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

利用混沌激光多位量化实时产生 14 Gb/s 的物理随机数

王龙生 赵彤 王大铭 吴旦昱 周磊 武锦 刘新宇 王安帮

14-Gb/s physical random numbers generated in real time by using multi-bit quantization of chaotic laser

Wang Long-Sheng Zhao Tong Wang Da-Ming Wu Dan-Yu Zhou Lei Wu Jin Liu Xin-Yu Wang An-Bang

引用信息 Citation: Acta Physica Sinica, 66, 234205 (2017) DOI: 10.7498/aps.66.234205
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.234205
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I23

利用混沌激光多位量化实时产生14 Gb/s的物理随机数*

王龙生[1)2)] 赵彤[1)2)] 王大铭[1)2)] 吴旦昱[3)] 周磊[3)] 武锦[3)]
刘新宇[3)†] 王安帮[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)

3) (中国科学院微电子研究所微波器件与集成电路研究室, 北京 100029)

(2017 年 7 月 12 日收到; 2017 年 8 月 4 日收到修改稿)

提出了一种基于混沌激光多位量化的高速物理随机数实时产生方法. 利用外腔反馈混沌半导体激光器作为物理熵源, 通过时钟速率为7 GHz 的多位模数转换器对其采样量化, 生成6 位有效位的二进制随机比特, 然后利用现场可编程软件抽取低2位有效位的随机序列并进行自延迟异或处理, 获得了实时速率为14 Gb/s 的物理随机数. 该随机数具有良好的统计随机性, 可成功通过随机数行业测试标准 (NIST SP 800-22).

关键词: 半导体激光器, 混沌激光, 多位量化, 物理随机数

PACS: 42.55.Px, 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.66.234205

1 引 言

随机数在数值模拟、加密通信等领域具有重要的应用潜力[1,2]. 根据产生方式划分, 随机数可分为伪随机数与物理随机数两大类. 伪随机数基于固定的算法与种子产生, 实时速率可达数Gb/s量级, 但受限于周期性与可重复性等固有缺陷, 其随机性不甚理想. 物理随机数基于物理随机现象产生, 如电阻热噪声、振荡器频率啁啾等, 其随机性优良可靠[3,4]. 然而, 受限于信号带宽, 随机数的实时产生速率仅为Mb/s量级, 难以满足实际应用. 特别是面向信息安全领域, 高速物理随机数的实时产生显得尤为重要.

近年来, 光子宽带熵源, 如放大自发辐射、激光相位抖动以及混沌激光等被广泛用于生成高速物理随机数. 特别是混沌激光因其高带宽、大幅度等特性, 被用作新一代物理熵源以解决物理随机数实时生成速率不足的问题, 获得了国际、国内学者的广泛关注[5−8]. 例如, 日本Uchida 等[5]利用外腔反馈混沌半导体激光器作为熵源, 通过1位模数转换器(ADC) 量化与异或逻辑门(XOR) 处理之后, 实时产生了1.7 Gb/s的物理随机数; 随后, 该课题组利用光子集成外腔反馈半导体激光器作为熵源将产生速率提升至2.08 Gb/s[6]; Wang等[7]结合外腔反馈混沌半导体激光器与1位延迟差分比较以及异或处理, 将实时速率进一步提升至4.5 Gb/s; 此外, 赵东亮等[8]利用1位差分比较器对外腔反馈混沌激光的离散脉冲序列进行自延迟比较, 在线实时获得了7 Gb/s的物理随机数. 然而, 基于外腔反馈混沌激光1位量化的随机数产生速率也面临瓶颈问题, 主要原因是1位量化速率依赖于熵源带宽,

* 国家自然科学基金 (批准号: 61475111, 61671316)、山西省优秀青年自然科学基金 (批准号: 2015021004)、山西省国际科技合作项目 (批准号: 201603D421008) 和国际科技合作项目 (批准号: 2014DFA50870) 资助的课题.

† 通信作者. E-mail: xyliu@ime.ac.cn

‡ 通信作者. E-mail: wanganbang@tyut.edu.cn

而外腔反馈混沌半导体激光器的熵源带宽受弛豫振荡限制几乎达到极限[9]. 通过光注入、光拍频等方法[10−14]虽然可以增加混沌激光的带宽以提高1位量化的实时生成速率, 但速率上升空间有限, 同时会引入系统复杂、成本高昂的缺陷, 不利于实际应用.

更加有效的解决方法是利用多位ADC对混沌激光进行量化, 通过抽取多位有效位的随机数来成倍增加生成速率[15−25]. 例如, 以色列Reidler等[15]利用8位ADC对外腔反馈混沌激光量化, 经一阶求导后续处理之后, 通过抽取低5位有效位获得了12.5 Gb/s的物理随机数; 唐曦等[16]利用8位ADC对互注入混沌激光量化, 通过抽取低7位有效位并结合异或处理获得了速率为17.5 Gb/s的物理随机数; Kanter等[17]利用8位ADC对外腔反馈混沌激光量化, 经多阶求导后续处理之后, 通过抽取低15位有效位获得了速率为300 Gb/s的物理随机数. Li等[18]利用8位ADC对外腔反馈混沌激光量化, 经高阶有限差分后续处理之后, 通过抽取低55位有效位获得了速率为2.2 Tb/s物理随机数. 值得注意的是, 尽管上述多位量化抽取方案能够获得超高速物理随机数, 但均是通过示波器存储混沌信号波形后进行离线处理得到的, 并非在线实时产生, 在一定程度上限制了实际应用.

本文提出了一种基于混沌激光多位量化的高速物理随机数实时产生方法并进行了实验验证. 以外腔反馈混沌半导体激光器作为熵源, 通过时钟速率为7 GHz的6位ADC对其采样量化, 生成从最高位至最低位6位有效位的0, 1序列, 利用现场可编程软件(FPGA)抽取低2位有效位并进行自延迟异或处理, 最终获得了实时速率为14 Gb/s的物理随机数. 该随机数具有良好的统计随机性, 可成功通过随机数行业测试标准(NIST SP 800-22).

2 实验装置

基于混沌激光多位量化实时产生高速物理随机数的实验装置如图1所示. 半导体激光器(DFB)经偏振控制器(PC)之后进入50 : 50耦合器(FC)分成两路, 其中一路进入镜面(FM)构成的外腔, 经衰减器(VA)进行强度调节之后, 返回激光器扰动产生混沌激光. 混沌激光经另外一路光纤通道输出至光电探测器(PD), 转换为电信号, 该信号随后经时钟(Clock)与FPGA 控制下的6位ADC采样量化, 输出从最高位至最低位6位有效位的随机序列, FPGA抽取低2位有效位并进行自延迟异或处理, 最终获得了实时高速的物理随机数.

实验中, 半导体激光器(Eblana, EP1550-DM-B05-FM)阈值电流为13.68 mA, 电流源(ILX Lightwave, LDX-3412)调节激光器工作电流为34 mA, 温控源(ILX Lightwave, LDT-5412)调节激光器工作波长为1550.486 nm; 外腔反馈延迟为107.9 ns, 衰减器调节外腔反馈强度为总输出强度的−10.2 dB; 光电探测器(BPDV2120R)带宽为45 GHz; 多位ADC为自主研发, 由四个6位子ADC构成[26], 实验中利用其中一个6位子ADC进行采样量化, 采样频率为7 GHz, 由时钟(Agilent, E8257D)控制; FPGA(Virtex-7 XC7 VX690 T)对6位ADC进行实时同步控制并抽取低2位随机序列进行自延迟异或处理, 延迟长度为70 bit. 此外, 混沌激光的光谱、功率谱以及时序分别由光谱仪(YOKOGAWA, AQ6370C, 0.02 nm)、频谱仪(Agilent, N9030A, 43 GHz)以及示波器(LeCroy, SDA806Zi-A, 16 GHz, 40 GS/s)测量.

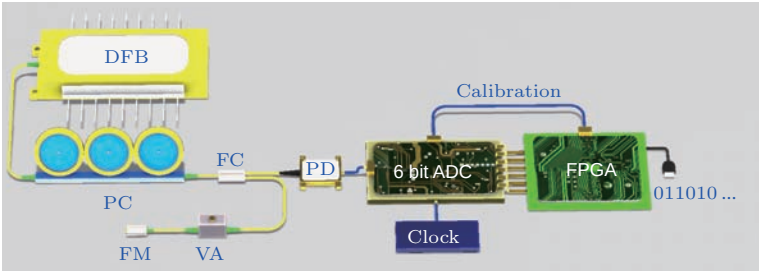

图1 基于混沌激光多位量化实时产生高速物理随机数的实验装置

Fig. 1. Experimental setup of real-time high-speed physical random number generation based on multi-bit quantization of laser chaos.

3 实验结果

3.1 混沌激光特性分析

图2 (a) 为混沌激光的功率谱 (黑线所示), 灰线为频谱仪的噪声基底, 按照功率谱能量80%计算[27], 混沌激光的带宽约为10 GHz, 大于实验中ADC的采样速率. 图2 (b) 为混沌激光的时序, 从时序可知, 外腔反馈半导体激光器输出具有高速的类噪声振荡, 且振荡幅度可达上百毫伏, 如此大幅度振荡有助于ADC的采样与量化. 图2 (c) 为混沌激光的幅值分布, 可以看出分布函数呈现明显的不对称, 其偏斜度为1.74, 该不对称性将导致0, 1 bit的比例不均衡, 降低随机数的随机性. 图2 (d) 为混沌激光的自相关曲线, 零峰处的相关系数迅速衰减至噪声基底附近, 而在外腔周期处 (107.9 ns) 又会出现另外一个相关峰, 该峰是由于外腔谐振导致, 称为时延特征[28]. 该特征将会导致混沌激光时域波形与之前的状态存在周期性的弱相关 (弱周期性), 恶化了生成随机数的随机性. 值得注意的是, 有效位抽取可在一定程度上削弱非对称幅值分布与时延特征带来的影响, 但通常需要结合其他后续处理, 如异或、求导以及比特反转等来彻底消除[29].

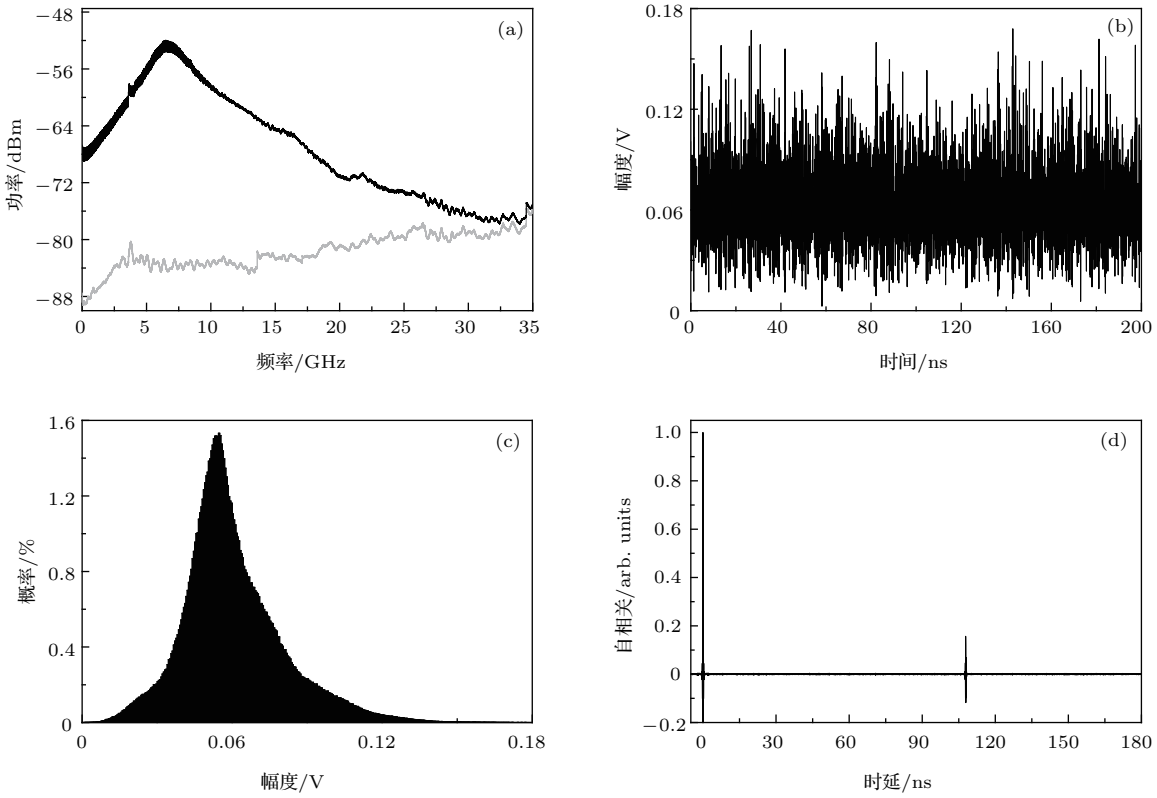

图2 混沌激光特性 (a) 功率谱; (b) 时序; (c) 幅值分布; (d) 自相关曲线

Fig. 2. Characteristics of laser chaos: (a) Power spectrum; (b) time series; (c) amplitude distribution; (d) autocorrelation trace.

3.2 随机数提取与测评

混沌激光经6位ADC采样量化之后生成多位有效位的随机比特, 通过FPGA抽取其中低2位并进行自延迟异或处理之后作为最终随机序列. 实验中得到的次低位 (2nd least significant bit 2nd LSB) 与最低位 (LSB) 随机比特的码型图与眼图分别如图3 (a) 与图3 (b) 所示. 由码型图可知, 随机码为非归零码, 7 bit位于1 ns之内, 表明1位有效位抽取时随机数的生成速率为7 Gb/s. 眼图张开良好, 眼图交叉点之间的间隔为143.4 ps (23.9×6), 等于一个码型宽度.

为了分析随机数的统计随机性, 定性研究了随机数经数模转换之后十进制波形的均衡性与相关性. 图4为低2位有效位随机数对应的十进制波形, 左侧纵轴为十进制水平 (0—3), 右侧纵轴为对应的

二进制水平(00—11), 十进制水平0代表二进制00, 十进制水平3代表二进制11; 其中二进制水平的左边一位代表2位有效位中的2nd LSB, 右边一位代表LSB.

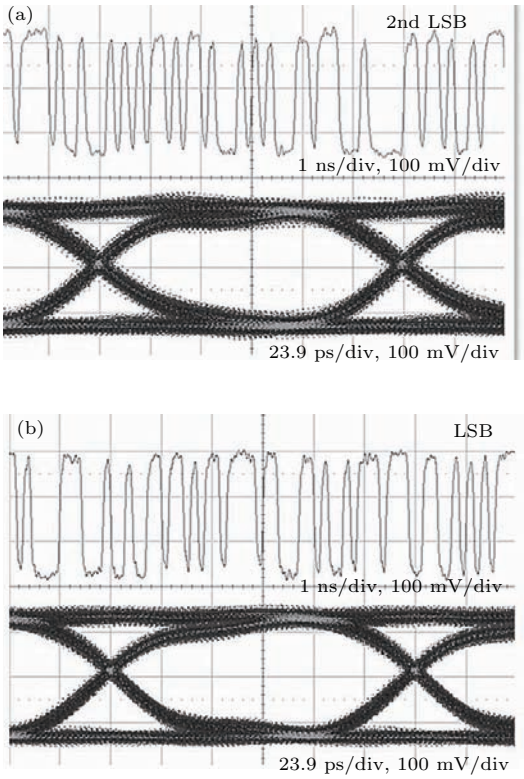

图3 随机比特的码型图与眼图 (a) 2nd LSB; (b) LSB

Fig. 3. Temporal waveforms and eye diagrams of random bits for (a) 2nd LSB and (b) LSB.

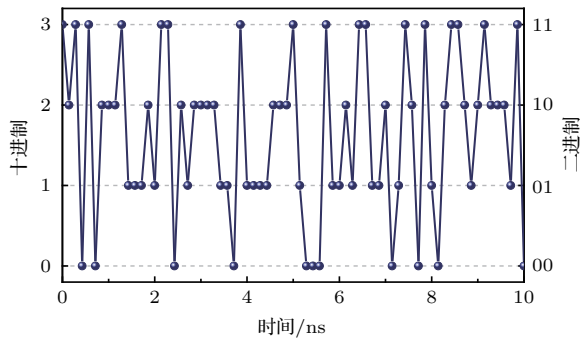

图4 低2位有效位随机数对应的十进制波形

Fig. 4. Decimal waveforms of binary sequence with 2LSBs.

图5 (a)与图5 (c)分别为异或处理之前十进制波形的幅值分布与自相关曲线, 图5 (b)与图5 (d)分别为异或处理之后十进制波形的幅值分布与自相关曲线. 如图5 (a)所示, 异或之前十进制波形的幅值分布呈现非均衡性, 主要体现在不同幅值的出现概率不同: 幅值2出现的概率明显高于其他幅值的出现概率; 异或之后, 如图5 (b)所示, 各个幅值的出现概率几乎相等, 有利于生成0, 1 bit均衡的物理随机数. 此外, 如图5 (c)所示, 异或之前十进制波形的自相关曲线在外腔周期处仍存在相关峰, 表明波形之间依然具有周期性的相关. 异或之后, 如图5 (d)所示, 该相关峰消失, 表明十进制波形得到了优化, 有利于生成随机性优良的物理随机数.

进一步定量研究了生成随机数的均衡性与相关性. 均衡性与相关性可分别通过计算0, 1 bit的偏斜函数$|e[N]|$与自相关函数$C[K]$来衡量, 定义如下:

$$e[N] = |\langle a[N]\rangle - 0.5|, \tag{1}$$

$$C[K] = \frac{\langle a[N]a[N+K]\rangle - \langle a[N]\rangle^2}{\langle a^2[N]\rangle - \langle a[N]\rangle^2}, \tag{2}$$

其中, $a[N]$, $a[N+K]$ 均为长度为N的0, 1随机序列, K为延迟比特的长度, $\langle\cdot\rangle$为统计平均运算. 对于一列有限长度的随机序列, 通常利用高斯统计分布估计$N[0, \sigma^2]$来评估其统计随机性. 对于高斯分布, 其偏斜函数$|e[N]|$的标准偏差σ_e和自相关函数$C[K]$的标准偏差σ_c分别为$(N^{-1/2})/2$和$N^{-1/2}$. 当$|e[N]|$和$C[K]$分别小于对应的三倍标准偏差, 即$3\sigma_e$与$3\sigma_c$, 随机序列可被认为是统计无偏和内部独立的[7].

图6 (a)为随机数异或前后偏斜函数的变化情况, 异或之前(绿色曲线所示), 在不同样本容量下(1—16 Mbits), 随机数偏斜量明显高于对应的三倍标准偏差(红色曲线)且基本保持不变. 相比之下, 异或之后(蓝色曲线所示), 不同样本容量随机数的偏斜量均小于对应的三倍标准偏差. 图6 (b)为16 Mbits随机数异或前后自相关函数的变化情况, 异或之前(绿色曲线所示), 随机数的相关系数高于对应的三倍标准偏差(红线所示), 更加明显的是, 在1511个延迟比特附近出现了大幅值的相关峰, 此峰是由外腔时延导致, 位置与外腔周期呈对应关系: 1511/14 = 107.9 ns. 对比之下, 异或之后随机数自相关系数(蓝色曲线所示)低于对应的三倍标准偏差. 以上结果表明, 本实验最终得到的由低2位有效位构成的随机序列是无偏且内部独立的.

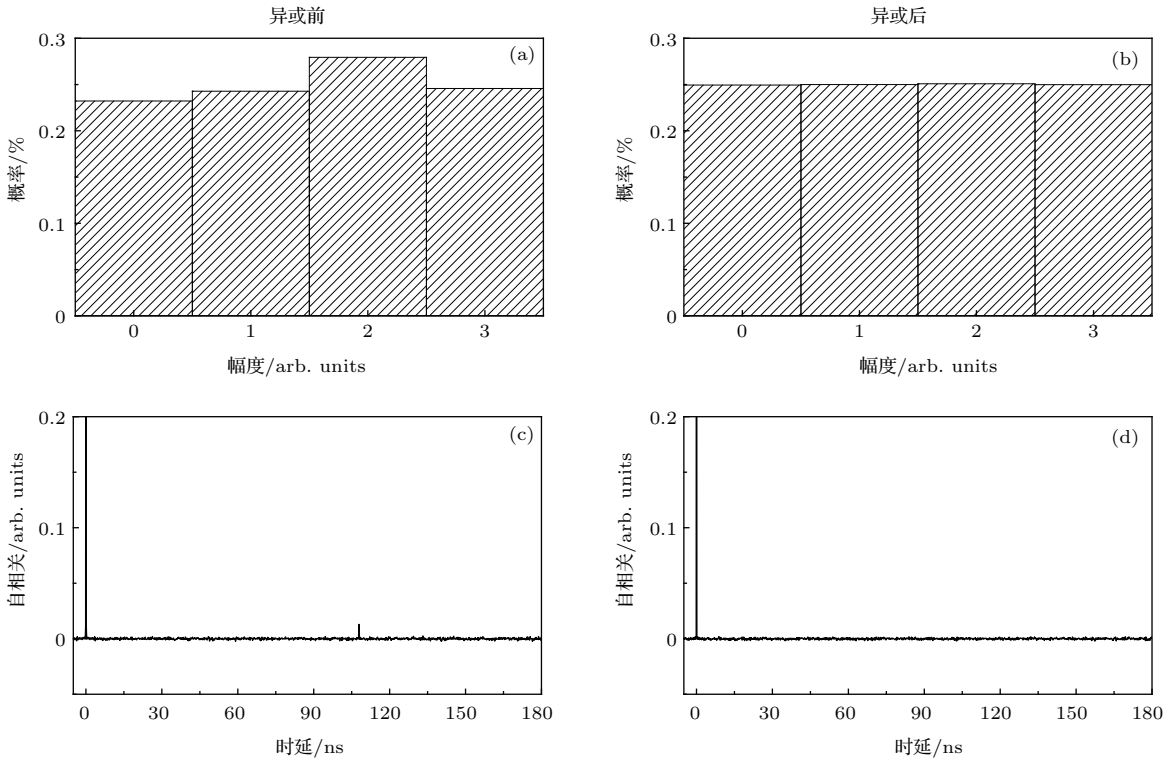

图 5 低 2 位随机数异或前后十进制波形的幅值分布与自相关曲线

Fig. 5. Amplitude distribution and autocorrelation trace of decimal waveforms of 2-LSBs random bits with and without XOR operation.

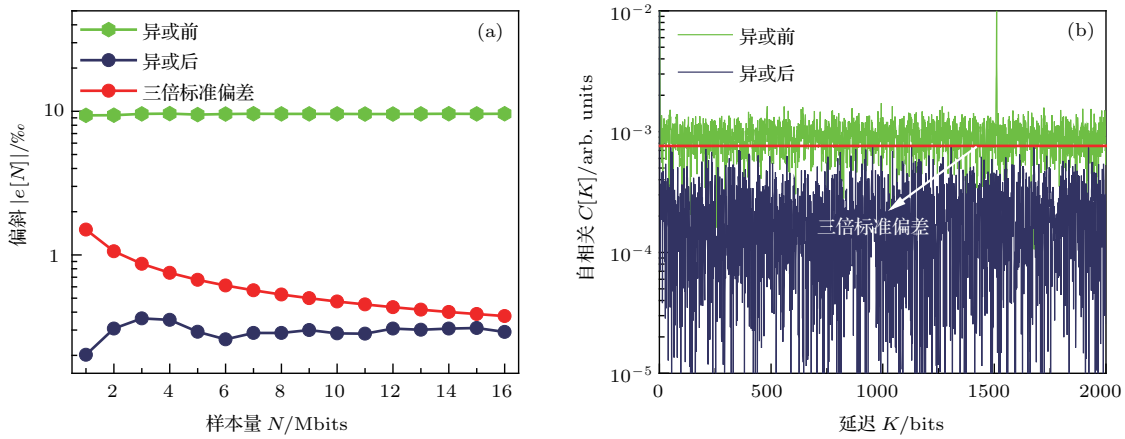

图 6 (网刊彩色) 低 2 位有效位随机数异或前后 0, 1 比特偏斜与独立性的定量评估 (a) 0, 1 偏斜 $|e[N]|$ 随样本量 N 的变化曲线; (b) 自相关函数 $C[K]$ 随延迟比特 K 的变化曲线

Fig. 6. (color online) Quantitative verification of bias and independence for 2-LSBs random bits with and without XOR operation: (a) Bias $|e[N]|$ as a function of sample size N; (b) autocorrelation function $C[K]$ as a function of delay bit K.

进一步采用国际行业测试标准 (NIST SP800-22) 对产生的随机数进行测试[30]. 该测试包含 15 个子测试项, 在显著水平大于 0.01 的基础上, 对 1000 组 1 Mbits 的随机数进行测试. 为了通过测试, 测试结果的一致性 (P 值) 应大于 0.0001, 且通过百分比在 0.99 ± 0.0094392 的范围之内. 表 1 为随机数的 NIST 测试结果, 对于具有多个 P 值和通过百分比的测试项, 本文只给出了最差的测试情况. 从测试结果来看, 该随机序列能够通过所有 15 项随机性测试, 说明其具有良好的统计随机性.

以上结果表明, 利用混沌激光多位量化可实时产生 14 Gb/s 的物理随机数. 我们也曾通过 1 位量

化实时产生了14 Gb/s的物理随机数[31], 其关键在于利用两个外腔半导体激光器的光外差来优化混沌激光的信号特征: 增加带宽与平坦度、改善幅值分布以及消除时延特征. 需注意, 1位量化速率主要依赖于混沌信号带宽, 在熵源带宽有限的条件下, 随机数的生成速率也受到了限制. 对比之下, 本方案仅需一个外腔半导体激光器作为生成随机数的信号源, 系统结构简单、操作灵活. 更加重要的是, 无需增加熵源信号带宽, 通过多位量化与有效位抽取便可成倍增加随机数的生成速率, 获得实时高速的物理随机数.

表1 NIST随机性测试结果

Table 1. Results of NIST statistical test.

统计测试指标	P值	百分比	结果
频率测试	0.370262	0.9950	通过
块内频率测试	0.867692	0.9900	通过
累加和测试	0.516113	0.9930	通过
游程测试	0.12962	0.9950	通过
块内长游程测试	0.106877	0.9880	通过
二进制矩阵秩测试	0.295391	0.9890	通过
离散傅里叶变换测试	0.092041	0.9840	通过
非重叠模块匹配测试	0.001276	0.9830	通过
重叠块比配测试	0.562591	0.9880	通过
全局通用统计测试	0.510153	0.9850	通过
近似熵测试	0.534146	0.9870	通过
随机游动测试	0.201925	0.9921	通过
随机游动变量测试	0.007276	0.9952	通过
串行测试	0.387264	0.9920	通过
线性复杂度测试	0.801865	0.9950	通过

4 结 论

提出了一种基于混沌激光多位量化的高速物理随机数的实时产生方法. 利用采样率为7 GHz的6位ADC对外腔混沌激光采样量化, 生成多位有效位的随机比特. 通过FPGA实时抽取低2位有效位并进行自延迟异或处理, 实验中获得了14 Gb/s的物理随机数. 该随机数具有良好的0, 1均衡比与内部独立性, 可通过国际行业标准测试(NIST SP800-22). 本项研究可为高速物理随机数的实时产生提供一种更加有效的解决途径, 促进物理随机数在信息安全领域的应用.

参考文献

[1] Metropolis N, Ulam S 1949 *J. Amer. Stat. Assoc.* **44** 335

[2] Zhao Q C, Yin H X 2013 *Optik* **124** 2161

[3] Petrie C S, Connelly J A 2000 *IEEE Trans. Circ. Syst. I: Fundam. Theory Appl.* **47** 615

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

[5] 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. Photon.* **2** 728

[6] Harayama T, Sunada S, Yoshimura K, Davis P, Tsuzuki K, Uchida A 2011 *Phys. Rev. A* **83** 031803

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

[8] Zhao D L, Li P, Liu X L, Guo X M, Guo Y Q, Zhang J G, Wang Y C 2017 *Acta Phys. Sin.* **66** 050501 (in Chinese) [赵东亮, 李璞, 刘香莲, 郭晓敏, 郭龑强, 张建国, 王云才 2017 物理学报 **66** 050501]

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

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

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

[12] Zhang M J, Liu T G, Li P, Wang A B, Zhang J Z, Wang Y C 2011 *IEEE Photon. Technol. Lett.* **23** 1872

[13] Hong Y H, Spencer P S, Shore K A 2012 *J. Opt. Soc. Amer. B* **29** 415

[14] Wang A B, Wang Y C, Yang Y B, Zhang M J, Xu H, Wang B J 2013 *Appl. Phys. Lett.* **102** 031112

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

[16] 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]

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

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

[19] 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]

[20] Akizawa Y, Yamazaki T, Uchida A, Harayama T, Sunada S, Araiet K, Yoshimura K, Davis P 2012 *IEEE Photon. Technol. Lett.* **24** 1042

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

[22] Li X Z, Li S S, Zhuang J P, Chan S C 2015 *Opt. Lett.* **40** 3970

[23] Tang X, Wu Z M, Wu J G, Deng T, Chen J J, Fan L, Zhong Z Q, Xia G Q 2015 *Opt. Express* **23** 33130

[24] Sun Y Y, Li P, Guo Y Q, Guo X M, Liu X L, Zhang J G, Sang L X, Wang Y C 2017 *Acta Phys. Sin.* **66** 030503 (in Chinese) [孙媛媛, 李璞, 郭龑强, 郭晓敏, 刘香莲, 张建国, 桑鲁骁, 王云才 2017 物理学报 **66** 030503]

[25] Wang A B, Wang L S, Li P, Wang Y C 2017 *Opt. Express* **25** 3153

[26] Wu D Y, Zhou L, Huang Y K, Wang P, Wu J, Jin Z, Liu X Y 2016 *Bipolar/BiCMOS Circuits and Technology Meeting* New Jersey, America, September 25–27 2016 p90

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

[28] Rontani D, Locquet A, Sciamanna M, Citrin D S, Ortin S 2009 *IEEE J. Quantum Electron.* **45** 879

[29] Sciamanna M, Shore K A 2015 *Nat. Photon.* **9** 151

[30] National Institute of Standards and Technology Special Publication 800-22, Revision1a http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf [2017-6-1]

[31] Wang L S, Zhao T, Wang D M, Wu D Y, Zhou L, Wu J, Liu X Y, Wang Y C, Wang A B 2017 *IEEE Photon. J.* **9** 7201412

14-Gb/s physical random numbers generated in real time by using multi-bit quantization of chaotic laser*

Wang Long-Sheng[1)2)] Zhao Tong[1)2)] Wang Da-Ming[1)2)] Wu Dan-Yu[3)] Zhou Lei[3)]
Wu Jin[3)] Liu Xin-Yu[3)†] Wang An-Bang[1)2)‡]

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

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

3) (*Microwave Devices and Integrated Circuit Laboratory, Institute of Microelectronics of Chinese Academy of Sciences, Beijing 100029, China*)

(Received 12 July 2017; revised manuscript received 4 August 2017)

Abstract

Real-time high-speed physical random numbers are crucial for a broad spectrum of applications in cryptography, communications as well as numerical computations and simulations. Chaotic laser is promising to construct high-speed physical random numbers in real time benefitting from its complex nonlinear dynamics. However, the real-time generation rate of physical random numbers by using single-bit extraction is confronted with a bottleneck because of the bandwidth limitation caused by laser relaxation, which dominates the laser chaos and then limits the effective bandwidth only to a few GHz. Although some bandwidth-enhanced methods have been proposed to increase the single-bit generation rate, the potential is very limited, and meanwhile the defects of system complexity will be introduced.

An alternative method is to construct high-speed physical random numbers by using the multi-bit extraction. In this method, each sampling point is converted to N digital bits by using multi-bit analog-to-digital converter (ADC) and their M ($M \leqslant N$) least significant bits are retained as an output of random bits, where N and M are the numbers of ADC bits and retained bits, respectively. The generation rate of random numbers is thus equal to M times sampling rate and can be greatly increased. Whereas, in the multi-bit extraction demonstrations, the intensity output of chaotic laser is usually

* Project supported by the National Nature Science Foundation of China (Grant Nos. 61475111, 61671316), the Natural Science Foundation for Excellent Young Scientists of Shanxi, China (Grant No. 2015021004), the International Science and Technology Cooperation Program of Shanxi Province, China (Grant No. 201603D421008), and the International Science and Technology Cooperation Program of China (Grant No. 2014DFA50870).

† Corresponding author. E-mail: xyliu@ime.ac.cn

‡ Corresponding author. E-mail: wanganbang@tyut.edu.cn

digitized by the commercial oscilloscope and then processed with least-significant-bit retention followed by other post-processing methods such as derivative, exclusive-OR, and bit-order reversal. These followed post-processing operations have to be implemented off-line and thus cannot support the real-time generation of random numbers. Resultantly, it is still an ongoing challenge to develop high-speed generation schemes of physical random numbers with the capability of real-time output.

In this paper, a real-time high-speed generation method of physical random numbers by using multi-bit quantization of chaotic laser is proposed and demonstrated experimentally. In the proposed generation scheme, an external-cavity feedback semiconductor laser is utilized as a source of chaotic laser. Through quantizing the chaotic laser with 6-bit ADC, which is triggered by a clock at a sampling rate of 7 GHz, a binary sequence with six significant bits can be achieved. After the selection of the two least-significant bits and self-delayed exclusive-OR operation in the field-programmable gate array (FPGA), a real-time 14-Gb/s binary stream is finally achieved. This binary stream has good uniformity and independence, and has passed the industry-standard statistical test suite provided by the National Institute of Standards and Technology (NIST), showing a good statistical randomness. It is believed that this work provides an alternative method of generating the real-time high-speed random numbers and promotes its applications in the field of information security.

Keywords: semiconductor laser, laser chaos, multi-bit quantization, physical random number

PACS: 42.55.Px, 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.66.234205