第 58 卷 第 4 期 2009 年 4 月
1000-3290/2009/58(04)/2184-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.58,No.4,April,2009

基于信道估计的自适应连续变量量子密钥分发方法*

朱畅华† 裴昌幸 权东晓 陈 南 易运晖

(西安电子科技大学综合业务网理论及关键技术国家重点实验室,西安 710071)

(2008 年 7 月 22 日收到;2008 年 9 月 10 日收到修改稿)

为使连续变量量子密钥分发协议获得稳定的密钥生成率,需要根据信道变化动态调整发送光脉冲的强度.将光纤量子信道看作加性玻色量子高斯信道,给出高斯态通过玻色量子高斯信道仍得到高斯态的证明过程.通过平衡零差检测后,采用最大似然估计法得到了信道参数,进而根据估计的噪声大小自适应调整 Alice 发送的光脉冲的强度,从而获得稳定的密钥生成率.

关键词:量子密钥分发,连续变量,玻色量子高斯信道,信道估计

PACC:0367,4250

1. 引 言

自从 1984 年 IBM 公司的 Bennett 和加拿大蒙特利尔大学的 Brassard 提出第一个量子密钥分发协议(简称为 BB84 协议[1])以来,量子密码获得了快速发展.量子密码应用了量子力学的海森堡不确定性原理和量子态不可克隆定理,真正实现了绝对的安全通信.目前,基于光纤的弱相干光(近似单光子源)量子密钥分发已达到了 122 km[2],基于纠缠光源的方案在自由空间也已达到 144 km[3],而基于诱骗态的量子密钥分发在自由空间和光纤中均已超过 100 km[4,5].基于单光子的量子密钥分发利用单光子的偏振态或相位携带信息,需要单光子源和单光子探测器,而目前还没有理想的单光子源,通信频段的单光子探测器效率较低,从而使得生成的密钥速率很低.连续变量量子密钥分发利用光源的相位和振幅等携带信息,采用普通光源和零差测量即可实现,因而密钥生成率高.

大量的研究集中于连续变量量子密钥分发[6—18],已提出了压缩态、纠缠态和相干态等各种方案.Lodewyck 实现了 25 km 光纤信道的连续变量量子密钥分发,密钥速率大于 2 kb/s[19].在连续变量量子密钥分发的实现方案中,真空噪声、线路噪声、接收端的零差测量噪声和电子噪声等都对密钥生成率和密钥传输的最大安全距离有着直接的影响.Lodewyck 等研究了线路噪声的影响[20],陈进建等研究了由于参考光的真空噪声、分束器的透射率和反射率不相等引入的平衡零差测量误差,以及探测器的电子噪声的影响[21].

在实际的通信系统中,往往要保证一定的密钥生成率,为了达到这一要求,就需要根据信道的噪声大小自适应调整发端(Alice)发送光信号的强度.本文将光纤量子信道近似为加性玻色量子高斯信道,研究了高斯态通过玻色量子高斯信道后的量子态,并分析获知可用最大似然估计法估计信道参数,进而给出如何根据估计的噪声大小获得稳定的密钥生成率.

2. 连续变量量子密钥分发的工作过程及密钥生成率

基于高斯调制相干态的连续变量量子密钥分发协议的工作过程如下[14,15]:(1) Alice 获取两个随机数 x_A 和 p_A,分别对应无量纲的位置和动量,其值都服从均值为 0、方差为 $V_A N_0$ 的高斯分布,这里 N_0 为散粒噪声(shot noise)方差;(2) Alice 向 Bob 发送相干态 $|x_A + ip_A\rangle$;(3) Bob 采用零差检测随机选择测量 X 或 P;(4)通过经典信道 Bob 通知 Alice 他测得的观测值,舍弃未经测量的数据,则 Alice 和 Bob 共享两个相关的高斯变量;(5) Alice 和 Bob 交换部分数据,判断通信是否安全有效,如果有效他们采用协

* 国家自然科学基金(批准号:60572147,60672119)资助的课题.

† E-mail:chhzhu@xidian.edu.cn

调协议将其转换为比特串；(6)进行密性放大，得到最终密钥.

采用反向协调(Reverse Reconcillation)的连续变量量子密钥分发协议获得的每个脉冲的密钥生成率为[15]：

$$\Delta I_{\mathrm{RR}} = -\frac{1}{2}\log_2[T^2(1+\chi)(V^{-1}+\chi)], \quad (1)$$

式中，χ 为 Bob 端的等效输入噪声(其值为 N_0 的倍数)，它包括由于光纤量子信道损耗引起的真空噪声(vacuum noise) χ_{vac} 和其他因素引起的额外噪声(excess noise) ε，T 表示信道传输率，则 $\chi_{\mathrm{vac}} = (1-T)/T$，$V = V_{\mathrm{A}} + 1$. 若工作于 1550 nm 波段的光纤的衰减常数为 L_1(dB/km)，则对于长为 D(km)的光纤，其传输率可近似为 $T = 10^{-(L_1 D/10)}$.

由(1)式可见，信道噪声对密钥生成率有着较大的影响，ΔI_{RR} 随 χ 的变化曲线如图 1 和图 2 所示，图 1 中给出了 V 分别为 2，11 和 51 时的结果，此时 $\varepsilon = 0$，$L_1 = 0.2$ dB/km，$D = 0.5$—15 km. 图 2 中给出了 ε 分别为 0，0.1 和 0.2 时的结果，此时 $V = 31$，$L_1 = 0.2$ dB/km，$D = 0.5$—15 km. 因此，要达到稳定的 ΔI_{RR} 必须根据 χ 来调整 V_{A} 的大小. 接下来研究信道噪声 χ 的估计. 在下文中用 N_{C} 表示信道噪声方差(对应于噪声光子数).

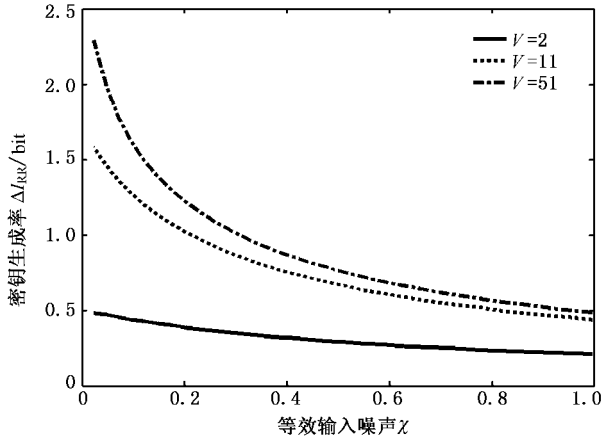

图 1　密钥生成率 ΔI_{RR} 与 χ 的关系

3. 玻色量子高斯信道参数的最大似然估计

玻色量子高斯信道是一类重要的量子信道，可

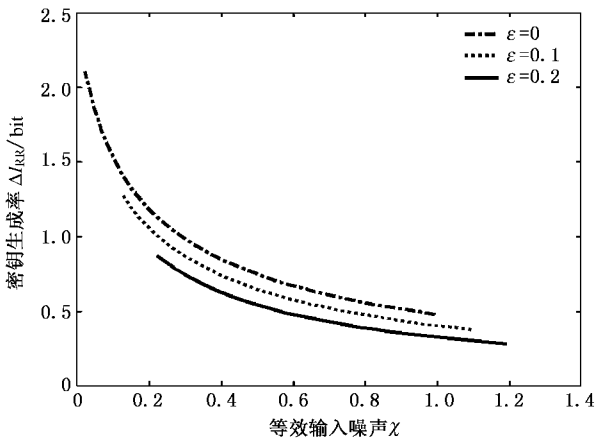

图 2　密钥生成率 ΔI_{RR} 与 χ 的关系

见于量子密码通信、量子信息处理等领域，有效建立信道模型对于系统的设计和优化具有重要意义. 量子信道估计有最大似然法[22]、贝叶斯估计[23]等. Holevo 研究了量子高斯信道的容量[24]，这里给出高斯态通过玻色量子高斯信道仍得到高斯态的证明过程，并采用最大似然估计法得到信道参数.

3.1. 高斯态经过玻色量子高斯信道后仍为高斯态

令 ρ_{in} 表示输入态的密度算子，则信道可看作一种映射，将输入态映射为输出态 ρ_{out}

$$\rho_{\mathrm{in}} \mapsto \rho_{\mathrm{out}} = C[\rho_{\mathrm{in}}]. \quad (2)$$

若信道输入为相干态 $|\alpha\rangle$，则 $\rho_{\mathrm{in}} = |\alpha\rangle\langle\alpha|$.

Holevo 给出了玻色量子高斯信道的表达式[24]：

$$\rho_{\mathrm{out}} = C[\rho_{\mathrm{in}}] = \int_C D(z)\rho_{\mathrm{in}}D^{\dagger}(z)p(z)\mathrm{d}^2 z, \quad (3)$$

式中平移算符 $D(z) = \mathrm{e}^{za^{\dagger} - z^{*}a}$，$a^{\dagger}$ 和 a 分别为输入态 $|\alpha\rangle$ 的生成算子和湮没算子，$p(z) = \frac{1}{\pi N_{\mathrm{C}}}\exp\left(-\frac{|z|^2}{N_{\mathrm{C}}}\right)$，$N_{\mathrm{C}}$ 为信道噪声的方差(即平均光子数).

量子光学高斯态的密度算子为[23]

$$\rho_{\mathrm{in}} = \frac{1}{\pi N}\int_C \mathrm{e}^{-\frac{|\alpha|^2}{N}}|\alpha\rangle\langle\alpha|\mathrm{d}^2\alpha. \quad (4)$$

处于高斯态的光脉冲的光子数服从泊松分布，平均光子数为 N. 我们有以下定理.

定理 1　对于玻色量子高斯信道，如果输入为高斯态，其方差为 N，则经过信道映射后的输出态也为高斯态，且其方差(平均光子数)变为 $N + N_{\mathrm{C}}$.

证明

$$\begin{aligned}\rho_{\text{out}} &= \int_{\mathrm{C}} D(z)\rho_{\text{in}}D^{\dagger}(z)p(z)\mathrm{d}^2z\\ &= \int_{\mathrm{C}} \frac{1}{\pi N}\mathrm{e}^{-\frac{|\alpha|^2}{N}}\left[\int_{\mathrm{C}} D(z)|\alpha\rangle\langle\alpha|D^{\dagger}(z)p(z)\mathrm{d}^2z\right]\mathrm{d}^2\alpha\\ &= \int_{\mathrm{C}} \frac{1}{\pi N}\mathrm{e}^{-\frac{|\alpha|^2}{N}}\left[\int_{\mathrm{C}} \frac{1}{\pi N_{\mathrm{C}}}\mathrm{e}^{-\frac{|z|^2}{N_{\mathrm{C}}}} D(z)\vdots\right.\\ &\quad\left.\times \mathrm{e}^{-(\alpha^{*}-a^{\dagger})(\alpha-a)}\vdots D^{\dagger}(z)\mathrm{d}^2z\right]\mathrm{d}^2\alpha\\ &= \int_{\mathrm{C}} \frac{1}{\pi N}\mathrm{e}^{-\frac{|\alpha|^2}{N}}\left[\frac{1}{\pi N_{\mathrm{C}}}\int_{\mathrm{C}}\mathrm{e}^{-\frac{|z|^2}{N_{\mathrm{C}}}}\vdots\right.\\ &\quad\left.\times \mathrm{e}^{-(z^{*}+\alpha^{*}-a^{\dagger})(z+\alpha-a)}\vdots\mathrm{d}^2z\right]\mathrm{d}^2\alpha\\ &= \int_{\mathrm{C}} \frac{1}{\pi N}\mathrm{e}^{-\frac{|\alpha|^2}{N}}\left[\frac{1}{\pi N_{\mathrm{C}}}\int_{\mathrm{C}}\mathrm{e}^{-\frac{|z-\alpha|^2}{N_{\mathrm{C}}}}|z\rangle\langle z|\mathrm{d}^2z\right]\mathrm{d}^2\alpha\\ &= \frac{1}{\pi(N+N_{\mathrm{C}})}\int_{\mathrm{C}}\mathrm{e}^{-\frac{|z|^2}{N+N_{\mathrm{C}}}}|z\rangle\langle z|\mathrm{d}^2z,\end{aligned}$$

所以，输出态也为高斯态，且其平均光子数变为 $N+N_{\mathrm{C}}$.

3.2. 玻色量子高斯信道参数的最大似然估计

对于高斯信道而言，高斯态可能是其最佳输入态[25]，因此用高斯态作为输入态. 平衡零差检测(Balance Homodyne Detection)是高斯态的常用检测方法. 对于高斯相干态，若本地谐振器的相位为 ϕ，则零差检测输出 y 服从高斯分布[22]：

$$p(y,\mu) = \sqrt{\frac{2}{\pi}}\exp\{-2[y-\mathrm{Re}(\mu\mathrm{e}^{-\mathrm{i}\phi})]^2\}, \quad (5)$$

其中 $|\mu|^2$ 为检测器输入信号态(高斯相干态)的光子数. 因此，参数 μ 可用最大似然法来估计，其对数似然函数为：

$$\begin{aligned}\ln L(\mu) &= \ln\left\{\prod_{k=1}^{K}\sqrt{\frac{2}{\pi}}\exp\{-2[y_k-\mathrm{Re}(\mu\mathrm{e}^{-\mathrm{i}\phi_k})]^2\}\right\}\\ &= \frac{K}{2}\ln\frac{2}{\pi}-2\sum_{k=1}^{K}[y_k-\mathrm{Re}(\mu\mathrm{e}^{-\mathrm{i}\phi_k})]^2. \quad (6)\end{aligned}$$

令 $\mu = Ae^{\mathrm{i}\psi}$，$A$ 为实数 μ 的模值，ψ 为相角，则

$$\ln L(A,\psi) = \frac{K}{2}\ln\frac{2}{\pi}-2\sum_{k=1}^{K}[y_k-A\cos(\psi-\phi_k)]^2. \quad (7)$$

最大似然估计器即为选择参数 A 和 ψ 使 $\ln L(A,\psi)$ 达到最大，即由 $\frac{\partial\ln L(A,\psi)}{\partial A}=0$，$\frac{\partial\ln L(A,\psi)}{\partial\psi}=0$ 可得

$$\hat{\psi} = \arctan\left(\frac{\overline{y\sin\phi}}{\overline{y\cos\phi}}\right), \quad (8)$$

$$\hat{A} = \frac{\overline{y\cos\phi}\cos\hat{\psi}+\overline{y\sin\phi}\sin\hat{\psi}}{\overline{\cos^2\phi}\cos^2\hat{\psi}+\overline{\sin\phi\cos\phi}\sin2\hat{\psi}+\overline{\sin^2\phi}\sin^2\hat{\psi}}. \quad (9)$$

在(8)和(9)式中，上划横线表示对所有 K 个样本求平均. 其估计值的方差分别满足

$$\begin{aligned}\sigma_{\psi}^2 &\geqslant \frac{1}{-K\cdot E\left[\frac{\partial^2 Lnp(y,A,\psi)}{\partial\psi^2}\right]}\\ &= \frac{1}{4KA^2\sin^2(\phi-\psi)} \geqslant \frac{1}{4KA^2}, \quad (10)\\ \sigma_{A}^2 &\geqslant \frac{1}{-K\cdot E\left[\frac{\partial^2 Lnp(y,A,\psi)}{\partial A^2}\right]}\\ &= \frac{1}{4K\cos^2(\phi-\psi)} \geqslant \frac{1}{4K}. \quad (11)\end{aligned}$$

当 $\phi-\psi=90^{\circ}$ 时，σ_{ψ}^2 取最小值. 当 $\phi-\psi=0^{\circ}$ 时，σ_{A}^2 取最小值.

至此得到 $\hat{\mu}=\hat{A}\mathrm{e}^{\mathrm{i}\hat{\psi}}$，则噪声方差

$$\hat{N}_{\mathrm{C}} = |\hat{\mu}|^2 - N = |\hat{A}|^2 - N, \quad (12)$$

所以，χ 的估计值为

$$\hat{\chi} = \frac{\hat{N}_{\mathrm{C}}hc}{\lambda N_0}, \quad (13)$$

其中 h 为普朗克常数，c 为光纤中的光速，λ 为工作波长(本文中为 1550 nm). 散粒噪声 N_0 可以通过测量获得. 对于固定长的光纤，若工作中光纤所在的环境基本不变，则 $T=10^{-(L_1D/10)}$ 可认为是固定常数，只与长度和衰减常数有关.

4. 依据噪声估计自适应调整高斯调制相干态的方差

由(1)式得

$$V_{\mathrm{A}} = \{[T^2(1+\chi)4^{\Delta I_{\mathrm{RR}}}]^{-1}-\chi\}^{-1}-1. \quad (14)$$

为获得稳定的密钥生成率 ΔI_{RR}，应根据估计得到的等效输入噪声 $\hat{\chi}$ 来调整 V_{A} 的大小，工作过程如下：

①制备高斯态 ρ_{in}，由(8)、(9)、(12)和(13)式估计等效输入噪声 $\hat{\chi}$；

② 根据设定的密钥生成率 ΔI_{RR} 及 $\hat{\chi}$，由(14)式计算得到 V_{A}，制备高斯调制的相干态，根据第 2 节所述过程进行量子密钥分发；

③经过时间段 TI 后，统计测量获得的密钥生成率 $\Delta I'_{\mathrm{RR}}$，若 $|\Delta I_{\mathrm{RR}}-\Delta I'_{\mathrm{RR}}|>\zeta$，$0<\zeta<1$，则执行步骤

①，估计等效输入噪声 $\hat{\chi}'$，以 $\hat{\chi}'$ 代替 $\hat{\chi}$，执行步骤②；

④重复执行步骤③直至量子密钥分发结束.

值得注意的是通过调整 V_A，对不同的噪声大小，ΔI_{RR} 不可能超越其最大值，即当 $V_A \to \infty$ 时的值，如图3所示.由图3可见，若估计的噪声大小处于 χ_1 和 χ_2 之间，则对应的密钥生成率最大值在 ΔI_{RRmax1} 和 ΔI_{RRmax2} 之间.通过调整可以使密钥生成率维持在 ΔI_{RRmax2} 以下的稳定值.

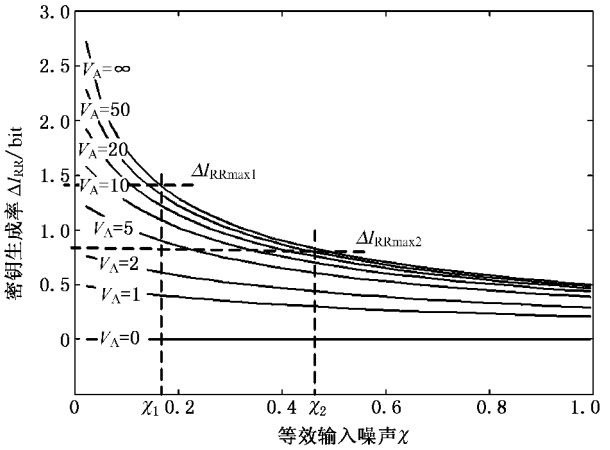

图3　V_A 随 χ 调整的示意图

由上述自适应调整 V_A 的过程可见，只要设置合适的 TI 值，则密钥分发过程中有 $|\Delta I_{RR} - \Delta I'_{RR}| \leqslant \zeta$，即实际获得的密钥生成率与设定值的误差控制在 ζ 以内，因此能维持稳定的 ΔI_{RR}.

5. 结　论

本文研究了光纤量子高斯信道噪声方差的估计，证明高斯态通过量子高斯信道后仍为高斯态，且其方差变为 $N + N_C$.采用平衡零差检测测量高斯态得到的输出服从高斯分布，应用最大似然估计得到信道的噪声参数，进而根据估计的噪声大小调整 Alice 发送光脉冲的强度，从而获得稳定的密钥生成率.下一步的工作是建立考虑退极化、衰减等因素的一般化信道模型，估计其参数，将其用于量子通信系统的设计.

[1] Bennett C H, Brassard G 1984 *Int. Conf. Comput. Syst. Signal Process.* (Bangalore, New York: IEEE) 175

[2] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[3] Ursin R, Tiefenbacher F, Schmitt-Manderbach T *et al* 2007 *Nature Physics* **3** 481

[4] Schmitt-Manderbach T, Weier H, Furst M *et al* 2007 *Phys. Rev. Lett.* **98** 010504

[5] Peng C Z, Zhang J, Yang D, Gao W B, Ma H X, Yin H, Zeng H P, Yang T, Wang X B, Pan J W 2007 *Phys. Rev. Lett.* **98** 010505

[6] Ralph T C 1999 *Phys. Rev.* A **61** 010303(R)

[7] Ralph T C 2000 *Phys. Rev.* A **62** 062306

[8] Hillery M 2000 *Phys. Rev.* A **61** 022309

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

[10] Gottesman D, Preskill J 2001 *Phys. Rev.* A **63** 022309

[11] Cerf N J, Levy M, Van Assche G 2001 *Phys. Rev.* A **63** 052311

[12] Reid M D 2000 *Phys. Rev.* A **62** 062308

[13] Silberhorn C, Korolkova N, Leuchs G 2002 *Phys. Rev. Lett.* **88** 167902

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

[15] Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf N, Grangier P 2003 *Nature* **421** 238

[16] Bencheikh K, Symul T, Jankovic A, Levenson J A 2001 *J. Mod. Optics* **48** 1903

[17] Silberhorn C, Ralph, T C, Lutkenhaus N, Leuchs G 2002 *Phys. Rev. Lett.* **89** 167901

[18] He G Q, Guo H B, Li Y D, Zhu S W, Zeng G H 2008 *Acta Phys. Sin.* **57** 2212 (in Chinese) [何广强、郭红斌、李昱丹、朱思维、曾贵华 2008 物理学报 **57** 2212]

[19] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W, Grangier P 2007 *Phys. Rev.* A **76** 042305

[20] Lodewyck J, Debuisschert T, Tualle-Brouri R, Grangier P 2005 *Phys. Rev.* A **72** 050303(R)

[21] Chen J J, Han Z F, Zhao Y B, Gui Y Z, Guo G C 2007 *Acta Phys. Sin.* **56** 5 (in Chinese) [陈进建、韩正甫、赵义博、桂有珍、郭光灿 2007 物理学报 **56** 5]

[22] Mauro D G, Paris M G A, Sacchi M F 2000 *Phys. Rev.* A **62** 023815

[23] Wang X B, Hiroshima T, Tomita A, Hayashi M 2007 *Phys. Rep.* **448** 1

[24] Holevo A S 2007 *Probl. Inform. Transm.* **43** 1

[25] Holevo A S, Shirokov M E www.arxiv.org/pdf/quant-ph/0408176v1

Adaptive continuous variable quantum key distribution based on channel estimation *

Zhu Chang-Hua† Pei Chang-Xing Quan Dong-Xiao Chen Nan Yi Yun-Hui
(*State Key Laboratory of Integrated Services Networks*, *Xidian University*, *Xi'an* 710071, *China*)
(Received 22 July 2008; revised manuscript received 10 September 2008)

Abstract

In order to obtain steady key rate for a continuous variable quantum key distribution system, Alice should adaptively adjust the intensity of optical pulses she sents. In this paper, an optical fiber channel is taken as the additive bosonic quantum Gaussian channel. It is proven that a Gaussian channel transforms Gaussian states into Gaussian states. The maximum-likelihood method is used to estimate the channel parameters after balanced homodyne detection. Then, Alice can change the intensity of optical pulses adaptively according to the estimated noise level, thereby a steady key rate can be obtained.

Keywords: quantum key distribution, continuous variable, bosonic quantum Gaussian channel, channel estimation
PACC: 0367, 4250

* Project supported by the National Natural Science Foundation of China (Grant Nos. 60572147, 60672119).

† E-mail: chhzhu@xidian.edu.cn