实际量子密钥分配扩展 BB84 协议窃听下的安全性分析*

陈志新[1] 唐志列[1] 廖常俊[2] 刘颂豪[2]
(1 华南师范大学物理与电信工程学院，广州 510631)
(2 华南师范大学信息光电子科技学院，广州 510631)

摘 要 考虑强衰减激光脉冲技术实现的准单光子源和量子信道损耗以及窃听者 Eve 窃听能力有限等实际情况，提出了一种窃听装置；同时对扩展 BB84 协议的各种窃听做了全面分析，计算得出发送者 Alice/窃听者 Eve 所获得的交互信息量和发送者 Alice/接收者 Bob 所能容忍的误码率上限，以此作为检测量子信道安全性的标准，同时得出 Breidbart 基/分束攻击相结合的方法是比截取/重发更为有效的窃听方案.

关键词 量子密码；交互信息量；误码率
中图分类号 TN918 **文献标识码** A

0 引言

量子密钥分配(QKD)协议是利用单光子固有的量子随机性实现具有无条件安全性的密钥分配，已成为量子信息领域中特别具有现实意义的研究方向[1~9]. 但目前单光子量子保密通信实验使用的不是理想的单光子源，现有技术是使用强衰减的弱激光脉冲实现的，由于受到统计规律的限制不能保证每脉冲为单光子，所以实际 QKD 系统的安全性就受到严峻考验.

关于理想 QKD 系统的窃听问题已有论述[10~13]，目前国内对实际 QKD 系统的窃听问题还很少报道. 本文提出了一种窃听装置，同时对扩展 BB84 协议的各种窃听做了全面分析.

1 理想单光子 QKD 系统的窃听原理

截取/重发策略是适合理想单光子 QKD 系统的一种常用的窃听方式，基于理想 QKD 系统 Breidbert 基窃听的具体问题杨理已讨论过[13]，并求得 Breidbert 基窃听的最佳窃听效率为 $P=0.7887$，结论表明：B/B 窃听在截取/重发策略下 Eve 获得的信息量最大. 如果用 B/B 窃听的话，Eve 给量子信道引入的误码率为

$$D=2P(1-P)=\frac{1}{3} \tag{1}$$

如果 Eve 只是窃听全部光子态的一部分 ε，没有窃听的部分光子 $1-\varepsilon$ 可以有 $\frac{1}{2}$ 的概率猜测，此时窃听效率为

$$P(\varepsilon)=\varepsilon P+\frac{1-\varepsilon}{2}=\frac{\varepsilon}{2}\left(1+\frac{1}{\sqrt{3}}\right)+\frac{1-\varepsilon}{2} \tag{2}$$

Eve 给量子信道引入的误码率为

$$D(\varepsilon)=\frac{\varepsilon}{3} \tag{3}$$

结合式(1)～(3)，Eve 能获得的窃听效率为

$$P(D)=\frac{1}{2}+\frac{\sqrt{3}}{2}D \tag{4}$$

当 $\varepsilon=1$ 时 $D_{\max}=\frac{1}{3}$，即窃听全部光子.

2 弱光脉冲的分束原理

在单光子量子密码通信中，合法通信者实际使用的单光子源都是用强衰减方法得到的弱激光相干脉冲，而不是真正的单光子，且在相干脉冲出现 n 个光子的概率服从泊松分布[14]

$$P(n,\mu)=\frac{\mu^n}{n!}\mathrm{e}^{-\mu} \tag{5}$$

式中 μ 为每脉冲的平均光子数，$P(n,\mu)$ 为探测到每脉冲 n 个光子的概率.

同时考虑光纤的损耗，设光纤的传输效率是 η，那么通过量子信道 Bob 的探测器探测到每脉冲 n 个光子的概率是

$$P(n,\eta\mu)=\frac{(\eta\mu)^n}{n!}\mathrm{e}^{-\eta\mu} \tag{6}$$

所以经过有损耗的光纤后，光子数的概率分布仍然符合泊松分布，只仅仅是每脉冲光子数降低而已.

考虑弱激光脉冲经过分束器的光子数分布的特点，如图1. 假设Eve使用的分束器是一个无损器

*国家"973"计划资助项目(2001CB309300)和广州市重大科技攻关项目(1999-2-035-01)资助
Tel:010-62282303 Email:czx236@sohu.com
收稿日期:2004-10-19

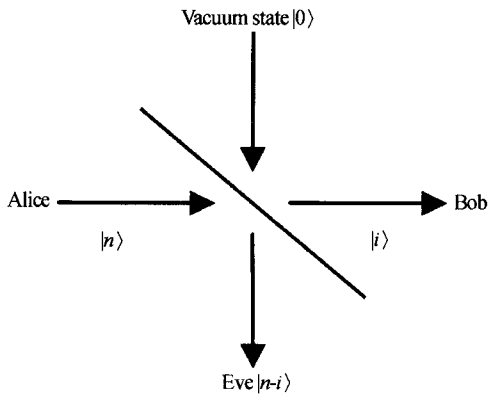


图 1　分束器窃听的原理图

Fig. 1　Schematic diagram of the eavesdropping of beamsplitter

件，Alice 发出服从泊松分布的光子态通过 Bob 处的传输效率为 t，通过 Eve 的传输效率是 r，且满足 $r+t=1$. 那么通过分束器后

$$\sum_{n=0}^{\infty}\sqrt{P_n}|n\rangle\otimes|0\rangle\rightarrow\sum_{n=0}^{\infty}\sqrt{P_n}\sum_{i=0}^{n}c_i|i\rangle\otimes|n-i\rangle \quad (7)$$

式中 c_i 为光子数分布权重，并且满足贝努利分布，即

$$c_i=C_n^i t^i r^{(n-i)}$$

由式(7)可知，通过 Bob 处出现每脉冲 i 个光子数的概率是

$$P(i)=|(\sum_{m=0}^{\infty}\langle i|\otimes\langle n-i|)(\sum_{n=0}^{\infty}\sqrt{P_n}\sum_{i=0}^{n}c_i|i\rangle\otimes|n-i\rangle)|^2=\sum_{n=0}^{\infty}P_n\sum_{i=0}^{n}|c_i|^2=\frac{(\mu t)^i}{i!}e^{-\mu t} \quad (8)$$

结合式(8)，同时经过分束器再经过光纤损耗到达 Bob 探测器后每脉冲光子数的分布可能出现下面四种情况[11]

1)保证每脉冲 Bob 和 Eve 都有光子输出，这时 Alice 就必须保证每脉冲两个光子以上的输入．经过光纤损耗后，出现的概率为

$$P_A=\sum_{n=2}^{\infty}P(n,\mu)\sum_{i=1}^{n-1}|c_i|_A^2=1+e^{-\mu}-e^{-\mu t}-e^{-\mu(1-t)} \quad (9)$$

2)每脉冲 Eve 获得 Alice 发出的全部光子输出，而 Bob 没有获得光子．此时出现的概率是

$$P_B=\sum_{n=1}^{\infty}P(n,\mu)|c_0|^2=e^{-\mu t}-e^{-\mu} \quad (10)$$

3)每脉冲 Eve 都有没有光子输出，而 Bob 获得全部光子．此时出现的概率是

$$P_c=\sum_{n=1}^{\infty}P(n,\mu)|c_n|^2=e^{-\mu(1-t)}-e^{-\mu} \quad (11)$$

4) Alice 发出的光子每脉冲中没有光子，此时出现的概率是

$$P_o=e^{-\mu} \quad (12)$$

结合式(6)、(8)，考虑实际 QKD 系统量子信道光纤损耗时，经过分束器后到达量子信道 Bob 处的探测器探测到每脉冲 n 个光子的概率就变成

$$P(n,\eta\mu t)=\frac{(\eta\mu t)^n}{n!}e^{-\eta\mu t} \quad (13)$$

由分析可知，用分束器窃听信息能够使 Bob 获得的光子数分布不仅服从泊松分布而且能够获得期望的光子数概率分布．

3　实际 QKD 中 Breidbart 窃听基/分束窃听的分析

由于 Alice 没有理想的单光子源，考虑到实际量子信道的传输损耗以及 Eve 的实际能力有限等问题，Eve 可以使用低损耗光纤代替 Alice/Bob 间的光纤并同时结合以下两种方式进行窃听，如图 2. 为计算方便，假设 Eve 和 Bob 的探测能力是相同的，把探测器的探测效率定为 1.

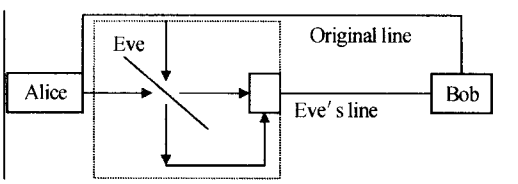


图 2　实际 QKD 系统中 Eve 的窃听装置原理图

Fig. 2　Schematic diagram of the eavesdropping of on practical quantum cryptography

1)在 Alice 旁用分束器窃听，如果 Eve 在每脉冲中能获得光子，则立即用 Breidbert 基窃听获得的这部分光子态，并且不会给合法通信双方引入误码，这时 Eve 的窃听效率是

$$P_{part1}^{correct}(D)=\frac{P_A P(D=\frac{1}{3})}{1-P_o-P_B} \quad (14)$$

2)如果 Eve 在每脉冲中没有获得任何光子，就可以用 Breidbert 基直接窃听以获取这部分的光子态，但会给合法通信双方引入误码．这时 Eve 的窃听效率是

$$P_{part2}^{correct}(D)=\frac{P_c P(D)}{1-P_o-P_B} \quad (15)$$

此时 Eve 窃听所有发出的光子态的窃听效率为

$$P_{total}^{correct}(D)=\frac{P_A P(D=\frac{1}{3})+P_c P(D)}{1-P_o-P_B}=\frac{3+\sqrt{3}}{6}+e^{-\mu(\frac{\eta_E-\eta_{AB}}{\eta_E})}[\frac{\sqrt{3}}{2}(D-\frac{1}{3})] \quad (16)$$

此时 Eve 引入的误码率为

$$D_{AB}(\varepsilon)=\frac{D(\varepsilon)P_c}{1-P_o-P_B}=D(\varepsilon)e^{-\mu(1-t)}=D(\varepsilon)e^{-\mu(\frac{\eta_E-\eta_{AB}}{\eta_E})} \quad (17)$$

计算中使用的是光纤通信中 1550 nm 波段标准通

信窗口，其光纤损耗为 0.2 dB/km，实际现有光纤损耗系数最小为[15]0.171 dB/km. 根据信息熵方程分别求出 Alice/Eve 的交互信息量为

$$I_{AE}=1+P(D)\log_2(P(D))+(1-P(D))\cdot\log_2(1-P(D)) \quad (18)$$

Alice/ Bob 的交互信息量为

$$I_{AB}=1+D_{AB}\log_2(D_{AB})+(1-D_{AB})\cdot\log_2(1-D_{AB}) \quad (19)$$

分别取分束比为50/50和10/90的分束器，即 $t=0.5$、$t=0.9$，当 $\mu=1$，结合式(3)、(4)、(16)～(19)，给出了传输距离与 I_{AB}，I_{AE}以及误码率 D_{AB}之间的关系，得到 Breidbart 基/分束攻击和 B/B 窃听两种不同窃听方式交互信息量和误码率之间的关系，如图 3、4.

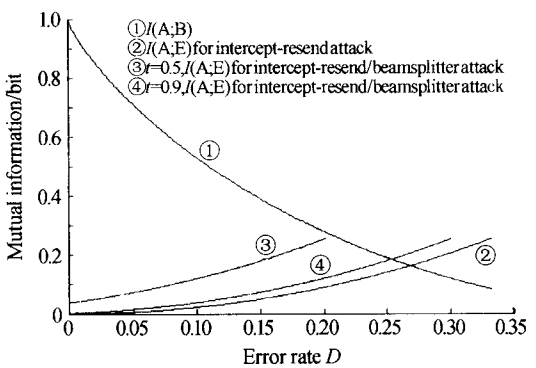


图 3 当 $t=0.5$ 和 $t=0.9$ 时交互信息量和误码率之间的关系图

Fig. 3 Schematic diagram of the relation between the mutual information and error rate with $t=0.5$ and $t=0.9$

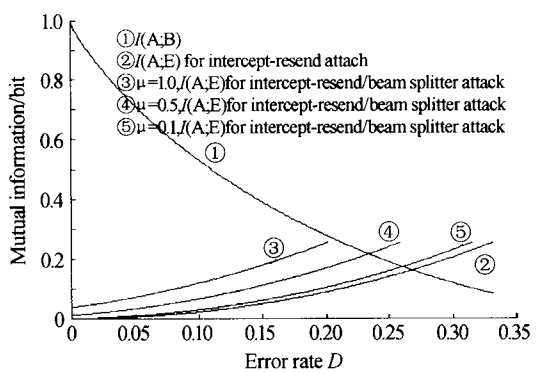


图 4 当 $t=0.5$ 时 $\mu=1$；$\mu=0.5$；$\mu=0.1$ 时交互信息量和误码率之间的关系图

Fig. 4 Schematic diagram of the relation between the mutual information and error rate with $t=0.5$ and $\mu=1$; $\mu=0.5$; $\mu=0.1$

结果表明：当 $\mu=0.1$ 或更小，即趋于理想单光子状态时，Breidbart 基/分束攻击和 B/B 窃听获得信息量是相同的；在误码率相同的情况下，Eve 用 Breidbart 基/分束攻击要比 B/B 窃听获得信息量要多，更有效.

实际的量子密码通信中，由于信道的损耗以及 Eve 窃听的介入，不可避免地给合法通信双方带来误码率，所以合法通信双方为了保证密码本的安全性，必须满足 $I(A;B)>I(A;E)=I(B;E)$，然后 Alice 和 Bob 通过保密加强的方法得到安全的密码本；这时，两种窃听方式给量子信道带来的误码率上限为

1) 对于截取/重发策略就可以得到

$$D<1-P(D)$$

即

$$D<2-\sqrt{3}$$

2) 对于 Breidbart 基/分束攻击相结合的策略可以得到

$$D_{AB}<1-P_{total}^{correct}$$

即

$$D_{AB}<\frac{9-5\sqrt{3}}{3}+\frac{2\sqrt{3}-3}{3}e^{-\mu\left(\frac{\eta_E-\eta_{AB}}{\eta_E}\right)}$$

所以当 Alice 和 Bob 双方的误码率达到这个上限时，双方就应该考虑窃听者的存在，密码本就应该放弃，然后重发. 还得出 Eve 用 Breidbart 基/分束攻击下获得的信息量随传输距离之间的关系，如图 5.

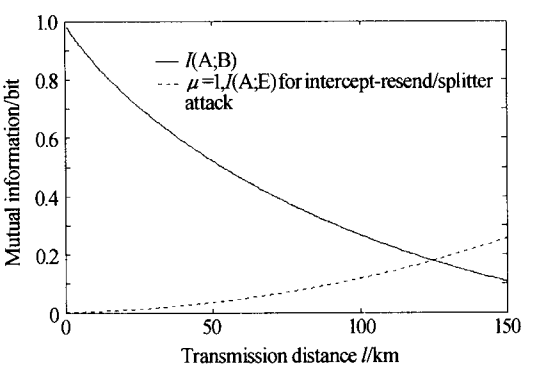


图 5 当 $\mu=1$ 时 Alice/Eve 的交互信息量和传输距离之间的关系图

Fig. 5 Schematic diagram of the relation between the mutual information and transmission distance in $\mu=1$

4 结论

在量子信道损耗和准单光子源的实际 QKD 系统下，提出了一种窃听装置，对扩展 BB84 协议采用 Breidbart 基/分束攻击相结合的方法，得出 Eve 可能获得的信息量和 Alice/Bob 所能容忍的误码率上限，同时得出了 Breidbart 基/分束攻击相结合的方法是比截取/重发策略和分束攻击更为有效的窃听方案，从而为合法通信者间的安全通信和对 Eve 的检测提供了判定的依据和标准.

参考文献

1 Wiesner S. Conjugate coding. *SIGACT News*, 1983, **15** (1): 78～88

2 Bennett C H, 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

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

4 Bennett C H, Bessette F, Brassard G, *et al*. Experimental quantum cryptography. *Journal of Cryptology*, 1992, **5**(1): 3～28

5 Brub D. Optimal eavesdropping in quantum cryptography with six states. *Phys Rev Lett*, 1998, **81**(14): 3018-3021

6 Philip H A, Bonfrate G, Buller G S, *et al*. Eighty kilometer transmission experiment using an InGaAs/InP SPAD-based quantum cryptography receiver operating at 1.55 μm. *Journal of Modern Optics*, 2001, **48**(13): 1957～1966

7 Buttler W T, Hughes R J, Lamoreaux S K, *et al*. Daylight quantum key distribution over 1. 6 km. *Phys Rev Lett*, 2000, **84**(34): 5652～5655

8 梁创，廖静，吴令安，等. 硅雪崩光电二极管单光子探测器. 光子学报，2000，**29**(12)：1139～1143
Liang C, Liao J, Wu L A, *et al*. *Acta Photonica Sinica*, 2000, **29**(12): 1139～1143

9 陈志新，唐志列，刘颂豪，等. QKD 系统在 Breidbart 基窃听下 BB84 协议的信息量研究. 光子学报，2004，**33**(12)：1469～1472
Chen Z X, Tang Z L, Liu S H, *et al*. *Acta Photonica Sinica*, 2004, **33**(12): 1469～1472

10 Huttner B, Ekert A K. Information gain in quantum eavesdropping. *Journal of modern Optics*, 1994, **41**(12): 2455～2466

11 Félix s, Gisin N, Stefanov A, *et al*. Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses. *Journal of Modern Optics*, 2001, **48**(13): 2009～2021

12 Williamson M, Vedral V. Eavesdropping on practical quantum cryptography. *Journal of Modern Optics*, 2003, **50**(13): 1989～2011

13 杨理，吴令安，刘颂豪，等. 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, *et al*. *Acta Physica Sinica*, 2002, **51**(5): 961～965

14 李福利. 高等激光物理学. 合肥：中国科学技术大学出版社，1992. 285～327
Li F L. Higher Laser Physics. HeFei: University of Science and Technology of China Press, 1992. 285～327

15 Kato T, Hirano M, Onishi M, *et al*. Ultra-low nonlinearity low-loss pure silica core fiber for long-haul WDM transmission. *Electron Lett*, 1999, **35**(19): 1615～1617

Practical Security Problem of Six States QKD Protocol

Chen Zhixin[1], Tang Zhilie[1], Liao Changjun[2], Liu Songhao[2]

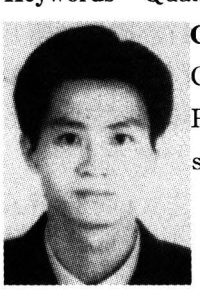
1 *Department of physics, South China Normal University, Guangzhou* 510631

2 *School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510631

Received date: 2004-10-19

Abstract It is used attenuated laser pulses as the signal source rather than single photons in practical QKD system. The channels is used to transmit are lossy. Eve′s eavesdropping ability is limited. On the basis of above three points, a eavesdropping device is presented. Meanwhile, the study is analyzed the calculation of the effective average Alice/Eve mutual information and Alice/Bob error rate′s upper limit in six states QKD protocol. It shows that Breidbart eavesdropping/beamsplitter is the more effective one compared with Breidbart eavesdropping (B/B strategy).

Keywords Quantum cryptography; Mutual information; Error rate



Chen Zhixin was born in JiangXi Province. He received the M. S. Degree from South China Normal University in 2004. Now he is studying for PH. D. in Beijing University of Posts and Telecommunications. His research interests include quantum cryptography, All-speed optical communication system and Broad-Band access network.