物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

基于散粒噪声方差实时监测的连续变量量子密钥分发系统的设计与实现

曹正文　张爽浩　冯晓毅　赵光　柴庚　李东伟

The design and realization of continuous-variable quantum key distribution system based on real-time shot noise variance monitoring

Cao Zheng-Wen　Zhang Shuang-Hao　Feng Xiao-Yi　Zhao Guang　Chai Geng　Li Dong-Wei

引用信息 Citation: Acta Physica Sinica, 66, 020301 (2017)　DOI: 10.7498/aps.66.020301
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.020301
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I2

基于散粒噪声方差实时监测的连续变量量子密钥分发系统的设计与实现*

曹正文[1)2)†] 张爽浩[1)] 冯晓毅[2)] 赵光[1)] 柴庚[1)] 李东伟[1)]

1) (西北大学信息科学与技术学院, 西安 710127)

2) (西北工业大学电子信息学院, 西安 710072)

(2016 年 8 月 15 日收到; 2016 年 11 月 2 日收到修改稿)

为了有效抵御窃听者对本振光的攻击, 提高连续变量量子密钥分发 (continuous-variable quantum key distribution, CVQKD) 系统的安全性, 提出了一种基于散粒噪声方差实时监测的 CVQKD 系统. 该系统采用散粒噪声方差标定技术, 在原有的 CVQKD 系统中加入散粒噪声方差实时监测模块, 通过本振光强和散粒噪声方差的线性关系评估出实时的散粒噪声方差, 再计算系统准确实时的密钥率来判断当前系统是否处于安全状态. 实验上也表明了该系统能够有效抵御 Eve 对本振光的攻击, 提高 CVQKD 系统的安全性.

关键词: 连续变量量子密钥分发系统, 散粒噪声方差标度技术, 本振光, 实时散粒噪声方差

PACS: 03.67.Dd, 03.67.Hk, 03.67.Mn **DOI:** 10.7498/aps.66.020301

1 引 言

连续变量量子密钥分发 (continuous-variable quantum key distribution, CVQKD) [1−6] 可以让分隔两地的通信双方 Alice 和 Bob, 通过量子信道和经过认证的经典信道获得密钥. Alice 利用高斯调制将密钥调制在光场的正则分量上, Bob 利用高效率的 Homodyne 或 Heterodyne 检测器提取密钥信息. 近几年来, CVQKD 在理论和实验方面 [7−10] 都取得了很大的进展. 2005 年, Lodewyck 等 [11] 首次使用光纤作为量子信道, 对 CVQKD 进行研究及分析了信道过噪声的主要来源. 2007 年, Lodewyck 等 [12] 设计并实现了在光纤中传输 25 km 的 CVQKD 实验系统, 并第一次使用了效率为 89% 的密钥协商算法完成最终的密钥提取. 2009 年, Fossier 等 [13] 在 Lodewyck 系统的基础上, 提出了改进的 CVQKD 的实际测试方案. 2010 年, 国防科技大学在实验室实现了自由空间中的四态调制 CVQKD 的原理验证性实验 [7]. 之后, Xu 等 [14] 在光纤中完成了 30 km 的四态调制 CVQKD 实验. 2013 年, 借助于多维协商算法 [15,16], Jouguet 等 [17] 完成了传输距离超过 80 km 的 CVQKD, 系统工作时钟频率为 1 MHz, 安全码率为 0.2 kbps. 2016 年, 上海交通大学 Huang 等 [18] 也将实验上能够实现的 CVQKD 系统传输距离记录成功推至 150 km.

然而在实际系统的安全性分析中, 一般将制备测量模型 (preparation measurement, PM) 等价为一个 entanglement-based(EB) 模型 [12] , 并根据散粒噪声标度技术 [19] 来进行安全性分析. 前者的缺陷是将散粒噪声方差当作了常数, 忽略了本振光会因窃听者 (Eve) 的攻击而改变, 进而散粒噪声方差也将发生改变. 后者的漏洞是用于计算密钥率的散粒噪声方差, 是在密钥分发前通过散粒噪声方差和本振光强的线性关系 [19] 而获得的, 并不是实时准确的散粒噪声方差. 一般在系统安全性分析中, 系统所有噪声参数都要归一化到散粒噪声方差. Eve 可以通过控制本振光的强度去将散粒噪声方差变

* 陕西省科技厅自然科学基金 (批准号: 2013JM8036) 和“十二五”“211 工程”创新人才培养项目 (批准号: YZZ15100) 资助的课题.

† 通信作者. E-mail: caozhw@nwu.edu.cn

小, 系统实际的过噪声因此将增大, 但合法通信方仍以原来较大的散粒噪声方差进行归一化, 从而导致合法通信方严重低估系统过噪声. 此时 Eve 可以通过采用截取重发等攻击获取密钥信息而不被合法通信方发现.

可见, 正确实时评估散粒噪声方差是保证系统安全性的一个重要因素. 针对上述现有技术中存在的缺陷或不足, 本文提出了基于散粒噪声方差实时监测的 CVQKD 系统. 通过采用散粒噪声方差标定技术, 在原有的 CVQKD 系统中加入散粒噪声方差实时监测模块, 进而对系统进行改进, 实现可自行通过本振光强和散粒噪声方差的线性关系评估出实时的散粒噪声方差. 同时, 系统在硬件中引入独立时钟, 软件中引入采样取峰值技术, 有效解决了以本振光为时钟源的 CVQKD 系统存在散粒噪声标度攻击的问题[19], 防止窃听者通过操作本振光的脉冲延时而改变先前标定好的线性关系. 最后, 系统可对密钥分发的安全性进行实时分析, 并显示系统的安全状态. 从实验结果也可看出, 该系统能够有效抵御 Eve 对本振光的攻击, 从而提高了 CVQKD 系统的安全性.

2 系统设计与实现

2.1 散粒噪声方差标定技术

在基于高斯调制相干态的 CVQKD 系统的基础上[12], Alice 端光路保持不变, 在 Bob 端内部光路中分别在信号光和本振光增加一个可调光衰减器 (ATT), 如图 1 所示.

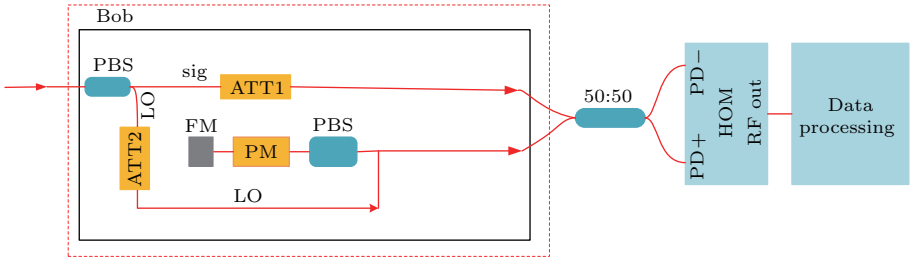

图 1 散粒噪声方差标定技术原理

Fig. 1. Principle of the shot noise variance calibration technology.

ATT1 用来调整信号光的强度, 当把 ATT1 调到最大衰减值, 即信号光强度为 0, 只让本振光通过 50 : 50 的分束器 (平衡后) 并用 Homodyne 检测器做差分放大, 测量输出电信号方差 N (单位 mV^2), 则有:

$$N = N_0 + \upsilon_{\mathrm{el}} N_0, \tag{1}$$

N_0 为散粒噪声方差, υ_{el} 为归一化到 N_0 时的检测器电噪声方差, 其可通过当 Homodyne 检测器未有光进入时采集数据获得. ATT2 用来改变本振光强的大小, 来取得不同本振光强下系统散粒噪声方差, 通过此技术采集数据, 可获得本振光强和散粒噪声方差的拟合线性关系:

$$N_0 = kP_{\mathrm{LO}} + n, \tag{2}$$

其中 k 为比例关系, P_{LO} 为本振光强度, n 为偏移量. 线性拟合关系如图 2 中的虚线所示, 其表达式为 $N_0 = 1.5P_{\mathrm{Lo}} + 16$. 所以, 可通过将实时采集到的本振光强度值 P_{Lo} 代入本振光强度与散粒噪声方差的线性拟合关系, 得到实时的散粒噪声方差.

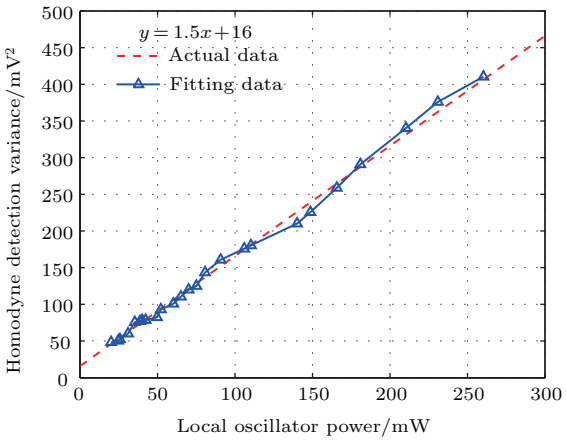

图 2 散粒噪声方差与本振光强度的线性拟合

Fig. 2. Linear fit of the shot noise variance and LO.

2.2 系统实验实现

2.2.1 传统的 CVQKD 系统

基于高斯调制相干态的 CVQKD 系统如图 3 所示, 实线为光信号传输路径, 虚线为电信

号传输路径. 激光光源产生光脉冲, 工作频率为100 kHz. 光脉冲通过1 : 99的分束器(BS1)分束为量子信号光(signal)和本振光(LO). 量子信号光经过幅度(AM)和相位(PM1)调制器完成高斯调制, 然后通过偏振分束器(PBS1)和法拉第镜(FM1), 再与本振光通过PBS2进行合束, 达到时分复用和偏振复用, 使量子信号光和本振光在同一条光纤信道中互不影响.

到达Bob端后, 首先通过动态偏振控制器(DPC)进行偏振校正, 然后通过PBS3将量子信号光和本振光分束. 其中本振光经过BS2分出10%经过光电检测(PD1)作为系统时钟信号, 剩下90%通过PBS4, PM2, FM2完成偏振态的恢复、测量基选择和时间延迟, 使本振光和量子信号光同时到达BS3并且偏振态相同. 最后进行Homodyne检测得到初始密钥.

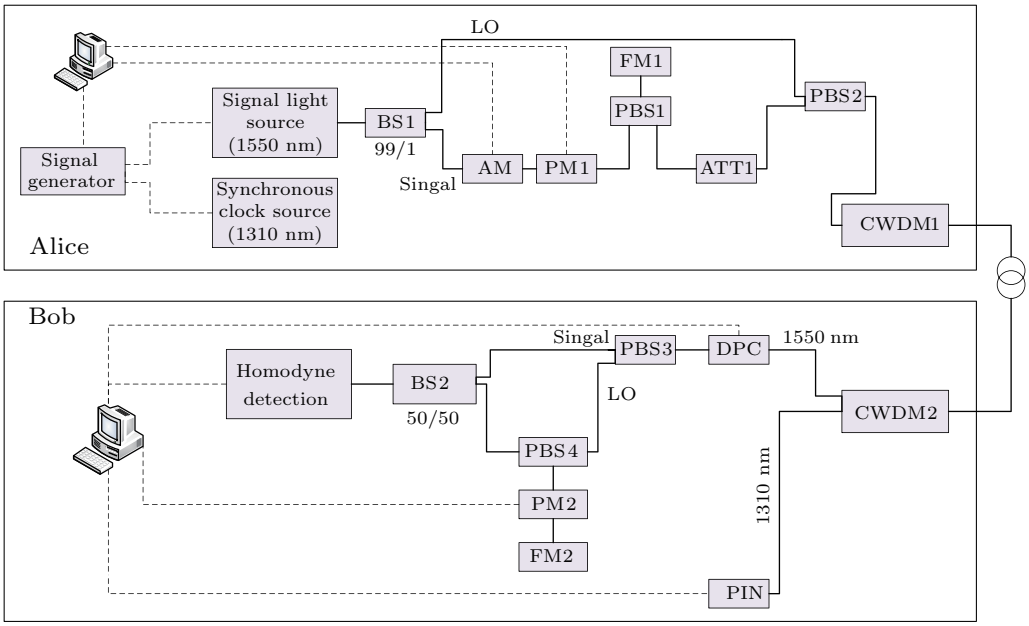

图3 基于高斯调制相干态的CVQKD系统

Fig. 3. The CVQKD system based on Gaussian-modulated coherent states.

2.2.2 基于散粒噪声方差监测的CVQKD系统

为了构建基于散粒噪声方差监测的CVQKD系统硬件平台, 我们在上述系统平台基础上加入了散粒噪声方差监测硬件模块, 并引入1310 nm光源作为系统独立时钟, 实现实时散粒噪声方差监测, 并且能够抵御散粒噪声方差标度攻击.

如图4所示, 为了实时监测系统散粒噪声方差, PD1将用来实时监测本征光强, 不再用来产生时钟信号. 时钟信号通过1310 nm激光模块产生10 MHz光脉冲提供, 通过波分复用器(CWDM)与信号光同信道传输, 最后通过PD2恢复成电信号. 在Bob端本振光路增加一个可调衰减器(ATT)来模拟Eve攻击本振光改变散粒噪声方差, 以检验系统的可行性.

Bob将接收到的1 MHz时钟脉冲进行倍频, 使得采样率为10 MHz, 即采集卡最大采样速率. 密钥分发信号频率为100 kHz, 每个脉冲被采样100个数据点, 在系统中采用取峰值算法, 即可得到峰值数据. 具体的取峰值算法如下: 运用选择排序算法思想, 在100个数据中假定第1个数据N_0为最大值$V_{\max}$, 逐一将其余的99个数据$V_j = \{V_1, V_2, \cdots, V_{99}\}$进行比较, 择取较大值, 最终获得峰值$V_{\max}$.

3 基于散粒噪声方差实时监测的CVQKD系统的安全性分析流程

为了验证本系统散粒噪声方差实时监测方法的有效性, 试验选择在威胁性和危险性都高的集体攻击下的CVQKD协议基础上, 进行安全性分析得到安全密钥率K_{R}. 若$K_{\mathrm{R}} > 0$, 说明密钥分发是无条件安全的; 若$K_{\mathrm{R}} < 0$, 则说明密钥分发不安全, 存在安全隐患.

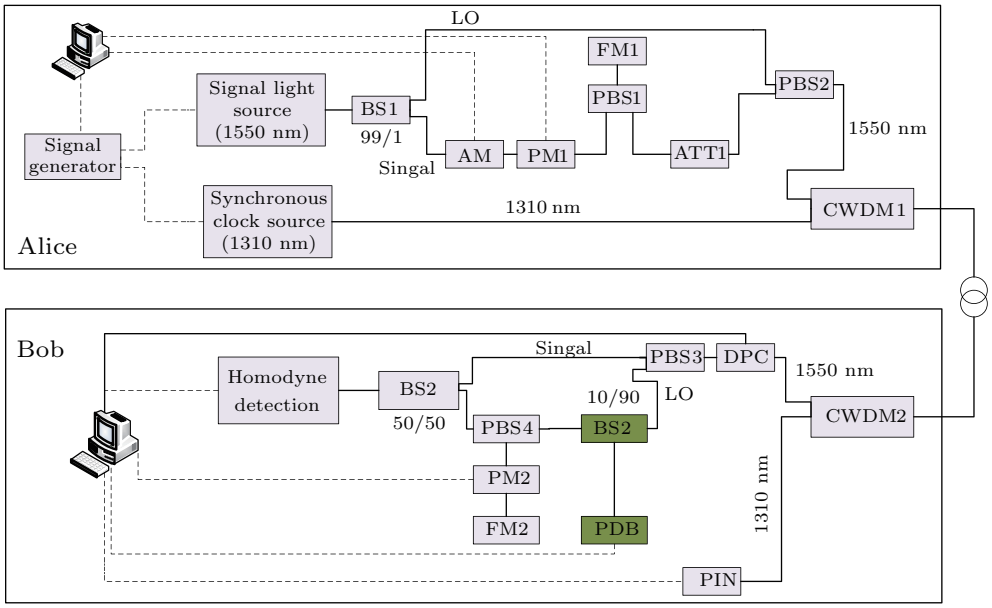

图 4 基于散粒噪声方差实时监测的 CVQKD 系统

Fig. 4. The CVQKD system based on real-time shot noise variance monitoring.

在集体攻击[12,21,22]方式下, 设通信双方为 Alice 和 Bob, 两者之间获得的安全密钥率:

$$K_{\mathrm{R}} = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{3}$$

其中, β 代表反向协商效率, 为已知量; I_{AB} 为 Alice 和 Bob 之间的互信息量; χ_{BE} 为 Eve 可以获得的最大信息量; K_{R} 为安全密钥率, K_{R} 是用来判断 CVQKD 系统密钥分发能否安全传输的条件参数.

当 Bob 采用 Homodyne 检测[3,20]时, Alice 和 Bob 的互信息量 I_{AB}[23]表示为

$$I_{\mathrm{AB}} = \frac{1}{2}\log_2\frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}} = \frac{1}{2}\log_2\frac{V+\chi_{\mathrm{tot}}}{1+\chi_{\mathrm{tot}}}, \tag{4}$$

$$V = V_{\mathrm{A}} + 1, \tag{5}$$

式中, $\chi_{\mathrm{hom}} = (1+\upsilon_{\mathrm{el}})/\eta - 1$, $\chi_{\mathrm{line}} = 1/T - 1 + \varepsilon_{\mathrm{c}}$, $\chi_{\mathrm{tot}} = \chi_{\mathrm{line}} + \chi_{\mathrm{hom}}/T$; T 为信道透过率, ε_{c} 为信道过噪声, υ_{el} 为归一化后的相对电噪声方差, η 为检测器量子效率, V_{A} 为 Alice 的调制方差, χ_{line} 为信道输入过噪声, χ_{hom} 为零差检测器的等效输入过噪声, χ_{tot} 为总过噪声.

Eve 能得到的最大信息量 χ_{BE}[12]受 Holeve 限[24]的限制, 对于高斯态, χ_{BE} 可简化[13]为

$$\chi_{\mathrm{BE}} = \sum_{i=1,2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3,4,5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{6}$$

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x, \tag{7}$$

λ_1, λ_2 和 $\lambda_{3,4,5}$ 是表征量子系统的协方差矩阵的辛本征值. 对应的辛本征值[13]为:

$$\lambda_{1,2}^2 = \frac{1}{2}\left[A \pm \sqrt{A^2 - 4B}\right], \tag{8}$$

$$A = (V_{\mathrm{A}}+1)^2(1-2T) + 2T + T^2(V+\chi_{\mathrm{line}})^2, \tag{9}$$

$$B = T^2[(V_{\mathrm{A}}+1)\chi_{\mathrm{line}} + 1]^2, \tag{10}$$

$$\lambda_{3,4}^2 = \frac{1}{2}\left[C \pm \sqrt{C^2 - 4D}\right],\ \lambda_5 = 1. \tag{11}$$

在 Homodyne 检测[12]下, 其中

$$C = \frac{A\chi_{\mathrm{hom}} + (V_{\mathrm{A}}+1)\sqrt{B} + T(V_{\mathrm{A}}+1+\chi_{\mathrm{line}})}{T(V_{\mathrm{A}}+1+\chi_{\mathrm{tot}})}, \tag{12}$$

$$D = \sqrt{B}\frac{(V_{\mathrm{A}}+1+\sqrt{B}\chi_{\mathrm{hom}})}{T(V+\chi_{\mathrm{tot}})}. \tag{13}$$

传统 CVQKD 系统稳定时, 散粒噪声方差在安全性分析的过程中始终保持不变, 因此认为其为固定值, N_0' 为原始的散粒噪声方差. 如果 Eve 通过控制本振光强度, 导致系统散粒噪声方差的改变, 此时存在实际的散粒噪声方差 N_0, 且 $N_0' \neq N_0$, 这将导致信道的过噪声评估发生偏差, 即此时实际过噪声[19]为

$$\varepsilon' = \varepsilon_{\mathrm{c}} + \frac{N_0 - N'_0}{T^2}, \tag{14}$$

ε_{c} 为原始散粒噪声方差对应的信道过噪声. 为了计算安全密钥率, 过噪声都要归一化到散粒噪声方差单位. 在安全性分析过程中, 若 Eve 进行了集体攻

击, 导致系统的散粒噪声方差改变, 则安全性分析过程中的以下五个参数在归一化后也随散粒噪声方差的改变而改变.

Alice的调制方差

$$V'_{\rm A}=\frac{V_{\rm A}\times N'_0}{N_0}, \tag{15}$$

电噪声方差

$$\nu'_{\rm el}=\frac{\nu_{\rm el}\times N'_0}{N_0}, \tag{16}$$

零差检测器的等效输入过噪声

$$\chi'_{\rm hom}=\frac{(1-\eta+\nu'_{\rm el})}{\eta}, \tag{17}$$

信道输入过噪声

$$\chi'_{\rm line}=\frac{1}{T}-1+\varepsilon', \tag{18}$$

总过噪声

$$\chi'_{\rm tot}=\chi'_{\rm line}+\chi'_{\rm hom}/T. \tag{19}$$

将方程(14)—(19)得到的Alice的调制方差、零差检测器的等效输入过噪声、信道输入过噪声和总过噪声代入方程(3)—(13), 得到密钥率, 从而可以通过安全密钥率的值来判断密钥分发是否安全.

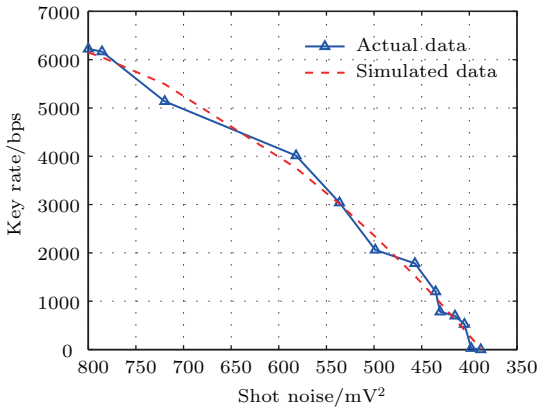

图5 不同散粒噪声方差下实际系统密钥率

Fig. 5. The actual secret key rate of system with different shot noise variance.

Alice端本振路的可调光衰减器如图2所示通过改变本振光强模拟Eve对本振光强的攻击; 利用表达式$N_0=1.5P_{\rm Lo}+16$得到实时散粒噪声方差并计算出密钥率, 从而能够评估系统的安全性. 安全性分析流程中, $V_{\rm A}=19.9$, $\varepsilon_{\rm c}=0.02$, $\eta=0.6025$, $\beta=0.89$. 每隔0.5 dB记录一次数据, 得到不同散粒噪声方差下对应的密钥率. 图5中实线和虚线分别为实际记录和仿真系统的实时散粒噪声方差及对应密钥率的关系曲线. 由数据分布可以看出, 密钥率在散粒噪声方差为388 mV^{2}时达到了零, 表明Eve能获取的信息量超出了Alice-Bob的互信息量[12], 此时不能生成密钥, 系统存在致命安全隐患. 因此Eve对本振光强的攻击会对系统带来严重的安全隐患, 这也体现了实时监测散粒噪声方差的重要性.

4 结 论

从以上实验数据可以看出, 该散粒噪声方差标定技术可通过获得散粒噪声方差和本振光强之间的线性关系计算出实时散粒噪声方差, 计算系统准确的密钥率来判断当前系统是否处于安全状态. 在基于散粒噪声方差实时监测的CVQKD系统的安全性分析流程中, 当Eve攻击本振光强时, 系统散粒噪声方差就会降低, 导致系统密钥率降低甚至小于零, 这表明Eve能完全得到密钥并且不被发现, 因此实时监测系统散粒噪声方差十分重要. 同时也表明本系统可以解决此类攻击的问题, 及时给予合法方警告. 最后, 系统可对密钥分发的安全性进行实时分析, 并显示系统的安全状态. 实验结果也可表明, 该系统能够有效抵御Eve对本振光的攻击, 从而提高了CVQKD系统的安全性.

参考文献

[1] Zeng G H 2006 *Quantum Cryptography* (Beijing: Science Press) pp128–132 (in Chinese) [曾贵华 2006 量子密码学 (北京: 科学出版社) 第128—132页]

[2] Scarani V, Bechmann P H, Cerf N J, Dusek M, Lütkenhaus N, Peev M 2009 *Rev. Mod. Phys.* **81** 1301

[3] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902

[4] Zeng G H 2010 *Quantum Private Communication* (Berlin: Springer-Verlag) pp289–297

[5] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2004 *Phys. Rev. Lett.* **93** 170504

[6] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C, Lam P K 2005 *Phys. Rev. Lett.* **95** 180503

[7] Shen Y, Zou H, Tian L, Chen P, Yuan J 2010 *Phys. Rev. A* **82** 022317

[8] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504

[9] Shen Y, Zou H X 2010 *Acta Phys. Sin.* **59** 1473 (in Chinese) [沈咏, 邹宏新 2010 物理学报 **59** 1473]

[10] Leverrier A, Grangier P 2011 *Phys. Rev. A* **83** 042312

[11] Lodewyck J, Debuisschert T, Tualle B R, Grangier P 2005 *Phys. Rev. A* **72** 050303

[12] Lodewyck J, Bloch M, García P R, Fossier S, Karpov E, Diamanti E, Grangier P 2007 *Phys. Rev. A* **76** 042305
[13] Fossier S, Diamanti E, Debuisschert T, Tualle B R, Grangier P 2009 *J. Phys. B* **42** 114014
[14] Xu Y W, Zeng L B, Shao F W, Yong M L, Kun C P 2013 *Chin. Phys. Lett.* **30** 010305
[15] Leverrier A, Alléaume R, Boutros J, Zémor G, Grangier P 2008 *Phys. Rev. A* **77** 042325
[16] Jouguet P, Kunz J S, Leverrier A 2011 *Phys. Rev. A* **84** 062317
[17] Jouguet P, Kunz J S, Leverrier A, Grangier P, Diamanti E 2013 *Nature Photon.* **7** 378
[18] Huang D, Huang P, Lin D, Zeng G 2016 *Sci. Rep.* **6** 19201
[19] Jouguet P, Kunz J S, Diamanti E 2013 *Phys. Rev. A* **87** 062313
[20] Grosshans F, van Assche G, Wenger J, Brouri R, Cerf N J, Grangier P 2003 *Nature* **421** 238
[21] Navascués M, Grosshans F, Acin A 2006 *Phys. Rev. Lett.* **97** 190502
[22] Garcia P R, Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[23] Grosshans F, Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905
[24] Holevo A S 1998 *IEEE Trans. Inf. Theory* **44** 269

The design and realization of continuous-variable quantum key distribution system based on real-time shot noise variance monitoring*

Cao Zheng-Wen[1)2)†] Zhang Shuang-Hao[1)] Feng Xiao-Yi[2)] Zhao Guang[1)]
Chai Geng[1)] Li Dong-Wei[1)]

1) (*School of Information Science and Technology, Northwest University, Xi'an 710127, China*)

2) (*School of Electronics and Information, Northwestern Polytechnical University, Xi'an 710072, China*)

(Received 15 August 2016; revised manuscript received 2 November 2016)

Abstract

In the safety assessment of the actual CVQKD (continuous-variable quantum key distribution) system, the preparation measurement model is generally equivalent to the entanglement-based model, whose major drawback is that the shot noise variance is treated as a constant. As the attacks on the LO (local oscillator) from the Eve, the shot noise variance will change with LO. And in the process of safety analysis based on the shot noise variance calibration technology, there are loopholes in which the shot noise variance for calculating secret key rate is obtained by the linear relationship between the shot noise variance and the LO before distributing the quantum key. However, the shot noise variance is not accurate nor real-time. In the security analysis of system, all the noise parameters of the system are normalized to the shot noise variance. The Eve can reduce the shot noise variance by controlling the strength of LO, thus actual excess noise of system will increase. But legal communicating parties are still normalized based on previous larger shot noise variance, so that the excess noise of system is substantially underestimated. As a consequence, the Eve can obtain secret key information without attracting the attention of legal communicating parties by adopting some attacks, such as intercept-resend attack. Thus it is an essential factor for ensuring the system security to evaluate real-time shot noise variance accurately. In order to effectively resist the above mentioned attacks on the LO from the Eve, a scheme of CVQKD system based on real-time shot noise variance monitoring is presented to improve the security of CVQKD system. The shot noise variance calibration technology is adopted in this system. By adding the real-time shot noise variance monitoring modules to the primary CVQKD system, the real-time shot noise variance is assessed by the linear relationship between the shot noise variance and the LO. In the hardware system, independent clocks are adopted. Sampling in peak algorithm is applied to software system, and this effectively solves the problem that CVQKD system with LO clock source is at risk of shot noise variance calibration attack. The scheme prevents the hazards that the Eve changes previously calibrated linear relationship by regulating the pulse delay of the LO, and thus judges whether the system is safe through calculating the accurate and real-time secret key rate. The system can analyze the real-time security of quantum key distribution and display safety status of system. The experimental results show that this system can defend effectively the LO attacks from the Eve and improve the security performance of the CVQKD system.

Keywords: continuous-variable quantum key distribution, shot noise variance calibration technology, local oscillator, real-time shot noise variance

PACS: 03.67.Dd, 03.67.Hk, 03.67.Mn **DOI:** 10.7498/aps.66.020301

* Project supported by the Natural Science Foundation of Shaanxi Province, China (Grant No. 2013JM8036) and the 211 Project of Innovative Talents Training in 12th Five-Year, China (Grant No. YZZ15100).

† Corresponding author. E-mail: caozhw@nwu.edu.cn