

基于峰值补偿的连续变量量子密钥分发方案

毛宜钰 王一军 郭迎 毛堉昊 黄文体

Continuous-variable quantum key distribution based on peak-compensation

Mao Yi-Yu Wang Yi-Jun Guo Ying Mao Yu-Hao Huang Wen-Ti

引用信息 Citation: *Acta Physica Sinica*, 70, 110302 (2021) DOI: 10.7498/aps.70.20202073

在线阅读 View online: <https://doi.org/10.7498/aps.70.20202073>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

您可能感兴趣的其他文章

Articles you may be interested in

基于量子催化的离散调制连续变量量子密钥分发

Discrete modulation continuous-variable quantum key distribution based on quantum catalysis

物理学报. 2020, 69(6): 060301 <https://doi.org/10.7498/aps.69.20191689>

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

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

物理学报. 2017, 66(2): 020301 <https://doi.org/10.7498/aps.66.020301>

微波连续变量极化纠缠

Continuous variable polarization entanglement in microwave domain

物理学报. 2019, 68(6): 064204 <https://doi.org/10.7498/aps.68.20181911>

基于混合编码的测量设备无关量子密钥分发的简单协议

A simple protocol for measuring device independent quantum key distribution based on hybrid encoding

物理学报. 2020, 69(19): 190301 <https://doi.org/10.7498/aps.69.20200162>

光纤偏振编码量子密钥分发系统荧光边信道攻击与防御

Eavesdropping and countermeasures for backflash side channel in fiber polarization-coded quantum key distribution

物理学报. 2019, 68(13): 130301 <https://doi.org/10.7498/aps.68.20190464>

参考系波动下的参考系无关测量设备无关量子密钥分发协议

Reference-frame-independent measurement-device-independent quantum key distribution under reference frame fluctuation

物理学报. 2019, 68(24): 240301 <https://doi.org/10.7498/aps.68.20191364>

基于峰值补偿的连续变量量子密钥分发方案*

毛宜钰¹⁾ 王一军¹⁾ 郭迎¹⁾ 毛堉昊²⁾³⁾ 黄文体^{4)†}

1) (中南大学自动化学院, 长沙 410083)

2) (中南大学商学院, 长沙 410083)

3) (湖南航天建筑工程有限公司, 长沙 410205)

4) (中南大学计算机学院, 长沙 410083)

(2020 年 12 月 7 日收到; 2021 年 1 月 13 日收到修改稿)

在实际的连续变量量子密钥分发系统中, 接收端模数转换器的有限采样带宽会导致脉冲峰值采样结果不准确, 从而使参数估计过程产生误差, 给窃听者留下了安全性漏洞. 针对这个问题, 本文提出一种基于峰值补偿的连续变量量子密钥分发方案, 利用高斯脉冲的基本特性来估计每个脉冲的最大采样值与脉冲峰值之间的偏差, 从而对该采样值进行峰值补偿, 使系统得到正确的采样结果. 本文详细分析了有限采样带宽对系统安全性的影响, 阐述了峰值补偿的具体步骤, 并讨论了峰值补偿前后系统估计的过噪声差别, 及其在高斯集体攻击下的安全性. 仿真实验结果表明, 该方案能准确找到每个脉冲的峰值, 纠正系统的参数估计误差. 与不采用峰值补偿的方案相比, 本方案消除了系统重复频率对密钥比特率的限制, 具有更长的安全传输距离和更高的密钥比特率.

关键词: 连续变量, 量子密钥分发, 采样带宽, 峰值补偿**PACS:** 03.67.Dd, 03.67.Hk**DOI:** 10.7498/aps.70.20202073

1 引言

量子密钥分发是量子技术的一项重要应用, 它能使远距离的通信双方在不安全的环境中建立一串无条件安全的密钥, 且这种无条件安全性是由量子力学的基本定律保证的. 近年来, 量子密钥分发技术取得了很大的进展, 主要可以分为离散变量量子密钥分发^[1-3] (discrete-variable quantum key distribution, DVQKD) 和连续变量量子密钥分发 (continuous-variable quantum key distribution, CVQKD) 两大类^[4,5]. 相比于 DVQKD, CVQKD 将密钥编码在光场的连续正则分量上, 一般以相干激光作为光源, 并采用平衡零差探测器进行探测,

具有更高的密钥率, 且能更好地与现有的光通信系统相结合^[6,7]. 利用连续变量进行密钥分发的概念在 1999 年由澳大利亚学者 Ralph^[8] 首次提出, 受到了量子保密通信研究者的广泛关注. 2002 年, Grosshans 和 Grangier^[9] 创造性地提出了一种基于弱相干态高斯调制和零差检测的 CVQKD 协议, 即著名的 GG02 协议. 该协议充分体现了 CVQKD 的优势, 具有重大的实际意义, 但它使用的正向协商方法使协议受到 3 dB 传输损耗的限制. 为了解决这个问题, Grosshans 等^[10] 在 2003 年又提出了反向协商方案, 该方案可以突破 3 dB 损耗限制, 并且具有更高的密钥率. 此后, 在 GG02 的基础上, 研究者们提出了大量改进方案, 推动了 CVQKD 的迅速发展. 例如, Weedbrook 等^[11] 在 2004 年提

* 国家自然科学基金 (批准号: 61871407, 61872390, 61801522) 资助的课题.

† 通信作者. E-mail: huangwenti@csu.edu.cn

出一种基于外差检测的 no-switching 协议, 使接收方能同时测量相干态的两个正则分量来提取密钥. 2008 年, Pirandola 等^[12]提出一种双路方案来提升协议的性能. 2009 年, Leverrier 和 Grangier^[13]提出了具有更远安全距离的离散调制方案, 并证明了其在线性量子信道条件下的安全性. 2012 年, Weedbrook 等^[14]提出以热态或加噪相干态为光源的 CVQKD 方案, 并分析了其在微波频段的可行性. 2015 年, Vladyslav 等^[15]提出了一维调制 CVQKD 方案, 通过只调制一个正则分量来简化系统的实现过程. 随着协议的不断改进和发展, 其相应的安全性证明也在持续跟进. 2004 年, Grosshans 和 Cerf^[16]证明了 CVQKD 在单体攻击下的安全性. 两年后, Navascués 等^[17]又发现了高斯攻击是针对高斯调制相干态 CVQKD 协议的最优攻击, 同年, García-Patrón 等^[18]也用另一种方法进一步证明了高斯攻击的最优性. 2009 年, Renner 等^[19]利用 de Finetti 定理证明了相干攻击和集体攻击对 DVQKD 和 CVQKD 而言都是等价的, 使得大部分 CVQKD 协议都可以基于简单的高斯集体攻击来进行安全性分析. 2010 年, Leverrier 等^[20]在 CVQKD 协议的理论安全性分析中考虑了有限长效应的影响, 并且在 2015 年完成了高斯调制相干态 CVQKD 协议的组合安全性证明^[21].

尽管高斯调制相干态 CVQKD 协议可以保证理论上的无条件安全, 但在实际实现的过程中, 器件的不完美或噪声等因素都可能会被窃听者 Eve 利用来获取信息, 使系统的无条件安全性受到影响. 目前已经提出的几种针对实际 CVQKD 系统的攻击方案有: 特洛伊木马攻击^[22]、校准攻击^[23]、本振光抖动攻击^[24]、波长攻击^[25–27]、饱和攻击^[28]、零差探测器致盲攻击^[29]、种子光注入攻击^[30]、不完美的态制备问题^[31]及有限采样带宽影响^[32]等. 其中, 有限采样带宽影响是指接收端的模数转换器 (analog-to-digital converter, ADC) 的有限采样带宽会降低密钥率的下界并限制密钥率和系统重复频率之间的关系, 从而被窃听者利用来隐藏其攻击. 为了解决有限采样带宽的影响, 研究者们也提出了相应的应对措施. 例如, Wang 等^[32]提出了一种双采样检测方案, 用两个由同一电路触发的 ADC 同时对零差探测器的输出和本振光进行采样, 来使散粒噪声方差的测量值与量子态正则分量的测量

值相对应, 从而保证接收方 Bob 能估计到正确的信道参数. 但由于光电二极管 (positive intrinsic-negative, PIN) 和其他的光电因素之间存在差异, 可能会使一个 ADC 的峰值与非峰值之比与另一个之间存在非线性, 从而对参数估计结果造成影响. Li 等^[33]利用一个动态时延调节模块和统计功率反馈控制算法来消除有限采样带宽的影响, 使 Bob 总是能采到脉冲的峰值. 但这种方法需要进行多步时延调节才能取得较好的效果, 可能会导致大量密钥的浪费, 也增加了系统运行的时间成本.

针对实际 CVQKD 系统的有限采样带宽问题, 本文提出了一种峰值补偿方案, 通过对接收端的采样结果的分析来判断采样值是否为峰值, 并在未采到峰值时对采样结果进行补偿, 使通信双方在后处理过程中能够正确估计信道参数, 消除由有限采样带宽影响导致的安全性漏洞. 这种方法可以直接在采样后的数据处理阶段完成, 不需要增加任何额外的设备, 相比之前提出的双采样方案和动态时延调节方案, 具有更高的准确性. 本文第 2 节简要介绍 ADC 的有限采样带宽对高斯调制相干态 CVQKD 系统的影响和峰值补偿的主要步骤; 第 3 节详细地讨论峰值补偿后的参数估计过程及系统在集体攻击下的安全性; 第 4 节对全文进行总结.

2 实际 CVQKD 系统的峰值补偿方案

2.1 有限采样带宽影响

在高斯调制相干态 CVQKD 协议中, 发送方 Alice 选择两组均值为 0, 方差为 $V_X = V_A N_0$ 的服从高斯分布的随机数, 用振幅调制器和相位调制器将这两组数据分别编码在信号光脉冲的正则分量 X_A 和 P_A 上, 得到相干态 $|X_A + iP_A\rangle$, 并将它们同本振光一起通过偏振复用和时分复用发送给接收方 Bob. Bob 使用的接收装置如图 1 所示, 偏振分束器将接收到的信号光和本振光分离出来, 本振光接着被一个 10:90 的分束器分离成两部分, 一部分连接光电二极管用于监测本振光强度, 另一部分与信号光干涉进行零差探测. 本振光路上的相位调制器随机将相位调整为 0 或 $\pi/2$ 来选择测量基. 最后, ADC 以频率 f_{samp} 对零差探测器的输出结果采样, 采样后的数据保存到 Bob 的电脑中进行后处理. 在这个过程中, Bob 测量到的相干态的正则分量值

由零差探测器输出电脉冲的峰值决定^[33]. 当 ADC 的采样频率无限大时, Bob 总是能准确采到脉冲的峰值得到信号光的正则分量, 从而估计到正确的信道参数. 但在实际系统中, ADC 的采样带宽是有限的, 这使得采样值可能与脉冲的峰值之间存在偏差, 如图 2 所示.

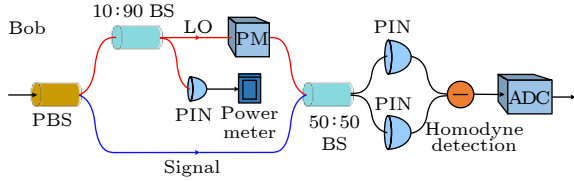


图 1 CVQKD 系统的接收端设备结构图. PBS 为偏振分束器, BS 为光分束器, PM 为相位调制器, PIN 为光电二极管, ADC 为模数转换器

Fig. 1. Structure of receiver's apparatus of a CVQKD system. PBS, polarization beam splitter; BS, beam splitter; PM, phase modulator; PIN, positive intrinsic-negative; ADC, analog-to-digital converter.

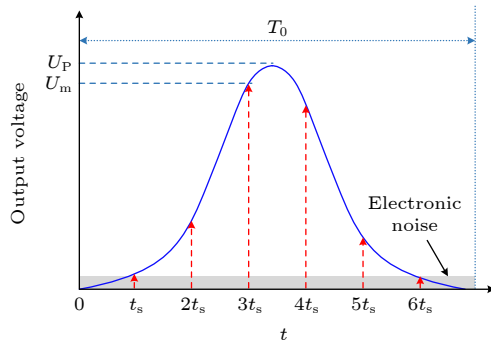


图 2 零差探测器输出脉冲的时域波形, 箭头表示采样位置. t_s 为采样间隔, U_p 为脉冲的峰值, U_m 为最大测量值, T_0 为脉冲持续时间

Fig. 2. Time-domain shape of an output pulse from the balanced homodyne detector. t_s , sampling interval; U_p , peak value of the pulse; U_m , maximal measurement value; T_0 , duration of each pulse.

通常, 对于一个高斯调制相干态 CVQKD 系统, 零差探测器的带宽远远大于系统重复频率 f_{rep} ^[34,35], 因此能保证零差探测器工作在其线性区域, 且探测器的响应相对于输入光场的正则分量是线性的. 在这种情况下, 探测前后的脉冲信号一般为高斯分布, 波形函数为^[32,33,36]

$$r(\tau) = U_p e^{-\frac{(\tau-\mu)^2}{2\sigma^2}}, \quad (1)$$

其中, U_p 为高斯脉冲的峰值, μ 和 σ^2 分别代表均值和方差. 为了简单起见, 我们选择 $\mu = T_0/2$, $\sigma^2 = T_0/8$, $T_0 = 1/f_{\text{rep}}$ 为脉冲持续时间. 如图 2 所示, 在

一个脉冲时间 T_0 内, ADC 进行了多次采样, 采样间隔为 $t_s = 1/f_{\text{samp}}$, 由于受到有限采样带宽的影响, 最大采样值 U_m 和 U_p 之间存在偏差, 定义为

$$\Delta U = U_p - U_m \leq U_p \left[1 - \exp\left(-\frac{t_s^2}{8\sigma^2}\right) \right]. \quad (2)$$

因此, 我们可以得到 U_m 和 U_p 之比为

$$\exp\left(-\frac{8f_{\text{rep}}^2}{f_{\text{samp}}^2}\right) \leq \frac{U_m}{U_p} \leq 1. \quad (3)$$

在这种情况下, Alice 和 Bob 会错误地估计信道参数 t 和 ε , 得到^[32]

$$t' = kt, \quad \varepsilon' = \varepsilon - (1 - k^2)/(k^2 t^2), \quad (4)$$

其中: $k = U_m/U_p$; $t = \eta T$, η 为零差探测器的探测效率, T 为信道透射比; ε 为系统的过噪声; t' 和 ε' 分别表示 t 和 ε 的估计值. 因此, 在没有采到脉冲的峰值时, Alice 和 Bob 会错误地估计系统的过噪声, 给窃听者留下安全漏洞.

2.2 峰值补偿

为了消除由 ADC 的有限采样带宽引入的安全性漏洞, 我们在图 1 的 ADC 后引入一个峰值补偿模块, 以实现峰值监测与补偿. 以图 2 为例, 我们的峰值补偿方案包括以下几个步骤. 1) 对于一个脉冲时间 T_0 内的所有采样值 $\{U_1, U_2, U_3, U_4, U_5, U_6\}$, 找出其最大值点 $U_m = U_3$ 以及与 U_m 相邻的两个采样值 U_2 和 U_4 . 2) 当 $U_2 = U_4$ 时, 可以判断 U_m 为峰值点; 当 $U_2 \neq U_4$ 时, 可以判断 $U_m < U_p$, 且根据高斯脉冲的性质, ΔU 可由 (5) 式得到:

$$\Delta U = U_m \left[\exp\left(-\frac{\Delta t^2 - 2t_m \Delta t + 2\Delta t t_u}{2\sigma^2}\right) - 1 \right], \quad (5)$$

其中, $t_m = 3t_s$ 为最大采样值对应的采样时间; $\Delta t = t_m - t_p$, t_p 为脉冲峰值对应的采样时间. 在已知 U_2 和 U_4 的前提下, 可得

$$\Delta t = \frac{\sigma^2}{2t_s} \ln \frac{U_2}{U_4}. \quad (6)$$

3) 用得到的 ΔU 补偿 U_m , 可得正确的脉冲峰值 U_p .

图 3(a) 是在系统重复率为 120 MHz、采样频率为 1 GHz 时一串高斯脉冲的被采样情况, 在这种情况下每个脉冲的最大采样值都不是脉冲的峰值点. 图 3(b) 是对最大采样值进行峰值补偿之后的采样情况, 我们发现补偿后的值刚好是每个脉冲的峰值点, 证明了提出的峰值补偿方案的有效性.

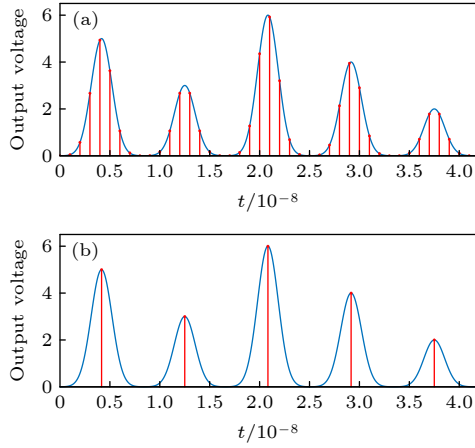


图 3 (a) 有限采样带宽影响下的高斯脉冲时域采样情况; (b) 峰值补偿后的采样值. 其中蓝色线表示脉冲时域波形, 红色圆点代表采样值

Fig. 3. (a) Sampling positions of Gaussian pulses effected by finite-sampling bandwidth; (b) sampling values after peak compensation. The blue line represents the time-domain shape of the pulses, and the red dots represent the sampled values.

3 基于峰值补偿的 CVQKD 系统的安全性分析

3.1 参数估计

2.1 节分析了在有限采样带宽影响下, Alice 和 Bob 估计的信道过噪声 ε 会小于其真实值, 从而高估系统的密钥率. 本节分析峰值补偿后系统对信道参数的估计.

在量子传输过程结束后, Alice 和 Bob 共享两个相关向量 $\mathbf{x} = (x_1, x_2, \dots, x_N)$ 和 $\mathbf{y} = (y_1, y_2, \dots, y_N)$, 其中 N 表示传输的脉冲数目. 它们之间的关系可以表示为^[37]

$$\mathbf{y} = t\mathbf{x} + \mathbf{z}, \quad (7)$$

其中, \mathbf{z} 表示系统的总噪声, 服从均值为 0, 方差为 $\sigma_n^2 = t^2\xi + N_0 + V_{el}$ 的高斯分布. N_0 表示系统的散粒噪声, $V_{el} = v_{el}N_0$ 表示零差探测器的电噪声, $\xi = \varepsilon N_0$ 表示信道过噪声, 这些参数都以它们各自的单位表示. 在不采取峰值补偿时, \mathbf{x}, \mathbf{y} 与系统参数之间的关系可以表示为

$$\begin{aligned} \langle x^2 \rangle &= V_X, \quad \langle xy \rangle = ktV_X. \\ \langle y^2 \rangle &= k^2t^2V_X + k^2t^2\xi + k^2N_0 + V_{el}. \end{aligned} \quad (8)$$

从而估计的信道参数如 (4) 式所示. 在采取峰值补偿时, 由于补偿后的 $U'_m = U_p$, 使得 $k = 1$, 因此估

计的信道参数

$$t' = t, \quad \varepsilon' = \varepsilon. \quad (9)$$

图 4 给出了在不同信道过噪声下的估计过噪声随系统重复率的变化情况. 从上到下的曲线分别代表 $\varepsilon = 0.04, \varepsilon = 0.02, \varepsilon = 0.01$ 时的结果. 显然, 在不进行峰值补偿时, 估计的过噪声会随系统重复率的增加而减小, 这意味着系统重复率越高, Eve 越容易隐藏自己; 而在进行峰值补偿后, 估计的过噪声在不同系统重复率下都保持恒定.

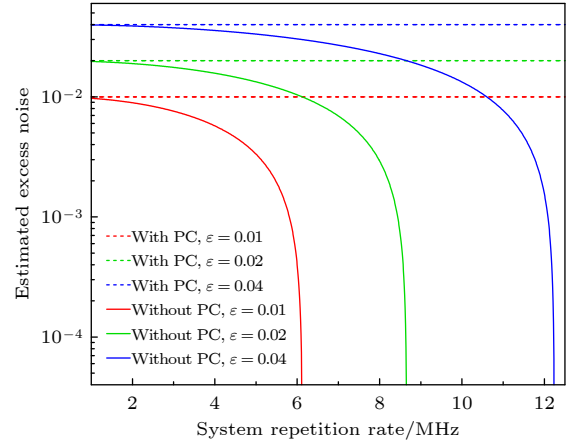


图 4 不同信道过噪声情况下的估计过噪声随系统重复率的变化. 图中 PC 表示峰值补偿 (peak-compensation, PC)
Fig. 4. The estimated excess noise as a function of the system repetition rate under different channel excess noise. PC in the figure represents peak-compensation.

3.2 集体攻击下的密钥率

对于一个 CVQKD 系统, 给定参数 $V_A, T, \varepsilon, \eta$ 和 v_{el} , Alice 和 Bob 可以计算出他们共享的信息量 I_{AB} 和 Eve 可获得的最大信息量 χ_{BE} . 因此, 在集体攻击下, Alice 和 Bob 可获得的安全密钥率为

$$K = \beta I_{AB} - \chi_{BE}, \quad (10)$$

其中, β 表示反向协商效率. 且

$$\begin{aligned} I_{AB} &= \frac{1}{2} \ln \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \\ \chi_{BE} &= \sum_{i=1,2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3,4,5} G\left(\frac{\lambda_i - 1}{2}\right). \end{aligned} \quad (11)$$

其中: $V = V_A + 1$; $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_{\text{hom}}/T$ 表示系统的总噪声, $\chi_{\text{line}} = T^{-1} + \varepsilon - 1$ 是信道输入过噪声, $\chi_{\text{hom}} = [(1 - \eta) + v_{el}]/\eta$ 是零差探测器的等效输入过噪声; $G(x) = (x + 1) \ln(x + 1) - x \ln x$; λ_i 是表示量子系统的协方差矩阵的辛本征值, 其中 $\lambda_{1,2}$ 为

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

$$A = V^2 + T^2(V + \chi_{\text{line}})^2 + 2T(1 - V^2),$$

$$B = T^2(1 + V\chi_{\text{line}})^2. \quad (12)$$

$\lambda_{3,4}$ 为

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

$$C = \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(V + \chi_{\text{line}})}{T(V + \chi_{\text{tot}})},$$

$$D = \frac{V\sqrt{B} + B\chi_{\text{hom}}}{T(V + \chi_{\text{tot}})}. \quad (13)$$

$\lambda_5 = 1$. 根据得到的安全密钥率, 可求出系统的密钥比特率为

$$R = f_{\text{rep}} K. \quad (14)$$

在不进行峰值补偿的情况下, 当系统估计的过噪声为 ε' 时, 实际的过噪声为

$$\varepsilon = \varepsilon' + \frac{1 - k^2}{k^2 t^2}; \quad (15)$$

在进行峰值补偿的情况下, 实际的过噪声等于估计的过噪声. 图 5(a) 给出了不同系统重复率 $f_{\text{rep}} = 2, 5, 8$ MHz 的安全密钥率随传输距离的变化, 从图中可知, 峰值补偿后系统的密钥率和传输距离不受系统重复率的影响, 且此时的安全传输距离大于不进行峰值补偿时的情况. 图 5(b) 给出了不同传输距离 $L = 30, 40, 50$ km 的密钥比特率随系统重复率的变化, 显然, 在进行峰值补偿后, 系统的密钥比特率随系统重复率的增加而呈正比持续增加; 而在不采取峰值补偿时, 密钥比特率随系统重复率的增加呈现先增加后减小的趋势. 因此, 本文提出的峰值补偿方案不仅增加了系统的安全性, 消除了由于有限采样带宽引入的安全性漏洞, 也解除了系统重复频率对密钥比特率的限制. 在计算密钥率的过程中, 涉及的系统参数分别设置为 $V_A = 20$, $v_{\text{el}} = 0.01$, $\beta = 0.95$, $\eta = 0.6$, $f_{\text{samp}} = 1$ GHz.

4 结 论

本文提出了一种基于峰值补偿的连续变量量子密钥分发方案, 通过在接收端的 ADC 后增加一个峰值补偿模块, 来解决由 ADC 的有限采样带宽引入的安全性问题. 详细介绍了有限采样带宽对系统安全性的影响, 描述了峰值补偿的具体步骤, 并

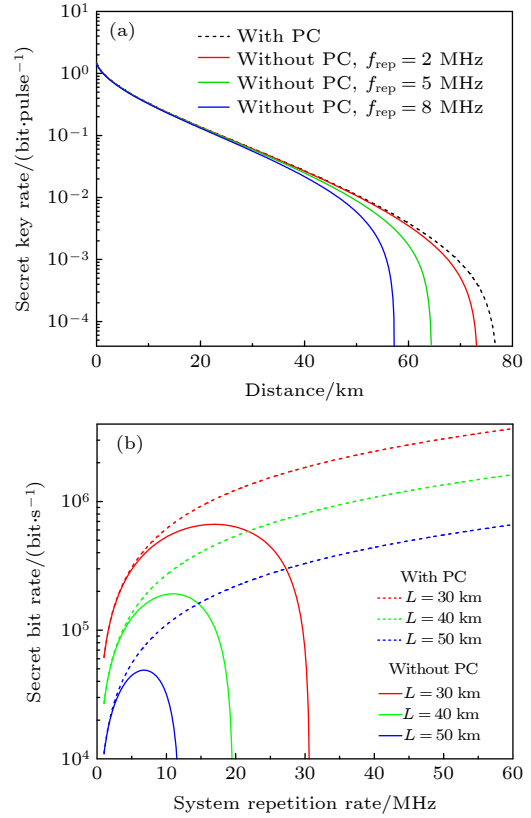


图 5 (a) 不同系统重复率下的密钥率随传输距离的变化; (b) 不同传输距离下的密钥比特率随系统重复率的变化

Fig. 5. (a) The secret key rate as a function of the transmission distance under different system repetition rate; (b) the secret bit rate as a function of the system repetition rate under different transmission distance.

基于仿真实验证明了该方案的有效性. 此外, 也针对采用峰值补偿和不采用峰值补偿两种情况, 分别分析了系统在集体攻击下的渐近安全性. 结果表明, 经过峰值补偿后, 系统能正确估计信道过噪声, 从而具有更长的安全传输距离, 其密钥比特率也不再受到系统重复率的限制, 随重复率的增加而呈正比持续增加.

值得注意的是, 该方案是基于一个脉冲内的三个采样值来实施峰值补偿, 因此 ADC 的采样频率必须大于三倍系统重复率, 这要求系统的重复率不能太高. 对目前的 CVQKD 系统而言, ADC 的采样频率通常在 GHz 级别, 而系统重复率通常在 MHz 级别, 这远远满足三倍重复率的要求. 在今后的研究工作中, 会进一步考虑这一要求对系统的影响, 以提高 CVQKD 系统的性能.

参考文献

- [1] Yin J, Li Y H, Liao S K, Yang M, Cao Y, Zhang L, Ren J G,

- Cai W Q, Liu W Y, Li S L, Shu R, Huang Y M, Deng L, Li L, Zhang Q, Liu N L, Chen Y A, Lu C Y, Wang X B, Xu F H, Wang J Y, Peng C Z, Ekert A K, Pan J W 2020 *Nature* **582** 501
- [2] Fang X T, Zeng P, Liu H, Zou M, Wu W J, Tang Y L, Sheng Y J, Xiang Y, Zhang W, Li H, Wang Z, You L, Li M J, Chen H, Chen Y A, Zhang Q, Peng C Z, Ma X, Chen T Y, Pan J W 2020 *Nat. Photonics* **14** 422
- [3] Wang B X, Mao Y Q, Shen L, Zhang L, Lan X B, Ge D W, Gao Y Y, Li J H, Tang Y L, Tang S B, Zhang J, Chen T Y, Pan J W 2020 *Opt. Express* **28** 12558
- [4] Zhang Y, Li Z, Chen Z, Weedbrook C, Zhao Y, Wang X, Huang Y, Xu C, Zhang X, Wang Z, Li M, Zhang X, Zheng Z, Chu B, Gao X, Meng N, Cai W, Wang Z, Wang G, Yu S, Guo H 2019 *Quantum Sci. and Technol.* **4** 035006
- [5] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B, Zhao Y, Xu B, Yu S, Guo H 2020 *Phys. Rev. Lett.* **125** 010502
- [6] Xu F, Ma X, Zhang Q, Lo H K, Pan J W 2020 *Rev. Mod. Phys.* **92** 025002
- [7] Laudenbach F, Pacher C, Fung C-H F, Poppe A, Peev M, Schrenk B, Hentschel M, Walther P, Hübel H 2018 *Adv. Quantum Technol.* **1** 1800011
- [8] Ralph T C 1999 *Phys. Rev. A* **61** 010303
- [9] Grosshans F, Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
- [10] Grosshans F, Cerf N J, Wenger J, Tualle-Brouiri R, Grangier P 2003 *Quantum Inf. Comput.* **3** 535
- [11] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C, Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
- [12] Pirandola S, Mancini S, Lloyd S, Braunstein S L 2008 *Nat. Phys.* **4** 726
- [13] Leverrier A, Grangier P 2009 *Phys. Rev. Lett.* **102** 180504
- [14] Weedbrook C, Pirandola S, Ralph T C 2012 *Phys. Rev. A* **86** 022318
- [15] Usenko V C, Grosshans F 2015 *Phys. Rev. A* **92** 062337
- [16] Grosshans F, Cerf N J 2004 *Phys. Rev. Lett.* **92** 047905
- [17] Navascués M, Grosshans F, Acín A 2006 *Phys. Rev. Lett.* **97** 190502
- [18] García-Patrón R, Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
- [19] Renner R, Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
- [20] Leverrier A, Grosshans F, Grangier P 2010 *Phys. Rev. A* **81** 062343
- [21] Leverrier A 2015 *Phys. Rev. Lett.* **114** 070501
- [22] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C, Leuchs G 2014 *New J. Phys.* **16** 123030
- [23] Jouguet P, Kunz-Jacques S, Diamanti E 2013 *Phys. Rev. A* **87** 062313
- [24] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **88** 022339
- [25] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C, Han Z F 2013 *Phys. Rev. A* **87** 062329
- [26] Ma X C, Sun S H, Jiang M S, Liang L M 2013 *Phys. Rev. A* **87** 052309
- [27] Huang J Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z Q, Wang S, Chen W, Guo G C, Han Z F 2014 *Phys. Rev. A* **89** 032304
- [28] Qin H, Kumar R, Alléaume R 2016 *Phys. Rev. A* **94** 012325
- [29] Qin H, Kumar R, Makarov V, Alléaume R 2018 *Phys. Rev. A* **98** 012312
- [30] Zheng Y, Huang P, Huang A, Peng J, Zeng G 2019 *Opt. Express* **27** 27369
- [31] Liu W, Wang X, Wang N, Du S, Li Y 2017 *Phys. Rev. A* **96**
- [32] Wang C, Huang P, Huang D, Lin D, Zeng G 2016 *Phys. Rev. A* **93** 022315
- [33] Li H, Wang C, Huang P, Huang D, Wang T, Zeng G 2016 *Opt. Express* **24** 20481
- [34] Huang D, Lin D, Wang C, Liu W, Fang S, Peng J, Huang P, Zeng G 2015 *Opt. Express* **23** 17511
- [35] Wang C, Huang D, Huang P, Lin D, Peng J, Zeng G 2015 *Sci. Rep.* **5** 14607
- [36] Qi B, Huang L L, Qian L, Lo H K 2007 *Phys. Rev. A* **76** 052323
- [37] Huang P, Huang J, Wang T, Li H, Huang D, Zeng G 2017 *Phys. Rev. A* **95** 052302

Continuous-variable quantum key distribution based on peak-compensation*

Mao Yi-Yu¹⁾ Wang Yi-Jun¹⁾ Guo Ying¹⁾

Mao Yu-Hao²⁾³⁾ Huang Wen-Ti^{4)†}

1) (*School of Automation, Central South University, Changsha 410083, China*)

2) (*School of Business, Central South University, Changsha 410083, China*)

3) (*Hunan Aerospace Construction Engineering Co., Ltd., Changsha 410205, China*)

4) (*School of Computer Science and Engineering, Central South University, Changsha 410083, China*)

(Received 7 December 2020; revised manuscript received 13 January 2021)

Abstract

Continuous-variable quantum key distribution (CVQKD) is an important application of quantum technology, which enables long-distance communicating parties to establish a string of unconditionally secure keys in an insecure environment. However, in a practical CVQKD system, the finite sampling bandwidth of the analog-to-digital converter (ADC) at the receiver may create inaccurate sampling results, leading to errors in parameter estimation process and leaving a security loophole for eavesdroppers. In order to eliminate the finite sampling bandwidth effect, we propose a peak-compensation-based CVQKD scheme, which estimates the discrepancy between the maximum sampling value and the peak value of each pulse based on the characteristics of Gaussian pulse. The maximum sampling values are compensated by the estimated discrepancy, so that the legitimate parties can obtain correct sampling results. We analyze the influence of the finite sampling bandwidth on the security of the system, expounding the specific steps of peak-compensation, comparing the estimated excess noise before and after peak-compensation, and discussing the security of the system under Gaussian collective attacks. Simulation results show that this scheme can greatly improve the accuracy of pulse peak sampling and remove the finite sampling bandwidth effect. Moreover, the channel parameters estimated by the communicating parties are also corrected by using the compensated values. Compared with the scheme without peak-compensation, this scheme eliminates the limitation of the system repetition to the secret key bit rate, and has longer secure transmission distance and higher secret key bit rate. In addition, compared with other methods of solving the finite sampling bandwidth effect, the proposed scheme can be directly implemented in data processing stage after sampling without any additional devices, and thus increasing no complexity of the system.

Keywords: continuous variable, quantum key distribution, sampling bandwidth, peak compensation

PACS: 03.67.Dd, 03.67.Hk

DOI: 10.7498/aps.70.20202073

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61871407, 61872390, 61801522).

† Corresponding author. E-mail: huangwenti@csu.edu.cn