第 59 卷 第 11 期 2010 年 11 月
1000-3290/2010/59(11)/7679-07

物 理 学 报
ACTA PHYSICA SINICA

Vol. 59, No. 11, November, 2010

外腔半导体激光器随机数熵源的腔长分析*

张继兵 张建忠 杨毅彪 梁君生 王云才†

(太原理工大学理学院物理系, 太原 030024)

(2010 年 2 月 7 日收到;2010 年 3 月 1 日收到修改稿)

利用光反馈半导体激光器产生的混沌激光作为随机数熵源,详细研究了混沌源外腔长度对 500 Mbit/s 随机数特性的影响. 研究表明: 在单路混沌源情况下,外腔反馈引起的谐振会使产生的随机序列具有弱周期性,且当外腔反馈时间与采样时间的比值为整数时,产生序列的随机性最差,仅能通过 NIST 统计测试 2,3 项;在两路混沌源情况下,当混沌源的外腔长不相等且不成比例时,通过两路异或处理可消除由外腔反馈引起的弱周期性,产生的随机序列能够通过 NIST 的全部统计测试项.

关键词: 混沌, 真随机数发生器, 半导体激光器, 外腔长

PACC: 0545, 0540

1. 引 言

随机数在密码学和测试等领域具有广泛的应用. 在密码学方面,对称加密算法的密钥必须是随机产生,公开加密算法在产生密钥对时也需要随机数. 此外许多数字签名算法和密码协议也要求使用随机数[1]. 在测试方面,随机数可用于眼图和误码率的测试,来检测通信系统的传输质量,可用作雷达中的测距信号,遥控遥测中的测控信号等.

随机数发生器一般可以分为伪随机数发生器(PRNG)与真随机数发生器(TRNG)两种. PNRG 是利用计算机,通过算法获得,随着算法的改进和计算机运算能力的提高,目前已可获得 2^{800}-1 码长的 PRNG. 经过仔细设计的 PRNG,可以在一定程度上保证攻击者在有限的计算资源下无法推测未知序列. 但是,PRNG 是由种子通过一个确定的算法生成的,并不是真正意义的随机数. 然而,TRNG 建立在一种称为熵源(entropy source)的不确定性源的基础上,所产生的随机序列无法预知,不可再现,因此能够更好地保障信息的安全. 产生真随机数的方法很多: 例如对电路或电子元件的热噪声直接放大[2]; 基于振荡器采样的随机数发生器[3]; 利用量子力学基本量的完全随机性产生随机数[4,5],如放射性元素的衰变,激光斑纹图案空间分布的随机性等; 通过构造混沌电路产生真随机数[6]以及通过采集生物的无规律行为产生随机数[7]等. 但受物理熵源中电子器件带宽的限制,以上方法产生的真随机数速率比较低,通常仅为几十 Mbit/s[8,9].

目前,半导体激光器在光反馈、光注入、光电反馈方式下,可产生数 GHz 带宽的混沌激光[10],已在混沌光通信[11],混沌激光雷达[12]、混沌光时域反射仪[13]等方面有了成功的应用. 2007 年,我们提出用光反馈半导体激光器产生的宽带混沌激光作为真随机数产生的物理熵源,构造快速真随机数发生器的专利方案[14]. 2008 年,Uchida 等人[15,16]基于光反馈半导体激光器,利用两路不相关的混沌激光经模数转换、逻辑异或处理首次实验产生了 1.7 Gbit/s 的真随机数. 2009 年,Kanter 研究小组[17]基于光反馈半导体激光器,提出使用 8 位模数转换器对混沌激光进行采样,并结合后续差分处理技术,可产生出 12.5 Gbit/s 的真随机数. 最近,他们进一步提出利用后续多级差分处理技术可获得码率达 300 Gbit/s 的真随机数[18]. 然而,理论和实验研究表明: 半导体激光器在光反馈下产生的混沌激光振荡状态中含有反馈引起的谐振成分,退化了混沌激光的无序性. 因而,在基于混沌激光产生真随机数的基础上,需进一步研究混沌源光反馈引起的谐振因素对随机数特性的影响,从而消除这一影响.

本文利用光反馈半导体激光器产生的宽带混

* 国家自然科学基金专项基金(批准号: 60927007), 量子光学与光量子器件国家重点实验室开放课题(批准号: 200903) 资助的课题.

† 通讯联系人. E-mail: wangyc @ tyut. edu. cn

沌激光作为熵源,实现了码率为 500 Mbit/s 的真随机数,通过了随机数统计测试标准(NIST SP 800-22). 基于 NIST 统计测试标准和归一化熵分析,分别研究了在单路和双路混沌源情况下,混沌源外腔长度对随机序列的随机性及码率的影响. 本研究为基于混沌激光源产生高速、高质量的真随机数提供理论指导.

2. 实验原理

图 1(a)为基于混沌激光产生随机数的装置示意图. 两个激光混沌源输出两路不相关的混沌光信号,经过光电探测器转换成电信号,并通过比较器、触发器进行模数转换,产生两路二进制码序列. 最后将两路不相关的二进制码序列进行逻辑异或运算产生一路真随机数序列. 随机数的码率是由加在触发器上的采样时钟确定. 在我们的研究中,混沌激光信号是实验上通过光反馈半导体激光器获得,如图 1(b)所示. 无光隔离器的分布反馈(DFB)半导体激光器(WTD LDM5S752,中心波长为 1550 nm,阈值电流为 22.5 mA)输出的光可通过光纤反射镜(FOM)反馈回谐振腔中,反馈光的强度和偏振态分别通过可调谐衰减器(VOA)和偏振控制器(PC)来调节,并用光功率计(OPM)监控反馈光强度;当反馈光的强度达到 10%,DFB 半导体激光器可通过耦合比为 40∶60(60% 输出,40% 反馈)的耦合器输出混沌激光. 利用带宽为 2 GHz 的光电探测器将输出的混沌光信号转换成电信号,然后将电信号输入到频谱分析仪(Agilent E4407B)中进行测量,并输入到带宽为 500 MHz,采样率为 5 Gs/s 的实时示波器(Tektronix TDS3052)中进行采集存储. 而后续的模数转换(包括比较、触发)、逻辑异或处理以及随机序列的输出都通过数字离线系统软件实现. 受示波器带宽的限制,通过数字离线系统软件设置采样时钟时,对存储的混沌信号每 10 个数据点提取出 1 个进行比较、触发,其输出作为随机序列的 1 位,最终产生的随机数序列码率为 500 Mbit/s.

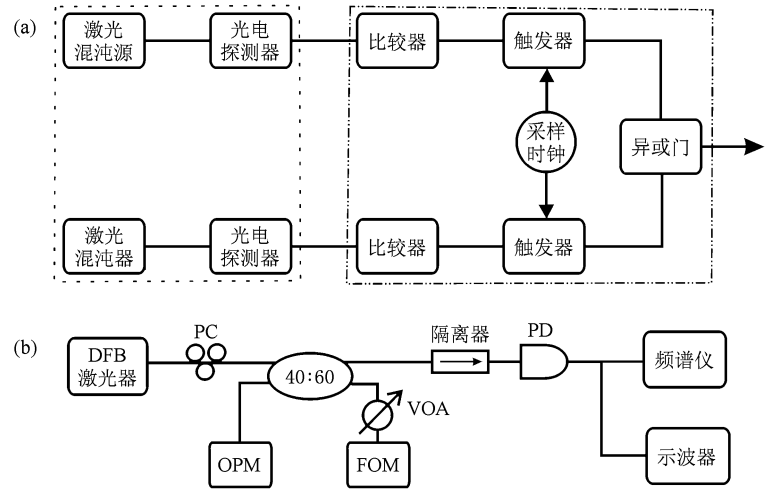

图 1 装置示意图 (a)基于混沌激光的随机数发生器;(b)混沌激光产生的实验装置图(PC 为偏振控制器,OPM 为光功率计,FOM 为光纤反射镜,VOA 为可调谐衰减器,PD 为光电探测器)

3. 随机序列的实现

利用光反馈半导体激光器产生宽带混沌激光,我们已经做了详细的实验研究[19]. 当 DFB 半导体激光器的工作电流为 1.5 倍阈值电流,外腔长为 7.5 m,反馈强度为 10% 时,可输出李雅普诺夫指数为 6.41 的混沌激光信号. 图 2 给出了混沌激光相应的频谱,经过计算带宽为 6.2 GHz. 图 3(a),(b)分别为混沌源 1 和混沌源 2 输出混沌的时序图,直线代表参考阈值,空心圆点代表在频率为 500 MHz 的采样时钟控制下,提取出的数据点. 图 3(c),(d)分别为图 3(a),(b)中提取出的数据点与参考阈值相比较产生的二进制码序列,码率为 500 Mbit/s,以非归零码形式输出. 图 3(e)为两路二进制码序列 3(c),(d)进行异或产生的真随机数序列.

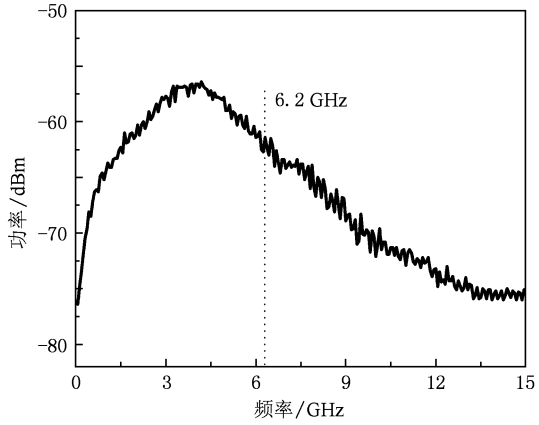

图 2　输出混沌激光的频谱图

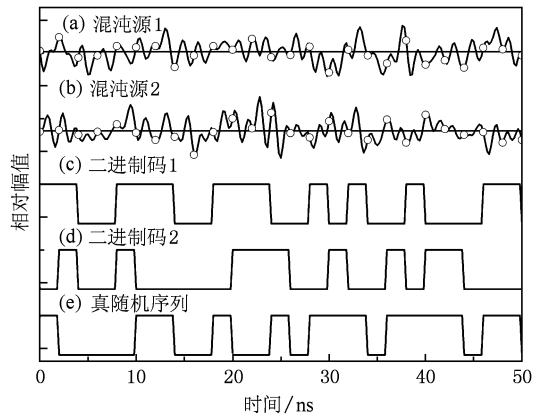

图 3　基于混沌激光产生的随机数　(a),(b)分别为混沌源 1 和混沌源 2 输出混沌的时序图,直线代表参考阈值,空心圆点代表在频率为 500 MHz 的采样时钟控制下,提取出的数据点;(c),(d)分别为与(a),(b)对应的二进制码序列;(e)为(c)和(d)异或后产生的真随机序列

本文采用美国国家标准和技术研究所(national institute of standards and technology,NIST)提供的 15 项统计测试标准(NIST special publication 800-22)对产生的随机数进行检测[1]. 在此,采集了 1000 组 1 Mbit 的二进制数据进行 15 项测试,其中,显著水平数值选为 $\alpha = 0.01$. 在测试中如果 $P > \alpha$, 表明通过了测试项. 进一步评估序列的有效性及正确性,要求在 1000 组数据中每项测试的通过概率超过 0.9806. 典型的 NIST 统计测试结果如表 1 所示.

表 1 说明利用两路不相关的混沌源产生的码率为 500 Mbit/s 的二进制码序列具有足够的随机性,能通过 NIST 的全部测试. 在实验中产生随机数的码率主要受限于采集数据的实时示波器 500 MHz 带宽的限制,若利用带宽更高的示波器或采集卡存储数据,随机数的码率还可以达到更高.

表 1　NIST 统计测试结果

测试名称	P	概率	结果
频数	0.040560	1.000	通过
块内频数	0.043534	0.991	通过
累加	0.053110	0.987	通过
游程	0.265361	0.989	通过
块内最长游程	0.062602	0.990	通过
矩阵秩	0.674793	0.988	通过
离散傅立叶变换	0.760384	0.994	通过
非重叠模板匹配	0.016624	0.996	通过
重叠模板匹配	0.404101	1.000	通过
通用统计	0.279316	0.998	通过
近似熵	0.524346	0.985	通过
随机游动	0.127385	1.000	通过
随机游动变量	0.123051	0.997	通过
连续性	0.710993	0.991	通过
线性复杂度	0.521757	0.994	通过

4. 混沌源外腔长对随机序列的影响

在单路混沌源的情况下,研究外腔反馈时间 τ_{ext}(光在外腔往返一周的时间)与采样时间 τ_s(采样时钟频率的倒数)的比值 τ_{ext}/τ_s 对生成序列随机性的影响. 首先对比较器的阈值进行仔细调节,优化 1/0 比率接近于 50∶50. 固定混沌源的外腔长不变,通过改变采样时间,选择 τ_{ext}/τ_s 不同比值下的二进制码序列,对其随机性进行 NIST 统计测试. 当外腔长分别为 5.6 m 和 8.4 m 时,其测试结果如图 4 所示.

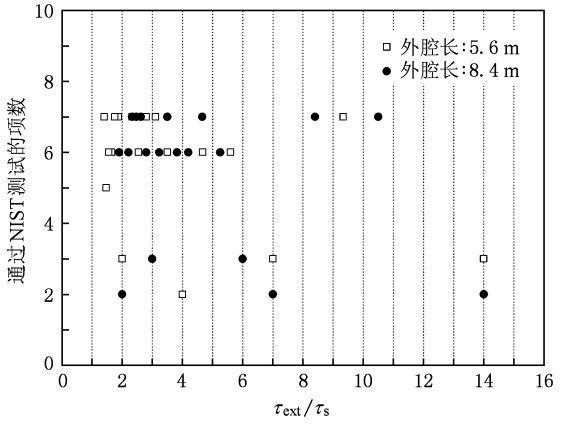

图 4　在不同 τ_{ext}/τ_s 组合下,通过 NIST 统计测试项数的情况

为了能够更好的凸显外腔长和采样时钟之间

的关系,选用单路混沌源产生随机数,即后续处理没有利用两路异或来改善随机性. 因此,从图中 4 看到,在上述的两种外腔长下,都没有出现 15 项测试全部通过的情况. 而且,我们发现随机序列通过 NIST 测试的项数随着 τ_{ext}/τ_s 的比值变化而改变. 当外腔长为 5.6 m(对应的 τ_{ext} 为 56 ns)时,通过改变采样时间 τ_s 为 2,4,6,8 至 40 ns,可使 τ_{ext}/τ_s 的比值分别取到整数和非整数. 当 τ_{ext}/τ_s 的比值分别为 2,4,7,14 等整数时,生成的随机序列通过 NIST 测试仅为 2,3 项. 而当 τ_{ext}/τ_s 的比值为 2.5,3.1,4.6 等非整数时,可以通过 6 至 7 项 NIST 测试. 对于外腔长为 8.4 m 时,可得到类似的结果,如图 4 所示. 这是由于在单路混沌源情况下,外腔反馈引起的谐振成分会使产生的随机数具有弱周期性. 当 τ_{ext}/τ_s 为整数时,外腔引起的弱周期性在生成的随机序列中显现,使其随机性变差;而当 τ_{ext}/τ_s 为非整数时,外腔引起的弱周期性受到一定程度的破坏,其随机性变好.

为了消除单路混沌源产生随机序列的弱周期性,可采用两路不相关随机序列进行异或处理. 因此,需分析在双路混沌源的情况下,外腔长对随机序列特性的影响.

在双路混沌源的情况下,研究在两个混沌源不同的外腔长组合时,产生的随机数通过 NIST 统计测试的情况,测试结果如表 2 所示(表中数值代表通过 NIST 测试的项数). 实验中,两个混沌源激光器的偏置电流均为 34.85 mA,外腔反馈强度均为 10%,选择两个混沌源的外腔长在 3.5 至 8.4 m 之间变化.

表 2 在两路混沌源不同外腔长组合下,通过 NIST 统计测试项数的情况

外腔长/m	3.5	5.6	6.3	7	7.5	8.4
3.5	14	15	15	14	15	15
5.6	15	14	15	15	15	15
6.3	15	15	13	15	15	15
7	14	15	15	13	15	15
7.5	15	15	15	15	14	15
8.4	15	15	15	15	15	10

从表中可以看出,当两路混沌源的外腔长不相等且不成比例时,产生随机数可以通过 NIST 的全部测试项. 而当两路混沌源的外腔长相等或成比例时,不能通过全部测试项. 为了说明原因,图 5 进一步给出了两路混沌源的外腔长相等与不相等时,输出的混沌信号和对应生成二进制码的自相关情况. 从图 5(a)和(b)可以看出,两个自相关曲线的次高峰分别在 56 和 63 ns 处,这表明两个混沌源的外腔长分别为 5.6 和 6.3 m,尽管作为混沌源的两个半导体激光器工作电流和反馈强度相同,但由于外腔长不同,会输出不同状态的混沌激光. 从这两路混沌激光中提取出两路不相关的二进制随机码,进而作异或处理可消除单路混沌源产生随机序列的弱

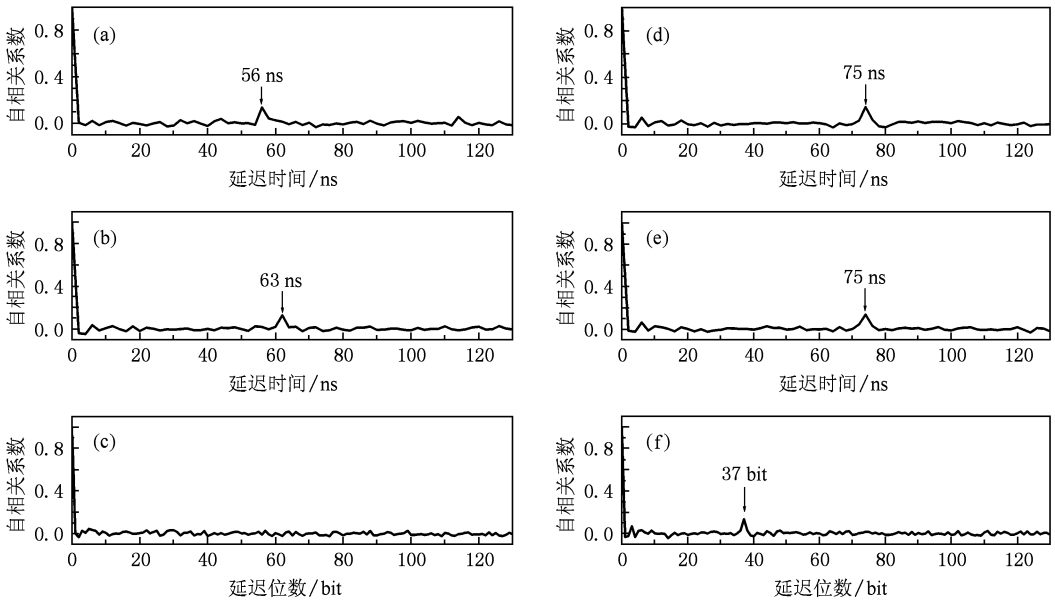

图 5 混沌信号和二进制码对应的自相关图 (a)和(b)外腔长分别为 5.6 和 6.3 m 输出的混沌信号;(c)为外腔长不同两路异或产生的二进制码;(d)和(e)外腔长都为 7.5 m 输出的混沌信号;(f)为腔长相同两路异或产生的二进制码

周期性，提高其随机性. 正如图 5(c)所示，利用两路混沌源产生二进制码序列的自相关曲线没有明显的次高峰. 而当两路混沌源外腔长相等都为 7.5 m 时，如图 5(d)和(e)所示，两个自相关曲线的次高峰都在 75 ns 处. 由于两个半导体激光器处在相同的工作状态下，以这两路混沌源产生的随机数具有非常强的相关性. 进行异或处理后，产生的二进制码序列对应的自相关曲线中仍然还有次高峰，如图 5(f)所示. 自相关曲线中的次高峰在 37 位处对应于外腔反馈时间与采样时间的比值，这说明通过外腔长相同的混沌源产生的两路随机序列异或处理不会消除外腔长引起的弱周期性. 因而，正如表 2 所示，当外腔长相等或成比例时，随机数测试不能通过全部的测试项.

5. 外腔长的归一化熵分析

熵是一种对随机性或不确定性的度量，随机数序列的理想情况是归一化熵值为 1，归一化熵的表达式为

$$H = -\frac{1}{m}\sum_{i=0}^{2^m-1} P_i \log_2 P_i, \qquad (1)$$

其中，m 为所选择的测试块长，每块的取值可以从 0 到 2^m-1. P_i 为在整个测试序列中，取值为 i 的块的概率 ($i = 0$—$2^m - 1$).

研究在不同外腔长组合下，归一化熵值随块长 m 的变化情况，包括：1)单独一路混沌源(外腔长为 5.6 m)，2)单独一路混沌源(外腔长为 7 m)，3)两路混沌源外腔长相等时(都为 7，7 m)，4)两路混沌源外腔长不相等时(分别为 7，6.3 m)，结果如图 6 所示. 可以看出，在单路混沌源情况下，归一化熵值会在块长 m 增大到某个特殊值时突然下降，该特殊值对应外腔反馈时间与采样时间的比值(此处采样时间定为 6 ns). 例如，当外腔长为 5.6 m 时，外腔反馈时间为 56 ns，采样时间为 6 ns，归一化熵值在块长 m 为 9 处突然下降. 说明在单路混沌源情况下，产生的随机数序列具有弱周期性，周期长度与外腔长成正比. 对于外腔长为 7 m 的情况，会出现同样的结果. 在双路混沌源情况下，当两路混沌源外腔长相等时(都为 7，7 m)，与单独一路混沌源时(外腔长为 7 m)相比较，其归一化熵值有明显提高，但当块长 m 为 11 时仍会突然下降. 说明外腔反馈引起的弱周期性仍然存在. 当两路混沌源外腔长不相等时(分别为 7，6.3 m)，归一化熵值不随块长 m 变化，保持为 1. 这和前面得到的结论相同：当两路混沌源的外腔长不相等且不成比例时，异或处理可以消除由外腔引起的弱周期性，可产生真随机数序列.

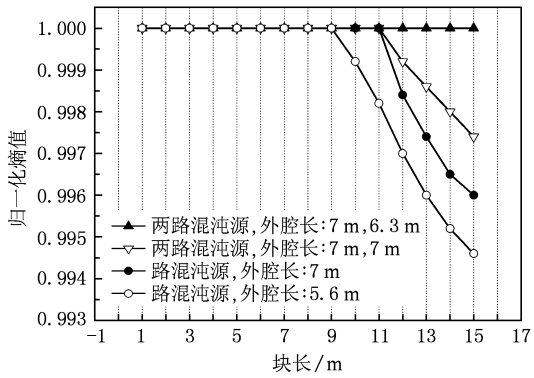

图 6　在不同的外腔长组合下，归一化熵值随块长 m 变化的四种情况 1)，2)单独一路混沌源(外腔长分别为 5.6，7 m)；3)两路混沌源外腔长相等时(都为 7 m)；4)两路混沌源外腔长不相等时(分别为 7，6.3 m)

6. 结　　论

本文利用光反馈半导体激光器产生的宽带混沌激光作为物理熵源，实现了码率为 500 Mbit/s 的随机数，并且通过了 NIST 的随机数统计测试标准(NIST SP 800-22). 实验研究了混沌源外腔长对随机数特性的影响，结果表明：在单路混沌源情况下，外腔反馈使产生的随机数具有弱周期性，产生的随机序列不能通过全部随机数统计测试项；在外腔长一定的情况下，当外腔反馈时间 τ_{ext} 与采样时间 τ_s 的比值 τ_{ext}/τ_s 为整数时，随机序列仅能通过 NIST 统计测试的 2，3 项. 因而，在外腔长取定的情况下，为了获得高质量的随机数，其采样时钟的速率 $1/\tau_s$ 是不可取的；在两路混沌源情况下，只有当两路外腔长不相等且不成比例时，通过异或处理才可有效消除由外腔反馈引起的弱周期性，产生的随机序列能够通过所有的 NIST 统计测试项. 本研究为基于混沌激光源产生高速、高质量的真随机数提供理论指导.

感谢山西省教育厅提供的资金支持，感谢陈莎莎、杨丛渊就本文工作展开的有益讨论.

[1] NIST Special Publication 800-22, http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html, 2001

[2] Petrie C S, Connelly J A 2000 *IEEE Trans. Circuits Syst.* Ⅰ **47** 615

[3] Bucci M, Germani L, Luzzi R, Trifiletti A, Varanonuovo M 2003 *IEEE Trans. Computers* **52** 403

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

[5] Feng M M, Qin X L, Zhou C Y, Xiong L, Ding L E 2003 *Acta Phys. Sin.* **52** 72 (in Chinese) [冯明明、秦小林、周春源、熊 利、丁良恩 2003 物理学报 **52** 72]

[6] Huang Z, Zhou T, Bai G Q, Chen H Y 2004 *Chinese Journal of Semiconductors* **25** 333 (in Chinese) [黄 谆、周涛、白国强、陈弘毅 2004 半导体学报 **25** 333]

[7] 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]

[8] Bucci M, Germani L, Luzzi R, Trifiletti A, Varanouvo M 2003 *IEEE Trans. Computers* **52** 403

[9] Dynes J F, Yuan Z L, Sharpe A W, Shields A J 2008 *Appl. Phys. Lett.* **93** 031109

[10] Argyris A, Hamacher M, Chlouverakis K E, Bogris A, Syvridis D 2008 *Phys. Rev. Lett.* **100** 194101

[11] Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fischer I, García-Ojalvo J, Mirasso C R, Pesquera L, Shore K A 2005 *Nature* **438** 343

[12] Lin F Y, Liu J M 2004 *IEEE J. Quantum Electron.* **40** 815

[13] Wang Y C, Wang B J, Wang A B 2008 *IEEE Photon. Technol. Lett.* **20** 1636

[14] Wang Y C, Tang J H, Zhang M J *Chinese patent* ZL200710062140.1 2007 (in Chinese) [王云才、汤君华、张明江 中国发明专利 ZL200710062140.1 2007]

[15] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashige T, Shiki M, Yoshimori S, Yoshimura K, Davis P 2008 *Nature Photon.* **2** 728

[16] Hirano K, Amano K, Uchida A, Naito S, Inoue M, Yoshimori S, Yoshimura K, Davis P 2009 *IEEE J. Quantum Electron.* **45** 1367

[17] Reidler I, Aviad Y, Rosenbluh M, Kanter I 2009 *Phys. Rev. Lett.* **103** 024102

[18] Kanter I, Aviad Y, Reidler I, Cohen E, Rosenbluh M 2010 *Nature Photon.* **4** 58

[19] Wang A B, Wang Y C, He H C 2008 *IEEE Photon. Technol. Lett.* **20** 1633

Randomness analysis of external cavity semiconductor laser as entropy source*

Zhang Ji-Bing Zhang Jian-Zhong Yang Yi-Biao Liang Jun-Sheng Wang Yun-Cai†

(*Department of Physics*, *College of Science*, *Taiyuan University of Technology*, *Taiyuan* 030024, *China*)

(Received 7 February 2010; revised manuscript received 1 March 2010)

Abstract

In this paper, we employ chaotic light as an entropy source, generated by semiconductor lasers with optical feedback induced by external cavity, to generate 500 Mbit/s random number sequence and then study specifically the influence of external cavity length on randomness. The results indicate that the generated random sequence has an weak periodicity caused by the external cavity feedback under a single-channel chaotic source, and can only pass two or three tests of the National Institute of Standards and Technology (NIST) when the external-cavity round trip delay time is an integral multiple of the sampling time. On the other hand, the weak periodicity can be eliminated by using two different chaotic sources when their external cavity lengths are unproportional to each other, and the obtained random sequence can pass all tests of the NIST after XOR processing.

Keywords: chaos, random number generator, semiconductor lasers, external cavity length

PACC: 0545, 0540

* Project supported by the Special Funds of the National Natural Science Foundation of China (Grant No. 60927007), the Open Subject of the State Key Laboratory of Quantum Optics and Quantum Optics devices of China (Grant No. 200903).

† Correspondence author. E-mail: wangyc @ tyut. edu. cn