基于单脉冲多位编码的全光纤连续变量量子密钥分发

陈 岩 沈 咏 邹宏新

国防科学技术大学理学院物理系, 湖南 长沙 410073

摘要 实现了一种基于单脉冲多位编码的离散调制连续变量量子密钥分发方案。该方案利用时分复用和偏振复用相结合的方式进行远距离光纤传输。实验光源采用脉宽为200ns,重复频率为1 MHz的准连续光。该准连续光的每一个光脉冲在时域上被分为四等份。对每小份都编码两个正交分量,从而增大了密钥率。在25 km光纤传输时,整套系统的安全码率为32.8 kbit/s。

关键词 量子光学; 量子密钥分发; 准连续光; 离散调制; 时分复用和偏振复用

中图分类号 TN918.1 **文献标识码** A

doi: 10.3788/AOS201535.0727001

An All-Fiber Continuous Variable Quantum Key Distribution Based on Multi-bits Coding of Single Pulse

Chen Yan Shen Yong Zou Hongxin

Department of Physics, National University of Defense Technology, Changsha, Hunan 410073, *China*

Abstract An all-fiber continuous variable quantum key distribution by implementing discrete-modulated coherent state protocol based on multi-bits coding of single pulse is realized. The system employs a scheme combining polarization and frequency multiplexing. The pulse width of quasi-continuous wave is 200 ns. Each pulse is divided into four equal parts in time domain. In order to increase the secure key rate, the two quadrature components of each part are encoded with random number. At a repetition rate of 1MHz, the system achieves a final secure key rate of 32.8kb/s over a distance of 25km of optical fiber.

Key words quantum optics; quantum key distribution; quasi-continuous wave; discrete-modulated; time divison and polarization multiplexing

OCIS codes 270.5568; 270.5565; 270.5585; 060.2330

1 引 言

基于BB84协议的单光子量子保密通信是最早提出的一种量子通信方案[1],其核心是量子密钥分发(QKD)。近三十年来,单光子量子保密通信的研究取得了巨大进展。目前,已报道的最远安全通信距离可达250 km[2]。基于相干态光场的连续变量量子保密通信方案是量子保密通信的可选方案之一,并且由于其高效的探测效率和编码效率,以及在物理实现上与标准光纤通信的兼容性,吸引了广泛的研究兴趣[3-4]。连续变量量子密钥分发(CV-QKD)在过去几年中取得了非常显著的成就。早在本世纪初,国际上提出了基于高斯调制相干态结合平衡零拍探测[5]或无开关协议的量子密钥分发方案[6],并进行了实验演示[7-8]。随后,法国的Leverrier等[9]又提出了一种基于离散调制的连续变量量子密钥分发协议-四态协议,并证明了该协议是无条件安全的。但目前,无论是采取高斯调制还是离散调制,受到探测器带宽、随机相位控制速率和数据后处理速度的影响,连续变量量子密钥分发的编码效率和安全码率都比较低[10-14]。例如,加拿大的Qi等[8]在重复频率100 kHz,激光脉冲200 ns,光纤长度为5 km的情况下,得到的安全码率为30 kbit/s;法国的Xuan等[14]采用

收到修稿日期: 2015-02-03; **收到修改稿日期**: 2015-02-04

基金项目: 国家自然科学基金项目(91436103、11204374)

作者简介: 陈 岩(1989—),男,硕士研究生,主要从事量子光学和激光技术方面的研究工作。Email: chenyanxyz@gmail.com

导师简介: 邹宏新(1979—),男,博士,副教授,主要从事激光技术、量子信息方面的研究工作。

E-mail: hxzou@nudt.edu.cn(通信联系人)

连续光和偏振复用的方案，在24 km光纤传输时的安全码率为3.45 kbit/s；澳大利亚的Lance等[7]利用连续光，在信道损失90%，边带频率为17 MHz的情况下，安全码率为1 kbit/s；欧洲的Jouguet等[13]在重复频率1 MHz，激光脉宽100 ns，光纤长度为80 km情况下，得到的安全码率仅为200 bit/s。

本文提出了一种基于单脉冲多位编码的连续变量量子密钥分发方案，并在实验上搭建了全光纤的连续变量量子密钥分发系统。研制了高速的平衡零拍探测器，并利用温度控制和相位调制相结合的方法，实现了光纤中光学相位的长期锁定。在发送端，Alice把每个光脉冲在时域上分为四等份，通过对每小份的两正交分量分别进行编码，从而大幅提高了编码效率。在接收端，Bob通过随机快速选择测量基进行平衡零拍探测。在25 km标准通信光纤中传输时，实现了安全码率32.8 kbit/s的量子密钥分发。

2 四态协议

早期的文献[15]证明四态协议具有更高的数据调和效率，能够使CV-QKD适用于更远的通信距离。本文所介绍的连续变量量子密钥分发实验采用的就是四态协议。该协议中，Alice随机向Bob发送相干态 $\left|\alpha_k\right\rangle=\left|\alpha\exp\left[i(2k+1)/4\right]\right\rangle$，$k\in\{0,1,2,3\}$。其中 α 为实数，可以通过优化其数值，使得安全码率达到最大。下面在理论上来分析一下采取该四态协议的安全通信码率。为了便于分析，理论上经常采取与制备-测量等价的方案——纠缠方案来进行分析。

由于制备-测量方案中的非理想调制、外加光源噪声，Alice制备的双模纠缠态不是纯相干态，而是一个掺有噪声的混合态。考虑到对称性，假定混合态对 X 分量和 P 分量引入的噪声相同；这些噪声不会被Eve利用，而可以当作是一个中立者Fred引入的。考虑到中立者Fred的存在，那么该情形的等价纠缠方案就变为了：Alice，Bob以及Fred三个子系统构成一个纯纠缠态。

假定攻击者Eve能力足够强，她可以用一条完美的信道代替Alice与Bob之间的实际信道，并且可以纯化 ρ_{ABF}，那么总系统 $\left|\psi_{\mathrm{ABEF}}\right\rangle$ 就是一个纯态。如果Eve还可以利用Fred手里的态，则无疑可以获得更多的信息。因此可以得到安全码率的下限[15-16]

$$\tilde{K}=\beta I(\mathrm{a{:}b})-\chi(\mathrm{b{:}EF}),\tag{1}$$

式中 β 为密钥提取效率，$I(a{:}b)$ 为Alice和Bob之间的互信息。Holevo界限 $\chi(\mathrm{b{:}EF})$ 的定义为[16]

$$\chi(\mathrm{b{:}EF})=S(\rho_{\mathrm{EF}})-\int p(b)S\rho_{\mathrm{EF}}^{\mathrm{b}}\mathrm{d}b.\tag{2}$$

在Bob测量之前，由于 $\left|\psi_{\mathrm{ABEF}}\right\rangle$ 是个纯态，可得

$$S(\rho_{EF})=S(\rho_{AB}).$$

在Bob测量后，ρ_{AEF} 塌缩成 $\left|\psi_{\mathrm{AEF}}^{\mathrm{b}}\right\rangle$。又由于 $\left|\psi_{\mathrm{AEF}}^{\mathrm{b}}\right\rangle$ 也是个纯态，可得，

$$S\left(\rho_{\mathrm{EF}}^{\mathrm{b}}\right)=S\left(\rho_{\mathrm{A}}^{\mathrm{b}}\right).\tag{3}$$

另外，由于 $S\left(\rho_{\mathrm{A}}^{\mathrm{b}}\right)$ 的取值和 b 无关，可得

$$\int p(b)S\left(\rho_{\mathrm{A}}^{\mathrm{b}}\right)\mathrm{d}b=S\left(\rho_{\mathrm{A}}^{\mathrm{b}}\right).\tag{4}$$

因此，可得安全码率下限

$$\tilde{K}=\beta I(a{:}b)-S(\rho_{\mathrm{AB}})+S\left(\rho_{\mathrm{A}}^{\mathrm{b}}\right).\tag{5}$$

假定连接Alice和Bob之间的信道透过率为 T_0，额外噪声 ε_0。当Alice发送 ρ_{B0} 给Bob后，ρ_{B0} 经演化成为 ρ_{B}，此时 ρ_{AB} 的协方差矩阵 γ_{AB} 为[17]

$$\gamma_{\mathrm{AB}}=\begin{bmatrix}(V_{\mathrm{A}}+1)\boldsymbol{I} & \sqrt{T_0}Z\sigma_z\\ \sqrt{T_0}Z\sigma_z & \left[T_0(V_{\mathrm{A}}+\varepsilon_0+\delta\varepsilon)+1\right]\boldsymbol{I}\end{bmatrix},\tag{6}$$

式中 $\boldsymbol{I}$ 为单位矩阵，Z 为相关函数，$V_{\mathrm{A}}=2\alpha^2$ 为Alice的调制方差，$\sigma_z=\mathrm{diag}(1,-1)$。

根据高斯攻击的最优性[16]，当协方差矩阵相同，ρ_{AB} 为高斯态的时候，$\tilde{K}$ 会达到最小[18]。对于高斯调制协议，当信道透过率为 T，额外噪声为 ε 时，Alice和Bob的混合态协方差矩阵为[17]

$$\gamma_{AB}^{G}=\begin{bmatrix}(V_A+1)\boldsymbol{I} & \sqrt{T_0}Z_{EPR}\sigma_z\\ \sqrt{T_0}Z_{EPR}\sigma_z & \left[T_0(V_A+\varepsilon)+1\right]\boldsymbol{I}\end{bmatrix},\tag{7}$$

令 $\gamma_{AB}^{G}=\gamma_{AB}$ 可以推得：

$$T=T_0\frac{Z^2}{Z_{EPR}^2},\ \varepsilon=\frac{Z_{EPR}^2}{Z^2}(V_A+\varepsilon_0+\delta\varepsilon)-V_A.\tag{8}$$

这样，对于一个调制方差为 V_A，信源噪声为 $\delta\varepsilon$，信道透过率为 T_0，额外噪声为 ε_0 的离散调制协议，其安全码率下限可以用一个等价的高斯调制安全码率来标定。等价高斯调制方案的透过率和噪声由(8)式来决定，将其代入(1)式，就可以得到系统的安全码率。

3 实验方案

实验中采用的光源是台式大功率光纤连续激光器，经过噪声抑制和强度调制后，连续光被调制为重复频率为 1 MHz，脉冲宽度为 200 ns 的准连续光，以便于采用时分复用方案在同一根光纤中进行远距离传输。总体的实验方案如图 1 所示。

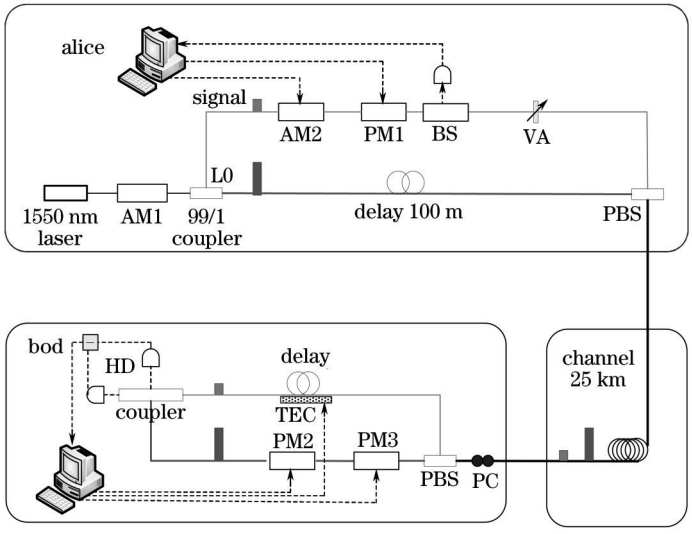

图 1 离散调制连续变量密钥分发系统方案

Fig.1 Setups of the discretely modulated continuous-variable quantum key distribution system

图 1 中 AM 表示强度调制器，PM 表示相位调制器，PC 为偏振控制器，BS 是分束器，PBS 是偏振分束器，VA 为可调衰减器，TEC 是控温元件，HD 为平衡零拍探测器。经调制后的准连续激光，先通过一个 99/1 的耦合器将脉冲光分成光强比为 1:99 的两束。其中较强的一束作为本地振荡光，较弱的一束作为信号光。Alice 端通过 AM2 和 PM1 以 20 MHz 的速率对信号光脉冲进行随机编码。也就对应着一个光脉冲的每个正交分量实现四位编码，如图 2 所示。而本地振荡光通过一段 100 m 的延时光纤，使得本地振荡光和信号光在时域上

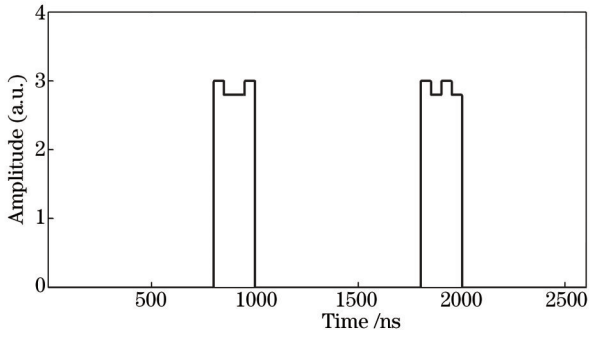

图 2 一个脉冲内实现四个编码的示意图

Fig.2 Scheme for encoding four codes in one pulse

有约300 ns的延迟间隔。另外为了降低本地振荡光对信号光的串扰,在实际通信时,采用偏振复用和时分复用相结合的方案[19]。即除了在时域上将两束光分开外,还在发送端的输出口利用PBS将两束偏振正交的光合成一路。为了保证系统的稳定性,在发送方和接收方所用的所有光纤器件都是保偏的。之后,将合束后的光通过一段25km的标准通信光纤传送给接收方。

在接收方,Bob首先利用PC对光信号进行偏振校准。对于一个实用的外场通信系统需要采用反馈电路对偏振进行自动校准。但在实验室中,光纤的偏振漂移很缓慢,因此可以暂时对偏振实行手动校准,然后通过一个偏振分束器将信道光纤中的信号光和本地振荡光分成两路,并用另一根长度同样为100 m的延时光纤将信号光延时。与Alice端不同的是,该100 m的延迟光纤放入到一个温控炉中。Bob端的延时光纤通过两个相位调制器PM2和PM3,PM2是由压电陶瓷驱动的相位调制器,用来锁定相对相位;PM3是高速的铌酸锂电光相位调制器,用来快速、随机的选择测量基。Bob通过仔细调节延时光纤的长度使得信号光和本地振荡光最终同时到达一个50:50耦合器的两个端口。发生干涉后的两路光信号用平衡零拍探测器进行探测,探测器的直流输出信号经过比例积分(PID)控制电路后分为两路,分别驱动压电陶瓷型相位控制器和温控仪。其中,温控仪通过加热或冷却延时光纤来慢速大范围地调节信号光的相位;PM2通过压电陶瓷挤压延时光纤来快速小范围的调节本地振荡光的相位。两路相结合实现了本地振荡光和信号光相对相位的稳定锁定[20]。

同样,Bob端也以20MHz的速率产生随机脉冲,并将产生的随机脉冲通过PM3加载到本征光上去,用来引入0或者是π/2相对相位差,以随机选取正弦分量X或者P进行测量。最后,平衡探测的数据通过NI公司PXIe-5122系列数据采集卡进行采集,采样频率为100 MHz。

4 实验结果及讨论

经过仔细校正后,平衡零拍探测器的探测效率η=0.8,其频谱曲线如图3。其中最下面的黑色曲线是频谱仪的电子学噪声,中间的蓝色曲线代表探测器和频谱仪总的电子学噪声,最上面红色的曲线则代表平衡零拍探测器的散离噪声。从图中可以看出,在200 MHz带宽处,平衡零拍探测信号的信噪比仍然有10 dB。

为了确定Bob端探测器的电噪声v_e以及由于调制引起的额外噪声ε_0,采集了四组数据,分别为:1) 无任何光信号时的探测器的电噪声;2) 本地光的噪声(电噪声与散粒噪声之和);3) 本地光和信号光的噪声(电噪声、散粒噪声与额外噪声之和);4) 本地光和调制后的信号光的噪声(电噪声、散粒噪声、额外噪声与调制方差之和)。经过数据处理后,以散粒噪声为单位,定义相同功率下的散粒噪声为1,可得电噪声$v_e=0.1$,额外噪声$\varepsilon_0=0.01$。通信信道为标准的通信光纤,在1550 nm波长窗口的损耗为0.02 dB/km。那么将上述参数带入到(8)式中,可得等价高斯调制的信道透过率T和额外噪声ε。另外,在信道透过率和额外噪声已知的情况下,密钥率和Alice端的调制方差一一对应(图4:其中电噪声0.1,探测效率0.8,协调效率0.8,透射率0.3),通过扫描Alice端的调制方差,可得到最优的调制方差$V_A=0.37$。

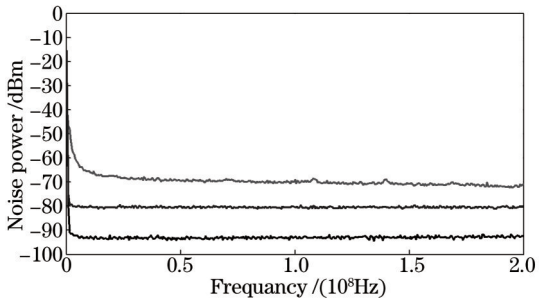

图3 平衡零拍探测器的频谱曲线

Fig.3 Frequency spectrum of the homodyne detector

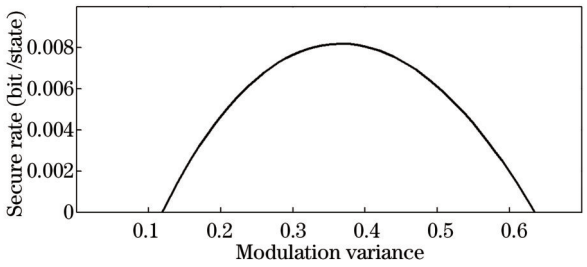

图4 调制方差-安全码率函数关系图

Fig.4 Relation between the modulation variance and the secret key rate

图5为信号光加上调制后采集到的两组数据。其中采集时间为100 μs,采样点数为10000。

Alice端实际发送的数据在相空间的分布表现为四个对称的高斯分布,四个高斯分布的中心点对应着四个理想的调制态,高斯分布的展宽则代表了额外噪声。在Bob端,由于信道衰减导致高斯分布的中心整体向

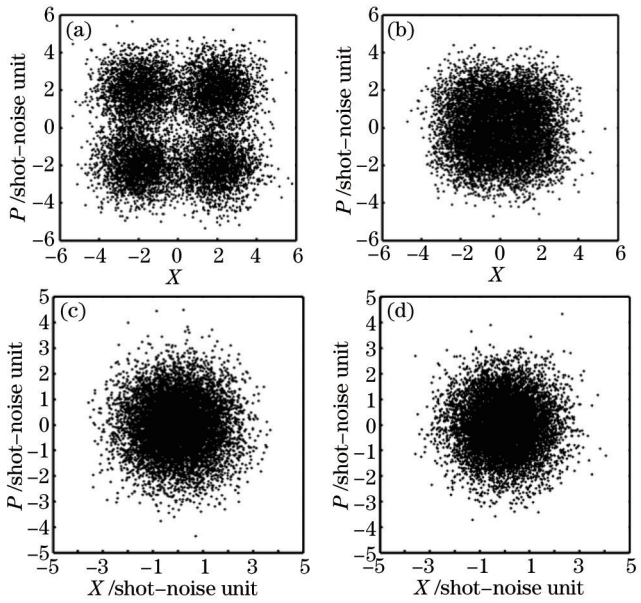

图5 (a) 调制方差为8时，Alice端发送的数据；(b) 调制方差为8时，Bob端实际采集到的数据；(c) 调制方差为最优值时；Alice端发送的数据；(d) 调制方差为最优值时，Bob实际采集到的数据

Fig.1 (a) Data Alice sends with the modulation varicance 8; (b) data Bob measures with the modulation variance 8; (c) data Alice sends with the optimal modulation variance; (d) data Bob measures with the optimal modulation variance

坐标原点靠拢，另外由于电噪声的存在，又导致了高斯分布的展开增大。图5(a) 显示当调制方差为8时，Alice端实际发送的数据，图5(b)为Bob端实际采集到的数据。可以看出，由于调制方差很大，四个高斯分布在相空间中清晰可辨；图5(c)则是调制方差为最优值0.37时，Alice端实际发送的数据，图5(d)为Bob端实际采集到的数据。此时，由于调制方差较小，无论是在发送端还是接收端，四个高斯分布都已几乎完全重合。

根据以上数据和(1)~(8)式，在25 km长的光纤传输，协调效率为80%的条件下，得到了 8.2×10^{-3} bit/pulse的安全码率。对于重复频率为1 MHz，单脉冲四位编码的情况，最终的安全码率为32.8kbit/s。为了便于比较，表1中列出了最近国内外的一些实验结果，其中文献[7]和[10]所提到的通信距离是按照标准光纤0.2dB/km的损耗换算过来的，实际中只是模拟了90%的损耗。通过比较可知，在同等的通信距离和重复率的情况下，采取的量子密钥分发方案拥有更高的安全码率。

表1 国内外量子密钥分发的部分实验结果

Table 1 Some QKD experiment result from international groups

Groups	Distance /km	Repetition rate /MHz	Secure rate /(kbit/s)
Lam Group[7]	50	17	1
Lo group[8]	5	0.1	30
Voss group[14]	24	50	3.45
Zou group[10]	50	10	46.8
Grangier group[13]	80	1	0.2
This work	25	1	32.8

5 结 论

采用准连续激光和离散调制方案，实现了全光纤的连续变量量子密钥分发。为了增大密钥产生效率，在一个脉冲内加载了四位编码。最终，在25km光纤长度，重复频率1MHz，最优调制方差 $V_A=0.37$ 的情况下，实现了32.8 kbit/s的安全码率。此时，安全码率还有进一步增大的空间，只需把重复频率增大即可。但是，重复频率上限是由脉宽和延迟光纤长度所决定的。因此，增加调制带宽和探测器带宽才是提高安全码率最有效的方法。另外，实验的安全码率是根据信道参数估计出来的值。如果要产生真正实用的安全密钥，还需要做大量的数据后处理工作，这也是目前限制连续变量量子密钥分发安全码率的核心部分。

参 考 文 献

1 C H Bennett, G Brassard. Quantum crytography: publicc key distribution and coin tossing[C]. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, 1984: 175-179.

2 D stucki, N Walenta, F Vannel, *et al*.. High rate, long distance quantum key distribution over 250km of ultra-low loss fibres[J]. New Journal of Physics, 2009,11(7): 075003.

3 T C Ralph. Continuous variable quantum cryptography[J]. Phys Rev A, 1999, 61(1): 010303.

4 F Grosshans, G V Assche, J Wenger, *et al*.. Quantum key distribution using guassian-modulated coherent states[J]. Nature, 2003, 421(6920): 238-241.

5 F Grosshans, P Grangier. Continuous variable quantum cryptography using coherent states[J]. Phys Rev Lett, 2002, 88(5): 057902.

6 C Weedbrook, A M Lance, W P Bowen, *et al*.. Quantum cryptography without swithching[J]. Phys Rev Lett, 2004,93(17):170504.

7 A M Lance, T Symul, V Sharma, *et al*.. No-switching quantum key distribution using broadband modulated coherent light[J]. Phys Rev Lett, 2005, 95(18): 180503.

8 B Qi, L L Huang, L Qian, *et al*.. Experimental study on the Gaussian modulated coherent-state quantum key distribution over standard telecommunication fibers[J]. Phys Rev A, 2007, 76(5): 052323.

9 A Leverrier, P Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation[J]. Phys Rev Lett, 2009, 102(18): 180504.

10 Y Shen, H X Zou, L A Tian, *et al*.. Experimental study on discretely modulated continuous-variable quantum key distribution[J]. Phys Rev A, 2010, 82(2): 022317.

11 J Lodewyck, M Block, R Garcia-Patron, *et al*.. Quantum key distribution over 25 km with an all-fiber continuous variable system[J]. Phys Rev A, 2007, 76(4): 042305.

12 S Fossier, E Diamanti, T Debuisschert, *et al*.. Field test of a continuous-variable quantum key distribution prototype[J]. New J Phys, 2009, 11(4): 045023.

13 P Jouguet, S Kunz-Jacques, A Leverrier, *et al*.. Experimental demonstration of long-distance continuous variable quantum key distribution[J]. Nature Photonics, 2013, 7(5): 378-381.

14 Q Xuan, Z Zhang, P L Voss. A 24-km fiber-based discretely signaled continuous variable quantum key distribution system[J]. Opt Express, 2009, 17(26): 24244-24249.

15 Y Shen, H Zou. Security bound of continuous-variable quantum key distribution with discrete modulation[J]. Acta Sin Phys, 2010, 59(3): 1473-1480.
沈 咏, 邹宏新. 离散调制连续变量量子密钥分发的安全边界[J]. 物理学报, 2010, 59(3): 1473-1480.

16 M Navascues, F Grosshans, A Acin. Optimality of Gaussian attacks in continuous-variable quantum cryptography[J]. Phys Rev Lett, 2006, 97(19): 190502.

17 F Grosshans, N J Cerf, J Wenger, *et al*.. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables[C]. Quantum Information & Computation, 2003, 3: 535-5552.

18 R García-Patrón, N J Cerf. Unconditional optimality of gaussian attacks against continuous variable quantum key distribution[J]. Phys Rev Lett, 2006, 97(19): 190503.

19 C Marand, P D Townsend, Quantum key distribution over distances as long as 30 km[J]. Opt Lett, 1995, 20(16): 1695-1697.

20 Y Shen, Y Chen, H Zou, *et al*.. A fiber-based quasi-continuous-wave quantum key distribution system[J]. Sci Rep, 2014, 4: 4563.

栏目编辑: 刘丰瑞