第 50 卷 第 3 期 2001 年 3 月
1000-3290/2001/50(03)/0467-06

物 理 学 报
ACTA PHYSICA SINICA

Vol. 50, No. 3, March, 2001

基于光量子的真随机源*

廖 静† 梁 创 魏亚军 吴令安 潘少华
(中国科学院物理研究所光物理开放实验室,北京 100080)
姚德成
(中国科学技术大学研究生院,北京 100039)

(2000 年 7 月 25 日收到;2000 年 8 月 15 日收到修改稿)

介绍基于单光子的量子随机性产生二元真随机序列的实验以及所采用的数学处理方法. 实验利用单光子探测器,较高速的信号处理电路和计算机数据采集系统,接收记录随机选择反射或折射路径通过 50/50 分束器的光子,从而获得原始的二元随机序列. 用 Huffman 编码方法把原始数据压缩为符合密码学要求的真随机序列. 随机序列采集的速率理论上可达 200 kbit/s.

关键词:真随机数源,单光子,光子束器,Huffman 编码及数据压缩
PACC:4250,0250,0762

1 引 言

"随机"是一个在物理学和数学上既基本又深刻的概念[1]. 随机数在很多领域中有重要的应用. 从数值计算中的 Monte Carlo 模拟方法到商业上的博彩业等,随机数都起着关键的作用. 尤其在信息安全领域,量子保密通讯是当今量子信息的热门,随机信号在量子密钥形成中起着关键的作用. 在大多数情况下,人们将计算机里的伪随机数发生器作为随机源. 由于这种随机源是经典的,总是与一定的算法对应,原则上总可以找到其中的规律性,因此可以被破解. 如果此随机信号被窃听者窃取,当通讯双方在公共信道上讨论探测结果时,窃听者就能完全获得密钥而不被发觉. 因此在强密码中必须引入量子的真随机源,以保证量子密码通讯的安全性.

人们一直在设法获得高速、稳定、随机性良好的随机源. 自然界存在着丰富的随机现象. 物理随机源就是利用物理量观测值本身的随机性获得真随机数. 在各类物理随机源中,基于光学系统随机性的随机源具有速率潜力大、稳定性易于控制、简单且容易产品化等优点,是物理真随机源的一个重要的发展方向. 目前大致有三种可能实现的方法. 被囚禁的单离子产生的共振荧光辐射,其光子间隙时间是随机分布的[2,3],利用这种随机特性,可以研制随机源. 激光斑纹图样的空间分布的随机特性也被用于二维随机数的产生[4,5]. 光子的量子性启发人们采用光学分束器来设计量子的随机源[6—8]:单个的光子通过透射率和反射率各为 50% 的光分束器,随机地选择走两条路径;或者 45°偏振的线偏振光子通过偏振分束器也是随机地分成垂直偏振和水平偏振两路. 这种随机源的随机性直接和量子理论的概率理论相联系,是量子真随机源. 直接利用光量子的随机特性来设计随机源,实现起来相对要简单得多,并且随机数产生的速度快,无须大型的设备仪器. 本文设计制作的随机源采用基于 50/50 光分束器这种方法.

2 实验原理和实现

2.1 光学部分

如图 1 所示,本实验用的光源波长为 632.8 nm 的线偏振 He-Ne 激光源,其输出的激光强度约为 1mW,用多级的衰减片组将激光光束衰减到约为 1×10^{-10}mW. 衰减后的激光光束经过一个 50/50 的

* 国家自然科学基金(批准号:19974073)资助的课题.

† E-mail: qo@aphy.iphy.ac.cn or wula@aphy.iphy.ac.cn

半透半反分束器，用精密的调节架手动调节镜片的角度，在强光下用纳瓦精度的光功率计检测，使反射和透射光强相等. 这样，光子流被分成透射(A)和反射(B)两路，分别用光电倍增管(PMT)探测，探测到的将是一些分立的电脉冲信号，可以认为这个被衰减后激光源是单光子源.

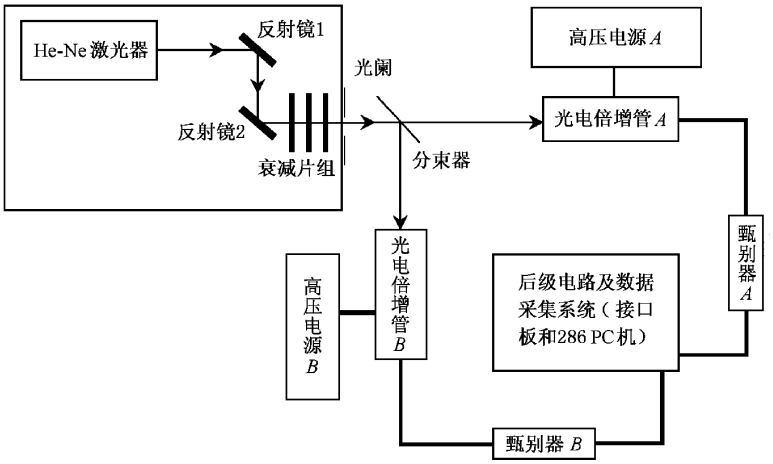

图 1 基于 50%/50%分束器的光量子随机源示意图

先分析一种理想的情况，即(1)保证光子是一个一个地先后入射到分束器上；(2)光电倍增管的量子效率是 100%；(3)分束器是理想的半透半反分束器，即当入射到分束器上的光子被反射或透射的概率是严格的 50%，没有任何散射或吸收损耗，这样对于任何一个入射的光子，无法判断该光子到底是会被反射还是被透射，但是由于分束器是理想的，它必定要么被透射，要么被反射. 如图 1 所示，光子被透射，由光电倍增管 A 接收，产生的脉冲信号经过放大甄别，进入后级电路并被计算机采集，定义此信号为“1”光子被反射，由光电倍增管 B 所接收到，产生的脉冲信号就被计算机记为“0”. 这样，光子流被分束器反射或透射，就在计算机里记录下一串 0，1 的序列. 量子物理的基本原理保证了这样的 0，1 序列是完全随机的.

但是完全理想的情况是不可能的. 首先，激光源的光子数分布遵从泊松分布，有可能出现几个光子几乎同时到达分束器的情况，就有可能 A 路和 B 路的探测器同时有信号产生，后级电路无法鉴别光子前后到达时间，从而使得最后采集到的随机序列受到影响. 其次，由于光电倍增管的量子效率远小于 1，并且即使是同一型号的产品，每个光电倍增管的量子效率都有差别. 本实验使用的光电倍增管的型号分别是：(A) Hamamatsu 公司的 R928P 和 (B) R955，对于 632.8nm 光波长，其量子效率为 5% 左右. 光电倍增管究竟响应了哪些光子是随机的. 此外，由于光电倍增管本身存在暗噪声，可能改变此随机序列. 这些因素的存在无法回避，所以需要仔细地讨论其是否对随机性的本质有影响. 首先，对于光子的聚束现象，可以用后级电路处理来消除. 如果两个探测器都同时接收到一个光子，并且都产生了电脉冲信号输入到后级电路，可让后级电路认为这两个脉冲都是无效的，不做记录. 这样虽然损失了一些信号，但随机性没有受到影响. 其次，光电倍增管量子效率的差异，会造成随机序列 0，1 比不是严格的 1∶1，但是此种影响也是随机性的和不可预测的，因此不会改变此序列的不可预测性. 我们通过调节两个光电倍增管的工作电压来调整其量子效率，从而使采集到的 0，1 序列的 0 和 1 的比非常接近 1∶1. 另外，适当选取放大甄别器的门槛电平，可以剔除光电倍增管的绝大多数噪声脉冲信号.

2.2 脉冲随机信号数值电路和时序

理想情况下，光源是严格的单光子源，稀疏的光子一个一个顺序地被分束器反射或透射，这样要么 A 路的探测器接收到信号，要么 B 路的探测器接收到信号. 如图 2 中 Ⅰ 区域(正常区域)所示，如果用 A、B 分别代表两路两个放大甄别器(EG&G Parc 公司的 1121A 型)出来的电脉冲信号，它们是 NIM 电平的负脉冲，脉冲宽度是 5ns. 箭头指向先输出的脉冲. 后级电路对它们的处理是：先把 NIM 脉冲用高速比较器 Max9686 转换成 TTL 正脉冲信号，然

后用 TTL 电路处理成计算机可以识别的数据流. 首先用 74HCT123 将它们展宽(至少应展宽到使后面的 TTL 电路能够对它们进行逻辑运算),两路脉冲通过一个异或门,形成时钟脉冲,并将此时钟脉冲作适当的延迟. 如果把延迟后的时钟脉冲作为后级串并转换的时钟,让其上升沿触发数据脉冲信号(即 A 或 B 经展宽后的脉冲). 设光子走 A 路表示 1,走 B 路表示 0,如果光子走 A 路,当时钟上升沿到来时,A 路的电平为高,记为 1;光子走 B 路,当时钟上升沿到来时,B 路的电平为高,记为 0. 这样就可以得到一组 0,1 的序列,并由计算机采集.

然而如果两光子时间间距很短,A,B 路的脉冲信号在时间上很接近时,可能有误码产生. 在图 2 Ⅱ区域(存在误码的区域)中可以看到,按照 A,B 两路信号先后到达的顺序,应该得到比特序列(101010),却得到比特序列(101 $\underline{100}$),显然出现了误码. 因此,用这种简单的异或方法是不够的.

最后设计的电路是将两路 NIM 信号脉冲 A 和 B 经过高速比较器后转变为 TTL 脉冲信号 A' 和 B',再做适当的展宽和延迟,转为 C 和 D 路脉冲信号,同时产生时钟脉冲 CP,使得当 A,B 两路信号脉冲接近到一定程度时,后到的信号自动消失,而当它们再接近到一定程度时,两路信号均消失.

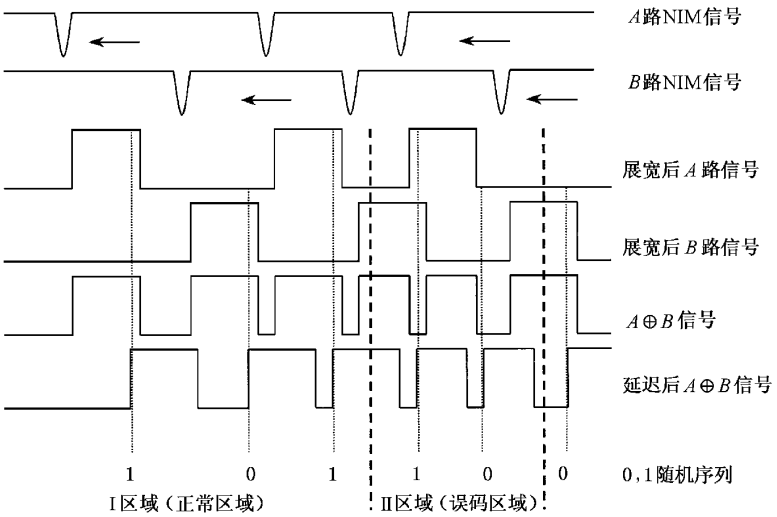

图 2　脉冲信号数据处理电路时序原理图及误码的产生

如图 3 所示,具体的处理方法是:(1)先将两路 Max9686 输出的脉冲 A' 和 B' 的脉宽展宽成约 400ns,之所以展得比较宽是为了保证电路进行正常

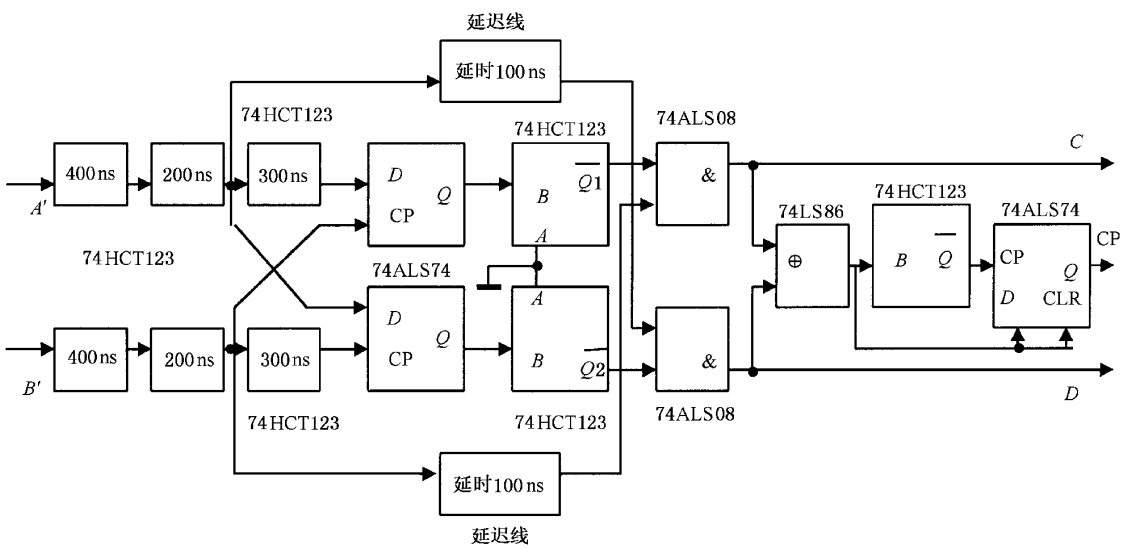

图 3　消除误码的随机信号变换电路原理图

的简单逻辑运算.(2)将两路脉冲的宽度又压缩成约 200ns.(3)将 200ns 的脉冲展宽成约 300ns.(4)用脉宽 200ns 的 A 路信号通过 D 触发器去触发展宽成 300ns 的 B 路信号,D 触发器的输出接单稳态触发器,调节 RC 常数,使其暂稳态的时间为 300ns,将单稳态触发器的 $Q2$ 非作为输出;同时用脉宽 200ns 的 B 路信号通过 D 触发器去触发已展宽成 300ns 的 A 路信号,将单稳态触发器的 $Q1$ 非作为输出.(5)分别将 200ns 的 A,B 两路信号延时 100ns.(6)把 A 延时后的信号和 $Q2$ 非相与,得到 C;同时将 B 延时后的信号和 $Q1$ 非相与,得到 D.(7)把 C 和 D 两路信号进行异或,再通过 74HCT123 和 74ALS74 构成的噪声消除电路,消除信号中两个脉冲彼此的时间间隔小于 20ns 的脉冲,得到输入给后级串并转换电路的时钟脉冲 CP.显然,采用这样的处理方法,会损失一些有效的信号,但为了消除误码,这样做是必要的.

2.3 串并转换电路及计算机数据采集系统

由于光子是顺序地入射的,原始的数据流是串行的,所以除了要把两路由甄别器输出的数据转换成串行的数据流外,还需要将串行数据流转换成并行数据流,以期提高数据采集的速度,充分利用储存空间.为此,本文设计制作了相应串并转换电路板.数据输入给计算机,采用 I/O31TN 接口板,其中的 8253 的输出作为计算机主机的中断请求信号.8253 的工作方式以写端口的方式写入.由于 8253 的分频数至少为 2,这使得数据至少损失一半.但前级的数据流速率可以调节得很快,可以抵消这里的损失.实验中使用 286 计算机做数据采集.运行相应的计算机程序,就可以进行随机数据的自动采集.

由于光电倍增管的响应非常快,产生随机数的速率主要取决于后级脉冲信号处理电路以及接口和计算机总线速度.根据本实验电路的设计和接口选择,随机数采集的速率理论上可以达到 200kbit/s,但实际上为了减少误码,确保系统工作的稳定,只让其工作在 20kbit/s 这个速率上.通过改进电路设计,采用更快的电路(如 ECL 电路)处理信号,使用更快的接口(如 DMA 控制的接口板)和计算机设备,还可以大大提高随机数产生效率.

3 数据处理和随机性检验

计算机采集到的 0,1 比特序列,虽然物理理论认为应该是随机的,但要作为实际的应用,仍然需要进行严格的随机性检验.

检验一个 0,1 序列是否是随机的序列,一般有 5 种检测方法来认定,即频数检验、序列检验、扑克检验、自相关检验和游程检验[9,10].自相关检验和游程检验是有关随机序列不可预测性和线形复杂度的检测方法.对于本实验,这一点是由物理原理来保证的.对实验所取得的原始序列的检验(采用专用的随机性检测软件)也表明,不可预测性和不重复性是良好的.而频数检验反映的是随机性的另一个方面.设有一个含 N 个比特的 0,1 序列,其中有 N_0 个“0”,N_1 个“1”,将 $x^2=(N_0-N_1)^2/N$ 和自由度为 1 的 χ^2 分布表进行比较,比如 5% 显著性水平的 χ^2 值是 3.84,当 $x^2\leqslant 3.84$ 时,可以认为,在 5% 显著性水平的要求内,频数检验通过.序列检验是检验 2 阶即(00,01,10,11)的均衡度,扑克检验是检验更高阶的均衡度.因此,频数检验是首要的一环,也是其他检测手段的基础.

理论上,实验采集的二进制的 0,1 随机数序列的 0,1 的比率应该是各 50%,但是,由于仪器的调节精度的限制,以及电源、电路稳定性的问题,实验所获取的随机数序列的 0,1 比,在一定取样时间和取样长度上,经常是不均衡的.

本实验所要解决的问题就是序列 0,1 的均衡问题,即通过频数的检验.通过对实验手段的改进如果还不能达到要求,就只有对采集到的原始数据进行数学上的处理.处理的方法有很多种,如 von Neumann 提出的方法,对改善序列 0,1 不均衡的有效率最高只有 25%[7];而用 Pere[11] 提出的方法,数据量将损失 50% 以上.而我们由 Huffman 编码方法得到启发,把实验采集到的原始数据压缩为符合密码学要求的真随机序列.

Huffman[12] 编码的思想很简单,它是对较常用的字符使用较短的位图样式.根据熵的概念,可以使这种思想定量化.假设输入字母表中有 N_{ch} 个字符,分别以概率 p_i($i=1,\cdots,N_{ch}$)出现在输入字符串中,因此 $\sum p_i=1$.根据信息论的基本定理,由这些字符组成的相互独立的随机序列平均地要求每个字符至少是 H 位,

$$H=-\sum p_i\log_2 p_i, \tag{1}$$

其中 H 是概率分布的熵.另外,一定存在这种可以任意接近这个边界值的编码方式.对于所有字符 $p_i=1/N_{ch}$ 等概率的情况,很容易得出 $H=\log_2 N_{ch}$,它

是无压缩的情况. p_i 的任意其他集合给出较小的熵,它允许进行有效的压缩.

注意,如果用长度为 $L_i = -\log_2 p_i$ 位的码对字符 i 进行编码,这样方程(1)将平均为 $\sum p_i L_i$,(1)式的边界就可以达到. 这种编码的麻烦是一般 $-\log_2 p_i$ 不是一个整数. Huffman 编码作了一种尝试,即实际上用 $1/2$ 的整数次幂来近似所有的概率 p_i ,因此所有的 L_i 都为整数. 如果所有的概率 p_i 实际上都是 2 的负整数次幂,则 Huffman 码的确达到熵边界 H.

假设某数据含 4 种字符 A(00),B(01),C(10),D(11),这 4 个字符出现的概率分别为 0.18,0.22,0.22,0.38,那么霍夫曼编码可以根据一棵二叉树来获得. 如图 4 所示,该树中的各节点右边的数值表示该节点的概率;每一个非叶子点均有两个树支,所连接的概率小的节点的树支为 0 树支,概率大的为 1 树支. 从根节点出发到任何一个叶子节点终止就构成了一个树支,每一个树支都是由 0,1 构成的一个序列,该序列就是一个叶子节点的霍夫曼码. 因此数据 *CDABD* 经过霍夫曼编码后成为 01001101110.

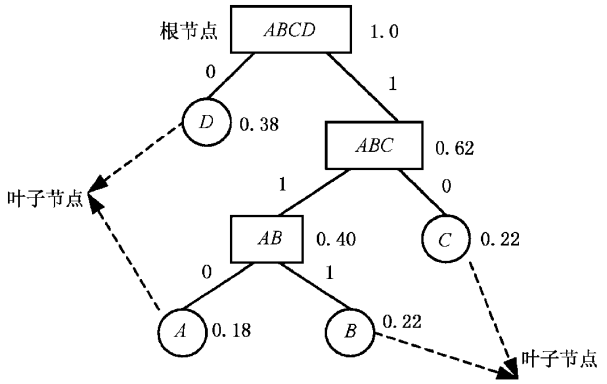

图 4　用二叉树表示的霍夫曼码表

表 1　Huffman 编码和数据压缩方法处理前后序列 0,1 平衡对照表

	处理前的原始序列(130 kbit)			处理后的新序列(130 kbit)		
	1 的比率/%	x^2	显著性水平 α/%	1 的比率/%	x^2	显著性水平 α/%
序列 1	0.496041	8.213	<0.5	0.499641	0.0675	75—90
序列 2	0.491280	39.84	<0.5	0.499336	0.2310	50—75
序列 3	0.489979	52.62	<0.5	0.500610	0.1950	50—70
序列 4	0.488785	65.91	<0.5	0.501099	0.6329	10—25

霍夫曼编码的核心是如何由已知的概率分布来求出相应的霍夫曼码表. 为此,编制了相应的数据处理程序,对实验采集到的原始数据进行了处理. 如表 1 所示,实验采集的原始序列长为 130kbit,对所有采集到的数据组都进行了处理,发现 0,1 不均衡现象都得到了改善. 表 1 选取了 4 组数据作代表,虽然由于实验设备的不稳定性,没有如理论分析那样,原始序列的 0,1 不均衡现象能得到完全的消除,但处理后新序列的显著性水平有显著的提高,并且使用这种处理方法,数据量损失理论上可以达到最小,这对于序列本身并不很长的情况是很重要的.

4　总　结

本文设计制作了基于 50/50 光分束器的二进制的量子物理真随机源,目前的采集速率可达 200kbit/s. 采集到的原始随机序列在使用 Huffman 编码和数据压缩方法处理后,经随机性检验,基本满足随机性的要求. 通过对实验设计的改进,如采用小型的半导体光源和探测器,以及采用新的更快的信号处理电路和数据采集系统,可望在经典信息安全系统、量子保密通讯等应用中实现实用化.

感谢郑伟谋教授在信息论和随机数处理方面的帮助和讨论;感谢吕述望教授在随机数的检测方面提供了帮助.

[1] A. Compagner, *Am. J. Phys.*, **59**(1991), 700.
[2] Th. Sauter, W. Neuhauser, R. Blatt, P. E. Toschek, *Phys. Rev. Lett.*, **57**(1986), 1696.
[3] W. M. Itano, J. C. Bergquist, R. G. Hulet, D. J. Wineland, *Phys. Rev. Lett.*, **59**(1987), 2732.
[4] J. Marron, A. J. Martino, G. M. Morris, *Appl. Opt.*, **25**(1986), 26.
[5] A. J. Martino, G. M. Morris, *Appl. Opt.*, **30**(1991), 981.
[6] J. G. Rarity, P. C. M. Owens, P. R. Tapster, *J. Mod. Opt.*, **41**(1994), 2435.
[7] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, H. Zbinden, Optical Quantum Random Number Generator (Los Alamos Eprint, quant-ph/9907006).
[8] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, A Fast and Compact Quantum Random Number Generator (Los Alamos Eprint, quant-ph/9912118).
[9] T. C. Lu, Information Encrpytion Tachniques (Sichuan Science and Technology Publishing Press, Chengdu, 1989) (in Chinese) [卢铁成 编著,信息加密技术(四川科学技术出版社,成都,1989)].
[10] Y. X. Yang, X. D. Lin, Coding Cryptology (Peoples Posts & Telecommunications Publishing House, Beijing, 1992) (in Chinese) [杨义先、林须端 著,编码密码学(人民邮电出版社,北京,1992)].
[11] Y. Peres, *Annals of Statistics*, **20**(1992), 590.
[12] W. H. Press, S. A. Teukolsky, W. T. Vetterling, B. P. Flannery, Numerical Reicipes in C——The Art of Scientific Computing, Second Edition (Cambridge University Press, Cambridge, 1988), p. 903.

TRUE RANDOM NUMBER GENERATOR BASED ON A PHOTON BEAMSPLITTER*

LIAO JING LIANG CHUANG WEI YA-JUN WU LING-AN PAN SHAO-HUA
(*Laboratory of Optical Physics, Institute of Physics, Chinese Academy of Sciences, Beijing* 100080, *China*)
YAO DE-CHENG
(*Graduate School, University of Science and Technology of China, Beijing* 100039, *China*)
(Received 25 July 2000; revised manuscript received 15 August 2000)

ABSTRACT

A quantum optical true random number generator based on splitting a beam of photons at a 50/50 beamsplitter has been demonstrated. A continuous stream of random numbers at a rate of 200 kbit/s can be generated. A mathematical method (Huffman coding and data compressing) is used to improve the ratio of 0 and 1 bits in the original random number arrays.

Keywords: true random number generator, single photons, beamsplitter, Huffman coding and data compressing
PACC: 4250, 0250, 0762

* Project supported by the National Natural Science Foundation of China (Grant No. 19974073).