doi:10.3788/gzxb20154406.0627003

等时间间隔内光子数奇偶随机性的光量子随机源

鄢秋荣[1],赵宝升[2],张华[1],廖庆洪[1],陈荣伶[1]
(1 南昌大学 信息工程学院,南昌 330031)
(2 中国科学院西安光学精密机械研究所 瞬态光学与光子技术国家重点实验室,西安 710119)

摘 要:提出一种基于等时间间隔内光子数奇偶随机性光量子随机源.将连续波激光二极管发射的光衰减成离散的单光子序列,利用雪崩光电二极管单光子探测模块来探测光子,通过测量等时间内探测到光子数的奇偶性来提取随机位.研制出了基于现场可编程门阵列的随机位提取电路,测试和分析了时间间隔大小和单光子计数模块的性能参量对所设计随机源提取随机数性能的影响.根据系统平均计数率自动设置时间间隔大小,实现了偏差小、速度快的随机位产生器.所设计随机源工作在计数率为 20 Mcps,时间间隔设置为 0.5 μs 时,可获得 2 Mbit/s 的随机位产生速率.运用随机性检测包 ENT 和 STS 对所获得的随机位序列进行测试,表明序列的随机性满足真随机数标准,不需要后续处理.

关键词:光量子随机源; 单光子探测; 随机数检测; 信息熵
中图分类号:O431.2; TN29 **文献标识码**:A **文章编号**:1004-4213(2015)06-0627003-5

Optical Quantum Random Number Generator Based on Parity of the Number of Photons Detected in Equal Time Intervals

YAN Qiu-rong[1], ZHAO Bao-sheng[2], ZHANG Hua[1], LIAO Qing-hong[1], CHEN Rong-ling[1]
(1 *Information Engineering School, Nanchang University, Nanchang* 330031, *China*)
(2 *State Key Laboratory of Transient Optics and Photonics, Xi'an Institute of Optics and Precision Mechanics, Chinese Academy of Sciences, Xi'an* 710119, *China*)

Abstract: An optical quantum random number generator based on parity of the number of photons detected in the equal time intervals was proposed. Light emitted from a continuous wave laser diode is attenuated into discrete single-photon sequence. The single photon is detected by a single-photon avalanche photodiode module. Random bit is extracted by measuring the parity of number of photons detected in equal time interval. The random bit extraction circuit based on field programmable gate array was developed. The influences of the size of time interval and the performance parameters of single photon module on performance of the designed random number generator were analyzed. In order to achieve a random bit generator with small deviation and fast generation rate, a method of setting time interval automatically according to average counting rate was proposed. A random bit generation rate of 2 Mbit/s was obtained when the designed random number generator works on a counting rate of 20 Mcps and the equal time interval is set as 0.5 μs. The random bit sequences were tested by random number test program ENT and STS. The test results show that the generated random bit sequences fully meet the standards of true random numbers, and do not require post-processin

Key words: Optical quantum random number generator; Single-photon detection; Randomness test; Information entropy
OCIS Codes: 270.5568; 270.5290; 030.5260; 040.5160; 270.5565

基金项目:国家自然科学基金青年科学基金(No. 61007017)、中国博士后基金 (No. 2013M540536)、江西省青年科学基金(No. 20142BAB217006)和江西省教育厅基金(No. GJJ14211)资助
第一作者:鄢秋荣(1982—),男,讲师,博士,主要研究方向为单光子探测技术及应用. Email:yanqiurong@ncu.edu.cn
收稿日期:2015-03-03;**录用日期**:2015-04-16

0 引言

随机数已被广泛应用于统计分析、计算机仿真、加密技术等领域.产生随机数的方法主要有两类,一是通过计算机由确定算法产生伪随机数,虽然该方法可以获得很高的随机数产生速率,但由于算法的内在决定性使得伪随机数不适用于某些应用.如量子密钥分配中,量子态的准备和量子态的探测都需要真随机数[1-2].二是从非决定性的物理过程中提取随机位,如电阻中的约翰逊噪音[3],激光的相位噪音[4-5],非决定性量子过程[6]等,一般认为这些利用非决定性物理过程产生的随机数为真随机数,但不同程度存在系统复杂、产生速率低或偏差大需要后处理等缺点.

利用光量子过程来产生物理真随机数是目前的研究热点,典型的光量子随机源是基于光子通过分束镜或偏振分束镜的空间随机性来实现的[7-9],但由于难以实现精确的50:50分束比且两个探测器的探测效率存在差异,产生的原始随机数据存在较大的偏差,即出现"1"的概率与出现"0"的概率不等,因此需要复杂的后续处理.廖静等[7]利用Huffman编码的方法对基于分束镜光量子随机源产生原始随机序列进行后处理来改善偏差.马海强等[9]利用下参量转换后的纠缠光子对来产生随机数,解决两个单光子探测器量子效率不同导致的偏差.最近报道的光量子随机源大多基于到达光子的时间信息[10-15],如根据等时间间隔内探测到光子数的随机性,对固定时间间隔探测到的光子数进行编码来产生随机位[13-14].由于固定时间间隔内探测到的光子数呈泊松分布,基于该方法的随机源所产生的原始数据存在较大的偏差需要进一步后处理.又如根据相邻光子的时间间隔的随机性,对相邻光子时间间隔离散化编码来产生随机位[15-18].由于相邻光子间的时间服从指数分布,该方案产生的原始随机数存在较大的偏差.为消除偏差获得满足真随机数标准的随机数,主要采用软件进行后处理.为获得偏差小的随机数,M Wayne等提出一种精密的光脉冲整形方法[18],以使光子时间间隔呈均匀分布,但该硬件方法极大地增加了系统的复杂度.

为了实现偏差小的光量子随机数产生器,本文提出并验证一种基于等时间间隔内光子数奇偶随机性的光量子随机源.该光量子随机源将连续波激光二极管衰减成离散的单光子序列,利用基于雪崩光电二极管的单光子探测器模块来探测单光子,通过测量等时间内探测到光子数的奇偶性来提取随机位.

1 原理及实现

本文提出的光量子随机源原理为:将连续波激光二极管衰减成离散的单光子序列,利用基于雪崩光电二极管的单光子计数模块(Single Photon Count Module, SPCM)来探测单光子,通过测量出等时间间隔 ΔT 内探测到光子数(S_1, S_2, S_3, …, S_n)的奇偶性来提取随机位.如果 S_n 为奇数则产生随机位"1",如果 S_n 为偶数则产生随机位"0",如图1.光强恒定光场中.由于光电子发射是泊松过程,各时刻产生的光电子是相互独立的,在一个光电子发射后的时间间隔 t 内,再探测到 n 个光电子发射的几率分布 $P(n,t)$ 为[19]

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

$W=\eta kt$ 为时间间隔 t 内产生的平均光电子数,η 为光电转换的量子效率,其中 k 为单位时间内的光子数,因此在给定时间间隔内的光子数是随机且相互独立,产生的随机位是"1"还是"0"是随机的,且随机位的输出"1"和"0"的概率也相等.

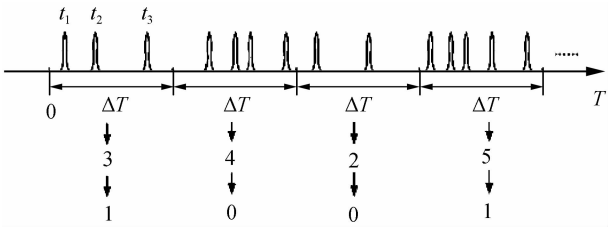

图1 随机数提取方法

Fig. 1 Random bit extraction method

所设计的基于等时间间隔内光子数奇偶随机性的光量子随机源如图2所示,由连续波激光二极管(Continuous-Wave laser, CW laser)、衰减器(Attenuator, ATT)、SPCM、基于现场可编程门阵列(Field Programmable Gate Array, FPGA)的随机位的提取电路、恒温晶振时钟(Oven Controlled Crystal Oscillator clock, OCXO clock)、通用串行总线2.0(Universal Serial Bus2.0, USB2.0)接口和计算机组成.激光二极管采用美国相干公司(Coherent Corporation)制造的型号OBIS660LX的激光二极管,其功率稳定度小于2%.单光子探测器模块的型号为SPCM-AQRH-15.为获得高频率稳定度的时钟,晶振采用频率为50 MHz,频率稳定度为±10 ppb的恒温晶振.激光二极管输出的连续波激光经衰减成离散的单光子序列,通过衰减片的数量来调节光子流的强度和使系统工作在不同的计数率下.离散的光子序列被

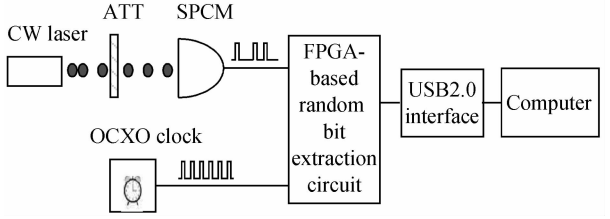

图2 光量子随机源的结构示意图

Fig. 2 Sketch of optical quantum random number generator

单光子探测模块探测到后输出随机的单光子脉冲,基于 FPGA 的随机位提取电路接收单光子脉冲后,进行随机位的提取并将提取的随机位通过 USB2.0 接口送至计算机.

基于 FPGA 的随机位提取电路如图 3,由 SPCM 输出的单光子随机脉冲和外部恒温时钟信号,输入 FPGA 随机位提取电路.外部恒温时钟信号经 FPGA 芯片用内部的数字时钟管理模块来实现倍频,将 50 MHz的外部恒温晶振时钟信号 4 倍频为 200 MHz 的高频率时钟,高频率时钟一方面作为 FPGA 内部所有设计模块工作的统一时钟提高运行速率,一方面经过分频模块后产生等时间间隔的定时信号,时间间隔的大小可根据单光子脉冲的平均计数率的大小调整.SPCM 输出的单光子脉冲信号进入 FPGA 进行边缘检测后输出离散的随机方波脉冲.

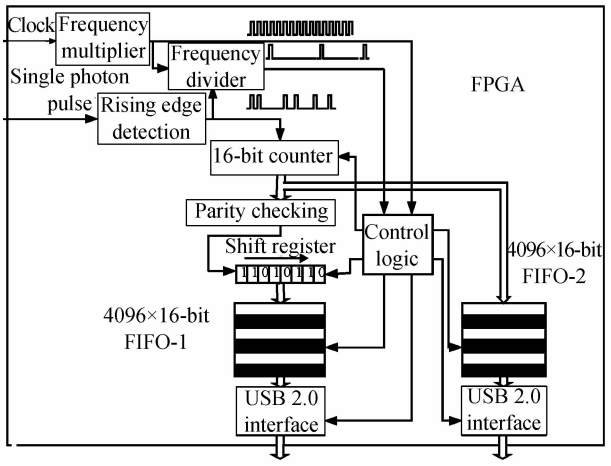

图 3 基于 FPGA 的随机位提取电路

Fig. 3 Sketch of FPGA-based random bit extraction circuit

随机位的提取在所设计的控制逻辑状态机的控制下进行,系统复位后,控制逻辑检测到等间间隔定时信号的上升沿时,16 位的计数器清零,并开始对单光子随机脉冲进行计数,当下一个定时信号脉冲到达时,计数器内的值为等时间间隔内光子脉冲的计数值.进行随机位提取的主要时序如图 4.当定时信号到达时进行以下操作:1)将计数器内的值直接存到先进先出存储器2(First In First Out-2,FIFO-2),以便通过USB2.0 接口直接输出等时间间隔内光子数,进行数据分析;2)对计数器内的值进行大小判决,如此时计数器的值在预设阈值范围内,则进行偶校验,偶校验采用按位取异或运算的方法实现,若 16 位计数器的 D15～D0 中有偶数个"1",则 D15 ⊕ D14 ⊕ D13 ⊕…⊕ D2 ⊕ D1 ⊕ D0=0,若 D15～D0 中有奇数个"1",则 D15 ⊕ D14 ⊕ D13 ⊕…⊕ D2 ⊕ D1 ⊕ D0=1.将校验值作为所提取的随机位移入移位寄存器; 3)当向移位寄存器内移入 16 位后,将移位寄存器的值存到先进先出存储器 1 (First In First Out-1,FIFO-1);4)如 FIFO-1 满,通过 USB2.0 接口模块向计算机发送数据,该数据为系统产生的随机数;5)将计数器清零,以便重新开始对单光子随机脉冲进行计数.当下一等间隔定时信号到达时,重复上述过程.

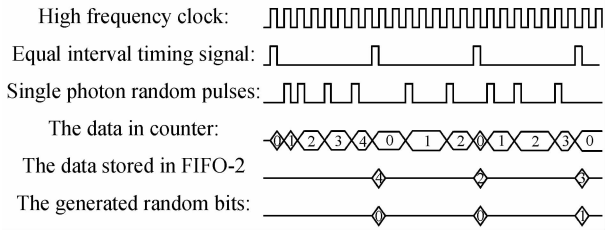

图 4 基于 FPGA 的随机位提取电路的工作时序

Fig. 4 Timing diagram of FPGA-based random bit extraction circuit

2 结果与讨论

随机源工作在平均计数率为 10 Mcps, 分别对时间间隔为 1 μs、5 μs、10 μs 内的探测到的光子数进行统计.因为时间间隔内探测到的光子计数值为整数,统计时步长设置为1,统计分布如图5,验证了等时间间隔

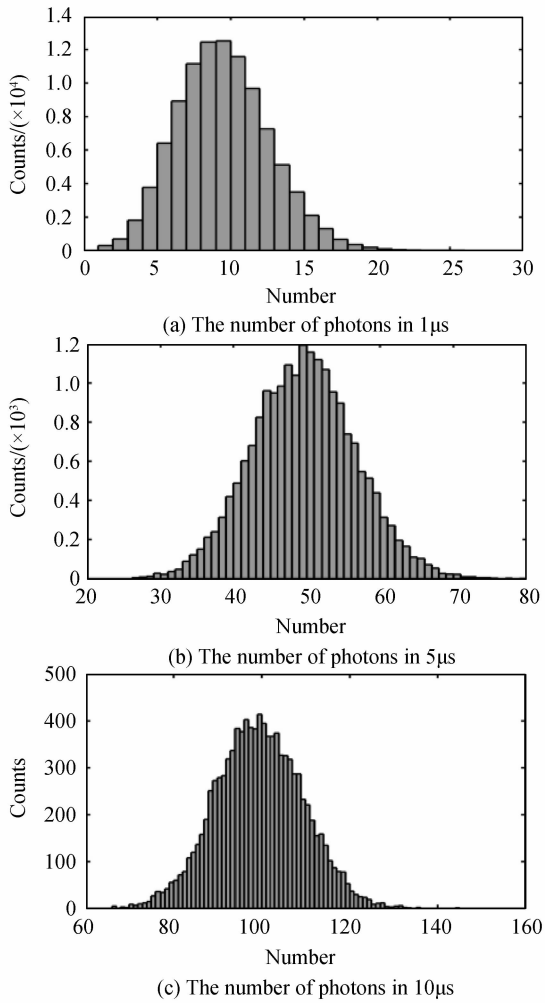

图 5 随机源工作在平均计数率为 10 Mcps 时,不同时间间隔内探测到光子数的分布

Fig. 5 Distribution of the number of photon detected in different time interval when the random number generator woks on average counting rate of 10 Mcps

内探测到的光子数服从式(1)所描述的泊松分布. ENT[20]检验为国际上通用的随机数检测程序,利用ENT可计算出随机数熵(Entropy), $\chi 2$ 检测(Chi-square Test),算术平均值(Arithmetic Mean),蒙特卡罗方法求 π(Monte Carlo value for Pi),序列相关系数(Serial Correlation Coefficient).时间间隔分别设置为 1 μs、5 μs、10 μs 时,所提取的随机数进行 ENT 随机性测试结果如表 1.测试结果表明,利用上述三种不同时间间隔内探测到光子数的奇偶性来提取的随机数随机性都非常好且不需要后续处理,完全满足真随机数的标准.表 1 所示的测试结果还表明随着时间间隔的变化,所提取随机数的随机性并没有明显的变化.但事实上,一方面时间间隔不能设置得太大.如设置时间间隔太大,虽然所产生随机数的随机性不受影响,但需要很多的光子数才能产生 1 个随机位,随机位的产生效率会很低.所设计随机源工作在计数率为 10 Mcps 的条件下,时间间隔设置为 10 μs 时,平均 100 个单光子事件才产生 1 个随机位,随机位的平均产生速率为 100 kbit/s,而时间间隔设置为 1 μs 时,平均 10 个单光子随机脉冲产生 1 个随机位,平均随机位的产生速率为1 Mbit/s.因此时间间隔设置越大,随机位的产生速率也越低.另一方面时间间隔也不能设置得太小.如图 6 光量子随机源工作平均计数率为 10 Mcps 的条件下,时间间隔设置为 0.3 μs 时的光子计数分布图.由于时间间隔设置太小,时间间隔内探测到的光子数为零的统计数占了很大的比重.时间间隔内探测到的光子数为零,偶校验进行随机位提取为"0",因此时间间隔设置太小,将会引入大量的"0"进入随机数,从而影响所提取随机数的随机性.为实现速率快、随机性能好的随机数产生器,时间间隔大小的设置要与系统工作的光子计数率相匹配,所设计随机源根据系统平均计数率的大小自动调整时间间隔,保证在设置的时间隔内平均探测到 10 个光子数.如在计数率为 10 Mcps 的条件下,时间间隔设置为 1 μs.

表 1 时间间隔分别为 1 μs、5 μs、10 μs 时,光量子随机源产生的随机数的 ENT 检测结果

Table 1 ENT test results of the optical quantum random number generator when the equal time interval is set as 1 μs、5 μs、10 μs respectively

ENT test items	t=1 μs	t=5 μs	t=10 μs	Ideal value
Entropy	1.000000	1.000000	1.000000	1.000000
Chi-Square distribution	67.64%	45.86%	77.84%	10%～90%
Arithmetic men value	0.5000	0.5000	0.5000	0.5000
Monte Carlo value for Pi	3.140674553	3.143816478	3.133466731	3.1415926
Serial correlation coefficient	0.000455	0.000347	−0.000332	0.0

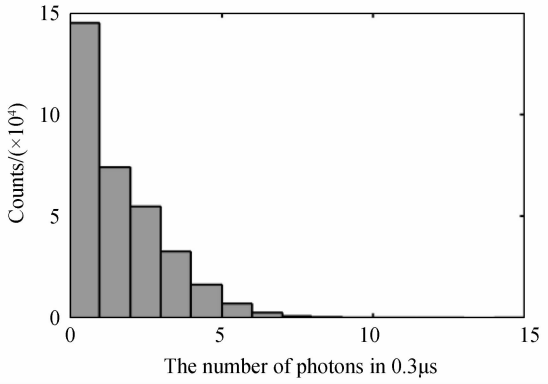

图 6 在平均计数率为 10 Mcps,时间间隔为 0.3 μs 内探测到光子数的分布

Fig. 6 Distribution of the number of photon detected in time interval of 0.3 μs when the random number generator woks on average counting rate of 10 Mcps

光量子随机源中,SPCM 的典型计数率为 35 Mcps,死时间为 32 ns,后脉冲概率为 1%,暗计数率为 50 cps.虽然出现的后脉冲不代表探测到一个光子,但紧跟在单光子脉冲的后脉冲也是随机出现的,所以 SPCM 输出的后脉冲不影响所设计随机源的随机性.同样 SPCM 输出的暗计数脉冲也是随机出现的,也不影响所设计随机源的随机性.当系统工作在低计数率时,死时间可以认为是对所有光子到达的一个固定延迟,因此死时间不影响所提取随机数的随机性.当系统工作在高计数率时,SPCM 模块在死时间之内不响应到达的另一个光子,因此很多单光子脉冲将丢失,SPCM 输出的信号中将有很多周期性脉冲.此时等时间间隔内探测到的光子数不服从泊松分布,从而影响所提取随机数的随机性,因此采用死时间小,计数率高的 SPCM 可实现更高的随机数产生速率.

除了上述 ENT 随机性测试包,还利用 STS[21]来评估所提取随机数的随机性.STS 是由美国国家标准和技术局开发的随机性检测包,用于测试密码学中伪随机数产生器所产生随机数的随机性.STS 由 16 项测试组成,每项测试输出一个 P 值.当所有测试的 P 值大于最小显著水平线 $\alpha=0.01$,满足 $P>\alpha$ 的序列占所有测试序列的比例应大于 0.976 时,认为通过了随机性测试.所设计光量子随机工作在最大计数率为 20 Mcps,等时间间隔设置为 0.5 μs,获得了平均计数率为 2 Mbit/s,将实验中所提取的一个长度为 5G 比特的随机序列分割成 5000 个短序列,所有的短序列都进行 STS 软件包中的 16 项测试,测试结果如图 7.所有测试的输出 P 值都通过了 $\alpha=0.01$ 的显著水平线,通过每个 STS 测试的比例在 0.981 5 到 0.996 3 范围内.

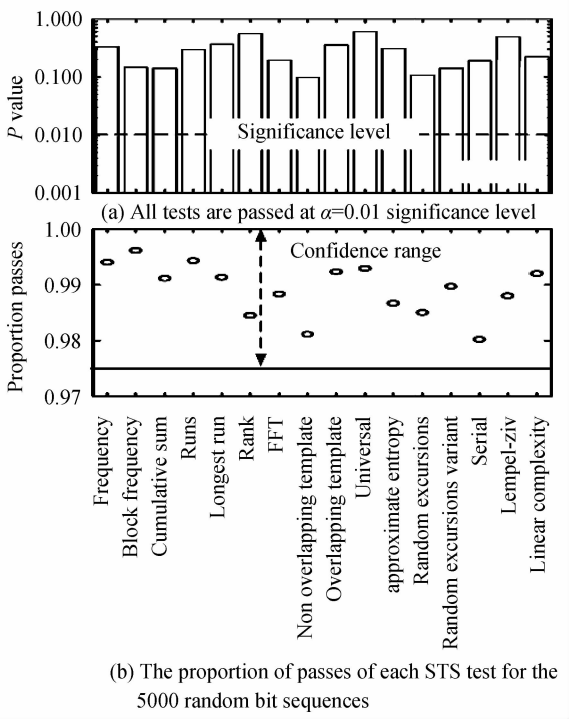

图 7　随机源产生的长度为 5 Gbit 的随机位序列的 STS 随机性测试结果

Fig. 7　Results of the STS statistical tests on 5 Gbit random bit sequences from our random bit generator

3　结论

本文提出一种基于等时间间隔内光子数奇偶随机性的光量子随机源，将连续波激光二极管衰减成离散的单光子序列，利用基于雪崩光电二极管的单光子探测器模块来探测单光子，通过测量出等时间间隔内探测到光子数的奇偶性来提取随机位. 实验结果表明时间间隔设置太大，随机位产生的效率低，时间间隔设置太小，影响所提取随机位的随机性. 为实现产生随机数速率快、随机性能好的随机数产生器，时间间隔的设置必须与系统工作的计数率相匹配，保证在所设置的时间隔内平均探测到 10 个光子数. 系统工作在平均计数率为 20 Mcps，时间间隔设置为 0.5 μs 时，获得了 2 Mbit/s的随机位产生速率. 采用死时间小，计数率高的 SPCM 可实现更高的随机数产生速率. 运用随机性测试程序 ENT 和 STS 对所获的随机位序列进行测试，测试结果表明序列的随机性非常好且不需要后续处理，满足真随机数的标准.

参考文献

[1] SUN Yong-mei, CHENG Xian-zhu, JI Yue-feng. A differentialized service providing scheme on trusted relay quantum key distribution networks [J]. *Acta Photonica Sinica*, 2014, **43**(7): 706009.
孙咏梅，程先柱，纪越峰. 用于可信任中继量子密钥分配网络的差异化服务提供机制[J]. 光子学报，2014，**43**(7)：706009.

[2] YANG You-feng, YE Zhi-qing. Scheme of two-way quantum teleportation and security[J]. *Acta Photonica Sinica*, 2013, **42**(5): 619-622.
杨幼凤，叶志清. 双向隐形传态方案及安全性分析[J]. 光子学报，2013，**42**(5)：619-622.

[3] PETRIE C S, CONNELLY J A. A noise-based IC random number generator for applications in cryptography[J]. *IEEE Transactions on, Circuits and Systems I: Fundamental Theory and Applications*, 2000, **47**(5): 615-621.

[4] QI B, CHI Y M, LO H K, *et al*. High-speed quantum random number generation by measuring phase noise of a single-mode laser[J]. *Optics Letters*, 2010, **35**(3): 312-314.

[5] UCHIDA A, AMANO K, INOUE M, *et al*. Fast physical random bit generation with chaotic semiconductor lasers[J]. *Nature Photonics*, 2008, **2**(12): 728-732.

[6] JENNEWEIN T, ACHLEITNER U, WEIHS G, *et al*. A fast and compact quantum random number generator[J]. *Review of Scientific Instrument*, 2000, **71**(4): 1675-1680.

[7] LIAO Jing, LIANG Chuang, WEI Ya-jun, *et al*. True random number generator based on photon a beam splitter[J], *Acta Physica Sinica*, 2001, **50**(3): 476-472.
廖静，梁创，魏亚军，等. 基于光量子的真随机源[J]. 物理学报，2001，**50**(3)：467-472.

[8] FENG Min-min, QIN Xiao-lin, ZHOU Chun-yuan, *et al*. Quantum random number generator based on polarization[J]. *Acta Physica Sinica*, 2003, **52**(1): 72-76.
冯明明，秦小林，周春源，等. 偏振光量子随机源[J]. 物理学报，2003，**52**(1)：72-76.

[9] MA Hai-qiang, WANG Su-mei, ZHANG Da, *et al*. A random number generator based on quantum entangled photon pairs [J]. *Chinese Physics Letters*, 2004, **21**(10): 1961-1965.

[10] STIPCEVIC M, ROGINA B M. Quantum random number generator based on photonic emission in semiconductors[J]. *Review of Scientific Instruments*, 2007, **78**(4): 045104.

[11] DYNES J F, YUAN Z L, SHARPE A W, *et al*. A high speed postprocessing free quantum random number generator [J]. *Applied Physics Letter*, 2008, **93**(3): 031109.

[12] FURST M, WEIER H, NAUERTH S, *et al*. High speed optical quantum random number generation [J]. *Optics Express*, 2010, **18**(12): 13029.

[13] WEI W, GUO H. Bias-free true random-number generator [J]. *Optics Letters*, 2009, **34**(12): 1876-1878.

[14] RENG M, WU E, LIANG Y, *et al*. Quantum random-number generator based on a photon-number-resolving detector[J]. *Physical Review A*, 2011, **83**(2): 023820-25.

[15] WAYNE M A, JEFFREY E R, AKSELROD G M, *et al*. Photon arrival time quantum random number generation[J]. *Journal of Modern Optics*, 2009, **56**(4): 516-522 .

[16] WAHL M, LEIFGEN M, BERLIN M, *et al*. An ultrafast quantum random number generator with provably bounded output bias based on photon arrival time measurements[J]. *Applied Physics Letters*, 2011, **98**(17): 171105-11.

[17] LI S, WANG L, WU L A, *et al*. True random number generator based on discretized encoding of the time interval between photons[J]. *Journal of the Optical Society America A*, 2013, **30**(1): 124-127.

[18] WAYNE M A, KWIAT P G. Low-bias high-speed quantum number generator via shaped optical pulses [J]. *Optics Express*, 2010, **18**(9): 9351-9357.

[19] MANDEL L. Sub-poissonian photon statistics in resonance fluorescence[J]. *Optics Letters*, 1979, **4**(7): 205-207.

[20] WALKER J. http://www.fourmilab.ch/random/.

[21] RUKHIN A, SOTO J, NECHVATAL J, *et al*. A statistical test suite for random and pseudorandom number generators for cryptographic applications[M]. NIST Special Publication, 2008 800-22, http://csrc.nist.gov/rng/.