

## 基于激光器阵列后处理的混沌熵源获取高品质随机数

吴佳辰 宋峥 谢溢锋 周心雨 周沛 穆鹏华 李念强

## High-quality random number sequences extracted from chaos post-processed by phased-array semiconductor laser

Wu Jia-Chen Song Zheng Xie Yi-Feng Zhou Xin-Yu Zhou Pei Mu Peng-Hua Li Nian-Qiang

引用信息 Citation: *Acta Physica Sinica*, 70, 104205 (2021) DOI: 10.7498/aps.70.20202034

在线阅读 View online: <https://doi.org/10.7498/aps.70.20202034>

当期内容 View table of contents: <http://wulixb.iphy.ac.cn>

## 您可能感兴趣的其他文章

### Articles you may be interested in

#### 线宽增强因子对光反馈半导体激光器混沌信号生成随机数性能的影响

Influence of the linewidth enhancement factor on the characteristics of the random number extracted from the optical feedback semiconductor laser

物理学报. 2017, 66(12): 124203 <https://doi.org/10.7498/aps.66.124203>

#### 利用混沌激光多位量化实时产生14 Gb/s的物理随机数

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

物理学报. 2017, 66(23): 234205 <https://doi.org/10.7498/aps.66.234205>

#### 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

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

物理学报. 2017, 66(3): 030503 <https://doi.org/10.7498/aps.66.030503>

#### 利用混沌激光脉冲在线实时产生7 Gbit/s物理随机数

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

物理学报. 2017, 66(5): 050501 <https://doi.org/10.7498/aps.66.050501>

#### 半导体激光器混沌输出的延时特征和带宽

Time delay signature and bandwidth of chaotic laser output from semiconductor laser

物理学报. 2020, 69(9): 090501 <https://doi.org/10.7498/aps.69.20191881>

#### 基于两正交互耦1550 nm垂直腔面发射激光器获取多路随机数

Multi-channel physical random number generation based on two orthogonally mutually coupled 1550 nm vertical-cavity surface-emitting lasers

物理学报. 2018, 67(2): 024204 <https://doi.org/10.7498/aps.67.20171902>

# 基于激光器阵列后处理的混沌熵源 获取高品质随机数\*

吴佳辰<sup>1)</sup> 宋峥<sup>1)</sup> 谢溢锋<sup>1)</sup> 周心雨<sup>1)</sup>

周沛<sup>1)2)†</sup> 穆鹏华<sup>3)</sup> 李念强<sup>1)2)‡</sup>

1) (光电科学与工程学院, 苏州纳米科技协同创新中心, 苏州大学, 苏州 215006)

2) (江苏省先进光学制造技术重点实验室, 教育部/江苏省现代光学技术重点实验室, 苏州大学, 苏州 215006)

3) (光电信息科学技术学院, 烟台大学, 烟台 264005)

(2020 年 12 月 2 日收到; 2020 年 12 月 19 日收到修改稿)

本文提出采用可集成的激光器阵列后处理光反馈半导体激光器的输出, 进而获得无时延特征的优质混沌熵源, 进一步获取高速高品质随机数序列. 方案中采用常规的 8 位模数转换采样量化和多位最低有效位异或提取处理, 采用国际公认的随机数行业测试标准 (NIST SP 800-22) 来检验产生的序列. 结果表明, 通过激光器阵列后处理的混沌熵源所获取的随机数序列具有均匀分布特性, 散点图无明显图案, 可以成功通过 NIST SP 800-22 的全部测试. 另外, 基于激光器阵列的可扩展性, 本方案可以拓展为可实现同时产生多路并行的高速高品质随机数发生器.

**关键词:** 半导体激光器, 激光器阵列, 混沌激光, 随机数

**PACS:** 42.55.Px, 05.45.-a, 05.45.Pq

**DOI:** 10.7498/aps.70.20202034

## 1 引言

随着计算机技术、通信技术的迅速发展, 特别是互联网的普及导致了信息量的爆炸式增长, 信息安全受到了各界的广泛关注. 在信息安全领域, 随机数有着至关重要的地位, 密钥管理、密码学协议、数字签名及身份验证等众多安全技术都需要用到随机数. 而且, 在目前规则下, 绝对安全的保密通讯需要满足 Shannon<sup>[1]</sup> 提出的“一次一密”理论, 这就要求大量、高速、安全随机数能实时、快速地产生. 近年来, 随机数的相关研究备受国内外学者

的关注, 因此各类随机数发生器被相继提出和验证<sup>[2-6]</sup>.

随机数可分为真随机数 (或物理随机数) 和伪随机数<sup>[7]</sup>. 伪随机数主要是基于算法产生的, 但是因为其固有的周期性使其长度有限, 而且只要获取随机源种子就可复制此类随机数, 不足以保证通信或信息交换、传输的绝对安全. 随着计算机运算能力的提升, 伪随机数用于加密通讯时被破解的可能性大幅度增加, 难以确保通信系统的安全性. 与之不同的是, 真随机数是由物理熵源产生的, 具有高度不可预测性, 使得通信系统的安全性更高. 真随机数的物理熵源主要有电阻热噪声、电子振荡器的

\* 国家自然科学基金 (批准号: 62004135, 62001317)、江苏省高等学校自然科学研究重大项目 (批准号: 20KJA416001) 和苏州大学科研启动经费 (批准号: Q415900119) 资助的课题.

† 通信作者. E-mail: [peizhou@suda.edu.cn](mailto:peizhou@suda.edu.cn)

‡ 通信作者. E-mail: [nli@suda.edu.cn](mailto:nli@suda.edu.cn)

频率抖动、电路混沌和激光器相位噪声等<sup>[7]</sup>. 此外, 利用量子力学基本量的完全随机性及采集生物的无规律行为也可以作为熵源, 通过后处理来提取真随机数<sup>[8–10]</sup>. 但此类物理熵源的带宽很小, 获取的随机数速率不高, 无法满足当前高速、大容量通信或高速计算模拟的需求. 因此, 寻找新的物理熵源, 通过后处理以实现高速高品质物理随机数发生器的研究成为了当前的研究热点.

幸运的是, 国内外学者研究发现普通商用半导体激光器在引入一个或多个附加自由度, 如光反馈、光注入或者光电反馈, 可以实现丰富的动力学行为 (单周期、多周期、类周期及混沌), 进一步通过优化参数配置即可获取大带宽、高复杂度的混沌熵源<sup>[11]</sup>. 2008 年, 日本 Uchida 教授的课题组<sup>[12]</sup>首次通过后处理两路混沌激光器信号, 实现了速率可达 1.7 Gb/s 的高速随机数生成. 2009 年, 以色列著名学者 Reidler 领导的团队<sup>[13]</sup>采用 8 位数模转换器 (analog-to-digital converter, ADC) 对混沌熵源进行采样量化, 获取了速率为 12.5 Gb/s 的随机数, 紧接着又采用多级差分处理技术实现了速率可达 300 Gb/s 的随机数<sup>[14]</sup>. 上述工作证明了混沌熵源产生高速随机数的可行性, 也把物理随机数的速率提高了多个量级, 掀起了国内外研究采用混沌激光熵源产生高速随机数的热潮<sup>[7,15–20]</sup>. 特别地, 在国内高校中, 太原理工大学提出了多种产生实时、高速随机数的研究方案, 也提出了基于激光混沌的全光随机数的概念, 最终还实现了随机数发生器样机<sup>[18,21–25]</sup>; 西南大学在随机数相关研究方面也走在了国际前列, 实现了多种并行随机数发生器<sup>[19,26–28]</sup>; 西南交通大学提出了采用信息理论区分混沌熵源产生的随机数类型, 并首次实现了基于混沌激光熵源的速率达到 2.2 Tb/s 量级的随机数<sup>[7,29,30]</sup>; 成都电子科技大学和西安电子科技大学课题组也在随机数发生器和安全密钥分发方面做了大量优秀的工作<sup>[31–34]</sup>. 值得注意的是, 在上述混沌熵源的多种产生方案中, 由于光反馈半导体激光器具有系统结构简单、成本低以及动力学丰富的特点, 成为了学者们关注的焦点, 其产生的混沌激光具有大带宽、大幅度 and 类随机起伏等优点, 因此常用于高速随机数发生器和保密通信领域<sup>[11]</sup>. 可是光反馈半导体激光器输出的混沌信号具有较高的时间延迟特征 (time-delay signature, TDS), 它会阻止生成的序列通过随机数测试标准<sup>[7]</sup>. 为此, 国

内外学者提出了许多可行的方案来削弱或消除这些 TDS, 如光注入后处理、光纤传输后处理、互注入或复杂反馈结构等<sup>[35–40]</sup>. 通过研究发现, 采用上述方案后, 混沌熵源的品质得以提高, 进而进行简单后处理即可产生高速、安全的随机数.

基于此, 本文采用集成化的激光器阵列作为后处理单元来优化外光反馈激光器产生的原始混沌信号, 消除了混沌信号中的弱周期性<sup>[41]</sup>. 该方法具有成本低、集成度高及可扩展性高的优点. 需要说明的是, 仿真模型产生的混沌信号与实验条件下的不同, 实验获得的混沌信号统计分布大都是类高斯分布的, 更利于获取随机数, 但在仿真条件下, 由于模型未考虑增益饱和器件或仪器带宽受限带来的滤波效应, 产生的混沌信号统计分布是类指数分布的. 因此, 在仿真条件下, 我们采用了稍微复杂的后处理来实现随机数提取, 其实在实验条件下, 只需采用更加简单的后处理即可. 在本文中, 我们首先将其原始混沌熵源与其自身延迟的信号作差, 然后通过 8 位 ADC 量化采样优化后的混沌熵源, 再采用同时提取多位最低有效位 (least significant bit, LSB) 和异或 (exclusive OR, XOR) 处理偏差, 获取了随机比特序列. 采用国际公认的随机数测试套件 NIST Special Publication 800-22<sup>[42]</sup>对上述比特序列进行测试, 证明了本方案产生的随机数可通过此测试标准, 进一步论证了采用激光器阵列后处理混沌熵源实现高品质随机数生成的可行性. 另外, 本方案中仅考虑了两节点激光器阵列, 如果引入更多的节点或实现大型激光器阵列, 通过合理设计, 可以保证每个节点输出混沌信号关联度很低, 最后分别通过后处理, 可实现多路并行的高速高品质随机数生成.

## 2 系统结构及理论模型

基于激光器阵列后处理的混沌熵源获取随机数的装置如图 1 所示, 它包含了产生混沌熵源和随机数提取两部分. 其中, 混沌熵源产生部分由光反馈半导体激光器和激光器阵列组成. 光反馈半导体激光器输出光作为原始混沌信号单向注入激光器阵列的节点激光器 A 中, 经激光器阵列中的两个激光器 A、B 处理后得到高质量混沌激光. 本文主要采用激光器阵列中的节点 B 输出作为混沌熵源产生高速高品质随机数. 在我们的仿真实验中,

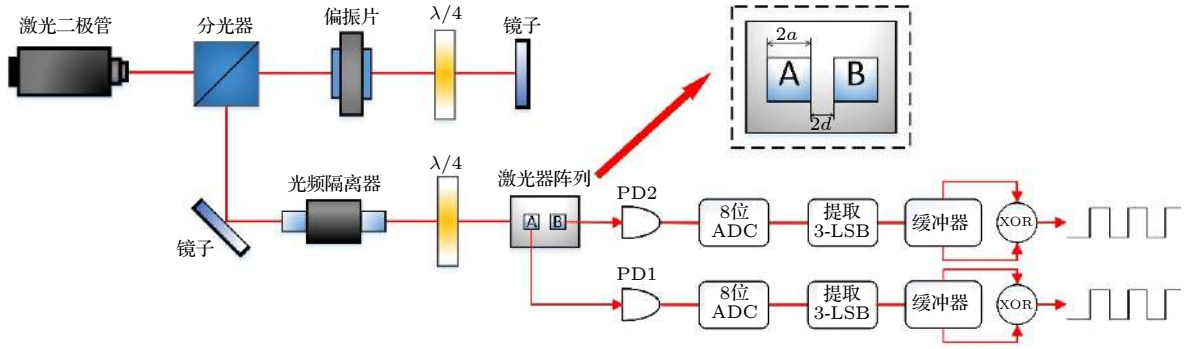


图 1 基于激光器阵列后处理的混沌熵源获取高品质随机数的示意图 ( $\lambda/4$  为  $1/4$  波片, PD1、PD2 为光电转换器, ADC 为模数转换器, LSB 为最低有效位, XOR 为异或处理)

Fig. 1. Schematic diagram of high quality random number generation based on the chaotic entropy source generated by ECSL and post-processed by phased-array semiconductor lasers ( $\lambda/4$ ,  $1/4$  wave plate; PD1 and PD2, photo detector; ADC, analog-to-digital converter; LSB, least significant bit; XOR, exclusive OR).

采用了 8 位 ADC 采样量化, m-LSB 提取和 XOR 处理. 本文以在每个样本点中提取 3-LSB 来获取随机数为例说明此方案产生高速高品质随机数的可行性.

根据图 1 所示装置, 混沌熵源的速率方程可写为 [41]:

$$\begin{aligned} \dot{E}_M = & \Gamma \frac{c}{2n_g} a_{\text{diff}} (N_M - N_{M\text{th}}) (1 - i\alpha_H) E_M \\ & + k_f E_M (t - \tau_f) \exp(-i\omega_M \tau_f), \end{aligned} \quad (1)$$

$$\begin{aligned} \dot{E}_{A,B} = & \Gamma \frac{c}{2n_g} a_{\text{diff}} (N_{A,B} - N_{A\text{th},B\text{th}}) (1 - i\alpha_H) E_{A,B} \\ & + i(\omega - \Omega_{A,B}) E_{A,B} + i\eta E_{B,A} \\ & + k_{\text{inj}} E_M (t - \tau_{\text{inj}}) \exp[-i(\omega_M - \omega)t], \end{aligned} \quad (2)$$

$$\dot{N}_j = P_j - N_j \gamma_N - \frac{c}{n} [g_{\text{th}} + a_{\text{diff}} (N_j - N_{j\text{th}})] |E_j|^2, \quad (3)$$

式中: 下标 M 表示光反馈半导体激光器, A 和 B 分别表示激光器阵列中的节点激光器 A 和 B,  $j = M, A, B$ ;  $E(t)$  表示电场;  $N(t)$  表示载流子浓度 ( $N_0$  为透明载流子密度); 下标 'th' 表征阈值;  $\Gamma$  为光场限制因子;  $c$  为光速;  $n_g$  为群折射率;  $a_{\text{diff}}$  为微分增益;  $\alpha_H$  为线宽增强因子;  $\Omega_{A,B}$  为腔谐振频率;  $P_{A,B}$  为抽运率 ( $P_{\text{th}}$  为阈值电流);  $\gamma_N$  为腔衰减速率;  $\tau_p$  为光子寿命;  $n$  为折射率;  $g_{\text{th}}$  为增益阈值 ( $\Gamma g_{\text{th}} = n_g / (c\tau_p)$ ). (1) 式表示光反馈半导体激光器中的反馈项, 其中  $k_f$  和  $\tau_f$  分别为反馈强度和反馈时间. (2) 式中右边第三项表征相控阵列中两全同激光器节点之间的横向耦合, 其中  $\eta$  为复耦合强度, 它的表达式可以在文献 [43] 中的

(1) 式中找到. (2) 式中最后一项表征从外光反馈半导体激光器的注入效应, 其中  $k_{\text{inj}}$  为注入强度,  $\tau_{\text{inj}}$  为光从外光反馈激光器到激光器阵列的传播时间 (不失一般性, 我们假定  $\tau_{\text{inj}} = 0$ ),  $\omega_M$  是外光反馈激光器的角频率,  $\omega$  是激光器阵列自由运行的角频率. 因此, 频率失谐可以表示为  $\Delta f = (\omega_M - \omega) / 2\pi$ . 本论文中, 注入项仅存在于激光器阵列中的节点 A 方程.

### 3 结果与讨论

利用四阶龙格-库塔算法对该系统速率方程进行数值求解, 得到激光器输出的混沌信号. 在本文数值模拟中, 相关参数取值如下 [41]:  $\alpha_H = 5$ ,  $a = 4 \mu\text{m}$ ,  $a_{\text{diff}} = 2.5 \times 10^{-16} \text{ cm}^2$ ,  $\gamma_N = 1.0 \text{ ns}^{-1}$ ,  $\tau_p = 1.53 \text{ ps}$ ,  $N_0 = 1 \times 10^{18} \text{ cm}^{-3}$ ,  $n = 3.4$ ,  $P = 1.5P_{\text{th}}$ . 除非特别说明, 我们选择激光器阵列中 A、B 节点间的分离比 ( $d/a$ ) 为 0.5, 其中  $d$  为 A、B 节点间距离的  $1/2$ ,  $a$  为激光器节点宽度的  $1/2$ , 波导参数选择带增益引导的反反射率引导, 具体定义和参数可参照我们前期的工作 [43]. 不失一般性, 我们选取反馈强度  $k_f = 5 \text{ ns}^{-1}$  和反馈时延  $\tau_f = 1 \text{ ns}$ , 此时光反馈半导体激光器工作在混沌状态, 其强度时间序列如图 2(a1) 所示. 通过计算强度时间序列的自相关 (autocorrelation function, ACF), 我们发现在反馈时延  $\tau_f = 1 \text{ ns}$  及其倍数处 ACF 出现峰值, 如图 2(a2) 所示. 通过观察图 2(a3) 给出的频谱, 同样可以发现等间隔的峰值, 频率间隔等于反馈时延  $\tau_f$  的倒数. 它们表明此原始混沌信号存在周期性, 不利于获取高品质随机数. 研究发现通过注入

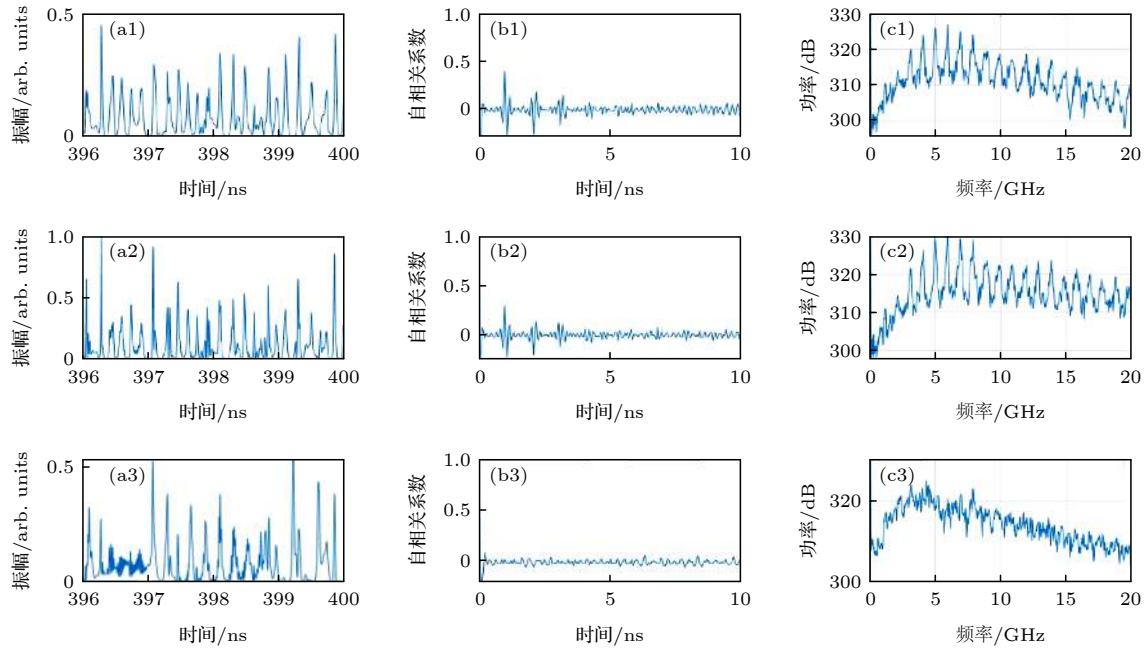


图 2 激光器输出混沌信号的时间序列 (左列), 自相关函数谱 (中列), 功率谱 (右列) (a) 光反馈半导体激光器; (b) 注入激光器; (c) 注入激光器阵列

Fig. 2. Time series (left column), autocorrelation function (middle column), and power spectra (right column) of the chaotic signal output by laser: (a) ECSL; (b) injection to a single laser A; (c) injection to phased-array lasers.

到单个激光器或激光器阵列可有效改善此时延特性, 特别地, 在同等注入条件下, 激光器阵列可在更大的参数空间内实现时延隐藏. 图 2(b) 和 2(c) 分别为光反馈半导体激光器产生的混沌信号注入单个激光器和两节点激光器阵列后的混沌熵源及其 ACF 与频谱特征. 上述图中选择以注入参数  $k_{inj} = 30 \text{ ns}^{-1}$  与  $\Delta f = -30 \text{ GHz}$  为例. 通过比较可以发现, 同等条件下, 激光器阵列更适合用于后处理混沌熵源, 其 ACF 和频谱均无明显峰值, 此结果与我们之前报道的结果具有一致性<sup>[41]</sup>.

在我们另外的工作中, 详细研究了不同波导参数、注入参数和耦合参数对于混沌熵源 ACF 特征的影响<sup>[44]</sup>. 图 3 以带增益引导的反折射率引导波导为例, 给出了时延处的 ACF 峰值随着注入参数和阵列中激光器分离比  $d/a$  的演化情况. 红色代表时延处 ACF 峰值明显的情况, 而蓝色则表示时延被抑制或消除. 从图 3 可见, 当分离比较小时, 注入强度不宜过大, 在负频率失谐区域更易实现时延隐藏; 随着分离比的增大, 激光器阵列更易实现时延隐藏. 因此, 通过合理设计, 激光器阵列能够有效提升光反馈半导体激光器产生的混沌熵源的性能. 本文重点证明采用激光器阵列后处理的混沌熵源获取高品质随机数的可行性, 对于时延特征的详

细分析不再赘述, 可参照我们的其他同步工作.

接着, 分析利用激光器阵列处理后的混沌熵源输出经过图 1 所示后处理产生的二进制序列的特性. 正如前面提到的, 在给定仿真参数下, 由于没考虑增益饱和效应和器件或仪器带宽受限, 混沌信号的统计直方图服从近似的指数分布, 远离理想的高斯分布, 并不利于随机数的直接提取, 这里采用混沌熵源与其延迟特定时间后的混沌信号作差. 所得的混沌熵源的统计直方图如图 4(a) 所示, 其分布的两边存在较长的尾巴. 将激光器输出的混沌信号经过 8 位 ADC 后转变为 8 位二进制序列, 其中 ADC 的采样速率为 20 GHz. 这里以 8 位二进制量化序列中提取 3 位 LSB 拼接为例, 其随机数生产速率可达 60 Gb/s (采用高阶差分 and 拓展激光器阵列节点数目, 可轻松实现 Tb/s 量级速率的随机数产生), 所得序列的分布如图 4(b) 所示, 此时分布的均匀性有所改善, 但仍能看到一些量化比特位出现的概率比其他的高一些. 最后采用常规的 XOR 处理, 得到如图 4(c) 所示的近似理想的均匀分布, 适合直接用于获取随机数.

为了进一步说明经过以上后处理的序列具有随机数分布特性, 这里采用散点图来表示. 如图 5 所示, 横纵坐标分别采用了 500 个“0”“1”比特位

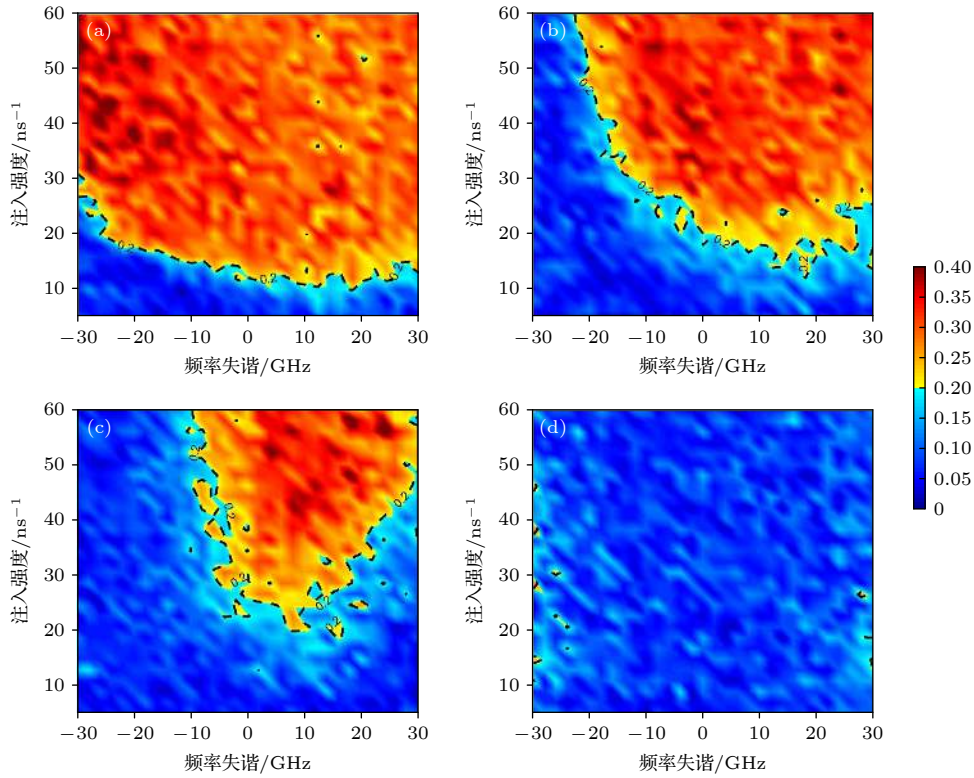


图 3 经过激光器阵列后处理混沌熵源的 ACF 时延处峰值随着注入参数和激光器分离比  $d/a$  的演化情况 (a)  $d/a = 0.2$ ; (b)  $d/a = 0.4$ ; (c)  $d/a = 0.6$ ; (d)  $d/a = 1.0$

Fig. 3. The evaluation of the ACF peak value located around the feedback delay of the chaotic entropy source that is processed by the phased-array in the plane of injection parameters for several values of laser separation: (a)  $d/a = 0.2$ , (b)  $d/a = 0.4$ , (c)  $d/a = 0.6$ , (d)  $d/a = 1.0$ .

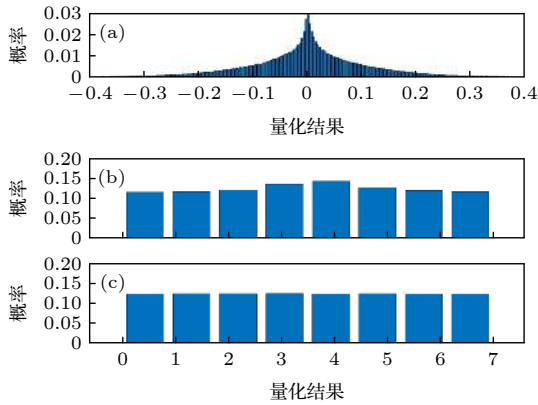


图 4 激光器 B 输出的混沌信号量化后的统计直方图 (a) 8 位 ADC 输出; (b) 3-LSB 输出; (c) XOR 输出

Fig. 4. Statistical histogram of the quantized chaotic signal of the laser B: (a) The output of 8 bit ADC; (b) the output of 3-LSB; (c) the output of XOR.

进行统计, 可以看出散点图中无明显的特殊图案, 具有随机分布的特点. 虽然这里仅采用了  $500 \times 500$  比特位来作图, 但是所提取的随机序列都满足本图所给的特征.

进一步, 我们运用美国国家标准技术研究所提供的 NIST SP 800-22 测试软件对所获得的 3 位

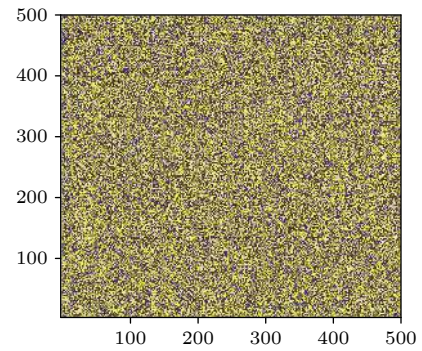


图 5 散点图

Fig. 5. Scatter diagram.

XOR 二进制序列进行随机性测试. NIST 测试项目共有 15 项, 每项测试结果用  $p$  表示. 若  $p$  值大于显著水平值  $\alpha = 0.01$ , 则说明该随机数序列通过了相应的测试 [39]. 本测试最终结果是多组多次测试的统计, 采用  $p$  的分布 P-value 来表征, 如果 P-value 大于  $q - 3\sqrt{q(1-q)/m}$  ( $q = 1 - \alpha$ ,  $m$  表示测试序列的组数字), 则表示通过该项随机数测试. 在本文的工作中, 我们采集了 500 组数据进行测试, 则要求每项测试通过率大于 0.977. 表 1 给

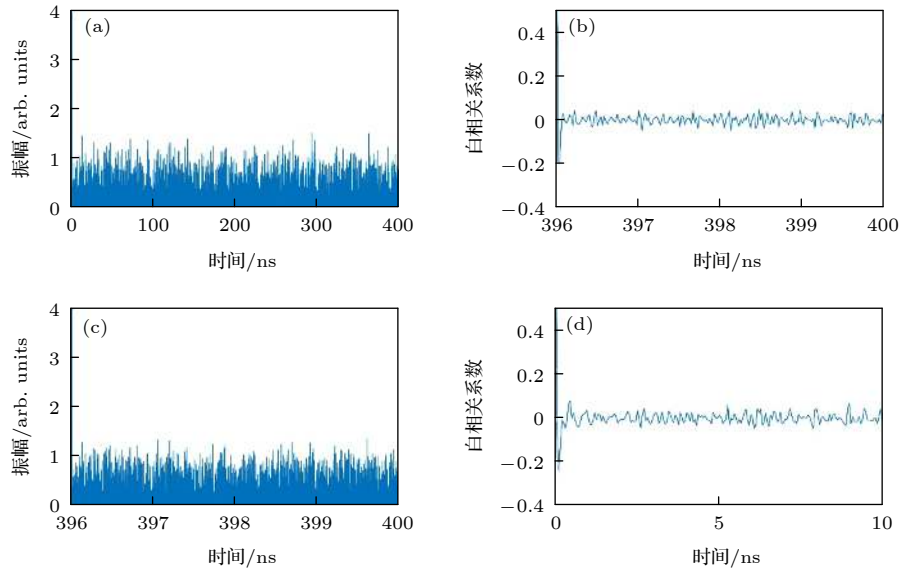


图6 激光器输出的时间序列与自相关函数 (a) A 激光器输出的时间序列; (b) A 激光器输出的自相关函数; (c) B 激光器输出的时间序列; (d) B 激光器输出的自相关函数

Fig. 6. Time series and autocorrelation function of the lasers: (a) Time series of laser A; (b) autocorrelation function of laser A; (c) time series of laser B; (d) autocorrelation function of laser. B.

表1 NIST 统计测试结果  
Table 1. Result of NIST statistical tests.

测试名称	P-value	概率	结果
频数	0.538182	0.992	通过
块内频数	0.239266	0.982	通过
累加	0.755819	0.994	通过
游程	0.140453	0.988	通过
块内最长游程	0.965860	0.988	通过
矩阵秩	0.281232	0.990	通过
离散傅里叶变换	0.206629	0.982	通过
非重叠模块匹配	0.020831	0.982	通过
重叠模块匹配	0.699313	0.984	通过
通用统计	0.510153	0.994	通过
近似熵	0.699313	0.994	通过
随机游动	0.443665	0.986	通过
随机游动变量	0.290158	0.983	通过
连续性	0.096578	0.984	通过
线性复杂度	0.340858	0.986	通过

出了测试结果,从中可以看出激光器阵列作为混沌熵源获取的随机数能够通过 NIST 的全部随机数测试标准.值得强调的是,我们对原混沌熵源(图 1(a))和注入单个激光器后的混沌熵源(图 1(b))采用了上述一样的后处理,得到的随机数序列均未完全通过 NIST 测试,这可以说明激光器阵列后处理的有效性和实用性.虽然这里只给出了一个典型结果,其实如图 3 所示的蓝色区域基本均表示激光

器阵列有效改善了混沌熵源,通过一系列后处理得到的随机数序列都达到以上测试条件.

最后,我们强调激光器阵列后处理光反馈激光器产生混沌信号的另一个优势,即是其可同时获取多路相关或不相关的随机数序列.通过选择参数,激光器阵列中 A、B 节点的混沌输出均不具有时延特征.如以  $k_{inj} = 7 \text{ ns}^{-1}$ ,  $\Delta f = -30 \text{ GHz}$  为例,结果如图 6 所示,激光器阵列中节点 A、B 均实现高维混沌输出,而且在 ACF 图中无时延特征峰值.通过必要后处理,很容易得到两路高品质的随机数序列.其实激光器阵列的可扩展性强,可以实现多节点甚至大型节点的激光器阵列,因此本文结果可为实时产生多路并行的高速高品质的随机数序列提供思路.

## 4 结 论

本文采用激光器阵列后处理光反馈半导体激光器产生的混沌熵源,再经过光电转换、模数转换采样量化及  $m$ -LSB 提取和 XOR 处理,最终产生随机数序列.研究表明,激光器阵列使得光反馈半导体激光器产生的原始混沌信号的弱周期性得到有效抑制,可作为混沌熵源来获取随机数.经过常规后处理,随机数序列分布均匀,通过了随机数行业测试标准 (NIST SP 800-22) 中的全部 15 项

测试, 如果扩展激光器阵列中的节点数, 则有望实现同时获取多路并行的高速高品质随机数.

## 参考文献

- [1] Shannon C E 1949 *Bell Syst. Tech. J.* **28** 656
- [2] Durt T, Beimonte C, Lamoureux L P, Panajotov K, van den Bergh F, Thienpont H 2013 *Phys. Rev. A* **87** 022339
- [3] Williams C R S, Salevan J C, Li X W, Roy R, Murphy T E 2010 *Opt. Express* **18** 23584
- [4] Guo H, Tang W Z, Liu Y, Wei W 2010 *Phys. Rev. E* **81** 051137
- [5] Ma X F, Xu F H, Xu H, Tan X Q, Qi B, Lo H K 2013 *Phys. Rev. A* **87** 062327
- [6] David P, Rosin, Damien Rontani, Daniel J. Gauthier 2013 *Phys. Rev. E Stat. Nonlin. Soft Matter Phys.* **87** 040902
- [7] Li N Q, Kim B, Chizhevsky V N, Locquet A, Bloch M, Citrin D S, Pan W 2014 *Opt. Express* **22** 6634
- [8] Guo H, Liu Y, Dang A H, Wei W 2009 *Chin. Sci. Bull.* **54** 3651 (in Chinese) [郭弘, 刘钰, 党安红, 韦韦 2009 科学通报 **54** 3651]
- [9] Ren M, Wu E, Liang Y, Jian Y, Wu G, Zeng H 2011 *Phys. Rev. A* **83** 023820
- [10] Zhou Q, Hu Y, Liao X F 2008 *Acta Phys. Sin.* **57** 5413 (in Chinese) [周庆, 胡月, 廖晓峰 2008 物理学报 **57** 5413]
- [11] Li N Q 2016 *Ph. D. Dissertation* (Chengdu: Southwest Jiaotong University) (in Chinese) [李念强 2016 博士学位论文 (成都: 西南交通大学)]
- [12] 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
- [13] Reidier I, Aviad Y, Rosenblush M, Kanter I 2009 *Phys. Rev. Lett.* **103** 024102
- [14] Kanter I, Aviad Y, Reidler I, Cohen E, Rosenblush M 2010 *Nat. Photon.* **4** 58
- [15] Harayama T, Sunada S, Yoshimura K, Davis P, Tsuzuki K, Uchida A 2011 *Phys. Rev. A* **83** 031803
- [16] Argyris A, Deligiannidis S, Pikasis E, Bogris A, Syvridis D 2010 *Opt. Express* **18** 18763
- [17] Zhang J Z, Wang Y C, Liu M, Xue L G, Li P, Wang A B, Zhang M J 2012 *Opt. Express* **20** 7496
- [18] Li P, Wang Y C, Zhang J Z 2010 *Opt. Express* **18** 20360
- [19] Wu J G, Tang X, Wu Z M, Xia G Q, Feng G Y 2012 *Laser Phys.* **22** 1476
- [20] Li X Z, Chan S C 2013 *IEEE J. Quantum Electron.* **49** 829
- [21] Wang A B, Li P, Zhang J G, Zhang J Z, Li L, Wang Y C 2013 *Opt. Express* **21** 20452
- [22] Li P, Zhang J G, Sang L X, Liu X L, Guo Y Q, Guo X M, Wang A B, Shore K A, Wang Y C 2017 *Opt. Lett.* **42** 2699
- [23] 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
- [24] Han T, Liu X L, Li P, Guo X M, Guo Y Q, Wang Y C 2017 *Acta Phys. Sin.* **66** 124203 (in Chinese) [韩韬, 刘香莲, 李璞, 郭晓敏, 郭冀强, 王云才 2017 物理学报 **66** 124203]
- [25] 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, 郭冀强, 张建国, 王云才 2017 物理学报 **66** 050501]
- [26] Tang X, Wu Z M, Wu J G, Deng T, Zhong Z Q, Chen J J, Xia G Q 2014 *Laser Phys. Lett.* **12** 015003
- [27] Ran C, Tang X, Wu Z M, Xia G Q 2018 *Laser Phys.* **28** 126202
- [28] Yao X J, Tang X, Wu Z M, Xia G Q 2018 *Acta Phys. Sin.* **67** 024204 (in Chinese) [姚晓洁, 唐曦, 吴正茂, 夏光琼 2018 物理学报 **67** 024204]
- [29] Li N Q, Pan W, Xiang S Y, Zhao Q C, Zhang L Y 2014 *IEEE Photon. Technol. Lett.* **26** 1886
- [30] Mu P H, Pan W, Xiang S Y, Li N Q, Liu X K, Zou X H 2015 *Mod. Phys. Lett. B* **29** 1550142
- [31] Wang Y, Xiang S Y, Wang B, Cao X Y, Wen A J, Hao Y 2019 *Opt. Express* **27** 8446
- [32] Xiang S Y, Wang B, Wang Y, Han Y N, Wen A J, Hao Y 2019 *J. Light. Technol.* **37** 3987
- [33] Xue C P, Jiang N, Qiu K, Lv Y X 2015 *Opt. Express* **23** 14510
- [34] Zhao A K, Jiang N, Wang Y J, Liu S Q, Li B C, Qiu K 2019 *Opt. Lett.* **44** 5957
- [35] Li N Q, Pan W, Locquet A, Citrin D S 2015 *Opt. Lett.* **40** 4416
- [36] Li S S, Li X Z, Chan S C 2018 *Opt. Lett.* **43** 4751
- [37] Xiang S Y, Wen A J, Pan W, Lin L, Zhang H X, Zhang H, Guo X X, Li J F 2016 *J. Light. Technol.* **34** 4221
- [38] Jiang N, Wang C, Xue C P, Li G L, Lin S Q, Qiu K 2017 *Opt. Express* **25** 14359
- [39] Jiang X X, Liu D M, Cheng M F, Deng L, Fu S N, Zhang M M, Tang M, Shum P 2016 *Opt. Lett.* **41** 1157
- [40] Ma Y T, Xiang S Y, Guo X X, Song Z W, Wen A J, Hao Y 2020 *Opt. Express* **28** 1665
- [41] Zhou P, Fang Q, Li N Q 2020 *Opt. Lett.* **45** 399
- [42] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dary J, Vo S 2001 [http://csrc.nist.gov/groups/ST/toolkit/rng/documentation\\_software.html](http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html) [2020-11-21]
- [43] Adams M J, Li N Q, Cemlyn B R, Susanto H, Henning I D 2017 *Phys. Rev. A* **95** 053869
- [44] Fang Q, Zhou P, Mu P H, Li N Q 2021 *IEEE J. Quantum Electron.* **57** 1200109.

# High-quality random number sequences extracted from chaos post-processed by phased-array semiconductor laser<sup>\*</sup>

Wu Jia-Chen<sup>1)</sup> Song Zheng<sup>1)</sup> Xie Yi-Feng<sup>1)</sup> Zhou Xin-Yu<sup>1)</sup> Zhou Pei<sup>1)2)†</sup>  
Mu Peng-Hua<sup>3)</sup> Li Nian-Qiang<sup>1)2)‡</sup>

1) (*School of Optoelectronic Science and Engineering, Collaborative Innovation Center of Suzhou Nano Science and Technology, Soochow University, Suzhou 215006, China*)

2) (*Key Lab of Advanced Optical Manufacturing Technologies of Jiangsu Province, Key Lab of Modern Optical Technologies of Education Ministry of China, Soochow University, Suzhou 215006, China*)

3) (*Institute of Science and Technology for Opto-Electronic Information, Yantai University, Yantai 264005, China*)

( Received 2 December 2020; revised manuscript received 19 December 2020 )

## Abstract

With the rapid development of the computer technology and communication technology, as well as the popularization of the Internet, information security has received much attention of all fields. To ensure the information security, a large number of random numbers must be generated. It is well accepted that random numbers can be divided into physical random numbers and pseudo random numbers. The pseudo random numbers are mainly generated based on algorithms, which can be reproduced once the seed is decoded. The physical random numbers are extracted from physical entropies. While the bandwidth of the traditional physical entropy source is quite small, the bit rate of generated physical random numbers is limited. In the literature, a lot of methods have been proposed to produce high-quality and high-speed random number sequences with the chaotic entropy source, which exhibits wide bandwidth, large amplitude and random fluctuations. Usually, a semiconductor laser with optical feedback, i.e., an external-cavity semiconductor laser (ECSL), is chosen as a chaotic entropy source to generate a chaotic signal output. However, the chaotic signal output has a high time delay characteristic, which is not conducive to the production of high-quality random numbers.

In this paper, to produce high-quality chaos with time-delay signature (TDS) being well suppressed, we propose to employ an integration-oriented phased-array semiconductor laser to post-process the original chaos generated by an ECSL. It is shown that the proposed laser array is effective in TDS suppression, which improves the quality of optical chaos. After certain necessary post-processing, high-speed and high-quality random number sequences can be achieved. In this paper, we employ the conventional post-processing techniques, which include an 8-bit analog-to-digital converter (ADC) for sampling and quantization, and m-bits least significant bit (m-LSB) and exclusive OR (XOR) for removing bias. The simulation results show that the random number sequences obtained from the chaotic entropy source comprised of an ECSL and phased-array semiconductor lasers have uniform distribution characteristic and their scatter diagram contains no obvious pattern. Meanwhile, the obtained random number sequences can pass all tests of the standard randomness benchmark, NIST SP 800-22. Additionally, based on the extensibility of phased-array semiconductor lasers, random number generators that can generate parallel random numbers are achievable.

**Keywords:** semiconductor lasers, phased-array semiconductor lasers, laser chaos, random number

**PACS:** 42.55.Px, 05.45.-a, 05.45.Pq

**DOI:** 10.7498/aps.70.20202034

<sup>\*</sup> Project supported by the National Natural Science Foundation of China (Grant Nos. 62004135, 62001317), the Natural Science Research Project of Jiangsu Higher Education Institutions, China (Grant No. 20KJA416001), and the Startup Funding of Soochow University, China (Grant No. Q415900119).

<sup>†</sup> Corresponding author. E-mail: [peizhou@suda.edu.cn](mailto:peizhou@suda.edu.cn)

<sup>‡</sup> Corresponding author. E-mail: [nli@suda.edu.cn](mailto:nli@suda.edu.cn)