文章编号：0258-7025(2003)Supplement-0059-05

光量子保密通信

刘颂豪，廖常俊
(华南师范大学信息光电子科技学院，广东 广州 510631)

摘要 分析量子密钥分配系统的组成和密钥传输方式，介绍了相位调制双 Mach-Zehnder 干涉方式和 Faraday 镜补偿双折射效应的方式之后，提出一种新的旋偏振量子态传输方式。

关键词 量子光学；量子通信；量子密钥分配；量子态；偏振态；量子码
中图分类号 TN918 **文献标识码** A

Optical Quantum Cryptography

LIU Song-hao, LIAO Chang-jun
(*School for Information and Optoelectronic Science and Engineering, South China Normal University, Guangzhou, Guangdong* 510631, *China*)

Abstract Quantum cryptography has been in practical interests that can ensure an unconditional security for the communication system. The quantum key distribution system has been analyzed to show the factors that are important to a successful quantum cryptography. After introducing two of the quantum key distribution systems including two Mach-Zehnder interferometers with phase modulation and the Faraday mirrors to compensates automatically any birefringence effects and polarization dependent loss, a new system is proposed that the rotating photons are used to transmit the quantum bits.

Key words quantum optics; quantum communication; quantum key distribution; quantum cryptography; quantum bit; polarization state

1 引 言

目前，量子信息技术已经进入大规模实验研究阶段.最早在这方面取得成功的是量子密钥分发[1-3]，这是一种依靠基本粒子的量子力学性质的通信技术，是一种理论上可以证明是绝对安全的保密通信技术. 这种通信技术在常规光纤通信线路上的使用成功是量子理论进入应用科学领域的又一个显著标志[4,5]。事实上，量子理论和量子技术的广泛应用是这一个世纪光电子技术的一个特点。这同时使得量子理论会在更大的范围普及，对量子理论的认识更深入，从而得到更大的发展。

保密通信自古以来就是关系国家安全的大事。到信息和网络时代的今天，保密和安全就更加重要了。传统的保密通信技术已经发展得相当成熟，而且借助于计算机已经变得非常复杂。然而提高加密算法的复杂程度和破译速度的提高是同时发生的。没有理论能证明，常规的加密算法是可以绝对安全的。相反的判断是数学加密的方法总是可以用数学方法解开的。有一种称为一次一密密码(one-time pad)是不可破译的，这种密码是完全随机序列，与密文一样长，而且只用一次。但是这种密码在传输过程中因可能被窃听和复制而泄密。

量子保密通信是一种物理加密过程，光量子的基本量子力学性质可以确认它的传输是绝对安全的。量子密钥分配系统采用单光子传输密码，严格讲是身处异地的 AB 双方共用同一个光子编制自己的密码，任何企图窃听这一过程的操作都会被立即发现。量子码由单光子的量子状态来表示。单光子是发射和接收的基本单位，它已经不能再分了，任何对它

*广州市资助科技研究项目

作者简介：刘颂豪(1930–)，男，广东人，中国科学院院士，中国激光技术开拓者之一，在中国科学院安徽光机所建成激光光谱学实验室，成为中国科学院首批开放实验室之一，从事激光及其应用技术的研究，目前主要从事激光在医学和通信中的应用。E-mail: liush@scnu.edu.cn

的操作,都会使原来的量子状态发生变化,这些操作包括复制。不可逆编制密码的 AB 双方会从误码率的变化判断传输系统的安全状态。

量子密钥分配系统已经在实际的通信线路上试用了,就是说,在常规光通信线路上开辟了保密信道。在进行常规通信的同时发送量子密码。比较知名的有三条: 由 University of Geneva 进行的通过日内瓦湖底光缆的 22.8 km 线路;由英国电讯(BT)进行的 55 km 光缆线路和美国在 Los Alamos 进行的 48 km 光缆线路。在这些通信线路中量子码由 1310 nm 光子传输,而常规信号在 1500 nm 波段。在自由空间的量子密钥分配也是成功的, 但是由于大气扰动和天光背景的干扰,传输距离还比较短[6]。

本文根据已经发表的在光纤中的量子密钥分配系统分析实现量子保密通信的基本要素, 包括单光子源、量子编码与量子信息的传输、单光子探测技术,并提出了一种新的量子编码与传输方案。

2 量子密钥分配系统

量子密钥分配系统(quantum key distribution)是量子通信中最简单, 也是最早得到应用的量子通信系统[7]。在这里,量子信息的载体是单光子。量子密钥分配可以由一点到多点分配[8,9]。但是,目前试验上很著名的传输系统是从点到点, 而且追求传输更长的距离。量子密钥分配系统由单光子源和量子码的产生、单光子探测器和量子码传输系统三部分组成。

2.1 单光子源和量子码的产生

理想的单光子源是一次只发射一个光子的体系[10],特别是由电注入发光的发光二极管。2002 年的 CLEO/QELS 会议上第一次报道了这种 LED(Paper QtuG1, See also Z. Yuan *et al*.. *Science*, 2002,**295**: 102)。类似的研究有经过量子点或人工原子(Artificial Atom), 色心或晶体结构缺陷发射单光子。实际应用的单光子源要求发射的单光子在发射波长、发射状态和发射时间方面都要得到控制,所以还有很多研究工作要做。例如发射波长选 1310 nm 有利于从常规光通信的 1550 nm 数据流中提取量子密码信号。发射状态是指发射光子的偏振状态和相位调制状态,涉及量子态的测量基,直接与量子编码相关。发射时间的控制是需要的,目的是与探测器控制线路和信号处理线路同步。

目前用于量子密钥分配的单光子都是激光器输出经过精密控制的强衰减技术得到的。通常控制得到大约 70 dB 的衰减,控制精度达到 0.01 dB。在承认光子统计服从泊松分布的基础上, 工作于锁模状态或脉冲工作状态的半导体激光器输出衰减到这样一个水平:按光子能量计算,每脉冲的光子数小于 1。例如取平均光子数等于 0.2 时,单光子出现的概率是 0.16,双光子出现的概率是 0.016。进一步降低平均光子数, 单光子对双光子和多光子数的比例还要增加。另外,还可以通过信号处理技术去除出现的双光子。衰减本身可以看成一个筛选或制备一个量子态的过程,这个量子态就是收信方作为依据的测量基。

偏振是表征量子态的基本参数。光子的偏振态在二维希尔伯特空间, 可以同时用三对正交的量子态来表示,这就是垂直正交线偏振态、倾斜 45°正交线偏振态和左右旋圆偏振态。这是三套互为共轭的矢量基,作为量子码测量的基础。要根据协议制备量子态作为测量基。在测量时,若采用不同的测量基进行测量,得到的结果是完全不确定的,因为它在正交的两个方向上出现的概率完全相等。对于特定光子的量子态,三种表达方式是等价的。例如,垂直线偏振光等于相位相同的倾斜正交线偏振的两个等幅矢量分量的叠加, 也等于左旋和右旋两个矢量波的叠加。分矢量的相位直接影响光子的量子态。对于所讨论的垂直线偏振态, 当倾斜线偏振态的一个分量有 $\pi/2$ 的相移时, 它将变为圆偏振态。再经过 $\pi/2$ 的相移,它就变成水平偏振态了。

保持光子的线偏振状态,利用相位调制形成光子的自干涉, 显示了光子作为量子力学能量波包的特点,类似于正交偏振时的情况,将光子分为等振幅的两部分,使两部分之间的相位差为 $0,\pi/2,\pi$ 和 $3\pi/2$, 同样可以得到互为共轭的两组测量基共四个态。

2.2 单光子探测

光探测器本质上是能量探测器, 而光子是原子或分子吸收或发射的基本单位。探测器的灵敏度是探测器能测量到的最低能量。所以,单光子探测器要求有很高的灵敏度。一个光子的能量是很小的,不足阿托焦耳(Atto Joule,1 aJ=10^{-18} J)。在光通信中所关心的几个波长的光子能量如表 1。

表 1 不同波长单光子的能量

Table 1 Energy of diffrent wavelength monophoton

Wavelength of photon /nm	Energy of photon /aJ
900	0.2209
1310	0.1526
1550	0.1281

要测量这样低的光能量，需要采用光电倍增管或雪崩光电二极管。探测器灵敏度是波长的函数，光电倍增管的倍增因子很高，但在红外波段灵敏度不高。从噪声特性和灵敏度两个因素考虑，目前可供选择的只有硅雪崩光电二极管(Si-APD)和铟镓砷雪崩光电二极管 (InGaAs-APD)。Si-APD 的工作波段在 400~1100 nm，而且可以有高达 400 V 的反偏压得到很高的倍增因子。InGaAs-APD 工作在 1000~1700 nm 波段，通常工作电压约 75 V，倍增因子一般为 10，在临近雪崩电压工作时，有可能达 40。这当然是很不够的。所以，研制高灵敏度的红外探测器依然是科学前沿一个重要课题，要继续改进器件结构和性能，采用制冷技术降低噪声使得可以有更高的工作电压，使探测器处于脉冲工作状态并与光子可能到达的时间同步，采用信号处理技术清除误码等。

2.3 量子码的传输

量子码的传输有与常规光通信类似的传输问题，但表现的形式不同。现在的光通信系统中由于吸收造成的损耗已经很小，这为单光子的传输创造了条件。而且量子密钥分配仅记录接收到的光子，用以形成密钥，光子的到达本身也是随机的，所以损耗不影响量子密钥分发的实现，而仅影响传输距离和密钥生成的速度。非线性散射问题因光子能量很小，也还没有有关研究的报道。对于量子码传输重要的问题是双折射问题，以及构成光子的一对正交的矢量波或同偏振形成干涉的一对矢量波在测量时同时到达，准确重叠的问题。光子本身到达的时间抖动或时间分散也应该尽量地小，以便与单光子探测系统同步操作，减小暗噪声和误码。

在常规光通信中表现为偏振模色散的双折射效应本身就是一个随机过程，它与光纤的制造过程有关，与光缆的铺设过程有关，与光通信系统中使用的元件有关，而且还与环境温度、应力、震动等因素有关，是一个难于解决的问题。双折射问题使得发信方用偏振方向设定的测量基变为不确定的。现代光通信已经注意到克服偏振模色散的问题，偏振模色散可以做得很小。在瑞士通过日内瓦湖底光缆 23 km 的量子密钥分发是使用两组正交线偏振态，采用偏振调制编码，偏振检测的方式实现的[11]。这种方式系统结构比较简单，但由于受双折射的限制，传输更长的距离就比较困难了。

目前，传输距离长，使用比较成功的是保持偏振状态，由相位调制编码，由干涉检测。这种方式使用了两个相同的 Mach-Zehnder 干涉器，收信方和发信方各有一个，并分别在干涉器的一个臂上根据双方协议进行相位调制，形成非正交的两个可能的量子态。这类传输系统有美国 Los Alamos 的 48 km 传输系统和英国 BT 的 55 km 传输系统[7]。系统结

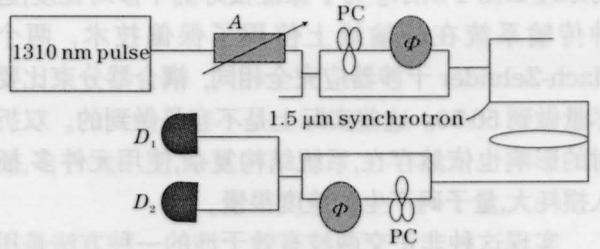

图 1 利用两个马赫-曾德尔干涉仪的量子密钥分配系统原理图。该系统成功利用马赫-曾德尔干涉仪对两非正交量子态演示了 B92 协议。单光子传输进入第一个干涉仪(Alice 端)，通过其一臂上的相位调制形成两个可能的量子态，在 B 方进行同样处理。根据 A，B 方协议，D_1 或 D_2 接收器将探测到设定的量子态。

Fig.1 Schematic of Quantum key distribution system with two Mach–Zehnder interferometers. This system has successfully implemented protocol known as B92 using two non-orthogonal quantum states in which two Mach-Zehnder interferometer have been used.

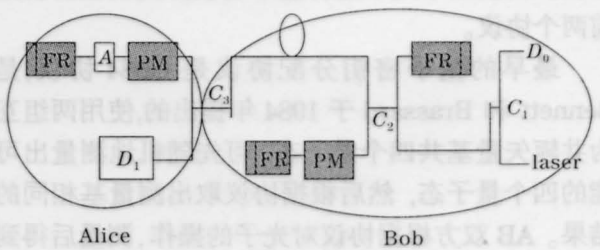

图 2 即插即用量子密钥分配系统原理图。用耦合器 C_2 将短脉冲分成两部分，一部分直接进入 A 方，而另一部分入 FR-PM-FR 延时线。A 方检测脉冲强度，并用 FR 反射光脉冲。经衰减器 A 衰减成单光子水平，并由 PM 解调。在返回到 B 方时，脉冲一部分以同方式延时，在接收器 D_0 处干涉图将告诉 B，A 二端设定的协议信息。

Fig.2 Schematic of plug-and-play system for quan- tum cryptography. Short laser pulses are split into two parts at coupler C_2. One part goes directly to Alice while the other is delayed by FR-PM-FR delay line. Alice measures the intensity of the pulses, reflects the pulses with Faraday Rotator mirror FR. Attenuator A attenuates it to single photon level and encoded by phase modulator PM. During transmission back to Bob, part of the pulses are delayed in the same way. The interference pattern at detector D_0 will tell the phase setting by Bob and Alice

构原理如图 1 所示。为了保证很好的干涉对比度,这种传输系统在传输线上使用了保偏技术，两个 Mach-Zehnder 干涉器应完全相同，耦合器分束比要尽量做到 50/50。这些实际上是不容易做到的。双折射的影响也依然存在,系统结构复杂,使用元件多,插入损耗大,量子码产生的速度很慢。

实现这种非正交两波有效干涉的一种方法是用法拉第镜补偿双折射效应的负面影响[12]。用耦合器分束和时延的方法将光脉冲分开，进行相位调制编码,由法拉第反射镜反射以后,又通过同样的光路和同样的时延,以及根据协议的相位调制,携带协议信息的两脉冲将准确地相干重叠。这样的传输方式被称为即插即用量子密钥分发系统。系统结构原理如图 2 所示。

2.4 量子协议

量子码是根据双方协议产生的，主要有 BB84 协议,B92 协议和 EPR(Einstein-Podolsky-Rosen)协议。而使用单光子进行量子密钥分配的主要就是前两个协议。

最早的量子密钥分配协议是 BB84 协议,是 Bennett 和 Brassard 于 1984 年提出的,使用两组互为共轭矢量基共四个量子态，可先随机地测量出可能的四个量子态，然后根据协议取出测量基相同的结果。AB 双方根据协议对光子的操作,测量后得到的结果是唯一的。

B92 协议仍然使用两套互为共轭的测量基,但只测量其中两个量子态。这样做会损失掉一部分光子,但系统结构简单了。采用相位调制、干涉测量的两个成功的实验系统都是采用 B92 协议,传输距离增加到 55 km。

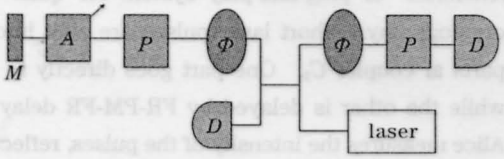

图 3 相位调制圆偏振态传输的量子分配系统示意图

Fig.3 Phase modulation and circular polarization transmission quantum cryptography

3 旋偏振态传输系统

由上面的分析可知,光子任何偏振态可以由三组互为共轭的矢量基中的任何一套来表示,而且任何量子态的变化,可以由组成它的两个分矢量之间的相位差的变化来实现。所以,不论对于正交的态矢量或非正交的态矢量,这里有四个特征的相位差:0,π/2,π,3π/2,分别对应于四个量子态。在相位调制和干涉测量的系统中，不论是 Mach-Zehnder 干涉方式或 plug-and-play 系统中,均是用耦合器将光分为两束后,对其中一束进行相位调制。实际的光纤中有双折射现象,这种现象导致偏振面的旋转,代表着不同偏振光受到不同的调制。根据这个原理,提出了一种新的量子编码和传输方式[13],这种方式直接对线偏振态光子进行相位调制编码，使其变成左旋偏振态或右旋偏振态，迅速旋转的光子态对于相对比较慢的光双折射效应有一种平均作用。用偏振分析技术,配合 AB 双方的协议,就可以产生量子密钥。

这个系统称为相位调制偏振编码传输系统,实验结构如图 3 所示。激光器发出的光脉冲在发信方的反射镜 M 处反射,经过衰减器 A 衰减使得平均每脉冲光子数大约为 0.1，由起偏器 P 变成线偏振光以后，在偏离 45°的方向上对该方向的偏振分量进行相位调制,结果是光子变成左旋或右旋的圆偏振态。圆偏振态为传输光子态。在收信方,对传输光子态进行偏振分析,即用类似的相位调制方法再次得到线偏振光,用偏振器测量,根据 AB 双方的协议,就可以知道发信方设定的量子态了。对于系统中已经存在的双折射效应,可以经过测量以后进行预补偿,即在未加编码信号之前,AB 双方都应该测量到线偏振光。由于采用圆偏振,线偏振光偏振面的旋转不影响测量结果。这也同样说明,这种传输方式受双折射效应的影响是比较小的。

用旋光编码传输的方式使用了全部三套互为共轭的量子态。而且系统结构简单,它不用耦合分束器,减少了插入损耗。信号是在同一光纤中传输的,不须另外增加时延控制,所以是一种更好的量子密钥分发方式。

4 结 论

本文介绍了一种新的编码传输方式。而且相信还会有更多更好的编码传输方式出现。当然,推动这一领域发展的还有元器件技术、单光子的产生和探测技术、量子态的制备和分析技术等。

参 考 文 献

1 C. H. Bennett,G. Brassard, S. Breidbart *et al*.. Quantum cryptography or unforgeable subway tokens [C] in CHAUM, D. R. L. Rivest, A. T. Sherman (Eds.). Advances in cryptology, Proceedings of Crypto '82 (Plenum Press, NY, 1983). 167~175

2 C. H. Bennett, F. Bessette, G. Brassard *at al.*. Experimental quantum cryptography[J], *J. Cryptollog*, 1992, **5**(1):3~28

3 Special issue on Quantum Communication. *J. Mod. Opt.*, 1994, **41**(12)

4 J. G. Rarity, P. C. M. Owens, P. R. Tapster. Quantum random-number generation and key sharing[J], *J. Mod. Opt.*, 1994, **41**(12):2435~2444

5 P. D. Townsend, J. G. Rarity, P. R. Tapster. Single photon interference in 10 km long optical fibre interferometer[J]. *Electron. Lett.*, 1993, **29**(7):634~635

6 J. G. Rarity, P. M. Gorman, P. R. Tapster. Secure key exchange over 1.9 km free-space range using quantum cryptography[J]. *Electron. Lett.*, 2001, **3**(8):512~513

7 P. Townsend. Optical encryption makes networks more secure[J]. *Fiber Systems International*, 2000, **1**(1):30~32

8 P. D. Townsend. Quantum cryptography on multi-user optical fibre networks. *Nature*, 1997, **389**(2):47~49

9 P. D. Townsend, S. J. D. Phoenix, K. J. Blow *et al.*. Design of quantum cryptography systems for passive optical networks[J]. *Electron. Lett.*, 1994,**30**(22):1875~1876

10 Valery Zwiller, Hans Blom, Nikolay Panev *et al.*. Single quantum dots emit single photons at a time: Antibunching experiments[J]. *Appl. Phys. Lett.*, 2001,**78**(17):2476~2478

11 A. Muller, H. Zbinden, N. Gisin, Quantum cryptography over 23 km in installed under-lake telecom fibre [J]. *Europhysics Lett.*, 1996, **33**(5):335~339

12 A. Muller, T. Herzog, B. Huttner *et al.*. Plug and play system for quantum cryptography[J]. *Appl. Phys. Lett.*, 1997, **70**(7):793~795

13 Liu Songhao, Liao Changjun. Quantum key distribution by rotating photons[C]. *Proc. SPIE*, 2002, **4917**:83~86