第 50 卷 第 8 期 2001 年 8 月
1000-3290/2001/50(08)/1429-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.50,No.8,August,2001

850nm 光纤中 1.1km 量子密钥分发实验*

梁 创[1)] 符东浩[2)] 梁 冰[1)] 廖 静[1)] 吴令安[1)] 姚德成[2)] 吕述望[2)]

[1)] (中国科学院物理研究所光物理开放实验室,北京 100080)

[2)] (中国科学院研究生院,北京 100039)

(2000 年 7 月 18 日收到;2000 年 11 月 17 日收到修改稿)

在 850nm 波长完成了一个全光纤量子密钥分发系统原型.该系统以单光子为信息载体,以光纤为量子信道,在通信双方建立起共享的密钥,从而完成量子密钥的分发,其安全性由量子力学基本原理——不确定性原理和量子不可克隆定理所保证.所采取的信息调制方式为相位调制,通信协议采取 BB84 协议.通信距离为 1.1km,有效数据传送速率为 3bit/s,误码率为 9% 左右.

关键词:量子密钥分发,BB84 协议,单光子,光纤

PACC:0365,4230,4250

1 引 言

经典物理学允许测量一个物体的所有性质而不对这些性质产生干扰,所以基于经典物理学的经典信道都有可能被窃听而不会被发现.这也是依赖于经典信道传送信息的经典密码学的困难所在.针对这一点,物理学家将量子力学与密码学相结合,提出量子密码技术[1].实现方法是:以单量子态为信息载体,通过量子信道在通信双方建立起共享的密钥.由量子力学的基本原理保证了量子密码技术的绝对安全性.对量子密码通信容易产生的误解主要有以下 3 点:

1. 量子密码通信传送的对象是密钥,而不是有具体信息的密文或明文.

2. 密钥产生的方式是在通信过程中,在通信双方共同作用下产生的,而不是从通信一方发往另一方.在通信结束前包括通信双方在内谁也不知道密钥到底是什么样的.

3. 量子密码技术防窃听的手段是被动的,一旦发现有人窃听就停止,而不是拒绝窃听.

量子密码通信的三大主流方案,BB84,B92 和 EPR 协议在 1992 年之后就已全部形成[2—4].量子密码技术从理论设想到今天几十公里长、接近实用的量子密钥传输系统,其发展之迅速顺应了人们对信息安全的要求[5—12].在我国,量子密码通信的研究刚刚起步.中国科学院物理研究所于 1995 年在国内首次做了演示性实验,它与 BB84 的第一次实验类似[13,14],华东师范大学用 B92 方案作了实验,但都是在自由空间中且距离较短.光纤是最具实际应用前景的传输信道,我们的工作致力于并于近期完成了国内第一个全光纤量子密码通信演示性实验.该实验的通信距离为 1.1 km,并且是国际上第一个 850 nm 波长的光纤量子密码通信实验.尽管其性能参量还不能满足实用的要求,但是该系统在成本较低的情况下完成了量子密钥分发的实验室研究.

2 实验方案

考虑到实用的意义,在光纤中建立量子信道.信息载体采用单光子,单光子源是将脉冲激光大幅度衰减产生的准单光子源——激光光源属相干光源,其光子数分布满足泊松分布,将脉冲激光衰减到平均每个脉冲 0.1 个光子时,每个脉冲含 2 个以上光子的概率仅为 0.5% .

量子密码术的信息调制方式有两种:偏振调制和相位调制.采用偏振调制时,在长距离光纤传送中光子偏振性的退化会造成误码率增加.若利用保偏光纤,则成本将大幅度上升.我们的系统采用的是相位调制编码.

检测相位信息的手段是利用干涉仪,如图 1 所

* 中国科学院院长基金(批准号:SZH9612)和国家自然科学基金(批准号:19974073)资助的课题.

示的 Mach-Zehnder(M-Z)干涉仪.下面简要阐述一下 BB84 协议.

图 1 中 Alice (A) 与 Bob (B) 各占有一个 M-Z 干涉仪的二分之一,并分别控制两臂中的相位调制器 ϕ_A、ϕ_B.A 从光分束器输入一串光脉冲,分束、合路器均为 1∶1 的.B 在合路器的两个输出口放置单光子探测器Ⅰ,Ⅱ.由于光子的干涉效应,信号光子脉冲出现在探测器Ⅰ的概率为(设初始相位为 0)

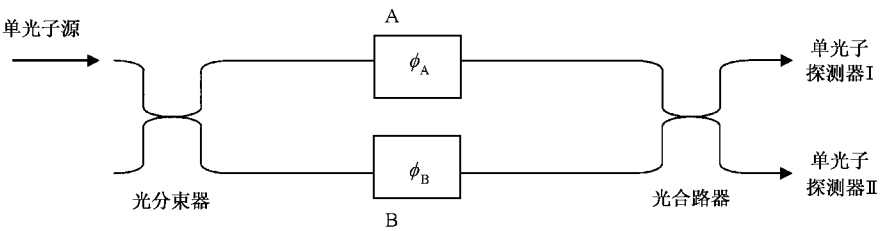

图 1 相位编码的量子密钥分发基本原理图

$$P_{\mathrm{I}} = \cos^2\left|\frac{\phi_A - \phi_B}{2}\right|, \quad (1)$$

而出现在探测器Ⅱ的概率为

$$P_{\mathrm{II}} = \sin^2\left|\frac{\phi_A - \phi_B}{2}\right|, \quad (2)$$

同时取决于两条光路.若 $\phi_B + \phi_A = \pi/2 + n\pi$($n$ 为整数)时,光子走的路径是不确定的,到达两个探测器的概率均等.A 随机选择 ϕ_A 为(0,π)或 (π/2, 3π/2) 两组基中的任一相位值,B 也独立地随机选择 ϕ_B 为两组基中的任意值并进行测量.规定 ϕ_A 为 0 或 π/2 时 A 记 0,为 π 或 3π/2 时记 1 光子到达Ⅰ时 B 记 1,到达Ⅱ时记 0.在二分之一的情况下 B 选的基会与 A 的一致,这时 B 能准确推知 A 选取的相位.双方基选的不同时,B 的测量结果是完全随机的.随后 B 在公开信道上宣布他所使用的基(不公布测量结果),A 告诉 B 哪些基选对了,双方保留基相同时对应的随机比特序列作为原始密码本.B 从原始密码本中随便抽取一部分告诉 A,供 A 确认有无窃听或错误.若确认无窃听或错误,则将剩下的数据保留作为密钥,否则抛弃所有数据.

单光子不可分割,不可采取分流的方法进行窃听.根据不确定性原理,若采取截断转发的方式则被窃听者 Eve (E)窃听过后转发的光子态将变成 E 所测得的态,必然有一定概率(具体值与 E 采取的窃听方式有关)与 A 发送的原始态不同,从而导致在 A,B 的通信系统中引起明显的误码而被发现.通过理论计算可以确定一个判别标准 Q,当误码率小于 Q 时认为不存在窃听.我们将 Q 选为 12% .

密钥是由 A,B 双方在传送过程中共同产生的,A 事先也不知道密钥会是怎样的,所以没有密码本传递过程中丢失的危险.即使因损耗等原因造成光子丢失也无关紧要,只是损失了一些比特.所产生的密码本属一次性便笺(vernam)型,但 A,B 可随时产生,不必存放大量数据,也不必担心密码本的丢失.

3 实验装置

我们的全光纤相位调制量子密钥分发系统分如下几部分.

光源为中心波长为 850nm、连续功率为 1mW 的带尾纤输出的单模半导体激光器.自制脉冲驱动电路,得到宽度为 100ns、重复频率在 100kHz—1MHz 内可调的脉冲激光.每一个脉冲中有 100pW 能量的光输出.考虑到每一个光子的能量为

$$h\nu = 6.63 \times 10^{-34} \times 3 \times 10^{8}/850 \times 10^{-9}\,\mathrm{W} = 2.34 \times 10^{-19}\,\mathrm{W}.$$

每次脉冲中的光子个数约为 4×10^{8} 个.将这束脉冲衰减 90dB,以保证每个脉冲中的平均光子数少于 0.1.

相位调制器是自制的压电陶瓷(PZT)光纤调制器.它的优点是,全光纤化节省了昂贵的光纤耦合技术,插入损耗低,缺点是带宽窄、调制速率较低.它导致了我们系统最终有效传输速率较低,并直接与系统误码率相联系.将所制作的 PZT 相位调制器置于等臂长 M-Z 干涉仪中,测得它们的半波电压为 3V 左右 加上 800Hz 的方波调制,可观测到的最好干涉对比度为 90% 以上.

光电倍增管在 850 nm 波段的量子效率极低，约为 0.08%，而硅雪崩光电二极管(Si-APD)工作在盖革模式下(工作电压高于雪崩击穿电压)量子效率可达 10% 左右. 我们选择带尾纤的 EG&G 公司 C30902E 型 Si-APD 来制作单光子探测器. 使用的是加门限电平(gate)有源抑制的工作方式. 它的响应时间可由计算机控制. 为了降低噪声采用半导体三级制冷堆，使得 APD 工作在 - 50℃的温度下.

图 2 是系统的光路示意图. 其中光纤耦合器分束、合路比均为 1∶1. LD 为单模半导体激光器，F 为 90dB 光衰减系统. L1—L4 分别代表两个不等长 M-Z 干涉仪的臂长，L1，L3 为长臂，L2，L4 为短臂. L 为 1.1km 长的传输光纤. 该光路整体上看可等效为一个 M-Z 干涉系统.

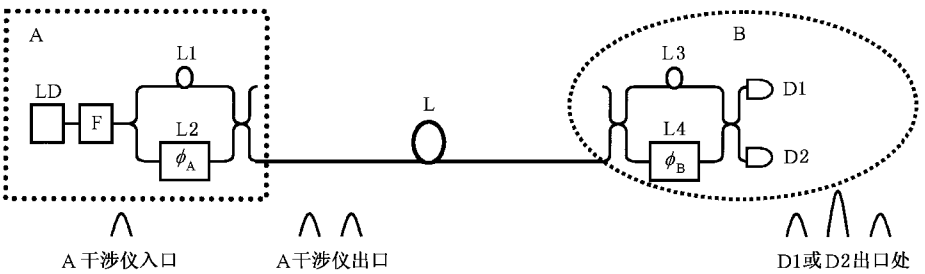

图 2　系统光路示意图

LD 为 850nm 半导体激光器；A 为衰减器，L1，L2，L3，L4 为各臂上的光纤；L 为传输光纤，ϕ_A，ϕ_B 为相位调制器；D1，D2 为单光子探测器.

在该干涉系统中，A 和 B 分别拥有完全相同的、不等臂长的 M-Z 干涉仪. 长臂和短臂的延时差 δT 远远大于光源的相干时间长度，因此在每个干涉仪中不存在干涉，只在 B 的出口处会发生干涉. 单个光子通过 A 的干涉仪后进入传输光纤的时刻有两种可能，其时间间隔为 δT. 为了便于说明，在图 2 中以两个概率幅表示，其中位于前面的表示光子走短臂的概率，位于后面的表示走长臂的概率. 经过 B 的干涉仪后，每一个概率幅又被分成两个：走短臂的和长臂的. 分别以“L2-L4”，“L2-L3”，“L1-L4”，“L1-L3”表示这 4 种时刻. 其中“L2-L4”或“L1-L3”不参与干涉，由于两个干涉仪的光程差是相等的，“L2-L3”和“L1-L4”之间发生干涉. 光子出现在“D1”的中央时刻的概率为

$$P_{D1} = \frac{1}{8}[1 + \cos(\phi_A - \phi_B)], \qquad (3)$$

而光子出现在“D2”的中央时刻的概率为

$$P_{D2} = \frac{1}{8}[1 - \cos(\phi_A - \phi_B)]. \qquad (4)$$

我们测得激光光源的相干长度优于 2cm，因此在烧制系统时精心地控制(L1 + L4)和(L2 + L3)的长度差使之小于 2cm，并且使得(L1 - L2) = (L3 - L4) = 6m. D1，D2 为 gate 方式有源抑制 Si-APD 单光子探测器. 针对光纤干涉系统非常容易受到外界扰动的影响，我们采取一些稳定系统的措施后得到系统稳定时间为 5 s 左右. 系统的电连接在此不详述，见文献[15].

我们使用两台 PC 机代表通信双方 A，B. 将半导体激光器驱动电路、相位调制器驱动电路、单光子探测器、数据处理部分等电路连接起来，模拟量子密码通信的全部过程. 整个密钥分发过程如下.

首先 A 通过公开信道告诉 B，她准备发送信息给他，B 做好接受准备后给 A 一个准备好信号. A 收到该信号之后根据时钟同步信号及由 A 方独立产生的四值随机数，向自己的 PZT 相位调制器发送调制信号，每一相位调制信号值持续 0.00125s. B 的计算机也独立地向 B 的 PZT 相位调制器发送调制信号. 在位于 B 方的 APD 单光子探测器处，可以通过计算机控制探测时间及采样时间. 探测到的信号经采样等数据处理电路后送入 B 的计算机中. 所有信号传输结束后，A 通过公开信道告诉 B 在每次同步传送时所采用的相位的基，B 对光子探测的结果进行处理，公开告诉 A 哪些脉冲的数据有效. 这些数据经安全增强处理后便成为密钥.

计算机与各部分的通讯通过 PC-1032TN 型数字 I/O，6 通道定时/计数器板实现. 两台计算机(一台 286，一台 486)之间用四根信号线、一根地线和一根时钟线构成了公开信道；光纤 M-Z 干涉系统提供量子信道. B 不仅要控制自己的相位调制器，同时还要采集探测信号，并且负担了编码的绝大部分计算工

作,所以用 486 计算机模拟 Bob.

4 实验结果与讨论

以 ϕ_0,ϕ_A,ϕ_B 分别表示系统初相位及 A 和 B 所加的调制相位.则干涉项中的相位差可表示为 $\phi_{总} = \phi_0 + \phi_A - \phi_B$.表 1 是我们在某次实验中得到的一个数据片段.前两列中以 0,1,2,3 分别表示调制相位等于 $-\pi/2$,0,$\pi/2$,π.探测到光子记 1,没探测到光子记 0,以 D1 在前 D2 在后,则可能记录到的结果为 00,01,10,11,在数据 data 列中分别以 0,1,2,3 表示.第 4 列中 Y 表示得到可用的密钥,* 表示误码.

表 1 实验中所采集到的数据片段,经过通信开始前的校准可知:ϕ_0 为 π 的整数倍

ϕ_A	ϕ_B	data	可用否(Y 表可用,* 为误码)
3	0	1	
3	1	2	Y
3	1	2	Y
0	3	1	
0	2	2	Y
0	0	3	
2	0	2	Y
1	0	1	
1	0	2	
2	2	2	Y
2	0	1	*
1	0	2	
1	2	1	
0	3	2	
0	2	2	Y
2	0	2	Y
2	0	2	Y
0	0	1	Y
3	0	1	
0	0	1	Y

实际通信中 ϕ_A,ϕ_B 是不可能事先知道的,这里为了简单起见将 ϕ_A,ϕ_B 及探测结果同时列出,并进行分析以验证实验的结果.在实际通信中的验证过程会复杂得多.依据 BB84 协议,不同基的调制对应的探测结果不做处理;单光子传输不可能出现两个探测器同时都探测到光子的情况,因此将结果为 0(00),3(11)的数据全部抛弃.可得到获取这个片段的时间约为 4s,其中有效数据 11 个,误码 1 个.在较稳定的条件下,获得有效原始数据采集速率约为 6bit/s(5min 传送的数据为 1800bit),有效传送数据(同基并且被探测器检测到的数据)速率约为 3bit/s.误码率则与系统稳定时间 5s 的量级相符合,在 5s 左右的时间段内系统传送误码率小于 10%,在更小的时间尺度上误码率可以更小.以 5s 的时间为每一段数据通信时间,在现有实验过程中加上测试系统稳定性的部分便可以初步完成实际通信任务.具体做法如下:5s 左右的时间内通常能传送 15bit,在通信开始前检测系统稳定性若发现 3 个与理论相符合的数据,则认为系统稳定可以开始通信,当接收到 5 个有效数据后,再次检测系统稳定性,若发现 3 个与理论符合且与通信前所检测的情况(初相位等)相同,则记录这 5 个数据,否则抛弃.由于调制、采集数据的速率较慢,导致实际通信速率很慢.该系统要实用化还必须改进,但已成功完成了量子密码通信的演示性实验.

要实用化,或者减小系统的长期误码率,或者提高系统的有效数据传送速率.产生误码的因素很多,有光探测器暗计数误码、偏振漂移产生的误码和相位漂移产生的误码.我们系统中的误码主要来自相位漂移和偏振漂移,以前者为主要,相位稳定时间最长为 10s(偏振稳定时间为分钟量级).系统的稳定性一定时,提高相位调制的速度可以提高系统的有效数据传送速率,同时大大降低误码率.如果速度提高到 10kHz,误码率就可降到 2% 左右,能满足实用的要求.

5 结 论

我们自行设计和制造了单光子源、单光子探测器、PZT 全光纤相位调制器、系统同步控制、数据采集和处理等关键性部件,采取相位调制和 BB84 通信协议,在 850 nm 波长完成了全光纤量子密钥分发系统原型.经过各种稳定系统的措施,目前的通讯距离为 1.1 km,有效数据传送速率为 3 bit/s,在系统稳定时间之内误码率降到 9% 左右.密钥积累起来,可以初步满足保密通信的需要.

下一步的工作是进一步改善系统性能,将波长改为通信波长、加长通信距离、提高通信速率以及进一步降低误码率,使量子密钥技术向实用化发展.

[1] R.J.Hughes, D.M.Alde, P.Dyer, G.G.Luther, G.L.Morgan, M.Schauer, *Contemp. Phys.*, **36**(1995), 149; L.A.Wu, *Physics*, **27**(1998), 544(in Chinese) [吴令安,物理,**27**(1998),544].

[2] C.H.Bennett, G.Brassard, Proc. IEEE Internat. Conf. Computers, Systems and Signal Processing (Bangalore, New York, IEEE, 1984).

[3] C.C. Bennett, *Phys. Rev. Lett.*, **68** (1992), 3121.

[4] A. K. Ekert, *Phys. Rev. Lett.*, **67** (1991), 661.

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

[6] P.D.Townsend, J.G.Rarity, P.R.Tapster, *Electron. Lett.*, **29** (1993), 634.

[7] P.D.Townsend, J.G.Rarity, P.R.Tapster, *Electron. Lett.*, **29** (1993), 1291.

[8] C.Marand, P.D.Townsend, *Opt. Lett.*, **20**(1995), 1695.

[9] A.Muller, H.Zbinden, N.Gisin, *Europhys. Lett.*, **33** (1996), 335.

[10] A.Muller, T.Herzog, B.Huttner, W.Tittel, H.Zbinden, N.Gisin, *Appl. Phys. Lett.*, **70**(1997), 793.

[11] J.D.Franson, B.C.Jacobs, *Electron. Lett.*, **31** (1995), 232; B.C.Jacobs, J.D.Franson, *Opt. Lett.*, **21** (1996), 1854.

[12] R.J.Hughes, G.J.Morgan, C.G.Peterson, Los Alamos Report, LA-UR-991593.

[13] J.Shao, L.A. Wu, *Quant. Opt.*, **1**(1995), 41(in Chinese) [邵进、吴令安,量子光学, **1** (1995),41].

[14] J.Liao, C.Liang, Y.J.Wei, L.A.Wu, S.H.Pan, *Acta Phys. Sin.*, **50** (2001), 467(in Chinese) [廖　静、梁　创、魏亚军、吴令安、潘少华,物理学报,**50**(2001),467].

[15] C.Liang, D.H.Fu, B.Liang, L.A.Wa, D.C.Yao, *J. Data Acquisition & Processing*, to be accepted (in Chinese) [梁　创、符东浩、梁　冰、吴令安、姚德成,数据采集与处理, 已接收].

QUANTUM KEY DISTRIBUTION OVER 1.1km IN AN 850nm EXPERIMENTAL ALL-FIBER SYSTEM*

LIANG CHUANG[1)]　FU DONG-HAO[2)]　LIANG BING[1)]　LIAO JING[1)]　WU LING-AN[1)]　YAO DE-CHENG[2)]　LÜ SHU-WANG[2)]

[1)] (*Laboratory of Optical Physics Institute of Physics, Chinese Academy of Sciences, Beijing* 100080, *China*)

[2)] (*Graduate School of Chinese Academy of Sciences, Beijing* 100039, *China*)

(Received 18 July 2000; revised manuscript received 17 November 2000)

ABSTRACT

A 1.1km long all-fiber quantum key distribution experimental setup has been realized for the first time at 850nm. The system employs the BB84 protocol to establish a secret key between two parties, the security of which is guaranteed by Heisenberg's uncertainty relationship and the quantum noncloning principle. Phase modulated single photons are used to carry the key. The effective transmission rate is 3 bit/s, with a bit error rate of 9%.

Keywords: quantum key distribution, BB84 protocol, single photon, optical fiber

PACC: 0365, 4230, 4250

* Project supported by the Presidential Foundation of the Chinese Academy of Sciences, China (Grant No. SZH9612) and by the National Natural Science Foundation of China (Grant No. 19974073).