混沌半导体激光器的弛豫振荡频率对随机序列速率的影响*

萧宝瑾[1)] 侯佳音[1)] 张建忠[2)] 薛路刚[2)] 王云才[2)3)†]

1) (太原理工大学信息工程学院, 太原 030024)

2) (太原理工大学物理与光电工程学院, 太原 030024)

3) (太原理工大学新型传感器与智能控制教育部重点实验室, 太原 030024)

(2011 年 11 月 8 日收到; 2012 年 1 月 6 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发生器的物理熵源, 分析了混沌信号自相关系数与随机序列游程数之间的联系, 在此基础上研究了激光器的弛豫振荡频率 f_{r} 与随机序列速率 f_n 在不同比值时, 序列游程数的变化情况. 研究发现, 当 $f_{\mathrm{r}}/f_n = (2k+1)/4$ 时, 随机序列的游程数容易满足 NIST SP800-22 随机数测试标准的要求. 当 $k = 1$ 时, 得到随机序列最大速率为 $f_n = 4f_{\mathrm{r}}/3$.

关键词: 混沌激光, 随机数发生器, 弛豫振荡频率, 随机序列游程

PACS: 05.40.Fb, 05.45.Gg

1 引 言

随机数在蒙特卡罗仿真、随机建模、安全通信、数字签名和身份认证等方面有着广泛的应用, 例如 GPS 系统中的 M 序列 [1] 和密码学中的密钥 [2], 都与随机数有着密切的关系, 因而需要对随机数的生成方法进行研究.

根据随机数产生的机理, 将随机数发生器 (random number generator, RNG) 分为基于算法的伪随机数发生器和基于物理过程的真随机数发生器. 随着计算机和网络技术的发展, 伪随机数由于具有周期性, 在安全性方面存在着隐患. 真随机数是从物理熵源中获得的, 具有不可预测性, 因而有较高的安全性. 通常电路噪声 [3]、电子振荡器的频率抖动 [4]、激光器的相位噪声 [5] 等都可以作为熵源. 但由于受到硬件带宽的限制, 所产生的随机数速率通常只有几十 Mbps.

研究表明半导体激光器在光反馈、光注入或光电反馈的扰动下, 可产生数 GHz 带宽的混沌激光信号 [6–8]. 另外, 由于混沌激光信号的自相关函数近似于 δ 函数, 与高斯白噪声相近, 因此具备了作为 RNG 熵源的条件. 2007 年, 我们提出用混沌激光作为物理熵源构造高速 RNG 的专利方案 [9], 随后完成了随机数的提取及混沌激光熵源的外腔长特性分析 [10–12]. 2008 年, Uchida 研究小组利用两个 1 位模数转换器 (ADC) 分别从两路独立的混沌激光信号中提取出两个随机序列, 再将它们异或, 通过实验获得了速率为 1.7 Gbps 的随机序列 [13]. 2009 年, Kanter 研究小组使用 8 位 ADC 从单路的混沌熵源中提取随机序列, 经过差分和并串转换等离线的后续处理, 相继得到 12.5 Gbps 和 300 Gbps 的随机序列 [14,15]. 2010 年, Uchida 研究小组对于带宽增强的混沌激光信号采用 8 位 AD 转换, 并通过软件进行延迟异或和并串转换获得了 75 Gbps 的

* 国家自然科学基金专项基金 (批准号: 60927007), 国家自然科学基金 (批准号: 60872019, 61001114), 山西省自然科学基金 (批准号: 2010021003-4) 和山西省高等学校中青年拔尖创新人才支持计划资助的课题.

† E-mail: wangyc@tyut.edu.cn

随机序列 [16]. 同年, 本课题组采用数值模拟方法实现了全光随机数发生器 [17]. 近来, 为了提高 RNG 的稳定性, Uchida 研究小组采用光子集成半导体混沌激光器作为物理熵源以产生高速随机数 [18]. 目前, 大部分相关文献都是研究基于混沌激光实现高速随机数的产生, 而关于混沌激光熵源特性对随机序列随机特性的影响研究得不多. 2009 年 Uchida 研究小组利用外腔半导体激光器作为混沌激光源, 分析了外腔长、注入电流和反馈强度等外部参数对随机序列测试结果的影响 [19], 但没有深入研究激光器内在的弛豫振荡频率对随机序列特性的影响.

本文利用单路混沌激光源作为 RNG 的物理熵源, 分析了混沌信号自相关系数与随机序列游程数的联系. 在此基础上, 讨论了半导体激光器弛豫振荡频率对随机序列速率的影响, 并给出了获得高质量、高速率随机序列的理论依据.

2 装置与原理

利用混沌激光产生随机数的 RNG 原理如图 1 所示. 半导体激光器 (LDM5S752) 输出的光通过 50:50 的耦合器后, 50%的光由光纤反射镜反馈回半导体激光器, 另一部分光作为输出. 其中利用偏振控制器和可调光衰减器分别控制偏振状态和反馈光强度. 光隔离器可保证混沌激光的单向传输. 光电探测器 (Thorlabs PDA8GS) 将输出的光信号转换为电信号, 并去除直流分量, 然后送到 1 位模数转换器与稳压源输出的参考电压 V_{ref} 进行比较, 产生二进制随机序列, 该序列的速率取决于时钟频率. 为了改善随机序列的随机特性, 一般需要对它进行后续处理. 本文主要研究混沌半导体激光器弛豫振荡频率对随机序列特性的影响, 为了凸显它们之间的相互关系, 因此没有进行后续处理.

图 2 给出了利用混沌信号产生二进制随机序列的过程. 在实验中, 利用 LeCroy 820Zi-A 型示波器对混沌信号进行采集, 得到一个采样速率为 $f_1 = 40$ GHz 的离散混沌序列

$$X_1 = \{x_0, x_1, \cdots, x_i, \cdots, x_{L-1}\},$$

用图 2(a) 中的小黑点表示. 并把该序列存入 PC 机中, 以便进行软件处理.

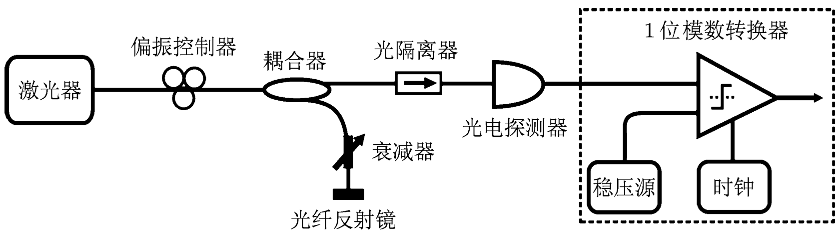

图 1 基于混沌激光源的 RNG 原理框图

首先对长度为 L 的混沌序列 X_1 每隔 n 个点采一个样, 得到一个长度为 M 的子序列

$$\begin{aligned} X_n &= \{x_0, x_n, x_{2n}, \cdots, x_{in}, \cdots, x_{(M-1)n}\} \\ &= \{y_0, y_1, y_2, \cdots, y_i, \cdots, y_{M-1}\}, \end{aligned}$$

其中, $M = [1 + (L-1)/n]$ 的整数部分. 此时随机序列的速率为 $f_n = f_1/n$, 采样间隔为 $t_n = 1/f_n$. 当 $n = 10$ 时, 所提取的子序列 X_{10} 用图 2(a) 中的小圆圈表示. 再将 X_n 二值化: 当 $y_i > V_{\mathrm{ref}}$ 时, $z_i = 1$; 当 $y_i \leqslant V_{\mathrm{ref}}$ 时, $z_i = -1$. 得到二进制随机序列

$$Z_n = \{z_0, z_1, z_2, \cdots, z_i \cdots, z_{M-1}\}.$$

图 2(b) 是相应的二进制随机序列 Z_{10} 的波形.

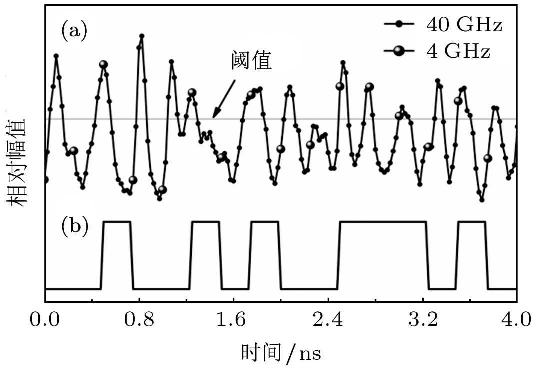

图 2 二进制随机序列的产生过程 (a) 混沌时序图; (b) 二进制随机序列图

3 混沌序列自相关系数与随机序列游程数的关系

3.1 混沌序列自相关系数与弛豫振荡频率的关系

图 3 为混沌激光源在外腔长为 16 m, 注入电流 $I = 30$ mA, 反馈强度为 20%时, 利用 Agilent E4407B 型频谱仪获得的混沌信号频谱图. 频谱峰值所对应的频率为弛豫振荡频率 $f_{\mathrm{r}} = 3.63$ GHz, 相应的弛豫振荡周期为 $t_{\mathrm{r}} = 1/f_{\mathrm{r}} = 0.275$ ns. 图 4 为该混沌序列 X_1 的归一化自相关函数, 即自相关系数 $R_{X_1}(\tau)$, 当 $|\tau| \leqslant 1.5$ ns 时, 它是一个幅度逐渐衰减的周期性函数, 周期与弛豫振荡周期相等.

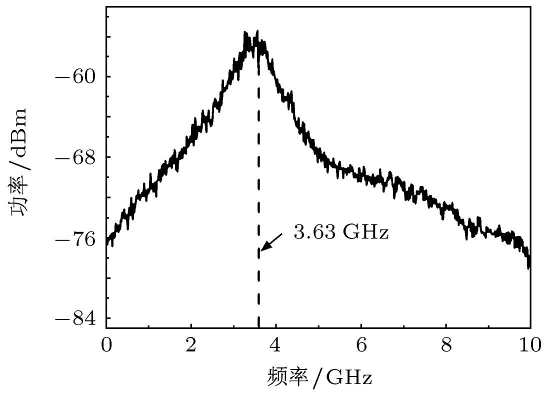

图 3 混沌激光信号频谱图

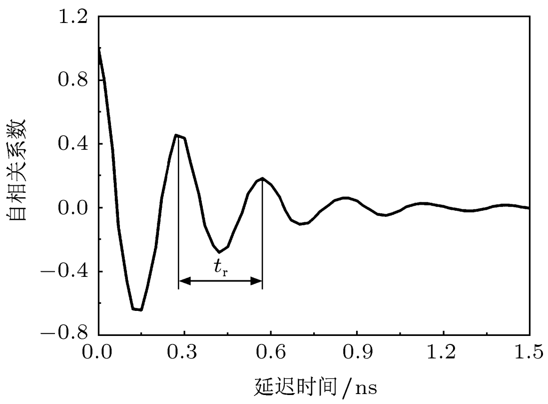

图 4 混沌激光信号自相关图

3.2 X_1 的自相关系数与 Z_n 的自相关系数的关系

将 X_1 的子序列 X_n 量化后得到 Z_n, 它们的自相关系数 $R_{X_1}(l)$, $R_{X_n}(m)$, $R_{Z_n}(m)$ 之间有着密切的联系. 在实验中序列 X_1 的长度 $L = n \times 10^6$, 为便于分析可把混沌序列视为无限长的平稳随机序列, 即令 $L \to \infty$, 且与时间起点无关. 因此可设 $X_1' = \{\cdots, x_{-2}, x_{-1}, x_0, x_1, x_2, \cdots\}$, 它的自相关系数为

$$R_{X_1'}(l) = \sum_{i=-\infty}^{\infty} x_i x_{i+l} \Big/ \sum_{i=-\infty}^{\infty} x_i^2,$$

式中, l 表示时间间隔为 $\tau = lt_1$.

再设序列 $X_n' = \{\cdots, x_{-2n}, x_{-n}, x_0, x_n, x_{2n}, \cdots,\} = \{\cdots, y_{-2}, y_{-1}, y_0, y_1, y_2, \cdots\}$, 它的自相关系数为

$$R_{X_n'}(m) = \sum_{k=-\infty}^{\infty} y_k y_{k+m} / \sum_{k=-\infty}^{\infty} y_k^2,$$

式中, m 表示时间间隔为 $\tau = mt_n$.

当 $l = n$ 时, 并利用 X_1 的平稳性, 可得

$$\begin{aligned} R_{X_1'}(n) &= \frac{\sum\limits_{i=-\infty}^{\infty} x_i x_{i+n}}{\sum\limits_{i=-\infty}^{\infty} x_i^2} = \frac{\sum\limits_{k=-\infty}^{\infty} \sum\limits_{j=0}^{n-1} x_{kn+j} x_{kn+n+j}}{\sum\limits_{k=-\infty}^{\infty} \sum\limits_{j=0}^{n-1} x_{kn+j}^2} \\ &= \frac{n \sum\limits_{k=-\infty}^{\infty} x_{kn} x_{kn+n}}{n \sum\limits_{k=-\infty}^{\infty} x_{kn}^2} = \frac{\sum\limits_{k=-\infty}^{\infty} y_k y_{k+1}}{\sum\limits_{k=-\infty}^{\infty} y_k^2} \\ &= R_{X_n'}(1). \end{aligned}$$

将 X_n' 量化后得到取值为 “+1” 和 “−1” 的二进制序列 $Z_n' = \{\cdots, z_{-2}, z_{-1}, z_0, z_1, z_2, \cdots\}$, 它的自相关系数为

$$R_{Z_n'}(m) = \sum_{k=-\infty}^{\infty} z_k z_{k+m} / \sum_{k=-\infty}^{\infty} z_k^2.$$

由于量化误差, 使得 $R_{X_n'}(1) \approx R_{Z_n'}(1)$, 从而得到 $R_{X_1'}(n) \approx R_{Z_n'}(1)$. 有限长的序列 X_1 可视为 X_1' 的一个样本空间, X_1' 的数字特征会近似地反映在 X_1 中, 故有

$$R_{X_1}(n) \approx R_{Z_n}(1). \tag{1}$$

图 5 给出了混沌序列和不同采样速率下随机序列的自相关系数, 其中用黑点表示混沌序列 X_1 的自相关系数 $R_{X_1}(l)$. 图 5(a), (b), (c), (d) 分别给出了 $n = 5, 11, 17, 20$ 时 Z_n 的自相关系数 $R_{Z_n}(m)$, 所对应的采样速率分别为 $f_n = 8, 3.66, 2.35, 2$ GHz. 图中用圆圈表示 $R_{Z_n}(1)$ 的值, 可以发现实验结果与理论推导是相符合的.

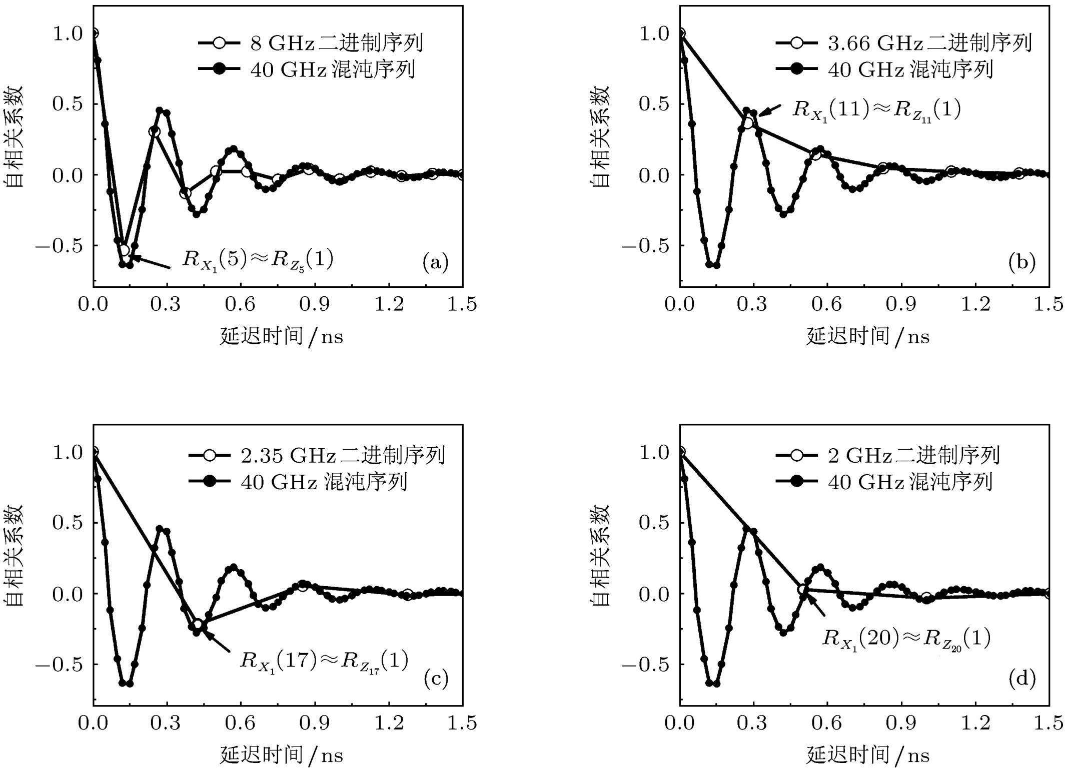

图 5 混沌序列及不同采样速率时二进制序列的自相关图 (a) $f_5 = 8$ GHz; (b) $f_{11} = 3.66$ GHz; (c) $f_{17} = 2.35$ GHz; (d) $f_{20} = 2$ GHz

3.3 Z_n 的自相关系数与游程数的关系

对于长度为 M 的序列 Z_n, 定义它的自相关系数为

$$R_{Z_n}(m) = \frac{1}{M-m}\sum_{i=0}^{M-m-1} z_i \cdot z_{i+m}. \tag{2}$$

定义它的游程数 V_n 为

$$V_n = 1 + \sum_{i=0}^{M-2} u(i),$$

其中 $u(i)$ 表示是否有跳变. 当 $z_i = z_{i+1}$ 时, 无跳变, $u(i) = 0$; 当 $z_i \neq z_{i+1}$ 时, 有跳变, $u(i) = 1$.

当 (2) 式中 $m = 1$ 时, 可得

$$\begin{aligned} R_{Z_n}(1) =& \frac{1}{M-1}\sum_{i=0}^{M-2} z_i \cdot z_{i+1} \\ =& \frac{1}{M-1}\sum_{i=0}^{M-2}[1-2u(i)] \\ =& \frac{1}{M-1}\left[M-1-2\sum_{i=0}^{M-2}u(i)\right] \\ =& [M-1-2(V_n-1)]/(M-1) \\ =& (M+1-2V_n)/(M-1). \end{aligned} \tag{3}$$

根据 NIST SP800-22 随机数测试标准 [20], 推荐序列长度为 $M = 1$ Mbit, 理想的游程数为 $V_n = M/2 = 5\times10^5$, 所允许的偏差 $|V_n - M/2| \leqslant 1288$. 代入 (3) 式, 可得

$$|R_{Z_n}(1)| \leqslant 0.002576.$$

3.4 X_1 的自相关系数与 Z_n 的游程数的关系

由 (1) 和 (3) 式得到 X_1 的自相关系数与 Z_n 的游程数的关系

$$R_{X_1}(n) \approx (M+1-2V_n)/(M-1).$$

当 $M \gg 1$ 时,

$$R_{X_1}(n) \approx (M-2V_n)/M.$$

可见混沌序列 X_1 的自相关系数 $R_{X_1}(n)$ 与随机序列 Z_n 的游程数 V_n 有关, 当 $V_n \to M/2$ 时, $R_{X_1}(n) \to 0$. 而 $R_{X_1}(n)$ 的周期等于弛豫振荡周

期, 因此随机序列的游程数必然会受到弛豫振荡频率的影响.

4 弛豫振荡频率对随机序列速率的影响

图 6 为激光器在不同注入电流 I 时混沌信号的频谱. 当注入电流 I 为 26 mA, 28 mA 和 30 mA 时, 所对应的弛豫振荡频率 f_{r} 分别为 2.35 GHz, 3.07 GHz 和 3.63 GHz. 图 7 给出了在上述 3 种不同注入电流下, 随机序列的游程数 V_n 随 f_{r}/f_n 变化的情况. 当 $f_{\mathrm{r}}/f_n = 0.75, 1.25, 1.75, 2.25$ 时, V_n 很接近 $M/2$, 满足 NIST 随机数测试标准的要求 $|V_n - M/2| \leqslant 1288$; 当 $f_{\mathrm{r}}/f_n = 0.5, 1, 1.5, 2$ 时, V_n 远离 $M/2$, 不能满足测试标准.

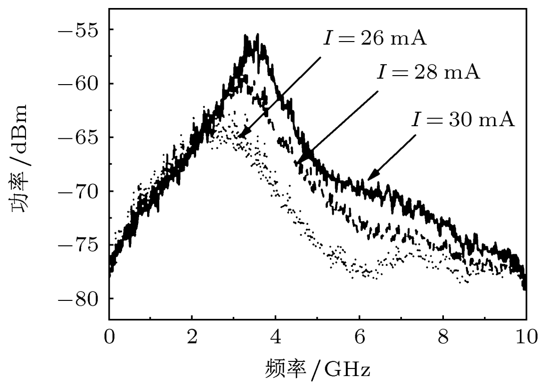

图 6　不同注入电流时混沌信号的频谱

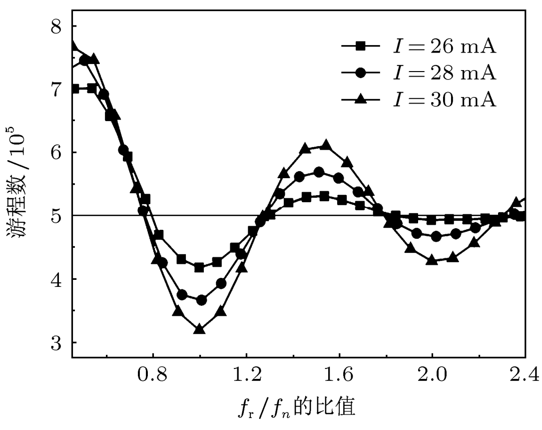

图 7　不同 f_{r}/f_n 时随机序列的游程数

弛豫振荡频率是由谐振腔内光子密度的变化快慢决定的. 光子密度的变化量 $\Delta S(t)$ 为 $\Delta S(t) \propto \exp(\mathrm{j}\omega_{\mathrm{r}}t - t/T_{\mathrm{d}}) = \lambda(t)\exp(\mathrm{j}\omega_{\mathrm{r}}t)$. 式中, ω_{r} 是弛豫振荡角频率, $\lambda(t) = \exp(-t/T_{\mathrm{d}})$ 为衰减因子 [21]. 光子密度的变化最终体现到半导体激光器输出的混沌激光信号中, 正如前面图 4 所示. 经过计算得到混沌信号的自相关系数为 $R(\tau) = \gamma(\tau)\cos(\omega_{\mathrm{r}}\tau)$, τ 为延迟时间. 当 $\omega_{\mathrm{r}}\tau = (k+1/2)\pi$ 时, $R(\tau) = 0$; 当 $\omega_{\mathrm{r}}\tau = k\pi$ 时, $R(\tau) = \gamma(\tau)$, 取得极值. 取 $\tau = 1/f_n$, 可得到

$$R(\tau) = \begin{cases} 0, & f_{\mathrm{r}}/f_n = (2k+1)/4, \\ \gamma(\tau), & f_{\mathrm{r}}/f_n = k/2, \end{cases}$$

其中, k 为非负整数.

当随机序列的采样速率为 $f_n = 4f_{\mathrm{r}}/(2k+1)$ 时, 混沌信号自相关系数为 0, 此时游程数 V_n 满足 $|V_n - M/2| \leqslant 1288$; 当 $f_n = 2f_{\mathrm{r}}/k$ 时, 混沌信号自相关系数取得极值, 此时游程数偏离理想值的程度较大. 图 7 中 V_n 随 f_{r}/f_n 变化的现象证实了这一结论. 对于 $f_n = 4f_{\mathrm{r}}/(2k+1)$ 的情况, 当 $k = 0$ 时, $f_n = 4f_{\mathrm{r}}$, 由图 6 可知, 此时混沌信号的能量已经很小, 难以保证随机序列的质量, 因此舍去该情况; 当 $k = 1, 2, 3, \cdots$ 时, 随着 k 的增大, 采样速率 f_n 不断降低. 所以在满足随机序列游程数 $|V_n - M/2| \leqslant 1288$ 的条件下, 取 $k = 1$ 时, 可获得随机序列的最大采样速率 $f_n = 4f_{\mathrm{r}}/3$.

5 结 论

本文利用光反馈半导体激光器输出的混沌激光信号作为随机数发生器的物理熵源, 分析了半导体激光器弛豫振荡频率 f_{r} 对随机序列速率 f_n 的影响. 推导出了混沌序列的自相关系数 $R_{X_1}(n)$ 与随机序列游程数 V_n 的关系式 $R_{X_1}(n) \approx (M - 2V_n)/M$. 在此基础上, 进一步讨论了 f_{r}/f_n 取不同值时, 随机序列游程数的变化情况. 当 $f_n = 4f_{\mathrm{r}}/(2k+1)$ 时, 序列游程数容易满足 NIST 随机数游程测试的要求. 最后给出了随机序列的最大采样速率为 $f_n = 4f_{\mathrm{r}}/3$. 这为利用混沌半导体激光器产生高质量、高速率的随机数提供了理论依据.

[1] Lei X J, Liu G B 2010 *Study On Optical Communications* **162** 64 (in Chinese) [雷雄俊, 刘光斌 2010 光通信研究 **162** 64]

[2] Su G P 2002 *Ph. D. Dissertation* (Beijing: Graduate University of Chinese Academy of Sciences) (in Chinese) [苏桂平 2002 博士学位论文 (北京: 中国科学院研究生院)]

[3] Xin Q, Zeng X Y, Zhang G Q, Guo Y W 2004 *Microelectronics & Computer* **21** 143 (in Chinese) [辛茜, 曾晓洋, 张国权, 郭亚炜 2004 微电子学与计算机 **21** 143]

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

[5] Qi B, Chi Y M, Lo H K, Qian L 2010 *Opt. Lett*. **35** 312

[6] Wang A B, Wang Y C, Wang J F 2009 *Opt. Lett.* **34** 1144

[7] 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, 张耕玮, 王安帮, 王冰洁, 李艳丽, 郭萍 2007 物理学报 **56** 372]

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

[9] Wang Y C, Tang J H, Zhang M J *Chinese Patent* ZL 200710062140.1 2007 (in Chinese) [王云才, 汤君华, 张明江 中国发明专利 ZL200710062140.1 2007]

[10] Zhang Y Y, Zhang J Z, Zhang M J, Wang Y C 2011 *Chinese Optics Letters* **9** 031404

[11] Chen S S, Zhang J Z, Yang L Z, Liang J S, Wang Y C 2011 *Acta Phys. Sin*. **60** 010501 (in Chinese) [陈莎莎, 张建忠, 杨玲珍, 梁君生, 王云才 2011 物理学报 **59** 010501]

[12] 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]

[13] Uchida A, Amano K, Inoue M, Hirano K, Natio S, Someya H, Owada I, Kurashige T, Shiki M, Yoshimori S, Yoshimura K, Davis P 2008 *Nat. Photon.* **2** 728

[14] Reidler I, Avaid Y, Rosenbuuh M, Kanter I 2009 *Phys. Rev. Lett*. **103** 024102

[15] Kanter I, Aviad Y, Reidler I, Cohen E, Resenbluh M 2010 *Nat. Photon.* **4** 58

[16] Hirano K, Yamazaki T, Morikatsu S, Okumura H, Aida H, Uchida A, Yoshimori S, Yoshimura K, Harayama T, Davis P 2010 *Opt. Express* **18** 5512

[17] Li P, Wang Y C, Zhang J Z 2010 *Opt. Express* **18** 20360

[18] Harayama T, Sunada S, Yoshimura K, Davis P, Tsuzuki K, Uchida A 2011 *Phys. Rev*. A **83** 031803

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

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

[21] Jiang J P 2000 *Semiconductor Laser* 1 (Beijing : Publishing House of Electronics Industry) p112—114 (in Chinese) [江剑平 2000 半导体激光器 第一版 (北京: 电子工业出版社) 第 112—114 页]

The effect of the relaxation oscillation frequency of chaotic semiconductor laser on the rate of random sequence*

Xiao Bao-Jin[1)] Hou Jia-Yin[1)] Zhang Jian-Zhong[2)] Xue Lu-Gang[2)]
Wang Yun-Cai[2)3)†]

1) (*College of Information Engineering, Taiyuan University of Technology, Taiyuan* 030024, *China*)

2) (*College of Physics and Optoelectronics Engineering, Taiyuan University of Technology, Taiyuan* 030024, *China*)

3) (*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Education, Taiyuan* 030024, *China*)

(Received 18 November 2011; revised manuscript received 6 January 2012)

Abstract

In this paper, chaotic light generated by semiconductor laser with optical feedback is employed as physical entropy source to generate high-speed random sequence. The relationship between autocorrelation coefficient of chaotic signal and run number of random sequence is analyzed. Based on the analysis, the changes of random sequence run number are further investigated at different ratios between laser relaxation oscillation frequency f_{r} and random sequence generation rate f_n. The results show that random sequence run can easily meet the requirement for run test of NIST SP800-22 when the ratio between f_{r} and f_n satisfies the equation of $f_{\mathrm{r}}/f_n = (2k+1)/4$. When k in the equation is equal to 1, the maximal rate $f_n = 4f_{\mathrm{r}}/3$ of random sequence is obtained.

Keywords: chaos light, random number generator, relaxation oscillation frequency, random sequence's runs

PACS: 05.40.Fb, 05.45.Gg

* Project supported by the Special Funds of the National Natural Science Foundation of China (Grant No. 60927007), the National Natural Science Foundation of China (Grant Nos. 60872019, 61001114), the Natural Science Foundation of Shanxi Province(Grant No. 2010021003-4), and the Top Young and Middle-aged Innovative Talents of Higher Learning Institutions of Shanxi.

† E-mail: wangyc@tyut.edu.cn