第 51 卷 第 11 期 2002 年 11 月
1000-3290/2002/51(11)/2446-06

物 理 学 报
ACTA PHYSICA SINICA

Vol.51,No.11,November,2002
©2002 Chin. Phys. Soc.

复合量子密钥分发系统双速协议及其安全性分析*

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)

(2002 年 3 月 11 日收到；2002 年 4 月 27 日收到修改稿)

基于真空光速 c 是极限信号速度这一基本假设，提出了复合量子密钥分发(QKD)系统和双速协议，并证明双速协议的安全性与原 BB84 协议的安全性相同.结果表明，双速协议在将量子密钥生成效率从 50% 提高到 100% 的同时，还降低了窃听者 Eve 可能得到的信息量.双速协议由于打破了公开讨论之前 Bob 和 Eve 的对等地位，使 QKD 在概念上有了明显的改进，使协议基的选择空间有了本质性的扩充.具体给出了三个双速协议的实例，并详细分析了它们在截取/重发攻击下的安全性.

关键词：量子密码，光纤量子密钥分发，双速协议

PACC：0365，4230，4250

1. 引 言

量子密钥分发(QKD)安全性[1—3]的基础是量子随机性和关于未知量子态的不可克隆定理[4,5].在 BB84 协议中，当 Eve 不知道 Alice 选取的是哪一组基时，她无法准确地测量 Alice 所发送的光子的极化状态.在四态协议中[6]，Eve 选择正确测量基的概率是 1/2 在六态扩展协议中[7—10]，Eve 选择正确测量基的概率只有 1/3.Eve 不能正确选择测量基使她无法准确判断 Alice 所发送的光子的极化状态，因而她补发给 Bob 的光子会以 1/4 的概率在 Bob 处引起可察觉的错误[11].这一结果保证了 Alice 和 Bob 之间所生成的密钥序列的安全性.显然，在 BB84 协议中，在与 Alice 公开讨论之前，Bob 与 Eve 的地位相同.由于 Bob 不能在测量前知道 Alice 选定的发送基是哪一组，她的测量效率也只能是 1/2(四态)或 1/3(六态).正是由于这个原因，BB84 类协议不适合自由地选取更多的基以提高系统的安全性.为此，本文基于真空光速 c 是极限信号速度这一基本假设，提出光纤 QKD 双速协议.协议的安全性与传统的 BB84 协议安全性等价，而安全密钥的生成效率则高于扩展 BB84 协议三倍以上.尤其是这一协议使 QKD 在概念上发生了明显的变化，Bob 与 Eve 的地位在 Alice 和 Bob 公开讨论之前就已经完全不同，这使得 Alice 和 Bob 可以随意选定发送和测量的基，而 Eve 却完全无法有效利用这一信息.这为设计更有效、安全的 QKD 系统提供了可能.本文具体给出三个非共轭多组基协议的例子，并分析了它们的密钥生成效率和安全性.

2. 双速 BB84 协议

光纤 QKD 系统是目前看来较有实用意义的 QKD 系统.由于光纤中光信号的传递速度只有 2/3 倍光速，本文提出下述双速 QKD(BB84)协议：

1. Alice 选择一组协议基，这组基的全部基矢量构成信号光子的容许态集合.在 $t=0$ 时刻 Alice 随机选择处于某一容许态的光子发送给 Bob；

2. Alice 在 $t=\tau$ 时刻公开宣布此光子处于哪一组基上，此经典信息以光速 c 沿公开信道传向 Bob.当经典信道为直线时，延时 τ 须满足

$$\tau = \frac{1}{c}[n_g(l + l_b) - d], \qquad (1)$$

其中 c 为真空光速，n_g 为光纤纤芯的群速度折射率，l 为从 Alice 到 Bob 安全区边缘的光纤长度，l_b 为 Bob 在安全区内预留的光纤长度，d 为 Alice 到

* 中国科学院知识创新工程项目、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.

Bob 的距离;

3. Bob 接收到 Alice 的经典信息后,选择正确的测量基,测量 Alice 所发送的光子的极化状态;

4. Bob 公布检测到了哪些光子;

5. Bob 公布部分测量结果,Alice 据此判断 Eve 是否存在;

6. Alice 和 Bob 将剩余的比特作为原始密钥.

3. 双速协议的安全性

显然,只须证明 Eve 的在线测量不能利用 Alice 公开发布的经典信息,就可知此协议的安全性与传统 BB84 协议的安全性相同.

以 Alice 所处位置为坐标原点,Alice 到 Bob 的方向为 x 轴方向,可知不论 Alice 和 Bob 之间的光纤链路怎样弯曲,量子信号 S_q 的速度(v_g)在 x 轴正向的投影始终小于 v_g,因而小于 c.当 Alice 的经典信号 S_c 发出后,其在 x 轴上的投影 x_c 以光速 c 前进(假设经典信道是直的),因此在整个传输过程中 S_c 都是在追赶 S_q.由(1)式可知,只有当 S_q 进入 Bob 的安全区后,S_c 才能追上 S_q,所以在 Bob 的安全区之外,S_c 始终落后于 S_q,因而只要光纤传输线是坐标 x 的单值函数,就始终有 $x_c < x_q$,其中 x_q 是量子信号在 x 轴上的投影.因此可知 Eve 若要利用 S_c 测量 S_q,就必须滞留 S_q,直到 S_c 到达.另一方面,Eve 若要使自己的窃听不被察觉,又必须在测量之后补发 S_q,而且使 Bob 能在原定时刻接收到它.可是,已知以光速 c 沿直线传向 Bob 的 S_c 要到 Bob 的安全区之内才能追赶上 S_q,即 S_q 到达 Bob 安全区边缘的时刻要早于 S_c.显然,Eve 无论如何也不能在利用 S_c 进行测量之后又能使补发的 S_q 比 S_c 更早进入 Bob 的安全区使 S_q 和 S_c 在 Bob 处有正确的时间差,所以用经典信道发送延时为 τ 的信号 S_c 是安全的,双速协议的安全性与原 BB84 协议相同.(1)式只适用于经典信道为直线的情形.当经典信道弯曲时,只需增大 l_b,满足 $\Delta l_b = \frac{1}{3}\Delta d$,其中 Δd 是经典信道由于弯曲而增加的长度,即可保证系统的安全性.如果计及大气中的光速略小于狭义相对论的极限信号速度,也可通过略微加长 l_b,以确保系统的安全性.

4. 双速协议中协议基的选取

双速协议可以采用原 BB84 协议的两组基,也可以采用扩展 BB84 协议的三组基,原则上这一协议对基的选取没有限制.这里'没有限制'的意义是:1)基的数目不受严格的限制,多选几组基不会降低密钥生成效率;2)基与基之间的关系不受限制,不必要求不同基之间相互共轭.因此可以认为双速协议为 QKD 协议的设计提供了充分的自由.

采用 BB84 协议的两组基时,双速协议的密钥生成效率是原 BB84 协议的两倍;采用扩展 BB84 协议的三组基时,双速协议效率是原扩展 BB84 协议效率的三倍.在上述两种情形下,Eve 可能得到的平均信息量仍然分别是 1/2 和 1/3.表面看来,只要增加协议采用的相互共轭基的数目,就可以在不降低密钥生成效率的同时有效地降低 Eve 的窃听效率.遗憾的是,描述光子极化状态的两两共轭的基最多只能有三组.下面给出这一证明.

首先来看两组正交基相互共轭的条件.不失一般性,设两组正交基分别为

$$\{e_0^1, e_1^1\} = \left\{\begin{pmatrix}\cos\theta_1\\ \sin\theta_1 e^{i\phi_1}\end{pmatrix}, \begin{pmatrix}\sin\theta_1\\ -\cos\theta_1 e^{i\phi_1}\end{pmatrix}\right\}, \quad (2a)$$

$$\{e_0^2, e_1^2\} = \left\{\begin{pmatrix}\cos\theta_2\\ \sin\theta_2 e^{i\phi_2}\end{pmatrix}, \begin{pmatrix}\sin\theta_2\\ -\cos\theta_2 e^{i\phi_2}\end{pmatrix}\right\}. \quad (2b)$$

设第一组基用第二组基表示为

$$e_0^1 = A_1 e_0^2 + B_1 e_1^2, \quad (3a)$$

$$e_1^1 = A_2 e_0^2 + B_2 e_1^2. \quad (3b)$$

由(2)和(3)式可得

$$A_1 = \cos\theta_1\cos\theta_2 + \sin\theta_1\sin\theta_2 e^{i(\phi_1-\phi_2)}, \quad (4a)$$

$$B_1 = \cos\theta_1\sin\theta_2 - \sin\theta_1\cos\theta_2 e^{i(\phi_1-\phi_2)} \quad (4b)$$

和

$$A_2 = \sin\theta_1\cos\theta_2 - \cos\theta_1\sin\theta_2 e^{i(\phi_1-\phi_2)}, \quad (4c)$$

$$B_2 = \sin\theta_1\sin\theta_2 + \cos\theta_1\cos\theta_2 e^{i(\phi_1-\phi_2)}. \quad (4d)$$

两组基共轭的含义是 $|A_1|^2 = |B_1|^2$, $|A_2|^2 = |B_2|^2$,由此可得两组基共轭条件为

$$\mathrm{tg}2\theta_1\,\mathrm{tg}2\theta_2 = -\sec(\phi_1 - \phi_2). \quad (5)$$

现在用反证法证明不能有三组以上的基两两共轭.设有四组基两两共轭,则由(5)式有

$$\mathrm{tg}2\theta_i\,\mathrm{tg}2\theta_j = -\sec(\phi_i - \phi_j), \quad 1 \leqslant i < j \leqslant 4. \quad (6)$$

记 $\mathrm{tg}2\theta_i = t_i$, $\cos(\phi_i - \phi_j) = -c_{ij}$,由(6)式可得

$$\frac{C_{23}}{C_{34}C_{24}} = t_4^2 = \frac{C_{13}}{C_{14}C_{34}}, \tag{7a}$$

$$\frac{C_{12}}{C_{13}C_{23}} = t_3^2 = \frac{C_{24}}{C_{23}C_{14}}, \tag{7b}$$

$$\frac{C_{13}}{C_{12}C_{23}} = t_2^2 = \frac{C_{14}}{C_{12}C_{24}}, \tag{7c}$$

$$\frac{C_{34}}{C_{13}C_{14}} = t_1^2 = \frac{C_{23}}{C_{12}C_{13}}. \tag{7d}$$

由上述诸式可得

$$C_{23}C_{14} = C_{13}C_{24}, \tag{8a}$$

$$C_{13}C_{24} = C_{12}C_{34}. \tag{8b}$$

由(8a)式有

$$\cos(\phi_1 + \phi_3 - \phi_2 - \phi_4) = \cos(\phi_2 + \phi_3 - \phi_1 - \phi_4),$$

从而有

$$\sin(\phi_3 - \phi_4)\sin(\phi_1 - \phi_2) = 0. \tag{9a}$$

由(8b)式有

$$\cos(\phi_3 + \phi_4 - \phi_1 - \phi_2) = \cos(\phi_2 + \phi_4 - \phi_1 - \phi_3),$$

从而有

$$\sin(\phi_4 - \phi_1)\sin(\phi_3 - \phi_2) = 0. \tag{9b}$$

由(9a)和(9b)式知 ϕ_1,ϕ_2,ϕ_3 和 ϕ_4 中至少有三个相等或相差 π 的整数倍.由于我们证论的前提是 ϕ_i 各不相同,相差 π 的偶数倍没有意义,因此只能是三个角度两两相差 π 的奇数倍.由于三个角度两两相差 π 的奇数倍不可能,所以知上述论证的前提不能成立,即不可能有四组基两两共轭.

一种更直观的证明是:在 Poincaré 球上可推出共轭条件(5)式将导致 $s_1 s_1' + s_2 s_2' + s_3 s_3' = 0$,即相互共轭的两组基所对应的两条直径相互垂直.由于在三维空间中最多只能有三条直径两两垂直,可知最多只能选出三组基相互共轭.

根据上述论证可知,如果协议基限于取共轭的正交基,则双速协议以选取扩展 BB84 协议的三组共轭基为优.下面讨论本协议更具特色的情形:协议基不完全是共轭基的情形.

5. 不定基协议

由于双速协议在增加协议基数目时不会降低密钥生成效率,现在首先考虑一种极端的情形.假设 Alice 和 Bob 事先并不约定协议基是什么,Alice 随机选取 Poincaré 球面上一点 S 发送给 Bob,并在延时 τ 之后用经典信道公布 S 所在直径.由于 Bob 是依据经典信号 S_c 进行测量,因此能准确知道 Alice 发送的是 S 还是 $-S$.Eve 与 Bob 完全不同.由于 Alice 的 S 点是随机选取的,所以 Eve 的窃听策略无论怎样其平均效果都相当于随便选取一条不动的直径进行测量.假定她选的是$(\pm 1,0,0)$,则 Alice 发送的光子的极化状态 S 在 Eve 选定的测量基上可一般性地表达为$(\cos\theta, \sin\theta e^{i\phi})$,Eve 判断正确的概率为 $\cos^2\theta$,这里限定 $0 < \theta < \pi/4$,这是因为 Eve 可以在收到 S_c 之后再判断自己的测量结果是倾向于 S,还是倾向于 $-S$.从 Poincaré 球上看就是 Eve 可以认定自己的测量基直径与 Alice 的发送基直径夹角小于 $\pi/2$.

下面考虑在 Poincaré 球面上均匀取基时 Alice/Eve 的交互信息量.为利用通常选取的描述光子极化的球坐标[12]

$$s_1 = s_0\cos2\chi\cos2\psi, \tag{10a}$$

$$s_2 = s_0\cos2\chi\sin2\psi, \tag{10b}$$

$$s_3 = s_0\sin2\chi, \tag{10c}$$

其中 s_0 为光场强度,χ 为椭圆率,ψ 为椭圆取向角,可以不失一般性地考虑光子极化态在基 $\{|L\rangle, |R\rangle\}$ 上的分解.这在表面上是假定 Eve 取 $\{|L\rangle, |R\rangle\}$ 为固定窃听基,但由于积分遍及整个球面,结果与窃听基选取无关,积分值反映的是 Alice 在 Poincaré 球面上随机选取发送基而 Eve 在 Poincaré 球面上随机选取窃听基时 Alice/Eve 的平均交互信息量.一般的发送态$(\cos\theta, \sin\theta e^{i\phi})$在 $\{|L\rangle, |R\rangle\}$ 上的分解为

$$\begin{pmatrix}\cos\theta \\ \sin\theta e^{i\phi}\end{pmatrix} = A\frac{1}{\sqrt{2}}\begin{pmatrix}1 \\ i\end{pmatrix} + B\frac{1}{\sqrt{2}}\begin{pmatrix}1 \\ -i\end{pmatrix}, \tag{11}$$

其中

$$A = \frac{1}{\sqrt{2}}\left(\cos\theta + \sin\theta\exp\left[i\left(\phi - \frac{\pi}{2}\right)\right]\right), \tag{12a}$$

$$B = \frac{1}{\sqrt{2}}\left(\cos\theta - \sin\theta\exp\left[i\left(\phi - \frac{\pi}{2}\right)\right]\right), \tag{12b}$$

可得

$$|A|^2 = \frac{1}{2}(1 + \sin2\theta\sin\phi). \tag{13}$$

不失一般性,取 $s_0 = 1$,则有[12]

$$s_3 = 2a_1a_2\sin\delta = \sin2\theta\sin\phi. \tag{14}$$

由(10c)和(13)式可得

$$|A|^2 = \frac{1}{2}(1 + \sin2\chi), \tag{15}$$

故知 Eve 的窃听效率为

$$\eta_\Sigma = \frac{1}{2}(1 + \sin2\chi). \tag{16}$$

Alice/Eve 的平均交互信息量为

$$I_{\Sigma}^{\mathrm{AE}} = 1 + \frac{1}{2\pi}\int_0^{\pi/2} \mathrm{d}(2\psi) \int_0^{\pi/2} \mathrm{d}(2\chi)\left(\eta_{\Sigma}\log_2\eta_{\Sigma} + (1-\eta_{\Sigma})\log_2(1-\eta_{\Sigma})\right)\cos 2\chi, \quad (17)$$

积分后得

$$I_{\Sigma}^{\mathrm{AE}} = 1 - \frac{1}{2}\log_2 e = 0.2787. \quad (18)$$

由此知 Alice 在 Poincaré 球面上随机选基将使 Eve 获得较扩展 BB84 协议更小的信息量，即采用这种选基方式的双速协议较扩展 BB84 协议更安全. 因此可知双速协议可以比扩展 BB84 协议更安全.

6. 四组基协议

本节考虑一个具体的四组基双速协议. 取协议的四组基为 Poincaré 球面的内接立方体的四条对角线所对应的四条直径. 由于这四条直径互相并不垂直，这是一个协议基为非共轭基的双速协议. 这一协议的 P 基窃听，即以四条对角线之一为窃听基的窃听，对于其他三条对角线上的态有相同的窃听效率：

$$\eta_{\mathrm{P}} = \cos^2\theta = \frac{1}{2}(s_1 s_1' + s_2 s_2' + s_3 s_3' + 1) = \frac{2}{3}, \quad (19)$$

因此

$$(I_{4\mathrm{P}}^{\mathrm{AE}})_{\text{异基}} = 1 + \frac{2}{3}\log_2\frac{2}{3} + \frac{1}{3}\log_2\frac{1}{3} = 0.0817, \quad (20)$$

所以此协议在 P 基攻击下的 Alice/Eve 平均交互信息量为

$$I_{4\mathrm{P}}^{\mathrm{AE}} = \frac{1}{4} + \frac{3}{4}(I_{4\mathrm{P}}^{\mathrm{AE}})_{\text{异基}} = 0.3113, \quad (21)$$

小于扩展 BB84 协议的 $I_{\mathrm{P}}^{\mathrm{AE}}$. 由于三组基协议和四组基协议同样需要 2 比特的 S_{c}，只要给出四组基协议易于操作的物理实现方案，这一协议有实用意义.

这一协议还有两种 Breidbart 基窃听方式. 其一是取固定的窃听基为平行于立方体某一边的一条直径，窃听效率为

$$\eta_{\mathrm{B}} = \frac{1}{2}(1+\cos\alpha) = \frac{1}{2}\left(1 + \frac{1}{\sqrt{3}}\right), \quad (22)$$

Alice/Eve 平均交互信息量为

$$I_{4\mathrm{B}}^{\mathrm{AE}} = 1 + \eta_{\mathrm{B}}\log_2\eta_{\mathrm{B}} + (1-\eta_B)\log_2(1-\eta_{\mathrm{B}}) = 0.2560; \quad (23)$$

其二是随机取某两组基对应直径的角分线为窃听基，共有 6 种等价取法. 可以证明另外两条直径与窃听基所在直径垂直，对交互信息量没有贡献. 相邻直径上态的窃听效率为

$$\eta_{\mathrm{B}'} = \frac{1}{2}(1+\cos\alpha') = \frac{1}{2}\left(1 + \sqrt{\frac{2}{3}}\right) = 0.9082, \quad (24)$$

$$I_{4\mathrm{B}'}^{\mathrm{AE}} = \frac{1}{2}[1 + \eta_{\mathrm{B}'}\log_2\eta_{\mathrm{B}'} + (1-\eta_{\mathrm{B}})\log_2(1-\eta_{\mathrm{B}})] = 0.2788. \quad (25)$$

由(21)，(23)和(25)式可知，不考虑纠错过程对 I_{4X}^{AE} 的影响时，四组基双速协议的窃听策略以 P 基窃听为优. 如果考虑纠错过程，各 I_{4X}^{AE} 会发生不同的变化. 首先看 $I_{4\mathrm{P}}^{\mathrm{AE}}$. 1/4 选对基的情形不在 Bob 处引起错误；3/4 选错基的情形在 Bob 处引起错误的概率为 $2\eta_{\mathrm{P}}(1-\eta_{\mathrm{P}}) = 4/9$，Eve 与 Bob 同为正确的概率为 $\eta_{\mathrm{P}}^2 = 4/9$. Eve 手中选错基的比特在纠错后正确率为

$$(\eta_{\mathrm{P}})_{\text{有效}} = \frac{\eta_{\mathrm{P}}^2}{1 - 2\eta_{\mathrm{P}}(1-\eta_{\mathrm{P}})} = \frac{4}{5}, \quad (26)$$

Alice/Eve 的有效平均交互信息量为

$$(I_{4\mathrm{P}}^{\mathrm{AE}})_{\text{有效}} = 0.4586. \quad (27)$$

对于固定窃听基的 B 窃听，类似可得

$$(\eta_{\mathrm{B}})_{\text{有效}} = \frac{2+\sqrt{3}}{4}, \quad (28)$$

$$(I_{4\mathrm{P}}^{\mathrm{AE}})_{\text{有效}} = 0.6454. \quad (29)$$

下面来看随机选取 6 个窃听基之一的窃听方式：B′ 窃听. 对于与窃听基共轭的两组基上的态，Eve 引起的错误率为 1/2；对于与窃听基相邻的两组基上的态，Eve 引起的错误率为 $2\eta_{\mathrm{B}'}(1-\eta_{\mathrm{B}'}) = 0.1667$. 对于后者，Eve 与 Bob 同为正确的概率为 $\eta_{\mathrm{B}'}^2 = 0.8248$，因此纠错后 Eve 手中比特的正确率为

$$(\eta_{\mathrm{B}'})_{\text{有效}} = 0.9898, \quad (30)$$

B′ 攻击下 Eve 获得的有效信息量总计为

$$(I_{4\mathrm{P}}^{\mathrm{AE}})_{\text{有效}} = 0.4589. \quad (31)$$

由(27)，(29)和(31)式可知，在 Alice 和 Bob 使用标准纠错手续公开纠错之后，Eve 获得的有效信息量以采用 B 基窃听时为最大.

综上所述可知，利用标准纠错手续公开纠错后，Eve 的信息量以 B 窃听为最大. 如果能排除 Eve 的 B 窃听，就可以使秘密性增强算法的强度下降 40%，从而较大幅度地提高安全密钥的生成效率. 因此，如何设计协议基的选取和公开讨论方案，以便更有效地排除 B 窃听，是一个需要进一步研究的问题.

7. 十组基协议

考虑取下述十组基的双速 QKD 协议：不但取上

节中讨论的四组基协议中的四组基为协议基，而且取上节中讨论的第二类 Breidbart 基攻击中的六组随机选取的 Breidbart 窃听基也为协议基. 从 Poincaré 球面的内接立方体上看，这十组基对应于过立方体中心的 4 条长为$\sqrt{3}$倍边长的对角线所在直径和 6 条平行于长为$\sqrt{2}$倍边长的两个对角棱中点连线的直径. 下面考虑此方案在 P 基攻击下的 Alice/Eve 平均交互信息量.

Eve 选择的窃听基与 Alice 选择的发送基的关系可分成三种情形：1)同在$\sqrt{3}$线所对应的四组基内；2)同在$\sqrt{2}$线所对应的六组基内；3)一在四组基内，一在六组基内. 对于情形 1)，由上节的讨论可知 Alice/Eve 交互信息量为 0.3113[见(21)式]；对于情形 2)，可以看出六组基中有一组基与窃听基垂直，对 I^{AE} 无贡献；另外四组基的窃听效率为 $\frac{1}{2}\left(1+\cos\frac{\pi}{3}\right)=\frac{3}{4}$，相应的 I^{AE} 为 0.1888，故得情形 2)的 Alice/Eve 平均交互信息量为 $\frac{1}{6}+\frac{4}{6}\times 0.1888=0.2925$；对于情形 3)，即 Eve 选择的窃听基和 Alice 选择的发送基一个属于$\sqrt{2}$线对应的六组基之一，一个属于$\sqrt{3}$线对应的四组基之一. 可以证明，(1)每一条$\sqrt{2}$线与两条不相邻的$\sqrt{3}$线互相垂直；(2)每一条$\sqrt{3}$线与三条不相邻的$\sqrt{2}$线互相垂直；(3)发送基与窃听基相邻时窃听效率为 0.9082[见(24)式]. 由此可得 Alice/Eve 平均交互信息量为 0.2788. 综上所述可知，本节提出的十组基协议在 P 基窃听下 Eve 可能获得的平均交互信息量为

$$I_{10P}^{AE}=0.3113\times\left(\frac{2}{5}\right)^2+0.2925\times\left(\frac{3}{5}\right)^2+0.2788\times 2\times\frac{2}{5}\times\frac{3}{5}=0.2890. \quad (32)$$

由(32)式可知，在 P 基窃听下，当不考虑纠错过程对 Eve 获得的信息量的影响时，十组基双速 QKD 协议明显较扩展 BB84 协议更为安全. 十组基协议在各种 B 基窃听下的安全性以及纠错过程对 Eve 信息量的影响有待分析.

8. 结 论

综上所述可知，本文基于真空光速为极限信号速度这一基本假设提出的复合 QKD 系统及相关的双速协议在提高 QKD 系统密钥生成效率的同时，提高了系统的安全性. 双速协议使 QKD 协议基的选择空间有了本质性的扩充. 由于这一系统在公开讨论前就已经打破了 Bob 与 Eve 的对等地位，从而为今后基于理论和实践的各种原因设计满足不同需要的有效、安全的系统提供了更多的选择. 本文提出的经典信号同步延时的思想可用来实现全效率的自由空间量子密钥分配.

[1] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3

[2] Lo M K and Chan H F 1999 *Science* **283** 2050

[3] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441

[4] Wootters W K and Zurek W H 1982 *Nature* **299** 802

[5] Mandel L 1983 *Nature* **304** 188

[6] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (New York: IEEE) pp 175—179

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

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

[9] Hwang W Y, Ahn D and Hwang S W 2000 *Preprint* quant-ph/0009006

[10] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 961 (in Chinese) [杨 理、吴令安、刘颂豪 2002 物理学报 **51** 961]

[11] Yang L 2001 *Quantum Cryptography System and Its Security Analysis*, the Research Reprot of Post-Doctor Postition in the State Key Laboratory of Information Security (in Chinese) [杨 理 2001 量子密码系统及其安全性分析(博士后研究报告)]

[12] Born M and Wolf E 1999 *Principles of Optics* 7th (expanded) ed (Cambridge: Cambridge University Press)

Dual-velocity protocol of hybrid QKD system and its security analysis*

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, South China Normal University, Guangzhou* 510631, *China*)

(Received 11 March 2002; revised manuscript received 27 April 2002)

Abstract

Based on the hypothesis that the velocity of light in vacuum is the maximum velocity possible for any signal, we present a dual-velocity protocol for a hybrid quantum key distribution (QKD) system, and prove that its security is the same as that for the BB84 protocol. We show that this protocol can improve the efficiency of quantum key generation from 50% to 100%, and, at the same time, reduce Eve's information. Because it breaks the symmetry between Bob and Eve before open discussion, the dual-velocity protocol extends the concept of QKD and increases our choice of protocol bases. We present three application examples and analyze in detail their security under intercept/resend attacks.

Keywords: quantum cryptography, fiber-optic quantum key distribution, dual-velocity protocol

PACC: 0365, 4230, 4250

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