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

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

姚晓洁　唐曦　吴正茂　夏光琼

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

Yao Xiao-Jie　Tang Xi　Wu Zheng-Mao　Xia Guang-Qiong

引用信息 Citation: Acta Physica Sinica, **67**, 024204 (2018)　DOI: 10.7498/aps.20171902
在线阅读 View online: http://dx.doi.org/10.7498/aps.20171902
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2018/V67/I2

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*

姚晓洁 唐曦 吴正茂† 夏光琼‡

(西南大学物理科学与技术学院, 重庆 400715)

(2017年8月26日收到; 2017年9月18日收到修改稿)

提出将正交互耦1550 nm垂直腔面发射激光器(1550 nm-VCSEL)在优化条件下输出的多路平均功率可比拟、延时特征(TDS)得到有效抑制的混沌信号作为混沌熵源, 经8位模数转换器(ADC)量化和最低有效位(m-LSB)后续处理获取多路物理随机数的方案, 并研究了系统参量对最终获取的比特序列随机性的影响. 首先, 基于VCSEL的自旋反转模型分析耦合强度和频率失谐对两个正交互耦合1550 nm-VCSEL输出动力学的影响, 初步确定利用该系统产生四路平均功率可比拟、TDS得到抑制的混沌信号所需的耦合强度和频率失谐优化范围; 在此基础上, 选择一个耦合强度值, 利用处于优化范围内的不同频率失谐下获取的四路混沌信号作为熵源, 经8位ADC量化和m-LSB后续处理得到最终的比特序列; 最后, 采用NIST Special Publication 800-22统计测试套件对获取的最终比特序列的随机性能进行测试, 确定了同时获取四路高质量随机数所需的参数范围.

关键词: 垂直腔面发射激光器, 正交互耦, 混沌熵源, 物理随机数

PACS: 42.55.Px, 05.45.Gg, 05.40.–a **DOI:** 10.7498/aps.67.20171902

1 引 言

随机数在保密通信[1]、密码学[2]、科学计算[3]等领域中具有广泛的应用. 根据产生方式的不同, 随机数可分为伪随机数和物理随机数. 伪随机数是由初始种子通过确定性算法生成的, 因伪随机数发生器获取的随机数是确定性的, 且长度有限, 存在周期性, 若应用于信息系统会存在安全隐患. 物理随机数是从物理随机现象中提取得到的, 具有不可预测、不可重复产生等特性, 因而具有更高的安全性, 更适合用于信息安全、保密通信等领域. 目前, 传统的物理随机数发生器大都使用振荡器中的频率抖动[4], 电阻热噪声[5]和电路的亚稳态等[6]真实物理现象作为随机数的熵源, 但利用这些方法产生的随机数码率受物理熵源带宽的限制, 速率多处于Mbit/s量级, 无法满足当前高速大容量通信的要求. 近年来, 基于量子随机数发生器[7−10]和光混沌随机数发生器[11−25]的方案逐渐成为研究热点. 其中, 半导体激光器(SL)的混沌输出作为物理熵源的方案可生成码率达Gbit/s量级的物理随机数, 因而受到业界的广泛关注.

日本Uchida课题组在2008年利用2路不相关的混沌激光经1位模数转换器(ADC)和异或(XOR)运算处理, 首次实时产生了1.7 Gbit/s高速随机数[11]. 该小组在2011年基于光子集成混沌激光系统获得了速率为2.08 Gbit/s的随机数[12], 在2015年借助混沌带宽增强技术获取了速率达1.2 Tbit/s的随机数[13]. 以色列Reidler小组在2009年利用8位ADC对基于外光反馈的分布

* 国家自然科学基金(批准号: 61475127, 61575163, 61775184, 11704316)和中央高校基本科研业务费专项资金(批准号: XDJK2017C063)资助的课题.

† 通信作者. E-mail: zmwu@swu.edu.cn

‡ 通信作者. E-mail: gqxia@swu.edu.cn

反馈式半导体激光器(DFB-SL)输出的混沌激光进行采样量化, 获得了速率为12.5 Gbit/s的随机数[14], 随后通过多级差分后处理技术获取了速率达300 Gbit/s的随机数[15]. 西班牙Oliver小组在2011年基于偏振旋转光反馈混沌半导体激光器改善混沌激光的随机特性, 实验获取4 Gbit/s随机数[16], 之后利用16位ADC以采样率40 GS/s进行高速采样, 并保留了最低有效位12-LSB, 从而获得了码率达480 Gbit/s的高速物理随机数[17]. 太原理工大学[18,19]以及西南交通大学[20,21]课题组都对基于混沌激光产生的物理随机数进行了相应的研究. 本课题组基于互注入DFB-SL输出的混沌激光信号, 获取并行多路高速物理随机数[22,23]. 我们注意到这一系列研究成果大都以边发射半导体激光器(EEL)输出的混沌作为熵源. 与传统的EEL相比, 垂直腔面发射激光器(VCSEL)拥有一些独特的优势[26−29], 如单纵模输出、低阈值电流、有源区体积小、光腔短、易集成为激光阵列. 在合适的参数条件下VCSEL中可能有两个正交的偏振分量(x-PC和y-PC)同时输出, 每一偏振分量输出的混沌信号均可作为混沌熵源, 为同时获取两路物理随机数提供了可能. 目前, 虽然基于VCSEL获取物理随机数已有一些报道[9,10,24], 但基于VCSEL输出的不同偏振分量混沌输出获取多路物理随机数的方案还鲜见报道. 由于在两个VCSEL构成的正交互耦系统中, 每个VCSEL都有可能同时激射两个偏振分量, 因而从理论上来说可以输出四路混沌信号, 若将其作为混沌熵源, 则具有同时产生四路随机比特序列的可能性. 如果进一步将这四路随机比特序列中相关性小的序列进行合并, 则系统具有获取速率加倍的随机比特序列的潜力.

基于此, 本文提出了基于正交互耦1550 nm-VCSEL各偏振分量输出的平均功率可比拟、时延特征(TDS)得到抑制的混沌信号来获取多路物理随机数的方案. 首先, 基于正交互耦1550 nm-VCSEL自旋反转模型, 确定两个VCSEL中x-PC和y-PC两正交偏振分量可同时输出功率相当、TDS得到较好抑制的四路混沌信号所需的频率失谐的范围; 利用两个VCSEL在优化参数条件下所产生的混沌输出作为混沌熵源, 经后续8位ADC采样和m-LSB截取的后续处理方法得到最终的四路随机比特序列; 利用NIST Special Publication 800-22统计测试套件[30]对基于不同频率失谐下VCSEL输出的混沌信号产生的随机比特序列的性能进行相关测试, 并给出相应的测试结果.

2 理论模型

根据自旋反转模型(SFM)[31], 正交互耦系统中两个VCSEL的速率方程为[32,33]

$$\begin{aligned}\frac{\mathrm{d}E_1^{x,y}}{\mathrm{d}t}=&k\left(1+\mathrm{i}\alpha\right)\left(N_1E_1^{x,y}-E_1^{x,y}\pm\mathrm{i}n_1E_1^{y,x}\right)\\&\mp\left(\gamma_\mathrm{a}+\mathrm{i}\gamma_\mathrm{p}\right)E_1^{x,y}+\eta E_2^{y,x}\left(t-\tau\right)\\&\times\exp\left[-\mathrm{i}\left(\omega_2\tau+\Delta\omega t\right)\right]+F_1^{x,y},\end{aligned}\tag{1}$$

$$\begin{aligned}\frac{\mathrm{d}E_2^{x,y}}{\mathrm{d}t}=&k\left(1+\mathrm{i}\alpha\right)\left(N_2E_2^{x,y}-E_2^{x,y}\pm\mathrm{i}n_2E_2^{y,x}\right)\\&\mp\left(\gamma_\mathrm{a}+\mathrm{i}\gamma_\mathrm{p}\right)E_2^{x,y}+\eta E_1^{y,x}\left(t-\tau\right)\\&\times\exp\left[-\mathrm{i}\left(\omega_1\tau-\Delta\omega t\right)\right]+F_2^{x,y},\end{aligned}\tag{2}$$

$$\begin{aligned}\frac{\mathrm{d}N_{1,2}}{\mathrm{d}t}=&\gamma_\mathrm{e}\Big[\mu-N_{1,2}\left(1+\left|E_{1,2}^x\right|^2+\left|E_{1,2}^y\right|^2\right)\\&+\mathrm{i}n_{1,2}\left(E_{1,2}^xE_{1,2}^{y^*}-E_{1,2}^yE_{1,2}^{x^*}\right)\Big],\end{aligned}\tag{3}$$

$$\begin{aligned}\frac{\mathrm{d}n_{1,2}}{\mathrm{d}t}=&-\gamma_\mathrm{s}n_{1,2}-\gamma_\mathrm{e}\Big[n_{1,2}\left(\left|E_{1,2}^x\right|^2+\left|E_{1,2}^y\right|^2\right)\\&+\mathrm{i}N_{1,2}\left(E_{1,2}^yE_{1,2}^{x^*}-E_{1,2}^xE_{1,2}^{y^*}\right)\Big],\end{aligned}\tag{4}$$

式中下标1, 2分别对应于VCSEL1和VCSEL2, 上标x和y分别表示VCSEL中的x-PC和y-PC; E表示光场的慢变复振幅, $|E|^2$表征光功率, N表示VCSEL导带和价带之间总的反转载流子密度, n表示自旋向上和自旋向下能级对应的载流子密度之差, k表示光场的衰减率, α表示线宽增强因子, γ_a为线性色散效应, γ_p为有源介质双折射效应, γ_e为总载流子衰减速率, γ_s为自旋反转速率, μ为归一化偏置电流, η表征VCSEL1与VCSEL2的互耦合强度, τ为激光器输出信号注入下一个激光器的延迟时间, ω_1和ω_2分别为VCSEL1, VCSEL2的中心角频率, $\Delta\omega=\omega_1-\omega_2$为激光器之间的角频率失谐, F为朗之万噪声源, 可表示为[28]

$$\begin{aligned}F_{1,2}^x=&\sqrt{\beta_\mathrm{sp}/2}\Big(\sqrt{N_{1,2}+n_{1,2}}\xi_{1,2}^1\\&+\sqrt{N_{1,2}-n_{1,2}}\xi_{1,2}^2\Big),\end{aligned}\tag{5}$$

$$\begin{aligned}F_{1,2}^y=&-\mathrm{i}\sqrt{\beta_\mathrm{sp}/2}\Big(\sqrt{N_{1,2}+n_{1,2}}\xi_{1,2}^1\\&-\sqrt{N_{1,2}-n_{1,2}}\xi_{1,2}^2\Big),\end{aligned}\tag{6}$$

式中ξ表示平均值为0、方差为1的高斯白噪声, β_sp为自发辐射速率.

通常评估时滞系统时延特征的方法有多种, 如自相关函数(SF)、互信息[34]、排列熵[35]. 本文采用

自相关函数来评估系统的时延特征. 自相关函数的定义为[34]

$$C(\Delta t)=\frac{\langle[S(t+\Delta t)-\langle S(t)\rangle][S(t)-\langle S(t)\rangle]\rangle}{\left[\langle S(t)-\langle S(t)\rangle\rangle^2\langle S(t+\Delta t)-\langle S(t)\rangle\rangle^2\right]^{1/2}}, \quad (7)$$

式中 $S(t)$ 为输出强度时间序列, $\langle\cdot\rangle$ 为时间平均值, Δt 为时移. 自相关函数的峰值及峰值所在位置呈现了输出信号的时延特征.

3 结果与讨论

从速率方程(1)—(4)式可以看出, 通过改变两正交互耦VCSEL之间的频率失谐以及耦合强度, 将导致VCSEL慢变场振幅 E 发生变化, 从而影响VCSEL输出的光功率以及稳定性. 利用四阶龙格-库塔 (Runge-Kutta) 算法, 可对速率方程(1)—(4)式进行数值求解, 得到VCSEL输出的慢变场振幅. 数值模拟中, 相关参数取值如下[36]: $k=300\ \mathrm{ns}^{-1}$, $\alpha=3$, $\gamma_\mathrm{e}=1\ \mathrm{ns}^{-1}$, $\gamma_\mathrm{s}=1000\ \mathrm{ns}^{-1}$, $\gamma_\mathrm{p}=192.1\ \mathrm{ns}^{-1}$, $\gamma_\mathrm{a}=1\ \mathrm{ns}^{-1}$, $\beta_\mathrm{sp}=10^{-6}\ \mathrm{ns}^{-1}$. 在后续讨论中, 我们假定 $\tau=3$ ns, 固定VCSEL2的中心频率 $f_2=\omega_2/(2\pi)=1.9355\times10^{14}$ Hz (对应的光波长为1550 nm), 通过调整VCSEL1的中心频率实现对频率失谐参数值的控制. 假设 $\mu=3$, 则根据激光器的弛豫振荡频率 $f_\mathrm{RO}=\sqrt{2k\gamma_\mathrm{e}(\mu-1)}/(2\pi)$, 可计算得到此时 $f_\mathrm{RO}=5.51$ GHz.

3.1 四路混沌熵源的获取

由于研究目标是基于激光器输出四路混沌信号而获取多路随机数, 因此正交互耦系统中两个VCSEL输出的四路混沌信号应该具有相比拟的平均功率. 在上述设置参数条件下, 单个自由运行的1550 nm-VCSEL中只有 y-PC 起振, 而 x-PC 被抑制. 当两VCSEL之间存在正交互耦合时, 通过改变耦合强度 η 和频率失谐 $\Delta f=(\omega_1-\omega_2)/(2\pi)$, 可对激光器中的不同偏振分量输出功率进行调控. 图1所示为正交互耦合VCSEL输出的偏振分量在 η 和 Δf 构成的参数空间的演化. 图中黄色区域表示 x-PC 占主导 (x-PC 的输出功率为 y-PC 输出功率的10倍以上), 浅绿色区域表示 y-PC 占主导 (y-PC 的输出功率为 x-PC 输出功率的10倍以上), 深绿色区域表示 x-PC 和 y-PC 双模共存输出 (相对功率之比在10 dB 以下)[37]. 从图1可以看出VCSEL1, VCSEL2呈现双模共存的区域分布是不同的, 存在镜像反演的关系. 在图1中白色虚线围成的区域内, 可使VCSEL1和VCSEL2输出的四个分量具有可比拟的输出功率.

图1确定了使两个正交互耦合的VCSEL输出四路平均功率相比拟的信号所需的参数范围. 还需要确定VCSEL输出的四路信号均为混沌信号所需的参数范围. 图2所示为正交互耦VCSEL在 η 和 Δf 构成的参数空间各偏振分量输出的动力学状态分布, 图中不同的颜色代表不同的动力学状态, 各动力学状态的判定标准参见文献[38]. 结合图1和图2可得, 当耦合强度和频率失谐分别满足 $50\ \mathrm{ns}^{-1}\leqslant\eta\leqslant100\ \mathrm{ns}^{-1}$, $-10\ \mathrm{GHz}\leqslant\Delta f\leqslant10\ \mathrm{GHz}$ 条件时, 两个激光器中的各偏振分量均呈现混沌输出, 且具有相比拟的平均功率.

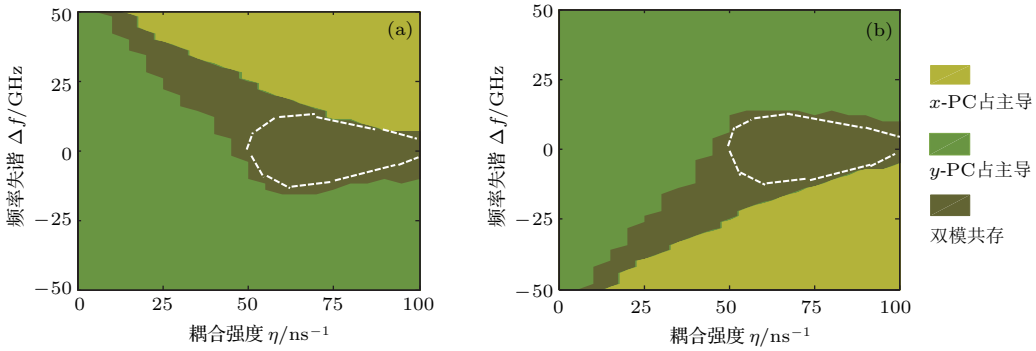

图1 VCSEL输出两偏振分量的相对强弱在 η 和 Δf 构成的参数空间中的演化 (白色虚线围成的区域表示激光器处于双模共存状态) (a) VCSEL1; (b) VCSEL2

Fig. 1. Evolution of the relative strength between x-PC and y-PC in two orthogonally and mutually coupled VCSELs in the parameter space of η and Δf (the regions surrounded by white dashed lines are for two-modes co-existing simultaneously in lasers): (a) VCSEL1; (b) VCSEL2.

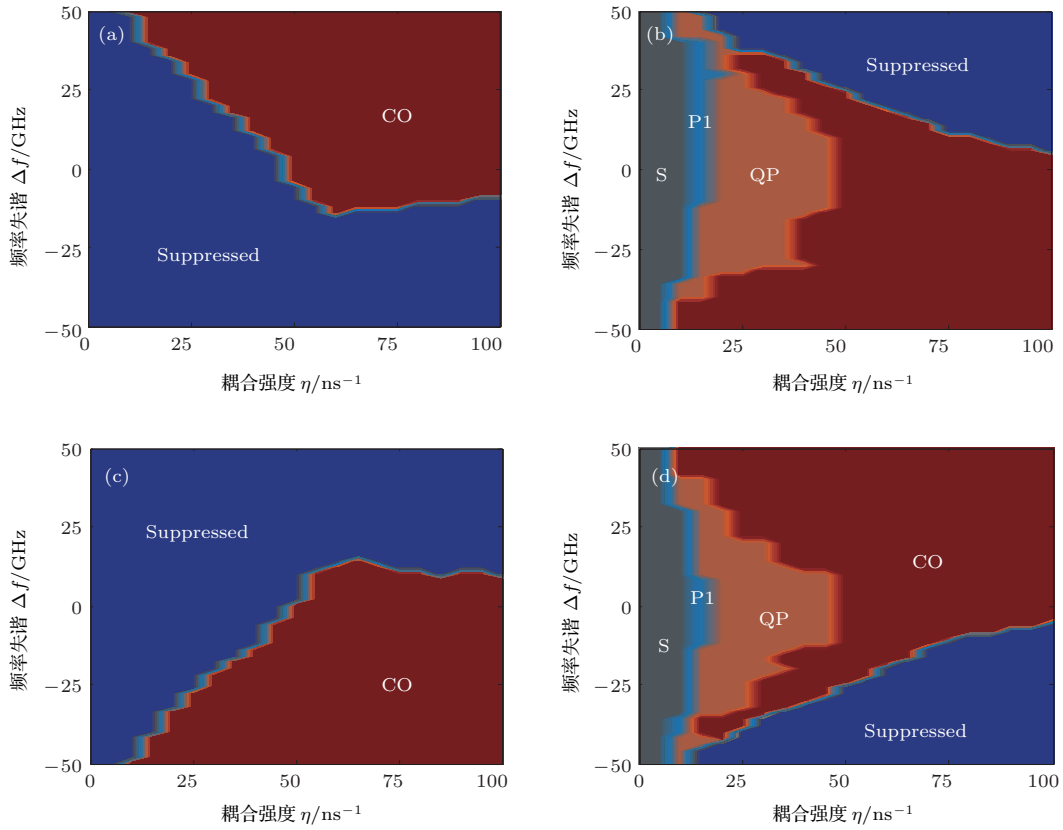

图 2 VCSEL 各偏振分量输出的动力学状态在 η 和 Δf 构成的参数空间中的分布 (S 为稳态; P1 为单周期态; QP 为准周期态; CO 为混沌态; Suppressed 为模式被抑制) (a) VCSEL1 x-PC; (b) VCSEL1 y-PC; (c) VCSEL2 x-PC; (d) VCSEL2 y-PC

Fig. 2. Distribution of dynamical states of x-PC and y-PC in two orthogonally and mutually coupled VCSELs in the parameter space of η and Δf (S is for steady state, P1 is for periodic state, QP is for quasi-periodic state, CO is for chaotic state, and Suppressed is for the case that the corresponding PC is suppressed): (a) VCSEL1 x-PC; (b) VCSEL1 y-PC; (c) VCSEL2 x-PC; (d) VCSEL2 y-PC.

已有的研究证明[11,14], 若采用具有明显 TDS 的混沌信号作为物理熵源, 将会导致所获取随机比特序列的统计特性劣化. 因此, 需要分析耦合参数对正交互耦合系统输出混沌信号 TDS 的影响, 以确定能同时产生四路平均功率相比拟、TDS 得到较好抑制的混沌信号所需的耦合参数范围. 基于前述自相关函数分析方法分析正交互耦系统输出混沌信号的 TDS, 利用自相关函数时移 Δt 在 $2\tau = 6$ ns 附近的 [5 ns, 7 ns] 区间内的最大峰值 σ_1 来标定延时特性的明显程度. σ_1 越大, 系统输出混沌信号的 TDS 越明显. 图 3 所示为不同耦合强度和频率失谐下四路混沌信号输出的 TDS. 图中不同颜色代表不同的 σ_1 值, 白色实线表示 $\sigma_1 = 0.4$ 的边界. 从图中可以看出, 当耦合强度 55 ns^{-1} $\leqslant \eta \leqslant$ 65 ns^{-1} 时, σ_1 的值大都小于 0.4; 而对于更高的耦合强度, 在所选取的频率失谐范围内, 两个 VCSEL 输出的四路混沌信号的 TDS 比较明显.

若考虑到产生的高速随机比特序列的合并, 则还需要考察这四路混沌信号的互相关性. 基于文献 [39] 中互相关的定义, 计算系统中两个 VCSEL 输出的四路信号之间的互相关峰值 σ_2 随 η 和 Δf 的变化, 如图 4 所示. 图中不同的颜色代表不同的 σ_2 值, 黑色虚线表示 $\sigma_2 = 0.4$ 的边界. 从图中看出, 在满足四路混沌信号输出的 TDS 峰值 σ_1 均小于 0.4 的区域 55 ns^{-1} $\leqslant \eta \leqslant$ 65 ns^{-1}, -10 GHz $\leqslant \Delta f \leqslant$ 10 GHz 范围内, 除同一 VCSEL 的两个模式之间的互相关峰值 σ_2 不小于 0.4 之外 (图 4 (b) 和图 4 (e)), 其余互相关峰值 σ_2 均小于 0.4. 因此, 除采用两个激光器输出的四路混沌信号作为混沌熵源可直接产生四路随机数外, 还可以合并四路中相关性小的混沌信号所生成的随机比特序列以获取两路速率加倍的随机数序列.

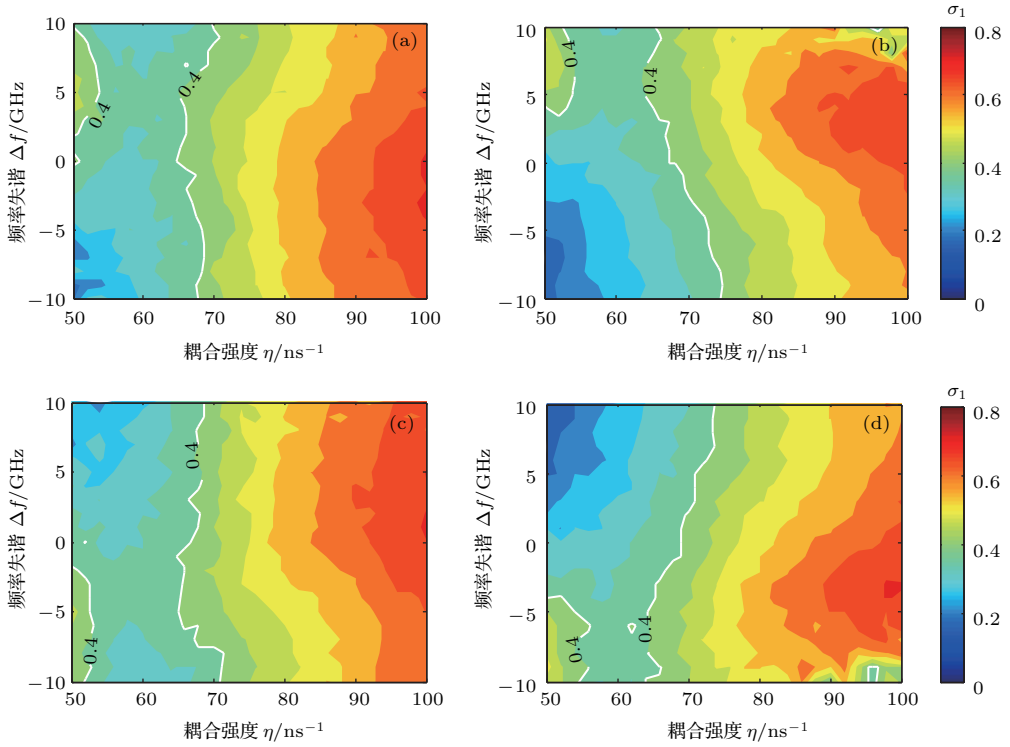

图 3 系统输出四路混沌信号的自相关函数峰值 σ_1 在 η 和 Δf 构成的参数空间中的演化 (白色实线表示 $\sigma_1 = 0.4$ 的边界) (a) VCSEL1 x-PC; (b) VCSEL1 y-PC; (c) VCSEL2 x-PC; (d) VCSEL2 y-PC

Fig. 3. Mappings of σ_1 in the parameter space of η and Δf for four channels of chaotic signals output from the system, where white solid lines label the boundary of $\sigma_1 = 0.4$: (a) VCSEL1 x-PC; (b) VCSEL1 y-PC; (c) VCSEL2 x-PC; (d) VCSEL2 y-PC.

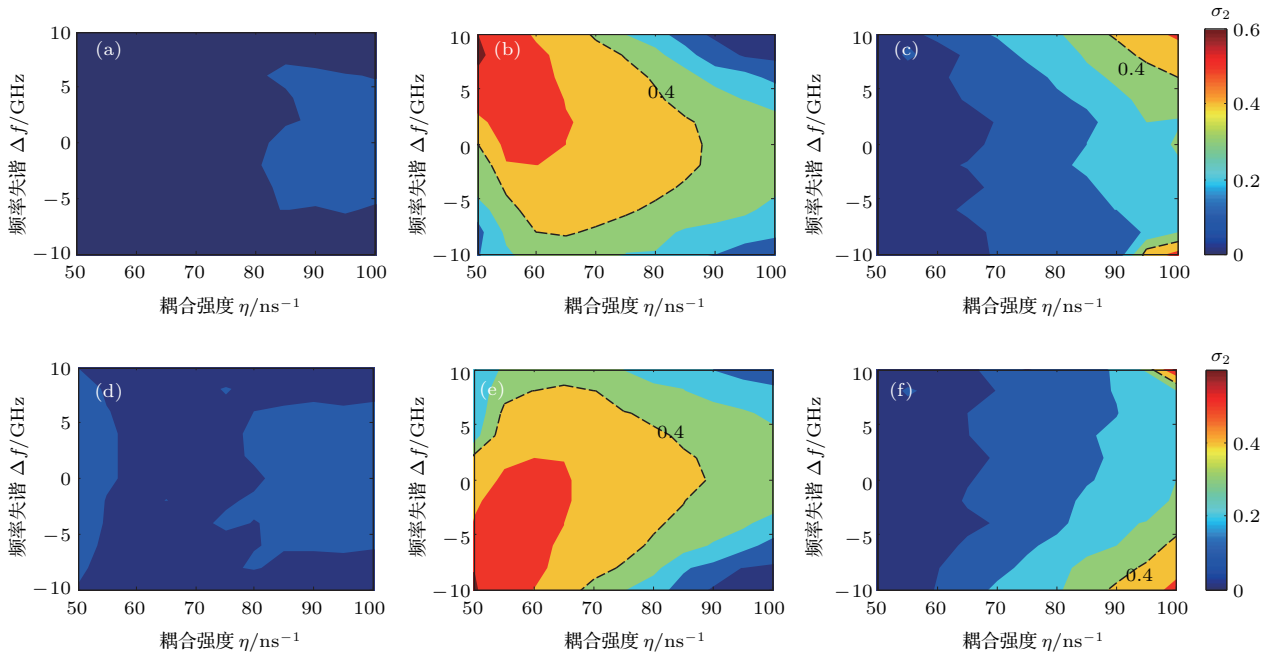

图 4 系统各偏振分量输出混沌序列之间的互相关峰值 σ_2 随 η 和 Δf 的变化 (黑色虚线表示 $\sigma_2 = 0.4$ 的边界) (a) SL1 x-PC 与 SL2 x-PC; (b) SL1 x-PC 与 SL1 y-PC; (c) SL1 x-PC 与 SL2 y-PC; (d) SL1 y-PC 与 SL2 y-PC; (e) SL2 x-PC 与 SL2 y-PC; (f) SL1 y-PC 与 SL2 x-PC

Fig. 4. Evolution of σ_2 between different polarization components in the parameter space of η and Δf, where the black dashed lines label the boundary of $\sigma_2 = 0.4$: (a) SL1 x-PC and SL2 x-PC; (b) SL1 x-PC and SL1 y-PC; (c) SL1 x-PC and SL2 y-PC; (d) SL1 y-PC and SL2 y-PC; (e) SL2 x-PC and SL2 y-PC; (f) SL1 y-PC and SL2 x-PC.

3.2 比特序列的产生和测试结果分析与讨论

在上述优化的参数范围内, 给定耦合强度, 对不同频率失谐下获取的四路混沌信号作为物理熵源, 经采样频率为20 GHz的8位ADC量化和m-LSB后续处理方法得到的比特序列的随机性进行分析与讨论. 从图3 TDS演化中可以得到, 两个VCSEL之间关于频率失谐存在镜面对称关系[40], 因此下文讨论中只针对正失谐. 给定$\eta = 60\ \mathrm{ns}^{-1}$, Δf 分别取0, 5, 10 GHz进行分析.

利用NIST Special Publication 800-22统计测试套件对四路随机比特序列的随机性进行评估. 该测试套件由15个测试项组成, 每个测试项的结果用p值表示, 若p值大于显著水平$\alpha = 0.01$, 则说明随机数列通过了相应的测试. 采用1000组1 Mbit样本序列进行测试, 当每项测试的p值高于显著水平α的比率大于0.9806, 并且所有p 值的均匀性(用P-value表征)大于0.0001 时, 认为输出的随机比特序列具有良好的随机性. 另外, 对于包含多个子测试的测试项, 以其中最差的结果作为评判依据. 图5所示为ADC采样速率为20 GHz时, m-LSB处理后获得的二进制比特序列通过NIST统计测试套件测试的项数随频率失谐的变化. 从图中可以看出, 随着频率失谐的增大, 通过检测的项数总体呈现下降趋势. 对于采用2-LSB(图5 (a))的情况, 在$\Delta f = 0$ GHz和$\Delta f = 5$ GHz 时, 两个VCSEL的四路混沌信号输出通过的项数均为15, 说明此时作为混沌熵源的四路混沌数据序列经过8位ADC采样后, 保留最后2位LSB能够获得概率分布均匀、不确定性较好的随机序列. 而对于采用3-LSB(图5 (b))和4-LSB (图5 (c))的情况, 不同频率失谐下四路二进制比特序列均不能完全通过测试, 说明此时四路混沌数据序列经过8位ADC采样后, 随着LSB保留位数的增加, 取值区间增多, 序列概率分布函数的均匀性变差, 不确定性逐渐劣化, 难以达到NIST统计测试套件的指标要求. 尽管如此, 在两个VCSEL频率失谐小于5 GHz的条件下, 仅通过2-LSB这一简单的后续处理方式可获得四路速率为40 Gbit/s、能通过NIST统计测试套件全部测试项目的随机比特序列. 需要指出的是, 由于本文仅采用m-LSB这一简单的后续处理方式, 作为熵源的四路混沌数据序列的统计特性至关重要, 因此需要通过优化系统参量尽可能提高混沌数据序列的统计特性.

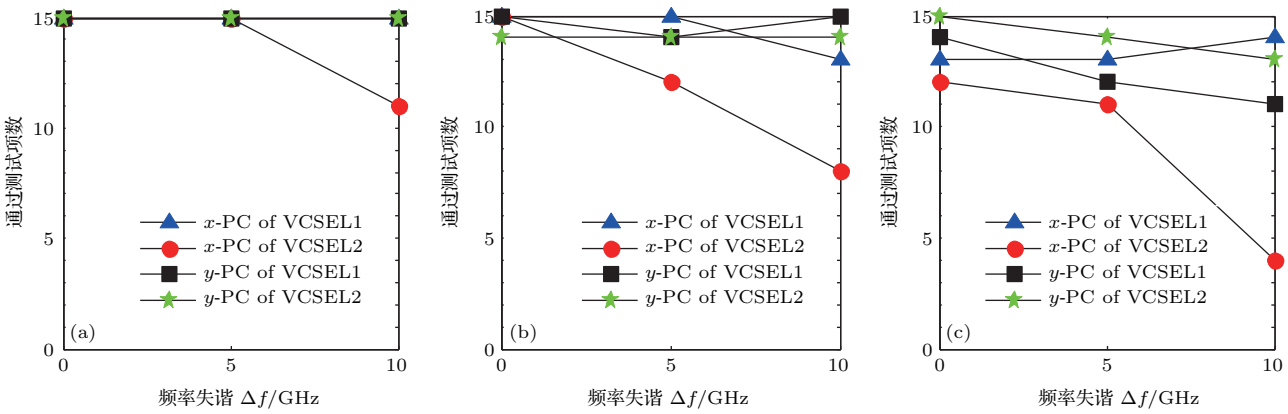

图5 ADC采样频率为20 GHz时m-LSB处理后获得的二进制比特序列通过NIST Special Publication 800-22软件测试的项数随频率失谐的变化 (a) 2-LSB; (b) 3-LSB; (c) 4-LSB

Fig. 5. Dependence of the number of passed terms in NIST Special Publication 800-22 test for binary sequence on the frequency detuning under ADC with a sampling rate of 20 GHz after m-LSB processing: (a) 2-LSB; (b) 3-LSB; (c) 4-LSB.

4 结 论

提出了基于正交互耦1550 nm-VCSEL输出的四路平均功率可比拟、TDS得到抑制的混沌信号来获取多路物理随机数的方案. 首先, 基于自旋反转模型, 利用自相关函数方法, 确定了两个1550 nm-VCSEL均能输出平均功率可比拟、TDS得到抑制的四路混沌信号所需的最优参数范围; 在优化的参数范围内, 选定耦合强度, 使用不同频率失谐

下系统输出的四路混沌信号作为物理熵源, 经速率为20 GHz的8 位ADC采样量化以及m-LSB处理后得到了四路随机比特序列; 最后, 利用NIST Special Publication 800-22统计测试套件对得到的四路随机比特序列的性能进行评估. 结果表明: 将两个正交互耦VCSEL系统在优化条件下输出的四路混沌信号作为熵源, 经过采样频率为20 GHz的ADC量化后, 再经2-LSB 处理得到的码率为40 Gbit/s的四路随机比特序列均可通过NIST统计测试套件的检测.

参考文献

[1] Gallager R G 2008 *Principles of Digital Communication* (New York: Cambridge University Press) pp199–244

[2] Stinson D R 2005 *Cryptography: Theory and Practice* (Ontario: CRC Press) pp423–452

[3] Asmussen S, Glynn P W 2007 *Stochastic Simulation: Algorithms and Analysis* (New York: Springer-Verlag) pp30–65

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

[5] Petrie C S, Connelly J A 2000 *IEEE Trans. Circuits Syst. I* **47** 615

[6] Danger J L, Guilley S, Hoogvorst P 2009 *Microelectron. J.* **40** 1650

[7] Gabriel C, Wittmann C, Sych D, Dong R, Mauerer W, Andersen U L, Marquardt C, Leuchs G 2010 *Nat. Photonics* **4** 711

[8] Marangon D G, Vallone G, Villoresi P 2017 *Phys. Rev. Lett.* **118** 060503

[9] Zhu M Y, Liu Y, Yu Q F, Guo H 2012 *Laser Phys. Lett.* **9** 775

[10] Guo H, Tang W Z, Liu Y, Wei W 2010 *Phys. Rev. E* **81** 051137

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

[13] Sakuraba R, Iwakawa K, Kanno K, Uchida A 2015 *Opt. Express* **23** 1470

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

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

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

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

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

[19] Li P, Jiang L, Sun Y Y, Zhang J G, Wang Y C 2015 *Acta Phys. Sin.* **64** 230502 (in Chinese) [李璞, 江镭, 孙媛媛, 张建国, 王云才 2015 物理学报 **64** 230502]

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

[21] Li N Q, Pan W, Xiang S Y, Zhao Q C, Zhang L Y 2014 *IEEE Photon. Technol. Lett.* **26** 1886

[22] Tang X, Wu Z M, Wu J G, Deng T, Fan L, Zhong Z Q, Chen J J, Xia G Q 2015 *Laser Phys. Lett.* **12** 015003

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

[24] Virte M, Mercier E, Thienpont H, Panajotov K, Sciamanna M 2014 *Opt. Express* **22** 17271

[25] Zhang L M, Pan B W, Chen G C, Guo L, Lu D, Zhao L J, Wang W 2017 *Sci. Rep.* **8** 45900

[26] Iga K 2000 *IEEE J. Sel. Top. Quantum Electron.* **6** 1201

[27] Koyama F 2006 *J. Lightwave Technol.* **24** 4502

[28] Xiang S Y, Pan W, Luo B, Yan L S, Zou X H, Jiang N, Li N Q, Zhu H N 2012 *IEEE Photon. Technol. Lett.* **24** 1267

[29] Liu Q X, Pan W, Zhang L Y, Li N Q, Yan J 2015 *Acta Phys. Sin.* **64** 024209 (in Chinese) [刘庆喜, 潘炜, 张力月, 李念强, 阎娟 2015 物理学报 **64** 024209]

[30] Rukhin A, Soto J, Nechvatal J, Smid M, Barker E, Leigh S, Levenson M, Vangel M, Banks D, Heckert A, Dray J, Vo S 2010 *NIST Special Publication 800-22 (Rev.1)* (Gaithersburg: National Institute of Standards and Technology)

[31] Martin-Regalado J, Prati F, San Miguel M, Abraham N B 1997 *IEEE J. Quantum Electron.* **33** 765

[32] Sciamanna M, Gatare I, Locquet A, Panajotov K 2007 *Phys. Rev. E* **75** 056213

[33] Xiang S Y, Pan W, Luo B, Yan L S, Zou X H, Li N Q 2013 *IEEE J. Sel. Top. Quantum Electron.* **19** 1700108

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

[35] Bandt C, Pompe B 2002 *Phys. Rev. Lett.* **88** 174102

[36] Torre M, Hurtado A, Quirce A, Valle A, Pesquera L, Adams M 2011 *IEEE J. Quantum Electron.* **47** 92

[37] Yang F, Tang X, Zhong Z Q, Xia G Q, Wu Z M 2016 *Acta Phys. Sin.* **65** 194207 (in Chinese) [杨峰, 唐曦, 钟祝强, 夏光琼, 吴正茂 2016 物理学报 **65** 194207]

[38] Cao T, Lin X D, Xia G Q, Chen X H, Wu Z M 2012 *Acta Phys. Sin.* **61** 114202 (in Chinese) [曹体, 林晓东, 夏光琼, 陈兴华, 吴正茂 2012 物理学报 **61** 114202]

[39] Quirce A, Valle A, Thienpont H, Panajotov K 2016 *J. Opt. Soc. Am. B* **33** 90

[40] Wu J G, Wu Z M, Xia G Q, Feng G Y 2012 *Opt. Express* **20** 1741

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

Yao Xiao-Jie Tang Xi Wu Zheng-Mao† Xia Guang-Qiong‡

(*School of Physical Science and Technology, Southwest University, Chongqing 400715, China*)

(Received 26 August 2017; revised manuscript received 18 September 2017)

Abstract

Physical random number, which is non-reproducible and non-periodical, has attracted much attention due to its potential applications in various fields such as secure communication, statistical analysis, and numerical simulation. Recently, fast physical random number generators based on optical chaotic entropy sources have been demonstrated to reach a rate of up to several hundreds of Gbit/s. Although many efforts have been made to optimize the schemeis of chaotic-based random number generation, most of them are based on distributed feedback semiconductor lasers and can only generate single-channel physical random number. After taking into account the costs and technological applications, the multi-channel physical random number generation technique needs developing. On the other hand, vertical-cavity surface-emitting lasers (VCSELs) can simultaneously emit two orthogonally polarized components under appropriate parameter conditions, and then each polarized component can be used as an entropy source for generating random number. As a result, VCSEL-based chaotic entropy sources may be suitable for multi-channel random number generation. In this work, a scheme for achieving multi-channel physical random number is proposed. Also the influence of the coupling parameters on the performance of the randomness of final bit sequences is investigated. For such a scheme, two orthogonally mutually coupled VCSELs are used to supply four-channel chaotic signals with a comparable output power and weak time-delay signature (TDS). The four-channel chaotic signals, which serve as chaotic entropy, are quantized by 8-bit analog-to-digital converters (ADCs) with 20 GHz sampling rate, and then the m least significant bit (m-LSB) post-processing method is adopted for generating final four-channel random bit sequences. Firstly, based on the spin-flip mode of VCSELs, the influences of coupling strength and frequency detuning on the dynamics of two orthogonally mutually coupled 1550 nm VCSELs are analyzed. Next, the optimized parameter regions for generating four-channel chaotic signals with comparable output power and weak TDS are preliminarily determined. For a given optimized value of coupling strength and different frequency detunings within the optimized parameter regions, the generated four-channel chaotic signals are taken as the entropy sources for obtaining final bit sequence by quantizing the 8-bit ADC and m-LSB post-processing. Finally, the randomness of the four final bit sequences is tested by NIST SP 800-22 statistical test suite, and the regions of preferred coupling parameters for simultaneously generating four-channel random numbers are determined.

Keywords: vertical-cavity surface-emitting lasers, orthogonally mutual coupling, chaotic entropy source, physical random number

PACS: 42.55.Px, 05.45.Gg, 05.40.–a **DOI:** 10.7498/aps.67.20171902

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61475127, 61575163, 61775184, 11704316) and the Fundamental Research Funds for the Central Universities of China (Grant No. XDJK2017C063).

† Corresponding author. E-mail: zmwu@swu.edu.cn

‡ Corresponding author. E-mail: gqxia@swu.edu.cn