引用本文：钱欣，卞宇翔，刘少君，等. 基于压缩光源的无需监控信号干扰的量子密钥分发[J]. 光通信技术，2020，44(2)：59-62.

基于压缩光源的无需监控信号干扰的量子密钥分发

钱 欣[1]，卞宇翔[2,3*]，刘少君[1]，冯 宝[2,3]

（1.国网江苏省电力有限公司 南京供电分公司，南京 210024；
2.南瑞集团有限公司（国网电力科学研究院有限公司），南京 211100；3.南京南瑞国盾量子技术有限公司，南京 211100）

摘要：量子密钥分发可以为通信双方提供无条件安全的密钥。提出使用压缩光源的无需监控信号干扰的量子密钥分发协议。该协议通过在接收端对量子信号进行循环移位并测量任意 2 个量子信号的相位差来实现量子密钥分发，不仅可以产生安全密钥，而且不需要监控信号干扰，降低实现的复杂度。此外，仅使用 2 种强度的诱骗态去估计安全密钥生成率。实验结果表明：所提出的协议可以极大地提高安全密钥率，并增大传输距离。此外，仅使用 2 种强度的诱骗态也可以获得接近使用无穷个诱骗态的结果。

关键词：量子光学；量子密钥分发；压缩光源；诱骗态；安全密钥

中图分类号：O431.2　**文献标识码**：A　**文章编号**：1002-5561(2020)02-0059-04

DOI：10.13921/j.cnki.issn1002-5561.2020.02.013　**开放科学(资源服务)标识码(OSID)**：

Quantum key distribution based on squeezed source without monitoring signal disturbance

QIAN Xin[1], BIAN Yuxiang[2,3*], LIU Shaojun[1], FENG Bao[2,3]

(1. State Grid Jiangsu Power Co. Ltd., Nanjing Power Supply Branch, Nanjing 210024, China; 2. NARI Group Corporation/State Grid Electric Power Research Institute, Nanjing 211100, China; 3. NRGD Quantum Technology Co. Ltd., Nanjing 211100, China)

Abstract: Quantum key distribution protocol can provide an unconditional secure key for two communication parties. This paper proposes a quantum key distribution protocol based on squeezed source without monitoring signal disturbance. The quantum key distribution is realized by cyclic shifting the quantum signal at the receiver and measuring the phase difference of any two quantum signals. This protocol can not only generate a secure key, but also do not need to monitor the signal disturbance so as to reduce the complexity of implementation. Moreover, a two-intensity decoy states method is applied into the proposed protocol to estimate the key rate. The experiment results show that both the maximum transmission distance and the security key rate of the proposed protocol is significantly improved. Moreover, only two-intensity decoy state is necessary for approaching the asymptotic limit with infinite decoy states in the proposed protocol.

Key words: quantum optics; quantum key distribution; squeezed source; decoy states; secure key

0 引言

量子密钥分发可以为通信双方（通常称为 Alice 和 Bob）提供无条件安全的密钥[1,2]。量子密钥分发自提出以来，历经 30 余年的发展，在理论和实验上均取得了巨大的发展与进步[3-9]。最近，一种无需监控信号干扰的新型量子密钥分发被提出并受到广泛的关注[10]。因为该新型量子密钥分发的信息泄露量仅由 Alice 的量子态制备决定，与窃听者（Eve）和信道噪声导致的量子信号干扰无关，因此该新型量子密钥分发不仅可以产生安全密钥，而且还无需监控信号干扰。由于该协议在接收端需要对量子信号进行循环移位并测量任意量脉冲量子信号的相位差，因此常被称为循环差分相移量子密钥分发，受到广泛的关注[11-18]。此外，该量

收稿日期：2019-07-15。

基金项目：国网江苏省电力有限公司科技项目（J2018061）资助。

作者简介：钱欣（1989-），女，江苏南京人，硕士，工程师。主要研究方向为电力物联网建设、信息系统防护、信息安全、信息化管理体系、信息网络、信通运维管理、量子通信技术研究、信息技术和两化融合管理体系等。2017 年参与了“基于江苏省域电力量子保密通信网的省级能源互联网业务安全提升示范应用项目”，2018 年参与了“量子保密通信技术在电力系统业务中的应用研究”和“基于量子保密通信机制的终端安全防护项目”。

*** 通信作者**：卞宇翔（E-mail：nrgd_lw@163.com）。

子密钥分发协议还可以容忍很高的量子比特错误率,理论上可以达到 50%。

目前,大部分的量子密钥分发都使用弱相干(WCS)脉冲作为量子光源[11-15]。但是弱相干脉冲空脉冲的比例很高,导致密钥生成率较低并且最大传输距离更短。此外,当使用诱骗态技术到无需监控信号干扰的量子密钥分发中时,需要使用 3 个或更多个诱骗态才能很好地估计无需监控信号干扰的量子密钥分发的系统性能[17,18]。而压缩光源[19-21]服从亚泊松分布,其空脉冲的比例非常低,当量子密钥分发应用压缩光源作为光源时可以获得非常好的效果。

因此,本文提出使用压缩光源和诱骗态的无需监控信号干扰的量子密钥分发协议。

1 方案描述和理论分析

使用压缩光源和诱骗态的无需监控信号干扰的量子密钥分发的示意图如图 1 所示。方案的具体步骤如下:

① Alice 利用压缩光源产生光脉冲。首先,Alice 使用经过衰减器的激光束作为光参量振荡器的泵浦光产生压缩光场。Alice 通过调节衰减器可以产生不同强度的光参量振荡器泵浦光,由此产生压缩光源的诱骗态脉冲 μ'、μ''和压缩光源的信号态脉冲 μ ($\mu>\mu'\geqslant\mu'',\mu>\mu'+\mu''$)。

②Alice 使用一个随机数发生器去产生一串 L 比特的 0/1 随机数序列:$s_1,s_2,\cdots,s_L$。Alice 利用强度调制器将压缩光脉冲生成为 L 个脉冲组成的脉冲序列。然后 Alice 使用相位调制器去随机地将一串 L 比特的 0/1 随机数序列($s_1,s_2,\cdots,s_L$)编码到这个脉冲序列的相位上(当 s_i=0 时,相位调制器将脉冲的相位调制为 0,当 s_i=1 时相位调制器将脉冲的相位调制为 π)。Alice 通过量子信道把脉冲序列发送给 Bob。

③Bob 接收到脉冲序列后,把脉冲序列送入一个马赫-曾德尔干涉仪中。脉冲序列进入第一个分束器时分为 2 个脉冲序列,其中一个通过下臂而另一个通过上臂,上臂有一个可变延迟器。Bob 使用随机数发生器产生随机数 $r(-L+1\leqslant r\leqslant -1$ 或者 $1\leqslant r\leqslant L-1)$并使用可变延迟器对上臂的脉冲序列延迟 r 个脉冲。

④Bob 使用另一个分束器将 2 个脉冲序列进行合并,2 个脉冲序列发生干涉。使用 2 个探测器 D_0 和 D_1 去测量干涉结果,仅当 2 个探测器中有且仅有一个探测器发生响应时才是一次成功测量;而当 2 个探测器都发生响应或者都不发生响应时为一次失败测量,Bob 需要放弃这次传输。当成功测量发生时,Bob 依据探测器 D_0 产生响应生成密钥 s_B=0,依据探测器 D_1 产生响应生成密钥 s_B=1,同时 Bob 记录下发生干涉的位置信息$\{i,j\}$,其中 i 是下臂的脉冲位置,j 是上臂的脉冲位置,Bob 通过经典信道将位置信息$\{i,j\}$告诉 Alice。

⑤Alice 依据位置信息$\{i,j\}$获得密钥 $s_A=s_i\oplus s_j$。然后 Alice 和 Bob 通过重复上述步骤,并通过错误更正和秘密放大来获得最终的安全密钥。可以看出,本文设计的量子密钥分发协议无需监控信号干扰就可以进行秘密放大操作,简化了量子密钥分发实现的复杂度。

压缩光是指在相干光的某个方向上做一个压缩操作(在实验上可以通过将相干光$|\alpha\rangle$入射到光参量振荡器晶体上来实现这一操作),从而得到光量子态[19-21],其包含 n 个光子的概率为 P_n。压缩光中出现真空脉冲和多光子脉冲的概率很小,这就意味着使用压缩光来进行密钥分配将会有更高的安全密钥产生率以及更远的安全通信距离。此外,当使用无穷个诱骗态时,可以准确地估计出错误率 e_nY_n 和生成率 Y_n。

量子比特错误率 $E_{1\mu}Q_{1\mu}$ 和密钥增益 $Q_{1\mu}$ 能通过实验直接获得:$Q_{1\mu}=\sum_{n=0}^{\infty}Y_nP_n$,$E_{1\mu}Q_{1\mu}=\sum_{n=0}^{\infty}e_nY_nP_n$。由此可以获得使用压缩光脉冲和无穷个诱骗态的无需监控信号干扰的量子密钥分发中平均每脉冲的密钥生成率 R:

$$R=\frac{1}{L}Q_{1\mu}[1-fH(E_{1\mu})-H_{PA}] \tag{1}$$

其中,$H(x)$是香农熵,$H(x)=-(1-x)\log_2(1-x)-x\log_2(x)$,

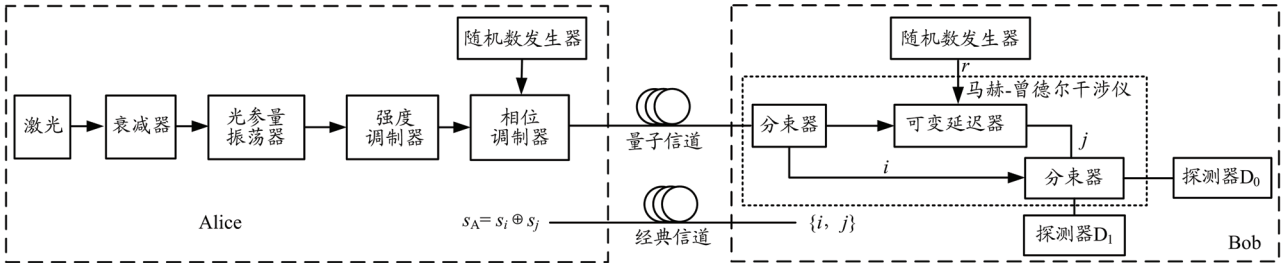

图 1 使用压缩光源和诱骗态的无需监控信号干扰的量子密钥分发示意图

f 是错误更正效率，H_{PA} 是由于秘密放大导致的密钥损耗率。秘密放大导致的总的密钥损耗为：

$$Q_{1\mu}H_{PA}=\sum_{n=0}^{n_{th}}Y_nP_nH\left(e_{ph}^{n_{th}}\right)+\sum_{n=n_{th}+1}^{\infty}Y_nP_nH\left(\frac{1}{2}\right) \quad (2)$$

其中，n_{th} 是阈值光子数（$n_{th}<\frac{L-1}{2}$），$e_{ph}^{n_{th}}$ 是包含有 n_{th} 个光子的脉冲序列的相位错误率，$e_{ph}^{n_{th}}=\frac{n_{th}}{L-1}$[10]。

由于使用压缩光脉冲和无穷个诱骗态的无需监控信号干扰的量子密钥分发中需要使用无穷个诱骗态，这在实际中是不可能实现的，因此需要考虑使用有限个诱骗态。本文通过计算可以得到使用压缩光源和 2 个诱骗态的无需监控信号干扰的量子密钥分发中平均每脉冲的密钥生成率：

$$R\geqslant\frac{1}{L}\left\{Q_1^L\left[1-H\left(e_{ph}^1\right)\right]-Q_{1\mu}fH\left(E_{1\mu}\right)\right\} \quad (3)$$

其中，$e_{ph}^1=\frac{1}{L-1}$，$Q_1^L=P_dP_0+Y_1^{L0}P_1$。Y_1^{L0} 是包含一个光子的脉冲序列的密钥生成率的下界。

2 结果分析

本文将量子密钥分发的仿真参数设置如表 1 所示，对使用 WCS 和无穷个诱骗态的无需监控信号干扰的量子密钥分发，使用压缩光脉冲和无穷个诱骗态的无需监控信号干扰的量子密钥分发，使用压缩光脉冲和 2 个诱骗态的无需监控信号干扰的量子密钥分发这 3 种量子密钥分发协议的密钥生成率进行了仿真对比，在 L=8 时，得到 3 种无需监控信号干扰的量子密钥分发协议密钥生成率的性能比较结果如图 2 所示；在 L=10 时，得到 3 种无需监控信号干扰的量子密钥分发协议密钥生成率的性能比较结果如图 3 所示。表 1 中，η_B 是 Bob 探测器的效率，e_0 是背景光导致的错误率，e_d 是不对准导致的错误率，P_d 是探测器暗计数率，f 是错误更正效率，α 是信道损耗率。

表 1 仿真参数

参数	值	参数	值
P_d	$1.7\times10^{-6}L$	η_B	4.5%
e_d	3.3%	α	0.2 dB/km
e_0	50%	f	1.15

由图 2 和图 3 可以看出，相比于基于弱相干态和诱骗态的无需监控信号干扰的量子密钥分发，基于压缩光脉冲和诱骗态的无需监控信号干扰的量子密钥分发的密钥生成率更高，安全传输距离更远。这是因为压缩光脉冲中的空脉冲比例远低于弱相干脉冲中的空脉冲比例。此外，在基于压缩光的无需监控信号干扰的量子密钥分发中，使用 2 个诱骗态的性能可以非常接近使用无穷个诱骗态的结果，2 种结果几乎重合。这表明仅使用 2 个诱骗态就足够满足性能要求，同时，使用 2 个诱骗态也可以减少因使用诱骗态导致的资源消耗。使得基于压缩光脉冲和诱骗态的无需监控信号干扰的量子密钥分发具有实用化价值。

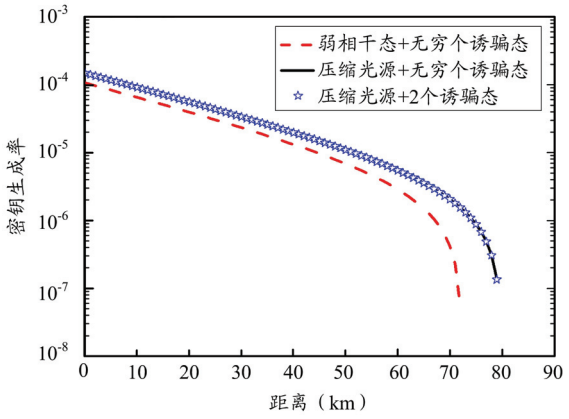

图 2 L=8 时，3 种无需监控信号干扰的量子密钥分发密钥生成率的性能比较

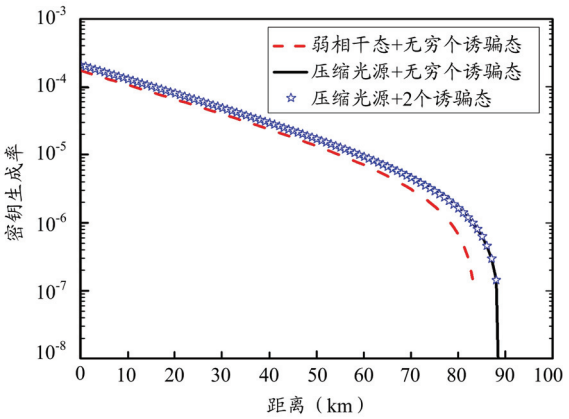

图 3 L=10 时，3 种无需监控信号干扰的量子密钥分发密钥生成率的性能比较

3 结束语

本文提出基于压缩光的无需监控信号干扰的量子密钥分发协议，同时仅需使用 2 个诱骗态即可获得和使用无穷个诱骗态一样的性能。实验结果表明：本协议的安全密钥生成率和最大安全传输距离都远优于基于弱相干态和诱骗态的无需监控信号干扰的量子密钥分发。此外，由于仅需使用 2 个诱骗态可以减少资源消耗。本协议具有实用化价值。

参考文献：

[1] WANG L, ZHAO S M, GONG L Y, et al. Free-space measurement-de-

vice-independent quantum-key-distribution protocol using decoy states with orbital angular momentum[J]. Chinese Physics B, 2015, 24(12): 120307-1–120307-8.

[2] MAO Q P, WANG L, ZHAO S M. Efficient quantum key distribution based on hybrid degrees of freedom [J]. Laser Physics, 2019, 29 (8): 085201-1–085201-7.

[3] MA X, QI B, ZHAO Y, et al. Practical decoy state for quantum key distribution[J]. Physical Review A, 2005, 72(1): 012326-1–012326-15.

[4] WANG X B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors [J]. Physical Review A, 2013, 87(1): 012320-1–012320-8.

[5] 胡康,毛钱萍,赵生妹. 基于预报单光子源和探测器诱骗态的循环差分相移量子密钥分发协议[J]. 光学学报,2017,37(5):339–345.

[6] 高中玲,赵生妹,马媛媛,等. 基于 MDI-QKD 协议的国际业务数据传输方案研究[J]. 量子电子学报,2019,36(1):34–39.

[7] 毛钱萍,赵生妹,王乐,等. 基于波分复用技术的测量设备无关量子密钥分发[J]. 量子电子学报,2017,34(1):46–53.

[8] SCHMITT-MANDERBACH T, WEIER H, FÜRST M, et al. Experimental demonstration of free-space decoy-state quantum key distribution over 144 km [J]. Physical Review Letters, 2007, 98 (1): 010504-1 – 010504-4.

[9] LIU Y, CHEN T Y, WANG L J, et al. Experimental measurement-device-independent quantum key distribution [J]. Physical Review Letters, 2013, 111(13): 130502-1–130502-5.

[10] SASAKI T, YAMAMOTO Y, KOASHI M. Practical quantum key distribution protocol without monitoring signal disturbance [J]. Nature, 2014, 509: 475–478.

[11] MAO Q P, WANG L, ZHAO S M. Plug-and-play round-robin differential phase-shift quantum key distribution [J]. Scientific Reports, 2017(7): 15435-1–15435-8.

[12] GUAN J Y, CAO Z, LIU Y et. al. Experimental Passive Round-Robin Differential Phase-Shift Quantum Key Distribution[J]. Physical Review Letters 2015, 144(18): 180502-1–180502-5.

[13] TAKESUE H, SASAKI T, TAMAKI K et. al. Experimental quantum key distribution without monitoring signal disturbance [J]. Nature Photonics, 2015(9): 827–831.

[14] WANG S, YIN Z Q, CHEN W, et. al. Experimental demonstration of a quantum key distribution without signal disturbance monitoring [J]. Nature Photonics, 2015(9): 832–836.

[15] ZHANG Z, YUAN X, CAO Z, et al. Practical round-robin differential-phase-shift quantum key distribution[J]. New Journal of Physics, 2017, 19(3): 033013-1–033013-11.

[16] YIN H L, FU Y, MAO Y, et al. Detector-decoy quantum key distribution without monitoring signal disturbance[J]. Physical Review A, 2016, 93 (2): 022330-1–022330-5.

[17] LIU L, GUO F Z, QIN S J, et al. Round-robin differential-phase-shift quantum key distribution with a passive decoy state method [J]. Scientific Reports, 2017(7): 42261-1–42261-7.

[18] WANG L, ZHAO S. Round-robin differential-phase-shift quantum key distribution with heralded pair-coherent sources [J]. Quantum Information Processing, 2017, 16(4): 100-1–100-15.

[19] LU Y J, ZHU L, OU Z Y. Security improvement by using a modified coherent state for quantum cryptography [J]. Physical Review A, 2005, 71 (3): 032315-1–032315-5.

[20] YIN Z Q, HAN Z F, SUN F W, et al. Decoy state quantum key distribution with modified coherent state [J]. Physical Review A, 2007, 76(1): 014304-1–014304-4.

[21] LI M, ZHANG C M, YIN Z Q, et al. Measurement-device-independent quantum key distribution with modified coherent state [J]. Optics Letters, 2014, 39(4): 880–883.