第 51 卷 第 5 期 2002 年 5 月
1000-3290/2002/51(05)/0961-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.51,No.5,May,2002

QKD 扩展 BB84 协议的 Breidbart 基窃听问题*

杨 理[1)] 吴令安[2)] 刘颂豪[3)]

[1)] (中国科学院研究生院信息安全国家重点实验室,北京 100039)

[2)] (中国科学院物理研究所,北京 100080)

[3)] (华南师范大学量子电子学研究所,广州 510631)

(2001 年 7 月 26 日收到;2001 年 10 月 17 日收到修改稿)

给出了六态扩展 BB84 协议的 Breidbart 基窃听方案,分析并计算了各种截取/重发策略下的 Alice/Eve 平均交互信息量和施行 QKD 标准纠错手续后的有效平均交互信息量,结果显示 Breidbart 基窃听/Breidbart 基重发策略(B/B 策略)最为有效.考虑到 Alice 和 Bob 可以在公开讨论阶段利用废弃数据检验是否存在 B/B 窃听以降低秘密性增强算法的强度,减少量子密钥的损失,提出了修改 BB84 协议的建议.给出了可能较 QKD 标准纠错手续更为安全的量子密钥二次生成纠错方法.

关键词:量子密码,BB84 协议,Breidbart 基窃听

PACC:0365,4230,4250

1. 引 言

量子密钥分配(QKD)[1—6] 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.1984 年提出的 BB84 协议[2] 是 QKD 的典型协议.由于 BB84 协议利用光子偏振态的两组共轭基生成量子密钥,窃听者 Eve 有 50% 的机会选择正确的基进行探测.其实,描述光子偏振态的共轭基共有三组[7,8],一种最自然的选择是选取两组共轭的线偏振基和一组圆偏振基.这一选择对应于选取 Poincaré 球上南北两极点和赤道上的两条互相垂直的直径所对应的态.采用这三组基的 BB84 协议称为扩展 BB84 协议(或六态协议)[7,8].

关于 QKD 协议的一个需要定量研究的问题是 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[9]进一步考虑了纠错过程对 Alice 和 Eve 间平均交互信息量的影响,得出就 QKD 标准纠错手续[4,10] 而言 Breidbart 基窃听更为有效的结论.文献[4]和[9]讨论的是四态协议的 Breidbart 基窃听问题,本文考虑六态协议的 Breidbart 基窃听方案.第 2 节给出了六态协议的 Breidbart 窃听方案,包括具体的物理操作手续,计算了各种窃听策略的效率.第 3 节分析比较了各种 Alice/Eve 策略在 Bob 处引起的错误率,计算了经标准纠错手续[1,10] 公开纠错后各策略所能达到的有效平均交互信息量.本文结论是:1)Breidbart 基窃听攻击下六态协议较四态协议更安全;2)文献[4,10]中比较子集奇偶性的纠错方法不利于 QKD 的安全性,本文提出了借助于经典纠错码的量子密钥二次生成纠错方法;3)Breidbart 基窃听/Breidbart 基重发是 Alice/Eve 有效平均交互信息量最高的截取/重发窃听策略,但这种窃听是能够被 Alice 和 Bob 利用废弃数据检测到的;4)这种反攻击方法的存在导致我们提出对标准 BB84 协议的一个小的修改,这种修改在完全不降低协议有效性的前提下能够防止 Eve 采取截取/重发攻击中最有效的 B/B 策略.应该说明的是,有必要采用这一修改的前提是 Alice 和 Bob 使用标准纠错手续[4,10].采用其他纠错方法时哪一种截取/重发窃听策略最为有效目前还不清楚,所以这时是否需要修改 BB84 协议也还不清楚.

* 中国科学院(信息安全国家重点实验室)知识创新工程项目,广州市科技攻关计划项目和中国博士后科学基金资助的课题.

2. 扩展 BB84(六态)方案的 Breidbart 基窃听

描述光子极化状态的两两共轭的基至多可选取三组.如一组圆偏振基和两组相互共轭的线偏振基.下面考虑三组共轭基为 $\{|H\rangle, |V\rangle\}$, $\{|L\rangle, |R\rangle\}$和$\left\{|\frac{\pi}{4}\rangle, |\frac{3\pi}{4}\rangle\right\}$的六态扩展 BB84 协议的 Breidbart 窃听问题.假设 Eve 截获光子后令其通过一个装置,使$|H\rangle$分量的相位较$|V\rangle$分量的相位超前$\frac{\pi}{4}$,则 $\{|L\rangle, |R\rangle\}$和 $\{|\frac{\pi}{4}\rangle, |\frac{3\pi}{4}\rangle\}$在变换后同时成为长轴在$\frac{\pi}{4}$方向和$\frac{3\pi}{4}$方向的椭圆偏振光,而 $\{|H\rangle, |V\rangle\}$在变换后仍为原方向的线偏振光.因此,本文试取 Eve 用于窃听的 Breidbart 基为沿 θ 方向和$\frac{\pi}{2}+\theta$ 方向的一组线偏振基,表为

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

此时有

$$\left|\frac{\pi}{4}\right\rangle' = \frac{1}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\pi}{4}}\\ 1\end{pmatrix} = A_1^\theta e^0 + B_1^\theta e^1, \tag{2a}$$

$$\left|\frac{3\pi}{4}\right\rangle' = \frac{1}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\pi}{4}}\\ 1\end{pmatrix} = A_2^\theta e^0 + B_2^\theta e^1, \tag{2b}$$

$$|L\rangle' = \frac{1}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\pi}{4}}\\ i\end{pmatrix} = A_3^\theta e^0 + B_3^\theta e^1, \tag{2c}$$

$$|R\rangle' = \frac{1}{\sqrt{2}}\begin{pmatrix}e^{i\frac{\pi}{4}}\\ -i\end{pmatrix} = A_4^\theta e^0 + B_4^\theta e^1, \tag{2d}$$

其中

$$A_1^\theta = \frac{1}{\sqrt{2}}(\sin\theta + e^{i\frac{\pi}{4}}\cos\theta), \tag{3a}$$

$$B_1^\theta = \frac{1}{\sqrt{2}}(\cos\theta - e^{i\frac{\pi}{4}}\sin\theta), \tag{3b}$$

$$A_2^\theta = \frac{1}{\sqrt{2}}(-\sin\theta + e^{i\frac{\pi}{4}}\cos\theta), \tag{3c}$$

$$B_2^\theta = \frac{1}{\sqrt{2}}(-\cos\theta - e^{i\frac{\pi}{4}}\sin\theta), \tag{3d}$$

$$A_3^\theta = \frac{1}{\sqrt{2}}(i\sin\theta + e^{i\frac{\pi}{4}}\cos\theta), \tag{3e}$$

$$B_3^\theta = \frac{1}{\sqrt{2}}(i\cos\theta - e^{i\frac{\pi}{4}}\sin\theta), \tag{3f}$$

$$A_4^\theta = \frac{1}{\sqrt{2}}(-i\sin\theta + e^{i\frac{\pi}{4}}\cos\theta), \tag{3g}$$

$$B_4^\theta = \frac{1}{\sqrt{2}}(-i\cos\theta - e^{i\frac{\pi}{4}}\sin\theta). \tag{3h}$$

可得

$$|A_1^\theta|^2 = \frac{1}{2}\left(1 + \frac{1}{\sqrt{2}}\sin 2\theta\right), \tag{4a}$$

$$|B_1^\theta|^2 = \frac{1}{2}\left(1 - \frac{1}{\sqrt{2}}\sin 2\theta\right), \tag{4b}$$

及

$$|A_2^\theta|^2 = |A_4^\theta|^2 = |B_3^\theta|^2 = |B_1^\theta|^2, \tag{5a}$$

$$|B_2^\theta|^2 = |B_4^\theta|^2 = |A_3^\theta|^2 = |A_1^\theta|^2, \tag{5b}$$

而

$$|H\rangle' = e^{i\frac{\pi}{4}}\begin{pmatrix}1\\ 0\end{pmatrix} = A_H e^0 + B_H e^1, \tag{6a}$$

$$|V\rangle' = \begin{pmatrix}1\\ 0\end{pmatrix} = A_V e^0 + B_V e^1. \tag{6b}$$

其中

$$A_H^\theta = \cos\theta e^{i\frac{\pi}{4}},\ B_H^\theta = -\sin\theta e^{i\frac{\pi}{4}}, \tag{7a}$$

$$A_V^\theta = \sin\theta,\ B_V^\theta = \cos\theta. \tag{7b}$$

因而

$$|A_H^\theta|^2 = \cos^2\theta,\ |B_H^\theta|^2 = \sin^2\theta, \tag{8a}$$

$$|A_V^\theta|^2 = \sin^2\theta,\ |B_V^\theta|^2 = \cos^2\theta. \tag{8b}$$

现在的问题是寻找角度 θ 使得 $\sum_i \big||A_i^\theta|^2 - |B_i^\theta|^2\big|$最大,这等价于求函数

$$F(\theta) = 4\big||A_1^\theta|^2 - |B_1^\theta|^2\big| + 2\big||A_H^\theta|^2 - |B_H^\theta|^2\big| \tag{9}$$

的极值点和极大值.将前述有关各式代入上式,有

$$F(\theta) = 2\sqrt{2}\,|\sin 2\theta| + 2|\cos 2\theta| = 2(\sqrt{2}\sin 2\theta + \cos 2\theta), \tag{10}$$

去掉上式中的绝对值符号是因为 $0 < \theta < \frac{\pi}{4}$. 由 $\left.\frac{dF}{d\theta}\right|_{\theta=\theta_m} = 0$ 得 $\mathrm{tg}2\theta_m = \sqrt{2}$,因此得 $F(\theta)$极值点为

$$\theta_m = \frac{1}{2}\mathrm{arctg}\sqrt{2}, \tag{11}$$

$F(\theta)$极大值为

$$F(\theta_m) = 2\left(\frac{2}{\sqrt{3}} + \frac{1}{\sqrt{3}}\right) = 2\sqrt{3}. \tag{12}$$

此时

$$|A_{1^m}^{\theta_m}|^2 = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right),$$

$$|B_1^{\theta_m}|^2 = \frac{1}{2}\left(1 - \frac{1}{\sqrt{3}}\right), \quad (13a)$$

$$|A_H^{\theta_m}|^2 = |A_1^{\theta_m}|^2, \ |B_H^{\theta_m}|^2 = |B_1^{\theta_m}|^2 \quad (13b)$$

知$\{|e_0^{\theta_m}\rangle, |e_1^{\theta_m}\rangle\}$为 Breidbart 窃听基，三组基上信号的窃听效率同为

$$\eta_B^{\theta_m} = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right) = \frac{3+\sqrt{3}}{6} = 0.7887. \quad (14)$$

3. 各窃听策略的有效平均交互信息量

下面称以 Breidbart 基为窃听基的窃听为 Breidbart 窃听(B 窃听)，而以协议本身所使用的正则基为窃听基的窃听为 Protocol 窃听(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．具体计算表明，由于交互信息量与窃听效率之间的非线性关系，当减除错误比特之后，P 窃听和 B 窃听的地位发生了逆转．即从有效交互信息量角度来衡量，B 窃听效率更高．下面就六态方案来讨论这一问题．

在六态方案的 P 基窃听中 Eve 选基正确的概率为$\frac{1}{3}$，此部分对平均交互信息量 $\tilde{I}_{\mathrm{P}}^{\mathrm{AE}}$ 的贡献为$\frac{1}{3}$．由于方案中选择的三组基相互共轭，Eve 选基错误的$\frac{2}{3}$比特的正确率为 50%，因此对交互信息量没有贡献．Alice 与 Eve 的平均交互信息量为

$$\tilde{I}_{\mathrm{B}}^{\mathrm{AE}} = \frac{1}{3}. \quad (15)$$

由(14)式知，B 基窃听时 Eve 与 Alice 的平均交互信息量为

$$\tilde{I}_{\mathrm{P}}^{\mathrm{AE}} = 1 + \eta_{\mathrm{B}}^{\theta_m}\log_2\eta_{\mathrm{B}}^{\theta_m} + (1-\eta_{\mathrm{B}}^{\theta_m})\log_2(1-\eta_{\mathrm{B}}^{\theta_m}).$$
$$= 0.2560, \quad (16)$$

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

下面考虑不同窃听策略在 Bob 处引起的错误率及 Alice/Eve 有效平均交互信息量．

1) P 基窃听/P 基重发．Eve 选基正确时不在 Bob 处引起附加的错误，而 Eve 选基错误时有$\frac{1}{2}$情形引起 Bob 的错误，故 Eve 将引起 Bob 处$\frac{1}{3}$的错误率．由于此时 Eve 手中确知正确的比特的集合与 Bob 的错误比特集合不相交，Alice 和 Bob 公开纠错之后 Eve 手中的确知正确比特仍占$\frac{1}{3}$，这部分对有效平均交互信息量的贡献为$\frac{3}{2}\times\frac{1}{3} = \frac{1}{2}$．Eve 选基错误的比特的正确率仍为 50%，因此对交互信息量没有贡献．由此得

$$(\tilde{I}_{\mathrm{P}}^{\mathrm{AE}})_{\text{有效}} = \frac{1}{2}. \quad (17)$$

2) B 基窃听，P 基重发．由(14)式知对于 B 基窃听有 $\eta_{\mathrm{B}}^{\theta_m} = 0.7887$．P 基重发时，Eve 选对基的概率为$\frac{1}{3}$，在概率为$\frac{2}{3}$的选错基情形中有$\frac{1}{2}$不会在 Bob 处产生错误结果，因此知 Eve 会在 Bob 处引起$\frac{1}{3}(1-\eta_{\mathrm{B}}^{\theta_m})+\frac{1}{3}$的错误，Eve 最终得到的比特的正确率为$\frac{2}{3}\eta_{\mathrm{B}}^{\theta_m}$．考虑到 Eve 手中比特总数剩下$\frac{1}{3}(1+\eta_{\mathrm{B}}^{\theta_m})$，因此 Eve 手中比特最终的正确率为

$$(\eta_{\mathrm{B/P}}^{\theta_m})_{\text{有效}} = \frac{\frac{2}{3}\eta_{\mathrm{B}}^{\theta_m}}{\frac{1}{3}(1+\eta_{\mathrm{B}}^{\theta_m})} = \frac{2\eta_{\mathrm{B}}^{\theta_m}}{1+\eta_{\mathrm{B}}^{\theta_m}}$$
$$= 0.8819. \quad (18)$$

相应的有效平均交互信息量为

$$(\tilde{I}_{\mathrm{B/P}}^{\mathrm{AE}})_{\text{有效}} = 0.4547. \quad (19)$$

3) B 基窃听/B 基重发．

B 基重发时，取重发基为将$|\mathrm{H}\rangle$分量相位超前$\frac{\pi}{4}$后的$\left\{|\theta_m\rangle, |\frac{\pi}{2}+\theta_m\rangle\right\}$，即

$$|\theta_m\rangle' = \begin{pmatrix}\cos\theta_m e^{i\frac{\pi}{4}}\\ \sin\theta_m\end{pmatrix} \quad (20a)$$

和

$$\left|\theta_m+\frac{\pi}{2}\right\rangle' = \begin{pmatrix}-\sin\theta_m e^{i\frac{\pi}{4}}\\ \cos\theta_m\end{pmatrix}. \quad (20b)$$

此时有

$$|\theta_m\rangle' = A_1^{\theta_m}\left|\frac{\pi}{4}\right\rangle + A_2^{\theta_m}\left|\frac{3\pi}{4}\right\rangle, \quad (21a)$$

$$\left|\theta_m+\frac{\pi}{2}\right\rangle' = B_1^{\theta_m}\left|\frac{\pi}{4}\right\rangle + B_2^{\theta_m}\left|\frac{3\pi}{4}\right\rangle, \quad (21b)$$

$$|\theta_m\rangle' = A_4^{\theta_m}|L\rangle + A_3^{\theta_m}|R\rangle, \quad (21c)$$

$$\left|\theta_m+\frac{\pi}{2}\right\rangle'=B_4^{\theta_m}\mid L\rangle+B_3^{\theta_m}\mid R\rangle,\quad(21\mathrm{d})$$

$$\mid\theta_m\rangle'=A_H^{\theta_m}\mid H\rangle+A_V^{\theta_m}\mid V\rangle,\quad(21\mathrm{e})$$

$$\left|\theta_m+\frac{\pi}{2}\right\rangle'=B_H^{\theta_m}\mid H\rangle+B_V^{\theta_m}\mid V\rangle.\quad(21\mathrm{f})$$

由(3),(11)和(20)式可知,当 Eve 以 $\left\{\mid\theta_m\rangle',\left|\theta_m+\frac{\pi}{2}\right\rangle'\right\}$ 为重发基时,无论 Alice 发送信号时选择的是哪一组基,Eve 手中的正确比特都是以概率 $\eta_{\mathrm{B}}^{\theta_m}$ 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 $(\eta_{\mathrm{B}}^{\theta_m})^2=\frac{2+\sqrt{3}}{6}$,在 Bob 处引起错误的概率为

$$2\eta_{\mathrm{B}}^{\theta_m}(1-\eta_{\mathrm{B}}^{\theta_m})=\frac{1}{2}\sin^2 2\theta_m=\frac{1}{3},$$

与 P 基窃听相同.所以减除错误比特后 Eve 手中比特的正确率为

$$(\eta_{\mathrm{B/B}}^{\theta_m})_{\text{有效}}=\frac{(\eta_{\mathrm{B}}^{\theta_m})^2}{1-\frac{1}{2}\sin^2 2\theta_m}=\frac{3}{2}(\eta_{\mathrm{B}}^{\theta_m})^2=\frac{2+\sqrt{3}}{4}.\quad(22)$$

于是得到在 Alice 和 Bob 公开纠错后 Alice 和 Eve 之间的有效平均交互信息量为

$$(\tilde{I}_{\mathrm{B/B}}^{\mathrm{AE}})_{\text{有效}}=0.6454.\quad(23)$$

由(17)和(23)式可知,$(\tilde{I}_{\mathrm{B/B}}^{\mathrm{AE}})_{\text{有效}}>(\tilde{I}_{\mathrm{P}}^{\mathrm{AE}})_{\text{有效}}$,因此可知对于扩展 BB84(六态)方案,B 基窃听/B 基重发策略较 P 基窃听/P 基重发策略有效.由(17)和(19)式可知,P 基窃听/P 基重发策略较 B 基窃听/P 基重发策略有效.

4. 结论与讨论

本文给出了扩展 BB84 协议的 Breidbart 基窃听策略.与文献[9]相同,我们强调了公开纠错后的 Alice/Eve 平均交互信息量的重要性.本文计算了各种策略下的 $(I_{\mathrm{B/B}}^{\mathrm{AE}})_{\text{有效}}$,结果显示 Eve 采用 B/B 策略时可获得最大的信息量.不过我们发现,即使 $(I_{\mathrm{B/B}}^{\mathrm{AE}})_{\text{有效}}>(I_{\mathrm{P}}^{\mathrm{AE}})_{\text{有效}}$,也不能说 B/B 策略优于 P/P 策略,原因是可以看出 B/B 窃听是 Alice 和 Bob 能够利用废弃数据检测到的: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 66.7%的正确率,而不是不存在 Eve 的 B 基测量时的 50%.如果 Alice 和 Bob 在生成量子密钥时不是仅仅核对 Bob 选基正确的比特,而且还核对 Bob 选基错误的比特,即在 BB84 协议的公开讨论部分增加核对 Bob 选基错误比特的错误率这一步,则可以防止截取/重发窃听中最有效的 B/B 策略,这是因为 Eve 可以监听 Alice 和 Bob 的公开讨论,只有当她发现公开讨论中不核对 Bob 选基错误的比特,才可以采取最为有效的 B/B 攻击。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 的接收错误率更确切地判断 Eve 所可能得到的信息量,从而正确地确定秘密性加强算法的强度,在保证密钥安全性的同时,尽量减小密钥生成效率的降低.

应该指出的是无论对于四态协议还是对于六态协议,这一结论的成立是有条件的,即 Alice 和 Bob 必须使用类似于文献[4,10]给出的比较子集奇偶性的 QKD 标准纠错手续.我们考虑如果不采用这种方法而是采用下述方法,结论可能会很不相同.

量子密钥的二次生成纠错方法:Alice 选择一随机序列作为新的密钥序列,用经典纠错码将其编码后用手中刚生成的有错误密钥对其加密,然后发送给 Bob;Bob 用手中有错误的密钥解密,解密后的序列与 Alice 加密前的序列略有不同.显然,只要该纠错编码足以对抗 Alice 和 Bob 手中量子密钥的不一致,Bob 译码后获得的新密钥序列必与 Alice 手中的新密钥序列一致.由于 Eve 手中正确密钥比特数远远少于 Bob 手中的正确密钥比特数(因为 Eve 只能少量窃听,不然 Alice 和 Bob 会由于 Bob 接收错误率过高而放弃数据),因此无法正确解开纠错编码下面的新密钥序列,估计 $(I_{\mathrm{P,B}}^{\mathrm{AE}})_{\text{有效}}$ 将有所降低.当然,用上述方法纠错后仍须照常对所得序列进行秘密性加强处理.从采用比较子集奇偶性的公开纠错方法后 Eve 手中所剩密钥比特的正确率(四态:97.15%,六态:93.30%)来看,该纠错方法很不利于 QKD 的安全性,因此我们认为有必要对上述量子密钥二次生成纠错方法进行进一步的分析.显然,如果能够证明上述量子密钥二次生成纠错方法或其他纠错方法能使 $(I_{\mathrm{B/B}}^{\mathrm{AE}})_{\text{有效}}$ 小于 $(I_{\mathrm{P}}^{\mathrm{AE}})_{\text{有效}}$,则 BB84 协议不必修改.

本文结果表明,六态协议较四态协议更为安全.这与文献[7,8,12]中关于六态协议在相干和非相干攻击下较四态协议更安全的结论一致.从 Poincaré 球上可以看出,六态协议除前面给出的 Breidbart 基窃听方式外,还有一种 Breidbart 基窃听方式,即随机

选取 Poincaré 球的三条直径：$\pm\left(\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}},0\right)$，$\pm\left(0,\frac{1}{\sqrt{2}},\frac{1}{\sqrt{2}}\right)$和$\pm\left(\frac{1}{\sqrt{2}},0,\frac{1}{\sqrt{2}}\right)$之一为窃听基的窃听方式.此时 $\tilde{I}_{B}^{AE}=0.2666$，略高于以$\pm\left(\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}},\frac{1}{\sqrt{3}}\right)$为窃听基的方案.公开纠错后$(\tilde{I}_{B'}^{AE})_{有效}=0.542$，低于前面讨论的情形.此种窃听方式仍然可以通过核对 Bob 选基错误比特来发现.

本文只限于考虑理想 QKD 方案，忽略了光子源的随机性、量子信道的噪声和损耗以及单光子探测器的量子效率和暗计数等问题.当考虑这些因素时，分束攻击将是对系统安全的一个有力的威胁[4,11].

[1] Wiesner S 1983 *Sigact News* **15** 78

[2] Bennett C H and Brassard 1984 *Proceedings of the IEEE International Conference on Computer, Systems, and Signal Processing, Bargalore, India* (New York: IEEE) pp 175 – 179

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

[4] Bennett C H *et al* 1992 *J. Cryptology* **5** 3

[5] Ekirt A E 1991 *Phys. Rev. Lett.* **67** 661

[6] Liang C *et al* 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁　创等 2001 物理学报 **50** 1429]

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

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

[9] Huttner B and Ekirt A 1994 *J. Mod. Opt.* **41** 2455

[10] Brassard G and Salvail L 1993 *Eurocrypt '93*, Lofthus, Norway

[11] Ekirt A, Huttner B, Palma G M and Peres A 1994 *Phys. Rev.* A **50** 1047

[12] Hwang W Y, Ahn D and Hwang S W Preprint quant-ph/0009006

On the Breidbart eavesdropping problem of the extended BB84 QKD protocol*

Yang Li[1)]　Wu Ling-An[2)]　Liu Song-Hao[3)]

[1)] (*State Key Laboratory of Information Security, Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)

[2)] (*Institute of Physics, Chinese Academy of Sciences, Beijing* 100080, *China*)

[3)] (*Institute of Quantum Electronics, Huanan Normal University, Guangzhou* 510631, *China*)

(Received 26 July 2001; revised manuscript received 17 October 2001)

Abstract

We discuss the Breidbart eavesdropping scheme of the extended BB84 quantum key distribution protocol. Calculation of the effective average Alice/Eve mutual information after performing a standard error-correction under various intercept/resend strategies shows that the Breidbart eavesdropping/Breidbart resend strategy (B/B strategy) is the most effective one. Sine Alice and Bob can test openly whether there is the B/B eavesdropping by making use of the rejected data, we suggest an amendment of the BB84 protocol to reduce the requirements of the privacy amplification algorithm and hence reduce the quantum key loss. Finally, we present a quantum key regeneration method for error-correction which may be more secure than the standard error-correction process.

Keywords: quantum cryptography, BB84 protocol, Breidbart eavesdropping

PACC: 0365, 4230, 4250

* Project supported by the Knowledge Innovation Program of the Chinese Academy of Sciences, and the Science Foundation for Post Doctorate of China.