一种新的单光源多波长双向量子密钥分发系统*

岳孝林[1)2)] 王金东[1)2)†] 魏正军[1)2)] 郭邦红[1)2)] 刘颂豪[1)2)]

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 510006)

2) (华南师范大学光子信息技术广东省高校重点实验室, 广州 510006)

(2012 年 2 月 21 日收到; 2012 年 3 月 15 日收到修改稿)

针对 “即插即用” 双向量子密钥分发系统传输效率低的实际问题, 详细分析了系统低效的原因和当前的解决方案, 提出了一种单光源多波长双向量子密钥分发方案. 该方案采用波分复用器件作为滤波器来产生量子密钥分发所需的多波长信号. 与其他多波长方案相比, 该方案的优点是在实现高速多波长量子密钥分发时, 不再受外界控制源调制速率和精度等性能的影响, 不再带来多激光器引入的边信道攻击的缺陷, 且整体系统易于集成. 该方案为 “即插即用” 量子密钥分发系统的高效研究提供了一个新的参考方案.

关键词: 量子保密通信, 双向系统, 瑞利散射, 多波长

PACS: 42.79.Sz, 03.67.Dd, 03.67.Hk

1 引 言

量子密钥分发 (quantum key distribution, QKD) 就是能使通信双方 (发送方 Alice, 接收方 Bob) 在即使存在窃听者 (Eve) 的信道中也能共享一串绝对安全的密码的一种新技术. 自 1984 年 Bennett 和 Brassard 提出第一个量子密钥分发协议 ——BB84 协议 [1] 以来, 量子密钥分发系统无论在原理 [2−7] 和实验 [2,4,8−11] 上都得到了迅猛的发展.

相比自由空间量子密钥分发系统 [12], 基于成熟的光纤网络的光纤量子密钥分发系统 [8−11] 成为各国研究人员关注的热点. 然而, 光纤介质也总存在一定缺陷 (如, 纤芯形状不规则、折射率不均匀等) 以及易受温度、应力等外界环境的影响, 导致了光信号偏振和相位的随机变化, 影响了系统的稳定性. 为了解决这些问题, 各国研究人员提出了很多的方法补偿光纤双折射对偏振的影响 [9,13] 和相位的随机漂移 [14−16], 系统的稳定性都有了一定的提高, 但是并未能从根本上解决这个问题. 早在 1997 年, Muller 等就提出了一种能自适应补偿偏振和相位漂移的系统 ——“即插即用”QKD 系统 [17], 该系统能够很好地补偿光纤双折射引起的偏振和相位漂移, 在无人干预的情况下可实现稳定通信. 但由于其单光纤双向通信的系统结构导致了该系统极易受到瑞利散射的影响, 从而也导致了系统的重复速率极低, 每次只能传输一个脉冲. 瑞利散射是指由于光纤制造过程或者其他原因引起的折射率分布起伏使强光脉冲四向散射, 是光纤固有的一种效应. 由于瑞利散射的影响, 在长程光纤中存在三部分光脉冲: Bob 发送到 Alice 的强光脉冲、Alice 反射回 Bob 的信号光脉冲、强光脉冲的瑞利散射光. 若瑞利散射光与信号光的传输方向一致 (如图 1 所示), 则瑞利散射光可能进入到 Bob 端并引起探测器响应, 从而引入误码.

为了减少瑞利散射引入的系统误码, Muller 等的方案中一次只传送一个光脉冲, 探测完该脉冲之后再发送下一个脉冲, 因此该系统的效率很低, 从而大大影响了该系统的实用化.

研究人员为提高单光纤双向系统的效率, 相继

* 国家自然科学基金重大研究计划 (批准号: 91121023)、国家自然科学基金 (批准号: 61108039, 60978009) 和国家重点基础研究发展计划 (批准号: 2011CBA00200) 资助的课题.

† E-mail: wangjd@scnu.edu.cn

提出了一些研究方案.

1) 存储环方案 [18]: 在原单光纤双向系统的 Alice 端插入一个存储环, 用来存储 Bob 端发送的脉冲串, 以避免返回的信号光与瑞利散射光的重叠. 在进入到存储环之前, Alice 对强光脉冲进行一次衰减, 此时在存储环内就只存在弱的光脉冲, 产生的瑞利散射光很小, 故可以忽略. 接收时, Bob 在接收完整串脉冲之后才开始发送下一串脉冲. 相对于原方案来说, 发送和接收单元是脉冲串, 而不是单个的脉冲, 整体的效率得到了一定的提高, 但是仍不能持续发送光脉冲进行密钥分发, 因此效率还有待提高.

2) 边带调制方案 [19]: 该方案在 Alice 端插入了一个调制器, 用来调制信号光的频率. Alice 对 Bob 发送的信号光进行边带调制, 将信号光的频率调制到邻近的频率上, 在反射回 Bob 端时, 强光与弱信号光的频率不一样, 因此可以使用滤波的方式将瑞利散射光与信号光分离, 避开瑞利散射光对系统的影响, 提高了系统的重复速率. 但是该系统需要外部的控制系统来实现对 Alice 端边带调制器和 Bob 端滤波器的高速调制, 因此最终的通信速率和误码率受制于外部控制系统的速率和精度, 不利于高速通信.

3) 多个波长脉冲通信方案 [20]: 方案在存储环方案 [18] 的基础上, 使用了两个以上不同波长的光脉冲进行通信. Bob 在不同的时间段发送不同波长的脉冲串, 相应地产生不同波长的瑞利散射光, Alice 使用存储环避开了相同波长的微弱信号光与相同波长的瑞利散射光的重叠. 如图 2 所示, 虽然反射回 Bob 端信号光 λ_1 和瑞利散射光 λ_2 在长程光纤中存在重叠, 但是到达 Bob 端之后, 可以使用滤波器将瑞利散射光 λ_2 滤掉. 文献 [20] 报道了使用两个以上单波长激光器或波长可调谐激光器来产生多个波长, 采用高速可调光滤波器来滤除瑞利散射光, 实现了系统效率的提高. 但是, 该方案中多个波长脉冲串的产生过程和滤波过程都需要外部控制系统对各波长进行快速精确地响应, 并且很容易受到边信道攻击 [21,22], 导致最终 QKD 系统的速度和安全性都依赖于外部控制系统. 另外价钱昂贵, 难以集成化, 这些都限制了该方案的实用.

上述各方案在一定程度上提高了双向 QKD 系统的效率, 但是系统的效率仍受制于存储环长度或者器件的外部控制系统的性能, 从而影响了系统实用化. 本文提出了一种单个光源产生多波长的方案, 该方案采用波分复用器件 (WDM) 作为滤波器来产生量子密钥分发所需的多波长信号, 使系统避免了由于使用多个激光器而引入的边信道攻击, 规避了瑞利散射光对系统重复速率的影响.

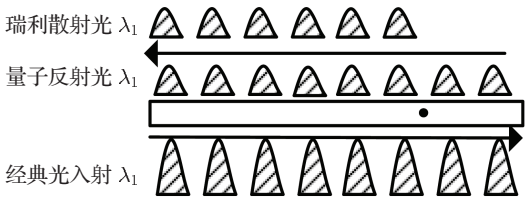

图 1 瑞利散射光对双向系统的影响 (图中黑点表示散射点)

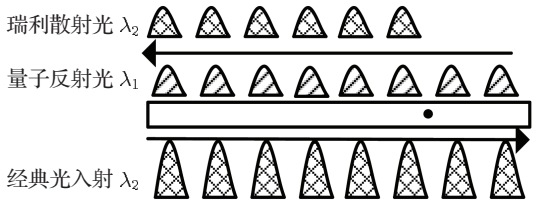

图 2 多波长规避瑞利散射光对双向系统影响的原理

2 一种新的单光源多波长 QKD 方案

根据前面的分析, 只要保证同一波长的强、弱两脉冲串不重叠, 就能很好地规避瑞利散射的影响. 本方案在前期研究的基础上, 使用一个宽带光源与纯无源器件结合来产生多波长脉冲串, 抑制了瑞利散射对系统的影响, 提高了系统的重复速率.

2.1 多波长脉冲串的产生

如图 3 所示, 宽带光源 LD 输出一串脉冲, 假设脉冲串的持续时间为 $\tau(\tau \cdot \nu_{\mathrm{g}} = \mathrm{QC}$, ν_{g} 表示群速度, QC 表示长程光纤长度). 光脉冲经过适当的衰减之后进入波分复用器 WDM_1, 通过 WDM_1 解复用出四个波长: λ_1, λ_2, λ_3, λ_4, 且四个波长分别进入对应的通道, 假设 λ_1 进入 1 路、λ_2 进入 2 路、λ_3 进入 3 路、λ_4 进入 4 路. 在各路加上不同长度的延迟环 SL_n ($n = 1, 2, 3$, $\mathrm{SL}_3 = 3\mathrm{SL}_1 = 3\mathrm{QC}$, $\mathrm{SL}_2 = 2\mathrm{QC}$), 对经过该路的脉冲进行不同的延时. 经过 WDM_2 合复用之后可以输出如图 4 所示分布的脉冲序列. 此处, 激光器的工作时长为 τ, 发送完

长一串脉冲串之后, 激光器停机, 探测器接收完 λ_1 的信号脉冲串之后, 激光器马上开始发送另外一串持续时间为 τ 的脉冲串. 循环进行如上的过程就可以实现多个波长脉冲串的不间断发送.

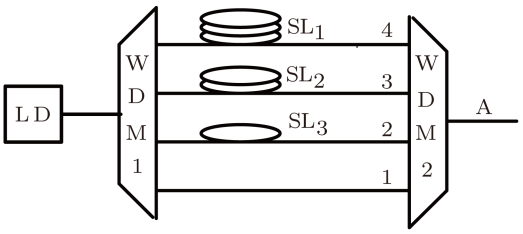

图 3 产生多波长脉冲的方案图 (LD, 宽带激光器; WDM_1 和 WDM_2; 波分复用器; SL_1—SL_3, 延迟环)

图 4 多波长脉冲串分布示意图

多个波长脉冲串在长程光纤中的传输过程如下: λ_1 最先进入光纤, 此时光纤中强光和瑞利散射光都为 λ_1, 但是此时单光子探测器不工作. t_2 时刻, 波长为 λ_1 的脉冲串经过衰减, 进入延迟环 DL($=$ QC$/2$). 在 λ_1 进入 DL 同时, 波长为 λ_2 的脉冲串开始进入 QC. 如图 5 所示, Bob 端开始接收 λ_1 的量子信号光时, 进入 QC 的强光脉冲波长为 λ_4, 后向瑞利散射光是 λ_3 和 λ_4, 进入到 WDM 后分别进入不同的信道, 信号光 λ_1 引起探测器响应. 待接收完 λ_1 时, 立刻开启激光器, 波长为 λ_1 的经典光开始进入 QC, Bob 端探测器开始接收 λ_2 的信号光. 以此类推, 探测器可以不间断工作, 效率得到了提高.

在进行探测时, WDM 可以作为一个多波长滤波器. 根据波分复用器的原理, 在 WDM 解复用之后, 不同的波长进入相应的通道, 在对应的通道上对各波长进行探测, 就可以减少其他波长的影响.

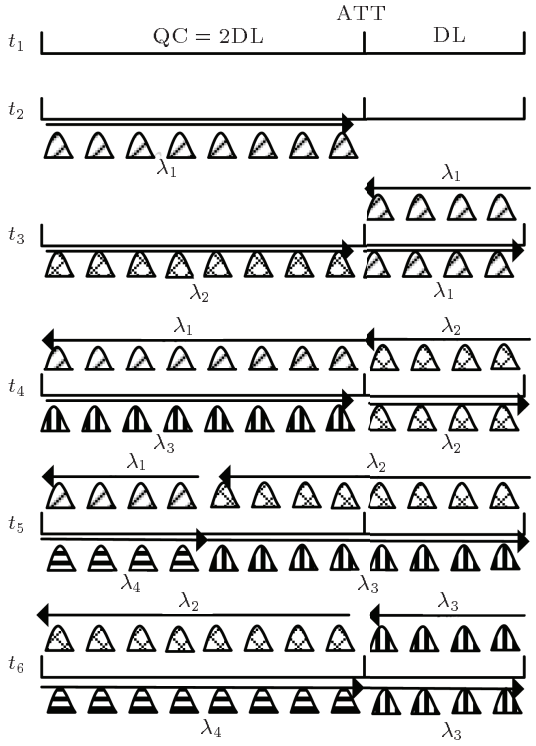

图 5 多波长脉冲串传输过程

2.2 一种新的单光源多波长双向量子密钥分发系统

通过使用上面的多波长产生方案与 “即插即用”QKD 系统结合, 构建了一个新的 QKD 系统, 如图 6 所示.

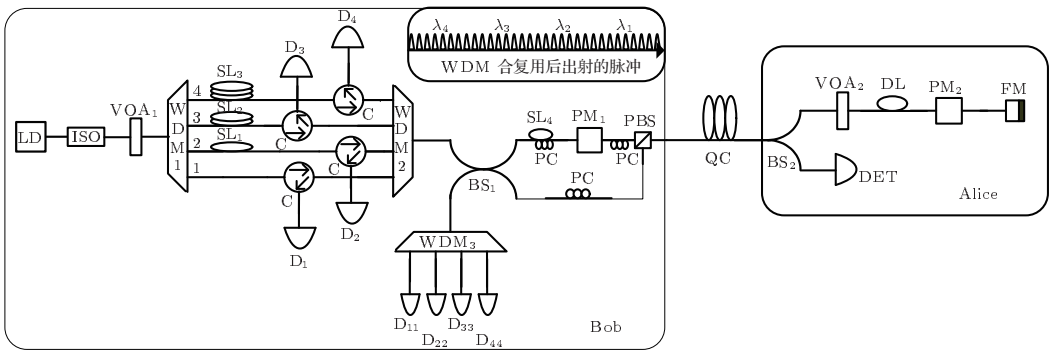

图 6 一种新的单光源多波长 QKD 系统原理图 (图中, LD 为宽带光源, ISO 为隔离器, VOA_n ($n = 1, 2$) 为可调衰减器, WDM_n 为波分复用/解复用器, $SL_n(n = 1, 2, 3, 4)$ 为脉冲存储环, C 为环形器, D_n ($n = 1, 2, 3, 4, 11, 22, 33, 44$) 为单光子探测器, PC 为偏振控制器, $PM_n(n = 1, 2)$ 为相位调制器, BS_1 为 50:50 分束器, BS_2 为不等分分束器, PBS 为偏振分束器, QC 为量子信道, DL 为延迟环, DET 为强光探测器, FM 为法拉第反射镜)

虽然该系统为多波长通信系统, 但是各个波长的密钥分发过程相对独立. 与 “即插即用”QKD 系统类似, 以 λ_1 为信号脉冲为例. 波长为 λ_1 的脉冲从 WDM_2 出来以后, 经 50:50 分束器 BS 分成两部分: P_1 和 P_2. P_1 经过短臂, P_2 经过长臂, 通过偏振控制器 PC 的调节后, 以最大功率通过 PBS 进入到 QC 中, 此时前后两个脉冲偏振态正交. 到达 Alice 端之后, P_1 又被分成两部分, 一部分进入到 DET, Alice 可以根据所测功率来控制 VOA_2 对脉冲进行衰减以达到单光子水平. P_1 的另外一部分经 Faraday 反射镜反射并被 VOA_2 衰减之后返回 Bob 端. P_2 与 P_1 类似, 不同之处在于, 相位调制器 PM_2 对 P_2 随机调制上一个相位 φ_2, 返回 Bob 端. 到达 Bob 端之后, 由于 PBS 的偏振选择, P_1 经过长臂, 并被 PM_1 调制相位 φ_1, P_2 经过短臂, P_1 和 P_2 同时到达 BS_1, 发生干涉. 若 $\varphi_1-\varphi_2=0$, 则发生相长干涉, 探测器 D_1 计数响应; 若 $\varphi_1-\varphi_2=\pi$, 则发生相消干涉, 探测器 D_{11} 计数响应. 其他波长脉冲串与 λ_1 脉冲串类似. 干涉之后的光脉冲根据不同的波长, 经过 WDM_2 和 WDM_3 滤波之后就会进入到对应的单光子探测器, 形成计数.

2.3 方案的改进

为了减少由于单光子探测器暗计数引起的误码, 就必须减少探测器的个数. 因此, 对上述的方案进行了改进, 将原来的 8 个探测器减少到了 4 个, 如图 7 所示.

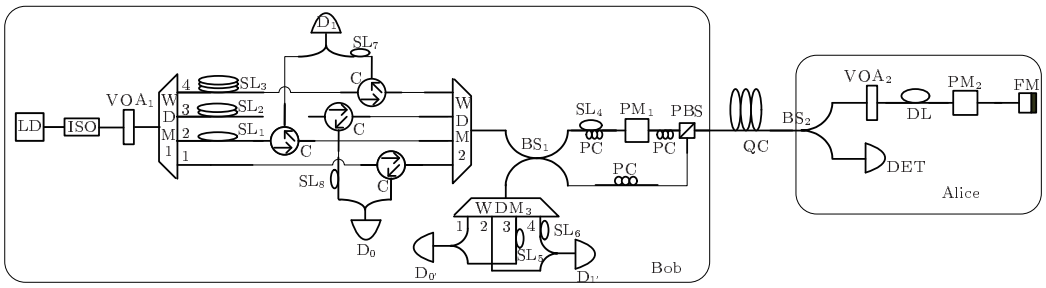

图 7 四探测器多波长 QKD 方案

与原方案不同的地方主要有:

1) 探测器个数 原方案中使用了 8 个探测器, 改进后只需要 4 个探测器, 其中波长为 λ_1 和波长为 λ_3 的光共用 D_0 和 $D_{0'}$, 波长为 λ_2 和波长为 λ_4 的光共用 D_1 和 $D_{1'}$;

2) 存储环个数 在原方案的基础上增加了 SL_5—SL_8 4 个延迟环, 其中 $SL_5=SL_6=SL_7=SL_8=QC$. 这样处理主要是为了在探测器 D_0 和 $D_{0'}$ 探测信号光 λ_1(或 λ_3) 时, 将波长为 λ_3(或 λ_1) 的瑞利散射光隔离在探测器的响应时间之外. 同样, 使用这样的方式可以在探测器 D_1 和 $D_{1'}$ 工作时, 避免 λ_2 与 λ_4 的影响.

3) 探测器响应时序 波长为 λ_1 的光脉冲解码后, 通过 WDM_2 或 WDM_3 的 1 路, 进入到探测器 D_0 或 $D_{0'}$, 引起计数响应. 此时, D_1 和 $D_{1'}$ 均处于不工作状态. 当波长为 λ_2 的光脉冲解码后, 通过 WDM_2 或 WDM_3 的 2 路, 可以引起 D_1 或 $D_{1'}$ 响应而 D_0 和 $D_{0'}$ 不工作. 当探测 λ_3 和 λ_4 时, 由于存储环 SL_5—SL_8 的影响, λ_3 引起 D_0 或 $D_{0'}$ 响应的时间将产生一个延迟, 同样 λ_4 引起 D_1 或 $D_{1'}$ 响应的时间也将延迟. 延迟的时间为 $\Delta t=\dfrac{SL_n}{c}=\dfrac{QC}{c}$, $n=5,6,7,8$. 总的探测器响应时序见表 1.

表 1 探测器响应时序

时间段	$t_1-t_2=\Delta t$	$t_2-t_3=\Delta t$	$t_3-t_4=\Delta t$	$t_4-t_5=\Delta t$	$t_5-t_6=\Delta t$
探测波长	λ_1	λ_2		λ_3	λ_4
工作探测器	D_0 或 $D_{0'}$	D_1 或 $D_{1'}$	均不响应	D_0 或 $D_{0'}$	D_1 或 $D_{1'}$

使用上述的方案, 在不影响 “即插即用”QKD 系统稳定性的情况下很好地提高了效率, 为 QKD 系统的实用化提供了参考.

3 讨 论

以上就是我们采用的多波长量子密钥分发方案, 该方案采用双向系统与多波长相结合, 在保证了系统稳定性的基础上, 使用多波长方案规避了瑞利散射的影响, 提高了系统的重复速率. 但是由于多波长的应用也引入了一些问题, 我们对这些问题及相应的解决方案分析如下.

1) 宽带光源引入的问题. 由于宽带光源的使用, 在 WDM_1 解复用之后仍然存在信道间的串扰, 若信号光中夹杂其他波长的光, 这些光将进入到探测器, 从而引起系统误码率的提高. 在该系统中的信道串扰可以包括两种情况: (i) 在解复用的时候, 由于 WDM 的隔离度有限, 相邻信道中的光波串扰进信号光信道并与信号光波重合; (ii) 信号光与瑞利散射光的重合. 对于第 (i) 种情况, 光脉冲从激光器输出之后, 由于 WDM_1 的隔离作用, 进入信号光信道的其他波长的光功率相对于信号光功率低, 以隔离度为 40 dB 的 WDM 为例, 进入信号光信道的其他波长的光功率将是信号光功率的 $1/10^4$. 在光子返回到 Bob 端时, 解码之后, 在 WDM_2 和 WDM_3 解复用时, 同样由于 WDM 的隔离作用, 进入到信号光通道的光功率比信号光功率再低四个量级. 因此进入到探测器的串扰光的功率是信号光功率的 $1/10^8$, 故由此引入的影响可以忽略不计. 对于第 (ii) 种情况, 同样由于 WDM 信道隔离度的影响, 相邻信道波长产生的瑞利散射光串扰到信号光信道时将存在衰减. 以隔离度为 40 dB 隔离度的 WDM 为例, 串扰进信号光信道的瑞利散射光功率就会衰减 40 dB. 因此, 只需通过 VOA_1 调节入射光功率, 瑞利散射光功率就可以降低到很小的值 [23], 而串扰进信号光信道的瑞利散射光功率对系统的影响也会更小.

2) 相位调制器对不同波长光脉冲调制引起的误码. 对于不同波长的光脉冲, 相位调制器在调制相同的相位时, 所需要的调制电压不同. 对于不同波长的精确相位调制, 可以采用以下两种方法. (i) 精确测量对各波长调制不同相位时, 相位调制器所需要的调制电压, 通过控制加载不同的电压来实现相位的精确加载. 采用这种方法, 在波长变化的时候, 相位调制器的电压就必须能够快速进行变换, 以便精确地调制到该波长所需的相位. (ii) 取中间波长为基准波长, 测量该波长调制不同相位时加载的电压, 并定为基准电压. 在调制相位时, 不论是哪个波长都采用基准电压进行调制. 这种方法虽然引入了一定的误码, 但是不需要受制于外部控制系统的性能, 更易实现高速的通信. 下面就对该方法引入的误码进行分析.

以铌酸锂相位调制器为例, 相位调制的关系式为

$$\varphi = \frac{2\pi}{\lambda}\left[(n_{\mathrm{o}} - n_{\mathrm{e}})L - \frac{LV}{2d}(n_{\mathrm{o}}^3\gamma_{13} - n_{\mathrm{e}}^3\gamma_{33})\right]$$

$$= \frac{2\pi L}{\lambda}(n_{\mathrm{o}} - n_{\mathrm{e}}) - \frac{\pi LV}{\lambda d}(n_{\mathrm{o}}^3\gamma_{13} - n_{\mathrm{e}}^3\gamma_{33}),$$

$n_{\mathrm{o}}, n_{\mathrm{e}}$ 分别为晶体对 o 光与 e 光的折射率, L 表示晶体的长度, d 表示电极宽度, γ_{13}, γ_{33} 为晶体的电光张量, 只与晶体材料有关.

方程的第一项是由于晶体本身对光信号产生的相位延迟; 第二项是由于电光晶体在加载电压之后对光信号引入的相位变化. 方程中第二项与调制电压有关.

若只考虑方程的第二项, 取中间波长 λ_0 为基准波长, 其他波长表示为 λ_n, $n = \pm1, \pm2, \pm3, \cdots$. 可以测得对基准波长 λ_0 调制不同相位时对应的调制电压如表 2 所示.

若使用上述的四个电压调制其他波长 λ_n 时, 调制之后的相位如表 3 所示.

表 2 对基准波长 λ_0 调制不同相位对应的调制电压

	0	$\frac{\pi}{2}$	π	$\frac{3\pi}{2}$
λ_0	$V_0 = 0$	$V_{\pi/2} = \frac{d\cdot\lambda_0}{2L(n_{\mathrm{e}}^3\gamma_{33} - n_{\mathrm{o}}^3\gamma_{13})}$	$V_{\pi} = \frac{d\cdot\lambda_0}{L(n_{\mathrm{e}}^3\gamma_{33} - n_{\mathrm{o}}^3\gamma_{13})}$	$V_{3\pi/2} = \frac{3d\cdot\lambda_0}{2L(n_{\mathrm{e}}^3\gamma_{33} - n_{\mathrm{o}}^3\gamma_{13})}$

表 3 波长 λ_n 调制的相位

	$V_0=0$	$V_{\pi/2}=\dfrac{d\cdot\lambda_0}{2L(n_{\rm e}^3\gamma_{33}-n_{\rm o}^3\gamma_{13})}$	$V_{\pi}=\dfrac{d\cdot\lambda_0}{L(n_{\rm e}^3\gamma_{33}-n_{\rm o}^3\gamma_{13})}$	$V_{3\pi/2}=\dfrac{3d\cdot\lambda_0}{2L(n_{\rm e}^3\gamma_{33}-n_{\rm o}^3\gamma_{13})}$
λ_0	0	$\dfrac{\pi}{2}$	π	$\dfrac{3\pi}{2}$
λ_n	0	$\dfrac{\lambda_0}{\lambda_n}\cdot\dfrac{\pi}{2}$	$\dfrac{\lambda_0}{\lambda_n}\cdot\pi$	$\dfrac{\lambda_0}{\lambda_n}\cdot\dfrac{3\pi}{2}$

由此可以看出, 当对不同的波长都采用基准波长的调制电压调制时, 将不能得到与基准波长相同的相位. 在干涉叠加时有

$$\begin{aligned}\Delta\varphi=&\left[\frac{2\pi L}{\lambda}(n_{\rm o}-n_{\rm e})-\frac{\pi LV_2}{\lambda d}(n_{\rm o}^3\gamma_{13}-n_{\rm e}^3\gamma_{33})\right]\\&-\left[\frac{2\pi L}{\lambda}(n_{\rm o}-n_{\rm e})-\frac{\pi LV_1}{\lambda d}(n_{\rm o}^3\gamma_{13}-n_{\rm e}^3\gamma_{33})\right]\\=&\frac{\pi LV_2}{\lambda d}(n_{\rm e}^3\gamma_{33}-n_{\rm o}^3\gamma_{13})\\&-\frac{\pi LV_1}{\lambda d}(n_{\rm e}^3\gamma_{33}-n_{\rm o}^3\gamma_{13})\\=&\varphi_2-\varphi_1.\end{aligned}$$

对于 λ_0,

$$\begin{aligned}\Delta\varphi&=\varphi_0-\varphi_0=\varphi_{\pi/2}-\varphi_{\pi/2}=\varphi_{\pi}-\varphi_{\pi}\\&=\varphi_{3\pi/2}-\varphi_{3\pi/2}=0,\\\Delta\varphi&=\varphi_{\pi}-\varphi_0=\varphi_{3\pi/2}-\varphi_{\pi/2}=\pi.\end{aligned}$$

而对于 λ_n, 假设各调制的相位用 φ'_{φ} 表示, 则有

$$\begin{aligned}\Delta\varphi'&=\varphi'_0-\varphi'_0\\&=\varphi'_{\pi/2}-\varphi'_{\pi/2}=\varphi'_{\pi}-\varphi'_{\pi}\\&=\varphi'_{3\pi/2}-\varphi'_{3\pi/2}=0,\\\Delta\varphi'&=\varphi'_{\pi}-\varphi'_0=\varphi'_{3\pi/2}-\varphi'_{\pi/2}=\frac{\lambda_0}{\lambda_n}\cdot\pi.\end{aligned}$$

在单光子干涉中, 由于相位偏差引入的误码率 [12] 可以表示为: $\mathrm{QBER}_{\mathrm{opt},\Delta\varphi}=\sin^2\dfrac{\Delta\Phi}{2}$, 其中, $\Delta\Phi=\Delta\varphi'-\Delta\varphi$ 为相位偏差.

所以,

$$\begin{aligned}\mathrm{QBER}_{\mathrm{opt},\Delta\varphi}&=\sin^2\frac{\Delta\Phi}{2}=\sin^2\frac{\Delta\varphi'-\Delta\varphi}{2}\\&=\sin^2\frac{\dfrac{\lambda_0}{\lambda_n}\cdot\pi-\pi}{2}\\&=\sin^2\left(\frac{\lambda_0}{\lambda_n}-1\right)\cdot\frac{\pi}{2}.\end{aligned}$$

由上式可知, 系统由于相位偏差引入的误码率与密钥分发的波长间隔有关. 例如, 若使系统由相位偏差引入的误码率 $\mathrm{QBER}_{\mathrm{opt},\Delta\varphi}\leqslant10^{-2}$, 我们可以控制系统中使用的波长与基准波长的间隔: 当波长比基准波长长 $\Delta\lambda$ 时, $\Delta\lambda\leqslant105$ nm; 当波长比基准波长短 $\Delta\lambda$ 时, $\Delta\lambda\leqslant93$ nm. 只要在上述的波长间隔之内选择波长来进行多波长量子密钥分发, 都不会引入大于 10^{-2} 的误码.

4 总 结

我们提出了一种新的产生多波长脉冲的方案, 实现了高效的双向量子密钥分发. 方案中使用了 WDM 进行滤波, 产生多波长脉冲, 采用单个探测器探测两个波长的干涉信息, 减少了因探测器暗计数引起的误码. 本文还分析了不同波长相位调制时由调制相位差别引入的误码, 以 $\mathrm{QBER}_{\mathrm{opt},\Delta\varphi}\leqslant10^{-2}$ 为例, 得出了最大波长间隔为 93 nm, 只要在这个范围内选取波长, 就可以实现低误码的传输. 该方案在继承了 “即插即用” 系统高稳定性的基础上, 采用多个波长脉冲串进行连续通信, 提高了效率, 且系统采用单个光源, 消除了多激光器系统引起的边信道攻击的缺陷, 为 “即插即用”QKD 系统的实用化提供了参考.

[1] Bennett C H, Brassard G 1984 *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, New York: IEEE 175

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

[3] Bennett C H, Brassard G, Mermin N D 1992 *Phys. Rev. Lett.* **68** 557

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

[5] Zhou N R, Zeng G H, Gong L H, Liu S Q 2007 *Acta Phys. Sin.* **56** 5066 (in Chinese) [周南润, 曾贵华, 龚黎华, 刘三秋 2007 物理

学报 **56** 5066]
[6] Zhou N R, Wang L J, Ding J, Gong L H 2010 *Physica Scripta* **81** 045009
[7] Zhou N R, Wang L J, Ding J, Gong L H 2010 *Int. J. Theor. Phys.* **49** 2035
[8] Inoue K, Waks E, Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[9] Mo X F, Zhu B, Han Z F, Gui Y, Guo G C 2005 *Opt. Lett.* **30** 19
[10] Gobby C, Yuan Z L, Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[11] Hu H P, Zhang J, Wang J D, Huang Y X, Lu Y 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]
[12] Wang J D, Lu W, Zhao F, Liu X B, Guo B H, Zhang J, Huang Y X, Lu Y Q, Liu S H 2008 *Acta Phys. Sin.* **57** 4214 (in Chinese) [王金东, 路巍, 赵峰, 刘小宝, 郭邦红, 张静, 黄宇娴, 路轶群, 刘颂豪 2008 物理学报 **57** 4214]
[13] Donald S B, William P R 2002 *New J. Phys.* **4** 42.1
[14] Chen W, Han Z F, Mo X F, Xu F X, Wei G, Guo G C 2008 *Chin. Sci. Bull.* **53** 1310
[15] Wang J D, Qin X J, Wei Z J, Liu X B, Liao C J, Liu S H 2010 *Acta Phys. Sin.* **59** 281 (in Chinese) [王金东, 秦晓娟, 魏正军, 刘小宝, 廖常俊, 刘颂豪 2010 物理学报 **59** 281]
[16] Zhang L J, Wang Y G, Yin Z Q, Chen W, Yang Y, Zhang T, Huang D J, Wang S, Li F Y, Han Z F 2011 *Chin. Sci. Bull.* **56** 2305
[17] Muller A, Herzog T, Huttner B, Tittel W, Zbinden H, Gisin N 1997 *Appl. Phys. Lett.* **70** 793
[18] Stucki D, Gisin N, Guinnard O, Ribordy G, Zbinden H 2002 *New J. Phys.* **4** 41.1
[19] Honjo T, Inoue K 2005 *Jpn. J. Appl. Phys.* **44** 6550
[20] Peng X, Jiang H, Guo H 2008 *J. Phys.* B: *At. Mol. Opt. Phys.* **41** 085509
[21] Antia L L, Christian K 2007 *Opt. Express* **15** 9388
[22] Sebastian N, Martin F, Tobias S M, Henning W, Harald W 2009 *New J. Phys.* **11** 065001
[23] Lee S H, Jeong K H, Kim S H, Kin K H 2008 *J. Korean Phys. Soc.* **52** 5

A new multi-wavelength two-way quantum key distribution system with a single optical source*

Yue Xiao-Lin[1)2)] Wang Jin-Dong[1)2)†] Wei Zheng-Jun[1)2)]
Guo Bang-Hong[1)2)] Liu Song-Hao[1)2)]

1) (*Laboratory of Nanophotonic Functional Materials and Devices, School of Information and Photoelectronic Science and Engineering, South China Normal University, Guangzhou* 510006, *China*)

2) (*Laboratory of Quantum Information Technology, South China Normal University, Guangzhou* 510006, *China*)

(Received 21 February 2012; revised manuscript received 15 March 2012)

Abstract

Low-efficiency is an important issue in "plug and play" quantum key distribution system for practical application. The inefficient reasons of system and the current solutions are analyzed. And then a new quantum key distribution scheme with multi-wavelength pulses is proposed, in which a broadband optical source and the WDMs are combined to generate the optical pulses with four wavelengths. Moreover, the WDMs can also be used as a filter to extract the signal in the proposed scheme. Compared with other schemes, this scheme is highly stable, more securate and independent of the response speed of the control systems. The scheme can be used in high efficiency "plug and play" quantum key distribution system in practice.

Keywords: quantum cryptography, bidirectional system, rayleigh scattering, multi-wavelength

PACS: 42.79.Sz, 03.67.Dd, 03.67.Hk

* Project supported by the Major Research Plan of the National Natural Science Foundation of China (Grant No. 91121023), the National Natural Science Foundation of China (Grant Nos. 61108039, 60978009), and the National Basic Research Program of China (Grant No. 2011CBA00200).

† E-mail: wangjd@scnu.edu.cn