基于BB84协议的实际QKD系统的窃听问题研究*

刘景锋[1] 梁瑞生[1] 唐志列[2] 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 华南师范大学物理系,广州 510631)

摘 要 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并不是单光子,量子密钥分配的信道不是无损耗的,窃听者的技术能力也不是无限的这些具体问题,采用了分束窃听与截获重发窃听策略相结合的方案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.

关键词 量子密钥;BB84协议;光子数统计分布;窃听策略

中图分类号 TN911.2 **文献标识码** A

0 引言

量子密钥分配(QKD)协议[1~3]利用单光子固有的量子随机性实现了具有无条件安全性的密钥分配. 从原理上来说,合法的通信双方(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. 但是在实际应用中,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.

有些窃听策略已被讨论[4~7]. 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,我们认为Alice和Bob用的是标准光纤,在1550 nm通信窗口其吸收系数$\alpha_{AB}=0.25\ \mathrm{dBkm^{-1}}$,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可以自由的进入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1550 nm的通信窗口光纤损耗一般为0.25 $\mathrm{dBkm^{-1}}$,我们假设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,就BB84协议来讨论Eve的窃听问题.

1 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[8]

$$|\alpha\rangle=e^{-\frac{1}{2}|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle \tag{1}$$

在相干态$|\alpha\rangle$中发现n个光子的几率为

$$p(n)=\langle\alpha|\alpha\rangle=\frac{|\alpha|^{2n}}{n!}e^{-|\alpha|^2} \tag{2}$$

令$|\alpha|^2=\mu$,则

$$P(n,\mu)=\frac{\mu^n}{n!}e^{-\mu} \tag{3}$$

这就是泊松分布. 即Alice向Bob发出的光子是泊松分布的光子,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,到达Bob探测器入口处的光子分布为

$$P(m,\mu F)=\sum_{n=0}^{\infty}P(n,\mu)C_n^mF^m(1-F)^{n-m}=\frac{(\mu F)^m}{m!}e^{-\mu F} \tag{4}$$

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.

下面我们来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. 真空态$|0\rangle_2$从通道2进入. 通过耦合器后得到

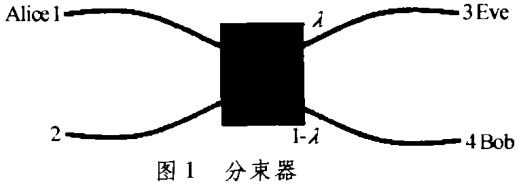


图1 分束器

Fig. 1 Beam splitter

*国家973(2001CB309300)项目及广州市(1999Z03501)资助项目

Tel:020-33351640 Email:jingfengliu@163.com

收稿日期:2003-09-26

$$|\alpha\rangle_1\otimes|0\rangle_2=\sum_{n=0}^{\infty}\sqrt{p_n}|n\rangle_1\otimes|0\rangle_2\rightarrow\sum_{n=0}^{\infty}\sqrt{p_n}\cdot\sum_{i=0}^{n}c_i|i\rangle_3\otimes|n-i\rangle_4 \tag{5}$$

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 $c_i=[C_n^i\lambda^c(1-\lambda)^{n-i}]^{1/2}$. 由式(5)，在通道 3 处输出 j 个光子的概率为

$$P(j)=|(\sum_{m=0}^{\infty}\langle j|_3\otimes\langle m-j|_4)(\sum_{n=0}^{\infty}\sqrt{p_n}\sum_{i=0}^{n}c_i|i\rangle_3\otimes|n-i\rangle_4)|^2=\sum_{m=0}^{\infty}p_m|c_j|^2 \tag{6}$$

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

$$P_1=\sum_{n=2}^{\infty}p_n\sum_{i=1}^{n-1}|c_i|^2=1+e^{-\mu}-e^{-\mu\lambda}-e^{-\mu(1-\lambda)} \tag{7}$$

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

$$P_2=\sum_{n=1}^{\infty}p_n|c_n|^2=e^{-\mu\lambda}-e^{-\mu} \tag{8}$$

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

$$P_3=\sum_{n=1}^{\infty}p_n|c_0|^2=e^{-\mu(1-\lambda)}-e^{-\mu} \tag{9}$$

另外由式(6)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

$$P[i,(1-\lambda)\mu]=e^{-\mu(1-\lambda)}\frac{[\mu(1-\lambda)]^i}{i!} \tag{10}$$

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.

2　基于单光子的截获重发窃听方案的基本原理

在 BB84 协议中，Alice 向 Bob 发出量子态是光子的 4 个极化态，它们的夹角为 π/4，如图 2，用量子态表示为 $|H\rangle$，$|V\rangle$，$|\pi/4\rangle$，$|-\pi/4\rangle$. 其关系为

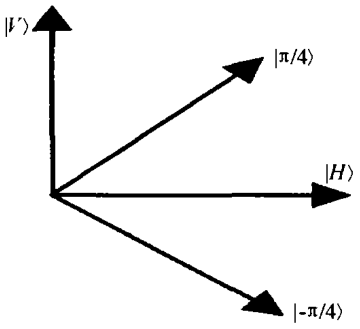


图 2　BB84 协议的 4 个基

Fig. 2　The four states of BB84 protocol

$$\left.\begin{aligned}|\pi/4\rangle&=(\sqrt{2})^{-1}(|H\rangle+|V\rangle)\\|-\pi/4\rangle&=(\sqrt{2})^{-1}(|V\rangle-|H\rangle)\end{aligned}\right\} \tag{11}$$

$|V\rangle$，$|\pi/4\rangle$ 量子态代表数字 1，$|H\rangle$，$|-\pi/4\rangle$ 量子态代表数字 0. Alice 和 Bob 利用这四个量子态建立起由 0 和 1 码字组成的量子密钥串. 由于 $\{|H\rangle,|V\rangle\}$ 和 $\{|-\pi/4\rangle,|\pi/4\rangle\}$ 是两组相互共轭的量子态，由测不准原理，Eve 不可能知道 Alice 发送光子的具体极化态，故不知道光路中具体传输的是码字 1 还是 0. 但是码字 0 和 1 出现的概率相等. Eve 构造一组正交投影算符 $\rho_0=|0\rangle\langle 0|$，$\rho_1=|1\rangle\langle 1|$，量子态 $|0\rangle$ 和 $|1\rangle$ 为 Eve 的窃听基，用量子态 $|H\rangle$，$|V\rangle$ 表示为

$$\left.\begin{aligned}|0\rangle&=\cos\theta|H\rangle-\sin\theta|V\rangle\\|1\rangle&=\sin\theta|H\rangle+\cos\theta|V\rangle\end{aligned}\right\} \tag{12}$$

$|0\rangle$ 和 $|1\rangle$ 是沿 $-\theta$ 和 $(\pi/2-\theta)$ 方向的量子态. 现在的问题是寻找 θ 使得 Eve 获得的信息量最大，θ 满足关系式[6,9,10]

$$F(\theta)=1/4[|\langle H|\rho_0|H\rangle-\langle V|\rho_0|V\rangle|+|\langle H|\rho_1|H\rangle-\langle V|\rho_1|V\rangle|+|\langle\frac{\pi}{4}|\rho_0|\frac{\pi}{4}\rangle-\langle-\frac{\pi}{4}|\rho_0|-\frac{\pi}{4}\rangle|+|\langle\frac{\pi}{4}|\rho_1|\frac{\pi}{4}\rangle-\langle-\frac{\pi}{4}|\rho_1|-\frac{\pi}{4}\rangle|]=1/2(\cos 2\theta+\sin 2\theta) \tag{13}$$

我们可以求出，当 $\theta=\pi/8$ 时，Eve 对两组信号的窃听效率最高并且同为 $P=\cos^2\theta=\frac{1}{2}(1+\frac{1}{\sqrt{2}})$，也就是猜对码字的最大概率为 $P=0.8542$. 此时量子态 $|0\rangle$ 和 $|1\rangle$ 就是我们知道的 Breidbart 基[10]，其对应的码字分别为 0 和 1.

Eve 探测到的要么是量子态 $|0\rangle$ 要么是 $|1\rangle$，然后把测量结果 $|0\rangle$ 或 $|1\rangle$ 发给 Bob. 如果 Alice 发送 $|H\rangle$ 给 Bob，Eve 进行截获测量并且得到码字 0 的概率为 P，然后把 $|0\rangle$ 量子态发给 Bob，Bob 有可能以概率得到量子态 $|V\rangle$. 但是 Eve 也可能以 $1-P$ 的概率得到码字 1，然后就把量子态 $|1\rangle$ 发给 Bob，Bob 就会以 P 的概率测到量子态 $|V\rangle$，认为 Alice 发出的是量子态 $|V\rangle$，通过公共信道比较基，就会发现错误. 由以上分析可知 Eve 可能导致误码的概率由全概率公式可得

$$D=(1-P)\langle 0|\rho_H|0\rangle+P\langle 1|\rho_H|1\rangle \tag{14}$$

式中 $\rho_H=|H\rangle<H|$，从而可得到

$$D=2P(1-P) \tag{15}$$

当 $P=\frac{1}{2}(1+\frac{1}{\sqrt{2}})$ 时，猜对码字的概率最大，但此时造成的误码也最多 $D=\frac{1}{4}$.

如果 Alice 和 Bob 发现在筛选过的密钥中有 1/4 的误码，那么可以肯定 Eve 在窃听. Eve 为了隐蔽自己在窃听，就测量部分量子态，在这种情况下，Eve

猜对总量子态的概率为

$$P(\xi)=\frac{\xi}{2}\left(1+\frac{1}{\sqrt{2}}\right)+\frac{1-\xi}{2} \tag{16}$$

对没有测量的量子态有 1/2 的可能猜对．那么它可能导致的错误为 $D(\xi)=\xi/4$，代入式(16)得到 P 与 D 的函数关系式

$$P(D)=\sqrt{2}D+\frac{1}{2} \tag{17}$$

当 $D=1/4$ 最大时，$\xi=1$ 即对全部脉冲窃听．

3 基于实际系统的窃听方案

图 3 是 Eve 窃听装置图，由于 Alice 的光子源不是真正的单光子源，而是光子数服从泊松分布的弱激光脉冲．利用这一缺点，Eve 用一个耦合器耦合出部分光子并立刻对这部分光子测量．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利用截获重发策略．

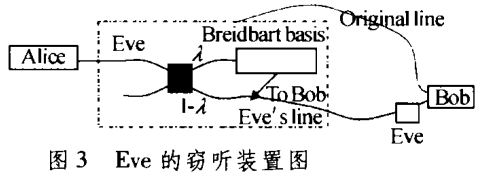


图 3 Eve 的窃听装置图

Fig. 3 Eve's set-up for Eavesdropping

经过分束耦合器后，通向Bob的非空脉冲为 $1-e^{-\mu(1-\lambda)}$，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 $1-e^{-\mu(1-\lambda)F_E}$，F_E 为 Eve 的光纤的传递效率．则脉冲传输系数为

$$\eta=\frac{1-e^{-\mu(1-\lambda)F_E}}{1-e^{-\mu(1-\lambda)}} \tag{18}$$

分两种情况来讨论：

1)耦合器耦合出部分光子，对应式(7)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 可能猜对每个码的概率为

$$P'\left(D=\frac{1}{4}\right)=\frac{\sqrt{2}+2}{4} \tag{19}$$

此时，Eve 猜对总码字的概率为

$$P_1^{\text{correct}}=\frac{\eta P_1 P'(D=1/4)}{1-e^{-\mu(1-\lambda)F_E}} \tag{20}$$

2) Eve 用分束器没有耦合到光子，对应式(8)的情况，测量部分通向 Bob 的脉冲，因为这种测量会在 Alice 和 Bob 的筛选密钥中造成误码，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 能观测到的误码率为

$$D=\frac{D(\xi)\eta P_2}{1-e^{-\mu(1-\lambda)F_E}} \tag{21}$$

在这种情况下，Eve 猜对总码字的概率为

$$P_2^{\text{correct}}=\frac{\eta P_2 P'[D(\xi)]}{1-e^{-\mu(1-\lambda)F_E}} \tag{22}$$

式中 $P'=\sqrt{2}D(\xi)+1/2$.

综合以上两种情况，Eve 猜对总码字的概率为

$$P_{\text{tot}}^{\text{correct}}=\frac{\eta P_1 P'(D=1/4)+\eta P_2 P'[D(\xi)]}{1-e^{-\mu(1-\lambda)F_E}}=\frac{P_1 P'(D=1/4)+P_2 P'[D(\xi)]}{1-e^{-\mu(1-\lambda)}} \tag{23}$$

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，我们使 $(1-\lambda)F_E=F_{AB}$．在此条件下，为了不引起 Alice 和 Bob 的怀疑，Eve 应尽可能的降低 Alice 与 Bob 的误码率．

由式(23)得

$$P_{\text{tot}}^{\text{correct}}=\frac{\sqrt{2}+2}{4}+\sqrt{2}e^{-\mu\left(\frac{F_E-F_{AB}}{F_E}\right)}\left[D(\xi)-\frac{1}{4}\right] \tag{24}$$

从式(21)可知，Alice 和 Bob 在筛选后的密钥中观察到的误码率为

$$D=D(\xi)e^{-\mu\left(\frac{F_E-F_{AB}}{F_E}\right)} \tag{25}$$

通过式(25)，Eve 可以控制误码率，并且通过测知光纤长度 L，由式(24)算出获得的正确的比特值．

4 Alice 和 Bob 的防范措施

若 Eve 获得的信息量小于 Alice 和 Bob 的互信息量，即 $I(A,B)\geqslant I(E)$，则 Alice 和 Bob 就可利用保密加强技术获得二者公用密钥[4]，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]

$$I(A,B)=1+D\log_2 D+(1-D)\log_2(1-D) \tag{26}$$

式中 D 是误码率，上式可写为[6]

$$I(A,B)=\frac{1}{2}\phi(1-2D) \tag{27}$$

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

$$I(E)=\frac{1}{2}\phi[1-2(1-P_{\text{tot}}^{\text{correct}})] \tag{28}$$

Alice和Bob要得到共享的密钥串，由限制条件 $I(A,B)\geqslant I(E)$ 与式(27)、(28)可得到

$$D<1-P_{\text{tot}}^{\text{correct}} \tag{29}$$

由上式与(25)式可得 Alice 和 Bob 所能接受的误码率上限为

$$D<\frac{2+\sqrt{2}\left[e^{-\mu\left(\frac{F_E-F_{AB}}{F_E}\right)}-1\right]}{4(1+\sqrt{2})} \tag{30}$$

由此可见，Alice 和 Bob 只有保证筛选后的密钥的误码率 D 小于 $\frac{2+\sqrt{2}\left[e^{-\mu\left(\frac{F_E-F_{AB}}{F_E}\right)}-1\right]}{4(1+\sqrt{2})}$ 二者才能利用保密加强技术获得公用密钥串．图 4 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.

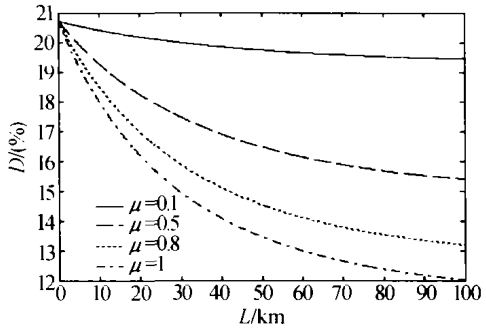


图 4　误码率与传输长度和平均光子数关系图

Fig. 4　Bit disturbance with transmission length and average photon

5　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并不是单光子，量子密钥分配的信道不是无损耗这些实际问题，采用分束窃听与截获重发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 只能获得部分信息保证密钥是绝对安全的.

参考文献

1　Bennett C, Brassard G. Quantum cryptography: Public-key distribution and coin tossing. In proceedings of the IEEE International Conference on Computers, *Systems and Signal Processing*, *Bangalore*, *India*, *New York*: *IEEE*, 1984. 175 ~ 179

2　Bennett C. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett*, 1992, **68**(21): 3121 ~ 3124

3　Ekert A. Quantum cryptography based on Bell's theorem. *Phys Rev Lett*, 1991, **67**(6): 661 ~ 663

4　Ekert A, Huttner B, Peres A, *et al*. Eavesddropping on quantum-cryptographical systems. *Phys Rev*(A), 1994, **50**(2): 1047 ~ 1056

5　Lütkenhaus N. Security against eavesdropping in quantum cryptography. *Phys Rev*(A), 1996, **54**(1): 97 ~ 111

6　Fuchs A, Gisin N, Peres A, *et al*. Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy. *Phys Rev*(A), 1997, **56**(2): 1163 ~ 1172

7　Félix s, Gisin N, Stefanov A, *et al*. Faint laser quantum key distribution: eavesdropping exploiting multiphoton pulses. *J Mod Optics*, 2001, **48**(13): 2009 ~ 2021

8　李福利. 高等激光物理学. 合肥：中国科学技术大学出版社, 1992. 304 ~ 308
Li F L. High Laser physics. Hefei: University of Science and Technology of China Press, 1992. 304 ~ 308

9　杨理，吴令安，刘颂豪. QKD 扩展 BB84 协议的 Breidbart 基窃听问题. 物理学报, 2002, **51**(5): 961 ~ 965
Yang L, Wu L A, Liu S H. *Acta Physics Sinica*, 2002, **51**(5): 961 ~ 965

10　Bennett C, Brassard G, Smolin J, *et al*. Experimental quantum cryptography. *J Crypto*, 1992, **5**(1): 3 ~ 28

11　周萌清. 信息论基础. 北京：北京航空航天大学出版社, 2002. 72 ~ 77
Zhou M Q. Information theory foundation. Beijing: Beihang University Press, 2002. 72 ~ 77

Eavesdropping of Practical QKD System Based on BB84 Protocol

Liu Jingfeng[1], Liang Ruisheng[1], Tang Zhilie[2], Wei Zhengjun[2], Chen Zhixin[2], Liao Changjun[1], Liu Songhao[1]

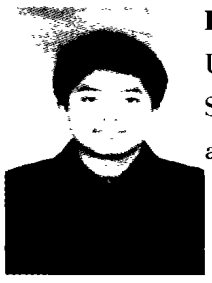
School for Information and Optoelectronics Science and Engineering, South China Normal University, Guangzhou 510631

Department of Physics, South China Normal University, Guangzhou 510631

Received date: 2003-09-26

Abstract　Practical implementations of quantum key distribution systems use attenuated laser pulses as the signal source rather than single photons. The channels used to transmit are lossy. On the basis of above two points, a combining eavesdropping strategy of intercept-resend and beamsplitting is discussed in terms of eavesdropper's technology requirement. At last, a maximum disturbance bound is derived for a given mean photon number and transmission length. Eavesdropper can be detected with the bound.

Keywords　Quantum key; BB84 protocol; Photon number statistics distributing; Eavesdropping strategy



Liu Jingfeng　was born in Aug. 1978, in Shandong Province. He studied in Liaocheng Normal University from 1997 to 2001 and received B. S. degree. Now he is studying for M. S. degree in South China Normal University. His research interests mainly include quantum key distribution and single-photon realization experiment.