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

面向全光物理随机数发生器的混沌实时光采样研究

李璞 江镭 孙媛媛 张建国 王云才

Study on real-time optical sampling of chaotic laser for all-optical physical random number generator

Li Pu Jiang Lei Sun Yuan-Yuan Zhang Jian-Guo Wang Yun-Cai

引用信息 Citation: Acta Physica Sinica, 64, 230502 (2015) DOI: 10.7498/aps.64.230502
在线阅读 View online: http://dx.doi.org/10.7498/aps.64.230502
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2015/V64/I23

面向全光物理随机数发生器的混沌实时光采样研究*

李璞 江镭 孙媛媛 张建国 王云才†

(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)

(太原理工大学物理与光电工程学院光电工程研究所, 太原 030024)

(2015 年 6 月 18 日收到; 2015 年 8 月 13 日收到修改稿)

基于混沌激光实现全光物理随机数发生器的物理基础是完成对混沌光信号的高速实时全光采样. 本文利用偏振无关的SOA 构建出TOAD 全光采样门, 以光反馈半导体激光器产生混沌激光, 对混沌激光的全光采样可行性进行了原理性实验论证, 实现了对光反馈半导体激光器产生的6.4 GHz 带宽的混沌激光5 GSa/s 的实时、高保真全光采样. 进一步研究显示, 光采样周期与外腔反馈时间成比例与否对混沌信号弱周期性的抑制水平影响显著. 当两者不成比例时, 可有效消除原始混沌信号的弱周期性, 有利于高质量物理随机数的产生.

关键词: 混沌激光, 随机数, 光采样, 太赫兹光非对称解复用器

PACS: 05.45.Jn, 05.45.Gg **DOI:** 10.7498/aps.64.230502

1 引 言

安全可靠的随机数(密钥)在保密通信领域有着重要应用. 根据Shannon 的“一次一密”理论(One-time Pad)[1], 绝对安全保密通信的实现需要满足以下条件: 1) 密钥是安全随机的; 2) 密钥长度不短于明文长度; 3) 密钥只用一次. 随着光纤通信WDM 技术的广泛应用, 当前数字通信系统单信道速率已突破10 Gb/s, 40 Gb/s 技术日趋成熟, 并朝向100 Gb/s 通信速率发展. 要保证如此大容量通信的绝对安全, 就要求大量、安全随机密钥的实时、快速产生.

利用自然界微观量子机理或宏观随机现象可产生出无法预测的随机数, 这种方法称作物理随机数发生器. 传统的物理随机数发生器多利用热噪声、振荡器相位抖动、单光子随机性[2] 及混沌电路等[3] 来提取随机数, 但受限于所用熵源的带宽, 其典型码率处于Mb/s 量级, 无法满足现代安全通信需要.

近些年来, 混沌激光由于具有高带宽、大幅度随机起伏等特性[4−9], 是构建安全、可靠、高速物理随机数发生器的理想熵源, 获得了人们的极大关注. 2007 年, 我们首次提出以光反馈半导体激光器产生的宽带混沌激光作为物理熵源, 可构建快速真随机数发生器的专利技术[10]. 2008 年, Uchida 课题组利用混沌激光和1 位电ADC 量化技术, 实现了实时速率达1.7 Gb/s 的物理随机序列的产生[11]; 2013 年, 我们课题组利用混沌激光延迟差分技术和1 位电ADC 量化技术, 构建了实时速率达4.5 Gb/s 物理随机数发生器[12]. 近年来, 许多研究小组采用多位ADC 提取技术获得了更高速率的物理随机数[13−19]. 然而, 这些超高速物理随机数的提取往往是先利用高速示波器对混沌信号进行采集存储, 然后进行离线的后续算法处理(移位寄存、高阶差分等), 并未实际产生. 事实上, 文献[12] 中报道的

* 国家自然科学基金科学仪器基础研究专款(批准号: 61227016)、国家自然科学基金青年科学基金(批准号: 61205142, 51404165) 和山西省自然科学基金(批准号: 2015021088) 资助的课题.

† 通信作者. E-mail: wangyc@tyut.edu.cn

4.5 Gb/s物理随机数是目前报道的实时速率最快的物理随机数发生器. 想进一步提高物理随机数的实时产生速率, 势必面临“电子瓶颈”的限制. 而且, 在Gb/s工作速率下, 电时钟的孔径抖动问题(ps量级)会在采样过程中严重劣化信号转换精度和信噪比, 并给关键器件(移位寄存器、异或门等)间精确同步的实际实现带来严峻挑战.

全光物理随机数发生器技术可有效克服上述方案的局限性. 2010年, 我们课题组首次提出利用宽带混沌熵源、全光采样器和全光比较器等构成全光高速物理随机数发生器实现方案, 并数值论证了10 Gb/s全光物理随机数实时产生的可行性[20]. 该类方案采用孔径抖动处于fs量级的锁模光纤激光器作为采样光时钟, 利用光纤环镜(NOLM)作为全光采样器直接在光域中对混沌激光进行采样, 进而利用四分之一波长相移DFB激光器作为全光比较器对其进行量化编码得到最终的随机数. 随后, 我们又对全光物理随机数发生器方案进行了优化[21]. 但截止目前, 尚未有实验报道.

全光物理随机数发生器物理实现的首要困难在于完成对混沌激光的实时光采样. 目前的全光采样技术多是利用光纤的四波混频[22,23]、交叉相位调制等[24,25]非线性效应实现. 这些方案或需要较高的光时钟功率, 或需要较长的高非线性光纤, 增加了系统复杂度, 极其不利于实际系统构建和集成. 本文利用增益饱和能量低、集成度高、稳定性好的半导体光放大器(SOA)构建太赫兹光非对称解复用器(TOAD)结构的全光采样门, 锁模光纤激光器作为光时钟, 对混沌光采样进行了原理性实验论证, 实现了对光反馈半导体激光器产生的6.4 GHz带宽的混沌激光5 GSa/s的低功耗、实时光采样; 并面向全光物理随机数发生器, 进一步实验分析了光采样率对所产生物理随机数质量的影响, 结果表明当光采样率与光反馈混沌激光器外腔长度不成比例时, 可有效消除原始混沌信号中的弱周期性, 能直接获得优质随机数. 这些工作扫清了全光物理随机数发生器的实现过程中的第一个技术障碍, 为其彻底实现奠定了基础.

2 实验装置及采样原理

2.1 实验装置

混沌激光实时光采样实验系统如图1所示, 该系统可分为三部分: 采样脉冲源、混沌激光源和TOAD全光采样门. 采样脉冲源为超快光时钟(UOC, Pritel, UOC-05-14 G-E)产生的高斯型脉冲序列. 该光时钟是一个主动锁模激光器构结构, 时延抖动小于50 fs. 混沌激光则由分布式反馈半导体激光器(DFB-LD, WTD, LDM5S752)利用光反馈的方式产生: 反馈光由一个反射率为99% 的光纤反射镜(FM)提供, 可调光衰减器(VOA2)和偏振控制器(PC1)分别调节反馈光的强度和偏振态.

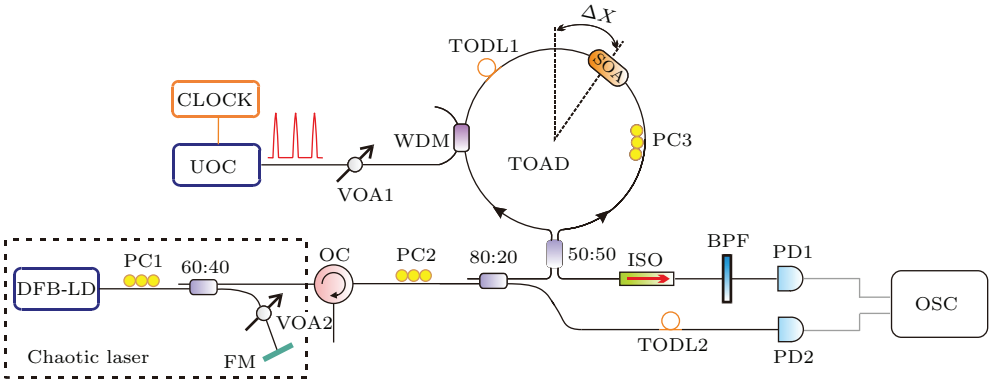

图1 (网刊彩色) 混沌激光实时光采样实验装置图(CLOCK, 射频时钟; UOC, 超快光时钟; VOA, 可调光衰减器; WDM, 波分复用器; TODL, 可调光延迟线; SOA, 半导体光放大器; PC, 偏振控制器; DFB-LD, 分布式反馈半导体激光器; OC, 光环行器; ISO, 光隔离器; BPF, 光带通滤波器; PD, 光电探测器; OSC, 数字示波器)

Fig. 1. (color online) Experimental setup of real-time optical sampling of chaotic laser, Clock: RF Clock, UOC: Ultrafast Optical Clock, VOA: Variable Optical Attenuator, WDM: Wavelength Division Mmultiplexer, TODL: Tunable Optical Delay Line, SOA: Semiconductor Optical Amplifier, PC: Polarization Controller, DFB-LD: Distributed Feedback Semiconductor Laser Diode, OC: Optical Circulator, ISO: Optical Isolator, BPF: Optical Band Pass Filter, PD: Photoelectric Detector, OSC: Digital Oscilloscope.

将分光比为60 : 40的光纤耦合器的40%端口作为反馈端, 60%端口作为输出端. 全光采样门为多量子阱结构的非线性半导体光放大器(SOA, Kamelian, SOA-NL-L1-C-FA)构建的TOAD结构. 此SOA偏振无关, 典型工作电流为300 mA, 相应的增益恢复时间为25 ps, 小信号增益为26 dB. 可调光衰减器(VOA1)用于调节采样所需的最佳采样脉冲功率, 环中的可调光延迟线(TODL1, General Photonics, MDL-002)用来改变SOA在光纤环中的非对称偏移量, 以实现不同宽度的采样窗口. 利用偏振控制器(PC2, PC3)调节混沌信号光进入环前和环路中的偏振态, 以消除SOA的残余偏振依赖. TOAD最终输出经带通滤波器(BPF)滤除采样脉冲和ASE噪声后, 再由光电探测器(PD1, U2 T, XPDV2120RA, 带宽44 GHz)光电转换后接入数字示波器(OSC, Lecroy, LabMaster10-36Zi, 带宽36 GHz). 与此同时, 作为被采样的混沌激光信号由分光比为80 : 20的光纤耦合器分出20%, 经可调光延迟线(TODL2, Newport, F-VDL-2-6-FP-S)适当延迟后, 由光电探测器(PD2, U2 T, XPDV2120RA, 带宽 44 GHz)接入示波器进行同步实时观察. TOAD输出端的光隔离器(ISO)是为了防止输出信号反射回TOAD造成干扰.

2.2 采样原理

混沌激光的采样原理如下: 采样光时钟脉冲由波分复用器(WDM)耦合进入TOAD环, 混沌激光信号经分光比为50 : 50的光耦合器进入TOAD环内, 分为沿顺时针方向(CW)和逆时针方向(CCW)传播的两路信号光, 绕环一周后回到耦合器发生干涉. 干涉输出信号满足以下关系式:

$$P_{\rm out}=\frac{1}{4}P_{\rm in}[G_{\rm CW}+G_{\rm CCW}-2\sqrt{G_{\rm CW}G_{\rm CCW}}\times\cos(\phi_{\rm CW}-\phi_{\rm CCW})], \quad (1)$$

式中, $P_{\rm in}$为输入混沌激光的功率, $G_{\rm CW}$, $G_{\rm CCW}$和$\phi_{\rm CW}$, $\phi_{\rm CCW}$分别为CW, CCW信号光经过SOA时经历的增益和相移. 由于SOA偏离环中心点一定位置, 两路信号光将在不同时刻经过SOA, 彼此之间时延差为$\Delta t=2\Delta x/v_{\rm g}$, $v_{\rm g}$为信号光在光纤环内的传输速度. 当无采样脉冲时, SOA对两路信号光的作用相同, 即$G_{\rm CW}$与$G_{\rm CCW}$相同, $\phi_{\rm CW}$与$\phi_{\rm CCW}$相等, 在耦合器干涉时无信号光输出. 当有采样脉冲时, 使SOA达到饱和, 载流子密度发生改变. 此时CW和CCW两路信号光将经历不同的增益和相位调制, 彼此之间存在相位差, 在耦合器干涉时则有信号光输出. 于是TOAD相当于打开了一个宽度约为Δt的时间窗口, 该窗口的幅度携带原始混沌激光相应时刻的强度信息, 这就实现了对混沌激光的采样. 该窗口随采样脉冲的到来而周期性地出现, 改变采样脉冲功率和SOA在环里的非对称偏移量可以改变SOA的动态响应特性, 从而控制TOAD传输特性.

3 实验结果

3.1 混沌激光特性

混沌激光的产生装置如图1中虚线框所示, 实验中DFB激光器偏置电流为37.4 mA ($1.7I_{\rm th}$), 中心波长为1553.658 nm, 反馈强度约为2%, 反馈腔长约为9.26 m, 产生的混沌激光特性如图2所示. 图2(a), (b), (c)分别为混沌激光的时序图、功率谱及自相关曲线. 时序图由示波器在40 GS/s采样率下获得, 功率谱图由频谱分析仪在分辨率带宽和视觉带宽分别为3 MHz和3 kHz下获得. 从图2(a)和(b)中可以看出, 混沌光在时序上具有类噪声的随机起伏特性, 在频谱上具有连续的宽带特性. 功率谱图中灰色曲线为激光器和探测器基底噪声的频谱, 按频谱能量的80%定义信号的带宽, 该混沌激光的带宽约为6.4 GHz. 由于光反馈外腔的存在, 其自相关曲线在外腔延迟时间τ及其整数倍处存在相关峰, 如图2(c)所示. 换句话说, 基于光反馈产生的混沌激光具有一定的弱周期性, 该周期对应于外腔往返时间τ($\tau=2nL/c$, L为反馈腔长, c和n分别为真空中光速和光纤折射率).

3.2 TOAD采样门特性

为使采样效果达到最佳, 首先分析了实验中TOAD全光采样门的相关特性. 为了方便观察采样门特性, 我们以直流光代替混沌激光作为探测光, 调节可调光衰减器(VOA2)使反馈强度为零, 此时DFB激光器即可发射稳定的直流光. UOC产生的采样脉冲重复频率为5 GHz, 脉冲半高全宽(FWHM)为2.2 ps. 图3给出了采样实验中TOAD全光采样门的相关特性. 图3(a)所示为采样脉冲

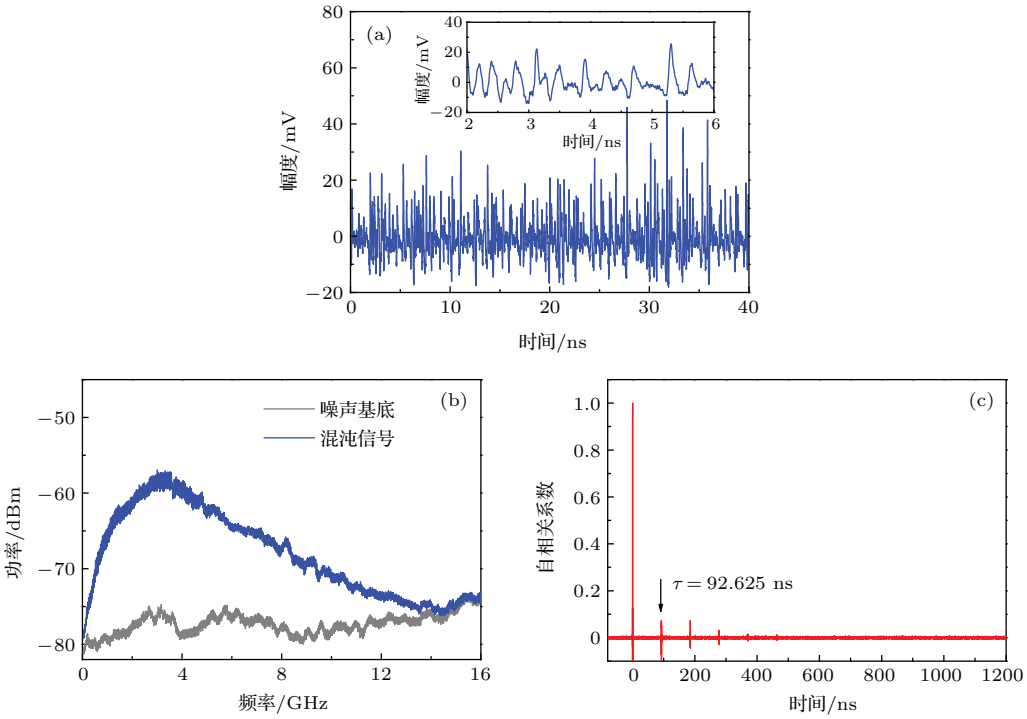

图 2 (网刊彩色) 混沌激光特性 (a) 时序; (b) 功率谱; (c) 自相关曲线

Fig. 2. (color online) Characteristics of chaotic laser: (a) Temporal waveform; (b) power spectrum (RBW: 3 MHz; VBW: 3 KHz); (c) autocorrelation curve.

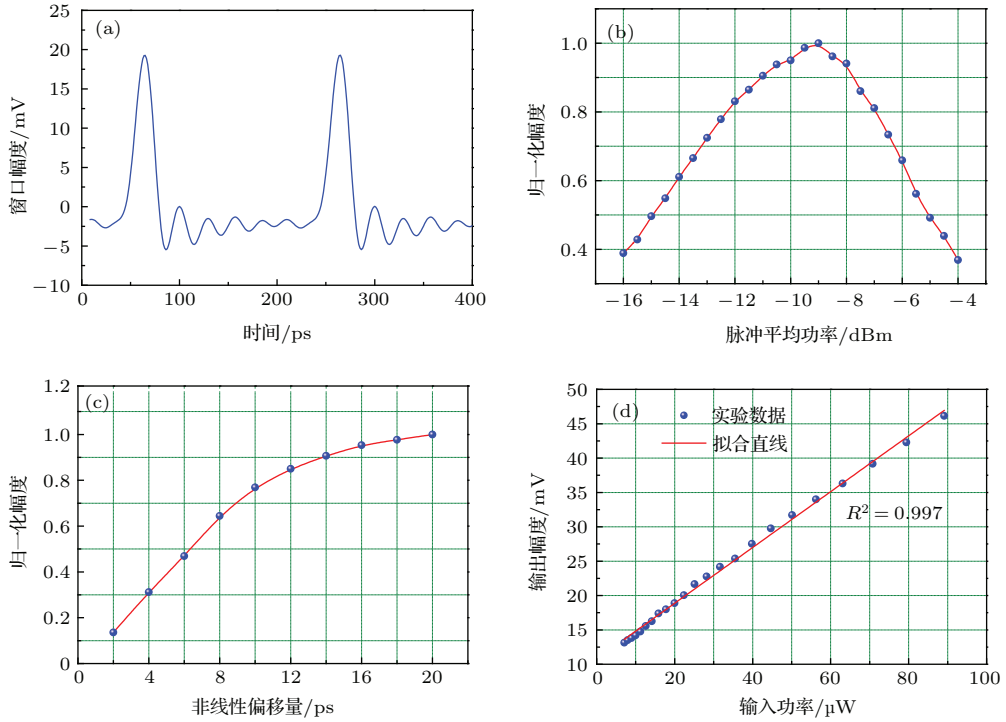

图 3 (网刊彩色) TOAD 采样门特性 (a) 采样窗口时域波形; (b) 不同采样脉冲功率下的采样窗口幅度; (c) 非对称偏移量对采样窗口幅度的影响; (d) 采样门线性度

Fig. 3. (color online) Characteristics of TOAD sampler: (a) Temporal waveform of sampling windows; (b) normalized amplitude of sampling windows under different sampling pulse power; (c) effect of the asymmetric offset on the normalized amplitude of the sampling window; (d) linearity of TOAD sampler.

平均功率为 −9 dBm, 非对称偏移量为15 ps时的采样窗口波形. 图中给出了两个采样窗口, 间隔为200 ps, 对应于采样脉冲5 GHz的重复频率. 非对称偏移量t', 由SOA偏离环中心点位置Δx决定. 定量地, $t'=\Delta x/v_{\rm g}$. 其中, $v_{\rm g}$是探测信号在光纤环内的群速度. 实验中, 通过 TODL1来改变Δx, 从而改变非对称偏移量t', 可实现不同宽度的采样窗口. 图3 (b) 所示为非对称偏移量为15 ps时, 采样窗口幅度随采样脉冲平均功率的变化关系曲线. 明显看出, 采样脉冲功率对采样输出具有显著影响, 存在一个最佳的采样脉冲功率(图中最高点所对应的功率). 从(1)式得知, 该功率即为实现CW与CCW信号光相位差为π时的最佳采样脉冲功率, 此值约为−9 dBm. 图3 (c) 所示为在最佳采样脉冲功率下, 非对称偏移量t'从 2 ps 到20 ps 以 2 ps为步进变化时, 采样窗口幅度随之变化的情况. 非对称偏移量较小(10 ps以下)时, 随着非对称偏移量的增大, 输出功率急剧增加, 这是采样窗口变宽的必然结果; 继续增大非对称偏移量, 采样门的输出功率已经逐渐接近信号光功率, 采样窗口对其影响自然减弱, 采样窗口的归一化幅度变化随之趋于平缓. 正是基于此, 本实验将非线性偏移量设定在平缓区的15 ps处, 以充分利用探测信号(待采样信号)的能量、提高信噪比. 图3 (d) 所示为在最佳采样脉冲功率下, 非对称偏移量为15 ps时, 采样窗口的输出幅度随输入的探测光功率的变化曲线, 反映了采样的精确程度. 经计算, 当输入待采样信号的功率小于90 μW时, 该线性度R^2为0.997, 可保证采样过程的高保真.

3.3 混沌光采样的实现及评估

结合上述TOAD采样门相关特性, 利用非对称偏移量为15 ps、最佳采样脉冲功率为−9 dBm时的全光采样门对光反馈半导体激光器产生的混沌激光进行了实时光采样. 采样中, DFB激光器工作在偏置电流为37.4 mA ($1.7I_{\rm th}$), 反馈强度约为2%, 反馈腔长约为9.26 m, 产生的混沌激光特性如图2所示. 图4给出了在此条件下混沌激光采样的同步时序结果图. 图4 (a) 所示为被采样的原始混沌激光信号, 幅值呈现随机起伏状态, 可以预想到采样后的脉冲峰值也应呈随机起伏状态. 图4 (b) 为重复频率为5 GHz的采样脉冲序列, 图4 (c) 即为在上述采样条件下, 采样后得到的混沌脉冲序列. 可以看到, 采样后脉冲的峰值呈现随机起伏状, 因此我们称采样后的脉冲序列为混沌脉冲序列. 为了更直观地观察采样效果, 我们在原始混沌激光时序中对被采样点进行了标记, 如图4 (a) 中的红色标记点所示. 对比这些红色标记点和对应时刻的混沌脉冲峰值, 可以发现混沌脉冲峰值的起伏与原始混沌激光起伏一致, 说明采样效果较好. 此外, 还发现采样得到的混沌脉冲相比原始混沌激光平均功率有所增益.

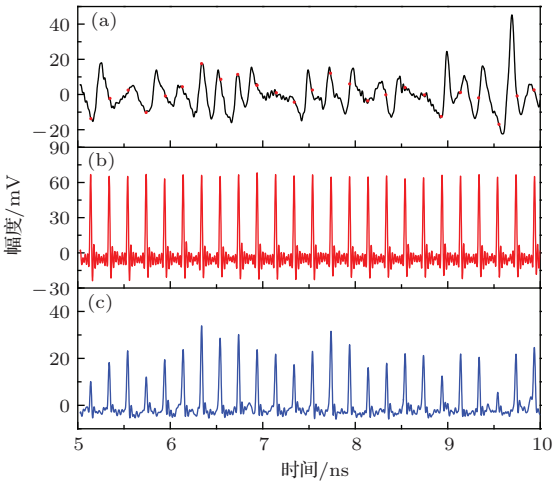

图4 (网刊彩色) 混沌激光实时光采样结果 (a) 混沌激光时序; (b) 采样脉冲序列; (c) 采样后的混沌脉冲序列

Fig. 4. (color online) Results of real-time optical sampling of chaotic laser: (a) temporal waveform of chaotic laser; (b) sampling pulses train; (c) chaotic pulses train after sampling.

3.4 光采样率对提取随机数质量的影响

混沌光采样是全光随机数发生器的实现基础, 对最终所提取随机数的质量有着重要的影响. 同其他随机数光电产生技术相同, 全光随机数的提取过程中, 光反馈半导体激光器产生的混沌激光所具有的弱周期性, 会遗传给所产生的随机数, 不利于优质随机数的产生, 必须设法消除之.

控制激光器的外腔长度、偏置电流、反馈强度等相关参数, 可在一定程度上有效降低混沌的弱周期性. 本实验中, 混沌激光信号的弱周期所对应的自相关系数被抑制在约0.07处, 如图2 (c) 所示. 基于此, 这里主要探讨光采样率(即采样周期)与混沌的弱周期成比例与否对产生随机数的影响. 需要说明的是, 这里混沌弱周期指的是利用光反馈方式产生混沌激光时的光反馈延迟时间. 由于混沌激光时

序的弱周期性可以通过自相关曲线方便地提取, 因此我们首先通过分析光采样前、后混沌自相关特性, 来探讨混沌激光的光采样周期与混沌周期成比例与否对混沌弱周期性的影响; 继而, 对利用8位模数转换(ADC)方式由混沌脉冲峰值提取出的随机数通过随机数行业测试标准NIST [26] 的情况进一步证实其对随机数质量的影响.

当光采样周期与混沌的弱周期不成比例时, 采样前、后混沌的自相关特性如图5所示. 图5(a-i), (a-ii)和(b-i), (b-ii)分别为采样前原始混沌信号和采样后混沌脉冲峰值的自相关曲线. 从图2(c)所示的自相关曲线可知, 被采样的混沌激光信号弱周期为92.625 ns. 图5(a-i)和(b-i)中, 光采样率为5 GS/s, 即光采样周期为0.2 ns, 92.625/0.2 = 463.125(非整数); 图5(a-ii)和(b-ii)中, 光采样率为5.100145 GS/s, 即光采样周期为0.19607286 ns, 92.625/0.19607286 = 472.401(非整数). 图5结果表明, 在这种条件下, 光采样周期与混沌的弱周期不成比例时, 采样前、后混沌的自相关曲线均没有任何旁瓣, 弱周期性可被消除.

当光采样周期与混沌的弱周期成比例时, 采样前、后混沌的自相关特性如图6所示, 图6(a-i), (a-ii)和(b-i), (b-ii)分别为采样前原始混沌信号和采样后混沌脉冲峰值的自相关曲线. 图6(a-i)和(b-i)中, 光采样率为5.031039 GS/s, 即光采样周期为0.1987661 ns, 92.625/0.1987661 = 466(整数); 图6(a-ii)和(b-ii)中, 光采样率为5.117409 GS/s, 即光采样周期为0.19541139 ns, 92.625/0.19541139 = 474(整数). 因此, 在这两组采样率下, 光采样周期与混沌的弱周期成比例. 如图中所示, 这种采样率情况下, 采样前、后混沌的自相关曲线仍有旁瓣出现, 意味着混沌弱周期性不能被完全抑制. 故而, 我们在提取随机数过程中选择采样光时钟速率时, 应该避免与原始混沌的弱周期成比例, 以免提取的随机数遗传到原始混沌信号的弱周期性.

这里需要说明的是, 采样前的自相关曲线是由原始混沌信号中的被采样点(如图4(a)中红色标记点)做自相关得到, 采样后的自相关曲线是由采样后混沌脉冲峰值点(如图4(c)中混沌脉冲各峰值点)做自相关得到, 制图所采用的点数均为1 Mbit.

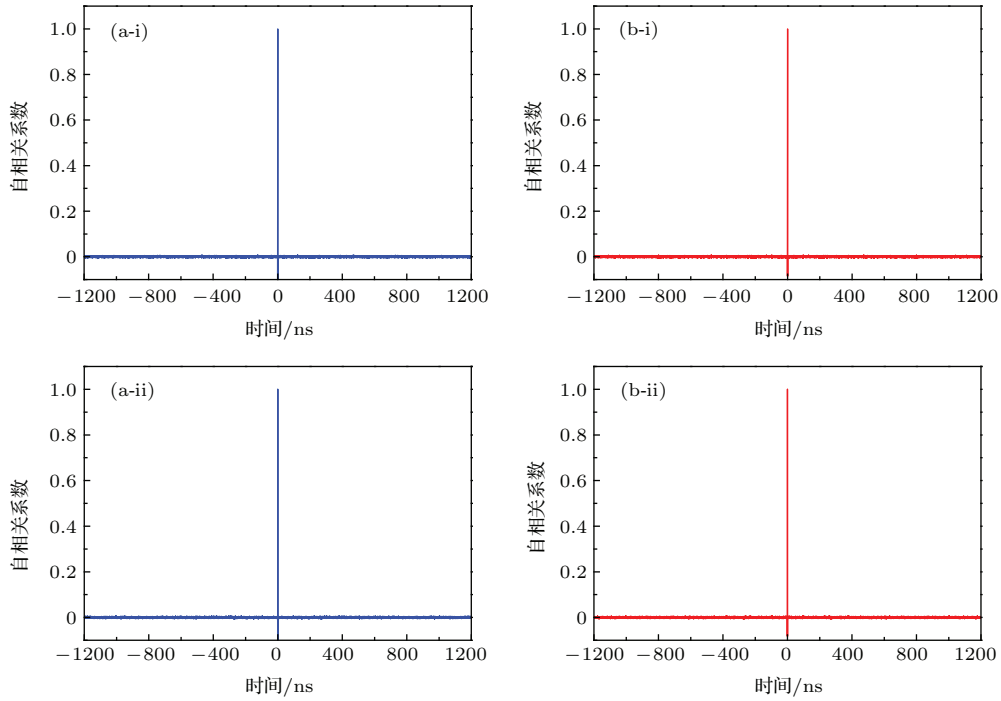

图5 (网刊彩色) 光采样周期与混沌弱周期不成比例时, 采样前原始混沌信号和采样后混沌脉冲峰值的自相关曲线 (a-i), (b-i) 光采样率为5 GS/s; (a-ii), (b-ii) 光采样率为5.100145 GS/s

Fig. 5. (color online) Autocorrelation curve of original chaotic signal before sampling and chaotic pulse peaks after sampling: (a-i), (b-i) The optical sampling rate is 5 GS/s; (a-ii), (b-ii) the optical sampling rate is 5.100145 GS/s.

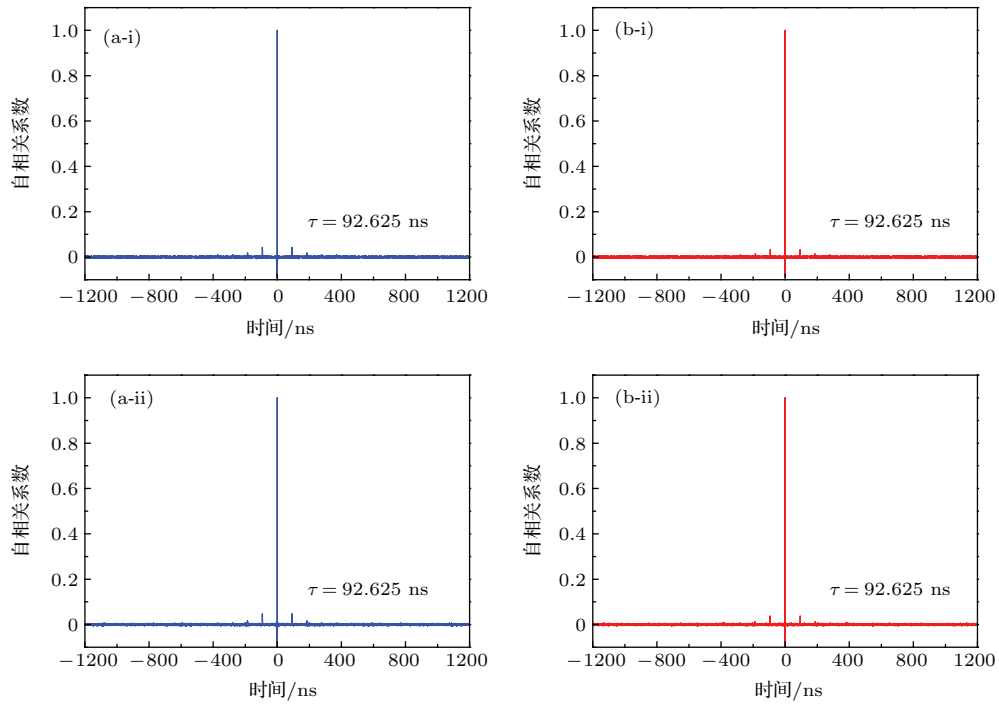

图 6 (网刊彩色) 光采样周期与混沌周期不成比例时, 采样前原始混沌信号和采样后混沌脉冲峰值的自相关曲线 (a-i), (b-i) 光采样率为 5.031039 GS/s; (a-ii), (b-ii) 光采样率为 5.117409 GS/s

Fig. 6. (color online) Autocorrelation curve of original chaotic signal before sampling and chaotic pulse peaks after sampling: (a-i), (b-i) The optical sampling rate is 5.031039 GS/s; (a-ii), (b-ii) the optical sampling rate is 5.117409 GS/s.

表 1 光采样率分别为 5 GS/s 和 5.333333 GS/s 时, 采样点的第 5 位最低有效位 (LSB) 的 NIST SP 800-22 测试结果, 测试数据样本为 1000 × 1 Mbit, 显著水平为 0.01, 成功通过测试时, 均匀性 P-value 值应大于 0.0001, 通过率应大于 0.9805608

Table 1. Typical results of statistical test suite NIST SP 800-22 for two sets of 1000 samples of 1 Mbit generated using the 5th LSB, separately from the optical sampling rate of 5 GS/s and 5.333333 GS/s. The significant level is 0.01. For successful pass, the P-value of the uniformity should be larger than 0.0001, and the proportion should be larger than 0.9805608.

NIST terms	5.333333 GS/s			5 GS/s		
	P-value	Proportion	Result	P-value	Proportion	Result
Frequency	0.119508	0.9810	Success	0.514582	0.9850	Success
Block Frequency	0.347257	0.9910	Success	0.004629	0.9940	Success
Cumulative Sums	0.000000	0.9800	Failure	0.357852	0.9900	Success
Runs	0.000000	0.9930	Failure	0.637119	0.9950	Success
Longest Run	0.779188	0.9880	Success	0.678686	0.9930	Success
Rank	0.610070	0.9960	Success	0.419021	0.9860	Success
FFT	0.000000	0.9700	Failure	0.002043	0.9870	Success
Non Overlapping Template	0.595549	0.9900	Success	0.670396	0.9880	Success
Overlapping Template	0.616305	0.9890	Success	0.137282	0.9920	Success
Universal	0.422325	0.9920	Success	0.123755	0.9870	Success
Approximate Entropy	0.000000	0.9680	Failure	0.471146	0.9930	Success
Random Excursions	0.771666	0.9816	Success	0.385864	0.9917	Success
Random Excursions Variant	0.354617	0.9857	Success	0.462674	0.9883	Success
Serial	0.096578	0.9920	Success	0.138069	0.9900	Success
Linear Complexity	0.531490	0.9900	Success	0.043567	0.9890	Success

为了进一步探究混沌激光采样过程中光采样率对产生随机数质量的影响, 我们利用8位ADC直接选取最低有效位(LSB)的方式从混沌脉冲信号中提取随机码, 然后对其进行NIST测试. 具体讲, 每个混沌脉冲峰值处幅值经过8位ADC后会被编码为8位二进制数, 我们将提取第5位LSB进行NIST测试, 其结果如表1所示. 右列浅红色和左列浅蓝色背景标注的分别为光采样率为5 GS/s和5.333333 GS/s时的测试结果. 每组光采样率下, 测试均采用了1000 × 1 Mbit数据点样本. NIST测试包括15项子测试, 显著水平为0.01时, 每个子测试的均匀性P-value值应大于0.0001, 每个子测试的样本通过率应大于0.9805608, 每个子测试均通过, 就说明NIST测试通过. 从表中可以看到, 光采样率为5.333333 GS/s时, 测试无法全部通过, 而光采样率为5 GS/s时, 测试全部通过. 其原因在于光采样为5.333333 GS/s时, 光采样间隔为0.1875 ns, 而混沌周期为92.625 ns, 光采样周期与混沌周期恰好成整数倍(92.625/0.1875 = 494), 这些采样点的自相关曲线具有明显的旁瓣, 致使提取的随机码遗传了原始混沌信号的弱周期性, 因此无法通过测试.

4 结 论

利用偏振无关的SOA构建TOAD全光采样门, 锁模光纤激光器作为光时钟, 对混沌激光采样进行了原理性实验论证, 实现了对光反馈半导体激光器产生的6.4 GHz带宽的混沌激光5 GSa/s的低功耗、实时光采样. 从同步采样前、后时序上对比分析了混沌激光的采样性能. 另外, 面向全光物理随机数发生器, 实验进一步分析了混沌激光实时光采样过程中光采样率对产生随机数质量的影响. 分析表明, 光采样周期与混沌的弱周期成比例时, 提取的随机数无法完全通过NIST标准测试; 当光采样周期与混沌周期不成比例时, 提取的随机数则可以完全通过. 因此, 我们在面向全光物理随机数发生器的混沌激光实时光采样过程中, 选择光采样速率时应该避免与混沌的弱周期成比例, 这对提取随机数至关重要.

参考文献

[1] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656

[2] Wang L, Ma H Q, Li S, Wei K J 2013 *Acta Phys. Sin.* **62** 100303 (in Chinese) [汪龙, 马海强, 李申, 韦克金 2013 物理学报 **62** 100303]

[3] Peng Z P, Wang C H, Lin Y, Luo X W 2014 *Acta Phys. Sin.* **63** 240506 (in Chinese) [彭再平王春华林愿骆小文 2014 物理学报 **63** 240506]

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

[5] Xiang S Y, Pan W, Luo B, Yan L S, Zou X H, Li N Q, Zhu H N 2012 *IEEE J. Quantum Electron.* **48** 1069

[6] Zhong Z Q, Wu Z M, Wu J G, Xia G Q 2013 *IEEE Photonics J.* **5** 1500409

[7] Zhao Q C, Yin H X 2013 *Laser Optoelectron. Prog.* **50** 23 (in Chinese) [赵清春, 殷洪玺 2013 激光与光电子学进展 **50** 23]

[8] Li P, Wang Y C 2014 *Laser Optoelectron. Prog.* **51** 06002 (in Chinese) [李璞, 王云才 2014 激光与光电子学进展 **51** 06002]

[9] Yang H B, Wu Z M, Tang X, Wu J G, Xia G Q 2015 *Acta Phys. Sin.* **64** 084204 (in Chinese) [杨海波, 吴正茂, 唐曦, 吴加贵, 夏光琼 2015 物理学报 **64** 084204]

[10] Wang Y C, Tang J H, Zhang M J 2007 CN200710062140.1 (in Chinese) [王云才, 汤君华, 张明江 2007 中国发明专利 CN200710062140.1]

[11] 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 *Nat. Photonics* **2** 728

[12] Wang A B, Li P, Zhang J G, Zhang J Z, Li L, Wang Y C 2013 *Opt. Express* **21** 20452

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

[14] Argyris A, Deligiannidis S, Pikasis E, Bogris A, Syvridis D 2010 *Opt. Express* **18** 18763

[15] Oliver N, Soriano M C, Sukow D W, Fischer I 2013 *IEEE J. Quantum Electron.* **49** 910

[16] Akizawa Y, Yamazaki T, Uchida A, Harayama T, Sunada S, Arai K, Yoshimura K, Davis P2012 *IEEE Photonics Technol. Lett.* **24** 1042

[17] Nguimdo R M, Verschaffelt G, Danckaert J, Leijtens X, Bolk J, Van der Sande G 2012 *Opt. Express* **20** 28603

[18] Li X Z, Chan S C 2013 *IEEE J. Quantum Electron.* **49** 829

[19] Li N, Pan W, Xiang S, Zhao Q, Zhang L 2014 *IEEE Photonics Technol. Lett.* **26** 1886

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

[21] Li P, Wang Y C, Wang A B, Yang L Z, Zhang M J, Zhang J Z 2012 *Opt. Express* **20** 4297

[22] Oda S, Maruta A, Kitayama K 2004 *IEEE Photonics Technol. Lett.* **16** 587

[23] Westlund M, Andrekson P A, Sunnerud H, Hansryd J, Li J 2005 *J. Lightwave Technol.* **23** 2012

[24] Li J, Westlund M, Sunnerud H, Olsson B, Karlsson M, Andrekson P A 2004 *IEEE Photon. Technol. Lett.* **16** 566

[25] Jolly A, Granier C 2008 *Opt. Commun.* **281** 3861

[26] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E http://csrc-nist. gov/groups/ST/toolkit/rng/ documentation_software.html [2015-6-12]

Study on real-time optical sampling of chaotic laser for all-optical physical random number generator*

Li Pu Jiang Lei Sun Yuan-Yuan Zhang Jian-Guo Wang Yun-Cai†

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

(*Institute of Optoelectronic Engineering, College of Physics & Optoelectronics, Taiyuan University of Technology, Taiyuan 030024, China*)

(Received 18 June 2015; revised manuscript received 13 August 2015)

Abstract

Absolutely secure communication should be implemented only through the 'one-time pad' proposed by Shannon, requires that physical random numbers with rates matched with the associated communication systems be used as secret keys. With the wide application of the WDM technology in optical communication, the single channel rate of the current digital communication system has exceeded 10 Gb/s and developed towards 100 Gb/s. To ensure the absolute security of such a large capacity communication, a large number of real-time, and secure random numbers are needed.

Secure random numbers are commonly produced through utilizing physical random phenomena, called physical random number generators. However, conventional physical random number generators are limited by the low bandwidth of the applied entropy sources such as thermal noise, photon-counting and chaotic electrical circuits, and thus have typical low bit rates of the order of Mb/s.

In recent years, chaotic lasers attracted wide attention due to their generation of secure, reliable and high-speed random number sequences, and so due to their coherent merits such as high bandwidth, large amplitude fluctuation and ease of integration. There have been lots of schemes based on laser chaos for high-speed random number generation, but most of them execute the random number extractions from the associated laser chaos in the electrical domain and thus their generation rates are faced with the well-known 'electrical bottleneck'. On the other hand, all-optical random number generation (AO-RNG) methods are all signal processes in the optical domain, so they can efficiently overcome this rate limitation and have a great potential in generating ultrafast random numbers of several dozens or hundreds of Gb/s. However, there is no experimental report on its realization of AO-RNG. One of the obstacles in the way for the AO-RNG achievement is to implement the fast and real-time all-optical sampling of the entropy signals (i.e., laser chaos).

In this paper, we present a principal experimental demonstration of the feasibility in the all-optical sampling of the chaotic light signal through constructing a TOAD-based all-optical sampler with a polarization-independent semiconductor optical amplifier (SOA). Specifically, we experimentally generate chaotic laser signals using an optical feedback semiconductor laser and finally complete a 5 GSa/s real-time and high-fidelity all-optical sampling of the

* Project supported by the Special Fund For Basic Research on Scientific Instruments of the National Natural Science Foundation of China (Grant No. 61227016), the Young Scientists Fund of the National Natural Science Foundation of China (Grant Nos. 61205142, 51404165), and the Natural Science Foundation of Shanxi Province, China (Grant No. 2015021088).

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

chaotic laser with a bandwidth of 6.4 GHz. Further experimental results show that whether the optical sampling period is proportional to the external cavity feedback time or not has a great effect on the weak periodic suppression of the chaotic signal: only when both of them are out of proportion, can the weak periodicity of the original chaotic signal be effectively eliminated; and this is favorable for the generation of high-quality physical random numbers. To the best of our knowledge, it is the first time to realize all-optical sampling of chaotic signal in experiments.

Keywords: chaotic laser, random numbers, optical sampling, terahertz optical asymmetric demultiplexer

PACS: 05.45.Jn, 05.45.Gg **DOI:** 10.7498/aps.64.230502