免疫联合旋转噪声的鲁棒量子对话协议

李冬芬[1,2]，王瑞锦[1,2]，秦志光[1]，张凤荔[1]

(1. 电子科技大学信息与软件工程学院 成都 611731；

2. Electrical Engineering and Computer Science, Northwestern University Evanston Illinois 60208-3118)

【摘要】噪声问题严重影响了量子对话在信息保真、信道容量和信息泄露方面的安全性。针对此问题，该文提出一种免疫联合旋转噪声的鲁棒量子对话协议。通过建立以团簇态为量子载体的，对联合旋转噪声免疫的逻辑量子态，构造相应的消相干自由子空间(DFS)，再构建纠缠交换的量子隐秘信道。通过隐写在信息伪装、信息隐蔽、窃听检测等方面的优势，实现能抵抗旋转噪声的保真量子对话模型，保证秘密信息交换的准确性和安全性。通过比较得出，该文所提出的协议具有最高量子比特效率，且测量只需要单光子。

关 键 词 消相干自由子空间； 联合旋转噪声； 量子对话； 隐写

中图分类号 TP309.3 **文献标志码** A doi:10.3969/j.issn.1001-0548.2017.03.019

Quantum Dialogue Agreement Immune Joint Rotation Noise Robust

LI Dong-fen[1,2], WANG Rui-jin[1,2], QIN Zhi-guang[1], and ZHANG Feng-li[1]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China Chengdu 611731;

2. Electrical Engineering and Computer Science, Northwestern University Evanston Illinois 60208-3118)

Abstract Noise is a serious challenge that militates against the security of quantum dialogue, quantum information fidelity, quantum channel capacity, and quantum information disclosure. In order to solve this problem, we propose a robust quantum dialogue protocol that is immune against joint rotation noise, establish a logical quantum state that is immune to the combined rotation noise in the cluster state which also serves as a quantum carrier, and then construct the corresponding decoherence free subspace (DFS). With advantages of the entangled exchange of quantum cryptography, steganography, and eavesdropping detection, etc, a quantum fidelity dialogue model is realized which is resistant against rotational noise. This model therefore ensures the accuracy and security of the exchange of confidential information through a quantum channel. By comparison, the proposed protocol has the highest quantum bit efficiency, and the measurement requires only a single photon.

Key words DFS; joint rotation noise; quantum dialogue; steganography

信息安全是信息化的生命线，密码系统是信息安全的核心。随着网络的全球化和社会的高度信息化，信息安全方面的事件逐年递增，因此，量子保密通信受到了国内外学术界、军事界和金融界的极大关注[1]。为了减少量子信息泄露，提高交换双方信息保真度和安全性的最主要方式是量子对话(quantum dialogue, QD)[2]。但在传统理想环境下的量子对话协议，无法完全抵御第三方窃听、信息隐藏和噪声干扰。由于光子旅行的时间窗比噪声源变化短，因此光子在量子对话过程中会受到噪声的影响，主要噪声源是联合噪声，包括联合旋转噪声(collective-rotation noise, CRN)和联合退相位噪声(collective-dephasing noise, CDN)[3]。最近的研究表明，由噪声引起的错误率为3.4%～6%[3]，而实际信道能容忍的错误率不能超过11%[4]。即在联合噪声环境下，如果错误率没有超过11%，但第三方攻击者实施了窃听，也会出现严重的“信息泄露”问题[4]，难以保证对话双方交换的秘密信息保真度。因此，联合噪声环境下的量子安全对话协议研究具有重大的科学意义。

量子对话(quantum dialogue, QD)是双向的QSDC(quantum secure direct communication)。这是一种能改变量子通信模式的新方法，可以更快更安全地进行秘密信息的传递，实现从接收者到发送者和

收稿日期：2015－11－09；修回日期：2016－04－15

基金项目：博士后基金(2015M572464)；四川省科技厅计划(2015JY0178, 2016ZC2575)

作者简介：李冬芬(1979－)，女，博士生，主要从事量子安全等方面的研究.

发送者到接收者之间的双向对话。并具备了QSDC及时性和无条件安全性的优点，能实现对话双方相互交换秘密信息，在QSDC领域中占有举足轻重的作用[5]。QD与QSDC的区别在于：前者采用双向通信方式，后者采用单向通信方式。QD提高了信息传递的及时性、保密性和安全性。近年来，量子对话成为研究的热点，并在军事、商业界产生了一定的应用。目前，典型的量子对话协议有：基于EPR纠缠的QD[6]、无信息泄露的QD协议[7]、“两步”协议和“乒乓”协议的QD[8]、基于Bell态和辅助粒子的双向QSDC协议[9]、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[10]、基于Bell态和two-qutrit 纠缠态的无信息泄露的QD协议[11]以及文献[12-16]提出的协议。

但现有的QD协议都是基于理想量子信道，不存在任何噪声的量子信道，且在联合噪声环境下不能同时优化可用性、信道利用率和安全性3个指标，导致了QD协议难以在军事、商业界实际应用。因此，实现高效的、无信息泄露的量子安全对话协议是目前亟需解决的关键性问题。

基于以上分析，本文在免疫联合退相位噪声的量子对话协议基础上，提出联合旋转噪声下鲁棒的量子对话协议。联合旋转噪声的特性，构造无消相干子空间(DFS)，该空间具有抗联合噪声不变的特性)[17]，能提高信息传递的准确性；基于信息隐匿特性进行窃听检测和身份验证，可进一步提高协议的效率和安全性。

1　协议设计

1.1　联合旋转噪声

联合旋转噪声对量子态的影响用幺正算子U_r表示：

$$U_r=\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}$$

其对单粒子态的作用如下：

$$U_d\left|0\right\rangle=\left|0\right\rangle \qquad U_d\left|1\right\rangle=\mathrm{e}^{i\theta}\left|1\right\rangle$$

1.2　以四粒子团簇态为量子载体，建立免疫的保真的量子对话模型

当遭遇联合旋转噪声变化时，光子的水平极化量子态$\left|0\right\rangle$在旋转信道中传输中，其状态将变为$\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle$；光子的垂直极化量子态$\left|1\right\rangle$在旋转信道中传输中，其状态变为$-\sin\theta\left|0\right\rangle+\cos\theta\left|1\right\rangle$。其中，$\theta$是联合噪声参数，它随时间而波动。两个光子可分别表示成逻辑量子态形式，$\left|0_r\right\rangle\equiv\left|\Phi^+\right\rangle=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)$和$\left|1_r\right\rangle\equiv\left|\Psi^-\right\rangle=\frac{1}{\sqrt{2}}(\left|01\right\rangle-\left|10\right\rangle)$(其中下标$r$表示抗联合噪声的逻辑态，$\left|\Phi^+\right\rangle$和$\left|\Psi^-\right\rangle$仅仅是4个原始贝尔态中的其中两个，它们在旋转噪声环境下可以不改变其状态)。两个逻辑态$\left|\Phi^+\right\rangle$和$\left|\Psi^-\right\rangle$的叠加态可以构成对噪声免疫的DFS[18]。在该空间中，另一个测量基为：$\left|+_r\right\rangle=\frac{1}{\sqrt{2}}(\left|0_r\right\rangle+\left|1_r\right\rangle)=\frac{1}{\sqrt{2}}(\left|\Phi^+\right\rangle+\left|\Psi^-\right\rangle)$和$\left|-_r\right\rangle=\frac{1}{\sqrt{2}}(\left|0_r\right\rangle-\left|1_r\right\rangle)=\frac{1}{\sqrt{2}}(\left|\Phi^+\right\rangle-\left|\Psi^-\right\rangle)$。对联合噪声也是免疫的。

在该子空间(DFS)下的两个非正交测量基为：$\{\left|0_r\right\rangle,\left|1_r\right\rangle\}$和$\left\{\left|+\right\rangle_r=\frac{1}{\sqrt{2}}(\left|0_r\right\rangle+\left|1_r\right\rangle),\left|-\right\rangle_r=\frac{1}{\sqrt{2}}(\left|0_r\right\rangle-\left|1_r\right\rangle)\right\}$。

在量子信道中进行通信时，首先发送方将物理的光子表示成逻辑量子态的形式，然后在该信道上进行传输，接收方接收到该逻辑量子态形式后，通过适当的幺正操作就可以恢复到原来的量子态，这样就可以保证传输过程中光子不受噪声的影响，提高光子传输的准确性。

有一个四粒子团簇态，可以表示为：

$$\left|\varphi^+\right\rangle_{XYZM}=\frac{1}{2}(\left|0000\right\rangle+\left|0011\right\rangle+\left|1100\right\rangle+\left|1111\right\rangle)_{XYZM}=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)_{XY}\otimes\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)_{ZM}$$

假设发送者Alice拥有处于最大纠缠的团簇态粒子X、Y、Z和M，如果她要将粒子Y和粒子M发送给接收者Bob。为了防止旋转噪声的影响，Alice首先要将粒子Y和粒子M表示成逻辑量子态，即：$\left|0\right\rangle_Y=\left|\Phi^+\right\rangle_{Y_1Y_2}$，$\left|1\right\rangle_Y=\left|\Psi^+\right\rangle_{Y_1Y_2}$和$\left|0\right\rangle_M=\left|\Phi^+\right\rangle_{M_1M_2}$，$\left|1\right\rangle_M=\left|\Psi^+\right\rangle_{M_1M_2}$，因此$\left|\varphi^+{}_{XYZM}\right\rangle$可表示成：

$$\left|\varphi^+{}_r\right\rangle_{XYZM}=\frac{1}{\sqrt{2}}(\left|0\right\rangle_X\left|\Phi^+\right\rangle_{Y_1Y_2}+\left|1\right\rangle_X\left|\Psi^-\right\rangle_{Y_1Y_2})\otimes\frac{1}{\sqrt{2}}(\left|0\right\rangle_Z\left|\Phi^+\right\rangle_{M_1M_2}+\left|1\right\rangle_Z\left|\Psi^-\right\rangle_{M_1M_2})=$$

$$\frac{1}{2}\left[\left|0\right\rangle_X(\left|00\right\rangle_{Y_1Y_2}+\left|11\right\rangle_{Y_1Y_2})+\left|1\right\rangle_X(\left|01\right\rangle_{Y_1Y_2}-\left|10\right\rangle_{Y_1Y_2})\right]\otimes\frac{1}{2}\left[\left|0\right\rangle_Z(\left|00\right\rangle_{M_1M_2}+\left|11\right\rangle_{M_1M_2})+\left|1\right\rangle_Z(\left|01\right\rangle_{M_1M_2}-\left|10\right\rangle_{M_1M_2})\right]$$

因此，发送者Alice只需要制备二维4量子比特的

贝尔态 $\left|\varphi^{+}\right\rangle_{XYZM}$。然后将粒子 Y_1Y_2 和 M_1M_2 发送给接收者Bob。Alice和Bob分别对粒子 X、Y_1Y_2 和 Z、M_1M_2 进行互换门(swap gate)操作，即 $S_X\otimes S_{Y_1}\otimes S_{Y_2}$ 和 $S_Z\otimes S_{M_1}\otimes S_{M_2}$ 操作(其中，互换门 $S=\begin{pmatrix}1&0\\0&i\end{pmatrix}=\alpha\left|0\right\rangle+i\beta\left|1\right\rangle$，$\alpha$ 和 β 是复数，满足 $\left|\alpha\right|^2+\left|\beta\right|^2=1$)，再进行阿达马门(hadamard gate)操作，即 $H_X\otimes H_{Y_1}\otimes H_{Y_2}$ 和 $H_Z\otimes H_{M_1}\otimes H_{M_2}$ 操作(其中，阿达马门 $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$，$\left|0\right\rangle\equiv\frac{\left(\left|0\right\rangle+\left|1\right\rangle\right)}{\sqrt{2}}$，$\left|1\right\rangle\equiv\frac{\left(\left|0\right\rangle-\left|1\right\rangle\right)}{\sqrt{2}}$)。此时，粒子 XY_1Y_2 和粒子 ZM_1M_2 的联合量子态将变为：

$$\left|\wp_r\right\rangle_{XYZM}=\frac{1}{\sqrt{2}}(\left|1\right\rangle_X\left|10\right\rangle_{Y_1Y_2}+\left|0\right\rangle_X\left|01\right\rangle_{Y_1Y_2})\otimes$$
$$\frac{1}{\sqrt{2}}(\left|1\right\rangle_Z\left|10\right\rangle_{M_1M_2}+\left|0\right\rangle_Z\left|01\right\rangle_{M_1M_2})$$

Bob在接收到逻辑量子态以后，进行适当的变换，就可以得到原始发送的信息。在此，Bob需要进行控制非(C-NOT)操作(其中，控制非C-NOT=$\begin{pmatrix}I&0\\0&I\end{pmatrix}$，$I=\begin{pmatrix}1&0\\0&1\end{pmatrix}=\alpha\left|0\right\rangle+\beta\left|1\right\rangle$，$\alpha$ 和 β 是复数，满足 $\left|\alpha\right|^2+\left|\beta\right|^2=1$)，将 Y_1 和 M_1 作为控制位，将 Y_2 和 M_2 作为靶位，就可以得到：

$$\left|\wp_r\right\rangle'_{XYZM}=\frac{1}{\sqrt{2}}(\left|1\right\rangle_X\left|11\right\rangle_{Y_1Y_2}+\left|0\right\rangle_X\left|01\right\rangle_{Y_1Y_2})\otimes$$
$$\frac{1}{\sqrt{2}}(\left|1\right\rangle_Z\left|11\right\rangle_{M_1M_2}+\left|0\right\rangle_Z\left|01\right\rangle_{M_1M_2})=$$
$$\frac{1}{\sqrt{2}}[(\left|0\right\rangle_X\left|0\right\rangle_{Y_1}+\left|1\right\rangle_X\left|1\right\rangle_{Y_1})\left|1\right\rangle_{Y2}]\otimes$$
$$\frac{1}{\sqrt{2}}[(\left|0\right\rangle_Z\left|0\right\rangle_{M_1}+\left|1\right\rangle_Z\left|1\right\rangle_{M_1})\left|1\right\rangle_{M2}]$$

可以看出，Bob拥有的粒子 Y_1、M_1 和Alice拥有的粒子 X、Z 都任然处于最大纠缠态。由此可以理解为，粒子 Y 和粒子 M 在传输过程中对联合旋转噪声是免疫的。

同样，在联合旋转噪声环境中，光子在信道中传输时 θ 随时间而波动。$\left|\varphi^{+}_{dp}\right\rangle$ 在不同的噪声(即 θ_1 和 θ_2)影响下，建立免疫的四粒子团簇态模型(容忍的量子模型可以通过线性公式表示)：

$$\left|\Phi^{+}{}_r\right\rangle_{12345678}=\frac{1}{\sqrt{2}}(\left|0_r\right\rangle\left|0_r\right\rangle+\left|1_r\right\rangle\left|1_r\right\rangle)_{1234}\otimes$$
$$\frac{1}{\sqrt{2}}(\left|0_r\right\rangle\left|0_r\right\rangle+\left|1_r\right\rangle\left|1_r\right\rangle)_{5678}=$$
$$\frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle)_{1234}\otimes$$
$$\frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle)_{5678}=$$
$$\frac{1}{2\sqrt{2}}[(\left|0_r\right\rangle\left|0_r\right\rangle+\left|1_r\right\rangle\left|1_r\right\rangle)\otimes(\left|0_r\right\rangle\left|0_r\right\rangle+\left|1_r\right\rangle\left|1_r\right\rangle)+$$
$$(\left|0_r\right\rangle\left|0_r\right\rangle-\left|1_r\right\rangle\left|1_r\right\rangle)\otimes(\left|0_r\right\rangle\left|0_r\right\rangle-\left|1_r\right\rangle\left|1_r\right\rangle)]=$$
$$\frac{1}{2\sqrt{2}}[(\left|00\right\rangle+\left|11\right\rangle)(\left|00\right\rangle+\left|11\right\rangle)+$$
$$(\left|01\right\rangle-\left|10\right\rangle)(\left|01\right\rangle-\left|10\right\rangle)]_{1234}\otimes$$
$$\frac{1}{2\sqrt{2}}[(\left|00\right\rangle+\left|11\right\rangle)(\left|00\right\rangle+\left|11\right\rangle)+$$
$$(\left|01\right\rangle-\left|10\right\rangle)(\left|01\right\rangle-\left|10\right\rangle)]_{5678}=$$
$$\frac{1}{2\sqrt{2}}[(\left|0000\right\rangle+\left|0101\right\rangle+\left|1010\right\rangle+\left|1111\right\rangle+$$
$$\left|0011\right\rangle-\left|0110\right\rangle-\left|1001\right\rangle+\left|1100\right\rangle]_{1324}\otimes$$
$$\frac{1}{2\sqrt{2}}[(\left|0000\right\rangle+\left|0101\right\rangle+\left|1010\right\rangle+\left|1111\right\rangle+$$
$$\left|0011\right\rangle-\left|0110\right\rangle-\left|1001\right\rangle+\left|1100\right\rangle]_{5768}=$$
$$\frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle)_{1324}\otimes$$
$$\frac{1}{\sqrt{2}}(\left|\Phi^{+}\right\rangle\left|\Phi^{+}\right\rangle+\left|\Psi^{-}\right\rangle\left|\Psi^{-}\right\rangle)_{5768}$$

由上述公式可知，在联合旋转噪声环境下，θ 随时间而波动时，四粒子团簇态在该信道中传输时不受噪声影响，即对联合旋转噪声是免疫的。

1.3 协议建立的过程

通信双方要规定：在身份的二进制字符串ID中当前位如果是“0”，则Alice需要制备相对应的逻辑量子态 $\left|0\right\rangle_r\equiv\left|\Phi^{+}\right\rangle$，$\left|1\right\rangle_r\equiv\left|\Psi^{-}\right\rangle$。否则需要制备的逻辑量子态为 $\left|+\right\rangle_r=\frac{(\left|0\right\rangle_r+\left|1\right\rangle_r)}{\sqrt{2}}$，$\left|-\right\rangle_r=\frac{(\left|0\right\rangle_r-\left|1\right\rangle_r)}{\sqrt{2}}$。

1) Alice按照规则制备了多个5粒子广义纠缠态序列，将其划分成 X、Y_1 和 Y_2 这3个子序列。其中，X 序列是由 x 个粒子组成的，Y_1 序列是由 y_1 个粒子组成的，Y_2 序列是由 y_2 个粒子组成的；

2) Alice 对序列 X 中的粒子进行测量，并记录下测量结果为 x_i，然后根据自己的身份识别码 $\mathrm{ID}^i{}_X$ 制备 N 个 2 粒子量子态作为诱骗态。如果 $\mathrm{ID}^i{}_X=0$，则 Alice 将第 i 个 2 粒子量子态制备成 $\left|0\right\rangle(\left|0'\right\rangle)$ 或者 $\left|+\right\rangle(\left|+'\right\rangle)$，否则，Alice 将第 i 个 2 粒子量子态制备成

$|1\rangle(|1'\rangle)$ 或者 $|-\rangle(|-'\rangle)$。Alice 将此诱骗态插入到序列 Y_1 中，可以得到一个新的序列 Y_1' 并发送给 Bob，记录下所有诱骗态的相应位置和初始的量子态；

3) Bob收到带有诱骗粒子的序列 Y_1' 后，告知Alice已经收到了粒子序列，则Alice告知Bob在序列 Y_1' 中诱骗粒子的位置，初始量子态以及相应的原理。Bob根据自己的身份识别码 $\mathrm{ID}^i{}_Y$ 依据规则进行操作，选用测量基对相对应的诱骗粒子进行测量，并公示测量结果 $\mathrm{ID}^i{}_M$；

4) Alice验证 $\mathrm{ID}^i{}_Y=\mathrm{ID}^i{}_X\oplus\mathrm{ID}^i{}_M$ 是否成立，如果等式成立，则证明Bob的身份是对的，并且信道是安全的；否则，说明Bob的身份有误或者是信道不安全。同样，Bob也可以验证Alice的身份和信道安全性。在确定等式成立后，可以继续通信。Bob除去诱骗态的粒子后对剩下的粒子 Y_1 进行测量，并记录测量结果为 y_i。根据广义纠缠态的特性可以知道，$x_i=y_i$；

5) Alice根据秘密信息 X_i 对序列 Y_2 中的粒子进行操作，得到新的序列 Y_2'，将新序列 Y_2' 中粒子的顺序打乱，然后制备N个处于 $|0\rangle(|0'\rangle),|1\rangle(|1'\rangle),|+\rangle(|+'\rangle),|-\rangle(|-'\rangle)$ 的2粒子量子态作为诱骗态，随机的插入到已打乱顺序的新序列 Y_2' 中，得到序列 Y_2'' 并发送给Bob，记录所有诱骗态的位置和初始的量子态。Bob收到序列 Y_2'' 后，告知Alice已经收到了序列 Y_2''。同样，Alice公布诱骗态的位置和对应的测量基，Bob用测量基对诱骗态进行测量，并公布测量结果。Alice和Bob对测量结果和初始诱骗进行对比，如果Bob的测量结果等于初始态，则证明信道是安全的，双方可以继续通信；如果Bob的测量结果不等于初始态，则证明信道是不安全的，丢弃这次通信，重新进行通信；

6) Alice通过经典信道告知Bob序列 Y_2' 的正确次序，Bob对序列 Y_2' 进行重新排序，进行适当的测量并公布测量结果。完成了量子的对话。

因此，利用隐写建立的量子安全对话协议既能一次传递两种同时具有不同安全等级的经典比特，又能进行身份验证和窃听检测，具有很高的安全性和良好的信息隐秘性。

2　安全性分析

2.1　信息泄露问题

按照四粒子团簇态的特性，和比特纠缠态 $\left|\Phi^+{}_r\right\rangle_{12345678}$ 的测量相关性，Alice能从她自己的测量结果可以推断出Bob，Bob拥有的粒子 Y_1、M_1 和Alice拥有的粒子 X，Z 都任然处于最大纠缠态，这样Bob就没有必要告知Alice他自己的测量结果。这样Eve就没有办法知道Bob的新的状态，因此，被Alice测量的结果 $\left|1_r\right\rangle_b$ 包含了Alice和Bob交换秘密信息的4种逻辑酉操作组合，即 $\{k_n=1,i_n=0\}$，$\{k_n=0,i_n=1\}$，$\{k_n=1,i_n=1\}$ 和 $\{k_n=0,i_n=0\}$。根据信息论Shannon的进行评估，对于Eve而言，包含：

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

的比特信息。可以看出，信息泄露问题不存在，说明四粒子团簇态的比特纠缠态 $\left|\Phi^+{}_r\right\rangle_{12345678}$ 能很好的免疫联合旋转噪声下的信息泄露问题。

2.2　截获-重发攻击

攻击者Eve事先准备了4个 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$ 态，构成一个逻辑量子比特序列T, 当Alice发送 $N+\Omega_2$ (混合序列)给Bob时，Eve拦截这个组合序列，然后他送给Bob逻辑量子比特序列T，而不是 $N+\Omega_2$，Bob收到后，检测两个信息的不同，因此Eve测量测量的概率是 $\frac{1}{2}$。

2.3　Eve的主动攻击

当Alice和Bob是开始量子对话时，窃听者Eve就可以进行不可见光子窃听和延迟光子木马的攻击[19]。Bob可以通过使用滤网过滤无形光子，然后通过使用分离器的光子数检测延迟光子[20]。本文协议进行了两次检测。因此，当Bob和Alice对话时，本文协议使用的诱骗光子技术[21]，由于诱骗光子随机处于以下4种状态 $\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$，因此等效于安全BB84协议[22]，确保对话的安全性。攻击者Eve可以不知道诱骗逻辑量子位的具体位置和测量的位置。如果攻击者Eve进行攻击，则在第二次安全检测时被检测出来。如果Eve截取了Alice和Bob的对话秘密顺序，她也无法知道信息逻辑量子比特的真实位置和初始状态，所以任何攻击都会被检测到。

据Stinespring扩张定理[23]，Eve的攻击可以被认为是在一个大的Hilbert空间 $H_{AB}\otimes H_E$ 上的执行统一的操作 $\hat{E}$。假设Eve的辅助状态为 $|e\rangle$，因此：

$$\hat{E}|0,e\rangle=\alpha|0,e_{00}\rangle+\beta|1,e_{01}\rangle$$
$$\hat{E}|1,e\rangle=\alpha'|0,e_{10}\rangle+\beta'|1,e_{11}\rangle$$

$\hat{E}|+,e\rangle$ 和 $\hat{E}|-,e\rangle$ 有4种状态。因为 $\hat{E}$ 是整体的操作，复杂的 α，β，α',β' 必须满足 $\hat{E}\hat{E}^{\dagger}=I$，因此，$|\alpha|^2=|\alpha'|^2$，$|\beta|^2=|\beta'|^2$，那么Eve攻击的概率 $e=|\beta|^2=1-|\alpha|^2$。

从信息论的观点来看，一个量子系统内可以得到信息不大于Holevo的极限，即 $\chi(\rho)=S(\rho)-\sum_i p_i S(\rho_i)$，其中，$S(\rho)$ 是冯·诺依曼的熵 ρ，$\rho=\sum_i P_i\rho_i$（ρ_i 的量子态的制备是通过Alice的概率为 ρ），如果Alice准备4诱骗通过光子的概率 $\frac{1}{4}$，那么诱骗照片的香农熵 $H(\rho)=-\sum_i P_i\log_2 P_i=2$，那么Eve可以得到的信息是

$$I_E \leqslant S(\rho)-\sum_i P_i S(\rho_i) < H(P)$$

因此，Eve不能得到诱骗光子的完整信息，并且可以通过对话方检测Eve的窃听行为。

3 讨 论

3.1 信息论效率

文献[24]的信息论效率被定义为 $\xi=\frac{b_s}{q_t+b_t}$，其中，b_s 是通信获得的秘密比特数，q_t 是量子比特数，b_t 是Alice和Bob传播者之间交换的比特数。本文协议的信息论效率为：

$$\xi=\frac{b_s}{q_t+b_t}=\frac{4}{4+1}\times 100\%=40\%$$

事实上，量子比特的制备和传输，比经典信息更加复杂。文献[24]信息论效率公式并不能完全充分衡量量子密码协议的效率。

对此，采用量子比特效率进行有效补充，其定义为 $\eta=\frac{b_n}{q_t}$，其中 b_n 是用到的量子比特，q_t 是总的量子比特传输，通常结合这两个参数进行评价评价信息论效率。通过计算得知，本文提出的免疫联合旋转噪声的鲁棒量子对话协议的效率是100%。

3.2 与其他量子对话协议相比

将本文协议与文献[25-27]的协议进行比较，结果如表1所示。

表1 与之前的协议的对比

对比项目	文献[17]的协议	文献[18]的协议	文献[19]的协议	本文协议
初始量子资源	逻辑Bell态	逻辑量子比特	两个逻辑Bell态	原始Bell态和单光子
量子测量	Bell态	Bell态	单光子	单光子
信息论效率/%	40	40	33.3	40
量子比特效率/%	60	60	66.4	100

从表1可知，在最初的量子资源的选择上，文献[25]选择逻辑Bell态，文献[26]选择逻辑量子位，文献[27]选择了两个原始Bell态，本文协议选择逻辑量子比特和单光子；在量子测量方面，文献[25-26]采用Bell测量，文献[27]和本文协议采用单光子测量；在信息论效率方面，文献[25-26]和本文协议是40%，文献[27]为33.3%。在量子比特效率方面，本文协议高达100%，但文献[25-27]只分别达到60%和66.4%。

4 结 束 语

本文在最新研究的免疫联合退相位噪声的量子对话协议基础上[12]，提出了联合旋转噪声下鲁棒的量子对话协议，针对联合旋转噪声的特性，构造无消相干子空间(DFS)，提高信息传递的准确性；基于隐写的信息隐匿特性，进行窃听检测和身份验证，进一步提高协议的效率和安全性。与其他协议相比较可知，本文协议具有最高量子比特效率，且测量只需要单光子。为了使协议更加适用于远距离通信需求，下一步将重点研究噪声中多自由度的连续变量量子隐形传态协议。

参 考 文 献

[1] LEANDRO A, FERMANDO D M, LUIZ D. Open-system dynamics of entanglement: a key issues review[J]. Reports on Progress in Physics, 2015, 78(4): 1-79.

[2] BEIGEE A, ENGLERT B G, KURTSIEFER C, et al. Secure communication with a publicly known key[J]. Acta Physica Polonica, 2002, 101(3): 357-368.

[3] YANG C W, TSAI C W, HANG T. Fault tolerant two-step quantum secure direct communication protocol against collective noises[J]. Science China Physics, Mechanics and Astronomy, 2011, 54(3): 496-501.

[4] WANG T J, SONG S Y, LONG G L. Complete analysis and generation of hyperentangled Greenberger-Horne-Zeilinger state for photons using quantum-dot spins in optical microcavities[EB/OL]. [2015-05-16]. http://arxiv.org/abs/1211.0082.

[5] XIN J, SHOU Z. Secure quantum dialogue based on single-photon[J]. Chinese Physics, 2006, 15(7): 1418-1420.

[6] FAN X J, LI A Y, TIAN S F, et al. Effects of relative phase in an open ladder system without incoherent pumping[J]. The European Physical Journal D, 2007, 42(3): 483-488.

[7] GAO F, GUO F Z, WEN Q Y, et al. Consistency of shared reference frames should be reexamined[J]. Physical Review A, 2008, 77(1): 77-89.

[8] El-AMRAOUI M, GADRET G, JULES J C, et al. Microstructured chalcogenide optical fibers from As 2 S 3 glass: Towards new IR broadband sources[J]. Optics Express, 2010, 18(25): 26655-26665.

[9] SHI G F. Bidirectional quantum secure communication scheme based on Bell states and auxiliary particles[J]. Optics Communications, 2010, 283(24): 5275-5278.

[10] CHATRCHYAN S, KHACHATRYAN V, SIRUNYAN A M, et al. Observation and studies of jet quenching in PbPb collisions at sNN= 2.76 TeV[J]. Physical Review C, 2011, 84(2): 11-20.
[11] BARTOLI B, BEMARDINI P, BI X J, et al. Light-component spectrum of the primary cosmic rays in the multi-TeV region measured by the ARGO-YBJ experiment[J]. Physical Review D, 2012, 85(9): 98-115.
[12] WANG Rui-jin, LI Dong-fen, QIN Zhi-guang. An immune quantum communication model for dephasing noise using four-qubit cluster state[J]. International Journal of Theoretical Physics, 2016, 55(1): 609-616.
[13] WANG Rui-jin, LI Dong-fen, DENG Fu-hu. Quantum information splitting of a two-qubit bell state using a five-qubit entangled state[J]. International Journal of Theoretical Physics. 2015, 54(9): 3229-3237.
[14] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li. Quantum information splitting of a two-qubit Bell state using a four-qubit entangled state[J]. Chinese Physics C, 2015, 39(4): 26-30.
[15] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li, et al. Quantum information splitting of arbitrary two-qubit state by using four-qubit cluster state and Bell-state[J]. Quantum Information Processing, 2015, 14(3): 1103-1116.
[16] LI Dong-fen, WANG Rui-jin, ZHANG Feng-li, et al. Quantum information splitting of arbitrary three-qubit state by using seven-qubit entangled state[J]. International Journal of Theoretical Physics, 2015, 54(6): 2068-2075.
[17] LI X H, DENG F G, ZHUO H Y. Efficient quantum key distribution over a collective noise channel[J]. Physical Review A, 2008, 78(2): 022321.
[18] WALTON Z D, ABOURADDY A F. Decoherence- free subspaces in quantum key distribution[J]. Physical Review Letters, 2003, 91(8): 1-4.
[19] GISIN N, RIBORDY G, TITTEL W, et al. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-152.
[20] LI X H, DENG F G, ZHOU H Y. Improving the security of secure direct communication based on the secret transmitting order of particles[J]. Physical Review A, 2006, 74(5): 1-22.
[21] LIU Z, FU B, YI X, et al. Co-doping of magnesium with indium in nitrides: First principle calculation and experiment[J]. RSC Advances, 2016, 6(6): 5111-5115.
[22] WANG T J, LIU L L, ZHANG R, et al. One-step hyperentanglement purification and hyperdistillation with linear optics[J]. Optics Express, 2015, 23(7): 9284-9294.
[23] STINESPRING W F. Positive functions on C*-algebras[J]. Proceedings of the American Mathematical Society, 1955, 6(2): 211-216.
[24] CABELLO A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635.
[25] YE T Y. Robust quantum dialogue based on a shared auxiliary logical Bell state against collective noise[J]. Scientia Sinica Physica, Mechanica & Astronomica, 2015, 45(4): 0301-0307.
[26] YANG C W, HANG T. Quantum dialogue protocols immune to collective noise[J]. Quantum Information Processing, 2013, 12(6): 2131-2142.
[27] YE Tian-yu. Information leakage resistant quantum dialogue against collective noise[J]. Science China Physics Mechanics, 2014, 57(12): 2266-2275.

编 辑 蒋 晓