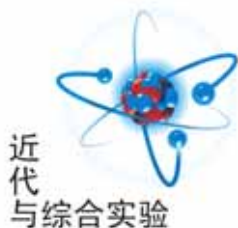


文章编号:1005-4642(2020)06-0001-08



基于液晶电光效应的量子密钥分发演示实验

齐雅静[†], 车修平[†], 孙梦琳, 白在桥

(北京师范大学物理学系, 北京 100875)

摘要: 设计了低成本演示量子密钥分发的 BB84 协议实验. 利用半导体激光器替代单光子发送信息, 并使用液晶盒调制激光的偏振状态. 通过编程 Arduino 单片机, 实现了发送端偏振态与接收端偏振基的随机选择. 采用外同步方式, 在保证无误码的前提下, 信号传输速率可达 25 Hz. 该实验将光的偏振和液晶的电光效应等大学物理实验传统教学内容与量子保密通信紧密结合, 有助于学生了解科学前沿知识.

关键词: 量子密钥分发; BB84 协议; 液晶; 电光效应; Arduino

中图分类号: TN918; O753. 2

文献标识码: A

DOI: 10.19655/j.cnki.1005-4642.2020.06.001

保密通信的基本原理是采用密钥将甲方要发送的信息加密, 再由乙方采用密钥从密文中提取信息. 传统密钥的缺点是通信双方难以判断密码是否已被窃听者复制过, 而量子保密通信以单量子态作为信息载体, 通信双方通过量子通信建立起共享密钥进行加密, 量子力学的不确定性原理和不可克隆原理保证了密钥的无条件安全性^[1].

量子密码学最初由 Stephen Wiesner 提出. 1984 年, Charles Henry Bennett 和 Gilles Brassard 提出了量子密钥分发协议: BB84 协议^[2]. 随后 B92 协议和 EPR 协议出现. 1989 年, Charles Henry Bennett 和 Gilles Brassard 进行了基于 BB84 协议的量子密钥分发实验^[3]. 量子密码通信迅速发展, 至今已搭建起上百公里接近实用的量子密钥传输系统. 2007 年在波士顿建立 10 节点量子密码网络. 2008 年, 剑桥大学与东芝合作的实验实现了在 20 km 光纤成码率达 1.02 Mbit/s 的量子密钥分发, 并且 100 km 光纤的成码率达到了 10.1 kbit/s^[4]. 我国对量子通信领域的研究亦十分重视, 中国科学技术大学潘建伟小组在 2008 年和 2009 年分别搭建了 3 节点和 5 节点的量子保密通信网, 于 2010 年利用诱骗态方法实现了距离超过 200 km 的量子密钥分发^[5], 这是当

时可以达到的最远距离. 2018 年, 我国墨子号卫星的实验成果之一——中国与奥地利之间进行量子保密视频会议, 成功入选年度国际物理学领域的 10 项重大进展.

量子密码通信已进入欧美许多国家的普通大学物理教学实验课程, 但是我国高校的本科生实验教学中却很少涉及. 量子通信作为量子力学的重要应用, 应该被相关专业的本科生广泛地了解和学习的^[6]. 长春大学盖永杰等完成了基于 BB84 协议的光纤密钥分发实验^[7], 但是其实验系统需要法兰式可调衰减器和准单光子探测器等, 虽然实现了准单光子发送信息, 但是成本很高, 难以推广到普通高校的实验室; 实验时需要操作单模耦合器、光纤跳线等, 涉及背景知识较多, 而且仪器操作难度较高, 不适合本科实验教学. THORLABS 公司推出用于教学的量子密钥分发演示装置^[8]. 这套装置的一大缺点是脉冲信号的发送和偏振状态的调制都需要手动完成, 实验效率低. 另外, 该产品将信号测量装置进行封装, 这不利于学生掌握清晰完整的物理图像. 本文在这套演示装置的基础上, 提出了改进方案, 主要思路是利用液晶的电光效应, 使用 Arduino 单片机控制激光信号的发射、液晶盒对偏振状态的调制, 以及信号的接收

收稿日期: 2020-04-05; 修改日期: 2020-04-28

作者简介: 齐雅静(1999—), 女, 河北平山人, 北京师范大学物理学系 2017 级本科生.

车修平(1998—), 女, 山东东营人, 北京师范大学物理学系 2017 级本科生.

通讯作者: 白在桥(1971—), 男, 重庆人, 北京师范大学物理学系副教授, 博士, 从事理论物理研究.

E-mail: phybai@163.com

[†]: 并列第一作者, 对本文贡献相同.



和处理,实现了信号发射与接收的自动化,提高了信息的传输速率.同时该方案紧密结合了本科阶段已有的偏振和液晶方面的实验教学内容,仪器操作简易,演示效果明显,实验成本低廉.该演示实验有利于学生了解科学前沿知识,提高专业学习的兴趣.

1 实验原理

1.1 量子通信

密码学,即信息和数据的加密,一直是通信领域的基础课题之一.加密消息只有在解码密钥已经知道的情况下才有意义,但是所有经典的密码学方法都无法确保密钥最终不会被“破解”.然而,这个难题可以用量子物理学来解决.量子通信是利用量子比特作为信息载体来进行信息交互的通信技术^[9],可以利用光子的水平偏振和垂直偏振、左旋和右旋来传递信息.测不准原理和量子不可克隆定理保证了量子通信的安全性.量子密钥分发应用量子力学的基本特性,确保任何企图窃取传送中的密钥的行为都会被合法用户所发现,这是量子密钥比传统密钥分发所具有的独特优势.

1.2 BB84 协议

BB84 协议使用光子偏振角度为 $0^\circ, 90^\circ, 45^\circ, -45^\circ$ 的 4 种偏振状态编码信息.这 4 种状态表示为 $|\rightarrow\rangle, |\uparrow\rangle, |\nearrow\rangle, |\nwarrow\rangle$. 其中 $|\rightarrow\rangle$ 和 $|\uparrow\rangle$ 组合为 + 基, $|\nearrow\rangle$ 和 $|\nwarrow\rangle$ 组合为 \times 基. + 基和 \times 基都是二维希尔伯特空间的正交基.信息的发送端 Alice 使用 + 基或 \times 基发送不同偏振状态的光子,接收端 Bob 也使用 + 基或 \times 基接收光子,其

中,使用 + 基可以准确测量 0° 和 90° 的偏振态,但当其测量偏振状态为 45° 和 -45° 的光子时,将会以 50% 的概率塌缩为 0° 或 90° 的偏振态; \times 基可以准确测量 45° 和 -45° 的偏振态,但测量偏振状态为 0° 和 90° 的光子时,将会以 50% 的概率塌缩为 45° 或 -45° 的偏振态.

Alice 随机产生比特信号 0 或 1,再随机选择 + 基或 \times 基对其进行编码.例如,当使用 + 基编码信息 0 时,会发送 $|\rightarrow\rangle$ 状态的光子,编码信息 1 时则发送 $|\uparrow\rangle$ 状态的光子.同理用 \times 基编码信息 0 会产生 $|\nearrow\rangle$ 状态的光子,编码信息 1 会产生 $|\nwarrow\rangle$ 状态的光子. Bob 也会随机选择使用 + 基或 \times 基测量光子.当二者选择基相同时得到的比特信号也相同,当二者选择的基不同时,量子态会塌缩,得到正确数据的概率只有 1/2.

BB84 协议的实现需要 2 个信道:经典信道和量子信道. Alice 和 Bob 在量子信道传输光子,传输过程中 2 人独立、随机地选择基.然后在经典信道交流基的选择.保留基选择相同时的信息,作为共有的密钥,从而完成密钥分发.量子密钥的一大优点在于传输信息的 2 人可以及时发现密钥是否被窃听.如果存在窃听者 Eve,他需要截取量子信道的信息,然后将接收到的信息发送给 Bob,最后获取通信双方基的选择来获得密钥.在量子通信中,Eve 对光子进行测量时,一旦与 Alice 的基不同,势必会引起量子态的塌缩,导致信息的改变.故而 Eve 的介入必然会导致额外的误码率, Alice 和 Bob 核对少量密钥就会发现窃听者的存在并结束信息数据的传输.

Eve 存在时的数据传输示例如表 1 所示.

表 1 Eve 存在时的数据传输

Alice 发送的数据	Alice 选择的基	Alice 发送的光子	Eve 选择的基	Eve 收发的光子	Bob 选择的基	Bob 收到的数据	2 人核对部分密钥	密钥核对结果	Eve 是否存在
0	\times	45°	+	90°	\times	0	\checkmark	0,0	否
1	+	90°	\times	45°	+	0	\checkmark	1,0	是
1	\times	45°	\times	45°	\times	1	\checkmark	1,1	否
0	+	0°	+	0°	\times	1	\times		不确定
1	\times	45°	+	90°	+	1	\times		不确定
0	+	0°	\times	-45°	+	1	\checkmark	0,1	是
0	\times	45°	\times	45°	+	1	\times		不确定
1	+	90°	\times	45°	\times	0	\times		不确定

1.3 液晶的电光效应

液晶的电光效应是指液晶在外电场作用下分子排列状态发生变化,从而引起液晶的光学性质也随之改变的电对光的调制现象^[10].

液晶具有光学各向异性,即双折射效应,可以使入射光的偏振状态发生变化.以液晶长轴方向为 x 方向,液晶短轴方向为 y 方向,光垂直于长短轴所在的平面入射,为 z 方向,则入射偏振光在 x 和 y 方向上的电矢量强度可以表示为

$$\begin{aligned} E_x &= E_0 \cos \theta \cos(\omega t - k_1 z), \\ E_y &= E_0 \sin \theta \cos(\omega t - k_2 z), \end{aligned} \quad (1)$$

其中, E_0 为电场强度, θ 为入射光的偏振方向与分子长轴夹角, ω 为光的角频率, $k_1 = \frac{\omega n_1}{c}$, $k_2 = \frac{\omega n_2}{c}$. 当入射光平行或垂直于液晶分子长轴时, E_x 或 E_y 有一方为 0, 即出射光仍为线偏振光.

液晶的介电各向异性表现为液晶分子在电场的作用下取向会发生改变(图 1). 外电场作用在平行和垂直于分子长轴方向, 感生电极矩的力矩大小分别为

$$\begin{aligned} M_1 &= E p_1 \sin \beta = \alpha_1 E^2 \sin \beta \cos \beta, \\ M_2 &= E p_2 \sin \beta = \alpha_2 E^2 \sin \beta \cos \beta, \end{aligned} \quad (2)$$

其中, E 为外加电场强度, p_1 和 p_2 分别为平行和垂直液晶分子长轴方向的感生电极矩, α_1 和 α_2 分别为外电场平行和垂直于液晶分子长轴时分子的极化率, β 为外电场与液晶分子长轴方向夹角. 由此可知, 垂直和平行分子长轴方向的极化率大小决定液晶分子趋向平行于电场还是垂直于电场.

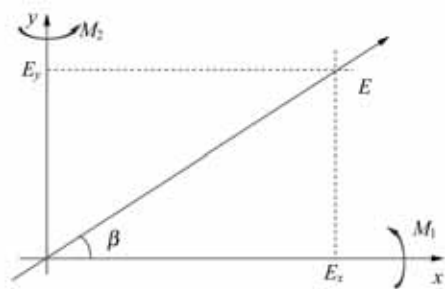


图 1 电场对液晶分子的取向

液晶盒由 2 块镀有透明导电薄膜的玻璃基片和封装在其中的液晶材料组成. 玻璃的表面经过特殊处理, 液晶分子的排列将受到玻璃表面的影响^[11]. 如果上下 2 块基片取向之间存在夹角, 2 块基片之间的液晶分子将均匀扭曲, 示意图如 2 所示.

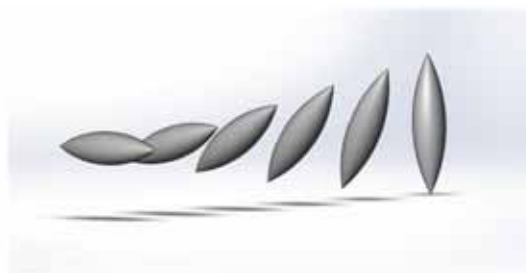


图 2 2 块基片间液晶分子均匀扭曲示意图

由于液晶的双折射效应, 当 1 束线偏振光平行(或垂直)液晶盒上基片处液晶分子长轴方向入射时, 将会以平行(或垂直)液晶盒下基片处分子长轴方向出射, 即偏振光的偏振方向会转过某角度, 该角度称之为旋光角. 由液晶的介电各向异性可知, 液晶盒的旋光角度受电场大小影响. 实验需要测旋光角度为 0° 和 45° 对应的电压 $V(0^\circ)$ 和 $V(45^\circ)$. 此外, 为了保证线偏振光经过液晶盒后仍为线偏振光, 需要调整液晶盒的摆放角度, 使入射光的偏振方向平行或垂直于分子长轴方向.

2 实验方案与实验装置

实验仪器包括激光器(可调制, 2 台)、偏振分束器(简称 PBS, 2 个)、液晶盒(2 个)、信号发生器、单片机(2 台)和光电探测器(2 台)等.

实验使用的液晶盒为自动变光焊工护目镜的镜片(使用时要剥去前后的偏振片), 其结构如图 3 所示. 实验装置示意图如图 4 所示, 实验装置主要分为 4 个模块: Alice 发射端、Bob 接收端、同步信号和经典信道.

Alice 发射端实现了 0° , 45° , -45° , 90° 4 种偏振状态的制备, Bob 接收端接收 Alice 端的信号并作出判断, 二者经过经典信道共享基的选择, 经过筛选得到密钥. 整个过程由同步信号实现 Alice 和 Bob 的同步发送和接收.

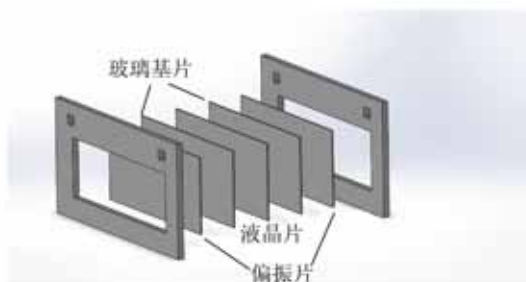


图 3 液晶盒的结构示意图

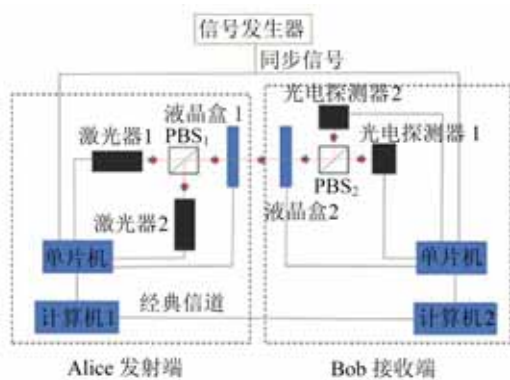


图4 实验装置示意图

2.1 Alice端的实现

如图4中的Alice模块,以受单片机控制的激光器1和2、液晶盒1以及 PBS_1 作为发送信号的Alice端.借助 PBS_1 调整光路,使得激光器1和2从相互垂直的方向射入 PBS_1 后,在主光路方向上得到2束偏振方向夹角为 90° 、光强大小相当的线偏振光.因此,只需要控制激光器1或者激光器2发光就可以得到 0° 或 90° 的线偏振光. Alice的程序框图如图5所示.

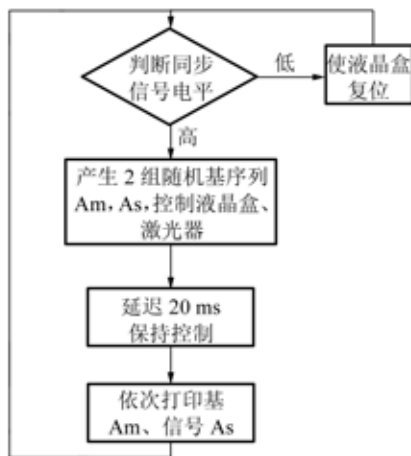


图5 Alice程序框图

通过调节液晶盒1的电压值,使其分别实现对入射光偏振方向改变 0° 和 45° .激光器与液晶盒效果叠加得到偏振角度为 $0^\circ, 45^\circ, 90^\circ$ 和 -45° 的4种线偏振光,其中 0° 和 90° 代表Alice选择+基发送信号, 45° 和 -45° 代表选择×基发送信号.每个偏振状态对应的信号如表2所示.

实验中,单片机产生2组0/1随机信号,一组为 A_m ,用于控制液晶盒的电压,决定基的选择,其中0代表+基,给液晶盒施加 $V(0^\circ)$,1代表×基,给液晶盒施加 $V(45^\circ)$,Bob的基选择同理;另

一组为 A_s ,用于控制激光器选择来决定信号发送.同时将这2组随机信号打印在Alice端的Arduino串口显示器中,以供经典信道的交流.

表2 Alice发送的数据

发送信号	Alice基	偏振角度	激光器	液晶盒电压
0	+	0°	1	$V(0^\circ)$
0	×	-45°	1	$V(45^\circ)$
1	+	90°	2	$V(0^\circ)$
1	×	45°	2	$V(45^\circ)$

2.2 Bob端的实现

如图4的Bob模块,以受液晶盒控制的光电探测器1和2、液晶盒2及 PBS_2 为接收信号的Bob端.通过单片机调节液晶盒2的电压值,使偏振方向改变 0° 和 45° ,搭配 PBS_2 ,把入射光分解到水平垂直方向和 $\pm 45^\circ$ 方向.其中选择 0° 代表以+基接收信号, 45° 代表以×基接收信号.

利用光电探测器和单片机比较 PBS_2 分解得到的2束偏振光的光强.光电探测器 D_1 沿光路方向, D_2 垂直于光路方向(反射光强),比较对应的光强 V_1 (沿光路方向)和 V_2 (垂直光路方向), V_1 大表示接收到信号0, V_2 大表示接收到信号1. Bob的程序框图如图6所示.

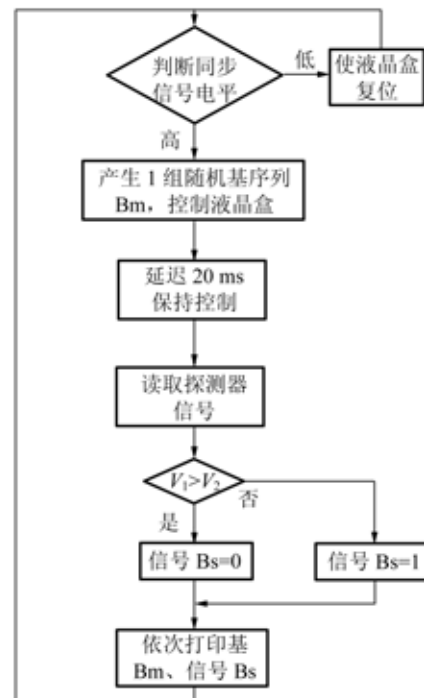


图6 Bob程序框图

单片机产生随机的 Bob 基序列 B_m , 通过单片机控制液晶盒电压, 并读取光电探测器数据实现信号接收. 例如, 当 Alice 选择 $+$ (0° 或 90°), Bob 选择 \times , 此时液晶盒使线偏振光再偏转 45° , 结合 PBS_2 将光分解到水平方向和垂直方向, 结合效果相当于直接把 Alice 的光在 \times 方向分解. 2 个分量光强大小一致, 电探测器接收到的信号大小相差无几, 将会以 50% 的概率判断为信号 0, 50% 的概率判断为信号 1, 以此来模拟量子态的塌缩. 将 Bob 端随机信号与光探测器接收并判断得到的信号打印在串口显示器. 所有情况列举如表 3 所示.

表 3 Bob 的接收情况

发送信号	Alice 基	Bob		接收信号
		基	电压较大	
0	$+(0^\circ)$	$+$	V_1	0
		\times	V_1/V_2	0/1
	$\times(-45^\circ)$	$+$	V_1/V_2	0/1
		\times	V_1	0
1	$+(90^\circ)$	$+$	V_2	1
		\times	V_1/V_2	0/1
	$\times(45^\circ)$	$+$	V_1/V_2	0/1
		\times	V_2	1

2.3 同步信号的实现

使用信号发生器产生 25 Hz 的方波信号, 同时传输给 Alice 和 Bob. 当 Alice 和 Bob 探测到方波的上升沿时分别开始发射和接收信号, 当二者探测到方波的下沿时停止发射与接收信号, 并将液晶盒的电压调整为 0, 使液晶盒复位. 再次探测到上升沿时重新开始, 如此往复, 达到信号发射与接收的同步.

2.4 经典信道的实现

通过将 Alice 与 Bob 导出的随机信号共享, 对两者数据进行简单处理, 找到二者同步开始的第 1 组信号, 并将之后产生的信号一一对应, 检验收发信号的一致性: 在理想情况下, 如果 Alice 端与 Bob 端选择基相同时收发信号一致, 且二者选择的基不同时收发信号有 50% 的概率一致.

3 实验数据处理与分析

3.1 液晶电光响应曲线的测量

改进实验的关键是利用液晶盒将线偏振光的

偏振角度转过 0° 或 45° , 且仍然保持线偏振性, 所以既需要找到合适的摆放角度使入射光偏振方向垂直或平行于液晶的长轴方向, 又需要找到使偏振方向转过 0° 和 45° 的电压大小 $V(0^\circ)$ 和 $V(45^\circ)$. 测量光路如图 7 所示, 测量结果如图 8 所示. 线偏振光的偏振面转过角度 $(\alpha - \alpha_0)$ 与所加电压关系如图 8 所示. 从图 8 可看到, 当液晶盒所加电压超过某一电压值 (约 3.50 V) 就对偏振光失去旋光作用, 方便起见, 选取 4.50 V 作为 $V(0^\circ)$. 测得 2 个液晶盒的摆放角度 γ 以及所加电压如表 4 所示.

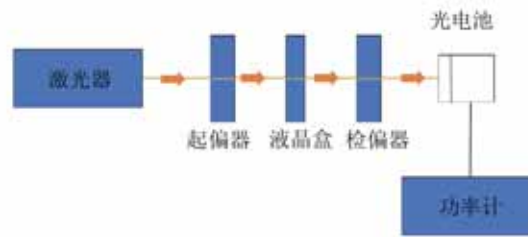


图 7 液晶的电光响应曲线测量装置示意图

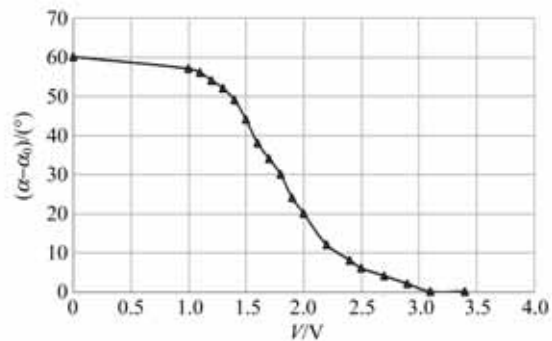


图 8 液晶的电光响应曲线

表 4 实验所用液晶盒的电压配置及摆放角度

液晶盒	$V(45^\circ)/V$	$V(0^\circ)/V$	$\gamma/(^\circ)$
1	1.46	4.50	156
2	1.80	4.50	235

3.2 液晶电光响应时间的测量

当施加在液晶盒上的电压改变时, 液晶改变其排列方式所需要的时间称为响应时间. 量子密钥分发演示实验的重要改进方向是提高传输速率, 在本实验中传输速率主要受液晶电光效应响应时间的限制. 液晶响应时间的测量光路如图 9 所示.

给液晶盒施加 12.5 Hz 的方波电压, 测量通

过液晶和检偏器后光强随时间的变化,得到的响应时间曲线如图 10 所示.

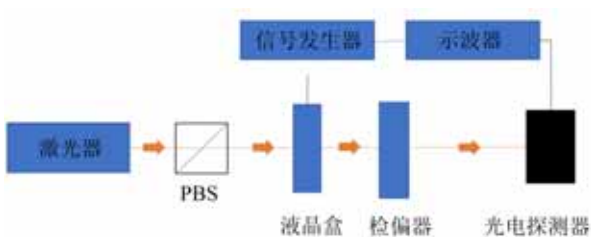


图 9 液晶的响应时间测量装置示意图



图 10 液晶的响应时间曲线

测量方波上升沿到光强达到最大值 90% 的时间 T_{on} , 下降沿到光强为最大值 10% 的时间 T_{off} . 测得 $T_{on} = 12 \text{ ms}$, $T_{off} = 13.2 \text{ ms}$. 所以理论上本实验能达到的传输速率约为 30 Hz.

3.3 加压时间对液晶电光响应曲线的影响

在实验过程中当液晶盒加电压一段时间后, 同电压下同样的线偏振光经过液晶盒出射光的偏振角度会发生改变, 即随着时间增加, 液晶的电光响应曲线会逐渐改变. 测量使偏振方向转过 45° 对应电压随时间的变化, 如图 11 所示.

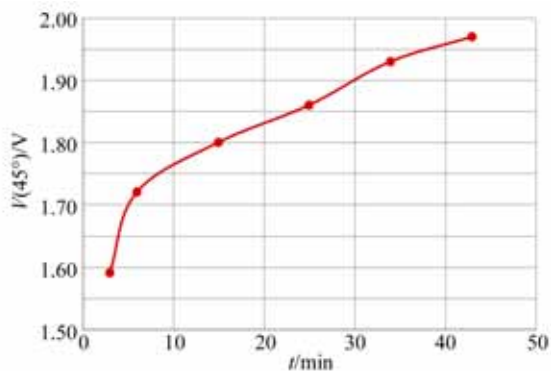


图 11 液晶盒 $V(45^\circ)$ 随时间变化曲线

可见使 $V(45^\circ)$ 发生稍明显变化的时间为 min 量级, 对于传输过程来说是相当长的一段时

间, 所以对信号传输的影响不大. 但为保证实验的准确性, 减小误码率, 使液晶盒在同步信号的下降沿到上升沿时间段内不加电压, 恢复状态.

3.4 实验结果与分析

摆放液晶盒并完成 Arduino 程序中的各液晶盒电压设置. 运行程序, 打开同步信号发生器控制二者同步开始工作, 待得到足够多的信号以后关闭同步信号发生器, 把 2 个串口输出导入 Excel 文件, 汇总整理截取部分数据如图 12 所示. 其中 0 和 1 分别代表 + 基和 \times 基. 从图 12 可看出, 实验得到的一段密钥为: 01000100101……当然, 在实际量子密钥分发时, Alice 和 Bob 只对比每次使用的基, 而信号需要各自保存, 不会通过经典信道进行比较(除了少量用于核对的信号之外).

	S	T	U	V	W
1	Alice的基	Bob的基	Alice的信号	Bob的信号	核对情况
2	1	0	1	0	wrong
3	0	1	0	0	wrong
4	0	0	0	0	0
5	1	0	0	0	wrong
6	0	1	0	1	wrong
7	1	1	1	1	1
8	1	0	1	1	wrong
9	1	0	1	0	wrong
10	0	0	0	0	0
11	1	0	0	0	wrong
12	0	0	0	0	0
13	0	0	0	0	0
14	0	1	1	0	wrong
15	1	0	0	0	wrong
16	0	0	1	1	1
17	0	0	0	0	0
18	0	0	0	0	0
19	1	1	1	1	1
20	0	1	0	0	wrong
21	0	1	1	1	wrong
22	1	0	0	0	wrong
23	0	0	0	0	0
24	0	0	1	1	1

图 12 处理数据

实验过程中在 158.36 s 内发送并接收成功了 3 953 组二进制信号, 统计结果如表 5 所示. 按照可能的情况, 数据可以分为 3 类:

第 1 类是双方使用基相同, 接收的信号与发送的信号也相同. 这类有效数据共有 1 964 组.

第 2 类是双方使用基相同, 但接收的信号与发送的信号不同. 这类错误信号计数为 0. 因此本装置的成码率约为 12.5 bit/s, 误码率为 0.

第 3 类是双方使用的基不相同, 这类无效传输数据共有 1 989 组. 在无效传输信号中, 发送与接收信号相同的有 962 组, 不相同的有 1 027 组, 比例接近 1 : 1, 总体上较好地模拟了量子态塌缩过程. 不过看具体的每个态, 情况并不如此. 比

如 Alice 在 + 基发送 1 时, Bob 在 × 基上收到 0 和 1 的次数分别是 365 和 121, 与理想情况相差很大. 原因可能是激光器 2 入射 PBS_1 的角度调节有误差. 更容易出问题的是, 在程序中简单地比较 2 个光传感器输出的大小决定读出信号是 0 或 1, 这样做只是依赖测量的随机误差使结果随机化. 如果改进为当 2 个光传感器输出相差小于某阈值时, 程序就按 0.5 的概率随机输出 0 或 1, 应该可以更好地模拟量子塌缩.

表 5 统计结果

传输结果	As	Am	Bm	Bs	数目	合计
有效传输	0	0	0	0	493	1 964
	1	1	1	1	518	
	0	1	1	0	461	
	1	0	0	1	492	
错误传输	0	0	0	1	0	0
	1	0	0	0	0	
	1	1	1	0	0	
	0	1	1	1	0	
无效传输	0	0	1	0	262	1 989
	0	0	1	1	232	
	1	0	1	1	121	
	1	0	1	0	365	
	0	1	0	0	242	
	0	1	0	1	255	
	1	1	0	0	175	
	1	1	0	1	337	

3.5 讨论

值得注意的是, 本实验在发送信号及接收信时由单片机产生的随机序列与真正量子密钥分发中的随机信号有本质的区别. 后者是由量子力学原理(波包塌缩)决定, 是真正的随机, 而前者只是伪随机. 另外, 量子密钥分发中使用单光子, 量子不可克隆原理保证被窃听了就一定可以被发现, 而本实验使用的激光脉冲信号是可以被复制的, 仍有被窃听的可能.

4 实验课程建议

针对本科生的近代物理实验学习情况与需求, 基于液晶电光效应的量子密钥分发演示实验的学习重点为: 了解量子通信, 学习掌握密钥分发的 BB84 协议, 探究液晶的旋光性和电光效应.

实验安排与对学生的要求:

1) 相关的学习内容应该包括: 量子通信的基本原理与发展前景, BB84 协议的相关内容, 液晶的介电各向异性、光学各向异性、电光效应与旋光性, 液晶盒的结构和使用方法.

2) 实验主要分为 2 部分. 第 1 部分是液晶相关参量的测量, 建议实验内容为测量液晶响应曲线及响应时间, 测量旋光角度分别为 0° 和 45° 对应的液晶盒加的电压和相应的摆放角度. 第 2 部分是模拟量子通信实验, 主要内容包括控制 Alice 端和 Bob 端同时运行程序, 控制信号发送与接收, 打开同步信号实现发送与接收的严格同步. 约 2 min 后结束程序, 记录数据, 在经典信道比较基的选择, 处理数据, 得出成码率和误码率. 对密钥分发过程进行评估. 建议学生根据测量结果自主搭建光路, 本实验的部分参量如液晶的 $V(45^\circ)$ 和 $V(0^\circ)$, 需要学生测量自己的液晶盒来确定, 实验中所用的同步信号的频率为 25 Hz, 学生也可以尝试自行设置, 但要考虑液晶的响应时间, 同时 Alice 和 Bob 的程序中也要做相应修改. 其他相关参量如光电探测器的具体电压等, 可以在程序中设置输出.

3) 实验的重点在于保证信号同步, 理解量子密钥分发演示实验传输速率的影响因素以及演示实验与真正的密钥分发在物理过程上的差异.

5 总结与展望

基于液晶的电光效应, 使用 Arduino 控制偏振态的调制与信号的接收, 实现了量子密钥分发实验的模拟和演示. 量子密钥分发装置成本低, 原理简单清晰, 操作简易, 演示效果明显, 适合本科生实验教学. 相较于现有 THORLABS 公司的量子密钥分发演示实验装置, 该实验将传输速率提高至 25 Hz, 而且与已有实验教学中的偏振和液晶内容承接. 该实验紧密结合了本科阶段专业课程、已有的实验教学内容以及量子信息发展的最新成果, 有利于学生更加直观地了解科学前沿. 该实验仍存在进一步完善的空间, 例如, 加入窃听者 Eve, Bob 判断信号时设定阈值来更精确地模拟量子塌缩, 选择对光偏振状态调制速度更快的材料, 等等.

参考文献:

- [1] Wootters W K, Zurek W H. A single quantum can-

- not be cloned [J]. *Nature*, 1982, 299:802-803.
- [2] Bennett C H, Brassard G. Quantum cryptography: Public key distribution and coin tossing [C]// Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing. Bangalore, 1984:175-179.
- [3] Bennett C H, Brassard G. The dawn of a new era for quantum cryptography: The experimental prototype is working ! [J]. *ACM SIGACT News*, 1989, 20(4):78-80.
- [4] Dixon A R, Yuan Z L, Dynes J F, et al. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate [J]. *Optics Express*, 2008, 16(23): 18790-18797.
- [5] Liu Yang, Chen Tengyun, Wang Jian, et al. Decoy-state quantum key distribution with polarized photons over 200 km [J]. *Optics Express*, 2010, 18(8):8587-8594.
- [6] 张子静, 王晓鸥, 霍雷, 等. 大学物理教学改革——量子通信教学浅析[J]. *大学物理*, 2019, 38(8): 54-58.
- [7] 盖永杰, 严冬, 韩家伟, 等. 基于 bb84 协议的光纤量子密钥分发实验[J]. *大学物理*, 2013, 32(10): 41-44.
- [8] Thorlabs Inc. Edu-qcry1 m-englishmanual [EB/OL]. [2020-04-05]. <https://www.thorlabs.us/thorproduct.cfm partnumber=EDU-QCRY1/M>.
- [9] 吴华, 王向斌, 潘建伟. 量子通信现状与展望[J]. *中国科学:信息科学*, 2014, 44(3):296-311.
- [10] 施善定, 黄嘉华, 李秀娥. 液晶与显示应用[M]. 上海:华东化工学院出版社, 1993.
- [11] 北京师范大学物理实验教学中心. 近代物理实验补充讲义[EB/OL]. [2020-04-05]. <http://physics.bnu.edu.cn/work/index.php>.

Quantum key distribution demonstration experiment based on the electro-optic effect of liquid crystal

QI Ya-jing[†], CHE Xiu-ping[†], SUN Meng-lin, BAI Zai-qiao

(Department of Physics, Beijing Normal University, Beijing 100875, China)

Abstract: A low-cost approach to demonstrate the BB84 protocol for quantum key distribution was designed. A semiconductor laser was used as a single-photon source, and liquid crystal cells were adopted to modify the polarization states of the photons. Two Arduino controllers were programmed to randomly pick the sender's states and the receiver's basis, respectively. The sender and receiver were synchronized with a square wave, and a transmission rate of 25 Hz without error code was realized. This experiment closely linked the traditional topics in college physics laboratory, properties of polarization and the electro-optic effect of liquid crystal, to quantum cryptography, which could help students in understanding the idea of this modern technique.

Key words: quantum key distribution; BB84; liquid crystal; electro-optic effect; Arduino

[责任编辑:任德香]