第 54 卷 第 2 期 2005 年 2 月
1000-3290/2005/54(02)/0517-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.54,No.2,February,2005

基于六态协议的实际 QKD 系统的窃听问题研究*

刘景锋[1)] 唐志列[2)†] 梁瑞生[1)] 李凌燕[1)] 魏正军[2)]
陈志新[2)] 廖常俊[1)] 刘颂豪[1)]

[1)](华南师范大学信息光电子科技学院,广州 510631)

[2)](华南师范大学物理与电信工程学院,广州 510631)

(2003 年 10 月 22 日收到;2004 年 7 月 7 日收到修改稿)

基于实际量子密钥分配系统中所使用的强衰减的激光脉冲不是单光子,量子密钥分配的信道不是无损耗的,光子计数器存在探测效率和暗计数以及窃听者的技术能力也不是无限的这些具体问题.采用了分束与 Breidbart 基相结合的窃听策略讨论了窃听问题并给出了合法用户在筛选后的密钥中所能容忍的误码率上限公式.

关键词:量子密钥分配,六态协议,光子数统计分布,Breidbart 基窃听

PACC:0365,4230,4250

1. 引 言

量子密钥分配(QKD)[1—4]协议利用单光子固有的量子随机性实现了具有无条件安全的密钥分配.从原理上来说,合法的通信双方(设为 Alice 和 Bob,窃听者为 Eve)传递密钥用的是绝对的单光子,并且不考虑光纤损耗,在以上情况下量子密钥的传递是绝对安全的.但在实际应用中,单光子往往被可能包含多个光子的弱激光脉冲代替,也没有不损耗的光纤.因而多光子的出现和信道损耗为高效的窃听策略所利用,这样量子密钥分配的安全性就受到威胁.

本文基于现实的技术问题来讨论窃听问题.首先收发双方没有理想的单光子源,单光子脉冲被弱激光脉冲代替.现实中也没有不损耗的光纤,本文假设 Alice 和 Bob 用的是标准光纤,在 1550nm 通信窗口其吸收系数为 $\alpha_{AB}=0.25\mathrm{dBkm}^{-1}$,其光纤的传输效率 $F=10^{-(\alpha_{AB}L+c)/10}$,式中 L 是光纤的长度,c 是固定损耗.其次,窃听者不可能拥有无限的技术能力,假设 Eve 的实际技术能力为

1) Eve 可能自由的进入 Alice 和 Bob 的办公室外的量子信道和安装一些光器件而不被觉察.

2) Eve 的光子计数器的探测效率为 1,但是不能进行无破坏性(QND)探测,也不能储存光子,所有的探测都是在接受到光子后探测基被宣布以前进行.

3) Eve 不可能拥有无损的光纤,在 1550nm 的通信窗口光纤总损耗一般为 $0.25\mathrm{dBkm}^{-1}$,本文假设 Eve 拥有较高技术能力,采用的光纤损耗系数为 $\alpha_E=0.15\mathrm{dBkm}^{-1}$.

本文基于以上的技术实际和杨理等讨论的结果[5],采用分束与 Breidbart 基相结合的窃听方案来讨论基于六态协议[6,7]的实际 QKD 系统的窃听问题.首先把所有的错误都认为是由 Eve 引起的,最后再讨论实际错误的来源;讨论了光子数分布统计问题;讨论了弱激光脉冲作光源且光纤有损耗的情况下的窃听问题,并给出了 Alice 和 Bob 在筛选后的密钥中所能容忍的误码率上限,利用这一上限可以判断信道是否安全.

2. 光子数统计分布

激光器在高于阈值工作时,产生的激光是相干态的光子,其光子数服从泊松分布

$$P(n,\mu)=\frac{\mu^n}{n!}\mathrm{e}^{-\mu}, \tag{1}$$

即 Alice 向 Bob 发出的光子是服从泊松分布的光子,而不是真正的单光子.考虑到光纤的 损耗,设光纤的传输效率为 F,则到达 Bob 探测器入口处的光子分布为[8]

* 国家重点基础研究发展规划项目(批准号:2001CB309300)及广州市科技攻关计划项目(批准号:1999Z03501)资助的课题.

† E-mail:tangzhl@scnu.edu.cn

$$P(m,\mu F) = \sum_{n=0}^{\infty} P(n,\mu) C_n^m F^m (1-F)^{n-m} = \frac{(\mu F)^m}{m!} e^{-\mu F}. \quad (2)$$

考虑到探测器的探测效率为 η,探测器探测到 l 个光子的概率为

$$P(l,\mu\eta F) = \sum_{n,m=0}^{\infty} P(n,\mu) C_n^m F^m (1-F)^{n-m} C_m^l \eta^l (1-\eta)^{m-l} = \frac{(\mu\eta F)}{l!} e^{-\mu\eta F}. \quad (3)$$

由(2)式可见经过有损耗的光纤后,光子的分布仍为泊松分布,仅仅是平均光子数降低.下面考虑经分束器分束后光子的统计分布,如图 1,分束器的通道 3 的耦合效率为 λ,相干态 $|\alpha\rangle_1$(下标代表通道号)从通道 1 进入耦合器.不考虑耦合器的反射,通过耦合器后得到[9]

$$|\alpha\rangle_1 = \sum_{n=0}^{\infty} \sqrt{p_n} |n\rangle_1 \rightarrow \sum_{n=0}^{\infty} \sqrt{p_n} \sum_{i=0}^{n} \sqrt{c_i} |i\rangle_3 |n-i\rangle_4, \quad (4)$$

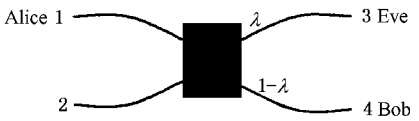

图 1 分束器

c_i 为出现每种情况的权重系数,每个光子走通道 3 或通道 4 是相互独立事件,光子走通道 3 或通道 4 服从二项式分布,则 $c_i = C_n^i \lambda^i (1-\lambda)^{n-i}$.由(3)式(考虑正交归一),在通道 3 处输出 j 个光子的概率为

$$P(j) = |(\sum_{m=0}^{\infty} \langle j|_3 \langle m-j|_4) \times (\sum_{n=0}^{\infty} \sqrt{p_n} \sum_{i=0}^{n} \sqrt{c_i} |i\rangle_3 |n-i\rangle_4|^2 = \sum_{m=0}^{\infty} p_m c_j. \quad (5)$$

下面分三种情况来讨论.

1) 3,4 通道都有光子输出,此时输入每脉冲中至少含有 2 个光子.则通道 3 处输出非空脉冲概率为

$$P_1 = \sum_{n=2}^{\infty} p_n \sum_{i=1}^{n-1} |c_i|^2 = 1 + e^{-\mu} - e^{-\mu\lambda} - e^{-\mu(1-\lambda)}. \quad (6)$$

2)只有通道 4 输出光子,Eve 用耦合器没有耦合出光子,发生这种情况的概率为

$$P_2 = \sum_{n=1}^{\infty} p_n |c_n|^2 = e^{-\mu\lambda} - e^{-\mu}. \quad (7)$$

3)只有通道 3 中有光子,此时光子全被 Eve 耦合出,发生这种情况的概率为

$$P_3 = \sum_{n=1}^{\infty} p_n |c_0|^2 = e^{-\mu(1-\lambda)} - e^{-\mu}. \quad (8)$$

另外由(5)式可求出经过耦合器后,在通道 4 中能探测到 i 个光子的概率为

$$P[i,(1-\lambda)\mu] = e^{-\mu(1-\lambda)} \frac{[\mu(1-\lambda)]^i}{i!}. \quad (9)$$

由上式看出经过分束器后,光子的分布仍属于泊松分布,也仅是平均光子数减小.

3. 基于实际系统的窃听方案

基于杨理等的讨论[5],采用 B 基窃听/B 基重发 Eve 的窃听效率最高

$$P = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right) = 0.7887, \quad (10)$$

此时在 Bob 的密钥中引起误码的概率为

$$e = 2P(1-P) = 1/3. \quad (11)$$

若 Eve 对每个非空脉冲都测量,则对筛选后的密钥串的窃听概率为 $P = 0.7887$,此时在 Alice 和 Bob 筛选后的密钥串中由 Eve 所引起的误码的概率为 $e = 1/3$.如果 Alice 和 Bob 发现在筛选后的密钥串中有 1/3 的误码,那么可以肯定 Eve 在窃听.Eve 为了隐蔽自己在窃听,就截取部分非空脉冲进行测量,截取的部分为 ξ,在这种情况下,Eve 猜对总码的概率为

$$P(\xi) = \frac{\xi}{2}\left(1 + \frac{1}{\sqrt{3}}\right) + \frac{1-\xi}{2}, \quad (12)$$

式中等号右边第 2 项是对没有测量的非空脉冲猜对码的概率为 1/2,那么 Eve 在筛选后的密钥中可能导致的误码率为 $e(\xi) = \xi/3$,代入(12)式得到 P 与 e 的函数关系式

$$P(e) = \frac{\sqrt{3}}{2} e + \frac{1}{2}. \quad (13)$$

从上式可见,当 $e = 1/3$,即 $\xi = 1$ 时,即对全部脉冲进行窃听,此时的窃听效率最高.下面就利用分束和 Breidbart 相结合的方案来讨论基于六态协议的实际 QKD 系统的窃听问题.

图 2 是 Eve 窃听装置图,由于 Alice 的光源不是真正的单光子源,而是光子数服从泊松分布的弱激

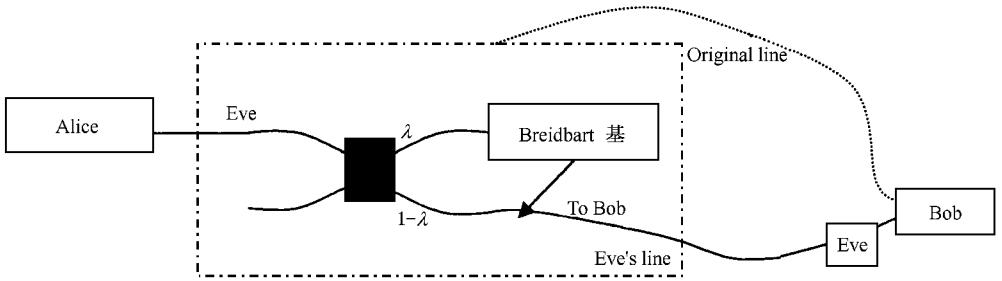

图 2　Eve 的窃听装置图

光脉冲.利用这一缺点,Eve 用一个耦合器耦合出 λ 部分光子并立刻对这部分光子利用 Breidbart 基窃听.在这种情况下,不会引起 Alice 与 Bob 的误码.若没耦合出光子,则忽略多光子脉冲的存在而在另一路利用 Breidbart 基窃听.

由(2),(3)式可知经过分束耦合器后,通向 Bob 的非空脉冲为 $1-\mathrm{e}^{-\mu(1-\lambda)}$,这部分脉冲经过 Eve 的光纤后到达 Bob 探测器入口处的非空脉冲为 $1-\mathrm{e}^{-\mu(1-\lambda)F_{\mathrm{E}}}$,$F_{\mathrm{E}}$ 为 Eve 的光纤的传递效率.Bob 可探测到光子的概率为 $1-\mathrm{e}^{-\mu\eta(1-\lambda)F_{\mathrm{E}}}$,式中 η 为探测器的探测效率.则从耦合器出来的光子能被探测到的概率为

$$\beta=\frac{1-\mathrm{e}^{-\mu\eta(1-\lambda)F_{\mathrm{E}}}}{1-\mathrm{e}^{-\mu(1-\lambda)}}. \tag{14}$$

下面分两种情况来讨论.

1)耦合器耦合出部分光子,对应(6)式的情况.Eve 的窃听不会在筛选后的密钥中造成误码,在这种情况下,Eve 可能猜对每个码字的概率为

$$P'\left(e=\frac{1}{3}\right)=\frac{3+\sqrt{3}}{6}. \tag{15}$$

此时,Eve 在筛选后的密钥串中能猜对总码的概率为

$$P_1^{\mathrm{correct}}=\frac{\beta P_1 P'(e=1/3)}{1-\mathrm{e}^{-\mu\eta(1-\lambda)F_{\mathrm{E}}}}. \tag{16}$$

2)Eve 用分束器没有耦合到光子,对应(7)式的情况,测量部分通向 Bob 的脉冲,因为这种测量会在 Alice 和 Bob 筛选后的密钥中造成误码,测量的脉冲越多,造成的误码就越多,我们选择测量其中的部分 ξ,从而 Alice 和 Bob 在筛选后的密钥中能观测到的误码率为

$$e=\frac{e(\xi)\beta P_2}{1-\mathrm{e}^{-\mu\eta(1-\lambda)F_{\mathrm{E}}}}. \tag{17}$$

在这种情况下,Eve 在筛选后的密钥串中能猜对总码的概率为

$$P_2^{\mathrm{correct}}=\frac{\beta P_2 P'[e(\xi)]}{1-\mathrm{e}^{-\mu\eta(1-\lambda)F_{\mathrm{E}}}}, \tag{18}$$

式中 $P'[e(\xi)]=\frac{\sqrt{3}}{2}e(\xi)+1/2$.

综合以上两种情况,Eve 在筛选后的密钥中能猜对总码的概率为

$$\begin{aligned}P_{\mathrm{tot}}^{\mathrm{correct}}&=\frac{\beta P_1 P'(e=1/3)+\beta P_2 P'[e(\xi)]}{1-\mathrm{e}^{-\mu\eta(1-\lambda)F_{\mathrm{E}}}}\\&=\frac{P_1 P'(e=1/3)+P_2 P'[e(\xi)]}{1-\mathrm{e}^{-\mu(1-\lambda)}}.\end{aligned} \tag{19}$$

Alice 与 Bob 拥有光纤的传输效率为 F_{AB},为了使 Bob 得到期望的光子数统计,使 $(1-\lambda)F_{\mathrm{E}}=F_{\mathrm{AB}}$.在此条件下,为了不引起 Alice 和 Bob 的怀疑,Eve 应尽可能降低探测部分 ξ 以至降低 Alice 与 Bob 的误码率.

由(19)式得

$$P_{\mathrm{tot}}^{\mathrm{correct}}=\frac{\sqrt{3}+3}{6}+\frac{\sqrt{3}}{2}\mathrm{e}^{-\mu\left(\frac{F_{\mathrm{E}}-F_{\mathrm{AB}}}{F_{\mathrm{E}}}\right)}\left[e(\xi)-\frac{1}{3}\right]. \tag{20}$$

从(17)式可知,Alice 和 Bob 在筛选后的密钥中观察到的误码率为

$$e=e(\xi)\mathrm{e}^{-\mu\left(\frac{F_{\mathrm{E}}-F_{\mathrm{AB}}}{F_{\mathrm{E}}}\right)}. \tag{21}$$

通过(21)式,Eve 可以控制误码率,并且通过测知光纤长度 L,由(20)式可算出获得正确比特值的概率.

若 Eve 获得的信息量小于 Alice 和 Bob 的互信息量,即 $I(\mathrm{A},\mathrm{B})\geqslant I(E)$[10],则 Alice 和 Bob 就可利用保密加强技术获得二者公用密钥,否则就不可能获得共享的密钥.对于二元对称信道,Alice 和 Bob 的互信息量为[11]

$$I(\mathrm{A},\mathrm{B})=1+e\log_2 e+(1-e)\log_2(1-e), \tag{22}$$

式中 e 是误码率,上式可写为[12]

$$I(\mathrm{A},\mathrm{B})=\frac{1}{2}\phi(1-2e). \tag{23}$$

Eve 猜错码的概率为 $(1-P_{\mathrm{tot}}^{\mathrm{correct}})$,从而窃听到的信息量为

$$I(\mathrm{E}) = \frac{1}{2}\phi[1 - 2(1 - P_{\mathrm{tot}}^{\mathrm{correct}})]. \quad (24)$$

Alice 和 Bob 要得到共享的密钥串，由限制条件 $I(\mathrm{A},\mathrm{B}) \geqslant I(\mathrm{E})$ 与(23)，(24)式可得到

$$e < 1 - P_{\mathrm{tot}}^{\mathrm{correct}}. \quad (25)$$

由上式与(20)，(21)式可得 Alice 和 Bob 所能接受的误码率上限为

$$e < \frac{3+\sqrt{3}[\mathrm{e}^{-\mu(\frac{F_{\mathrm{E}}-F_{\mathrm{AB}}}{F_{\mathrm{E}}})}-1]}{3(2+\sqrt{3})}. \quad (26)$$

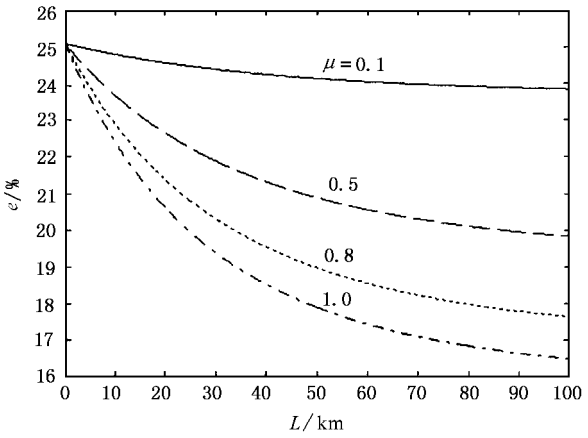

图 3 误码率与传输长度和平均光子数关系图

由此可见，Alice 和 Bob 只有保证筛选后的密钥串中的误码率 e 小于 $\frac{3+\sqrt{3}[\mathrm{e}^{-\mu(\frac{F_{\mathrm{E}}-F_{\mathrm{AB}}}{F_{\mathrm{E}}})}-1]}{3(2+\sqrt{3})}$，二者才能利用保密加强技术获得公用密钥串.图 3 给出了 Alice 和 Bob 在不同的平均光子数和不同的传输距离下所能接受的最大误码率曲线图，若误码率在每条曲线之下，Alice 和 Bob 就能通过保密加强技术获得二者公用的密钥，否则就认为信道不安全，有 Eve 存在，必须丢掉这组数据后重发.在以上的讨论中，把所有导致误码的结果都归咎于 Eve 的作用，在实际当中在筛选后的密钥中量子比特误码主要来源于：1)仪器本身的缺陷导致了干涉或偏振对比度的精度不高；2)探测器暗计数；3)后脉冲的影响；4) Eve 的窃听.我们把 $\frac{3+\sqrt{3}[\mathrm{e}^{-\mu(\frac{F_{\mathrm{E}}-F_{\mathrm{AB}}}{F_{\mathrm{E}}})}-1]}{3(2+\sqrt{3})}$ 作误码率上限，其实它是由以上四部分组成，Eve 导致的误码仅是其中的一部分，故实际上 Eve 获得的信息量小于通过(22)式算出的信息量，从而可保证形成 Alice 和 Bob 公用的密钥串.

4. 结 论

本文基于实际量子密钥分配系统所使用的强衰减的激光脉冲不是单光子、量子密钥分配的信道不是无损耗以及光子计数器存在探测效率和暗计数这些实际问题，采用分束与 Breid-bart 基窃听策略相结合的方案讨论了窃听问题，并给出了 Alice 和 Bob 在筛选后的密钥中所能接受的最大误码率公式.基于误码率上限公式，Alice 和 Bob 可以判断在量子信道中是否有窃听者存在，从而限制 Eve 只能获得部分信息而保证密钥是绝对安全的.

[1] Bennett C and Brassard G 1984 *Proceedings of the IEEEE International Conference on Computers. Systems and Signal Processing*, *Bangalore*, *India* (New York: IEEE) p175—179

[2] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[3] Ekert A E 1991 *Phys. Rev. Lett.*, **67** 661

[4] Liang C *et al* 2001 *Acta. Phys. Sin.* **50** 1429 (in Chinese) [梁创 等 2001 物理学报 **50** 1429]

[5] Yang L *et al* 2002 *Acta. Phys. Sin.* **51** 961 (in Chinese) [杨 理 等 2002 物理学报 **51** 961]

[6] Bruss D 1998 *Phys. Rev. Lett.* **81** 3018

[7] Bechmann-Pasquinucci H and Gisin N 1999 *Phys. Rev.* A **59** 4238

[8] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[9] Li F L 1992 *High Laser Physics* (Hefei: University of science and technology of China press) p304—308 (in Chinese) [李福利 1992 高等激光物理学(合肥：中国科学技术大学出版社)第 304—308 页]

[10] Ekert A *et al* 1994 *Phys. Rev.* A **50** 1047

[11] Zhou M Q 2002 *Information theory foundation* (Beijing: Beihang University Press) p72—77 (in Chinese) [周萌清 2002 信息论基础(北京 北京航空航天大学出版社)第 72—77 页]

[12] Fuchs A *et al* 1997 *Phys. Rev.* A **56** 1163

Eavesdropping on practical QKD system based on six-state protocol*

Liu Jing-Feng[1)]　Tang Zhi-Lie[2)]　Liang Rui-Sheng[1)]　Li Ling-Yan[1)]
Wei Zheng-Jun[2)]　Chen Zhi-Xin[2)]　Liao Chang-Jun[1)]　Liu Song-Hao[1)]
[1)] (*School for Information and Optoelectronics Science and Engineering*, *South China Normal University*, *Guangzhou* 510631, *China*)
[2)] (*School of Physics and Telecommunication Engineering*, *South China Normal University*, *Guangzhou* 510631, *China*)
(Received 22 October 2003; revised manuscript received 7 July 2004)

Abstract

Based on practical implementations of quantum cryptography with the attenuated laser pulses as the signal source rather than single photon, as well as lossy channels, detection efficiency, dark count of single-photon counter, and technological possibilities of a realistic eavesdropping, we discuss a combining eavesdropping strategy of Breidbart basis and beamsplitting, and give a bound on maximum disturbance for a given mean photon number and transmission length for which a secret key can be distilled.

Keywords: quantum key distribution, six-state protocol, photon number statistics distributing, Breidbart basis
PACC: 0365, 4230, 4250

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 2001CB309300) and the Foundation for Science and Technology of Guangzhou, China (Grant No. 1999Z03501).