量子保密通信用的光精密控制强衰减技术*

刘景锋[1] 梁瑞生[1] 刘伟平[3] 唐志列[2] 郑力明[3] 魏正军[2]
陈志新[2] 廖常俊[1] 刘颂豪[1]

(1 华南师范大学信息光电子科技学院,广州 510631)
(2 华南师范大学物理系,广州 510631)
(3 暨南大学电子工程系,广州 510630)

摘 要 光衰减技术是一种重要的光学技术,它在许多领域有重要的应用. 在量子密钥分配中采用光衰减技术可获得单光子序列,这是量子保密通信的基础. 用线性分束耦合器形成多个输出口,将光强的时序衰减变为光强沿输出口的空间分布,研制出了量子保密通信用的精密控制强衰减器,实现了对光子数的精密控制.

关键词 单光子;量子密钥分配;分束耦合器;光衰减
中图分类号 TN929.1 **文献标识码** A

0 引言

自从1984年量子密钥分配协议的提出[1]和1992年量子密钥分配演示实验的成功[2]以来,量子保密通信有了长足的进展. 在理论方面,主要有BB84协议和1992年Bennett根据非正交量子态提出的B92协议[3],以及1991年Ekert提出的基于双光子纠缠量子态与Bell不等式的EPR协议[4]. 在实验方面,在光纤中实现了量子密码的传输[5,6],在自由空间传输方面量子密钥分配也取得了可喜的成绩[7],现在它正逐步走向商业应用[8].

量子保密通信具有防窃听功能,是绝对安全的密钥分配技术,国内外都在开展理论和实验研究. 实现量子保密通信有两大技术关键——单光子脉冲技术[9,10]和单光子探测技术[11,12]. 单光子是量子保密通信的基础,这是由量子力学基本原理中未知量子态不能完全被克隆的定理决定的. 如果发射脉冲中含有两个或多个光子,那么窃听者就有可能截取多余光子进行检测而不被知晓. 理想的方法是只发射单光子[13],但是要真正获得单光子无论在理论上还是技术上都有很多问题有待研究. 目前实际使用的单光子源是由精密控制的强衰减技术得到的.

光衰减是一种重要的光学技术被广泛应用于时域、频域以及能量领域. 在时域中光衰减可用于调Q、锁模和脉冲成形等;在频域中光衰减可用于制造各种带通滤波器以用于图像处理;近代,在能量领域中光衰减显得尤为重要. 在宽带光通信中增益平坦的光纤放大器、在军事中有重要应用并用于保护光探测器的光限幅效应、在非线性光学中所研究的以能量为自变量的各种光学现象以及在量子信息技术中变得越来越重要的光子数控制技术都用到了光衰减. 目前发展起来一种精密控制的强衰减技术,可以产生满足量子保密通信所需的单光子序列. 本文介绍一种用分束耦合器加可变衰减器组成可精密控制的强衰减系统,可用于点到点的量子密钥分配和点到多点的量子网络分配系统,实现了对光子数的精密控制.

1 强衰减系统的设计原理

1.1 衰减量

激光器产生的激光是相干态的光子,其分布是泊松分布

$$P(n,\mu)=\frac{\mu^n}{n!}e^{-\mu} \tag{1}$$

式中n为弱脉冲中包含的光子数,μ为每脉冲平均光子数. 由式(1),单光子脉冲出现的概率为

$$P(1,\mu)=\mu e^{-\mu} \tag{2}$$

由图1可知,当$\mu=1$时出现单光子脉冲的概率最

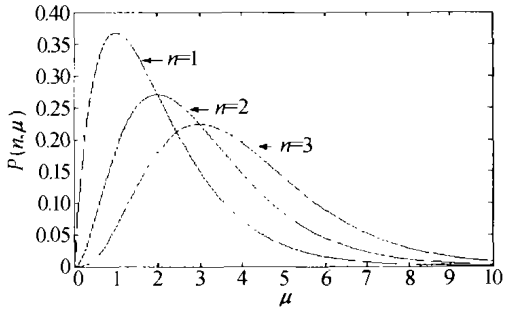


图1 随平均光子数变化光子数概率分布图
Fig. 1 Photon counting probability with the average number of photon per pulse

*国家973(2001CB309300)项目及广州市(1999-Z-035-01)资助项目
Tel:020-33351640 Email:jingfengliu@163.com
收稿日期:2003-07-03

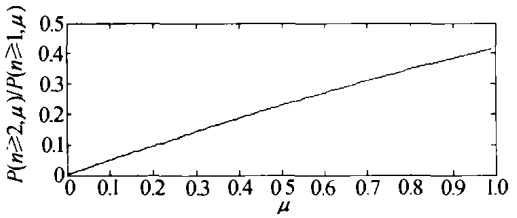
大,此时多光子脉冲出现的概率是

$$P(n\geqslant 2,\mu)=1-P(0,\mu)-P(1,\mu) \tag{3}$$

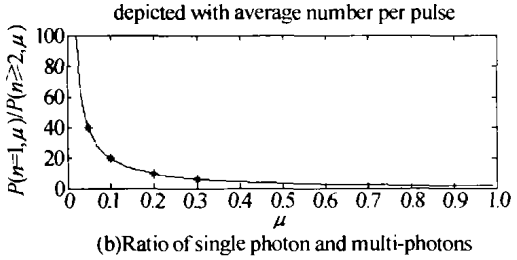
出现单光子脉冲是多光子脉冲的 1.4 倍,从图 1 还可看出,$\mu>1$ 时光路中传输的主要是多光子脉冲,因此$\mu\geqslant 1$ 不满足单光子脉冲传输的实验要求,必须 $\mu<1$,此时非空弱相干脉冲中多光子脉冲出现的概率为

$$P(n\geqslant 2\mid n\geqslant 1,\mu)=\frac{1-P(0,\mu)-P(1,\mu)}{1-P(0,\mu)}=\frac{1-\mathrm{e}^{-\mu}(1+\mu)}{1-\mathrm{e}^{-\mu}} \tag{4}$$

从图 2(a)可看出,μ 值越小,出现多光子脉冲的概率越小,从图 2(b)可知 μ 越小,出现单光子脉冲与多光子脉冲的比值越大. 当 $\mu=0.1$ 时,出现单光子脉冲是多光子脉冲的 19 倍,当 $\mu=0.01$ 时,出现单光子脉冲是多光子脉冲的 199 倍,但此时出现的单光子脉冲数也相应地减少. 在实验中我们把光衰减到平均光子数 $\mu=0.1$,其含义是仅 5% 的非空脉冲包含多个光子,此时若能探测到光子即可被认定为单光子脉冲. 在实验中,我们采用的是 1310 nm 的 DFB 半导体激光器 ,激光器的输出功率为 1 mW,调制频率为 2 MHz,则每脉冲的光子数为 3.3×10^{9} 个,对光进行强衰减使平均每 10 个脉冲中包含 1 个光子,则衰减量为



(a)Probability of multi-photon counting plot depicted with average number per pulse



(b)Ratio of single photon and multi-photons

图 2 单光子与多光子关系图

Fig. 2 Relationship of single photon and multi-photons

$$\alpha_{\mathrm{dB}}=-10\log\frac{0.1}{3.3\times10^{9}}=105.2(\mathrm{dB}) \tag{5}$$

我们把输入光衰减 105.2 dB,就可认为在光路中传输的是单光子脉冲.

1.2 线性分束耦合器

光衰减的方式很多,吸收、散射和耦合损耗等都是比较常用的方法,这些方法都是按时序衰减的方法,即光脉冲在传输过程中光子数减少. 我们运用分束实现衰减,分束耦合器之间固定连接,由此可以实现光子流向按比例分配,将光强度按时序的衰减变为光强沿输出口的空间分布. 在光子流强的一端用常规光探测器测量光强进行精密的实时控制,在分束比小的部位实现单光子输出. 下面对分束耦合器的特性进行了实验研究,我们对所测数据作最小二乘法线性处理,分束比与插入损耗分别满足下列关系

$$\alpha_{\mathrm{InL}}=-0.0001x+13.2619 \tag{6}$$

$$M_{\mathrm{SR}}=-0.0001x+19.0028 \tag{7}$$

α_{InL}为插入损耗,M_{SR}为分束比,x 为光功率. 在可测范围内,其标准差分别为 0.096 和 0.067,我们可把内插的思想用于外推[14],在 −100 dBm 时,插入损耗与分束比分别为 13.2719 dB 与 19.0128,从而可看出,在 0 ~ 100 dBm 之间,它们的变化分别是 0.01 dB 与 0.01. 可以认为耦合器的分束比与插入损耗不随输入光功率的变化而发生变化. 从能量守恒判断,这是耦合器应具备的性质. 现在在可测范围内证明了这种性质,这是在可测范围内对极微弱光衰减控制的基础. 在对光衰减到 −100 dBm 时,若光源的调制频率为 2 MHz,每脉冲光能量近似为 10^{-19} J,即每脉冲包含光子数近似是 1,在可测范围对光衰减到 −80 dBm,外推的是极小的一段,这在理论上是可以的. 也可从耦合器的物理机制分析插入损耗与分束比不随光强的变化而变化的性质,耦合器的耦合区就相当于两个波导,在波导中存在吸收和损耗,因而传播常数 β_z 是个复数,由下式给出

$$\beta_z=\beta_r+j\frac{\alpha}{2} \tag{8}$$

式中 β_r 是传播常数的实部,α 是波导光损耗系数,耦合器的传输特性可通过模式耦合理论方法表示为[15]

$$P_{\mathrm{c}}=P_{\mathrm{in}}\sin^{2}(\kappa z)\mathrm{e}^{-\alpha z} \tag{9}$$

式中 κ 是耦合系数,为波长 λ 与耦合区 z 的函数,P_{c} 是耦合臂端口输出功率,P_{in}是输入功,则耦合器的插入损耗、分束比分别为

$$\alpha'=-10\log\frac{P_{\mathrm{c}}}{P_{\mathrm{in}}}=-10\log\left[\sin^{2}(\kappa z)\mathrm{e}^{-\alpha z}\right] \tag{10}$$

$$M=\frac{P_{\mathrm{s}}}{P_{\mathrm{c}}}=\sin^{2}(\kappa z)\mathrm{e}^{-\alpha z} \tag{11}$$

P_{s} 为直通臂功率,从式(10)、(11)可看出耦合器的插入损耗 α'、分束比 M 均是 z,λ 的函数,但它们都是定值,故耦合器的分束比、插入损耗不因光强的变化而变化. 图 3 是插入损耗与光强关系图,图 4 是分束比与光强关系图,图中直线是我们做的最小二乘拟合直线. 从图 3、图 4 可知道,耦合器的插入损耗与分束比同光强变化无关,图 5 是耦合器的数量

与衰减量的关系图，说明了衰减量与耦合器的数量呈线性关系．

从实验结果可看出，分束比、衰减量不随输入光强的变化而发生变化，分束比保持在19.01，插入损耗是13.02 dB.

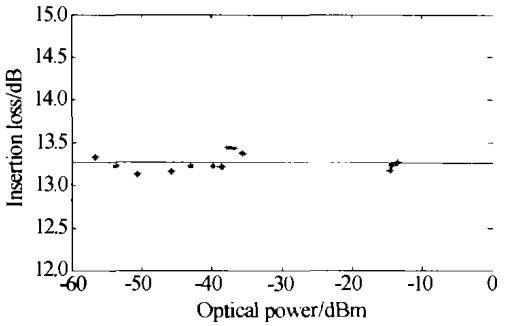


图3　插入损耗随光功率变化关系图

Fig. 3　Insertion loss with different input optical power

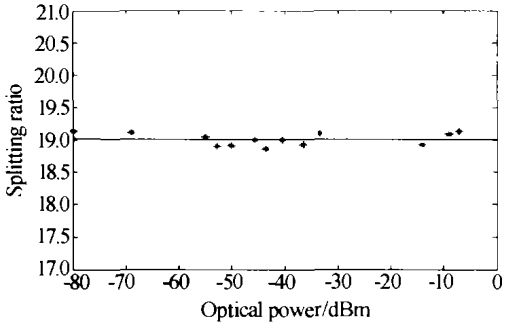


图4　分束比随光功率变化关系图

Fig. 4　Splitting ratio with different input optical power

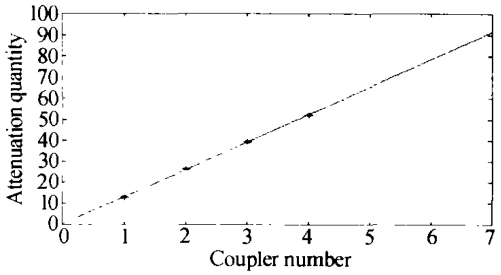


图5　衰减量与分束耦合器只数的关系图

Fig. 5　Attenuation linearly measured with the number of couplers of same splitting ratio

2　仪器设计

要达到实验要求，即需对强光衰减 100 dB 以上，我们设计用 7 只 95:5 的分束耦合器，再有 1 只可调衰减器和 1 只 50:50 分束耦合器构成强衰减系统．图 6 是我们研制的强衰减系统的结构图，用 Coupler1-7(95:5 的光纤耦合器)、Coupler(50:50 光纤耦合器)构成固定衰减部分．单光子从 Coupler 输出，Output:b 是单光子输出口，Output:a 是可能的多路出口．Monitor1 ~ 3 是监控器，用于调试和运行时的监控，Monitor 的探测器是铟镓砷(InGaAs PIN)二极管．Variable Attenuator 是可调衰减器，上述器件的参数如表 1、表 2 所示．

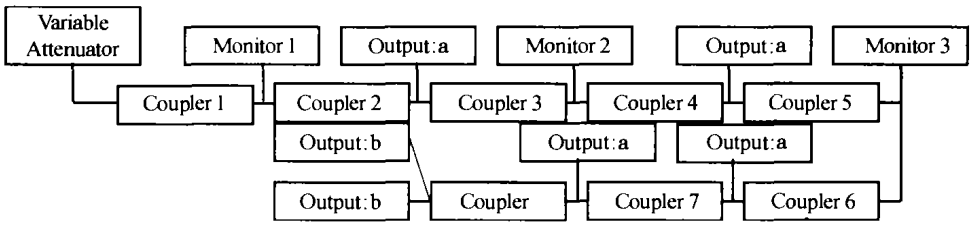


图6　产生单光子序列的分束强衰减系统图

Fig. 6　Heavily attenuated optical splitting system to emit single photon series

表 1　铟镓砷二极管光探测器

型号	灵敏度	对应功率	1Gb/s 时光子数/脉冲
PTRE-17	-50	0.01 μW	66
	-30	0.005 μW	33

表 2　可调衰减器

型号	衰减范围	分辨能力	插入损耗
OVA-620	0 ~ 20 dB	0.1 dB	1.5 dB

此系统的最后一个 Coupler 的每一路都可形成一路单光子输出，由此可用作一点到多点的量子密钥分发，我们研制的这套系统，工作稳定，受外界环境的影响小，可实现精密实时监控．Monitor 可以监控到 -70 dBm 的弱光情况．

3　结论

本文提出了一种用光纤分束耦合器制作强衰减器的方案，利用这种方案我们研制出了可精密控制的强衰减器．常用的位移型光衰减器[16]最大衰减量是 65 dB，一般情况都在 25 dB 内，且微调能力差，一般在 0.5 ~ 1 dB，难于精密控制．与位移光衰减器相比，我们研制的光衰减器衰减量可达 100 dB 以上，可调量达 20 dB，微调能力 0.1 dB，实现了精密控制，可用作量子保密通信用的单光子源．另外我们研制的光衰减器最后一个分束器的每一路都可以形成一路单光子输出，由此可用作一点到多点的量子密钥分配，不做多点分配时，分出的一路可用于监测和控制．

参考文献

1　Bennett C, Brassard G. Quantum cryptography: Public-key distribution and coin tossing, In proceedings of the IEEE International Conference on Computers. Systems and Signal Processing, Bangalore, India, New York: IEEE, 1984. 175 ~ 179

2 Bennett C, Brassard G, *et al.* Experimental quantum cryptography. *J Crypto*, 1992, **5**(1): 3 ~ 28

3 Bennett C. Quantum cryptography using any two nonorthogonal states. *Phys Rev Lett*, 1992, **68**(21): 3121 ~ 3124

4 Ekert A. Quantum cryptography based on Bell's theorem. *Phys Rev Lett*, 1991, **67**(6): 661 ~ 663

5 Muller A, Zbinden H, Gisin N. Quantum cryptography over 23 km in installed under-lake telecom fiber. *Europhys Lett*, 1996, **33**(5): 335 ~ 339

6 Marand C, Townsend P. Quantum key distribution over distances as long as 30 km. *Opt Lett*, 1995, **20**(16): 1695 ~ 1697

7 Hughes R, Buttler R, *et al.* Free-space key distribution in daylight. *J Mod Optics*, 2000, **47**(2/3): 549 ~ 562

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

9 Michler P, Imamoglu A, *et al.* Quantum correlation among photons from a single quantum dot at room temperature. *Nature*, 2000, **406**(6799): 968 ~ 970

10 Michler P, Kiraz A, *et al.* A quantum dot single-photon turnstile device. *Science*, 2000, **290**(5500): 2282 ~ 2285

11 Ribordy G, Gautier J, *et al.* Performance of InGaAs/InP avalanche photodiodes as gated-mode photon counters. *Appl Optics*, 1998, **37**(11): 2272 ~ 2277

12 Hiskett P, Buller G, *et al.* Performance and design of InGaAs / InP photodiodes for single - photon counting at 1.55 μm. *Appl Optics*, 2000, **39**(36): 6818 ~ 6829

13 Lütkenhaus N. Security against eavesdropping in quantum cryptography. *Phys Rev*(*A*), 1996, **54**(1): 97 ~ 111

14 仇维礼,徐根兴,赵恩广,等译. 数据处理和误差分析. 北京:知识出版社,1986. 250
Translated by Chou W L, Xu G X, Zhao E G, *et al.* Date Processing and Error Analysis. Beijing: Publishing House of Knowledge, 1986. 250

15 李玉权,崔敏,蒲涛,等译. 光纤通信. 第三版. 北京:电子工业出版社,2002. 313 ~ 315
Translated by Li Y Q, Cui M, Pu T, *et al.* Optical Fiber Communications. 3rd ed. Beijing: Publishing House of Electronics Industry, 2002. 313 ~ 315

16 姚建,刘秋华,方罗珍. 位移型单模光纤衰减器研究. 光通信技术,1997, **22**(4): 307 ~ 310
Yao J, Liu Q H, Fang L Z, *et al. Opt Commun Tech*, 1997, **22**(4): 307 ~ 310

Precise Controlled Optical Attenuator for Quantum Security Communication

Liu Jingfeng[1], Liang Ruisheng[1], Liu Weiping[3], Tang Zhilie[2], Zheng Liming[3], Wei Zhengjun[2], Chen Zhixin[2], Liao Changjun[1], Liu Songhao[1]

1 *School for Information and Optoelectronics Science and Engineering, South China Normal University, Guangzhou* 510631

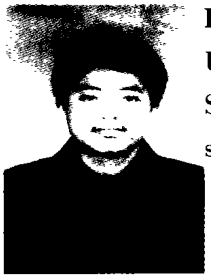
2 *Department of Physics, South China Normal University, Guangzhou* 510631

3 *Department of Electronic Engineering, Jinan University, Guangzhou* 510630

Received date: 2003-07-03

Abstract Optical attenuation, widely applied in many fields, can be adopted to acquire single-photon sequence that is foundational in quantum key distribution. Single-photon sequence can be obtained by precisely controlled optical power distribution along manifold outlets consisted of beam splitters . This can realize optical power spatial distribution instead of attenuation by time sequence due to loss.

Keywords Single-photon; Quantum Key Distribution; Beam splitter; Attenuation



Liu Jingfeng was born in Aug. 1978, in Shandong Province. He studied in Liaocheng Normal University from 1997 to 2001 and received B. S. degree. Now he is studyingfor M. S. degree in South China Normal University. His research interests mainlyinclude quantum key distribution and single-photon realization experiment.