联合调制量子密钥分配系统*

郭邦红[1)] 杨理[2)†] 向憧[2)] 关翀[2)] 吴令安[3)] 刘颂豪[1)]

1) (华南师范大学信息光电子科技学院, 广东省微纳光子功能材料与器件重点实验室, 广州 510631)

2) (中国科学院信息工程研究所, 信息安全国家重点实验室, 北京 100093)

3) (中国科学院物理研究所光物理开放实验室, 北京 100080)

(2012 年 11 月 4 日收到; 2013 年 3 月 15 日收到修改稿)

本文提出了一种对每一个单光子信号进行相位和偏振两种编码调制的联合调制量子密钥分配 (QKD) 系统. 结合复合 QKD 系统的双速协议, 本文给出了在理想情形下可以通过一个信号光子生成两比特密钥的 QKD 协议, 明显提高了 QKD 协议的内禀光子利用率. 在稳定性方面, 本文发展了联合调制的 Michelson 型 QKD 系统, 从而在原理上解决了联合调制 QKD 系统的稳定性问题.

关键词: 量子密钥分配, 双速协议, 联合调制, 量子密钥分配系统的稳定性

PACS: 03.67.Dd **DOI:** 10.7498/aps.62.130303

1 引 言

量子密钥分配 (QKD) 协议能使通信双方 (Alice 和 Bob) 共享一个无条件安全的密钥 [1,2], 因而引起了人们广泛的研究和关注, 国内同行也做了很多工作 [3−6]. QKD 协议最常见的两种是使用共轭编码的 BB84 协议和使用非正交态的 B92 协议. 实现 QKD 协议的系统包含一个经典信道和一个量子信道 (单模光纤或自由空间), 其量子信道的编码调制主要有偏振调制和相位调制两种方式. 所谓联合调制是指同一个 QKD 系统既采用偏振调制, 也采用相位调制. 在通常的 BB84 协议中 Alice 和 Bob 不能同步选取量子信号的基, 联合调制方式增加了系统的复杂度, 却无助于提高系统的光子利用率, 因此没有必要采用这种调制方式. 具体而言, 当 QKD 系统采用 BB84 协议时, 偏振调制部分可以有四态协议和六态协议两种选择 [7]. 当偏振调制取四态协议时, 可求出联合调制协议的平均光子利用率为 1, 等于单纯的偏振调制协议的平均光子利用率 (1/2) 加上单纯的相位调制协议的平均光子利用率 (1/2); 当偏振调制部分取六态协议时, 可求出联合调制协议的平均光子利用率仅为 5/6, 同样等于偏振调制部分的光子利用率 (1/3) 加上相位调制部分的光子利用率 (1/2) , 可见这种调制方式没有实质性的优势 (详细讨论见本文第四节) .

安全、高码率、稳定传输的 QKD 系统是当前 QKD 系统走向实用需要探索的问题, 文献 [8—13] 提出的方案分别提高了 QKD 系统的效率、稳定性或安全性. 2006 年, 杨理等在量子光学会议的一个特邀报告 [14] 中首次提出了将相位调制与偏振调制联合使用、在一个信号光子上编码两个密钥比特的 QKD 方案, 这是一个将联合调制与复合 QKD 系统 [15] 相结合的方案. 该方案将 QKD 的 BB84 协议的内禀光子利用率由 0.5 提高到 2, 但一直没有解决稳定性问题. 本文借鉴文献 [16, 17] 中的方案, 给出了具有良好稳定性的联合调制 QKD 系统的原理性设计方案. 由于这一方案采用复合 QKD 系统双速协议, 其理想情形下平均光子利用率为 2, 因而具有一定的理论意义和实用价值.

2 联合调制 QKD 系统

本文的联合调制 QKD 系统是基于复合 QKD

* 国家自然科学基金 (批准号: 61173157) 和广东省自然科学基金重点项目 (批准号: 10251063101000001) 资助的课题.

† 通讯作者. E-mail: yangli@iie.ac.cn

系统双速协议 [15] 提出的. 基于真空光速为极限信号速度这一物理学基本假设, 文献 [15] 提出复合 QKD 系统的双速协议并证明了这个协议的安全性. 复合 QKD 系统双速协议如下:

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那一组基上, 此经典信息以光速 c 沿公开信道传向 Bob. 假设经典信道为直线, 延时 τ 除了要能保证在 Alice 和 Bob 的安全区之外经典信号永远落后于量子信号一个可分辨的时间差外, 还须满足

$$\tau < \frac{1}{c}[n_{\rm g}(l+l_{\rm b})-d], \tag{1}$$

以保证 Bob 可以利用经典信号进行测量 (但 Eve 却不能不被察觉地利用这一信号). 其中 c 为真空光速, $n_{\rm g}$ 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, $l_{\rm b}$ 为 Bob 在安全区内预留的光纤长度, d 为 Alice 到 Bob 的直线距离.

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.

复合 QKD 系统的双速协议在设计中巧妙利用了真空光速是极限信号速度这一狭义相对论的断言, 使得 Eve 无法和 Bob 一样有效利用经典信道发送的测量基信息, 从而为实际保密通信系统的各种需求提供了更多的选择 [15]. 文献 [15] 曾将双速协议的安全性归约到 BB84 协议的安全性, 而邀请报告 [18] 中则给出了双速协议 (该文称之为相对论量子密钥分配协议) 无条件安全性的一个直接的证明. 下面我们来看联合调制量子密钥分配系统的基本结构. 文献 [14] 中给出的联合调制光纤 M-Z 型 QKD 量子密钥分配系统的基本结构如图 1 所示.

在这个系统 (图 1) 中, 对每一个脉冲都会同时进行相位调制编码和偏振调制编码. 首先来分析各个调制单元的具体方案和调制的具体过程. 发送端的相位调制单元 $U_{1\rm A}$ 和偏振调制单元 $U_{2\rm A}$ 的构造如图 2 所示.

为了讨论方便, 定义水平偏振方向的脉冲为 $|H\rangle$, 垂直偏振方向的脉冲为 $|V\rangle$, 假设光源发出的处于 $|\pi/4\rangle = 1/\sqrt{2}(|H\rangle+|V\rangle)$ 的脉冲经衰减成单光子脉冲, 设 x 为沿光路前进方向的位置, t 为传输时间, 则进入 $U_{1\rm A}$ 之前的脉冲可以表示为: $F(x,t)|\pi/4\rangle$, 这里简单地取 $F(x,t)=f(\kappa x-\omega t)=\alpha {\rm e}^{-\beta(\kappa x-\omega t)^2}$ 为高斯脉冲. 系统开始运行后, Alice 首先随机选择四个随机参数 $m,n,k,l\in\{0,1\}$. 在相位调制单元 $U_{1\rm A}$ 中, 偏振分束器 PBS1 对水平偏振和垂直偏振脉冲进行分束, PBS2 对水平偏振和垂直偏振脉冲进行合束, MA 对脉冲加入相位 ${\rm e}^{{\rm i}\theta_{\rm A}}$, $\theta_{\rm A}=\dfrac{k}{2}\pi+l\pi$. 所以经过 $U_{1\rm A}$ 进行相位调制之后的脉冲可以表示为: $F(x,t)|H\rangle+F(x+\Delta L,t){\rm e}^{{\rm i}\theta_{\rm A}}|V\rangle$, 这里 ΔL 为长短光臂的路程差.

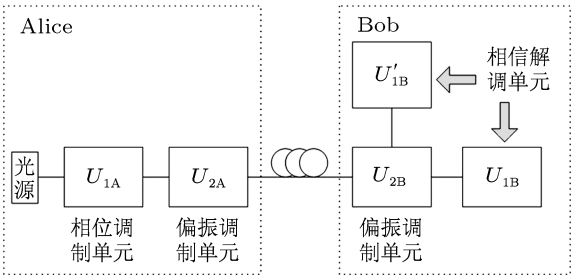

图 1 联合调制量子密钥分发系统框图

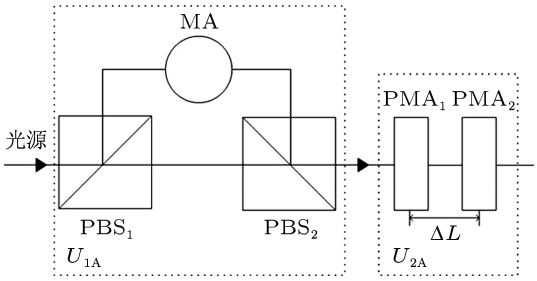

图 2 发送端调制单元. 其中 PBS 为偏振分束器、MA 为相位调制器, PMA 为偏振调制器, ΔL 等于长短光臂的路程差

当脉冲进入偏振调整单元 $U_{2\rm A}$ 后, 水平偏振的脉冲到达 $\rm PMA_2$ 处时, 垂直偏振的脉冲正好到达 $\rm PMA_1$, 然后同时对两个偏振方向进行调制, 这里 $\rm PMA_1$ 处对垂直偏振分量旋转 $\varphi_{\rm A1}=\dfrac{m}{4}\pi+\dfrac{n-1}{2}\pi$, $\rm PMA_2$ 处对水平偏振分量旋转 $\varphi_{\rm A2}=\dfrac{m}{4}\pi+\dfrac{n}{2}\pi$, 于是经过调制之后的脉冲可以表示为

$$\begin{aligned} &F(x,t)\left|\frac{m}{4}\pi+\frac{n}{2}\pi\right\rangle \\ &\quad+F(x+\Delta L,t){\rm e}^{{\rm i}\theta_{\rm A}}\left|\frac{m}{4}\pi+\frac{n}{2}\pi\right\rangle, \end{aligned} \tag{2}$$

此时前后两个脉冲将处于同一偏振态 $\left|\dfrac{m}{4}\pi+\dfrac{n}{2}\pi\right\rangle$, 调制完成后 Alice 将脉冲对通过光纤发送给 Bob, 同时将参数 m,k 通过经典信道发送给 Bob.

接收端的偏振解调单元 U_{2B} 和相位解调单元 U_{1B}, U'_{1B} 的构造如图 3 所示.

当脉冲到达 Bob 处时, 先进入 U_{2B} 进行偏振解调. 这里 PMB_1 和 PMB_2 旋转 $\varphi_{B1}=\varphi_{B2}=-\dfrac{m}{4}\pi$, 解调之后的脉冲为

$$F(x,t)|n\pi/2\rangle + F(x+\Delta L,t)\,e^{i\theta_A}|n\pi/2\rangle,$$

于是当 $n=0$ 时, 前后两个脉冲都处于水平偏振方向, 当 $n=1$ 时, 前后两个脉冲都处于垂直偏振方向. PBS_3 的作用是对水平偏振和垂直偏振脉冲进行分束, 使前后两个脉冲将进入同一个相位解调单元. PMB_3 (PMB_4) 的作用是对其中一个脉冲进行偏振调制 $\pi/2$ ($-\pi/2$), PMB_3 使得跑在前面的脉冲转为垂直偏振方向 $|V\rangle$, PMB_4 使得跑在前面的脉冲转为水平偏振方向 $|H\rangle$. 于是通过偏振解调之后的脉冲为

$$F(x+\Delta L,t)\,e^{i\theta_A}|H\rangle + F(x,t)|V\rangle.$$

下面分析相位解调过程. 以相位解调单元 U_{1B} 为例, 其中 PBS_4 为水平偏振和垂直偏振的分束器, MB_1 对脉冲加入相位 $e^{i\theta_B}$, 这里 $\theta_B=\dfrac{k}{2}\pi+\dfrac{\pi}{2}$, 而 $\dfrac{\lambda}{2}$ 波片则会对脉冲进行偏振调制 $-\pi/2$, 设长短臂的路程差同样是 ΔL, 则两个光路的脉冲可以在 BS_1 处进行干涉. 到达 BS_1 之前的脉冲可以表示为

$$F(x+\Delta L,t)\,e^{i\theta_A}|H\rangle_{短} + F(x+\Delta L,t)\,e^{i\theta_B}|H\rangle_{长},$$

两项处于同一偏振方向, 根据相位不同, 当 $l=0$ 时, 干涉仪两个输入脉冲在在 D_1 端干涉相涨, D_2 端干涉相消, 则我们能够在 D_1 处测得信号; 当 $l=1$ 时, 我们能够在 D_4 处测得信号. 协议中的具体参数如表 1 所示.

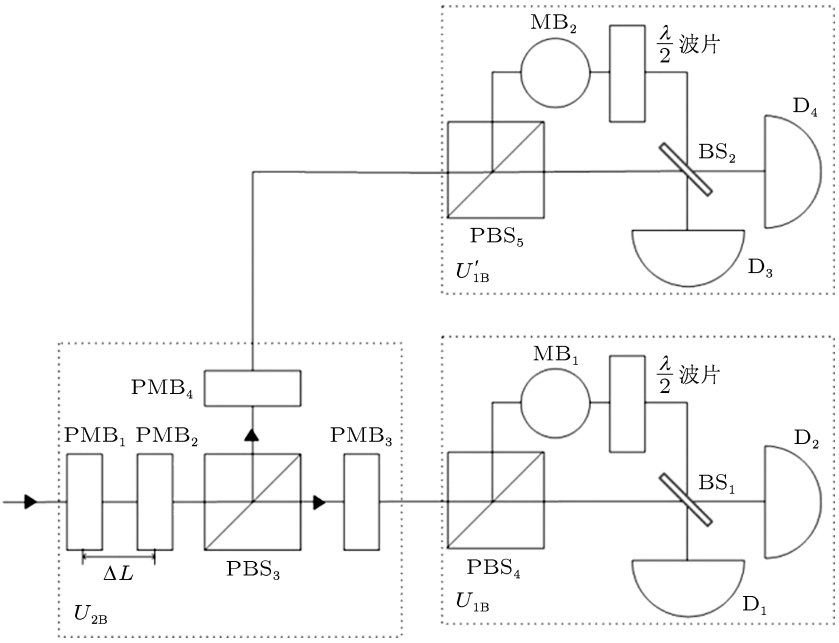

图 3 接收端调制单元. 其中 PBS 为偏振分束器、MB 为相位调制器, PMB 为偏振调制器, BS 为分束器, D 为探测器

3 具有稳定性的联合调制 QKD 系统

为了提高系统的稳定性, 我们通过将 Michelson 干涉型相位调制 QKD 系统发展为联合调制 QKD 系统, 给出了抗干扰的联合调制 QKD 方案 (见图 4).

设进入 U_{1A} 之前的脉冲可以表示为: $F(x,t)|\pi/4\rangle$. 系统开始运行时, Alice 首先选择四个随机参数 $m,n,k,l\in\{0,1\}$. 在相位调制单元 U_{1A} 中, 偏振分束器 PBS_1 对水平偏振和垂直偏振脉冲进行分束, MA 对脉冲加入相位 $e^{i\theta_A}$, $\theta_A=\dfrac{k}{2}\pi+l\pi$. FM_1 和 FM_2 将到达的脉冲旋转 $\pi/2$, 设长短臂的路程差 ΔL, 于是所以经过 U_{1A} 进行相位调制之后的脉冲可以表示为

$$\begin{aligned}&-\exp[i(\theta_{SA}+\theta_A)]F(x,t)|H\rangle\\&-\exp[i(\theta_{LA})]F(x+\Delta L,t)|V\rangle.\end{aligned}\qquad(3)$$

表 1 联合调制的密钥分发协议

相位比特	MA	MB	偏振比特	PMA_1	PMA_2	PMB_1	PMB_2	测量结果				传输比特	信息比特
k,l	θ_A	θ_B	m,n	φ_{A1}	φ_{A2}	φ_{B1}	φ_{B2}	D_1	D_2	D_3	D_4	m,k	n,l
0 0	0	$\pi/2$	0 0	$-\pi/2$	0	0	0	1	0	0	0	0 0	0 0
			1 0	$-\pi/4$	$\pi/4$	$-\pi/4$	$-\pi/4$	1	0	0	0	1 0	0 0
			0 1	0	$\pi/2$	0	0	0	0	1	0	0 0	1 0
			1 1	$\pi/4$	$3\pi/4$	$-\pi/4$	$-\pi/4$	0	0	1	0	1 0	1 0
1 0	$\pi/2$	π	0 0	$-\pi/2$	0	0	0	1	0	0	0	0 1	0 0
			1 0	$-\pi/4$	$\pi/4$	$-\pi/4$	$-\pi/4$	1	0	0	0	1 1	0 0
			0 1	0	$\pi/2$	0	0	0	0	1	0	0 1	1 0
			1 1	$\pi/4$	$3\pi/4$	$-\pi/4$	$-\pi/4$	0	0	1	0	1 1	1 0
0 1	π	$\pi/2$	0 0	$-\pi/2$	0	0	0	0	1	0	0	0 0	0 1
			1 0	$-\pi/4$	$\pi/4$	$-\pi/4$	$-\pi/4$	0	1	0	0	1 0	0 1
			0 1	0	$\pi/2$	0	0	0	0	0	1	0 0	1 1
			1 1	$\pi/4$	$3\pi/4$	$-\pi/4$	$-\pi/4$	0	0	0	1	1 0	1 1
1 1	$3\pi/2$	π	0 0	$-\pi/2$	0	0	0	0	1	0	0	0 1	0 1
			1 0	$-\pi/4$	$\pi/4$	$-\pi/4$	$-\pi/4$	0	1	0	0	1 1	0 1
			0 1	0	$\pi/2$	0	0	0	0	0	1	0 1	1 1
			1 1	$\pi/4$	$3\pi/4$	$-\pi/4$	$-\pi/4$	0	0	0	1	1 1	1 1

其中相位比特 k,l 和偏振比特 m,n 由 Alice 选择, 传输比特 m,k 通过经典信道发送给 Bob, 信息比特 n,l 则由最后的测量结果对应获得. MA 的相位调制角度 $\theta = k\pi/2 + l\pi$, MB_1 (MB_2) 的相位调制角度 $\theta_B = (k+1)\pi/2$; PMA_1 旋转 $\varphi_{A1} = m\pi/4 + (n-1)\pi/2$, PMA_2 旋转 $\varphi_{A2} = m\pi/4 + n\pi/2$, PMB_1 和 PMB_2 旋转 $\varphi_{B1} = \varphi_{B2} = -m\pi/4$.

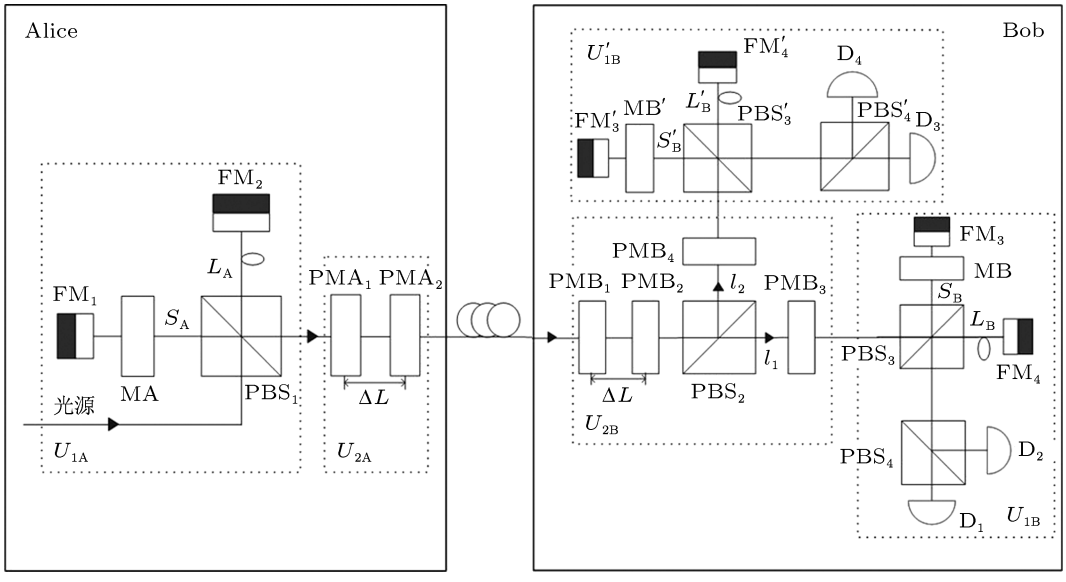

图 4 基于 Faraday-Michelson 调制单元的联合调制 QKD 系统原理图. 其中 PBS 为偏振分束器, MA, MB 为相位调制器, FM 为法拉利旋转镜, PMA, PMB 为偏振调制器, D 为探测器

偏振调制单元 U_{2A} 与相同, 调制之后的脉冲处于相同偏振方向, 可以表示为

$$-\exp[\mathrm{i}(\theta_{SA}+\theta_A)]F(x,t)\left|\frac{m}{4}\pi+\frac{n}{2}\pi\right\rangle$$
$$-\exp[\mathrm{i}(\theta_{LA})]F(x+\Delta L,t)\left|\frac{m}{4}\pi+\frac{n}{2}\pi\right\rangle, \quad (4)$$

Alice 将该脉冲通过光纤发送给 Bob, 同时通过经典信道发送 m,k 给 Bob.

接收端偏振解调跟前文相同, Bob 首先利用偏振解调单元 U_{2B}, 按照接收到的参数 m 进行偏振解调, 当 $n=0$ 时脉冲进入 U_{1B} 进行相位解调, 否则进入 U'_{1B}. U_{2B} 偏振解调后脉冲可以表示为 $-\exp[\mathrm{i}(\theta_{SA}+\theta_A)]F(x,t)|H - \exp[\mathrm{i}(\theta_{LA})]F(x+\Delta L,t)|V\rangle$. 以 U_{1B} 为例, 长短臂的路程差同样为 ΔL,

其中 PBS_3 为垂直偏振和水平偏振的分束器, PBS_4 则为 $|\pi/4\rangle$ 和 $|3\pi/4\rangle$ 的分束器, MB 为相位解调器, 调制相位为 $e^{i\theta_B}$, 这里 $\theta_B=\frac{k}{2}\pi$, 假设线路引起的相位影响 $e^{i\theta}$ 满足 $\theta=\theta_{SA}+\theta_{LB}=\theta_{SB}+\theta_{LA}$, 于是在 PBS_4 处, 当 $l=0$ 时脉冲为

$$\exp[i(\theta+k\pi/2)]F(x+\Delta L,t)(|H\rangle+|V\rangle), \quad (5)$$

于是经过 PBS_4 之后只会在 D_1 处测得结果, 而 $l=1$ 时则为

$$\exp[i(\theta+k\pi/2)]F(x+\Delta L,t)(|H\rangle-|V\rangle), \quad (6)$$

此时 D_2 处会测得结果. 同理, 当 $n=1$ 时, 脉冲在 U'_{1B} 中进行解调, $l=0$ 时 D_3 处测得结果, 而 $l=1$ 时 D_4 处测得结果.

4 讨论与结论

本节我们对协议的效率, 安全性以及稳定性分别进行讨论.

1) 效率方面. 本方案为联合调制的双速协议 MD, 我们对比采用联合调制的非双速协议 M, 采用四态偏振调制的双速协议 D, 和采用四态偏振调制的非双速协议 S. 这里的非双速协议, 指协议双方在量子消息传递过程中, 并不进行经典信息传输, 所以在发送方随机调制的基础上, 接收方按照协议内容, 随机从可能的解调方案中选取一种进行解调, 在测量完毕之后, 双方再共享选择的方案, 通过对比调制和解调方案, 决定最终获取的密钥.

上述的几种方案单次传递的传输效率如表 2 所示.

表 2 几种方案单次传递的传输效率

协议	MD	M	D	S
共享比特数	2	1	1	1/2

其中 MD 方案如前文所述, 每次传递可以有效共享 2 bit 的密钥. 对于其余的三种方案:

方案 S 接收方每次传递有一半概率选取到错误的解调方案, 且成功传递的情况下, 每次只能共享 1 bit 的密钥, 所以单次传递的传输效率只有 1/2 bit.

方案 D 采取双速协议, 保证每次都能有效的进行密钥共享, 不过因为只采用了偏振调制, 所以单次传递的传输效率只有 1 bit.

方案 M 采用联合调制, 所以当接收方以 1/4 概率选取到正确解调方案时, 可以共享 2 bit 的密钥; 而当接收方以 1/4 概率选对偏振解调方案, 但是选错相位解调方案时, 根据探测器的结果, 双方可以共享 1 bit 的经典参数 n 作为密钥 (D_1 或 D_2 有信号时 $n=0$, 否则 $n=1$); 同样, 当接收方以 1/4 概率选对相位解调方案, 但是选错偏振解调方案时, 由探测器的结果, 双方可以共享 1 bit 的经典参数 l 作为密钥 (D_1 或 D_3 有信号时 $l=0$, 否则 $l=1$); 所以单次传递的传输效率为 $\frac{1}{4}\times 2+\frac{1}{4}\times 1+\frac{1}{4}\times 1=1$ bit.

所以对于四态的偏振调制, 双速协议有效的提高了一倍传递效率; 而联合调制虽然也提高了一倍的传输效率, 但是到该方案实现的复杂度也提高了一倍.

不过对于六态偏振调制的非双速协议 S_1, 其联合调制的改造方案 M_1 和双速协议改造方案 D_1, 以及联合调制的双速协议方案 MD_1, 单次传递的传输效率如表 3 所示.

表 3

协议	MD_1	M_1	D_1	S_1
共享比特数	2	5/6	1	1/3

此时联合调制对传输效率的提高超过一倍 (S_1 至 M_1), 同时双速协议对传递效率的提高也超过了一倍 (S_1 至 D_1). 具体分析过程与四态方案类似.

2) 安全性方面. 双速协议的安全性在文献 [15] 中已经有过证明, 基于经典信号传递速度不能超过真空光速的前提, 将双速协议的安全性归约到了原始 BB84 协议的安全性上. 在文献 [18] 中我们对复合 QKD 系统双速协议的安全性也进行了直接的证明. 不过, 上述安全性分析并不完整, 这是因为协议的安全性不但依赖于经典信号的最大传递速度不能超过真空光速, 也依赖于量子信号的最大传递速度不能超过真空光速. 如果没有后者, 攻击者可以首先截取量子信号, 等待经典信号到达之后完成测量, 再利用量子信号的超光速传输方法按时将截留的量子信号传递到 Bob 的安全区, 完成攻击. 不过, 虽然 "量子信号的最大传递速度不能超过真空光速" 这一假设并不是一个可以直接从狭义相对论得到的结论, 我们可以利用反证法证明, 它同样可以归结到经典信号不能超过光速的前提中, 即我们可以得到下述引理.

引理 如果不存在超光速的经典信号传递, 那

么一定不存在确定量子信号的超光速传递.

证明 假设能够实现确定量子信号的超光速传递, 不妨设能够以超光速传递水平偏振态和垂直偏振态. 那么对于发送方 Alice 和接收方 Bob, Alice 若想传递经典信号 0, 那么她就以超光速向 Bob 发送水平偏振态; 若想传递经典信号 1, 那么她就以超光速向 Bob 发送垂直偏振态. 而 Bob 总以水平垂直基对接收到的量子信号进行测量, 根据唯一确定的测量结果他就可以获得 Alice 希望传递的经典信号. 于是我们就实现了超光速的经典信号传递, 与命题假设矛盾. 所以原命题成立.

3) 稳定性方面. 影响 QKD 系统稳定性的三个主要因素是: 信道的双折射效应, 发送、接收端干涉仪光臂中的双折射效应, 和环境对本地干涉仪双臂光程差的影响. 第一个因素对最终生成密钥的错误率影响较小, 这是因为前后两个相干涉的脉冲几乎同时通过信道的每一个部分. 对于剩余效应的累积, 目前只有往返式 QKD 系统可以部分抵消, 而且当系统跨度较大时这种抵消作用也会明显减弱. 对于第三个因素目前除了大约半小时校正一次外没有更好的办法. 我们这里所提出的稳定 QKD 系统设计方案, 与这方面大多数工作一样, 是针对第二个因素. 在每条本地光臂中, 我们利用法拉第旋转镜来消除双折射效应的影响, 注意到进入每一条光臂的脉冲, 不管初始偏振方向处于水平或者垂直, 都将分别以水平和垂直两种偏振方向经过同一条光臂 (来回) , 所以在光臂中所受到的双折射效应造成的影响每次都相同. 具体而言, 从 Michelson 型 QKD 系统两端干涉仪的一个臂来看, 其传输矩阵等价为一个相位因子与法拉第镜传输矩阵的乘积 [16,17]:

$$T = \overleftarrow{T}_{\text{forward}} \cdot T_{\text{FM}} \cdot \overrightarrow{T}_{\text{backward}} = \exp(\mathrm{i}\beta) T_{\text{FM}},$$

其中 $\overleftarrow{T}_{\text{forward}}$ 为前向传输矩阵, $\overrightarrow{T}_{\text{backward}}$ 为后向传输矩阵, T_{FM} 为法拉第镜的传输矩阵, β 是光纤传输的双折射引起的相位漂移. 可见由于法拉第镜对输入偏振态有 90° 旋转, 这种结构将自动消除光路中的各种双折射效应.

总之, 联合调制 QKD 系统通过对每个单光子信号加载 4 个经典比特, 并借助经典信道延时发送 Alice 的选基参数给 Bob, 实现了每个光信号传输 2 bit 信息的目标, 较原始的 $\mathrm{BB8_4}$ 协议提高了内禀光子利用率 4 倍. 本文通过发展 Michelson 型 QKD 系统给出了可以稳定工作的联合调制 QKD 系统的原理性设计方案.

[1] Bennett C H, Brassard G 1984 *Int. Conf. Computers Systems & Signal Processing* (New York: IEEE) 175

[2] Gisin N, Ribordy G, Tittle W, Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[3] Liang C, Fu D H, Liang B, Liao J, Wu L A, Yao D C, Lv 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 textbf50 1429]

[4] Tang Z L, Li M, Wei Z J, Lu F, Liao C J, Liu S H 2005 *Acta Phys. Sin.* **54** 2534 (in Chinese) [唐志列, 李铭, 魏正军, 卢非, 廖常俊, 刘颂豪 2005 物理学报 **54** 2534]

[5] He G Q, Zeng G H 2006 *Chin. Phys.* **15** 1284

[6] Guo B H, Wang F Q, Liao C J, Liu S H 2007 *Acta Phys. Sin.* **56** 3695 (in Chinese) [郭邦红, 王发强, 廖常俊, 刘颂豪 2007 物理学报 **56** 3695]

[7] Yang, L, Wu L A, 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]

[8] Inoue K, Waks E, Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[9] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[10] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[11] Fabio A M, Rubens V R 2006 arXiv: quant-ph/0609065

[12] Chen X, Wang F Q, Lu T 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]

[13] Hu H P, Zhang J, Wang J D, Huang Y X, Lu T Q, Liu S H, Lu W 2008 *Acta Phys. Sin.* **57** 5605 (in Chinese) [胡华鹏, 张静, 王金东, 黄宇娴, 路轶群, 刘颂豪, 路巍 2008 物理学报 **57** 5605]

[14] Yang L, Wu L A, Zhao Z S, Liu S H, Mixed modulated quantum key distribution system (Invited Talk) 2006 *Annual Symposium of Chinese Optics Society* (Conference of quantum optics) (in Chinese) [杨理, 吴令安, 赵震声, 刘颂豪 2006 混合调制量子密钥分发系统 (量子光学专题, 特邀报告) 中国光学学会 2006 年学术大会]

[15] Yang L, Wu L A, Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese) [杨理, 吴令安, 刘颂豪 2002 物理学报 **51** 2446]

[16] Mo X F, Zhu B, Gui Y Z, Han Z F, Guo G C 2005 *Opt. Lett.* **30** 2633

[17] Ma H Q, Zhao J L, Wu L A 2007 *Opt. Lett.* **32** 698

[18] Zhuang S S, Yang L, Unconditional security of relativistic quantum key distribution protocol (Invited Paper) 2010 *Photonics Asia*, October 18–21, Beijing, 2010 78460I

Quantum key distribution system based on combined modulation*

Guo Bang-Hong[1)] Yang Li[2)†] Xiang Chong[2)] Guan Chong[2)]
Wu Ling-An[3)] Liu Song-Hao[1)]

1) (*Laboratory of Nanophotonic Functional Materials and Devices School of Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou* 510631, *China*)

2) (*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*)

3) (*Laboratory of optical physicas, Institute of Physics , Chinese Academy of Sciences, Beijing* 100080, *China*)

(Received 4 November 2012; revised manuscript received 15 March 2013)

Abstract

We suggest a combined modulation quantum key distribution (QKD) system which encodes each single-photon signal with both phase modulation and polarization modulation. With the aid of dual-velocity protocol of hybrid QKD system, we construct a scheme to realize this combined modulation QKD which generates two-bit key with one signal for increasing the efficiency of QKD. We also develop a combined modulation Michelson QKD system, then solve the stability problem of the combined modulation QKD system in principle.

Keywords: quantum key distribution, dual-velocity protocol, hybrid modulation, stability of QKD system

PACS: 03.67.Dd **DOI:** 10.7498/aps.62.130303

* Project supported by the National Natural Science Foundation of China (Grant No. 61173157), and the Natural Science Foundation of Guangdong (Grant No. 10251063101000001).

† Corresponding author. E-mail: yangli@iie.ac.cn