基于互注入半导体激光器的混沌输出产生 17.5 Gbit/s 随机码*

唐 曦 吴加贵 夏光琼 吴正茂†

(西南大学物理学院,重庆 400715)

(2011 年 1 月 19 日收到;2011 年 2 月 17 日收到修改稿)

采用两个借助光纤连接的相互注入半导体激光器,实验获取了 10 GHz 超宽带混沌种子信号. 通过 8-bit 模数转换器将混沌信号转换为二进制数据流,并进行进一步的逻辑异或处理和舍弃最高有效位操作,最终获得了能顺利通过美国国家标准与技术研究院(National Institute of Standard and Technology,简记为 NIST)800-22 标准测试以及 Diehard 测试,速率达 17.5 Gbit/s 的高速随机码.

关键词: 随机码, 混沌激光, 互注入半导体激光器

PACS: 05.45.Gg, 05.40.-a, 42.55.Px

1. 引 言

当前,随机码已被广泛地应用到人们生产生活以及科学研究的各个领域. 特别在以密码学为核心的信息安全领域中,随机码的质量决定密匙的安全性从而决定了数据加密的安全性. 此外,用于保证数据传输安全性、完整性的安全协议和数字签名[1,2]等手段都需要采用随机码,在核医学、金融、计算化学和材料科学[3]等许多领域中所用到的数值计算、蒙特卡罗建模等也都需要用到随机码.

根据产生随机码的方法可把随机码划分为两大类:伪随机码和真随机码. 伪随机码是采用确定性的数学算法生成的. 当两个伪随机码发生器采用相同的初始条件时,其生成的随机码是完全一致的. 随着量子计算、云计算等技术的发展,伪随机码生成的密钥有可能被拥有足够运算能力的攻击者破解,从而难以满足人们对信息安全的需求. 而真随机码是基于物理过程产生的. 真随机码发生器选取真实物理世界的随机现象如光子噪声、电阻器件中的热噪声、振荡器中的频率抖动等[4—8]作为随机码熵源. 由于这类熵源本质上是一不确定性的物理过程,因而能够生成具有很好随机统计特性、不可预测和不可再现的真随机码.

近年来,真随机码发生器的研究进展迅速. 其中一大热点是量子随机码发生器. 量子随机码发生器中比特位的布尔选择由探测的信息如光量子的到达时间、空间位置或偏振态等[7,9,10]决定,因此能够生成可靠的真随机码. 但由于受目前光子探测器的探测效率以及激光线宽等的限制,其典型的码率只有 20 Mbit/s 左右. 而基于其他的物理过程如电阻元件或二极管等器件的热噪声信号放大后,通过选择恰当探测阈值并对信号做后续处理,最终也能产生真随机码. 但这些方法产生随机码的速率仍然较低,因而迫切需要开发高速率的真随机码发生器. 最近,基于混沌输出的一些真随机码发生器方案由于能产生高速率的真随机码而受到人们的关注[11,12]. 混沌具有对初始状态非常敏感的特性, 即便初始值的微小变化也会导致系统出现完全不同的演化过程,因此非常适合作为随机码熵源. 在各种类型的混沌系统中,外部扰动下的半导体激光器由于能产生带宽达数 GHz 的混沌激光输出[13—17]而成为高速随机码的理想熵源,相关的研究也取得了重大突破[18—20]. 2008 年,Uchida 等[18]利用两路光

* 国家自然科学基金(批准号:61178011, 60978003, 61078003, 11004161)、重庆市自然科学基金(批准号: 2010BB9125)和中央高校基本科研业务费专项资金(批准号: XDJK2009B010, XDJK2010C021, XDJK2010C022)资助的课题.

† 通讯联系人. E-mail: zmwu@swu.edu.cn

反馈半导体激光器产生的互不相关的宽带宽混沌激光,经由数模转换和后续逻辑异或处理后最终得到了速率高达 1.7 Gbit/s 的真随机码. 然而这种结构的真随机码发生器也有一定缺憾:为了使产生的随机码无偏差(bias)必须使混沌光的平均功率保持恒定,从而对环境的稳定性要求较高. 2009 年,Kanter 等[19]采用了更为简洁的方案:采用单个半导体激光器在外部空间光反馈的作用下产生混沌激光输出,再经由 8 位数字采集卡对光强采样探测,并对生成的比特序列做差分处理,最终获得码率达 12.5 Gbit/s 的随机码. 2010 年,该小组又报道了通过多级差分处理方案把生成的随机码码率提高到了 300 Gbit/s[20]. 然而该方案是基于外部空间光反馈,因此系统对外部环境的变化仍然十分敏感,例如轻微震动或温度起伏都会使激光器混沌输出态发生变化,从而影响生成随机码的随机特性. 与此同时,我国的一些相关研究机构和小组也同步开展了相关研究,并取得了可喜的进展. 如最近太原理工大学王云才教授课题组报道了基于外腔反馈半导体激光器混沌熵源获取 1Gbit/s 真随机数的实验结果[21]. 同时该小组还理论上提出了一个基于半导体激光器混沌熵源获取 10 Gbit/s 真随机数的全光方案[22],该方案采用了两个半导体激光器,其中一个激光器作为混沌熵源,而另一个激光器的作用是通过其输出单向注入到该熵源中以提高熵源的混沌带宽.

与以上文献报道不同,本文所采用的混沌熵源是基于光纤连接的互注入半导体激光器,通过选取合适的互注入强度,实验获得宽带宽激光混沌输出. 另外,由于混沌熵源采用光纤架构,因而具有较好的稳定性. 通过后续的数据处理,获得了能通过美国国家标准和技术研究所(NIST)基于其 800-22 随机数测试标准[23]开发的一套统计检验软件——STS 测试以及 Diehard 测试的速率为 17.5 Gbit/s 的高速随机码.

2. 实　　验

基于互耦半导体激光器混沌输出产生随机码的实验装置如图 1 所示,该系统为全光纤型结构. 两只参数匹配较好的光纤型分布反馈(DFB)激光器通过光纤、偏振控制器以及可变衰减器连接而实现相互耦合. 其中,偏振控制器用以保证激光器偏振态的一致性,而可调衰减器用来控制两激光器的互耦强度. 当耦合率为 0.02 时,激光器 1(温度为 18.1 ℃,工作电流为 18.2 mA)和激光器 2(温度为 19.9 ℃,工作电流为 17.29 mA)均能产生宽带混沌激光输出. 本文着重讨论以激光器 2 的混沌输出作为随机码种子源信号的情况. 激光器 2 产生的宽带混沌激光通过耦合器、隔离器和型号为 New Focus 1544-B 高速光电探测器后转化为电信号输入到 Agilent 生产的型号为 E54855A 数字示波器中,由数字示波器中的 8 bit 精度的模数转换器(ADC)将信号转化为 8 位的二进制码. 利用集成软件系统对位移前后输出的二进制码做逻辑异或(XOR)运算处理,得到二进制比特序列. 再利用 NIST 800-22 标准测试以及 Diehard 测试软件对其进行随机性的甄别.

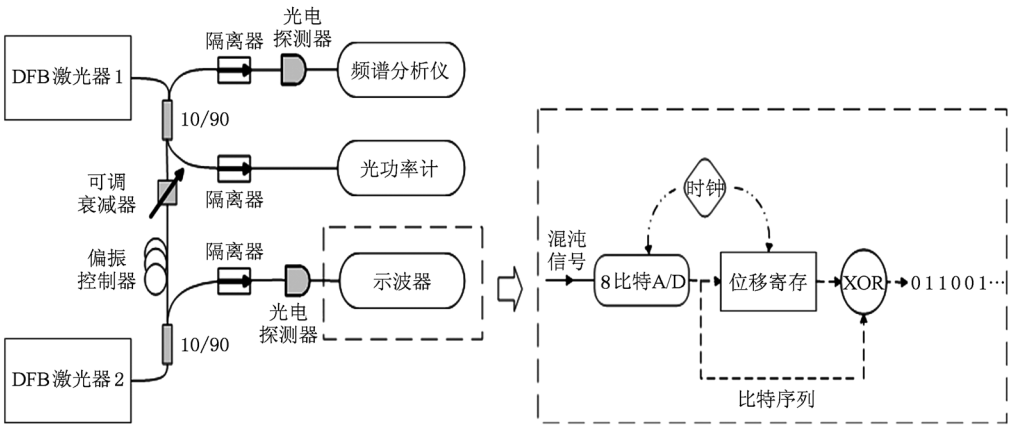

图 1　实验装置示意图

图 2 给出了由混沌信号转为随机比特序列的过程. 由于对混沌信号的连续两次采样的时间间隔必

须大于混沌的自相关时间,才能保证采样获得的相邻两个随机码之间的随机性[19]. 因此,采样速率必须小于混沌信号的带宽. 在实验中,ADC 的触发时钟频率设定为 2.5 GHz,即在混沌信号的时间序列中每隔 0.4 ns 抽取一个采样点进行模数转换,则对于 4 ns 长度的时间序列采样点数为 10 个(如图 2 中小黑点所示). 由于采样信号幅值并不符合正态分布的统计特性,因此数模转换后生成的二进制比特序列中"0"、"1"码分布不均衡,即统计特性有明显偏差,因此需要做进一步后续处理. 这里我们首先对比特序列进行移位,然后对位移前后的比特序列做 XOR 运算,得到偏差较小甚至无偏差的比特序列. 实验中,XOR 运算后能得到初级码率为 20 Gbit/s(=8 ×2.5 Gbit/s)的二进制比特序列.

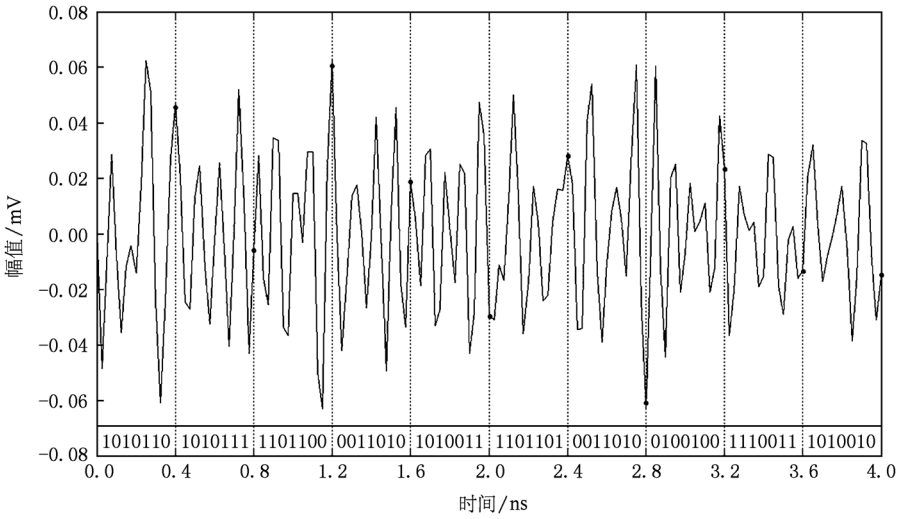

图 2 从混沌信号中提取随机比特序列

3. 结果与讨论

我们采用国际上权威的两套测试工具对产生的二进制比特序列进行随机性质量评估. 首先我们采用美国国家标准和技术研究所(NIST)基于其 800-22 随机数测试标准开发的一套统计检验软件——STS[23]对生成的随机码序列进行测试. NIST 提供的随机码测试项目共包含 15 项测试,用 P 值反映每项测试结果. 若 P 值大于显著水平值 $\alpha = 0.01$,则说明该随机码序列通过了相应的测试. 最终测试结果给出了每一个测试项目的 P 值(即 uniformity of P-values). P 值是对某一测试项结果给出的一系列 P 值做 χ^2 拟合优度分布检验(goodness-of-fit distributional test)后得到的计算值,当 P 值大于 10^{-4} 时并且每项测试的通过率也大于 $P - 3\sqrt{P(1-P)/m}$ 时($P = 1 - \alpha$, m 表示测试序列的组数),则输出的随机码达到了 800-22 标准,质量合格. 本实验我们采用的测试序列组数达 1000 组,则要求每项测试的通过率大于 0.9806. 实验中我们事先并不清楚经过 XOR 运算后串行输出的数据保留多少有效位数才能通过 STS 测试,因此我们首先保留全部 8 位的二进制码,如果串行输出的比特序列不能通过 NIST 的 800-22 测定标准,则舍弃一位最高有效位(MSB),继续采用 NIST 的 800-22 标准进行测试. 重复进行这一过程,直到所获得的串行比特序列通过 NIST 的 800-22 标准的所有测试. 测试结果表明:当保留全部 8 位二进制码时,串行输出的比特序列只能通过其中 5 项测试,因此随机性不能达到标准. 舍弃最高有效数位,即保留 7 位二进制码时,其 STS 的测试结果如表 1 所示. 其中对于有多个子项目的部分项目,我们只给出了测试结果最差时的情况. 由表 1 可以看出所有测试项目全部通过,从而可以获得码率为 17.5 Gbit/s(=7 ×2.5 Gbit/s)的随机码.

此外,我们也采用了 Diehard 随机数测试工具[24]进行验证,以进一步确保生成随机码的质量. Diehard 测试一共包含 18 项测试,如表 2 所示. 表 2 中部分测试项的 P 值是经由 Kolmogorov-Smirnov (KS)检验后给出的运算结果,其余包含多个子项目

的测试项我们给出了 P 值最小时的情况. 在显著水平值 $\alpha = 0.01$ 的情况下, P 值需大于 10^{-4}, 该测试项目才能通过. 由表 2 可以看出, 我们获得的 17.5 Gbit/s 的随机码能够通过全部的测试项目, 达到 Diehard 测试设定的标准.

表 1 NIST 统计测试结果 样本为 1000 组 1 Mbit 的比特序列

NIST 测试项目	P 值	通过率	结果
频数测试	0.645448	0.9950	通过
块内频数测试	0.941144	0.9890	通过
累加和测试	0.397688	0.9930	通过
游程测试	0.832561	0.9900	通过
块内最长游程测试	0.480771	0.9900	通过
二元矩阵秩测试	0.723804	0.9880	通过
离散傅立叶变换测试	0.463512	0.9850	通过
非重叠模块匹配测试	0.020548	0.9820	通过
重叠模块匹配测试	0.417219	0.9910	通过
通用统计测试	0.322135	0.9890	通过
近似熵测试	0.043455	0.9847	通过
随机偏移测试	0.018008	0.9847	通过
随机偏移变异测试	0.018008	0.9816	通过
序列测试	0.278461	0.9910	通过
线性复杂度测试	0.167184	0.9920	通过

表 2 Diehard 统计测试结果 样本为 74 Mbit 的随机序列

Diehard 测试项目	P 值	结果
生日间隔检验	0.983636(KS)	通过
重叠 5-置换检验	0.233805	通过
31×31 二元矩阵秩检验	0.578092	通过
32×32 二元矩阵秩检验	0.341039	通过
6×8 二元矩阵秩检验	0.484156(KS)	通过
比特流检验	0.06087	通过
OPSO 检验	0.0312	通过
OQSO 检验	0.0067	通过
DNA 检验	0.0255	通过
比特 1 计数检验	0.882205	通过
特定字节比特 1 计数检验	0.039073	通过
泊车检验	0.270593(KS)	通过
最小距离检验	0.404092(KS)	通过
三维圆球检验	0.351607(KS)	通过
减数检验	0.031994	通过
重叠累计和检验	0.252767	通过
游程检验	0.069216(KS)	通过
掷骰检验	0.461058	通过

4. 结 论

采用两个由光纤连接的互注入 DFB 激光器, 实验产生了 10 GHz 带宽的混沌激光输出. 通过模数转换以及后续处理最终获得了能够通过 STS 测试和 Diehard 测试、码率高达 17.5 Gbit/s 的高速随机码. 此方案具有结构简单、性能稳定、易于调试等优点. 本工作能为高速真随机码的获得提供一些有益的借鉴和参考.

[1] Eastlake D, Schiller J, Crocker S 2005 http://tools.ietf.org/html/rfc4086

[2] *FIPS PUB* 140-2 2001 http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

[3] Metropolis N, Ulam S 1949 *J. Am. Statist. Assoc.* **44** 335

[4] Dynes J F, Yuan Z L, Sharpe A W, Shields A J 2008 *Appl. Phys. Lett.* **93** 031109-1

[5] Gleeson J T 2002 *Appl. Phys. Lett.* **81** 1949

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

[7] Dynes J F, Yuan Z L, Sharpe A W, Shields A J 2008 *Appl. Phys. Lett.* **93** 1

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

[9] Stefanov A, Guinnard O, Guinnard L, Zbinden H, Gisin N 2000 *J. Mod. Opt.* **47** 595-8

[10] Jennewein T, Achleitner U, Weihs G, Weinfurter H, Zeilinger A 2000 *Rev. Sci. Instrum.* **71** 1675

[11] Stojanovski T, Kocarev L 2001 *IEEE Trans. Circ. Syst. Fund. Theor. Appl.* **48** 281

[12] Stojanovski T, Pihl J, Kocarev L 2001 IEEE Trans. *Circ. Syst. Fund. Theor. Appl.* **48** 382

[13] Yan S L 2010 *Acta Phys. Sin.* **59** 3810 (in Chinese) [颜森林 2010 物理学报 **59** 3810]

[14] Liu S F, Xia G Q, Wu J G, Li L F, Wu Z M 2008 *Acta Phys. Sin.* **57** 1502 (in Chinese) [刘胜芳、夏光琼、吴加贵、李林福、吴正茂 2008 物理学报 **57** 1502]

[15] Li X F, Pan W, Ma D, Luo B, Zhang W L, Xiong Y 2006 *Acta Phys. Sin.* **55** 5094 (in Chinese) [李孝峰、潘 炜、马 冬、罗 斌、张伟利、熊 悦 2006 物理学报 **55** 5094]

[16] Liu H J, Feng J C 2009 *Acta Phys. Sin.* **58** 1484 (in Chinese) [刘惠杰、冯久超 2009 物理学报 **58** 1484]

[17] Chao L P, Xia G Q, Deng T, Lin X D, Wu Z M 2010 *Acta Phys. Sin.* **59** 5541 (in Chinese) [操良平、夏光琼、邓 涛、林晓东、吴正茂 2010 物理学报 **59** 5541]

[18] 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

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

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

[21] 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 **60** 010501]

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

[23] National Institute of Standard and Technology, Special Publication 800-22 Revision 1a, 2010 http://csrc.nist.gov/publications/nist pubs/800-22-rev1/SP800-22rev1a.pdf

[24] Diehard: A Battery of Tests of Randomness, 1996 http://stat.fsu.edu/geo

17.5 Gbit/s random bit generation using chaotic output signal of mutually coupled semiconductor lasers*

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

(*School of Physics, Southwest University, Chongqing* 400715, *China*)

(Received 19 January 2011; revised manuscript received 17 February 2011)

Abstract

Based on two mutually coupled semiconductor lasers linked by fiber, a chaotic seed signal with a 10 GHz ultra-broadband is obtained experimentally. Adopting an 8-bit analog-to-digital converter, the seed signal is converted into a binary bit stream. By an exclusive-OR operation and the most significant bit rejection, a random bit sequence at a rate up to 17.5 Gbit/s, which has passed both the National Institute of Standard and Technology statistical test and the Diehard test, is obtained.

Keywords: random bit, chaotic laser, mutually coupled semiconductor lasers

PACS: 05.45.Gg, 05.40.-a, 42.55.Px

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61178011, 60978003, 61078003, 11004161), the Natural Science Foundation of Chongqing Municipal Administration (Grant No. 2010BB9125), and the Fundamental Research Funds for the Central Universities (Grant Nos. XDJK2009B010, XDJK2010C021, XDJK2010C022).

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