物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

反馈强度对外腔反馈半导体激光器混沌熵源生成的随机数序列性能的影响

杨海波　吴正茂　唐曦　吴加贵　夏光琼

Influence of feedback strength on the characteristics of the random number sequence extracted from an external-cavity feedback semiconductor laser

Yang Hai-Bo　Wu Zheng-Mao　Tang Xi　Wu Jia-Gui　Xia Guang-Qiong

引用信息 Citation: Acta Physica Sinica, 64, 084204 (2015)　DOI: 10.7498/aps.64.084204
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.084204
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I8

反馈强度对外腔反馈半导体激光器混沌熵源生成的随机数序列性能的影响*

杨海波 吴正茂 唐曦 吴加贵 夏光琼†

(西南大学物理科学与技术学院, 重庆 400715)

(2014 年 7 月 15 日收到; 2014 年 10 月 25 日收到修改稿)

外腔反馈半导体激光器在合适的反馈强度下将呈现混沌态, 其输出的激光混沌信号可作为物理熵源获取物理随机数序列. 着重研究了外腔反馈强度对最后获取的二元码序列的随机性的影响. 数值仿真结果表明, 随着反馈强度的增加, 外腔反馈半导体激光器输出的混沌信号的延时时间特征峰值呈现先逐渐减小再逐渐增大的过程, 而对应的排列熵特征值呈现先增大、后缓慢降低的过程, 即存在一个优化的反馈强度可使输出的混沌信号的延时特征得到有效抑制且复杂度高. 利用 NIST Special Publication 800-22 软件对基于不同反馈强度下外腔半导体激光器输出的混沌信号所产生的二元码序列的随机性进行了相关测试, 并讨论了反馈强度的大小对测试结果的影响.

关键词: 外腔反馈半导体激光器, 反馈强度, 混沌, 随机数

PACS: 42.55.Px, 05.45.–a, 05.45.Gg, 05.40.–a **DOI:** 10.7498/aps.64.084204

1 引 言

随机数在通信和计算等领域具有广泛的应用[1−4]. 在信息安全领域, 随机数可应用于密钥管理、数字签名以及身份认证等众多安全技术中, 以确保信息的机密性、真实性和完整性; 随机数也可用于解决材料科学、生物物理学和金融业等领域的数值采样计算问题.

随机数可分为伪随机数和真随机数. 伪随机数是由初始种子通过一个确定算法计算生成的. 伪随机数发生器具有易构建、速率高的优点, 但其生成的序列长度有限且存在周期性, 如果应用于信息系统会存在极大的安全隐患[5]. 真随机数则是由物理熵源产生的, 真随机数序列具有不可预测性, 因而具有更高的安全性. 电阻热噪声[6]、电子振荡器的频率抖动[7]、电路混沌[8]、激光器相位噪声等[9]都可以用作真随机数发生器的熵源. 此外, 利用量子力学基本量的完全随机性以及采集生物的无规律行为也可以用作真随机数发生器的熵源[10−12]. 但是由于熵源带宽的限制, 这些真随机数发生器产生随机数的速率多处于 Mbit/s 量级, 无法满足当前高速大容量通信的需要.

已有的研究表明, 半导体激光器在光反馈、光注入或光电反馈等扰动下, 可产生数 GHz 带宽的激光混沌信号[13−20]. 近些年来, 基于半导体激光器在外部扰动下获得的宽带混沌信号作为物理熵源获取高速的真随机数逐渐受到相关领域学者和业界的高度关注. 例如, Uchida 等[21]利用两个独立的外腔半导体激光器所产生的两路混沌激光分别经过 1 位模数转换器 (ADC) 转换后做异或 (XOR) 运算, 实验获得了速率为 1.7 Gbit/s 的真随机数序列. Kanter 等使用 8 bit ADC 将单路激光混沌信号转换成 8 bit 的二元码序列, 通过后续的一级差分处理和选取 m 最低有效位 (LSBs) 获得了速率为 12.5 Gbit/s 的真随机数[22], 进一步采用多级差分

* 国家自然科学基金 (批准号: 61178011, 61275116, 61475127, 11474233)、重庆市自然科学基金 (批准号: 2012jjB40011) 和中央高等学校基本科研业务费专项资金 (批准号: XDJK2014C079) 资助的课题.

† 通信作者. E-mail: gqxia@swu.edu.cn

处理获得了300 Gbit/s的真随机数[23]. 国内太原理工大学、西南大学等单位的相关课题组在基于半导体激光器获取真随机数方面也取得了一些重要进展[24,25]. 在目前报道的基于半导体激光器输出的混沌信号获取高速随机数的方案中, 一方面可通过采用XOR、多级差分等后续运算处理以提高所产生的随机数的速率, 另一方面对混沌熵源本身的优化也是提高所产生的随机数性能的重要途径. 目前, 关于物理熵源中一些关键参数对所获取的随机数性能的影响已受到人们的关注. 近年来关于外腔长度、反馈强度、激光器的偏置电流、激光器的弛豫振荡频率等对基于外腔反馈半导体激光器产生的随机数序列速率的影响等方面的研究相继被报道[26−29]. 其中, 目前已报道的关于外腔反馈强度对基于外腔反馈半导体激光器获取随机数性能的影响所用的系统构架[26]是采用1位ADC对两个独立外腔半导体激光器所产生的混沌信号进行模数转换再进行XOR生成的随机数. 所得实验结果显示: 反馈强度值越大, 所获得的二元码序列能通过NIST Special Publication 800-22软件测试的项目数越多, 即随机性越好. 由于过大的反馈强度会导致外腔半导体激光器已不再处于混沌态, 所产生的二元码序列显然不会具有很好的随机性, 因此文献[26]的结论仅仅只能反映反馈强度在一个局部小范围内变化时的结果. 那么究竟反馈强度对基于外腔反馈半导体激光器产生的随机数性能有何影响? 这正是本文所要研究的内容. 考虑到目前通常采用8位ADC再选取m位LSBs的后续处理方式来提取高速随机数, 因此本文也采用该后续处理方式.

2 系统结构

基于外腔半导体激光器输出的混沌信号获取高速随机数的系统原理如图1所示. 随机数熵源为一外腔反馈半导体激光器. 分布反馈半导体激光器(DFB-SL)的输出光通过一个偏振控制器和耦合器后分成两部分, 其中一部分通过可调光衰减器、光纤反射镜后反馈回DFB-SL, 而另一部分输出经过光隔离器后将作为产生高速随机数的熵源. 可调光衰减器用于控制反馈回激光器的光的强度, 偏振控制器用来调节反馈光的偏振态, 而光隔离器可保证混沌激光的单向传输. 通过隔离器输出的激光混沌信号首先经过光电探测器转换为电信号, 再经过8位ADC将电信号采样量化后转换为8位二进制码. 从8位二进制码中提取m-LSBs得到m bit的二进制数据流, 并与利用缓冲器对该数据流进行延时后所得到的数据流进行XOR运算, 得到m bit的XOR二元码数序列. 利用NIST Special Publication 800-22测试软件对该数据流的随机性进行认证, 若能通过所有的测试, 则所得到的数据为真随机数[30].

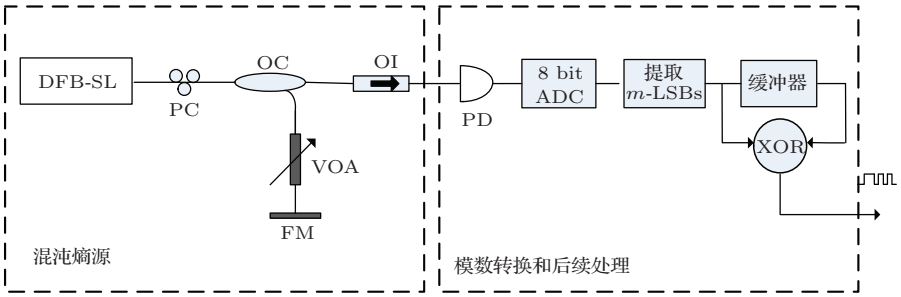

图1 基于外腔反馈半导体激光器混沌熵源产生随机数示意图. DFB-SL为分布反馈半导体激光器, PC为偏振控制器, OC为耦合器, VOA为可调光衰减器, FM为光纤反射镜, OI为光隔离器, PD为光电转换器, ADC为模数转换器, XOR为异或

Fig. 1. Schematic diagram of the generation of random number based on a semiconductor laser under external cavity feedback. DFB-SL, distributed-feedback semiconductor laser; PC, polarization controller; OC, optical coupling; VOA, variable optical attenuator; FM, fiber mirror; OI, optical isolator; PD, photodetector; ADC, analog-to-digital converter; XOR, exclusive-OR.

3 理论模型

描述DFB-SL在外部反馈作用下的动力学特性的速率方程为[31]

$$\frac{\mathrm{d}E}{\mathrm{d}t}=\frac{(1+\mathrm{i}\alpha)}{2}\left[\frac{g(N-N_0)}{1+\varepsilon|E|^2}-\frac{1}{\tau_\mathrm{p}}\right]E+\frac{\kappa_\mathrm{f}}{\tau_\mathrm{in}}E(t-\tau)\,\mathrm{e}^{-\mathrm{i}\omega\tau}+\sqrt{2\beta_\mathrm{sp}N}\xi, \tag{1}$$

$$\frac{\mathrm{d}N}{\mathrm{d}t}=PJ_{\mathrm{th}}-\frac{N}{\tau_{\mathrm{N}}}-\frac{g(N-N_0)}{1+\varepsilon|E|^2}|E|^2, \quad (2)$$

式中, E 为慢变场振幅, N 为载流子数密度, α 为线宽增强因子, g 为微分增益系数, N_0 为透明载流子密度, τ_{p} 为光子寿命, τ_{N} 为载流子寿命, τ_{in} 为光在激光腔内往返的时间, τ 为光在外腔中的往返时间, ω 为DFB-SL的中心角频率, P 为抽运因子, J_{th} 为阈值电流密度 ($J_{\mathrm{th}}=N_{\mathrm{th}}/\tau_{\mathrm{N}}$, $N_{\mathrm{th}}=N_0+1/(g\tau_{\mathrm{p}})$), κ_{f} 表征外部反馈的强度. 方程 (1) 中的最后一项为激光器的自发辐射噪声, β_{sp} 为自发辐射速率, ξ 为高斯白噪声.

分析外腔反馈半导体激光混沌系统的延时特性的方法有很多, 如自相关函数、互信息、填充因子分析法以及局部线性模型等. 本文采用自相关法进行延时特性的分析, 即通过输出混沌信号的时间序列的自相关函数谱来获取外腔反馈延时特性. 自相关函数的定义为

$$C(\Delta t)=\frac{\langle[I(t+\Delta t)-\langle I(t)\rangle][I(t)-\langle I(t)\rangle]\rangle}{\sqrt{\langle I(t+\Delta t)-\langle I(t)\rangle\rangle^2\langle I(t)-\langle I(t)\rangle\rangle^2}}, \quad (3)$$

式中, I 为激光器输出的信号的强度, Δt 为移动时间, $\langle\cdot\rangle$ 表征时间平均.

对混沌复杂度的度量, 可以使用Lyapunov指数, Kolmogorov-Sinai熵, 相关维数以及基于信息理论的排列熵 (PE) 等方法. 与其他算法相比, PE方法在计算速度和抗干扰容忍度等多方面具有优势 [32−34]. 基于此, 本文利用PE方法来分析系统混沌输出的复杂度.

4 结果与讨论

利用四阶龙格-库塔法可对方程 (1) 和 (2) 进行数值求解. 数值模拟中所用到的参数取值如下 [35]: $\alpha=5.0$, $g=8.4\times10^{-13}$ m^3·s^{-1}, $N_0=1.4\times10^{24}$ m^{-3}, $\tau_{\mathrm{p}}=1.927\times10^{-12}$ s, $\tau_{\mathrm{in}}=8.0\times10^{-12}$ s, $\tau_{\mathrm{N}}=2.04\times10^{-9}$ s, $\varepsilon=2.5\times10^{-23}$ m^3, $\beta_{\mathrm{sp}}=1\times10^3$ s^{-1}, $P=1.44$. 外腔的反馈延时时间 $\tau=40.1$ ns.

已有的研究结果表明: 外腔反馈强度是影响输出混沌信号的延时特性以及复杂度的关键参数 [36,37]. 图2给出了不同反馈强度下外腔反馈半导体激光器输出的混沌信号的时间序列 (左列)、相应的功率谱 (中列) 以及自相关函数谱 (右列). 从图2可以看出: 在所给的反馈强度下, 外腔半导体激光器输出的时间序列呈现无规则的起伏, 功率谱呈连续分布, 说明此时外腔半导体激光器输出混沌信号. 从时间序列的自相关函数上可以看到有明显的延时特征峰, 其出现在 Δt 为延时时间的整倍数的位置. 当 $\kappa_{\mathrm{f}}=0.1$ 时 (图2 (b3)), 外腔延时时间特征峰值相对较小.

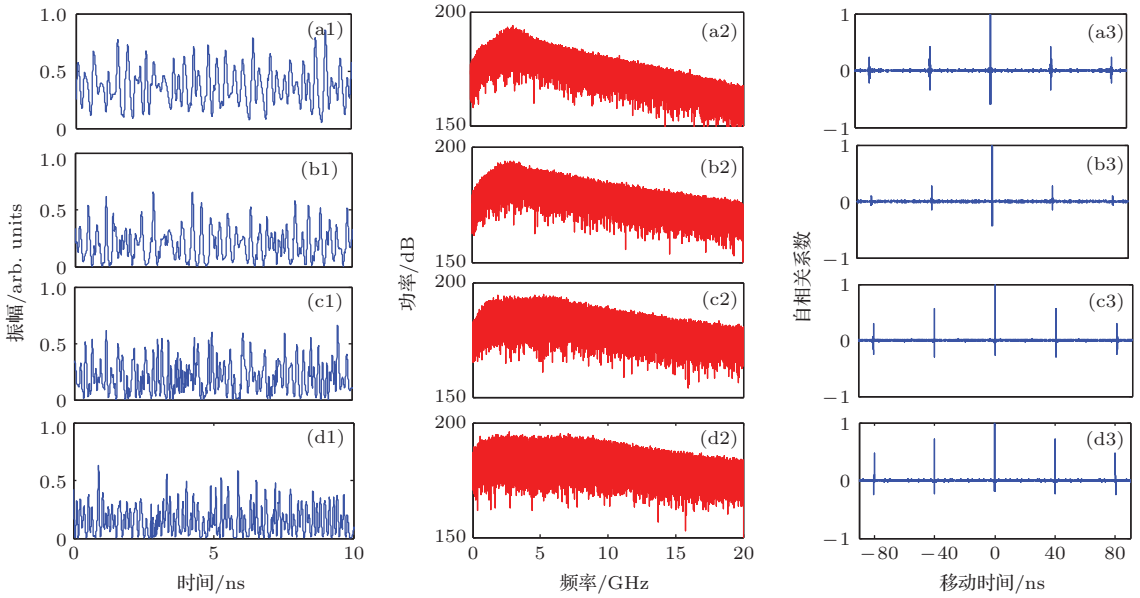

图2 (网刊彩色) 不同反馈强度 κ_{f} 下外腔半导体激光器输出的时间序列 (左列) 和对应的功率谱 (中列) 及自相关函数谱 (右列) (a) $\kappa_{\mathrm{f}}=0.05$; (b) $\kappa_{\mathrm{f}}=0.1$; (c) $\kappa_{\mathrm{f}}=0.2$; (d) $\kappa_{\mathrm{f}}=0.3$

Fig. 2. (color online) Time series (left column), associated power spectrum (middle column), and autocorrelation function (right column) under different feedback strength κ_{f}: (a) $\kappa_{\mathrm{f}}=0.05$; (b) $\kappa_{\mathrm{f}}=0.1$; (c) $\kappa_{\mathrm{f}}=0.2$; (d) $\kappa_{\mathrm{f}}=0.3$.

为了更清晰地说明外腔反馈强度对半导体激光器输出混沌信号特性的影响, 图3给出了激光器输出随反馈强度的分岔图、混沌信号的延时时间特征峰值和PE 特征值随反馈强度的变化. 由图3 (a)所示的分岔图可知: 当反馈强度从0逐渐增加到0.016, 外腔反馈半导体激光器经历稳态、单周期、倍周期、多周期后进入混沌态; 随着反馈强度的进一步增大, 激光器从混沌态进入多周期, 直至反馈强度达到0.026以上, 激光器又呈现混沌态. 由于本文的工作是基于激光器输出混沌信号这一前提, 因此在后面的讨论中我们把反馈强度设定在0.026—1范围. 在数值模拟过程中, 混沌信号延时时间的特征峰值为在外腔延时时间τ(40.1 ns)附近的[35 ns, 45 ns] 时间窗口内自相关函数的极大值; 同时PE的特征值为混沌信号的PE在嵌入延时$\tau_{\rm e}$位于外腔延时时间τ 附近时的极小值, 计算过程中嵌入维度D设为6[33,34]. 如图3 (b)所示, 随着反馈强度的增加, 混沌信号延时时间的特征峰值先逐渐减小, 在达到一个极小值后再继续增加. 这一变化趋势与文献[36]报道的结果相符, 这是外腔反馈半导体激光器中复杂的非线性动力学特性引起的. 混沌信号延时时间的特征峰值出现最小值的位置与激光器的参数以及外部反馈强度和反馈延时时间都有关系, 在本文给定的参数条件下, 当反馈系数$\kappa_{\rm f}=0.1$时混沌信号延时时间的特征峰值达到极小. 而从图3 (c)可以得知, 随着反馈强度增加, PE特征值先增大后减少, 在反馈系数$\kappa_{\rm f}=0.1$时达到PE特征值的最大值, 即系统的混沌输出复杂度呈先增大后缓慢减少的趋势.

接下来, 分析利用外腔半导体激光器输出的混沌信号经过后续处理后所产生的二进制序列的特性. 从激光器输出的混沌信号经过8位ADC转换成8 bit二进制序列, ADC的采样速率为5 GHz. 通过在8 bit二进制序列中截取最低的m位LSB可得到m bit的二进制序列, 这一m bit 的二进制序列再与其经过缓存器延时20 ns后所得到二进制序列做XOR运算, 得到m bit的XOR 二元码序列. 利用相关的测试软件对m bit的XOR二元码序列的随机性进行评估. 图4给出了基于$k_{\rm f}=0.05$时激光器输出的混沌信号保留m-LSBs所得的二元码序列的统计直方图, 其中图4 (a)—(e)分别对应m从8减小到4, 图4 (f)为截取4-LSBs后进一步做XOR处理的输出结果. 在该图中, 横坐标表示量化后的幅值, 即将信号幅值分为2^m个单元, 纵坐标则表示每个单元幅值的分布概率. 从图4 (a)可以看出, 当保留全部8位数据时, 信号幅度的分布不均匀, 不能直接用来生成随机数. 但随着所保留的LSBs m的减小, 分布的均匀性将逐渐得到改善. 考虑到实际仪器的探测窗口大小[38], 本文在量化过程中, 采样窗口对应的置信区间$CI\approx\pm3.5\sigma$ (σ为信号幅度值的标准差), 可保证波形的99.93%能够落在采样窗口中.

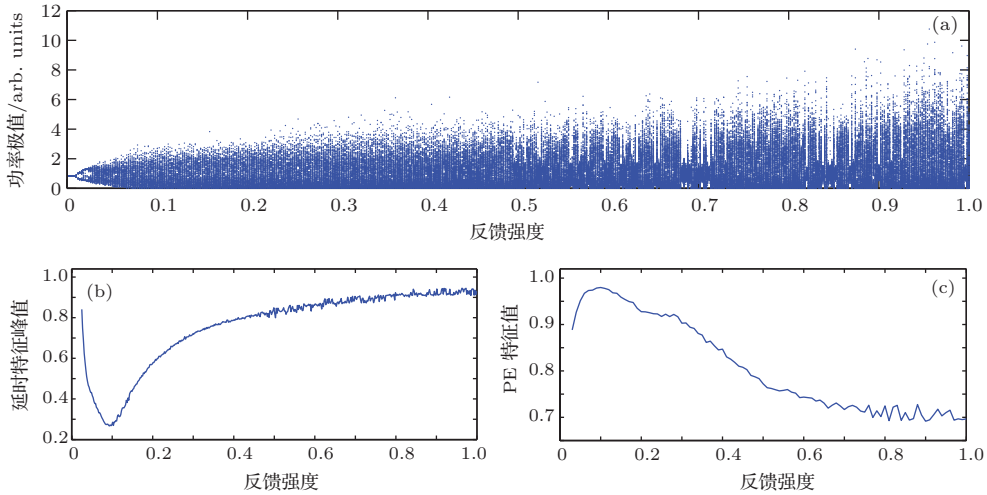

图3 (网刊彩色) (a) 激光器输出随反馈强度的分岔图; (b) 混沌信号的延时时间特征峰值随反馈强度的变化; (c) 混沌信号的PE特征值随反馈强度的变化

Fig. 3. (color online) (a) Bifurcation diagram of laser output with feedback strength. (b) Time delay characteristic peak of the chaotic signal with feedback strength. (c) PE characteristic value of the chaotic signal with feedback strength.

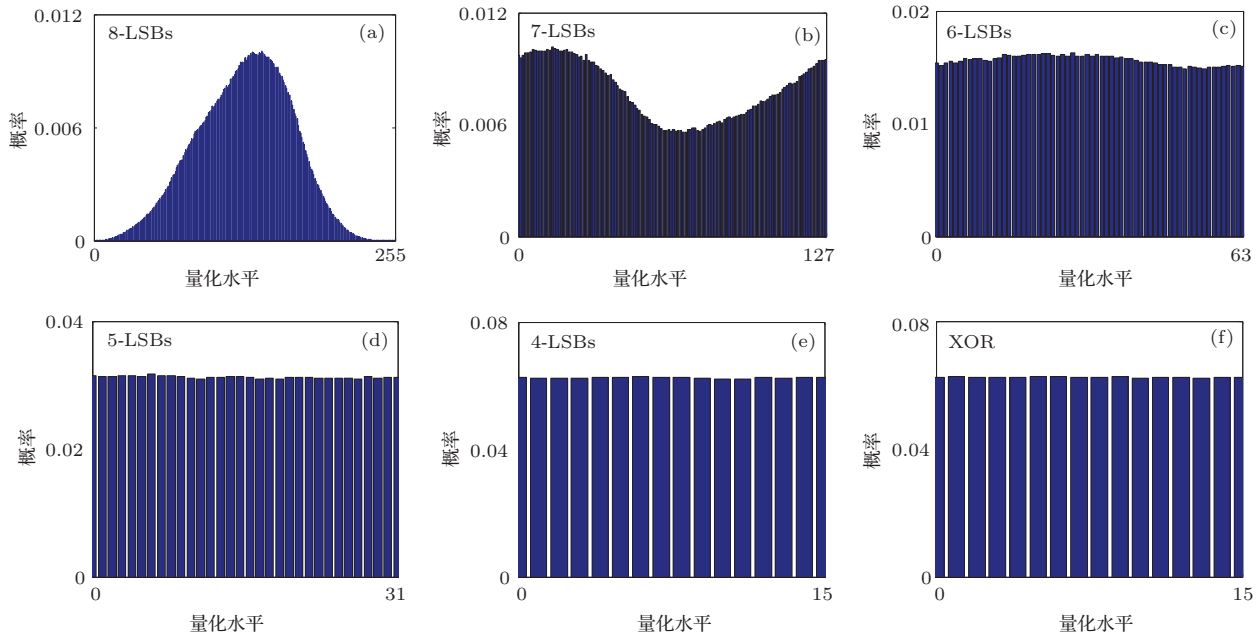

图 4 (网刊彩色) 基于 $\kappa_{\rm f}=0.05$ 时激光器输出的混沌信号保留 m-LSBs 后的统计直方图 (a)—(e) 分别对应 m 从 8 减小到 4; (f) 截取 4-LSBs 后进一步做 XOR 操作的输出结果

Fig. 4. (color online) Statistical histogram of the retained m-LSBs bit sequence obtained by chaotic signal from DFB-SL under $\kappa_{\rm f}=0.05$. m in panels (a)–(e) decreases from 8 to 4; (f) 4-LSBs are retained for a bitwise XOR operation.

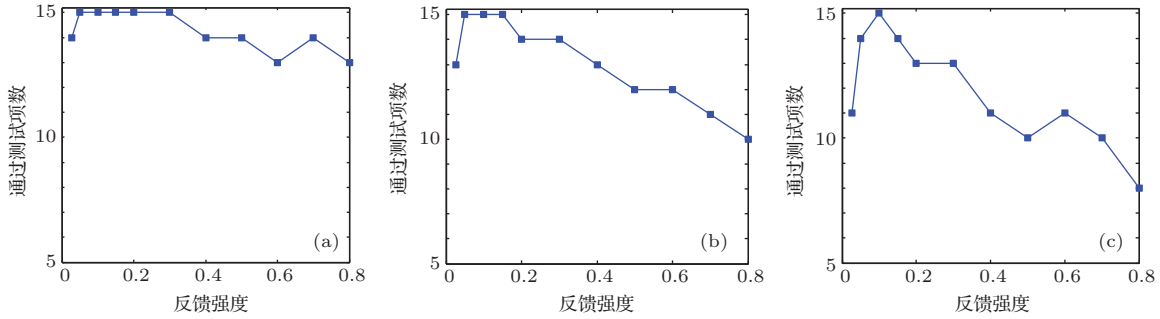

图 5 ADC 采样速率为 5 GHz 时, m bit XOR 二元码序列通过 NIST Special Publication 800-22 软件测试的项数随反馈强度的变化 (a) 3-LSBs; (b) 4-LSBs; (c) 5-LSBs

Fig. 5. Dependences of the number of passed terms of NIST Special Publication 800-22 test for m-bit XOR binary sequence on the feedback strength under ADC with a sampling rate of 5 GHz: (a) 3-LSBs; (b) 4-LSBs; (c) 5-LSBs.

进一步地, 我们采用美国国家标准技术研究所 (NIST) 提供的 NIST Special Publication 800-22 测试软件对基于不同反馈强度下激光器输出的混沌信号所获得的 m bit XOR 二元码序列进行随机性测试. NIST 提供的随机数测试标准共包含 15 项测试, 每项测试结果用 p-value 表示. 若 p-value 大于显著水平值 $\beta=0.01$, 则说明该随机数通过了相应的测试. 对于多组测试序列而言, 最终测试报告给出了每一个测试项目的 P, P 是对某一测试项的一系列 p-value 做 χ^2 拟合优度检验 (goodness-of-fit distributional test) 后得到的计算值. 当 P 值大于 10^{-4} 且对某一项目的测试通过率大于 $p-3\sqrt{\dfrac{p(1-p)}{n}}$ 时 ($p=1-\beta$, n 为测试序列的组数), 我们认为该检测项目通过, 反之则不通过. 由于我们在计算过程中选取 $n=1000$ 组数据进行测试, 因此要求每项测试的通过率需大于 0.9806 才算通过. 同时, 对于包含多项子测试的测试项, 我们以其中最小的测试值作为评判依据. 对于 ADC 的采样速率为 5 GHz 时, m bit XOR 二元码序列的随机性测试结果如图 5 所示, 图 5 (a)—(c) 分别对应 $m=3$, 4, 5. 需要说明的是, 由于反馈强度 $\kappa_{\rm f}$ 增加到 0.026 以后才能出现混沌态输出, 因此下面的讨论中反馈强度均从 0.026 开始. 如图 5 (a) 所示: 如果选择只保留后面三位有效位形成最后的 XOR

二元码序列, 当反馈强度 $0.026 < \kappa_{\rm f} < 0.03$ 时能通过 14 项测试; 当反馈强度 $0.03 < \kappa_{\rm f} < 0.3$ 时能通过全部 15 项测试, 即此时所输出的为真随机数序列; 随着反馈强度的进一步增大, 3 bit 的 XOR 二元码序列能通过的测试项数总体上出现下降的趋势. 当 $m = 4$ 时 (图 5 (b)), 反馈系数 $0.05 < \kappa_{\rm f} < 0.15$ 时所得到的 4 bit XOR 二元码序列能通过全部的 15 项测试, 其他反馈强度下仅能部分通过. 当 $m = 5$ 时, 仅当反馈系数在 0.1 附近很小的区域时所得到的二元码序列能通过所有的测试, 其速率为 ADC 采样速率取 5 GHz 所能达到的最高速率 25 GHz. 从图 3 可知, 此时外腔半导体激光器输出的混沌信号的延时时间特征峰值是最小的. 因此, 为了得到高速率的随机数序列, 有必要调制外腔反馈半导体激光器的反馈强度从而使激光器输出混沌信号的反馈延时特征峰值达到最小.

表 1 NIST 统计测试结果

Table 1. Result of NIST statistical tests.

测试名称	P	概率	结果
频数	0.399442	0.9880	通过
块内频数	0.915317	0.9940	通过
累加	0.071177	0.9880	通过
游程	0.765632	0.9920	通过
块内最长游程	0.784927	0.9880	通过
矩阵秩	0.143686	0.9900	通过
离散傅里叶变换	0.755819	0.9860	通过
非重叠模块匹配	0.024688	0.9930	通过
重叠模块匹配	0.459717	0.9840	通过
通用统计	0.695200	0.9900	通过
近似熵	0.976878	0.9840	通过
随机游动	0.057753	0.9917	通过
随机游动变量	0.035174	0.9867	通过
连续性	0.544254	0.9900	通过
线性复杂度	0.277082	0.9860	通过

由于最后所产生的随机数的速率为 ADC 采样速率的 $m_{\rm max}$ ($m_{\rm max}$ 为能通过 NIST 测试的 LSBs 的极大值) 倍, 而 $m_{\rm max}$ 随着 ADC 采样速率的增加会呈现一个总体下降的趋势, 因此对于一个确定的混沌信号熵源, 能达到的随机数序列的速率存在一个极大值. 我们选取前面已经证实能获得最好的延时特征抑制效果的混沌信号, 即反馈强度为 0.1 时的外腔半导体激光器输出的混沌信号作为熵源, 此时混沌信号的带宽为 8.73 GHz (此处带宽定义为: 从 0 频算起, 包含功率谱总能量 80% 的频率范围). 在不同的 ADC 采样速率下, 得到 m bit XOR 二元码序列, 对该二元码序列进行 NIST Special Publication 800-22 软件测试, 找到能通过所有测试项目的最大的 LSB 位数 $m_{\rm max}$, $m_{\rm max}$ 与采样速率的乘积即为系统能获得的最大随机数序列速率. 不断加大采样速率, 找到所产生的随机序列能通过 NIST Special Publication 800-22 软件的全部测试项时保留的 LSBs 的极大值 $m_{\rm max}$, 最终确定该系统在所给的参数条件下能达到的随机数序列最大速率为 4×12.5 Gbit/s. 具体的测试结果如表 1 所列, 所产生的 50 Gbit/s 的 4-LSBs XOR 二元码序列能够通过 NIST 的全部随机数测试标准, 即该系统能产生 50 Gbit/s 的随机数序列.

5 结 论

本文对基于外腔反馈半导体激光器输出的激光混沌信号作为物理熵源, 经过光电转换、ADC 采样以及 m-LSBs 和 XOR 处理后所获得的 m bit XOR 二元码序列的随机性与外腔反馈强度的依赖关系进行了理论研究. 研究结果表明: 外腔反馈半导体激光器所产生的混沌信号的延时时间特征峰值随反馈强度的增加呈现先减小、再经历一极小值后再增大的过程, 而混沌信号的 PE 特征值随反馈强度的增加先逐渐增加, 然后缓慢减小; 由不同反馈强度下外腔半导体激光器输出的混沌信号作为混沌熵源, 经过后续处理后所获得的二元码序列通过 NIST Special Publication 800-22 软件测试的项目数与反馈强度的大小紧密相关. 同时, 降低所保留的 LSB 的数目 m 将使能得到真随机数输出的反馈强度范围增大, 但相应的随机数的速率减小; 对于采样率为 5 Gbit/s 的 ADC, 此时能获取的随机数序列的最高速率为 25 Gbit/s; 在本文所给的系统参数条件下, 该系统所产生的随机数序列的最高速率可达 50 Gbit/s, 这一速率是在 ADC 的采样率设为 12.5 Gbit/s 时得到的, 此时能通过 NIST Special Publication 800-22 软件测试的最大的 LSB 位数为 4 位.

参考文献

[1] Gallager R G 2008 *Principles of Digital Communication* (New York: Cambridge University Press) pp199–244

[2] Metropolis N, Ulam S 1949 *J. Am. Stat. Assoc.* **44** 335

[3] Asmussen S, Glynn P W 2007 *Stochastic Simulation: Algorithms and Analysis* (New York: Springer-Verlag) pp30–65
[4] Stinson D R 2005 *Cryptography: Theory and Practice* (Ontario: CRC Press) pp423–452
[5] Aaldert C 1991 *J. Stat. Phys.* **63** 883
[6] Holman W T, Connelly J A, Dowlatabadi A B 1997 *IEEE Trans. Circuits Syst. Regul. Pap.* **44** 521
[7] Fairfield R C, Mortenson R L, Coulthart K B 1985 *An LSI Random Number Generator (RNG)* (Berlin: Springer-Verlag) p203
[8] Kuusela T 1993 *J. Nonlinear Sci.* **3** 445
[9] Qi B, Chi Y M, Lo H K, Qian L 2010 *Opt. Lett.* **35** 312
[10] Guo H, Liu Y, Dang A H, Wei W 2009 *Chin. Sci. Bull.* **54** 3651 (in Chinese) [郭弘, 刘钰, 党安红, 韦韦 2009 科学通报 **54** 3651]
[11] Ren M, Wu E, Liang Y, Jian Y, Wu G, Zeng H 2011 *Phys. Rev. A* **83** 023820
[12] 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]
[13] Wu J G, Wu Z M, Tang X, Lin X D, Deng T, Xia G Q, Feng G Y 2011 *IEEE Photon. Technol. Lett.* **23** 759
[14] Ren X L, Wu Z M, Fan L, Xia G Q 2014 *Chin. Sci. Bull.* **59** 259 (in Chinese) [任小丽, 吴正茂, 樊利, 夏光琼 2014 科学通报 **59** 259]
[15] Xiang S Y, Pan W, Luo B, Yan L S, Zou X H, Li N Q, Zhang L Y 2012 *Opt. Commun.* **285** 5293
[16] Yan S L 2010 *Opt. Commun.* **283** 3305
[17] Zhang M J, Liu T G, Li P, Wang A B, Zhang J Z, Wang Y C 2011 *IEEE Photon. Technol. Lett.* **23** 1872
[18] Zhong D Z, Wu Z M 2009 *Opt. Commun.* **282** 1631
[19] Xie Y Y, Wu Z M, Deng T, Tang X, Fan L, Xia G Q 2013 *IEEE Photon. Technol. Lett.* **25** 1605
[20] Argyris A, Hamacher M, Chlouverakis K E, Bogris A, Syvridis D 2008 *Phys. Rev. Lett.* **100** 194101
[21] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashige T, Shiki M, Yoshimiri S, Davis P 2008 *Nat. Photon.* **2** 728
[22] Reidler I, Aviad Y, Rosenbluh M, Kanter I 2009 *Phys. Rev. Lett.* **103** 024102
[23] Kanter I, Aviad Y, Reidler I, Cohen E, Rosenbluh M 2010 *Nat. Photon.* **4** 58
[24] Li P, Wang Y C, Zhang J Z 2010 *Opt. Express* **18** 20360
[25] Wu J G, Tang X, Wu Z M, Xia G Q, Feng G Y 2012 *Laser Phys.* **22** 1476
[26] Hirano K, Amano K, Uchida A, Naito S, Inoue M, Yoshimiri S, Yoshinura K, Davis P 2009 *IEEE J. Quantum Electron.* **45** 1367
[27] Zhang J B, Zhang J Z, Yang Y B, Liang J S, Wang Y C 2010 *Acta Phys. Sin.* **59** 7679 (in Chinese) [张继兵, 张建忠, 杨毅彪, 梁君生, 王云才 2010 物理学报 **59** 7679]
[28] Xiao B J, Hou J Y, Zhang J Z, Xue L G, Wang Y C 2012 *Acta Phys. Sin.* **61** 150502 (in Chinese) [萧宝瑾, 侯佳音, 张建忠, 薛路刚, 王云才 2012 物理学报 **61** 150502]
[29] Zhang J Z, Wang Y C, Xue L G, Hou J Y, Zhang B B, Wang A B, Zhang M J 2012 *Appl. Opt.* **51** 1709
[30] Rukhin A, Rukhin J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M 2008 *NIST Special Publication 800-22* (rev. 1) (Gaithersburg: National Institute of Standards and Technology)
[31] Lang R, Kobayashi K 1980 *IEEE J. Quantum Electron.* **16** 347
[32] Bandt C, Pompe B 2002 *Phys. Rev. Lett.* **88** 174102
[33] Zunino L, Rosso O A, Soriano M C 2011 *IEEE J. Sel. Top. Quantum Electron.* **17** 1250
[34] Soriano M C, Zunino L, Rosso O A 2011 *IEEE J. Lightwave Technol.* **29** 2173
[35] Mikami T, Kanno K, Aoyama K, Uchida A, Ikeguchi T, Harayama T, Sunada S, Arai K, Yoshimura K, Davis P 2012 *Phys. Rev. Lett.* **85** 016211
[36] Rontani D, Locquet A, Sciamanna M, Citrin D S 2007 *Opt. Lett.* **32** 2960
[37] Wu J G, Xia G Q, Tang X, Lin X D, Deng T, Fan L, Wu Z M 2010 *Opt. Express* **18** 6661
[38] Argyris A, Pikasis E, Deligiannidis S, Syvridis D 2012 *J. Lightwave Technol.* **30** 1329

Influence of feedback strength on the characteristics of the random number sequence extracted from an external-cavity feedback semiconductor laser*

Yang Hai-Bo Wu Zheng-Mao Tang Xi Wu Jia-Gui Xia Guang-Qiong†

(*School of Physical Science and Technology, Southwest University, Chongqing 400715, China*)

(Received 15 July 2014; revised manuscript received 25 October 2014)

Abstract

Under proper feedback strength, an external-cavity feedback semiconductor laser can operate at a chaos state, and its chaotic output can be used as a physical entropy source to generate a physical random number sequence. In this paper, we focus on the influence of feedback strength on the randomness of the obtained binary code sequence. The simulation results show that with the increase of feedback strength, the time delay characteristic peak of the chaotic signal from an external-cavity feedback semiconductor laser first decreases and then increases gradually, meanwhile, the permutation entropy characteristic value of chaotic signal first increases and then decreases gradually, namely, there exists an optimized feedback strength for obtaining the chaotic signal with the weakest time delay signature and high complexity. The randomness of binary code sequences, generated by the chaotic signal from the external-cavity feedback semiconductor laser under different feedback strengths, is tested by NIST Special Publication 800-22, and the influence of feedback strength on the test results is also discussed.

Keywords: external-cavity feedback semiconductor laser, feedback strength, chaos, random number

PACS: 42.55.Px, 05.45.–a, 05.45.Gg, 05.40.–a **DOI:** 10.7498/aps.64.084204

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61178011, 61275116, 61475127, 11474233), the Natural Science Foundation of Chongqing City, China (Grant No. 2012jjB40011), and the Fundamental Research Funds for the Central Universities, China (Grant No. XDJK2014C079).

† Corresponding author. E-mail: gqxia@swu.edu.cn