基于混沌激光产生 1 Gbit/s 的随机数*

陈莎莎 张建忠 杨玲珍 梁君生 王云才†

(太原理工大学理学院物理系,太原 030024)

(2010 年 3 月 8 日收到;2010 年 5 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,通过 8 位 ADC 将熵源信息转化为二进制码,并经后续差分运算处理改善其随机性,最终获得了 1 Gbit/s 的随机数. 所产生的随机数通过了 NIST Special Publication 800-22 的全部测试项.

关键词: 混沌激光, 随机数发生器, 半导体激光器, 模数转换

PACS: 05.40.Fb, 05.45.Jn

1. 引 言

随着计算机技术、通信技术的迅速发展,特别是互联网的普及,信息安全已受到社会各界的广泛重视. 在信息安全领域,随机数扮演着极为关键的角色,比如密钥管理、密码学协议、数字签名、以及身份认证等众多安全技术中都需要用到随机数.

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出的数值. 随着计算机运算能力的提高,伪随机序列用于加密被破解的可能性增加,将难以满足信息无条件安全的需要[1]. 真随机数则是建立在物理熵源的基础上,将采集到的熵源信息经过模数转换处理后提取出的信号,它是无法预知、不可再现的. 目前,真随机数发生器的熵源主要是基于电阻热噪声[2]、振荡器中的频率抖动[3]、电路混沌[4]和生物无规则特性[5]等物理现象. 受物理熵源电子器件带宽的限制,这些真随机数发生器产生随机数的速率比较低. 例如基于电阻热噪声和电子振荡器频率抖动产生的真随机数典型速率分别为 2 Mbit/s 和 10 Mbit/s. 此外,利用量子力学基本量的完全随机性也可以用作真随机数发生器的熵源[6,7]. 如基于单光子的路径选择随机性已研制出最高速率为 4 Mbit/s 的光量子真随机数发生器. 随着光纤通信 WDM 系统单信道传输速率已达 10 Gbit/s 并向 40 Gbit/s 发展,要实现大容量高速光通信的无条件安全,需采用一次一密的加密方式,这就要求实时大量地产生高速真随机数. 上述真随机数发生器的速率显然已经捉襟见肘,不能满足应用需求. 幸运的是,半导体激光器在光反馈、光注入或光电反馈条件下可轻易产生带宽为数 GHz 的混沌激光[8—10]. 2007 年 6 月,我们提出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,构造快速的真随机数发生器,并获得专利[11]. 2008 年 12 月,Uchida[12,13]利用两路不相关的混沌激光经过模数转换和异或处理,实验实现了 1.7 Gbit/s 真随机数的输出. 但是,为了使产生的随机数能够通过随机数测试标准,需满足强的约束条件,即要求混沌光的平均功率保持恒定,且需仔细调节比较器的判决阈值. 2009 年 7 月,Kanter 研究小组采用更简单的结构,利用 8 位模数转换器(ADC)从一路混沌激光中提取信息,通过后续的一级差分处理和多位串行输出可获得速率为 12.5 Gbit/s 的真随机数[14]. 随后,在 2010 年 1 月,该研究小组进一步采用多级差分处理获得了 300 Gbit/s 的真随机数[15]. 此方案产生的真随机数码率明显提高,且无需设定判决阈值. 但产生的混沌激光是半导体激光器通过自由空间光反馈(即外部放置反射镜)获得,这种反馈方式对周围环境条件极为敏感. 例如轻微的震动或者温度的起伏都会使混沌激光的混沌态发生变化,从而会影响真随机码序列的随机特性. 而利用光纤反射镜替代平面反射镜实现全

* 国家自然科学基金专项基金(批准号:60927007)和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

光纤结构的光反馈,可产生稳定的混沌激光,确保获得随机特性优良的真随机数.

本文利用半导体激光器在光纤反射镜提供光反馈作用下产生的混沌激光作为随机数发生器的熵源,通过模数转换和后续的差分运算处理,最终将熵源的混沌信号转换成 1 Gbit/s 的随机数. 利用 NIST Special Publication 800-22[16] 对所产生的随机数进行测试,测试结果表明所产生的随机数能够通过全部测试项.

2. 装置及原理

基于混沌激光产生高速随机数的装置如图 1 所示. 混沌源输出的混沌激光信号经过光电探测器转换为电信号. 在时钟的触发下,8 位 ADC 将电信号转化为二进制码,并利用移位寄存器对二进制码进行移位输出. 通过减法器实现对 ADC 前后时刻输出的二进制码进行差分运算处理,然后从差分运算处理后的 8 位二进制码中提取 2 位串行输出,最终获得随机数序列.

半导体激光器在光纤反射镜提供光反馈的作用下获得的混沌激光信号作为随机数熵源,实验装置如图 2 所示. DFB 半导体激光器(LDM5S752,中心波长为 1550 nm,阈值电流 I_{th} 为 22.5 mA)输出的光通过 40∶60 的耦合器后,40% 的光由光纤反射镜(FOM)反馈回半导体激光器中,另一部分光作为输出,外腔长为 7.4 m. 可调光衰减器(VOA)控制反馈回半导体激光器的反馈光强度,偏振控制器调节反馈光的偏振态,并用光功率计(OPM)监控反馈光强度. 当激光器的工作电流为 1.6 I_{th},反馈强度为 10% 时,DFB 半导体激光器输出混沌激光. 利用带宽为 2 GHz 的光电探测器将输出的混沌光信号转换为电信号,并将电信号输入到带宽为 500 MHz,采样率为 5 Gs/s 的实时示波器(Tektronix TDS3052)中进行观测和数据存储,同时利用频谱分析仪(Agilent E4407B)对输出的混沌激光频谱进行测量.

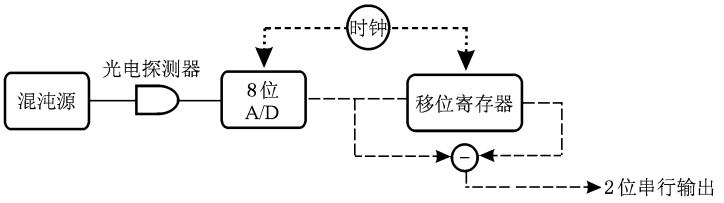

图 1 基于混沌激光产生随机数的框图

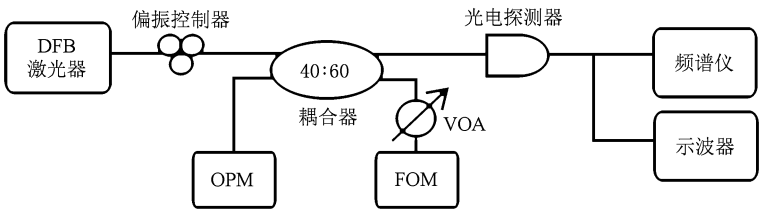

图 2 混沌源的实验装置图

实验测得带宽为 6.2 GHz[17] 混沌激光的频谱如图 3 中的黑色曲线所示,图中的灰色曲线为测试中噪声对应的频谱图. 图 4 为混沌光信号归一化后相应的自相关图,具有类似 δ 函数的形状. 其中次高峰位置对应反馈光在外腔中往返一周的延迟时间,约为 74 ns,表明输出的混沌信号具有外腔反馈引起的谐振成分. 基于一路混沌激光简单通过模数转换提取随机数,随机序列会显现弱周期性,因此需要后续利用差分运算处理来消除这一弱周期性.

将示波器采集到的混沌信号数据利用数字离线系统软件进行模数转换和后续差分运算处理. 受实验中示波器 500 MHz 带宽的限制,因此设置 ADC 的触发时钟频率为 500 MHz. 图 5 表示混沌信号的时序图,星点代表 5 GHz 实时示波器采集到的混沌信号幅值,圆点代表在触发时钟控制下 ADC 所采样的幅值点. 在数据处理中,对示波器存储的混沌信号每隔 10 个数据点提取 1 个进行量化,并转换成二进制码.

信号幅度分布概率服从正态分布是此信号作为随机信号提取源的必要条件. 图 6(a)表示混沌激

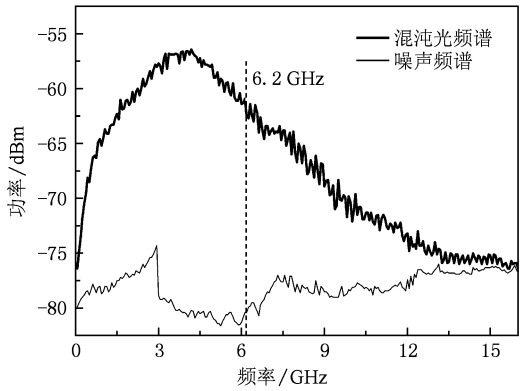

图 3 混沌激光频谱图

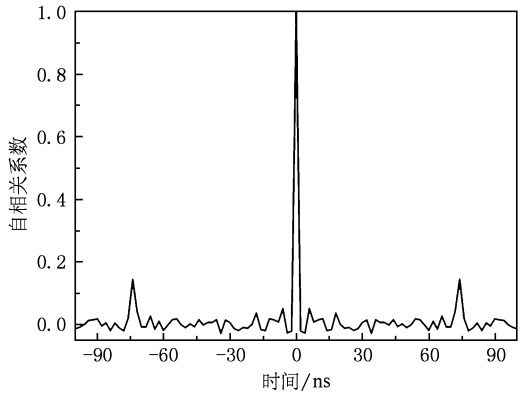

图 4 混沌光信号的自相关图

光信号由 8 位 ADC 转换后电压幅度统计分布直方图,横坐标代表采集到信号的电压幅度(其中电压幅度被分为 2^8 个单元),纵坐标代表每个单元中电压的分布概率. 可以看出信号幅度的分布概率相对于正态分布有明显偏差,产生的随机数不会满足随机性的要求. 为了得到偏差较小甚至无偏差的正态分布,使产生的随机数“0”和“1”分布均匀,将 ADC 前、后采样时刻采集到的混沌信号电压幅值利用差

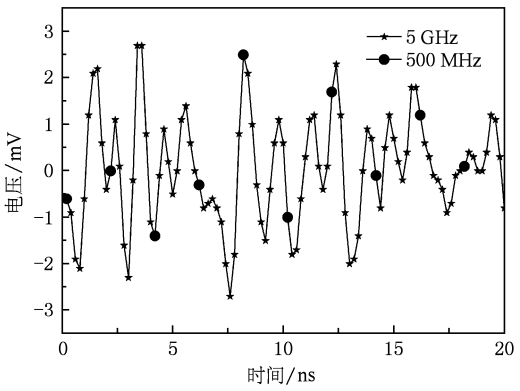

图 5 混沌信号时序图

分运算进行后续处理. 图 6(b)为经过差分处理后的信号电压幅度分布统计直方图,由此看出经过处理后的信号幅值服从完全对称的正态分布,从而提高了随机序列中“0”和“1”码分布的均衡性. 实际上,对 ADC 前、后采样时刻的信号幅度值进行差分运算相当于对其模数转换后的二进制码移位前、后对应的随机序列进行异或处理. 在 500 MHz 时钟的共同触发下,移位寄存器和 8 位 ADC 的输出有 2 ns 的时间延迟(移位 1 位),利用减法器将两者的输出相减,实现了对移位前、后得到的随机数序列的异或处理. 假设混沌信号经过 8 位 ADC 模数转换后得到 8 位二进制码,其中 1 位输出 0,1 码的概率分别为 $P(0) = \frac{1}{2} - \delta$ 和 $P(1) = \frac{1}{2} + \delta$ (δ 为 0,1 码的偏差值),则经过异或处理以后输出的 0,1 码的概率分别为

$$P_{\text{xor}}(0) = P(1)P(1) + P(0)P(0) = \frac{1}{2} + 2\delta^2,$$

$$P_{\text{xor}}(1) = P(1)P(0) + P(0)P(1) = \frac{1}{2} - 2\delta^2.$$

由此可以看出,异或处理后 0,1 的均衡性能够得到

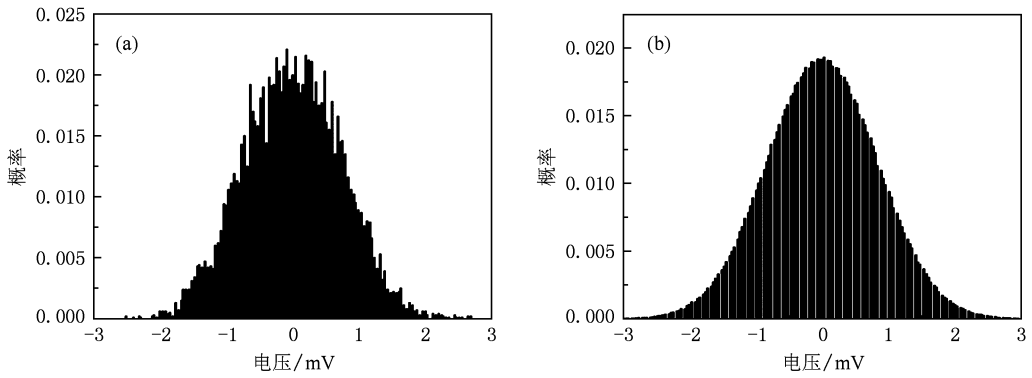

图 6 电压幅度统计直方图 (a),(b)分别表示差分处理前后对应的分布

改善,所占比率更接近于0.5.

3. 结果及讨论

经过后续的差分运算处理后,最终可获得1 Gbit/s的随机数输出,输出情况如图7所示.8位ADC的触发时钟为500 MHz,即从混沌激光的时序图中每隔2 ns提取1点进行模数转换和差分处理,如图7(a)所示.对于每1点提取的混沌信号经过8位ADC转换后可以产生8位二进制码,任意串行输出其中的2位,使得生成随机数的码率为触发时钟速率的2倍,即可输出如图7(b)所示的1 Gbit/s随机数.图8进一步给出了生成的1 Gbit/s随机序列的自相关图.与图4相比,自相关曲线中的次高峰已经消失,这说明经过差分处理后信号的弱周期性已被消除.

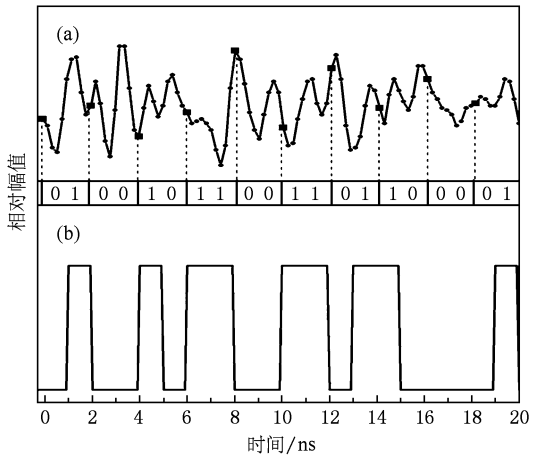

图7 基于混沌激光实现1 Gbit/s随机数的输出 (a)混沌信号输出;(b)二进制码输出

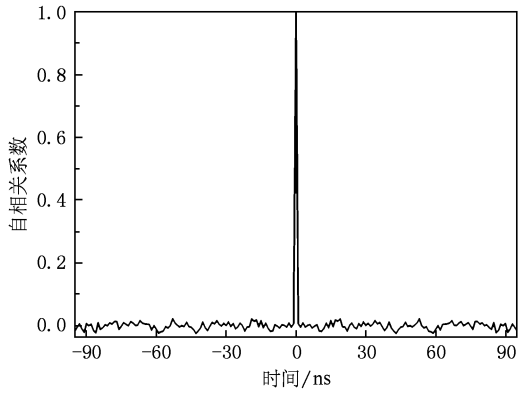

图8 随机序列的自相关图

然后,我们采用美国国家标准和技术研究所(NIST)提供的Special Publication 800-22随机数测试标准对生成的随机数序列进行了测试.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$\alpha = 0.01$,则说明该随机数序列通过了相应的测试.并计算了每项测试的通过率来进一步验证序列随机特性的有效性及正确性.当每项测试的通过率大于$p - 3\sqrt{\frac{p(1-p)}{m}}$时($p = 1 - \alpha$, m表示测试序列的组数),认为输出的随机数具有良好的随机性.采集1000组1 Mbit的二进制数据进行15项测试.在$m = 1000$组测试数据中,要求每项测试的通过率大于0.9806.表1给出了测试结果,其中加*表示测试中包含多项子测试,表格中仅给出这些子测试的最小测试结果.从表1可以看出,产生的1 Gbit/s随机数能够通过NIST的全部随机数测试标准.

表1 随机数测试结果

测试名称	$p_$value	通过率	结果
FT	0.993231	0.996	通过
FBT	0.351661	0.998	通过
CST*	0.684836	0. 997	通过
RT	0.649671	0.994	通过
LROBT	0.470294	0.994	通过
AET	0.388942	0.993	通过
ST*	0.943805	0.987	通过
RBMRT	0.651304	0.995	通过
DFTT	0.340245	0.998	通过
ATMT*	0.284854	0.999	通过
PTMT	0.051567	0.997	通过
MUST	0.510808	0.989	通过
RET*	0.630797	0.994	通过
REVT*	0.295072	0.996	通过
LCT	0.481680	0.994	通过

基于宽带混沌激光熵源,利用模数转换和差分运算处理提取随机数的过程中,影响随机数码率的主要因素有以下三点:1)混沌信号带宽.若从混沌激光信号中采样获得随机数序列,必须保证相邻两个随机数之间无相关性.要求采样间隔时间大于混沌信号的相关时间,即混沌信号的带宽应大于采样速率.2)ADC的精度.ADC精度越高,串行输出的位数越多,从而理论上可以提高随机数的码率.3)差分运算处理的级数.利用差分运算处理能够降低混

沌采样数据之间的相关性,差分处理的级数越高,数据间的相关性越弱,从而可通过提高差分处理的级数,突破混沌信号带宽对采样速率的限制[15]. 因此,在混沌信号带宽一定的情况下,可以提高差分运算处理的级数,从而极大地提高随机数的码率.

4. 结 论

本文利用半导体激光器在光纤反射镜提供光反馈作用下所获得的混沌激光信号作为随机数熵源,通过模数转换输出 8 位二进制码,从中任意提取 2 位串行输出,最终获得 1 Gbit/s 的随机数. 同时,利用后续的差分运算处理,可消除光反馈引起的随机数序列所显现的弱周期性. 基于宽带混沌激光产生的 1 Gbit/s 随机数能够通过 NIST 的全部测试项. 该方案仅从一路混沌激光信号中提取随机数,结构简单,易于集成,且具有不易受周围环境条件影响的优点,产生的高速随机数可应用于军事、通信、遥感以及混沌保密通信等领域.

[1] Aaldert C 1991 *Am. J. Phys.* **59** 700

[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] Stojanovski T, Pihl J, Kocarev L 2001 *IEEE Trans. Circuits Syst.* I **48** 382

[5] 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]

[6] 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]

[7] 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]

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

[9] 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** 4372]

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

[11] 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]

[12] 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

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

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

[15] Kanter I, Aviad Y, Reidler I, Cohen E, Rosenbluh M 2010 *Nature Photonics* **4** 58

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

[17] Lin F Y, liu J M 2003 *Opt. Commun.* **221** 173

One Gbit/s random bit generation based on chaotic laser*

Chen Sha-Sha Zhang Jian-Zhong Yang Ling-Zhen Liang Jun-Sheng Wang Yun-Cai†

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

(Received 8 March 2010; revised manuscript received 6 May 2010)

Abstract

In this paper, chaotic light generated by optical feedback semiconductor laser is employed as entropy source. The output waveform of chaotic laser is converted into a binary bit stream by an 8-bit ADC. The generated binary sequences are optimized to equalize the ratio of 1 and 0 by the difference between consecutive sampled 8-bit values. Finally a random bit sequence at rates of up to 1 Gbit/s is realized, and the randomness of long bit strings is verified by the NIST Special Publication 800-22 tests.

Keywords: chaotic laser, random bit generator, semiconductor laser, analog-to-digital conversion

PACS: 05.40.Fb, 05.45.Jn

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

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