QKD 系统在 Breidbart 基窃听下 BB84 协议的信息量研究*

陈志新[1] 唐志列[1] 魏正军[1] 刘景锋[1] 廖常俊[2] 刘颂豪[2]

（1 华南师范大学物理系，广州 510631）

（2 华南师范大学信息光电子科技学院，广州 510631）

摘 要 给出了 BB84 协议的 Breidbart 基窃听的方案，分析并计算了各种截取/重发策略下施行 QKD 标准纠错手续后 Alice/Eve 的有效平均交互信息量和对 Bob 引起的错误率．结果显示了 Breidbart 基窃听/Breidbart 基重发策略（B/B 策略）最为有效，并提出了各种窃听方案下 Alice 和 Bob 采取相应的反攻击策略．

关键词 量子密码；Breidbart 基窃听；有效平均交互信息量

中图分类号 TN918 **文献标识码** A

0 引言

量子密钥分配（QKD）协议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，是目前量子信息领域中特别具有现实意义的研究方向[1~12]．1984 年 Bennett C. H 和 Brassard G 首先提出的 BB84 协议[2]是 QKD 的典型协议．关于 QKD 协议的安全性问题有一个必须解决的是 Eve 不透明窃听的策略问题．文献[4]依据两种窃听方式各自的 Alice\Eve 平均交互信息量 I^{AE} 的大小判断，正则基窃听优于 Breidbart 基窃听；文献[11]进一步考虑了纠错过程对 Alice\Eve 间的平均交互信息量的影响，得到 QKD 标准纠错手续中 Breidbart 基窃听更为有效的结论．本文主要对 BB84 协议的 Breidbart 基窃听做了全面的分析，得出了各种 Breidbart 基窃听的方案及具体的物理操作过程和各种窃听策略的效率，同时比较了 Alice\Eve 策略在 Bob 处引起的错误率，计算了经标准纠错手续公开纠错后各策略所能达到的有效平均交互信息量和各种窃听方式下对 Alice\Eve 间的平均交互信息量的影响，结论得出了在 Breidbart 基窃听下的安全性问题，同时也进一步验证了文献[4]、[13]的结论，同时还提出了各种窃听方案下 Alice 和 Bob 相应的反窃听策略．

1 BB84 协议中的 Breidbart 基窃听原理分析

在 BB84 协议中采用的两两共轭基是一组圆偏振基和一组线偏振基．为了计算方便，我们采用两两共轭的两组线偏振基，合法通信者 Alice 和 Bob 分别随机选择光子的任何两组共轭测量基的偏振态（这里取偏振方向为 0°和 90°，45°和 135°的两组线偏振态，并定义 0°和 45°代表量子比特‘0’，90°和 45°代表量子比特‘1’），并且 Alice 随机发射和 Bob 随机测量．下面来考虑一下 BB84 协议中的 Breidbart 基窃听方案问题，本文 Eve 采用 Breidbart 基为沿 θ 方向和 $\theta+\frac{\pi}{2}$ 方向的一组线偏振基来窃听，如图 1 所示．即

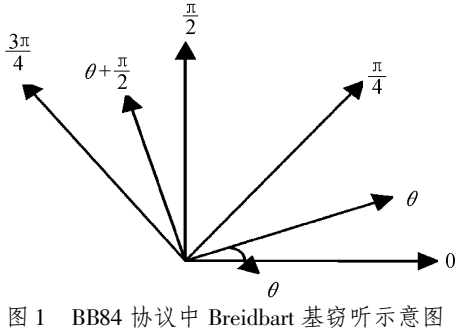

图 1 BB84 协议中 Breidbart 基窃听示意图

Fig. 1 Schematic diagram of the the Breidbart eavesdropping in BB84 protocol

$$e_0^\theta=\begin{pmatrix}\cos\theta\\ \sin\theta\end{pmatrix}\quad e_1^\theta=\begin{pmatrix}-\sin\theta\\ \cos\theta\end{pmatrix}\tag{1}$$

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix}=A_1^\theta e_0^\theta+B_1^\theta e_1^\theta\tag{2}$$

$$|\frac{\pi}{4}\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}=A_2^\theta e_0^\theta+B_2^\theta e_1^\theta\tag{3}$$

$$|\frac{\pi}{2}\rangle=\begin{pmatrix}0\\1\end{pmatrix}=A_3^\theta e_0^\theta+B_3^\theta e_1^\theta\tag{4}$$

$$|\frac{3\pi}{4}\rangle=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}=A_4^\theta e_0^\theta+B_4^\theta e_1^\theta\tag{5}$$

得到

*国家“973”计划（2001CB309300）及广州市重大科技攻关 1999-2-035-01 资助项目

Tel：010-62284290 Email：czx236@sohu.com

收稿日期：2003-09-28

$$A_1^{\theta}=\cos\theta \tag{6}$$

$$B_1^{\theta}=-\sin\theta \tag{7}$$

$$A_2^{\theta}=\frac{1}{\sqrt{2}}(\sin\theta+\cos\theta) \tag{8}$$

$$B_2^{\theta}=\frac{1}{\sqrt{2}}(\cos\theta-\sin\theta) \tag{9}$$

$$A_3^{\theta}=\sin\theta \tag{10}$$

$$B_3^{\theta}=\cos\theta \tag{11}$$

$$A_4^{\theta}=\frac{1}{\sqrt{2}}(-\sin\theta+\cos\theta) \tag{12}$$

$$B_4^{\theta}=\frac{1}{\sqrt{2}}(-\cos\theta-\sin\theta) \tag{13}$$

可得

$$|A_2^{\theta}|^2=|B_4^{\theta}|^2=\frac{1}{2}(1+\sin 2\theta) \tag{14}$$

$$|B_2^{\theta}|^2=|A_2^{\theta}|^2=\frac{1}{2}(1-\sin 2\theta) \tag{15}$$

$$|A_1^{\theta}|^2=|B_3^{\theta}|^2=\cos^2\theta \tag{16}$$

$$|B_1^{\theta}|^2=|A_3^{\theta}|^2=\sin^2\theta \tag{17}$$

为求 Breidbart 基窃听的最佳窃听角度，我们定义一个函数 $F(\theta)=\sum_{i=1}^{4}||A_i^{\theta}|^2-|B_i^{\theta}|^2|$，并求出函数极值点对应的最佳窃听角度 θ，这等价于求函数

$$F(\theta)=2|\sin 2\theta|+2|\cos 2\theta|=2\sin 2\theta+2\cos 2\theta\quad(\frac{\pi}{4}\geqslant\theta\geqslant 0) \tag{18}$$

的极值点，由 $\frac{\mathrm{d}F}{\mathrm{d}\theta}|_{\theta=\theta_m}=0$ 得 $\tan 2\theta_m=1$，因此得 $F(\theta)$ 的极值点为

$$\theta_m=\pi/8 \tag{19}$$

也即 $\theta_m=\pi/8$ 为 Breidbart 基窃听的最佳窃听角度.

此时

$$|A_1^{\theta_m}|^2=|A_2^{\theta_m}|^2=\frac{1}{2}(1+\frac{1}{\sqrt{2}}) \tag{20}$$

$$|B_1^{\theta_m}|^2=|B_2^{\theta_m}|^2=\frac{1}{2}(1-\frac{1}{\sqrt{2}}) \tag{21}$$

由于 $|e_0^{\theta_m}\rangle$，$|e_1^{\theta_m}\rangle$ 为 Breidbart 窃听基，两组基上信号的窃听效率都为

$$\eta^{\theta_m}=|A_1^{\theta_m}|^2=|A_2^{\theta_m}|^2=0.8536 \tag{22}$$

2 Breidbart 基窃听策略下的全面分析

下面称以 Breidbart 基为窃听基的窃听为 B 窃听，而以协议本身所使用的正则基（Protocol 基）为窃听基的窃听为 P 窃听. 由于 Alice 和 Bob 在公开讨论时要设法排除双方的不一致比特，因此窃听效果应是以 Alice 和 Bob 纠错之后 Eve 与 Alice 之间的平均交互信息量（本文称之为有效平均交互信息量）来衡量. 计算表明当减除错误比特之后，P 窃听和 B 窃听的地位发生了逆转，即从有效信息量角度来衡量，B 窃听效率更高. 下面就 BB84 协议来讨论这个问题.

在 BB84 协议中 P 基窃听中 Eve 选基正确的概率是 1/2，此部分对平均交互信息量 $\tilde{I}_{\mathrm{P}}^{\mathrm{AE}}$ 的贡献是 1/2，由于协议中选择的是两组基相互共轭，Eve 选基错误的 1/2 比特的正确率为 50%，但对交互信息量没有贡献，所以 Alice 和 Eve 的平均交互信息量为

$$\tilde{I}_{\mathrm{P}}^{\mathrm{AE}}=1/2 \tag{23}$$

由式（22）可知，B 基窃听时 Alice\Eve 的平均交互信息量为

$$\tilde{I}_{\mathrm{B}}^{\mathrm{AE}}=1+\eta^{\theta_m}\log_2\eta^{\theta_m}+(1-\eta^{\theta_m})\log_2(1-\eta^{\theta_m})=0.3991 \tag{24}$$

由于 $\tilde{I}_{\mathrm{P}}^{\mathrm{AE}}>\tilde{I}_{\mathrm{B}}^{\mathrm{AE}}$，从平均交互信息量来看 P 窃听更为有效[4].

下面我们主要考虑的是在不同 Breidbart 基窃听下经过纠错手续后在 Bob 处引起的错误率及计算出 Alice\Eve 的有效平均交互信息量，并进行了详细的比较分析.

2.1 P 基窃听/P 基重发

Eve 选基准确时不会在 Bob 处引起附加的错误率，而 Eve 选基错误时有 1/2 的概率引起 Bob 的错误，故 Eve 将引起 Bob 处的错误率为 1/4. Alice 和 Bob 公开纠错之后 Eve 手中正确比特仍为 1/2，这部分对有效信息量的贡献为 1/2. Eve 选基错误的比特的正确率仍为 50%，但对交互信息量没有贡献，由此得

$$|\tilde{I}_{\mathrm{P/P}}^{\mathrm{AE}}|_{\text{有效}}=\frac{50\%}{75\%}=\frac{2}{3} \tag{25}$$

2.2 B 基窃听/P 基重发

由式（22）知对于 B 基窃听有 $\eta^{\theta_m}=0.8536$. P 基重发时，Eve 选对基的概率为 1/2；在概率为 1/2 的选错基情形中有 1/2 不会在 Bob 处引起错误结果，因此 Eve 会在 Bob 处引起 $\frac{3}{4}-\frac{1}{2}\eta^{\theta_m}=33\%$ 的错误. Eve 最终得到的正确比特数为 $\frac{3}{4}\eta^{\theta_m}$，最后到 Eve 手中的比特总数为 $\frac{1}{4}+\frac{1}{2}\eta^{\theta_m}$，最终 Eve 手中的比特准确率为

$$|\eta_{\mathrm{B/P}}^{\theta_m}|_{\text{有效}}=\frac{\frac{3}{4}\eta^{\theta_m}}{(\frac{1}{4}+\frac{1}{2}\eta^{\theta_m})}=0.9459 \tag{26}$$

相应的有效平均交互信息量为

$$|\tilde{I}^{AE}_{B/P}|_{有效}=0.6964 \tag{27}$$

2.3 B 基窃听/B 基重发

B 基重发时，当 Eve 以$|e_0^{\theta_m}\rangle$，$|e_1^{\theta_m}\rangle$为重发基时，即

$$|e_0^{\theta_m}\rangle=A_1^{\theta_m}|0\rangle-B_1^{\theta_m}|\frac{\pi}{2}\rangle \tag{28}$$

$$|e_1^{\theta_m}\rangle=B_1^{\theta_m}|0\rangle+A_1^{\theta_m}|\frac{\pi}{2}\rangle \tag{29}$$

$$|e_0^{\theta_m}\rangle=A_1^{\theta_m}|\frac{\pi}{4}\rangle+B_1^{\theta_m}|\frac{3\pi}{4}\rangle \tag{30}$$

$$|e_1^{\theta_m}\rangle=B_1^{\theta_m}|\frac{\pi}{4}\rangle-A_1^{\theta_m}|\frac{3\pi}{4}\rangle \tag{31}$$

无论 Alice 发送信号时选择的是哪组基时，Eve 手中的准确比特都是以概率 $\eta_B^{\theta_m}$ 在 Bob 处测量为正确. 因此 Eve 手中同时为 Alice 和 Bob 共享，即在 Bob 处无错误的比特概率为$(\eta^{\theta_m})^2/2=0.7286$，在 Bob 处引起的错误率为

$$2\eta^{\theta_m}(1-\eta^{\theta_m})=1/4 \tag{32}$$

所以减少错误比特后 Eve 手中的正确率为

$$|\eta^{\theta_m}_{B/B}|_{有效}=\frac{[(\eta^{\theta_m})^2/2]}{[1-2\eta^{\theta_m}(1-\eta^{\theta_m})]}=0.9715 \tag{33}$$

于是在 Alice\Bob 公开纠错后 Alice\Eve 之间的有效平均交互信息量为

$$|\tilde{I}^{AE}_{B/B}|_{有效}=0.8130 \tag{34}$$

通过比较 P 基窃听/P 基重发和 B 基窃听/B 基重发的对 Bob 引起的错误率都是 1/4，当 Alice 和 Bob 在公共信道核对密码本同时采取奇偶校验的纠错方法进行防窃听时，如果信道的误码率达到或超过 1/4 时，就可能考虑 Eve 的存在并放弃原密码本重新建立新密码本. 同时由式(25)、(27)、(34)可知，$|\tilde{I}^{AE}_{B/B}|_{有效}>|\tilde{I}^{AE}_{B/P}|_{有效}>|\tilde{I}^{AE}_{P/P}|$有效，因此可知 BB84 协议中，B 窃听/B 重发比 P 窃听/P 重发和 B 窃听/P 重发的策略更有效. 但需要指出的是：即使 $|\tilde{I}^{AE}_{B/B}|_{有效}>|\tilde{I}^{AE}_{B/P}|_{有效}>|\tilde{I}^{AE}_{P/P}|_{有效}$，也不能说 B/B 策略肯定优于其他策略，原因是 B/B 策略窃听时由于 Eve 的 B 基测量使 Bob 处的各组基完全等价，Bob 用错误基检测时仍有与选用正确基检测时相同的准确率，所以 Alice 和 Bob 可以通过废弃的数据对比检测到，所以 Alice 和 Bob 在生成量子密钥时不仅要核对 Bob 选基正确的比特，而且还要核对 Bob 选基错误的比特，即在 BB84 协议的公共信道讨论时增加核对 Bob 选基错误率的这一步，才可以防止截取/重发中最有效的 B/B 策略，因为 Eve 只要发现 Alice 和 Bob 在公共信道公开讨论中不核对 Bob 选基错误的比特时，B/B 窃听最为有效的. 从 Alice 和 Bob 的角度来讲，只有核对 Bob 选基错误的比特以排除 Eve 的 B/B 攻击，才能依据 Bob 的接收错误率来更确切地判断 Eve 所获得的信息量，从而准确地确定安全性加强算法的强度，以保证密钥安全性.

3 结论

本文全面分析了 BB84 协议中的各种 Breidbart 基窃听策略，计算出 Eve 可能获得的最大信息量，结果表明 B\B 策略时可获得最大交互信息量，同时在各种窃听方案下对 Alice 和 Bob 提出了相应的反攻击策略，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. 当然本文的结论是有前提的，即 Alice 和 Bob 必须使用类似于文献[4]给出的比较子集奇偶性的 QKD 标准纠错手续. 在这里我们只是分析了一种常用的窃听方式，如果采用不同的方法 Eve 可能获得的信息量也会不同的[14]，这都有待我们进一步的研究. 本文只限于考虑理想 QKD 系统，忽略考虑了随机发生源的随机性、量子信道的噪声和损耗以及单光子探测器的量子效率、暗记数，环境因素等问题的影响，但可以为实际的QKD系统的数据分析提供有效的理论依据.

参考文献

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

2 Bennett C H, Brassard G, *et al*. Quantum cryptography: Public-key distribution and coin tossing, Inproceedings of the IEEE International Conference on Computers, Systems and SignalProcessing , Bangalore, India, 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 Bennett C H. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett*, 1992, **68**(21): 3121 ~ 3123

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

7 Liang C, Fu D H, Liang B, *et al*. Quantum key distribution over 1.1 km in an 850 nm experimental all-fiber system. *Acta Physica Sinica*, 2001, **50**(8): 1429 ~ 1433

8 Hughes R J, Morgan G L, Peterson C G, *et al*. Quantum key distribution over a 48 km optical fibre network. *J Mod Opt*, 2000, **47**(2/3): 533 ~ 547

9 Philip A H, 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

10 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

11 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

12 刘景锋, 梁瑞生, 刘颂豪, 等. 量子保密通信用的光精密控制强衰减技术. 光子学报, 2004, **33**(7): 867 ~ 870
Liu J F, Liang R S, Liu S H, *et al*. *Acta Photonica Sinica*, 2004, **33**(7): 867 ~ 870

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

14 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

On the Breidbart Eavesdropping Information Problem of BB84 QKD Protocol

Chen Zhixin[1], Tang Zhilie[1], Wei Zhengjun[1], Liu Jingfeng[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: 2003-09-28

Abstract The Breidbart eavesdropping scheme of BB84 QKD protocol discussed. Calculation of the effective average Alice/Eve mutual information after performing a standard error correction under various intercept/resend strategies shows that Breidbart eavesdropping/Breidbart(B/B strategy) is the most effective one. Since Alice and Bob can test openly whether there is the B/B eavesdropping by making use of the rejected data and advise Alice and Bob's various corresponding anti-eavesdropping scheme.

Keywords Quantum cryptography; Breidbart eavesdropping; Effective average mutual information

Chen Zhixin was born in Jiangxi Province. He graduated from Department of Physics of Jinggangshan Normal College. Now he is studying as a graduate student majoring in Quantum cryptographic communication and optics information, in South China Normal University.