基于光子间隙随机分布的真随机数源*

汪龙[1)] 马海强[1)†] 李申[2)] 韦克金[1)]

1) (北京邮电大学理学院, 北京 100876)

2) (中国科学院空间科学与应用研究中心, 北京 100190)

(2012年9月16日收到; 2012年12月2日收到修改稿)

提出了利用模数转换器提高真随机数源速率的方案, 该方案基于衰减脉冲激光光子间隙随机分布, 可使随机数的产生速率提高十几倍. 实验中将时间幅度转换仪与 16 位模数转换器相结合, 产生的各比特位随机数序列顺利通过了国际通用的随机数检测程序统计测试标准, 该方案实验装置简单, 增强了系统的抗干扰能力.

关键词: 衰减式单光子源, 模数转换, 延时符合, 随机数检测

PACS: 03.67.−a, 03.67.Dd, 03.67.Hk, 42.50.Ar **DOI:** 10.7498/aps.62.100303

1 引 言

随机数广泛应用于数值计算、Monte Carlo 模拟、彩票和博彩业等多个领域. 如今随着计算机和通信技术的提高、互联网的广泛普及, 信息的安全性显得愈发重要. 此外保密通信、数字签名、身份认证和密码协议等信息安全技术的重要领域中, 随机数都扮演着一个不可或缺的角色.

人们一直在设法获得高速、稳定、随机性良好的随机源, 总的来说随机数的产生有两种方法, 即伪随机数发生器和真随机数发生器. 伪随机数是通过数学公式计算产生的, 从这一点上来讲其已经不是随机的了, 因为它的产生是可预知的, 对于同样的种子, 产生的随机序列将会是相同的. 在加密应用中如果攻击者拥有了足够的计算能力, 就可以对伪随机数加密进行破解. 真随机数具有真正的随机性和不可预知性, 真随机数一般来源于物理过程: 振荡器的频率抖动 [1]、电阻热噪声 [2]、生物无规特性 [3]、混沌激光 [4−6]、光子间隙随机分布 [7,8] 等.

基于光学系统随机性的随机数源具有操作简单、稳定性易于控制等特点, 目前已经产生了几种真随机数生成方案, 如被囚禁的单离子产生的共振荧光辐射, 利用这种随机性可以研制随机源 [9,10], 但是由于难以进行数据采集所以不常用; 激光斑纹图样空间分布的随机特性也被用于二维随机数的产生 [11,12], 然而由于这些方法产生的随机数速率低、系统较复杂, 限制了它们的应用范围.

本文设计了基于光子间隙随机分布的真随机数源, 通过时幅转换和模数转换将相邻光子的时间间隙差转换为真随机序列, 该方案具有速率快、抗干扰能力强、操作简单易于集成化等优点.

2 实验原理和装置

2.1 实验原理

众所周知, 激光脉冲的光子数呈现泊松分布, 即

$$p_n = \mu^n \mathrm{e}^{-\mu}/n!, \tag{1}$$

上式表示光脉冲中含 n 个光子的概率, μ 表示平均光子数. 当 $\mu \ll 1$ 时脉冲中不包含光子的概率为

$$p_0 = \mathrm{e}^{-\mu} \approx 1 - \mu + \frac{\mu^2}{2}, \tag{2}$$

* 国家重点基础研究发展计划 (批准号: 2010CB23202)、国家自然科学基金 (批准号: 10805006, 61178010, 61177085) 和中央高校基本科研业务费专项资金 (批准号: BUPT2010ZX04) 资助的课题.

† 通讯作者. E-mail: hqma@bupt.edu.cn

脉冲含有一个光子的概率为

$$p_1 = \mu \mathrm{e}^{-\mu}, \tag{3}$$

所以脉冲中含有两个和两个以上光子的概率为

$$p_{n\geqslant 2} = 1 - p_0 - p_1 = 1 - \mathrm{e}^{-\mu}(1+\mu), \tag{4}$$

将一束脉冲激光衰减后, 每个脉冲的平均光子数会降到 0.1 左右. 由 (4) 式可以计算出脉冲中含两个或两个以上光子的概率约为 0.5%, 所以衰减后的脉冲激光器可以等效为一个单光子源. 衰减后的激光脉冲平均每十个脉冲含有一个光子, 该光子在十个脉冲中的位置分布是随机的, 如图 1 所示. 实验中所用激光器 (advanced Laser Diode Systems, Pilas PIL131DFB-SM) 工作的中心波长为 1310 nm, 光脉冲宽度约为 20 ps, 由外部信号发生器提供触发信号, 频率为 1 MHz. 衰减成平均每十个光脉冲含有一个光子, 利用示波器观测光子的到达时间如图 1 所示. 在图 1 中, 示波器的横轴是时间档, 每个格子代表的是 5 μs, 纵轴表示的是电压, 每个格子代表 2 V. 图中的脉冲就是单光子探测器对光子到来时的一个响应输出, 可以清晰地看出相邻脉冲间的时间间隔是很不均匀的、随机的.

2.2 实验装置图分析

基于光子间隙随机分布的真随机源实验装置如图 2 所示. 信号发生器 SFG 为半导体激光器 LD 提供触发信号 (触发频率为 1 MHz, 由于单光子探测其的最大工作频率为 1 MHz, 所以实验系统的时钟频率选在了 1 MHz, 这不影响该方案的原理性演示). 将激光器的输出经过可调衰减器, 衰减 65 dB 至单光子级别, 光子经过光纤和 Y 型耦合器后有 50%的概率进入上面的支路, 被单光子探测器 APD1 接收, 也有 50%的概率进入下面的支路, 被单光子探测器 APD2 接收. 当单光子探测器接收到光子之后会输出一个 TTL 信号, 如图 2 中所示, APD1 的 TTL 输出连接到时幅转换仪 TAC 的 START 端口, APD2 的 TTL 输出连接到 STOP 端口, TAC 会将两个端口所接收到的信号之间的时间差线性地转换为电压值输出, 电压值的范围为 0—10 V.

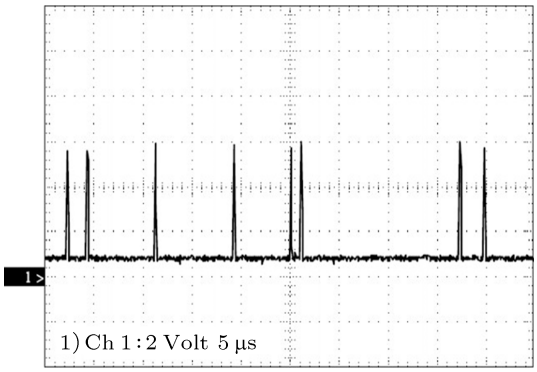

图 1 光子间的时间间隙分布

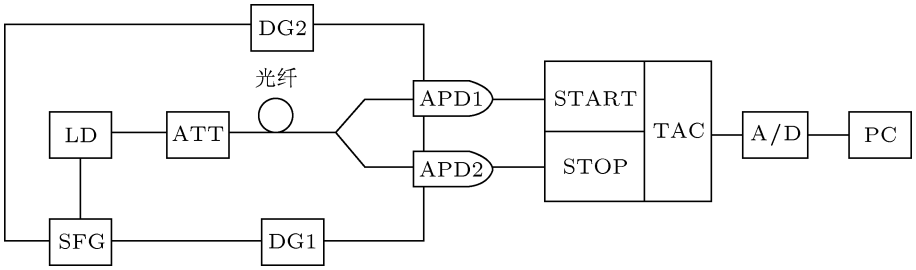

图 2 基于光子间的时间间隙随机分布的真随机源功能框图 LD, 半导体激光器; ATT, 衰减器; APD, 单光子探测器; TAC, 时幅转换仪; A/D, 模数转换器; DG, 延时器; SFG, 信号发生器; PC, 电脑

2.3 延时处理和计算机数据的采集

试验中所用的单光子探测器管芯是 JDS Uniphase EPM239BA InGaAs 雪崩二极管, 暗计数 (噪声) 是雪崩二极管本身固有的性质, 所以暗计数是单光子探测器不可消除的一个因素. 虽然单光子探测器的暗计数是随机的, 理论上暗计数对随机性没有影响, 但是为了对光子间隙的随机性有个正确的体现, 我们采取了缩短探测器的门控时间和延时处理的方式使暗计数的影响几乎降到了零. 在实验中, 单光子探测器工作在没有输入光子且无死时间控制的情况下, 暗计数率约为 650 个/s. 当设置门控时间为 2.5 ns 后, 死时间为 10 μs 时, 测得暗计数率降至 0—5 个/s 而 Y 型耦合器每条支路光子计数率约为 50000 个/s, 暗计数的影响几乎可以忽略. 由于单光子探测器的响应延迟以及光在光路中的传播延时, 所以光子从激光器输出到被探测器接收需要一定的时间. 探测器的门控时间仅为 2.5 ns, 所以必

须通过延时器 DG1 和 DG2 调节单光子探测器的触发信号的延时, 使得光子到达探测器时, 探测器正好被触发工作, 从而能捕获到光子.

TAC 的输出为幅值在 0—10 V 之间变化的脉冲信号, 本文采用了 16 位输出的模数转换器将 TAC 输出的脉冲信号转换为计算机可识别的数字信号, 以便于计算机采集. TAC 的输出为幅值在 0—10 V 之间变化的脉冲信号, 本文采用了 16 位输出的模数转换器将 TAC 输出的脉冲信号转换为计算机可识别的数字信号, 以便于计算机采集, 同时解决了利用激光光子的随机数发生器的随机数生成率低的问题. 2001 年吴令安小组 [13] 利用了单光子透过反射率和透射为 50%的光分束器随机选择路径的方案实现了真随机数发生器, 实现了一个光子对应 1 bit 随机数的生成率, 此方案简单易用, 但是由于激光器必须工作在单光子级别, 其平均光子数很小, 限制了随机数生成的速率, 所以在实验中我们采用了 A/D 转换两个光子之间的时间差所生成的电压信号, A/D 的精度越高, 也即 A/D 每次转换后输出的 bit 位越多, 其可提取的用来作为随机数的 bit 位也相应地增加, 所以提高 A/D 的精度可以提高随机数生成的速率, 实验结果也证明了我们实验方案的正确性与优越性.

3 随机性检验和抗干扰性分析

3.1 结果分析

利用实验中得到的 2662784 bit 的 A/D 的原始输出, 然后将原始的序列分组, 得到 16 组 A/D 每一位的随机数序列, 用 ENT 对其进行了随机性检测. A/D 的最低有效位 (第 14, 15, 16 位) 的检测结果如表 1, 2, 3 所示.

上面 3 位序列的测试结果的各项测试参数都达到了非常好的数值, 符合真随机数的标准, 测试结果还验证了高精度 A/D 对提高随机数产生效率的原理的正确性.

3.2 抗干扰及 A/D 转换电子噪声分析

本文实验方案的最大优点就是其稳定性, 抗干扰能力极强. 实验中我们在 Y 型耦合器的上支路加入一个相位调制器, 等同于人为引入一个相位噪声. 同时相位调制器对上支路的光造成一定的衰减, 使 APD1 的光子计数下降. 然后对 A/D 的结果进行采集和检测, 引入噪声后 A/D 输出的最低有效位 (第 16 位) 的 ENT 检测结果如表 4 所示.

表 1 A/D 的第 16 位输出序列 ENT 检测结果

```
Entropy = 0.999999 bits per bit.

Optimum compression would reduce the size
of this 166424 bit file by 0 percent.

Chi square distribution for 166424 samples is 0.32, and randomly
would exceed this value 56.96 percent of the times.

Arithmetic mean value of data bits is 0.5007 (0.5 = random).
Monte Carlo value for Pi is 3.143928468 (error 0.07 percent).
Serial correlation coefficient is -0.000507 (totally uncorrelated = 0.0).
```

表 2 A/D 的第 15 位输出序列 ENT 检测结果

```
Entropy = 0.999998 bits per bit.

Optimum compression would reduce the size
of this 166424 bit file by 0 percent.

Chi square distribution for 166424 samples is 0.56, and randomly
would exceed this value 45.32 percent of the times.

Arithmetic mean value of data bits is 0.5009 (0.5 = random).
Monte Carlo value for Pi is 3.165849438 (error 0.77 percent).
Serial correlation coefficient is 0.002737 (totally uncorrelated = 0.0).
```

表 3 A/D 的第 14 位输出序列 ENT 检测结果

```
Entropy = 0.999994 bits per bit.

Optimum compression would reduce the size
of this 166424 bit file by 0 percent.

Chi square distribution for 166424 samples is 1.35, and randomly
would exceed this value 24.53 percent of the times.

Arithmetic mean value of data bits is 0.4986 (0.5 = random).
Monte Carlo value for Pi is 3.176233055 (error 1.10 percent).
Serial correlation coefficient is -0.002291 (totally uncorrelated = 0.0).
```

表 4 引入噪声后 A/D 的第 16 位输出序列 ENT 检测结果

```
Entropy = 0.999993 bits per bit.

Optimum compression would reduce the size
of this 21408032 bit file by 0 percent.

Chi square distribution for 21408032 samples is 3182.42, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bits is 0.5061 (0.5 = random).
Monte Carlo value for Pi is 3.075695067 (error 2.10 percent).
Serial correlation coefficient is -0.001821 (totally uncorrelated = 0.0).
```

由于在 TAC 之后引入了 A/D 转换电路去转换 TAC 输出的电压信号, 而 A/D 转换电路的电子学噪声会不会对生成的随机数的随机性造成影响呢? 电路中的电子学噪声是不可能消除的, 但是噪声本身也是一种随机源, 理论上不会对随机数的随机性造成影响, 本文做了下面的对比性验证.

在其他的实验条件不变的情况下, 换用同类型的 A/D 来代替先前实验中的 A/D 模块, 再多次进行数据的采集、分析后, 依然可以得到随机性良好的随机数序列 (如表 5 所示), 由此可见这种随机的电子学噪声不会对我们的随机数序列造成坏的影响.

表 5 更换 A/D 后的第 16 位输出序列的 ENT 检测结果

```
Entropy = 0.999998 bits per bit.

Optimum compression would reduce the size
of this 587864 bit file by 0 percent.

Chi square distribution for 587864 samples is 230.00, and randomly
would exceed this value less than 0.01 percent of the times.

Arithmetic mean value of data bits is 0.4991 (0.5 = random).
Monte Carlo value for Pi is 3.153473504 (error 0.38 percent).
Serial correlation coefficient is -0.000813 (totally uncorrelated = 0.0).
```

4 结 论

本文提出了一个基于光子间隙随机分布的真随机数源, 采用了两个单光子探测、TAC 及高精度的 A/D, 将其随机的光子之间的时间间隙线性地转换为电压值, 并转换为高质量多个的真随机数序列, 通过了 ENT 全部测试. 该方案结构简单, 易于集成, 具有极强的抗干扰能力, 并且能提高随机数生成的效率.

[1] Bucci M, Germani L, Luzzi R, Trifiletti A, Varanonuovo M 2003 *IEEE Trans. Comput.* **52** 403
[2] Petrie C S, Connelly J A 2000 *IEEE Trans. Circuits Syst.* I **47** 615
[3] Zhou Q, Hu Y, Liao X F 2008 *Acta Phys. Sin.* **57** 5413 (in Chinese) [周庆, 胡月, 廖晓峰 2008 物理学报 **57** 5413]
[4] Argyris A, Hamacher M, Chlouverakis K E, Bogris A, Syvridis D 2008 *Phys. Rev. Lett.* **100** 194101
[5] Wang A B, Wang Y C, Wang J F 2009 *Opt. Lett.* **34** 1144
[6] Wang Y C, Zhang G W, Wang A B, Wang B J, Li Y L, Guo P 2007 *Acta Phys. Sin.* **56** 4372 (in Chinese) [王云才, 张耿玮, 王安帮, 王冰洁, 李艳丽, 郭萍 2007 物理学报 **56** 4372]
[7] Ma H Q, Xie Y J, Wu L A 2005 *Appl. Opt.* **36** 7760
[8] Michael W, Matthias L, Michael B, Tino Röhlicke, Hans-Jüürgen R, Oliver B 2011 *Appl. Phys. Lett.* **98** 171105
[9] Sauter Th, Neuhauser W, Blatt R, Toschek P E 1986 *Phys. Rev. Lett.* **57** 1696
[10] MItano W, Bergquist J C, Hulet R G, Wineland D J 1987 *Phys. Rev. Lett.* **59** 2732
[11] Matron J, Martino A J, Morris G M 1986 *Appl. Opt.* **25** 26
[12] Martino A J, Morris G M 1991 *Appl. Opt.* **30** 981
[13] Liao J, Liang C, Wei Y J, Wu L A, Pan S H, 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]

High-speed truly random number generator based on the random time distribution of single photons*

Wang Long[1)] Ma Hai-Qiang[1)†] Li Shen[2)] Wei Ke-Jin[1)]

1) (*School of Sciences, Beijing University of Posts and Telecommunications, Beijing* 100876*, China*)

2) (*Center for Space Science and Applied Research, Chinese Academy of Sciences, Beijing* 100876*, China*)

(Received 16 September 2012; revised manuscript received 2 December 2012)

Abstract

In this paper, we present a high-speed physical quantum random number generator using analog/digital converter (ADC), which is based on the random time distribution of single photons emitted by the stongly attenuated pulsed laser diode. With this scheme, the generation rate of random numbers can increase more than tenfold. A preliminary experiment consists of the time amplitude converter and 16 bit ADC, and the data generated by the system pass the pseudo-random number test program test standards. The experimental setup is efficient and robust against mechanical and temperature disturbances.

Keywords: attenuate single photon source, analog-to-digital conversion, delay coincidence, number test program test

PACS: 03.67.−a, 03.67.Dd, 03.67.Hk, 42.50.Ar **DOI:** 10.7498/aps.62.100303

* Project supported by the National Basic Research Program of China (Grant No. 2010CB23202), the National Natural Science Foundation of China (Grant Nos. 10805006, 61178010, 61177085) and the Fundamental Research Funds for the Central Universities of China (Grant No. BUPT2010ZX04).

† Corresponding author. E-mail: hqma@bupt.edu.cn