基于相干态光场的连续变量测量设备无关Cluster态量子通信

王 宇* 苏 琦
(密码科学技术国家重点实验室 北京 100878)

摘 要：由于量子通信协议理论上可以发现任何窃听者的攻击行为，因此其天然具有抗量子计算机攻击的能力。高斯相干态光场相较于纠缠态光场更容易制备和实现，利用其实现量子通信网络更具经济价值和实用价值。该文提出一种利用连续变量(CV)相干态光场就可以实现的测量设备无关(MDI)Cluster态量子通信网络协议。在此网络上可以方便地执行量子秘密共享(QSS)协议和量子会议(QC)协议。该文提出了线型Cluster态实现任意部分用户间QSS协议、星型Cluster态四用户QSS协议和QC协议，并利用纠缠模型分析了选用对称和非对称网络结构时，每种协议密钥率和传输距离之间的变化关系。结论为在量子网络中利用相干态实现QSS和QC协议提供了理论依据。

关键词：量子通信；相干态；连续变量；测量设备无关；Cluster态
中图分类号：TN918 **文献标识码**：A **文章编号**：1009-5896(2020)02-0307-08
DOI: 10.11999/JEIT190661

Continuous Variable Measurement-Device-Independent Cluster State Quantum Communication Based on Coherent State

WANG Yu SU Qi
(*State Key Laboratory of Cryptology*, *Beijing* 100878, *China*)

Abstract: Even attacks by quantum computer can be theoretically discovered if utilizing quantum communication protocols. Compared with entangled states, the Continuous Variable (CV) Gaussian coherent state is easier to be prepared. The schemes of quantum communication network based on coherent state will be more economical and practical. A Measurement-Device-Independent (MDI) Cluster state quantum communication network scheme by using coherent state is proposed. Quantum Secret Sharing (QSS) and Quantum Conference (QC) protocols can be implemented in this network. A linear Cluster state scheme is poposed to implement t-out-of-n QSS protocol, a star Cluster state scheme to implement four-user QSS protocol and QC protocol. The entanglement-based CV MDI scheme is used to analyze the relationship between the key rates and transmission distance for each symmetric and asymmetric protocol. The presented schemes provide a concrete reference for establishing CV MDI quantum QSS and QC protocol in quantum networks by using coherent state.

Key words: Quantum communication; Coherent state; Continuous Variable (CV); Measurement-Device-Independent(MDI); Cluster state

1 引言

理论上使用量子比特的计算机性能在多个方面都会远超普通经典计算机，因此近些年对其研究成为学术界、产业界等领域的热点，并且已经有许多重要的进展。虽然真正实现量子计算机面临重重困难，但它拥有光明的前景已经是学术界的共识。一旦量子计算机研制成功，将会对现有密码体制，特别是公钥密码体制形成巨大的冲击。世界各国都争相研究抗量子密码算法和抗量子技术，以应对量子计算机所带来的日益增长的量子威胁。量子通信技术的安全性机理是建立在量子力学的基本原理上的，因此其天然具备抵抗量子计算攻击的属性，是一种有效应对量子计算机威胁的技术手段。

量子密钥分发(Quantum Key Distribution, QKD)技术是最先实用化的量子信息技术，是量子通信的重要方向。光场的传播速度快且不易受外界环境的影响，是量子信息和量子计算的理想载体。

收稿日期：2019-08-30；改回日期：2019-12-06；网络出版：2019-12-20
*通信作者： 王宇 wangy@sklc.org
基金项目：国家自然科学基金(61602045, 61602046)，国家重点研发计划(2016YFA0302600, 2018YFA0306404)
Foundation Items: The National Natural Science Foundation of China (61602045, 61602046), The National Key Research and Development Program of China (2016YFA0302600, 2018YFA0306404)

全光学方法实现量子信息的协议有很多种，根据可观测量本征值的连续性或是分离性的不同，可以将量子光学研究问题分为两大类。第1类是使用少数光子携带信息的方案，其依赖于单光子探测来提取最终的信息，被称为离散变量方案。第2类是依赖于光场的正交分量携带信息，这种方案需要零差探测提取信息，被称为连续变量(CV)方案[1]。连续变量方案拥有许多优点，如可以较好地抵抗退相干效应，拥有无限大的希尔伯特空间来隐藏信息等。然而，这些优势中最显著的是可以确定性的产生量子资源[2]，例如，目前已经可以利用时间复用产生数以百万计的Cluster纠缠模式[3]，而这种多模纠缠态是基于测量的单向量子计算模型[4,5]的基本资源。

量子信息技术能够提供更安全的通讯环境和更快速的计算能力，量子信息的网络化必然成为发展趋势。随着科学研究的深入，多体系统成为了更具实际应用价值的重要资源。近年来，随着QKD器件和技术的逐渐成熟，QKD网络也越来越受到人们的关注。随着量子通信网络用户数的不断增加，有必要研究更加简洁、高效的多用户参与的量子通信网络架构和网络通信协议。目前研究比较广泛的多用户参与的量子通信协议包含量子秘密共享(Quantum Secret Sharing, QSS)协议、量子会议协议(Quantum Conference, QC)等。在QSS协议[6]中，信息发送者可以在n个参与者之间任意分发密钥，只有合法的参与者子集内部才能重建密钥。为了实现QC协议[7]，所有合法的参与者都需要共享一组相同的密钥，用于实现合法参与成员之间的加密通信。

测量设备无关(MDI)协议可以抵御敌手针对探测器的所有侧信道攻击，有效弥补了系统实际安全漏洞，同时它也是设备无关类协议中最易于实验实现的一种，已成为量子通信协议的研究热点之一。目前已有多个课题组实验实现了测量设备无关类协议[8–10]。连续变量测量设备无关量子网络通信协议首先在2016年被提出，他们利用3组份GHZ态设计了连续变量测量设备无关QC和QSS协议[11]。2018年，英国学者[12]提出了一种利用GHZ态实现通用测量设备无关星型网络协议。2019年，一种利用连续变量纠缠态和纠缠交换技术，实现类Cluster态测量设备无关网络协议被提出[13]。相比于GHZ态，利用Cluster态可以设计更灵活的组网结构，更适用于复杂的网络架构中。选择合适的Cluster纠缠态后，在任意子用户之间都可以实现QSS协议，这是GHZ态不具备的优势。文献[13]中使用的量子资源是连续变量压缩态或纠缠态。由于压缩态或纠缠态制备比较困难，因此极大地限制了其使用场景的应用范围。本文在之前工作的基础上，提出只要利用连续变量相干态就可以实现的测量设备无关QC和QSS协议，并结合等价纠缠模型分析了上述协议安全码率，拓展了原有协议的使用范围。由于相干态的制备和使用技术在量子通信中已经比较成熟，因此这种协议相较于压缩态具有更广泛的使用前景。

2 基于相干态的测量设备无关Cluster量子通信网络

连续变量Cluster态是一种多组份最大量子纠缠图态，它是单向量子计算模型的基本资源[2,14]。连续变量多组份纠缠态各节点之间满足关系式

$$\left(\hat{\boldsymbol{p}}_a-\sum_{b\in N_a}c_{ab}\hat{\boldsymbol{x}}_b\right)\to 0,\quad \forall a\in G \tag{1}$$

其中，$\hat{\boldsymbol{x}}_a=\left(\hat{\boldsymbol{a}}+\hat{\boldsymbol{a}}^{\dagger}\right)/2$和$\hat{\boldsymbol{p}}_a=\left(\hat{\boldsymbol{a}}-\hat{\boldsymbol{a}}^{\dagger}\right)/2i$分别代表光学模式$\hat{\boldsymbol{a}}$的正交振幅和正交位相分量。$a$表示图$G$中的一个节点，$b\in N_a$表示与$a$相关的所有节点，$c_{ab}$表示相邻节点之间的相互作用强度。实验上制备的Cluster纠缠态是确定性的，但是不完美的。根据各个节点关联方式的不同，4组份Cluster纠缠态可以分为3种：线型Cluster态、矩形Cluster态和星型Cluster态[15]。通过简单的傅里叶变换可以将线型Cluster态变换为矩形Cluster态，因此这两种态在一定程度上可以认为是等价的[15]。另外如果对星型Cluster纠缠态中间节点进行位相变换可以将其变为4组份GHZ态，因此星型Cluster态和4组份GHZ态也可以认为是等价的。

基于相干态光场的测量设备无关量子通信网络架构如图1所示。包含N个用户的网络中，每一个用户制备各自的相干态光场发给不可信中继(untrusted relay)。根据通信协议的不同，不可信中继对接收到的相干态光场进行广义的多模Bell态探测，并将结果公布。通过公布的结果，网络中的用户之间可以生成合适的Cluster态。利用不同的Cluster态，用户之间可以开展不同的量子通信协议，如QC协议和任意数量用户之间的QSS协议。

多组份Cluster态相比于GHZ态的优势之一就是其图态的组成形式多种多样。正是拥有这样灵活

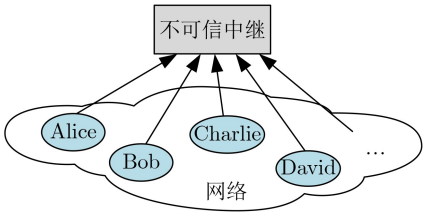


图 1 测量设备无关网络架构

多变的组成形式，使得其可以更灵活的在任意数量用户之间开展测量设备无关QSS协议。构造不同种类的Cluster态可以实现不同需求的任意数量用户之间的QSS协议。由于3组份GHZ态和Cluster态是相同的，因此本文以4组份Cluster态为例介绍其如何实现QC和QSS协议。

如果有4个合法通信用户(Alice, Bob, Charlie和David)需要开展基于相干态光场的测量设备无关量子通信QC或者QSS协议，其网络架构可以如图2搭建。网络中除了包含4个合法通信用户之外，还包含1个不可信中继，通信用户可以完全不相信这个中继，甚至其可以被窃听者Eve控制。协议执行流程如下：

步骤 1　合法通信用户分别通过各自的激光器(Laser)和光学调制器(OM)分别制备输入相干态光场$\hat{\boldsymbol{a}}_i$, $i\in\{1,2,3,4\}$，并将此光场发送给不可信中继(untrusted relay)；

步骤 2　4束光场经过由3个50%分束器(HBS)组成的网络后得到输出态光场$\hat{\boldsymbol{c}}_i$, $i\in\{1,2,3,4\}$。输出态可以表示为输入态的叠加：$\hat{\boldsymbol{c}}_1{=}1/\sqrt{2}\ (\hat{\boldsymbol{a}}_1+\hat{\boldsymbol{a}}_2)$, $\hat{\boldsymbol{c}}_2{=}1/2\ (-\hat{\boldsymbol{a}}_1+\hat{\boldsymbol{a}}_2+\hat{\boldsymbol{a}}_3+\hat{\boldsymbol{a}}_4)$ ， $\hat{\boldsymbol{c}}_3{=}1/2\ (\hat{\boldsymbol{a}}_1-\hat{\boldsymbol{a}}_2+\hat{\boldsymbol{a}}_3+\hat{\boldsymbol{a}}_4)$, $\hat{\boldsymbol{c}}_4{=}1/\sqrt{2}\ (-\hat{\boldsymbol{a}}_3+\hat{\boldsymbol{a}}_4)$ ；

步骤 3　对输出态光场进行Bell态探测得到结果($\gamma=\{x_{c_1},p_{c_2},x_{c_3},x_{c_4}\}$)，并将结果公开发布；

步骤 4　合法通信用户通过测量结果对自己的信号进行相应的修正，最终得到所需的通信密钥。

通过协议，合法通信用户之间最终得到的是类Cluster态信息，通过Cluster态之间的关联关系，合法用户之间可以进行测量设备无关QC和任意用户之间的QSS协议。

2.1　类线型Cluster态实现任意部分用户间QSS协议

秘密共享协议是当存在n个用户时，需要其中t个用户共享信息才能够恢复出发送者的信息，而小于t个用户参与的情况下是不可能恢复出发送者的信息，这种协议被称为(t, n)秘密共享协议[16]。当$t{=}n$时，为全用户参与的秘密共享协议，这种协议可以很容易的利用GHZ态实现[12]。文献[13]提出了一种利用纠缠态实现量子秘密共享的协议。在这里本文提出只需要利用相干态光场就可以实现(t,n)量子秘密共享协议，大大降低了实验的复杂度。

下面介绍利用相干态光场实现最简单的$(2,3)$测量设备无关量子秘密共享协议的实验方案。在4用户的网络中，如果任意3个用户想实现QSS协议而不被第4个用户窃听，有以下4种情况。分别是Alice, Bob和Charlie之间的QSS协议；Alice, Bob和David之间的QSS协议；Alice, Charlie和David之间的QSS协议，以及Bob, Charlie和David之间的QSS协议。通过以上4种协议就可以实现4用户网络中任意3用户之间的$(2,3)$QSS协议，任意两个用户都可以在没有第3个人帮助的情况下重构这个信息，但任何一个用户无法独自获得任何有用的信息。

如果Alice, Bob和Charlie之间想实现QSS协

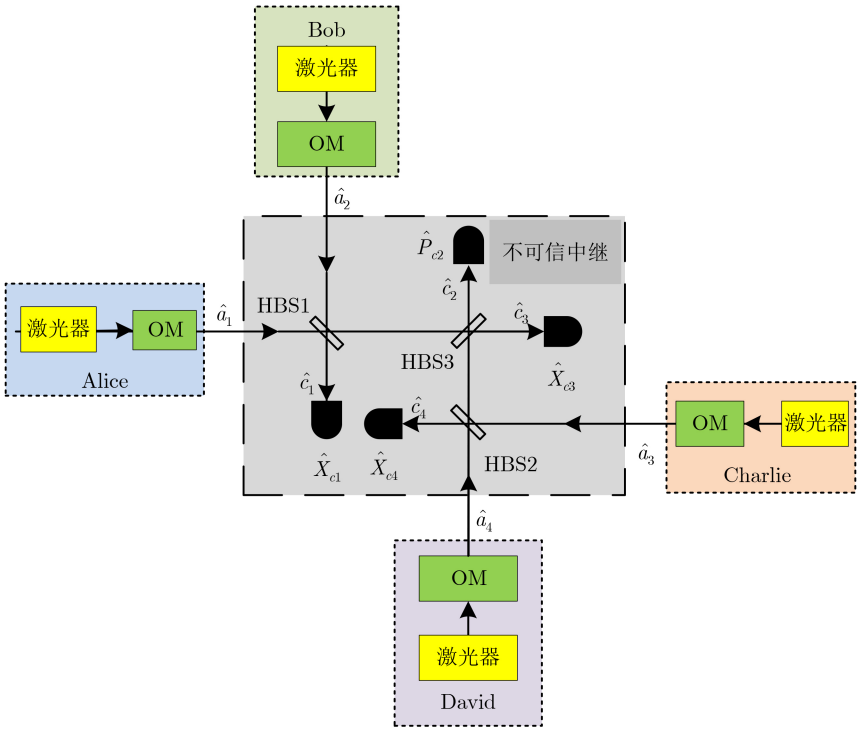


图 2 4用户相干态测量设备无关量子通信网络

议。首先Alice, Bob, Charlie和David分别制备输入相干态光场$\hat{a}_i$, $i\in\{1,2,3,4\}$，并将此光场发送给不可信中继。在得到不可信中继的测量结果γ后，Alice将其所拥有的信息变换为$x_{a_1'}=x_{a_1}-2x_{c_3}+\sqrt{2}x_{c_4}$, Bob, Charlie不做变化。此时理想情况下，Alice, Bob和Charlie满足式(2)，利用此关系式，Bob和Charlie可以重构出信息发送者Alice的信息。

$$x_{a_1'}-x_{a_2}+2x_{a_3}=0 \tag{2}$$

不仅如此，还可以通过不同的反馈方式实现其余的3方参与QSS协议。对于Alice, Bob和David参与的QSS协议，Alice将其所拥有的信息变换为$x_{a_1'}=x_{a_1}-2x_{c_3}-\sqrt{2}x_{c_4}$, Bob, David不做变化。此时理想情况下，Alice, Bob和David满足式(3)，利用此关系式，Bob和David可以重构出信息发送者Alice的信息。

$$x_{a_1'}-x_{a_2}+2x_{a_4}=0 \tag{3}$$

对于Alice, Charlie和David参与的QSS协议，Alice将其所拥有的信息变换为$x_{a_1'}=x_{a_1}-1/\sqrt{2}\,x_{c_1}-x_{c_3}$, Charlie, David不做变化。此时理想情况下，Alice, Charlie和David满足式(4)，利用此关系式，Charlie和David可以重构出信息发送者Alice的信息。

$$2x_{a_1'}+x_{a_3}+x_{a_4}=0 \tag{4}$$

不仅如此，Bob, Charlie和David参与的QSS协议同样可以实现。Charlie将其所拥有的信息变换为$x_{a_3'}=x_{a_3}+\sqrt{2}x_{c_1}-2x_{c_3}$, Bob, David不做变化。此时理想情况下，Bob, Charlie和David满足式(5)，利用此关系式，Bob和David可以重构出信息发送者Charlie的信息。

$$2x_{a_2'}+x_{a_3}+x_{a_4}=0 \tag{5}$$

以上所介绍的4种(2,3)QSS协议中，3个参与协议用户的信息与第4个用户的信息不存在关联，因此第4个用户无法获得协议参与用户之间的信息。

2.2 星型Cluster态4用户QSS协议和QC协议

所有用户都参与的QSS协议和QC协议利用GHZ态或者Cluster态都可以实现。利用Cluster态4用户QSS协议的实现如图2所示。得到不可信中继的测量结果γ后，Alice将其所拥有的信息变换为$p_{a_1'}=p_{a_1}-2p_{c_2}$, Bob, Charlie和David不做变化。此时理想情况下，Alice, Bob, Charlie和David满足式(6)，利用此关系式，Bob, Charlie和David可以重构出信息发送者Alice的信息。

$$-p_{a_1'}+p_{a_2}+p_{a_3}+p_{a_4}=0 \tag{6}$$

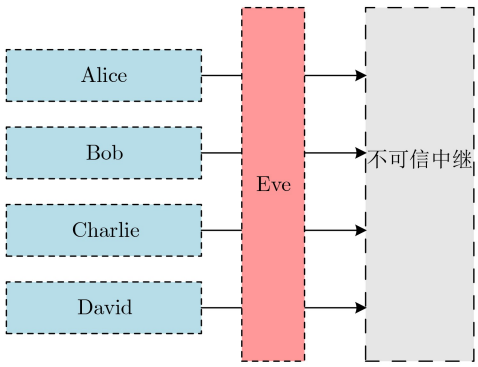
利用图2的4用户相干态测量设备无关量子通信网络还可以实现4用户QC协议。为了实现QC协议，Alice需要将其信息发送给其余3个用户。得到不可信中继的测量结果γ后，Bob对其信息进行操作得到$x_{a_2'}=x_{a_2}-\sqrt{2}x_{c_1}$, Charlie对其信息进行操作得到$x_{a_3'}=x_{a_3}-1/\sqrt{2}\,x_{c_1}-x_{c_3}+1/\sqrt{2}\,x_{c_4}$, David对其信息进行操作得到$x_{a_4'}=x_{a_4}-1/\sqrt{2}\,x_{c_1}-x_{c_3}-1/\sqrt{2}\,x_{c_4}$。此时，在理想情况下，4用户之间满足式(7), Bob, Charlie和David分别都拥有了Alice的信息，4个用户可以执行QC协议。

$$-x_{a_1}=x_{a_2'}=x_{a_3'}=x_{a_4'} \tag{7}$$

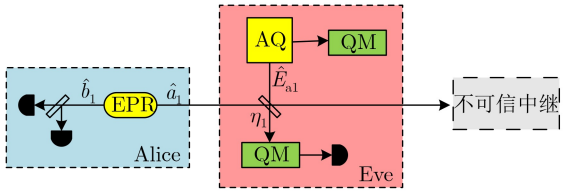
3 安全性分析

本文分析了QSS和QC协议在相干攻击下的安全性。图2表示的是制备测量模型下相干态测量设备无关量子通信网络结构，本文采用与之等价的基于纠缠的模型(如图3所示)来分析其安全性。在纠缠模型中当Alice, Bob, Charlie和David对模式$\hat{\boldsymbol{b}}_i$进行零差测量时，等效于制备测量模型中用户制备的是压缩态。与之相对应的是，当用户对模式$\hat{\boldsymbol{b}}_i$进行外差测量时，等效于制备测量模型中用户制备的是相干态。本文所提出的协议中使用的是相干态，所以对模式$\hat{\boldsymbol{b}}_i$进行外差测量。

不可信中继和4个链路中假设存在窃听者Eve，他将采用相干攻击窃听策略对线路中所有的信息进行窃取。Eve截获用户发送所有4种模式($\hat{\boldsymbol{a}}_i$, $i\in\{1,2,3,4\}$)，并将其与辅助真空模式相互耦合。Eve的输出模式一部分被发送到不可信中继继续执行协议(如图3(a)所示)，剩余的模式存储在量子存储器中。量子存储器中的各个模式会在通信者执行



(a) 相干攻击下网络架构



(b) 等价纠缠模型时攻击方案图

图 3 Eve的输出模式和攻击方案

协议后进行测量。为了发现是否存在相干攻击，用户需要通过公共通道比较一小部分已生成的数据，并判断其错误概率。图3(b)表示Eve对Alice的攻击方案，Eve对其余用户发出光场的攻击行为都类似，图中AQ和QM分别表示Eve所拥有的辅助量子态和量子存储器。

Alice, Bob, Charlie和David首先分别制备独立的EPR纠缠态，初始的协方差矩阵可以表示为

$$\left.\begin{aligned}&\boldsymbol{V}_{A,B,C,D}=\oplus_{i=1}^{4}\boldsymbol{V}_i\\&\boldsymbol{V}_{\mathrm{i}}=\begin{pmatrix}v_i\boldsymbol{I} & \sqrt{v_i^2-1}\boldsymbol{\sigma}_Z\\ \sqrt{v_i^2-1}\boldsymbol{\sigma}_Z & v_i\boldsymbol{I}\end{pmatrix}\end{aligned}\right\}\tag{8}$$

其中，$v_i=\cosh(2r)$表示EPR纠缠态的幅度，r表示压缩参数，$\boldsymbol{I}$表示单位矩阵，$\boldsymbol{\sigma}_{\mathrm{Z}}$表示Pauli Z矩阵。为了方便计算，本文选取$v_A=v_B=v_C=v_D=v$。

Eve为了将窃听到的信息最大化，采用纠缠态进行攻击，此量子态的协方差矩阵可以表示为

$$\boldsymbol{V}_{E_A,E_B,E_C,E_D}=\begin{pmatrix}v_{E_{a_1}}\boldsymbol{I} & g_1\boldsymbol{I} & g_4\boldsymbol{I} & g_6\boldsymbol{I}\\ g_1\boldsymbol{I} & v_{E_{a_2}}\boldsymbol{I} & g_2\boldsymbol{I} & g_5\boldsymbol{I}\\ g_4\boldsymbol{I} & g_2\boldsymbol{I} & v_{E_{a_3}}\boldsymbol{I} & g_3\boldsymbol{I}\\ g_6\boldsymbol{I} & g_5\boldsymbol{I} & g_3\boldsymbol{I} & v_{E_{a_4}}\boldsymbol{I}\end{pmatrix}\tag{9}$$

其中，$v_{E_{a_i}}$表示Eve发出量子态的幅度，g_1—g_6表示各个量子态之间的相互作用强度。此时可以写出包含窃听者在内的系统初始状态总的协方差矩阵

$$\boldsymbol{V}_{A,B,C,D,\mathrm{Eve}}=\boldsymbol{V}_{A,B,C,D}\oplus\boldsymbol{V}_{E_A,E_B,E_C,E_D}\tag{10}$$

Eve发出的量子态分别与4用户发出量子态经过BS耦合后发送至不可信中继。不可信中继经过3个透射率为50%的BS耦合后，得到最终的量子态$\hat{c}_i,\ i\in\{1,2,3,4\}$。最终系统的协方差矩阵可以表示为

$$\boldsymbol{V}_{\boldsymbol{b_1b_2b_3b_4c_1c_2c_3c_4\mathrm{Eve}}}=\boldsymbol{U}_{\mathrm{R}}\boldsymbol{U}_{\mathrm{Eve}}\boldsymbol{V}_{A,B,C,D,\mathrm{Eve}}\boldsymbol{U}_{\mathrm{Eve}}^{\mathrm{T}}\boldsymbol{U}_{\mathrm{R}}^{\mathrm{T}}\tag{11}$$

其中，$\boldsymbol{U}_{\mathrm{R}}$表示不可信中继中的HBS协方差矩阵，$\boldsymbol{U}_{\mathrm{Eve}}$表示Eve耦合所用到BS的协方差矩阵。透射率为$\eta_i$的BS的协方差矩阵可以表示为$\mathbf{BS}=\begin{pmatrix}\sqrt{\eta_i}\boldsymbol{I} & \sqrt{1-\eta_i}\boldsymbol{I}\\ -\sqrt{1-\eta_i}\boldsymbol{I} & \sqrt{\eta_i}\boldsymbol{I}\end{pmatrix}$。

不可信中继对量子态$\hat{c}_i$相应的正交振幅或正交位相进行零差测量之后，得到最终的协方差矩阵为

$$\mathbf{V}_{\boldsymbol{b_1b_2b_3b_4\mathrm{Eve}}|\boldsymbol{c_1c_2c_3c_4}}=\boldsymbol{V}_{\boldsymbol{b_1b_2b_3b_4\mathrm{Eve}}}-\boldsymbol{C}\boldsymbol{H}_{\mathrm{hom}}\boldsymbol{C}^{\mathbf{T}}\tag{12}$$

其中，$\boldsymbol{C}$表示矩阵的非对角元素，$\boldsymbol{H}_{\mathrm{hom}}=(\boldsymbol{W}\boldsymbol{V}_{c_1c_2c_3c_4}\boldsymbol{W})^{\mathrm{MP}}$表示量子态$\hat{c}_i$进行零差测量，MP表示矩阵的Moore Penrose转置，$\boldsymbol{W}=\boldsymbol{x}\oplus\boldsymbol{p}\oplus\boldsymbol{x}\oplus\boldsymbol{x}$，$\boldsymbol{x}=\begin{pmatrix}1&0\\0&0\end{pmatrix}$表示对正交振幅测量，$\boldsymbol{p}=\begin{pmatrix}0&0\\0&1\end{pmatrix}$表示对正交位相测量。如果对相应的模式进行外差测量，则需要用$\boldsymbol{H}_{\mathrm{het}}=(\boldsymbol{V}_{c_1c_2c_3c_4}+\boldsymbol{I})^{-1}$代替$\boldsymbol{H}_{\mathrm{hom}}$。

当协议的合法用户得到测量结果γ后，对自己拥有的模式$\hat{b}_i$外差测量得到结果β_i。此时拥有模式$\hat{b}_j$的合法用户所拥有的态也会随之塌缩到$\hat{\rho}_{b_j|b_i\gamma}$上。此时可以计算2个合法用户之间和互信息量$I(\beta_i:\beta_j)$，Eve可以获得的最大信息量用Holevo边界$H(\beta_i:\rho_{\mathrm{Eve}})$刻画。

对于4个用户参与的QSS协议，假设Alice为信息的发送者，Bob, Charlie和David可以联合恢复出Alice的信息。反向调和协议下，安全密钥率可以表示为

$$K_{ABCD}^{\mathrm{QSS_{RR}}}=\beta I(b_2,b_3,b_4:b_1)-H(b_1:\rho_{\mathrm{Eve}})\tag{13}$$

其中β为反向调和系数，受实验参数限制；$I(b_2,b_3,b_4:b_1)=\frac{1}{2}\log_2\frac{V(b_1)}{V(b_1|b_2,b_3,b_4)}$表示Alice和Bob, Charlie, David之间的互信息量，$V(b_1|b_2,b_3,b_4)$表示$\hat{b}_2,\hat{b}_3,\hat{b}_4$模式被外差探测时$\hat{b}_1$的条件方差；$H(b_1:\rho_{\mathrm{Eve}})=S(\rho_{\mathrm{Eve}})-S(\rho_{\mathrm{Eve}}|b_1)$表示$\hat{b}_1$和Eve之间的Holevo边界，由于假设整体系统是封闭的，因此$H(b_1:\rho_{\mathrm{Eve}})=S(\rho_{\mathrm{b_1b_2b_3b_4}})-S(\rho_{b_2b_3b_4}|b_1)$，其中$S(M)=\sum_i h(m_i)$表示冯诺依曼熵，$h(x):=\frac{x+1}{2}\log_2\frac{x+1}{2}-\frac{x-1}{2}\log_2\frac{x-1}{2}$，$m_i$表示协方差矩阵$\boldsymbol{M}$的辛本征值。

对于3用户参与的QSS协议，反向调和协议下，安全密钥率分别可以表示为

$$\left.\begin{aligned}K_{ABC}^{\mathrm{QSS_{RR}}}&=\beta I(b_2,b_3:b_1)-H(b_1:\rho_{\mathrm{Eve}})\\K_{ABD}^{\mathrm{QSS_{RR}}}&=\beta I(b_2,b_4:b_1)-H(b_1:\rho_{\mathrm{Eve}})\\K_{ACD}^{\mathrm{QSS_{RR}}}&=\beta I(b_3,b_4:b_1)-H(b_1:\rho_{\mathrm{Eve}})\\K_{BCD}^{\mathrm{QSS_{RR}}}&=\beta I(b_2,b_4:b_3)-H(b_3:\rho_{\mathrm{Eve}})\end{aligned}\right\}\tag{14}$$

对于QC协议，假设Alice和其余合法用户共享她的信息，反向调和协议下，安全密钥率分别可以表示为

$$\left.\begin{aligned}K_{AB}^{\mathrm{QC_{RR}}}&=\beta I(b_1:b_2)-H(b_1:\rho_{\mathrm{Eve}})\\K_{AC}^{\mathrm{QC_{RR}}}&=\beta I(b_1:b_3)-H(b_1:\rho_{\mathrm{Eve}})\\K_{AD}^{\mathrm{QC_{RR}}}&=\beta I(b_1:b_4)-H(b_1:\rho_{\mathrm{Eve}})\end{aligned}\right\}\tag{15}$$

4　计算结果

为了保证Eve的协方差矩阵有效性，需要满足$v_{E_{a_i}}>1$。Eve所使用的各个量子态之间的关联强度受到g_i影响，为使其满足纠缠态要求，此协方差矩阵$\boldsymbol{V}_{E_A,E_B,E_C,E_D}$需要满足bona fide条件$\mu^2\geq1$[17]，其中$\mu$为矩阵的最小辛本征值。在理论估算中，本文取反向调和系数$\beta=0.95$, Eve所使用纠缠态各个

模式的幅度均为$v_{E_{a_i}}=0.5$。假设协议的合法用户和不可信中继之间采用标准单模光纤(损耗$\alpha=0.2\,\mathrm{dB/km}$)，则线路中的损耗可以由传输距离表示为$\eta_i=10^{-\alpha\frac{L_i}{10}}$，其中$L_i$分别为各个通信用户与不可信中继的距离。

对于4用户参与的QSS协议，如果Eve对Bob,Charlie和David采用同等强度的攻击。为了计算Eve选用不同量子态攻击时不同的效果，本文选取3个状态分析(如图4所示)：状态1(图4中红色线)，$g_1=g_4=g_6=-0.65$, $g_2=g_3=g_5=0$；状态2(图4中蓝色线)，$g_1=g_4=g_6=0$, $g_2=g_3=g_5=0$；状态3(图4中绿色线)，$g_1=g_4=g_6=0.65$, $g_2=g_3=g_5=0$。在实际情况下，信息发送者Alice可能与其余协议用户距离均不同，此时本文也分为3种情况分析：情况1(图4中实线)，所有用户距离不可信中继距离均相等，即$L_1=L_2=L_3=L_4=L$；情况2(图4中虚线)，信息发送者Alice和不可信中继位于同一位置，其余用户距离不可信中继距离相等，即$L_1=0.01\,\mathrm{km}$且$L_2=L_3=L_4=L$；情况3(图4中点划线)，Alice和不可信中继位于相同位置，Bob和不可信中继距离确定，假设$L_1=0.01\,\mathrm{km}$, $L_2=1.00\,\mathrm{km}$且$L_3=L_4=L$。这些情况下安全密钥率和传输距离的变换关系如图4所示。图4中Eve选取的不同状态代表其使用的量子态各个子模式之间拥有不同的纠缠类型[13]。当Eve选用状态1攻击时，Eve的攻击效果最差，协议中合法用户之间的安全密钥率最高。与之相反，当Eve选用状态3的量子态攻击时，其攻击效果最好，造成用户之间的安全密钥率最少。另一方面，安全密钥率的大小与合法用户和不可信中继之间的距离紧密相关，当其中一个或几个用户与不可信中继之间的距离减少时(图4中情况3)，剩余用户与不可信中继之间的安全传输距离将大大增加。

3个用户参与的QSS协议有4种，由于情况类似，本文只选取Alice, Bob和Charlie参与的协议为例分析说明。依然选取不同的状态分析此协议的安全密钥率与传输距离的关系(如图5所示)。当Eve选取不同的量子态攻击时，不同的攻击效果分别选取3种状态分析：状态1(图5中红色线)，$g_1=g_4=-0.80$, $g_2=0$；状态2(图5中蓝色线)，$g_1=g_4=g_2=0$；状态3(图5中绿色线)，$g_1=g_4=0.80$, $g_2=0$。合法用户与不可信中继的距离也分为3种情况分析：情况1(图5中实线)，所有用户距离不可信中继距离均相等，即$L_1=L_2=L_3=L$；情况2(图5中虚线)，信息发送者Alice和不可信中继位于同一位置，其余用户距离不可信中继距离相等，即$L_1=0.01\,\mathrm{km}$且$L_2=L_3=L$；情况3(图5中点划线)，Alice和不可信中继位于相同位置，Bob和不可信中继距离确定，Charlie距离变化，假设$L_1=0.01\,\mathrm{km}$, $L_2=1.00\,\mathrm{km}$且$L_3=L$。和4用户参与的QSS协议类似，3用户参与的QSS协议密钥率(如图5所示)也与Eve所选用的量子态，用户与不可信中继之间的距离等因素有关。当Eve选取状态1窃听比选取状态3窃听的效果差，协议用户可以获得的安全密钥率较多。当Alice处于不可信中继处，若Bob和不可信中继之间的距离较短时，允许Charlie可以在更远距离生成安全密钥。

同样，对于QC协议，依然选取不同的状态分析此协议的安全密钥率K_{AC}或K_{AD}与传输距离的关系(如图6所示)。当Eve选取不同的量子态攻击时，不同的攻击效果分别选取3种状态分析：状态1(图6中红色线)，$g_1=g_4=g_6=-0.65$, $g_2=g_3=g_5=0$；

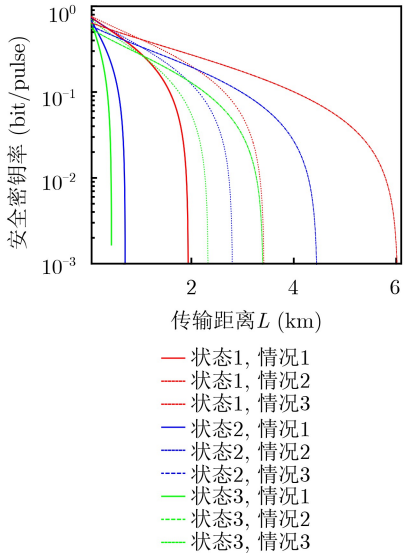


图 4 4用户参与QSS协议安全密钥率和传输距离的关系

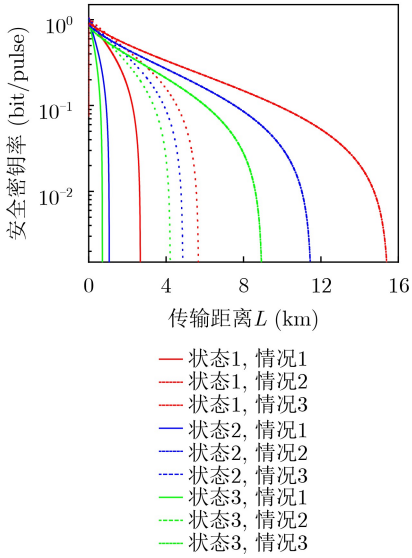


图 5 3用户参与QSS协议安全密钥率和传输距离的关系

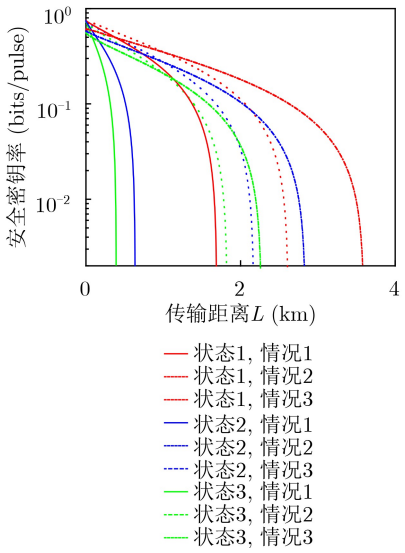


图 6 QC协议安全密钥率和传输距离的关系

状态2(图6中蓝色线)，$g_1 = g_4 = g_6 = 0$, $g_2 = g_3 = g_5 = 0$；状态3(图6中绿色线)，$g_1 = g_4 = g_6 = 0.65$, $g_2 = g_3 = g_5 = 0$。合法用户与不可信中继的距离也分为3种情况分析：情况1(图6中实线)，所有用户距离不可信中继距离均相等，即$L_1 = L_2 = L_3 = L_4 = L$；情况2(图6中虚线)，信息发送者Alice和不可信中继位于同一位置，其余用户距离不可信中继距离相等，即$L_1 = 0.01\,\text{km}$且$L_2 = L_3 = L_4 = L$；情况3(图6中点划线)，Alice和不可信中继位于相同位置，Bob和不可信中继距离确定，其余用户距离变化，假设$L_1 = 0.01\,\text{km}$, $L_2 = 1.00\,\text{km}$且$L_3 = L_4 = L$。和QSS协议类似，QC协议的安全密钥率也与Eve所选取的量子态和用户与不可信中继之间的 距离有关。当Eve选取状态3窃听比选取状态1窃听的效果更好，协议用户可以获得的安全密钥率降低。当Alice和Bob分别选取处于不可信中继较近距离处，剩余用户可以在更远的距离生成安全密钥。

以上分析可以看出，安全密钥率和Eve所选取的量子态种类、合法用户和不可信中继的距离等多个因素有关。在非对称情况下，即信息发送者Alice与不可信中继点距离接近的情况下，合法用户可以安全传输量子信息的距离更远。并且其中一个合法用户距离不可信中继点固定较近的情况，剩余两个用户的安全传输距离会大幅增加。

5　结束语

本文提出了一种利用相干态就可以实现的量子通信网络协议，网络中可以实现测量设备无关QC协议和任意用户数量的QSS协议。本文中提出了利用线型Cluster态实现任意3用户之间的QSS协议、利用星型Cluster态实现4用户之间的QSS和QC协议，并结合等价纠缠模型分析了上述协议安全码率。结果表明，选择合适的Cluster态，可以实现全体用户和任意部分用户之间的测量设备无关QC和QSS协议。首先，本量子通信网络协议的安全性原理是基于基本物理原理保障的，任何攻击行为(包括量子计算机)都可以很容易被发现，因此具有天然的抗量子计算属性；其次，本协议是一种测量设备无关量子密码通信协议，可以抵御来自测量设备端的任何攻击行为；再次，本协议仅使用相干态光场即可以实现。相较于纠缠态、压缩态等其他量子态，相干态具有制备简单、应用前景广泛等特点。本协议为在量子网络中利用相干态实现QSS和QC协议提供了理论依据，推动了量子通信协议的发展和实用化进程。

参 考 文 献

[1] BRAUNSTEIN S L and VAN LOOCK P. Quantum information with continuous variables[J]. *Reviews of Modern Physics*, 2005, 77(2): 513–577. doi: 10.1103/RevModPhys.77.513.

[2] ZHANG Jing and BRAUNSTEIN S L. Continuous-variable Gaussian analog of cluster states[J]. *Physical Review A*, 2006, 73(3): 032318. doi: 10.1103/PhysRevA.73.032318.

[3] YOKOYAMA S, UKAI R, ARMSTRONG S C, *et al*. Ultra-large-scale continuous-variable cluster states multiplexed in the time domain[J]. *Nature Photonics*, 2013, 7(12): 982–986. doi: 10.1038/nphoton.2013.287.

[4] BRIEGEL H J and RAUSSENDORF R. Persistent entanglement in arrays of interacting particles[J]. *Physical Review Letters*, 2001, 86(5): 910–913. doi: 10.1103/PhysRevLett.86.910.

[5] WANG Yu and SU Qi. Implementing classical Hadamard transform algorithm by continuous variable cluster state[J]. *Chinese Physics Letters*, 2017, 34(7): 070302. doi: 10.1088/0256-307X/34/7/070302.

[6] CLEVE R, GOTTESMAN D, and LO H K. How to share a quantum secret[J]. *Physical Review Letters*, 1999, 83(3): 648–651. doi: 10.1103/PhysRevLett.83.648.

[7] ZHAO Yi, FUNG C H F, Qi Bing, *et al*. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems[J]. *Physical Review A*, 2008, 78(4): 042333. doi: 10.1103/PhysRevA.78.042333.

[8] YIN Hualei, CHEN Tengyun, YU Zongwen, *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber[J]. *Physical Review Letters*, 2016, 117(19): 190501. doi: 10.1103/PhysRevLett.117.190501.

[9] LUCAMARINI M, YUAN Z L, DYNES J F, *et al*. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters[J]. *Nature*, 2018, 557(7705): 400–403. doi: 10.1038/s41586-018-0066-6.

[10] WANG Shuang, HE Deyong, YIN Zhenqiang, *et al*. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system[J]. *Physical Review X*, 2019, 9(2): 021046. doi: 10.1103/PhysRevX.9.021046.

[11] WU Yadong, ZHOU Jian, GONG Xinbao, *et al*. Continuous-variable measurement-device-independent multipartite quantum communication[J]. *Physical Review A*, 2016, 93(2): 022325. doi: 10.1103/PhysRevA.93.022325.

[12] OTTAVIANI C, LUPO C, LAURENZA R, *et al*. High-rate secure quantum conferencing[J]. ArXiv: 1709.06988, 2017.

[13] WANG Yu, TIAN Caixing, SU Qi, *et al*. Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state[J]. *Science China Information Sciences*, 2019, 62(7): 72501. doi: 10.1007/s11432-018-9705-x.

[14] MENICUCCI N C, VAN LOOCK P, GU M, *et al*. Universal quantum computation with continuous-variable cluster states[J]. *Physical Review Letters*, 2006, 97(11): 110501. doi: 10.1103/PhysRevLett.97.110501.

[15] YUKAWA M, UKAI R, VAN LOOCK P, *et al*. Experimental generation of four-mode continuous-variable cluster states[J]. *Physical Review A*, 2008, 78(1): 012301. doi: 10.1103/PhysRevA.78.012301.

[16] BEIMEL A. Secret-sharing schemes: A survey[C]. The 3rd International Conference on Coding and Cryptology (IWCC'11), Qingdao, China, 2011: 11–46.

[17] ADESSO G and ILLUMINATI F. Entanglement in continuous-variable systems: Recent advances and current perspectives[J]. *Journal of Physics A*: *Mathematical and Theoretical*, 2007, 40(28): 7821–7880. doi: 10.1088/1751-8113/40/28/S01.

王 宇：男，1982年生，副研究员，研究方向为量子密码和量子计算.

苏 琦：男，1985年生，助理研究员，研究方向为量子随机数和量子协议.