第 52 卷 第 1 期 2003 年 1 月
1000-3290/2003/52(01)/0072-05

物 理 学 报
ACTA PHYSICA SINICA

Vol.52,No.1,January,2003

偏振光量子随机源

冯明明 秦小林 周春源 熊 利 丁良恩

(光谱学与波谱学教育部重点实验室,华东师范大学物理系,上海 200062)

(2002 年 4 月 1 日收到;2002 年 5 月 21 日收到修改稿)

报道了一种基于偏振光量子的随机效应产生的随机源,这种方法利用了单个偏振光子在偏振分束镜表现出来的量子随机性.用同步符合单光子检测技术,对衰减的偏振单光子源在偏振分束镜表现的随机性进行检测,利用计算机和数据采集卡,获得了二元随机码.利用国际通用的随机数检测程序(ENT)对直接获得的数据进行随机性分析,结果完全满足真随机数的标准.

关键词:随机数,单光子,偏振分束镜,同步符合

PACC:4250,0250,0762,0760

1. 引 言

随机数在很多领域都是一个既基础而又重要的部分,从计算机系统安全中的加密,通讯中的认证,数值计算中的 Monte Carlo 模拟方法,到商业中的彩票和博采机等[1].现在,随机数在量子保密通讯和量子信息处理领域又有了极其重要的应用价值[2].因为在量子保密通讯中,光子信息的传输是通过随机数进行编码的,若通讯加码中所用的随机数不是真随机数,编码信息就有可能被窃听者破译,从而使得信息泄漏.因此真随机数的获得是量子保密通讯实现必不可少的条件.

一般来说,随机数的产生有两大途径:利用计算机的某些算法产生伪随机数和利用物理随机量得到随机数.基于算法的伪随机数,存在被同种算法破解的可能性.利用物理量产生真随机源主要有两种方法.一是利用经典系统中的噪声或随机量,如利用电路中的噪声,但是无论多庞大和多复杂的经典系统在理论上都存在噪声或随机量随时间演化的过程,并且外界因素对经典系统的影响也是存在的,因此这种方法并不是产生随机数的最佳方案.另一种物理方法是利用量子力学基本量的随机性,这些基本量是完全随机的,既无规律也不会重复.在这里有较多的方案可供选择:如放射性元素(^{85}Kr,^{60}Co)的衰变可用于实现随机源[3],但由于使用上的不方便和数据采集上的难度并不常用;激光斑纹图案的空间分布随机性也可用于随机数的产生[4,5];被囚禁的单离子共振荧光辐射的光子发射周期是随机的,也可作为随机源[6,7].这些方法产生的随机速率较低,系统较复杂,不易构成实用化的模块,应用的范围受到了限制.近年来,利用光子在界面透反的量子性引起了人们的注意,利用光子在 50% 分束镜透反路径的随机特性研制成光量子随机源[8],有较好的随机性检测结果,该方法产生随机数的速率远远高于上述列举的方案.但考虑到在实验进行中对分束镜的分束比进行微调的困难,本文采用了偏振的方法实现随机源的方案.

2. 实验原理及装置

在理想情况下,当光子以 45°偏振入射到水平或垂直的偏振分束镜时,光子将各有 50% 的概率以水平和垂直偏振从偏振分束镜输出.由光量子的特性可知,这种偏振输出是完全随机的,两个正交偏振方向出射的光子之间互不关联,决定了基于光偏振特性产生随机源的可行性.

随机源实验框图如图 1 所示.虚线框内的为偏振光子随机源,其他还包括提供准单光的单光子源,产生同步信号的信号发生源,随机源信号采集的计

* 上海市重点学科和国家重点基础研究发展规划(973)项目(批准号:001CB309301)资助的课题.

数机.

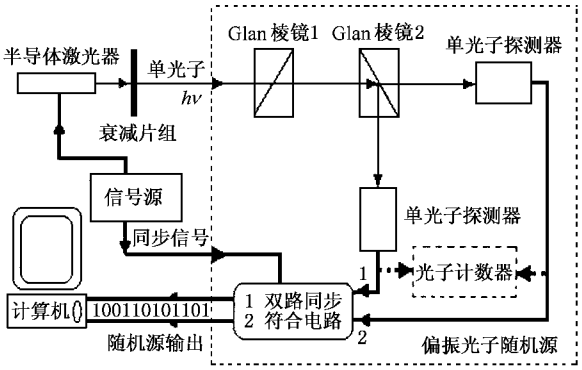

图 1　偏振光量子随机源的实验框图

准单光子源由波长 780nm 的半导体激光器,信号源,衰减片组组成.信号源输出信号对激光头进行幅度调制,调制的脉冲宽度为 50ns,调制重复频率为 1MHz.单脉冲调制的能量为 10^{-10}J,利用衰减片组的 100dB 衰减,以单个光子能量为 2.55×10^{-19}J 计算,则每个调制脉冲中包含的光子数小于 0.1 个光子,满足准单光子的要求.

偏振光子随机源由光随机发生和随机检测处理电路组成.光路随机发生包括 Glan 棱镜 1(G1)和 Glan 棱镜 2(G2).G1 与 G2 的起偏方向互成 45°,由 G1 起偏经 G2 检偏分束,调节 G1 的起偏角,使得光子从 G2 两路正交出射的概率比刚好是 1/1,而且这种调节可以在实验数据采集中进行,若获得的数据随机性不好,可以通过调节使得随机性加强.基于偏振的随机源比基于分束镜的随机源在随机数据的修正上就显示了较大的优势.

随机检测处理电路由双路同步符合单光子检测实现,包括两个单光子探测器(EG&GSPCM-AQ13),双路同步符合电路.SPCM-AQ13 的光敏元件是硅雪崩光电二极管,在 780nm 处的量子效率可达到 70% 以上.输出的光电信号是标准的 TTL 电平,可直接输入同步符合电路中.

若进入随机发生的是严格单光子,并且光子探测器为理想的无噪声探测器,在图 1 所示的两个单光子探测器输出端 1,2 的光电子脉冲序列,已构成了真随机数.但是,通过衰减办法形成的单光子源,存在多光子重叠的概率;光子探测器的暗噪声脉冲也会形成对真随机数的干扰.所以,实验中采取了同步符合的检测技术,以消除多光子重叠和暗噪声的影响.同步符合的基本方法是:利用调制激光的脉冲同步信号对两路单光子探测器的输出信号进行符合,仅当脉冲同步信号存在期间且光子信号出现在两个光子探测器之一时,光子信号才有效,并发生响应的随机数 0 或 1.实现的逻辑关系如图 2 所示.在同步信号 1,2,4 的时间上,只有一路有输入高电平,所以在相应的端口有输出高电平信号;在同步信号 3 的时间上,两路都有高电平输入信号,即两路都检测到了光子,反应了多光子的重叠现象,因此输出应为低电平;当然两路都没有输入时,输出都为低电平.在同步信号门内有高电平信号输出的写入随机数列,并定义 1 端有高电平输出为 1,2 端有高电平输出为 0,对两路都为低电平的情况不写入随机数列,所以图 2 中得到的随机数列为 101.逻辑功能由 74 系列逻辑门实现.随机数列信号的采集由计算机数据采集接口完成.

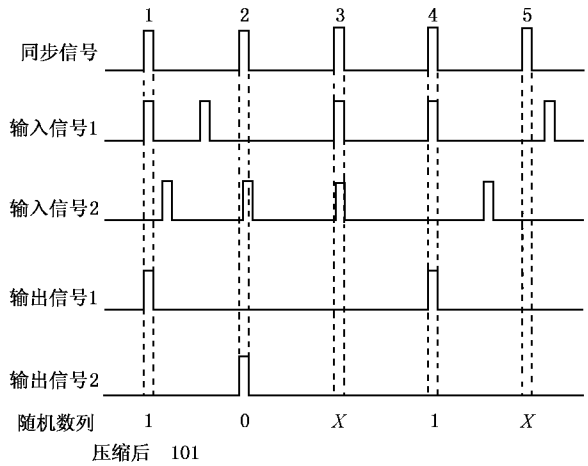

图 2　双路同步符合逻辑关系图

随机数的产生速率由激光幅度调制重复频率决定,在 1MHz 的重复频率下,每脉冲只有 0.1 个光子的单光子源,因此产生随机数的速率一般可达到 100kbit/s.

获取真随机数之前,先用光子计数器(Photon Counter-SR400-Stanford Research System Ins.)对两个单光子探测器输出的数据量进行预先检测,判断两路输出的计数量是否相等,如不等,可通过 Glan 棱镜 2 对光的偏振方向进行微调,使两路输出数据量相等.在实验中,得到的计数率为 100kbit/s,这也就是随机数产生的速率.之后将数据流导入双路同步符合电路,再用计算机接口对数据进行采集,采集的数据以二进制格式保存在文件中,以便对数据进行随机性分析.

3. 数据的随机性检验

现在,对于随机性还没有一个确切的定义,但有两点是被广为接受的随机性特征,即无序性(chaotic),典型性(typical).无序性描述了数列的算法复杂程度,典型性表征了任意随机数列间的不可区分性.因此计算机利用某种算法产生的随机数只能是伪随机数,总可以通过数学的方法找出这种算法,而对随机数进行破译.

国际上常用的随机数检测指标有以下几个:熵(Entropy),χ^2 检测(Chi-square Test),算术平均值(Arithmetic Mean),Monte Carlo 方法求 π,序列相关系数(Serial Correlation Coefficient).本文利用国际上通用的随机数测试程序——ENT 检测实验所得二进制数列的随机性.ENT 是伪随机数序列测试程序的简称,这一测试程序被广泛应用在对加密的伪随机数生成的估计,采样统计以及密集编码等方面.

ENT 对本实验的数据列的测试结果如图 3 所示.

Entropy = 0.999999 bits per bit.

Optimum compression would reduce the size
of this 53528 bit file by 0 percent.

Chi square distribution for 53528 samples is 0.05, and randomly
would exceed this value 75 percent of the times.

Arithmetic mean value of data bits is 0.4995 (0.5 = random).
Monte Carlo value for Piis 3.095964126 (error 1.45 percent).
Serial correlation coefficient is 0.062845 (totally uncorrelated = 0.0).

图 3 ENT 真随机数测试结果

对随机数检测标准简述如下.

1)熵

熵表征了一个系统的混乱程度,熵越大表示系统越无绪.在对 n 位数列的随机性分析中,定义熵为

$$H_n = -\sum_n p_i \log_2 p_i, \qquad (1)$$

p_i 表示在数据列中第 i 个数据出现的概率,对任意一个真随机数列,n 位比特的数据列对应的熵应为 n.例如对于一个 8 位的真随机数列,其最大的熵为 8.因此可以用熵值对数据随机性进行分析.实验得到二进制 1 位随机数列的熵 = 0.999999,说明这个数列的随机性很好.

2)χ^2 检测

χ^2 检测是随机数均匀性检测常用的一种方法,它用来检测随机序列是否均匀的分布在[0,1]的区间上.ENT 程序对随机数列进行 χ^2 分布的计算,并将结果表示为一个绝对数和一个百分比形式.百分比表示了真随机序列与计算值的偏离程度,用这一百分比作为检验随机性的一个标准.如果这一百分比大于 99%或者小于 1%,这一数列就可以确定是完全不随机的 如果这一百分比在 99%到 95%之间或者在 1%到 5%之间,那么认为这一数列可能是不随机的 如果百分比在 90%到 95%之间或者在 5%到 10%之间,则表明数列可能是随机的;那么百分比在 10%到 90%之间,说明它的随机性很好.对实验中所得随机二进制数列的测试结果是 53528 个数据位的 χ^2 分布是 0.05,百分比值为 75%.

3)算术平均数

算术平均数定义为输入数据列中的所有比特求和,再将其除以数据列的长度就可求得.如果一个字节的数据列是近似随机的,那么这个平均值应在 127.5 左右.如果一个比特的数据列是随机的,那么这个平均值应在 0.5 左右.实验所得数据列的算术平均值为 0.4995.

4)Monte Carlo 方法计算 π 值

利用 Monte carlo 方法计算 π 值是通用的随机性检测方法.当计算所得的 π 值接近真实 π 值时,就可认为数列的随机性比较好.实验中得到的数列计算的结果为 3.095964126,偏差 1.45%.

5)序列相关系数

序列相关系数是用来衡量文件中的每一个字节对前一个字节的依赖程度.对于真随机序列,相关系数将接近于零.实验数据列的序列相关系数为 0.062845.

利用国际上通用的随机数检测程序(NET)对实验得到的二进制数列进行随机性检测,结果表明完全满足随机数的标准.

Entropy = 0.999653 bits per bit.

Optimum compression would reduce the size
of this 33376 bit file by 0 percent.

Chi square distribution for 33376 samples is 16.05, and randomly
would exceed this value 0.01 percent of the times.

Arithmetic mean value of data bits is 0.4890 (0.5 = random).
Monte Carlo value for Pi is 3.263309353 (error 3.87 percent).
Serial correlation coefficient is 0.061030 (totally uncorrelated = 0.0).

图 4 ENT 伪随机数列测试结果

为了说明偏振方案的优点,我们特将一组偏振

角不为 45°(约为 44°)的随机数据列的测试结果(如图 4)和真随计数列的测试结果(图 3)做一个对比.

从图 4 中可看到,熵值为 0.999653,明显比真随机数的熵值 0.999999 接近 1 的程序小,熵值的变小表现了系统从无序性到有序性的一个变化;图 4 中算术平均值为 0.4890,比真随机数的算术平均值 0.4995 小,与完全随机数的算术平均值的 0.5 的差距更大.更加重要的是图 4 中,χ^2 检测结果中,百分比值为 0.01%,由以上的分析可得到小于 1% 的 χ^2 检测百分比表征了这个随机数列的完全不随机性,而为 0.01% 的百分比表明了这个数列完全不随机,这个结果和真随机数 75% 的 χ^2 分布百分比相比有本质上的差别.因此当我们测得这样的结果后,可对 G1 进行微调,使得棱镜 G1 和 G2 的偏振角尽可能的接近 45°,再对采集的数据进行分析.如果数据偏差继续增大,则要向相反的方向微调;如果偏差减小,就还可以朝同一方向调节.经过数次调节后,随机数列的随机性可得到本质上的改善,即可得到真随机数.

4. 总　　结

本文中利用单光子在偏振分束镜表现出来的量子随机性,获得的量子随机数完全达到了国际上通用真随机数的测试标准,可以满足量子保密通讯中对真随机数的需要,在进一步的量子保密通讯系统中可以得到应用.随机数产生速率还可以通过提高激光幅度调制频率来实现.通过改进,随机源系统可以小型化,达到即插即用的要求.

[1] Marsaglia G 1993 *Computers & Mathematics with Applications* **9** 1

[2] Bennett C H *et al* 1992 *Scientific American* **257** 50

[3] Jennewein T, Achleitner U, Weihs G, Weinfurter H and Zeilinger A *A Fast and Compact Quantum Random Number Generator* (Los Alamos Eprint, quant-ph/9912118)

[4] Martino A J, Morris G M 1991 *Appl Opt*. **30** 981

[5] Morris G M 1985 *Opt*. *Engin*. **24** 86
Marron J, Martino A J and Morris G M 1986 *Appl*. *Opt*. **25** 26

[6] Itano W M, Bergquist J C, Hulet R G and Wineland D J 1987 *Phys*. *Rev*. *Lett*. **59** 2732

[7] Sauter Th, Neuhauser W, Blatt R and Toschek P E 1986 *Phys*. *Rev*. *Lett*. **57** 1696

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

Quantum random number generator based on polarization

Feng Ming-Ming Qin Xiao-Lin Zhou Chun-Yuan Xiong Li Ding Liang-En

(*Key Laboratory of Optics and Magnetic Resonance Spectroscopy, and Department of Physics, East China Normal University, Shanghai* 200062, *China*)

(Received 1 April 2002; revised manuscript received 21 May 2002)

Abstract

We present a set of random number generator based on a quantum mechanical source, which is the process of splitting a beam of photons on a polarizing beam splitter. The randonmess of the polarizing photon is detected by the synchronous single-photon coincidence detection technique. The random bit data are transferred to a personal computer via a digital I/O interface. The random numbers are tested by the Pseudo-random Number Sequence Test Program (ENT) which is the most popular random number test program in the world. The result is perfect.

Keywords: random number generator, single photon, polarizing beam splitter, coincidence detection

PACC: 4250, 0250, 0762, 0760

* Project supported by the State Key Development Program for Basic Research of China (Grant No. 001CB309301) and the Shanghai Priority Academic Discipline.