| + |V'\rangle\langle V'|,$$
$$U_1' = I_{\rm A} \otimes (-{\rm i}\sigma_y)_{\rm B} = |V'\rangle\langle L'| - |L'\rangle\langle V'|, \quad (14)$$
$$I = |0\rangle\langle 0| + |1\rangle\langle 1|, -{\rm i}\sigma_y = |1\rangle\langle 0| - |0\rangle\langle 1|. \quad (15)$$

幺正变换 U_1' 对测量基的变换为

$$U_1'|L'\rangle = |V'\rangle, \quad U_1'|V'\rangle = -|L'\rangle, \quad (16)$$
$$U_1'|+'\rangle = -|-'\rangle, \quad U_1'|-'\rangle = |+'\rangle. \quad (17)$$

Alice和Bob事先商定 $|L'\rangle$ ($|0\rangle$), $|V'\rangle$($|1\rangle$) 分别代表经典比特0和1; 并协商幺正变换 U_0', U_1' 分别代表经典比特0 和1. 并构造5粒子广义GHZ态 $|\phi\rangle_{ab_1b_2}$,

$$|\varphi\rangle_{ab_1b_2} = \frac{1}{\sqrt{2}}(|0L'L'\rangle + |1V'V'\rangle)_{ab_1b_2}$$
$$= \frac{1}{\sqrt{2}}(|0\rangle|\phi^+\rangle|\phi^+\rangle + |1\rangle|\psi^-\rangle|\psi^-\rangle)_{ab_1b_2}, \quad (18)$$

其中 a, b_1 和 b_2 分别有1, 2和2个粒子.

2.3 QD协议的具体通信过程

抵抗集体消相干噪声(集体旋转噪声)的QD协议的具体通信过程如下:

1) Alice制备 N 个5粒子广义GHZ态, 并将其划分为 A, B_1 和 B_2 三个序列串, 其中 A 由 a 粒子构成, 而 B_1 和 B_2 分别由 b_1 和 b_2 粒子组成. Alice测量 A 中所有 a 粒子并记录测量结果 a_i, 其中 $a_i \in \{0,1\}$, $0 < i \leqslant N$.

2) Alice根据自己的身份标识码 ID_A^i, $0 < i \leqslant N$ 制备 N 个2粒子量子态作为诱骗态, 若 $ID_A^i = 0$, Alice将第 i 个2粒子量子态制备成 $|L\rangle$ 或者 $|+\rangle$ ($|L'\rangle$ 或者 $|+'\rangle$); 否则, 为 $|V\rangle$ 或者 $|-\rangle$ ($|V'\rangle$ 或者 $|-'\rangle$). Alice将诱骗态随机插入到 B_1 得到新序列串 B_1^* 发给Bob, 并记录所有诱骗态的位置和初始量子态.

3) Bob接收 B_1^* 的全部粒子后, 返回已接收全部粒子的信息给Alice. Alice公布制备诱骗态的原理、诱骗态的位置和对应测量基. Bob根据自己的 $ID_{\rm B}^i$, 选用对应幺正变换作用于诱骗态. 例如, 若 $ID_B^i = 0$, Bob选择幺正变换 U_0 (U_0'); 否则, 选择 U_1 (U_1'). Bob选用测量基测量对应的诱骗态, 并公布测量结果 ID_M^i. Alice验证 $ID_{\rm B}^i = ID_{\rm A}^i \oplus ID_{\rm M}^i$ 是否成立, 其中 $\oplus$ 是模2 加. 若等式成立, 既验证了Bob的身份又验证了信道是安全的. 否则, 说明Bob的身份有误或者信道不安全. 同时, Bob也通过 $ID_{\rm A}^i = ID_{\rm B}^i \oplus ID_{\rm M}^i$ 验证Alice的身份和信道是否安全. 只有Alice和Bob都验证对方的身份无误时, 才继续下一步通信; 否则, 返回步骤1).

4) Bob测量 B_1^* 除去诱骗态剩余的所有粒子 B_1 并记录测量结果 b_i, 其中 $b_i \in \{0,1\}$, $0 < i \leqslant N$. 根据广义GHZ态的纠缠特性可知 $a_i = b_i$.

5) Alice根据自己的秘密信息 A_i 选用对应的幺正变换作用于 B_2 中的 b_2^i 粒子, 得到新序列串 B_2^* 并打乱次序. 例如, 若 $A_i = 0$, 选择幺正变换 U_0 (U_0'); 否则, 选择 U_1 (U_1'). Alice再制备 N 个2粒子量子态作为诱骗态, 随机处于 $|L\rangle, |V\rangle, |+\rangle, |-\rangle$ ($|L'\rangle$, $|V'\rangle$, $|+'\rangle$, $|-'\rangle$) 态. Alice将诱骗态随机插入到已打乱次序的 B_2^* 中, 得到序列串 B_2^{**} 发给Bob, 并记录所有诱骗态的位置和初始量子态.

6) Bob接收 B_2^{**} 的全部粒子后, 返回已接收全部粒子的信息给Alice. Alice公布诱骗态的位置和对应的测量基, Bob选用测量基测量对应的诱骗态, 并公布测量结果. Alice将诱骗态初态和Bob的测量结果做统计比对, Bob的测量结果等于对应初态, 说明信道是安全的, Alice和Bob继续通信; 否则, 返回步骤1).

7) Alice通过经典信道通知Bob序列串 B_2^* 的正确次序.

8) Bob重新排列 B_2^* 的次序. Bob根据自己的秘密信息 B_i 选用对应的幺正变换作用于 B_2^* 中的 b_2^i 粒子; Bob测量 B_2^* 中的 b_2^i 粒子, 并公布测量结果 M_i, 其中 $M_i \in \{0,1\}$.

9) 完成量子对话. Alice根据自己的秘密信

息 A_i, 测量结果 a_i 和步骤 8) Bob 的测量结果 M_i, 可获得 Bob 的秘密信息 $B_i = A_i \oplus a_i \oplus M_i$. 同时, Bob 根据自己的秘密信息 B_i, 测量结果 b_i 和步骤 8) Bob 的测量结果 M_i, 也可获得 Alice 的秘密信息 $A_i = B_i \oplus b_i \oplus M_i$.

该协议的信道是否安全是通过诱骗态来检测的, 诱骗态的基本思想是: 量子信息发送者 Alice 使用不同强度的诱骗脉冲和信号脉冲作为信源, 窃听者无法区分信号脉冲和诱骗脉冲, 因此可以通过诱骗脉冲来检测是否存在窃听者 [26]. 在该协议中, 第一次传输过程将 b_1 粒子的量子态作为信号态, 根据 ID_{A}^{i} 制备诱骗态, 并用该诱骗态检测信道是否安全以及相互验证对方的身份; 第二次传输的过程中, b_2 粒子的量子态作为信号态, 而诱骗态是由 Alice 另外特意制备的; 即该协议在传输量子信号前就已确定诱骗态.

由 QD 原理可知, QD 协议需要传输已携带秘密信息的信号态, 因此在传输量子信号前必须确定信号态和诱骗态. 而基于诱骗态的量子密钥分发协议不同于 QD 协议, 其整个通信过程不需要加密与解密过程, 在量子信息传输前不需要区分诱骗态和信号态, 并且一般情况下是由量子信号的接收者随机决定哪些量子态作为诱骗态. 相比于诱骗态量子密钥分发协议, QD 协议传输量子信号前确定诱骗态, 接收者 Bob 需要等待 Alice 公布诱骗态的位置和测量基后才可合作检测信道是否安全, 延长了接收者 Bob 存储量子信号态的时间, 增加了实现的难度; 但 QD 协议传输量子信号前确定诱骗态, 可增加诱骗态的功能, 如身份认证.

QD 协议的通信双方可同时交换彼此的秘密信息. 若将秘密信息作为密钥, 那么 QD 协议便可作为量子密钥分发协议, 并且其分配给通信双方的密钥可以不同. 该协议与常见诱骗态量子密钥分发协议的比较如表 1 所示.

表 1 本文协议与诱骗量子密钥分发的比较

	诱骗态量子密钥分发	本文协议
主要用途	分发密钥	交换秘密信息或分发密钥
所需信道	辅助经典信道、量子信道	辅助经典信道、量子信道
所用的诱骗态	发送者制备、接收者随机选定	发送者制备并指定

3 同时抵抗两种集体噪声的 QD 协议

以上抵抗集体消相干噪声和抵抗集体旋转噪声的两种 QD 协议都是针对其中一种集体噪声而设计的. 假如量子信道中同时存在两种集体噪声, 则以上两种 QD 协议都是不安全的. 接下来, 设计一个可以同时抵抗两种集体噪声的 QD 协议. 根据两种集体噪声对量子态影响特性, 同时免疫两种集体噪声的逻辑量子比特可选为 [27]

$$\begin{aligned}|L''\rangle &= \frac{1}{2}(|01\rangle - |10\rangle) \otimes (|01\rangle - |10\rangle),\\ |V''\rangle &= \frac{1}{2\sqrt{3}}[2(|1100\rangle + |0011\rangle)\\ &\quad - (|01\rangle + |10\rangle) \otimes (|01\rangle + |10\rangle)],\end{aligned} \tag{19}$$

其中 $|L''\rangle$, $|V''\rangle$ 分别代表逻辑比特 0 和 1; $\{|L''\rangle, |V''\rangle\}$ 可作为一组测量基, 另一组测量基可选择

$$|\pm''\rangle = \frac{1}{\sqrt{2}}(|L''\rangle \pm |V''\rangle). \tag{20}$$

同理, $|\langle +''|L''\rangle|^2 = |\langle +''|V''\rangle|^2 = |\langle -''|L''\rangle|^2 = |\langle -''|V''\rangle|^2$. 因此, $\{|L''\rangle, |V''\rangle\}$ 和 $\{|+''\rangle, |-''\rangle\}$ 可构成集体噪声信道上的两组无偏的基. 再选两个广义幺正变换 U_0'' 和 U_1'' 使每组测量基中的基底可以相互转换,

$$\begin{aligned}U_0'' &= |L''\rangle\langle L''| + |V''\rangle\langle V''|,\\ U_1'' &= |V''\rangle\langle L''| - |L''\rangle\langle V''|.\end{aligned} \tag{21}$$

U_1'' 对测量基的变换为

$$U_1''|L''\rangle = |V''\rangle, \quad U_1''|V''\rangle = -|L''\rangle, \tag{22}$$

$$U_1''|+''\rangle = -|-''\rangle, \quad U_1''|-''\rangle = |+''\rangle. \tag{23}$$

Alice 和 Bob 事先商定 $|L''\rangle$ ($|0\rangle$), $|V''\rangle$ ($|1\rangle$) 分别代表 0 和 1; 并协商幺正变换 U_0'', U_1'' 分别代表 0 和 1. 同理, 构造 9 粒子广义 GHZ 态 $|\Phi\rangle_{ab_1b_2}$:

$$|\Phi\rangle_{ab_1b_2} = \frac{1}{\sqrt{2}}(|0L''L''\rangle + |1V''V''\rangle)_{ab_1b_2}, \tag{24}$$

其中 a, b_1 和 b_2 分别有 1, 4 和 4 个粒子.

同时抵抗两种集体噪声的 QD 协议的具体通信过程与以上两协议相似, 不同的是所用的广义 GHZ 态、广义幺正变换以及诱骗态. 该协议的设计需 9 粒子广义纠缠态、广义幺正变换以及相应测量

基, 在理论上是可以实现的. 因此, 该协议在理论上也是可以实现的.

4 效率与安全性分析

上述三个协议基于"两步"协议的思想, Alice将所制备的广义GHZ态的粒子分为3个序列串 A, B_1 和 B_2, 并将序列串 B_1 和 B_2 分两步发给Bob. 第一步, Alice把 B_1 发给Bob, 为了告诉Bob B_2 中 b_2^i 粒子的量子初态; 第二步, Alice将自己秘密信息加载于 b_2^i 粒子并发给Bob. 在整个通信过程中, 窃听者Eve只有获得粒子 b_1^i 和 b_2^i (经Alice加密后的 b_2^i) 两量子态时, 才可准确推知通信双方所交换的秘密信息. 该通信过程中的两次安全性检测便可提高协议的安全性. 另外, 第一次安全性检测加入了通信双方的身份认证, 既可验证对方的身份, 又可检验信道是否安全, 实际上提高了协议的安全性和效率.

4.1 QD协议的效率分析

Yang等[11]将量子协议的量子比特效率定义为: $\eta = \dfrac{c}{q}$, 其中 c 是协议中交换的经典秘密比特总数, q 是协议中所需的量子比特总数. 率分析以上三个QD协议的效率.

在抵抗集体消相干噪声和抵抗集体旋转噪声的两QD协议中, Alice需制备 N 个5粒子纠缠态 (即 $5N$ 量子比特), 以及步骤2)和5)分别制备了 N 个2粒子诱骗态 (即 $2N$ 量子比特), Alice和Bob相互交换了 N 比特经典秘密信息. 因此, 该协议的效率为 $\eta = \dfrac{2}{9}$. 同理同时抵抗两种集体噪声信道的QD协议的效率为 $\eta = \dfrac{2}{17}$.

4.2 QD协议的安全性分析

一个可行的QD协议必须能够抵御各种攻击, 如干扰攻击、特洛伊木马攻击、截获重发攻击、纠缠测量攻击, 并且协议不能存在信息泄露问题.

4.2.1 干扰攻击

三个抵抗集体噪声的QD协议中, 只有步骤2)和5)传送粒子. 攻击者Eve随意采用幺正变换作用于这些粒子, 不仅干扰携带秘密消息粒子的量子态, 还可能干扰诱骗态. 每次传送的粒子有一半是诱骗态, 假设Eve采用 n 个幺正变换分别作用于 n 个不同的粒子, 干扰步骤2)和5)传送的粒子, 则该干扰分别不被步骤3)和6)检测到的概率为

$$p = \frac{C_N^n}{C_{2N}^n} = \frac{1}{2^n}, \tag{25}$$

当 n 足够大时, p 将趋于0. 因此, 步骤3)和6)可以分别检测到步骤2)和5)传送的粒子是否被干扰.

4.2.2 特洛伊木马攻击

特洛伊木马攻击可分为两种, 一种是由Li等[28]提出的延迟光子攻击, 另一种是由Cai和Li[29]提出的不可见光子攻击. 为了抵御延迟光子攻击, 只要在系统中引入光子数目分割器(PNS: 50/50), 将每个信号分成两份. 对于不可见光子攻击, 在Bob的接收装置前添加一个滤波器(选择波长接近于所操作粒子的波长的光子通过), 就可抵御这种攻击. 因此该方案可以抵御特洛伊木马攻击.

4.2.3 截获重发攻击

假设Eve截获了步骤2)和5)所传输的所有粒子, 并测量每一粒子, 根据测量结果重新发送一个序列给Bob. 传输的序列有 $2N$ 个逻辑量子比特随机分布于 $|L\rangle, |V\rangle, |+\rangle, |-\rangle$ (或者 $|L'\rangle, |V'\rangle, |+'\rangle, |-'\rangle$; $|L''\rangle, |V''\rangle, |+''\rangle, |-''\rangle$), 其中诱骗态占有 N 个逻辑量子比特, 有一半诱骗态处于 $|L\rangle, |V\rangle$ (或者 $|L'\rangle, |V'\rangle$; $|L''\rangle, |V''\rangle$) 态. 假设Eve选择测量基为 $\{|L\rangle, |V\rangle\}$ (或者 $\{|L'\rangle, |V'\rangle\}$; $\{|L''\rangle, |V''\rangle\}$) 的概率为 c, $0 < c \leqslant 1$, 则该攻击被步骤3)和6)检测到的概率为 $D = 1 - \left(\dfrac{c}{2}\right)^N$. 当 N 足够大时, D 将趋于1. 因此Eve的截获重发攻击将被步骤3)和6)检测到.

4.2.4 纠缠测量攻击

窃听者Eve为了获取通信双方所交换的秘密信息, 她需要获知步骤2)和5)所传输的 B_1^* 和 B_2^{**} 所有粒子的量子态. Eve拦截步骤2)和5)传送的粒子, 并通过 $U_{\rm E}$ 操作使辅助粒子 $E = \{|E_1\rangle, |E_2\rangle, \cdots, |E_m\rangle\}$ 与所拦截粒子形成纠缠态, 形成新序列串 $B_1^{*'}$ 和 $B_2^{**'}$, 其中 $U_{\rm E}$ 满足 $U_{\rm E}^{\dagger}U_{\rm E} = U_{\rm E}U_{\rm E}^{\dagger} = I$. Eve将 $B_1^{*'}$ 和 $B_2^{**'}$ 重新发给Bob. 然而, Eve对逻辑量子比特执行幺正操作 $U_{\rm E}$ 将产生新的结果.

例如, 在抵抗集体消相干噪声的QD协议中, Eve对逻辑量子比特 $\{|L\rangle, |V\rangle\}$ 和 $\{|+\rangle, |-\rangle\}$ 执行幺正操作 $U_{\rm E}$ 将产生新的结果:

$$U_{\rm E}|L\rangle|E_i\rangle = \alpha_{00}|00\rangle|e_0e_0\rangle + \alpha_{01}|01\rangle|e_0e_1\rangle$$

$$+\alpha_{10}|10\rangle|e_1e_0\rangle + \alpha_{11}|11\rangle|e_1e_1\rangle, \tag{26}$$

$$U_{\rm E}|V\rangle|E_i\rangle = \beta_{00}|00\rangle|e'_0e'_0\rangle + \beta_{01}|01\rangle|e'_0e'_1\rangle + \beta_{10}|10\rangle|e'_1e'_0\rangle + \beta_{11}|11\rangle|e'_1e'_1\rangle, \tag{27}$$

$$\begin{aligned} U_{\rm E}|\pm\rangle|E_i\rangle = \frac{1}{2}\Big\{ & |\phi^+\rangle[(\alpha_{00}|e_0e_0\rangle + \alpha_{11}|e_1e_1\rangle) \pm (\beta_{00}|e'_0e'_0\rangle + \beta_{11}|e'_1e'_1\rangle)] \\ & + |\phi^-\rangle[(\alpha_{00}|e_0e_0\rangle - \alpha_{11}|e_1e_1\rangle) \pm (\beta_{00}|e'_0e'_0\rangle - \beta_{11}|e'_1e'_1\rangle)] \\ & + |\psi^+\rangle[(\alpha_{01}|e_0e_1\rangle + \alpha_{10}|e_1e_0\rangle) \pm (\beta_{01}|e'_0e'_1\rangle + \beta_{10}|e'_1e'_0\rangle)] \\ & + |\psi^-\rangle[(\alpha_{01}|e_0e_1\rangle - \alpha_{10}|e_1e_0\rangle) \pm (\beta_{01}|e'_0e'_1\rangle - \beta_{10}|e'_1e'_0\rangle)]\Big\}, \end{aligned} \tag{28}$$

其中, $|E_i\rangle$ 是Eve的辅助粒子的量子初态; $|e_0e_0\rangle$, $|e_0e_1\rangle$, $|e_1e_0\rangle$ 和 $|e_1e_1\rangle$ 是Eve可区分的四个量子态; 并且有

$$\begin{aligned} &|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 \\ =&|\beta_{00}|^2 + |\beta_{01}|^2 + |\beta_{10}|^2 + |\beta_{11}|^2 = 1. \end{aligned} \tag{29}$$

假如, 诱骗态处于 $\{|L\rangle, |V\rangle\}$, 为了防止被检测到, 由 (26) 和 (27) 式可知, Eve必须使得

$$\alpha_{00} = \alpha_{10} = \alpha_{11} = \beta_{00} = \beta_{01} = \beta_{11} = 0; \tag{30}$$

若诱骗态处于 $\{|+\rangle, |-\rangle\}$, 为了防止被检测到, 结合 (28) 和 (30) 式可知, Eve 必须使得

$$\begin{aligned} &\alpha_{01}|e_0e_1\rangle - \alpha_{10}|e_1e_0\rangle + \beta_{01}|e'_0e'_1\rangle - \beta_{10}|e'_1e'_0\rangle \\ =&\alpha_{01}|e_0e_1\rangle + \alpha_{10}|e_1e_0\rangle - \beta_{01}|e'_0e'_1\rangle - \beta_{10}|e'_1e'_0\rangle \\ =&\mathbf{0}. \end{aligned} \tag{31}$$

只有在 (30) 和 (31) 式成立的情况下, Eve的纠缠测量攻击才不会被检测到. 当 (30) 式成立时, (31) 式简化为

$$\alpha_{01}|e_0e_1\rangle - \beta_{10}|e'_1e'_0\rangle = \mathbf{0}. \tag{32}$$

若 (32) 式成立, Eve无法区分量子态 $\alpha_{01}|e_0e_1\rangle$ 和 $\beta_{10}|e'_1e'_0\rangle$, 即无法区分量子态 $|L\rangle$ 和 $|V\rangle$. Eve无法通过测量辅助粒子来获得任何有用的量子态信息, 也就无法推知通信双方所交换的秘密信息. 相反, 假如Eve可以区分辅助粒子的量子态 (即使得 $\alpha_{01}|e_0e_1\rangle \neq \beta_{10}|e'_1e'_0\rangle$) 来获取 B_1^* 和 B_2^{**} 所有粒子的量子态, 推知通信双方所交换的秘密信息. 导致 (31) 和 (32) 式不成立, 该攻击干扰到诱骗态 $\{|+\rangle, |-\rangle\}$, 步骤 (3) 和 (6) 可以检测到这种攻击.

同理, 抵抗集体旋转噪声的QD协议和同时抵抗两种集体噪声的QD协议都可抵抗Eve这种纠缠测量攻击.

在三个抵抗集体噪声的QD协议中, Bob最终只公布携带秘密信息粒子的测量结果. Eve猜对携带秘密信息 b_2^i 粒子的量子初态的概率为1/2, Eve根据正确的 b_2^i 量子初态和公布的测量结果推算出正确秘密信息的概率为1/2, 因此, Eve根据通信双方所公开的信息推算出通信双方所交换的秘密信息的概率为1/4, 相当于Eve有 $-\sum p_i \log_2 p_i = -4 \times \frac{1}{4}\log_2\frac{1}{4} = 2$ 比特的秘密消息是未知的, 即通信双方总共交换的2比特秘密消息都是安全的. 若要使QD协议不存在信息泄露必须满足 $-\sum p_i \log_2 p_i \geqslant n$, 其中 n 表示通信双方所交换秘密信息的比特总数, 在等概率的情况下, $p_i \leqslant \frac{1}{2^n}$.

5 结 论

本文提出三个集体噪声信道上带身份认证的量子对话协议, 分别用于抵抗集体消相干噪声、集体旋转噪声以及同时抵抗这两种集体噪声. 通过分析集体噪声对量子态的影响, 利用DFS可免疫集体噪声影响的特性, 构造广义GHZ态和广义幺正变换, 设计集体噪声信道上的量子对话协议. 通信过程的设计是基于"两步"协议的思想, Alice制备广义GHZ态, 保留粒子 a 并将另外两粒子 b_1, b_2 分两次发给Bob; Alice发送粒子 b_1 给Bob告诉Bob粒子 b_2 的量子初态; 确定粒子 b_1 被安全传送后, Alice将自己的秘密信息通过幺正变换加载于 b_2 粒子并发给Bob; Bob同样将自己的秘密信息加载于 b_2 粒子, 测量 b_2 粒子并公布测量结果; 通信双方根据自己的秘密信息, $a(b_1)$ 粒子的测量结果以及Bob公布 b_2 粒子的测量结果便可推知对方的秘密信息, 完成量子对话任务. 通过协议的效率和安全性分析, 该协议能够抵御攻击者Eve的各种攻击, 如干扰攻击、特洛伊木马攻击、截获重发攻击和纠缠测量攻击, 并且不存在信息泄露问题.

参考文献

[1] Beige A, Englert B G, Kurtsiefer C, Weinfurtet H 2002 *J. Phys. A: Math. Gen.* **35** 407

[2] Boström K, Felbinger T 2002 *Phys. Rev. Lett.* **89** 1879021
[3] Wojcik A 2003 *Phys. Rev. Lett.* **90** 157901
[4] Cai Q Y 2003 *Phys. Rev. Lett.* **91** 109801
[5] Cai Q Y, Li B W 2004 *Phys. Rev. A* **69** 054301
[6] Deng F G, Long G L, Liu X S 2003 *Phys. Rev. A* **68** 423171
[7] Zhou N R, Huang P, Liu Y, Gong L H 2008 *Acta Sin. Quantum Opt.* **14** 388 (in Chinese) [周南润, 黄鹏, 刘晔, 龚黎华 2008 量子光学学报 **14** 388]
[8] Yi X J, Nie Y Y, Zhou N R, Huang Y B, Hong Z H 2008 *Int. J. Theor. Phys.* **47** 3401
[9] Yi X J, Nie Y Y, Zhou N R, Hong Z H, Li S S 2008 *Commun. Theor. Phys.* **50** 81
[10] Chong S K, Hwang T 2011 *Opt. Commun.* **284** 515
[11] Yang C W, Tsai C W, Hwang T 2011 *Sci. China G: Phys. Mech. Astron.* **54** 496
[12] Gu B, Zhang C Y, Cheng G S, Huang Y G 2011 *Sci. China G: Phys. Mech. Astron.* **54** 942
[13] Huang W, Wen Q Y, Jia H Y, Qin S J, Gao F 2012 *Chin. Phys. B* **21** 1003081
[14] Liu D, Chen J L, Jiang W 2012 *Int. J. Theor. Phys.* **51** 2923
[15] Wang J, Chen H Q, Zhang Q, Tang C J 2007 *Acta Phys. Sin.* **56** 673 (in Chinese)[王剑, 陈皇卿, 张权, 唐朝京 2007 物理学报 **56** 673]
[16] Wang T Y, Qin S J, Wen Q Y, Zhu F C 2008 *Acta Phys. Sin.* **57** 7452 (in Chinese)[王天银, 秦素娟, 温巧燕, 朱甫臣 2008 物理学报 **57** 7452]
[17] Nguyen B A 2004 *Phys. Lett. A* **328** 6
[18] Ji X, Zhang S 2006 *Chin. Phys.* **15** 1418
[19] Wen X J, Liu Y, Zhou N R 2007 *Opt. Commun.* **275** 278
[20] Gao F, Guo F Z, Wen Q Y, Zhu F C 2008 *Sci. China G: Phys. Mech. Astron.* **51** 559
[21] Gao G 2010 *Opt. Commun.* **283** 2283
[22] Shi G F 2010 *Opt. Commun.* **283** 5275
[23] Gao G, Fang M, Wang Y, Zang D J 2011 *Int. J. Theor. Phys.* **50** 3089
[24] Wang H, Zhang Y Q, Hu Y P 2012 *Int. J. Theor. Phys.* **52** 1745
[25] Wang H, Zhang Y Q, Hu Y P, Tian Y L, Zhu Z C 2012 *J. National Univ. Defense Technol.* **34** 10 (in Chinese) [王鹤, 张玉清, 胡予濮, 田养丽, 朱珍超 2012 国防科技大学学报 **34** 10]
[26] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[27] Yang J, Wang C, Zhang R 2010 *Chin. Phys. B* **19** 110306
[28] Li C Y, Zhou H Y, Wang Y, Deng F G 2005 *Chin. Phys. Lett.* **22** 1049
[29] Cai Q Y, Li B W 2004 *Chin. Phys. Lett.* **21** 601

Quantum dialogue protocols with identification over collection noisy channel without information leakage*

Wu Gui-Tong[1)] Zhou Nan-Run[2)†] Gong Li-Hua[2)] Liu San-Qiu[1)]

1) (*Department of Physics, Nanchang University, Nanchang 330031, China*)

2) (*Department of Electronic Information Engineering, Nanchang University, Nanchang 330031, China*)

(Received 10 June 2013; revised manuscript received 6 October 2013)

Abstract

Three quantum dialogue protocols with identification are proposed under the condition of collection noise. They are used to resist collective-dephasing noise, collective-rotation noise and both collective noises respectively. The two communication parties encode their own secret information into the quantum states with the generalized unitary transformation. Each communication party can deduce the secret message of his counterpart according to his secret message and the two quantum states (one is quantum state before being encoded, and the other is quantum state after being encoded), to achieve a quantum dialogue. It is important that our protocols all should be able to resist various attacks, such as disturbance attack, Trojan horse attack, intercept-resend attack and entanglement measure attack. Moreover, the efficiency and the information leakage of the proposed protocol are analyzed in detail.

Keywords: collection noise, identification, quantum dialogue, without information leakage

PACS: 03.67.–a, 42.50.Ar, 42.79.Sz, 95.75.Kk **DOI:** 10.7498/aps.63.060302

* Project supported by the National Natural Science Foundation of China (Grant No. 10647133), the Foundation for Young Scientists of Jiangxi Province (Jinggang Star), China (Grant No. 20122BCB23002), and the Research Foundation of the Education Department of Jiangxi Province, China (Grant No. GJJ13057).

† Corresponding author. E-mail: znr21@163.com