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

利用混沌激光脉冲在线实时产生 7 Gbit/s 物理随机数

赵东亮 李璞 刘香莲 郭晓敏 郭龑强 张建国 王云才

Online real-time 7 Gbit/s physical random number generation utilizing chaotic laser pulses

Zhao Dong-Liang Li Pu Liu Xiang-Lian Guo Xiao-Min Guo Yan-Qiang Zhang Jian-Guo Wang Yun-Cai

引用信息 Citation: Acta Physica Sinica, 66, 050501 (2017) DOI: 10.7498/aps.66.050501
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.050501
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I5

利用混沌激光脉冲在线实时产生7 Gbit/s物理随机数*

赵东亮[1)2)] 李璞[1)2)†] 刘香莲[1)2)] 郭晓敏[1)2)] 郭龑强[1)2)]
张建国[1)2)] 王云才[1)2)]

1) (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)

2) (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)

(2016 年 9 月 30 日收到; 2016 年 12 月 2 日收到修改稿)

提出了一种基于混沌激光的在线实时产生高速物理随机数的方法, 通过对连续的混沌激光进行光采样得到离散的混沌激光脉冲序列, 利用差分比较器对混沌脉冲序列进行自延迟比较, 在线实时输出高速物理随机数. 并以光反馈半导体激光器这一典型混沌激光产生装置作为物理熵源, 对所提方法进行了原理性实验论证, 实现了实时速率为7 Gbit/s 的物理随机数在线产生, 可成功通过随机数行业测试标准 (NIST SP 800-22).

关键词: 混沌激光, 物理随机数, 光采样, 延时比较

PACS: 05.45.Vx, 05.45.Gg **DOI:** 10.7498/aps.66.050501

1 引 言

随机数在保密通信领域有着重要应用, 常被用作密钥对明文信息进行加密. 根据香农 (Shannon) 的“一次一密”理论 [1], 为保证通信的绝对安全就要产生大量码率不低于通信速率的随机数, 且必须保证随机数是不可预测的.

利用复杂算法可产生高速“伪”随机数, 但它具有周期性, 长度有限, 存在极大安全隐患 [2]. 采用自然界随机现象作为物理熵源, 可产生无限长度、不可预测的物理随机数 (又称真随机数), 但受限于传统熵源 (如热噪声 [3]、振荡器抖动 [4] 等) 带宽, 码率多处于 Mbit/s 量级, 距离现代通信速率有很大差距.

鉴于此, 采用宽带光子熵源——混沌激光 [5−9]——产生高速物理随机数在近年来获得了广泛关注. 例如, 日本埼玉大学 Uchida 等 [10] 利用两路光反馈半导体激光器产生互不相关的混沌激光, 经由 1 位模数转换器 (ADC) 和异或门处理, 实现了实时速率达 1.7 Gbit/s 的物理随机数产生. 但是, 该方法需不断调节 ADC 的判决阈值, 以使产生的随机数统计无偏, 从而可通过随机数行业测试标准. Wang 等 [11] 也利用 1 位 ADC 和异或门构建出了实时速率可达 4.5 Gbit/s 物理随机数产生装置. 此外, 相关研究学者还陆续提出了多种利用多位 ADC 和复杂后续处理相结合的物理随机数产生方案. 例如, 以色列巴伊兰大学 Reidler 等 [12] 利用 8 位 ADC 对光反馈半导体激光器产生的混沌激光进行采集, 离线证明了等效速率为 12.5 Gbit/s 的随机数可行性. 西南大学唐曦等 [13] 以互注入半导体激光器作为熵源, 将 8 位 ADC 与离线逻辑异或处理和舍弃最高有效位操作相结合产生了速率为 17.5 Gbit/s 的随机数. 最近, 西南交通大学 Li 等 [14] 使用 8 位

* 国家自然科学基金科学仪器基础研究专款项目 (批准号: 61227016)、国家自然科学基金 (批准号: 61505137, 61405138, 51404165)、国家国际科技合作专项 (批准号: 2014DFA50870)、山西省自然科学基金 (批准号: 2015021088) 和山西省高等学校科技创新项目 (批准号: 2015122) 资助的课题.

† 通信作者. E-mail: lipu@tyut.edu.cn

ADC和离线高阶有限差分算法证实了利用光反馈混沌激光半导体激光器可产生速率为2.2 Tbit/s的随机数. 然而, 这些基于多位ADC的方案均是利用示波器将混沌信号波形存储后进行的离线处理, 并未能实时在线产生随机数.

限制高速率“实时”随机数产生的核心技术问题在于: 现有技术均使用电ADC(由采样-保持电路、比较器和触发器三部分构成)对熵源信号进行采样和量化, 继而进行后续处理. 但是, 电时钟的孔径抖动限制了ADC的处理速度. 并对ADC及后续处理涉及器件(如异或门、移位寄存器等)之间的同步提出了严峻挑战.

本文中, 使用锁模光脉冲在光域中对混沌激光进行采样, 通过差分比较器对采样得到的混沌激光脉冲序列进行自延迟比较, 实现了实时物理随机数的高速产生. 该方法的整个信号处理过程无须电时钟和后续处理器件参与, 亦避免了判决阈值需不断调谐的技术局限. 并以光反馈半导体激光器这一典型混沌激光产生装置作为物理熵源, 对上述方法进行了原理性实验论证, 在线产生了实时速率为7 Gbit/s的物理随机数. 该随机数产生速率主要受限于所用混沌信号的带宽, 若采用更高带宽的混沌激光, 产生速率有望获得进一步提高.

2 实验装置

基于混沌激光在线实时产生物理随机数的装置如图1所示. 混沌激光脉冲源(chaotic laser pulse source)输出混沌激光脉冲序列, 经脉冲光放大器(PEDFA), 由50 : 50光耦合器等分为两路. 这两路混沌光脉冲由各自对应的光电探测器(PD)转化为电信号后, 分别接入差分比较器(COM)的“+”, “−”输入端. 其中, 在差分比较器的“+”输入端的光电探测器前端置入一可调谐光延迟线(ODL), 使进入差分比较器的两路脉冲之间存在一合适的延迟时间. 当“+”输入端的混沌脉冲幅值与相应“−”输入端的脉冲幅值的差值大于零时, 比较器输出高电平(编码为“1”); 反之, 比较器输出低电平(编码为“0”). 从而实现了对混沌脉冲信号的自延迟比较, 这些随机出现的高、低电平, 即为最终的实时物理随机数序列.

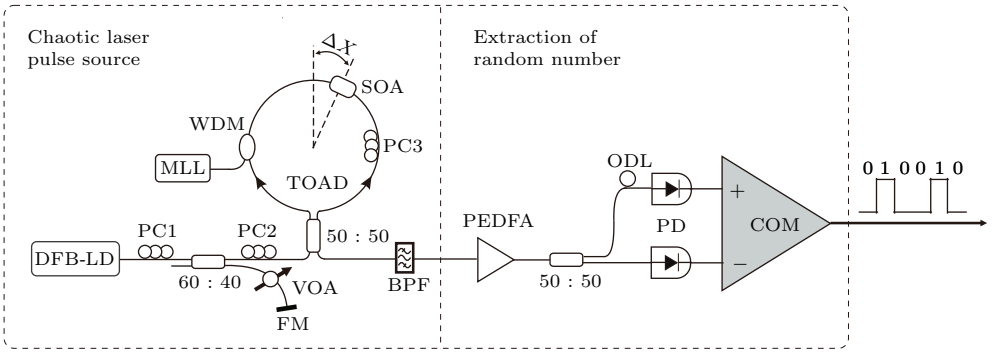

图1 在线实时产生物理随机数装置图 DFB-LD, 半导体激光器; PC1, PC2, PC3, 偏振控制器; VOA, 可调光衰减器; FM, 光纤反射镜; MLL, 锁模脉冲激光器; WDM, 波分复用器; SOA, 半导体光放大器; BPF, 光带通滤波器; PEDFA, 脉冲光放大器; ODL, 可调谐光延迟线; PD, 光电探测器; COM, 差分比较器

Fig. 1. Schematic for online real-time physical random number generation. DFB-LD, distribute feedback laser diode; PC1, PC2, PC3, polarization controllers; VOA, variable optical attenuator; FM, fiber mirror; MLL, mode-locked laser; WDM, wavelength division multiplexer coupler; SOA, semiconductor optical amplifier; BPF, optical bandpass filter; PEDFA, Pulse optical amplifier; ODL, optical delay line; PD, photodetector; COM, differential comparator.

混沌激光脉冲源(chaotic laser pulse source)是通过对混沌激光进行全光采样实现的. 具体地, 半导体激光器(DFB-LD)输出的激光通过60 : 40的光纤耦合器分为两路, 其中40%的一路由光纤反射镜(FM)反馈回半导体激光器中. 通过可调光衰减器(VOA)和偏振控制器(PC)调节反馈光强度和偏振状态, 可使DFB-LD进入混沌振荡. 所产生的混沌激光由上述光纤耦合器的60%端口输出, 进入全光采样门, 该采样门是在光纤环中非对称地放置一个非线性半导体光放大器(SOA)构成的太赫兹光非对称解复用器(TOAD)结构[15,16]. 混沌激光作为信号光经50 : 50光纤耦合器进入TOAD环,

分别沿着顺时针 (CW) 和逆时针 (CCW) 方向传输. 与此同时, 锁模脉冲激光器 (MLL) 输出的锁模光脉冲作为控制光, 经波分复用器 (WDM) 耦合进入TOAD环. 当有控制光脉冲到达SOA时, 会使SOA的非线性系数发生改变. 由于SOA偏离环中心点位置Δx, 此时先后进入SOA的CW和CCW两路信号光会经历不同的相位调制, 产生相位差. 选择合适的控制光功率, 调节偏振控制器PC2和PC3可使该相位差等于π, 两路信号光会在50 : 50光纤耦合器另一输出端干涉输出. 这样, 信号光 (即混沌激光) 随着超短光脉冲的到来而周期性地输出, 从而实现了对混沌激光的全光采样. 最终, 采样得到的混沌激光脉冲通过带通滤波器 (BPF) 滤出.

3 实验结果

3.1 混沌激光脉冲源特性

图2 (a) 为利用频谱分析仪 (signal and spectrum analyzer, Rohde & Schwarz, FSW26) 实验测得的混沌激光的频谱, 而图2 (b) 为混沌激光的时序图. 实验中, 光反馈半导体激光器的偏置电流设置为37.4 mA, 中心波长为1554.13 nm. 调节可调光衰减器, 使反馈强度约为2.5%. 按照频谱能量计算[17], 此时混沌激光的带宽约7.5 GHz.

图2 (c) 为锁模脉冲激光器 (MLL) 发出的重复频率为7 GHz锁模光脉冲序列 (控制光) 波形图, 而图2 (d) 则是经光采样得到的混沌激光脉冲时序图. 实验中, SOA偏置电流设置为300 mA, 位于偏离环中心20 ps处. 锁模脉冲激光器发出的锁模光脉冲序列的重复频率为7 GHz, 平均功率为−7.2 dBm. 上述信号波形均是由80 GSa/s采样率和36 GHz带宽的示波器 (OSC, Lecroy, LabMaster10-36Zi) 记录所得. 通过对比图2 (b) 和图2 (d), 可以看出采样后得到的混沌脉冲序列的峰值包络与被采样信号完全一致. 这意味着利用锁模光脉冲在光域中实现了对混沌激光的高保真全光采样.

另外需要指出的是, 该混沌激光脉冲源不会遗传光反馈混沌激光固有的弱周期性[18]. 前期研究表明[19], 当光采样门的采样率低于混沌激光信号的带宽且采样周期不是外腔反馈时间的整数倍时, 混沌激光的弱周期性可以被抑制. 因此, 将光采样门的采样率设置为7 GSa/s (对应采样周期约为0.1428 ns), 对带宽为7.5 GHz的光反馈混沌激光进行采样. 连续混沌激光信号自相关特性曲线如图3 (a) 所示, 可以看出外腔反馈时间为103.8 ns, 与光采样周期不成整数倍关系. 图3 (b) 则是实验中获得的混沌脉冲信号幅值的自相关曲线, 可以看出, 与预期相符, 混沌脉冲信号不再表现出弱周期性, 这为下一步优质随机数提取创造了有利条件.

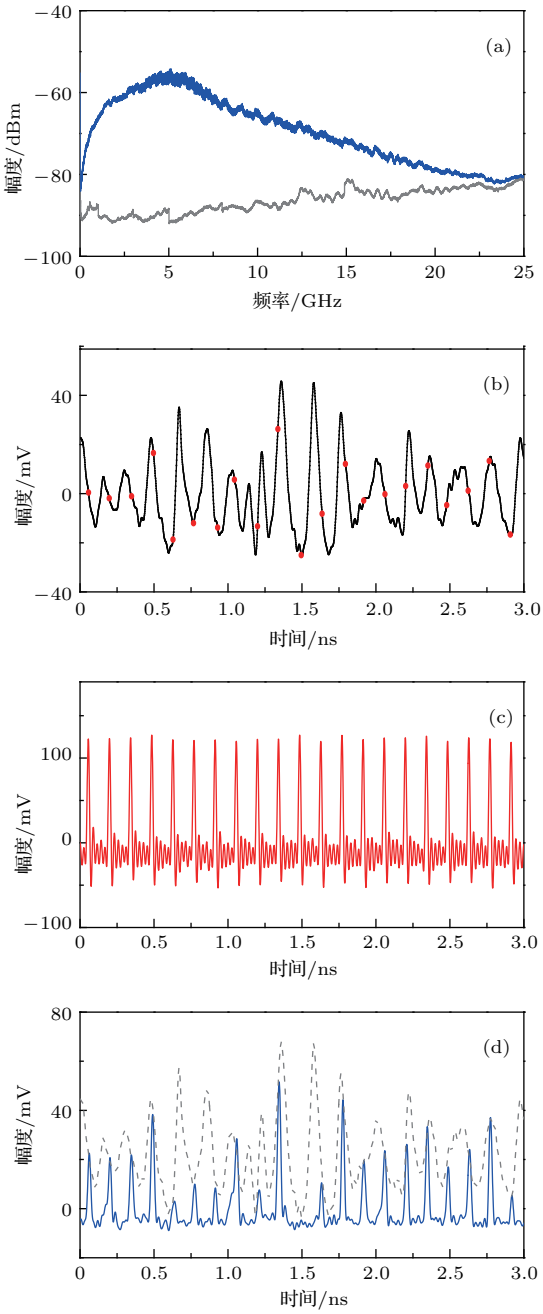

图2 混沌脉冲源的工作特性 (a) 混沌激光的频谱; (b) 混沌激光时序; (c) 控制光脉冲时序; (d) 混沌脉冲序列

Fig. 2. Characteristics of the chaotic laser pulse source: (a) Frequency spectrum of the optical feedback chaotic laser; (b) waveforms of the chaotic laser; (c) waveforms of the optical control pulses; (d) chaotic pulse sequences.

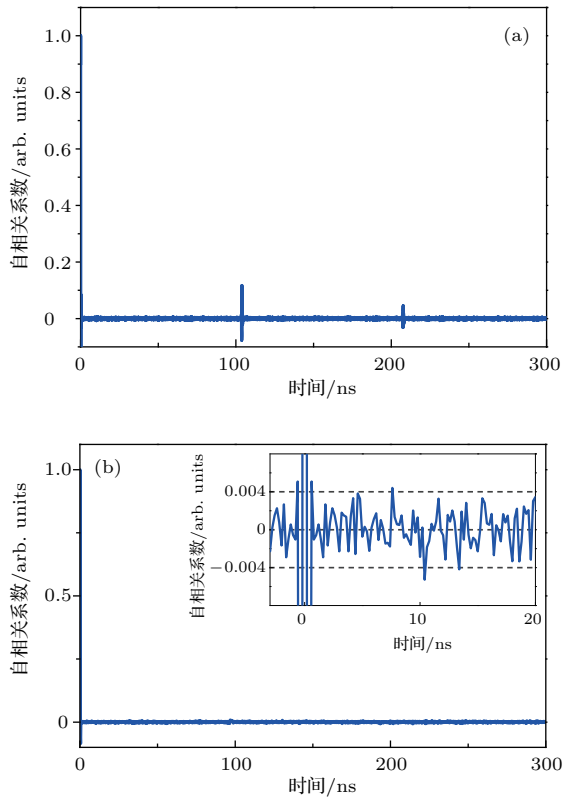

图 3 (a) 混沌激光的自相关特性曲线; (b) 混沌脉冲的自相关特性曲线

Fig. 3. (a) Autocorrelation curves of the optical feedback chaotic laser; (b) autocorrelation curves of the chaotic pulses.

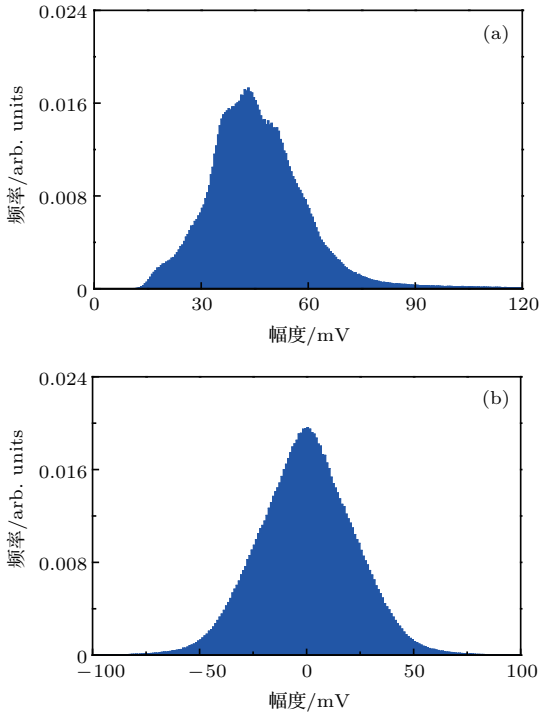

图 4 (a) 和 (b) 分别为作差运算前、后混沌激光脉冲峰值的幅值分布

Fig. 4. (a) and (b) are Normalized distributions of the peak amplitudes of chaotic pulses before and after the differential operation.

3.2 随机数实时提取

3.2.1 自延迟比较分析

混沌激光不对称的幅值分布是一个不利于产生优质随机数的因素. 图 4 (a) 为实验中混沌激光脉冲信号峰值的幅值概率密度分布曲线, 可以看出混沌脉冲信号的幅值概率分布呈现明显的不对称性. 这也是采用单一阈值进行比较提取随机数时 [10], 需要不断调谐才可产生统计无偏随机数的根本原因.

本方法中采用的自延迟比较技术, 是对输入到差分比较器的两路自延迟混沌脉冲进行作差运算, 从而确定随机数序列中的“0”和“1”码, 无须设置阈值即可获得统计无偏的优质随机数. 这个结论可以在理论上分析混沌脉冲作差运算前、后的幅值概率分布得到证明. 设输入到差分比较器的混沌脉冲信号 $s(t)$ 与其延迟信号 $s(t+\tau)$ 幅值概率密度函数分别是 $f(x)$ 和 $f(y)$, 联合概率密度函数是 $f(x,y)$. 混沌脉冲信号 $s(t)$ 与其延迟信号 $s(t+\tau)$ 作差后的信号用 $g(t)$ 表示, 于是有 $g(t)=s(t)-s(t+\tau)$. 它的幅值分布函数用 $F(z)$ 表示:

$$\begin{aligned} F(z) =& P(x-y<z) \\ =& \int_{-\infty}^{+\infty}\left[\int_{-\infty}^{z+y} f(x,y)\mathrm{d}x\right]\mathrm{d}y, \end{aligned} \tag{1}$$

做变量代换 $x=u+y$, 可得

$$\begin{aligned} F(z) =& \int_{-\infty}^{+\infty}\left[\int_{-\infty}^{z} f(u+y,y)\mathrm{d}u\right]\mathrm{d}y \\ =& \int_{-\infty}^{z}\left[\int_{-\infty}^{+\infty} f(u+y,y)\mathrm{d}y\right]\mathrm{d}u. \end{aligned} \tag{2}$$

对 (2) 式求导可得到幅值概率密度函数为

$$f_z(z)=\int_{-\infty}^{+\infty} f(z+y,y)\mathrm{d}y. \tag{3}$$

若 $s(t)$ 和 $s(t+\tau)$ 相互独立, 则有 $f(x,y)=f(x)f(y)$. 代入 (3) 式中可得

$$\begin{aligned} f_z(z) =& \int_{-\infty}^{+\infty} f(z+y,y)\mathrm{d}y \\ =& \int_{-\infty}^{+\infty} f(z+y)f(y)\mathrm{d}y, \end{aligned} \tag{4}$$

那么有

$$f_z(-z)=\int_{-\infty}^{+\infty} f(-z+y,y)\mathrm{d}y, \tag{5}$$

令 $v=-z+y$, 有

$$f_z(-z)=\int_{-\infty}^{+\infty} f(v,v+z)\mathrm{d}v$$
$$=\int_{-\infty}^{+\infty} f(v)f(v+z)\mathrm{d}v. \quad (6)$$

由 (4) 式和 (6) 式可以得到

$$f_z(z)=f_z(-z). \quad (7)$$

由 (7) 式可知, 经过延迟作差运算后的混沌脉冲信号的幅值概率密度函数服从对称分布, 为使用自延迟比较技术获得统计无偏的随机数提供了理论支持.

从上述理论分析中可以看出, 自延迟比较技术的前提是保证自延迟的两路混沌脉冲信号不相关. 根据图 3 (b) 的插图, 实验中选择了一个脉冲重复周期整数倍的延迟时间 0.714 ns. 在此延迟时间下, 混沌脉冲的自相关系数降低到 0.004 以下, 可以认为两路混沌脉冲信号是不相关的. 进一步, 我们对实验中的混沌脉冲序列峰值进行了延迟作差分析. 图 4 (b) 是延迟时间为 0.714 ns 时, 两路自延迟混沌脉冲信号作差运算后的幅值概率分布曲线. 通过对比图 4 (a) 和图 4 (b), 可以发现作差运算后的曲线呈现出高度对称的分布, 这就实验证实了采用自延迟比较技术确实可以消除混沌脉冲信号的幅值概率不对称分布, 从而获取统计无偏的随机数.

3.2.2 比较器输出结果

实验中基于自延迟比较技术的随机数提取 (extraction of random number) 实现过程如图 1 所示, 这里不再赘述. 图 5 (a) 为差分比较器 (ADI, HMC675LP3E) 输出的随机数时序图. 由图可见, 所产生的随机数序列属于非归零码 (NRZ). 进一步可以发现, 该随机数序列的实时速率由锁模脉冲激光器的重复频率直接决定, 为 7 Gbit/s, 峰峰值电压为 400 mV. 图 5 (b) 为差分比较器输出的随机数序列的自相关曲线. 可以看出随机数序列不包含任何混沌信号的时延特性. 图 5 (c) 为产生的随机数序列所转换成的二维黑白点图, 随机数序列中的 "0" 和 "1" 码分别对应随机点图中的白点和黑点. 点图中没有任何明显的图样, 说明随机数序列中 "0" 和 "1" 码的分布是均匀的.

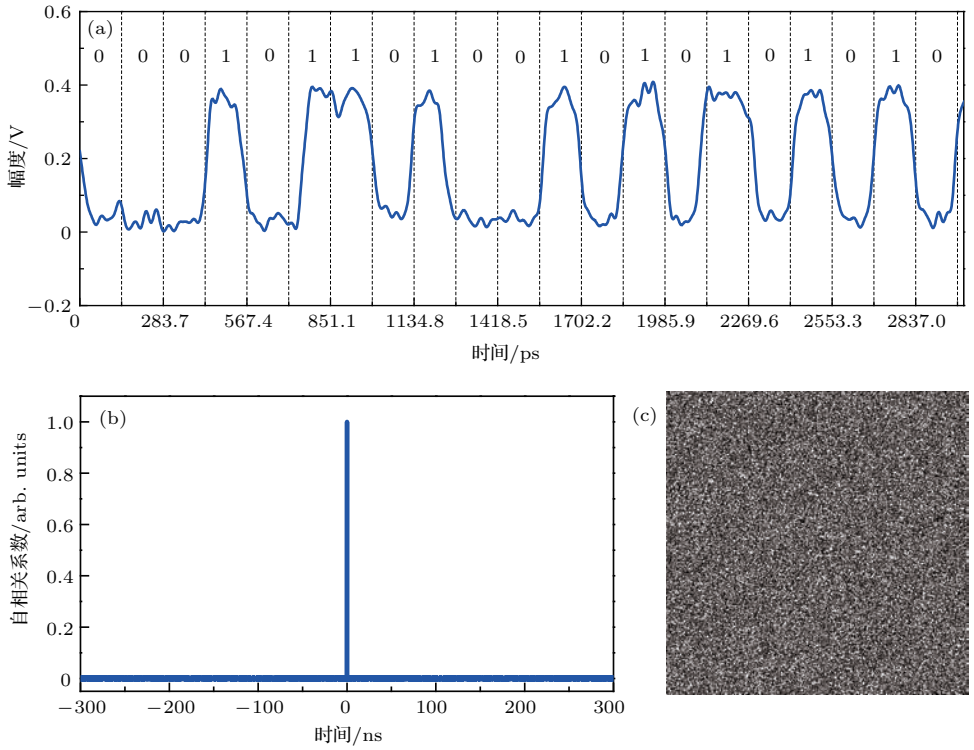

图 5 比较器输出的随机数序列的特性 (a) 时序图; (b) 自相关图; (c) 随机点图

Fig. 5. Characteristics of real-time output random bit sequences: (a) Waveforms of the random sequences; (b) autocorrelation curves of the random sequences; (c) a random dot diagram of the random sequences.

3.3 随机数测试结果分析

为了验证所获随机数的性能, 我们采用美国国家标准和技术研究所 (NIST) 提供的15项统计测试标准 (NIST SP800-22) [20], 对产生的随机数进行测试. NIST测试标准包含15项测试, 每项测试结果用 P 值来表示. 若 P 值大于显著水平 $\alpha = 0.01$, 则说明该随机数序列通过了相应的测试项. 进一步, 为了验证序列的随机特性的有效性及正确性, NIST测试标准要求在1000组1 Mbit的随机数数据测试中, 每项测试的通过率须大于0.9806. 图6是本实验所得随机数数据的测试结果. 其中, 图6 (a) 和图6 (b) 分别为每个子测试项对应的 P 值和通过率, 横坐标轴上的数字1—15代表NIST测试的15个测试项, 分别为频率、块内频数、累积和、游程、块内最长游程、矩阵秩、离散傅里叶变换、非重叠模块匹配、重叠模块匹配、通用统计、近似熵、随机游动、随机游动变量、串行和线性复杂度测试. 由图6可见, 所产生的随机数可通过NIST SP800-22中的全部15项测试.

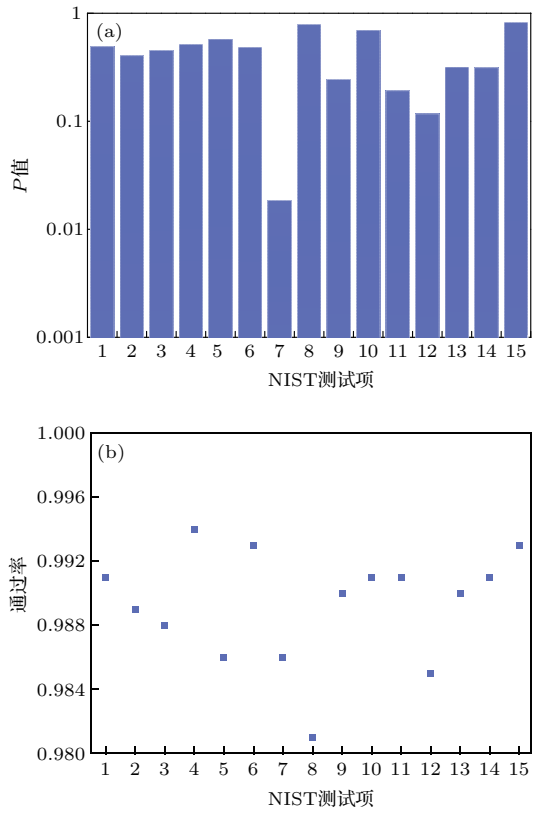

图6 NIST测试结果 (a) 各测试项的 P 值; (b) 各测试项的通过率

Fig. 6. Results of NIST statistical test: (a) P-value of each test item; (b) pass rate of each test item.

4 讨 论

本文图1中ODL的延迟量对随机数的质量有比较大的影响. 延迟量的选择取决于相应延迟量下混沌脉冲的自相关系数 [见图3 (b)]. 大量的实验发现, 当选取的延迟量对应的混沌脉冲自相关系数低于0.004时, 产生的随机数可通过NIST测试, 如图7所示. 本方案中, 选择了自相关系数为0.004时所对应的ODL延迟量0.714 ns.

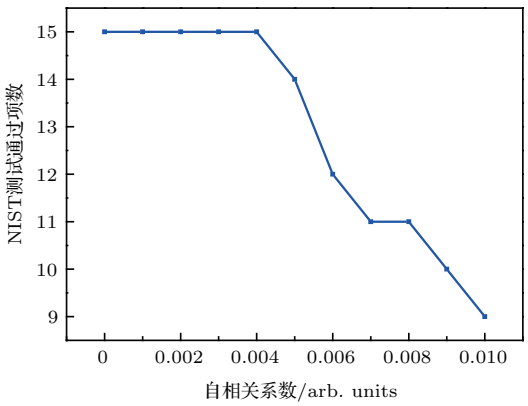

图7 不同的混沌脉冲自相关系数下, 通过NIST测试的项数变化情况

Fig. 7. The number of passed tests for NIST at different chaotic pulse autocorrelation coefficients.

在本文所述原理性论证实验中, 使用差分比较器对采样得到的混沌脉冲序列进行自延迟比较, 实时在线产生的物理随机码属于NRZ码. 若要产生RZ码, 只需要在差分比较器后添加一NRZ-RZ转换器即可. 目前市场上NRZ-RZ转换器的产品成熟, 比如, ADI公司生产的型号为HMC706的NRZ-RZ转换器, 速率可达13 Gbps.

5 结 论

本文提出了一种基于混沌激光的在线实时产生高速物理随机数的方法, 并对其进行了原理性实验论证. 利用锁模脉冲激光器产生的光脉冲作为控制光信号控制全光采样门, 实现了对光反馈半导体激光器产生的带宽为7.5 GHz的混沌激光的7 GSa/s实时全光采样, 有效抑制了光反馈混沌激光固有的弱周期性. 继而使用差分比较器对采样得到的重复频率为7 GHz的混沌脉冲序列进行自延迟比较, 消除了统计偏差的影响, 实时在线产生了码率为7 Gbit/s的物理随机数, 可以通过随机数行

业测试标准(NIST SP 800-22)中的全部15项测试. 该随机数产生速率主要受限于所用混沌信号的带宽, 若采用更高带宽的混沌激光, 有望获得进一步提高.

参考文献

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

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

[3] Xu P, Wong Y L, Horiuchi T K, Abshire P A 2006 *Electron. Lett.* **42** 1346

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

[5] Wang A B, Wang Y C, He H C 2008 *IEEE Photonics Technol. Lett.* **20** 1633

[6] Uchida A, Heil T, Liu Y, Davis P, Aida T 2003 *IEEE J. Quantum Electron.* **39** 1462

[7] Zhang M J, Liu T G, Wang A B, Zheng J Y, Meng L N, Zhang Z X, Wang Y C 2011 *Opt. Lett.* **36** 1008

[8] 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]

[9] Soriano M C, Garcíaojalvo J, Mirasso C R, Fischer I 2013 *Rev. Mod. Phys.* **85** 421

[10] 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

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

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

[13] Tang X, Wu J G, Xia G Q, Wu Z M 2011 *Acta Phys. Sin.* **60** 110509 (in Chinese) [唐曦, 吴加贵, 夏光琼, 吴正茂 2011 物理学报 **60** 110509]

[14] Li N Q, Kim B, Chizhevsky V N, Locquet A, Bloch M, Citrin D S, Pan W 2014 *Opt. Express* **22** 6634

[15] Jiang L, Li P, Zhang J Z, Sun Y Y, Hu B, Wang Y C 2015 *Acta Phys. Sin.* **64** 154213 (in Chinese) [江镭, 李璞, 张建忠, 孙媛媛, 胡兵, 王云才 2015 物理学报 **64** 154213]

[16] Li P, Jiang L, Zhang J G, Zhang J Z, Wang Y C 2015 *IEEE Photonics J.* **7** 7801108

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

[18] 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]

[19] Li P, Sun Y Y, Liu X L, Yi X G, Zhang J G, Guo X M, Guo Y Q, Wang Y C 2016 *Opt. Lett.* **41** 3347

[20] National Institute of Standard and Technology Special Publication 800-22 Revision1a, 2010 http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Online real-time 7 Gbit/s physical random number generation utilizing chaotic laser pulses*

Zhao Dong-Liang[1)2)] Li Pu[1)2)†] Liu Xiang-Lian[1)2)] Guo Xiao-Min[1)2)] Guo Yan-Qiang[1)2)]
Zhang Jian-Guo[1)2)] Wang Yun-Cai[1)2)]

1) (*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Eduction and Shanxi Province, Taiyuan University of Technology, Taiyuan 030024, China*)

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

(Received 30 September 2016; revised manuscript received 2 December 2016)

Abstract

Random numbers are used to encrypt the information in the field of secure communications. According to "one-time pad" theory found by Shannon, the absolute security of the high-speed communication requires the ultrafast reliable random numbers to be generated in real-time.

Using complex algorithms can generate pseudorandom numbers, but they can be predicted due to their periodicity. Random numbers based on physical stochastic phenomena (such as electronic noise, frequency jitter of oscillator) can provide reliable random numbers. However, their generation rates are at a level of Mbit/s typically, limited by the bandwidth of traditional physical sources.

In recent years, high-speed physical random number generation based on chaotic laser has attracted much attention. Common methods of extracting random numbers are to sample and quantitate the chaotic signal in electronic domain with a 1-bit or multi-bit analog-to-digital converter (ADC) triggered by an RF clock and then post-process the original binary sequences into random numbers. However, the large jitter of the RF clock severely restricts the speed of ADC. Moreover, the existence of the subsequent post-processing process put a huge challenge to how the synchronization is kept among all the devices (e.g., XOR gates, memory buffers, parallel serial converters) by using an RF clock. Thus, to our knowledge, the fastest real-time speed of the reported physical random number generator is less than 5 Gbit/s.

In this paper, we propose a novel method of generating the real-time physical random numbers by utilizing chaotic laser pulses. Through sampling the chaotic laser in all-optical domain by using a mode-locked pulsed laser, chaotic laser pulse sequences can be obtained. Then, real-time physical random numbers are obtained directly by self-delay comparing the chaotic pulse sequences with no need of RF clock nor any post-processing.

Furthermore, a proof-of-principle experiment is carried out, in which an optical feedback chaotic semiconductor laser is employed as an entropy source. Experimental results show that the real-time random number sequences at rates of up to 7 Gbit/s can be achieved. The real-time speed is mainly limited by the bandwidth of the applied chaotic signal. If the chaotic laser with a higher bandwidth is adopted, the real-time generation rate can be further enhanced.

Keywords: chaotic laser, physical random numbers, optical sampling, delay compare

PACS: 05.45.Vx, 05.45.Gg **DOI:** 10.7498/aps.66.050501

* Project supported by the Special Fund for Basic Research on Scientific Instruments of the National Natural Science Foundation of China (Grant No. 61227016), the National Natural Science Foundation of China (Grant Nos. 61505137, 61405138, 51404165), the Funds for International Cooperation and Exchange of the National Natural Science Foundation of China (Grant No. 2014DFA50870), the Natural Science Foundation of Shanxi Province, China (Grant No. 2015021088), and the Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi Province, China (Grant No. 2015122).

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