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

基于混沌激光的无后处理多位物理随机数高速产生技术研究

孙媛媛 李璞 郭龑强 郭晓敏 刘香莲 张建国 桑鲁骁 王云才

Chaotic laser-based ultrafast multi-bit physical random number generation without post-process

Sun Yuan-Yuan Li Pu Guo Yan-Qiang Guo Xiao-Min Liu Xiang-Lian Zhang Jian-Guo Sang Lu-Xiao Wang Yun-Cai

引用信息 Citation: Acta Physica Sinica, 66, 030503 (2017) DOI: 10.7498/aps.66.030503
在线阅读 View online: http://dx.doi.org/10.7498/aps.66.030503
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2017/V66/I3

基于混沌激光的无后处理多位物理随机数高速产生技术研究*

孙媛媛[1)2)] 李璞[1)2)] 郭龑强[1)2)] 郭晓敏[1)2)] 刘香莲[1)2)] 张建国[1)2)]
桑鲁骁[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 8 月 12 日收到; 2016 年 10 月 13 日收到修改稿)

提出一种基于混沌激光的无后处理多位物理随机数高速提取方法. 该方法在光域中利用锁模激光器作为光时钟, 通过太赫兹光非对称解复用器完成对混沌激光的超低抖动光采样, 无需射频时钟及后续逻辑处理过程的参与, 经多位比较量化可直接产生优质物理随机数. 并以光反馈半导体激光器这一典型的混沌激光产生装置作为熵源对所提方法进行了原理性实验论证. 结果显示, 光反馈半导体激光器产生的6 GHz混沌激光经5 GSa/s实时、低抖动光采样后, 利用并行输出型多位比较器对所获混沌脉冲序列进行量化处理, 选取最低有效位4位, 可直接产生速率达20 Gb/s的随机数. 该随机数速率由选取的量化结果最低有效位数和光采样率联合决定, 而当前光采样率受限于所用混沌激光熵源的带宽. 本文工作可为硬件上实现更高速物理随机数的实时、在线产生提供有力的技术和理论支撑.

关键词: 混沌激光, 物理随机数, 光采样, 保密通信

PACS: 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.66.030503

1 引 言

绝对安全的保密通信需要依靠香农(Shannon)[1]提出的“一次一密”技术. 该技术采用随机数作为密钥对明文信息进行加密, 要求密钥只用一次且长度不短于明文长度. 对于当今高速、大容量的数字通信系统, “一次一密”技术实现的最主要困难之一在于高速、大量随机数的实时获取.

基于算法的伪随机数发生器能产生快速随机数, 但其固有的周期性致使其长度有限, 不足以保证通信的绝对安全. 物理随机数发生器则以自然界的随机过程作为熵源(如电阻热噪声[2]、振荡器频率抖动[3]、量子随机性[4]等), 可产生安全、可靠的随机数, 但受物理熵源带宽的限制, 速率多处于Mb/s量级, 亦无法满足现代Gb/s高速保密通信的绝对安全需要.

近年来, 混沌激光[5−7]因其高带宽、大幅度等特性, 被用作新一代物理熵源以期解决传统物理随机数发生器实时速率不足的问题, 获得了国际上的广泛关注[8−13]. 典型地, 2008年日本Uchida课题组[8]利用两路无关的混沌激光源分别经过1位模数转换器(ADC)和异或逻辑门(XOR)处理后, 首次实时产生了1.7 Gb/s的高速物理随机数. 2010年, 以色列Kanter等[9]则离线证实利用8位ADC及高阶差分后续处理技术可将物理随机数的产生速率提高到300 Gb/s. 我国学者在该领域也取得了众多引人注目的研究进展. 例如, 2011年西南大

* 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: 61405138, 61505137, 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: wangyc@tyut.edu.cn

学夏光琼课题组将互注入半导体激光器输出的混沌激光信号与8位ADC和多位XOR运算后处理相结合, 离线证实了并行产生17.5 Gb/s物理随机数的可行性[14], 并于2015年将该产生速率进一步提升到了1.12 Tb/s[15]; 2014年, 西南交通大学潘炜课题组[16]更是离线证明了将光反馈半导体激光器和高阶有限差分(HFD)后处理技术相结合可产生2.2 Tb/s物理随机数; 我们课题组也在国家基金委支持下取得了一系列成果[17−19].

然而, 目前国内外的研究工作多是将混沌激光转换为电信号, 继而在电域中利用1位或者多位ADC和逻辑处理器件(XOR、减法器、缓存器、移位寄存器)等对混沌电信号进行采样、量化及后续处理(HFD、多级XOR等)来产生随机数. 并且, 大部分研究工作是离线实施的理论预期, 并非在线实时产生. 据我们所知, 文献[19]中报道的4.5 Gb/s物理随机数样机仍是目前已实现的最快实时速率.

限制其实时码率进一步提升的核心困难包括以下两个方面. 第一, 电子ADC面临的“电子抖动瓶颈”. 现有技术都是将连续混沌激光转换为电信号, 在电域中利用电子ADC对混沌电信号进行采样、量化等处理. 具体地, 电ADC对信号的采样处理是通过“采样-保持”电路来完成, 需由射频电时钟来驱动. 然而当前最尖端的电时钟工作在100—400 MHz频率范围内时存在ps以上量级的大幅度孔径抖动, 且随着工作频率的升高, 该抖动呈指数型恶化. 这导致了当前电ADC的响应速率多处于Gb/s以下的电子瓶颈. 第二, 现有物理随机数产生技术均需采用后续处理过程以保证所产生随机数的质量. 然而, 后续处理实现过程中涉及的众多单元器件(如XOR、减法器、缓存器、移位寄存器)亦需通过电时钟来控制彼此间的严格同步. 当工作于Mb/s速率时, 电时钟抖动影响不严重, 可以忽略. 但是当达到Gb/s以上工作频率时, 电时钟的抖动使后续处理元件之间时间同步的实际实现变成一个难以逾越的技术障碍.

在全光域完成对混沌激光的采样过程无需电时钟的参与, 可有效解决上述问题. 常见的全光采样技术都是利用非线性晶体[20−22]、高非线性光纤[23,24]等介质中的四波混频、光参量放大和交叉相位调制(XPM)等效应实现的. 受限于较低的转换效率, 需要W量级以上的高功率控制脉冲, 且长距离的光纤存在不易集成的弊端. 半导体光放大器(SOA)因其非线性系数大、集成度高、增益饱和能量低等优点, 适合应用于全光采样技术中[25]. 基于SOA的XPM效应的太赫兹光非对称解复用器(TOAD)[26,27]具有开关能量低、易于集成等优点, 可作为性能优异的全光采样门.

本文提出一种基于混沌激光的无后处理多位物理随机数高速提取方法, 利用时延抖动处于fs量级的锁模激光器(MLL)作为采样时钟在光域中完成对混沌激光的采样, 继而采用多位比较量化直接完成高速随机数的提取. 整个方案的信号处理过程不再涉及需射频电时钟驱动的“采样-保持”电路和后续处理过程, 因而能有效解决电ADC面临的电子抖动瓶颈, 并克服由后续处理过程引入的电子元件之间的同步难题.

具体地, 本文以混沌激光的典型产生装置(光反馈半导体激光器)作为物理熵源, 采用非线性SOA构建TOAD全光采样门, 结合8位比较器(等效于不含“采样-保持”电路的并行比较型8位ADC)作为量化器件, 对所提方案进行了原理性实验论证. 实验结果显示, 无需射频电时钟和任何后续离线处理算法(如XOR, HFD等)的参与, 通过选取量化结果的4个最低有效位(LSB), 本方法可直接产生20 Gb/s (= 5 GSa/s × 4 LSBs)分布均衡、高质量的物理随机数.

需要指出的是, 本方案中的随机数速率由选取的量化结果最低有效位数和光采样率联合决定. 在原理性论证实验中, 受限于光反馈混沌激光6 GHz的带宽, 光采样率选定在5 GSa/s. 考虑到TOAD的超快响应速率, 只要混沌激光带宽足够高, 采用本方案有望实现数十乃至上百Gb/s物理随机数的产生. 本文工作为硬件上实现更高速物理随机数的实时、在线产生提供了有力的技术和理论支撑.

2 实验装置及工作原理

所提方案的原理性论证实验装置如图1所示. 该系统分为三部分: 混沌激光源(chaotic laser)、全光采样门(optical sampling)和多位比较器. 这里的多位比较器是指不含“采样-保持”电路的并行比较型8位ADC. 混沌激光源由分布式反馈半导体激光器(DFB-LD)和光纤反射镜(FM)联合构成, 该结构是用于提取高速随机数的最典型的混沌激光产生结构. 具体地, DFB-LD输出光经偏振

控制器(PC)后, 进入分光比60∶40的光纤耦合器分为两路, 其中40%输出端口的输出光经可调光衰减器(VOA)到达FM, 形成外腔反馈; 利用VOA调节反馈光强度, 可使DFB-LD工作在混沌振荡态. 所产生的混沌激光由60∶40光纤耦合器的60%端口输出. TOAD是一个光纤环形镜结构, 由偏离环中心Δx位移的非线性SOA, 3 dB光纤耦合器(50∶50)、波分复用器(WDM)、偏振控制器(PC1, PC2)及光带通滤波器(BPF)构成. MLL(Pritel, UOC-05-14 G-E)输出的超短光脉冲作为控制光, 经WDM耦合进入TOAD环中. 混沌激光则作为信号光经PC1后, 由3 dB光纤耦合器等分为两路进入TOAD环: 一路为顺时针(CW)光, 另一路为逆时针(CCW)光. 由于SOA位于偏离环中心Δx处, 因此CW光和CCW光将分先后到达SOA, 形成一个$2\Delta x/v_{\rm g}$的时延窗口($v_{\rm g}$为信号光在TOAD环内的群速度). 每当一个控制光脉冲到达SOA时, SOA达到增益饱和态, 而后逐渐恢复. 这样就使得先后进入SOA的CW光和CCW光分别经历SOA的饱和态和非饱和态, 因此形成了相对相移. 合理选择控制光功率, 可调控该相对相移等于π, 在TOAD输出端(3 dB光纤耦合器的另一端)相干相长输出. 这样就在光域中实现了对混沌激光的低抖动采样. 通过BPF将采样得到的混沌光脉冲序列滤出后, 利用快速光电探测器(PD)转换为电信号, 通过8位比较器(等效于不含"采样-保持"电路的并行比较型8位ADC)量化处理后, LSB 4位的直接输出即为最终的物理随机数序列.

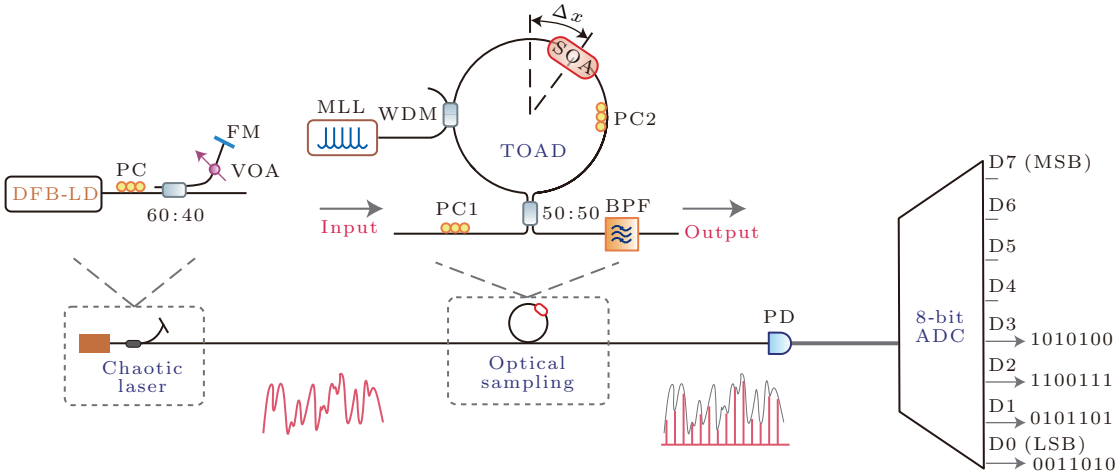

图1 (网刊彩色)由混沌激光源、全光采样门、多位比较器构成的高速物理随机数产生实验装置(DFB-LD, 分布式反馈半导体激光器; PC, PC1, PC2, 偏振控制器; VOA, 可调光衰减器; FM, 光纤反射镜; MLL, 锁模激光器; WDM, 波分复用器; SOA, 半导体光放大器; BPF, 光带通滤波器; PD, 光电探测器; 8-bit ADC, 不含"采样-保持"电路的8位模数转换器)

Fig. 1. (color online) Schematic of the ultrafast physical random number generator consisting of chaotic laser, optical sampling and multi-bit quantization: DFB-LD, distribute feedback laser diode; PC, PC1, PC2, 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; PD, photodetector; 8-bit ADC, 8-bit analog to digital converter without S/H circuit.

3 实验结果

3.1 混沌激光熵源

图1所示的光反馈混沌激光(chaotic laser)实验装置中, DFB-LD的偏置电流为35.2 mA (阈值电流$I_{\rm th}=22$ mA), 工作在中心波长1554.13 nm处; 调节VOA使反馈强度处于1.85%; 反馈腔长约10.5 m. 图2是上述工作状态下输出混沌激光的功率谱、时序及自相关特性曲线. 其中, 功率谱(图2(a))由频谱分析仪(RF Analyzer, Agilent Technologies, N9020A)在分辨率带宽和视觉带宽分别为3 MHz和3 kHz下获得; 时序图(图2(b))由示波器(OSC, Lecroy, LabMaster10-36Zi)在40 GSa/s采样率下获得. 由图2(a)和图2(b)可见, 混沌激光具有很高的带宽, 并呈现大幅度的随机起伏. 按照频谱能量80%计算[28], 混沌激光带宽约6 GHz. 正是其高带宽和类噪声特性, 使得混沌激光被广泛用作提取高速随机数的物理熵源.

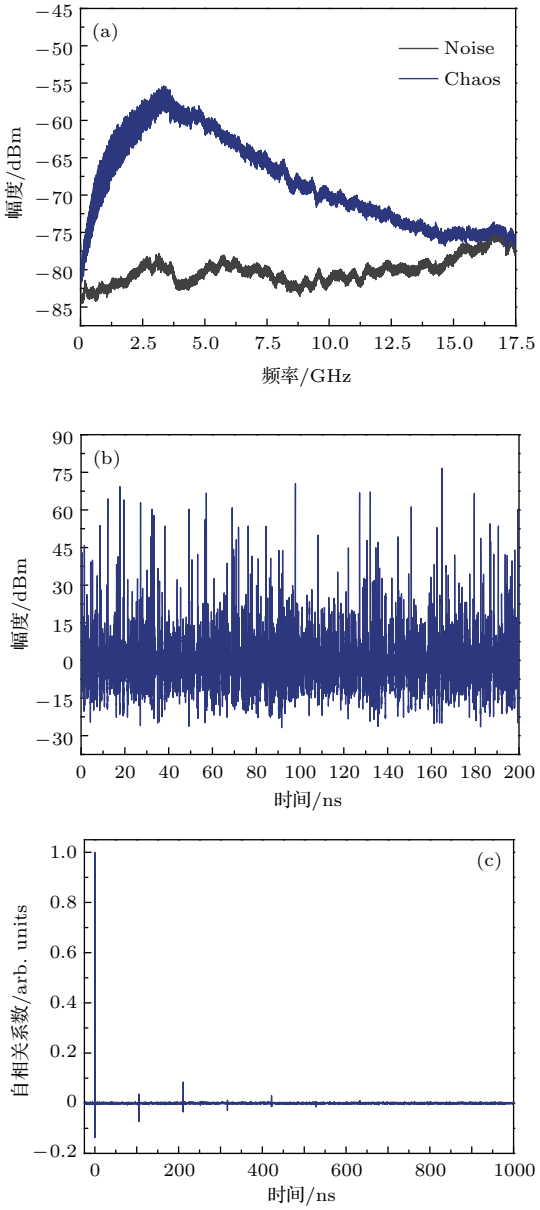

图 2 (网刊彩色) 光反馈混沌激光特性 (a) 功率谱; (b) 时序; (c) 自相关特性曲线

Fig. 2. (color online) Characteristics of the optical feedback chaotic laser: (a) Power spectrum; (b) temporal waveform; (c) autocorrelation curve.

尽管如此, 我们必须注意到, 外腔反馈的引入给混沌激光产生优质随机数带来了一个不利因素, 即“时延特性”. 该时延特性可以通过自相关特性曲线明确标定并量化. 如图 2 (c) 所示, 混沌激光信号的自相关特性曲线在 105.5 ns 及其整数倍处存在一些谐振峰, 105.5 ns 处谐振峰对应的自相关系数被用来表征“时延特性”的强弱. 通过优选激光器偏置电流、反馈强度和偏振状态等关键参数, “时延特性”可在一定程度上受到抑制, 但难以彻底消除. 本实验中, 混沌激光的时延特性被抑制在了 0.036 左右, 如图 2 (c) 所示.

3.2 全光采样混沌激光

图 3 所示为混沌激光经全光采样门 (optical sampling) 采样前、后的时序对比图. 实验中, TOAD 采样门输出的混沌光脉冲序列经 PD 转换为电信号, 由示波器在 80 GSa/s 采样率和 36 GHz 带宽下监测得到. 图 3 (a) 中黑色曲线为被采样的混沌激光时序, 其中的红点标定了被采样点; 蓝色曲线对应的恒定光时钟信号是 MLL 发出的控制光 (图示幅度约为实际控制光功率的 10%). 图 3 (b) 中的红色曲线为 TOAD 采样后得到的混沌脉冲序列, 而灰色虚线为该时刻被采样的混沌激光包络. 由图 3 (b) 中采样结果与被采样信号的同步对比可以看出, 采样后得到的混沌脉冲峰值与被采样点的幅值完全符合, 实现了高保真的实时光采样. 这里要指出的是, 实验中的 SOA 工作在 300 mA 偏置电流下, 相应的增益谱中心波长和小信号增益分别是 1550 nm 和 26 dBm, 增益恢复时间为 25 ps. 采样窗口宽度 ($2\Delta x/v_{\rm g}$) 由 SOA 在环内的非对称偏移量 Δx 决定, 随着 Δx 增加, 窗口宽度和幅度逐渐增大.

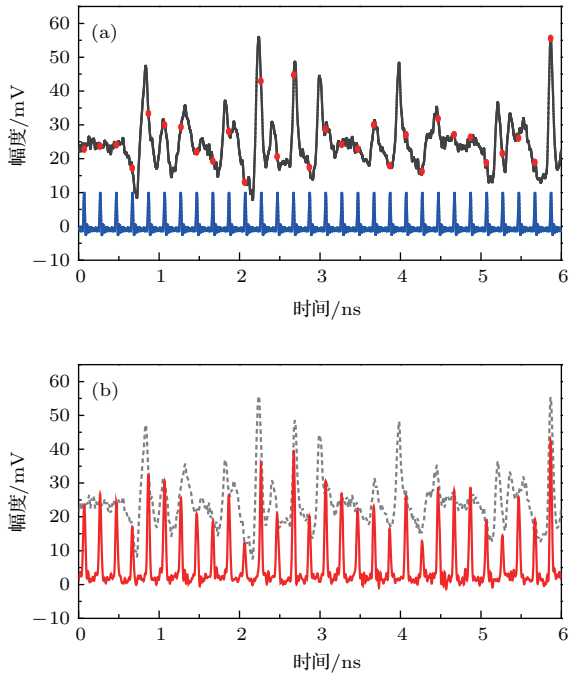

图 3 (网刊彩色) 混沌激光实时光采样结果 (a) 混沌激光及控制光脉冲时序; (b) 采样后的混沌脉冲序列

Fig. 3. (color online) Results of real-time optical sampling of chaotic laser: (a) Temporal waveforms of the laser chaos and the optical clock pulse; (b) chaotic pulses output from the TOAD sampler.

而当Δx远大于SOA的增益恢复时间时, 采样输出将呈现双窗口. 本实验中, SOA位于偏离环中心20 ps处, 因此采样窗口宽度约40 ps. MLL发出的控制光为重频5 GHz、脉宽2.2 ps、时延抖动小于50 fs的超短脉冲序列. 进入TOAD环内的控制光平均功率精确控制在−9 dBm, 此时CW光与CCW光的相位差达到π, 干涉效率最高, 可实现对混沌激光的最优消光比采样. 需要说明的是, 实验中TOAD的采样率由MLL产生的光脉冲重频决定. 采样装置中使用的SOA增益恢复时间小于25 ps, 即本套装置的最高采样率可达40 GSa/s以上. 但考虑到光反馈混沌激光的有限带宽(6 GHz), 为保证物理随机数的优质产生, 实验中将采样率设置为低于混沌激光带宽的5 GSa/s.

进一步, 我们对采样后得到的混沌脉冲序列峰值点的幅值分布进行了分析, 它们是下一步随机数提取的量化对象. 如图4所示, 混沌脉冲峰值完全遗传了原始连续混沌激光的幅度信息, 其峰值点的幅值分布呈现出了明显的不对称性. 不对称的幅值分布是混沌激光固有的另一个不利于产生优质随机数的因素, 需设法消除.

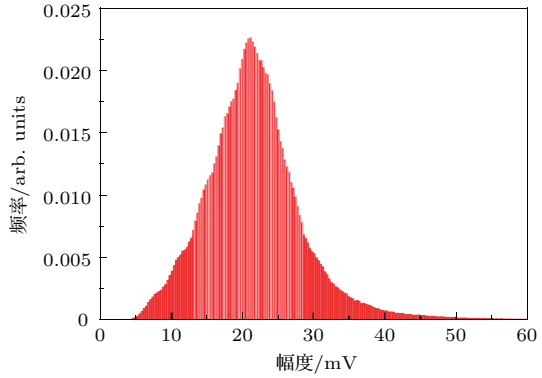

图4 (网刊彩色) 混沌脉冲峰值的幅值分布

Fig. 4. (color online) Normalized distribution for the peak amplitudes of chaotic pulses after sampling.

3.3 物理随机数提取及测评

为了消除混沌激光的上述两个缺陷和提高信息利用率, 我们采用多位比较量化技术从混沌脉冲序列中提取物理随机数. 具体地, 实验中利用8位比较器(不含"采样-保持"电路的并行比较型8位ADC)和选取有限LSB位数来实现, 如图1所示.

除了量化阈值数目不等之外, 不同有效位数的多位比较器工作原理是完全相同的. 对于N位比较器, 量化阈值数为2^N-1个. 为简明起见, 这里仅以3位比较器为例来介绍多位比较器的工作原理. 如图5所示: 灰色曲线为采样后得到的混沌脉冲序列; 蓝色虚线为3位比较器的量化阈值, 共2^3-1个. 3位比较器的工作过程就是按照其量化阈值将采样得到的混沌脉冲序列峰值点(如图5中红色*标注)划分为该阈值区间对应的3位二进制01码, 如图5右侧纵坐标所示. 这3位二进制01码按从右到左依次对应图1中ADC的D0, D1和D2. D0输出称为LSB 1位; D0, D1输出称为LSB 2位; D0, D1, D2输出为LSB 3位. 3位二进制码对应的十进制量化水平如图5左侧纵坐标所示. 8位比较器除了将上述量化阈值增加到2^8-1个, 有效位总数增加到8个, 其他过程与上述类似, 不再赘述.

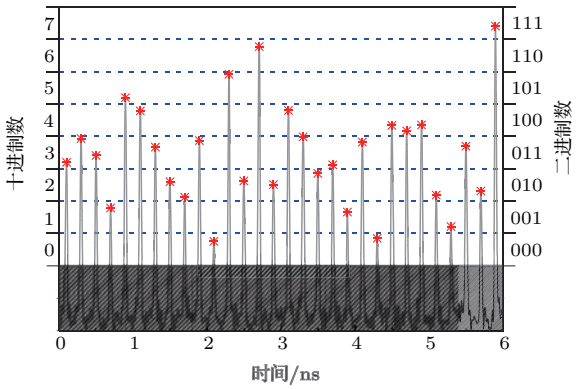

图5 (网刊彩色) 混沌脉冲峰值量化方法(以3位量化为例)

Fig. 5. (color online) Quantification method of chaotic pulses train (take 3-bit quantification for example).

多位比较器量化输出结果有效位数的选取是优质随机数产生的关键, 需考虑以下两个方面: 第一, 量化结果幅值分布的均衡性(它决定了随机数的0/1偏差); 第二, 量化结果的自相关特性(它决定了统计随机数的相关程度是否显著). 具体地, 图6(a)—(h)分别为取LSB 1位至8位对应量化结果的幅值分布. 图7(a)—(h)分别为取LSB 1位至8位对应量化结果的自相关特性曲线. 可以看到图6(h)中, 全8位量化结果与采样后的混沌脉冲峰值的幅值分布(图4)几乎完全一致, 遗传了混沌激光的非对称分布. 而随着所取LSB位数的降低, 幅值分布的均衡性逐渐得到改善, 但量化结果对应的频率仍然有很大差别, 如图6(g)—(e)所示. 直到取LSB 4位及以下(图6(d)—(a))时, 量化结果呈现非常均衡的幅值分布. 与此同时, 可以观察到LSB 1位至4位量化结果的自相关特性曲线

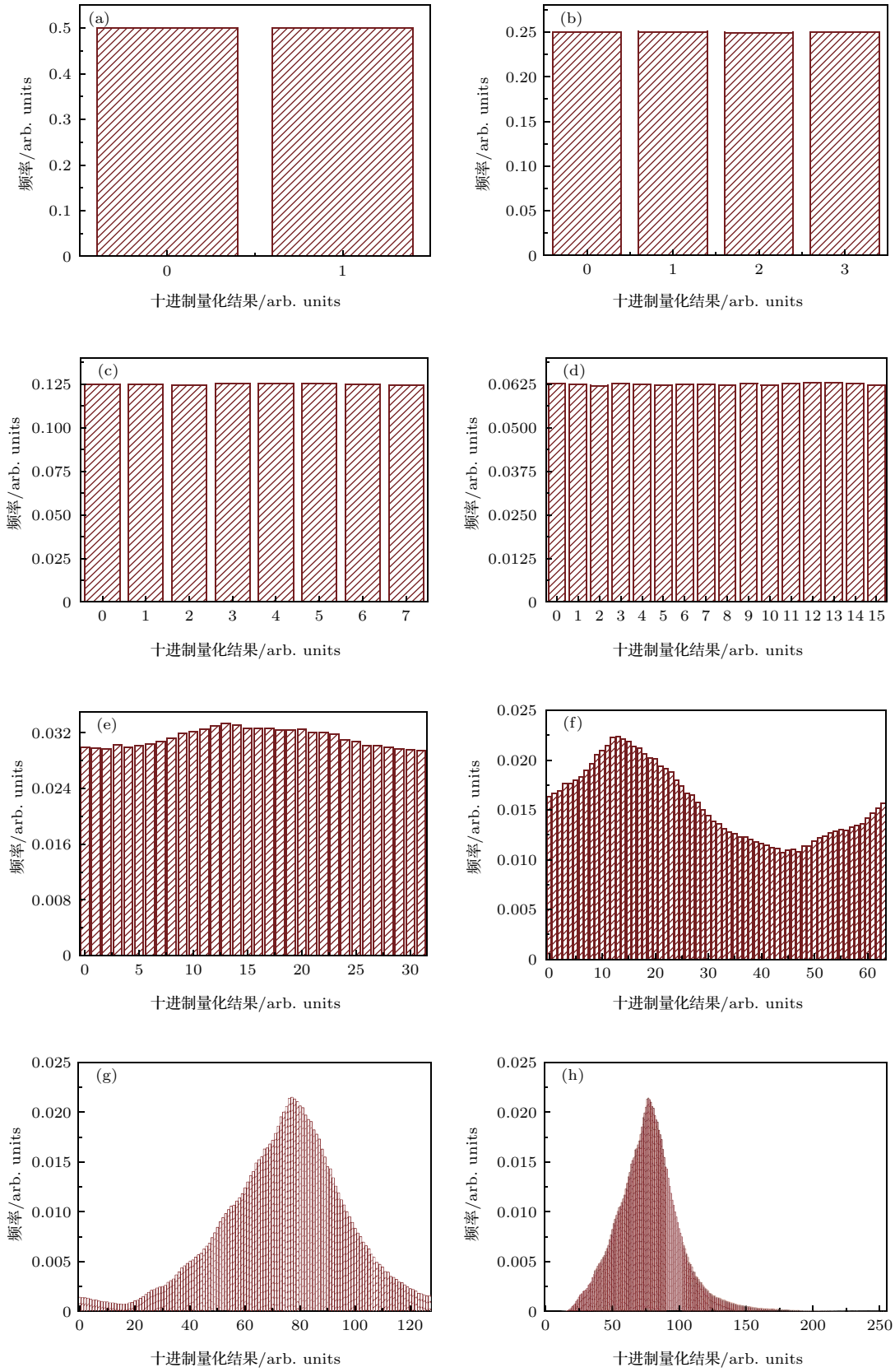

图 6 (网刊彩色) LSB 1 位至 8 位量化结果的幅值分布 (a) 最低位; (b) 低 2 位; (c) 低 3 位; (d) 低 4 位; (e) 低 5 位; (f) 低 6 位; (g) 低 7 位; (h) 全 8 位

Fig. 6. (color online) Normalized distributions for the decimal quantization values generated by retaining m-LSBs for cases: (a) $m = 1$; (b) $m = 2$; (c) $m = 3$; (d) $m = 4$; (e) $m = 5$; (f) $m = 6$; (g) $m = 7$; (h) $m = 8$.

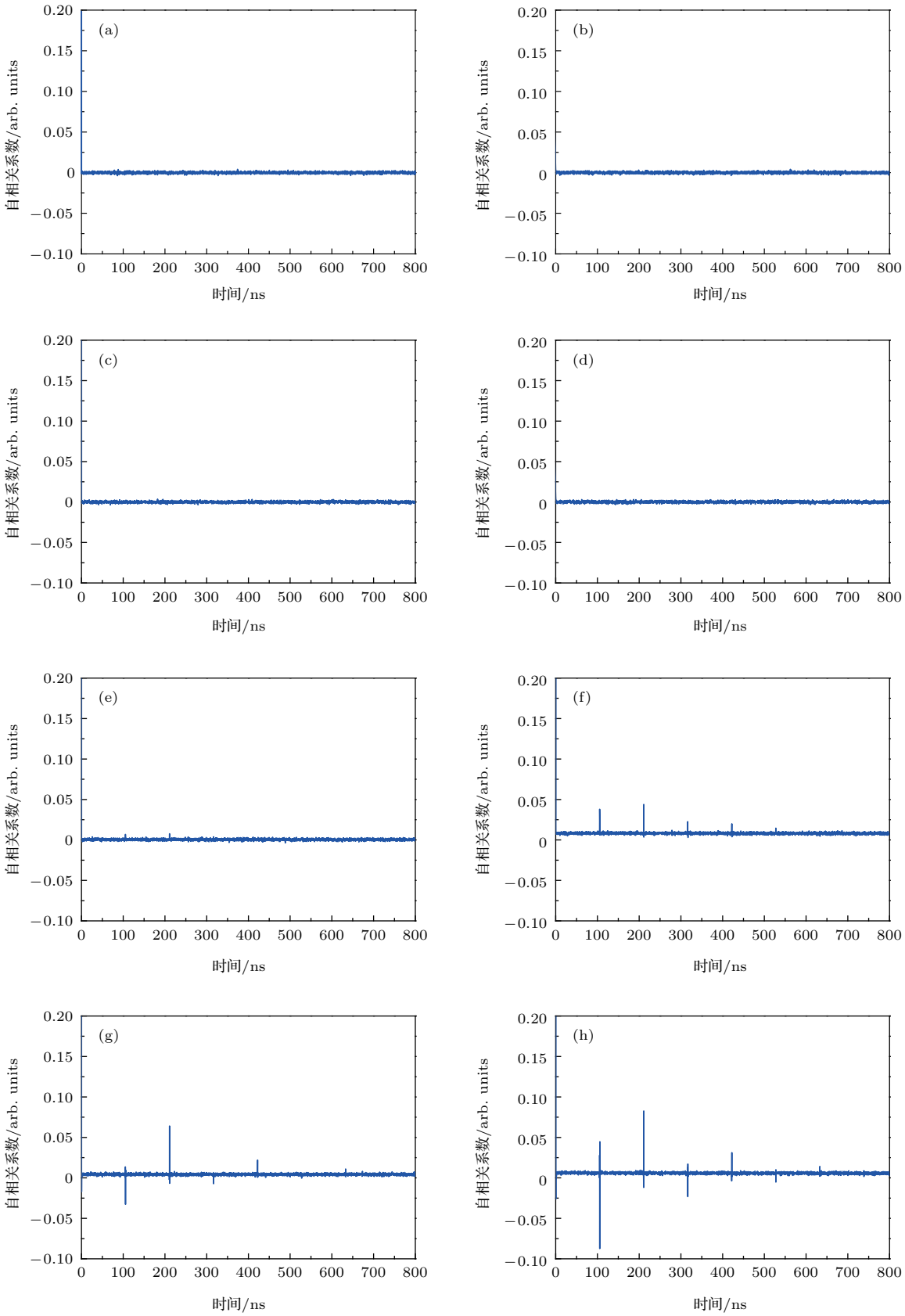

图 7 LSB 1 位至 8 位量化结果的自相关特性曲线 (a) 最低位; (b) 低 2 位; (c) 低 3 位; (d) 低 4 位; (e) 低 5 位; (f) 低 6 位; (g) 低 7 位; (h) 全 8 位

Fig. 7. Autocorrelation curves of the decimal quantization values generated by retaining m-LSBs for cases: (a) $m = 1$; (b) $m = 2$; (c) $m = 3$; (d) $m = 4$; (e) $m = 5$; (f) $m = 6$; (g) $m = 7$; (h) $m = 8$.

(图 7 (a)—(d)) 中不存在任何与“时延特性”信息相对应的谐振峰, 具有良好的随机特性. LSB 5 位至 8 位量化结果的自相关特性曲线 (图 7 (e)—(h)) 则包含越来越明显的谐振峰, 谐振峰所在位置对应的时间信息与混沌激光的反馈腔长一致, 即携带了混沌激光不利于产生优质随机数的“时延特性”, 且“时延特性”随所取有效位数的递增呈增强趋势. 为了在保障随机数质量的基础上获取高速物理随机数, 本实验选用 LSB 4 位作为最终的输出结果, 得到了 20 Gb/s 的优质物理随机数.

为了验证所获随机数的性能, 我们进一步采用随机数行业测试标准——NIST SP800-22 对其进行了测试, 测试结果如图 8 所示. 测试选用 1000 组 1 Mb 的随机数样本, 显著水平 α 设置为 0.01. 这样, 当每个子测试的均匀性 P 值大于 0.0001 且样本通过率在 0.99±0.0094392 范围内时, 说明 NIST SP800-22 测试通过. 图 8 (a) 和图 8 (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, 由图 8 可见, 所产生的随机数可成功通过 NIST SP800-22 中的全部 15 项测试.

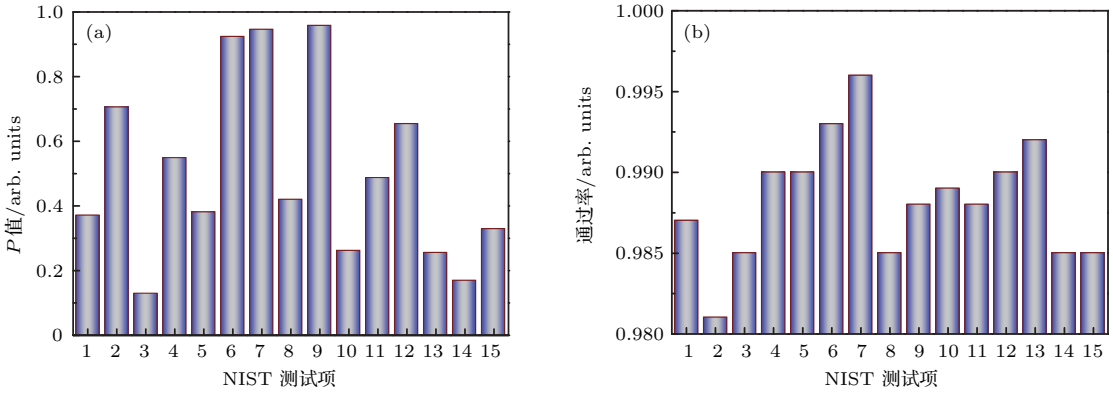

图 8 NIST 测试结果 (a) 各测试项的均匀性 P 值; (b) 各测试项的通过率; 横坐标数字 1—15 分别代表 NIST 测试的 15 个测试项, 分别为频率、块内频率、累积和、游程、块内最长连续、二元矩阵秩、离散傅里叶变换、非重叠模块匹配、重叠模块匹配、全局通用统计、近似熵、随机偏移、随机偏移变量、串行和线性复杂度测试

Fig. 8. Typical results of NIST statistical test: (a) P-value of each test item; (b) pass proportion of each test item. The numbers on the horizontal axis represent 15 different statistical tests in the NIST test suit, which are named as ‘frequency’, ‘block frequency’, ‘cumulative sums’, ‘runs’, ‘longest-run’, ‘rank’, ‘discrete Fourier transform’, ‘non-periodic templates’, ‘overlapping templates’, ‘universal’, ‘approximate entropy’, ‘random excursion’, ‘random excursions variant’, ‘serial’ and ‘linear complexity’, respectively.

4 讨 论

在本实验采用的方法中, 所获随机数速率由选取的量化结果有效位数和光采样率的乘积决定. 要进一步提高随机数速率, 应考虑增加所取量化结果有效位数和提高光采样率, 而影响这两项指标的主要因素分别为混沌激光的时延特性和带宽.

通过抑制外腔反馈混沌激光的时延特性, 可以尽量减小时延特性对提取自混沌激光的随机数的影响, 能够获得更高位的量化结果输出. 常见的调节反馈光强度、偏振态等简单方法, 可在一定程度上抑制时延特性. 另外, 采用双光反馈半导体激光混沌系统 [29], 利用相位调制双路反馈 [30], 将反馈元件由反射镜换为滤波器 (光栅或法布里-珀罗干涉仪) 形成滤波反馈等 [31] 方法能进一步有效抑制时延特性.

本文所述原理性论证实验中, 光采样率受限于光反馈混沌激光的带宽. 采用超宽带混沌激光作为物理熵源, 以更高的光采样率完成采样过程, 可在保证随机数质量的同时提高随机码速率. 目前可获取超宽带混沌激光的方案包括: 将光反馈混沌激光注入从激光器, 能够将信号带宽提高至 12 GHz 以上 [32]; 利用连续波激光注入混沌半导体激光器, 可获得频谱平坦的宽带混沌激光 [33]; 将该方法改进为双光注入, 即利用两台主激光器注入混沌半导体激光器, 适当调谐三个波长间的失谐量, 可得到更宽的混沌信号.

5 结 论

提出了一种基于混沌激光的无后处理多位物理随机数高速产生方法, 并对其进行了原理性实验论证. 利用主动锁模激光器产生的高重频光脉冲作为时钟信号触发TOAD全光采样门, 实现了对光反馈半导体激光器产生的6 GHz混沌激光5 GSa/s低抖动、实时光采样; 继而通过8位比较量化处理采样后的混沌脉冲序列, 无需后续逻辑处理过程, 最终获得了20 Gb/s (= 5 GSa/s × 4 LSBs)的高质量随机数. 当前随机数速率受到了混沌激光带宽的限制. 考虑到TOAD的超快响应速率, 只要混沌激光带宽足够高, 采用本方案有望实现数十、乃至上百Gb/s物理随机数的实时产生.

参考文献

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

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

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

[4] 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]

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

[6] Zhao Q C, Yin H X 2013 *Laser Optoelectron. Prog.* **50** 030003 (in Chinese) [赵清春, 殷洪玺 2013 激光与光电子学进展 **50** 030003]

[7] 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]

[8] 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

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

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

[11] Li X Z, Chan S C 2012 *Opt. Lett.* **37** 2163

[12] Oliver N, Soriano M C, Sukow D W, Fischer I 2011 *Opt. Lett.* **36** 4632

[13] Nguimdo R M, Verschaffelt G, Danckaert J, Leijten X, Bolk J, Sande G V D 2012 *Opt. Express* **20** 28603

[14] 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]

[15] 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

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

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

[18] Zhang J Z, Wang Y C, Liu M, Xue L G, Li P, Wang A B, Zhang M J 2012 *Opt. Express* **20** 7496

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

[20] Duguay M A, Hansen J W 1968 *Appl. Phys. Lett.* **13** 178

[21] Takara H, Kawanishi S, Yokoo A, Yokoo A, Tomaru S 1996 *Electron. Lett.* **32** 2256

[22] Nogiwa S, Kawaguchi Y, Ohta H, Endo Y 2000 *Electron. Lett.* **36** 1727

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

[24] Wang W R, Yu J L, Luo J, Han B C, Wu B, Guo J Z, Wang J, Yang E Z 2011 *Acta Phys. Sin.* **60** 104220 (in Chinese) [王文睿, 于晋龙, 罗俊, 韩丙辰, 吴波, 郭精忠, 王菊, 杨恩泽 2011 物理学报 **60** 104220]

[25] Zhang S J, Zhang Y L, Liu S, Li H P, Liu Y 2012 *Proc. SPIE* **8552** 85520B

[26] Deng K L, Runser R J, Glesk I, Prucnal P R 1998 *IEEE Photon. Technol. Lett.* **10** 397

[27] Li P, Jiang L, Zhang J G, Zhang J Z 2015 *IEEE Photon. J.* **7** 1

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

[29] Ding L, Wu J G, Xia G Q, Shen J T, Li N Y, Wu Z M 2011 *Acta Phys. Sin.* **60** 014210 (in Chinese) [丁灵, 吴加贵, 夏光琼, 沈金亭, 李能尧, 吴正茂 2011 物理学报 **60** 014210]

[30] Xiang S, Pan W, Zhang L, Wen A, Shang L, Zhang H, Lin L 2014 *Opt. Commun.* **324** 38

[31] Wu Y, Wang B J, Zhang J Z, Wang A B, Wang Y C 2013 *Math. Probl. Eng.* **2013** 571393

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

[33] 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

Chaotic laser-based ultrafast multi-bit physical random number generation without post-process*

Sun Yuan-Yuan[1)2)] Li Pu[1)2)] Guo Yan-Qiang[1)2)] Guo Xiao-Min[1)2)] Liu Xiang-Lian[1)2)]
Zhang Jian-Guo[1)2)] Sang Lu-Xiao[1)2)] Wang Yun-Cai[1)2)†]

1) (*Key Laboratory of Advanced Transducers and Intelligent Control System, Ministry of Eduction, 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 12 August 2016; revised manuscript received 13 October 2016)

Abstract

Random numbers have great application value in the fields of secure communications, which are commonly used as secret keys to encrypt the information. To guarantee that the information is absolutely secure in the current high-speed communication, the applied random keys should possess a generation speed not less than the encrypted data rate, according to "one-time pad" theory found by Shannon (Shannon C E 1949 *Bell. Syst. Tech. J.* **28** 656)

Pseudo-random numbers generated by algorithm may easily reach a fast speed, but a certain periodicity makes them difficult to meet the aforementioned demand of information security. Utilizing physical stochastic phenomena can provide reliable random numbers, called physical random number generators (RNGs). However, limited by the bandwidth of the conventional physical sources such as electronic noise, frequency jitter of oscillator and quantum randomness, the traditional physical RNG has a generation speed at a level of Mb/s typically. Therefore, real-time and ultrafast physical random number generation is urgently required from the view of absolute security for high-speed communication today.

With the advent of wideband photonic entropy sources, in recent years lots of schemes for high-speed random number generation are proposed. Among them, chaotic laser has received great attention due to its ultra-wide bandwidth and large random fluctuation of intensity. The real-time speed of physical RNG based on chaotic laser is now limited under 5 Gb/s, although the reported RNG claims that an ultrafast speed of Tb/s is possible in theory.

The main issues that restrict the real-time speed of RNG based on chaotic laser are from two aspects. The first aspect is "electrical jitter bottleneck" confronted by the electrical analog-to-digital converter (ADC). Specifically, most of the methods of extracting random numbers are first to convert the chaotic laser into an electrical signal by a photodetector, then use an electrical ADC driven by radio frequency (RF) clock to sample and quantify the chaotic signal in electronic domain. Unfortunately, the response rate of ADC is below Gb/s restricted by the aperture jitter (several picoseconds) of RF clock in the sample and hold circuit. The second aspect comes from the complex post-processes, which are fundamental in current RNG techniques to realize a good randomness. The strict synchronization among post-processing components (e.g., XOR gates, memory buffers, high-order difference) is controlled by an RF clock. Similarly, it is also an insurmountable obstacle to achieve an accurate synchronization due to the electronic jitter of the RF clock.

In this paper, we propose a method of ultrafast multi-bit physical RNG based on chaotic laser without any post-process. In this method, a train of optical pulses generated by a GHz mode-locked laser with low temporal jitter at

* 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. 61405138, 61505137, 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: wangyc@tyut.edu.cn

a level of fs is used as an optical sampling clock. The chaotic laser is sampled in the optical domain through a low switching energy and high-linearity terahertz optical asymmetric demultiplexer (TOAD) sampler, which is a fiber loop with an asymmetrical nonlinear semiconductor optical amplifier. Then, the peak amplitude of each sampled chaotic pulse is digitized by a multi-bit comparator (i.e., a multi-bit ADC without sample and hold circuit) and converted into random numbers directly.

Specifically, a proof-of-principle experiment is executed to demonstrate the aforementioned proposed method. In this experiment, an optical feedback chaotic laser is used, which has a bandwidth of 6 GHz. Through setting a sampling rate to be 5 GSa/s and selecting 4 LSBs outputs of the 8-bit comparator, 20 Gb/s (= 5 GSa/s × 4 LSBs) physical random number sequences are obtained. Considering the ultrafast response rate of TOAD sampler, the speed of random numbers generated by this method has the potential to reach several hundreds of Gb/s as long as the used chaotic laser has a sufficient bandwidth.

Keywords: chaotic laser, physical random numbers, optical sampling, secure communications

PACS: 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.66.030503