第 57 卷 第 9 期 2008 年 9 月
1000-3290/2008/57(09)/5605-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.9,September,2008

双协议量子密钥分发系统实验研究*

胡华鹏[1)] 张 静[1)] 王金东[1)†] 黄宇娴[1)] 路轶群[1)] 刘颂豪[1)] 路 巍[2)]

1)(华南师范大学信息光电子科技学院,光子信息技术广东省高校重点实验室,广州 510006)

2)(中国科学院合肥智能研究所,合肥 230031)

(2007 年 12 月 13 日收到;2008 年 4 月 11 日收到修改稿)

提出了一种改进的基于时间和相位混合编码的量子密钥分发方案,并进行了实验研究.在以 BB84 协议为基础的相位编码量子密钥分发系统上,利用了系统中原来舍弃的脉冲进行时间编码,使成码率提高为原方案的二倍.系统同时获得时间编码密钥和相位编码密钥,现在可以将两组密钥组合成新密钥,提高了成码率和监测窃听灵敏度.同时在系统的接收端用双 FM 反射式干涉仪代替传统的光纤 M-Z 干涉仪,提高了系统的稳定性.实验上已实现 90 km 光纤量子密钥分发,实验表明本系统具有安全性高,稳定性好,成本低的优点.

关键词:量子保密通信,量子密钥分发,相位编码,时间编码

PACC:4250,4230Q,0365

1. 引 言

自 1984 年 Bennett 等人提出第一个 QKD 协议之后[1],量子保密通信引起了人们极大的关注,并逐步从实验走向应用[2—5].在实际的 QKD 系统中,根据编码方式的不同,可分为以下几类:偏振编码[6],相位编码[7],频率编码[8]和时间编码[9,10]等.目前,QKD 系统的传输介质主要是光纤及自由空间.用光子偏振态作为信息载体简单易控,偏振编码常被用在自由空间 QKD 系统中[6,11].但由于光纤本身存在的随机双折射及其引起的偏振模色散效应,长距离传输会导致偏振态的随机变化,光子相位编码在光纤中传输抗干扰能力较强,在光纤中得到了广泛的应用,光纤量子保密通信获得了巨大的发展走向了实用阶段[12—14].

最近 Fabio 等人提出一种混合的并行 QKD 协议[15],该系统使用并行 QKD 方案和介观相干态(mesoscopic coherent states)提高有效系统的传输效率.理论上此协议的效率是 BB84 协议的 4 倍,但由于引入了介观相干态,导致实际探测时两种不同模式的相干态不易分辨,若要得到较高的分辨率,就会降低整个系统的安全性.而且该系统实验装置结构复杂,不适合大规模应用.另外一些学者运转了差分和相位编码双协议 QKD 系统,从碰撞理论出发证明了双协议有更好的安全性[13],但它不是真正的并行运转是串接双协议.我们提出了一种改进的混合并行运转 QKD 实验系统,在以相位编码的 BB84 协议的基础上,充分利用了系统中舍弃的一半脉冲进行时间编码,实现了对脉冲的两次编码,因此,这种混合方案成码率是原方案的二倍.还可以利用经典技术组合两类密钥形成新密钥,Even 和 Goldreich[16]从理论上证明两密钥的直接连接安全性不低于其中任一个,但密钥长度增加了成码率提高了,在实际应用中密码放大更有效,窃听灵敏度可提高.我们从互信息角度分析了双协议系统的安全性.实验上完成了 90 km 光纤量子密钥分发,实验表明该系统有一定的实用价值.

2. 双协议量子密钥分发方案

图 1 为混合编码 QKD 系统原理图.在原有的双 M-Z 相位编码 QKD 系统基础上加以改进,利用双 FM 反射式干涉仪代替 Bob 端的光纤 M-Z 干涉仪,其中臂长满足关系式

$$\frac{l_1 - l_2}{c} = \frac{2(l_3 - l_4)}{c}. \tag{1}$$

Alice 发出一个脉冲经 M-Z 干涉仪,光纤,环形器,

* 国家重点基础研究发展规划(973)项目(批准号:2007CB307001)资助的课题.

† 通信联系人. E-mail:jindongwang@yeah.net

FM 反射式干涉仪后，有四种可能的路径到达 Bob 端的单光子探测器：(l_2，l_4，l_4)，(l_1，l_4，l_4)，(l_2，l_3，l_3)和(l_1，l_3，l_3)，其中经过(l_2，l_4，l_4)的脉冲所经光程最短最早到达探测器，根据臂长关系经过(l_1，l_4，l_4)和(l_2，l_3，l_3)两个不同路径的脉冲应该会同时到达探测器发生干涉现象，经过(l_1，l_3，l_3)的脉冲最后到达探测器，产生了一个三脉冲串 A，B，C(如图 1 中所示)，Alice 和 Bob 分别调制相位调制器 PM_1 和 PM_2 的相位，使 B 脉冲的强度随相位差的不同而发生变化，从而实现相位编码. 而非干涉产生的 A 和 C 脉冲在进入单光子探测器前通过门控过滤掉，探测器只探测 B 脉冲，完成相位编码密钥分配.

在我们的混合编码 QKD 方案中，B 脉冲仍用

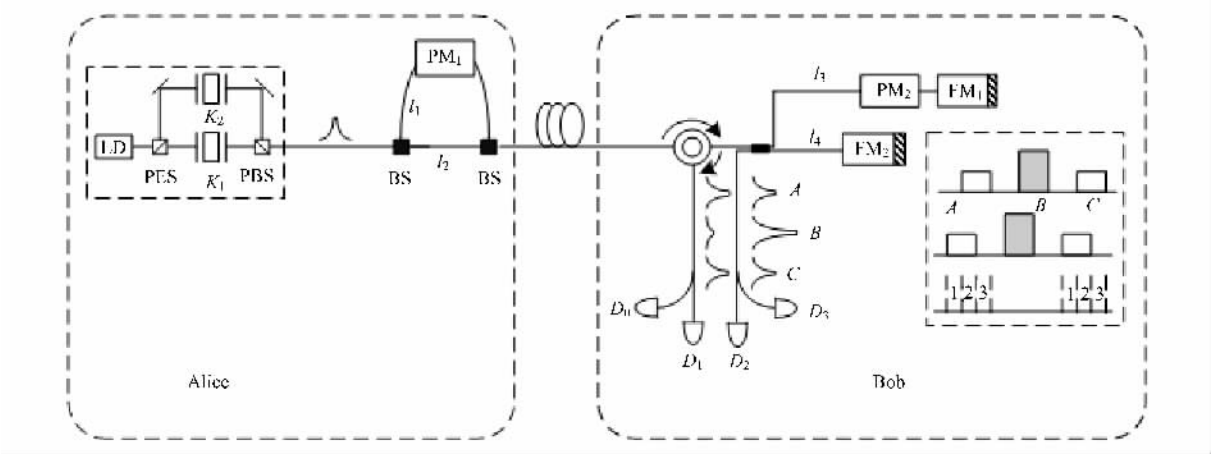

图 1 混合编码系统原理图

来进行相位编码，而原来相位编码方案中舍弃的 A 和 C 脉冲则用来进行时间编码. 时间编码[9,10]是利用随机的延迟脉冲来实现编码，为此我们设计了一个光源系统来代替原有的双 M－Z 相位编码 QKD 系统中的光源，如图 2 所示，光开关两支路的光纤长度差 Δl 需满足$\frac{\Delta l}{c}=\frac{T}{2}$，$T$ 为脉冲宽度，随机的控制光开关的开合就实现了对脉冲随机的延迟 0 或 $T/2$，满足了时间编码的基本要求.

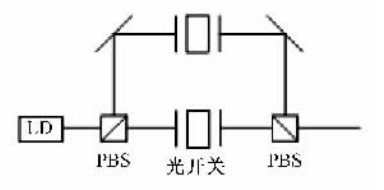

图 2 QKD 系统的光源

现在 Alice 端的激光器再发出一个脉冲经上述光源系统对其进行随机延迟后，在 Bob 端的探测器处将会有二种三脉冲串，如图 1 中 Bob 端中的虚框内所示，其中 B 脉冲仍用来实现相位编码，而 A 脉冲和 C 脉冲则用来进行时间编码，同时形成时间编码密钥和相位编码密钥，成码率是原方案的 3/2 倍(若 A，C 脉冲都用就是两倍).

2.1. 时间编码原理和操作

图 3 是时间编码二态协议原理图[9]. Alice 端激光器根据参考时间发出脉冲宽度为 T 的脉冲，经过设计的光源系统后脉冲被随机的延迟了 0 或 $T/2$，如果我们将延迟时间为 0 和 $T/2$ 的脉冲分别记为比特‘0’和‘1’，那么 Alice 随机的发出延迟时间为 0 或 $T/2$ 的脉冲，即随机的选择发送‘0’或‘1’，实现了时间编码. 这两种不同延迟时间的脉冲到达 Bob 端的探测器时在时域上存在相对重叠的时隙，即图 3 中的时隙 2，如果 Bob 在此时隙探测到光子，将无法判断 Alice 的发送状态，故将其舍去. 若 Bob 在时隙 1 或 3 探测到光子，那么他就能推断出 Alice 的发送状态. 就可以实现时间编码密钥分配. 由于形成两套密钥，存在窃听时两套密钥误码率会升高

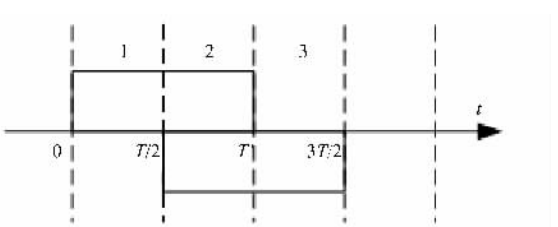

图 3 时间编码原理

(嵌入式计算机软件包中有纠错部分比对误码率计算功能)，在没有超出允许的最大误码率时，继续进行数据协调(改错)和密性放大获得高度保密的数据，一旦超出允许的最大误码率的值，Alice 和 Bob 之间的信息将会小于 Eve 窃听到的信息，从而无法进行单向的密性放大来使 Eve 窃听到的信息变成无效，进而将无法获得安全的密钥要终止本次通信，即可认为实现监测窃听者的目的.

2.2.双协议实验研究

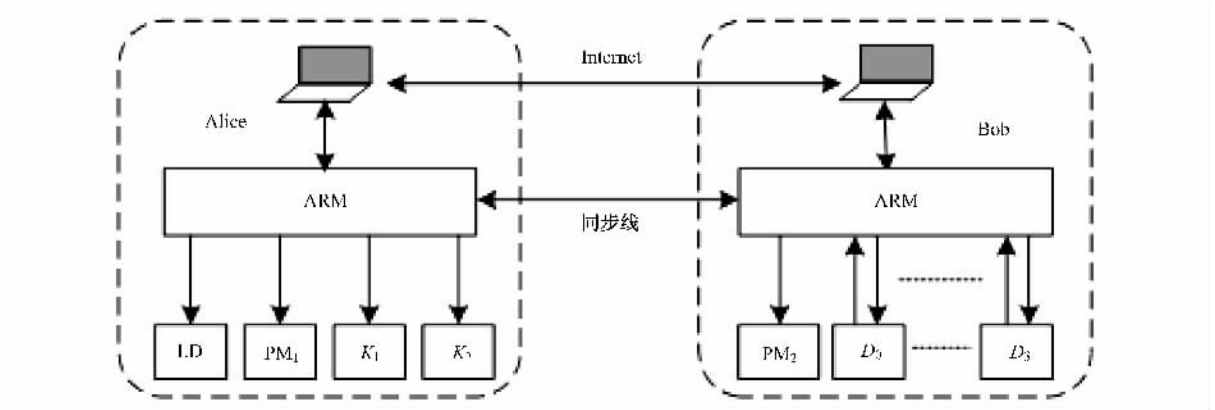

图 4　双协议实验框图

Alice 和 Bob 俩计算机通过网络相连构成公开信道，双方各自的嵌入式计算 ARM 由小于 5 m 导线连接同步. 量子信道由 90 km 光纤(光纤损耗为 0.3 dB/km)相连接. 通信时，Alice 计算机通过 ARM 控制激光器，光开关，相位调制器 PM_1 进行时间和相位调制并通过 90 km 光纤传送至 Bob 处，Bob 处的 ARM 在小于 5 m 导线同步下，考虑到 90 km 相应延迟，调制 PM_2，控制 D_0，D_1，D_2，D_3 门控(D_1，D_2 用于相位编码，D_0，D_3 用于时间编码)并将它们的计数输入 ARM 嵌式计算机. 双方 ARM 通过网络公开信道和各自密钥分配软硬件 (密钥分配，纠错，放大，比对等功能) 完成密钥分配，获得时间编码和相位编码密钥，Alice 和 Bob 处 ARM 把获取的密钥输到相应计算机. Alice 通过计算机利用所得的密钥对明文加密传送给 Bob，随后 Bob 利用获得的密钥对密文进行解密获得原文，完成了 90 km 量子保密通信，误码率小于 4%. 表 1，2 是它们各自的 16 进制密钥，在嵌入式计算机软件包内有一个选择功能：1)一般我们用相位编码进行保密通信，时间编码进行实时监测窃听者，本来一般用 1/3 码进行在公用信道上误码校对，现在用时间编码所得密钥全部双方公布比对，误码率精度高，窃听监测灵敏度大大提高，从这个角度来看等效提高了安全性. 2)可以选择并行运转功能. 把相位编码和时间编编码获得密钥直接连接，文献[14]中证明了两密钥串直接串接成的密钥安全性不低于原来的，但窃听监测灵敏度提高了. 另外，从互信息原理出发这种双协议增加 Alice 和 Bob 间的互信息，提高窃听难度，即可认为增加了安全性. 这里的双协议是 BB84 协议和时间编码协议同时运行. 本文改进的双 FM 反射式干涉仪相位调制系统能自动补偿瞬时偏振漂移，提高了干涉稳定性. 在实验中两种模式都成功运行，在室内实现了 90 km 光纤量子密钥分配. 表 1，表 2 密钥是相位编码 Alice 和 Bob 处生成的密钥，时间编码用于监控，直接给出每次误码率，误码率超标自动终止通信，重新开始. 激光发射速率为 20 kHz，密钥生成 1024 个密钥码就自动停止，密钥生成时间由嵌入计算机自动决定，够了 1024 码就结束发送，有时因接插损耗大，光纤扭曲大生成不了密钥，嵌入式计算机会给出提示终止密钥分配，只能重新启动. 本实验在正常时成功率 95%.

表 1　Alice 端密钥本

Alice 端密钥
B1 B2 B3 55 AA 41 D9 1D 0D D9 AB C9 12 E5 CF 3B E9 72 B5 12 52 D5 3D AB 61 D2 53 DD 5F 39 9C DC 5B 63 A1 AD 11 1D 43 B9 34 95 61 11 23 41
11 17 D1 F5 63 31 A5 F4 AD B1 8A 6A E1 AF 39 12 19 C9 D5 5F 79 5B 79 7C A5 6A C5 FD A6 31 AD 7D 99 63 CC 3D 19 45 2C FD 22 6E 15 B5 D3 79
B3 F1 C2 7D EB 79 B7 1D DF 43 B6 E1 F2 75 BE 69 11 53 8C 3B 7D FC E9 DF 6B 48 51 D5 3D CB B1 B4 C3 DD 6A FA D7 1D F6 D6 D8 55 AA

表 2 Bob 端密钥本

Bob 端密钥
B1 B2 B3 55 AA 31 D9 1D 1D D9 AB 39 72 E5 CF 3B C9 72 B5 12 52 D5 3D DB 6F D2 53 DD 51 19 9C DC 5B 61 A1 AD 11 5D 43 B9 34 95 11 11 23 41 11 15 D1 F5 63 3B A5 F4 AD B1 8A 6E E1 AF 39 52 19 C9 D5 5F 69 5B 79 7C A5 6A C5 FD A6 31 AD 7D 99 63 CC 3D 19 45 2C FD 22 6E 15 B5 D3 79 B1 F1 C2 7D FB 79 B7 1D CF 43 B1 E1 F2 75 BE 69 11 13 8C 3B 7D FC E9 D5 6B 48 51 D5 3D CB BA B4 C3 DD 6A 1A D1 1D F6 D6 D8 55 AA

2.3. 安全性分析

下面我们以最常见的截获重发攻击为例,从互信息的角度来讨论运行双协议(相位编码和时间编码混合)系统的安全性. 现在用 $I(\alpha,\beta)$ 表示 Alice 与 Bob 之间的互信息,$I(\alpha,e)$ 表示 Alice 与 Eve 之间的互信息,当 $I(\alpha,\beta)\geqslant I(\alpha,e)$[17,18] 时采用单向的密性放大可以将 Eve 窃取的信息变为无效,最终获得高度保密的密钥,反之则无法进行密性放大,也就无法获得高度保密的密钥不安全,故 $I(\alpha,\beta)\geqslant I(\alpha,e)$ 是目前普遍采用的安全判据,根据它就可以评估系统的安全性.

由文献[19,20]可知 Alice 与 Bob 之间的互信息可表示为

$$I(\alpha,\beta) = 1 - H(D) = 1 + D\log_2(D) + (1-D)\log_2(1-D), \quad (2)$$

其中 D 为系统总的误码率,包括相位编码引起的误码率 D_1,时间编码引起的误码率 D_2. 双协议方案中相位编码和时间编码同时进行互不影响,可看作相互独立的事件,分别记为事件 x 和 y,那么 Alice 与 Eve 之间的互信息 $I(\alpha,e)$ 可表示为

$$I(\alpha,e) = I(x,e) + I(y,e), \quad (3)$$

其中 $I(x,e)$ 满足相位编码互信息关系式,由文献[6]得

$$I(x,e) = \frac{2}{\ln 2}D_1 + O(D_1)^2 \approx 2.9D_1, \quad (4)$$

而对于 $I(y,e)$,我们将根据文献[9]具体分析. 在时间编码系统中令 C 为干涉对比度,$\mathrm{d}C$ 为对比度衰落,在没有窃听情况下的理想干涉对比度为 1/2,一般情况都存在对比度衰落,则 C 的关系式为

$$C = \frac{1}{2}(1-\mathrm{d}C). \quad (5)$$

同时文献[9]中也给出时间编码对比度关于误码率 D_2,互信息 $I(y,e)$,信道的传输效率 η 的函数表达式,在只考虑理想情况 $\eta = 100\%$ 时,

$$C = \frac{1}{2}\left[\sqrt{2D_2 + \frac{1-\eta}{\eta}}\sqrt{I(y,e)} + \sqrt{2D_2}\sqrt{I(y,e) - \frac{1-\eta}{\eta}} + 1 - I(y,e) - 2D_2\right]$$

$$= \frac{1}{2}\left[2\sqrt{2D_2 I(y,e)} - I(y,e) - 2D_2 + 1\right], \quad (6)$$

于是联合(5)和(6)式解方程得出时间编码过程 Alice 和 Eve 之间互信息 $I(y,e)$ 的表达式为

$$I(y,e) = 2D_2 \pm 2\sqrt{2D_2\cdot\mathrm{d}C} + \mathrm{d}C. \quad (7)$$

依据本双协议的特点,Bob 端进行测量时相当于三个事件,每个事件引起的误码率都是均等的,所以相位编码引起的误码率为 $D_1 = \frac{1}{3}D$,时间编码引起的误码率为 $D_2 = \frac{2}{3}D$,代入(4)和(7)式并联合(3)式得到 Alice 与 Eve 之间的互信息为

$$I(\alpha,e) = 2.3D \pm \frac{4}{3}\sqrt{3D\cdot\mathrm{d}C} + \mathrm{d}C. \quad (8)$$

设想最坏情况,在讨论安全性时 $I(\alpha,e)$ 取上式中较大的值即

$$I(\alpha,e) = 2.3D + \frac{4}{3}\sqrt{3D\cdot\mathrm{d}C} + \mathrm{d}C. \quad (9)$$

现在我们将 $I(\alpha,\beta)$ 和 $I(\alpha,e)$ 绘制成关于误码率 D 的函数图来直观的讨论系统的安全性,如图 5 所示,其中对比度衰落 $\mathrm{d}C$ 是参量. 图中曲线 a,b 和 c 分别表示令 $\mathrm{d}C$ 为 0.5,0.2 和 0.1 时 Alice 和 Eve 间的互信息,由图像可知系统的误码率存在一个最大允许值(图 5 中交点所对应横坐标值),当超出这个值时则表明 $I(\alpha,\beta)\geqslant I(\alpha,e)$ 不再成立,从而无法进行单向密性放大获得安全密钥,故不再安全. 图中 a,b,c 三种情况对应的误码率的最大允许值分别为 2.7%,7.1% 和 9.6%,而 BB84 协议为 14.6%,可见适当调节对比度衰落可以提高系统的安全性. 但实际上不论 $\mathrm{d}C$ 为多少,当实际通信过程 D 值越小时,$I(\alpha,\beta)$ 与 $I(\alpha,e)$ 的差值越大,即 Alice 与 Bob 能获得的保密信息的理论值 $[I(\alpha,\beta) - I(\alpha,e)]$ 越大,通信会越安全.

2.4. 稳定性分析

以下用矩阵光学的方法简单分析系统的稳定性. 双 FM 干涉仪原理图见图 1. 设从耦合器入射端

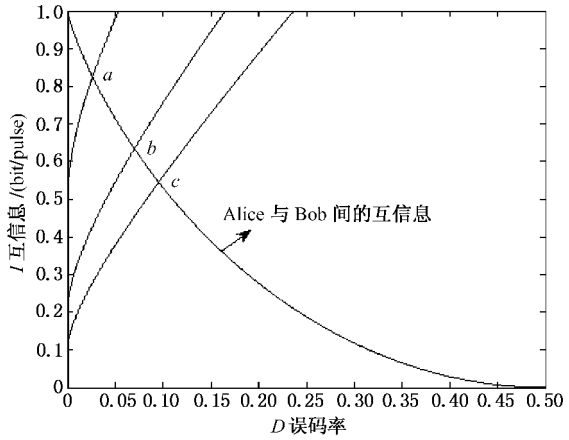

图 5　互信息与误码率间的函数关系图

入射的光波电场矢量为 E_{in}，耦合到输出端两路光波经由 FM 反射在光纤段 l_3，l_4 中往返，而后经耦合器再回到入射端处的电场矢量为 E_1，E_2. 我们通过光波经过的光学器件和光纤的传输矩阵就可以推导出它们的表达式，然后就可以讨论偏振衰落情况.

依据耦合波理论，假设耦合比为 1∶1 的 2 × 2 耦合器是偏振无关的，考虑到传输损耗，耦合器的 Johes 矩阵为

$$J_{13} = J_{31} = J_{24} = J_{42} = \frac{\sqrt{2}}{2} t_{\text{J}} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad (10)$$

$$J_{14} = J_{41} = J_{23} = J_{32} = \frac{\sqrt{2}}{2} t_{\text{J}} \begin{bmatrix} j & 0 \\ 0 & j \end{bmatrix}, \quad (11)$$

其中 t_{J} 为损耗的幅度传输系数.

法拉第镜的 Johes 矩阵为

$$T = t \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}, \quad (12)$$

考虑光波在光纤 l_3，l_4 段往返传输的过程. 光波相位的延迟和光强的衰减，用矩阵 F_3，F_4 来表示

$$F_i = t_{si} \mathrm{e}^{\mathrm{j}\phi_i} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad (i = 3,4), \quad (13)$$

式中 t_{si} 为幅度传输系数. 光纤的双折射光纤效应可以等效看成一个椭圆延迟器，可以写成

$$S_{+i} = \frac{\alpha_{si}}{d_{si}} \begin{bmatrix} \alpha_{si} & -b_{si}^{*} \\ b_{si} & \alpha_{si}^{*} \end{bmatrix} \quad (i = 3,4), \quad (14)$$

式中 $d_{si}^2 = \alpha_{si}\alpha_{si}^{*} + b_{si}b_{si}^{*}$，$\alpha_{si}$ 为在光纤 l_i 段的传输损耗，α_{si}，b_{si} 与光纤的双折射特性有关，返回的过程光纤的双折射等效为一个反向的椭圆延迟器，即

$$S_{-i} = \frac{\alpha_{si}}{d_{si}} \begin{bmatrix} \alpha_{si} & -b_{si} \\ b_{si}^{*} & \alpha_{si}^{*} \end{bmatrix} \quad (i = 3,4). \quad (15)$$

联合(10)到(15)式得出

$$E_1 = J_{31} \cdot F_3 \cdot S_{-3} \cdot T \cdot S_{+3} \cdot F_3 \cdot J_{13} \cdot E_{in}$$
$$= \frac{1}{2} \alpha_{s3}^2 t_{s3}^2 t_{\text{J}}^2 t \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} E_{\text{in}} \exp(2\mathrm{j}\phi_3), \quad (16)$$

$$E_2 = J_{41} \cdot F_4 \cdot S_{-4} \cdot T \cdot S_{+4} \cdot F_4 \cdot J_{14} \cdot E_{\text{in}}$$
$$= \frac{1}{2} \alpha_{s4}^2 t_{s4}^2 t_{\text{J}}^2 t \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} E_{\text{in}} \exp(2\mathrm{j}\phi_4),$$
$$= \frac{1}{2} \alpha_{s4}^2 t_{s4}^2 t_{\text{J}}^2 t \begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix} E_{\text{in}}$$
$$\times \exp(\mathrm{j}\pi + 2\mathrm{j}\phi_4), \quad (17)$$

其中 $2\phi_3$ 和 $2\phi_4$ 表示光波往返经过光纤 l_3，l_4 的相位延迟. 光纤 l_3，l_4 的长度都较短且长度差别不大，故 $\alpha_{s3} \approx \alpha_{s4}$，$t_{s3} \approx t_{s4}$ 代入(16)和(17)式可以得出，E_1 和 E_2 是两个偏振方向始终相同的电场矢量，如果这两个信号发生干涉，不会产生偏振衰落，因此双 FM 反射式干涉仪代替传统的 M-Z 干涉仪自动补偿了环境变化带来的偏振抖动和相位漂移，提高了系统的稳定性，实现了高稳定的密钥分配.

3. 结论和讨论

本文中的实验方案分析及实验表明：1)双协议的运行，对于 Eve 判断系统何时采用何种协议进而采用相应的攻击手段而言增加了难度，增加了系统的信息传输率，提高了监测窃听灵敏度，增加了安全性. 2)稳定性好. 在 Bob 端，利用双 FM 反射式干涉仪代替光纤 M－Z 干涉仪，自动补偿了环境引起的偏振抖动和光纤双折射引起的相位漂移. 3)结构简单，成本低，有很好的应用前景.

但同时本实验系统在进行实际实验过程中仍还存在一些缺陷，如光源不是理想的单光子源，信道是有损耗的，探测器的探测效率有限等等，窃听者根据这些缺陷采取相应的攻击可能会对 QKD 的安全性会造成一定的影响. 首先，光子数分束(PNS)攻击会破坏系统的安全性. 光源为非理想的单光子源，存在多光子脉冲窃听者 Eve 就可以实行 PNS 攻击：Eve 先利用非破坏性测量技术(QND)测量出 Alice 发出的信号脉冲中的光子数，然后有选择地截获单光子脉冲，而将多光子脉冲进行光子分裂保留一份将另一份经无损耗信道传送给 Bob，从而达到了窃取信息的目的破坏了 QKD 的安全性. 为了防止 PNS 攻击可以在我们的双协议系统的基础上应用 PDS (photon-number-resolving decoy-state)[21] 量

子密钥分配方法：一方面，在信号态脉冲中引入一些与信号态脉冲强度不同的脉冲即诱惑态脉冲，这可以通过 Alice 随机地选择发出不同强度的脉冲来实现，由于信号态脉冲和诱惑态脉冲的特性相同致使 Eve 不能够区分出来，Eve 的攻击必将改变信号态脉冲和诱惑态的传输情况而被发现，这样就能够确保 QKD 的安全性；另一方面，采用光子数目分辨(photon-number-resolving)技术把多光子脉冲删除掉，彻底克服光子数分束攻击. 其次，特洛伊木马攻击[22]，IPE (invisible photon eavesdropping)方案[23]等等实际攻击可能也会对我们的实验系统的安全性造成一定的影响，但由于采用了双协议运行，这类攻击的影响将会比单协议运行时小得多. 总之，本系统在具有安全性高，稳定性好，成本低的优点，在不远的将来会有很好的市场应用前景.

[1] Bennett C H, Brassard G 1984 *Int. Conf. Computers Systems & Signal Processing* (New York: IEEE) p175

[2] Liang C, Fu D H, Liang B, Liao J, Wu L A, Yao D C, Lü S W 2001 *Acta Phys. Sin.* **50** 1429 (in Chinese) [梁 创、符东浩、梁 冰、廖 静、吴令安、姚德成、吕述望 2001 物理学报 **50** 1429]

[3] Wu G, Zhou C Y, Chen X L, Han X H, Zeng H P 2005 *Acta Phys. Sin.* **54** 3622 (in Chinese) [吴 光、周春源、陈修亮、韩晓红、曾和平 2005 物理学报 **54** 3622]

[4] Li M M, Wang F Q, Lu Y Q, Zhao F, Chen X, Liang R S, Liu S H 2006 *Acta Phys. Sin.* **55** 4642 (in Chinese) [李明明、王发强、路轶群、赵 峰、陈 霞、梁瑞生、刘颂豪 2006 物理学报 **55** 4642]

[5] Zhao F, Lu Y Q, Wang F Q, Chen X, Li M M, Guo B H, Liao C J, Liu S H 2007 *Acta Phys. Sin.* **56** 2175 (in Chinese) [赵 峰、路轶群、王发强、陈 霞、李明明、郭邦红、廖常俊、刘颂豪 2007 物理学报 **56** 2175]

[6] Gisin N, Ribordy G, Tittel W *et al* 2002 *Rev. Mod. Phys.* **74** 145

[7] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762

[8] Merolla J M, Mazurenko Y, Goedgebuer J P *et al* 1999 *Opt. Lett.* **24** 104

[9] Debuisschert T, Boucher W 2004 *Phys. Rev.* A **70** 042306

[10] Debuisschert T, Boucher W 2005 *Phys. Rev.* A **72** 062325

[11] Miao E L, Mo X F, Gui Y Z, Han Z F, Guo G C 2004 *Acta Phys. Sin.* **53** 2123 (in Chinese) [苗二龙、莫小范、桂有珍、韩正甫、郭光灿 2004 物理学报 **53** 2123]

[12] Mo X F, Zhu B, Han Z F, Gui Y Z, Guo G C 2005 *Opt. Lett.* **30** 2632

[13] Chen X, Wang F Q, Lu Y Q, Zhao F, Li M M, Mi J L, Liang R S, Liu S H 2007 *Acta Phys. Sin.* **56** 6434 (in Chinese) [陈 霞、王发强、路轶群、赵 峰、李明明、米景隆、梁瑞生、刘颂豪 2007 物理学报 **56** 6434]

[14] Guo B H, Lu Y Q, Wang F Q, Zhao F, Hu M, Lin Y M, Liao C J, Liu S H 2007 *Acta Phys. Sin.* **56** 3695 (in Chinese) [郭邦红、路轶群、王发强、赵峰、胡 敏、林一满、廖常俊、刘颂豪 2007 物理学报 **56** 3695]

[15] Fabio Alencar Mendonca, Rubens Viana Ramos: Hybrid Parallel Quantum Key Distribution Protocol. arXive e-print quantph/0609065 (2006)

[16] Even S, Goldreich O 1985 "*On the power of Cascade Ciphers*", *ACM Trans. on Comp. Sys.* Vol 3, No 2 pp108—116

[17] Ekert A K, Bruno Huttner, Massimo Palma G, Asher Peres 1994 *Phys. Rev.* A **50** 1047

[18] Csiszar I, Korner J 1978 *IEEE Trans. Info. Theory* **24** 339

[19] Lüthenhaus N 1996 *Phys. Rev.* A **54** 97

[20] Gilbert G, Hamrick M, e-print, ar Xiv, quant-ph/0106043

[21] Cai Q Y, Tan Y G 2006 *Phys. Rev.* A **73** 032305

[22] Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G 2006 *Phys. Rev.* A **73** 022320

[23] Cai Q Y 2006 *PLA* **351** 23

Experimental quantum key distribution with double protocol *

Hu Hua-Peng[1)] Zhang Jing[1)] Wang Jin-Dong[1)†] Huang Yu-Xian[1)] Lu Yi-Qun[1)] Liu Song-Hao[1)] Lu Wei[2)]

1)(*Laboratory of Photonic Information technology, School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

2)(*Heifei Institute of Intelligent Machines, Chinese Academy of Sciences, Heifei* 230031, *China*)

(Received 13 December 2007; revised manuscript received 11 April 2008)

Abstract

We propose one kind of improved QKD scheme based on time coding and phase coding. The pulse which had been discarded on the BB84 protocol phase coding QKD system is used to realize the time coding protocol, thus the useful bits rate in the present scheme can be doubled. At the same time, the phase coding keys and the time coding keys are obtained, we may combine both as new keys which can enhance the generated rate and the sensitivity of monitor. At Bob's side, a Fraday-Michelson is used instead of a traditional M-Z interferometer, which improves the stability of the interference visibility. With the proposed experimental setup, a stable quantum key distribution was performed over 90 km fiber. It is shown in our experiment that the characteristics of our system are as follows: secure, stable and economical.

Keywords: quantum privacy communication, quantum key distribution, phase coding, time coding

PACC: 4250, 4230Q, 0365

* Project supported by the National Basic Research Program of China (Grant No. 2007CB307001).

† Correspondence author. E-mail: jindongwang@yeah.net