基于 Si_3N_4 微环混沌光频梳的 Tbit/s 并行实时物理随机数方案*

王永博[1)2)#] 唐曦[1)2)#] 赵乐涵[1)2)#] 张鑫[1)2)] 邓进[1)2)] 吴正茂[1)2)]
杨俊波[4)] 周恒[3)†] 吴加贵[1)2)‡] 夏光琼[1)2)††]

1) (西南大学物理科学与技术学院, 重庆 400715)

2) (西南大学, 微纳结构光电子学重庆市重点实验室, 重庆 400715)

3) (电子科技大学, 光纤传感与通信教育部重点实验室, 成都 610097)

4) (国防科技大学物质与材料科学实验中心, 长沙 410073)

(2023 年 12 月 5 日收到; 2024 年 1 月 18 日收到修改稿)

本文结合片上 Si_3N_4 超高 Q 微环的混沌光频梳和高速现场可编程门阵列, 提出并实验验证了一种超高速的并行实时物理随机数方案. 结果表明, Si_3N_4 超高 Q 微环实验得到的光频梳齿包含数百个信道, 通过调节 Si_3N_4 微环的工作状态使其处于光学混沌态, 从而成为性能优良的物理熵源. 采用现场可编程门阵列 (FPGA) 板载的多位模数转换器, 对滤波后频梳的光混沌信号进行离散采样量化, 生成 8 位二进制比特流. 对该比特流进行实时的自延迟异或处理, 并保留 4 位最低有效位, 实验最终实现了单信道实时速率达 5 Gbits/s 的合格物理随机比特流. 结合实验中数目达 294 的混沌光频梳齿, 本方案的并行实时随机数的吞吐量可望达到 1.74 Tbits/s. 这些结果可为实时物理随机数源提供集成、超高速的新可选方案.

关键词: 物理随机数, 实时, 混沌, 光频梳, 现场可编程门阵列

PACS: 42.65.–k, 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.73.20231913

1 引 言

混沌系统有对初值极度敏感、宏观不可预测性等特点, 因此在私人通信、抗干扰传感、强化学习、密钥分发、多输入多输出 (MIMO) 雷达和随机调制连续波 (RMCW) 激光雷达等领域都有广泛的应用潜力[1–8]. 近年来, 激光混沌因其具有随机波动大、带宽高、易获取等优点, 特别适合作为熵源, 因此在高速物理随机数 (PRN) 生成领域备受关注[9–26].

近年来, 相关研究工作多关注于通过优化光源性能, 增强输出混沌激光的带宽来提升 PRN 的生成速率. 目前已报道的混沌激光熵源带宽已高达 50 GHz 以上, 通过大带宽光电探测器和示波器进行采样量化后, 可产生离线速率为 640 Gbits/s 的 PRN[13]. 然而需要指出的是, 单一通道的 PRN 输出速率上限较易受制于系统硬件瓶颈, 为了获得更

* 国家自然科学基金 (批准号: 61775184, 61875167)、重庆市自然科学基金杰出青年基金 (批准号: cstc2021jcyj-jqX0027) 和西南大学创新研究 2035 先导计划 (批准号: SWU-XDPY22012) 资助的课题.

同等贡献作者.

† 通信作者. E-mail: zhouheng@uestc.edu.cn

‡ 通信作者. E-mail: mgh@swu.edu.cn

†† 通信作者. E-mail: gqxia@swu.edu.cn

高的数据吞吐量, 文献 [14—18] 报道了通过使用多光源组合实现系统并行化输出的方案. 这些方案大都为离线方案, 尽管能够将 PRN 的离线生成速率提高到 Tbits/s 量级, 但并行通道数量较少且系统架构相对复杂, 不利于实现实时 PRN 的高速稳定输出. 最近, 我们注意到混沌光频梳[27,28]有潜力解决上述问题. 混沌光频梳具有高度非线性和复杂动力学特性, 其每个梳齿都表现出混沌态振荡, 通过波分复用技术将每个梳齿信道提取出来, 从而能够获得大规模并行输出的混沌熵源. 这为 PRN 并行化生成方案提供了巨大的便利.

本文提出并实验验证了一种基于 Si_3N_4 混沌光频梳的超高速并行 PRN 实时产生方案. 在微环芯片上可以同时输出数百个波长通道, 且每个通道均进入混沌态. 通过滤波后提取单信道的混沌信号作为熵源, 采用 8 位模数转换器 (ADC) 对其采样量化后生成初始比特序列. 随后用现场可编程门阵列 (FPGA) 对初始比特序列进行延时异或 (XOR) 处理[29]并保留 4 位最低有效位 (LSB), 最终生成单信道速率为 5 Gbits/s 的实时 PRN. 实验中, 通过高速 ADC 实时采样, 将复杂混沌信号量化为实时比特流. 随后, 获得的原始比特流通过 FPGA 进行实时逻辑处理和变换, 最终以高速随机比特流或码型图的形式实时输出[30,31]. 由于实验得到的混沌光频梳的梳齿信道数高达 294 根, 因此可以生成数据吞吐量高达 1.74 Tbits/s (5 Gbits/s× 294 =1.47 Tbits/s) 的并行实时 PRN. 该方案产生的实时 PRN 具有良好的统计特性, 能够通过 NIST SP 800-22 统计检验套件的全部测试项目. 本文工作有望极大提升 PRN 发生器的实时数据吞吐量, 在大规模 MIMO 等前沿技术领域有广泛的应用价值.

2 基于微梳的大规模并行混沌信号生成

基于混沌光频梳结合 FPGA 产生并行实时 PRN 的实验装置如图 1(a) 所示. 在实验中, 可调谐半导体激光器作为泵浦激光源, 将连续的泵浦光注入到微谐振器来产生混沌光频梳. 如图 1(b) 所示, 实验所用为圆形的 Si_3N_4 微环, 其自由光谱范围 (free spectral range, FSR) 值约为 100 GHz, 则对应微环直径约为 400 μm. 如图 1(d) 所示, 环在 1550 nm 的色散曲线接近零, 这有利于产生宽带光频梳[32,33]. 进一步如图 1(e) 的冷腔传输曲线所示, 在微环 1550 nm 附近的模式线宽约 0.0007 nm, 则其负载 Q 值根据估算公式 $Q=\dfrac{\lambda}{\Delta\lambda}=1550\ \text{nm}/0.0007\ \text{nm}\approx 2.2\times10^6$. Si_3N_4 材料具有足够的光学非线性使频率梳齿达到混沌态[34]. 较高的泵浦光能量可以使谐振腔生成数量庞大的混沌光梳齿. 因此将输出泵浦光的功率通过掺铒光纤放大器 (EDFA) 放大到 32 dBm, 通过准直镜使能量进入微环内, 对应的微腔的片上功率 (即 on-chip power) 约为 29.75 dBm. 在环中, 由于高 Q 环的储能作用, 环中光强度可超过 Si_3N_4 材料的非线性阈值而激发显著的 Kerr 非线性效应. 在这个过程中, Kerr 效应还会引发相位调制和频率漂移, 导致不同梳齿间的调制不稳定行为[33]. 当泵浦光波长不断靠近微环的本证谐振波长值时, 调制不稳定行为越来越强烈, 而最终得到大量的并行的混沌光频梳齿. 在测量过程中, 须采用温度控制器保证微谐振器的温度稳定在 37.5 ℃. 在稳定的温度条件下, 光频梳幅值波动总体平稳、输出功率保持恒定. 此外, 可利用光纤布拉格光栅 (FBG) 抑制泵浦光所在梳齿高度, 使附近各梳齿的能量分布尽可能均衡.

随后, 通过多路分配器对产生的光频梳进行滤波, 将滤波后各个波长的梳齿分别输入到光电探测器中转化为混沌电信号. 通过采样频率为 1.25 GHz 的 ADC 对熵源信号采样量化为初始比特序列后, 利用 FPGA 对序列进行自延迟异或处理并保留 4 位最低有效位, 最终实现实时 PRN 输出. 图 1(c) 呈现的是 FPGA 的电路板 (5SGXEA7K2F40C2N), 是由 Altrea 公司生产的 Stratix®V GX 系列的板卡. 板卡包含的资源丰富, 其中有可配置逻辑块 (CLB) 234720 个, 总 RAM 位数为 59939840 位以及可用 I/O 数为 696 个. 板卡的最高数据速率能力为 12.5 Gb/s. 在图 1(d) 中, 通过超高分辨率布里渊光谱分析仪 (BOSA), 可以直观观察到光频梳整体呈梯形状, 覆盖范围从 O 波段到 L 波段, 重复频率为 100 GHz, 覆盖 1430 —1675 nm 的数百个波长通道, 信噪比可达 60 dBm. 图 1(d) 中 C 波段的梳齿能量分布较高, 功率变化相对不明显. 为了详细观察光频梳的梳齿, 图 1(e) 中展示了部分 C 波段的光谱放大视图, 其覆盖波长范围从 1535 nm 到 1565 nm, 自由光谱范围小于 0.8 nm.

3 光频梳混沌特性分析

为了详细讨论各梳齿的混沌特性, 从混沌频率梳中分别滤出多个波长的梳齿进行分析. 图 2 展示

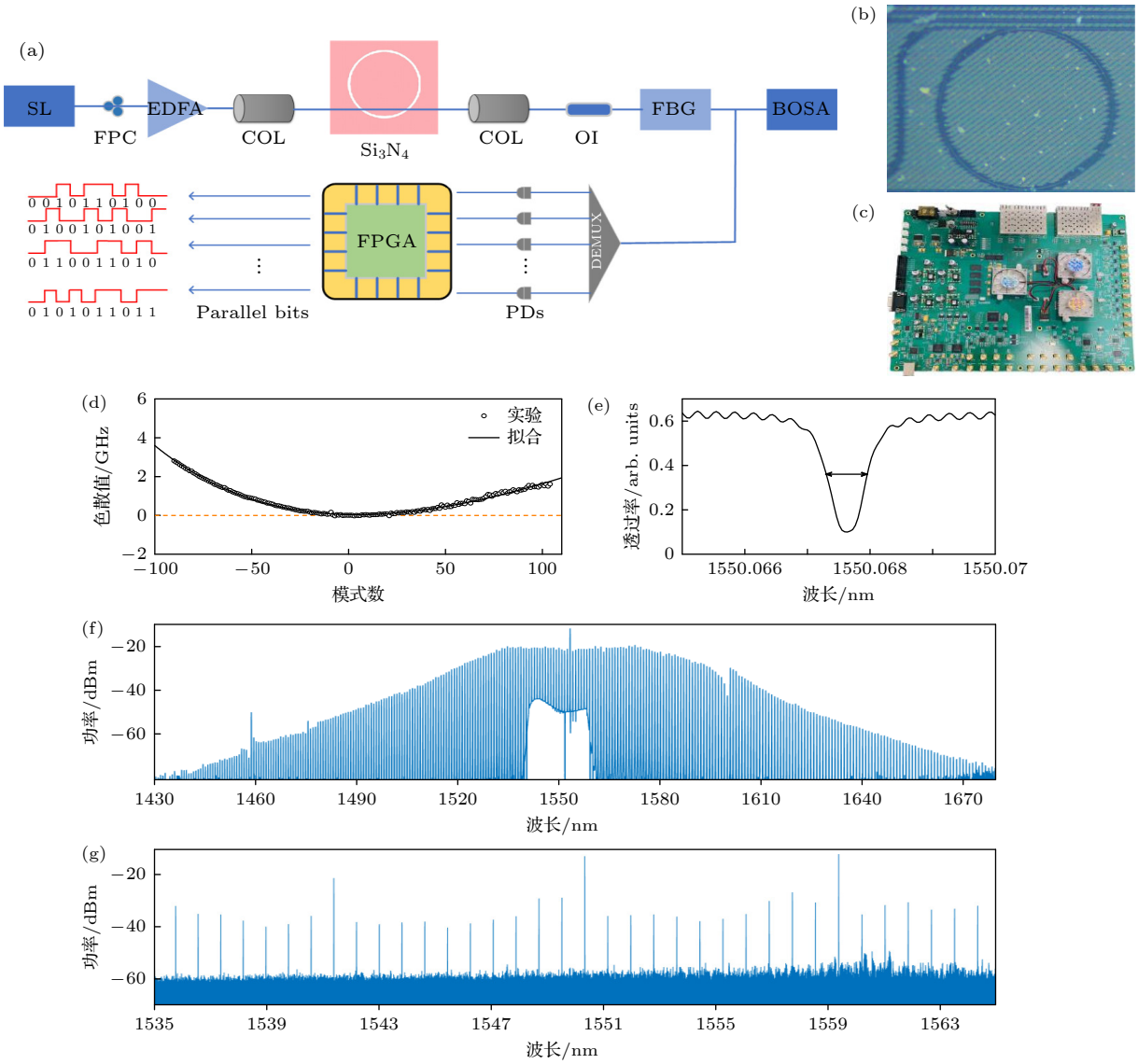

图 1 基于混沌光频梳的实时大规模并行混沌信号生成 (a) 基于大规模并行光子集成电路实时 PRN 发生器实验装置, 其中 SL 为半导体激光器, FPC 为光纤偏振控制器, EDFA 为掺铒光纤放大器, COL 为准直镜头, OI 为光隔离器, FBG 为光纤布拉格光栅, DEMUX 为多路分配器, PD 为光电探测器, BOSA 为布里渊光谱分析仪; (b) Si_3N_4 微谐振器图像; (c) FPGA 电子板; (d) 色散曲线; (e) 冷腔传输曲线; (f) 生成的混沌梳的光谱; (g) 混沌微梳从 1535 nm 放大到 1565 nm

Fig. 1. Microcomb based real-time massively parallel chaotic signal generation: (a) Experimental setup for real-time PRN generator with massively parallel photonic integrated circuit, SL represents semiconductor laser, FPC represents fiber polarization controller, EDFA represents erbium-doped optical fiber amplifier, COL represents collimating lens, OI represents isolator, FBG represents fiber Bragg grating, DEMUX represents demultiplexer, PD represents photodetector, BOSA represents Brillouin optical spectral analyzer; (b) image of Si_3N_4 microresonator; (c) FPGA electronic board; (d) dispersion curve; (e) cold cavity transmission line; (f) the optical spectrum of the generated chaotic comb; (g) zoom in of chaotic microcomb covering from 1535 nm to 1565 nm.

了对不同波长的梳齿进行滤波处理的结果, 通过各梳齿信道的输出光谱、时间序列以及时间序列对应的自相关曲线来分析混沌信号的质量. 图 2(a1) 展示了 1536.33 nm 处的梳齿的光谱细节. 通过图示发现, 梳齿的光谱明显展宽呈现混沌态特征. 梳齿的时域信号如图 2(b1) 所示, 由于腔内场经历了时空混沌, 时间序列的振幅抖动迅速而剧烈, 呈现无序特征. 图 2(c1) 给出了与图 2(b1) 中时间序列对应的自相关曲线. 我们注意到自相关曲线并未出现明显的时延特征峰值. 这表明该混沌信号没有明显的弱周期成分, 统计特性较好, 能够作为高质量的混沌熵源. 此外, 我们也对波长在 1540.94, 1541.33 和 1551.32 nm 的混沌梳齿分别进行了分析, 如图 2 中第 2 行—第 4 行所示. 上述表明, 所有梳齿均处

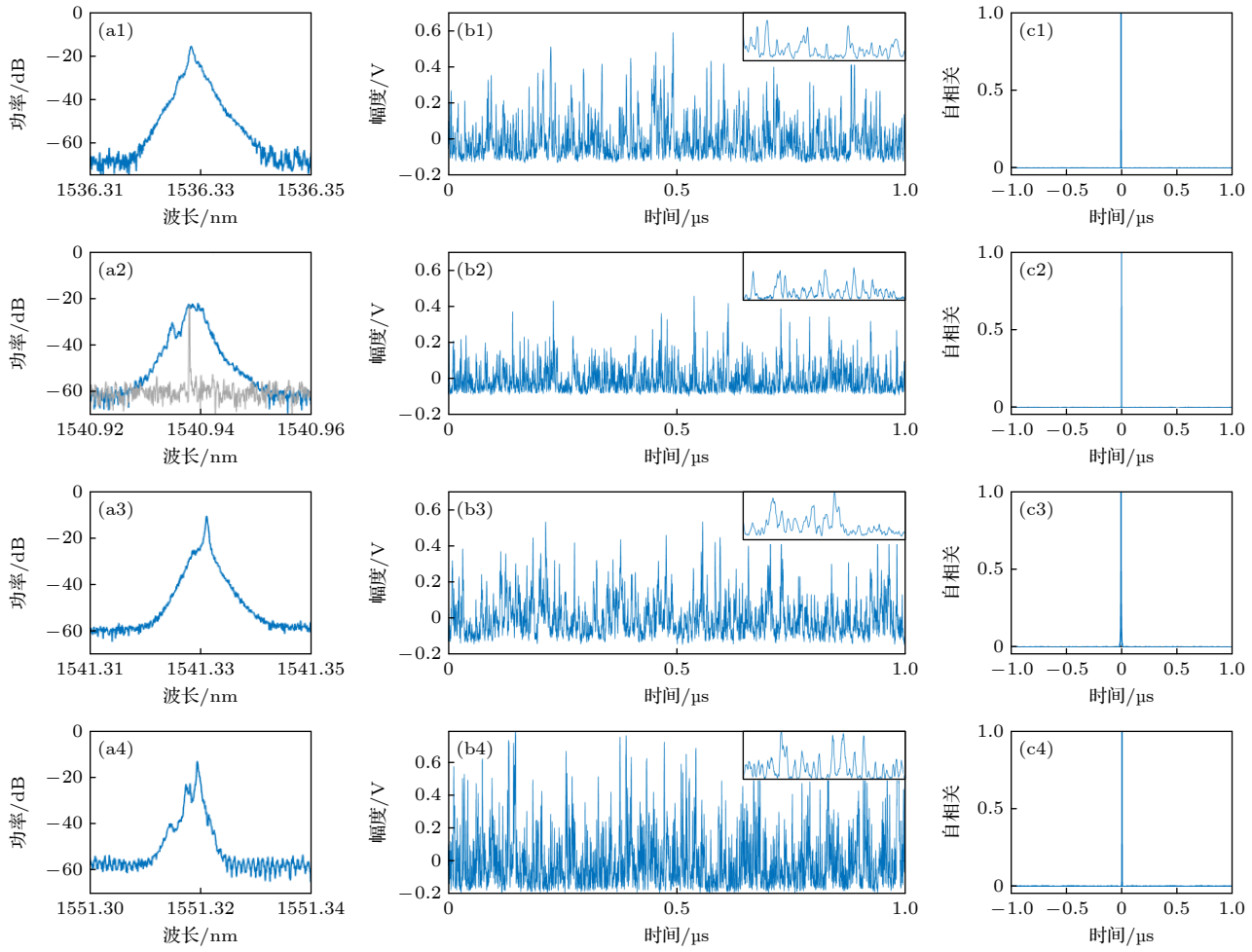

图 2 不同波长单信道梳齿的光谱、对应的时间序列和时间序列的自相关 (a1), (b1), (c1) 1536.33 nm; (a2), (b2), (c2) 1540.94 nm, 其中蓝色曲线表示混沌态, 灰色曲线表示稳定态; (a3), (b3), (c3) 1541.33 nm; (a4), (b4), (c4) 1551.32 nm

Fig. 2. The spectrum of a single optical frequency comb with different wavelengths, the corresponding time sequence, and the auto-correlation of time sequence: (a1), (b1), (c1) 1536.33 nm; (a2) , (b2), (c2) 1540.94 nm, the blue curve represents the chaotic state, while the grey curve represents the stable state; (a3), (b3), (c3) 1541.33 nm; (a4), (b4), (c4) 1551.32 nm.

于混沌态输出, 且未含有时延特征. 其中需要说明的是, 在各混沌梳齿中, 与泵浦对称的梳齿间存在由四波混频引起的相关性[35], 因此在进一步的实时随机数提取过程中, 应规避这些具有显著相关性的梳齿.

4 实时随机数提取与测评

光混沌梳齿的熵源后处理方法流程如图 3(a)所示. 超宽带光频梳通过多路分配器得到不同波长的梳齿, 每个梳齿由光电探测器 (PD) 滤波和收集. 集成在 FPGA 板卡上的 ADC 采用外部输入时钟信号进行时钟同步处理, 最大采样率为 1.25 G/s, FPGA 对 ADC 进行实时同步控制. ADC 对混沌信号的采样方式为并行采样, 这种方法能够提高数据处理效率. ADC 并行采样量化得到的 8 路比特序列通过串并转换合并为一路比特序列, FPGA 将该序列分别送入两个通道进行延时和反转, 随后将两组数据按位异或, 随后保留 4 位最低有效位, 最终生成单信道速率 5 Gbits/s 实时 PRN. 图 3(b)展示了熵源信号经采样量化后的统计特性分布情况. 可以看出在 8 位的采样量化下, 熵源信号的柱状图呈类高斯曲线状分布, 且存在明显的非对称性. 图 3(c) 展示了经过 4-LSB 处理后的比特序列生成的二维黑白图像, 图像大小为 1000 × 1000. 在图像中, 我们使用白点表示比特位“1”, 使用黑点表示比特位“0”, 在这张二维图像中黑白点的分布均匀, 无明显规律性纹理. 图 3(d) 展示的是经后处理的随机比特序列直方图. 如图所示, 保留 4 位最低有效位的情况下生成数据序列的直方图分布

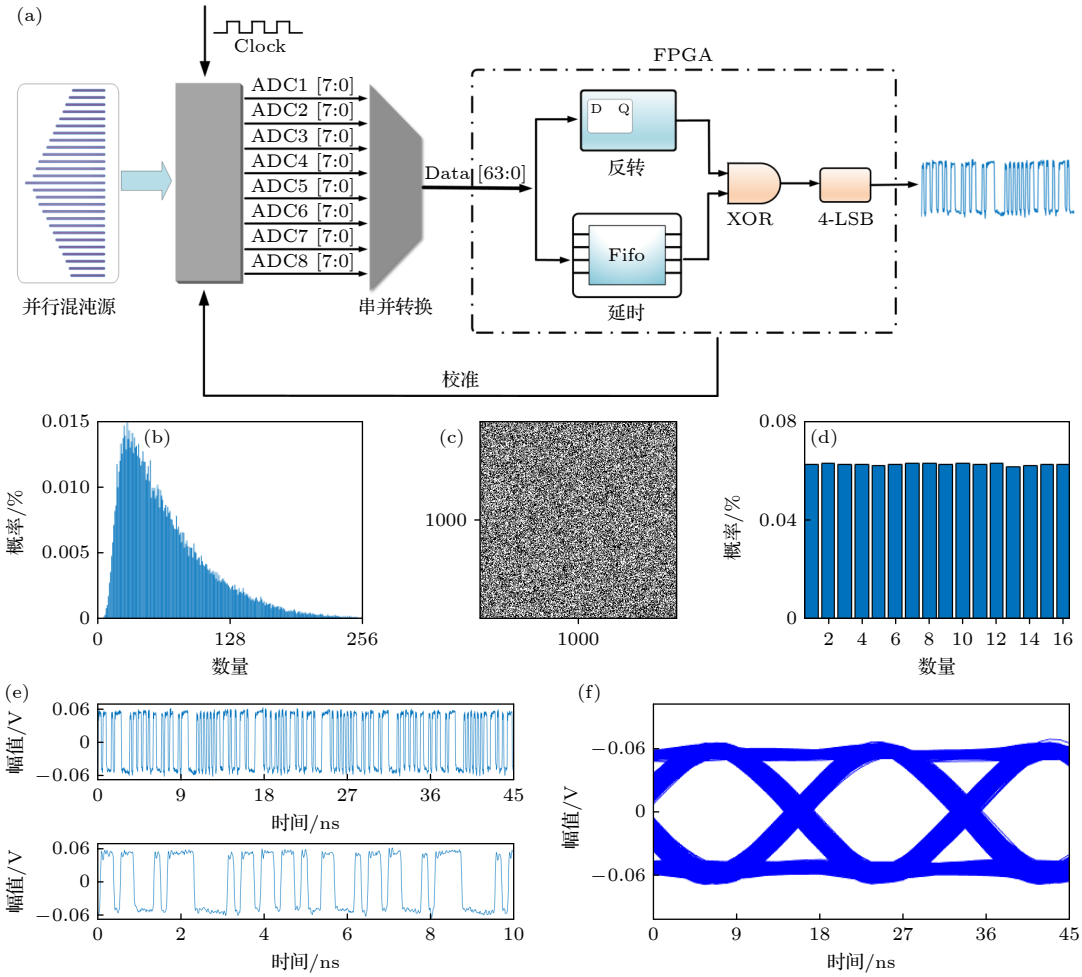

图 3 实时随机位的生成 (a) 混沌梳齿熵源实时后处理流程图; (b) 熵源采样量化后序列的直方图; (c) 4-LSB 处理下比特序列前 1 M 点的二维图, 格式为 1000×1000, 其中位“1”和位“0”分别转换为白点和黑点; (d) 提取的 4-LSB 分布直方图; (e) 随机比特的码型图; (f) 随机比特对应的眼图

Fig. 3. Generation of real-time random bits: (a) Flow chart of real-time post-processing for the entropy source of chaotic comb tooth; (b) entropy source sampled and quantized sequence histograms; (c) two-dimensional graph generated the first 1 M points in the bits sequence under 4-LSB processing in the form of 1000×1000, where bits“1”and bits“0”are converted into white and black dots, respectively; (d) histograms of distribution of the extracted 4-LSB; (e) temporal waveforms of random bits; (f) eye diagram of random bits.

十分均衡, 这有利于 PRN 的生成. 实验得到 PRN 生成的实时码型图和对应的细节图如图 3(e)所示, 通过码型图可以看出, PRN 的生成速率为 5 Gbits/s, 码型图正负电压分布对称, 峰峰值电压为 1.2 V. 图 3(f) 给出与码型图对应的眼图. 如图所示, 眼图打开良好, 表明生成的实时 PRN 序列性能良好.

基于各信道混沌熵源最终生成的 PRN 还必须通过 NIST SP 800-22 统计检验套件的评估, 以确保输出随机数的质量达标. 图 4 展示了随机选择的波长为 1536, 1540, 1541, 1551 nm 的 4 个梳齿的混沌输出作为熵源所生成的 PRN 统计检验结果, 后处理均保留了 4 位最低有效位. 4 个梳齿所生成的 PRN 均完全通过了 NIST 套件的全部 15 项测试. 由于本文中所述光频梳在 1430—1675 nm 范围内含有 294 个处于混沌态的梳齿, 这些梳齿的输出经滤波提取后作为独立的混沌熵源, 因此该实验系统所生成的实时 PRN 的数据吞吐量上限有望达到 1.74 Tbits/s (5 Gbits/s×294 = 1.47 Tbits/s).

5 结 论

本文展示了一种基于片上 Si_3N_4 微环的混沌光频梳并结合现场可编程门阵列产生并行超高速实时随机数的实施方案. 首先, 深入研究了一种自由频谱范围为 100 GHz, 覆盖 1430—1675 nm 高度并行化的混沌源, 其可以同时产生 294 个不同波长的信道. 随后, 实验验证了混沌态下光频梳提取大

Statistical test	1536 nm		
	P-value	Proportion	Result
Frequency	0.042808	0.983	Success
Block frequency	0.217857	0.994	Success
Cumulative sums	0.008691	0.983	Success
Runs	0.024855	0.987	Success
Longest run	0.190654	0.989	Success
Rank	0.060875	0.992	Success
FFT	0.159020	0.988	Success
Non overlapping template	0.249284	0.983	Success
Overlapping template	0.319084	0.986	Success
Universal	0.803720	0.995	Success
Approximate entropy	0.641284	0.992	Success
Random excursions	0.458216	0.980	Success
Random excursions variant	0.006393	0.980	Success
Serial	0.055361	0.993	Success
Linear complexity	0.139655	0.990	Success

Statistical test	1540 nm		
	P-value	Proportion	Result
Frequency	0.390721	0.985	Success
Block frequency	0.009333	0.989	Success
Cumulative sums	0.328297	0.984	Success
Runs	0.168112	0.984	Success
Longest run	0.552383	0.990	Success
Rank	0.643366	0.988	Success
FFT	0.655854	0.984	Success
Non overlapping template	0.108791	0.981	Success
Overlapping template	0.510153	0.989	Success
Universal	0.190654	0.987	Success
Approximate entropy	0.583145	0.991	Success
Random excursions	0.560780	0.982	Success
Random excursions variant	0.432747	0.987	Success
Serial	0.205531	0.987	Success
Linear complexity	0.825505	0.991	Success

Statistical test	1541 nm		
	P-value	Proportion	Result
Frequency	0.093720	0.980	Success
Block frequency	0.340858	0.985	Success
Cumulative sums	0.250558	0.981	Success
Runs	0.260930	0.988	Success
Longest run	0.892036	0.982	Success
Rank	0.160805	0.992	Success
FFT	0.037813	0.993	Success
Non overlapping template	0.506194	0.981	Success
Overlapping template	0.203351	0.984	Success
Universal	0.277082	0.987	Success
Approximate entropy	0.075254	0.992	Success
Random excursions	0.340803	0.978	Success
Random excursions variant	0.864660	0.986	Success
Serial	0.556460	0.985	Success
Linear complexity	0.934599	0.989	Success

Statistical test	1551 nm		
	P-value	Proportion	Result
Frequency	0.006906	0.985	Success
Block frequency	0.106246	0.993	Success
Cumulative sums	0.153763	0.987	Success
Runs	0.979788	0.989	Success
Longest run	0.727851	0.993	Success
Rank	0.064822	0.986	Success
FFT	0.769527	0.989	Success
Non overlapping template	0.352107	0.982	Success
Overlapping template	0.788728	0.984	Success
Universal	0.689019	0.992	Success
Approximate entropy	0.536163	0.993	Success
Random excursions	0.986256	0.985	Success
Random excursions variant	0.708385	0.980	Success
Serial	0.106877	0.988	Success
Linear complexity	0.268917	0.986	Success

图 4 保留 4-LSB 下, 波长在 1536, 1540, 1541, 1551 nm 的混沌梳齿输出所产生的 PRN 的 NIST 测试结果

Fig. 4. Results of NIST tests for PRN generated by the output signals of chaotic comb tooth with wavelength of 1536, 1540, 1541, and 1551 nm under 4-LSB reservation.

规模并行混沌熵源的能力. 通过将多个混沌梳齿分别进行滤波, 能够获得多路高质量无时延特征的混沌熵源信号. 利用 8 位 ADC 分别对各熵源信号进行采样量化, 获得的初始比特数据流再通过 FPGA 实时进行后处理并保留 4 位 LSB, 最终产生每路通道速率达 5 Gbits/s 的实时 PRN. 随机抽取多个梳齿所产生的 PRN 进行统计检验, 均成功通过了 NIST 统计检验套件的测试. 考虑到该方案能同时获取 294 路混沌熵源, 因此生成的实时 PRN 的数据吞吐量上限可望达到 1.74 Tbits/s. 本文实验结果开拓性地为高并行度、低成本的超快速实时 PRN 生成提供了可行的集成解决方案.

参考文献

[1] Argyris A, Syvridis D, Larger L, Annovazzi-Lodi V, Colet P, Fischer I, Garcia-Ojalvo J, Mirasso C, Pesquera L, Shore K A 2005 *Nature* **438** 343

[2] Wang L S, Mao X X, Wang A B, Wang Y C, Gao Z S, Li S S, Yan L S 2020 *Opt. Lett.* **45** 4762

[3] Garcia-Ojalvo J, Roy R 2001 *Phys. Rev. Lett.* **86** 5204

[4] Gao H, Wang A B, Wang L S, Jia Z W, Guo Y Y, Gao Z Z, Yan L S, Qin Y W, Wang Y C 2021 *Light. Sci. Appl.* **10** 172

[5] Feng W Z, Jiang N, Zhang Y Q, Jin J Y, Zhao A K, Liu S Q, Qiu K 2022 *Opt. Express* **30** 4782

[6] Cheng C H, Chen Y C, Lin F Y 2015 *IEEE Photon. J.* **8** 1

[7] Lin F Y, Liu J M 2004 *IEEE J. Sel. Top. Quant. Electron.* **10** 991

[8] Chen J D, Wu K W, Ho H L, Lee C T, Lin F Y 2022 *IEEE J. Sel. Top. Quant. Electron.* **28** 1

[9] Uchida A, Amano K, Inoue M, Hirano K, Naito S, Someya H, Oowada I, Kurashig T, Shiki M, Yoshimori S, Yoshimura K, Davis P 2008 *Nat. Photonics* **2** 728

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

[11] Hirano K, Yamazaki T, Morikatsu S, Okumura H, Aida H, Uchida A, Yoshimori S, Yoshimura K, Harayama T, Davis P 2010 *Opt. Express* **18** 5512

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

[13] Zhang L, Pan B, Chen G, Guo L, Lu D, Zhao L, Wang W 2017 *Sci. Rep.* **7** 1

[14] Wu J G, Tang X, Wu Z M, Xia G Q, Feng G Y 2012 *Laser. Phys.* **22** 1476

[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] Han Y N, Xiang S Y, Wang Y, Wang Y T, Wang B, Wen A J, Hao Y 2020 *Photon. Res.* **8** 1792

[17] Zhao A K, Jiang N, Peng J F, Liu S Q, Zhang Y Q, Qiu K 2022 *Opto-Electron. Adv.* **5** 200026

[18] Wu J C, Song Z, Xie Y F, Zou X Y, Zou F, Mu P H, Li N Q 2021 *Acta Phys. Sin.* **70** 104205 (in Chinese) [吴佳辰, 宋峥, 谢溢锋, 周心雨, 周沛, 穆鹏华, 李念强 2021 物理学报 **70** 104205]

[19] Cai Q, Li Q, Shi Y C, Jia Z W, Ma L, Xu B J, Chen X F, Shore A K, Wang Y C 2023 *Opt. Laser. Technol.* **162** 109273

[20] Shi B L, Luo C W, Flores J G F, Lo G Q, Kwong D L, Wu J G, Wong C W 2020 *Opt. Express* **28** 36685

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

[22] 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]

[23] Li P, Li K Y, Guo X M, Guo Y Q, Liu Y M, Xu B J, Bogris A, Shore A K, Wang Y C 2019 *Opt. Lett.* **44** 2447

[24] Qiao L J, Lv T S, Xu Y, Zhang M J, Zhang J Z, Wang T, Zhou R K, Wang Q, Xu H C 2019 *Opt. Lett.* **44** 5394

[25] 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** 1

[26] Li X Z, Chan S C 2013 *IEEE. J. Quantum. Electron.* **49** 829

[27] Ji X C, Yao X W, Klenner A, Gan Y, Gaeta A L, Hendon C P, Lipson M 2019 *Opt. Express* **27** 19896

[28] Marchand P J, Riemensberger J, Skehan J C, Ho J J, Pfeiffer M H P, Liu J Q, Hauger C, Lasser T, Kippenberg T J 2021 *Nat. Commun.* **12** 427

[29] Wang L S, Zhao T, Wang D M, Wu D L, Zou L, Wu J, Liu X Y, Wang A B 2017 *Acta Phys. Sin.* **66** 234205 (in Chinese) [王龙生, 赵彤, 王大铭, 吴旦昱, 周磊, 武锦, 刘新宇, 王安帮 2017 物理学报 **66** 234205]

[30] Ugagin K, Terashime Y, Iwakawa K, Uchida A, Harayama T, Yoshimura K, Inubushi M 2017 *Opt. Express* **25** 6511

[31] Yang J, Liu J N, Su Q, Li Z Y, Fan F, Xu B J, Guo H 2016 *Opt. Express* **24** 27475

[32] Peccianti M, Pasquazi A, Park Y, Little B E, Chu S T, Moss D J, Morandotti R 2012 *Nat. Commun.* **3** 765

[33] Chang L, Liu S, Bowers J E 2022 *Nat. Photonics* **16** 95

[34] Xiao Z Y, Li T, Cai M, Zhang H, Huang Y, Li C, Yao B, Wu K, Chen J 2023 *Light Sci. Appl.* **12** 33

[35] Shen B T, Shu H W, Xie W Q, Chen R X, Liu Z, Ge Z F, Zhang X G, Wang Y M, Zhang Y H, Cheng B W, Yu S H, Chang L, Wang X J 2023 *Nat. Commun.* **14** 4590

A Tbit/s parallel real-time physical random number scheme based on chaos optical frequency comb of Si_3N_4 micro-ring*

Wang Yong-Bo [1)2)#] Tang Xi [1)2)#] Zhao Le-Han [1)2)#] Zhang Xin [1)2)]
Deng Jin [1)2)] Wu Zheng-Mao [1)2)] Yang Jun-Bo [4)] Zhou Heng [3)†]
Wu Jia-Gui [1)2)‡] Xia Guang-Qiong [1)2)††]

1) (*School of Physical Science and Technology, Southwest University, Chongqing* 400715, *China*)
2) (*Chongqing Key Laboratory of Micro & Nano Structure Optoelectronics, Southwest University, Chongqing* 400715, *China*)
3) (*Key Lab of Optical Fiber Sensing and Communication Networks, University of Electronic Science and Technology of China, Chengdu* 610097, *China*)
4) (*Center of Material Science, National University of Defense Technology, Changsha* 410073, *China*)

(Received 5 December 2023; revised manuscript received 18 January 2024)

Abstract

Physical random numbers (PRNs) own various advantageous characteristics, including unpredictability, non-repeatability, higher security and reliability. Meanwhile, laser chaos has attracted great attention in the field of PRN. In terms of single channel PRN, laser chaos schemes can achieve a much higher bit-rate than traditional quantum PRN schemes. So far, various laser chaos PRN schemes have been discussed in order to enhance the performance of single channel laser chaos PRN. However, considering the limited bandwidth of laser chaos, especially the bandwidth of digital electronic circuit, the development potential of single channel PRN should be limited and may fall into the trap of high performance and expensive cost. Recently, the applications of multi-channel parallel PRN schemes have been developed. These parallel types may balance the high performance of PRN in a low cost. Recent progress indicates that chaotic micro-comb may have good potential. The micro-comb exhibits highly nonlinear and complex dynamic characteristics, and each comb tooth may show chaotic oscillation. The wavelength division multiplexing technology enables large-scale optical parallel output, providing the possiblity for large-scale parallel PRN generation. However, most of these PRN schemes are offline rather than true online and real-time random numbers. Thus, the development of real, online real-time parallel PRN solutions has great interest and research value in related fields.

Herein we experimentally demonstrat an ultra-high-speed parallel real-time physical random number generator, which is achieved though the combination of chaotic micro-comb of chip-scale Si_3N_4 ultra-high Q micro-resonator and a high-speed field programmable gate array (FPGA). The results show that the Si_3N_4 ultra-high Q micro-resonator generates a micro-comb with hundreds of channels, each channel can route into an optically chaotic state, and become an excellent physical entropy source. Using FPGA onboard multi-bit analog-to-digital converter, the filtered optical chaos signal from the micro-comb is discretely sampled and quantized, and resulting in an 8-bit binary bitstream. Taking real-time self-delayed exclusive or (XOR) processing of bitstream and preserving 4 least significant bits, the qualified physical random bitstream with real-time 5 Gbits/s rate is realized experimentally. Considering that there are 294 chaotic comb teeths, our approach anticipates a throughput of 1.74 Tbits/s of real-time physical random bits. Our results could offer a new integrated and ultra-high-speed option for real-time physical random number sources.

Keywords: physical random number, real-time, chaos, optical frequency comb, field programmable gate array

PACS: 42.65.–k, 05.45.Gg, 05.45.Vx **DOI:** 10.7498/aps.73.20231913

* Project supported by the National Natural Science Foundation of China (Grant Nos. 61775184, 61875167), the Science Funds for Distinguished Young Scientists of Chongqing, China (Grant No. cstc2021jcyj-jqX0027), and the Innovation Research 2035 Pilot Plan of Southwest University, China (Grant No. SWU-XDPY22012).

# These authors contributed equally.
† Corresponding author. E-mail: zhouheng@uestc.edu.cn
‡ Corresponding author. E-mail: mgh@swu.edu.cn
†† Corresponding author. E-mail: gqxia@swu.edu.cn

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

基于Si_3N_4微环混沌光频梳的Tbit/s并行实时物理随机数方案

王永博 唐曦 赵乐涵 张鑫 邓进 吴正茂 杨俊波 周恒 吴加贵 夏光琼

A Tbit/s parallel real-time physical random number scheme based on chaos optical frequency comb of Si_3N_4 micro-ring

Wang Yong-Bo Tang Xi Zhao Le-Han Zhang Xin Deng Jin Wu Zheng-Mao Yang Jun-Bo Zhou Heng Wu Jia-Gui Xia Guang-Qiong

引用信息 Citation: Acta Physica Sinica, 73, 084203 (2024) DOI: 10.7498/aps.73.20231913
在线阅读 View online: https://doi.org/10.7498/aps.73.20231913
当期内容 View table of contents: http://wulixb.iphy.ac.cn