基于混沌激光的 500 Mb/s 高速真随机数发生器

吕玉祥 牛利兵 张建忠 王云才
(太原理工大学理学院物理系，山西 太原 030024)

摘要 基于光反馈半导体激光器产生混沌激光作为熵源，设计制作了放大器、比较器及触发器等高频电子器件，实现对混沌激光的模数转换，产生一路随机数，与另一路不相关的随机数异或处理，无需后续数字处理，最快可实现 500 Mb/s 输出。产生的随机数序列通过了美国国家标准与技术研究院(NIST)的统计测试标准(SP800-22)。该随机数发生器码率可调，易集成，有利于产品化。

关键词 激光器；混沌激光；随机数发生器；高速
中图分类号 TN29 **文献标识码** A **doi**：10.3788/CJL201138.0502010

500 Mb/s Fast True Random Bit Generator Based on Chaotic Laser

Lü Yuxiang Niu Libing Zhang Jianzhong Wang Yuncai
(*Department of Physics, College of Science, Taiyuan University of Technology, Taiyuan, Shanxi* 030024, *China*)

Abstract A high speed random bit generator is proposed with chaotic semiconductor laser used as the entropy source. Analogue-to-digital conversion is realized by high frequency electronic devices such as amplifier, comparator, and trigger. One bit sequence is generated and exclusive OR (XOR) operated with other different bit sequences, and data processing in computer is needless. The generator outputs a 500 Mb/s random bit sequence. The obtained sequence passed the statistic test of national institute of standards and technology (NIST, SP800-22). It has the advantages of tunable speed and compact size, which make it easy to become a production.

Key words lasers; chaotic laser; random number generator; fast
OCIS codes 140.1540; 190.3100; 270.3100

1 引 言

随机数广泛应用于密码学、通信和国家信息安全等领域。随机数通常由算法运算和提取物理现象中随机信息两种方式产生[1,2]。通过算法生成随机数很容易在计算机平台上实现，但由于决定于运算法则的初值，要实现完全不可预测是不现实的，只要攻击者获得运算法则的初始条件就可以复制随机数。通常这种随机数叫作伪随机数[3]。而利用物理现象生成的随机数在专门硬件平台实现，所产生的随机数无法预知，不可再现，通常这种随机数被叫作真随机数。目前产生真随机数的方法有：直接放大电路或电子元件的热噪声[4]；基于振荡器采样产生随机数[5]；利用量子力学基本量的完全随机性产生随机数[6,7]——如放射性元素的衰变和激光斑纹图案空间分布的随机性等。但由于它们用于产生随机数的熵源的带宽有限，最终产生的随机数的码率被限制在每秒几十兆比特。基于光反馈半导体激光器可以产生大幅的几吉赫兹宽带的混沌激光，从而为生成高速真随机数提供物理熵源。2007 年，利用混沌激光产生作为随机数发生器熵源的构想被提出[8,9]。2008 年，原理性实验得以完成[10,11]。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(XOR)处理后，产生了 1.7 Gb/s的真随机数。原理性研究进一步证明，使用多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，可产生出更高速率的真随机数——12.5 Gb/s[12]。进而利用后续多级差分处理技术可获得码率达 300 Gb/s 的真随机数[13]。

本文利用混沌激光作为熵源，基于已有的原理性研究[14,15]，利用通用标准器件自主设计出高频硬

收稿日期：2010-12-08；**收到修改稿日期**：2011-02-18
基金项目：国家自然科学基金专项基金(60927007)和量子光学与光量子器件国家重点实验室开放课题(200903)资助课题。
作者简介：吕玉祥(1964—)，男，硕士，教授，主要从事光电技术方面的研究。E-mail：lyx823@126.com

件电路，最终实现了低成本的 500 Mb/s 高速真随机数发生器。产生的随机数通过了美国国家标准与技术研究院(NIST)的 15 项测试标准(SP800-22)。

2　实验装置

图 1 为基于高频硬件电路实现真随机数发生器原理图。实验中，混沌激光信号通过光反馈半导体激光器获得。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。两路不相关的混沌激光信号，经过光电探测器转换成混沌电信号，混沌电信号通过线性高频放大器进行放大，然后依次输入传输时延为 700 ps 的高速比较器和传输时延为 365 ps 的高速 D 类触发器生成两路二进制码，最后将两路不相关的二进制码进行逻辑异或运算产生一路真随机数。所使用的 D 类触发器上加可编程锁相环(PLL)合成时钟，5～800 MHz可调，随机数的码率由加在 D 类触发器上的时钟确定。实验中分别利用频谱分析仪和实时示波器来观察混沌信号的频谱以及所获得随机数的波形。

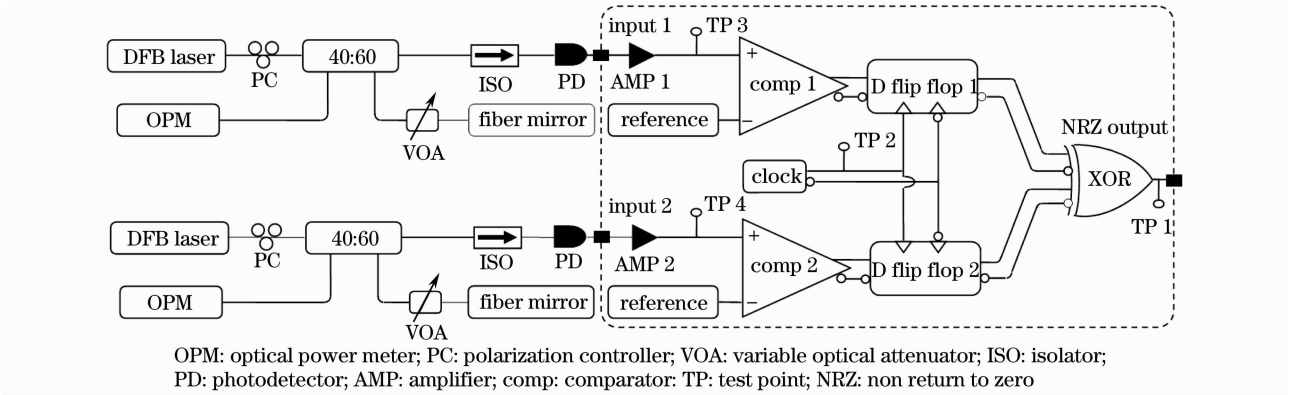

图 1　基于混沌激光实现真随机数发生器的装置图

Fig. 1　Setup of true random number generator based on chaotic laser

3　实验结果

3.1　随机数的实现

利用光反馈半导体激光器产生宽带混沌激光，本课题组已在前期工作中做了详细的实验研究[16]。当 DFB 半导体激光器的工作电流为 1.6 倍阈值电流，外腔长为 6.9 m，反馈强度为 10%时，可输出李雅普诺夫指数为 5.97 的混沌激光信号。图 2 为该混沌激光的频谱，带宽为 6.2 GHz。

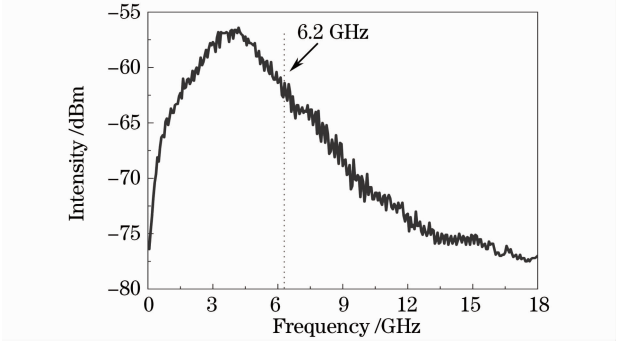

图 2　输出混沌激光的频谱图

Fig. 2　Chaotic laser output spectrum

图 3 为两路混沌激光产生真随机数，混沌激光 laser 1 和混沌激光 laser 2 为放大后的信号，时钟 clock 为 500 Mb/s，最小码率 tclk 为 2 ns。

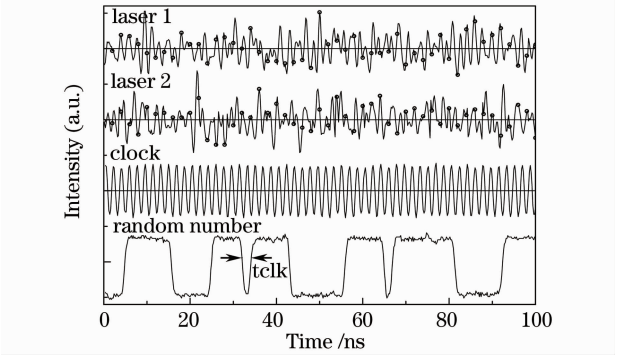

图 3　两路混沌激光产生真随机数

Fig. 3　Random number generated from two chaotic lasers

图 4 为两路二进制随机数经过异或后产生的真随机数。图 4(a)为一段 11111000000011100001000

01111111110001111111001111111111100111111110000 的非归零(NRZ)码，码率为 200 Mb/s，图 4(b)为一段000111110000011110111110000001111011111111000000111111100000111110000111 的 NRZ 码，码率为 500 Mb/s，两路由独立混沌激光生成的随机序列通过异或组合成一路的方法有效地改进了随机性。

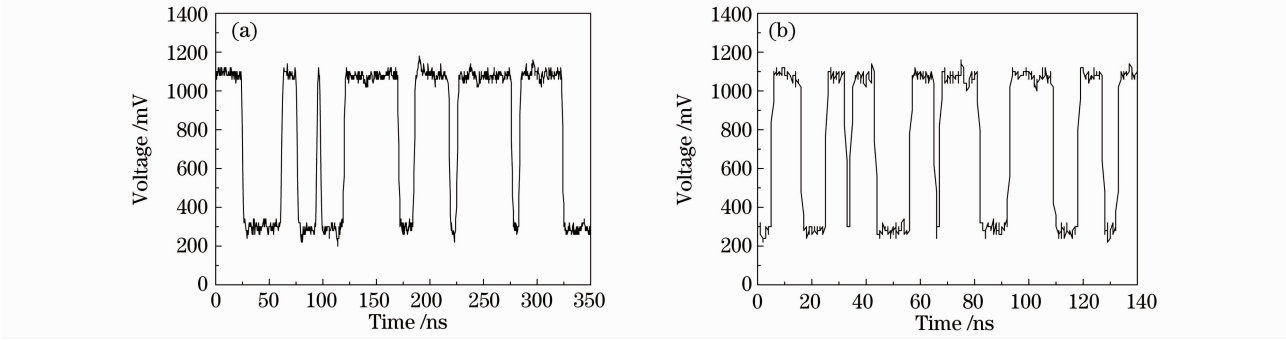

图 4 两路二进制随机数经过异或后产生的真随机数。(a)码率为 200 Mb/s，(b)码率为 500 Mb/s

Fig. 4 Random number is generated after two binary random numbers are XOR. (a) rate is 200 Mb/s, (b) rate is 500 Mb/s

采用 NIST 提供的 15 项统计测试标准(SP800-22)对产生的随机数进行检测。在此，采集了 1000 组 1 Mb 的二进制数据进行 15 项测试，其中显著水平数值选为 $\alpha=0.01$。在测试中如果观察到的显著水平 $P>\alpha$，表明通过了测试项。进一步评估随机数的有效性及正确性，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(15 项测试标准)的 P 值和通过概率统计测试结果如图 5(a)，(b)所示，当 15 项测试标准的 P 值大于 0.01 且通过概率超过 0.9806 时，认为通过 NIST 统计测试。图 5 中的数据说明利用两路不相关的混沌激光产生的码率为 500 Mb/s的二进制码序列的随机性通过 NIST 的全部测试。

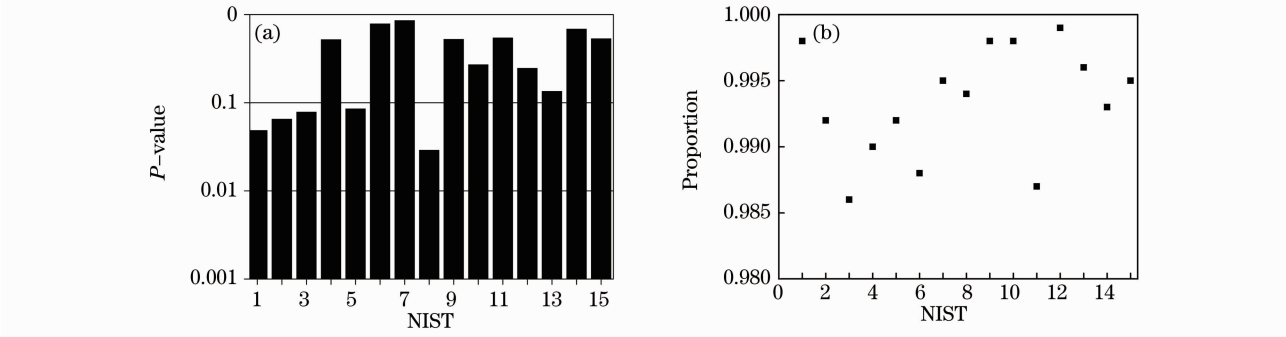

图 5 NIST 统计测试结果。(a)15 项测试标准的 P 值，(b)15 项测试标准的通过概率

Fig. 5 NIST statistical test results. (a) P-value of 15 test standards, (b) proportion of 15 test standards

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。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，测试结果如图 6 所示。

从图 6 中看到，在上述两种外腔长下，都没有出现 15 项测试全部通过的情况，而且随机序列通过 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 时，τ_{ext}/τ_s 的比值分别取到整数和非整数；当 τ_{ext}/τ_s 的比值为整数时，生成的随机序列通过 NIST 测试仅为 2、3 项；而当 τ_{ext}/τ_s 的比值为非整数时，可以通过 6～7 项 NIST 测试。当外腔长为 8.4 m 时，可得到类似的结果，如图 6 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

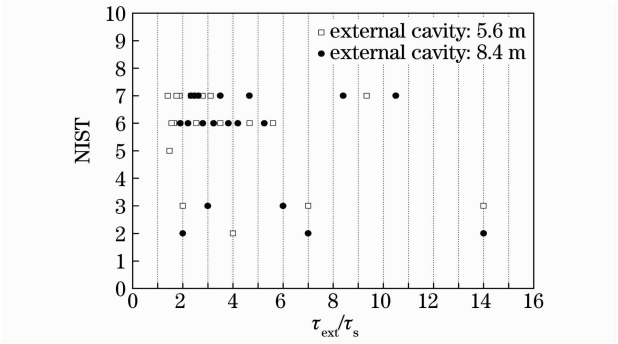

图 6　不同 τ_{ext}/τ_s 组合下，通过 NIST 统计测试项数的情况

Fig. 6　Results of passing the NIST statistical test in different τ_{ext}/τ_s combinations

性，可采用两路不相关随机序列进行异或处理。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，测试结果表明，当两路混沌源的外腔长不成比例时，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成比例时，不能通过全部测试项。

3.2　高频器件对随机数随机性的影响

测试高频硬件电路的高频放大器对随机数随机性影响，同时测试码率的可控性。把带宽为 10 MHz～26.5 GHz 射频合成仪(Agilent E8257D)生成的标准交流信号输入高频硬件电路，再利用带宽为 500 MHz，采样率为 5 GS/s 实时示波器(Tektronix TDS3052)通过预留的测试点 TP3 和 TP4 对放大器的频率和增益进行测试，测试结果如图 7 所示，表明在5～1000 MHz的频率范围内高频放大器增益平坦度为±0.9 dB，在此带宽范围内信号得到线性放大，这段带宽的混沌信号随机性得到保障，满足了 500 Mb/s 高速真随机数发生器的设计。

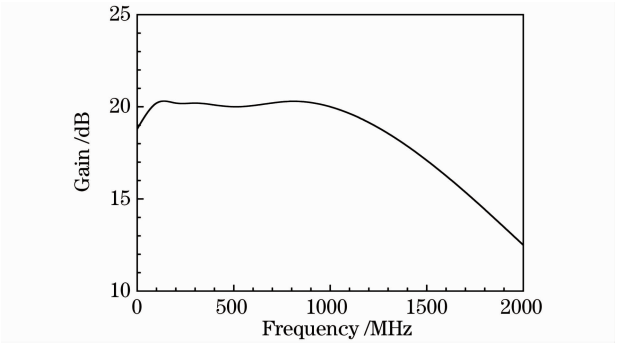

图 7　高频放大器增益平坦度曲线

Fig. 7　Curve of gain flatness for high frequency amplifier

从测试点 TP 3 和 TP 4 得到放大后的混沌激光信号如图 8(a)，(b)所示，放大后的混沌信号为交流信号，平均值为 0～1 mV，这样选择比较器的参考电压为 0 mV，进一步保证了随机数的随机性。

在设计中，码率可通过加在 D 类触发器上的时钟实现可调。通过预留的测试点 TP 2 可以对时钟进行测试。如图 9 所示，图中为加在 D 类触发器上的时钟，两路二进制随机数经过异或后，最终输出如图 4 的真随机数，当时钟频率不同时，相应的出码率也不同。图 9(a)频率为 200 Mb/s，对应图 4(a)；图 9(b)频率为 500 Mb/s，对应图 4(b)。

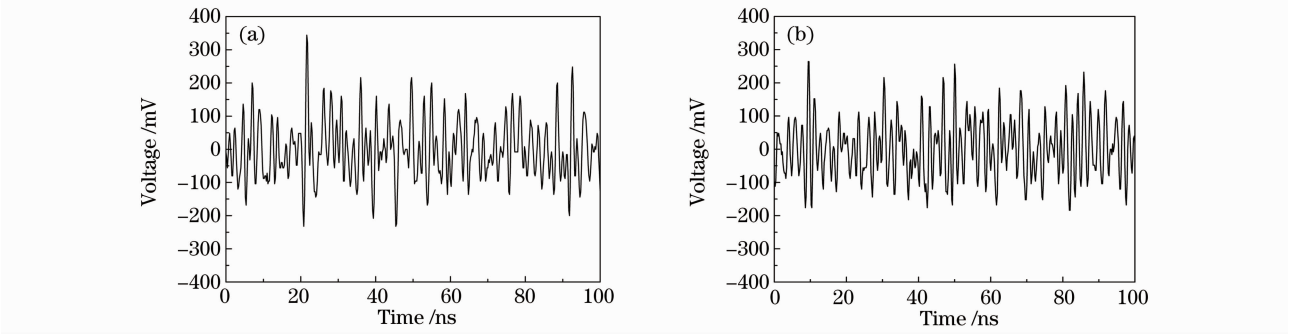

图 8　经过放大的混沌激光信号。(a)放大后的 1 路混沌信号，(b)放大后的 2 路混沌信号

Fig. 8　Chaotic laser signals after amplification. (a) 1 way chaotic signal after amplified, (2) 2 way chaotic signal after amplified

4　结　　论

利用设计的高频硬件电路实现了码率为 500 Mb/s的高速真随机数发生器. 该随机数发生器的物理熵源为基于光反馈半导体激光器产生的宽带混沌激光，将混沌激光的强度随机起伏通过比较器和 D 触发器转换为时间随机序列输出，所获得的随机数通过了 NIST 的随机数统计测试标准(SP800-22)。该方案的实现可为需要高速真随机数发生器的领域提供可靠的速率及可调节的高速随机数。

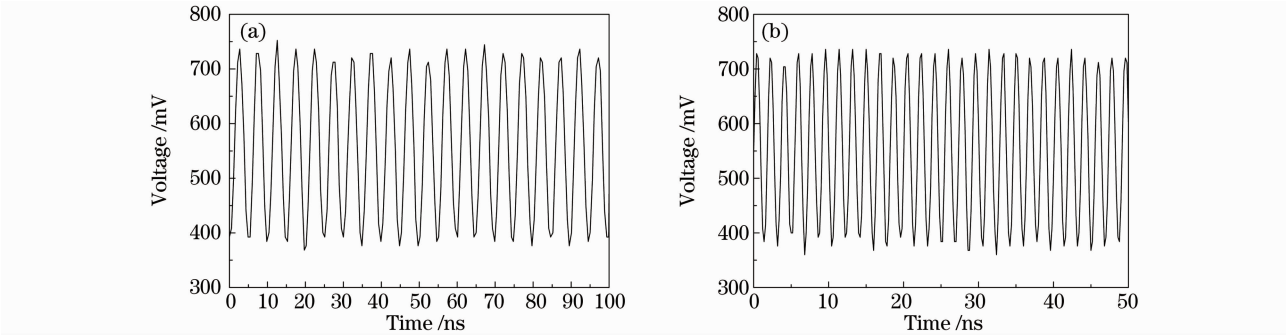

图 9 加在 D 类触发器上的时钟。(a)频率为 200 Mb/s,(b)频率为 500 Mb/s

Fig. 9 Clock added to the D flip-flop. (a) frequency of 200 Mb/s, (b) frequency of 500 Mb/s

参 考 文 献

1 F. Galton. Dice for statistical experiments[J]. *Nature*, 1890, **42**(1070): 13～14

2 B. Schneier. Applied Crytography[M]. New York: Jone Wiley & Sons, 1994. 301～307

3 E. M. Thomas, R. Rajarshi. Chaotic lasers: the world's fastest dice[J]. *Nature Photonics*, 2008, **2**(12): 714～715

4 C. S. Petrie, J. A. Connelly. A noise-based IC random number generator for applications in cryptography[J]. *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, 2000, **47**(5): 615～621

5 M. Bucci, L. Germani, R. Luzzi *et al*.. A high-speed IC random-number source for SmartCard microcontrollers[J]. *IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications*, 2003, **50**(11): 1373～1380

6 Liao Jing, Liang Chuang, Wei Yajun *et al*.. True random number generator based on a photon beamsplitter[J]. *Acta Physica Sinica*, 2001, **50**(3): 467～472
廖 静, 梁 创, 魏亚军 等. 基于光量子的真随机源[J]. 物理学报, 2001, **50**(3): 467～472

7 Feng Mingming, Qin Xiaolin, Zhou Chunyuan *et al*.. Quantum random number generator based on polarization[J]. *Acta Physica Sinica*, 2003, **52**(1): 72～76
冯明明, 秦小林, 周春源 等. 偏振光量子随机源[J]. 物理学报, 2003, **52**(1): 72～76

8 Wang Yuncai, Tang Junhua, Zhang Mingjiang. A laser-based chaotic random code generator and produce true random code method[P]. Chinese patent, 2007, ZL200710062140.1
王云才, 汤君华, 张明江. 一种基于混沌激光的真随机码发生器及其产生随机码的方法[P]. 中国发明专利, 2007, ZL200710062140.1

9 Wang Yuncai. Generation and applications of chaotic laser[J]. *Laser & Optoelectronics Progress*, 2009, **46**(4): 13～21
王云才. 混沌激光的产生与应用[J]. 激光与光电子学进展, 2009, **46**(4): 13～21

10 A. Uchida, K. Amano, M. Inoue *et al*.. Fast physical random bit generation with chaotic semiconductor lasers[J]. *Nature Photonics*, 2008, **2**(10): 728～732

11 K. Hirano, K. Amano A. Uchida *et al*.. Characteristics of fast physical random bit generation using chaotic semiconductor lasers [J]. *IEEE J. Quantum Electron.*, 2009, **45**(11): 1367～1379

12 I. Reidler, Y. Aviad, M. Rosenbluh *et al*.. Ultrahigh-speed random number generation based on a chaotic semiconductor laser [J]. *Phys. Rev. Lett.*, 2009, **103**(2): 024102

13 I. Kanter, Y. Aviad, I. Reidler *et al*.. Optical ultrafast random bit generator[J]. *Nature Photonics*, 2010, **4**(1): 58～61

14 Zhao Qingchun, Wang Yuncai. Research progress in security analysis of chaotic optical communication [J]. *Laser & Optoelectronics Progress*, 2010, **47**(3): 030602
赵清春, 王云才. 混沌激光通信的保密性能研究进展[J]. 激光与光电子学进展, 2010, **47**(3): 030602

15 Lü Ling, Li Gang, Meng Le *et al*.. Synchronization of chaotic lasers in unidirectional chain-connection network[J]. *Chinese J. Lasers*, 2010, **37**(10): 2533～2536
吕 翎, 李 钢, 孟 乐 等. 单向链式网络的激光混沌同步[J]. 中国激光, 2010, **37**(10): 2533～2536

16 A. B. Wang, Y. C. Wang, H. C. He. Enhancing the bandwidth of the optical chaotic signal generated by semiconductor laser with optical feedback[J]. *IEEE Photon. Technol. Lett.*, 2008, **20**(19): 1633～1635