基于四粒子纠缠态的两方量子密钥协商协议

何业锋

(西安邮电大学通信与信息工程学院 西安 710121)

【摘要】量子密钥协商协议允许参与者通过公开的量子信道公平地协商一个共享秘密密钥，任何参与者的子集都不能独立地确定该共享密钥。它的安全性由量子力学原理保证，因此能够实现无条件安全，已经吸引了大量的关注。该文基于四粒子纠缠态和逻辑量子比特，提出了两个分别抵抗集体退相位噪声和集体旋转噪声的鲁棒的两方量子密钥协商协议。安全性分析证明这两个协议既能抵抗参与者和外部攻击，也能成功地抵抗两种特洛伊木马攻击。另外，这两个协议也能达到比较高的量子比特效率。

关 键 词 四粒子纠缠态；外部攻击；参与者攻击；量子密钥协商；量子密码

中图分类号 TN918.1 **文献标志码** A doi:10.3969/j.issn.1001-0548.2017.02.004

Two-Party Quantum Key Agreement Protocols Based on Four-Particle Entangled States

HE Ye-feng

(School of Telecommunication and Information Engieering, Xi'an University of Posts and Telecommunications Xi'an 710121)

Abstract Quantum key agreement (QKA) protocols allow participants to negotiate a classical shared secret key fairly via public quantum channels. Furthermore, the shared key cannot be determined independently by any subset of the participants. Their security is assured by the quantum mechanics principles, so they can achieve unconditional security and have drawn considerable attention. Based on four-particle entangled states and logical qubits, two robust two-party quantum key agreement protocols against collective-dephasing noise and collective-rotation noise are proposed. The security analysis shows that the two protocols can not only resist against participant attacks and outsider attacks, but also resist against two kinds of Trojan horse attacks. Furthermore, the two protocols also achieve higher qubit efficiency.

Key words four-particle entangled state; outsider attack; participant attack; QKA; quantum cryptography

量子密码是密码学和量子力学结合的产物，它的安全性是由量子力学基本原理保证的(例如海森堡测不准原理和量子不可克隆原理)，而不是基于数学假设。因此，量子密码协议能够实现无条件安全，已经成为国内外量子信息领域的研究热点。目前，许多种类的量子密码协议已经被提出，包括：量子密钥分发[1]、量子秘密共享[2]、量子安全直接通信[3]和量子密钥协商(QKA)[4-5]等。其中，量子密钥协商协议允许参与者通过量子信道公平地协商一个经典的共享秘密密钥，并且任何一个参与者或参与者的子集都不能独立地确定该共享密钥。目前，它已经成为量子密码协议的新研究热点。

文献[4]基于量子隐形传态技术提出了第一个QKA协议。然而，文献[6]发现在此协议中一个不诚实的参与者可以完全独立地确定共享密钥而不会被检测到，因此该协议不能抵抗参与者攻击。文献[5]基于单光子基和幺正变换也提出了一个QKA协议，但此协议不能抵抗CNOT攻击[7]。文献[8]基于BB84协议[1]提出了一个成功的两方QKA协议。这个协议主要基于幺正变换和延迟测量技术，并且该协议能实现很高的量子比特效率。基于Bell态，几个新的双方QKA协议也被提出，如文献[9-10]。文献[10]将两方QKA协议的概念推广到了多方QKA协议。许多三方和多方的QKA协议也被提出[11-12]。这些协议中有些是安全的，也有些存在安全漏洞。但上述协议大多数是基于单粒子或Bell态的。文献[13]利用四粒子的团簇态提出了一个双方QKA协议，此协议具有较高的量子比特效率。因此，设计更多的基于多粒子

收稿日期：2015 – 10 – 25；修回日期：2016 – 03 – 30
基金项目：国家自然科学基金(61373171, 61472472, 61272037)；陕西省教育厅专项科研计划(14JK1659)
作者简介：何业锋(1978 –)，女，博士，副教授，主要从事通信与网络安全方面的研究.

纠缠态的QKA协议是非常有意义的。然而，上述QKA协议几乎都是在理想量子信道上进行密钥协商，并未考虑量子信道中噪声的影响。而在实际通信中，量子信道中的噪声是不可避免的。通常，人们将信道噪声视为集体噪声。这主要是因为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[14-17]。为了消除集体噪声的影响，一个有效的方法是构造无消相干子空间(decoherence-free subspace, DFS)[16,18-20]，因为无消相干态几乎不受集体噪声的影响。目前，研究者已经提出了一些基于无消相干态的鲁棒量子密码协议，如鲁棒量子密钥分发协议[14-16]和鲁棒量子对话[19-20]等。然而，基于无消相干态的鲁棒QKA协议相对较少。文献[21]基于EPR对和单粒子测量提出了一个两方QKA协议，并利用无消相干态给出了它在噪声信道上的实现。文献[22]又基于无消相干态给出了免疫集体噪声的鲁棒QKA协议。

本文基于四粒子 χ 态和逻辑量子比特(2量子比特DF态)设计了两个分别抵抗集体退相位噪声和集体旋转噪声的鲁棒QKA协议。这两个QKA协议都有较高的量子比特效率。安全性分析表明它们能抵抗已有的参与者攻击和外部攻击。而且，由于这两个QKA协议中的每个粒子仅被传输一次，因此攻击者也无法执行特洛伊木马攻击[23-24]。

1　理论知识

众所周知，$\{|0\rangle,|1\rangle\}$ 形成了*Z*基，$\{|+\rangle,|-\rangle\}$ 形成了*X*基，其中 $|+\rangle=1/\sqrt{2}(|0\rangle+|1\rangle)$，$|-\rangle=1/\sqrt{2}(|0\rangle-|1\rangle)$。4个Bell态为：

$$|\phi^+\rangle=1/\sqrt{2}(|00\rangle+|11\rangle)\quad |\phi^-\rangle=1/\sqrt{2}(|00\rangle-|11\rangle)$$
$$|\psi^+\rangle=1/\sqrt{2}(|01\rangle+|10\rangle)\quad |\psi^-\rangle=1/\sqrt{2}(|01\rangle-|10\rangle) \quad (1)$$

它们形成了四维Hilbert空间的一组完全正交基，即Bell基。 χ 态是四粒子的最大纠缠态，本文的协议使用如下的一个 χ 态作为量子信源[25]，即：

$$\begin{aligned}|\chi^{00}\rangle_{ABCD}=&\frac{1}{2\sqrt{2}}(|0000\rangle+|0011\rangle-|0101\rangle+|0110\rangle+\\&|1001\rangle+|1010\rangle+|1100\rangle-|1111\rangle)_{ABCD}=\\&\frac{1}{2}(|\phi^+\rangle_{AB}|00\rangle_{CD}-|\psi^-\rangle_{AB}|01\rangle_{CD}+\\&|\psi^+\rangle_{AB}|10\rangle_{CD}+|\phi^-\rangle_{AB}|11\rangle_{CD})\end{aligned} \quad (2)$$

根据上式可知，若对 $|\chi^{00}\rangle_{ABCD}$ 的粒子 *A* 和 *B* 执行Bell测量，对粒子 *C* 和 *D* 执行 $Z\otimes Z$ 基测量($Z\otimes Z=\{|00\rangle,|01\rangle,|10\rangle,|11\rangle\}$)，则系统分别以1/4的概率塌缩到态 $|\phi^+\rangle_{AB}|00\rangle_{CD}$，$|\psi^-\rangle_{AB}|01\rangle_{CD}$，$|\psi^+\rangle_{AB}|10\rangle_{CD}$ 和 $|\phi^-\rangle_{AB}|11\rangle_{CD}$。

2　新的两方量子密钥协商协议

2.1　抗集体退相位噪声的量子密钥协商协议

一个量子信道上的集体退相位噪声对两个极化光子 $|0\rangle$ 和 $|1\rangle$ 的影响可以表述为[16]：

$$U_{dp}|0\rangle=|0\rangle\quad U_{dp}|1\rangle=e^{i\varphi}|1\rangle \quad (3)$$

式中，φ 是随时间变化的集体退相位噪声参数。两个逻辑量子比特 $|0\rangle_{dp}=|01\rangle$，$|1\rangle_{dp}=|10\rangle$ 以及它们的叠加态 $|\pm\rangle_{dp}=1/\sqrt{2}(|0\rangle_{dp}\pm|1\rangle_{dp})=1/\sqrt{2}(|01\rangle\pm|10\rangle)$ 都不受集体退相位噪声的影响[18-20]。

假设Alice和Bob两人想协商一个秘密密钥。首先，Alice和Bob协商如下量子态的编码：

$$\begin{aligned}&|\phi^+\rangle_{AB}\to 00\quad |\psi^-\rangle_{AB}\to 01\quad |\psi^+\rangle_{AB}\to 10\\&|\phi^-\rangle_{AB}\to 11\quad |00\rangle_{CD}\to 00\quad |01\rangle_{CD}\to 01\\&|10\rangle_{CD}\to 10\quad |11\rangle_{CD}\to 11\end{aligned} \quad (4)$$

协议步骤如下：

1) Alice准备 *n* 个逻辑 χ 态 $|\chi^{00}_{dp}\rangle_{ABCD}$：

$$\begin{aligned}|\chi^{00}_{dp}\rangle_{ABCD}=&\frac{1}{2\sqrt{2}}(|0\rangle|0\rangle|0\rangle_{dp}|0\rangle_{dp}+|0\rangle|0\rangle|1\rangle_{dp}|1\rangle_{dp}-\\&|0\rangle|1\rangle|0\rangle_{dp}|1\rangle_{dp}+|0\rangle|1\rangle|1\rangle_{dp}|0\rangle_{dp}+\\&|1\rangle|0\rangle|0\rangle_{dp}|1\rangle_{dp}+|1\rangle|0\rangle|1\rangle_{dp}|0\rangle_{dp}+\\&|1\rangle|1\rangle|0\rangle_{dp}|0\rangle_{dp}-|1\rangle|1\rangle|1\rangle_{dp}|1\rangle_{dp})_{ABCD}=\\&\frac{1}{2\sqrt{2}}(|00\rangle_{AB}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}+|00\rangle_{AB}|10\rangle_{C_1C_2}|10\rangle_{D_1D_2}-\\&|01\rangle_{AB}|01\rangle_{C_1C_2}|10\rangle_{D_1D_2}+|01\rangle_{AB}|10\rangle_{C_1C_2}|01\rangle_{D_1D_2}+\\&|10\rangle_{AB}|01\rangle_{C_1C_2}|10\rangle_{D_1D_2}+|10\rangle_{AB}|10\rangle_{C_1C_2}|01\rangle_{D_1D_2}+\\&|11\rangle_{AB}|01\rangle_{C_1C_2}|01\rangle_{D_1D_2}-|11\rangle_{AB}|10\rangle_{C_1C_2}|10\rangle_{D_1D_2})\end{aligned} \quad (5)$$

并将所有粒子分成4个有序的序列，其中序列 S_A 和 S_B 分别由所有的光子 *A* 和 *B* 组成；而序列 S_C 和 S_D 分别由所有的逻辑量子比特 *C* 和 *D* 组成。Alice从集合 $\{|0\rangle_{dp},|1\rangle_{dp},|+\rangle_{dp},|-\rangle_{dp}\}$ 中随机选出足够多(例如 2*m* 个)的诱骗逻辑量子比特，并且随机地插入序列 S_C 和 S_D 得到新的序列 S'_C 和 S'_D。Alice保留序列 S_A 和 S_B，将序列 S'_C 和 S'_D 发送给Bob。

2) 当Bob收到序列 S'_C 和 S'_D 后，通过经典认证信道告知Alice。Alice公布诱骗逻辑量子比特的位置与相应的制备基。则Bob用正确的测量基去测量相应的

诱骗逻辑量子比特，并将测量结果告诉Alice。Alice比较测量结果和诱骗逻辑量子比特的初始状态，并计算错误率，根据错误率的值判断窃听者Eve是否存在。如果错误率低于预先给定的门限值(例如0.1～0.2之间的某个值)，则Alice和Bob继续此协议的下一步。否则，认为存在Eve窃听，Alice和Bob停止此协议并且重新开始。

3) 除去诱骗粒子后，序列 S_C' 和 S_D' 又恢复为序列 S_C 和 S_D。Bob对序列 S_C 中的每一个逻辑量子比特中的光子 C_1 和 C_2 执行CNOT操作，其中 C_1 作为控制量子比特，C_2 作为目标量子比特。同样，Bob也对序列 S_D 中的每一个逻辑量子比特中的光子 D_1 和 D_2 执行CNOT操作，其中 D_1 作为控制量子比特，D_2 作为目标量子比特。执行两次CNOT操作后，每一个逻辑 χ 态 $\left|\chi_{dp}^{00}\right\rangle_{ABCD}$ 变为一个新的量子态 $\left|\Lambda_{dp}\right\rangle_{ABCD}$：

$$\begin{aligned}\left|\Lambda_{dp}\right\rangle_{ABCD}=&\frac{1}{2\sqrt{2}}(\left|00\right\rangle_{AB}\left|01\right\rangle_{C_1C_2}\left|01\right\rangle_{D_1D_2}+\\&\left|00\right\rangle_{AB}\left|11\right\rangle_{C_1C_2}\left|11\right\rangle_{D_1D_2}-\\&\left|01\right\rangle_{AB}\left|01\right\rangle_{C_1C_2}\left|11\right\rangle_{D_1D_2}+\left|01\right\rangle_{AB}\left|11\right\rangle_{C_1C_2}\left|01\right\rangle_{D_1D_2}+\\&\left|10\right\rangle_{AB}\left|01\right\rangle_{C_1C_2}\left|11\right\rangle_{D_1D_2}+\left|10\right\rangle_{AB}\left|11\right\rangle_{C_1C_2}\left|01\right\rangle_{D_1D_2}+\\&\left|11\right\rangle_{AB}\left|01\right\rangle_{C_1C_2}\left|01\right\rangle_{D_1D_2}-\left|11\right\rangle_{AB}\left|10\right\rangle_{C_1C_2}\left|10\right\rangle_{D_1D_2})=\\&\frac{1}{2\sqrt{2}}(\left|0000\right\rangle+\left|0011\right\rangle-\left|0101\right\rangle+\left|0110\right\rangle+\\&\left|1001\right\rangle+\left|1010\right\rangle+\left|1100\right\rangle-\left|1111\right\rangle)_{ABC_1D_1}\left|11\right\rangle_{C_2D_2}=\\&\left|\chi^{00}\right\rangle_{ABC_1D_1}\left|11\right\rangle_{C_2D_2}\end{aligned}\tag{6}$$

因此，Alice和Bob已经共享了 n 个 χ 态 $\left|\chi^{00}\right\rangle_{ABC_1D_1}$。Alice对序列 S_A 和 S_B 中序号相同的两个粒子执行Bell测量，而Bob对序列 S_C 和 S_D 中序号相同的两个粒子 C_1 和 D_1 执行 $Z\otimes Z$ 基测量。由于 χ 态 $\left|\chi^{00}\right\rangle_{ABC_1D_1}$ 的测量相关性和事先两人协商的量子态的编码，Alice和Bob能共享相同的 $2n$ 比特的经典秘密密钥，即为两人的共享密钥。

下面举例说明为什么Alice和Bob能得到相同的密钥。设 $n=1$，在协议的步骤3)，Alice和Bob分别拥有同一个 χ 态 $\left|\chi^{00}\right\rangle_{ABC_1D_1}$ 的两个粒子，即Alice拥有粒子 A 和 B，而Bob拥有粒子 C_1 和 D_1。当Alice对粒子 A 和 B 执行Bell测量，Bob对粒子 C_1 和 D_1 执行 $Z\otimes Z$ 基测量后，$\left|\chi^{00}\right\rangle_{ABC_1D_1}$ 态必然以1/4的概率塌缩到态 $\left|\phi^+\right\rangle_{AB}\left|00\right\rangle_{C_1D_1}$，$\left|\psi^-\right\rangle_{AB}\left|01\right\rangle_{C_1D_1}$，$\left|\psi^+\right\rangle_{AB}\left|10\right\rangle_{C_1D_1}$ 和 $\left|\phi^-\right\rangle_{AB}\left|11\right\rangle_{C_1D_1}$ 中的某一个。假设 $\left|\chi^{00}\right\rangle_{ABC_1D_1}$ 态塌缩到态 $\left|\psi^-\right\rangle_{AB}\left|01\right\rangle_{C_1D_1}$。则Alice的Bell测量结果为 $\left|\psi^-\right\rangle_{AB}$，根据事先协商的量子态的编码，Alice得到的共享密钥为01。而Bob的 $Z\otimes Z$ 基测量结果为 $\left|01\right\rangle_{C_1D_1}$，根据事先协商的量子态的编码，Alice得到的共享密钥也为01。因此，Alice和Bob得到了相同的共享密钥。

2.2 抗集体旋转噪声的量子密钥协商协议

一个量子信道上的集体旋转噪声对两个极化光子 $\left|0\right\rangle$ 和 $\left|1\right\rangle$ 的影响可以表述为[18-20]：

$$\begin{aligned}U_r\left|0\right\rangle&=\cos\theta\left|0\right\rangle+\sin\theta\left|1\right\rangle\\U_r\left|1\right\rangle&=-\sin\theta\left|0\right\rangle+\cos\theta\left|1\right\rangle\end{aligned}\tag{7}$$

式中，θ 是随时间变化的集体旋转噪声参数。两个逻辑量子比特 $\left|0\right\rangle_r=\left|\phi^+\right\rangle$，$\left|1\right\rangle_r=\left|\psi^-\right\rangle$ 以及它们的叠加态 $\left|\pm\right\rangle_r=1/\sqrt{2}(\left|0\right\rangle_r\pm\left|1\right\rangle_r)$ 都不受集体旋转噪声的影响[18-20]。

假设Alice和Bob两人想协商一个秘密密钥。首先，Alice和Bob协商如下量子态的编码：

$$\begin{aligned}&\left|\phi^+\right\rangle_{AB}\to00\quad\left|\psi^-\right\rangle_{AB}\to01\\&\left|\psi^+\right\rangle_{AB}\to10\quad\left|\phi^-\right\rangle_{AB}\to11\\&\left|\phi^+\right\rangle_{C_1C_2}\left|\phi^+\right\rangle_{D_1D_2}\to00\quad\left|\phi^+\right\rangle_{C_1C_2}\left|\psi^-\right\rangle_{D_1D_2}\to01\\&\left|\psi^-\right\rangle_{C_1C_2}\left|\phi^+\right\rangle_{D_1D_2}\to10\quad\left|\psi^-\right\rangle_{C_1C_2}\left|\psi^-\right\rangle_{D_1D_2}\to11\end{aligned}\tag{8}$$

协议步骤如下：

1) Alice准备 n 个逻辑 χ 态 $\left|\chi_r^{00}\right\rangle_{ABCD}$：

$$\begin{aligned}\left|\chi_r^{00}\right\rangle_{ABCD}=&\frac{1}{2\sqrt{2}}(\left|0\right\rangle\left|0\right\rangle\left|0\right\rangle_r\left|0\right\rangle_r+\left|0\right\rangle\left|0\right\rangle\left|1\right\rangle_r\left|1\right\rangle_r-\\&\left|0\right\rangle\left|1\right\rangle\left|0\right\rangle_r\left|1\right\rangle_r+\left|0\right\rangle\left|1\right\rangle\left|1\right\rangle_r\left|0\right\rangle_r+\\&\left|1\right\rangle\left|0\right\rangle\left|0\right\rangle_r\left|1\right\rangle_r+\left|1\right\rangle\left|0\right\rangle\left|1\right\rangle_r\left|0\right\rangle_r+\\&\left|1\right\rangle\left|1\right\rangle\left|0\right\rangle_r\left|0\right\rangle_r-\left|1\right\rangle\left|1\right\rangle\left|1\right\rangle_r\left|1\right\rangle_r)_{ABCD}=\\&\frac{1}{4\sqrt{2}}[\left|00\right\rangle_{AB}(\left|00\right\rangle+\left|11\right\rangle)_{C_1C_2}(\left|00\right\rangle+\left|11\right\rangle)_{D_1D_2}+\\&\left|00\right\rangle_{AB}(\left|01\right\rangle-\left|10\right\rangle)_{C_1C_2}(\left|01\right\rangle-\left|10\right\rangle)_{D_1D_2}-\\&\left|01\right\rangle_{AB}(\left|00\right\rangle+\left|11\right\rangle)_{C_1C_2}(\left|01\right\rangle-\left|10\right\rangle)_{D_1D_2}+\\&\left|01\right\rangle_{AB}(\left|01\right\rangle-\left|10\right\rangle)_{C_1C_2}(\left|00\right\rangle+\left|11\right\rangle)_{D_1D_2}+\\&\left|10\right\rangle_{AB}(\left|00\right\rangle+\left|11\right\rangle)_{C_1C_2}(\left|01\right\rangle-\left|10\right\rangle)_{D_1D_2}+\\&\left|10\right\rangle_{AB}(\left|01\right\rangle-\left|10\right\rangle)_{C_1C_2}(\left|00\right\rangle+\left|11\right\rangle)_{D_1D_2}+\\&\left|11\right\rangle_{AB}(\left|00\right\rangle+\left|11\right\rangle)_{C_1C_2}(\left|00\right\rangle+\left|11\right\rangle)_{D_1D_2}-\\&\left|11\right\rangle_{AB}(\left|01\right\rangle-\left|10\right\rangle)_{C_1C_2}(\left|01\right\rangle-\left|10\right\rangle)_{D_1D_2}]=\\&\frac{1}{4\sqrt{2}}[(\left|00\right\rangle+\left|11\right\rangle)_{AB}(\left|00\right\rangle+\left|11\right\rangle)_{C_1C_2}(\left|00\right\rangle+\left|11\right\rangle)_{D_1D_2}+\\&(\left|00\right\rangle-\left|11\right\rangle)_{AB}(\left|01\right\rangle-\left|10\right\rangle)_{C_1C_2}(\left|01\right\rangle-\left|10\right\rangle)_{D_1D_2}-\end{aligned}$$

$$(|01\rangle-|10\rangle)_{AB}(|00\rangle+|11\rangle)_{C_1C_2}(|01\rangle-|10\rangle)_{D_1D_2}+$$
$$(|01\rangle+|10\rangle)_{AB}(|01\rangle-|10\rangle)_{C_1C_2}(|00\rangle+|11\rangle)_{D_1D_2}]=$$
$$\frac{1}{4\sqrt{2}}[|\phi^+\rangle_{AB}|\phi^+\rangle_{C_1C_2}|\phi^+\rangle_{D_1D_2}+|\phi^-\rangle_{AB}|\psi^-\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}-$$
$$|\psi^-\rangle_{AB}|\phi^+\rangle_{C_1C_2}|\psi^-\rangle_{D_1D_2}+|\psi^+\rangle_{AB}|\psi^-\rangle_{C_1C_2}|\phi^+\rangle_{D_1D_2}] \quad (9)$$

并将所有粒子分成4个有序的序列，其中序列 S_A 和 S_B 分别由所有的光子 A 和 B 组成；而序列 S_C 和 S_D 分别由所有的逻辑量子比特 C 和 D 组成。Alice从集合 $\{|0\rangle_r,|1\rangle_r,|+\rangle_r,|-\rangle_r\}$ 中随机选出足够多(例如 $2m$ 个)的诱骗逻辑量子比特，并且随机地插入序列 S_C 和 S_D 得到新的序列 S'_C 和 S'_D。Alice自己保留序列 S_A 和 S_B，将序列 S'_C 和 S'_D 发送给Bob。

2) 当Bob收到序列 S'_C 和 S'_D 后，他通过经典认证信道告知Alice。Alice和Bob用与前一个协议完全类似的窃听检测方法进行安全检测。 如果错误率低于预先给定的门限值，则Alice和Bob继续此协议的下一步。否则，认为存在Eve窃听，Alice和Bob停止此协议并且重新开始。

3) 除去诱骗逻辑量子比特后，序列 S'_C 和 S'_D 又恢复为序列 S_C 和 S_D。因此，Alice和Bob已经共享了 n 个逻辑 χ 态 $|\chi_r^{00}\rangle_{ABC_1C_2D_1D_2}$。Alice对序列 S_A 和 S_B 中序号相同的两个粒子执行Bell测量。Bob对序列 S_C 中的每一个逻辑量子比特中的两个光子 C_1 和 C_2 执行Bell测量，也对序列 S_D 中的每一个逻辑量子比特中的两个光子 D_1 和 D_2 执行Bell测量。由于逻辑 χ 态 $|\chi_r^{00}\rangle_{ABC_1C_2D_1D_2}$ 的测量相关性和事先两人协商的量子态的编码，Alice和Bob能共享相同的 $2n$ 比特的经典秘密密钥，即为两人的共享密钥。

3　安全性和效率分析

一个安全的QKA协议不仅能抵抗外部攻击，而且也能抵抗参与者攻击[6-7]。由于两个QKA协议是类似的，不失一般性，本文仅以抗集体退相位噪声的QKA协议为例进行安全性分析。

3.1　参与者攻击

下面说明一个不诚实的参与者不可能独自获得这个共享密钥。不失一般性，假设Alice是一个不诚实的参与者，她想让共享密钥中的 $2l$ 比特全是0，她需要用Bell基测量序列 S_A 和 S_B 中序号相同的 l 对粒子。然而，根据量子纠缠态的特性，每一对粒子的测量结果都是随机的下面4种情况之一：$|\phi^+\rangle_{AB}$，$|\psi^-\rangle_{AB}$，$|\psi^+\rangle_{AB}$，$|\phi^-\rangle_{AB}$，即Alice以1/4的概率得到00，01，10或11。因此，$2l$ 比特中的每2位随机的是00，01，10或11，Alice无法独立决定共享密钥中任意一个比特。所以该协议能抵抗参与者攻击。

3.2　外部攻击

假设Eve是一个想窃取共享密钥的窃听者，她攻击的可能方法有：特洛伊木马攻击、测量-重发攻击、截获-重发攻击和纠缠-测量攻击。

特洛伊木马攻击：在本协议中，由于量子信道中的每个光子仅被传输一次，因此Eve无法执行不可见光子窃听(IPE)木马攻击[23]和延迟光子木马攻击[24]。因此，该协议能自动抵抗两种特洛伊木马攻击。

测量-重发攻击：Eve可以对序列 S'_C 和 S'_D 中的粒子执行测量-重发攻击。然而，Eve的测量将会影响序列 S'_C 和 S'_D 中诱骗逻辑量子比特的状态。在2.1节的协议步骤2)的窃听检测中，Alice和Bob能以 $1-(3/4)^m$ 的概率发现Eve的攻击，其中 m 表示用来检测这个攻击的诱骗逻辑量子比特的数量。

截获-重发攻击：若Eve执行截获-重发攻击，她首先截获序列 S'_C 和 S'_D，然后发送她的伪造序列给Bob。当协议结束后，她再对序列 S'_C 和 S'_D 中的粒子执行相应的测量。然而，Eve并不知道诱骗逻辑量子比特的位置和初始态，因此她伪造的序列并不能通过第2.1节的协议步骤2)的窃听监测。当 m 个诱骗逻辑量子比特被用于监测这个窃听攻击时，相应的窃听检测率[2]为 $1-(1/2)^m$。因此，Eve的截获-重发攻击也失败了。

纠缠-测量攻击：Eve也可以用自己预先准备的辅助粒子去纠缠传输序列 S'_C 和 S'_D 中的粒子，然后将传输粒子再发给Bob。当协议结束后，她通过测量自己的辅助粒子，去提取关于共享密钥的有用信息。然而，Eve在窃听检测前并不知道诱骗逻辑量子比特的位置，她的纠缠操作 U 肯定也会被执行到诱骗逻辑量子比特 $|0\rangle_{dp}$，$|1\rangle_{dp}$，$|+\rangle_{dp}$ 和 $|-\rangle_{dp}$ 上。由于与文献[19]使用了相同的诱骗逻辑量子比特，因此关于纠缠-测量攻击的分析与文献[19]的分析相同。根据文献[19]的详细分析可知，Eve的纠缠-测量攻击可能无法窃听到关于共享密钥的任何有用信息，也有可能她的攻击将干扰诱骗逻辑量子比特的初始状态。因此，Eve的攻击将被Alice和Bob发现，并且每个诱骗逻辑量子比特的窃听检测率至少为1/4[26]。

4 效率分析

一个QKA协议的Cabello量子比特效率[27]定义为 $\eta=\frac{c}{q}$，其中 c 表示协商的经典比特的数量，q 表示协议中用到的量子比特的数量。通过分析发现，本文给出的抗集体退相位噪声的QKA协议与抗集体旋转噪声的QKA协议有相同的量子比特效率。并且，这两个QKA协议的量子比特效率均为 $\eta=\frac{2n}{6n+4m}$，其中 n 表示协议中使用的逻辑 χ 态的数量，m 表示一个传输序列中诱骗逻辑量子比特的数量。令 $m=n$，有 $\eta=1/5=20\%$。目前，已有的基于无消相干态的鲁棒QKA协议的量子比特效率分别为10%[22]和16.67%[21]。因此，这两个鲁棒QKA协议有更高的量子比特效率。QKA协议的信息论效率[20]为 $\eta=\frac{b_s}{q_t+b_t}$，其中 b_s、q_t 和 b_t 分别是期望收到的秘密比特数、所使用的量子比特数以及双方交换的经典比特数。易计算两个QKA协议的信息论效率均为 $\eta=33.3\%$。另外，在两个鲁棒QKA协议中仅用到单粒子测量和Bell测量，也相对比较容易实现。

5 结 束 语

本文基于四粒子 χ 态和逻辑量子比特提出了两个分别抵抗集体退相位噪声和集体旋转噪声的鲁棒QKA协议。安全性分析证明了这两个QKA协议能抵抗参与者攻击、外部攻击以及两种特洛伊木马攻击。最后通过分析它们的量子比特效率，发现这两个QKA协议有较高的效率。由于这两个鲁棒QKA协议中仅用到单粒子测量和Bell测量，因此它们也比较容易实现。

参 考 文 献

[1] BENNETT C H, BRASSARD G. Quantum cryptography: Public-key distribution and coin tossing[C]//Proceedings of IEEE International Conference on Computers, Systems and Signal Processing. Bangalore, India: IEEE, 1984: 175-179.

[2] LIN J, HWANG T. New circular quantum secret sharing for remote agents[J]. Quantum Information Processing, 2013, 12(1): 685-697.

[3] YIN X R, MA W P, LIU W Y, et al. Efficient bidirectional quantum secure communication with two-photon entanglement[J]. Quantum Information Processing, 2013, 12(9): 3903-3102.

[4] ZHOU N, ZENG G, XIONG J. Quantum key agreement protocol[J]. Electronics Letter, 2004, 40(18): 1149-1150.

[5] HSUEH, C C, CHEN C Y. Quantum key agreement protocol with maximally entangled states[C]//Proceedings of the 14th Information Security Conference (ISC 2004). Taipei, China: National Taiwan University of Science and Technology, 2004: 236-242.

[6] TSAI C W, HWANG T. On “quantum key agreement protocol”[R]. CS-I-E, NCKU. Taiwan, China: R.O.C, 2009.

[7] TSAI C W, CHONG S K, HWANG T. Comment on quantum key agreement protocol with maximally entangled states[C]//Proceedings of the 20th Cryptology and Information Security Conference (CISC 2010). Hsinchu: National Chiao Tung University, 2010: 210-213.

[8] CHONG S K, HWANG T. Quantum key agreement protocol based on BB84[J]. Optics Communications, 2010, 283(6): 1192-1195.

[9] CHONG S K, TSAI C W, HWANG T. Improvement on quantum key agreement protocol with maximally entangled states[J]. International Journal of Theoretical Physics, 2011, 50(6): 1793-1802.

[10] SHI R H, ZHONG H. Multi-party quantum key agreement with Bell states and Bell measurements[J]. Quantum Information Processing, 2013, 12(2): 921-932.

[11] YIN X R, MA W P, LIU W Y. Three-party quantum key agreement with two-photon entanglement[J]. International Journal of Theoretical Physics, 2013, 52(11): 3915-3921.

[12] XU G B, WEN Q Y, GAO F, et al. Novel multiparty quantum key agreement protocol with GHZ states[J]. Quantum Information Processing, 2014, 13(12): 2587-2594.

[13] SHEN D S, MA W P, WANG L L. Two-party quantum key agreement with four-qubit cluster states[J]. Quantum Information Processing, 2014, 13(10): 2313-2324.

[14] LI X H, DENG F G, ZHOU H Y. Efficient quantum key distribution over a collective noise channel[J]. Physical Review A, 2008, 78(2): 022321.

[15] LI X H, ZHAO B K, SHENG Y B, et al. Fault tolerant quantum key distribution based on quantum dense coding with collective noise[J]. International Journal of Quantum Information, 2009, 7(8): 1479-1489.

[16] WALTON Z D, ABOURADDY A F, SERGIENKO A V, et al. Decoherence-free subspaces in quantum key distribution[J]. Physical Review Letters, 2003, 91(8): 087901.

[17] WANG R J, LI D F, LIU Y, et al. Two ways of robust quantum dialogue by using four-qubit cluster state[J]. International Journal of Theoretical Physics, 2015: 10.1007/s10773-015-2850-5.

[18] WANG R J, LI D F, QIN Z G. An immune quantum communication model for dephasing noise using four-qubit cluster state[J]. International Journal of Theoretical Physics, 2016, 55(1): 609-616.

[19] 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[J]. 中国科学: 物理学力学天文学, 2015, 45(4): 040301.
YE Tian-yu. Robust quantum dialogue based on a shared auxiliary logical Bell state against collective noise[J]. Sci Sin-Phys Mech Astron, 2015, 45(4): 040301.

[20] 叶天语. 基于逻辑量子比特和控制非操作的鲁棒量子对话[J]. 中国科学: 物理学力学天文学, 2015, 45(3): 030301.
YE Tian-yu. Robust quantum dialogue based on logical qubits and controlled-not operations[J]. Sci Sin-Phys Mech Astron, 2015, 45(3): 030301.
[21] HUANG W, WEN, Q Y, LIU B, et al. Quantum key agreement with EPR pairs and single-particle measurements[J]. Quantum Inf Process Quantum Information Processing, 2014, 13(3): 649-663.
[22] HUANG W, SU Q, WU X, et al. Quantum key agreement against collective decoherence[J]. International Journal of Theoretical Physics, 2014, 53(9): 2891-2901.
[23] CAI Q Y. Eavesdropping on the two-way quantum communication protocols with invisible photons[J]. Physics Letters A, 2006, 351(1-2): 23-25.
[24] DENG F G, LI X H, ZHOU H Y, et al. Improving the security of multiparty quantum secret sharing against Trojan horse attack[J]. Physical Review A , 2005, 72(4): 044302.
[25] YE T Y. Quantum dialogue without information leakage using a single quantum entangled state[J]. International Journal of Theoretical Physics, 2014, 53(11), 3719-3727.
[26] HE Y F, MA W P. Quantum key agreement protocols with four-qubit cluster states[J]. Quantum Information Processing, 2015, 14(9): 3483-3498.
[27] CABELLO A. Quantum key distribution in the Holevo limit[J]. Physical Review Letters, 2000, 85(26): 5635-5638.

编 辑 叶 芳